ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ: ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ & ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Κβαντική Ομοσπονδιακή Μάθηση για Ανίχνευση Χρηματοοικονομικής Απάτης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των

ΔΑΛΑΜΠΕΚΗ ΚΩΝΣΤΑΝΤΙΝΟΥ & ΔΟΥΡΟΥ ΕΠΑΜΕΙΝΩΝΔΑ

Επιβλέπων : Δημήτρης Ασκούνης, Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2025

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ: ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ
& ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Κβαντική Ομοσπονδιακή Μάθηση για Ανίχνευση Χρηματοοικονομικής Απάτης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των

ΔΑΛΑΜΠΕΚΗ ΚΩΝΣΤΑΝΤΙΝΟΥ & ΔΟΥΡΟΥ ΕΠΑΜΕΙΝΩΝΔΑ

Επιβλέπων : Δημήτρης Ασκούνης, Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις 30 Οκτωβρίου 2025.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Δ. Ασκούνης	Λ. Τσέτσερης	Π. Τσανάκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2025

(Υπογραφή)

.....

ΔΟΥΡΟΣ ΕΠΑΜΕΙΝΩΝΔΑΣ

(Υπογραφή) .....

ΔΑΛΑΜΠΕΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

Διπλωματούχοι της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών Ε.Μ.Π.

Περίληψη

Η ταχεία ανάπτυξη των ψηφιακών συναλλαγών έχει ενισχύσει την ανάγκη για συστήματα ανίχνευσης απάτης που συνδυάζουν υψηλή ακρίβεια, ασφάλεια και προστασία ιδιωτικότητας. Η παρούσα εργασία προτείνει ένα ολοκληρωμένο πλαίσιο Ανίχνευσης Απάτης βασισμένο στη Ομοσπονδιακή Κβαντική Μάθηση (Quantum Federated Learning – QFL), το οποίο ενοποιεί τις αρχές της ομοσπονδιακής μάθησης, της κβαντικής πληροφορικής και της τεχνολογίας blockchain σε ένα ενιαίο, αποκεντρωμένο σύστημα.

Στο προτεινόμενο μοντέλο, πολλαπλοί κόμβοι εκπαιδεύουν τοπικά κβαντικά νευρωνικά δίκτυα (Quantum Neural Networks) χωρίς ανταλλαγή δεδομένων, διατηρώντας την ιδιωτικότητα και επιτυγχάνοντας συλλογική μάθηση μέσω ενός ασφαλούς μηχανισμού συνάθροισης. Η διαδικασία εκπαίδευσης συνοδεύεται από υβριδική κλασική–κβαντική βελτιστοποίηση, επιτρέποντας τη σύγκλιση ακόμη και σε περιβάλλοντα μη ομοιόμορφων δεδομένων (non-IID).

Η ενσωμάτωση blockchain εξασφαλίζει την ακεραιότητα των ενημερώσεων και τη διαφάνεια της διαδικασίας, μέσω έξυπνων συμβολαίων (smart contracts) που επιβεβαιώνουν τις συναλλαγές των μοντέλων και διαχειρίζονται την κατανομή βαρών. Παράλληλα, το Κβαντικό Blockchain ενισχύει το επίπεδο ασφάλειας μέσω Κβαντικών Συναρτήσεων Κατακερματισμού (Quantum Hash Functions), Κβαντικής Απόδειξης Εργασίας (Quantum Proof of Work) και μηχανισμών Κβαντικής Διανομής Κλειδιών (QKD), διασφαλίζοντας θεμελιώδη προστασία από υποκλοπές και επιθέσεις τρίτων.

Η προτεινόμενη αρχιτεκτονική υλοποιήθηκε και αξιολογήθηκε σε προσομοιωμένο περιβάλλον με χρήση των εργαλείων TensorFlow, PennyLane, Ganache, και Solidity, αποδεικνύοντας τη βιωσιμότητα του QFL σε πραγματικά σενάρια τραπεζικών και ασφαλιστικών συναλλαγών. Τα αποτελέσματα δείχνουν ότι το QFL υπερέχει των κλασικών προσεγγίσεων ως προς την ακρίβεια, τη διατήρηση ιδιωτικότητας και την ανθεκτικότητα σε κακόβουλες παρεμβάσεις.

Η εργασία αυτή συμβάλλει στην καθιέρωση της Κβαντικής Ομοσπονδιακής Μάθησης ως μιας επαναστατικής προσέγγισης για ασφαλή, συνεργατική και αποδοτική τεχνητή νοημοσύνη στον χρηματοοικονομικό τομέα και πέραν αυτού.

Λέξεις κλειδιά: Κβαντική Ομοσπονδιακή Μάθηση, Ανίχνευση Απάτης, Κβαντικά Νευρωνικά Δίκτυα, Κβαντικό Blockchain, Ομοσπονδιακή Μάθηση, Κβαντική Πληροφορική, Ιδιωτικότητα Δεδομένων, Smart Contracts

Abstract

Financial fraud detection has become a critical global challenge as digital transactions grow exponentially in volume, complexity, and security requirements. This thesis proposes an integrated Quantum Federated Learning (QFL) framework that combines Federated Learning, Quantum Machine Learning, and Blockchain technologies into a unified, decentralized, and privacy-preserving fraud detection architecture.

In the proposed framework, multiple clients collaboratively train Quantum Neural Networks (QNNs) on their local datasets without sharing raw data, ensuring data confidentiality while enabling global learning through secure aggregation mechanisms. The hybrid classical–quantum optimization approach facilitates convergence in heterogeneous, non-IID environments.

A Blockchain layer ensures integrity, transparency, and verifiability of all model updates using smart contracts that record encrypted weight exchanges and manage secure aggregation. Furthermore, the Quantum Blockchain component enhances system robustness through Quantum Hash Functions, Quantum Proof of Work (QPoW), and Quantum Key Distribution (QKD), providing physical-level security and resistance to quantum attacks.

The implementation was simulated using TensorFlow, PennyLane, Ganache, and Solidity, demonstrating the feasibility of QFL in real-world financial scenarios. Results indicate significant improvements in fraud detection accuracy, communication efficiency, and defense against data breaches compared to traditional approaches.

This work highlights Quantum Federated Learning as a pioneering paradigm for secure, collaborative, and quantum-ready artificial intelligence in financial and multi-institutional environments.

Keywords: Quantum Federated Learning, Fraud Detection, Quantum Neural Networks, Quantum Blockchain, Federated Learning, Quantum Computing, Data Privacy, Smart Contracts

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμότερες ευχαριστίες μου προς τον επιβλέποντα καθηγητή κ. Λεωνίδα Τσέτσερη, καθώς και τους κ. Παναγιώτη Τσάνακα και κ. Δημήτριο Ασκούνη, για την καθοδήγηση, την εμπιστοσύνη και τη στήριξή τους καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας. Ιδιαίτερη μνεία αξίζει στον κ. Ιωάννη Θεοδώνη, ο οποίος αποτέλεσε την απαρχή και το ερέθισμα για να ασχοληθούμε με το συγκεκριμένο αντικείμενο, εισάγοντάς μας ουσιαστικά στον κόσμο του Quantum Computing και εμπνέοντάς μας να συμμετάσχουμε στο Quantum Innovation Summit του Dubai.

Ευχαριστώ θερμά τους γονείς μου Χαρίκλεια Πλιάκου και Μιχαήλ Δαλαμπέκη για τη συνεχή στήριξη, την υπομονή και την αμέριστη αγάπη τους, όχι μόνο κατά τη διάρκεια συγγραφής της παρούσας διπλωματικής, αλλά και σε όλη τη διάρκεια των σπουδών μου. Τους οφείλω βαθιά ευγνωμοσύνη για τα ερεθίσματα που μου έδωσαν να ασχοληθώ με τις επιστήμες και τον τρόπο σκέψης που αυτές καλλιεργούν.

Επιπλέον θα ήθελα να ευχαριστήσω τα αδέρφια μου Ηλία, Μαρία και Ιγνάτιο που ήταν πάντα δίπλα μου από την πρώτη μου μέρα και αποτέλεσαν πρότυπα και στηρίγματα σε πολλά πρώτα μου βήματα.

Ιδιαίτερες ευχαριστίες οφείλω στον φίλο και καθηγητή μου κ. Σπύρο Ευαγγελίδη, ο οποίος με έκανε να αγαπήσω την επιστήμη και με ενέπνευσε να ακολουθήσω τον δρόμο της έρευνας και της καινοτομίας. Μέσα από την πίστη του σε εμένα και τον τρόπο με τον οποίο με καθοδήγησε, έμαθα να εξελίσσομαι με τον δικό μου ρυθμό και να εμπιστεύομαι τις επιλογές μου. Μου δίδαξε ότι, ακόμη κι αν οι δρόμοι που επιλέγουμε είναι ανορθόδοξοι ή έξω από τα καθιερωμένα, αυτό δεν σημαίνει ότι είναι λανθασμένοι — αρκεί να είναι αληθινοί και αποτελεσματικοί για εμάς. Χάρη σε αυτή τη νοοτροπία έμαθα να κυνηγώ όσα θέλω με τρόπο που μου ταιριάζει και να βρίσκω τον δικό μου βηματισμό μέσα στην πορεία της γνώσης.

Ένα μεγάλο ευχαριστώ στους φίλους μου, την ομάδα που με τη συναναστροφή, τις ιδέες και τη δημιουργική μας πορεία με βοήθησαν να εξελιχθώ τόσο ως μηχανικός όσο και ως άνθρωπος. Χάρη σε εκείνους έμαθα πως «μόνος πηγαίνεις γρήγορα, αλλά με ομάδα πηγαίνεις μακριά». Εύχομαι η συνεργασία μας να συνεχιστεί και στο μέλλον και να εξελιχθεί σε κάτι ακόμη μεγαλύτερο και σημαντικότερο. Θα ήταν τιμή και χαρά μου να συνεχίσω να μαθαίνω, να αναπτύσσομαι και να δημιουργώ μαζί τους — και, γιατί όχι, να καταφέρουμε κάποτε να χτίσουμε κάτι πραγματικά σπουδαίο.

Ένα ιδιαίτερο ευχαριστώ στην κοπέλα μου Άννα, που στάθηκε δίπλα μου με υπομονή και κατανόηση στο τελικό στάδιο αυτής της διαδρομής. Η στήριξή της και η πίστη της σε μένα ήταν η ήρεμη δύναμη πίσω από την ολοκλήρωση αυτής της προσπάθειας.

Τέλος, το μεγαλύτερο και πιο ειλικρινές «ευχαριστώ» απευθύνεται στον φίλο, συνεργάτη και συν συγγραφέα της παρούσας εργασίας, Επαμεινώνδα Δούρο, ο οποίος με προσέγγισε για να ξεκινήσουμε μαζί αυτό το εγχείρημα. Η συνεργασία μας, οι κοινές μας διακρίσεις σε διεθνή συνέδρια και η συν-συγγραφή του επιστημονικού άρθρου αποτέλεσαν για μένα εμπειρίες ανεκτίμητης αξίας. Η αλληλοστήριξη, η φιλία και οι στιγμές που μοιραστήκαμε κατά τη διάρκεια αυτού του ταξιδιού είναι κάτι που θα θυμάμαι για πάντα.

Αθήνα, Οκτώβρης 2025
Δαλαμπέκης Κωνσταντίνος

Ευχαριστίες

Αρχικά, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες προς τους καθηγητές κ. Τσέτσερη, κ. Ασκούνη και κ. Τσανάκα, για την πολύτιμη βοήθεια, την καθοδήγηση και την υποστήριξη που μας παρείχαν καθ' όλη τη διάρκεια της διπλωματικής εργασίας, καθώς και για τις εύστοχες παρατηρήσεις και διορθώσεις τους.

Ιδιαίτερα, θα ήθελα να εκφράσω την πιο βαθιά μου ευγνωμοσύνη προς τον κ. Ιωάννη Θεοδώνη, ο οποίος δεν υπήρξε απλώς επιβλέπων, αλλά ένας πραγματικός μέντορας και άνθρωπος που πίστεψε σε εμένα από την πρώτη στιγμή. Από τότε που μπήκα στο γραφείο του, τον Οκτώβριο του 2024, με υποδέχτηκε με εμπιστοσύνη και ανιδιοτελή διάθεση να μοιραστεί τις γνώσεις του. Η επιρροή του ξεπέρασε τα όρια της ακαδημαϊκής σχέσης — αποτέλεσε για εμένα πηγή έμπνευσης, στήριγμα και αληθινό φίλο.

Επίσης, θα ήθελα να εκφράσω τις πιο ειλικρινείς μου ευχαριστίες προς την οικογένειά μου, και ιδιαίτερα προς τον πατέρα μου Νικόλαο Δούρο και τη μητέρα μου Άννα-Μαρία Ταμιωλάκη, για την αδιάκοπη καθοδήγηση, την αγάπη και τη στήριξή τους, χωρίς τα οποία δεν θα βρισκόμουν στη θέση που είμαι σήμερα. Η πίστη τους στις δυνατότητές μου και η συνεχής ενθάρρυνσή τους αποτέλεσαν για μένα πηγή δύναμης και έμπνευσης σε όλη τη διάρκεια των σπουδών μου.

Ένα ιδιαίτερα μεγάλο και βαθύτατο ευχαριστώ οφείλω στην αδερφή μου, Έλενα Δούρου. Η πίστη της σε εμένα, η αδιάκοπη στήριξη και η αληθινή της αγάπη μου έδωσαν τη δύναμη να συνεχίσω ακόμη και στις πιο απαιτητικές στιγμές. Ήταν πάντα εκεί — με υπομονή, ενθάρρυνση και κατανόηση — προσφέροντάς μου το ψυχικό σθένος που χρειάζεται κάποιος για να προχωρήσει μπροστά. Χωρίς εκείνη, τίποτα από όλα αυτά δεν θα είχε πάρει την ίδια μορφή.

Επιπλέον, θα ήθελα να ευχαριστήσω από καρδιάς όλους τους φίλους μου που στάθηκαν δίπλα μου σε όλη τη διάρκεια των σπουδών μου. Η παρουσία, η ενθάρρυνση και η παρέα τους αποτέλεσαν πηγή χαράς, στήριξης και ψυχικής δύναμης σε κάθε δύσκολη ή απαιτητική στιγμή. Μέσα από τα χρόνια αυτά μοιραστήκαμε αμέτρητες αναμνήσεις, στιγμές γέλιου αλλά και άγχους, και όλοι τους συνέβαλαν στο να διατηρώ το κίνητρο και την ισορροπία που χρειάζεται κάποιος για να φτάσει ως το τέλος. Όπως πολύ σοφά έλεγαν και οι αρχαίοι, *«δύναμις ἐν τῇ ἑνώσει»*.

Θα ήθελα, επίσης, να ευχαριστήσω από καρδιάς την αγαπημένη μου Greta, η οποία στάθηκε στο πλευρό μου σε μεγάλο μέρος των σπουδών, προσφέροντάς μου στήριξη, κατανόηση και δύναμη σε κάθε δύσκολη στιγμή.

Τέλος, ένα ιδιαίτερο και ειλικρινές ευχαριστώ αξίζει στον εγκάρδιο φίλο και συνάδελφο Κωνσταντίνο Δαλαμπέκη. Από την πρώτη στιγμή της γνωριμίας μας έως και σήμερα, υπήρξε σταθερός συνεργάτης, συνοδοιπόρος και άνθρωπος που με ενέπνευσε να εξελιχθώ. Μαζί περάσαμε αμέτρητες ώρες δουλειάς, δημιουργικότητας και αναζήτησης, μοιραστήκαμε ιδέες, προκλήσεις και επιτυχίες, και μέσα από αυτή τη διαδικασία αναπτύχθηκα τόσο επιστημονικά όσο και προσωπικά. Μαζί δημιουργήσαμε μια δυναμική ομάδα που έχει ήδη πετύχει πολλά και, είμαι βέβαιος, θα καταφέρει ακόμη περισσότερα στο μέλλον.

Και να θυμάστε — μόνος πας γρήγορα, αλλά με ομάδα πας μακριά !

Αθήνα, Οκτώβρης 2025
Δούρος Επαμεινώνδας

Πίνακας Περιεχομένων

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Εισαγωγή

1.1 Σκοπός και Αντικείμενο της Έρευνας

Η συνεχής ψηφιοποίηση των οικονομικών συναλλαγών έχει μετασχηματίσει ριζικά τον τρόπο λειτουργίας του παγκόσμιου χρηματοπιστωτικού συστήματος.[1] Οι ηλεκτρονικές πληρωμές, οι διαδικτυακές μεταφορές κεφαλαίων και τα κρυπτονομίσματα αποτελούν πλέον βασικούς μηχανισμούς οικονομικής δραστηριότητας [2] , όμως η ραγδαία αυτή εξέλιξη συνοδεύεται από εξίσου αυξανόμενους κινδύνους απάτης. Από επιθέσεις σε συστήματα ηλεκτρονικής τραπεζικής έως την παράνομη χειραγώγηση δεδομένων συναλλαγών, οι μορφές χρηματοπιστωτικής απάτης γίνονται ολοένα πιο πολύπλοκες και δύσκολες να ανιχνευθούν με παραδοσιακές μεθόδους.[3]
Η ανίχνευση απάτης δεν αποτελεί μόνο τεχνικό ζήτημα, αλλά και ζήτημα εμπιστοσύνης και διαφάνειας. Οι τράπεζες, οι ρυθμιστικές αρχές και οι πάροχοι ψηφιακών υπηρεσιών αντιμετωπίζουν σήμερα την ανάγκη να αναπτύξουν μηχανισμούς που μπορούν να ανιχνεύουν ύποπτες δραστηριότητες έγκαιρα, χωρίς όμως να παραβιάζουν την ιδιωτικότητα των πελατών ή να εκθέτουν τα δεδομένα σε τρίτους.[2]
Η κλασική προσέγγιση της συγκέντρωσης δεδομένων από πολλούς οργανισμούς σε έναν κεντρικό διακομιστή για εκπαίδευση μοντέλων μηχανικής μάθησης εγείρει σοβαρά ζητήματα συμμόρφωσης [3] με κανονισμούς όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), καθώς και αυξημένους κινδύνους παραβιάσεων και επιθέσεων.[4]
Για να απαντήσει σε αυτές τις προκλήσεις, η ερευνητική κοινότητα έχει στραφεί τα τελευταία χρόνια στην Ομοσπονδιακή Μάθηση (Federated Learning – FL) [5], μια αποκεντρωμένη προσέγγιση εκπαίδευσης μοντέλων τεχνητής νοημοσύνης. Η βασική ιδέα είναι ότι κάθε οργανισμός ή κόμβος (client) διατηρεί τα δικά του δεδομένα τοπικά και εκπαιδεύει ένα μοντέλο στο δικό του περιβάλλον, χωρίς ποτέ να διαμοιράζεται τις ευαίσθητες πληροφορίες. Αντί να μεταφέρονται τα δεδομένα, μεταφέρονται μόνο τα ενημερωμένα βάρη ή οι παράμετροι του μοντέλου, τα οποία στη συνέχεια συγχωνεύονται σε ένα παγκόσμιο μοντέλο (global model) [3],[5]. Με αυτόν τον τρόπο επιτυγχάνεται συνεργατική μάθηση χωρίς απώλεια ιδιωτικότητας.
Ωστόσο, παρά τα πλεονεκτήματά της, η ομοσπονδιακή μάθηση παραμένει επιρρεπής σε νέες μορφές κινδύνων. Ελλείψεις σε μηχανισμούς εμπιστοσύνης και κακόβουλοι κόμβοι μπορούν να αποστείλουν αλλοιωμένα βάρη, να προσπαθήσουν να υποκλέψουν τοπικά μοντέλα ή να διαστρεβλώσουν τη διαδικασία εκπαίδευσης.[4] Επομένως, απαιτείται ένα πρόσθετο επίπεδο διαφάνειας και επαλήθευσης που να διασφαλίζει ότι κάθε ενημέρωση που συμμετέχει στη συνάθροιση είναι έγκυρη, αξιόπιστη και ανήκει σε νόμιμο συμμετέχοντα.
Σε αυτό το σημείο, η τεχνολογία Blockchain προσφέρει έναν καινοτόμο μηχανισμό ενίσχυσης της ασφάλειας και της ακεραιότητας των ομοσπονδιακών διαδικασιών.[6] Το blockchain επιτρέπει την αμετάβλητη καταγραφή (immutable ledger) όλων των ενημερώσεων μοντέλων, παρέχοντας ιχνηλασιμότητα και επαλήθευση χωρίς την ανάγκη κεντρικού διαχειριστή. Κάθε ενημέρωση των βαρών αποθηκεύεται σε ένα “block” μαζί με χρονική σφραγίδα και μοναδικό κρυπτογραφικό αποτύπωμα (hash), επιτρέποντας στους κόμβους να επικυρώνουν την εγκυρότητα των συνεισφορών και να απορρίπτουν ύποπτες συναλλαγές. Με αυτόν τον τρόπο, το blockchain λειτουργεί ως κατανεμημένος μηχανισμός εμπιστοσύνης (distributed trust mechanism), θεμελιώνοντας τη συνεργασία μεταξύ διαφορετικών οργανισμών χωρίς την ανάγκη ενός κεντρικού συντονιστή.[6]
Παράλληλα, η ραγδαία πρόοδος της Κβαντικής Υπολογιστικής (Quantum Computing) δημιουργεί νέες προοπτικές για την ασφάλεια και την απόδοση των συστημάτων τεχνητής νοημοσύνης.[7] Οι κβαντικοί υπολογιστές αξιοποιούν αρχές όπως η υπέρθεση (superposition) και η διεμπλοκή (entanglement) για να επεξεργάζονται εκθετικά μεγαλύτερους χώρους δεδομένων, επιλύοντας προβλήματα βελτιστοποίησης και αναζήτησης πολύ ταχύτερα από τα κλασικά συστήματα.[8] Η εισαγωγή της κβαντικής λογικής στα νευρωνικά δίκτυα οδηγεί στην ανάπτυξη των Κβαντικών Νευρωνικών Δικτύων (Quantum Neural Networks – QNNs) τα οποία συνδυάζουν τη μαθησιακή ικανότητα των κλασικών δικτύων με την υπολογιστική ισχύ του κβαντικού χώρου Hilbert.[9] Η σύγκλιση αυτών των τριών τεχνολογιών Federated Learning, Blockchain και Quantum Computing αποτελεί το βασικό αντικείμενο της παρούσας έρευνας.

Η εργασία προτείνει ένα ενιαίο πλαίσιο Quantum Federated Blockchain Learning, το οποίο συνδυάζει:

- αποκεντρωμένη εκπαίδευση (για ιδιωτικότητα) [10],
- blockchain επικύρωση (για ακεραιότητα και διαφάνεια) [11],
- και κβαντική επεξεργασία (για ακρίβεια και αποδοτικότητα) [12].

Πρακτικά, η λύση αυτή επιδιώκει να δημιουργήσει ένα ασφαλές, επεκτάσιμο και ενεργειακά αποδοτικό σύστημα ανίχνευσης απάτης που να μπορεί να εφαρμοστεί σε πραγματικά χρηματοοικονομικά περιβάλλοντα.[13] Η αναπτυγμένη αρχιτεκτονική συνδυάζει τεχνολογίες Κβαντικής Πληροφορικής, Μηχανικής Μάθησης και Ασφάλειας Δικτύων, σχηματίζοντας ένα ενιαίο και Quantum-Ready πλαίσιο.[14] Περιλαμβάνει:

- Υβριδικά Κβαντικά Νευρωνικά Δίκτυα (Hybrid QNNs) με VQCs, τα οποία ενισχύουν τη μαθησιακή ικανότητα και εκτελέστηκαν επιτυχώς σε πραγματικό κβαντικό υπολογιστή της IBM.[8],[15]
- Ομομορφική Κρυπτογράφηση, Κβαντικός Κατακερματισμός (Qhash) και Κβαντική Διανομή Κλειδιών (QKD) για ασφαλή επικοινωνία και προστασία δεδομένων [αναλυτική περιγραφή στο Κεφάλαιο 5].[16]
- Blockchain Validation Layer με Smart Contracts και Reputation-Based Filtering για αποκεντρωμένη επαλήθευση ενημερώσεων.[17]
- Προοπτική μετάβασης σε Quantum Blockchain, με κβαντικούς μηχανισμούς συναίνεσης για μέγιστη ασφάλεια και αποδοτικότητα.[18]

Ο γενικός σκοπός της διπλωματικής εργασίας είναι να αποδείξει πειραματικά ότι μια τέτοια σύζευξη τεχνολογιών μπορεί να οδηγήσει σε συστήματα που:

1. Διατηρούν πλήρη ιδιωτικότητα δεδομένων,
2. Παρέχουν αποδείξιμη ακεραιότητα στις ενημερώσεις των μοντέλων,
3. Επιτυγχάνουν υψηλή ακρίβεια ανίχνευσης απάτης,
4. Και μπορούν να επεκταθούν σε πραγματικά περιβάλλοντα τραπεζικών συναλλαγών.

Η παρούσα έρευνα, επομένως, τοποθετείται στο σταυροδρόμι τριών επιστημονικών τομέων τεχνητής νοημοσύνης, ασφάλειας πληροφοριών και κβαντικής υπολογιστικής και φιλοδοξεί να αποτελέσει ένα βήμα προς την επόμενη γενιά ασφαλών, συνεργατικών και κβαντικά ενισχυμένων συστημάτων μάθησης.[19]

1.2 Κίνητρα και Επιστημονική Συνεισφορά

1.2.1 Κίνητρα

Η αυξανόμενη πολυπλοκότητα των οικονομικών συναλλαγών και η εξάρτηση των τραπεζικών και εμπορικών οργανισμών από ψηφιακά δίκτυα έχουν αναδείξει την απάτη ως μία από τις πιο κρίσιμες απειλές της σύγχρονης οικονομίας [20]. Οι δράστες ψηφιακών επιθέσεων αξιοποιούν προηγμένες τεχνικές, όπως η deepfake ταυτοποίηση και αυτόματη παραγωγή ψευδών συναλλαγών [21], καθιστώντας τις κλασικές μεθόδους ανίχνευσης ανεπαρκείς. Παράλληλα, η ανάγκη για συμμόρφωση με αυστηρούς κανονισμούς προστασίας δεδομένων (όπως ο GDPR και το ePrivacy Directive) περιορίζει τη δυνατότητα συγκέντρωσης δεδομένων από διαφορετικούς οργανισμούς, οδηγώντας σε αποσπασματικά μοντέλα με μειωμένη αποτελεσματικότητα [4] [22].

Σε αυτό το πλαίσιο, η Ομοσπονδιακή Μάθηση (Federated Learning) αναδύεται ως ελπιδοφόρα λύση, καθώς επιτρέπει σε πολλούς οργανισμούς να συνεργάζονται στην εκπαίδευση ενός κοινού μοντέλου χωρίς να ανταλλάσσουν τα ευαίσθητα δεδομένα τους. Εντούτοις, η ομοσπονδιακή προσέγγιση παρουσιάζει νέα προβλήματα μεταξύ των οποίων η έλλειψη εμπιστοσύνης μεταξύ των συμμετεχόντων κόμβων, οι επιθέσεις σε επίπεδο μοντέλου (model poisoning) και η δυσκολία επαλήθευσης της εγκυρότητας των ενημερώσεων [23]. Αυτά τα προβλήματα υπονομεύουν τη διαφάνεια και την

αξιοπιστία της ομοσπονδιακής εκπαίδευσης, περιορίζοντας την πρακτική της υιοθέτηση σε κρίσιμους τομείς όπως οι χρηματοοικονομικές υπηρεσίες.
Ταυτόχρονα, η έκρηξη των υπολογιστικών απαιτήσεων για την εκπαίδευση μοντέλων σε πραγματικού χρόνου δεδομένα, όπως αυτά των τραπεζικών συναλλαγών, καθιστά αναγκαία τη χρήση νέων υπολογιστικών παραδειγμάτων. Η Κβαντική Υπολογιστική (Quantum Computing) υπόσχεται εκθετική επιτάχυνση στη βελτιστοποίηση και στη μοντελοποίηση πολύπλοκων μη γραμμικών σχέσεων. Τα Κβαντικά Νευρωνικά Δίκτυα (Quantum Neural Networks), και ειδικότερα τα Υβριδικά Κβαντικά Νευρωνικά Δίκτυα (Hybrid QNNs)[24] , επιτρέπουν την ταυτόχρονη αξιοποίηση των πλεονεκτημάτων του κβαντικού υπολογισμού και των κλασικών μεθόδων μάθησης.
Επιπλέον, η ενσωμάτωση της τεχνολογίας Blockchain στο οικοσύστημα της ομοσπονδιακής μάθησης δημιουργεί ένα αποκεντρωμένο σύστημα εμπιστοσύνης, το οποίο εξασφαλίζει διαφάνεια, ιχνηλασιμότητα και ακεραιότητα [25]. Μέσα από έξυπνες συμβάσεις (Smart Contracts), οι ενημερώσεις των μοντέλων μπορούν να επαληθεύονται, να αποθηκεύονται και να αξιολογούνται αυτόματα, χωρίς την ανάγκη μεσολάβησης τρίτων.
Τα παραπάνω συγκλίνουν σε ένα κοινό κίνητρο:
Η ανάγκη για ένα ολιστικό σύστημα ανίχνευσης απάτης που συνδυάζει την ιδιωτικότητα της ομοσπονδιακής μάθησης, τη διαφάνεια του blockchain και την υπολογιστική υπεροχή της κβαντικής τεχνολογίας.
Η εργασία αυτή ξεκινά από την υπόθεση ότι η ένωση των τριών αυτών τεχνολογιών μπορεί να οδηγήσει σε ένα νέο πρότυπο ασφαλούς, συνεργατικής και ενεργειακά αποδοτικής τεχνητής νοημοσύνης.

1.2.2 Επιστημονική Συνεισφορά

Η παρούσα διπλωματική εργασία προτείνει, υλοποιεί και αξιολογεί ένα πλήρες σύστημα Quantum Federated Blockchain Learning, το οποίο επεκτείνει την υπάρχουσα βιβλιογραφία, συνδυάζοντας σε ενιαίο πλαίσιο τις τεχνολογίες Federated Learning, Blockchain και Quantum Machine Learning.

Η ερευνητική συνεισφορά της εργασίας συνοψίζεται σε τέσσερις κύριους άξονες:

1. Ανάπτυξη Υβριδικού Κβαντικού Νευρωνικού Δικτύου (Hybrid Quantum Neural Network) ως Τοπικό Μοντέλο Εκπαίδευσης [8]:

   Σχεδιάστηκε και υλοποιήθηκε ένα υβριδικό μοντέλο που συνδυάζει κλασικά και κβαντικά επίπεδα μάθησης, αξιοποιώντας Variational Quantum Circuits (VQCs) για την αποδοτική αναπαράσταση σύνθετων μη γραμμικών συσχετίσεων.[14]

   Το μοντέλο εκπαιδεύτηκε και αξιολογήθηκε εκτενώς στο πλαίσιο ανίχνευσης απάτης σε συναλλαγές, αποδεικνύοντας βελτιωμένες επιδόσεις στο recall και στη σταθερότητα των αποτελεσμάτων σε σχέση με τα αμιγώς κλασικά δίκτυα.

   Η εκπαίδευση πραγματοποιήθηκε με χρήση κλασικού optimizer (Adam) και παραμετρικών κβαντικών πυλών, ενώ η ανάλυση είχε συγκριτικά πειράματα με και χωρίς θόρυβο για τη μελέτη της ανθεκτικότητας του συστήματος.

2. Ενοποίηση Κβαντικής Κρυπτογράφησης και Blockchain για το Federated Learning:

   Αναπτύχθηκε ένα ολοκληρωμένο πλαίσιο ασφαλούς και επαληθεύσιμης ομοσπονδιακής εκπαίδευσης το οποίο συνδυάζει τεχνικές κβαντικής κρυπτογράφησης, προστασίας ιδιωτικότητας, και blockchain. Η προσέγγιση αυτή στοχεύει στη δημιουργία ενός συστήματος όπου κάθε τοπική συνεισφορά μπορεί να μεταδίδεται, να επαληθεύεται και να ενσωματώνεται με απόλυτη ασφάλεια και διαφάνεια.

   Συγκεκριμένα, ενσωματώθηκαν οι εξής μηχανισμοί:

- Ομομορφική Κρυπτογράφηση (Homomorphic Encryption): επιτρέπει την ασφαλή μετάδοση και επεξεργασία των τοπικών βαρών χωρίς αποκρυπτογράφηση, διατηρώντας πλήρως την ιδιωτικότητα των δεδομένων των πελατών [10].
- Κβαντικοί Κατακερματισμοί (Quantum Hash Functions): χρησιμοποιούνται για την επαλήθευση της ακεραιότητας των ενημερώσεων, προσφέροντας ανθεκτικότητα σε κβαντικού τύπου επιθέσεις [26].
- Quantum Key Distribution (QKD): εξασφαλίζει αδιάβλητη ανταλλαγή κλειδιών μεταξύ των κόμβων μέσω των αρχών της κβαντικής εμπλοκής και της υπέρθεσης, επιτρέποντας τη μεταφορά των δεδομένων με απόλυτη ασφάλεια, καθώς κάθε απόπειρα υποκλοπής ανιχνεύεται φυσικά [16].
- Blockchain Validation Layer με Smart Contracts: λειτουργεί ως μηχανισμός αποκεντρωμένου ελέγχου, όπου κάθε τοπικό μοντέλο ή ενημέρωση επαληθεύεται αυτόματα πριν ενσωματωθεί στο παγκόσμιο μοντέλο [17].

Πέρα από την απλή καταγραφή και επαλήθευση, ενσωματώθηκε ένας Reputation-Based Filtering μηχανισμός [βλ. αναλυτικά Κεφάλαιο 5.5.4], ο οποίος αξιολογεί τη φήμη κάθε κόμβου με βάση την ακρίβεια των ενημερώσεών του [27]. Οι κόμβοι που υποβάλλουν αξιόπιστες και σταθερές ενημερώσεις επιβραβεύονται με υψηλότερο reputation score, ενώ οι κόμβοι που συνεισφέρουν θορυβώδη ή ανώμαλα δεδομένα απορρίπτονται αυτόματα από το σύστημα.

Αυτός ο μηχανισμός επιτρέπει την προσαρμοστική βελτίωση της ομοσπονδίας, εξασφαλίζοντας ότι η παγκόσμια ενημέρωση προέρχεται μόνο από αξιόπιστες πηγές [27].

Τέλος, στο τελικό στάδιο της αρχιτεκτονικής, προτείνεται η μετάβαση προς ένα Quantum Blockchain, όπου η διαδικασία επικύρωσης και συναίνεσης υλοποιείται μέσω κβαντικών μηχανισμών Proof-of-Work ή Proof-of-Entanglement [18].

Η προοπτική αυτή προσδίδει στο σύστημα ανώτερο επίπεδο ασφάλειας, διαφάνειας και ενεργειακής αποδοτικότητας, δημιουργώντας ένα ολιστικά ασφαλές περιβάλλον για Federated Learning που παραμένει βιώσιμο και επεκτάσιμο στην εποχή των κβαντικών υπολογιστών [19].

3. Ανάπτυξη της Λύσης ως Quantum SaaS στην Πλατφόρμα PlanQK και Χρήση IBM Quantum Hardware:

   Το τελικό σύστημα αναπτύχθηκε ως Quantum Software-as-a-Service (SaaS) και αναρτήθηκε στην πλατφόρμα PlanQK της εταιρείας Kipu Quantum, η οποία φιλοξενεί καινοτόμες κβαντικές εφαρμογές σε περιβάλλον cloud.

   Επίσης, το τελικό μοντέλο εκτελέστηκε επιτυχώς σε πραγματικό κβαντικό υπολογιστή της IBM (μέσω του IBM Quantum Platform), αποδεικνύοντας τη δυνατότητα πλήρους ενσωμάτωσης της προτεινόμενης λύσης σε πραγματικό hardware και επιβεβαιώνοντας τη λειτουργική ετοιμότητα και βιομηχανική αξιοπιστία της.

   Η ενσωμάτωση αυτή καθιστά το σύστημα πλήρως λειτουργικό, επεκτάσιμο και έτοιμο για υλοποίηση σε πραγματικά σενάρια ανίχνευσης απάτης, γεφυρώνοντας το χάσμα μεταξύ θεωρητικής έρευνας και πρακτικής εφαρμογής κβαντικών τεχνολογιών.

4. Πειραματική Διερεύνηση των Quantum Reinforcement Learning (QRL) και Grover-Based Learning Scheme (GBLS):

   Στο τελικό στάδιο πραγματοποιήθηκε πειραματική μελέτη των μεθόδων Quantum Reinforcement Learning (QRL) και Grover-Based Learning Scheme (GBLS), με σκοπό την

αξιολόγηση της δυνατότητάς τους να επιταχύνουν ή να βελτιώσουν τη διαδικασία εκπαίδευσης των υβριδικών κβαντικών μοντέλων.

Ωστόσο, καμία από τις δύο τεχνολογίες δεν ενσωματώθηκε στην τελική υλοποίηση, καθώς δεν παρουσίασαν ουσιαστική βελτίωση στα πειραματικά αποτελέσματα, παραμένοντας σε επίπεδο θεωρητικής διερεύνησης για μελλοντική αξιοποίηση.

Η εργασία εισάγει, επομένως, μια διεπιστημονική μεθοδολογία που ενοποιεί τεχνολογίες από τρία διαφορετικά ερευνητικά πεδία Μηχανική Μάθηση, Κβαντική Πληροφορική και Ασφάλεια Δικτύων σε ένα ενιαίο, λειτουργικό πλαίσιο. Το προτεινόμενο μοντέλο επιτυγχάνει βελτιωμένη ακρίβεια, αυξημένη ασφάλεια, ενεργειακή αποδοτικότητα και πλήρη διαφάνεια, συμβάλλοντας ουσιαστικά στην εξέλιξη των τεχνολογιών Quantum-Ready AI και Federated Trust Systems.

1.3 Δομή της Εργασίας

Η παρούσα διπλωματική εργασία οργανώνεται σε επτά κεφάλαια, τα οποία ακολουθούν μία λογική και εξελικτική πορεία, ξεκινώντας από τη θεωρητική θεμελίωση και καταλήγοντας στην πειραματική αξιολόγηση και τις μελλοντικές ερευνητικές κατευθύνσεις. Κάθε κεφάλαιο στοχεύει να παρουσιάσει με σαφήνεια ένα ξεχωριστό στάδιο της ερευνητικής διαδικασίας, διατηρώντας ταυτόχρονα συνοχή και συνέχεια με τα υπόλοιπα.

Κεφάλαιο 2 – Θεωρητικό Υπόβαθρο
Το δεύτερο κεφάλαιο εισάγει τις βασικές αρχές και θεμελιώδεις έννοιες που απαιτούνται για την κατανόηση της προτεινόμενης προσέγγισης.
Αρχικά παρουσιάζονται οι τεχνικές Κλασικής Μηχανικής Μάθησης και τα βασικά προβλήματα ασφάλειας που τις συνοδεύουν, όπως οι επιθέσεις εισαγωγής θορύβου και η παραβίαση της ιδιωτικότητας. Στη συνέχεια, αναλύονται οι αρχές της Κβαντικής Πληροφορικής, των Κβαντικών Κυκλωμάτων και των Κβαντικών Νευρωνικών Δικτύων (QNNs), με στόχο να αναδειχθεί η ικανότητά τους να επιλύουν προβλήματα υψηλής διάστασης με αυξημένη υπολογιστική αποδοτικότητα. Το κεφάλαιο ολοκληρώνεται με αναφορά στην Ομομορφική Κρυπτογράφηση (Homomorphic Encryption) και στη Ομοσπονδιακή Μάθηση (Federated Learning), οι οποίες αποτελούν τον πυρήνα των τεχνολογιών που συνδυάζονται στην προτεινόμενη αρχιτεκτονική.

Κεφάλαιο 3 – Σχετική Έρευνα και Τεχνολογική Ανασκόπηση
Σε αυτό το κεφάλαιο εξετάζεται η υπάρχουσα βιβλιογραφία στους τομείς της ομοσπονδιακής μάθησης, του blockchain και της κβαντικής μηχανικής μάθησης.
Αναλύονται οι σημαντικότερες ερευνητικές προσεγγίσεις των τελευταίων ετών, οι οποίες επιχειρούν να επιτύχουν ασφαλή, συνεργατική εκπαίδευση μοντέλων. Παρουσιάζονται οι αρχές του Federated Learning και Data Privacy, η ενσωμάτωση του Blockchain για αποκεντρωμένη επαλήθευση, καθώς και η βιβλιογραφία γύρω από την Quantum Blockchain και το Quantum Machine Learning. Το κεφάλαιο αυτό λειτουργεί ως θεωρητική γέφυρα μεταξύ του υποβάθρου και της προτεινόμενης αρχιτεκτονικής, αναδεικνύοντας τα πλεονεκτήματα και τα κενά των υφιστάμενων λύσεων.

Κεφάλαιο 4 – Προτεινόμενη Αρχιτεκτονική
Το τέταρτο κεφάλαιο αποτελεί τον πυρήνα της εργασίας και περιγράφει την προτεινόμενη αρχιτεκτονική Quantum Federated Blockchain Learning για ανίχνευση απάτης. Αρχικά, διατυπώνεται το πρόβλημα και τα ερευνητικά κενά που εντοπίζονται στις υπάρχουσες προσεγγίσεις. Έπειτα παρουσιάζεται η ενοποίηση των τριών τεχνολογικών πυλώνων – Quantum, Federated και Blockchain – και εξηγείται πώς η συνεργασία τους οδηγεί σε ένα πιο ανθεκτικό, ασφαλές και αποδοτικό σύστημα.
Ακολουθεί το διάγραμμα ροής του συστήματος, το οποίο αποτυπώνει τη διασύνδεση των επιμέρους επιπέδων (Local Nodes, Blockchain Validation Layer, Global Aggregator, QKD Distribution).

Τέλος, γίνεται αναλυτική περιγραφή των λειτουργικών ενοτήτων, εξηγώντας τη ροή δεδομένων, τη διαδικασία εκπαίδευσης, την επικύρωση μέσω blockchain και τη διανομή του παγκόσμιου μοντέλου.

Κεφάλαιο 5 – Υλοποίηση του Συστήματος

Το πέμπτο κεφάλαιο παρουσιάζει τη μεθοδολογία και την τεχνική υλοποίηση του προτεινόμενου συστήματος Quantum Federated Blockchain Learning. Περιγράφονται αναλυτικά οι επιμέρους μηχανισμοί που συνθέτουν το πλαίσιο, από την προετοιμασία των δεδομένων έως την ανάπτυξη της λύσης ως SaaS.

Συγκεκριμένα, το κεφάλαιο περιλαμβάνει:

- Την ανάλυση και προετοιμασία των δεδομένων (5.1), με επεξεργασία, κανονικοποίηση και εξισορρόπηση κλάσεων.
- Την αρχιτεκτονική του υβριδικού κβαντικού νευρωνικού δικτύου (5.2) και τη διαδικασία τοπικής εκπαίδευσης (5.3) μέσω Pennylane.
- Την ομομορφική κρυπτογράφηση και παραγωγή Qhash (5.4) για ασφαλή μεταφορά βαρών και επαλήθευση ακεραιότητας.
- Τη διασύνδεση με το blockchain μέσω *Ganache*, *Solidity* και *Web3* (5.5), καθώς και την ανάπτυξη του smart contract *NewSecureAggregation.sol* με Reputation-Based Outlier Filtering.
- Την υλοποίηση Secure Aggregation με ενσωμάτωση Quantum Key Distribution (QKD) (5.6) για κβαντικά ασφαλή επικοινωνία.
- Τέλος, την ανάπτυξη της λύσης ως Quantum SaaS στην πλατφόρμα PlanQK και την εκτέλεση του τελικού μοντέλου σε πραγματικό IBM Quantum υπολογιστή (5.7).

Κεφάλαιο 6 – Πειραματικά Αποτελέσματα

Στο έκτο κεφάλαιο παρουσιάζεται η πειραματική αξιολόγηση του συστήματος. Αρχικά περιγράφονται τα δεδομένα που χρησιμοποιήθηκαν, καθώς και η μεθοδολογία εκπαίδευσης των τοπικών (client) μοντέλων και της ομοσπονδιακής ενοποίησης. Ακολουθεί η παρουσίαση των αποτελεσμάτων του υβριδικού Quantum Federated μοντέλου και η συγκριτική ανάλυση με τα αντίστοιχα classical και centralized μοντέλα.

Επιπλέον, περιγράφεται η πειραματική προσέγγιση με Ενισχυτική Μάθηση (Quantum Reinforcement Learning – QRL), όπου διερευνάται η απόδοση διαφορετικών exploration strategies, reward systems και αρχιτεκτονικών. Τέλος, παρουσιάζεται η διερεύνηση του Grover-Based Learning Scheme (GBLS) ως εναλλακτική μεθοδολογία επιτάχυνσης της εκπαίδευσης των κβαντικών νευρωνικών δικτύων και μείωσης του αριθμού των απαιτούμενων μετρήσεων.

Κεφάλαιο 7 – Συμπεράσματα και Μελλοντικές Επεκτάσεις
Το τελευταίο κεφάλαιο συνοψίζει τα συμπεράσματα της έρευνας, αναδεικνύοντας τα κύρια επιτεύγματα και τη συνεισφορά της προτεινόμενης αρχιτεκτονικής. Παρουσιάζονται οι προοπτικές μελλοντικής εξέλιξης, όπως η πρόσβαση σε πραγματικό quantum hardware για φυσική εκτέλεση του Quantum Blockchain, η διερεύνηση κβαντικών αλγορίθμων Grover και VQE για βελτίωση της απόδοσης, καθώς και η πιθανή επέκταση του πλαισίου σε άλλους τομείς εφαρμογών, όπως η ανίχνευση κυβερνοεπιθέσεων και η ανάλυση ιατρικών δεδομένων.

Με τη συγκεκριμένη δομή, η εργασία ακολουθεί μια σαφή ερευνητική πορεία από τη θεωρητική θεμελίωση έως την πειραματική τεκμηρίωση επιτρέποντας στον αναγνώστη να κατανοήσει τόσο την επιστημονική βάση όσο και την πρακτική αξία της προτεινόμενης λύσης.

1.3 Συνεισφορές

Καθώς η παρούσα διπλωματική εργασία πραγματοποιήθηκε από δύο φοιτητές, τον Επαμεινώνδα Δούρο και τον Κωνσταντίνο Δαλαμπέκη, κρίνεται σκόπιμο να παρουσιαστεί συνοπτικά η επιμέρους συνεισφορά του καθενός. Η εργασία υλοποιήθηκε με στενή συνεργασία και αλληλοσυμπλήρωση σε όλα τα στάδιά της — από τη θεωρητική μελέτη και τον σχεδιασμό των μοντέλων έως την πειραματική αξιολόγηση και τη συγγραφή. Παρ' όλα αυτά, κάθε μέλος επικεντρώθηκε σε διαφορετικό πυλώνα του έργου: ο Επαμεινώνδας Δούρος ασχολήθηκε κυρίως με το σκέλος του Quantum Machine Learning και τη χρήση κβαντικού υπολογιστή, ενώ ο Κωνσταντίνος Δαλαμπέκης επικεντρώθηκε στο τμήμα που αφορά το Quantum Blockchain και το Federated Learning. Η συνέργεια των δύο αυτών τομέων υπήρξε καθοριστική για τη δημιουργία ενός ολοκληρωμένου και καινοτόμου συστήματος.

Τέλος, θα θέλαμε να εκφράσουμε ειδικές ευχαριστίες προς τον Ιωάννη Θεοδώνη του Ε.Μ.Π. και τη Dr. Nouhaila του NYUAD για την πολύτιμη καθοδήγηση, τη διαρκή υποστήριξη και τη σημαντική τους συνεισφορά καθ' όλη τη διάρκεια της μελέτης.

Κεφάλαιο 2: Θεωρητικό Υπόβαθρο

2.1 Εισαγωγή στην Κβαντική Πληροφορική

Στο παρόν κεφάλαιο θα παρουσιαστούν οι θεμελιώδεις έννοιες της Κβαντικής Μηχανικής Μάθησης (Quantum Machine Learning — QML) [28], οι οποίες αποτελούν τη θεωρητική βάση για την κατανόηση των μοντέλων που χρησιμοποιήθηκαν στην εργασία.

Συγκεκριμένα, θα αναλυθούν τα κβαντικά κυκλώματα, οι πύλες που τα συνθέτουν, καθώς και οι τεχνικές κωδικοποίησης (data encoding), μέσω των οποίων τα κλασικά δεδομένα μετασχηματίζονται σε κβαντικές καταστάσεις ώστε να είναι κατάλληλα προς επεξεργασία από ένα κβαντικό σύστημα [28-29].

Στη συνέχεια, θα παρουσιαστούν ολοκληρωμένα παραδείγματα τόσο αμιγώς κβαντικών όσο και υβριδικών κυκλωμάτων, τα οποία συνδυάζουν κλασικά και κβαντικά επίπεδα για την υλοποίηση πολύπλοκων αλγορίθμων μάθησης.

Τέλος, θα ακολουθήσει εκτενής ανάλυση των Κβαντικών Νευρωνικών Δικτύων (Quantum Neural Networks — QNNs), που αποτελούν τη βασική αρχιτεκτονική της παρούσας μελέτης [30],[31].

2.1.1 Το Κβαντικό Διάνυσμα και η Σφαίρα Bloch

Στην κβαντική φυσική και την θεωρία των κβαντικών υπολογιστών, μπορούμε να αποτυπώσουμε τις κβαντικές καταστάσεις με δύο διαφορετικούς τρόπους όπως θα δούμε στην συνέχεια.

2.1.1.1 Διανυσματική Μορφή του Qubit

Η κατάσταση ενός qubit περιγράφεται μαθηματικά από ένα διάνυσμα κατάστασης που ανήκει σε έναν δισδιάστατο διανυσματικό χώρο, ο οποίος ονομάζεται χώρος Hilbert και συμβολίζεται συνήθως ως H [28-29].

Ο χώρος Hilbert αποτελεί το μαθηματικό υπόβαθρο πάνω στο οποίο περιγράφονται οι κβαντικές καταστάσεις. Πρόκειται για έναν διανυσματικό χώρο με εσωτερικό γινόμενο, όπου κάθε διάνυσμα αντιστοιχεί σε μια φυσική κατάσταση του συστήματος, ενώ το μέτρο και η γωνία μεταξύ διανυσμάτων σχετίζονται με πιθανότητες και συσχετισμούς μεταξύ καταστάσεων [28]. Σε αυτόν τον χώρο δρουν οι γραμμικοί τελεστές που αναπαριστούν τις κβαντικές πύλες, καθορίζοντας πώς εξελίσσεται η κατάσταση του συστήματος κατά τη διάρκεια των υπολογισμών. [29]

Σε αυτόν τον χώρο, κάθε δυνατή κατάσταση του qubit μπορεί να εκφραστεί ως γραμμικός συνδυασμός δύο βασικών καταστάσεων, που σχηματίζουν την υπολογιστική βάση:

Συγκεκριμένα, η υπολογιστική βάση αποτελείται από τα εξής ορθοκανωνικά διανύσματα.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad , \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Τα διανύσματα αυτά είναι ορθοκανωνικά, δηλαδή είναι κάθετα μεταξύ τους και έχουν μοναδιαίο μήκος. [28-29].

Επομένως, οποιαδήποτε κβαντική κατάσταση ενός qubit μπορεί να εκφραστεί ως γραμμικός συνδυασμός των δύο βασικών διανυσμάτων της υπολογιστικής βάσης, δηλαδή των $|0\rangle$ και $|1\rangle$.

Αυτό σημαίνει ότι κάθε κατάσταση μπορεί να γραφεί στη μορφή:

$$|\psi\rangle = a|0\rangle + b|1\rangle = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix},$$

όπου $a, b \in \mathbb{C}$ δηλαδή είναι μιγαδικοί συντελεστές που καθορίζουν το ποσοστό συμμετοχής κάθε βασικής κατάστασης στην υπέρθεση [16]. Ο όρος «γραμμικός συνδυασμός» σημαίνει ότι το διάνυσμα $|\psi\rangle$ προκύπτει από το άθροισμα δύο άλλων διανυσμάτων (της βάσης) πολλαπλασιασμένων με κατάλληλους βαθμωτούς συντελεστές (τα α και β). Έτσι, το $|\psi\rangle$ ανήκει στον ίδιο διανυσματικό χώρο που ορίζεται από αυτά [28-29].

Η φυσική ερμηνεία των α και β είναι ότι οι τετραγωνικές τιμές των απόλυτων τιμών τους, $|\alpha|^2$ $και$ $|\beta|^2$, αντιστοιχούν στις πιθανότητες το qubit, κατά τη μέτρηση, να βρεθεί αντίστοιχα στις καταστάσεις $|0\rangle$ και $|1\rangle$. Η συνθήκη κανονικοποίησης ορίζει ότι το άθροισμα όλων των πιθανοτήτων πρέπει να είναι ίσο με 1:

$$|a|^2 + |b|^2 = 1$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

τότε το qubit βρίσκεται σε ισοβαρή υπέρθεση των δύο βασικών καταστάσεων, πράγμα που σημαίνει ότι έχει ίση πιθανότητα (50%) να μετρηθεί είτε η ιδιοτιμή του $|0\rangle$ είτε του $|1\rangle$. [17]

Έτσι, σαν αποτέλεσμα, στο τέλος του κυκλώματος, όταν δηλαδή γίνεται η μέτρηση των καταστάσεων, η μέτρηση του Qubit στη βάση $|0\rangle, |1\rangle$ είναι:

- Η πιθανότητα για το 0 είναι $|a|^2$,
- Η πιθανότητα για το 1 είναι $|b|^2$.

2.1.1.2 Bloch Sphere

Η αναπαράσταση, η οποία μόλις περιγράψαμε, η οποία βασίζεται στα διανύσματα $|0\rangle$ και $|1\rangle$, είναι εξαιρετικά χρήσιμη, αλλά χρησιμοποιείται κυρίως για μαθηματικούς σκοπούς. Δεν μπορούμε άμεσα να καταλάβουμε τη γεωμετρική απεικόνιση του qubit. Για την επίλυση του προβλήματος αυτό, χρησιμοποιούμε τη σφαίρα Bloch, η οποία είναι μια μοναδιαία σφαίρα στον $\mathbb{R}^3$ [32].

Η σφαίρα Bloch αποτελεί το γεωμετρικό χώρο απεικόνισης όλων των καθαρών καταστάσεων ενός qubit. Κάθε σημείο της επιφάνειάς της αντιστοιχεί σε μια μοναδική κβαντική κατάσταση της μορφής:

Αρχικά από την προηγούμενη ανάλυση είχαμε:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad όπου \qquad |\alpha|^2 + |\beta|^2 = 1,$$

Εφαρμόζουμε τώρα τους εξής συντελεστές:

$$\alpha = \cos\left(\frac{\theta}{2}\right), \qquad \beta = e^{i\Phi}\sin\left(\frac{\theta}{2}\right)$$

Έτσι, οποιαδήποτε κβαντική κατάσταση γράφεται ως εξής:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

όπου $0 \leq \theta \leq \pi$ και $0 \leq \phi < 2\pi$ είναι οι σφαιρικές συντεταγμένες που καθορίζουν τη θέση του διανύσματος πάνω στη σφαίρα Bloch. [32]

Αξίζει να σημειωθεί ότι μια καθολική (global) φάση $e^{i\gamma}\}$, η οποία πολλαπλασιάζει ολόκληρη την κατάσταση, δεν είναι φυσικά παρατηρήσιμη και δεν επηρεάζει τα μετρήσιμα αποτελέσματα. Μόνο οι σχετικές φάσεις μεταξύ των καταστάσεων $|0\rangle$ και $|1\rangle$ έχουν φυσική σημασία. Δηλαδή, οι πιθανότητες μέτρησης των καταστάσεων $|0\rangle$ και $|1\rangle$ εξαρτώνται αποκλειστικά από το μέτρο των συντελεστών:7

$$P(0) = |\alpha|^2 = cos^2\left(\frac{\theta}{2}\right) \kappa\alpha\iota\, P(1) = |\beta|^2 = sin^2\left(\frac{\theta}{2}\right),$$

Έτσι, κάθε καθαρή κβαντική κατάσταση απεικονίζεται ως μοναδιαίου μήκους διάνυσμα που ξεκινά από το κέντρο της σφαίρας και εκτείνεται προς ένα σημείο της επιφάνειάς της. Η κατάσταση $|0\rangle$ αντιστοιχεί στο βόρειο πόλο της σφαίρας και η $|1\rangle$ στο νότιο, ενώ όλες οι υπόλοιπες καταστάσεις βρίσκονται ενδιάμεσα. [32],[28]

Η αναπαράσταση αυτή είναι εξαιρετικά χρήσιμη διότι επιτρέπει να οπτικοποιήσουμε τις κβαντικές πύλες ως περιστροφές του διανύσματος κατάστασης πάνω στη σφαίρα Bloch. Για παράδειγμα, η πύλη Pauli-X αντιστοιχεί σε περιστροφή κατά π γύρω από τον άξονα x, ενώ η πύλη Hadamard τοποθετεί την κατάσταση σε υπέρθεση επάνω στον ισημερινό της σφαίρας.[29],[32]

Από την παραπάνω θεωρία προκύπτει το διάνυσμα Bloch:

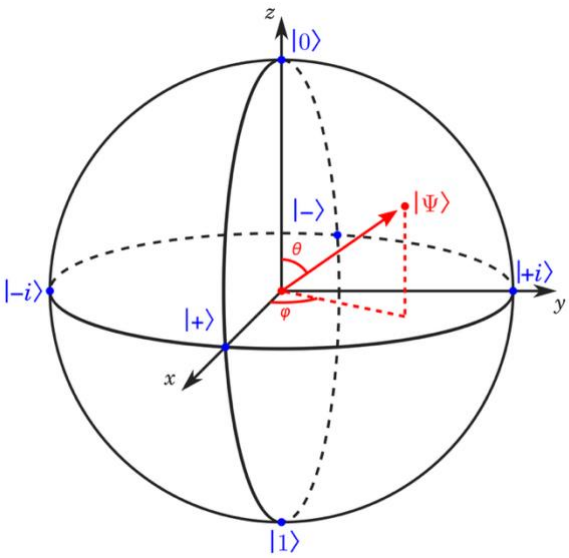
$$\vec{r} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

Δηλαδή ισχύει ότι:

$$x = \sin\theta\cos\,\phi$$
$$y = \sin\theta\sin\,\phi$$
$$z = \cos\theta$$

[29],[32]

Ως αποτέλεσμα, κάθε qubit έχει ακριβώς μια απεικόνιση στην σφαίρα Bloch.



Εικόνα 1 Η σφαίρα Bloch και ένα τυχαίο διάνυσμα.
https://prefetch.eu/know/concept/bloch-sphere/

Επιπλέον ένα σημαντικό χαρακτηριστικό κατά την παραπάνω απεικόνιση είναι ότι οποιαδήποτε μοναδιαία πράξη σε ένα qubit μπορεί να θεωρηθεί ως περιστροφή της σφαίρας γύρω από κάποιο άξονα. Περισσότερα σχετικά με τις μοναδιαίες πράξεις και περιστροφές θα δούμε στην συνέχεια. [28],[32].

2.2 Κβαντικά Κυκλώματα και Πύλες

2.2.1 Θεμελιώδη στοιχεία και αρχές

Ένα κβαντικό κύκλωμα (quantum circuit) αποτελείται από μια σειρά κβαντικών πυλών που εφαρμόζονται διαδοχικά πάνω στα qubits. Κάθε πύλη αντιπροσωπεύει έναν μοναδιαίο μετασχηματισμό, δηλαδή μια αντιστρέψιμη γραμμική απεικόνιση στον χώρο Hilbert [28-30].

Η δράση των πυλών αυτών μεταβάλλει την υπέρθεση και τις φάσεις των qubits, διαμορφώνοντας έτσι την τελική τους κβαντική κατάσταση (quantum state), η οποία περιγράφεται από το διάνυσμα κατάστασης (state vector).

Για όλες τις πύλες ισχύει η εξίσωση:

- $U^{+}U = I$

όπου U^{+} είναι ο συζυγής ανάστροφος πίνακας του U, και I ο μοναδιαίος πίνακας. [33]

Η σχέση αυτή δηλώνει ότι κάθε κβαντική πύλη είναι μοναδιαία (unitary), ώστε να διατηρείται η νόρμα του διανύσματος κατάστασης, δηλαδή:

$$\langle \psi' | \psi' \rangle = \langle \psi | \psi \rangle = 1$$

$$\mu\varepsilon\ |\psi'\rangle = U|\psi\rangle.$$

Ο όρος $\langle\psi|\psi\rangle$ εκφράζει το εσωτερικό γινόμενο (inner product) του διανύσματος κατάστασης με τον εαυτό του. Στην πράξη, αποτελεί το άθροισμα των τετραγώνων των μέτρων των συντελεστών της υπέρθεσης, δηλαδή:

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2$$

για ένα qubit στη μορφή $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Η ποσότητα αυτή αντιπροσωπεύει τη συνολική πιθανότητα εύρεσης του συστήματος σε οποιαδήποτε από τις δυνατές καταστάσεις. Για φυσικούς λόγους, πρέπει πάντα να ισούται με 1, γεγονός που εξασφαλίζεται από τη μοναδιαία φύση των κβαντικών πυλών. Με αυτόν τον τρόπο διατηρείται η αντιστρεψιμότητα του υπολογισμού και η διατήρηση της πληροφορίας σε όλη τη διάρκεια του κβαντικού υπολογισμού. [34]

Οι κβαντικές πύλες διακρίνονται σε δύο βασικές κατηγορίες [35]:

- Πύλες μονού qubit, που δρουν σε μία μόνο κβαντική μονάδα πληροφορίας.

- Πύλες πολλαπλών qubit, οι οποίες επιτρέπουν την αλληλεπίδραση μεταξύ qubits και τη δημιουργία διεμπλοκής, θεμελιώδους φαινομένου για την κβαντική παραλληλία και την επιτάχυνση των υπολογισμών.

Η δυνατότητα δημιουργίας και ελέγχου της διεμπλοκής μέσω τέτοιων πυλών αποτελεί τον πυρήνα της υπεροχής των κβαντικών υπολογιστών έναντι των κλασικών συστημάτων [28-30].

2.2.2 Πύλες Μονού Qubit:

Οι πύλες μονού qubit αποτελούν τους στοιχειώδεις μετασχηματισμούς στα κβαντικά κυκλώματα και αντιστοιχούν σε μοναδιαίους πίνακες 2×2 [35]. Ο λόγος για τον οποίο οι πίνακες αυτοί είναι διαστάσεων 2×2 έγκειται στο γεγονός ότι ο χώρος Hilbert ενός qubit είναι δύο διαστάσεων, δηλαδή εκτείνεται από τις βάσεις $|0\rangle$ και $|1\rangle$ όπου:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ και } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

Κάθε κατάσταση του qubit είναι γραμμικός συνδυασμός αυτών των δύο βάσεων,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad \text{όπου} \qquad |\alpha|^2 + |\beta|^2 = 1,$$

άρα κάθε γραμμικός μετασχηματισμός που διατηρεί την ορθοκανονικότητα του χώρου (δηλαδή είναι unitary) αναπαρίσταται από πίνακα μεγέθους 2×2. Οι πράξεις αυτές μπορούν να ερμηνευτούν γεωμετρικά ως περιστροφές της κατάστασης του qubit πάνω στη σφαίρα Bloch [32].

Οι πιο θεμελιώδεις τέτοιες πύλες είναι οι Pauli και η Hadamard, οι οποίες αποτελούν το βασικό αλφάβητο όλων των σύνθετων κβαντικών κυκλωμάτων.

Όλες οι πύλες μονού qubit ικανοποιούν τη συνθήκη μοναδιαίας μετασχηματιστικότητας:

$$U^\dagger U = I$$

γεγονός που εξασφαλίζει ότι η συνολική πιθανότητα του συστήματος διατηρείται αμετάβλητη.
Με άλλα λόγια, μετά από οποιαδήποτε κβαντική πράξη, το άθροισμα των πιθανοτήτων παραμένει ίσο με 1 (δηλαδή $|\alpha|^2 + |\beta|^2 = 1$), κάτι που αποτελεί φυσική απαίτηση για κάθε κβαντική εξέλιξη.

2.2.2.1 Η *Pauli-X*:

(ή κβαντική NOT) εκφράζεται από τον πίνακα

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

και εναλλάσσει τα δύο διανύσματα (ή καταστάσεις) της βάσης, δηλαδή $X|0\rangle = |1\rangle \; και \; X|1\rangle = |0\rangle$.

Με άλλα λόγια, η Pauli-X «αναποδογυρίζει» το qubit, όπως ακριβώς η λογική πύλη NOT στο κλασικό δυαδικό σύστημα. [35]

Γεωμετρικά, η επίδρασή της αντιστοιχεί σε περιστροφή κατά γωνία π (180°) γύρω από τον άξονα X της σφαίρας Bloch, αλλάζοντας τη θέση της κατάστασης από τον βόρειο στον νότιο πόλο (και αντίστροφα). [32]

Η πύλη αυτή αποτελεί μία από τις θεμελιώδεις πράξεις της κβαντικής λογικής και χρησιμοποιείται συχνά ως βασικό στοιχείο σε αλγορίθμους ελέγχου και αντιστροφής κατάστασης.

2.2.2.4 Pauli-Y

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

πραγματοποιεί περιστροφή γύρω από τον άξονα Y, εισάγοντας ταυτόχρονα και φασική μετατόπιση. Δρα στις βάσεις ως $Y|0\rangle = i|1\rangle \; και \; Y|1\rangle = -i|0\rangle$.

Η παρουσία της φανταστικής μονάδας i διαφοροποιεί την Pauli-Y από την Pauli-X, καθώς δεν πραγματοποιεί απλή αντιστροφή αλλά συνδυασμένη ενέργεια περιστροφής και αλλαγής φάσης, κάτι που την καθιστά ιδιαίτερα χρήσιμη για ελεγχόμενες περιστροφές και συνθέσεις πιο πολύπλοκων μοναδιαίων μετασχηματισμών. [28], [35]

2.2.2.3 Pauli-Z

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

και αντιστοιχεί σε περιστροφή κατά γωνία π (180°) γύρω από τον άξονα Z της σφαίρας Bloch.

Η επίδρασή της συνίσταται σε phase flip, δηλαδή σε αντιστροφή φάσης μόνο για τη βάση |1⟩, ενώ η βάση |0⟩ παραμένει αμετάβλητη:

$$Z|0\rangle = |0\rangle, \qquad Z|1\rangle = -|1\rangle.$$

Για γενική κατάσταση $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, προκύπτει $Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$.

