UDC 343.14:004.438
DOI: 10.63341/naia-herald/3.2026.42

ISSN 2410-3594
E-ISSN 2786-7382

Materials and conclusions of a blockchain systems analyst: Issues of admissibility and the application of law in criminal proceedings

Dmytro Ovsianiuk*
PhD in Law
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-1846-4167

Andrii Okushko
PhD in Law
Cyber Police Department of the National Police of Ukraine
02093, 19 Boryspilska Str., Kyiv, Ukraine
https://orcid.org/0009-0003-3627-2489

Yevhenii Panchenko
International Police Cooperation Department of the National Police of Ukraine
01024, 1 Akademik Bogomolets Str., Kyiv, Ukraine
https://orcid.org/0000-0001-5755-7457

■ **Abstract.** This study aimed to substantiate the legal nature of the materials and conclusions of a blockchain systems analyst, establish criteria for their procedural assessment, and synthesise approaches to use in criminal proceedings. The methodological design combined a review of scholarly literature with formal legal and comparative legal methods, case-law analysis, and conceptual modelling. The study substantiates the legal nature of materials and conclusions prepared by a blockchain systems analyst as independent results of applying specialised knowledge, generated through the professional analytical processing of distributed-ledger data. Distinctions between the analyst's materials and conclusions were identified in terms of their legal nature, content, functional purpose, and role in the evidential process; both were also differentiated from a forensic expert's opinion and a specialist's consultation. It was established that the procedural assessment of an analyst's materials and conclusions should be based on the classical criteria of relevance, admissibility, and reliability, taking account of the particularities of their formation rather than the technical characteristics of blockchain technology. Relevance is determined by the connection between the results of blockchain analysis and the facts to be proved; admissibility, by the lawfulness of obtaining the source data, the transparency of the analytical methodology, and the possibility of its independent verification; and reliability, by the reproducibility of results, the verifiability of heuristic models, algorithmic transparency, and the scientific soundness of the conclusions drawn. A conceptual model for the comprehensive procedural assessment of a blockchain systems analyst's materials and conclusions was developed. It comprises three interrelated stages: assessment of the source of evidential information, assessment of the blockchain-analysis methodology, and assessment of the results of analytical activity. The findings may be used by investigators, prosecutors, defence counsel, forensic experts, and blockchain systems analysts when assessing blockchain-analysis materials,

■ **Suggested Citation:**
Ovsianiuk, D., Okushko, A., & Panchenko, Ye. (2026). Materials and conclusions of a blockchain systems analyst: Issues of admissibility and the application of law in criminal proceedings. *Scientific Journal of the National Academy of Internal Affairs,* 31(3), 42-58. doi: 10.63341/naia-herald/3.2026.42.

■ *Corresponding author (*dmtr.ovsianiuk@hotmail.com*)

■ Received: 04.06.2026; Revised: 05.09.2026; Accepted: 29.09.2026; Published: 02.10.2026



Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

determining their evidential value, and ensuring consistent approaches to the use of such evidential information in criminal proceedings

■ **Keywords:** criminal proceedings; digital evidence; evidential information; procedural assessment; virtual assets

■ Introduction

The development of blockchain technology and the growing use of crypto-asset transactions have led to the use in criminal proceedings of new sources of digital information generated from distributedledger data. In the investigation of criminal offences, materials and conclusions prepared by blockchain systems analysts are used following the analysis of transactions and relationships between crypto-assets. At the same time, the criminal procedure legislation of most states does not define their procedural status or the procedures for obtaining, verifying, and assessing them. This creates uncertainty regarding their admissibility and evidential value. The limited treatment of these issues in procedural law necessitates comprehensive scholarly research into the legal foundations for using the materials and conclusions of blockchain systems analysts as a source of evidential information.

The expanding use of virtual assets and blockchain technologies in various areas of social relations has given rise to a distinct field of research concerning their application in the detection, investigation, and proof of criminal offences. The first group of scholarly studies comprises studies on forensic support for the investigation of criminal offences involving virtual assets and blockchain technologies. V.M. Shevchuk (2026) examined blockchain as one of the promising tools for providing forensic support to law-enforcement activities and demonstrated that its use creates additional opportunities for recording, preserving, and verifying digital information. The author associated the practical value of this technology not only with ensuring data integrity, but also with expanding the possibilities for documenting evidential information under martial law and amid the growing number of cyber threats. The practical application of blockchain technologies was further considered by D. Ovsianiuk *et al.* (2025a). Drawing on international experience, the authors showed that the effectiveness of investigating criminal offences involving virtual assets depends on the use of specialised tools for analysing blockchain transactions, the capacity for international information exchange, and the application of contemporary forensic methodologies. Summarising developments in this field, K.V. Martynenko (2026) drew attention to trends in research on the investigation of criminal offences involving virtual assets. The analysis showed that the most extensively developed issues remained the identification and seizure of crypto-assets, international cooperation between competent authorities, and the use of specialised software in investigations.

The proliferation of digital assets in criminal proceedings has prompted another strand of research concerned with their legal nature, their place in the evidential framework, and the criteria for their procedural assessment. Unlike forensic studies focusing on the detection and analysis of digital assets, scholars working in this area have concentrated on identifying procedural mechanisms for using such information in criminal proceedings and defining the conditions under which it may acquire evidential value. In this context, O.P. Metelev (2025) proposed an approach whereby virtual assets should be assessed not only as a new category of digital objects, but also as a source of evidential information whose use requires due regard to the particularities of proof in criminal proceedings. The author argued that the evidential value of crypto-assets is determined not solely by their technological properties, but also by the lawfulness of obtaining the relevant information, the possibility of verifying it, and its proper procedural assessment. This approach was further developed in the study of O.S. Starenkyi (2026), which focused on the use of virtual assets in proof in criminal proceedings. The author concluded that applying traditional rules of evidential assessment to digital assets involves a number of difficulties arising from insufficient legal certainty regarding their procedural status. At the same time, the study demonstrated that resolving this issue requires clear criteria for the admissibility of such information, capable of ensuring consistent approaches to its assessment in criminal proceedings. Issues concerning the procedural assessment of digital evidence were further explored by V.V. Romaniuk & S.Ye. Ablamskyi (2024). Having synthesised the provisions of criminal procedure legislation and contemporary judicial practice, the authors concluded that the admissibility of digital evidence is determined not by its electronic form, but by compliance with general procedural requirements governing the collection, recording, examination, and assessment of evidential information.

A separate strand of research has developed around the use of blockchain technology as a means of ensuring the integrity of digital evidence and improving forensic procedures for handling it. S.M. Shinde & V.R. Gurrala (2023) examined the issue of ensuring the integrity of digital evidential information in cloud forensics. The authors demonstrated that

integrating blockchain technology with digital-evidence storage systems enabled changes to information to be monitored, improved its protection, and provided additional safeguards for confirming the authenticity of digital data. Blockchain was therefore considered primarily as a technological tool for maintaining the integrity of digital information in forensic practice. The development of this line of research can also be seen in the study of I. Lavín & D.R. Llanos (2026), who linked the use of blockchain technology to ensuring continuity in the chain of custody of digital evidence. The solutions proposed by the authors were based on the possibility of recording every procedural action involving digital information. This provides additional safeguards for transparency in handling evidence and simplifies verification of its processing history.

An analysis of the scholarly literature showed that existing studies address the use of blockchain technologies and virtual assets in criminal proceedings, including forensic aspects of examining digital assets, ensuring the integrity of digital evidence, and determining its procedural status. However, comprehensive studies of the legal nature of the materials and conclusions prepared by blockchain systems analysts as a result of applying specialised knowledge in criminal proceedings are virtually absent. The criteria for their procedural assessment and the particularities of their use in the practice of applying the law also remain insufficiently explored. The study aimed to determine the legal nature of the materials and conclusions prepared by a blockchain systems analyst, substantiate criteria for their admissibility in criminal proceedings, and systematise approaches to their use in the application of the law. Its objectives were to clarify the legal nature of such materials and conclusions and determine their place within the evidential framework of criminal proceedings; examine the criteria for assessing their admissibility, relevance, and reliability, as well as the procedural features of their use as evidential information; and analyse the practice of US courts in using the materials and conclusions of blockchain systems analysts in criminal proceedings and synthesise the approaches developed for their procedural assessment.

