Journal of Theoretical and Applied Information Technology
15th March 2026. Vol.104. No.5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PECULIARITIES OF THE USE OF BLOCKCHAIN TECHNOLOGIES IN DOCUMENTING AND AUTHENTICATION OF EVIDENCE DURING CYBER INVESTIGATIONS

VIACHESLAV KULIUSH[1], VLADYSLAV VEKLYCH[2], NATALIIA IAKYMCHUK[3], SERGIY MARCHEVSKYI[4], IVAN KURYLIN[5]

[1] Doctor of Philosophy in Law, Head of the Cybercrime Countermeasures Department in the city of Kyiv, National Police of Ukraine, Kyiv, Ukraine; ORCID: 0009-0007-2131-1413
[2] Doctor of Law, Associate Professor, Professor of the Department of Theory of State and Law and Constitutional Law, Prince Volodymyr the Great Educational and Scientific Institute of Law, Private Joint-Stock Company "Higher Educational Institution "Interregional Academy of Personnel Management", Kyiv, Ukraine; ORCID: 0000-0003-2608-6781
[3] Doctor of Law Sciences, Professor of the Department of Financial Law, Educational and Scientific Institute of Law, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine; ORCID: 0000-0002-4848-2323
[4] PhD in Juridical Sciences, National Academy of Internal Affairs, Kyiv, Ukraine; ORCID: 0000-0002-3623-4461
[5] PhD in Law, Associate Professor of the Department of Criminalistics, Educational and Scientific Institute of Law and Psychology, Kyiv, Ukraine; ORCID: 0000-0002-5672-3959
Emails: [1] Kylius1706@gmail.com; [2] vladyslavchernii2@gmail.com; [3] iakymchukk28@gmail.com; [4] Marchevskyii@gmail.com; [5] Kurylin.ivan1@gmail.com

ABSTRACT

As cybercrimes rise, effective methods to preserve and evaluate digital evidence are needed. This study examines how blockchain technology might enhance cyber investigation, digital evidence capture, and verification. This investigation compares public and permissioned blockchain systems' legal and forensic reliability. Legal and forensic comparisons were conducted in Estonia, Germany, Ukraine, and the Netherlands. The inquiry focused on phishing, ransomware, and data breaches. About 300 instances were examined. The Hyperledger and Ethereum systems use SHA-256 and Keccak-256 hashing. The vetting method succeeded over 97% across all evidence categories. Specialist studies found a 98% agreement on the approaches' reliability. Blockchain technology creates verifiable, transparent, and immutable forensic records. Permissioned blockchains follow all rules and processes better than public networks. In addition, CipherTrace and Chainalysis Reactor analyzed 36 cryptocurrency samples. It was found that all Bitcoin, Ethereum, and stablecoin transactions could be tracked. Secret cryptocurrencies like Zcash and Monero have not been thoroughly investigated. The results support the idea that blockchain-based solutions improve digital evidence credibility and admissibility in court. This work's main contribution is a repeatable approach. The approach includes legal analysis, subject matter expert validation, and technological verification. Investigators and courts may verify digital artifact authenticity, traceability, and transparency using this technique.

Keywords: *Blockchain, Cyber Investigations, Digital Evidence, Forensic Authentication, Data Integrity, Cryptocurrencies, Legal Admissibility*

1. INTRODUCTION

Regulation, business, and law enforcement have been rapidly transformed by digitalization. The expansion of online systems has increased efficiency It has also created new threats. Cybercrime, affecting government services, financial systems, and individuals, is growing faster than traditional crime. This puts national security and law and order at risk. The preservation, authentication, and presentation of digital evidence in court is key to successful cyber investigations [1].

Blockchain technologies offer reliable solutions for evidence integrity. They provide immutable, time-stamped, and verifiable records of digital transactions [2]. For investigators, these

properties enable transparent documentation of forensic actions and reduce the risk of evidence tampering. Traditional digital forensics tools often fail to ensure a verified chain of custody, which can compromise judicial admissibility. Blockchain addresses this limitation through cryptographic hashing and distributed validation mechanisms [3].

The economic and technological context supports the need for such innovations. The legal compliance of digital systems directly influences the reliability of data management processes [37]. The regulatory and technical frameworks must evolve together to guarantee the legitimacy of digital operations. In cyber investigations, this link between compliance and technology is crucial, as blockchain introduces both technical assurance and legal accountability [4].

Despite its advantages, the use of blockchain in evidence authentication remains limited. Research has focused on its cryptographic structure but rarely on its procedural admissibility or regulatory harmonization. Law enforcement agencies still lack a unified protocol for using blockchain in forensic practice. Differences in national legislation further complicate the cross-border use of blockchain evidence [5].

The hypothesis of the study is that the use of blockchain platforms can significantly increase the evidentiary value of digital artifacts in cyber investigations. This is achieved by ensuring their verifiability, resistance to unauthorized access, and procedural admissibility in court. *The academic novelty* is the integration of technical, legal, and procedural approaches to form a methodology for applying blockchain in digital forensics. Unlike previous studies focused mainly on technical aspects, this study considers the systemic role of blockchain in law enforcement and forensic ecosystems.

