Revista JURÍDICA PORTUCALENSE

www.upt.pt

Nº 37 | Universidade Portucalense | Porto | 2025

https://doi.org/10.34625/issn.2183-2705(37)2025

Viktor SEZONOV, Oleksandr YUKHNO, Olena MARTOVYTSKA, Hennadii HLOBENKO, Inna STROK

The role of forensic expertise in the investigation of crimes related to forgery of digital documents and cryptocurrencies in Ukraine

DOI: https://doi.org/10.34625/issn.2183-2705(37)2025.ic-11

Secção

Investigação Científica / Scientific Research*

* Os artigos presentes nesta secção foram sujeitos a processo de revisão segundo o método *blind peer review* / The articles in this section have undergone a blind peer review process.

The role of forensic expertise in the investigation of crimes related to forgery of digital documents and cryptocurrencies in Ukraine

O papel da perícia forense na investigação de crimes relacionados com a falsificação de documentos digitais e criptomoedas na Ucrânia

Viktor SEZONOV[a]
Oleksandr YUKHNO[b]
Olena MARTOVYTSKA[c]
Hennadii HLOBENKO[d]
Inna STROK[e]

Abstract. With the advancement of digital technologies and the proliferation of cryptocurrency transactions, new types of crimes have emerged, including the forgery of digital documents and illicit activities involving cryptocurrencies. Thus, the role of forensic expertise has become increasingly significant, as it enables the identification of forged documents, the analysis of cryptocurrency transactions, and the detection of criminal schemes. The purpose of the study is to establish the importance of forensic expertise in investigating crimes and criminal offences related to digital document forgery and cryptocurrencies in Ukraine. The paper involved a comparative analysis of existing legal provisions, which revealed problematic issues, paths, and forms for improving current legislation concerning the modernisation of legal provisions related to the forensic characteristics of documents. The study also identified factors influencing the regulation of forensic expertise in criminal proceedings and current challenges in this field. The study determines the most substantial types of expertise during the investigation of criminal offences involving forged digital documents and cryptocurrencies: forensic economic expertise (accounting and tax records; financial and economic activities; financial and credit operations), forensic (handwriting analysis, technical and forensic document examination), and computer-technical expertise. The importance of providing high-quality comparative samples for identifying

[a] Department of Forensic Investigation of Vehicles and Registry Maintenance, Kharkiv Scientific Research, Forensic Center of the Ministry of Internal Affairs of Ukraine, 61036, 34 Kovtun Str., Kharkiv, Ukraine. ORCID: 0000-0002-2580-2953. E-mail: viktorsezonov2@gmail.com
[b] Department Criminalistics, Forensic Science and Pre-Medical Training, Kharkiv National University of Internal Affairs, 61080, 27 L. Landau Ave., Kharkiv, Ukraine. ORCID: 0000-0002-4771-0531. E-mail: ale.yukhno@outlook.com
[c] Department of Criminal Procedure and Organization of Pre-Trial Investigation, Kharkiv National University of Internal Affairs, 61080, 27 L. Landau Ave., Kharkiv, Ukraine. ORCID: 0009-0002-7956-8610. E-mail: martovytska-l@hotmail.com
[d] Department of Criminal Procedure and Organization of Pre-Trial Investigation, Kharkiv National University of Internal Affairs, 61080, 27 L. Landau Ave., Kharkiv, Ukraine. ORCID: 0000-0002-1533-9213. E-mail: he.hlobenko@outlook.com
[e] Department of Criminal Procedure and Organization of Pre-Trial Investigation, Kharkiv National University of Internal Affairs, 61080, 27 L. Landau Ave., Kharkiv, Ukraine. ORCID: 0000-0002-0423-714X. E-mail: innastrok@hotmail.com

individuals and devices used in document forgery is emphasised. It is noted that addressing tasks in pre-trial investigations concerning forged documents often requires complex examinations by multiple experts and the provision of a joint report. The study proposes procedural enshrinement of the status of complex, repeated, additional, and commission-based expert examinations conducted by forensic experts. The study formulates and justifies recommendations that may improve the legal regulation of forensic expertise in Ukraine.
Keywords: Economic security; Virtual assets; Asset recovery; Blockchain; Mining.

Resumo. Com o avanço das tecnologias digitais e a proliferação das transações com criptomoedas, surgiram novos tipos de crimes, incluindo a falsificação de documentos digitais e atividades ilícitas envolvendo criptomoedas. Nesse contexto, o papel da perícia forense tornou-se cada vez mais relevante, ao permitir a identificação de documentos falsificados, a análise de transações com criptomoedas e a deteção de esquemas ilegais. O objetivo do estudo é estabelecer a importância da perícia forense na investigação de crimes e infrações penais relacionados com a falsificação de documentos digitais e com criptomoedas na Ucrânia. O artigo inclui uma análise comparativa das disposições legais existentes, que revelou questões problemáticas, caminhos e formas de aperfeiçoar a legislação atual no que se refere à modernização das normas jurídicas relativas às características forenses dos documentos. O estudo identificou ainda os fatores que influenciam a regulação da perícia forense nos processos penais e os desafios atuais neste domínio. Determinam-se os tipos de perícia mais relevantes durante a investigação de infrações penais que envolvem documentos digitais falsificados e criptomoedas: perícia forense económica (registos contabilísticos e fiscais; atividades financeiras e económicas; operações financeiras e de crédito), perícia forense (análise da escrita manual; exame técnico-forense de documentos) e perícia técnico-informática. É sublinhada a importância da disponibilização de amostras comparativas de elevada qualidade para identificação de indivíduos e dispositivos utilizados na falsificação de documentos. Salienta-se que a resolução de questões em investigações preliminares relativas a documentos falsificados requer frequentemente exames complexos realizados por vários peritos e a emissão de um relatório conjunto. O estudo propõe a consagração processual do estatuto dos exames periciais complexos, repetidos, adicionais e realizados em comissão por peritos forenses. O estudo formula e justifica recomendações que podem contribuir para o aperfeiçoamento da regulação legal da perícia forense na Ucrânia.
Palavras-chave: Segurança económica; Ativos virtuais; Recuperação de ativos; Blockchain; Mineração.

1. Introduction

The financial payment system has undergone substantial changes due to the introduction of advanced digital payment technologies, which create increased risks of money laundering and terrorism financing through technologically complex schemes that criminals can exploit for illicit gain. The rapid advancement of technology outpaces legislative adaptation, leading to the emergence of legal gaps. Financial transactions, previously conducted exclusively via cash or derivatives, are now performed using new

technological solutions, impacting the effectiveness of traditional methods for investigating financial crimes, complicating the work of law enforcement agencies, and presenting new challenges for financial investigations. The detection and investigation of criminal offences related to forged documents require the application of specialised knowledge.[1] Typically, this involves documentary checks, consultations with experts, investigative actions involving specialists, and the conduct of forensic examinations. Expert involvement at the pre-trial investigation stage is critical for determining whether document forgery exists. The practical value of criteria for differentiating forms of specialised knowledge usage, on which scholars have yet to reach a consensus, is considerable. The application of such knowledge at various stages of the investigation greatly affects the progress of criminal proceedings, ensuring objectivity and accuracy in findings.[2]

The issue of forensic expertise in cryptocurrencies in Ukraine is the subject of research by only a few researchers. According to V.S. Sezonov,[3] forensic investigations confirm the existence of documents where the information provided is accurate, but the physical medium may be forged. Such cases of forgery are classified as material, although the forensic characteristics of such documents have specific attributes. Indeed, the methodologies used for examining documents that fall under forgery and intellectual forgeries remain inadequately developed. I.V. Pashynska[4] developed recommendations for the use of specialised knowledge in investigating economic crimes. These recommendations consider current realities and outline the areas for applying specialised knowledge during such investigations. Among these areas are expertise in the field of informatics, which allows for the analysis of patterns in the generation of electronic traces; practical techniques and methods for documenting and retrieving various electronic traces; technical and forensic support for the examination of computer equipment and the retrieval of electronic documents; and the improvement of methodologies for the examination of computer hardware and

[1] DZYUBLENKO, Iryna and ZHABINETS, Nataliia. Current trends in international organised crime combating cooperation. *Foreign Affairs*, 2024, vol. 34, n.º1, pp. 71-78. ISSN: 2663-2675.
[2] DUPUIS, Daniel and GLEASON, Kimberly. Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, August 2020, vol. 28, n.º1, pp. 60-74. ISSN: 1359-0790.
3 SEZONOV, Viktor. The concept of the document in Forensic science. *Law and Safety,* March 2024, vol. 84, n.º1, pp. 215-224. ISSN: 2617-2933.
[4] PASHYNSKA, Iryna. *Theoretical and methodological foundations of investigation of organized crime in the field of economic activity*. PhD dissertation, Kharkiv National University of Internal Affairs, Kharkiv, 2023.

software products, as well as telecommunications systems and devices.[5] These measures enable the resolution of a broad range of diagnostic and identification tasks while analysing electronic traces.

