applied sciences

MDPI

Systematic Review

Anomaly Detection in Blockchain: A Systematic Review of Trends, Challenges, and Future Directions

Ruslan Shevchuk [1,2,*], Vasyl Martsenyuk [1], Bogdan Adamyk [3], Vladlena Benson [3] and Andriy Melnyk [2,4]

[1] Department of Computer Science and Automatics, University of Bielsko-Biala, 43-309 Bielsko-Biala, Poland; vmartsenyuk@ubb.edu.pl
[2] Department of Computer Science, West Ukrainian National University, 46009 Ternopil, Ukraine; ame@wunu.edu.ua
[3] Aston Business School, Aston University, Birmingham B4 7ET, UK; b.adamyk@aston.ac.uk (B.A.); v.benson@aston.ac.uk (V.B.)
[4] Department of Clinical Engineering, Academy of Silesia, 40-555 Katowice, Poland
* Correspondence: rshevchuk@ubb.edu.pl

Abstract

Blockchain technology's increasing adoption across diverse sectors necessitates robust security measures to mitigate rising fraudulent activities. This paper presents a comprehensive bibliometric analysis of anomaly detection research in blockchain networks from 2017 to 2024, conducted under the PRISMA paradigm. Using CiteSpace 6.4.R1, we systematically map the knowledge domain based on 363 WoSCC-indexed articles. The analysis encompasses collaboration networks, co-citation patterns, citation bursts, and keyword trends to identify emerging research directions, influential contributors, and persistent challenges. The study reveals geographical concentrations of research activity, key institutional players, the evolution of theoretical frameworks, and shifts from basic security mechanisms to sophisticated machine learning and graph neural network approaches. This research summarizes the state of the field and highlights future directions essential for blockchain security.

Keywords: blockchain; anomaly detection; domaine map analysis; scientometric database; trends; knowledge graph; CiteSpace

check for updates

Academic Editors: Konstantinos Rantos and George Drosatos

Received: 5 July 2025
Revised: 23 July 2025
Accepted: 24 July 2025
Published: 26 July 2025

Citation: Shevchuk, R.; Martsenyuk, V.; Adamyk, B.; Benson, V.; Melnyk, A. Anomaly Detection in Blockchain: A Systematic Review of Trends, Challenges, and Future Directions. *Appl. Sci.* **2025**, *15*, 8330. https://doi.org/10.3390/app15158330

1. Introduction

Blockchain technology has emerged as one of the most transformative innovations of the 21st century, offering unprecedented capabilities in distributed storage, peer-to-peer transmission, strong confidentiality, and convenient traceability [1–3]. Since its inception with Bitcoin in 2008, blockchain technology has undergone substantial evolution, extending its applications far beyond cryptocurrencies into a wide array of sectors, including financial services, supply chain management, healthcare, emergency response, and the management of Internet of Things (IoT) ecosystems [4–10].

Despite the inherent security features of blockchain technology, such as cryptographic verification and distributed consensus, blockchain networks remain vulnerable to various attacks and fraudulent activities, necessitating robust anomaly detection systems [11–15].

Recent reports indicate a significant surge in fraudulent activities, attacks, and security incidents within blockchain networks, posing a serious threat to users' personal assets [16–21].

Anomalies in blockchain networks can take various forms, including malicious accounts, Ponzi schemes, PoW vulnerabilities, cryptojacking, spam transactions, wallet attacks, phishing scams, and more [22–25]. Detecting anomalies in blockchain networks is particularly challenging due to factors such as the immutability of records, the large volume and dynamic nature of transactions, the sophistication of attacks, and the class imbalance caused by the rarity of anomalous nodes [26–30].

These challenges have made anomaly detection a key area of research in blockchain systems. This growing interest has led to the publication of numerous surveys and review papers that aim to synthesize the state of the art in this field [31–38]. However, the majority of these surveys rely on traditional, narrative methodologies—they classify techniques, models, or domain-specific applications, often without providing a comprehensive, data-driven overview of the knowledge structure or research evolution.

For example, the survey article by Muneeb Ul Hassan et al. [31] provides a detailed overview of the integration of anomaly detection models at various blockchain layers, emphasizing the importance of timely response to threats. Similarly, Liu et al. [37], in their review, focus on the characteristics of anomalous transactions and methods for their detection in both financial and non-financial sectors.

Other surveys, such as the studies by Oussama Mounnan et al. [32] and Christos Cholevas et al. [33], analyze the use of deep learning and unsupervised algorithms in the context of blockchain anomalies. They highlight the potential of these methods for detecting complex and novel types of anomalies without the need for pre-labeled data.

The review by Vasavi Chithanuru and Mangayarkarasi Ramaiah [34] examines the interaction between artificial intelligence and blockchain, specifically how AI techniques contribute to improving the accuracy and adaptability of anomaly detection systems. Similar conclusions are drawn in the survey by Huy Tran Tien et al. [35], which demonstrates the effectiveness of combining blockchain and data mining methods for financial monitoring and fraud prevention.

Additionally, the survey by Xiaoqi Li et al. [37] offers a systematic analysis of real attacks on blockchain systems and describes modern protection mechanisms, including anomaly detection methods that combine cryptography and machine learning.

Crucially, none of the existing studies incorporate a bibliometric approach, nor do they follow a systematic review protocol such as PRISMA to ensure replicability and transparency. The absence of bibliometric mapping means that current overviews do not adequately highlight influential contributions, emerging trends, or structural research gaps at a macro-level.

This review fills a key gap by offering a structured, data-driven overview of blockchain anomaly detection research. We apply the PRISMA methodology to select 363 high-quality research papers from the Web of Science Core Collection (WoSCC) and utilize CiteSpace v6.4.R1 to generate quantitative knowledge maps. Through co-citation clustering, keyword timeline analysis, and citation bursts, we capture the intellectual foundations and research frontiers of blockchain anomaly detection. In addition, our analysis of author and institutional collaboration networks reveals how research efforts are distributed and interconnected globally. The study focuses on the following research questions (RQs):

RQ1: Which countries, institutions, and authors collaborate in research on blockchain anomaly detection, and what are their key contributions to advancing this field?

RQ2: What are the main research clusters, hotspots, and evolving trends in the application of blockchain anomaly detection techniques?

RQ3: What are the emerging challenges and future research directions for anomaly detection in blockchain networks?

The main contributions of this paper are as follows:

1. We present a bibliometric mapping of blockchain anomaly detection research from 2017 to 2024 based on 363 articles indexed in WoSCC. The analysis outlines the global

research landscape, major thematic areas, and the evolution of key topics in this rapidly developing field.

2. Using CiteSpace v6.4.R1, we conducted analyses of country and institutional collaboration networks, co-citation networks, references with citation bursts, and keyword co-occurrence. These results uncover the intellectual structure of the field and identify influential authors, leading institutions, and methodological innovations.
3. Through keyword timeline and burst detection, we highlight a shift in research focus from foundational mechanisms, such as rule-based and consensus-level detection—to advanced approaches including unsupervised learning, lightweight federated learning, and graph neural networks. These insights help researchers to understand how the field is evolving and where innovation is emerging.
4. Our analysis reveals distinct geographical clusters of research activity, with China, the United States, and India dominating publication output. Key institutions identified as major contributors include Beijing University of Posts and Telecommunications (China), Brandon University (Canada), and Nirma University (India). The most productive scholars hail predominantly from Canada, India, and China, collectively forming the core group driving the field's publication impact.
5. We outline open challenges and future research directions in blockchain anomaly detection, including federated learning and privacy-preserving techniques, the integration of multimodal and heterogeneous data sources, the development of explainable and interpretable AI models, real-time adaptive detection systems, cross-domain specialized applications, and the imperative need for standardization and regulatory frameworks.

The structure of the remaining part of the paper is as follows. Section 2 provides details on the research methodology employed in this study. Section 3 presents the findings of the bibliometric analysis, including insights from reference co-citation clustering, emerging research trends, highly cited references, and a network map that revealed major distinct clusters, which were subsequently evaluated. Section 4 discusses the study's findings, noting limitations and outlining directions for future work. The Section 5 provides the conclusions of this study.

2. Materials and Methods

2.1. Data Collection

To conduct this bibliometric investigation, data was extracted from the WoSCC database. This database is widely recognized for its comprehensive coverage of more than 21,000 influential, international, interdisciplinary, and high-impact academic journals across various disciplines, with its extensive temporal range spanning from 1900 to the present [39]. The choice of WoSCC has garnered broad acclaim among numerous researchers. Furthermore, visual analysis using CiteSpace has shown that WoSCC can yield superior bibliometric mapping effects [40,41]. Therefore, we reasonably selected the WoSCC as the data source for our study.

The literature search in the WoSCC was conducted within a single day, specifically up to 17 March 2025, to avoid any potential biases caused by ongoing database updates. The search strategy employed the terms "anomaly detection" and "blockchain", with the publication time span limited from 1 January 2017 to 31 December 2024. The search was conducted across All Fields, allowing the query to match occurrences of the terms in any searchable field, including titles, abstracts, keywords, and full metadata. To ensure the relevance and quality of the dataset, records such as early-access articles, editorial materials, conference abstracts, letters, book reviews, corrections, and news items were excluded. Only articles published in English were considered.

The study followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure methodological transparency and replicability [42,43]. The literature screening process was supported by an online tool based on the R package v1.1.3 for PRISMA 2020 [44], which generated the standardized flow diagram (Figure 1).

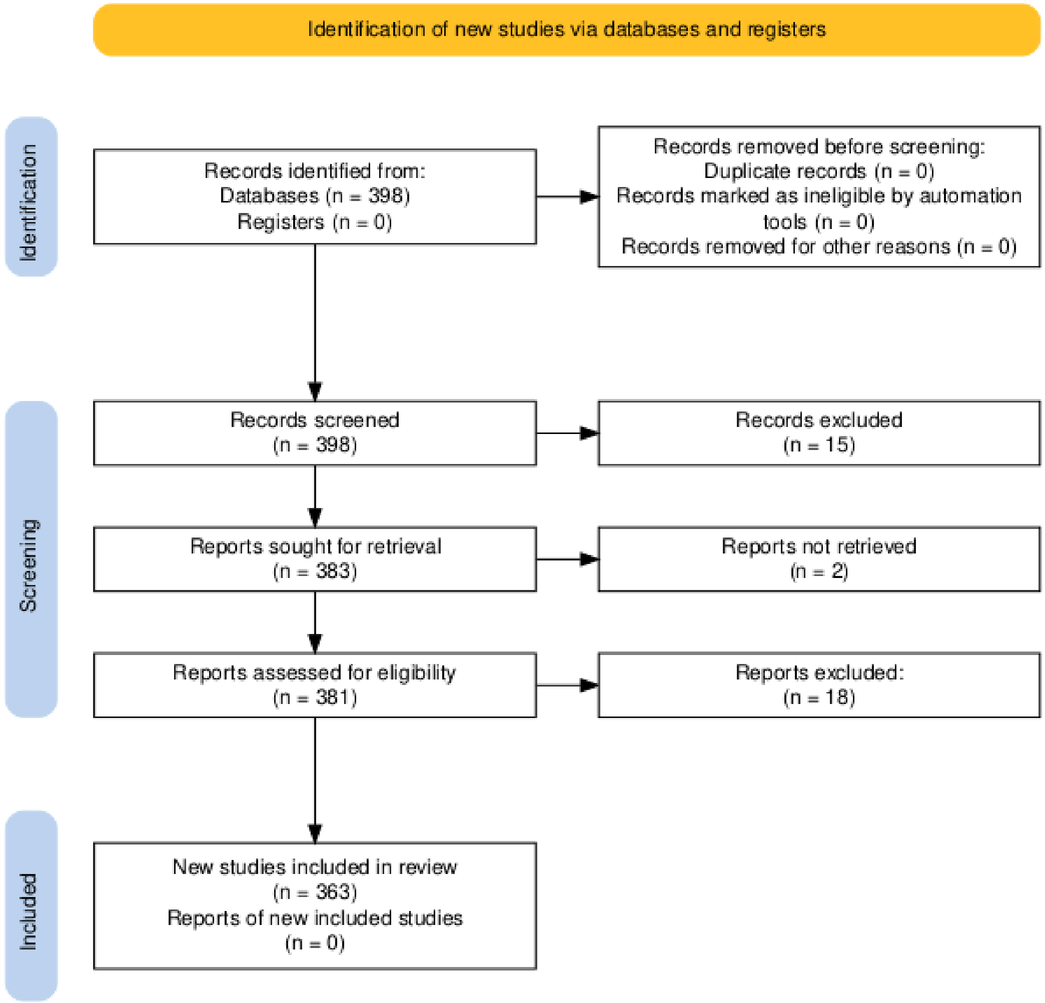

Identification of new studies via databases and registers
Identification
Screening
Included
Records identified from:
Databases (n = 398)
Registers (n = 0)
Records removed before screening:
Duplicate records (n = 0)
Records marked as ineligible by automation tools (n = 0)
Records removed for other reasons (n = 0)
Records screened
(n = 398)
Records excluded
(n = 15)
Reports sought for retrieval
(n = 383)
Reports not retrieved
(n = 2)
Reports assessed for eligibility
(n = 381)
Reports excluded:
(n = 18)
New studies included in review
(n = 363)
Reports of new included studies
(n = 0)

Figure 1. PRISMA flow diagram for the search process.

