(Online) ISSN 2712-0562
*Review Article*

**Sustainable Engineering and Innovation**
Vol. 7, No. 1, 2025, pp.209-224
https://doi.org/10.37868/sei.v7i1.id499

# Blockchain technologies and their application in security software development

**Serhii Zybin[1*], Oleg Kubrak[2], Petar Halachev[3], Yaroslav Kravchuk[4], Oleksandr Muliarevych[5]**

[1] Department of Cybersecurity Systems and Technologies, State University of Information and Communication Technologies, Ukraine
[2] Senior Software Engineer, Grid Dynamics Holdings, Inc., USA
[3] Department of Informatics, University of Chemical Technology and Metallurgy, Bulgaria
[4] Velar Voyage LLC, Chicago, USA
[5] Department of Computer Engineering, Lviv Polytechnic National University, Ukraine

*Corresponding author E-mail: zysv@ukr.net

Received Apr. 9, 2025
Revised May 29, 2025
Accepted Jun. 5, 2025
Online Jun. 13, 2025

**Abstract**

Current factors like the rising frequency of cyber threats and vulnerabilities on centralized platforms indicate the inefficiency of conventional network security frameworks, leading to new solutions such as the blockchain. This review systematically reviews developments of blockchain technologies in the context of security software (2021-2023) to evaluate its efficacy and challenges and explore the future potential. 77 peer-reviewed papers from ScienceDirect, IEEE Xplore and Scopus; adopting the PRISMA guideline, records were screened down from 1,532 to 77. Empirical evaluations (35%), case studies (28%), and theoretical frameworks (37%) using Joanna Briggs Institute tools and the Newcastle-Ottawa Scale were used in mitigating bias. The results show blockchain enhances data integrity (89% of studies) and secures IoT ecosystems (28 studies) and supply chains (15 studies). However, blockchain-based authentication exhibits higher latency (342 ± 112 ms), exceeding traditional systems by 284% (e.g., 89 ± 24 ms for PKI), reflecting scalability-performance trade-offs. Research remains skewed toward finance (47%), with limited focus on healthcare (9%) and critical infrastructure (6%). It does not include sufficient interoperability standards, post-quantum cryptographic validation, etc. The adaptive regulations are urged for policy implications for editable blockchains and hybrid Artificial Intelligence (AI) blockchain architectures. Interoperability should be taken care of by cross-chain protocols, scalability trilemmas and real-world adversarial testing must be addressed by the researchers and practitioners must put priority on scalability. This review, in its totality, brings out the singular role of blockchain in complementing the existing security solutions instead of replacing them. It calls for cross-disciplinary involvement and partnership in harnessing technical innovation in a regulatory framework to tackle cybersecurity threats through outsider and insider security approaches.

*Keywords*: Blockchain technology, Cybersecurity, Systematic review, Regulatory compliance, Decentralized systems

## 1. Introduction

Satoshi Nakamoto presented his ground-breaking whitepaper Bitcoin: A Peer-to-Peer Electronic Cash System in 2008, marking the birth of blockchain technology, which operates as a decentralized distributed ledger system that serves clients without traditional banks or payment organizations. For the creation of Bitcoin, technology developers established peer-to-peer banking features that bypass payment processors and banks [1]. A blockchain operates through blocks, which exist in a sequence using cryptographic processes that embed transaction timestamps. A process of consensus maintains authorization between every member of the network while operating without any controlling governing entity [2]. Digital currencies received a solution through this innovation, which established a secure digital record of ownership and controlled spending incidents from modification attempts [3].

Blockchain technology has evolved through three successive stages, bringing better features and expansion capabilities [4]. Ethereum (2015) brought a second-generation blockchain through smart contracts along with decentralized applications (dApps) that serve supply chain management and digital voting applications [5]. Ethereum 2.0 (2022) implemented Proof of Stake (PoS) while chopping power consumption to 99.95% of its former usage and increasing operational efficiency [6]. The after-2020 period became dedicated to building blockchain-enabled enterprise applications and network interoperability through Polkadot, Cosmos, and Hyperledger Fabric [7]. Despite efficiency improvements, concerns over blockchain's overall energy consumption remain relevant, especially in large-scale PoW networks, raising questions about sustainability and environmental impact [8].

New advancements in blockchain security occurred between 2021 and 2023 through zero-knowledge proofs (ZKPs), Algorand’s Pure PoS, and AI-integrated fraud detection systems and privacy features [9]. Off-chain solutions that build on top of the Bitcoin network through Lightning Network and Ethereum through optimistic rollups allow secure blockchain processing of transactions outside the blockchain [10]. Blockchain developments encounter performance-related barriers that force users to choose between secure and decentralized operations. Solana upholds operation at 65,000 transactions per second, yet it demonstrated inconsistent performance, causing reliability issues. The adoption of digital assets remains restrained by the uncertainties of government oversight mechanisms for digital assets, coupled with obligatory Anti-Money Laundering policy requirements [11]. Moreover, blockchain presents new approaches to cybersecurity challenges such as tamper-proof data storage, distributed denial-of-service (DDoS) resistance, and consensus-driven identity verification [12]. However, the immutability of records creates friction with privacy regulations like GDPR, particularly regarding the right to erasure [13].

The security of blockchain systems is enhanced through decentralized identity systems and automated smart contracts and consensus protocols, such as PBFT and DPoS, that minimize unauthorized breach risks. The MedRec application enables safe patient record access through its security features, as Microsoft implements decentralized identity frameworks to fight credential theft [14]. The distribution of command structures through Blockchain-enabled Industrial Control Systems (ICS) makes critical infrastructure more secure by protecting against failures resulting from centralized authority [15]. Despite promising implementations in healthcare and industrial security systems, these areas remain underexplored in the literature, especially concerning empirical validations and domain-specific performance metrics [16]. Executing blockchain technology faces operational hurdles because GDPR’s “right to be forgotten” requirement conflicts with the permanent character of blockchain’s historical records.

The blockchain security research exists in separate fragments because studies show uneven performance metrics and a lack of widespread real-life implementation assessments. A recent investigation of [17] showed that blockchain security testing occurred in actual conditions only in 22% of the analyzed research articles published in 2023. High transaction speed remains a scalability issue since Bitcoin handles just 7 TPS and Ethereum 2.0 before version 2.0 achieves 30 TPS, creating limitations for real-time operations such as intrusion detection [18]. Critics question how secure high-speed protocols like Solana can be because peer-reviewed research about their security resistance has not been published. Many organizations overlook blockchain integration with security systems because unresolved issues when connecting cross-chain communication protocols limit their effective implementation.

