Enhancing Digital Financial Security with LSTM and Blockchain Technology

Thanyah Aldaham[1], Hedi HAMDI[2]
Department of Computer Science, Jouf University. Sakkaka, Saudi Arabia[1, 2]
Manouba University, Manouba, Tunisia[2]

***Abstract*—The growing dependence on digital financial and banking transactions has brought about a significant focus on implementing strong security protocols. Blockchain technology has proved itself throughout the years to be a reliable solution upon which transactions can safely take place. This study explores the use of blockchain technology, specifically Ethereum Classic (ETC), to enhance the security of digital financial and banking transactions. The aim is to develop a system using an LSTM model to predict and detect anomalies in transaction data. The proposed LSTM model was trained before being tested and the results prove that the proposed model can effectively enhance the security, especially when compared to other studies in the same domain. The proposed model achieved a prediction accuracy of 99.5%, demonstrating its effectiveness in enhancing security by preventing overfitting and identifying potential threats in network activities. The results suggest significant improvements in digital transaction security, enhancing both the traceability and transparency of blockchain transactions while reducing fraud rates. Future work will extend this model's applicability to larger-scale decentralized finance systems.**

***Keywords*—Digital financing; block chain; ETC; security; anomaly detection; machine learning; LSTM**

I. Introduction

Financial transactions are essential to both the national and global economy. Each day, trillions of dollars are traded in the global financial networks that serve a vast number of individuals. Nakamoto [1] claims that although the financial system still uses an underlying trust-based methodology, it works well enough for the majority of transactions. He said that because financial organizations must arbitrate disputes, irrevocable transactions are not feasible. The banking sector is heavily regulated and conservative, and the revenue model hasn't changed in many years. Financial institutions already deal with a number of problems that impair their effectiveness and performance, including high transaction costs, high fraud rates, centralized control that might be challenged by pirates, and a lack of traceability and transparency [2]. Blockchain technology may boost a company's level of trust and control. Performance is impacted when banking institutions attempt to adapt to new client registration and money transfer procedures. Recently, crypto currencies have attracted the attention of both industry and academia. According to Coinmarketcap [3], the capital market for Bitcoin which is the original cryptocurrency, is expected to reach $880 billion. Thus, the influence of blockchain technology acceptance on financial transactions and implementation concerns in the banking sector are determined by this research.

ETC which is known today as legitimate and famous decentralized platform for cryptocurrency other than ETH. In particular, as balanced books are maintained and computers do everything very quickly, the system create such a secure digital stamp, just from the blockchain [4].

Digital technology in the form that has already existed in the pre-digital era and has been introduced and popularized can change and acquire new functions such that it can involve completely new tools and services [5]. Cybersecurity is already integrated in many aspects of digital forensics, which poses as a necessary cornerstone to achieving desirable level of security in Internet of Things [6]. Nevertheless, banking industry represents the bunker of all different kinds of money and private conversations and the secrete storage for people's monetary resources. Competitive factors such as efficiency, performance enhancement, and deposit security have significantly propelled the financial sector forward. However, there is a risk that grows in proportion to the increasing number of users for whom the system is designed or as the system becomes more sophisticated. This situation is not a fair play because people started exploring the system's flaws [7].

The identification of errors in blockchain networks is an enormous task because you may find similar issues if you are looking for attacks or fraudulent activities. Anomaly detection plays out as a key element in blockchain security, allowing for deviations to encrypted content or other unexpected events through the monitoring of blockchain data. A quick recognition and response to the anomaly help minimize the possible damage by attackers and safeguard the whole web [8].

Although Blockchain technology has significantly enhanced security in financial transactions, several gaps remain, particularly in detecting sophisticated anomalies such as 51% attacks. Existing machine learning methods have not fully addressed these gaps, often struggling with overfitting and real-time detection issues. This research seeks to bridge this gap by leveraging an Encoder-Decoder LSTM model within the Ethereum Classic blockchain ecosystem to improve anomaly detection and enhance transaction security.

In this paper, the following contributions can be considered:

- Use of Encoder-Decoder LSTM approach for Ethereum Classic Blockchain (ETC) attack detection enhances blockchain security.

- LSTM model's ability to identify sequential dependencies improves accuracy in anomaly detection.
- Encoder-Decoder LSTM model excels in learning from serialized data.
- Application of recurrent neural networks, particularly LSTM, enhances current blockchain security.
- Improved anomaly detection aids in early detection of threats.
- Enhancements contribute to the reliability of blockchain systems.

II. Literature Review

Blockchain technology has been utilized by the majority of today's companies in order to improve the safety of their data. It is one of the newest technologies that is gaining the greatest traction in the field of protecting the digital world. This section explores a variety of approaches, surveys, strategies, and procedures that have been used in blockchain to address concerns around data sharing and security.

Javaid et al. [9], explored the potential applications of blockchain technology for financial service providers seeking to improve risk management, authenticity, and security. In order to create smart contracts, improve efficiency and transparency, and open up new revenue streams, a lot of organizations are aggressively integrating blockchain into trade and finance systems. The adoption of blockchain-enabled IDs is growing widespread in the banking industry, as the unique recordkeeping capabilities of blockchain render traditional clearing and settlement procedures obsolete. In addition to stressing the transfer of asset ownership and the need of keeping accurate financial ledgers, the study highlights the significance of enterprises anticipating upcoming trends in financial blockchain applications. The measurement, communication, and analysis of financial data are the main areas of concentration for accounting experts. The paper focuses on the importance of blockchain technology for financial services by methodically locating and analyzing pertinent papers. It also explores a range of tools, tactics, and featured services. At the end, major applications of blockchain technology in financial services are identified and evaluated, demonstrating the technology's superior security in credit reporting and its potential to open up new markets, cut costs for issuers, and reduce counterparty risk by customizing digital financial instruments. Blockchain provides a single trustworthy source of truth for network users, making it simpler for members of the business network to collaborate, handle data, and reach consensus by utilizing mutualized standards, protocols, and shared procedures.

Trivedi et al. [10], focused in their study on how blockchain technology is used in the financial and e-finance industries. Research questions about the technology's development, acceptance obstacles, and useful applications are examined. After conducting a thorough analysis of 76 scholarly articles, the study narrowed its attention to 59 articles and created a three-dimensional classification framework that encompasses blockchain development, obstacles, and financial sector applications. The results point to untapped blockchain potential in the finance industry and point to areas in need of technological advancement. The report highlights that the technology is now unregulated, suggesting that it is still in its early stages and that there is ample opportunity for further growth and research in this area.

Hartmann and Hasan [11] drew attention to the abundance of Decentralized Finance (DeFi) Peer-to-Peer (P2P) lending platforms that either demand collateral from users or use conventional credit scoring techniques based on variables like credit history. Some users may find these requirements burdensome, nevertheless. The authors suggest using social media, which has a wealth of publicly accessible personal data and is used by over 55% of the world's population, as an alternative risk mitigator for lending. A user's professional behavior and dependability can be inferred by examining their social media accounts, which results in the creation of a "social score". The study's major contribution is the creation of a fully decentralized lending network that is enabled by the Ethereum blockchain and depends on this social score. With the help of this cutting-edge platform, consumers can obtain a loan even in the event that they don't have enough credit or collateral. The study also explores privacy issues, offering an improved platform that is intended to safeguard the borrower's privacy.

Liao et al. [12] focused on the open banking (OB) adoption trend that financial institutions are currently experiencing for service innovation and integration. Third-party service providers (TSPs) can now access user financial data in an effort to improve user experiences and find the best offers. However, the OB ecosystem's success depends on public confidence in third parties, which raises questions regarding data sharing, privacy protection, and the integration of digital identities. Although there are already decentralized applications (DApps) that address these issues, their integration into a workable three-phase OB method is still lacking, especially in areas like Taiwan. The study presents a blockchain-based identity management and access control (BIMAC) framework and lists the main needs of OB participants. The BIMAC framework creates a trustworthy platform for personal information transaction security control (PITSC) by utilizing smart contracts and a stateless authentication method. This platform provides features like online bank account opening, decentralized third-party login (TPL), integrated payouts, data authorization/revocation, and TSP access monitoring. The evaluation's findings show that the suggested framework's frequently executed functions have less computational overhead than the typical Ethereum transaction cost.

