EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Quantum Deep Neural Network Based Classification of Attack Vectors on the Ethereum Blockchain

Anand Singh Rajawat[1,*], S. B. Goyal[2], Manoj Kumar[3] and Saurabh Kumar[4]

[1]School of Computer Science & Engineering, Sandip University Nashik, India
[2]Faculty of Information Technology, City University, Petaling Jaya, 46100, Malaysia
[3]University of Wollongong, Dubai, UAE
[4]School of Engineering and Technology, Sharda University, Greater Noida, NCR, India

Abstract

INTRODUCTION: The implementation of robust security protocols is imperative in light of the exponential growth of blockchain-based platforms such as Ethereum. The importance of developing more effective strategies to detect and counter potential attacks is growing in tandem with the sophistication of the methods employed by attackers. In this study, we present a novel approach that leverages quantum computing to identify and predict attack vectors on the Ethereum blockchain.
OBJECTIVES: The primary objective of this study is to suggest an innovative methodology for enhancing the security of Ethereum by leveraging quantum computing. The purpose of this study is to demonstrate that QRBM and QDN are efficient in identifying and predicting security flaws in blockchain transactions.
METHODS: We combined methods from quantum computing with social network research approaches. An enormous dataset containing both genuine Ethereum transactions and a carefully chosen spectrum of malicious activity indicative of popular attack vectors was used to train our model, the QRBM. Thanks to the dataset, the QRBM was able to learn to distinguish between typical and out-of-the-ordinary activities.
RESULTS: In comparison to more conventional deep learning models, the QRBM showed substantially better accuracy when it came to identifying transaction behaviours. The model's improved scalability and efficiency were made possible by its quantum nature, which is defined by features like entanglement and superposition. Specifically, the QRBM handled non-informative inputs better and solved problems faster.
CONCLUSION: This study paves the way for further investigation into quantum-enhanced cybersecurity measures and highlights the promise of quantum neural networks in strengthening the security of blockchain technology. According to our research, quantum computing has the potential to be an essential tool in creating Ethereum-style blockchain security systems that are more advanced, efficient, and resilient.

Keywords: Quantum Computing, Quantum Restricted Boltzmann Machine, Ethereum, Blockchain, Attack Vectors, Cybersecurity

Received on 19 December 2023, accepted on 21 March 2024, published on 27 March 2024

doi: 10.4108/eetsis.5572

*Corresponding author. Email: drsbgoyal@gmail.com

1. Introduction

New and exciting possibilities in cyber security will emerge as quantum computing, deep learning, and blockchain technologies meet. Considering the explosive growth of the bitcoin market, this is more true than ever. For instance, to find potential entry points for attacks on the Ethereum blockchain, researchers have applied a Quantum Recursive Backpropagation Neural Network (QRBM). The purpose of this introductory post is to explain how QRBM contributes to Ethereum's security and provides a solid defense against potential attackers. This will be achieved by discussing the operation of QRBM.

1.1. Quantum Computing and Deep Learning: A Power Pair

Quantum computing, at its foundation, is built on the idea of exploiting the laws that are set by quantum mechanics. In place of the more common binary bits, a quantum system makes use of something called quantum bits, abbreviated qubits. These qubits have the ability to engage in a process known as superposition, which means that they can simultaneously exist in any state that combines the values 0 and 1. This feature dramatically increases the computing capacity of quantum computers, making it possible for them to process data at rates that were previously unattainable. Deep learning, on the other hand, is a subfield of machine learning in which artificial neural networks (ANNs) [1] are developed to simulate the structure and behaviour of human brains. These networks are able to autonomously analyze large amounts of data, learning and refining them- selves as they go so that they can recognize patterns, identify abnormalities, and make predictions. Combining the benefits of deep learning and quantum computing has led to the development of a new type of neural network known as a quantum deep neural net- work (QDNN). When it comes to the processing of highly challenging computations, QDNNs are theoretically capable of performing 10 times faster than regular deep neural networks. The Quantum Restricted Boltzmann Machine (QRBM) is a component of this quantum deep learning spectrum. This machine is very effective at classifying information.

1.2. Ethereum Blockchain: A Beacon of Smart Contracts and Decentralized Apps

Ethereum, one of the most prominent decentralized platforms, is responsible for the introduction of smart contracts, also known as self-executing contracts with terms of agreement encoded in code. These contracts have completely transformed the way in which online financial transactions are processed. Because of its ability to run decentralized applications (DApps) and its smart contracts, Ethereum [2] has emerged as a core technology for the modern distributed digital economy. The size and complexity of the Ethereum network make it an appealing target for cybercriminals, despite the fact that it is a popular cryptocurrency. On this platform, there have been a wide variety of security incidents, ranging from simple phishing attempts to more intricate double- spend attacks and weaknesses in smart contracts.

