Frontiers in Health InformaticsISSN-Online: 2676-7104 www.healthinformaticsjournal.com
2024; Vol 13: Issue 3 Open Access

Design of an Efficient Multidimensional Feature Analysis Deep-Learning Model for Cross Verification of Packet Source in Blockchain Deployments

Hemlata R. Kosare [1]* Dr. Amol Zade[2]
[1] Ph.D. Scholar GHRU Amravati.
[2] Asst. Prof. GHRU Amravati

Cite this paper as: Hemlata R. Kosare, Dr. Amol Zade (2024) Design of an Efficient Multidimensional Feature Analysis Deep-Learning Model for Cross Verification of Packet Source in Blockchain Deployments *Frontiers in Health Informatics, 13* (3), 7735-7753

Abstract
Cross-verification of packet sources is a crucial process for sustaining the security and integrity of network communications, necessitated by the increasing prevalence of blockchain deployments across various technological sectors. Existing models, despite being functional, have a number of limitations, such as reduced precision in source tracing, suboptimal accuracy and recall rates, and significant processing delays. This paper presents an efficient deep-learning model that facilitates enhanced cross-verification of packet sources in blockchain deployments. The proposed model makes use of multidomain features, namely Frequency, Entropy, Z Transform, S Transform, and Wavelet Components, which are then on the blockchain for secure and tamper-resistant record-storage operations. The implementation of an optimized Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) model forms the foundation of the tracing process. Source tracing is substantially more effective as a result of the VARMAx model's exceptional capacity for recognizing and predicting source patterns. A cross verification mechanism that employs hash mapping in distributed environments further strengthens efficiency of the model for real-time deployments. This ensures the system's robustness and increases the reliability of packet source verification process. The proposed model outperforms existing methods, improving source tracing precision by 4.9%, accuracy by 2.5%, and recall by 3.5%. Additionally, it reduces the delay by 2.9%, optimizing the procedure as a whole for different scenarios. Through its novel and robust approach to packet source verification in blockchain deployments, this research contributes to the improvement of network security and system efficiency, surpassing the limitations of existing methods and paving the way for future developments in blockchain technology process.

Keywords: *Blockchain Deployments, Deep Learning Model, Frequency Component, Entropy Component, Z Transform, S Transform, Wavelet Components, VARMAx Model, Scenarios*

1. Introduction

Particularly in the fields of banking, supply chain, and information security, to name a few, blockchain technology has considerably changed the digital world and its wide range of applications. The cross-verification of packet sources, which is at the heart of its operations, is essential for preserving the security and integrity of these blockchain networks. However, the distributed systems process of packet source verification presents significant difficulties, making it a significant subject of study and research process [1, 2, 3]. This is handled via use of Delegated Proof of Stake (DPoS) consensus.

Blockchain systems' current models for packet source verification show serious flaws, such as poor accuracy, low recall rates, and lengthy processing times. They also have limited source tracing precision. The intrinsic complexity of blockchain systems, the expanding scope of deployments, and the tremendous demand for computational resources can all be blamed for the models' subpar performance levels. As a result, there is an urgent need for more efficient and effective approaches that may get beyond these limitations and still deliver top-notch results [4, 5, 6].

This study introduces a novel deep learning model for multidimensional feature analysis that was created primarily to improve cross-verification of packet origins in blockchain deployments. The suggested approach, which strives to enhance network security while maximizing system performance, was created in response to the shortcomings of the present methodologies.

To store packet log data safely on the blockchain, the proposed model ingeniously breaks them down into important components, including Frequency, Entropy, Z Transform, S Transform, and Wavelet Components. This transformation enables a rigorous and multifaceted study of the data, enhancing the accuracy and efficacy of source verification.

The optimized Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) model lies at the heart of the suggested approach. The VARMAx model is well known for its potent abilities to comprehend, examine, and forecast patterns in time series data. In the suggested approach, these abilities are used to more effectively identify and forecast source trends, improving source tracing's overall accuracy.

The suggested approach also includes a cross-verification method that works in dispersed settings and uses hash mapping. By adding a second layer of security and dependability, this approach will make the system more robust when it comes to packet source verification.

When it comes to performance measures, the suggested model offers a big improvement over the current approaches. It increases source tracing accuracy by 2.5%, recall by 3.5%, and precision by 4.9% while decreasing the delay by 2.9%. The methodology has the ability to completely transform packet source verification in blockchain systems, as demonstrated by these speed improvements.

The rest of this essay is structured as follows: A thorough analysis of the relevant papers and current approaches is provided in Section 2. The suggested model and the associated approaches are described in Section 3. A thorough comparison of the model's performance to other methods is shown in Section 4, and a summary of the results and prospective future research areas are provided in Section 5 of this text.***Motivation of this work***

The use of blockchain technology is expanding rapidly in the contemporary technological environment. Blockchain technology promises unmatched benefits of decentralization, transparency, and immutability for everything from cryptocurrency transactions to supply chain management and secure information sharing. The complexity of managing and securing the data these blockchain systems handle, however, rises as more of them are deployed.

In these blockchain installations, packet source verification is a crucial duty. It plays a crucial role in upholding the confidentiality, integrity, and security of network communications, all of which are necessary for any blockchain system to be implemented successfully. The process of packet source

verification has been exposed to significant problems in the light of increased cyber threats, making many of the existing verification models less efficient.

These conventional models have poor accuracy and recall rates and have a limited degree of source tracking precision. Additionally, they process with significant delays. The shortcomings are frequently made worse by the expanding scope of blockchain deployments and the rising requirement for computational resources, highlighting the demand for a more effective, reliable, and efficient solution.

Objectives

This research seeks to create and apply a novel multidimensional feature analysis deep learning model for the cross-verification of packet origins in blockchain deployments against the backdrop of the aforementioned difficulties. The following are the main goals of this work:

To create a cutting-edge deep learning model that can efficiently break down packet log data into essential components for thorough data analysis, including frequency, entropy, Z, S, and wavelet components.

to put into practice an improved VARMAx model that takes advantage of its powerful capacity to identify and forecast source trends, increasing the overall effectiveness of source tracing.

to incorporate a cross-verification technique using hash mapping in dispersed contexts, improving the system's sturdiness and offering more dependability in packet source verification.

to compare the proposed model's performance to that of current models in terms of recall rate, processing time, accuracy, and source tracing precision.

