A Blockchain-Based System for Tamper-Evidence and Integrity Verification of Digital Evidence

A Capstone Project by

Philip Lee Anthony Artianza
Steven Benedict Bernabe
John Pruds Colot
Jino Taer

Submitted to the Information Technology Department, College of Technologies
Bukidnon State University

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Science in Information Technology

June 04, 2027

1 INTRODUCTION

1.1 Background of the Study

Digital evidence has become increasingly critical in modern legal proceedings, serving as a definitive basis for decisions in criminal investigations and civil lawsuits (Rana et al., 2023; Satapathy & Nagasshree MN, 2025). Traditional digital evidence management often relies on physical hard disk drives from collection to court submission, creating a **risk of damage and manipulation** where the chain of custody cannot be guaranteed (Kim et al., 2021). Digital evidence was admitted in **72% of cybercrime cases, while 28% was rejected**. A total of **50 cybercrime cases** were analyzed (Abdullah et al., 2025). This high acceptance rate indicates the increasing use of digital forensics in technology-based crimes (Abdullah et al., 2025). This vulnerability can lead to evidence being dismissed in court due to questions about its reliability (Kim et al., 2021). Statistics from South Korea highlight the growing volume of digital evidence, which increased from **14,899 cases in 2014 to 45,103 in 2018**, underscoring the escalating need for secure and systematic management (Kim et al., 2021). In the Asia-Pacific region, cybercrime has surged dramatically, with the Philippines ranking **second globally in cyber threats and attacks** during the onset of pandemic due to increased digital platform usage (G. Pasinhon & M. Donato, 2024).

Pre-existing digital evidence management tools are generally centralized in design most institutions still store and manage sensitive case data on a single device or within a centralized system, despite escalating reliance on digital evidence in investigations and trials (Shatakshi Johri, 2024). The existing systems for evidence storage often rely on **centralized databases** or servers,

making them vulnerable to hacks, data breaches, and unauthorized access, which is prone to **tampering** (Patil et al., 2024). These systems are often maintained by a central authority or organization, which creates vulnerabilities and opportunities for manipulation (Mustafa M et al., 2024). Without stronger mechanisms to secure and verify the integrity of evidence, the reliability of centralized systems remains questionable, and this challenge is even more evident in localities like Malaybalay City, where no blockchain-based digital evidence framework currently exists.

The alteration or tampering of digital evidence represents a serious threat to the justice system, as it undermines the very foundation of fairness and objectivity in legal proceedings. When evidence presented in court cannot be trusted to be authentic, its probative value is diminished, often resulting in the dismissal of critical cases or worse, **wrongful conviction,** which is need to be avoided (Abdullah et al., 2025). According to Sanchirico (2004, as cited in Vanini et al., (2024)), the intentional act of **altering, concealing, or falsifying evidence** poses significant dangers, as fictitious or fake traces can easily alter or sabotage criminal investigations. The absence of a robust solution to this problem continues to pose challenges in ensuring justice in an increasingly digital world.

This study proposes the utilization of blockchain technology as a framework for enhancing the management and security of digital evidence. Unlike traditional centralized systems, blockchain operates on a **decentralized** network where records are distributed across multiple nodes, making it extremely difficult for any single party to manipulate data undetected. Each transaction or record stored on the blockchain is cryptographically linked together, creating an immutable ledger of information (Singh, 2025). Blockchain technology is a solution for digital evidence because it ensures

immutability, transparency, and non-repudiation of both access control mechanisms and the digital evidence itself, thereby addressing the limitations of traditional digital forensics where data can be altered or tampered with (Miller & Singh, 2024). By applying this technology to digital evidence management, the proposed system will provide a **tamper-evident** mechanism where any attempt to alter evidence will be recorded and flagged. Additionally, the transparency offered by blockchain ensures that all stakeholders can trace the history of evidence, including its origin, access points, and any modifications, thereby strengthening the chain of custody. Such a system will not only improve security but also promote accountability and trust in the handling of digital evidence.

A review of digital-forensics and blockchain literature indicates that existing solutions address individual aspects of evidence management but never combine all the features envisioned for this capstone. Some research uses the Polygon blockchain with IPFS to decentralize the storage and management of digital evidence, while other work employs zero-knowledge proofs (ZKPs) for privacy-preserving verification in unrelated contexts such as academic record systems. However, **no existing study integrates real-time monitoring, automated ZKP generation, IPFS decentralized storage, the Polygon blockchain, and support for multimedia evidence** into a single framework. This absence underscores the novelty of a Real-Time ZKP-Verified Multimedia Evidence Protection System with Automated Tamper Detection on an IPFS-Polygon architecture.

The core of this integrity lies in **cryptographic hashing**, where any change to a document's data will generate a completely different hash, making any manipulation immediately **detectable** and ensuring **authenticity** (Kailas Bharati, 2025). Any attempt to manipulate digital evidence is thus made **transparent** through blockchain’s consensus and verification mechanisms, ensuring that

discrepancies are identified. Ultimately, this **blockchain-based framework aims to strengthen the integrity of legal processes**, reduce the risks associated with centralized evidence storage, and contribute to a more trustworthy and just judicial system in the digital age.

This work's key contributions are twofold. First, it utilizes **cryptographic hashing** to make any **manipulation** of digital evidence immediately **detectable**, ensuring **authenticity**. Second, it leverages **blockchain's transparency** to strengthen the entire **legal process**, reducing the risks of **centralized storage** and promoting a more **just judicial system**.

1.2 Objectives of the Study

General Objective:

To develop a blockchain-based system for tamper-evidence and integrity verification of digital evidence, specifically:

Specific Objectives:

a) Gather data on the current practices of digital evidence management in Malaybalay City, including challenges faced by law enforcement agencies.

b) Design a system architecture that ensures the cryptographic protection and access control of digital evidence.

c) Develop the system's core functionality for uploading and immutably retaining the metadata of digital evidence on the blockchain and uploads and store the digital evidence through IPFS.

d) Conduct system testing to validate its functionality, security, reliability, and accuracy.

e) Evaluate the system's usability employing the System Usability Scale (SUS) questionnaire.

1.3 Significance of the Study

The development of a blockchain-based digital evidence system will provide **significant benefits** to multiple stakeholders in the criminal justice ecosystem:

Bukidnon State University (BukSU): As the academic institution of the researchers, this study contributes to the body of knowledge on blockchain applications in digital forensics and provides a foundation for future research in information security and governance.

