Formosa Journal of Applied Sciences (FJAS)
Vol. 5, No. 7 2026: 1475-1492

The Evidentiary Strength of Blockchain Transactions as Electronic Evidence in the Indonesian Criminal Procedure Law System

Aloysius Wisnubroto[1]*, Winarno[2]
Universitas Atma Jaya Yogyakarta
Corresponding Author: Aloysius Wisnubroto al.wisnubroto@uajy.ac.id

A R T I C L E I N F O

Keywords: Blockchain Transactions, Criminal Procedure Law, Electronic Evidence

Received : 14, March
Revised : 16, May
Accepted: 18, July

A B S T R A C T

This study examines the evidentiary strength of blockchain transaction data as electronic evidence within the Indonesian criminal procedure law system. The research aims to clarify the legal positioning and probative value of blockchain-based records in criminal proceedings, contributing to the development of digital evidence doctrine. A normative legal research method was applied using statutory and conceptual approaches, analyzing the Criminal Procedure Code (KUHAP) and the Electronic Information and Transactions Law (UU ITE). The analysis focuses on blockchain transactions as legal concepts of electronic information supported by forensic interpretation. The study finds that blockchain data is admissible as electronic evidence but its evidentiary strength depends on authentication, integrity, and linkage to legal identity. The results imply the need for standardized blockchain forensic procedures in Indonesian criminal justice practice.

DOI prefik: https://doi.org/10.55927/fjas.v5i7.73
ISSN-E: 2962-6447
https://journalfjas.my.id/index.php/fjas

INTRODUCTION

Blockchain technology has emerged as one of the most significant digital innovations in the contemporary legal and technological landscape. As a decentralized, cryptographically secured, and immutable ledger, blockchain enables the recording of digital transactions in a manner that is verifiable, transparent, and highly resistant to unauthorized alteration (Drescher, 2017; Narayanan et al., 2016). Initially developed as the underlying infrastructure of cryptocurrency, blockchain has expanded into various sectors, including finance, public administration, digital identity, supply-chain governance, and legal technology. Its core features, particularly decentralization, transparency, cryptographic validation, and immutability, create new possibilities for securing digital information and verifying transactional records. In the context of criminal justice, these characteristics are increasingly relevant because many contemporary crimes leave digital traces that can be examined, verified, and presented as evidence in legal proceedings.

The development of cryptocurrency-based transactions has introduced both opportunities and challenges for law enforcement. On the one hand, blockchain enables rapid peer-to-peer value transfer without reliance on traditional financial intermediaries. On the other hand, the same technology may be misused for criminal purposes, including investment fraud, ransomware payments, money laundering, illicit trading of digital assets, and other forms of cyber-enabled crime (Azzahra, 2024; Ilmi & Lubis, 2025). In such cases, blockchain transaction data may contain important information regarding wallet addresses, transaction hashes, timestamps, transfer values, and movement of digital assets across multiple addresses. These data can potentially assist investigators in tracing the flow of funds, identifying suspicious transaction patterns, and linking digital activities to criminal conduct. However, the technical availability of blockchain data does not automatically guarantee its legal admissibility or evidentiary strength in court.

In the Indonesian legal context, the evidentiary status of blockchain transactions must be examined in relation to criminal procedure law and electronic information law. The Indonesian Criminal Procedure Code, or KUHAP, traditionally recognizes evidence such as witness testimony, expert testimony, documents, indications, and statements of the accused. Meanwhile, the Electronic Information and Transactions Law, particularly as amended through Law Number 1 of 2024, recognizes electronic information and electronic documents as legally valid evidence. This legal development provides a normative basis for the use of digital data in legal proceedings. Nevertheless, blockchain evidence presents a distinct challenge because it is not merely a conventional electronic document, but a technically complex record generated through decentralized validation, cryptographic mechanisms, and distributed network consensus. Therefore, its legal recognition requires careful examination of both its technical characteristics and its compatibility with procedural safeguards.

Although blockchain is often described as immutable and tamper-resistant, its evidentiary value in criminal proceedings remains legally contingent. Blockchain data must still be authenticated, verified, interpreted, and connected to relevant facts of the case. Important issues include the integrity of the data extraction process, the reliability of forensic tools, the maintenance of chain of custody, the competence of digital forensic experts, and the correlation between on-chain data and off-chain evidence. For example, a transaction hash may prove that a transfer occurred on a blockchain network, but it does not automatically prove the real-world identity of the person controlling a wallet address. To establish probative value, blockchain transaction records must be supported by additional evidence, such as exchange account data, Know Your Customer documentation, device seizure results, communication records, banking information, or expert analysis (Atlam et al., 2024; Bonomi et al., 2020; Conti et al., 2018).

This study addresses a significant gap in the existing literature by connecting the technological characteristics of blockchain with the evidentiary framework of Indonesian criminal law. Previous studies have generally focused on either the technical aspects of blockchain analysis or the broader regulation of cybercrime and cryptocurrency. However, limited attention has been given to how blockchain transaction data should be positioned within Indonesian criminal procedure, particularly in terms of admissibility, authentication, probative strength, and judicial assessment. This research therefore offers a doctrinal and practical contribution by situating blockchain evidence within the procedural and normative context of Indonesia. It also provides an operational perspective for legal practitioners, investigators, prosecutors, judges, and digital forensic experts in assessing blockchain-based evidence.