The flow diagram shows three phases: identification, screening, and inclusion. We retrieved 398 publications, exported them to Excel, and excluded 15 irrelevant records based on titles and abstracts. Two articles were removed due to unavailable full texts, and eighteen more after full content review. Finally, 363 original research articles were selected for analysis in CiteSpace. The complete content of each record, including "full record and cited references", was downloaded and saved in plaintext format to preserve data integrity and ensure future accessibility.

Since this is a bibliometric study, formal bias assessment was not applicable.

2.2. Research Methodology

The visualization of abstract data relationships through interactive graphical representations, known as knowledge graphs, enables researchers to comprehend intricate information connections and patterns [45].

For our methodological approach, we employed CiteSpace—a widely recognized bibliometric analysis software created by professor Chen Chaomei that has gained significant traction across scientific communities. This tool analyzes links between researchers, publications, and domains by extracting data such as author names, affiliations, keywords, and journal venues from scientific databases [46,47].

The primary objective of our analytical approach is to identify predominant research clusters, developmental trajectories, and evolving trends within the blockchain anomaly detection domain. To support interpretation, we visualized the data using bibliometric mapping techniques. Our implementation specifically utilized CiteSpace version 6.4.R1, configured with the following analytical parameters: temporal segmentation into one-year intervals, g-index parameterization at 25, maximum node selection threshold (Top N) established at 50, and percentage-based selection criteria (TopN%) configured at 10.

The results were synthesized through a combination of quantitative and visual analyses using CiteSpace. Specifically, bibliometric networks were generated to identify and display co-authorship patterns, institutional collaborations, keyword co-occurrence clusters, and citation bursts. These visual knowledge graphs were supported by descriptive statistics. This integrative approach allowed for the comprehensive exploration of structural and temporal dynamics in the research domain.

3. Results

3.1. Assessment of Publication Count

The bibliometric data extracted from the WoSCC database demonstrates a clear upward trajectory in scholarly output from 2017 through 2024 (Figure 2).

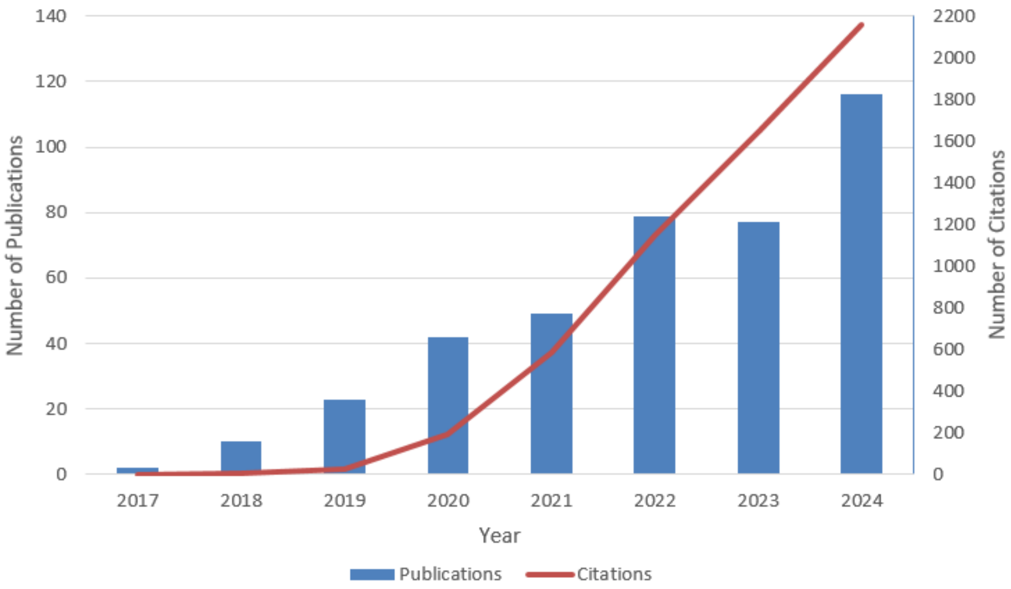


Figure 2. Number of citations and publications in the field of anomaly detection in blockchain from 2017 to 2024.

The nascent stage of this research area is evident in the minimal publication count of just two articles in 2017, representing the earliest formal investigations into anomaly detection specifically within blockchain contexts. This initial modest output quickly accelerated, with publication volume expanding fivefold to 10 articles in 2018, followed by continued substantial growth to 23 publications in 2019.

The field gained considerable momentum during 2020 and 2021, with annual outputs of 39 and 46 publications, respectively, signaling the growing recognition of blockchain security challenges within the academic community. A dramatic surge occurred in 2022, with 76 published works.

While 2023 showed a slight moderation with 67 publications, this temporary plateau was followed by unprecedented growth in 2024, which recorded 115 publications—the highest annual output to date. This reflects a 72% annual increase and a 57-fold growth since 2017.

From 2017 to 2024, citations increased from 0 to more than 2100, with 86% of all citations occurring in the last three years. This trend highlights the growing impact and recognition of blockchain anomaly detection research.

3.2. Analysis of the Collaboration Network Among Countries

Figure 3 illustrates the global collaboration network among countries involved in blockchain anomaly detection research, comprising 77 countries connected by 254 collaborative links.

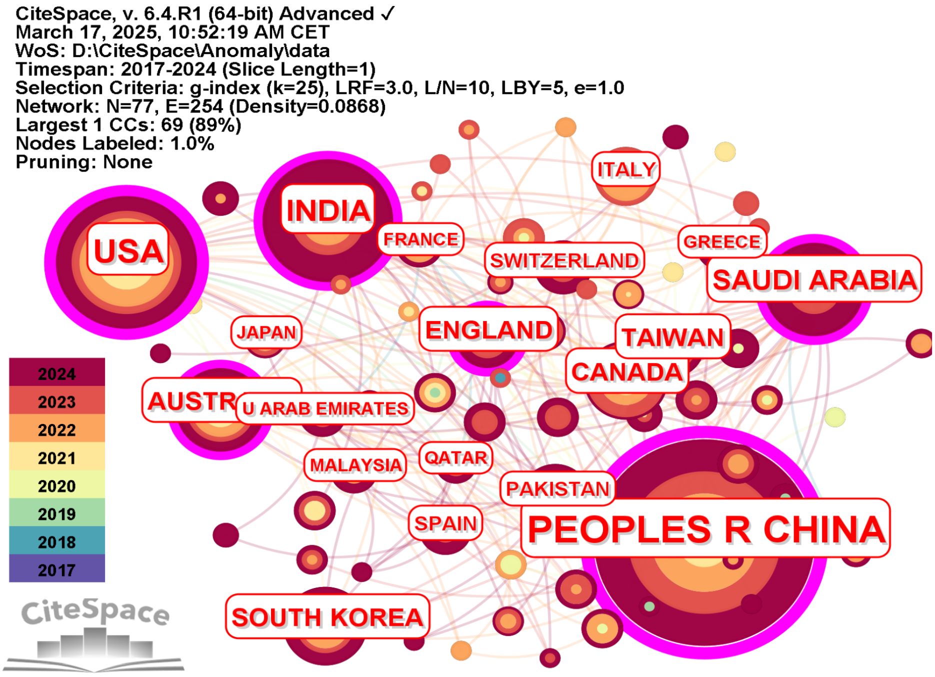


Figure 3. The collaboration network among countries.

With a network density of 0.0868, this structure reveals a relatively sparse yet highly concentrated research landscape. A low density suggests that, while strong collaborative clusters exist, overall global cooperation is not yet fully integrated. This implies potential challenges for efficient knowledge diffusion and the establishment of unified research priorities across the field.

China dominates the field with 137 publications (34.42% of total), demonstrating significant strategic investment in blockchain security research. The United States (63 publications, 15.83%) and India (51 publications, 12.81%) form the second tier, collectively accounting for nearly two-thirds of global output. Saudi Arabia emerges as a regional leader with 34 publications (8.54%), surpassing several technologically advanced nations.

The analysis of the research ecosystem reveals a landscape characterized by four distinct geographical clusters:

1. Asian cluster: Dominated by China (34.42%), which reflects the country's national blockchain development strategy and centralized research funding mechanisms. South Korea (6.03%) and Taiwan (4.77%) demonstrate strong technical capabilities, particularly in cryptographic implementations. India's (12.81%) growth in this area correlates with its Digital India initiative and the increasing adoption of cryptocurrency [48].

2. North American cluster: Led by USA (15.83%) researchers and institutions, who are pioneers in developing advanced detection methods, particularly using graph neural networks. Canada (5.28%) also contributes to this cluster.

3. Middle Eastern cluster: Saudi Arabia (8.54%) leads with its NEOM smart city project and $6.4 billion blockchain investment plan [49]. UAE (2.01%) and Qatar (1.76%) are also emerging as key players with expertise in financial blockchain applications.

4. European cluster: This cluster presents a more fragmented landscape, but demonstrates high-impact contributions from countries such as England (4.77%), Italy (3.02%), Switzerland (2.51%), and Germany (1.76%). Several collaborative projects in Europe focus on blockchain anomaly detection, bringing together expertise from academia, industry, and international organizations to enhance blockchain security. Notable initiatives include the MSCA Digital Finance project, the anomaly and fraud detection in blockchain networks project by Bern University [50], the project to prevent the criminal use of blockchain technology [51], and the Ontochain initiative [52], all of which address key challenges in fraud detection, security, and innovation within blockchain.

The long-tail distribution includes 58 countries with 5 or fewer publications, indicating growing global interest.

This geographical analysis underscores the critical need for standardized international frameworks to address blockchain security challenges, particularly given the technical disparities between leading and emerging research nations. The concentration of research capabilities in specific regions may create asymmetries in global blockchain governance frameworks.

3.3. Analysis of the Collaboration Network Involving Leading Institutions

CiteSpace software was used to perform a comprehensive analysis of the institutional collaboration landscape, revealing a knowledge graph comprising 210 different institutional nodes (Figure 4).

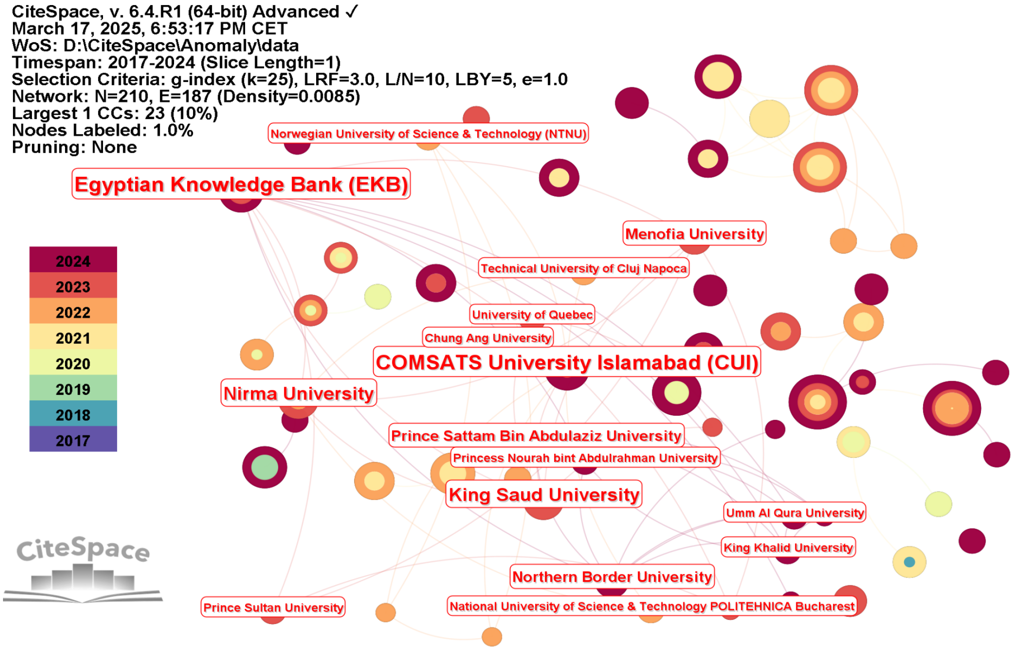

CiteSpace, v. 6.4.R1 (64-bit) Advanced ✓
March 17, 2025, 6:53:17 PM CET
WoS: D:\CiteSpace\Anomaly\data
Timespan: 2017-2024 (Slice Length=1)
Selection Criteria: g-index (k=25), LRF=3.0, L/N=10, LBY=5, e=1.0
Network: N=210, E=187 (Density=0.0085)
Largest 1 CCs: 23 (10%)
Nodes Labeled: 1.0%
Pruning: None
2024
2023
2022
2021
2020
2019
2018
2017
CiteSpace
Norwegian University of Science & Technology (NTNU)
Egyptian Knowledge Bank (EKB)
Menofia University
Technical University of Cluj Napoca
University of Quebec
Chung Ang University
COMSATS University Islamabad (CUI)
Nirma University
Prince Sattam Bin Abdulaziz University
Princess Nourah bint Abdulrahman University
King Saud University
Umm Al Qura University
King Khalid University
Northern Border University
Prince Sultan University
National University of Science & Technology POLITEHNICA Bucharest

Figure 4. The collaboration network between institutions.

