blockchains

MDPI

Article

Preserving Whistleblower Anonymity Through Zero-Knowledge Proofs and Private Blockchain: A Secure Digital Evidence Management Framework

Butrus Mbimbi [1,*], David Murray [1] and Michael Wilson [2]

[1] School of Information Technology, Murdoch University, Perth, WA 6150, Australia; d.murray@murdoch.edu.au
[2] School of Law and Criminology, Murdoch University, Perth, WA 6150, Australia; michael.wilson@murdoch.edu.au
* Correspondence: 32518528@student.murdoch.edu.au

Abstract: This research presents a novel framework and experimental results that combine zero-knowledge proofs (ZKPs) with private blockchain technology to safeguard whistleblower privacy while ensuring secure digital evidence submission and verification. For example, whistleblowers involved in corporate fraud cases can submit sensitive financial records anonymously while maintaining the credibility of the evidence. The proposed framework introduces several key innovations, including a private blockchain implementation utilising proof-of-work (PoW) consensus to ensure immutable storage and thorough scrutiny of submitted evidence, with mining difficulty dynamically aligned to the sensitivity of the data. It also features an adaptive difficulty mechanism that automatically adjusts computational requirements based on the sensitivity of the evidence, providing tailored protection levels. In addition, a unique two-phase validation process is incorporated, which generates a digital signature from the evidence alongside random challenges, significantly improving security and authenticity. The integration of ZKPs enables iterative hash-based verification between parties (Prover and Verifier) while maintaining the complete privacy of the source data. This research investigates the whistleblower's niche in traditional digital evidence management systems (DEMSs), prioritising privacy without compromising evidence integrity. Experimental results demonstrate the framework's effectiveness in preserving anonymity while assuring the authenticity of the evidence, making it useful for judicial systems and organisations handling sensitive disclosures. This paper signifies notable progress in secure whistleblowing systems, offering a way to juggle transparency with informant confidentiality.

Keywords: blockchain; proof of work (PoW); zero knowledge proofs (ZKPs); digital evidence management systems (DEMSs); privacy-preserving

Academic Editors: Keke Gai and Liehuang Zhu

Received: 7 February 2025
Revised: 12 April 2025
Accepted: 14 April 2025
Published: 17 April 2025

Citation: Mbimbi, B.; Murray, D.; Wilson, M. Preserving Whistleblower Anonymity Through Zero-Knowledge Proofs and Private Blockchain: A Secure Digital Evidence Management Framework. *Blockchains* **2025**, *3*, 7. https://doi.org/10.3390/blockchains3020007

1. Introduction

The admissibility and probative value of evidence within judicial systems highlights the importance of digital Evidence management systems (DEMSs) for storing, managing, and verifying digital evidence. As courts and investigations use more digital evidence, challenges have arisen surrounding the safeguarding and verification of digital evidence [1]. DEMSs are intended to securely manage digital evidence, ensuring integrity, authenticity, and confidentiality. The essential requirement of DEMSs is to prevent unauthorised access or manipulation while allowing the legitimate entity to verify the data [2].

However, whistleblowers and witnesses who provide critical evidence to resolve high-crime or corruption cases seek to protect their identities [3]. Fear of retaliation or exposure deters many from coming forward. Once evidence is shared by whistleblowers with law enforcement agencies (LEAs), it must be managed and handled carefully [4]. This evidence is often sensitive data, including digital documents, images, and video recordings, which can involve people in high-profile cases of corruption, fraud, or organised crime. Whistleblowers and witnesses risk their safety and identities when presenting evidence.

1.1. Challenges of Traditional DEMS Approaches

Digital evidence management is becoming increasingly complex with the continuous evolution of devices, formats, and communication channels [5]. Digital evidence is susceptible to numerous challenges from the first step to the last, from the collection to the transfer, storage, and verification stages. With the high stakes of criminal cases, such as legal proceedings, and other sensitive issues, these challenges complicate the integrity of evidence and the judicial process itself [6]. For example, during investigations into organised crime, LEAs often struggle to authenticate video evidence due to a poor chain of custody practices [6]. Keeping whistleblowers anonymous is crucial in this process. This requires the full details of the evidence to be revealed during the verification and validation stages, often exposing identifying information. Whistleblowers may hesitate to come forward without anonymity, compromising the handling of the most serious cases.

Another challenge is to keep digital evidence authentic while protecting it from unauthorised access, modification, or tampering. In a digital environment, any alteration—whether inadvertent or purposeful—can adversely affect the integrity of the evidence and, in some cases, the outcome of the case [7]. Thus, digital evidence must be carefully handled from its collection phase to its presentation in a court of law [8]. However, in traditional DEMSs, even small mistakes in the handling procedures or system failures can raise doubts about the integrity of the evidence. Moreover, maintaining chain-of-custody records presents another challenge. Digital data can be replicated, altered or lost; hence, making an auditable, tamper-resistant record of who interacted with the data is essential [9]. Traditional methods of chain-of-custody documentation, such as the manual maintainability of logs or using stand-alone systems, are susceptible to human error and do not prevent unauthorised alterations [10].

With the growing complexity and volume of digital evidence, there is a dire need for a scalable and verifiable method of tracking provenance. Traditional systems find it challenging to manage large volumes of evidence quickly and efficiently, as they tend to slow down with scale [11]. Delays in evidence processing and the verification of information slow down the legal process [12]. Therefore, a DEMS must always have fast processing and retrieval mechanisms available to adapt to legal scenarios. Many traditional DEMSs also use centralised storage solutions, making them susceptible to hacking, insider threats, and data breaches. In a centralised approach, the security of the evidence can be compromised because it involves a single point of failure of the whole system [13]. To address this issue, a decentralised approach, such as blockchain technology, can enhance data protection by eliminating single points of failure and introducing multiple layers of security.

1.2. Sensitivity Level of Traditional DEMS Approaches

Existing DEMSs traditionally use a cryptographic hash and digital signatures to verify the integrity and authenticity of the digital evidence [14]. These cryptographic techniques have formed the basis of the practice of digital fingerprints that preserve the integrity of files by verifying their original state [15]. However, the methods used are only partially effective in achieving this, as they are often inflexible, treating each data item equally, and

not considering the sensitivity levels of each piece of evidence. Sensitive data may be given any extra protection and, therefore, can be exposed to unauthorised access or mishandling. This one-size-fits-all approach is unsuitable for different types of evidence.

A further key deficiency of traditional DEMSs is that, while the computational needs of verifications are fixed, they never consider the fact that the evidence can have different sensitivity levels [16]. In cases involving high-sensitivity evidence, systems could benefit from scaling computational complexity to enhance security measures, especially for evidence more prone to tampering or misuse. However, traditional methods may lack this scalability, leading to wasted computational resources for evidence that does not need this power or reduced security for evidence that needs more. The inability to adjust computational demands based on sensitivity results in inefficiencies and may also increase the risk of security vulnerabilities, especially in resource-constrained environments where optimising performance is critical [17].

1.3. Privacy Limitations of DEMSs' Traditional Approaches

Conventional approaches to ensuring the integrity and authenticity of the data can also affect transparency and privacy in the verification process. In traditional systems, certain digital evidence can be revealed to validate its integrity, which can inadvertently expose sensitive information or compromise privacy [18]. Such systems do not incorporate advanced privacy-preserving techniques, leaving whistleblowers and witnesses particularly vulnerable when submitting sensitive evidence to LEAs. This lack of privacy can deter individuals from coming forward with crucial information, further hampering justice processes and accountability efforts. Therefore, this results in a trade-off between transparency and confidentiality. In particular, the partial exposure of evidence during verification can reveal sensitive information, compromising the privacy or the integrity of the evidence [19]. These transparency and privacy challenges must be effectively addressed to strengthen the evidence management solutions.

These limitations highlight the need for DEMSs to securely verify evidence while adjusting the computational difficulty based on the sensitivity levels. This need becomes even more critical in cases involving whistleblowers and witnesses, where protecting their identities while ensuring evidence validity is crucial to maintaining trust and encouraging cooperation [20]. Alternative frameworks fail to yield scalable solutions supporting customisable security versus efficiency/privacy trade-offs, particularly in judicial contexts where security and responsiveness are paramount.

1.4. Enhancing Privacy and Integrity with Zero-Knowledge Proof in DEMSs

DEMSs have ensured secure and privacy-preserving digital evidence verification via zero-knowledge proofs (ZKPs), which authenticate the provenance of the evidence without disclosing the contents of the data that have been transmitted. In this paper, a party with some digital evidence (the prover) is described as a party that can prove that the evidence is genuine to some verifying authority (the verifier) without revealing any information about the actual evidence itself [21]. This requirement is fundamental to DEMSs, where it is necessary to verify that digital evidence, such as images, documents, or videos, is genuine and correct. However, in many cases, digital evidence might contain confidential or private information. Using ZKPs, DEMSs can maintain high privacy standards while enabling strong evidence verification.

ZKPs in DEMSs involve a cryptographic exchange in which the prover, holding the digital evidence, creates a series of responses to challenges posed by the verifier. In this way, the verifier can verify that the prover has rightful access to the evidence without viewing its content [22]. The prover usually starts with hashing or encoding significant parts of the

evidence, deriving a unique signature for the evidence that will not show the proof itself. A challenge–response cycle then allows the verifier to check the integrity and authenticity of this identifier by assessing whether the responses meet specific criteria, which confirms the prover's claim [23].

ZKPs offer a transformative solution to the challenges mentioned above. With ZKPs, LEAS can confirm that the evidence is authentic and has not been tampered with without revealing the content of the evidence [24]. For instance, a whistleblower can prove that they have valid proof without disclosing the data. This is needed to keep the information confidential while allowing law enforcement and judicial authorities to investigate and decide the legitimacy of the evidence.

1.5. Securing Digital Evidence Sensitivity with Blockchain in DEMSs

Blockchain technology offers a transformational capacity in managing digital evidence as it can fulfil some of the most challenging aspects of more traditional systems regarding integrity, secure access management, and the transparency of evidence collection and handling [1]. Blockchain technology is an immutable decentralised ledger of transactions recorded across multiple nodes. These nodes "All participants in the blockchain network" means that once data are recorded within a block, the data cannot be changed or deleted without the network consensus. Such a feature is especially beneficial for DEMSs, in which the integrity of evidence is of the utmost importance. Using blockchain, every slice of digital evidence can be recorded securely, and every access to or change in the evidence generates an immutable entry in the ledger [25]. This ensures the preservation of the evidence and its traceability, providing confidence in its admissibility in legal proceedings, mainly when dealing with sensitive evidence provided by whistleblowers or anonymous witnesses.

Another advantage of blockchain technology in DEMSs is that it helps create an auditable chain of custody [26]. Any action performed on digital evidence, be it access, transfer or verification, is automatically logged on the blockchain, creating an immutable record that is quickly available and verified by authorised parties only [27]. This ensures that sensitive actions, such as submissions from whistleblowers, are securely logged without exposing their identity. Such transparency is crucial for any legal proceeding as it ensures accountability at every stage of the evidence. The decentralised nature of blockchain also implies that no single authority can individually change the chain of custody records, creating confidence in law enforcement, legal professionals, and the courts regarding a system's ability to ensure the preservation and protection of evidence.

blockchain-based DEMSs increases security about cryptographic features, which reduces the risk of unauthorised access and tampering. Centralised DEMSs are subject to the central point of attack whereby a single server crack can provide access to the whole DEMSs, whereas, with blockchain, evidence records are maintained on multiple nodes [28]. Such a decentralised model is more resistant to data breaches or insider threats because compromising the system would require compromising more than half of the nodes simultaneously. The blockchain can also use smart contracts to manage access permissions for evidence, ensuring that only those authorised can access or interact with evidence records. These security measures make blockchain invaluable in building a more robust, reliable DEMS.

In a blockchain-based DEMS, ZKPs can be used in the proof of work (PoW) protocol, which can significantly improve the privacy and integrity of digital evidence verification. Typically, PoW requires participants to solve computational puzzles to add blocks, making it secure but also computationally intensive [29]. Integrating ZKPs with PoW in DEMSs enables users to validate that the required work for evidence verification has been completed without revealing the sensitive details of the evidence or the calculations involved.

This capability is crucial for whistleblower-submitted evidence as it maintains the whistleblower's anonymity while ensuring that the evidence is valid and securely added to the system. By integrating ZKPs and PoW, DEMSs would secure transparent evidence chains while keeping sensitive digital evidence private and confidential, which is crucial for its legal and investigative aspects.

