2024, Vol. 1
https://fupress.org/journal

Blockchain Evidence in Criminal Trials: Admissibility, Integrity, and Chain of Custody

Melissa Ortega [1*]

[1] Dr., Faculty of Law and Criminology, University of Buenos Aires, Buenos Aires, Argentina
* **Corresponding Author:** m.ortega@uba.ar

ARTICLE INFO

Received: 13 May 2024
Accepted: 25 Aug 2024

ABSTRACT

The increasing use of blockchain technology in financial transactions, digital communications, and decentralized systems presents new challenges and opportunities for criminal litigation. This article examines the legal implications of admitting blockchain-based evidence in criminal trials, focusing on issues of admissibility, data integrity, and chain of custody. Drawing on comparative legal frameworks and emerging jurisprudence, it explores how courts may assess the evidentiary value of blockchain entries, the reliability of decentralized data records, and whether traditional evidentiary standards can accommodate cryptographically secured and distributed evidence. The article concludes with recommendations for policymakers and legal practitioners regarding the standardization and certification of blockchain evidence.

Keywords: Blockchain, Digital Communications, Criminal Trials, Evidence.

INTRODUCTION

Blockchain technology, initially developed to support cryptocurrencies such as Bitcoin, has evolved into a broader tool for decentralized recordkeeping and verification. Its unique features—immutability, distributed consensus, and cryptographic integrity—offer a novel way to store and authenticate information. As the use of blockchain expands into identity management, contract execution, and digital forensics, its intersection with criminal procedure law becomes increasingly relevant.

This article addresses a fundamental question: Can blockchain records be effectively and fairly used as evidence in criminal trials? More specifically, it evaluates whether blockchain evidence meets existing legal standards for admissibility, how its integrity can be assessed in judicial contexts, and what implications arise for maintaining a legally sound chain of custody.

Criminal procedure law is deeply rooted in the principles of fairness, reliability, and transparency. Evidence introduced in court must not only meet the threshold of admissibility but must also be subject to contestation and scrutiny. Traditional digital evidence—from emails to metadata—has challenged legal practitioners to adapt rules of authentication and verification. Blockchain, with its distributed and encrypted infrastructure, adds a new layer of complexity to these debates.

One of the core dilemmas is whether the decentralized nature of blockchain systems can be reconciled with the centralized authority of courts. Unlike conventional records stored in institutional databases, blockchain entries are spread across nodes, each holding a copy of the ledger. This raises questions about which entity, if any, can vouch for the authenticity of the record.

Moreover, blockchain evidence may originate from systems or platforms that lack formal oversight, jurisdictional clarity, or user accountability. For instance, a smart contract that logs user behavior in a decentralized finance application could be relevant in proving fraud or intent. Yet, its evidentiary weight would depend heavily on the court's ability to interpret the code, validate the input, and attribute authorship.

Comparative legal systems show varying degrees of preparedness in dealing with blockchain evidence. Some common law jurisdictions have started to develop jurisprudence around digital assets and distributed records.

Civil law systems, with their codified structures, are exploring statutory amendments or regulatory guidance. Despite these efforts, a consistent framework is lacking, and practitioners are often left navigating a legal grey zone.

This article builds on interdisciplinary research from law, computer science, and forensic studies to offer a structured analysis of the main legal challenges posed by blockchain evidence. Sections 2 through 4 provide detailed examinations of admissibility criteria, data integrity considerations, and chain of custody implications. The final section outlines actionable recommendations for policymakers and legal professionals.

ADMISSIBILITY OF BLOCKCHAIN EVIDENCE

In most legal systems, for evidence to be admissible in a criminal trial, it must be relevant, authentic, and not unduly prejudicial. Blockchain records often meet these requirements in principle, especially regarding authenticity, due to their cryptographic signatures and time-stamped entries.

However, admissibility is complicated by the technical opacity of blockchain systems. Judges and juries may not fully understand the underlying technology, leading to concerns about the transparency and contestability of such evidence. Moreover, blockchain data typically require expert interpretation, which raises questions about the neutrality and qualifications of those experts.

Different jurisdictions have taken varying approaches. In the United States, Federal Rule of Evidence 901 allows for authentication of digital records if a witness with knowledge testifies about their accuracy. Blockchain logs have been admitted under this rule when accompanied by proper expert testimony. In the EU, the eIDAS Regulation (EU Regulation 910/2014) provides a framework for recognizing electronic records and signatures, but its application to decentralized blockchain entries remains debated (De Filippi & Hassan, 2016).

Admissibility also depends on how the blockchain was used. If the data were recorded on a public blockchain with verified nodes and consensus protocols, courts may view it as more trustworthy than entries on a private or permissioned chain controlled by a single entity.

The use of smart contracts adds additional layers of complexity. For example, the execution of smart contracts can trigger automatic transfers or record events that may later be relevant to a criminal case. However, their self-executing nature and lack of human intervention raise questions about intent, voluntariness, and foreseeability—key considerations in criminal liability (D. Tapscott & Tapscott, 2018).

Moreover, questions of hearsay may arise. Blockchain entries may be considered out-of-court statements, requiring exceptions or novel interpretations under hearsay rules. While some scholars argue that cryptographic verification substitutes for human testimony, others warn against conflating technical reliability with legal trustworthiness.