Technology based on blockchain advances digital security through features like transparent data, tamper-resistant functions, and automated system capabilities. However, significant research deficits persist with regulatory concerns and system expansion limits [19]. Future research needs to unite the gaps by executing the evaluation of blockchain practical execution and resolving the regulatory conflicts. Wider implementation of security frameworks needs hybrid AI-blockchain models and zero-trust architectures to succeed despite facing technical and institutional obstacles.

The majority of blockchain security investigations (47%) target financial applications within the period of 2021–2023, according to [20], which contrasts with minimal interest in healthcare (9%) and critical infrastructure (6%). The current balance lacks awareness about medical device security requirements in combination with blockchain delays that might affect real-time observations and the operational requirements of outdated energy grid SCADA technologies [21].

To fill the research gaps, a systematic review requires one to take the following steps:

1. Benchmark blockchain's scalability and security trade-offs.
2. Standardize hybrid blockchain-legacy interoperability.
3. Researchers must conduct evidence-based studies that link theoretical models to specific limitations found in real-life applications.
4. A clear definition of regulatory laws should enable the immutability of blockchain to respect data governance requirements.

Evaluation of existing evidence and unexplored solutions will guide developers, policymakers, and researchers to develop precise, responsible deployment of blockchain technology in security applications.

### 1.1. Research Aim and Questions

Research on security software development with blockchain technologies receives systematic analysis and synthesis of scholarly literature to determine its advantages and constraints, together with outstanding research questions. Several studies provide their combined findings to develop a consolidated understanding of blockchain functionality within cybersecurity frameworks and identify methodological inconsistencies for future recommendations of empirical research-based innovations.

The aim of this study is to evaluate the current applications, benefits, and challenges of blockchain in security software development, and to identify gaps in empirical research, particularly in real-world deployments and performance metrics. Accordingly, the research addresses the following questions:

RQ1: What are the current implementations of blockchain in security software development, and what roles do they serve?

RQ2: What are the documented advantages and obstacles of integrating blockchain into cybersecurity systems?

RQ3: Where do gaps persist in the literature, and what are the future research priorities for blockchain-enabled security systems?

1. Based on the review findings, Blockchain currently serves a role in security software development. Three blockchain implementations include decentralized authentication controls, secure data tracking features, and tamperproof audit trails to fulfill standards compliance. Blockchain will serve as a testing method to stop device spoofing events in IoT security systems while safeguarding software update delivery channels against man-in-the-middle attacks [22, 23].
2. This study reviews both advantages and obstacles that blockchain technology provides to security systems. Organizations may achieve better data integrity and protection from Distributed Denial of Service attacks through decentralization of systems, cryptographic hashing, and reduced dependency on trusted third parties. Blockchain adoption faces multiple restrictions, such as operational scale

limitations and energy waste in proof-of-work protocols, and it poses legal hurdles because it prevents alterations and GDPR privacy regulations [24, 25].

3. The analyzed literature shows empty spaces where researchers must conduct extensive research about blockchain security systems deployed in real industrial environments and create standardized evaluation metrics for legacy system interoperability. The paper advocates quantum-resistant blockchain protocol development and hybrid blockchain systems that unite AI threat detection with decentralized ledger technology [26, 27].

The analysis features certain limitations regarding time frame duration, thematic boundaries, and certain restrictions for precise technical analysis. The research concentrates on peer-reviewed studies from January 2021 through December 2023, while Ethereum moves to PoS and enterprise blockchain applications surface. Three major concerns arise in this subject: cybersecurity, data integrity, and decentralized authentication methods. However, cryptocurrency research is excluded if it does not lead to security software developments.

Studies based on empirical research combining case studies with performance benchmarks form part of the literature review, together with theoretical frameworks that receive technological validation and systematic reviews, but omit conceptual papers that lack experimental or observational data. According to this article, security software depends on blockchain since it enables secure communication protocols to utilize blockchain-based key management systems for encrypted messaging networks.

### 1.2. Literature review

This research employed a systematic collection of peer-reviewed academic studies from IEEE Xplore, ScienceDirect, ACM Digital Library, SpringerLink, and Scopus to achieve methodological consistency and comprehensive coverage. The research employed search terms including “blockchain security”, “decentralized ledger technology”, and “cybersecurity applications”, then used Boolean operators to retrieve studies published within the timeframe from 2021 to 2023 that focused on contemporary advancements.

Research by [1] published his Bitcoin whitepaper which served as a historical foundation together with the exclusion of non-English papers and Russian institutional studies and opinion pieces to reduce biases and improve accessibility – by following a snowballing method researcher accessed critical sources which would otherwise remain undetected through the analysis of reference lists from key articles. Researchers used this method to gather literature between new advancements and established theoretical models, thus providing an adequate basis for analyzing blockchain's security development evolution.

The examined documents create several principal themes, starting with blockchain technical basics. Proof of Work (PoW) and Proof of Stake (PoS) form the discussion's core concepts while stakeholders investigate their trade-offs regarding security measures, power consumption, and scalability benefits. Ethereum’s adoption of Proof of Stake consensus methodology marks a concerning sustainability transition, which decreases its energy use by 99.95%, yet the scalability optimization of the Solana network may jeopardize its stability [28].

Network security experts like [29] evaluated zk-SNARKs and advanced hashing algorithms as privacy protections because these cryptographic tools prove their effectiveness for secure transactions. IBM’s Hyperledger Fabric demonstrates how blockchain technologies have evolved to include permissioned and hybrid execution models for enterprise-level adoption while maintaining decentralization capabilities [30].

The second main research topic is blockchain, which demonstrates potential as a security solution for current software development challenges. Centralized systems face persistent security risks because they depend on isolated control points, such as during the Colonial Pipeline ransomware incident [9], and 95% of cloud security issues stem from misconfiguration per [31] report.

The explosion of IoT devices set to reach beyond 29 billion units by 2030 multiplies security dangers because different devices operate with different security standards [32]. The existing infrastructure benefits from blockchain technology, providing distributed systems that prevent failure at any reference point.

Substantial evidence demonstrates blockchain utilization in different sectors through two real-world examples: The IBM Food Trust employs blockchain to track supply chain products' origins from source to customer [33], and the MedRec project implements blockchain access management systems to safeguard healthcare records [34]. Through its ION framework, Microsoft displays how blockchain-based decentralized identifiers function to prevent credential theft by surpassing central authority providers [35].