Local Government Unit (LGU) of Malaybalay City: The system can support LGU initiatives toward digitalization and modernization of public services, ensuring transparency in processes that involve sensitive data.

Philippine National Police (PNP): As primary users of digital evidence, the police will directly benefit from a secure, tamper-evident system that strengthens the chain of custody and increases the reliability of evidence in court.

Judiciary and Legal Practitioners: The proposed system enhances confidence in the integrity of digital evidence, supporting fair and transparent court proceedings.

Community and Citizens: By ensuring that digital evidence is authentic and untampered, the system reinforces trust in the justice system and contributes to the promotion of peace, order, and public trust.

1.4 Scope and Delimitations

This study is driven by the need to enhance the integrity and trustworthiness of digital evidence management for law enforcement agencies in Malaybalay City, Bukidnon. To ensure a focused and feasible investigation, the research is bounded by specific technical, geographical, and operational parameters. The following sections detail the precise focus (Scope) and the intentional boundaries (Delimitations) of this project.

Scope:

This study focuses on the design, development, and evaluation of a blockchain-based system for tamper evidence and integrity verification of digital evidence, implemented strictly as a browser-based web application. It will cover the process of collecting digital evidence, recording it on the blockchain, securing it against tampering, and maintaining transparency in the chain of custody. The solution will be delivered exclusively as a web application with no native mobile or desktop clients, accessed via standard web browsers. The system will be tested in

a controlled environment within Malaybalay City, involving law enforcement representatives, academic evaluators, and local stakeholders for validation.

Delimitations:

The study is geographically limited to Malaybalay City, Bukidnon, and does not extend to other jurisdictions or regions. The system design and requirements analysis are based specifically on the local context and may not be directly applicable to other locations without modification. The research focuses exclusively on digital evidence management and does not address physical evidence handling or storage. The system does not include features for evidence analysis, content examination, or forensic investigation tools beyond evidence protection and chain of custody maintenance. The study does not encompass integration with existing national or international criminal justice information systems, limiting its scope to local implementation. Cross-jurisdictional evidence sharing and inter-agency collaboration features are not included in the current system design. The research does not address legal framework modifications or policy changes that may be required for blockchain evidence admissibility in Philippine courts. The study assumes current legal standards and focuses on technical implementation rather than legal reform.

2 REVIEW OF RELATED LITERATURE

2.1 Digital Evidence in Legal Systems

Digital evidence has become increasingly critical in modern legal proceedings, serving as a definitive basis for decisions in criminal investigations and civil lawsuits (Rana et al., 2023; Satapathy & Nagasshree MN, 2025). The evolution of digital technology has fundamentally transformed the nature of evidence collection, preservation, and presentation in judicial systems worldwide. Unlike traditional physical evidence, digital evidence encompasses a wide range of data formats including electronic documents, emails, audio-video recordings, network logs, mobile device data, and multimedia files that can be extracted from various digital sources (Dhulavvagol et al., 2024).

The admissibility and reliability of digital evidence in court proceedings depend on several critical factors, including authenticity, completeness, reliability, and credibility (Loffi et al., 2025). According to research conducted by Abdullah et al. (2025), digital evidence was admitted in 72% of cybercrime cases, while 28% was rejected out of a total of 50 cybercrime cases analyzed. This high acceptance rate indicates the increasing use of digital forensics in technology-based crimes and underscores the growing dependence of judicial systems on digital evidence to establish facts and support legal decisions. The significance of digital evidence extends beyond mere documentation; it serves as the cornerstone for establishing truth, proving guilt or innocence, and ensuring justice in an increasingly digital society.

However, the increasing reliance on digital evidence also brings substantial challenges. Digital evidence is inherently volatile and susceptible to manipulation or alteration throughout its lifecycle, from collection to presentation in court (Peelam et al., 2025). The fragile nature of digital data means that improper handling, inadequate preservation methods, or unauthorized access can compromise the integrity of evidence, potentially leading to wrongful convictions or the dismissal of legitimate cases. As cybercrime investigations become more complex and involve multiple jurisdictions, the need for robust, tamper-proof systems to manage digital evidence has never been more critical.

2.2 Traditional Evidence Management Vulnerabilities

Traditional digital evidence management often relies on physical hard disk drives from collection to court submission, creating a risk of damage and manipulation where the chain of custody cannot be guaranteed (Kim et al., 2021). This conventional approach to evidence handling introduces numerous vulnerabilities that can compromise the integrity and admissibility of critical evidence in judicial proceedings. The centralized nature of traditional evidence management systems creates single points of failure that can be exploited by malicious actors or compromised through technical failures, administrative errors, or institutional weaknesses.

Pre-existing digital evidence management tools are generally centralized in design, with most institutions still storing and managing sensitive case data on a single device or within a centralized system, despite escalating reliance on digital evidence in investigations and trials (Johri, 2024). The existing systems for evidence storage often rely on centralized databases or servers,

making them vulnerable to hacks, data breaches, and unauthorized access, which is prone to tampering (Patil et al., 2024). These centralized systems are often maintained by a central authority or organization, which creates vulnerabilities and opportunities for manipulation (Mustafa M et al., 2024). The concentration of control and authority in a single entity or system creates inherent security risks and reduces accountability, as there are limited mechanisms for external verification or independent audit of evidence handling procedures.

The vulnerability of centralized evidence management systems is particularly concerning in the context of high-profile cases or situations where institutional corruption or coercion may be present. According to Shahaab et al. (2021), evidence destruction and tampering is a time-tested tactic to protect powerful perpetrators, criminals, and corrupt officials, especially in countries where law enforcing institutions and judicial systems can be compromised. Without stronger mechanisms to secure and verify the integrity of evidence, the reliability of centralized systems remains questionable, and this challenge is even more evident in localities like Malaybalay City, where no blockchain-based digital evidence framework currently exists.

Research has identified several critical research gaps in the field of forensic evidence management concerning the integration of blockchain and distributed storage systems. These gaps include the absence of specific studies focusing on the combination of blockchain technologies with decentralized storage for forensic evidence management, limited attention to scalability and performance in blockchain-based solutions, insufficient exploration of distributed file systems like IPFS for decentralized forensic evidence storage and retrieval, and a lack of practical implementation and evaluation of blockchain frameworks in real-world forensic scenarios (Dhulavvagol et al., 2024).

The absence of comprehensive frameworks integrating blockchain, decentralized storage, and automated verification mechanisms represents a significant gap that the proposed system aims to address.

