The 8th Open Society Conference (OSC) 2026
Faculty of Law, Social and Political Science
Universitas Terbuka
DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

The Convergence of Quantum Computing and Criminal Evidence Law: Rethinking the Admissibility of Electronic Evidence in the Digital Era

Abdurrahman[1], Qorina Khoirunisa[2]
[1] Faculty of Law, Universitas Sriwijaya, Palembang, Indonesia
[2] Faculty of Sharia and Law, Universitas Islam Negeri (UIN) Raden Fatah, Palembang, Indonesia
e-mail: abdurrahman@fh.unsri.ac.id

Abstract

The advancement of emerging digital technologies has created new challenges for existing legal frameworks, particularly concerning electronic evidence, which has been recognised as a valid form of evidence under criminal procedural law. The management of electronic evidence faces several challenges, including the vulnerability and volatility of digital data, encrypted technologies, and cross-border jurisdictional complexities. The emergence of quantum computing is expected to significantly transform digital security systems. Its ability to break current cryptographic algorithms may jeopardize the authenticity, integrity, and confidentiality of electronic evidence, while simultaneously providing opportunities for law enforcement through enhanced decryption and digital forensic capabilities. These developments raise concerns regarding the preparedness of criminal procedural law in responding to technological advancement. This study examines the implications of quantum computing for electronic evidence admissibility, evaluates the existing legal framework, and proposes directions for criminal procedural law reform. Using a doctrinal legal research method with statutory, conceptual, and comparative approaches, this study finds that quantum computing does not currently affect the legal admissibility of electronic evidence but may compromise the reliability of mechanisms ensuring authenticity, integrity, and non-repudiation. Therefore, legal reform should focus on strengthening electronic evidence regulation, establishing authentication and integrity standards, harmonising relevant regulations, and implementing post-quantum cryptographic standards.

Keywords: *Electronic Evidence, Quantum Computing, Criminal Procedure, Evidence Law*

INTRODUCTION

The Within criminal procedural law, electronic evidence has long been recognized as a legally admissible form of evidence. This recognition has been reinforced by the development of legal frameworks across various jurisdictions. An increasing number of countries have accepted and incorporated electronic data, including emails, online chat records, and digital transaction records, into the evidentiary framework applicable to criminal proceedings [1]. This paradigm shift is not merely an administrative response to technological developments. Rather, it reflects a broader legal recognition that digital traces may contain information of evidentiary significance comparable to that of conventional forms of evidence in establishing the occurrence of a criminal offense. As

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

social and commercial interactions increasingly move into the digital environment, the law of evidence is likewise required to adapt so that it remains capable of capturing new forms of interaction and legally relevant conduct emerging within that environment.

The handling of electronic evidence, however, is accompanied by a range of challenges. Electronic or digital data are inherently vulnerable to alteration, deletion, or loss of accessibility within a relatively short period of time. If such data are not secured promptly, their evidentiary value may be compromised and the investigative process may be adversely affected. Digital data should therefore be secured from the earliest stage of an investigation [2]. This vulnerability requires investigators to act rapidly and to adopt procedures that differ in important respects from those applicable to conventional physical evidence. Even a short delay may result in the loss of digital traces that could prove critical to the reconstruction and disclosure of a criminal offense. The challenges do not end with the inherently volatile nature of digital data. The use of encryption technologies may also complicate investigators ability to access and examine relevant data or evidence. Although encryption is essential for protecting data, information, and evidence from unauthorized access, it may simultaneously create barriers to the acquisition of evidence relevant to the investigation and prosecution of criminal offenses.

The examination of digital evidence involves more than merely locating, acquiring, and collecting data. It also requires assurance that the data have been obtained through appropriate procedures, have remained unaltered throughout the examination process, and can be traced back to their origin and the processes through which they were handled. The examination of digital evidence therefore requires an appropriate strategy from the outset. Decisions made and actions taken at the initial stage of an investigation may determine what data can subsequently be examined and relied upon as evidence in criminal proceedings [3]. The investigation of digital data does not always proceed without difficulty. At every stage, errors may occur that affect the accuracy and reliability of forensic findings [4]. Limitations relating to technology, procedural safeguards, and the competence of forensic examiners may influence how digital traces are interpreted and subsequently transformed into information capable of acquiring evidentiary value [2].

The successful acquisition of digital evidence does not, in itself, establish that such evidence can immediately be regarded as reliable. The process must be properly examined and documented so that every step taken can subsequently be reconstructed and subjected to accountability [5]. The central challenge in handling electronic evidence therefore extends beyond the mere acquisition of data. It concerns the preservation of its integrity, the traceability of every process to which it has been subjected, and the assurance that the resulting information can genuinely be relied upon to support the proof of a criminal offense.