Materials and Methods

The study is a theoretical legal investigation incorporating case-law analysis and conceptual modelling. Its methodological design combined a review of scholarly literature with formal legal and comparative legal methods, case-law analysis, and conceptual modelling. The literature review was used to systematise doctrinal approaches to defining the legal nature of the materials and conclusions prepared by blockchain systems analysts and to establish their place within the evidential process in criminal proceedings. The comparative legal method was used to compare the materials and conclusions of blockchain systems analysts with comparable outputs arising from the application of specialised knowledge in criminal proceedings, particularly a forensic expert's opinion and a specialist's consultation or explanation. The comparison was conducted according to the criteria of legal nature, the person responsible for preparing the material, the subject matter of the examination, the content of the result obtained, and its functional purpose in criminal proceedings. The theoretical basis for the comparative analysis comprised the scholarly studies of T.D. Albright (2023) and A.M. Ayub *et al.* (2025), which address the use of specialised knowledge, digital evidence, and the results of blockchain analysis in criminal proceedings.

The formal legal method was applied to examine the regulatory foundations for using the materials and conclusions of blockchain systems analysts in criminal proceedings. At the international level, Articles 14, 16, 18, and 19 of the Convention on Cybercrime[1], which govern procedural mechanisms for obtaining, preserving, seizing, and disclosing computer data, were analysed. Articles 7-9 of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence[2], concerning international access to electronic evidence and cooperation between competent authorities and service providers, were also examined. To assess whether blockchain-analysis materials comply with international standards for the use of digital evidential information, the provisions of the Financial Action Task Force (2021), which establish approaches to obtaining, documenting, and using electronic evidence in cross-border criminal investigations, were also analysed. At the national level, the study was based on Articles 71, 84-86, 94, and 101 of the Criminal Procedure Code of Ukraine[3], which govern the use of specialised knowledge, define the concept of evidence, establish criteria for its relevance, admissibility, and reliability, regulate the assessment of evidence, and determine the legal nature of a forensic expert's opinion. The analysis of these provisions aimed to establish the applicability of general procedural rules of proof to the materials and conclusions of blockchain systems analysts and to

[1] Convention on Cybercrime. (2001, November). Retrieved from https://www.coe.int/en/web/cybercrime/convention-on-cybercrime.
[2] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. (2022, May). Retrieved from https://www.coe.int/en/web/cybercrime/second-additional-protocol.
[3] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17?lang=en&utm#Text.

determine their place within the evidential framework of criminal proceedings. The conceptual modelling method was used to develop a model for the comprehensive procedural assessment of the materials and conclusions of blockchain systems analysts. The model was constructed by synthesising the findings of the literature review and international and national legal instruments. The modelling process identified the structural elements of procedural assessment, including the stage of comprehensive assessment, the subject matter of assessment, the content of procedural verification, and the assessment outcome.

The case-law analysis method was used to examine approaches to the use of blockchainanalysis materials in criminal proceedings. The empirical basis for this stage of the study comprised the following US court decisions: Case of the United States v. Gratkowski[1], Case of the United States v. Harmon[2], and Case of the United States v. Sterlingov[3]. Ukrainian court decisions were also analysed, namely the Ruling of the Appeal Chamber of the High Anti-Corruption Court in Case No. 991/10335/23[4] and the Ruling of the Shevchenkivskyi District Court of Kyiv in Case No. 761/11447/24[5]. The US cases were selected because they contain reasoned judicial assessments of blockchain analysis, including its use to reconstruct the movement of digital assets, establish links between crypto-addresses, and assess the analytical methods employed. The Ukrainian cases were incorporated into the empirical basis in order to examine the various national methods of assessing information about virtual assets, crypto-wallets, and transactions, as well as the evidential value of such information in criminal proceedings. The application of US case law was purely comparative and did not involve the transfer of any US procedural standards into Ukrainian criminal procedure. It enabled a comparison between the conceptual model developed in this study and the ways in which blockchain analysis is treated in another legal system, while the Ukrainian court decisions were used to check whether the model was compatible with the nation's own procedural approaches.

■ Results

Legal nature of the materials and conclusions of a blockchain systems analyst in criminal procedure

The development of distributed ledgers and the increasing use of transactions involving crypto-assets have changed both the methods employed for recording digital information and the way in which this information is used in criminal investigations. When blockchain technology was first being developed, it was mainly seen as a means of ensuring that data could not be altered. But since large amounts of transaction data have been accumulated, this has given rise to a particular kind of professional activity concerned with examining the digital traces left in distributed ledgers. As a result, the aspect of interest in legal proceedings is not the blockchain entries themselves, which are publicly accessible and can be checked by any member of the network, but rather the outcomes of the specialised analytical work carried out on them. This type of analysis enables the reconstruction of the movement of digital assets, the identification of links between addresses, the determination of the nature of the financial transactions, and the drawing of conclusions about circumstances that may be pertinent to criminal proceedings (Wu & Zheng, 2020; Watters, 2023).

An examination of the various scholarly methods shows that legal doctrine is slowly becoming more distinct between the notions of "blockchain data", "blockchain evidence", and "blockchainanalysis materials", even though their exact meanings have still not been uniformly established (Harris, 2023; Chen *et al.*, 2024). It is still generally the case that evidential value is linked to the distributed-ledger entries themselves. Yet this view does not take into account the fact that blockchain records only contain information regarding transactions that have already taken place, while determining their legally relevant significance requires specialised knowledge, analytical algorithms, and a professional interpretation of the results. Because of this, it is not the individual blockchain entries that have procedural importance, but rather the materials and conclusions produced by a blockchain systems analyst as a result of a thorough analysis of the digital data.

Even though there has been an increasing amount of research into the analytical examination of blockchain data, legal scholarship has not arrived at a consensus regarding the term for the professional who carries out this type of work. Different scholarly publications refer to this person as a specialist in blockchain data analysis, a researcher of digital transactions, a specialist in forensic blockchain analysis, or a specialist in investigating crypto-asset transactions

[1] Case of the United States v. Gratkowski. (2020, June). Retrieved from https://www.govinfo.gov/app/details/USCOURTS-ca5-19-50492.
[2] Case of the United States v. Harmon. (2020, July). Retrieved from https://case-law.vlex.com/vid/united-states-v-harmon-893236324.
[3] Case of the United States v. Sterlingov. (2024, February). Retrieved from https://caselaw.findlaw.com/court/us-dis-crt-dis-col/115886148.html.
[4] Ruling of the Appeal Chamber of the High Anti-Corruption Court in Case No. 991/10335/23. (2024, October). Retrieved from https://opendatabot.ua/court/122788762-d3bb098fe38ee6185f61abea1e44ec47.
[5] Ruling of the Shevchenkivskyi District Court of Kyiv in Case No. 761/11447/24. (2024, April). Retrieved from https://zakononline.ua/court-decisions/show/118588220.

(Pasupuleti, 2024; Pérez *et al.*, 2025). No matter what terms are employed, the essence of this professional activity is unchanged: it involves examining data from a distributed ledger using special methods for analysing digital transactions. This analysis leads to the conclusion that the duties of such a specialist do not stop at the technical processing of information. They also include setting up connections between digital assets, reconstructing the paths that these assets have taken, identifying transaction patterns, interpreting the results obtained, and reaching conclusions about circumstances which might be of legal significance in criminal proceedings. On this basis, a blockchain systems analyst should be regarded as a specialist who uses specialised knowledge, analytical methods, and dedicated software to carry out a thorough examination of distributed-ledger data, to identify the informational links between digital objects, and to prepare the materials and conclusions for use in establishing circumstances that are legally relevant in criminal proceedings.

The materials prepared by a blockchain systems analyst represent an independent outcome of intellectual and analytical work. They are based on the original information found in a distributed ledger and also include the results of its systematisation, classification, visualisation, and interpretation. Different from the information which is directly stored in the blockchain, these materials are the result of specialised analytical techniques that enable the detection of hidden connections between digital assets, crypto-wallet addresses, the temporal features of transactions, and other information elements (Ovsianiuk *et al.*, 2025b). Hence, they must not be seen as a simple reproduction of blockchain data, since they include extra informational value that has been generated through professional analytical processing.

Blockchain analysis does not generate any new digital evidence and does not change the content of the information stored in a distributed ledger. Instead, its aim is to organise, compare, and interpret large amounts of transaction data so as to identify legally relevant connections between digital assets, crypto-wallet addresses, and other informational objects. The materials and conclusions produced by a blockchain systems analyst are therefore independent outcomes of professional analytical work. They are not simply a direct reflection of the entries in the blockchain, since they result from the application of specialised knowledge, analytical techniques, and professional judgement to the digital data in question. It is this which gives them independent value in legal proceedings and means that their procedural aspects must be examined separately from the features of blockchain technology. This way of proceeding is in line with trends in digital justice, where blockchain is used not only as a technology for ensuring the integrity of information but also as a means of producing analytical materials that have evidential importance for the application of the law (Alyas *et al.*, 2025; Ardian *et al.*, 2025).