Boughaci et al. [13] introduced, blockchain technology and its fundamental ideas opens the discussion. The paper explores machine learning as a sophisticated instrument for examining large datasets and spotting potentially harmful transactions in untrusted networks. For the purpose of making wise decisions in the fields of banking and finance, the synergy of these clever strategies is highlighted. The suggested method is applied to the Bitcoin system, using the Elliptic dataset available on Kaggle as a standard. Because the dataset is not fully labeled, unlabeled data is divided into two primary clusters using the kmeans technique, and labeled data is allocated to the appropriate cluster. Four machine learning approaches are then used for a thorough classification of the data. The results show promise, especially when k-means and the random forest classifiers are combined, indicating the potential effectiveness of this integrated approach in boosting security precautions.

Song and Chen [14], conducted research on the security of digital financial transactions using blockchain technology. To begin, the security of sdte is examined, as well as the DoS attacks that each role may launch, the assaults that a single role may send, and the attacks that numerous roles may launch in cooperation. It demonstrates that sdte can withstand various assaults and has robust security. Then, the system test's environment is detailed. Then, performance testing and analysis are performed on the key security transmission, smart contract execution in the trusted environment SGX, and overall running time. The testing findings demonstrate that employing the k-nearest neighbor (KNN) method to process data takes less than 0.45 seconds. At the same time, the system's additional cost is acceptable.

With the advent of post-quantum cryptography, it has become increasingly important to stay informed about the latest developments in cryptographic techniques and systems. Post-quantum cryptography is a branch of cryptography that aims to develop cryptographic systems that are secure against quantum computers. Quantum computers have the potential to break many of the classical cryptographic systems currently in use, such as RSA and ECC, by solving the underlying mathematical problems (like integer factorization and discrete logarithms) much more efficiently. As a result, researchers and organizations are actively working on developing cryptographic algorithms that can withstand attacks from quantum computers. Several relevant papers discussing advances in post-quantum cryptography and related topics, such as low-cost S-box implementations for AES [15], a survey on quantum-resistant algorithms and their applications, and strategies for optimizing cryptographic systems to resist quantum attacks [16]. Additionally, studies on lightweight cryptographic techniques for resource-constrained environments and their relevance in the post-quantum era provide further insights into the field [17]. Jalali [18] offer insights into the development of efficient and secure post-quantum cryptographic algorithms. This work, for example, presents a constant-time software library for the CSIDH (Commutative Supersingular Isogeny Diffie-Hellman) protocol, optimized for 64-bit ARM processors, and discusses its potential in the quantum era, particularly regarding its resistance to timing attacks. Another paper by Koziel et al. [19] focuses on the optimization of cryptographic algorithms based on Binary Edwards Curves (BEC), which are designed to be both efficient and secure, particularly for resource-constrained environments such as embedded systems and IoT devices.

Side-channel attacks (SCA) pose a significant threat to the security of cryptographic implementations, particularly in lightweight cryptography designed for resource-constrained environments such as IoT devices. Lightweight cryptographic algorithms such as PRINCE and GIFT-128 offer efficiency in power and memory usage, making them suitable for applications with strict resource limitations. However, their compact designs often expose vulnerabilities to side-channel attacks. For instance, in the work by Xue et al. [20], an SCA was demonstrated against the PRINCE cipher, which utilizes an unrolled architecture optimized for low latency but requires careful handling to prevent leakages during encryption rounds. Similarly, Benjamin et al. [21] explored deep learning-based side-channel attacks on GIFT-128, revealing the effectiveness of neural networks like CNNs in recovering cryptographic keys, even in scenarios involving desynchronized traces. Furthermore, a comprehensive survey by Chao Su and Qingkai Zeng [22] provides an analysis of CPU cache-based side-channel attacks, discussing security models and mitigation strategies, emphasizing the need for resilient designs in modern cryptography. These studies highlight the pressing need for enhanced countermeasures to safeguard lightweight cryptographic algorithms from the growing threat of side-channel attacks.

Table I shows the comparison of the related work mentioned earlier.

TABLE I. COMPARISON OF RELATED WORK

Work	Method	Technologies	Advantages	Limitations
[9]	Integration, smart contracts, revenue	Blockchain technology	Improved risk management, authenticity, security	Privacy concerns, data verification challenges
[10]	Study, examination of development, acceptance, applications	Blockchain technology	Untapped potential, areas for advancement	Lack of regulations, need for further research
[11]	Risk mitigation, social score creation	Ethereum blockchain	Decentralized lending, accessibility for users without credit or collateral	Privacy issues, reliance on social media
[12]	Blockchain-based identity management, access control	Blockchain technology	Improved user experiences, data sharing, privacy protection	Lack of integration, regulatory challenges
[13]	Analysis of large datasets, identification of harmful transactions	Blockchain technology, machine learning	Enhanced decision-making in banking and finance	Limited labeled data, computational overhead
[14]	Analyzing the security of digital financial transactions using blockchain technology, using KNN algorithm to process data for digital financial transaction security.	Blockchain technology, machine learning.	Offering strong security against various attacks and acceptable performance costs.	Lack of extensive studies and established frameworks to build upon.

IV. Background

A. Blockchain in Financial and Banking Transactions

Blockchain is a distributed ledger technology that makes it possible for all parties to check and agree on a transaction before it is added to the value chain [23]. The banking industry has tried out new ways to use technology to improve customer flexibility, the speed of transactions and efficiency. Blockchain technology, as part of Industry 4.0, has the potential to transform business operations across a wide range of industries. Blockchain has been widely adopted and used in the banking and finance industries. Many financial institutions are often run by trusted third parties who are in charge of their operations. In the last step of a digital payment, a bank, credit or debit card, or other service provider acts as a trusted central expert and charges a fee to complete the transaction. For this operation to work, it needs an infrastructure that is both expensive and inefficient. The largest financial institutions in the world are now using this technology (see Fig. 1).

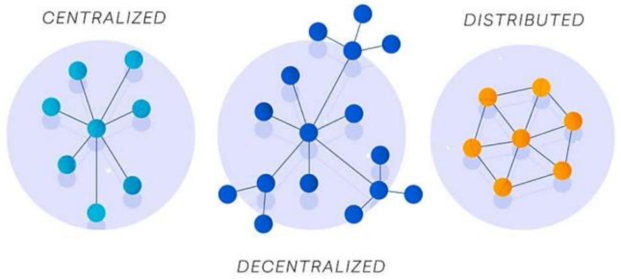

Fig. 1. Decentralization [24].

A blockchain can accommodate any new digital asset across multiple nodes. If a node fails, the data remains accessible and can be delivered by the other nodes. Since the blockchain is a public ledger, any sensitive personal information stored on it must be encrypted and can only be viewed by two parties. Data on the blockchain is encrypted using a public key and decrypted using a private key. Due to its consensus mechanism, the blockchain is immutable and cannot be duplicated. A block is added to the chain if there is consensus that the transactions within it are valid [25]. Despite this, blockchain is not yet widely adopted in the investment sector. However, industries are expected to quickly move towards implementing blockchain-integrated infrastructure in business organizations [26].

