Mapping Deep Learning to Blockchain Security: A Survey

Vanessa Ortiz[†,*], Alexandria Bates[‡,*], Gaby G. Dagher[♮], Jun Zhuang[♮], and Tim Andersen[♮]
[†]Montclair State University, [‡]The Pennsylvania State University
[♮]Boise State University
[†]vegavegav1@montclair.edu,[‡]atb5640@psu.edu,
[♮]{gabydagher, junzhuang, tandersen}@boisestate.edu

ABSTRACT

This survey explores how specific artificial neural networks (such as GNNs, CNNs, RNNs, LSTMs, GANs, Transformers, MLPs, and hybrid models) have been applied to secure blockchain systems. Blockchain technology continues to expand across various fields due to its decentralized, tamper-resistant qualities. However, several concerns have been raised since they are more vulnerable to real-time threats and attacks. Deep learning, a branch of artificial intelligence (AI), presents itself as a promising solution for enhancing blockchain security due to its ability to learn from complex datasets. We categorize current research by neural network type, the application domain of the model, applied blockchain layers, security/privacy, and attack/defense, and identify existing patterns, challenges, and research gaps. Several conclusions include data scarcity issues, latency, and limited deployment across all blockchain layers (such as the consensus layer and hardware layer). After studying and comparing several existing surveys, we provide a unique contribution by explaining deep learning techniques specifically tailored for blockchain security, which enables us to highlight numerous opportunities for future researchers to address current limitations, such as scalability and privacy.

1. INTRODUCTION

Blockchain technology is currently quite prominent in both academic and industrial fields, such as healthcare [53; 40; 67], financial services [51; 69], smart contracts [13; 41; 32], and many other areas. These areas exploit its unique strengths, such as data immutability and its tamper-resistant nature [4; 15; 9]. Despite the wide range of strengths offered by blockchain technology, these systems are still susceptible to security threats and anomaly attacks [12; 32]. As blockchain technology continues to scale up in size and become more complex, security systems struggle to meet real-time demands [8; 25]. Real-time threat detection is necessary for these systems to accurately handle threats and anomalies that attempt to compromise sensitive data [25; 38], which blockchain technology is struggling to match.

Deep learning, a subset of machine learning, is an emerging technology that could potentially address the previously mentioned issues with blockchain systems [33; 26]. Its ability to learn from large-scale data and adapt to distinctive environments could properly address issues found with blockchain security, allowing new paths for researchers hoping to improve blockchain security and privacy. Various neural network architectures have demonstrated capabilities in strengthening blockchain systems, such as Graph Neural Networks (GNNs) [25; 14; 32; 30; 12; 42; 57; 33; 54; 11; 56], Convolutional Neural Networks (CNNs) [26; 69; 7; 31; 5], Long Short-Term Memory Networks (LSTMs) [4; 39; 13; 50; 41; 37; 9], and transformers [40; 8; 1; 16; 36]. Models that utilize neural networks can provide contributions towards security (e.g., anomaly detection and threat mitigation) and privacy (e.g., decentralized data protection) [39; 57]. The functionality of deep learning for security and privacy heavily depends on model type, data availability, and the applied blockchain layer(s). Therefore, we clearly classify and analyze each paper that discusses deep learning for blockchain security (DL4BCS) to properly demonstrate which characteristics existing research has. This survey will also state the neural network(s) utilized in an article, along with what blockchain layer(s) the system employs. We also go in-depth on whether a study features a system with build specifications meant to defend from threats, or to attack threats. Finally, we clearly state an application domain for each paper, showcasing how each researcher would apply their system in real-world conditions.

To explore the intersection of deep learning for blockchain security (DL4BCS), this survey paper explores current research that focuses on the potential this field could provide. Our goal is to address the following research questions:

RQ1. How has deep learning been used to address existing blockchain-related security concerns?

RQ2. How do different types of neural networks contribute to blockchain security?

RQ3. What are the main similarities and gaps found in Deep Learning for Blockchain Security between different neural networks?

RQ4. What potential research directions could we provide for DL4BCS-related studies?

Based on these questions, there is a clear focus on how deep learning can impact blockchain security, which provides a specific scope for our research. This survey will provide an in-depth analysis and categorization of current research that discusses this specific topic. Any papers that discuss alternative, yet similar topics, such as large language models (LLMs) for blockchain, or machine learning for blockchain,

[*]First two authors contributed equally to this work.

Table 1: **Overview of Existing Related Surveys.** Based on our stated search criteria in Section 3, we found and compared related surveys about blockchain technology and machine learning from various perspectives, such as whether the survey is machine learning for blockchain or vice versa (with a specific focus on LLMs or deep learning). We also categorize whether a paper discusses security, architecture-based analysis, and future research. This table provides a visualization of whether (i) papers focus on using artificial intelligence for blockchain or the other way around, (ii) a survey discusses LLMs or deep learning, (iii) a paper addresses a model that applies to security, (iv) a paper provides definitions and specifics for various neural networks, and (v) a paper provides researchers several potential research directions for DL4BCS based on existing research. We denote ●, ◐, and ○ as a full, partial, and no discussion of the corresponding items.

Source	**ML for BC**		**BC for ML**		**Security**	**Architecture-based** *Analysis*	**Future Research Directions**
	LLM	*DL**	*LLM*	*DL**			
Ressi et al. 2024 [48]	◐	●	○	◐	●	○	●
He et al. 2024 [27]	●	○	○	○	●	○	●
Zhang et al. 2020 [73]	○	●	○	◐	◐	○	◐
Ural and Yoshigoe 2023 [63]	○	○	○	●	◐	○	●
Shafay et al. 2022 [55]	○	◐	○	●	◐	○	●
Geren et al. 2025 [21]	○	○	●	○	●	○	●
Ortiz et al. 2025 (This Survey)	○	●	○	○	●	●	●

* DL refers to deep learning techniques with the exception of LLMs.

or even blockchain for deep learning, are notably not included in our scope, as we aim to discuss purely how deep learning could potentially improve blockchain security. Although we don't provide an in-depth analysis of articles within these alternative research fields, we will later discuss several surveys that focus on these alternatives.

In order to properly distinguish our review from other similar existing surveys that discuss artificial intelligence (AI) and blockchain, we provide an in-depth comparison of several reviews in this field. Ressi et al. [48] provide a general review on how integrating AI and blockchain can maximize blockchain technology to its full potential, opening doors to many real-world applications. He et al. [27] focus specifically on how LLMs can improve blockchain security. Although similar to DL4BCS, LLMs are a specific deep learning model trained to generate and understand human text. Therefore, this survey focuses on how LLMs can improve blockchain security purely from pre-trained data. Zhang et al. [73] inspect blockchain and deep learning simultaneously, discussing how security can apply to certain systems without including it within its general scope. Ural and Yoshigoe [63] wrote their survey on how blockchain can enhance machine learning, which is notably the complete opposite of He et al. [27]. In a similar manner, Geren et al. [21] discuss how blockchain can be used for LLM in a security and safety aspect unlike He et al. [27] (with the additional range of discussing safety). Shafay et al. [55] discuss how blockchain can be integrated with deep learning in hopes of improving deep learning overall. Notably, this survey serves as the opposite of DL4BCS with an included area of focus for security.

To summarize, existing surveys focus on how AI can be used for blockchain (or vice versa). However, there are existing gaps on how deep learning could be used to improve upon blockchain security. To further close this gap, we provide a summary of distinctions between this survey and other existing reviews in Table 1. From this table, we can see that our survey paper features a unique contribution showcasing an architecture-based analysis for various neural networks. We provide our review **contributions** and highlight the specific impacts to answer our research questions as follows:

1. We first properly define blockchain and deep learning in Section 2 by examining technological history and presenting diagrams to explain deep learning and blockchain integration. We then provide a comprehensive literature review within Section 4. We provide detailed definitions and collected resources from each paper to provide a proper in-depth understanding of current research. This section is split into several subsections, each focusing on a specific neural network. We deliver insights within these research projects, providing in-depth explanations on how each study focuses on DL4BCS. This review provides explanations on how researchers choose to integrate deep learning and blockchain, and how researchers could continue to improve this area of study in the future [**RQ1**] [**RQ2**] [**RQ3**] [**RQ4**].
2. We provide several tables for each paper in our methodology, categorized by different deep learning architectures. We specify whether each article discusses security/privacy and attack/defense. We also clearly state an application domain alongside a clear distinction of which blockchain layer(s) are used for the proposed model. For instance, Table 3 focuses on Graph Neural Network Papers, Table 4 discusses Convolutional Neural Network Papers, and so on up to Table 9, which discusses Hybrid Papers. With these tables, we clearly show how deep learning currently addresses blockchain security concerns [**RQ1**] [**RQ3**]. We also present clear similarities and differences between each neural network in current DL4BCS research, which ultimately provides general research directions for each neural network [**RQ2**] [**RQ4**].
3. We highlight specific papers within DL4BCS research by presenting diagrams that accurately reflect models discussed by researchers. For GNNs, we created Figure 3

to display and highlight Cai et al. [11]. For Generative Adversarial Networks (GANs), we created Figure 4 to display the system created in Rabieinejad et al. [45]. Finally, for Hybrid Networks, we created Figure 5 to exhibit the system provided in Saveetha et al. [51]. We chose to present diagrams for these papers due to their strong explanations on how specific neural networks have directly affected blockchain security in some way [**RQ1**] [**RQ2**]. These diagrams also provide a visual demonstration of how certain systems and models can be similar and/or different, even when using different neural networks [**RQ3**]. These similar and different traits can be further elaborated into potential research directions, which will be discussed within this review [**RQ4**].

The remaining sections of this paper are organized in this manner: In Section 2, we provide a clear background of blockchain technology and deep learning. We also define and explain the neural networks included in our methodology, and provide a history as to how these neural networks came to be. We propose a visualization of the layers of blockchain in Figure 1, and provide a taxonomy in Figure 2 that shows how various layers and neural networks can integrate for various application domains. In Section 3, we explain our methodology, clearly stating what criteria we followed and stating how we searched for articles that discuss DL4BCS. In Section 4, we provide an analysis for each article included in our methodology. To go in-depth on certain models within existing research, we also provide diagrams to highlight several key uses for deep learning and blockchain integration. To summarize every paper included in our methodology, we provide tables for each neural network to clearly show similarities and differences between each paper and neural network. In Section 5, we address challenges that currently impact researchers when integrating deep learning and blockchain together, which overall hinders research advancements. In Section 6, we discuss potential research directions within the field of DL4BCS. Finally, in Section 7, we sum up our review of the literature on current research on DL4BCS.

2. BACKGROUND

The application of deep learning to blockchain technology has created new opportunities for cybersecurity, automation, and decentralized intelligence. In order to understand how these technologies come together, it is important to study their foundations. This section introduces blockchain technology, going in-depth on its origin and how it operates. We will also explore the fundamentals of deep learning, including how neural networks function and how they learn from data. We then discuss key neural networks commonly used with blockchain technology, focusing on their design, capabilities, and original contributions. Together, these foundations give context for the applications and challenges discussed in this paper.

2.1 Blockchain

Blockchain is a type of digital ledger technology that allows secure and transparent transactions across distributed networks, making it a unique technology. It first appeared back in 2008 when Satoshi Nakamoto introduced the concept in "Bitcoin: A Peer to Peer Electronic Cash System." [43]. Nakamoto describes a decentralized mechanism that uses Proof-of-Work (PoW) to validate blocks of transactions. PoW is made up of complex cryptographic puzzles that are solved by network participants, who are typically referred to as miners. This method ensures that each block has a time stamp and is tamper resistant. By introducing the element of tamper-resistance, this prevents users from double-spending and removes the need for a third party.

Blockchain consists of different layers, with each layer contributing specific part in the systems functionality and security, as shown in Figure 1. The very base layer is the data layer, which is responsible for data organization and management, including nodes and underlying data storage technology [61; 60]. Above the data layer is the network layer, which handles peer-to-peer protocols and block distribution across the network [60]. Next is the consensus layer, which implements algorithms such as PoW or Proof-of-Stake (PoS). This layer is extremely important, as it ensures that all participants in the network agree on one single source of truth [60]. On top of the consensus layer, we find the hardware layer. This is where transaction logic is executed and where the general state of blockchain is maintained [29]. Next, the contract layer allows programmable logic in the form of smart contracts and enabling decentralized applications, which is often found in platforms like Ethereum [60]. It is important to note that we didn't include the contract layer within our blockchain layer classification for each paper throughout this survey due to this layer not having particularly unique traits in comparison to other layers. The top layer of blockchain is called the application layer, which includes end-user interfaces and tools such as wallets and trading platforms. These interfaces are able to directly interact with smart contracts and the underlying network [29; 60].