The network exhibits a very low density of 0.0085, indicating weak overall connectivity between institutions. This means that, although many institutions are contributing to the field, they tend to work in isolation or within small, localized clusters rather than forming widespread global partnerships.

This sparse structure is particularly striking when contrasted with the high volume of research outputs. This suggests that blockchain anomaly detection remains a fragmented research area, where institutional silos dominate over broader collaborative frameworks. As a result, the limited cross-institutional collaboration may hinder the flow of knowledge and best practices across regions. It also raises concerns about the potential emergence of isolated research traditions, with institutions possibly developing inconsistent methodologies and technical standards due to limited interaction with the broader research community.

An analysis of the contributions from 15 leading institutions to blockchain anomaly detection research reveals a distinctive leadership pattern characterized by geographic concentration, as presented in Table 1.

Table 1. Leading institutions by publication count.

#	Research Institution	Country	Count
1	Beijing University of Posts and Telecommunications	China	10
2	University of Electronic Science and Technology of China	China	10
3	Brandon University	Canada	8
4	China Medical University Taiwan	Taiwan	8
5	King Saud University	Saudi Arabia	8
6	Chinese Academy of Sciences	China	7
7	Egyptian Knowledge Bank	Egypt	6
8	Guangzhou University	China	6
9	National Institute of Technology System	India	6
10	Nirma University	India	6
11	Northern Border University	Saudi Arabia	6
12	Texas A&M University System	USA	6
13	University System of Georgia	USA	6
14	Vellore Institute of Technology	India	6
15	Xidian University	China	6

Particularly noteworthy is the equal representation of institutions from developed and developing economies, suggesting that blockchain security constitutes an area where traditional technological hierarchies may be less pronounced.

Chinese research institutions demonstrate particular prominence, with Beijing University of Posts and Telecommunications and the University of Electronic Science and Technology of China jointly leading with 10 publications each. Five Chinese institutions collectively account for one-third of publications among the top-fifteen contributors, demonstrating China's coordinated approach to blockchain security research. Indian institutions demonstrate a significant collaborative presence, with three representatives (National Institute of Technology System, Nirma University, and Vellore Institute of Technology) among the leading contributors, each with six publications. Similarly, Saudi Arabian institutions (King Saud University and Northern Border University) have established themselves as regional centers of excellence, potentially leveraging blockchain technologies to support national economic diversification strategies.

3.4. The Analysis of the Collaboration Network Leading Authors

The bibliometric analysis of the area reveals a dynamic authorship landscape characterized by both concentrated productivity and distinct citation patterns. Among the 363 analyzed papers, contributions came from 220 unique researchers, indicating moderate authorship concentration, with an average of 1.8 publications per author.

Table 2 provides details on the top-10 authors, specifically their names, affiliations, publication count, and the year of their first publication.

Table 2. Top 10 authors based on publication count.

#	Author	Research Institution	Count	Year
1	Srivastava Gautam	Brandon University, Canada	8	2021
2	Tanwar Sudeep	Nirma University, India	6	2022
3	Kumar Prabhat	National Institute of Technology, India	5	2021
4	Li Tao	Guizhou University, China	5	2019
5	Zhang Kaiwen	Ecole de Technologie Supérieure, Canada	5	2022
6	Chang Sang-Yoon	University of Colorado, USA	4	2021
7	Fan Wenjun	University of Colorado, USA	4	2021
8	Kim Jinoh	Texas A&M University, USA	4	2021
9	Kumar Randhir	National Institute of Technology, India	4	2021
10	Li Ji	SKL-MEAC, China	4	2020

Notably, 7 of the 10 most productive authors began publishing in this field in 2021 or later, indicating a recent acceleration in specialized research activity.

An analysis of the co-citation network reveals a distinct stratification between publication productivity and intellectual influence (Table 3).

Table 3. Top-10 most frequently co-cited authors.

#	Author	Research Institution	Centr.	Count	Year
1	Satoshi Nakamoto	—	0.17	206	2018
2	Mohamed Amine Ferrag	Guelma University, Algeria	0.07	58	2020
3	Zibin Zheng	Sun Yat-Sen University, China	0.04	32	2019
4	Gavin Wood	Ethereum Foundation, UK	0.06	29	2018
5	Varun Chandola	University of Minnesota, USA	0.09	28	2018
6	Thai T. Pham	Stanford University, USA	0.05	27	2020
7	Nour Moustafa	University of New South Wales at ADFA, Australia	0.02	27	2020
8	Ayoub Khan	University of Bisha, Saudi Arabia	0.06	24	2019
9	Pradeep Kumar	Indian Institute of Management Ranchi, India	0.05	23	2021
10	Weili Chen	Sun Yat-Sen University, China	0.04	23	2021

Most notably, Satoshi Nakamoto, the pseudonymous creator of Bitcoin, demonstrates overwhelming citation dominance, with 206 citations and the highest centrality measure (0.17). This citation pattern underscores the foundational nature of Bitcoin's original technical documentation in anchoring subsequent blockchain security research.

Nakamoto (206 citations) and Wood (29 citations) represent blockchain architecture pioneers whose conceptual frameworks continue to inform security research despite predating the specialized anomaly detection literature. Varun Chandola (University of Minnesota), with 28 citations and a centrality of 0.09, has contributed fundamental anomaly detection techniques that researchers have adapted to blockchain contexts.

3.5. Keyword Network Analysis

The visualization of keyword co-occurrence networks provides critical insights into the conceptual structure and thematic evolution of blockchain anomaly detection research. Using CiteSpace software, we constructed a network visualization where nodes represent individual keywords and connecting lines indicate the frequency of co-occurrence in research publications. The node size corresponds to keyword frequency, while line thickness represents co-occurrence strength, collectively revealing the semantic landscape of this emerging research domain.

As shown in Figure 5, "anomaly detection" stands out as the central node, appearing 168 times and clearly representing the core concept of the field.

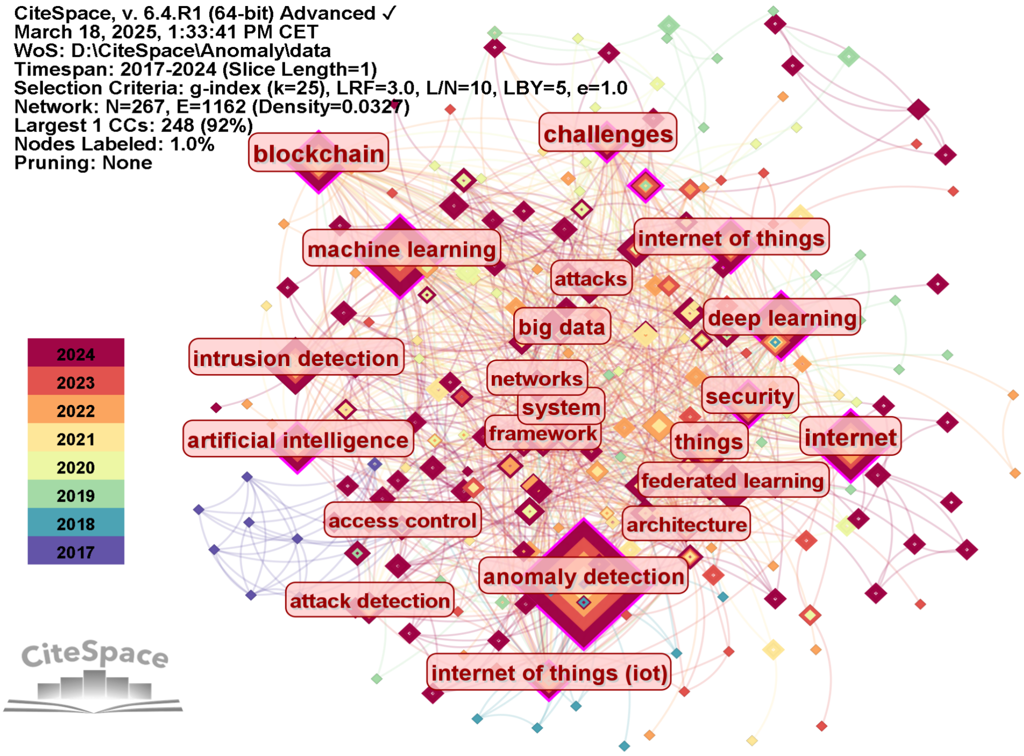

CiteSpace, v. 6.4.R1 (64-bit) Advanced ✓
March 18, 2025, 1:33:41 PM CET
WoS: D:\CiteSpace\Anomaly\data
Timespan: 2017-2024 (Slice Length=1)
Selection Criteria: g-index (k=25), LRF=3.0, L/N=10, LBY=5, e=1.0
Network: N=267, E=1162 (Density=0.0327)
Largest 1 CCs: 248 (92%)
Nodes Labeled: 1.0%
Pruning: None

Figure 5. Network visualization map of keywords.

The second-most frequent keyword is "machine learning" (75 occurrences), underlining the field's strong reliance on intelligent algorithmic methods. Other high-frequency terms such as "internet" (49), "deep learning" (46), "blockchain" (43), and "internet of things" (30) reflect the interdisciplinary nature of the domain, bridging cybersecurity, data science, and distributed systems. Additional keywords with notable presence include "artificial intelligence," "federated learning," "big data," "IoT architecture," and "authentication", highlighting emerging technical approaches and application areas.

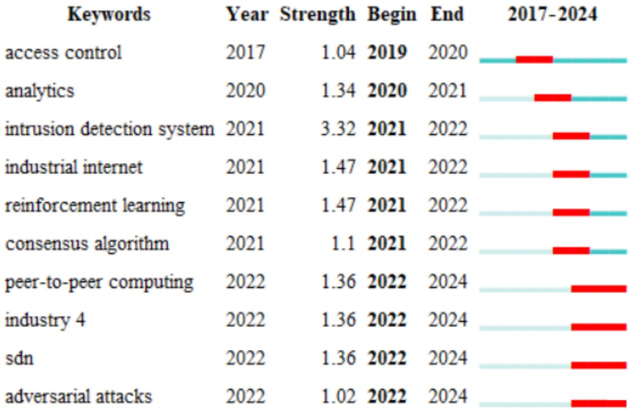
The burst detection analysis provides critical insights into the dynamic evolution of research priorities over time. Figure 6 presents the top-ten keywords with the strongest citation bursts, revealing distinct phases in the field's development between 2017 and 2024:

1. Foundation phase (2019–2020): Early research emphasized fundamental security concepts, with "access control" experiencing a citation burst (strength 1.04). This period represented the initial adaptation of established security principles to blockchain environments.

2. Analytical development phase (2020–2021): The emergence of "analytics" as a burst keyword (strength 1.34) signaled a transition toward data-centric approaches, reflecting the growing recognition of anomaly detection as fundamentally a data analysis challenge.

3. Methodological diversification phase (2021–2022): This period witnessed the simultaneous emergence of multiple specialized methodological approaches, with "intrusion detection system" registering the strongest burst across all periods (strength 3.32). Concurrent bursts in "reinforcement learning" (1.47), "industrial internet" (1.47), and "consensus algorithm" (1.10) indicate the rapid diversification of both methodological approaches and application domains.

4. Integration and resilience phase (2022–2024): The most recent period exhibits a shift toward architectural integration and security resilience concerns. Keywords experiencing ongoing bursts include "peer-to-peer computing," "industry 4," "sdn" (software-defined networking), and notably "adversarial attacks," signaling increased attention to offensive security perspectives.



Keywords	Year	Strength	Begin	End	2017-2024
access control	2017	1.04	**2019**	2020	
analytics	2020	1.34	**2020**	2021	
intrusion detection system	2021	3.32	**2021**	2022	
industrial internet	2021	1.47	**2021**	2022	
reinforcement learning	2021	1.47	**2021**	2022	
consensus algorithm	2021	1.1	**2021**	2022	
peer-to-peer computing	2022	1.36	**2022**	2024	
industry 4	2022	1.36	**2022**	2024	
sdn	2022	1.36	**2022**	2024	
adversarial attacks	2022	1.02	**2022**	2024	

Figure 6. Top-10 keywords with the strongest citation bursts.

In the Figure 6, cyan bar indicates the overall citation timeline of the keyword, while the red segment highlights the period of the most intense citation burst activity. "Strength" refers to the intensity of the citation burst for a given keyword—the higher the value, the more frequently the keyword appeared during that period.

3.6. Research Hotspots and Evolution Trend Analysis

In this section, we use co-citation analysis to gain insights into research development and identify emerging trends within the field of blockchain anomaly detection. We conducted a clustering analysis of co-cited references using CiteSpace software, resulting in a network map categorized into 11 major clusters (Figure 7).

The network quality metrics confirm the reliability of our analysis. The mean silhouette value (S) of 0.9202, significantly exceeding the threshold of 0.7, indicates highly homogeneous clusters. Similarly, the modularity value (Q) of 0.758, well above the 0.3 threshold, demonstrates clear boundaries between different research streams. These metrics validate the robustness of the identified intellectual structure.

Figure 8 demonstrates the evolution of research within each cluster, where the points on the horizontal axis represent frequently cited references by publication year, the connecting lines show the cocitation relationships, and the size of the point indicates the frequency of citation.