2.3 Evidence Tampering Threats

The alteration or tampering of digital evidence represents a serious threat to the justice system, as it undermines the very foundation of fairness and objectivity in legal proceedings. When evidence presented in court cannot be trusted to be authentic, its probative value is diminished, often resulting in the dismissal of critical cases or worse, wrongful conviction, which needs to be avoided (Abdullah et al., 2025). The manipulation of digital evidence can occur at various stages of the evidence lifecycle, including during collection, storage, analysis, transfer, or presentation, and can be perpetrated by various actors including criminals, corrupt officials, or even compromised forensic professionals.

According to Sanchirico (2004, as cited in Vanini et al., 2024), the intentional act of altering, concealing, or falsifying evidence poses significant dangers, as fictitious or fake traces can easily alter or sabotage criminal investigations. The consequences of evidence tampering extend far beyond individual cases; they erode public trust in the judicial system, undermine the rule of law, and can lead to systemic failures in the administration of justice. In cases where evidence has been tampered with, innocent individuals may be wrongfully convicted while guilty parties escape justice, representing a fundamental failure of the legal system to fulfill its core purpose of protecting society and ensuring fair treatment under the law.

The vulnerability of digital evidence to tampering is exacerbated by the ease with which digital data can be modified without leaving obvious traces. Unlike physical evidence, which often shows visible signs of tampering, digital evidence can be altered in sophisticated ways that may be difficult or impossible to detect without specialized forensic analysis and robust integrity verification mechanisms. Research by Chukwuani and Ikemefuna (2025) emphasizes that traditional chain-of-custody mechanisms in digital forensics rely heavily on centralized systems, manual logging, and institutional trust, all of which are prone to human error, tampering, and data loss.

The absence of a robust solution to prevent evidence tampering continues to pose challenges in ensuring justice in an increasingly digital world. According to research on evidence management systems, maintaining data integrity during storage and transfer is challenging, and real-time data access for forensic investigations is limited in conventional centralized systems (Loffi et al., 2025). The proposed blockchain-based framework aims to address these fundamental weaknesses by providing cryptographic mechanisms and decentralized verification processes that make tampering immediately detectable and practically impossible to conceal.

2.4 Blockchain for Evidence Security

This study proposes the utilization of blockchain technology as a framework for enhancing the management and security of digital evidence. Unlike traditional centralized systems, blockchain operates on a decentralized network where records are distributed across multiple nodes, making it extremely difficult for any single party to manipulate data undetected. Each transaction or record stored on the blockchain is cryptographically linked together, creating an immutable ledger of

information (Singh, 2025). The fundamental properties of blockchain technology—including decentralization, immutability, transparency, and cryptographic security—make it exceptionally well-suited for addressing the critical challenges of digital evidence management in forensic and judicial contexts.

Blockchain technology is a solution for digital evidence because it ensures immutability, transparency, and non-repudiation of both access control mechanisms and the digital evidence itself, thereby addressing the limitations of traditional digital forensics where data can be altered or tampered with (Miller & Singh, 2024). The decentralized architecture of blockchain eliminates single points of failure and reduces the risk of centralized attacks or institutional manipulation. By distributing the ledger across multiple trusted nodes in a forensic network, blockchain ensures that evidence records cannot be altered without detection, as any attempt to modify a block would require altering all subsequent blocks across the majority of nodes—a computationally infeasible task (Rana et al., 2023).

By applying this technology to digital evidence management, the proposed system will provide a tamper-evident mechanism where any attempt to alter evidence will be recorded and flagged. Additionally, the transparency offered by blockchain ensures that all stakeholders can trace the history of evidence, including its origin, access points, and any modifications, thereby strengthening the chain of custody. The chain of custody refers to the documented and unbroken process that demonstrates the control, transfer, and analysis of evidence from the moment of acquisition to its presentation in court (Loffi et al., 2025). In traditional environments, this process relies on physical logs, manual documentation, and trust in human intermediaries to maintain

evidentiary integrity; however, when applied to digital evidence, these manual systems are often inadequate (Chukwuani & Ikemefuna, 2025).

Such a blockchain-based system will not only improve security but also promote accountability and trust in the handling of digital evidence. Research has demonstrated that blockchain-enabled systems can provide a secure, transparent, and tamper-proof process for handling digital evidence, involving multiple stakeholders such as the police, the court, and authorized forensic professionals through web interfaces (Dhulavvagol et al., 2024). Blockchain technology ensures data integrity and security, while distributed storage systems like IPFS provide efficient decentralized storage. This approach offers trustworthiness and accountability throughout forensic evidence management, addressing the critical vulnerabilities inherent in traditional centralized systems.

The practical implementation of blockchain in evidence management has been explored in various research contexts. For example, the SHARD-FEMF framework, which integrates blockchain sharding and IPFS technologies, demonstrates significant improvements in memory utilization (25%), reduction in gas utilization (21.5%), and enhancement in transaction scalability (23%) compared to existing centralized schemes (Dhulavvagol et al., 2024). These performance improvements indicate that blockchain-based solutions are not only theoretically sound but also practically viable for real-world forensic applications.

2.5 Real-Time ZKP Multimedia Protection

A review of digital forensics and blockchain literature indicates that existing solutions address individual aspects of evidence management but never combine all the features envisioned for this capstone. Some research uses the Polygon blockchain with IPFS to decentralize the storage and management of digital evidence, while other work employs zero-knowledge proofs (ZKPs) for privacy-preserving verification in unrelated contexts such as academic record systems. However, no existing study integrates real-time monitoring, automated ZKP generation, IPFS decentralized storage, the Polygon blockchain, and support for multimedia evidence into a single framework. This absence underscores the novelty of a Real-Time ZKP Verified Multimedia Evidence Protection System with Automated Tamper Detection on an IPFS-Polygon architecture.

The integration of zero-knowledge proofs with blockchain technology represents a significant advancement in evidence verification while maintaining privacy and confidentiality. Zero-knowledge proofs allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement itself. In the context of evidence management, ZKPs enable forensic professionals and judicial authorities to verify the integrity and authenticity of evidence without exposing sensitive details about the evidence content or the cryptographic keys used for protection (Li et al., 2019). This privacy-preserving characteristic is particularly important in cases involving sensitive personal information, ongoing investigations, or national security matters.