The emergence of quantum computing introduces a new dimension to the security challenges confronting the digital environment. Unlike conventional computers, quantum computers process information based on principles derived from quantum mechanics,

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

including superposition and quantum entanglement. This difference has significant implications for the public-key cryptographic systems that are widely used today to encrypt data, facilitate secure key exchange, and authenticate the identities of users. Through Shor's algorithm, sufficiently powerful quantum computers may solve integer factorization and related mathematical problems far more efficiently than conventional computers. These computational problems, however, constitute fundamental security assumptions underlying cryptographic systems such as RSA, Diffie–Hellman, and elliptic-curve cryptography (ECC) [6].

The threat posed by quantum computing becomes more significant because modern cryptography is embedded in numerous components of the digital environment. Cryptographic mechanisms protect the confidentiality of data, secure user identities, and prevent unauthorized modification of information. Telecommunications networks and internet-connected devices likewise rely on cryptography to protect information against interception and unauthorized access [7]. If the cryptographic algorithms currently in use become insufficiently secure against quantum attacks, the consequences would extend beyond the mere exposure of protected data. The mechanisms used to authenticate users and establish the authenticity and integrity of information could also be compromised. Yet replacing legacy cryptographic systems with quantum-resistant alternatives is far from straightforward. Digital systems consist of interconnected components, including hardware, software, infrastructure, and communication protocols [8].

Discussions regarding quantum computing and digital evidence have largely proceeded along separate tracks. Legal studies typically focus on intellectual property, data protection, and regulatory readiness, while the implications for the law of evidence remain underexplored [9]. Research in digital forensics has begun to question the admissibility of quantum-secured evidence in court, yet most studies approach the issue from a technological perspective—such as quantum digital signatures and quantum key distribution—rather than from the standpoint of criminal procedural law [10]. A similar trend is observed in research on the chain of custody; while studies propose the use of blockchain and self-sovereign identity, there is limited discussion regarding post-quantum cryptography or the legal consequences should the technology originally used to secure the evidence become compromised [11] ,[12] Legal research on digital evidence has addressed the lack of uniform regulations for evidence management but has not specifically examined shifts in cryptographic security after the evidence has been deemed admissible [13]. This raises a critical issue: evidence is often presumed to meet legal requirements and remain trustworthy from the moment of acquisition, as if that status were immutable. In reality, the technologies safeguarding evidence evolve and may eventually become vulnerable. The relationship between such technological changes and the continued trustworthiness of admitted electronic evidence remains under-researched, particularly within the context of Indonesian criminal procedural law [14]. Few studies have addressed whether admitted electronic evidence retains its trustworthiness when the

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

cryptographic systems protecting it become vulnerable over time—an issue that warrants further examination from the perspective of Indonesian criminal procedural law. Accordingly, this study examines whether admitted electronic evidence remains trustworthy when the cryptographic systems protecting it later become vulnerable, with particular attention to Indonesian criminal procedural law.

The intersection between electronic evidence and quantum computing raises a fundamental question: whether electronic evidence can continue to be regarded as trustworthy when the technological foundations supporting its reliability are themselves transformed. Digital evidence has traditionally been considered reliable because various technological mechanisms operate to establish that data are accurate, authentic, unaltered, and traceable throughout the examination process [15]. This dependence on digital security mechanisms becomes increasingly apparent when cryptographic systems are confronted with the capabilities of quantum computing, particularly in the context of public-key cryptography [16]. The issue is therefore not limited to whether data can still be accessed. More fundamentally, it concerns whether technological developments may undermine the authenticity, integrity, and reliability of electronic evidence [5]. Changes in technological capabilities also challenge criminal procedural law to ensure that the legal validity and evidentiary status of electronic evidence remain adequately protected [17]. This issue is particularly significant because quantum forensics remains at an early stage of development. The central question is whether existing concepts of evidentiary validity and reliability remain adequate when the cryptographic foundations upon which those concepts implicitly depend undergo fundamental technological change. Against this background, this study examines the implications of quantum computing for the validity and evidentiary use of electronic evidence, analyses the extent to which the existing legal framework is capable of anticipating these technological developments, and proposes directions for reforming criminal procedural law to respond more effectively to the convergence of quantum computing and electronic evidence.

METHOD

The study makes use of doctrinal legal research, with an emphasis on the Indonesian laws that deal with electronic evidence. The key legal documents looked at include Law No. 1 of 2024, which amends the Electronic Information and Transactions Law (ITE Law), Law No. 20 of 2025 on the Criminal Procedure Code (KUHAP), Government Regulation No. 71 of 2019 concerning the administration of electronic systems and transactions, and Law No. 27 of 2022 on Personal Data Protection, to the extent that these laws address electronic information security and digital data. The study also takes into account the provisions relating to electronic signatures, electronic system security, digital forensics, and the acquisition, preservation, examination, and presentation of electronic evidence. These regulations are studied together with academic literature, technical standards, and publications from institutions in order to examine how the legal requirements interact with the technologies employed to ensure the authenticity and

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

integrity of electronic evidence.