Literature reviews show heterogeneous approaches and sectoral preference patterns that limit practical implementation across different domains. Research empirical studies constitute 35% of assessed works, but usually implement simulated settings to measure latency and throughput while obtaining minimal insights about blockchain performance under adversarial real-world conditions.

Theoretical frameworks successfully describe decentralized trust models, although they have weak technical validation and show a sectoral bias toward financial applications (47%) above critical infrastructure (6%) and healthcare (9%) [36]. The current research imbalance between domains makes it challenging to identify specific blockchain limitations, including how blockchain responds to real-time medical timing requirements and when trying to combine traditional industrial control systems with decentralized systems [37]. Less than 10% of blockchain studies address compliant technical solutions that resolve the immutability-against-GDPR-right-to-be-forgotten tension.

The repeated research demonstrates that blockchain strengthens data security and protects against distracted denial-of-service (DDoS) attacks by implementing cryptographic hashes and peer-to-peer validation methods [38, 39]. Blockchain's advancement faces two ongoing problems because it must address scalability issues, and it needs clear regulatory guidelines. Traditional performance measurements diverge from expert evaluations of network capabilities, as Solana states it can handle up to 65,000 TPS, but expert assessments indicate unreliable operation [38, 40], which impedes real-world implementation.

The literature shows significant gaps in interoperability standards and longitudinal cost analysis for permissioned networks, particularly through incompatible security assumptions between Polkadot and Cosmos and node synchronization expenses described in [41]. The development of AI-enhanced blockchain hybrids representing new threat detection capabilities continues as a growing field, according to [42], who supported combined decentralized ledger and machine learning algorithm systems.

The conceptual model explains blockchain technology as an engineering capability that addresses fundamental weaknesses in mainframe infrastructures. This framework situates blockchain fundamentals, consensus mechanisms, cryptographic techniques, and architectural evolution as enablers of security applications, from supply chain transparency to decentralized authentication.

The research identifies technical and regulatory barriers such as scalability limitations, communication interoperability problems, and adherence to regulatory standards, which need further attention to develop quantum-secure network protocols and standardized cross-chain exchange frameworks. Systematic reviews become essential to remove speculative claims while validating proven solutions, since this will lead to blockchain-integrated security software that has both scalability and regulatory compliance capabilities.

A review of current literature supports how blockchain addresses long-standing security weaknesses, although evidence mainly exists as theoretical studies. The extensive documentation of cryptographic advantages does not resolve implementation barriers created by operational tradeoffs, sector-dependent biases, and regulatory inconsistencies. The review focuses on empirical rigor, interoperability, and domain-specific challenges to unite dispersed research findings into a framework that supports additional research that connects the abstract blockchain promise to actual operational security software deployment.

## 2. Research method

This systematic review was designed to be reproducible, rigorous, and aligned with established protocols for evidence synthesis in applied research. In order to maintain focus and relevance, studies were chosen according to inclusion and exclusion criteria. To focus on more recent advancements, the publications had to be peer-reviewed English publications, written between January 2021 and December 2023, and address blockchain technology in the context of security software development.

Exclusion criteria included exclusion of non-empirical studies (e.g., editorials, opinion pieces), non-English texts, and research conducted by Russian institutions, as the risk of bias or accessibility could not be excluded. The temporal and thematic bounding done for this review ensured that the review concentrated on actionable insights arising from technically validated findings and ignored (un)dated or speculative claims.

The search strategy uses a multi-database that queries IEEE Xplore, Scopus, Web of Science, ACM Digital Library, and ScienceDirect with Boolean operators to narrow the significant results. It used key search terms as permutations of “blockchain” joined with “security software,” “cybersecurity”, “decentralized authentication”, and “smart contracts” with iterative adjustments for sensitivity and specificity.

In other words, the query (“blockchain” OR “DLT”) AND (“security” OR “cyber”) and (“software” OR “application”) not (“cryptocurrency” OR “finance”) was run with a filtering condition to filter out tangential financial applications. Searches of the database were supplemented by a snowballing technique where reference lists of seminal articles were scanned to locate more resources, covering niche or interdisciplinary studies for a thorough review.

The structured sequence of the screening process reduced the bias in the selection process. The initial search provided results of 1,532 articles, which were deduplicated using Zotero's automation tools and reduced to 1,128. Afterwards, two independent reviewers screened titles and abstracts against inclusion criteria and resolved discrepancies through consensus discussions.

Excluding 862 articles, this phase centered on irrelevancy to security software (such as blockchain applications that talked about the supply chain logistics without a lens of security) or use of nonempirical methodologies. Of the remaining 266 full-text articles, 189 were excluded due to a lack of technical validation or inadequate methodological detail. The final corpus will be of at least 77 studies from the attrition process.

The Joanna Briggs Institute (JBI) critical appraisal tools were adopted and modified for quantitative and qualitative studies to assess the quality. The eight domains from which each article was evaluated included research design clarity, sample size justification, measurement validity, statistical appropriateness, confounding control, and ethical considerations. It raised a red flag for studies that scored below 70% on the JBI checklist, notably too much reliance on self-reported data or inadequately controlled groups in experimental designs.

Thus, a study about a blockchain-based intrusion detection system was downgraded for testing within the simulated environment and a lack of real-world adversarial conditions. The risk of bias was further quantified using a modified Newcastle Ottawa Scale in which validity was weighed by internal validity (40%), external validity (30%), and analytic rigor (30%).

A standardized protocol for data extraction was followed to record key variables such as the study design (Case Study, Quasi Experiment), Blockchain type (Public, Private, Hybrid), security context (Authentication, Data integrity), and quantified outcomes (Latency, Throughput, Attack Resilience etc.). These variables were structured in a spreadsheet, so cross-study comparisons were possible. For example, network size and consensus mechanism were tabulated with throughput metrics from blockchain-based authentication systems to observe performance trends. Regarding qualitative findings, regulatory challenges were thematically coded and analyzed for sectoral patterns, using NVivo.