In 2014, blockchain technology was expanded by Vitalik Buterin in "Ethereum: A Next Generation Smart Contract and Decentralized Application Platform" [10]. Ethereum

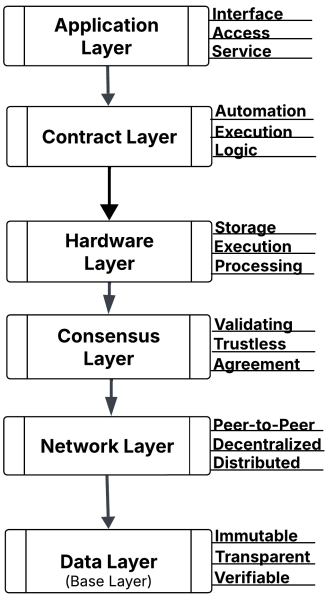

Figure 1: Blockchain layers and their corresponding key functionality.

builds on several elements of Bitcoin's blockchain architecture while introducing the concept of *smart contracts*. Smart contracts are programmable scripts that execute automatically under predefined conditions within the Ethereum Virtual Machine (EVM). This allows blockchain to support rich decentralized applications and transform them into programmable ecosystems. As a result, they're able to execute financial contracts, apply to supply chain coordination, and improve autonomous digital services.

2.2 Deep Learning

Deep learning is a powerful part of artificial intelligence. It is centered on layered networks made up of simple computation units, which are defined as neurons. Each neuron multiplies inputs by learned weights, adds a bias, and applies a nonlinear activation. After the activation is completed, it passes the result forward. An example of a neural network is the Multilayer Perceptron (MLP). MLP is a model where neurons come together and are arranged in fully connected layers. An MLP with a single hidden layer can approximate any continuous function, which has been demonstrated to show theoretical potential by Cybenko [17].

However, as research increased on neural networks, it became clear that there was a need to analyze images efficiently. As a result, Convultional Neural Networks (CNNs) were introduced by LeCun et al. [34]. The CNN architecture uses convolutional filters and layers to learn spatial feature hierarchies in an automatic form. This achieves high-level performance when it comes to recognizing handwriting and digits. Having this neural network facilitates the recognition of classic zip code datasets with minimal need for manual preprocessing.

Some problems were discovered with respect to time dependent data. To help mitigate this issue, Recurrent Neural Networks (RNNs) were developed in 1990 by Elman [20]. RNNs allowed information retention through hidden-state representation, which resulted in trouble modeling long-term dependencies. To mitigate this situation and create a potential solution, Hochreiter and Schmidhuber came up with a new neural network called Long Short-Term Memory (LSTM) in 1997 [28]. LSTMs use input, output, and logic gates to control how data flows through memory cells. This allows for effective modeling of time series data as well as long dependencies.

In blockchain transaction networks, graph-structured data is very common. However, this type of data requires a very specialized model. Gori, Monfardini, and Scarselli introduced Graph Neural Networks (GNNs) to serve as a solution [24]. In GNNs, neurons spread information along edges of the graph and update node states iteratively, allowing relational learning. In 2014, Generative Adversarial Network (GANs) were introduced by Goodfellow et al. [23]. GANs are made up of a generator (which creates synthetic data) and a discriminator (which learns to differentiate real from fake). This process provides realistic data and supports certain applications, such as transaction simulations. In the beginning, neural networks relied on sequential processing. This changed when transformers were introduced in 2017 by Vaswani et al. [64]. Transformers have the ability to analyze data by evaluating dependencies between all elements in a sequence simultaneously. This allows for much faster computation as well as high-level performance when it comes to language and log analysis.

These neural networks serve as essential tools in blockchain analytics and cybersecurity. The potential of these neural networks is extensive in terms of improving blockchain technology. GNNs are able to detect illegal transaction patterns by learning relational flows. CNNs can process visualized data and flag anomalies. RNNs, LSTMs, and transformers are very effective for modeling behaviors over time, auditing logs, and auditing contract code. Finally, GANs are able to generate synthetic blockchain data to improve detection systems. In summary, deep learning models have the potential to make blockchain's immutable system much stronger for fraud detection, automated audits, and smart contract-based attack detection systems. We equip researchers with a visual taxonomy of how blockchain layers and specific domains currently apply to existing DL4BCS based on various deep learning architectures in Figure 2. It is also quite common to see multiple deep learning architectures within one singular system, which are referred to as hybrid models. We provide a complete comparison table on the various neural networks reviewed within this survey in Table 2.

3. RESEARCH METHODOLOGY

Our ability to properly discuss how deep learning can be used for blockchain technology requires a proper exploration of the existing literature related to the subject. Before gathering articles, we first had to come up with a feasible method to ensure that the paper is related to deep learning for blockchain rather than blockchain for deep learning. We also had to create an organizational method to differentiate the scope of these papers. In order to correctly identify scopes and keep current research organized, we used a variety of tables, charts, keywords, and other techniques.

3.1 Literature Search and Strategy

Our primary search tool was Google Scholar, supplemented with searches on IEEE Xplore. We used Boolean logic (such as 'AND', 'OR') within our searches to ensure certain keywords were included. We also tested combinations of relevant model names and concepts, including 'CNN blockchain', 'GNN blockchain', 'LSTM security', and so on. Ultimately, we searched for specific neural networks while including other relevant keywords, such as 'blockchain', 'security', or 'ledger'. We also chose to use a variety of phrases like 'neural networks for blockchain', 'deep learning for blockchain', 'deep learning for blockchain privacy', and 'deep learning in relation to blockchain security'. We then verified that each paper described deep learning for blockchain and not vice versa by reading the abstract, introduction, and background sections of each paper.

3.2 Paper Organization and Categorization

To manage and analyze the articles, we created a system of folders named after each neural network model that were widely used to protect blockchains. As a result, we had eight folders for eight different deep learning architectures: 'CNN'. 'GAN', 'GNN', 'LSTM', 'MLP', 'RNN', 'Transformers', and 'Hybrid'. This allowed us to group the papers by architecture to compare their blockchain-related applications.

We also used tables in Google Sheets to catalog papers, track citation information, identify common methodologies,

	GNN	CNN	GAN	LSTM	MLP	RNN	Transformer
Data Type	Graph	Image/Grid	Various (Synthetic Generation)	Time Series	Structured	Time Series/ Text	Text Sequence
Strength	Understanding Connections between Nodes	Finding Patterns (Shapes)	Making realistic new examples	Remembering Long-Term Patterns	General Tasks	Learning Recent Steps	Handles Full context fast
Limitation	Slow with big network	Not good with time or sequence data	Hard to train/ Unstable	Slow and Complex	Not great for images or sequences	Forgets older steps (Short Term Memory)	Needs substantial data and computing power

Table 2: Neural Network Comparison Table: This table displays the core characteristics of common neural networks, highlighting input data types, strengths, and limitations.

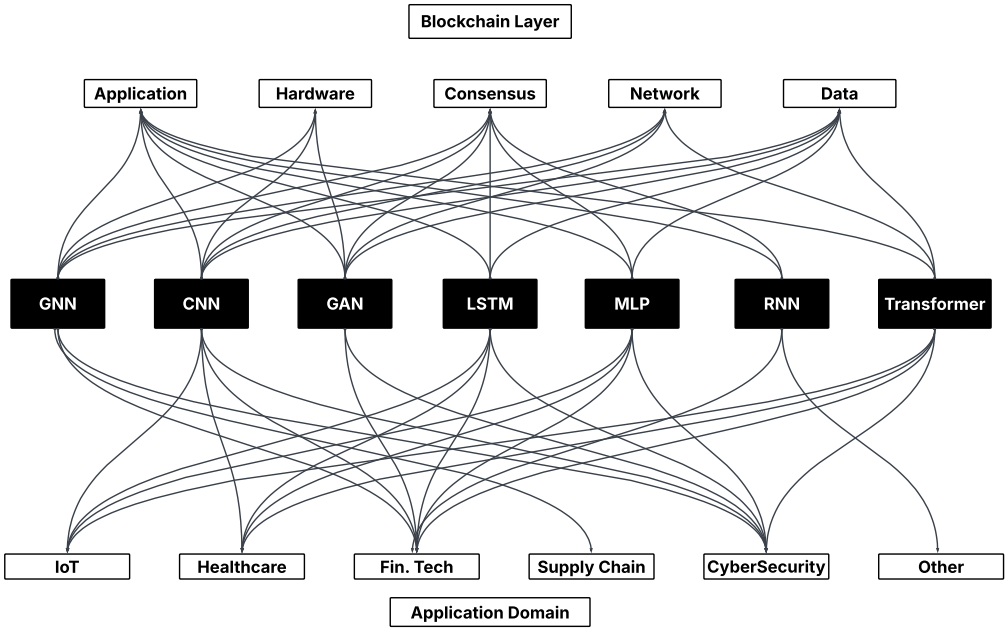

Figure 2: Blockchain and Deep Learning Taxonomy: This taxonomy illustrates the relationship between neural network models and their applications across multiple domain applications (including healthcare, IoT, supply chain, and cybersecurity). It highlights the versatility of individual neural network architectures, demonstrating their capacity to support multiple application areas. Additionally, the diagram reveals how these models interact with different layers of the blockchain, offering insight into their functional integration. The taxonomy also exposes current gaps and deficits within both application domains and blockchain layers, suggesting areas for further research and development.

and note key distinctions. Each entry in the table included model type, blockchain domain, privacy versus security, evaluation strategies, and publication metadata. To differentiate between security-focused and privacy-focused papers, we manually scanned abstracts and full texts for relevant keywords. For example, we classified a paper as security-based if it included keywords and phrases such as 'intrusion detection', 'fraud', 'DDoS attacks', and 'vulnerability'. For privacy, however, we searched for privacy-based indicators such as 'de-anonymization', 'metadata leakage', and 'differential privacy'. This tagging process allowed us to categorize papers and facilitate downstream gap analysis. Our completed table with every research paper we have gathered was a useful tool for finding the most common trends (such as models frequently used for specific blockchain tasks, and highlighting areas with a lack of coverage). It is important to note that although our exact tables from Google Sheets is not presented in this survey, we have replicated our tables for each specific neural network throughout various neural network sections in Section 4.

3.3 Inclusion and Exclusion Criteria

To ensure the quality and relevance of the reviewed material, we applied both inclusion and exclusion criteria. We included articles that applied deep learning models to meaningful blockchain-related challenges such as anomaly detection, smart contract analysis, and data privacy. We excluded papers that approached the topic from the opposite direction, meaning using blockchain to improve deep learning, and papers that lacked technical depth or clear experimental validation. We also omitted papers written in languages other than English, published before 2020, found in peer-to-peer review repositories, PhD submissions, or thesis-only documents. This filtering helped build a clear, high-quality set of papers for meaningful analysis.

3.4 Research Gaps and Limitations

In order to properly organize our findings, we identified clear trends and gaps across the literature we've gathered. GNNs, Transformers, and LSTM models appeared most frequently in blockchain applications. In contrast, RNNs were notably underrepresented, which shows an opportunity for further exploration. While several papers demonstrated promising simulation results, there was a distinct lack of studies on real-world use as well as a scarcity of standardized evaluation benchmarks, which limits comparability across various approaches. We also observed that certain blockchain domains, such as consensus mechanisms, permissioned networks, and decentralized identities, have received limited attention. This suggests several areas where deep learning could be further investigated.

However, our review has limitations. Papers were restricted to those published in English and after 2020, which may have excluded relevant earlier papers or non-English contributions. We also excluded PhD thesis documents and non-peer-reviewed materials, which may have eliminated some emerging or experimental approaches. All combined findings in our methodology highlight the progress and blind spots in current research, serving as a foundation to identify promising directions for future work.