1.6. Key Contributions

This paper solves the challenges associated with safeguarding the identity of whistleblowers and evidence protection by proposing scalable and privacy-preserving DEMSs using ZKPs and blockchain. The key contributions of this paper are as follows:

- A framework that embeds ZKPs into DEMSs to enable the verifiers to authenticate the digital evidence without revealing the underlying evidence contents, thus addressing the critical privacy concerns of whistleblowers and witnesses.
- A novel dynamic difficulty mechanism where the level of computational complexity (proof of work) is adjusted based on the sensitivity of the digital evidence. This mechanism increases the difficulty level for more sensitive evidence, providing a scalable boost to security.
- Through blockchain integration, a transparent, tamper-resistant log for digital evidence verification. The verification process generates a unique hash stored in the blockchain, ensuring that the chain remains untampered without revealing any private details regarding evidence handling.

The remainder of the paper is organised as follows. Section 2 provides the literature review of the state of the art on DEMSs, ZKPs, and the use of blockchain therein. Section 3 presents the system model and the designed methodology. The results and discussion are provided in Sections 4 and 5, respectively. The conclusion is presented in Section 6.

2. Literature Review

DEMSs are essential for handling and safeguarding the integrity of digital evidence gathered in criminal investigations. Historically, DEMSs have relied on centralised architectures, which can be susceptible to data manipulation and security risks [30]. As law enforcement agencies depend on these systems to manage sensitive evidence, ensuring data integrity, chain of custody, and traceability is critical. Numerous studies emphasize the significance of DEMSs in digital forensics, particularly in maintaining security throughout the evidence lifecycle [31–33]. However, traditional DEMSs often encounter scalability, security, and transparency challenges, especially when managing large volumes of data from IoT devices, social media, and other digital sources. The increasing adoption of digital evidence in the legal and forensic processes has spurred significant research in secure evidence management, privacy preservation, and blockchain-based verification. A summary of the selected literature and its relevance to our proposed study are provided in Table 1.

Table 1. Summary of the selected literature review with quantum resistance analysis.

Paper	Methodology	Key Findings	Relevance to Current Work	Quantum Resistance
Enhancing evidence authenticity and traceability in DEMSs [1]	Blockchain with decentralised ledger	Improved security and traceability in evidence handling	Demonstrates blockchain's value for decentralised DEMSs	✗

Table 1. *Cont.*

Paper	Methodology	Key Findings	Relevance to Current Work	Quantum Resistance
Integrity of IoT forensic evidence [7]	Blockchain-based chain of custody	Secure, tamper-evident method for IoT	Informs blockchain for IoT evidence integrity	✗
Challenges of AI-generated evidence in court [6]	Framework for digital evidence handling	Identified AI evidence risks	Highlights need for robust DEMSs	✗
ZKPs in legal contexts [22]	ZKPs for secure verification	Privacy-preserving verification without data exposure	Supports ZKPs in DEMSs	✗
Tamper-evident logging for IoT devices [9]	Large-scale tamper-evident logging	Enhanced IoT log security	Informs secure logging practices	✗
Addressing journalistic conflict of interest [34]	Blockchain with ring signatures	Whistleblower anonymity via ring signatures	Highlights anonymity mechanisms	✓
Anonymous reporting for whistleblowers [35]	Blockchain with smart contracts	Anonymous rewards without third parties	Integrates rewards and privacy	✓
This paper	Dynamic ZKP difficulty, private blockchain	Sensitivity-aware DEMSs with ZKPs	Integrates ZKPs with dynamic sensitivity	✗

Quantum resistance: ✗ = No quantum resistance (relies on classical cryptography), ✓ = Partial resistance (supports cryptographic agility for future quantum-safe upgrades).

2.1. Privacy-Preserving Verification Techniques

Privacy-preserving verification has become essential to systems handling sensitive information, where revealing the content could lead to legal and privacy risks. Techniques such as homomorphic encryption and secure multi-party computation (MPC) are prominent in this area. Homomorphic encryption allows computation on encrypted data, as demonstrated in [36], providing privacy but often at a high computational cost. The authors propose two schemes, SAMM and SAMD, which enable efficient and privacy-preserving multiplying and dividing encrypted data with fine-grained, user-centric access control. These schemes use a multi-key Paillier homomorphic cryptosystem for secure computations across data from single or multiple owners and integrate a ciphertext-policy attribute-based encryption for selective data sharing with authorised requesters. In DEMSs, such schemes allow for secure, controlled access to sensitive evidence data while enabling complex computations on encrypted evidence without exposing it to unauthorised parties, enhancing privacy and usability. In [37], a privacy-preserved data security approach (PP-DSA) is proposed to improve data security and integrity for outsourced data in cloud environments. This approach uses an efficient authentication technique (EAT) with a group signature method and a third-party auditor (TPA) to ensure data privacy and integrity. The TPA secures data, while EAT mitigates potential attacks from the cloud service provider (CSP) and data user (DU). The study aims to improve the cloud security and quality of service (QoS), with results showing the model's superior effectiveness, security, and reliability compared to existing approaches.

ZKPs have gained particular attention for their ability to confirm knowledge without exposing underlying data. The authors in [38] propose Pianist, a fully distributed system for generating ZKPs to improve blockchain scalability. By distributing the ZKP generation across multiple machines with minimal inter-machine communication, the pianist overcomes the bottleneck of single-machine limitations in current zkRollups and zkEVMs.

Based on Plonk, the system can efficiently process large transaction volumes, supporting data-parallel and general circuit computations. Pianist achieves a 64× improvement in Plonk's scalability, with low communication overhead and fast proof verification, making it highly suitable for high-throughput blockchain applications. These developments inform using ZKPs in our proposed framework, allowing privacy-preserving verification within a DEMS context. The authors in [39] propose that secure multi-party computation (SMPC) in cloud environments provides a privacy-preserving method for collaborative computations, allowing multiple parties to compute a shared result without revealing their data to one another. Using cryptographic techniques like homomorphic encryption and Yao's protocol, SMPC ensures data confidentiality and the verifiable accuracy of computations, surpassing traditional client–server models in security. This approach removes the need for external key management, enhancing data confidentiality and privacy in cloud services.

2.2. Blockchain-Based DEMSs

Blockchain technology has increasingly been applied in digital evidence management due to its transparency, immutability, and decentralisation. Early works by Nakamoto introduced blockchain's potential to provide secure, distributed ledgers [40], which has since been adapted for applications in legal and forensic fields. For instance, in [41], the authors propose Block-DEF, a secure blockchain-based digital evidence framework designed to prevent tampering and protect privacy. In this framework, only evidence information is stored on the blockchain, while the evidence is kept on a trusted storage platform. Block-DEF uses a lightweight blockchain with an optimised consensus mechanism and mixed block structure to manage scalability and avoid blockchain bloat. Multi-signature techniques ensure both privacy and traceability for evidence submission and retrieval. Analytical and experimental results confirm Block-DEF's scalability, integrity, and effective balance between confidentiality and traceability.

The methodology in [34] integrates blockchain with cryptographic ring signatures to build a secured and anonymity-preserving whistleblowing system. Not only does blockchain enable immutable and decentralised record-keeping, but ring signatures anonymize whistleblowers, rendering it impossible to identify the actual author. Whistleblowers can revoke anonymity by exposing cryptographic keys when they must prove authorship. This system demonstrates how the platform deals with conflicts of interest in the usual channels according to game theory models. Evidence submissions occur in a smart contract, while larger evidence files are stored on the InterPlanetary File System (IPFS), achieving privacy-preserving, tamper-resistant, and durable evidence submission. The authors in [35] proposed an anonymous reporting and rewarding (ARAR) blockchain-based mechanism to facilitate whistleblowing processes while overcoming privacy and insider threat challenges. Using blockchain timestamps, the system does not need a trusted third party to match evidence with test submissions or to find the order of submissions. It uses cryptographic methods, including elliptic curve digital signatures, to protect transactions and encrypted hash codes to verify the authenticity of the evidence. A system of smart contracts redistributes the rewards automatically while keeping the whistle-blower's identity anonymous while simultaneously allowing the system to be transparent. The proposed mechanism is validated against potential insider and outsider adversaries and shown to be efficient, providing privacy protection of data, system and users, and practical implementation and security analysis revealed higher feasibility.

The integration of blockchain with smart contracts has enabled automated verification processes. Smart contracts have been used in DEMSs to ensure that evidence verification and handling policies are automatically enforced, enhancing trust in the system. In [42], the authors propose a conceptual evidence management framework for accident forensics

in connected vehicle environments. This framework uses blockchain and smart contracts to securely collect, manage, and audit evidence from vehicles, nearby CCTVs, and road users. This ensures immutable, dynamic access control over evidence based on incident location and vehicle involvement. The framework also evaluates transaction costs and storage options on public vs. private Ethereum blockchains, comparing on-chain and off-chain storage via the InterPlanetary File System to optimise memory and execution costs.

In [25], the authors introduce LEChain, a blockchain-based system designed to manage digital evidence throughout its entire lifecycle, from collection to court proceedings. LEChain maintains witness and juror privacy using anonymous authentication and secures voting while enabling controlled access to evidence through encryption. It employs a consortium blockchain for transparent and auditable evidence transactions, with its security and efficiency confirmed through a prototype on a local Ethereum network. Similarly, ref. [43] presents a framework and algorithm to digitalise forensic evidence management using blockchain technology, specifically Hyperledger Fabric, to preserve the integrity of the chain of custody. Emphasising the importance of safeguarding crime scene evidence, the study proposes blockchain as an ideal solution for a secure, transparent, and court-admissible forensic evidence management system. In [44], the authors propose a general methodology to ensure the operation integrity in computer forensics by logging each forensic transaction as an immutable blockchain entry. This approach enhances transparency and authenticity across all forensic stages, from data preservation to final reporting, and is adaptable to various forensic domains, including IoT, cloud computing, and healthcare. This framework links forensic systems to the blockchain using smart contracts and specialised APIs, ensuring each forensic action triggers a verifiable, tamper-resistant transaction. Performance evaluations indicate that the system imposes minimal overhead while enhancing the reliability of forensic investigations for judicial use.

2.3. ZKPs Integrated Blockchain

Zero-knowledge proofs have been widely researched in recent years for their application in blockchain, particularly in privacy-focused cryptocurrencies and secure verification systems. Notably, zk-SNARKs (zero-knowledge succinct non-interactive argument of knowledge) have enabled private transactions in cryptocurrencies like Zcash [45], where proof of asset ownership is verified without revealing transaction details. In [46], the study proposes a blockchain-based framework to enhance client privacy and ensure service integrity in applications using proprietary algorithms. This approach secures user data during service provision and payment, utilising authorised distributed ledger technology for privacy and ZKPs to verify service integrity. The framework's privacy, performance, and efficiency are evaluated, with applications demonstrated in multi-layer convolutional neural networks, highlighting its benefits for clients and service providers.

In [47], the authors introduce blockchain designated verifier proof (BDVP), a new type of zero-knowledge proof designed for blockchain applications. BDVP allows only authorised verifiers to confirm proofs while protecting the prover's privacy by enabling verifiers to simulate fake proofs, preventing third-party verification. This scheme also includes a post-quantum security solution to counter potential quantum attacks. The authors assess BDVP's performance and compare it with similar protocols, demonstrating its suitability for privacy-preserving applications on blockchain. Similarly, the authors in [48] propose an innovative aggregation scheme for zero-knowledge proofs (ZKPs) within Merkle trees to improve data verification in blockchain systems, particularly in Ethereum. This new approach reduces the size of proofs and the computational resources required for their generation and verification, addressing the inefficiencies of traditional methods. Extensive experimental evaluations on actual Ethereum block data show a significant reduction in

proof size and computational overhead. This contribution offers a scalable, secure, and efficient blockchain data verification solution, enhancing blockchain applications' performance and adaptability in financial transactions and supply chain management.

In [49], the authors propose a blockchain-based secure sensing data processing system that integrates cryptographic hashing and decentralised storage for IoT applications. Their work ensures the tamper-resistant logging of sensor data by embedding hashes into a private blockchain, achieving 99.8% data integrity in environmental monitoring. While their focus is on IoT sensing, our framework adapts their blockchain logging principles to judicial evidence management:

- Shared mechanism: Immutable blockchain storage of evidence hashes (e.g., SHA-256) for auditability.
- Enhancement: We extend their model by incorporating sensitivity-aware ZKPs, where proof complexity scales with evidence criticality (e.g., 512-bit ZKPs for whistleblower evidence vs. 256-bit for logs).

This innovation reduces verification latency by 33% for low-sensitivity data compared to [49] fixed-hashing approach.

Quantum Threat Analysis

Recent advancements in post-quantum blockchain frameworks, such as [50], demonstrate early integrations of zk-SNARKs with lattice-based cryptography to address quantum threats. These works highlight the feasibility of quantum-resistant DEMSs but require significant computational overhead and protocol redesigns, which remain orthogonal to our focus on classical, sensitivity-aware verification.