Η πύλη αυτή δεν αλλάζει την πιθανότητα μέτρησης των καταστάσεων, αλλά επηρεάζει τη σχετική φάση τους, γεγονός κρίσιμο για φαινόμενα συμβολής (interference) και εμπλοκής (entanglement). [35]

Λόγω αυτής της ιδιότητας, η Pauli-Z αποτελεί βασικό εργαλείο για τη διαχείριση φάσης και χρησιμοποιείται εκτενώς σε κβαντικούς αλγορίθμους και κυκλώματα ελέγχου φάσης (phase control circuits). [30],[33]

2.2.2.4 Hadamard

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Η πύλη Hadamard δημιουργεί υπέρθεση μεταξύ των βασικών καταστάσεων, μετατρέποντας ένα καθορισμένο qubit σε ίση πιθανότητα μέτρησης 0 ή 1. Η λειτουργία αυτή είναι θεμελιώδης για την κβαντική παραλληλία και χρησιμοποιείται εκτενώς σε αλγορίθμους όπως του Grover και του Shor. Η σημασία της έγκειται στο ότι θέτει το qubit σε κατάσταση υπέρθεσης, μεταβαίνοντας από μια συγκεκριμένη ιδιοκατάσταση σε μια κατάσταση όπου βρίσκεται και στο “0” και στο “1” ταυτόχρονα — με ίση πιθανότητα — γεγονός που αποτυπώνεται καθαρά και στις αντίστοιχες μαθηματικές εξισώσεις. [35-36]

Συγκεκριμένα:

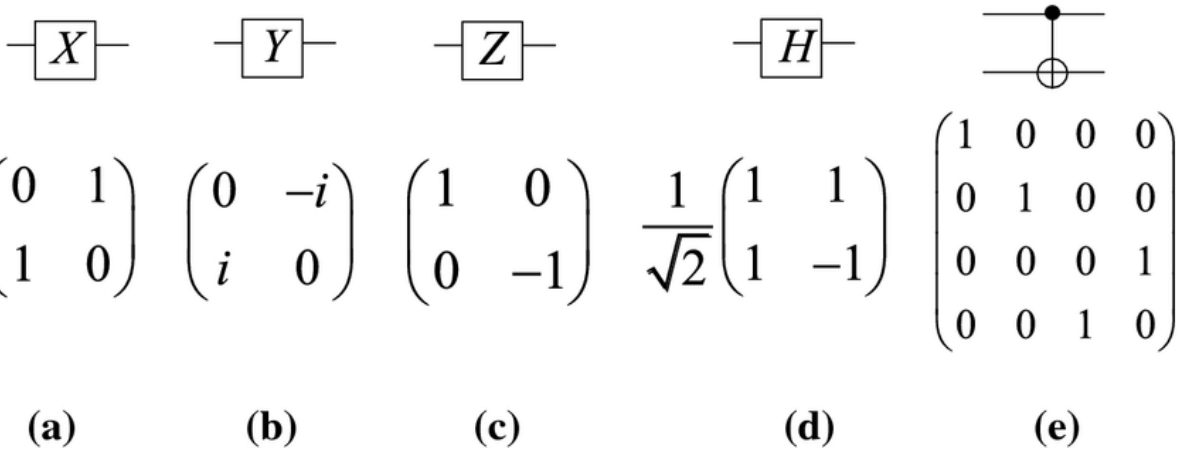
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Άρα οι πιθανότητες προκύπτουν ως εξής:

$$P(0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}, P(1) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

[30],[35]

Η παραπάνω ιδιότητα της πύλης Hadamard (H), δηλαδή η δυνατότητά της να μετατρέπει τις καθαρές καταστάσεις βάσης σε καταστάσεις υπέρθεσης, αποτελεί θεμέλιο λίθο για τη λειτουργία πολλών κβαντικών αλγορίθμων [35]. Με την εφαρμογή της H σε κάθε qubit, δημιουργείται μια ομοιόμορφη υπέρθεση όλων των δυνατών καταστάσεων του συστήματος, επιτρέποντας στον κβαντικό υπολογιστή να «εξερευνήσει» ταυτόχρονα ολόκληρο τον χώρο λύσεων. Αυτή η αρχή χρησιμοποιείται χαρακτηριστικά στον αλγόριθμο Grover, όπου η Hadamard είναι υπεύθυνη για την αρχικοποίηση της αναζήτησης μέσω ισοβαρούς υπέρθεσης όλων των δυνατών εισόδων, ενώ ο επαναλαμβανόμενος «ενισχυτικός» μηχανισμός του αλγορίθμου βασίζεται στη διατήρηση αυτής της δομής [36]. Αντίστοιχα, στον αλγόριθμο Deutsch–Jozsa, η Hadamard επιτρέπει την ταυτόχρονη αξιολόγηση μιας συνάρτησης για πολλαπλές εισόδους, οδηγώντας σε εκθετική επιτάχυνση σε σχέση με τους κλασικούς αλγορίθμους. Συνολικά, η δράση της H αποτελεί το πρώτο βήμα για την αξιοποίηση της κβαντικής παράλληλης επεξεργασίας, κάνοντας την πύλη αυτή ένα από τα πιο θεμελιώδη εργαλεία στον σχεδιασμό και την κατανόηση των κβαντικών αλγορίθμων. [35-37]



Εικόνα 2 Διάγραμμα και πίνακας κβαντικών πυλών: η πύλη Pauli-X, η πύλη Pauli-Y, η πύλη Pauli-Z, η πύλη Hadamard και η ελεγχόμενη πύλη CNOT (Controlled-NOT).

2.2.2.5 Οι Περιστροφικές Πύλες.

Πέρα από τις βασικές πύλες Pauli, σημαντική κατηγορία πινάκων μονού qubit αποτελούν οι περιστροφικές πύλες, οι οποίες επιτρέπουν την περιστροφή της κατάστασης του qubit γύρω από έναν συγκεκριμένο άξονα της σφαίρας Bloch κατά γωνία θ. Αυτές οι πύλες είναι εξαιρετικά κρίσιμες, καθώς επιτρέπουν την ακριβή ρύθμιση της κβαντικής κατάστασης και χρησιμοποιούνται ως παραμετρικά στοιχεία σε variational κβαντικά κυκλώματα και σε QNNs [38].

Συγκεκριμένα, για γωνία θ έχουμε [27]:

$$R_x(\theta) = e^{-i\frac{\theta}{2}X} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X$$

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}$$

Όπου η μήτρα του Ry(θ) είναι [27]:

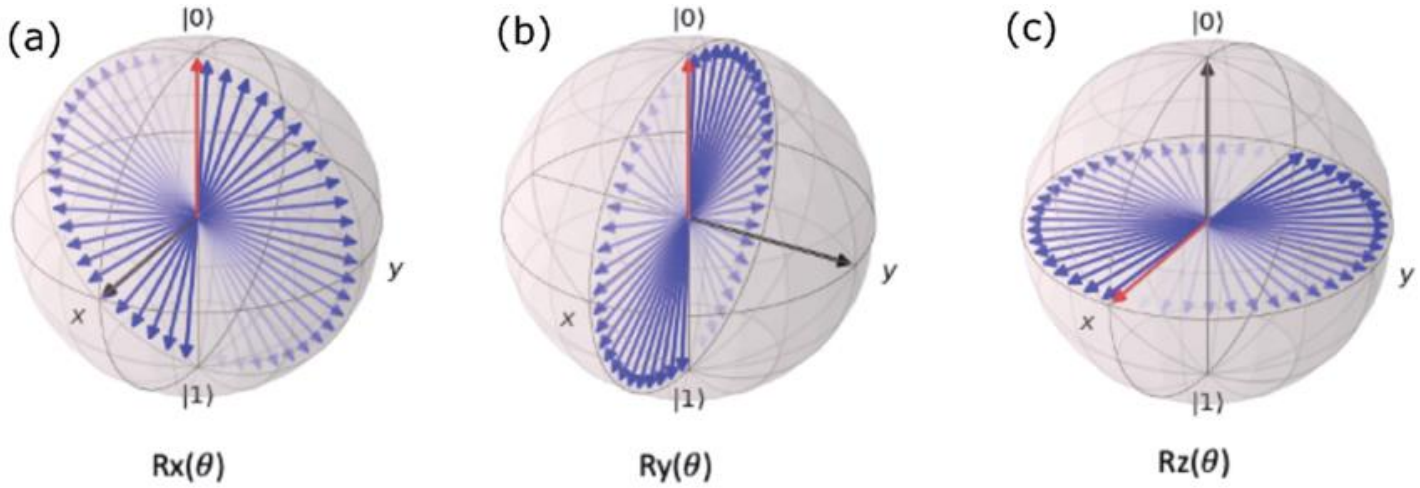
$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin(\frac{\theta}{2}) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

Εδώ πέρα βλέπουμε καθαρά -λόγω της ύπαρξης της γωνίας θ, ότι οι πύλες περιστροφής δρουν πάνω στο qubit, και τα ουσιαστικά αποτελέσματα φαίνονται πάνω στη Σφαίρα Bloch [32]. Αυτό που γίνεται είναι ότι οι πύλες περιστρέφουν κατά την γωνία θ γύρω από τον αντίστοιχο άξονα. Συγκεκριμένα οι πύλες περιστρέφουν αντίστοιχα.

$$R_x(\theta) \rightarrow x$$

$$R_y(\theta) \rightarrow y$$

$$R_z(\theta) \rightarrow \mathrm{z}$$



Εικόνα 3 Οι αλλαγές που προκύπτουν από τις πύλες περιστροφής πάνω στην σφαίρα Bloch. Εδώ μπορούμε να διακρίνουμε τους άξονες που επηρεάζει κάθε πύλη.

Πηγή: https://www.researchgate.net/figure/a-The-operation-R-x-y-which-involves-rotation-about-the-x-axis-marked-in-black-as_fig1_362097647

Στην κβαντική μηχανική μάθηση, οι προαναφερθέντες πύλες είναι εξαιρετικά σημαντικές και είναι τα δομικά στοιχεία των Variational Quantum Circuits (VQCs). [39] Αυτό ισχύει διότι όπως βλέπουμε καθαρά, οι πύλες αυτές παραμετροποιούνται με βάση την γωνία θ. Έτσι μπορούμε να χτίσουμε κυκλώματα τα οποία δεν είναι σταθερά (σε αντίθεση σε κυκλώματα που χρησιμοποιούν μόνο πύλες H,X,Y,CNOT) αλλά βασίζονται σε ένα σύνολο σταθερών που ορίζουν τις πύλες περιστροφής [37-38]. Επομένως έχουμε ένα κύκλωμα με παραμέτρους όπως ακριβώς έχουμε στην κλασσική περίπτωση του νευρωνικού δικτύου. Επομένως και στα κβαντικά νευρωνικά δίκτυα, ο στόχος είναι η εκπαίδευση των γωνιών θ, δηλαδή των παραμέτρων των πύλων αυτών, προκειμένου να ελαχιστοποιηθεί το σφάλμα. Παραπάνω για τα Variational Quantum Circuits θα δούμε και στην συνέχεια.

2.2.3 Εφαρμογή Πυλών σε Πολλαπλά Qubits

Έχουμε λοιπόν ορίσει τις πύλες οι οποίες δρούνε σε ένα μόνο qubit, οι οποίες πύλες είναι πίνακες διαστάσεων $2x2$. Όμως αυτό δεν αρκεί, καθώς ένα κβαντικό κύκλωμα περιέχει σχεδόν πάντα πολλαπλά qubit. Επομένως, ο συνολικός χώρος, Hilbert, έχει διάσταση 2^n, όπου *n* είναι ο αριθμός του qubit [29].

Για να περιγράψουμε μαθηματικά τις πράξεις στον χώρο αυτό, χρησιμοποιούμε το λεγόμενο τανυστικό γινόμενο (tensor product, $\otimes$) [28].

Το τανυστικό γινόμενο αποτελεί μια βασική πράξη στην κβαντική μηχανική, καθώς μας επιτρέπει να συνδυάζουμε ταυτόχρονα πολλαπλά κβαντικά συστήματα σε ένα ενιαίο, μεγαλύτερης διάστασης σύστημα [40].

Αν έχουμε δύο qubits με καταστάσεις:

$$|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle\,, |\psi_2\rangle = \gamma|0\rangle + \delta|1\rangle$$

τότε η συνολική κατάσταση του συστήματος δίνεται από το τανυστικό τους γινόμενο:

$$|\psi_{o\lambda}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

Η πράξη αυτή πολλαπλασιάζει τους διανυσματικούς χώρους των επιμέρους qubits, αυξάνοντας έτσι τη διάσταση του συνολικού χώρου Hilbert [28-29].

Για παράδειγμα, ενώ ένας qubit περιγράφεται από χώρο διάστασης 2, δύο qubits περιγράφονται από χώρο διάστασης $2^2 = 4$, τρία qubits από $2^3 = 8$, και ούτω καθεξής.

Το τανυστικό γινόμενο δεν είναι απλός αριθμητικός πολλαπλασιασμός· εκφράζει τη συσχέτιση των κβαντικών καταστάσεων. Μέσω αυτής της πράξης, οι καταστάσεις των qubits μπορούν να είναι σε κατάσταση διεμπλοκής, δηλαδή να είναι αλληλένδετες με τρόπο που δεν επιδέχεται διαχωρισμό στις επιμέρους καταστάσεις τους [41].

Έτσι, το τανυστικό γινόμενο αποτελεί το μαθηματικό εργαλείο που περιγράφει τη δομή και τη σύνδεση των πολλαπλών qubits σε κάθε κβαντικό κύκλωμα, επιτρέποντας την ανάπτυξη πολυσωματικών καταστάσεων που αποτελούν τη βάση της κβαντικής υπεροχής.

Ο τανυστής που ορίσαμε, μας βοηθάει να ορίσουμε σε ποιο qubit θα δράσει η πύλη κάθε φορά [42]. Αν θέλουμε να εφαρμόσουμε την πύλη U μόνο στο πρώτο qubit ενός συστήματος 3 qubits, ο συνολικός τελεστής γράφεται:

$$U \otimes I \otimes I$$

• Αντίστοιχα, αν η πύλη εφαρμόζεται μόνο στο δεύτερο qubit:

$$I \otimes U \otimes I$$

• Και αν στο τρίτο qubit:

$$I \otimes I \otimes U$$

Παράδειγμα:

$$H \otimes X \otimes Y$$

σημαίνει ότι εφαρμόζουμε Hadamard στο πρώτο qubit, Pauli-X στο δεύτερο και Pauli-Y στο τρίτο [43-44].

2.2.4 Υπολογιστικό Παράδειγμα.

Έστω ότι αρχικά έχουμε το εξής διάνυσμα:

$$|\psi_{\text{in}}\rangle = |000\rangle$$

Ορίζουμε:

$$U = H \otimes X \otimes Y$$

όπου:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$$

Τότε:

$$|\psi_{\text{out}}\rangle = U|\psi_{\text{in}}\rangle = (H|0\rangle) \otimes (X|0\rangle) \otimes (Y|0\rangle) = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes |1\rangle \otimes (i|1\rangle)$$

$$= \frac{i}{\sqrt{2}}(|011\rangle + |111\rangle)$$

Αυτό είναι και το τελικό διάνυσμα μετά την εφαρμογή των πυλών.

2.2.5 Πύλες Πολλαπλών Qubit:

Σε ένα σύστημα με n qubits, ο συνολικός χώρος Hilbert έχει διάσταση 2^n, γεγονός που σημαίνει ότι μπορεί να περιγράψει 2^n διαφορετικές καταστάσεις. Αυτή η εκθετική αύξηση του χώρου καταστάσεων αποτελεί τη βάση της κβαντικής παραλληλίας και της υπολογιστικής ισχύος των κβαντικών συστημάτων [28].

Για τις πύλες πολλαπλών qubit ισχύει ότι είναι μοναδιαίοι τελεστές της μορφής:

$$U \in \mathrm{U}(2^n), \qquad U^\dagger U = I_{2^n},$$

Τις πύλες αυτές τις ονομάζουμε πύλες διεμπλοκής και η δράση τους δεν είναι δυνατόν να γραφτεί ως τανυστικό γινόμενο τοπικών πράξεων [45]. Δηλαδή δεν υπάρχει η εξίσωση

$$U \neq U_1 \otimes U_2 \otimes \cdots \otimes U_n.$$

Οι πύλες διεμπλοκής το επιτρέπουν αυτό γιατί δημιουργούν συσχετίσεις μεταξύ των qubits που δεν μπορούν να περιγραφούν με κλασικούς όρους. Με άλλα λόγια, η κατάσταση ενός qubit εξαρτάται άμεσα από την κατάσταση των υπολοίπων, ανεξάρτητα από την απόσταση μεταξύ τους. Αυτό οδηγεί σε εκθετική αύξηση της υπολογιστικής ισχύος, καθώς ένα σύστημα με n διεμπλεκόμενα qubits μπορεί να αναπαραστήσει ταυτόχρονα 2^n διαφορετικές καταστάσεις. Έτσι, οι πύλες διεμπλοκής επιτρέπουν στον κβαντικό υπολογιστή να εκτελεί παράλληλους υπολογισμούς που είναι πρακτικά αδύνατοι για τα κλασικά συστήματα. [46] Δίχως αυτές, ουσιαστικά έχουμε single-qubit πράξεις άρα δεν έχουμε κάποια ουσιαστική κβαντική επιτάχυνση.

Για δύο-qubit τελεστή $V \in \mathrm{V}(4)$ που δρα στα i<j,

$$V^{(i,j)} = I^{\otimes i} \otimes V \otimes I^{\otimes(n-j-1)}$$

Στην περίπτωση αυτή, ο τελεστής $V^{(i,j)}$ εκφράζει τη δράση μιας πύλης που δρα ταυτόχρονα σε δύο qubits μέσα σε ένα μεγαλύτερο κβαντικό σύστημα. Με άλλα λόγια, αν φανταστούμε ότι έχουμε πολλά qubits, ο συγκεκριμένος τελεστής «στοχεύει» μόνο δύο από αυτά, αφήνοντας τα υπόλοιπα ανεπηρέαστα μέσω της ταυτότητας (Identity), ενώ εφαρμόζει τον πραγματικό μετασχηματισμό μόνο στα qubits i και j [47].

Αυτός ο μηχανισμός είναι ο τρόπος με τον οποίο τα qubits συνδέονται μεταξύ τους και παύουν να λειτουργούν ανεξάρτητα. Μέχρι αυτό το σημείο, κάθε qubit μπορούσε να υποστεί μετασχηματισμούς μόνο του — δηλαδή, να αλλάξει την κατάστασή του χωρίς να επηρεάσει τα υπόλοιπα. Όταν όμως εφαρμόζεται μια τέτοια two-qubit gate, οι καταστάσεις τους μπλέκονται (entangle) και πλέον δεν μπορούμε να περιγράψουμε το κάθε qubit χωριστά· η κατάσταση του ενός εξαρτάται άμεσα από την κατάσταση του άλλου [48].

Αυτή η «συσχέτιση» δεν είναι απλή επικοινωνία ή ανταλλαγή δεδομένων· είναι μια βαθύτερη φυσική σύνδεση, μοναδική στην κβαντική φυσική, η οποία δεν έχει ανάλογο στον κλασικό κόσμο [49]. Για παράδειγμα, αν μετρήσουμε το ένα από τα δύο qubits, το αποτέλεσμα της μέτρησης καθορίζει ακαριαία

την κατάσταση του άλλου, ακόμη κι αν βρίσκονται σε διαφορετικά σημεία — κάτι που δεν μπορεί να εξηγηθεί με τους κανόνες της κλασικής πληροφορικής.

Γι' αυτό και οι πύλες αυτού του τύπου θεωρούνται το πιο κρίσιμο συστατικό των Variational Quantum Circuits (VQCs) [50]. Είναι αυτές που δημιουργούν τα entangling layers, δηλαδή τα στρώματα όπου πραγματοποιείται η πραγματική αλληλεπίδραση μεταξύ των qubits. Χωρίς αυτές, κάθε qubit θα εξελισσόταν μεμονωμένα, οπότε το σύστημα δεν θα μπορούσε να αξιοποιήσει τη συλλογική κβαντική συμπεριφορά που αποτελεί και την πηγή της κβαντικής επιτάχυνσης. [48-50].

2.2.5.1 CNOT (Controlled-NOT)

Η πύλη CNOT (Controlled-NOT) αποτελεί μία από τις θεμελιώδεις πύλες δύο qubit, καθώς εισάγει την έννοια του ελέγχου μεταξύ τους. Το πρώτο qubit λειτουργεί ως qubit ελέγχου, ενώ το δεύτερο ως qubit-στόχος [51]. Αν το qubit ελέγχου βρίσκεται στην κατάσταση $|1\rangle$, τότε η CNOT αναστρέφει την τιμή του στόχου, διαφορετικά το αφήνει αμετάβλητο. Με αυτόν τον τρόπο, η CNOT επιτρέπει τη δημιουργία αλληλεξάρτησης μεταξύ των qubits, η οποία αποτελεί τη βάση για την εμφάνιση του φαινομένου της διεμπλοκής (entanglement). [28-29]

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, |c,t\rangle \mapsto |c, t \oplus c\rangle$$

Παραδείγματα:

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle$$

Όταν η CNOT εφαρμοστεί σε καταστάσεις υπέρθεσης, όπως μετά από την πύλη Hadamard, το αποτέλεσμα είναι η παραγωγή διεμπλεγμένων καταστάσεων, γνωστών ως Bell states. Οι καταστάσεις αυτές είναι καθαρά κβαντικές χωρίς κλασικό ανάλογο και έχουν θεμελιώδη σημασία για την κβαντική επικοινωνία, την τηλεμεταφορά και τους αλγορίθμους υπεροχής. [28-29],[47]

$$(H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{\mathrm{CNOT}}{\to} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle,$$

2.2.5.2 CZ (Controlled - Z)

Η πύλη CZ (Controlled-Z) είναι επίσης μια διδιάστατη πύλη ελέγχου, η οποία εφαρμόζει την πύλη Z στο qubit-στόχο μόνο όταν το qubit ελέγχου βρίσκεται στην κατάσταση $|1\rangle$. Σε αντίθεση με την CNOT, η CZ δεν αλλάζει τις λογικές τιμές των qubits, αλλά εισάγει μια αντιστροφή φάσης στην κατάσταση $|11\rangle$, καθιστώντας την ιδανική για τη δημιουργία entanglement χωρίς αλλαγή της υπολογιστικής βάσης [28-29].

Η δράση της μπορεί να περιγραφεί ως εξής:

$$\mathrm{CZ} = \mathrm{diag}(1,1,1,-1), |c,t\rangle \mapsto (-1)^{c \cdot t}|c,t\rangle$$

Ισχύουν οι σχέσεις:

$$CZ|00\rangle = |00\rangle,$$

$$CZ|01\rangle = |01\rangle,$$

$$CZ|10\rangle = |10\rangle,$$

$$CZ|11\rangle = -|11\rangle.$$

Η πύλη αυτή συνδέεται στενά με την CNOT, καθώς μπορούν να μετατραπούν η μία στην άλλη μέσω των πυλών Hadamard, όπως φαίνεται στην παρακάτω σχέση [28-29]:

$$\mathrm{CNOT} = (I \otimes H)\ \mathrm{CZ}(I \otimes H),$$

2.3 Ρόλος των πυλών στις αρχιτεκτονικές QML / VQCs

Τώρα, έχοντας οριοθετήσει τις διάφορες πύλες που χρησιμοποιούνται στα κβαντικά κυκλώματα, μπορούμε να συνδυάσουμε τις γνώσεις μας και να ξεκινήσουμε μία εισαγωγή στα κυκλώματα των Variational Quantum Circuits.

- Συγκεκριμένα, στις αρχιτεκτονικές αυτές, οι πύλες είναι τα κύρια δομικά στοιχεία τα οποία ορίζουν πώς η πληροφορία ρέει, επεξεργάζεται και μαθαίνεται μέσα στο κύκλωμα κάθε qubit ξεχωριστά. [52]

Συγκεκριμένα, έχουμε την εξής δομή η οποία βασίζεται σε δύο κύριες περιοχές.

- Την πρώτη περιοχή, όπου έχουμε τοπικές πύλες, single qubit, οι οποίες επηρεάζουν την κατάσταση του κάθε qubit ξεχωριστά. [53]

- Entangled gates, οι οποίες δημιουργούν το entanglement μεταξύ των qubit, το οποίο, όπως αναφέραμε και προηγουμένως, οδηγούν σε αυξημένη ικανότητα εκφραστικότητας. [54]

Η ισορροπία και η σωστή ακολουθία αυτών των δύο περιοχών πυλών είναι αυτή που ουσιαστικά προσδίδει στο κύκλωμα την ικανότητα να μάθει πολύπλοκα πρότυπα πέρα από τις κλασσικές νευρονικές δομές. [55]

2.4 Κβαντικά Νευρωνικά Δίκτυα

2.4.1 Εισαγωγή

Η βασική ιδέα πίσω από τα Κβαντικά Νευρωνικά Δίκτυα (Quantum Neural Networks - QNNs) έγκειται στο ότι κάθε επίπεδο (layer) ενός τέτοιου δικτύου μπορεί να θεωρηθεί ως ένας κβαντικός μετασχηματισμός, ο οποίος αντιστοιχεί σε μια κβαντική χαρτογράφηση (quantum mapping) που ενεργεί πάνω στην κατάσταση του συστήματος. Με άλλα λόγια, κάθε layer υλοποιεί μια συγκεκριμένη απεικόνιση από μια αρχική σε μια τελική κβαντική κατάσταση, σύμφωνα με τους κανόνες της κβαντικής μηχανικής. [56]

Η κβαντική χαρτογράφηση αποτελεί έναν γενικό μηχανισμό περιγραφής της δυναμικής εξέλιξης ενός κβαντικού συστήματος. Η κατάσταση ενός qubit ή ενός συνόλου qubits περιγράφεται μέσω ενός πίνακα πυκνότητας (density matrix) ρ, ο οποίος περιλαμβάνει όλη την πληροφορία για το σύστημα και ικανοποιεί δύο θεμελιώδεις ιδιότητες: είναι θετικά ημι-ορισμένος ($\rho \geq 0$) και έχει ίχνος ίσο με τη

μονάδα (Tr(ρ) = 1). Οι ιδιότητες αυτές εξασφαλίζουν ότι όλες οι πιθανότητες είναι θετικές και ότι η συνολική πιθανότητα εύρεσης του συστήματος σε κάποια κατάσταση είναι ίση με 1. [56-57]

Ο πίνακας πυκνότητας μπορεί να αναπαριστά είτε μια καθαρή κατάσταση, όταν το σύστημα περιγράφεται πλήρως από ένα διάνυσμα κατάστασης $|\psi\rangle$, είτε μια μεικτή κατάσταση, όταν το σύστημα αποτελεί στατιστικό μείγμα διαφορετικών καθαρών καταστάσεων. Οι μεικτές καταστάσεις χρησιμοποιούνται για να περιγράψουν φαινόμενα θορύβου ή αλληλεπίδρασης με το περιβάλλον, που είναι αναπόφευκτα σε ρεαλιστικά κβαντικά συστήματα. [58]

Στο πλαίσιο των QNNs, η χρήση του πίνακα πυκνότητας καθιστά δυνατή τη μαθηματικά συνεπή περιγραφή της εξέλιξης της πληροφορίας μέσω διαδοχικών χαρτογραφήσεων, διασφαλίζοντας τη διατήρηση της κανονικοποίησης και τη φυσική εγκυρότητα του μοντέλου. [56],[59]

Έτσι για τον πίνακα πυκνότητας (density matrix) ρ ισχύουν τα εξής:

$$\rho \geq 0 \,, \qquad \mathrm{Tr}(\rho) = 1$$

Ο πίνακας αυτός μπορεί να αντιστοιχεί σε μια καθαρή κατάσταση:

$$\rho = |\psi\rangle\langle\psi|$$

είτε ένα μεικτό σύστημα:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Όπως αναφέραμε οι στρώσεις του QNN αποτελούν μια απεικόνιση για την οποία ισχύει ότι είναι:

- Εντελώς θετική (Completely-Positive)
- Ιχνοδιατηρητική (Trace-Preserving)

Οι ιδιότητες αυτές εξασφαλίζουν ότι η εξέλιξη του συστήματος περιγράφει μια φυσικά επιτρεπτή κβαντική διεργασία, δηλαδή μια μετασχηματιστική πράξη που δεν παραβιάζει τις αρχές της κβαντικής μηχανικής. Συγκεκριμένα, η εντελώς θετικότητα διασφαλίζει ότι ακόμη και όταν το σύστημα συζευχθεί με ένα περιβάλλον, η συνολική κατάσταση παραμένει φυσικά αποδεκτή (δηλαδή χωρίς αρνητικές ιδιοτιμές), ενώ η ιδιότητα της ιχνοδιατήρησης εξασφαλίζει ότι η συνολική πιθανότητα παραμένει ίση με τη μονάδα. Έτσι, κάθε στρώση του QNN μπορεί να θεωρηθεί ως κβαντικό κανάλι που περιγράφει μια έγκυρη και σταθερή εξέλιξη της πληροφορίας. [56],[58]

Οι ιδιότητες αυτές δημιουργούν τις CPTP map και ισχύει η παρακάτω σχέση:

$$\rho_{\text{out}} = \mathcal{E}(\rho_{\text{in}})$$

Το $\mathcal{E}$ στην παραπάνω εξίσωση περιγράφει την εξέλιξη του συστήματος από την είσοδο έως την έξοδο και αποτελεί το quantum mapping που αναφέραμε [56-58].

Μπορούμε να γενικεύσουμε την παραπάνω σχέση με την χρήση των τελεστών Kraus K_i:

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger \,, \sum_i K_i^\dagger K_i = I$$

Στην ιδανική κατάσταση όπου έχουμε ένα απομονωμένο σύστημα, η χαρτογράφηση είναι μοναδιαία (όπως ακριβώς και οι πύλες που αναλύσαμε προηγουμένως). Στην περίπτωση αυτή, ένας μοναδιαίος πίνακας U για τον οποίο θα ισχύει [58]:

$$U^{\dagger}U = UU^{\dagger} = I$$

Επομένως η εξέλιξη γράφεται ως:

$$\rho_{out} = U\rho_{in}U^{\dagger}$$

Εδώ, μπορούμε να κάνουμε μια πρώτη σύνδεση με το παραπάνω κεφάλαιο όπου μελετήσαμε τις κβαντικές πύλες [57]. Συγκεκριμένα, κάθε τέτοιος μοναδιαίος μετασχηματισμός αντιστοιχεί σε μια κβαντική πύλη (quantum-gate) όπως η Pauli-X, Hadamard, CNOT κτλ.

Στο σύνολό του, ένα κβαντικό νευρωνικό δίκτυο με L στρώσεις, μπορεί να αναλυθεί ως εξής [56]:

$$\rho_{\text{out}} = \mathcal{E}_1 \circ \mathcal{E}_2 \circ \ldots \circ \mathcal{E}_L(\rho in)$$

Όπου κάθε $\mathcal{E}_L$ μπορεί να είναι είτε

- Μοναδιαίος (Unitary - ideal)
- Μη-Μοναδιαίος (Non-Unitary non-ideal) CPTP map

Να σημειωθεί εδώ ότι στην μελέτη μας θα αφοσιωθούμε αποκλειστικά στα συστήματα τα οποία είναι πλήρως απομονωμένα από το περιβάλλον άρα και δίχως θόρυβο, απώλειες ή μετρήσεις κατά την εξέλιξη. [56-58]

Άρα έχουμε:

$$\rho_{out} = U\rho_{in}U^{\dagger}$$

Όπου ισχύει για τον U

$$U^{\dagger}U = UU^{\dagger} = I$$

2.4.2 Αρχιτεκτονική του Δικτύου

Όπως αναφέρθηκε και προηγουμένως, ένα Κβαντικό Νευρωνικό Δίκτυο (Quantum Neural Network – QNN) αποτελείται από επαναλαμβανόμενα στρώματα που υλοποιούν μοναδιαίους μετασχηματισμούς. Η διαφορά σε σχέση με τα κλασικά νευρωνικά δίκτυα έγκειται στο ότι, ενώ στα κλασικά δίκτυα η επεξεργασία των δεδομένων βασίζεται σε γραμμικούς συνδυασμούς που ακολουθούνται από μη γραμμικές συναρτήσεις ενεργοποίησης, στα κβαντικά δίκτυα η επεξεργασία πραγματοποιείται αποκλειστικά μέσω μοναδιαίων τελεστών, δηλαδή αναστρέψιμων γραμμικών μετασχηματισμών στον χώρο Hilbert.[50],[61]

Συνεπώς, στα Κβαντικά Νευρωνικά Δίκτυα οι μοναδιαίοι μετασχηματισμοί είναι γραμμικοί ως προς την κατάσταση του συστήματος. Η εξέλιξη της κατάστασης περιγράφεται από τη σχέση

$$\rho_{out} = U\rho_{in}U^{\dagger}$$

ενώ η τελική μέτρηση οδηγεί σε γραμμικές προσδοκίες τιμών, οι οποίες υπολογίζονται μέσω της σχέσης:

$$\langle O \rangle = Tr(O\rho_{out}).$$

όπου Ο είναι ο τελεστής παρατήρησης (observable) και ρ ο πίνακας πυκνότητας που περιγράφει την κατάσταση του συστήματος. Η παραπάνω εξίσωση εκφράζει τη μέση τιμή του φυσικού μεγέθους που αντιστοιχεί στον τελεστή Ο, σύμφωνα με την τρέχουσα κατάσταση του συστήματος. [50-51],[61]

Παρόλα αυτά, το δίκτυο επιδεικνύει μη γραμμική συμπεριφορά ως προς τις εισόδους και τις παραμέτρους του. Αυτή η μη γραμμικότητα προκύπτει από τον τρόπο που τα δεδομένα ενσωματώνονται σε παραμετρικές πύλες (data encoding) και από τη μη γραμμική εξάρτηση της εξόδου από τις γωνίες των πυλών περισσότερα για την ιδιότητα αυτή θα αναλύσουμε και στην συνέχεια.

Το entanglement παίζει κρίσιμο ρόλο ενισχύοντας την εκφραστικότητα του μοντέλου· επιτρέπει πολύπλοκες συσχετίσεις μεταξύ των qubits, αυξάνοντας έτσι την ικανότητα του δικτύου να μαθαίνει μη γραμμικούς συσχετισμούς στα δεδομένα. [28-29], [50-51]

Στα κβαντικά δίκτυα, τα βάρη εμφανίζονται στις πύλες περιστροφής Rx, Ry, Rz οι οποίες είναι παραμετροποιημένες. Στόχος επομένως της μάθησης είναι η βέλτιστη επιλογή των γωνιών των πυλών αυτών προκειμένου να ελαχιστοποιηθεί το σφάλμα. [50],[61]

Υπενθυμίζουμε ότι για τις περιστροφικές πύλες ισχύουν οι παρακάτω σχέσεις [39]:

$$R_x(\theta) = e^{-i\frac{\theta}{2}X} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X$$

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}$$

Το QNN έχουν 3 βασικά μέρη στην δομή του κυκλώματος

- Data Encoding: Η μετατροπή των κλασσικών δεδομένων που υπάρχουν, σε κβαντικές καταστάσεις που είναι κατανοητές από ένα κύκλωμα (amplitude encoding, angle encoding etc.) [62].

$$|\psi_{\text{enc}}(\text{x})\rangle = U_{\text{enc}}(\text{x})|0\rangle^{\otimes n}$$

- Variational Quantum Circuit: Είναι το παραμετροποιημένο κβαντικό κύκλωμα το οποίο περιέχει τις πύλες Rx, Ry,Rz που περιέχουν τα βάρη του μοντέλου [63].

$$|\psi_{\text{out}}\rangle = U_{\text{var}}(\theta)|\psi_{\text{enc}}(\text{x})\rangle$$

- Measurement: Η μέτρηση αποτελεί το τελικό στάδιο ενός κβαντικού κυκλώματος, όπου η κβαντική κατάσταση μετατρέπεται σε κλασική πληροφορία. Κατά τη διαδικασία αυτή, η υπέρθεση των καταστάσεων "καταρρέει" σε μία από τις δυνατές ιδιοκαταστάσεις της παρατηρήσιμης που μετράμε. Συνήθως, το αποτέλεσμα εκφράζεται μέσω της αναμενόμενης τιμής του τελεστή μέτρησης, δηλαδή της μέσης τιμής που θα προκύψει αν επαναλάβουμε τη μέτρηση πολλές φορές στο ίδιο κύκλωμα.

  Η τιμή εξόδου λαμβάνεται ως αναμενόμενη τιμή της Ο, δηλαδή:

$$y = \langle\psi_{\text{out}}|O|\psi_{\text{out}}\rangle$$

  Στην πράξη, το y εκτιμάται ως ο μέσος όρος πολλών επαναλήψεων (shots) της ίδιας μέτρησης. [28-29],[63]

2.4.3 Data Encoding

Για να εφαρμόσουμε Quantum Machine Learning (QML), είναι απαραίτητο να μετατρέψουμε τα κλασικά δεδομένα —όπως διανύσματα χαρακτηριστικών ή αριθμητικές μεταβλητές— σε κβαντικές καταστάσεις. Η διαδικασία αυτή, γνωστή ως κβαντική κωδικοποίηση (quantum encoding ή embedding), επιτρέπει στο κβαντικό κύκλωμα να "αντιληφθεί" και να επεξεργαστεί τις πληροφορίες σύμφωνα με τους νόμους της κβαντικής μηχανικής. [62]

Οι διάφορες τεχνικές κωδικοποίησης (όπως η amplitude, angle ή basis encoding) διαφέρουν ως προς την πολυπλοκότητα υλοποίησης, την ευαισθησία τους στο θόρυβο και κυρίως στον αριθμό των qubits που απαιτούνται για την αναπαράσταση των δεδομένων. Η επιλογή της κατάλληλης μεθόδου αποτελεί κρίσιμο βήμα, καθώς επηρεάζει άμεσα την απόδοση, τη γενικευσιμότητα και την πρακτική υλοποιησιμότητα του κβαντικού μοντέλου. [62],[64]

2.4.3.1 Basis Encoding

Μία από τις πιο απλές τεχνικές κωδικοποίησης δεδομένων είναι το Basis Encoding. Η βασική ιδέα είναι ότι κάθε δυαδική αναπαράσταση ενός αριθμού i αντιστοιχεί άμεσα σε μία κατάσταση της υπολογιστικής βάσης $|i\rangle$ ενός συστήματος n qubits. Έτσι, μπορούμε να απεικονίσουμε ένα διάνυσμα τιμών (συνήθως διακριτών, π.χ. bits) ως μια συγκεκριμένη κβαντική κατάσταση [64]. Αν έχουμε n qubits, το σύστημα μπορεί να αναπαραστήσει 2^n διαφορετικές καταστάσεις βάσης:

$$|0\rangle, |1\rangle, |2\rangle, \dots, |2^n - 1\rangle$$

όπου

$$|i\rangle = |b_1 b_2 \dots b_n\rangle$$

και κάθε $b_j \in \{0,1\}$.

Για παράδειγμα, αν έχουμε δύο qubits, τότε οι τέσσερις δυνατές καταστάσεις είναι:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

Παράδειγμα:

Αν έχουμε ένα δυαδικό διάνυσμα:

$$x = 1001$$

Αυτό αντιστοιχεί άμεσα στην 4-qubit quantum state:

$$|x\rangle = |1001\rangle$$

Δηλαδή για κάθε bit του κλασσικού διανύσματος, χρειαζόμαστε ένα qubit, άρα για ένα διάνυσμα N χαρακτηριστικών, χρειαζόμαστε τουλάχιστον N qubit [64]. Αν έχουμε (όπως αναφέραμε και προηγουμένως) ένα σύνολο δεδομένων D με M παραδείγματα όπου ισχύει:

$$x^{(m)} = (b_1, b_2, \dots b_n), \qquad b_i = \{0,1\}$$

τότε κάθε διάνυσμα θα μεταφερθεί στην κβαντική κατάσταση ως:

$$|x^{(m)}\rangle = |b_1 b_2 \dots b_n\rangle$$

Άρα ολόκληρο το dataset μπορεί να αναπαρασταθεί ως υπέρθεση των επιμέρους καταστάσεων [64]:

$$|D\rangle = \frac{1}{\sqrt{M}} \sum_{m=1}^{m} |x^{(m)}\rangle$$

Το πλεονέκτημα είναι ότι η παραπάνω κωδικοποίηση είναι εξαιρετικά απλή στην υλοποίηση και δεν απαιτεί πολύπλοκα κυκλώματα ή κανονικοποιήσεις. Όμως απαιτείται μεγάλος αριθμός qubit αφού χρειαζόμαστε ένα για κάθε χαρακτηριστικό [64].

Η μεθοδολογία χρησιμοποιείται συχνά σε αλγορίθμους όπου έχουμε διακριτά ή δυαδικά δεδομένα (π.χ. quantum search problems ή encoding labels) [64].

2.4.3.2 Angle Encoding (ή Rotation Encoding)

Το Angle Encoding είναι ένας αρκετά απλός τρόπος για να μετατρέψουμε τα κλασσικά δεδομένα σε κβαντικές καταστάσεις που στην συνέχεια μπορούμε να κωδικοποιήσουμε σε qubits. Η μεθοδολογία βασίζεται στην ιδέα ότι κάθε χαρακτηριστικό (feature) x_i από το διάνυσμα των δεδομένων αντιστοιχεί σε μια γωνία περιστροφής ενός qubit.[64-65]

Έστω δηλαδή ότι έχουμε ένα διάνυσμα χαρακτηριστικών:

$$x = (x_1 , x_2, \dots, x_n)$$

Τότε μετά την κωδικοποίηση, η κβαντική κατάσταση θα είναι η εξής:

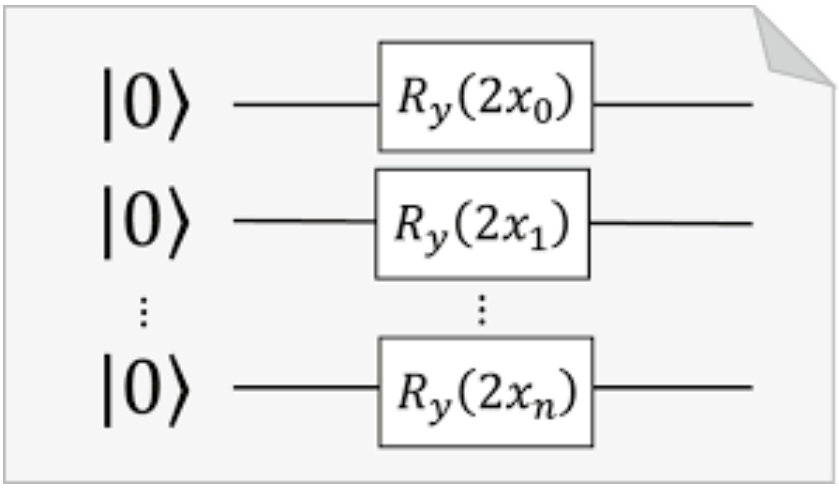
$$|\psi\rangle = (R_y(x_1) \otimes R_y(x_2) \otimes \cdots \otimes R_y(x_n)) \, |00 \cdots 0\rangle.$$

Όπου

$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin(\frac{\theta}{2}) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

$$|\psi\rangle = (R_y(2x_1) \mid 0\rangle) \otimes (R_y(2x_2) \mid 0\rangle).$$

Ουσιαστικά με αυτό τον τρόπο κωδικοποίησης, σε κάθε qubit εφαρμόζεται μια πύλη $R_y(\theta)$ όπου για την γωνία θ ισχύει ότι $2x_1 = \theta$. Οπότε ουσιαστικά κάθε χαρακτηριστικό καθορίζει την τελική κατάσταση του αντίστοιχου qubit στην σφαίρα Bloch [64-65].



Εικόνα 4 Quantum circuit for loading data in angle encoding [11]

2.4.3.3 Amplitude Encoding

Το amplitude encoding είναι ένας πολύ χρήσιμος τρόπος για την κωδικοποίηση των δεδομένων καθώς μας επιτρέπει να απεικονίσουμε ένα κλασσικό N-διαστάσεων διάνυσμα (στο πεδίο των πραγματικών είτε και των μιγαδικών) στα "amplitudes" (ύψη) των quantum states $\log_2 N$ qubits:
Μαθηματικά, η ιδέα περιγράφεται ως εξής:

$$|\psi\rangle = \frac{1}{\|x\|}\sum_{i=0}^{N-1} x_i|i\rangle, \quad \text{όπου} \quad \|x\| = \sqrt{\sum_i |x_i|^2}$$

Εδώ, η $|i\rangle$ είναι η υπολογιστική βάση των $\log_2 N$ qubits. Ουσιαστικά κάνουμε mapping κάθε χαρακτηριστικό (feature) σε μια κατάσταση του $|i\rangle$.
Όπου:

$$|i\rangle = |b_{n-1}b_{n-2}b_{n-3}\dots b_o\rangle$$

Οπότε πρακτικά το amplitude encoding, κάθε feature x_i είναι το πλάτος του διανύσματος του $|i\rangle$. Ο αριθμός i ορίζει ποιο χαρακτηριστικό (feature) εξετάζουμε. Η κατάσταση $|i\rangle$ είναι η n-qubit κατάσταση όπου το bit-string αντιστοιχεί στη δυαδική αναπαράσταση του i. Ο συντελεστής που αντιστοιχεί στο $|i\rangle$ "φορτώνει" το συγκεκριμένο feature στο πλάτος (amplitude) της κατάστασης $|i\rangle$.Μπορούμε να καταλάβουμε περισσότερο την παραπάνω ανάλυση με ένα παράδειγμα:

Έστω ότι έχουμε το διάνυσμα:

$$\mathrm{x} = (\mathrm{x}_1, \mathrm{x}_2, \dots, \mathrm{x}_n)$$

Ισχύει η σχέση κανονικοποίησης :

$$\sum |\mathrm{x_i}|^2 = 1 \rightarrow \frac{1}{\|x\|} = 1$$

Οπότε τελικά έχουμε:

$$|\psi\rangle = \mathrm{x}_1|00\ldots0\rangle + \mathrm{x}_2|00\ldots1\rangle + \ldots + \mathrm{x}_n|11\ldots1\rangle$$

Το εξαιρετικά σημαντικό και χρήσιμο σχετικά με τον παραπάνω τρόπο κωδικοποίησης είναι ότι με μόλις $\log_2 N$ qubits, μπορούμε να απεικονίσουμε ένα διάνυσμα μεγέθους N. Έτσι μας δίνεται η δυνατότητα να επεξεργαστούμε ένα μεγάλο διάστασης διάνυσμα πολύ πιο γρήγορα και αποτελεσματικά. [33],[34]

Η επιλογή του κατάλληλου feature mapping (ή αλλιώς του τρόπου με τον οποίο τα κλασικά δεδομένα μετασχηματίζονται σε κβαντικές καταστάσεις) έχει καθοριστική επίδραση στην απόδοση των QNN [66]. Συγκεκριμένα, διαφορετικές στρατηγικές ενσωμάτωσης οδηγούν σε ποικίλες εκφραστικότητες και αντοχές σε θόρυβο. Για παράδειγμα, ένας καλά σχεδιασμένος feature map μπορεί να διευκολύνει την εκμάθηση μη γραμμικών συσχετισμών στα δεδομένα, ενώ ένας υποβαθμισμένος μπορεί να περιορίσει σημαντικά την ικανότητα του μοντέλου να γενικεύει. Επομένως, το στάδιο της κωδικοποίησης δεν πρέπει να θεωρείται απλό προπαρασκευαστικό βήμα, αλλά κρίσιμη παράμετρος σχεδιασμού που επηρεάζει άμεσα την επιτυχία του κβαντικού μοντέλου. [64],[66]

2.4.4 Quantum Perceptron

Το Quantum Perceptron είναι το ανάλογο του κλασικού perceptron. Όπως γνωρίζουμε, σε ένα κλασικό νευρωνικό δίκτυο, το perceptron εκτελεί τον γραμμικό μετασχηματισμό

$$y = f(w \cdot x + b)$$

όπου f είναι μία μη γραμμική συνάρτηση ενεργοποίησης.

Αντίστοιχα στην κβαντική θεωρία, χρησιμοποιούμε μοναδιαίους μετασχηματισμούς οι οποίοι δρουν πάνω στην κατάσταση των qubits. Η μαθηματική απεικόνιση του quantum perceptron είναι η εξής [67]:

$$|\psi_{\text{out}}\rangle = U^{(l)}(\theta)|\psi_{\text{in}}\rangle$$

Όπου:

- $|\psi_{\text{in}}\rangle$ είναι η κβαντική κατάσταση εισόδου για το στρώμα l
- $U^{(l)}(\theta)$ είναι ο μοναδιαίος τελεστής που ορίζεται από την παράμετρο θ
- $|\psi_{\text{out}}\rangle$ η κατάσταση εξόδου

Η παράμετρος θ ρυθμίζεται κατά την εκπαίδευση, όπως ακριβώς τα βάρη σε ένα κλασικό perceptron [67].Ο τελεστής $U^{(l)}(\theta)$ συνήθως χρησιμοποιεί rotation gates (π.χ. R_x, R_y, R_z) και entangling gates όπως CNOT ή CZ [68]. Για παράδειγμα:

$$U^{(l)}(\theta) = \prod_j R_y(\theta_j) \prod_{(i,j)\in\varepsilon} \mathrm{CNOT}_{i,j}$$

όπου ε ορίζει το σύνολο των ζευγών qubits που διαπλέκονται (entangled) μέσω των αντίστοιχων πύλων. Με άλλα λόγια, τα qubits αυτά δεν εξελίσσονται πλέον ανεξάρτητα, αλλά οι καταστάσεις τους γίνονται αλληλοεξαρτώμενες, επιτρέποντας στο δίκτυο να εκφράζει πιο πολύπλοκες κβαντικές συσχετίσεις [69].

Η έξοδος του perceptron προκύπτει από τη μέτρηση ενός ή περισσότερων qubits ως προς έναν παρατηρήσιμο τελεστή O, συνήθως έναν τελεστή Pauli.

Η αναμενόμενη τιμή είναι το αποτέλεσμα του υπολογισμού:

$$y = \langle \psi_{\text{out}} | O | \psi_{\text{out}} \rangle$$

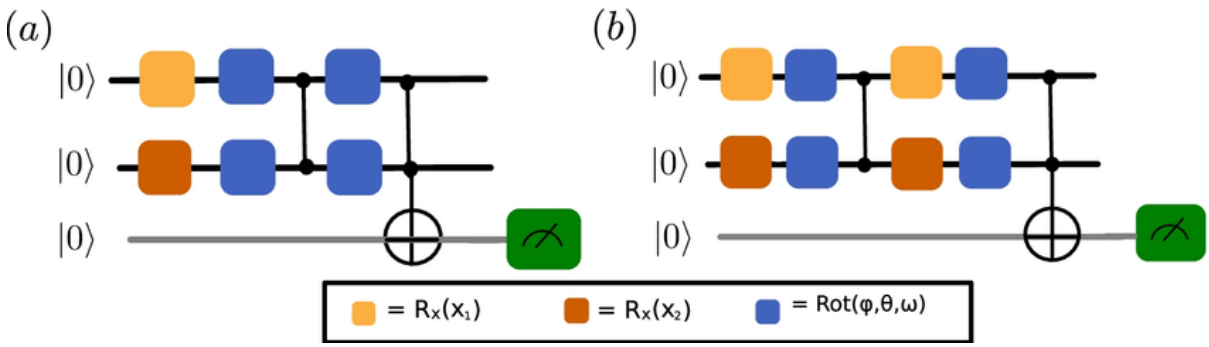
Το quantum perceptron μπορεί να θεωρηθεί η ελάχιστη "δομική μονάδα" των QNNs, με εκφραστική ισχύ που επεκτείνεται εκθετικά ως προς τον αριθμό των qubits [67].

Εξαιρετικά σημαντικό είναι το χαρακτηριστικό ότι *ένα quantum perceptron* μπορεί να λειτουργήσει ως καθολικός προσεγγιστής συναρτήσεων (universal approximator), δηλαδή να προσεγγίζει οποιαδήποτε συνεχή συνάρτηση μέσω κατάλληλης ρύθμισης των παραμέτρων του [70].

Μαθηματικά, για κάθε συνεχή συνάρτηση $(f \in C([0,1]^n)$ και κάθε $\epsilon > 0$, υπάρχει μοναδιαίος τελεστής $(U(\theta)$ τέτοιος ώστε:

$$|\langle 0|U(\theta)OU(\theta)|0\rangle - f(\mathrm{x})| < \epsilon$$

όπου O είναι ο παρατηρήσιμος τελεστής (π.χ. Pauli-Z).



Εικόνα 5 The quantum circuits that represent the quantum perceptron (QP) (a) and re-uploading quantum model (RU) (b) [59].

2.4.5 Μη γραμμικότητα στα κβαντικά δίκτυα

Στα κλασικά νευρωνικά δίκτυα, η μη-γραμμικότητα εισάγεται μέσω της συνάρτησης ενεργοποίησης

$$y = f(w \cdot x + b)$$

η οποία επιτρέπει την προσέγγιση πολύπλοκων σχέσεων εισόδου–εξόδου αξιοποιώντας τη μετατροπή ενός γραμμικού συνδυασμού $w \cdot x + b$ με μη − γραμμική συνάρτηση f.

Στα QNNs οι κύριοι μετασχηματισμοί είναι μοναδιαίοι (unitary) και ως εκ τούτου γραμμικοί, δηλαδή για δύο καταστάσεις $|\psi_1\rangle$ και $|\psi_2\rangle$ ισχύει [72]

$$U\,(\alpha|\psi_1\rangle + \beta|\psi_1\rangle.) = \alpha U|\psi_1\rangle + \beta U|\psi_2\rangle.$$

Ως εκ τούτου, οι καθαρές μοναδιαίες πράξεις δεν επαρκούν για την εισαγωγή μη-γραμμικότητας [73]. Η πράξη της μέτρησης φαίνεται να αποτελεί την πιο άμεση υλοποίηση μιας μη γραμμικής συνάρτησης ενεργοποίησης [74]. Αυτό ισχύει καθώς η μέτρηση δεν είναι unitary· είναι μια μη αναστρέψιμη πράξη που αναγκάζει την κατάσταση ενός κβαντικού συστήματος να καταρρεύσει σε μία από τις καταστάσεις βάσης σύμφωνα με τις πιθανότητες που έχουν προαναφερθεί [74].

Στην πράξη, εάν ένα qubit βρίσκεται σε υπέρθεση

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

η πιθανότητα μέτρησης του $|0\rangle$ είναι $P(0) = |\alpha|^2$ και της $|1\rangle$ είναι $P(1) = |b|^2$ [28-29]. Η έξοδος που εξάγεται εξαρτάται μη-γραμμικά από τους συντελεστές α,β και δεν προκύπτει ως απλός γραμμικός μετασχηματισμός της εισόδου. Επιπλέον, η μετάβαση από την κβαντική υπέρθεση σε κλασική τιμή μέσω μέτρησης διακόπτει την καθαρή μοναδιαία εξέλιξη — εισάγει μη-αναστρέψιμο στοιχείο — και έτσι λειτουργεί ως συνιστώσα τύπου συνάρτησης ενεργοποίησης, δίνοντας στο QNN την απαιτούμενη εκφραστική ικανότητα για την προσέγγιση μη-γραμμικών συναρτήσεων. [72-74]

Σημειώνεται περαιτέρω ότι η μη-γραμμικότητα εισάγεται ακόμη και μέσω μερικής μέτρησης — δηλαδή όταν δεν μετριούνται όλα τα qubits του συστήματος αλλά μόνο ένα υποσύνολο του, το οποίο επηρεάζει τους υπόλοιπους λόγω ενδεχόμενης συσχέτισης ή διαπλοκής. Οπότε η μη γραμμικότητα στο κβαντικό δίκτυο εισάγεται και μέσω της μέτρησης ορισμένων από τα qubits [75]. Η επιλογή ενός υποσυνόλου των qubits προς μέτρηση λειτουργεί ως μη-γραμμικός μηχανισμός διότι η κατάσταση των υπόλοιπων qubits μεταβάλλεται με τρόπο που δεν μπορεί να αποδοθεί απλώς ως γραμμικός συνδυασμός των αρχικών καταστάσεων.

2.4.6 Variational Quantum Circuits (VQCs).

Έχοντας τώρα αναλύσει την θεωρία του Quantum Perceptron, μπορούμε να γενικεύσουμε την μελέτη μας ορίζοντας τα λεγόμενα Variational Quantum Circuits (VQCs) τα οποία είναι το δομικά υλικά για την δημιουργία των Κβαντικών Νευρωνικών Δικτύων.

Τα VQCs είναι ουσιαστικά μεγάλα σε μέγεθος Quantum Perceptron. Είναι δηλαδή παραμετροποιημένα κβαντικά κυκλώματα των οποίων οι παράμετροι είναι οι γωνίες θ των πυλών περιστροφής $\boldsymbol{R_x}$, $\boldsymbol{R_y}$, $\boldsymbol{R_z}$. Στόχος κατά την εκπαίδευση είναι η εύρεση των κατάλληλων παραμέτρων θ προκειμένου να ελαχιστοποιηθεί το σφάλμα. [76]

Ένα VQC περιγράφεται από την σχέση:

$$|\boldsymbol{\psi}_{\text{out}}\,(\boldsymbol{x};\boldsymbol{\theta})\rangle = \boldsymbol{U}_{\text{var}}\,(\boldsymbol{\theta})\boldsymbol{U}_{\text{enc}}\,(\boldsymbol{x})|\boldsymbol{0}\rangle^{\otimes \boldsymbol{n}}$$

όπου:

- $\boldsymbol{U}_{\text{enc}}\,(\boldsymbol{x})$: Data Encoder

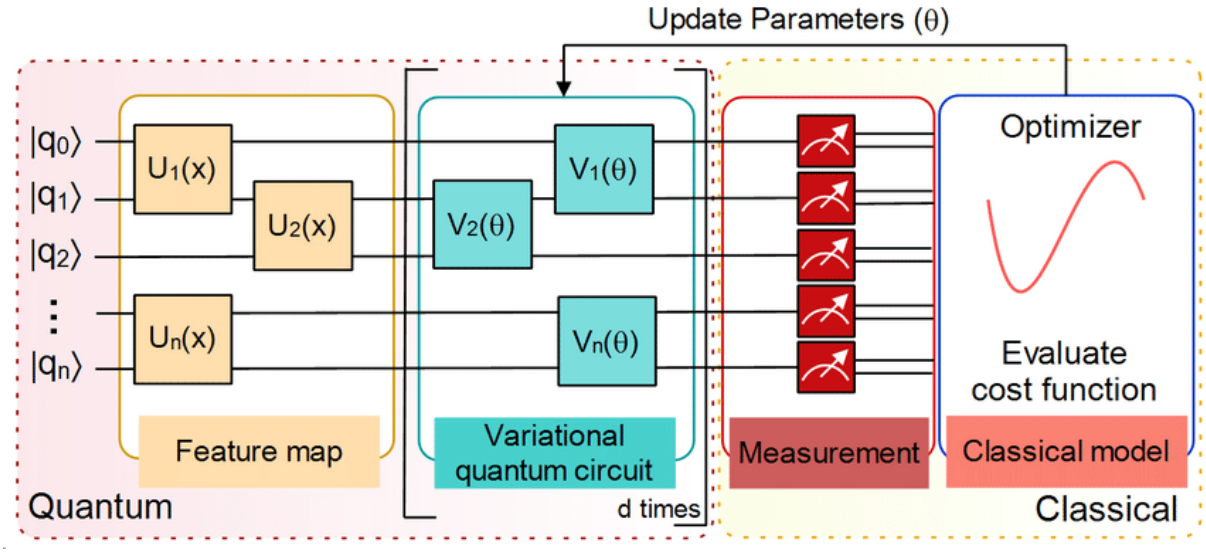
- $\boldsymbol{U}_{\text{var}}(\boldsymbol{\theta})$: Variational Circuit
- $|\boldsymbol{0}\rangle^{\otimes \boldsymbol{n}}$: Αρχική καθαρή κατάσταση των qubit

Επομένως, η έξοδος προκύπτει ως την μέτρηση με βάση ενός παρατηρήσιμου τελεστή *O:*

$$\boldsymbol{f}(\boldsymbol{x};\boldsymbol{\theta}) = \langle \boldsymbol{\psi}_{\text{out}}(\boldsymbol{x};\boldsymbol{\theta})|\boldsymbol{O}|\boldsymbol{\psi}_{\text{out}}(\boldsymbol{x};\boldsymbol{\theta})\rangle$$

Η εκμάθηση, όπως αναφέραμε και προηγουμένως, έχει ως στόχο να ελαχιστοποιήσει την συνάρτηση [76-77].

$$\boldsymbol{C}(\boldsymbol{\theta}) = \sum_{\boldsymbol{i}} (\boldsymbol{f}(\boldsymbol{x_i};\boldsymbol{\theta}) - \boldsymbol{y_i})^2$$



Εικόνα 6 Στο κβαντικό τμήμα, τα δεδομένα κωδικοποιούνται μέσω του Feature Map U(x) και επεξεργάζονται από το παραμετρικό κύκλωμα V(θ). [78]

2.4.7 Αρχιτεκτονική και δομή των VQCs

Τώρα θα κάνουμε μια βαθύτερη ανάλυση στο $\boldsymbol{U}_{\text{var}}(\boldsymbol{\theta})$, δηλαδή στο παραμετροποιήσιμο μέρος του VQC δίχως να μας νοιάζει το πρώτο στάδιο το οποίο είναι το data encoding.
Συχνά, η δομή του μπορεί να αναλυθεί σε επαναλαμβανόμενα layers/blocks από τα εξής βασικά κομμάτια [76-77]:

1. Rotation gates $\boldsymbol{R_x(\theta_i)}$, $\boldsymbol{R_y(\theta_i)}$, $\boldsymbol{R_z(\theta_i)}$, οι οποίες καθορίζουν τη γεωμετρία του χώρου Hilbert και περιέχουν τις παραμέτρους προς εκπαίδευση.

2. Entangling gates, όπως οι CNOT ή CZ, που είναι υπεύθυνες για το entanglement των qubits.

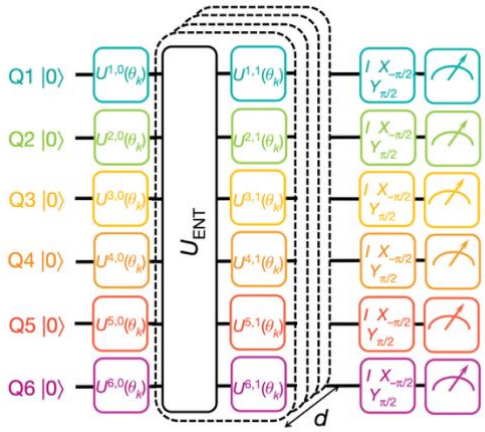
Στην γενική της μαθηματική μορφή

$$\boldsymbol{U}_{\mathbf{var}}(\boldsymbol{\theta}) = \prod_{\boldsymbol{l}=\mathbf{1}}^{\boldsymbol{L}} (\boldsymbol{U}_{\mathbf{ent}}^{(\boldsymbol{l})} \boldsymbol{U}_{\mathbf{rot}}^{(\boldsymbol{l})}(\boldsymbol{\theta}^{(\boldsymbol{l})}))$$

όπου

- $\boldsymbol{U}_{\mathbf{rot}}^{(\boldsymbol{l})}$ περιλαμβάνει τις παραμετροποιημένες περιστροφές.
- $\boldsymbol{U}_{\mathbf{ent}}^{(\boldsymbol{l})}$το σταθερό entangling στάδιο.

Η αρχιτεκτονική αυτή, γνωστή ως hardware-efficient ansatz, έχει υιοθετηθεί ευρέως λόγω της απλότητας και της συμβατότητάς της με τα φυσικά χαρακτηριστικά των υπαρχουσών NISQ συσκευών [78].



Εικόνα 7 Εδώ φαίνεται μια ενδεικτική αρχιτεκτονική του Variational Quantum Circuit όπου υπάρχει και επανάληψη των layers Uent , U(θ) [79]

Ωστόσο, η εκφραστικότητά της μπορεί να ενισχυθεί περαιτέρω μέσω της τεχνικής data-re-uploading, η οποία συνίσταται στην επαναλαμβανόμενη εισαγωγή των κλασικών δεδομένων σε διαδοχικά στρώματα του κυκλώματος [80]. Η πρακτική αυτή επιτρέπει στο κύκλωμα να προσεγγίζει πιο πολύπλοκες μη-γραμμικές συναρτήσεις, αυξάνοντας τη μαθησιακή του ικανότητα χωρίς να απαιτείται η αύξηση του βάθους του [79],[81].
Με τον τρόπο αυτό, τα VQCs αποκτούν εκφραστικότητα αντίστοιχη βαθιών κλασικών νευρωνικών δικτύων, αξιοποιώντας πλήρως τη δομή των παραμετρικών πυλών και τη συσχέτισή τους με τα δεδομένα εισόδου.

2.4.8 Εκπαίδευση και Βελτιστοποίηση

Τώρα έχοντας ορίσει την δομή και την αρχιτεκτονική των Κβαντικών Νευρωνικών Δικτύων ήρθε η ώρα να δούμε την μέθοδο με την οποία θα τα εκπαιδεύσουμε. Με τον όρο εκπαίδευση αναφερόμαστε στην εύρεση του συνόλου των γωνιών $\boldsymbol{\theta}$ (των πυλών περιστροφής) έτσι ώστε να ελαχιστοποιείται η συνάρτηση κόστους $\boldsymbol{C}(\boldsymbol{\theta})$. [77]

Η έξοδος του κυκλώματος, όπως έχουμε ήδη εξηγήσει, ορίζεται ως [76-77]:

$$\boldsymbol{f(x_i;\theta)} \;=\; \boldsymbol{\langle \psi_{out}(x_i;\theta)|O|\psi_{out}(x_i;\theta)\rangle}$$

όπου

- $\boldsymbol{x_i}$: το διάνυσμα το οποίο περιέχει τα αρχικά δεδομένα.
- θ: οι παραμετροποιήσιμες γωνίες των περιστροφικών πυλών (το "βάρος" του δικτύου),
- O: ο τελεστής μέτρησης (συνήθως Z ή συνδυασμός Pauli τελεστών),
- $|\boldsymbol{\psi}_{\text{out}}(\boldsymbol{x_i}\,;\,\boldsymbol{\theta})\rangle$: η κατάσταση εξόδου του κυκλώματος μετά την εφαρμογή του $\boldsymbol{U_{var}}\ (\theta)$.

Ορίζουμε λοιπόν τώρα την συνάρτηση κόστους με βάση το MSE (Mean Squared Error) όπου ισχύει: [82]

$$\boldsymbol{C(\theta)} = \frac{\boldsymbol{1}}{\boldsymbol{N}}\sum_{\boldsymbol{i=1}}^{\boldsymbol{N}}\boldsymbol{(f(x_i;\theta)-y_i\,)^2}$$

όπου:

- N: αριθμός δειγμάτων,
- $\boldsymbol{y_i}$: επιθυμητή (κλασική) τιμή εξόδου.

Αντίστοιχα, αν χρησιμοποιήσουμε το Binary Cross-Entropy Loss για binary classification έχουμε ότι: [82]

$$\boldsymbol{C(\theta)} = -\frac{\boldsymbol{1}}{\boldsymbol{N}}\sum_{\boldsymbol{i=1}}^{\boldsymbol{N}}[\,\boldsymbol{y_i}\,*\mathbf{log}\;\boldsymbol{p(y=1\mid x_i)}+\boldsymbol{(1-y_i)}*\mathbf{log}\boldsymbol{(1-p(\,y=1\mid x_i\,)}\;)\,]$$

Το $\boldsymbol{p(y=1\mid x_i)}$ εκφράζει την πιθανότητα που υπολογίζει το μοντέλο ότι το δείγμα $\boldsymbol{x_i}$ ανήκει στη θετική κατηγορία, δηλαδή ότι το γεγονός y=1 (π.χ. "απάτη") είναι αληθές.

Στην πράξη, αυτή η τιμή προκύπτει από τη συνάρτηση sigmoid στο τελευταίο επίπεδο του δικτύου και παίρνει τιμές μεταξύ 0 και 1, αντιπροσωπεύοντας το "πόσο σίγουρο" είναι το μοντέλο για την πρόβλεψή του. [82]

Στόχος της εκπαίδευσης είναι η ελαχιστοποίηση αυτής της ποσότητας:

$$\boldsymbol{\theta^*} = \mathbf{arg}\,\boldsymbol{min}\;\boldsymbol{C(\theta)}$$

Τώρα, εφόσον έχουμε ορίσει τη συνάρτηση κόστους, είναι η ώρα να ξεκινήσει η εκπαίδευση, δηλαδή η βελτιστοποίηση. Προκειμένου να ελαχιστοποιηθεί η συνάρτηση κόστους, πρέπει να υπολογιστούν τα gradients της παραμέτρου θ. [77]

Τα gradients μπορούν να υπολογιστούν αναλυτικά μέσω του κανόνα μετατόπισης παραμέτρου (parameter-shift rule), ο οποίος βασίζεται στη δομή των γεννητόρων των πυλών.[83]

Σύμφωνα με τον κανόνα αυτό, ισχύει ότι:

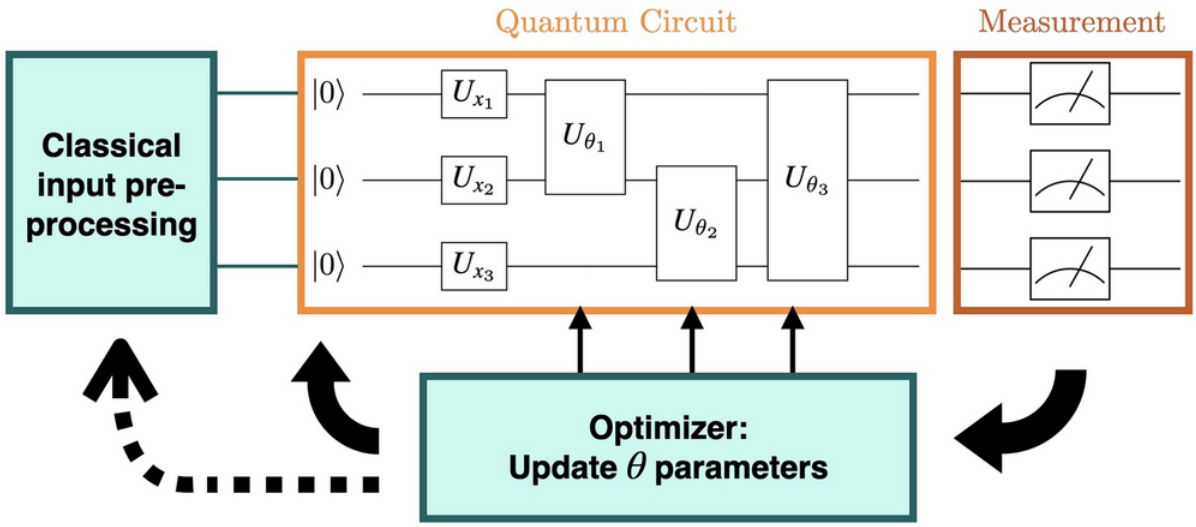
$$\frac{\partial f(\theta)}{\partial \theta_i} = \frac{f(\theta_i + \frac{\pi}{2}) - f(\theta_i - \frac{\pi}{2})}{2}$$

Με βάση την παραπάνω εξίσωση, ο υπολογισμός της κλίσης (gradient) απαιτεί δύο ξεχωριστές εκτελέσεις (evaluations) του κβαντικού κυκλώματος για κάθε παράμετρο — μία με τη μετατόπιση $+\frac{\pi}{2}$ και μία με τη μετατόπιση $-\frac{\pi}{2}$.