The primary advantages of blockchain in the banking sector include improved efficiency, enhanced security, immutable records, faster transaction times, and the elimination of third-party involvement, which reduces costs. One of the key benefits of blockchain is its history of unchangeable transactions—once a transaction is made, it cannot be undone, thereby reducing threats to financial institutions. Blockchain utilizes smart contracts, which are sets of rules agreed upon by the contracting parties. These contracts allow digital information to be stored, accessed, or altered only under specific conditions. Blockchain accelerates transaction processing and, due to its decentralized nature, reduces the need for financial intermediaries. This makes currency conversion cheaper and easier compared to traditional banking methods, while also protecting against scams, money laundering, and trust issues. Financial institutions are expected to adopt blockchain technology very soon, and the banking industry is planning for rapid growth in its use.

B. Ethereum Classic (ETC) Blockchain

Ethereum Classic functions as both a smart contract platform and a cryptocurrency. It's important to note that Ethereum Classic (ETC) should not be mistaken for Ethereum (ETH), despite their shared origins prior to a contentious disagreement that resulted in a split. Below, we delve into the factors that precipitated this divergence.

Ethereum Classic closely resembles Ethereum due to their shared origin. Both are blockchains that facilitate the development of other applications on top of them. These decentralized applications, often referred to as dapps, utilize smart contracts, enabling individuals to exchange money, property, or any other valuable assets without the need for intermediaries. ETC serves as the network's native currency. Additionally, the Ethereum Classic network allows dApps on its platform to create their own tokens, including NFTs [27].

In summary, Ethereum Classic is a decentralized public ledger based on proof-of-work, featuring an embedded Turing-complete programming language that enables the creation of smart contracts and decentralized applications [28][29].

The underlying principles of the Ethereum Classic blockchain closely resemble those of Bitcoin, which stands as the most renowned and prosperous cryptocurrency presently [30]. The consistency of a public ledger in a proof-of-work system is maintained through decentralized mining. Miners continually attempt to solve a complex computational puzzle to find a hash value lower than a specified target. Upon success, miners can generate a block and receive a reward from it.

Fig. 2 represents an example of the general scheme of a blockchain system.

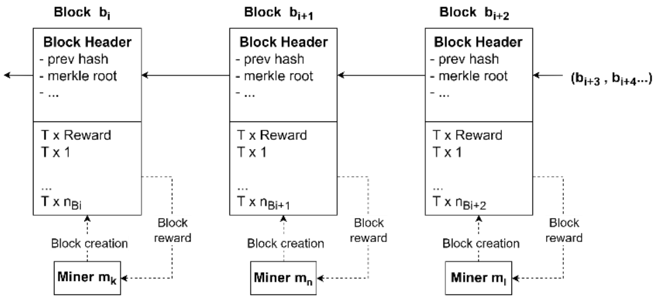

Fig. 2. General scheme of a blockchain system [31].

We won't delve deeply into the technical intricacies of the Ethereum platform here, but notable differences from Bitcoin include the use of accounts instead of UTXO, enhanced internal structures, and Turing-complete scripting languages. Those keen on exploring further can find comprehensive details in the original sources [28]. Instead, we'll focus on a few aspects relevant to the proposed treasury system.

Firstly, it's important to note that the average block time is approximately 14 seconds. This translates to approximately $B_{month} = 1851428$ blocks generated every 30 days.

Top of Form

Another significant distinction lies in the block reward system. Each block incorporates a special reward payment for the miner who mined it. Presently, in Ethereum Classic, this reward amounts to 5 newly created coins per block (uncle blocks excluded). This translates to approximately 9,257,140 coins generated per month $R_{month} = B_{month} \cdot 5 = 9257140$. Miners receive the entirety of these rewards, constituting the sole source of new coins within the system.

In summary, while Ethereum introduces advanced features such as a Turing-complete programming language, enhanced Merkle trees, and a modified GHOST protocol, its foundational principles remain akin to those employed in Bitcoin and other proof-of-work altcoins.

C. *Ethereum Classic Security Challenges*

In the early days, Ethereum stood alone. A collective known as The DAO (decentralized autonomous organization) utilized Ethereum to establish what essentially functioned as a venture capital fund. Ordinary individuals could invest using ETH, participate in decisions regarding asset allocation, and ideally, reap profits. The venture amassed over $100 million through token sales. However, a vulnerability in the fund's code was exploited, resulting in millions of dollars’ worth of ETH being siphoned out and causing panic among investors. Developers had a 28-day window to devise a solution before the hackers could convert the tokens, representing a substantial portion of Ethereum's market capitalization at that time. The prevailing solution involved implementing a hard fork to nullify the hack and reimburse affected individuals. Although endorsed by Buterin and other prominent figures, this moves triggered backlash from purists advocating for the blockchain principle of non-interference with the ledger—arguing that the blockchain should persist with the theft intact. Those advocating for maintaining the status quo remained on the original platform, renaming it Ethereum Classic. Meanwhile, the majority of miners, developers, and users migrated to the forked network, which retained the Ethereum name [27].

Similar to Ethereum, the Ethereum Classic blockchain operates on a "proof of work" mining mechanism, where individuals worldwide utilize hardware and software to validate transactions and maintain network security, earning ETC as a reward. Users can send ETC to each other, akin to Bitcoin or Ethereum transactions with BTC or ETH, respectively. Furthermore, ETC can be used to engage with applications on the Ethereum Classic network, including decentralized exchanges for token swapping. However, it's worth noting that the Ethereum Classic ecosystem isn't as vibrant as Ethereum or other smart contract networks like Solana. As of February 2022, Ethereum Classic exhibited minimal activity in decentralized finance applications, as reported by DeFi Llama. This lower usage rate has raised concerns. Blockchain security hinges on having a diverse group of users actively operating the network; insufficient participation can leave the blockchain susceptible to vulnerabilities. Between 2019 and 2020, the Ethereum Classic network faced several "51% attacks," allowing a hacker to seize control of the majority of the network's computational power. This enabled them to manipulate the ledger and acquire more ETC. Despite these challenges, Ethereum Classic enthusiasts persist in network maintenance and code updates. In December 2020, core developers enhanced the network to render 51% attacks economically unfeasible. The latest upgrade, the Mystique hard fork, occurred in 2022 [27].

D. *Machine Learning in Anomaly Detection of Blockchain Transactions*

The merging of both technologies: Machine Learning and Blockchain Technology, has the potential to provide outcomes that are strong and of practical value. This chapter provides an overview of distributed ledger technology and investigates the ways in which machine learning skills may be incorporated into a system that is based on distributed ledgers. In addition to that, it highlighted a number of well-known uses and instances of how this connected method might be used [32].

The capacities for learning that machine learning algorithms possess are very remarkable. These features can be implemented in the blockchain, which will result in the chain becoming wiser than it was in the past. This collaboration could be useful in helping to enhance the safety of the blockchain's shared ledger in some way. Also, the processing power of ML can be used to take advantage of the shorter time it takes to find the best nonce, and ML can also be used to improve how data is exchanged. Additionally, it is able to construct a great many improved models of machine learning by utilizing the decentralized design characteristics that distributed ledger technology offers [33].

The selfish mining assault, often referred to as a transaction holdback attack, is a deliberate effort to compromise the integrity of the decentralized network. Once one member of a mining pool tries to prevent a correctly verified block from being announced to the others in the mining group cluster, this is known only as "selfish miner assault." This selfish operator shows greater proof-of-work than all the other prospectors in the network as a consequence of hiding their correctly extracted block from the community before moving onto the next frame. By doing this, the community as a whole may accept their transaction methods while the self-centred node keeps the block benefits or cash benefits [32].

V. System Model and Problem Formulation

A. *Problem Formulation*

In today's world of digital finance and banking, the security and integrity of financial transactions are at risk due to increased reliance on technology and growing cyber risks. For example, consider a business owner who transfers funds between accounts frequently using online banking services. Suddenly he notices unauthorized transactions on his account, which indicates a violation in security. In addition to causing financial loss, this incident also damages people's trust in the banking sector.