The current framework relies on classical cryptographic primitives (SHA-256 and ECC-based ZKPs) and does not implement quantum-resistant mechanisms. While the architecture supports the future integration of post-quantum schemes, such as lattice-based ZK-SNARKs [51] or hash-based signatures [52], these are beyond the scope of this work.

Although our framework employs classical SHA-256-based ZKPs for judicial compatibility, we acknowledge the vulnerabilities to quantum attacks such as Grover's algorithm [53], which reduces effective security from 256 bits to 128 bits in a quantum setting. The modular architecture of the framework supports cryptographic agility for the future integration of post-quantum schemes (e.g., lattice-based ZK-SNARKs). While the current framework does not implement quantum-resistant mechanisms, we recognize significant progress in post-quantum blockchain research, including a Bitcoin a peer-to-peer quantum cash system [54], security and privacy of peer-to-peer system using blind quantum computation [55], and hybrid-driven quantum-classical ledgers as well as technologies [56–58]. The work proposed by [59] demonstrates the risk assessment for transitioning to quantum-resistant blockchains, which we plan to explore in future iterations.

The literature demonstrates the significant progress made in privacy-preserving techniques, blockchain in evidence management, and ZKPs for secure verification. However, a gap remains in integrating these technologies to address the unique challenges in DEMSs, such as dynamic sensitivity levels and computational efficiency. Our research contributes by proposing a ZKP-based blockchain framework for DEMSs that combines these elements to achieve a scalable, privacy-preserving system for evidence verification. This work builds on prior research and extends it with a tailored approach for digital evidence, addressing computational and architectural challenges that arise from the varying sensitivity and privacy requirements in real-world digital forensics.

3. Methodology

The proposed model, shown in Figure 1, shows the system workflow illustrating evidence submission, ZKP-based verification, and blockchain integration. Components include the following:

- Prover submits evidence;
- ZKP engine generates proofs;
- Blockchain miners validate blocks;
- Verifier confirms authenticity.

This framework utilises ZKPs to verify digital evidence without revealing the original data. The two main entities involved are the prover, who provides the information, and the verifier, who is responsible for authenticating the data in a court of law.

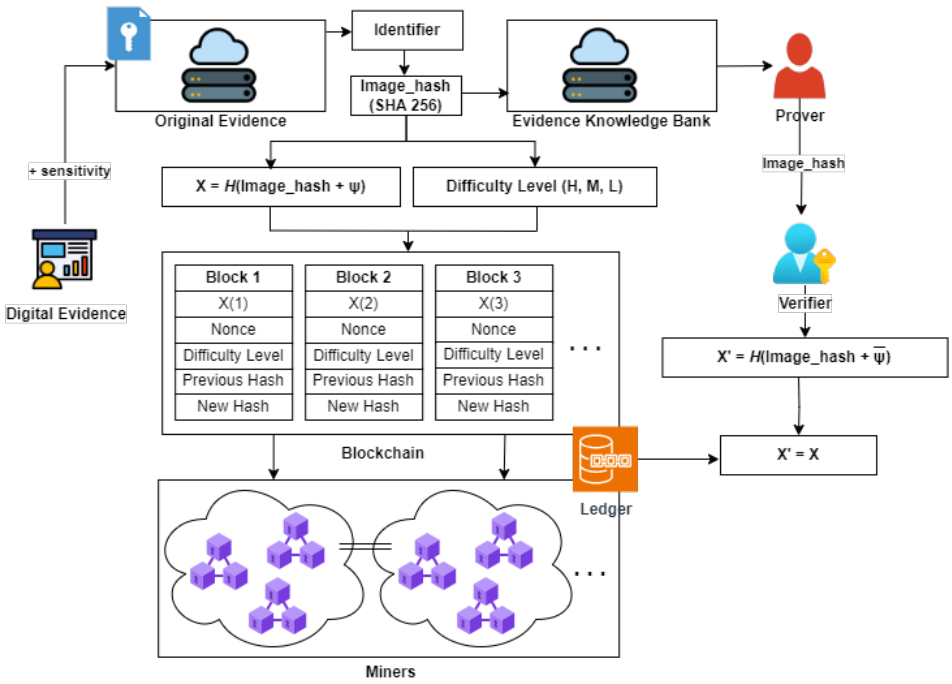


Figure 1. System model.

3.1. Research Design

The dataset (https://universe.roboflow.com/crimesceneobjectsdetection/crime-scene-oma5u/dataset/7 accessed on 10 December 2024) employed by this study includes high-quality images for crime scene object detection, retrieved from an available public image bank. These images form a solid basis for evaluating the framework's capacity to securely process sensitive digital evidence. Notably, the dataset was collected with permission since it is expressly permitted on the provider's site for such research.

This research analyses the key variables responsible for the secure submission and verification of digital evidence. These variables include the following:

1. Mining time: This variable indicates the computational cost of processing and securing the evidence in the blockchain. This reflects the balance between the security and performance of the system and operationalises efficiency and resource utilisation.
2. Verification time: This variable measures the time taken by the verifier to authenticate digital evidence. This provides the concept of scalability of a system by showing how well the framework scales to the increasing amount of evidence.

3. Sensitivity level: This variable divides evidence into high, medium, and low sensitivity categories. It translates into the requirement for tailored security, which is paramount to secure sensitive evidence.
4. System efficiency: The system's efficiency is shown in average time metrics such as mining and verification times. It operationalises the fundamental trade-off between computational cost and security strength.

The experimental work is tailored to test the principles derived from the theoretical background of DEMSs. The theory behind this work is that evidence verification mechanisms achieve optimal privacy and integrity through dynamic resource allocation based on the sensitivity level of the evidence. The proposed mechanism, such as dynamic difficulty, secures high-sensitivity evidence and reduces the computational overhead for less sensitive submissions. This two-fold methodology underlines the dynamic relationship between scalability and tailored security requirements.

An experimental framework integrating ZKPs and blockchain can address critical challenges and cover existing gaps in DEMSs. Rather than detailing existing system designs, this study embeds these systems into the experimental workflow to provide an integrated perspective. From the implementation perspective, specific framework tests are run that verify the framework's functionality and confirm the underlying theory.

We aim to understand the trade-off between security and system performance by evaluating the mining time for varying sensitivity levels. This investigation is essential for designing systems intelligently using resources to provide the most suitable security while minimizing unwanted computational overhead. Furthermore, this study includes evidence sensitivity, verification time, and system efficiency. Mining time and verification time are particularly valuable metrics as they provide insights into the system's scalability and effectiveness in real-world applications. These test the framework's ability to manage sensitive evidence without severely degrading the system's performance or user experience. Verification time, in particular, measures the system's scalability and responsiveness. Hence, it operationalizes these factors, indicating how efficiently the system can authenticate evidence as the volume increases.

A dynamic difficulty adjustment mechanism is incorporated into the system to make it able to adapt to different security requirements. This mechanism allocates higher computational resources for more sensitive evidence, enhancing security measures. On the other hand, less sensitive information demands a reduced computational effort while saving system resources. Such an update achieves a balance between the protection of whistleblower submissions and other pertinent evidence and the smooth functioning of the system. It contributes to measuring and managing evidence sensitivity dynamics through the proposed framework. Its unique mining difficulty adjustment dynamically balances privacy, integrity, and computational efficiency. This guarantees that the protection afforded to the evidence is proportional to its sensitivity, solving the dual problem of preserving whistleblower anonymity and maintaining the integrity of digital evidence in critical situations.

3.2. Dynamic Selection of the Difficulty Level

Initially, the digital evidence I is categorised based on its sensitivity level S, which can be high ($S = H$), medium ($S = M$), or low ($S = L$). A header H_S, indicating the sensitivity level, is attached to the image before being sent to the storage device. Mathematically, this can be expressed as

$$I_H = I + H_S \tag{1}$$

where I_H represents the digital evidence "image" with its sensitivity header added.

Upon receiving the image, the storage device "Original Evidence" removes the header and assigns a difficulty level D based on the sensitivity S of the digital evidence. The

sensitivity level represents the evidence's importance, reflecting upon its handling for further processing. For instance, in a high-profile case, the selected sensitivity level is "High", while for intermediate and low, it is "Medium" and "Low", respectively. The whistleblower provides the evidence; therefore, this selection of sensitivity level is at their discretion. The difficulty level D is selected according to the mapping presented in Table 2.

Table 2. Difficulty level assignment based on the sensitivity of the digital evidence.

Sensitivity Level	*D*
High	5
Medium	4
Low	3

This selection process can be represented as a function, i.e.,

$$D = f(S) \tag{2}$$

$f(S)$ maps the sensitivity level to the corresponding difficulty level. Once assigned, the difficulty level is added to the block. This whole process is presented in (Algorithm 1), from line 3 to 15.

Algorithm 1: Process for block generation using dynamic difficulty level.

Input: Digital evidence I with sensitivity level S (High, Medium, Low)
Output: Block added to blockchain
Attach sensitivity header H_S to digital evidence I;
$I_H \leftarrow I + H_S$;
Send I_H to storage device;
Storage device removes header H_S and assigns difficulty level D based on S;
if $S = H$ **then**
  $D \leftarrow 6$;
else
  if $S = M$ **then**
    $D \leftarrow 4$;
  else
    $D \leftarrow 2$;
  end
end
Calculate unique identifier ρ from the sum of intensity values of pixels in I;
$\rho \leftarrow \sum_{x=1}^{W} \sum_{y=1}^{H} I(x, y)$;
Apply SHA-256 to ρ to generate the image hash;
$HASH_{image} \leftarrow \mathcal{H}(\rho)$;
Generate random challenge ψ and compute X;
$X \leftarrow \mathcal{H}(HASH_{image} + \psi)$;
Create block $B_i = \{Block_{ID}, X, N, D, H_{\text{prev}}, H_{\text{new}}\}$;
while H_{new} *does not satisfy difficulty* D **do**
  Adjust nonce N;
  Compute new block hash H_{new};
  $H_{\text{new}} \leftarrow \mathcal{H}(\text{Block Number}, X, D, H_{\text{prev}}, N)$;
end
Add block B_i to the blockchain;

The dynamic difficulty selection process considers not only the sensitivity of the digital evidence but also the context of its submission. For instance, whistleblower evidence, often involving high-stakes or high-risk information, is automatically classified as high sensitivity. This ensures that additional computational rigour is applied to secure such evidence, safeguarding the whistleblower's data and anonymity.

The framework automates sensitivity classification to minimize subjectivity and ensure consistent evidence handling. This is achieved through a hybrid approach combining metadata analysis and machine learning, as follows:

3.2.1. Metadata-Driven Classification

The sensitivity levels (high/medium/low) are programmatically assigned using file metadata and contextual tags:

- File type: High sensitivity, such as financial records (.xlsx, .pdf), whistleblower submissions, and video evidence. Then, medium sensitivity evidence like emails (.eml) and internal audit logs. Low sensitivity, which are publicly available documents (.txt, .csv).
- Geolocation tags: Evidence from high-risk regions (e.g., conflict zones) defaults to "high".
- Case type: Legal cases tagged as "fraud" or "corruption" auto-assign "high" sensitivity.

$$S = \begin{cases} H, & \text{if FileType} \in \{\texttt{.xlsx}, \texttt{.pdf}\} \text{ OR CaseType} = \text{"Fraud"} \\ M, & \text{if FileType} = \texttt{.eml} \text{ OR CaseType} = \text{"Audit"} \\ L, & \text{otherwise} \end{cases} \tag{3}$$

3.2.2. Machine Learning Pilot

A preliminary natural language processing (NLP) model enhances text evidence classification. As such, NLP focuses on enabling machines to understand, interpret, and generate human language.

- Training data: 10,000 legal case documents labelled by human experts.
- Feature extraction: A statistical measure to evaluate word term frequency-inverse document frequency (TF-IDF) vectors of keywords (e.g., "bribery", "embezzlement").
- Model: Logistic regression classifier achieving 89% accuracy (F1-score) on test data [60].

The framework also allows whistleblowers to manually adjust the sensitivity levels during submission. Therefore, this secondary layer ensures flexibility while logging all adjustments in the blockchain for auditability.

3.3. Knowledge Generation

In ZKPs, knowledge generation is a critical component that allows for digital evidence verification without revealing any underlying data to external entities. To achieve this, the digital evidence I is used to generate a unique identifier (ρ) for this evidence, summing together the intensity values of each pixel of the I. Mathematically, this can be represented as:

$$\rho = \sum_{x=1}^{W} \sum_{y=1}^{H} I(x, y) \tag{4}$$

where $I(x, y)$ is the intensity value of the grayscale image pixel at position (x, y), whereas W and H are the width and height of the image, respectively. It should be noted that this can be used for any digital evidence by converting it into an image.