The Polygon blockchain offers specific advantages for forensic applications compared to other blockchain platforms. Polygon is a Layer 2 scaling solution for Ethereum that provides

enhanced transaction throughput, reduced costs, and improved scalability while maintaining the security guarantees of the underlying Ethereum network (Rana et al., 2023). The use of Polygon addresses one of the primary limitations of public blockchains like Ethereum—high transaction fees and slow processing times—which have restricted their use in large-scale forensic operations (Loffi et al., 2025). By implementing the evidence management system on Polygon, the proposed framework can achieve cost-effective and scalable operations suitable for real-world deployment in law enforcement agencies and judicial institutions.

The integration of IPFS (InterPlanetary File System) for decentralized storage addresses another critical challenge in blockchain-based evidence management: the limitation of on-chain storage capacity. Storing large multimedia files directly on the blockchain is impractical due to size constraints and high storage costs. IPFS provides a distributed, content-addressed storage system where files are broken down into smaller data chunks and distributed across a network of nodes (Dhulavvagol et al., 2024). This decentralization enhances reliability by eliminating single points of failure and introduces content-based addressing, where each piece of evidence is associated with a unique cryptographic hash derived from its content, ensuring tamper-proofing and efficient retrieval.

The proposed system's support for multimedia evidence—including images, videos, audio recordings, and documents—represents a significant advancement over existing solutions that primarily focus on textual data or generic digital files. Multimedia evidence is increasingly common in modern investigations, particularly in cases involving surveillance footage, body camera recordings, digital photography, and communication records (Peelam et al., 2025). The ability to securely manage and verify multimedia evidence while maintaining its integrity throughout the

evidence lifecycle is essential for ensuring the admissibility and reliability of such evidence in court proceedings.

Real-time monitoring and automated tamper detection constitute critical innovations in the proposed framework. Traditional evidence management systems typically rely on periodic manual audits or post-incident forensic analysis to detect tampering or unauthorized access. The proposed system implements continuous monitoring mechanisms that automatically detect and flag any unauthorized access attempts, integrity violations, or suspicious activities in real-time (Ghimire et al., 2020). This proactive approach significantly enhances the security posture of evidence management systems and enables rapid response to potential security incidents before they can compromise critical evidence.

2.6 Cryptographic Integrity Verification

The core of evidence integrity lies in cryptographic hashing, where any change to a document's data will generate a completely different hash, making any manipulation immediately detectable and ensuring authenticity (Bharati, 2025). Cryptographic hash functions are mathematical algorithms that take an input of arbitrary size and produce a fixed-size output (the hash value or digest) that uniquely represents the input data. The properties of cryptographic hash functions—including determinism, avalanche effect, pre-image resistance, and collision resistance—make them ideal for verifying data integrity in forensic contexts.

In the proposed evidence management system, cryptographic hashing serves multiple critical functions. First, at the point of evidence collection, a cryptographic hash is computed for each

piece of evidence and recorded on the blockchain. This original hash serves as a "digital fingerprint" that uniquely identifies the evidence in its original state. Any subsequent modification to the evidence, no matter how minor, will result in a completely different hash value, immediately revealing that tampering has occurred (Singh, 2025). This mechanism provides mathematical certainty regarding evidence integrity that far exceeds the reliability of traditional manual verification methods.

The implementation of hash-based integrity verification in blockchain systems has been extensively validated in forensic research. Studies have shown that blockchain-based evidence management systems using SHA-256 or SHA-3 hashing algorithms can detect even single-bit modifications to evidence files, providing extremely high levels of tamper detection sensitivity (Dhulavvagol et al., 2024). The cryptographic strength of these hash functions ensures that it is computationally infeasible for an attacker to modify evidence in a way that produces the same hash value, effectively making evidence tampering detectable with very high probability.

Any attempt to manipulate digital evidence is thus made transparent through blockchain's consensus and verification mechanisms, ensuring that discrepancies are identified. The consensus protocols used in blockchain networks require that multiple nodes verify and agree upon the validity of transactions before they are permanently recorded on the ledger (Chukwuani & Ikemefuna, 2025). This distributed verification process creates multiple independent checks on evidence integrity, making it extremely difficult for malicious actors to successfully tamper with evidence without detection. Even if an attacker manages to compromise a single node in the network, the consensus mechanism ensures that such tampering will be rejected by the honest majority of nodes.

The integration of Merkle trees and Merkle proofs provides additional layers of verification efficiency. Merkle trees are hierarchical data structures that allow for compact and efficient integrity proofs by organizing hash values in a tree structure where each non-leaf node is the hash of its child nodes (Loffi et al., 2025). This structure enables the verification of specific pieces of evidence without requiring access to the entire evidence database, improving both efficiency and privacy. Merkle proofs can confirm the integrity of evidence without revealing the full dataset, which is particularly valuable in scenarios where evidence confidentiality must be maintained while still allowing for integrity verification.

2.7 Blockchain-Enhanced Legal Processes

Ultimately, this blockchain-based framework aims to strengthen the integrity of legal processes, reduce the risks associated with centralized evidence storage, and contribute to a more trustworthy and just judicial system in the digital age. The transformation of evidence management through blockchain technology has profound implications not only for the technical aspects of forensic science but also for the broader functioning of judicial systems and the maintenance of public trust in legal institutions. By providing verifiable, tamper-proof records of evidence handling, blockchain-based systems address fundamental concerns about the reliability and credibility of digital evidence in court proceedings.

The enhancement of evidence integrity through blockchain has direct implications for reducing wrongful convictions and ensuring that judicial verdicts are based on reliable, authenticated evidence. Research has shown that flaws in evidence handling and chain-of-custody procedures

have contributed to miscarriages of justice in numerous cases (Abdullah et al., 2025). By implementing robust technological safeguards that make evidence tampering practically impossible and immediately detectable, blockchain-based evidence management systems can significantly reduce the risk of such failures and enhance confidence in judicial outcomes.

The transparency and auditability provided by blockchain technology also promote accountability among all stakeholders involved in evidence handling. In traditional systems, it may be difficult or impossible to determine who accessed evidence, when access occurred, or what actions were taken. Blockchain-based systems maintain a complete, immutable audit trail that documents every interaction with evidence, creating clear lines of accountability and deterring potential misconduct (Shahaab et al., 2021). This enhanced accountability extends not only to law enforcement officers and forensic analysts but also to judicial officials, legal representatives, and other parties who may interact with evidence during the course of an investigation or trial.