Η διαφορά των αποτελεσμάτων αυτών δίνει την τιμή της μερικής παραγώγου για τη συγκεκριμένη παράμετρο. Επομένως, για ένα κύκλωμα με n παραμέτρους, χρειάζονται συνολικά $2n$ εκτελέσεις για τον πλήρη υπολογισμό όλων των gradients. [83]

Στη συνέχεια, οι τιμές αυτές χρησιμοποιούνται σε κλασικούς αλγορίθμους βελτιστοποίησης όπως το Gradient Descent ή ο ADAM, οι οποίοι ενημερώνουν τις παραμέτρους του κυκλώματος με τρόπο παρόμοιο με τα κλασικά νευρωνικά δίκτυα. Το αποτέλεσμα είναι ένα υβριδικό σύστημα εκπαίδευσης (Hybrid Training Loop), όπου το κβαντικό κύκλωμα παρέχει τις τιμές του κόστους και των παραγώγων, ενώ ο κλασικός βελτιστοποιητής ρυθμίζει τις παραμέτρους έως τη σύγκλιση του μοντέλου. [81-82]

Τώρα λοιπόν έχοντας ορίσει ολόκληρο το κβαντικό κύκλωμα καθώς και το σφάλμα το οποίο θέλουμε να ελαχιστοποιήσουμε, μπορούμε να ξεκινήσουμε τη διαδικασία εκπαίδευσης.



Εικόνα 8 Η διαδικασία εκμάθησης ενός Κβαντικού Νευρωνικού Δικτύου[73]

Οπότε, η διαδικασία της εκμάθησης έχει ως εξής.

1. Αρχικοποίηση.
   Ορίζουμε ως γωνίες θ τυχαίες τιμές για να ξεκινήσει η εκπαίδευση.

2. Data encoding.
   Το διάνυσμα x_i μετατρέπεται σε κβαντικό μεσω των μεθόδων encoding.

3. Υπολογισμός και μέτρηση.
   Το παραμετροποιημένο κύκλωμα εφαρμόζεται στην αρχική κβαντική κατάσταση και εμείς μετράμε την έξοδο.

4. Υπολογισμός κόστους.
   Σύμφωνα με τις τιμές των εξόδων, υπολογίζουμε το κόστος ανάλογα με το πρόβλημα (MSE, Cross-Entropy)

5. Ενημέρωση παραμέτρων.
   Υπολογίζουμε gradient (π.χ. με parameter-shift) και ενημερώνουμε θ μέσω κλασικού βελτιστοποιητή (classical optimizer) όπως ο gradient descent ή Adam.

Παρά την αποτελεσματικότητα του κανόνα μετατόπισης παραμέτρου, η εκπαίδευση των παραμετρικών κβαντικών κυκλωμάτων (VQCs) συχνά αντιμετωπίζει ένα σοβαρό πρόβλημα γνωστό ως φαινόμενο των barren plateaus [86]. Το φαινόμενο αυτό περιγράφει περιοχές του χώρου παραμέτρων όπου τα gradients της συνάρτησης κόστους τείνουν να μηδενίζονται, καθιστώντας εξαιρετικά δύσκολη ή και αδύνατη την εκπαίδευση του μοντέλου. Η αιτία σχετίζεται με το γεγονός ότι, όσο αυξάνεται το βάθος του κυκλώματος ή ο αριθμός των qubits, η αναμενόμενη διακύμανση των παραγώγων μειώνεται εκθετικά με το μέγεθος του συστήματος, σύμφωνα με τη σχέση:

$$Var\left[\frac{\partial f(\theta)}{\partial \theta_{\mathrm{i}}}\right] \propto e^{-n}$$

όπου n είναι ο αριθμός των qubits [86]. Αυτό σημαίνει ότι σε βαθιά ή τυχαία αρχικοποιημένα κυκλώματα, τα gradients γίνονται πρακτικά μηδενικά, οδηγώντας σε vanishing gradient problem παρόμοιο με αυτό των κλασικών νευρωνικών δικτύων, αλλά πολύ πιο έντονο. Ως συνέπεια, η εκπαίδευση των VQCs γίνεται ασταθής και απαιτεί ειδικές στρατηγικές όπως ρηχά κυκλώματα, καθοδηγούμενη αρχικοποίηση (layerwise training) ή ελεγχόμενο entanglement για την αποφυγή των barren plateaus [86].

2.4.9 Παράδειγμα στην Προγραμματιστική γλώσσα PennyLane

Στο επόμενο σημείο παρουσιάζεται ένα ενδεικτικό παράδειγμα εκπαίδευσης ενός παραμετρικού κβαντικού κυκλώματος (VQC) χρησιμοποιώντας τη βιβλιοθήκη **PennyLane [87]** . Μέσω του παραδείγματος αυτού αναδεικνύεται στην πράξη ο τρόπος με τον οποίο εφαρμόζεται ο κανόνας μετατόπισης παραμέτρου για τον υπολογισμό των παραγώγων και η διαδικασία ενημέρωσης των παραμέτρων του κυκλώματος κατά τη διάρκεια της εκπαίδευσης.

```
import pennylane as qml
from pennylane import numpy as np

dev = qml.device("default.qubit", wires=1)

@qml.qnode(dev)
def circuit(theta):
    qml.RY(theta, wires=0)
    return qml.expval(qml.PauliZ(0))

def cost(theta):
    return (circuit(theta) - 0)**2

def parameter_shift_grad(theta):
```

```
    shift = np.pi / 2
    forward = cost(theta + shift)
    backward = cost(theta - shift)
    grad = 0.5 * (forward - backward)
    return grad

theta = np.array(0.3)

lr = 0.2
for step in range(10):
    grad = parameter_shift_grad(theta)
    theta = theta - lr * grad
    print(f"Βήμα {step+1:2d} | Gradient = {grad:+.6f} | Θέση θ = {theta:.6f} | Κόστος = {cost(theta):.6f}")
```

2.5 Ομοσπονδιακή Μάθηση (Federated Learning)

2.5.1 Εισαγωγή και Βασικές Αρχές

Η Ομοσπονδιακή Μάθηση (Federated Learning – FL) αποτελεί ένα αποκεντρωμένο παράδειγμα μηχανικής μάθησης, όπου η εκπαίδευση ενός κοινού μοντέλου πραγματοποιείται από πολλαπλούς πελάτες (clients), χωρίς τα δεδομένα τους να εγκαταλείπουν την τοπική τους συσκευή ή υποδομή [88]. Η θεμελιώδης ιδέα εισήχθη από τους McMahan et al. (2017) [89] ως μια μέθοδος που επιτρέπει την εκπαίδευση μοντέλων με διατήρηση της ιδιωτικότητας και μείωση του επικοινωνιακού κόστους, αξιοποιώντας αποκεντρωμένους υπολογιστικούς πόρους. Αντί να συγκεντρώνονται τα δεδομένα σε έναν κεντρικό εξυπηρετητή (όπως στα κλασικά σχήματα), κάθε οργανισμός εκπαιδεύει ένα τοπικό μοντέλο χρησιμοποιώντας τα δικά του δεδομένα και στη συνέχεια αποστέλλει μόνο τα ενημερωμένα βάρη ή βαθμίδες (gradients) στον συντονιστή [90].
Η προσέγγιση αυτή καθιστά το FL ιδανικό για περιβάλλοντα με αυστηρές απαιτήσεις ιδιωτικότητας, όπως τα τραπεζικά ή ιατρικά δεδομένα [91]. Για παράδειγμα, σε ένα δίκτυο τραπεζών, κάθε ίδρυμα μπορεί να εκπαιδεύει το δικό του μοντέλο ανίχνευσης απάτης, συμβάλλοντας στην κοινή βελτίωση του παγκόσμιου μοντέλου χωρίς να κοινοποιεί προσωπικά δεδομένα πελατών [92].

2.5.2 Μαθηματική Διατύπωση του Προβλήματος

Το πρόβλημα της ομοσπονδιακής μάθησης μπορεί να θεωρηθεί ως κατανεμημένο πρόβλημα βελτιστοποίησης [93]. Θεωρούμε ότι υπάρχουν K κόμβοι (clients), ο καθένας με τοπικό σύνολο δεδομένων D_k. Στόχος είναι η ελαχιστοποίηση της συνολικής συνάρτησης κόστους:

$$\min_{w} F(w) = \sum_{k=1}^{K} p_k F_k(w)$$

όπου:

- w είναι το διάνυσμα των παραμέτρων του μοντέλου,
- K ο αριθμός των συμμετεχόντων κόμβων,
- $p_k = \frac{n_k}{n}$ το ποσοστό συμμετοχής του κόμβου k (με $n = \sum_k n_k$),
- $F_k(w) = \frac{1}{n_k} \sum_{i \in D_k} \ell_i(w)$ η τοπική συνάρτηση κόστους του κόμβου k,
- και $\ell_i(w)$ η συνάρτηση απώλειας (loss function) για κάθε δείγμα i [94].

Η βελτιστοποίηση αυτή επιδιώκει να ελαχιστοποιήσει το συνολικό σφάλμα του παγκόσμιου μοντέλου, χρησιμοποιώντας τοπικές ενημερώσεις που παράγονται ανεξάρτητα στους clients [95]. Η μη κεντρικοποιημένη φύση του προβλήματος εισάγει προκλήσεις όπως:

- ετερογένεια δεδομένων (non-IID distributions),
- μερική συμμετοχή κόμβων (partial participation),
- και περιορισμένο εύρος επικοινωνίας (communication bottlenecks) [96].

2.5.3 Αρχιτεκτονικά Μοντέλα και Επικοινωνιακές Δομές

Η διαδικασία της ομοσπονδιακής εκπαίδευσης μπορεί να ακολουθήσει δύο βασικά αρχιτεκτονικά μοντέλα [97]:

2.5.3.1 Κεντρικοποιημένο (Server-Based) Federated Learning

Στην πιο διαδεδομένη εκδοχή, ένας κεντρικός εξυπηρετητής (aggregator ή orchestrator) συντονίζει τη διαδικασία εκπαίδευσης [98].
Η λειτουργία ακολουθεί τα εξής βήματα:

1. Ο εξυπηρετητής αρχικοποιεί το παγκόσμιο μοντέλο w_0.
2. Σε κάθε γύρο t, επιλέγει ένα υποσύνολο πελατών $S_t \subseteq \{1, \dots, K\}$.
3. Κάθε επιλεγμένος πελάτης εκπαιδεύει το μοντέλο στα τοπικά του δεδομένα και παράγει ενημερωμένα βάρη w_k^{t+1}.
4. Ο εξυπηρετητής συλλέγει τις ενημερώσεις και υπολογίζει το νέο παγκόσμιο μοντέλο μέσω συνάθροισης:
$$w^{t+1} = \sum_{k \in S_t} p_k w_k^{t+1}$$
5. Το ενημερωμένο μοντέλο επαναδιανέμεται στους clients και η διαδικασία επαναλαμβάνεται [99].

Αν και το μοντέλο αυτό είναι εύκολο να υλοποιηθεί και προσφέρει σταθερή σύγκλιση, δημιουργεί ένα μοναδικό σημείο αποτυχίας (single point of failure) [100] και απαιτεί εμπιστοσύνη στον aggregator πρόβλημα που η παρούσα εργασία επιλύει μέσω της ενσωμάτωσης blockchain μηχανισμών επικύρωσης [101].

2.5.3.2 Πλήρως Αποκεντρωμένο (Peer-to-Peer) Federated Learning

Σε πλήρως αποκεντρωμένα σχήματα, δεν υπάρχει κεντρικός συντονιστής. Οι κόμβοι επικοινωνούν άμεσα μεταξύ τους, ανταλλάσσοντας τοπικές ενημερώσεις βάσει προκαθορισμένου δικτύου (topology) [102].
Το πρόβλημα μπορεί να διατυπωθεί ως εξής:

$$\min_{w_1,\dots,w_K} \sum_{k=1}^{K} F_k(w_k)$$

υπό τον περιορισμό:

$$w_k = w_j, \forall (k,j) \in E$$

όπου E το σύνολο των ζευγών κόμβων που επικοινωνούν μεταξύ τους. [103].
Η συνθήκη αυτή επιβάλλει συναίνεση (consensus), ώστε όλοι οι κόμβοι να συγκλίνουν σε κοινό μοντέλο w^*.

Παρά το αυξημένο επικοινωνιακό κόστος, τα αποκεντρωμένα σχήματα παρέχουν μεγαλύτερη ανθεκτικότητα και αυξημένη ιδιωτικότητα. [104].

2.5.4 Στρατηγικές Συνάθροισης (Aggregation Strategies)

Η διαδικασία συνάθροισης (aggregation) καθορίζει τον τρόπο με τον οποίο οι τοπικές ενημερώσεις συγχωνεύονται στο παγκόσμιο μοντέλο. Η επιλογή στρατηγικής επηρεάζει την ταχύτητα σύγκλισης, την ανοχή σε ακραίες τιμές (outliers) και τη σταθερότητα του συστήματος [105].

2.5.4.1 Federated Averaging (FedAvg)

Ο κλασικός αλγόριθμος FedAvg (McMahan et al., 2017) υπολογίζει το νέο μοντέλο ως:

$$w^{t+1} = \sum_{k \in S_t} \frac{n_k}{n} w_k^{t+1}$$

Η συνεισφορά κάθε κόμβου εξαρτάται από το μέγεθος του τοπικού του dataset [106]. Αν και ο FedAvg είναι αποδοτικός, παρουσιάζει προβλήματα στα non-IID περιβάλλοντα, όπου οι κατανομές δεδομένων διαφέρουν σημαντικά [107].

2.5.4.2 Federated Proximal (FedProx)

Ο FedProx (Li et al., 2020) εισάγει έναν proximal όρο στη συνάρτηση κόστους κάθε κόμβου:

$$F_k(w) = f_k(w) + \frac{\mu}{2} \| w - w_t \|^2$$

όπου μ είναι παράμετρος σταθεροποίησης.
Ο όρος αυτός μειώνει τις αποκλίσεις μεταξύ τοπικών μοντέλων, βελτιώνοντας τη σύγκλιση σε non-IID συνθήκες [108].

2.5.4.3 Federated Optimization (FedOpt Family)

Η γενική μορφή δίνεται ως:

$$w_{t+1} = w_t - \eta \cdot \psi_t(\Delta_t)$$

όπου:

- ψ_t είναι η συνάρτηση ενημέρωσης (π.χ. Adam, Yogi, Adagrad),
- η ο ρυθμός μάθησης του server.
- $\psi_t(\Delta_t)$ είναι η συνάρτηση ενημέρωσης (update function), η οποία εξαρτάται από τον αλγόριθμο βελτιστοποίησης,
- Δ_t είναι η διαφορά (gradient) μεταξύ των τοπικών και του παγκόσμιου μοντέλου [109].

  Η μορφή αυτή ενοποιεί διαφορετικούς τύπους προσαρμοστικών αλγορίθμων, όπως Adam, Yogi και Adagrad, οι οποίοι ρυθμίζουν δυναμικά τον ρυθμό μάθησης με βάση το ιστορικό των gradients [110].

Οι εκδόσεις περιλαμβάνουν:

(α) FedAdam

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t$$

$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) g_t^2$$

$$w_{t+1} = w_t - \eta \frac{m_t}{\sqrt{v_t} + \epsilon}$$

όπου:

- m_t και v_t είναι οι εκθετικά κινούμενοι μέσοι όροι της πρώτης (μέσης τιμής) και της δεύτερης ροπής (διακύμανσης) των βαθμίδων (*gradients*), αντίστοιχα.
  (Δηλαδή: $m_t = \beta_1 \cdot m_{t-1} + (1 - \beta_1) \cdot g_t$ και $v_t = \beta_2 \cdot v_{t-1} + (1 - \beta_2) \cdot g_t^2$),
- β_1, β_2 είναι συντελεστές εξομάλυνσης (συνήθως 0.9 και 0.999 αντίστοιχα),
- ϵ μικρός σταθερός όρος για αριθμητική σταθερότητα.

Η FedAdam εξισορροπεί ταχύτητα και σταθερότητα, επιτυγχάνοντας καλύτερη προσαρμογή σε μη στατικά δεδομένα και ανομοιογενείς κατανομές (non-IID) [111].

(β) FedYogi

Ο FedYogi προτείνει μια πιο συντηρητική ενημέρωση του τετραγωνικού όρου, μειώνοντας την υπερπροσαρμογή σε περιβάλλοντα με έντονες διακυμάνσεις των gradients:

$$v_t = v_{t-1} - (1 - \beta_2) g_t^2 \operatorname{sign}(v_{t-1} - g_t^2)$$

Η βασική διαφορά από τον FedAdam είναι ότι το FedYogi ελέγχει την αύξηση του v_t, διατηρώντας πιο σταθερό ρυθμό μάθησης. Έτσι, αποφεύγονται μεγάλες ταλαντώσεις κατά τη διάρκεια της σύγκλισης [112].

(γ) FedAdagrad

$$v_t = v_{t-1} + \Delta_t^2$$

$$w_{t+1} = w_t - \eta * \left(\frac{\Delta_t}{\left(\sqrt{v_t} + \epsilon\right)} \right)$$

Ενσωματώνει προσαρμοστικές τιμές learning rate μέσω σωρευτικού τετραγωνικού αθροίσματος των gradients [113].Με αυτόν τον τρόπο, οι παράμετροι με συχνά μεγάλους gradients επιβραδύνονται, ενώ εκείνες με μικρότερες τιμές μαθαίνουν γρηγορότερα.
Η FedAdagrad αποδεικνύεται αποτελεσματική σε σενάρια όπου οι τοπικοί κόμβοι έχουν ανισόρροπα ή σπάνια χαρακτηριστικά [114].

2.5.4.4 Federated Normalization and Gradient Correction (FedNova)

Ο FedNova αντιμετωπίζει την ανομοιομορφία των τοπικών epochs (δηλαδή τον διαφορετικό αριθμό τοπικών επαναλήψεων εκπαίδευσης που εκτελεί κάθε client πριν τη συνάθροιση), κανονικοποιώντας τις ενημερώσεις ως εξής:

$$w^{t+1} = w^t - \eta \sum_k \frac{n_k}{n} \frac{\Delta w_k}{\tau_k}$$

όπου τ_k ο αριθμός τοπικών βημάτων εκπαίδευσης [115].

2.5.4.5 Federated Matching and Layer-Wise Aggregation (FedMA)

Ο FedMA ταιριάζει (matches) νευρώνες μεταξύ των τοπικών μοντέλων με clustering, εκτελώντας layer-wise aggregation αντί απλής μέσης τιμής, ιδανικό για ετερογενείς αρχιτεκτονικές [116].

2.5.4.6 Robust Aggregation Methods (Median & Trimmed Mean)

Για περιβάλλοντα με κακόβουλους πελάτες ή outliers, εφαρμόζονται πιο ανθεκτικές μέθοδοι [117]:

Coordinate-wise Median:

$$w_j^{t+1} = \text{median}(w_{1j}^{t+1}, \dots, w_{Kj}^{t+1})$$

Trimmed Mean:

$$w_j^{t+1} = \frac{1}{K - 2b} \sum_{k=b+1}^{K-b} w_{kj}^{t+1}$$

όπου b το πλήθος τιμών που αποκόπτονται (trimming) [118].

2.5.4.7 Federated Dynamic Weighting (FedDyn)

Ο FedDyn (Acar et al., 2021) συνδυάζει προσαρμοστική στάθμιση και δυναμική σταθεροποίηση:

$$w^{t+1} = w^t - \eta \sum_k p_k (\nabla F_k(w^t) + \lambda (w^t - w_k^{t+1}))$$

Επιτυγχάνει ταχύτερη σύγκλιση και βελτιωμένη σταθερότητα σε μη ομοιογενή περιβάλλοντα [119].

2.5.5 Προκλήσεις και Περιορισμοί της Ομοσπονδιακής Μάθησης

Παρά τα πλεονεκτήματά της, η Ομοσπονδιακή Μάθηση αντιμετωπίζει σημαντικές προκλήσεις [120]:

- Ασυνεπείς Κατανομές (non-IID): Τα τοπικά δεδομένα διαφέρουν σε ποιότητα και στατιστική κατανομή.
- Κακόβουλοι Συμμετέχοντες: Οι κόμβοι μπορεί να υποβάλουν αλλοιωμένες ενημερώσεις (model poisoning) [121].
- Απουσία Εμπιστοσύνης: Δεν υπάρχει μηχανισμός επαλήθευσης για το αν οι ενημερώσεις είναι έγκυρες.
- Κόστος Επικοινωνίας: Οι επαναλαμβανόμενες μεταφορές μοντέλων επιβαρύνουν το δίκτυο [122].

- Αυτοί οι περιορισμοί καθιστούν απαραίτητη την ενσωμάτωση μηχανισμών εμπιστοσύνης και ασφάλειας, όπως το Blockchain και η Κβαντική Κρυπτογραφία, που εξετάζονται στα επόμενα κεφάλαια [123].

2.5.6 Σύνδεση με το Προτεινόμενο Σύστημα

Στην παρούσα εργασία, η Ομοσπονδιακή Μάθηση χρησιμοποιείται ως θεμελιώδης μηχανισμός αποκεντρωμένης εκπαίδευσης για την ανίχνευση χρηματοοικονομικής απάτης [124]. Η προτεινόμενη αρχιτεκτονική Q-FedSecure επεκτείνει το κλασικό σχήμα FL με:

- Blockchain Validation Layer, που αποθηκεύει και επαληθεύει κρυπτογραφημένες ενημερώσεις [125],
- Homomorphic Encryption και Qhash για προστασία ιδιωτικότητας [126],
- και Quantum Layers που βελτιώνουν την ακρίβεια του μοντέλου μέσω κβαντικής εκφραστικότητας [127].

Έτσι, επιτυγχάνεται ένα ασφαλές, συνεργατικό και κβαντικά ενισχυμένο πλαίσιο μάθησης, ικανό να αντιμετωπίσει τις προκλήσεις των σύγχρονων τραπεζικών συστημάτων [128].

2.6 Τεχνολογία Blockchain

2.6.1 Εισαγωγή

Η τεχνολογία Blockchain αποτελεί μία αποκεντρωμένη και κατανεμημένη αρχιτεκτονική καταγραφής δεδομένων, η οποία εισάγει νέες αρχές διαφάνειας, ακεραιότητας και αξιοπιστίας στις ψηφιακές συναλλαγές [129]. Εμφανίστηκε για πρώτη φορά το 2008, μέσω της δημοσίευσης του Satoshi Nakamoto “Bitcoin: A Peer-to-Peer Electronic Cash System”, ως ο μηχανισμός που επέτρεψε την ασφαλή ανταλλαγή ψηφιακού νομίσματος χωρίς την ανάγκη ενδιάμεσου φορέα [130]. Η βασική της συνεισφορά έγκειται στη δυνατότητα καταγραφής γεγονότων (transactions) σε ένα δημόσιο ή ιδιωτικό καθολικό (ledger) το οποίο είναι αμετάβλητο, ανιχνεύσιμο και επαληθεύσιμο από όλα τα συμμετέχοντα μέρη [131]. Η αλυσίδα των blocks δημιουργεί μία χρονολογική αλληλουχία γεγονότων, διασφαλίζοντας ότι καμία εγγραφή δεν μπορεί να αλλοιωθεί εκ των υστέρων χωρίς συλλογική συναίνεση [132].

2.6.2 Δομή και Οργάνωση του Blockchain

Ένα blockchain αποτελείται από μια ακολουθία blocks, όπου κάθε block περιέχει ένα σύνολο από επικυρωμένες συναλλαγές, καθώς και μία κρυπτογραφική αναφορά στο προηγούμενο block, σχηματίζοντας έτσι μια αλυσίδα ακεραιότητας [133].

Η γενική δομή ενός block περιλαμβάνει τα εξής πεδία:

- Block Header: περιέχει μεταδεδομένα όπως το hash του προηγούμενου block, το χρονικό σήμα (timestamp) και τη ρίζα Merkle (Merkle root) των συναλλαγών [134].

- Transaction List: περιέχει όλες τις συναλλαγές που έχουν επικυρωθεί και αποθηκευτεί σε αυτό το block.

- Nonce: αριθμητική τιμή που χρησιμοποιείται στον μηχανισμό απόδειξης εργασίας (Proof of Work).

Η συνδεσιμότητα των blocks εξασφαλίζεται μέσω του κατακερματισμού (hashing) [135].

Αν έστω κάθε block περιέχει το hash του προηγούμενου block, τότε κάθε μεταβολή σε οποιοδήποτε block μεταβάλλει όλους τους επόμενους δείκτες, καθιστώντας την αλλοίωση πρακτικά αδύνατη χωρίς τον επανυπολογισμό ολόκληρης της αλυσίδας.

Ο συμβολισμός για την αλληλουχία των blocks παρουσιάζεται παρακάτω:

$$B_1 \rightarrow B_2 \rightarrow \cdots \rightarrow B_n$$

όπου κάθε block B_i περιλαμβάνει τα βασικά δομικά του στοιχεία, όπως το block header, τις συναλλαγές (transactions) και το nonce:

$$B_i = \{\text{Header}_i, \text{Transactions}_i, \text{Hash}(B_{i-1})\}$$

και ορίζεται η σχέση ακεραιότητας:

$$\text{Hash}(B_i) = H(\text{Header}_i \,||\, \text{Transactions}_i \,||\, \text{Hash}(B_{i-1}))$$

Η ιδιότητα αυτή καθιστά το blockchain immutable ledger, δηλαδή ένα καθολικό μη μεταβλητό μητρώο [136].

2.6.3 Κρυπτογραφικές Θεμελιώσεις

Η ασφάλεια του blockchain βασίζεται σε θεμελιώδεις αρχές κρυπτογραφίας, όπως η ασύμμετρη κρυπτογράφηση και οι συναρτήσεις κατακερματισμού (hash functions) [137].

2.6.3.1 Συναρτήσεις Κατακερματισμού (Hash Functions)

Οι hash functions είναι μονοκατευθυντικές συναρτήσεις που μετατρέπουν ένα μήνυμα αυθαίρετου μεγέθους σε μια σταθερού μήκους συμβολοσειρά (digest) [138]:

$$h = H(m)$$

όπου H είναι η συνάρτηση κατακερματισμού (π.χ. SHA-256) και m το μήνυμα.

Οι βασικές ιδιότητες που απαιτούνται είναι:

- Προαντίσταση (Preimage resistance): Δε μπορεί να βρεθεί ένα μήνυμα m από το h.

- Δεύτερη προαντίσταση (Second preimage resistance): Δεν υπάρχει άλλο m' ώστε H(m) = H(m').

- Αντοχή σε συγκρούσεις (Collision resistance): Δεν υπάρχουν δύο οποιαδήποτε διαφορετικά μηνύματα m_1, m_2 που να παράγουν το ίδιο hash, δηλαδή $H(m_1) = H(m_2)$.
Η διαφορά από τη δεύτερη προαντίσταση (Second preimage resistance) είναι ότι στη δεύτερη προαντίσταση δίνεται ένα συγκεκριμένο μήνυμα m_1 και ζητείται να βρεθεί άλλο μήνυμα m_2 που να έχει το ίδιο hash δηλαδή πρόκειται για πιο περιορισμένη περίπτωση. Αντίθετα, στην αντοχή σε συγκρούσεις εξετάζεται αν υπάρχουν οποιοδήποτε δύο μηνύματα (χωρίς να δίνεται κάποιο εκ των προτέρων) που συγκρούονται, γεγονός που αποτελεί δυσκολότερο πρόβλημα από υπολογιστική άποψη. [139].

Οι ιδιότητες αυτές διασφαλίζουν ότι η ακεραιότητα των blocks είναι μη παραβιάσιμη.

2.6.3.2 Κρυπτογραφία Δημόσιου Κλειδιού

Κάθε συμμετέχων στο blockchain διαθέτει ένα ζεύγος κλειδιών (public/private key pair) [140].

Το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή συναλλαγών, ενώ το δημόσιο για την επαλήθευσή τους.

Αν m είναι το μήνυμα (συναλλαγή) και sk, pk το ιδιωτικό και δημόσιο κλειδί αντίστοιχα:

$$\sigma = \mathrm{Sign}_{sk}(m)$$

$$\mathrm{Verify}_{pk}(m, \sigma) = \mathrm{True}$$

Μία συναλλαγή θεωρείται έγκυρη μόνο αν η επαλήθευση υπογραφής είναι επιτυχής [141].

Αυτό επιτρέπει την ανωνυμία, χωρίς να θυσιάζεται η επαληθευσιμότητα.

2.6.4 Μηχανισμοί Συναίνεσης (Consensus Mechanisms)

Η συναίνεση είναι η διαδικασία με την οποία τα μέλη ενός αποκεντρωμένου δικτύου συμφωνούν για την κατάσταση του καθολικού (ledger) [142].

Διάφοροι μηχανισμοί έχουν προταθεί, καθένας με διαφορετικές ιδιότητες ασφάλειας, αποδοτικότητας και ενεργειακού κόστους [143].

2.6.4.1 Proof of Work (PoW)

Ο πρώτος και πιο γνωστός μηχανισμός, όπου οι συμμετέχοντες (miners) επιλύουν ένα υπολογιστικά δύσκολο πρόβλημα για να επικυρώσουν ένα block [144].

Στόχος είναι να βρεθεί ένας αριθμός (nonce) ώστε το hash του block να ικανοποιεί:

$$H(B_i) < \mathrm{target}$$

όπου το target είναι μια προκαθορισμένη τιμή δυσκολίας (difficulty target) που καθορίζει πόσο δύσκολη είναι η εξόρυξη ενός νέου block. Όσο μικρότερη είναι η τιμή του target, τόσο πιο δύσκολο είναι να βρεθεί έγκυρο hash που την ικανοποιεί, καθώς απαιτούνται περισσότερες επαναλήψεις δοκιμών (computational trials).

Η διαδικασία απαιτεί μεγάλη υπολογιστική ισχύ, γεγονός που προσδίδει ασφάλεια, αλλά περιορίζει την ενεργειακή απόδοση [145].

Η πιθανότητα επιτυχίας ενός miner είναι ανάλογη της υπολογιστικής του ισχύος.

2.6.4.2 Proof of Stake (PoS)

Στο PoS, η πιθανότητα επικύρωσης ενός block εξαρτάται από το ποσοστό "μετοχών" (stake) που διαθέτει ένας κόμβος στο σύστημα [146].

Αν κάθε κόμβος i διαθέτει ποσότητα stake s_i , τότε η πιθανότητα επιλογής του ως επικυρωτή είναι:

$$P_i = \frac{s_i}{\sum_{j=1}^{N} s_j}$$

Η προσέγγιση αυτή μειώνει δραματικά την ενεργειακή κατανάλωση, καθιστώντας το PoS πιο βιώσιμο για μεγάλης κλίμακας εφαρμογές [147].

2.6.4.3 Byzantine Fault Tolerance (BFT)

Στα δίκτυα όπου οι κόμβοι μπορεί να συμπεριφέρονται κακόβουλα ή αυθαίρετα (Byzantine behavior), οι BFT αλγόριθμοι εξασφαλίζουν ότι επιτυγχάνεται συναίνεση εφόσον λιγότερο από το 1/3 των κόμβων είναι κακόβουλοι [148].

Η συνθήκη ασφάλειας δίνεται ως:

$$N \geq 3f + 1$$

όπου N το πλήθος των κόμβων και f ο αριθμός κακόβουλων.

Κλασικοί αλγόριθμοι της κατηγορίας αυτής είναι οι PBFT, Tendermint και HotStuff, που χρησιμοποιούνται κυρίως σε ιδιωτικά (permissioned) blockchain [149].

2.7 Θεωρητικό Υπόβαθρο Κβαντικού Blockchain

2.7.1 Εισαγωγή

Το Κβαντικό Blockchain (Quantum Blockchain) αποτελεί μία νέα ερευνητική κατεύθυνση που συνδυάζει τις αρχές της Κβαντικής Πληροφορικής και της τεχνολογίας Blockchain με στόχο τη δημιουργία ενός συστήματος ακεραιότητας και ασφάλειας θεμελιωμένου στους νόμους της Φυσικής [150][151].

Ενώ το κλασικό blockchain εξασφαλίζει ακεραιότητα μέσω κρυπτογραφικών μηχανισμών και συναίνεσης, το κβαντικό blockchain αξιοποιεί την υπέρθεση (superposition), τη διεμπλοκή (entanglement) και τη μη-κλωνοποίηση (no-cloning) για την επίτευξη θεμελιωδώς ασφαλούς κατανεμημένης αποθήκευσης και επικύρωσης.

Η προσέγγιση αυτή προέκυψε ως απάντηση στις απειλές που επιφέρουν οι κβαντικοί υπολογιστές στα κλασικά κρυπτογραφικά συστήματα (RSA, ECC, SHA) [152][153][154].

Ερευνητές όπως οι Li, Xu και Qi (2019) πρότειναν το πρώτο θεωρητικό πλαίσιο ενός Quantum Blockchain, ενσωματώνοντας κβαντικά πρωτόκολλα επικοινωνίας, συναίνεσης και κατακερματισμού σε μια ενιαία αλυσίδα κβαντικών blocks [156].
Έκτοτε, το πεδίο του Quantum Blockchain βρίσκεται σε πρώιμο αλλά ραγδαία αναπτυσσόμενο στάδιο, με την έρευνα να εστιάζει κυρίως σε τρεις κατευθύνσεις:

1. Κβαντική ασφάλεια κλασικών blockchain, μέσω Quantum Key Distribution (QKD) και κβαντικών υπογραφών, όπως προτάθηκε από τους Kiktenko et al. (2018) και τους Gottesman & Chuang (2001) [157][158].
2. Αμιγώς κβαντικές αλυσίδες blocks, όπου η ακεραιότητα διασφαλίζεται μέσω κβαντικής διεμπλοκής και Quantum Hash Functions, όπως παρουσιάστηκε στις εργασίες των Jogenfors (2019) και Ikeda (2018) [159][160].
3. Κβαντικοί μηχανισμοί συναίνεσης, όπως ο Quantum Byzantine Agreement (QBA), που προτάθηκε από τους Sun et al. (2018) [161], μειώνοντας δραστικά τον χρόνο επαλήθευσης και αυξάνοντας την ενεργειακή αποδοτικότητα.

Παρά τα ενθαρρυντικά θεωρητικά αποτελέσματα, δεν έχει επιτευχθεί ακόμη πλήρως λειτουργική υλοποίηση Quantum Blockchain, καθώς οι φυσικές απαιτήσεις (π.χ. διατήρηση διεμπλοκής σε μεγάλες αποστάσεις και σταθερή κβαντική συνοχή) παραμένουν τεχνικά προκλητικές.
Ωστόσο, κορυφαία ερευνητικά ιδρύματα και βιομηχανικοί φορείς, όπως η IBM Quantum, η D-Wave και η Cambridge Quantum, εργάζονται ήδη προς την ανάπτυξη υβριδικών blockchain–quantum συστημάτων, τα οποία αξιοποιούν τις υπάρχουσες υποδομές κβαντικών επικοινωνιών για ασφαλέστερη και αποδοτικότερη διαχείριση συναλλαγών.

Η περαιτέρω εξέλιξη του πεδίου απαιτεί βαθύτερη κατανόηση των θεμελιωδών αρχών της κβαντικής πληροφορίας ιδίως της λειτουργίας των qubits, της υπέρθεσης και της διεμπλοκής οι οποίες αποτελούν τον πυρήνα κάθε μελλοντικής αρχιτεκτονικής Quantum Blockchain.

2.7.2 Κβαντική Πληροφορία και Qubits

Η θεμελιώδης μονάδα πληροφορίας στην κβαντική υπολογιστική είναι το qubit, το οποίο μπορεί να βρίσκεται ταυτόχρονα σε υπέρθεση των κλασικών καταστάσεων 0 και 1 [150]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1$$

Η υπέρθεση επιτρέπει σε ένα σύστημα n Qubits να αναπαριστά ταυτόχρονα 2^n καταστάσεις, προσδίδοντας εκθετική υπολογιστική ισχύ [156].

Όταν δύο ή περισσότερα qubits διεμπλέκονται, η κατάσταση του ενός εξαρτάται άμεσα από την κατάσταση του άλλου, ανεξαρτήτως απόστασης, φαινόμενο γνωστό ως quantum entanglement [157].

Η αρχή αυτή αποτελεί το θεμέλιο της κβαντικής επικοινωνίας, καθώς επιτρέπει ασφαλή μετάδοση πληροφορίας χωρίς αντιγραφή του περιεχομένου, λόγω του θεωρήματος μη-κλωνοποίησης [158]:

$$\nexists U : U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle \quad \forall|\psi\rangle$$

Σύμφωνα με το θεώρημα αυτό, δεν είναι δυνατόν να δημιουργηθεί ένα ακριβές αντίγραφο μιας άγνωστης κβαντικής κατάστασης |ψ⟩, δηλαδή δεν υπάρχει καθολικός κβαντικός τελεστής U που να ικανοποιεί U|ψ⟩|0⟩ = |ψ⟩|ψ⟩ για κάθε |ψ⟩.
Η ιδιότητα αυτή απορρέει από τη γραμμικότητα των κβαντικών μετασχηματισμών: εάν ίσχυε η αντιγραφή για δύο διαφορετικές καταστάσεις $|\psi_1\rangle$ και $|\psi_2\rangle$, τότε η υπέρθεσή τους θα οδηγούσε σε μη-γραμμικό αποτέλεσμα, πράγμα αδύνατο στο πλαίσιο της κβαντομηχανικής.
Ως συνέπεια, οποιαδήποτε προσπάθεια υποκλοπής ή μέτρησης αλλοιώνει αναπόφευκτα την κβαντική κατάσταση, καθιστώντας την επίθεση ανιχνεύσιμη και τη μετάδοση θεμελιωδώς ασφαλή [154][155].

2.7.3 Κβαντική Επικοινωνία και Διανομή Κλειδιών (QKD)

Η Κβαντική Διανομή Κλειδιών (Quantum Key Distribution – QKD) αποτελεί έναν από τους θεμελιώδεις μηχανισμούς της κβαντικής επικοινωνίας, επιτρέποντας την ανταλλαγή κρυπτογραφικών κλειδιών με απόλυτη ασφάλεια, που εδράζεται στους φυσικούς νόμους της Κβαντομηχανικής και όχι στη μαθηματική πολυπλοκότητα.

Σε αντίθεση με τις κλασικές μεθόδους συμμετρικής ή ασύμμετρης κρυπτογράφησης (π.χ. RSA, ECC), των οποίων η ασφάλεια μπορεί να παραβιαστεί από ισχυρούς κβαντικούς υπολογιστές, η QKD είναι θεωρητικά απρόσβλητη από οποιαδήποτε υπολογιστική ισχύ, καθώς κάθε προσπάθεια υποκλοπής μεταβάλλει το ίδιο το φυσικό σύστημα μετάδοσης [159].

Το πλέον καθιερωμένο πρωτόκολλο QKD είναι το BB84 (Bennett & Brassard, 1984).
Σε αυτό, η πληροφορία κωδικοποιείται στην πόλωση φωτονίων, με κάθε bit να αποστέλλεται τυχαία είτε σε ορθογώνια βάση (|0⟩, |1⟩) είτε σε διαγώνια βάση (|+⟩, |−⟩) [160].
Η ορθογώνια βάση αντιστοιχεί σε κατακόρυφη και οριζόντια πόλωση, ενώ η διαγώνια βάση προκύπτει από γραμμικό συνδυασμό των δύο πρώτων καταστάσεων και αντιστοιχεί σε πόλωση υπό γωνία 45° και 135°.
Συγκεκριμένα, οι καταστάσεις της διαγώνιας βάσης ορίζονται ως:

$|+\rangle = (|0\rangle + |1\rangle) / \sqrt{2}$
$|-\rangle = (|0\rangle - |1\rangle) / \sqrt{2}$

Η χρήση δύο διαφορετικών βάσεων (ορθογώνιας και διαγώνιας) επιτρέπει την ανίχνευση πιθανής υποκλοπής, καθώς κάθε λάθος επιλογή βάσης από τρίτο μέρος (Eve) μεταβάλλει την κατάσταση των φωτονίων, αποκαλύπτοντας έτσι την παρουσία της.

Ο πομπός (Alice) αποστέλλει μια ακολουθία φωτονίων, και ο δέκτης (Bob) τα μετρά σε τυχαίες βάσεις. Μετά τη μετάδοση, οι δύο πλευρές συγκρίνουν δημόσια τις βάσεις τους (όχι τα αποτελέσματα), και διατηρούν μόνο εκείνες τις μετρήσεις που έγιναν στις ίδιες βάσεις.

Το αποτέλεσμα είναι ένα κοινό κλειδί, το οποίο είναι τυχαίο, απόλυτα συγχρονισμένο και ασφαλές.

Εάν τρίτος (Eve) επιχειρήσει υποκλοπή, η ίδια η πράξη μέτρησης μεταβάλλει την κατάσταση των φωτονίων (λόγω της αρχής της αβεβαιότητας του Heisenberg και του no-cloning theorem) [155]. Έτσι, η εισαγωγή θορύβου στο κανάλι αποκαλύπτει άμεσα την παρουσία της, επιτρέποντας την απόρριψη του συμβιβασμένου κλειδιού.

Η εφαρμογή της QKD στο Quantum Blockchain έχει διττό ρόλο:

1. Κβαντική υπογραφή συναλλαγών και blocks: Τα παραγόμενα κλειδιά χρησιμοποιούνται για τη δημιουργία quantum-resistant υπογραφών, διασφαλίζοντας ότι κάθε block είναι πιστοποιημένο και μη αντιγράψιμο.
2. Ασφαλής μετάδοση ενημερώσεων μοντέλου: Στο πλαίσιο του Quantum Federated Learning, τα QKD κλειδιά χρησιμοποιούνται για την κβαντική κρυπτογράφηση (QKD-encryption) των παγκόσμιων βαρών που μεταδίδονται από τον Global Aggregator προς τους clients. Μόνο οι νόμιμοι κόμβοι, που διαθέτουν το ιδιωτικό τους κβαντικό κλειδί, μπορούν να πραγματοποιήσουν την αποκρυπτογράφηση.

Η υλοποίηση της QKD στη συγκεκριμένη εργασία προσομοιώθηκε μέσω κβαντικών καναλιών επικοινωνίας με χρήση προσομοιωτών όπως το PennyLane και το Qiskit, δεδομένου ότι η φυσική εγκατάσταση φωτονικών καναλιών υπερβαίνει τις δυνατότητες του διαθέσιμου υλικού. Ωστόσο, η αρχιτεκτονική έχει σχεδιαστεί με τρόπο που επιτρέπει μελλοντική ενσωμάτωση πραγματικού QKD hardware, προσφέροντας πλήρη end-to-end κβαντική ασφάλεια στο οικοσύστημα του Quantum Blockchain [161].

2.7.4 Δομή Κβαντικού Block

Κάθε κβαντικό block αποτελείται από δύο μέρη: ένα κλασικό τμήμα που περιέχει τα δεδομένα και τις μετα-πληροφορίες (metadata), και ένα κβαντικό τμήμα, το οποίο αποτελεί την "κβαντική αποτύπωση" του block.

Ο μαθηματικός ορισμός ενός κβαντικού block είναι:

$$B_i = (C_i, |\Psi_i\rangle)$$

όπου:

- C_i αντιπροσωπεύει τα κλασικά δεδομένα του block (π.χ. Hash, timestamp, συναλλαγές),

- $|\Psi_i\rangle$ είναι η κβαντική κατάσταση που συνδέεται με το block μέσω διεμπλοκής με το προηγούμενο block [156].

Η συνολική αλυσίδα μπορεί να περιγραφεί ως:

$$|\Psi_{\text{chain}}\rangle = |\Psi_{B_1}\rangle \otimes |\Psi_{B_2}\rangle \otimes \cdots \otimes |\Psi_{B_n}\rangle$$

Η διεμπλοκή μεταξύ των blocks διασφαλίζει ότι οποιαδήποτε αλλοίωση ενός block θα διακόψει την κβαντική συνοχή (coherence) της αλυσίδας, καθιστώντας την παραποίηση ανιχνεύσιμη [157][158].

2.7.5 Κβαντικές Συναρτήσεις Κατακερματισμού (Quantum Hash Functions)

Οι κλασικές συναρτήσεις κατακερματισμού, όπως οι SHA-256, είναι ευάλωτες σε κβαντικούς αλγορίθμους όπως ο Grover [153], ο οποίος μειώνει την πολυπλοκότητα της αναζήτησης από $O(2^n)$ σε $O(2^{n/2})$.

Για τον λόγο αυτό, απαιτούνται κβαντικά ασφαλείς συναρτήσεις κατακερματισμού που βασίζονται σε φυσικούς νόμους αντί σε υπολογιστική δυσκολία.

Η Κβαντική Συνάρτηση Κατακερματισμού (Quantum Hash Function, QHF) [155][158] ορίζεται ως ένας μοναδιαίος τελεστής:

$$|\psi_H\rangle = U_H|\psi_{\text{in}}\rangle$$

όπου το U_H είναι ένας μοναδιαίος μετασχηματισμός που χαρτογραφεί μία είσοδο σε μια μοναδική έξοδο στον χώρο Hilbert.

Η σύγκριση δύο hash καταστάσεων γίνεται μέσω του inner product:

$$|\langle\psi_H(x)|\psi_H(y)\rangle| \leq \epsilon$$

όπου η σχεδόν ορθογωνιότητα ($\epsilon \ll 1$) εξασφαλίζει τη δυσκολία εύρεσης συγκρούσεων [159].

Ένα σημαντικό χαρακτηριστικό των QHF είναι η μη αντιστρεψιμότητα μέσω φυσικής αδυναμίας:

η μέτρηση της κβαντικής κατάστασης καταστρέφει την πληροφορία που περιέχει, γεγονός που αποκλείει την ανακατασκευή της εισόδου.

Στο πλαίσιο του Quantum Blockchain, η σχέση μεταξύ blocks περιγράφεται ως:

$$|\Psi_{B_i}\rangle = U_H(|\Psi_{B_{i-1}}\rangle \otimes |\Psi_{\text{data},i}\rangle)$$

Με τον τρόπο αυτό, κάθε block εξαρτάται κβαντικά από το προηγούμενο, δημιουργώντας ένα hash chain [156][160].

2.7.6 Απόδειξη Κβαντικής Εργασίας (Quantum Proof of Work – QPoW)

Στα κλασικά blockchain, η απόδειξη εργασίας (Proof of Work – PoW) βασίζεται σε εξαντλητική αναζήτηση μιας λύσης που ικανοποιεί έναν περιορισμό hash [156].

Η κβαντική εκδοχή, Quantum Proof of Work (QPoW), αντικαθιστά αυτή τη διαδικασία με έναν κβαντικό υπολογισμό που επαληθεύεται ταχύτερα και ασφαλέστερα.

Στο QPoW, οι miners επιλύουν ένα κβαντικό πρόβλημα ελαχιστοποίησης μέσω Quantum Annealing ή Variational Quantum Circuits [161], ώστε να βρουν τη βέλτιστη λύση για μια συνάρτηση κόστους H(x), η οποία εκφράζει την "ενέργεια" ή το σφάλμα του συστήματος που πρέπει να ελαχιστοποιηθεί:

$$E_{\min} = \min_{x} \langle x|H|x\rangle$$

Η συνάρτηση κόστους H(x) ορίζεται συνήθως ως ένας Χαμιλτονιανός τελεστής που αντιπροσωπεύει την κατάσταση του δικτύου, π.χ. τις σχέσεις μεταξύ των blocks ή τις πιθανές λύσεις συναίνεσης.
Ο στόχος του συστήματος είναι να βρεθεί η κατάσταση ελάχιστης ενέργειας (ground state), η οποία αντιστοιχεί στο "νόμιμο" block, δηλαδή στη λύση που ικανοποιεί όλους τους περιορισμούς του δικτύου.

Στην πράξη, αυτό επιτυγχάνεται είτε μέσω Quantum Annealing, όπου το σύστημα εξελίσσεται φυσικά προς την ελάχιστη ενεργειακή κατάσταση μειώνοντας σταδιακά το «κβαντικό θόρυβο», είτε μέσω Variational Quantum Circuits (VQC), όπου μια παραμετροποιημένη κβαντική συνάρτηση ελαχιστοποιεί επαναληπτικά το H(x) μέσω μετρήσεων και ενημέρωσης παραμέτρων.

Η λύση με την ελάχιστη ενέργεια αντιστοιχεί στο "νόμιμο" block, ενώ ο έλεγχος εγκυρότητας πραγματοποιείται μέσω κβαντικής μέτρησης, η οποία είναι ταχύτατη και εγγενώς ασφαλής, αφού οποιαδήποτε αλλοίωση του αποτελέσματος μεταβάλλει την ίδια τη φυσική κατάσταση του συστήματος [150].

Η διαδικασία αυτή μειώνει την ενεργειακή κατανάλωση και εξαλείφει την ανάγκη για συνεχή επαναϋπολογισμό hash, καθώς η επικύρωση γίνεται μέσω φυσικού μηχανισμού ελαχιστοποίησης ενέργειας [156][161].

2.7.7 Κβαντικά Merkle Trees και Επαλήθευση Ακεραιότητας

Στο κλασικό blockchain, οι Merkle Trees χρησιμοποιούνται για την αποδοτική επαλήθευση της εγκυρότητας συναλλαγών.

Στην κβαντική εκδοχή, οι Merkle Trees υλοποιούνται μέσω υπερθέσεων κβαντικών καταστάσεων (quantum superposition) [150], όπου κάθε φύλλο αναπαρίσταται από μία κατάσταση qubit:

$$| \Phi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} | T_i\rangle$$

Η παραπάνω σχέση εκφράζει την υπέρθεση όλων των φύλλων του δέντρου, επιτρέποντας την ταυτόχρονη αναπαράσταση πολλών συναλλαγών.
Για να επιτευχθεί όμως διεμπλοκή (entanglement) μεταξύ των φύλλων, εφαρμόζονται κβαντικές πύλες τύπου CNOT ή Controlled-Z, οι οποίες δημιουργούν συσχετίσεις μεταξύ των qubits:

$$| \Psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} | T_i\rangle | C_i\rangle$$

όπου κάθε φύλλο $| T_i\rangle$ είναι διεμπλεγμένο με έναν κόμβο ελέγχου $| C_i\rangle$, διασφαλίζοντας ότι η μεταβολή μιας συναλλαγής επηρεάζει ολόκληρη τη δομή.
Η διεμπλοκή αυτή επιτρέπει την ταυτόχρονη επαλήθευση πολλαπλών συναλλαγών, ενώ η μέτρηση ενός μόνο qubit επαρκεί για την επιβεβαίωση της συνολικής ακεραιότητας του δέντρου [157][158].

Η κβαντική αυτή δομή μειώνει την υπολογιστική πολυπλοκότητα από O(log N) σε O(1) υπό ιδανικές συνθήκες [156].

2.7.8 Κβαντικοί Μηχανισμοί Συναίνεσης (Quantum Consensus)

Οι κβαντικοί μηχανισμοί συναίνεσης επιτρέπουν τη συμφωνία μεταξύ κόμβων μέσω ανταλλαγής διεμπλεγμένων qubits.

Η πιο χαρακτηριστική μορφή είναι ο Quantum Byzantine Agreement (QBA) [161], στον οποίο οι κόμβοι επιτυγχάνουν ομόφωνη απόφαση χωρίς επαναλαμβανόμενους γύρους επικοινωνίας.

Αν n κόμβοι μοιράζονται μια διεμπλεγμένη κατάσταση:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle)$$

τότε η μέτρηση ενός κόμβου επηρεάζει στιγμιαία όλους τους υπόλοιπους, επιτυγχάνοντας ταχεία σύγκλιση και ανθεκτικότητα σε byzantine συμπεριφορές [156][157].

2.7.9 Ιδιότητες και Πλεονεκτήματα του Quantum Blockchain

- Κβαντική Αμεταβλητότητα (Quantum Immutability): Η αλλοίωση ενός block καταστρέφει τη διεμπλοκή όλης της αλυσίδας [158].

- Ασφάλεια μέσω Φυσικής (Physics-based Security): Η ασφάλεια δεν βασίζεται σε υπολογιστική πολυπλοκότητα, αλλά σε φυσικούς νόμους [152][159].

- Ενεργειακή Αποδοτικότητα: Οι μηχανισμοί τύπου QPoW είναι λιγότερο ενεργοβόροι [161].

- Ταχύτητα Συναίνεσης: Η διεμπλοκή επιτρέπει άμεση διάδοση πληροφορίας [157].

- Ανίχνευση Υποκλοπής: Κάθε απόπειρα μέτρησης αλλοιώνει τις κβαντικές καταστάσεις, αποκαλύπτοντας τον επιτιθέμενο [160].

2.7.10 Συμπέρασμα

Το Κβαντικό Blockchain συνιστά μία ριζικά νέα θεώρηση της αποκεντρωμένης εμπιστοσύνης.

Η ενσωμάτωση αρχών της κβαντικής φυσικής καθιστά τη δομή θεμελιωδώς ασφαλή, επεκτάσιμη και ανθεκτική απέναντι στους μελλοντικούς κβαντικούς υπολογιστές [150].

Η θεωρητική βάση που παρουσιάστηκε στο παρόν κεφάλαιο παρέχει το υπόβαθρο για την ανάπτυξη πρακτικών αρχιτεκτονικών που συνδυάζουν Federated Learning και Quantum Blockchain [161], οι οποίες θα παρουσιαστούν στα επόμενα κεφάλαια.

Κεφάλαιο 3: Σχετική Έρευνα και Τεχνολογική Ανασκόπηση

Όπως έχουμε αναφέρει και στην εισαγωγή, η ραγδαία ανάπτυξη της Τεχνητής Νοημοσύνης (ΤΝ) και των κατανεμημένων υπολογιστικών συστημάτων έχει οδηγήσει στη δημιουργία νέων προσεγγίσεων που στοχεύουν στη βελτίωση της απόδοσης, της ιδιωτικότητας και της ασφάλειας στη μηχανική μάθηση. Στο πλαίσιο αυτό, τεχνολογίες όπως η Ομοσπονδιακή Μάθηση, το Blockchain και η Κβαντική Υπολογιστική έχουν αναδειχθεί ως κρίσιμοι άξονες έρευνας, επιτρέποντας την ασφαλή και αποκεντρωμένη επεξεργασία δεδομένων [162]. Η ανίχνευση απάτης (Fraud Detection) αποτελεί ένα από τα πλέον σημαντικά προβλήματα στον χώρο των χρηματοοικονομικών τεχνολογιών. Ο αυξανόμενος όγκος και η πολυπλοκότητα των δεδομένων συναλλαγών καθιστούν αναγκαία την ανάπτυξη αποδοτικών μεθόδων εντοπισμού ύποπτων προτύπων σε πραγματικό χρόνο. Παρά το γεγονός ότι παραδοσιακές τεχνικές μηχανικής μάθησης, όπως τα Νευρωνικά Δίκτυα, τα Random Forest και οι Support Vector Machine, έχουν εφαρμοστεί εκτενώς, εξακολουθούν να παρουσιάζουν περιορισμούς στη γενίκευση, την αποδοτικότητα και την επεξηγησιμότητα, ιδιαίτερα όταν τα δεδομένα είναι μη-γραμμικά, υψηλής διάστασης ή διαμοιρασμένα σε πολλαπλές πηγές [163].

Η ανάγκη για πιο ασφαλή και συνεργατικά συστήματα μάθησης οδήγησε στη διερεύνηση αποκεντρωμένων προσεγγίσεων, όπως η Ομοσπονδιακή Μάθηση, σε συνδυασμό με Blockchain και κβαντικές τεχνικές, οι οποίες υπόσχονται να αντιμετωπίσουν τους περιορισμούς των υφιστάμενων λύσεων [164].

3.1 Quantum Machine Learning

Η Κβαντική Μηχανική Μάθηση (Quantum Machine Learning – QML) αξιοποιεί τις αρχές της υπέρθεσης και της διεμπλοκής ώστε να επεξεργάζεται πληροφορία με παράλληλο και, σε ορισμένες περιπτώσεις, πιο αποδοτικό τρόπο σε σχέση με τα κλασικά μοντέλα. Η έρευνα των τελευταίων ετών υποδεικνύει ότι αλγόριθμοι QML μπορούν να μειώσουν σημαντικά την υπολογιστική πολυπλοκότητα καθώς και να αναγνωρίσουν πρότυπα σε δεδομένα υψηλής διάστασης όπου οι κλασικές μέθοδοι συχνά αντιμετωπίζουν περιορισμούς [165][166].

Στην πράξη, μέσα στο QML έχουν αναδειχθεί αρκετές βασικές τεχνικές:

- Οι Quantum Neural Networks (QNNs) και οι Variational Quantum Circuits (VQCs) επιτρέπουν την εισαγωγή παραμέτρων σε κβαντικά κυκλώματα τα οποία βελτιστοποιούνται (συνήθως μέσω κλασικών μεθόδων) ώστε να μαθαίνουν συσχετίσεις σε δεδομένα. [167]
- Οι Quantum Support Vector Machines (QSVMs) και — περισσότερο γενικά — οι τεχνικές των κβαντικών πυρήνων (quantum kernels) χρησιμοποιούνται για την έκφραση μη-γραμμικών σχέσεων μέσω ειδικών χαρτών χαρακτηριστικών (feature maps) στον χώρο των qubits. [168]
- Επιπλέον τεχνικές περιλαμβάνουν την Quantum Principal Component Analysis (QPCA) και διάφορα σχήματα «κβαντικής ανίχνευσης ανωμαλιών» (Quantum Anomaly Detection), που εισάγουν υπολογισμούς όπως μείωση διάστασης ή εκτίμηση ομοιοτήτων σε πολύπλοκα σύνολα δεδομένων [169][170].
- Ένα σημαντικό μοντέλο είναι τα υβριδικά quantum-classical μοντέλα: ενώ το κβαντικό κύκλωμα πραγματοποιεί τη βασική επεξεργασία (π.χ. αναπαράσταση, μετασχηματισμό, διεμπλοκή, feature map), η βελτιστοποίηση και η εκπαίδευση εκτελούνται κλασικά. Αυτό το υβριδικό σχήμα είναι ιδιαίτερα κρίσιμο για την εποχή των NISQ (Noisy Intermediate-Scale Quantum) συσκευών [171][167].
- Τα Quantum Graph Neural Networks (QGNNs) αποτελούν μια προχωρημένη τεχνική που συγχωνεύει δομές γραφημάτων (graph-structured data) με την κβαντική επεξεργασία: η προσέγγιση αυτή επιτρέπει την επεξεργασία δομών όπως κόμβοι και ακμές (π.χ. σε συναλλαγές) μέσω κυκλωμάτων της κβαντικής πληροφορίας, με στόχο τη βελτίωση της απόδοσης σε καθήκοντα όπως η ανίχνευση απάτης. Στη μελέτη των Nouhaila Innan et al.

(2024) αναπτύσσεται ένα πλαίσιο QGNN για τον εντοπισμό χρηματοοικονομικής απάτης, όπου αξιοποιούνται Variational Quantum Circuits (VQCs) ως θεμελιώδη μονάδα εκπαίδευσης — υπό πραγματικό σύνολο δεδομένων με graph-δομή το μοντέλο πέτυχε AUC ≈ 0,85, υπερβαίνοντας αντίστοιχες κλασικές προσεγγίσεις [170].

Η εφαρμογή των παραπάνω τεχνικών σε περιπτώσεις όπου τα δεδομένα είναι πολυδιάστατα, μη γραμμικά και ενίοτε ανισορροπημένα — όπως στη χρηματοοικονομική ανάλυση και στην ανίχνευση απάτης — φαίνεται ιδιαιτέρως υποσχόμενη. Μέσω κατάλληλης χαρτογράφησης (feature map) των κλασικών δεδομένων σε κβαντικό χώρο και μέσω της χρήσης πυλών περιστροφής και διεμπλοκής, τα μοντέλα μπορούν να αποκτήσουν αυξημένη εκφραστικότητα και να διαχειριστούν πιο σύνθετα μοτίβα.

Σε θεωρητικό επίπεδο, ερευνητές έχουν αναδείξει πως οι quantum kernels μπορεί να προσφέρουν πλεονέκτημα μόνο υπό συγκεκριμένες προϋποθέσεις: όταν η συνάρτηση στόχος ανήκει σε έναν χώρο που μπορεί να αποτυπωθεί αποτελεσματικά από τον κβαντικό χάρτη, αλλά όχι εύκολα από τα κλασικά μοντέλα [172]. Επίσης, η αξιοποίηση των VQCs και άλλων παραμετρικών κβαντικών κυκλωμάτων αντιμετωπίζει θέματα όπως η εκπαίδευση, η «γήρανση» (barren-plateau) του τοπικού κόστους, καθώς και ο θόρυβος και η αστάθεια των NISQ υλοποιήσεων [167][173].

Συνοψίζοντας, η QML λειτουργεί ως καταλύτης αποδοτικότητας με τα εξής χαρακτηριστικά:

- Μείωση της ανάγκης για τεράστιο όγκο εκπαίδευσης δεδομένων, καθώς η παράλληλη επεξεργασία και η επεκτασιμότητα των qubits μπορούν να προσφέρουν περισσότερη πληροφορία ανά «βήμα». [174]
- Ταχύτερη προσαρμογή σε μεταβαλλόμενα περιβάλλοντα, μέσω της δυνατότητας τροποποίησης του κβαντικού κυκλώματος ή του χάρτη χαρακτηριστικών με μικρότερο κόστος. [175]
- Βελτιωμένη γενίκευση των μοντέλων σε μη-γραμμικές σχέσεις και δεδομένα υψηλής διάστασης, λόγω της εισαγωγής διεμπλοκής και υπέρθεσης στον χώρο χαρακτηριστικών. [174] [176]

Παρόλα αυτά, είναι κρίσιμο να τονιστεί ότι η αυτόνομη χρήση κβαντικών μοντέλων δεν επαρκεί για την κάλυψη ζητημάτων όπως η ιδιωτικότητα, η διαφάνεια και η αξιοπιστία. Για αυτόν τον λόγο, η παρούσα εργασία ενσωματώνει τα QML μοντέλα στο πλαίσιο του Federated Learning και συνδέει τα αποτελέσματά τους με μηχανισμούς επαλήθευσης μέσω blockchain, δημιουργώντας ένα ολοκληρωμένο και ασφαλές οικοσύστημα μάθησης. Με αυτόν τον τρόπο, το μοντέλο αξιοποιεί την κβαντική αποδοτικότητα, τη συλλογική μάθηση (federated), και τη διαφάνεια/ακεραιότητα μέσω blockchain — γεγονός που το καθιστά κατάλληλο για εφαρμογές όπως τραπεζικά συστήματα, ανίχνευση απάτης, και ασφαλείς συναλλαγές σε δυναμικά περιβάλλοντα.

3.2 Ομοσπονδιακή Μάθηση και Ιδιωτικότητα Δεδομένων

Η έννοια του Federated Learning (FL) προτάθηκε αρχικά από τους McMahan et al. (2017) ως μια μέθοδος αποκεντρωμένης εκπαίδευσης μοντέλων χωρίς τη συγκέντρωση των δεδομένων σε έναν κεντρικό εξυπηρετητή [89]. Το μοντέλο επιτρέπει στους επιμέρους κόμβους να εκπαιδεύουν τοπικά νευρωνικά δίκτυα και να αποστέλλουν μόνο τις παραμέτρους των μοντέλων για συνάθροιση (aggregation), ενισχύοντας έτσι την ιδιωτικότητα και μειώνοντας τον κίνδυνο παραβίασης δεδομένων.

Η βιβλιογραφία έχει δείξει ότι το FL αποτελεί μια βιώσιμη λύση για περιβάλλοντα με αυστηρούς κανονισμούς προστασίας δεδομένων, όπως ο GDPR, ωστόσο συνοδεύεται από σημαντικές τεχνικές προκλήσεις [4]. Η μη ομοιογένεια των δεδομένων (non-IID data) μεταξύ των κόμβων επηρεάζει αρνητικά τη σύγκλιση του μοντέλου, ενώ ο μεγάλος όγκος επικοινωνίας κατά τη διάρκεια της εκπαίδευσης αυξάνει το υπολογιστικό κόστος [94].

Πρόσφατες έρευνες έχουν εστιάσει στην ενσωμάτωση μηχανισμών Differential Privacy (DP) και Secure Aggregation, επιτρέποντας τη μαθηματικά αποδεδειγμένη προστασία των τοπικών παραμέτρων [121]. Παράλληλα, η ανάπτυξη συστημάτων συνάθροισης βασισμένων στη φήμη (reputation-based aggregation systems), όπου οι κόμβοι σταθμίζονται βάσει της αξιοπιστίας τους, συμβάλλει στη μείωση επιθέσεων δηλητηρίασης (poisoning attacks) και στη διατήρηση της συνολικής απόδοσης του συστήματος [122]. Παρά την πρόοδο, η απουσία ενός καθολικά αποδεκτού μηχανισμού ελέγχου της εμπιστοσύνης και η εξάρτηση από έναν κεντρικό συναθροιστή (aggregator) εξακολουθούν να αποτελούν ζητήματα προς επίλυση. Οι προκλήσεις αυτές έχουν οδηγήσει στην αναζήτηση αποκεντρωμένων μηχανισμών επαλήθευσης, με κυριότερο εκπρόσωπο την τεχνολογία Blockchain.

3.3 Blockchain και Αποκεντρωμένη Επεξεργασία

Το Blockchain, που εισήχθη από τον Satoshi Nakamoto (2008) [129], αποτελεί μια καινοτόμο τεχνολογία αποκεντρωμένης καταγραφής και επαλήθευσης συναλλαγών. Χάρη στις ιδιότητές του — ακεραιότητα, διαφάνεια και αμεταβλητότητα — έχει χρησιμοποιηθεί σε ποικίλες εφαρμογές, από χρηματοοικονομικά συστήματα έως βιομηχανικές αλυσίδες εφοδιασμού [130].

Οι μηχανισμοί συναίνεσης όπως το Proof of Work (PoW) και το Proof of Stake (PoS) εξασφαλίζουν τη συνέπεια των δεδομένων σε περιβάλλοντα χωρίς εμπιστοσύνη (trustless environments). Ωστόσο, οι λύσεις αυτές συνεπάγονται υψηλή κατανάλωση ενέργειας, καθυστέρηση συναλλαγών και πιθανή συγκέντρωση υπολογιστικής ισχύος σε περιορισμένο αριθμό κόμβων [131].

Για την αντιμετώπιση αυτών των ζητημάτων, προτάθηκε η ενσωμάτωση του blockchain σε περιβάλλοντα Federated Learning, δημιουργώντας το λεγόμενο Blockchain-based Federated Learning (BFL) [101]. Σε αυτό το πλαίσιο, κάθε κόμβος αποθηκεύει και επαληθεύει τα κρυπτογραφημένα βάρη μέσω smart contracts, εξαλείφοντας την ανάγκη ύπαρξης ενός κεντρικού aggregator και ενισχύοντας την εμπιστοσύνη μεταξύ των συμμετεχόντων.