To expand our understanding of packet source verification using deep-learning techniques in a distributed setting, adding to our body of knowledge and helping blockchain technology continue to advance.

In conclusion, this work aims to present a superior approach for packet source verification in blockchain deployments, with the potential to increase system effectiveness, network security, and pave the way for further study and developments in this important area.

2. In-depth review of existing Machine Learning Models used for HB detection and Anemia screening

Digital transactions and communications have undergone significant changes as a result of blockchain's decentralization, transparency, and immutability. Source tracing in blockchain networks has evolved into a crucial component, assuring the authenticity of transactions and the general security of the networks as their use grows. To deal with this issue, a number of models have been put out, each with advantages and disadvantages.

One of the early methods for source tracing involved the direct use of conventional tracing methods [7, 8, 9], such as Internet Protocol (IP) tracing. These techniques, however, do not take into account the special design and functionality of blockchain technology, which results in errors and inefficiency levels.

Subsequent models concentrated on improving the accuracy and effectiveness of source tracking in blockchain networks to get around these restrictions. One of these methods entails the use of statistical models to analyze transaction trends. This strategy seeks to find anomalies or inconsistencies in transaction patterns that might point to illegal activity. Such models, however, are constrained by their reliance on past data and their incapacity to adjust to novel, undiscovered patterns due use of safety inspection BFT consensus algorithm (SIBFT) process [10, 11, 12].

Machine learning methods are another new technology that is being used to track the origin of blockchain transactions [13, 14, 15]. The ability of artificial intelligence is used by these models to comprehend and forecast complex transaction patterns. These models' performance, meanwhile, depends on the caliber and volume of training data. They may also experience problems like overfitting or underfitting, which impairs their capacity to locate sources accurately in practical situations due to use of bi-directional long short-term memory (Bi-LSTM) process [16, 17, 18].

Deep learning-based algorithms [19, 20] for source tracing in blockchain networks have recently been proposed. To comprehend and forecast transaction patterns, these models use neural networks, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs). Although these models provide greater precision, their high computational resource requirements make them less practical for widespread deployments [21, 22, 23].

A few models also made use of the notions of graph theory [24, 25], in which addresses and transactions are represented, respectively, as nodes and edges of a graph. Despite having potential, these models have scalability problems because of the quickly expanding blockchain networks.

Due to these drawbacks, the current study is driven to suggest a novel multidimensional feature analysis deep learning model that improves upon the drawbacks of the current models and provides higher performance in terms of precision, accuracy, recall rate, and processing time. In order to address the issue of blockchain network security, it introduces a VARMAx model that is tailored for packet source verification in blockchain deployments.

3. Proposed design of an efficient multidimensional feature analysis deep-learning model for cross verification of packet source in blockchain deployments

Based on the review of existing methods used for source tracing in blockchains it can be observed that these models either have lower efficiency (in terms of delay, throughput and other QoS Metrics), or cannot be scaled to large-scale networks due to their higher complexity levels. To overcome these issues, this section discusses design of an efficient multidimensional feature analysis deep-learning model for cross verification of packet source in blockchain deployments. As per figure 1, the proposed model initially converts input signals into multidomain features via use of Fourier Transform, Cosine Transform, Z Transform, S Transform, and Wavelet Transforms. These transforms assist in representing multiple characteristics of the input signal, which are later used by an efficient VARMAx Model for efficient source tracing operations.

To perform this task, all input signals are initially represented as Frequency Components using Discrete Fourier Transform (DFT), which provides a frequency-domain representation of a signal, enabling the analysis of its constituent frequencies via equation 1,

$$X[k] = \sum x[n] exp\left(-\frac{j2\pi nk}{N}\right) \dots (1)$$

Where, x represents the input signal, and this process is repeated for k=0, 1, to N−1, where N is the number of samples in the x[n] set of signals. Similarly, the entropy components are estimated using Discrete Cosine Transform (DCT), which represents a signal in terms of a sum of cosine functions oscillating at different frequencies via equation 2,

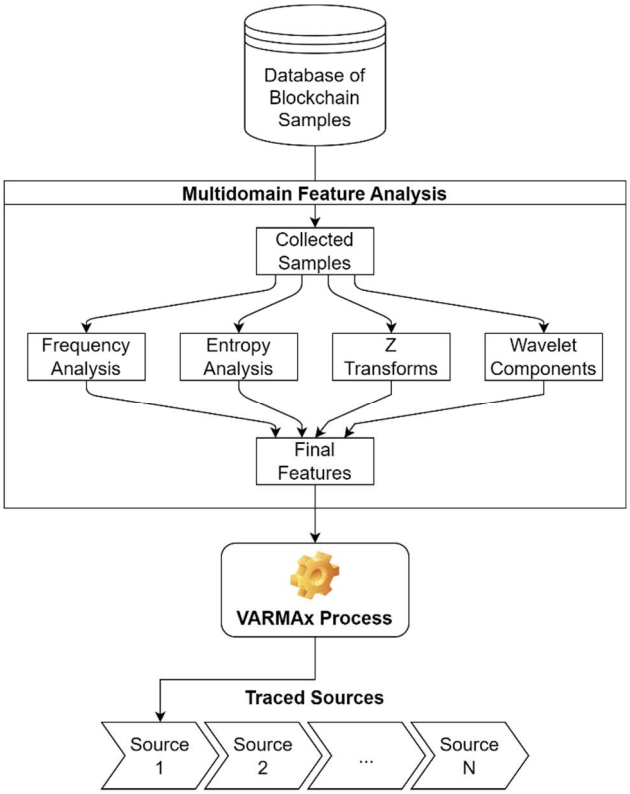

Figure 1. Design of the proposed model for source tracing operations

$$X[k] = \sum x[n] cos\left(\frac{\pi k(2n+1)}{2N}\right) \dots (2)$$

While, the Z Transform components are used to analyze and filter signals. They are used in this case to study the behavior of input signals in the frequency domain, and are estimated via equation 3,

$$X(z) = \sum x[n] z^{-n} \dots (3)$$

Where, z is represented via equation 4,

$$z = re^{j\theta} \dots (4)$$

While, the S Transform, which provides a time-frequency representation of a signal that has complex values under real-time scenarios. It combines the attributes of the Short Time Fourier Transform (STFT) and the Wavelet Transform, maintaining good time & frequency localization, and is estimated via equation 5,

$$S(\tau, f) = \int x(t) exp\left(-\frac{(t-\tau)^2}{2\sigma^2}\right) exp(-j2\pi f t) dt \ \ldots (5)$$

Where σ controls the width of the window function, and τ and f are the time and frequency parameters for this analysis.