The novelty of this paper lies in its systematic examination of blockchain as a hybrid form of electronic evidence. On the technical side, blockchain records are highly reliable because they are cryptographically secured, publicly verifiable, and resistant to alteration. On the legal side, however, their evidentiary strength depends on procedural compliance, expert explanation, and their connection with other legally admissible evidence. This dual nature makes blockchain evidence both promising and complex. Accordingly, this research contributes to the enrichment of legal knowledge in three main ways: it expands doctrinal understanding of electronic evidence in emerging digital contexts, it focuses specifically on blockchain transactions within Indonesian criminal cases, and it proposes evaluative parameters for forensic and judicial practice.

Based on this background, this research aims to investigate the legal position of blockchain transactions as admissible electronic evidence under Indonesian law, assess the factors that determine their evidentiary strength in criminal proceedings, and formulate conceptual recommendations for integrating blockchain data into legal practice while ensuring compliance with due process principles. By doing so, this study contributes theoretically to the development of evidentiary doctrine in the digital era and practically to the formulation of forensic validation and judicial evaluation guidelines for blockchain-based evidence.

LITERATURE REVIEW

Blockchain Technology as a Distributed Ledger System

Blockchain technology is widely recognized as a distributed ledger system that enables decentralized recording of transactions through cryptographic validation and consensus mechanisms. Unlike traditional centralized databases, blockchain distributes data across multiple nodes, ensuring that no single authority controls the system. Each transaction is grouped into a block, which is then cryptographically linked to previous blocks, forming a continuous chain of records that is resistant to unauthorized modification (Zohar, 2015; Crosby et al., 2016). This structural design creates a tamper-evident ledger where alteration of historical data becomes computationally impractical.

From a technical perspective, blockchain relies on cryptographic hashing, digital signatures, and distributed consensus protocols. These mechanisms ensure data integrity, authentication, and transparency. Although blockchain is often described as immutable, its immutability is technical rather than absolute in legal interpretation, since the meaning and attribution of data still depend on external validation processes (Pilkington, 2016; Swan, 2015).

Blockchain, Cryptocurrency, and Cybercrime Risks

The development of blockchain-based cryptocurrencies has introduced both innovation and risk in the financial and legal landscape. Cryptocurrencies enable peer-to-peer transactions without intermediaries, offering efficiency and global accessibility. However, the same characteristics also enable misuse in cybercrime contexts, including ransomware, fraud, darknet transactions, and money laundering activities (Foley et al., 2019; Choo, 2015). The pseudonymous nature of blockchain systems creates a significant evidentiary challenge. While transaction data are publicly accessible, they are linked only to alphanumeric wallet addresses rather than real-world identities. This creates a gap between on-chain activity and legal attribution. Therefore, blockchain data must often be combined with off-chain evidence such as exchange records, device forensics, and KYC data to establish criminal liability (Europol, 2023).

Digital Forensics and Blockchain Evidence Handling

Digital forensic science provides the methodological foundation for managing electronic evidence in criminal investigations. Digital evidence must be collected, preserved, analyzed, and presented in a manner that ensures integrity and reproducibility (Casey, 2011). Within this framework, chain of custody is a critical principle that documents every stage of evidence handling from acquisition to courtroom presentation. Blockchain technology has also been proposed as a tool to enhance forensic processes. Some studies suggest that blockchain can strengthen chain of custody systems by creating immutable logs of evidence handling activities, thereby improving transparency and accountability (Bonomi et al., 2020). In forensic contexts, blockchain analytics tools are also used to trace transaction flows, identify clustering patterns, and analyze suspicious financial movements across networks (Anderson et al., 2020).

Despite these advancements, blockchain forensic evidence still requires careful interpretation. Technical traceability does not automatically translate into legal attribution, making expert analysis essential in bridging this gap.

Electronic Evidence in Criminal Law Framework

Electronic evidence has become increasingly important in modern criminal justice systems due to the rise of digital communication and transactions. In general, electronic evidence refers to any information stored or transmitted in digital form that can be presented in legal proceedings. In Indonesia, the legal framework for electronic evidence is governed by the Criminal Procedure Code (KUHAP) and the Electronic Information and Transactions Law (UU ITE). KUHAP provides the traditional evidentiary categories, while UU ITE expands admissibility to include electronic information and electronic documents. This creates a hybrid evidentiary system where digital data, including blockchain records, may be accepted as legal evidence provided that procedural requirements are met. However, admissibility does not automatically guarantee probative value. Courts must still evaluate authenticity, reliability, and relevance before accepting electronic evidence in criminal proceedings.