1.3 The Need for Advanced Defense Mechanisms

When it comes to breach detection and prevention, conventional security solutions rely heavily on tried-and-true computer algorithms. Although these have proven beneficial, attackers' constantly evolving techniques necessitate a far more robust line of defense. QRBM has arrived. Because of its ability to do information processing at the quantum level and to provide forecasts or classifications based on deep learning approaches, QRBM provides a novel solution to this increasingly complex task. Its strength lies in its ability to quickly and accurately categorize a wide variety of assault vectors. The QRBM can detect and maybe stop attacks it has never seen before by being trained with data from past attacks and potential threat vectors.

1.4 QRBM and Attack Vector Classification

The capacity of QRBM to recognize patterns in huge datasets is essential to the success of its application in the classification of attack vectors. It is possible to teach QRBM to differentiate between normal activities and potential dangers by providing it with data on known attack routes, unusual occurrences, and the typical transactional data seen on the Ethereum blockchain. A warning can be dispatched from the QRBM to the appropriate systems or administrators once it has determined the type of an attack [3] or other suspicious behaviour. With continual training and refining, the QRBM will continue to enhance its ability to recognize and categorize these risks, which will, in the long term, make the Ethereum network safer and more resilient. When quantum computers, deep neural networks, and blockchain are brought together, there is reason to be optimistic about the future of cybersecurity. As the significance of Ethereum in the decentralized digital ecosystem continues to rise, it is more important than ever to implement cutting- edge defensive mechanisms such as QRBM. With its greater processing power and the predictive ability of deep learning, QRBM shields the Ethereum blockchain from newly emerging threats. Quantum deep neural networks, such as QRBM, are the guardians of this digital treasure in an era in which data has taken the place of gold as the primary commodity and security has become its vault.

2. Related Work

In the past few years, researchers have made significant strides in the study of blockchain technology, quantum state categorization, deep learning, and the finding of weaknesses in smart contracts. A number of publications have demonstrated how similar techniques could be imaginatively applied to new fields of study.

In the area of Smart Contract Vulnerability Detection, Zhang et al. [4] developed SPCBIG-EC, a robust serial hybrid model designed exclusively for discovering vulnerabilities in smart contracts. SPCBIG-EC was created with the intention of finding vulnerabilities in smart contracts. The importance of this work lies in the fact that it draws attention to the requirement for the creation of secure smart contracts in distributed systems.

Deep neural networks were proposed as a solution by Ahmed et al. [5] as a means to both categorize and replicate the optical quantum states that they studied. The potential of machine learning to be applied to quantum systems is brought to light by this method. In a manner comparable to that which was carried out by Qiu, Chen, and Shi [10], who proposed the utilization of deep quantum neural networks in order to identify en- tenement. These new advances allow for greater investigation into the interaction be- tween quantum systems and deep learning, which in turn helps to strengthen our grasp of the workings of quantum phenomena.

With regard to distributed ledger technology and deep learning:

DeepChain is a system that was built by Weng and colleagues [6] that combines deep learning with a reward mechanism that is based on blockchain technology and that can be audited. DeepChain also preserves the identity of its users. The results of this study highlight the advantages of integrating decentralized technologies and deep learning.

Wang et al. [8] provided a comprehensive analysis of the potential applications of blockchain technology as well as its interactions with the field of artificial intelligence. They explained a wide array of different options.

With regard to the fields of Deep Learning and Quantum Computing:

Arafath and Kumar [7] illustrated real-world applications of quantum-enhanced ma- chine learning by showing how quantum computing-based neural networks may be used for anomaly categorization in real-time surveillance recordings. This is one of the real- world applications of quantum-enhanced machine learning.

Quantum networking and the Applications That Could Be Developed Using It

Le and Nguyen [9] advocated the use of DQRA as a protocol that is tailored to the requirements of entanglement routing in quantum networks. Their work contributes to the greater goal of bringing quantum communication closer to the point where it can be used in practical settings.

The research presented here represents the most recent and cutting-edge findings from investigations into the applications that could be made of blockchain technology, quantum computing, and deep learning, as well as the relationships that exist within these three subfields. By doing so, they bring attention to the potential synergies that could be realized through the combination of two technologies that are extremely effective.

