Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Μετα-κβαντική Κρυπτογραφία σε Τεχνολογίες Blockchain

Νικόλαος Σακελλίων

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης - Καθηγητής (Μέλος ΣΕΠ)

Μάιος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Μετα-κβαντική Κρυπτογραφία σε Τεχνολογίες Blockchain

Νικόλαος Σακελλίων

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης - Καθηγητής (Μέλος ΣΕΠ)

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2020

Περίληψη

Η τεχνολογία blockchain αποτελεί μία από τις σημαντικότερες εξελίξεις των τελευταίων ετών, με συνεχώς αυξανόμενες εφαρμογές σε ποικίλους τομείς τείνει να αποτελέσει παγκόσμιο πρότυπο και να αντικαταστήσει τις συμβατικές μεθόδους δοσοληψίας, αφού προσφέρει διαφάνεια και ακεραιότητα στο σύνολό της. Παράλληλα, η κατασκευή ισχυρών κβαντικών υπολογιστών φαίνεται να είναι πιο κοντά από ποτέ και αναμένεται με προσμονή, αφού θα μπορέσουν να επιλύσουν πολλά προβλήματα σε διάφορους τομείς των θετικών επιστημών. Ταυτόχρονα όμως, θα έχουν την δυνατότητα να «επιτεθούν» στους μηχανισμούς ασφαλείας στους οποίους βασίζεται η blockchain τεχνολογία και το διαδίκτυο γενικότερα. Στόχος της παρούσας μεταπτυχιακής διατριβής, λοιπόν, είναι να μελετηθούν σε βάθος και να αξιολογηθούν, τα τρέχοντα κβαντο-ανθεκτικά μοντέλα κρυπτογραφίας που θα μπορούσαν να καταστήσουν την τεχνολογία blockchain ασφαλή στην μετα-κβαντική εποχή.

Συγκεκριμένα, στο πλαίσιο της παρούσας διατριβής πραγματοποιήθηκε ενδελεχής μελέτη όλων των κρυπτογραφικών μηχανισμών μετα-κβαντικής κρυπτογραφίας, υπό το πρίσμα της χρήσης τους σε τεχνολογίες blockchain. Παράλληλα, μελετήθηκαν και τα διάφορα είδη τεχνολογιών blockchain, προκειμένου να αποσαφηνιστεί ο βαθμός στον οποίο η ασφάλειά τους πλήττεται με την έλευση των κβαντικών υπολογιστών. Περαιτέρω, χρησιμοποιήθηκε και η μέθοδος της πειραματικής έρευνας πάνω σε μια πρωτοπόρα τεχνολογία κβαντο-ανθεκτικής blockchain, τη λεγόμενη QRL (Quantum Resistant Ledger), η πρώτη τεχνολογία σε αυτόν τον τομέα, με σκοπό την εξαγωγή συμπερασμάτων που αφορούν την απόδοση της τεχνολογίας – σε απλό σημερινό οικιακό υπολογιστικό σύστημα – σε σύγκριση με το θεωρητικό μοντέλο.

Τα αποτελέσματα που εξήχθησαν από την θεωρητική έρευνα αποκαλύπτουν δυνατά και αδύναμα σημεία κάθε κβαντο-ανθεκτικής τεχνολογίας στους διάφορους τομείς της κρυπτογραφίας. Για αυτό άλλωστε, ίσως δούμε στο μέλλον να υπερισχύουν υβριδικά μοντέλα που θα συνδυάζουν δύο ή περισσότερες από αυτές τις τεχνολογίες. Επιπλέον, υπάρχουν παράγοντες που πρέπει να ληφθούν σοβαρά υπόψιν στην αξιολόγηση των τεχνολογιών αυτών και αφορούν την αφομοίωσή τους από την βιομηχανία και την κοινωνία γενικότερα. Τα αποτελέσματα της πειραματικής έρευνας, από την άλλη, ήταν ενθαρρυντικά και οι μετρήσεις που έγιναν στα διάφορα σενάρια χρήσης έδωσαν τιμές πλησίον των αναμενόμενων βάσει θεωρίας.

Summary

Blockchain technology constitutes one of the most significant technological developments in recent years. It has been envisioned to become the new global standard, replacing conventional contracting methods. That is possible because blockchain has been built so as to inherently achieve, transactional integrity and transparency. In parallel, scientists are seemingly closer than ever to construct powerful quantum computers that will be able to solve many modern problems in the fields of medicine, chemistry, etc. using their superior computing power. The same power though can be used to compromise the security of cryptographic techniques on which blockchain is based, rendering them obsolete. That makes it imperative to develop quantum-resistant technologies, more than ever.

Therefore, this Master thesis aims to provide an in-depth study and evaluation of the current quantum-resistant cryptographic models that could make blockchain technology secure in the post-quantum age.

In the context of this thesis, a thorough study of all cryptographic post-quantum cryptographic mechanisms is carried out, in the light of their use in blockchain technologies. At the same time, the various types of blockchain technologies were studied, to clarify the degree to which their security is affected by the advent of quantum computers. Furthermore, an experimental analysis has been carried out, based on a pioneering quantum-resistant blockchain technology, the so-called QRL (Quantum Resistant Ledger), the first technology in this field, in order to assess the performance of technology - using a simple current home computer system with respect to the theoretical model.

The results obtained from the theoretical research reveal strong and weak points of each quantum-resistant technology in the various fields of cryptography. That is why we may see hybrid models dominating in the future that combine two or more of these technologies. Besides, some factors need to be considered when evaluating these technologies and their assimilation by industry and society at large. The results of the experimental research, on the other hand, were encouraging and the measurements made in the various scenarios of use illustrate that post-quantum cryptographic primitives in blockchain scenarios are indeed feasible, even in conventional computing systems.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω από καρδιάς τον καθηγητή μου στην θεματική ενότητα της Κρυπτογραφίας και επιβλέποντα της παρούσας μεταπτυχιακής διατριβής, κ. Κωνσταντίνο Λιμνιώτη για την εμπιστοσύνη που έδειξε στο πρόσωπό μου, την διαρκή υποστήριξη και ανάδραση σε όλες τις φάσεις τις εργασίας μου και κυρίως για τον ενθουσιασμό που μου μετέφερε, δίνοντάς μου όλο και περισσότερη ενέργεια και κουράγιο ώστε να την φέρω σε πέρας.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

«*Μέχρι το 2025, το 10% του παγκόσμιου GDP αναμένεται να βρίσκεται αποθηκευμένο σε blockchains ή τεχνολογικές λύσεις που βασίζονται σε blockchains*», σύμφωνα με αναφορά που εκδόθηκε από το Παγκόσμιο Οικονομικό Φόρουμ τον Σεπτέμβρη του 2017 (World Economic Forum 2017:8).

Η τεχνολογία blockchain έγινε ιδιαιτέρως γνωστή τα τελευταία χρόνια, ιδίως μέσα από την εφαρμογή της για την λειτουργία του δημοφιλέστερου – έως σήμερα – κρυπτονομίσματος στον κόσμο, του Bitcoin. Η μεγάλη δημοσιότητα του Bitcoin κέντρισε το ενδιαφέρον πολλών ερευνητών και καινοτόμων πάνω στην τεχνολογία αυτή. Έκτοτε, υπάρχει έντονη κινητικότητα και προσπάθεια, ώστε να εφαρμοστεί και σε άλλους τομείς της καθημερινότητας πέρα των κρυπτονομισμάτων, όπως η υγεία, το εμπόριο και γενικότερα σε όποιον τομέα υπάρχει δοσοληψία υλικών ή αύλων αγαθών μεταξύ δύο η περισσοτέρων μερών.

Δομικός λίθος της ασφάλειας της blockchain τεχνολογίας και της ακεραιότητας των συναλλαγών των χρηστών της, είναι ένα σύνολο ειδικών αλγορίθμων που βασίζονται σε γνωστά μαθηματικά προβλήματα. Τα προβλήματα αυτά απαιτούν πολλά χρόνια συνεχών υπολογισμών ακόμα και από τους ισχυρότερους υπολογιστές προκειμένου να λυθούν και για αυτό θεωρούνται άλυτα σε πραγματικό χρόνο. Ρήγμα σε αυτό τον λίθο όμως, φαίνεται να δημιουργεί η επικείμενη έλευση των κβαντικών υπολογιστών. Εταιρείες κολοσσοί όπως η IBM, Google, Intel, κ.α. αλλά και κράτη ολόκληρα όπως η Κίνα, δαπανούν εκατομμύρια δολάρια στην έρευνα και ανάπτυξη προκειμένου να κατασκευάσουν έναν πλήρως λειτουργικό κβαντικό υπολογιστή. Οι μέχρι τώρα επίσημες προσπάθειες έχουν βρει ισχυρά εμπόδια κι έτσι οι κβαντικοί υπολογιστές που έχουν κατασκευαστεί μέχρι σήμερα έχουν περιορισμένες δυνατότητες και λειτουργούν ως

πρωτότυπα για την περαιτέρω ανάπτυξή τους. Είναι αδύνατον να γνωρίζουμε πότε τα εμπόδια αυτά θα ξεπεραστούν, καθώς μια πολύ μικρή εξέλιξη μπορεί να αποδειχθεί επαναστατική και να επιταχύνει την διαδικασία. Το σίγουρο είναι, πως τα νέα αυτά υπολογιστικά συστήματα λόγω των ιδιοτήτων τους θα μπορούν να επιλύσουν προβλήματα όπως τα παραπάνω σε πραγματικό – και άρα αποδεκτό – χρόνο κάτι που μάλιστα, αποδείχτηκε στο μακρινό 1994 από τον μαθηματικό Peter Shor με τον ομώνυμο αλγόριθμό του.

Συνυπολογίζοντας τα παραπάνω, γίνεται αντιληπτό πως η επιστημονική κοινότητα έχει στα χέρια της μια ωρολογιακή βόμβα που όταν σκάσει, θα καταστήσει την ασφάλεια των blockchains αλλά και γενικότερα την κρυπτογραφία δημοσίου κλειδιού που χρησιμοποιείται σήμερα στο διαδίκτυο, επισφαλής. Για τον λόγο αυτό, τα τελευταία χρόνια γίνονται εντατικές προσπάθειες ώστε να σχεδιαστούν, να ελεγχθούν και να βελτιωθούν κβαντο-ανθεκτικά σχήματα κρυπτοσυστημάτων ώστε να αντικαταστήσουν, προληπτικά, τα υπάρχοντα πριν τον ερχομό ισχυρών κβαντικών υπολογιστών. Μάλιστα, το Εθνικό Ίδρυμα Τεχνολογίας και Προτύπων (National Institute of Standards and Technology, NIST) των Η.Π.Α., ξεκίνησε το 2016 διαδικασία αξιολόγησης κι επιλογής υποψηφίων σχημάτων με απώτερο στόχο την δημιουργία ενός κβαντο-ανθεκτικού προτύπου το αργότερο μέχρι το 2024.

1.1 Σκοπός – Ερευνητικά Ερωτήματα

Σκοπός λοιπόν της παρούσας μεταπτυχιακής διατριβής είναι η μελέτη των υπαρχουσών και προτεινόμενων κρυπτογραφικών τεχνολογιών με εφαρμογή στις blockchains που θα παρέχουν ασφάλεια και στη μετα-κβαντική εποχή. Εύλογα από την μελέτη αυτή ανακύπτουν και τα εξής ερευνητικά ερωτήματα τα οποία και θα επιχειρήσουμε να απαντήσουμε:

1. Υπάρχουν σήμερα ολοκληρωμένες κβαντο-ανθεκτικές τεχνολογίες που να μπορούν να παρέχουν ασφάλεια στη μετα-κβαντική εποχή;
2. Πόσο αποδοτικά είναι υπάρχοντα κβαντο-ανθεκτικά συστήματα σε χρήση τους σε συμβατικά σημερινά υπολογιστικά συστήματα;
3. Μπορεί να δημιουργηθεί αλγόριθμος (ή συνδυασμός αλγορίθμων) που να καθιστά ένα blockchain που τον υλοποιεί, απόλυτα ασφαλές σε επιθέσεις από κβαντικούς υπολογιστές;
4. Η κβαντο-ανθεκτικότητα θα έρθει σε κόστος κάποιας άλλης ιδιότητας των

blockchains (πχ ιδιωτικότητα);

5. Τελικά, θα προλάβει η κβαντο-ανθεκτική τεχνολογία να ασφαλίσει σε ικανοποιητικό βαθμό τα blockchains που την υιοθετούν ή οι κβαντικοί υπολογιστές θα έρθουν πρώτα, κλονίζοντας τα θεμέλια των blockchains και των τεχνολογιών κρυπτογραφίας που αυτές χρησιμοποιούν;

1.2 Μεθοδολογία

Ένα σημαντικό τμήμα της διατριβής βασίστηκε, εκ της φύσης του αντικειμένου, σε θεωρητική έρευνα. Έγινε συλλογή, επεξεργασία και επιλογή της κατάλληλης βιβλιογραφίας για την ανάλυση της τεχνολογίας της blockchain, των κβαντικών υπολογιστών και κυρίως των κρυπτογραφικών σχημάτων που παρουσιάζουν ανθεκτικότητα στους κβαντικούς υπολογιστές. Έγινε λεπτομερής βιβλιογραφική επισκόπηση, εις βάθος μελέτη των κβαντο-ανθεκτικών σχημάτων και παρουσίαση των πιο σημαντικών υλοποιήσεών τους. Στη συνέχεια παρουσιάστηκαν, αναλύθηκαν και συγκρίθηκαν τα δεδομένα της έρευνας, εξάγοντας και τα σχετικά συμπεράσματα.

Έπειτα, η θεωρητική έρευνα συνεχίστηκε εξετάζοντας την QRL (Quantum Resistant Ledger), την πιο χαρακτηριστική μετα-κβαντική blockchain που υπάρχει σήμερα. Μελετήθηκαν αναλυτικά τα κρυπτογραφικά χαρακτηριστικά μετα-κβαντικής κρυπτογραφίας που υλοποιεί, η αποτελεσματικότητά τους βάσει των σχετικών αναφορών της βιβλιογραφίας, καθώς και ζητήματα που πρόκειται να αντιμετωπιστούν στο (εγγύς) μέλλον.

Περεταίρω, πραγματοποιήθηκε πειραματική έρευνα η οποία έλαβε χώρα στην blockchain του QRL, υλοποιώντας συναλλαγές, (δημιουργία «ψηφιακού πορτοφολιού» κτλ.), προκειμένου να διαπιστωθεί, σε ένα ρεαλιστικό περιβάλλον σημερινού συμβατικού υπολογιστή, η απόδοσής της και η εν γένει ευχέρεια λειτουργίας της (μέτρηση χρόνων για τη δημιουργία ψηφιακών υπογραφών μετα-κβαντικής κρυπτογραφίας, μέτρηση άλλων μεγεθών όπως μεγέθη block, χρόνος δημιουργίας τους, μεγέθη υπογραφών κτλ). Η πειραματική έρευνα έγινε με χρήση οικιακού συμβατικού υπολογιστικού συστήματος ώστε να αξιολογηθούν οι αποδόσεις και οι επιδόσεις της συγκεκριμένης blockchain για τον τελικό χρήστη, πάντα σε σύγκριση με το θεωρητικό μοντέλο και τι περιμέναμε βάσει αυτού.

Εν κατακλείδι, το εν λόγω θέμα έχει πολύ έντονο τρέχον ερευνητικό ενδιαφέρον. Οι εξελίξεις στον τομέα των blockchains, των κβαντικών υπολογιστών αλλά κυρίως σε ότι αφορά τα κβαντο-ανθεκτικά σχήματα είναι συνεχής και καταιγιστικές. Η βιβλιογραφία φαίνεται σε πολλές περιπτώσεις να μην μπορεί να συμβαδίσει χρονικά με αυτές και αν επιθυμούμε να ενημερωθούμε για το σήμερα και το τώρα, θα πρέπει να ανατρέξουμε και σε πηγές από παρουσιάσεις βίντεο και σε ειδικούς ιστοτόπους παράθεσης κώδικα προγραμματισμού. Για τον λόγο αυτό, η βιβλιογραφία που χρησιμοποιήθηκε για την παρούσα μεταπτυχιακή διατριβή, περιέχει επιπροσθέτως και τέτοιου είδους πηγές από καταξιωμένους επιστήμονες και επαγγελματίες του χώρου.

1.3 Δομή της Διατριβής

Στο δεύτερο κεφάλαιο, γίνεται παρουσίαση της τεχνολογίας blockchain αναλύοντας την δομή της, τον τρόπο λειτουργίας και τα ιδιαίτερα χαρακτηριστικά που την κάνουν ξεχωριστή. Τέλος, εξετάζουμε μερικές από τις πολλές μελλοντικές της εφαρμογές, οπότε αναδεικνύεται η σπουδαιότητά της και ο σημαντικός ρόλος που θα έχει στο άμεσο μέλλον ώστε να γίνει κατανοητή η ανάγκη να διατηρηθεί ασφαλής στην μετα-κβαντική εποχή. Στο τρίτο κεφάλαιο, παρουσιάζεται μια σύντομη περιγραφή ενός κβαντικού υπολογιστή. Ιδιαίτερη έμφαση δίνεται στις ιδιότητες του αυτές που μπορούν δυνητικά στο μέλλον να αποτελέσουν πρόβλημα στην ασφάλεια των blockchain αλλά και της κρυπτογραφίας γενικότερα. Έτσι, στο τέταρτο κεφάλαιο γίνεται μια ενδελεχής μελέτη και ανάλυση των κρυπτογραφικών συστημάτων που φέρουν κβαντο-ανθεκτικές ιδιότητες και θα μπορούσαν να αποτελέσουν τον ακρογωνιαίο λίθο της κρυπτογραφίας στην μετα-κβαντική εποχή. Επίσης, παρουσιάζονται οι πιο σημαντικοί αλγόριθμοι που βασίζονται στα κρυπτοσυστήματα αυτά. Στο πέμπτο κεφάλαιο, γίνεται σύγκριση των παραπάνω μοντέλων κρυπτογραφικών συστημάτων. Παρουσιάζονται τα δυνατά και αδύνατά τους σημεία καθώς και εξάγεται συμπέρασμα σχετικό με ποια από αυτά είναι πιθανότερο να καλύψουν συγκεκριμένους τομείς της μετα-κβαντικής κρυπτογραφίας, σύμφωνα με τα δεδομένα που έχει η επιστημονική κοινότητα σήμερα. Στο έκτο κεφάλαιο, εξετάζεται μια συγκεκριμένη υλοποίηση κβαντο-ανθεκτικού μοντέλου με εφαρμογή σε blockchain κρυπτονομίσματος. Αναλύεται η δομή και λειτουργία της που αφορά την κβαντο-ανθεκτικότητα και στη συνέχεια γίνεται πειραματική έρευνα και αξιολόγηση των λειτουργιών της, σε δοκιμαστικό περιβάλλον και με χρήση οικιακού υπολογιστή, εξάγοντας και τα απαραίτητα συμπεράσματα.

Κεφάλαιο 2

Αλυσίδα Κοινοποιήσεων

Πριν ερευνήσουμε τις μετα-κβαντικές κρυπτογραφικές τεχνολογίες εφαρμοσμένες σε αλυσίδες κοινοποιήσεων, είναι απαραίτητο να αποδομήσουμε το ερευνητικό μας θέμα στα πρωτογενή συστατικά του. Έτσι, είναι σημαντικό να καταλάβουμε τι είναι αυτή η αλυσίδα κοινοποιήσεων στην οποία αναφέρονται διαρκώς όλοι και περισσότεροι ειδικοί της τεχνολογίας, αλλά και της οικονομίας και πολιτικής, τι την κάνει να ξεχωρίζει από άλλα παρόμοια μοντέλα και ποιες είναι οι δυνατότητες που προσφέρει στον πολίτη του σήμερα και του αύριο. Έτσι, θα μπορέσει να γίνει αντιληπτή η ανάγκη της εξέλιξής με σκοπό την διαφύλαξή της στην εποχή που θα συνυπάρχουμε με τους κβαντικούς υπολογιστές.

2.1 Τι είναι η Αλυσίδα Κοινοποιήσεων (blockchain)

Αναφερόμενοι στον όρο blockchain πρέπει να καταστεί σαφές πως πρόκειται για μια τεχνολογία και όχι μια μοναδική ψηφιακή οντότητα (digital entity). Η τεχνολογία αυτή στην εφαρμογή της, απεικονίζεται σε μια δομή που, όπως προκύπτει και από την ετυμολογία της ίδιας της λέξης, αποτελείται από μια αλυσίδα (chain) από πακέτα δεδομένων (blocks) [σ.σ. Στην πορεία, ο όρος blockchain έφτασε να αναφέρεται σε τέτοιες αλυσίδες ως υλοποιήσεις της τεχνολογίας και με αυτό τον τρόπο θα χρησιμοποιηθεί και στην παρούσα διατριβή].

Κάθε blockchain περιγράφεται ως ένας αποκεντρωμένος κατανεμημένος κατάλογος (decentralized distributed ledger). Αυτό σημαίνει πως δεν επιβλέπεται ούτε διαχειρίζεται

από κάποια κεντρική Αρχή (central authority), αλλά είναι στο σύνολό της κατανεμημένη σε όλους τους χρήστες της συγκεκριμένης. Επιπλέον, έχει την ιδιότητα να μην επιδέχεται αλλαγές σε υπάρχοντα block της, αλλά μόνο προσθήκες στο τέλος της (append only), ακόμα και αν αυτές οι προσθήκες αφορούν διορθωτικές πληροφορίες/κινήσεις από παλαιότερα blocks (Zheng et al 2017:557).

Η ιδέα πίσω από την τεχνολογία αυτή είχε περιγραφεί από τα πρώτα χρόνια της δεκαετίας του 1990, αλλά δεν είχε χρησιμοποιηθεί ευρέως μέχρι που το 2009 ένα άτομο (ή ομάδα ατόμων) με το ψευδώνυμο Satoshi Nakamoto, περιέγραψε το πρώτο και δημοφιλέστερο μέχρι σήμερα ψηφιακό κρυπτονόμισμα (cryptocurrency) Bitcoin βασισμένο στην τεχνολογία blockchain.

2.2 Δομή

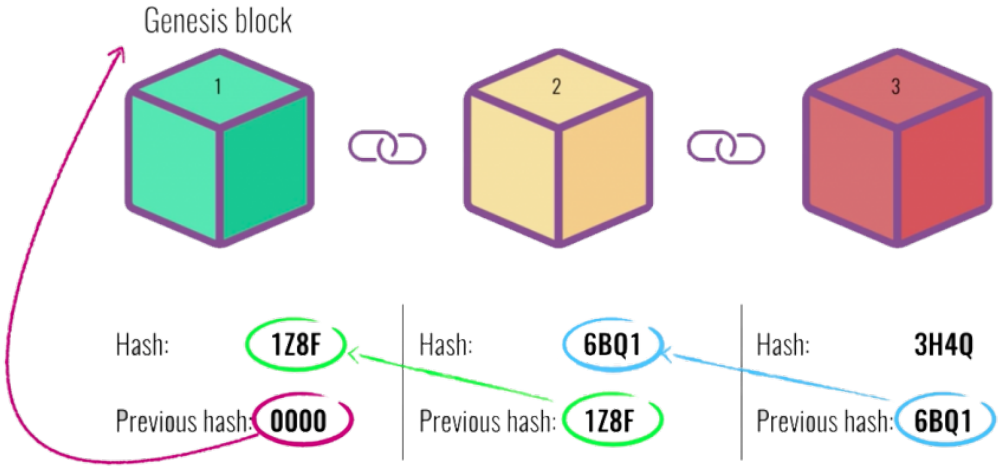
Κάθε block που ανήκει σε μία τέτοια blockchain αποτελείται από τρία βασικά στοιχεία:
(α) Τα δεδομένα (data) *d* που είναι αποθηκευμένα σε αυτό. Ο τύπος των δεδομένων που περιέχονται σε ένα block εξαρτάται από την υλοποίηση (τον τύπο δηλαδή) της blockchain. Στην περίπτωση του Bitcoin, τα δεδομένα περιγράφουν τις λεπτομέρειες μια συναλλαγής κρυπτονομίσματος (αποστολέας, παραλήπτης, αξία συναλλαγής). Σημαντικό είναι να τονίσουμε, πως κάθε μπλοκ δεν περιέχει μία και μόνο συναλλαγή (transaction), αλλά πολύ περισσότερες (συγκεκριμένα για το Bitcoin blockchain σε κάθε block περιέχονται περίπου δύο χιλιάδες συναλλαγές).
(β) Την τιμή συνάρτησης κατακερματισμού (hash value) h_{prev} του προηγούμενου block (previous ή parent hash). Στην περίπτωση που πρόκειται για το πρώτο block της αλυσίδας, η τιμή αυτή είναι μηδέν (0) και το block καλείται γεννήτορας (genesis block) (Zheng et al 2017:559). Το στοιχείο αυτό μάλιστα, είναι που δημιουργεί και την δομή της αλυσίδας, την αρχικοποιεί.
(γ) Την hash value *h* του block. Η τιμή αυτή προκύπτει από την εφαρμογή συγκεκριμένης συνάρτησης κατακερματισμού (hash function, πχ SHA-256 για το Bitcoin) πάνω σε όλα τα περιεχόμενα του block (data και previous hash). Κάθε hash function, βάσει ορισμού έχει τις εξής ιδιότητες (Mathhew Green 2018:1):

1. δεν είναι αναστρέψιμη, δηλαδή δε μπορεί να βρεθεί η αρχική πληροφορία από την hash value της (pre-image resistance),
2. δεν μπορεί να βρεθεί διαφορετική πληροφορία d_1 που να δίνει το ίδιο αποτέλεσμα hash value με την αρχική (second pre-image resistance) και

3. δεν μπορούν να βρεθούν δύο διαφορετικές πληροφορίες *d1*, *d2* που να έχουν την ίδια hash value h(*d1*) = h(*d2*) (collision resistance),

που σημαίνει πως η τιμή *h* θεωρείται, πρακτικά, μοναδική αφού οποιαδήποτε μεταβολή στα αρχικά δεδομένα, θα αλλάξει και την *h*.

Η hash value, επομένως, λειτουργεί ως η ταυτότητα του block αφού το διαχωρίζει από και το καθιστά μοναδικό σε σχέση με τα άλλα blocks.



Εικόνα 1. Παράδειγμα δομής blockchain

2.3 Ασφάλεια – τι την κάνει ιδιαίτερη

Η παραπάνω δομή, θυμίζει σε μεγάλο βαθμό την συνδεδεμένη λίστα (linked list). Αυτό που ξεχωρίζει και κάνει μοναδική την blockchain, είναι οι ιδιότητες ασφάλειας (security properties) που ενσωματώνει στον τρόπο λειτουργίας της.

2.3.1 Αποτυπώματα (Hashes)

Όπως αναφέραμε και παραπάνω, εάν αλλάξει το περιεχόμενο των δεδομένων σε ένα blockchain block B_N, τότε θα αλλάξει και η hash value του. Αυτό θα καταστήσει το συγκεκριμένο block, αλλά και όλα τα επόμενα από αυτό blocks μη-έγκυρα, μιας και στο σημείο που άλλαξε η hash value θα χαθεί η αναφορά h_{prev} από το block B_{N+1}, ουσιαστικά "σπάζοντας" την αλυσίδα. Με τον τρόπο αυτό, γίνεται αντιληπτή οποιαδήποτε μεταβολή σε block της αλυσίδας (πλην του τελευταίου), αφού για να το πράξει κάποιος κακόβουλα και να περάσει απαρατήρητος, θα πρέπει να επαναϋπολογίσει και να αλλάξει όλες τις hash values και τα previous hashes για όλα τα επόμενα blocks B_{N+K} της αλυσίδας.

2.3.2 Συναίνεση (Consensus)

Παρότι η χρήση των hashes προσφέρει ένα πρώτο επίπεδο ασφάλειας στην ακεραιότητα μιας blockchain, πρέπει να τονίσουμε πως υπάρχει ήδη αρκετή υπολογιστική ισχύς ώστε κάποιος να μπορεί να επαναϋπολογίσει χιλιάδες hash values μέσα σε λίγα δευτερόλεπτα και να ενημερώσει τα αντίστοιχα blocks ώστε να είναι έγκυρη και πάλι η blockchain. Για την αναχαίτιση αυτής της απειλής, στην καρδιά της blockchain τεχνολογίας υπάρχει ένας μηχανισμός που καλείται μηχανισμός συναίνεσης (consensus mechanism).

Ο μηχανισμός αυτός έχει τεράστια σημασία για την ορθή λειτουργία των blockchain και αποτελεί θέμα έρευνας ετών ακόμα και σε τομείς πέραν την τεχνολογίας, όπως ο οικονομικός και ο πολιτικός. Πρόκειται για το πρόβλημα εύρεσης ενός ασφαλούς τρόπου να έρθουν σε συμφωνία διαφορετικοί κόμβοι σε ένα αποκεντρωμένο σύστημα, με τρόπο τέτοιο που θα προφυλάσσει και ταυτόχρονα αποκλείει περιπτώσεις που μέρος των κόμβων του συστήματος δρα κακόβουλα με σκοπό την διασπορά ψευδής πληροφορίας. Στον τομέα της πληροφορικής, το πρόβλημα αυτό αποτυπώθηκε ως το πρόβλημα των Βυζαντινών στρατηγών (The Byzantine Generals problem) (Lamport et al 1982:1). Είναι σημαντικό να τονίσουμε, πως τέτοιο πρόβλημα δεν υφίσταται στα συγκεντρωτικά (centralized) συστήματα. Εκεί η κεντρική Αρχή (central authority) έχει εξ ορισμού την τυφλή εμπιστοσύνη όλων των μελών-κόμβων του συστήματος της, οπότε υπάρχει αυτομάτως συναίνεση σε ότι αυτή ορίσει. Τέτοιο σύστημα όμως, πάσχει από την έννοια του μοναδικού-σημείου-αστοχίας (single point of failure), σε περίπτωση που η κεντρική Αρχή είναι κακόβουλη και θέλει να βλάψει τα μέλη της ή δεχτεί επίθεση και εκτεθεί σε κίνδυνο. Αντίθετα, σε αποκεντρωμένα συστήματα όπως η blockchain πρέπει να υπάρχει συναίνεση της πλειοψηφίας, δηλαδή η πλειοψηφία των κόμβων που συμμετέχουν σε αυτή να έρθουν σε συμφωνία για το ποιο είναι το περιεχόμενο του κοινού αυτού καταλόγου καθώς και για το ποιες συναλλαγές θα προστεθούν σε αυτό και με ποια σειρά.

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί να επιτευχθεί μια τέτοια συναίνεση και κάθε blockchain υλοποιεί έναν ή περισσότερους τύπους μηχανισμών συναίνεσης στην δομή της.

- Απόδειξη Εργασίας (Proof of Work - PoW):
  Πρόκειται για τον πιο γνωστό μηχανισμό συναίνεσης αφού τον χρησιμοποιούν δύο από τις πιο δημοφιλείς blockchains κρυπτονομισμάτων, Bitcoin και Ethereum. Στο proof of work, οι κόμβοι που το επιθυμούν ανταγωνίζονται μεταξύ τους για

το ποιος θα λύσει πρώτος ένα δύσκολο και απρόβλεπτο υπολογιστικό πρόβλημα και να παρουσιάσουν στους υπόλοιπους την απόδειξη για την επιτυχή τους αυτή εργασία. Το πρωτόκολλο της κάθε blockchain, λαμβάνοντας υπόψιν την συνολική επεξεργαστική ισχύ των συμμετεχόντων κόμβων (nodes) σε ότι αφορά το πλήθος των συναρτήσεων hash που μπορούν να εκτελέσουν σε κάθε δευτερόλεπτο (hash rate) αλλά και τον ρυθμό με τον οποίο έχει ορισθεί πως πρέπει να προστίθεται ένα block στην αλυσίδα, μεταβάλλει δυναμικά τον βαθμό δυσκολίας του προβλήματος αυτού. Συγκεκριμένα, παρουσιάζει στους συμμετέχοντες κόμβους μια τυχαία τιμή hash (hash value) σταθερού μήκους, ως αναφορά, η αξία της οποίας όμως είναι αντιστρόφως ανάλογη με τον βαθμό δυσκολίας που θέτει το πρωτόκολλο τη δεδομένη στιγμή. Έτσι, όσο πιο δύσκολο επιθυμεί να είναι το πρόβλημα, τόσο μικρότερη η τιμή της hash (δηλαδή με περισσότερα μηδενικά στις υψηλές θέσεις των bits) που δίνει στο δίκτυο. Οι συμμετέχοντες κόμβοι καλούνται να εκτελέσουν την συνάρτηση hash στο δικό τους υποψήφιο block και να βρουν τιμή μικρότερη ή ίση με αυτήν που έδωσε ως στόχο το πρωτόκολλο. Επειδή όμως τα στοιχεία του block που διαθέτει κάθε κόμβος τη δεδομένη στιγμή είναι σταθερά – και άρα θα δίνουν πάντα την ίδια τιμή hash ως αποτέλεσμα – υπεισέρχεται στην όλη διαδικασία μια μεταβλητή που καλείται *nonce* (που προκύπτει από την έκφραση «αριθμός που χρησιμοποιείται μόνο μια φορά», Number only used ONCE). Η μεταβλητή *nonce* είναι ένας αριθμός μήκους 32bit τον οποίο επιλέγει τυχαία ο κόμβος ώστε όταν προστεθεί στο block του να δίνει το επιθυμητό αποτέλεσμα hash. Έτσι, το πρόβλημα για το PoW, ανάγεται στην εύρεση του κατάλληλου κάθε φορά *nonce*. Κάθε κόμβος χρησιμοποιεί την υπολογιστική ισχύ του συστήματός του για να δοκιμάσει όσο περισσότερες τιμές *nonce* μέχρι τελικά να λύσει πρώτος το πρόβλημα. Η δυσκολία του προβλήματος είναι τέτοια, που για την επίλυσή του, απαιτείται πολύς χρόνος (στην περίπτωση του Bitcoin ορίζεται κατά μέσο όρο δέκα λεπτά, ενώ το Ethereum επιθυμώντας να μειώσει δραστικά τον χρόνο αυτό, εισήγαγε μηχανισμό τυχαίας επιλογής κόμβων από ένα προϋπολογισμένο μη κυκλικό γράφημα). Παράλληλα, δαπανούνται και τεράστια ποσά ενέργειας για την τροφοδοσία των υπολογιστικών συστημάτων που εργάζονται για την λύση αυτή. Αν μάλιστα συνυπολογίσουμε πως από όλα τα συστήματα αυτά, μόνο ένα ξόδεψε την ενέργεια του με επιτυχία και όλα τα υπόλοιπα εργάζονταν ουσιαστικά χωρίς κανένα αντίκτυπο, τότε σίγουρα πρόκειται έναν πολύ ενεργοβόρο μηχανισμό (Wenbing Zhao et al 2019:1). Για τον λόγο αυτό, αναπτύχθηκαν

διαφορετικοί μηχανισμοί συναίνεσης που απαιτούν λιγότερο χρόνο και ενέργεια για να λειτουργήσουν.

- Απόδειξη Συμμετοχής (Proof of Stake - PoS):

  Στην περίπτωση του proof of stake, ο κόμβος που θα προσθέσει το επόμενο block με συναλλαγές επιλέγεται μεταξύ όλων των υποψηφίων κόμβων με κλήρωση μέσω ενός συστήματος λοταρίας. Κάθε κόμβος που επιθυμεί να αυξήσει τις πιθανότητες του να κληρωθεί, ποντάρει ένα ποσό σε κρυπτονόμισμα. Όσο μεγαλύτερο το ποσό συμμετοχής, τόσο μεγαλύτερες και οι πιθανότητές του να κληρωθεί. Συγκριτικά με το PoW, το proof of stake έχει ελάχιστη απαίτηση σε ενέργεια από τους κόμβους, καθώς το μόνο που χρειάζεται να κάνουν είναι να αποδείξουν πως έχουν στην κατοχή τους το ποσό που πόνταραν. Στην περίπτωση που ο κόμβος που κληρωθεί είναι κακόβουλος και στη συνέχεια το block που κατασκευάσει απορριφθεί από τον μηχανισμό συναίνεσης, τότε χάνει το ποσό που πόνταρε. Επειδή το σύστημα αυτό ευνοεί τα πλούσια μέλη της blockchain κάνοντάς τα ακόμη πλουσιότερα, έχουν προταθεί παραλλαγές του όπου συνυπολογίζονται εκτός από το μέγεθος του ποσού των κρυπτονομισμάτων και η ηλικία τους. Στο σενάριο αυτό, ο κόμβος που απέκτησε παλαιότερα από τους υπόλοιπους υποψήφιους τα κρυπτονομίσματα που ποντάρει, σε συνάρτηση με την αξία τους, έχει και τις περισσότερες πιθανότητες να κληρωθεί (Zheng et al 2017:560). Παράδειγμα blockchain που χρησιμοποιεί το proof of stake είναι η Cardano’s ouroboros.
- Πρακτική Αντοχή Σφάλματος στο πρόβλημα των Βυζαντινών Στρατηγών (Practical byzantine fault tolerance – PBFT) (Zheng et al 2017:560):

  Αυτός ο μηχανισμός συναίνεσης, προσφέρει ασφάλεια ακόμα και στην περίπτωση που το 1/3 των συμμετεχόντων κόμβων είναι κακόβουλοι. Για να το καταφέρει αυτό, χωρίζει την διαδικασία προσθήκης νέου block, σε τρεις φάσεις: την προ-παρασκευαστική (pre-prepared), την φάση παρασκευής (prepared) και την φάση εκτέλεσης (commit). Κάθε υποψήφιος κόμβος, προκειμένου να περάσει για κάθε μία φάση στην επόμενη, πρέπει να ζητήσει και να λάβει ψήφο εμπιστοσύνης από τα 2/3 των υπόλοιπων κόμβων ώστε να φτάσει στην τελευταία και να μπορέσει να κάνει αυτός την προσθήκη. Η Zilliqa είναι μια blockchain που χρησιμοποιεί αυτόν τον μηχανισμό συναίνεσης.
- Απόδειξη Εξουσίας (Proof of Authority - PoA) (De Angelis et al 2018:3–4):

  Το proof of authority βασίζεται σε έμπιστους κόμβους που καλούνται αρχές

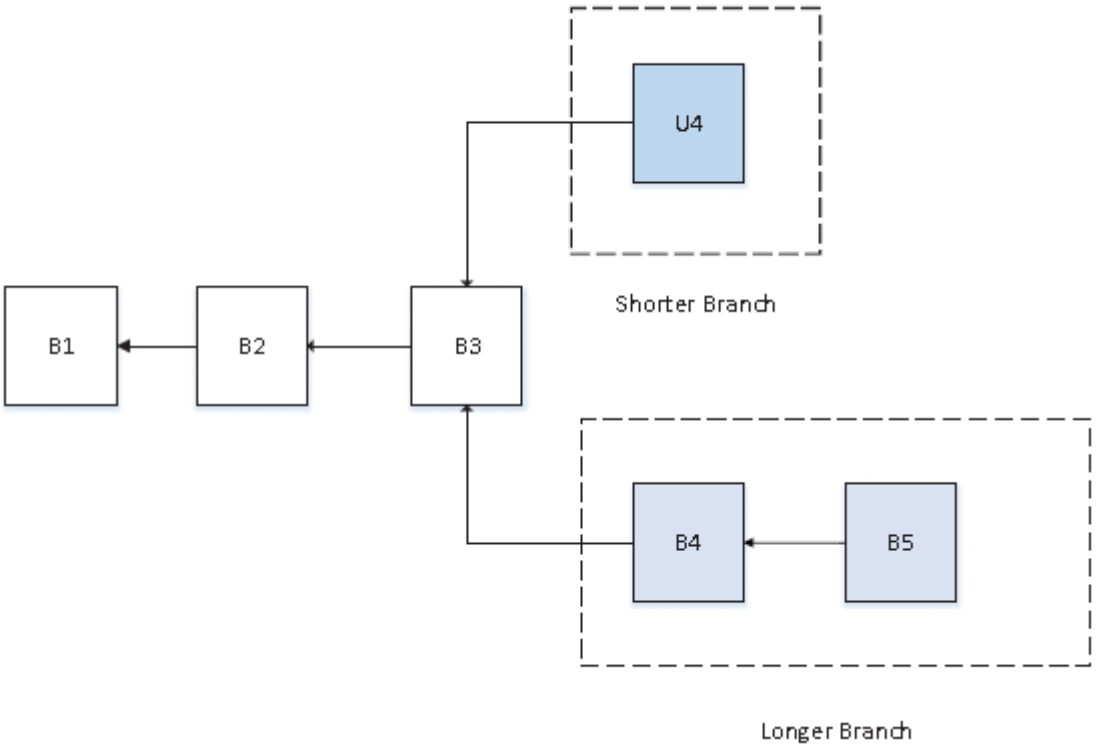
(*authorities*). Για να λειτουργήσει σωστά ο μηχανισμός χρειάζονται τουλάχιστον οι N/2 + 1, δηλαδή πάνω από τους μισούς, να είναι πραγματικά έμπιστοι. Αρχικά, όλοι οι κόμβοι αυτοί λαμβάνουν μοναδικό κωδικό αναγνώρισης και εκτελούν μια διαδικασία συναίνεσης για να αποφασιστεί η σειρά με την οποία θα εγκριθούν οι συναλλαγές που προκύπτουν από τα υπόλοιπα μέλη-πελάτες (clients) της blockchain. Η συναίνεση αυτή βασίζεται σε κυκλικό αλγόριθμο ο οποίος αφού χωρίσει τον χρόνο σε τμήματα (steps), επιλέγει διαφορετικό authority node ως αρχηγό σε κάθε step, ώστε να διαμοιραστεί η ευθύνη των περιεχομένων του επόμενου block σε πολλούς. Η Ethereum kovan testnet είναι μια blockchain που υλοποιεί το PoA.

