Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 17 No. 3, September 2026 - www.cisdijournal.net

A Systematic Literature Review of Blockchain-Based Community Intelligence for Countering Criminal Logistics

[1]Ojerinde O.A., [2]Ojeniyi J.A., [2]Uduimoh A.A & [1]Noibi A.K.
[1]Department of Computer Science
[2]Department of Cybersecurity Science
Federal University of Technology Minna
Minna Niger state
Email: o.ojerinde@futminna.edu.ng, ojeniyija@futminna.edu.ng, a.uduimoh@futminna.edu.ng, abdulsalaam.m2203569@st.futminna.edu.ng

ABSTRACT

The increasing prevalence of kidnappings and armed banditry has intensified the need to disrupt the logistical networks that sustain criminal operations. These criminal networks pose significant threats to national security, socio-economic stability, and public safety. Blockchain technology and decentralised threat intelligence (DTI) platforms offer considerable potential for addressing these challenges through secure data management, informant anonymity, tamper-resistant record-keeping, and trusted information sharing. This systematic literature review synthesises recent studies on decentralised technologies and community-driven intelligence systems aimed at enhancing public safety and disrupting criminal logistics. Following PRISMA guidelines, the review examines peer-reviewed studies published from 2020 to 2026, retrieved from IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Web of Science, and Scopus. It analyses blockchain applications for digital evidence management, smart contract-based access control, and decentralised threat intelligence, while evaluating the datasets and performance metrics used to assess these systems. The review identifies several limitations in existing approaches, including deployment challenges in resource-constrained environments, the absence of mechanisms for tracking physical criminal supply chains, and the privacy risks associated with conventional centralised reporting systems. Although blockchain-based architectures demonstrate strong capabilities in ensuring data integrity, transparency, and resistance to single points of failure, current solutions remain largely focused on securing digital information rather than supporting the real-time disruption of illicit logistics in low-resource and violence-prone environments. These findings reveal a significant research gap in decentralised systems capable of integrating trusted community intelligence with operational support for disrupting physical criminal activities in resource-constrained environments. The findings establish a research foundation for the design of a Decentralised Autonomous Security Network (DASN), providing a pathway toward blockchain-enabled public safety and resilient community intelligence systems.

Keywords - Blockchain-Based Community Intelligence, Countering Criminal Logistics, Literature

CISDI Journal Reference Format
Ojerinde O.A., Ojeniyi J.A., Uduimoh A.A & Noibi A.K. (2026): A Systematic Literature Review of Blockchain-Based Community Intelligence for Countering Criminal Logistics. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 17 No 3, Pp 1-22. Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V17N3P1

1. INTRODUCTION

Blockchain-enabled technologies have emerged as promising tools for addressing complex security challenges in modern societies. The increasing sophistication of kidnapping, armed banditry, and other forms of organised crime has transformed criminal operations into highly coordinated socio-technical systems involving the movement of people, finances, information, and logistics across distributed networks. These activities exploit digital communication channels and decentralised operational structures that are difficult to monitor using conventional intelligence-gathering and centralised reporting mechanisms. Consequently, existing security frameworks often struggle to provide timely intelligence, secure information sharing, and effective coordination among multiple stakeholders involved in crime prevention and response.

Blockchain technology has attracted considerable attention as a decentralised infrastructure capable of improving security, transparency, trust, and data integrity in distributed environments such as the Internet of Things (IoT), finance, healthcare, and cyber-physical systems (Idrees et al., 2021). By eliminating reliance on trusted third parties, blockchain enables immutable record keeping, secure data exchange, and automated decision-making through smart contracts, thereby strengthening the resilience of distributed applications (Zubaydi et al., 2023). Recent systematic literature reviews have demonstrated the effectiveness of blockchain in securing cyber-threat intelligence platforms, industrial systems, and IoT ecosystems through decentralised architectures that facilitate trusted information sharing, intrusion detection, and collaborative threat analysis (Gugueoth et al., 2023; Saxena et al., 2023).

These capabilities suggest that blockchain can provide the technological foundation for a Decentralised Autonomous Security Network (DASN) that securely collects, verifies, and correlates community-generated intelligence to support the disruption of criminal logistics. By combining blockchain with decentralised threat intelligence principles, such a framework can facilitate tamper-evident record management, secure information exchange, and resilient collaboration without introducing a single point of failure (Nicolas et al., 2021).

Despite these advances, existing systematic reviews primarily examine blockchain from the perspectives of cybersecurity, industrial applications, decentralised finance (DeFi), healthcare, and IoT security (Gugueoth et al., 2023). Similarly, studies investigating blockchain architecture have focused on consensus mechanisms, security threats, and architectural design principles for distributed systems (Ahmadjee et al., 2022). While these contributions provide valuable insights into blockchain security, they offer limited evidence regarding the application of decentralised technologies to support community intelligence and disrupt the operational logistics of organised criminal networks.

Furthermore, existing research on decentralised threat intelligence and intrusion detection systems predominantly addresses cyber-domain threats and does not adequately consider the integration of localised community intelligence, anonymous reporting, and physical logistics monitoring within blockchain-enabled security architectures, particularly in fragile and violence-affected environments such as Nigeria (Ahakonye et al., 2024). Consequently, there remains a significant gap in the literature concerning context-specific blockchain frameworks capable of supporting intelligence-driven disruption of kidnapping and banditry logistics.

This systematic literature review (SLR) seeks to address this gap by critically evaluating and synthesising existing research on blockchain-based security solutions relevant to community intelligence and criminal logistics disruption. Specifically, the review examines blockchain architectures, decentralised threat intelligence models, smart contract applications, evaluation metrics, datasets, deployment challenges, and existing research limitations to establish a comprehensive knowledge base for the development of blockchain-enabled community intelligence systems.

The major contributions of this review are summarised as follows:

i. A comprehensive synthesis of blockchain-based security architectures applicable to community intelligence.
ii. A comparative analysis of datasets and evaluation metrics used to assess blockchain-enabled security frameworks.
iii. An assessment of the technical, operational, and infrastructural limitations affecting real-world deployment.
iv. Identification of existing research gaps and emerging directions for blockchain-supported public safety systems.
v. Development of a conceptual foundation for a Decentralised Autonomous Security Network (DASN) for disrupting criminal logistics through secure community intelligence.

The remainder of this paper is organised as follows. Section II describes the systematic literature review methodology, including the search strategy, study selection process, inclusion and exclusion criteria, quality assessment, and data extraction procedures. Section III presents the synthesised findings on blockchain security architectures, community intelligence models, decentralised threat intelligence, and criminal logistics disruption. Section IV discusses evaluation metrics, datasets, deployment challenges, research gaps, and future research opportunities, culminating in the conceptual foundation for a blockchain-enabled DASN framework.

2. PROCESS OF SLR

This systematic literature review (SLR) follows established guidelines for conducting evidence-based reviews, drawing on widely adopted SLR methodologies and reporting practices proposed by Kitchenham and Charters (2007), the PRISMA framework, and recent blockchain-focused systematic reviews (e.g., Zubaydi et al., 2023; Gugueoth et al., 2023). These methodologies provide a structured and transparent process for identifying, selecting, evaluating, and synthesising relevant literature while minimising selection bias and improving the reliability of the review. The review process is organised into three major phases: planning the review, conducting the review, and reporting the review.

2.1 Planning the Review

The planning phase establishes the foundation of the review by defining its objectives, justifying the need for the study, identifying the research questions, and selecting appropriate review protocols. This phase also ensures that the adopted methodology aligns with established SLR standards for blockchain and cybersecurity research, thereby enhancing the transparency, reproducibility, and credibility of the review.