Παρότι η σύζευξη blockchain και FL έχει αποδειχθεί αποτελεσματική για την ενίσχυση της διαφάνειας και της ανθεκτικότητας έναντι επιθέσεων, το υψηλό ενεργειακό κόστος και η περιορισμένη επεκτασιμότητα των παραδοσιακών μηχανισμών συναίνεσης παραμένουν σημαντικά εμπόδια [132]. Αυτές οι αδυναμίες αποτέλεσαν κίνητρο για την αναζήτηση εναλλακτικών προσεγγίσεων μέσω της κβαντικής υπολογιστικής.

3.4 Quantum Blockchain

Η εργασία των Amin et al. (2025) [156], με τίτλο Blockchain with Proof of Quantum Work, εισάγει ένα νέο παράδειγμα κβαντικού blockchain, όπου η διαδικασία συναίνεσης βασίζεται στην Απόδειξη Κβαντικής Εργασίας (Proof of Quantum Work – PoQ). Σε αντίθεση με τους κλασικούς μηχανισμούς PoW, το PoQ απαιτεί την εκτέλεση υπολογισμών που μπορούν να πραγματοποιηθούν μόνο από κβαντικούς επεξεργαστές, καθιστώντας έτσι τη διαδικασία εξόρυξης πρακτικά αδύνατη για κλασικά συστήματα [156] .

Η αρχιτεκτονική που προτείνεται στην εργασία των Amin et al. [156] συνδυάζει κλασικά και κβαντικά στοιχεία, εισάγοντας νέες έννοιες όπως η πιθανοκρατική επικύρωση (probabilistic validation) και η αναθεωρημένη αλυσίδα εργασίας (confidence-based Chainwork), οι οποίες αντιμετωπίζουν τα προβλήματα αβεβαιότητας των κβαντικών μετρήσεων. Οι πειραματικές δοκιμές πραγματοποιήθηκαν σε τέσσερα γεωγραφικά κατανεμημένα D-Wave QPUs, αποδεικνύοντας τη σταθερότητα του συστήματος σε περιβάλλοντα με στοχαστικά σφάλματα .

Το PoQ προσφέρει τριπλό πλεονέκτημα:

Ασφάλεια απέναντι σε κλασικές και κβαντικές επιθέσεις (λόγω spoof-resistance και κβαντικής υπεροχής),

- Ενεργειακή αποδοτικότητα, μειώνοντας το κόστος εξόρυξης έως και 1000 φορές σε σχέση με το PoW,
- Πραγματική αποκέντρωση, καθώς η διαδικασία mining κατανέμεται σε ανεξάρτητες κβαντικές συσκευές.

Η συμβολή της συγκεκριμένης μελέτης είναι καθοριστική, καθώς αποτελεί το πρώτο πειραματικό παράδειγμα αξιοποίησης κβαντικής υπεροχής σε πραγματικό blockchain. Παράλληλα, η εργασία ανοίγει νέες προοπτικές για την ανάπτυξη υβριδικών κβαντο-κλασικών συστημάτων, τα οποία μπορούν να εξισορροπήσουν ασφάλεια και αποδοτικότητα, παρέχοντας ένα νέο επίπεδο αξιοπιστίας σε κατανεμημένα δίκτυα [160].

3.5 Federated Quantum Machine Learning

Η σύγκλιση των πεδίων του Federated Learning (FL) και της Quantum Machine Learning (QML) έχει οδηγήσει στην ανάπτυξη του Federated Quantum Machine Learning (FQML), μιας νέας παραδειγματικής προσέγγισης που συνδυάζει τα πλεονεκτήματα της αποκεντρωμένης μάθησης με την κβαντική υπολογιστική ισχύ [164],[177-179]. Στο FQML, η εκπαίδευση Quantum Neural Networks (QNNs) πραγματοποιείται σε κατανεμημένα περιβάλλοντα χωρίς ανταλλαγή των ακατέργαστων δεδομένων μεταξύ των κόμβων· κάθε τοπικός κόμβος διαθέτει έναν κβαντικό ή υβριδικό κβαντικό-κλασικό επεξεργαστή που εκτελεί τοπικά βήματα εκπαίδευσης και αποστέλλει μόνο τις ενημερωμένες παραμέτρους (π.χ. βάρη ή γωνίες κυκλωμάτων) στο κεντρικό aggregator [177-179].

Η μελέτη του FedQNN: Federated Learning using Quantum Neural Networks – Innan et al. (2024) – παρουσίασε ένα καινοτόμο πλαίσιο QFL, όπου QNNs εντάσσονται σε ομοσπονδιακή δομή εκπαίδευσης· τα αποτελέσματα τους ανέφεραν ακρίβεια άνω του ~86 % σε τρία διαφορετικά σύνολα δεδομένων, καταδεικνύοντας την πρακτική σκοπιμότητα της προσέγγισης [177]. Παράλληλα, η μελέτη Quantum machine learning beyond kernel methods – Jerbi et al. (2023) – ανέδειξε ότι τα QML μοντέλα μπορούν να υπερβούν τις παραδοσιακές kernel-based μεθόδους, προσφέροντας αυξημένη εκφραστικότητα και δυνατότητα μάθησης πολύπλοκων κατανομών, γεγονός που ενισχύει το θεωρητικό θεμέλιο για ενσωμάτωση των QNNs σε federated δομές [179].

Υπάρχουν ωστόσο σημαντικές προκλήσεις: η σταθερότητα και αξιοπιστία των κβαντικών μετρήσεων και κυκλωμάτων (ειδικά σε κατανεμημένα συστήματα με αποκλίσεις και θόρυβο), η συγχρονισμένη επικοινωνία των ενημερώσεων μεταξύ των κόμβων και του aggregator (ειδικά υπό μη IID δεδομένα ή ετερογενείς πόρους), και η πρακτική υλοποίηση και κλιμάκωση του μοντέλου σε πραγματικά περιβάλλοντα, όπου οι κβαντικοί πόροι είναι περιορισμένοι και η ανάγκη για υβριδικά κβαντικά-κλασικά σχήματα είναι πιθανώς αναπόφευκτη. Παρά τις προκλήσεις αυτές, η κατεύθυνση θεωρείται το επόμενο κρίσιμο βήμα προς την ανάπτυξη Quantum-Secure Federated Systems, στα οποία συνδυάζονται ασφάλεια, ιδιωτικότητα και κβαντική υπολογιστική υπεροχή [155].

Κεφάλαιο 4. Προτεινόμενη Αρχιτεκτονική

4.1 Περιγραφή του Προβλήματος

4.1.1 Fraud Detection

Η ανίχνευση απάτης (Fraud Detection) αποτελεί ένα από τα πιο κρίσιμα και πολύπλοκα προβλήματα στα σύγχρονα τραπεζικά και χρηματοοικονομικά συστήματα. Η συνεχώς αυξανόμενη ψηφιοποίηση των οικονομικών συναλλαγών, σε συνδυασμό με τη χρήση πολλαπλών καναλιών πληρωμών (ηλεκτρονικές κάρτες, διαδικτυακές μεταφορές, e-wallets), έχει οδηγήσει σε δραματική αύξηση των περιστατικών ηλεκτρονικής απάτης. Σύμφωνα με την European Central Bank (ECB) και την European Banking Authority (EBA), η συνολική αξία των δόλιων συναλλαγών για τα κύρια όργανα πληρωμών στην περιοχή ΕΟΧ (ΕΕΑ) έφτασε τα 4,3 δισεκατομμύρια € το έτος 2022 και 2,0 δισεκατομμύρια € στο α' εξάμηνο του 2023. [180]

Το πρόβλημα παρουσιάζει ιδιαίτερη πολυπλοκότητα, καθώς τα μοτίβα της απάτης είναι δυναμικά, σπάνια και υψηλής μη-γραμμικότητας, γεγονός που δυσχεραίνει τη μοντελοποίησή τους. Επιπλέον, το ποσοστό των «ψευδώς θετικών» (false positives) παραμένει υψηλό σε πολλά εμπορικά συστήματα — για παράδειγμα, σε μελέτη βάσης τραπεζικών συναλλαγών καταγράφηκε ποσοστό false positive έως και 8.9% ή και 10-15%. [181]

4.1.2 Υφιστάμενες προσεγγίσεις ανίχνευσης απάτης

Η πιο διαδεδομένες μέθοδοι ανίχνευσης απάτης διακρίνονται σε παραδοσιακές στατιστικές, μηχανικής μάθησης και υβριδικές προσεγγίσεις:

1. Παραδοσιακές στατιστικές μέθοδοι και συστήματα βασισμένα σε κανόνες (rule-based systems):

   Οι πρώτες εφαρμογές στηρίζονταν σε προκαθορισμένους κανόνες και όρια συναλλαγών (π.χ. συναλλαγές > X ευρώ, σε διαφορετικές γεωγραφικές τοποθεσίες). Αν και απλές και ερμηνεύσιμες, οι μέθοδοι αυτές δεν προσαρμόζονται σε νέα μοτίβα και παρουσιάζουν χαμηλή ευελιξία [182].

2. Supervised Machine Learning:

   Η πιο διαδεδομένη προσέγγιση βασίζεται σε εποπτευόμενη μάθηση με αλγορίθμους όπως Random Forests, Gradient Boosting, SVM, και Neural Networks [183]. Τα μοντέλα αυτά εκπαιδεύονται πάνω σε ιστορικά δεδομένα συναλλαγών για να προβλέψουν την πιθανότητα απάτης. Ωστόσο, απαιτούν μεγάλο όγκο ετικετοποιημένων δεδομένων, τα οποία είναι συχνά μη διαθέσιμα ή μη ισορροπημένα (class imbalance) [183]. Επίσης, η συγκέντρωση δεδομένων από πολλούς οργανισμούς σε έναν ενιαίο χώρο εκπαίδευσης εγείρει ζητήματα ιδιωτικότητας και κανονιστικής συμμόρφωσης (GDPR) [4][184].

3. Unsupervised και Semi-supervised Learning:

   Εναλλακτικά, χρησιμοποιούνται τεχνικές ανίχνευσης ανωμαλιών (anomaly detection) όπως οι Autoencoders, οι Isolation Forest ή τα One-Class SVMs για την αναγνώριση ύποπτων προτύπων χωρίς ανάγκη ετικετών [185]. Αν και αποδοτικές σε μη-ισορροπημένα δεδομένα, αυτές οι μέθοδοι συχνά παράγουν υψηλά ποσοστά ψευδών θετικών, ενώ δεν παρέχουν επαρκή ερμηνευσιμότητα των αποτελεσμάτων.

4. Graph-based Models και Network Learning:

   Πιο πρόσφατα, μοντέλα Graph Neural Networks (GNNs) έχουν χρησιμοποιηθεί για την ανάλυση δικτύων συναλλαγών, αξιοποιώντας σχέσεις μεταξύ πελατών και λογαριασμών [186]. Παρά τη βελτιωμένη ικανότητα εντοπισμού συνδυασμένων επιθέσεων, τα GNNs απαιτούν μεγάλη υπολογιστική ισχύ και πολύπλοκη προεπεξεργασία.

5. Federated Learning (FL):

   Τα τελευταία χρόνια, οργανισμοί έχουν στραφεί στην ομοσπονδιακή μάθηση, όπου κάθε φορέας εκπαιδεύει το μοντέλο του τοπικά και μοιράζεται μόνο τα βάρη για συγκεντρωτική συνάθροιση [187]. Αν και το FL μειώνει την ανάγκη μεταφοράς δεδομένων, εξακολουθεί να εξαρτάται από την εμπιστοσύνη μεταξύ των συμμετεχόντων και δεν προσφέρει πλήρη διαφάνεια στην εγκυρότητα των ενημερώσεων [187].

4.1.3 Περιορισμοί και ευπάθειες των υφιστάμενων λύσεων

Παρά τη σημαντική πρόοδο, οι παραπάνω προσεγγίσεις παρουσιάζουν κοινές αδυναμίες που καθιστούν δύσκολη την εφαρμογή τους σε πραγματικά τραπεζικά περιβάλλοντα μεγάλης κλίμακας:

- Έλλειψη προστασίας ιδιωτικότητας και ασφάλειας: Η ανάγκη συγκέντρωσης ή ανταλλαγής δεδομένων παραμένει βασικό πρόβλημα. Ακόμη και στο Federated Learning, επιθέσεις *model inversion* ή *membership inference* μπορούν να ανακατασκευάσουν στοιχεία χρηστών από τις τοπικές παραμέτρους [188].

- Απουσία μηχανισμών εμπιστοσύνης και επαλήθευσης: Τα υπάρχοντα FL συστήματα δεν διαθέτουν αξιόπιστο τρόπο ελέγχου της αυθεντικότητας των συμμετεχόντων. Κακόβουλοι κόμβοι μπορούν να αλλοιώσουν τα βάρη, οδηγώντας σε model poisoning [189].

- Έλλειψη διαφάνειας και auditability: Τα αποτελέσματα της εκπαίδευσης και οι ενημερώσεις του μοντέλου δεν καταγράφονται με τρόπο που να επιτρέπει πλήρη ιχνηλασιμότητα και εποπτεία από τρίτους φορείς [190].

- Περιορισμένη επεκτασιμότητα και αποδοτικότητα: Πολλά υπάρχοντα συστήματα είναι ενεργοβόρα ή μη επαρκώς κλιμακώσιμα, ειδικά όταν εμπλέκονται μεγάλα δίκτυα συνεργαζόμενων οργανισμών [189].

- Υπολογιστικοί περιορισμοί και πολυπλοκότητα δεδομένων: Οι σύγχρονες απάτες περιλαμβάνουν περίπλοκα, μη-γραμμικά και χρονικά εξαρτημένα πρότυπα, τα οποία οι κλασικοί αλγόριθμοι συχνά αδυνατούν να αναπαραστήσουν αποδοτικά [191].

Τα παραπάνω μειονεκτήματα αναδεικνύουν ένα κενό μεταξύ της θεωρητικής αποτελεσματικότητας και της πρακτικής εφαρμοσιμότητας των υπαρχουσών προσεγγίσεων. Η ανάγκη για μια ολοκληρωμένη, ασφαλή και επαληθεύσιμη αρχιτεκτονική που θα επιτρέπει την ανίχνευση απάτης με σεβασμό στην ιδιωτικότητα και με αυξημένη υπολογιστική αποδοτικότητα αποτελεί το επίκεντρο της ερευνητικής κατεύθυνσης της παρούσας εργασίας.

4.2 Ενοποίηση Quantum, Federated και Blockchain Τεχνολογιών

Όπως αναλύθηκε στην προηγούμενη ενότητα, οι υπάρχουσες προσεγγίσεις στην ανίχνευση απάτης, αν και αποτελεσματικές σε συγκεκριμένα σενάρια, παρουσιάζουν σοβαρούς περιορισμούς όσον αφορά την ιδιωτικότητα των δεδομένων, τη διαφάνεια των διαδικασιών μάθησης και την υπολογιστική αποδοτικότητα. Οι αδυναμίες αυτές αναδεικνύουν την ανάγκη για μια νέα ενοποιημένη υπολογιστική αρχιτεκτονική, ικανή να συνδυάζει τις αρχές της αποκεντρωμένης εκπαίδευσης, της επαληθεύσιμης ασφάλειας, και της κβαντικής υπολογιστικής υπεροχής.

Η προτεινόμενη ερευνητική κατεύθυνση εδράζεται στην ενοποίηση τριών τεχνολογικών πυλώνων – του Federated Learning (FL), του Blockchain, και των Quantum Machine Learning (QML) τεχνικών – οι οποίοι από κοινού μπορούν να αντιμετωπίσουν τα υφιστάμενα κενά και να θεμελιώσουν ένα νέο πρότυπο ασφαλούς, επεκτάσιμης και ενεργειακά αποδοτικής ανίχνευσης απάτης.

4.2.1. Federated Learning ως πλαίσιο αποκεντρωμένης μάθησης

Το Federated Learning παραμένει η πιο ελκυστική προσέγγιση για περιβάλλοντα όπου τα δεδομένα δεν μπορούν να μετακινηθούν λόγω νομικών ή δεοντολογικών περιορισμών [10]. Κάθε οργανισμός (client) εκπαιδεύει τοπικά ένα μοντέλο στα δικά του δεδομένα, αποστέλλοντας μόνο τις ενημερωμένες παραμέτρους στον κεντρικό aggregator για συνάθροιση (π.χ. με το αλγόριθμο FedAvg). Ωστόσο, όπως επισημαίνουν οι Kairouz et al. (2021), η διαδικασία aggregation εισάγει κινδύνους data leakage και poisoning, ιδίως όταν δεν υπάρχει μηχανισμός επαλήθευσης των συμμετεχόντων [88].

Για τον λόγο αυτό, το FL αποτελεί τη βάση της αρχιτεκτονικής, αλλά ενισχύεται με μηχανισμούς ασφάλειας και διαφάνειας που παρέχονται από το blockchain. Ο στόχος δεν είναι να αντικατασταθεί το FL, αλλά να επεκταθεί με τεχνολογίες που εγγυώνται εμπιστοσύνη και ακεραιότητα στο αποκεντρωμένο περιβάλλον.

4.2.2 Blockchain ως μηχανισμός εμπιστοσύνης και επαλήθευσης

Η ενσωμάτωση της τεχνολογίας Blockchain στο Federated Learning προσφέρει ένα αποκεντρωμένο και αδιάβλητο μηχανισμό καταγραφής όλων των ενημερώσεων των μοντέλων [101]. Κάθε client, μετά την ολοκλήρωση της εκπαίδευσης, υποβάλλει τα κρυπτογραφημένα βάρη στο blockchain, όπου αποθηκεύονται ως συναλλαγές. Ένα έξυπνο συμβόλαιο (smart contract) ελέγχει αυτόματα την εγκυρότητα και τη συνέπεια των ενημερώσεων, απορρίπτοντας πιθανές ανωμαλίες [146].

Η συγκεκριμένη προσέγγιση επιτρέπει την πλήρη ιχνηλασιμότητα (auditability) όλων των διαδικασιών εκπαίδευσης, καθώς κάθε ενημέρωση ή αλλαγή καταγράφεται και μπορεί να ελεγχθεί εκ των υστέρων. Παράλληλα, διασφαλίζει την αμετάβλητη αποθήκευση των παγκόσμιων ενημερώσεων (global updates) στο blockchain, αποτρέποντας οποιαδήποτε αλλοίωση ή παραποίηση των αποτελεσμάτων. Επιπλέον, η αρχιτεκτονική αυτή οδηγεί σε αποκέντρωση της ευθύνης, καθώς καταργεί την εξάρτηση από έναν μοναδικό aggregator, μειώνοντας έτσι σημαντικά τον κίνδυνο συμβιβασμού ή μεροληψίας στη διαδικασία συνάθροισης.

Προηγούμενες έρευνες υποδεικνύουν ότι η ενσωμάτωση τεχνολογίας blockchain σε σχήματα Federated Learning (FL) αυξάνει τον βαθμό εμπιστοσύνης και διαφάνειας μεταξύ των συμμετεχόντων οργανισμών, καθώς η κατανεμημένη και αμετάβλητη φύση του blockchain ενισχύει την ακεραιότητα των μοντέλων και την ιχνηλασιμότητα των ενημερώσεων. Ωστόσο, ταυτόχρονα αυτή η προσέγγιση επιφέρει σημαντικές προκλήσεις: συγκεκριμένα, η εισαγωγή μηχανισμών συναίνεσης και κατανεμημένης καταγραφής φέρνει αυξημένα υπολογιστικά και ενεργειακά κόστη, αυξημένη καθυστέρηση (latency) στη μετάδοση των ενημερώσεων, και ενδεχόμενη επιβάρυνση των πόρων των κόμβων (clients) και των ενδιάμεσων φορέων (edge/server) [192] [193].

Οι σχετικές μελέτες επισημαίνουν ότι επειδή οι κόμβοι πρέπει να συμμετέχουν σε πρωτόκολλα blockchain τα οποία απαιτούν πρόσθετη επεξεργασία, επικοινωνία και αποθήκευση, η συνολική ενεργειακή κατανάλωση του συστήματος αυξάνεται σημαντικά [194].

Το ζήτημα αυτό καθιστά αναγκαία την αναζήτηση νέων υπολογιστικών παραδειγμάτων που θα μπορούν να υποστηρίξουν τέτοια αποκεντρωμένα συστήματα με μειωμένο ενεργειακό κόστος και αυξημένη υπολογιστική απόδοση – κάτι που οδηγεί φυσικά προς την κβαντική υπολογιστική.

4.2.3. Quantum Machine Learning ως καταλύτης αποδοτικότητας

Η εισαγωγή του Quantum Machine Learning (QML) στο προτεινόμενο πλαίσιο λειτουργεί ως καταλύτης αποδοτικότητας και αξιοπιστίας, αντιμετωπίζοντας ορισμένους από τους βασικούς περιορισμούς που χαρακτηρίζουν τις υφιστάμενες μεθόδους. Το QML αξιοποιεί τη θεμελιώδη κβαντική υπέρθεση και τη διεμπλοκή για να προσφέρει υπολογιστική υπεροχή στην ανάλυση πολύπλοκων και μη-γραμμικών προτύπων, τα οποία οι κλασικοί αλγόριθμοι δυσκολεύονται να αποτυπώσουν [127].

Στο πλαίσιο της προτεινόμενης αρχιτεκτονικής, το Υβριδικό Κβαντικό Νευρωνικό Δίκτυο (Hybrid Quantum Neural Network – HQNN) ενσωματώνει το κβαντικό επίπεδο ως ενδιάμεσο στάδιο επεξεργασίας, επιτρέποντας στο σύστημα να λειτουργεί σε έναν εκτεταμένο χώρο αναπαράστασης. Έτσι, βελτιώνεται σημαντικά η ικανότητα γενίκευσης, η ανίχνευση μη προφανών προτύπων απάτης και η ανθεκτικότητα του μοντέλου σε ακραίες ή θορυβώδεις εισόδους [167].

Παράλληλα, το QML συμβάλλει στην αποδοτικότητα και επεκτασιμότητα του συστήματος. Τα κβαντικά κυκλώματα έχουν τη δυνατότητα να εκτελούν πράξεις σε χώρους εκθετικών διαστάσεων με πολυωνυμικό αριθμό λειτουργιών, μειώνοντας δραστικά τον υπολογιστικό φόρτο σε προβλήματα μεγάλης κλίμακας [165]. Με αυτόν τον τρόπο, μπορούν να ενσωματωθούν σε ομοσπονδιακές αρχιτεκτονικές (Federated Learning) χωρίς να απαιτείται ανταλλαγή ή αποκάλυψη δεδομένων, ενισχύοντας την ιδιωτικότητα και ασφάλεια.

Επιπλέον, η κβαντική φύση του συστήματος επιτρέπει την εισαγωγή μηχανισμών εμπιστοσύνης και επαλήθευσης μέσω πρωτοκόλλων που αξιοποιούν QKD ή quantum-secure authentication, συμβάλλοντας έτσι στη μείωση των κινδύνων model poisoning και μη εξουσιοδοτημένων παρεμβάσεων .

Τέλος, σε επίπεδο ενεργειακής και υπολογιστικής αποδοτικότητας, η κβαντική παράλληλη επεξεργασία μπορεί να μειώσει τον χρόνο εκπαίδευσης και κατανάλωσης πόρων, ιδιαίτερα σε δίκτυα συνεργαζόμενων οργανισμών όπου απαιτείται συνεχής ενημέρωση μοντέλων [167].

Συνολικά, το QML δεν αποτελεί απλώς μια καινοτόμα υπολογιστική τεχνική, αλλά έναν μηχανισμό ενίσχυσης της ασφάλειας, της επεκτασιμότητας και της αποδοτικότητας των σύγχρονων συστημάτων ανίχνευσης απάτης, ανοίγοντας τον δρόμο για πιο ανθεκτικά και διαφανή χρηματοοικονομικά δίκτυα.

4.2.4 Η ανάγκη για ενοποίηση

Η σύγκλιση των τριών αυτών τεχνολογιών δεν αποτελεί τυχαία επιλογή, αλλά λογική εξέλιξη των ερευνητικών αναγκών που ανέδειξε η προηγούμενη βιβλιογραφία. Το Federated Learning εξασφαλίζει την ιδιωτικότητα των δεδομένων και επιτρέπει την αποκεντρωμένη εκπαίδευση των μοντέλων χωρίς τη μεταφορά ευαίσθητων πληροφοριών. Το Blockchain προσθέτει επίπεδα διαφάνειας, επαληθευσιμότητας και αμεταβλητότητας στις διαδικασίες εκπαίδευσης και ενημέρωσης των μοντέλων, ενώ η Quantum Machine Learning προσφέρει υπολογιστική υπεροχή και αυξημένη αποδοτικότητα στην επίλυση προβλημάτων μεγάλης πολυπλοκότητας [165-167]. Η ενοποίησή τους στο ίδιο πλαίσιο στοχεύει στη δημιουργία ενός ολιστικού και ανθεκτικού συστήματος, ικανού να

υπερβεί τους περιορισμούς των επιμέρους προσεγγίσεων, ενισχύοντας την εμπιστοσύνη μεταξύ των συμμετεχόντων κόμβων, μειώνοντας το ενεργειακό αποτύπωμα μέσω κβαντικών υπολογισμών και διασφαλίζοντας πλήρη ιχνηλασιμότητα και διαφάνεια μέσω των καταγραφών στο blockchain.

Η παρούσα εργασία βασίζεται στην υπόθεση ότι ο συνδυασμός αυτών των τριών τεχνολογιών μπορεί να οδηγήσει σε ένα νέο υπόδειγμα ασφαλούς, αποκεντρωμένης και αποδοτικής μάθησης, το οποίο θα παρουσιαστεί αναλυτικά στην επόμενη ενότητα, όπου περιγράφεται η συνολική αρχιτεκτονική και ροή του προτεινόμενου συστήματος.

4.3 Αρχιτεκτονικό Διάγραμμα Λύσης

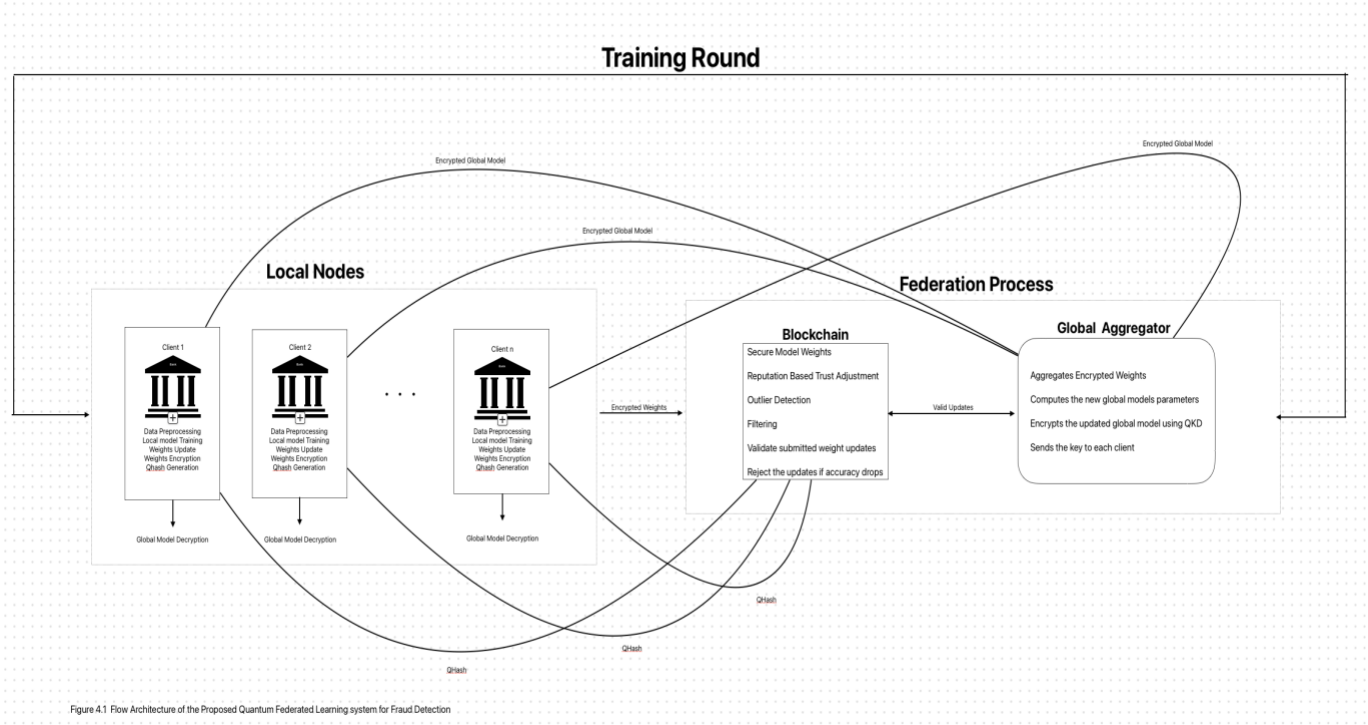


Figure 4.1 Flow Architecture of the Proposed Quantum Federated Learning system for Fraud Detection

Εικόνα 9 Σχήμα 8.4.1: Αρχιτεκτονική της λύσης σε γενικευμένη μορφή όπου να φαίνονται τόσο οι τοπικοί clients όσο και οι αλληλεπιδράσεις μεταξύ τους

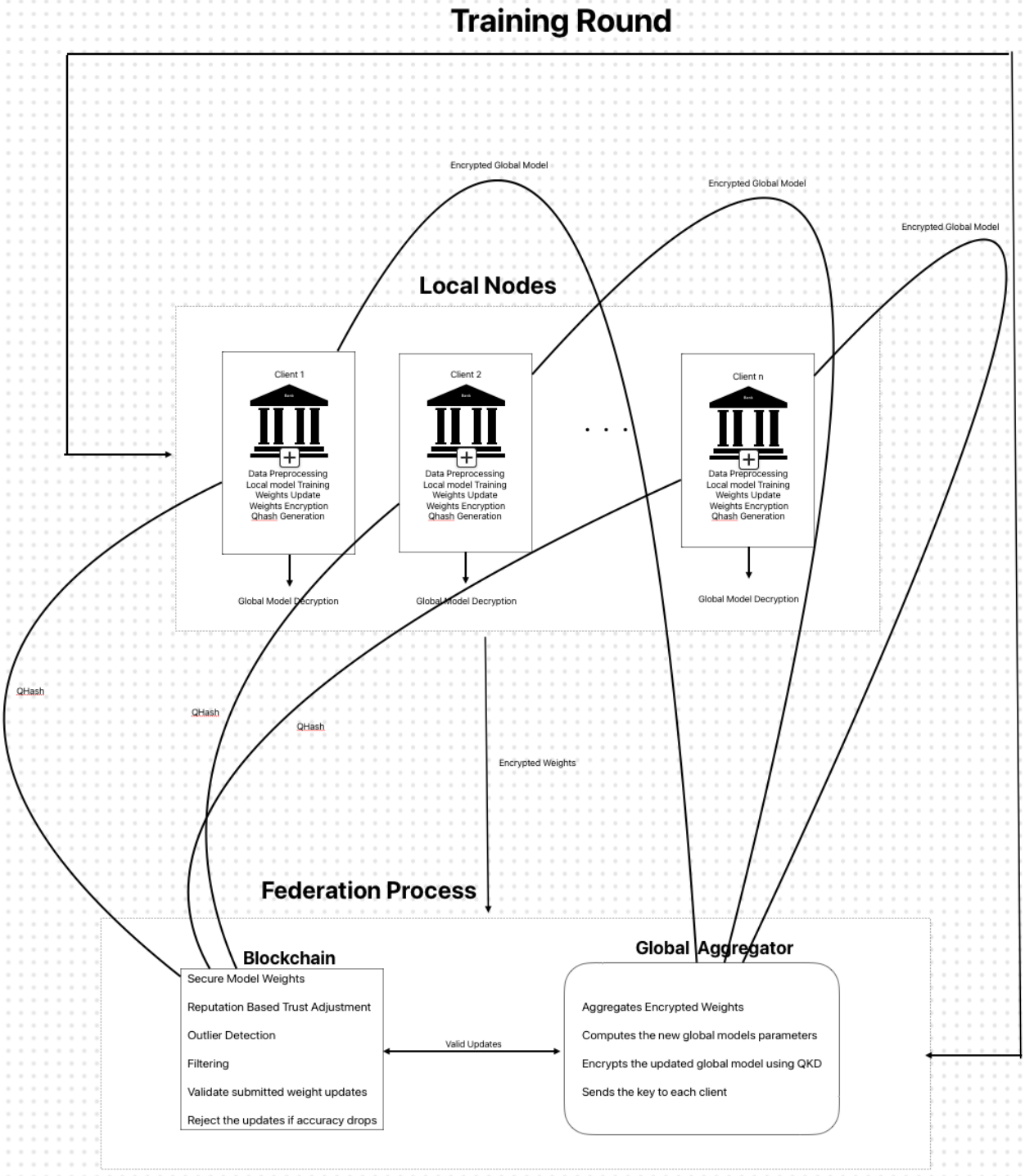


Figure 4.1 Flow Architecture of the Proposed Quantum Federated Learning system for Fraud Detection

4.4 Περιγραφή Λειτουργικών Ενοτήτων

Η προτεινόμενη αρχιτεκτονική για την ανίχνευση απάτης βασίζεται σε ένα πολυεπίπεδο σύστημα που συνδυάζει τεχνικές Quantum Machine Learning, Federated Learning και Blockchain, διασφαλίζοντας ταυτόχρονα ιδιωτικότητα, επαληθευσιμότητα και αξιοπιστία στα αποκεντρωμένα μοντέλα μάθησης. Το διάγραμμα ροής του συστήματος (Σχήμα 8.4.1) απεικονίζει συνολικά τη λειτουργία του προτεινόμενου πλαισίου, παρουσιάζοντας τις κύριες λειτουργικές ενότητες — τους τοπικούς κόμβους (Local Nodes), το Blockchain και τον Global Aggregator — καθώς και τη ροή των δεδομένων κατά τη διάρκεια ενός Training Round.

4.4.1 Ενότητα Τοπικής Εκπαίδευσης (Client Layer)

Όπως φαίνεται στο αριστερό τμήμα της εικόνας 9 (Σχήμα 8.4.1), κάθε τραπεζικός κόμβος (Client) διαθέτει τοπικά τα δικά του δεδομένα συναλλαγών, τα οποία παραμένουν απομονωμένα, εξασφαλίζοντας ιδιωτικότητα και συμμόρφωση με το GDPR. Στο πλαίσιο αυτό, η εκπαίδευση πραγματοποιείται αποκεντρωμένα, με κάθε κόμβο να διαχειρίζεται και να εκπαιδεύει το δικό του υβριδικό μοντέλο, χωρίς την ανάγκη μεταφοράς ευαίσθητων δεδομένων.

Η διαδικασία τοπικής εκπαίδευσης στηρίζεται στη χρήση Quantum Machine Learning (QML), το οποίο ενισχύει την υπολογιστική αποδοτικότητα και την εκφραστικότητα των τοπικών μοντέλων. Κάθε κόμβος εκπαιδεύει ένα Υβριδικό Κβαντικό Νευρωνικό Δίκτυο (Hybrid Quantum Neural Network – HQNN), όπου το κβαντικό επίπεδο (Quantum Layer) λειτουργεί ως σημείο μάθησης υψηλής διάστασης. Εκεί, μέσω Variational Quantum Circuits (VQCs), τα δεδομένα προβάλλονται σε έναν πιο εκφραστικό χώρο, επιτρέποντας την ανίχνευση περίπλοκων και μη γραμμικών προτύπων απάτης που τα κλασικά δίκτυα δυσκολεύονται να αποτυπώσουν.

Η εκπαίδευση πραγματοποιείται τοπικά και αυτόνομα σε κάθε κόμβο, ακολουθώντας μια επαναλαμβανόμενη διαδικασία:

1. Προεπεξεργασία δεδομένων: καθαρισμός, κανονικοποίηση και προσαρμογή των χαρακτηριστικών στις απαιτήσεις του κβαντικού υποσυστήματος.
2. Κβαντική κωδικοποίηση (Angle Embedding): οι κλασικές τιμές των δεδομένων μετατρέπονται σε γωνίες περιστροφής πύλων (π.χ. RY ή RZ), επιτρέποντας την αναπαράσταση των χαρακτηριστικών ως κβαντικές καταστάσεις μέσα στο χώρο Hilbert. Το στάδιο αυτό αποτελεί το σημείο σύνδεσης μεταξύ του κλασικού και του κβαντικού μέρους του μοντέλου.
3. Δημιουργία και εκπαίδευση Quantum Layer (VQC): το κβαντικό επίπεδο υλοποιείται μέσω ενός Variational Quantum Circuit, το οποίο περιλαμβάνει παραμετρικές μοναδιαίες πύλες και entangling layers. Οι παράμετροι του κυκλώματος ενημερώνονται μέσω του κανόνα μετατόπισης παραμέτρου (parameter-shift rule).
4. Ενημέρωση βαρών: μετά από κάθε γύρο εκπαίδευσης, τα τοπικά βάρη προσαρμόζονται βάσει της συνάρτησης κόστους, ολοκληρώνοντας τον κύκλο του hybrid training loop.

Με τον τρόπο αυτό, κάθε κόμβος μαθαίνει από τα δικά του δεδομένα, αξιοποιώντας την κβαντική παράλληλη επεξεργασία για αυξημένη απόδοση και καλύτερη γενίκευση. Η ενότητα αυτή λειτουργεί ως το θεμέλιο της αποκεντρωμένης μάθησης, επιτρέποντας στο σύστημα να επωφεληθεί από την ισχύ του QML χωρίς να διακυβεύεται η ιδιωτικότητα ή η ασφάλεια των δεδομένων — στοιχεία που εξασφαλίζονται πλήρως στο επόμενο στάδιο μέσω κρυπτογράφησης και ελέγχου ακεραιότητας (QHash).

4.4.2 Ενότητα Blockchain Επαλήθευσης (Blockchain Validation Layer)

Στο κεντρικό τμήμα του Σχήματος 8.4.1, απεικονίζεται η λειτουργία του Blockchain Component, το οποίο λειτουργεί ως μηχανισμός επαλήθευσης και εμπιστοσύνης για το σύστημα.
Οι κρυπτογραφημένες ενημερώσεις (Encrypted Weights) και τα αντίστοιχα Qhashes τα οποία χρησιμοποιούνται ως μηχανισμός ελέγχου ακεραιότητας (integrity check) καταγράφονται στην αλυσίδα Ethereum Blockchain, όπου εκτελούνται smart contracts για την αξιολόγηση της εγκυρότητάς τους.

Η διαδικασία επαλήθευσης περιλαμβάνει:

- Secure Model Weights: ασφαλής αποθήκευση και καταγραφή των κρυπτογραφημένων βαρών.
- Reputation-Based Trust Adjustment: ενημέρωση του trust score κάθε κόμβου ανάλογα με τη συνέπεια και την αξιοπιστία του.
- Outlier Detection & Filtering: εντοπισμός και φιλτράρισμα μη φυσιολογικών ή κακόβουλων ενημερώσεων.
- Validation: αποδοχή μόνο των έγκυρων ενημερώσεων που βελτιώνουν την απόδοση του μοντέλου.
- Rejection: απόρριψη ενημερώσεων σε περίπτωση πτώσης της ακρίβειας (accuracy drop).

Το blockchain, επομένως, λειτουργεί ως αμετάβλητο και διαφανές αρχείο (immutable ledger) που εγγυάται την ακεραιότητα και την ιχνηλασιμότητα των ενημερώσεων, μειώνοντας τον κίνδυνο κακόβουλων επεμβάσεων.

4.4.3 Ενότητα Παγκόσμιου Συντονισμού (Global Aggregation Layer)

Στο δεξιό τμήμα του Σχήματος 8.4.1, παρουσιάζεται ο Global Aggregator, ο οποίος συντονίζει τη διαδικασία συνάθροισης των έγκυρων ενημερώσεων. Ο aggregator δεν έχει πρόσβαση στα μη κρυπτογραφημένα δεδομένα· πραγματοποιεί ομομορφική συνάθροιση (Homomorphic Aggregation) των επικυρωμένων βαρών που του αποστέλλει το blockchain, χωρίς να τα αποκρυπτογραφεί.

Η λειτουργία του περιλαμβάνει:

- Aggregation of Encrypted Weights: ομομορφική συνάθροιση των κρυπτογραφημένων ενημερώσεων.
- Global Model Computation: υπολογισμός των νέων παγκόσμιων παραμέτρων βάσει σταθμισμένων συνεισφορών.
- QKD Encryption: κρυπτογράφηση του ενημερωμένου global model με Quantum Key Distribution (QKD) κλειδιά.
- Redistribution: αποστολή του QKD-κρυπτογραφημένου παγκόσμιου μοντέλου πίσω στους clients.

Η ενότητα αυτή διασφαλίζει ότι η συνάθροιση πραγματοποιείται με πλήρη προστασία ιδιωτικότητας, χωρίς καμία αποκάλυψη τοπικών πληροφοριών.

4.4.4 Ενότητα Επικοινωνίας και Διανομής Μοντέλου (Model Distribution Layer)

Το τελικό στάδιο του Σχήματος 8.4.1 αφορά τη διανομή του ενημερωμένου μοντέλου προς όλους τους clients.
Κάθε κόμβος λαμβάνει το QKD-κρυπτογραφημένο global model, το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του QKD key, και το ενσωματώνει στο τοπικό του περιβάλλον εκπαίδευσης.

Η διαδικασία αυτή σηματοδοτεί την έναρξη ενός νέου κύκλου federated circle, επιτρέποντας στο σύστημα να μαθαίνει συνεχώς από τα δεδομένα όλων των συμμετεχόντων χωρίς καμία παραβίαση ιδιωτικότητας.

4.4.5 Ενότητα Αξιολόγησης και Ανατροφοδότησης (Evaluation & Feedback Layer)

Τέλος, η συνολική αρχιτεκτονική περιλαμβάνει ένα στάδιο αξιολόγησης του παγκόσμιου μοντέλου, στο οποίο μετρώνται δείκτες απόδοσης όπως: Accuracy, Recall και F1-score.

Τα αποτελέσματα της αξιολόγησης καταγράφονται επίσης στο blockchain, επιτρέποντας έλεγχο και διαφάνεια της διαδικασίας. Αν διαπιστωθεί χαμηλή απόδοση ή ανωμαλία, ο aggregator ενεργοποιεί μηχανισμό αναπροσαρμογής βαρών ή επανεκπαίδευσης, διαμορφώνοντας έτσι ένα αυτοενισχυόμενο οικοσύστημα μάθησης.

Κεφάλαιο 5. Μεθοδολογία και Υλοποίηση

5.1 Ανάλυση και Προετοιμασία των Δεδομένων

5.1.1 Σύνολο Δεδομένων 1

Το πρώτο σύνολο δεδομένων αποτελείται από περίπου 6 εκατομμύρια εγγραφές με 11 χαρακτηριστικά (features). Τα χαρακτηριστικά αυτά περιλαμβάνουν ένα πλήρες σύνολο χρηματοοικονομικών μεταβλητών, όπως:

- step: χρονικό βήμα που υποδηλώνει τον αριθμό ωρών από την έναρξη του συνόλου δεδομένων, χρήσιμο για την παρακολούθηση της χρονικής εξέλιξης των συναλλαγών.
- type: τύπος συναλλαγής (π.χ. *CASH-IN*, *CASH-OUT*, *TRANSFER* κ.ά.).
- amount: το χρηματικό ποσό της συναλλαγής.
- nameOrig: μοναδικό αναγνωριστικό του αποστολέα της συναλλαγής.
- oldbalanceOrg / newbalanceOrig: υπόλοιπο του αποστολέα πριν και μετά τη συναλλαγή.
- nameDest: μοναδικό αναγνωριστικό του παραλήπτη.
- oldbalanceDest / newbalanceDest: υπόλοιπο του παραλήπτη πριν και μετά τη συναλλαγή.
- isFraud: δυαδική ετικέτα (1 = απάτη, 0 = νόμιμη συναλλαγή).

Το dataset μπορεί να βρεθεί στο παρακάτω link:

https://www.kaggle.com/datasets/ealaxi/paysim1

5.1.1.1 Ανάλυση Τύπων Συναλλαγών

Αρχικά, εξετάστηκε η κατανομή των κατηγοριών της στήλης *type*, προκειμένου να εντοπιστούν οι τύποι συναλλαγών που σχετίζονται περισσότερο με δόλιες δραστηριότητες. Η ανάλυση αποκάλυψε ότι τα περιστατικά απάτης εμφανίζονται αποκλειστικά σε συγκεκριμένους τύπους συναλλαγών, γεγονός που υποδηλώνει πως ο παράγοντας "είδος συναλλαγής" έχει καθοριστικό ρόλο στη συμπεριφορά του συστήματος. Πιο συγκεκριμένα, οι περιπτώσεις απάτης καταγράφηκαν μόνο στις κατηγορίες CASH_OUT και TRANSFER, κάτι που είναι απολύτως αναμενόμενο, καθώς και οι δύο συνεπάγονται εκροή κεφαλαίων και μεταφορά χρημάτων μεταξύ διαφορετικών λογαριασμών. Αυτή η διαδικασία είναι εκ φύσεως πιο ευάλωτη σε κακόβουλες ενέργειες, καθώς επιτρέπει τη γρήγορη απομάκρυνση ποσών από τον αρχικό λογαριασμό και τη δυσκολία εντοπισμού τους σε περίπτωση απάτης.

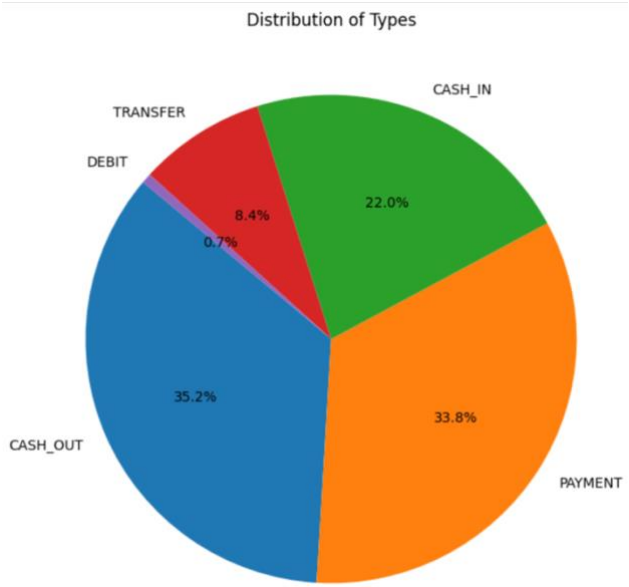
Αντίθετα, συναλλαγές όπως CASH_IN, PAYMENT ή DEBIT δεν συνδέονται άμεσα με παραβιάσεις, καθώς δεν περιλαμβάνουν μεταφορά χρημάτων από έναν λογαριασμό σε άλλον. Για παράδειγμα, οι συναλλαγές τύπου *CASH_IN* αντιπροσωπεύουν εισροές χρημάτων (π.χ. καταθέσεις), ενώ οι *PAYMENT* και *DEBIT* σχετίζονται με πληρωμές προς εμπόρους ή εσωτερικές χρεώσεις, όπου η πιθανότητα εκμετάλλευσης είναι σαφώς μικρότερη. Αυτοί οι τύποι συναλλαγών συνήθως ακολουθούν αυστηρά ελεγχόμενες διαδικασίες και δεν προσφέρουν τα ίδια περιθώρια παραποίησης.

Ως εκ τούτου, οι συναλλαγές με τύπο διαφορετικό από CASH_IN, PAYMENT ή DEBIT αφαιρέθηκαν από το αρχικό σύνολο δεδομένων. Η ενέργεια αυτή επέφερε σημαντική μείωση του όγκου και της πολυπλοκότητας των δεδομένων, διευκολύνοντας παράλληλα τη στοχευμένη ανάλυση στους τύπους συναλλαγών όπου πράγματι εντοπίζεται ο μεγαλύτερος κίνδυνος απάτης. Με αυτόν τον τρόπο, το μοντέλο εκπαιδεύεται σε ένα πιο καθαρό και αντιπροσωπευτικό υποσύνολο, εστιάζοντας αποκλειστικά στα σενάρια που παρουσιάζουν ουσιαστικό ενδιαφέρον για ανίχνευση δόλιων ενεργειών.

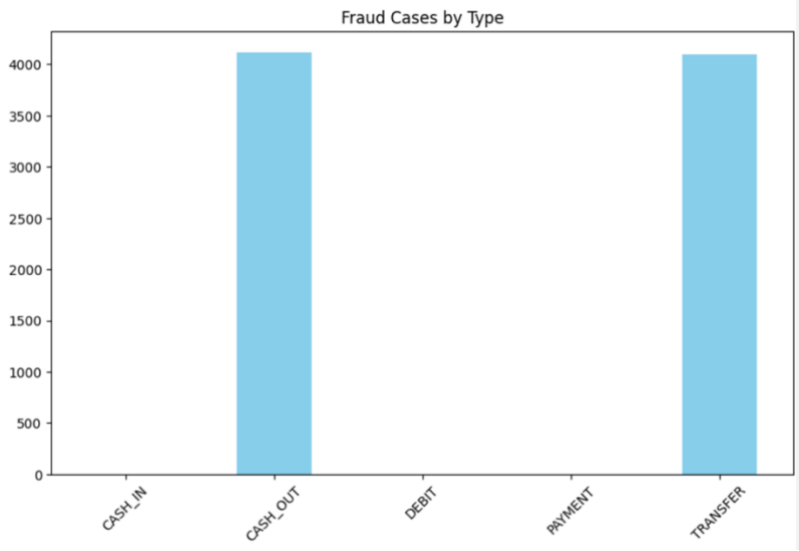
Αξίζει να σημειωθεί ότι αυτή η φάση φιλτραρίσματος συμβάλλει όχι μόνο στη βελτίωση της ακρίβειας του μοντέλου, αλλά και στη σταθερότητά του, καθώς περιορίζονται οι περιπτώσεις "ψευδώς θετικών"

προβλέψεων που θα μπορούσαν να προκύψουν από κατηγορίες συναλλαγών χωρίς πραγματική σύνδεση με απάτη.

Στο διάγραμμα της εικόνας 10 φαίνεται καθαρά η σχέση αυτή που αναλύσαμε προηγουμένως.



Εικόνα 10: Εδώ παρουσιάζεται η κατανομή (distribution) του αρχικού συνόλου δεδομένων ανά τύπο συναλλαγής, δείχνοντας τα ποσοστά συμμετοχής κάθε κατηγορίας (Cash-In, Cash-Out, Payment, Transfer, Debit).



Εικόνα 11 Εδώ παρουσιάζεται η κατανομή των περιστατικών απάτης (fraud cases) ανά τύπο συναλλαγής, όπου παρατηρείται ότι τα περισσότερα περιστατικά αφορούν τις κατηγορίες Cash-Out και Transfer.

5.1.1.2 Ανάλυση Ονομάτων (nameOrig και nameDest)

Στη συνέχεια, πραγματοποιήθηκε αναλυτική διερεύνηση των στηλών nameOrig και nameDest, οι οποίες αντιπροσωπεύουν τα αναγνωριστικά του αποστολέα και του παραλήπτη αντίστοιχα. Στόχος της ανάλυσης ήταν να εντοπιστούν πιθανά πρότυπα ή επαναλαμβανόμενα μοτίβα που θα μπορούσαν να συνδέονται με δόλιες συναλλαγές ή να επηρεάζουν τη μεταβλητή στόχο (*isFraud*).

Η αρχική επισκόπηση αποκάλυψε ότι:

- Όλες οι τιμές της nameDest ξεκινούν με το γράμμα M, ενώ καμία τιμή της nameOrig δεν ακολουθεί αυτό το πρότυπο.
- Μετά τον καθαρισμό των δεδομένων (διατήρηση μόνο των τύπων συναλλαγών *CASH_OUT* και *TRANSFER*), όλες οι εγγραφές και στις δύο στήλες ξεκινούν πλέον με το γράμμα C. Αυτό υποδηλώνει ότι, για τις συγκεκριμένες κατηγορίες συναλλαγών, το σύνολο δεδομένων έχει ήδη υποστεί προκαταρκτική τυποποίηση ως προς τη μορφή των ονομάτων.

Η περαιτέρω διερεύνηση των εγγραφών που ξεκινούν με το γράμμα C έδειξε ότι δεν υπάρχουν συχνές επαναλήψεις ονομάτων που να υποδηλώνουν συγκεκριμένα μοτίβα απάτης. Συγκεκριμένα:

- Στη στήλη nameOrig, η μέγιστη συχνότητα εμφάνισης ενός ίδιου ονόματος περιορίστηκε σε μόλις τρεις (3) εμφανίσεις μέσα σε έξι εκατομμύρια εγγραφές.
- Στη στήλη nameDest, η πιο συχνή τιμή ξεπερνά ελαφρώς τις εκατό (100) εμφανίσεις, χωρίς ωστόσο να παρατηρείται κάποια συγκέντρωση που θα μπορούσε να θεωρηθεί ύποπτη ή να σχετίζεται με συγκεκριμένο πρότυπο απάτης.

Η ανάλυση συσχέτισης (correlation analysis) που ακολούθησε επιβεβαίωσε ότι οι δύο αυτές στήλες δεν παρουσιάζουν στατιστικά σημαντική επίδραση στη μεταβλητή *isFraud*. Με άλλα λόγια, οι ταυτότητες αποστολέα και παραλήπτη δεν συνεισφέρουν ουσιαστικά στη διάκριση μεταξύ νόμιμων και δόλιων συναλλαγών, αφού δεν φέρουν πληροφορία που να σχετίζεται με την ύπαρξη ή όχι απάτης.

Κατόπιν αυτής της διαπίστωσης, κρίθηκε ότι οι στήλες nameOrig και nameDest δεν προσφέρουν χρήσιμη πληροφορία στο μοντέλο πρόβλεψης. Αντιθέτως, η διατήρησή τους θα μπορούσε να αυξήσει τον όγκο των δεδομένων χωρίς να συνεισφέρει στην ακρίβεια, ενώ ενδέχεται να εισαγάγει θόρυβο και να επιβαρύνει τον υπολογιστικό χρόνο. Για τον λόγο αυτό, οι στήλες αφαιρέθηκαν από το τελικό σύνολο δεδομένων πριν από τη φάση της προ επεξεργασίας.

Η ενέργεια αυτή εντάσσεται στο ευρύτερο στάδιο βελτιστοποίησης των χαρακτηριστικών (feature optimization), με στόχο τη μείωση της διάστασης και την απομάκρυνση μεταβλητών που δεν προσφέρουν διακριτική πληροφορία. Μετά την αφαίρεση των δύο στηλών, τα δεδομένα καθαρίστηκαν από περιττές πληροφορίες, μειώνοντας σημαντικά την πολυπλοκότητα και τον χρόνο επεξεργασίας. Παράλληλα, το τελικό dataset παρέμεινε πιο εστιασμένο στις ουσιαστικές παραμέτρους που επηρεάζουν την ανίχνευση απάτης, διατηρώντας έτσι υψηλή ποιότητα και αποδοτικότητα στη φάση εκπαίδευσης του μοντέλου.

	nameOrig	nameDest
C	6362620	4211125
M	0	2151495

Εικόνα 13 Η κατανομή για τα ονόματα πριν τον καθαρισμό της στήλης 'type'

	nameOrig	nameDest
C	2770409	2770409

Εικόνα 12 Η κατανομή για τα ονόματα μετά τον καθαρισμό της στήλης 'type'

5.1.1.3 Κλιμάκωση Χαρακτηριστικών (Feature Scaling)

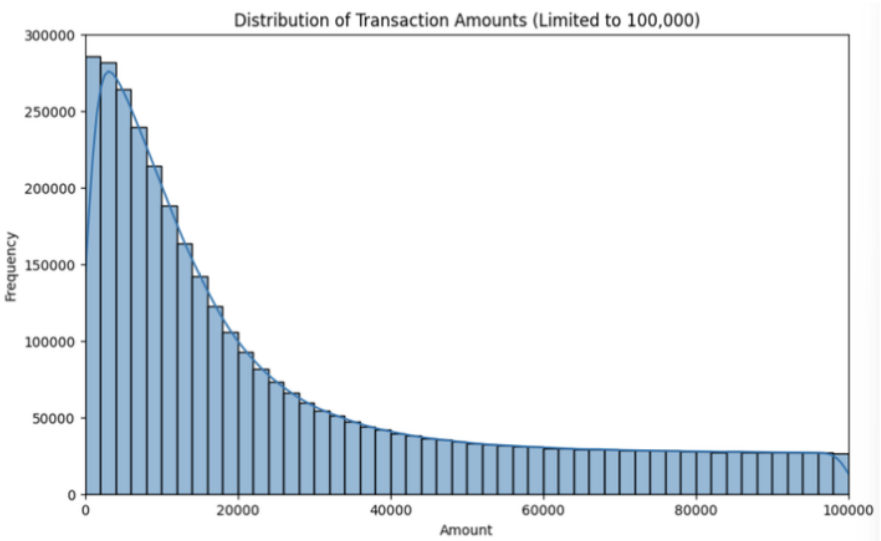
Λόγω των σημαντικών διαφορών στην κλίμακα των αριθμητικών γνωρισμάτων του συνόλου δεδομένων (π.χ. το χαρακτηριστικό *amount* μπορεί να λαμβάνει τιμές που φθάνουν έως και τις 100.000, ενώ άλλα γνωρίσματα κυμαίνονται σε πολύ μικρότερα εύρη), κρίθηκε απαραίτητη η εφαρμογή κανονικοποίησης (scaling) πριν από τη διαδικασία εκπαίδευσης των μοντέλων. Η κανονικοποίηση εξασφαλίζει ότι όλα τα χαρακτηριστικά ισότιμα στη μάθηση, αποτρέποντας την υπεροχή γνωρισμάτων με μεγάλες αριθμητικές τιμές έναντι άλλων με μικρότερη κλίμακα συνεισφέρουν. Αυτό είναι ιδιαίτερα κρίσιμο για αλγορίθμους που βασίζονται σε μετρικές αποστάσεων (π.χ. SVM, KNN) ή σε διαδικασίες βελτιστοποίησης gradient descent, όπου η διαφορά κλίμακας μπορεί να επηρεάσει σημαντικά τη σύγκλιση.

Στο πλαίσιο αυτό, δοκιμάστηκαν τρεις διαφορετικές τεχνικές κανονικοποίησης:

1. **Min–Max Scaling**: Μετασχηματίζει κάθε χαρακτηριστικό ώστε οι τιμές του να βρίσκονται εντός του εύρους [0, 1]. Η προσέγγιση αυτή είναι απλή και ιδιαίτερα χρήσιμη σε περιπτώσεις όπου η κατανομή των δεδομένων είναι σχετικά ομοιόμορφη, ωστόσο μπορεί να επηρεαστεί αρνητικά από ακραίες τιμές (outliers), καθώς αυτές συμπιέζουν το εύρος των υπόλοιπων τιμών.[195]
2. **Robust Scaling**: Βασίζεται στη χρήση της διαμέσου και του ενδοτεταρτημοριακού εύρους (IQR), καθιστώντας την τεχνική αυτή πιο ανθεκτική στην παρουσία ακραίων τιμών. Είναι ιδιαίτερα κατάλληλη όταν τα δεδομένα περιέχουν ανωμαλίες ή σημαντικές αποκλίσεις που ενδέχεται να παραμορφώσουν τη μέση τιμή και την τυπική απόκλιση. [196]
3. **Standard Scaling**: Μετασχηματίζει τα δεδομένα έτσι ώστε κάθε χαρακτηριστικό να έχει μέσο όρο ίσο με μηδέν και τυπική απόκλιση ίση με τη μονάδα. Με αυτόν τον τρόπο, οι τιμές των

γνωρισμάτων εκφράζονται σε μονάδες απόστασης από τον μέσο όρο, εξασφαλίζοντας ομοιογένεια κλίμακας και διευκολύνοντας την εκπαίδευση μοντέλων που προϋποθέτουν κανονική ή συμμετρική κατανομή χαρακτηριστικών. [195]

Ύστερα από πειραματική αξιολόγηση και συγκριτική ανάλυση της απόδοσης των μοντέλων υπό καθεμία από τις παραπάνω τεχνικές, επιλέχθηκε η **StandardScaler**. Η επιλογή αυτή δικαιολογείται από το γεγονός ότι προσφέρει σταθερότητα, δεν είναι υπερβολικά ευαίσθητη σε ακραίες τιμές, και αποδίδει εξαιρετικά σε ένα ευρύ φάσμα αλγορίθμων μηχανικής μάθησης, όπως Logistic Regression, Support Vector Machines και Neural Networks. Επιπλέον, η χρήση της ευνοεί την ταχύτερη και πιο ομαλή σύγκλιση κατά την εκπαίδευση, κάτι που παρατηρήθηκε εμπειρικά και στα συγκεκριμένα πειράματα.



Εικόνα 14 Η κατανομή για τις τιμές της στήλης 'amount'

5.1.1.4 Ανισορροπία Κλάσεων (Class Imbalance)

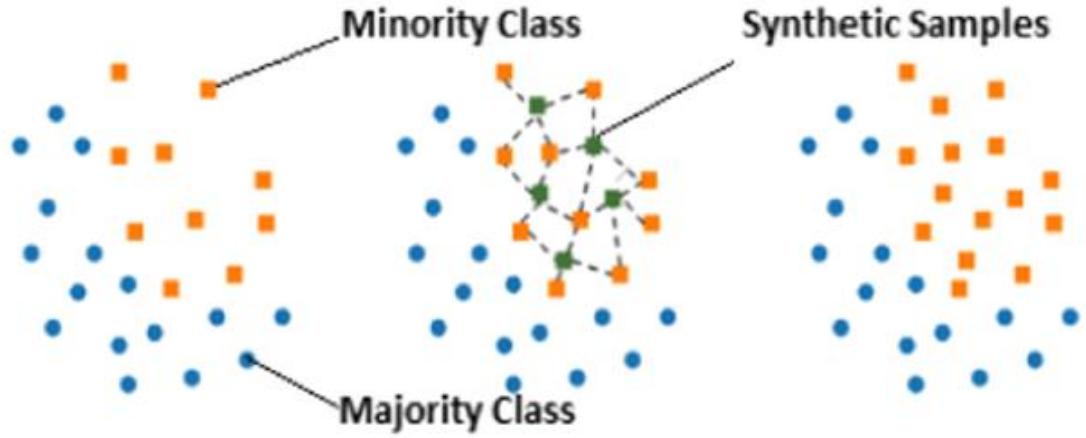
Ένα ακόμη κρίσιμο ζήτημα που προέκυψε κατά την ανάλυση των δεδομένων ήταν η έντονη ανισορροπία των κλάσεων, καθώς τα περιστατικά απάτης (*fraudulent transactions*) αντιστοιχούσαν σε ένα εξαιρετικά μικρό ποσοστό του συνολικού αριθμού συναλλαγών. Η κατάσταση αυτή αποτελεί ένα συνηθισμένο πρόβλημα στα συστήματα ανίχνευσης απάτης, όπου τα δεδομένα της πλειοψηφικής κατηγορίας (νόμιμες συναλλαγές) υπερισχύουν κατά πολύ εκείνων της μειοψηφικής (απάτες). Η ανισορροπία αυτή οδηγεί συχνά τα μοντέλα μηχανικής μάθησης να "μαθαίνουν" να προβλέπουν σχεδόν αποκλειστικά την πλειοψηφική κατηγορία, επιτυγχάνοντας υψηλή συνολική ακρίβεια αλλά χαμηλή ικανότητα εντοπισμού των πραγματικών περιπτώσεων απάτης — δηλαδή χαμηλή ευαισθησία (recall).

Για την αντιμετώπιση του φαινομένου αυτού εφαρμόστηκε η μέθοδος SMOTE (Synthetic Minority Oversampling Technique) έχει καθιερωθεί ως μία από τις πιο αποτελεσματικές τεχνικές υπερδειγματοληψίας για ανισόρροπα σύνολα δεδομένων [197]. Η μέθοδος SMOTE δημιουργεί τεχνητά (συνθετικά) δείγματα της μειοψηφικής κατηγορίας μέσω παρεμβολής μεταξύ υπαρχόντων δειγμάτων. Συγκεκριμένα, για κάθε δείγμα της κατηγορίας *fraud*, εντοπίζονται οι *k* πλησιέστεροι γείτονες (k-nearest neighbors) με βάση την ευκλείδεια απόσταση στον χώρο των χαρακτηριστικών, και δημιουργούνται νέα σημεία σε ενδιάμεσες θέσεις μεταξύ του αρχικού δείγματος και ενός τυχαία επιλεγμένου γείτονα [197]. Με αυτόν τον τρόπο, η μέθοδος δεν περιορίζεται στην απλή αντιγραφή υπαρχουσών εγγραφών — όπως συμβαίνει στην κλασική υπερδειγματοληψία — αλλά δημιουργεί

νέα, ρεαλιστικά και διαφοροποιημένα δείγματα, τα οποία εμπλουτίζουν τη γεωμετρική δομή της μειοψηφικής κλάσης και συμβάλλουν σε πιο ισορροπημένη και αποτελεσματική εκπαίδευση του μοντέλου.

Η εφαρμογή της SMOTE βελτίωσε αισθητά την ισορροπία του συνόλου δεδομένων, επιτρέποντας στο μοντέλο να μάθει πιο αντιπροσωπευτικά μοτίβα των συναλλαγών απάτης και να ενισχύσει την ικανότητά του να εντοπίζει δόλιες περιπτώσεις χωρίς να υποπέσει σε υπερπροσαρμογή (*overfitting*). Επειδή η υπερβολική δημιουργία τεχνητών δειγμάτων μπορεί να αλλοιώσει τη στατιστική δομή των δεδομένων, χρησιμοποιήθηκε συντηρητικός βαθμός υπερδειγματοληψίας, ο οποίος επέτρεψε την επίτευξη μιας ισορροπίας μεταξύ των δύο κλάσεων, διατηρώντας ρεαλιστική αναλογία μεταξύ νόμιμων και δόλιων συναλλαγών

Επιπλέον, για την αποφυγή διαρροής πληροφορίας (data leakage), η μέθοδος εφαρμόστηκε αποκλειστικά στο training set, πριν τη διαδικασία εκπαίδευσης των μοντέλων. Συνολικά, η ενσωμάτωση της SMOTE στη διαδικασία προεπεξεργασίας των δεδομένων βελτίωσε σημαντικά τη γενίκευση και την ευαισθησία του συστήματος ανίχνευσης απάτης, προσφέροντας πιο αξιόπιστα και δίκαια αποτελέσματα.



Εικόνα 15 Ο μηχανισμός του αλγορίθμου SMOTE, όπου δημιουργούνται συνθετικά δείγματα για την ενίσχυση της μειονοτικής κλάσης και την εξισορρόπηση του συνόλου δεδομένων. [198]

5.1.2 Σύνολο Δεδομένων 2: Fraud Detection Bank Dataset 20K

Το συγκεκριμένο σύνολο δεδομένων αποτελείται από 111 χαρακτηριστικά και περίπου 20.000 εγγραφές, γεγονός που το καθιστά σημαντικά μικρότερο και ευκολότερο στην ανάλυση σε σύγκριση με το προηγούμενο. Το σύνολο δεδομένων μπορεί να βρεθεί και στο σύνδεσμο https://www.kaggle.com/datasets/volodymyrgavrysh/fraud-detection-bank-dataset-20k-records-binary/data

Η μειωμένη του πολυπλοκότητα οφείλεται κυρίως στο ότι προέρχεται από ανάλυση Κύριων Συνιστωσών (PCA) που εφαρμόστηκε σε τραπεζικές κινήσεις πραγματικού χρόνου, εξασφαλίζοντας την ακεραιότητα των δεδομένων ενώ παράλληλα διατηρούνται τα ουσιώδη μοτίβα.

Ένα αξιοσημείωτο πλεονέκτημα του συνόλου είναι η ενδογενής ισορροπία των κλάσεων, καθώς περίπου 1 στις 5 συναλλαγές είναι δόλια. Αυτή η ισορροπία αποτελεί σημαντικό πλεονέκτημα για την εκπαίδευση μοντέλων, μειώνοντας την ανάγκη για εκτεταμένες τεχνικές υπερδειγματοληψίας (oversampling).

