The Indonesian Journal of Computer Science
www.ijcs.net
Volume 15, Issue 1, February 2026
https://doi.org/10.33022/ijcs.v15i1.5069

A Forensic-Ready Virtual Currency Reward Framework for Metaverse-Based Work Environments

Shelley-Anne Robertson[1], Stacey Omeleze Baror[2], Hein Salomon Venter[3]
shelley.robertson@tuks.co.za[1], stacey.baror@tuks.co.za[2], hventer@cs.up.ac.za[3]
[1,2,3] University of Pretoria, South Africa

Article Information

Received : 5 Jan 2026
Revised : 10 Feb 2026
Accepted : 20 Feb 2026

Keywords

Metaverse, Virtual Currency, Digital Forensic Readiness, Reward Systems, Motivation-Aware Incentives

Abstract

As immersive and distributed work environments expand within metaverse platforms, organisations face increasing challenges in maintaining trust, accountability, and integrity in digital reward systems. Virtual currency–based incentives offer flexibility and scalability but introduce risks related to integrity, dispute resolution, and evidentiary reliability. Existing approaches often rely on blockchain immutability alone, which is insufficient to support proactive preservation of digital evidence within reward systems. This paper proposes a forensic-ready architectural framework for virtual currency–based organisational reward systems, in which Digital Forensic Readiness is embedded as a core system design principle rather than a post-hoc security layer. The Metaward framework integrates motivational event instrumentation, forensic logging, traceability, and governance mechanisms to generate verifiable digital traces during normal operation. A conceptual instantiation and scenario-based analysis, supported by an illustrative proof-of-concept instantiation, demonstrate the feasibility of the proposed approach within metaverse-based work environments.

A. Introduction

The increasing adoption of digitally mediated and immersive work environments has expanded organisational reliance on virtual platforms for collaboration, task execution, and performance management. Beyond conventional collaboration tools, immersive virtual environments, commonly referred to as the Metaverse, are emerging as potential digital workplaces that enable persistent interaction, social presence, and new forms of value exchange [1], [2]. While such environments offer novel opportunities for engagement, they also challenge established approaches to employee motivation, accountability, and trust.

Reward systems have long been used to support motivation, engagement, and performance in organisational contexts [3]–[8]. In digitally mediated environments, however, traditional incentive mechanisms often lose effectiveness due to reduced visibility of effort, limited social feedback, and weakened perceptions of fairness. As a result, virtual currencies have gained attention as flexible and programmable reward instruments capable of supporting participation and engagement in online and immersive contexts [9], [10]. Although extensively explored in gaming and consumer platforms, the application of virtual currencies as organisational reward mechanisms remains underexamined, particularly with respect to governance, security, and evidentiary reliability [10].

As organisational activity migrates into immersive and distributed environments, risks related to integrity, traceability, and dispute resolution become more pronounced [11], [12]. Actions that influence incentives, such as task completion, validation, reward allocation, ranking updates, and penalty enforcement, generate digital traces that may later be contested. Conventional digital forensic approaches are predominantly reactive, focusing on post-incident investigation rather than proactive evidence preservation [13]-[16]. In environments characterised by ephemeral and system-mediated interactions, this reactive posture is increasingly insufficient.

Blockchain technologies have been widely proposed as integrity mechanisms for digital transactions due to their tamper-resistant and decentralised nature [17], [18]. Incentive systems built on blockchain infrastructures benefit from enhanced transparency and non-repudiation, enabling verification of transactional histories without reliance on a central authority. However, while blockchain ensures immutability of recorded transactions, it does not inherently capture the contextual, procedural, or causal information required for comprehensive forensic analysis [15], [16], [19], [20]. As a result, blockchain-based reward systems often address integrity but fall short of supporting evidentiary readiness, governance, and dispute resolution.