The reduction of risks associated with centralized evidence storage is particularly important in contexts where institutional weaknesses or corruption may compromise traditional evidence management systems. By distributing evidence records across multiple nodes and eliminating single points of control, blockchain-based systems reduce the vulnerability to institutional failure or malicious manipulation (Peelam et al., 2025). This decentralization of authority and verification creates a more resilient system that can maintain integrity even in the face of attempts at corruption or coercion.

The proposed framework also contributes to the broader goal of judicial modernization and digital transformation. As societies become increasingly digital and technology-dependent, judicial

systems must evolve to effectively handle the types of evidence and investigative challenges that arise in digital contexts. The integration of advanced technologies like blockchain, zero-knowledge proofs, and decentralized storage systems represents a forward-looking approach that positions judicial institutions to effectively address the challenges of digital crime and maintain credibility in an era of rapid technological change.

2.8 Framework Contributions

This work's key contributions are twofold. First, it utilizes cryptographic hashing to make any manipulation of digital evidence immediately detectable, ensuring authenticity. The implementation of robust cryptographic mechanisms throughout the evidence lifecycle provides mathematical certainty regarding evidence integrity that exceeds the capabilities of traditional verification methods. By computing and recording cryptographic hashes at the point of evidence collection and validating these hashes at every subsequent stage of evidence handling, the system creates multiple layers of verification that collectively ensure that evidence presented in court is authentic and unaltered (Bharati, 2025).

The cryptographic approach adopted in the proposed framework goes beyond simple hash verification. It incorporates advanced techniques such as digital signatures, merkle tree structures, and zero-knowledge proofs to provide comprehensive security while maintaining efficiency and privacy. Digital signatures ensure that evidence records are not only tamper-proof but also attributable to specific individuals or systems, creating clear accountability for evidence handling actions (Rana et al., 2023). The use of merkle trees allows for efficient verification of large evidence

collections without requiring access to all evidence files, improving both performance and privacy (Loffi et al., 2025).

Second, it leverages blockchain's transparency to strengthen the entire legal process, reducing the risks of centralized storage and promoting a more just judicial system. The transparency provided by blockchain technology serves multiple critical functions in the context of evidence management. It enables all authorized stakeholders—including investigators, prosecutors, defense attorneys, judges, and forensic experts—to independently verify the integrity and chain of custody of evidence without relying on trust in any single authority or institution (Chukwuani & Ikemefuna, 2025).

This transparency does not compromise the confidentiality of sensitive evidence or investigative information. The proposed framework implements role-based access controls and privacy-preserving mechanisms that ensure only authorized parties can access specific pieces of evidence or evidence details, while still maintaining a transparent audit trail of all access and handling events (Li et al., 2019). This balance between transparency and confidentiality is essential for maintaining both the security of ongoing investigations and the fairness of legal proceedings.

The reduction of centralization risks is achieved through the distributed architecture of blockchain networks, where evidence records are replicated across multiple independent nodes. This distribution ensures that evidence cannot be lost, destroyed, or manipulated through compromise of a single system or institution (Dhulavvagol et al., 2024). Even in scenarios where multiple nodes are compromised, the consensus mechanisms of blockchain networks ensure that malicious modifications will be detected and rejected by the honest nodes in the network.

The promotion of a more just judicial system is the ultimate goal and most significant contribution of the proposed framework. By providing technological guarantees of evidence integrity, transparent audit trails, and decentralized verification mechanisms, the system addresses fundamental vulnerabilities in traditional evidence management that have contributed to wrongful convictions and miscarriages of justice. The enhanced reliability and credibility of evidence handling procedures enabled by blockchain technology can strengthen public confidence in judicial institutions and support the fair and effective administration of justice (Abdullah et al., 2025).

Table 1 Comparative Analysis

Feature	Systems											
	1	2	3	4	5	6	7	8	9	10	11	12
Blockchain Type	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart Contracts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPFS Integration	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗	✓
Chain of Custody (CoC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Immutability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Access Control/RBAC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encryption	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hash-based Verification	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Timestamp/Audit Trail	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Decentralization	✓	✗	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓
Scalability Solutions	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓

ZKP Generation	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Real-time Monitoring	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Multimedia Support	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 2. Comparative Analysis

Feature	**System**											
	13	14	15	16	17	18	19	20	21	22	23	24
Blockchain Type	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart Contracts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPFS Integration	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓
Chain of Custody (CoC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Immutability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Access Control/RBAC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encryption	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✓	✓
Hash-based Verification	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Timestamp/Audit Trail	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Decentralization	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓
Scalability Solutions	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓
ZKP Generation	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Real-time Monitoring	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Multimedia Support	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓

Table 3. Comparative Analysis

Feature	Systems	
	25	26
Blockchain Type	✓	✓
Smart Contracts	✓	✓
IPFS Integration	✗	✗
Chain of Custody (CoC)	✓	✓
Immutability	✓	✓
Access Control/RBAC	✓	✓
Encryption	✓	✓
Hash-based Verification	✓	✓
Timestamp/Audit Trail	✓	✓
Decentralization	✓	✓
Scalability Solutions	✗	✗
ZKP Generation	✗	✗
Real-time Monitoring	✗	✗
Multimedia Support	✓	✗

Table 4. System Studies

System	Title	Authors	Year
1	Smart Contracts for Managing the Chain-of-Custody of Digital Evidence: A Practical Case of Study	Santamaría, P., Tobarra, L., Pastor-Vargas, R., Robles-Gómez, A.	2023
2	Forensic Evidence System Using Blockchain	Gawade, S., Lokare, P., Kshirsagar, V., Jadhav, L.B.	2024
3	LogStamping: A Blockchain-Based Log Auditing Approach for Large-Scale Systems	Islam, M.S., Rahman, M.S.	2025