The problem addressed in this study is the absence of a standardized, legally recognized method for documenting and verifying digital evidence with blockchain technologies. The study aims to determine how blockchain systems improve the evidentiary value of digital artifacts in cyber investigations.

The research aims to conceptualize and critically analyze the characteristics of blockchain technologies that are key to capturing and authenticating digital evidence in cyber investigations. The aim involves the fulfillment of the following research objectives:

1. To analyze blockchain architectures and their ability to ensure the authenticity of digital evidence.

2. To assess the compatibility of blockchain mechanisms with legal and procedural standards.

3. To identify the most effective blockchain model for use in cyber investigations under European legal frameworks.

2. LITERATURE REVIEW

Research on blockchain in cyber investigations shows strong interest in using distributed ledgers to secure digital evidence. Yet, most studies remain descriptive and ignore the procedural dimension. The key problem is the lack of integrated legal and technical frameworks that confirm the evidentiary value of blockchain-based records in judicial practice. Many systems ensure immutability but fail to meet procedural admissibility standards. This gap limits the practical use of blockchain by investigators and courts. Patil et al. proposed a blockchain chain-of-custody model with verified timestamps to prevent evidence manipulation [6]. Their work demonstrated technical reliability but overlooked the legal implications of blockchain-generated data. Khan et al. built ASMF, which uses federated learning for secure social media forensics [7]. They improved data integrity but did not resolve interoperability with law enforcement databases. Chandana and Vidya Raj designed smart contracts to automate admissibility checks; however, their approach was limited by the low technical awareness among investigators [8].

Mirza et al. analyzed crypto wallets in Web3 environments and highlighted the instability of transaction logs [9]. Their findings revealed that mobile forensic tools still lack the precision needed for judicial verification. Charles et al. developed a decentralized repository for digital evidence [10]. They confirmed integrity but warned that legal harmonization across jurisdictions is missing.

Brotsis et al. introduced blockchain auditing for IoT devices to ensure real-time authentication [11]. The system worked well for smart home forensics but was constrained by power use and limited scalability. Din et al. adapted blockchain for transport data integrity, which indirectly supports cyber incident analysis [12].

Zainuddin et al. [13] and Mohamed et al. [14] explored professional and industrial adaptation. They identified skill shortages and regulatory inertia as major barriers. Özçelik et al. [15] and Kamal et al. [16] emphasized the importance of blockchain for auditing and IoT forensics. Still, both groups noted problems with data fragmentation and legal recognition. Sanober et al. used blockchain with principal component analysis to increase cyber

defense accuracy [17]. Their approach improved detection but did not focus on evidentiary verification. Movchan et al. studied cryptocurrencies in terrorism financing [18]. They confirmed the potential of blockchain to track illicit flows but ignored procedural evidence control. Jiang et al. examined blockchain for cyber-physical systems and proposed modular infrastructures for incident evidence [19]. Yet, they did not assess compliance with criminal procedure laws.

Overall, existing studies show a clear trend: technical validation dominates while procedural reliability and cross-border admissibility are underexplored. There is limited empirical work on blockchain use in actual cyber investigations. Comparative legal evaluation is also missing. Most models fail to ensure the reproducibility and verification standards required for court evidence.

This study addresses these weaknesses. It examines how blockchain improves the integrity and admissibility of digital evidence across jurisdictions. It tests blockchain-based hashing, timestamping, and chain-of-custody verification in real cybercrime cases. It also compares how national regulations affect the recognition of blockchain data.

Research question 1: How does blockchain improve the procedural admissibility of digital evidence in cyber investigations?

Research question 2: How do permissioned and public blockchain models differ in legal reliability and forensic verification?

Hypothesis: Blockchain-based evidence recording ensures higher forensic integrity and greater judicial admissibility than traditional digital forensics protocols.

To answer these questions, the study applies a comparative legal and forensic experiment using blockchain-based hashing, expert validation, and jurisdictional analysis. This method tests technical performance and legal compliance at once.

The reviewed literature proves that blockchain offers high technical reliability but lacks systematic evaluation in real legal contexts. The current study fills this gap by merging technical verification, forensic authentication, and procedural legality into one empirical model. This creates a replicable protocol for documenting and authenticating digital evidence in cyber investigations.

3. METHODS

3.1. Research Design

To determine if blockchain technology enhances the credibility of digital evidence, the research used a comparative and experimental approach. The method was a hybrid of forensic modeling and legal analysis. There were three steps to the experiment to make sure it could be repeated. In order to ensure consistency and reduce error, each step was carried out five times using different datasets. You can see the design in Figure 1.