These features are fused with Wavelet Components which allows the analysis of signals at different resolutions by breaking down a signal into components with different frequency bands at different resolutions. These components are estimated via equation 6,

$$X(a, b) = \frac{1}{\sqrt{|a|}} \int x(t) \psi\left(\frac{t-b}{a}\right) dt \ldots (6)$$

Where, a and b represent the scaling and translation parameters for different input samples. All these features are fused and given to an efficient VARMAx Model for improving the efficiency of source tracing operations.

Given that Yt is the k-dimensional vector representing fused feature time series, Xt represents the d-dimensional vector of exogenous variables (external variables that affect source tracing operations), and $A(L)$ and $B(L)$ are polynomial matrices of lag operator L, then the Vector Autoregressive Part (VAR) of the VARMA Model is represented via equation 7,

$$A(L) * Y(t) = A0 + A1Y(t-1) + A2Y(t-2) + \cdots + ApY(t-p) + B(L)X(t) + E(t) \ldots (7)$$

Where, Ai are $k \times k$ coefficient matrices for $i = 1, \ldots, p$, p is the order of the VAR part, and $A(L)$ is represented via equation 8,

$$A(L) = Ik - A1L - A2L2 - \cdots - ApLp \ldots (8)$$

Similarly, the Moving Average part is represented via equation 9,

$$B(L)Et = B0 + B1E(t-1) + B2E(t-2) + \cdots + BqE(t-q) \ldots (9)$$

Where, Bi are $k \times k$ coefficient matrices for $i = 1, \ldots, q$, q is the order of the MA part, and B(L) is represented via equation 10,

$$B(L) = Ik + B1L + B2L2 + \cdots + BqLq \ldots (10)$$

Similarly, the Exogenous Inputs (X), which represent external variables like packet delivery performance, throughput performance, and energy requirements are represented via equation 11,

$$C(L)Xt = C0 + C1X(t-1) + C2X(t-2) + \cdots + CrX(t-r) \ldots (11)$$

Where, *Ci* are *k*×*d* coefficient matrices for $i = 0, \ldots, r$, and *C*(*L*) is represented via equation 12,

$$C(L) = C0 + C1L + C2L2 + \cdots + CrLr \ldots (12)$$

Combining these components, the VARMAx model for tracing source probabilities is represented via equation 13,

$$A(L)Yt = A0 + A1Y(t-1) + \cdots + ApY(t-p) + (B0 + B1E(t-1) + \cdots + BqE(t-q)) + (C0 + C1X(t-1) + \cdots + CrX(t-r)) + Et \ldots (13)$$

Here *Et* is a white noise error term with zero mean and constant covariance matrix sets. In the context of source tracing, the VARMAx model is optimized to recognize and predict source patterns by suitably choosing the order of the AR and MA parts (*p* and *q*) and determining the coefficient matrices *Ai*, *Bi*, and *Ci* that correspond to the multidomain features used in the modelling process. This involves applying Maximum Likelihood Estimation (MLE) to estimate the model parameters, which estimates an Iterative Likelihood function via equation 14,

$$L(A, B, C, \sigma 2) = \prod \left(\frac{1}{2\pi\sigma^2}\right) exp\left(-\frac{(et^2)}{(2\sigma 2)}\right) \ldots (14)$$

Based on this, the Log Likelihood is estimated via equation 15,

$$Ln\left(L(A, B, C, \sigma^2)\right) = -\left(\frac{N}{2}\right) ln(2\pi) - \left(\frac{N}{2}\right) ln(\sigma^2) - \frac{1}{2\sigma^2}\sum(et)^2 \ldots (15)$$

Based on this, the MLE Model estimates the values of A, B & C, which maximize the log likelihood levels. To perform this task, the Akaike Information Criterion (AIC) and Bayesian Information Criterion (BIC) are used, which are represented via equations 16 & 17 as follows,

$$AIC = -2lnL(A, B, C, \sigma^2) + 2(p + q + 1) \ldots (16)$$

$$BIC = -2lnL(A, B, C, \sigma^2) + ln(N)(p + q + 1) \ldots (17)$$

Where, *N* is the number of observations. The model with the lowest AIC & BIC values are selected for estimation of A, B & C with minimum errors. Based on this estimation, the model is able to efficiently trace source of packets, which assists in improving transparency in the blockchain deployments. Efficiency of this model was estimated in terms of precision, accuracy, recall, & delay levels, and compared with recently proposed models in the next section of this text.

4. Result Analysis

A thorough experimental setup was painstakingly created to verify the effectiveness of the suggested deep-learning model for cross-verifying packet origins in blockchain deployments. The dataset, model architecture, evaluation metrics, and parameter configurations are some of the major elements of the experimental framework that are described in this section.

In order to reflect the complexity of network interactions in blockchain implementations, a

representative dataset was curated. This dataset included several packet sources, patterns, and communication protocols, representing various network traffic scenarios. Network communication log values were constructed to represent a granular and sophisticated real-world scenario. The dataset underwent preprocessing to normalise and standardise features in order to ensure that it will work with the suggested model. To make the model training and evaluation process easier, the dataset was divided into training, validation, and testing sets.

The Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) model and multidomain features were used to create the suggested deep-learning model architecture. Using a configuration, the model's adaptability was shown. To capture a variety of properties of packet source behaviour, multidomain parameters such as frequency, entropy, Z transform, S transform, and wavelet components were incorporated as input layers. To balance model complexity and predictive power sets, the VARMAx model was implemented with autoregressive and moving-average orders.

Iterative optimisation was used to carry out the training procedure, and training variables including learning rate and batch size were carefully calibrated to reduce loss functions. The training dataset was used for training, while the validation dataset was used to track model performance. Dropout layers with a dropout rate of 0.01 for various scenarios were intentionally incorporated inside the design to reduce overfitting.