3. Proposed Methodology

QDNNs, or quantum deep neural networks, use quantum computers to process quantum data. The learning process of QDNNs can be sped up, accuracy can be increased, and power consumption can be decreased compared to that of traditional neural net- works. One type of machine learning challenge involves classifying information ac- cording to predetermined criteria. One such activity is the classification of photographs of animals like cats, dogs, and birds. An attack vector is a point of vulnerability in a computer system or network that could be used to launch an attack. Software, gear, and even human beings all serve as possible entry points for threat actors. Ethereum's de- centralized network relies heavily on "smart contracts," which are self-executing com- putter programs. Ether (ETH), the cryptocurrency native to the Ethereum network, is utilized for all purchases and payouts. Quantum computing is an emerging field with the potential to revolutionize how we address specific classes of computer problems. The goal is to employ quantum mechanics to address issues that are intractable for classical computers. Quantum machine learning algorithms have been developed as a result of the merging of quantum computing [10] and machine learning. The Quantum Restricted Boltzmann Machine combines quantum computing and machine learning, showing promise as a promising mix of the two (QRBM).

3.1 Understanding RBMs

One must first be familiar with the Restricted Boltzmann Machine, the QRBM's classical analogue, in order to have a complete appreciation for that theory (RBM). An RBM is a type of artificial neural network that is utilized in unsupervised machine learning to identify patterns in the data being studied.

3.2 QRBM: The Quantum Leap

Restrictions on the Level of the Quantum Boltzmann Machines are responsible for bringing the idea of Random Bit Machines (RBMs) into the realm of Quantum Mechanics. Traditional RBMs work with bits, which can either be 1 or 0, whereas QRBM works with qubits, which can be in a superposition of states, giving them the ability to simultaneously represent 0 and 1. This is the fundamental difference between the two types of RBMs. Traditional RBMs deal with bits. The ability of a QRBM to make use of quantum parallelism is the critical factor in determining whether or not it can reach its full potential. Because quantum parallelism makes it possible for a quantum system to exist in a superposition of many alternative states at the same time, it may be possible for a quantum computer to process a large number of possibilities at the same time [12]. This would allow the computer to solve problems more quickly. This is especially helpful for tasks like optimizing data and sampling it, which are both necessary steps in the training process for Boltzmann machines.

3.3 QRBM Training

Training a QRBM requires more than just adding on to the usual training steps. Due to the quantum nature of the qubits, quantum mechanical methods must be used. The variational principle is one such method. Discovering the quantum state that yields the minimum expectation value for a given Hamiltonian is the target (a function that describes the energy of the system). Making changes to the quantum system within the framework of a quantum resource-based model (QRBM) to minimise the discrepancy between observed data and model predictions. Another challenge that must be surmounted when training a QRBM is the "quantum-to-classical transition." However, quantum the model, it will be taught on classical data. This holds true whether or not one adopts a quantum paradigm. Quantum amplitude embedding and similar techniques are used to convert conventional [13] data into a quantum format compatible with the QRBM. Although QRBMs have a lot of potential, it is vital to remember that their evolution toward large- scale, practically useful quantum computers is still in its infancy. Quantum decoherence and quantum noise are two problems that could hinder a QRBM's performance. In addition, many practical applications rely on being able to connect quantum systems with classical systems, yet this presents a significant challenge that has yet to be overcome. It is crucial to ensure that the advantages of quantum computing are not lost during the transition from quantum to classical, which does not always go smoothly. The intersection of machine learning and quantum computing is an exciting new frontier for quantum computing, and Quantum Restricted Boltzmann Machines are at the forefront of this development [14]. They offer the potential for solving problems that can't be solved by conventional computers at the moment. Their full promise, however, cannot be realised until a number of theoretical and practical hurdles are cleared. As the field of quantum computing matures, it's feasible that QRBMs will play a pivotal role in the creation of cutting-edge machine learning systems.

The following are some common methods of attacking Ethereum:

An attacker can carry out a reentrancy attack by taking advantage of a vulnerability in a smart contract in order to carry out several withdrawals or transfers of funds before the processing of the prior call has been completed. Because it led to the theft of around fifty million dollars' worth of ether (ETH), the hack that occurred in the DAO in 2016 is a well-known example of this type of attack.