Forensic examinations play a crucial role in investigating criminal offences involving forged documents. According to V.K. Zherdiev,[6] key types of expertise identified as critical include forensic economic (covering accounting and tax records, financial and economic activities, and financial-credit operations), forensic (handwriting analysis, technical and forensic document examination), and computer-technical expertise. Forensic economic examinations are vital for uncovering financial manipulations, while forensic and computer-technical examinations determine the skills needed for analysing documents and digital traces.[7] This comprehensive approach to expertise enhances the effectiveness of investigations and aids in detecting and uncovering criminal activities. On the other hand, this anonymity encourages an increase in the quantity and variety of criminal offences aimed at the illicit use of cryptocurrency. This situation underscores the importance of developing effective measures for controlling and managing cryptocurrency use to prevent criminal activities. According to V. Khomutenko and A. Khomutenko,[8] like any other system, the forensic expertise system is open to influences from its external environment, which it engages with through processes of interaction, receiving important stimuli for its operations. External links to the forensic expertise system occur through appointing expertise, submitting requests by initiators, and providing them with the results of forensic examinations.

In contrast, the issue has received extensive discussion in the USA, India, and Europe. Specifically, A. Selim and I. Ali[9] emphasise the critical role of digital forensics experts in investigating crimes, highlighting their collaboration with law enforcement

[5] METELSKYI, Ihor and KRAVCHUK, Mariana. Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 2023, vol. 1, n.º1, pp. 18-25. ISSN: 2786-8761.
[6] ZHERDIEV, Vladyslav. *Forensic characteristics and features of investigation of criminal offenses committed in the field of economic activity using counterfeit documents*. PhD dissertation, Kharkiv National University of Internal Affairs, Kharkiv, 2024.
[7] APAKHAYEV, Nurlan, KOISHYBAIULY, Kuanysh, KHUDAIBERDINA, Gulnura, URISBAYEVA, Ainur, KHAMZINA, Zhanna and BURIBAYEV, Yermek. Legal basis for ensuring freedom of access to information on the operation of state administration bodies in Kazakhstan. *Journal of Advanced Research in Law and Economics*, 2017, vol. 8, n.º3, pp. 722-729. ISSN: 2068-696X.
[8] KHOMUTENKO, Vira and KHOMUTENKO, Alla. The dual nature of forensic expertise. *Law Herald*, June 2022, vol. 2, pp. 139-147.
[9] SELIM, Aybeyan and ALI, İlker. The role of digital forensic analysis in modern investigations. *Journal of Emerging Computer Technologies*, December 2024, vol. 4, n.º. 1, pp. 1-5. ISSN: 2757-8267.

and legal entities. Their findings align with the importance of a specialised approach to digital evidence. A. Trozze et al.[10] note that the pseudo-anonymity of cryptocurrencies does not always guarantee complete confidentiality, as other sources of information may reveal users' identities. Consequently, although cryptocurrencies are considered pseudo-anonymous, they do not guarantee full confidentiality, and transactions with transparent characteristics may leave traceable evidence. Some aspects of the subject remain unexplored, particularly the effectiveness of using technologies in forensic expertise and the potential impact of legal innovations on investigating crimes and criminal offences. Therefore, the purpose of the study is to establish the role of forensic expertise in investigating crimes and offences related to digital document forgery and use of cryptocurrencies in Ukraine. The main objectives of the study are as follows:

1. To analyse the legal and regulatory framework governing forensic expertise in the field of digital documents and cryptocurrencies.

2. To investigate the methods and tools of forensic expertise used for detecting and investigating digital document forgeries.

3. To identify the prospects for the development of forensic expertise in the context of the ongoing advancement of digital technologies and cryptocurrencies.

2. Materials and Methods

Forensic expertise plays a crucial role in investigating crimes associated with the forgery of digital documents and cryptocurrencies. It ensures the reliability of evidence and helps establish the facts necessary for a fair adjudication of cases. The study involved an analysis of legal instruments regulating the interaction between law enforcement agencies and experts in this field. This analysis allowed for an assessment of the current state of the issue and the identification of potential improvements. The study engaged norms from various legal sources, including the Criminal Procedural Code of Ukraine,[11] Law of Ukraine "On Virtual Assets",[12] Law of Ukraine "On Forensic Examination",[13] Order of the Ministry of Justice of Ukraine "On

[10] TROZZE, Arianna, KAMPS, Josh, AKARTUNA, Eray Arda, HETZEL, Florian, KLEINBERG, Bennett, DAVIES, Toby and JOHNSON, Shane. Cryptocurrencies and future financial crime. *Crime Science*, January 2022, vol. 11, 1. ISSN: 2193-7680.

[11] Criminal Procedural Code of Ukraine No. 4651-VI. 2013. https://zakon.rada.gov.ua/laws/show/4651-17#Text

[12] Law of Ukraine "On Virtual Assets" No. 2074-IX. 2023. https://zakon.rada.gov.ua/laws/show/2074-20#Text

[13] Law of Ukraine "On Forensic Expertise" No. 4038-XII. 1994. https://zakon.rada.gov.ua/laws/show/4038-12#Text

Approval of the Instruction on Appointment and Conduct of Forensic Examinations and Expert Studies and Scientific and Methodological Recommendations on Preparation and Appointment of Forensic Examinations and Expert Studies",[14] and several judicial decisions:

- The Decision of the Transcarpathian Court of Appeal on case No. 308/2124/20[15] deals with the forgery of digital documents with a view to the fraudulent transfer of property rights. Forensic experts employed metadata analysis and technical document examination to detect unauthorised modifications, with the main challenge arising from the use of advanced software tools to mimic legitimate documents and encryption methods that concealed traces of tampering. This case demonstrates the necessity for ongoing advancements in forensic methodologies to counteract the evolution of forgery techniques.
- The Decision of the Odesa Court of Appeal on case No. 495/10329/23 1-ks/495/2129/23[16] addresses the issue of unauthorised access and theft of cryptocurrency from a digital wallet, highlighting the significance of computer-technical expertise in tracing the movement of stolen assets across multiple blockchain addresses. The case also underscores the challenges posed by the pseudonymous nature of transactions and the use of rapid transfers to obfuscate the financial trail. This case underscores the importance of collaboration between forensic experts and cryptocurrency exchanges to access Know Your Customer data for identifying perpetrators.
- The Decision of the Kyiv Court of Appeal on case No. 760/19180/23[17] pertains to the use of forged digital signatures to authorise fraudulent financial transactions. Handwriting analysis and cryptographic verification of digital signatures revealed discrepancies indicative of forgery. The primary challenge in this case was the unauthorised use of compromised private keys, which rendered detection difficult. This

[14] Order of the Ministry of Justice of Ukraine "On Approval of the Instruction on Appointment and Conduct of Forensic Examinations and Expert Studies and Scientific and Methodological Recommendations on Preparation and Appointment of Forensic Examinations and Expert Studies" No. 53/5. 1998. https://zakon.rada.gov.ua/laws/show/z0705-98#Text

[15] Decision of the Transcarpathian Court of Appeal on case No. 308/2124/20. 2020. https://reyestr.court.gov.ua/Review/88922416

[16] Decision of the Odesa Court of Appeal on case No. 495/10329/23 1-ks/495/2129/23. 2023. https://reyestr.court.gov.ua/Review/114307295

[17] Decision of the Kyiv Court of Appeal on case No. 760/19180/23. 2023. https://reyestr.court.gov.ua/Review/114895442

case demonstrates vulnerabilities in digital signature systems and underscores the need for robust key management practices to enhance security.

- The Decision of the High Anti-Corruption Court on case No. 991/2747/22[18] concerns the laundering of illicit funds through cryptocurrency transactions, where forensic economic expertise was employed to analyse financial records and blockchain data, thereby unveiling layering techniques employed to obscure the origin of funds. The investigation was further complicated by the use of mixing services and cross-border transfers. This case underscores the importance of integrating traditional financial analysis with blockchain technology to effectively combat digital money laundering.
- The Decision of the Kirovskyi District Court of Kirovohrad on case No. 404/8091/21[19] concerns the creation and distribution of counterfeit digital certificates falsely attributed to governmental authorities. Technical examinations analyzed metadata, issuance dates, and embedded security features to expose inconsistencies. The investigation revealed that the perpetrators had produced high-fidelity replicas of official templates and had also tampered with the metadata to deceive the system by emulating legitimate issuance patterns. This case underscores the significance of a centralized verification system for the efficient authentication of digital documents.