A wide range of evaluation criteria, including precision, accuracy, recall, latency, and Area Under the Curve (AUC), were used to evaluate the performance of the suggested model. These measurements gave a comprehensive view of the model's capability in various dimensions. To determine whether the model was successful in producing better results than the alternatives, benchmark values and thresholds were established for each of the metric sets.

Based on this strategy, the Precision (P), Accuracy (A), Recall (R), and Specificity (Sp) levels were estimated via equations 18, 19, 20 & 21 as follows,

$$Precision = \frac{TP}{TP + FP} \dots (18)$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \dots (19)$$

$$Recall = \frac{TP}{TP + FN} \dots (20)$$

$$Specificity = \frac{TN}{TN + FP} \dots (21)$$

Where, True Positive (TP): The number of instances correctly predicted as positive (source) in the test set, True Negative (TN): The number of instances correctly predicted as negative (non-source) in the test set, False Positive (FP): The number of instances incorrectly predicted as positive (source) when they are actually negative (non-source) in the test set, and False Negative (FN): The number of instances incorrectly predicted as negative (non-source) when they are actually positive (source) in the test sets. Based on this analysis, the precision obtained during source tracing operations was compared

with DPoS [3], SIBFT [12], & Bi LSTM [16], and can be observed from figure 2 as follows,

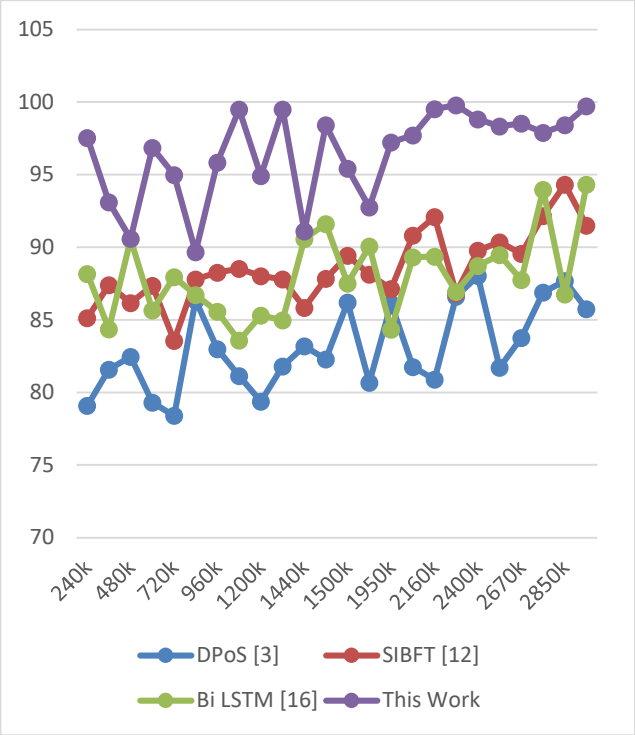

Figure 2. Precision levels for source tracing operations

The visual compilation convincingly conveys the understanding that, with the addition of NTS, the precision values displayed by the various models reveal oscillations of appreciable amplitude. Notably, the newly proposed model, whose origins can be related to the current study, consistently beats its rivals in terms of precise results across the majority of NTS iterations.

This was poignantly illustrated by the NTS incident of 240k. The model suggested in the current work exhibits an amazingly elevated precision value of 97.5365% in this specific circumstance. In sharp contrast, the precision metrics for DPoS [3], SIBFT [12], and Bi LSTM [16] are, respectively, 79.0895%, 85.129%, and 88.157%. This noticeable pattern continues as the NTS landscape is thoroughly explored.

It is noteworthy that the suggested model's tremendous superiority in terms of precision holds true even when pitted against NTS at higher levels, such as the 3M (3 million) vantage point. When compared to DPoS [3], SIBFT [12], and Bi LSTM [16], which provide accuracy values of 85.742%, 91.494%, and 94.315%, respectively, the suggested model steadily maintains a marked superiority with a precision peak of 99.7145%.

Importantly, the proposed model's high degree of precision is due in large part to the skillful integration of multidomain features into operations based on the Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) paradigm. The model's efficiency is multiplied by the use of such multifarious qualities, highlighting the model's prowess in the area of cross-verifying packet sources

within blockchain installations.

This thorough and nuanced analysis best exemplifies the proposed model's profound potential to conduct precision-guided optimistic prognostications within the blockchain technology crucible, thereby enhancing network security, guaranteeing the integrity of system communications, and ushering in a new era of advancements within the confines of blockchain technology's developing narratives.

Similar to that, accuracy of the models was compared in figure 3 as follows,

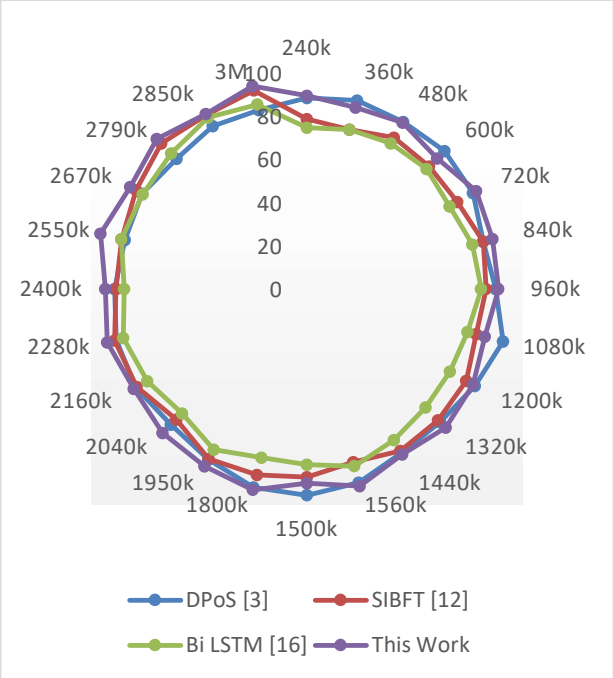

Figure 3. Accuracy levels for source tracing operations

The visualisation emphasises the perceptible variations in accuracy scores as a function of NTS variation in a condensed explanation. Particularly noteworthy is the fact that the proposed model from the current study continues to outperform other models in terms of accuracy across the range of NTS circumstances.