Digital Forensic Readiness (DFR) addresses these limitations by advocating proactive preparation for the identification, collection, preservation, and protection of potential digital evidence before incidents occur [14], [15], [16], [21]. Core DFR principles include structured evidence identification, secure and verifiable logging, controlled access to forensic artefacts, and policy-driven evidence management. DFR frameworks have been proposed for a range of organisational contexts, including cloud environments and enterprise information systems, emphasising the integration of forensic capabilities directly into system architectures rather than treating them as external monitoring functions [15], [16].

Despite its relevance, DFR is seldom embedded into motivational or incentive-driven systems. Existing organisational reward platforms prioritise engagement and visibility but typically treat auditability and evidentiary preservation as secondary concerns. Conversely, standalone DFR frameworks focus on security and compliance without accounting for incentive-driven interactions that directly influence behaviour. This separation represents a significant gap in Metaverse-based work environments, where rewards, rankings, and disciplinary actions occur entirely within digital systems and where disputes over incentives may carry organisational or legal consequences [22].

To address this gap, this paper proposes a conceptual framework, referred to as Metaward, that integrates Digital Forensic Readiness into a virtual currency-based organisational reward system designed for Metaverse-based work environments. Rather than introducing forensic mechanisms as an external security layer, the framework embeds forensic logging, traceability, and governance controls directly into reward-related workflows. An illustrative instantiation and scenario-based analysis are used to demonstrate the feasibility of the proposed approach and to show how forensic readiness can coexist with motivational design principles such as recognition, competition, and reward flexibility. The primary contribution of this work is a forensic-ready incentive architecture that aligns motivation, accountability, and evidentiary assurance within immersive digital work environments.

Unlike prior forensic-ready system models, Metaward embeds evidentiary generation directly into incentive-driven workflows, aligning motivational design and forensic preparedness within the same operational processes.

B. Research Method

This research adopts a design-oriented methodology to develop and examine a forensic-ready virtual currency–based reward system for Metaverse-based work environments [23] The approach focuses on conceptual system design and illustrative instantiation rather than empirical performance evaluation, consistent with the framework-oriented nature of the study.

The research process comprised three primary stages. First, design requirements were derived from an analysis of existing literature on organisational reward systems, virtual currencies in immersive environments, blockchain-based integrity mechanisms, and Digital Forensic Readiness (DFR). These requirements informed the identification of motivational, forensic, and governance concerns relevant to digitally mediated work environments.

Second, a conceptual system architecture, referred to as the Metaward framework, was developed. The framework integrates motivational reward mechanisms with proactive forensic readiness by embedding evidence generation directly into reward-related workflows. Rather than introducing forensic capabilities as a standalone monitoring or security layer, the design positions DFR as a foundational system principle. Reward-related actions, such as task completion, validation outcomes, reward allocation, ranking updates, and penalty enforcement, are explicitly identified as potential evidence-generating events and are instrumented to produce verifiable digital traces during normal system operation. The design of the Metaward framework draws on prior research in

immersive digital work environments, virtual currency–based incentive systems, and forensic-ready system architectures [1], [2], [10], [15], [16], [19], [21].

The Metaward framework is organised into three interacting conceptual layers, reflecting established approaches to incentive-based system design, forensic readiness by design, and governance-driven integrity control in distributed digital environments [3], [5], [17], [18], [22]. The motivational layer is responsible for task management, incentive logic, recognition mechanisms, and user-facing reward structures. The forensic readiness layer identifies, captures, and preserves potential digital evidence associated with reward-related events, including relevant metadata such as timestamps, user identifiers, and outcome states. The governance and integrity layer enforces policies governing access control, evidence retention, and integrity protection, ensuring alignment with organisational and regulatory requirements.