The aim of the project is to use blockchain technology to improve the security of online banking services and financial transactions. The paper covers a number of important topics such as cyber risk prevention, protecting data privacy, maximizing business efficiency and assessing the pros and cons of integrating blockchain technology into the financial sector. Given the weaknesses of current digital financial transactions (lack of trust, inefficient data sharing, privacy concerns and immutable data silos) a comprehensive review is needed to build a robust and secure blockchain framework.

B. System Model

A number of processes are involved in the suggested methodology for anomaly detection in the Ethereum Classic Blockchain (ETC), beginning with database analysis, employing the Encoder-Decoder LSTM architecture, and evaluating the outcomes as shown in Fig. 3.

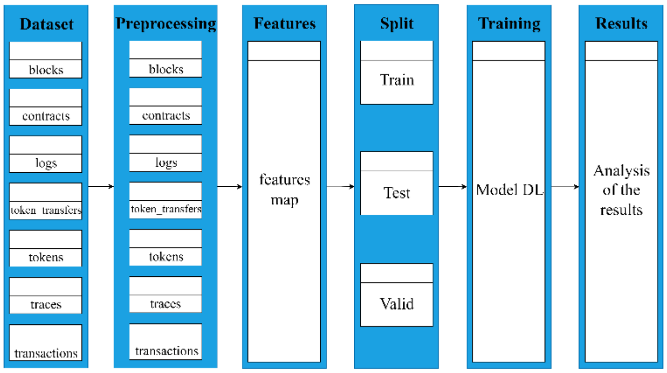

Fig. 3. Methodology used in the research.

VI. PROPOSED SOLUTION

A. Introduction

Ethereum Classic Blockchain has risen to prominence as one of the leading decentralized platforms leveraging the immutable nature of a ledger to undertake safe and transparent transactions. As blockchain technology progresses and is used in more and more industries, the importance of securing and protecting the immutability of blockchain networks grows more important. Given that these systems contain significant monetary transactions and sensitive data, they are prime targets for cybercriminals looking for areas to exploit. Aside from cryptocurrency exchange platforms, another significant challenge that threatens the credibility of blockchain networks is maintaining the safety and security of blockchain networks.

Detecting anomalies is one of the most important challenges to keep blockchain networks trustworthy since these might suggest possible attacks or malicious actions. It is an essential part of proactive measures that help identify any movements or actions that are not consistent with normal blockchain behavior. Early detection and appropriate responses to such anomalies can minimize the consequences of an attack and protect the network.

Deep learning methods have shown impressive results recently in a number of fields, from natural language processing to computer vision. The Encoder-Decoder Long Short-Term Memory (LSTM) architecture in particular has become well-known due to its capacity to learn and represent intricate sequential patterns. This project focuses on using the Encoder-Decoder LSTM architecture to address the anomaly identification problem on the Ethereum Classic Blockchain by utilizing deep learning.

The Encoder-Decoder LSTM model is a good fit for jobs involving anomaly detection because it can efficiently identify temporal patterns and long-term dependencies in sequential data. The model can be trained on past ETC blockchain data to find patterns in the expected behavior of the network and then spot variations that might point to possible attacks or anomalies. The model effectively captures the subtle patterns that rule-based or statistical approaches may miss because of its capacity to encapsulate the input data and produce insightful representations.

B. Methodology

1) Database Analysis: Ethereum Classic is a public, open-source distributed computing platform built on the blockchain. It is notable for having smart contract capabilities, which enable scripts to run on the Ethereum Virtual Machine (EVM), a decentralized Turing-complete virtual machine. An international network of public nodes enables this functionality.

Ethereum Classic is notable for having a native value token called "ether." Ether is a cryptocurrency that may be held in wallets, transferred between users on the network, and used to pay nodes for the processing power they provide to the Ethereum platform.

Over the course of four years, from July 2015 to July 2019, we conducted tests on a section of the ETC blockchain as part of our research. The seven tables in the dataset we used are blocks, transactions, contracts, logs, token transfers, tokens, and traces. It can be accessed on Kaggle. These tables include important details regarding the blocks themselves, the operation of the network, and network use.

Multiple preprocessing stages were carried out in order to get the data ready for additional analysis. First, we carried out feature engineering, which included aggregation, correlation analysis, filtering, and the selection of the most relevant features. In order to rescale values and lessen the possibility of instability impacts during neural modeling, we secondly normalized the data. In addition, the process of normalization attempted to regularize the data by removing trending, cyclic, and seasonal irregularities. Using a shifting quantile ratio, we were able to achieve normalization.

The two parameters that the function first requires are {x}, which stands for the input data, and `window}, which indicates the rolling window's size (the default value is 20). Next, we make an object that rolls windows.

Next, we compute the first quartile. The value that divides the lowest 25% of the data from the remaining 75% is determined by passing the argument {0.25}. Furthermore, we set {interpolation='midpoint'} to ascertain the quartile value estimation technique.

In addition, we compute the third quartile. This time, the parameter {0.75} is passed in order to determine the value that divides the bottom 75% of the data from the top 25%. Lastly, we use the formula:

$$S= \{(x - q2) / (1.5 * (q3 - q1))\}$$

The original data is denoted by {df}, the median by {q2}, the first quartile by {q1}, and the third quartile by {q3}. Taking into consideration the interquartile range, the algorithm scales each value in the DataFrame according to how far it is from the median.

In a similar manner, we get the median by using the rolling window object's `median () ` function. The center figure that divides the data's upper and lower halves is known as the median.

2) Model architecture: The model's architecture is made up of multiple layers and hyperparameters that are specifically engineered to handle and evaluate data sequences as represented in Fig. 4. First, the training set is used to extract the length of the sequence and the number of features. One kind of recurrent neural network is the LSTM layer, which has 64 cells or neurons in its configuration. Additionally, the model has attention mechanisms with four attention heads, each with 64 dimensions. In addition, a convolutional neural network (CNN) layer with 64 filters and a kernel size of three is included in the architecture. Regularization methods like L1 and L2 regularization are used with lambda values of 0.2 to avoid overfitting.

Sequence support is defined for the input layer. Masking is applied to the input layer to manage sequences of varying lengths. To lessen overfitting, the model then incorporates numerous CNN layers with L2 regularization, dropout layers, and ReLU activation functions. To extract significant features and downsample the output, max pooling layers are used. The ReLU activation function and the designated number of cells are integrated into the LSTM layer. Furthermore, a multi-head attention layer is added to capture sequence relationships. Next come further CNN layers, dropout layers, and max pooling layers, then another LSTM layer.

To create the output sequence, a time-distributed dense layer is added last. The mean squared error loss function and Adam optimizer are used to construct the model. The model's summary is printed, together with information on its layers and parameter count. A predetermined path is used to save the trained model, and checkpoints are made to save the optimal model in accordance with validation loss. Additionally, a CSV logger is used to monitor the training progress.

The model has a batch size of 100, a validation split of 0.3, and is trained for 50 epochs on the training data. The model checkpoint and CSV logger are two of the callbacks that are used in the training process.

The architecture we've adopted to predict data, whether it's an attack or normal data. In our model, the green blocks represent the inputs and outputs. Then, there's the masking block, which allows us to handle data of different sizes. When we preprocess the data, we take a fixed-size sliding window. However, at the end of each time sequence, we have a set of data whose size is smaller than the window's size. So, instead of discarding this data, we add it to the model. Thus, the data won't have a fixed size altogether, and there won't be data of different sizes. Therefore, we have to deal with this data, and that's where we use the masking block.

Moving on, the blue block represents the convolutional layer, and the yellow block represents the dropout layer. Here, we'll use two sets, each consisting of two convolutional layers followed by a dropout layer. In the first set, the dropout will be 0.5, and in the second set, it will be 0.8. After finishing the second set, we'll transition to the LSTM layer. Then, after the LSTM layer, we'll apply a multi-head attention layer. At the end of the architecture, in the last group, we have two LSTM layers, and in between, there's a multi-head attention layer. After the LSTM layer, we'll enter two more sets, each comprising two convolutional layers and a dropout layer. The dropout rate will be reversed here, with the first set at 0.8 and the second at 0.5. The transition between them will be done through max pooling, and finally, we'll have the output layer.