In determining the specifics of forensic examination in investigating crimes related to the forgery of digital documents and cryptocurrencies, general forms, properties, classifications, and applications of digital documents were outlined. Exploring this subject required thorough analysis and systematisation, which revealed its complex structure and functional characteristics. The application of principles such as historicism, comprehensiveness, and complexity helped to identify paths and forms for improving existing legislation concerning the modernisation of legal provisions related to forensic characteristics of documents.

To identify contemporary trends in the involvement of forensic experts in cases related to cryptocurrency forgery/theft and digital document forgery, materials from recent court cases were examined, including the Decision of the Eastern Commercial

[18] Decision of the High Anti-Corruption Court on case No. 991/2747/22. 2022. https://reyestr.court.gov.ua/Review/105596649

[19] Decision of the Kirovskyi District Court of Kirovohrad on case No. 404/8091/21. 2021. https://reyestr.court.gov.ua/Review/102374040

Court of Appeal on case No. 922/95/20,[20] Decision of the Kyiv Court of Appeal on case No. 760/19180/23, the Decision of the Kyiv Court of Appeal on case No. 757/46845/19-c.[21] This examination allowed for an assessment of the current state of the problem and the identification of potential directions for improving legal regulation in the face of global challenges. The research into various aspects of forensic expertise in investigating crimes related to forged digital documents and cryptocurrencies enabled the identification of relevant areas for enhancing forensic practice. It also highlighted key needs such as the improvement of the regulatory framework, the upgrading of expert qualifications, and the provision of access to modern technologies. Furthermore, the study identified key structures and mechanisms that ensure effective investigations, including specialised units within law enforcement agencies and appropriate methodological approaches.

3. Results

Documents are considered items that contain information about circumstances of legal significance in proceedings. Special attention should be given to electronic documents, particularly cryptocurrencies. In Ukraine, the Law of Ukraine “On Virtual Assets” formalises cryptocurrency as an object of legal activity, along with the associated legal relations that arise from the use of this new type of electronic document. According to this law, the term “cryptocurrency” is synonymous with “virtual asset,” which aligns it with electronic documents having specific characteristics that require specialised forensic investigation. The law defines “virtual asset” as “an intangible good, which is an object of civil rights, holds value, and is represented by a collection of data in electronic form of type I.” The existence and transferability of virtual assets are guaranteed by a system that regulates their transactional relations (Figure 1).

[20] Decision of the Eastern Commercial Court of Appeal on case No. 922/95/20. 2020 https://reyestr.court.gov.ua/Review/93327784

[21] GJORGJEV, Jelena, RAMADHAN, Fajar and DHAMAYANA, Sonny. Blockchain forensics - unmasking anonymity in dark web transactions. *International Journal of Criminology and Sociology*, March 2025, vol. 14, pp. 68-75. ISSN: 1929-4409.

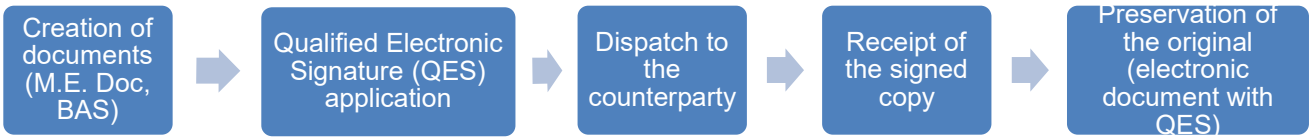

Figure 1. Digital document management scheme

Source: compiled by the authors based on Law of Ukraine "On Virtual Assets" No. 2074-IX.

3.1. Legal and Forensic Classification of Cryptocurrencies

A primary challenge in forensic investigations involving digital assets and electronic documents is the issue of anonymity. Cryptocurrencies, by design, offer pseudo-anonymity, meaning that while all transactions are recorded on the blockchain, the identity of the parties involved remains obscured unless additional investigative methods are employed. This anonymity is exploited by criminals to launder money, finance illegal activities, or conceal illicit transactions.[22] In contrast to traditional banking systems, which maintain records of account holders, cryptocurrency transactions do not necessarily have a clear link to an individual's real identity.

Investigators often face difficulties in tracing cryptocurrency transactions back to their origin, particularly when funds are moved through multiple wallets, mixing services, or decentralised exchanges. Another significant issue in forensic investigations is data integrity and security. Unlike physical evidence, digital evidence is susceptible to tampering, deletion or corruption, which necessitates the adoption of secure methods for the collection, preservation and analysis of electronic data.[23] Investigators must therefore employ specialised forensic tools to ensure the integrity of electronic evidence, such as cryptographic hashing techniques, write-blocking devices and blockchain analysis tools. Furthermore, regulatory gaps serve to further complicate forensic investigations. While some jurisdictions have developed legal frameworks to regulate cryptocurrency transactions, others lack clear policies, making cross-border investigations difficult. To address these challenges, forensic

[22] Decision of the Kyiv Court of Appeal on case No. 757/46845/19-c. 2021. https://reyestr.court.gov.ua/Review/95524461

[23] ZILE, Aelita, PALKOVA, Karina and VILKS, Andrejs. Study of the Influence of External Conditions and Materials on the Preservation of Hidden Prints under Water. *Pakistan Journal of Criminology*, April-June 2023, vol. 15, n.º2, pp. 305-322. ISSN: 2074-2738.

investigators must develop innovative approaches for tracking digital assets, authenticating digital documents, and ensuring the admissibility of electronic evidence in court.[24]

Real cases of crimes associated with cryptocurrency theft from exchanges, brokers, and electronic wallets encompass a broad range of activities, including fraud, extortion, and theft, all of which are facilitated through computer technologies. This necessitates the immediate development of forensic methodologies for investigating such crimes, identifying the crime objects, means of locating criminal activities, and analysing the primary methods and means of perpetrating these crimes. Furthermore, the sources from which information about digital traces arising from cryptocurrency theft is obtained require a detailed analysis.

3.2. Forensic Methods for Investigating Cryptocurrency Crimes

Specialised knowledge used in the investigation of cryptocurrency-related crimes includes expertise in network technologies and information systems, as well as hardware and software tools that assist in tracking the processes and features of criminal activities. One procedural tool for applying this specialised knowledge is forensic examination. The legal framework governing forensic analysis and expert reports plays a crucial role in determining the admissibility and reliability of forensic evidence in criminal investigations. The Law of Ukraine “On Forensic Expertise” establishes the legal basis for conducting forensic examinations by defining them as specialised investigations that rely on scientific, technical, and other expert knowledge to provide conclusions on matters of legal significance. These examinations are used to analyse documents, financial transactions, and digital evidence, among other forms of forensic data.

Furthermore, the Criminal Procedure Code of Ukraine delineates the status and rights of forensic experts, stating in Part 1 of Article 69 that an expert is a person with recognised scientific, technical, or other specialized knowledge who is authorised to conduct forensic examinations as prescribed by law. This means that experts must meet certain professional qualifications, including certification by state institutions, to ensure the credibility of their conclusions. However, the document also acknowledges

[24] ATLAM, Hany, EKURI, Ndifon, AZAD, Muhammad and LALLIE, Harjinder. Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics*, September 2024, vol. 13, n.º17, 3568. ISSN: 2079-9292.

the existence of legal gaps in defining the extent of expert authority and the procedural requirements for different types of forensic analyses. In order to address these gaps, the document proposes legislative amendments to establish clear standards for forensic examinations involving digital evidence and cryptocurrencies. Such individuals have the right to conduct investigations of objects, phenomena, and processes that contain information about the circumstances of criminal offences and to provide conclusions on issues that arise during criminal proceedings and fall within their field of expertise. Forensic examination in legal proceedings is a key form of utilising specialised knowledge conducted by entities engaged in forensic expert activity.[25] Experts from forensic units of judicial institutions and independent experts involved in investigative actions actively employ their professional knowledge. During an investigation, the primary tasks of forensic work include analysing accounting and tax documents, determining the extent of shortages or surpluses of material values and financial assets, and investigating transactions involving these, including all aspects of their accounting and interrelations in financial and economic agreements.[26] Consultation with a forensic expert regarding transactions with digital assets may arise in various situations, such as cryptocurrency theft through the hacking of an electronic wallet or online account on a cryptocurrency exchange.