Table 1. Metaward Framework Layers and Responsibilities

Conceptual Layer	**Primary Responsibilities**	**Functional Focus**	**Outputs / Artefacts**
Motivational Layer	Task definition, assignment, validation, and incentive logic	Management of reward structures, badges, penalties, and ranking mechanisms	Task records, reward allocations, penalty outcomes, ranking updates
Forensic Readiness Layer	Identification, capture, and preservation of reward-related digital evidence	Event logging, metadata generation, traceability, and evidence lifecycle management	Event logs, timestamps, user identifiers, state transitions
Governance and Integrity Layer	Enforcement of policies governing access control, integrity, and evidence retention	Policy definition, validation checks, alert triggering, and integrity protection	Policy rules, audit constraints, alerts, evidence retention controls

Figure 1 presents an illustrative workflow-based instantiation of these layers, demonstrating how forensic readiness mechanisms augment reward-related processes during system operation rather than depicting the layers as separate structural components.

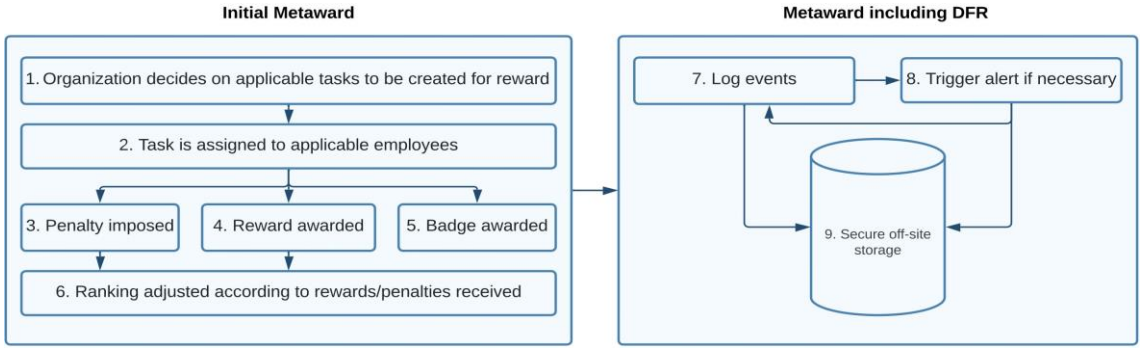

Figure 1. Workflow-based instantiation of the Metaward framework showing the integration of digital forensic readiness mechanisms into reward-related processes.

Third, the framework was examined through an illustrative instantiation and a set of scenario-based analyses. The instantiation maps the conceptual layers of the framework to a minimal set of functional components without prescribing a specific technology stack or deployment model. Its purpose is to demonstrate technical and logical feasibility rather than to provide a production-ready system or reusable artefact.

The scenarios represent common organisational interactions in digitally mediated work environments, including task completion and reward allocation, ranking updates and recognition, and penalty enforcement following policy violations. Each scenario traces the interaction between motivational mechanisms and forensic readiness components, illustrating how evidentiary integrity and traceability are preserved throughout the lifecycle of reward-related events, as shown in Figure 2 [1], [2], [4], [10], [15], [16], [19], [21]. By analysing these scenarios, the research evaluates whether forensic readiness can be embedded into incentive-driven workflows without disrupting motivational effectiveness or introducing intrusive monitoring.