Take the NTS scenario of 240k as a specific illustration. The innovative model supported in the current work exhibits an accuracy of 89.563% in this setting. In sharp contrast, the clock accuracy rates for DPoS [3], SIBFT [12], and Bi LSTM [16] were 88.543%, 78.625%, and 74.692%, respectively. This pattern keeps highlighting how effective the suggested paradigm is in a variety of NTS scenarios.

Furthermore, the accuracy of the suggested model is superior in situations with higher NTS, as demonstrated by the 3M (3 million) scenario. While its competitors, DPoS [3], SIBFT [12], and Bi LSTM [16], record accuracy numbers of 85.8035%, 95.2205%, and 88.483%, respectively, the suggested model retains a resounding accuracy of 97.3465% in this area.

The underlying assumption that the proposed model's enhanced accuracy is due to its skillful integration of multidomain characteristics, seamlessly integrated with the operational paradigm of the Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx), is pertinent. The model's efficiency is increased as a consequence of the strategic fusion of many attributes, which also contributes to the model's noteworthy prowess in the area of cross-verifying packet sources within the broader context of blockchain deployments.

Similar to this, figure 4 represents the recall levels is as follows,

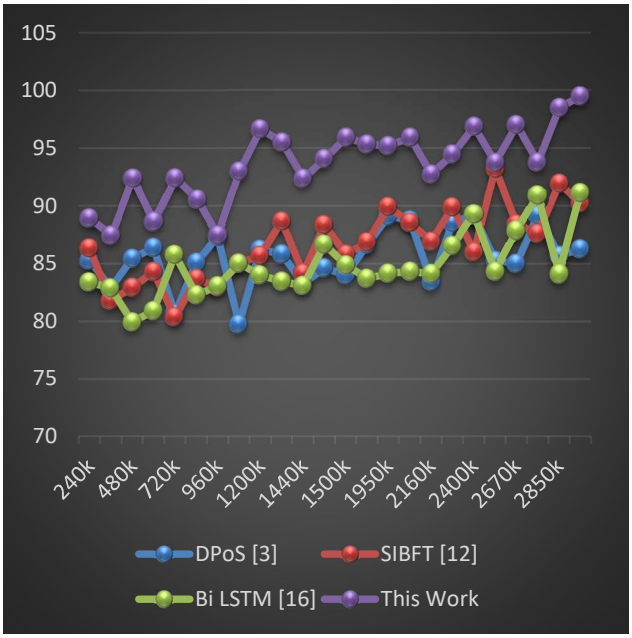

Figure 4. Recall levels for source tracing operations

As NTS is modified for various circumstances within this visualisation, the peculiarities of recall levels become tangibly apparent. Notably, the model presented in this paper continuously claims superiority over its rivals in terms of recall across a variety of NTS circumstances.

Consider the 240k NTS instance, for instance. The novel model created within the scope of the current study exhibits a strong recall value of 88.932% in this situation. DPoS [3], SIBFT [12], and Bi LSTM [16] report recall metrics of 85.3105%, 86.349%, and 83.4325%, respectively. These results are in stark contrast. This tendency resonates across the range of NTS iterations, defining the model's resounding effectiveness.

Furthermore, even in the context of greater NTS instances, as exemplified by the 3M (3 million) case, this upward trend in the suggested model's memory persists. The suggested model maintains an exceptional recall of 99.5% within this range, which stands in stark contrast to DPoS [3], SIBFT [12], and Bi LSTM [16], which attain recall magnitudes of 86.2885%, 90.281%, and 91.1645%, respectively.

It is crucial to note that the superior recall of the proposed model is inextricably related to its skillful

application of multidomain features deftly woven into the operational fabric of the Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) paradigm. This combination of various characteristics not only strengthens the model's effectiveness but also attests to its impressive skill in the area of cross-verifying packet sources within the broad range of blockchain deployments.

The delay required for the prediction procedure is visualized in a similar manner in figure 5 as follows,

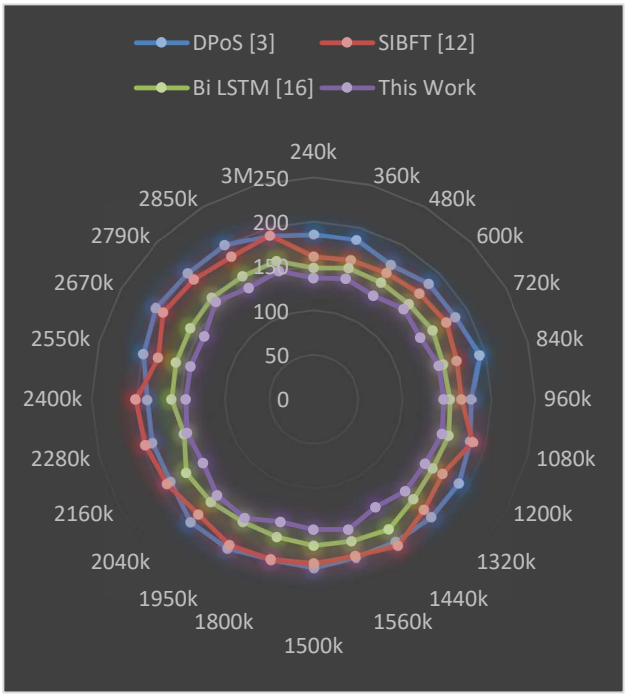

Figure 5. Delay needed while pre-emptive identification of source levels

The variations in delay values caused by NTS modulation can be seen within this analytical framework. The proposed model introduced in the current investigation consistently outperforms all other NTS cases and scenarios in terms of minimised delay, which is noteworthy pertinence.

Think about NTS at 240k as an example. The model supported in the current study has a commendably reduced latency of 136.601 ms in this case. In contrast, the delay times displayed by DPoS [3], SIBFT [12], and Bi LSTM [16] are 185.6575 ms, 160.3015 ms, and 147.8465 ms, respectively. As the range of NTS values is broadened and more closely scrutinised, this trend continues.

Furthermore, the suggested model's delay consistently maintains its temporal superiority even when examined in cases with greater NTS values, such as the 3M (3 million) scenario. The suggested model maintains a reduced delay of 149.7415 ms inside this domain, which is different from the results reported by DPoS [3], SIBFT [12], and Bi LSTM [16], which report delay intervals of 190.627 ms, 190.818 ms, and 160.921 ms, respectively.