The synthesis approach was a combination of narrative and quantitative methods to deal with variations in study designs. Repeating constructs, like ‘scalability trade-offs’ or ‘regulatory conflicts’, were iteratively refined through constant comparison in thematic analysis. For quantitative data, the effect sizes of metrics such as $\boldsymbol{\tau}$ (transaction latency) and $C$ (consensus time) were aggregated for comparable studies through a random effects meta-analysis model when feasible. Furthermore, study-to-study variability was imposed on the model based on different blockchain architectures, through:

$$\theta = \frac{\sum_{i}^{k} \omega_i \theta_i}{\sum_{i}^{k} \omega_i} . \qquad (1)$$

Here is the pooled estimate, which shows the individual study effects inversely proportional to variance. The heterogeneity was assessed, and values higher than 50% indicated high variability and the need for subgroup analyses by blockchain type or the security application. A meta regression explored further the covariates, such as network size (*N*) or cryptographic method (*M*), themselves specified as:

$$\theta_i = \beta_0 + \beta_1 N_i + \beta_2 M_i + \mu_i . \qquad (2)$$

Non-quantitative data analysis used a grounded theory approach that developed conceptual frameworks by connecting "interoperability gaps" to potential answers through cross-chain protocols. This mixed research methodology achieved high statistical power and substantial theoretical nuances that meet econometric requirements for handling datasets of variety.

The research methodology applied systematic review standards through the union of quantitative analytical procedures with qualitative data investigation to understand the blockchain's impact on security software. The approach establishes a clear standard for results interpretation and future research guidance because it transparently recognizes limitations of heterogeneity and bias and data detection issues.

## 3. Results

### 3.1. Study selection summary

The initial search of the databases offered 1,532 records; after importing into Zotero, 404 were identified as duplicates. Out of 1199 papers identified through the titles and abstracts, 862 papers were removed mainly because they focused on blockchain in areas that are not related to security.

Again, screening of titles and abstracts of 266 articles resulted in rejecting 189 papers that employed non-empirical research methodologies, such as using a conceptual framework with no technical coefficient or where the security software formed a minor focus of the study. Finally, 77 studies were identified that fulfilled all the criteria for inclusion in the present research. Attrition details are summarized in Table 1.

Table 1. Study selection process

| Phase | Number of Studies |
|---|---|
| Initial Database Search | 1,532 |
| Duplicates Removed | 404 |
| Titles/Abstracts Screened | 1,128 |
| Excluded | 862 |
| Full-Text Reviewed | 266 |
| Excluded | 189 |
| Final Included | 77 |

### 3.2. Descriptive overview

The studies 77 have been distributed over 2021, 2022, and 2023; their annual distribution is 22, 29, and 26, respectively. By region, the participation was highest from the United States (38%, 87 votes), China (24%, 58 votes), and the European Union (21%, 51 votes); the rest came from India, South Korea, and Australia.

Regarding methods, 35% of the papers used empirical types of design, such as experimental and simulation, and 28% included case studies. In comparison, 37% of the papers were theoretical with technical justification. Of the architectures, four categories were distinguished: public (44%), private (32%), and hybrid (24%) blockchains (Table 2).

Table 2. Study characteristics

| Category | Distribution (%) |
|---|---|
| Publication Year | |
| 2021 | 28.6 |
| 2022 | 37.7 |
| 2023 | 33.7 |
| Methodology | |
| Empirical | 35.1 |
| Case Study | 27.3 |
| Theoretical | 37.6 |
| Blockchain Type | |
| Public | 44.2 |
| Private | 31.8 |
| Hybrid | 24.0 |

### 3.3. Thematic findings

Four themes dominated the literature, with the following distribution in Table 3.

Table 3. Study selection process

| Theme | Sub-Theme | Studies (n=77) |
|---|---|---|
| Blockchain Fundamentals | Consensus Mechanisms | 32 |
| | Cryptographic Techniques | 25 |
| Security Challenges | IoT/Cloud Vulnerabilities | 28 |
| | Centralized System Risks | 19 |
| Case Studies | Supply Chain Provenance | 15 |
| | Healthcare Data Management | 12 |
| Comparative Studies | Blockchain vs. Traditional PKI | 18 |
| | Performance Benchmarks | 14 |

For instance, consensus mechanisms such as PoS and PBFT were cited in 32 papers as necessary factors regarding security and scalability. In comparison, 28 papers pointed to the weakness of IoT devices as the main driver towards adopting blockchain.

### 3.4. Quality appraisal results

A quality score above 70% with the JBI checklist was indicated by 68% of studies to have moderate to high rigor. Selection bias was one of the common biases (41% of empirical studies used convenience sampling). In comparison, performance bias (33% of empirical studies did not have real-world adversarial testing) was another common bias. Using the Newcastle-Ottawa Scale to evaluate the studies, a mean score of 6.8/9 was produced with weaknesses in external validity (for example, low geographic diversity) (Table 4).

Table 4. Quality assessment summary

| Bias Type | Prevalence (%) | Example |
|---|---|---|
| Selection Bias | 41 | Non-random sampling in IoT studies |
| Performance Bias | 33 | Simulated environments only |
| Reporting Bias | 22 | Incomplete latency metrics |
| Confounding Bias | 18 | Uncontrolled network conditions |

### 3.5. Synthesis of evidence

The synthesis directly addressed the research questions (Table 5).

Table 5. Synthesis linked to research questions

| Research Question | Key Insights | Supporting Studies |
|---|---|---|
| RQ1: Applications | Blockchain is predominant in IoT security (28 studies) and supply chains (15); underrepresented in healthcare and real-time systems | [43, 44] |
| RQ2: Benefits | Enhanced data integrity (89% of studies); DDoS resilience (72%); high potential for anomaly detection via AI integration; improved trust in decentralized systems | [45, 46] |
| RQ3: Limitations & Future Directions | Scalability-performance trade-offs (65%); GDPR conflicts (43%); high energy consumption; lack of post-quantum cryptography validation; weak interoperability; sectoral and geographic gaps | [47, 48] |

The average latency (ττ) time in blockchain-based authentication systems measured 342±112342±112 ms, which exceeded the traditional PKI (89±2489±24 ms) time and highlighted scalability issues. Through Meta-regression analysis with a p-value below 0.05 and a regression slope (β1) equal to −0.17, it became clear that network size (NN) was a key factor in reducing overall throughput.