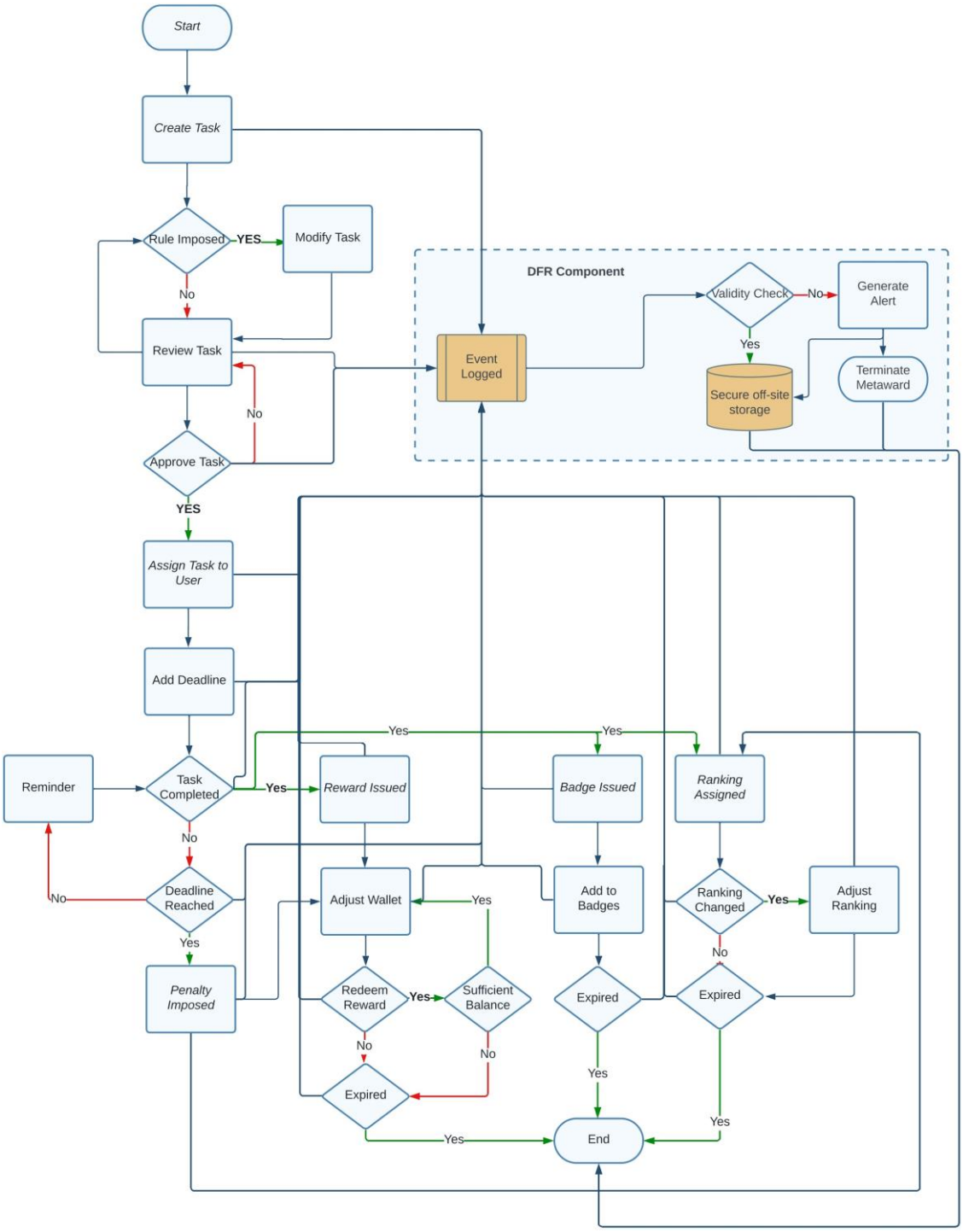

Figure 2. Reward lifecycle and event flow illustrating the integration of digital forensic readiness mechanisms into task execution, incentive allocation, and ranking adjustment processes.

To operationalise forensic readiness within the Metaward framework, reward-related events are explicitly mapped to corresponding forensic artefacts and metadata to support traceability, integrity, and post-event analysis.