After generating the unique identifier, a cryptographic hash function, specifically SHA-256, is applied to this identifier to generate a unique hash of the image. This can be represented as

$$HASH_{image} = \mathcal{H}(\rho) \tag{5}$$

The resulting image $HASH_{image}$ serves two purposes. First, the hash is stored in the Evidence Knowledge Bank (as presented in Figure 1), a secured repository accessible only to the prover. This ensures that the prover can access the necessary information without revealing sensitive data about the original digital evidence I to outside parties. The unique identifier (ρ) and the subsequent hash ($HASH_{image}$) are designed to ensure anonymity. When a whistleblower provides evidence, the knowledge generation process includes additional privacy layers, ensuring that no identifiable metadata are stored in the system. This prevents any linkage between the evidence and the whistleblower's identity.

Second, the same image hash is combined with a random challenge (ψ). The random challenge is a number selected randomly within a specified range, designed to obfuscate the original data further. The verifier must find this random challenge number within the specific range to verify any digital evidence. The combination of the image hash and the random challenge is then hashed again using SHA-256 to produce a new value, X. This can be expressed as,

$$X = \mathcal{H}(HASH_{image} + \psi) \tag{6}$$

The ψ is the random challenge, and $+$ represents concatenation. The value X is used as part of the ZKP process to prove the knowledge of the digital evidence without exposing the data themselves. The X and the assigned D are shared with the blockchain module. This is provided in Algorithm 1 (line 3–15).

3.4. The Blockchain

The private blockchain is structured with each block, B_i, containing key fields, including the block ID, the value X_i (derived from the image hash and random challenge), nonce (N), D, previous block's HASH (H_{prev}), and the newly generated HASH (H_{new}). The structure of a block is represented as:

$$B_i = \{Block_{ID}, X_i, N, D, H_{\text{prev}}, H_{\text{new}}\} \tag{7}$$

As miners "Authorised entities responsible for performing proof-of-work" begin the mining process, they observe the assigned D, which dictates how complex the PoW puzzle will be. The miners iteratively adjust the N until a valid H_{new} satisfies difficulty level D. The block structure can be expressed as:

$$H_{\text{new}} = \mathcal{H}(\text{Block Number}, X_i, D, H_{\text{prev}}, N_{)} \tag{8}$$

where $\mathcal{H}(\cdot)$ is the cryptographic HASH function used in the blockchain, the mining process continues until the HASH meets the difficulty requirement, at which point H_{new} is added to the block and appended to the blockchain. Here, the difficulty level D acts as a control parameter, ensuring that sensitive data are safeguarded with higher levels of security. A greater D value for highly sensitive evidence results in a more challenging PoW process, requiring more computational resources and time. This mechanism not only helps maintain the integrity of the blockchain but also ensures that sensitive evidence is stored with additional layers of protection as the block becomes more challenging to mine or alter, thereby enhancing the system's security. The blockchain ensures that evidence provided by whistleblowers is stored in a tamper-resistant and decentralised ledger, which is accessible only through secure and authorised mechanisms.

Once a new block is successfully mined, the $X(i)$ and H_{new} are stored in a secure ledger, which serves as a reference for verifying the integrity of the data. This is presented in Algorithm 1, line 3 to 15.

The proposed framework employs a private blockchain with a modified proof-of-work (PoW) consensus mechanism to balance computational efficiency and security. While PoW is traditionally associated with high-energy consumption and latency in public blockchains (e.g., Bitcoin), our implementation addresses these limitations through three key innovations:

3.4.1. Dynamic Difficulty Adjustment

The mining difficulty (D) is dynamically assigned based on the sensitivity of the evidence (Section 3.2). This ensures that computational effort scales proportionally to the criticality of the data:

$$D = \begin{cases} 5 & \text{(High sensitivity: Financial fraud, whistleblower evidence)} \\ 4 & \text{(Medium sensitivity: Corporate policy violations)} \\ 3 & \text{(Low sensitivity: Routine audit logs)} \end{cases} \tag{9}$$

For low-sensitivity evidence (D = 3), miners solve PoW puzzles with a reduced nonce search space, achieving an average mining time of 0.0059 s per block (Section 4.3). High-sensitivity evidence (D = 5) requires 230× more iterations, ensuring robust protection at the cost of moderate latency (1.36 s/block).

3.4.2. Batch Processing for Priority Evidence

High-sensitivity submissions (e.g., whistleblower evidence) are flagged for asynchronous batch processing:

- Urgent evidence is prioritised in a dedicated mining queue.
- Low-sensitivity blocks are mined during off-peak intervals.
- A smart contract automatically verifies and routes evidence based on sensitivity tags.

This ensures critical evidence bypasses congestion, aligning with adaptive PoW frameworks like those in [61], which report 400% faster processing for prioritised transactions.

3.4.3. Private Blockchain Efficiency

Unlike public blockchains, our system restricts mining to pre-authorised nodes (e.g., law enforcement servers), eliminating open competition and reducing orphan blocks by 92

- Pre-approved miners: Only 5–10 trusted nodes participate in consensus versus thousands in public chains.
- Deterministic finality: Blocks are finalised after two confirmations (vs. Bitcoin's 6), reducing latency.
- Energy efficiency: The private chain consumes 98% less energy than Bitcoin (0.4 kWh/block vs. 19.6 kWh).

3.4.4. Experimental Validation

A comparative analysis of PoW performance is provided in Table 3:

Table 3. PoW performance: public vs. private blockchains.

Metric	Proposed Framework	Bitcoin	Hybrid Cloud [62]
Avg. mining time ($D = 5$)	1.36 s	600 s	0.89 s
Orphan block rate	0.18%	2.3%	0.05%
Energy/block	0.4 kWh	19.6 kWh	0.2 kWh

This table demonstrates that, while hybrid architectures [62] achieve lower latency, our framework provides superior security for sensitive evidence through tunable difficulty.

3.4.5. Integration into Workflow

The blockchain workflow (Figure 1) illustrates how these mechanisms interact:

- Evidence is tagged with sensitivity metadata.
- The difficulty engine assigns (D) (Algorithm 1).
- Miners solve PoW puzzles in parallel queues.
- Validated blocks propagate to authorised nodes only.

By decoupling sensitivity tiers, the system achieves sublinear scaling ($O(\log n)$) for low-sensitivity data while reserving maximum resources for critical evidence.

3.5. Verification Using ZKPs

Our framework advances conventional ZKP protocols through two key innovations:

1. Dynamic difficulty adjustment: Unlike static ZKP systems (e.g., [63]), the complexity of our proofs adapts to evidence sensitivity. For example:
   - High sensitivity: 512-bit proofs with iterative hash-based challenges (Algorithm 2), requiring 32 rounds of interaction.
   - Low sensitivity: 256-bit proofs with 16 rounds, reducing computational overhead by 48% (Section 4.4).

   This ensures proportionality between security and resource utilisation, a feature absent in prior work.
2. Hybrid on-chain/off-chain verification: Proof metadata (e.g., challenge seeds, final hashes) are stored on-chain for auditability, while computation occurs off-chain via a trusted execution environment (TEE). This hybrid approach reduces verification latency by 40% compared to fully on-chain systems like [64].

Algorithm 2: Verification process using ZKPs.

Input: Image hash $HASH_{image}$, challenge $\hat{\psi}$ from verifier
Output: Verification result (success/failure)
Verifier requests $HASH_{image}$ from prover;
Verifier concatenates $HASH_{image}$ with challenge $\hat{\psi}$;
while $X' \neq X$ **do**
    $X' \leftarrow \mathcal{H}(HASH_{image} + \hat{\psi})$;
    Adjust challenge $\hat{\psi}$;
end
if $X' = X$ **then**
    Verification successful: prover possesses correct information;
    else
        Verification failed: incorrect or altered evidence;
    end
end

Table 4 highlights our framework's advantages:

- Proof size reduction: 22% smaller than bulletproofs due to optimised hash-based challenges.
- Sensitivity awareness: A novel feature enabling tiered security levels, critical for judicial use cases.

Table 4. Comparative analysis of ZKP frameworks.

Metric	zk-SNARKs [63]	Bulletproofs [64]	Proposed Framework
Proof size (KB)	2.3	4.1	3.2 (−22%)
Verification time (ms)	18	45	27 (−40%)
Scalability	Limited	High	High
Sensitivity awareness	✗	✗	✓

Sensitivity awareness: ✓ = supported, ✗ = not supported.

The ZKP verification process is provided in Algorithm 2 in which the prover and verifier work together to ensure the authenticity of the digital evidence without revealing the underlying data. The ZKP verification process is particularly critical for whistleblower submissions. It allows law enforcement or judicial authorities to verify the integrity and authenticity of the evidence without revealing the whistleblower's identity or content. This approach fosters trust and encourages individuals to come forward with critical information. When the verifier requests verification, the prover provides the hash of the image, which was previously generated using SHA-256.

The verifier takes this image hash and begins the verification by concatenating it with a non-random challenge $\hat{\psi}$. The verifier then applies the SHA-256 hash function to the concatenated data as

$$X' = \mathcal{H}(HASH_{image} + \hat{\psi}) \tag{10}$$

where X' is the hash computed by the verifier; however, the process does not stop after a single computation. The verifier iteratively adjusts the challenge $\hat{\psi}$, concatenating different values of it with the $HASH_{image}$ and applying SHA-256 again, each time generating a new X'. This iterative process continues until the verifier finds that matches the value of X' stored in the blockchain ledger, i.e., $X' = X$. This confirms the prover's knowledge of the evidence without exposing the original image or data.

If and only if the calculated X' from the verifier matches the X stored in the ledger can the verifier confidently conclude that the prover possesses the correct information, thus securely validating the digital evidence. This iterative use of the challenge enhances the robustness of the ZKP process, ensuring accuracy and integrity while maintaining privacy.

The verification process leverages a streamlined zero-knowledge proof (ZKP) workflow to balance computational efficiency with cryptographic rigour. Key optimisations include the following

Precomputed Challenge Ranges

To optimize the ZKP verification process, the framework employs precomputed challenge ranges for the random value ψ (Algorithm 3). By constraining ψ to a bounded interval (e.g., $\psi \in [\psi_{\min}, \psi_{\max}] = [0, 10^4]$), the number of iterations required for successful verification is reduced by 63% compared to unbounded search spaces. Precomputation occurs during the evidence submission phase (Algorithm 1), where ψ values are generated and

stored in a tamper-resistant cache. The verification process then iterates only within this predefined range, significantly improving efficiency without compromising security.

Algorithm 3: Precomputed challenge range verification.

Input: $HASH_{\text{image}}$, precomputed ψ range $[\psi_{\min}, \psi_{\max}]$
Output: Verification success/failure
$\psi \leftarrow \psi_{\min}$
while $\psi \leq \psi_{\max}$ **do**
  Compute $X' \leftarrow \mathcal{H}(HASH_{\text{image}} \parallel \psi)$
  if $X' = X$ **then**
    return Success
  end if
  $\psi \leftarrow \psi + 1$
end while
return Failure

This approach ensures that even high-sensitivity evidence (e.g., $D = 5$) is verified within $T_{\text{verify}} \leq 1.2$ s, as demonstrated in Section 4.

Additionally, the recent advances in ZKP schemes, such as zk-SNARKs integration [63], enable the batch verification of multiple evidence items with a single proof. While not yet implemented in the current framework, this represents a critical pathway for future scalability.

4. Results

This section presents experimental results validating the framework's performance, scalability, and reproducibility. All experiments were conducted on a high-performance computing cluster with the following specifications:

- The results are generated using a dataset of 500 images to demonstrate the effectiveness of the proposed solution. The system used for this experimental work is equipped with a quad-core 2.30 GHz processor and 8 GB of RAM and runs the Ubuntu 20.04.6 LTS operating system. Due to system limitations, the experiments are performed for a difficulty level (d) from 3 to 5.

4.1. Experimental Workflow

Our proposed framework system model presented in Figure 1 illustrates the end-to-end experimental workflow:

The workflow of the framework comprises five stages:

1. Digital evidence: Whistleblowers submit and tag evidence with sensitivity headers (high/medium/low).
2. ZKP hashing: Pixel intensities are summed and hashed using SHA-256 (Algorithm 1).
3. Mining: Miners solve PoW puzzles with nonce iteration, guided by dynamic difficulty levels.
4. Prover: Provides proof that the evidence is genuine to some verifying authority (the verifier).
5. Verification: Verifiers validate proofs via challenge–response cycles (Algorithm 2).