The color of each circle conveys the relative influence and temporal dynamics of individual publications. Red circles indicate references that experienced the strongest citation bursts, reflecting publications that attracted significant attention during specific periods. Orange circles represent works with a moderate level of influence, characterized by steady but less intense citation activity. In contrast, blue and grey circles correspond to references with lower impact. Circles outlined in purple highlight publications with high betweenness centrality, emphasizing their role as critical connectors between thematic clusters.

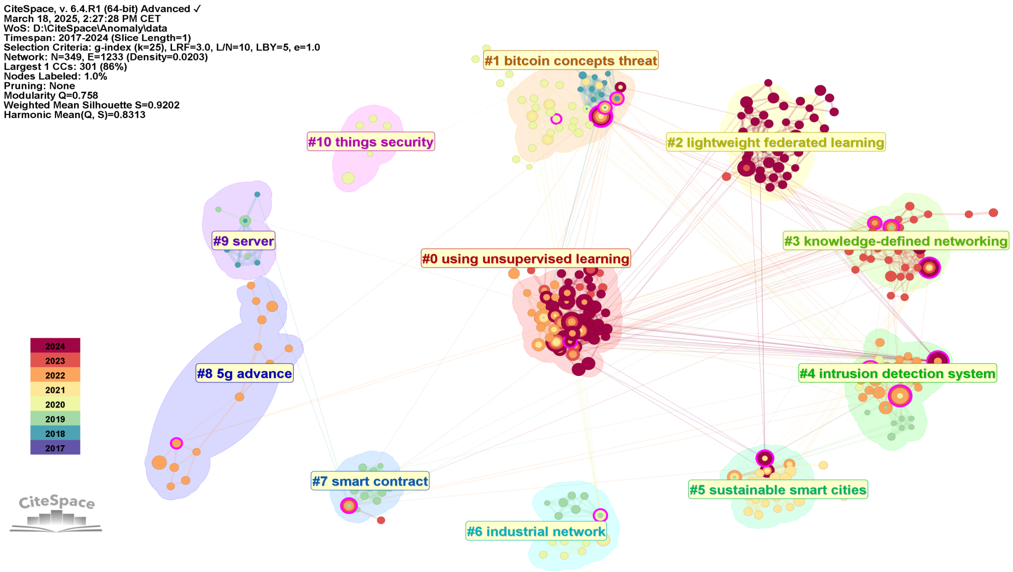

CiteSpace, v. 6.4.R1 (64-bit) Advanced ✓
March 18, 2025, 2:27:28 PM CET
WoS: D:\CiteSpace\Anomaly\data
Timespan: 2017-2024 (Slice Length=1)
Selection Criteria: g-index (k=25), LRF=3.0, L/N=10, LBY=5, e=1.0
Network: N=349, E=1233 (Density=0.0203)
Largest 1 CCs: 301 (86%)
Nodes Labeled: 1.0%
Pruning: None
Modularity Q=0.758
Weighted Mean Silhouette S=0.9202
Harmonic Mean(Q, S)=0.8313
#1 bitcoin concepts threat
#10 things security
#2 lightweight federated learning
#9 server
#0 using unsupervised learning
#3 knowledge-defined networking
2024
2023
2022
2021
2020
2019
2018
2017
#8 5g advance
#4 intrusion detection system
#7 smart contract
#5 sustainable smart cities
#6 industrial network
CiteSpace

Figure 7. Visualization of the research clusters in the co-citation network.

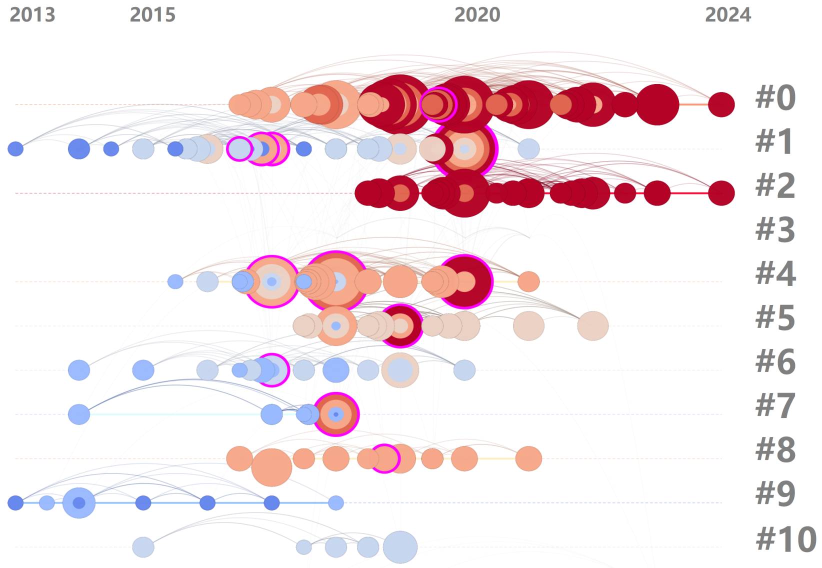
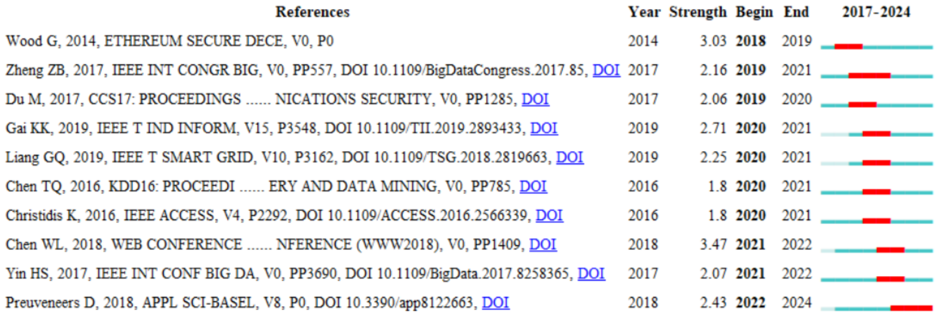


Figure 8. Visualization of the timeline map of reference co-citation.

The timeline map illustrates how burst patterns manifest within the broader intellectual structure of the field. The horizontal distribution of nodes reveals how research focus has progressively shifted from foundational topics like “bitcoin concepts threat” (#1), “industrial network” (#6), “smart contract” (#7), and “server” (#9), toward methodologically advanced domains like “using unsupervised learning” (#0) and “lightweight federated learning” (#2).

Figure 9 presents the top-10 references exhibiting the strongest citation bursts within the blockchain anomaly detection research landscape. These bursts highlight pivotal works that significantly influenced the field during specific periods, shaping subsequent research directions and methodological innovations. The selected references span a publication period from 2014 to 2019, with burst periods ranging from 2018 to 2024.



References	Year	Strength	Begin	End	2017-2024
Wood G, 2014, ETHEREUM SECURE DECE, V0, P0	2014	3.03	**2018**	2019	
Zheng ZB, 2017, IEEE INT CONGR BIG, V0, PP557, DOI 10.1109/BigDataCongress.2017.85, DOI	2017	2.16	**2019**	2021	
Du M, 2017, CCS17: PROCEEDINGS ...... NICATIONS SECURITY, V0, PP1285, DOI	2017	2.06	**2019**	2020	
Gai KK, 2019, IEEE T IND INFORM, V15, P3548, DOI 10.1109/TII.2019.2893433, DOI	2019	2.71	**2020**	2021	
Liang GQ, 2019, IEEE T SMART GRID, V10, P3162, DOI 10.1109/TSG.2018.2819663, DOI	2019	2.25	**2020**	2021	
Chen TQ, 2016, KDD16: PROCEEDI ...... ERY AND DATA MINING, V0, PP785, DOI	2016	1.8	**2020**	2021	
Christidis K, 2016, IEEE ACCESS, V4, P2292, DOI 10.1109/ACCESS.2016.2566339, DOI	2016	1.8	**2020**	2021	
Chen WL, 2018, WEB CONFERENCE ...... NFERENCE (WWW2018), V0, PP1409, DOI	2018	3.47	**2021**	2022	
Yin HS, 2017, IEEE INT CONF BIG DA, V0, PP3690, DOI 10.1109/BigData.2017.8258365, DOI	2017	2.07	**2021**	2022	
Preuveneers D, 2018, APPL SCI-BASEL, V8, P0, DOI 10.3390/app8122663, DOI	2018	2.43	**2022**	2024	

Figure 9. Top-10 references with the strongest citation bursts. References cited in the figure: [26,27,53–60].

The Ethereum whitepaper by Wood G. (2014) [53], a foundational work in blockchain development, saw a strong citation burst from 2018 to 2019 (strength: 3.03). This burst reflects Ethereum's critical role in enabling decentralized applications (DApps) and smart contracts, as well as its influence on subsequent research in blockchain technologies.

The introduction of DeepLog, a deep learning model using LSTM for anomaly detection in system logs described in paper [26], had a citation burst from 2019 to 2020 (strength: 2.12).

The comprehensive survey of blockchain technology by Zheng ZB. et al. (2017) [54] experienced a citation burst from 2019 to 2021 (strength: 2.01). This paper catalyzed research into blockchain scalability, security, and consensus mechanisms -areas critical for secure and efficient anomaly detection in decentralized networks.

Research on detecting Ponzi schemes in blockchain environments through machine learning, conducted by Chen WL. (2018) [55], had the highest citation burst (strength: 3.31) between 2021 and 2022, highlighting the rising concerns over fraud in decentralized financial systems, particularly in Ethereum-based smart contracts.

The introduction of blockchain-based federated learning for enhanced anomaly detection, described in Preuveneers D. (2018) [27], saw a burst from 2022 to 2024 (strength: 2.51). This work reflects the increasing focus on privacy-preserving machine learning frameworks, combining federated learning with blockchain for greater transparency in model updates.

The study by Yin HS. (2017) [56] on classifying cyber-criminal entities in the Bitcoin ecosystem had a citation burst from 2021 to 2022 (strength: 1.99). This underscores the growing emphasis on identifying illicit activities in blockchain networks, particularly Bitcoin, and the need for anomaly detection systems to flag criminal behaviors in cryptocurrency transactions.

Table 4 presents a summary of the largest co-cited reference clusters identified within the blockchain anomaly detection research landscape. These clusters represent groups of publications that are frequently cited together, indicating thematic coherence and shared intellectual foundations.

The clusters exhibit a range of sizes, from 56 references in Cluster 0 to 7 references in Cluster 10. The silhouette score, a measure of cluster cohesion and separation, is consistently high across all clusters, ranging from 0.866 to 1.000. This indicates well-defined and distinct clusters, suggesting a robust underlying structure in the co-citation network.

In this paper, we provide an in-depth analysis of the three largest clusters (#0, #1, and #2) by examining key sentences within the publications of each cluster using CiteSpace. These clusters, characterized by their high credibility scores, represent the most significant areas of research in the field.

Table 4. Summary of the largest co-cited reference clusters.

ID	Size	Silhouette	Label (LLR)	Year	Major Publications
0	56	0.904	using unsupervised learning	2020	[28,29,33,55,61–70]
1	45	0.924	bitcoin concepts threat	2017	[37,57,71–77]
2	43	0.884	lightweight federated learning	2021	[27,78–90]
3	33	0.920	knowledge-defined network-ing	2020	[34,91–99]
4	31	0.890	intrusion detection system	2018	[100–106]
5	28	0.928	sustainable smart cities	2019	[107–112]
6	16	0.987	industrial network	2017	[58,113–117]
7	15	0.951	smart contract	2017	[98,118–125]
8	14	1.000	5G advance	2019	[80,85,126–130]
9	9	0.866	server	2015	[53,131,132]
10	7	1.000	things security	2018	[98,133,134]

As shown in Figure 7, the largest cluster (#0) comprises 56 members, with an exceptionally high silhouette value of 0.904, indicating strong thematic coherence. This cluster, centered on unsupervised learning approaches to blockchain anomaly detection, represents a significant methodological advancement in the field.

The intellectual core of this cluster is built around several highly influential works: Sayadi et al. [28] with 19 citations, establishing methodological foundations for unsupervised anomaly detection in blockchain networks; Farrugia et al. [29] with 17 citations, presenting an effective method for detecting illicit accounts on the Ethereum network using the XGBoost classifier; and Chen et al. [55,61], where the authors proposed an effective approach for detecting smart Ponzi schemes on the Ethereum blockchain using data mining and machine learning techniques, achieving high accuracy and highlighting the importance of monitoring smart contracts for early scam detection.

Major citing articles within this cluster reveal a diversification of unsupervised learning approaches [33,62–64]. Particularly noteworthy is Kamran at al., who introduced the AHEAD model, which effectively detects multiple anomalies in blockchain transactions and users across different layers [65]. Notable contributions to this cluster include studies [66–68].

The second largest cluster (#1) contains 45 members with an exceptionally high silhouette value of 0.924, representing the foundational security research focused on Bitcoin's threat landscape. Studies within this cluster explore various attack vectors such as double-spending, ransomware, and illegal transactions, reflecting a deepening concern over the security vulnerabilities of decentralized cryptocurrencies. This cluster's average publication year of 2017 positions it as the intellectual foundation upon which subsequent research streams have built.