One example of the involvement of forensic experts is case No. 922/95/20, which dealt with the forgery of digital documents and theft of cryptocurrencies. In case No. 495/10329/23 1-ks/495/2129/23, forensic experts conducted a thorough analysis of digital traces and documentation, which allowed for the identification of forgery and tracking of stolen cryptocurrencies. Through advanced forensic methods, experts were able to identify sources of falsification and determine the individuals involved in the crime. Another example is case No. 757/46845/19-c, where expert work focused on verifying the representation of cryptocurrency transactions in the accounting records of a company. The forensic expert analysed financial documents and transactions, uncovering discrepancies and possible attempts to conceal income through the use of cryptocurrencies.

The examination results served as substantial evidence in the judicial process,

[25] SPYTSKA, Liana. Analysis of the most unusual court decisions in the world practice in terms of the right to justice. *Social and Legal Studios*, 2022, vol. 5, n.º4, pp. 39-45. ISSN: 2617-4162.
[26] REZAEE, Zabihollah and WANG, Jim. Toward integration of blockchain, cryptocurrencies into forensic accounting education. *Journal of Forensic Accounting Research*, December 2024, vol. 9, n.º1, pp. 445–469. ISSN: 2380-2138.

helping to establish the truth and ensure a fair decision.[27] Thus, forensic expertise is a crucial tool for analysing cryptocurrency transactions, including their representation in declarations, accounting records, and the assessment of the movement of digital assets between counterparties. Forensic economists can verify the conformity of these transactions with market conditions and financial agreements, which allows for the establishment of the justification and legality of actions related to digital assets and the provision of objective conclusions in accordance with current legislation. One of the most effective methods for detecting traces of crimes involving the use of cryptocurrencies and their illicit use is conducting a telecommunications examination and, in some cases, a comprehensive telecommunications-computer-technical examination. This is due to the fact that traces of crimes in this sphere arise from external or internal illegal influences on telecommunications systems, individual electronic devices, software, or computer information, representing any changes in these objects that occurred as a result of the commission of a crime using computer technologies.[28]

The increasing complexity of forensic economic examination is determined not only by the growing popularity of this type of expertise but also by advances in scientific and technological progress, as well as the emergence of new types of digital assets and transactions, particularly the application of blockchain technology. This technology enables the creation of decentralised digital assets, including cryptocurrencies, and facilitates the development of innovative solutions in value exchange, authentication, information exchange, and investment.[29] Identification and collection of electronic evidence are crucial stages in the forensic economic examination process. This process involves the detection of relevant digital artefacts, such as electronic mail, documents, transaction logs, and metadata. Experts in this field must ensure the preservation of digital evidence to guarantee its integrity for subsequent analysis and

[27] MAULENOV, Kalybek, KUDUBAYEVA, Saule and UVALIYEVA, A. Studying a Face Search Method Based on the Idea of Sparse Data Representation by Generating Random Points. In: *SIST 2021 - 2021 IEEE International Conference on Smart Information Systems and Technologies* (article number 9465986). Institute of Electrical and Electronics Engineers, Nur-Sultan, 2021.
[28] KOZII, Vasyl. Criminal liability for illegal possession of cryptocurrency in Ukraine. *Social and Legal Studios,* March 2023, vol. 6, n.º1, pp. 33-40. ISSN: 2617-4170.
[29] SHUPLAT, Olena, SHEVCHENKO, Valentyna, LUTSIV, Nataliia, NEKRASOV, Serhii and HOVDA, Halyna. Financing the fixed assets reproduction of woodworking enterprises: innovation and investment aspect. *Financial and Credit Activity: Problems of Theory and Practice*, August 2022, vol. 4, n.º45, pp. 48-57. ISSN: 2306-4994.

presentation in court.[30] To address this task, it is necessary to utilise modern forensic tools and methods, including write-blocking devices, to prevent alterations of digital evidence during its collection. Furthermore, specialised software for data extraction and signature-based analysis allows for the recovery of deleted or hidden files, contributing to a more comprehensive understanding of the case. Forensic examiners must possess in-depth knowledge of these technologies to uncover complex financial operations and trace illegal activities on decentralised platforms.

3.3. Challenges and Prospects for Forensic Investigations of Digital Crimes

The challenge of blockchain and cryptocurrency in forensic economic examination primarily relates to the issue of pseudo-anonymity, which complicates tracking the owners of such transactions. Addressing this problem requires the development and enhancement of transaction analysis technologies and the use of clustering methods to identify users. Blockchain technology provides a high level of decentralisation, which complicates the identification of specific owners and transaction executors. The anonymity of cryptocurrencies, in particular, creates difficulties in tracking financial operations. Therefore, the development of transaction analysis algorithms that allow for the establishment of connections between wallet addresses and real individuals becomes an important tool in forensic analysis.[21]

Forensic economic examination at the pre-trial investigation stage is appointed in cases where the investigator has specific questions that can only be resolved using specialised knowledge and where the criminal proceeding materials contain sufficient data for conducting the examination. The investigator determines the timing of the examination appointment, considering each case's specifics. At the pre-trial investigation stage, forensic economic examination is appointed in the following cases: when the findings of financial audits of a company contradict other documents related to business transactions, necessitating expert analysis to determine the causes of discrepancies; when an auditor refuses to consider materials submitted by responsible parties due to their non-presentation or improper documentation; when a suspect or accused requests a forensic economic examination; when there are inconsistencies between the results of accounting audits; when the methods used by auditors or tax

[30] AVDEEVA, Galina and ŻYWUCKA-KOZLOWSKA, Elzbieta. Problems of using digital evidence in criminal justice of Ukraine and the USA. *Theory and Practice of Forensic Science and Criminalistics*, March 2023, vol. 1, n.º30, pp. 126-143. ISSN: 1993-0917.

inspectors to investigate a company's financial and economic activities are questionable; when a more detailed investigation of specific issues requiring specialised knowledge in accounting is needed; and when the need for forensic economic examination arises from the conclusions of experts in other fields (e.g., handwriting analysis).[31]

A forensic economic examination can be conducted based on the results of audits or documents and accounting records provided directly to the investigator by the company. If the forensic economist deems it necessary to obtain explanations from an auditor-accountant, they should request the investigator to interrogate the auditor with their participation. The materials provided to the expert should be sufficiently comprehensive to ensure a documented basis for establishing the extent of shortages or surpluses in inventory and cash within enterprises, institutions, organisations, and their separate divisions and for determining the period during which these discrepancies occurred. This also applies to justifying transactions related to the acquisition, storage, production, and sale of various assets and services and their representation in financial accounting.[32] The documentary basis must also support the disclosure of payroll, tax, and other compulsory payment operations, including corporate profit tax and value-added tax.

An essential element in conducting a forensic economic examination is the clear definition of the investigator's questions to the expert. To achieve this, the investigator must thoroughly understand the materials of the criminal proceedings, be familiar with the fundamental principles of economic expertise, and clearly understand its capabilities and limitations. In this context, it is important to apply and adapt methodologies used for analysing financial assets, as their characteristics are often similar to those of cryptocurrencies.

3.4. Role of Forensic Economic Examination in Digital Asset Investigations

Forensic economic examination of cryptocurrencies becomes crucial in the contemporary legal context as it enables the uncovering of complex financial schemes and illegal activities conducted through digital assets. Special attention should be paid

[31] CHORNA, Nelia. Development of Agrarian business in Ukraine under influence of world financial and economic crisis. *Actual Problems of Economics*, 2009, vol. 11, pp. 40-48. ISSN: 1993-6788.
[32] SPYTSKA, Liana. Prospects for the legalization of cryptocurrency in Ukraine, based on the experience of other countries. *Social and Legal Studios*, December 2023, vol. 6, n.º4, pp. 226-232. ISSN: 2617-4170.

to the features of the formation and transformation of digital traces when conducting a broad range of forensic examinations, such as technical document examination or identification of individuals and equipment.[33] For instance, when establishing a document created through copying or computer technology, it is necessary to consider the specifics of the creation process and the potential for detecting forgery. This is evident from the analysis of existing legal practice, particularly from the case materials of No. 991/2747/22. Similarly, identifying the individual who created a text or image using a computer or determining the type and identification of computer equipment from produced documents requires the ability to distinguish digital traces from real artefacts.