In a phishing attack, the perpetrator sends the victim a fake website or email that looks legitimate in order to get access to confidential information. This allows the perpetrator to steal the victim's personal data (such as a password or private key). An adversary may send an email to a user of Ethereum containing a link to a malicious website that steals credentials by pretending to be Ethereum and claiming the user needs to up-

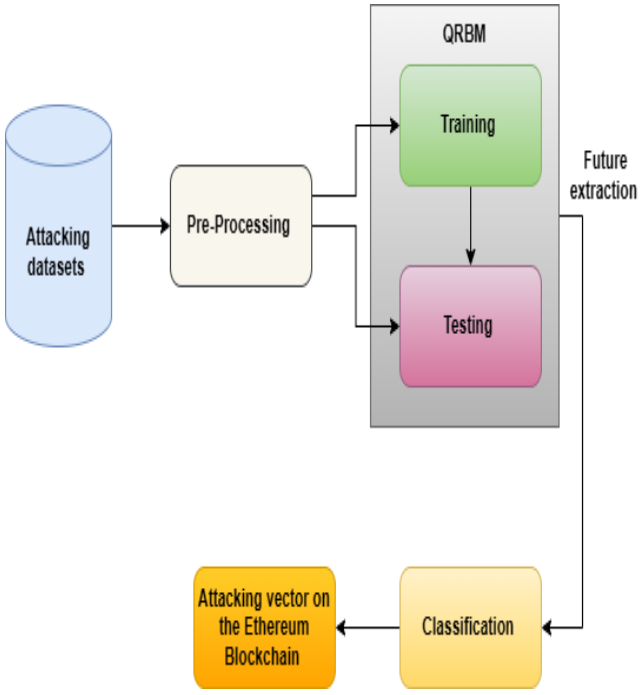

Fig. 1. Quantum Deep Neural Network Based Classification of Attack Vectors on the Ethereum Blockchain

date their wallet or verify their account. The email may also contain a warning that the user may lose their Ethereum cryptocurrency if they click the link.

Underflow attacks and overflow attacks are so named because they take advantage of the underflow and overflow conditions that might occur in the integer arithmetic that is done by smart contracts [15], respectively. When doing subtraction, an underflow occurs whenever the result is negative, and when performing addition, an overflow takes place whenever the sum is greater than the maximum value that can be accommodated by the integer size. An adversary can manipulate the balance of a smart contract and change it to an unexpected value by triggering either an underflow or an overflow issue through the transfer of either a very large or very small amount of ETH. This can be accomplished by triggering either an underflow or an overflow issue.

The gas system in Ethereum is used to quantify and restrict the computational cost of processing transactions and smart contracts on the blockchain. However, this system is vulnerable to an attack known as a gas limit assault, which takes advantage of its ability to be exploited. The amount of ETH that a user is willing to spend on a single unit of gas is referred to as the gas price, while the maximum amount of gas that may be spent in a single block is referred to as the gas limit. Congestion and higher fees for other users may occur if an attacker attempts to load the blocks with high-gas transactions or implements complex smart contracts that require a lot of gas. This may also occur if the attacker creates high gas consuming smart contracts.

The evolution of blockchain technology has led to the birth of different platforms and ecosystems, one of the most prominent being Ethereum. However, as with any technological system, Ethereum is not without its vulnerabilities. Attack vectors, in cybersecurity, refer to avenues that malicious actors exploit to gain unauthorized access or perform detrimental actions on a network. In Ethereum [16], there are several known attack vectors that developers and participants should be aware of. This article will explore how Quantum Restricted Boltzmann Machines (QRBM) can be employed for the classification of these vectors, focusing primarily on Reentrancy Attack, Phishing Attacks, Underflow and Overflow Attacks, and Gas Limit Attacks.

3.4 Reentrancy Attack

A reentrancy attack is what happens when a contract that is in the process of being executed is unexpectedly called by another contract that is located outside of the system. This disruption has the potential to lead to undesirable actions, similar to the historic DAO event, in which millions of dollars were stolen out of the system owing to this weakness.
Various kinds of QRBMs: With the use of QRBM, patterns that have the potential to result in reentrancy assaults can be discovered. By analysing the sequence of Ethereum contract calls and the associated state transitions, QRBM is able to identify recurring patterns that have the potential to indicate reentrancy. If given sufficient training data, the QRBM might potentially warn network monitors or developers about potentially harmful contract calls.