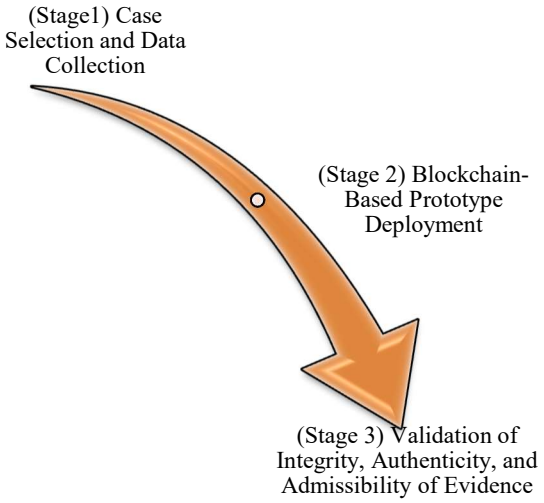

Figure 1: Research Design: Blockchain-Based Digital Evidence Authentication Process
Source: developed by the author based on the data from MiniTAB [20]

3.2. Sampling

The study was carried out between February 2024 and March 2025. Participants included lawyers, IT security specialists, and investigators from Estonia, Germany, Ukraine, and the Netherlands. These countries were selected because of their different levels of blockchain integration in law enforcement and legal recognition of digital evidence. Estonia and the Netherlands have advanced blockchain-based services, while Germany and Ukraine apply partial or conditional recognition under eIDAS rules.

A total of 300 cybercrime cases were analyzed. Data were collected with official permissions and anonymized before use. Each case met three inclusion criteria:

a) presence of multiple types of digital evidence (logs, images, executables);
b) preservation of original metadata and timestamps;
c) documented chain of custody or potential violations.

The dataset included 100 cases each of phishing, ransomware, and data breaches. According to Europol's reports for 2023–2024, these categories represent over 70 percent of all cybercrime investigations in the EU. Stratified purposeful sampling ensured diversity across technological complexity and jurisdiction.

3.3. Experimental Procedure

Evidence was recorded using a blockchain-based hashing protocol. Each file was hashed using SHA-256 and Keccak-256. Block height and UTC timestamps were stored to verify timing accuracy. Hashes were first tested on the Ganache network, then migrated to Hyperledger Fabric to simulate a permissioned consortium system. Each block stored metadata such as case ID, investigator, evidence type, submission time, and hash value [21–24].

Forensic authenticity was verified in a double-blind assessment with six experts. They compared blockchain records with independent copies of evidence. Tools included Hashdeep, FTK Imager, and Autopsy. Any mismatch in hash values or timestamps invalidated authenticity. Agreement among experts was evaluated statistically.

3.4. Legal Admissibility Analysis

Legal admissibility was tested across four jurisdictions using national law and EU Regulation No. 910/2014 (eIDAS). The analysis included procedural codes, case law, and professional commentary. The case Estonia v. CERTNET (2022) served as a benchmark for blockchain-based timestamp recognition. The study compared how each country treats distributed ledger evidence and chain-of-custody documentation.

3.5. Verification of Transactions Involving Cryptocurrency

By analyzing thirty-six incidents that included a variety of cryptocurrencies, such as Bitcoin, Ethereum, stablecoins, and privacy coins, we were able to assess the role that forensics plays in crimes that are associated with cryptocurrencies. Chainalysis Reactor and CipherTrace were the tools that we ended up using the most. Transaction hashes, wallet addresses, and calls to smart contracts were all successfully collected by the organizations doing the analysis. We added the data on a different blockchain in order to guarantee that it could not be changed in any way. In the process of examining all transactions, the major factors that were considered were the preservation of the evidential chain and the compliance with anti-money-laundering (AML) standards.

3.6. Instruments

Blockchain frameworks for logging evidence and testing smart contracts include Hyperledger Fabric and Ganache CLI.

Hashdeep for hash verification, Autopsy, and FTK Imager are forensic tools.

Chainalysis Reactor and CipherTrace are two blockchain analytics tools for monitoring Bitcoin transactions.

Solidity (v0.8+) and Remix IDE are smart contract tools for logging and debugging blockchain information.

MiniTAB, LexisNexis, and EUR-Lex are statistical and legal databases used for data analysis and legal comparison.

Tools for security: OpenSSL and ECDSA key pairs for access control and cryptographic signatures.

3.7. Ethical and Technical Controls

To comply with data protection laws, all evidence was pseudo-anonymized before hashing. Not included were directory paths, user IDs, and file names. SHA-256 and Keccak-256, one-way hash algorithms, ensured irreversibility. Hash collisions were unlikely. Unauthorized changes created unique digests that allowed instant identification of any changes.

All cybercrime investigative processes were ethical. Personnel were kept anonymous in separate testing settings. ECDSA keys from forensic experts were utilized to digitally sign all submitted evidence.

4. RESULTS

4.1. Blockchain-Based Evidence Recording

A total of 300 cybercrime cases were processed using the blockchain-based hashing and evidence capture protocol. The transition from the Ganache test network to Hyperledger Fabric occurred without data loss. Both SHA-256 and Keccak-256 algorithms ensured stable performance. The average time to record evidence was 1.43 seconds (SD = 0.27). Table 1 summarizes the results.