2.2 Conducting the Review

The review was conducted through six sequential stages adapted from established SLR methodologies.

i. Research Questions (RQs): Research questions were formulated to define the scope of the review and guide the identification of relevant studies concerning blockchain-enabled security, community intelligence, and criminal logistics disruption. The formulation of these questions follows established practices adopted in previous blockchain-focused SLRs (Zubaydi et al., 2023).
ii. Search Strategy (SS): A comprehensive search strategy was developed to retrieve relevant studies from major scientific databases, including IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Scopus, and Web of Science. Appropriate keywords and Boolean search expressions were employed to maximise the retrieval of relevant literature while minimising irrelevant results.
iii. Study Selection Criteria (SSC): Explicit inclusion and exclusion criteria were established to reduce selection bias during the screening process. Studies were screened in multiple stages based on their titles, abstracts, and full texts to ensure that only relevant and high-quality publications were included.
iv. Quality Assessment Criteria (QAC): Each selected study was critically evaluated using predefined quality assessment criteria that considered methodological rigour, research design, evaluation procedures, and relevance to the review objectives. This assessment ensured that only credible and scientifically rigorous studies contributed to the synthesis.
v. v. Data Extraction and Management (DEM): Relevant information was systematically extracted from the selected studies using a structured data extraction process. This included documenting research objectives, methodologies, blockchain architectures, datasets, evaluation metrics, key findings, and identified limitations.
vi. Data Synthesis (DS): The extracted data were synthesised using a thematic analysis approach. Where appropriate, quantitative comparisons were also performed to identify trends, similarities, differences, and research gaps across the selected studies.

2.3 Reporting the Review

The findings of the review are presented in a structured format that addresses each research question and summarises the current state of knowledge, research gaps, and future research opportunities relevant to blockchain-enabled community intelligence and criminal logistics disruption.

2.4 Research Questions (RQs)

The formulation of research questions is a fundamental step in any systematic literature review, as it defines the scope of the investigation and guides the search, selection, and synthesis of relevant evidence. Based on the objectives of this study, five research questions (RQ1–RQ5) were developed to examine the application of blockchain technology in community intelligence and criminal logistics disruption. These research questions are presented in Table 1.

TABLE 1. Define research questions for the SLR.

QID	Research Questions	Objectives
RQ1	How do blockchain architectures help in community intelligence and the disruption of criminal logistics?	To analyse how blockchain technology is utilised to create secure, decentralised intelligence networks and disrupt criminal logistics.
RQ2	What datasets are commonly used with blockchain-based security and logistics disruption models?	To identify and utilise benchmark peer-reviewed and non-peer-reviewed datasets commonly paired with blockchain frameworks for training and evaluating community intelligence models.
RQ3	What evaluation metrics are used to compute the performance of intelligence and logistics disruption models using blockchain?	To identify the evaluation metrics commonly used to assess the performance (examples: latency, throughput, threat detection accuracy, and anonymity preservation) of security models utilising blockchain architecture.
RQ4	How do blockchain-based community intelligence frameworks perform compared to traditional centralised reporting models?	To critically evaluate and compare the operational efficiency, data security, and informant anonymity of decentralised blockchain architectures against standard centralised policing and crowdsourcing models.
RQ5	What are the infrastructural and operational challenges of deploying blockchain-based community intelligence frameworks in low-resource or high-risk environments?	To identify and analyse the technical, infrastructural (e.g., internet connectivity, power), and socio-technical barriers to implementing decentralised security solutions for real-time crime disruption.

2.5 Search Strategy (SS)

For a complete analysis, we referred to several top-level academic databases and not just one database. To maintain scientific rigour and peer-review standards, only those academic forums that were most relevant to our topic were given priority, and these are described below.

- ACM Digital Library
- ScienceDirect
- IEEE Xplore Digital Library
- SpringerLink
- Web of Science
- Scopus

The sources include prestigious journals, conferences, and scholarly repositories. In order to find the most relevant and up-to-date developments within decentralised technology and security, the timeframe of the search was limited to January 2020 until June 2026.

2.6 Search Keywords and Terms

Search terms for the systematic literature review (SLR) in question are divided into three main categories: blockchain technology, community intelligence and logistics, and disruption of crime. Terms pertaining to blockchain include:

- Blockchain and Decentralisation: "blockchain", "distributed ledger", "decentralised intelligence", "smart contracts", "decentralised network", and "consensus mechanism".
- Community Intelligence and Logistics: "community intelligence", "logistics disruption", "crowdsourced intelligence", "logistics mapping", "supply chain disruption", and "dynamic intelligence".
- Crime, Kidnapping, and Banditry: "kidnapping", "banditry", "criminal logistics", "public safety", "crime prevention", "illicit supply chain", and "security interception".

2.7 Boolean Search

It is intended to collect as many works as possible that are relevant to our research questions. During the collection of studies on blockchain-based security and logistics disruption, we included combinations of related search phrases to avoid any bias. The key idea involves using Boolean terminology to combine those searching terms with AND or OR operators. The search string can be outlined primarily as ("Blockchain" OR "Distributed Ledger" OR "Decentralised Network" OR "Smart Contracts") AND ("Community Intelligence" OR "Logistics Disruption" OR "Crowdsourced Intelligence" OR "Logistics Mapping" OR "Security Interception") AND ("Kidnapping" OR "Banditry" OR "Criminal Logistics" OR "Public Safety" OR "Crime Prevention" OR "Illicit Supply Chain")

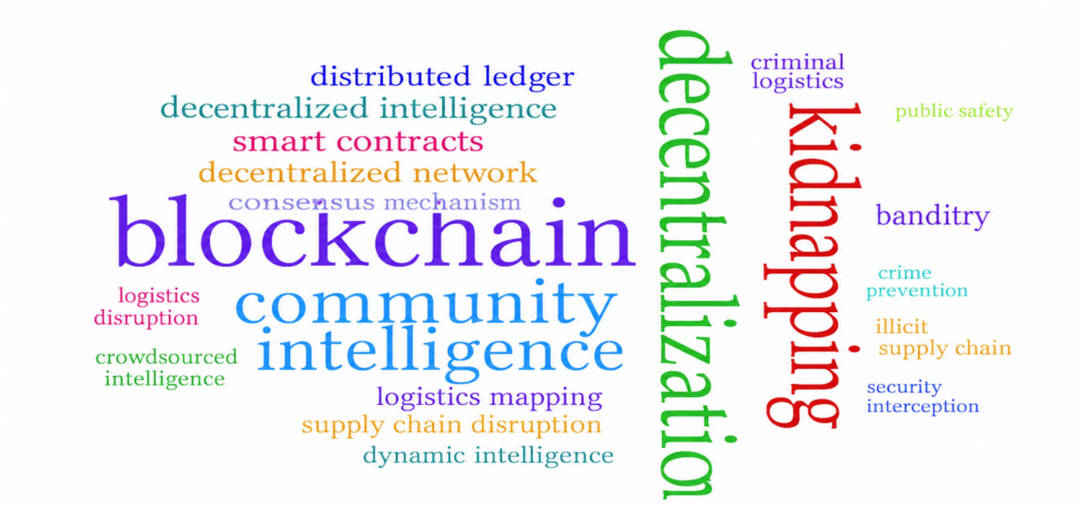

Fig. 1: Word cloud analysis regarding the use of blockchain technology for community intelligence to combat kidnapping and banditry

2.8 Study Selection Process

The evidence gathering process is documented in a PRISMA flowchart, as depicted in Figure 2, which outlines the data selection and evaluation stages.