Expert investigations are crucial for establishing the fact of forgery and uncovering manufacturing methods when counterfeit documents, such as licences or stamps with special security features, are examined. For instance, in case No. 404/8091/21, involving an excise stamp used for marking tobacco products, the expert determined that all background images and markings were applied using high-printing technologies. Consequently, given these findings, the investigator deemed it necessary to impose a seizure on the aforementioned property. Modern technologies allow for the imitation of security elements; hence, document examination now includes not only the analysis of materials and manufacturing technologies but also the detection of concealed security features.[34] The comprehensive use of computer-technical methods in forensic examinations enables the detection of even the most sophisticated forgery attempts, which is critical in combating crimes related to digital technologies.

Comprehensive expertise, as part of forensic investigation, has unique capabilities for addressing complex issues, such as establishing the use of genuine paper document elements to create electronic versions. This includes the complete conversion of a document into an electronic format and the partial use of its elements, such as seals, signatures, or stamps. Therefore, the investigation of electronic document forgery requires a holistic approach and the use of various expert

[33] RAZA, Syed Atir, SHAIKH, Mehwish and TAHIRA, Khadija. Cryptocurrency investigations in digital forensics: Contemporary challenges and methodological advances. *Information Dynamics and Applications*, July 2023, vol. 2, n.º3, pp. 126-134. ISSN: 2958-1494.

[34] TSVYETKOV, Andriy. Legal regulation of cryptocurrencies in Europe: Challenges of harmonisation and development prospects. *Scientific Journal of the National Academy of Internal Affairs*, November 2024, vol. 29, n.º. 4, pp. 47-60. ISSN: 2410-3594.

methodologies. Forensic economic examination of cryptocurrencies is a relatively new but simultaneously modern and promising field within forensic expertise. The effectiveness of investigating crimes involving cryptocurrencies and crimes where cryptocurrency is the subject of illegal encroachment largely depends on the contemporary capabilities and quality of forensic examinations. Current legislation, specifically the Law of Ukraine “On Forensic Expertise”, lacks a clear definition of the status and procedures for conducting comprehensive examinations. This creates challenges in understanding and applying these investigations in the practice of criminal investigations within the business sector. The only mention of comprehensive examination is found in the Order of the Ministry of Justice of Ukraine, where this type of examination is interpreted as a study involving various specialised knowledge to resolve a common task. Expert institutions and qualified specialists from other central executive authorities or specialised services not belonging to state expert institutions may be involved in such comprehensive examinations when necessary.

To clarify the status of comprehensive, repeated, additional, and commission-based examinations, Article 69 of the Criminal Procedure Code of Ukraine is proposed to be amended as follows: “Forensic experts may conduct initial, repeated, additional, comprehensive, and commission-based forensic examinations”. This amendment would help avoid situations where expert conclusions become contradictory, or their evidence is rendered inadmissible in legal proceedings. Thus, expert investigations are an exceptionally crucial component of the judicial process, as they ensure the accuracy, depth, and completeness of analysis. Expert opinions constitute significant evidence, which is meticulously regulated and substantially contributes to legal practice. Forensic investigations rely on specialized tools for evidence collection. However, their application faces limitations due to time constraints, expertise gaps, and evolving technological challenges. Consequently, improving forensic practices to adapt to contemporary technological realities in crimes is highly relevant.

The forensic practice in digital documents and cryptocurrencies faces challenges due to the lack of a standardized framework for conducting economic examinations. This lack of a cohesive methodology leads to inconsistencies in investigations, hindering comparisons across diverse cases. To address this, a study proposes an amendment to the Criminal Procedure Code that would formally recognize advanced forensic techniques. This would include explicit definitions of comprehensive, repeated, additional, and commission-based forensic examinations, ensuring forensic

experts can conduct in-depth investigations while maintaining high legal and procedural validity.

Furthermore, the rapid evolution of financial crimes and the increasing complexity of digital assets necessitates continuous updating of forensic expert training and certification. Experts require advanced technical competencies to conduct thorough investigations and detect illicit activities involving digital assets. Incorporating specialized training programs within forensic education is crucial to equip professionals with the necessary tools and methodologies to address the evolving threats posed by financial and cybercrime investigations.[35]

A well-defined regulatory framework is essential for the efficacy of forensic investigations in cryptocurrency-related crimes. This should include clearer legal provisions for transaction monitoring, cryptocurrency wallet identification, and international cooperation in forensic investigations. A harmonised international legal approach is necessary to combat financial crimes effectively. Regulatory adjustments should focus on facilitating cross-border investigations, ensuring forensic expertise can be applied efficiently in cases involving international cryptocurrency transactions and digital fraud.[36]

To address these issues, legislative reforms, training initiatives, and methodological advancements are needed. The evolving nature of digital financial crime underscores the need for continuous improvements in forensic methodologies, expert qualifications, and legal regulations to ensure forensic practice remains a reliable tool for justice.

4. Discussion

4.1. The Importance of Forensic Expertise in Digital Crime Investigations

The findings of this study emphasize the pivotal role of forensic expertise in the investigation of crimes pertaining to the forgery of digital documents and cryptocurrencies. The analysis demonstrates that forensic economic, technical, and computer-technical examinations are indispensable in the identification and

[35] MAULENOV, Kalybek, KUDUBAYEVA, Saule and RAZAKHOVA, Bibigul. Modern Problems of Face Recognition Systems and Ways of Solving Them. *Revue d'Intelligence Artificielle*, February 2023, vol. 37, n.º1, pp. 209-214. ISSN: 0992-499X

[36] BOTHA, Johannes, BOTHA, Danielle and LEENEN, Louise. An analysis of crypto scams during the Covid-19 pandemic: 2020-2022. *Proceedings of the 18th International Conference on Cyber Warfare and Security,* February 2023, vol.18, n.º1, pp. 39-48. ISSN: 2048-9889.

substantiation of digital forgeries and illicit cryptocurrency transactions. However, a key issue that remains unresolved is the lack of universally accepted standards for forensic cryptocurrency investigations.[37] One of the primary challenges facing forensic investigators is the legal admissibility of blockchain-based forensic evidence. While blockchain technology provides a transparent and immutable record of transactions, forensic analysts must contend with algorithmic biases and false positives in clustering heuristics. In addition, the increasing sophistication of crypto obfuscation techniques, such as mixing services and privacy-enhancing cryptocurrencies, presents substantial forensic challenges.[38]

In comparison with the results of other researchers, S. Samdani and A. Malik[39] also highlight that the object of investigation considers the nature of the traces and the boundaries of the expert's competence. This corroborates the conclusion that a comprehensive analysis requires consideration of all components of the hardware and software system used in document creation. The study results indicate substantial differences between the direct objects of technical document examination and computer-technical examination. In technical document examination, the focus is on the properties of the printer's mark-making mechanisms, whereas in computer-technical examination, the emphasis is on the software used for operating the printer.

4.2. The Impact of Cryptocurrency Anonymity on Forensic Investigations

According to other researchers, such as J.G. Botha and L. Leenen,[40] it is important to consider the properties of the entire hardware-software complex, including the computer, printer, and software. This supports the findings that a holistic approach to the investigation enables a more precise determination of the document origin and the identification of individuals who had access to the equipment used for its creation. Therefore, it can be concluded that a comprehensive approach to analysing

[37] FRÖWIS, Michael, GOTTSCHALK, Thilo, HASLHOFER, Bernhard, RÜCKERT, Christian and PESCH, Paulina. Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation*, June 2020, vol. 33, 200902. ISSN: 2666-2825.
[38] AGARWAL, Udit, RISHIWAL, Vinay, TANWAR, Sudeep and YADAV, Mano. Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, December 2023, vol. 34, n.º2, e2255. ISSN: 1055-7148.
[39] SAMDANI, Sans and MALIK, Ausaf. Understanding the role of data privacy in the investigation and prosecution of digital crimes and real crimes. *NIU International Journal of Human Rights*, December 2023, vol. 10, pp. 338-352. ISSN: 2394-0298.
[40] BOTHA, Johannes and LEENEN, Louise. Cryptocurrency-crime investigation: Fraudulent use of bitcoin in a divorce case. *Proceedings of the 19th International Conference on Cyber Warfare and Security*, March 2024, vol.19, n.º1, pp. 34-42. ISSN: 2048-9889.

documents on electronic media and their machine copies provides a more detailed understanding of the document creation process and can be valuable for determining the source of their origin and the individuals with access to the relevant equipment. Researchers thus agree on the concept of specialised knowledge and the purpose of forensic examinations in investigating crimes related to the forgery of digital documents and cryptocurrencies.