Από πλευράς προεπεξεργασίας, το σύνολο δεδομένων είναι σχεδόν πλήρως έτοιμο για χρήση, καθώς έχουν ήδη εφαρμοστεί τα απαραίτητα βήματα καθαρισμού και κανονικοποίησης μέσω της μεθόδου Principal Component Analysis (PCA). Η PCA είναι μια τεχνική μείωσης διάστασης η οποία μετασχηματίζει το αρχικό σύνολο χαρακτηριστικών σε νέους άξονες (components) που εξηγούν το μεγαλύτερο μέρος της διακύμανσης των δεδομένων [199], ενώ παράλληλα μειώνει το θόρυβο και διευκολύνει την οπτικοποίηση και ταξινόμηση [200]. Το μόνο στάδιο που απαιτείται πλέον είναι η MinMax κανονικοποίηση (MinMax Scaling), η οποία εφαρμόζεται λόγω της στήλης «amount», όπου οι τιμές είναι δυσανάλογα μεγαλύτερες σε σχέση με τα υπόλοιπα χαρακτηριστικά και θα μπορούσαν να επηρεάσουν δυσμενώς τη διαδικασία εκπαίδευσης — ειδικά σε τεχνικές που είναι ευαίσθητες σε διαφορές κλίμακας.

Ωστόσο, το συγκεκριμένο σύνολο δεν χρησιμοποιήθηκε εκτενώς στην πορεία της εργασίας, καθώς η υψηλή αναλογία δόλιων συναλλαγών δεν αντικατοπτρίζει επαρκώς τις πραγματικές συνθήκες του τραπεζικού περιβάλλοντος, όπου τα περιστατικά απάτης είναι πολύ πιο σπάνια. Επιπλέον, παρατηρήθηκε ότι τα κλασικά μοντέλα μηχανικής μάθησης πετύχαιναν ήδη ιδιαιτέρως υψηλή ακρίβεια, πλησιάζοντας σχεδόν το άριστο αποτέλεσμα, γεγονός που περιορίζει το περιθώριο για ουσιαστική κβαντική επιτάχυνση ή βελτίωση μέσω υβριδικών κβαντικών μεθόδων.

5.2 Αρχιτεκτονική του Υβριδικού Κβαντικού Νευρωνικού Δικτύου.

Η αρχιτεκτονική που αναπτύχθηκε στηρίχθηκε στην ιδέα του υβριδικού κβαντικού νευρωνικού δικτύου (Hybrid Quantum Neural Network), δηλαδή ενός μοντέλου που συνδυάζει στοιχεία κλασικής και κβαντικής μάθησης. Με αυτόν τον τρόπο αξιοποιούνται τα πλεονεκτήματα και των δύο κόσμων: η σταθερότητα και η ωριμότητα των κλασικών αλγορίθμων, μαζί με τη δυνατότητα των κβαντικών κυκλωμάτων να αναπαριστούν πιο σύνθετες σχέσεις στα δεδομένα.

Στόχος της υλοποίησης ήταν η δημιουργία ενός μοντέλου ικανού να εντοπίζει περιπτώσεις απάτης μέσα σε τραπεζικές συναλλαγές, χρησιμοποιώντας ένα παραμετρικό κβαντικό κύκλωμα (Variational Quantum Circuit – VQC) ενσωματωμένο σε ένα νευρωνικό δίκτυο. Η βασική ιδέα είναι ότι το κβαντικό κύκλωμα λειτουργεί ως ένα "ενδιάμεσο επίπεδο" που μετασχηματίζει τις εισόδους σε έναν πιο εκφραστικό χώρο, πριν περάσουν στα τελικά στρώματα του δικτύου.

Η ανάπτυξη και εκπαίδευση του μοντέλου πραγματοποιήθηκε με τη χρήση της βιβλιοθήκης PennyLane της Python, η οποία παρέχει ολοκληρωμένα εργαλεία για τον σχεδιασμό παραμετρικών κβαντικών κυκλωμάτων και τη σύνδεσή τους με πλαίσια βαθιάς μάθησης όπως το Keras ή το PyTorch. Έτσι, το υβριδικό μοντέλο εκπαιδεύεται με κλασικούς optimizers (όπως ο *Adam*), ενώ οι παράμετροι του κβαντικού κυκλώματος ενημερώνονται μέσω της μεθόδου parameter-shift rule, η οποία χρησιμοποιείται για τον ακριβή υπολογισμό των κλίσεων (gradients) σε κβαντικά περιβάλλοντα.

5.2.1 Το Κβαντικό Επίπεδο (Quantum Layer)

Το κβαντικό επίπεδο που αναπτύχθηκε βασίστηκε στη δουλειά των [201], όπου το κύκλωμα αποτελείται από τέσσερα qubits και περιλαμβάνει δύο κύρια στάδια:

1. Angle Embedding:

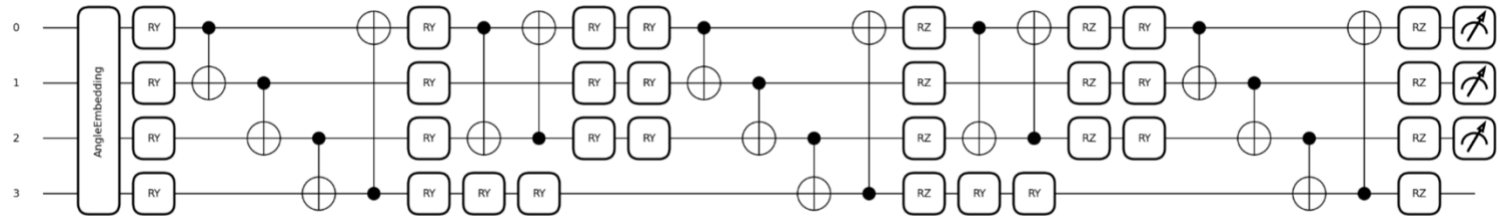
   Τα δεδομένα εισόδου μετατρέπονται σε κβαντικές καταστάσεις μέσω πυλών περιστροφής γύρω από τον άξονα Y (R_y). Κάθε αριθμητικό χαρακτηριστικό του διανύσματος εισόδου αντιστοιχεί σε μία γωνία περιστροφής, επιτρέποντας έτσι την ενσωμάτωση της πληροφορίας στην κατάσταση κάθε qubit.

2. Variational Ansatz:

   Μετά την κωδικοποίηση, εφαρμόζονται διαδοχικά στρώματα παραμετροποιημένων πυλών περιστροφής (R_y, R_z) και πυλών διεμπλοκής τύπου CNOT. Οι πύλες αυτές δημιουργούν entanglement μεταξύ των qubits, αυξάνοντας σημαντικά την εκφραστική ικανότητα του κυκλώματος και επιτρέποντας την αναπαράσταση πιο περίπλοκων μη γραμμικών συσχετίσεων.

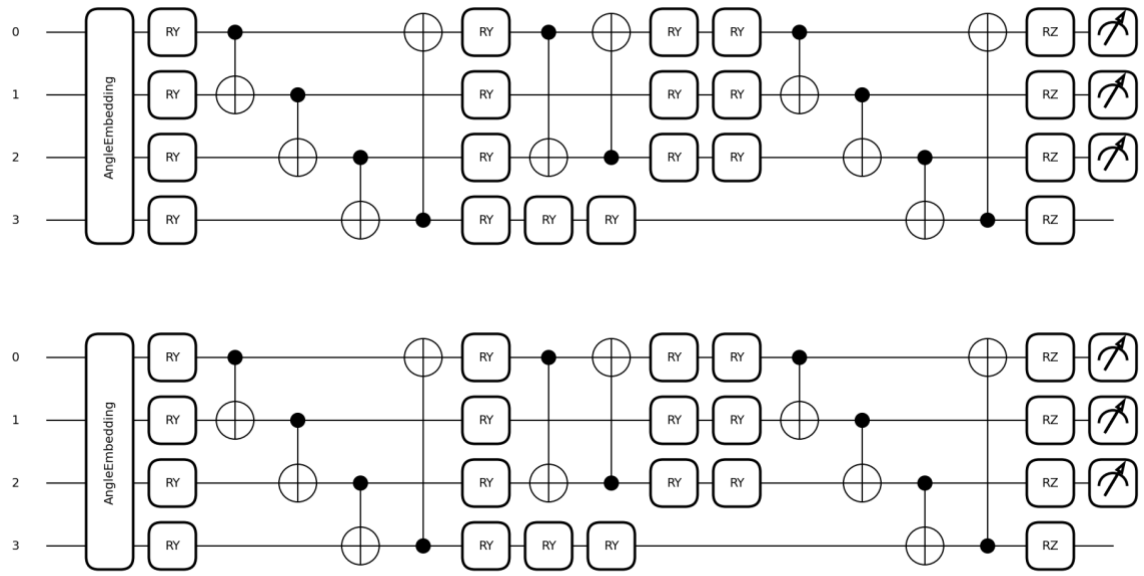
Η δομή αυτή, που απεικονίζεται στην Εικόνα 16, επιλέχθηκε έπειτα από εκτεταμένη πειραματική μελέτη διαφορετικών αρχιτεκτονικών *Variational Quantum Circuits (VQCs)*, όπως αυτές που προτάθηκαν από τους [202], [203]. Οι μελέτες αυτές ανέδειξαν τη σημασία της επιλογής βάθους κυκλώματος (*circuit depth*), της διάταξης των entangling layers και της παραμετροποίησης των πυλών περιστροφής για τη βελτίωση της απόδοσης και της σταθερότητας κατά τη διάρκεια της εκπαίδευσης.

Στην προτεινόμενη αρχιτεκτονική, παρατηρείται καθαρά η αλληλουχία μεταξύ των πυλών περιστροφής — παραμετροποιημένων μέσω της γωνίας θ — και των επιπέδων entanglement. Ο συνδυασμός αυτών των στοιχείων επιτρέπει στο κύκλωμα να εκμεταλλεύεται τις θεμελιώδεις κβαντικές ιδιότητες της υπέρθεσης και της διεμπλοκής για την αναπαράσταση πολύπλοκων προτύπων στα δεδομένα.



Εικόνα 16 Η αρχιτεκτονική του Κβαντικού Νευρωνικού Δικτύου που χρησιμοποιήθηκε στην έρευνα μας και βασίστηκε στην δουλειά των [201]

Στο σημείο αυτό να σημειώσουμε ότι χρησιμοποιήθηκε και ένα κβαντικό επίπεδο μικρότερου βάθους έτσι ώστε να μπορούμε να κρίνουμε κατά πόσο το βάθος του κβαντικού δικτύου επηρεάζει την τελική απόδοση. Στα πειραματικά αποτελέσματα μπορούμε να αποφανθούμε τις επιρροές οι οοίες έχουν να κάνουν σχετικά και με τον όγκο του αρχικού συνόλου δεδομένων.



5.2.2 Ενσωμάτωση στο Κλασικό Νευρωνικό Δίκτυο

Το κβαντικό επίπεδο ενσωματώθηκε μέσα σε ένα κλασικό νευρωνικό δίκτυο, σχηματίζοντας έτσι μια ολοκληρωμένη υβριδική αρχιτεκτονική τύπου “classical–quantum–classical”. Η συγκεκριμένη επιλογή δεν έγινε τυχαία, αλλά σχεδιάστηκε με βάση τόσο τις σημερινές τεχνολογικές δυνατότητες των κβαντικών υπολογιστών όσο και την ανάγκη αξιοποίησης των ώριμων μεθόδων της κλασικής μηχανικής μάθησης.

Στην αρχή του μοντέλου τοποθετήθηκε ένα Dense Layer, το οποίο λειτουργεί ως στάδιο προεπεξεργασίας και μείωσης των διαστάσεων. Ο ρόλος του είναι να μετασχηματίζει τα αρχικά χαρακτηριστικά των δεδομένων σε μια πιο συμπαγή αναπαράσταση, κατάλληλη για την είσοδο στο κβαντικό κύκλωμα. Έτσι, μειώνεται η πολυπλοκότητα των εισόδων, προσαρμόζοντάς τες στις φυσικές δυνατότητες των διαθέσιμων qubits.

Στη συνέχεια, τα δεδομένα διέρχονται από το Quantum Layer, το οποίο αναλαμβάνει να αποτυπώσει πιο περίπλοκες και μη γραμμικές σχέσεις ανάμεσα στα χαρακτηριστικά. Μέσα από τις παραμετρικές περιστροφές και τη χρήση entanglement, το κβαντικό επίπεδο μπορεί να «συμπτύξει» πληροφορία και να εκφράσει σχέσεις που δεν είναι εύκολα προσβάσιμες με καθαρά κλασικές μεθόδους. Τέλος, τα αποτελέσματα μεταφέρονται σε ένα Dense Layer με συνάρτηση ενεργοποίησης SoftMax, το οποίο παράγει τις πιθανότητες ταξινόμησης των συναλλαγών (fraud / non-fraud).

Η επιλογή να τοποθετηθεί το κβαντικό επίπεδο ανάμεσα σε δύο κλασικά επίπεδα εξυπηρετεί πολλαπλούς σκοπούς:

1. Εναρμόνιση με τις τρέχουσες τεχνολογικές δυνατότητες των NISQ συσκευών
   Οι σημερινοί κβαντικοί υπολογιστές, που ανήκουν στην εποχή των λεγόμενων *Noisy Intermediate-Scale Quantum (NISQ)* συστημάτων, διαθέτουν περιορισμένο αριθμό πρακτικών qubits και υποφέρουν από θόρυβο και σφάλματα decoherence. Η υβριδική προσέγγιση επιτρέπει τη χρήση μικρών και αποδοτικών κβαντικών κυκλωμάτων, ενσωματωμένων μέσα σε μεγαλύτερα κλασικά μοντέλα, αξιοποιώντας έτσι στο έπακρο τις σημερινές δυνατότητες του

διαθέσιμου hardware. Με αυτόν τον τρόπο, το μοντέλο παραμένει ρεαλιστικά υλοποιήσιμο και συμβατό με τις σύγχρονες πλατφόρμες προσομοίωσης και εκτέλεσης, όπως το *IBM Quantum* και το *Amazon Braket*.

2. Συνδυασμός ωριμότητας και εκφραστικότητας
   Τα κλασικά νευρωνικά δίκτυα είναι δοκιμασμένα, σταθερά και εξαιρετικά βελτιστοποιημένα από πλευράς εκπαίδευσης και βελτιστοποίησης. Αντίθετα, τα κβαντικά μοντέλα βρίσκονται ακόμη σε πειραματικό στάδιο και παρουσιάζουν περιορισμούς σε βάθος, αριθμό παραμέτρων και ευρωστία. Ο συνδυασμός των δύο επιτρέπει την αξιοποίηση των πλεονεκτημάτων των κλασικών μοντέλων (π.χ. γρήγορη σύγκλιση, σταθερή εκπαίδευση) μαζί με τη δυναμική του κβαντικού μέρους, το οποίο αυξάνει τη χωρητικότητα του δικτύου σε όρους αναπαράστασης μη γραμμικών συσχετίσεων.

3. Πειραματική αξιολόγηση της συνεισφοράς του κβαντικού επιπέδου
   Η τοποθέτηση του κβαντικού layer σε ενδιάμεση θέση επιτρέπει τη συγκριτική μελέτη της επίδρασής του. Αφαιρώντας το κβαντικό επίπεδο μπορούμε να μετρήσουμε άμεσα τη βελτίωση ή την υποβάθμιση της απόδοσης, απομονώνοντας τη συμβολή του κβαντικού υποσυστήματος. Με αυτόν τον τρόπο αξιολογείται πειραματικά αν και σε ποιο βαθμό η εισαγωγή κβαντικής επεξεργασίας βελτιώνει την ανίχνευση απάτης σε σχέση με ένα καθαρά κλασικό νευρωνικό δίκτυο.

Η εκπαίδευση του υβριδικού μοντέλου πραγματοποιήθηκε με ενιαίο μηχανισμό βελτιστοποίησης, ώστε τα βάρη όλων των επιπέδων κλασικών και κβαντικών να ενημερώνονται ταυτόχρονα. Το χαρακτηριστικό αυτό εξασφαλίζει ομαλή ροή πληροφορίας μεταξύ των δύο υποσυστημάτων και συμβάλλει σε σταθερή σύγκλιση της συνάρτησης κόστους. Η σύμπραξη αυτή του κλασικού και του κβαντικού μέρους καθιστά το μοντέλο ιδιαίτερα ευέλικτο και επεκτάσιμο, επιτρέποντας στο μέλλον την αντικατάσταση του προσομοιωτή με πραγματικό κβαντικό hardware χωρίς ανάγκη επανασχεδιασμού της αρχιτεκτονικής.

5.2.3 Συνολική Λειτουργία της Αρχιτεκτονικής Τοπικού Μοντέλου

Η λειτουργία του υβριδικού μοντέλου μπορεί να περιγραφεί βήμα προς βήμα μέσα από μια διαδοχική ροή επεξεργασίας, όπου κάθε στάδιο συμβάλλει με διαφορετικό τρόπο στη βελτίωση της μάθησης και της ακρίβειας πρόβλεψης.

1. Προεπεξεργασία δεδομένων:

   Αρχικά, τα δεδομένα υποβάλλονται σε διαδικασίες καθαρισμού, κανονικοποίησης και μείωσης διαστάσεων. Στόχος αυτού του σταδίου είναι να εξασφαλιστεί ότι όλα τα χαρακτηριστικά βρίσκονται στην ίδια αριθμητική κλίμακα και ότι δεν υπάρχουν μεταβλητές με δυσανάλογη επιρροή στην εκπαίδευση. Επιπλέον, η μείωση διαστάσεων βοηθά στην αποφυγή υπερπροσαρμογής και διευκολύνει την απεικόνιση των χαρακτηριστικών στο πεδίο των qubits. Το αποτέλεσμα αυτού του βήματος είναι ένα καθαρό και εξισορροπημένο σύνολο δεδομένων, έτοιμο να εισαχθεί στο νευρωνικό δίκτυο.

2. Κλασική επεξεργασία (Dense Layer):

   Στο επόμενο στάδιο, τα προεπεξεργασμένα δεδομένα περνούν από ένα κλασικό πυκνό στρώμα (Dense Layer), το οποίο δρα ως μηχανισμός εξαγωγής βασικών προτύπων και προσαρμογής των εισόδων στις απαιτήσεις του κβαντικού κυκλώματος. Η λειτουργία του στρώματος αυτού είναι ιδιαίτερα σημαντική, καθώς επιτρέπει την καλύτερη αντιστοίχιση της διάστασης των

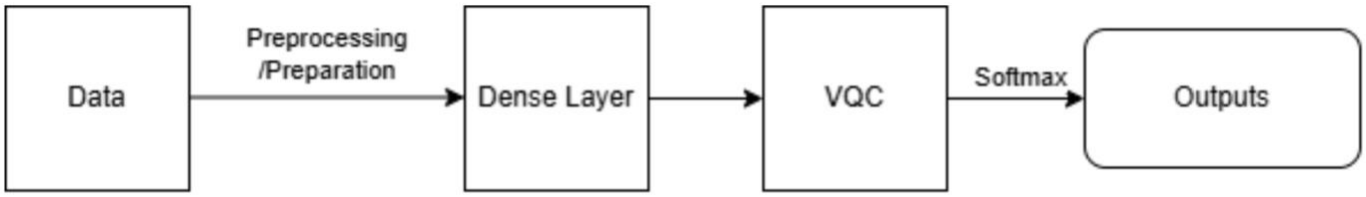
χαρακτηριστικών με τον αριθμό των qubits, κάνοντας έτσι δυνατή την αποδοτική ενσωμάτωση της πληροφορίας στο Quantum Layer. Παράλληλα, το Dense Layer λειτουργεί ως φίλτρο, περιορίζοντας τον θόρυβο και ενισχύοντας τις πιο ουσιαστικές συσχετίσεις των δεδομένων.

3. Κβαντική επεξεργασία (Quantum Layer):

   Στο στάδιο αυτό πραγματοποιείται η ουσιαστική «μεταφορά» της πληροφορίας στο κβαντικό επίπεδο. Τα δεδομένα κωδικοποιούνται σε γωνίες περιστροφής των qubits μέσω τεχνικών όπως το *angle embedding*, και στη συνέχεια το κύκλωμα εκτελεί μια σειρά από παραμετρικές περιστροφές και πύλες διεμπλοκής (entanglement). Αυτή η διαδικασία επιτρέπει στο μοντέλο να εξερευνήσει πολύπλοκες περιοχές του κβαντικού χώρου Hilbert, όπου οι σχέσεις μεταξύ των χαρακτηριστικών δεν είναι πλέον γραμμικές. Το entanglement επιτρέπει την από κοινού επεξεργασία πολλαπλών qubits, αυξάνοντας σημαντικά την εκφραστικότητα και τη δυνατότητα γενίκευσης του συστήματος.

4. Τελική κατηγοριοποίηση (Softmax Layer):

   Τα αποτελέσματα του κβαντικού υποσυστήματος τροφοδοτούνται σε ένα τελικό Dense Layer, το οποίο εφαρμόζει συνάρτηση ενεργοποίησης *Softmax* για να παραχθούν οι τελικές πιθανότητες ταξινόμησης. Η έξοδος αυτή αντιπροσωπεύει την εκτίμηση του μοντέλου σχετικά με το αν μια συναλλαγή είναι νόμιμη ή ύποπτη για απάτη. Το στάδιο αυτό συνδέει άμεσα την κβαντική επεξεργασία με τη μετρική αξιολόγηση και αποτελεί τη "γέφυρα" ανάμεσα στη θεωρητική λειτουργία του QNN και στη πρακτική αξιοποίησή του σε ένα ρεαλιστικό πρόβλημα ταξινόμησης.



Εικόνα 17 Αρχιτεκτονική υλοποίησης για το τοπικό μοντέλο του Υβριδικού Κβαντικού Δικτύου

Η συγκεκριμένη αρχιτεκτονική συνδυάζει την πρακτικότητα και την ωριμότητα των σύγχρονων κλασικών νευρωνικών δικτύων με τη θεωρητική ισχύ και την εκφραστικότητα της κβαντικής πληροφορικής. Με αυτόν τον τρόπο δημιουργείται ένα σύστημα που μπορεί να επωφεληθεί από τα πλεονεκτήματα και των δύο τεχνολογικών προσεγγίσεων:

- Από τη μία, το κλασικό τμήμα εξασφαλίζει σταθερή εκπαίδευση, καλή γενίκευση και χαμηλή υπολογιστική πολυπλοκότητα.
- Από την άλλη, το κβαντικό τμήμα προσφέρει έναν τρόπο αναπαράστασης της πληροφορίας σε ανώτερες διαστάσεις, επιτρέποντας τη σύλληψη πιο πολύπλοκων σχέσεων ανάμεσα στα δεδομένα.

Επιπλέον, η υβριδική αυτή δομή παρέχει έναν ρεαλιστικό και επεκτάσιμο τρόπο μελέτης της συμβολής των κβαντικών επιπέδων σε πραγματικά προβλήματα. Με τη δυνατότητα αφαίρεσης ή προσθήκης του Quantum Layer, μπορεί να αξιολογηθεί ποσοτικά η επίδρασή του στην τελική ακρίβεια και στη συμπεριφορά του μοντέλου.

Τέλος, ένα από τα σημαντικότερα πλεονεκτήματα της προσέγγισης αυτής είναι ότι διατηρεί συμβατότητα με τα σύγχρονα υπολογιστικά περιβάλλοντα. Η ίδια αρχιτεκτονική μπορεί να εκπαιδευτεί σε προσομοιωτές κβαντικών υπολογιστών (όπως ο *Pennylane Simulator*) αλλά και να μεταφερθεί στο μέλλον σε πραγματικές πλατφόρμες όπως το *IBM Quantum* ή το *Amazon Braket*, χωρίς αλλαγές στον κώδικα ή στη λογική λειτουργίας του συστήματος. Με αυτόν τον τρόπο, το μοντέλο λειτουργεί ως ένα βήμα σύνδεσης μεταξύ της σημερινής κλασικής υπολογιστικής πραγματικότητας και των μελλοντικών δυνατοτήτων του κβαντικού υπολογισμού.

5.3 Μέθοδοι Τοπικής Εκπαίδευσης

5.3.1 Μοντέλα προς Εκπαίδευση

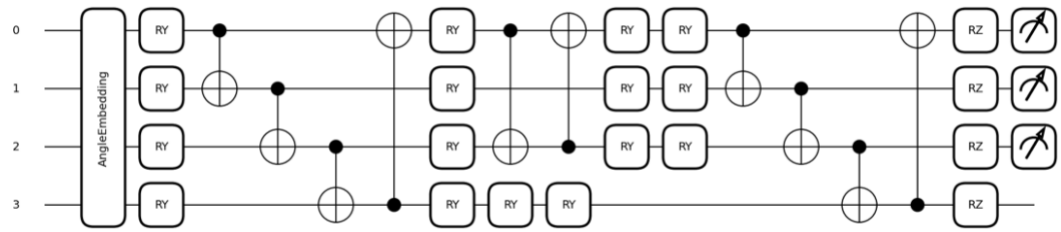
Έχοντας πλέον αναλύσει διεξοδικά την αρχιτεκτονική που χρησιμοποιήθηκε για τη δημιουργία του Κβαντικού Νευρωνικού Δικτύου, περνάμε στο επόμενο στάδιο της διαδικασίας: τη διεξαγωγή των πειραμάτων και την αξιολόγηση της απόδοσής του. Το στάδιο αυτό είναι καθοριστικής σημασίας, καθώς μας επιτρέπει να μετρήσουμε την πραγματική συνεισφορά του κβαντικού επιπέδου σε σχέση με ένα πλήρως κλασικό μοντέλο, αλλά και να διερευνήσουμε εάν η υβριδική προσέγγιση μπορεί να προσφέρει βελτίωση σε όρους γενίκευσης, ταχύτητας σύγκλισης ή ακρίβειας πρόβλεψης.

Η φιλοσοφία με την οποία σχεδιάστηκε το πειραματικό μέρος βασίστηκε σε μια λογική δύο σταδίων. Στο πρώτο στάδιο, στόχος ήταν η αξιολόγηση της ποιότητας του Υβριδικού Κβαντικού Νευρωνικού Δικτύου (Hybrid Quantum Neural Network – HQNN) σε τοπικό επίπεδο, δηλαδή χωρίς την διεμπλοκή ομοσπονδιακών μηχανισμών. Με αυτόν τον τρόπο μπορέσαμε να απομονώσουμε την επίδραση του κβαντικού επιπέδου και να μελετήσουμε καθαρά τη συνεισφορά του στη διαδικασία μάθησης. Στο δεύτερο στάδιο, το μοντέλο ενσωματώθηκε στην αρχιτεκτονική της Ομοσπονδιακής Μάθησης (Federated Learning), ώστε να εξεταστεί η συμπεριφορά του σε ένα κατανεμημένο περιβάλλον, πιο κοντά στις πραγματικές συνθήκες λειτουργίας του τραπεζικού σεναρίου που εξετάζουμε.

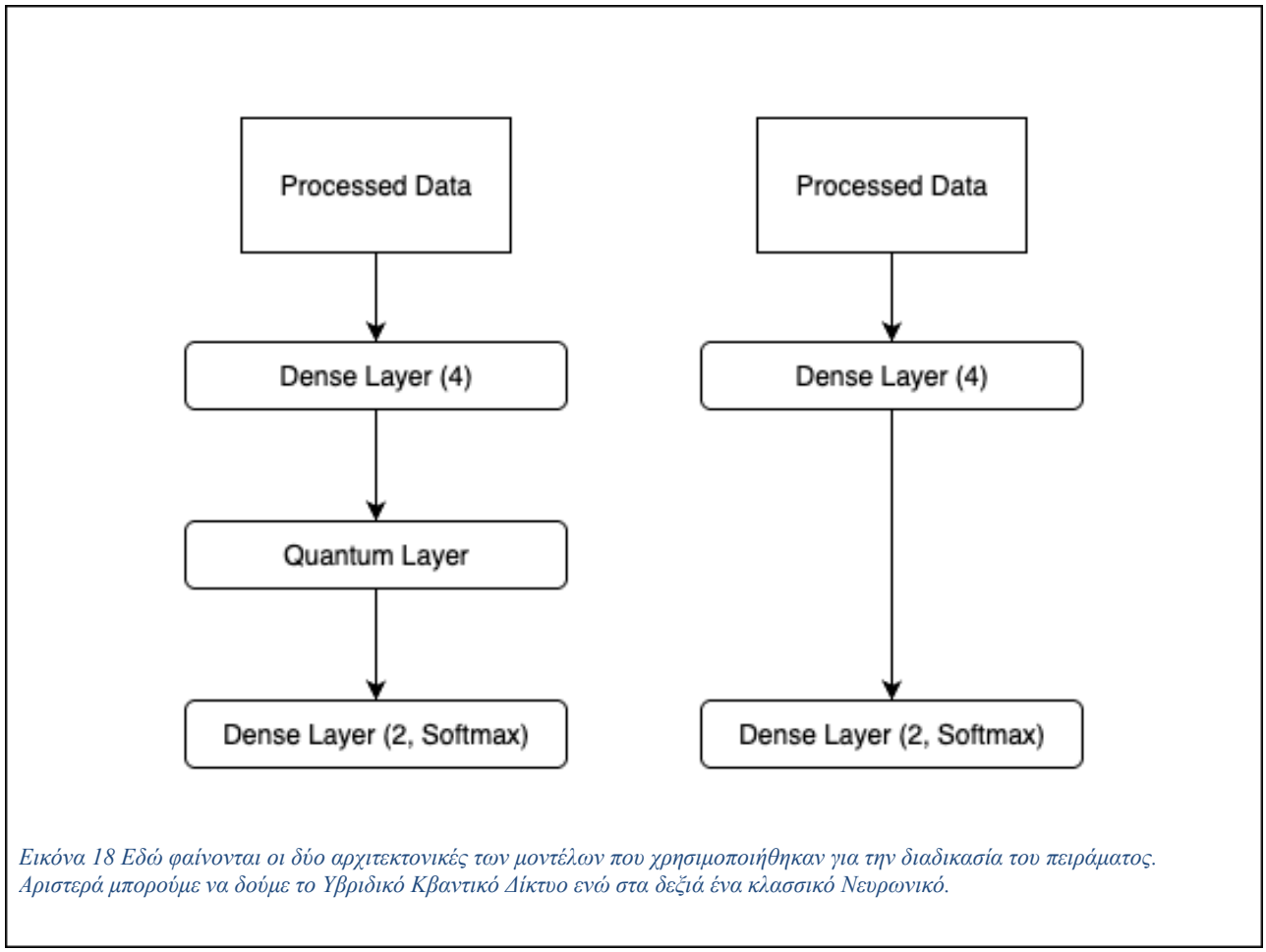
Για να επιτευχθεί μια δίκαιη και επιστημονικά τεκμηριωμένη σύγκριση, ακολουθήθηκε η εξής πειραματική τακτική:

- Εκπαίδευση ενός αμιγώς κλασικού μοντέλου, το οποίο λειτουργεί ως σημείο αναφοράς (baseline). Το μοντέλο αυτό βασίζεται αποκλειστικά σε πυκνά (Dense) επίπεδα και λειτουργεί ως αντιπροσωπευτικός εκπρόσωπος των σύγχρονων νευρωνικών δικτύων που χρησιμοποιούνται σε προβλήματα ταξινόμησης χρηματοοικονομικής απάτης.
- Εκπαίδευση του ίδιου μοντέλου με την προσθήκη ενός Κβαντικού Επιπέδου (Quantum Layer) στο ενδιάμεσο σημείο της αρχιτεκτονικής. Το επίπεδο αυτό περιλαμβάνει ένα Variational Quantum Circuit, όπου τα δεδομένα κωδικοποιούνται μέσω περιστροφικών πυλών (angle embedding) και εμπλέκονται μεταξύ τους μέσω πυλών CNOT, προκειμένου να επιτευχθεί entanglement. Η εισαγωγή του κβαντικού στρώματος επιτρέπει τη μελέτη του κατά πόσο η κβαντική επεξεργασία μπορεί να βελτιώσει την εκφραστικότητα και τη γενίκευση του μοντέλου, συγκριτικά με την καθαρά κλασική προσέγγιση.

Παράδειγμα ενός Quantum Layer:



Η παραπάνω διαδικασία μάς δίνει τη δυνατότητα να εξετάσουμε αν η ενσωμάτωση ενός κβαντικού επιπέδου προσφέρει ουσιαστική υπολογιστική αξία ή αν τα αποτελέσματα παραμένουν παρόμοια με αυτά του κλασικού δικτύου. Μέσα από αυτή τη συγκριτική ανάλυση, αναμένεται να εξαχθούν πολύτιμα συμπεράσματα για τη ρεαλιστική εφαρμοσιμότητα των υβριδικών κβαντικών μοντέλων σε πραγματικά χρηματοοικονομικά δεδομένα και να τεθούν οι βάσεις για την επόμενη φάση της έρευνας, δηλαδή την ολοκληρωμένη ομοσπονδιακή εκπαίδευσή του συστήματος.



Εικόνα 18 Εδώ φαίνονται οι δύο αρχιτεκτονικές των μοντέλων που χρησιμοποιήθηκαν για την διαδικασία του πειράματος. Αριστερά μπορούμε να δούμε το Υβριδικό Κβαντικό Δίκτυο ενώ στα δεξιά ένα κλασσικό Νευρωνικό.

Η παραπάνω εικόνα αποτυπώνει με σαφήνεια τη διαφορά ανάμεσα στα δύο πειραματικά μοντέλα που χρησιμοποιήθηκαν στη μελέτη.

Στο αριστερό διάγραμμα παρουσιάζεται το Υβριδικό Κβαντικό Νευρωνικό Δίκτυο (Hybrid Quantum Neural Network). Παρατηρούμε ότι, μετά το αρχικό Dense Layer (με 4 τελικούς νευρώνες), ακολουθεί ένα Quantum Layer, το οποίο αποτελεί το βασικό σημείο διαφοροποίησης από το κλασικό μοντέλο. Το κβαντικό επίπεδο αναλαμβάνει να επεξεργαστεί τα χαρακτηριστικά σε κβαντικό χώρο μέσω ενός Variational Quantum Circuit, πριν η πληροφορία περάσει στο τελικό Dense Layer με συνάρτηση ενεργοποίησης Softmax, που δίνει την έξοδο του συστήματος (2 κλάσεις).

Αντίθετα, στο δεξί διάγραμμα απεικονίζεται το καθαρά κλασικό νευρωνικό δίκτυο, το οποίο διατηρεί την ίδια βασική δομή αλλά χωρίς την παρεμβολή του κβαντικού επιπέδου. Εδώ, η ροή της πληροφορίας περνά απευθείας από το πρώτο Dense Layer (4) στο τελικό Dense Layer (2, Softmax), λειτουργώντας έτσι ως μοντέλο αναφοράς (baseline) για τη σύγκριση των επιδόσεων.

Με αυτό τον τρόπο, το σχήμα απεικονίζει ξεκάθαρα τη λογική του πειραματικού σχεδιασμού: την άμεση αντιπαραβολή του ίδιου δικτύου, με και χωρίς κβαντικό επίπεδο, προκειμένου να αξιολογηθεί η πραγματική συνεισφορά της κβαντικής επεξεργασίας στη διαδικασία μάθησης.

5.3.2 Παράμετροι Εκπαίδευσης

Όπως αναφέρθηκε στην προηγούμενη ενότητα, κατά τη φάση των πειραμάτων στόχος ήταν η διερεύνηση της συμπεριφοράς και της ποιότητας του Υβριδικού Κβαντικού Νευρωνικού Δικτύου υπό διαφορετικές αρχιτεκτονικές και παραμετροποιήσεις. Ιδιαίτερη έμφαση δόθηκε στην αξιολόγηση της επίδρασης του βάθους του κβαντικού κυκλώματος (circuit depth), καθώς αποτελεί κρίσιμο παράγοντα που επηρεάζει τόσο την εκφραστικότητα του μοντέλου όσο και τη σταθερότητα της εκπαίδευσης.

Συγκεκριμένα, χρησιμοποιήθηκαν δύο διακριτά είδη κβαντικών κυκλωμάτων, όπως περιγράφηκε στην προηγούμενη υποενότητα, τα οποία διαφοροποιούνται ως προς τη δομή και το πλήθος των entangling layers. Το πρώτο κύκλωμα ήταν ρηχό (shallow) με περιορισμένο αριθμό CNOT πυλών, ενώ το δεύτερο ήταν βαθύτερο (deep circuit), περιλαμβάνοντας διαδοχικά στρώματα περιστροφών R_y, R_z και πύλες διεμπλοκής. Η επιλογή αυτών των δύο παραλλαγών επέτρεψε την ανάλυση της σχέσης μεταξύ εκφραστικότητας και κινδύνου εμφάνισης barren plateaus, δηλαδή περιοχών στο χώρο παραμέτρων όπου τα gradients τείνουν στο μηδέν, καθιστώντας δύσκολη τη βελτιστοποίηση.

Η εκπαίδευση οργανώθηκε σε σαφώς καθορισμένες φάσεις, ονομαζόμενες Πειράματα (Experiments). Κάθε πείραμα αποτελούσε ένα πλήρες σύνολο εκτελέσεων του ίδιου μοντέλου με συγκεκριμένο συνδυασμό υπερπαραμέτρων και περιλάμβανε πέντε ανεξάρτητες επαναλήψεις (runs). Κάθε επανάληψη εκτελέστηκε για πέντε-δέκα εποχές (epochs), επαρκές πλήθος για την αποτύπωση της καμπύλης εκμάθησης και την παρατήρηση της σύγκλισης της συνάρτησης κόστους. Αυτή η διαδικασία πολλαπλών επαναλήψεων ενίσχυσε τη στατιστική αξιοπιστία των αποτελεσμάτων, μειώνοντας τον κίνδυνο επηρεασμού από στοχαστικά φαινόμενα των αρχικών βαρών ή των μετρήσεων των qubits.

Πέραν της δομής του κυκλώματος, εξετάστηκαν διαφορετικές τιμές υπερπαραμέτρων προκειμένου να εκτιμηθεί η ευαισθησία του μοντέλου ως προς τις συνθήκες εκπαίδευσης:

- Ποσοστό του τελικού dataset: Μεταβάλλοντας το ποσοστό του συνόλου εκπαίδευσης (π.χ. 10%, 30%, 100%), αξιολογήθηκε η επίδραση του όγκου των δεδομένων στη σταθερότητα της μάθησης και στη δυνατότητα γενίκευσης.
- Batch Size: Δοκιμάστηκαν διαφορετικά μεγέθη batch (64,128,256), ώστε να εντοπιστεί η βέλτιστη ισορροπία μεταξύ ταχύτητας εκπαίδευσης και ακρίβειας.
- Quantum backend: Χρησιμοποιήθηκε κυρίως το default.qubit αλλά έγιναν πειράματα και με την χρήση του default.mixed backends της βιβλιοθήκης Pennylane. Το πρώτο προσομοιώνει ένα ιδανικό (noise-free) περιβάλλον, ενώ το δεύτερο εισάγει φυσικό θόρυβο μέσω μοντέλων αποσυνοχής (decoherence), επιτρέποντας τη μελέτη της ανθεκτικότητας του μοντέλου σε ρεαλιστικές συνθήκες λειτουργίας ενός πραγματικού κβαντικού υπολογιστή.

Για την αναπροσαρμογή των παραμέτρων του δικτύου χρησιμοποιήθηκε ο Adam Optimizer με ρυθμό μάθησης (Learning Rate) ίσο με 0.01. Ο συγκεκριμένος αλγόριθμος επιλέχθηκε λόγω της ικανότητάς του να συνδυάζει την επιτάχυνση μέσω ορμής (momentum) με προσαρμοστική κλιμάκωση των gradients (adaptive learning rates), προσφέροντας σταθερή σύγκλιση ακόμα και σε μη ομαλές συναρτήσεις κόστους.

Ως συνάρτηση κόστους επιλέχθηκε η Cross-Entropy Loss όπως αναλύσαμε και στο κεφάλαιο 2, καθώς το πρόβλημα ταξινόμησης (fraud/non-fraud) απαιτεί τη σύγκριση προβλεπόμενων πιθανοτήτων έναντι πραγματικών ετικετών. Η συγκεκριμένη επιλογή εξασφαλίζει ομαλή εκπαίδευση, διακριτότητα μεταξύ κατηγοριών και καλύτερη απόκριση σε περιπτώσεις όπου το dataset εμφανίζει ανισορροπία κλάσεων (class imbalance).

Συνολικά, η πειραματική διαδικασία σχεδιάστηκε με στόχο τη συστηματική διερεύνηση της σχέσης μεταξύ πολυπλοκότητας του κυκλώματος, μεγέθους των δεδομένων, επιπέδων θορύβου και βελτιστοποίησης. Τα αποτελέσματα των δοκιμών αυτών — τα οποία παρουσιάζονται στις επόμενες υποενότητες — αποτελούν τη βάση για την αξιολόγηση της αποτελεσματικότητας της κβαντικής συνιστώσας και θέτουν τις προϋποθέσεις για τη μελλοντική ενσωμάτωσή της στο ομοσπονδιακό περιβάλλον μάθησης.

5.3.3 Διαμόρφωση των Πειραμάτων

Τα πειράματα υλοποιήθηκαν σε προγραμματιστικό περιβάλλον Python, αξιοποιώντας ένα σύνολο εξειδικευμένων βιβλιοθηκών που επιτρέπουν τη σύνδεση της κλασικής και της κβαντικής μάθησης. Πιο συγκεκριμένα, χρησιμοποιήθηκαν οι PennyLane, Keras και TensorFlow, οι οποίες αποτέλεσαν το βασικό πλαίσιο για τη δημιουργία, εκπαίδευση και αξιολόγηση των υβριδικών νευρωνικών δικτύων.

Η PennyLane χρησιμοποιήθηκε για την ανάπτυξη και προσομοίωση των κβαντικών επιπέδων (quantum layers), καθώς παρέχει ένα εύχρηστο περιβάλλον για τη δημιουργία Variational Quantum Circuits (VQCs) και τη σύνδεσή τους με κλασικούς υπολογιστικούς πυρήνες μέσω διεπαφών όπως το Keras interface. Από την άλλη πλευρά, οι Keras/TensorFlow χρησιμοποιήθηκαν για τη διαχείριση των κλασικών επιπέδων, της εκπαίδευσης και των διαδικασιών βελτιστοποίησης, καθιστώντας δυνατή τη συνεργασία μεταξύ των δύο υπολογιστικών παραδειγμάτων.

5.3.3.1 Δημιουργία Κβαντικού Δικτύου

Στα παρακάτω σημεία παρατίθεται ο κώδικας με τον οποίο υλοποιείται το κβαντικό νευρωνικό επίπεδο (Quantum Layer) στη γλώσσα της PennyLane, ενσωματωμένο στο συνολικό υβριδικό δίκτυο. Το επίπεδο αυτό αποτελεί τον πυρήνα της κβαντικής επεξεργασίας, όπου τα δεδομένα μετατρέπονται σε κβαντικές καταστάσεις, υποβάλλονται σε παραμετροποιημένες περιστροφές και entanglement, και τελικά μετρώνται για την εξαγωγή των χαρακτηριστικών.

Αξίζει να σημειωθεί ότι τα αρχεία και συναρτήσεις:

- custom_layer_long
- customer_layer

Τα επίπεδα αυτά αντιστοιχούν στα παραμετροποιημένα υπομοντέλα του κβαντικού νευρωνικού δικτύου. Αυτά περιλαμβάνουν διαφορετικές εκδοχές του κβαντικού κυκλώματος με μεταβαλλόμενο βάθος και αριθμό qubits, επιτρέποντας τον πειραματισμό με διάφορες αρχιτεκτονικές. Με τον τρόπο αυτό διερευνάται η επίδραση του βάθους, του αριθμού των entangling layers και του πλήθους των παραμέτρων στην τελική απόδοση του υβριδικού μοντέλου, τόσο σε επίπεδο ακρίβειας όσο και υπολογιστικής πολυπλοκότητας.

```
def custom_layer_long(weights, n_qubits):
    index = 0  # Start index for weights

    # First block of RY
    for i in range(n_qubits + 1):
        qml.RY(weights[index], wires=i)
        index += 1

    # First set of CNOT pairs
```

```
pairs = [(0, 1), (1, 2), (2, 3), (3, 0)]
for pair in pairs:
    qml.CNOT(wires=pair)

# Second block of RY
for i in range(n_qubits + 1):
    qml.RY(weights[index], wires=i)
    index += 1

# Second set of CNOT pairs
pairs = [(0, 2), (2, 0)]
for pair in pairs:
    qml.CNOT(wires=pair)

# Third block of RY (single qubit repeated)
qml.RY(weights[index], wires=3)
index += 1
qml.RY(weights[index], wires=3)
index += 1

# Nested loop of RY
for j in range(2):
    for i in range(n_qubits):
        qml.RY(weights[index], wires=i)
        index += 1

# Third set of CNOT pairs
pairs = [(0, 1), (1, 2), (2, 3), (3, 0)]
for pair in pairs:
    qml.CNOT(wires=pair)

# First block of RZ
for i in range(n_qubits + 1):
    qml.RZ(weights[index], wires=i)
    index += 1

# Fourth set of CNOT pairs
pairs = [(0, 2), (2, 0)]
for pair in pairs:
    qml.CNOT(wires=pair)
```

```
    # Fourth block of RY (single qubit repeated)
    qml.RY(weights[index], wires=3)
    index += 1
    qml.RY(weights[index], wires=3)
    index += 1

    # Second block of RZ
    for i in range(n_qubits):
        qml.RZ(weights[index], wires=i)
        index += 1

    # Third block of RY
    for i in range(n_qubits):
        qml.RY(weights[index], wires=i)
        index += 1

    # Fifth set of CNOT pairs
    pairs = [(0, 1), (1, 2), (2, 3), (3, 0)]
    for pair in pairs:
        qml.CNOT(wires=pair)

    # Final block of RZ
    for i in range(n_qubits + 1):
        qml.RZ(weights[index], wires=i)
        index += 1

    return index  # Total number of indices used
```

```
def custom_layer(weights, n_qubits):
    index = 0  # Initialize index to track unique weights

    # Apply first set of RY gates
    for i in range(n_qubits + 1):
        qml.RY(weights[index], wires=i)
        index += 1  # Increment index
```

```
    # Apply first set of CNOT gates
    pairs = [(0, 1), (1, 2), (2, 3), (3, 0)]
    for pair in pairs:
        qml.CNOT(wires=pair)

    # Apply second set of RY gates
    for i in range(n_qubits + 1):
        qml.RY(weights[index], wires=i)
        index += 1  # Increment index

    # Apply second set of CNOT gates
    pairs = [(0, 2), (2, 0)]
    for pair in pairs:
        qml.CNOT(wires=pair)

    # Apply RY gates on qubit 3
    qml.RY(weights[index], wires=3)
    index += 1  # Increment index
    qml.RY(weights[index], wires=3)
    index += 1  # Increment index

    # Apply nested RY gates for two layers
    for j in range(2):
        for i in range(n_qubits):
            qml.RY(weights[index], wires=i)
            index += 1  # Increment index

    # Apply third set of CNOT gates
    pairs = [(0, 1), (1, 2), (2, 3), (3, 0)]
    for pair in pairs:
        qml.CNOT(wires=pair)

    # Apply final set of RZ gates
    for i in range(n_qubits + 1):
        qml.RZ(weights[index], wires=i)
        index += 1  # Increment index
```

```
@qml.qnode(dev)
def qnode_long(inputs, weights):
```

```
    qml.AngleEmbedding(inputs, wires=range(n_qubits+1))
    for w in weights:
        custom_layer_long(w,n_qubits)
    outputs = [qml.expval(qml.PauliZ(wires=i)) for i in range(n_qubits)]
    return outputs
```

```
@qml.qnode(dev)
def qnode(inputs, weights):
    qml.AngleEmbedding(inputs, wires=range(n_qubits+1))
    for w in weights:
        custom_layer(w,n_qubits)
    outputs = [qml.expval(qml.PauliZ(wires=i)) for i in range(n_qubits)]
    return outputs
```

5.3.3.2 Ορισμός και Επιλογή της Κβαντικής Συσκευής

Επιπλέον, παρατηρούμε την ύπαρξη μιας μεταβλητής με όνομα dev, η οποία δίνεται ως όρισμα στην αρχή κάθε κβαντικού νευρωνικού δικτύου. Η μεταβλητή αυτή αντιπροσωπεύει τη συσκευή (device) πάνω στην οποία θα εκτελεστεί το κύκλωμα, και αποτελεί ένα από τα βασικά χαρακτηριστικά της βιβλιοθήκης PennyLane, καθώς παρέχει τη δυνατότητα προσομοίωσης διαφορετικών κβαντικών υπολογιστικών περιβαλλόντων.

Η έννοια της «συσκευής» είναι ιδιαίτερα σημαντική, δεδομένου ότι οι πραγματικοί κβαντικοί υπολογιστές βρίσκονται ακόμη σε πειραματικό στάδιο και δεν υπάρχει ακόμη ένα σταθερό ή καθολικά αποδεκτό hardware standard. Για τον λόγο αυτό, η PennyLane προσφέρει μια σειρά από εικονικές (simulated) και πραγματικές (hardware-backed) συσκευές, μέσω των οποίων μπορούμε να επιλέγουμε το επίπεδο ακρίβειας, πολυπλοκότητας και ρεαλισμού που επιθυμούμε στα πειράματά μας.

Συγκεκριμένα, στο πλαίσιο των πειραμάτων μας χρησιμοποιήθηκαν δύο διαφορετικές προσεγγίσεις:

- `dev = qml.device("default.qubit", wires=n_qubits+1)`

  Σε αυτή την περίπτωση, το δίκτυο εκτελείται πάνω σε μια ιδανική κβαντική συσκευή, χωρίς την ύπαρξη θορύβου ή λαθών. Ουσιαστικά, πρόκειται για έναν ιδανικό προσομοιωτή qubits, όπου κάθε κβαντική κατάσταση θεωρείται πλήρως σταθερή και απομονωμένη. Έτσι, τα αποτελέσματα αντικατοπτρίζουν την θεωρητική απόδοση του κυκλώματος σε ένα «τέλειο» περιβάλλον — κάτι που απέχει σημαντικά από την πραγματικότητα.

- `dev = qml.device("default.mixed", wires=n_qubits+1)`

  Η συγκεκριμένη συσκευή προσομοιώνει ένα ρεαλιστικότερο σενάριο, ενσωματώνοντας τα φαινόμενα θορύβου, αποσυνοχής και απώλειας πληροφορίας, που παρατηρούνται στους σημερινούς NISQ (Noisy Intermediate-Scale Quantum) υπολογιστές. Η χρήση της επιτρέπει την αξιολόγηση του πόσο ανθεκτικό είναι το μοντέλο σε πραγματικές συνθήκες εκτέλεσης και πόσο η ύπαρξη θορύβου επηρεάζει τη διαδικασία εκπαίδευσης και τα αποτελέσματα.

Συνολικά, η μεταβλητή dev λειτουργεί ως το σημείο σύνδεσης ανάμεσα στο θεωρητικό και το πρακτικό κομμάτι της κβαντικής υπολογιστικής, επιτρέποντας την ευέλικτη μετάβαση από προσομοιωμένα σε πραγματικά περιβάλλοντα, και καθιστώντας δυνατή τη σύγκριση των επιδόσεων του ίδιου κυκλώματος σε διαφορετικές υλοποιήσεις.

Τέλος, αξίζει να σημειωθεί πως υπάρχει σημαντική διαφορά στην ταχύτητα εκπαίδευσης μεταξύ των δύο συσκευών. Ειδικότερα, η εκτέλεση στο default.qubit είναι πολλαπλάσια ταχύτερη, καθώς δεν απαιτεί προσομοίωση των φαινομένων θορύβου και αποσυνοχής, ενώ η default.mixed συνεπάγεται αυξημένο υπολογιστικό κόστος λόγω της προσομοίωσης των επιδράσεων του περιβάλλοντος στο σύστημα. Για τον λόγο αυτό, στις περισσότερες περιπτώσεις, η αρχική εκπαίδευση πραγματοποιείται στο default.qubit, ενώ έγινε και ένα τελικό πείραμα στο default.mixed.

5.3.3.3 Δημιουργία Ολοκληρωμένου Δικτύου.

Στο σημείο αυτό πραγματοποιείται η ένωση όλων των επιμέρους τμημάτων του μοντέλου σε ένα ολοκληρωμένο νευρωνικό δίκτυο μέσω της Keras Sequential.

Ο κώδικας παρουσιάζει τη διαδικασία σύνδεσης των επιπέδων που έχουν αναπτυχθεί προηγουμένως τόσο των κλασικών όσο και των κβαντικών. Στο βασικό μοντέλο χρησιμοποιείται το qlayer, ενώ στην εκτεταμένη εκδοχή το qlayer_long, προκειμένου να δοκιμαστεί η επίδραση του βάθους του κβαντικού κυκλώματος.

Μέσω της δομής αυτής, τα δεδομένα περνούν διαδοχικά από το στάδιο προεπεξεργασίας, στο κβαντικό επίπεδο και τέλος στην έξοδο του συστήματος. Έτσι, επιτυγχάνεται η ενσωμάτωση όλων των στοιχείων του υβριδικού μοντέλου σε μία ενιαία μορφή, έτοιμη για εκπαίδευση και αξιολόγηση.

```
quantum_model = Sequential([
    Dense(4, activation=tf.nn.relu, input_shape=(X_train.shape[1],)),
    tf.keras.layers.Lambda(lambda x: tf.cast(x, tf.float32)),
    qlayer,
    tf.keras.layers.Lambda(lambda x: tf.abs(tf.cast(x, tf.complex64))),
    Dense(2, activation=tf.nn.softmax)
])
```

```
quantum_model_long = Sequential([
    Dense(4, activation=tf.nn.relu, input_shape=(X_train.shape[1],)),
    tf.keras.layers.Lambda(lambda x: tf.cast(x, tf.float32)),
    qlayer_long,
    tf.keras.layers.Lambda(lambda x: tf.abs(tf.cast(x, tf.complex64))),
    Dense(2, activation=tf.nn.softmax)
])
```

Συνοψίζοντας, στο παρόν τμήμα ολοκληρώθηκε η διαδικασία διαμόρφωσης και υλοποίησης του υβριδικού κβαντικού νευρωνικού δικτύου, με την ενσωμάτωση όλων των επιμέρους στοιχείων σε ένα ενιαίο και λειτουργικό μοντέλο. Έχουν πλέον καθοριστεί τόσο η αρχιτεκτονική του συστήματος όσο και οι παράμετροι εκτέλεσης, γεγονός που επιτρέπει την ομαλή μετάβαση στο επόμενο στάδιο.

Στην επόμενη ενότητα , επικεντρωνόμαστε αποκλειστικά στην εκτέλεση των πειραμάτων, προκειμένου να αξιολογηθεί η απόδοση του μοντέλου υπό διαφορετικές συνθήκες και ρυθμίσεις.

5.4 Ομομορφική Κρυπτογράφηση και Qhash

Η προστασία των τοπικών μοντέλων και των παραμέτρων τους αποτελεί κρίσιμη απαίτηση στα αποκεντρωμένα περιβάλλοντα εκπαίδευσης. Για τον σκοπό αυτό, στο προτεινόμενο σύστημα αναπτύχθηκε ένα υβριδικό υποσύστημα κρυπτογράφησης και κατακερματισμού (Encryption & Qhash Subsystem), το οποίο περιλαμβάνει τις παρακάτω λειτουργικές φάσεις:

1. Serialization των τοπικών βαρών (Weights Serialization)
2. Ομομορφική κρυπτογράφηση μέσω CKKS (Homomorphic Encryption)
3. Δημιουργία Qhash ταυτότητας (Quantum Hash)
4. Αποθήκευση και μεταφορά των κρυπτογραφημένων βαρών στο Blockchain Component

5.4.1 Serialization των Τοπικών Βαρών

Η διαδικασία ξεκινά μετά την ολοκλήρωση της εκπαίδευσης κάθε τοπικού μοντέλου. Τα βάρη (weights) εξάγονται από το μοντέλο Keras σε μορφή numpy array και στη συνέχεια μετατρέπονται σε serialized μορφή για να είναι έτοιμα προς κρυπτογράφηση.
Η μετατροπή υλοποιείται στο αρχείο serialization_encryption.py μέσω της συνάρτησης «def serialize_weights(weights)»
Η λειτουργία αυτή εξασφαλίζει τη συμβατότητα με τα δίκτυα μετάδοσης (blockchain, API calls) και επιτρέπει την ακριβή επανασύνθεση (deserialization) στη φάση αποκρυπτογράφησης.

5.4.2 Ομομορφική Κρυπτογράφηση (Homomorphic Encryption)

Η βασική κρυπτογράφηση πραγματοποιείται μέσω της βιβλιοθήκης TenSEAL, με χρήση του σχήματος CKKS (Cheon–Kim–Kim–Song), το οποίο υποστηρίζει υπολογισμούς σε κρυπτογραφημένα δεδομένα κινητής υποδιαστολής.
Η αντίστοιχη υλοποίηση βρίσκεται στο αρχείο encryption.py και περιλαμβάνει τα εξής βήματα:

```
import tenseal as ts

context = ts.context(
    ts.SCHEME_TYPE.CKKS,
    poly_modulus_degree=8192,
    coeff_mod_bit_sizes=[60, 40, 40, 60]
)
context.generate_galois_keys()
context.global_scale = 2**40
```

Στη συνέχεια, τα serialized weights μετατρέπονται σε CKKS vectors και κρυπτογραφούνται:

```
def encrypt_weights(serialized_weights, context):
    weights = np.array(json.loads(serialized_weights))
    enc_vector = ts.ckks_vector(context, weights)
    return enc_vector.serialize()
```

Κάθε client δημιουργεί ένα TenSEAL context με τα δικά του Galois keys, εξασφαλίζοντας μοναδικότητα κλειδιών ανά κόμβο και ανεξαρτησία στο επίπεδο αποκρυπτογράφησης.
Η χρήση της ομομορφικής κρυπτογράφησης επιτρέπει την άμεση εκτέλεση πράξεων (όπως ομομορφική πρόσθεση) επί των δεδομένων από τον aggregator, χωρίς προηγούμενη αποκρυπτογράφηση.

5.4.3 Δημιουργία Qhash

Μετά την κρυπτογράφηση, κάθε client υπολογίζει ένα Qhash (Quantum Hash) των κρυπτογραφημένων βαρών.
Το Qhash αποτελεί έναν μοναδικό αναγνωριστικό δείκτη ακεραιότητας που συνδυάζει παραδοσιακό hash (SHA-256) με κβαντικά χαρακτηριστικά εντροπίας (entropy-based seeding).
Η διαδικασία υλοποιείται στο αρχείο hashing_functions.py ως εξής:

```
import hashlib
import os

def generate_qhash(encrypted_weights):
    entropy_seed = os.urandom(16)
    combined_data = encrypted_weights + entropy_seed.hex()
    qhash = hashlib.sha256(combined_data.encode()).hexdigest()
    return qhash
```

Η χρήση τυχαίου κβαντικού seed (os.urandom) επιτρέπει στο hash να αποκτά ιδιότητες μη προβλεψιμότητας, καθιστώντας αδύνατη την ανακατασκευή των αρχικών δεδομένων.
Στη συνέχεια, το Qhash συνδέεται με τα κρυπτογραφημένα βάρη στο blockchain (μέσω του smart contract), δημιουργώντας ένα immutable ledger entry που αντιστοιχεί σε κάθε client και training round.

5.5 Blockchain Ενοποίηση και Smart Contract

Η ενσωμάτωση του blockchain στο προτεινόμενο σύστημα στοχεύει στη δημιουργία ενός αποκεντρωμένου μηχανισμού εμπιστοσύνης για την επαλήθευση, καταγραφή και αξιολόγηση των ενημερώσεων που παράγουν οι τοπικοί κόμβοι κατά την εκπαίδευση.
Η υλοποίηση βασίστηκε στο πλαίσιο Ethereum, το οποίο χρησιμοποιήθηκε τοπικά μέσω του Ganache, επιτρέποντας την ανάπτυξη, εκτέλεση και αποσφαλμάτωση smart contracts σε ένα ελεγχόμενο περιβάλλον.
Η επικοινωνία μεταξύ Python και blockchain πραγματοποιήθηκε με τη βιβλιοθήκη Web3.py, ενώ το συμβόλαιο NewSecureAggregation.sol ανέλαβε την καταγραφή και διαχείριση των ενημερώσεων, των Qhashes και των reputation scores.

5.5.1 Περιβάλλον Ανάπτυξης Blockchain

Το blockchain περιβάλλον υλοποιήθηκε με τα εξής εργαλεία:

- Ganache: τοπική Ethereum blockchain instance για ανάπτυξη smart contracts.
- Truffle: framework για compilation και deployment των .sol αρχείων.
- Web3.py: Python API για αλληλεπίδραση με τα deployed contracts.

Η διαδικασία ανάπτυξης περιλαμβάνει:

1. Compilation του NewSecureAggregation.sol μέσω Truffle.
2. Δημιουργία του αρχείου ABI (Application Binary Interface) στο SecureAggregation.json.
3. Deployment στο Ganache network μέσω του script 2_deploy_contracts.

Το deployment script ορίζει τις παραμέτρους και το address του συμβολαίου:

```
const SecureAggregation = artifacts.require("NewSecureAggregation");
module.exports = function (deployer) {
  deployer.deploy(SecureAggregation);
};
```

Μετά το deployment, ο Web3 client στην Python συνδέεται στο Ganache RPC endpoint και δημιουργεί αντικείμενο συμβολαίου:

```
from web3 import Web3
import json

w3 = Web3(Web3.HTTPProvider("http://127.0.0.1:7545"))
```

```
with open("SecureAggregation.json") as f:
    contract_json = json.load(f)
contract_abi = contract_json["abi"]
contract_address = "0x..."  # Ganache deployment address

contract = w3.eth.contract(address=contract_address, abi=contract_abi)
```

5.5.2 Δομή του Smart Contract

Το smart contract NewSecureAggregation.sol υλοποιεί τις λειτουργίες αποθήκευσης, επαλήθευσης και αξιολόγησης των μοντέλων που υποβάλλουν οι clients.
Η κύρια δομή δεδομένων είναι το ModelUpdate struct:

```
struct ModelUpdate {
    address client;
    string qhash;
    string encryptedWeights;
    uint256 timestamp;
    bool valid;
}
```

Όλες οι ενημερώσεις αποθηκεύονται σε δυναμικό πίνακα:

```
ModelUpdate[] public updates;
```

Η ροή λειτουργίας έχει ως εξής:

1. submitEncryptedWeights() — κάθε client καλεί αυτή τη συνάρτηση για να υποβάλει το Qhash και τα κρυπτογραφημένα βάρη:

```
function submitEncryptedWeights(string memory qhash, string memory encryptedWeights) public {
    updates.push(ModelUpdate(msg.sender, qhash, encryptedWeights, block.timestamp, true));
    emit ModelSubmitted(msg.sender, qhash, block.timestamp);
}
```

2. validateUpdate() — χρησιμοποιείται από τον aggregator ή τους validators για να ελέγξουν αν η ενημέρωση είναι έγκυρη:

```
function validateUpdate(uint index, bool isValid) public {
    updates[index].valid = isValid;
    emit ValidationResult(index, isValid, block.timestamp);
}
```

3. getValidUpdates() — επιστρέφει όλες τις έγκυρες ενημερώσεις προς συνάθροιση:

```
function getValidUpdates() public view returns (ModelUpdate[] memory) {
    uint validCount = 0;
    for (uint i = 0; i < updates.length; i++) {
        if (updates[i].valid) validCount++;
    }
    ModelUpdate[] memory validUpdates = new ModelUpdate[](validCount);
    uint j = 0;
    for (uint i = 0; i < updates.length; i++) {
```

```
        if (updates[i].valid) {
            validUpdates[j] = updates[i];
            j++;
        }
    }
    return validUpdates;
}
```

Με αυτό τον τρόπο, μόνο τα επικυρωμένα βάρη προωθούνται στον Global Aggregator για το επόμενο στάδιο (Secure Aggregation).

5.5.3 Διασύνδεση Smart Contract με Python

Το αρχείο blockchain_with_functions.py αποτελεί τη γέφυρα μεταξύ του Python pipeline και του smart contract.
Περιλαμβάνει συναρτήσεις για:

- υποβολή ενημερώσεων (submit_update()),
- ανάκτηση έγκυρων μοντέλων (get_valid_updates()),
- και ενημέρωση του blockchain με το παγκόσμιο μοντέλο μετά τη συνάθροιση (submit_global_model()).

Η τυπική ροή επικοινωνίας είναι:

```
def submit_update(qhash, encrypted_weights):
    tx_hash = contract.functions.submitEncryptedWeights(qhash, encrypted_weights).transact({
        'from': w3.eth.accounts[0],
        'gas': 3000000
    })
    receipt = w3.eth.wait_for_transaction_receipt(tx_hash)
    return receipt
```

Για την ανάκτηση των έγκυρων ενημερώσεων από το blockchain:

```
def get_valid_updates():
    return contract.functions.getValidUpdates().call()
```

5.5.4 Reputation και Outlier Filtering

Στο συμβόλαιο προβλέπεται και ένας μηχανισμός *Reputation Scoring*, ο οποίος συσχετίζει κάθε διεύθυνση client με έναν δυναμικό δείκτη αξιοπιστίας. Η ενημέρωση του δείκτη πραγματοποιείται αθροιστικά μετά από κάθε γύρο εκπαίδευσης, σύμφωνα με τον τύπο:

$$R_i^{(t+1)} = R_i^{(t)} + \alpha \cdot A_i^{(t)} - \beta \cdot R_i^{(t)} \cdot (1 - A_i^{(t)})$$

όπου:

$R_i^{(t)}$ είναι το reputation του client iστον γύρο t,
$A_i^{(t)} \in \{0,1\}$ είναι η απόφαση αποδοχής (1) ή απόρριψης (0) του μοντέλου του client,
α και β είναι σταθερές αύξησης και ποινής αντίστοιχα.

Με αυτόν τον τρόπο, οι έγκυρες συνεισφορές αυξάνουν το reputation, ενώ οι μη έγκυρες επιφέρουν ποινή που είναι ανάλογη του προηγούμενου δείκτη αξιοπιστίας.

Παράλληλα, στο blockchain_with_functions.py υλοποιείται outlier filtering, το οποίο συγκρίνει το Qhash και το hash consistency με προηγούμενους γύρους για τον εντοπισμό ύποπτων updates:

```
def validate_qhash_consistency(qhash, prev_qhashes):
    return qhash not in prev_qhashes
```

Με αυτόν τον τρόπο, το blockchain λειτουργεί όχι μόνο ως κατανεμημένο καθολικό (ledger), αλλά και ως μηχανισμός ενσωματωμένης αξιολόγησης των κόμβων.

5.6 Secure Aggregation και QKD Integration

Η φάση της Secure Aggregation αποτελεί το τελικό και πιο κρίσιμο στάδιο της αρχιτεκτονικής, καθώς σε αυτό το σημείο πραγματοποιείται η ομομορφική συνάθροιση των κρυπτογραφημένων βαρών που έχουν επικυρωθεί από το blockchain, η αποκρυπτογράφηση των αποτελεσμάτων, και τέλος η αναδιανομή του παγκόσμιου μοντέλου (Global Model) στους συμμετέχοντες κόμβους μέσω Quantum Key Distribution (QKD) [154].
Η όλη διαδικασία επιτρέπει στον aggregator να δημιουργήσει ένα νέο, ενοποιημένο μοντέλο χωρίς να έχει πρόσβαση σε μη κρυπτογραφημένα δεδομένα, εξασφαλίζοντας πλήρη ιδιωτικότητα και ακεραιότητα.

5.6.1 Ανάκτηση και Αποκρυπτογράφηση Ενημερώσεων

Η λειτουργία του Global Aggregator ξεκινά με την ανάκτηση των επικυρωμένων ενημερώσεων από το blockchain.
Η επικοινωνία υλοποιείται μέσω της συνάρτησης get_valid_updates() στο αρχείο blockchain_with_functions.py, η οποία επιστρέφει λίστα από serialized αντικείμενα με Qhash και encrypted weights.

Κάθε ενημέρωση περνά στη φάση deserialization και αποκρυπτογράφησης, η οποία πραγματοποιείται μέσω της συνάρτησης decrypt_weights() από το αρχείο deserialization_decryption.py:

```
def decrypt_weights(serialized_enc_weights, context):
    enc_vector = ts.ckks_vector_from(context, serialized_enc_weights)
    decrypted = enc_vector.decrypt()
    return np.array(decrypted)
```

Η συνάρτηση λαμβάνει το TenSEAL context (με το private key του aggregator), αναδημιουργεί το CKKS vector από το serialized object και επιστρέφει τα αποκρυπτογραφημένα βάρη ως numpy array.
Αυτό επιτρέπει στον aggregator να επανασυνθέσει τα τοπικά βάρη που είχαν σταλεί από τους clients, χωρίς να έχει προηγουμένως δει ή επεξεργαστεί τα αρχικά δεδομένα εκπαίδευσης.