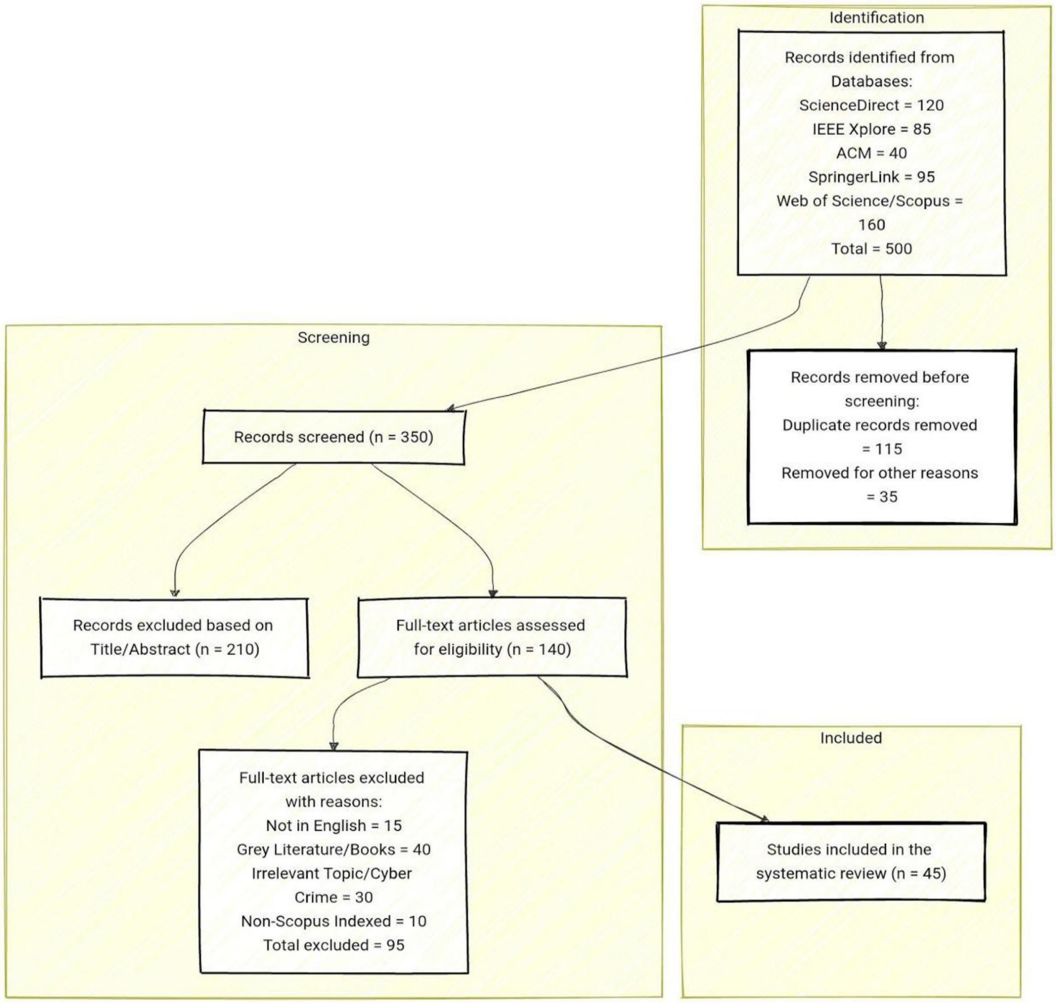

Fig2: PRISMA flow diagram reporting the data selection and screening process.

2.9 Inclusion and Exclusion Criteria

We considered different inclusion and exclusion criteria to gather relevant studies for our systematic review. The criteria used to select articles were as follows:

Inclusion criteria:

i. **Published** peer-reviewed articles, journals, and conference papers between January 2020 and June 2026.
ii. Articles that proposed, developed, or analysed blockchain architectures, decentralised frameworks, smart contracts, or distributed ledger technologies for community intelligence, public safety, and criminal logistics disruption.
iii. Articles directly related to our research questions that focus on the solution domain of utilising decentralised network architectures to combat security threats, track illicit operations, or enhance real-time crowdsourced intelligence tracking.

Exclusion criteria:

i. Duplicate articles were found across various academic databases.
ii. Papers written in any language other than English.
iii. Sources which do not cover blockchain technology, distributed ledger solutions or decentralised intelligence architecture.
iv. Articles which are only concerned about socio-political or historical aspects of crime, banditry and kidnapping without providing any technological solution, domain or framework architecture.
v. (v) General overview papers, surveys or online sources which are not peer reviewed and do not present any methodology or performance analysis.

With the use of this methodology, this review made sure that all relevant articles were included in the systematic review while irrelevant ones were filtered out.

2.10 Quality Assessment

The evaluation of the quality of evidence in a systematic review is just as important as the analysis of the evidence itself. There may be certain methodological errors in the weaker studies, and such problems should be considered properly. Studies with weak methods or problems that may affect the accuracy of their results should be identified and/or eliminated from the literature review. It is necessary to choose the criteria for assessing the credibility of the information and identify possible problems in each study. Using proper methodology criteria, this systematic review made sure that the selected frameworks provided scientifically proven evidence in the solution domain.

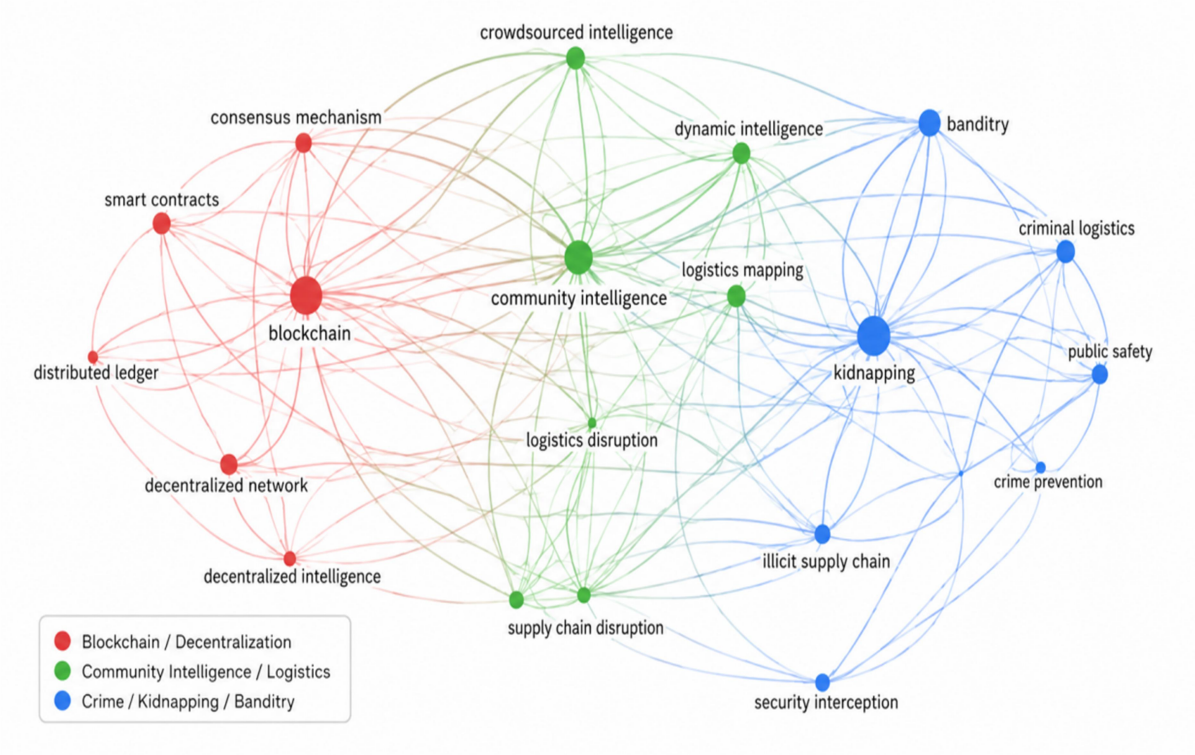

Fig. 3. Keyword co-occurrences visualisation analysis of eligible studies using the VOSviewer tool.