The analysis utilizes statutory, conceptual, and comparative approaches. Relevant legal provisions are evaluated through the frameworks of admissibility, authenticity, integrity, reliability, non-repudiation, and chain of custody, and are compared with legal developments in the United States and the European Union. The comparative analysis emphasizes requirements for electronic evidence, safeguards for authentication and integrity, forensic standards, cryptographic security, and preparedness for post-quantum cryptography. Legal materials are reviewed for the period 2017-2025 and selected based on relevance and legal authority. This analysis assesses whether Indonesia's current regulatory framework offers adequate legal support for the long-term verification and protection of electronic evidence in the context of advancing quantum computing.

RESULTS AND DISCUSSION

Implications of Quantum Computing for the Validity and Proof of Electronic Evidence

The admissibility of electronic evidence in Indonesian criminal proceedings must be assessed against the evidentiary provisions currently applicable under Indonesian law. Law No. 1 of 2024, which amended the Electronic Information and Transactions Law, expressly maintains the recognition of electronic information and electronic documents as admissible evidence subject to the statutory requirements. This recognition is further reinforced by Law No. 20 of 2025 on the Criminal Procedure Code (KUHAP). Article 235(1)(f) expressly includes electronic evidence within the recognized forms of evidence, while Article 242 extends the evidentiary framework to electronic information, electronic documents, and electronic systems related to criminal offenses.

Electronic evidence has therefore moved beyond its earlier position as a technological extension or derivative of conventional physical evidence and has acquired an independent statutory foundation.

Before the enactment of Law No. 1 of 2024 and Law No. 20 of 2025 on the Criminal Procedure Code (KUHAP), electronic evidence was recognized primarily through sector-specific legislation. This included Article 26A of Law No. 20 of 2001, which amended Law No. 31 of 1999 on the Eradication of Corruption. The recognition of electronic evidence was further reinforced by Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016. In practice, however, courts under the former KUHAP frequently treated electronic evidence as falling within the categories of documentary evidence or circumstantial evidence under Article 188 of Law No. 8 of 1981 on the Criminal Procedure Code [18]. Since the former KUHAP did not establish formal standards for electronic evidence, its legal validity and evidentiary weight largely depended on judicial assessment and digital forensic examination at trial. With the enactment of Law No. 20 of 2025, the evidentiary framework has been broadened to expressly recognize electronic evidence under Article 235(1)(f)

Its legal recognition, however, does not dispense with the requirement that its

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

authenticity and manner of acquisition be established. The court retains the authority to evaluate these matters. From the perspective of digital forensics, the assessment of electronic evidence principally concerns authenticity, integrity, and reliability [19]. Government Regulation No. 71 of 2019 likewise requires electronic systems to be operated in a secure and reliable manner. The legal framework consequently establishes the conditions governing the admissibility of evidence, while technological mechanisms provide the means by which the authenticity and integrity of such evidence may be demonstrated.

The evidentiary status of electronic data therefore depends upon an interaction between legal norms and technological safeguards. Electronic evidence must be supported by mechanisms capable of demonstrating that the data are genuine, have not been altered, and can be attributed to the relevant person or system. Digital signature schemes such as RSA and ECDSA have traditionally derived their security from mathematical problems that are computationally difficult for conventional computers to solve within a feasible period. The development of sufficiently powerful quantum computers, however, may undermine this security assumption. Shor's algorithm provides a theoretical basis for solving mathematical problems underlying public-key cryptographic schemes and potentially recovering private keys previously regarded as secure [20]. The compromise of a private key could enable the creation of fraudulent digital signatures that nevertheless appear cryptographically valid [21]. Such a development would directly affect the evidentiary function of digital signatures.

Integrity presents a related but distinct problem. Cryptographic hash functions are commonly employed to demonstrate that digital data have remained unchanged. Grover's algorithm poses a comparatively less severe threat to hash-based cryptography than Shor's algorithm poses to public-key cryptography, and the security of hash functions may be strengthened through appropriate increases in security parameters [22]. Nevertheless, a successful compromise of hash-based integrity mechanisms would create difficulties in establishing whether the digital evidence presented before a court is identical to the evidence originally acquired or seized. The issue is therefore not merely whether data remain accessible but whether their evidentiary identity can still be established with sufficient certainty.

A similar concern arises in relation to non-repudiation, understood as the capacity of a digital signature mechanism to associate an electronic act with the holder of the relevant private key. Once a private key has been compromised through a quantum attack, a mathematically valid signature may no longer provide conclusive assurance regarding the identity of the person who actually generated it [23]. The evidentiary relationship between the digital act, the cryptographic credential, and its purported author may consequently become subject to challenge. Quantum computing thus has implications not merely for information security but also for the attributional function upon which the evidentiary significance of digital signatures partly depends.