- Αντιπροσωπευτική Απόδειξη Συμμετοχής (Delegated proof of stake – DpoS) (Zheng et al 2017:560–561):

  Πρόκειται για παραλλαγή του PoS, στην οποία οι κάτοχοι των στοιχημάτων (stakes), εκλέγουν τους αντιπροσώπους τους ως υποψήφιους για την παραγωγή και επιβεβαίωση νέων block. Ο μηχανισμός αυτός, προσφέρει μεγαλύτερη ταχύτητα στην επιβεβαίωση των συναλλαγών, ευελιξία στο μέγεθος και στον χρόνο μεταξύ των blocks τα οποία μπορούν να ρυθμιστούν από τους εκλεγμένους αντιπροσώπους. Επιπλέον, κακόβουλοι αντιπρόσωποι μπορούν να αποκλειστούν όταν αποκαλυφθούν αφού θα σταματήσουν να εκλέγονται από τους υπολοίπους. Η Eos και η Bitshares blockchains είναι υλοποιήσεις που χρησιμοποιούν τον εν λόγω μηχανισμό.
- Λιγότερο γνωστοί μηχανισμοί συναίνεσης ή παραλλαγές των παραπάνω αποτελούν οι: Απόδειξη Χώρου (Proof of Space – PoSp) (Wenbing Zhao et al 2019:3), Απόδειξη Παρερχόμενου Χρόνου (Proof of Elapsed Time – PoET) (Wenbing Zhao et al 2019:3–4), Ripple (Zheng et al 2017:561), Tendermint (Zheng et al 2017:561), κ.α. για τους οποίους όμως δεν θα επεκταθούμε στην παρούσα μεταπτυχιακή διατριβή.

Αξίζει να σημειωθεί εδώ, πως οι παραπάνω διαδικασίες έχουν σκοπό να επιλέξουν έναν κόμβο στον οποίο θα δοθεί το δικαίωμα να προσθέσει το επόμενο block στην αλυσίδα. Παρόλα αυτά, μπορεί για διάφορους λόγους (ισοψηφίας, καθυστέρησης ενημέρωσης του συστήματος, κ.α.), να επιλεγούν και να λάβουν το δικαίωμα αυτό δύο ή περισσότεροι κόμβοι ταυτόχρονα. Στην περίπτωση αυτή, η blockchain χωρίζεται (fork) αποκτώντας κλαδιά (branches). Η διαδικασία προσθήκης νέων block συνεχίζεται πλέον για κάθε κλαδί.

Επειδή όμως είναι εξαιρετικά δύσκολο και το επόμενο block να προστεθεί ταυτόχρονα, το κλαδί στο οποίο προστίθεται πρώτο νέα blocks (κανόνας του μακρύτερου κλαδιού, longer branch), είναι και αυτό που θα παραμένει και θα συνεχίσει την αρχική αλυσίδα, ενώ το άλλο (shorter branch) θα αποκλειστεί (Zheng et al 2017:560).



Εικόνα 2. Διακλάδωση blockchain όπου το μακρύτερο κλαδί υπερισχύει ως συνέχιση της αρχικής αλυσίδας

Ανεξάρτητα από το εάν προκύψει διακλάδωση της αρχικής αλυσίδας ή όχι, κάθε κόμβος που αποκτά το δικαίωμα και κατασκευάζει νέο block, το στέλνει στην συνέχεια στους πλησιέστερους κόμβους του (παρομοιάζοντας τον τρόπο λειτουργίας ενός δικτύου peer-to-peer, P2P), για έλεγχο. Οι κόμβοι αυτοί, επιθεωρούν το block και αν είναι έγκυρο το προωθούν στους δικούς τους πλησιέστερους κόμβους, διαφορετικά το απορρίπτουν και η διαδικασία τερματίζεται εκεί. Με τον τρόπο αυτό μάλιστα, το σύστημα προστατεύεται από επιθέσεις άρνησης υπηρεσίας (denial of service, DOS) κακόβουλων κόμβων που θέλουν να πλημμυρίσουν το δίκτυο χρηστών μιας blockchain με λανθασμένες εγγραφές προκειμένου να τους κρατούν απασχολημένους και να μην μπορούν να εργαστούν για την επικύρωση ορθών block. Εάν, λοιπόν, το νέο block επικυρωθεί ως έγκυρο από την πλειοψηφία των κόμβων της blockchain, τότε έχει επέλθει συναίνεση, το block θεωρείται έγκυρο και όλοι το προσθέτουν στο αντίγραφο της blockchain που διαθέτουν. Η

διαδικασία αυτή, παρέχει την μέγιστη ασφάλεια σε ότι αφορά την ακεραιότητα των blocks αλλά συνοδεύεται από κόστος απόδοσης, αφού για να επέλθει η συμφωνία αυτή, απαιτείται πολύς χρόνος.

Είδαμε όμως πως η διαδικασία προσθήκης ενός block είναι κοστοβόρα για τον κόμβο που την εκτελεί και για τον λόγο αυτό υπάρχει και σχετική ανταμοιβή. Κάθε συναλλαγή που συμμετέχει στο block αυτό έχει ένα ποσό αμοιβής σε κρυπτονόμισμα. Έτσι, με την επίτευξη της συναίνεσης, ο κόμβος λαμβάνει το άθροισμα των αμοιβών για όλες τις συναλλαγές που περιέχει το block το οποίο πρόσθεσε με επιτυχία στην blockchain. Ειδικά για τις blockchains κρυπτονομισμάτων, ο κόμβος λαμβάνει επιπλέον ανταμοιβή που προέρχεται από την δημιουργία νέων μονάδων κρυπτονομίσματος της αλυσίδας αυτής (πχ bitcoins στην περίπτωση της Bitcoin blockchain). Ουσιαστικά, ο κόμβος προσομοιάζει την λειτουργία της εξόρυξης και για αυτό το λόγο όσοι ανταγωνίζονται για την δημιουργία blocks σε cryptocurrency blockchains καλούνται μεταλλωρύχοι (miners). Γενικά, η ιδέα πίσω από αυτούς τους μηχανισμούς είναι να καταστεί περισσότερο κερδοφόρο για κάθε κόμβο μιας blockchain να εργάζεται για την διαφύλαξη της ορθότητας και την επέκτασή της, παρά να προσπαθεί να της επιτεθεί.

Συμπερασματικά σε ό,τι αφορά την ασφάλεια σε μια blockchain, προκειμένου να μπορέσει κάποιος κακόβουλα να αλλοιώσει τα περιεχόμενα σε ένα block και να καταφέρει να το διατηρήσει ως έγκυρο μέσα σε αυτήν, πρέπει:

- να επαναϋπολογίσει τα hash values για όλα τα blocks μετά το αλλοιωμένο,
- να εκτελέσει το proof-of-work (στην περίπτωση που αυτό υλοποιείται στην εν λόγω blockchain) για όλα τα blocks μετά το αλλοιωμένο,
- να μπορέσει να αποκτήσει έλεγχο σε πάνω από τους μισούς χρήστες του δικτύου P2P της blockchain ώστε να σημειώσουν το block ως έγκυρο, να επιτευχθεί η συναίνεση κι έτσι να γίνει αποδεκτό και από τους υπόλοιπους.

Βλέπουμε λοιπόν πως είναι σχεδόν αδύνατον να αλλοιωθούν δεδομένα μέσα σε μια blockchain. Μάλιστα, τα τελευταία χρόνια εμφανίζονται νέες blockchains οι οποίες υλοποιούν συνδυασμούς των μηχανισμών συναίνεσης προκειμένου να ενισχύσουν περεταίρω την ασφάλειά τους.

2.4 «Έξυπνα Συμβόλαια»

Μία από τις πρώτες εξελίξεις που έλαβαν μέρος στην τεχνολογία blockchain, είναι η

δυνατότητα προσθήκης «έξυπνων συμβολαίων» (smart contracts). Πρόκειται για προγράμματα (αλγορίθμους), τα οποία αποθηκεύονται μαζί με τα δεδομένα μέσα στο κάθε block και ενεργοποιούνται όταν ικανοποιηθούν συγκεκριμένα και ορισμένα κάθε φορά κριτήρια-συνθήκες. Αυτό δίνει μεγάλη ευελιξία στον τρόπο λειτουργίας μιας blockchain και ανοίγει τεράστιες δυνατότητες για επέκτασή της (Zheng et al 2017:563). Το Ethereum, είναι ένα από τα πιο γνωστά κρυπτονομίσματα που υλοποιεί smart contracts.

2.5 Τύποι blockchain

Οι blockchains που είδαμε έως τώρα, και ειδικά όσες αφορούν κρυπτονομίσματα, φέρουν ένα κοινό χαρακτηριστικό, τον δημόσιο χαρακτήρα τους. Αυτό σημαίνει πως ο καθένας, μπορεί να δημιουργήσει προσωπική διεύθυνση λογαριασμού και να λάβει μέρος σε αυτές είτε ως απλός χρήστης είτε ακόμα και να συμμετέχει στην διαδικασία επέκτασής τους ως miner. Οι blockchains αυτού του τύπου καλούνται δημόσιες (public) και άνευ-αδείας (permisionless) καθώς για να γίνει κανείς μέλος, δεν απαιτείται η αδειοδότησή του από κάποιον φορέα. Παρότι είναι ο πιο δημοφιλής τύπος blockchain όμως, δεν είναι και ο μοναδικός. Έτσι, οι blockchains χωρίζονται σε:

- Public, permisionless, οι οποίες όπως είδαμε είναι αποκεντρωμένες, προσφέρουν διαφάνεια και ελέγχονται από τον κανόνα της συναίνεσης.
- Ιδιωτικές (private), με-άδεια (permissioned). Πρόκειται για κλειστά οικοσυστήματα που συνήθως χρησιμοποιούν μεγάλοι οργανισμοί και εταιρικές κοινοπραξίες. Σε μια permissioned blockchain, δεν μπορεί ο καθένας να συμμετέχει και να έχει πρόσβαση στις συναλλαγές που περιέχονται ή να προσθέσει δικές του. Το δικαίωμα πρόσβασης και οι επιτρεπόμενες λειτουργίες του κάθε μέλους καθορίζονται κι εγκρίνονται από μια σειρά κριτηρίων που έχουν θεσπίσει οι ιδιοκτήτες της, οι οποίοι χρησιμοποιούν την δυναμική που τους προσφέρει η blockchain τεχνολογία για εσωτερικές επιχειρησιακές διεργασίες. Γίνεται αντιληπτό πως, στην περίπτωση αυτή, η συναίνεση ως εργαλείο για την διενέργεια αλλαγών στην αλυσίδα μπορεί να μην λειτουργεί με τον ίδιο τρόπο όπως στις δημόσιες blockchains αλλά να πηγάζει από μία μονάδα ή ομάδα οντοτήτων. Η συναίνεση έτσι επιτυγχάνεται ταχύτερα, εις βάρος όμως του ελέγχου της ακεραιότητας των blocks καθώς πλέον δεν έχει την έγκριση και αποδοχή της πλειοψηφίας αλλά ενός οργανισμού στον οποίο έχουν αποδώσει εμπιστοσύνη οι χρήστες με την συμμετοχή τους στην αλυσίδα αυτή. Στην ουσία

δηλαδή απαλείφεται ο αποκεντρωμένος χαρακτήρας της blockchain.

- Public, permissioned. Πρόκειται για ένα υβριδικό μοντέλο προσομοιάζει μια κοινή πηγή διαθέσιμων πόρων (Common-pool Resource, CPR). Μια blockchain που ανήκει στον τύπο αυτό, είναι δημόσια και ανοικτή προς όλους, αλλά για να γίνει κάποιος μέλος της και να μπορεί να συμμετέχει χρειάζεται να αποδείξει την ταυτότητά του. Ο λόγος για αυτή την διαφοροποίηση είναι πως συγκεκριμένες υλοποιήσεις χρειάζονται να υπάρχει μια φυσική ή νομική οντότητα πίσω από τον εγγεγραμμένο χρήστη για την παροχή της υπηρεσίας τους, για απόδοση ευθυνών εάν κι εφόσον αυτό χρειαστεί. Φυσικά μέσα στο οικοσύστημα της blockchain προσωπικά στοιχεία δεν θα είναι ορατά παρά μόνο όταν ζητηθεί ή όταν ο ίδιος ο χρήστης τα παρέχει προς συγκεκριμένα υποκείμενα ως απαραίτητη συνθήκη για μια υπηρεσία (πχ. ιατρικός φάκελος σε ιατρικό προσωπικό για διάγνωση) (Ruiz 2020:1). Τέτοιου τύπου blockchains βρίσκουν εφαρμογή σε υπηρεσίες του Δημοσίου (public services), υγείας, πανεπιστήμια, όπου ο μηχανισμός συναίνεσης γίνεται κι εδώ ταχύτερα από τις public blockchains καθώς θα εκτελείται από επιλεγμένους χρήστες-κόμβους οι οποίοι θα είναι διακεκριμένοι και κοινά αποδεκτοί ως έμπιστοι (πχ. γιατροί, καθηγητές, δημόσιοι λειτουργοί, κτλ). Ομοίως όμως, αυτό θα έρχεται σε κόστος της ασφάλειας της ακεραιότητας του block καθώς ένας κακόβουλος επιτιθέμενος θα χρειάζεται να αποκτήσει πρόσβαση στο 51% επί των κόμβων που συμμετέχουν στην διαδικασία συναίνεσης και όχι επί του συνόλου των χρηστών της blockchain.

Τα παραπάνω συνοψίζονται στον πίνακα που ακολουθεί (Zheng et al 2017:559):

	Public Permisionless	**Private Permissioned**	**Public Permissioned**
Συναίνεση από	Όλους	Έναν οργανισμό	Επιλεγμένους κόμβους
Πρόσβαση στα δεδομένα	Δημόσια	Επιλεγμένη	Επιλεγμένη
Ακεραιότητα block	Διασφαλισμένη	Θα μπορούσε να εκτεθεί σε κίνδυνο	Θα μπορούσε να εκτεθεί σε κίνδυνο
Απόδοση/Ταχύτητα	Χαμηλή	Υψηλή	Υψηλή
Αποκεντρωμένη	Ναι	Όχι	Μερικώς

Πίνακας 1. Σύγκριση τύπων blockchain

2.6 Χρήσεις

Ο κατανεμημένος ρόλος κάθε blockchain ανεξάρτητα από τον τύπο της, προωθεί την διαφάνεια, εξαλείφει την ανάγκη παρουσίας κι ελέγχου από ενδιάμεσους φορείς και οι ιδιότητες ασφάλειας που υλοποιεί, την κάνουν ιδιαιτέρως ελκυστική για εκμετάλλευση. Όπως γίνεται εύκολα αντιληπτό, η τεχνολογία αυτή έχει μεγάλες δυνατότητες και αποτελεί έναν κλάδο που εξελίσσεται συνεχώς. Για τον λόγο αυτό έχει κεντρίσει το παγκόσμιο ενδιαφέρον τεχνολόγων ερευνητών, επιχειρήσεων και κυβερνήσεων ώστε η τεχνολογία αυτή να αξιοποιηθεί και σε άλλες εφαρμογές πέρα από τα κρυπτονομίσματα που χρησιμοποιείται κυρίως μέχρι σήμερα.

2.6.1 Προσωπικά Στοιχεία & Τομέας υγείας

Σε blockchain θα μπορούσε κάποιος να αποθηκεύσει τα προσωπικά του στοιχεία, αλλά και το ιατρικό ιστορικό του. Στη συνέχεια με χρήση smart contracts και ψηφιακής υπογραφής, θα μπορούσε να επιτρέπει (ή να απαγορεύει) την πρόσβαση σε τμήμα της πληροφορίας σε τρίτους (πχ γιατρούς) (Mertz 2018:6).

2.6.2 Φυσική & Πνευματική ιδιοκτησία

Εκτός από τις συναλλαγές σε ψηφιακό κρυπτονόμισμα, σε blockchain θα μπορούσε να αποθηκευτεί και οποιαδήποτε συναλλαγή και περιουσιολόγιο, εξαλείφοντας την ανάγκη και τα έξοδα για συμβολαιογράφους (Yapa et al 2018:2–3).

Παρομοίως, ψηφιακές υπηρεσίες πρόσβασης σε προϊόντα πνευματικής ιδιοκτησίας (πχ μουσική), θα μπορούσαν να λειτουργούν σε blockchain. Οι πελάτες των υπηρεσιών θα πληρώνουν συνδρομή και με χρήση smart contracts, θα αποδίδεται αυτόματα μέρος της συνδρομής αυτής στους ιδιοκτήτες των μουσικών κομματιών ανάλογα με το πόσες φορές ακούστηκαν τα κομμάτια τους από τους συνδρομητές (Sijia Zhao and O'Mahony 2018:2–4).

2.6.3 Αυτοκίνητα

Αντικαθιστώντας τους απλούς χιλιομετρητές των αυτοκινήτων με "έξυπνους", μπορούμε να στέλνουμε τα συνολικά χιλιόμετρα που έχει καλύψει το αυτοκίνητο σε δεδομένες χρονικές στιγμές σε μια blockchain μαζί με άλλα επιλεγμένα στοιχεία που έχουν συλλεχθεί από τον εγκέφαλό του. Έτσι, μπορεί να καταπολεμηθεί η διαστρέβλωση των χιλιομετρητών που οδηγεί σε απάτες πώλησης και πιο φθαρμένα και άρα επικίνδυνα

αυτοκίνητα στους δρόμους (Abbade et al 2020:64–68) (Chanson et al 2017:14).

2.6.4 Τρόφιμα

Με την ίδια λογική, κάθε διαδικασία και στάδιο από το οποίο περνάει ένα τρόφιμο (ή μια συγκεκριμένη παρτίδα τροφίμων) από την παραγωγή μέχρι να φτάσει στον τελικό καταναλωτή, μπορεί να καταγράφεται σε μια blockchain. Έτσι, ο καταναλωτής έχει τη δυνατότητα ανά πάσα στιγμή να ελέγξει το ιστορικό του τρόφιμου που επιθυμεί να αγοράσει αλλά και οι ελεγκτικοί μηχανισμοί να εντοπίσουν και να αποσύρουν εύκολα, γρήγορα και με ακρίβεια τρόφιμα που έχουν εντοπιστεί να είναι αλλοιωμένα και επικίνδυνα για την δημόσια υγεία (Lin et al 2018:3–5).

Φυσικά, εκτός από τα τρόφιμα, θα μπορούσε να βρει εφαρμογή σε οποιοδήποτε καταναλωτικό αγαθό, έτσι ώστε να καταπολεμηθεί και η νοθεία αφού με αυτό τον τρόπο είναι εύκολο να εντοπιστεί ο πραγματικός κατασκευαστής και χώρα προέλευσης σε κάθε προϊόν που έχει το ιστορικό του σε μια blockchain (Perboli et al 2018:62026).

Φυσικά, οι παραπάνω περιπτώσεις δεν είναι οι μοναδικές στις οποίες θα μπορούσε να εφαρμοστεί η τεχνολογία blockchain για να προσφέρει μεγαλύτερη διαφάνεια, ασφάλεια και ταχύτητα. Αντιθέτως, οι δυνατότητες είναι ατέλειωτες και νέες αναδύονται καθημερινά καθώς η συγκεκριμένη τεχνολογία εξελίσσεται και ωριμάζει.

2.7 Κρυπτογραφία

Ένα από τα πιο ουσιαστικά ζητήματα σε ότι αφορά την καταγραφή των κινήσεων (transactions) σε μια blockchain, είναι η ταυτότητα και η ταυτοποίηση των εμπλεκομένων υποκειμένων. Οι συναλλαγές στις blockchains, κατά κανόνα, δεν γίνονται ονομαστικά. Κάτι τέτοιο θα ήταν παράλογο στην πλειοψηφία των περιπτώσεων, καθώς κάθε μέλος της έχει πρόσβαση σε όλα της τα δεδομένα κι έτσι θα ήταν ορατά προσωπικά (αλλά και ευαίσθητα προσωπικά σε ειδικές περιπτώσεις) στοιχεία.

Αντί αυτού, αξιοποιούνται τεχνικές ασύμμετρης κρυπτογραφίας για την δημιουργία και ταυτοποίηση συναλλαγών μέσω blockchain. Αυτό γίνεται με την χρήση ειδικών αλγορίθμων (με χαρακτηριστικό παράδειγμα τον Elliptic Curve Digital Signature Algorithm – ECDSA) οι οποίοι έχουν την δυνατότητα να παράγουν δύο ψηφιακά κλειδιά (αριθμούς), το ιδιωτικό (private key, *SK*) και το δημόσιο (public key, *PK*) (Zheng et al

2017:558). Τα κλειδιά αυτά συσχετίζονται με μαθηματική σχέση που πηγάζει από τον αλγόριθμο που χρησιμοποιήθηκε για την παραγωγή τους και προσδίδει σε αυτά τις εξής ιδιότητες:

- Μπορεί να υπολογιστεί το δημόσιο κλειδί, όταν το ιδιωτικό κλειδί είναι γνωστό
- Είναι υπολογιστικά αδύνατο να βρεθεί το ιδιωτικό κλειδί, όταν το δημόσιο κλειδί είναι γνωστό. Αυτό ισχύει διότι οι αλγόριθμοι αυτοί βασίζονται σε γνωστά δυσεπίλυτα μαθηματικά προβλήματα (πχ ο ECDSA, στο πρόβλημα διακριτού λογαρίθμου σε ελλειπτικές καμπύλες – ECDLP) κατά τα οποία θα χρειαστούν μερικές χιλιάδες χρόνια ασταμάτητων προσπαθειών για το πιο ισχυρό υπολογιστικό σύστημα προκειμένου να δοκιμάσει όλους τους πιθανούς συνδυασμούς κι επομένως να βρει με επιτυχία το ιδιωτικό κλειδί κάποιου γνωρίζοντας μόνο το δημόσιο κλειδί του.
- Η σχέση τους είναι ένα-προς-ένα. Δηλαδή δεν μπορεί να υπάρχουν περισσότερα από ένα ιδιωτικά κλειδιά που να αντιστοιχούν σε ένα δημόσιο κλειδί και το αντίστροφο.

Με βάση αυτές τις ιδιότητες, σε μια blockchain κρυπτονομισμάτων (πχ Bitcoin), το δημόσιο κλειδί γίνεται – ή χρησιμοποιείται για να δημιουργηθεί μονοσήμαντα – η δημόσια διεύθυνση του ψηφιακού πορτοφολιού του χρήστη, που μπορεί να χρησιμοποιεί για τις συναλλαγές του (πχ ως παραλήπτης κρυπτονομισμάτων) και είναι αυτό που καταγράφεται σε μια transaction μέσα στο blockchain. Φυσικά, από μόνο του ένα public key δεν μπορεί σε καμία περίπτωση να αντιστοιχηθεί σε κάποιο φυσικό πρόσωπο κι έτσι επιτυγχάνεται η πλήρης ψευδωνυμοποίηση. Στη συνέχεια, ο κάτοχος του ιδιωτικού κλειδιού (και μόνο εκείνος), πρέπει να έχει πρόσβαση στα κρυπτονομίσματα που έλαβε μέσα στο ψηφιακό πορτοφόλι του.

Για τους ίδιους λόγους, κάθε χρήστης Α μιας οποιουδήποτε τύπου blockchain μπορεί να υπογράψει μια ψηφιακή συναλλαγή με το ιδιωτικό του κλειδί (SK_A) και να τοποθετήσει το αποτέλεσμα στην blockchain. Τα υπόλοιπα μέλη της μπορούν στη συνέχεια να επιβεβαιώσουν πως πρόκειται για αυτό τον χρήστη Α εφόσον γνωρίζουν το δημόσιο κλειδί του (PK_A). Ξανά, ο υπολογισμός του ιδιωτικού κλειδιού που χρησιμοποιήθηκε για την υπογραφή, θεωρείται αδύνατος. Όλα αυτά όμως αναθεωρούνται τάχιστα, καθώς η υλοποίηση των κβαντικών υπολογιστών (quantum computers) είναι προ των πυλών.

Κεφάλαιο 3

Κβαντικοί Υπολογιστές

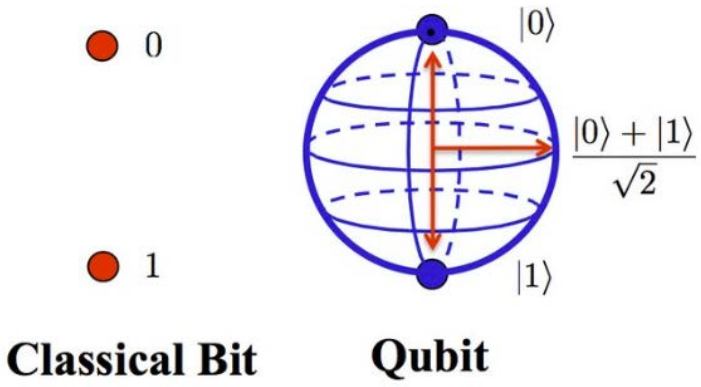
Οι κλασικοί, «παραδοσιακοί», «συμβατικοί» ηλεκτρονικοί υπολογιστές (Η/Υ) που γνωρίζουμε και χρησιμοποιούμε εδώ και δεκαετίες, λειτουργούν με δυαδικά ψηφία (bits). Κάθε δυαδικό ψηφίο (bit) μπορεί να λάβει δύο διακριτές καταστάσεις μηδέν ή ένα (0/1). Το πλήθος των bits που μπορεί ένα υπολογιστικό σύστημα να επεξεργαστεί ταυτόχρονα σε κάθε κύκλο εργασίας του, ορίζουν την υπολογιστική δύναμη του συστήματος καθώς χρησιμοποιούνται για να αποθηκεύονται προσωρινά δεδομένα προς επεξεργασία. Διπλασιάζοντας τα bits, διπλασιάζεται και η υπολογιστική του δύναμη που σημαίνει πως η σχέση του πλήθους των bits με την ισχύ του συστήματος είναι γραμμική. Έτσι, ακόμα και αν ο νόμος του Moore (που προβλέπει τον διπλασιασμό των τρανζίστορ σε ένα ολοκληρωμένο κύκλωμα κάθε δύο περίπου χρόνια (Rao 2017:1021)) συνεχίσει να επαληθεύεται για πολλά χρόνια ακόμα, προκειμένου να υπάρξει σημαντική πρόοδος στην δυναμική των κλασικών ηλεκτρονικών υπολογιστών, χρειάζεται μεγάλη προσπάθεια με δυσανάλογα (μικρά) αποτελέσματα. Από την άλλη, η ιδέα για έναν κβαντικό υπολογιστή (quantum computer), παρότι υπάρχει αρκετά χρόνια, δεν είχε ωριμάσει παρά μόνο την τελευταία δεκαετία όπως θα δούμε και παρακάτω. Μάλιστα, η λέξη υπολογιστής, μπορεί να είναι παραπλανητική καθότι οι κβαντικοί υπολογιστές δεν μοιάζουν οπτικά (τουλάχιστον ακόμα) με τους κλασικούς.

3.1 Ιδιότητες

Οι κβαντικοί υπολογιστές λειτουργούν, κατά αντιστοιχία, με κβαντικά δυαδικά ψηφία (quantum-bits, πιο γνωστά ως qubits). Κάθε qubit, είναι ένα κβαντομηχανικό σύστημα δύο θέσεων (μηδέν/ένα) που υπακούει σε τρεις αρχές, της υπέρθεσης , της εμπλοκής και της μη-κλωνοποίησης, που είναι υπεύθυνες για τις μοναδικές ιδιότητες των κβαντικών υπολογιστικών συστημάτων (AL-Mubayedh et al 2019:1).

- Υπέρθεση (Superposition)

  Σύμφωνα με την αρχή της υπέρθεσης, η κατάσταση (τιμή) για κάθε qubit μπορεί να είναι 0 ή 1 αλλά μέχρι να μετρηθεί διατηρεί και όλες οι ενδιάμεσες τιμές μεταξύ των δύο αυτών αριθμών (το qubit θεωρείται πως στην κατάσταση υπέρθεσης έχει και τις δύο τιμές μαζί, δηλαδή 0 και 1 ταυτόχρονα) (Rao 2017:1022). Ουσιαστικά, υπολογίζουμε την πιθανότητα ενός qubit να μας δίνει μηδέν ή ένα. Όπως ισχύει στα κύματα της κλασικής Φυσικής, έτσι και οι καταστάσεις (states) ενός qubit μπορούν να προστεθούν δίνοντας μια νέα καινούργια έγκυρη κατάσταση, την υπέρθεση. Η κατάσταση αυτή θα μπορούσε να αναπαρασταθεί ως μια γραμμική συνάρτηση που προκύπτει από την πρόσθεση άλλων διακριτών κβαντικών καταστάσεων. Για αυτό σχηματικά, όλες οι πιθανές καταστάσεις ενός qubit παριστάνονται από την σφαίρα του Bloch όπως φαίνεται στην παρακάτω εικόνα (AL-Mubayedh et al 2019:2).



Εικόνα 3. Σχηματική απεικόνιση ενός κλασικού bit κι ενός qubit (σφαίρα του Bloch)

- Εμπλοκή (Entanglement)

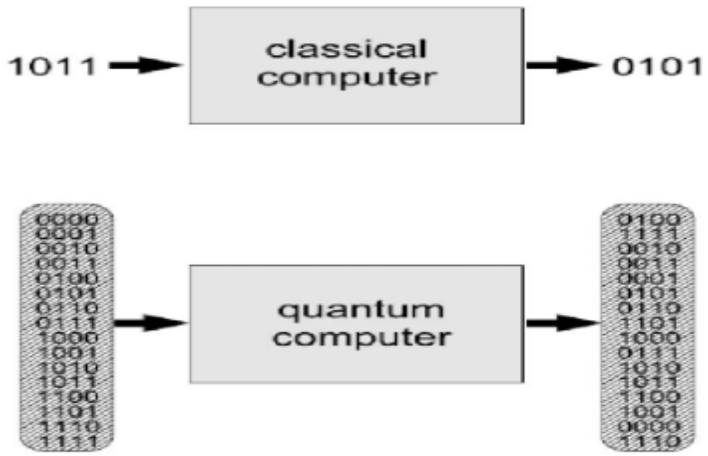
  Η κβαντική εμπλοκή είναι μια ειδική σύνδεση που λαμβάνει χώρα μεταξύ δύο qubits. Όταν δύο qubits έρθουν πολύ κοντά και κάτω από ειδικές συνθήκες που μπορούν να προϋπάρχουν, να τύχουν ή να προκληθούν (Orzel 2017:1), δημιουργείται ένας ιδιαίτερος δεσμός που τα συγχρονίζει. Ο δεσμός αυτός γίνεται εμφανής, κατά την μέτρηση των τιμών των qubits, οπότε και δίνουν πάντα την ίδια τιμή όποια και αν είναι αυτή. Αυτό που κάνει μοναδική την ιδιότητα της κβαντικής εμπλοκής, είναι πως όταν αυτή υπάρξει ή δημιουργηθεί, διατηρείται ακόμα και αν τα qubits απομακρυνθούν σε τεράστιες αποστάσεις το ένα από το άλλο (AL-Mubayedh et al 2019:2).

- Μη-Κλωνοποίηση (Non-Clonability)

  Η αρχή της μη-κλωνοποίησης που είναι λογική συνέπεια της κβαντικής φύσης των qubits έχει ιδιαίτερη σημασία για τον τομέα της ασφάλειας υπολογιστών και δικτύων. Σύμφωνα με αυτή, δεν υπάρχει γνωστή διαδικασία που να μπορεί να αντιγράψει την κβαντική κατάσταση ενός qubit όταν αυτή είναι άγνωστη. Έτσι, τυχών κακόβουλος επιτιθέμενος που θα προσπαθήσει να υποκλέψει επικοινωνία που βασίζεται σε qubits, δεν θα μπορέσει να πραγματοποιήσει την επίθεσή του αυτή καθώς τη στιγμή που θα επιχειρήσει να διαβάσει (μετρήσει) την τιμή ενός qubit, θα αλληλοεπιδράσει μαζί του με αποτέλεσμα να επηρεάσει την τιμή του (AL-Mubayedh et al 2019:2).

3.2 Σύγκριση Κλασικού με Κβαντικού Υπολογιστή – Ένα παράδειγμα

Για να γίνει καλύτερα κατανοητή η διαφορά στην δυναμική μεταξύ των κλασικών υπολογιστικών συστημάτων με τα κβαντικά, ας δούμε σε παράθεση έναν κλασικό ΗΥ (classical computer) των 4 bits κι έναν κβαντικό (quantum computer) των 4 qubits. Ο κλασικός ΗΥ δέχεται ως είσοδο (input) 4 bits, τα οποία επεξεργάζεται δίνοντας ως έξοδο (output) αποτέλεσμα που αποτελείται πάλι από 4 bits. Ο κβαντικός υπολογιστής με 4 qubits, μπορεί να δεχτεί και να υπολογίζει ταυτόχρονα όλες τις δυνατές τιμές των 4 bits δηλαδή $4^2 = 16$ περιπτώσεις. Αυτή η έννοια του παραλληλισμού (parallelism), του ταυτόχρονου δηλαδή υπολογισμού, είναι η σημαντικότερη ιδιότητα των κβαντικών υπολογιστών και αυτό που τους διαφοροποιεί από τους κλασικούς (Spector 2008:251).



Εικόνα 4. Σύγκριση ενός κλασικού υπολογιστή 4bits με έναν κβαντικό 4qubits

Γίνεται εύκολα αντιληπτό λοιπόν, πως ενώ η σχέση της αύξησης των bits με την επεξεργαστική ισχύ στους κλασικούς υπολογιστές είναι γραμμική, η αντίστοιχη των qubits στους κβαντικούς, είναι εκθετική. Έτσι, με κάθε μικρή πρόοδο στην εξέλιξη των κβαντικών υπολογιστών, τα οφέλη στην υπολογιστική ισχύ είναι τεράστια.

3.3 Δυσκολίες στην εξέλιξη

Φυσικά όμως, όλα δεν είναι ιδανικά. Βρισκόμαστε ακόμα σε πειραματικό στάδιο και απέχουμε από την κατασκευή εμπορικού κβαντικού υπολογιστή με πραγματικά χρηστική επεξεργαστική ισχύ. Οι πιο αισιόδοξοι επιστήμονες μιλούν για δύο έως δέκα έτη ενώ οι πιο συγκρατημένα αισιόδοξοι αναφέρουν πως θα χρειαστούν άνω των δεκαπέντε ετών για την κατασκευή εμπορικών κβαντικών υπολογιστών (Easttom 2019:0811). Οι λόγοι που καθυστερούν τόσο την εξέλιξη αυτή είναι πολλοί:

- Όταν προσπαθήσουμε να μετρήσουμε την τιμή σε ένα qubit, αλληλοεπιδρούμε μαζί του και αυτή η αλληλεπίδραση το αναγκάζει να εκπέσει από την κατάσταση της υπέρθεσης, σε μια διακριτή τιμή ίση με μηδέν ή ένα. Τότε όμως μπορεί να επέλθει απώλεια πληροφορίας. Αυτό ονομάζεται φαινόμενο της μη-συνοχής (decoherence) και οφείλεται στην εξαιρετικά ευαίσθητη και ασταθή φύση των qubits και την αδυναμία τους να διατηρήσουν την κατάστασή τους παρά μόνο για μερικά κλάσματα του δευτερολέπτου. Για την καταπολέμηση του προβλήματος αυτού, απαιτείται το κβαντομηχανικό σύστημα να είναι απομονωμένο με ασφάλεια από εξωτερικές επιδράσεις. Ως αντίμετρο, έχουν αναπτυχθεί αλγόριθμοι διόρθωσης σφάλματος οι οποίοι παρέχουν μερική ανοχή σε σφάλματα λόγω της μη-συνοχής (Spector 2008:251).
- Για να επιτευχθεί η σταθεροποίηση κι επομένως η υπέρθεση των qubits και να ελαττωθεί ο «θόρυβος» χρειάζονται πολύ χαμηλές θερμοκρασίες που φτάνουν τους -273° Celsius (3°-5° Kelvin) (Easttom 2019b:10). Η επίτευξη τόσο χαμηλών θερμοκρασιών γίνεται με υγρό Ήλιο (Helium) ή άλλες ειδικές τεχνικές ψύξης (Van Meter and Oskin 2006:37) . Μόνο εταιρείες με μεγάλη οικονομική δυνατότητα (ή πρόσβαση σε κρατικές επιδοτήσεις) μπορούν να κατασκευάσουν πειραματικά εργαστήρια με τέτοιες δυνατότητες ψύξης και να τα στελεχώσουν ανάλογα.
- Για να μπορέσουμε να θεωρήσουμε έναν κβαντικό υπολογιστή χρήσιμο στην επίλυση προβλημάτων, πρέπει να περιέχει πάνω από εκατό χιλιάδες qubits. Ο αριθμός των qubits που έχουν επιτευχθεί μέχρι σήμερα είναι αρκετός μόνο για πειραματισμούς και μελέτη (Easttom 2019b :9).

- Η αποθήκευση των qubits γίνεται πειραματικά σε ιόντα θετικά ή αρνητικά φορτισμένων ατόμων. Όμως λόγω της φύσης και της τάσης των ατόμων να κάνουν χημικούς δεσμούς με άλλα άτομα ώστε να αποκτήσουν ουδέτερο φορτίο, η λύση αυτή παρουσιάζει εξαιρετικές δυσκολίες. Μια νεότερη εξέλιξη στον τομέα, εξετάζει την αποθήκευση σε ουδέτερα άτομα (neutral atoms) που όμως είναι πολύ δυσκολότερη να επιτευχθεί (Easttom 2019b:12, Weiss and Saffman 2017:45–50).

3.4 Ορόσημα Εξέλιξης

Ας δούμε παρακάτω ένα χρονοδιάγραμμα των πιο σημαντικών σημείων (milestones) της μέχρι τώρα εξέλιξης των quantum υπολογιστών. Πολλές φορές μπορεί να υπάρχει η αίσθηση της στασιμότητας, όμως όπως είπαμε και παραπάνω, μια μικρή εξέλιξη στον τομέα, μπορεί να φέρει επαναστατική πρόοδο. Σχηματικά, θα μπορούσε να παρουσιαστεί σαν μια ανοδική σκάλα.

1982 – Ο διακεκριμένος φυσικός και νομπελίστας Richard Feynman περιέγραψε την ιδέα ενώ κβαντομηχανικού υπολογιστή (συγκεκριμένα αναρωτήθηκε σχολιάζοντας σε μια συζήτηση εάν θα γινόταν να χρησιμοποιηθεί η κβαντική Φυσική για την κατασκευή και λειτουργία ενός τέτοιου υπολογιστικού συστήματος) (Singh and Singh 2016:268).
1998 – Το MIT μαζί με τα εργαστήρια του Los Alamos, προσομοίωσαν το πρώτο qubit με τη χρήση αμινοξέων (Ningtyas and Mutiara 2010:5).
1998 – Η πρώτη μηχανή με δύο qubits κατασκευάστηκε στο Berkeley (Πανεπιστήμιο της Καλιφόρνια) (Chuang et al 1998:3408).
2005 – Το Institute of Quantum Optics & Quantum Information του Πανεπιστημίου Innsbruck της Αυστρίας, κατασκεύασε το πρώτο σύστημα με 8 qubits (1ο quantum byte) (Ningtyas and Mutiara 2010:6).
2007 – Η Καναδική νεοσύστατη (startup) εταιρεία D-Wave παρουσίασε έναν κβαντικό υπολογιστή των 16qubits ο οποίος μπόρεσε να επιλύσει έναν γρίφο Sudoku καθώς και άλλα προβλήματα αντιστοίχισης. Ο ισχυρισμός της εταιρείας πως μέχρι το 2008 θα μπορέσει να κατασκευάσει πρακτικά κβαντικά υπολογιστικά συστήματα αντιμετωπίζεται με σκεπτικισμό (Ningtyas and Mutiara 2010:6).
2009 – Το Πανεπιστήμιο του Yale, κατασκεύασε τον πρώτο quantum επεξεργαστή (DiCarlo et al 2009:1).
2009 – Ο οργανισμός NIST κάνει επίδειξη διάφορων υπολογιστικών διαδικασιών πάνω σε qubits (Hanneke et al 2009:1).