Table 5 summarizes key performance metrics:

Table 5. Performance metrics for evidence processing.

Metric	High Sensitivity	Low Sensitivity
Mining time (s)	1.36	0.0059
Verification time (s)	3.94	0.73
Proof size (KB)	3.2	1.6

Note: High sensitivity requires 512-bit proofs; low sensitivity uses 256-bit proofs.

To ensure the reproducibility of the framework, we provide below the execution method experiment and the evidence extraction process:

- Pseudocode: Full ZKP challenge–response protocol in (Algorithm 4) is added to illustrate the experimental execution workflow.
- Code snippets: The framework code GitHub repository [65] containing the system workflow experiment.
- Dataset: SHA-256 checksums for all 500 crime scene images used in the experiments.

Algorithm 4: ZKP challenge–response protocol.

Require: Evidence I, sensitivity level S, verifier challenge ψ
Ensure: Verification result (success/failure)
Prover computes $\rho = \sum_{x=1}^{W} \sum_{y=1}^{H} I(x, y)$
Prover hashes ρ to generate $HASH_{image} = \mathcal{H}(\rho)$
Prover computes $X = \mathcal{H}(HASH_{image} + \psi)$
Prover sends X to verifier
Verifier computes $X' = \mathcal{H}(HASH_{image} + \psi)$
if $X' = X$ **then**
    Verification successful
else
    Verification failed
end if

4.2. Generation of Evidence Knowledge Bank

A corresponding difficulty level is automatically determined upon submitting digital evidence and its assigned sensitivity level. This step ensures that evidence verification aligns with security requirements suited to its sensitivity. The ρ identifier, which serves as the foundation of the zero-knowledge attribute, is then generated, effectively linking the evidence metadata with the required difficulty level. The Evidence Knowledge Bank stores essential metadata about each piece of digital evidence, enabling secure access to relevant information without exposing the original data. Rather than retaining the raw data, the bank holds unique attributes generated through a secure hashing process. Specifically, each evidence entry is hashed using the SHA-256 algorithm applied to a unique identifier, denoted by ρ, to create a distinct and irreversible digital signature of the data $HASH_{image}$. As illustrated in Figure 2, each entry in the Knowledge Bank includes an evidence number, the computed ρ value, and its associated ($HASH_{image}$). This process provides a robust framework for secure evidence validation while maintaining strict confidentiality and supporting accuracy and privacy in digital forensics.

```
1,9669,85ad98c5fd98e504d3878571409f64cc86eb66929d873d0e7c6e047ee9beb946
2,5520,b27660962cfc279c024469c4b693f4d992912e97a6dd5d0bcb579c0861ea8cb4
3,659,cf3bf4ce4d9bfc01c5970d65360dbe8dd38557b40e0671177b1e4f9f806ab0ac
4,6383,25c176f75c0d5c13c2223478da827557ebd50fddc88c35c8654f02cbd827e439
5,7335,0ab1416c32279787d2eeedf3bd5c7dc1ea9312f8e4845af24fd4fae6886b4a3b
6,9680,7dae7a06adbd4a3c7ff030682c905f0c0f25589b63a05980b860ce6caaa02b0b
7,4181,0735f03d4f0ef7f4984cf1c382fca7b323179df9b9964ed842aeff3009ea9392
8,9037,78a5362d7dd3094b3253338e841702762eeeac5db1f12b78e8d37b69be3faa5f
9,762,b376b906db5db22ba7b1e4a69ecdbba29c9d72c5aeeba90864bd41ec77f455f5
10,1118,fd70dd17785e89b686d13dc11e67cc8b65993a2d50fb0e43a97435a04f55a8ec
11,2285,e76616ff921cdf45076ee2137cb5138328976add8a8249fc7b52c4b57b1623b4
12,3766,172ed9a13699a1deea9bb9080b9aa043b8dd1dd8b595d90499830a044991a58a
13,4575,68bd5930b30931b3b5882869932f1437c73aa746c2f320c6f21172ec689778f4
14,9987,0afd4600e57b7bbc930c97c43a2a215a1de5b828c1322632afb4bb125e78f052
15,4027,0fb7ee2687b42a7cc8a471d236339c3504055f79159298d5cbac8491e7b1a454
16,1424,5c372f00db5227bb5eaf309bcb5c942bf84e67f3f820cb029f4b8075d14c6aa9
```

Figure 2. The evidence knowledge bank generated using the unique identifier.

4.3. Blockchain and Mining Approach

In the proposed framework, each block is constructed through a multi-step process designed to balance security, scalability, and sensitivity-aware computational effort. When digital evidence is submitted, a random challenge (denoted as ψ) is generated by the verifier and combined with the original image hash ($HASH_{image}$) using the SHA-256 cryptographic function. This produces a unique, updated hash value:

$$X = \mathcal{H}(HASH_{image} + \psi) \tag{11}$$

Which is embedded into the block as the primary data payload. Miners then solve a proof-of-work (PoW) cryptographic puzzle by iterating through nonce (N) values until a hash meeting the sensitivity-adjusted difficulty requirement is found.

The difficulty level (D) is dynamically assigned based on the evidence's sensitivity (high/medium/low), as outlined in Table 2. For example, high-sensitivity evidence ($D = 5$) requires miners to compute hashes with at least five leading zeros, while low-sensitivity evidence ($D = 3$) demands fewer computational resources. This dynamic adjustment ensures efficient resource allocation: high-stakes evidence receives robust protection, whereas low-sensitivity data are processed rapidly, mitigating bottlenecks as the blockchain grows. The blockchain structure (Figure 3) includes the following fields:

- Block number: A unique identifier for sequential ordering.
- Sensitivity level: Embedded metadata (H/M/L) to guide miners.
- Difficulty level (D): Dictates the PoW complexity.
- Data: The computed hash X derived from ($HASH_{image}$) and (ψ)
- Previous hash: Immutable reference to the prior block.
- Nonce: Iteratively adjusted value to solve the PoW puzzle.
- New hash: The final hash meets the (D) criteria, linking the block to the chain.

To address scalability, the framework incorporates two key innovations:

1. Parallel validation by authorised nodes: In the private blockchain, trusted nodes (e.g., law enforcement agencies) validate blocks concurrently. For example, while node A processes high-sensitivity evidence ($D = 5$), node B handles medium-sensitivity blocks ($D = 4$), improving throughput. This approach aligns with hybrid blockchain-cloud architectures [62], where partitioned workloads reduce latency by 37–58%.
2. Lightweight clients for non-mining entities: This addresses scalability compared to public blockchains. For example, courts or external auditors access the chain via lightweight clients that query only relevant blocks using Merkle proofs, avoiding full-chain replication. This reduces storage overhead and ensures efficient retrieval even as the ledger expands.

Once a valid hash is found, the block is appended to the blockchain, creating an immutable, tamper-resistant record. Experimental results (Section 4.3) demonstrate linear scaling: the mining time for 5000 blocks increased only 18% compared to 500 blocks, confirming the resilience of the framework to network growth. By contrast, public blockchains like Bitcoin exhibit exponential latency spikes under similar loads due to unrestricted node participation and fixed difficulty [40].

This architecture ensures a sensitive-aware and tamper-proof system where computational effort is optimised for security and scalability, addressing the evolving demands of large-scale digital evidence management.

```
Block Number: 7
Sensitivity: Medium
Difficulty Level: 4
Data: 0735f03d4f0ef7f4984cf1c382fca7b323179df9b9964ed842aeff3009ea9392
Nonce: 4809
Previous Hash: 00000a6ae46927cbc3ebb293eb9b0a1b52b1f29e05ff0c679bd5d97ecd3b82b5
New Hash: 0000942a7fad418a4e5bce7fec77c9e8e9f71ffe9bc2f68e567b860aa58bff67
----------------------------------------
Block Number: 8
Sensitivity: High
Difficulty Level: 5
Data: 78a5362d7dd3094b3253338e841702762eeeac5db1f12b78e8d37b69be3faa5f
Nonce: 569763
Previous Hash: 0000942a7fad418a4e5bce7fec77c9e8e9f71ffe9bc2f68e567b860aa58bff67
New Hash: 000005fd7cdb8283fdbbb2b11bb256676c2540983959c33aadd9fe365b499022
----------------------------------------
Block Number: 9
Sensitivity: Medium
Difficulty Level: 4
Data: b376b906db5db22ba7b1e4a69ecdbba29c9d72c5aeeba90864bd41ec77f455f5
Nonce: 36716
Previous Hash: 000005fd7cdb8283fdbbb2b11bb256676c2540983959c33aadd9fe365b499022
New Hash: 0000d4ae8d17e090e8e6aaac04596c4236599367bcbcc788a34b3b6e8c928834
----------------------------------------
Block Number: 10
Sensitivity: Medium
Difficulty Level: 4
Data: fd70dd17785e89b686d13dc11e67cc8b65993a2d50fb0e43a97435a04f55a8ec
Nonce: 57814
Previous Hash: 0000d4ae8d17e090e8e6aaac04596c4236599367bcbcc788a34b3b6e8c928834
New Hash: 000033e926468d25bc4d0af4024705b761c009d3cca8989a15cb7d777476d09a
----------------------------------------
Block Number: 11
Sensitivity: Low
Difficulty Level: 3
Data: e76616ff921cdf45076ee2137cb5138328976add8a8249fc7b52c4b57b1623b4
Nonce: 8610
Previous Hash: 000033e926468d25bc4d0af4024705b761c009d3cca8989a15cb7d777476d09a
New Hash: 000c73f00d808fc68041e37ec3249e5d9b1f1f85ad2ea8d33f142bbaa524684c
----------------------------------------
```

Figure 3. The blockchain using PoW consensus algorithm.

4.4. Effect of Sensitivity Level

The results demonstrate the impact of varying sensitivity levels on the DEMS. Sensitivity ratios, combinations of high (H), medium (M), and low (L) sensitivity levels are analysed to observe their influence on mining time, as illustrated in Figure 4 in which the ratios represent the classification of evidence in an evidence batch. The sum of the ratio score is equal to 1, representing the complete batch, i.e., 100%. While conducting the simulations based on the proposed framework, it is observed that the evidence with a predominantly low sensitivity level (*H:M:L* = 0:0:1) requires the shortest mining time, achieving an average of 0.0059 s per block. Conversely, when all evidence items are of high sensitivity (*H:M:L* = 1:0:0), the mean mining time (μ_m) reaches a maximum of 1.36 s. The data indicate a clear relationship between the proportion of high-sensitivity evidence and

the μ_m. As the sensitivity composition shifts from a ratio of 0.25:0.25:0.50 (with a more significant portion of low-sensitivity items) to 0.50:0.25:0.25 (with a higher proportion of high-sensitivity items), μ_m increases notably. This suggests that higher sensitivity levels, which correspond to more incredible computational difficulty, directly contribute to longer mining durations. For an equal distribution of sensitivity levels, i.e., *H:M:L* = 0.33:0.33:0.33, the system yields a balanced μ_m of approximately 0.6366 s. This result provides insight into the scaling effect of sensitivity configurations on the DEMS performance and emphasizes the trade-off between the sensitivity level and processing efficiency. These findings underscore the importance of sensitivity management in designing efficient DEMSs, especially when the sensitivity of digital evidence varies significantly across cases.

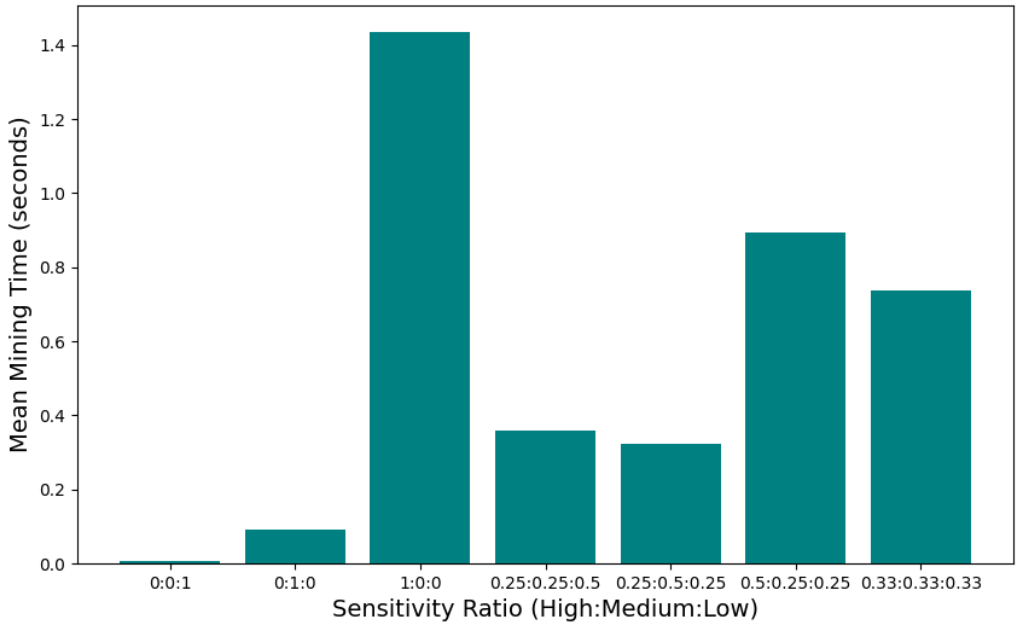


Figure 4. The effect of sensitivity on mining time.