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

For this reason, the legal assessment of electronic evidence must distinguish between legal admissibility and technical reliability. Compliance with statutory requirements may establish that evidence is legally admissible, but such compliance does not necessarily determine the evidentiary weight that should be attributed to it. Authenticity and integrity provide important indicators that the evidence is genuine and has remained unchanged, whereas reliability concerns the processes through which the evidence was acquired, preserved, examined, and attributed to its source [19]. Digital forensic practice further requires adequate documentation of examination procedures because deficiencies in documentation may undermine confidence in the evidentiary quality of the resulting findings [24]. The inability to validate the methods and forensic tools used may produce similar concerns. These developments explain the increasing importance of post-quantum cryptography in addressing the vulnerability of existing cryptographic infrastructures.[25]. The court must ultimately determine not only whether evidence satisfies the requirements for admission but also whether the evidence possesses sufficient reliability and probative value to support the establishment of a relevant fact [26].

As demonstrated, quantum computing should not be regarded exclusively as a threat to electronic evidence. Its computational capabilities may also create new investigative opportunities by enabling access to data previously protected by encryption. In principle, sufficiently advanced quantum computing could assist investigators in recovering or analyzing information that would be computationally impracticable to access using conventional systems. Such information may generate investigative leads or reveal evidence that was previously inaccessible. Nevertheless, the successful recovery of encrypted data does not, by itself, confer evidentiary admissibility upon the resulting information. The investigator must still demonstrate that the evidence was obtained lawfully, preserved appropriately, documented adequately, and examined in accordance with applicable procedural requirements. Quantum computing therefore presents a dual evidentiary implication: it may undermine the cryptographic foundations protecting electronic evidence while simultaneously enhancing investigative access to previously concealed information. The deployment of such capabilities must remain bounded by lawful investigative authority and the procedural and evidentiary safeguards governing criminal proceedings.

A. The Readiness of the Existing Criminal Procedural Law Framework

The regulation of electronic evidence in Indonesia extends beyond its recognition as a means of proof to encompass its acquisition, preservation, and use in criminal proceedings. Law No. 20 of 2025 on the Criminal Procedure Code (KUHAP) recognizes electronic evidence subject to requirements concerning authenticity and lawful acquisition. Similarly, Law No. 1 of 2024 recognizes Electronic Information and Electronic Documents as admissible evidence based on the principles of integrity, authenticity, and reliability. These provisions are supplemented by Government

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

Regulation No. 71 of 2019 on the Administration of Electronic Systems and Transactions, Law No. 27 of 2022 on Personal Data Protection, and other regulations governing criminal investigations and the handling of electronic evidence. Thus, Indonesian law has established a legal basis for both the recognition and use of electronic evidence. However, legal recognition does not necessarily provide the technical standards required to ensure that such evidence remains authentic and unaltered.

Technically, the integrity of digital evidence depends on forensic procedures governing its acquisition, preservation, documentation, examination, and chain of custody.[19]. At present, however, no universally applicable standard exists for determining the reliability of forensic methods and technologies in criminal investigations [5]. Standards such as ISO/IEC 27037, 27041, 27042, and 27043 therefore serve as important references for digital evidence examination [27]. Hash values, digital signatures, timestamps, and chain-of-custody records are particularly relevant. Nevertheless, demonstrating a hash value alone is insufficient to establish the integrity of digital evidence. It is also necessary to establish when and how the evidence was preserved and whether subsequent alterations can be identified and traced. The question therefore arises whether Indonesian law sufficiently regulates these technical requirements or whether their implementation remains dependent on institutional practices and the technical competence of law enforcement authorities.

This issue becomes more significant in light of the rapidly changing security landscape of cryptographic technologies. Electronic evidence may need to remain legally and technically reliable for years, even though the cryptographic mechanisms used to authenticate it may subsequently become vulnerable. Indonesian law currently contains no explicit requirement to transition to post-quantum cryptography in response to the threat of quantum computing. Nor does the existing framework expressly require the re-verification of electronic evidence when the algorithms used for its digital signatures or hash values become obsolete or vulnerable. This creates a potential "retroactive verification problem": criminal procedural law does not yet provide a clear mechanism for reassessing the reliability of electronic evidence when the cryptographic standards supporting its authenticity are later compromised. This gap is particularly important because developments in quantum computing may progress more rapidly than the ability of criminal procedural law to update its security requirements.