2011 – Η εταιρεία D-Wave κατασκευάζει τον D-Wave One, τον πρώτο – όπως ισχυρίζεται – κβαντικό υπολογιστή (Singh and Singh 2016:268).

2012 – Η εταιρεία D-Wave καταφέρνει κβαντικούς υπολογισμούς με την χρήση 84 qubits (Bian et al 2013:14).

2012 – Η αστάθεια των qubits περιορίστηκε για διάστημα δύο δευτερολέπτων σε θερμοκρασία δωματίου με την χρήση ακτίνων laser σε άτομα Άνθρακα-13 (Maurer et al 2012:1).

2015 – Η εταιρεία D-Wave Systems Inc. ανακοίνωσε πως στις 22 Ιουνίου έσπασε το φράγμα των 1.000 qubits (Singh and Singh 2016:268).

2017 – Η IBM παρουσιάζει κβαντικό υπολογιστή με 17 qubits (Bauer 2017:1).

2017 – Η IBM παρουσιάζει λειτουργικό κβαντικό υπολογιστή με 50 qubits ο οποίος μπορεί να διατηρήσει την κβαντική συνοχή των qubits για 90 microseconds (Knightarchive page 2017:1).

2018 – Η Google ανακοίνωσε την κατασκευή κβαντικού chip με 72 qubits το οποίο ονόμασε “Bristlecone” (Kelly 2018:1).

2018 – Η Intel επιβεβαιώνει την ανάπτυξη δοκιμαστικού υπεραγώγιμου chip που αποτελείται από 49 qubits και το οποίο ονομάζει “Tangle Lake” (Intel Corporation 2018:1).

2019 – Η IBM παρουσιάζει τον πρώτο εμπορικό κβαντικό υπολογιστή, με ονομασία “IBM Q System One” που χρησιμοποιεί ολοκληρωμένα κυκλώματα και αποτελείται από 20 qubits (Nay 2019a:1).

2019 – Η IBM παρουσιάζει τον 14^{ο} κβαντικό της υπολογιστή 53ων qubits (Nay 2019b:1).

3.5 Δυνατότητες – Χρήσεις

Η ουσία και το «επαναστατικό» που προκύπτει από την κατασκευή τέτοιων κβαντικών υπολογιστών, είναι πως λόγω της παραλληλίας, θα είναι πολύ γρήγοροι στην επεξεργασία δεδομένων κι έτσι θα μπορούν να εκτελέσουν υπολογισμούς και να απαντήσουν σε υπερβολικά πολύπλοκα ερωτήματα σε αποδεκτό χρόνο, την ώρα που οι πιο ισχυροί σύγχρονοι υπολογιστές σήμερα χρειάζονται πολλά χρόνια συνεχής επεξεργασίας για να το καταφέρουν. Οι δυνατότητες που θα φέρουν στην επιστημονική κοινότητα τα πρώτα χρηστικά κβαντικά υπολογιστικά συστήματα θα είναι ανεξάντλητες και καθώς εξελίσσονται, οι χρήσεις τους θα είναι όλο και περισσότερες. Οι τομείς που αναμένεται να εκμεταλλευτούν την δυναμική των κβαντικών υπολογιστών είναι (Kershaw and Palmer (2019):1):

- Κρυπτογραφία

  Πρόκειται για την πιο γνωστή εφαρμογή των κβαντικών υπολογιστών. Η σημασία της επίδρασης αυτής μάλιστα είναι τεράστια, αφού θα επηρεάσει τα κρυπτογραφικά μοντέλα που χρησιμοποιούνται σήμερα στο διαδίκτυο καθιστώντας τα απαρχαιωμένα. Λόγω της ταχύτητάς τους, οι κβαντικοί υπολογιστές θα μπορούν αποδεδειγμένα (βλ. Κεφ.4) να επιλύσουν, σε σύντομο χρονικό διάστημα, μαθηματικά προβλήματα που χαρακτηρίζονται ως Δυσκολίας Μη-Ντετερμενιστικού Πολυωνυμικού χρόνου (Nondeterministic Polynomial Hard, NP-Hard) και χρησιμοποιούνται για να εξασφαλίσουν την ιδιωτικότητα και την ακεραιότητα των επικοινωνιών στο διαδίκτυο σήμερα.

- Προσομοιώσεις

  Μοντέλα όπως πολύπλοκα μόρια χημικών στοιχείων και διεργασίες όπως η φωτοσύνθεση, είναι τόσο σύνθετα που δεν μπορούν να προσομοιωθούν πλήρως από τα σημερινά υπολογιστικά συστήματα. Οι κβαντικοί υπολογιστές αναμένεται να προσφέρουν αυτή τη δυνατότητα, με άμεση επίδραση στην κατανόηση και εκμετάλλευση αυτών των συστημάτων. Χαρακτηριστικό παράδειγμα αποτελεί η νιτρογενάση (nitrogenase), ένα ένζυμο που χρησιμοποιείται σε λιπάσματα. Η μοντελοποίηση από κβαντικούς υπολογιστές της δομής του ενζύμου αυτού, θα μπορούσε να οδηγήσει σε βαθύτερη κατανόησή του με άμεση επίπτωση την ελάττωση της εκπομπής αερίων που επιβαρύνουν το φαινόμενο του θερμοκηπίου.

- Βελτιστοποίηση

  Αλγόριθμοι που χρησιμοποιούνται σήμερα σε διάφορους τομείς, θα μπορούν να βελτιστοποιηθούν αφού οι κβαντικοί υπολογιστές θα μπορούν να υπολογίσουν περισσότερες παραμέτρους με ενδεχόμενες νέες πιθανές λύσεις. Τομείς που αναμένεται να επωφεληθούν άμεσα από την βελτιστοποίηση των διαδικασιών τους είναι η ροή κυκλοφορίας οχημάτων, οι μεταφορές γενικότερα, η επιμελητεία (logistics), η υγειονομική περίθαλψη και διάγνωση αλλά και η τεχνολογία υλικών.

- Εκμάθηση Μηχανών (Machine Learning)

  Ο τομέας του machine learning και γενικότερα της τεχνητής νοημοσύνης (artificial intelligence, AI), περιλαμβάνει πολύπλοκα μοντέλα και υπολογισμούς σε τεράστιες δομές δεδομένων. Οι κβαντικοί υπολογιστές θα προσφέρουν εκθετικά ταχύτερες λύσεις από αυτές των κλασικών υπολογιστικών συστημάτων που υπάρχουν σήμερα, βοηθώντας έτσι στην επίλυση προβλημάτων όπως η ενεργειακή κρίση και η κλιματική αλλαγή.

Παρόλα αυτά, οι κβαντικοί υπολογιστές δεν αποτελούν πανάκεια. Δεν πρόκειται να είναι καλύτεροι σε όλα από τους κλασικούς υπολογιστές και υπάρχουν πολλές περιπτώσεις και υπολογισμοί στους οποίους ένας κλασικός υπολογιστής θα κάνει καλύτερη και πιο γρήγορη δουλειά από έναν σύγχρονης τεχνολογίας (state-of-the-art) quantum αντίστοιχό του (Spector 2008:252). Ακόμα όμως κι έτσι, για προβλήματα τα οποία λύνονται σήμερα με τους κλασικούς υπολογιστές, είναι επιπόλαιο να χρησιμοποιηθούν κβαντικοί, καθότι ο χειρισμός των qubits είναι (τουλάχιστον με τις τρέχουσες μεθόδους) πολύ πιο δύσκολος από αυτόν των bits. Έτσι, οι κβαντικοί υπολογιστές θα αποτελέσουν συμπληρωματικά συστήματα των κλασικών υπολογιστών και όχι αντικαταστάτες τους.

3.6 Απειλές για την Κρυπτογραφία

Οι τεράστιες δυνατότητες που θα δώσουν στην επιστημονική κοινότητα οι κβαντικοί υπολογιστές και τα πολλά προβλήματα που θα επιλύσουν, είναι η μία όψη του νομίσματος. Η άλλη είναι πως κάποιες από τις δυνατότητες αυτές, δύναται να αξιοποιηθούν για διαφορετικούς, λιγότερο «ευγενείς» σκοπούς. Το μεγαλύτερο πρόβλημα που θα αντιμετωπίσει η παγκόσμια κοινότητα στο διαδίκτυο είναι πως ουσιαστικά οι κβαντικοί υπολογιστές θα καταστήσουν ανεπαρκείς τους σημερινούς αλγόριθμους ασύμμετρης κρυπτογράφησης (δημοσίου κλειδιού) οι οποίοι είναι δημοφιλείς. Όπως είναι γνωστό, η κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιείται στην πλειοψηφία των επικοινωνιών μέσω διαδικτύου (ανταλλαγή συμμετρικού κλειδιού, ασφαλείς ιστοσελίδες μέσω του πρωτοκόλλου HTTPs, emails), στις ψηφιακές υπογραφές, τις online υπηρεσίες (web banking, e-commerce, etc) κι επομένως στις blockchains.

Συγκεκριμένα, οι πιο συχνά χρησιμοποιούμενοι αλγόριθμοι ασύμμετρης κρυπτογράφησης:

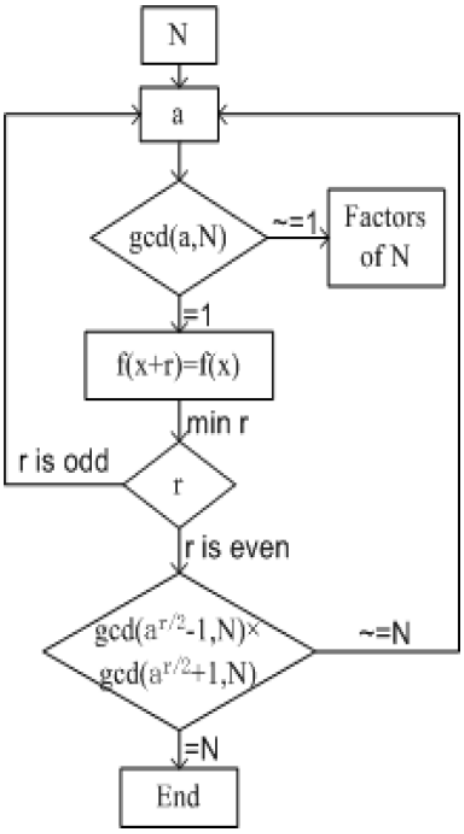
- RSA (Rivest-Shamir-Adleman): Βασίζει την ασφάλειά του στο μαθηματικό πρόβλημα της παραγοντοποίησης πολύ μεγάλων ακέραιων αριθμών σε γινόμενο πρώτων αριθμών (factoring).
- DH (Diffie-Hellman): Βασίζεται στο μαθηματικό πρόβλημα του διακριτού λογαρίθμου (Discrete Logarithm).
- ECDSA (Elliptic Curve Digital Signature Algorithm): Βασίζεται επίσης στο πρόβλημα διακριτού λογαρίθμου με εφαρμογή σε ελλειπτικές καμπύλες.

Οι κβαντικοί υπολογιστές όμως, θα μπορούν να επιλύσουν όλα τα παραπάνω μαθηματικά προβλήματα σε πρακτικό χρόνο. Η πραγματικότητα είναι βέβαια πως και οι κλασικοί υπολογιστές απειλούν να λύσουν τα παραπάνω προβλήματα σε όλο και μικρότερο χρόνο. Η απειλή αυτή αναχαιτίζεται όμως με την χρήση όλο και μεγαλύτερων κλειδιών στην διαδικασία της κρυπτο/αποκρυπτογράφησης. Αυτό στην ουσία αποτελεί ένα προσωρινό ημίμετρο, αφού για έναν κβαντικό υπολογιστή το μέγεθος του κλειδιού δεν θα επηρεάζει σημαντικά την ικανότητά του να «σπάσει» τους κρυπτογραφικούς αλγορίθμους.

3.6.1 Ο αλγόριθμος του Shor

Ο λόγος που κάνει πιο επικίνδυνες τις παραπάνω απειλές, είναι το γεγονός πως η ισχύς τους έχει αποδειχτεί από τον «αλγόριθμο του Shor» πολλά χρόνια πριν τις πρώτες προσπάθειες για κατασκευή κβαντικών υπολογιστών. Ο αλγόριθμος του Shor, περιεγράφηκε από τον Peter Shor το 1994 και απέδειξε πως ένας κβαντικός υπολογιστής (όταν κατασκευαστεί), θα μπορεί να παραγοντοποιήσει έναν πολύ μεγάλο ακέραιο αριθμό N, σε γινόμενο πρώτων αριθμών σε πολυωνυμικό χρόνο (ίσο με logN) σε αντίθεση με τον υποεκθετικό που απαιτείται για έναν κλασικό υπολογιστή. Με τον αλγόριθμο αυτό δηλαδή, κρυπτογραφικοί αλγόριθμοι (όπως ο RSA) που βασίζουν την δύναμή τους στο πρόβλημα της παραγοντοποίησης, ουσιαστικά καθίστανται ευάλωτοι. Στη συνέχεια αυτή η απόδειξη επεκτάθηκε ώστε να συμπεριλάβει το πρόβλημα του διακριτού λογαρίθμου (discrete logarithm problem) (Nagaich and Goswami 2015:165) αλλά και της παραλλαγής του σε ελλειπτικές καμπύλες (elliptic curve discrete logarithm problem) επηρεάζοντας κατά τρόπο παρόμοιο κρυπτογραφικούς αλγορίθμους όπως τον Diffie-Hellman, El Gamal αλλά και Elliptic Curve Digital Signature Algorithm (ECDSA).

Ουσιαστικά, ο αλγόριθμος του Shor, αποδεικνύει πως όλοι οι ασύμμετροι (δημοσίου κλειδιού) κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούμε σήμερα θα βρίσκονται σε κίνδυνο στην μετα-κβαντική εποχή (Van Meter and Oskin 2006:57) και πρέπει να αντικατασταθούν. Στην παρακάτω εικόνα, παρουσιάζεται σε διάγραμμα ροής (flowchart) ο αλγόριθμος του Shor (Zhang et al 2007:779).



Εικόνα 5. Διάγραμμα Ροής του Αλγορίθμου του Shor

3.6.2 Ο αλγόριθμος του Grover

Αξίζει εδώ να συμπληρώσουμε, πως οι ασύμμετροι κρυπτογραφικοί αλγόριθμοι δεν είναι οι μόνοι που κινδυνεύουν στην μετα-κβαντική εποχή. Ο Lov Grover, ανακάλυψε τον ομώνυμο αλγόριθμο αναζήτησης και απέδειξε πως αν αυτός χρησιμοποιηθεί από έναν κβαντικό υπολογιστή, μπορεί να βρει με επιτυχία οποιοδήποτε στοιχείο *a* σε ένα σύνολο *N* στοιχείων σε χρόνο τέσσερις φορές ταχύτερο από έναν κλασικό υπολογιστή. (Almazrooie et al 2018:2) Αυτό σημαίνει πως θα μπορούσε να κρυπταναλύσει ένα συμμετρικό κρυπτογραφικό αλγόριθμο (πχ AES) σε μη-απαγορευτικό χρόνο. Ευτυχώς όμως, ο χρόνος αυτός δεν μπορεί ποτέ να γίνει πολυωνυμικός όπως στην περίπτωση του Shor και των ασύμμετρων αλγορίθμων κι έτσι θεωρητικά η απειλή αυτή μπορεί να αναχαιτιστεί διπλασιάζοντας το μέγεθος των κλειδιών που χρησιμοποιούνται σήμερα για την κρυπτογράφηση (Chen et al 2016:8). Για παράδειγμα, ένας συμμετρικός αλγόριθμος με μέγεθος κλειδιού 256 bits θα παρέχει ασφάλεια στη μετακβαντική εποχή ισοδύναμη με αυτή ενός αλγορίθμου με μέγεθος κλειδιού 128 bits στους συμβατικούς υπολογιστές. Τα βήματα του αλγορίθμου του Grover, παρουσιάζονται στην παρακάτω εικόνα.

Input: An unstructured set $N = \{a_1, a_2, \ldots, a_n\}$
Output: $a_i \in N$
Step 1: Initialization of the quantum register:
all the qubits $x^{\otimes n}$ to $|0\rangle$ state and the oracle qubit q to $|1\rangle$ state:
$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$
Step 2: Put the register in an uniformly distributed superposition:
apply **H** Hadamard gate::
$|\psi_1\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{N-1} |i\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
Step 3: Apply Grover iterations:
for $2^{n/2}$ *times*, **do**
    a – Apply the oracle:
    $|x\rangle \xrightarrow{o} (-1)^{f(x)} |x\rangle, \qquad f(x)\ as\ in\ eq.\ (3)$
    b – Perform Grover operator (inversion about the mean):
    i. Apply $H^{\otimes n}$
    ii. Conditionally shift phase
    iii. Apply $H^{\otimes n}$
Step 4: Measure the quantum register

Εικόνα 6. Τα βήματα του αλγορίθμου του Grover

Σημειώνουμε σε αυτό το σημείο, ότι δεν θα γίνει περαιτέρω μελέτη και ανάλυση των αλγορίθμων του Shor και του Grover, καθώς οι λεπτομέρειες τους εκφεύγουν του αντικειμένου της παρούσας μεταπτυχιακής διατριβής.

Κεφάλαιο 4

Μετα-Κβαντικά Κρυπτοσυστήματα

Είδαμε λοιπόν, ότι οι κβαντικοί υπολογιστές έρχονται αργά ή γρήγορα και φέρνουν μαζί τους πολλές υποσχέσεις αλλά και αρκετούς κινδύνους. Αξίζει, στο σημείο αυτό, να αναλογιστούμε πως η υποδομή για την κρυπτογραφία δημοσίου κλειδιού που χρησιμοποιούμε σήμερα, χρειάστηκε περίπου δύο δεκαετίες για να ολοκληρωθεί, ενώ βασίζεται σε αλγορίθμους που κατασκευάστηκαν τρεις και τέσσερις δεκαετίες πριν (RSA 1977, Diffie–Hellman 1976, ECDSA 1992). Συνεπάγεται λοιπόν, πως είναι κρίσιμο στην περίπτωση αυτή, να λειτουργήσει η επιστημονική κοινότητα προληπτικά και όχι θεραπευτικά. Χρειάζεται να υπάρχουν έτοιμες, δοκιμασμένες λύσεις αλγορίθμων ανθεκτικών στη νέα πραγματικότητα που θα εισάγουν οι κβαντικοί υπολογιστές (quantum resistant algorithms). Για τον λόγο αυτό, διεξάγονται μελέτες και έχουν ήδη προταθεί λύσεις ώστε να αντιμετωπίσουν τον επερχόμενο αυτό κίνδυνο για την κρυπτογραφία γενικότερα αλλά και ειδικά για τις blockchains κρυπτονομισμάτων των οποίων αποτελούν δομικό στοιχείο.

Συγκεκριμένα, ο Αμερικανικός οργανισμός National Institute of Standards and Technology (NIST) ξεκίνησε το 2016 μια διαδικασία αναζήτησης και αξιολόγησης κρυπτογραφικών αλγορίθμων ανθεκτικών στην κβαντική εποχή. Τελικός σκοπός αυτής της διαδικασίας θα είναι η δημιουργία τυποποίησης (Standardization) ώστε να είναι δυνατή η δημιουργία νέων κρυπτογραφικών συστημάτων, εν είδη καθολικά αποδεκτών προτύπων, τα οποία θα είναι ανθεκτικά και ασφαλή σε επιθέσεις κβαντικών αλλά και κλασικών υπολογιστικών συστημάτων. Θα παρέχουν έτσι ασφαλή υποδομή για μελλοντικές απειλές από τους κβαντικούς υπολογιστές αλλά ταυτόχρονα θα είναι και

συμβατά με τα υπάρχοντα δίκτυα και πρωτόκολλα επικοινωνίας (NIST 2017a:1). Η διαδικασία, την στιγμή της συγγραφής της παρούσας μεταπτυχιακής διατριβής, βρίσκεται στον δεύτερο γύρο, όπου έχουν προκριθεί 26 υποψήφιοι αλγόριθμοι από τους 69 που υποβλήθηκαν στον πρώτο γύρο, μετά από μια σειρά δοκιμών κι ελέγχων. Μέσα στο 2020 ή το 2021, θα ολοκληρωθεί και ο δεύτερος γύρων ελέγχων και δοκιμών και θα ανακοινωθούν οι αλγόριθμοι που θα προκριθούν στον τρίτο και τελευταίο γύρο αξιολόγησης. Αναμένεται μέσα στο 2022 – 2024 να ανακοινωθεί ο τελικός κρυπτογραφικός αλγόριθμος που θα χρησιμοποιηθεί ως μετα-κβαντικό πρότυπο (post-quantum standard) (NIST 2017b:1).

Τα κριτήρια αξιολόγησης των υποψηφίων αλγορίθμων είναι:

1. Η ασφάλεια. Αναμφίβολα πρόκειται για το σημαντικότερο κριτήριο που πρέπει να πληροί ένας αλγόριθμος, αφού ο NIST σκοπεύει να τον χρίσει ως πρότυπο για πολλά πρωτόκολλα δικτύων όπως τα Transport Layer Security (TLS), Secure Shell (SSH), Internet Protocol Security (IPSec), Internet Key Exchange (IKE) και Domain Name System Security Extensions (DNSSEC). Στον βαθμό ασφαλείας κάθε αλγορίθμου θα συνυπολογιστούν και άλλα χαρακτηριστικά ασφαλείας όπως η ανθεκτικότητα σε γνωστές επιθέσεις (chosen cyphertext, chosen plaintext, chosen message, side-channel, multi-key, κ.α.) (Alagic et al 2019:4).
2. Το κόστος. Πρόκειται για τις απαιτήσεις σε μνήμη και υπολογιστική ισχύ που έχει ο αλγόριθμος, καθώς και μεγέθη και χρόνους υλοποίησης ψηφιακών υπογραφών, κρυπτοκειμένων και κλειδιών κρυπτογράφησης ανάλογα με την κατηγορία στην οποία ανήκει (Alagic et al 2019:5).
3. Χαρακτηριστικά σχεδιασμού και υλοποίησης. Αξιολογούνται σχεδιαστικές καινοτομίες και ευελιξία του κάθε αλγορίθμου ώστε να μπορεί να χρησιμοποιηθεί με αξιοπιστία και χωρίς να στερεί σε επιδόσεις σε πληθώρα πρωτοκόλλων (Alagic et al 2019:5).

Όλοι οι υποψήφιοι αλγόριθμοι, αποτελούν υλοποιήσεις των πέντε βασικών κατηγοριών – οικογενειών κρυπτογραφικών αλγορίθμων που χάρη στις ιδιότητές τους θεωρούνται ανθεκτικές σε επιθέσεις από κβαντικούς υπολογιστές κι επομένως θα μπορούσαν να βρουν εφαρμογή σε τεχνολογίες blockchain. Κάθε μία από τις κατηγορίες αυτές, εμφανίζει πλεονεκτήματα αλλά και μειονεκτήματα στις υλοποιήσεις της όπως θα δούμε και παρακάτω.

4.1 Κρυπτογραφία Πλέγματος

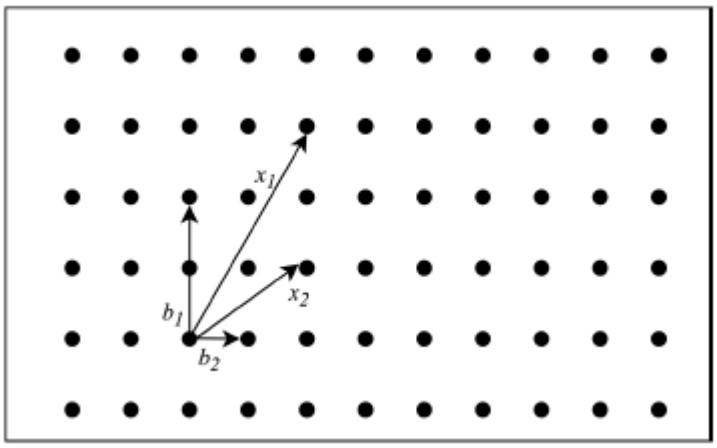
Οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται σήμερα βασίζουν την ασφάλειά τους σε αλγεβρικά προβλήματα. Παρόλα αυτά, υπάρχει μια κατηγορία κρυπτογραφικών αλγορίθμων που στηρίζονται σε γεωμετρικά προβλήματα. Οι αλγόριθμοι αυτοί καλούνται αλγόριθμοι πλέγματος (lattice-based algorithms) και έχουν θέσει ισχυρή υποψηφιότητα να αποτελέσουν την βάση πάνω στην οποία θα δομηθούν ανθεκτικοί αλγόριθμοι στην μετα-κβαντική εποχή.

Με απλά λόγια, lattice καλείται ένα πολλών διαστάσεων γεωμετρικό πλέγμα ομοιόμορφα τοποθετημένων σημείων, το οποίο εκτείνεται προς όλες τις διευθύνσεις στο άπειρο (Pradhan et al 2019:2). Ο μαθηματικός ορισμός ενός lattice *L*, αναφέρει πως πρόκειται για σύνολο άπειρων διακριτών σημείων τοποθετημένα σε Ευκλείδειο χώρο n-διαστάσεων με περιοδική δομή. Ως βάση *B* του lattice ορίζονται τα γραμμικά ανεξάρτητα n-διανύσματα b_1, b_2,..., b_n έτσι ώστε *B* = [b_1, b_2,..., b_n]. Από κάθε βάση *B*, μπορούμε να κατασκευάσουμε ολόκληρο το lattice, παίρνοντας όλους τους δυνατούς γραμμικούς συνδυασμούς ακέραιων αριθμών που παράγονται από αυτή. Ισχύει δηλαδή πως:

$$\mathcal{L}(B) = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}, 1 \leq i \leq n \right\}$$

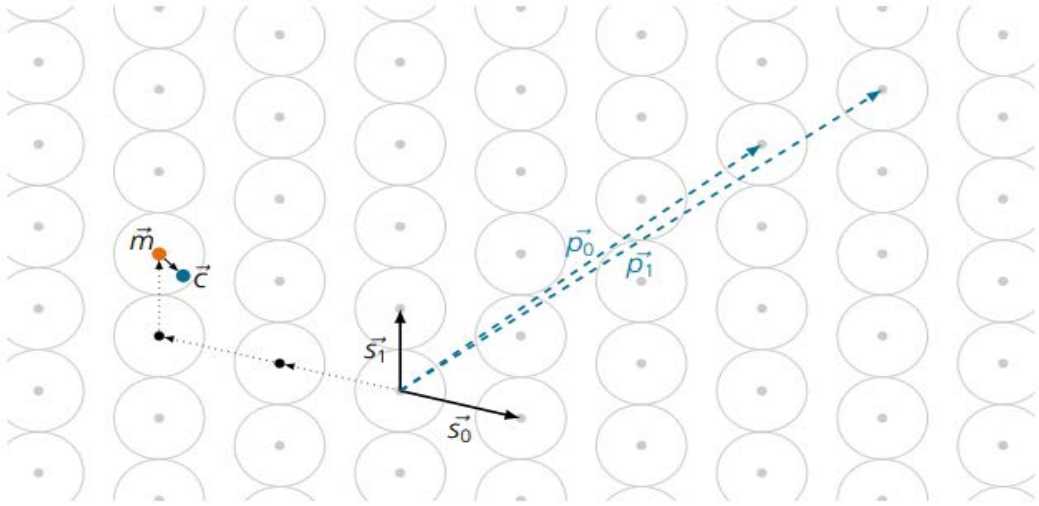
Τύπος 1. Μαθηματικός ορισμός ενός Lattice (Nejatollahi et al 2019:129:3)

Σε κάθε lattice *L*, μπορούν να ορισθούν πολλές βάσεις *B*. Για παράδειγμα, σε ένα lattice *L*, δύο (2) διαστάσεων, ορίζουμε δύο βάσεις *B* = [b_1, b_2] και *X* = [x_1, x_2]. Η βάση *B* καλείται «καλή» (με την έννοια της ορθής, της ελάχιστου μεγέθους βάσης που μπορεί να χρησιμοποιηθεί για την κατασκευή ολόκληρου του *L*, well-formed) βάση, ενώ η *X* «κακή» (scrambled, κατά κανόνα έχει μεγαλύτερο μέγεθος από μια well-formed βάση).



Εικόνα 7. Καλά σχηματισμένη [b1,b2] και όχι-καλά σχηματισμένη βάση [x1,x2] σε ένα Lattice

Σύμφωνα με τα παραπάνω, υλοποιείται κρυπτοσύστημα δημοσίου κλειδιού βασισμένο σε lattice. Σε ένα lattice *L* πολλών διαστάσεων, ο παραλήπτης χρησιμοποιεί ως ιδιωτικό κλειδί κρυπτογράφησης μια well-formed βάση s = {s_0, s_1} του *L* ενώ ως δημόσιο κλειδί μια scrambled βάση p = {p_0, p_1} του *L*. Ένας αποστολέας που θέλει να στείλει μήνυμα *m* στον παραλήπτη, θα χρησιμοποιήσει το *p* ώστε να ορίσει την θέση του *m* μέσα στο lattice *L*. Στην συνέχεια, προσθέτει τυχαίο σφάλμα στο *m*, με τέτοιο τρόπο ώστε το νέο σημείο *c* (cipher point) του *L* που προκύπτει, να είναι το πλησιέστερο σημείο στο *m* από οποιοδήποτε άλλο σημείο σε ολόκληρο το lattice. Το σημείο *c* αποστέλλεται τελικά στον παραλήπτη, ο οποίος έχοντας στην κατοχή του την καλά διαμορφωμένη βάση *s* (private key) του *L*, μπορεί εύκολα να υπολογίσει το *m* ως το πλησιέστερο σημείο του *c* κι έτσι να λάβει το αρχικό μήνυμα. Ακριβώς εδώ είναι που κρύβεται και η πραγματική δύναμη των lattices σε ό,τι αφορά την ασφάλεια σε ένα κρυπτοσύστημα που βασίζεται σε αυτά. Σε ένα lattice πολλών διαστάσεων, είναι πολύ δύσκολο να υπολογιστεί το πλησιέστερο σημείο ως προς ένα άλλο σημείο του το οποίο είναι γνωστό, όταν κάποιος έχει στην κατοχή του μια μη καλά διαμορφωμένη (not well-formed) βάση του. Το πρόβλημα αυτό καλείται Closest Vector Problem (CVP). Επιπλέον, είναι εξίσου δύσκολο να συνάγει κάποιος μια καλά διαμορφωμένη βάση σε ένα lattice, από μια μη καλά διαμορφωμένη και αυτό καλείται Shortest Vector Problem (SVP). Τα δύο αυτά προβλήματα, θεωρούνται υπολογιστικά δύσκολα ακόμα και για κβαντικούς υπολογιστές (Niederhagen and Waidner, Prof. Dr. Michael 2017:12).



Εικόνα 8. Παράδειγμα κρυπτογραφίας σε Lattice δύο διαστάσεων

Η επιστημονική κοινότητα θεωρεί πως η lattice-based κρυπτογραφία είναι πολλά υποσχόμενη καθώς μπορεί να οδηγήσει σε πλήρως ομομορφική κρυπτογράφηση (fully homomorphic encryption), δηλαδή στην δυνατότητα εφαρμογής διαδικασιών πάνω σε κρυπτογραφημένα δεδομένα χωρίς να μπορούν αυτές (ή να χρειάζεται) να τα αποκρυπτογραφήσουν πρώτα (Gentry 2009:169). Επιπλέον, έχουν προταθεί σχήματα βασισμένα σε lattices τα οποία εκτελούν «συσκότιση» κώδικα (code obfuscation) (Cheng and Zhang 2015:1648, Boneh et al 2017:247).

4.1.1 Εκμάθηση με χρήση Σφαλμάτων

Παραλλαγές κρυπτογραφικών σχημάτων πλέγματος, χρησιμοποιούν το πρόβλημα της «Εκμάθησης με χρήση Σφαλμάτων» (Learning With Errors, LWE). Το LWE συσχετίζεται με την θεωρία κωδίκων κι έχει ως ελάχιστη ασφάλεια ίση με παραλλαγές του SVP (Niederhagen and Waidner, Prof. Dr. Michael 2017:12). Πρόκειται για ένα πρόβλημα που συνδυάζει δύο επιστημονικούς τομείς, της εκμάθησης μηχανών (machine learning) εφαρμοσμένης στην κρυπτογραφία (Easttom 2019:0812) και θεωρείται πολύ δύσκολο στην επίλυσή του ακόμα και από κβαντικούς υπολογιστές. Χρησιμοποιείται σε σχήματα κρυπτογραφίας δημοσίου κλειδιού και – θέτοντάς το απλουστευμένα – αφορά στην δυσκολία εύρεσης του ιδιωτικού κλειδιού s στον τύπο $A\ s + e \bmod q$, όπου A πίνακας τυχαία επιλεγμένων τιμών από το Lattice, e πίνακας τιμών «σφαλμάτων» και q πρώτος αριθμός (Nejatollahi et al 2019:129:4-129:5). Γνωστές και με πολλές υλοποιήσεις είναι επίσης και οι παραλλαγές του LWE με χρήση δακτυλίων (Ring-LWE) και Module-LWE (MLWE).

4.1.2 Παραδείγματα – Υλοποιήσεις αλγορίθμων

Πολλά είναι τα σχήματα βασισμένα σε lattices που έχουν προταθεί για την εφαρμογή τους στην κρυπτογραφία δημοσίου κλειδιού (public key encryption, PKE) και στον μηχανισμό ανταλλαγής κλειδιών (Key Exchange Mechanism, KEM) στην μετα-κβαντική εποχή. Τα πιο σημαντικά από αυτά που μάλιστα έχουν προκριθεί στον δεύτερο γύρο αξιολόγησης του NIST, είναι:

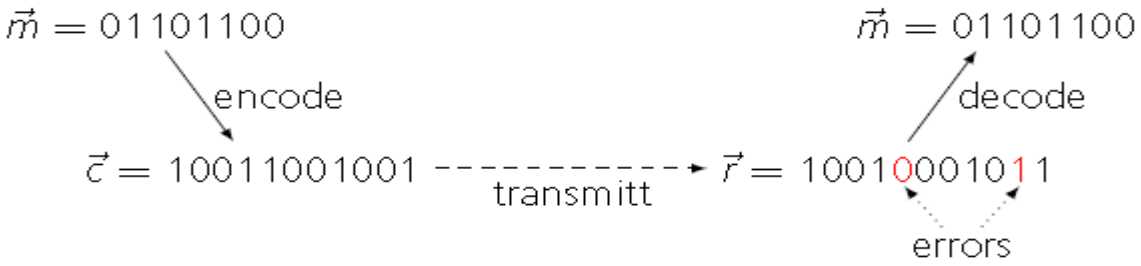
- NTRU (Alagic et al 2019:8). Πρόκειται για το πιο δημοφιλές κρυπτογραφικό σχήμα δημοσίου κλειδιού βασισμένο σε lattices και προήλθε από την συνένωση δύο προϋπαρχόντων σχημάτων των NTRUEncypt και NTRU-HRSS-KEM. Είναι ταχύτερο από τα υπάρχοντα κρυπτοσυστήματα, αλλά παράγει δημόσια κλειδιά μεγαλύτερου μεγέθους από αυτά του RSA (Campagna et al 2014:18).
- NewHope (Alagic et al 2019:8). Μηχανισμός ανταλλαγής κλειδιού βασισμένος στο πρόβλημα του Ring Learning with Errors, με χρήση εφήμερων δημοσίων κλειδιών και δύο γύρους για την συμφωνία κλειδιών (key agreement) (Niederhagen and Waidner, Prof. Dr. Michael 2017:13).
- NTRU Prime (Alagic et al 2019:9). Σχήμα PKE, ως παραλλαγή του NTRU με χρήση Ring-LWE.
- Round5 (Alagic et al 2019:9). Σχήμα για PKE αλλά και KEM, αφού προήλθε ως συνένωση των αλγορίθμων Round2 και Hila5 και χρησιμοποιεί το πρόβλημα LWE.
- CRYSTALS-KYBER, ως KEM (Alagic et al 2019:7)
- FrodoKEM, ως KEM (Alagic et al 2019:7)
- LAC, ως PKE (Alagic et al 2019:7)
- SABER ως PKE και KEM βασισμένο στο MLWE (Alagic et al 2019:10)
- Three Bears, ως KME (Alagic et al 2019:10)

Τέλος, lattice-based σχήματα έχουν προταθεί και στον τομέα των ψηφιακών υπογραφών και ανήκουν είτε στην κατηγορία κατακερματισμού-και-υπογραφής (hash-and-sign) είτε στις υπογραφές Fiat-Shamir (Nejatollahi et al 2019:129:13):

- CRYSTALS-DILITHIUM (Alagic et al 2019:14), που βασίζει την ανθεκτικότητά του στο πρόβλημα του MLWE κι έχει κατασκευαστεί με την χρήση του ευρετικού (heuristic) των Fiat-Shamir.
- FALCON (Alagic et al 2019:14–15), βασισμένο σε lattice του NTRU αλλά με δειγματοληψία του Gauss.
- qTESLA (Alagic et al 2019:15), βασισμένο στο RLWE.

4.2 Κρυπτογραφία με χρήση αλγορίθμων βασισμένους σε Κώδικες

Οι βασισμένοι σε κώδικα (code-based) κρυπτογραφικοί αλγόριθμοι, βασίζουν τον τρόπο λειτουργίας τους στην τεχνική που ακολουθείται για την διόρθωση σφαλμάτων (error-correction) κατά την μετάδοση πληροφορίας σε μη αξιόπιστο κανάλι. Σύμφωνα με αυτή την τεχνική, χρησιμοποιούνται ειδικοί κώδικες αποσφαλμάτωσης (error-correction codes) οι οποίοι μπορούν να εντοπίσουν και να διορθώσουν ορισμένο αριθμό *t* bits από σφάλματα κατά την μετάδοση.



Εικόνα 9. Παράδειγμα αποσφαλμάτωσης σε μη-αξιόπιστο κανάλι επικοινωνίας

Παρόμοιοι κώδικες εφαρμόζονται προκειμένου να αποκρύψουν το περιεχόμενο της μετάδοσης σε μια υλοποίηση κρυπτογράφησης δημοσίου κλειδιού. Στην περίπτωση αυτή, το κανάλι μετάδοσης θεωρείται αξιόπιστο και τα δεδομένα αλλοιώνονται σκόπιμα προκειμένου να προστατευτεί το περιεχόμενό τους. Ένα παράδειγμα τέτοιου κώδικα είναι οι κώδικες Goppa (Goppa codes), οι οποίοι εάν χρησιμοποιηθούν με τέτοιο τρόπο ώστε οι συναρτήσεις κωδικοποίησης και αποκωδικοποίησης να μείνουν κρυφοί, μπορούν να μετατραπούν σε ένα πολύ ασφαλές σχήμα κωδικοποίησης. Στην περίπτωση αυτή, θα δημοσιεύεται μόνο μια παραλλαγμένη συνάρτηση κωδικοποίησης μέσω της οποίας θα γίνεται αντιστοίχιση του αρχικού μηνύματος με ένα σύνολο ανακατεμένων κωδικολέξεων, ενώ η αποκωδικοποίηση θα μπορεί να γίνει μόνο από τους κατόχους της κρυφής συνάρτησης αποκωδικοποίησης. Η διαδικασία αυτή, βασίζεται στο μαθηματικό πρόβλημα που καλείται «Αποκωδικοποίηση βάσει συνδρόμου» (syndrome decoding), θεωρείται NP-Hard πρόβλημα όταν ο κώδικας είναι «τυχαίος» (δηλαδή όταν δεν έχει κάποια προσεγμένα επιλεγμένη δομή που να επιτρέπει την αποκωδικοποίηση) και είναι υπολογιστικά δύσκολο να αντιστραφεί από κλασικούς αλλά ακόμα και από κβαντικούς υπολογιστές (Campagna et al 2014:17).