4. EXISTING LITERATURE REVIEW

This section reviews current literature on deep learning for blockchain security (DL4BCS). The studies are categorized in several ways, such as the neural network architecture, similarities and differences, the application domain(s) discussed, datasets used, and any other technical focuses. We also discuss any revealing patterns along with gaps in the methodology, both for each individual neural network and as a whole. Notably, a small number of papers throughout this analysis also apply to privacy. Since privacy is the minority within existing research, we go in-depth on explaining key distinctions on privacy-based research compared to security-based research.

4.1 Graph Neural Networks (GNNs)

Recently, Graph Neural Networks (GNNs) have become one of the most promising architectures for analyzing blockchain systems due to their ability to model complex data structures in blockchain systems. This can include address graphs, protocol interactions, and transaction flows.

Graph neural networks have also evolved into specialized architectures to handle more complex graphs. Primary examples of this evolution include heterogeneous GNNs and temporal GNNs. Heterogeneous GNNs are designed for graphs that contain multiple types of nodes or edges [68]. This type of GNN is particularly useful for applications such as social networks, citation graphs, and fraud detection. In a blockchain-based identity verification system, the interaction between users, devices, and smart contracts forms a heterogeneous graph structure.

On the other hand, temporal GNNs are suited for dynamic graphs where the relationship between entities evolves over time [49]. These models incorporate time-stamped edge events and are designed to capture both structural and temporal dependencies. Temporal GNNs are especially effective in applications like real-time fraud detection, blockchain transaction forecasting, and cyberattack monitoring. For these applications, the sequence and timing of events matter as much as the connections themselves. For instance, in a blockchain ledger, transaction history over time can be modeled as a temporal graph to detect anomalous patterns.

Within current DL4BCS research, many researchers take advantage of GNNs to detect anomalies in transaction networks [30]. For instance, [25] suggests a spatial-temporal GNN model that uses time series behavior of addresses to identify suspicious cryptocurrency transactions. Additionally, [14] discusses a multi-distance message passing approach to capture the temporal and relational distance between transactions in a more accurate form. By implementing these temporal dynamics methods into the graph structure, the accuracy of fraud detection in blockchain improves. To continue, [56] created a dual-level GNN framework. This dual-level network analyzes account behavior and transaction graph features to detect anomalies. This reflects the importance of hierarchical representations when it comes to modeling a blockchain ecosystem. A paper that dives deep into this concept is [11], which integrates GNN and blockchain, showing its potential in analysis and smart ledger architecture. This paper is particularly groundbreaking because it discusses an end-to-end integration of GNNs into blockchain.

While other papers limit GNNs to auxiliary analytical tasks such as fraud detection, GTxChain [11] discusses an enhanced block structure and a new consensus protocol that uses graph representations of transactions directly in block validation and the decision-making process. This model builds a diverse transaction graph where nodes represent accounts and smart contracts. Edges also encrypt transaction types, temporal order, and value flow. This system uses a multi-relational GNN with hierarchical attention mechanisms, allowing it to learn contextual embeddings for nodes that reflect both local behaviors and global structural dependencies. This embedding procedure is used in consensus voting, allowing the system to prioritize blocks that have higher behavioral legitimacy scores. As a result, this reduces the acceptance of malicious transactions. GTxChain also discusses a graph-based Proof-of-Learning (PoL) mechanism. This mechanism replaces regular Proof-of-Work (PoW) or stake-based validation by using a trusted weighted GNN classification task. Through the experiment in [11], the results show that GTxChain outperforms existing consensus protocols both in security and efficiency. Not only does it stay low-latency, but it also reduces the spreading of anomalous transactions. By implanting intelligence into the blockchain, this adaptive, self-aware ledger system constantly learns from transactional behavior. Due to the high significance this paper holds in DL4BCS research, we provide Figure 3, which provides a visual explanation of how GTxChain works.

Current research is often focused on security applications. For instance, Chang et al. [12] and Jeyakumar et al. [30] mention using message-passing networks to identify nodes or transactions with abnormal patterns. Because of this, it is possible to secure blockchain from threats like sybil attacks or illicit fund flows. While most papers focused on security, there were a select few that focused on privacy. For example, Shen et al. [57] expose privacy risks through the process of applying GNN-based deanonymization techniques. These techniques show that address clustering can

reveal user identities, which is a concern for platforms like Bitcoin.

Next, MuhsnHasan et al. [42] use graph-based modeling and apply it to logistics and origin verification, demonstrating its real-world use outside of finance. Additionally, [54] show a new transaction fingerprinting system, which provides insights into behavioral modeling of blockchain participants. One consistent pattern found is the usage of directed or temporal graphs that mirror transaction flows and account behavior. Models seem to vary in their graph construction and temporal encoding. Some papers focused on utilizing blockchain statistic snapshots, while others use temporal features with edge time stamps or sequence-based modeling.

In summary, GNN has shown high efficacy for blockchain transaction modeling, fraud detection, identity inference, and protocol optimization. The adaptability GNN offers to graph-structured data makes it well-suited for blockchain analysis. Future research should prioritize explainability, real-time deployment, and integration into production-level blockchain systems. To provide a visual culmination of our analyzed research, we provide Table 3, which showcases how each paper distinctively falls under various categories we've previously discussed.

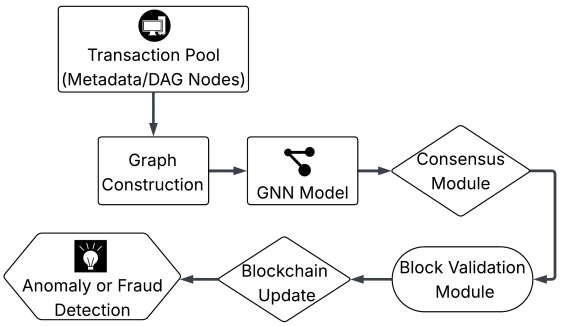

Figure 3: GTxChain [11] is a blockchain system powered by Graph Neural Networks (GNNs). The central focus of the system is the use of GNN, which means the method can learn patterns from both on-chain and off-chain transaction data. Off-chain data includes user behavior or external triggers, which is processed through the Lightning Network. This enables fast and scalable microtransactions that eventually interact with Directed Acyclic Graph (DAG) nodes representing the on-chain structure. GNN receives input from DAG nodes as well as metadata from a decentralized file storage system and off-chain streams. This allows the system to form a comprehensive graph of transactional relationships and behaviors. The GNN generates intelligent node encodings, which are compact representations that capture both who is transacting and how they behave over time. These encodings add to a graph-aware consensus mechanism, which uses them to assess how legitimate the blocks or transactions are before adding to the blockchain. This entire process reduces fraud, detects anomalies, and makes sure that only trusted data is validated. GTxChain represents a blockchain that doesn't just record transactions but also learns from them to improve security, efficiency, and trust.

4.2 Convolutional Neural Networks (CNNs)

Although traditional uses of Convolutional Neural Networks (CNNs) include image and pattern recognition, they have begun to be adapted for blockchain to reshape data into structured matrices or visual representations. CNNs are quite useful due to their ability to learn spatial hierarchies and detect subtle patterns. This makes them suitable for transaction pattern recognition [69], biometric verification [7], and fraud detection [26].

Various studies in current existing research use CNNs to operate on transaction data. For example, Hasan et al. [26] discuss the idea of converting blockchain transaction logs into two-dimensional matrices that mimic grayscale images, allowing the CNN-based system to detect fraudulent behavior through visual spatial analysis. Jones et al. [31] examine the use of CNNs to classify secure and malicious behavior. This is done by encoding the behavioral features of blockchain nodes into maps that can be interpreted by CNN filters.

CNNs can be seen within various domains throughout blockchain technology. A specific example would include biometric security. Asem et al. [7] suggest using a CNN-based architecture that can process biometric inputs, such as fingerprint and facial data. This experimental process provided both high-accuracy classification and tamper-proof audit trails.

Healthcare systems are another common domain where CNN applications stand out, specifically for preserving privacy. As an example, Alzubi et al. [5] place CNNs in federated learning platforms, allowing patient health data to remain on local devices. The CNN model learns from local data and contributes to the decentralized blockchain model without exposing raw information. This method combines privacy preservation with high performance, specifically for both disease classification and anomaly detection.

Other studies focused on CNN with the intention of improving temporal and contextual awareness. For instance, Wang et al. [69] merge CNN-based extraction with transformer-based temporal attention. This method gives better anomaly detection in blockchain transactions by encrypting spatial local patterns via CNN, along with sequence-level dependencies via a transformer. This solves the common weakness of CNNs when it comes to modeling long-term dependencies.

Principally, all CNN-based models focus on spatial pattern recognition in some way. Most methods convert blockchain data into structured formats like matrices and tensors. These are then passed through convolutional filters to extract features, making CNNs effective for spotting recurring patterns or anomalies.

CNN methods also have differences, including the input preprocessing methods and model architecture. Some models rely on spatial input formats, such as biometric and health records, while others rely on artificially structured transactional data. Some studies use CNN in isolation, while others use a more hybrid approach to make up for their temporal limitations.

Throughout this review, several gaps are noticeable due to pre-existing challenges in standardizing how blockchain data is formatted for spatial learning, specifically for CNNs. There is not much consistency in how transactional data is converted into image-like structures, which limits cross-study comparisons. The lack of interpretability also remains a concern, resulting in a lack of research on how CNN maps contribute to decision-making in blockchain contexts. There is also limited evidence of CNN usage in lower blockchain

Table 3: **Graph Neural Network Papers.** This table summarizes every gathered paper discussing deep learning for blockchain security (DL4BCS), specifically for GNNs.

Citation	Priv./Secur.	Att./Def.	Application Domain	Blockchain Layer(s)
[25]	Security	Defense	Crypto-based blockchain for fraud detection	Application, Data, Hardware
[14]	Security	Defense	Crypto-based blockchain for anomaly detection	Application, Data, Hardware
[32]	Security	Defense	Crypto-based blockchain for smart contract vulnerability detection	Application, Data
[30]	Security	Defense	Crypto-based blockchain for malicious transaction detections	Application, Data
[12]	Security	Defense	Crypto-based blockchain for anomalous node detection	Application, Data
[42]	Security	Defense	Anomaly detection for supply chain blockchains	Application, Data
[57]	Privacy	Attack	Crypto-based blockchain for identity inference and entity clustering	Application, Data
[33]	Security	Defense	Crypto-based blockchain for fraud detection	Application, Data, Hardware
[54]	Security	Attack	Crypto-based blockchain for monitoring encrypted network traffic	Application, Data
[11]	Both	Defense	Intrusion detection using smart blockchain	Application, Consensus, Data
[56]	Security	Defense	Crypto-based blockchain for anomaly detection	Application, Data

layers like consensus and network, while the most commonly studied layers have been the application and data layer. CNNs are currently applied at the application and data layers within research, specifically where privacy, pattern recognition, and classification tasks are dominant. In hybrid systems, CNNs function as the initial feature extractor. It feeds processed data into sequential models for enhanced context modeling. We continue our discussion of the prominence of CNN-based architectures in Section 4.5. We also provide an in-depth summary of all the papers surveyed on integrating CNNs and blockchain in Table 4.

In conclusion, CNNs are a versatile tool for blockchain security and privacy research. The fact that CNNs can adapt to non-image data shows potential for innovation, but standardized preprocessing protocols and interpretability frameworks are necessary for improved use in other areas. The real-world validation of CNN models for blockchain technology is an area that could be explored more in-depth in the future.

4.3 Generative Adversarial Networks (GANs)

Generative Adversarial Networks (GANs) offer a transformative approach to blockchain security and privacy. GANs offer the most opportunities in augmenting datasets, simulating adversarial behavior, and generating synthetic data to test detection models. Since high-quality labeled blockchain data can be hard to retrieve (especially when it comes to fraud and attack scenarios), GANs feature a solution for gaining data that can benefit the stress-testing of a system. A GAN includes a generator (which can create synthetic data) and a discriminator (which differentiates between real and generated data). As the generator and discriminator interact, realistic data is continuously generated. The relationship between the generator and the discriminator allows for continuous improvement in relation to a vast variety of blockchain applications, especially for security purposes.