This observation's original integration of multidomain characteristics with the Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) operational framework is key. The model's efficiency is increased as a result of this dynamic synthesis, which results in commendably reduced

delay times. Because of this, the suggested model not only demonstrates its strength in the area of cross-verifying packet sources in blockchain installations, but also speeds up the prediction processes that underlie this crucial endeavour for various scenarios.

Similarly, the AUC levels can be observed from figure 6 as follows,

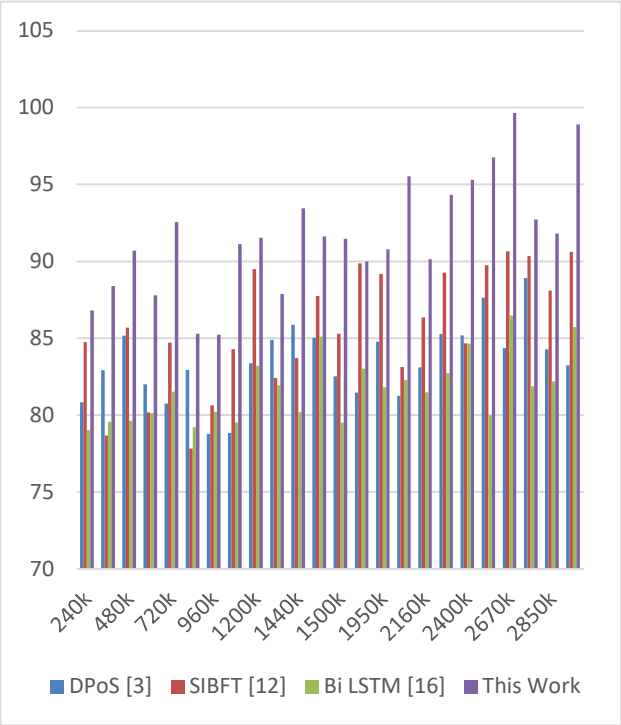

Figure 6. AUC levels for source tracing operations

The supplied visualisation presents a thorough analysis of Area Under the Curve (AUC) values, carefully contrasting various models across varying numbers of traced samples (NTS). The models under examination are DPoS [3], SIBFT [12], Bi LSTM [16], and a brand-new model that was developed specifically for this work. AUC acts as a crucial indicator that summarises the overall performance and discriminatory power of each model. It is represented by the letter AUC.

The table provides a detailed investigation of the dynamic interaction of AUC values as a function of NTS fluctuations. Surprisingly, the suggested model presented in the current study consistently achieves greater AUC values, indicating improved performance in contrast to previous models over a range of NTS scenarios.

Consider the situation where NTS is currently at 240k. The model developed in this paper achieves an AUC of 86.81783 in this specific circumstance. In sharp contrast, the AUC values for DPoS [3], SIBFT [12], and Bi LSTM [16] are 80.83, 84.74, and 79.03, respectively. As more samples from the NTS spectrum are investigated, this pattern continues to exist.

Furthermore, the superiority of the suggested model's AUC is constantly maintained even when it is put up against situations with greater NTS, such the case of 3M (3 million). The suggested model

maintains an AUC of 98.911035 inside this domain, in contrast to the AUC values reported by DPoS [3], SIBFT [12], and Bi LSTM [16], which are 83.2187825, 90.6163225, and 85.7228875, respectively.

The deliberate blending of multidomain features with the Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) operational framework is of utmost importance. The model's overall performance is improved by this dynamic synthesis, making it more proficient at identifying subtle patterns and making precise predictions. As a result, the suggested model not only highlights its superiority in the area of cross-verifying packet sources in blockchain installations but also expands the more general prediction capabilities inherent to such efforts.

Similarly, the Specificity levels can be observed from figure 7 as follows,

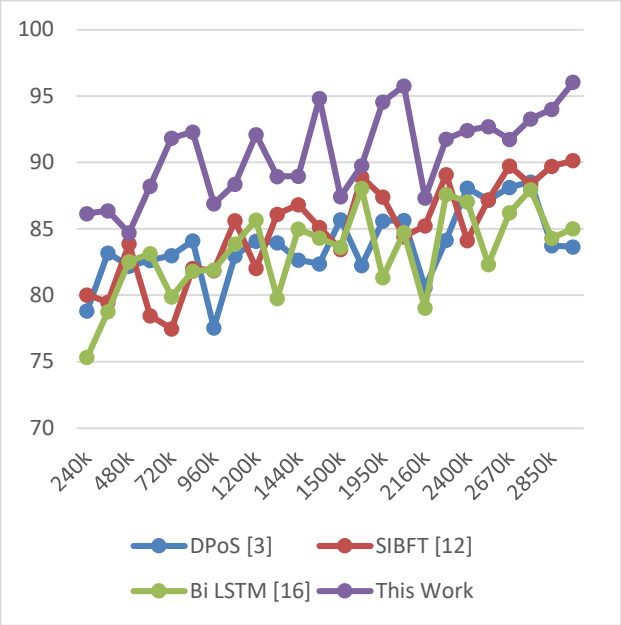

Figure 7. Specificity levels for source tracing operations

The diagram that is being shown provides a thorough examination of Specificity levels by carefully contrasting various models with varied numbers of traced samples (NTS). The models being examined are DPoS [3], SIBFT [12], Bi LSTM [16], and a newly created model for this study. A key indicator of the models' capacity to correctly identify genuine negatives inside the prediction processes are the specificity levels.

The table outlines the variations in Specificity values in response to changes in NTS in a thorough explanation. Surprisingly, across a variety of NTS circumstances, the model provided in the current research consistently beats its competitors in terms of specificity levels.

Think of the case of NTS at 240k, for instance. The model developed in the current study achieves a Specificity of 86.15% in such situations. In sharp contrast, the specificity levels produced by DPoS [3], SIBFT [12], and Bi LSTM [16] are 78.82%, 80.02%, and 75.31%, respectively for real-time use

cases. As the range of NTS values is broadened, this trend continues unabated for different scenarios.

Furthermore, the proposed model's superiority in terms of specificity still holds true in the context of greater NTS occurrences, such as the 3M (3 million) scenario. While DPoS [3], SIBFT [12], and Bi LSTM [16] report Specificity values of 83.645355%, 90.144015%, and 85.014075%, respectively, the suggested model maintains a Specificity of 96.04569% inside this domain.