Table 2. Mapping of Reward-Related Events to Forensic Artefacts in the Metaward Framework

Reward-Related Event	Forensic Artefact Generated	Captured Metadata	Forensic Purpose
Task assignment	Assignment event log	Task ID, user ID, timestamp, task parameters	Establish accountability for task allocation
Task completion	Completion record	Task ID, user ID, completion time, outcome state	Verify claims of task completion
Task validation	Validation decision log	Validator ID, decision outcome, timestamp	Support dispute resolution
Reward allocation	Reward transaction record	Reward type, amount, recipient ID, timestamp	Trace incentive distribution
Penalty enforcement	Penalty execution record	Penalty type, violated rule, timestamp	Demonstrate policy enforcement
Ranking update	Ranking state-change log	Previous rank, new rank, triggering event	Reconstruct incentive impact
Policy violation	Alert and violation record	Rule ID, violation context, system state	Enable proactive investigation

This design-based methodology enables examination of the Metaward framework's alignment with its stated objectives—motivational effectiveness, forensic readiness by design, transparency and accountability, and architectural separation of concerns—while remaining consistent with the conceptual scope of the research.

C. Result and Discussion

This section presents and discusses the results derived from the design-oriented evaluation of the Metaward framework. As the study adopts a conceptual and illustrative methodology rather than empirical experimentation, results are expressed in terms of **architectural properties, behavioural guarantees, and evaluative outcomes** observed through scenario-based analysis. The evaluation focuses on whether the framework satisfies its stated design objectives when applied to representative organisational reward scenarios in metaverse-based work environments.

The framework was evaluated against four primary criteria derived from the research objectives and methodological design:

1. **Forensic readiness by design**, assessed through the ability to generate and preserve verifiable digital evidence during normal system operation;
2. **Traceability and transparency**, evaluated by examining whether reward-related actions can be reconstructed and audited post hoc;

3. **Motivational compatibility**, assessed by determining whether forensic instrumentation interferes with or alters incentive mechanisms; and
4. **Governance and integrity support**, evaluated through the enforceability of policies and accountability controls embedded within the framework.

Each scenario was evaluated against these criteria to assess whether forensic accountability emerged as a by-product of normal reward system operation, rather than as an externally imposed monitoring mechanism.

Scenario-Based Evaluation Outcomes

To examine these criteria, the Metaward framework was analysed using three representative organisational scenarios: task completion and reward allocation, ranking updates and recognition, and policy violation with penalty enforcement [22]. The evaluation results are summarised in Table 3.

Across all scenarios, the framework demonstrated **consistent forensic readiness properties**. Reward-related actions were successfully identified as evidence-generating events, producing structured logs and artefacts containing sufficient metadata to support post-event analysis. This indicates that forensic readiness can be embedded as a foundational design principle without relying on ad hoc monitoring or retrospective data collection, aligning with prior work on forensic-ready software systems and secure evidence preservation [16], [19], [21], [22], [24].

From a transparency perspective, the scenarios show that ranking changes, reward allocations, and penalties can be reconstructed in a verifiable manner. This supports dispute resolution and auditability, addressing a known limitation of incentive systems that rely solely on immutable ledgers without contextual traceability [1], [17], [18]. Importantly, the scenario analysis indicates that forensic instrumentation operates alongside motivational mechanisms rather than replacing or constraining them, preserving the behavioural intent of reward-based engagement systems [3], [9], [10].

Governance and integrity outcomes were also observed across scenarios. Policy violations triggered auditable enforcement actions, and penalty execution was accompanied by preserved evidentiary records [22], [25]. Such governance mechanisms align with established information security and organisational control standards that emphasise policy definition, enforcement, and accountability as foundational elements of secure system design [26]. This supports organisational accountability while reducing reliance on manual investigation processes. These results are consistent with design-oriented approaches to governance-aware system architectures and reinforce the feasibility of integrating policy enforcement and forensic readiness within distributed reward systems [15], [16], [22], [25], [27].