4	Blockchain Driven Evidence Management System	Rahath, T., Manaswini, V., Manisha, S., Pavani, N.	2025
5	Internet-of-Forensic (IoF): A Blockchain Based Digital Forensics Framework for IoT Applications	Kumar, G., Saha, R., Lal, C., Conti, M.	2021
6	B-DEC: Digital Evidence Cabinet Based on Blockchain for Evidence Management	Yunianto, E., Prayudi, Y., Sugiantoro, B.	2020
7	Evidence Management System Using Blockchain	Rajlaskhmi, K., Gaikwad, S., Ponde, A., Bhogade, V., Chavan, V.	2025
8	Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain	Rana, S.K., Rana, A.K., Rana, S.K., Sharma, V., Lilhore, U.K., Khalaf, O.I., Galletta, A.	2023
9	Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution	Ratul, M.H.A., Mollajafari, S., Wynn, M.G.	2024
10	Forensic Evidence Security System Using Blockchain Technology	Akinseye, O.C., Oguntimilehin, A., Bello, O.A.	2023
11	Two-Level Blockchain System for Digital Crime Evidence Management	Kim, D., Ihm, S.-Y., Son, Y.	2021
12	Chain of Custody and Evidence Integrity Verification Using Blockchain Technology	Miller, A., Singh, A.	2024
13	Preserving Integrity of Forensic Evidence using Blockchain Technology	Steffi, D.S., Ramu, S., Harish, G., Saranraj, R., Gughan, S.	2024
14	Digital Evidence Security System Design Using Blockchain Technology	Sunardi, Kusuma, R.S.	2023
15	SHARD-FEMF: Adaptive Forensic Evidence Management Framework using Blockchain Sharding and IPFS	Dhulavvagol, P., Totad, S., Anagal, A.	2024

16	Preventing Spoliation of Evidence with Blockchain: A Perspective from South Asia	Shahaab, A., Hewage, C., Khan, I.	2021
17	Tamperproof IoT with Blockchain	Yu, G., Liu, R.P., Zhang, J.A., Guo, Y.J.	2022
18	Secure Cross-Chain Provenance for Digital Forensics Collaboration	Akbarfam, A.J., Dorai, G., Maleki, H.	2024
19	Block-Chain Based Document Verification System Using IPFS	Kumar, K.R., Supraja, H., Deekshitha, M., Sireesha, B., Sadiya, S.	2025
20	Blockchain-Based Chain-of-Custody Models for Tamper-Proof Evidence Preservation in Digital Forensics Investigations	Chukwuani, E.N., Ikemefuna, C.D.	2025
21	Blockchain Based Evidence Management System	Kumar, V.S., Udayasree, N., Savitha, G., Sravani, M.	2024
22	ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability	Akbarfam, A.J., Heidaripour, M., Maleki, H., Dorai, G., Agrawal, G.	2023
23	Blockchain in the Security and Integrity of Legal Evidence: A Futuristic Proposal for Nigeria	Enokie, B.K.	2025
24	An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody under ISO 27037	Lavín, I., Llanos, D.R.	2025
25	CustodyBlock: A Distributed Chain of Custody Evidence Framework	Alruwaili, F.F.	2021
26	Accountability of Things: Large-Scale Tamper-Evident Logging for Smart Devices	Koisser, D., Sadeghi, A.-R.	2023

Analysis of Systems from Tables 1–4

The comparative analysis across Tables 1–4 reveals the current state of blockchain-based digital evidence management systems, examining 26 different implementations across various technological features and capabilities.

Universal Features Across All Systems (1–26)

- Blockchain technology: All systems utilize blockchain as their core infrastructure
- Smart contracts: Universal implementation for automated evidence management processes
- Chain of custody (CoC): Complete coverage ensuring legal compliance and traceability
- Immutability: All systems provide tamper-proof evidence storage capabilities
- Hash-based verification: Cryptographic integrity verification implemented across all systems
- Timestamp/audit trail: Comprehensive logging and tracking mechanisms in all implementations

Significant Technological Gaps Identified

Access control and security:

- Access control/RBAC: Implemented in all 26 systems
- Encryption: Present in 22 out of 26 systems (85%), with gaps in systems 16, 17, 21, and 22

Advanced features with limited adoption:

- IPFS integration: Only 9 systems (35%) implement decentralized storage (systems 3, 4, 7, 8, 12, 15, 19, 23, and 24)
- Decentralization: 18 systems (69%) achieve true decentralization, while 8 systems remain centralized
- Scalability solutions: Only 6 systems (23%) address blockchain scalability challenges

Critical innovation gaps:

- ZKP generation: Only 1 system (4%) implements zero-knowledge proofs (system 1)
- Real-time monitoring: Only 1 system (4%) provides continuous tamper detection (system 3)
- Multimedia support: 25 systems (96%) support multimedia evidence, with only system 26 lacking this feature

System Development Strategy

Based on this comprehensive analysis, we will develop a system that integrates all the essential features identified across these 26 systems while addressing their critical limitations. Our proposed system will incorporate:

- Universal core features: Blockchain infrastructure, smart contracts, chain of custody, immutability, hash-based verification, and audit trails

- Advanced security: Complete access control, encryption, and decentralization
- Scalability solutions: Addressing the performance limitations found in 77% of existing systems
- Comprehensive storage: IPFS integration for efficient multimedia evidence management
- Privacy-preserving verification: ZKP generation for confidential evidence authentication
- Proactive security: Real-time monitoring for immediate tamper detection
- Complete multimedia support: Full capability for images, videos, documents, and audio evidence

Innovation Statement

The analysis reveals that while individual systems excel in specific areas, none achieve comprehensive integration of advanced features. However, no existing study integrates real-time monitoring, automated ZKP generation, IPFS decentralized storage, the Polygon blockchain, and support for multimedia evidence into a single framework. This represents a significant research gap where existing solutions address isolated aspects of evidence management but fail to provide a holistic approach that combines privacy-preserving verification, continuous security monitoring, scalable decentralized storage, and comprehensive multimedia support within a unified architecture.

Our proposed “Real-Time ZKP-Verified Multimedia Evidence Protection System with Automated Tamper Detection on an IPFS-Polygon Architecture” will be the first to bridge this gap, delivering a

complete solution that surpasses the limitations identified in the current landscape of digital evidence management systems.