In the context of this issue, S. Seo et al.[41] highlight the necessity of involving specialists in utilising technical means for recording the progress and results of investigative actions and participating in the interrogation of suspects and experts. This is corroborated by S. Singh and R. Kumar,[42] who point to the need for comprehensive forensic-economic and computer-technical examinations to investigate financial and economic transactions, document changes, and other aspects. As noted in the research results, electronic and paper-based documents in forensic economic examination reflect actual business operations and financial-economic outcomes. The results of the study may reveal instances of data not being recorded in accounting documents or being inaccurately represented.

Analysing the results regarding forged documents, it becomes evident that a substantial number of such documents become subjects of forensic-technical examination. The study shows that this type of examination explores various aspects of documents, such as attributes, stamps and seal imprints, text creation methods, and additional records. The specific purpose of the technical examination depends on several factors, including the widespread use of computer technology in document creation and the production of stamps and seals using foreign technologies.[43] Other researchers, including J. Yiye et al.,[44] also note a considerable number of forged documents that become subjects of forensic-technical examination, confirming the

[41] SEO, Seunghee, SEOK, Byoungjin and LEE, Changhoon. Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing*, January 2023, vol. 79, pp. 9467-9485. ISSN: 1573-0484.

[42] SINGH, Satyendra and KUMAR, Rajesh. Image forgery detection: Comprehensive review of digital forensics approaches. *Journal of Computational Social Science*, April 2024, vol. 7, pp. 877-915. ISSN: 2432-2725.

[43] KHODA, Valentyn, LESHCHUK, Nadiia, TOPALOV, Andrii, ROBOTKO, Serhii, KLYMENKO, Oleksandr and NEKRASOV, Serhii. Computerized Lathe Control System based on Internet of Things Technology. In: *Proceedings - International Conference on Advanced Computer Information Technologies, ACIT* (pp. 674–677). Institute of Electrical and Electronics Engineers, Ceske Budejovice, 2024. ISSN: 2770-5218.

[44] YIYE, Justina, MUSTAPHA, Rabi, AHMAD, Muhammad Aminu, BASSI, Haruna. Digital forensic investigation of cyberstalking and social media harassment using network forensic analysis. *Journal of Science Technology and Education*, September 2022, vol. 10, n.º. 3, pp.1-10. ISSN: 2277-0011.

conclusions obtained in this study. They indicate that this type of examination involves a comprehensive analysis of violations in the creation of documents as a whole and in their individual parts. Further analysis of the results shows that one common type of forgery is the creation of digital records and signatures using computer technology. In such cases, experts analyse, for example, the strokes of a signature made with a laser printer, which visually are hardly distinguishable from strokes made with a black ink gel pen. However, upon microscopic analysis, the morphological features of the strokes easily distinguish the different methods of creating the signature. M. Varalakshmi and S. Petikam[45] confirm this, noting that digital signatures and records created using computer technology can be detected through microscopic analysis. Their conclusions support our findings that the morphological features of the strokes enable experts to distinguish digital signatures from those created using traditional methods.

4.3. The Structure and Components of the Information Field in Digital Documents

A detailed analysis of each attribute, the printing materials used, and the technical means of document creation allow for the disclosure of methods for applying text, forming characters, and creating imprints. This supports the thesis that the structure of the information field of a document consists of various components, each of which requires separate consideration for a complete understanding of the document creation process. Other researchers have also noted this aspect. For example, G. Horsman and N. Sunde,[46] A. Singh et al.[47] examined the structure of the information field of a document from various components, including attributes, printing materials, and technical means used. Our results are consistent with their findings, demonstrating that the analysis of each part of a document reveals the methods of its creation. The research results suggest that the use of blockchain technology can ensure maximum security, integrity, and transparency in the audit process, which helps determine the origin of documents and prevent potential cases of fraud in digital forensic systems.

[45] VARALAKSHMI, M, and PETIKAM, Sailaja. Role of cyber forensic expert in crime investigation. *International Journal of Research in Management Sciences (IJRMS),* July 2022, vol. 10, n.º1, pp. 14-27. ISSN: 2347-5943.
[46] HORSMAN, Graeme and SUNDE, Nina. Unboxing the digital forensic investigation process. *Science & Justice*, March 2022, vol. 62, n.º2, pp. 171-180. ISSN: 1355-0306.
[47] SINGH, Arpita, SINGH, S, SINGH, Nilu and NAYAK, Sandeep. An algorithm for crime detection in digital forensics. *Journal of Survey in Fisheries Sciences*, April 2023, vol. 10, n.º3, pp. 1281-1290. ISSN: 2368-7487.

This platform guarantees high integrity, traceability, and immutability of data, contributing to the improvement of the security of forensic evidence. These conclusions are corroborated by V. Potdar et al.,[48] who also identified that blockchain technology ensures maximum security and transparency, which is crucial for fraud prevention.

In investigating methods to protect cryptocurrency owners, it was discovered that crypto wallets offer various approaches to ensuring security and privacy.[49] For example, the Trezor wallet creates hidden wallets that do not appear in the standard interface, providing an additional level of privacy. Moreover, some wallets feature automatic transfer functions to other wallets under certain conditions, using various algorithms for key and seed word generation, making their operation even more reliable and difficult to breach. These results are supported by S. Taylor et al.,[50] who present different approaches to protecting cryptocurrency owners and ensuring additional privacy and security. The obtained results align with their studies, emphasising the importance of complex algorithms for key generation and the use of hidden wallets to enhance protection. For instance, M. Tampubolon[51] points to the critical importance of continuously updating legislation and regulatory frameworks in the field of digital security, especially in connection with the increasing complexity and development of digital face editing methods. A.S.N. Mantiri and E. Sumanti[52] highlight those new technologies pose challenges for forensic examination, which plays a key role in detecting digital manipulation of facial photographs. In light of these statements, it is important to emphasise that considering the continuous development of image editing technologies, it is essential to have effective forensic methods to detect manipulations.

4.4. Prospects for Improving Forensic Expertise in Ukraine

[48] POTDAR, Veena, SANTHOSH, Lavanya, HRITHIK, H, KANISH, B, HARSHA, C and MAHANTESH, S. Forensic evidences made tamper-proof using block chain. *International Journal of All Research Education and Scientific Methods (IJARESM)*, July 2023, vol. 11, n.º7, pp. 34-45. ISSN: 2455-6211.
[49] DE-ALMEIDA-E-PAIS, José Edmundo, RAPOSO, Hugo, FARINHA, José Torres, CARDOSO, Antonio J. Marques, LYUBCHYK, Svitlana and LYUBCHYK, Sergiy. Measuring the Performance of a Strategic Asset Management Plan through a Balanced Scorecard. *Sustainability (Switzerland)*, November 2023, vol. 15, n.º22, 15697. ISSN: 2071-1050.
[50] TAYLOR, Sarah, KIM, Steve, ARIFFIN, Khairol Akram Zainol and ABDULLAH, Siti Norul Huda Sheikh. A comprehensive forensic preservation methodology for cryptowallets. *Forensic Science International: Digital Investigation*, October–December 2022, vol. 42-43, 301477. ISSN: 2666-2817.
[51] TAMPUBOLON, Manotar. Digital face forgery and the role of digital forensics. *International Journal for the Semiotics of Law*, August 2023, vol. 37, pp. 753-767. ISSN: 1572-8722.
[52] MANTIRI, Astria Santa Natalia and SUMANTI, Elvis. The role of digital forensics in the preliminary investigation. *Klabat Accounting Review*, June 2022, Vol.3, n.º1, pp. 79-95. ISSN: 2721-723X.

The analysis of research into the role of digital forensic experts in uncovering, interpreting, and presenting digital evidence has shown that their work is essential for ensuring that evidence meets legal standards. The results of the study highlight the importance of a specialised approach to digital evidence in law enforcement, where digital forensics experts ensure the authenticity and integrity of evidence. Other researchers have also noted this aspect. Therefore, the detection of forgery in electronic documents is a task that requires the development of new methods for effective resolution. This is a complex process, as conventional methods used in diagnostic and identification studies in handwriting analysis or technical forensic examination of stamps and seals are not always effective in this context. In addition, the computer and printer software used for printing can influence the appearance of an electronic document, complicating the forgery detection process. Forensic examination is central in investigating crimes related to the forgery of digital documents and cryptocurrencies.[53] Its importance is due to the complexity and technical sophistication of such crimes, which require specialised knowledge for the identification, authentication, and analysis of digital evidence. Forensic experts provide a reliable evidential basis, assist investigative agencies in uncovering forgery mechanisms, and track suspicious cryptocurrency transactions.[54] They also offer consultations during court proceedings, aiding in the accurate interpretation of the technical aspects of the case.