Comparable challenges can be observed in other jurisdictions. In the United States, for instance, the National Institute of Standards and Technology (NIST) established three post-quantum cryptographic standards in 2024, namely FIPS 203, FIPS 204, and FIPS 205. These standards respond to the prospective vulnerability of conventional cryptographic mechanisms, including those based on RSA and ECDSA. The transition is relevant to electronic evidence because quantum computing may undermine the cryptographic protections used to secure digital signatures, manifests, timestamps, and other components of the chain of custody. Consequently, evidence that appears authentic

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

under existing standards may not remain technically reliable in the face of future cryptographic attacks [28]. The European Union has similarly addressed issues concerning electronic authentication and trust services through its eIDAS framework. However, electronic signatures recognized for legal purposes may still depend on cryptographic algorithms that are theoretically vulnerable to quantum attacks based on Shor's algorithm. This has encouraged legal scholars to reconsider the standards governing the reliability and admissibility of electronic evidence, particularly where evidence is used across multiple jurisdictions [29].

Indonesia therefore possesses a substantial legal foundation for the use of electronic evidence in criminal proceedings, but its regulatory approach remains predominantly reactive. Existing rules respond to technologies already incorporated into law enforcement rather than anticipating technological developments that may undermine the reliability of existing evidentiary safeguards. A more adaptive approach is consequently required. Indonesian criminal procedural law should anticipate the implications of quantum computing and facilitate the transition toward post-quantum cryptography (PQC). The legal framework should also provide mechanisms for updating cryptographic requirements and re-verifying electronic evidence when existing security standards become obsolete. Such an approach would ensure that the evidentiary reliability of electronic records does not depend solely on cryptographic standards that are secure only at the present time.

B. Directions for Criminal Procedural Law Reform: Convergence of Quantum Computing and Criminal Evidence Law

The reform of criminal procedural law should recognize that electronic evidence involves two separate dimensions: legal admissibility and technical reliability. Evidence may be legally admissible where it has been lawfully obtained and submitted in accordance with procedural requirements. Yet legal admissibility alone does not guarantee that the evidence is reliable. Its authenticity and integrity must also be established by demonstrating that it has not been improperly altered or manipulated. Research on quantum computing indicates that the changing security of cryptographic systems requires policymakers to adopt legal standards capable of adapting to technological developments. Criminal procedural law should therefore refrain from treating any particular cryptographic algorithm as a permanent and exclusive standard for the admissibility of electronic evidence. Instead, the law should establish adaptable technical requirements that can evolve alongside changes in technology and security risks. Given the importance of the chain of custody in maintaining the integrity of digital evidence, such requirements should ensure that the authenticity and integrity of evidence remain verifiable and that every stage of its handling can be fully documented and traced.

This perspective shifts the focus of criminal procedural law. The question is no longer limited to whether electronic evidence was legally admissible when it was presented. It must also be asked whether evidence that was once validly admitted remains trustworthy when the technology used to authenticate it has changed or become vulnerable. Two areas

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

of reform therefore warrant particular attention. First, the law should establish a stronger link between the legal admissibility of electronic evidence and its technical reliability. Second, the chain of custody should incorporate cryptographic security as part of the evidentiary trail. These two areas are discussed as follows:

1. **Legal Admissibility and Technical Reliability as Distinct Dimensions of Electronic Evidence**

   The reform of criminal procedural law should commence with a conceptual distinction between two dimensions of electronic evidence that are frequently conflated: legal admissibility and technical reliability. The former concerns the legal conditions under which evidence may be introduced before a court, including lawful acquisition, identifiable provenance, procedural compliance, and the absence of unlawful methods of collection. The latter concerns whether the evidence can reasonably be relied upon as an accurate representation of the underlying data. Although authenticity, integrity, and reliability are closely connected to the evidentiary treatment of electronic information, their existence cannot simply be presumed from formal admissibility. They must be established by reference to the processes, methodologies, and technological systems through which the evidence has been created, acquired, preserved, examined, and maintained.

   This distinction is particularly important because existing legal practice tends to treat procedural validity as if it were sufficient to establish evidentiary trustworthiness. Once electronic evidence has been lawfully obtained and admitted, the legal inquiry may effectively be regarded as concluded. Yet procedural admissibility merely determines whether evidence may enter the judicial process; it does not necessarily establish whether the evidence accurately reflects the underlying facts. An electronic document may have a legitimate source and may have been lawfully obtained while nevertheless being vulnerable to alteration, corruption, or undetected manipulation. The central question must therefore extend beyond whether the evidence is permissible to whether the evidentiary process provides sufficient assurance that the evidence can be trusted.

   The distinction should accordingly be institutionalized within the legal framework by treating legal admissibility and technical reliability as separate but interdependent requirements. Lawful acquisition should preserve the legal status of evidence even where a cryptographic vulnerability is subsequently discovered. Such a vulnerability should instead trigger an assessment of whether it affects the evidence's authenticity, integrity, or capacity for subsequent verification. In other words, the discovery of a weakness in the technology securing electronic evidence should not automatically produce the legal invalidation of that evidence. Rather, its consequences should be assessed in

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

relation to the evidentiary material and circumstances of the particular case.