A common application of GANs in relation to blockchain is anomaly detection. In Rawlins et al. [47], the overall concept features a lightweight GAN architecture that is designed for low-latency environments. A realistic example of this would be real-time fraud detection in blockchain-based transaction systems. The model proposes a balance between efficiency and performance, which makes it ideal for edge deployment while still maintaining high classification accuracy. Other researchers have taken a similar concept but used a more heavyweight approach. A particular example of this would be Pawar et al. [44], which uses a gradient penalty to ensure training stability and better quality. This paper focuses on high-impact attacks and demonstrates how Wasserstein improves convergence and robustness in terms of detecting adversarial patterns in complex transaction networks.

Another way GANs have been used in current research is to simulate cyberattacks on the blockchain infrastructure. In Rabieinejad et al. [45], the researchers propose a GAN-based detection model that focuses on identifying malicious patterns and threat indicators in Ethereum transaction graphs. This method uses adversarial mimicry, in which a generator produces synthetic attack samples with a discriminator that

Table 4: **Convolutional Neural Network Papers.** This table summarizes every gathered paper discussing deep learning for blockchain security (DL4BCS), specifically for CNNs.

Citation	Priv./Secur.	Att./Def.	Application Domain	Blockchain Layer(s)
[26]	Security	Defense	Fraud detection using blockchain	Application, Data
[69]	Security	Defense	Blockchain transaction classification system	Application, Data
[7]	Both	Defense	Biometric verification using private blockchains	Application, Data
[31]	Security	Defense	IoT security using IoT-based blockchain	Application, Consensus, Data, Network
[5]	Both	Defense	Secure model update logging using private blockchain	Application, Data, Hardware, Network

learns to differentiate them from safe transaction behavior. This refines its threat detection capability over successive iterations. Unlike static or rule-based approaches, this method allows for real-time adaptation to emerging zero-day threats. This paper mentions that their model outperforms the baseline classifiers when it comes to precision and recall. This is a perfect example of the benefits of GAN-generated training augmentation for blockchain cyber defense. They also discuss the ability of GANs to uncover hidden vulnerabilities in transaction patterns, which provides a tool to locate threats in permissionless environments. We provide a visual explanation of the two-phase deep learning architecture found in [45] in Figure 4.

In addition to [45], Lei et al. also use GANs to simulate attacks [35]. This paper presents a forensic framework that supports comprehensive model training and forensic auditing on blockchain. There exists additional research that uses GANs to discuss data privacy and biometric spoofing defense. For example, Ghani et al. [22] talk about how GANs can be used to simulate fake biometric data (and defend against it) using blockchain as an audit layer. This method highlights GAN-based applications and how they can simulate attacks as detailed as training systems to defend against them. The authors talk about using blockchain to provide traceability and trust in the data generation process, which would strengthen the security of biometric verification systems.

GANs can also be applied to improve the quality of data for blockchain logs. In particular, Qadear et al. [2] discuss GANs ability to complete incomplete blockchain transaction records. This method contributes to blockchain analytics in situations where data may be missing due to latency, corruption, or inconsistent formatting.

Another area of interest is the hardware and deployment perspective. In particular, Dirgantoro et al. [18] discuss a privacy-preserving data generation system designed for edge nodes in blockchain-hybrid Internet of Things (IoT) systems. The researchers mention how GANs can generate synthetic sensor data while maintaining user privacy and reducing the need to rely on cloud infrastructure. This method features a federated or edge-distributed GAN-based architecture for privacy-conscious deployments.

With the many possibilities that GANs offer, there are still several gaps in existing research for DL4BCS. The lack of explainability in GAN-generated outputs includes weak reasoning for why synthetic samples improve detection. Another concern includes integrity evaluation. Since GAN models generate fake data, it is very important to develop strict metrics and validation frameworks to assess their fidelity, diversity, and impact on tasks. Most of these studies evaluate GANs on custom-built or non-public datasets, which hinders replication and benchmarking.

GAN-based models are also rarely applied to all blockchain layers. Most focus on the data and application layers, which typically aims at fraud detection or privacy enhancement. Very few studies mention the consensus layer or the network layer, although these layers have proven to be very important to blockchain security.

To summarize, GANs can be a powerful and flexible tool for blockchain research. GAN-based models allow synthetic data generation, adversarial simulation, and model enhancement, which can be used in fraud detection, biometric spoofing, threat modeling, and privacy-preserving data generation. However, there is much room for this field of study to evolve and become more interpretable, standardized, and reproducible. The use of GANs to improve blockchain security is incredibly promising for future research. We provide a visual, in-depth summary of all DL4BCS research articles collected that use GAN-based models in Table 5.

4.4 Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNNs)

Long short-term memory (LSTM) and other recurrent neural networks (RNNs) are prevalent neural networks that can be seen within a substantial amount of published papers. Both LSTM and RNN models excel in sequential data modeling for blockchain. A consistent theme is the use of time-series data, but models differ in memory span, bidirectionality, and hybridization. For instance, some researchers integrate RNNs with transformer encoders to improve context awareness. While LSTM models are versatile, gaps exist in adapting them for high-volume blockchain environments with low latency requirements. Also, a few studies validate their robustness against adversarial inputs. These models frequently engage the application, network, and consensus layers. Therefore, we can conclude that work is needed to bridge model complexity with real-time deployment feasibility.

Across the papers we have gathered specifically for LSTM models, there is a clear pattern in the type of blockchain

Table 5: **Generative Adversarial Network Papers.** This table summarizes every gathered paper discussing deep learning for blockchain security (DL4BCS), specifically for GANs.

Citation	Priv./Secur.	Att./Def.	Application Domain	Blockchain Layer(s)
[74]	Both	Defense	Blockchain to improve secure communications and access control	Application, Data
[45]	Security	Attack	Ethereum-based blockchain for cyber threat hunting	Application, Data
[18]	Security	Defense	Ethereum-based blockchain for smart security systems	Application, Data
[2]	Both	Attack	Data augmentation and anomaly detections using blockchain	Application, Data
[75]	Security	Attack	Data augmentation using bitcoin-based blockchain	Application, Data
[47]	Security	Defense	Crypto-based blockchain for fraud predictions	Application, Data
[22]	Both	Attack	Using private blockchains for authenticity and tamper resistance	Application, Data
[44]	Security	Defense	Smart contract based attack detection system	Application, Data
[35]	Security	Attack	Audit trails in network intrusion detection	Application, Data

used for a significant number of papers. Among the LSTM-based papers we refer to within this paper, half of these papers use IoT as the main focus for its blockchain type. Meanwhile, the other half of these papers discuss blockchain technology in general terms, and applies blockchain primarily as a decentralized ledger system. Our findings also allowed us to discover a singular paper that uses a mix of both IoT and smart contracts as its blockchain type, creating a very unique distinction and system compared to the other papers [41]. RNN-based studies decide to take an approach with a different type of blockchain, with one paper employing Proof-of-Authority (PoA) [65] and the other making use of cryptocurrency, with a focus of both Bitcoin and Ethereum [46]. From this, we can see that papers using RNN or LSTM architectures use blockchain in general terms or IoT as the primary focus, which allows room for more research using different types of blockchain, such as supply chain or even smart contracts.

It is important to clearly state that some researchers create models purely for security purposes, while others create systems that can be used for both security and privacy purposes. A distinctive paper in our search creates a system just for privacy using an LSTM model [39], making this paper extremely unique within these specific neural networks.

There is a special mix of how researchers choose to apply their concepts in real-world scenarios. For instance, several of these papers consist of solutions to improve or assist certain systems that require much more security and immutability. Some areas of focus would include healthcare due to patient-privacy laws (such as HIPAA) [13; 9], energy management [65], and mobile financial fraud detection systems [46]. Other papers focus more on data security as a whole, such as proper storage of IDS data [4] and improvements on Collaborative Intrusion Detection Systems (CIDS) [41].

Unlike how there is a special mix of applications of blockchain within each individual paper, each paper applies its system towards specific layers of blockchain, with no unique pattern. For instance, several papers that use RNN or LSTM architectures decide to apply to both the application layer and the consensus layer of blockchain. However, other existing research applies only to the application layer [41; 37] or the consensus layer [65].

If we were to introduce how the data layer applies to existing LSTM and RNN research for DL4BCS, it is crucial to note that current research that uses RNNs does not apply to the data layer at all. The cause of this could be related to the structure differences between RNNs and blockchain. RNNs focus on sequential data, while the data layer of blockchain handles data retrieval in a structured format. However, one model that uses LSTM applies in both the application and data layer of blockchain [37], while another uses the data layer only [13]. We can therefore conclude that LSTM-based models may provide more flexibility for researchers due to their ability to take advantage of several blockchain layers within one system.

There are several notable gaps that we can clearly state within DL4BCS, specifically for LSTM and RNN. As mentioned above, only one study refers to the use of deep learning for blockchain for privacy purposes [39]. Deep learning models require a substantial amount of data in order to properly train and learn effectively, which ultimately results in many privacy concerns. In order to address these privacy concerns, more research on integrating deep learning for blockchain should be considered. Based on the five layers of blockchain, we can also see that there was no usage of the network layer or hardware layer within these articles. The network layer is important to allow communication between nodes on a blockchain, and deep learning should absolutely be seen as a potential candidate to improve this communication system. The hardware layer of blockchain could be improved with deep learning, specifically with LSTM and

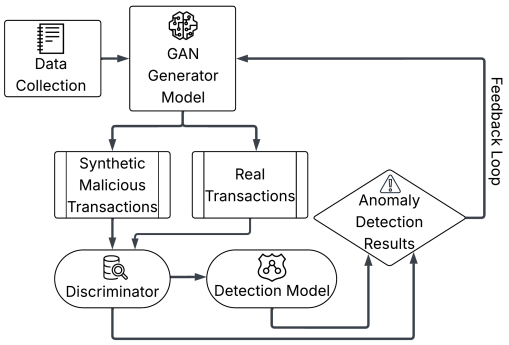

Figure 4: Generative Adversarial Networks for Cyber Threat Hunting in Ethereum Blockchain [45]. This diagram illustrates the two-phase deep learning architecture mentioned for adversarial threat detection in Ethereum blockchain networks. In phase one, real Ethereum transaction data is used to train a Conditional Tabular GAN (CTGAN). Once the data goes to the GAN generator, it uses the real transactions to create malicious synthetic transactions. Both real transactions and newly generated synthetic transactions then get sent off to the discriminator. The discriminator uses multiple iterations to improve its ability to detect fakes and simulate realistic adversarial activity. While still in the discriminator, both the synthetic and the real transactions get merged into a unified dataset. In phase two, the dataset is now sent off to a detection model called a bi-directional long short-term memory (BiLSTM) network. This detection model captures sequential patterns to accurately identify subtle adversarial behaviors. The system effectively detects malicious attacks during early phases of execution, which achieves a near-perfect accuracy in distinguishing malicious transactions from trustworthy transactions. To conclude, these results are then sent to the user.

RNN models, as the hardware layer allows for anomaly detection and enhancing security as well as privacy. Based on previous statements about gaps in Section 3.4, it is clear that RNNs are extremely underrepresented in comparison to LSTMs, which seems to be widely represented in existing DL4BCS research. As a visual summary, we provide Table 6 and Table 7, which shows existing research and how they fall under specific categories.

4.5 Multilayer Perceptrons (MLPs) and Hybrid Models

Multilayer Perceptrons (MLPs) are widely used in lightweight or hybrid blockchain architectures. These models serve as classification layers in federated learning systems or low-resource edge nodes. MLPs consistently act as the final decision layer in hybrid systems, typically following CNN or RNN-based feature extraction. Although MLPs often act as the final layer when it comes to hybrid systems, many of the hybrid-based articles that exist in current research for DL4BCS consist of many unique combinations of different neural networks. These combinations allow researchers to create extremely specific systems to solve problems and apply results to certain real-world applications. We will dive deep into how each paper classifies itself in terms of privacy or security and how each neural network is combined within these hybrid papers. The interaction of various deep learning architectures impacts the overall application of blockchain. Similar to previous sections, a table has been provided for both MLPs (Table 8) and hybrid models (Table 9) to assist readers with viewing similarities and gaps between our methodology for these architectures.