Table 3. Scenario-Based Evaluation of the Metaward Framework

Scenario	Motivational Mechanism	Forensic Readiness Support	Evaluated Outcome
Task completion	Virtual currency	Event logging	Verifiable proof of task

Scenario	Motivational Mechanism	Forensic Readiness Support	Evaluated Outcome
and reward allocation	incentive	and secure evidence storage	fulfilment and reward justification
Ranking update and recognition	Competitive ranking and recognition mechanisms	Traceable ranking state changes	Transparent reconstruction of ranking outcomes
Policy violation and penalty enforcement	Penalty and loss of incentives	Alert generation and evidentiary capture	Auditable enforcement of organisational rules

Critical Reflection and Limitations

While the results demonstrate that the Metaward framework satisfies its core design objectives, several limitations should be acknowledged. First, the evaluation is conceptual and illustrative, and does not quantify system performance, scalability, or storage overhead associated with forensic instrumentation. Second, the effectiveness of forensic readiness is contingent on correct and consistent implementation of logging and governance mechanisms, which may vary across deployments. Finally, the framework assumes organisational commitment to policy definition and enforcement; misconfigured or weak governance controls could reduce evidentiary value despite the presence of forensic-ready design.

These limitations do not diminish the conceptual contribution of the work but instead highlight areas for future empirical evaluation and system-level optimisation. Within the scope of this study, the results demonstrate that integrating Digital Forensic Readiness into virtual currency–based reward systems is both technically feasible and architecturally compatible with motivational design goals in metaverse-based work environments.

The scenario-based evaluation is intended to assess architectural feasibility and evidentiary coherence rather than to measure behavioural impact, user adoption, or system performance, which are left for future empirical investigation.

D. Conclusion

This paper addressed the challenge of sustaining employee motivation while ensuring accountability and evidentiary trust in digitally mediated and immersive work environments. As organisations increasingly explore Metaverse-based platforms for collaboration and productivity, conventional reward systems and reactive digital forensic approaches prove insufficient when applied in isolation.

The primary contribution of this work is the integration of Digital Forensic Readiness (DFR) into a virtual currency–based organisational reward system. By treating reward-related interactions as potential sources of digital evidence and embedding forensic readiness directly into incentive workflows, the proposed Metaward framework shifts forensic preparedness from a reactive activity to a proactive system design principle. This approach enables organisations to

preserve evidentiary integrity, support dispute resolution, and strengthen accountability without disrupting motivational effectiveness.

Through an illustrative instantiation and scenario-based analysis, the study demonstrated the feasibility of embedding forensic readiness into incentive-driven workflows operating in immersive digital environments. The results show that motivational mechanisms, governance controls, and forensic instrumentation can coexist within a unified architectural framework, reinforcing trust and transparency while maintaining engagement.

Overall, the Metaward framework contributes a forensic-ready incentive architecture suitable for Metaverse-based work environments, addressing a critical gap in existing research by aligning motivation, accountability, and evidentiary assurance within a single system design.

E. Acknowledgment

The author would like to acknowledge the support and guidance received during the completion of the Master's research from which this work is derived. Appreciation is extended to the academic supervisors and colleagues whose feedback contributed to the development of the concepts presented in this paper. The author also acknowledges the institutional support provided during the course of the research.

F. References

[1] M. Xu, Y. Guo, Q. Hu, Z. Xiong, D. Yu, and X. Cheng, "A trustless architecture of blockchain-enabled metaverse," High-Confidence Computing, vol. 3, no. 1, p. 100088, 2023.

[2] T. R. Gadekallu et al., "Blockchain for the metaverse: A review," arXiv preprint arXiv:2203.09738, 2022.

[3] B. J. Ali and G. Anwar, "An empirical study of employees' motivation and its influence on job satisfaction," International Journal of Engineering, Business and Management, vol. 5, no. 2, pp. 21–30, 2021.

[4] S. D. Hussain et al., "The impact of employees' recognition, rewards and job stress on job performance: Mediating role of perceived organizational support," SEISENSE Journal of Management, vol. 2, no. 2, pp. 69–82, 2019.

[5] N. A. A. Abdullah et al., "Coping with post COVID-19: Can work from home be a new norm?" European Journal of Social Sciences Studies, vol. 5, no. 6, 2020.