This model provides a balance between legal certainty and the pursuit of material truth. Legal certainty requires that evidence previously admitted in accordance with applicable law should not become automatically invalid whenever technological developments reveal weaknesses in previously accepted cryptographic mechanisms. Otherwise, the legal status of historical electronic evidence would remain perpetually vulnerable to technological change. At the same time, the pursuit of material truth requires courts to examine whether a particular technical vulnerability has actually compromised the evidence before them. The two dimensions should therefore remain analytically independent while functioning together within the evidentiary process.

Accordingly, criminal procedural law could adopt a technology-neutral framework under which lawfully obtained electronic evidence remains admissible, subject to verification of its authenticity, integrity, and reliability according to applicable and periodically updated technical standards. This approach would be preferable to prescribing specific algorithms in legislation. A statutory reference to a particular hash algorithm, for example, could become problematic once that algorithm is rendered insecure or technologically obsolete. By delegating the formulation and periodic revision of technical standards to appropriate implementing regulations, the law could maintain stable normative principles while allowing technical requirements to evolve.

The distinction also clarifies the consequences of cryptographic vulnerabilities. A weakness in a cryptographic algorithm should not automatically be equated with the invalidity of the evidence. Instead, the relevant inquiry should be whether the vulnerability has materially affected the authenticity or integrity of the evidence in the particular proceedings. This approach is consistent with the direction of Indonesian scholarship concerning electronic evidence, which emphasizes the need for more precise methods of assessing its reliability and consistency. The practical consequence is the need to strengthen the concept of a cryptographic chain of custody. Reliability cannot remain merely a formal declaration; it must be supported by a traceable evidentiary history and concrete mechanisms for verification and re-verification. Only through such mechanisms can the distinction between legal admissibility and technical reliability acquire substantive meaning within criminal proceedings.

2. Establishing a "Cryptographic Chain of Custody"

The conventional chain of custody in criminal proceedings is designed to establish who collected the evidence, who possessed and examined it, when it was transferred, and what was done to it at each stage. Its primary function is to demonstrate that the evidence presented before the court is the same evidence

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

originally obtained by investigators and has not been altered during its handling. For electronic evidence, however, this conventional model is insufficient. The integrity and authenticity of digital information depend not only on human custodians but also on the technologies used to preserve and verify the evidence. Provenance, integrity, authenticity, and traceability must therefore be treated as integral components of the electronic chain of custody.

This technological dimension distinguishes electronic evidence from physical evidence. Physical alterations may in some circumstances be observable or otherwise detectable through conventional inspection. Digital information, by contrast, may be modified at the level of a single bit without producing any perceptible physical indication. Without appropriate cryptographic and forensic controls, the alteration may therefore remain invisible. The chain of custody of electronic evidence must consequently move beyond the traditional question of "who handled the evidence?" to include the equally important question of "what technological mechanisms preserved the evidentiary integrity of the information?"

Quantum computing makes this additional inquiry increasingly important. The conventional chain of custody must now account not only for the persons who handled the evidence and the procedures applied to it, but also for the cryptographic assumptions upon which its authenticity and integrity depend. The relevant inquiry should therefore include the cryptographic algorithms used to generate hash values, digital signatures, timestamps, and other authentication mechanisms [30]. These mechanisms function as technological assurances connecting the evidence presented in court to the evidence originally acquired during the investigation. If the underlying cryptographic algorithm becomes vulnerable to quantum attacks, the reliability of that connection may be called into question.

This problem may be illustrated through the analogy of a lock protecting a cabinet containing evidence. The integrity of the cabinet's contents is trusted because the lock is assumed to prevent unauthorized access. If technological developments subsequently make it possible to defeat the lock without visibly opening the cabinet, the reliability of that protection becomes uncertain. The same principle applies to cryptographic algorithms. The fact that no unauthorized person is known to have accessed or modified the evidence does not necessarily eliminate concerns once the cryptographic mechanism used to establish its integrity is shown to be vulnerable.

Therefore, the chain of custody needs to evolve into a "Cryptographic Chain of Custody" a mechanism that incorporates information regarding cryptographic algorithms as an official component of an electronic evidence item's legal and technical history. At a minimum, this information must include the hash

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

algorithms and digital signatures employed, the time of their application, hash values, timestamps, key holder identities, verification processes, and any changes in the algorithm's security status throughout the evidence's storage period. Under this concept, should an algorithm later be found to be weak, law enforcement officials and judges would not lose the trail; they could still trace back the mechanisms used to establish the evidence's authenticity and integrity. Essentially, the concept is akin to maintaining a comprehensive log of the "locks" used; if the evidence is challenged in the future, one simply consults the records rather than resorting to guesswork. The crucial point is not to mandate a specific algorithm as an absolute prerequisite for the validity of evidence, since the validity of all evidence relying on that algorithm would be compromised once it became obsolete. But rather to integrate the cryptographic security history into the chain of custody itself. This allows criminal procedural law to track two parallel paths: the physical journey of the evidence as it changes hands, and the technological journey that underpins trust in its integrity. These two complementary trails ensure the evidentiary system remains robust, even as technology continues to evolve.