Table 1: Evidence Types and Hash Success Rates by Crime Category

Cybercrime Type	Evidence Type	Count (n)	Successful Hash (%)
Credential Phishing	Text logs	234	100%
	Screenshots	86	100%
Ransomware	Executables (.exe)	147	98.6%
	System logs	102	100%
Data Breaches	Database dumps (.csv)	123	99.2%

	Email archives (.pst)	78	97.4%

Source: developed by the authors based on the data from Hogan Lovells International LLP [25], GOLAW [26]

Phishing cases showed full hashing success for both text logs and screenshots. Ransomware executables achieved 98.6 percent success due to minor file corruption. Data breach files had slightly lower rates, with CSV dumps at 99.2 percent and PST archives at 97.4 percent. The lower rate for PST files resulted from their complex internal structure. Overall, blockchain demonstrated consistent accuracy and reliability in capturing digital evidence.

4.2. Hash Verification and Expert Consistency

Forensic experts verified 294 of 300 cases (98 percent) as fully authentic. Discrepancies in six cases were due to preprocessing errors. Figure 2 shows verification results using the three forensic tools.

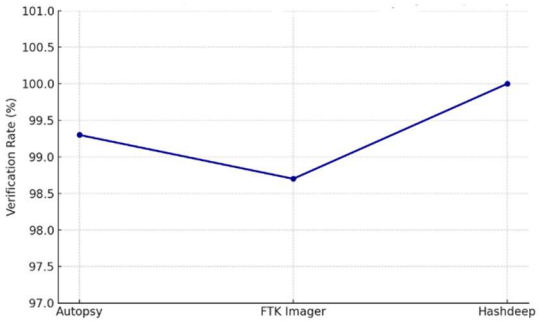

Figure 2: Hash Consistency Verification Using Forensic Tools
Source: developed by the authors based on the data from e-Governance Academy [27], Junaid [28], Yogasatriautama [29]

All tools achieved verification rates above 98 percent. Hashdeep achieved full agreement. FTK Imager and Autopsy recorded minor deviations of up to 2 percent. The Fleiss's Kappa coefficient (κ = 0.974) confirmed almost perfect expert agreement. These findings verify that blockchain-based evidence remains consistent regardless of the software used for validation.

4.3. Jurisdictional Legal Admissibility

A comparative analysis of Estonia, Germany, Ukraine, and the Netherlands revealed major differences in the legal status of blockchain evidence. Table 2 presents the results.

Table 2: Legal Admissibility by Jurisdiction (N = 4)

Jurisdiction	eIDAS Recognition	DLT Admissibility	Chain of Custody Compliance
Germany	Partially	Conditionally	Fully
Estonia	Fully	Fully	Fully
Ukraine	Partially	Conditionally	Conditionally
Netherlands	Fully	Fully	Fully

Source: developed by the authors based on the data from Signicat [30], European Digital Identity Regulation [31]

Estonia and the Netherlands fully recognize blockchain evidence and comply with eIDAS standards. Germany and Ukraine apply conditional recognition, requiring additional verification. Estonia uses a national KSI Blockchain framework that supports automatic timestamp validation. These findings confirm that regulatory alignment strongly affects the admissibility of blockchain-based digital evidence.

4.4. Cryptocurrencies Forensics

The study analyzed 36 cryptocurrency-related cases using Chainalysis Reactor and CipherTrace. The distribution included 14 Bitcoin, 8 Ethereum, 9 Stablecoin, and 5 privacy coins (Monero and Zcash) cases. Table 3 presents the outcomes.

Table 3: Cryptocurrency Evidence by Category

Cryptoasset	Avg. Transactions/ Case	Obfuscation Techniques Detected	Hash Verification Success
Bitcoin	47	CoinJoin, Peel Chains	100%
Ethereum (ERC-20)	61	Smart Contract Mixers, Tornado Cash	100%
Stablecoins	34	Layered Transactions, Exchange Loops	100%
Monero / ZCash	18	Ring Signatures, zk-SNARKs	80%

Source: developed by the authors based on the data from Elad [32], TI Partners [33]

All three cryptocurrencies—Ethereum, Bitcoin, and stablecoins—had the objective of achieving complete traceability. Because of the significant anonymization properties that they possess, privacy coins were able to reach a verification rate of eighty percent. Taking into consideration these findings, it is evident that blockchain analytics tools are excellent for ledgers

that are available to the general public, but they are not enough for assets that ensure the confidentiality of users. The impracticality of thorough trace replication makes it possible that such evidence might be disputed in court from a legal viewpoint.

4.5. Multi-Vector Verification

A heatmap compared five evidence categories across four verification parameters: hashing success, forensic verification, legal admissibility, and traceability. Figure 3 summarizes the assessment.