Ultimately, for blockchain evidence to be admitted, courts must establish a chain of logical and procedural steps demonstrating how the data were generated, recorded, and preserved. This often entails the presentation of system architecture, validation mechanisms, and access logs, alongside expert witness testimony. Legal frameworks may need to evolve to codify such protocols.

INTEGRITY AND RELIABILITY OF BLOCKCHAIN DATA

One of blockchain's core features is its resistance to tampering. Once data are entered into a blockchain, altering them retroactively without network consensus is practically infeasible. This immutability contributes to the probative value of blockchain evidence. Yet, this strength can also be a limitation: if erroneous or malicious data are entered, they become permanently embedded.

Another concern is that while the blockchain ensures data integrity post-entry, it cannot verify the authenticity of inputs at the moment of entry. The principle of "garbage in, garbage out" remains valid—if fraudulent data are entered, the blockchain will preserve them as faithfully as legitimate entries (Wright & De Filippi, 2015).

Thus, blockchain’s evidentiary reliability depends heavily on the credibility of the data input mechanisms. Evidence derived from smart contracts, IoT devices, or user-generated logs must be evaluated in light of their source reliability and security.

The forensic evaluation of blockchain data must also consider the type of blockchain—public, private, or consortium-based—and the consensus mechanism in use (e.g., proof of work, proof of stake, or Byzantine fault

tolerance). These variables affect the level of decentralization, fault tolerance, and security.

Moreover, technical vulnerabilities in blockchain implementations, such as 51% attacks or smart contract bugs, can undermine data integrity. Forensic experts must be able to detect anomalies, audit code, and reconstruct timelines with precision.

Blockchain metadata, such as block height, transaction hash, and wallet addresses, can provide critical corroborative evidence. However, without proper decryption or contextual interpretation, such metadata may confuse rather than clarify. Courts may require explanatory charts, timelines, or simulation tools to assess such evidence.

Courts must also consider the forensic soundness of blockchain interactions. Technical documentation of node operations, consensus algorithms, and hashing processes may need to be included as part of the evidentiary package. Without such context, blockchain data may be dismissed as incomprehensible or inadmissible.

Finally, questions of interoperability and standardization remain unresolved. Not all blockchain platforms operate under common protocols, and forensic tools may not yet support the full range of ledgers. This hampers cross-border investigations and complicates international legal cooperation.

CHAIN OF CUSTODY IN DECENTRALIZED CONTEXTS

The chain of custody is a critical requirement for criminal evidence: it ensures that data have not been altered, substituted, or tampered with between collection and presentation in court. Traditional chain of custody logs are linear, human-verified, and centralized. Blockchain upends this model.

In decentralized contexts, maintaining a coherent chain of custody requires novel methods. Timestamped blockchain entries can serve as automatic custody logs, recording who accessed or transferred data and when. Some blockchain applications even allow for tokenized tracking of digital evidence, improving auditability.

However, the challenge lies in mapping these technical logs onto legally recognized procedures. Courts must be able to trace evidentiary provenance through metadata, key signatures, and access controls. Questions also arise about who controls the blockchain, what jurisdiction governs it, and whether smart contracts used to manage evidence access are legally valid.

Blockchain-based evidence tracking systems can provide tamper-evident logs, but their legal acceptance depends on whether courts recognize automated logs as substitutes for human attestations. Some jurisdictions may require notarized certification of blockchain entries or supplemental affidavits from administrators.

Furthermore, the anonymity and pseudonymity inherent in blockchain networks pose difficulties for assigning legal responsibility. If access logs are linked only to wallet addresses or cryptographic keys, courts may struggle to establish user identity without additional investigative methods.

Chain of custody is not just a technical issue—it is a legal narrative about control, responsibility, and continuity. Hybrid systems that combine blockchain timestamping with manual entries, biometric verification, or third-party certification may offer more legally robust solutions.

Legal reforms may also be necessary to define how blockchain-based custody records can be contested, amended, or cross-examined. Without procedural safeguards, the evidentiary weight of blockchain logs could become either overstated or underutilized.

Ultimately, for blockchain to contribute meaningfully to the evidentiary chain, its logs must be integrated into a broader evidentiary ecosystem that includes legal accountability, forensic transparency, and procedural fairness.

RECOMMENDATIONS AND CONCLUSION

Blockchain evidence presents a promising but complex frontier for criminal justice. Its immutability and auditability can enhance evidentiary rigor, but only if legal standards evolve to accommodate its unique features. Based on the foregoing analysis, this article offers the following recommendations:

Standardize Expert Protocols: Judicial systems should define clear qualifications and protocols for experts presenting blockchain evidence.

Update Legal Frameworks: Legislators should develop specific rules for digital ledger evidence, possibly as amendments to existing codes of criminal procedure.

Support Hybrid Custody Systems: Legal authorities should promote integrated custody models combining

blockchain logging with traditional documentation.

Invest in Judicial Education: Judges and legal professionals should receive training in distributed ledger technologies to ensure informed evaluation.

As blockchain applications continue to grow in sectors relevant to criminal law—such as finance, identity, and surveillance—it is imperative that courts be equipped to handle their evidentiary byproducts. While blockchain cannot guarantee truth, it can reinforce the traceability and transparency essential to justice.

References

De Filippi, P., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday, 21*(12). https://doi.org/10.5210/fm.v21i12.7113

Tapscott, D., & Tapscott, A. (2018). *Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world*. Penguin.

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2580664