CONCLUSION

This study concludes that although Indonesian law recognizes electronic evidence as admissible, via the ITE Law and the latest Criminal Procedure Code, the current criminal procedural framework is not yet fully prepared to address the threat quantum computing poses to the cryptographic foundations underpinning the authenticity, integrity, and reliability of such evidence. Reactive regulations, combined with the absence of mandates for migrating to post-quantum cryptography or re-verification mechanisms within the chain of custody, create a "retroactive verification problem" that could jeopardize the future validity of electronic evidence. To address this issue, the study proposes a reform model featuring a clear distinction between legal validity and technical reliability, alongside the transformation of the chain of custody into a "Cryptographic Chain of Custody" that documents cryptographic security history as part of the evidentiary record. Through this model, criminal procedural law is expected to sustain confidence in electronic evidence, not only at the time of initial acquisition but also as the underlying authentication technologies evolve. Further empirical research is required to test the practical application of this model within Indonesian criminal investigation and judicial proceedings.

DECLARATION OF GENERATIVE AI

In the course of preparing this manuscript, the Authors employed Claude and ChatGPT as research and editorial assistance tools. These artificial intelligence tools were utilized to support the exploration of relevant literature, the development of the analytical framework, the paraphrasing of selected passages for enhanced clarity and readability,

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

and translating to english legal academic writing. Following the use of these tools/services, the Authors conducted a thorough review, verification, and revision of the resulting content as necessary, and the Authors assume full and sole responsibility for the content of this publication.

ACKNOWLEDGEMENTS

No specific acknowledgements are necessary for this manuscript. This research was conducted without external funding or financial support from any institution or organization.

REFERENCES

[1] Z. Guo, "Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications," *Computer Law & Security Review*, vol. 48, p. 105774, Apr. 2023, doi: 10.1016/J.CLSR.2022.105774.

[2] M. Bérubé, L. A. Beaulieu, S. Allard, and V. Denault, "From digital trace to evidence: Challenges and insights from a trial case study," *Science & Justice*, vol. 65, no. 5, p. 101306, Sep. 2025, doi: 10.1016/J.SCIJUS.2025.101306.

[3] G. Horsman, "Digital evidence strategies for digital forensic science examinations," *Science & Justice*, vol. 63, no. 1, pp. 116–126, Jan. 2023, doi: 10.1016/J.SCIJUS.2022.11.004.

[4] G. Horsman, "Sources of error in digital forensics," *Forensic Science International: Digital Investigation*, vol. 48, p. 301693, Mar. 2024, doi: 10.1016/J.FSIDI.2024.301693.

[5] R. Stoykova and K. Franke, "Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations," *Forensic Science International: Digital Investigation*, vol. 45, p. 301554, Jun. 2023, doi: 10.1016/J.FSIDI.2023.301554.

[6] K. Li, P. G. Yan, and Q. Y. Cai, "Quantum computing and the security of public key cryptography," *Fundamental Research*, vol. 1, no. 1, pp. 85–87, Jan. 2021, doi: 10.1016/J.FMRE.2020.12.001.

[7] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," *Network Security*, vol. 2020, no. 9, pp. 9–15, Sep. 2020, doi: 10.1016/S1353-4858(20)30105-7.

[8] D. Closser and E. Bou-Harb, "A live digital forensics approach for quantum mechanical computers," *Forensic Science International: Digital Investigation*, vol. 40, p. 301341, Apr. 2022, doi: 10.1016/J.FSIDI.2022.301341.

[9] K. Balarabe, "Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap," *European Journal of Risk Regulation*, vol. 16, no. 2, pp. 794–813, 2025, doi: DOI: 10.1017/err.2025.8.

[10] S. Alhazmi, K. Elleithy, and A. Elleithy, "Digital Forensics of Quantum Computing: The Role of Quantum Entanglement in Digital Forensics—Current Status and Future Directions," Dec. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/quantum7040044.

[11] L. Loffi, G. L. Camillo, C. A. De Souza, C. M. Westphall, and C. B. Westphall, "Management of the Chain of Custody of Digital Evidence Using Blockchain and Self-Sovereign Identities: A Systematic Literature Review," 2025, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2025.3560191.

[12] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "The pseudo metadata concept for the chain of custody of digital evidence," 2019.