Authentication, Integrity, and Chain of Custody in Digital Evidence

Authentication is a core requirement in determining whether digital evidence can be admitted in court. It involves proving that the evidence is genuine and corresponds to what it purports to represent. In blockchain-related cases, authentication may involve verifying transaction hashes, block confirmations, and wallet activity using forensic tools. Integrity refers to the assurance that evidence has not been altered during collection, storage, or analysis. Although blockchain itself provides strong integrity at the network level, the integrity of extracted data depends on forensic handling procedures. Screenshots or secondary data extraction methods may weaken evidentiary reliability compared to raw blockchain data verification. Chain of custody ensures that all handling of evidence is properly documented. Any break in this chain may undermine the credibility of evidence in court. In blockchain investigations, maintaining chain of custody becomes more complex due to the involvement of multiple tools, platforms, and intermediaries during data extraction and analysis.

Judicial Interpretation and Probative Value of Blockchain Evidence

The probative value of blockchain evidence depends on its ability to establish legally relevant facts in criminal proceedings. While blockchain data can prove that a transaction occurred, it does not automatically prove ownership, intent, or criminal involvement. Judicial interpretation plays a critical role in assessing blockchain evidence. Courts must determine whether blockchain data are relevant, reliable, and sufficiently linked to the accused. This often requires expert testimony from digital forensic specialists who can explain blockchain mechanisms, transaction tracing, and analytical limitations. However, judicial caution is necessary to avoid over-reliance on technical evidence. Blockchain data

should be considered as part of a broader evidentiary framework that includes both on-chain and off-chain evidence.

Synthesis and Research Positioning

The literature demonstrates that blockchain technology offers strong technical guarantees of transparency and integrity, yet its legal application as evidence remains complex. Cybercrime studies highlight its dual-use nature, while forensic research emphasizes methodological rigor in handling digital evidence. Legal frameworks, particularly in Indonesia, have begun to accommodate electronic evidence, but specific integration of blockchain data into criminal procedure remains underdeveloped. This study positions blockchain transaction data as a hybrid form of electronic evidence that requires multidimensional evaluation. Its evidentiary strength depends not only on cryptographic validity but also on procedural compliance, forensic interpretation, and judicial reasoning. Therefore, blockchain evidence should be assessed through integrated legal and technical standards to ensure fairness, reliability, and due process in criminal justice systems.

METHODOLOGY

This research applies a normative legal research method, which focuses on the examination of legal norms, statutory provisions, legal doctrines, and conceptual principles relevant to the use of blockchain transactions as electronic evidence in Indonesian criminal procedure law. Normative legal research is appropriate for this study because the main issue does not concern empirical measurement or field data, but rather the legal position and evidentiary strength of blockchain transaction records within the framework of criminal evidence law. Therefore, the analysis is directed toward understanding how existing legal instruments regulate electronic evidence and how such instruments may be interpreted in relation to blockchain-based transaction data.

This study uses two main approaches, namely the statutory approach and the conceptual approach. The statutory approach is applied by examining laws and regulations relevant to electronic evidence and criminal procedure in Indonesia. The primary legal materials include Law Number 8 of 1981 concerning Criminal Procedure Law (KUHAP), Law Number 11 of 2008 concerning Electronic Information and Transactions as amended, including Law Number 1 of 2024, and other relevant regulations concerning electronic information, digital transactions, cybercrime, and criminal evidentiary procedure. Through this approach, the research identifies the legal basis for recognizing blockchain transaction records as electronic information or electronic documents that may be submitted as evidence in criminal proceedings.

The conceptual approach is used to analyze legal concepts related to evidence, admissibility, probative value, authentication, integrity, relevance, and chain of custody. This approach is important because blockchain transactions have specific technical characteristics that differ from conventional electronic documents. Blockchain data are decentralized, cryptographically secured, time-stamped, and generally resistant to unauthorized alteration. However, these technical characteristics must be translated into legal concepts before they can be

properly assessed in court. Accordingly, this study examines whether blockchain transaction records can satisfy the legal requirements of valid electronic evidence and how courts should assess their evidentiary weight.

The sources of legal materials in this research consist of primary, secondary, and tertiary legal materials. Primary legal materials include statutes, regulations, and official legal instruments governing criminal procedure and electronic evidence in Indonesia. Secondary legal materials include journal articles, books, legal commentaries, research reports, and scholarly writings discussing blockchain technology, cryptocurrency-related crimes, digital forensics, electronic evidence, and criminal evidentiary law. Tertiary legal materials, such as legal dictionaries and encyclopedic sources, are used to clarify technical and legal terminology where necessary.

Data collection is conducted through library research by tracing and reviewing relevant legal sources and academic literature. The collected materials are selected based on their relevance to three main themes: the regulation of electronic evidence in Indonesian law, the technical nature of blockchain transactions, and the requirements for proving digital evidence in criminal proceedings. Materials that directly discuss authentication, integrity verification, forensic examination, and the linkage between on-chain and off-chain evidence are prioritized because they are closely related to the evidentiary strength of blockchain transaction data.

The legal materials are analyzed using qualitative descriptive analysis. The analysis is carried out by interpreting statutory provisions, comparing them with legal doctrines on electronic evidence, and evaluating their applicability to blockchain transactions. The study does not use statistical tools because it is not designed as quantitative research. Instead, the analysis relies on legal reasoning, doctrinal interpretation, and conceptual evaluation. The interpretation is conducted systematically by connecting the provisions of KUHAP and the Electronic Information and Transactions Law with the technical characteristics of blockchain records.