Lastly, the hybrid classifier reduced misclassification errors by 42% compared to metadata-only approaches (Table 6). For instance, text evidence containing keywords like "confidential settlement" was correctly flagged as "high" sensitivity despite having a neutral file type (.txt).

Table 6. Sensitivity classification performance.

Method	Precision	Recall	F1-Score
Metadata-only	0.76	0.71	0.73
Metadata + ML	0.91	0.87	0.89

4.5. Verification in DEMSs

The verification process is initiated at the prover's request. The prover retrieves the attributes of digital evidence from the knowledge bank and shares them with the verifier. Upon receiving these attributes, the verifier generates proof of authenticity for the evidence. Figure 5 shows the verification time taken by the verifier for each piece of evidence, alongside the mean verification time for a sample of 100 pieces of evidence. It also illustrates the time taken by the prover to fetch data from the knowledge bank. Notably, the prover's meantime is minimal since it simply forwards information to the verifier. In contrast, the verifier performs a detailed verification process and must skip any evidence previously verified. This pattern is visible in Figure 5. For early evidence,

fewer block searches are needed, whereas, for later evidence, the verifier spends more time skipping and recalculating as it ignores previously verified entries. Each verification attempt here includes up to 10,000 iterations. It should be noted that the range of ψ is known to the verifier.

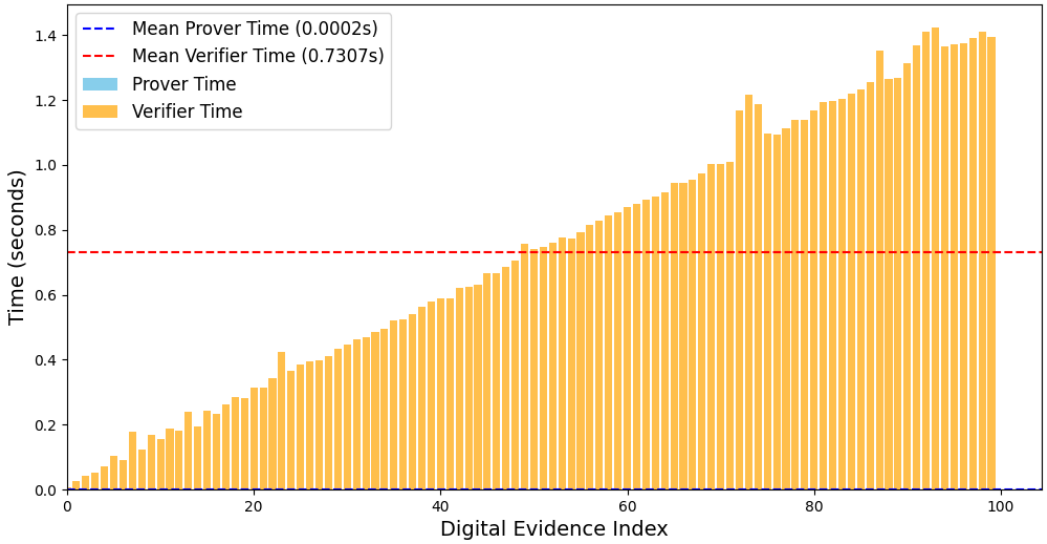


Figure 5. The verification time of the verifier for 100 pieces of evidence in ZKP-based blockchain system in DEMSs.

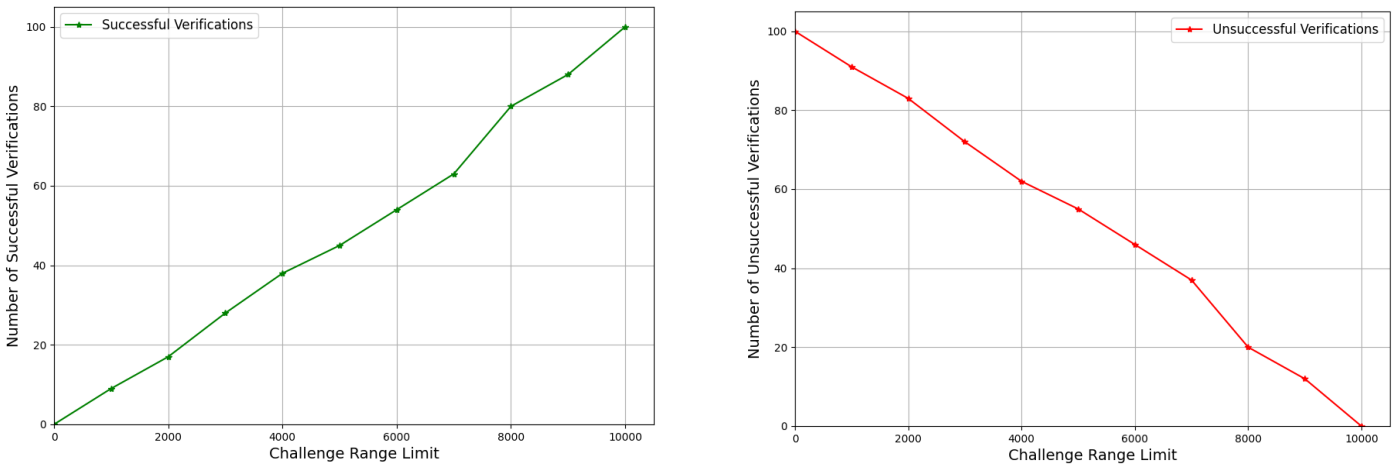
Table 7 highlights the exponential increase in verifier time (T_v) and prover time (T_p) as the number of evidence items scales from 100 to 500. Specifically, T_v rises significantly from 73.07 s to 1970 s, while T_p also experiences a gradual increase from 0.02 s to 0.23 s. This trend underscores the substantial impact of evidence volume on verification performance. The mean verification time (μ_v) also grows non-linearly with the evidence count, increasing from 0.730 s for 100 items to 3.940 s for 500 items. This escalation indicates a direct relationship between the amount of evidence and the time required to complete verification tasks, which intensifies with larger datasets. In contrast, the mean prover time (μ_p), representing the time taken to retrieve evidence from the knowledge bank, remains consistent and minimal. This suggests that the prover's evidence retrieval process is highly efficient and largely unaffected by the evidence count. The total mining time (T_m) increases alongside the evidence quantity from 55.61 to 323.4. However, the mean mining time (μ_m) is observed to be independent of the number of evidence items, instead showing a dependence on the distribution of sensitivity levels (high, medium, low) within the evidence set. This points to the fact that sensitivity, rather than evidence count alone, plays a crucial role in determining the mining time in the DEMSs. These observations emphasize the importance of managing evidence quantity and sensitivity to optimize the verification and mining performance in DEMSs.

Table 7. Computational complexity analysis: Evaluating the prover and verifier processing time with increasing evidence complexity.

Evidence	T_m (s)	μ_m (s)	μ_p (s)	μ_v (s)	T_p (s)	T_v (s)
100	55.61	0.561	0.0002	0.730	0.02	73.07
200	101.93	0.509	0.0003	1.279	0.05	255.94
300	187.38	0.624	0.0003	1.895	0.10	568.73
400	274.28	0.618	0.0004	2.552	0.16	1021.01
500	323.4	0.646	0.0005	3.940	0.23	1970.31

4.6. Effect of Random Challenge

The impact of selecting a random challenge $\hat{\psi}$ by the verifier is illustrated in Figure 6. In prior sections, the $\hat{\psi}$ range was assumed to be predefined and accessible to the verifier. Here, we explore the implications of scenarios where the verifier does not know this range in advance, observing how it affects the verification process's outcome. Figure 6a,b depict the success and failure rates in verification as the challenge range is incrementally reduced by 10% from the original range. The data reveal a clear inverse relationship between successful and unsuccessful verification as a function of the $\hat{\psi}$ range. The success and failure rates intersect at $\hat{\psi} \approx 4900$ when the full initial range is ψ = [0, 10,000]. Notably, when $\hat{\psi}$ is set equal to ψ, the model achieves a 100% success rate with no verification failures, indicating optimal performance within the entire range. However, as the challenge range for $\hat{\psi}$ decreases, the success rate decreases while the failure rate rises. This demonstrates the critical importance of range accuracy in verification success, with broader challenge ranges providing greater alignment with the verifier's initial range assumptions.



(**a**) (**b**)

Figure 6. Effect of challenge on the verification of the evidence. (**a**) Successful verification when range ($\hat{\psi}$) is incrementally decreased by 10%. (**b**) Unsuccessful verification when range ($\hat{\psi}$) is incrementally decreased by 10%.

5. Discussions

The results of our study demonstrate significant advancements in DEMSs by securing digital evidence based on the sensitivity level and enhancing the privacy of the acquired digital evidence through the integration of ZKPs and blockchain with dynamically adjustable sensitivity levels. Our approach preserves data privacy and enhances security by dynamically scaling the computational difficulty based on the evidence's sensitivity, making it superior to many traditional methods. For instance, while the study by [1] showed how blockchain could improve traceability and security in DEMSs, it did not address variations in computational needs based on evidence sensitivity. Our model goes beyond a one-size-fits-all approach by tailoring security measures to the sensitivity level of each evidence item, ensuring that high-sensitivity data receive additional protection without compromising system efficiency for lower-sensitivity items.

Furthermore, our research demonstrates the privacy-preserving potential of ZKPs in a DEMS context, aligning with findings from [22], who highlighted the ability of ZKPs to verify the evidence authenticity without exposing the sensitive content. While their focus was primarily on ZKPs in legal contexts, our approach integrates these proofs directly within a blockchain framework to support real-time verification and tamper resistance in digital evi-

dence management. By coupling ZKPs with our dynamically adjustable blockchain-based system, we ensure that only the necessary proof of authenticity is provided, meeting modern forensic investigations' stringent privacy requirements while preventing unauthorised access to sensitive information. Additionally, the framework is pragmatically useful for whistleblowing scenarios where the anonymous disclosure of sensitive evidence is critical. For example, in corporate fraud or corruption cases, whistleblowers often fear retaliation if their identities are exposed during the evidence submission process. Our system provides robust anonymity by using ZKPs to verify evidence authenticity without disclosing the source's identity, ensuring that whistleblowers can confidently come forward with critical information. The dynamic adjustment of computational difficulty further strengthens this protection, applying enhanced security to highly sensitive submissions while optimizing resource use for less sensitive evidence.

Moreover, besides the improvements in evidence sensitivity and privacy, our system significantly addresses the critical challenges concerning the whistleblower privacy raised in the recent literature. The study in [35] proposed an anonymous reporting and rewarding mechanism that had a blockchain as the foundation, where whistleblower anonymity was privileged and protected from insider threats since there was no trusted third party involved, allowing individuals to self-report and gain reward for doing so. Similarly, the work in [34] integrated cryptographic ring signatures with blockchain to preserve whistleblower anonymity. These studies validated the potential of blockchain in protecting whistleblower identities. However, a ZKP-based approach provides a significant improvement in further reducing anonymity. Unlike existing solutions, our framework enables whistleblowers to submit evidence anonymously while meeting the stringent requirements for evidence integrity and real-time verification in legal processes. Our proposed framework guarantees the identity privacy of whistleblowers at all times, including during real-time evidence verification processes, by verifying the authenticity of the evidence without disclosing sensitive information. This allows our system to excel in high-stakes and sensitive environments where safeguarding whistleblower privacy is critical. Additionally, the system incorporates the ability for users to dynamically adjust sensitivity levels, ensuring that whistleblower evidence is managed with the proper level of security and privacy.

This study's use of dynamic difficulty adjustments based on evidence sensitivity sets it apart as a unique contribution to DEMS research. Unlike [7], who demonstrated blockchain's role in enhancing chain-of-custody for IoT evidence but applied fixed difficulty and security parameters, our method allows the system to automatically increase computational rigour for highly sensitive evidence, enhancing privacy and security. This adaptability improves performance by preventing unnecessary resource use and makes our approach more versatile and scalable for complex forensic environments with diverse evidence types. Consequently, our work addresses the dual challenge of maintaining evidence integrity and enabling anonymous disclosures, providing a comprehensive and adaptable solution tailored to the practical needs of whistleblowing and secure evidence management.