Moreover, a rigorous verification procedure was used to determine the papers selected to ensure consistency between different sources of information and verify that these sources were directly related to decentralised security systems. After the process of evaluation and use of inclusion and exclusion criteria, a total of 50 relevant papers was selected, covering topics such as blockchain technology, crowd intelligence, and disruption of criminal logistics. Figure 3 shows the co-occurrence of keywords analysis, demonstrating how often certain terms related to the research appear in the selected papers.

3. CRIMINAL LOGISTICS AND TRADITIONAL INTELLIGENCE GATHERING METHODS

Armed banditry in Nigeria, particularly in the northwest region, has progressed from occasional rural conflicts to a highly organised and sophisticated criminal network. According to Ojo et al. (2023), the recent trend of insecurity in Nigeria goes beyond insurgency and works through a complex network of visible and invisible actors. These networks disrupt socio-economic activities and displace populations through attacks and kidnappings. The success and speedy development of these syndicates depend, to a large extent, on efficient financial networks. Ejiofor (2025) argues that criminal logistics are actively supported by different terrorism financing mechanisms such as ransom kidnapping, illegal mining, and extortion.

In combination, these articles show that modern-day banditry represents a well-supported and geographically widespread system which needs logistical support to be sustained. However, the literature proposes the reorganisation of traditional policing to fight these highly financed and resourced networks. For instance, Ojewale (2023) shows how the geography of attacks is distributed and proposes a multi-level policing system. This traditional model attempts to counter banditry using an integrated approach of regular policing combined with state police and joint task forces, as well as hybrid forms of local policing.

Nevertheless, while the aim of these models lies in increasing physical presence, they are severely limited by the use of traditional intelligence and physical command structures. An analysis of these conventional strategies reveals multiple flaws. First, the use of the traditional policing models cannot provide the necessary scalability to cover the vast and largely ungovernable rural areas where the syndicates operate (Ojewale, 2023). Second, traditional models cannot provide the required security for the informants. Due to the strong connections of these networks with the local political economy (Ejiofor, 2025), people risk retaliation when reporting any suspicious logistical activities to the local authorities. Lastly, these models experience serious deployment problems, as the security personnel cannot react promptly to the movement of weapons and abducted people within the challenging terrain.

The inability of physically oriented traditional policing models to safely collect the information from communities, ensure the security of informers, and quickly interfere in the movement of the supply chains demonstrates a serious flaw of the current system. Hence, in order to compensate for the lack of scalability, inefficiency in real-time intelligence gathering, and promptness, there is an urgent need to go beyond mere reorganisation of the physical policing structure. These challenges make one move on to the question of technological interventions in security disruption.

3.1 Technological Interventions in Security Disruption

In order to neutralise the logistical advantages of armed bandits and kidnapping syndicates, technologically oriented interventions have gained ground among both researchers and security agencies. First, the existing literature presents several examples of efforts aimed at implementing digital technologies to prevent crimes. For example, Emekumeh et al. (2026) developed a technological framework which combines the use of the Internet of Things (IoT), GPS transmission, and geofencing in tracking the movements of kidnapping victims. This research shows how location-based technologies can successfully be used to monitor spatial movements and collect information about victims. In addition, geospatial technologies such as Geographic Information Systems (GIS) are actively used in crime analysis. A recent space-based analysis in Niger State demonstrated the use of spatial analysis to map areas with high rates of banditry activities. Therefore, technology can successfully map ungoverned rural routes and logistics networks of criminal groups (Haruna et al., 2026).

Nevertheless, despite the evident benefits of technological interventions in crime prevention, their practical implementation raises concerns related to the operational limitations. First of all, the key problem in terms of using these technologies lies in the fact that these centralised systems suffer from inefficiency and slow reactions. As stated in a 2026 study analysing the cases of kidnapping in Enugu State, overreliance on physical surveillance technologies such as drones and digital checkpoints proved to be ineffective without community intelligence in real time. Additionally, it was discovered that the surveillance conducted with the help of drones did not manage to prevent 63% of kidnappings due to routine drone flight schedules and lack of coordination between various security agencies. (Akoji et al., 2026).

Additionally, technologies such as IoT tracking and GIS mapping have obvious difficulties in deployment in the context of rural Nigeria since they rely heavily on stable internet connections and centralised databases, making them highly vulnerable to possible network problems and even cyber-attacks by technologically-sophisticated criminal syndicates (Emekumeh et al., 2026). Most importantly, these technological frameworks ignore the human element of intelligence; for example, a drone can map a forest but cannot get reliable tips from a scared villager. All mentioned limitations related to hardware-dependent and centralised frameworks show that there is a need for the creation of a system which would combine human reporting and technological security measures. Since the existing technologies do not provide any adequate infrastructure that will protect the identities of informants, the limitations above lead to the need for centralised and crowdsourced community intelligence models, where human intelligence can be digitised.

3.2 Centralised and Crowdsourced Community Intelligence Models

In order to overcome the slow responses associated with conventional methods, recent technological initiatives aim at harnessing crowdsourced community intelligence. The fundamental principle of crowdsourcing involves giving the ability to normal citizens to become real-time informers through their phones. The empirical studies done in this field illustrate the feasibility of such crowdsourcing models through mobile applications where civilians can communicate with the law enforcers directly. For example, the Bantay model demonstrates how crowdsourcing enables real-time intelligence from civilians to be used by the police to make decisions and respond quickly to any event (Malang & Solis, 2024). Usability studies of crowdsourced crime-reporting systems, such as the Melden application, demonstrate the potential of civilian-enabled reporting and mapping to improve the usability and efficiency of crime-reporting processes (Rey, 2024).

Another aspect of crowdsourcing involves integrating the reports provided by civilians with the location-tracking technology. Recent frameworks such as E-report MO integrate interactive spatial mapping with SMS-based authentication mechanisms to support the submission and verification of civilian crime reports (Mangrobang & Genove, 2025). Therefore, it is clear from the above discussion that crowdsourcing allows civilians to provide real-time and accurate intelligence that would otherwise be difficult for conventional patrols to acquire.

Nevertheless, a critical evaluation of the crowdsourcing models highlights some significant systematic weaknesses, especially concerning the utilisation of the centralised database architecture. First, the key limitation of crowdsourcing models involves the lack of true anonymity. The use of SMS OTP in systems such as E-Report MO links the crime reports to the citizen's phone number (Mangrobang & Genove, 2025). In regions where there is a lot of violence by bandit groups, making civilian informants give their personal information on the central server would pose a big danger to their lives. Furthermore, such crowdsourcing models suffer from poor deployability and scalability in such risky areas. If civilians think that their central police database could be hacked or accessed by insiders, then they might stop utilising the application, and the crowdsourced intelligence network fails. Centralised servers form the single point of failure. Thus, if the server fails, the whole community intelligence network would also fail.

The inherent weakness of centralised crowdsourcing models in ensuring absolute informant anonymity and preventing the central server manipulation poses a serious problem when dealing with such a dangerous and well-organised kidnapping syndicate. There is, therefore, the need for a system where citizens can report criminal logistics with substantially reduced risk of exposure, and the limitations of these centralised platforms establish the need for blockchain applications in public safety, where decentralised technology can secure intelligence without relying on a vulnerable central authority.

3.3 Blockchain Applications in Public Safety and Evidence Management

In order to protect crime-reporting databases from various risks involved, recent research has started looking for decentralised structures with a special emphasis on blockchain technology. Initially invented as an open and distributed accounting system of financial transactions, blockchain represents a distributed and immutable database where information is replicated across many nodes rather than stored on a single server. For law enforcement purposes, researchers have already successfully applied blockchain technologies in protecting sensitive police data. For example, in their research, Park & Jeong (2026) introduced a blockchain-based digital evidence management system which would prevent any manipulations of the records of crimes.