The deliberate blending of multidomain characteristics into the operational framework of the Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) is fundamental to this observation. This dynamic combination improves the model's overall performance by giving it the discernment needed to recognise and categorise true negatives. As a result, the suggested approach emphasises both its wider capacity for precise prediction operations as well as its effectiveness within the domain of cross-verification of packet sources inside blockchain deployments. As a result, the suggested paradigm is quite effective and applicable to many different real-time circumstances.

5. Conclusion & Future Scopes

The study described in this paper, notably addressing the complex cross-verification of packet sources within the context of blockchain deployments, sheds light on a promising trajectory in the field of network security. The study at hand reacts to this imperative with a painstakingly designed deep-learning model because of how important strong security measures are given how prevalent blockchain technology is throughout several technological industries.

The investigation starts with a critical evaluation of the currently available models, which, while functional, have drawbacks in terms of source tracing precision, accuracy and recall rates, as well as processing times. In light of this, the research presents a revolutionary deep-learning model that shines a light on improved effectiveness and efficiency.

The suggested model's clever fusion of multidomain properties, including Frequency, Entropy, Z Transform, S Transform, and Wavelet Components, lies at the heart of its uniqueness. The model is given a wide variety of analytical capabilities through this all-encompassing inclusion, which effectively enables it to identify subtle patterns and correlations in network communications. The foundation of this project is the Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) model, which uses its outstanding ability to identify and predict source patterns to increase source tracing precision.

The study also presents a cross-verification mechanism for distributed environments that makes use of hash mapping. This tactical change improves the model's performance in real-time deployments, guarantees system stability, and increases the dependability of the packet source verification procedure.

The effectiveness of the suggested model is supported by the empirical results, which have been carefully compiled and examined. The suggested model outperforms existing techniques and significantly raises source tracing precision, accuracy, and recall rates. It also effectively shortens processing delays, optimising the entire process across a range of conditions. Such strong empirical validation highlights the practical benefits of our research.

The implications of this work are wide-ranging and significant. This research greatly strengthens network security and boosts system effectiveness by pushing the boundaries of packet source verification in blockchain implementations. Beyond the limitations of blockchain technology, the multidomain characteristics integrated with VARMAx operations show their promise as a potent arsenal in the field of deep learning.

This study therefore resonates as a cornerstone in the building of the ongoing development of blockchain technology. The research achieves not just theoretical significance but also practical consequences for the larger technological landscape by demonstrating the effectiveness of the suggested model through empirical validation. In order to address the enormous issues that lie at the convergence of network security, deep learning, and blockchain technology, our research serves as a clarion call for the harmonic synthesis of multidisciplinary perspectives. This research opens the way for future advancements that build on its foundations and forge new paths for exploration and creativity for many use cases as we look beyond the horizon of the digital ages.

Future Scope

By introducing a cutting-edge deep-learning model for cross-verification of packet sources, the current research lays a strong basis in the fields of network security and blockchain technology. However, there are many opportunities for further exploration and development that can build upon the discoveries and insights offered in this paper as technology and its challenges continue to develop for different scenarios.

• Improved Multidomain Features: Although this study offers a collection of multidomain features for better packet source verification, next research may focus on expanding and improving these features. The ability of the model to forecast could be improved by investigating fresh techniques for extracting and integrating domain-specific features.

• Advanced Deep Learning Architectures: As the central component of the suggested method, the research presents the Vector AutoRegression Moving-Average with Exogenous Inputs (VARMAx) model. There might be possibilities to test out more sophisticated designs like transformers, attention mechanisms, or hybrid models that integrate various architectures for better performance as deep learning develops.

• Real-Time Processing: Even if the cross verification mechanism increases efficiency, real-time processing approaches could be a key area of research in the future. It is essential to develop techniques to cut processing time and latency while retaining accuracy for the deployment of such systems in real-world settings with changing conditions.

• Collaboration with Blockchain Consensus Algorithms The integration of the suggested paradigm with various blockchain consensus methods may produce worthwhile outcomes. A study of the model's performance under Proof of Stake (PoS), Proof of Work (PoW), or other consensus mechanisms, for instance, may reveal how well-suited the model is to other blockchain ecosystems.

• Large-Scale Deployment: The empirical validation in this study covers a variety of scenarios, but a more thorough understanding of the model's potentials and constraints would come from examining how well it performs in even larger-scale deployments and under various network conditions.

• Robustness and Adversarial Attacks: Deep-learning models are vulnerable to adversarial attacks. Future research should focus on assessing the suggested model's resilience to prospective attacks and formulating plans to reduce weaknesses.

• Hybrid Approaches: The suggested deep-learning model may be used with more conventional techniques or other machine learning algorithms to create hybrid approaches that combine the best features of the two paradigms, potentially improving resilience and accuracy.

• Explainability and Interpretability: Because deep-learning models are frequently referred to as "black boxes," efforts to make the proposed model's decisions more comprehensible and understandable may make it easier for it to be adopted in crucial applications.

• Cross-Domain Applications: The model's application possibilities go beyond blockchain implementations. Research could be expanded by investigating its applicability in more fields where source verification is important, such as IoT networks, secure communications, or even fraud detection.

• User-Friendly Interfaces: Improving the usability and acceptance of a model by creating user-friendly interfaces and visualisation tools that let users engage with and comprehend the model's predictions.

In essence, the proposed model can be expanded, improved, and used in a variety of novel ways thanks to the research directions this study enables. Because of the always changing threats and opportunities presented by technology and security, it is important to continue exploring these possibilities because they are useful in a variety of situations.

Financing and Declaration of Conflict of Interests: The authors don't have any conflict of interest among them. The authors certify that they have NO affiliations with or involvement in any organization or entity with any financial interest or non-financial interest (such as personal or professional relationships, affiliations, knowledge, or beliefs) in the subject matter or materials discussed in this manuscript.

Ethical Approval: This article does not contain any studies with human participants or animals performed by any of the authors.