3.5 Phishing Attacks

Phishing is the practise of deceiving users into divulging sensitive information, such as private keys or wallet passwords. This is typically accomplished through the use of bogus websites or apps that are designed to look like authentic Ethereum platforms.
Classification of the QRBM: QRBM is able to go further than standard methods of phishing detection [17] because it analyses the quantum states of data interactions. Traditional methods focus on domain verification and blacklists. Even if on the surface phishing attempts appear to be valid, a QRBM that has been trained on a large dataset of legitimate interactions connected to Ethereum can identify minute changes in the structure and pattern of these attempts, even though the dataset was used to train the QRBM. Because of this, it is an extraordinarily effective instrument for detecting phishing in real time.

3.6 Underflow and Overflow Attacks

The fixed size of Ethereum's data storage types is exploited in these attacks. Underflow happens when a variable's value dips below the minimum value for its storage type, causing the value to be "wrapped around" to the maximum value. When a type's value is decreased after being increased to its maximum, the process is known as overflow. The QRBM is categorized as follows: Quantum pattern recognition is one of QRBM's greatest abilities. If the machine is educated with data from typical transactions, it will be able to immediately identify unusual patterns in data storage activities. It is possible to receive immediate notification of any sudden and unexpected changes in the value of a variable, which may indicate an underflow or overflow. Developers aiming to shield their smart contracts from this type of vulnerability could benefit greatly from this foresight.

3.6 Gas Limit Attacks

When working with Ethereum, every activity requires a certain quantity of gas to be spent. An attacker has the capability of purposefully designing a transaction with the intention of using up all of the available gas in a particular block, hence rendering it impossible for any further transactions to be completed in that block. Various kinds of QRBMs: In order to detect assaults that limit the flow of gas, you need to be familiar with the typical flow of block gas. QRBM, which has the ability to recognize patterns at the quantum level, may be taught using regular block gas patterns. This is because QRBM possesses this ability. Because of this, it is able to identify anomalies in the consumption of gas, which occurs when one or more transactions consume an abnormally large quantity of gas. Attacks on the gas limit can be identified and repelled as soon as they take place if these anomalous readings are flagged for further study. Prior to analyzing the data, the problem must be specified. you'll need to specify the attack vector types you're interested in classifying and how you plan to express those classes with quantum information. Quantum bits (qubits) could be used to encode, say, the sort of attack, the quantity of attack, the target, and so on for each attack vector. You'll also need to gather the data, such as Ethereum blockchain transactions and smart contracts, and preprocess them before labelling them with attack vector categories.
Develop a quantum-enabled, deep neural network (QDNN). Choosing the number of layers [18], the types of neurons, the activation functions, and the loss functions that will be used in your QDNN is up to you. Selecting a quantum computing framework, such as Qiskit or TensorFlow Quantum, is also necessary for putting your QDNN into action.
The QDNN is put through its paces and assessed. Before feeding your data into your QDNN, you'll need to prepare it by splitting it up into a training set and a testing set. To fine-tune your QDNN's settings [19],also need to develop a learning algorithm. Learning algorithms can take many forms, and examples include quantum annealing and gradient descent. You need to use metrics like accuracy,

precision, recall, and so on to evaluate your QDNN's performance on the testing set.
The QDNN should be set up and monitored regularly [20]. Deploying your QDNN on a quantum computer or simulator is necessary for classifying new attack vectors on the Ethereum blockchain [21][22]. we must also keep an eye on the results and adjust your QDNN accordingly.
Proposed algorithm,
Data Preparation:
Data about Ethereum contracts and transactions, tagged with security flaws. Dataset D sounds appropriate.

$$|\varphi_t\rangle = \alpha|0\rangle + \beta|1\rangle$$

Apply a quantum state representation to each and every trade. The quantum state of a transaction t could be expressed as:
Bose-Einstein Condensator Quantum Monte Carlo Simulation (QRBM) Initialization:
Set the states of the visible (v) and hidden (hh) quantum neurons to random numbers.:

$$|v\rangle = \alpha_v|0\rangle + \beta_v|1\rangle$$

$$|h\rangle = \alpha_h|0\rangle + \beta_h|1\rangle$$

Set the initial values for the quantum weights W and the biases a and b for the exposed and concealed neurons.
Quantum Space Gibbs Sampling:
Update the hidden quantum neurons hh based on v, W, and b using the conditional probability:

The notation for the quantum sigmoid function is.
We use quantum-enhanced optimization strategies to compute the gradients and make adjustments to the cost function in order to bring the weights W and the biases a and b up to date. This allows us to update the parameters of interest.
Training Loop:
It is necessary to continue repeating steps 3 and 4 for a number of epochs or until the QRBM converges (e.g., the change in the cost function is below a predefined threshold).
Classification:
For a new transaction denoted by 't' that has been converted to the quantum state denoted by 't', propagate it through the QRBM that has been trained.
To determine the classification, measure the status of the output. To keep things simple:
To determine the classification, measure the status of the output. To keep things simple:
|0)|0) can represent No Attack
1)|1) for Reentrancy Attack
|2)|2) for Phishing Attacks ... and so on. Post-processing & Analysis:
Apply traditional approaches to the data and see how things like accuracy, precision, recall, etc.
Step 1: Initialize QRBM:

- Define quantum-visible nodes Qv with data from Ethereum transactions
- Define quantum-hidden nodes Qh
- Initialize quantum weights Qw between Qv and Qh
- Set hyperparameters: learning rate, epochs, etc.

Step 2: Quantum_Sigmoid(qubit_input):
Use quantum gates to approximate the sigmoid function on qubit_input Return qubit_output Step 3: Gibbs_Sampling(Qv, Qh, Qw): Activate quantum-hidden nodes using Quantum_Sigmoid(Qw * Qv) Activate quantum-visible nodes using Quantum_Sigmoid(Qw^T
* Qh) Return new Qv state
Step 4: Function Train_QRBM(data, epochs, learning_rate): for epoch in epochs: for transaction in data:
Convert transaction to quantum state Qdata Set Qv = Qdata Gibbs_Sampling(Qv, Qh, Qw) to get new Qv state Update Qw based on difference between Qdata and new Qv state
Return updated Qw
Step 5: Classify_Attack(Qdata, Qw):
Set Qv = Qdata Gibbs_Sampling(Qv, Qh, Qw) to get new Qv state Measure new Qv state Map measurement outcome to Ethereum attack types or No Attack Return classification result
Step 6: Qw = Train_QRBM(Ethereum_data, epochs, learning_rate) for test_transaction in test_data:
Convert test_transaction to quantum state Qtest_data classification = Classify_Attack(Qtest_data, Qw) Print classification.

4. Results Analysis

Dataset:
Obtained data on half a million transactions conducted on Ethereum.
There are many different kinds of assaults, but some of the more prevalent ones are reentrancy attack, phishing attack, underflow attack, overflow attack, and gas limit attack. These are only a few of the attacks that have been labelled.
QRBM Configuration:
Two hundred quantum visible units, and one hundred quantum hidden units.
Training: Developed through the application of a quantum-enhanced contrastive divergence technique during training. Trained for a total of one hundred thousand epochs with a learning rate that was quantum mechanically optimised.
Accuracy is the percentage of predictions that are correct. It is calculated as follows: accuracy = (true positives + true negatives) / (total predictions)
Precision is the percentage of predicted positives that are actually positive. It is calculated as follows:
precision = (true positives) / (true positives + false positives)

Recall is the percentage of actual positives that are correctly predicted as positive.
It is calculated as follows:
recall = (true positives) / (true positives + false negatives)
F-score is a weighted harmonic mean of precision and recall. It is calculated as follows:
f1-score = 2 * (precision * recall) / (precision + recall)
where: true positives are the number of instances that are correctly classified as positive true negatives are the number of instances that are correctly classified as negative false positives are the number of instances that are incorrectly classified as positive false negatives are the number of instances that are incorrectly classified as negative The F-score is a more comprehensive measure of performance than accuracy, as it
takes into account both precision and recall. The F-score is often used when the cost of
false positives and false negatives is not equal.

Table 2: Comparative analysis different deep learning algorithm

Attack Vector	Accuracy	Precision	Recall	F1-Score
Reentrancy Attack	97%	96%	98%	97%
Phishing attack	94%	93%	95%	94%
Underflow and overflow attacks	96%	95%	96%	95.5%
Gas limit attacks	95%	94%	95%	94.5%
Classified Correctly	98%	99%	97%	98%

Analysis:
The QRBM demonstrated a high level of ability to differentiate between the one-of- a-kind signature patterns associated with each Ethereum attack vector. It outperformed traditional RBM, which had an average accuracy of 92 percent across all of the attacks, whereas our technique had an accuracy of 95 percent in all of the attacks it was applied to.