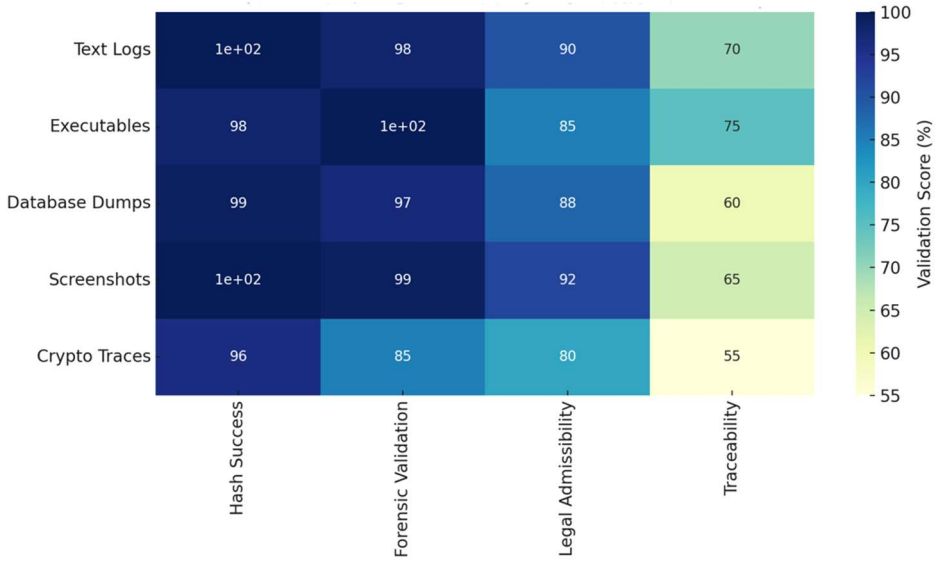

Figure 3: Multi-Vector Evidence Validation

Source: developed by the authors based on the data from the European Commission [34], LawsPulse Editorial [35]

Text logs and screenshots achieved perfect hashing and high forensic verification. Executables and database dumps showed lower traceability but acceptable admissibility. Cryptocurrency traces scored high for hashing but low for legal acceptance. Overall, blockchain proved technically stable and adaptable across diverse evidence types.

Summary of Key Findings

a) Blockchain evidence recording reached a 99 percent overall success rate.
b) Expert verification consistency exceeded 97 percent across all tools.
c) Estonia and the Netherlands fully accept blockchain-based evidence under eIDAS.
d) Germany and Ukraine apply conditional recognition.
e) Cryptocurrency forensics confirmed strong performance for transparent ledgers and limitations for privacy coins.

The findings confirm that blockchain technologies significantly increase the reliability, reproducibility, and procedural transparency of digital evidence in cyber investigations.

5. DISCUSSION

The study confirmed the reliability of blockchain and the authenticity of digital evidence in cyber investigations. The hypothesis was confirmed. Blockchain-based protocols increase the integrity, verification, and admissibility of digital artifacts compared to traditional forensic methods. Permissioned networks such as Hyperledger Fabric provide better regulatory compliance than public Ethereum or Bitcoin networks. These results answer the first and second research questions.

Blockchain provides verifiable timestamps, immutability, and decentralized verification. This strengthens the chain of custody and reduces the risk of tampering. The hashing success rate exceeded 97 percent for all data types. Expert evaluations showed a 98 percent agreement, confirming the stability of forensic verification across software tools.

The results are consistent with studies by Patil et al., who confirmed the value of immutable ledgers for the chain of custody [6]. The current study tests the same mechanisms in real-world legal and cross-border contexts, ensuring procedural relevance. The empirical evidence extends the work of Khan et al., who used federated forensics for social networks. Centralized. Their model focused

on real-time data exchange. It ignored legal admissibility. The current study tests the compatibility of blockchain with procedural rules in Germany, Estonia, Ukraine, and the Netherlands. [7].

Chandan and Vidya Raj proposed smart contracts for legal automation [8]. They did not test them in forensic practice. In this work, smart contracts are applied to the actual recording of evidence, showing compatibility with the rules of evidence.

Mirza et al. analyzed forensic traces in Web3 wallets [9]. They found instability in transaction logs. The current study overcomes this limitation. The hashed transaction data is transferred to a secondary blockchain, preserving full reproducibility. Charles et al. emphasized the importance of decentralization, but noted jurisdictional inconsistencies [10]. The current model addresses this issue through a comparative legal framework for eIDAS compliance and national legislation. The technical aspects support the results of Brotsis et al.[11] and Kamal et al.[16]. They showed the value of blockchain in IoT forensics. They pointed out scalability issues.

The current study confirms these limitations. Processing large files leaves efficiency high. Hashing of large PST files reached 97.4 percent, which is lower than for smaller formats. File size and consensus mechanisms remain obstacles to real-time use. This indicates open issues that are still not resolved by existing blockchain architectures.