At the same time, the materials and the conclusions of a blockchain systems analyst should not be considered as equivalent products of professional activity. They differ from each other both in terms of content and in their functional role within the evidential process. The materials give an account of the course and the results of the analysis carried out, comprising analytical reports, diagrams showing the movement of digital assets, tables of transactions, the results of address clustering, graphical models of the links between crypto-wallets, the temporal features of the transactions, and other information derived from the examination of distributed-ledger data (Fahmideh *et al.*, 2023). Their main function is to establish and document the informational links and to allow the results of the analysis to be verified. The conclusion of a blockchain systems analyst has a different legal status. It is not merely a summary or a visual representation of the data collected, but the outcome of a professional assessment of the facts as established, using specialised knowledge and analytical techniques. It is in the conclusion that the information obtained is interpreted, the causal relationships between the digital objects under investigation are proved, and general findings are set out regarding the routes by which digital assets have been transferred, the nature of the interactions between crypto-addresses, and other circumstances which may be relevant to criminal proceedings. The distinction proposed allows the materials and the conclusions of a blockchain systems analyst to be seen as closely related yet separate outputs of analytical work. While the materials mainly serve an informative and documentary purpose, the conclusion offers an analytical synthesis of the findings and their professional interpretation. This relationship enables the legal character of both to be described not as separate items of blockchain data, but as the result of applying specialised knowledge to the information contained in a distributed ledger.

To ascertain the legal status of the materials and conclusions produced by a blockchain systems analyst, it is necessary to differentiate them from the results obtained when specialised knowledge is applied in the course of criminal proceedings. Even though all these outputs are aimed at establishing circumstances pertinent to criminal proceedings, the materials and conclusions of a blockchain systems analyst are different from a forensic expert's opinion or a specialist's consultation or explanation in respect of the way in which they are prepared, the kind of specialised knowledge used, the content of the results

arrived at, and their role in the evidential process. A thorough comparative analysis is therefore required in order to establish their legal nature. The findings of this analysis are given in Table 1.

Table 1. Comparative characteristics of the results of applying specialised knowledge in criminal proceedings

Comparison criterion	Materials of a blockchain systems analyst	Conclusion of a blockchain systems analyst	Forensic expert's opinion	Specialist's consultation or explanation
Legal nature	Result of professional analytical activity documenting the findings of an examination of distributed-ledger data	Result of the professional assessment and interpretation of the findings of an analysis of distributed-ledger data	Result of an expert examination carried out through the application of specialised knowledge	Result of applying specialised knowledge to provide technical, scientific, or advisory assistance in criminal proceedings
Prepared by	Blockchain systems analyst	Blockchain systems analyst	Forensic expert	Specialist
Subject matter of examination	Distributed-ledger data, digital transactions, crypto-assets, crypto-wallet addresses, and digital links	Results of analysing digital transactions and the patterns and links established between them	Material, digital, or other objects whose examination requires specialised knowledge	Circumstances requiring specialised knowledge to explain them or provide technical support for procedural actions
Content of the result	Analytical reports, transaction tables, address-clustering results, graphical diagrams of digital-asset movements, visualisations of network links, and other outputs of analytical processing	A synthesis of examination results, interpretation of the facts established, substantiation of relationships between digital objects, and formulated analytical conclusions	Answers to the questions posed, substantiated by the results of the expert examination performed	Oral or written explanations, recommendations, and technical consultations enabling the use of specialised knowledge
Functional purpose	Recording, systematising, and documenting the results of blockchain-data analysis for subsequent use in criminal proceedings	Providing a professional assessment of the facts established and explaining their legally significant relationships	Providing a substantiated forensic expert's opinion on circumstances requiring specialised knowledge	Facilitating procedural actions and clarifying issues requiring specialised knowledge

Source: compiled based on T.D. Albright (2023), A.M. Ayub *et al.* (2025)

What the comparison shows is that the findings and conclusions of a blockchain systems analyst belong to a distinct category of results obtained as a result of the application of specialised knowledge and cannot be entirely included within any of the conventional institutions of criminal procedure. The way in which their studies differ from that of a forensic expert is not merely because it does not result from a formal expert examination, but primarily due to the nature of the analytical work involved. This involves processing large amounts of distributed-ledger data, detecting hidden links between pieces of information, and then interpreting them in a professional manner. At the same time, it is different from a specialist's consultation or explanation in the extent of the analytical processing and in the fact that it focuses on producing a coherent set of findings rather than just assisting with individual procedural steps.

Given what has been said above, the position that the materials and conclusions of a blockchain systems analyst should have within the evidential framework of criminal proceedings must be based on their informational and cognitive purpose. On their own, they do not prove legal facts nor do they determine their evidential value. Yet they do allow for the gathering, organisation, and professional interpretation of information which may either confirm or disprove the circumstances that are within the scope of proof. The informational value of such materials consists not just in recording individual transactions or the technical features of how a blockchain operates, but mainly in the ability to establish connections between digital assets, crypto-addresses, the temporal aspects of transactions, the behavioural patterns of the people who carry out the transactions, and other circumstances that cannot be seen from the original data of a distributed ledger alone. It is precisely their ability to build a coherent informational model of the events under investigation that gives them a stand-alone importance within the structure of criminal procedural proof and sets them apart from other outcomes of the application of specialised knowledge.

Admissibility of the materials and conclusions of a blockchain systems analyst as evidential information

The fact that the materials and conclusions of a blockchain systems analyst cannot be judged merely on the technical features of blockchain technology should be obvious. While the immutability of entries in a distributed ledger, the cryptographic protection of the information, and the decentralised storage of data describe how digital data is created, they do not determine the evidence value of that data in criminal proceedings. Since the analyst's materials and conclusions are the result of specialised knowledge being applied to the information found in the blockchain, their procedural assessment must follow the general

rules relating to proof in criminal cases rather than the technical features of the information system.

The conclusion is in line with the international standards relating to electronic evidential information. Specifically, Articles 14, 16, 18 and 19 of the Convention on Cybercrime[1] set out the procedural procedures for obtaining, preserving and seizing computer data, yet they do not include any special rules for evaluating different kinds of digital information. The same approach is taken in Articles 7-9 of the Second Additional Protocol to the Convention on Cybercrime concerning Enhanced Co-operation and the Disclosure of Electronic Evidence[2], since these Articles regulate international access to electronic evidence and cooperation between the competent authorities and service providers without changing the general procedural criteria for assessing it. International legal regulation thus starts from the idea that the way in which electronic information is obtained does not affect the general requirements applicable to its evidential value.

The same approach is taken in Ukraine's criminal procedure law. Articles 84-86 of the Criminal Procedure Code of Ukraine[3] set out what constitutes evidence and determine its relevance and admissibility without providing for a special procedural regime regarding information obtained through blockchain technologies. Article 94 of the Criminal Procedure Code of Ukraine lays down general rules for evaluating any evidence on the grounds of its relevance, admissibility, reliability and sufficiency when taken as a whole. The use of specialist knowledge is regulated by Article 71 of the Criminal Procedure Code of Ukraine, which deals with specialists, and by Article 101, which concerns the forensic expert's opinion. These provisions form the basis for deciding where the materials and conclusions of blockchain systems analysts fit within the evidential framework of criminal proceedings. The analysis leads to the conclusion that their procedural evaluation should involve modifying the traditional criteria of relevance, admissibility and reliability to take account of the particular features of how they are produced. Blockchain analysis does not give rise to a separate kind of procedural evidence and does not call for a distinct set of assessment criteria. What is specific about it is the combination of the original distributed-ledger data, the specialised methods of analytical processing and the professional interpretation of the results obtained. Because of this composite character, the traditional evidential criteria must be clarified in relation to the materials and conclusions of blockchain systems analysts, not their regulatory basis being altered.

The fact that the materials and conclusions of a blockchain systems analyst are relevant does not depend on the fact that they are based on data from a distributed ledger, but rather on their ability to confirm or disprove the circumstances that are within the scope of what must be proven in a particular criminal case (Tsymbaliuk, 2025). From this point of view, information about transactions, crypto-wallet addresses, or the routes taken by crypto-assets has no standalone evidential value. Such value only appears when an objective link has been made between the results of the blockchain analysis and legally relevant facts which have to be proven. Hence, the criterion of relevance should not be seen as simply the presence of digital information in a distributed ledger, but rather as the capacity of that information to confirm specific elements of the subject matter of proof.