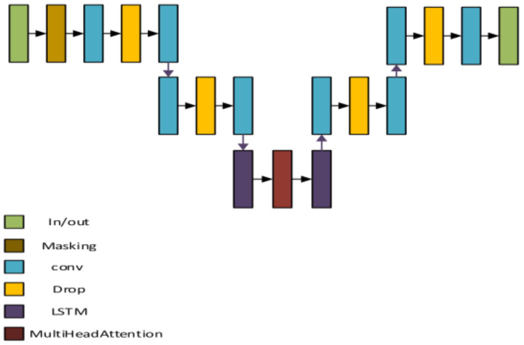

Fig. 4. Architecture of the proposed model.

a) LSTM layer: One kind of recurrent neural network (RNN) layer that is frequently utilized for sequence modeling is the Long Short-Term Memory (LSTM) layer [34]. The LSTM layer in this architecture is set up with 64 cells, or neurons. By preserving a memory state, LSTM cells are made to detect long-term dependencies in sequential input. Rectified Linear Unit (ReLU), the activation function utilized in this layer, gives the output non-linearity.

The LSTM (Long Short-Term Memory) layer employs a gating mechanism to regulate the memorization process. Through gates that open and close, you can store, write, or read information within LSTMs. An LSTM layer comprises the following components as can be seen in Fig. 5:

Forget gate: Responsible for deciding what information to retain and what to discard.

Input gate: Updates the cell state by incorporating information from the current input state (x) and the previous hidden state (h).

Cell state: Stores information based on the previous cell state (c) and new layer state. The current cell state is denoted as g.

Output gate: Determines the value of the next hidden state (h).

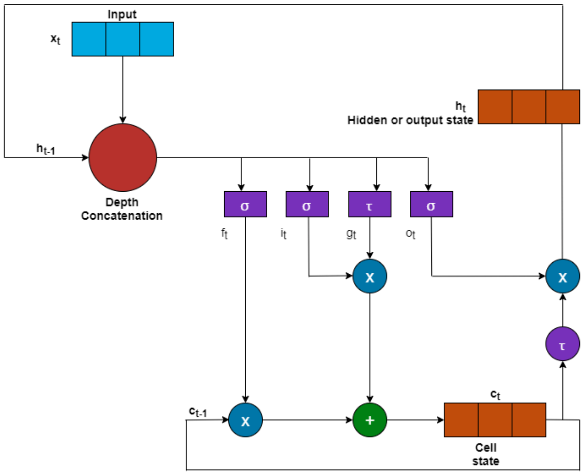

Fig. 5. The components of an LSTM layer [34].

b) Multi-Head attention layer: For the purpose of identifying linkages within the sequence, the Multi-Head Attention layer [35] is essential. It makes use of an attention mechanism with several attention heads, each of which focuses on a distinct segment of the input sequence. This enables the model to extract useful features by concentrating on pertinent data. With four attention heads and a key dimension of 64, the Multi-Head Attention layer in this design is applied to the LSTM layer's output.

At their core, they consist of keys (k) and values (v). We can create queries (q) to interact with these (k,v) pairs in a way that remains valid regardless of the size of the database.

The same query can yield varied responses depending on the database's contents. Let $D = \{(k_1, v_1), \ldots, (k_m, v_m)\}$ represent a database of key-value pairs, and denote a query. We can define attention over D as:

$$Attention(q, D) = \sum_{i=1}^{m} \propto (q, k_i)\ v_i$$

Where $\propto (q, k_i) \in \mathbb{R}\ (i = 1, \ldots, m)$ represents scalar attention weights, with the operation commonly known as attention pooling. The term "attention" stems from the focus placed on terms with significant weights $\propto$, implying larger values. Consequently, attention over D produces a linear combination of database values. Notably, this encompasses the earlier example as a special case where all weights except one are zero.

Given a query$q \in \mathbb{R}^{p_q}$, a key $k \in \mathbb{R}^{p_k}$, and a value $v \in \mathbb{R}^{p_v}$, each attention head $h_i(\ i = 1, \ldots h)$ is computed as:

$$h_i = f\left(\ W_i^q q\ , W_i^k k\ , W_i^v v\ \right) \in \mathbb{R}^{p_v}$$

Where $W_i^q \in \mathbb{R}^{p_q \times d_q}$, $W_i^k \in \mathbb{R}^{p_k \times d_k}$, $W_i^v \in \mathbb{R}^{p_v \times d_v}$ are learnable parameters and is attention pooling, such as additive attention and scaled dot product attention .The multi-head attention output is another linear transformation via learnable parameters $W_o \in \mathbb{R}^{p_o \times h p_v}$ of the concatenation of heads:

$$W_o \begin{bmatrix} h_1 \\ \vdots \\ h_h \end{bmatrix} \mathbb{R}^{p_o}$$

According to this structure, each head has the ability to focus on distinct segments of the input, which allows for the expression of more complex functions beyond simple weighted averages.

The components of a Multi-Head Attention layer are shown in Fig. 6.

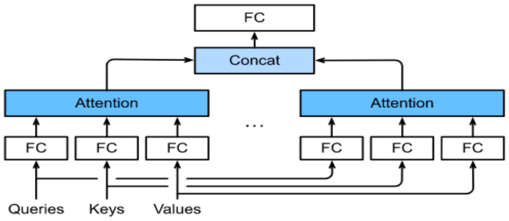

Fig. 6. The components of a Multi-Head Attention layer [36].

c) Convolutional Neural Network (CNN) layers: When attempting to extract geographical and temporal information from data, CNN layers are frequently employed. CNN layers are used in this model to examine the sequence data. Multiple CNN layers with the same configuration are part of the architecture. A predetermined number of filters make up each CNN layer, and these filters are in charge of identifying various patterns and features in the input. When a kernel size of three is employed, the CNN layer scans the input sequence using a three-size window. ReLU is the activation function used in these layers, which gives the output non-linearity. Furthermore, padding is set to'same' to guarantee that the length of the output and the input sequence match.

d) Dropout layers: A regularization method called dropout layers is employed to stop overfitting. During training, they arbitrarily deactivate ˋ set of the neurons, which compels the model to (2) ıire more resilient and comprehensive representations. Dropout layers with a dropout rate of 0.5 or 0.8 are placed after specific CNN layers in this architecture. Dropout layers are strategically placed to improve the model's generalization ability and lessen its sensitivity to noise.

e) Max pooling layers: The most notable aspects of the data are captured by downsampling the output using max pooling layers. They remove less significant data by dividing the input into non-overlapping parts and keeping just the largest value within each zone. By keeping the most important attributes, this downsampling aids in lowering the dimensionality of the data. In order to help with relevant information extraction and efficient feature representation, this design uses many max pooling layers after certain CNN layers.

f) Time-Distributed dense layer: The output sequence is produced at the end of the architecture using the Time-Distributed Dense layer. It separately applies a dense (completely linked) layer to every time step. As a result, the temporal relationships in the data are captured by the model, which can now generate predictions for every element in the sequence. Since the aim in this scenario is to predict a single value for each element in the sequence, a dense layer with a single unit is used.

VII. Results

The results that were obtained in this study are divided into three categories, the first of which is the output of the Preprocessing stage, where the data scanning process was applied. The second category, which is model training, is summarized using the loss function. Finally, the third stage is predicting attack data.