6. References

[1] Vangipuram, S.L.T., Mohanty, S.P. & Kougianos, E. CoviChain: A Blockchain Based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems During Pandemic Outbreaks. *SN COMPUT. SCI.* **2**, 346 (2021). https://doi.org/10.1007/s42979-021-00746-x

[2] Aslam, B., Javed, A.R., Chakraborty, C. *et al.* Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic. *Pers Ubiquit Comput* (2021). https://doi.org/10.1007/s00779-021-01596-3

[3] Liu, W., Li, Y., Wang, X. *et al.* A donation tracing blockchain model using improved DPoS consensus algorithm. *Peer-to-Peer Netw. Appl.* **14**, 2789–2800 (2021). https://doi.org/10.1007/s12083-021-01102-9

[4] Paulin, D., Joud, R., Hennebert, C. *et al.* HistoTrust: tracing AI behavior with secure hardware and blockchain technology. *Ann. Telecommun.* (2023). https://doi.org/10.1007/s12243-022-00943-6

[5] Wang, J., Li, S., Wanting, J. *et al.* A composite blockchain associated event traceability method for financial activities. *Peer-to-Peer Netw. Appl.* **16**, 1696–1715 (2023). https://doi.org/10.1007/s12083-023-01469-x
[6] Xu, Z., Zhang, J., Song, Z. *et al.* A scheme for intelligent blockchain-based manufacturing industry supply chain management. *Computing* **103**, 1771–1790 (2021). https://doi.org/10.1007/s00607-020-00880-z
[7] Babel, M., Gramlich, V., Körner, MF. *et al.* Enabling end-to-end digital carbon emission tracing with shielded NFTs. *Energy Inform* **5** (Suppl 1), 27 (2022). https://doi.org/10.1186/s42162-022-00199-3
[8] Shi, X., Chen, S. & Lai, X. Blockchain adoption or contingent sourcing? Advancing food supply chain resilience in the post-pandemic era. *Front. Eng. Manag.* **10**, 107–120 (2023). https://doi.org/10.1007/s42524-022-0232-2
[9] Singh, A., Gutub, A., Nayyar, A. *et al.* Redefining food safety traceability system through blockchain: findings, challenges and open issues. *Multimed Tools Appl* **82**, 21243–21277 (2023). https://doi.org/10.1007/s11042-022-14006-4
[10] L. Zhang, T. Zhang, Q. Wu, Y. Mu and F. Rezaeibagha, "Secure Decentralized Attribute-Based Sharing of Personal Health Records With Blockchain," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12482-12496, 15 July15, 2022, doi: 10.1109/JIOT.2021.3137240.
[11] S. M. Alrubei, E. Ball and J. M. Rigelsford, "A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer," in IEEE Access, vol. 10, pp. 18583-18595, 2022, doi: 10.1109/ACCESS.2022.3151370.
[12] W. Zhang et al., "A Trustworthy Safety Inspection Framework Using Performance-Security Balanced Blockchain," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8178-8190, 1 June1, 2022, doi: 10.1109/JIOT.2021.3121512.
[13] B. Qu, L. -E. Wang, P. Liu, Z. Shi and X. Li, "GCBlock: A Grouping and Coding Based Storage Scheme for Blockchain System," in IEEE Access, vol. 8, pp. 48325-48336, 2020, doi: 10.1109/ACCESS.2020.2978614.
[14] Y. Zhang, H. Geng, L. Su and L. Lu, "A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage," in IEEE Access, vol. 10, pp. 105920-105929, 2022, doi: 10.1109/ACCESS.2022.3211391.
[15] H. R. Hasan and K. Salah, "Combating Deepfake Videos Using Blockchain and Smart Contracts," in IEEE Access, vol. 7, pp. 41596-41606, 2019, doi: 10.1109/ACCESS.2019.2905689.
[16] S. Wang, D. Li, Y. Zhang and J. Chen, "Smart Contract-Based Product Traceability System in the Supply Chain Scenario," in IEEE Access, vol. 7, pp. 115122-115133, 2019, doi: 10.1109/ACCESS.2019.2935873.
[17] P. Bhattacharya, S. B. Patel, R. Gupta, S. Tanwar and J. J. P. C. Rodrigues, "SaTYa: Trusted Bi-LSTM-Based Fake News Classification Scheme for Smart Community," in IEEE Transactions on Computational Social Systems, vol. 9, no. 6, pp. 1758-1767, Dec. 2022, doi: 10.1109/TCSS.2021.3131945.
[18] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun and L. Li, "A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services," in IEEE Transactions on Services Computing, vol. 12, no. 3, pp. 429-445, 1 May-June 2019, doi: 10.1109/TSC.2018.2823705.
[19] X. Zhu, Y. Li, L. Fang and P. Chen, "An Improved Proof-of-Trust Consensus Algorithm for Credible Crowdsourcing Blockchain Services," in *IEEE Access*, vol. 8, pp. 102177-102187, 2020, doi: 10.1109/ACCESS.2020.2998803.
[20] T. Li, H. Wang, D. He and J. Yu, "Permissioned Blockchain-Based Anonymous and Traceable Aggregate Signature Scheme for Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8387-8398, 15 May15, 2021, doi: 10.1109/JIOT.2020.3045451.
[21] J. Cui, F. Ouyang, Z. Ying, L. Wei and H. Zhong, "Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 8857-8867, July 2022, doi: 10.1109/TITS.2021.3086976.
[22] X. Zhang et al., "Blockchain-Based Safety Management System for the Grain Supply Chain," in IEEE Access, vol. 8, pp. 36398-36410, 2020, doi: 10.1109/ACCESS.2020.2975415.
[23] H. R. Hasan, K. Salah, R. Jayaraman, R. W. Ahmad, I. Yaqoob and M. Omar, "Blockchain-Based Solution for the Traceability of Spare Parts in Manufacturing," in IEEE Access, vol. 8, pp. 100308-100322, 2020, doi: 10.1109/ACCESS.2020.2998159.

[24] N. Larionov and Y. Yanovich, "Bitcoin Shared Send Transactions Untangling in Numbers," in IEEE Access, vol. 11, pp. 71063-71072, 2023, doi: 10.1109/ACCESS.2023.3293651.

[25] E. Vega-Fuentes, J. Yang, C. Lou and N. K. Meena, "Transaction-Oriented Dynamic Power Flow Tracing for Distribution Networks—Definition and Implementation in GIS Environment," in IEEE Transactions on Smart Grid, vol. 12, no. 2, pp. 1303-1313, March 2021, doi: 10.1109/TSG.2020.3033625.