4.2.1 Κρυπτοσύστημα βασισμένο σε κώδικα του McEliece

Το πρώτο κρυπτοσύστημα δημοσίου κλειδιού βασισμένο σε τέτοιους κώδικες, παρουσιάστηκε από τον Robert McEliece (21 Μαΐου 1942 – 8 Μαΐου 2019) το 1978 (McEliece 1978:114). Σύμφωνα με αυτό, προσθέτουμε εσκεμμένα σφάλματα στα δεδομένα προς μετάδοση ώστε να γίνουν ακατάληπτα προς όποιον προσπαθήσει να τα υποκλέψει. Για παράδειγμα, έστω πως θέλουμε να αποστείλουμε το μήνυμα m. Αρχικά, κωδικοποιούμε το m παίρνοντας το κωδικοποιημένο μήνυμα c, με τέτοιο τρόπο ώστε το c να είναι μεγαλύτερο από το m. Έτσι, υπάρχουν πλεονάζοντα bits που εξυπηρετούν στην ανίχνευση ή/και στην διόρθωση σφαλμάτων κατά την μετάδοση. Πριν την μετάδοσή του c, κάποια bits του αλλάζουν αφού σε αυτά προστίθεται (XOR) το μήνυμα e το οποίο αποτελείται από τα bits ελέγχου που θα εισάγουν το σφάλμα στο προς μετάδοση c. Το e έχει συγκεκριμένο και ορισμένο από πριν αριθμό bits που ισούνται με 1 και αυτό καλείται βάρος w. Ο παραλήπτης του μηνύματος με αυτό τον τρόπο λαμβάνει ένα νέο και διαφορετικό μήνυμα $r = c \oplus e$. Στη συνέχεια, προσπαθεί να αντιστοιχίσει το ληφθέν r στην πλησιέστερη του κωδικολέξη c' κι έπειτα αφαιρεί το σφάλμα από αυτή. Στην περίπτωση που το βάρος w του e που εισάχθηκε πριν είναι μικρότερο ή ίσο από τον αριθμό t των σφαλμάτων που μπορούν να διορθωθούν ($w \leq t$), τότε το $c' = c$. Τέλος, ο παραλήπτης εφαρμόζει την συνάρτηση αποκωδικοποίησης για να λάβει το αρχικό μήνυμα m. Στην περίπτωση δε, που $w > t$, τότε ο παραλήπτης δεν μπορεί να συμπεράνει το c κι έτσι η αποκωδικοποίηση του c' αποτυγχάνει.

Η δυναμική της παραπάνω διαδικασίας σε ότι αφορά την ασφάλεια, πηγάζει από την δυσκολία της αποκωδικοποίησης μιας τέτοιας τυχαίας συμβολοσειράς, δηλαδή μιας κωδικής λέξης που έχει προκύψει από «τυχαίο» κώδικα ο οποίος και δεν επιτρέπει την αποκωδικοποίησή της. Οι μόνοι γνωστοί αλγόριθμοι αποκωδικοποίησης μέχρι σήμερα χρειάζονται χρόνο εκθετικά αυξανόμενο βάση των ρυθμιζόμενων παραμέτρων της διαδικασίας. Αυτό, τους κάνει ανθεκτικούς ακόμα και στην περίπτωση της χρήσης τους από κβαντικούς υπολογιστές.

Στο κρυπτοσύστημα δημοσίου κλειδιού του McEliece, το δημόσιο κλειδί του παραλήπτη είναι μια μήτρα γεννήτορας (generator matrix) G_{pub}. Ο αποστολέας έτσι το χρησιμοποιεί για να κρυπτογραφήσει το μήνυμα m που θέλει να στείλει και στο αποτέλεσμα προσθέτει (XOR) το σφάλμα e. Έτσι παράγεται το αλλοιωμένο μήνυμα $c = mG_{pub} \oplus e$ από το οποίο ο παραλήπτης θα εξάγει το αρχικό μήνυμα m. Το δημόσιο κλειδί G_{pub} είναι ορισμένο και

δομημένο με τέτοιο τρόπο ώστε να πετυχαίνει τον διττό του στόχο.
(α) Να παρουσιάζει τυχαία κατανομή των δεδομένων ώστε να μην δίνει καμία πληροφορία στον επιτιθέμενο για το ποιον αλγόριθμο αποκωδικοποίησης θα πρέπει να εφαρμόσει στο αλλοιωμένο μήνυμα *c* ώστε να εξάγει το αρχικό μήνυμα *m*.
(β) Να επιτρέπει στον κάτοχο του ιδιωτικού κλειδιού να αποκωδικοποιεί μηνύματα που έχουν κωδικοποιηθεί με την χρήση του δικού του δημόσιου κλειδιού G_{pub}.

Το κρυπτοσύστημα, δεν χρησιμοποιείται πλέον στην πρωταρχική του μορφή μιας και είναι μη-ασφαλές με τις αρχικές του παραμέτρους. Παρόλα αυτά, δεν έχει παραβιαστεί δομικά και με τη χρήση διαφορετικών παραμέτρων (πχ με χρήση δυαδικών κωδικών Goppa) θεωρείται ασφαλές κι έτσι αποτελεί υποψήφιο για την υιοθέτησή του σε κρυπτογραφικές λύσεις σε τεχνολογίες blockchain στην μετα-κβαντική εποχή. Το μόνο ισχυρό του μειονέκτημα είναι το μέγεθος των κλειδιών που φτάνουν ακόμα και τα 4MB. Μια παραλλαγή του κρυπτοσυστήματος του McEliece που έρχεται να βελτιώσει τον τομέα αυτό είναι το κρυπτοσύστημα του Niederreiter (Niederhagen and Waidner, Prof. Dr. Michael 2017:11).

4.2.2 Κρυπτοσύστημα βασισμένο σε κώδικα του Niederreiter

Στο κρυπτοσύστημα του Niederreiter, δεν εισάγεται τυχαίος κωδικός σφάλματος *e* όπως σε αυτό του McEliece. Αντίθετα, ολόκληρο το μήνυμα προς μετάδοση, κωδικοποιείται σαν σφάλμα δηλαδή σε μια σειρά bits βάρους *w*. Τη θέση του δημόσιου κλειδιού λαμβάνει μία μήτρα ελέγχου parity-bit (parity check matrix) H_{pub}. Σε μία ανταλλαγή μηνυμάτων λοιπόν, ο αποστολέας υπολογίζει και στέλνει το $s = H_{pub}\, e^w$ και ο παραλήπτης χρησιμοποιώντας κατάλληλο αλγόριθμο αποκωδικοποίησης υπολογίζει το *e*. Όπως στο κρυπτοσύστημα McEliece, έτσι και σε αυτό του Niederreiter, ο πίνακας ελέγχου ισοτιμίας (parity check matrix) H_{pub} πρέπει να είναι δομημένος με τρόπο που να παρουσιάζεται ως τυχαίος έτσι ώστε να μην φανερώνει καμία ιδιότητα του στον επιτιθέμενο. Το κρυπτοσύστημα του Niederreiter καταφέρνει με αυτό τον τρόπο να μειώσει το μέγεθος του δημοσίου κλειδιού στο 1MB περίπου, που ακόμα όμως θεωρείται ιδιαίτερα μεγάλο.

Η κρυπτογραφική κοινότητα είναι ιδιαίτερα αισιόδοξη σε ότι αφορά τους code-based αλγορίθμους και τον ρόλο που θα παίξουν σε μελλοντικά πρότυπα κρυπτογραφίας ειδικά σε ότι αφορά την ανθεκτικότητά τους σε επιθέσεις από κβαντικούς υπολογιστές. Το μεγάλο μέγεθος του δημοσίου κλειδιού παραμένει το κύριο πρόβλημά τους – ειδικά αν το

φανταστούμε σε υλοποίηση μιας blockchain αφού θα αυξάνει το μέγεθος κάθε block κι επομένως ολόκληρης της blockchain σε τεράστια μεγέθη. Για τον λόγο αυτό, έχουν γίνει προσπάθειες κυρίως μέσω τεχνικών συμπίεσης ώστε να μειωθεί το μέγεθος του δημοσίου κλειδιού σε αυτό το είδος των αλγορίθμων. Σε πολλές περιπτώσεις όμως το αποτέλεσμα εμφάνισε τρωτότητα από επιθέσεις κλασικών υπολογιστών κι έτσι οι λύσεις αυτές απορρίφθηκαν (Nejatollahi et al 2019:11).

4.2.3 Παραδείγματα – Υλοποιήσεις αλγορίθμων

Σχήματα κρυπτογραφικών συστημάτων βασισμένα σε κώδικα, έχουν επίσης υλοποιηθεί και προταθεί στον NIST. Όσα προκριθεί στον δεύτερο γύρο αξιολόγησης, αφορούν σχήματα κρυπτογραφίας δημοσίου κλειδιού (PKE) και ανταλλαγής κλειδιών (KEM):

- Classic McEliece ως KEM. Πρόκειται για το κρυπτοσύστημα που είδαμε παραπάνω και βασίζεται σε τυχαίο δυαδικό κώδικα Goppa και στην υπόθεση πως αυτός δεν μπορεί να διαχωριστεί από έναν τυχαίο γραμμικό κώδικα. Παράγει πολύ μικρά κρυπτοκείμενα (ciphertexts) της τάξης των 200bytes, έχει καλούς χρόνους εκτέλεσης ενθυλάκωσης και αποθυλάκωσης, ενώ όπως είδαμε το μειονέκτημα του είναι τα πολύ μεγάλα δημόσια κλειδιά (Alagic et al 2019:10–11).
- BIKE ως KEM (Alagic et al 2019:11–12).
- HQC ως PKE (Alagic et al 2019:12).
- LEDAcrypt που προήλθε από την συνένωση δύο παρόμοιων code-based σχημάτων των LEDAkem και LEDApkc (Alagic et al 2019:12).
- NTS-KEM ως KEM, που βασίζει την λειτουργία του στον classic McEliece με ελάχιστες διαφορές, όπως του ότι παράγει τα κλειδιά του με διαφορετικό τρόπο (Alagic et al 2019:11).
- ROLLO ως συνένωση τριών υποψηφίων του πρώτου γύρου αξιολόγησης του NIST και συγκεκριμένα των LAKE, LOCKER και Ouroboros-R (Alagic et al 2019:13).
- RQC ως PKE (Alagic et al 2019:13–14).

4.3 Κρυπτογραφία με Χρήση Πολυωνύμων Πολλαπλών Μεταβλητών

Τα πολυώνυμα πολλαπλών μεταβλητών (Multivariate Polynomial) σε πεπερασμένο σώμα, αποτελούν την βάση για μια ακόμη μέθοδο κρυπτογραφίας εφαρμοσμένη σε λύσεις δημοσίου κλειδιού αλλά και ψηφιακών υπογραφών. Για την λύση ενός τέτοιου συστήματος πολυωνύμων, χρησιμοποιείται η μέθοδος υπολογισμού της βάσης Gröbner

(Buchmann et al 2004:13). Το πρόβλημα αυτό καλείται MQ (MQ problem) και απαιτείται μη-ντετερμινιστικός πολυώνυμος χρόνος (Nondeterministic Polynomial Hard – NP Hard problem) για την επίλυσή του. Αυτό αποτελεί και το συστατικό που το κάνει κατάλληλο για την χρησιμοποίησή του στην κρυπτογραφία (Yasuda et al 2015:105). Στην εικόνα που ακολουθεί, παρουσιάζεται παράδειγμα ενός απλού τέτοιου συστήματος τεσσάρων εξισώσεων με τέσσερις μεταβλητές x_0, x_1, x_2, x_3 (Niederhagen and Waidner, Prof. Dr. Michael 2017:16).

$$x_0x_3 + x_2x_3 + x_0 + 1 = 0$$
$$x_0x_1 + x_2x_3 + x_2 + 1 = 0$$
$$x_0x_1 + x_0x_3 + x_0 + x_1 + 1 = 0$$
$$x_1x_2 + x_2x_3 + x_3 = 0$$

Εικόνα 10. Παράδειγμα συστήματος τεσσάρων εξισώσεων με τέσσερις μεταβλητές

Η λειτουργία ενός τέτοιου συστήματος τόσο στην κρυπτογράφηση όσο και στις ψηφιακές υπογραφές περιγράφεται ως εξής(Yasuda et al 2015:105):

- Αρχικά, χρειάζεται ένας χάρτης πολυώνυμου συστήματος πολλαπλών μεταβλητών (multivariate polynomial map). Το επιλεγμένο σύστημα πρέπει να είναι τέτοιο ώστε να μπορεί να υπολογιστεί εύκολα ο αντίστροφος χάρτης του (inverse map).
- Ο αντίστροφος αυτός χάρτης, καλείται κεντρικός χάρτης (central map). Ορίζεται central map $G : K^n \rightarrow K^m$ (που αποτελείται από m πολυώνυμα σε n μεταβλητές).
- Ορίζεται multivariate polynomial map $F : K^n \rightarrow K^m$ τέτοιος ώστε $F = L \circ G \circ R$, όπου L και R είναι συγγενείς μετασχηματισμοί στα K^m και K^n αντίστοιχα.
- Ο χάρτης F, παίζει το ρόλο της μονόδρομης συνάρτησης κι έτσι γίνεται το δημόσιο κλειδί
- Το ιδιωτικό κλειδί, αποτελείται από τα G, L και R όπως αυτά ορίσθηκαν παραπάνω.

Στην περίπτωση της κρυπτογράφησης, οι G και F πρέπει να είναι σχεδόν ένα-προς-ένα (injective), δηλαδή να έχουν περισσότερα πολυώνυμα από ότι μεταβλητές, άρα $m \geq n$. Έστω αποστολέας έχει μήνυμα M προς κρυπτογράφηση. Υπολογίζει το κρυπτοκείμενο ως $C = F(M) \in K^m$. Ο Παραλήπτης προκειμένου να λάβει το αρχικό κείμενο M, υπολογίζει με την σειρά τα: $E_1 = L^{-1}(C)$, στη συνέχεια $E_2 = G^{-1}(E_1)$ και τέλος $E = R^{-1}(E_2)$. Το E, είναι το

M που έστειλε ο αποστολέας (Yasuda et al 2015:105–106). Παραδείγματα τέτοιων σχημάτων κρυπτογράφησης βασισμένα σε multivariate polynomials δεν υπάρχουν πολλά που να θεωρούνται ασφαλή. Ένα από αυτά είναι το PMI-plus το οποίο θεωρείται ασφαλές, αλλά επειδή είναι αρκετά νέο, υπάρχει συγκρατημένη αισιοδοξία μέχρι να δοκιμαστεί σε βάθος χρόνου (Niederhagen and Waidner, Prof. Dr. Michael 2017:17).

Στην περίπτωση της ψηφιακής υπογραφής, οι *G* και *F* πρέπει να είναι επιρριπτικοί (surjective), με $m \leq n$. Έστω μήνυμα *M* προς υπογραφή. Ο αποστολέας υπολογίζει με την σειρά τα: M' = hash(M), $S_1 = L^{-1}(M')$, $S_2 = G^{-1}(S_1)$ και τέλος $S = R^{-1}(S_2)$. Το *S*, είναι και η ψηφιακή υπογραφή του *M*. Ο παραλήπτης, υπολογίζει το $F(S) \in K^m$ (όπου *F* είναι το public key του αποστολέας) και εάν $F(S)$ = hash(M), τότε θεωρεί πως η υπογραφή είναι έγκυρη.

Σε ό,τι αφορά την ασφάλεια των παραπάνω συστημάτων, ένας επιτιθέμενος θα πρέπει να μπορεί να υπολογίσει *X* τέτοιο ώστε $F(X) = C$ (για το μοντέλο της κρυπτογράφησης) ή $F(X) = M$ (για το μοντέλο της ψηφιακής υπογραφής) προκειμένου να τα μπορέσει να αντιστρέψει τον *F* και να εκθέσει το αντίστοιχο σύστημα. Εδώ όμως είναι το σημαντικό πλεονέκτημα των συστημάτων αυτών αφού το συγκεκριμένο πρόβλημα είναι NP-Hard για τους κλασικούς υπολογιστές κι επιπλέον δεν έχει βρεθεί ακόμα κάποιος αλγόριθμος ο οποίος να είναι ταχύτερος σε κβαντικό υπολογιστή και να το επιλύει. Επιπλέον, σε ότι αφορά τις ψηφιακές υπογραφές, ένα κρυπτοσύστημα multivariate polynomials απαιτείται να έχει τουλάχιστον 200-256 μεταβλητές για να θεωρηθεί κβαντο-ανθεκτικό, οπότε και παράγει μέγεθος δημοσίου κλειδιού 500kB με 1MB. Ταυτόχρονα, το μέγεθος των υπογραφών που παράγεται, είναι αρκετά μικρότερο από άλλες προτεινόμενες κβαντοανθεκτικές λύσεις κάνοντας τα πολυώνυμα πολλαπλών μεταβλητών έναν ισχυρό υποψήφιο για εφαρμογή στην μετα-κβαντική κρυπτογραφία και λύσεις σε τεχνολογίες blockchain (Niederhagen and Waidner, Prof. Dr. Michael 2017:17) [11, p. 105].

4.3.1 Παραδείγματα – Υλοποιήσεις αλγορίθμων

Αντίθετα με τους code-based αλγορίθμους, οι multivariate έχουν παρουσιάσει μόνο σχήματα για ψηφιακές υπογραφές που έχουν περάσει στον δεύτερο γύρο αξιολόγησης του NIST:

- Rainbow. Πρόκειται για γενίκευση του σχήματος Unbalanced Oil and Vinegar (UOV) το οποίο αποτελεί αντικείμενο μελέτης για πάνω από είκοσι χρόνια στην κρυπτογραφία πολυωνύμων. Το Rainbow μελετάται για περίπου δεκαπέντε

χρόνια με διάφορες παραμετροποιήσεις ακόμα και σε εφαρμογές «ελαφρού» τύπου (lightweight) (Alagic et al 2019:16–17). Είναι πιο αποτελεσματικός από το UOV παρουσιάζοντας μικρότερα μεγέθη υπογραφών και κρυπτογραφικών κλειδιών, ενώ αυτά μπορούν να μειωθούν περαιτέρω εάν χρησιμοποιηθεί περισσότερος χρόνος για την δημιουργία του ζεύγους κλειδιών (Campagna et al 2014:20).

- GeMSS. Ανήκει στην οικογένεια Hidden Field Equations (HFEv-) που αποτελεί ένα από τα πιο πολυμελετημένα μοντέλα υπογραφών. Παρουσιάζει πολύ μικρό μέγεθος υπογραφών και χρόνους επαλήθευσής τους, όμως το μέγεθος των δημοσίων κλειδιών και ο χρόνος για την υπογραφή είναι αρκετά υψηλά (Alagic et al 2019:15).
- LUOV, το οποίο βασίζεται κι αυτό στο σχήμα UOV και παρουσιάζει το μικρότερο μέγεθος αθροίσματος του δημοσίου κλειδιού και του μήκους της υπογραφής από τους άλλους multivariate αλγορίθμους (Alagic et al 2019:16).
- MQDSS (Alagic et al 2019:16)

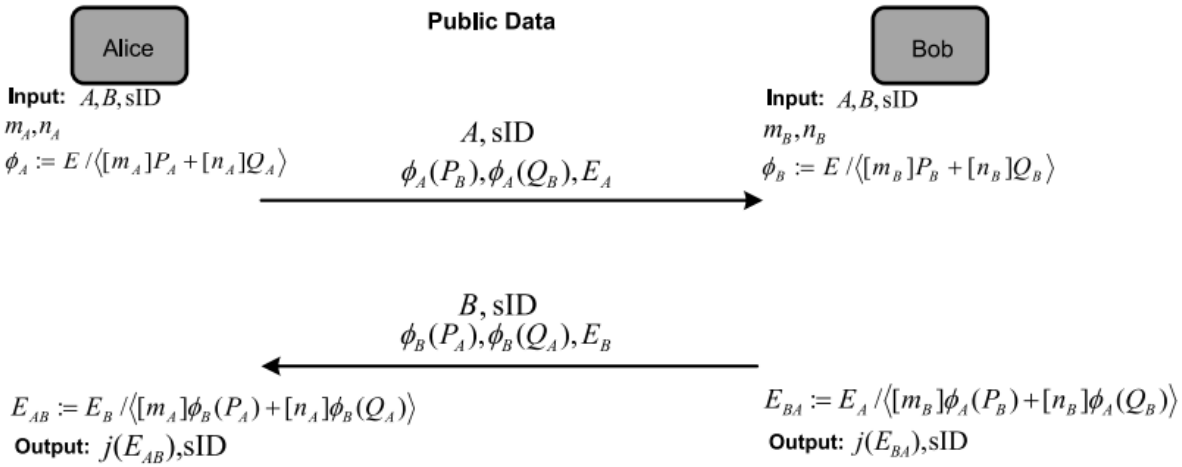
4.4 Κρυπτογραφία Υπερκείμενης Ελλειπτικής Καμπύλης με χρήση Ισογενών

Είδαμε παραπάνω ότι η κρυπτογραφία κλασικής ελλειπτικής καμπύλης (classical elliptic-curve cryptography - ECC), η οποία βασίζεται σε πράξεις μεταξύ σημείων μιας τέτοιας καμπύλης, είναι ευάλωτη σε επιθέσεις από κβαντικούς υπολογιστές. Πράξεις όμως μπορούν να γίνουν και μεταξύ των σημείων δύο διαφορετικών ελλειπτικών καμπυλών (Niederhagen and Waidner, Prof. Dr. Michael 2017:18). Μάλιστα, υπάρχουν αλγεβρικές αντιστοιχήσεις μεταξύ δύο καμπυλών που ικανοποιούν τον νόμο ομάδων των ελλειπτικών καμπυλών (Weisstein 2020:1) και παρουσιάζουν συγκεκριμένες ιδιότητες. Τέτοιες αντιστοιχήσεις καλούνται ισογενή (isogenies).

Τα ισογενή μελετήθηκαν ως λύση για την κατασκευή κρυπτογραφικών σχημάτων και βασίζονται στην δυσκολία υπολογισμού των ισογενών μεταξύ ελλειπτικών καμπύλων (Koziel et al 2017:87). Συγκεκριμένα, το 2006 οι Rostovtsev και Stolbunov κατασκεύασαν κρυπτοσύστημα δημοσίου κλειδιού βασισμένο σε τέτοια ισογενή. Όμως το σύστημα αυτό παρουσίαζε μεγάλους χρόνους στις διαδικασίες της κρυπτογράφησης και αποκρυπτογράφησης (Niederhagen and Waidner, Prof. Dr. Michael 2017:18). Επιπλέον,

τέσσερα χρόνια αργότερα βρέθηκε επίθεση από κβαντικό υπολογιστή σε υποεκθετικό χρόνο που καθιστούσε το κρυπτοσύστημα ευάλωτο (Koziel et al 2017:87) άρα και πρακτικά μη χρήσιμο. Έναν χρόνο αργότερα, μελετήθηκε η ιδέα της εφαρμογής των ισογενών σε μια ειδική κατηγορία ελλειπτικών καμπυλών τις υπερκείμενες ελλειπτικές καμπύλες (Supersingular Elliptic-Curves). Βρέθηκε λοιπόν πως όχι μόνο δεν παρουσίαζαν την παραπάνω αδυναμία στη συγκεκριμένη επίθεση αλλά επιπροσθέτως οι χρόνοι της κρυπτογράφησης και αποκρυπτογράφησης είχαν μειωθεί σημαντικά.

Τα ισογενή σε υπερκείμενες ελλειπτικές καμπύλες έχουν βρει εφαρμογή σε λύσεις που προσομοιάζουν την ανταλλαγή κλειδιού κατά Diffie-Hellman (DH). Σε αυτό βοήθησε η συμμετρία που παρουσιάζουν η οποία μοιάζει πολύ με την δομή των κρυπτογραφικών σχημάτων DH και Elliptic Curve Diffie Hellman (ECDH). Για τον λόγο αυτό, οι λύσεις αυτές καλούνται Supersingular isogeny Diffie Hellman (SIDH) και παρουσιάζουν πολύ καλές επιδόσεις σε χρόνους και μεγέθη μηνυμάτων κάνοντάς τις ιδιαιτέρως ανταγωνιστικές.



Εικόνα 11. Παράδειγμα ανταλλαγής κλειδιού για την συνεδρία με μοναδικό κωδικό sID σε Supersingular isogeny Diffie Hellman (Koziel et al 2017:88)

Εάν τα ισογενή σε υπερκείμενες ελλειπτικές καμπύλες, αποδειχτούν και ανθεκτικά σε επιθέσεις από κλασικούς και κβαντικούς υπολογιστές, τότε θα μπορούσαν να θέσουν ισχυρή υποψηφιότητα να αποτελέσουν πρότυπο για την κατασκευή κρυπτοσυστημάτων στην μετα-κβαντική εποχή (Niederhagen and Waidner, Prof. Dr. Michael 2017:18) με εφαρμογή σε blockchains. Επειδή όμως πρόκειται για σχετικά νέα λύση που δεν έχει δοκιμαστεί ιδιαιτέρως, δεν υπάρχει ακόμα απόλυτη εμπιστοσύνη από την επιστημονική κοινότητα στα κρυπτοσυστήματα αυτά.

4.4.1 Παραδείγματα – Υλοποιήσεις αλγορίθμων

Παρόλα αυτά, υπάρχει ένα σχήμα κρυπτοσυστήματος δημοσίου κλειδιού σε Supersingular Elliptic-Curves, που κατάφερε να προκριθεί στον δεύτερο γύρο του NIST. Ο αλγόριθμος SIKE, ο οποίος παρουσιάζει το μικρότερο σε μέγεθος δημόσιο κλειδί από όλα τα εναπομείναντα σχήματα (≤ 750 bytes), ενώ το γεγονός πως βασίζεται στον πυρήνα του στις ελλειπτικές καμπύλες, επιτρέπει στην κατασκευή υβριδικών κλασικών και μετα-κβαντικών κρυπτοσυστημάτων. Μεγάλο του μειονέκτημα είναι το γεγονός πως είναι πολύ πιο αργός από τους περισσότερους άλλους υποψήφιους στην κατηγορία αυτή αλγορίθμους (Alagic et al 2019:14).

4.5 Κρυπτογραφία βασισμένη σε Συναρτήσεις Κατακερματισμού

Το κρυπτογραφικό σύστημα που βασίζεται σε συναρτήσεις κατακερματισμού (hash-based cryptographic system) παρουσιάζει μεγάλο ενδιαφέρον και θεωρείται ιδιαίτερα ανθεκτικό στις επιθέσεις από κβαντικούς υπολογιστές. Όπως δηλώνει και το όνομά του, βασίζεται στις μονόδρομες (ή μονής κατεύθυνσης) συναρτήσεις κατακερματισμού (hash) οι οποίες λαμβάνουν ως είσοδο ένα μήνυμα *m* (input string) οποιουδήποτε μήκους και παράγουν ένα αποτύπωμα αυτής (digest) *h* συγκεκριμένου μήκους *n*. Οι συναρτήσεις αυτές χαρακτηρίζονται από τρεις βασικές ιδιότητες τις οποίες και κληροδοτούν στο κρυπτογραφικό σύστημα:

(α) Ανθεκτικότητα Προ-Εικόνας (Pre-image Resistance): Η βασική ιδιότητα μιας hash function, η οποία είναι και η αιτία που χαρακτηρίζεται ως μονόδρομη (μιας κατεύθυνσης – one way). Αυτό σημαίνει πως από το αποτέλεσμα (digest) *Y* μιας hash function *H*, είναι υπολογιστικά αδύνατο (για την ακρίβεια, να απαιτείται τέτοιο χρονικό διάστημα που να θεωρείται μη-αποδεκτό) να βρεθεί το αρχικό μήνυμα *X*. Δηλαδή, δεδομένου του *Y* μην μπορεί να βρεθεί μήνυμα *X* τέτοιο ώστε $H(X) = Y$.

(β) Δεύτερη Ανθεκτικότητα Προ-Εικόνας (Second pre-image Resistance): Η δεύτερη ιδιότητα μιας hash function αποτελεί παραλλαγή της πρώτης και ορίζει πως έχοντας ένα αρχικό μήνυμα *X*, να είναι υπολογιστικά αδύνατο να βρεθεί διαφορετικό μήνυμα *X΄* που να παράγει ίδιο digest με το *X*, δηλαδή $H(X) = H(X')$.

(γ) Ανθεκτικότητα Σύγκρουσης (Collision Resistance): Η τρίτη ιδιότητα, αποτελεί γενίκευση της δεύτερης και σύμφωνα με την οποία θα πρέπει να είναι υπολογιστικά αδύνατο να βρεθούν δύο οποιαδήποτε μηνύματα X_1, X_2 που να παρουσιάζουν το ίδιο

digest ως αποτέλεσμα εφαρμογής της hash function πάνω τους, δηλαδή $H(X_1) = H(X_2)$.

Είναι σημαντικό να εξετάσουμε σε αυτό το σημείο, την επίδραση των αλγορίθμων Grover και Shor στις παραπάνω ιδιότητες. Ο αλγόριθμος του Grover επιταχύνει τους χρόνους υπολογισμού με μέθοδο «εξαντλητικής αναζήτησης» (brute force) για την preimage ιδιότητα, σε χρόνους τετραγωνικής ρίζας σε σχέση με τους αντίστοιχους κλασικούς αλγορίθμους. Επιπλέον, βελτιώνει τους χρόνους υπολογισμού συγκρούσεων (collisions) πάλι με μέθοδο brute force κατά κυβική ρίζα, κάτι που όμως δεν είναι ακόμα κοινά αποδεκτό. Ο αλγόριθμος του Shor από την άλλη, δεν επηρεάζει με κανένα τρόπο τις συναρτήσεις κατακερματισμού. Ένα κρυπτογραφικό σύστημα με τις παραπάνω ιδιότητες και αφού εξορισμού δεν είναι εφικτό να αντιστραφεί μια συνάρτηση κατακερματισμού, δεν μπορεί να χρησιμοποιηθεί αυτοτελώς για κρυπτογραφία δημοσίου κλειδιού, όμως μπορεί να υλοποιήσει λύση ψηφιακής υπογραφής (Niederhagen and Waidner, Prof. Dr. Michael 2017:14). Μάλιστα, η ιδέα αυτή εμφανίστηκε πίσω στο 1979 οπότε και ο μαθηματικός Leslie Lamport περιέγραψε ένα ισχυρό σύστημα ψηφιακής υπογραφής που θα βασίζεται πάνω σε απλή μονόδρομη συνάρτηση όπως μια hash.

4.5.1 Lamport One-Time Signatures

Το σύστημα που περιέγραψε ο Lamport λειτουργεί ως εξής. Έστω ένας αποστολέας μηνύματος *M* μήκους *m* bits που επιθυμεί να το υπογράψει ψηφιακά. Αρχικά δημιουργεί *m* ζεύγη τυχαίων σειρών bits (bitstring), ένα ζεύγος για κάθε bit του αρχικού μηνύματος προς υπογραφή. Από το κάθε ζευγάρι, το ένα τυχαίο bitstring θα αντιστοιχηθεί στην περίπτωση που το bit είναι ίσο με μηδέν και το άλλο στην περίπτωση που το bit είναι ίσο με ένα. Έχουμε δηλαδή:

$sk_0 = sk_1^0,\ sk_2^0, \dots,\ sk_m^0$ (για bit = 0)

$sk_1 = sk_1^1,\ sk_2^1, \dots,\ sk_m^1$ (για bit = 1)

Η λίστα (sk_0, sk_1), αποτελεί το ιδιωτικό κλειδί (secret key) του αποστολέα που θα χρησιμοποιήσει για την ψηφιακή υπογραφή του *M*. Προκειμένου στη συνέχεια να δημιουργήσει το δημόσιο κλειδί (public key), απλά εφαρμόζει συνάρτηση hash *H* σε κάθε ένα από αυτά τα τυχαία bitstrings.

$pk_0 = H(sk_1^0), H(sk_2^0), \dots, H(sk_m^0)$ (για bit = 0)

$pk_1 = H(sk_1^1), H(sk_2^1), \dots, H(sk_m^1)$ (για bit = 1)

Έτσι, η λίστα (pk_0, pk_1) αποτελεί το δημόσιο κλειδί του αποστολέα.

Για να υπογράψει λοιπόν το αρχικό μήνυμα *M*, ο αποστολέας διανύει bit προς bit (parse) το μήνυμα για κάθε θέση *i* με $1 \leq i \leq m$. Εάν το $bit_i = 0$ τότε επιλέγει το στοιχείο sk_0^i, ενώ εάν $bit_i = 1$ το sk_1^i. Έχοντας επαναλάβει την παραπάνω διαδικασία για κάθε bit του *M*, ενώνει τα επιλεγμένα bitstrings σε αυτό που θα αποτελεί την ψηφιακή υπογραφή *sig* του μηνύματος.

Ένας παραλήπτης του μηνύματος *M* με την ψηφιακή υπογραφή *sig*, κάτοχος του δημοσίου κλειδιού (pk_0 , pk_1) που επιθυμεί να επικυρώσει τον αποστολέα και υπογράφοντα, ακολουθεί την εξής απλή διαδικασία.
Για το *i*-ιοστό bit του μηνύματος με $1 \leq i \leq m$, παίρνει το αντίστοιχο τμήμα της ψηφιακής υπογραφής sig_i και υπολογίζει την hash τιμή του, $H(sig_i)$. Εάν το bit στη θέση *i* είναι μηδέν ($M_i = 0$) τότε η υπολογισθείσα τιμή πρέπει να ισούται με την τιμή του δημοσίου κλειδιού στην ίδια θέση για bit =0, δηλαδή $H(sig_i) = pk_0^i$, ενώ αντίστοιχα εάν $M_i = 1$, πρέπει $H(sig_i) = pk_1^i$. Έτσι, εάν με τον τρόπο αυτό επαληθευτούν όλα τα bits του *M*, τότε η ψηφιακή υπογραφή θεωρείται έγκυρη. (Mathhew Green 2018:3,4)

Παρότι η διαδικασία υπολογισμού των hash values είναι εξαιρετικά γρήγορη και ασφαλής, το παραπάνω σύστημα πάσχει σε δύο βασικά σημεία. Αρχικά, όπως γίνεται άμεσα αντιληπτό, το μέγεθος των κλειδιών (δημόσιο και ιδιωτικό) και των υπογραφών, μπορεί να γίνει πολύ μεγάλο. Για παράδειγμα έστω πως γίνεται χρήση της hash συνάρτησης SHA256 για την υπογραφή ενός μηνύματος μήκους 256 bits. Στην περίπτωση αυτή, το δημόσιο κλειδί θα είχε μέγεθος 256 bits (hash digest) * 256 (αριθμός bits μηνύματος) * 2 (ένα για bit=0 κι ένα για bit=1) και η υπογραφή 256 (secret key position *i* element bits) * 256 bits. Προσθέτοντας μόνο αυτά τα δύο φτάνουμε σε μέγεθος 24,5 KB, ενώ αν χρησιμοποιούσαμε αντίστοιχα την SHA512 η αξία θα εκτινασσόταν στα 98KB (Chalkias et al 2018:3). Για ένα τόσο μικρό μήνυμα, ακόμα και για τις ταχύτητες μεταγωγής δεδομένων που υπάρχουν σήμερα, σε μια blockchain θα αύξανε το μέγεθός της σε δυσθεώρητα ύψη (Matier and Waterland 2016:3).

Το πιο σημαντικό πρόβλημα όμως με το σύστημα Lamport, είναι πως το κάθε ιδιωτικό και δημόσιο κλειδί (άρα και κάθε υπογραφή), μπορεί να χρησιμοποιηθεί μόνο μία φορά για να υπογράψει ένα μήνυμα (One Time Signature, OTS). Πράγματι, εάν ο αποστολέας προσπαθήσει να υπογράψει ένα δεύτερο μήνυμα M_2 με την ίδια υπογραφή (ίδια κλειδιά) που χρησιμοποίησε για το αρχικό *M*, τότε για κάθε bit στη θέση *i* στο οποίο θα διέφεραν

τα δύο αυτά μηνύματα $M_2^i \neq M^i$ τότε θα είχε φανερώσει το ζευγάρι της ψηφιακής υπογραφής και για τις δύο περιπτώσεις στην θέση αυτή (sig_i^0, sig_i^1). Έτσι, ένας τρίτος (κακόβουλος επιτιθέμενος), θα μπορούσε να συντάξει ένα διαφορετικό μήνυμα M_3 όπου στις θέσεις των bits που έχει φανερωθεί το ζεύγος της υπογραφής, να επιλέξει bit όποιας τιμής θέλει. Το M_3 θα ήταν διαφορετικό από τα M, M_2 αλλά θα είχε έγκυρη υπογραφή χωρίς ο επιτιθέμενος να γίνει αντιληπτός (Mathhew Green 2018:4). Στην εφαρμογή του μάλιστα σε μια blockchain και ειδικά τύπου δοσοληψίας κρυπτονομισμάτων, θα σήμαινε μετά από οποιαδήποτε συναλλαγή τα χρήματα θα έπρεπε να μετακινούνται σε νέα διεύθυνση διαφορετικά θα υπήρχε κίνδυνος υποκλοπής τους (Matier and Waterland 2016:5).

Φυσικά, υπάρχει ο ισχυρισμός πως εφόσον το σύστημα ψηφιακής υπογραφής του Lamport είναι ασφαλές, κάποιος που θα ήθελε να στείλει N μηνύματα ψηφιακά υπογεγραμμένα, θα μπορούσε να προ-υπολογίσει και προ-κατασκευάσει N διαφορετικές OTS Lamport υπογραφές και να χρησιμοποιεί μία (διαφορετική κάθε φορά) για κάθε μήνυμα (Mathhew Green 2018:5). Αυτό όμως αυξάνει γραμμικά το πλήθος των δημοσίων και ιδιωτικών κλειδιών κάνοντας την λύση αυτή ασύμφορη σε ότι αφορά τον όγκο των δεδομένων που θα έπρεπε να διακινηθούν και να αποθηκευτούν. Κάθε παραλήπτης θα έπρεπε να κατέχει αντίγραφο όλων των δημοσίων κλειδιών του αποστολέα προκειμένου να ελέγξει την εγκυρότητα κάθε μηνύματος αφού δεν θα μπορούσε από πριν να γνωρίζει ποιο δημόσιο κλειδί θα αντιστοιχούσε στο ιδιωτικό που χρησιμοποιήθηκε για την υπογραφή του μηνύματος.

4.5.2 Winternitz OTS

Ο Robert Winternitz, βασισμένος σε μια παλαιότερη ιδέα του Ralph Merkle, πρότεινε μια παραλλαγή του σχήματος υπογραφών του Lamport-OTS η οποία προσφέρει σημαντική μείωση στο μέγεθος των υπογραφών και των δημοσίων κλειδιών με κόστος στον χρόνο υπογραφής και επαλήθευσής της (τεχνική time-space tradeoff). Το βασικό σκεπτικό της παραλλαγής του Winternitz είναι η μαζική υπογραφή w αριθμού bits του αρχικού μηνύματος M αντί για την υπογραφή κάθε ενός bit κατά Lamport. Για την υπογραφή του μηνύματος m bits, θα δημιουργηθεί μια λίστα m/w αριθμού ιδιωτικών κλειδιών:

$sk_0 = (sk_0^1, \dots\ sk_0^{m/w})$,

η οποία θα είναι το αρχικό ιδιωτικό κλειδί του αποστολέα. Για να δημιουργηθεί η επόμενη λίστα κλειδιών θα εφαρμοστεί μονόδρομη συνάρτηση hash H στην προηγούμενη έτσι

ώστε:

sk_1 = (sk_1^1, … $sk_1^{m/w}$) = ($H(sk_0^1)$, … H($sk_0^{m/w}$)), κ.ο.κ.

Η διαδικασία αυτή θα επαναληφθεί 2^w φορές, δημιουργώντας w-1 λίστες ιδιωτικών κλειδιών. Η τελευταία λίστα (δηλαδή η τελευταία φορά που θα εφαρμοστεί η hash συνάρτηση), θα είναι και το δημόσιο κλειδί pk του αποστολέα. Το σχήμα υπογραφών αυτό το οποίο καλείται W-OTS (από το επίθετο του Winternitz), έχει το ισχυρό πλεονέκτημα πως τελικά ο υπογράφων χρειάζεται να αποθηκεύσει μόνο την αρχική λίστα ιδιωτικών κλειδιών (sk_0) καθώς οι υπόλοιπες όπως και η μοναδική λίστα δημοσίων κλειδιών pk = (pk_1, … $pk_{m/w}$) μπορούν να υπολογιστούν από το sk_0.