5. Conclusions

The analysis of cryptocurrency transactions necessitates the expertise of forensic economists, who play a critical role in ensuring compliance with market conditions and financial agreements. This contributes to legal clarity regarding digital transactions. The detection of cryptocurrency-related crimes necessitates advanced forensic methods, particularly telecommunication forensic examinations and, where necessary, comprehensive telecommunication-computer-technical examinations. These approaches facilitate in-depth investigations of digital traces, enabling the identification

[53] RYSIN, Maria and SUKH, Yaroslav. Digital solutions as an effective approach to combat corruption in public procurement. *Democratic Governance*, 2024, vol. 17, n.º2, pp. 18-29. ISSN: 2070-4038.
[54] SILAGADZE, Avtandil, GAGANIDZE, Giorgi, ZUBIASHVILI, Tamaz and ATANELISHVILI, Tamar. Cryptocurrency regulation in post-Soviet countries: Balancing global practices and local specifics. *Scientific Bulletin of Mukachevo State University. Series "Economics"*, 2025, vol. 12, n.º1, pp. 103-117. ISSN: 2313-8114.

of fraudulent activities. A key aspect of forensic document analysis is determining whether documents have been altered using digital editing tools or reproduction technologies. Additionally, forensic examination must establish the origin of digital content, identify the creators of electronic texts and images, and trace the devices used for document forgery. The forensic analysis of video, audio, and photographic evidence further aids in authenticating digital records and reconstructing original file formats.

A significant challenge encountered in the context of forensic economic investigations of blockchain-based assets pertains to the absence of a standardised methodology. However, it is noteworthy that forensic experts have the capacity to adapt extant financial forensic techniques for the analysis of cryptocurrency transactions. The efficacy of forensic economic examinations is contingent upon the development of sophisticated investigative tools and the calibre of expert analysis. In light of the intricacy inherent in blockchain and cryptocurrency-related crimes, the continuous enhancement of forensic technologies is imperative for the enhancement of investigative precision. The development of a unified conceptual framework for forensic economic examinations and the standardisation of expert methodologies are necessary steps to strengthen legal clarity and procedural consistency. The establishment of a structured classification of forensic examinations would ensure uniformity in investigative practices and facilitate the accurate assessment of digital assets within the broader forensic system. The collection and evaluation of evidential information require specialised knowledge. It is crucial to correctly select the type of forensic examination based on the nature of the crime and the methods used to commit it. Thus, it is important to enshrine in legislation the possibility of conducting various types of forensic examinations to avoid doubts about the compliance of their conclusions with legal standards. To clarify the status of not only comprehensive but also supplementary, additional, and commission examinations, it is recommended that Article 69 of the Criminal Procedure Code of Ukraine be amended. This would solidify the status of these types of examinations at the legislative level and prevent situations where expert conclusions become contradictory, or their evidence is deemed inadmissible in court.

Future research prospects include the development and implementation of new methods and tools for more effective detection and investigation of forged electronic documents, examining the impact of new technologies digital forensics, and formulating recommendations for their use. Furthermore, there is a need to explore the

legal aspects of using technologies such as blockchain in the collection and analysis of digital evidence.

References

AGARWAL, Udit, RISHIWAL, Vinay, TANWAR, Sudeep and YADAV, Mano. Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, December 2023, vol. 34, n.º2, e2255. ISSN: 1055-7148

APAKHAYEV, Nurlan, KOISHYBAIULY, Kuanysh, KHUDAIBERDINA, Gulnura, URISBAYEVA, Ainur, KHAMZINA, Zhanna and BURIBAYEV, Yermek. Legal basis for ensuring freedom of access to information on the operation of state administration bodies in Kazakhstan. *Journal of Advanced Research in Law and Economics*, 2017, vol. 8, n.º3, pp. 722-729. ISSN: 2068-696X.

ATLAM, Hany, EKURI, Ndifon, AZAD, Muhammad and LALLIE, Harjinder. Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics*, September 2024, vol. 13, n.º17, 3568. ISSN: 2079-9292.

AVDEEVA, Galina and ŻYWUCKA-KOZLOWSKA, Elzbieta. Problems of using digital evidence in criminal justice of Ukraine and the USA. *Theory and Practice of Forensic Science and Criminalistics*, March 2023, vol. 1, n.º30, pp. 126-143. ISSN: 1993-0917.

BOTHA, Johannes and LEENEN, Louise. Cryptocurrency-crime investigation: Fraudulent use of bitcoin in a divorce case. *Proceedings of the 19th International Conference on Cyber Warfare and Security,* March 2024, vol.19, n.º1, pp. 34-42. ISSN: 2048-9889.

BOTHA, Johannes, BOTHA, Danielle and LEENEN, Louise. An analysis of crypto scams during the Covid-19 pandemic: 2020-2022. *Proceedings of the 18th International Conference on Cyber Warfare and Security,* February 2023, vol.18, n.º1, pp. 39-48. ISSN: 2048-9889.

CHORNA, Nelia. Development of Agrarian business in Ukraine under influence of world financial and economic crisis. *Actual Problems of Economics*, 2009, vol. 11, pp. 40-48. ISSN: 1993-6788.

DE-ALMEIDA-E-PAIS, José Edmundo, RAPOSO, Hugo, FARINHA, José Torres, CARDOSO, Antonio J. Marques, LYUBCHYK, Svitlana and LYUBCHYK, Sergiy. Measuring the Performance of a Strategic Asset Management Plan through a Balanced Scorecard. *Sustainability (Switzerland)*, November 2023, vol. 15, n.º22, 15697. ISSN: 2071-1050.

DUPUIS, Daniel and GLEASON, Kimberly. Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, August 2020, vol. 28, n.º1, pp. 60-74. ISSN: 1359-0790.

DZYUBLENKO, Iryna and ZHABINETS, Nataliia. Current trends in international organised crime combating cooperation. *Foreign Affairs*, 2024, vol. 34, n.º1, pp. 71-78. ISSN: 2663-2675.

FRÖWIS, Michael, GOTTSCHALK, Thilo, HASLHOFER, Bernhard, RÜCKERT, Christian and PESCH, Paulina. Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation*, June 2020, vol. 33, 200902. ISSN: 2666-2825.

GJORGJEV, Jelena, RAMADHAN, Fajar and DHAMAYANA, Sonny. Blockchain forensics - unmasking anonymity in dark web transactions. *International Journal of Criminology and Sociology*, March 2025, vol. 14, pp. 68-75. ISSN: 1929-4409.

HORSMAN, Graeme and SUNDE, Nina. Unboxing the digital forensic investigation process. *Science & Justice,* March 2022, vol. 62, n.º2, pp. 171-180. ISSN: 1355-0306.

KHODA, Valentyn, LESHCHUK, Nadiia, TOPALOV, Andrii, ROBOTKO, Serhii, KLYMENKO, Oleksandr and NEKRASOV, Serhii. Computerized Lathe Control System based on Internet of Things Technology. In: *Proceedings - International Conference on Advanced Computer Information Technologies, ACIT* (pp. 674–677). Institute of Electrical and Electronics Engineers, Ceske Budejovice, 2024. ISSN: 2770-5218.

KHOMUTENKO, Vira and KHOMUTENKO, Alla. The dual nature of forensic expertise. *Law Herald*, June 2022, vol. 2, pp. 139-147.

KOZII, Vasyl. Criminal liability for illegal possession of cryptocurrency in Ukraine. *Social and Legal Studios*, March 2023, vol. 6, n.º1, pp. 33-40. ISSN: 2617-4170.

MANTIRI, Astria Santa Natalia and SUMANTI, Elvis. The role of digital forensics in the preliminary investigation. *Klabat Accounting Review,* June 2022, Vol.3, n.º1, pp. 79-95. ISSN: 2721-723X.

MAULENOV, Kalybek, KUDUBAYEVA, Saule and RAZAKHOVA, Bibigul. Modern Problems of Face Recognition Systems and Ways of Solving Them. *Revue d'Intelligence Artificielle*, February 2023, vol. 37, n.º1, pp. 209-214. ISSN: 0992-499X.

MAULENOV, Kalybek, KUDUBAYEVA, Saule and UVALIYEVA, A. Studying a Face Search Method Based on the Idea of Sparse Data Representation by Generating Random Points. In: *SIST 2021 - 2021 IEEE International Conference on Smart Information Systems and Technologies* (article number 9465986). Institute of Electrical and Electronics Engineers, Nur-Sultan, 2021.