The analytical process is divided into several stages. First, the research identifies the legal framework governing evidence in Indonesian criminal procedure. Second, it examines the recognition of electronic information and electronic documents as valid legal evidence. Third, it evaluates whether blockchain transaction data can be categorized as electronic evidence under Indonesian law. Fourth, it analyzes the factors that influence the probative value of blockchain evidence, including authenticity, data integrity, forensic reliability, chain of custody, expert testimony, and the connection between wallet addresses and real-world legal identity. Finally, the research formulates legal arguments concerning how blockchain transactions should be assessed in criminal proceedings to ensure both evidentiary reliability and protection of due process.

Through this methodology, the study seeks to provide a doctrinal and practical understanding of blockchain transactions as electronic evidence. The method enables the research to explain not only the legal admissibility of blockchain data, but also the conditions under which such data may possess strong evidentiary value in Indonesian criminal justice practice.

DISCUSSION

The analysis of blockchain transactions as electronic evidence in Indonesian criminal procedure law demonstrates that the evidentiary value of blockchain cannot be assessed only from its technological sophistication. Blockchain is often described as secure, transparent, decentralized, and immutable, but these characteristics do not automatically transform blockchain data into conclusive legal proof. In criminal proceedings, evidence must be evaluated through legal standards, procedural safeguards, and judicial reasoning. Therefore, the discussion of blockchain evidence requires an integrated analysis between the technological nature of blockchain records and the normative principles of criminal proof.

In the Indonesian legal system, the position of blockchain transactions as evidence must first be placed within the broader framework of electronic evidence. The Indonesian Criminal Procedure Code, or KUHAP, traditionally recognizes five forms of evidence: witness testimony, expert testimony, documents, indications, and the statement of the accused. This classical evidentiary framework was formulated before the rapid development of digital technology. Consequently, it does not expressly mention blockchain, cryptocurrency transactions, transaction hashes, digital wallets, or decentralized ledgers. However, the recognition of electronic information and electronic documents under the Electronic Information and Transactions Law has expanded the scope of legally admissible evidence in Indonesia. This expansion allows blockchain transaction data to be interpreted as electronic information or electronic documents, provided that such data are relevant, accessible, intact, and accountable in legal proceedings.

The doctrinal position of blockchain transactions can therefore be understood as part of electronic evidence. A blockchain transaction contains digital information generated, stored, transmitted, and verified through an electronic system. It records certain transactional elements, such as wallet addresses, transaction hashes, timestamps, transfer values, block numbers, and confirmation status. These elements may be legally relevant in criminal cases involving cryptocurrency fraud, ransomware, illegal investment, money laundering, terrorism financing, or concealment of criminal proceeds. In this sense, blockchain records can assist law enforcement officers in reconstructing the flow of digital assets and identifying transactional patterns connected to criminal conduct.

However, the admissibility of blockchain evidence must be distinguished from its probative strength. Admissibility refers to whether evidence is legally acceptable before the court, while probative strength refers to the extent to which such evidence can convince the judge about the existence of a legally relevant fact. This distinction is important because blockchain data may be admissible as electronic evidence, but its evidentiary weight may vary depending on authentication, integrity, relevance, forensic handling, and its connection to the accused. As emphasized in digital evidence scholarship, electronic evidence must be assessed not merely based on its existence, but also based on its

reliability, originality, and the method through which it was obtained and presented (Casey, 2011).

Blockchain transactions possess certain technical advantages compared to ordinary electronic documents. Traditional digital files can be edited, copied, deleted, or manipulated without leaving clear traces if they are not properly secured. In contrast, blockchain transactions are recorded in a distributed ledger and linked through cryptographic mechanisms. Once a transaction is validated and inserted into a block, altering the historical record becomes technically difficult because such alteration would require changing subsequent blocks and overcoming the consensus mechanism of the network. This feature supports the integrity of blockchain data and makes it valuable for evidentiary purposes (Nakamoto, 2008; Zohar, 2015).

Nevertheless, immutability must not be misunderstood. Blockchain immutability refers primarily to the technical difficulty of altering records already validated by the network. It does not automatically guarantee that the legal interpretation of the transaction is correct. A blockchain record may prove that a transaction occurred between two wallet addresses, but it does not by itself prove the legal identity of the wallet controller, the intention behind the transaction, or the criminal nature of the asset movement. This limitation is crucial because criminal liability requires proof of actus reus and mens rea, namely the prohibited act and the guilty mind. Blockchain data may help establish the occurrence of a digital transfer, but additional evidence is required to establish attribution and criminal intent.

The problem of attribution is one of the most significant challenges in the use of blockchain transactions as criminal evidence. Most public blockchain systems, including Bitcoin and Ethereum, operate through pseudonymous addresses. A wallet address does not directly reveal the name, nationality, occupation, or legal identity of its controller. Therefore, a transaction hash showing that a wallet sent or received cryptocurrency cannot automatically identify the person behind the wallet. This evidentiary gap has been widely recognized in studies on cryptocurrency-related crime, where investigators often need to combine on-chain data with off-chain information, such as exchange records, Know Your Customer data, bank records, IP logs, device forensics, and communication evidence (Meiklejohn et al., 2013; Foley et al., 2019).