Για παράδειγμα, έστω ότι ως hash function χρησιμοποιούμε την SHA-256 και πως θα «χωρίσουμε» το μήνυμα (hash digest) σε τμήματα των 8 bits (δηλαδή 1 byte). Αυτό σημαίνει m = 256, w = 8, θα δημιουργηθούν 2^8-1 = 256-1 = 255 λίστες ιδιωτικών κλειδιών, ενώ το αρχικό ιδιωτικό κλειδί sk_0 καθώς και το δημόσιο κλειδί pk θα έχουν μέγεθος
s = (256/8) * 256 / 8 bytes = 1kB (Matier and Waterland 2016:3). Ο αποστολέας, προκειμένου να υπογράψει το πρώτο byte (w=8bits) του μηνύματος, θα επιλέξει το πρώτο στοιχείο sk_x^1 από την λίστα ιδιωτικών κλειδιών που ορίζεται ανάλογα με την τιμή του byte αυτού, κ.ο.κ. . Ο παραλήπτης για να επαληθεύσει το byte αυτό της υπογραφής (sig_1), χρειάζεται να εφαρμόσει την hash συνάρτηση πάνω στο συγκεκριμένο byte της υπογραφής τόσες φορές, ανάλογα με την τιμή και την θέση του στο μήνυμα (index, i) (Mathhew Green 2018:9). Συγκεκριμένα,
SHA-256 ^ 2^{w-1}(sig_x) = SHA-256 ^ 2^7 (sig_1), δηλαδή να εφαρμόσει την συνάρτηση 255 φορές και να συγκρίνει το αποτέλεσμα με το στοιχείο pk_1 του δημοσίου κλειδιού του αποστολέα (Matier and Waterland 2016:3). Εάν όλα τα στοιχεία του μηνύματος επαληθευτούν, τότε η υπογραφή είναι έγκυρη.

Στο παραπάνω παράδειγμα, προκειμένου να υπολογιστεί η λίστα με τα στοιχεία του δημόσιου κλειδιού, θα απαιτηθούν $i = m/w * 2^{w-1}$ = 256/8 * 2^7 = 8160 επαναλήψεις εφαρμογής της hash συνάρτησης. Σε περίπτωση που θελήσουμε να μεταβάλουμε το w και να υπογράψουμε τμήματα για παράδειγμα των 16bits, w = 16, τότε το πλήθος των κλειδιών και το μέγεθος των υπογραφών θα μειωθεί στο μισό, αλλά το i = 1.048.560 που είναι απαγορευτικός αριθμός επαναλήψεων κάθε που θα χρειαστεί να υπολογιστεί το δημόσιο κλειδί (Matier and Waterland 2016:3). Για αυτό είναι πολύ σημαντικό να βρεθεί και να υπολογιστεί το ιδανικό w που θα φέρει ισορροπία μεταξύ του χρόνου

υπολογισμών και του μεγέθους των κλειδιών και των υπογραφών.

Επιπλέον, μια προφανή αδυναμία ασφάλειας του W-OTS σχήματος είναι πως επειδή τα ιδιωτικά κλειδιά συνδέονται μεταξύ τους βάση της σχέσης $sk_i = H(sk_{i-1})$, ένας επιτιθέμενος μπορεί να αυξήσει την τιμή ενός byte του μηνύματος, να μεταβάλει αναλόγως το τμήμα της υπογραφής που το αφορά (εφαρμόζοντας ανάλογα την hash function πάνω στην αρχική τιμή της υπογραφής για το τμήμα αυτό) επιτυγχάνοντας έτσι να αλλάξει το περιεχόμενο του μηνύματος και να το υπογράψει με έγκυρη υπογραφή. Για τον λόγο αυτό, ο αποστολέας υπολογίζει και υπογράφει μαζί με το μήνυμα ένα άθροισμα ελέγχου (checksum) το οποίο υπολογίζεται από τον τύπο: $\sum_{i=1}^{\ell} 255 - M_i$ (Matthew Green 2018:1). Παρόλα αυτά, το σχήμα W-OTS θεωρείται ανθεκτικό στις επιθέσεις από κβαντικούς υπολογιστές αφού και αυτό βασίζεται στις ιδιότητες των hash συναρτήσεων και ειδικά στο pre-image resistance.

4.5.3 Winternitz OTS +

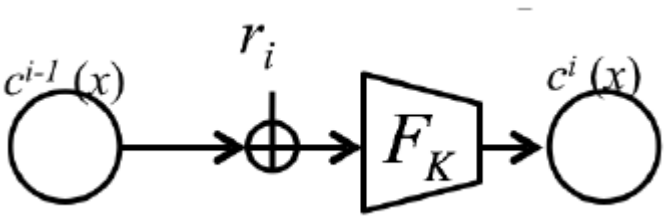
Μια παραλλαγή του Winternitz OTS συστήματος υπογραφών, περιέγραψε ο Johannes Buchmann. Σύμφωνα με αυτή, που ονομάστηκε Winternitz OTS + (ή απλά W-OTS+), στην αλυσιδωτή εφαρμογή της hash συνάρτησης κατά τον υπολογισμό των ιδιωτικών κλειδιών, προστίθεται και μια XOR λειτουργία ενώ πλέον το μήνυμα δεν χωρίζεται σε τμήματα των w bits αλλά σε $\log_2(w)$ bits, πράγμα που μειώνει το πλήθος των επαναλήψεων εφαρμογής της hash αλλά αυξάνει τον αριθμό των κλειδιών και το μέγεθος των υπογραφών (Matier and Waterland 2016:3).

Συγκεκριμένα, ορίζεται συνάρτηση αλυσίδας $c_k^i(x,r)$ τέτοια ώστε:

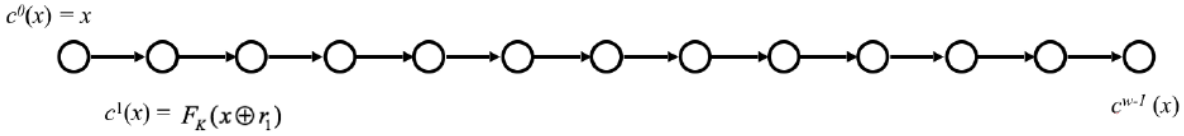
$$c^i(x,r) = \begin{cases} x & \text{if } i = 0; \\ f_k(c_k^{i-1}(x,r) \oplus r_i) & \text{if } i > 0; \end{cases}$$

Τύπος 2. Τύπος Συνάρτησης Αλυσίδας W-OTS+ (Matier and Waterland 2016:4)

Ενώ σχηματικά αποδίδεται:



Εικόνα 12. Συνάρτηση Αλυσίδας W-OTS+ (Matier and Waterland 2016:4)



Εικόνα 13. Παράδειγμα δημιουργίας αλυσίδας hash (Matier and Waterland 2016:4)

Σύμφωνα με τα παραπάνω, με εξαίρεση το πρώτο βήμα (*i*=0) της διαδικασίας, κάθε επόμενη εφαρμογή της hash συνάρτησης γίνεται πάνω στο αποτέλεσμα της *c* του προηγούμενου βήματος αφού πρώτα προστεθεί XOR σε αυτό, ένα στοιχείο τυχαιότητας r_i.

Το W-OTS+ σχήμα, προσφέρει ασφάλεια τουλάχιστον $n - w - 1 - 2\log(lw)$ bits, όπου το *n* εξαρτάται από την επιλεγμένη hash function (*n*=256 για την SHA-256), και $l = l_1 + l_2$ με

$$l_1 = \lceil \frac{m}{log_2(w)} \rceil, \quad l_2 = \lfloor \frac{log_2(l_1(w-1))}{log_2(w)} \rfloor + 1$$

Τύπος 3. Τύποι υπολογισμού των l_1, l_2
για τον ορισμό του βαθμού ασφάλειας στο W-OTS+ σχήμα

Μια υπογραφή με $w = 16$ και επιλεγμένη hash function την SHA-256 (*n*=256, *m*=256) έχει μέγεθος 2,1 kB.

4.5.4 Merkle Trees

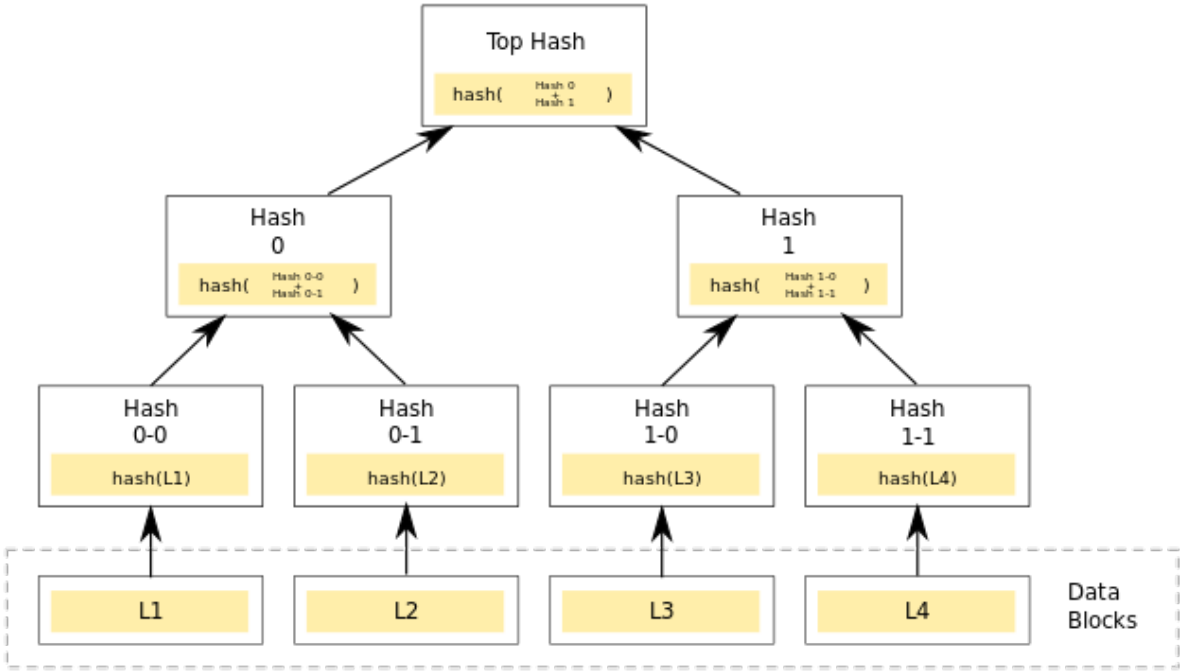
Την παραπάνω κοστοβόρα λύση έρχεται να βελτιώσει ο μαθητής του Martin Hellman (βλ. Diffie-Hellman) Ralph Merkle. Ο Merkle πρότεινε μια δυαδική δενδροειδή δομή με *n* φύλλα βάσης (επίπεδο 0) και ύψος *h* μέχρι την κορυφή όπου βρίσκεται η ρίζα του δέντρου. Η δομή αυτή ονομάστηκε Merkle Tree (ή hash Tree) και λειτουργεί ως εξής:

- Αρχικά, με τη χρήση συνάρτησης hash *H*, υπολογίζονται οι hash values για κάθε

data block που θέλουμε να αποτυπώσουμε στο Merkle Tree

- Τοποθετούνται οι hash values στα φύλλα του Merkle Tree
- Σε κάθε κόμβο (node) του δέντρου που προέρχεται από δύο φύλλα ή δύο άλλους κόμβους, υπολογίζεται και τοποθετείται η hash value των δεδομένων που προκύπτουν από την συνένωση (concatenation) των hash values των φύλλων ή κόμβων αυτών.
- Ομοίως, τελικά υπολογίζεται και η ρίζα του δέντρου ως η hash value της συνένωσης των hash values των δύο τελευταίων κόμβων.

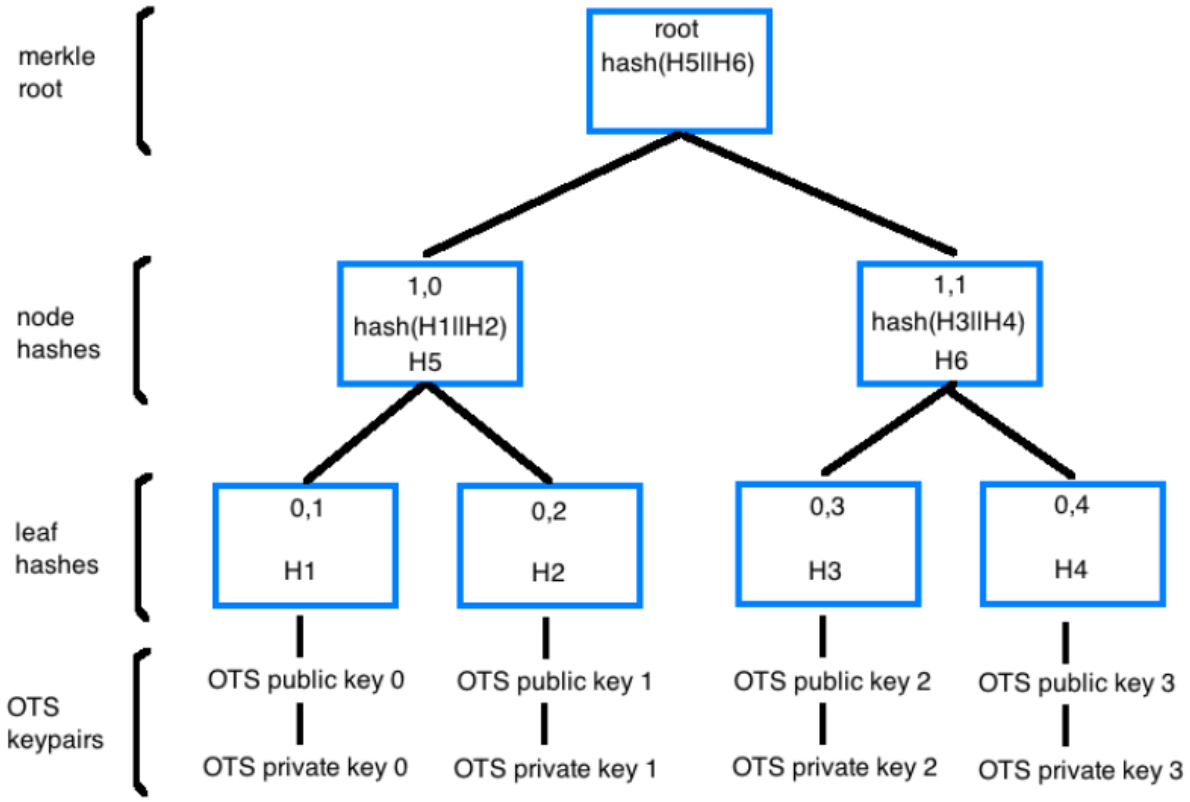
Τα παραπάνω αποτυπώνονται στο παράδειγμα του σχήματος που ακολουθεί (Wikipedia 2020:1, Matier and Waterland 2016:5)



Εικόνα 14. Δομή Merkle Tree

Αξιοποιώντας την παραπάνω δομή για την βελτίωση του συστήματος Lamport, ο αποστολέας υπολογίζει αρχικά τα ζεύγη των OTS κλειδιών για όσα μηνύματα θέλει να υπογράψει έστω (public key 0, private key 0), (public key 1, private key 1), … , (public key *n*, private key *n*). Στην συνέχεια, υπολογίζει τις hash values των public keys και τις τοποθετεί στα φύλλα ενός Merkle Tree. Τέλος, υπολογίζει τις hash values κάθε κόμβου προς τα πάνω μέχρι και την ρίζα με τον τρόπο που περιγράψαμε παραπάνω. Η hash value της ρίζας (root) είναι και το public key του αποστολέα το οποίο θα διαμοιράζει στους παραλήπτες των μηνυμάτων του και θα έχει μέγεθος ανάλογα με την hash συνάρτηση

που χρησιμοποιήθηκε (256 bits για την περίπτωση της SHA-256). Για παράδειγμα, ένα Merkle Tree που δημιουργείται για τέσσερις One Time Signatures θα μοιάζει με το παρακάτω:



Εικόνα 15. Παράδειγμα Merkle Tree με τέσσερα ζεύγη κλειδιών OTS

Ο αποστολέας που θα επιθυμεί να υπογράψει ψηφιακά ένα μήνυμα *M* με μία OTS υπογραφή s από το παραπάνω Merkle Tree, θα χρειαστεί να αποστείλει στον παραλήπτη, το μήνυμα *M* και ένα πακέτο υπογραφής *S* το οποίο θα αποτελείται από:

- την ψηφιακή υπογραφή *s*, από την οποία μπορεί να βρεθεί το OTS public key
- τον αριθμό *n* της OTS υπογραφής που χρησιμοποιήθηκε από το Merkle Tree
- την απόδειξη πως το OTS public key που χρησιμοποιήθηκε για την *s*, ανήκει στο Merkle Tree το οποίο ορίζεται από το δημόσιο κλειδί του αποστολέα που είναι το root του δένδρου αυτού. Η απόδειξη αυτή καλείται Merkle authentication path και περιλαμβάνει την ελάχιστη πληροφορία που χρειάζεται ο παραλήπτης για να μπορέσει να κατασκευάσει εκ νέου το δένδρο κι έτσι να δεχτεί πως το μήνυμα *M* υπογράφηκε από έγκυρη υπογραφή.

Για παράδειγμα, έστω πως ο αποστολέας θέλει να υπογράψει ένα μήνυμα με το ζεύγος OTS κλειδιών για *n*=1 (OTS public key 1, OTS private key 1). Στην περίπτωση αυτή το

πακέτο υπογραφής *S* θα περιλαμβάνει τα *s*, *n*, *H1*, *H6*. Ο παραλήπτης στη συνέχεια, έχοντας το OTS Public key 1 μπορεί να υπολογίσει το *H2* που μαζί με το *H1* μπορεί να βρει το *H5* (hash *H1*||*H2*). Έχοντας στην κατοχή του και το *H6*, μπορεί να υπολογίσει το root (hash *H5*||*H6*). Εάν το root που υπολογίσει με την χρήση αυτού του authentication path είναι ίδιο με το public key (root) που έχει δημοσιεύσει ο αποστολέας, τότε ξέρει πως η υπογραφή είναι έγκυρη, αφού χάρη στον τρόπο δημιουργίας των ζευγών κλειδιών και τις ιδιότητες των hash functions, μόνο ο αποστολέας θα μπορούσε να γνωρίζει το OTS private key-*n* το οποίο συσχετίζεται με το αντίστοιχο public key-*n* και από το οποίο θα μπορούσε να έχει δημιουργηθεί το Merkle Tree με root hash ίση με το public key του.

Τα Merkle Trees, λοιπόν, μπορούν να μετατρέψουν τις One Time Signatures σε ένα Multi-Time Signature σύστημα, που είναι και το μεγάλο τους πλεονέκτημα. Επιπλέον, το μέγεθος της τελικής υπογραφής είναι σχετικά μικρό, ο χρόνος που απαιτείται για την επικύρωση της υπογραφής (verification) είναι ελάχιστος (Chalkias et al 2018:3) και το public key (root της δενδροειδούς δομής) είναι μικρό σε σχέση με όλα τα προηγούμενα σχήματα, ίσο με το μέγεθος της εξόδου της hash συνάρτησης που χρησιμοποιήθηκε (συνήθως 256 ή 512 bits) (Mathhew Green 2018:6).

Το μειονέκτημα των Merkle Trees είναι πως ο αποστολέας πρέπει από πριν να γνωρίζει (ή να υπολογίσει) το σύνολο των μηνυμάτων που θα χρειαστεί να υπογράψει μιας και όλα τα ζεύγη κλειδιών κατασκευάζονται μαζί ώστε να δημιουργηθεί η δομή του Merkle Tree. Ο χρόνος που θα απαιτηθεί για αυτή την αρχικοποίηση αυξάνεται εκθετικά ανάλογα με το ύψος *h* του δέντρου. Συγκεκριμένα, δενδροειδείς δομές Merkle για πάνω από 256 OTS ζεύγη κλειδιών θεωρούνται επεξεργαστικά και χρονικά ασύμφορες να κατασκευαστούν (Matier and Waterland 2016:6). Τέλος, σημαντικό μειονέκτημα αποτελεί πως η λύση αυτή απαιτεί από τον αποστολέα να τηρεί ενημερωμένη την κατάσταση των κλειδιών που έχει χρησιμοποιήσει και αυτών που είναι διαθέσιμα ώστε να μην κάνει χρήση κάποιων key pairs δεύτερη φορά. Η ιδιότητα αυτή καλείται stateful (Chalkias et al 2018:3) και μπορεί να αποτελέσει μεγάλο «πονοκέφαλο» για τον υπογράφοντα μιας και πέρα από επιπλέον κόστος που μπορεί να εισάγει σε μια εφαρμογή, είναι δυνατόν να είναι προβληματικό σε περιπτώσεις ανάκτησης δεδομένων από αντίγραφα ασφαλείας (recovery from backup) αφού δεν θα είναι ασφαλές να επιστρέψει η κατάσταση ενημέρωσης του Merkle Tree σε προηγούμενο στάδιο σε περίπτωση απώλειας δεδομένων (Niederhagen and Waidner, Prof. Dr. Michael 2017:15).

Παρόλα αυτά μια δομή blockchain όπως την περιγράψαμε παραπάνω θα μπορούσε να εξυπηρετεί τον σκοπό του ελέγχου και ανίχνευσης των κλειδιών που έχουν χρησιμοποιηθεί από συγκεκριμένο stateful σχήμα υπογραφών αποτυπωμένο σε Merkle Tree.

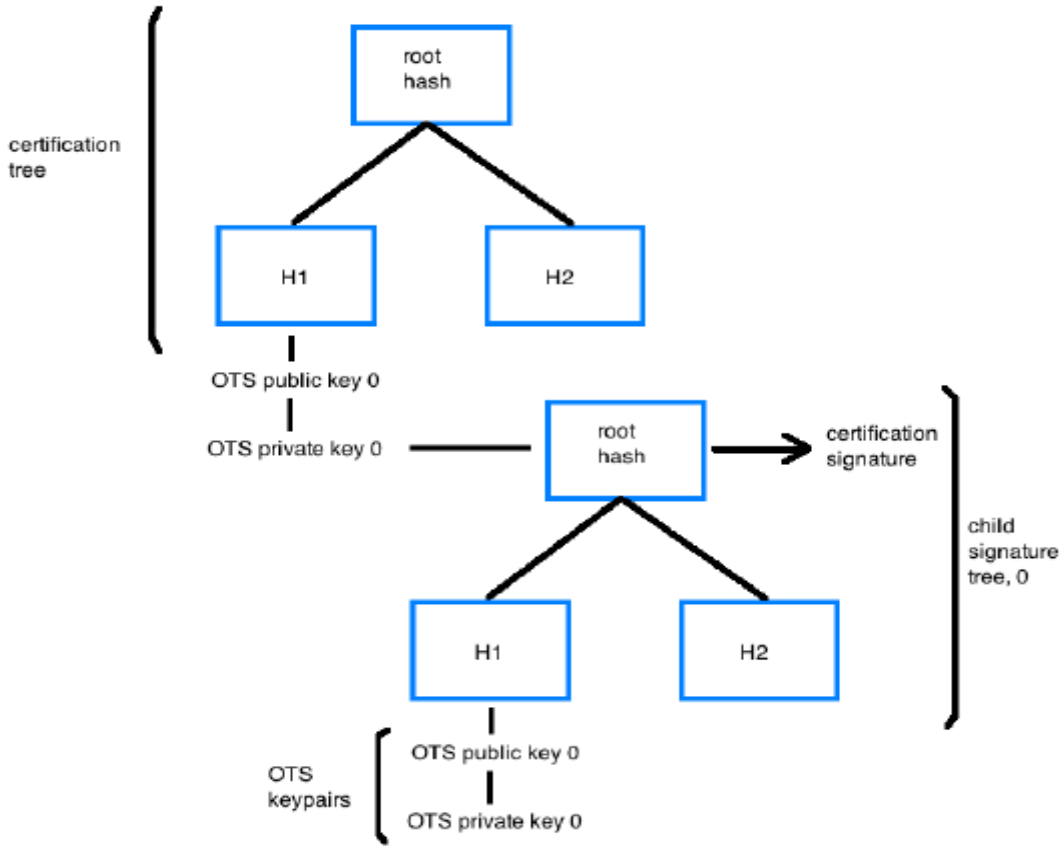
Υπάρχουν όμως και σχήματα hash-based υπογραφών που δεν διατηρούν την κατάσταση των χρησιμοποιημένων-διαθέσιμων κλειδιών και αυτά καλούνται stateless. Αυτό έχει επίπτωση στο μέγεθος της υπογραφής, το οποίο αυξάνεται σημαντικά. Χαρακτηριστικό παράδειγμα τέτοιου σχήματος είναι η οικογένεια hash-based signature schemes SPHINCS η οποία παράγει υπογραφές με 128 bits ασφάλεια (δηλ χρειάζονται 2^{128} προσπάθειες για περιπτώσεις brute force επίθεσης) (Matier and Waterland 2016:6) και μέγεθος υπογραφής περίπου στα 40kBytes (Niederhagen and Waidner, Prof. Dr. Michael 2017:15) (συγκεκριμένα η SPHINCS-256 δημιουργεί υπογραφές μεγέθους 41kBytes) (Chalkias et al 2018:3).

4.5.5 Υπερδέντρα (HyperTrees)

Τα Υπερδέντρα (Hypertrees) είναι δομές σχήματος υπογραφών παρόμοιες με τα κλασικά Merkle Trees (MSS), αλλά με την διαφορά πως ένα Hypertree μπορεί να αποτελείται από δύο ή περισσότερα Merkle Trees. Η ιδέα πίσω από αυτή την δομή είναι να χρησιμοποιείται το OTS ιδιωτικό κλειδί ενός φύλλου δέντρου (leaf) Merkle για την υπογραφή του στοιχείου ρίζας (root hash) ενός άλλου δέντρου. Το δέντρο από το οποίο χρησιμοποιήθηκε το φύλλο καλείται δέντρο πιστοποίησης (certification tree), ενώ το νέο δέντρο που παράγεται καλείται δέντρο-απόγονος υπογραφών (child signature tree). Η στρατηγική αυτή, μειώνει σημαντικά τον χρόνο κατασκευής των διαθέσιμων κλειδιών αφού δεν κατασκευάζεται απευθείας ολόκληρο το Hypertree, ενώ ταυτόχρονα δίνει την δυνατότητα για επέκταση του αριθμού των κλειδιών ανάλογα με την ζήτηση καθώς νέα child signature trees μπορούν να κατασκευαστούν κάτω από διαθέσιμα φύλλα ανά πάσα στιγμή πολλαπλασιάζοντας τα διαθέσιμα κλειδιά. Ένα Hypertree δεν χρειάζεται να είναι συμμετρικό και θεωρητικά δεν έχει περιορισμό στο συνολικό του ύψος (δηλαδή στα πόσα certification και signature trees θα κατασκευαστούν το ένα κάτω από το άλλο). Επίσης, ο αριθμός των φύλλων των δέντρων που αποτελούν ένα Hypertree μπορεί να διαφέρει (Matier and Waterland 2016:6).

Παρακάτω εικονίζεται ένα Hypertree στην πιο απλή μορφή του, που αποτελείται από ένα

certification tree με δύο φύλλα (OTS ζεύγη κλειδιών) και ύψος h=2 κι ένα πανομοιότυπο child signature tree με root hash που παράγεται από ένα από τα διαθέσιμα κλειδιά (OTS private key 0) του certification tree. Όταν τα δύο διαθέσιμα ζεύγη κλειδιών OTS του signature tree χρησιμοποιηθούν, υπάρχει η δυνατότητα να κατασκευαστεί ένα δεύτερο signature tree από το άλλο διαθέσιμο OTS κλειδί του certification tree κλειδιά (OTS private key 1).



Εικόνα 16. Παράδειγμα υπερδέντρο με ένα signature κι ένα certification tree

Η τεχνική αυτή αυξάνει εκθετικά τον αριθμό των διαθέσιμων OTS υπογραφών και γραμμικά το μέγεθος της υπογραφής, με την προσθήκη κάθε νέου child signature tree. Πράγματι, κάθε υπογραφή S που παράγεται από ένα hypertree προκειμένου να επικυρωθεί ως έγκυρη από τον παραλήπτη, πρέπει να συμπεριλαμβάνει (Matier and Waterland 2016:7):

1. Από το signature tree, την υπογραφή s, τον δείκτη n_s, το *merkle path*$_s$ και το *root*$_s$.
2. Για κάθε certification tree πριν το signature tree, το s (του root για το child merkle tree που ακολουθεί), τον δείκτη n_c, το *merkle path*$_c$ και το *root*$_c$.

Σε ένα πιο σύνθετο παράδειγμα, έστω πως έχουμε ένα Hypertree όπου το certification

tree έχει ύψος h_1=4, άρα 2^4 ζεύγη OTS κλειδιών (όσα και τα φύλλα του δέντρου). Αν κάθε φύλλο του certification tree χρησιμοποιηθεί για να κατασκευαστεί ένα signature tree με ύψος επίσης h_2=4, τότε το συνολικό Hypertree θα υποστηρίζει $2^{4+4}=2^8=256$ υπογραφές. Αν μάλιστα μετρήσουμε τον χρόνο δημιουργίας ενός τέτοιου Hypertree και τον συγκρίνουμε με ένα απλό Merkle Tree ίδιας δυναμικής υπογραφών, τότε θα διαπιστώσουμε πως το Hypertree κατασκευάζεται περίπου 15 φορές ταχύτερα. Αυτή η διαφορά στον χρόνο κατασκευής γίνεται περισσότερο αντιληπτή όσο μεγαλώνει το ύψος ενός Hypertree, με αντίστοιχη όμως επιβάρυνση στο μέγεθος των υπογραφών που παράγονται από αυτό.

4.5.5 Επεκταμένο Σχήμα Υπογραφών Merkle

Από όλες τις hash-based signatures schemes που συναντήσαμε ως τώρα, η πιο ολοκληρωμένη ως λύση και ταυτόχρονα η πιο ισχυρή υποψήφια για προτυποποίηση σε μια μετα-κβαντική εποχή με εφαρμογή στις blockchains, είναι το Επεκταμένο Σχήμα Υπογραφών Merkle (eXtended Merkle Signature Scheme, XMSS). Όπως και τα προηγούμενα hash-based σχήματα, έτσι κ αυτό δεν βασίζει την δύναμή του στην δυσκολία επίλυσης γνωστών μαθηματικών προβλημάτων, αλλά στην κρυπτογραφική ισχύ των συναρτήσεων hash. Το σημαντικό πλεονέκτημα του XMSS είναι πως είναι δομημένο με τέτοιο τρόπο ώστε να παραμένει ασφαλές ακόμα και αν παραβιαστεί η τρίτη ιδιότητα των hash συναρτήσεων (collision resistance). Ταυτόχρονα, είναι σχετικά απλό στην υλοποίηση και ανθεκτικό σε side-channel επιθέσεις. Εφαρμόζει την πρακτική του hypertree που είδαμε παραπάνω κι έτσι έχει μικρούς χρόνους κατασκευής των κλειδιών, ενώ παρουσιάζει και την μικρότερη σε μέγεθος υπογραφή από όλα τα άλλα stateful hash-based schemas (Huelsing et al 2018:1).

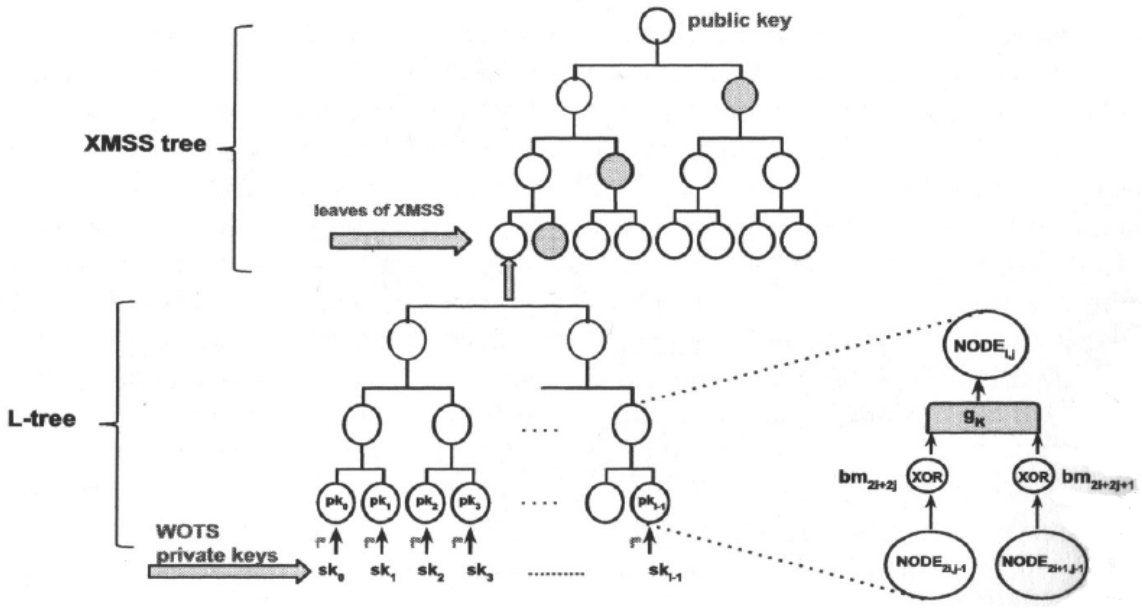
Για να πετύχει όλα τα παραπάνω, ένα XMSS δομείται ως ένα Merkle Tree όπου (Matier and Waterland 2016:8):

- Εφαρμόζεται XOR πρόσθεση μια μάσκας από τυχαία bits (bitmask) στις hash values των κόμβων-παιδιών πριν αυτές συνενωθούν για τον σχηματισμό της hash του κόμβου-γονέα (parent node). Η bitmask, παράγεται από ειδικές συναρτήσεις που καλούνται «ψευτο-τυχαίες συναρτήσεις» (Pseudo-Random Functions – PRF) κι έχουν μεγάλη χρησιμότητα σε υπάρχοντα αλλά και θεωρητικά κρυπτογραφικά μοντέλα, αφού είναι απλές και η τυχαιότητά τους δεν μπορεί να διαχωριστεί από μια πραγματική συνάρτηση τυχαιότητας (Bogdanov and Rosen 2017:2). Η XOR

πρόσθεση είναι που αντικαθιστά ουσιαστικά την ιδιότητα collision resistance της hash συνάρτησης.

- Τα φύλλα του αρχικού δένδρου γίνονται ρίζες άλλων δέντρων που καλούνται λ-Δέντρα (ή L-Trees ή Lambda-Trees). Τα L-Trees μοιάζουν με τα Merkle Trees αλλά δεν έχουν τον περιορισμό το ύψος του κάθε κόμβου-φύλλο να είναι το ίδιο. Είναι δηλαδή δενδροειδής δομές χωρίς ισορροπία (unbalanced) (Huelsing et al 2018:23). Ανεξάρτητα από αυτό όμως, επεκτείνουν το αρχικό Merkle Tree και για αυτό η τελική δομή καλείται επεκταμένο (extended) Merkle Tree με συνολικό ύψος H.
- Στα φύλλα των L-Trees βρίσκονται τα ζεύγη των κλειδιών (δημόσια και ιδιωτικά) που χρησιμοποιούνται για την δημιουργία των ψηφιακών υπογραφών. Το συνολικό πλήθος των φύλλων (και άρα των ζευγών OTS υπογραφών) είναι ίσο με L.
- Οι υπογραφές παράγονται σύμφωνα με την μέθοδο Winternitz OTS+ που περιγράψαμε παραπάνω. Μια XMSS υπογραφή έχει μήκος $(L + H)$ n bits, όπου το n ορίζεται από την W-OTS+ .
- Το δημόσιο κλειδί του XMSS (root hash του αρχικού Merkle Tree) έχει μήκος $(2\ (H + logL) + 1)\ n$ bits.
- Τα ιδιωτικά κλειδιά έχουν μήκος < 2 n.

Σχηματικά, ένα XMSS παρουσιάζεται ως εξής:



Εικόνα 17. Δομή ενός XMSS

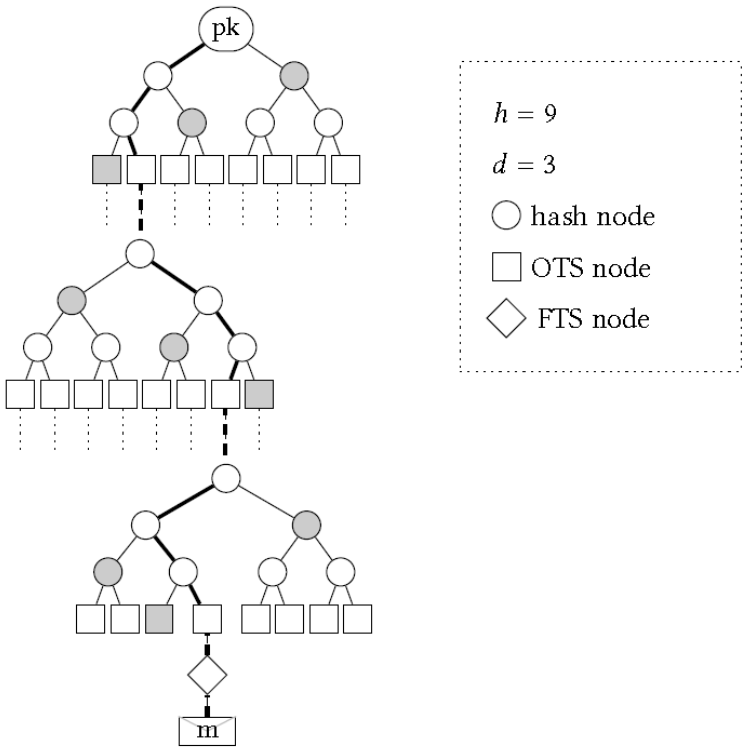
Σε ότι αφορά τις επιδόσεις μιας τέτοιας δομής, έστω XMSS με ύψος H=20, winternitz

μεταβλητή *w*=16 και κρυπτογραφική hash συνάρτηση την SHA-256 που παράγει περίπου ένα εκατομμύριο ψηφιακές υπογραφές. Σε ένα μέτριας δυναμικής ηλεκτρονικό υπολογιστικό σύστημα (intel i5 @ 2.5GHz, 8GB Ram) η υπογραφή μηνύματος χρειάστηκε 7ms, η επικύρωση της 0,52ms ενώ η διαδικασία της κατασκευής όλων των ζευγαριών κλειδιών (key generation) 466s. Η ασφάλεια που επιτεύχθηκε είναι μεγέθους 196 bits με δημόσιο κλειδί μεγέθους 1,7kB, ιδιωτικά κλειδιά μεγέθους 280bits το κάθε ένα που δημιουργούν υπογραφή 2,8 kB (Matier and Waterland 2016:9).

Συμπερασματικά, η δομή XMSS είναι πολλά υποσχόμενη και ελκυστική για την εφαρμογή της σε λύσεις ψηφιακών υπογραφών που είναι ανθεκτικές στην μετακβαντική εποχή και θα έχουν άμεση εφαρμογή σε quantum resistant blockchains.

4.5.6 Παραδείγματα – Υλοποιήσεις αλγορίθμων

Όπως στα κρυπτοσυστήματα που βασίζονται σε Supersingular Elliptic Curve Isogeny, έτσι και στα hash-based, μόνο ένα υποψήφιο σχήμα κατάφερε να προκριθεί στον δεύτερο γύρο αξιολόγησης του NIST στην κατηγορία των ψηφιακών υπογραφών το SPHINCS+ (Bernstein et al 2019:2129–2146). Πρόκειται για ένα stateless σχήμα το οποίο βασίζεται σε δύο διαφορετικά σχήματα υπογραφών στην υλοποίησή του, το WOTS+ που χρησιμοποιεί υπογραφές μίας χρήσης όπως είδαμε και παραπάνω, και το Forest of Random Subsets (FORS) που χρησιμοποιεί υπογραφές λίγων χρήσεων. Το σχήμα του SPHINCS+ κατασκευάζεται από Merkle hash δέντρα πολλαπλών επιπέδων. Στα φύλλα, βρίσκονται ζεύγη κλειδιών FORS και χρησιμοποιούνται για την υπογραφή μηνυμάτων. Κάθε δημόσιο κλειδί FORS καθώς και η ρίζα κάθε Merkle δέντρου, υπογράφονται με WOTS+ (Alagic et al 2019:17). Παράδειγμα αυτής της δομής φαίνεται στην παρακάτω εικόνα.



Εικόνα 18. Δομή ενός SPHINCS+ hypertree (Bernstein et al 2019:2130)

Τα πλεονεκτήματα του SPHINCS+ είναι πως η ασφάλειά του βασίζεται μόνο στην pre-image resistance της hash συνάρτησης που χρησιμοποιείται, ενώ και τα δημόσια κλειδιά του έχουν σχετικά μικρό μέγεθος της τάξης των 32 έως 64 bytes. Το SPHINCS+ μειονεκτεί στον χρόνο και το μέγεθος των υπογραφών που είναι αρκετά μεγάλα (Alagic et al 2019:18).