Immediately, we noticed a lack of DL4BCS articles that utilize MLPs only. This could be due to how MLPs are typically used as the final layer in hybrid systems, as mentioned above. However, each paper features a unique blockchain application along with different layers of blockchain. To begin, only one paper in our methodology aims to improve both privacy and security while using MLPs and AI of Things (AIoT) [15]. Other researchers have different applications, as they focus purely on security improvements. Interestingly enough, papers that focus on security have their own individual methods of applying deep learning to blockchain. While one paper discusses blockchain in general terms to help identify hostile nodes in Proof-of-Stake (PoS) blockchain networks [6], another discusses how general healthcare blockchains can be used to help protect against threats [53], and another article discusses how cryptocurrency (such as Bitcoin) can create threat and anomaly detection systems [19]. There are no patterns within blockchain layers to which these systems and concepts are applied using MLPs. For instance, existing discussions about identity management [15] and threat protection in healthcare [53] utilize the application and data layers in blockchain. Meanwhile, the identification of malicious nodes in blockchain networks [6] uses only the consensus layer, while another paper that discusses threat and anomaly detection with cryptocurrency [19] uses only the data layer. It is intriguing to see that each research paper has taken a unique approach, although each paper focuses purely on using MLPs to their advantage to improve DL4BCS.

Hybrid models are able to use several neural network architectures within one model to create solutions and improvements to systems. Notably, currently existing hybrid papers don't feature an application or system that focuses on privacy, which has proven to be common. A majority of existing research focuses purely on creating an application or system for security purposes, while others focus on implementation for both privacy and security. This is crucial to show that hybrid neural networks have the capabilities to improve both security and privacy, depending on the target for the researcher.

Each paper that applies to both security and privacy features different types of blockchain. From cryptocurrency-based blockchains [36] to healthcare blockchain [9], many researchers have taken unique approaches to creating systems using the different types of blockchain. Notably, most of these papers share the same application of their research. These papers discuss applying their hybrid models to various types of detection systems, even by using various types of neural networks, blockchain types, and different blockchain layers. For example, Elangovan et al. [19] focus on using both RNNs and auto-encoders to create a system for anomaly detection in healthcare systems by using smart contracts in the application layer, traffic analysis in the network layer, and the data layer [19]. Research has also resulted in using MLPs and Denoising Auto-Encoders (DAE) together on the supply chain blockchain to detect anomalies, which utilizes the application and network layer as well, with the addition of the consensus layer [59].

Table 6: **Long Short-Term Memory Network Papers** This table summarizes every gathered paper discussing deep learning for blockchain security (DL4BCS), specifically for LSTMs.

Citation	Priv./Secur.	Att./Def.	Application Domain	Blockchain Layer(s)
[4]	Security	Defense	Storing IDS data using blockchain	Application, Consensus
[39]	Privacy	Neither	Sentiment analysis using blockchain	Application, Consensus
[13]	Both	Defense	Ethereum-Improving healthcare blockchain using smart contracts and ethereum	Data
[50]	Security	Defense	HO-Auth using IoT	Consensus
[41]	Security	Defense	Creating a CIDS using smart contracts and IoT	Application
[37]	Security	Attack	Detecting LDDoS attacks with IoT	Application, Data
[9]	Both	Defense	IoT for healthcare	Consensus

Table 7: **Recurrent Neural Network Papers** This table summarizes every gathered paper discussing deep learning for blockchain security (DL4BCS), specifically for RNNs.

Citation	Priv./Secur.	Att./Def.	Application Domain	Blockchain Layer(s)
[65]	Security	Defense	Energy management with PoA blockchain	Consensus
[46]	Security	Defense	Crypto-based mobile financial transactions and fraud detection	Application, Consensus

As mentioned in Section 4.2, CNN-based architectures are commonly found in hybrid models. CNN and LSTM can be used together with the data layer of the cryptocurrency-based blockchain to create a structure for financial predictions [52] and threat detections [62]. CNN and transformers are also commonly used together for blockchain technology based on financial transactions to improve threat detection, which is similarly based specifically on the blockchain data layer [69; 51]. For instance, Saveetha et al. [51] focus on improving DDoS attack detection, updating minor nodes, and updating transaction requests to improve node reputations, creating a global model [51]. To properly demonstrate how this system works and elaborate upon its prominence in existing DL4BCS research, we provide Figure 5.

Additionally, Airlangga and Gregorius [3] is based purely on the data layer of blockchain, using CNN, LSTM, and MLP to create a threat detection and fraud analysis system with open metaverse blockchain, making this paper completely unique compared to others in our methodology. Yazdinejad et al. [71] discuss security improvements and is also unique since it applies to the hardware layer of blockchain, which, as we have seen, is very difficult to find within existing research. To be specific, [71] introduces a mix of RNN and LSTM for cryptocurrency blockchain to aid with malware detection, focusing primarily on the hardware layer of blockchain.

Now that we have thoroughly distinguished each paper that discuss security applications, we can begin to address papers that have focused on both security and privacy. Right away, there is a clear distinction showing that a majority of these papers seem to focus primarily on the application layer, consensus layer, network layer, and data layer of blockchain. This is an important note showing that researchers who focus primarily on both privacy and security will have to apply more layers of blockchain to their research. Several of these papers focus on permissioned hyperledger blockchain, with one group of researchers utilizing RNN and Bidirectional Long Short-Term Memory (BiLSTM) to introduce a new intrusion detection system [38], and another using transformers along with BiLSTM for financial applications such as risk identification and transaction management [70]. Vijay Anand et al. [66] focus on application, consensus, network, and data using CNN and LSTM (with a specification on auto-encoders) to introduce a new model for threat detection and secure blockchain transactions. A final significant study in our collection of hybrid-based papers features the usage of Hyperledger blockchain, applying purely to the network layer (by featuring data-streaming storage) and the data layer (by using cryptographic ledgers to store information) [58]. By using a substantial mix of neural networks such as LSTM, CNNs, Artificial Neural Networks (ANNs), and Gated Recurrent Units (GRUs), the end goal of this research paper is to apply its content conceptually to a wearable IoT [58].

Existing hybrid research within DL4BCS holds unique statuses within every category we chose to analyze. From different usages of various combinations of neural networks, to discussing both privacy and security (or just strictly security), there is no set pattern that can be seen within our methodology of hybrid papers for DL4BCS. However, it is easy to identify several gaps across these articles. For instance, as mentioned above, there is no research on privacy-based applications. There were also a significant number of papers that used the application layer, consensus layer, network layer, and data layer. However, we only successfully found one hybrid paper that chose to focus primarily on the hardware layer of blockchain, which seems to be a consistent theme between not just hybrid papers, but all papers on DL4BCS in our methodology. As mentioned previously, regardless of whether the paper addresses both security and

privacy or decides to focus on just security, the final application of blockchain remains consistent in current research. Each paper had a final application to create a system to detect threats, anomalies, intrusions, or even malware. Hybrid technology has proven to be successful in improving security. Overall, their reliance on preprocessed or feature-rich inputs limits their adaptability in complex blockchain-based systems.

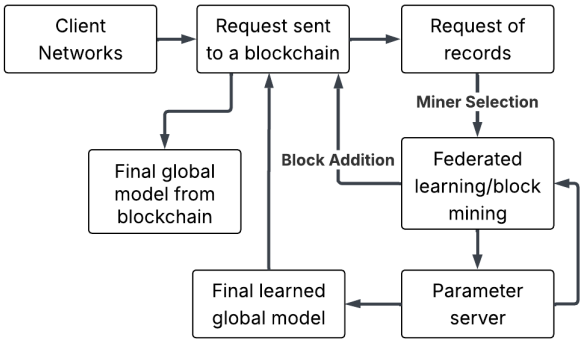

Figure 5: Performance Analysis of Blockchain-Based Secured Distributed Deep Federated Learning for Wearable Internet of Things [51]. This diagram captures the main concept of this research. It presents the idea of using federated learning to detect DDoS attacks in a framework that is integrated with blockchain. Client networks begin by starting data requests, which are ultimately sent to a blockchain and placed in a request queue. Reputation-based miner selection occurs, where miners are evaluated on several factors (such as model accuracy and prior wins). Then, miners participate in federated learning and block mining. These updates are sent to a parameter server and cycle through federated learning, allowing the parameter to repeat iteratively. Once training is completed, the final learned global model gets sent back to the blockchain as a new stored block. The secure global model gets retrieved from the blockchain to be used by clients and miners for DDoS detection. The overall purpose of federated learning with blockchain in this case is to create a tamper-resistant model as well as reliable DDoS detection.

4.6 Transformer Networks

Transformer models have recently been adapted for blockchain tasks that demand context-rich sequence modeling. They excel in phishing detection [16], risk prediction in financial records [36], and federated health data management [8]. Transformers can be applied to analyze transaction propagation patterns, protocol interactions, and user behavior across blockchains. Due to these unique attributes, transformers are commonly used in existing DL4BCS research.

Existing research on transformer models in DL4BCS present unique characteristics between every paper, which separates them from research papers that use different deep learning architectures. However, we are able to identify that these papers seem to properly use the data layer of blockchain, whether it is for transaction-based purposes or to store hashes to make their systems tamper-resistant. It is also important to state that existing research does not focus only on privacy. Each paper is stuck between focusing only on improving security or improving both security and privacy simultaneously. Much like previous neural networks we have discussed, there is once again a clear gap of research in systems that improve privacy alone without inclusion of security. We can also see that a majority of existing research focuses on cryptocurrency-based blockchain, whether it's Ethereum [16] or Bitcoin [1].

It's evident that each article seems to focus on creating a detection system, even with each paper focusing on different threat types. For instance, Mnasri et al. [40] focus on using transformers for healthcare and the Ethereum blockchain, choosing to focus on improving the security and privacy of medical records. Therefore, the researchers have decided to use the application layer (for smart contracts) and the data layer (for hash protection). Next, Batool et al. [8] discuss integrating transformers and IoTs for anomaly detection in networks, which also uses the application and data layer for security purposes. There are two papers within our methodology that also share practically the same attributes. For instance, Abasi et al. [1] discuss using Bitcoin and transformers to improve threat and anomaly detection systems, while Choi et al. [16] use Ethereum to create a fraud and phishing detection system. Both share the trait of using only the data layer to analyze transaction attributes. Finally, Liu et al. [36] decide to merge cryptocurrency and smart contract blockchains to advance a threat detection and financial prediction system, which essentially focuses on both privacy and security. We can conclude that this article is unique since it chooses to prioritize the network layer rather than the data layer to create their concepts.

A common strength is efficiency and parallelism in sequence modeling. However, there are differences in architecture depth and attention mechanisms. To be specific, some use Bidirectional Encoder Representations from Transformers (BERT) embeddings (since BERT can improve natural language processing), while others employ full encoder-decoder setups. One significant gap is the scarcity of transformers in smart contract security, despite their success in natural language processing. These models primarily function at the application and data layers, although network-level applications are emerging. More domain-specific pre-training and explainability tools would enhance their utility.

4.7 Cross-Network Comparison

Our analyzed literature demonstrates diversity in terms of using different neural network architectures in various application domains in DL4BCS research. Each neural network architecture offers unique strengths in current studies. However, they also come with domain-specific limitations. Graph Neural Networks (GNNs) demonstrate superior performance in terms of capturing the relational structure of blockchain transaction graphs, especially for tasks such as node classification, fraud detection, identity inference, and anomaly detection. Notable implementations use spatial-temporal GNNs to model transaction propagation over time. A primary reason why these models stand out is their interpretability and alignment with the graph-based topology of blockchain. They do, however, find standard dataset availability and scalability for ledgers to be one of their major challenges.

Convolution Neural Networks (CNNs) are applied by converting transaction data into spatial matrices or biometric

Table 8: **Multilayer Perceptron Papers.** This table summarizes every gathered paper discussing deep learning for blockchain security (DL4BCS), specifically for MLPs.

Citation	Priv./Secur.	Att./Def.	Application Domain	Blockchain Layer(s)
[15]	Both	Defense	BSecure identity management with AIoT	Application, Data
[6]	Security	Defense	Detecting malicious nodes in PoS blockchain networks	Consensus
[53]	Security	Defense	Healthcare and threat protection using general-purpose healthcare blockchain	Application
[19]	Security	Defense	Threat and anomaly detections using Bitcoin	Data

Table 9: **Hybrid Papers.** This table summarizes every gathered paper discussing deep learning for blockchain security (DL4BCS), specifically for hybrid models.