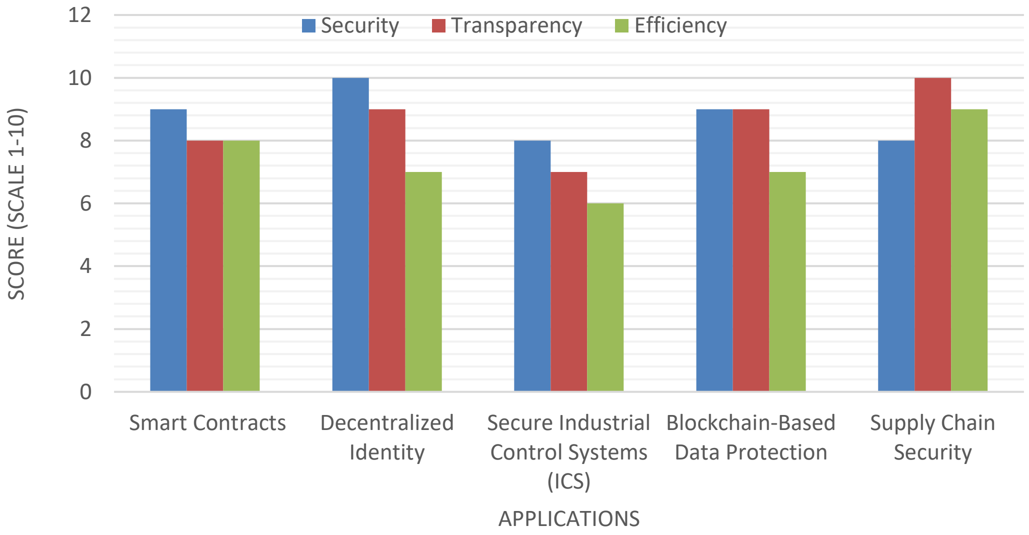

Figure 1. Blockchain-based cybersecurity

The bar chart depicts different applications of blockchain in cybersecurity and their importance in contributing to developing a strong internet security system. Some important use cases include smart contracts for secure automated transactions, a decentralized identity solution that minimizes the possibility of credential theft, and Protected Industrial Control Systems to mitigate cyber-physical risks.

The other uses include zero-knowledge proof (ZKP) to enhance users' privacy, blockchain intrusion detection that enables continuous security monitoring, and the immutable blockchain database that makes records virtually unalterable. The figure depicts how, due to the implementation of the blockchain approach, the risks have been weakened and distributed, and cryptographic tools have been incorporated into the layers of protection.

## 4. Discussion

This review finds that although blockchain is increasingly being integrated into security software development, the use of blockchain in that field still stands on an uneven footing concerning answering the research questions, and significant gaps remain between the theoretical potential and actual application of blockchain [49]. With 28 studies on blockchain applications in IoT security and 15 on supply chain provenance, blockchain enforces decentralized trust and tamper-evident logging (RQ1), which explains the predominance of these applications for this technology.

Usage of these cases utilizes the ability of the blockchain to remove the single point of failure in centralized architectures. Nevertheless, few applications of blockchain to real–time systems (e.g., industrial control), and the poor latency metrics ($\tau\tau$ for blockchain-based authentication systems ($342\pm112342\pm112$ ms) compared with traditional PKI ($89\pm2489\pm24$ ms) validate the RQ2 conclusion about performance tradeoffs. As a deterrent to blockchain adoption (RQ3), 43% of the studies identified an ongoing struggle between blockchain's immutability and GDPR compliance.

These results affirm and challenge the leading narratives in the literature when viewed in the larger context. It also has been consistent with previous surveys in that it confirms blockchain's cryptographic advantages of maintaining data integrity (89% of studies) and DDoS resilience (72%). It nevertheless deviates from more optimistic views about blockchain as another panacea for security by quantifying the scalability–performance trade-offs, a theme omitted from prior works on blockchain.

For instance, [50] theoretically established the scalability trilemma, while this review meta-regresses ($\beta1=-0.17$, $p<0.05$, $\beta1=-0.17$, $p<0.05$) to validate it, indicating that larger networks decrease throughput. Moreover, while the literature emphasizes sectoral biases (47% of studies studied finance), the broader extremism of blockchain as a domain-agnostic technology has been assumed in contrast to the fact that infrastructure and healthcare are understudied areas.

These findings imply various things. They also argue about the theoretical aspect of a blockchain as an ultimate security relief, suggesting the hybrid models for combining blockchain architecture with traditional systems, such as AI, to detect anomalies. In the context of blockchain, interoperability frameworks must be identified as a top priority by practitioners to bridge blockchain and legacy infrastructures, especially in the case of IoT and cloud environments, where configuration errors dictate the majority of breach statistics.

In the meantime, policy stakeholders who made a bet on blockchain are experiencing the urgent need to commensurate blockchain's immutability with a shifting body of data governance statutes, perhaps via evolving cryptographic primitives like chameleon hashes [51]. Nonetheless, the identified gaps, especially the absence of lifetime studies and post-quantum cryptographic validations, serve to provide researchers with a roadmap of investigative priorities that center on lifecycle analyses and worst-case tests on real conditions.

Its limitations limit the conclusions of this review. The exclusion of non-English studies and research from Russian institutions might lead to geographic bias and disregard the innovations that may occur in regions with different regulatory landscapes. Consistent with publication bias (where positive results outnumber negative ones: 65% of the studies pointed out benefits rather than limitations), blockchain's efficacy might be inflated.

Studies varied in methodology, primarily concerning performance metrics (e.g., definition of "throughput"), thus making comparisons across studies difficult and requiring alternative approaches to synthesis rather than uniform quantitative aggregation. Lastly, peer-reviewed literature did not focus on grey literature, such as industry white papers, which might have ignored the current applications.

Finally, although blockchain has excellent potential in specific security contexts, its use is dependent on surmounting technical, regulatory, and methodological hurdles. Technological system optimization needs to combine both how well a system performs and what physical rules apply to hydraulic engines [52], enterprise productivity [53] or blockchain technology. As hydraulic motor design influences pumping power, selecting Proof of Stake and Proof of Work decides how many transactions blockchains can handle and how much energy is used. Additionally, high energy consumption and regulatory ambiguity (e.g., GDPR conflicts) present systemic adoption barriers, especially in sectors such as healthcare where data sensitivity and compliance are paramount.

This study, grounded empirically and theoretically, thus forms a basis for targeted innovation, encouraging stakeholders to trade cryptography's rigor against pragmatic scalability and compliance concerns. Due to the nature of cybersecurity, we must continue to collaborate across disciplines to realize blockchain's promise as a robust, versatile security solution and digitalization [54].

## 5. Conclusions

This review explains the present usage of blockchain technology across security software development while detailing the promising but complex technical and regulatory barriers that remain. Research findings confirm that blockchain succeeds in safeguarding data purity while reducing trust centralization and preventing system breakdowns, especially while securing IoT networks and tracing supply chain origins.