This method is in line with the general principles of proof in criminal proceedings, according to which only evidence that is either directly or indirectly connected with the facts of the case is considered to be relevant (Articles 84 and 85 of the Criminal Procedure Code of Ukraine). The same kind of reasoning can be found in the Convention on Cybercrime[4], where Articles 14, 16, 18 and 19 set out the procedural rules for obtaining and preserving computer data without attributing to it any predetermined evidential value. This shows that the international standards also require electronic information to be evaluated on the basis of its connection with the subject matter of the proof, and not according to the way in which it was created or stored.

The particular value of the materials and conclusions produced by a blockchain systems analyst stems from the fact that their informational worth does not come from looking at individual blockchain entries, but rather from the results of a thorough analytical analysis (Mollajafari & Bechkoum, 2023). It is only through the analytical identification of the connections between transactions, crypto-addresses, digital assets, the temporal features of transactions, and other information elements that it becomes possible to link the findings to the subject matter of the proof. Hence, when assessing the relevance of such materials, it is not adequate to examine each distributedledger entry on its own, but rather the evidential value of the analytical model that has been developed – which shows the relationship between the digital data and the circumstances pertinent to the

[1] Convention on Cybercrime. (2001, November). Retrieved from https://www.coe.int/en/web/cybercrime/convention-on-cybercrime.
[2] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. (2022, May). Retrieved from https://www.coe.int/en/web/cybercrime/second-additional-protocol.
[3] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17?lang=en&utm.
[4] Convention on Cybercrime. (2001, November). Retrieved from https://www.coe.int/en/web/cybercrime/convention-on-cybercrime.

criminal proceedings – should be taken into account. By adopting this approach, the traditional criterion of relevance can be applied consistently to the materials from blockchain analysis without the need to establish a special procedural regime for this kind of evidential information.

The admissibility of the materials and conclusions prepared by a blockchain systems analyst depends on whether the way in which the information has been obtained, processed, and presented is in line with the requirements of criminal procedure law. The fact that specialised analytical tools have been used does not by itself give rise to procedural grounds for treating the materials as admissible evidence. The key factors are whether it is possible to establish the lawful origin of the source data, to trace the sequence of the analytical processing carried out, to verify the methods employed, and to ensure that procedural safeguards are in place so that all parties involved in the criminal proceedings can check the results (Oliinyk *et al.*, 2020).

This method is in line with the general provisions of criminal procedure law as they pertain to the admissibility of evidence. So far as the Criminal Procedure Code of Ukraine[1] is concerned, Article 86 defines admissibility on the grounds of the lawfulness of the procedure used to obtain evidential information, whereas Article 94 deals with its assessment in terms of relevance, admissibility, reliability and sufficiency when taken into account together with other evidence. Moreover, Articles 16, 18 and 19 of the Convention on Cybercrime[2] lay down the rules concerning the rapid preservation, production, search and seizure of computer data and ensure the procedural legitimacy of the source of digital information, but do not create a presumption of admissibility for information obtained from electronic systems. The same approach is taken in Articles 7-9 of the Second Additional Protocol to the Convention on Cybercrime concerning Enhanced Co-operation and Disclosure of Electronic Evidence[3], which regulate access to electronic evidence in cases that are transnational and require compliance with procedural safeguards regardless of the means by which the digital information is obtained.

The analysis shows that, when it comes to a blockchain systems analyst, the question of procedural admissibility goes beyond just checking that the primary blockchain data was obtained lawfully. It is also necessary to examine the whole analytical process, including the specialised software employed, the analytical algorithms used, the criteria for clustering addresses, the methods employed for linking up digital assets, and the possibility of independently reproducing the results obtained. If any one of these elements cannot be verified or if its application cannot be open to objective examination, this casts doubt not only on the reliability of the analyst's conclusions but also on the procedural admissibility of the materials produced as evidence.

This conclusion is in line with the international methods of using blockchain analysis in financial investigations. The Financial Action Task Force's (2021) recommendations on virtual assets and virtual asset service providers call on competent authorities to make use of analytical tools in order to track the movement of digital assets, while stressing the importance of ensuring that the information acquired is verifiable and can be used in criminal proceedings in accordance with national law. The admissibility of the materials and conclusions of a blockchain systems analyst should therefore be seen as a combined procedural criterion involving the legality of obtaining the original digital information, the transparency of the analytical method, the possibility of independently verifying the methods employed, and the protection of the procedural rights of the parties involved in the criminal proceedings. It is this combination of factors, not the technical features of blockchain technology or the reputation of a specific analytical platform, that decides whether the results of the blockchain analysis can be accepted as admissible evidence.

One cannot equate the reliability of the materials and the conclusions of a blockchain systems analyst with the immutability of the entries in a distributed ledger. While the immutability of blockchain data ensures the integrity of the information in the relevant ledger, it does not guarantee that the results of any subsequent analytical processing are correct. It follows that a procedural assessment should cover not only the original digital data but also the methodology employed to examine it, the analytical algorithms used, the soundness of the conclusions reached, and the possibility of verifying them independently. This method of assessment is in line with the general principle laid down in Article 94 of the Criminal Procedure Code of Ukraine[4], which provides that the court is to evaluate each item of evidence in terms of its relevance, admissibility, reliability, and sufficiency when taken together with the other evidence.

[1] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17?lang=en&utm#Text.
[2] Convention on Cybercrime. (2001, November). Retrieved from https://www.coe.int/en/web/cybercrime/convention-on-cybercrime.
[3] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. (2022, May). Retrieved from https://www.coe.int/en/web/cybercrime/second-additional-protocol.
[4] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17?lang=en&utm#Text.

It has been determined that the special feature of blockchain analysis is the multi-stage processing of digital data, involving the use of clustered addresses, the identification of digital assets, the mapping of network links, and a number of other analytical techniques. At this stage, information is generated which is not directly present in the blockchain but is the result of the application of specialised analytical methods. As a result, the reliability of an analyst's findings and conclusions depends not just on the authenticity of the source data but also on the scientific validity of the methods employed and on the possibility of verifying the results by independent means.

A sign of the reliability of blockchain analysis is the ability to reproduce the results. Where the same method is applied to identical source data and yet different results are obtained, this shows that the conclusions reached cannot be adequately verified and therefore have reduced probative value. Just as important is the transparency of the analytical algorithms employed. When closed software packages are used, and their mode of operation cannot be checked by the other parties involved in the criminal proceedings, it becomes impossible to evaluate the reliability of the materials produced. For this reason, research in the field of digital forensics stresses that the probative value of blockchain analysis depends directly on recording all the stages of the analytical process, allowing the analysis to be carried out independently again, and making the methods used transparent (Dudani *et al.*, 2023; Su, 2025). Special attention is also paid to the evaluation of the heuristic models used to cluster crypto-addresses and to establish connections between digital assets. Unlike the cryptographic mechanisms that underlie the operation of blockchain, heuristic algorithms are based on probabilistic assumptions regarding the behaviour of network users, and this may result in incorrect outcomes (Vozniuk *et al.*, 2020). It is possible therefore that crypto-addresses will be incorrectly attributed, that independent wallets will be improperly grouped, or on the other hand that the actual links between them will fail to be detected. It follows that the clustering results cannot be regarded as definitive proof of the circumstances in question and must be checked against other sources of evidence.

The analysis indicates that relying solely on the criteria of relevance, admissibility, and reliability does not allow for a full evaluation of the materials and conclusions produced by a blockchain systems analyst. Although each of these criteria relates to a separate feature of evidential information, none of them by itself is sufficient to enable an assessment of the specific nature of the results obtained from blockchain analysis, since these results are the product of combining digital data with specialised methods for examining it and with professional interpretation. It has been shown that a proper procedural assessment of such materials involves three closely related lines of review. The first of these relates to adherence to the procedural rules concerning the acquisition and use of evidential information. The second deals with the scientific validity of the blockchain-analysis methodology, covering the verifiability of the algorithms employed, the transparency of the analytical procedures, and the reproducibility of the results achieved. The third is concerned with the content of the conclusions reached, examining their logical consistency, completeness, and agreement with the digital data obtained as a result of the examination. Consequently, because of the special characteristics of the materials and the conclusions produced by a blockchain systems analyst, a thorough procedural assessment is required. This assessment must be carried out not only by means of the normal evidential criteria, but also via an interconnected system involving procedural-legal, scientific-methodological, and evidentialanalytical review. This approach to evaluation is due to the particular nature of blockchain analysis when it is applied in criminal proceedings (Table 2).