This condition indicates that blockchain evidence should not be treated as self-sufficient evidence. It should be positioned as part of a broader evidentiary construction. In Indonesian criminal proceedings, this is consistent with the principle that a conviction must be based on legally valid evidence and the judge's conviction. Blockchain data may contribute to the formation of judicial conviction, but it should be supported by other forms of evidence. For example, in a cryptocurrency fraud case, blockchain data may show that victims transferred assets to a specific wallet. However, to prove that the defendant controlled the wallet, investigators may need evidence from an exchange account registered under the defendant's identity, device seizure showing wallet access, recovery phrases found in the defendant's possession, or communication records instructing victims to transfer assets to that wallet.

The evidentiary strength of blockchain transactions is therefore relational. It becomes stronger when blockchain data are supported by corroborating evidence. It becomes weaker when blockchain data stand alone without attribution to a legal subject. This is particularly relevant because blockchain transactions are technical facts, while criminal responsibility is a legal conclusion. A technical fact may show that a transfer occurred, but a legal conclusion requires a chain of reasoning connecting that transfer to the accused, the criminal event, and the required mental element. Without this connection, blockchain evidence may only establish the existence of digital movement, not criminal liability.

Authentication plays a central role in bridging technical data and legal proof. Authentication requires the party presenting evidence to show that the evidence is what it claims to be. In the context of blockchain, authentication may involve verifying transaction hashes, matching wallet addresses, confirming block height, checking timestamps, reviewing transaction status, and comparing data from different blockchain explorers or forensic tools. The purpose is to ensure that the transaction record presented in court corresponds to the actual data recorded on the blockchain network. In digital forensic practice, authentication is essential because digital evidence is easily duplicated and must be connected to a reliable source (Carrier, 2002).

In blockchain cases, authentication should not rely only on screenshots of blockchain explorers. Screenshots may be useful as preliminary documentation, but they have limited evidentiary value because they can be edited or taken out of context. Stronger authentication requires forensic reporting that explains the source of the data, the method of extraction, the tools used, the date and time of verification, and the consistency of the transaction data across verifiable sources. A transaction hash should ideally be independently verifiable by the court or by a digital forensic expert. This approach is consistent with the principle of repeatability in digital forensic analysis, where another competent examiner should be able to verify the same result using a similar method (Goodison, Davis, & Jackson, 2015).

Integrity is another important factor in determining probative value. Blockchain technology provides integrity at the network level because the ledger is cryptographically secured. However, the evidence presented in court is often not the blockchain itself, but a forensic report, transaction chart, exported file, analytical table, or expert explanation derived from blockchain data. These derivative forms of evidence must also be protected from alteration. Therefore, the integrity of blockchain evidence depends not only on the blockchain network, but also on the procedures used by investigators and experts in collecting, storing, analyzing, and presenting the data. The National Institute of Standards and Technology emphasizes that digital evidence handling requires proper identification, collection, examination, analysis, and reporting to ensure reliability (Kent et al., 2006).

The chain of custody is especially significant in this context. Chain of custody refers to the documentation of every stage of evidence handling, from discovery to presentation in court. It records who handled the evidence, when it was handled, what actions were taken, what tools were used, and how the evidence was preserved. In blockchain investigations, chain of custody may involve several stages: identifying the transaction hash, recording the wallet address, preserving the blockchain explorer result, exporting analytical data, obtaining exchange records, seizing devices, extracting wallet-related files, and preparing expert reports. Any gap in this process may create reasonable doubt regarding the reliability of the evidence.

Although blockchain records themselves may be difficult to alter, the investigative interpretation of those records is still vulnerable to error. Investigators may incorrectly associate wallet addresses, misread transaction flows, overlook mixing services, fail to distinguish custodial and non-custodial wallets, or misinterpret smart contract interactions. For example, a wallet may interact with an exchange deposit address, but that does not necessarily mean the same person controls the entire exchange wallet. Likewise, funds passing through a mixer or decentralized finance protocol may complicate the tracing process. These technical complexities demonstrate that expert interpretation is indispensable in blockchain-related criminal cases (Möser, Böhme, & Breuker, 2013).

Expert testimony has a strategic function in explaining blockchain evidence to the court. Judges and prosecutors may not possess sufficient technical knowledge to understand transaction hashes, private keys, block confirmations, wallet clustering, token transfers, or decentralized exchange mechanisms. A digital forensic expert can explain how blockchain data are generated, how transactions are verified, how tracing is conducted, and what limitations exist in the analysis. However, expert testimony must remain transparent and cautious. Experts should distinguish between facts that are technically certain and conclusions that are inferential. For example, an expert may state with high confidence that a transaction occurred at a certain time, but the conclusion that the defendant controlled the wallet may require additional supporting evidence.