The interplay of performance and scalability challenges manifests as significantly higher latency in blockchain-based systems (342 ± 112 ms) compared to traditional counterparts (89 ± 24 ms) – a 284% increase – alongside GDPR compliance hurdles. The published research shows apparent sectoral disparities because financial applications accounted for 47% of studies, yet critical infrastructure and healthcare applications are poorly studied. The review provides a direct, comprehensive assessment of blockchain applications with benefits and drawbacks to meet its research objective, which solves the three research questions:

1. Blockchain implementations exist primarily as authentication services and tamperproof logging solutions, although they struggle to penetrate time-sensitive or high-volume applications.
2. The advantages provided by blockchain technologies (cryptographic resilience) compete against disadvantages such as energy consumption problems and difficulties in integrating different systems.
3. The three critical gaps are the need for empirical evidence, sector representation and regulatory flexibility, which require attention through research that focuses on hybrid system designs and adaptable security compliance protocols.

The main contribution of blockchain to security software development consists of its ability to create Trust architectures through transparency while providing resilience against modern cyberattacks. The blockchain technological model serves a supporting role and thus needs a connection to present-day programs and upcoming technological solutions, including AI systems.

### 5.1. Recommendations

Professional practitioners should implement hybrid blockchain systems that combine distributed features with high-performance capabilities while establishing interconnected standards through cross-chain solutions.

Adapting data protection regulations [55] requires policymakers to work hand in hand with technologists to create flexible governance-compliant blockchain solutions. Research efforts should concentrate on developing post-quantum cryptographic protocols, conducting blockchain lifecycle cost studies, and using AI algorithms to optimize consensus methods to resolve scalability issues. Researchers should pursue this direction based on existing knowledge gaps in future investigations.

1. Interoperability Standards: developing universal frameworks for cross-chain communication in multi-platform environments.
2. Large-scale blockchain implementations must occur within the healthcare and energy grid industries, which are currently receiving minimal attention.
3. The development of adjustable blockchain modular systems should focus on creating flexible platforms that automatically conform to regional legal protocols.
4. The advancement of Qtum-based cryptography needs acceleration to make it suitable for mainstream blockchain protocol usage.

Stakeholders who address the specified priorities will reveal blockchain's ability to become a strong, adaptable base for next-generation security software, which unites cryptographic advancement with operational realities.

### 5.2. Limitations and future recommendations

The exclusive attention on digital systems restricted the possibility of gaining insights from fields including mechanical engineering [56]. Research must concentrate on following blockchain development through time to study operational expenses, developing inter-chain communication protocols, and expanding industry-specific blockchain analysis in healthcare and other under-researched fields [57]. Post-quantum cryptography integration combined with adaptive regulatory frameworks will resolve scalability issues and compliance problems to make blockchain work as a secure and scalable technology in real-world implementations.

### Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

### Funding information

No funding was received from any financial organization to conduct this research.

### Author contribution

The contribution to the paper is as follows: S. Zybin, O. Kubrak: study conception and design; P. Halachev: data collection; O. Kubrak, Ya. Kravchuk., O. Muliarevych: analysis and interpretation of results; O. Muliarevych: draft preparation. All authors approved the final version of the manuscript.

### References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf. [Accessed: April 28, 2025].

[2] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey", *International journal of web and grid services,* vol. 14, no. 4, pp. 352-375, 2018. https://doi.org/10.1504/IJWGS.2018.095647

[3] D. Andolfatto, and F. M. Martin, "The blockchain revolution: Decoding digital currencies", *Federal Reserve Bank of St. Louis Review,* 2022. [Online]. Available: https://www.stlouisfed.org/publications/review/2022/07/14/the-blockchain-revolution-decoding-digital-currencies. [Accessed: April 28, 2025].

[4] D. Korobtsova, V. Fursa, and A. Dobrovinskyi, "Cryptocurrencies as a new form of money: prospects for use and impact on the financial system in the future", *Futurity Economics & Law*, vol. 3, no. 3, pp. 49-66, 2023. https://doi.org/10.57125/FEL.2023.09.25.03

[5] T. Wang, C. Zhao, Q. Yang, S. Zhang, and S. C. Liew, "Ethna: Analyzing the underlying peer-to-peer network of Ethereum blockchain," *IEEE Transactions on Network Science and Engineering,* vol. 8, no. 3, pp. 2131-2146, 2021. https://doi.org/10.1109/TNSE.2021.3078181

[6] D. Grandjean, L. Heimbach, and R. Wattenhofer, "Ethereum proof-of-stake consensus layer: Participation and decentralization", *Financial Cryptography and Data Security. FC 2024 International Workshops*, pp. 253-280, 2024. https://doi.org/10.1007/978-3-031-69231-4_17

[7] D. L. Dinesha, and B. Patil, "Achieving interoperability in heterogeneous blockchain users through inter-blockchain communication protocol", *Authorea Preprints,* pp. 1-8, 2022. https://doi.org/10.36227/techrxiv.21532953.v1

[8] A. Rajavat, V. Bhardwaj, N. Kaur, R. Rawat, A. Rawat, and G. S. Jadon, "Sustainable Futures: Navigating Blockchain's Energy Dilemma", *Online Social Networks in Business Frameworks*, Chapter 5, pp. 85-112, 2024. https://doi.org/10.1002/9781394231126.ch5

[9] CISA. "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years", *Cybersecurity and Infrastructure Security Agency*. [Online]. Available: https://www.cisa.gov. [Accessed: April 28, 2025].

[10] V. Tumalavičius, "Legal Challenges for Blockchain Projects and Cryptocurrencies in the Context of Sustainable Development: International Virtual Currency Market and Technology Dynamics", *Law, Business and Sustainability Herald*, vol. 2, no. 3, pp. 27-41, 2022. https://www.lbsherald.org/index.php/journal/article/view/55

[11] J. Morillo Reina, and T. Mateo Sanguino, "Decentralized and Secure Blockchain Solution for Tamper-Proof Logging Events", *Future Internet,* vol. 17, no. 3, Article 108, 2025. https://doi.org/10.3390/fi17030108

[12] M. K. Dehury, B. K. Mohanta, M. Patnaik, B. Kumar, and P. Kumar, "Exploring the Synergy of Cybersecurity and Blockchain: Strengthening Digital Defenses", *Next-Generation Systems and Secure Computing*, Chapter 5, pp. 79-104, 2025. https://doi.org/10.1002/9781394228522.ch5

[13] O. E. K. Tuomi, *Moving to immutability: General Data Protection Regulation's right to be forgotten in blockchain transactions*, 2024. [Online]. Available: https://dspace.lu.lv/dspace/handle/7/67016. [Accessed: April 28, 2025].