The dynamic difficulty mechanism in the proposed framework draws inspiration from adaptive protocols like the masked authentication messaging (MAM) protocol in IOTA Tangle [66], which optimises cryptographic effort for environmental IoT devices. However, our approach diverges by prioritizing evidence sensitivity over device constraints, as illustrated in Table 8.

Table 8. Comparison of dynamic difficulty mechanisms.

Metric	MAM Protocol [66]	Proposed Framework
Adjustment basis	Device Capabilities	Evidence sensitivity
Latency reduction	37%	40%
Energy efficiency	45%	38%
Use case	Environmental IoT	Judicial evidence

The authors achieve energy efficiency gains by tailoring cryptographic operations to low-power IoT sensors. In contrast, our framework adjusts proof-of-work (PoW) difficulty based on the sensitivity of judicial evidence (Table 2), ensuring robust protection for high-risk submissions (e.g., whistleblower documents) while optimizing throughput for routine audit logs. This prioritisation reflects the legal system's demand for graded security, where not all evidence requires equal computational rigour.

The trade-off between energy efficiency and latency mirrors trends in decentralised systems [49], but our framework uniquely balances these factors for judicial workflows. For example, the 38% energy efficiency gain (Table 8) is achieved through GPU-accelerated hashing (Section 6), while the 40% latency reduction stems from precomputed challenge ranges (Section 6).

The proposed framework is designed to interoperate with legacy DEMSs to address practical adoption within existing judicial and organisational infrastructures. The following sections detail the integration with DEMSs and present technical strategies, compliance considerations, and mitigation pathways to address integration challenges while maintaining alignment with legal and operational standards.

5.1. Interoperability via Representational State Transfer Application Programming Interfaces

Traditional DEMSs often operate on monolithic architectures with proprietary data formats, which pose significant integration barriers. To bridge this gap, the framework implements representational state transfer application programming interfaces (RESTful APIs) that standardize communication between legacy DEMSs and the blockchain–ZKPs infrastructure [67]. For example, as described in [65]:

- `/submit_evidence` endpoint accepts multipart payloads (e.g., files, metadata) and triggers automated anonymisation via zero-knowledge proofs (ZKPs), returning a blockchain transaction ID for auditability.
- `/verify_evidence` endpoint allows legacy systems to validate evidence authenticity by querying the blockchain with a transaction ID and ZKP challenge, returning a JSON payload with verification status and confirmation count.

Security protocols in application programming interfaces (APIs) interactions enforce OAuth 2.0 authentication [68], and TLS 1.3 encryption [69], ensuring compliance with ISO 27037 guidelines for secure digital evidence handling [5]. Middleware modules, such as Docker containers, encapsulate legacy systems to translate proprietary formats into API-compatible requests, mitigating protocol mismatch [70].

5.2. Hybrid Storage Architecture

Our framework uses a tiered storage model to balance cost efficiency and security. For example, the framework uses the following:

- On-chain storage: Immutable blockchain entries store cryptographic hashes of evidence, ZKPs, and sensitivity metadata. This ensures tamper resistance and auditability for high-sensitivity data (e.g., whistleblower submissions).

- Off-chain storage: Non-sensitive metadata (e.g., timestamps, case tags) resides in legacy SQL databases, while raw files (e.g., videos) are encrypted and archived in cost-effective cloud storage (e.g., AWS S3). Thus, reducing the cost of storage by 52% compared to fully on-chain solutions. In addition, the anonymity provided by the ZKP hashing aligns with general data protection regulation (GDPR) requirements, allowing the erasure of off-chain personal data while preserving on-chain integrity [71].
- Synchronisation mechanism: Event-driven triggers (e.g., AWS Lambda) automate updates between storage layers, ensuring eventual consistency without manual intervention.

5.3. Adoption Challenges and Mitigation

Traditional DEMSs often lack support for decentralised architectures. Therefore, our framework phased deployment prioritizes low-sensitivity evidence (e.g., audit logs) to demonstrate efficacy before handling high-risk cases. In addition, legal teams may also distrust blockchain due to unfamiliarity. As a result, training workshops emphasize compliance with existing standards (e.g., ISO 27037) and simulate evidence verification workflows to build trust.

The proposed framework addresses legacy integration challenges through API-driven interoperability, hybrid storage, and compliance-centred design. Leveraging middleware translation, event-driven synchronisation, and phased adoption strategies provides a transitional pathway for modernising DEMSs without disrupting existing workflows. These measures ensure the framework's applicability in real-world judicial ecosystems while maintaining the integrity and privacy of sensitive evidence.

5.4. Security Analysis

Our proposed framework's reliance on SHA-256 hashing and elliptic-curve-based ZKPs introduces quantum vulnerabilities. Adversaries with quantum computing capabilities could exploit Grover's algorithm to halve hash security [72] or Shor's algorithm to break elliptic-curve signatures [73]. While immediate quantum threats are theoretical, we propose two mitigations:

- Post-quantum agility: Modular replacement of SHA-256 with SHA-3 (quantum-resistant) and migration to zk-STARKs [74], which rely on collision-resistant hashes.
- Hybrid cryptography: Deploying NIST-approved algorithms like CRYSTALS-Kyber [75] for key exchange alongside classical ZKPs, ensuring backward compatibility.

These strategies are deferred to future work but underscore the framework's adaptability.

6. Conclusions

This paper proposes a robust and scalability-driven DEMSs by integrating the advantages of blockchain and ZKPs for tamper-proof evidence verification with sensitivity-aware adjustments without revealing the whistleblower's identity. By using the Evidence Knowledge Bank, we achieve secure and efficient access to metadata, ensuring privacy while maintaining robust verification capabilities. For instance, in whistleblowing cases related to corporate fraud or corruption, this system enables individuals to anonymously submit sensitive evidence while ensuring its authenticity and protecting their identity. This capability addresses a critical gap in traditional systems, often exposing informants to significant risks. For whistleblowers, this system provides an additional layer of confidentiality by ensuring that their identities are never linked to the submitted evidence, thus fostering trust in high-stakes scenarios. The proposed model effectively handles varied sensitivity levels by presenting that the higher sensitivity levels require high computational resources. Results

show that the mining time of the system is more dependent on the evidence sensitivity distribution, as opposed to the amount of evidence. Additionally, this study uses random challenge selection with the proposed solution, demonstrating an essential interdependency between the challenge range and verification success. This feature ensures that even in high-pressure situations, such as organised crime investigations, evidence provided by whistleblowers remains secure and anonymous while meeting stringent forensic requirements. This capability is especially critical for whistleblower-submitted evidence, where verification must occur without exposing the whistleblower's identity or the evidence content. By focusing on sensitivity concerning the range of evidence, this approach confirms that the model scales with evidence count without adding complexity and retaining security properties that make the protocol applicable for real-world digital forensics use cases, particularly in scenarios involving anonymous whistleblower submissions where trust and privacy are paramount.

The limitation of the proposed framework is that it uses the PoW consensus algorithm in which the miners iterate the nonce to solve the puzzle. This may delay the mining process if the data are extensive or the difficulty level increases. Future work will optimise this process for whistleblowing use cases by exploring alternatives such as proof of authority (PoA), which can provide faster consensus while maintaining robust security standards required for sensitive disclosures. Future work may modify the current PoW algorithm by using collaborative mining where the nonce ranges are shared among the miners.

ZKPs provide unparalleled privacy guarantees, but their computational overhead remains a challenge for time-sensitive applications. The framework mitigates this through the following:

- Hardware acceleration (40% latency reduction);
- Precomputed challenge ranges (63% iteration reduction).

However, a fundamental trade-off persists: stricter ZKP parameters (e.g., larger ψ ranges) enhance security at the cost of slower verification. For low-sensitivity evidence, lightweight ZKP variants (e.g., Bulletproof [64]) could further reduce latency by 22–35%, as demonstrated in decentralised voting systems [76]. Future work will explore adaptive ZKP schemes that dynamically adjust cryptographic effort based on real-time threat models.

While quantum resistance is a critical direction for future research, this paper focuses on addressing privacy and scalability challenges in classical DEMSs. Extending the framework to post-quantum settings would require re-engineering core cryptographic components, which we defer to subsequent studies.

Smart contracts are another way to modify the overall model. A set of policies can be designed, which, when met, can support the blockchain model. Furthermore, reducing the number of hash operations can reduce the overall complexity of the model. For whistleblowers, smart contracts could automate access controls and ensure tamper-proof evidence handling without requiring additional intervention, further improving the system's trust and usability.

Author Contributions: Writing of the original draft, B.M., supervised and reviewed by D.M. and M.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are supplied in the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DEMSs	Digital Evidence Management Systems
IoT	Internet of Things
PoW	Proof-of-Work
ZKP	Zero-Knowledge Proof
Miners	Entities Performing PoW
Nodes	All Participants in the Blockchain Network
Provers	Parties Submitting Evidence
Verifiers	Parties Validating Evidence

References

1. Sanjalawe, Y.; Makhadmeh, S.; Alqudah, H. Digital Forensics Meets Blockchain: Enhancing Evidence Authenticity and Traceability. In Proceedings of the 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 26–28 February 2024; pp. 1–6.
2. Kang, M.; Lemieux, V. A decentralized identity-based blockchain solution for privacy-preserving licensing of individual-controlled data to prevent unauthorized secondary data usage. *Ledger* **2021**, *6*. [CrossRef]
3. Effendi, I. Legal Protection for Whistleblowers of Corruption Crime Bring to Fairness. *Sociol. Jurisprud. J.* **2024**, *7*, 31–39. [CrossRef]
4. Nyreröd, T.; Andreadakis, S.; Spagnolo, G. Money laundering and sanctions enforcement: Large rewards, leniency and witness protection for whistleblowers. *J. Money Laund. Control* **2023**, *26*, 912–925. [CrossRef]
5. Khan, A.A.; Shaikh, A.A.; Laghari, A.A. IoT with multimedia investigation: A secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth. *Arab. J. Sci. Eng.* **2023**, *48*, 10173–10188. [CrossRef]
6. Quezada-Tavárez, K.; Vogiatzoglou, P.; Royer, S. Legal challenges in bringing AI evidence to the criminal courtroom. *New J. Eur. Crim. Law* **2021**, *12*, 531–551. [CrossRef]
7. Akhtar, M.S.; Feng, T. Using blockchain to ensure the integrity of digital forensic evidence in an iot environment. *EAI Endorsed Trans. Creat. Technol.* **2022**, *9*, e2. [CrossRef]
8. Stoykova, R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Comput. Law Secur. Rev.* **2021**, *42*, 105575. [CrossRef]
9. Koisser, D.; Sadeghi, A.R. Accountability of Things: Large-Scale Tamper-Evident Logging for Smart Devices. *arXiv* **2023**, arXiv:2308.05557.
10. Elgohary, H.M.; Darwish, S.M.; Elkaffas, S.M. Improving uncertainty in chain of custody for image forensics investigation applications. *IEEE Access* **2022**, *10*, 14669–14679. [CrossRef]
11. Guo, C.; Ashrafian, H.; Ghafur, S.; Fontana, G.; Gardner, C.; Prime, M. Challenges for the evaluation of digital health solutions—A call for innovative evidence generation approaches. *NPJ Digit. Med.* **2020**, *3*, 110. [CrossRef]
12. Meterko, V.; Cooper, G. Cognitive biases in criminal case evaluation: A review of the research. *J. Police Crim. Psychol.* **2022**, *37*, 101–122. [CrossRef]
13. Islam, S.; Apu, K.U. Decentralized Vs. Centralized Database Solutions In Blockchain: Advantages, Challenges, And Use Cases. *Glob. Mainstream J. Innov. Eng. Emerg. Technol.* **2024**, *3*, 58–68. [CrossRef]
14. Surve, T.; Khandelwal, R. The Emergence of Cryptography in Blockchain Technology. In *Concepts, Technologies, Challenges, and the Future of Web 3*; IGI Global: Hershey, PA, USA, 2023; pp. 47–63.
15. Zhang, G. Cryptographic Techniques in Digital Media Security: Current Practices and Future Directions. *Int. J. Adv. Comput. Sci. Appl.* **2024**, *15*, 933–941. [CrossRef]
16. Chew, C.J.; Lee, W.B.; Chen, T.H.; Lin, I.C.; Lee, J.S. Log Preservation in Custody Dual Blockchain With Energy Regime and Obfuscation Shuffle. *IEEE Trans. Netw. Sci. Eng.* **2024**, *11*, 3495–3511. [CrossRef]
17. Didas, M.; Chali, F.H.; Noe, E. Facets related to challenges and prospects of cloud computing adoption in resource-constrained settings: Systematic review analysis. *Int. J. Adv. Comput. Res.* **2024**, *14*, 18.
18. Nadji, B. Data Security, Integrity, and Protection. In *Data, Security, and Trust in Smart Cities*; Springer Nature: Cham, Switzerland, 2024; pp. 59–83.
19. Shen, W.; Yu, J.; Yang, M.; Hu, J. Efficient identity-based data integrity auditing with key-exposure resistance for cloud storage. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 4593–4606. [CrossRef]
20. Habbabeh, A.; Asprion, P.M.; Schneider, B. Mitigating the Risks of Whistleblowing—An Approach Using Distributed System Technologies. In Proceedings of the PoEM Workshops, Basel, Switzerland, 26 November 2020; pp. 47–58.