There are seven parameters in the database, the result of the Preprocessing for each variable will be presented separately. Regarding the attack data, it will be identified the same for all the data, so that it is possible to see at what timestamp it was determined to be attack data. To show the experimental results, initially the results of data processing are displayed after being pre-processed such that the horizontal axis represents the timestamps, and the vertical axis represents the different variables. Fig. 7 plots the normalized average gas provided along the time window to show the effect of the preprocessing processes. The red lines within the graphs indicate the attack-prone periods.

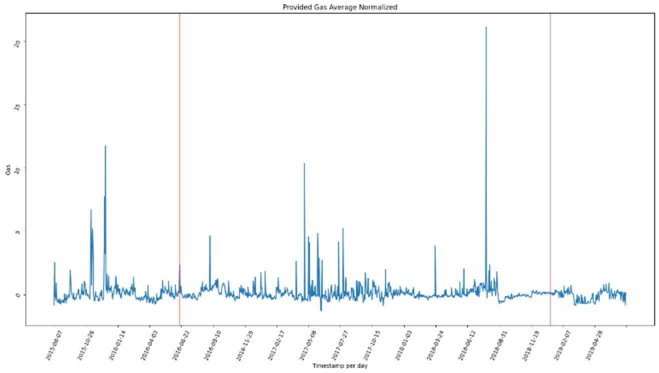

Fig. 7. Relationship of provided gas average with timestamp after normalization.

Similarly, Fig. 8 shows the timestamps represented on the horizontal axis, while the normalized transaction number is represented on the vertical axis. The red lines also represent attack data at these timestamps.

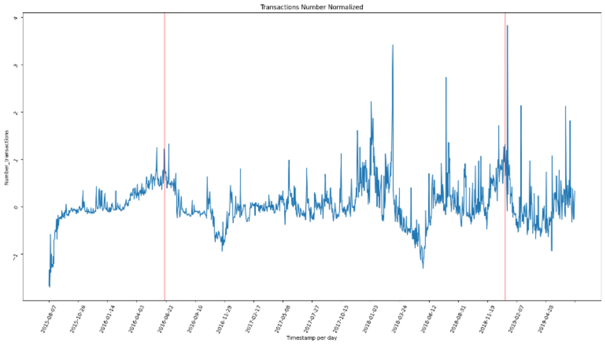

Fig. 8. Relationship of Transactions Number with Timestamp after normalization.

Fig. 9 shows the relationship between Block Difficult Average and Timestamp after normalization, where the horizontal axis represents the timestamps, while the vertical axis represents the normalized Block difficult average.

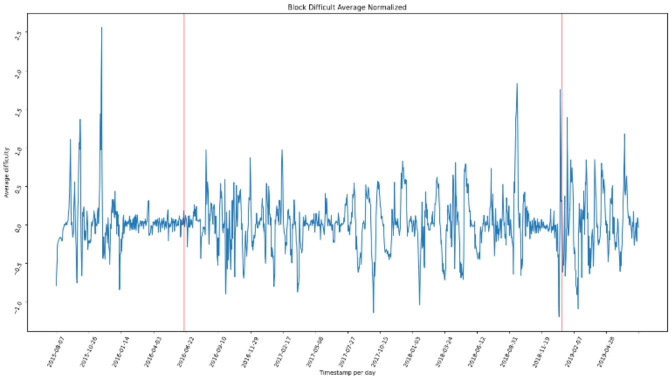

Fig. 9. Relationship of Block Difficult Average with Timestamp after normalization.

Another figure, Fig. 10 illustrates the relationship between block size average and timestamp after normalization, where timestamps are represented on the horizontal axis, whereas the block size average is represented on the vertical axis.

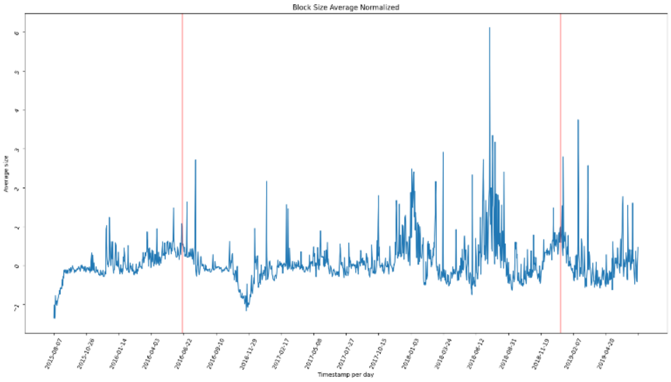

Fig. 10. Relationship of Block Size Average with Timestamp after normalization.

Fig. 11 shows the relationship between the gas used sum and the timestamps, where the latter is plotted on the horizontal axis, whereas the sum of used gas is plotted on the vertical axis.

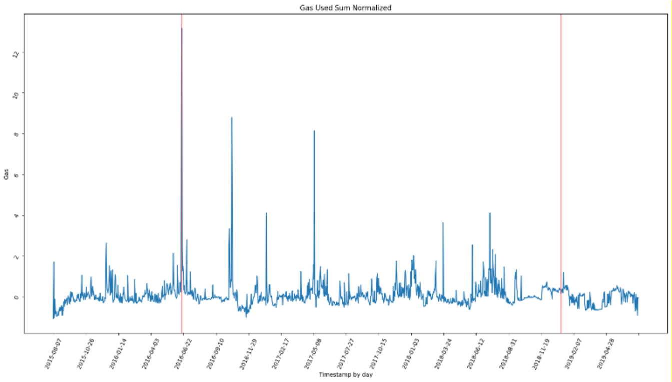

Fig. 11. Relationship of Gas Used Sum with Timestamp after normalization.

Fig. 12 and Fig. 13 show the relationship between the timestamps and the transaction average per plot, and the gas average per transaction respectively.

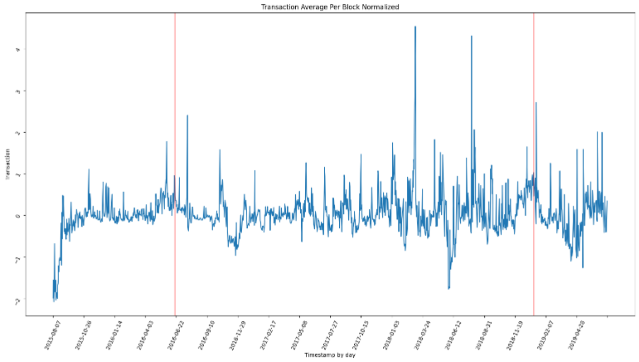

Fig. 12. Relationship of Transaction Average per Block with Timestamp after normalization.

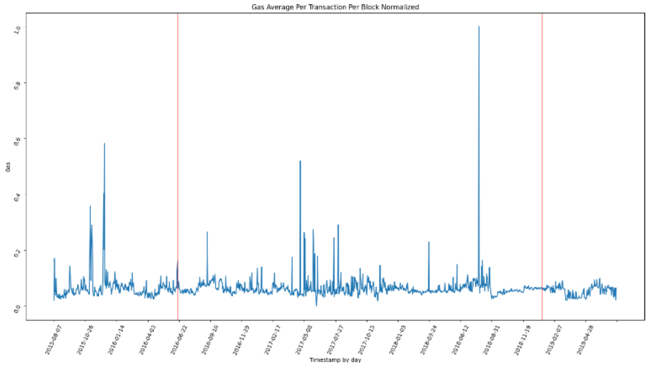

Fig. 13. Relationship of Gas Average Per Transaction Per Block with Timestamp after normalization.

The second part of the results involves the model training process. Fig. 14 shows the training loss for both training (orange) and testing (blue), where it is noticed that the presented model completely handles overfitting as a result of the L2 regularization with a value of 0.02 and the two dropout layers. A dropout rate of 0.8 is considered high enough to address overfitting, so the overfitting ratio was nearly zero from the beginning to the end of the training. However, this will affect the model's accuracy, making it lower than usual or expected, which is also compensated for by data scanning and pre-processing. Therefore, the model with almost have no overfitting and achieve high accuracy.