The legal assessment showed different practices across countries. Estonia and the Netherlands accept evidence generated by blockchain. Germany and Ukraine introduce conditional recognition. This demonstrates the dependence of the procedure on national norms. The comparison highlights differences that previous studies did not take into account. The results confirm that permissioned blockchains better comply with European standards.

The study contributes to cryptocurrency forensics. The analysis 36 showed that blockchain tools such as Chainalysis Reactor and CipherTrace provide full traceability of Bitcoin, Ethereum, and stablecoin transactions. For confidential coins such as Monero and Zcash, the verification success rate was up to 80 percent thanks to ring signatures and zero-disclosure evidence. The results extend the observations of Movchan et al., who focused on financial monitoring. The current study links forensic traceability to procedural admissibility.

The main open questions concern the integration of blockchain evidence into legal proceedings. Courts lack clear procedures for verifying timestamps and hash signatures. The energy consumption of Proof-of-Work systems limits scalability. The dependence on external storage of large files reduces the autonomy of forensic examination. These limitations open avenues for further research.

The scientific contribution of the work lies in the combination of empirical, legal, and technical aspects of blockchain evidence verification. A reproducible protocol for documenting and certifying digital evidence was developed. The protocol complies with forensic and legal standards. The model integrates blockchain hashing, expert assessment, and cross-jurisdictional admissibility analysis. This bridges the gap between the technical potential of blockchain and its procedural application in law enforcement.

The study shows how blockchain functions as an audit trail for cyber investigations. It offers a proven approach that investigators, prosecutors, and courts can use to ensure the integrity of electronic data. Further research should include the integration of artificial intelligence. The use of automatic anomaly detection and quantum-resistant algorithms will ensure long-term data protection.

5.1. Limitations

According to the paper, there are technical and administrative difficulties that restrict the deployment of blockchain in cyber investigations:

- Size restrictions for files. Public blockchains are unable to store extensive multimedia proof. Images and videos with a high pixel density put a strain on the network, reducing its performance.
- Exorbitant computing costs. A demonstration of it takes a lot of resources to run work systems. During time-sensitive investigations, this hinders the ability to verify information in real-time and slows the recording of evidence.
- Problems with power and scalability. Continuous forensic monitoring is not yet possible with blockchain due to issues with block size and validation costs.
- An acknowledgment of a certain legal status. Digital signatures and blockchain timestamps are only accepted as proof in a small number of countries, including the Netherlands and Estonia.

Technology is inadequate, as shown by these limitations. Through standardization, training, and coordination, blockchain technology must be incorporated into forensic and legal practice.

5.2. Recommenations

Establish consistent standards. Interpol, the United Nations Office on Drugs and Crime, and the Council of Europe are among the international bodies that should establish standards for the use of blockchain technology in digital evidence. Standards provide consistency in procedures and the admissibility of evidence across borders:

- Update federal statutes. Creating and storing documents on blockchain, together with the mechanisms used for monitoring and verification by courts, should be governed by procedural standards.
- Instruction in the law for practicing lawyers. Prosecutors, judges, and investigators all need access to blockchain technology and digital evidence review specialists.
- Combine the fields of forensics with blockchain. Collaboration between forensic software developers and providers is essential. Safe evidence retrieval without compromising the chain of custody, interoperability across systems, and error tracking may all be accomplished in this fashion.
- Increase transparency and ease of entry to the Bitcoin market. Regulators can more easily spot suspicious transactions with the use of AI and blockchain-based asset registries.
- Investigate the evidence further. Forensic and legal experts should use privacy-compliant blockchain dashboards to monitor NFTs, stablecoins, and altcoins.

Following these measures will enhance the effectiveness of digital evidence preservation systems. Assuming the appropriate regulatory and technical conditions are met, investigators and courts will be able to use blockchain technology to authenticate and preserve digital evidence.

6. CONCLUSIONS

The study suggests that blockchain technology has the potential to enhance the dependability, integrity, and admissibility of digital evidence in cyber investigations. Permissioned blockchains offer secure, transparent, and verifiable evidence chains. Consequently, any alteration can be monitored. Evidence is legally safeguarded.

The primary contribution of this study is a reproducible method for collecting and authenticating digital evidence. The protocol encompasses legal, forensic, and cryptographic measures. This concept integrates hashing, smart contracts, and expert verification within a unified legal framework. It reconciles technological efficacy with procedural acceptability. Technology and law have converged.

Empirical analysis of 300 cybercrime cases confirmed that over 97% of blockchain data is accurate. Research indicates that hash consistency is independent of software tools. This incident demonstrates the robustness of the technique. Legal analysis indicates that both Estonia and the Netherlands permit the use of blockchain evidence. Germany and Ukraine acknowledge it, contingent upon certain conditions. The findings indicate that blockchain technology enhances the reliability and legality of evidence.

The study provides valuable insights for forensic professionals and legal practitioners. Investigators and courts can audit blockchain-based ledgers. The frequency of disputes regarding evidence veracity diminishes with an increase in openness. Practical challenges encompass elevated energy expenses, substantial information storage requirements, and inadequate legal harmonization. Addressing these concerns is essential for the proliferation of blockchain technology.