The cluster's seminal contributions include Li et al. [37] with 17 citations, establishing a comprehensive taxonomy of threats in blockchain systems, and Apostolaki et al. [71], Liang et al. [57], and Dai et al. [72], each with 5 citations, addressing specialized attack vectors, including routing attacks, smart grid vulnerabilities, and vehicular network security. These works collectively established the conceptual framework for understanding blockchain security challenges.

Major citing articles within this cluster demonstrate its continuing influence, with Rahouti et al. [73] receiving 65 citations for their work synthesizing Bitcoin concepts, threats, and machine-learning security solutions, and Alkadi et al. [74] garnering 45 citations for their comprehensive review of intrusion detection and blockchain applications in cloud environments. The cluster also encompasses specialized applications in transportation systems [75] and smart contracts [76], indicating the extension of foundational security concepts to diverse implementation contexts.

The third-largest cluster (#2) encompasses 43 members with a silhouette value of 0.884, representing the cutting edge of research focused on privacy-preserving machine learning techniques, particularly in decentralized networks. Federated learning enables model training without the need to centralize data, which is crucial in ensuring privacy and security in blockchain and IoT environments. The cluster highlights research on optimizing federated learning frameworks to ensure low computational costs while maintaining high model accuracy.

The intellectual foundations of this cluster include Lu et al. [83] with 11 citations, pioneering the application of federated learning to industrial blockchain environments; Derhab et al. [84] with 6 citations, developing sensor-based detection frameworks; and Mothukuri et al. [85] and Alsaedi et al. [86], each with 5 citations, advancing specialized applications in IoT security and edge computing contexts.

Recent citing articles demonstrate the accelerating research interest in this domain, with Ali et al. [87] receiving 40 citations for their survey of blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks. This cluster shows strong connections to adjacent technology domains, including medical IoT security [88], cloud computing [89], and DDoS attack detection [90].

The prominence of this cluster underscores the growing recognition of federated learning as a promising approach to reconciling privacy preservation with effective anomaly detection in blockchain environments, with key contributions also provided by studies [27,78–82].

4. Discussion

4.1. Comparative Analysis with the Existing Literature

As noted in Section 1, previous literature reviews in the field of anomaly detection in blockchain networks have mostly provided qualitative syntheses of models, techniques, and application domains [31–38]. These studies typically classify approaches by algorithmic type (e.g., deep learning, unsupervised methods), levels of blockchain architecture, or industry-specific application scenarios. While they offer valuable thematic structuring, their primarily descriptive nature and lack of quantitative rigor limit the ability to identify key trends, research gaps, and evolutionary patterns in the field's development. Table 5 presents a comparison between our survey and previous studies.

Table 5. Existing surveys on anomaly detection in blockchain topics and our research contributions.

Ref.	Type	Methodology	Period	Trend Analysis	Bibliometric Analysis	Future Directions	Blockchain Platforms
[31]	Review	Narrative	N/S	–	–	+	General
[32]	Review	Narrative	2012–2024	+	–	+	General
[33]	Review	Narrative	2014–2023	+	–	+	General
[34]	Article	Narrative	2018–2023	–	–	+	Infrastructure
[35]	Brief Review	Narrative	N/S	–	–	–	Financial
[36]	Conf. Paper	Narrative	N/S	–	–	+	General
[37]	Article	Narrative	N/S	–	–	+	General
[38]	Conf. Paper	Narrative	N/S	–	–	+	Financial
Our	**Systematic**	**PRISMA**	**2017–2024**	**+**	**+**	**+**	**General**

Notably, the majority of existing surveys lack of trend and bibliometric analysis, and their discussions on future research directions remain limited in scope. In contrast, our work addresses these gaps by conducting a PRISMA-guided systematic bibliometric review of the anomaly detection literature within the blockchain domain. By combining bibliometric evidence with detailed qualitative synthesis, our work provides a more comprehensive and forward-looking understanding of the field, thereby identifying key opportunities for advancing anomaly detection in blockchain.

4.2. Drivers and Implications of Research Trends

The evolution of anomaly detection research in blockchain ecosystems reflects a dynamic interplay of technological advancements, security needs, and strategic policy initiatives. Bibliometric cluster analysis reveals a clear progression from basic rule-based methods to advanced machine learning, graph neural networks, and privacy-preserving federated learning systems. One of the key enablers of this transition is the exponential growth of blockchain data. Traditional systems have proven inadequate for the real-time analysis of high-volume transactions, prompting a shift toward scalable, data-driven approaches. Machine learning models, particularly those employing graph neural networks, have demonstrated high accuracy in capturing complex transactional patterns and interdependencies.

Simultaneously, the nature of blockchain threats has evolved. Between 2020 and 2024, the landscape shifted from isolated technical exploits to multi-vector attacks involving social engineering, cross-chain vulnerabilities, and oracle manipulation.

The development of anomaly detection solutions has also been influenced by national priorities. China, USA, and India lead in research output, driven by strategic investments and regulatory frameworks [135,136]. China's centralized investment strategy contrasts with the USA's decentralized, regulation-led approach. In Europe, the MiCA regulation [137] fosters security innovation by emphasizing compliance.

Cluster transitions indicate a movement from unsupervised learning (cluster #0) and basic cryptocurrency security (cluster #1) toward lightweight, federated learning architectures (cluster #2), reflecting several key trendsseveral emerging trends in the field. First, there is growing emphasis on methods that support the proactive detection of complex anomalies, particularly those capable of capturing relational structures within blockchain networks. Techniques based on graph neural networks have demonstrated notable effectiveness in this regard. Second, privacy-preserving collaboration is becoming increasingly important. Approaches such as federated learning enable anomaly detection across multiple organizations without requiring direct data sharing, thereby aligning with modern data protection regulations. Third, the demand for explainable artificial intelligence is rising, driven by the need for transparency and regulatory compliance. Techniques that improve the interpretability of detection outcomes—such as SHAP [138] and LIME [139]—are being progressively adopted to enhance trust in automated systems used by auditors, developers, and regulators.

4.3. Limitations of the Study

Although this study offers a thorough bibliometric analysis of anomaly detection in blockchain systems, several limitations should be acknowledged.

The data sources were limited to the Web of Science Core Collection (WoSCC). While WoSCC is a reputable and extensive database, restricting the analysis to this single platform may have excluded relevant studies indexed in other databases such as Scopus, IEEE Xplore, or Google Scholar.

The study focused exclusively on peer-reviewed research articles and reviews within the Science Citation Index and Social Sciences Citation Index. This focus excludes other valuable sources like conference proceedings, books, and gray literature, which might provide additional perspectives on emerging techniques and practical applications in blockchain anomaly detection.

The language restriction to English publications introduces a bias, potentially overlooking important contributions published in other languages such as Chinese, Spanish, or French. This may limit the inclusion of diverse regional insights and alternative approaches to blockchain security.

The bibliometric analysis relied on the CiteSpace 6.4.R1 software. Although CiteSpace is a recognized and specialized tool, the results may vary depending on the parameters, algorithms, and visualization methods used. Employing different analytical tools or methodologies could produce alternative yet valid interpretations.

4.4. Open Challenges and Future Directions

This section explores the anticipated future directions in the realm of anomaly detection in blockchain, based on the analysis of co-citation clusters, top-cited papers, their abstracts, and emerging trends identified in Section 3. These directions reflect not only current technological capabilities but also fundamental challenges that require comprehensive solutions to ensure the resilience and security of blockchain systems.

We identified six key areas encompassing critical challenges and future research opportunities:

1. *Federated learning and privacy-preserving technologies.* The analysis of the keyword map (Figure 5), timeline map of reference co-citation (Figure 8), citation bursts (Figure 9), and core publications in cluster #2 demonstrates a growing interest in federated learning and highlights open challenges within the context of blockchain security [27,78–83,87,90]. Combining blockchain with federated learning offers a unique opportunity to create transparent, auditable anomaly detection models without centralizing training data. However, several open challenges remain, which future research will need to address to advance the domain:
    - developing attack-resistant federated models for anomaly detection in scalable blockchain networks;
    - implementing differential privacy techniques in federated models to balance detection accuracy with user privacy protection.
2. *Integration of multimodadata and heterogeneous sources.* The analysis of the keyword map (Figure 5), timeline map of reference co-citation (Figure 8), citation bursts (Figure 9), and core publications in clusters related to machine and deep learning (specifically, clusters #0, #3, #4) demonstrates a growing interest in comprehensive approaches to anomaly detection. Current research reveals a significant shift from one-dimensional transaction analysis, based on individual data types, to an all-encompassing approach that considers diverse aspects of blockchain data [26,33,55,56,61,66–68,73,91,95–98,100,101,103,140]. This shift underscores the need for integrating heterogeneous data to enhance the effectiveness of detecting complex anomalies that might be unnoticeable when analyzing only one type of information. Achieving such integration in blockchain anomaly detection requires robust systems capable of securely managing and processing diverse datasets. In this context, innovative data storage and processing systems such as SecuDB [141], LedgerDB [142], and VeDB [143] can play a pivotal role. These technologies provide a high level of security, data integrity, and verifiability, which are critically important for identifying deviations from normal behavior in decentralized environments. Future research in this direction may include the following:
    - developing algorithms that simultaneously analyze on-chain and off-chain data for comprehensive anomaly detection;

- creating systems that integrate blockchain data with traditional financial transactions to detect cross-platform fraud schemes;
- applying natural language processing methods to analyze smart contracts along with user behavioral patterns;
- leveraging secure database technologies to provide scalable and tamper-resistant analytics platforms.

3. *Explainable AI and interpretable detection models.* The results of our study demonstrate a clear shift from basic security mechanisms to sophisticated machine learning and graph neural network approaches in blockchain anomaly detection. Specifically, some publications in clusters related to machine and deep learning (e.g., clusters #0, #3, #4) reveal a growing interest in employing these advanced methods [66–70,99,106]. Many research studies use ensemble learning and explainable AI for fraud detection in blockchain transactions, indicating the growing importance of interpretability in AI-based security solutions [65,144–147]. This direction highlights the need for transparency in complex models, such as those used in deep and unsupervised learning, so that their decisions are understandable to security experts. Future research will likely pay more attention to the following:

   - developing anomaly detection models with built-in mechanisms for interpreting results;
   - creating intuitive visual explanations for identified anomalies to help security experts make informed decisions;
   - combining expert knowledge and algorithmic approaches to form hybrid detection systems with improved interpretability.

4. *Real-time and adaptive detection systems.* The increasing complexity of fraud schemes and the rapid evolution of attack methods fundamentally necessitate the development of anomaly detection systems that operate in real-time. This need is not merely theoretical but is clearly demonstrated by the characteristics and demands of various application domains, as reflected in several prominent co-citation clusters (#1, #5, #6, #7, #8, #10). For instance, in the publications associated with cluster #1 [71,73,77], which focus on cryptocurrency networks, the speed and unpredictability of attacks necessitate immediate detection and rapid, adaptive responses to emerging malicious behaviors. A similar urgency is evident in sustainable smart cities (cluster #5) [107–112] and industrial networks (cluster #6) [58,113,116,117], where massive volumes of real-time data are continuously generated by IoT and IIoT devices. In such environments, timely and adaptive anomaly detection is critical to ensure the uninterrupted operation of essential infrastructure and safeguard public safety. The situation is even more acute in the domain of smart contracts (cluster #7) [98,124,125], where anomalies such as vulnerabilities or malicious executions can result in immediate and irreversible financial damages. Moreover, the emergence of 5G advanced networks (cluster #8) [126,130], characterized by ultra-low latency and high throughput, both enables and necessitates the deployment of anomaly detection systems that can match the network's speed and complexity. These systems must be capable of processing vast data flows with minimal delay while maintaining high detection accuracy. Lastly, the publications in cluster #10 [98,133,134] highlight that highly dynamic and heterogeneous ecosystems require continuous anomaly identification and response mechanisms that can adapt in real time to evolving threats, device malfunctions, or behavioral deviations. Despite the lack of pronounced representation in recent citation bursts, the shift toward real-time, adaptive anomaly detection is a critical direction for practical applications of academic research. Moving forward, this entails the following:

- implementing incremental learning methods to continuously adapt models to new types of attacks;
- developing early warning systems capable of detecting anomalies at the formation stage;
- creating distributed monitoring systems that minimize detection latency without compromising accuracy.