As shown by the study, due to its structure and functioning based on cryptographic hashing, blockchain creates a tamper-evident chain of custody. Therefore, unauthorised alteration of a record becomes immediately detectable. In addition, administration of the whole security protocol is possible in an automated way. According to Y. Zhang et al. (2019), integration of smart contracts, which represent self-executing code in the blockchain technology, allows implementing decentralised access control and disclosure of the information in case of necessity to authorised officers without using a vulnerable central administrator.

Finally, apart from providing a high level of security of digital data, blockchain has proved its efficiency in tracking real-world actions. For example, Hasan & Salah (2018) presented the use of distributed ledgers and smart contracts in creating a verifiable system for monitoring the logistics and delivery of physical goods by several companies. In this way, the location and custodian of an asset can be verified at any point in the chain. However, despite being promising examples showing the high potential of blockchain as a highly secured technology, these studies have some important shortcomings related to the usage of the technology for active crime prevention. First, the system proposed by Park and Jeong (2026) focuses on securing static data and protecting the results of the crime after it has been done but not on preventing or stopping any crime. Secondly, although in the model of Hasan & Salah (2018) there is a possibility to track the logistics, it is supposed that everyone, especially delivery drivers, agrees to be monitored, and therefore, such a model cannot be used for tracking the logistics of active crimes. Hence, it is clear that blockchain is very efficient when it comes to ensuring the security of static public safety information, but blockchain has not proved to be efficient in disrupting criminal enterprises in real time. In light of the deficiencies in the static evidence paradigm, a decentralised threat intelligence framework is needed whereby the blockchain system works alongside crowdsourced intelligence.

3.4 Decentralised Threat Intelligence Frameworks

In light of the increasing limitations of centralised databases, current research has increasingly shifted towards decentralised threat intelligence (DTI) models. Such approaches leverage blockchain technology to allow multiple entities to share security information without depending on a single trusted authority. For instance, Riesco et al. (2020) designed an architecture with the help of smart contracts that allows the automatic sharing of threat intelligence among various parties. Since the ledger is distributed, this design makes unilateral alteration or deletion of shared intelligence detectable.

One of the key benefits of decentralised systems is the possibility to work with crowdsourced information safely. Patel et al. (2022) argued that blockchain integration into collaborative threat detection allows distinct communities or network nodes to detect intrusions independently from a single vulnerable central server. Overall, it is possible to conclude that decentralised architectures can resolve many privacy, trust and single-point-of-failure issues associated with traditional crowdsourcing applications.

Nonetheless, a critical analysis of the advanced models shows that there is one crucial limitation of such DTI architectures, which is their application to physical crimes. The model proposed by Riesco et al. (2020) is likewise concerned exclusively with digital threats. Similarly, Patel et al. (2022) focused on a blockchain and deep learning-based collaborative intelligence framework for detecting malicious activities and supporting public safety through surveillance data, rather than on civilian crowdsourced crime reporting. These digital frameworks rely on computers automatically communicating with one another in high-resource, high-connectivity environments. They lack the deployment feasibility required for low-resource environments and do not account for human-driven, physical intelligence gathering. Specifically, these existing models lack the spatial and logistical mapping capabilities necessary to track physical criminal movements, such as a kidnapping convoy navigating through rural terrains.
Therefore, while decentralised networks have solved the problem of secure intelligence sharing in the digital space, there is a critical need for a framework designed for the physical world in order to successfully combat the complex operations of armed syndicates; the cryptographic security and

anonymity of these DTI models must be adapted into a system built for physical community reporting. These limitations establish the need for a Decentralised Autonomous Security Network (DASN) framework, which bridges this exact gap by utilising blockchain to safely gather, map, and disrupt real-world criminal logistics.

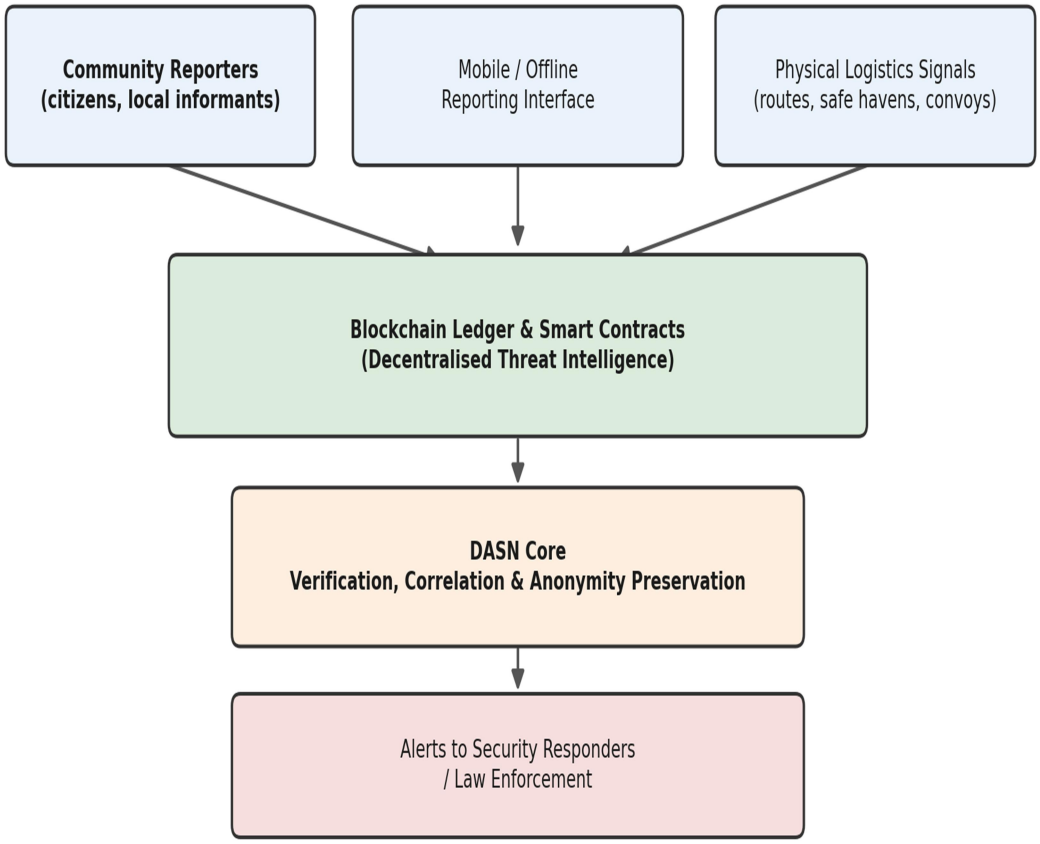

Fig. 4. Conceptual architecture of the proposed Decentralised Autonomous Security Network (DASN), showing community reporting inputs, the blockchain-based decentralised threat intelligence layer, and the verification/alerting pathway to security responders.

RQ1: How are blockchain architectures applied for community intelligence and criminal logistics disruption?

Rathod et al. (2023) present a layered blockchain AI–6G architecture for public safety, where IoT devices collect crime-related data (examples: location, type, and weapon), which are stored in an IPFS-based blockchain so police and public safety authorities can securely access attack-free datasets. The immutability and transparency of the ledger are used to detect or expose data-injection attempts on crime records, protecting criminal intelligence from manipulation and supporting more reliable decision-making. Patel et al. (2022) propose BlockCrime, a collaborative intelligence framework that combines an Xception CNN with blockchain.

Detected crime scenes are written to a blockchain via smart contracts, which automatically store incident locations and trigger alerts to nearby law-enforcement agencies, creating a tamper-resistant, shared operational picture for early disruption of malicious activity. Karambe (2023) describes a global criminal-records blockchain in which national police databases are integrated via APIs and stored in an encrypted, immutable, distributed ledger. This architecture lets investigative agencies worldwide query unified criminal histories of transnational offenders, which reduces delays in background checks and limits opportunities to exploit jurisdictional gaps in criminal logistics.