[6] R. M. Ryan and E. L. Deci, "Intrinsic and extrinsic motivations: Classic definitions and new directions," Contemporary Educational Psychology, vol. 25, no. 1, pp. 54–67, 2000.

[7] L. Festinger, "A theory of social comparison processes," Human Relations, vol. 7, no. 2, pp. 117–140, 1954.

[8] K. R. Christy and J. Fox, "Leaderboards in a virtual classroom: A test of social comparison theory," Computers in Human Behavior, vol. 47, pp. 66–75, 2015.

[9] J. Hamari, "Do badges increase user activity? A field experiment on the effects of gamification," Computers in Human Behavior, vol. 71, pp. 469–478, 2017.

[10] S. M. Robertson, S. O. Baror, and H. S. Venter, "Virtual currencies as a mechanism for employee engagement and retention in metaverse work

environments" in Proc. European Conf. on Cyber Warfare and Security (ECCWS), pp. 289–298, 2024.
[11] N. Pombo and H. Santos, "Lessons learned from the development of a computerized badge-based reward tool for student engagement in learning activities," in Proc. IEEE World Engineering Education Conf. (EDUNINE), pp. 1–5, 2023.
[12] O. Ogunseyi and A. Adedayo, "Cryptography and data privacy in digital forensic investigations," IEEE Access, vol. 11, pp. 1–15, 2023.
[13] K. Kent and M. Chevalier, "Guide to integrating forensic techniques into incident response," NIST Special Publication 800-86, National Institute of Standards and Technology, 2006.
[14] International Organization for Standardization, "ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence," ISO, Geneva, Switzerland, 2012.
[15] A. Valjarevic and H. S. Venter, "Harmonised digital forensic investigation process model," in Proc. Information Security for South Africa, IEEE, pp. 1–10, 2012.
[16] A. Singh, R. A. Ikuesan, and H. S. Venter, "Secure storage model for digital forensic readiness," IEEE Access, vol. 10, pp. 19469–19480, 2022.
[17] Z. Zheng et al., "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congress on Big Data, pp. 557–564, 2018.
[18] Z. Zheng et al., "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.
[19] I. Reyes et al., "Digital forensic readiness in blockchain systems," Future Generation Computer Systems, vol. 100, pp. 234–248, 2019.
[20] Jodeiri Akbarfam et al. Forensiblock: A provenance-driven blockchain framework for data forensics and auditability. arXiv preprint, 2023. URL https://arxiv.org/abs/2309.01456.
[21] L. Pasquale et al., "Towards forensic-ready software systems," in Proc. Int. Conf. on Software Engineering (ICSE), pp. 9–12, 2018.
[22] S. M. Robertson, "Digital Forensic Readiness of Reward Systems," Master's dissertation, University of Pretoria, 2025. https://repository.up.ac.za/handle/2263/107296
[23] R. S. Pressman and B. R. Maxim, Software Engineering: A Practitioner's Approach, 8th ed. New York, NY, USA: McGraw-Hill, 2015.
[24] F. Rivera-Ortiz and L. Pasquale, "Towards automated logging for forensic-ready software systems," in Proc. IEEE Int. Requirements Engineering Conf. Workshops (REW), pp. 157–163, 2019.
[25] S. M. Robertson, S. O. Baror, and H. S. Venter, "Enhancing Metaward: Integrating Digital Forensic Readiness in the Metaverse" in Proc. European Conf. on Cyber Warfare and Security (ECCWS), pp. 411–420, 2024.
[26] Iso/iec 27002:2022 – information security, cybersecurity and privacy protection — controls. ISO/IEC Standard, 2022.
[27] Rachel Adams, Fola Adeleke, Dominique Anderson, Ahmed Bawa, Nicola Branson, Alan Christoffels, Jantina de Vries, Harriet Etheredge, Eleni Flack-

Davison, Mark Gaffley, et al. Popia code of conduct for research. South African Journal of Science, 117(5-6), 2021.