5. *Cross-domain integration and specialized applications.* The analysis of the keyword map (Figure 5), the timeline map of reference co-citation (Figure 8), and the core publications in clusters #5, #6, and #10 reveals a consistent and accelerating trend toward the specialization of anomaly detection methods tailored to distinct application domains within the blockchain security ecosystem. In particular, publications in cluster #5 emphasize the integration of blockchain-based security mechanisms into smart city infrastructures [107,110]. The convergence of diverse IoT devices and public service networks necessitates anomaly detection approaches that are domain-aware and capable of responding to complex interdependencies between systems. Cluster #6 publications [58,113,116,117] focus on the implementation of anomaly detection in operational technology and industrial control system environments. These settings, characteristic of Industry 4.0, require context-specific models that support real-time monitoring and low-latency decision-making. Cluster #10 publications [98,133,134] address the distinct challenges of securing resource-constrained IoT devices that operate within or alongside blockchain frameworks. Given the heterogeneous nature of IoT ecosystems and their vulnerability to both device-level and network-level threats, this area underscores the need for lightweight, efficient, and adaptive anomaly detection methods. These thematic concentrations point toward several key directions for future research:
    - developing specialized anomaly detection models for industrial blockchain systems in the context of Industry 4.0;
    - creating lightweight algorithms for resource-constrained IoT devices in blockchain networks;
    - integrating blockchain security with traditional critical infrastructure security systems.
6. *Standardization and regulatory frameworks.* Numerous review studies [31,36,38,105,133] consistently highlight persistent challenges, open questions, and the lack of unified methodologies, all of which hinder the large-scale adoption and interoperability of anomaly detection systems across different blockchain platforms. This fragmentation not only complicates technical integration but also impairs collective efforts to combat cyber threats in blockchain ecosystems. Moreover, research focusing on anomaly detection within highly regulated or financially sensitive domains—such as finance, emergency management, healthcare, cybersecurity, and critical energy infrastructure—emphasizes the urgent need for international cooperation [19,69,96,103,125,147,148]. In these sectors, combating cybercrime, including fraud and anomalous behavior, is a critical priority. Addressing this challenge requires the establishment of harmonized regulatory frameworks and international standards that can ensure the effectiveness and interoperability of anomaly detection systems, regardless of their underlying architecture or blockchain platform. Accordingly, future research and policy development should prioritize the following:
    - developing harmonized methodologies for evaluating the effectiveness of anomaly detection systems in blockchain;

- forming international standards for the interoperability of anomaly detection systems across different blockchain platforms.

4.5. Main Findings

Our findings based on the research questions defined can be summarized as follows.

RQ1: We found that the results obtained in this study demonstrate an uneven yet dynamically growing scientific interest in the field of blockchain anomaly detection.

Publication activity is primarily concentrated in countries with strong techno-scientific infrastructures. The highest research intensity is observed in China, which has emerged as a major hub for the generation of knowledge in the field of blockchain analytics. The United States and India also exhibit significant scholarly output, indicating the global relevance of security issues in distributed systems.

Interestingly, the group of active contributors includes not only traditionally dominant scientific powers but also countries undergoing accelerated digital transformation over the past decade, such as Saudi Arabia. This suggests the emergence of a new map of international participation in blockchain-related research, where state-led initiatives and strategic investments in innovation play a pivotal role.

The key institutions contributing to research development are primarily Asian technical universities. Identified academic centers in China hold central positions in the structure of institutional cooperation. At the same time, universities from other regions, notably Canada, India, and the Middle East, also demonstrate visible activity.

However, institutional linkages remain underdeveloped, as evidenced by the low connectivity of the academic collaboration network. This may reflect the absence of well-established international consortia or the limited interregional coordination in this area. Instead, the landscape is dominated by isolated or regionally focused research groups formed around local thought leaders.

A group of leading authors has been identified as actively shaping both theoretical and applied approaches to anomaly detection in blockchain networks. Researchers combining expertise in cybersecurity, artificial intelligence, and distributed computing play a particularly influential role. The most productive contributors include scholars from Canada, India, and China, who collectively constitute the core of the field's publication impact.

Notably, a substantial number of these researchers have joined the academic discourse relatively recently - after 2020 - highlighting the emerging and innovative nature of this subfield. Author collaboration within individual publications reveals a tendency toward thematic clustering, though inter-cluster cooperation remains limited.

Within the scope of citation analysis, special attention is drawn to the figure of Satoshi Nakamoto, who, despite not being directly involved in anomaly detection research, remains central in the historical and methodological context due to the foundational role in conceptualizing blockchain technology itself.

RQ2: Using the CiteSpace software, an analysis was conducted of the keyword network and co-citation cohorts in studies dedicated to anomaly detection in blockchain. This enabled the identification of major research clusters and current hotspots and the tracing of evolving trends in the field.

The largest research cluster is related to unsupervised learning methods. It includes more than fifty works focused on the application of unsupervised learning algorithms for detecting anomalies in blockchain. The second-largest cluster is dedicated to Bitcoin security. This area covers research on primary threats such as double-spending attacks, ransomware, and illicit transactions, thereby forming foundational knowledge about cryptocurrency security. Another important direction is lightweight federated learning, which is gaining popularity due to its ability to ensure privacy protection and enhance the efficiency of anomaly detection in distributed systems, particularly in the IoT domain, while minimizing computational overhead.

Among the research hotspots, anomaly detection is the dominant concept most frequently encountered in studies. Considerable attention is given to the application of machine learning and deep learning, as well as topics related to IoT, artificial intelligence, federated learning, big data, and authentication. There is a growing interest in protection against attacks, including adversarial attacks, intrusion detection systems, and consensus algorithms.

Regarding trend evolution, the period from 2019 to 2020 was characterized by a focus on fundamental security issues such as access control. In 2020–2021, the emphasis shifted to data analytics for anomaly detection. The years 2021–2022 saw the introduction of diverse methods, including intrusion detection systems and reinforcement learning. From 2022 to 2024, the focus has been on integrating technologies into industrial ecosystems, the development of peer-to-peer computing, and strengthening defenses against sophisticated attacks.

Influential works in this area include the Ethereum whitepaper [53], which serves as a foundational and widely cited document; the DeepLog model based on LSTM for anomaly detection in logs [26]; the blockchain technology survey by Zheng et al. [54], which laid the groundwork for scalability and security research; and Chen's study on detecting Ponzi schemes using machine learning [55].

RQ3: Based on the analysis of clusters in this study, we identified six main avenues for future research and development (see Section 4.4), including federated learning and privacy-preserving technologies, the integration of multimodal data and heterogeneous sources, explainable AI and interpretable detection models, real-time and adaptive detection systems, cross-domain integration, and specialized applications, as well as standardization and regulatory frameworks.

5. Conclusions

This paper presents a bibliometric analysis of anomaly detection research in blockchain networks conducted between 2017 and 2024. Using the PRISMA methodology and CiteSpace, we examined publication trends, identified key research themes, and highlighted the most active authors, institutions, and countries in this field.

The findings indicate a rapid increase in interest in blockchain security, driven by the growing number of attacks, fraudulent schemes, and the rising complexity of contemporary threats. The shift from basic protection methods to machine learning, deep neural networks, graph models, and federated learning reflects the field's growing sophistication and diversity.

The analysis of international and institutional collaborations reveals that China, the United States, and India are the most significant contributors to anomaly detection research in blockchain. Among the leading research institutions are Beijing University of Posts and Telecommunications, Brandon University, and Nirma University. At the same time, there is a notable trend toward expanding international cooperation and forming interdisciplinary research teams.

The main scientific clusters identified include unsupervised learning, Bitcoin security, and lightweight federated learning. Key topics include anomaly detection, machine learning, IoT security, and explainable AI for improving detection transparency.

Despite substantial progress, the field faces several open challenges. These include the need to develop private and scalable federated learning models, design adaptive real-time systems, integrate multimodal data sources, and improve the interpretability of models. Particular attention must be paid to balancing anomaly detection performance with data privacy, as well as developing universal approaches applicable across different types of blockchain networks.

This study summarizes the current state of research and outlines future directions for anomaly detection in blockchain. The results can serve as a roadmap for future research, support the development of effective cybersecurity strategies, and foster greater trust in blockchain technologies across a variety of application domains.

Author Contributions: Conceptualization, R.S.; methodology, R.S. and V.M.; software, V.M.; validation, V.M., V.B. and A.M.; formal analysis, V.B., B.A. and R.S.; investigation, R.S., V.M., B.A. and A.M.; resources, B.A.; data curation, V.M. and B.A.; writing—original draft preparation, R.S.; writing—review and editing, R.S., V.M. and B.A.; supervision, R.S.; project administration, R.S.; funding acquisition, R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Research data collected for this study will be made available if requested by contacting the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Payandeh, R.; Delbari, A.; Fardad, F.; Helmzadeh, J.; Shafiee, S.; Ghatari, A.R. Unraveling the potential of blockchain technology in enhancing supply chain traceability: A systematic literature review and modeling with ISM. *Blockchain Res. Appl.* **2024**, *6*, 100240. [CrossRef]
2. Rajasekaran, A.S.; Azees, M.; Al-Turjman, F. A comprehensive survey on blockchain technology. *Sustain. Energy Technol. Assessments* **2022**, *52*, 102039. [CrossRef]
3. Bennet, D.; Maria, L.; Sanjaya, Y.P.A.; Zahra, A.R.A. Blockchain technology: Revolutionizing transactions in the digital age. *ADI J. Recent Innov.* **2024**, *5*, 192–199. [CrossRef]
4. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R.; Khan, S. A review of Blockchain Technology applications for financial services. *BenchCouncil Trans. Benchmarks, Stand. Eval.* **2022**, *2*, 100073. [CrossRef]
5. Moosavi, J.; Naeni, L.M.; Fathollahi-Fard, A.M.; Fiore, U. Blockchain in supply chain management: A review, bibliometric, and network analysis. *Environ. Sci. Pollut. Res.* **2021**, 1–15. [CrossRef]
6. Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain application in healthcare systems: A review. *Systems* **2023**, *11*, 38. [CrossRef]
7. Rejeb, A.; Rejeb, K.; Appolloni, A.; Jagtap, S.; Iranmanesh, M.; Alghamdi, S.; Alhasawi, Y.; Kayikci, Y. Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 1–18. [CrossRef]
8. Cheshun, V.; Muliar, I.; Yatskiv, V.; Shevchuk, R.; Kulyna, S.; Tsavolyk, T. Safe Decentralized Applications Development Using Blockchain Technologies. In Proceedings of the 2020 10th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, 16–18 September 2020; pp. 800–805. [CrossRef]
9. Shevchuk, R.; Lishchynskyy, I.; Ciura, M.; Lyzun, M.; Kozak, R.; Kasianchuk, M. Application of Blockchain Technology in Emergency Management Systems: A Bibliometric Analysis. *Appl. Sci.* **2025**, *15*, 5405. [CrossRef]
10. Lukić, I.; Köhler, M.; Krpić, Z.; Švarcmajer, M. Advancing Smart City Sustainability Through Artificial Intelligence, Digital Twin and Blockchain Solutions. *Technologies* **2025**, *13*, 300. [CrossRef]
11. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
12. Kuznetsov, O.; Sernani, P.; Romeo, L.; Frontoni, E.; Mancini, A. On the integration of artificial intelligence and blockchain technology: A perspective about security. *IEEE Access* **2024**, *12*, 3881–3897. [CrossRef]
13. Aggarwal, S.; Kumar, N. Attacks on blockchain. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 399–410.
14. Mahtani, U.S. Fraudulent practices and blockchain accounting systems. *J. Account. Ethics Public Policy* **2022**, *23*, 97.
15. Shevchuk, R.; Martsenyuk, V. Neural networks toward cybersecurity: Domaine map analysis of state-of-the-art challenges. *IEEE Access* **2024**, *12*, 81265–81280. [CrossRef]