[13] N. AllahRakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations," *Mexican Law Review*, vol. 16, no. 2, pp. 23–54, Jan. 2024,

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

doi: 10.22201/iij.24485306e.2024.2.18892.
[14] R. de Wolf, "The potential impact of quantum computers on society," *Ethics Inf. Technol.*, vol. 19, no. 4, pp. 271–276, Dec. 2017, doi: 10.1007/s10676-017-9439-z.
[15] C. Neale, "Fool me once: A systematic review of techniques to authenticate digital artefacts," *Forensic Science International: Digital Investigation*, vol. 45, p. 301516, Jun. 2023, doi: 10.1016/J.FSIDI.2023.301516.
[16] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, "Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition," *Comput. Secur.*, vol. 150, p. 104272, Mar. 2025, doi: 10.1016/J.COSE.2024.104272.
[17] N. Sunde and V. N. L. Franqueira, "Adding transparency to uncertainty: An argument-based method for evaluative opinions," *Forensic Science International: Digital Investigation*, vol. 47, p. 301657, Dec. 2023, doi: 10.1016/J.FSIDI.2023.301657.
[18] R. Muhammad and S. Abdul Adjid, "Penggunaan Alat Bukti Elektronik dalam Konteks Penyadapan Menurut Peraturan Tindak Pidana Korupsi," *Legal Spirit*, vol. 9, no. 2, pp. 455–466, 2025, [Online]. Available: http://publishing-widyagama.ac.id/ejournal-v2/index.php/jhls/
[19] H. Wu and G. Zheng, "Electronic evidence in the blockchain era: New rules on authenticity and integrity," *Computer Law & Security Review*, vol. 36, p. 105401, Apr. 2020, doi: 10.1016/J.CLSR.2020.105401.
[20] L. Luo and J. Zhou, "BlockTour: A blockchain-based smart tourism platform," *Comput. Commun.*, vol. 175, pp. 186–192, Jul. 2021, doi: 10.1016/J.COMCOM.2021.05.011.
[21] T. Kim, L. Dũng, H. Tho, and H. Nguyen Hoang, "Quantum Resistant Digital Signatures Constructed from a Nonstandard Discrete Logarithm Problem over Finite Fields," *Journal of Communications*, vol. 21, pp. 1–11, Jan. 2026, doi: 10.12720/jcm.21.1.1-11.
[22] S. Ali *et al.*, "Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity—Threats, Mitigations, and Solutions," *Computers and Electrical Engineering*, vol. 128, p. 110649, Dec. 2025, doi: 10.1016/J.COMPELECENG.2025.110649.
[23] D. Gurung, S. R. Pokhrel, and G. Li, "Performance analysis and evaluation of postquantum secure blockchained federated learning," *Computer Networks*, vol. 255, p. 110849, Dec. 2024, doi: 10.1016/J.COMNET.2024.110849.
[24] R. Stoykova, S. Andersen, K. Franke, and S. Axelsson, "Reliability assessment of digital forensic investigations in the Norwegian police," *Forensic Science International: Digital Investigation*, vol. 40, p. 301351, Mar. 2022, doi: 10.1016/J.FSIDI.2022.301351.
[25] P. R. Babu, S. A. P. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," *Comput. Sci. Rev.*, vol. 54, p. 100676, Nov. 2024, doi: 10.1016/J.COSREV.2024.100676.
[26] R. Stoykova, "Digital evidence: Unaddressed threats to fairness and the presumption of innocence," *Computer Law & Security Review*, vol. 42, p. 105575, Sep. 2021, doi: 10.1016/J.CLSR.2021.105575.
[27] M. Matijević Gostojić and Ž. Vuković, "A knowledge-based system for supporting the soundness of digital forensic investigations," *Forensic Science International: Digital Investigation*, vol. 46, p. 301601, Sep. 2023, doi: 10.1016/J.FSIDI.2023.301601.
[28] V. R. Kebande, "Quantum Computing in Industrial Internet of Things (IIoT) Forensics: Framework, Implications, Opportunities, and Future Directions," *WIREs Forensic Science*, vol. 7, no. 3, p. e70013, Sep. 2025, doi: https://doi.org/10.1002/wfs2.70013.
[29] D. Dogra, "Law and Digital Forensics: Evidentiary Standards, Chain of Custody, and Admissibility in the Digital Age," *Juris Quantum: Journal of Emerging Technology and Law*, vol. 1, no. 1, 2026, [Online]. Available: https://jurisquantum.com/index.php/jqjetl/article/view/7

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.

DOI: doi.org/10.33830/osc.v4i1.9278/ ISSN: 3032-2227

[30] G. Comandè and M. Varilek, "The many features which make the eIDAS 2 Digital Wallet either risky or the ideal vehicle for the transition to post-quantum encryption," *Computer Law & Security Review*, vol. 54, p. 106022, Sep. 2024, doi: 10.1016/J.CLSR.2024.106022.

Copyright © 2026, Abdurrahman, Qorina Khoirunisa.