2.9 Concept of the Study

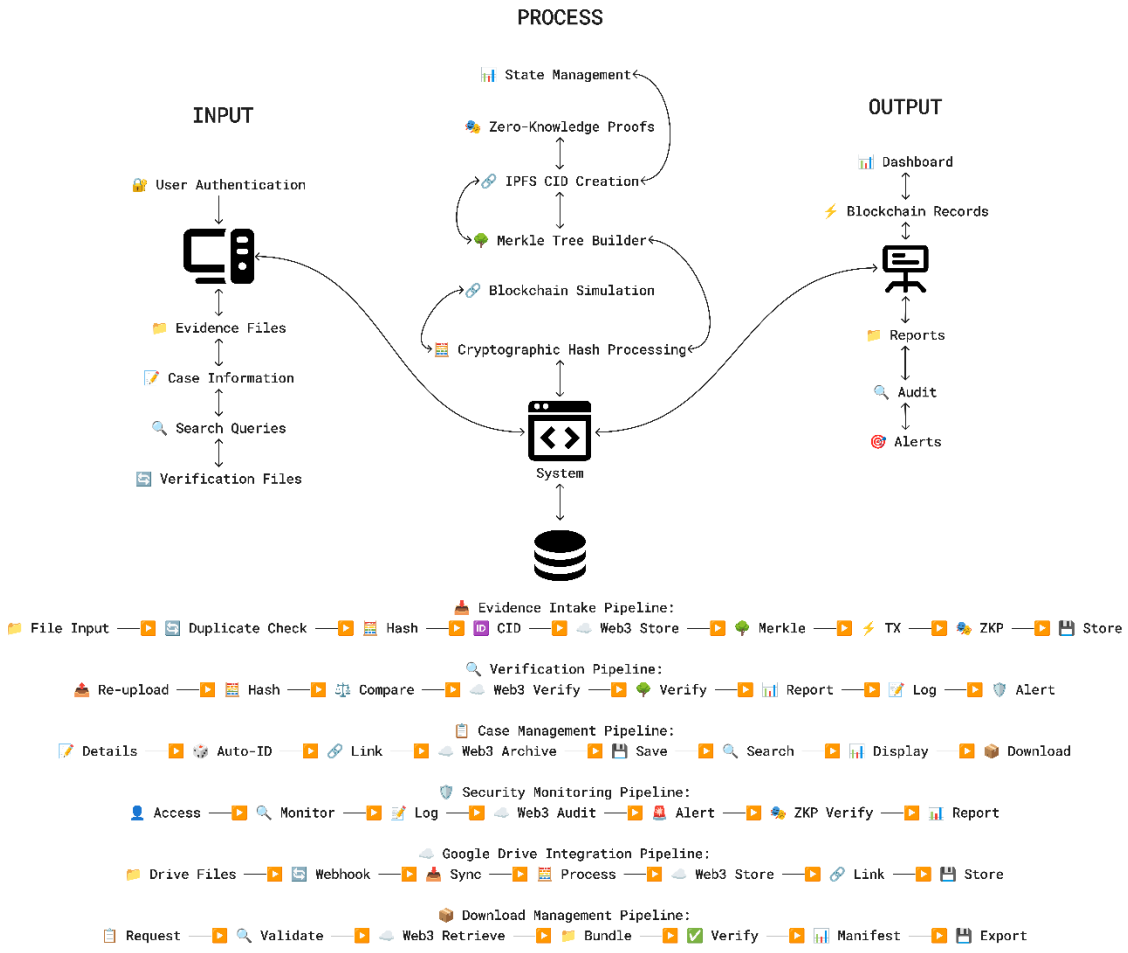

Figure 1. Conceptual Framework Diagram

Figure 2.9-1 presents the comprehensive conceptual framework of the proposed blockchain-based digital evidence management system, illustrating the systematic transformation of raw digital artifacts into legally admissible, tamper-proof evidence through an integrated Input-Process-Output (IPO) model with both automated and manual tamper detection capabilities, enhanced security monitoring, enterprise-grade download management, and comprehensive cloud integration.

Input Components

The input layer encompasses six critical categories of system inputs that initiate the evidence lifecycle:

1. **Digital Evidence Files** – Includes multimedia content such as images, videos, documents, and audio recordings collected from various forensic sources and Google Drive synchronization.

2. **User Authentication** – Encompasses comprehensive access control including login credentials, protected route verification, password reset functionality, admission portal access, and multi-tier session management for investigators, forensic analysts, legal practitioners, and judicial personnel.

3. **Case Information** – Consists of metadata including case identifiers, investigative context, collection timestamps, jurisdictional parameters, and case-level download management configurations.

4. **Search Queries and Verification Files** – Enable evidence retrieval, integrity validation, manual tamper verification through file re-upload functionality, and advanced duplicate detection throughout the legal process.

5. **Google Drive Files** – Facilitates cloud storage integration through webhook-based synchronization, enabling seamless evidence collection from distributed storage sources with real-time monitoring capabilities.

6. **Sensitive Access Requests** – Manages high-security evidence access with zero-knowledge proof verification, real-time monitoring, and automated alert generation for sensitive information handling.

Process Architecture

The central processing layer operationalizes a sophisticated six-stage workflow that ensures cryptographic security, legal compliance, and comprehensive tamper detection. State management coordinates system operations across distributed nodes while continuously monitoring evidence integrity. Zero-Knowledge Proof (ZKP) generation enables privacy-preserving verification that allows authorized parties to confirm evidence authenticity without exposing sensitive content details. IPFS Content Identifier (CID) creation transforms evidence files into content-addressed objects stored on the InterPlanetary File System, ensuring decentralized and tamper-resistant storage. Web3.Storage integration provides enterprise-grade decentralized storage with content verification and retrieval capabilities across all processing stages. Merkle Tree construction organizes evidence hashes into hierarchical verification structures, enabling efficient batch integrity validation. Blockchain simulation and recording anchor evidence metadata and cryptographic fingerprints to the Polygon blockchain

through smart contracts, creating immutable audit trails. Advanced duplicate detection automatically identifies and resolves duplicate files with user-controlled resolution workflows. Cryptographic hash processing generates SHA-256 fingerprints that serve as unique digital signatures for each piece of evidence, enabling both automatic real-time tamper detection (which continuously compares current file hashes against blockchain-stored originals) and manual verification capabilities (which allow authorized users to re-upload suspected files for immediate integrity comparison and tamper assessment).

Output Deliverables

The output layer produces legally actionable artifacts that satisfy judicial requirements and enterprise security standards. These include the enhanced dashboard interface, which provides real-time system status, evidence management capabilities, tamper detection alerts, and comprehensive duplicate management; blockchain records, which contain permanent distributed ledger entries establishing provenance and chain of custody; enterprise download management, featuring bulk export capabilities with professional folder structures, verification manifests, and comprehensive audit trails; security monitoring reports documenting real-time access monitoring, sensitive information alerts, and zero-knowledge proof verification outcomes; comprehensive reports documenting evidence integrity, access history, tamper detection results, and verification outcomes in court-admissible format; advanced audit trails maintaining chronological records of all evidence interactions, automated integrity checks, manual verification attempts, download activities, and security events with cryptographic timestamps; Google Drive integration status providing cloud synchronization reports, webhook activity logs, and distributed storage verification; and security

alerts providing immediate notification of any tampering attempts, integrity violations, sensitive access events, or suspicious activities detected through both automated monitoring and manual verification processes.