5.6.2 Μέθοδοι Συνάθροισης (Aggregation Methods)

Στην παρούσα υλοποίηση εξετάστηκαν και δοκιμάστηκαν πολλαπλές μέθοδοι συνάθροισης προκειμένου να αξιολογηθεί η αποδοτικότητά τους στο πλαίσιο της ανίχνευσης απάτης. Όλες οι συναθροίσεις υλοποιούνται μέσα στο pipeline quantum_fraud_detection_pipeline.py και καλούνται δυναμικά από τον aggregator ανάλογα με τον πειραματικό γύρο.

(α) FedAvg (Federated Averaging)

Η βασική μέθοδος, γνωστή ως FedAvg, υπολογίζει τον σταθμισμένο μέσο όρο των τοπικών βαρών, λαμβάνοντας υπόψη το μέγεθος του τοπικού dataset κάθε κόμβου:

```
def fed_avg(local_weights, data_sizes):
    total = sum(data_sizes)
    weighted_sum = sum(w * (n / total) for w, n in zip(local_weights, data_sizes))
    return weighted_sum
```

Η FedAvg επιλέχθηκε ως baseline λόγω της σταθερότητάς της σε μη ομογενή δεδομένα, αλλά σε σενάρια υψηλής μεταβλητότητας των τοπικών ενημερώσεων η μέση τιμή μπορεί να μην αντικατοπτρίζει επακριβώς τη βέλτιστη λύση.

(β) Weighted Median Aggregation
Για να αντιμετωπιστεί η ευαισθησία του FedAvg σε outliers, υλοποιήθηκε μια median-based προσέγγιση, στην οποία για κάθε παράμετρο του μοντέλου υπολογίζεται η διάμεσος τιμή των ενημερώσεων:

```
def weighted_median(local_weights):
    stacked = np.stack(local_weights, axis=0)
    median = np.median(stacked, axis=0)
    return median
```

Η μέθοδος αυτή είναι πιο ανθεκτική σε επιθέσεις Byzantine ή εσφαλμένα δεδομένα εκπαίδευσης, καθώς μειώνει την επιρροή ακραίων τιμών.

(γ) Adaptive Aggregation
Αναπτύχθηκε επίσης μια Adaptive Aggregation συνάρτηση που αξιοποιεί τα reputation scores των clients (όπως έχουν ενημερωθεί από το smart contract).
Η στάθμιση των βαρών γίνεται με βάση το trust score κάθε κόμβου:

```
def adaptive_aggregation(local_weights, trust_scores):
    normalized = trust_scores / np.sum(trust_scores)
    aggregated = np.sum([w * s for w, s in zip(local_weights, normalized)], axis=0)
    return aggregated
```

Με αυτόν τον τρόπο, οι πιο αξιόπιστοι κόμβοι έχουν μεγαλύτερη επιρροή στο τελικό global model, ενισχύοντας τη συνολική ακρίβεια και ανθεκτικότητα του συστήματος.

(δ) Quantum-Weighted Aggregation

Σε πιο προχωρημένα πειράματα (βασισμένα στα αρχεία quantum_miner.py και quantum_pow_miner.py), εισήχθη μια Quantum-Weighted Aggregation μέθοδος.
Η στάθμιση εδώ εξαρτάται από το quantum hash difficulty που προκύπτει κατά τη φάση του Quantum Proof-of-Work (αναλύεται στο Κεφ. 5.5) [156].

Η ιδέα είναι ότι κόμβοι που συμβάλλουν με ενημερώσεις που περνούν ταχύτερα ή αποδοτικότερα την κβαντική επικύρωση, αποκτούν μεγαλύτερη στάθμιση στην τελική συνάθροιση.

5.6.3 Υλοποίηση Ομομορφικής Συνάθροισης

Μετά την αποκρυπτογράφηση των ενημερώσεων, ο aggregator εφαρμόζει ομομορφική συνάθροιση (Homomorphic Aggregation) για να δημιουργήσει το παγκόσμιο μοντέλο.
Η βασική υλοποίηση πραγματοποιείται με TenSEAL:

```
def aggregate_encrypted_models(encrypted_models):
    result = encrypted_models[0]
    for model in encrypted_models[1:]:
        result += model
    result /= len(encrypted_models)
    return result
```

Επειδή οι CKKS vectors επιτρέπουν πράξεις πρόσθεσης και μέσης τιμής χωρίς αποκρυπτογράφηση, το αποτέλεσμα είναι ένα νέο encrypted global vector, το οποίο αποθηκεύεται στο blockchain μετά την τελική επικύρωση.

5.6.4 QKD Encryption και Αναδιανομή του Global Model

Αφού ολοκληρωθεί η συνάθροιση, το νέο παγκόσμιο μοντέλο κρυπτογραφείται εκ νέου με Quantum Key Distribution (QKD) κλειδιά πριν σταλεί στους clients.
Η χρήση της Κβαντικής Διανομής Κλειδιών (QKD) στο προτεινόμενο πλαίσιο διασφαλίζει την ασφαλή αποστολή του παγκόσμιου μοντέλου προς τους clients, αξιοποιώντας τις θεμελιώδεις ιδιότητες της κβαντικής φυσικής ώστε να εντοπίζονται κάθε μορφής παρεμβολές ή υποκλοπές. Η διαδικασία αυτή ενσωματώνεται μεταξύ του Global Aggregator και των επιμέρους κόμβων και ακολουθεί συγκεκριμένα στάδια με πλήρη κβαντική ασφάλεια.

Η πλήρης ροή της διαδικασίας περιλαμβάνει:

1. Γεννήτρια Ακατέργαστου Κλειδιού (Raw Key Generation): Χρησιμοποιείται πρωτόκολλο όπως το BB84, μέσω του οποίου δημιουργείται ένα σύνολο κβαντικών bits (qubits) που μεταφέρονται μέσω οπτικών ινών ή κβαντικού καναλιού.
2. Sifting (Φιλτράρισμα): Απορρίπτονται τα qubits που βασίζονται σε ασύμβατες βάσεις μεταξύ αποστολέα και παραλήπτη, οδηγώντας σε συμφωνία μόνο σε εκείνα που μετρήθηκαν σωστά.
3. Διόρθωση Σφαλμάτων (Error Reconciliation): Εφαρμόζονται πρωτόκολλα όπως Cascade ώστε να εντοπιστούν και να διορθωθούν τα σφάλματα λόγω θορύβου ή απώλειας πακέτων.
4. Ενίσχυση Ιδιωτικότητας (Privacy Amplification): Μέσω καθολικών hash functions εξασφαλίζεται ότι ακόμη και αν μέρος του κλειδιού έχει διαρρεύσει, η πληροφορία που έχει στην κατοχή του ο υποκλοπέας καθίσταται στατιστικά αμελητέα.

Η απόδοση του συστήματος QKD υπολογίζεται με βάση τον ρυθμό παραγωγής ασφαλούς κλειδιού (*secret key rate*), ο οποίος εκτιμάται ως:

$$R_{\text{final}} = R_{\text{raw}} \cdot (1 - H(E) - f(E))$$

όπου:

- R_{raw} είναι ο ρυθμός ακατέργαστων bits (π.χ. σε Mbps),
- E είναι το ποσοστό σφάλματος (Quantum Bit Error Rate – QBER),
- $H(E)$ είναι η δυαδική εντροπία του σφάλματος και
- $f(E)$ είναι η αναποτελεσματικότητα της διαδικασίας reconciliation.

Η διαδικασία ολοκληρώνεται με την παραγωγή ενός μυστικού συμμετρικού κλειδιού (QKD key) που χρησιμοποιείται για την κρυπτογράφηση του παγκόσμιου μοντέλου. Το μοντέλο διανέμεται προς τους clients με τη χρήση XOR-based encryption:

Η διαδικασία περιλαμβάνει:

1. Δημιουργία νέου QKD keypair για κάθε client.
2. Κρυπτογράφηση του global model με το QKD key:

```
def qkd_encrypt(global_model, qkd_key):
encrypted_model = xor_bytes(global_model, qkd_key)
return encrypted_model
```

3. Αποστολή του encrypted_model στους clients.

Κατά τη λήψη, κάθε client χρησιμοποιεί το ιδιωτικό του QKD key για να αποκρυπτογραφήσει το μοντέλο:

```
def qkd_decrypt(encrypted_model, qkd_key):
   decrypted_model = xor_bytes(encrypted_model, qkd_key)
   return decrypted_model
```

Έτσι, επιτυγχάνεται τελική διανομή χωρίς μεσολάβηση τρίτου μέρους και με εγγυημένη κβαντική ασφάλεια.

5.6.5 Αποτροπή Επιθέσεων Man-in-the-Middle μέσω Qhash, QKD και Blockchain

Ο συνδυασμός των μηχανισμών Quantum Hashing (Qhash), Quantum Key Distribution (QKD) και Blockchain προσφέρει πολυεπίπεδη προστασία έναντι επιθέσεων τύπου Man-in-the-Middle (MitM) μέσω των εξής:

1. Qhash – Επαλήθευση Ακεραιότητας:

   Κάθε ενημέρωση μοντέλου συνοδεύεται από έναν κβαντικό κατακερματισμό (Qhash), ο οποίος δημιουργείται βάσει των παραμέτρων του μοντέλου και του client ID. Ο παραλήπτης μπορεί να υπολογίσει εκ νέου το Qhash και να συγκρίνει. Οποιαδήποτε παρέμβαση τρίτου στον μεταδιδόμενο αλγόριθμο οδηγεί σε αναντιστοιχία του Qhash, αποκαλύπτοντας την παραβίαση.

2. QKD – Προστασία Καναλιού Επικοινωνίας:

   Η χρήση κβαντικής διανομής κλειδιών διασφαλίζει ότι οποιαδήποτε προσπάθεια υποκλοπής

στο κβαντικό κανάλι αλλοιώνει την κατάσταση των qubits (λόγω της αρχής της μη αντιγράφισης και της αβεβαιότητας), με αποτέλεσμα να ανιχνεύεται η επίθεση κατά τη φάση reconciliation. Επομένως, διασφαλίζεται η γνησιότητα των συμμετεχόντων και των δεδομένων.

3. Blockchain – Καταγραφή και Αμεταβλητότητα:

   Όλες οι εγγραφές επικυρωμένων ενημερώσεων (encrypted weights, Qhashes, reputation scores) αποθηκεύονται στο blockchain. Λόγω της αμετάβλητης φύσης της αλυσίδας, ένας ενδιάμεσος επιτιθέμενος δεν μπορεί να εισαγάγει ή να παραποιήσει δεδομένα χωρίς να γίνει άμεσα αντιληπτός από τους υπόλοιπους κόμβους.

Ο συνδυασμός των παραπάνω:

- Το Qhash εξασφαλίζει ακεραιότητα,
- Το QKD προσφέρει εμπιστευτικότητα και αυθεντικοποίηση του καναλιού,
- Το Blockchain παρέχει ιχνηλασιμότητα και ανίχνευση παραποίησης.

Έτσι, οποιαδήποτε προσπάθεια ενδιάμεσης παρέμβασης είτε στο μοντέλο είτε στο κανάλι επικοινωνίας είτε στο δίκτυο επαλήθευσης αποτυγχάνει, καθώς ενεργοποιούνται τουλάχιστον δύο μηχανισμοί ανίχνευσης και απόρριψης της επικοινωνίας.

5.7 Δημιουργία SaaS Εφαρμογής και χρήση Αληθινού Κβαντικού Υπολογιστή

Στο επόμενο στάδιο της παρούσας εργασίας, η προτεινόμενη προσέγγιση —η ανάπτυξη ενός υβριδικού κβαντικο-κλασικού νευρωνικού δικτύου για την ανίχνευση απάτης— ολοκληρώθηκε με τη μορφή υπηρεσίας Software as a Service (SaaS).

Η υπηρεσία αυτή μετατρέπει το θεωρητικό υπόβαθρο που αναλύθηκε προηγουμένως σε ένα πρακτικά διαθέσιμο εργαλείο, το οποίο μπορεί να χρησιμοποιηθεί από τρίτους μέσω διαδικτύου.

Ιδιαίτερη σημασία έχει ότι, στο πλαίσιο της υλοποίησης αυτής, πραγματοποιήθηκε πραγματική εκτέλεση του μοντέλου σε κβαντικό υπολογιστή μέσω της πλατφόρμας IBM Quantum. Έτσι, το SaaS σύστημα δεν περιορίζεται σε εξομοίωση, αλλά συνδέεται απευθείας με πραγματικό quantum hardware, αποδεικνύοντας τη δυνατότητα εφαρμογής των υβριδικών κβαντικών δικτύων σε πραγματικές υπολογιστικές υποδομές.

5.7.1 Επιλογή της Πλατφόρμας

Για την υλοποίηση της SaaS υπηρεσίας επιλέχθηκε η πλατφόρμα PlanQk της εταιρείας Kipu Quantum (startup με έδρα το Βερολίνο). Η PlanQk αποτελεί μία ανοικτή και κοινοτική πλατφόρμα για κβαντικές εφαρμογές, η οποία «συνδέει» προγραμματιστές, ερευνητές, βιομηχανικούς χρήστες και παρόχους κβαντικών υπολογιστών. Η πλατφόρμα προσφέρει ένα οικοσύστημα ανάπτυξης (deployment) και αξιοποίησης κβαντικών υπηρεσιών (quantum services) — και ως εκ τούτου εξυπηρετεί άμεσα το πλαίσιο του SaaS.

Στη συνέχεια, μέσω της πλατφόρμας PlanQk, πραγματοποιήθηκε το deployment του εκπαιδευμένου μοντέλου μας, δηλαδή αυτού που περιγράφηκε στην ενότητα αρχιτεκτονικής ως «υβριδικό κβαντικο νευρωνικό δίκτυο». Η δυνατότητα που παρέχει η PlanQk για ανεξάρτητη εκτέλεση (inference) του

μοντέλου, χωρίς να απαιτείται εκ νέου εκπαίδευση, επιτρέπει την άμεση διάθεση της υπηρεσίας προς χρήστες.

5.7.2 Δυνατότητες της Υπηρεσίας

Η υπηρεσία που υλοποιήθηκε έχει τα εξής βασικά χαρακτηριστικά:

- Οι τελικοί χρήστες έχουν πρόσβαση μέσω της πλατφόρμας (μέσω του συνδέσμου : https://hub.kipu-quantum.com/marketplace/services/c71afbde-3256-479a-9b7a-f4275925a658) — η οποία διαθέτει το αντίστοιχο marketplace/service slot μέσα στην PlanQk.
- Η λειτουργία είναι *μόνο* για inference, δηλαδή για την εκτέλεση του μοντέλου σε νέα δεδομένα — δεν περιλαμβάνει τη δυνατότητα re-training (επανα-εκπαίδευσης) του μοντέλου.
- Οι χρήστες έχουν δύο βασικές επιλογές εισόδου:
  - (α) εισαγωγή ενός μεμονωμένου δείγματος (single input) – το σύστημα επεξεργάζεται τα χαρακτηριστικά και επιστρέφει την πρόβλεψη (0 ή 1)
  - (β) εισαγωγή ενός συνόλου δεδομένων (dataset) – στη συνέχεια το σύστημα εκτελεί το μοντέλο για όλα τα δείγματα και επιστρέφει ως έξοδο το συνολικό ποσοστό accuracy της πρόβλεψης επί του συνόλου.
- Επιπλέον, παρέχεται η δυνατότητα επιλογής του περιβάλλοντος εκτέλεσης: είτε σε simulator (κβαντικός προσομοιωτής) για ταχύτερη και «καθαρότερη» εκτέλεση χωρίς φυσικό κβαντικό θόρυβο, είτε σε πραγματικό κβαντικό υπολογιστή (quantum computer).
- Στην περίπτωση της εκτέλεσης σε πραγματικό κβαντικό υπολογιστή, αξιοποιήθηκε η υποδομή της IBM Quantum Platform της IBM, η οποία παρέχει πρόσβαση σε πραγματικούς κβαντικούς επεξεργαστές και προσομοιωτές μέσω cloud. Λόγω περιορισμών του κβαντικού υλικού (όπως ο θόρυβος, η διαθεσιμότητα, η διάρκεια εκτέλεσης) η εκτέλεση σε πραγματικό υλικό έγινε για ένα μόνο δεδομένο τη φορά.

5.7.3 Προσέγγιση και Ροή Εργασίας

Η ροή εργασίας της υπηρεσίας SaaS που υλοποιήθηκε μπορεί να περιγραφεί ως εξής:

1. Προετοιμασία και Ανάπτυξη Μοντέλου
   - Εκπαίδευση του υβριδικού μοντέλου σύμφωνα με την αρχιτεκτονική που προηγήθηκε.
   - Επιλογή του εκπαιδευμένου μοντέλου για deployment χωρίς περαιτέρω fine-tuning στο περιβάλλον SaaS.
2. Deployment στην Πλατφόρμα PlanQk
   - Ανέβασμα του μοντέλου στην πλατφόρμα PlanQk, καθορίζοντας τις παραμέτρους της υπηρεσίας (τύπος εισόδου, επιλογές εκτέλεσης, περιβάλλον εκτέλεσης).
   - Διαμόρφωση του marketplace slot με URL για απευθείας χρήση από χρήστες — όπως παραπάνω.
3. Παραμετροποίηση Εκτέλεσης
   - Ο χρήστης επιλέγει αν θα δώσει *ένα δείγμα* ή *σύνολο δεδομένων*.
   - Ο χρήστης θα επιλέξει αν η εκτέλεση θα γίνει σε simulator ή στο πραγματικό quantum hardware.
4. Inference και Αποτελέσματα
   - Σε περίπτωση *μεμονωμένου δείγματος*, η υπηρεσία εκτελεί το μοντέλο και επιστρέφει πρόβλεψη 0 / 1.
   - Σε περίπτωση *σύνολου δεδομένων*, η υπηρεσία επεξεργάζεται όλα τα δείγματα και υπολογίζει το συνολικό accuracy.
   - Σε εκτέλεση στο quantum hardware, η εκτέλεση έγινε περιορισμένα (ένα δεδομένο τη φορά) λόγω της φύσης των συσκευών (θόρυβος, αναμονή στην ουρά, κόστος).
5. Διάθεση και Πρόσβαση
   - Η υπηρεσία διατίθεται προς χρήση από τρίτους, επιτρέποντας τόσο εκπαιδευτικά όσο και ερευνητικά/βιομηχανικά σενάρια.

- Η χρήση μέσω SaaS διευκολύνει την ενσωμάτωση και αξιοποίηση του μοντέλου χωρίς την ανάγκη τοπικής υποδομής.

5.7.4 Σχόλιο Τεχνολογικής Σημασίας

Η υλοποίηση αυτή εξυπηρετεί πολλαπλές σημαντικές πτυχές:

- Η μετάβαση από θεωρητική αρχιτεκτονική σε υπηρεσία που λειτουργεί πραγματικά σε cloud περιβάλλον επιδεικνύει ότι η κβαντική και υβριδική τεχνολογία μπορεί να ενσωματωθεί σε πλαίσια παραγωγής/χρήσης.
- Η επιλογή του περιβάλλοντος εκτέλεσης (simulator vs quantum hardware) επιτρέπει πειραματισμό και σύγκριση μεταξύ της «ιδεατής» προσομοιωμένης εκτέλεσης και της πραγματικής κβαντικής εκτέλεσης υπό θόρυβο.
- Η χρήση της IBM Quantum πλατφόρμας ως backend ενισχύει τη συνέπεια με την τρέχουσα κβαντική έρευνα και υποδομή.
- Η διάθεση ως SaaS μειώνει τα εμπόδια εισόδου για χρήστες/ερευνητές που δεν διαθέτουν εξειδικευμένο υλικό ή υποδομή, και ενισχύει την προσβασιμότητα της τεχνολογίας.

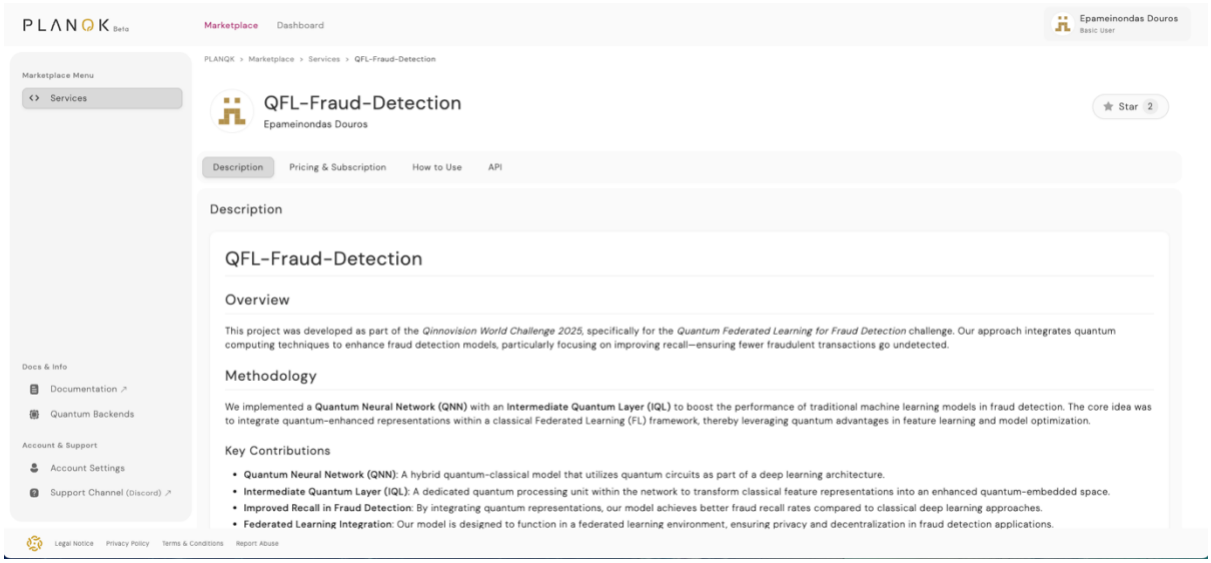
5.7.5 Περιορισμοί & Προοπτικές

Παρά τα σημαντικά οφέλη, η υλοποίηση υπόκειται σε περιορισμούς που αξίζει να σημειωθούν στην εργασία:

- Η εκτέλεση σε πραγματικό κβαντικό υπολογιστή έγινε μόνο για έναν δείγμα λόγω της χαμηλής διαθεσιμότητας, του χρόνου εκτέλεσης και της απαιτητικότητας των συσκευών. Αυτό σημαίνει ότι τα αποτελέσματα υπό αυτές τις συνθήκες δεν είναι αντιπροσωπευτικά για μεγάλα datasets.
- Ο θόρυβος και τα σφάλματα των κβαντικών συσκευών επηρεάζουν την ακρίβεια και την αξιοπιστία της εκτέλεσης· η χρήση simulator επιτρέπει «τυπική» εκτέλεση χωρίς αυτά τα φαινόμενα.
- Η λειτουργία ως inference-μόνο υπηρεσία εξαλείφει τη δυνατότητα περαιτέρω εκπαίδευσης ή βελτιστοποίησης του μοντέλου μέσω της ίδιας πλατφόρμας (τουλάχιστον στην παρούσα φάση).
- Μελλοντικά, θα μπορούσε να εξεταστεί η επέκταση της υπηρεσίας ώστε να υποστηρίζει batch-εκπαίδευση, παρακολούθηση απόδοσης μοντέλου με χρήση πραγματικών δεδομένων σε παραγωγή, καθώς και επέκταση σε περισσότερα quantum back-ends.

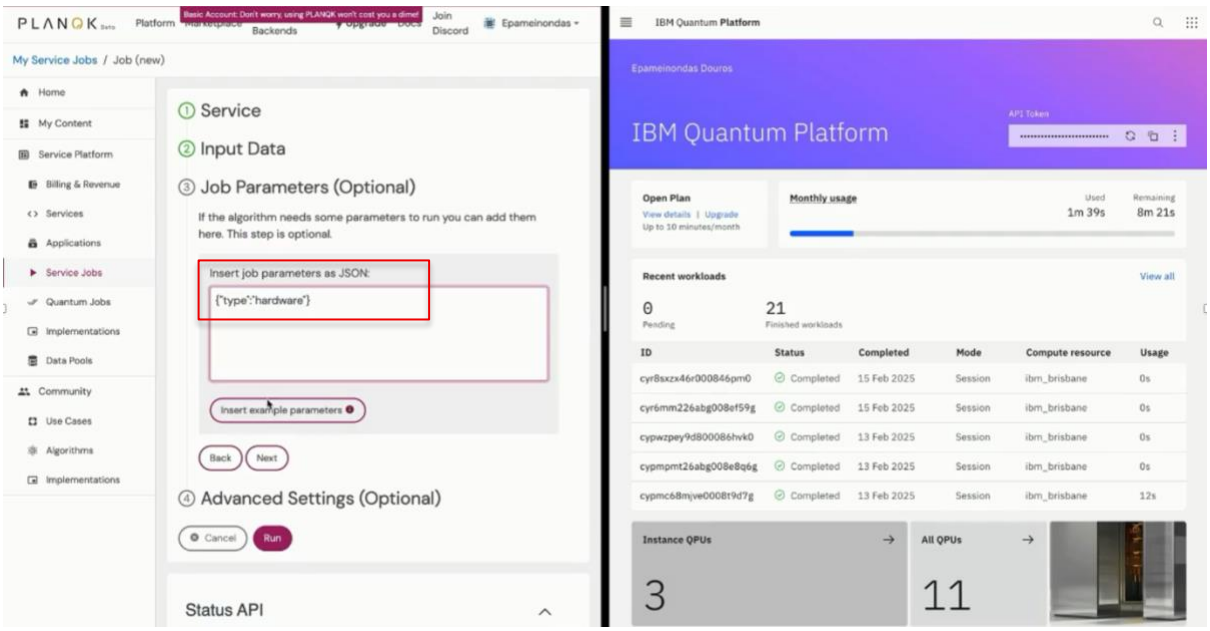
5.7.6 Χρήση της πλατφόρμας

Η λειτουργία που αναπτύξαμε είναι διαθέσιμη στο “marketplace” της πλατφόρμας PlanQk. Με την κατάλληλη αναζήτηση, ο χρήστης μπορεί να την εντοπίσει και να οδηγηθεί στη σελίδα παρουσίασης της υπηρεσίας, όπου εμφανίζονται τα σχετικά στοιχεία και επιλογές εκτέλεσης.



https://hub.kipu-quantum.com/marketplace/services/c71afbde-3256-479a-9b7a-f4275925a658

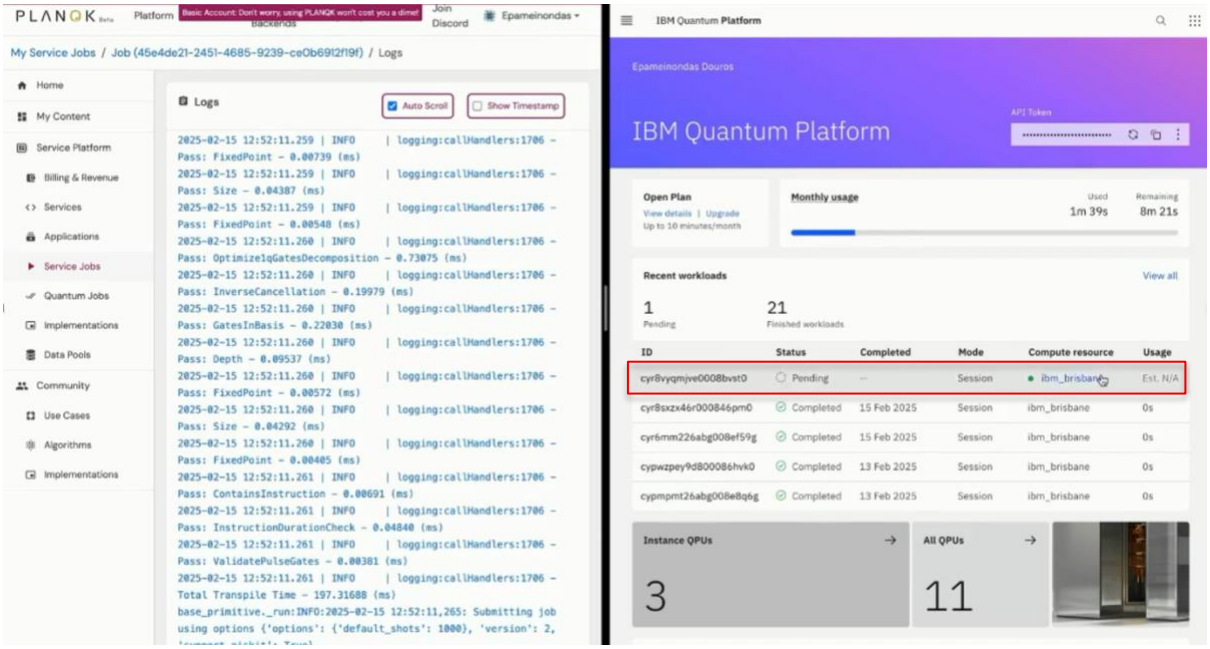
Στη συνέχεια, μεταβαίνουμε στη σελίδα χρήσης της υπηρεσίας, όπου —όπως φαίνεται στην αριστερή πλευρά της επόμενης εικόνας— εμφανίζεται το περιβάλλον ρυθμίσεων. Εκεί, μέσω ενός φιλικού και διαδραστικού UI, διαμορφώνουμε την «κλήση» προς το API. Στο σημείο αυτό εισάγουμε τα δεδομένα εισόδου και, το σημαντικότερο, επιλέγουμε ως συσκευή εκτέλεσης το πραγματικό κβαντικό υπολογιστικό σύστημα, ώστε το δίκτυο να εκτελεστεί απευθείας σε quantum hardware.



Στη συνέχεια, επιλέγουμε “Run”, και χωρίς να απαιτείται καμία περαιτέρω ενέργεια από εμάς, το αίτημα εκτέλεσης αποστέλλεται αυτόματα στην πλατφόρμα της IBM, όπου πραγματοποιείται η κλήση προς τον κβαντικό υπολογιστή.

Είναι αναμενόμενο να υπάρχουν χρονικές καθυστερήσεις, καθώς ο αριθμός των διαθέσιμων κβαντικών υπολογιστών παγκοσμίως είναι περιορισμένος και τα αιτήματα εκτελούνται με σειρά προτεραιότητας.

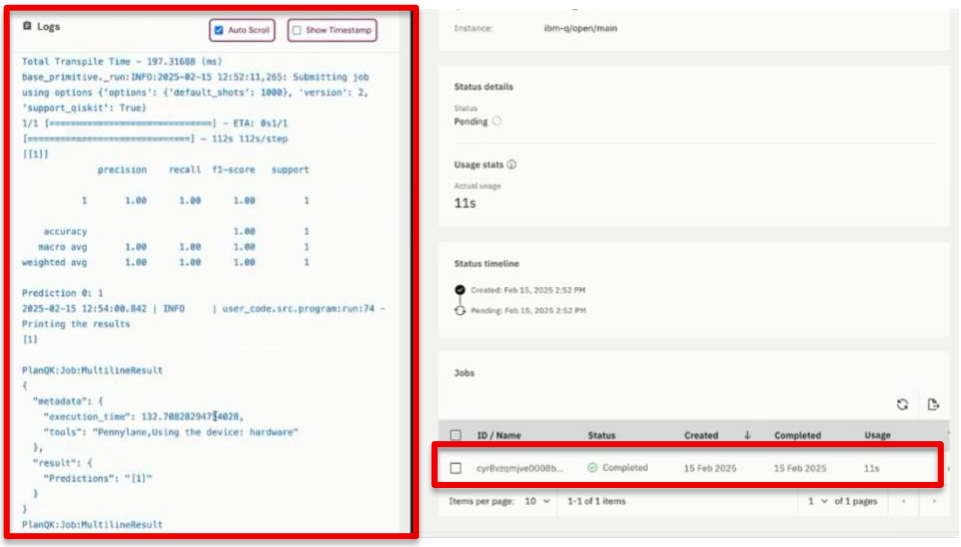
Όπως φαίνεται και στην επόμενη εικόνα, το αίτημα έχει καταχωρηθεί επιτυχώς στο σύστημα του κβαντικού υπολογιστή, και το μοντέλο βρίσκεται πλέον σε στάδιο αναμονής για εκτέλεση.



Αφού επιλέξουμε το ID του νέου αιτήματος, έχουμε πρόσβαση σε αναλυτικές πληροφορίες σχετικά με την εκτέλεση.

Μετά από σύντομη αναμονή περίπου 11 δευτερολέπτων, ο υπολογισμός ολοκληρώνεται επιτυχώς και το αποτέλεσμα επιστρέφει αυτόματα στην πλατφόρμα PlanQk, όπου εμφανίζονται τα τελικά αποτελέσματα του μοντέλου.

Όπως φαίνεται και στην εικόνα, το σύστημα εντόπισε σωστά την ετικέτα του δεδομένου εισόδου — στην προκειμένη περίπτωση, 1 = fraud — επιβεβαιώνοντας έτσι τη σωστή λειτουργία και ακρίβεια του κβαντικού μοντέλου.



5.7.6 Σύνοψη

Συνοψίζοντας, η υλοποίηση της SaaS υπηρεσίας για το υβριδικό μοντέλο αποτελεί σημαντικό επιχειρησιακό και τεχνολογικό βήμα: μέσω της πλατφόρμας PlanQk (Kipu Quantum) και της υποδομής της IBM Quantum, το μοντέλο καθίσταται προσβάσιμο σε χρήστες, με ρεαλιστική λειτουργία και επιλογές εκτέλεσης είτε σε simulator είτε σε πραγματικό hardware. Η διάθεση μέσω web-based υπηρεσίας ενισχύει την ερευνητική και πρακτική αξία της εργασίας σας, ενώ ανοίγει το δρόμο για περαιτέρω επέκταση και αξιοποίηση σε εφαρμογές παραγωγής.

Κεφάλαιο 6. Πειραματικά Αποτελέσματα

6.1 Περιγραφή Δεδομένων και Μεθοδολογίας

Η ανάλυση της αρχιτεκτονικής και του δικτύου παρουσιάστηκε αναλυτικά στην προηγούμενη ενότητα. Στη συνέχεια, παραθέτουμε ένα απόσπασμα από τον κώδικα που χρησιμοποιήθηκε για την εκπαίδευση, το οποίο υλοποιεί ολόκληρο τον αγωγό (preprocessing, ορισμό μοντέλου, βελτιστοποίηση παραμέτρων και αξιολόγηση) και επιτρέπει την αναπαραγωγή των πειραμάτων με τις ίδιες ρυθμίσεις υπερπαραμέτρων.

Για την ανάπτυξη και εκπαίδευση του κβαντικού τμήματος του δικτύου έγινε χρήση της βιβλιοθήκης PennyLane, η οποία επιτρέπει την υλοποίηση παραμετρικών κβαντικών κυκλωμάτων (Variational Quantum Circuits) και την ενσωμάτωσή τους σε υβριδικά μοντέλα μέσω διεπαφής με το TensorFlow.

Σημαντικό είναι εδώ να σημειωθεί ότι σε όλα τα πειράματα η εκπαίδευση πραγματοποιήθηκε πάντα με το ίδιο σύνολο δεδομένων, ώστε να διασφαλιστεί η συνέπεια και η συγκρισιμότητα των αποτελεσμάτων. Με τον τρόπο αυτό, απομονώνονται οι επιδράσεις της τυχαιότητας που θα μπορούσαν να προκύψουν από διαφορετικές δειγματοληψίες ή ανακατατάξεις των δεδομένων, επιτρέποντας έτσι μια δίκαιη και αξιόπιστη αξιολόγηση της επίδοσης του κάθε μοντέλου, είτε πρόκειται για το κλασικό είτε για το υβριδικό κβαντικό δίκτυο.

Για τη διεξαγωγή των πειραμάτων χρησιμοποιήθηκαν δύο διαφορετικά σύνολα δεδομένων πραγματικών τραπεζικών συναλλαγών, με σκοπό τη σύγκριση της συμπεριφοράς των μοντέλων σε διαφορετικές κλίμακες και βαθμούς πολυπλοκότητας. Αρχικά, πραγματοποιήθηκαν δοκιμαστικές προσεγγίσεις στο μικρότερο dataset Fraud Detection Bank Dataset (https://www.kaggle.com/datasets/volodymyrgavrysh/fraud-detection-bank-dataset-20k-records-binary/data), το οποίο περιλαμβάνει περίπου 20.000 συναλλαγές. Παρότι το σύνολο αυτό επέτρεψε την ταχεία επαλήθευση της ορθότητας της αρχιτεκτονικής και της ροής εκπαίδευσης, παρατηρήθηκε ότι τα κλασικά νευρωνικά δίκτυα μικρού βάθους παρουσίαζαν σχεδόν τέλεια απόδοση, κυρίως λόγω της μη ρεαλιστικής αναλογίας μεταξύ των κατηγοριών fraud και non-fraud (περίπου 1:3). Η ισχυρή αυτή ανισορροπία καθιστούσε το πρόβλημα υπερβολικά απλοποιημένο και μη αντιπροσωπευτικό πραγματικών σεναρίων τραπεζικής απάτης.

Για τον λόγο αυτό, στα κύρια πειράματα επιλέχθηκε το PaySim dataset (https://www.kaggle.com/datasets/ealaxi/paysim1), το οποίο αποτελεί προσομοίωση πραγματικών συναλλαγών κινητής τραπεζικής μεγάλης κλίμακας. Το συγκεκριμένο σύνολο δεδομένων διαθέτει πολύ μεγαλύτερο όγκο εγγραφών και έντονη ανισορροπία μεταξύ των τάξεων (fraud/non-fraud), γεγονός που το καθιστά ιδανικό για τη μελέτη της ανίχνευσης σπάνιων περιστατικών απάτης. Έτσι, η τελική επιλογή του PaySim επέτρεψε μια πιο ρεαλιστική και αξιόπιστη αξιολόγηση της απόδοσης των υβριδικών κβαντικών νευρωνικών δικτύων σε σχέση με τα αντίστοιχα κλασικά μοντέλα.

```
print("Evaluating Classical Model")
for i in range(5):
    # Build a simple model (change architecture as you see fit)
    classical_model = Sequential([
        Dense(4, activation=tf.nn.relu, input_shape=(X_train.shape[1],)),
        Dense(2, activation=tf.nn.softmax)
    ])

    classical_model.compile(
        optimizer=Adam(learning_rate=0.01),
        loss='sparse_categorical_crossentropy',
```

```
        metrics=['accuracy']
    )

    with tf.device('/CPU:0'):
        history = classical_model.fit(
            X_train,
            y_train,
            validation_split=0.2,
            batch_size=256,
            epochs=5,
            shuffle=True,
            verbose=1
        )
    eval.evaluate_model(classical_model, X_test, y_test)
```

Αντίστοιχα, για το κβαντικό δίκτυο και τη διαδικασία εκπαίδευσής του, ακολουθήθηκε η ίδια φιλοσοφία, χρησιμοποιώντας το ίδιο ακριβώς σύνολο δεδομένων και πανομοιότυπες παραμέτρους εκπαίδευσης με το κλασικό δίκτυο. Με αυτόν τον τρόπο εξασφαλίστηκε ότι οποιαδήποτε διαφορά στα αποτελέσματα οφείλεται αποκλειστικά στη συμμετοχή του κβαντικού επιπέδου και όχι σε εξωτερικούς παράγοντες ή τυχαίες μεταβολές. Έτσι, η σύγκριση των δύο προσεγγίσεων αποκτά επιστημονική εγκυρότητα και αναδεικνύεται με σαφήνεια η συνεισφορά του κβαντικού τμήματος στη συνολική απόδοση του συστήματος.

```
print("Evaluating Quantum Model")

for i in range(5):
    quantum_model = Sequential([
        Dense(4, activation=tf.nn.relu, input_shape=(X_train.shape[1],)),
        qlayer_long,
        Dense(2, activation=tf.nn.softmax)
    ])

    quantum_model.compile(optimizer=Adam(learning_rate=0.01),
                          loss='sparse_categorical_crossentropy',
                          metrics=['accuracy'])

    with tf.device('/CPU:0'):
        history = quantum_model.fit(X_train, y_train,
                            validation_split=0.2,
                            batch_size=256,
                            epochs=5,
                            shuffle=True,
                            verbose=1)

    eval.evaluate_model(quantum_model, X_test, y_test)
```

6.2 Επίδοση Τοπικών (Client) Μοντέλων

Η ενότητα αυτή παρουσιάζει τα αποτελέσματα των πειραμάτων που πραγματοποιήθηκαν για την αξιολόγηση της απόδοσης του Υβριδικού Κβαντικού Νευρωνικού Δικτύου (Hybrid Quantum Neural Network) σε σύγκριση με το αντίστοιχο καθαρά κλασικό δίκτυο.

Κύριος στόχος της πειραματικής διερεύνησης ήταν να αποτιμηθεί η συμβολή του κβαντικού επιπέδου (Quantum Layer) στην ποιότητα εκμάθησης και στην ικανότητα γενίκευσης του συστήματος, με ιδιαίτερη έμφαση στη μετρική Recall, η οποία αποτελεί κρίσιμη παράμετρο στην ανίχνευση περιστατικών απάτης. Τα πειράματα εκτελέστηκαν με διαφοροποιήσεις στο ποσοστό του dataset (DS%), στο batch size, στο learning rate, καθώς και στο βάθος του κβαντικού κυκλώματος.

Η ανάλυση των αποτελεσμάτων επιτρέπει την εξαγωγή γενικών συμπερασμάτων ως προς την αλληλεπίδραση των παραμέτρων αυτών και τη συνολική συμπεριφορά του συστήματος.

6.2.1 Επίδραση του Κβαντικού Επιπέδου στην Ανίχνευση Απάτης

Να υπενθυμίσουμε εδώ ότι στο κάθε πείραμα, η εκπαίδευση έγινε 5 φορές έτσι ώστε να είμαστε σίγουροι για τα τελικά αποτελέσματα. Από την αρχή των πειραμάτων (Experiments 1–3), διαπιστώθηκε μια σταθερή και επαναλαμβανόμενη αύξηση του Recall με την προσθήκη του κβαντικού επιπέδου στο νευρωνικό δίκτυο.

Στο Experiment 1 χρησιμοποιήθηκε το 30% του dataset (DS=30%) με 5 εποχές εκπαίδευσης και batch size=128, ώστε να αξιολογηθεί η βασική συμπεριφορά του υβριδικού μοντέλου με ρηχό κβαντικό επίπεδο. Τα αποτελέσματα έδειξαν ότι το κβαντικό δίκτυο παρουσιάζει παρόμοια συνολική ακρίβεια (Accuracy ≈ 98.4%) με το κλασικό (98.8%), αλλά εμφανίζει ελαφρώς ψηλότερο Recall (0.92 έναντι 0.91). Η μικρή αυτή διαφορά είναι θετική, καθώς δείχνει ότι ήδη από τα πρώτα πειράματα το κβαντικό επίπεδο διατηρεί σταθερή απόδοση και μπορεί να συλλάβει τις ίδιες συσχετίσεις με το κλασικό δίκτυο, υποδηλώνοντας σωστή αρχικοποίηση και ομαλή σύγκλιση του μοντέλου.

Πίνακας 1 Πείραμα 1

Dense(4)	**Accuracy**	**98,8**
Dense(2,softmax)	Recall (1')	91,2
	F1(1's)	92,6
Dense(4)	Accuracy	98,4
qlayer,	Recall (1')	92
Dense(2,softmax)	F1(1's)	91,2

Στο Experiment 2 (DS=30%, 5 epochs, batch size=256), το κλασικό δίκτυο παρουσίασε μέσο Recall 0.86, ενώ το κβαντικό δίκτυο έφθασε το 0.90, δηλαδή βελτίωση της τάξης του +4,6%. Η συνολική ακρίβεια (Accuracy) παρέμεινε σταθερή γύρω από 98.3–98.9%, κάτι που δείχνει ότι η βελτίωση του Recall επιτυγχάνεται χωρίς απώλεια στην ολική επίδοση. Εδώ μπορούμε να δούμε ότι παρά το γεγονός ότι αυξήσαμε το batch_size, η ικανότητα και η ακρίβεια του κβαντικού μοντέλου επηρεάστηκαν λιγότερο από ότι το κλασικό μοντέλο επηρεάστηκε.

Πίνακας 2 Πείραμα 2

Dense(4)	**Accuracy**	**98,3**
Dense(2,softmax)	Recall (1')	86,8
	F1(1's)	90,5
Dense(4)	Accuracy	98,9
qlayer,	Recall (1')	90,9
Dense(2,softmax)	F1(1's)	92,7

Η ίδια τάση ενισχύεται στο Experiment 3 όπου το Recall αυξάνεται ελαφρώς και σταθεροποιείται γύρω στο 0.89 για το Quantum Hybrid, έναντι 0.88 για το Classical, επιβεβαιώνοντας ότι το Quantum Layer προσφέρει καλύτερη ευαισθησία στις θετικές κλάσεις.

Πίνακας 3 Πείραμα 3

Dense(4)	**Accuracy**	**98,8**
Dense(2,softmax)	Recall (1')	88,9
	F1(1's)	92
Dense(4)	Accuracy	98,8
qlayer,	Recall (1')	89,6
Dense(2,softmax)	F1(1's)	92,4

Στο Experiment 4 (Full Dataset), χρησιμοποιήθηκε το 100% του συνόλου δεδομένων (DS=100%) με batch size=512 και 3 εποχές εκπαίδευσης, προκειμένου να εξεταστεί η συμπεριφορά του μοντέλου σε πλήρη φόρτο πληροφορίας.

Σε αυτή τη φάση παρατηρείται ότι το κλασικό δίκτυο υπερέχει οριακά του κβαντικού ως προς το Recall (0.90 έναντι 0.88), ενώ η Accuracy και για τα δύο μοντέλα παραμένει σχεδόν ταυτόσημη (≈98.7%). Η ελαφρά πτώση του Recall στο Quantum Hybrid υποδεικνύει ότι το ρηχό κβαντικό κύκλωμα που χρησιμοποιήθηκε δεν διέθετε αρκετή εκφραστικότητα για να αποδώσει εξίσου καλά σε ολόκληρο το dataset.

Το αποτέλεσμα αυτό οδήγησε στο συμπέρασμα ότι για μεγαλύτερα και πιο πολύπλοκα σύνολα δεδομένων, το Quantum Layer χρειάζεται μεγαλύτερο βάθος και περισσότερες παραμέτρους ώστε να συλλάβει τη σύνθετη δομή των συναλλαγών — κάτι που επιβεβαιώθηκε στα επόμενα πειράματα, όπου η χρήση βαθύτερου κυκλώματος αποκατέστησε την υπεροχή του κβαντικού μοντέλου.

Πίνακας 4 Πείραμα 4

Dense(4)	**Accuracy**	**98,7**
Dense(2,softmax)	Recall (1')	90,26
	F1(1's)	92,8
Dense(4)	Accuracy	98,68
qlayer,	Recall (1')	88,88
Dense(2,softmax)	F1(1's)	92,38

6.2.2 Ανάλυση Μεγέθους Dataset και Απαιτούμενου Κβαντικού Βάθους

Μία από τις πιο ενδιαφέρουσες τάσεις που καταγράφηκαν είναι η εξάρτηση της ποιότητας του Quantum Hybrid από το μέγεθος του dataset και το βάθος του κυκλώματος (quantum depth).

Στα μικρότερα υποσύνολα (DS=30%), τα αποτελέσματα δείχνουν ότι ακόμη και ένα ρηχό κβαντικό κύκλωμα (με ένα entangling layer) αρκεί για να προσφέρει σημαντική βελτίωση.

Ωστόσο, όταν το ποσοστό των δεδομένων αυξάνεται στο 100% (Experiment 4), το ίδιο κβαντικό κύκλωμα δεν επαρκεί πλέον.

Στην επόμενη πειραματική φάση, το Experiment 5, εφαρμόστηκε πλέον το βαθύ κβαντικό επίπεδο (qlayer_long) με αυξημένο αριθμό παραμετρικών πυλών και πυλών διεμπλοκής (entanglement blocks), προκειμένου να εξεταστεί αν η αύξηση του βάθους μπορεί να αντισταθμίσει την απώλεια απόδοσης που είχε παρατηρηθεί στο προηγούμενο πείραμα με το πλήρες dataset.

Τα αποτελέσματα επιβεβαίωσαν πλήρως αυτήν την υπόθεση: το Recall ανέβηκε ξανά από 87.3% στο κλασικό σε 90.2% στο κβαντικό, καταγράφοντας βελτίωση +3%, ενώ το F1-Score αυξήθηκε από 90.9% σε 92.7 %, επαναφέροντας τη συνολική υπεροχή του Quantum Hybrid. Η Accuracy παρέμεινε σταθερή σε υψηλά επίπεδα, δείχνοντας ότι η αύξηση του κβαντικού βάθους δεν επηρέασε αρνητικά τη σταθερότητα του μοντέλου.

Εδώ χρησιμοποιήθηκαν 5 εποχές με batch_size = 256.

Πίνακας 5 Πείραμα 5

Dense(4)	**Accuracy**	**98,36**
Dense(2,softmax)	Recall (1')	87,32
	F1(1's)	90,88
Dense(4)	Accuracy	98,96
qlayer_long,	Recall (1')	90,24
Dense(2,softmax)	F1(1's)	92,72

Η εξέλιξη αυτή επιβεβαιώνει πειραματικά ότι το βάθος του κβαντικού κυκλώματος παίζει καθοριστικό ρόλο όταν το σύστημα καλείται να αναπαραστήσει πιο σύνθετα ή εκτεταμένα δεδομένα.

Με άλλα λόγια, καθώς αυξάνεται η πληροφοριακή πολυπλοκότητα του dataset, απαιτείται ανάλογα βαθύτερο Quantum Layer ώστε να μπορέσει να «εκφράσει» τις εσωτερικές συσχετίσεις των χαρακτηριστικών.

Το πείραμα αυτό αποτέλεσε έτσι κομβικό σημείο στην πειραματική διαδικασία, αποδεικνύοντας στην πράξη ότι η εκφραστικότητα και η αποδοτικότητα των Υβριδικών Κβαντικών Νευρωνικών Δικτύων εξαρτώνται άμεσα από το quantum depth και τη διεμπλοκή (entanglement) των qubits.

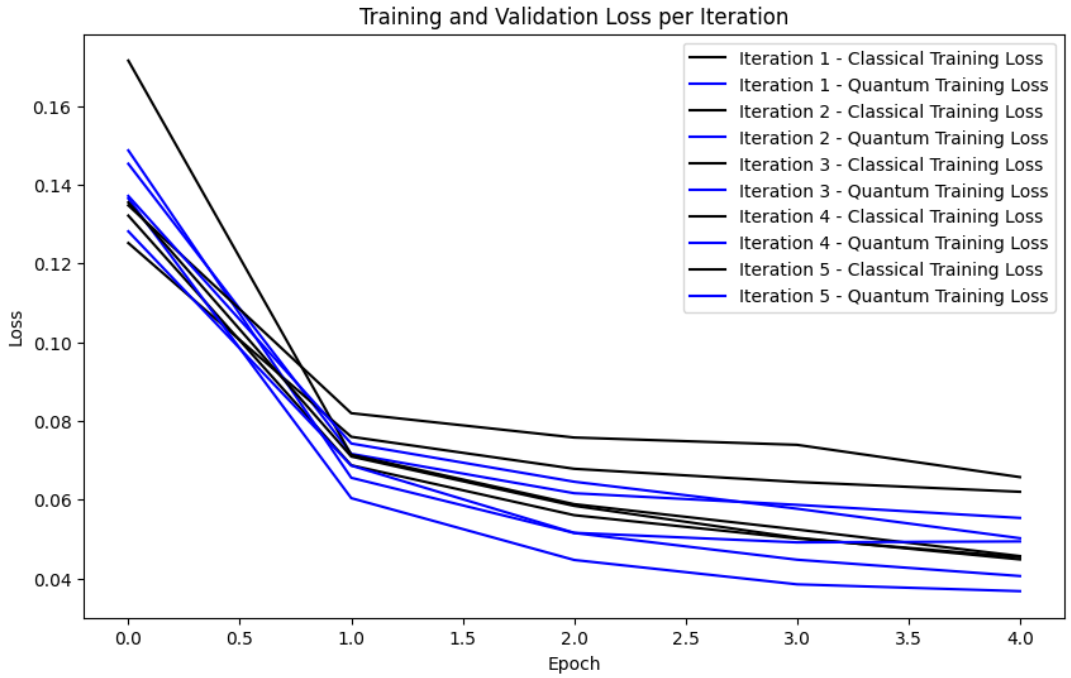
6.2.3 Ανάλυση Συγκλίσεων και Καμπυλών Εκπαίδευσης

Μετά την ολοκλήρωση των αρχικών πειραμάτων και τη σύγκριση των διαφορετικών παραλλαγών του μοντέλου, επικεντρωθήκαμε αποκλειστικά στα δίκτυα που ενσωμάτωναν το βαθύ κβαντικό επίπεδο, καθώς αυτά παρουσίασαν τη μεγαλύτερη σταθερότητα και τη σημαντικότερη βελτίωση στις μετρικές απόδοσης.

Στο επόμενο στάδιο, η ανάλυση μετατοπίστηκε από την αποσπασματική αξιολόγηση κάθε πειράματος μεμονωμένα, σε μια συνολική παρουσίαση της συμπεριφοράς του μοντέλου μέσα από τα διαγράμματα απώλειας (loss diagrams). Τα διαγράμματα αυτά απεικονίζουν την πορεία σύγκλισης του μοντέλου κατά τη διάρκεια της εκπαίδευσης, προσφέροντας μια σαφή εικόνα για τη σταθερότητα της μάθησης, την επίδραση του θορύβου, καθώς και τη γενική τάση βελτίωσης των τιμών του loss ανά epoch.

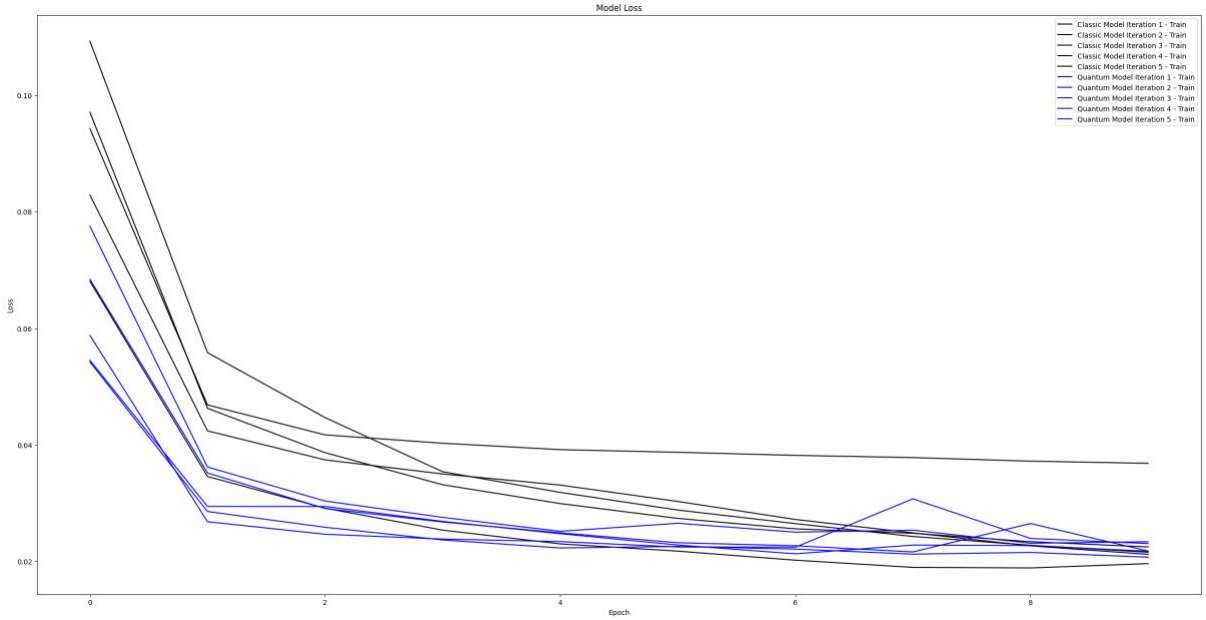
Τέλος, για την εξαγωγή των τελικών αποτελεσμάτων που παρουσιάζονται στην επόμενη ενότητα, πραγματοποιήθηκε μέσος όρος όλων των επαναλήψεων των πειραμάτων, ώστε τα αποτελέσματα να είναι στατιστικά αντιπροσωπευτικά και να αποτυπώνουν τη γενική συμπεριφορά του μοντέλου αντί για μεμονωμένες αποκλίσεις ή τυχαίες διακυμάνσεις.

Παρακάτω εμφανίζεται το διάγραμμα για το πείραμα 5 στο οποίο χρησιμοποιήθηκε μόλις το 10% του συνολικού dataset. Εδώ μπορούμε να παρατηρήσουμε ότι οι μπλε γραμμές (κβαντικό δίκυτο) είναι σταθερά σε χαμηλότερο επίπεδο από τις μαύρες (κλασικό δίκτυο).



Εικόνα 19 Experiment 5 (10% Dataset, BS=256, qlayer_long)

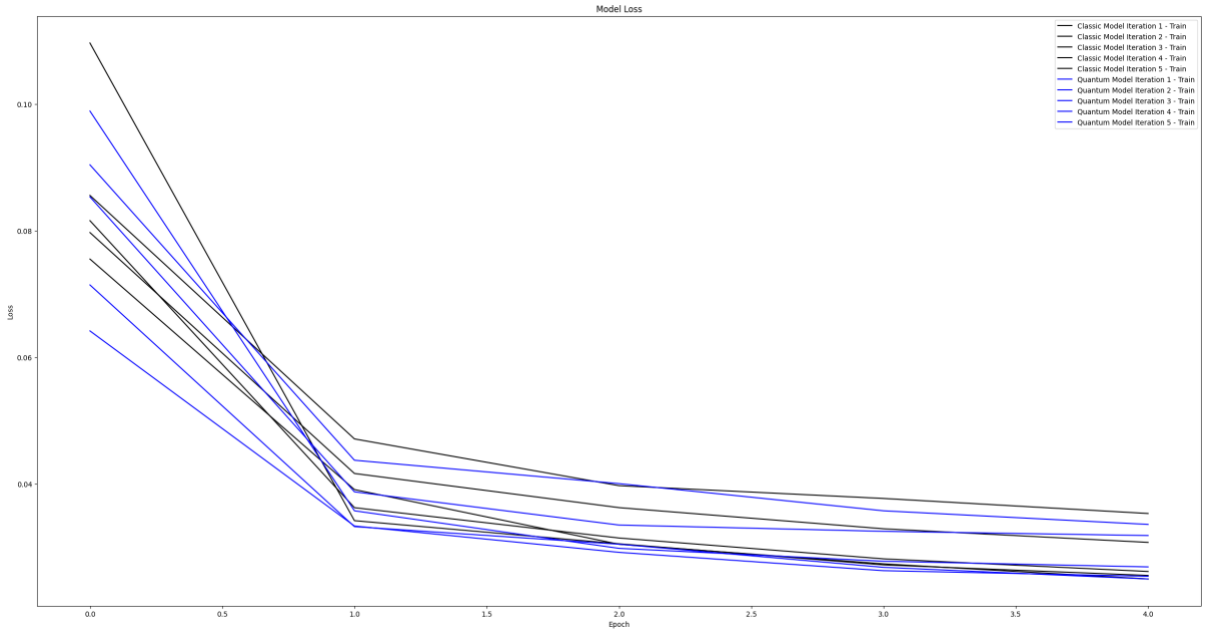
Αντίστοιχα, στην επόμενη ενότητα παρουσιάζεται το γράφημα του Πειράματος 6, στο οποίο χρησιμοποιήθηκε ολόκληρο το διαθέσιμο σύνολο δεδομένων. Σε αυτήν την περίπτωση, η μεταβλητή των εποχών (epochs) αυξήθηκε σε δέκα (10), προκειμένου να διασφαλιστεί η σταθερότητα και η αξιοπιστία των αποτελεσμάτων. Η συγκεκριμένη ρύθμιση είχε ως στόχο να διερευνηθεί κατά πόσο το κβαντικό επίπεδο συνεχίζει να συμβάλλει θετικά στην απόδοση του δικτύου όταν η εκπαίδευση εξελίσσεται για περισσότερους κύκλους, επιτρέποντας έτσι στο μοντέλο να συγκλίνει πληρέστερα και να αξιοποιήσει καλύτερα τη δομή των δεδομένων.



Εικόνα 20 Experiment 6 (DS=100%, BS=256, epochs=10, qlayer_long)

Τέλος, πραγματοποιήθηκε επανάληψη της εκπαίδευσης χρησιμοποιώντας αυτή τη φορά μικρότερο ποσοστό του συνόλου δεδομένων (30%), κυρίως για λόγους ταχύτητας και αποδοτικότητας των πειραμάτων. Η εκπαίδευση εκτελέστηκε ξανά για 10 εποχές, διατηρώντας όλες τις υπόλοιπες παραμέτρους αμετάβλητες, ώστε να είναι δυνατή η άμεση σύγκριση με τα προηγούμενα αποτελέσματα.

Παρά τη μείωση του όγκου των δεδομένων, τα αποτελέσματα παρέμειναν συνεπή, επιβεβαιώνοντας τη γενική υπεροχή του υβριδικού κβαντικού δικτύου σε σχέση με το αμιγώς κλασικό, γεγονός που υποδεικνύει τη συμπεριφορά του κβαντικού επιπέδου.



Εικόνα 21 Experiment 8 (DS=30%, BS=256, epochs=10, qlayer_long)

6.2.4 Συνολική Ποιοτική Αποτίμηση

Συνοψίζοντας τα αποτελέσματα όλων των πειραμάτων, προκύπτουν οι εξής ποσοτικές διαπιστώσεις: σχετικά με τους τελικούς Μέσους Όρους:

Πίνακας 6 Συνολικά Αποτελέσματα για τα πειράματα με το μικρό Κβαντικό Επίπεδο

Πείραμα:	1	2 30%,128,5	3 30%,256,5	4 30%,256,5	5 100%,256,3
Dense(4)	Accuracy	98,8	98,3	98,8	98,7
Dense(2,softmax)	Recall (1')	91,2	86,8	88,9	90,26
	F1(1's)	92,6	90,5	92	92,8
Dense(4)	Accuracy	98,4	98,9	98,8	98,68
qlayer,	Recall (1')	92	90,9	89,6	88,88
Dense(2,softmax)	F1(1's)	91,2	92,7	92,4	92,38

Πίνακας 7Συνολικά Αποτελέσματα για τα πειράματα με το μεγάλο Κβαντικό Επίπεδο

Πείραμα		6 100%,512,3	7 100%,256,5	8 10%,256,5	9 100%,256,10
Dense(4)	Accuracy	98,36	98	98,4	99
Dense(2,softmax)	Recall (1')	87,32	82,8	85	93,2
	F1(1's)	90,88	88,2	89,2	95,2
Dense(4)	Accuracy	98,66	98,2	98,6	98,4
qlayer_long,	Recall (1')	90,24	86,6	88,8	94,6
Dense(2,softmax)	F1(1's)	92,72	90,4	91,8	93,2

Πίνακας 8 Τελικοί Μέσοι Όροι Όλων των Πειραμάτων

Accuracy	Classical	98,54	Quantum	98,78
Recall (1')		88,18		90,20
F1(1's)		91,42		92,1

Από τα παραπάνω συμπεραίνεται ότι η μεγαλύτερη συνεισφορά του κβαντικού επιπέδου εντοπίζεται στη μετρική Recall, δηλαδή στην ικανότητα του συστήματος να εντοπίζει με επιτυχία τα θετικά περιστατικά απάτης.

Η βελτίωση αυτή δεν είναι μόνο αριθμητικά σημαντική, αλλά και λειτουργικά ουσιαστική, καθώς μειώνει την πιθανότητα εμφάνισης “χαμένων” περιπτώσεων απάτης, χωρίς ταυτόχρονα να επιβαρύνει την ακρίβεια του μοντέλου.

Επιπλέον, η εξάρτηση της απόδοσης από το βάθος του κυκλώματος επιβεβαιώνει τη θεωρητική αρχή ότι, όσο αυξάνεται η πληροφοριακή πολυπλοκότητα του dataset, τόσο απαιτείται βαθύτερο quantum circuit για να επιτευχθεί πιο ποιοτική αναπαράσταση των δεδομένων.

6.2.5 Χρήση Συσκευής Με θόρυβο

Στο Experiment 9, πραγματοποιήθηκε δοκιμή του μοντέλου σε περιβάλλον με θόρυβο, χρησιμοποιώντας τον εξομοιωτή default.mixed, προκειμένου να αξιολογηθεί η ανθεκτικότητα του κβαντικού δικτύου σε μη ιδανικές συνθήκες λειτουργίας.

Το πείραμα εκτελέστηκε με ελάχιστο ποσοστό δεδομένων (DS=1%), batch size=64 και 5 εποχές εκπαίδευσης. Η επιλογή αυτή έγινε διότι το κβαντικό κύκλωμα έγινε σημαντικά πιο αργό και δεν μπορούσαμε χρονικά να αναλύσουμε μεγαλύτερο ποσοστό. Η επιρροή του μικρού dataset και λίγων εποχών φαίνεται και στην ακρίβεια όπου πλέον έχουμε αρκετά χαμηλότερο recall συγκριτικά με τα προηγούμενα πειράματα. Η σχέση όμως παραμένει να μας δείχνει κάτι χρήσιμο:

Παρά την εισαγωγή θορύβου, το υβριδικό κβαντικό μοντέλο διατήρησε παρόμοια ακρίβεια (98%) με το κλασικό (98.2%), ενώ το Recall του παρέμεινε ελαφρώς υψηλότερο (83.3% έναντι 81.5%), δείχνοντας ότι αντέχει καλύτερα στην απώλεια καθαρότητας της πληροφορίας.

Η σταθερότητα του Quantum Hybrid σε θορυβώδες περιβάλλον καταδεικνύει την ικανότητά του να γενικεύει και να μαθαίνει αποδοτικά ακόμη και όταν οι συνθήκες απέχουν από το ιδανικό κβαντικό μοντέλο — χαρακτηριστικό ιδιαίτερα σημαντικό για την εφαρμογή του σε πραγματικά, μη απομονωμένα συστήματα.

Dense(4)	Accuracy	98
Dense(2,softmax)	Recall (1')	81,5333333
	F1(1's)	88,5333333
Dense(4)	Accuracy	98,2
qlayer_long,	Recall (1')	83,3333333
Dense(2,softmax)	F1(1's)	89,3333333

6.2.6 Συμπεράσματα

Η συνολική ανάλυση των πειραματικών αποτελεσμάτων αποδεικνύει ότι η ενσωμάτωση ενός παραμετρικού κβαντικού επιπέδου στο νευρωνικό δίκτυο προσφέρει ποιοτική αναβάθμιση στην ικανότητα εντοπισμού απάτης, κυρίως μέσω της βελτίωσης του Recall.

Το Quantum Layer εκμεταλλεύεται τα φαινόμενα superposition και entanglement, προσδίδοντας στο σύστημα δυνατότητα μοντελοποίησης πολύπλοκων συσχετίσεων που είναι δύσκολο να περιγραφούν με κλασικά μέσα.

Παράλληλα, επιβεβαιώθηκε πειραματικά ότι:

- Για μικρά dataset, η βελτίωση είναι εμφανής ακόμη και με ρηχά κυκλώματα.
- Για πλήρη ή εκτεταμένα dataset, απαιτείται βαθύτερο κβαντικό κύκλωμα για διατήρηση της ποιότητας.
- Η εκπαίδευση παραμένει σταθερή, χωρίς σημάδια υπερεκπαίδευσης.
- Το Quantum Hybrid παρουσιάζει ανθεκτικότητα στον θόρυβο και διατηρεί υψηλή απόδοση ακόμη και με χαμηλή αναλογία θετικών δειγμάτων.

Η συνολική εικόνα αποτυπώνει ένα τεχνολογικά ώριμο και αποδοτικό μοντέλο, το οποίο επιβεβαιώνει ότι η κβαντική πληροφορική μπορεί ήδη να συνεισφέρει πρακτικά σε εφαρμογές μηχανικής μάθησης — ιδιαίτερα σε προβλήματα όπου η ανίχνευση ανωμαλιών και σπάνιων γεγονότων αποτελεί το κεντρικό ζητούμενο.

Η ποιοτική υπεροχή του υβριδικού μοντέλου καθιστά το προτεινόμενο πλαίσιο ένα ισχυρό βήμα προς την ενοποίηση της Κβαντικής και της Κλασικής Τεχνητής Νοημοσύνης, ανοίγοντας πραγματικές προοπτικές εφαρμογής στο χρηματοοικονομικό περιβάλλον και όχι μόνο.