Luo (2020) and subsequent law-enforcement-focused works apply blockchain as a forensic and evidence-chain substrate, recording law-enforcement evidence and operational data in a tamper-proof ledger. This law-enforcement-data-on-blockchain approach is intended to strengthen the integrity, availability, and auditability of case and logistics information used to plan and execute operations against criminal networks.

RQ2: What datasets are commonly used with blockchain-based security and logistics disruption models?

We found several blockchain and supply-chain datasets that are widely used to train and evaluate security and logistics anomaly models. These datasets cover cryptocurrency fraud, ransomware, network-level attacks, synthetic supply-chain logs, and custom crime datasets on blockchain ledgers.

Common Blockchain Security & Fraud Datasets

1. Raw Bitcoin Transactions (Kaggle Bitcoin dataset): A large-scale Bitcoin transaction dataset (≈30 million transactions, 11 attributes), used for classifying fraudulent vs. legitimate transactions; many studies downsample to ≈30,000 records for computation. (Ashfaq et al., 2022)
2. Bitcoin Heist Ransomware Dataset (Kaggle / UCI): Public multiclass dataset converted to binary (normal vs. ransomware), with 2,916,697 instances and 10 features; widely used for fraud and ransomware detection on Bitcoin. (Nayyer et al., 2023)
3. Labelled Ethereum Transactions Dataset: A benchmark Ethereum transactions dataset designed for intrusion/anomaly detection, with transaction-based features (examples: gas price, gas cost, token amount), built on a real Ethereum network and publicly available for tuning and comparing IDS models. (Son et al., 2024)
4. Open-Metaverse Blockchain Transactions Dataset: A 78,600-transaction dataset capturing diverse user behaviours and transaction types in a metaverse blockchain environment, used to benchmark multiple ML models for anomaly and fraud detection. (Airlangga, 2024)
5. Generic Blockchain Crime / Forensics Dataset (SentinelFusion): A custom blockchain-stored crime dataset with attributes such as timestamps, access logs, encryption levels, network traffic, and malware indicators, used for crime classification and prediction in computer forensics. (Islam et al., 2025)

Blockchain-Enabled Supply Chain & Logistics Datasets

1. Smart Farming Data 2024 (Agricultural Supply Chain): Supply-chain data for smart farming, preprocessed and stored on IPFS/blockchain, then used with Graph Neural Networks for anomaly detection in agricultural blockchain supply chains. (Muhsn Hasan et al., 2025)
2. Laboratory BSC Network Traffic Dataset: Network-layer traffic from an implemented Ethereum-based supply-chain system, containing normal and attack traffic, used for anomaly detection (DAE-MLP) across network and consensus layers. (Son et al., 2024)
3. Simulated Procurement / Business-Process Logs: Event logs generated from a simulated procurement process in a global supply chain, used as a testbed for ontology-based anomaly classification in blockchain-enabled business workflows. (Musa & Bouras, 2021)
4. Blockchain-Based Electronic Health Records (EHR): Encrypted logs from a decentralized ledger simulating medical stakeholder interactions, featuring transactional metadata, timestamps, cryptographic verdicts, and secure patient data exchanges, used to study system security, privacy, and the mitigation of centralized failures.(Kiania et al.,2023)
5. Blockchain Supply-Chain Time-Series Data (iTransformer System): Supply-chain time-series data (examples: contract status, delivery time, environmental conditions) are recorded on blockchain and used to benchmark iTransformer-based forecasting and anomaly detection.

RQ3: What evaluation metrics are used to compute the performance of intelligence and logistics disruption models using blockchain?

This section summarises how blockchain-enabled intelligence and logistics-disruption models, mainly anomaly/crime detection and logistics theft control, are evaluated. Classification-based detection is the most common approach used, with confusion matrix-based metrics being developed from it.

Confusion Matrix

A 2×2 (or multi-class) confusion matrix counts true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN), providing a visual means of evaluating and comparing classification performance in blockchain anomaly-detection and blockchain-based crime-forensics frameworks (Kamran et al., 2024; Islam et al., 2024).

Table 2: Confusion matrix for blockchain-based detectors

	Actual Positive	Actual Negative
Predicted Positive	TP	FP
Predicted Negative	FN	TN

Core Classification Metrics

The following metrics are widely used:

1. Accuracy: overall correctness of anomaly/crime or theft-risk prediction; explicitly used in blockchain anomaly detection and logistics theft control.
2. Precision: proportion of predicted anomalies/crimes/thefts that are truly malicious (controls false alarms).
3. Recall / True Positive Rate (TPR): the proportion of actual malicious or anomalous events correctly detected.
4. F1-score: harmonic mean of precision and recall; used extensively to balance missed detections and false alarms in blockchain anomaly and forensics settings.

5. ROC curve & AUC: used in crime-detection and forensic blockchain frameworks to study trade-offs between TPR and FPR and to summarise discrimination ability.

Table 3: Key evaluation metrics in blockchain-based intelligence/logistics disruption

Metric	Role in evaluation
Accuracy	Overall correctness of detection
Precision	Controls false positives
Recall/TPR	Captures missed anomalies/crimes
F1-score	Balances precision and recall
ROC–AUC	Threshold-independent discrimination

RQ4: How do blockchain-based community intelligence frameworks perform compared to traditional centralised reporting models?

Research on blockchain-based community intelligence and reporting generally compares them to centralised or earlier blockchain/CTI models using throughput, latency, accuracy, scalability, and security/privacy metrics.

1. Incident & Crime Reporting Performance

Diallo et al. (2024) propose a decentralised Incident Reporting System (IRS) on Quorum-Raft for urban communities. It is evaluated on:

- Incident notification delay (from user submission to blockchain storage and IPFS write/read) and end-to-end response time (including emergency services action).
- Throughput and scalability: empirically, the system sustains up to 200 incidents/s with latency under 15 s even at high transaction rates and is deemed cost-effective for 16 organisations over 5 years (< USD 1.99M) (Diallo et al., 2024).

Compared to traditional centralised systems not reimplemented in this paper, the authors argue for improved efficiency, transparency, scalability and cost-effectiveness, based on these empirical figures and qualitative analysis. A blockchain-based FIR registration system likewise reports better transaction throughput, security and operational efficiency than centralised FIR platforms, though detailed numbers are not provided (Parab et al., 2025).

2. Anonymous / Decentralised Reporting vs Other Protocols

The ARSnCA anonymous reporting protocol removes a central authority using a virtual blockchain. In comparative evaluations against ring-signature and related reporting protocols, ARSnCA achieves 62% and 92% faster reporting speeds, respectively, indicating clear latency advantages over prior (non-blockchain or centrally controlled) designs (Far & Asaar, 2023).

3. Cyber-Threat / Community Intelligence Sharing

Zhang & Miao present a consortium-blockchain CTI sharing model with a proof-of-reputation consensus. They compare latency and throughput to other blockchain CTI models (CFT/BFT-based):

- Latency: PoR is slightly worse than CFT (≈20% overhead) but better than BFT-based models;
- Throughput: PoR outperforms BFT-based models and loses ≈30% throughput compared with CFT, trading some speed for Byzantine fault tolerance (X. Zhang & Miao, 2021)

4. Block-Intel-Chain, a blockchain-based CTI framework, is benchmarked against centralised platforms MISP, ThreatConnect, IBM X-Force and prior blockchain CTI systems.