This distinction prevents the overvaluation of blockchain evidence. In modern criminal justice, digital evidence often carries a perception of scientific objectivity. Courts may be tempted to give excessive weight to technical evidence because it appears neutral and precise. However, digital evidence is not free from interpretive limitations. The tools used to analyze data may have errors, the analyst may make assumptions, and the evidentiary chain may be incomplete. Therefore, courts must assess blockchain evidence critically, not mechanically. Judicial reasoning should evaluate whether the evidence is relevant, reliable, lawfully obtained, properly authenticated, and sufficiently linked to the accused (Roberts & Zuckerman, 2010).

The issue of legality in obtaining blockchain evidence also deserves attention. Public blockchain data are generally accessible because transactions can be viewed through blockchain explorers. However, many forms of supporting evidence are not publicly accessible. Exchange account records, private communications, device contents, bank data, IP logs, and identity documents require lawful acquisition procedures. If investigators obtain such evidence without proper legal authority, the admissibility or probative value of the evidence may be challenged. Therefore, the use of blockchain evidence must remain consistent with due process, privacy protection, and procedural legality. Technological usefulness cannot override procedural safeguards.

In Indonesian criminal procedure, the integration of blockchain evidence must also be understood in relation to the minimum evidentiary requirement. A judge may not convict solely on the basis of weak or isolated evidence. Blockchain records may function as documentary evidence, electronic evidence, expert-supported evidence, or a basis for indications when combined with other facts. For instance, repeated transfers from victim wallets to a wallet associated with the defendant may form a pattern. If this pattern is supported by victim testimony, exchange data, and device forensics, it may strengthen the evidentiary construction. In this way, blockchain data can contribute to the formation of indications or circumstantial evidence that supports the prosecution's argument.

The probative value of blockchain transactions also differs depending on the type of criminal case. In ransomware cases, blockchain data may be important for tracing ransom payments from victims to attacker-controlled wallets. In investment fraud cases, blockchain records may show the collection of funds from multiple victims into a central wallet. In money laundering cases, transaction tracing may show layering patterns through multiple addresses, exchanges, bridges, or mixers. In corruption or bribery cases involving digital assets, blockchain records may help identify the movement of assets if they can be linked to the parties involved. Each type of case requires a different evidentiary strategy because the legal elements to be proven are different.

In money laundering cases, for example, blockchain evidence may support the identification of placement, layering, and integration stages. However, tracing funds through blockchain alone may not be sufficient to prove that the assets are proceeds of crime. Prosecutors still need to establish the predicate crime, the knowledge or reasonable suspicion of the accused, and the purpose of concealing or disguising the origin of assets. Thus, blockchain evidence functions as a transactional map, but the legal narrative must be completed through other evidence. This confirms that blockchain analysis is a tool for proof, not a substitute for legal reasoning.

The use of blockchain evidence also raises challenges related to cross-border cooperation. Cryptocurrency transactions can move across jurisdictions quickly. Wallets may interact with exchanges located outside Indonesia, and service providers may be subject to foreign laws. This creates difficulties for investigators who need identity data, transaction records, or account information from foreign platforms. Mutual legal assistance, international cooperation, and coordination with financial intelligence units become important in such cases. Without access

to off-chain records held by foreign entities, attribution may remain incomplete even when the on-chain transaction trail is clear (FATF, 2021).

Another challenge concerns the development of privacy-enhancing technologies. Some cryptocurrencies and blockchain tools are designed to obscure transaction details. Privacy coins, mixers, tumblers, chain-hopping techniques, cross-chain bridges, and decentralized finance protocols can make tracing more difficult. These technologies do not necessarily make investigation impossible, but they increase the complexity of analysis and require higher forensic competence. Courts must be aware that the absence of direct traceability does not automatically negate criminal conduct, but it may affect the strength of proof. Conversely, prosecutors must avoid presenting speculative tracing conclusions when the analytical basis is weak.

The Indonesian legal framework currently provides a general basis for admitting electronic evidence, but it does not yet provide detailed technical standards for blockchain evidence. This creates uncertainty for law enforcement officers, prosecutors, judges, and digital forensic experts. General recognition of electronic evidence is useful, but blockchain transactions have distinctive characteristics that require more specific guidance. Standard operating procedures should address how blockchain data are identified, preserved, verified, analyzed, and reported. They should also regulate the minimum content of blockchain forensic reports, including transaction hashes, wallet addresses, analytical tools, verification methods, assumptions, limitations, and supporting evidence.

The need for standardization is consistent with international digital forensic principles. Digital evidence should be handled in a manner that preserves integrity, enables verification, and supports reproducibility. Standards such as ISO/IEC 27037 emphasize identification, collection, acquisition, and preservation of digital evidence. Although such standards are not designed specifically for blockchain, their principles can be adapted to blockchain investigations. Indonesian institutions may develop specific forensic guidelines for blockchain evidence by combining general digital forensic standards with the unique requirements of decentralized ledger analysis.

From a practical perspective, investigators should avoid treating blockchain evidence as merely a printout of transaction history. A transaction record should be accompanied by a clear explanation of how it was obtained and what it proves. Prosecutors should also present blockchain evidence in a structured manner. Rather than overwhelming the court with technical charts, they should explain the legal relevance of each transaction. The presentation should answer several key questions: What transaction occurred? When did it occur? Which wallets were involved? How is the wallet connected to the defendant? How is the transaction connected to the criminal act? What supporting evidence confirms the interpretation? These questions help transform technical data into legally meaningful evidence.