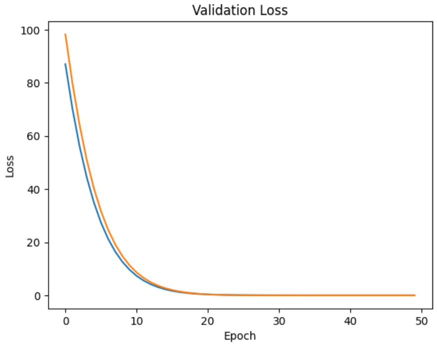

Fig. 14. Training and Validation Loss.

Fig. 15 shows the results of testing the proposed model on the test data, which includes attack data consistent with the reference study 1 [37]. This data includes a set of natural data over a period of time. Within these time periods, there will be attack data. This model output shows that the data marked by the red lines are attack data, while the rest of the data is natural. The test results show that the pre-processing and the proposed model give good performance for detecting logger anomalies on the network. Within the test data, it is worth noting that the test accuracy of the proposed model is 0.995.

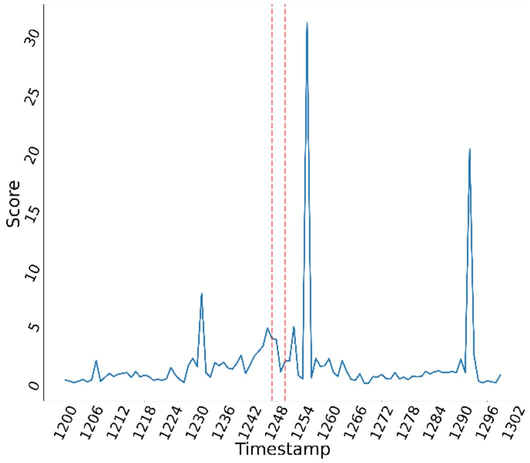

Fig. 15. Results obtained by the proposed model.

VIII. Discussion

Fig. 16 and Fig. 17 represent a comparison between the results obtained in this study and the results found in study 1 [37] and study 2 [38]. The red line represents attack data, while the other data points represent normal data. In both our model and the reference study, the horizontal axis represents the timestamp, while the vertical axis represents a parameter from the database, such as average gas. As we can see, there is a difference because we applied preprocessing to our data, while the reference study used a different preprocessing method. Therefore, there is a slight difference in the data representation. However, both studies practically cover the same time period. We also observed that both models identify attack data during the same time periods. The difference lies in the fact that our model achieved higher accuracy in testing, i.e. in classifying this data as either attack or natural.

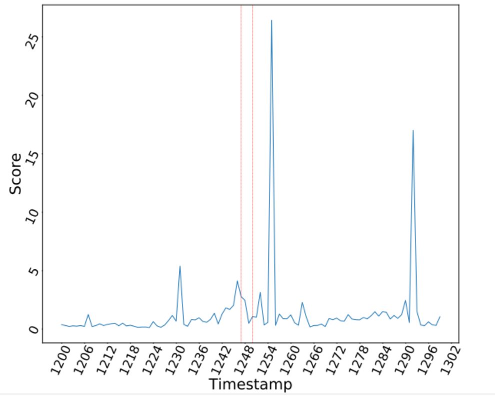

Fig. 16. Comparison of Results with reference Study 1 [37].

The anomaly detection results of the proposed model and results of Study 2 are shown in Fig. 17.

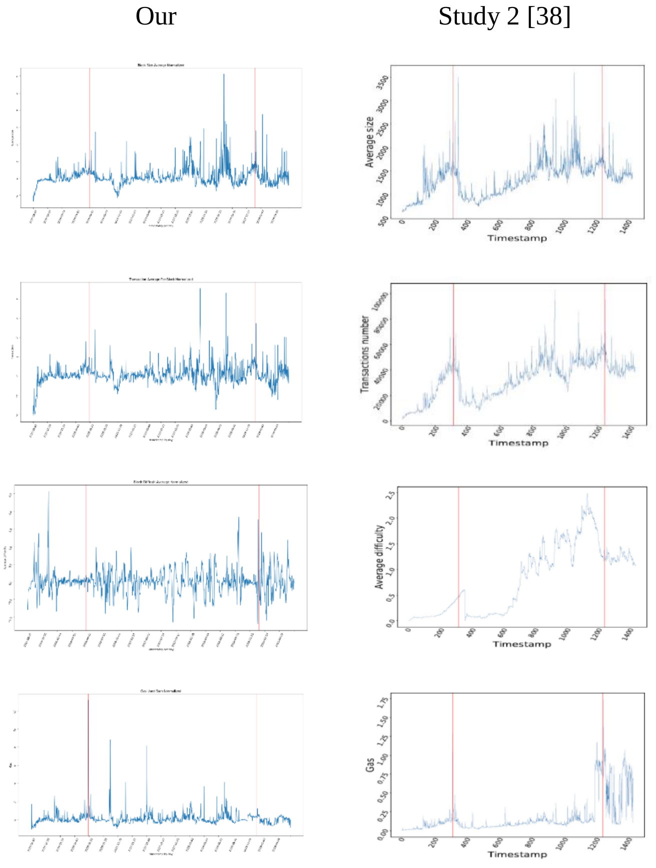

Fig. 17. Comparison of results with reference study 2 [38].

As a result, the proposed model shows the ability to predict the detection of anomalies for activities recorded on the network. It also efficiently addresses the challenge of overfitting during model training. It also achieves a prediction accuracy rate of 0.995 for the model on test data. Compared with reference studies, we find that the proposed model has the ability to capture dependencies. It is time efficient and has the ability to detect attacks on the network. For further development, we recommend using more general training data, as well as testing transformers on this type of challenges.

IX. Open Issues and Research Challenges

Open issues and research challenges in the field of enhancing the security of digital financial and banking transactions through blockchain-enabled approaches, particularly the implementation of a Long Short-Term Memory (LSTM) model, remain to be addressed. One of the key challenges is the need to develop more sophisticated anomaly detection techniques to effectively identify and mitigate potential threats in network-recorded activities. Additionally, there is a requirement for further exploration of the scalability and performance implications of using blockchain technology in large-scale financial systems, as well as the development of robust security systems to withstand evolving cyberattacks. Furthermore, the integration of blockchain technology with existing regulatory frameworks and compliance standards poses legal and regulatory challenges that need to be addressed for widespread adoption. These open issues call for continued research and collaboration among academia, industry, and regulatory bodies to ensure the successful implementation and utilization of blockchain-enabled security solutions in the realm of digital financial and banking transactions.

X. Conclusion

Blockchain has shown to be a revolutionary technology, but its widespread adoption has been hampered by a number of restrictions. Our project focused on enhancing the security of digital financial and banking transactions using blockchain technology. It addresses the challenges faced by the banking industry, such as inefficiency, high fraud rates, and lack of transparency, and proposes a solution through the implementation of blockchain. The research aims to develop an analytical model capable of detecting attacks and anomalies on the Ethereum Classic (ETC) blockchain by employing an Encoder-Decoder LSTM architecture. The study emphasizes the importance of cybersecurity in the banking sector and the potential of blockchain technology to revolutionize the industry by providing a secure, efficient, and transparent platform for financial transactions. The thesis outlines the methodology used, the results obtained, and the contributions made to the field of blockchain security. It concludes with suggestions for future research directions, highlighting the ongoing need for innovation in the realm of digital financial security.

The project's findings revealed that adding machine learning and blockchain technology may significantly improve and refine numerous security sectors. However, this study is simply the beginning of a broader and more extensive inquiry into this type of integration, underlining the need for more research that looks into numerous authentication elements across diverse datasets to balance security and usability.