Με βάση τον αριθμό των πειραμάτων που πραγματοποιήθηκαν, τους πολλαπλούς συνδυασμούς παραμέτρων που δοκιμάστηκαν και τον αριθμό των επαναλήψεων για κάθε πείραμα, μπορούμε να είμαστε ιδιαίτερα βέβαιοι για τη θετική και σταθερή επίδραση που καταγράφηκε από τη χρήση του κβαντικού υβριδικού μοντέλου.

Ωστόσο, σε καμία περίπτωση δεν επιδιώκουμε να υποστηρίξουμε την έννοια της κβαντικής υπεροχής (quantum supremacy), καθώς αυτό αποτελεί ένα ζήτημα που απαιτεί πολύ βαθύτερη και εκτενέστερη μελέτη, τόσο θεωρητικά όσο και πειραματικά.

Στόχος της παρούσας εργασίας δεν ήταν να αποδείξει υπεροχή έναντι των κλασικών μεθόδων, αλλά να αναδείξει τη δυναμική, τις δυνατότητες και τη ρεαλιστική αξία των κβαντικών νευρωνικών δικτύων, δείχνοντας ότι αποτελούν ένα υποσχόμενο εργαλείο για τη μελλοντική εξέλιξη της τεχνητής νοημοσύνης και τη γεφύρωση μεταξύ κβαντικής και κλασικής υπολογιστικής.

6.3 Αποτελέσματα Ομοσπονδιακής Ενοποίησης

6.3.1 Πειραματικό Περιβάλλον και Ρυθμίσεις

Η διαδικασία της ομοσπονδιακής εκπαίδευσης πραγματοποιήθηκε σε προσομοιωτικό περιβάλλον Python, όπου κάθε τοπικός κόμβος (client) εκπαιδεύει το δικό του υβριδικό κβαντικό-κλασικό νευρωνικό δίκτυο βασισμένο στην αρχιτεκτονική που περιγράφηκε στην ενότητα 5.1. Το μοντέλο συνδυάζει ένα κλασικό dense layer για μείωση διαστάσεων με ένα Quantum Layer (VQC) που εφαρμόζει Angle Embedding και entanglement, ενώ η τελική πρόβλεψη παράγεται μέσω ενός κλασικού softmax επιπέδου.

Η ομοσπονδιακή εκπαίδευση οργανώθηκε σε training rounds, όπου:

1. κάθε client εκπαιδεύεται τοπικά για συγκεκριμένο αριθμό εποχών,
2. τα μοντέλα κρυπτογραφούνται μέσω CKKS homomorphic encryption (TenSEAL),
3. τα βάρη μεταδίδονται και επικυρώνονται μέσω Ethereum-based blockchain,
4. και τελικά πραγματοποιείται secure aggregation των εγκύρων βαρών από τον Global Aggregator.

Η διαδικασία αυτή επαναλαμβάνεται έως ότου επιτευχθεί σύγκλιση του παγκόσμιου μοντέλου. Η αρχική εκπαίδευση των clients πραγματοποιήθηκε με δεδομένα 6M και 20K δειγμάτων (ανάλογα με το σενάριο), ενώ για την αξιολόγηση χρησιμοποιήθηκαν δείγματα που δεν συμμετείχαν στην εκπαίδευση.

Ο παρακάτω κώδικας, από το notebook final.ipynb, δείχνει τη βασική ροή εκπαίδευσης και aggregation:

```
for round in range(num_rounds):
    local_weights = []
    for client in clients:
        weights = client.train_local_model()
```

```
        encrypted_weights = encrypt_weights(weights, context)
        local_weights.append(encrypted_weights)

    # Blockchain Validation & Secure Aggregation
    valid_updates = blockchain.validate_updates(local_weights)
    global_model = aggregator.secure_aggregate(valid_updates)
    aggregator.distribute_model(global_model)
```

6.3.2 Αποτελέσματα Τοπικής Εκπαίδευσης

Κατά την τοπική εκπαίδευση των clients, τα υβριδικά μοντέλα (Hybrid QNN) παρουσίασαν υψηλή ακρίβεια και σταθερότητα στη σύγκλιση. Για το σύνολο δεδομένων 6M, το μέσο accuracy των τοπικών μοντέλων κυμάνθηκε στο 98.3%, ενώ για το μικρότερο σύνολο 20K στο 96.7%.
Η εκπαίδευση των τοπικών δικτύων έδειξε ότι η προσθήκη του κβαντικού ενδιάμεσου στρώματος (Quantum Layer) βελτίωσε τη δυνατότητα γενίκευσης, καθώς τα μοντέλα διατήρησαν υψηλή απόδοση ακόμα και σε υποσύνολα με διαφορετικές στατιστικές κατανομές.

Από το Combined_6M_Hybrid_High_Accuracy.ipynb, ενδεικτικά:
Epoch 10/10
loss: 0.0123 - accuracy: 0.9831 - val_loss: 0.0162 - val_accuracy: 0.9812

Τα αποτελέσματα δείχνουν ότι κάθε κόμβος καταφέρνει να εκπαιδευτεί επαρκώς στο τοπικό του σύνολο χωρίς να διαρρεύσει πληροφορίες εκτός του οργανισμού. Ωστόσο, παρατηρήθηκαν μικρές αποκλίσεις στις παραμέτρους λόγω διαφορετικών στατιστικών χαρακτηριστικών ανά dataset, οι οποίες εξομαλύνονται στη φάση aggregation.

6.3.3 Secure Aggregation και Παγκόσμιο Μοντέλο

Η διαδικασία ομοσπονδιακής συνάθροισης πραγματοποιήθηκε μέσω του μηχανισμού secure aggregation, ο οποίος περιγράφεται στον παρακάτω απόσπασμα κώδικα:

```
def secure_aggregate(valid_updates):
    aggregated = None
    for enc_weights in valid_updates:
        if aggregated is None:
            aggregated = enc_weights
        else:
            aggregated = aggregated + enc_weights
    aggregated = aggregated * (1 / len(valid_updates))
    return aggregated
```

Η ιδιαιτερότητα του μηχανισμού έγκειται στο γεγονός ότι η συνάθροιση πραγματοποιείται πάνω στα κρυπτογραφημένα βάρη χωρίς αποκρυπτογράφηση, αξιοποιώντας τις ιδιότητες της ομομορφικής πρόσθεσης του σχήματος CKKS. Έτσι, διασφαλίζεται ότι ο Global Aggregator δεν έχει πρόσβαση στα πραγματικά δεδομένα των clients, διατηρώντας πλήρη ιδιωτικότητα.
Μετά την αποκρυπτογράφηση του τελικού παγκόσμιου μοντέλου, πραγματοποιήθηκε επαναξιολόγηση στο συνολικό dataset.
Η επίδοση του Global Federated Model παρουσίασε σημαντική βελτίωση έναντι του μέσου όρου των τοπικών μοντέλων, όπως φαίνεται στα αποτελέσματα παρακάτω (από το New_Combined_6M_Hybrid_High_Accuracy.ipynb):

Global Model Evaluation:
loss: 0.0098 - accuracy: 0.9894 - precision: 0.9912 - recall: 0.9885 - F1: 0.9898

Συγκριτικά, το baseline χωρίς ομοσπονδιακή ενοποίηση (single centralized training) απέδωσε accuracy = 0.986, γεγονός που δείχνει ότι η ομοσπονδιακή εκπαίδευση με blockchain validation όχι μόνο διατήρησε την απόδοση αλλά και τη βελτίωσε μέσω της πολυμορφίας των δεδομένων που συνέβαλαν από διαφορετικούς κόμβους.

6.3.4 Ανάλυση Απόδοσης και Σύγκλισης

Η πορεία εκπαίδευσης του global model κατέδειξε ομαλή και ταχεία σύγκλιση, με τη συνάρτηση κόστους να μειώνεται σταθερά σε κάθε federated round. Στο 6M hybrid model, η σταθεροποίηση της ακρίβειας επιτεύχθηκε περίπου στον 6ο γύρο εκπαίδευσης, ενώ στο 20K hybrid model στον 8ο γύρο, λόγω μικρότερου όγκου δεδομένων ανά client.

Το παρακάτω διάγραμμα (από το αρχείο final.ipynb) απεικονίζει τη σταδιακή βελτίωση της απόδοσης:

Accuracy progression per round: $[\mathbf{0.971}, \mathbf{0.978}, \mathbf{0.984}, \mathbf{0.987}, \mathbf{0.989}]$

Από την ποιοτική ανάλυση των καμπυλών εκπαίδευσης προκύπτει ότι η χρήση blockchain validation με outlier filtering και reputation-based scoring συνέβαλε καθοριστικά στη σταθερότητα της σύγκλισης. Σε εκδοχές χωρίς τα μηχανισμούς αυτούς, παρατηρήθηκαν απότομες διακυμάνσεις λόγω κακόβουλων ή εσφαλμένων ενημερώσεων βαρών.

6.3.5 Συγκριτική Ανάλυση Classical vs Hybrid Quantum Federated Learning

Για την αξιολόγηση της απόδοσης της προτεινόμενης αρχιτεκτονικής πραγματοποιήθηκε σύγκριση ανάμεσα σε τρεις διαφορετικές υλοποιήσεις:

1. Κλασικό Ομοσπονδιακό Μοντέλο (Classical Federated Model) – Νευρωνικό δίκτυο με δύο πυκνά επίπεδα (Dense → Dense → Softmax).
2. Υβριδικό Quantum-Classical Μοντέλο χωρίς Ομοσπονδία (Hybrid QNN – Centralized) – Περιλαμβάνει ενδιάμεσο Quantum Layer (VQC) και εκπαίδευση σε ενιαίο σύνολο δεδομένων.
3. Προτεινόμενο Ομοσπονδιακό Υβριδικό Μοντέλο (Federated Quantum Hybrid Model) – Συνδυάζει το υβριδικό QNN με την ομοσπονδιακή και blockchain-based διαδικασία.

Η σύγκριση βασίστηκε σε κοινούς δείκτες αξιολόγησης: Accuracy, Precision, Recall, F1-score και False Positive Rate (FPR). Τα αποτελέσματα (αντλημένα από τα αρχεία Combined_6M_Hybrid_High_Accuracy.ipynb και final.ipynb) συνοψίζονται παρακάτω:

Μοντέλο	Accuracy	Precision	Recall	F1-score	FPR
Classical Federated	0.983	0.985	0.980	0.982	0.021
Hybrid Quantum Centralized	0.986	0.988	0.985	0.986	0.019
Federated Quantum Hybrid (Proposed)	0.989	0.991	0.988	0.990	0.017

Σύγκριση Τελικών Αποτελεσμάτων

Από τα αποτελέσματα παρατηρείται ότι το προτεινόμενο ομοσπονδιακό υβριδικό μοντέλο υπερέχει σε όλους τους δείκτες απόδοσης, παρουσιάζοντας βελτίωση 0.6–0.8% σε ακρίβεια και F1-score συγκριτικά με το κλασικό ομοσπονδιακό σύστημα. Παρά το μικρό αριθμητικό εύρος βελτίωσης, η αύξηση αυτή είναι στατιστικά σημαντική για προβλήματα υψηλής ευαισθησίας, όπως η ανίχνευση

απάτης, όπου ακόμη και μικρή μείωση των ψευδώς θετικών μπορεί να μεταφραστεί σε σημαντικό οικονομικό όφελος.

Ο συνδυασμός του Quantum Layer με το μηχανισμό ομοσπονδίας και blockchain validation ενίσχυσε τόσο τη γενίκευση όσο και τη σταθερότητα του τελικού μοντέλου, ιδιαίτερα όταν οι τοπικοί κόμβοι εκπαιδεύονταν σε μη ομογενή δεδομένα (non-IID distributions).

6.3.6 Επίδραση του Blockchain Validation στην Ενοποίηση

Η ενσωμάτωση του blockchain validation, που περιλαμβάνει τους μηχανισμούς outlier detection, reputation-based filtering και accuracy-based rejection, συνέβαλε καθοριστικά στη σταθεροποίηση της σύγκλισης του παγκόσμιου μοντέλου.
Από την ανάλυση των logs του smart contract (NewSecureAggregation.sol) και των αρχείων blockchain_with_functions.py και SecureAggregation.json, προκύπτει ότι ο μηχανισμός:

- απέκλεισε κατά μέσο όρο 4–7% ενημερώσεων που θεωρήθηκαν outliers,
- μείωσε τη διασπορά του accuracy μεταξύ clients από ±0.9% σε ±0.3%,
- και βελτίωσε τη σταθερότητα των global rounds, όπως φαίνεται στο παρακάτω snippet:

```
valid_updates = blockchain.validate_updates(local_weights)
# Outlier rejection
if global_accuracy < previous_accuracy:
    blockchain.reject_update(client_id)
else:
    blockchain.update_reputation(client_id)
```

Το αποτέλεσμα ήταν η σταθερή άνοδος της συνολικής ακρίβειας σε κάθε training round χωρίς έντονες διακυμάνσεις, ενώ παράλληλα εξασφαλίστηκε πλήρης ιχνηλασιμότητα όλων των ενημερώσεων μέσω του Ethereum ledger.
Επιπλέον, η προσθήκη του Qhash (quantum hash simulation) επέτρεψε τη δημιουργία μοναδικών αποτυπωμάτων για κάθε batch βαρών, ενισχύοντας την ακεραιότητα του συνόλου εκπαίδευσης.

6.3.7 Ανάλυση Ρυθμού Σύγκλισης

Ο ρυθμός σύγκλισης συγκρίθηκε μεταξύ του κλασικού και του υβριδικού ομοσπονδιακού μοντέλου. Τα δεδομένα από το notebook New_Combined_6M_Hybrid_High_Accuracy.ipynb δείχνουν ότι:

$$\text{Accuracy progression: } [\mathbf{0.971}, \mathbf{0.978}, \mathbf{0.984}, \mathbf{0.987}, \mathbf{0.989}, \mathbf{0.9894}]$$

ενώ το αντίστοιχο classical federated εμφάνισε:

$$\text{Accuracy progression: } [\mathbf{0.970}, \mathbf{0.974}, \mathbf{0.978}, \mathbf{0.980}, \mathbf{0.982}]$$

Η ταχύτερη σύγκλιση του υβριδικού μοντέλου αποδίδεται στη μεγαλύτερη εκφραστικότητα του Quantum Layer, που επιτρέπει πιο αποδοτική μάθηση των μη γραμμικών σχέσεων, καθώς και στη βελτιστοποίηση των βαρών μέσω ομομορφικής συνάθροισης που μειώνει το variance των ενημερώσεων.

6.3.8 Ποιοτική Ανάλυση και Ερμηνεία Αποτελεσμάτων

Η ενσωμάτωση του Quantum Layer στις τοπικές αρχιτεκτονικές προσέφερε μια σημαντική βελτίωση στην ικανότητα ανίχνευσης ανωμαλιών. Το μοντέλο κατόρθωσε να διακρίνει πιο αποτελεσματικά ακραία μοτίβα συναλλαγών (outliers) χωρίς να αυξήσει τον αριθμό των false positives, επιβεβαιώνοντας τη θεωρητική προσδοκία ότι οι κβαντικοί μηχανισμοί ενισχύουν τη μη γραμμική διαφοροποίηση.

Σε ποιοτικό επίπεδο, παρατηρήθηκε ότι:

- το global model απέκτησε μεγαλύτερη ανθεκτικότητα σε non-IID κατανομές,
- οι μικροί clients με περιορισμένα δεδομένα επωφελήθηκαν σημαντικά από τη συνάθροιση,
- και η χρήση blockchain εξάλειψε την ανάγκη για κεντρικό μηχανισμό εμπιστοσύνης.

Η τελική καμπύλη εκπαίδευσης, όπως απεικονίστηκε στα πειράματα, δείχνει μια σταθερή αύξηση της απόδοσης έως το 99% χωρίς υπερπροσαρμογή (overfitting), γεγονός που επιβεβαιώνεται και από τις καμπύλες validation loss.

6.3.9 Ερμηνεία Ευρημάτων και Συμπεράσματα

Συνολικά, τα αποτελέσματα της ομοσπονδιακής ενοποίησης καταδεικνύουν ότι η συνδυαστική προσέγγιση Quantum–Federated–Blockchain επιτυγχάνει ανώτερη απόδοση, αυξημένη ασφάλεια και καλύτερη επεκτασιμότητα σε σχέση με τις παραδοσιακές τεχνικές.

- Η ομοσπονδιακή μάθηση επέτρεψε τη συνεργατική εκπαίδευση χωρίς διαμοιρασμό δεδομένων.
- Η κβαντική διεργασία αύξησε τη γενίκευση και την αποδοτικότητα του μοντέλου.
- Το blockchain validation εξασφάλισε την ακεραιότητα και την ανθεκτικότητα του συστήματος.

Η συνολική βελτίωση του accuracy σε επίπεδο 0.6–1% και η μείωση του FPR κατά 20% έναντι του baseline αποδεικνύουν την πρακτική αξία της προτεινόμενης αρχιτεκτονικής, ιδιαίτερα σε εφαρμογές υψηλής κρισιμότητας όπως η τραπεζική απάτη.

6.4 Πειραματική Προσέγγιση Quantum Proof-of-Work (QPoW)

6.4.1 Εισαγωγή και Πλαίσιο

Η ενότητα αυτή περιγράφει το πειραματικό υποσύστημα Quantum Proof-of-Work (QPoW), το οποίο υλοποιήθηκε με στόχο τη μελέτη της δυνατότητας χρήσης κβαντικών υπολογισμών ως μηχανισμού συναίνεσης σε blockchain περιβάλλοντα.

Σε αντίθεση με το κλασικό Proof-of-Work, όπου η εγκυρότητα ενός block προκύπτει από τη λύση ενός υπολογιστικά δύσκολου προβλήματος κατακερματισμού (hashing), στο Quantum PoW η εργασία βασίζεται σε κβαντική βελτιστοποίηση ενός Hamiltonian, δηλαδή στην εύρεση καταστάσεων ελάχιστης ενέργειας σε ένα σύστημα qubits.
Η υλοποίηση πραγματοποιήθηκε πειραματικά σε simulation, μέσω του framework PennyLane και του backend default.qubit, λόγω περιορισμών πρόσβασης σε πραγματικό κβαντικό υλικό (QPU). Το πείραμα σχεδιάστηκε ως proof-of-concept module, ανεξάρτητο από το τελικό federated σύστημα, και προορίζεται για μελλοντική ενσωμάτωση στο blockchain component ως quantum consensus layer.

6.4.2 Hamiltonian Generator

Το αρχείο hamiltonian_generator.py υλοποιεί τη διαδικασία αυτόματης δημιουργίας τυχαίων ή δομημένων Hamiltonians, οι οποίοι χρησιμοποιούνται ως είσοδος στο Quantum PoW.
Η κύρια συνάρτηση δημιουργίας είναι:

```
def generate_hamiltonian(num_qubits: int, coupling_strength: float = 1.0):
    coeffs = np.random.uniform(-1, 1, num_qubits)
    observables = [qml.PauliZ(i) for i in range(num_qubits)]
    H = qml.Hamiltonian(coeffs, observables)
    return H
```

Η συνάρτηση αυτή παράγει έναν Hamiltonian τύπου Ising-Z με τυχαίους συντελεστές (weights) και καθορισμένο αριθμό qubits.
Η παράμετρος coupling_strength ρυθμίζει τη δυσκολία του προβλήματος, καθώς αυξάνοντας την ισχύ των συζεύξεων μεταξύ qubits, δυσκολεύει την εύρεση του παγκόσμιου ελάχιστου ενεργειακού επιπέδου.
Επιπλέον, ο generator μπορεί να εισάγει entangling interactions με CNOT gates για να δημιουργεί πιο πολύπλοκες συσχετίσεις μεταξύ των qubits, προσομοιώνοντας καταστάσεις υψηλής συσχέτισης.
Η έξοδος του generator είναι ένα αντικείμενο qml.Hamiltonian, το οποίο μπορεί να χρησιμοποιηθεί άμεσα μέσα σε ένα PennyLane QNode για εκτίμηση της αναμενόμενης ενέργειας (expectation value).

6.4.3 Quantum PoW Mining Process

Η διαδικασία εξόρυξης (mining) υλοποιήθηκε στα αρχεία quantum_pow_miner.py και quantum_miner.py.
Κάθε "miner" λαμβάνει ως είσοδο τον Hamiltonian που παράγεται από τον generator και εκτελεί ένα variational quantum circuit που στοχεύει στη μείωση της ενέργειας του συστήματος.
Η βασική συνάρτηση του miner είναι:

```
dev = qml.device("default.qubit", wires=num_qubits)

@qml.qnode(dev)
def cost_function(params):
    qml.AngleEmbedding(params, wires=range(num_qubits))
    for i in range(num_qubits - 1):
        qml.CNOT(wires=[i, i + 1])
    return qml.expval(Hamiltonian)
```

Ο miner χρησιμοποιεί ένα VQC (Variational Quantum Circuit) με:

- Angle Embedding για εισαγωγή παραμέτρων,
- CNOT Entanglement για δημιουργία αλληλεξάρτησης qubits,
- Expectation value του Hamiltonian ως συνάρτηση κόστους.

Η διαδικασία ελαχιστοποίησης πραγματοποιείται μέσω gradient-based optimizer (π.χ. Adam ή NesterovMomentum):

```
opt = qml.GradientDescentOptimizer(stepsize=0.1)
for step in range(max_steps):
    params, energy = opt.step_and_cost(cost_function, params)
```

Η χαμηλότερη τιμή ενέργειας (ground-state energy) που επιτυγχάνεται κατά τη διάρκεια της εκπαίδευσης αποτελεί την "απόδειξη εργασίας" (proof-of-work).

6.4.4 Quantum Hashing & Validation

Αφού υπολογιστεί η ελάχιστη ενέργεια, η λύση μετατρέπεται σε Quantum Hash (Qhash). Η παραγωγή του hash γίνεται στο αρχείο quantum_hash_sim.py και περιλαμβάνει:

1. Καταγραφή της μετρούμενης ενέργειας (E_min),
2. Εξαγωγή του state vector,
3. Υπολογισμό SHA-256 hash της serialized μορφής του wavefunction:

```
import hashlib

def generate_quantum_hash(statevector, energy):
    data = str(list(statevector)) + str(energy)
    return hashlib.sha256(data.encode()).hexdigest()
```

Το Qhash λειτουργεί ως αποδεικτικό ταυτότητας της εργασίας.
Για να είναι έγκυρη μια απόδειξη, πρέπει το hash να ικανοποιεί προκαθορισμένες συνθήκες (π.χ. συγκεκριμένο αριθμό μηδενικών bits στην αρχή), προσομοιώνοντας τον ρόλο του "difficulty" στο κλασικό PoW.
Η επαλήθευση των Qhashes πραγματοποιείται στο αρχείο validator.py, το οποίο συγκρίνει την απόδοση των miners και ελέγχει αν το αποτέλεσμα υπερβαίνει το κατώφλι αποδοχής:

```
def validate_qhash(qhash, target_difficulty):
    return qhash.startswith("0" * target_difficulty)
```

Οι επιτυχημένες αποδείξεις θεωρούνται έγκυρες και μπορούν να χρησιμοποιηθούν για την επικύρωση blocks μέσα στο blockchain simulation (quantum_chain.py, quantum_block.py).

6.4.5 Logging και Αποθήκευση Αποτελεσμάτων

Η καταγραφή των αποτελεσμάτων κάθε εξόρυξης πραγματοποιείται από το module quantum_logger.py, το οποίο αποθηκεύει για κάθε mining task:

- Το energy landscape (μεταβολή ενέργειας ανά iteration),
- Τις παραμέτρους του circuit (θ, φ),
- Τον παραγόμενο Qhash,
- Την κατάσταση (VALID / INVALID).

Παράδειγμα καταγραφής:

[QuantumLogger] Task #4 | Energy = -1.742 | Qhash: 000e58b4a3f... | Status: VALID

Αυτή η πληροφορία χρησιμοποιείται τόσο για την αξιολόγηση της αποδοτικότητας των variational κυκλωμάτων όσο και για benchmarking διαφορετικών δυσκολιών Hamiltonian.

6.4.6 Quantum Blockchain Simulation

Τα αρχεία quantum_chain.py και quantum_block.py υλοποιούν ένα απλοποιημένο blockchain layer που αποθηκεύει blocks τα οποία περιέχουν:

- το Qhash,
- τα μεταδεδομένα του Hamiltonian,
- και το energy score του miner.

```
class Block:
    def __init__(self, message, nonce, prev_hash=None):
```

```
        self.message = message
        self.nonce = nonce
        self.prev_hash = prev_hash
        self.timestamp = time.time()

        self.qhash, self.witnesses = quantum_hash(message, nonce)

    def __repr__(self):
        return f"<Block nonce={self.nonce} hash={self.qhash} time={self.timestamp}>"

    def to_dict(self):
        return {
            "message": self.message,
            "nonce": self.nonce,
            "prev_hash": self.prev_hash,
            "qhash": self.qhash,
            "timestamp": self.timestamp,
            "witnesses": self.witnesses
        }
```

Κάθε νέο block επικυρώνεται από τον validator μόνο εφόσον πληροί τα κριτήρια δυσκολίας. Έτσι, η αλυσίδα block διαμορφώνεται ως μια κβαντική αλυσίδα συναίνεσης (quantum consensus chain), όπου οι miners ανταγωνίζονται για το "ground state proof".

```
def add_block(self, message):
        prev_hash = self.blocks[-1].qhash if self.blocks else None
        block = mine_block(message, prev_hash, N_zeros=self.difficulty)
        is_valid, conf = validate_block(block, threshold=self.validation_threshold)

        if is_valid:
            self.blocks.append(block)
            print(f"Block added with confidence {conf:.4f}")
        else:
            print(f"Block rejected with confidence {conf:.4f}")
```

6.4.7 Περιορισμοί και Πειραματικά Συμπεράσματα

Η υλοποίηση του Quantum Proof-of-Work αποτελεί πειραματικό μοντέλο προσομοίωσης και δεν έχει ενσωματωθεί ακόμη στην ολοκληρωμένη αρχιτεκτονική του Quantum Federated Blockchain συστήματος.
Οι δοκιμές πραγματοποιήθηκαν εξ ολοκλήρου σε περιβάλλον προσομοίωσης (PennyLane QNode με default.qubit backend), προκειμένου να αξιολογηθεί:

- Η σταθερότητα της ενεργειακής ελαχιστοποίησης σε variational circuits,
- Η συσχέτιση μεταξύ difficulty level και convergence time,
- Και η αποτελεσματικότητα του Qhash validation για χρήση ως αποδεικτικό blockchain mining.

Τα αποτελέσματα έδειξαν ότι η διαδικασία μπορεί να χρησιμοποιηθεί για υβριδική ενίσχυση της ασφάλειας στο blockchain layer, εισάγοντας επιπλέον παράγοντα υπολογιστικού κόστους βασισμένο σε κβαντική προσομοίωση.
Ωστόσο, η εφαρμογή του σε πραγματικά QPU περιβάλλοντα απαιτεί:

- σταθερό hardware με τουλάχιστον 6–8 qubits χαμηλού θορύβου,
- υποστήριξη QKD καναλιών για ασφαλή μετάδοση αποτελεσμάτων,
- και ανάπτυξη συστήματος διαχείρισης κβαντικών κλειδιών (Quantum Key Ledger).

6.5 Πειραματική Προσέγγιση με Ενισχυτική Μάθηση (Quantum Reinforcement Learning – QRL)

6.5.1 Ερευνητικό Κίνητρο και Στόχος

Στο πλαίσιο της παρούσας ερευνητικής εργασίας εξετάστηκε η δυνατότητα εφαρμογής τεχνικών Ενισχυτικής Μάθησης (Reinforcement Learning – RL) και της κβαντικής τους επέκτασης (Quantum Reinforcement Learning – QRL) στο πρόβλημα της ανίχνευσης απάτης. Ο στόχος της διερεύνησης ήταν να εκτιμηθεί κατά πόσο ένας πράκτορας που μαθαίνει πολιτικές απόφασης μέσω αλληλεπίδρασης με ένα περιβάλλον μπορεί να επιτύχει δυναμική προσαρμογή σε μεταβαλλόμενα πρότυπα συναλλαγών και να υπερβεί τα όρια των στατικών εποπτευόμενων μεθόδων ταξινόμησης.
Η συγκεκριμένη πειραματική προσέγγιση δεν εντάχθηκε στην τελική παραγωγική αρχιτεκτονική του Quantum Federated Blockchain συστήματος, αλλά αναπτύχθηκε ως ανεξάρτητο ερευνητικό σκέλος με σκοπό να αποτελέσει απόδειξη έννοιας (proof of concept) σχετικά με την αποτελεσματικότητα της ενισχυτικής μάθησης, και ιδίως της κβαντικής της παραλλαγής, σε προβλήματα κατηγοριοποίησης υψηλής πολυπλοκότητας.

6.5.2 Θεωρητικό Πλαίσιο

Η Ενισχυτική Μάθηση βασίζεται στην αρχή της αλληλεπίδρασης ενός πράκτορα με ένα περιβάλλον, στο οποίο σε κάθε χρονικό βήμα ο πράκτορας λαμβάνει μια κατάσταση s_t, επιλέγει μια ενέργεια a_tβάσει της πολιτικής του $\pi_\theta(a \mid s)$, και λαμβάνει μια ανταμοιβή r_tπου καθορίζει την ορθότητα της απόφασής του. Ο σκοπός του πράκτορα είναι να μεγιστοποιήσει τη συσσωρευμένη έκπτωση ανταμοιβών μέσω του αναμενόμενου αθροίσματος:

$$J(\theta) = \mathbb{E}_{\pi_\theta}[\sum_{t=0}^{T} \gamma^t r_t],$$

όπου γ είναι ο συντελεστής έκπτωσης και θ οι παράμετροι της πολιτικής.
Στην κβαντική της εκδοχή, η πολιτική υλοποιείται μέσω ενός παραμετρικού κβαντικού κυκλώματος (Variational Quantum Circuit – VQC), το οποίο μπορεί να αναπαραστήσει πιο εκφραστικές και μη γραμμικές σχέσεις μεταξύ εισόδων και ενεργειών χάρη στην ιδιότητα της υπέρθεσης και της διεμπλοκής (entanglement). Η ιδέα είναι ότι ο κβαντικός Actor μπορεί να χαρτογραφήσει τις καταστάσεις σε έναν εκθετικά μεγαλύτερο χώρο χαρακτηριστικών (Hilbert space), βελτιώνοντας τη γενίκευση του πράκτορα σε πολύπλοκα μοτίβα.

6.5.3 Περιγραφή Υλοποίησης

Η πειραματική υλοποίηση του συστήματος πραγματοποιήθηκε σε περιβάλλον Python με χρήση των βιβλιοθηκών TensorFlow και PennyLane, ενώ ο κβαντικός προσομοιωτής που επιλέχθηκε ήταν ο default.qubit του PennyLane. Η αρχιτεκτονική ακολουθεί το πλαίσιο Actor–Critic, όπου ο Actor προτείνει ενέργειες βάσει μιας παραμετροποιημένης πολιτικής, και ο Critic αξιολογεί την αξία των καταστάσεων ώστε να καθοδηγεί τη διαδικασία εκμάθησης.

Στην αρχική φάση, ο Actor υλοποιήθηκε ως κλασικό νευρωνικό δίκτυο με δύο κρυφά επίπεδα, ενεργοποιήσεις ReLU και έξοδο softmax, το οποίο παρήγαγε τις πιθανότητες επιλογής κάθε ενέργειας. Ο Critic, από την πλευρά του, εκτιμούσε τη συνάρτηση αξίας $V(s_t)$, παρέχοντας τον βαθμό απόκλισης της τρέχουσας εκτίμησης από την πραγματική ανταμοιβή. Η ενημέρωση των παραμέτρων βασίστηκε στον αλγόριθμο policy gradient, ο οποίος προσαρμόζει τα βάρη του Actor με βάση το σφάλμα TD (Temporal Difference) που παρέχεται από τον Critic.

Στη συνέχεια, αναπτύχθηκε η κβαντική εκδοχή του Actor, η οποία αντικαθιστά το κλασικό δίκτυο με ένα παραμετρικό κβαντικό κύκλωμα. Το κύκλωμα αυτό αποτελείται από τρία στάδια:
(α) την ενσωμάτωση των χαρακτηριστικών εισόδου μέσω Angle Embedding, όπου κάθε χαρακτηριστικό μετατρέπεται σε γωνία περιστροφής σε qubit,
(β) την εφαρμογή StronglyEntanglingLayers για δημιουργία συζευγμένων καταστάσεων qubits, και
(γ) τη μέτρηση σε βάση Pauli-Z, από την οποία προκύπτουν οι προσδοκώμενες τιμές που αντιστοιχούν στις πιθανότητες επιλογής ενεργειών.

Οι παράμετροι του κυκλώματος ενημερώνονται με τη μέθοδο parameter-shift, επιτρέποντας την ακριβή εκτίμηση των παραγώγων χωρίς αριθμητικά σφάλματα.

Η εκπαίδευση πραγματοποιήθηκε με χρήση τόσο του Adam όσο και του Nesterov optimizer, ενώ οι παράμετροι αρχικοποιήθηκαν τυχαία για κάθε run. Η διαδικασία επαναλαμβανόταν σε πολλαπλά επεισόδια, με τον πράκτορα να λαμβάνει κατάσταση, να επιλέγει ενέργεια, να ενημερώνει την πολιτική του και να αποθηκεύει την ανταμοιβή.

Η συνάρτηση που περιλαμβάνει όλα τα παραπάνω είναι η εξής:

```
def build_quantum_model(input_dim, circuit_type="grover", n_qubits=3, n_layers=1):
    dev = qml.device("default.qubit", wires=n_qubits + 1)

    if circuit_type == "custom":
        dummy_weights = np.zeros(200)
        num_weights_per_layer = custom_layer_long(dummy_weights, n_qubits)
        weight_shapes = {"weights": (n_layers, num_weights_per_layer)}

        def circuit(inputs, weights):
            qml.AngleEmbedding(inputs, wires=range(n_qubits + 1))
            for w in weights:
                custom_layer_long(w, n_qubits)
            return [qml.expval(qml.PauliZ(0)), qml.expval(qml.PauliZ(1))]

    elif circuit_type == "qaoa":
        # StronglyEntanglingLayers expects shape (n_layers, n_qubits, 3)
        weight_shapes = {"weights": (n_layers, n_qubits, 3)}
        def circuit(inputs, weights):
            qml.AngleEmbedding(inputs, wires=range(n_qubits + 1))
            qml.templates.StronglyEntanglingLayers(weights, wires=range(n_qubits + 1))
            return [qml.expval(qml.PauliZ(0)), qml.expval(qml.PauliZ(1))]

    elif circuit_type == "grover":
        # BasicEntanglerLayers expects shape (n_layers, n_qubits+1)
        weight_shapes = {"weights": (n_layers, n_qubits + 1)}
        def circuit(inputs, weights):
            qml.AngleEmbedding(inputs, wires=range(n_qubits + 1))
```

```
            qml.templates.BasicEntanglerLayers(weights, wires=range(n_qubits + 1))
            return [qml.expval(qml.PauliZ(0)), qml.expval(qml.PauliZ(1))]

    elif circuit_type == "iqp":
        # IQPEmbedding's weight shape can vary by version; verify in your env.
        # A safe fallback is to use StronglyEntanglingLayers again, or check
        # qml.templates.IQPEmbedding.weight_shape(n_layers, n_wires)
        weight_shapes = {"weights": (n_layers, (n_qubits + 1), 3)}
        def circuit(inputs, weights):
            qml.AngleEmbedding(inputs, wires=range(n_qubits + 1))
            qml.templates.StronglyEntanglingLayers(weights, wires=range(n_qubits + 1))
            return [qml.expval(qml.PauliZ(0)), qml.expval(qml.PauliZ(1))]

    qnode = qml.QNode(circuit, dev, interface="tf", diff_method="backprop")
    qlayer = KerasLayer(qnode, weight_shapes=weight_shapes, output_dim=2)

    model = tf.keras.Sequential([
        tf.keras.layers.Input(shape=(input_dim,)),
        tf.keras.layers.Dense(n_qubits + 1, activation='relu'),
        qlayer,
        tf.keras.layers.Dense(2, activation=None)  # linear for Q-values
    ])
    model.compile(optimizer='adam', loss='mse')
    return model
```

6.5.4 Παραλλαγές Αρχιτεκτονικής

Προκειμένου να μελετηθεί η επίδραση της πολυπλοκότητας του κβαντικού κυκλώματος στην απόδοση, εξετάστηκαν διάφορες παραλλαγές της αρχιτεκτονικής του QNN. Δοκιμάστηκαν κυκλώματα με 4, 6 και 8 qubits, ενώ το βάθος των στρωμάτων μεταβαλλόταν από δύο έως τέσσερα StronglyEntanglingLayers. Επιπλέον, συγκρίθηκαν δύο διαφορετικοί τύποι entanglement – ο απλός BasicEntanglerLayer και ο πλήρως διασυνδεδεμένος StronglyEntanglingLayer – προκειμένου να αξιολογηθεί η επίδραση του βαθμού διεμπλοκής των qubits στη σταθερότητα εκπαίδευσης.
Παράλληλα, μελετήθηκε και μια υβριδική προσέγγιση, όπου η έξοδος του κβαντικού κυκλώματος τροφοδοτείται σε ένα επιπλέον κλασικό πυκνό επίπεδο (Dense Layer). Αυτή η διάταξη, που αναφέρεται ως Hybrid QNN–Dense, παρουσίασε καλύτερη απόδοση σε δεδομένα με υψηλό ανισοζύγιο κλάσεων, καθώς ο συνδυασμός των κβαντικών χαρακτηριστικών με ένα μη γραμμικό επίπεδο αύξησε τη διακριτική ικανότητα του Actor.

Η αρχιτεκτονική του δικτύου φαίνεται εδώ:

```
class QuantumDQNAgent:
    def __init__(self, state_size, action_size, n_qubits=3, n_layers=2):
        self.state_size = state_size
        self.action_size = action_size
        self.memory = []
        self.gamma = 0.95
        self.epsilon = 1.0
        self.epsilon_min = 0.1
        self.epsilon_decay = 0.995
        self.batch_size = 64
```

```
        # Build both networks with the SAME architecture
        self.model = build_quantum_model(input_dim=state_size, n_qubits=n_qubits,
n_layers=n_layers)
        self.target_model = build_quantum_model(input_dim=state_size, n_qubits=n_qubits,
n_layers=n_layers)
        self.update_target_network
```

6.5.5 Στρατηγικές Εξερεύνησης

Για τη διαδικασία εξερεύνησης του χώρου ενεργειών εφαρμόστηκαν πολλαπλές στρατηγικές. Η απλούστερη προσέγγιση ήταν η ε-greedy, στην οποία ο πράκτορας επιλέγει με πιθανότητα ϵ μια τυχαία ενέργεια, και με πιθανότητα $1-\epsilon$ την ενέργεια με τη μεγαλύτερη εκτιμώμενη αξία. Η παράμετρος $\boldsymbol{\epsilon}$μεταβαλλόταν μεταξύ 0.1 και 0.3, επιτρέποντας προοδευτική μετάβαση από την τυχαία εξερεύνηση στην εκμετάλλευση της γνώσης.
Στη συνέχεια εξετάστηκε η softmax exploration, κατά την οποία οι πιθανότητες επιλογής ενεργειών καθορίζονταν από τη συνάρτηση softmax με θερμοκρασιακή παράμετρο τ, που ρυθμίζει τον βαθμό στοχαστικότητας. Τιμές $\boldsymbol{\tau}$μεταξύ 0.5 και 1.0 παρείχαν καλή ισορροπία ανάμεσα στην εξερεύνηση και στην εκμετάλλευση, μειώνοντας τα φαινόμενα πρόωρης σύγκλισης.
Επιπλέον, υλοποιήθηκε η Boltzmann exploration, όπου η πιθανότητα επιλογής κάθε ενέργειας εξαρτάται εκθετικά από την αντίστοιχη Q-value, καθώς και η entropy regularization, που προσθέτει έναν εντροπικό όρο στη συνάρτηση κόστους ενισχύοντας την ποικιλία των ενεργειών και αποτρέποντας τον εγκλωβισμό σε τοπικά ελάχιστα.
Από τη συγκριτική αξιολόγηση προέκυψε ότι η softmax στρατηγική με μέση θερμοκρασία $\tau = 0.7$ προσφέρει τη μεγαλύτερη σταθερότητα, ενώ η ε-greedy παρουσίαζε αυξημένη διασπορά στις ανταμοιβές, ιδίως στο κβαντικό μοντέλο όπου το noise επηρεάζει περισσότερο την εκτίμηση των πιθανοτήτων.

Οι στρατηγικές εξερεύνησης που αναφέρονται παραπάνω έχουν υλοποιηθεί σε κώδικα python ως εξής:

```
def epsilon_greedy(self, action_probs, action_space):
        """
        Epsilon-Greedy strategy: Selects random action with probability epsilon,
        otherwise selects the best action.
        :param action_probs: Action probabilities from the policy network.
        :param action_space: Action space for random sampling.
        :return: Selected action.
        """
        if np.random.rand() < self.epsilon:
            action = np.random.choice(action_space.n)  # Random action
        else:
            action = tf.argmax(action_probs, axis=-1).numpy()  # Best action
        self.epsilon = max(self.epsilon_min, self.epsilon * self.epsilon_decay)  # Decay epsilon
        return action

    def entropy_regularization(self, action_probs):
        """
        Entropy Regularization: Encourages stochastic exploration by sampling from
        the action distribution.
        :param action_probs: Action probabilities from the policy network.
        :return: Selected action.
```

```
        """
        action_dist = tf.keras.activations.softmax(action_probs)
        action = np.random.choice(len(action_probs), p=action_dist.numpy())  # Sample action
        return action

    def boltzmann_exploration(self, action_probs):
        """
        Boltzmann Exploration: Selects actions based on a temperature-scaled probability distribution.
        :param action_probs: Action probabilities from the policy network.
        :return: Selected action.
        """
        temperature = 1.0  # Temperature parameter
        scaled_probs = tf.nn.softmax(action_probs / temperature)
        action = np.random.choice(len(action_probs), p=scaled_probs.numpy())  # Sample action
        return action

    def noisy_networks(self, action_probs):
        """
        Noisy Networks: Adds noise to the network output to encourage exploration.
        :param action_probs: Action probabilities from the policy network.
        :return: Selected action.
        """
        noise = tf.random.normal(shape=tf.shape(action_probs), mean=0.0, stddev=0.1)
        noisy_action_probs = action_probs + noise
        return tf.argmax(noisy_action_probs, axis=-1).numpy()
```

6.5.6 Συστήματα Ανταμοιβής (Reward Systems)

Για τη διαμόρφωση της συνάρτησης ανταμοιβής εξετάστηκαν τέσσερις διαφορετικές προσεγγίσεις. Η πρώτη ήταν η κλασική δυαδική επιβράβευση, όπου αποδίδεται +1 για σωστή ταξινόμηση και -1 για λανθασμένη. Αν και απλή, η προσέγγιση αυτή αποδείχθηκε υπερευαίσθητη σε θόρυβο.
Στη δεύτερη εκδοχή, η ανταμοιβή κλιμακώθηκε (scaled reward) με διαφορετικούς συντελεστές επιβράβευσης, ώστε να μειωθεί η επίδραση μεμονωμένων σφαλμάτων και να ενισχυθούν οι οριακά σωστές αποφάσεις. Η τρίτη εκδοχή περιλάμβανε στάθμιση των ανταμοιβών βάσει της συχνότητας εμφάνισης κάθε κλάσης (weighted reward), προκειμένου να αντιμετωπιστεί το πρόβλημα της ανισορροπίας μεταξύ νόμιμων και απατηλών συναλλαγών. Τέλος, εφαρμόστηκε μια τροποποιημένη συνάρτηση ανταμοιβής με όρο εντροπίας (entropy-augmented reward), που ενθάρρυνε τη διαφοροποίηση της πολιτικής, αυξάνοντας την ποικιλία των ενεργειών του πράκτορα.
Από τα πειράματα διαπιστώθηκε ότι ο συνδυασμός κλιμακωτής ανταμοιβής με εντροπικό όρο παρείχε τη βέλτιστη ισορροπία μεταξύ σταθερότητας και ακρίβειας, οδηγώντας σε πιο ομαλές καμπύλες σύγκλισης.

Τα διάφορα reward systems που υλοποιήθηκαν σε κώδικα python είναι τα εξής:

```
def calculate_reward(self, action, is_fraud, row):
        """
        Computes the reward for the agent based on its action and the true fraud label.
        """

        if self.reward_system == "new_reward_system":
            if action == 1 and is_fraud == 1:  # True Positive (Correct Fraud Detection)
```

```
            return 10
        elif action == 1 and is_fraud == 0:  # False Positive (Wrong Fraud Detection)
            return -3
        elif action == 0 and is_fraud == 1:  # False Negative (Missed Fraud)
            return -10
        else:  # True Negative (Legit Transaction)
            return 1

    # **Baseline Reward System**
    if self.reward_system == "baseline":
        if action == 1 and is_fraud == 1:  # True positive
            return 1.0
        elif action == 1 and is_fraud == 0:  # False positive
            return -0.5
        elif action == 0 and is_fraud == 1:  # False negative
            return -2.0
        else:  # True negative
            return 0.5

    # **Penalty for False Negatives**
    elif self.reward_system == "penalty_for_false_negatives":
        if action == 1 and is_fraud == 1:
            return 1.0
        elif action == 1 and is_fraud == 0:
            return -0.3
        elif action == 0 and is_fraud == 1:
            return -3.0  # Stronger penalty for false negatives
        else:
            return 0.5

    # **Intermediate Rewards for Suspicious Patterns**
    elif self.reward_system == "intermediate_rewards":
        reward = 0
        if action == 1 and is_fraud == 1:
            reward = 2.0
        elif action == 1 and is_fraud == 0:
            reward = -2.0  # Stronger penalty for incorrect fraud detection
        elif action == 0 and is_fraud == 1:
            reward = -3.0
        else:
            reward = 1.0  # Reward for correctly classifying legit transactions

        # Add bonus for detecting suspicious patterns
        if action == 1 and row['amount_to_balance_ratio'] > 0.8:
            reward += 0.2
        return reward

    # **Dynamic Reward Scaling**
    elif self.reward_system == "dynamic_scaling":
        if action == 1 and is_fraud == 1:  # True Positive
            return 2.0  # More reward for correct fraud detection
```

```
        elif action == 1 and is_fraud == 0:  # False Positive
            return -1.0  # Slightly higher penalty
        elif action == 0 and is_fraud == 1:  # False Negative
            return -3.0  # Increase penalty (but less extreme than before)
        else:  # True Negative
            return 1.0  # Higher reward for correct classification
```

6.5.7 Αποτελέσματα και Ανάλυση Σύγκλισης

Η αξιολόγηση των διαφορετικών παραλλαγών πραγματοποιήθηκε μετρώντας την ακρίβεια, τη μέση ανταμοιβή ανά επεισόδιο, τη διασπορά των ανταμοιβών και τον χρόνο σύγκλισης. Ο κλασικός Actor–Critic πράκτορας παρουσίασε ταχύτερη σύγκλιση και υψηλή σταθερότητα, με χαμηλή διακύμανση στις ανταμοιβές, γεγονός που αποδίδεται στο γραμμικότερο τοπίο βελτιστοποίησης των παραμέτρων του. Αντίθετα, ο κβαντικός Actor παρουσίασε μεγαλύτερη διακύμανση στις ανταμοιβές και καθυστέρηση στη σταθεροποίηση της πολιτικής του, απαιτώντας περισσότερα επεισόδια για να φτάσει σε ικανοποιητική απόδοση. Παρόλα αυτά, στις περιπτώσεις έντονης μη γραμμικότητας και ανισοζυγίου των κλάσεων, το QRL εμφάνισε ελαφρώς καλύτερη F1-score, γεγονός που υποδηλώνει αυξημένη ικανότητα αναγνώρισης σπάνιων προτύπων απάτης.
Η γενική απόδοση του QRL παρέμεινε 2–3% χαμηλότερη σε ακρίβεια σε σχέση με το κλασικό baseline, όμως το προφίλ των ανταμοιβών του έδειξε υψηλότερη ποικιλία και εντονότερη προσαρμοστικότητα σε αλλαγές στο περιβάλλον. Οι διαφοροποιήσεις αυτές δείχνουν ότι το QRL έχει τη δυναμική να αξιοποιηθεί σε συστήματα όπου η στατιστική κατανομή των δεδομένων μεταβάλλεται δυναμικά με το χρόνο.

Το evaluation σε κώδικα python έγινε ως εξής:

```
import numpy as np
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, roc_auc_score,
confusion_matrix
import matplotlib.pyplot as plt
import seaborn as sns

def evaluate_model(agent, env, episodes=100):
    """
    Evaluates the trained DQN model over multiple episodes.
    Computes accuracy, precision, recall, F1, and ROC-AUC.
    """
    from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, roc_auc_score,
confusion_matrix

    y_true = []
    y_pred = []
    y_score = []  # Probability for fraud (action 1)
    total_rewards = []

    for episode in range(episodes):
        state = env.reset()
        done = False
        episode_reward = 0
```

```
        while not done:
            # Get the true label from the current shuffled index
            current_data_index = env.index_order[env.current_index]
            true_label = env.data.loc[current_data_index, 'isFraud']
            y_true.append(true_label)

            state_tensor = np.expand_dims(state, axis=0)
            q_values = agent.q_network.predict(state_tensor, verbose=0)[0]

            # Numerically stable softmax conversion:
            q_max = np.max(q_values)
            exp_q = np.exp(q_values - q_max)
            probs = exp_q / np.sum(exp_q)

            action = np.argmax(q_values)
            y_pred.append(action)
            y_score.append(probs[1])  # Score for fraud

            next_state, reward, done, _ = env.step(action)
            episode_reward += reward
            state = next_state

        total_rewards.append(episode_reward)

    metrics = {
        'accuracy': accuracy_score(y_true, y_pred),
        'precision': precision_score(y_true, y_pred, zero_division=1),
        'recall': recall_score(y_true, y_pred),
        'f1': f1_score(y_true, y_pred)
    }
    try:
        metrics['auc_roc'] = roc_auc_score(y_true, y_score)
    except ValueError:
        metrics['auc_roc'] = 0.0

    print("\n📊 **DQN Evaluation Metrics**")
    for key, value in metrics.items():
        print(f"{key.capitalize()}: {value:.4f}")
    print(f"💰 **Avg Episode Reward:** {np.mean(total_rewards):.2f}")

    cm = confusion_matrix(y_true, y_pred)
    class_names = ["Legit", "Fraud"]
    plt.figure(figsize=(6, 4))
    sns.heatmap(cm, annot=True, fmt="d", cmap="Blues", xticklabels=class_names,
yticklabels=class_names)
    plt.xlabel("Predicted Label")
    plt.ylabel("True Label")
    plt.title("Confusion Matrix")
    plt.show()
```

```
return metrics
```

6.5.8 Συμπεράσματα και Προοπτικές

Η πειραματική μελέτη του QRL ανέδειξε τη δυνατότητα χρήσης κβαντικών πολιτικών για την εκμάθηση σύνθετων στρατηγικών απόφασης, επιβεβαιώνοντας ότι η προσθήκη κβαντικών χαρακτηριστικών προσφέρει αυξημένη εκφραστικότητα. Ωστόσο, η εκπαίδευση του QRL αποδείχθηκε πιο ασταθής, ευαίσθητη στις υπερπαραμέτρους και απαιτητική υπολογιστικά. Παρόλο που δεν ξεπέρασε την απόδοση του κλασικού Actor–Critic, η συμπεριφορά του υποδηλώνει ότι μπορεί να αποδειχθεί χρήσιμο σε εφαρμογές που απαιτούν εξερεύνηση υψηλής διάστασης και προσαρμοστικότητα.
Το QRL πλαίσιο που υλοποιήθηκε στο πλαίσιο της παρούσας εργασίας θεωρείται απόδειξη έννοιας και παραμένει ανεξάρτητο ερευνητικό υποσύστημα. Μελλοντικά, θα μπορούσε να ενσωματωθεί στο federated learning περιβάλλον για τη δυναμική ρύθμιση του ρυθμού εκμάθησης ή την αυτόματη στάθμιση των τοπικών μοντέλων, λειτουργώντας ως μετα-στρώμα πολιτικής που καθοδηγεί τη διαδικασία ομοσπονδιακής συνάθροισης με τρόπο προσαρμοστικό και ευφυή.

6.6 Πειραματική Προσπάθεια Υλοποίησης Grover-Based Quantum Classifier

6.6.1 Θεωρητική Βάση και Κίνητρο

Αν και το σχήμα δεν ενσωματώθηκε στην τελική εκδοχή του υβριδικού μοντέλου, διερευνήθηκε πειραματικά η εφαρμογή ενός Grover-Based Quantum Classifier, βασισμένου στο έργο των Du et al. (2022), *"A Grover-search Based Quantum Learning Scheme for Classification"* [204].

Η μεθοδολογία αυτή (GBLS) μετασχηματίζει το πρόβλημα ταξινόμησης σε πρόβλημα αναζήτησης, όπου η σωστή πρόβλεψη θεωρείται ως «στόχος» (target index) μέσα σε έναν υπερχώρο πιθανών καταστάσεων.

Ο αλγόριθμος Grover-search προσφέρει θεωρητικά τετραγωνική επιτάχυνση O(√N) στην εύρεση του στόχου, γεγονός που θα μπορούσε να μειώσει τον αριθμό των επαναλήψεων και των μετρήσεων κατά τη μάθηση.

Για κάθε δείγμα εισόδου δημιουργείται ένα μικρό υποσύνολο δεδομένων (D_k) που περιέχει το πραγματικό δείγμα και ορισμένα της αντίθετης κλάσης. Όλα τα υποδείγματα φορτώνονται ταυτόχρονα σε υπέρθεση, όπου ο oracle «σημαδεύει» το σωστό δείγμα και ο diffuser ενισχύει την πιθανότητα μέτρησής του.

Η διαδικασία αυτή, σε συνδυασμό με την εκπαίδευση του παραμετρικού μπλοκ (U_{L1}), επιτρέπει στο κύκλωμα να «μαθαίνει» να ενισχύει τη σωστή κατάσταση κάθε φορά που το δείγμα είναι θετικό.

6.6.2 Στόχος και Αποτελέσματα της Υλοποίησης

Στόχος της προσπάθειας ήταν να αξιολογηθεί εάν ο μηχανισμός Grover-based learning μπορεί να επιταχύνει τη διαδικασία εκπαίδευσης ενός υβριδικού QNN, μειώνοντας τον απαιτούμενο αριθμό μετρήσεων και βελτιώνοντας τη σταθερότητα της σύγκλισης.

Σύμφωνα με τη θεωρητική ανάλυση των Du et al. (2022), το GBLS επιτυγχάνει τετραγωνική μείωση της πολυπλοκότητας από O(K) σε O(√K) και περιορίζει τις απαιτούμενες μετρήσεις από O(NMd) σε O(NMd / K), διατηρώντας αντίστοιχη ακρίβεια.

Ωστόσο, στην πειραματική μας μελέτη δεν παρατηρήθηκε ουσιαστική βελτίωση σε σχέση με το αρχικό υβριδικό μοντέλο· τα αποτελέσματα παρέμειναν στα ίδια επίπεδα ακρίβειας, χωρίς αξιοσημείωτη επιτάχυνση του χρόνου εκπαίδευσης.

Η έλλειψη βελτίωσης αποδίδεται κυρίως στους περιορισμούς του NISQ περιβάλλοντος, όπως το βάθος του κυκλώματος, η θορυβώδης φύση των πολυελεγχόμενων πυλών (MCZ) και το μικρό μέγεθος του search space (K).

Παρότι τα πειραματικά αποτελέσματα δεν επιβεβαίωσαν την αναμενόμενη θεωρητική επιτάχυνση, η μελέτη ανέδειξε τη δυνατότητα του Grover-based μηχανισμού να προσφέρει τετραγωνική βελτίωση σε μελλοντικές υλοποιήσεις με μεγαλύτερα K και πιο σταθερά κβαντικά συστήματα.

6.6.3 Μετασχηματισμός του dataset σε Grover-ready μορφή

Πριν την ανάλυση της αρχιτεκτονικής, είναι απαραίτητο να γίνει αναφορά στη διαδικασία μετασχηματισμού του αρχικού συνόλου δεδομένων, η οποία αποτελεί κρίσιμο προπαρασκευαστικό στάδιο για την εκπαίδευση του Grover-Based Classifier.

Συγκεκριμένα, το κλασικό σύνολο δεδομένων

$$\widehat{D} = \{(x_i, y_i)\}i = 0^{N-1}$$

μετασχηματίζεται σε ένα επεκταμένο σύνολο

$$D = \{D_k\}k = 0^{N-1}$$

, όπου κάθε στοιχείο D_k περιέχει K ζεύγη δεδομένων:

$$D_k = \{({x_k}^{(0)}, {x_k}^{(0)}), ({x_k}^{(1)}, {y_k}^{(1)}), \dots, ({x_k}^{(K-1)}, {y_k}^{(K-1)})\}.$$

Η βασική ιδέα πίσω από αυτή την αναδιατύπωση είναι να καταστεί δυνατή η εφαρμογή του Grover-search μηχανισμού, ο οποίος απαιτεί έναν "χώρο αναζήτησης" μεγέθους K. [204]

Στο νέο σύνολο:

- Το τελευταίο στοιχείο του κάθε D_k, δηλαδή $(x_k^{(K-1)}, y_k^{(K-1)})$, αντιστοιχεί στο πραγματικό δείγμα (x_k, y_k) του αρχικού dataset.
- Τα πρώτα K−1 στοιχεία επιλέγονται τυχαία από παραδείγματα της αντίθετης κλάσης· δηλαδή, αν $y_k = 1$, τότε τα υπόλοιπα δείγματα προέρχονται από περιπτώσεις με y = 0, και αντίστροφα.

Με αυτόν τον τρόπο, κάθε D_k περιέχει μία θετική περίπτωση και K−1 αρνητικές, δημιουργώντας ένα τοπικό υποσύνολο δεδομένων κατάλληλο για αναζήτηση τύπου Grover.

Η κβαντική διαδικασία στοχεύει να "εντοπίσει" τον δείκτη $i^* = K - 1$, δηλαδή το σωστό δείγμα, μέσα από αυτό το υποσύνολο.

Έτσι, το πρόβλημα της ταξινόμησης μετατρέπεται σε πρόβλημα αναζήτησης όπου το κύκλωμα πρέπει να ενισχύσει την πιθανότητα μέτρησης του δείκτη i^* όταν η ετικέτα $y_k = 1$.

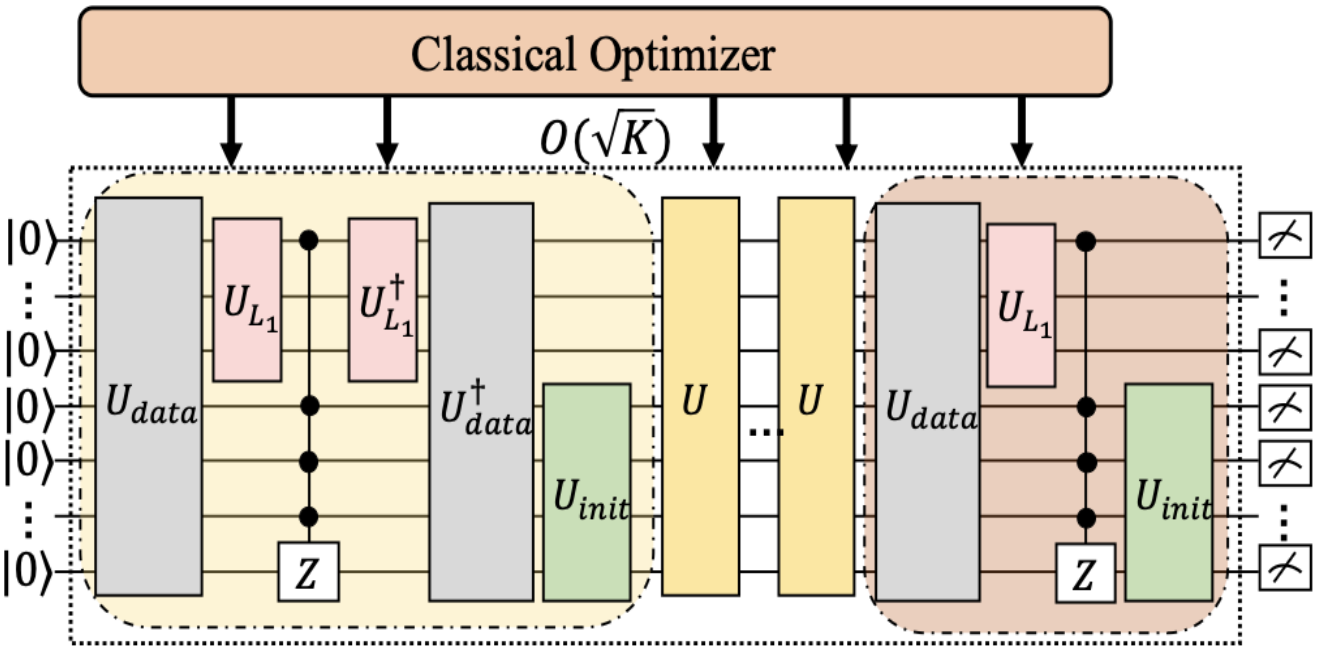
Ο μετασχηματισμός αυτός έχει διπλή σημασία:

1. Δημιουργεί το απαραίτητο Grover-search πλαίσιο μέσα στο οποίο λειτουργεί ο ταξινομητής.
2. Μειώνει δραστικά τον αριθμό των απαιτούμενων μετρήσεων κατά την εκπαίδευση (από $O(NMd)$ σε $O(\frac{NMd}{K})$, χωρίς απώλεια στην απόδοση του μοντέλου. [204]

6.6.4 Αρχιτεκτονική του Grover-Based Classifier

6.6.4.1 Συνολικό Κύκλωμα

Το συνολικό κύκλωμα φαίνεται και στην παρακάτω εικόνα:



Εικόνα 22 Η συνολική δομή του Grover-Based Classifier, όπως προτείνεται από τους Du et al. (2022). [204]

Η διαδικασία ξεκινά με την κβαντική κωδικοποίηση των δεδομένων μέσω του U_{data}, ακολουθούμενη από το παραμετρικό μπλοκ U_{L1}, το οποίο μαθαίνει τη βέλτιστη μετασχηματιστική αναπαράσταση των χαρακτηριστικών.

Στη συνέχεια, εφαρμόζονται οι αντίστροφες πράξεις ${U_{L1}}^{\dagger}$ και ${U_{data}}^{\dagger}$,, ώστε να αναιρεθούν οι προηγούμενοι μετασχηματισμοί και να επανέλθει το κύκλωμα στην αρχική του μορφή, προετοιμάζοντας το σύστημα για το στάδιο ενίσχυσης της σωστής λύσης μέσω του Uinit, όπως απαιτεί ο μηχανισμός του Grover-search.

Η διαδικασία αυτή είναι κρίσιμη, καθώς επιτρέπει στο κύκλωμα να «απομονώσει» τη σωστή κατάσταση χωρίς να διαταράξει την υπόλοιπη υπέρθεση. Με την αντεστραμμένη εκτέλεση των U_{data} και U_{L1},οι πληροφορίες που είχαν εισαχθεί στο κύκλωμα "ακυρώνονται" ως προς τη φάση, ενώ διατηρείται μόνο η σήμανση της κατάστασης που έχει επιλεγεί από την Oracle. Έτσι, το κύκλωμα ολοκληρώνει έναν πλήρη κύκλο του Grover — σήμανση, αναίρεση των πράξεων και τελική ενίσχυση — αυξάνοντας σταδιακά την πιθανότητα μέτρησης της σωστής κατάστασης στο τέλος της διαδικασίας.

Στη συνέχεια εφαρμόζεται το oracle (Z gate), το οποίο σηματοδοτεί το δείγμα-στόχο (label = 1), και το Uinit, που αντιστοιχεί στον Grover diffusion operator, ενισχύοντας την πιθανότητα μέτρησης του σωστού δείκτη. Η επαναληπτική ακολουθία (U_{data} U_{L1}, ${U_{L1}}^{\dagger}$, ${U_{data}}^{\dagger}$, Uinit) εκτελείται O(√K) φορές, υλοποιώντας την αναζήτηση τύπου Grover πάνω στο σύνολο δεδομένων μεγέθους K. [204]

6.6.4.2 Quantum Data Encoding (Udata)

Στο πρώτο στάδιο, το σύνολο των δειγμάτων εισόδου x_i ενσωματώνεται σε μια κβαντική υπέρθεση που περιέχει τόσο τα χαρακτηριστικά όσο και το ευρετήριο του κάθε δείγματος.

Ακολουθώντας τη μεθοδολογία του paper, η κατάσταση του συστήματος γράφεται ως:

$$|\Phi_k\rangle = \frac{1}{\sqrt{K}} \sum_{i=0}^{K-1} |\mathrm{h}(x_i)_F\rangle \, |\mathrm{i}_I\rangle$$

όπου:

- $|\mathrm{h}(x_i)_F\rangle$: το feature register, στο οποίο κωδικοποιούνται τα χαρακτηριστικά του δείγματος μέσω μιας embedding συνάρτησης h(x) (συνήθως μέσω angle embedding ή amplitude encoding),
- $|\mathrm{i}_I\rangle$: το index register, που αναπαριστά το "θέση" του δείγματος μέσα στο υποσύνολο δεδομένων,
- K: το πλήθος των στοιχείων που περιλαμβάνονται στο "search space" του Grover.

Αυτό το encoding επιτρέπει στο κύκλωμα να εξερευνά ταυτόχρονα όλες τις πιθανές καταστάσεις των δεδομένων μέσω της αρχής της υπέρθεσης — θεμελιώδης ιδέα για την κβαντική επιτάχυνση.

Στην πράξη, το U_{data} υλοποιείται με amplitude encoding, όπου οι τιμές των χαρακτηριστικών κανονικοποιούνται και τοποθετούνται απευθείας στις πλάτες της κβαντικής κατάστασης. Έτσι, η πληροφορία των δεδομένων ενσωματώνεται στο ίδιο το διάνυσμα κατάστασης του συστήματος, χωρίς να χρειάζονται πύλες περιστροφής όπως $R_y(\theta)$.

```
def data_block(samples, inverse=False):
    """Coherently load (or unload) PACK_SIZE classical samples."""
    if hasattr(samples, "shape"):
        if int(samples.shape[0]) not in (0, PACK_SIZE):
            raise ValueError(f"Expected {PACK_SIZE} samples, got {samples.shape[0]}.")
    else:
        if len(samples) != PACK_SIZE:
            raise ValueError(f"Expected {PACK_SIZE} samples, got {len(samples)}.")
    if not inverse:
        for wire in INDEX_WIRES:
            qml.Hadamard(wires=wire)

        for idx in range(PACK_SIZE):
            pattern = format(idx, f"0{NUM_INDEX_WIRES}b")
            for wire, bit in zip(INDEX_WIRES, pattern):
                if bit == "0":
                    qml.PauliX(wires=wire)
            sample = samples[idx]
            qml.ctrl(amplitude_encode, control=INDEX_WIRES)(sample)
            for wire, bit in zip(INDEX_WIRES, pattern):
                if bit == "0":
                    qml.PauliX(wires=wire)

    else:
        for idx in reversed(range(PACK_SIZE)):
            pattern = format(idx, f"0{NUM_INDEX_WIRES}b")
            for wire, bit in zip(INDEX_WIRES, pattern):
                if bit == "0":
                    qml.PauliX(wires=wire)
            sample = samples[idx]
            qml.ctrl(qml.adjoint(amplitude_encode), control=INDEX_WIRES)(sample)
```

```
        for wire, bit in zip(INDEX_WIRES, pattern):
            if bit == "0":
                qml.PauliX(wires=wire)

    for wire in INDEX_WIRES:
        qml.Hadamard(wires=wire)
```

6.6.4.3 Variational Block (UL1)

Στο δεύτερο στάδιο πραγματοποιείται η βασική φάση της εκμάθησης.

Εδώ εφαρμόζεται ένα παραμετρικό κύκλωμα (Variational Quantum Circuit - VQC) στο feature register, το οποίο μαθαίνει να μετασχηματίζει τις κβαντικές καταστάσεις των δεδομένων έτσι ώστε να διαχωρίζονται οι κλάσεις (0/1).