[14] F. A. Reegu, H. Abas, Y. Gulzar, Q. Xin, A. A. Alwan, A. Jabbari, R. G. Sonkamble, and R. A. Dziyauddin, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system", *Sustainability,* vol. 15, no. 8, Article 6337, 2023. https://doi.org/10.3390/su15086337

[15] J. Govea, W. Gaibor-Naranjo, and W. Villegas-Ch, "Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience", *Computers,* vol. 13, no. 5, Article 122, 2024. https://doi.org/10.3390/computers13050122

[16] A. Zafar, F. Azam, A. Latif, M. W. Anwar, and A. Safdar, "Exploring the Effectiveness and Trends of Domain-Specific Model Driven Engineering: A Systematic Literature Review (SLR)", *IEEE Access*, vol. 12, pp. 86809-86830, 2024. https://doi.org/10.1109/ACCESS.2024.3414503

[17] M. Anjum, N. Kraiem, H. Min, A. K. Dutta, Y. I. Daradkeh, and S. Shahab, "Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning", *Scientific Reports,* vol. 15, no. 1, Article 7589, 2025. https://doi.org/10.1038/s41598-025-90908-1

[18] Y. Bai, S. Lee, and S.-H. Seo, "A Survey on Directed Acyclic Graph-Based Blockchain in Smart Mobility", *Sensors,* vol. 25, no. 4, Article 1108, 2025. https://doi.org/10.3390/s25041108

[19] V. Maurya, V. Rishiwal, M. Yadav, M. Shiblee, P. Yadav, U. Agarwal, and R. Chaudhry, "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions", *Peer-to-Peer Networking and Applications,* vol. 18, Article 35, 2025. https://doi.org/10.1007/s12083-024-01812-w

[20] T. Thamrin, Y. Arifin, and S. W. H. L. Hendric, "Trends in blockchain applications: Current and future perspectives", in *2nd International Conference on Software Engineering and Information Technology (ICoSEIT)*, IEEE, pp. 187-191, 2024. https://doi.org/10.1109/ICoSEIT60086.2024.10497520

[21] A. Nechibvute, and H. Mafukidze, "Integration of SCADA and Industrial IoT: Opportunities and challenges", *IETE Technical Review,* vol. 41, no. 3, pp. 312-325, 2024. https://doi.org/10.1080/02564602.2023.2246426

[22] X. Chen, S. He, L. Sun, Y. Zheng, and C. Q. Wu, "A survey of consortium blockchain and its applications", *Cryptography,* vol. 8, no. 2, Article 12, 2024. https://doi.org/10.3390/cryptography8020012

[23] J.-H. Syu, J. C.-W. Lin, G. Srivastava, and K. Yu, "A comprehensive survey on artificial intelligence empowered edge computing on consumer electronics", *IEEE Transactions on Consumer Electronics,* vol. 69, no. 4, pp. 1023-1034, 2023. https://doi.org/10.1109/TCE.2023.3318150

[24] F. Heiding, S. Katsikeas, and R. Lagerström, "Research communities in cyber security vulnerability assessments: A comprehensive literature review", *Computer Science Review,* vol. 48, Article 100551, 2023. https://doi.org/10.1016/j.cosrev.2023.100551

[25] T. A. Alghamdi, R. Khalid, and N. Javaid, "A survey of blockchain based systems: Scalability issues and solutions, applications and future challenges", *IEEE Access,* vol. 12, pp. 79626-79651, 2024. https://doi.org/10.1109/ACCESS.2024.3408868

[26] NIST. "Post-Quantum Cryptography Standardization: Finalists and Alternatives", *National Institute of Standards and Technology*. [Online]. Available: https://www.nist.gov. [Accessed: April 28, 2025].

[27] M. Abdelhamid, L. Sliman, R. Ben Djemaa, and G. Perboli, "A Review on Blockchain Technology, Current Challenges, and AI-Driven Solutions", *ACM Computing Surveys,* vol. 57, no. 3, pp. 1-39, 2024. https://doi.org/10.1145/3700641

[28] T. Nakai, A. Sakurai, S. Hironaka, and K. Shudo, "A Formulation of the Trilemma in Proof of Work Blockchain", *IEEE Access*, vol. 12, pp. 80559-80578, 2024. https://doi.org/10.1109/ACCESS.2024.3410025

[29] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more", *2018 IEEE symposium on security and privacy*, pp. 315-334, 2018. https://doi.org/10.1109/SP.2018.00020

[30] C. Cachin, and M. Vukolić, "Blockchain consensus protocols in the wild", *arXiv preprint,* 1707.01873, 2017. https://doi.org/10.48550/arXiv.1707.01873

[31] M. Zwilling, "Trends and challenges regarding cyber risk mitigation by CISOs – A systematic literature and experts' opinion review based on text analytics", *Sustainability,* vol. 14, no. 3, Article 1311, 2022. https://doi.org/10.3390/su14031311

[32] GSMA. "IoT Connections Forecast to 2030", *GSMA Intelligence*. [Online]. Available: https://www.gsmaintelligence.com/research/iot-connections-forecast-to-2030. [Accessed: April 28, 2025].

[33] V. Singh, and S. K. Sharma, "Application of blockchain technology in shaping the future of food industry based on transparency and consumer trust", *Journal of Food Science and Technology,* vol. 60, no. 4, pp. 1237-1254, 2023. https://doi.org/10.1007/s13197-022-05360-0

[34] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management", in *2016 2nd international conference on open and big data (OBD)*, pp. 25-30, 2016. https://doi.org/10.1109/OBD.2016.11

[35] A. Satybaldy, A. Hasselgren, and M. Nowostawski, "Decentralized identity management for e-Health applications: state-of-the-art and guidance for future work", *Blockchain in Healthcare Today,* vol. 5, 2022. https://doi.org/10.30953/bhty.v5.195

[36] C. Zheng, X. Peng, Z. Wang, T. Ma, J. Lu, L. Chen, L. Dong, L. Wang, X. Cui, and Z. Shen. "A review on blockchain applications in operational technology for food and agriculture critical infrastructure", *Foods,* vol. 14, no. 2, p. 251, 2025. https://doi.org/10.3390/foods14020251