Future work will focus on addressing the scalability of the proposed LSTM model within larger decentralized financial ecosystems, particularly those operating on multiple blockchain platforms. Additionally, further research will explore the integration of reinforcement learning techniques to enhance real-time anomaly detection. Another promising avenue is the application of this model to emerging blockchain networks to determine its effectiveness in varied contexts. Extending the study to multi-blockchain scenarios could also provide insights into cross-network security enhancements.

Acknowledgment

The authors would like to thank the Deanship of Graduate Studies and Scientific Research at Jouf University for funding and supporting this research through the initiative of DGSR, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] M. Casey and P. Vigna, "In blockchain we trust," MIT Technol. Rev., 2018.

[3] "Bitcoin BTC," Coinmarketcap, 2022. [Online]. Available: https://coinmarketcap.com/.

[4] T. I. Team, "Ethereum Classic (ETC) definition, history, future," Investopedia, 31 May 2023. [Online]. Available: https://www.investopedia.com/terms/e/ethereum-classic.asp. [Accessed: Mar. 21, 2024].

[5] M. Paige, "The evolution of digital transformation: From pre-internet to post-pandemic," Hatchworks, 3 Feb 2023. [Online]. Available: https://hatchworks.com/blog/product-design/history-digital-transformation/. [Accessed: Mar. 21, 2024].

[6] M. Kirmani and M. T. Banday, "Digital forensics in the context of the Internet of Things," in Cryptographic Security Solutions for the Internet of Things, 2019, pp. 296-324.

[7] A. Demirgüç-Kunt, "Is bank competition a threat to financial stability?," World Bank, 10 Apr 2012. [Online]. Available: https://blogs.worldbank.org/en/allaboutfinance/is-bank-competition-a-threat-to-financial-stability. [Accessed: Mar. 21, 2024].

[8] M. U. Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," arXiv, 2022.

[9] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of blockchain technology applications for financial services," BenchCouncil Trans. Benchmarks, Standards, and Evaluations, vol. 2, 2022.

[10] S. Trivedi, K. Mehta, and R. Sharma, "Systematic literature review on application of blockchain technology in E-finance and financial services," J. Technol. Manage. Innov., vol. 16, no. 3, pp. 89-102, 2021.

[11] J. Hartmann and O. Hasan, "Privacy considerations for a decentralized finance (DeFi) loans platform," Cluster Comput., vol. 26, no. 4, pp. 2147-2161, 2023.

[12] C. H. Liao, X. Q. Guan, J. H. Cheng, and S. M. Yuan, "Blockchain-based identity management and access control framework for open banking ecosystem," Future Gener. Comput. Syst., vol. 135, pp. 450-466, 2022.

[13] D. Boughaci and A. A. Alkhawaldeh, "Enhancing the security of financial transactions in blockchain by using machine learning techniques: Towards a sophisticated security tool for banking and finance," in Proc. 2020 1st Int. Conf. Smart Syst. Emerg. Technol. (SMARTTECH), 2020, pp. 110-115.

[14] H. Song and Y. Chen, "Digital financial transaction security based on blockchain," J. Phys.: Conf. Ser., vol. 1744, 2021.

[15] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A low-cost S-box for the advanced encryption standard using normal basis," in Proc. IEEE Int. Conf. Electro/Inf. Technol., 2009.

[16] K.-K. R. Choo, M. M. Kermani, R. Azarderakhsh, and M. Govindarasu, "Emerging embedded and cyber physical system security challenges and innovations," IEEE Trans. Depend. Secure Comput., vol. 14, no. 3, pp. 235-246, 2017.

[17] M. Mozaffari-Kermani, R. Azarderakhsh, C.-Y. Lee, and S. Bayat-Sarmadi, "Reliable concurrent error detection architectures for extended Euclidean-based division over GF(2m)," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 22, no. 5, pp. 995-1003, 2014.

[18] A. Jalali, R. Azarderakhsh, M. M. Kermani, and D. Jao, "Towards optimized and constant-time CSIDH on embedded devices," in Proc. Springer, vol. 11421, pp. 215–231, 2019.

[19] B. Koziel, R. Azarderakhsh, and M. Mozaffari-Kermani, "Low-resource and fast binary Edwards curves cryptography," in Proc. Springer, vol. 9462, pp. 347–369, 2015.

[20] J. Xue, X. Jiang, P. Li, W. Xi, C. Xu, and K. Huang, "Side-channel attack of lightweight cryptography based on MixColumn: Case study of PRINCE," Electronics, vol. 12, no. 544, 2023.

[21] A. Benjamin, J. Herzoff, L. Babinkostova, and E. Serra, "Deep learning based side channel attacks on lightweight cryptography (student abstract)," in Proc. AAAI Conf. Artif. Intell., 2022.

[22] C. Su and Q. Zeng, "Survey of CPU cache-based side-channel attacks: Systematic analysis, security models, and countermeasures," Secur. Commun. Netw., vol. 2021, no. 1, pp. 1-15, 2021.

[23] R. Walters, Blockchain technology and the future of banking, Robert Walters, 2021.

[24] PinkExc, "PinkExc," Twitter, 11 Oct 2019. [Online]. Available: https://twitter.com/pinkexc/status/1182550209944944640. [Accessed: May 2024].

[25] W. Kersten, T. Blecker, and C. Ringle, "Digitalization in supply chain management and logistics: Smart and digital solutions for an Industry 4.0 environment," in Hamburg Int. Conf. Logist. (HICL), Berlin, 2017.

[26] CIP, "CIU's must use blockchain technology for working together and share data, citizen by investment," CIP J., 2018.

[27] K. C. Tran and J. Benson, "What is Ethereum Classic?," Decrypt, 2 Feb 2022. [Online]. Available: https://decrypt.co/resources/what-is-ethereum-classic-explained-guide-cryptocurrency. [Accessed: Mar. 27, 2024].

[28] E. Erdmann, Strengths and drawbacks of voting methods for political elections, University of Minnesota, 2011.

[29] S. Park and R. Rivest, "Towards secure quadratic voting," Eprint, 2016.

[30] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, "Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis," arXiv, 2024.

[31] D. Kaidalov, L. Kovalchuk, A. Nastenko, M. Rodinko, O. Shevtsov, and R. Oliynykov, "Ethereum Classic treasury system proposal," Input | Output, 2017.

[32] J. Li, C. Gu, F. Wei, and X. Chen, "A survey on blockchain anomaly detection using data mining techniques," in Blockchain and Trustworthy Systems, 2020, pp. 491-504.

[33] G. BigQuery, M. Risdal, A. Day, and Y. Khoury, "Ethereum Classic blockchain," Kaggle, 2019. [Online]. Available: https://www.kaggle.com/datasets/bigquery/crypto-ethereum-classic?select=transactions. [Accessed: Apr. 22, 2024].

[34] MathWorks, "How Deep Learning HDL Toolbox compiles the LSTM layer," [Online]. Available: https://www.mathworks.com/help/deep-learning-hdl/ug/how-deep-learning-hdl-toolbox-compiles-the-lstm-layer.html. [Accessed: Apr. 22, 2024].

[35] A. Zhang, Z. C. Lipton, M. Li, and A. J. Smola, "Multi-head attention," in Dive into Deep Learning, Cambridge University Press, 2023.

[36] Google Colab, "Multihead-attention.ipynb," 2021. [Online]. Available: https://colab.research.google.com/github/deepjavalibrary/d2l-java/blob/colab/chapter_attention-mechanisms/multihead-attention.ipynb. [Accessed: Apr. 22, 2024].

[37] F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco, and G. Manco, "A deep learning approach for detecting security attacks on blockchain," in Proc. 4th Italian Conf. Cyber Secur. (ITASEC), Ancona, Italy, 2020.

[38] S. Dhandapani and G. Maragatham, "Design of blockchain-enabled intrusion detection model for detecting security attacks using deep learning," Pattern Recognit. Lett., vol. 153, 2021.