4.6 Κρυπτογραφία βασισμένη σε Απόδειξη Μηδενικής Γνώσης

Τέλος, ένα ενδιαφέρον και σχετικά νέο κρυπτοσύστημα είναι αυτό που βασίζεται στην απόδειξη μηδενικής γνώσης (Zero-Knowledge Proof of Knowledge, ZKP). Η ιδέα πίσω από αυτή διατυπώθηκε παρόλα αυτά αρκετά παλαιότερα, το 1985 από τους Goldwasser et al. (Goldwasser et al 1985:291–304). Το ZPK βασίζεται σε αλγορίθμους συμμετρικού κλειδιού, χρησιμοποιεί hash συναρτήσεις και για αυτό δεν θεωρείται ξεχωριστή κατηγορία post-quantum κρυπτογραφικό σχήμα, αλλά μία επέκταση του μοντέλου των hash-based με τη χρήση ασφαλούς αλγορίθμου συμμετρικού κλειδιού.

4.6.1 Ορισμός - Πλεονεκτήματα

Πρόκειται για ένα μοντέλο στο οποίο αποδεικνύεται πως κάτι είναι αληθές χωρίς να αποκαλύπτεται η τιμή (value) του. Έστω λοιπόν πως ένας χρήστης *P* κατέχει-γνωρίζει ένα μυστικό *s* και θέλει να αποδείξει σε έναν άλλο χρήστη *V* πως πράγματι το γνωρίζει, χωρίς να αποκαλύψει το *s* καθαυτό. Αυτό επιτυγχάνεται μέσα από μια σειρά ερωταποκρίσεων (challenge-response) μεταξύ των *P* (ας τον καλούμε αποδεικνύων, prover) και *V* (ας τον καλούμε επιβεβαιωτή, verifier) μέσα από τις οποίες συνάγεται με σχετική βεβαιότητα η αλήθεια του αρχικού ισχυρισμού του *P* από τον *V*. Η επίτευξη του στόχου δεν κάνει γνωστό το *s* στον *V* και για αυτό το λόγο το μοντέλο αυτό καλείται μηδενικής γνώσης. Ένα πρωτόκολλο προκειμένου να θεωρηθεί μηδενικής γνώσης, πρέπει να ικανοποιεί τρία κριτήρια (Blum et al 1988:106):

1. Πληρότητα (Completeness), που ορίζει πως η πιθανότητα επιτυχίας στην απόδειξη ενός αληθούς ισχυρισμού είναι συντριπτικά μεγάλη.
2. Ορθότητα (Soundness), που ορίζει πως η πιθανότητα λανθασμένης απόδειξης ενός ψευδούς ισχυρισμού είναι αμελητέα.
3. Μηδενική Γνώση (Zero Knowledge), που ορίζει πως η απόδειξη ενός ισχυρισμού δεν περιέχει καμία επιπλέον πληροφορία παρά μόνο την εγκυρότητα αυτού.

Το μοντέλο ZKP χωρίζεται σε δύο κατηγορίες ανάλογα με τον τρόπο λειτουργίας του. Ο τρόπος που περιγράψαμε παραπάνω, απαιτεί την αλληλεπίδραση μεταξύ δύο μερών (συγκεκριμένα των χρηστών *P*, *V*) μέχρι να επέλθει η επιβεβαίωση – ή η απόρριψη – του αρχικού ισχυρισμού και για αυτό τον λόγο καλείται αλληλεπιδραστική (interactive). Ο τρόπος αυτός όμως έχει περιορισμένη δυνατότητα μεταφοράς της απόδειξης του ισχυρισμού σε τρίτο. Έτσι, σε περίπτωση που ο *P* χρειαστεί να αποδείξει την κατοχή-γνώση του *s* σε έναν άλλο χρήστη *Q*, τότε θα χρειαστεί να επαναλάβει αντίστοιχη διαδικασία αλληλεπίδρασης από την αρχή. Επίσης, τα αλληλεπιδραστικά πρωτόκολλα επιφέρουν, αναπόφευκτα, καθυστέρηση. Για τον λόγο αυτό, υπάρχει και μια δεύτερη κατηγορία ZKP που καλείται μη-αλληλεπιδραστική (non-interactive) όπου ο καθένας, με τη χρήση ειδικού αλγορίθμου (τροποποίηση του Fiat-Shamir), μπορεί να επαληθεύσει από μόνος του την εγκυρότητα ενός ισχυρισμού – δηλαδή χωρίς αλληλουχία διαφόρων ερωτήσεων-απαντήσεων. Αυτό βέβαια είναι πολύ σημαντικό, καθώς σε μια blockchain για παράδειγμα ο καθένας που έχει δικαίωμα πρόσβασης στις εγγραφές της, θα μπορεί να επαληθεύει την εγκυρότητά τους. Διαφορετικά, στην περίπτωση που υπήρχε μόνο η interactive λειτουργία του μοντέλου, ο κάθε χρήστης που έπρεπε να επαληθεύσει μια

εγγραφή, θα έπρεπε να εκτελεί την διαδικασία με κάθε άλλο μέλος της blockchain.

Όπως γίνεται εύκολα αντιληπτό, το πλεονέκτημα του μοντέλου ZPK είναι η διαφύλαξη της ιδιωτικότητας της πληροφορίας. Γίνεται γνωστή μόνο η ουσία της πληροφορίας που απαιτείται για συγκεκριμένο σκοπό, χωρίς να αποκαλύπτονται επιπλέον λεπτομέρειες για αυτήν, που στην πραγματικότητα είναι περιττές. Αυτό έχει ιδιαίτερη σημασία στην ασφάλεια των επικοινωνιών. Ένας κακόβουλος χρήστης που θα «παρακολουθεί» το κανάλι επικοινωνίας, δε θα μπορέσει να αποκτήσει ποτέ γνώση της μυστικής πληροφορίας, καθώς αυτή δεν θα επικοινωνηθεί ποτέ.

4.6.2 Μειονεκτήματα

Όπως όμως είναι αναμενόμενο, το ZPK δεν είναι ένα τέλειο μοντέλο. Ένα από τα βασικά του μειονεκτήματα προκύπτει από τον τρόπο λειτουργίας του, άρα είναι δομικό κι έτσι δεν μπορεί να αναιρεθεί πλήρως. Ο μηχανισμός της επαλήθευσης με τις συνεχείς ερωταποκρίσεις είτε πρόκειται για την interactive, είτε για την non-interactive λειτουργία δεν επιβεβαιώνει με απόλυτη βεβαιότητα σε ποσοστό εκατό τοις εκατό τον ισχυρισμό. Αυτό που κάνει, είναι να ελαχιστοποιήσει όσο είναι δυνατόν περισσότερο την πιθανότητα του λάθους. Πράγματι, όταν γίνουν *N* ερωταποκρίσεις (challenge – response) και για μεγάλες τιμές του *N*, τότε η πιθανότητα κάποιος κακόβουλος χρήστης να «μαντέψει» τις σωστές απαντήσεις κάθε φορά και να επικυρώσει έναν ψευδή ισχυρισμό γίνονται σχεδόν μηδενικές, αλλά ποτέ ίσες με το μηδέν (σε ένα δυαδικό σύστημα η πιθανότητα είναι $0,5^N$). Ένα ακόμη μειονέκτημα του ZPK, είναι πως είναι αρκετά «κοστοβόρο». Στην περίπτωση της interactive λειτουργίας, απαιτεί πολλές αλληλεπιδράσεις μεταξύ του prover και του verifier κι έτσι δημιουργεί μεγάλο όγκο δεδομένων στο δίκτυο (traffic). Στην περίπτωση της non-interactive λειτουργίας, απαιτούνται πολλοί υπολογισμοί από τον verifier προκειμένου να επιβεβαιώσει την ορθότητα της πληροφορίας που ερευνά. Αυτό καθιστά την εφαρμογή της λειτουργίας αυτής δύσκολη σε συσκευές με χαμηλότερη επεξεργαστική ισχύ (αν και τα τελευταία χρόνια έχουν προταθεί λύσεις που μειώνουν κατά πολύ την απαίτηση αυτή και την καθιστούν δυνατή ακόμα και σε συσκευές IoT (Schukat and Flood 2014:1–5)). Τέλος, το μοντέλο ZPK είναι τόσο ικανό να διαφυλάσσει μυστικές πληροφορίες που εάν οι κάτοχοί τους τις απωλέσουν, τότε αυτές χάνονται για πάντα. Πράγματι, το μόνο που θα έχει παραμείνει (πχ. σε μια εγγραφή σε blockchain) είναι η απόδειξη της κατοχής του μυστικού αυτού και όχι το μυστικό καθαυτό.

4.6.3 Πρακτικές Εφαρμογές του μοντέλου

Το μοντέλο ZKP έχει ήδη βρει μερικές πρακτικές εφαρμογές. Μία από τις πιο γνωστές αφορά τον τραπεζικό όμιλο ING, ο οποίος χρησιμοποιεί μια παραλλαγή του μοντέλου με όνομα Αποδείξεις Διαστημάτων Μηδενικής Γνώσης (Zero-Knowledge Range Proofs, ZKRP). Το ZKRP, επιτρέπει την απόδειξη του ισχυρισμού, πως ένας αριθμός βρίσκεται εντός ορισμένου διαστήματος (range). Αυτό μπορεί να επιτρέψει, για παράδειγμα, σε έναν πελάτη της τράπεζας να αποδείξει πως ο μισθός του ανήκει σε ένα ορισμένο διάστημα επιτρέποντάς του έτσι να αιτηθεί έκδοση δανείου, χωρίς να αποκαλύψει το ακριβές ποσό του μισθού του. Το σημαντικότερο όμως είναι, πως αυτό θα βοηθήσει τους οικονομικούς φορείς να πλησιάσουν με περισσότερη εμπιστοσύνη τις τεχνολογίες blockchain καθώς η εφαρμογή του μοντέλου μηδενικής γνώσης μέσω της προστασίας της ιδιωτικότητας που προσφέρει, ικανοποιεί τις προσταγές του Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR). Μια άλλη γνωστή εφαρμογή του ZKP, είναι στην blockchain του γνωστού κρυπτονομίσματος zCash, που υλοποιεί την τεχνολογία Μηδενικής Γνώσης Μη-Αλληλεπιδραστικό Συνοπτικό Επιχείρημα Γνώσης (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, zkSNARKs).

4.6.4 Παραδείγματα – Υλοποιήσεις κβαντο-ανθεκτικών αλγορίθμων

Το Picnic, είναι το μοναδικό σχήμα ψηφιακών υπογραφών που βασίζεται στο μοντέλο ZKP και κατάφερε να προκριθεί στον δεύτερο γύρο αξιολόγησης του NIST. Η ασφάλειά του ανάγεται σε αυτή της κρυπτογραφίας αλγορίθμων συμμετρικού κλειδιού που θεωρούνται ανθεκτικοί σε «επιθέσεις» από κβαντικούς υπολογιστές. Για να το πετύχει αυτό, το Picnic, κατασκευάζει το ζεύγος κλειδιών (δημοσίου-ιδιωτικού) έτσι ώστε να ισχύει PublicKey = F(SecretKey), όπου F μια μονόδρομη συνάρτηση που υλοποιείται με την χρήση κρυπτογραφικού αλγορίθμου τμήματος (block cipher). Το τμήμα του Picnic που συνδέεται με το μοντέλο απόδειξης μηδενικής γνώσης, υλοποιείται με την χρήση κρυπτογραφικών πρωτοκόλλων που ανήκουν στην κατηγορία «υπολογισμών με ασφάλεια από πολλά μέρη» (Secure Multi-Party Computation, Secure MPC), μια διαδικασία όπου t μέρη λαμβάνουν ένα τμήμα μιας μυστικής πληροφορίας που μπορεί να χρησιμοποιηθεί για την εύρεση του ιδιωτικού κλειδιού με τέτοιο τρόπο ώστε εάν t-1 μέρη συνδυάσουν τα τμήματα της πληροφορία τους, να μην είναι δυνατό να μάθουν οτιδήποτε σχετικό με την αρχική μυστική πληροφορία (στη γενικότερη περίπτωση, t-k μέρη δεν επαρκούν, αν ανταλλάξουν πληροφορίες μεταξύ τους, να ανακτήσουν το κοινό μυστικό, όπου το k αποτελεί σχεδιαστική παράμετρο του πρωτοκόλλου). Επιπλέον, υλοποιείται

ειδικό σχήμα για challenges με την χρήση hash συναρτήσεων που καλείται Σχέδιο Δέσμευσης (Commitment Scheme) και μαζί με το MPC, καθιστούν την παραγόμενη υπογραφή μηδενικής γνώσης – δηλαδή δεν μπορεί να παραχθεί καμία γνώση για το ιδιωτικό κλειδί από αυτήν (Dinur 2018:11–16).

Οι υπογραφές του Picnic είναι μεγάλες σε μέγεθος, οι χρόνοι υπογραφής και επαλήθευσης είναι αργοί, ενώ το μέγεθος των δημοσίων κλειδιών είναι μικρό. Πρόκειται για ένα σχετικά νέο σχήμα με αναφορές για επιτυχημένες επιθέσεις εναντίον του. Παρόλα αυτά, λόγω του αρθρωτού του σχεδιασμού ο οποίος βασίζεται σε συνάρτηση hash και block cipher, παρουσιάζει δυνατότητες επέκτασης με ευέλικτο τρόπο (Alagic et al 2019:17).

Κεφάλαιο 5

Σύγκριση Μετα-Κβαντικών Κρυπτογραφικών Σχημάτων

Οι κρυπτογραφικοί αλγόριθμοι που εξετάσαμε παραπάνω ανταγωνίζονται καθημερινά στον στίβο που θα καθορίσει ποιοι θα υπερισχύσουν και θα αναλάβουν να μεταφέρουν την κρυπτογραφία σε μια νέα εποχή με νέες δυνατότητες αλλά και προκλήσεις με μεγαλύτερη αυτή της έλευσης των κβαντικών υπολογιστών. Η εξέλιξη των αλγορίθμων είναι συνεχής αφού διαρκώς αναζητούνται τρόποι βελτίωσής τους, ενώ νέες ιδέες εμφανίζονται (κι εξαφανίζονται) σε τακτά χρονικά διαστήματα. Είναι βέβαιο, πως καθώς εξελίσσεται και η αξιολόγηση του NIST, οι αλγόριθμοι αυτοί θα αλλάζουν σύμφωνα με τις υποδείξεις του ή μπορεί να έχουμε συγχωνεύσεις αλγορίθμων ακόμα και από διαφορετικές οικογένειες σχημάτων προκειμένου να επιτευχθεί το επιθυμητό αποτέλεσμα.

Όπως είναι αναμενόμενο, η ανθεκτικότητα σε κβαντικούς υπολογιστές, δεν έρχεται χωρίς κόστος οποιοδήποτε και αν είναι το σχήμα που εξετάζουμε, σε σύγκριση με τους κλασικούς αλγορίθμους που χρησιμοποιούνται σήμερα. Οι κβαντοανθεκτικοί αλγόριθμοι, παρουσιάζουν λοιπόν μεγαλύτερου μεγέθους δημόσια κλειδιά, ψηφιακές υπογραφές, κρυπτοκείμενα και χρόνους υπογραφών από ότι οι RSA, ECC και DH. Μάλιστα, σε περιπτώσεις που έγινε προσπάθεια τα μεγέθη και οι χρόνοι αυτοί να μειωθούν σε συγκεκριμένους αλγορίθμους, οδήγησε σε επιτυχημένες επιθέσεις εναντίον τους. Ακολουθεί μια γενικότερη σύγκριση κρυπτοσχημάτων για κάθε κατηγορία που επιθυμούμε να ασφαλίσουμε από κβαντικούς υπολογιστές (Niederhagen and Waidner, Prof. Dr. Michael 2017:19). Η σύγκριση γίνεται βάση των μέχρι τώρα γενικότερων αποτελεσμάτων επιδόσεων των σχημάτων, λαμβάνοντας όμως υπόψιν και τους

υποψήφιους αλγορίθμους στην αξιολόγηση του NIST. Παράλληλα παρατίθενται συγκριτικοί πίνακες για επιλεγμένους αλγορίθμους (που συμμετέχουν ή όχι στην αξιολόγηση NIST) σε σύγκριση πάντα με τους κλασικούς αντίστοιχους αλγορίθμους. Οι μετρήσεις που αναφέρονται στους πίνακες, δεν είναι εργαστηριακές (benchmarks) κι επομένως δεν είναι ακριβής. Παρουσιάζονται για γενικότερη σύγκριση και αποτελούν συλλογή πληροφοριών από διάφορες πηγές (Campagna et al 2014:20).

- Ψηφιακές Υπογραφές (Digital Signatures)

  Στην κατηγορία των κβαντο-ανθεκτικών ψηφιακών υπογραφών, το σχήμα που φαίνεται να συγκεντρώνει τις περισσότερες πιθανότητες να αποτελέσει πρότυπο, είναι αυτό των hash-based ψηφιακών υπογραφών. Τα δημόσια κλειδιά τους έχουν μέγεθος 64 – 1.056 bytes που είναι πολύ κοντά με αυτό των κλασικών υπογραφών που έχουμε σήμερα με χρήση των RSA και ECC. Αντίθετα, το μέγεθος των υπογραφών που παράγουν είναι αρκετά μεγαλύτερο από αυτό των κλασικών υπογραφών και φτάνει τα 2,5 – 41 kB. Παράλληλα, εξετάζονται και τα σχήματα κβαντο-ανθεκτικών υπογραφών που βασίζονται σε πολυώνυμα και τα οποία μπορεί να χρειάζονται δημόσια κλειδιά μεγάλου μεγέθους 500 kB – 1 MB, αλλά παράγουν υπογραφές πολύ μικρού μεγέθους (Niederhagen and Waidner, Prof. Dr. Michael 2017:19) . Τα βασισμένα σε κώδικα σχήματα, θεωρούνται τα πιο αδύναμα καθώς υστερούν σε επιδόσεις από τα υπόλοιπα (Campagna et al 2014:18).

Αλγόριθμοι		Χρόνος Παραγωγής Κλειδιού (σύγκριση με RSA)	Χρόνος Υπογραφής (σύγκριση με RSA)	Χρόνος Επαλήθευσης Υπογραφής (σύγκριση με RSA)	Δημόσιο Κλειδί (μέγεθος σε bits για την επίτευξη 128 bits ασφάλειας)	Ιδιωτικό Κλειδί (μέγεθος σε bits για την επίτευξη 128 bits ασφάλειας)	Υπογραφή (μέγεθος σε bits)
Post-Quantum	**XMSS** (hash-based, stateful, για 2^{20} υπογραφές)	100000	2	0,2	7296	152	19608
	BLISS (lattice-based, δεν κατέθεσε πρόταση στον NIST παρότι θεωρείται	0,005	0,02	0,01	7000	2000	5600

	ισχυρός)(Howe et al 2015:41:18)						
	Rainbow (multivariate)	20	0,02	0,02	842400	561352	264
Classic	**RSA**	50	1	0,01	3072	24576	3072
	DSA	0,2	0,2	0,2	3072	3328	3072
	ECDSA	0,05	0,05	0,05	512	768	512

Πίνακας 2. Σύγκριση Μετα-κβαντικών αλγορίθμων σε σχήματα ψηφιακών υπογραφών (Campagna et al 2014:21)

- Κρυπτογράφηση Δημοσίου Κλειδιού (Public Key Encryption, PKE)

  Σε ότι αφορά την κβαντο-ανθεκτική κρυπτογράφηση δημοσίου κλειδιού, υπάρχει μεγάλη αισιοδοξία της επιστημονικής κοινότητας στα σχήματα των McEliece και Niederreiter με χρήση κωδικών Goppa. Μπορεί να παρουσιάζουν πολύ μεγάλα δημόσια κλειδιά συγκριτικά με τα κλασικά σχήματα (μεγέθους περίπου 1 MB), αλλά το κρυπτοκείμενο τους είναι πολύ μικρό. Σχήματα που βασίζονται σε κρυπτογραφία πλέγματος θεωρούνται επίσης αξιόλογα, αλλά ακόμη δεν έχουν τύχει ανάλογης εμπιστοσύνης (Niederhagen and Waidner, Prof. Dr. Michael 2017:19).

Αλγόριθμοι		Χρόνος Παραγωγής Κλειδιού (σύγκριση με χρόνο αποκρυπτογράφησης RSA)	Χρόνος Αποκρυπτογράφησης (σύγκριση με χρόνο αποκρυπτογράφησης RSA)	Χρόνος Κρυπτογράφησης (σύγκριση με χρόνο αποκρυπτογράφησης RSA)	Δημόσιο Κλειδί (μέγεθος σε bits για την επίτευξη 128 bits ασφάλειας)	Ιδιωτικό Κλειδί (μέγεθος σε bits για την επίτευξη 128 bits ασφάλειας)	Κρυπτοκείμενο (μέγεθος σε bits)
Post-Quantum	**McEliece** (code-based)	2	0,5	0,01	1537536	64861	2860
	NTRU (lattice-based)	5	0,05	0,05	4939	1398	4939
Classic	**RSA**	50	1	0,01	3072	24576	3072
	DSA	0,2	0,2	0,2	3072	3238	3072
	ECDSA	0,05	0,05	0,05	256	256	512

Πίνακας 3. Σύγκριση Μετα-κβαντικών αλγορίθμων σε σχήματα κρυπτογράφησης (Campagna et al 2014:20)

- Μηχανισμός Ανταλλαγή Κλειδιών (Key Exchange Mechanism, KEM)

  Κβαντο-ανθεκτικοί μηχανισμοί ανταλλαγής κλειδιών μπορούν να κατασκευαστούν από σχήματα κρυπτογράφησης δημοσίου κλειδιού τα οποία δημιουργούν και μεταδίδουν νέα κλειδιά για κάθε συνεδρία. Ένα τέτοιο σχήμα είναι το βασισμένο σε κρυπτογραφία πλέγματος NewHope το οποίο όμως αποστέλλει πακέτα των 2 kB σε αντίθεση με τα 32 – 64 bytes του κλασικού ECDH. Το supersingular-isogeny του Diffie-Hellman (SIDH) από την άλλη, στέλνει πακέτα 564 bytes, αλλά αυτό από μόνο του δεν είναι αρκετό, καθώς το συγκεκριμένο σχήμα είναι πολύ νέο και δεν έχει κερδίσει ακόμη την εμπιστοσύνη της επιστημονικής κοινότητας.

Αλγόριθμοι		Μέγεθος Δεδομένων (bytes)
Post-Quantum	**NewHope** (lattice -based)	2860
	SIDH (supersingular isogenies-based)	4939
Classic	**DH**	3072
	ECDH	3072

Πίνακας 4. Σύγκριση Μετα-κβαντικών αλγορίθμων ως μηχανισμοί ανταλλαγής κλειδιών (Niederhagen and Waidner, Prof. Dr. Michael 2017:20)

Πέρα όμως από τα τεχνικά χαρακτηριστικά και τις επιδόσεις των αλγορίθμων που θα κρίνουν την πορεία και την θέση τους στην μετα-κβαντική εποχή, υπάρχουν και άλλα βασικά κριτήρια που πρέπει να ληφθούν σοβαρά υπόψιν προκειμένου αυτοί να βρουν πρακτική εφαρμογή.

1. Προτυποποίηση

   Είναι πολύ σημαντικό, η διαδικασία που έχει ξεκινήσει ο NIST το 2016, να συνεχιστεί αλλά και να υιοθετηθεί και από τον αντίστοιχο Ευρωπαϊκό φορέα που είναι το Ινστιτούτο Προτυποποίησης Ευρωπαϊκών Τηλεπικοινωνιών (European Telecommunications Standards Institute, ETSI), ώστε να δημιουργηθούν πρότυπα που θα βασίζονται στην ανάδραση από τον ακαδημαϊκό αλλά και βιομηχανικό χώρο (Niederhagen and Waidner, Prof. Dr. Michael 2017:8).

2. Υλοποίηση

   Η υλοποίηση των μετα-κβαντικών σχημάτων, θα πρέπει να γίνει με τέτοιο τρόπο ώστε να είναι συμβατή με το υπάρχων λογισμικό και υλισμικό (τουλάχιστον των

τελευταίων ετών), ώστε να μην καταστούν αυτά ξεπερασμένα κι επικίνδυνα προς χρήση. Παράλληλα, κάθε νέο λογισμικό και συσκευές (πχ έξυπνες κάρτες, usb tokens ψηφιακών υπογραφών) που θα αναπτυχθεί, θα πρέπει να λάβει υπόψιν στον σχεδιασμό του και να υλοποιεί την μετα-κβαντική κρυπτογραφία (Niederhagen and Waidner, Prof. Dr. Michael 2017:21).

3. Δοκιμές

   Η εμπιστοσύνη στα κρυπτογραφικά συστήματα είναι κάτι που κερδήθηκε με το πέρασμα του χρόνου στο παρελθόν. Τέτοια πολυτέλεια χρόνου, είναι πολύ πιθανόν να μην υπάρχει με τα κβαντο-ανθεκτικά σχήματα (Niederhagen and Waidner, Prof. Dr. Michael 2017:6). Για τον λόγο αυτό είναι αποφασιστικής σημασίας να γίνουν εκτεταμένες δοκιμές και έλεγχοι στα σχήματα αυτά, αλλά και στις υλοποιήσεις τους σε λογισμικό και υλισμικό (Niederhagen and Waidner, Prof. Dr. Michael 2017:21).

4. Ενημέρωση – Εκπαίδευση

   Ίσως το πιο σημαντικό προαπαιτούμενο κομμάτι για την εφαρμογή των νέων κβαντο-ανθεκτικών κρυπτοσυστημάτων είναι η ενημέρωση του κοινού και ιδιαιτέρως των ατόμων που είναι σε καίριες διευθυντικές θέσεις, των πολιτικών και των μηχανικών υπολογιστών και λογισμικού για την σημασία των συστημάτων αυτών. Δυστυχώς, ακόμη και σήμερα υπάρχουν αρκετές παρανοήσεις σχετικά με τους κβαντικούς υπολογιστές και τις πραγματικές τους δυνατότητες (Niederhagen and Waidner, Prof. Dr. Michael 2017:8). Είναι ζωτικής σημασίας, να παρουσιαστούν οι θετικές συνέπειες από τις εφαρμογές τους σε τομείς όπως η φυσική, η χημεία, η βιολογία, η ιατρική, κ.α. αλλά και να τονιστούν οι κίνδυνοι που ελλοχεύουν από την κακόβουλη χρήση των δυνατοτήτων των υπολογιστών αυτών (Niederhagen and Waidner, Prof. Dr. Michael 2017:21). Τότε μόνο, ο κόσμος στο σύνολό του θα κατανοήσει την ανάγκη ύπαρξης κβαντο-ανθεκτικών σχημάτων κρυπτογραφίας και θα αγκαλιάσει με θέρμη κάθε προσπάθεια που οδηγεί σε μια ασφαλέστερη μετα-κβαντική εποχή.

Κεφάλαιο 6

Η Λύση του Κβαντο-Ανθεκτικού Καταλόγου

Στο κεφάλαιο 4, είδαμε τα κρυπτογραφικά σχήματα που είναι υποψήφια να μας μεταφέρουν με ασφάλεια στην εποχή των κβαντικών υπολογιστών. Υλοποιήσεις και μοντέλα έχουν αναπτυχθεί για κάθε ένα από αυτά και εξελίσσονται διαρκώς. Στο κεφάλαιο αυτό, θα μελετήσουμε μία από αυτές τις λύσεις, η οποία εφαρμόζεται και αφορά blockchain και μάλιστα στον τομέα των κρυπτονομισμάτων. Η λύση αυτή ονομάζεται Κβαντο-Ανθεκτικός Κατάλογος (Quantum Resistant Ledger - QRL) και βασίζεται στο σχήμα των hash-based υπογραφών. Πρόκειται για μια επαγγελματική πλατφόρμα δημόσια και ανοικτή blockchain, εξωτερικά ελεγχόμενη, η οποία υπόσχεται ασφάλεια τόσο απέναντι σε απειλές επιθέσεων που υπάρχουν σήμερα από κλασικούς υπολογιστές, όσο και ανθεκτικότητα σε αυτές που η θεωρία αναφέρει πως θα παραχθούν από κβαντικούς υπολογιστές στο μέλλον (QRL Foundation 2019:1).

6.1 Σχήμα υπογραφής

Το σχήμα υπογραφής του QRL είναι stateful και συμβατό με το σχέδιο συστάσεων (draft recommendations) του NIST για τις μετα-κβαντικές υπογραφές (Cooper 2019:14–18) .

6.1.1 Δομή

Το QRL χρησιμοποιεί τα υπερδέντρα (hypertrees) προκειμένου να δομήσει το επιθυμητό

σχήμα υπογραφής. Κάθε τέτοιο hypertree, αποτελείται από ένα ή περισσότερα XMSS trees, ο αριθμός των οποίων θα καθορίσει και το διαθέσιμο πλήθος ψηφιακών υπογραφών αλλά και το μέγεθος που θα έχουν αυτές. Υπενθυμίζουμε, πως σε μια τέτοια δομή, καθώς αυξάνεται ο αριθμός των δέντρων που συνιστούν ένα hypertree, αυξάνεται εκθετικά το πλήθος των διαθέσιμων υπογραφών ενώ ταυτόχρονα αυξάνεται γραμμικά το μέγεθος τους σε bytes. Για παράδειγμα, ένα XMSS hypertree αποτελούμενο από 4 δέντρα, με βάθος j = 3, ύψος h = 5 το οποίο θα παρείχε 2^{20} ψηφιακές υπογραφές, κατασκευάζεται σε λιγότερο από 3 δευτερόλεπτα κι έχει υπογραφή μεγέθους 8,84kB. Μια αντίστοιχης δυναμικής δομή αποτελούμενη από ένα μόνο δέντρο XMSS, χρειάζεται περίπου 466 δευτερόλεπτα να κατασκευαστεί όμως παρέχει υπογραφές μεγέθους 2,69kB περίπου (Matier and Waterland 2016:10).

Το QRL προτείνει αυτά τα hypertrees να ξεκινούν από ένα μόνο δέντρο XMSS και να επεκτείνονται ασύμμετρα με την προσθήκη επιπλέον XMSS δέντρων όταν απαιτούνται περισσότερες υπογραφές. Αυτό δίνει την δυνατότητα στον χρήστη να μπορεί να παράγει άμεσα διευθύνσεις καταλόγου (ledger addresses) blockchain και να υπογράφει ψηφιακά συναλλαγές χωρίς να έχει να αντιμετωπίσει καθυστερήσεις για την δημιουργία μεγάλων XMSS δενδροειδών δομών (Matier and Waterland 2016:10). Έτσι, ένα τυπικό QRL Hypertree αναμένεται να έχει (και να μην χρειαστεί να υπερβεί τις παρακάτω προδιαγραφές) (Matier and Waterland 2016:11):

- βάθος $j = 0$, με $j \in \{0 \leq x \leq 2\}$,
- ύψος $h = 12$, με $h \in \{1 \leq x \leq 14\}$
- ελάχιστο μέγεθος υπογραφής 2,21kB
- μέγιστο μέγεθος υπογραφής 7,65 kB

6.1.2 Υπογραφή

Σε ότι αφορά τις υπογραφές, το QRL χρησιμοποιεί το μοντέλο των W-OTS+ όπως αυτό περιεγράφηκε παραπάνω. Ως PRF συνάρτηση χρησιμοποιείται μια παραλλαγή της HMAC και συγκεκριμένα η Deterministic Random Bit Generator HMAC (Matier and Waterland 2016:12) (HMAC_DRBG όπως περιγράφεται στο πρότυπο NIST SP 800-90A (Woodage and Shumow 2018:6)). Με την χρήση της hash συνάρτησης SHA-256 και επιλεγμένη μεταβλητή w = 16, το μοντέλο αυτό προσφέρει ασφάλεια από brute-force επιθέσεις κλασικών και κβαντικών υπολογιστών ίση με 196 bits, η οποία σύμφωνα με τις εκτιμήσεις είναι αρκετή μέχρι το έτος 2164 (Matier and Waterland 2016:10).

6.1.3 Παράδειγμα

Έστω πως έχουμε το πιο μεγάλο QRL Hypertree σύμφωνα με τα άνω όρια των προδιαγραφών τους, δηλαδή $j = 2$ και $h = 14$ που θα μπορεί να δημιουργήσει μέχρι $2^{14} = 16.384$ υπογραφές. Έστω μήνυμα m προς υπογραφή και n ο δείκτης του ζεύγους OTS κλειδιών που χρησιμοποιείται από κάθε δέντρο XMSS του hypertree. Μια υπογραφή στην περίπτωση αυτή θα απαιτούσε (Matier and Waterland 2016:11):

- από το δέντρο υπογραφής (signature tree), δηλαδή για $j = 2$: την OTS υπογραφή του m, τον δείκτη n, την απόδειξη αυθεντικότητας (authentication path) του Merkle tree και την ρίζα του δέντρου αυτού (signature Merkle tree root),
- από το δέντρο πιστοποίησης (certification tree), δηλαδή για $j = 1$: την OTS υπογραφή του Merkle root του signature tree (j=2), το n, το authentication proof του Merkle tree και την Merkle root του certification tree,
- και τέλος, από το αρχικό δέντρο XMSS, δηλαδή για $j = 0$: την OTS υπογραφή του Merkle root για το certification tree (j=1), το n, το authentication proof του Merkle tree και την Merkle root.

Για την πιστοποίηση της εγκυρότητας της παραπάνω υπογραφής, θα χρειαζόταν κατά αντιστοιχία:

- Από το μήνυμα m και την υπογραφή, θα παραχθεί το OTS public key. Επιπλέον, από τον έλεγχο και με τη χρήση του signature Merkle tree authentication proof, κατασκευάζεται η ρίζα (root) του signature Merkle tree, που θα αποτελέσει το μήνυμα για την επόμενη OTS υπογραφή.
- Το παραπάνω μήνυμα μαζί με την αντίστοιχη OTS υπογραφή χρησιμοποιούνται για την παραγωγή του επόμενου OTS public key. Αυτή τη φορά, το certification Merkle tree authentication proof, χρησιμοποιείται για τον υπολογισμό του certification Merkle tree root, που με τη σειρά του αποτελεί το μήνυμα για το παραπάνω certification Merkle tree.
- Η παραπάνω διαδικασία επαναλαμβάνεται για όλα τα certification Merkle trees μέχρι να φτάσουμε στο αρχικό XMSS tree (j=0). Εάν με την ίδια διαδικασία, υπολογιστεί και επαληθευτεί και η root του αρχικού δέντρου τότε η υπογραφή του αρχικού μηνύματος m, θεωρείται έγκυρη.

Αξίζει να σημειωθεί, πως μέσα σε μια QRL υπογραφή οι τιμές των root για κάθε δέντρο μπορούν να παραληφθούν εάν η διεύθυνση (address) ledger του αποστολέα-υπογράφοντα είναι γνωστή. Αυτό ισχύει επειδή η ledger address παράγεται

υπολογιστικά από την root του αρχικού XMSS δέντρου (j=0). Τέλος, μιας και όλο αυτό το σχήμα υπογραφής είναι stateful, στο QRL πορτοφόλι (wallet) του χρήστη για δεδομένη public ledger address, χρειάζεται να διατηρείται και να ενημερώνεται η τιμή n για κάθε δέντρο που παράγεται μέσα στο hypertree της διεύθυνσης αυτής (Matier and Waterland 2016:11).

6.2 Σχεδιαστικές παράμετροι του QRL κρυπτονομίσματος

Εφόσον αναφερόμαστε σε ledger, δηλαδή blockchain, τότε είναι απαραίτητο να διευκρινιστούν και οι σχετικές παράμετροι που αφορούν τα blocks όπως το μέγεθος, ο χρόνος κατασκευής για το καθένα, ο μηχανισμός συναίνεσης, ανταμοιβές (εφόσον υπάρχουν) των miners καθώς και τα τέλη συναλλαγών. Επιπροσθέτως, μιας και το QRL εντάσσεται στην κατηγορία των κρυπτονομισμάτων, χρειάζεται να γίνει αναφορά στην έκδοση, τις μονάδες και τις υποδιαιρέσεις του κρυπτονομίσματος αυτού αλλά και να αναλυθεί η δομή των ledger διευθύνσεων των χρηστών της blockchain του QRL.

6.2.1 Τεμάχια (Blocks)

Σε ό,τι αφορά το μέγεθος κάθε block, το QRL υιοθετεί μια προσαρμοστική λύση, βασισμένη στην πρόταση της BitPay, σύμφωνα με την οποία το μέγεθος κάθε block αυξάνεται βάσει ενός πολλαπλασιαστή x, που σχετίζεται με την μέση τιμή μεγέθους y, των τελευταίων z blocks. Τα x, z θα αποτελούν αυστηρούς και άκαμπτους κανόνες με τους οποίους συναινεί κάθε μέλος του δικτύου της blockchain. Η μέση τιμή y από την άλλη, χρησιμοποιείται προκειμένου το μέγεθος των blocks να μην ορίζεται από κακόβουλες πράξεις χρηστών που προσπαθούν να συμπεριλάβουν μηδενικά ή πολύ μεγάλου μεγέθους blocks στην αλυσίδα. Έτσι, το μέγιστο μέγεθος που μπορεί να φτάσει ένα block μπορεί να είναι: $b_{max} = x\,y$ (Matier and Waterland 2016:13).

Ο χρόνος δημιουργίας νέου block ορίζεται από το QRL στα 60 δευτερόλεπτα. Ενδεικτικά, στο Bitcoin ο αντίστοιχος χρόνος είναι αυτή τη στιγμή περίπου στα 10 λεπτά, ενώ νεότερα κρυπτονομίσματα έχουν επιτύχει πολύ χαμηλότερους χρόνους, όπως για παράδειγμα το Ethereum που χρειάζεται περίπου 15 δευτερόλεπτα χωρίς αρνητικές επιπτώσεις στο επίπεδο ασφάλειας της blockchain τους (Matier and Waterland 2016:12).

Κάθε νέο block που δημιουργείται στην QRL blockchain, θα περιέχει μια εγγραφή συναλλαγής (transaction) στην οποία θα αναφέρεται η public ledger address του miner που δημιούργησε το εν λόγω block. Στην διεύθυνση αυτή, θα αποστέλλονται το σύνολο των τελών συναλλαγών (transaction fees) που περιέχονται στο block μαζί με ένα επιπλέον ποσό-έπαθλο. Το ποσό αυτό, θα επαναϋπολογίζεται από τον mining node μετά από την δημιουργία κάθε νέου block και θα συσχετίζεται με το πρόγραμμα έκδοσης των κρυπτονομισμάτων όπως θα δούμε και παρακάτω (Matier and Waterland 2016:12).

6.2.2. Μηχανισμός Συναίνεσης

Το QRL χρησιμοποιεί τον Proof of Work μηχανισμό συναίνεσης. Μέχρι πρόσφατα χρησιμοποιούσε τον αλγόριθμο CryptoNight για την λειτουργία του μηχανισμού αυτού, ενώ μόλις πρόσφατα τον αντικατέστησε με τον RandomX σε καθολική αναβάθμιση – «διακλάδωση» (hardfork) που έλαβε χώρα μόλις στις 8 Απριλίου 2020 (Matier 2020a:1). Ο RandomX είναι ειδικά σχεδιασμένος για επεξεργαστές γενικής χρήσης (όπως αυτοί που χρησιμοποιούνται σε υπολογιστές οικιακής χρήσης) και χρησιμοποιεί ειδικές τεχνικές εκτέλεσης τυχαίου κώδικα για να παρέχει ανθεκτικότητα σε κυκλώματα ειδικού σκοπού (Tevador 2020:1). Τα κυκλώματα αυτά καλούνται Ολοκληρωμένα Κυκλώματα για Συγκεκριμένες Εφαρμογές (Application Specific Integrated Circuits, ASICs) και Προγραμματιζόμενες Συστοιχίες Πυλών Ειδικού Πεδίου (Field Programmable Gate Arrays, FPGAs) και αφορούν εξειδικευμένο υλισμικό (hardware) που κατασκευάζουν εταιρείες με μοναδικό σκοπό αυτό να χρησιμοποιηθεί για mining (ατομικό ή σε συστοιχίες – farms). Αυτές οι συσκευές όμως καταλήγουν να αποτρέπουν τους απλούς χρήστες από την διαδικασία του mining καθώς δεν μπορούν να τις συναγωνιστούν με τους οικιακούς τους υπολογιστές ούτε να τις προμηθευτούν λόγω κόστους, με αποτέλεσμα τελικά να χάνουν το ενδιαφέρον τους για τις blockchains γενικότερα. Για τον λόγο αυτό, αναπτύσσονται ειδικοί αλγόριθμοι σαν τον RandomX που καλούνται ανθεκτικοί σε ASICs (ASICs resistant) και είναι σχεδιασμένοι με τέτοιο τρόπο ώστε να μην δίνουν πλεονέκτημα σε αυτές τις συσκευές ειδικού σκοπού σε ότι αφορά το mining, καθιστώντας παράλληλα κοστοβόρα και χρονοβόρα την διαδικασία της σχεδιαστικής προσαρμογής τους για να μπορέσουν τελικά να άρουν αυτή την ανθεκτικότητα των αλγορίθμων. Στο τέλος όμως, αργά ή γρήγορα αυτό συμβαίνει και για αυτό τον λόγο απώτερος στόχος του QRL είναι τελικά να αντικαταστήσει τον μηχανισμό συναίνεσης Proof of Work με έναν Proof of Stake ή έστω ένα υβριδικό μοντέλο PoW-PoS.