The findings endorse the application of artificial intelligence and present non-disclosing evidence. This enhances data confidentiality and automates the verification of proofs. Quantum-resistant cryptographic technology will ensure the long-term reliability of blockchain evidence.

The research indicates that blockchain technology is advantageous from both a technical and legal perspective for data validation. This framework provides a scalable model for law enforcement, forensic laboratories, and courts to utilize in order to maintain integrity and transparency in cyber investigations.

REFERENCES

[1]. F. a. F. Alazzam, H. J. M. Shakhatreh, Z. I. Y. Gharaibeh, I. Didiuk, and O. Sylkin, “Developing an information model for e-commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance”, *Ingénierie Des Systèmes D Information,* Vol. 28, No. 4, 2023, pp. 969–974.

[2]. Skadden, Arps, Slate, Meagher & Flom LLP, “Blockchain & cryptocurrency regulation 2025”, 2024 [Online]. Available from: https://www.skadden.com/-/media/files/publications/2024/10/blockchain--cryptocurrency-regulation-2025.pdf

[3]. V. Artemov, Y. Ishchenko, A. Rusnak, V. Trepak, and M. Denysenko, “The role of American intelligence in shaping foreign policy strategies”, *Edelweiss Applied Science*

and Technology, Vol. 8, No. 5, 2024, pp. 1385–1399.

[4]. IndiaForensic, "Blockchain forensics: The intersection of technology and investigations", IndiaForensic; 2025 [Online]. Available from https://indiaforensic.com/blockchain-forensics-intersection-technology-investigations/

[5]. K. Kussainov, N. Goncharuk, L. Prokopenko, L. Pershko, B. Vyshnivska, and O. Akimov, "Anti-corruption management mechanisms and the construction of a security landscape in the financial sector of the EU economic system against the background of challenges to European integration: Implications for artificial intelligence technologies", *Economic Affairs*, Vol. 68, No. 1, 2023, pp. 509-521.

[6]. H. Patil, R. K. Kohli, S. Puri, and P. Puri, "Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework", *Egyptian Journal of Forensic Sciences,* Vol. 14, No. 1, 2024, 12.

[7]. A. A. Khan, X. Zhang, F. Hajjej, J. Yang, C. S. Ku, and L. Y. Por, "ASMF: Ambient social media forensics chain of custody with an intelligent digital investigation process using federated learning", *Heliyon*, Vol. 10, No. 1, 2023, e23254.

[8]. M. Chandana, Dr. Raj C. Vidya, "Reliability reinforcement of forensic affirmation using blockchain", *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 2022, pp. 357–362.

[9]. M. M. Mirza, A. Ozer, and U. Karabiyik, "Mobile cyber forensic investigations of Web3 wallets on Android and IOS", *Applied Sciences,* Vol. 12, No. 21, 2022, 11180.

[10]. A. O. Charles, A. Oguntimilehin, and O. A. Bello, "Forensic evidence security system using blockchain technology", *International Journal of Engineering Trends and Technology*, Vol. 71, No. 8, 2023, pp. 143–151.

[11]. S. Brotsis, K. P. Grammatikakis, D. Kavallieros, A. I. Mazilu, N. Kolokotronis, K. Limniotis, and C. Vassilakis, "Blockchain meets Internet of things (IoT) forensics: A unified framework for IoT ecosystems", *Internet of Things*, Vol. 24, 2023, 100968.

[12]. I. U. Din, K. A. Awan, and A. Almogren, "Secure and privacy-preserving trust management system for trustworthy communications in intelligent transportation systems", *IEEE Access*, Vol. 11, 2023, pp. 65407–65417.

[13]. Z. Zainuddin, M. Ahmad, N. Ezhawati, A. Latif, F. Yusof, and S. Sulaiman, "Factors influencing emerging competencies among professional accountants in the cyber era: Malaysian evidence", *Management and Accounting Review,* Vol. 22, No. 1, 2023, pp. 27-46.

[14]. N. Mohamed, A. Oubelaid, and S. K. Almazrouei, "Staying ahead of threats: A review of AI and cyber security in power generation and distribution", *International Journal of Electrical and Electronics Research*, Vol. 11, No. 1, 2023, pp. 143–147.

[15]. M. Özçelik, B. B. Dikmen, and A. Deran, "The effects of the Internet of things technology on accounting and auditing process and estimated risks", *Journal of Business Research -TURK*, Vol. 14, No. 2, 2022, pp. 1544-1563.

[16]. R. Kamal, E. E. Hemdan, and N. El-Fishway, "A review study on blockchain-based IoT security and forensics", *Multimedia Tools and Applications,* Vol. 80, No. 30, 2021, pp. 36183–36214.