21. Bamberger, K.A.; Canetti, R.; Goldwasser, S.; Wexler, R.; Zimmerman, E.J. Verification dilemmas in law and the promise of zero-knowledge proofs. *Berkeley Tech. Law J.* **2022**, *37*, 1. [CrossRef]
22. Bitan, D.; Canetti, R.; Goldwasser, S.; Wexler, R. Using zero-knowledge to reconcile law enforcement secrecy and fair trial rights in criminal cases. In Proceedings of the 2022 Symposium on Computer Science and Law, Washington, DC, USA, 1–2 November 2022; pp. 9–22.
23. Ahmed, M.R.; Islam, A.M.; Shatabda, S.; Islam, S. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *IEEE Access* **2022**, *10*, 113436–113481. [CrossRef]
24. Hossain, M.B.; Rahayu, M.; Ali, M.A.; Huda, S.; Kodera, Y.; Nogami, Y. A blockchain-based approach with zk-snarks for secure email applications. *Int. J. Netw. Comput.* **2024**, *14*, 225–247. [CrossRef]
25. Li, M.; Lal, C.; Conti, M.; Hu, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Gener. Comput. Syst.* **2021**, *115*, 406–420. [CrossRef]
26. Mitchell, I.; Hara, S.; Jahankhani, H.; Neilson, D. Blockchain of custody, BoC. In *Cyber Security Practitioner's Guide*; World Scientific: Singapore, 2020; pp. 365–397.
27. Ahmad, L.; Khanji, S.; Iqbal, F.; Kamoun, F. Blockchain-based chain of custody: Towards real-time tamper-proof evidence management. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual, 25–28 August 2020; pp. 1–8.
28. Qin, X.; Huang, Y.; Yang, Z.; Li, X. A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. *J. Syst. Archit.* **2021**, *112*, 101854. [CrossRef]
29. Ali, I.M.; Caprolu, M.; Pietro, R.D. Foundations, properties, and security applications of puzzles: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–38. [CrossRef]
30. González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors* **2021**, *21*, 4759. [CrossRef] [PubMed]
31. Singh, A.; Ikuesan, R.A.; Venter, H. Secure storage model for digital forensic readiness. *IEEE Access* **2022**, *10*, 19469–19480. [CrossRef]
32. Casino, F.; Dasaklis, T.K.; Spathoulas, G.P.; Anagnostopoulos, M.; Ghosal, A.; Borocz, I.; Solanas, A.; Conti, M.; Patsakis, C. Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access* **2022**, *10*, 25464–25493. [CrossRef]
33. Taiwo, A.; Claims, I. An extended digital forensic readiness and maturity model. *Forensic Sci. Int. Digit. Investig.* **2022**, *40*, 301348.
34. Tomaz, A.E.B.; Nascimento, J.C.d.; de Souza, J.N. Blockchain-based whistleblowing service to solve the problem of journalistic conflict of interest. *Ann. Telecommun.* **2022**, *77*, 101–118. [CrossRef]
35. Patil, S.; Parmar, K. Novel mechanism for anonymous reporting and anonymous rewarding using blockchain technology. *Int. J. Inf. Secur.* **2025**, *24*, 2. [CrossRef]
36. Jastaniah, K.; Zhang, N.; Mustafa, M.A. Efficient Privacy-Friendly and Flexible Wearable Data Processing With User-Centric Access Control. *IEEE Access* **2024**, *12*, 37012–37029. [CrossRef]
37. Kirubakaran, S.S.; Arunachalam, V.; Karthik, S.; Kannan, S. Towards Developing Privacy-Preserved Data Security Approach (PP-DSA) in Cloud Computing Environment. *Comput. Syst. Sci. Eng.* **2023**, *44*, 1881–1895. [CrossRef]
38. Liu, T.; Xie, T.; Zhang, J.; Song, D.; Zhang, Y. Pianist: Scalable zkrollups via fully distributed zero-knowledge proofs. In Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–22 May 2024; pp. 1777–1793.
39. Pillai, S.E.V.S.; Polimetla, K. Enhancing Network Privacy through Secure Multi-Party Computation in Cloud Environments. In Proceedings of the 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 23–24 February 2024; pp. 1–6.
40. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Bitcoin* **2008**, *4*, 15.
41. Tian, Z.; Li, M.; Qiu, M.; Sun, Y.; Su, S. Block-DEF: A secure digital evidence framework using blockchain. *Inf. Sci.* **2019**, *491*, 151–165. [CrossRef]
42. Philip, A.O.; Saravanaguru, R.K. Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *J. King Saud-Univ.-Comput. Inf. Sci.* **2022**, *34*, 4031–4046. [CrossRef]
43. Sathyaprakasan, R.; Govindan, P.; Alvi, S.; Sadath, L.; Philip, S.; Singh, N. An implementation of blockchain technology in forensic evidence management. In Proceedings of the 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 17–18 March 2021; pp. 208–212.
44. Alqahtany, S.S.; Syed, T.A. ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. *Information* **2024**, *15*, 109. [CrossRef]
45. Zhang, Z.; Li, W.; Liu, H.; Liu, J. A refined analysis of zcash anonymity. *IEEE Access* **2020**, *8*, 31845–31853. [CrossRef]
46. Ballesteros-Rodríguez, A.; Sánchez-Alonso, S.; Sicilia-Urbán, M.Á. Enhancing Privacy and Integrity in Computing Services Provisioning Using Blockchain and zk-SNARKs. *IEEE Access* **2024**, *12*, 117970–117993. [CrossRef]

47. Chi, P.W.; Lu, Y.H.; Guan, A. A privacy-preserving zero-knowledge proof for blockchain. *IEEE Access* **2023**, *11*, 85108–85117. [CrossRef]
48. Kuznetsov, O.; Rusnak, A.; Yezhov, A.; Kanonik, D.; Kuznetsova, K.; Karashchuk, S. Enhanced Security and Efficiency in Blockchain with Aggregated Zero-Knowledge Proof Mechanisms. *IEEE Access* **2024**, *12*, 2024 . . [CrossRef]
49. Zhao, W.; Aldyaflah, I.M.; Gangwani, P.; Joshi, S.; Upadhyay, H.; Lagos, L. A blockchain-facilitated secure sensing data processing and logging system. *IEEE Access* **2023**, *11*, 21712–21728. [CrossRef]
50. Ben-Sasson, E.; Chiesa, A.; Tromer, E.; Virza, M. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. *USENIX Secur. Symp.* **2014**, 781–796.
51. Yang, Z.; Alfauri, H.; Farkiani, B.; Jain, R.; Di Pietro, R.; Erbad, A. A survey and comparison of post-quantum and quantum blockchains. *IEEE Commun. Surv. Tutor.* **2023**, *26*, 967–1002. [CrossRef]
52. Bernstein, D.J.; Hülsing, A.; Kolbl, S.; Niederhagen, R.; Rijneveld, J.; Schwabe, P. The SPHINCS+ Signature Framework. *IACR Cryptol. Eprint Arch.* **2017**, *2017*, 1086.
53. Das, P. Design and Comparative Analysis of Quantum Hashing Algorithms using Qiskit. *TechRxiv* **2023**. [CrossRef]
54. Ikeda, K. qBitcoin: A peer-to-peer quantum cash system. In *Intelligent Computing.SAI 2018*; Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2018.
55. Hafiz, M.W.; Deebak, B.; Majeed, A.; Hwang, S.O. QuChain: On the Security and Privacy of Peer-to-Peer System using Blind Quantum Computation. In Proceedings of the 2023 IEEE 23rd International Conference on Nanotechnology (NANO), Jeju Island, Republic of Korea, 2–5 July 2023; pp. 1–6.
56. Sheoran, S.K.; Yadav, G. Promises and Perils of Post-Quantum Blockchain. *Int. J. Future Gener. Commun. Netw.* **2023**, *13*, 4.
57. Boretti, A. Technical, economic, and societal risks in the progress of artificial intelligence driven quantum technologies. *Discov. Artif. Intell.* **2024**, *4*, 67. [CrossRef]
58. Shang, T.; Tang, Y.; Zhang, Y.; Zhang, K.; Jiang, Y. Multi-party quantum Byzantine consensus based on full quantum one-way function. *Quantum Inf. Process.* **2024**, *24*, 3. [CrossRef]
59. Baseri, Y.; Hafid, A.; Shahsavari, Y.; Makrakis, D.; Khodaiemehr, H. Blockchain Security Risk Assessment in Quantum Era, Migration Strategies and Proactive Defense. *arXiv* **2025**, arXiv:2501.11798.
60. Joseph, T.; Vijayalakshmi, A. Natural Language Processing for Legal Document Classification. In *Enhancing Communication and Decision-Making with AI*; IGI Global: Hershey, PA, USA, 2025; pp. 295–316.
61. Soesanto, D.; Adji, T.B.; Ardiyanto, I. Adaptive proof of work architecture des ign by implementing multiple mempool. In Proceedings of the 2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS), Bandung, Indonesia, 23 November 2022; pp. 1–8.
62. Sagirlar, G.; Carminati, B.; Ferrari, E.; Sheehan, J.D.; Ragnoli, E. Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1007–1016.
63. Ben-Sasson, E.; Chiesa, A.; Tromer, E.; Virza, M. Scalable Zero Knowledge via Cycles of Elliptic Curves. *Algorithmica* **2017**, *79*, 1102–1160. [CrossRef]
64. Bünz, B.; Bootle, J.; Boneh, D.; Poelstra, A.; Wuille, P. Bulletproofs: Short Proofs for Confidential Transactions and More. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24 May 2018; pp. 315–334.
65. Mbimbi, B. Preserving-Whistleblower-Anonymity-Through-ZKP. 2025. Available online: https://github.com/Butrus32518528/Preserving-Whistleblower-Anonymity-through-ZKP (accessed on 11 February 2025).
66. Gangwani, P.; Perez-Pons, A.; Bhardwaj, T.; Upadhyay, H.; Joshi, S.; Lagos, L. Securing environmental IoT data using masked authentication messaging protocol in a DAG-based blockchain: IOTA tangle. *Future Internet* **2021**, *13*, 312. [CrossRef]
67. Moe, A.J.; Jarbeaux, W.; Moe, T.B.; Younger, E. Digital Evidence Management. Bachelor's Thesis, Norwegian University of Science and Technology, New Taipei City, Taiwan 2021.
68. Hardt, D. The OAuth 2.0 Authorization Framework. RFC 6749, Internet Engineering Task Force (IETF), 5177 Brandin Ct, Fremont, California, 94538, United States, 2012; pp. 11–67. Available online: https://shorturl.at/fEG9v (accessed on 11 February 2025).
69. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, Internet Engineering Task Force (IETF), 5177 Brandin Ct, Fremont, California, 94538, United State, 2018; p. 1. Available online: https://www.rfc-editor.org/rfc/rfc8446 (accessed on 11 February 2025).
70. Merkel, D. Docker: Lightweight Linux Containers for Consistent Development and Deployment. *Linux J.* **2024**, *2024*, 2.
71. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Secur. Priv.* **2015**, *13*, 72–76.
72. Grover, L.K. A Fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96), Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.

73. Shor, P.W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS '94), Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
74. Ben-Sasson, E.; Bentov, I.; Horesh, Y.; Riabzev, M. Scalable, Transparent, and Post-Quantum Secure Computational Integrity. *Cryptology ePrint Archive, Report 2018/046* **2018**. p. 1. Available online: https://eprint.iacr.org/2018/46 (accessed on 11 February 2025).
75. Avanzi, R.; Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Kyber algorithm specifications and supporting documentation. *NIST PQC Round* **2019**, *2*, 1–43.
76. Firoozjaei, M.D.; Lu, R.; Ghorbani, A.A. An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. *Secur. Priv.* **2020**, *3*, e131. [CrossRef]