Table 2. Conceptual model for the procedural assessment of the materials and conclusions of a blockchain systems analyst

Stage of comprehensive assessment	Subject of assessment	Content of procedural review	Assessment outcome
I. Assessment of the source of evidential information	Materials and conclusions prepared by the analyst as outputs arising from the acquisition and use of digital information	Verification of the lawfulness of obtaining the source data, the relevance of the materials to the subject matter of proof, and compliance with procedural requirements for their preparation and use	Establishing the procedural permissibility of using the materials and conclusions in criminal proceedings
II. Assessment of the research methodology	Blockchain-analysis methods and the procedure used to conduct the analytical examination	Assessment of the transparency of the algorithms applied, the reproducibility of results, the verifiability of heuristic models, and the completeness of the documentation of analytical procedures	Establishing the scientific soundness and reliability of blockchain-analysis results
III. Assessment of the results of analytical activity	Materials and conclusions prepared by a blockchain systems analyst	Verification of the logical consistency of the conclusions, their correspondence with the source digital data, the completeness of the interpretation of the facts established, and consistency with other evidence in criminal proceedings	Establishing the evidential value of the materials and conclusions of a blockchain systems analyst

Source: compiled based on O. Olukoya (2021), F. Casino *et al.* (2022), F. Nujumudeen *et al.* (2026)

The model suggested changes the way in which the procedural evaluation of the materials and findings of a blockchain systems analyst is carried out by shifting the emphasis from examining the individual characteristics of the evidential information to evaluating the whole process by which it is generated. It enables the results of a blockchain analysis to be treated as a single entity in the context of procedural review, with the legality of the way digital data was obtained, the scientific validity of the methodology used, and the logical strength of the conclusions reached being interconnected components of this one assessment process. The practical advantage of the model is that it offers a general approach to the assessment of the materials and conclusions of a blockchain systems analyst, regardless of the software employed, the kind of blockchain network involved, or the type of digital assets under examination. It permits the use of consistent criteria for procedural review both in the pre-trial investigation and in judicial proceedings, and at the same time provides a methodological foundation for establishing a uniform legal practice in the use of blockchain analysis.

Application of the materials and conclusions of a blockchain systems analyst in criminal proceedings

It is necessary to test the consistency of a theoretical model designed for assessing the materials and findings of a blockchain systems analyst against the actual methods that have developed in legal practice. The evidential value of the results of a blockchain analysis is finally determined at trial, the court having not only to decide whether the results can be used to support circumstances pertinent to a criminal case but also to judge whether the examination methods employed were adequate, whether the conclusions reached are well grounded, and whether they are in agreement with the other evidence. Thus, by examining the case law, it is possible to discover the criteria which in fact come into use when evaluating blockchain-analysis materials, no matter what the specific features of the individual criminal cases are.

The decisions of the courts show a change in the way blockchain-analysis evidence is evaluated: rather than viewing blockchain technology as a technical tool for recording digital information, the courts now assess the outcome of professional analytical work carried out by examining distributed-ledger data. Today's judicial scrutiny does not stop at information regarding the movement of digital assets; it also looks at the validity of the methods employed to reconstruct that information, the verifiability of the algorithms used, the reliability of the connections made between crypto-addresses, and the extent to which the analytical conclusions are sufficient to support legally relevant facts. This suggests that a comprehensive approach has developed towards the evaluation of the materials and conclusions provided by a blockchain systems analyst, one that goes beyond checking the technical accuracy of the entries in the blockchain. It is for this reason that the following analysis aims to identify general patterns in the way such materials and conclusions are used in criminal proceedings and to ascertain how well the judicial approach corresponds with the conceptual model of comprehensive procedural assessment set out in this study.

Approaches to the use of blockchain-analysis materials in criminal proceedings are most fully illustrated by judicial decisions in which the results of analyses of public blockchain networks have been assessed. An examination of such decisions shows that the scope of judicial review increasingly encompasses not only information on digital transactions, but also the methods used for its analytical processing. This is directly relevant to determining the evidential value of the materials and conclusions of a blockchain systems analyst. The only case in which the court examined the admissibility of blockchain-analysis material was the Case of the United States v. Gratkowski[1]. This case dealt with whether information derived from examining publicly available data on the Bitcoin network could be used to prove certain circumstances in a criminal trial. The court started from the assumption that transaction data is stored in a publicly accessible distributed ledger and that its analytical processing allows the reconstruction of the pathways of digital asset movements and the establishment of links between individual transactions. The court admitted the use of specialised blockchain-analysis tools for tracing cryptoassets and for subsequently identifying digital addresses, even though the court did not independently assess the scientific validity of the methods employed.

The same approach can be seen in the Case of the United States v. Harmon[2], with the difference that blockchain analysis was applied on a wider scale. Beyond reconstructing the flow of digital assets, the findings from the analytical investigation were employed to establish financial connections between various transactions, to identify the methods used for hiding the origin of crypto-assets, and to confirm that a money-laundering scheme had operated via the Helix cryptocurrency-mixing service. In reaching its conclusion, the court essentially acknowledged that the results of blockchain analysis can be used to reconstruct complicated financial relationships, on the

[1] Case of the United States v. Gratkowski. (2020, June). Retrieved from https://www.govinfo.gov/app/details/USCOURTS-ca5-19-50492.
[2] Case of the United States v. Harmon. (2020, July). Retrieved from https://case-law.vlex.com/vid/united-states-v-harmon-893236324.

condition that they are supported by other evidence. At the same time, the main emphasis continued to be on the evidential value of the circumstances proven, while the scientific reliability of the methodology in question had not yet become an independent matter for procedural evaluation.

A more thorough method of evaluating materials obtained from blockchain analysis is demonstrated in the Case of the United States v. Sterlingov[1], in which the court's analysis did not stop at the results of the blockchain analysis but also included a judgment of the scientific validity of the methodology employed to arrive at those results. The court looked into the operating principles of the Chainalysis Reactor software, the specific aspects of applying techniques for clustering cryptoaddresses, the means by which digital assets were attributed to particular individuals, and the possibility of testing the methodology against scientific-reliability standards established in the case law using the Case of Daubert v. Merrell Dow Pharmaceuticals, Inc.[2]. In that case, the court did not merely consider the findings and conclusions of the blockchain systems analyst but also examined the reproducibility of the analytical results, the transparency of the algorithms employed, and the possibility of independently verifying the conclusions reached. This kind of approach indicates that judicial evaluation involves not just the outcome of the blockchain analysis but also the process by which that outcome is reached, something which is directly pertinent to assessing the evidential value of the materials in question.

An examination of court rulings shows that, even though there are differences in the factual situations of criminal cases, the way in which the courts have evaluated materials produced by blockchain analysis is in line with the model of comprehensive procedural assessment set out in this study. In the Case of the United States v. Gratkowski[3], the emphasis was placed on deciding whether information derived from a public blockchain could be used, in other words, on judging the source of the evidential information. In the Case of the United States v. Harmon[4], the court evaluated the evidential value of the blockchain-analysis results together with other evidence, thus showing a move towards looking at the outcomes of the analytical work. The most thorough approach is seen in the Case of the United States v. Sterlingov[5], where the court looked not only at the findings of the analysis but also at the scientific validity of the blockchain-analysis methodology employed. This demonstrates that the model proposed is not merely an abstract theoretical idea, but rather mirrors actual patterns that are already present in current legal practice when assessing the materials and conclusions of blockchain systems analysts. The need for the source data to have a lawful and verifiable origin, for the analytical results to be linked to the subject matter of the case, for the methodology to be transparent, and for the results to be reproducible, independently verifiable, and supported by other evidence is common to all cases. These criteria are in agreement with the general provisions of Articles 84-86 and 94 of the Criminal Procedure Code of Ukraine[6] and can therefore be applied when assessing blockchain-analysis materials in Ukraine. At the same time, the Daubert standard, the procedural rules concerning the admission of expert evidence, the binding character of court decisions, and the US courts' views on reasonable expectations of privacy with regard to public blockchain data reflect the specific features of the American legal system. They can therefore be used only as a point of comparison, and not as criteria to be directly applied in Ukrainian criminal procedure.