- Achieves 923 TPS at 500 nodes with 99.6% consensus success, maintaining low CPU overhead.
- FL-based models reach 96.4% malware, 94.7% phishing, and 95.2% anomaly detection accuracy, exceeding centralised baselines (~93.2%) and with 28% lower training latency and 35% reduced communication overhead (Tolah, 2025).
- Overall performance score 89.6/100 vs 69.6 for earlier blockchain CTI and 62.0 for MISP, with the largest gains in decentralisation and privacy. (Tolah, 2025)

Table 4: Comparative performance of blockchain-based and traditional centralised systems

Framework / Model	Baseline / Comparator	Key Metrics & Results
IRS (Quorum–Raft) (Diallo et al., 2024)	Traditional centralised incident management	≤15 s latency; up to 200 incidents/s; multi-org cost < USD 1.99M / 5 years; claimed gains in efficiency, transparency, scalability and cost-effectiveness. (Diallo et al., 2024)
BlockFIR, Decentralised FIR (Parab et al., 2025)	Centralised FIR systems	Higher transaction throughput, security and operational efficiency (qualitative, no exact figures).
ARSnCA reporting (Far & Asaar, 2023)	Ring-signature & related protocols	62% and 92% faster reporting performance than comparator protocols.
PoR-based CTI sharing (Zhang & Miao, 2021)	CFT, BFT blockchain CTI models	Latency slightly higher than CFT but lower than BFT; throughput higher than BFT, ~30% lower than CFT due to Byzantine tolerance.
BlockIntelChain CTI (Tolah, 2025)	MISP, ThreatConnect, IBM X-Force, prior blockchain CTI	923 TPS @500 nodes; 94.7–96.4% detection accuracy vs 93.2% centralised; 28% less training latency, 35% less communication; overall score 89.6 vs 62–69.6.

RQ5: What are the infrastructural and operational challenges of deploying blockchain-based community intelligence frameworks in low-resource or high-risk environments?

This section highlights main limitations and challenges for real-world deployment, focusing on infrastructure, operations, and context rather than algorithm design.

Infrastructure-Centric Limitations

Scalability, latency, and resource constraints: Public blockchains suffer from low throughput, high latency, large storage, and high energy use; these issues are tightly linked to consensus design and hinder practical IoT and smart-environment deployments. (Saeed et al., 2022) The paper studies the IoT ecosystem with constraints on the amount of storage space, weak wireless networks, and computational costs related to encryption and mining that create the need for optimisation of block placement and collaborative storage (Leng et al., 2022). The increase in throughput (about 300–400 transactions per second) is possible in telecommunication and blockchain implementation but demands greater computational cost.

Heterogeneous network and geographic aspects: Community intelligence networks have to be developed in different organisations and in different geographic locations having different bandwidths and latencies. This heterogeneity makes the network creation and operation challenging (Tolah, 2025). Furthermore, the choice and funding of the infrastructure, on-premises, IaaS, or SaaS are connected to costs, efficiency, and scalability issues that are often underestimated. Security, privacy, and governance limitations: Organisations are hesitant to exchange their intelligence because of the risks connected to privacy issues, lack of legislation, and fear of information leakage or manipulation. In addition, the blockchain-based CTI systems can be exposed to Byzantine behaviour, lies, and insider attacks.

4. CONCLUSION

This systematic literature review (SLR) evaluates the modern attempts to use blockchain technology and decentralisation methods for community intelligence and the prevention of criminal logistics based on 50 papers published between January 2020 and June 2026. The paper focuses on the solution area of using decentralised networks to address critical security problems and provides the general conclusions as follows:

- The SLR indicates that blockchain architectures, when used for public safety and threat intelligence, perform highly effectively in securing data integrity and ensuring informant anonymity, especially when combined with automated smart contracts.
- The review finds that recent decentralised security systems are mostly evaluated on the basis of cyber threat databases or law enforcement supply chain logs, revealing a significant absence of data sets that demonstrate illegal logistics operations in the physical world.
- According to the results of the Systematic Literature Review (SLR), the three most used performance criteria to evaluate the efficiency of such decentralised systems are the latency of the system, throughput of transactions, and anonymity conservation. Thus, it can be concluded that there are significant opportunities for decentralised systems compared to centralised ones in relation to security and anonymity of the data; however, experimental evidence and validation of disruption of physical logistics of criminals are significantly insufficient in the current literature.

In general, it becomes clear from the results that the blockchain provides a significant solution for securing community intelligence and protecting vulnerable civilian sources. However, taking into account considerable infrastructural problems (lack of Internet connectivity and unreliable electricity supply in rural areas where criminal armed syndicates operate), application of decentralised architectures to disrupt criminal operations in real time faces certain technical and operational difficulties. This SLR is offered as a key source of information for further research and security organisations in the creation of detection and protection mechanisms and serves as a background for the suggested Decentralised Autonomous Security Network (DASN) framework.

REFERENCES

Ahakonye, L. A. C., Nwakanma, C., & Kim, D.-S. (2024). Tides of Blockchain in IoT Cybersecurity. *Sensors*, *24*. https://doi.org/10.3390/s24103111

Ahmadjee, S., Mera-Gómez, C., Bahsoon, R., & Kazman, R. (2022). A Study on Blockchain Architecture Design Decisions and Their Security Attacks and Threats. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, *31*, 1–45. https://doi.org/10.1145/3502740

Airlangga, G. (2024). Anomaly Detection in Blockchain Transactions: A Machine Learning Approach within the Open Metaverse. *Jurnal Informatika Ekonomi Bisnis*. https://doi.org/10.37034/infeb.v6i2.864

Akoji, R. O., Kosok, D., Gabriel, V. A., & Oduntan, J. O. (2026). The limits of technology-led security, community exclusion and kidnapping along Ugwuogo Road, Enugu State, Nigeria. Journal of Arts and Sociological Research, 11(6). https://doi.org/10.70382/ajasr.v11i6.095

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A., Alsafari, S., & Hameed, I. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors*, *22*. https://doi.org/10.3390/s22197162

Diallo, E.-H., Abdallah, R., Dib, M., & Dib, O. (2024). Decentralized Incident Reporting: Mobilizing Urban Communities with Blockchain. *Smart Cities*. https://doi.org/10.3390/smartcities7040090

Ejiofor, P. F. (2025). Accumulation by/for terrorism: the political economy of terrorism financing in Nigeria. *Small Wars and Insurgencies*, *36*(1), 120–159. https://doi.org/10.1080/09592318.2024.2425181

Emekumeh, O. S., Abel, E. E., & Opuh, J. I. (2026). HYBRID TECHNOLOGIES FOR COMBATING KIDNAPPING. *FUDMA JOURNAL OF SCIENCES*, *10*(2), 390–399. https://doi.org/10.33003/fjs-2026-1002-4386

Far, S. B., & Asaar, M. (2023). A blockchain-based anonymous reporting system with no central authority: Architecture and protocol. *Cyber Secur. Appl.*, *2*, 100032. https://doi.org/10.1016/j.csa.2023.100032

Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. *Comput. Sci. Rev.*, *50*, 100585. https://doi.org/10.1016/j.cosrev.2023.100585

Haruna, M., Ogbole, J. O., Shar, J. T., Salman, S. K., Dalhatu, A., Agu, V. N., Nsofor, C., Ojukwu, P. N., & Adebowale, K. O. (2026). Space-Based Assessment of Banditry and its Nexus with Ungoverned Spaces in Niger State, Nigeria. LASU Journal of Peace and Security Studies (LAJOPSS), 2(1), 212–234. https://doi.org/10.5281/zenodo.19729197

Hasan, H. R., & Salah, K. (2018). Blockchain-Based Proof of Delivery of Physical Assets with Single and Multiple Transporters. *IEEE Access*, *6*, 46781–46793. https://doi.org/10.1109/ACCESS.2018.2866512

Hossain, M. S., Islam, M., Ali, M., Chy, K. S., & Hossain, M. S. (2025). Blockchain AI for Supply Chain Transparency: Integrating Blockchain with AI to Detect Fraud and Ensure Transparency Across Multi-Tier Global Supply Chains. *Business and Social Sciences, 3(1), 1-12, 10457* https://doi.org/10.25163/business.3110457