METELSKYI, Ihor and KRAVCHUK, Mariana. Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 2023, vol. 1, n.º1, pp. 18-25. ISSN: 2786-8761.

PASHYNSKA, Iryna. *Theoretical and methodological foundations of investigation of organized crime in the field of economic activity*. PhD dissertation, Kharkiv National University of Internal Affairs, Kharkiv, 2023.

POTDAR, Veena, SANTHOSH, Lavanya, HRITHIK, H, KANISH, B, HARSHA, C and MAHANTESH, S. Forensic evidences made tamper-proof using block chain. *International Journal of All Research Education and Scientific Methods (IJARESM),* July 2023, vol. 11, n.º7, pp. 34-45. ISSN: 2455-6211.

RAZA, Syed Atir, SHAIKH, Mehwish and TAHIRA, Khadija. Cryptocurrency investigations in digital forensics: Contemporary challenges and methodological advances. *Information Dynamics and Applications*, July 2023, vol. 2, n.º3, pp. 126-134. ISSN: 2958-1494.

REZAEE, Zabihollah and WANG, Jim. Toward integration of blockchain, cryptocurrencies into forensic accounting education. *Journal of Forensic Accounting Research*, December 2024, vol. 9, n.º1, pp. 445–469. ISSN: 2380-2138.

RYSIN, Maria and SUKH, Yaroslav. Digital solutions as an effective approach to combat corruption in public procurement. *Democratic Governance*, 2024, vol. 17, n.º2, pp. 18-29. ISSN: 2070-4038.

SAMDANI, Sans and MALIK, Ausaf. Understanding the role of data privacy in the investigation and prosecution of digital crimes and real crimes. *NIU International Journal of Human Rights*, December 2023, vol. 10, pp. 338-352. ISSN: 2394-0298.

SELIM, Aybeyan and ALI, İlker. The role of digital forensic analysis in modern investigations. *Journal of Emerging Computer Technologies,* December 2024, vol. 4, n.º. 1, pp. 1-5. ISSN: 2757-8267.

SEO, Seunghee, SEOK, Byoungjin and LEE, Changhoon. Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing,* January 2023, vol. 79, pp. 9467-9485. ISSN: 1573-0484.

SEZONOV, Viktor. The concept of the document in Forensic science. *Law and Safety,* March 2024, vol. 84, n.º1, pp. 215-224. ISSN: 2617-2933.

SHUPLAT, Olena, SHEVCHENKO, Valentyna, LUTSIV, Nataliia, NEKRASOV, Serhii and HOVDA, Halyna. Financing the fixed assets reproduction of woodworking enterprises: innovation and investment aspect. *Financial and Credit Activity: Problems of Theory and Practice*, August 2022, vol. 4, n.º45, pp. 48-57. ISSN: 2306-4994.

SILAGADZE, Avtandil, GAGANIDZE, Giorgi, ZUBIASHVILI, Tamaz and ATANELISHVILI, Tamar. Cryptocurrency regulation in post-Soviet countries: Balancing global practices and local specifics. *Scientific Bulletin of Mukachevo State University. Series "Economics"*, 2025, vol. 12, n.º1, pp. 103-117. ISSN: 2313-8114.

SINGH, Arpita, SINGH, S, SINGH, Nilu and NAYAK, Sandeep. An algorithm for crime detection in digital forensics. *Journal of Survey in Fisheries Sciences*, April 2023, vol. 10, n.º3, pp. 1281-1290. ISSN: 2368-7487.

SINGH, Satyendra and KUMAR, Rajesh. Image forgery detection: Comprehensive review of digital forensics approaches. *Journal of Computational Social Science*, April 2024, vol. 7, pp. 877-915. ISSN: 2432-2725.

SPYTSKA, Liana. Analysis of the most unusual court decisions in the world practice in terms of the right to justice. *Social and Legal Studios*, 2022, vol. 5, n.º4, pp. 39-45. ISSN: 2617-4162.

SPYTSKA, Liana. Prospects for the legalization of cryptocurrency in Ukraine, based on the experience of other countries. *Social and Legal Studios*, December 2023, vol. 6, n.º4, pp. 226-232. ISSN: 2617-4170.

TAMPUBOLON, Manotar. Digital face forgery and the role of digital forensics. *International Journal for the Semiotics of Law,* August 2023, vol. 37, pp. 753-767. ISSN: 1572-8722.

TAYLOR, Sarah, KIM, Steve, ARIFFIN, Khairol Akram Zainol and ABDULLAH, Siti Norul Huda Sheikh. A comprehensive forensic preservation methodology for cryptowallets. *Forensic Science International: Digital Investigation,* October–December 2022, vol. 42-43, 301477. ISSN: 2666-2817.

TROZZE, Arianna, KAMPS, Josh, AKARTUNA, Eray Arda, HETZEL, Florian, KLEINBERG, Bennett, DAVIES, Toby and JOHNSON, Shane. Cryptocurrencies and future financial crime. *Crime Science,* January 2022, vol. 11, 1. ISSN: 2193-7680

TSVYETKOV, Andriy. Legal regulation of cryptocurrencies in Europe: Challenges of harmonisation and development prospects. *Scientific Journal of the National Academy of Internal Affairs*, November 2024, vol. 29, n.º. 4, pp. 47-60. ISSN: 2410-3594.

VARALAKSHMI, M, and PETIKAM, Sailaja. Role of cyber forensic expert in crime investigation. *International Journal of Research in Management Sciences (IJRMS*), July 2022, vol. 10, n.º1, pp. 14-27. ISSN: 2347-5943.

YIYE, Justina, MUSTAPHA, Rabi, AHMAD, Muhammad Aminu, BASSI, Haruna. Digital forensic investigation of cyberstalking and social media harassment using network forensic analysis. *Journal of Science Technology and Education,* September 2022, vol. 10, n.º. 3, pp.1-10. ISSN: 2277-0011.

ZHERDIEV, Vladyslav. *Forensic characteristics and features of investigation of criminal offenses committed in the field of economic activity using counterfeit documents*. PhD dissertation, Kharkiv National University of Internal Affairs, Kharkiv, 2024.

ZILE, Aelita, PALKOVA, Karina and VILKS, Andrejs. Study of the Influence of External Conditions and Materials on the Preservation of Hidden Prints under Water. *Pakistan Journal of Criminology*, April-June 2023, vol. 15, n.º2, pp. 305-322. ISSN: 2074-2738.

Case Law

Decision of the Eastern Commercial Court of Appeal on case No. 922/95/20. 2020 https://reyestr.court.gov.ua/Review/93327784

Decision of the High Anti-Corruption Court on case No. 991/2747/22. 2022. https://reyestr.court.gov.ua/Review/105596649

Decision of the Kirovskyi District Court of Kirovohrad on case No. 404/8091/21. 2021. https://reyestr.court.gov.ua/Review/102374040

Decision of the Kyiv Court of Appeal on case No. 757/46845/19-c. 2021. https://reyestr.court.gov.ua/Review/95524461

Decision of the Kyiv Court of Appeal on case No. 760/19180/23. 2023. https://reyestr.court.gov.ua/Review/114895442

Decision of the Odesa Court of Appeal on case No. 495/10329/23 1-ks/495/2129/23. 2023. https://reyestr.court.gov.ua/Review/114307295

Decision of the Transcarpathian Court of Appeal on case No. 308/2124/20. 2020. https://reyestr.court.gov.ua/Review/88922416

Legislative documents

Criminal Procedural Code of Ukraine No. 4651-VI. 2013. https://zakon.rada.gov.ua/laws/show/4651-17#Text

Law of Ukraine “On Forensic Expertise” No. 4038-XII. 1994.

https://zakon.rada.gov.ua/laws/show/4038-12#Text
Law of Ukraine "On Virtual Assets" No. 2074-IX. 2023. https://zakon.rada.gov.ua/laws/show/2074-20#Text
Order of the Ministry of Justice of Ukraine "On Approval of the Instruction on Appointment and Conduct of Forensic Examinations and Expert Studies and Scientific and Methodological Recommendations on Preparation and Appointment of Forensic Examinations and Expert Studies" No. 53/5. 1998. https://zakon.rada.gov.ua/laws/show/z0705-98#Text

Data de submissão do artigo: 04/02/2025

Data de aprovação do artigo: 26/04/2025

Edição e propriedade:
Universidade Portucalense Cooperativa de Ensino Superior, CRL
Rua Dr. António Bernardino de Almeida, 541 - 4200-072 Porto
Email: upt@upt.pt