16. Krause, D. The $1.4 Billion Bybit Hack: Cybersecurity Failures and the Risks of Cryptocurrency Deregulation. 2025. Available online: https://ssrn.com/abstract=5150171 (accessed on 30 March 2025).
17. Partz, H. Atomic Wallet Faces Lawsuit over $100M Crypto Hack Losses: Report. 2025. Available online: https://cointelegraph.com/news/crypto-atomic-wallet-faces-class-action-over-100m-crypto-hack-losses (accessed on 30 March 2025).
18. Chainalysis. The Chainalysis 2025 Crypto Crime Report. 2025. Available online: http://go.chainalysis.com/2025-Crypto-Crime-Report.html (accessed on 30 March 2025).
19. Kovalchuk, O.; Shevchuk, R.; Banakh, S. Cryptocurrency crime risks modeling: Environment, e-commerce, and cybersecurity issue. *IEEE Access* **2024**, *12*, 50673–50688. [CrossRef]
20. Turksen, U.; Benson, V.; Adamyk, B. Legal implications of automated suspicious transaction monitoring: Enhancing integrity of AI. *J. Bank. Regul.* **2024**, *25*, 359–377. [CrossRef]
21. Adamyk, B.; Benson, V.; Adamyk, O.; Liashenko, O. Risk Management in DeFi: Analyses of the Innovative Tools and Platforms for Tracking DeFi Transactions. *J. Risk Financ. Manag.* **2025**, *18*, 38. [CrossRef]
22. Hafid, A.; Hafid, A.S.; Samih, M. A tractable probabilistic approach to analyze sybil attacks in sharding-based blockchain protocols. *IEEE Trans. Emerg. Top. Comput.* **2022**, *11*, 126–136. [CrossRef]
23. Arifeen, M.M.; Al Mamun, A.; Ahmed, T.; Kaiser, M.S.; Mahmud, M. A blockchain-based scheme for sybil attack detection in underwater wireless sensor networks. In *Proceedings of the International Conference on Trends in Computational and Cognitive Engineering: Proceedings of TCCE 2020*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 467–476.
24. Xu, J.J. Are blockchains immune to all malicious attacks? *Financ. Innov.* **2016**, *2*, 25. [CrossRef]
25. König, L.; Unger, S.; Kieseberg, P.; Tjoa, S.; Blockchains, J.R.C. The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks. *J. Internet Serv. Inf. Secur.* **2020**, *10*, 110–127.
26. Du, M.; Li, F.; Zheng, G.; Srikumar, V. Deeplog: Anomaly detection and diagnosis from system logs through deep learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1285–1298.
27. Preuveneers, D.; Rimmer, V.; Tsingenopoulos, I.; Spooren, J.; Joosen, W.; Ilie-Zudor, E. Chained anomaly detection models for federated learning: An intrusion detection case study. *Appl. Sci.* **2018**, *8*, 2663. [CrossRef]
28. Sayadi, S.; Rejeb, S.B.; Choukair, Z. Anomaly detection model over blockchain electronic transactions. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 895–900.
29. Farrugia, S.; Ellul, J.; Azzopardi, G. Detection of illicit accounts over the Ethereum blockchain. *Expert Syst. Appl.* **2020**, *150*, 113318. [CrossRef]
30. Apiecionek, Ł.; Karbowski, P. Fuzzy Neural Network for Detecting Anomalies in Blockchain Transactions. *Electronics* **2024**, *13*, 4646. [CrossRef]
31. Hassan, M.U.; Rehmani, M.H.; Chen, J. Anomaly detection in blockchain networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2022**, *25*, 289–318. [CrossRef]
32. Mounnan, O.; Manad, O.; Boubchir, L.; El Mouatasim, A.; Daachi, B. A review on deep anomaly detection in blockchain. *Blockchain Res. Appl.* **2024**, *5*, 100227. [CrossRef]
33. Cholevas, C.; Angeli, E.; Sereti, Z.; Mavrikos, E.; Tsekouras, G.E. Anomaly detection in blockchain networks using unsupervised learning: A survey. *Algorithms* **2024**, *17*, 201. [CrossRef]
34. Chithanuru, V.; Ramaiah, M. An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions—A review. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7724. [CrossRef]
35. Tien, H.T.; Tran-Trung, K.; Hoang, V.T. Blockchain-data mining fusion for financial anomaly detection: A brief review. *Procedia Comput. Sci.* **2024**, *235*, 478–483. [CrossRef]
36. Liu, Z.; Gao, H.; Lei, H.; Liu, Z.; Liu, C. Blockchain anomaly transaction detection: An overview, challenges, and open issues. In Proceedings of the International Conference on Information Science, Communication and Computing, Chongqing, China, 2–5 June 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 126–140.
37. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
38. Xu, T.; Liu, Z.; Gao, H.; Lei, H.; Ma, Q. Anomaly Detection on Blockchain in Financial Fields: A Comprehensive Survey. In Proceedings of the 2024 4th International Conference on Computer Communication and Artificial Intelligence (CCAI), Xi'an, China, 24–26 May 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 199–207.
39. Clarivate. Web of Science—Web of Science Group. 2025. Available online: https://clarivate.com/academia-government/scientific-and-academic-research/research-discovery-and-referencing/web-of-science/ (accessed on 10 March 2025).
40. Falagas, M.E.; Pitsouni, E.I.; Malietzis, G.A.; Pappas, G. Comparison of PubMed, Scopus, web of science, and Google scholar: Strengths and weaknesses. *FASEB J.* **2008**, *22*, 338–342. [CrossRef]

41. Martín-Martín, A.; Thelwall, M.; Orduna-Malea, E.; Delgado López-Cózar, E. Google Scholar, Microsoft Academic, Scopus, Dimensions, Web of Science, and OpenCitations' COCI: A multidisciplinary comparison of coverage via citations. *Scientometrics* **2021**, *126*, 871–906. [CrossRef]
42. Sohrabi, C.; Franchi, T.; Mathew, G.; Kerwan, A.; Nicola, M.; Griffin, M.; Agha, M.; Agha, R. PRISMA 2020 statement: What's new and the importance of reporting guidelines. *Int. J. Surg.* **2021**, *88*, 105918. [CrossRef] [PubMed]
43. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ* **2009**, *339*. [CrossRef]
44. Haddaway, N.R.; Page, M.J.; Pritchard, C.C.; McGuinness, L.A. PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell Syst. Rev.* **2022**, *18*, e1230. [CrossRef] [PubMed]
45. Peng, C.; Xia, F.; Naseriparsa, M.; Osborne, F. Knowledge graphs: Opportunities and challenges. *Artif. Intell. Rev.* **2023**, *56*, 13071–13102. [CrossRef]
46. Lin, M.; Chen, Y.; Chen, R. Bibliometric analysis on Pythagorean fuzzy sets during 2013–2020. *Int. J. Intell. Comput. Cybern.* **2021**, *14*, 104–121. [CrossRef]
47. Zhang, J.; Quoquab, F. Documenting the knowledge of pro-environmental travel behaviour research: A visual analysis using CiteSpace. *J. Tour. Futur.* **2022**, *10*, 277–298. [CrossRef]
48. Behl, R.; Sharma, S. Will Cryptocurrency Become the Future of Digital India? A Comparative Study of Generation Y and Z to Identify the Intention to Adopt Cryptocurrency. In *Corporate Democracy, Open Innovation, and Growth: Business Transformation in Developing Economies*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 183–207.
49. Wired. Saudi Arabia Unveils More Than $6.4 bn in Technology and Startup Investment at LEAP22. 2022. Available online: https://www.thenationalnews.com/business/technology/2022/02/01/saudi-arabia-unveils-more-than-64bn-in-technology-and-start-up-investment-at-leap/ (accessed on 17 March 2025).
50. MSCA Digital Finance. Anomaly and Fraud Detection in Blockchain Networks. 2024. Available online: https://www.digital-finance-msca.com/blockchain?utm_source=chatgpt.com (accessed on 11 March 2025).
51. Austrian Institute of Technology. Project to Prevent Criminal Use of Blockchain Technology Launched by International Consortium. 2017. Available online: https://www.interpol.int/ar/1/1/2017/Project-to-prevent-criminal-use-of-blockchain-technology-launched-/by-international-consortium (accessed on 17 March 2025).
52. Ontochain. A New Software Ecosystem for Trusted, Traceable and Transparent Ontological Knowledge. 2025. Available online: https://ontochain.ngi.eu/ (accessed on 17 March 2025).
53. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
54. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE international congress on big data (BigData congress), Honolulu, HI, USA, 25–30 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 557–564.
55. Chen, W.; Zheng, Z.; Cui, J.; Ngai, E.; Zheng, P.; Zhou, Y. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In Proceedings of the 2018 World Wide Web Conference, Lyon, France, 23–27 April 2018; pp. 1409–1418.
56. Yin, H.S.; Vatrapu, R. A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 3690–3699.
57. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z.Y. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Trans. Smart Grid* **2018**, *10*, 3162–3173. [CrossRef]
58. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans. Ind. Informatics* **2019**, *15*, 3548–3558. [CrossRef]
59. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
60. Chen, T.; Guestrin, C. XGBoost: A scalable tree boosting system. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA, USA, 13–17 August 2016; ACM: New York, NY, USA, 2016; pp. 785–794.
61. Chen, W.; Zheng, Z.; Ngai, E.C.H.; Zheng, P.; Zhou, Y. Exploiting blockchain data to detect smart ponzi schemes on ethereum. *IEEE Access* **2019**, *7*, 37575–37586. [CrossRef]
62. Hisham, S.; Makhtar, M.; Aziz, A.A. Combining multiple classifiers using ensemble method for anomaly detection in blockchain networks: A comprehensive review. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 8. [CrossRef]
63. Kamišalić, A.; Kramberger, R.; Fister, I., Jr. Synergy of blockchain technology and data mining techniques for anomaly detection. *Appl. Sci.* **2021**, *11*, 7987. [CrossRef]
64. Kabla, A.H.H.; Anbar, M.; Manickam, S.; Al-Amiedy, T.A.; Cruspe, P.B.; Al-Ani, A.K.; Karuppayah, S. Applicability of intrusion detection system on Ethereum attacks: A comprehensive review. *IEEE Access* **2022**, *10*, 71632–71655. [CrossRef]

65. Kamran, M.; Rehan, M.M.; Nisar, W.; Rehan, M.W. AHEAD: A Novel Technique Combining Anti-Adversarial Hierarchical Ensemble Learning with Multi-Layer Multi-Anomaly Detection for Blockchain Systems. *Big Data Cogn. Comput.* **2024**, *8*, 103. [CrossRef]
66. Hasan, M.; Rahman, M.S.; Janicke, H.; Sarker, I.H. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis. *Blockchain Res. Appl.* **2024**, *5*, 100207. [CrossRef]
67. Podgorelec, B.; Turkanović, M.; Karakatič, S. A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection. *Sensors* **2019**, *20*, 147. [CrossRef]
68. Ashfaq, T.; Khalid, R.; Yahaya, A.S.; Aslam, S.; Azar, A.T.; Alsafari, S.; Hameed, I.A. A machine learning and blockchain based efficient fraud detection mechanism. *Sensors* **2022**, *22*, 7162. [CrossRef]
69. Li, X.; Yang, Y.; Li, B.; Li, M.; Zhang, J.; Li, T. Blockchain cryptocurrency abnormal behavior detection based on improved graph convolutional neural networks. In Proceedings of the 2023 International Conference on Data Security and Privacy Protection (DSPP), Xi'an, China, 16–18 October 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 216–222.
70. Behdadnia, T.; Thoelen, K.; Zobiri, F.; Deconinck, G. Spatial-temporal graph neural network for detecting and localizing anomalies in pmu networks. In Proceedings of the European Dependable Computing Conference, Leuven, Belgium, 8–11 April 2024; Springer: Berlin/Heidelberg, Germany, 2024; pp. 75–82.
71. Apostolaki, M.; Zohar, A.; Vanbever, L. Hijacking bitcoin: Routing attacks on cryptocurrencies. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–24 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 375–392.
72. Dai, Y.; Xu, D.; Zhang, K.; Maharjan, S.; Zhang, Y. Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4312–4324. [CrossRef]
73. Rahouti, M.; Xiong, K.; Ghani, N. Bitcoin concepts, threats, and machine-learning security solutions. *IEEE Access* **2018**, *6*, 67189–67205. [CrossRef]
74. Alkadi, O.; Moustafa, N.; Turnbull, B. A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions. *IEEE Access* **2020**, *8*, 104893–104917. [CrossRef]
75. Belhadi, A.; Djenouri, Y.; Srivastava, G.; Lin, J.C.W. SS-ITS: Secure scalable intelligent transportation systems. *J. Supercomput.* **2021**, *77*, 7253–7269. [CrossRef]
76. Shao, W.; Wang, Z.; Wang, X.; Qiu, K.; Jia, C.; Jiang, C. LSC: Online auto-update smart contracts for fortifying blockchain-based log systems. *Inf. Sci.* **2020**, *512*, 506–517. [CrossRef]
77. Hu, Z.; Yu, X.; Liu, L.; Zhang, Y.; Yu, H. ASOD: An Adaptive Stream Outlier Detection Method Using Online Strategy. *J. Cloud Comput.* **2024**, *13*, 120. [CrossRef]
78. Pokhrel, S.R.; Yang, L.; Rajasegarar, S.; Li, G. Robust Zero Trust Architecture: Joint Blockchain based Federated learning and Anomaly Detection based Framework. In Proceedings of the SIGCOMM Workshop on Zero Trust Architecture for Next Generation Communications, Sydney, Australia, 4–8 August 2024; pp. 7–12.
79. Wang, X.; Liu, W.; Lin, H.; Hu, J.; Kaur, K.; Hossain, M.S. AI-empowered trajectory anomaly detection for intelligent transportation systems: A hierarchical federated learning approach. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 4631–4640. [CrossRef]
80. Cui, L.; Qu, Y.; Xie, G.; Zeng, D.; Li, R.; Shen, S.; Yu, S. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. *IEEE Trans. Ind. Informatics* **2021**, *18*, 3492–3500. [CrossRef]
81. Liu, S.; Shang, Y. Federated learning with anomaly client detection and decentralized parameter aggregation. In Proceedings of the 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Baltimore, MD, USA, 27–30 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 37–43.
82. Arazzi, M.; Nicolazzo, S.; Nocera, A. A fully privacy-preserving solution for anomaly detection in iot using federated learning and homomorphic encryption. *Inf. Syst. Front.* **2023**, *27*, 367–390. [CrossRef]
83. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4177–4186. [CrossRef]
84. Derhab, A.; Guerroumi, M.; Gumaei, A.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors* **2019**, *19*, 3119. [CrossRef] [PubMed]
85. Mothukuri, V.; Khare, P.; Parizi, R.M.; Pouriyeh, S.; Dehghantanha, A.; Srivastava, G. Federated-learning-based anomaly detection for IoT security attacks. *IEEE Internet Things J.* **2021**, *9*, 2545–2554. [CrossRef]
86. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access* **2020**, *8*, 165130–165150. [CrossRef]
87. Ali, S.; Li, Q.; Yousafzai, A. Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. *Ad Hoc Netw.* **2024**, *152*, 103320. [CrossRef]
88. Messinis, S.; Temenos, N.; Protonotarios, N.E.; Rallis, I.; Kalogeras, D.; Doulamis, N. Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Comput. Biol. Med.* **2024**, *170*, 108036. [CrossRef]
89. Alzoubi, Y.I.; Mishra, A.; Topcu, A.E. Research trends in deep learning and machine learning for cloud computing security. *Artif. Intell. Rev.* **2024**, *57*, 132. [CrossRef]