Integrated Pipeline Operations

The framework demonstrates six specialized processing pipelines enhanced with comprehensive tamper detection and security mechanisms:

- **Evidence Intake Pipeline** (File Input → Duplicate Check → Hash → CID → Web3 Store → Merkle → Transaction → ZKP → Store) ensures secure evidence ingestion with baseline integrity establishment and duplicate resolution.
- **Verification Pipeline** (Re-upload → Hash → Compare → Web3 Verify → Merkle Verify → Report → Log → Alert) enables both continuous automated integrity monitoring and on-demand manual verification through file re-upload and hash comparison.
- **Case Management Pipeline** (Details → Auto-ID → Link → Web3 Archive → Save → Search → Display → Download) facilitates comprehensive case administration with integrated tamper detection reporting and enterprise download capabilities.
- **Security Monitoring Pipeline** (Access → Monitor → Log → Web3 Audit → Alert → ZKP Verify → Report) provides real-time sensitive information access monitoring with automated security alerts and comprehensive audit trails.
- **Google Drive Integration Pipeline** (Drive Files → Webhook → Sync → Process → Web3 Store → Link → Store) enables seamless cloud storage synchronization with distributed verification and monitoring capabilities.

• **Download Management Pipeline** (Request → Validate → Web3 Retrieve → Bundle → Verify → Manifest → Export) provides enterprise-grade bulk download capabilities with comprehensive verification and professional audit trail generation.

Enhanced System Interface

The system provides seven comprehensive interface pages designed for different stakeholder needs:

- **Dashboard Page** – Enhanced upload zone with duplicate detection, comprehensive batch display with Web3.Storage status, advanced verification panel with real-time monitoring, detailed statistics summary with security metrics, and integrated Google Drive synchronization status.

- **Polygon Transparency Page** – Blockchain transaction explorer with Web3.Storage integration, comprehensive event feed with security monitoring, advanced filter tools with access controls, detailed audit trail with download tracking, and real-time cloud synchronization monitoring.

- **Cases Page –** Advanced case search with duplicate filtering, comprehensive case list with download capabilities, enhanced metadata view with security classifications, dynamic status badges with verification states, and integrated export tools with audit trails.

- **Download Management Page** – Enterprise bulk download capabilities with folder structure customization, comprehensive audit trail generation with verification manifests,

professional naming conventions with case-based organization, integrity verification with Web3.Storage validation, and progress tracking with security monitoring.

- **Sensitive Access Monitor Page** – Real-time security monitoring with automated threat detection, comprehensive alert system with zero-knowledge proof verification, detailed access logging with behavioral analysis, security report generation with compliance documentation, and sensitive information protection with privacy-preserving verification.

- **Authentication Pages** – Secure login portal with multi-factor authentication, comprehensive password reset functionality with security verification, admission landing page with role-based access control, protected route management with session monitoring, and comprehensive user session management with security tracking.

- **Google Drive Integration Page** – Real-time cloud storage monitoring with webhook management, comprehensive synchronization status with conflict resolution, distributed file verification with integrity checking, webhook activity logging with security monitoring, and cloud-to-evidence pipeline management with audit capabilities.

This integrated architecture addresses the critical vulnerabilities of traditional centralized evidence management systems by eliminating single points of failure, ensuring cryptographic immutability, maintaining transparent auditability, providing automated real-time tamper detection, enabling manual verification through file re-upload, delivering privacy-preserving verification capabilities, implementing enterprise-grade download management with comprehensive audit trails, providing real-time security monitoring with automated threat detection, and enabling seamless cloud

integration with distributed verification—all essential for modern digital forensics and judicial proceedings.

2.10 Definition of Terms

Blockchain In this system, blockchain specifically utilizing the Polygon network serves as the immutable ledger where evidence metadata, cryptographic hashes, and chain-of-custody records are permanently stored. When evidence is uploaded, its hash and case details are recorded on the blockchain via smart contracts, creating a tamper-proof audit trail that can be independently verified by all stakeholders in legal proceedings.

Chain of Custody Maintained through automated blockchain logging that records every evidence interaction with timestamps, user identities, and action types. The system captures the complete lifecycle from initial upload through verification attempts, creating a chronological record that satisfies legal requirements for evidence admissibility without relying on manual documentation.

Cryptographic Hashing Applied to each piece of digital evidence using SHA-256 algorithms to generate unique fingerprints. These hashes are stored on the blockchain and serve as the foundation for all integrity verification processes throughout the evidence lifecycle.

Digital Evidence Any multimedia file including images, videos, documents, and audio processed by the system. Upon upload, each piece of evidence receives cryptographic hashing, IPFS content addressing, Merkle tree inclusion, blockchain anchoring, and ZKP verification capabilities, transforming raw files into forensically-sound digital evidence.

Immutability Achieved through blockchain's cryptographic linking and consensus mechanisms, ensuring that once evidence hashes and metadata are recorded, they cannot be altered without detection. This creates permanent records that provide legal certainty about evidence authenticity and handling history.

Tamper-Evident Implemented through real-time hash verification that immediately detects file modifications. The system displays verification status and logs all integrity checks to the blockchain transparency ledger.

Centralized System The architecture this system is designed to replace. Unlike traditional centralized evidence storage that creates single points of failure and trust dependencies, this system distributes evidence verification across blockchain nodes and uses IPFS for decentralized storage, eliminating institutional vulnerabilities.

IPFS (InterPlanetary File System) The decentralized storage network used to store actual evidence files off-chain while maintaining content-addressed references on the blockchain. Each file receives a unique content identifier based on its hash, ensuring files cannot be altered without changing their address and enabling distributed storage.

Zero-Knowledge Proofs (ZKPs) Cryptographic protocols that allow the system to verify evidence authenticity without revealing sensitive details about the evidence content. ZKPs enable authorized parties to confirm evidence integrity while maintaining confidentiality of ongoing investigations and protecting sensitive information.

Merkle Trees Hierarchical data structures that organize evidence hashes in a tree format, allowing efficient verification of multiple pieces of evidence through a single root hash. The system uses Merkle trees to batch evidence verification, enabling quick integrity checks of entire evidence collections without requiring individual verification of each file.

Smart Contracts Automated blockchain programs that execute evidence management rules and access controls without human intervention. Smart contracts handle evidence registration, permission verification, timestamp recording, and tamper detection, ensuring consistent application of forensic protocols and eliminating human error in evidence handling procedures.