Citation	Neural Networks	Priv./Secur.	Att./Def.	Application Domain	Blockchain Layer(s)
[67]	RNN, Auto-encoder	Security	Defense	Detection in healthcare using IoMT	Application, Data, Network
[59]	MLP, DAE	Security	Defense	Supply chain-based blockchain for anomaly detections	Application, Consensus, Network
[52]	CNN, LSTM	Security	Defense	IoT and bitcoin blockchains for financial predictions	Data
[66]	CNN, LSTM, Auto-encoder	Both	Defense	Threat detection using general blockchain	Application, Data, Network, Consensus
[62]	CNN, LSTM	Security	Defense	Crypto-based blockchain for threat detections	Data
[69]	CNN, Transformer	Security	Defense	Anomaly detections with financial transactions	Data
[58]	LSTM, CNN, ANN, GRU	Both	Defense	Hyperledger-based blockchain for wearable IoT	Data, Network
[51]	MLP, CNN	Security	Defense	Transaction-based blockchain for threat detection	Data
[3]	MLP, CNN, LSTM	Security	Defense	Open metaverse blockchain for threat detection and fraud analysis	Data
[38]	RNN, BiLSTM	Both	Defense	Permissioned hyperledger intrusion detection system	Application, Consensus, Network, Data
[71]	RNN, LSTM	Security	Defense	Crypto-based blockchain for malware detection	Hardware
[70]	BiLSTM, Transformers	Both	Defense	Permissioned hyperledger for financial risk identification and transaction management	Application, Consensus, Network, Data

Table 10: **Transformer Papers.** This table summarizes every gathered paper discussing deep learning for blockchain security (DL4BCS), specifically for transformers.

Citation	Priv./Secur.	Att./Def.	Application Domain	Blockchain Layer(s)
[40]	Both	Defense	Ethereum-based blockchain to secure medical records	Application, Data
[8]	Security	Defense	Anomaly detections in networks using IoT blockchain	Application, Data
[1]	Security	Defense	Bitcoin-based blockchain for threat and anomaly detection	Data
[16]	Security	Defense	Ethereum-based blockchain for fraud and phishing detection	Data
[36]	Both	Neither	Smart contracts and crypto-based blockchain for threat detection/financial predictions	Network, Data

maps. Their strength can be seen in fraud detection and privacy-preserving applications, especially when embedded in federal edge systems or IoT medical record frameworks. CNNs also appear frequently in hybrid frameworks where they handle spatial feature extraction before Long Short-Term Memory (LSTM) or transformer modules come in for sequential interpretation. However, CNNs lack adaptability across heterogeneous data formats since they require significant preprocessing.

Recurrent Neural Networks (RNNs), especially LSTMs, are important in time series modeling for sequential transaction analysis, intrusion detection, and malware propagation tracking. Their ability to keep a memory of past transactions makes them useful for detecting long-range patterns in decentralized systems. Many LSTM implementations are deployed in privacy environments such as healthcare and IoT, where latency and integrity are critical. However, LSTM and RNN-based systems often lack robustness when it comes to adversarial settings and are computationally intensive, limiting real-world deployments at scale. A subset of models integrates bidirectional or attention-enhanced variants to address these weaknesses.

Generative Adversarial Networks (GANs) contribute through synthetic data generation, adversarial attack simulation, and data augmentation for training classifiers. As seen in our analysis, various studies use GANs to simulate fraudulent behavior in cryptocurrency systems or biometric signals to test defensive mechanisms. They are also used to reconstruct missing transaction features or fill training data sets. GANs have critical gaps when it comes to interpretability and are very rarely accompanied by explainability modules, which poses a challenge in regulatory compliance and trust in sensitive domains such as finance.

Although transformer-based architectures are relatively new in blockchain applications, they have gained traction since they outperform LSTMs when tasked with handling context-rich sequences. Proper context handling can allow models to identify threats properly through pattern shifts and trends. Transformers are often merged into hybrid models or fine-tuned with domain-specific embeddings, but still struggle when it comes to computational demands and lack pre-trained models for blockchain structures.

While Multilayer Perceptrons (MLPs) can be viewed as a simpler architecture, they serve a very important role in lightweight systems. Their presence is consistent in Proof-of-Stake (PoS) monitoring, where interpretability and rapid execution are prioritized. However, MLPs lack the representational depth required for complex sequence or graph analysis and thus are rarely deployed as standalone models.

As mentioned above, hybrid-based architectures combine two or more neural networks. They represent a dominant trend in recent literature. For example, CNN-LSTM combinations are great in fraud prediction by merging spatial encoding and sequential learning, while GNN-Transformer hybrids attempt to bridge structural and temporal contexts. The idea of combining different neural networks is promising, but it requires careful coordination of model training and data integration pipelines. Hybrid models often get the highest benchmark scores in both privacy and security tasks, indicating their strong practical potential even though they require greater computational and engineering effort.

Across all architectures, some common traits can be concluded within current DL4BCS research. For example, the prevalence of hybrid models, the need for better standardization of datasets, and the growing focus on privacy-preserving and federated learning deployments are becoming more apparent. A persistent gap across most models is the lack of explainability tools, despite the increasing regulatory attention blockchain systems have. Another concern is deployment scalability; few models are validated outside of simulated environments, resulting in real-world applications (especially in enterprise settings or cross-chain systems) being limited. Comparably, security applications (like intrusion detection, fraud analysis, and malicious behavior simulation) are widely researched, while privacy-focused tasks (such as anonymization, secure recordkeeping, and identity protection) still require deeper exploration. This comprehensive combination of DL4BCS literature suggests that, while neural networks hold great promises to enhance blockchain, future work must address reproducibility, interpretability, and deployment barriers to unlock their full potential.

5. CHALLENGES IN DL4BCS

Although there are many promising results from integrating deep learning with blockchain, there are still many chal-

lenges that need to be addressed. These challenges are typically a result of limitations that are outside the control of researchers. These challenges range from data limitations to latency, and even include unfortunate trade-offs when attempting to make an area of a system stronger.

5.1 Data Scarcity and Quality Challenges

Major existing issues in DL4BCS research are data availability and quality. Data cannot be made available in their entirety to users due to the privacy-preserving feature of blockchain networks. Even when data is available, it is poor in quality and filled with errors. These errors range from incompleteness, outdated information, inconsistencies, and biases. Low-quality data limits the potential of a proposed system to capture real-world dynamics accurately. These limitations severely impede the development of real-time security models, since poor quality data is devastating to both training efficacy and model reliability [14; 25].

Additionally, the time-critical and high-dimensional nature of blockchain transactions complicates the gathering of data. Supervised learning techniques, particularly those rooted in Graph Neural Networks (GNNs) and Convolutional Neural Networks (CNNs), heavily rely on accurate labeling and adequate temporal information to effectively detect fraud and anomalies [32; 31]. The decentralized anonymous property of blockchain compounds these issues by diffusing available data and limiting access for necessary contextual data [5]. To counter these limitations, others have attempted to find other approaches, such as data augmentation strategies specially those that involve the use of Generative Adversarial Networks (GANs) [75]. Such methods are valuable in terms of directions, but are still limited by the original training data quality, including how representative the created samples are [47; 2]. In conclusion, the lack of quality standards and privacy-oblivious datasets poses a significant obstacle to further advancement of deep learning models in blockchain security (DL4BCS). Future research will need to address the creation of benchmark datasets and privacy-oblivious data collection methods to enable further development of the discipline.

5.2 Real-Time Constraints

In order to have a successful integration of deep learning with blockchain for security purposes, there are several real-time constraints that researchers should be aware of. Real-time performance is critical for blockchain security, as malicious threats and anomalies need to be detected within seconds to properly respond. However, there are several challenges included in this requirement, such as latency. Latency severely limits the ability to detect and respond to threats in time before damage has occurred within a system. Deep learning models also have high computational demands, especially when it comes to continuously updating blockchain data, which can also negatively delay the system response speed to detect threats [25; 14].

Processing time-sensitive data repeatedly can be seen as one of the main issues in this area of study. Blockchain networks have the ability to generate large amounts of transactions, requiring in-depth analysis. However, deep learning models are usually dependent on complex data pipelines that involve formatting, aggregation, and structural updates before any predictions can be made [31; 5]. This preprocessing increases latency for the entire system, particularly in environments where network conditions vary and where data is inconsistent.

High time complexity is involved in training and inference for many deep learning models, which serves as another obstacle. Some approaches in existing research rely on temporal dependencies, which may require sequence construction. This results in delays in threat and anomaly detection that are behind real-time detection expectations [32]. Although some models are designed to be more efficient, they can still fall short when deployed in live blockchain networks. Communication delays, consensus mechanisms, and hardware limitations can further worsen latency and speed of a threat detection system [4; 50].

Researchers have attempted to reduce latency by implementing several methods in their deep learning models. Common methods include slimming models, offloading computations, or coordinating processing with federated learning [66]. Although these methods have proven to be efficient towards lowering latency, there is often a trade-off by implementing one of these methods, including sacrificing accuracy, decentralization, or scalability [47; 15; 8]. It is important to state that these methods cannot completely eliminate latency issues due to real-world constraints. This, therefore, serves as a temporary solution to reduce latency while weakening other areas of the system at the same time.

There is a notable amplification of real-time constraints in systems that integrate deep learning with blockchain consensus. In order to synchronize these two technologies, there must be a standard of consistency across distributed nodes. However, the required synchronization often results in delays that can hinder responses from the system [8]. Intuitively, latency causes models to typically report below-average inference times when placed under test conditions. However, when applied to real-world blockchain environments, there are additional factors to consider, such as communication lag and transaction throughput, which weakens performance and increase load [65; 66; 58].

Low-latency inference in blockchain security is still incredibly sought after, as there are many factors that contribute to latency issues. Although these issues are typically out of researchers' control, they should be viewed as an open challenge that can be addressed through model optimization. It could also be improved upon with more developments of blockchain-compatible architectures that prioritize both speed and accuracy equally, rather than choosing one over the other.

5.3 Privacy Constraints

A big concern regarding deep learning and blockchain integration is managing the trade-off between obtaining quality data for detection accuracy and preserving user privacy. Deep learning methods require access to sensitive information, such as transaction histories and activity logs. The transparency and immutability of blockchain clash with deep learning requirements, which raises concerns regarding data exposure [13]. Model input often needs to be fully visible in order to accomplish meaningful learning. However, doing this creates an opportunity for privacy breaches. CNN models seemingly require raw transaction matrices, but very few existing DL4BCS articles that use CNN-based models incorporate encryption, masking, or other measures to pro-

tect data during processing [5]. Similarly, GNN-based models risk leaking information or being manipulated through adversarial transactions if node embedding is not adequately secured [54]. Although node access controls are implemented, feature-level privacy remains largely unaddressed, as seen in some supply chain use cases [42].

GAN models bring about new privacy risks by using sensitive real data to create synthetic samples. Although having the ability to generate synthetic data can reduce the reliance on raw data sets, existing research does not currently evaluate whether synthetic outputs might accidentally expose private information. A common gap is the lack of methods to preserve privacy. Some examples of possible bypasses could be differential privacy [72] or federated training [22], which is presented in multiple sources. Hybrid models are especially prone to this situation as they combine multiple deep learning techniques to take advantage of their unique strengths. However, this also results in each of their vulnerabilities inflicting a significant effect in systems. In domains like healthcare or finance, where information is very sensitive and regulations limit access to full datasets, neural network models often require continuous data that blockchain systems simply are unable to provide. Without clear transparency controls or consent mechanisms, these models risk violating privacy while enhancing fraud detection. While blockchain ensures traceability and tamper-resistance, the integration of deep learning introduces new privacy challenges despite its security-enhancing potential. However, the complex tradeoffs that come with it are something that most systems are not yet prepared to resolve.

5.4 Opposing Demands of Scalability, Accuracy, and Speed

A challenge found in various deep learning approaches was managing the trade-off between accuracy, speed, and scalability within blockchain environments. Blockchain systems generate high-frequency, high-volume data, demanding timely and precise threat detection. However, many models struggle to meet all three demands simultaneously. As authors tried to improve detection accuracy through various methods, including adding layers, using spatial-temporal features, or generating synthetic samples, they consistently increased computational overhead. For example, transforming blockchain transaction records into a graph-like structure or image-like inputs adds heavy processing overhead. This slows the inference times, making models less suitable for real-time anomaly detection or fraud monitoring on fast-moving blockchain networks. Even lightweight models can cause memory strain and latency, which slows down their effectiveness in large or continuously updating blockchains.