6.2.3 Τέλη συναλλαγών

Το QRL έχει θεσπίσει, σε επίπεδο πρωτοκόλλου, μια ελάχιστη αξία τέλους συναλλαγής (transaction fee) για κάθε συναλλαγή. Κάθε συναλλαγή για την οποία καταβάλλεται τουλάχιστον το ελάχιστο τέλος, θεωρείται έγκυρη. Από εκεί και πέρα, οι miners/nodes, ανταγωνίζονται μεταξύ τους για τα τέλη που ζητούν για κάθε συναλλαγή (συγκεκριμένα αλλάζοντας σχετική μεταβλητή στο αρχείο διαμόρφωσης config.py (Ttechno et al 2020:1)). Επιτρέπεται δηλαδή στην «αγορά» να καθορίσει την αξία αυτή, όπως αρμόζει περισσότερο σε μια δημόσια και ανοικτή blockchain, και όχι σε κάποιον αλγόριθμο όπως γίνεται στην περίπτωση του Bitcoin. Έτσι, οι miners θα μπορούν να επιλέγουν συγκεκριμένες συναλλαγές που βρίσκονται σε αναμονή προκειμένου να προστεθούν στο επόμενο block (Matier and Waterland 2016:12)

6.2.4 Μονάδες – Έκδοση κρυπτονομίσματος QRL

Το QRL χρησιμοποιεί ως μονάδα βάσης για το κρυπτονόμισμά του, το ένα quantum (πληθυντικός αριθμός quanta). Υποδιαίρεση του quantum είναι οι μονάδες Shor σε αναλογία: 1 quantum = 10^9 Shor. Σε πλήθος Shor μονάδων μάλιστα, υπολογίζονται και καταβάλλονται τα τέλη συναλλαγών που είδαμε παραπάνω (Matier and Waterland 2016:13).

Σύμφωνα με το QRL foundation, η αρχική έκδοση των κρυπτονομισμάτων είναι ίση με 52 * 10^6 quanta, επιπλέον 13 * 10^6 quanta θα κατανεμηθούν σε σχετικά ιδρύματα και τέλος άλλα 40 * 10^6 quanta θα κατανεμηθούν σε ένα πρόγραμμα έκδοσης που θα ακολουθεί εκθετική μείωση μέχρι το έτος 2218 μ.Χ., ανεβάζοντας έτσι το συνολικό αριθμό στα 105 * 10^6 quanta (Matier and Waterland 2016:14). Υιοθετείται δηλαδή το μοντέλο του Bitcoin το οποίο βασίζεται στην ύπαρξη ενός ανώτατου ορίου έκδοσης κρυπτονομισμάτων και στον ορισμό της αξίας του βάση της έλλειψης του. Από την άλλη, η εκθετική μείωση σε ό,τι αφορά τον ρυθμό έκδοσης των τελευταίων 40 * 10^6 quanta, θα αποτρέψει το φαινόμενο μείωσης στο μισό των επάθλων των miners που ισχύει στο Bitcoin κάθε 210.000 blocks (περίπου κάθε τέσσερα χρόνια και καλείται Bitcoin Halving) (Batabyal 2019:1). Υπολογίζεται πως μέχρι το 2218 μ.Χ. οπότε και θα εκδοθούν τα τελευταία quanta, θα έχουν παραχθεί 105189120 blocks με ρυθμό ενός block ανά 60 δευτερόλεπτα. Εάν θεωρήσουμε ως Z_0 το σημείο από όπου θα ξεκινήσει η εκθετική μείωση στον ρυθμό έκδοσής τους, τότε για κάθε νέο block t από το Z_0 και μετά, τα διαθέσιμα προς προμήθεια quanta θα υπολογίζονται από τον τύπο: $Z_t = Z_0 \, e^{-\lambda t}$. Ο συντελεστής λ υπολογίζεται από

τον τύπο: $\lambda = \ln Z_0 / t$, όπου t είναι το πλήθος των εναπομεινάντων block σύμφωνα με το πρόγραμμα διάθεσης μέχρι τα τελευταία quanta. Κατά αντιστοιχία, το έπαθλο b για κάθε block υπολογίζεται από τον τύπο: $b = Z_{t-1} - Z_t$ (Matier and Waterland 2016:14–15).

6.2.5 Δομή διευθύνσεων λογαριασμών QRL

Οι διευθύνσεις λογαριασμών στο QRL έχουν σχεδιαστεί ώστε να είναι επεκτάσιμες και να υποστηρίζουν διάφορες μορφοποιήσεις και παραμετροποιήσεις.

Όνομα	Bytes	Πλήθος	Περιγραφή
DESC	0 … 2	3	Περιγραφή Διεύθυνσης
DATA	3 … N	N – 3	Το N εξαρτάται από την μορφοποίηση της διεύθυνσης

Πίνακας 5. Δομή διεύθυνσης λογαριασμών QRL (Matier and Waterland 2016:13)

Τα τρία πρώτα bytes κάθε διεύθυνσης περιέχουν πληροφορίες σχετικές με την συνάρτηση hash, το σχήμα υπογραφής, την μορφοποίηση της διεύθυνσης και επιπλέον παραμέτρους.

Όνομα	Bits	Πλήθος	Περιγραφή
HF	0 … 3	4	Συνάρτηση Hash
SIG	4 … 7	4	Σχήμα υπογραφής
P1	8 … 11	4	Παράμετροι 1
AF/P2	12 … 15	4	Μορφοποίηση Διεύθυνσης
P3	16 … 23	8	Παράμετροι 2

Πίνακας 6. Ανάλυση δομής των τριών πρώτων bytes μιας διεύθυνσης QRL (Matier and Waterland 2016:14)

Αυτή τη στιγμή, υποστηρίζονται μόνο η μορφοποίηση διεύθυνσης SHA256_2X και το XMSS ως σχήμα υπογραφής. Έτσι, τα τρία πρώτα bytes διαμορφώνονται ως εξής:

Όνομα	Bits	Πλήθος	Περιγραφή
HF	0 … 3	4	SHA2_256, SHAKE128, SHAKE256
SIG	4 … 7	4	XMSS
P1	8 … 11	4	XMSS Height / 2
AF/P2	12 … 15	4	Μορφοποίηση Διεύθυνσης
P3	16 … 23	8	<δεν χρησιμοποιείται>

Πίνακας 7. Τιμές των πεδίων στα τρία πρώτα bytes μιας διεύθυνσης QRL στην περίπτωση του XMSS (Matier and Waterland 2016:14)

Ακολουθούν οι δυνατές τιμές των πεδίων που εμφανίζονται στα τρία πρώτα bytes μιας QRL διεύθυνσης.

HF – Hash Function (Συνάρτηση Hash)	
Τιμή	**Περιγραφή**
0	SHA256_2X
1	SHAKE128
2	SHAKE256
3 … 15	Κατοχυρωμένα για μελλοντική χρήση

Πίνακας 8. Δυνατές τιμές του πεδίου HF (Matier and Waterland 2016:14)

SIG – Signature Type (Σχήμα Υπογραφής)	
Τιμή	**Περιγραφή**
0	XMSS
1 … 15	Κατοχυρωμένα για μελλοντική χρήση

Πίνακας 9. Πιθανές τιμές του πεδίου SIG (Matier and Waterland 2016:14)

AF – Address Format (Μορφοποίηση Διεύθυνσης)	
Τιμή	**Περιγραφή**
0	SHA256_2X
1 … 15	Κατοχυρωμένα για μελλοντική χρήση

Πίνακας 10. Πιθανές τιμές του πεδίου AF (Matier and Waterland 2016:14)

6.3 Φιλοσοφία – Επόμενη ημέρα

Το QRL αποτελεί την πρώτη blockchain που δημιουργήθηκε με πρωταρχικό στόχο την κβαντο-ανθεκτικότητα. Έτσι, η κατασκευή της έγινε από μηδενική βάση, χωρίς την χρήση μεθόδων ή έτοιμων λύσεων από blockchains που προϋπήρχαν στον χώρο. Αυτό έδωσε το πλεονέκτημα στο QRL να αποφύγει παγίδες και παθογένειες άλλων blockchains αλλά από την άλλη όντας πρωτοπόρος στον τομέα, την κάνει ευάλωτη σε προβλήματα που δεν έχουν προβλεφθεί ή εμφανιστεί σε άλλες υλοποιήσεις ως τώρα.

Η φιλοσοφία που διακατέχει τα ιδρυτικά μέλη του QRL, είναι πως «ποτέ δεν είναι αρκετά νωρίς» σε ότι αφορά τον τομέα της ασφάλειας και ότι η πρόληψη είναι πάντα καλύτερη από την αντίδραση. Για τον λόγο αυτό, η πλατφόρμα του QRL πέρασε με επιτυχία δύο ανεξάρτητους ελέγχους ασφάλειας που έγιναν από την Red4Sec και την x41sec, πράγμα που δεν συνηθίζεται στον τομέα των blockchains (Peter Waterland 2019:1). Μπορεί η κβαντο-ανθεκτικότητα να μοιάζει με «πολυτέλεια» σήμερα, αλλά αυτό είναι κάτι το προσωρινό, μιας και ένα μέλλον με κβαντικούς υπολογιστές θεωρείται αναπόφευκτο. Τονίζουν την λέξη «ανθεκτική» (resistant) στην ονομασία της blockchain τους και προειδοποιούν πως είναι αδύνατο κάποιος να κατασκευάσει – ή να ισχυριστεί πως κατασκεύασε – μια απόλυτα ασφαλή blockchain από επιθέσεις κβαντικών υπολογιστών (quantum proof). Μάλιστα, για να το κάνουν πιο κατανοητό, χρησιμοποιούν το παράδειγμα των αδιάβροχων ρολογιών (water resistant, water proof) λέγοντας πως πάντα θα υπάρχει ένα όριο πάνω από το οποίο κάθε ρολόι θα απωλέσει την ανθεκτικότητά του. Στο QRL, δεν υποστηρίζουν και δεν επιθυμούν το μονοπώλιο. Δεν πιστεύουν πως το να επιβιώσει μια blockchain, ακόμα και αν είναι η δική τους, στην μετακβαντική εποχή (“one chain to rule them all”) είναι καλό για το οικοσύστημα, γιατί έτσι η blockchain αυτή θα γίνει ο βασιλιάς των «χαλασμάτων» (king of the rubble) και ουσιαστικά δεν θα έχει καμία αξία. Αντιθέτως, μια υγιής αγορά όπου το QRL θα είναι ο πρωτοπόρος, θα είναι το καλύτερο και πιο επιθυμητό σενάριο. Συγκεκριμένα, ευαγγελίζονται πως ο συναγωνισμός είναι καλός, η ποικιλία είναι υπέροχη και η δυνατότητα επιλογής απαραίτητη. Για τον λόγο αυτό, υποστηρίζουν έντονα πως όλες οι υπάρχουσες blockchains που αφορούν κρυπτονομίσματα, πρέπει να σκεφτούν άμεσα την επόμενη ημέρα και να θωρακιστούν έναντι κβαντικών επιθέσεων. Τονίζουν, μάλιστα, πως ακόμα και εάν ένα μικρό ποσοστό της τάξης του 5% των πορτοφολιών κρυπτονομισμάτων (cryptocurrency wallets), τα οποία έχουν συμμετάσχει σε κάποια συναλλαγή κι επομένως το δημόσιο κλειδί τους έχει «φανερωθεί» σε blockchain, μείνει

εκτεθειμένο σε κβαντο-επιθέσεις τότε αρκεί για να κλονίσει την αξία των κρυπτονομισμάτων και τελικά την εμπιστοσύνη του κόσμου στην τεχνολογία αυτή (Beadles and Koltun 2019:1). Έτσι, θεωρούν πως οποιοσδήποτε οργανισμός επιθυμεί να προσθέσει ένα επιπλέον επίπεδο κβαντο-ανθεκτικής ασφάλειας στην blockchain του, μπορεί εύκολα να το πράξει μέσα από την πλατφόρμα ανοικτού κώδικα (open source) του QRL (Peaster 2018:1).

Στο πρόσφατο hardfork της blockchain, πέρα από την μετάβαση στον RandomX consensus algorithm, ενεργοποιήθηκαν και οι κβαντο-ανθεκτικές διευθύνσεις και συναλλαγές πολλαπλών υπογραφών. Οι μοναχοί πριν πολλούς αιώνες κλείδωναν πολύτιμα και ιερά λείψανα (relics) σε δωμάτια ή δοχεία με πολλαπλές διαφορετικές κλειδαριές και ο καθένας διατηρούσε ένα από τα κλειδιά ώστε να μπορούν να ανοιχτούν μόνο όταν όλοι είναι παρόντες. Με παρόμοια λογική, το σχήμα πολλαπλών υπογραφών δημιουργεί ένα είδος κοινόχρηστων λογαριασμών από τους οποίους για να γίνουν συναλλαγές χρειάζεται να υπογραφούν, ως μορφή έγκρισης, από όλους (ή την οριζόμενη πλειοψηφία από) τους κατόχους. Αυτό, πέρα από τις διάφορες εφαρμογές που μπορεί να βρει (κοινοί λογαριασμοί ταμιευτηρίου, αμοιβαία κεφάλαια, κ.α.), προσφέρει ένα επιπλέον επίπεδο ασφάλειας σε ότι αφορά την απώλεια κρυπτονομισμάτων λόγο ιδιωτικών κλειδιών που χάθηκαν ή καταστράφηκαν κατά λάθος (Strike 2020:1). Στο ίδιο hardfork, ενεργοποιήθηκε και το Εφήμερο Σύστημα Μηνυμάτων (Ephemeral Messaging System, EMS). Χρησιμοποιείται για την ανταλλαγή ασύγχρονων κρυπτογραφημένων από άκρο σε άκρο (end to end) μηνυμάτων μεταξύ των QRL κόμβων σε ξεχωριστό επίπεδο από αυτό της blockchain (Pete Waterland 2019:1–8).

Με τέτοια χαρακτηριστικά να προστίθενται, η επόμενη ημέρα για το QRL διακατέχεται από συγκρατημένη αισιοδοξία. Στο επόμενο hardfork της blockchain αναμένεται να ενσωματωθούν τα «έξυπνα συμβόλαια», ενώ αμέσως επόμενη προτεραιότητα είναι η μετάβαση σε μηχανισμό συναίνεσης που βασίζεται σε proof-of-stake αλγόριθμο. Ιδιαίτερης σημασίας για το QRL, είναι και το επερχόμενο QRL Enqlave. Πρόκειται για έναν μηχανισμό ο οποίος θα μπορεί να εφαρμοστεί σε «πορτοφόλια» (wallets) του Ethereum και να τα ασφαλίσει από κβαντικές επιθέσεις (Matier 2020b:1). Αυτό, θα είναι ξεχωριστής σημασίας για το QRL καθώς θα το καταστίσει blockchain πολλαπλών αλυσίδων και μάλιστα με το δεύτερο γνωστότερο κρυπτονόμισμα που υπάρχει αυτή τη στιγμή στην αγορά.

Κεφάλαιο 7

Πρακτική εφαρμογή

Το QRL στην πράξη

Για το πειραματικό στάδιο της μελέτης του QRL, χρησιμοποιήθηκε οικιακός ηλεκτρονικός υπολογιστής με τα παρακάτω χαρακτηριστικά:
CPU: Intel Core2Duo E6750 @ 2,66GHz
RAM: 6 GB, DDR2 @ 400MHz
OS: Windows 10 Pro, 64bit

Το QRL προσφέρει πέρα της επίσημης blockchain του (Mainnet) και μια δοκιμαστική (Testnet) όπου χρήστες μπορούν να δημιουργήσουν πορτοφόλια (wallets) να τα γεμίσουν με εικονικά κρυπτονομίσματα, τύπου Quanta που προσφέρει το QRL, και να πειραματιστούν με συναλλαγές που αργότερα θα προστεθούν σε block και από εκεί και πέρα θα προσαρτηθούν στην Testnet blockchain. Για να πραγματοποιηθούν όλα αυτά, το QRL έχει αναπτύξει μια διαδικτυακή διεπαφή (web interface) με τα αντίστοιχα εργαλεία δημιουργίας και διαχείρισης πορτοφολιών, αποστολής εικονικών Quanta και περιήγησης στην blockchain όπου μπορεί κανείς να δει δοκιμαστικές κινήσεις που έκανε ο ίδιος ή άλλοι χρήστες της Testnet. Πέρα από αυτό, το QRL είναι ανοικτού κώδικα (open source) (https://github.com/theQRL) και περιέχει βιβλιοθήκες γραμμένες σε Python, C++ , JavaScript και Goland (Go). Επιπλέον, προσφέρει το API του για όποιον επιθυμεί να το χρησιμοποιήσει σε δική του εφαρμογή (https://api.theqrl.org/).

7.1 Δημιουργία Πορτοφολιών

Αρχικά δημιουργήσαμε μερικά δοκιμαστικά πορτοφόλια με διαφορετικές παραμέτρους

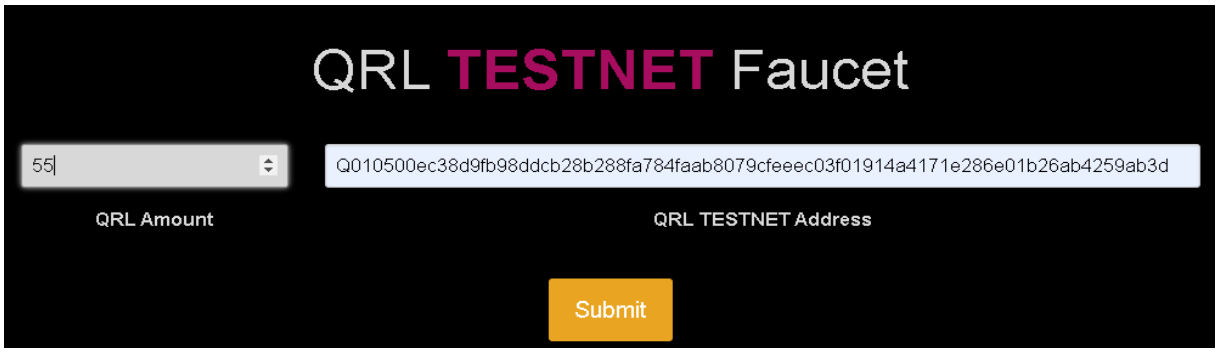
μεγέθους και συνάρτησης hash και μετρήσαμε τους αντίστοιχους χρόνους κατασκευής τους. Κάθε πορτοφόλι, δημιουργεί ένα κρυπτογραφημένο αρχείο JSON το οποίο προστατεύεται από την κωδική φράση (passphrase) που επέλεξε ο χρήστης. Με την δημιουργία του, παρατίθενται στον χρήστη η δημόσια διεύθυνση του πορτοφολιού (QRL Address), μια μνημονική φράση (mnemonic phrase) που αποτελείται από 34 τυχαίες λέξεις καθώς και μια συμβολοσειρά που καλείται Hexseed: όλα αυτά αποτελούν τρόπους πρόσβασης και ανάκτησης στο πορτοφόλι. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα, όπου αναγράφονται και τα Hexseeds τους για όποιον θέλει να δει ή να συνεχίσει τις δοκιμές με τα εν λόγω πορτοφόλια.

#	XMSS Tree Height	# Υπογραφών	Hash Function / Algorithm	Χρόνος Δημιουργίας	QRL Address	Hexseed
1	18	262.144	SHA2_256 / SHA2	1ω 10λ 49δ	Q0009002725cb6c19c cc8d74aa84a51ebdf84 c255fde50420c6a36aa c5a06430355b85a25e 4f950	000900bf4bc1acbc45f8cc80 c706d5b4e100f3de04798ca 96beec3c31dd46f9febdf7d3 7f7af85e875414086bff1fb1 24c1ad0
2	10	1.024	SHAKE_128 / SHA3	11δ	Q010500ec38d9fb98d dcb28b288fa784faab8 079cfeeec03f01914a4 171e286e01b26ab425 9ab3d	01050016323ead2d8fe509 c6c80e8850ffefedcd0b32a6 771ccee055a2306807b033 370278f072e803c229f2ca8 69f50c4fa19
3	12	4.096	SHA2_256/ SHA2	1λ 20δ	Q0006002f329b0e3b9 d1e43717fe4ef7cdfc4 a8591b5ee559fff5a1a d334a0d0848f3fdf19a a393	0006007d12a8569c3539ec 4b4a608aab55bacfc16b6cc 7c4b2b4c8b48bfbd573a1b 270bfc31ba35cac3e747f7af 64f01289c2f
4	12	4.096	SHAKE_128 / SHA3	48δ	Q0106006cf37da35af 54ecdd7c3bf59930d7 c23d0df58ba40e12f65 59477628e161712e7 741b8dc	01060038a0f42e0ae0898a d0fd6d4b7ec24c1ea59dc90 347431ff584740e1abc2944 aeb194c8863718fee864610 2f375d1f392
5	12	4.096	SHAKE_256 / SHA3	46δ	Q020600c66a8353e86 fff46d60836b227ae1c d049bd633756d08bdf 153cbac2d476759bbe 88ab9c	0206008004f9142e219d6a ed63efd41dea937329b851 27d446e8723752647c3d85 8f106b643ce740b44cf6e33 78096e98d78df

Πίνακας 11. Δημιουργία Πορτοφολιών

Στη συνέχεια προσθέσαμε από το ειδικό εργαλείο (https://testnet-faucet.qrl.tips/)

μερικά Quanta σε κάποια πορτοφόλια ώστε να έχουν νομίσματα για να εκτελέσουμε συναλλαγές μεταξύ τους.

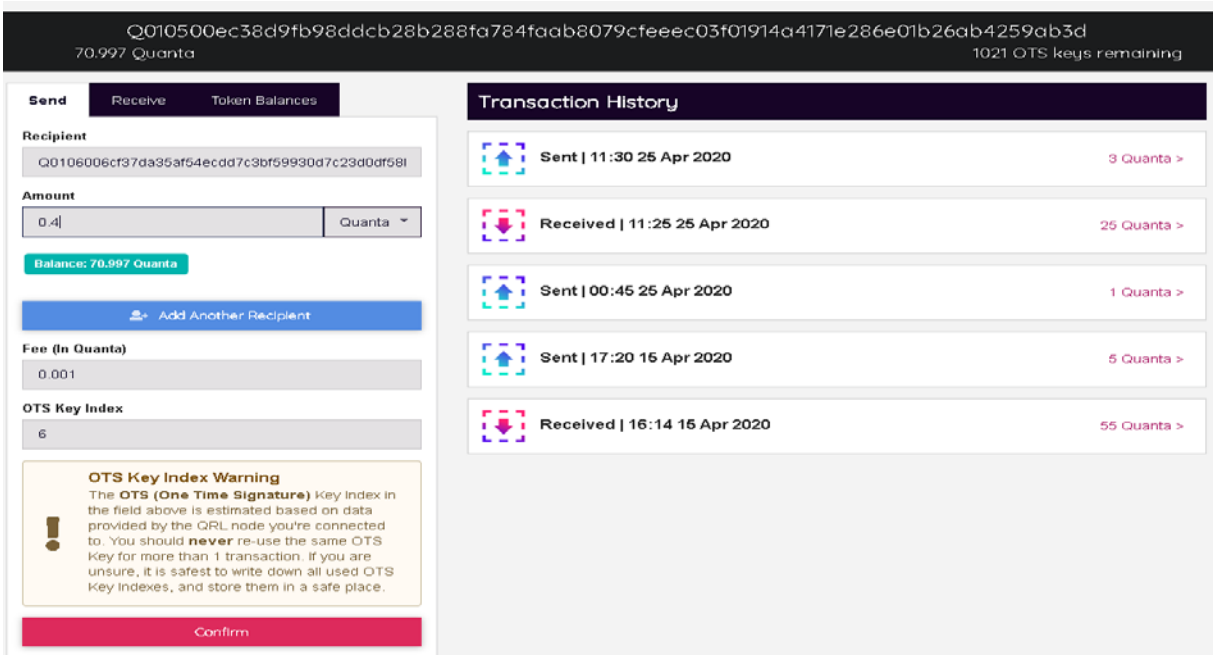


Εικόνα 19. Αποστολή Εικονικών Quanta σε wallet με επιλεγμένη διεύθυνση

7.2 Συναλλαγές

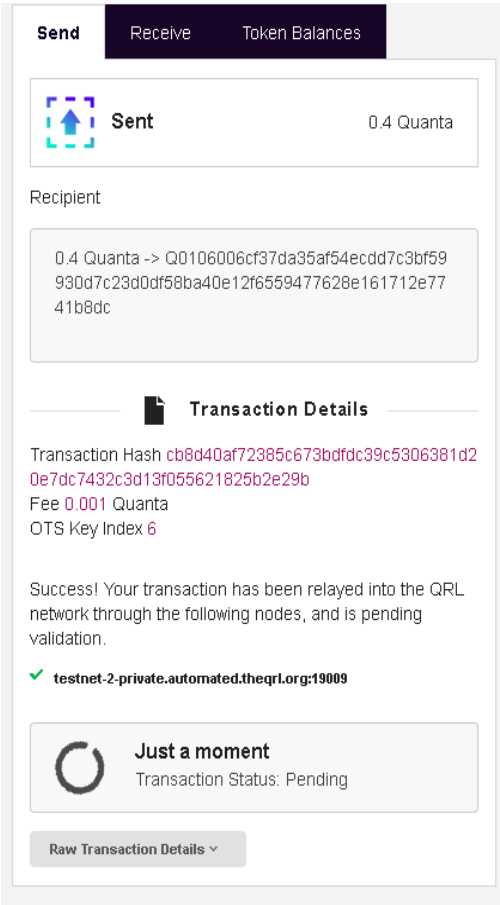
Έπειτα, εκτελέσαμε διάφορες συναλλαγές για να δούμε την διαδικασία υπογραφής, επικύρωσης, προσθήκης σε block και τελικά στην blockchain παίρνοντας ταυτόχρονα μετρήσεις μεγεθών και χρόνου εκτέλεσης. Ακολουθούν ενδεικτικές εικόνες της διαδικασίας για μία από αυτές.

Συνδεθήκαμε στο πορτοφόλι #2 και στείλαμε στο πορτοφόλι #4 κρυπτονομίσματα αξίας 0,4 Quanta.



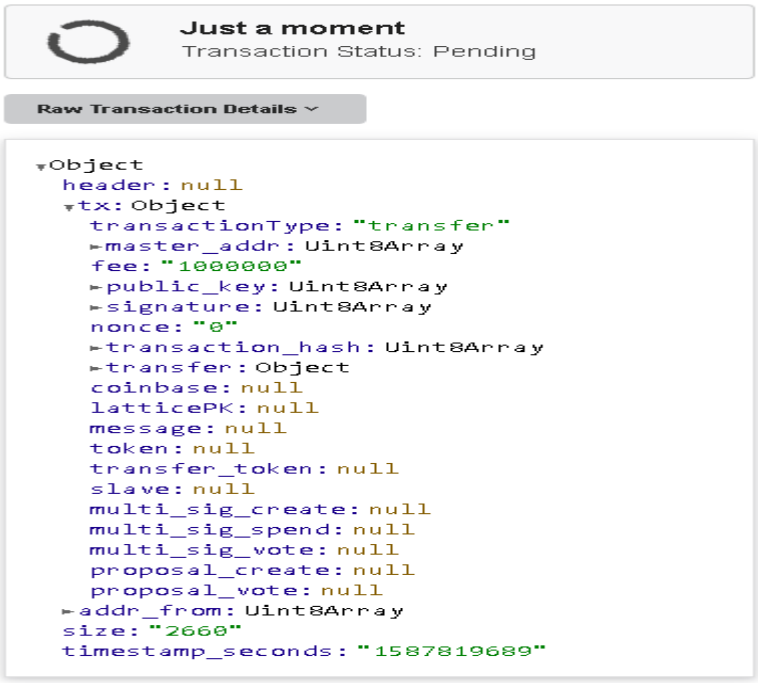
Εικόνα 20. Αποστολή Quanta

Η συναλλαγή δημιουργήθηκε και στην συνέχεια πέρασε στην διαδικασία έγκρισης.



Εικόνα 21. Δημιουργία Συναλλαγής προς έγκριση

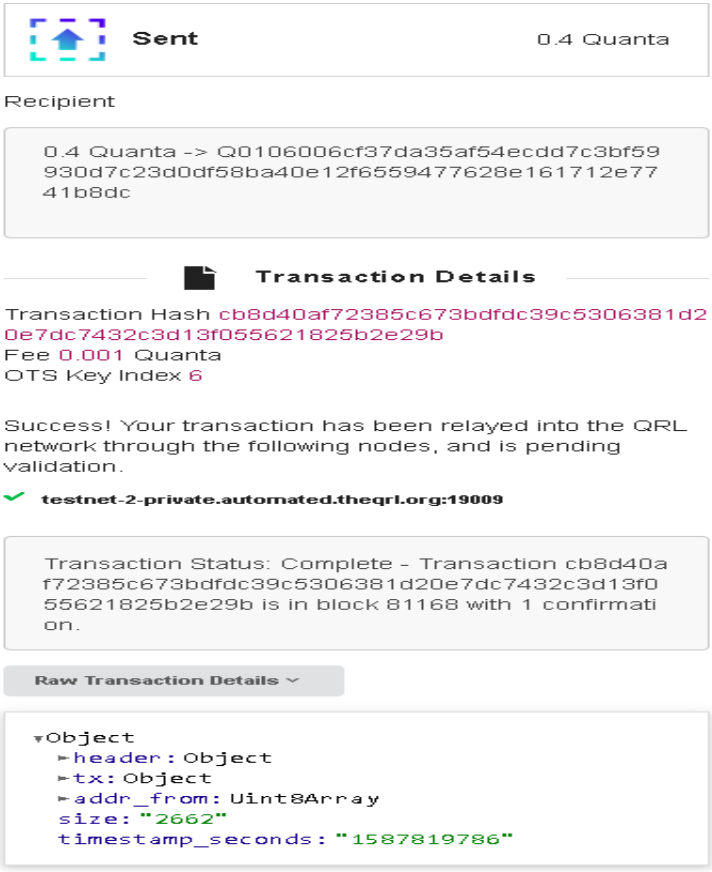
Τα μεταδεδομένα της κίνησης είναι



Εικόνα 22. Μεταδεδομένα κίνησης συναλλαγής

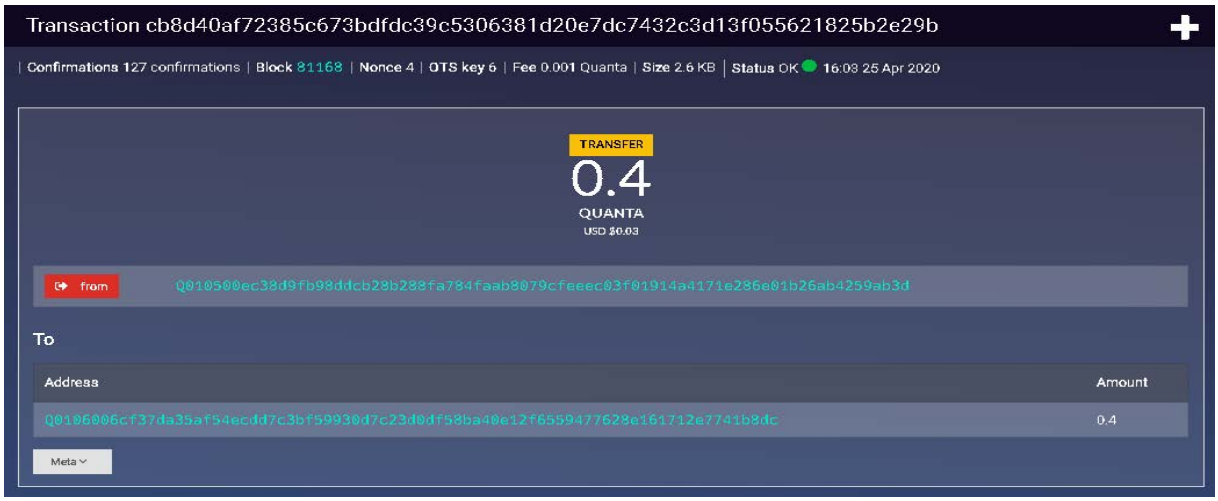
Και τελικά εγκρίνεται και προστίθεται στο block 81168 της Testnet blockchain όπως

αναφέρει και παρακάτω



Εικόνα 23. Επιτυχής έγκριση - προσθήκη σε block

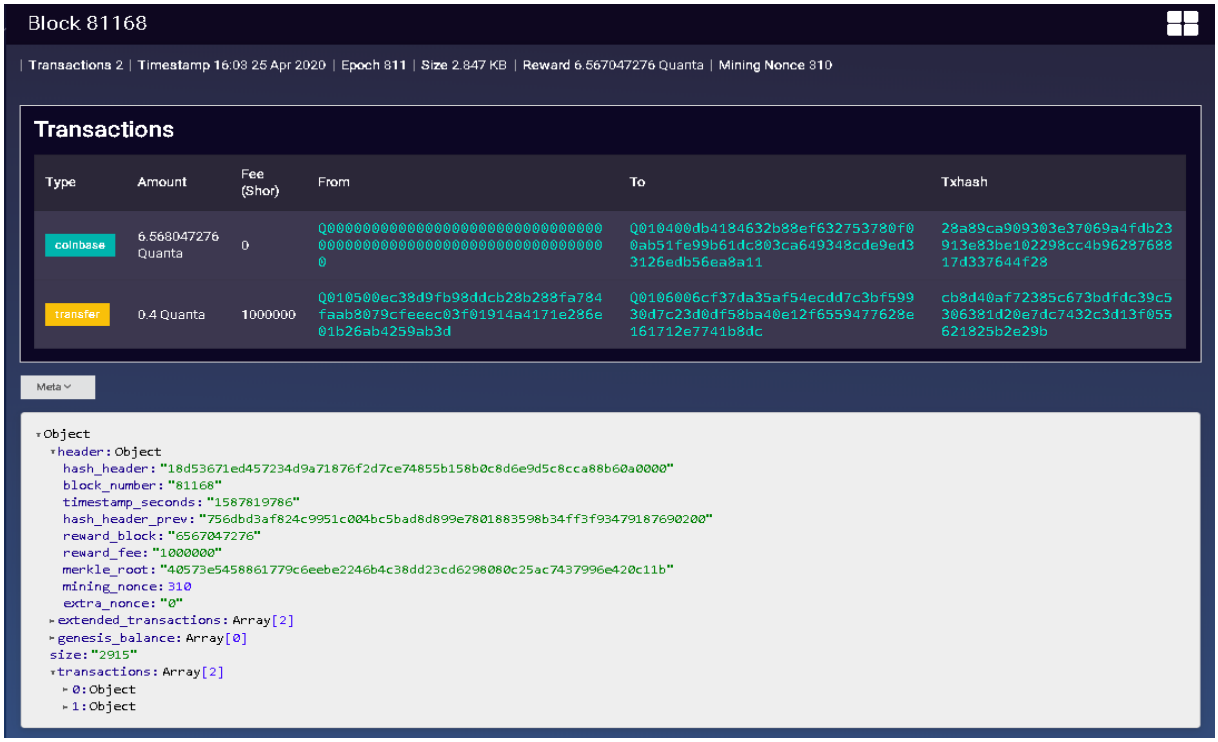
Συνδεόμαστε στην πλατφόρμα περιήγησης block (block explorer, https://testnet-explorer.theqrl.org) για το συγκεκριμένο wallet address και βλέπουμε πράγματι την συναλλαγή με το block στο οποίο προστέθηκε, το μέγεθός του, το πλήθος επιβεβαιώσεων (confirmations) αλλά και το OTS κλειδί που χρησιμοποιήθηκε (εδώ $n = 6$).



Εικόνα 24. Εμφάνιση συναλλαγής στον QRL block explorer

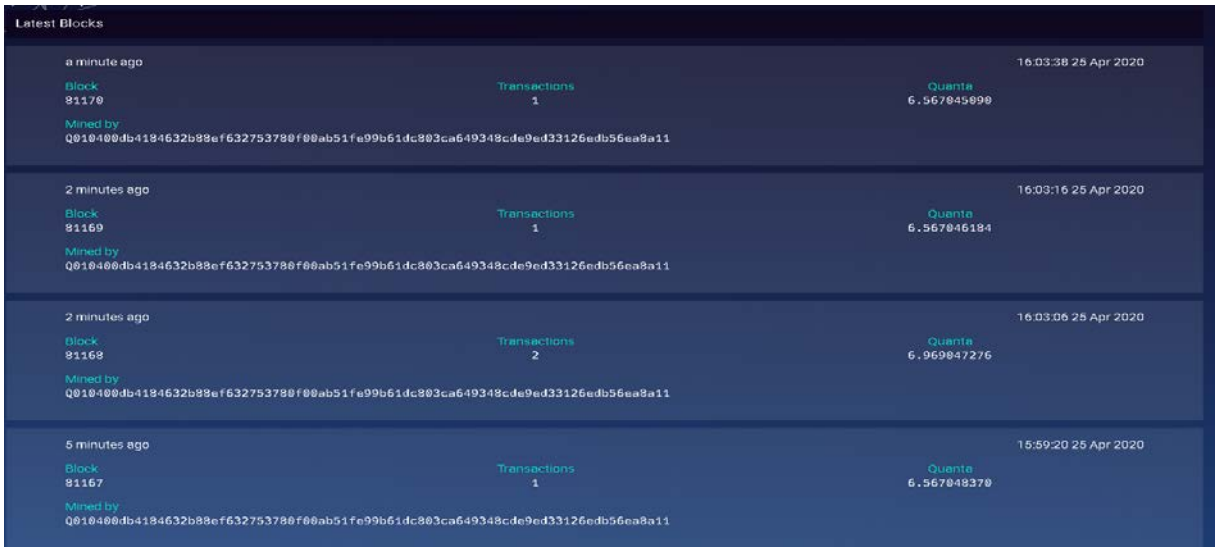
Στα στοιχεία του block #81168 όπου ανήκει η συναλλαγή μας, βλέπουμε και την κίνηση

που δημιουργείται αυτόματα και αφορά την αμοιβή του miner – με QRL διεύθυνση Q010400db4184632b88ef632753780f00ab51fe99b61dc803ca649348cde9ed33126edb56ea8a11 – που πρόσθεσε το block στην blockchain. Στα μεταδεδομένα μπορούμε να παρατηρήσουμε επιπλέον λεπτομέρειες όπως το previous block hash.



Εικόνα 25. Λεπτομέρειες block 81168

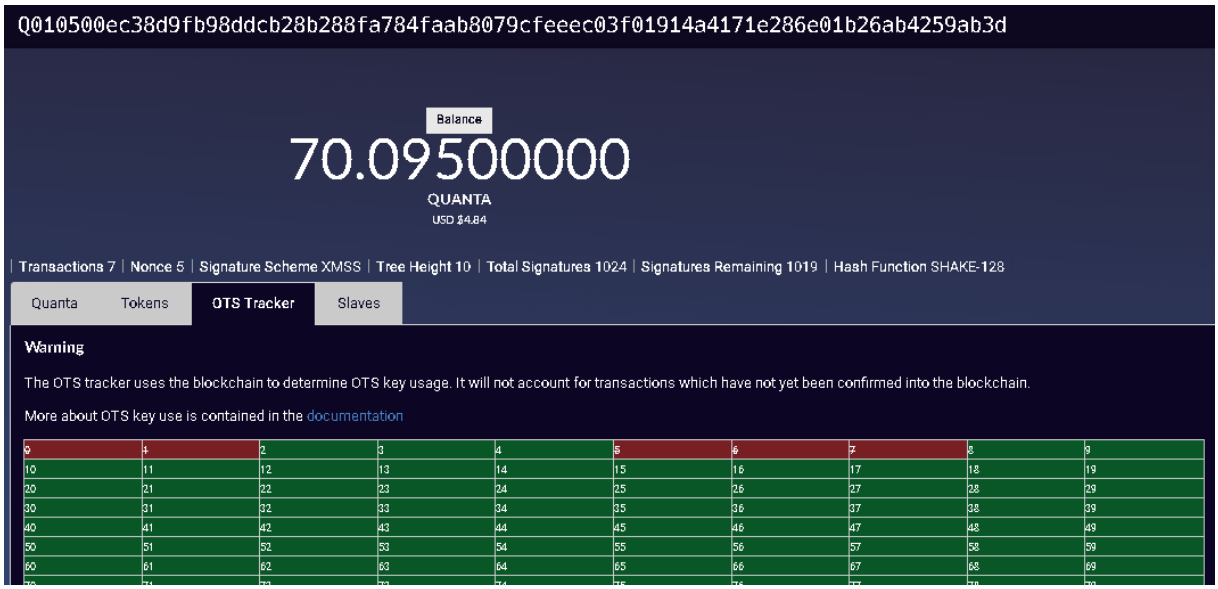
Ενώ παρακάτω φαίνονται τα τελευταία blocks της blockchain την στιγμή εκείνη από όλους τους χρήστες της.