Judges also need adequate digital literacy to evaluate blockchain evidence. They do not need to become blockchain engineers, but they must understand the basic distinction between transaction existence, wallet control, identity attribution, and criminal responsibility. Judicial education on digital evidence is therefore important. Without such understanding, courts may either reject blockchain evidence due to unfamiliarity or accept it uncritically due to excessive trust in technology. Both approaches are problematic. A balanced approach requires legal actors to appreciate the evidentiary potential of blockchain while remaining aware of its limitations.

The defense also has an important role in maintaining fairness. Defendants must be given the opportunity to challenge the validity of blockchain evidence. They may question the method of data extraction, the reliability of forensic tools, the competence of the expert, the completeness of the chain of custody, or the inference connecting the wallet to the accused. This adversarial testing is important because it prevents one-sided reliance on technical evidence. In criminal proceedings, the right to challenge evidence is part of the broader protection of due process and fair trial principles.

Blockchain evidence can also be understood as a hybrid evidentiary object. It may function as electronic information under electronic transaction law, as documentary evidence when presented in a forensic report, as expert-supported evidence when interpreted by a digital forensic expert, and as circumstantial evidence when combined with other facts. This hybrid character requires flexible doctrinal interpretation. The court should not force blockchain evidence into a rigid category without considering its actual function in the case. What matters is not merely the label of the evidence, but whether it can assist the court in establishing legally relevant facts through lawful and reliable means.

The findings of this study support the argument that blockchain transactions have significant evidentiary potential but conditional probative value. Their evidentiary strength is high in proving the existence, time, and technical pathway of a digital transaction. Their evidentiary strength is moderate when used to show transaction patterns or asset flows. Their evidentiary strength becomes limited when used to prove personal identity, intent, or criminal responsibility without supporting evidence. Therefore, the court must evaluate blockchain evidence based on the specific fact it is intended to prove.

This discussion also shows that blockchain evidence should be assessed through four main parameters. First, authenticity: whether the transaction data genuinely originate from the relevant blockchain network. Second, integrity: whether the data and their forensic derivatives have been protected from alteration. Third, attribution: whether the wallet or transaction can be linked to a legal subject. Fourth, relevance: whether the transaction is connected to the alleged criminal act. These parameters can help law enforcement officers and courts avoid both underestimating and overestimating blockchain evidence.

In conclusion, blockchain transactions may occupy an important position as electronic evidence in Indonesian criminal procedure law. Their legal position is supported by the recognition of electronic information and electronic documents, while their technical structure provides strong potential for verifying digital transactions. However, their evidentiary strength is not absolute. Blockchain evidence must be authenticated, preserved, interpreted, and connected to other evidence. The most persuasive use of blockchain evidence occurs when on-chain data are supported by off-chain evidence, expert testimony, and a clear chain of custody. Therefore, the future integration of blockchain evidence into Indonesian criminal justice requires clearer forensic standards, stronger institutional capacity, and careful judicial reasoning. Only through this integrated approach can blockchain transactions contribute effectively to criminal proof while preserving fairness, legality, and due process.

CONCLUSIONS AND RECOMMENDATIONS

This study concludes that blockchain transactions may be legally positioned as electronic evidence within the Indonesian criminal procedure law system. Although the Indonesian Criminal Procedure Code does not expressly regulate blockchain, the recognition of electronic information and electronic documents under the Electronic Information and Transactions Law provides a normative basis for admitting blockchain transaction records in criminal proceedings. In this context, blockchain data may be understood as electronic information that records digital transaction elements such as wallet addresses, transaction hashes, timestamps, block numbers, transfer values, and confirmation status. These elements may be relevant in criminal cases involving cryptocurrency fraud, ransomware, money laundering, illegal investment, and other cyber-enabled crimes.

However, the evidentiary strength of blockchain transactions is not absolute. Blockchain technology offers strong technical reliability because its records are cryptographically secured, distributed, time-stamped, and resistant to unauthorized alteration. These characteristics make blockchain evidence particularly useful in proving the existence, timing, and technical pathway of a digital transaction. Nevertheless, blockchain evidence does not automatically prove the real-world identity of the wallet controller, the intention behind the transaction, or the criminal responsibility of the accused. Therefore, blockchain transactions must not be treated as self-sufficient or conclusive evidence. Their probative value depends on authentication, data integrity, forensic reliability, chain of custody, expert interpretation, and their correlation with other legally admissible evidence.

The study also finds that the strongest evidentiary value of blockchain transactions emerges when on-chain data are supported by off-chain evidence. Blockchain records may show that a transaction occurred, but attribution to a legal subject requires corroboration through exchange account records, Know Your Customer data, device forensics, banking information, communication records, IP logs, or other supporting evidence. This confirms that blockchain evidence should be placed within a broader evidentiary construction. It functions

not merely as a technical record, but as part of a legal reasoning process that connects digital transactions to criminal acts, legal identity, and the elements of criminal liability.