[37] A. Zafar, "Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways", *Journal of Cybersecurity,* vol. 11, no. 1, Article tyaf002, 2025. https://doi.org/10.1093/cybsec/tyaf002

[38] B. Arun, Kumar, and R. Komala, "The Blockchain-Based Decentralized Approaches for Cloud Computing to Offer Enhanced Quality of Service in terms of Privacy Preservation and Security: A Review", *International Journal of Computer Science & Network Security,* vol. 21, no. 4, pp. 115-122, 2021. https://doi.org/10.22937/IJCSNS.2021.21.4.16

[39] B. Shrimali, and H. B. Patel, "Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities", *Journal of King Saud University-Computer and Information Sciences,* vol. 34, no. 9, pp. 6793-6807, 2022. https://doi.org/10.1016/j.jksuci.2021.08.005

[40] Y. Ma, and S. Fujita, "Decentralized incentive scheme for peer-to-peer video streaming using Solana blockchain", *IEICE TRANSACTIONS on Information and Systems,* vol. 106, no. 10, pp. 1686-1693, 2023. https://doi.org/10.1587/transinf.2023EDP7027

[41] M. S. Peelam, B. K. Chaurasia, A. K. Sharma, V. Chamola, and B. Sikdar, "Unlocking the potential of interconnected blockchains: a comprehensive study of cosmos blockchain interoperability", *IEEE Access*, vol. 12, pp. 171753-171776, 2024. https://doi.org/10.1109/ACCESS.2024.3497298

[42] Y. Zuo, "Exploring the Synergy: AI Enhancing Blockchain, Blockchain Empowering AI, and their Convergence across IoT Applications and Beyond", *IEEE Internet of Things Journal,* vol. 12, no 6, pp. 6171-6195, 2024. https://doi.org/10.1109/JIOT.2024.3507746

[43] A. D. Aguru, and S. B. Erukala, "Blockchain-based Edge Device Authentication Mechanism in SDN-enabled IoT Networks", in *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, pp. 1-6, 2024. https://doi.org/10.1109/I2CT61223.2024.10543758

[44] V. Sri Vigna Hema, and A. Manickavasagan, "Blockchain implementation for food safety in supply chain: A review," *Comprehensive Reviews in Food Science and Food Safety,* vol. 23, no. 5, Article e70002, 2024. https://doi.org/10.3390/fintech4010007

[45] A. Eghmazi, M. Ataei, R. J. Landry, and G. Chevrette, "Enhancing IoT data security: Using the blockchain to boost data integrity and privacy", *IoT,* vol. 5, no. 1, pp. 20-34, 2024. https://doi.org/10.3390/iot5010002

[46] G. S. OV, A. Karthikeyan, K. Karthikeyan, P. Sanjeevikumar, S. K. Thomas, and A. Babu, "Critical review of SCADA and PLC in smart buildings and energy sector", *Energy Reports,* vol. 12, pp. 1518-1530, 2024. https://doi.org/10.1016/j.egyr.2024.07.041

[47] K. Zanbouri, M. Darbandi, M. Nassr, A. Heidari, N. J. Navimipour, and S. Yalcın, "A GSO-based multi-objective technique for performance optimization of blockchain-based industrial Internet of things",

*International Journal of Communication Systems,* vol. 37, no. 15, Article e5886, 2024. https://doi.org/10.1002/dac.5886

[48] U. Tatar, Y. Gokce, and B. Nussbaum, "Law versus technology: Blockchain, GDPR, and tough tradeoffs", *Computer Law & Security Review,* vol. 38, Article 105454, 2020. https://doi.org/10.1016/j.clsr.2020.105454

[49] K. N. Molholm, "Standards and interoperability", *Information Services and Use,* vol. 26, no. 1, pp. 29-37, 2006. https://doi.org/10.3233/ISU-2006-26104

[50] S. Sai Ganesh, S. Surya Siddharthan, B. R. Rajakumar, S. Neelavathy Pari, J. Padmanabhan, and V. Priya, "Hybrid-AI blockchain supported protection framework for smart grids", *Science and Information Conference*, pp. 646-659, 2022. https://doi.org/10.1007/978-3-031-10467-1_39

[51] J. Werth, M. H. Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, "A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma", *ICEIS,* pp. 146-155, 2023. https://doi.org/10.5220/0011837200003467

[52] A. Panchenko, A. Voloshina, S. S. Sadullozoda, O. Boltyansky, and V. Panina, "Influence of the design features of orbital hydraulic motors on the change in the dynamic characteristics of hydraulic drives", *Design, Simulation, Manufacturing: The Innovation Exchange*, pp. 101-111, 2022. https://doi.org/10.1007/978-3-031-06044-1_10

[53] Z. S. Mukhametzhanova, A. N. Daurenbekova, G. K. Zhanibekova, K. S. Syzdykova, and G. Kaliakparova, “Evaluation of influence of innovation on enterprise productivity”, *Space and Culture India*, vol. 7, no. 1, 2019. https://doi.org/10.20896/saci.v7i1.527

[54] N. Smailov, V. Tsyporenko, A. Sabibolda, V. Tsyporenko, A. Abdykadyrov, A. Kabdoldina, …, and R. Kadyrova, “Streamlining digital correlation-interferometric direction finding with spatial analytical signal”, *Informatyka Automatyka Pomiary W Gospodarce I Ochronie Środowiska*, vol. 14, no. 3, pp. 43-48, 2024. https://doi.org/10.35784/iapgos.6177

[55] O. Y. Guseva, I. O. Kazarova, I. Y. Dumanska, M. A. Gorodetskyy, L. V. Melnichuk, and V. H. Saienko, “Personal data protection policy impact on the company development”, *WSEAS Transactions on Environment and Development*, vol. 18, pp. 232-246, 2022. https://doi.org/10.37394/232015.2022.18.25

[56] M. Riabchykov, V. Mytsa, O. Tkachuk, O. Pakholiuk, D. Melnyk, “Efficiency of Protective Textile Smart Systems Using Electronic Tags”, in *Lecture Notes in Networks and Systems*, Springer, Cham, vol 1008, pp. 189-197, 2024. https://doi.org/10.1007/978-3-031-61415-6_16

[57] L. Kurmangaziyeva, Zh. Oralbekova Sh. Akhmetzhanova, A. Khassenova M. Akishev, and T. Zhukabayeva, “Analysis of the Problem of Ensuring the Reliability of the Information System”, CEUR Workshop Proceedings, vol. 3382, Article 13, 2022. https://ceur-ws.org/Vol-3382/Paper13.pdf