The way in which the Ukrainian judicial system evaluates documents relating to virtual assets is somewhat different. In its Ruling of the Appeal Chamber of the High Anti-Corruption Court in Case No. 991/10335/23[7] examined information about crypto-wallets, transactions involving Bitcoin and Tether USD, a seed phrase (which is a mnemonic phrase used to regain access to a crypto-wallet), the records of the inspection of the information, and the transaction data in order to conclude that the virtual assets in question belonged to a specific person. The court placed more emphasis on evidence showing the establishment of the wallets, the possession of them, and actual control over the assets, taking into account the entire body of this information. It also considered separately the documents relating to the inspection of the information on the virtual assets and the transactions, as well as the arguments that the seed phrase and the crypto-wallets belonged

[1] Case of the United States v. Sterlingov. (2024, February). Retrieved from https://caselaw.findlaw.com/court/us-dis-crt-discol/115886148.html.
[2] Case of Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993, June). Retrieved from https://www.govinfo.gov/app/details/USREPORTS-509/USREPORTS-509-579.
[3] Case of the United States v. Gratkowski. (2020, June). Retrieved from https://www.govinfo.gov/app/details/USCOURTS-ca5-19-50492.
[4] Case of the United States v. Harmon. (2020, July). Retrieved from https://case-law.vlex.com/vid/united-states-v-harmon-893236324.
[5] Case of the United States v. Sterlingov. (2024, February). Retrieved from https://caselaw.findlaw.com/court/us-dis-crt-discol/115886148.html.
[6] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17?lang=en&utm.
[7] Ruling of the Appeal Chamber of the High Anti-Corruption Court in Case No. 991/10335/23. (2024, October). Retrieved from https://opendatabot.ua/court/122788762-d3bb098fe38ee6185f61abea1e44ec47.

to someone else. Finally, the court decided that the circumstances established were enough to keep the relevant virtual assets seized.

Another feature of the Ukrainian approach can be seen in the Ruling of the Shevchenkivskyi District Court of Kyiv in Case No. 761/11447/24[1]. In this case, a detective from the Department of Detectives for Economic Protection in the Field of Virtual Assets of the Bureau of Economic Security of Ukraine submitted an application for temporary access to certain items and documents. The court rejected the application since the prosecution had not stated which circumstances in the criminal proceedings were to be proven by the information requested or what material importance it had in establishing those circumstances. The ruling therefore demonstrates the application of the general procedural criterion of evidential value irrespective of the digital form of the information: access to information must be justified by its specific connection with the circumstances to be established in criminal proceedings.

A comparison of USA and Ukrainian judicial practice indicates different degrees of development in approaches to the procedural assessment of blockchain-analysis materials. In US practice, the subject of judicial assessment has gradually expanded from verifying the source of blockchain information and its evidential value to examining the scientific reliability of blockchain-analysis methods. In Ukraine, this method is still in its early stages of development. Although Ukrainian courts have already incorporated various aspects of the proposed model – particularly when looking at the link between digital information and the circumstances in issue, the information's origin, and its consideration together with other evidence – a full evaluation of the blockchain-analysis methodology, including its reproducibility and scientific reliability, has not yet reached the level of development found in current US practice. This indicates a transformation of blockchain analysis from an auxiliary technical tool into a specialised means of obtaining evidential information. The identified patterns support the need to distinguish blockchain-analysis materials from the conclusion of a blockchain systems analyst as distinct procedural forms through which specialised knowledge is used.

Discussion

The study substantiated that the materials and conclusions of a blockchain systems analyst are products of applying specialised knowledge and cannot be reduced to a reproduction of information contained in a distributed ledger. This approach made it possible to distinguish primary blockchain data from the results of their professional analytical processing and to determine the independent place of the analyst's materials and conclusions within the evidential framework of criminal proceedings. The findings are consistent with those of H.F. Atlam *et al.* (2024), whose systematic review of research in blockchain forensics showed that the principal areas of development remain the improvement of transaction-analysis methods, crypto-address clustering, and the tracing of digitalasset movements. However, the authors focused primarily on the functional capabilities of blockchain-analysis tools, while the procedural status of the results of such analytical activity was not examined separately. In the present study, the focus was shifted from the technological characteristics of blockchain analysis to the legal nature of the materials and conclusions produced through its use, which made it possible to identify them as independent products of applying specialised knowledge.

M. Fröwis *et al.* (2020) examined the conditions under which the results of cryptocurrency forensic examinations retain their evidential value. The authors demonstrated that documenting the examination procedure, the possibility of reproducing it, and control over the integrity of the results are decisive. This approach accords with the findings of the present study, but addresses the forensic aspect of the issue primarily. The study further shows that, even where the requirements of forensic reliability are met, the materials and conclusions of a blockchain systems analyst require a separate procedural-legal assessment. Their evidential value depends not only on the manner in which the examination was conducted, but also on the nature of the analytical result produced. The evidential value of blockchain data was also examined by O.A. Musbih (2026) in a study devoted to the use of blockchain entries in criminal proceedings. The author argued that the defining characteristics of such entries are their authenticity, integrity, and verifiability, which permit their use as a source of evidential information. The findings of the present study do not contradict this conclusion, but offer a different level of analysis. Whereas O.A. Musbih regarded blockchain entries themselves as the object of assessment, the present study identifies the materials and conclusions of a blockchain systems analyst as the result of intellectual and analytical activity formed on the basis of those entries. This distinction explains why the procedural assessment of blockchain-analysis results cannot be confined to verifying the properties of primary distributed-ledger data.

The study also substantiated that the procedural assessment of the materials and conclusions of a

[1] Ruling of the Shevchenkivskyi District Court of Kyiv in Case No. 761/11447/24. (2024, April). Retrieved from https://zakononline.ua/court-decisions/show/118588220.

blockchain systems analyst cannot be limited to verifying their compliance with the traditional criteria of relevance, admissibility, and reliability. The proposed conceptual model is based on the need for a comprehensive assessment of three interrelated components: the lawfulness of obtaining and using digital information, the scientific soundness of the blockchain-analysis methodology applied, and the logical cogency of the analytical conclusions drawn. This approach takes account of the particular manner in which evidential information is formed through the professional analytical processing of distributed-ledger data. A similar issue was explored by I.A. Haji *et al.* (2026) in a study on ensuring continuity in the chain of custody of digital evidence and assessing its lawfulness in criminal proceedings related to post-conflict investigations. The authors argued that the evidential value of digital information depends on the ability to confirm the immutability of digital data, trace every stage of their processing, and ensure oversight of the lawfulness of their use. The findings of the present study accord with this approach, but extend its scope. Whereas the study by I.A. Haji *et al.* associates procedural reliability primarily with compliance with requirements for preserving digital evidence, the present study demonstrates that this is insufficient for assessing blockchain-analysis materials. In addition to verifying the source of digital information, it is also necessary to assess the scientific soundness of the methods used to examine it and the reasoning underlying the analytical conclusions drawn.

The integrity of digital evidence was also examined by A.Y. Krishna & N. Kumar Chaudhary (2026), who proposed a model for using blockchain technology to document, preserve, and monitor digital evidence in criminal proceedings. Their study concluded that the use of blockchain increases confidence in digital evidence by preventing unauthorised alteration and making information-recording procedures transparent. The present study does not challenge this conclusion, but demonstrates that ensuring the integrity of digital data is not equivalent to confirming the evidential value of blockchain-analysis results. The immutability of information concerns the properties of the source data, but does not enable an assessment of the validity of the analytical methodology applied or the soundness of the conclusions based on it. For this reason, the proposed model of procedural assessment encompasses not only the properties of digital information, but also the procedure for its analytical interpretation.

Another line of research is represented by the study of Y. Park & D. Jeong (2026), which developed a digital-evidence management model combining forensic procedures with multi-level access-verification mechanisms. The authors proceed from the premise that the proper organisation of processes for storing, documenting, and using digital evidence creates the necessary conditions for ensuring its evidential value. The present findings generally accord with this position, but support a broader conclusion. Effective digital-evidence management does not in itself resolve the issue of assessing the materials and conclusions of a blockchain systems analyst, as this requires verification not only of the process of handling digital information, but also of the scientific soundness of the blockchain-analysis methods used and the logical coherence of the conclusions drawn. In this respect, the conceptual model proposed in the study may be regarded as a procedural complement to existing technical models of digital-evidence management, as it establishes criteria for assessing the outputs of analytical activity, rather than merely requirements for their preparation and storage.