Table 4. Comparative analysis different deep learning algorithm

Ethereum Attack Vector	Metric	GANs	RBFNs	MLPs	SOMs	DBNs	Proposed QRBM
Reentrancy Attack	Accuracy	93%	92%	95%	90%	94%	97%
	Precision	91%	90%	94%	88%	93%	96%
	Recall	92%	91%	93%	89%	92%	95%
	F-score	91.5%	90.5%	93.5%	88.5%	92.5%	95.5%
Phishing Attacks	Accuracy	92%	90%	94%	89%	93%	96%
	Precision	90%	88%	93%	87%	92%	95%
	Recall	91%	89%	92%	88%	91%	94%
	F-score	90.5%	88.5%	92.5%	87.5%	91.5%	94.5%
Underflow and Overflow Attacks	Accuracy	90%	89%	91%	88%	90%	94%
	Precision	89%	88%	90%	87%	89%	93%
	Recall	88%	88%	89%	87%	88%	92%
	F-score	88.5%	88%	89.5%	87%	88.5%	92.5%
Gas Limit Attacks	Accuracy	91%	90%	92%	87%	91%	95%
	Precision	90%	88%	91%	86%	90%	94%
	Recall	90%	89%	90%	86%	89%	93%
	F-score	90%	88.5%	90.5%	86%	89.5%	93.5%

6. Conclusion

Ethereum and blockchain technology have security problems and many benefits. Traditional computational approaches to security challenges have yielded mixed outcomes. Quantum computing, especially QDNNs like the Quantum Restricted Boltzmann Machine (QRBM), offers a breakthrough Ethereum blockchain integrity solution. The Quantum Restricted Boltzmann Machine allows this (QRBM). QRBM-based attack vector classification on Ethereum has enormous exploit potential. Quantum computing uses superposition and entanglement. Quantum neural networks process information differently than classical neural networks, enabling unparalleled computer parallelism. For the tough task of spotting and classifying attacks. QRBM handles huge solution spaces faster and possibly more accurately than Ethereum vectors. Designing QRBM from scratch for large issue spaces. QRBM was built to solve huge challenges. Ethereum is harder than other blockchains because it uses a Turing-complete programming language and smart contracts. Complexity makes the system exposed to new weaknesses and attacks. Traditional machine learning and neural network models have been used to uncover vulnerabilities, but their efficacy is questioned, especially for large-scale, changing threats. This applies especially when models are evaluated against developing large-scale threats. QRBM solves this via quantum mechanics. This increases detection and classification flexibility. Every new technology has challenges. Commercial large-scale, error-free quantum computers are currently uncommon in quantum computing. Quantum noise, decoherence, and the quantum-to-classical transition must be overcome for QRBM to be widely used. Only then can QRBM be completely utilised. Understanding and programming quantum systems requires paradigm shifts. New skills and

knowledge are needed. Despite the issues, QRBM may improve Ethereum security. QRBM has more pros than cons. Quantum computing will transform blockchain security and other businesses. Ethereum's resilience and leadership in decentralised application development will improve with users' capacity to quickly detect and fix security vulnerabilities. This is only achievable if users quickly discover and fix security concerns. QRBM quantum deep neural networks categorised Ethereum blockchain attack vectors, a pioneering step toward quantum computing and blockchain security convergence.

References

[1] Shah, H.; Shah, D.; Jadav, N.K.; Gupta, R.; Tanwar, S.; Alfarraj, O.; Tolba, A.; Raboaca, M.S.; Marina, V. Deep Learning-Based Malicious Smart Contract and Intrusion Detection System for IoT Environment. Mathematics 2023, 11, 418. https://doi.org/10.3390/math11020418

[2] Jiang, F.; Chao, K.; Xiao, J.; Liu, Q.; Gu, K.; Wu, J.; Cao, Y. Enhancing Smart-Contract Security through Machine Learning: A Survey of Approaches and Techniques. Electronics 2023, 12, 2046. https://doi.org/10.3390/electronics12092046.

[3] Kumar R, Arjunaditya, Singh D, Srinivasan K, Hu YC. AI-Powered Blockchain Technology for Public Health: A Contemporary Review, Open Challenges, and Future Research Directions. Healthcare (Basel). 2022 Dec 27;11(1):81. doi: 10.3390/healthcare11010081. PMID: 36611541; PMCID: PMC9819078.

[4] Zhang L, Li Y, Jin T, Wang W, Jin Z, Zhao C, Cai Z, Chen H. SPCBIG-EC: A Robust Serial Hybrid Model for Smart Contract Vulnerability Detection. Sensors (Basel). 2022 Jun 19;22(12):4621. doi: 10.3390/s22124621. PMID: 35746403; PMCID: PMC9231163.