Based on these conclusions, several recommendations can be proposed. First, law enforcement agencies should develop standardized procedures for handling blockchain evidence. These procedures should regulate the identification, collection, verification, preservation, analysis, and reporting of blockchain transaction data. Investigators should not rely solely on screenshots from blockchain explorers because such documentation may be vulnerable to manipulation and may not sufficiently explain the source, method, and reliability of the evidence. A proper blockchain forensic report should include transaction hashes, wallet addresses, block height, timestamps, analytical tools used, verification methods, assumptions, limitations, and supporting off-chain evidence.

Second, prosecutors should present blockchain evidence through a clear legal narrative. The presentation of blockchain data should not merely display technical transaction charts, but must explain the relevance of each transaction to the elements of the alleged crime. Prosecutors should be able to answer what transaction occurred, when it occurred, which wallets were involved, how the wallet is connected to the defendant, and how the transaction supports the criminal charge. This approach is necessary to transform technical data into legally meaningful evidence.

Third, judges should assess blockchain evidence through balanced judicial reasoning. Courts should neither reject blockchain evidence merely because it is technologically complex nor accept it uncritically because it appears scientifically reliable. Judicial assessment should focus on four main parameters: authenticity, integrity, attribution, and relevance. Judges should also rely on expert testimony when the technical meaning of blockchain transactions requires specialized explanation. At the same time, the defense must be given a fair opportunity to challenge the reliability of tools, methods, expert conclusions, and the chain of custody.

Fourth, policymakers and criminal justice institutions should formulate specific guidelines for blockchain forensic practice in Indonesia. These guidelines should be aligned with general digital forensic standards, electronic evidence principles, privacy protection, due process, and international cooperation mechanisms. Since cryptocurrency transactions often involve foreign exchanges, cross-border wallets, decentralized finance platforms, and privacy-enhancing technologies, Indonesian law enforcement requires stronger institutional capacity and cooperation with relevant domestic and international authorities. Through these measures, blockchain transactions can be used effectively as evidence while still protecting legality, fairness, and the rights of the accused.

ADVACED RESEARCH

Further research is recommended to investigate the evidentiary challenges posed by emerging privacy-enhancing technologies, such as privacy coins, mixers, and decentralized finance (DeFi) protocols, within the Indonesian criminal justice framework

REFERENCES

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics, 13*(17), Article 3568. https://doi.org/10.3390/electronics13173568.

Azzahra, N. R. G. (2024). Model investasi cryptocurrency dalam upaya pencegahan tindak pidana pencucian uang. *Mahkamah: Jurnal Riset Ilmu Hukum, 1*(4), 181–192. https://doi.org/10.62383/mahkamah.v1i4.208.

Bonomi, S., Casini, M., & Ciccotelli, C. (2020). B-CoC: A blockchain-based chain of custody for evidences management in digital forensics. *OpenAccess Series in Informatics, 71*, Article 12. https://doi.org/10.4230/OASIcs.Tokenomics.2019.12.

Carrier, B. (2002). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence, 1*(4), 1–12.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet* (3rd ed.). Academic Press.

Choo, K.-K. R. (2015). Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In D. Lee Kuo Chuen (Ed.), *Handbook of digital currency* (pp. 283–307). Academic Press. https://doi.org/10.1016/B978-0-12-802117-0.00015-1.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review, 2*, 6–19.

Drescher, D. (2017). *Blockchain basics: A non-technical introduction in 25 steps*. Apress. https://doi.org/10.1007/978-1-4842-2604-9.

Europol. (2022). *Cryptocurrencies: Tracing the evolution of criminal finances*. European Union Agency for Law Enforcement Cooperation.

Financial Action Task Force. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies, 32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015.

Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C., & Pesch, P. (2019). Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation, 33*, Article 200902. https://doi.org/10.1016/j.fsidi.2019.200902.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence*. RAND Corporation. https://doi.org/10.7249/RR890.

Ilmi, M., & Lubis, P. M. L. (2025). Tantangan pembuktian tindak pidana pencucian uang melalui cryptocurrency dalam sistem hukum pidana Indonesia. *El-Iqthisady: Jurnal Hukum Ekonomi Syariah, 7*(1), 448–455.

International Organization for Standardization. (2012). *ISO/IEC 27037:2012: Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the 2013 Internet Measurement Conference* (pp. 127–140). Association for Computing Machinery. https://doi.org/10.1145/2504730.2504747.

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In *2013 APWG eCrime Researchers Summit* (pp. 1–14). IEEE. https://doi.org/10.1109/eCRS.2013.6805780.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. X. Olleros & M. Zhegu (Eds.), *Research handbook on digital transformations* (pp. 225–253). Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019.

Republik Indonesia. (1981). *Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Hukum Acara Pidana*.

Republik Indonesia. (2008). *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Republik Indonesia. (2024). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Roberts, P., & Zuckerman, A. (2010). *Criminal evidence* (2nd ed.). Oxford University Press.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.

Zohar, A. (2015). Bitcoin: Under the hood. *Communications of the ACM, 58*(9), 104–113. https://doi.org/10.1145/2701411.