Attempts to address these issues through federated learning, lightweight architectures, or synthetic data augmentation often led to new constraints. Models such as federated CNNs, which are trained across decentralized blockchain nodes, experienced synchronization delays and struggled with performance degradation when local nodes had limited data variety. While GANs have proven to be helpful for creating synthetic blockchain transaction data to address class imbalance, they can become too slow when scaled up to support broader blockchain use cases.

Several GNN models also had difficulties maintaining up-to-date representations of rapidly evolving blockchain graphs, where deeper architectures increased precision but significantly reduced speed and scalability. Across various neural networks, including CNN, GNN, and GANs, authors discussed that improving one dimension generally comes at the cost of another. For example, model depth often comes at the cost of efficiency. This requires task-specific trade-off analysis or adaptive modeling. However, this can be seen with alternative elements, such as a trade-off between security and privacy.

6. FUTURE RESEARCH DIRECTIONS

Throughout the above-discussed papers, there were various research gaps due to the number of challenges that researchers face while merging deep learning and blockchain. In this section, we provide several possible research directions for researchers to consider. Giving more attention and focus to these areas could potentially result in solving the challenges researchers seem to be constantly running into. It could also solve long-term struggles to improve systems that use deep learning to improve blockchain.

6.1 Research for Privacy

Although blockchain features a transparent and immutable design, its functionality to protect sensitive data decreases when merged with deep learning networks. A vast amount of existing research discusses security applications, with very few papers discussing privacy improvements. Since there is a lack of privacy-focused research, there is plenty of room for discovery and academic improvements. Although we previously mentioned trade-offs in Section 5.3 and Section 5.4, there seems to be a common trade-off between security and privacy. When integrating deep learning and blockchain, security may increase within a system, but privacy gets put at risk. While most of the reviewed models assume unlimited access to data, this is unfortunately not realistic due to ethical and regulatory laws for protecting sensitive data. These rules lead researchers to struggle with a lack of data due to the importance of keeping privacy intact.

In the future, it is critical to develop techniques that enable deep learning to enhance blockchain functionalities without compromising confidentiality laws or degrading blockchain performance. As previously discussed, there are methods that can be used to aid with this situation, such as differential privacy, homomorphic encryption, and federated learning. These methods can allow neural networks to learn ethically in order to improve blockchain by avoiding sensitive data. However, there is not enough research to offer a full-proof solution, which leads to a vast need for future research on ethical privacy-based experiments. Overall, researchers have successfully created a vast number of systems that focus on improving security in blockchain, and the focus should be considerably shifted towards privacy improvements.

6.2 Understudied Blockchain Layers

Blockchain currently allows for a deep data hierarchy far beyond what the bulk of existing research currently has access to. While many papers focus on transactions versus accounts (including account statistics), smart construct internals, state transitions, and pending transaction pools, output behavior seems to be scattered.

Future research must look at how certain layers of blockchain can be utilized more for neural models. For instance, the hardware layer of blockchain is severely underused. Improvements with this layer could result in fixing common issues with deep learning and blockchain integration, such as latency. This could be achieved by developing new bytecode-feature encoders, which use graph representations of function calls, or by synchronizing time-sensitive data with confirmed transactions for reliable inputs for neural models.

Specifically, the consensus layer remains underused for model integrations, which introduces a potential research direction to explore how neural networks could be embedded directly into consensus logic. We could also consider the possibility of whether neural networks could be stored directly on-chain, such as using smart contracts to host neural networks. Smart contracts could also benefit from off-chain access, allowing smart contracts to call a neural network to classify images or flag certain behaviors.

Overall, deep learning could be integrated into the network via on-chain integration. Consensus and hardware layers in future research could also potentially make blockchain systems more adaptive and secure, particularly for fraud/attack detection. The overall goal is to build more models that can interpret lower-level information to detect more blockchain threats, which could be done by using underexplored blockchain layers(specifically, the hardware layer or consensus layer).

6.3 Neural Network and Blockchain Interoperability

To achieve the full potential that AI offers in decentralized systems, neural networks must be callable and verifiable using smart contracts. Higher-quality blockchain applications have a significant dependence on off-chain computation, which can impose reliance on external systems. As a result, this can break trust assumptions. Future research should explore model structures or approximation techniques that are on-chain or in trusted execution zones. Furthermore, researchers explore emerging technologies, such as zero-knowledge proofs, which can allow smart contracts to confirm outputs without revealing private data. A trusted pipeline from model to contract (and back) could unlock autonomous, real-time, decentralized intelligence, which has yet to be achieved in current designs and research. In summary, the access of the neural model within smart contracts can result in improvements for overall systems in many various areas, bringing the potential to solve the various issues found in current designs.

7. CONCLUSION

This survey provides a comprehensive overview of how deep learning has been applied to enhance the security of blockchain systems. We have defined this specific field of study as deep learning for blockchain security (DL4BCS). We began with an explanation of blockchain origins, providing an in-depth description of its unique structure. We also properly defined deep learning, elaborating on specific neural networks and their unique properties. By referring to the articles where these technologies have originated, we provided a combined definition of how deep learning and blockchain could be integrated to improve security in models and systems.

We organized current work within our methodology based on neural network architectures, blockchain layers, attack and defense roles, and application domains. Through this comprehensive examination of Graph Neural Networks (GNNs), Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Generative Adversarial Networks (GANs), Multilayer Perceptrons (MLPs), Recurrent Neural Networks (RNNs), transformers, and hybrid models, we uncovered clear patterns, strengths, gaps, and weaknesses of existing research in DL4BCS. To help understand this methodology, we created various tables and diagrams to allow readers to visualize our analysis.

From our results, we can identify that GNNs, GANs, and LSTMs are the most researched architectures. GNNs are prominent since they serve a special role for modeling relational data in transaction networks and can detect complex fraud patterns. LSTMs and RNNs are similar since they can both be applied for sequential modeling, intrusion detection, and anomaly tracing (specifically for IoT and healthcare-based blockchain platforms). At the same time, CNNs and GANs can be applied to blockchain due to their spatial learning capacity and ability to generate fake data. However, their applications may be restricted to specific layers of a blockchain, such as the data layer and application layer.

Although transformer models have recently started applying to improve blockchain security, they have substantial potential due to their long-range dependencies and ability to complete complex security tasks. However, their computational requirements and lack of pre-trained blockchain models serve as barriers for researchers.

As we have seen, hybrid models merge two or more neural networks, serving as a particularly powerful technological integration with improved performance on benchmarks. These models demonstrate the applied use of multi-model learning in blockchain systems, but this typically comes at the cost of increased data preprocessing efforts.

Despite promising advances in this field of study, our survey identifies a number of challenges and issues. Within existing constraints, data availability has proven to be quite common across all existing DL4BCS research. The decentralized, privacy-preserving nature of blockchain makes it difficult for large labeled datasets to train deep learning models. The absence of standardized criteria also contributes to making performance comparisons difficult across DL4BCS studies. Additionally, the majority of present literature focuses on the application and data layers of blockchain, which results in less focus on consensus, network, and hardware. All layers of blockchain serve important purposes for security, but more research could result in privacy improvements. But, it's difficult to improve privacy if realistic datasets are protected, restricting researchers to using synthetic data to train deep learning modules. As a result, systems are restricted to using synthetic data or temporary solutions (such as federated learning). This also means that privacy-preserving approaches (including identity protection and differential privacy) are less understood when compared to security focuses. Real-time constraints have created several issues as well, introducing inference delays and latency within systems. We have also proven that trade-offs are unfortunately common in this area of study. Improving speed often results in sacrificing accuracy, and vice versa.

With both advances and challenges in mind, we identified

various directions for future research. First, publicly available and standardized DL4BCS datasets should be created to make benchmarking and reproducibility much simpler. By doing this, researchers will have increased opportunities to produce more privacy-based models and systems. This also ensures the protection of researchers in terms of specific laws and regulations that focus on preserving data privacy. We also encourage researchers to provide explainability so that trust can be established within these models. Second, more effort needs to be focused on understudied blockchain layers, such as the consensus layer and the hardware layer of blockchain technology. Although alternative layers, including the application layer, are heavily represented in current DL4BCS research, all blockchain layers can provide substantial improvements to blockchain security, especially when integrated with deep learning. Third, we encourage researchers to consider neural network and blockchain interoperability to unlock the full potential of AI. Accessing neural networks within smart contracts serves as a potential solution to improve systems, not just for security purposes but overall.

In conclusion, the integration of neural networks and blockchain has proven to be much more than applying deep learning to a new data source. It requires changing how deep learning models are trained, used, and evaluated within decentralized ecosystems. The presented solutions are not only in technical innovation but also interlace the use of AI, cryptography, distributed computing, and system engineering. By continuing to push boundaries and refine the combination of these technologies, research communities can unlock new methods and models to improve blockchain security by using deep learning architectures. In the far future, we hope that this field of study will motivate the development of safer, more expandable solutions that can be used across a larger variability of both blockchain and deep learning environments.

8. REFERENCES

[1] A. K. Abasi, M. Aloqaily, M. Guizani, and Z. Alatoom. Enhancing anomaly detection in blockchain transactions with transformer-based models. In *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, pages 574–579. IEEE, 2024.

[2] H. S. A. Abdel Qadear and A. I. A. El-Shora. Using deep generative networks for data analysis and quality enhancement in blockchain networks. *Commerce and Finance*, 45(1):152–184, 2025.

[3] G. Airlangga. Deep learning for anomaly detection and fraud analysis in blockchain transactions of the open metaverse. *Jurnal Informatika Ekonomi Bisnis*, pages 324–329, 2024.

[4] A. A. Aliyu, J. Liu, and E. Gilliard. A decentralized and self-adaptive intrusion detection approach using continuous learning and blockchain technology. *Journal of Data Science and Intelligent Systems*, 2024.

[5] J. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran. Cloud-iiot-based electronic health record privacy-preserving by cnn and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics*, 19(1):1080–1087, 2022.

[6] N. T. Anthony, M. Shafik, and H. F. Atlam. An effective mlp model for detecting malicious nodes in pos permissionless blockchains. In *MATEC Web of Conferences*, volume 401, page 10003. EDP Sciences, 2024.

[7] E. Asem, L. M. Abouelmagd, A. E. Tolba, and S. Elmougy. Biometric cnn model for verification based on blockchain and hyperparameter optimization. *International Journal of Computational Intelligence Systems*, 17(1):256, 2024.

[8] Z. Batool, K. Zhang, Z. Zhu, S. Aravamuthan, and U. Aivodji. Block-fest: A blockchain-based federated anomaly detection framework with computation offloading using transformers. In *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)*, pages 1–6. IEEE, 2022.

[9] B. R. Bezanjani, S. H. Ghafouri, and R. Gholamrezaei. Privacy-preserving healthcare data in iot: a synergistic approach with deep learning and blockchain. *The Journal of Supercomputing*, 81(4):533, 2025.

[10] V. Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.

[11] J. Cai, W. Liang, X. Li, K. Li, Z. Gui, and M. K. Khan. Gtxchain: A secure iot smart blockchain architecture based on graph neural network. *IEEE Internet of Things Journal*, 10(24):21502–21514, 2023.

[12] Z. Chang, Y. Cai, X. F. Liu, Z. Xie, Y. Liu, and Q. Zhan. Anomalous node detection in blockchain networks based on graph neural networks. *Sensors*, 25(1):1, 2024.

[13] K. K. Chanumolu and G. M. Nagamani. An enhanced model for smart healthcare by integrating hybrid ml, lstm, and blockchain. *Ingenierie des Systemes d'Information*, 30(1):43, 2025.

[14] S. Chen, Y. Liu, Q. Zhang, Z. Shao, and Z. Wang. Multi-distance spatial-temporal graph neural network for anomaly detection in blockchain transactions. *Advanced Intelligent Systems*, page 2400898, 2025.

[15] C. Chi, Z. Yin, Y. Liu, and S. Chai. A trusted cloud–edge decision architecture based on blockchain and mlp for aiot. *IEEE Internet of Things Journal*, 11(1):201–216, 2023.

[16] S.-H. Choi and S.-J. Buu. Learning to traverse cryptocurrency transaction graphs based on transformer network for phishing scam detection. *Electronics*, 13(7):1298, 2024.

[17] G. Cybenko. Approximation by superpositions of a sigmoidal function. *Mathematics of control, signals and systems*, 2(4):303–314, 1989.