Idrees, S., Nowostawski, M., Jameel, R., & Mourya, A. K. (2021). Security Aspects of Blockchain Technology Intended for Industrial Applications. *Electronics*, *10*, 951. https://doi.org/10.3390/electronics10080951

Islam, U., Alsadhan, A. A., Alwageed, H. S., Al-Atawi, A. A., Mehmood, G., Ayadi, M., & Alsenan, S. (2024). SentinelFusion based machine learning comprehensive approach for enhanced computer forensics. PeerJ Computer Science, 10, e2183. https://doi.org/10.7717/peerj-cs.2183

Kamran, M., Rehan, M. M., Nisar, W., & Rehan, M. W. (2024). AHEAD: A novel technique combining anti-adversarial hierarchical ensemble learning with multi-layer multi-anomaly detection for blockchain systems. Big Data and Cognitive Computing, 8(9), 103. https://doi.org/10.3390/bdcc8090103

Karambe, A. (2023). Blockchain-based approach for tracking global criminals. International *Journal of Scientific Research in Engineering and Management, 7(4).* https://doi.org/10.55041/IJSREM19377

Kiania, K., Jameii, S., & Rahmani, A. (2023). Blockchain-based privacy and security preserving in electronic health: a systematic review. *Multimedia Tools and Applications*, 1–27. https://doi.org/10.1007/s11042-023-14488-w

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering.

Leng, J., Zhou, M., Zhao, L., Huang, Y., & Bian, Y. (2022). Blockchain Security: A Survey of Techniques and Research Directions. *IEEE Transactions on Services Computing*, *15*, 2490–2510. https://doi.org/10.1109/tsc.2020.3038641

Luo, W. (2020). Research and Application of Blockchain Technology in Transportation Administrative Law Enforcement. *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, 766–770. https://doi.org/10.1109/itoec49072.2020.9141836

Ma, X., Yu, D., Du, Y., Li, L., Ni, W., & Lv, H. (2023). A Blockchain-Based Incentive Mechanism for Sharing Cyber Threat Intelligence. *Electronics (Switzerland)*, *12*(11). https://doi.org/10.3390/electronics12112454

Malang, B. P., & Solis, J. (2024). BANTAY: An analytical crowdsourcing mobile application for improving peace and order in the town of San Miguel, Bulacan. In 2024 2nd International Conference on Computing and Data Analytics (ICCDA). IEEE. https://doi.org/10.1109/ICCDA64887.2024.10867333

Mangrobang, A. N., & Genove, G. P. (2025). E-report MO: A crime reporting mobile application with interactive map and SMS service. AIP Conference Proceedings, 3287(1), 030012. https://doi.org/10.1063/5.0262370

MuhsnHasan, M., K, P., Shahebaaz, A., Devi, M., & Sushama, C. (2025). Securing Blockchain based Supply Chains in Agriculture using Graph Neural Networks for Anomaly Detection. *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)*, 1–5. https://doi.org/10.1109/iciscn64258.2025.10934647

Musa, T. H. A., & Bouras, A. (2021). *Anomaly Detection in Blockchain-Enabled Supply Chain: An Ontological Approach*. 253–266. https://doi.org/10.29117/quarfe.2021.0169

Nayyer, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N., & Jamil, M. (2023). A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities. *IEEE Access*, *11*, 90916–90938. https://doi.org/10.1109/access.2023.3308298

Nicolas, K., Wang, Y., Giakos, G., Wei, B., & Shen, H. (2021). Blockchain System Defensive Overview for Double-Spend and Selfish Mining Attacks: A Systematic Approach. *IEEE Access*, *9*, 3838–3857. https://doi.org/10.1109/access.2020.3047365

Ojewale, O. (2023). Theorising and illustrating plural policing models in countering armed banditry as hybrid terrorism in northwest Nigeria. *Cogent Social Sciences*, *9*(1). https://doi.org/10.1080/23311886.2023.2174486

Ojo, J. S., Oyewole, S., & Aina, F. (2023). Forces of Terror: Armed Banditry and Insecurity in North-west Nigeria. *Democracy and Security*, *19*(4), 319–346. https://doi.org/10.1080/17419166.2023.2164924

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., . . . Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Parab, P., Patil, S., Patil, V., Patil, G., & Patil, R. (2025). Blockchain-Based Decentralized FIR Registration and Monitoring System: Enhancing Transparency and Security in Law Enforcement. *International Journal of Darshan Institute on Engineering Research and Emerging Technologies*. https://doi.org/10.32692/ijdi-eret/14.1.2025.2504

Park, Y., & Jeong, D. (2026). A blockchain-based digital evidence management system: Integrating forensic procedures and multi-party authorization. *Information Processing & Management*, *63*(5), 104654. https://doi.org/10.1016/J.IPM.2026.104654

Patel, D., Sanghvi, H., Jadav, N. K., Gupta, R., Tanwar, S., Florea, B. C., Taralunga, D. D., Altameem, A., Altameem, T., & Sharma, R. (2022). BlockCrime: Blockchain and deep learning-based collaborative intelligence framework to detect malicious activities for public safety. Mathematics, 10(17), 3195. https://doi.org/10.3390/math10173195

Rathod, T., Jadav, N., Tanwar, S., Sharma, R., Tolba, A., Răboacă, M., Verdes, M., & Said, W. (2023). Blockchain-Driven Intelligent Scheme for IoT-Based Public Safety System beyond 5G Networks. *Sensors*, *23*. https://doi.org/10.3390/s23020969

Rey, W. P. (2024). An empirical study on the usability of Melden: A crowdsourcing-based mobile crime reporting application using the PACMAD model. In 2024 8th International Conference on Communication and Information Systems (ICCIS). IEEE. https://doi.org/10.1109/ICCIS63642.2024.10779432

Riesco, R., Larriva-Novo, X., & Villagra, V. A. (2020). Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information. *Telecommunication Systems*, *73*(2), 259–288. https://doi.org/10.1007/s11235-019-00613-4

Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., Bukhari, W. A., & Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. *PLoS ONE*, *17*. https://doi.org/10.1371/journal.pone.0266462

Saxena, R., Gayathri, E., & Kumari, L. S. (2023). Semantic analysis of blockchain intelligence with proposed agenda for future issues. *International Journal of System Assurance Engineering and Management*, *14*, 34–54. https://doi.org/10.1007/s13198-023-01862-y

Siam, M. K., Saha, B., Hasan, M., Faruk, M. J. H., Anjum, N., Tahora, S., Siddika, A., & Shahriar, H. (2025). Securing Decentralized Ecosystems: A Comprehensive Systematic Review of Blockchain Vulnerabilities, Attacks, and Countermeasures and Mitigation Strategies. *Future Internet*, *17*, 183. https://doi.org/10.3390/fi17040183

Son, D., Manh, B. D., Khoa, T. V., Trung, N., Hoang, D., Hoang, T.-M., Alem, Y., & Minh, L. Q. (2024). Semi-Supervised Learning for Anomaly Detection in Blockchain-Based Supply Chains. *2024 23rd International Symposium on Communications and Information Technologies (ISCIT)*, 140–145. https://doi.org/10.1109/iscit63075.2024.10793673

Tolah, A. (2025). BlockIntelChain: a blockchain-based cyber threat intelligence sharing architecture. *Scientific Reports*, *15*. https://doi.org/10.1038/s41598-025-29152-6

Zhang, X., & Miao, X. (2021). A Reputation-based Approach using Consortium Blockchain for Cyber Threat Intelligence Sharing. *ArXiv*, *abs/2107.06662*. https://doi.org/10.1155/2022/7760509

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, *6*(2), 1594–1605. https://doi.org/10.1109/JIOT.2018.2847705

Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors*, *23*. https://doi.org/10.3390/s23020788