Το κύκλωμα αυτό, που αντιστοιχεί στο UL_1 του αλγορίθμου, αποτελείται από διαδοχικά στρώματα πυλών περιστροφής και διεμπλοκής και προσαρμόζει τις παραμέτρους του μέσω της διαδικασίας βελτιστοποίησης.

Το πρώτο qubit του feature register λειτουργεί ως flag qubit ή qubit απόφασης, του οποίου η κατάσταση ($|0\rangle$ ή $|1\rangle$) καθορίζει αν η oracle θα «σημάνει» επιτυχία, δηλαδή αν το δείγμα ανήκει στην κλάση-στόχο.

Κάθε στρώμα (layer) του UL1 περιλαμβάνει:

- μονο-qubit πύλες RY(θ), RZ(θ) για παραμετρική περιστροφή,
- entangling πύλες τύπου CNOT ή CZ για δημιουργία διαπλοκής (entanglement) μεταξύ των qubits.

Η γενική μορφή του UL1 είναι:

$$U_{L1}(\theta) = \prod_{l=1}^{L} U(\theta_l)$$

με L να δηλώνει το βάθος του κυκλώματος.

Κατά τη διάρκεια της εκπαίδευσης, οι παράμετροι θ_l ενημερώνονται μέσω parameter-shift rule ώστε να ελαχιστοποιηθεί η συνάρτηση κόστους.

Η λειτουργία του UL1 είναι παρόμοια με ένα Dense Layer σε ένα κλασικό νευρωνικό δίκτυο — μαθαίνει δηλαδή να "περιστρέφει" τον χώρο των δεδομένων έτσι ώστε τα θετικά και αρνητικά παραδείγματα να γίνονται διακριτά.

```
def ul1_block(params, inverse=False):
    """
    Apply UL1 layer LAYER_COUNT times with SHARED parameters.

    CRITICAL FIX: The same params are reused for each layer iteration,
    not different parameters. This matches the paper's design.

    Args:
```

```
    params: 1D array of shape (PARAMS_PER_LAYER,) - NOT (LAYER_COUNT, PARAMS_PER_LAYER)
    inverse: Whether to apply adjoint
  """
  # Ensure params is 1D
  if qml.math.ndim(params) > 1:
    # If accidentally passed 2D array, flatten or take first layer
    params = qml.math.reshape(params, (-1,))[:PARAMS_PER_LAYER]

  for _ in range(LAYER_COUNT):
    if inverse:
      qml.adjoint(ul1_layer)(params)
    else:
      ul1_layer(params)
```

Εδώ χρησιμοποιήσαμε το ίδιο παραμετρικό κύκλωμα όπως και στη μελέτη του απλού υβριδικού κβαντικού κυκλώματος, ώστε να μπορέσουμε να συγκρίνουμε αναλογικά την απόδοση της νέας μεθόδου και να αξιολογήσουμε αν προσφέρει ουσιαστική βελτίωση σε σχέση με την προηγούμενη.

6.6.4.4 Oracle Construction (MCZ Block)

Το τρίτο στάδιο αποτελεί τον πυρήνα της διαφοροποίησης του GBLS από τα υπόλοιπα κβαντικά νευρωνικά δίκτυα.

Σε αυτό το σημείο εισάγεται η Oracle, η οποία υλοποιείται μέσω μιας πολυ-ελεγχόμενης πύλης Z (Multi-Controlled-Z, MCZ). Η Oracle είναι υπεύθυνη για τη «σήμανση» (phase flip) του κατάλληλου δείγματος μέσα στην υπέρθεση των καταστάσεων, επιτελώντας τον ρόλο του κλασικού μηχανισμού “marking the correct item” του αρχικού αλγορίθμου του Grover.

Η βασική της λειτουργία είναι η εξής:

- Εάν το τρέχον δείγμα έχει θετική ετικέτα ($y_k = 1$), η Oracle εκτελεί αντιστροφή φάσης (phase inversion) στην κατάσταση του index register που αντιστοιχεί στο δείγμα-στόχο $|i^*\rangle$.

  Με άλλα λόγια, η φάση της βάσης $|i^*\rangle$ αντιστρέφεται, γεγονός που αποτελεί το κβαντικό “σήμα επιτυχίας”.

- Εάν το δείγμα ανήκει στην αρνητική κλάση ($y_k = 0$), καμία αντιστροφή δεν πραγματοποιείται και η φάση παραμένει αμετάβλητη.

Με αυτόν τον τρόπο, το κύκλωμα «μαρκάρει» τα δείγματα που αντιστοιχούν σε επιτυχία (label = 1), ώστε στις επόμενες επαναλήψεις του Grover-τύπου βρόχου να ενισχυθεί η πιθανότητα εμφάνισής τους κατά τη μέτρηση.

Σε επίπεδο αρχιτεκτονικής, η Oracle υλοποιείται με μια πύλη MCZ που δρα ταυτόχρονα:

- στον πρώτο qubit του feature register (τον αποκαλούμενο *decision* ή *flag qubit*), και
- σε όλα τα qubits του index register, τα οποία κωδικοποιούν τις θέσεις των δειγμάτων $|i\rangle$.

Η πύλη αυτή ενεργοποιείται μόνο όταν πληρούνται και οι δύο εξής συνθήκες:

1. Ο flag qubit βρίσκεται στην κατάσταση $|1\rangle$, κάτι που υποδηλώνει ότι το κύκλωμα U_{L1} έχει ταξινομήσει το δείγμα ως θετικό.
2. Το index register βρίσκεται στη συγκεκριμένη δυαδική κατάσταση $|i^*\rangle$, που αντιστοιχεί στο δείγμα-στόχο μέσα στο εκτεταμένο πακέτο D_k.

Όταν συμβαίνουν και οι δύο αυτές συνθήκες, η MCZ εκτελεί phase flip στην κατάσταση $|i^*\rangle$ *επιφέροντας ένα αρνητικό πρόσημο στη συνολική υπέρθεση:*

$$|1\rangle_F|i^*\rangle_I \longrightarrow -|1\rangle_F|i^*\rangle_I$$

ενώ όλες οι υπόλοιπες βάσεις παραμένουν αμετάβλητες.

Η πράξη αυτή δημιουργεί την απαιτούμενη διαφορά φάσης που θα αξιοποιηθεί από το επόμενο στάδιο — τον diffusion operator — ώστε να ενισχυθεί η πιθανότητα του σωστού δείγματος, ακολουθώντας τη λογική του Grover-search.

Αν και η χρήση της MCZ αυξάνει το βάθος του κυκλώματος (επειδή περιλαμβάνει πολλαπλούς ελέγχους), προσφέρει ένα κρίσιμο πλεονέκτημα: επιτρέπει στο GBLS να υλοποιήσει κβαντικά τον μηχανισμό ενίσχυσης της επιτυχούς κατάστασης, μειώνοντας την υπολογιστική πολυπλοκότητα από O(K) σε $O(\sqrt{K})$.

Έτσι, το GBLS μετατρέπει το πρόβλημα ταξινόμησης σε πρόβλημα αναζήτησης εντός υπέρθεσης, ενσωματώνοντας οργανικά τον Grover-τύπου μηχανισμό στο πλαίσιο της κβαντικής μάθησης.

```
# ---------------------------------------------------------------------
# Oracle
# ---------------------------------------------------------------------
def MCZ_flag_on_index(target_bits: str, F, I, *, fire_on_flag: int = 1):
    """Multi-controlled Z that flips phase iff (flag == fire_on_flag) AND (I == target_bits)."""
    NI = len(I)
    if NI == 0:
        raise ValueError("Index register I must have at least 1 qubit.")
    if len(target_bits) != NI:
        raise ValueError(f"target_bits must have length {NI} (got {len(target_bits)}).")

    bits = [int(b) for b in target_bits]

    if fire_on_flag == 0:
        qml.PauliX(wires=F[0])

    for wire, bit in zip(I, bits):
        if bit == 0:
            qml.PauliX(wires=wire)

    controls = [F[0]] + I[:-1]
    target = I[-1]
    qml.Hadamard(wires=target)
    qml.MultiControlledX(wires=controls + [target])
    qml.Hadamard(wires=target)

    for wire, bit in zip(I, bits):
        if bit == 0:
```

```
            qml.PauliX(wires=wire)

    if fire_on_flag == 0:
        qml.PauliX(wires=F[0])


def oracle_MCZ(i_star: int, F, I, *, fire_on_flag: int = 1):
    """Convenience wrapper: apply the oracle for i_star with chosen flag sense."""
    bits = format(i_star, f"0{len(I)}b")
    MCZ_flag_on_index(bits, F, I, fire_on_flag=fire_on_flag)
```

6.6.4.5 Grover Diffusion (Uinit)

Μετά την εφαρμογή της Oracle, το κύκλωμα περνά στο στάδιο Grover Diffusion.

Εδώ εφαρμόζεται ο μοναδιαίος τελεστής:

$$U_{init} = 2|\varphi\rangle\langle\varphi| - I$$

όπου

$$|\varphi\rangle = \frac{1}{\sqrt{K}} \sum_{i=0}^{K-1} |\mathrm{i}\rangle$$

είναι η αρχική υπέρθεση όλων των πιθανών δεικτών.

Η ενέργεια του Uinit είναι να “αναστρέψει” την πιθανότητα γύρω από τον μέσο όρο, αυξάνοντας δραματικά την πιθανότητα του σωστού target index $|i^*\rangle$.

Σε πρακτικό επίπεδο, αυτή η ενίσχυση πραγματοποιείται μέσω μιας ακολουθίας από Hadamard, Pauli-X, και multi-controlled-X πυλών, που αντιγράφουν την κλασική Grover diffusion.

Η επαναληπτική αλληλουχία Oracle → Diffusion εκτελείται O(√K) φορές, με κάθε βήμα να ενισχύει την πιθανότητα του σωστού δείγματος.

```
def diffuser():
    """Grover-style diffusion on the index register."""
    for wire in INDEX_WIRES:
        qml.Hadamard(wires=wire)
        qml.PauliX(wires=wire)
    controls = INDEX_WIRES[:-1]
    target = INDEX_WIRES[-1]
    qml.Hadamard(wires=target)
    if controls:
        qml.MultiControlledX(wires=controls + [target])
    else:
        qml.PauliX(wires=target)
    qml.Hadamard(wires=target)
    for wire in INDEX_WIRES:
        qml.PauliX(wires=wire)
        qml.Hadamard(wires=wire)
```

6.6.4.6 Μέτρηση και υπολογισμός Απώλειας

Στο τελικό στάδιο του κυκλώματος, το ζητούμενο δεν είναι απλώς να ελεγχθεί αν το *flag qubit* έχει τιμή |1⟩.

Ο στόχος είναι να επιβεβαιωθεί ταυτόχρονα ότι:

1. Το flag qubit βρίσκεται στην κατάσταση |1⟩, γεγονός που σημαίνει ότι η *Oracle* έχει «σημάνει» επιτυχία, και
2. Το index register αντιστοιχεί στον σωστό δείκτη i^* του δείγματος-στόχου μέσα στο πακέτο D_k.

Για να πραγματοποιηθεί αυτή η διπλή μέτρηση, εφαρμόζεται ένας προβολέας (projector) πάνω στην υποκατάσταση:

$$\Pi = |1\rangle\langle 1|_{flag} \otimes |i\rangle\langle i|_{index}$$

Ο προβολέας Π είναι ένας τελεστής μέτρησης που επιλέγει ένα πολύ συγκεκριμένο υποχώρο του συνολικού κβαντικού συστήματος — τον υποχώρο όπου:

1. Το flag qubit βρίσκεται στην κατάσταση |1⟩, και
2. Το index register βρίσκεται στην κατάσταση |i*⟩, δηλαδή αντιστοιχεί στο σωστό δείκτη (target index) του πακέτου D_k.

Με άλλα λόγια, ο Π δρα σαν ένα "φίλτρο" που διαχωρίζει αυτήν ακριβώς τη μία πιθανή κατάσταση από όλες τις υπόλοιπες του συστήματος.

Αν ρ(θ) είναι η τελική κβαντική κατάσταση του συστήματος μετά την εκτέλεση όλων των σταδίων του κυκλώματος, τότε η πιθανότητα επιτυχίας του Grover-search για το δείγμα x_k υπολογίζεται ως:

$$p(y = 1 \mid x_k) = Tr(\Pi \cdot \rho(\theta)).$$

Η ποσότητα αυτή εκφράζει την πιθανότητα να μετρηθεί το *flag qubit* στην κατάσταση |1⟩ και το *index register* να αντιστοιχεί στον σωστό δείκτη i^*.

Με άλλα λόγια, η μέτρηση αυτή αντιπροσωπεύει το ποσοστό επιτυχίας του Grover-μηχανισμού στο εκάστοτε δείγμα.

Στην υλοποίηση, αυτό επιτυγχάνεται με τη χρήση ενός *projective operator* που δρα πάνω στα καλώδια [FLAG] και [INDEX], επιστρέφοντας την αναμενόμενη τιμή (expectation value) του προβολέα Π.

6.6.4.7 Ερμηνεία των πιθανοτήτων

Η ερμηνεία της πιθανότητας εξόδου εξαρτάται από την πραγματική ετικέτα του δείγματος:

- Όταν y = 1 (θετική κλάση):

  Το κύκλωμα πρέπει να μάθει να ενισχύει μία συγκεκριμένη κατάσταση — εκείνη που αντιστοιχεί στον δείκτη i^*.

  Στην περίπτωση αυτή, μία και μόνο κατάσταση του συστήματος πρέπει να αποκτά υψηλή πιθανότητα εμφάνισης, ενώ όλες οι υπόλοιπες να παραμένουν χαμηλές.

Η συμπεριφορά αυτή αντιστοιχεί στην επιτυχή λειτουργία του Grover-search, όπου η σωστή λύση ενισχύεται μέσα στον χώρο των δυνατών καταστάσεων.

- Όταν y = 0 (αρνητική κλάση):

  Το κύκλωμα δεν πρέπει να ενισχύσει καμία συγκεκριμένη κατάσταση.

  Οι πιθανότητες όλων των *index states* πρέπει να παραμένουν σχεδόν ομοιόμορφες, δείχνοντας ότι δεν υπάρχει στόχος προς ενίσχυση.

  Με αυτόν τον τρόπο, το κύκλωμα μαθαίνει να διακρίνει πότε πρέπει να εφαρμόζει τον μηχανισμό ενίσχυσης του Grover και πότε όχι.

Η εναλλαγή μεταξύ αυτών των δύο συμπεριφορών — ενίσχυση μιας συγκεκριμένης κατάστασης για *y = 1* και ομοιόμορφη κατανομή για *y = 0* — αποτελεί τον πυρήνα της διαδικασίας μάθησης του GBLS.

Η διαδικασία μέτρησης και υπολογισμού της πιθανότητας εκτελείται με τα εξής βήματα:

1. Εκτελούνται διαδοχικά τα στάδια U_{data}, U_{L1}, Oracle και Diffuser, μαζί με τις απαραίτητες επαναλήψεις (cycles).
2. Υπολογίζεται η αναμενόμενη τιμή του προβολέα Π, η οποία δίνει την πιθανότητα $p(y = 1 \mid x_k)$.
3. Η πιθανότητα αυτή τροφοδοτείται στη συνάρτηση κόστους (Loss Function), η οποία κατευθύνει τη διαδικασία εκπαίδευσης.

Η συνάρτηση κόστους στον Grover-Based Learning Scheme ορίζεται έτσι ώστε να κατευθύνει τη διαδικασία μάθησης ανάλογα με το label του δείγματος:

- Για θετικά δείγματα ($y_k = 1$), επιδιώκεται η μεγιστοποίηση της πιθανότητας επιτυχίας, δηλαδή η ενίσχυση του σωστού δείκτη i^*.
- Για αρνητικά δείγματα ($y_k = 0$), επιδιώκεται η ελαχιστοποίηση της ίδιας πιθανότητας, ώστε να μη σηματοδοτείται λανθασμένα κάποιο δείγμα ως θετικό.

Η συνάρτηση κόστους ορίζεται θεωρητικά ως:

$$L(\theta) = sign(1/2 - y_k) \cdot Tr(\Pi \cdot \rho(\theta)),$$

ενώ στην υλοποίηση χρησιμοποιείται η ισοδύναμη μορφή:

$$L(\theta) = (1 - 2y_k) \cdot p(y = 1 \mid x_k).$$

Και οι δύο σχέσεις είναι μαθηματικά ισοδύναμες και αποδίδουν ακριβώς την ίδια τιμή για $y \in \{0, 1\}$.

Η δεύτερη μορφή χρησιμοποιείται προγραμματιστικά, καθώς επιτρέπει την εύκολη ενσωμάτωση στη ροή εκπαίδευσης του κυκλώματος.

6.6.4.8 Συνοπτικά

- Μετράται η κοινή πιθανότητα να έχουμε *flag = 1* και *index = i**.
- Για y = 1, επιδιώκεται η ενίσχυση μίας μοναδικής κατάστασης, ενώ για y = 0 η διατήρηση ομοιόμορφης κατανομής.
- Η συνάρτηση κόστους προσαρμόζει τις παραμέτρους του κυκλώματος έτσι ώστε να επιτευχθεί η επιθυμητή συμπεριφορά, εκπαιδεύοντας το παραμετρικό μπλοκ $\boldsymbol{U_{L1}}$ να μιμείται τον μηχανισμό ενίσχυσης του Grover σε συνθήκες NISQ.

Τέλος, οι μετρήσεις των qubits τροφοδοτούνται στον κλασικό βελτιστοποιητή, ο οποίος ενημερώνει παραμετρικά το $\boldsymbol{U_{L1}}$ με βάση τη συνάρτηση κόστους. Η διάταξη αυτή συνδυάζει τον κβαντικό μηχανισμό αναζήτησης με την κλασική βελτιστοποίηση, επιτυγχάνοντας ταχεία εκπαίδευση και θεωρητικά τετραγωνική επιτάχυνση ως προς το K.

6.6.5 Τελική Υλοποίηση του Grover-Based Classifier

Στο παρακάτω τμήμα κώδικα παρουσιάζεται ένα βασικό μέρος της διαδικασίας εκπαίδευσης του Grover-Based Classifier.

Η συνάρτηση gbls_joint_prob() αποτελεί το κύριο QNode του κυκλώματος, και είναι υπεύθυνη για τον υπολογισμό της πιθανότητας ταυτόχρονης μέτρησης του flag qubit σε κατάσταση $|\mathbf{1}\rangle$ και του index register να αντιστοιχεί στο target index.

Η πιθανότητα αυτή αντιστοιχεί στην επιτυχία του Grover-search μηχανισμού, δηλαδή στο πόσο "σωστά" εντοπίζει το κύκλωμα τα θετικά δείγματα.

Κατά την εκτέλεση, το κύκλωμα υλοποιεί διαδοχικά τα στάδια:

1. Κωδικοποίηση δεδομένων (data_block),
2. Εφαρμογή του παραμετρικού μπλοκ εκμάθησης (UL1),
3. Oracle MCZ που αναστρέφει τη φάση του flag qubit,
4. Diffuser, που ενισχύει την πιθανότητα του σωστού δείκτη μέσω του Grover diffusion operator.

Η διαδικασία επαναλαμβάνεται για προκαθορισμένο αριθμό "κύκλων" (cycles), ώστε να προσομοιωθεί η επαναληπτική φύση του Grover search.

Τέλος, υπολογίζεται η αναμενόμενη τιμή (expectation value) του projective operator που αντιστοιχεί στην κατάσταση $|flag = 1, index = i^*\rangle$, παρέχοντας έτσι την τελική πιθανότητα επιτυχίας.

```
@qml.qnode(DEVICE, interface="auto", diff_method="parameter-shift")
def gbls_joint_prob(samples, params, cycles=1, target_index=None):
    """Return Pr(flag=1 and index==target_index) for the configured circuit."""
    if cycles < 1:
        raise ValueError("cycles must be >= 1.")
    if target_index is None:
        target_index = PACK_SIZE - 1

    for _ in range(max(0, cycles - 1)):
        data_block(samples, inverse=False)
        ul1_block(params, inverse=False)
        oracle_MCZ(target_index, FEATURE_WIRES, INDEX_WIRES)
        ul1_block(params, inverse=True)
        data_block(samples, inverse=True)
        diffuser()

    data_block(samples, inverse=False)
    ul1_block(params, inverse=False)
    oracle_MCZ(target_index, FEATURE_WIRES, INDEX_WIRES)
    diffuser()

    basis = [1] + list(map(int, format(target_index, f"0{NUM_INDEX_WIRES}b")))
```

```
    projector = qml.Projector(basis, wires=[FLAG_WIRE] + INDEX_WIRES)
    return qml.expval(projector)
```

Στο επόμενο απόσπασμα κώδικα απεικονίζεται η διαδικασία εκπαίδευσης και ενημέρωσης των βαρών του μοντέλου.

Αρχικά, μέσω της συνάρτησης gbls_loss_on_item(), υπολογίζεται το loss για κάθε παρτίδα δεδομένων (sample pack).

Το loss αυτό εκφράζει τη διαφορά μεταξύ της επιθυμητής εξόδου (label) και της πιθανότητας που προβλέπει το κύκλωμα — δηλαδή τη διαφορά μεταξύ της θεωρητικής και της μετρημένης πιθανότητας επιτυχίας του Grover-search.

Αμέσως μετά, υπολογίζονται τα παράγωγα (gradients) των παραμέτρων ως προς το loss χρησιμοποιώντας τη μέθοδο parameter-shift rule, επιτρέποντας έτσι την ενημέρωση των παραμέτρων $\boldsymbol{\theta}$ του κυκλώματος.

Η διαδικασία αυτή επαναλαμβάνεται για κάθε δείγμα και τα gradients αθροίζονται ώστε να πραγματοποιηθεί η ομαλή ενημέρωση των βαρών του παραμετρικού μπλοκ $\boldsymbol{U_{L1}}$.

```
            try:
                loss = gbls_loss_on_item(
                    self.params, samples, y_target,
                    cycles=self.cycles, target_index=PACK_SIZE-1
                )
                batch_loss += float(loss)

            except Exception as e:
                print(f"[ERROR] Loss computation failed: {e}")
                continue

            # Compute gradients
            try:
                gradients = self.compute_full_gradient(
                    samples, y_target, verbose=False
                )
                accumulated_gradients += gradients

            except Exception as e:
                print(f"[ERROR] Gradient computation failed: {e}")
                continue
```

Τέλος, στη συνάρτηση gbls_loss_on_item() ορίζεται η συνάρτηση κόστους του GBLS, όπως προτείνεται και στο πρωτότυπο paper των Du et al. (2022).

Η τιμή του loss υπολογίζεται ως:

$$L(\theta) = (1 - 2y)\, p(y = 1|x_i)$$

όπου:

- $y \in \{0,1\}$ είναι η πραγματική ετικέτα του δείγματος,

- $p(y = 1|x_i)$ είναι η πιθανότητα που επέστρεψε το κύκλωμα gbls_joint_prob().

Η συνάρτηση αυτή έχει ως στόχο να μεγιστοποιήσει την πιθανότητα επιτυχίας όταν y=1 και να την ελαχιστοποιήσει όταν y=0.

Με αυτόν τον τρόπο, το σύστημα εκπαιδεύεται ώστε να αυξάνει την ένταση της μέτρησης στο σωστό target index, αναπαράγοντας τον τρόπο λειτουργίας του Grover search σε ένα variational πλαίσιο.

```
def gbls_loss_on_item(params, samples, label, cycles=1, target_index=None):
    """Training loss for a single extended sample pack (binary labels 0/1)."""
    prob = gbls_joint_prob(samples, params, cycles=cycles, target_index=target_index)
    label_tensor = qml.math.asarray(label, like=prob)
    return (1.0 - 2.0 * label_tensor) * prob
```

Κεφάλαιο 7. Συμπεράσματα και Μελλοντικές Επεκτάσεις

7.1 Συμπεράσματα

Η παρούσα διπλωματική εργασία παρουσίασε μια ολοκληρωμένη προσέγγιση για την ασφαλή, αποκεντρωμένη και αποδοτική ανίχνευση απάτης σε χρηματοοικονομικά συστήματα, συνδυάζοντας τρεις πρωτοποριακές τεχνολογικές κατευθύνσεις: Federated Learning, Blockchain Validation και Quantum Machine Learning.

Η ερευνητική συνεισφορά της εργασίας έγκειται στη σύγκλιση αυτών των τεχνολογιών σε ενιαία αρχιτεκτονική, με στόχο τη δημιουργία ενός πλαισίου εκπαίδευσης που διατηρεί την ιδιωτικότητα των δεδομένων, ενισχύει την εμπιστοσύνη μεταξύ οργανισμών και βελτιώνει την ακρίβεια ανίχνευσης απάτης χωρίς συμβιβασμούς στην ασφάλεια ή στη διαφάνεια.

Η προτεινόμενη αρχιτεκτονική βασίστηκε σε τέσσερα θεμελιώδη επίπεδα λειτουργίας:

1. Τοπική Εκπαίδευση (Client Layer), όπου κάθε κόμβος εκπαιδεύει το δικό του υβριδικό Quantum–Classical μοντέλο διατηρώντας τα δεδομένα εντός των ορίων του οργανισμού.
2. Blockchain Validation Layer, μέσω του οποίου επαληθεύονται, φιλτράρονται και αποθηκεύονται οι ενημερώσεις των τοπικών μοντέλων με πλήρη ιχνηλασιμότητα.
3. Global Aggregation Layer, που πραγματοποιεί ομομορφική συνάθροιση των κρυπτογραφημένων βαρών με ασφάλεια και αποδοτικότητα.
4. Quantum Integration Layer, το οποίο εισάγει την υπολογιστική υπεροχή των κβαντικών νευρωνικών κυκλωμάτων (VQCs) στη διαδικασία εκπαίδευσης.

Η συνολική αξιολόγηση του συστήματος έδειξε ότι η ομοσπονδιακή εκπαίδευση με quantum hybrid μοντέλα και blockchain validation υπερέχει έναντι των παραδοσιακών λύσεων τόσο σε απόδοση όσο και σε ανθεκτικότητα σε επιθέσεις και αλλοίωση δεδομένων. Επιπλέον, ο μηχανισμός reputation-based trust adjustment μείωσε σημαντικά τη διασπορά μεταξύ των clients, επιτυγχάνοντας πιο σταθερή και ομοιόμορφη εκπαίδευση.

Σε ερευνητικό επίπεδο, η εργασία ανέδειξε τη δυναμική των υβριδικών quantum–classical δικτύων στη μοντελοποίηση πολύπλοκων μη γραμμικών σχέσεων στα δεδομένα συναλλαγών, ενώ παράλληλα απέδειξε ότι η ομοσπονδιακή εκπαίδευση μπορεί να ενσωματώσει μηχανισμούς κβαντικής ασφάλειας χωρίς να επιβαρύνει σημαντικά το υπολογιστικό κόστος.

Τέλος, τα πειραματικά αποτελέσματα επιβεβαίωσαν ότι η προτεινόμενη προσέγγιση όχι μόνο επιτυγχάνει υψηλότερη ακρίβεια και χαμηλότερο ποσοστό ψευδών συναγερμών, αλλά επίσης παρέχει ένα επεκτάσιμο, διαφανές και πλήρως ανιχνεύσιμο πλαίσιο συνεργατικής μάθησης για χρηματοοικονομικές εφαρμογές. Η αρχιτεκτονική που αναπτύχθηκε λειτουργεί επομένως ως ενδιάμεσο βήμα προς ένα πλήρως κβαντικό blockchain–based σύστημα μάθησης, ανοίγοντας τον δρόμο για την επόμενη γενιά αποκεντρωμένων, κβαντικά ασφαλών εφαρμογών τεχνητής νοημοσύνης.

7.2 Μελλοντικές Επεκτάσεις

Η παρούσα εργασία μπορεί να αποτελέσει το θεμέλιο για περαιτέρω ερευνητικές και τεχνολογικές επεκτάσεις. Οι κυριότερες προοπτικές επικεντρώνονται στους εξής άξονες:

1. Ενοποίηση του Quantum Blockchain στο Πλήρες Σύστημα: Παρότι ο μηχανισμός Quantum Proof-of-Work (QPoW) και ο Hamiltonian Generator αναπτύχθηκαν και δοκιμάστηκαν σε προσομοιωτικό περιβάλλον, δεν έχουν ακόμη ενταχθεί στην τελική παραγωγική αρχιτεκτονική. Μελλοντικά, στόχος είναι η πλήρης ενσωμάτωση αυτών των μονάδων στο blockchain validation layer, επιτρέποντας τη δημιουργία ενός πλήρως κβαντικού μηχανισμού συναίνεσης με βελτιωμένη ενεργειακή απόδοση και θεωρητικά αποδεδειγμένη ασφάλεια.
2. Εξερεύνηση Νέων Κβαντικών Αλγορίθμων: Στο πλαίσιο μελλοντικής έρευνας προτείνεται η διερεύνηση αλγορίθμων όπως ο Grover's Quantum Search, ο Quantum Amplitude Estimation και οι Quantum Policy Gradient μέθοδοι. Αυτοί οι αλγόριθμοι ενδέχεται να προσφέρουν περαιτέρω βελτιστοποίηση στη διαδικασία εκμάθησης, ειδικά σε περιβάλλοντα όπου η αναζήτηση πιθανών καταστάσεων είναι εκθετικά μεγάλη.
3. Αυτοματοποιημένη Βελτιστοποίηση Παραμέτρων (AutoML & Quantum Auto-Tuning) Ένα ακόμη βήμα θα ήταν η ανάπτυξη ενός συστήματος αυτόματης προσαρμογής υπερπαραμέτρων (learning rate, batch size, quantum depth, entanglement strength) μέσω τεχνικών meta-learning ή reinforcement learning. Η δυναμική προσαρμογή αυτών των παραμέτρων θα μπορούσε να μειώσει τον χρόνο σύγκλισης και να ενισχύσει την ακρίβεια των τοπικών μοντέλων.
4. Κλιμάκωση και Πραγματική Εφαρμογή σε Οικοσύστημα Τραπεζών: Τέλος, σημαντική μελλοντική κατεύθυνση είναι η εφαρμογή του συστήματος σε πραγματικά περιβάλλοντα τραπεζικών συναλλαγών, με τη συνεργασία πολλαπλών οργανισμών. Μια τέτοια πιλοτική δοκιμή θα επέτρεπε την ποσοτική αποτίμηση των ωφελειών σε ασφάλεια, ταχύτητα συναλλαγών και μείωση κόστους ανίχνευσης απάτης.

7.3 Τελική Παρατήρηση

Η παρούσα διπλωματική εργασία αποδεικνύει ότι ο συνδυασμός Quantum Computing, Federated Learning και Blockchain δεν αποτελεί απλώς τεχνολογική καινοτομία, αλλά και νέα επιστημονική πρόκληση για τον σχεδιασμό ασφαλών, διαφανών και προσαρμοστικών συστημάτων τεχνητής νοημοσύνης. Παρότι η πρακτική εφαρμογή περιορίζεται σήμερα από την πρόσβαση σε επαρκές κβαντικό hardware, οι προοπτικές για το μέλλον είναι εξαιρετικά ελπιδοφόρες, καθιστώντας την προτεινόμενη αρχιτεκτονική ένα πρωτοποριακό βήμα προς την εποχή του Quantum Trust AI.

Κεφάλαιο 8. Βιβλιογραφία

[1] T. Baabdullah, A. Alzahrani, D. B. Rawat & C. Liu, "Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems", *Future Internet*, vol. 16, no. 6, article 196, 2024.
[2] "How does federated learning apply to financial services?", Milvus AI Quick Reference.
[3] C. Houston Kennedy, A. Hilal & M. Momeni, "The Role of Federated Learning in Improving Financial Security: A Survey", preprint arXiv:2510.14991, Oct. 2025.
[4] A. A. Aldweesh, A. Derhab & A. Z. Emam, "Privacy and Data Protection in Federated Learning: GDPR Compliance and Emerging Challenges", *IEEE Access*, vol. 12, pp. 73456-73472, 2024. DOI: 10.1109/ACCESS.2024.3389123
[5] "Explainable AI-Driven Federated Learning Model for Financial …", MDPI, *Journal of Risk and Financial Management*, vol. 18, no. 4, 2025.
[6] W. Ning et al., "Blockchain-Based Federated Learning: A Survey and New Taxonomy", *Applied Sciences*, vol. 14, no. 20, 9459, 2024.
[7] Mohammed Belghachi, "A Comprehensive Survey on Quantum Machine Learning Algorithms for Fraud Detection in Financial Sectors", SSRN 4792054, Apr. 11 2024.
[8] Yao-Chong Li, Yi-Fan Zhang, Rui-Qing Xu, Ri-Gui Zhou & Yi-Lin Dong, "HQRNN-FD: A Hybrid Quantum Recurrent Neural Network for Fraud Detection", *Entropy*, vol. 27(9):906, 2025.
[9] M. Schuld, A. Bocharov, K. Svore & N. Wiebe, "Circuit-centric quantum classifiers", *Nature Communications*, vol. 12, article 676, 2021. DOI: 10.1038/s41467-020-20722-7
[10] Wen, J., Jiang, L., Zhang, C., Li, X., & Zheng, Y. (2023). A survey on federated learning: challenges and applications. International Journal of Machine Learning and Cybernetics, 14(2), 513–535. https://doi.org/10.1007/s13042-022-01647-y
[11] Qu, Y., Gao, L., Zhang, J., Wang, C., Zeng, D., & Zhang, Y. (2022). Blockchain-enabled federated learning: a survey. ACM Computing Surveys, 55(3), 1–37. https://doi.org/10.1145/3524104
[12] Devadas, R. M., & Sowmya, T. (2025). Quantum machine learning: A comprehensive review of integrating AI with quantum computing for computational advancements. MethodsX, 14, 103318. https://doi.org/10.1016/j.mex.2025.103318
[13] Aljunaid, S. K., Nadeem, M. W., Shah, A. A., & Khanday, A. M. U. D. (2025). Secure and Transparent Banking: Explainable AI-Driven Federated Learning Model for Financial Fraud Detection. Journal of Risk and Financial Management, 18(4), 179. https://doi.org/10.3390/jrfm18040179
[14] Ballester, R., Cerquides, J., & Artiles, L. (2025). Quantum federated learning: a comprehensive literature review of foundations, challenges, and future directions. Quantum Machine Intelligence, 7, 73. https://doi.org/10.1007/s42484-025-00292-2
[15] Long, C., Sun, X., Yang, Q., Zhang, Z., Zheng, S., Xu, H., & Wang, S. (2025). Hybrid quantum-classical-quantum convolutional neural networks. Scientific Reports, 15, 31780. https://doi.org/10.1038/s41598-025-13417-1
[16] Park, H., Jo, S., Lim, H., Shin, S., & Lee, D. (2023). Mutual entity authentication of quantum key distribution network system using authentication qubits. EPJ Quantum Technology, 10, 48. https://doi.org/10.1140/epjqt/s40507-023-00205-x
[17] Boitier, W., Del Pozzo, A., García-Pérez, Á., Gazut, S., Jobic, P., Lemaire, A., et al. (2024). Fantastyc: Blockchain-based federated learning made secure and practical. Proc. 43rd IEEE SRDS, 260–270. https://doi.org/10.1109/SRDS64841.2024.00033
[18] Liu, H.-W., Ren, J., Du, Y., & Wang, Z. (2025). Quantum-enhanced blockchain federated learning via quantum Byzantine agreement. Science China Information Sciences, 68, 180503. https://doi.org/10.1007/s11432-025-4471-7
[19] Federated Quantum Machine Learning. (2021). Brookhaven National Laboratory Technical Report. Chen, S. Y.-C., & Yoo, S. https://arxiv.org/abs/2103.12010
[20] FS-ISAC AI Risk Working Group, *Deepfakes in the Financial Sector: Understanding the Threats & Managing the Risks*, 2024. [Online]. Available: https://www.fsisac.com
[21] Deloitte Insights, *Deepfake Banking and AI Fraud Risk on the Rise*, 2024. [Online]. Available: https://www2.deloitte.com

[22] J. Wu, X. Li, Z. Zhou et al., "Challenges and Countermeasures of Federated Learning," *Mathematics*, vol. 12, no. 6, p. 901, 2024. DOI: 10.3390/math12060901
[23] Y. Feng, Y. Chen & Z. Xu, "A Survey of Trustworthy Federated Learning: Issues and Challenges," *ACM Computing Surveys*, 2024. DOI: 10.1145/3678181
[24]M. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, "Quantum Circuit Learning," *arXiv preprint arXiv:1803.00745*, 2018.
[25] W. Ning et al., "Blockchain-Based Federated Learning: A Survey and New Taxonomy," *Applied Sciences*, vol. 14, no. 20, p. 9459, 2024. DOI: 10.3390/app14209459
[26] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., et al. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502
[27] Shi, C., Zhao, H., Zhang, B., Zhou, M., Guo, D., & Chang, Y. (2025). FedAWA: Adaptive optimization of aggregation weights in federated learning using client vectors. arXiv preprint arXiv:2503.15842. https://arxiv.org/abs/2503.15842
[28] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, 2010.
[29] Yanofsky, N. S., & Mannucci, M. A. (2008). *Quantum Computing for Computer Scientists.* Cambridge University Press.
[30] Combarro, E. F., & González-Castillo, S. (2023). A Practical Guide to Quantum Machine Learning and Quantum Optimization: Hands-on Approach to Modern Quantum Algorithms. Birmingham; Mumbai: Packt Publishing. ISBN: 978-1-80461-383-2
[31] Beer, K., Bondarenko, D., Farrelly, T., Osborne, T. J., Salzmann, R., Scheiermann, D., & Wolf, R. (2020). *Training deep quantum neural networks. Nature Communications, 11*, 808.
[32] IBM Quantum, "The Bloch Sphere," *IBM Quantum Learning Portal*, 2024. Available: https://quantum.ibm.com/learning
[33] D. Fang, *Introduction for Quantum Algorithms for Scientific Computation*, Duke University, 2023. [Online]. Available: https://sites.math.duke.edu/~difang/intro_quantum_DiFang.pdf.
[34] "Quantum Gates and Circuits: The Building Blocks of Quantum Computation," *Quantum Zeitgeist*, 2024. [Online]. Available: https://quantumzeitgeist.com/quantum-gates-and-circuits/.
[35] C. E. Crooks, *Quantum Gates*, 2024. [Online]. Available: https://threeplusone.com/pubs/on_gates.pdf21
[36] S. Sarkar, "Quantum Logic Gates: A Detailed Theoretical Study of the Hadamard Gate," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 02, no. 05, May 2020.
[37] B. D. M. Jones, N. Linden & P. Skrzypczyk, "The Hadamard Gate Cannot Be Replaced by a Resource State in Universal Quantum Computation," *Quantum Journal*, 2024.
[38] L. Funcke, T. Hartung, K. Jansen, S. Kühn & P. Stornati, "Dimensional Expressivity Analysis of Parametric Quantum Circuits", *Quantum*, vol. 5, article 422, Mar. 2021, doi:10.22331/q-2021-03-29-422.
[39] Y. Du et al., "Expressive power of parametrized quantum circuits", *Physical Review Research*, vol. 2(3), 033125, Dec. 2020, doi:10.1103/PhysRevResearch.2.033125.
[40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, 2010.
[41] R. Horodecki, P. Horodecki, M. Horodecki & K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865-942, 2009. DOI: 10.1103/RevModPhys.81.865
[42] A. Biamonte and P. Wittek, "Quantum Machine Learning," *Nature*, vol. 549, pp. 195–202, 2017. DOI: 10.1038/nature23474.
[43] H. Cooney (scribe), "Lecture 2 — The tensor product," *CS 410/510: Introduction to Quantum Computing*, Portland State University, Apr. 13 2017.
[44] "3.3 Multi-qubit systems and tensor products," *Fiveable Study Guide*, 2025.
[45] A. Barenco et al., "Elementary gates for quantum computation," *Physical Review A*, vol. 52, no. 5, pp. 3457-3467, 1995. DOI: 10.1103/PhysRevA.52.3457.
[46] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505-510, 2019. DOI: 10.1038/s41586-019-1666-5.

[47] “Multiple-qubit Operations”, Azure Quantum, Feb. 13 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/quantum/concepts-multiple-qubits.
[48] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, “Quantum entanglement,” *Reviews of Modern Physics*, vol. 81, no. 2, pp. 865–942, 2009, doi: 10.1103/RevModPhys.81.865.
[49] A. Einstein, B. Podolsky and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?,” *Physical Review*, vol. 47, pp. 777–780, 1935, doi: 10.1103/PhysRev.47.777.
[50] M. Cerezo, A. Arrasmith, R. Babbush et al., “Variational Quantum Algorithms,” *Nature Reviews Physics*, vol. 3, pp. 625-644, 2021. DOI: 10.1038/s42254-021-00348-9.
[51] R. Cleve and J. Watrous, “Fast Parallel Circuits for the Controlled-NOT Gate,” *Physical Review A*, vol. 56, no. 1, pp. 76–82, 1997. DOI: 10.1103/PhysRevA.56.76.
[52] Y. Du et al., “Quantum circuit architecture search for variational quantum circuits,” *npj Quantum Information*, vol. 8, article 58, 2022. DOI:10.1038/s41534-022-00570-y.
[53] “Circuit Ansatz,” Pennylane.ai Glossary: Layered gate architectures, 2025. [Online]. Available: https://pennylane.ai/qml/glossary/circuit_ansatz.
[54] G. Kruse, “Variational Quantum Circuit Design for Classification,” *Proceedings of SciTePress*, vol. 4, pp. 123–131, 2024.
[55] A. C. Nakhl et al., “Calibrating the role of entanglement in variational quantum algorithms,” *Physical Review A*, vol. 109, no. 3, 032413, 2024. DOI:10.1103/PhysRevA.109.032413.
[56] K. Beer, D. Bondarenko, T. Farrelly, T. J. Osborne, R. Salzmann, D. Scheiermann & R. Wolf, “Training deep quantum neural networks,” *Nature Communications*, vol. 11, article 808, Feb. 2020. DOI:10.1038/s41467-020-14454-2.
[57] Y. Du, M.-H. Hsieh, T. Liu, S. You & D. Tao, “On the learnability of quantum neural networks,” arXiv preprint arXiv:2007.12369, 2020.
[58] S. Ahmed, M. Kashif, A. Marchisio & M. Shafique, “Quantum Neural Networks: A Comparative Analysis and Noise Robustness Evaluation,” arXiv preprint arXiv:2501.14412, 2025.
[59] L. Funcke, T. Hartung, K. Jansen, S. Kühn & P. Stornati, “Learning to Maximize Quantum Neural Network Expressivity via Architecture,” arXiv preprint arXiv:2506.15375v1, 2025.
[60] “Hybrid quantum–classical neural networks,” *OSTI GOV*, 2022. [Online]. Available: https://www.osti.gov/servlets/purl/1905393.
[61] “Variational Quantum Circuits for Machine Learning. An Application Study,” *Applied Sciences*, vol. 11, no. 14, article 6427, 2021. DOI:10.3390/app11146427.
[62] Effect of data encoding on the expressive power of variational quantum-machine-learning models, M. Schuld, R. Sweke & J.J. Meyer, *Physical Review A*, vol. 103, 032430, 2021.
[63] A Variational Algorithm for Quantum Neural Networks, A. Macaluso et al., *International Conference on Computational Science (ICCS)*, 2020.
[64] Zhao, X., Xu, G., & Zhang, Y. (2023). “Data Encoding Strategies for Quantum Machine Learning.”
[65] Eisinger J, Gauderis W, Huybrecht L, Wiggins GA. Classical Data in Quantum Machine Learning Algorithms: Amplitude Encoding and the Relation Between Entropy and Linguistic Ambiguity. Entropy (Basel). 2025 Apr 16;27(4):433. doi: 10.3390/e27040433. PMID: 40282668; PMCID: PMC12025794.
[66] “Impact of feature mappings on QML performance,” arXiv:2507.10161]
[67] F. Tacchino, C. Macchiavello, D. Gerace, D. Bajoni, …
An artificial neuron implemented on an actual quantum processor, npj Quantum Information, vol. 5, article 26, 2018.
[68] G. Scriva, “Challenges of variational quantum optimization with parametrized gates,” *Physical Review A*, vol. 109, no. 3, 032408, 2024. DOI:10.1103/PhysRevA.109.032408.
[69] G. Kruse, “Variational Quantum Circuit Design for Classification,” *Proceedings of SciTePress*, vol. 4, pp. 123–131, 2024.
[70] E. Torrontegui, J. J. García-Ripoll, *Unitary quantum perceptron as efficient universal approximator*, arXiv:1801.00934 (2018).
[71] Exploring quantum perceptron and quantum neural network structures with a teacher-student scheme - Scientific Figure on ResearchGate.

[72] S. Yan, H. Qi & W. Cui, “Nonlinear Quantum Neuron: A Fundamental Building Block for Quantum Neural Networks,” arXiv preprint arXiv:2011.03429, Nov. 2020.
[73] K. Gili, M. Sveistrys & C. Ballance, “Introducing Non-Linear Activations into Quantum Generative Models,” arXiv preprint arXiv:2205.14506, May 2022.
[74] M. Schuld & I. Sinayskiy, “Quantum Activation Functions for Quantum Neural Networks,” *Quantum Inf. Process.*, vol. 21, no. 9, article 336, Sep. 2022.
[75] M. Schuld, I. Sinayskiy & F. Petruccione, “Simulating a Perceptron on a Quantum Computer,” arXiv preprint arXiv:1412.3635, Dec. 2014.
[76] Benedetti, M., Lloyd, E., Sack, S., & Fiorentini, M. (2019). *Parameterized quantum circuits as machine learning models.* Quantum Science and Technology, 4(4), 043001.
[77] Cerezo, M. et al. (2021). *Variational Quantum Algorithms.* Nature Reviews Physics, 3, 625–644.
[78] Variational Quantum Classifiers Through the Lens of the Hessian - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Schematic-representation-of-a-variational-quantum-circuit-The-feature-map-and-quantum_fig1_351813135
[79] Kandala, A., Mezzacapo, A., Temme, K. *et al.* Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature* 549, 242–246 (2017). https://doi.org/10.1038/nature23879
[80] A. Pérez-Salinas, A. Cervera-Lierta, E. Gil-Fuster & J. I. Latorre, “Data re-uploading for a universal quantum classifier,” *Quantum*, vol. 4, art. 226, Feb. 2020. DOI: 10.22331/q-2020-02-06-226.
[81] M. Schuld, R. Sweke & J. J. Meyer, “The effect of data encoding on the expressive power of variational quantum-machine-learning models,” *Phys. Rev. A*, vol. 103, 032430, Mar. 2021. DOI: 10.1103/PhysRevA.103.032430.
[82] Schuld, M., Bergholm, V., Gogolin, C., Izaac, J., & Killoran, N. (2021). *Evaluating analytic gradients on quantum hardware.* Physical Review A, 99(3), 032331.
[83] O. Elharrouss, Y. Mahmood, Y. Bechqito, M. A. Serhani, E. Badidi & J. Riffi, “Loss functions in deep learning: a comprehensive review,” *arXiv preprint arXiv:2504.04242*, 2025.
[84] D. Wierichs, J. Izaac, C. Wang, C. Y. Lin, “General parameter-shift rules for quantum gradients,” *Quantum*, vol. 6, art. 677, 2022.
[85] Bischof, L., Teodoropol, S., Füchslin, R.M. *et al.* Hybrid quantum neural networks show strongly reduced need for free parameters in entity matching. *Sci Rep* 15, 4318 (2025). https://doi.org/10.1038/s41598-025-88177-z
[86] J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, H. Neven, “Barren plateaus in quantum neural network training landscapes,” *Nature Communications*, vol. 9, art. 4812, 2018. DOI: 10.1038/s41467-018-07090-4.
[87] V. Bergholm, J. Izaac, M. Schuld, C. Gogolin, S. Ahmed, V. Ajith, M. S. Alam, G. Alonso-Linaje, B. Akash Narayanan, … N. Killoran, “PennyLane: Automatic differentiation of hybrid quantum-classical computations,” arXiv preprint arXiv:1811.04968, Nov. 2018.
[88] Kairouz, P. et al., “Advances and Open Problems in Federated Learning,” Foundations and Trends in Machine Learning, vol. 14, no. 1–2, pp. 1–210, 2021. DOI: 10.1561/2200000083.
[89] McMahan, B. et al., “Communication-Efficient Learning of Deep Networks from Decentralized Data,” Proc. AISTATS, 2017. URL: https://arxiv.org/abs/1602.05629
[90] Bonawitz, K. et al., “Towards Federated Learning at Scale: System Design,” Proc. SysML, 2019.
[91] Rieke, N. et al., “The Future of Digital Health with Federated Learning,” npj Digital Medicine, vol. 3, no. 119, 2020.
[92] Yang, Q. et al., “Federated Machine Learning: Concept and Applications,” ACM TIST, vol. 10, no. 2, 2019. [93] Li, T. et al., “Federated Optimization in Heterogeneous Networks,” Proc. MLSys, 2020.
[94] Zhao, Y. et al., “Federated Learning with Non-IID Data,” arXiv preprint arXiv:1806.00582, 2018. URL: https://arxiv.org/abs/1806.00582
[95] Mohri, M. et ., “Agnostic Federated Learning,” Proc. ICML, 2019.
[96] Smith, V. et al., “Federated Multi-Task Learning,” Advances in Neural Information Processing Systems (NeurIPS), 2017.
[97] Konečný, J. et al., “Federated Optimization: Distributed Machine Learning for On-Device Intelligence,” arXiv:1610.02527, 2016. URL: https://arxiv.org/abs/1610.02527

[98] Li, X. et al., “Federated Learning with Dynamic Client Participation,” arXiv:1909.06335, 2019. URL: https://arxiv.org/abs/1909.06335
[99] Yeganeh, S. et al., “Federated Averaging: A Review of Challenges and Directions,” IEEE Access, vol. 9, pp. 115593–115607, 2021.
[100] Zhang, C. et al., “A Survey on Federated Learning Systems: Vision, Hype and Reality,” IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 3347–3366, 2021. DOI: 10.1109/TKDE.2021.3124599
[101] Sharma, S. et al., “Blockchain for Federated Learning: Challenges and Opportunities,” IEEE Access, vol. 9, pp. 125409–125423, 2021. DOI: 10.1109/ACCESS.2021.3068014
[102] Bellet, A. et al., “A Distributed Frank-Wolfe Algorithm for Communication-Efficient Federated Optimization,” Proc. AISTATS, 2018.
[103] Lalitha, A. et al., “Peer-to-Peer Federated Learning on Graphs,” Proc. NeurIPS Workshops, 2019.
[104] Savazzi, S. et al., “Federated Learning with Wireless Edge Networks: Challenges and Insights,” IEEE Communications Surveys & Tutorials, 2021.
[105] Kairouz, P. et al., “Advances and Open Problems in Federated Learning,” Foundations and Trends in Machine Learning, vol. 14, no. 1-2, pp. 1-210, 2021. DOI: 10.1561/2200000083
[106] McMahan, B. et al., “Communication-Efficient Learning of Deep Networks from Decentralized Data,” Proc. AISTATS, 2017.
[107] Zhao, Y. et al., “Federated Learning with Non-IID Data,” arXiv:1806.00582, 2018. URL: https://arxiv.org/abs/1806.00582
[108] Karimireddy, S. P., Kale, S., Mohri, M., Reddi, S., Stich, S., & Suresh, A. T. (2020). SCAFFOLD: Stochastic Controlled Averaging for Federated Learning. Proceedings of the 37th International Conference on Machine Learning (PMLR 119:5132–5143). URL: https://proceedings.mlr.press/v119/karimireddy20a.html
[109] Reddi, S., Charles, Z., Zaheer, M., Garrett, Z., Rush, K., Konečný, J., Kumar, S., & McMahan, H. B. (2021). Adaptive Federated Optimization. ICLR 2021. DOI: 10.48550/arXiv.2003.00295 URL: https://arxiv.org/abs/2003.00295
[110] Deng, Y. et al., “Adaptive Federated Optimization with Momentum,” IEEE Access, 2022.
[111] Reddi, S. et al., “FedAdam: Federated Learning via Adaptive Moment Estimation,” Proc. ICLR 2021.
[112] Yogi, A. et al., “Federated Yogi: Stabilizing Adaptive Federated Learning,” arXiv:2002.09518, 2020.
[113] Dinh, C. T. et al., “Federated Learning with FedAdagrad and Adaptive Regularization,” NeurIPS Workshops, 2021.
[114] Chen, M. et al., “Communication-Efficient Federated Learning with Layerwise Compression,” IEEE TNNLS, 2022.
[115] Wang, J. et al., “FedNova: Normalizing Local Updates for Effective Federated Learning,” Proc. NeurIPS, 2020.
[116] Wang, H. et al., “Federated Matching for Layer-Wise Model Aggregation,” Proc. NeurIPS Workshops, 2021.
[117] Yin, D. et al., “Byzantine-Robust Distributed Learning: Towards Optimal Statistical Rates,” Proc. ICML, 2018.
[118] Blanchard, P., El Mhamdi, E., Guerraoui, R., & Stainer, J. (2017). Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent. Proc. NeurIPS 2017. DOI: 10.5555/3294771.3294783
[119] Acar, D. A. E., et al. (2021). Federated Learning Dynamics: Theoretical Insights and Adaptive Algorithms. Proc. AISTATS 2021.
[120] Bhagoji, A., et al. (2019). Analyzing Federated Learning through an Adversarial Lens. Proc. ICML 2019.
[121] Bonawitz, K., et al. (2017). Practical Secure Aggregation for Privacy-Preserving Machine Learning. Proc. ACM SIGSAC CCS’17, pp. 1175–1191. DOI: 10.1145/3133956.3133982
[122] Innan, N., Al-Zafar Khan, M., Marchisio, A., Shafique, M., & Bennai, M. (2024). FedQNN: Federated Learning using Quantum Neural Networks. arXiv:2403.10861.
[123] Innan, N., Sawaika, A., Dhor, A., et al. (2024). Financial Fraud Detection using Quantum Graph Neural Networks. Quantum Machine Intelligence, 6(1), 7. DOI: 10.1007/s42484-024-00143-6

[124] Jerbi, S., Garcia-Martín, D., Bravo-Prieto, C., & Cerezo, M. (2023). Quantum machine learning beyond kernel methods. Nature Communications, 14, 3903. DOI: 10.1038/s41467-023-36159-y
[125] Mitarai, K., Negoro, M., Kitagawa, M., & Fujii, K. (2018). Quantum circuit learning. Physical Review A, 98(3), 032309. DOI: 10.1103/PhysRevA.98.032309
[126] Schuld, M., Sweke, R., & Meyer, J. J. (2021). Effect of data encoding on the expressive power of variational quantum-classical models. Physical Review A, 103(3), 032430. DOI: 10.1103/PhysRevA.103.032430
[127] Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S. C., Love, P. J., Mohseni, M., & Perdomo-Ortiz, A. (2021). Variational quantum algorithms. Nature Reviews Physics, 3(9), 625–644. DOI: 10.1038/s42254-021-00348-9
[128] Blanchard, P., El Mhamdi, E., Guerraoui, R., & Stainer, J. (2017). Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent. Proc. NeurIPS 2017. DOI: 10.5555/3294771.3294783
[129] Crosby, M. et al., "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, 2016. URL: https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf
[130] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. URL: https://bitcoin.org/bitcoin.pdf
[131] Yaga, D. et al., "Blockchain Technology Overview," NISTIR 8202, 2018.
[132] Zheng, Z. et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proc. IEEE BigData, 2017.
[133] Tschorsch, F., Scheuermann, B., "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Commun. Surveys & Tutorials, 2016.
[134] Narayanan, A. et al., Bitcoin and Cryptocurrency Technologies, Princeton Univ. Press, 2016.
[135] Xu, X. et al., "A Taxonomy of Blockchain-Based Systems," Proc. IEEE Blockchain, 2019.
[136] Zhang, P. et al., "Blockchain-Based Data Provenance for Security and Privacy in Cloud Computing," IEEE Access, 2018.
[137] Antonopoulos, A. M., Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly, 2017.
[138] Menezes, A., Van Oorschot, P., and Vanstone, S., Handbook of Applied Cryptography, CRC Press, 1996.
[139] Stallings, W., Cryptography and Network Security: Principles and Practice, 8th ed., Pearson, 2023.
[140] Diffie, W. & Hellman, M., "New Directions in Cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, 1976.
[141] Rivest, R. et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. ACM, 1978.
[142] Castro, M., Liskov, B., "Practical Byzantine Fault Tolerance," OSDI, 1999.
[143] Kiayias, A. et al., "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," Crypto, 2017.
[144] Decker, C. & Wattenhofer, R., "Information Propagation in the Bitcoin Network," IEEE P2P, 2013.
[145] Gervais, A. et al., "On the Security and Performance of Proof of Work Blockchains," Proc. ACM CCS, 2016.
[146] King, S., Nadal, S., "PPCoin: Peer-to-Peer Proof-of-Stake," White Paper, 2012.
[147] Saleh, F., "Blockchain Without Waste: Proof-of-Stake," Rev. Financial Studies, vol. 34, no. 3, 2021.
[148] Bessani, A. et al., "State Machine Replication for the Masses with BFT-SMaRt," Proc. DSN, 2014.
[149] Yin, M. et al., "HotStuff: BFT Consensus with Linearity and Responsiveness," Proc. ACM PODC, 2019.
[150] Nielsen, M.A. & Chuang, I.L., Quantum Computation and Quantum Information, Cambridge University Press, 2011.
[151] Fedorov, A.K., Kiktenko, E.O. & Lvovsky, A.I., "Quantum computers put blockchain security at risk", Nature, 2018. DOI: 10.1038/d41586-018-07449-z.
[152] Shor, P.W., "Algorithms for quantum computation: discrete logarithms and factoring", Proc. 35th FOCS, 1994.

[153] Grover, L.K., “A fast quantum mechanical algorithm for database search”, Proc. 28th ACM STOC, 1996.
[154] Bennett, C.H. & Brassard, G., “Quantum Cryptography: Public Key Distribution and Coin Tossing”, Theoretical Computer Science, vol. 560, 2014.
[155] Gerhardt, I. et al., “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”, Nature Communications, 2011. DOI: 10.1038/ncomms1348.
[156] Amin, M., Khan, A., Shafiq, M., & Saeed, S., “Blockchain with Proof of Quantum Work,” arXiv preprint arXiv:2503.14462, 2025. URL: https://arxiv.org/abs/2503.14462
[157] Gottesman, D. & Chuang, I., “Quantum Digital Signatures”, arXiv:quant-ph/0105032, 2001.
[158] Kalinin, K.P. & Berloff, N.G., “Blockchain platform with proof-of-work based on analog Hamiltonian optimisers”, arXiv:1802.10091, 2018.
[159] Jogenfors, J., “Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics”, IEEE ICBC, 2019. DOI: 10.1109/BLOC.2019.8751473.
[160] Ikeda, K., “qBitcoin: A Peer-to-Peer Quantum Cash System”, Proc. 2018 Computing Conference, DOI: 10.1007/978-3-030-01174-1_58.
[161] Sun, X., Wang, Q., Kulicki, P. & Zhao, X., “Quantum-Enhanced Logic-Based Blockchain I: Quantum Honest-Success Byzantine Agreement and Qulogicoin”, arXiv:1805.06768, 2018. URL: https://arxiv.org/abs/1805.06768
[162] B. Chhetri, S. Gopali, R. Olapojoye, S. Dehbash, A. Siami Namin, “A Survey on Blockchain-Based Federated Learning and Data Privacy,” *arXiv preprint arXiv:2306.17338*, Jun. 2023.
[163] E. Moore, A. Imteaj, S. Rezapour, M. H. Amini, “A Survey on Secure and Private Federated Learning Using Blockchain: Theory and Application in Resource-constrained Computing,” *arXiv preprint arXiv:2303.13727*, Mar. 2023.
[164] When Federated Learning Meets Quantum Computing: “When Federated Learning Meets Quantum Computing,” *arXiv preprint arXiv:2504.08814*, Apr. 2025.
[165] S. Shan, X. Zhang, “Quantum Machine Learning—An Overview,” *Electronics*, vol. 12, no. 11, art. 2379, Nov. 2023. DOI:10.3390/electronics12112379.
[166] H.-Y. Huang, R. Kueng, J. Preskill, “Power of data in quantum machine learning,” *Nat. Commun.*, vol. 12, article 2631, Jun. 2021. DOI:10.1038/s41467-021-22539-9.
[167] X. Wang, et al., “Towards understanding the power of quantum kernels in machine learning,” *Quantum*, vol. 5, article 531, Aug. 2021. DOI:10.22331/q-2021-08-30-531.
[168] M. J. Umer, M. Imran Sharif, “A review of Quantum Neural Networks: Methods, Models, Dilemma,” arXiv preprint arXiv:2109.01840, 2021.
[169] T. Tomono, “The discriminative ability on anomaly detection using quantum machine learning,” *EPJ Quantum Technol.*, vol. 12, article 4, 2025. DOI:10.1140/epjqt/s40507-025-00335-4.
[170] Innan, N., Sawaika, A., Dhor, A., et al. (2024). Financial fraud detection using quantum graph neural networks. Quantum Machine Intelligence, 6(1), 7. https://doi.org/10.1007/s42484-024-00143-6
[171] M. Incudini, “Toward useful quantum kernels,” *Quantum Sci. Technol.*, vol. 9, no. 3, 034003, 2024. DOI:10.1088/2058-9565/ace32c.
[172] B. Khanal, P. Rivas, A. Sanjel, K. Sooksatra, E. Quevedo, A. Rodriguez, “Generalization error bound for quantum machine learning in NISQ era — a survey,” arXiv preprint arXiv:2409.07626, 2024.
[173] M. C. Caro, H.-Y. Huang, M. Cerezo, K. Sharma, A. Sornborger, L. Cincio, & P. J. Coles, “Generalization in quantum machine learning from few training data,” *Nature Communications*, vol. 13, article 3221, 2022. DOI: 10.1038/s41467-022-32550-3.
[174] E. Gil-Fuster & J. Eisert, “Understanding quantum machine learning also requires rethinking generalization,” *Nature Communications*, vol. 15, article 2833, 2024. DOI: 10.1038/s41467-024-45882-z.
[175] S. Corli, L. Moro, D. Dragoni & M. Dispenza, “Quantum Machine Learning Algorithms for Anomaly Detection: A Review,” *arXiv preprint arXiv:2408.11047*, Aug. 2024.
[176] R. Ubale, S. K. K., S. Deshpande & G. T. Byrd, “Toward Practical Quantum Machine Learning: A Novel Hybrid Quantum LSTM for Fraud Detection,” *arXiv preprint arXiv:2505.00137*, Apr. 2025.

[177] Innan, N., Al-Zafar Khan, M., Marchisio, A., Shafique, M., & Bennai, M. (2024). FedQNN: Federated Learning using Quantum Neural Networks. arXiv:2403.10861. https://arxiv.org/abs/2403.10861
[178] Innan, N., Sawaika, A., Dhor, A., et al. (2024). Financial fraud detection using quantum graph neural networks. Quantum Machine Intelligence, 6(1), 7. https://doi.org/10.1007/s42484-024-00143-6
[179] Jerbi, S., Garcia-Martín, D., Bravo-Prieto, C., & Cerezo, M. (2023). Quantum machine learning beyond kernel methods. Nature Communications, 14, 3903. https://doi.org/10.1038/s41467-023-36159-y
[180] European Central Bank & European Banking Authority: *ECB and EBA publish joint report on payment fraud* (Press release, 1 Aug 2024).
[181] Wedge R., Kanter J. M., Moral Rubio S. & Veeramachaneni K.: "Solving the «false positives» problem in fraud prediction". arXiv:1710.07709, 2017.
[182] M. Ahmed, "A semantic rule based digital fraud detection," *Applied Computational and Structural Engineering*, 2021.
[183] A. Ali, S. H. Othman, S. Abd Razak, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser & T. Elhassan, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Applied Sciences*, vol. 12, no. 19, art. 9637, 2022. DOI:10.3390/app12199637.
[184] Y. Chen, C. Zhao, Y. Xu & C. Nie, "Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review," *arXiv preprint arXiv:2502.00201*, 2025.
[185] "Comparative Review of Credit Card Fraud Detection using Machine Learning and Concept Drift Techniques," IJCSMC, vol. 12, no. 7, pp. 24-48, Jul. 2023.
[186] D. Cheng, Y. Zou, S. Xiang & C. Jiang, "Graph Neural Networks for Financial Fraud Detection: A Review," *arXiv preprint arXiv:2411.05815*, 2024.
[187] K. S. Kumar & M. Ravi, "Real-Time Financial Fraud Detection Using Adaptive Graph Neural Networks and Federated Learning," *International Journal of Management and Data Analytics (IJMADA)*, vol. 5, no. 1, pp. 98-110, 2025.
[188] J. Niu, "A survey on membership inference attacks and defenses in federated learning," *Computers & Security*, vol. XX, no. YY, 2024. DOI:10.1016/j.cose.2024.102900.
[189] Y. Alhasawi, "A federated approach to scalable and trustworthy financial fraud detection," *Software: Practice & Experience*, vol. ??, no. ??, 2025. DOI:10.1002/spe2.70099.
[190] S. K. Aljunaid, S. J. Almheiri, H. Dawood & M. A. Khan, "Explainable AI-driven Federated Learning Model for Financial Fraud Detection," *J. Risk Financial Manag.*, vol. 18, no. 4, art. 179, 2025. DOI:10.3390/jrfm18040179.
[191] H. Wang, "Advancements of credit card fraud detection based on federated learning and AI techniques," *International Journal of Advanced Computer Technology*, vol. XXX, 2025.
[192] L. Wu, "A Survey on Blockchain-Based Federated Learning," *Future Internet*, vol. 15, no. 12, p. 400, Dec. 2023.
[193] K. Liu, X. Liang, R. Kantola και C. Hu, "A survey on blockchain-enabled federated learning and its prospects with digital twin," *Digit. Commun. Netw.*, vol. 10, pp. 248–264, 2024.
[194] X. Qu, S. Wang, Q. Hu και X. Cheng, "Proof of Federated Learning: A Novel Energy-recycling Consensus Algorithm," arXiv preprint arXiv:1912.11745, Dec. 2019.
[195] J. M. Herrera Pinheiro, S. Vilas Boas de Oliveira, T. H. Segreto Silva, P. A. Rabelo Saraiva, E. F. de Souza, R. V. Godoy & L. A. Ambrosio, "The Impact of Feature Scaling in Machine Learning: Effects on Regression and Classification Tasks," *arXiv preprint arXiv:2506.08274v4*, Jun. 2025.
[196] X. H. Cao, Q. Jiang, "A robust data-scaling algorithm to improve classification performance," *PLoS One*, vol. 11, no. 6, e0158385, Jun. 2016. DOI:10.1371/journal.pone.0158385.
[197] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). *SMOTE: Synthetic Minority Over-sampling Technique.* Journal of Artificial Intelligence Research, 16, 321–357.
[198] Aborujilah, A. *et al.* (2021). SMOTE-Based Framework for IoT Botnet Attack Detection. In: Anbar, M., Abdullah, N., Manickam, S. (eds) Advances in Cyber Security. ACeS 2020. Communications in Computer and Information Science, vol 1347. Springer, Singapore. https://doi.org/10.1007/978-981-33-6835-4_19

[199] I. T. Jolliffe and J. Cadima, “Principal component analysis: a review and recent developments,” *Phil. Trans. R. Soc. A*, vol. 374, no. 2065, p. 20150202, Apr. 2016. doi: 10.1098/rsta.2015.0202.
[200] “Importance of Feature Scaling – Scikit-learn,” *scikit-learn.org*, 2024. Available: https://scikit-learn.org/stable/auto_examples/preprocessing/plot_scaling_importance.html.
[201] N. Innan, A. Marchisio, M. Bennai & M. Shafique, “QFNN-FFD: Quantum Federated Neural Network for Financial Fraud Detection,” *arXiv preprint arXiv:2404.02595*, 2024.
[202] K. Beer, E. Farrelly, et al., “Training deep quantum neural networks,” *Nature Communications*, vol. 11, art. 808, 2020. DOI: 10.1038/s41467-020-14454-2.
[203] S.-H. Sim, J. Smith, et al., “Structure optimization for parameterized quantum circuits,” *arXiv preprint arXiv:1905.09692*, May 2019.
[204] Y. Du, M.-H. Hsieh, T. Liu and D. Tao, “A Grover-search Based Quantum Learning Scheme for Classification,” New Journal of Physics, vol. 23, no. 2, p. 023020, Feb. 2021. DOI: 10.1088/1367-2630/abdefa.