The analysis of legal practice showed that the procedural assessment of the materials and conclusions of a blockchain systems analyst is gradually moving beyond verification of the authenticity of digital data. Judicial assessment now concerns not only information obtained from a distributed ledger, but also the methods of its analytical processing, the soundness of the research methods used, and the persuasiveness of the conclusions drawn. This makes it possible to regard blockchain-analysis materials as an independent object of procedural assessment, whose evidential value is determined by a combination of legal, scientific-methodological, and analytical characteristics. Similar trends are evident in the study by S. Kaya *et al.* (2026), which addressed the evidential value of blockchain technology in civil justice. The authors concluded that the use of blockchain entries in judicial proceedings is gradually shifting from viewing them as a technical means of confirming the authenticity of information to assessing their evidential value in conjunction with other evidence and the procedural circumstances of the case. The present findings accord with this approach, but extend it to criminal procedure. The study showed that, in criminal proceedings, the subject of judicial assessment is broader, as it encompasses not only the properties of blockchain entries, but also the results of professional analytical activity formed on their basis. This indicates that the procedural significance of blockchain-analysis materials is not determined in isolation, but in the context of assessing the manner in which they are formed and used in the evidential process.

Another dimension of the issue is addressed in the study by N. Xiao *et al.* (2024), which proposed a blockchain-based digital-forensics model for ensuring the preservation of evidence and supporting investigations in industrial Internet of Things networks. The authors argued that the use of blockchain ensures the integrity of digital information, transparency in its processing, and the possibility of monitoring all

operations involving evidence. This approach accords with developments in digital forensics, although its main emphasis is on the technological mechanisms by which the system operates. The findings of the present study make it possible to complement this approach with a procedural dimension, showing that even proper technical arrangements for handling digital evidence do not remove the need for a separate assessment of the materials and conclusions of a blockchain systems analyst. The evidential value of such materials is determined not only by the possibility of tracing the provenance of digital information, but also by the soundness of its analytical interpretation and its capacity to confirm circumstances falling within the subject matter of proof.

A synthesis of the findings supports the conclusion that the development of blockchain technologies in criminal proceedings is accompanied by a gradual shift in emphasis from examining the technical characteristics of digital evidence to developing procedural approaches for assessing the results of its professional analytical processing. Accordingly, future research should be directed not only towards improving blockchain-analysis technologies, but also towards developing uniform procedural criteria for assessing the materials and conclusions of blockchain systems analysts. This approach will help align advances in digital forensics with the requirements of proof in criminal proceedings and ensure a more consistent use of blockchain-analysis results in legal practice.

■ Conclusions

It was established that these outputs of professional activity cannot be regarded as a type of blockchain data or as a technical reproduction of information contained in a distributed ledger. They constitute independent products of applying specialised knowledge, formed through the comprehensive analytical processing and interpretation of digital data and the identification of legally significant links between digital assets, crypto-addresses, and other information objects. The comparison of the materials and conclusions of a blockchain systems analyst with a forensic expert's opinion and a specialist's consultation or explanation according to five criteria – their legal nature, the person responsible for their preparation, the subject matter of the examination, the content of the result, and their functional purpose – supports the conclusion that they constitute an independent category of results arising from the application of specialised knowledge in criminal procedure. This indicates that they cannot be fully equated with existing procedural institutions.

It was substantiated that the procedural assessment of the materials and conclusions of a blockchain systems analyst should be based on the general criteria of relevance, admissibility, and reliability, although their content requires adaptation to the particularities of blockchain analysis. Relevance is determined by the connection between the results of analytical processing and the subject matter of proof. Admissibility encompasses not only the lawfulness of obtaining the source data, but also the verifiability of the entire analytical-processing cycle. Reliability depends on the reproducibility of the examination results, the transparency of the algorithms used, the verifiability of heuristic models, and the possibility of independently confirming the conclusions drawn. The study resulted in the development of a conceptual model for the comprehensive procedural assessment of the materials and conclusions of a blockchain systems analyst. The study resulted in a conceptual model that submits the materials and conclusions of a blockchain systems analyst to three interdependent stages of procedural scrutiny: the source of the evidential information, the methodology of the blockchain analysis, and the results of the analytical activity. Unlike the conventional approach, the proposed model considers the entire process through which evidential information is formed, from the lawfulness of obtaining digital data to the logical soundness of the analytical conclusions.

The analysis of court decisions confirmed that legal practice is gradually moving from assessing the technical properties of blockchain technology to examining the scientific soundness of blockchain-analysis methods, the reliability of the conclusions drawn, and the possibility of their independent verification. The identified progression of judicial approaches indicates that the proposed model is practically consistent with current trends in the use of blockchain analysis in criminal proceedings. The study is limited by its reliance on decisions of US courts, where issues concerning the use of blockchain analysis have received the most thorough procedural treatment. This makes it necessary to expand the comparative basis of the research by examining the judicial practice of other states as it develops. Further research should focus on developing procedural requirements for the formal presentation of the materials and conclusions of blockchain systems analysts, defining criteria for assessing individual blockchain-analysis methods, and examining the use of analytical findings from different types of blockchain networks in criminal proceedings.

■ Acknowledgements

None.

■ Funding

None.

■ Conflict of Interest

None.

References

[1] Albright, T.D. (2023). A scientist's take on scientific evidence in the courtroom. *Proceedings of the National Academy of Sciences of the United States of America*, 120(41), article number e2301839120. doi: 10.1073/pnas.2301839120.

[2] Alyas, T., Abbas, Q., Niazi, S., Alqahtany, S.S., Alghamdi, T., Alzahrani, A., Tabassum, N., & Ibrahim, A.M. (2025). Multi blockchain architecture for judicial case management using smart contracts. *Scientific Reports*, 15, article number 8471. doi: 10.1038/s41598-025-92842-8.

[3] Ardian, R.E., Rozi, F., & Soetikno, N. (2025). The implementation of blockchain technology in the criminal justice system: Opportunities, challenges, and its implications for transparency and accountability. *Hakim: Jurnal Ilmu Hukum dan Sosial*, 3(2), 1207-1220. doi: 10.51903/ndjn0n19.

[4] 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 number 3568. doi: 10.3390/electronics13173568.

[5] Ayub, A.M., Syed, F.R., & Peng, H. (2025). Breaking barriers: The admissibility of forensic evidence in US courts and the struggles with cutting-edge science. *Science & Justice*, 65(6), article number 101355. doi: 10.1016/j.scijus.2025.101355.

[6] Casino, F., Dasaklis, T.K., Spathoulas, G.P., Anagnostopoulos, M., Ghosal, A., Böröcz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, 10, 25464-25493. doi: 10.48550/arXiv.2108.04634.

[7] Chen, S., Rajamanickam, R., & Manap, N.A. (2024). Legal framework for authenticity of blockchain electronic evidence in China: Under a comparative law perspective. *Hasanuddin Law Review*, 10(3), 272-291. doi: 10.20956/halrev.v10i3.5638.

[8] Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The current state of cryptocurrency forensics. *Forensic Science International: Digital Investigation*, 46, article number 301576. doi: 10.1016/j.fsidi.2023.301576.

[9] Fahmideh, M., *et al.* (2023). Engineering blockchain-based software systems: Foundations, survey, and future directions. *ACM Computing Surveys*, 55(6), article number 110. doi: 10.1145/3530813.

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

[11] Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C., & Pesch, P. (2020). Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation*, 33, article number 200902. doi: 10.1016/j.fsidi.2019.200902.

[12] Haji, I.A., Mohammed, S.D., & Mousa, K.M. (2026). Blockchain based chain of custody and digital evidence legality in post conflict prosecutions. *Frontiers in Blockchain*, 9, article number 1801364. doi: 10.3389/fbloc.2026.1801364.

[13] Harris, M. (2023). Blockchain-based evidence in courts: Standards, reliability, and admissibility challenges. *Legal Studies in Digital Age*, 2(3), 49-63.

[14] Kaya, S., Kurt Konca, N., & Kıyak, E. (2026). The evidentiary value of blockchain in civil litigation: Comparative insights and future directions. *Frontiers in Blockchain*, 9, article number 1783805. doi: 10.3389/fbloc.2026.1783805.

[15] Krishna, A.Y., & Kumar Chaudhary, N. (2026). Enhancing evidence integrity and trust in the criminal justice system: A design and evaluation of the blockchain enabled evidence securing and tracking (BEST) application. *IETE Journal of Research*, 72(5-6), 1099-1108. doi: 10.1080/03772063.2026.2617871.