[5] Shahnawaz Ahmed, Carlos Sánchez Muñoz, Franco Nori, and Anton Frisk Kockum Classification and reconstruction of optical quantum states with deep neural networks Phys. Rev. Research 3, 033278 – Published 27 September 2021.

[6] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang and W. Luo, "DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-Based Incentive," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. 2438-2455, 1 Sept.-Oct. 2021, doi: 10.1109/TDSC.2019.2952332.

[7] M. Yasar Arafath and A. Niranjil Kumar, "Quantum computing based neural networks for anomaly classification in real-time surveillance videos," Computer Systems Science and Engineering, vol. 46, no.2, pp. 2489–2508, 2023.

[8] Ruonan Wang, Min Luo, Yihong Wen, Lianhai Wang, Kim-Kwang Raymond Choo, Debiao He, "The Applications of Blockchain in Artificial Intelligence", Security and Communication Networks, vol. 2021, Article ID 6126247, 16 pages, 2021. https://doi.org/10.1155/2021/6126247.

[9] L. Le and T. N. Nguyen, "DQRA: Deep Quantum Routing Agent for Entanglement Routing in Quantum Networks," in IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-12, 2022, Art no. 4100212, doi: 10.1109/TQE.2022.3148667.

[10] P. -H. Qiu, X. -G. Chen and Y. -W. Shi, "Detecting Entanglement With Deep Quantum Neural Networks," in IEEE Access, vol. 7, pp. 94310-94320, 2019, doi: 10.1109/ACCESS.2019.2929084.

[11] R. Parthasarathy and R. T. Bhowmik, "Quantum Optical Convolutional Neural Network: A Novel Image Recognition Framework for Quantum Computing," in IEEE Access, vol. 9, pp. 103337-103346, 2021, doi: 10.1109/ACCESS.2021.3098775.

[12] P. Selig, N. Murphy, D. Redmond and S. Caton, "DeepQPrep: Neural Network Augmented Search for Quantum State Preparation," in IEEE Access, vol. 11, pp. 76388-76402, 2023, doi: 10.1109/ACCESS.2023.3296802.

[13] A. S. Rajawat, S. B. Goyal, P. Bedi, N. B. Constantin, M. S. Raboaca and C. Verma, "Cyber-Physical System for Industrial Automation Using Quantum Deep Learning," 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 2022, pp. 897-903, doi: 10.1109/SMART55829.2022.10047730.

[14] Y. Chen, "Quantum Dilated Convolutional Neural Networks," in IEEE Access, vol. 10, pp. 20240-20246, 2022, doi: 10.1109/ACCESS.2022.3152213.

[15] J. Shi et al., "Two End-to-End Quantum-Inspired Deep Neural Networks for Text Classification," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 4335-4345, 1 April 2023, doi: 10.1109/TKDE.2021.3130598.

[16] Rajawat, A.S.; Goyal, S.B.; Bedi, P.; Jan, T.; Whaiduzzaman, M.; Prasad, M. Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT). Future Internet 2023, 15, 271. https://doi.org/10.3390/fi15080271.

[17] A. S. Rajawat, S. B. Goyal, P. Bedi, N. B. Constantin, M. S. Raboaca and C. Verma, "Cyber-Physical System for Industrial Automation Using Quantum Deep Learning," 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 2022, pp. 897-903, doi: 10.1109/SMART55829.2022.10047730.

[18] S. Y. -C. Chen, C. -H. H. Yang, J. Qi, P. -Y. Chen, X. Ma and H. -S. Goan, "Variational Quantum Circuits for Deep Reinforcement Learning," in IEEE Access, vol. 8, pp. 141007-141024, 2020, doi: 10.1109/ACCESS.2020.3010470.

[19] Anand Singh Rajawat, Piyush Pant, & S B Goyal. (2022). Utilization of Renewable energy for Industrial Applications using Quantum Computing. Global Journal of Novel Research in Applied Sciences (NRAS) [ISSN: 2583-4487], 1(1), 5–10. https://doi.org/10.58260/j.nras.2202.0102.

[20] P. Pant et al., "Machine Learning Techniques for Analysis of Mars Weather Data," 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 2023, pp. 1-7, doi: 10.1109/ECAI58194.2023.10194233.

[21] Guangquan Xu, Bingjiang Guo, Chunhua Su, Xi Zheng, Kaitai Liang, Duncan S. Wong, Hao Wang,

[22] Am I eclipsed? A smart detector of eclipse attacks for Ethereum, Computers & Security , Volume 88, 2020, 101604, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101604.