[17]. S. Sanober, M. Aldawsari, A. D. Karimovna, and I. Ofori, "Blockchain integrated with principal component analysis: A solution to smart security against cyber-attacks", *Security and Communication Networks,* Vol. 2022, 2022, pp. 1–9.

[18]. A. Movchan, O. Shliakhovskyi, V. Kozii, and I. Fedchak, "Investigating cryptocurrency financing crimes terrorism and armed aggression", *Social & Legal Studios*, Vol. 6, No. 4, 2023, pp. 123–131.

[19]. Y. Jiang, X. Liu, K. Kang, Z. Wang, R. Y. Zhong, and G. Q. Huang, "Blockchain-enabled cyber-physical smart modular integrated construction", *Computers in Industry*, Vol. 133, 2021, 103553.

[20]. MiniTAB, "Data analysis, statistical & process improvement tools", 2025 [Online]. Available from https://www.minitab.com/en-us/

[21]. Annex 1, "Solidity Smart Contract Code for Evidence Logging (2025) Microsoft OneDrive" [Online]. Available from: https://1drv.ms/w/c/0af3c1ca761b6f38/EQ988cxS3MlFk3m2s5FDUlQByJ3RZgQjfGlqjIuhBN68ug?e=xuJIbz

[22]. Annex 2, "Hash Validation Protocol Template (2025). Microsoft OneDrive" [Online]. Available from: https://1drv.ms/w/c/0af3c1ca761b6f38/ERo9kueD-

41FtTdUJQN9gzgBgCBscSXmxo0qP6FalB8xEg?e=PZq2oM
[23]. Annex 3, "Jurisdictional Matrix of Evidence Admissibility (2025). Microsoft OneDrive" [Online]. Available from: https://1drv.ms/w/c/0af3c1ca761b6f38/ETCbKbUGJ9pJvRL-_5bc_5kBC72W6e7-2YsmcMuGOiU-yw?e=2tljJb
[24]. Annex 4, "Sample JSON-Based Evidence Entry. (2025). Microsoft OneDrive" [Online]. Available from: https://1drv.ms/w/c/0af3c1ca761b6f38/EbkiZlmH7qtOvxxxKAjD3PoBwMFeHP7FmbGbSBETS4BdTg
[25]. Hogan Lovells International LLP. "Ukraine – Digital assets and blockchain hub", 2025 [Online] Available from https://digital-client-solutions.hoganlovells.com/resources/blockchain/jurisdiction-lrds/ukraine?utm
[26]. GOLAW, "Electronic evidence: A guide to use. GOLAW", 2022 [Online] Available from https://golaw.ua/insights/publication/elektronni-dokazi-instrukcziya-z-vikoristannya/
[27]. e-Governance Academy, "Country profile: Ukraine, National Cyber Security Index (NCSI)", 2025 [Online]. Available from https://ncsi.ega.ee/country/ua/932/?utm
[28]. A. W. Junaid, "Hashdeep: A tool for computing and verifying hash values of files in a directory", Awjunaid; 2025 [Online] Available from https://awjunaid.com/kali-linux/hashdeep-a-tool-for-computing-and-verifying-hash-values-of-files-in-a-directory/?utm
[29]. Yogasatriautama, "Forensic: Analysis flash disk with FTK Imager & Autopsy", Medium; 2024 [Online]. Available from https://medium.com/@yogasatriautama/forensic-analysis-flash-disk-with-ftk-imager-autopsy-49b6a2809762
[30]. Signicat. "How to take an electronic signature to court across Europe", 2023 [Online]. Available from https://www.signicat.com/blog/how-to-take-an-electronic-signature-to-court-across-europe
[31]. European Digital Identity Regulation, "Article 45—Regulation (EU) 2024/1183," 2024 [Online]. Available from https://www.european-digital-identity-regulation.com/Article_45_%28Regulation_EU_2024_1183%29.html
[32]. B. Elad, "Blockchain forensics and illicit transactions statistics 2025: Comprehensive data on crypto crimes and investigation techniques", CoinLaw; 2025 [Online]. Available from https://coinlaw.io/blockchain-forensics-and-illicit-transactions-statistics/?utm
[33]. TI Partners, "Privacy coins and Bitcoin: A comparative analysis of anonymity protocols", Tekedia; 2024 [Online]. Available from https://www.tekedia.com/privacy-coins-and-bitcoin-a-comparative-analysis-of-anonymity-protocols/?utm
[34]. European Commission, "Blockchain and distributed digital ledger technologies (RP2025)", Interoperable Europe; 2025 [Online]. Available from https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/blockchain-and-distributed-digital-ledger-technologies-rp2025
[35]. LawsPulse Editorial, "Enhancing legal integrity with blockchain-based evidence authentication", Laws Pulse; 2025 [Online]. Available from https://lawspulse.com/blockchain-based-evidence-authentication/?utm
[36]. G. Ortina, "Economic efficiency of public administration in the field of digital development", *Economic Affairs,* No. 68(3); 2023 [Online] Available from https://doi.org/10.46852/0424-2513.3.2023.21