[16] Lavín, I., & Llanos, D.R. (2026). An analysis of blockchain solutions for digital evidence chain of custody. In R. Pastor-Vargas, A. Carrera, B. Molnár, Ó. Lage, J. Prieto, A. Nongaillard (Eds.), *Blockchain and Applications, 7th International Congress* (pp. 221-231). Cham: Springer. doi: 10.1007/978-3-032-05877-5 21.

[17] Martynenko, K.V. (2026). Organization of the investigation of criminal offenses related to the use of virtual assets: Problems and the current state of scientific research. *Analytical and Comparative Jurisprudence*, 3(2), 138-147. doi: 10.24144/2788-6018.2026.02.3.19.

[18] Metelev, O.P. (2025). Legal nature and current issues of evaluating virtual assets (crypto-assets) as evidence in criminal proceedings. *Herald of Criminal Justice*, 3-4, 52-68. doi: 10.59835/2413-5372.2025.3-4/52-68.

[19] Mollajafari, S., & Bechkoum, K. (2023). Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy. *Sustainability*, 15(18), article number 13401. doi: 10.3390/su151813401.

[20] Musbih, O.A. (2026). The evidentiary value of blockchain records in the criminal justice system: A comparative analytical study. *International Review of Law*, 15(1), 37-64. doi: 10.29117/irl.2026.0361.
[21] Nujumudeen, F., Mubarak, D.M., Hussain, T., & Pinjala, P.K. (2026). Adaptive blockchain framework for reliable authentication and preservation of digital forensic evidence. *Discover Computing*, 29, article number 158. doi: 10.1007/s10791-026-10034-y.
[22] Oliinyk, O., Farynyk, V., Vozniuk, A., Volobuieva, O., & Beryslavska, O. (2020). The principles of criminal law in the aspect of protection of constitutional rights of citizens. *Amazonia Investiga*, 9(27), 445-459. doi: 10.34069/AI/2020.27.03.49.
[23] Olukoya, O. (2021). Distilling blockchain requirements for digital investigation platforms. *Journal of Information Security and Applications*, 62, article number 102969. doi: 10.1016/j.jisa.2021.102969.
[24] Ovsianiuk, D., Okushko, A., & Panchenko, Ye. (2025a). Application of AI to detect anomalous transactions as a new direction in combating money laundering. *Law Journal of the National Academy of Internal Affairs*, 15(4), 75-87. doi: 10.63341/naia-chasopis/4.2025.75.
[25] Ovsianiuk, D., Okushko, A., & Panchenko, Ye. (2025b). Methodology of detection and forensic features of investigation of crimes involving virtual assets: A comparative analysis of international practices. *Scientific Journal of the National Academy of Internal Affairs*, 30(2), 119-137. doi: 10.63341/naia-herald/2.2025.119.
[26] Park, Y., & Jeong, D. (2026). A blockchain-based digital evidence management system: Integrating forensic procedures and multi-party authorization. *Information Processing & Management*, 63(5), article number 104654. doi: 10.1016/j.ipm.2026.104654.
[27] Pasupuleti, M.K. (2024). AI and blockchain in law: Shaping the future of legal practice. In *Legal Tech and the Future of Law: Transforming Legal Practices with AI and Blockchain* (pp. 307-325). London: National Education Services. doi: 10.62311/nesx/46649.
[28] Pérez, C., López, I., & López, F. (2025). Blockchain-based evidence and legal validity: Reformulating norms for decentralized justice systems. *Rechtsnormen Journal of Law*, 3(2), 180-189. doi: 10.70177/rjl.v3i2.2215.
[29] Romaniuk, V.V., & Ablamskyi, S.Ye. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law and Safety*, 93(2), 140-150. doi: 10.32631/pb.2024.2.13.
[30] Shevchuk, V.M. (2026). The use of blockchain technology as an innovative component of criminalistic support for law enforcement activities in war conditions. *Uzhhorod National University Herald. Series: Law*, 5(93), 241-251. doi: 10.24144/2307-3322.2026.93.5.30.
[31] Shinde, S.M., & Gurrala, V.R. (2023). Preserving integrity of evidence with blockchain technology in cloud forensics for immigration management. *Journal of Telecommunications and Information Technology*, 91(1), 78-87. doi: 10.26636/jtit.2023.164522.
[32] Starenkyi, O.S. (2026). The use of virtual assets in criminal procedural proof: Problems of legal certainty and admissibility criteria. *Herald of Criminal Justice*, 1, 247-273. doi: 10.59835/2413-5372.2026.1/247-273.
[33] Su, Z. (2025). Evidentiary value and evidentiary status of blockchain evidence. *The International Journal of Evidence & Proof*, 29(1), 58-76. doi: 10.1177/13657127241238020.
[34] Tsymbaliuk, A.I. (2025). Legal perspectives on blockchain technologies and smart contracts in the Ukrainian legal system. *Uzhhorod National University Herald. Series: Law*, 3(90), 426-432. doi: 10.24144/2307-3322.2025.90.3.62.
[35] Vozniuk, A.A., Savchenko, A.V., Tarasevych, T.Y., Dudorov, O.O., & Klymenko, O.A. (2020). Electronic money and payments as means of committing crimes. *Academic Journal of Interdisciplinary Studies*, 9(4), 150-159. doi: 10.36941/ajis-2020-0069.
[36] Watters, C. (2023). When criminals abuse the blockchain: Establishing personal jurisdiction in a decentralised environment. *Laws*, 12(2), article number 33. doi: 10.3390/laws12020033.
[37] Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Security Review*, 36, article number 105401. doi: 10.1016/j.clsr.2020.105401.
[38] Xiao, N., Wang, Z., Sun, X., & Miao, J. (2024). A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. *Alexandria Engineering Journal*, 86, 631-643. doi: 10.1016/j.aej.2023.12.021.

Матеріали та висновки аналітика блокчейн-систем: проблеми допустимості і правозастосування в кримінальному процесі

Дмитро Овсянюк
Доктор філософії у галузі права
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-1846-4167

Андрій Окушко
Кандидат юридичних наук
Департамент кіберполіції Національної поліції України
02093, вул. Бориспільська, 19, м. Київ, Україна
https://orcid.org/0009-0003-3627-2489

Євгеній Панченко
Управління міжнародного поліцейського співробітництва Національної поліції України
01024, вул. Академіка Богомольця, 1, м. Київ, Україна
https://orcid.org/0000-0001-5755-7457

■ **Анотація.** Метою дослідження було обґрунтування правової природи матеріалів і висновків аналітика блокчейн-систем, визначення критеріїв їх процесуальної оцінки й узагальнення підходів до використання в кримінальному провадженні. Методологічний дизайн дослідження ґрунтувався на поєднанні аналізу наукової літератури, формально-юридичного, порівняльно-правового методів, аналізу судової практики та концептуального моделювання. У дослідженні з'ясовано правову природу матеріалів і висновків аналітика блокчейн-систем як самостійних результатів застосування спеціальних знань, сформованих унаслідок професійної аналітичної обробки даних розподілених реєстрів. Виокремлено відмінності між матеріалами та висновком аналітика блокчейн-систем за їхньою правовою природою, змістом, функціональним призначенням і місцем у процесі доказування, а також обґрунтовано їх відмежування від висновку судового експерта та консультації спеціаліста. Встановлено, що процесуальна оцінка матеріалів і висновків аналітика має здійснюватися на основі класичних критеріїв належності, допустимості та достовірності з урахуванням особливостей їх формування, а не технічних характеристик блокчейн-технології. Доведено, що критеріями належності є зв'язок результатів блокчейн-аналітики з предметом доказування, допустимості – законність отримання вихідних даних, прозорість аналітичної методики та можливість її незалежної перевірки, а достовірності – відтворюваність результатів, перевірюваність евристичних моделей, прозорість алгоритмів і наукова обґрунтованість сформульованих висновків. Розроблено концептуальну модель комплексної процесуальної оцінки матеріалів і висновків аналітика блокчейн-систем, яка охоплює три взаємопов'язані етапи: оцінку джерела доказової інформації, оцінку методології блокчейн-аналізу та оцінку результатів аналітичної діяльності. Отримані результати можуть бути використані слідчими, прокурорами, адвокатами, судовими експертами й аналітиками блокчейн-систем під час оцінювання матеріалів блокчейн-аналітики, окреслення їх доказового значення та забезпечення єдиних підходів до використання такої доказової інформації в кримінальному провадженні

■ **Ключові слова:** кримінальне провадження; цифрові докази; доказова інформація; процесуальна оцінка; віртуальні активи