90. Park, J.H.; Yotxay, S.; Singh, S.K.; Park, J.H. PoAh-enabled federated learning architecture for DDoS attack detection in IoT networks. *Hum.-Centric Comput. Inf. Sci.* **2024**, *14*, 1–25.
91. Wijesekara, P.A.D.S.N.; Gunawardena, S. A review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges. *Network* **2023**, *3*, 343–421. [CrossRef]
92. Rico-Pena, J.J.; Arguedas-Sanz, R.; Lopez-Martin, C. Models used to characterise blockchain features. A systematic literature review and bibliometric analysis. *Technovation* **2023**, *123*, 102711. [CrossRef]
93. Alkadi, O.; Moustafa, N.; Turnbull, B.; Choo, K.K.R. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet Things J.* **2020**, *8*, 9463–9472. [CrossRef]
94. Dey, S. Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work. In Proceedings of the 2018 10th Computer Science and Electronic Engineering (CEEC), Colchester, UK, 19–21 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 7–10.
95. Salah, K.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and open research challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
96. Song, A.; Seo, E.; Kim, H. Anomaly VAE-transformer: A deep learning approach for anomaly detection in decentralized finance. *IEEE Access* **2023**, *11*, 98115–98131. [CrossRef]
97. Ge, B.; Bao, J.; Li, B.; Mou, X.; Zhao, J.; Liu, X. Img: Deep representation graph learning for anomaly detection in industrial control system. *J. Signal Process. Syst.* **2024**, *96*, 555–567. [CrossRef]
98. Demertzis, K.; Iliadis, L.; Tziritas, N.; Kikiras, P. Anomaly detection via blockchained deep learning smart contracts in industry 4.0. *Neural Comput. Appl.* **2020**, *32*, 17361–17378. [CrossRef]
99. Zkik, K.; Sebbar, A.; Fadi, O.; Kamble, S.; Belhadi, A. Securing blockchain-based crowdfunding platforms: An integrated graph neural networks and machine learning approach. *Electron. Commer. Res.* **2024**, *24*, 497–533. [CrossRef]
100. Mathew, S.S.; Hayawi, K.; Dawit, N.A.; Taleb, I.; Trabelsi, Z. Integration of blockchain and collaborative intrusion detection for secure data transactions in industrial IoT: A survey. *Clust. Comput.* **2022**, *25*, 4129–4149. [CrossRef]
101. Khonde, S.R.; Ulagamuthalvi, V. Hybrid intrusion detection system using blockchain framework. *EURASIP J. Wirel. Commun. Netw.* **2022**, *2022*, 58. [CrossRef]
102. Liang, W.; Xiao, L.; Zhang, K.; Tang, M.; He, D.; Li, K.C. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. *IEEE Internet Things J.* **2021**, *9*, 14741–14751. [CrossRef]
103. Zheng, G.; Ni, Q.; Lu, Y. Privacy-Aware Anomaly Detection and Notification Enhancement for VANET Based on Collaborative Intrusion Detection System. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 21172–21182. [CrossRef]
104. Al-E'mari, S.; Anbar, M.; Sanjalawe, Y.; Manickam, S.; Hasbullah, I. Intrusion detection systems using blockchain technology: A review, issues and challenges. *Comput. Syst. Sci. Eng.* **2022**, *40*, 87–112. [CrossRef]
105. Meng, W.; Tischhauser, E.W.; Wang, Q.; Wang, Y.; Han, J. When intrusion detection meets blockchain technology: A review. *IEEE Access* **2018**, *6*, 10179–10188. [CrossRef]
106. Signorini, M.; Pontecorvi, M.; Kanoun, W.; Di Pietro, R. BAD: A blockchain anomaly detection solution. *IEEE Access* **2020**, *8*, 173481–173490. [CrossRef]
107. Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* **2021**, *115*, 101954. [CrossRef]
108. Kumar, R.; Tripathi, R. DBTP2SF: A deep blockchain-based trustworthy privacy-preserving secured framework in industrial internet of things systems. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4222. [CrossRef]
109. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Gadekallu, T.R.; Srivastava, G. SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. *Comput. Netw.* **2021**, *187*, 107819. [CrossRef]
110. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
111. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Gener. Comput. Syst.* **2019**, *100*, 779–796. [CrossRef]
112. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. [CrossRef]
113. Chen, L.; Kuang, X.; Xu, A.; Yang, Y.; Suo, S. Anomaly Detection on Time-series Logs for Industrial Network. In Proceedings of the 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China, 23–25 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 81–86.
114. Chen, L.; Lv, H.; Fan, K.; Yang, H.; Kuang, X.; Xu, A.; Yang, Y. A survey: Machine learning based security analytics approaches and applications of blockchain in network security. In Proceedings of the 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China, 23–25 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 17–22.
115. Li, T.; Ma, J.; Pei, Q.; Song, H.; Shen, Y.; Sun, C. DAPV: Diagnosing Anomalies in MANETs Routing With Provenance and Verification. *IEEE Access* **2019**, *7*, 35302–35316. [CrossRef]

116. Zhou, J.; Chen, Z.; Du, M.; Chen, L.; Yu, S.; Li, F.; Chen, G.; Xuan, Q. Adversarial enhancement for community detection in complex networks. *arXiv* **2019**, arXiv:1911.01670.
117. Li, T.; Ma, J.; Sun, C. Dlog: Diagnosing router events with syslogs for anomaly detection. *J. Supercomput.* **2018**, *74*, 845–867. [CrossRef]
118. Bagozi, A.; Bianchini, D.; De Antonellis, V.; Garda, M.; Melchiori, M. Services as Enterprise Smart Contracts in the Digital Factory. In Proceedings of the 2019 IEEE International Conference on Web Services (ICWS), Milan, Italy, 8–13 July 2019; pp. 224–228. [CrossRef]
119. Bagozi, A.; Bianchini, D.; De Antonellis, V.; Garda, M.; Melchiori, M. Exploiting Blockchain and Smart Contracts for Data Exploration As a Service. In Proceedings of the 1st International Conference on Information Integration and Web-Based Applications & Services, New York, NY, USA, 2–4 December 2020; pp. 393–402. [CrossRef]
120. Lopes, V.; Alexandre, L.A. Detecting Robotic Anomalies using RobotChain. In Proceedings of the 2019 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC), Gondomar, Portugal, 24–26 April 2019; pp. 1–6. [CrossRef]
121. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018. [CrossRef]
122. Casado-Vara, R.; Prieto, J.; la Prieta, F.D.; Corchado, J.M. How blockchain improves the supply chain: Case study alimentary supply chain. *Procedia Comput. Sci.* **2018**, *134*, 393–398. [CrossRef]
123. Ndiaye, M.; Diallo, T.A.; Konate, K. ADEFGuard: Anomaly detection framework based on Ethereum smart contracts behaviours. *Blockchain Res. Appl.* **2023**, *4*, 100148. [CrossRef]
124. Sammy, F.; Vigila, S.M.C. Anomaly Detection in Cloud Using Hexabullus Optimisation-Enabled Fuzzy Classifier with Smart Contract-Enabled Secure Communication. *J. Inf. Knowl. Manag.* **2024**, *23*, 2350058. [CrossRef]
125. Chen, D.; Liao, Z.; Chen, R.; Wang, H.; Yu, C.; Zhang, K.; Zhang, N.; Shen, X. Privacy-Preserving Anomaly Detection of Encrypted Smart Contract for Blockchain-Based Data Trading. *IEEE Trans. Dependable Secur. Comput.* **2024**, *21*, 4510–4525. [CrossRef]
126. Vaezi, M.; Azari, A.; Khosravirad, S.R.; Shirvanimoghaddam, M.; Azari, M.M.; Chasaki, D.; Popovski, P. Cellular, Wide-Area, and Non-Terrestrial IoT: A Survey on 5G Advances and the Road Toward 6G. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1117–1174. [CrossRef]
127. Wang, J.; Jin, H.; Chen, J.; Tan, J.; Zhong, K. Anomaly detection in Internet of medical Things with Blockchain from the perspective of deep neural network. *Inf. Sci.* **2022**, *617*, 133–149. [CrossRef]
128. Nguyen, T.D.; Marchal, S.; Miettinen, M.; Fereidooni, H.; Asokan, N.; Sadeghi, A.R. DÏoT: A Federated Self-learning Anomaly Detection System for IoT. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–9 July 2019; pp. 756–767. [CrossRef]
129. Liu, Y.; Garg, S.; Nie, J.; Zhang, Y.; Xiong, Z.; Kang, J.; Hossain, M.S. Deep Anomaly Detection for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach. *IEEE Internet Things J.* **2021**, *8*, 6348–6358. [CrossRef]
130. Fernandez Maimo, L.; Perales Gómez, Á.L.; García Clemente, F.J.; Gil Pérez, M.; Martínez Pérez, G. A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. *IEEE Access* **2018**, *6*, 7700–7712. [CrossRef]
131. Nguyen, H.L.; Eisenbarth, J.P.; Ignat, C.L.; Perrin, O. Blockchain-Based Auditing of Transparent Log Servers. In Proceedings of the Data and Applications Security and Privacy XXXII (DBSec 2018), Bergamo, Italy, 16–18 July 2018; Lecture Notes in Computer Science; Kerschbaum, F., Paraboschi, S., Eds.; Springer: Cham, Switzerland, 2018; Volume 10980, pp. 19–34. [CrossRef]
132. Careem, M.A.A.; Dutta, A. SenseChain: Blockchain based Reputation System for Distributed Spectrum Enforcement. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11–14 November 2019; pp. 1–10. [CrossRef]
133. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. [CrossRef]
134. Huang, J.; Kong, L.; Chen, G.; Wu, M.Y.; Liu, X.; Zeng, P. Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3680–3689. [CrossRef]
135. Kuo, C.C.; Shyu, J.Z. A cross-national comparative policy analysis of the blockchain technology between the USA and China. *Sustainability* **2021**, *13*, 6893. [CrossRef]
136. Kukrety, N.; Kaushik, P.; Pande, S.S. Blockchain Technology and Legal Framework in India: A Systematic Review. *Empir. Econ. Lett.* **2023**, *22*, 1–18.
137. Conlon, T.; Corbet, S.; Oxley, L. The influence of European MiCa regulation on cryptocurrencies. *Glob. Financ. J.* **2024**, *63*, 101040. [CrossRef]
138. Ponce-Bobadilla, A.V.; Schmitt, V.; Maier, C.S.; Mensing, S.; Stodtmann, S. Practical guide to SHAP analysis: Explaining supervised machine learning model predictions in drug development. *Clin. Transl. Sci.* **2024**, *17*, e70056. [CrossRef]
139. Dieber, J.; Kirrane, S. Why model why? Assessing the strengths and limitations of LIME. *arXiv* **2020**, arXiv:2012.00093. [CrossRef]

140. Patel, V.; Pan, L.; Rajasegarar, S. Graph deep learning based anomaly detection in ethereum blockchain network. In Proceedings of the International Conference on Network and System Security, Melbourne, Australia, 25–27 November 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 132–148.
141. Yang, X.; Yue, C.; Zhang, W.; Liu, Y.; Ooi, B.C.; Chen, J. SecuDB: An in-enclave privacy-preserving and tamper-resistant relational database. *Proc. VLDB Endow.* **2024**, *17*, 3906–3919. [CrossRef]
142. Yang, X.; Zhang, Y.; Wang, S.; Yu, B.; Li, F.; Li, Y.; Yan, W. LedgerDB: A centralized ledger database for universal audit and verification. *Proc. VLDB Endow.* **2020**, *13*, 3138–3151. [CrossRef]
143. Yang, X.; Zhang, R.; Yue, C.; Liu, Y.; Ooi, B.C.; Gao, Q.; Zhang, Y.; Yang, H. VeDB: A software and hardware enabled trusted relational database. *Proc. ACM Manag. Data* **2023**, *1*, 1–27. [CrossRef]
144. Chen, Z.; Duan, J.; Kang, L.; Qiu, G. Supervised anomaly detection via conditional generative adversarial network and ensemble active learning. *IEEE Trans. Pattern Anal. Mach. Intell.* **2022**, *45*, 7781–7798. [CrossRef] [PubMed]
145. Raza, A.; Hardy, L.; Roehrer, E.; Yeom, S.; Kang, B.H. GPSPiChain-blockchain and AI based self-contained anomaly detection family security system in smart home. *J. Syst. Sci. Syst. Eng.* **2021**, *30*, 433–449. [CrossRef]
146. Regev, Y.A.; Vassdal, H.; Halden, U.; Catak, F.O.; Cali, U. Hybrid ai-based anomaly detection model using phasor measurement unit data. In Proceedings of the 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), Irvine, CA, USA, 7–11 November 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
147. Olawale, O.P.; Ebadinezhad, S. Cybersecurity anomaly detection: Ai and ethereum blockchain for a secure and tamperproof ioht data management. *IEEE Access* **2024**, *12*, 131605–131620. [CrossRef]
148. Kuznetsov, O.; Frontoni, E.; Kuznetsova, K.; Shevchuk, R.; Karpinski, M. NFT Technology for Enhanced Global Digital Registers: A Novel Approach to Tokenization. *Future Internet* **2024**, *16*, 252. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.