Εικόνα 26. Τελευταία blocks της Testnet blockchain την συγκεκριμένη στιγμή

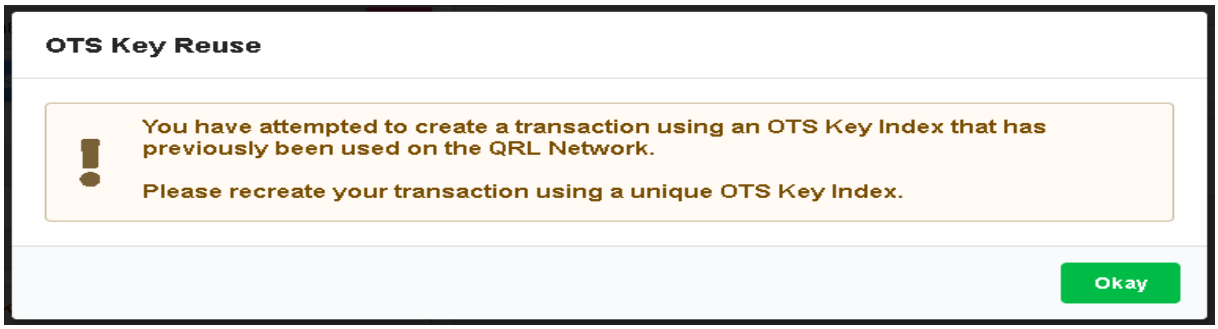
Υπάρχει και ιχνηλασιμότητα (tracking) των OTS κλειδιών που έχουμε χρησιμοποιήσει

(κόκκινο χρώμα) και αυτών που είναι ακόμα διαθέσιμα (πράσινο χρώμα).



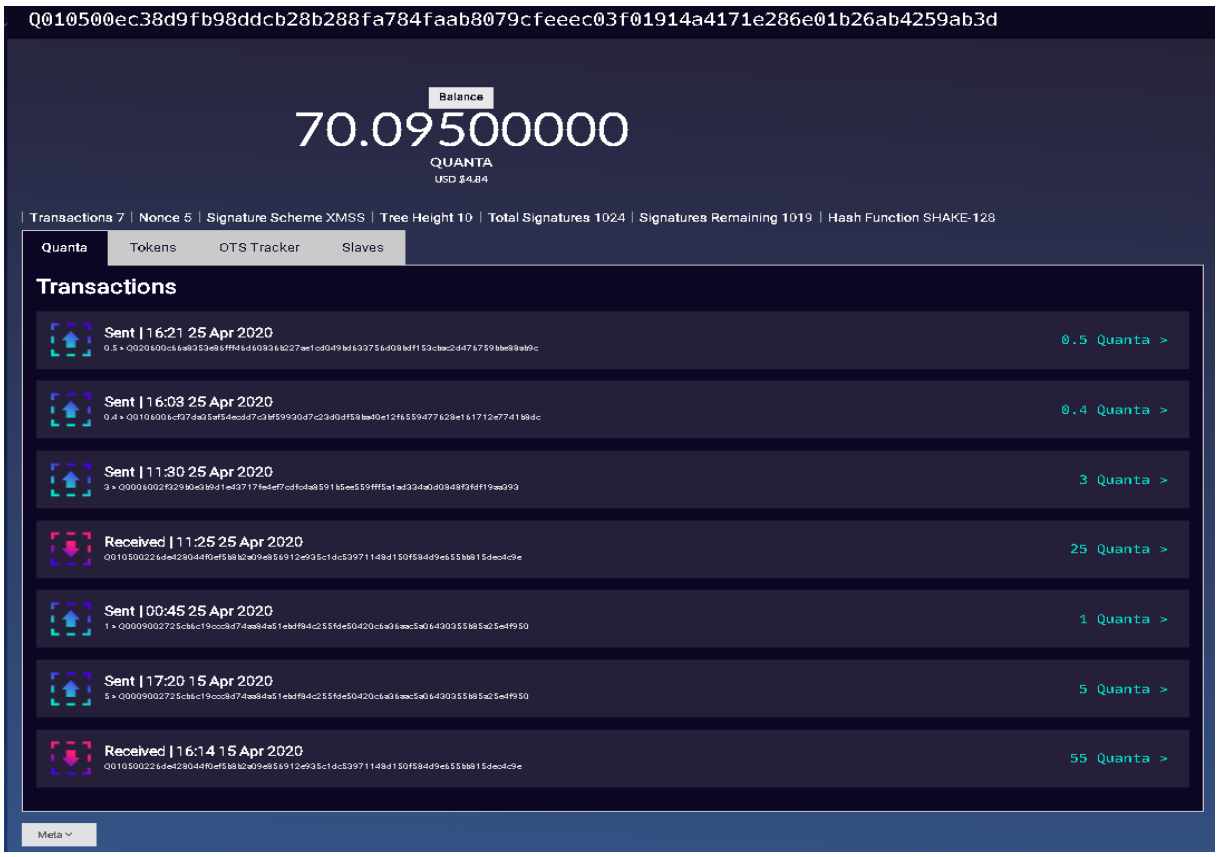
Εικόνα 27. Ιχνηλασιμότητα OTS κλειδιών

Ενώ σε περίπτωση που σε μια νέα συναλλαγή, χειροκίνητα αλλάξουμε τον δείκτη κλειδιού με το οποίο επιθυμούμε να την υπογράψουμε, βάζοντας κάποιο κλειδί που έχουμε ήδη χρησιμοποιήσει, το σύστημα μας εμποδίζει την επαναχρησιμοποίησή του με το κατάλληλο μήνυμα – κάτι που είναι προφανώς πολύ σημαντικό από την πλευρά της ασφάλειας.



Εικόνα 28. Απαγόρευση επαναχρησιμοποίησης OTS κλειδιού

Μετά από μερικές δοκιμαστικές συναλλαγές, ο explorer για το πορτοφόλι #2 φαίνεται ως εξής



Εικόνα 29. Κινήσεις πορτοφολιού #2

Ανοίγοντας τα μεταδεδομένα για κάθε κίνηση μπορούμε να δούμε επιπλέον πληροφορίες όπως το δημόσιο κλειδί που χρησιμοποιήθηκε αλλά και την υπογραφή που υπογράφει την κίνηση αυτή.

Εικόνα 30. Μεταδεδομένα κίνησης

Συγκεντρώνοντας όλες τις δοκιμαστικές κινήσεις που αφορούν το πορτοφόλι #2, έχουμε

Transaction ID	Transaction Size (bytes)	Signing Time	Signature Size (bytes)	Verification Time	Block #	Block Size (bytes)
86756025fc59a2d8f4e051c7d9384591dc6c18fc6d5529523b6db63b1f216a8d	2662	1δ	2500	4λ 36δ	81188	2915
cb8d40af72385c673bdfdc39c5306381d20e7dc7432c3d13f055621825b2e29b	2662	1δ	2500	9δ	81168	2915
deeb192db9323e1d0d22891c4222b8f5a000434e448e4b351e5b45d08441f8ef	2662	1δ	2500	3λ 0δ	80944	2915
6420cc41112f326318e37c807a7e2d26496c090484f5a443714d0f35428df4f3	2704	-	2500	-	80939	2958
720d645f15afa6ce7aeae4415701a3515fac5003dd30b7340decf0c1f0502676	2662	1δ	2500	1λ 2δ	80205	2915
03c73a0a92b2dbe1eb53fcc1dd6bb87b06e3d04f28620a7c54f5459b556f25bc	2662	1δ	2500	24δ	66804	2915
706c112c713c07f11c7016a16b52e9f5a0b77aa940b8b062ed4e237f0d896170	2705	-	2500	-	66739	2959

Πίνακας 12. Στατιστικά Κινήσεων Πορτοφολιού #2

Αξίζει να παρατηρήσουμε πως το μέγεθος της υπογραφής είναι σταθερό. Βάσει σχεδιασμού, οι υπογραφές στο QRL σχετίζονται με το ύψος του XMSS δέντρου που τις παράγει και το μέγεθός τους ορίζεται από τον τύπο 2180 + (height * 32) bytes. Στο συγκεκριμένο παράδειγμα το δέντρο έχει ύψος h = 10, οπότε και οι υπογραφές έχουν μέγεθος 2180 + 320 = 2500 bytes. Ένας άλλος τρόπος να το υπολογίσουμε είναι να πάρουμε την υπογραφή από μια κίνηση, να μετρήσουμε τους χαρακτήρες και να διαιρέσουμε το πλήθος τους διά δύο. Πράγματι, οι υπογραφές έχουν 5000 χαρακτήρες, αλλά επειδή πρόκειται για δεκαεξαδικούς, χρειάζονται δύο τέτοιοι χαρακτήρες για να μετρήσουμε ένα byte μεγέθους. Άρα, έχουμε και πάλι 5000 / 2 = 2500 bytes. Επίσης, το μέγεθος της συναλλαγής φαίνεται να είναι σταθερό, ενώ για τις δύο κινήσεις αποδοχής (receive) κρυπτονομισμάτων, υπάρχει μια μικρή διαφορά. Για τις κινήσεις αυτές άλλωστε δεν έχουμε χρόνους υπογραφής και επαλήθευσής της καθώς εκτελέστηκαν από τον εσωτερικό μηχανισμό (faucet) που είδαμε και παραπάνω. Σε ό,τι αφορά το μέγεθος του block υπάρχει σταθερότητα, με μικρές διακυμάνσεις ξανά στις κινήσεις αποδοχής. Ο αριθμός των blocks και το μέγεθός τους είναι τόσο μικρό ώστε δεν μπορεί να αναδειχτεί

ο τύπος υπολογισμού του μεγέθους κάθε block που περιγράψαμε παραπάνω (υποενότητα 5.2.1). Μεγάλες διακυμάνσεις παρατηρούμε στους χρόνους επαλήθευσης των υπογραφών συναλλαγών. Αυτό πιθανότατα να οφείλεται στο γεγονός ότι στο δοκιμαστικό περιβάλλον που εργαζόμαστε, όλες οι κινήσεις μας επαληθεύονται και προστίθενται σε block από τον ίδιο miner. Ίσως οι χρόνοι αυτοί να σχετίζονται με τον φόρτο που «αντιμετωπίζει» ο miner στο δίκτυο της Testnet blockchain. Τέλος, βάσει σχεδιασμού στο QRL έχει ορισθεί και το μέγεθος του δημοσίου κλειδιού στα 67 bytes.

7.3 Συμπεράσματα

Συμπερασματικά, βάσει της πειραματικής έρευνας, συμπεραίνουμε πως τα μεγέθη και οι χρόνοι υπογραφών είναι πολύ κοντά στο θεωρητικό μοντέλο των XMSS trees. Αυτό που προβληματίζει είναι ο τεράστιος χρόνος κατασκευής του της δομής όταν ζητήθηκε δέντρο με ύψος $h = 18$. Θα μπορούσε εν μέρη να αιτιολογηθεί από την παλαιότητα του υπολογιστικού συστήματος στο οποίο έγιναν οι δοκιμές. Οι χρόνοι κατασκευής στα υπόλοιπα, μικρότερα, δέντρα φαίνονται φυσιολογικοί κι εντός των αναμενόμενων ορίων.

Τέλος, αξίζει να τονιστεί πως λάβαμε τεράστια υποστήριξη από την κοινότητα του QRL στο κανάλι τους στο Discord. Οι συνεργάτες και συνεισφέροντες (contributors) στο έργο του QRL από την πρώτη στιγμή προσέφεραν οδηγίες και τεχνική υποστήριξη σε κάθε βήμα που ζητήθηκε η συνδρομή τους.

Κεφάλαιο 8

Επίλογος

Συμπερασματικά, είδαμε πως υπάρχουν ήδη αρκετά έτοιμα κρυπτογραφικά σχήματα που φαίνεται να μπορούν να προσφέρουν ασφάλεια στην μετα-κβαντική εποχή. Σημαντικό ρόλο θα παίξει η διαδικασία αξιολόγησης κι επιλογής από τον NIST, η οποία θα εξάγει κάποια ασφαλή συμπεράσματα και μία στιβαρή βάση πάνω στην οποία μπορεί να οικοδομηθεί κάτι ακόμη καλύτερο στο μέλλον. Χρειάζεται η διαδικασία αυτή να ενισχυθεί και να εξεταστεί και από άλλους φορείς πιστοποίησης παγκοσμίως (πχ ETSI). Μην ξεχνάμε, πως η πραγματική δυναμική των κβαντικών υπολογιστών είναι κάτι που μένει να αποδειχτεί στην πράξη. Εάν έχει υπερτιμηθεί, τότε θα υπάρχει δυνατότητα τα κβαντο-ανθεκτικά συστήματα να ελαττώσουν τις απαιτήσεις τους ώστε να εξάγουν μικρότερα μεγέθη υπογραφών και κλειδιών και άρα να είναι πιο εύχρηστα χωρίς όμως αυτό να επηρεάσει την κβαντο-ανθεκτικότητα τους στο σύνολό της. Εάν έχει υποτιμηθεί, τότε αντίστοιχα τα σχήματα αυτά ίσως χρειαστεί να χρησιμοποιήσουν μεγαλύτερα κλειδιά και πιο πολύπλοκες διαδικασίες για να επιτύχουν μεγαλύτερη κβαντο-ανθεκτικότητα. Αναπόφευκτο είναι τόσο πριν όσο και μετά την έλευση των πρώτων ισχυρών κβαντικών υπολογιστών, η διαδικασία ελέγχου και δοκιμών των σχημάτων να είναι συνεχής και εξαντλητική. Το οικοσύστημα που αποτελείται από την δυναμική των κβαντικών υπολογιστών, την τεχνολογία blockchain και τα κβαντο-ανθεκτικά σχήματα, είναι διαρκώς μεταβαλλόμενο κι έτσι γρήγορες αλλά προσεκτικές πρέπει να είναι και οι προσαρμοστικές αντιδράσεις της επιστημονικής κοινότητας.

Όπως αναφέραμε και προηγουμένως, αλγόριθμος απόλυτα ασφαλής σε κβαντικές επιθέσεις δεν υπάρχει. Πάντα θα υπάρχει ένα όριο ασφάλειας το οποίο δυνητικά θα μπορεί να ξεπεραστεί με αρκετή υπολογιστική ισχύ. Όμως, είδαμε αλγορίθμους που είναι σχεδιασμένοι να αντέχουν σε τέτοιες επιθέσεις. Οι αλγόριθμοι αυτοί προέρχονται από διαφορετικό μαθηματικό υπόβαθρο και εμφανίζουν ξεχωριστά πλεονεκτήματα και

μειονεκτήματα. Ακόμη δεν γνωρίζουμε εάν θα υπάρχει ένα κρυπτογραφικό σχήμα που θα υπερτερήσει έναντι των άλλων και ποιο θα είναι αυτό. Φυσικά, θα μπορούσε τελικά να δημιουργηθεί ένας συνδυασμός αλγορίθμων, διαφορετικών «οικογενειών» σχημάτων που να προσφέρει ακόμη μεγαλύτερο βαθμό ασφάλειας, χωρίς απαγορευτικό κόστος στην υλοποίηση και στα μεγέθη δεδομένων που παράγει.

Παραλλαγές και βελτιώσεις υπαρχόντων κβαντο-ανθεκτικών αλγορίθμων προτείνονται διαρκώς. Παράδειγμα τέτοιας πρότασης, αποτελεί το σύστημα κβαντο-ανθεκτικών υπογραφών με τίτλο «Μετα-Κβαντικές Υπογραφές για Blockchain» (Blockchained Post-Quantum Signatures, BPQS). Πρόκειται για ένα σύστημα που χρησιμοποιεί και παραλλάσει την hash-based XMSS δομή και υπό συνθήκες έχει καλύτερες επιδόσεις από υπάρχοντες hash-based post-quantum αλγορίθμους, ενώ παράλληλα υποστηρίζει εναλλακτικό μηχανισμό που επιτρέπει σε ανεξάντλητο πλήθος υπογραφών. Μάλιστα, το BPQS σχεδιάστηκε με τέτοιο τρόπο ώστε να εκμεταλλεύεται αλυσιδωτές δομές όπως οι blockchains και να προσφέρει ακόμα χαμηλότερους χρόνους υπογραφής κι επικύρωσης αλλά και μικρότερα σε μέγεθος κλειδιά και υπογραφές (Chalkias et al 2018:1). Το BPQS, προσφέρει πολλές επιλογές παραμετροποίησης χαρίζοντας στο σχήμα μεγάλη προσαρμοστικότητα ανάλογα εάν κάποιος επιθυμεί να το χρησιμοποιήσει ως σύστημα υπογραφής μίας, λίγων ή πολλών χρήσεων. Επιπλέον, σύμφωνα με τον σχεδιασμό του, μπορεί να χρησιμοποιηθεί για την κατασκευή πρωτοποριακών σχημάτων που είναι ταυτόχρονα ορισμένης (stateful) και μη-ορισμένης κατάστασης (stateless), ως συνδετικός κρίκος συμβατότητας με προγενέστερα ή μεταγενέστερα συστήματα (backward, forward compatibility) ή για περιπτώσεις που χρειαστεί να επαναχρησιμοποιηθεί κάποιο κλειδί μεταξύ δύο ανεξάρτητων και ασύμβατων blockchain (Chalkias et al 2018:8). Είναι σίγουρο πως σχήματα υποσχόμενα όπως αυτό, χρήζουν περαιτέρω μελέτης και δοκιμών για την επίτευξη post-quantum ledgers.

Αυτό που φαίνεται να είναι σίγουρο, είναι πως η κβαντο-ανθεκτικότητα δεν θα έρθει σε κόστος κάποιας άλλης σημαντικής ιδιότητας των blockchains. Τα σχήματα που έχουν προταθεί ως τώρα, δεν επηρεάζουν τον τρόπο που οι συναλλαγές δημιουργούνται, επικυρώνονται και προστίθενται σε blocks στην αλυσίδα. Ομοίως οι μηχανισμοί συναίνεσης παρουσιάζονται ανεξάρτητοι από τους αλγορίθμους που θα εξασφαλίζουν την κβαντο-ανθεκτικότητα. Η ιδιωτικότητα από την άλλη, θα μπορούσε μάλιστα να ενισχυθεί όπως είδαμε με την εφαρμογή του μοντέλου μηδενικής γνώσης σε μια

blockchain. Η μόνη αρνητική επίδραση της κβαντο-ανθεκτικότητας στις blockchain είναι το επιπλέον κόστος σε χρόνο υλοποίησης των διαδικασιών (υπογραφή) και σε όγκο δεδομένων (μέγεθος κλειδιών), κάτι που όμως είναι αναμενόμενο.

Σε ό,τι αφορά το πότε θα έχουμε κβαντικούς υπολογιστές, υπάρχουν σίγουρα τεχνικά εμπόδια που είναι δύσκολο να ξεπεραστούν σύντομα ώστε να κατασκευαστούν χρηστικοί κβαντικοί υπολογιστές. Η ιστορία όμως έχει δείξει πολλές φορές ως τώρα, πως η ανθρωπότητα έχει ξεπεράσει δυσκολίες και έχει επιτύχει πράγματα που φαινομενικά δεν θα έπρεπε να μπορεί (Easttom 2019b:11). Άλλωστε ας αναλογιστούμε ότι έχει τροποποιηθεί και το σχετικό ερώτημα και πλέον από το ΑΝ μπορέσουμε να κατασκευάσουμε κάποτε κβαντικούς υπολογιστές, έχει μετατραπεί σε ΠΌΤΕ θα γίνει αυτό εφικτό. Οι εξελίξεις είναι καταιγιστικές και ο κόσμος των επιχειρήσεων φαίνεται πως ετοιμάζεται οργανωτικά αλλά και τεχνολογικά για αυτή την νέα εποχή. Μεγάλες τράπεζες δημιουργούν θέσεις εργασίας σχετικές με blockchain τεχνολογίες (DiCamillo 2019:1), νέες τεχνικές δοκιμάζονται για την αποθήκευση των qubits (Venkateshvaran 2019:1) ενώ μεγάλες εταιρείες ανταγωνίζονται στην κατασκευή του πιο ισχυρού κβαντικού υπολογιστή (Wogan 2020:1). Επιπλέον, πρέπει να έχουμε πάντα στην άκρη του μυαλού μας, πως πολλές κυβερνήσεις χρηματοδοτούν με υπέρογκα ποσά ερευνητικούς και τεχνολογικούς τομείς για την ανάπτυξη κι εξέλιξη των κβαντικών υπολογιστών. Ελλοχεύει πάντα ο κίνδυνος, μια χώρα να τα καταφέρει και να μην μοιραστεί αυτή την επιτυχία της με τον υπόλοιπο κόσμο, προκειμένου να το εκμεταλλευτεί προς όφελός της στην σκακιέρα της κυριαρχίας. Εάν συμβεί αυτό και δεν έχουν αντικατασταθεί οι αλγόριθμοι κρυπτογραφίας που χρησιμοποιούνται για πάνω από πενήντα χρόνια (Diffie Hellman 1976, RSA 1977), με μοντέρνους και ανθεκτικούς σε επιθέσεις κβαντικών υπολογιστών τότε θα γίνουμε μάρτυρες μιας πρωτοφανούς διαδικτυακής Αποκάλυψης.

Υπάρχει όμως τελικά αισιοδοξία. Έτοιμα κβαντο-ανθεκτικά κρυπτοσυστήματα υπάρχουν ήδη και συνεχώς βελτιώνονται. Ένα από αυτά είναι και το QRL με εφαρμογή ήδη σε εμπορική blockchain το οποίο ερευνήσαμε πειραματικά αποκομίζοντας πολύ θετικές εντυπώσεις από την απόδοσή του – ακόμα και σε οικιακό υπολογιστικό σύστημα χαμηλών επιδόσεων – αφού οι πειραματικές μετρήσεις συμφωνούν με τις θεωρητικά αναμενόμενες. Το γεγονός ότι ικανοποιεί το σχέδιο συστάσεων του NIST για τα post quantum XMSS δέντρα, ότι έχει πολύ δυνατή κοινότητα χρηστών που ασχολούνται

καθημερινά για την εξέλιξή της και πως πρόκειται να εφαρμόσει την τεχνογνωσία του για να θωρακίσει ένα από τα πιο δημοφιλή κρυπτονομίσματα σήμερα, δείχνει πως είναι στον σωστό δρόμο για να προσφέρει ασφάλεια στις blockchains έναντι επιθέσεων τόσο από κλασικούς όσο και από κβαντικούς υπολογιστές.

Βιβλιογραφία

Abbade LR, Ribeiro FM, Silva MH da, Morais AFP, Morais ES de, Lopes EM, Alberti AM and Rodrigues JJPC (2020) Blockchain Applied to Vehicular Odometers. *IEEE Network*. paper presented at the IEEE Network 34(1): 62–68.

Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Liu Y-K, Miller C, Moody D, Peralta R, Perlner R, Robinson A and Smith-Tone D (2019) *Status report on the first round of the NIST post-quantum cryptography standardization process*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf.

Almazrooie M, Abdullah R, Samsudin A and Mutter KN (2018) Quantum Grover Attack on the Simplified-AES. *Proceedings of the 2018 7th International Conference on Software and Computer Applications - ICSCA 2018*. paper presented at the the 2018 7th International Conference. Kuantan, Malaysia: ACM Press, 204–211. Available at: http://dl.acm.org/citation.cfm?doid=3185089.3185122.

AL-Mubayedh D, AL-Khalis M, AL-Azman G, AL-Abdali M, AIFosail M and Nagy N (2019) Quantum Cryptography on IBM QX. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. paper presented at the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). Riyadh, Saudi Arabia: IEEE, 1–6. Available at: https://ieeexplore.ieee.org/document/8769567/.

Batabyal A (2019) *Bitcoin Halving 2020 | Bitcoin Halving Explained*. *coinswitch*. Available at: https://coinswitch.co/news/bitcoin-halving-2020-bitcoin-halving-explained-read-more.

Bauer MR (2017) IBM Just Made a 17 Qubit Quantum Processor, Its Most Powerful One Yet. *Vice*. Available at: https://www.vice.com/en_us/article/wnwk5w/ibm-17-qubit-quantum-processor-computer-google.

Beadles R, Koltun A (2019) *QRL Quantum Resistant Ledger - Saving us from Quantum Computer Crypto Hacks?* . Available at: https://www.youtube.com/watch?v=PKe6Q6bIl7k.

Bernstein DJ, Hülsing A, Kölbl S, Niederhagen R, Rijneveld J and Schwabe P (2019) The SPHINCS+ Signature Framework. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. London, United Kingdom: Association for Computing Machinery, 2129–2146. Available at: https://doi.org/10.1145/3319535.3363229.

Bian Z, Chudak F, Macready WG, Clark L and Gaitan F (2013) Experimental determination of Ramsey numbers. *Physical Review Letters* 111(13): 23.

Blum M, Feldman P and Micali S (1988) Non-interactive zero-knowledge and its applications. *Proceedings of the twentieth annual ACM symposium on Theory of computing*. Chicago, Illinois, USA: Association for Computing Machinery, 103–112. Available at: https://doi.org/10.1145/62212.62222.

Bogdanov A and Rosen A (2017) *Pseudorandom Functions: Three Decades Later*. , 72. Available at: http://eprint.iacr.org/2017/652.

Boneh D, Ishai Y, Sahai A and Wu DJ (2017) Lattice-Based SNARGs and Their Application to More Efficient Obfuscation. In: Coron J-S and Nielsen JB (eds) *Advances in Cryptology – EUROCRYPT 2017*. Cham: Springer International Publishing, 247–277.

Buchmann J, Coronado C, Döring M, Engelbert D, Ludwig C, Overbeck R, Schmidt A, Vollmer U and Weinmann R-P (2004) *Post-Quantum Signatures*. , 30. Available at: http://eprint.iacr.org/2004/297.

Campagna M, Chen L, Dagdelen Ö, Ding J, Fernick J, Gisin N, Hayford D, Jennewein T, Lütkenhaus N, Mosca M, Neill B, Pecen M, Perlner R, Ribordy G, Schanck J, Stebila D, Walenta N, Whyte W and Zhang Z (2014) *Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges*. , 48. Available at: https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf.

Chalkias K, Brown J, Hearn M, Lillehagen T, Nitto I and Schroeter T (2018) Blockchained Post-Quantum Signatures. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. paper presented at the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 1196–1203.

Chanson M, Fleisch E, Bogner A and Wortmann F (2017) Blockchain as a privacy enabler : AnOdometer Fraud Prevention System. . Available at: https://dl.acm.org/doi/pdf/10.1145/3123024.3123078.

Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner R and Smith-Tone D (2016) *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology, 15. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

Cheng R and Zhang F (2015) Lattice-based obfuscation for re-encryption functions. *Security and Communication Networks* 8(9): 1648–1658.

Chuang IL, Gershenfeld N and Kubinec M (1998) Experimental Implementation of Fast Quantum Searching. , 3408–3411.

Cooper DA (2019) *Recommendation for Stateful Hash-Based Signature Schemes*. preprint. , 1–54. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208-

draft.pdf.

De Angelis S, Aniello L, Baldoni R, Lombardi F, Margheri A and Sassone V (2018) PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain. paper presented at the Italian Conference on Cyber Security (06/02/18), 11. Available at: https://eprints.soton.ac.uk/415083/.

DiCamillo N (2019) *Bank of America Is Now Hiring in Blockchain, Not Just Filing Patents*. *CoinDesk*. Available at: https://www.coindesk.com/bank-of-america-is-now-hiring-in-blockchain-not-just-filing-patents.

DiCarlo L, Chow J, Bishop L, Johnson B, Schuster D, Frunzio L, Girvin S, Schoelkopf R, Gambetta J, Majer J and Blais A (2009) *Scientists create first electronic quantum processor*. *YaleNews*. Available at: https://news.yale.edu/2009/06/28/scientists-create-first-electronic-quantum-processor.

Dinur I (2018) The Picnic Post-Quantum Signature Scheme and its Security Analysis. .

Easttom C (2019a) An Analysis of Leading Lattice-Based Asymmetric Cryptographic Primitives. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. paper presented at the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). Las Vegas, NV, USA: IEEE, 0811–0818. Available at: https://ieeexplore.ieee.org/document/8666459/.

Easttom C (2019b) *Quantum Computing and Cryptography*. Future of Information and Communication Conference (FICC) 2019, The Park Central San Francisco. Available at: https://www.youtube.com/watch?v=0mpSU0Y2d_4.

Gentry C (2009) Fully homomorphic encryption using ideal lattices. *Proceedings of the forty-first annual ACM symposium on Theory of computing*. Bethesda, MD, USA: Association for

Computing Machinery, 169–178. Available at: https://doi.org/10.1145/1536414.1536440.

Goldwasser S, Micali S and Rackoff C (1985) The knowledge complexity of interactive proof-systems | Proceedings of the seventeenth annual ACM symposium on Theory of computing. 291–304.

Green Mathhew (2018) Hash-based Signatures: An illustrated Primer – A Few Thoughts on Cryptographic Engineering. *https://blog.cryptographyengineering.com/*. blog. . Available at: https://blog.cryptographyengineering.com/2018/04/07/hash-based-signatures-an-illustrated-primer/.

Green Matthew (2018) Winternitz Checksum. *A Few Thoughts on Cryptographic Engineering*. Available at: https://blog.cryptographyengineering.com/winternitz-checksum/.

Hanneke D, Home JP, Jost JD, Amini JM, Leibfried D and Wineland DJ (2009) *NIST Demonstrates 'Universal' Programmable Quantum Processor for Quantum Computers*. *NIST*. Available at: https://www.nist.gov/news-events/news/2009/11/nist-demonstrates-universal-programmable-quantum-processor-quantum.

Howe J, Pöppelmann T, O'neill M, O'sullivan E and Güneysu T (2015) Practical Lattice-Based Digital Signature Schemes. *ACM Transactions on Embedded Computing Systems* 14(3): 1–24.

Huelsing A, Butin D, Gazdag S, Rijneveld J and Mohaisen A (2018) *XMSS: eXtended Merkle Signature Scheme*. RFC Editor, 1–74. Available at: https://www.rfc-editor.org/info/rfc8391.

Intel Corporation (2018) *2018 CES: Intel Advances Quantum and Neuromorphic Computing Research*. *Intel Newsroom*. Available at: https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/.

Kelly J (2018) A Preview of Bristlecone, Google's New Quantum Processor. *Google AI Blog*. Available at: http://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

Kershaw N and Palmer C (2019) *What can quantum computers do? - Microsoft Quantum*. . Available at: https://docs.microsoft.com/en-us/quantum/overview/quantum-computers.

Knightarchive page W (2017) *IBM Raises the Bar with a 50-Qubit Quantum Computer*. *MIT Technology Review*. Available at: https://www.technologyreview.com/2017/11/10/147728/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/.

Koziel B, Azarderakhsh R, Mozaffari Kermani M and Jao D (2017) Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves. *IEEE Transactions on Circuits and Systems I: Regular Papers*. paper presented at the IEEE Transactions on Circuits and Systems I: Regular Papers 64(1): 86–99.

Lamport L, Shostak R and Pease M (1982) The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*. ACM 382–401.

Lin J, Shen Z, Zhang A and Chai Y (2018) Blockchain and IoT based Food Traceability for Smart Agriculture. *Proceedings of 3rd International Conference on Crowd Science and Engineering Engineering,*. paper presented at the International Conference on Crowd Science and Engineering Engineering. Singapore: ACM, 6. Available at: https://dl.acm.org/doi/abs/10.1145/3265689.3265692.

Matier J (2020a) *The QRL Bromine Hardfork: A look inside*. *Medium*. Available at: https://medium.com/the-quantum-resistant-ledger/the-qrl-bromine-hardfork-a-look-inside-2eed61ea90fd.

Matier J (2020b) *Announcing Ethereum Enklave: Quantum Security for the Ethereum Blockchain*. *Medium*. Available at: https://medium.com/the-quantum-resistant-ledger/announcing-ethereum-enklave-quantum-security-for-the-ethereum-blockchain-d0f424814980.

Matier J and Waterland P (2016) The QRL Whitepaper. info@theqrl.org. Available at: https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf.

Maurer PC, Kucsko G, Latta C, Jiang L, Yao NY, Bennett SD, Pastawski F, Hunger D, Chisholm N, Markham M, Twitchen DJ, Cirac JI and Lukin MD (2012) Room-Temperature Quantum Bit Memory Exceeding One Second. *Science* 336(6086): 1283–1286.

McEliece R (1978) *A Public-Key Cryptosystem Based on Algebraic Coding Theory*. DSN Progress Report. , 114–116. Available at: https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

Mertz L (2018) (Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution. *IEEE Pulse*. paper presented at the IEEE Pulse 9(3): 4–7.

Nagaich S and Goswami YC (2015) Shor's Algorithm for Quantum Numbers Using MATLAB Simulator. *2015 Fifth International Conference on Advanced Computing & Communication Technologies*. paper presented at the 2015 Fifth International Conference on Advanced Computing & Communication Technologies (ACCT). Haryana, India: IEEE, 165–168. Available at: http://ieeexplore.ieee.org/document/7079073/.

Nay C (2019a) *IBM Unveils World's First Integrated Quantum Computing System for Commercial Use*. *IBM News Room*. Available at: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use.

Nay C (2019b) *IBM Opens Quantum Computation Center in New York; Brings World's Largest Fleet of Quantum Computing Systems Online, Unveils New 53-Qubit Quantum System for Broad Use*. *IBM News Room*. Available at: https://newsroom.ibm.com/2019-09-18-IBM-Opens-Quantum-Computation-Center-in-New-York-Brings-Worlds-Largest-Fleet-of-Quantum-Computing-Systems-Online-Unveils-New-53-Qubit-Quantum-System-for-Broad-

Use.

Nejatollahi H, Dutt N, Ray S, Regazzoni F, Banerjee I and Cammarota R (2019) Post-Quantum Lattice-Based Cryptography Implementations: A Survey. *ACM Computing Surveys* 51(6): 1–41.

Niederhagen DR and Waidner, Prof. Dr. Michael (2017) Practical Post-Quantum Cryptography. 1–31.

Ningtyas DK and Mutiara AB (2010) Simulating Grover's Quantum Search in a Classical Computer. *arXiv:1003.1930 [cs]* 1–24.

NIST CSD (2017a) *Post-Quantum Cryptography - Project Overview*. *CSRC | NIST*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography.

NIST CSD (2017b) *Post-Quantum Cryptography - Workshops and Timeline*. *CSRC | NIST*. Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline.

Orzel C (2017) *How Do You Create Quantum Entanglement? Forbes*. Available at: https://www.forbes.com/sites/chadorzel/2017/02/28/how-do-you-create-quantum-entanglement/.

Peaster W (2018) *On Quantum Computing with Quantum Resistant Ledger's Adam Koltun*. *Bitsonline*. Available at: https://bitsonline.com/adam-koltun-quantum-resistant-ledger/.

Perboli G, Musso S and Rosano M (2018) Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases. *IEEE Access*. paper presented at the IEEE Access 6: 62018–62028.

Pradhan PK, Rakshit S and Datta S (2019) Lattice Based Cryptography : Its Applications, Areas

of Interest Future Scope. *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*. paper presented at the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 988–993.

QRL Foundation (2019) *QRL: The Quantum Resistant Ledger*. . Available at: https://theqrl.org/.

Rao KB (2017) Computer systems architecture vs quantum computer. *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*. paper presented at the 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), 1018–1023.

Ruiz J (2020) *Public-Permissioned blockchains as Common-Pool Resources*. *LjnkedIn*. Available at: https://www.linkedin.com/pulse/public-permissioned-blockchains-common-pool-resources-jesus-ruiz.

Schukat M and Flood P (2014) Zero-knowledge proofs in M2M communication. *25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*. paper presented at the 25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), 269–273.

Singh J and Singh M (2016) Evolution in Quantum Computing. *2016 International Conference System Modeling & Advancement in Research Trends (SMART)*. paper presented at the 2016 International Conference System Modeling & Advancement in Research Trends (SMART). Moradabad, India: IEEE, 267–270. Available at: http://ieeexplore.ieee.org/document/7894533/.

Spector L (2008) Quantum computing. *Proceedings of the 10th annual conference companion on Genetic and evolutionary computation*. Atlanta, GA, USA: Association for Computing Machinery, 2865–2894. Available at: https://doi.org/10.1145/1388969.1389082.

Strike M (2020) *What Does a Quantum Secure Implementation of MultiSig Look Like?* Available at: https://www.youtube.com/watch?v=7ysFB-IgueI.

Tevador (2020) *RandomX - Proof of work algorithm based on random code execution*. C++. . Available at: https://github.com/tevador/RandomX.

Ttechno C, Leni J, Waterland P, Donald S and Lomas J (2020) *The QRL GitHub*. *GitHub*. Available at: https://github.com/theQRL/QRL/blob/master/src/qrl/core/config.py#L67.

Van Meter R and Oskin M (2006) Architectural implications of quantum computing technologies | ACM Journal on Emerging Technologies in Computing Systems. 2(1): 31–63.

Venkateshvaran D (2019) *'Molecular spintronics': new technology offers hope for quantum computing*. *The Conversation*. Available at: http://theconversation.com/molecular-spintronics-new-technology-offers-hope-for-quantum-computing-124441.

Waterland Pete (2019) *The QRL Ephemeral*. *GitHub*. Available at: https://github.com/theQRL/ephemeral.

Waterland Peter (2019) The QRL Foundation: Leveraging The Power Of Blockchain To Enhance Crypto-Security. *Business APAC*. Available at: https://www.businessapac.com/the-qrl-foundation-leveraging-the-power-of-blockchain/.

Weiss DS and Saffman M (2017) Quantum computing with neutral atoms. *Physics Today* 70(7): 44–50.

Weisstein EW (2020) *Elliptic Curve Group Law*. Text. Wolfram Research, Inc. Available at: https://mathworld.wolfram.com/EllipticCurveGroupLaw.html.

Wikipedia (2020) Merkle tree. *Wikipedia*. Available at: https://en.wikipedia.org/w/index.php?title=Merkle_tree&oldid=939344203.

Wogan T (2020) *Honeywell says it will soon release 'the most powerful quantum computer yet'*. *Physics World*. Available at: https://physicsworld.com/a/honeywell-says-it-will-soon-release-the-most-powerful-quantum-computer-yet/.

Woodage J and Shumow D (2018) *An Analysis of the NIST SP 800-90A Standard*. , 1–54. Available at: http://eprint.iacr.org/2018/349.

World Economic Forum (2017) *Blockchain is not a magic bullet for security. Can we trust it?* . Available at: https://www.weforum.org/agenda/2019/08/blockchain-security-trust/.

Yapa I, Heanthenna S, Bandara N, Prasad I and Mallawarachchi Y (2018) Decentralized Ledger for Land and Property Transactions in Sri Lanka Acresense. *2018 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*. paper presented at the 2018 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 1–6.

Yasuda T, Dahan X, Huang Y-J, Takagi T and Sakurai K (2015) A multivariate quadratic challenge toward post-quantum generation cryptography. *ACM Communications in Computer Algebra* 49(3): 105–107.

Zhang W, Xu C, Li F and Feng J (2007) A Period-Finding Method for Shor's Algorithm. *2007 International Conference on Computational Intelligence and Security (CIS 2007)*. paper presented at the 2007 International Conference on Computational Intelligence and Security (CIS 2007). Harbin, China: IEEE, 778–780. Available at: http://ieeexplore.ieee.org/document/4415451/.

Zhao S and O'Mahony D (2018) BMCProtector: A Blockchain and Smart Contract Based Application for Music Copyright Protection. *Proceedings of the 2018 International Conference on Blockchain Technology and Application*. paper presented at the ICBTA 2018, 1–5. Available at: https://dl.acm.org/doi/abs/10.1145/3301403.3301404.

Zhao W, Yang S and Luo X (2019) On Consensus in Public Blockchains. *Proceedings of the 2019 International Conference on Blockchain Technology*. Honolulu, HI, USA: Association for Computing Machinery, 1–5. Available at: https://doi.org/10.1145/3320154.3320162.

Zheng Z, Xie S, Dai H, Chen X and Wang H (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*. paper presented at the 2017 IEEE International Congress on Big Data (BigData Congress). Honolulu, HI, USA: IEEE, 557–564. Available at: http://ieeexplore.ieee.org/document/8029379/.