[18] K. P. Dirgantoro, J. M. Lee, and D.-S. Kim. Generative adversarial networks based on edge computing with blockchain architecture for security system. In *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pages 039–042. IEEE, 2020.

[19] V. Elangovan, S. Revathi, N. Jabeen, A. J. Obaid, and R. Kumar. Block chain technology: Anomaly detection in bitcoin using rfmlpalgorithm. In *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, pages 1–6. IEEE, 2024.

[20] J. L. Elman. Finding structure in time. *Cognitive science*, 14(2):179–211, 1990.

[21] C. Geren, A. Board, G. G. Dagher, T. Andersen, and J. Zhuang. Blockchain for large language model security and safety: A holistic survey. *ACM SIGKDD explorations newsletter*, 26(2):1–20, 2025.

[22] M. A. N. U. Ghani, K. She, M. A. Rauf, M. Alajmi, Y. Y. Ghadi, and A. Algarni. Securing synthetic faces: A gan-blockchain approach to privacy-enhanced facial recognition. *Journal of King Saud University-Computer and Information Sciences*, 36(4):102036, 2024.

[23] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio. Generative adversarial nets. *Advances in neural information processing systems*, 27, 2014.

[24] M. Gori, G. Monfardini, and F. Scarselli. A new model for learning in graph domains. In *Proceedings. 2005 IEEE International Joint Conference on Neural Networks, 2005.*, volume 2, pages 729–734 vol. 2, 2005.

[25] A. Harper and M. D. Lee. Scalable blockchain fraud detection using spatial-temporal graph neural networks. *Frontiers in Applied Physics and Mathematics*, 2(1):1–12, 2025.

[26] M. Hasan, M. S. Rahman, M. J. M. Chowdhury, and I. H. Sarker. Cnn based deep learning modeling with explainability analysis for detecting fraudulent blockchain transactions. *Cyber Security and Applications*, page 100101, 2025.

[27] Z. He, Z. Li, S. Yang, H. Ye, A. Qiao, X. Zhang, X. Luo, and T. Chen. Large language models for blockchain security: A systematic literature review. *arXiv preprint arXiv:2403.14280*, 2024.

[28] S. Hochreiter and J. Schmidhuber. Long short-term memory. *Neural Computation*, 9(8):1735–1780, 1997.

[29] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski. The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE Communications Surveys & Tutorials*, 23(1):341–390, 2020.

[30] S. T. Jeyakumar, A. C. Eugene Yugarajah, Z. Hóu, and V. Muthukkumarasamy. Detecting malicious blockchain transactions using graph neural networks. In *International Symposium on Distributed Ledger Technology*, pages 55–71. Springer, 2023.

[31] C. B. Jones and D. J. Kingsley. Decentralized blockchain with convolutional neural network model for security attack mitigation. *ICTACT Journal on Communication Technology*, 14(1), 2023.

[32] V. K. Kasula, A. R. Yadulla, M. Yenugula, B. Konda, and S. Ayyamgari. Improved blockchain security through gnn-based address identification. *Available at SSRN 5139560*, 2025.

[33] A. Laurent. Graph neural networks for blockchain security: A deep learning approach to anomaly detection. *Frontiers in Interdisciplinary Applied Science*, 2(1):93–105, 2025.

[34] Y. LeCun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, and L. D. Jackel. Backpropagation applied to handwritten zip code recognition. *Neural computation*, 1(4):541–551, 1989.

[35] Y. Lei, Z. Chaoyang, I. Alam, and M. A. Mushtaq. Smart network forensics with generative adversarial networks leveraging blockchain for anomaly detection and immutable audit trails. *Power System Technology Volume 48 Issue 1*, 2023.

[36] T. Liu, Y. Wang, J. Sun, Y. Tian, Y. Huang, T. Xue, P. Li, and Y. Liu. The role of transformer models in advancing blockchain technology: A systematic survey. *arXiv preprint arXiv:2409.02139*, 2024.

[37] Z. Liu and X. Yin. Lstm-cgan: Towards generating low-rate ddos adversarial samples for blockchain-based wireless network detection models. *IEEE Access*, 9:22616–22625, 2021.

[38] E. B. Mbaya, E. Adetiba, J. A. Badejo, J. S. Wejin, O. Oshin, O. Isife, S. C. Thakur, S. Moyo, and E. F. Adebiyi. Secfedidm-v1: A secure federated intrusion detection model with blockchain and deep bidirectional long short-term memory network. *IEEE Access*, 11:116011–116025, 2023.

[39] A. F. Mendi. A sentiment analysis method based on a blockchain-supported long short-term memory deep network. *Sensors*, 22(12):4419, 2022.

[40] S. Mnasri, D. Salah, and H. Idoudi. A hybrid blockchain and federated learning attention-based bert transformer framework for medical records management. *The Journal of Supercomputing*, 81(1):317, 2025.

[41] A.-A. Monirah and M. Ykhlef. Deepblock: a collaborative intrusion detection framework based on blockchain and deep learning. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*, pages 180–185. IEEE, 2023.

[42] M. MuhsnHasan, K. Priyanka, A. Shahebaaz, M. Devi, and C. Sushama. Securing blockchain based supply chains in agriculture using graph neural networks for anomaly detection. In *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)*, pages 1–5. IEEE, 2025.

[43] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[44] P. P. Pawar, D. Kumar, B. Ananthan, S. B. Christopher, and R. Surya. An advanced wasserstein-enabled generative adversarial network enabled attack detection for blockchain-assisted intelligent transportation system. In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)*, pages 1–6. IEEE, 2024.

[45] E. Rabieinejad, A. Yazdinejad, R. M. Parizi, and A. Dehghantanha. Generative adversarial networks for cyber threat hunting in ethereum blockchain. *Distributed Ledger Technologies: Research and Practice*, 2(2):1–19, 2023.

[46] H. Ranganatha and A. S. Mustafa. Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d quasi-recurrent neural network and blockchain technologies. *Expert Systems with Applications*, 260:125179, 2025.

[47] C. Rawlins, S. Jagannathan, and D. Wunsch. Prediction of blockchain transaction fraud using a lightweight

generative adversarial network. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*, pages 116–121. IEEE, 2023.

[48] D. Ressi, R. Romanello, C. Piazza, and S. Rossi. Ai-enhanced blockchain technology: A review of advancements and opportunities. *Journal of Network and Computer Applications*, 225:103858, 2024.

[49] E. Rossi, B. Chamberlain, F. Frasca, D. Eynard, F. Monti, and M. Bronstein. Temporal graph networks for deep learning on dynamic graphs. *arXiv preprint arXiv:2006.10637*, 2020.

[50] M. M. Salim, V. Shanmuganathan, V. Loia, and J. H. Park. Deep learning enabled secure iot handover authentication for blockchain networks. *Human-centric Computing and Information Sciences*, 11(21):10–19, 2021.

[51] D. Saveetha, G. Maragatham, V. Ponnusamy, and N. Zdravković. An integrated federated machine learning and blockchain framework with optimal miner selection for reliable ddos attack detection. *IEEE Access*, 2024.

[52] G. C. Sekhar and A. Rajendran. A secure framework of blockchain technology using cnn long short-term memory hybrid deep learning model. *Indonesian Journal of Electrical Engineering and Computer Science*, 28(3):1786–1795, 2022.

[53] S. Selvi, R. DH, et al. Securing healthcare data from trojan using blockchain and multilayer perceptron. *Grenze International Journal of Engineering & Technology (GIJET)*, 10, 2024.

[54] M. Seo, J. Kim, M. You, S. Shin, and J. Kim. gshock: A gnn-based fingerprinting system for permissioned blockchain networks over encrypted channels. *IEEE Access*, 2024.

[55] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar. Blockchain for deep learning: review and open challenges. *Cluster Computing*, 26(1):197–221, 2023.

[56] A. Sharma, P. K. Singh, E. Podoplelova, V. Gavrilenko, A. Tselykh, and A. Bozhenyuk. Graph neural network-based anomaly detection in blockchain network. In *International Conference on Computing, Communications, and Cyber-Security*, pages 909–925. Springer, 2022.

[57] J. Shen, J. Zhou, Y. Xie, S. Yu, and Q. Xuan. Identity inference on blockchain using graph neural network. In *Blockchain and Trustworthy Systems: Third International Conference, BlockSys 2021, Guangzhou, China, August 5–6, 2021, Revised Selected Papers 3*, pages 3–17. Springer, 2021.

[58] S. Singh, A. Arora, G. Garg, A. Goyal, and N. Gandhi. Performance analysis of blockchain-based secured distributed deep federated learning for wearable internet of things. *Cluster Computing*, 28(5):1–30, 2025.

[59] D. H. Son, B. D. Manh, T. V. Khoa, N. L. Trung, D. T. Hoang, H. T. Minh, Y. Alem, and L. Q. Minh. Semi-supervised learning for anomaly detection in blockchain-based supply chains. In *2024 23rd International Symposium on Communications and Information Technologies (ISCIT)*, pages 140–145, 2024.

[60] M. H. Tabatabaei, R. Vitenberg, and N. R. Veeraragavan. Understanding blockchain: Definitions, architecture, design, and system comparison. *Computer Science Review*, 50:100575, 2023.

[61] P. Tasca and C. J. Tessone. Taxonomy of blockchain technologies. principles of identification and classification. *arXiv preprint arXiv:1708.04872*, 2017.

[62] Q. Umer, J.-W. Li, M. R. Ashraf, R. N. Bashir, and H. Ghous. Ensemble deep learning-based prediction of fraudulent cryptocurrency transactions. *IEEE Access*, 11:95213–95224, 2023.

[63] O. Ural and K. Yoshigoe. Survey on blockchain-enhanced machine learning. *IEEE Access*, 11:145331–145362, 2023.

[64] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin. Attention is all you need. *Advances in neural information processing systems*, 30, 2017.

[65] V. Veerasamy, L. P. M. I. Sampath, S. Singh, H. D. Nguyen, and H. B. Gooi. Blockchain-based decentralized frequency control of microgrids using federated learning fractional-order recurrent neural network. *IEEE transactions on smart grid*, 15(1):1089–1102, 2023.

[66] R. Vijay Anand, G. Magesh, I. Alagiri, M. G. Brahmam, B. Balusamy, C. P. Selvan, H. M. Alshahrani, M. Getahun, and B. O. Soufiene. Design of an improved model using federated learning and lstm autoencoders for secure and transparent blockchain network transactions. *Scientific Reports*, 15(1):1–18, 2025.

[67] J. Wang, H. Jin, J. Chen, J. Tan, and K. Zhong. Anomaly detection in internet of medical things with blockchain from the perspective of deep neural network. *Information Sciences*, 617:133–149, 2022.

[68] X. Wang, H. Ji, C. Shi, B. Wang, Y. Ye, P. Cui, and P. S. Yu. Heterogeneous graph attention network. In *The world wide web conference*, pages 2022–2032, 2019.

[69] Z. Wang, A. Ni, Z. Tian, Z. Wang, and Y. Gong. Research on blockchain abnormal transaction detection technology combining cnn and transformer structure. *Computers and Electrical Engineering*, 116:109194, 2024.

[70] Y. Wu. Enterprise financial sharing and risk identification model combining recurrent neural networks with transformer model supported by blockchain. *Heliyon*, 10(12), 2024.

[71] A. Yazdinejad, H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, G. Srivastava, and M.-Y. Chen. Cryptocurrency malware hunting: A deep recurrent neural network approach. *Applied Soft Computing*, 96:106630, 2020.

[72] J. Yu, H. Xue, B. Liu, Y. Wang, S. Zhu, and M. Ding. Gan-based differential private image privacy protection framework for the internet of multimedia things. *Sensors*, 21(1):58, 2020.

[73] Y. Zhang, Y. Liu, and C.-H. Chen. Survey on blockchain and deep learning. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1989–1994. IEEE, 2020.

[74] W. Zheng, K. Wang, and F.-Y. Wang. Gan-based key secret-sharing scheme in blockchain. *IEEE transactions on cybernetics*, 51(1):393–404, 2020.

[75] F. Zola, J. L. Bruse, X. E. Barrio, M. Galar, and R. O. Urrutia. Generative adversarial networks for bitcoin data augmentation. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 136–143. IEEE, 2020.