ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Επισκόπηση της Ασφάλειας στο Blockchain

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Ευάγγελου Γεροντούκου

Επιβλέπων :
Κρητικός Κυριάκος, Καθηγητής Τμήματος ΜΠΕΣ

Μέλη εξεταστικής επιτροπής:
Κοκολάκης Σπυρίδων, Καθηγητής Τμήματος ΜΠΕΣ
Στεργιόπουλος Γεώργιος, Καθηγητής Τμήματος ΜΠΕΣ

Σάμος, Οκτώβριος 2023

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον κύριο Κυριάκο Κρητικό που ήταν ο επιβλέπων καθηγητής της παρούσας διπλωματικής εργασίας. Εκτός από την καθοδήγηση του, την υποστήριξη του και τον χρόνο που αφιέρωσε βοηθώντας με στην εκπόνηση της εργασίας μου, θα ήθελα να τον ευχαριστήσω και για την ευκαιρία που μου έδωσε να ερευνήσω ένα θέμα που πάντα μου φαινόταν ενδιαφέρον και ήθελα να μάθω περισσότερα για αυτό.

Θα ήθελα επίσης να ευχαριστήσω την οικογένεια μου για την υποστήριξη τους και την κατανόηση τους όλα αυτά τα χρόνια, χωρίς τις οποίες δεν θα ήταν δυνατή η ολοκλήρωση των σπουδών μου.

Τέλος θα ήθελα να ευχαριστήσω την κοπέλα μου αλλά και τους πολύ καλούς φίλους που έκανα κατά την διάρκεια των φοιτητικών μου χρόνων στην Σάμο, για την στήριξη τους αλλά και γιατί έκαναν όλα αυτά τα χρόνια ξεχωριστά.

Περιεχόμενα

Λίστα Εικόνων

Λίστα Πινάκων

Περίληψη

Η εισαγωγή της τεχνολογίας Blockchain έχει φέρει επανάσταση σε διάφορους κλάδους προσφέροντας αποκεντρωμένες, αμετάβλητες και διαφανείς λύσεις διαχείρισης δεδομένων. Έτσι η τεχνολογία αυτή έχει εξελιχθεί σε μια ευέλικτη πλατφόρμα με εφαρμογές τόσο στην οικονομία με την χρήση κρυπτονομισμάτων, όσο και στην διαχείριση περιουσιακών στοιχείων, υγειονομικής περίθαλψης κα. Ωστόσο, καθώς η υιοθέτηση του Blockchain πολλαπλασιάζεται, προκύπτουν ερωτήματα σχετικά με τα τρωτά σημεία ασφαλείας που μπορεί να έχει, τι επιπτώσεις μπορεί να έχουν αυτά αλλά και πως μπορούν να αντιμετωπιστούν. Στην παρακάτω έρευνα, αφού αναλυθεί η τεχνολογία Blockchain και τα χαρακτηριστικά της, θα κατηγοριοποιηθούν και θα αναλυθούν οι κύριες τρωτότητες και επιθέσεις που μπορούν να συμβούν σε αυτήν. Στην συνέχεια θα παρουσιαστούν αντίμετρα και τρόποι αντιμετώπισης τους, αλλά και μερικά κενά πάνω στην εν λόγω έρευνα και προτάσεις μελλοντικής κατεύθυνσης ως προς αυτά. Σκοπός της παρακάτω έρευνας, είναι η εξοικείωση του αναγνώστη με την τεχνολογία Blockchain, η ενημέρωση του ως προς τους κινδύνους ασφάλειας που μπορεί να προκύψουν πάνω σε αυτή, αλλά και οι πιθανοί τρόποι αντιμετώπισης τους. Το Blockchain είναι μια τεχνολογία πολύ χρήσιμη που θα χρησιμοποιηθεί αρκετά στο μέλλον και οι χρήστες του θα πρέπει να είναι καλά ενήμεροι για αυτό.

Λέξεις Κλειδιά: *Blockchain, Κρυπτονομίσματα, Ασφάλεια, Τρωτότητες, Επιθέσεις, Αντίμετρα*

Abstract

The introduction of Blockchain technology has revolutionized various industries by offering decentralized, immutable and transparent data management solutions. Thus, this technology has evolved into a versatile platform with applications in both finance using cryptocurrencies and also in asset management, healthcare, etc. However, as the adoption of Blockchain proliferates, questions arise about the security vulnerabilities it may have, what impact these may have and how they can be addressed. In the following research, after analyzing the Blockchain technology and its characteristics, the main vulnerabilities and attacks that can occur on it will be categorized and analyzed. Then countermeasures and ways to address them will be presented, as well as some gaps on this research and suggestions for future directions in this regard. The purpose of the following research, is to familiarize the reader with Blockchain technology, to inform the reader as to the security risks that may arise on it, and possible ways of dealing with them. Blockchain is a very useful technology that will be used a lot in the future and its users should be well aware of it.

Keywords: *Blockchain, Cryptocurrencies, Security, Vulnerabilities, Countermeasures*

1. Εισαγωγή

1.1 Αντικείμενο Διπλωματικής

Η διπλωματική αυτή πραγματεύεται την ασφάλεια της τεχνολογίας blockchain.

Η έννοια του blockchain θα έλεγε κανείς ότι ξεκινάει πίσω στο 1982 [1] όπου ο κρυπτογράφος David Chaum πρότεινε στην διατριβή του ένα πρωτόκολλο, που έμοιαζε με αυτό του blockchain, για την ασφαλή αποθήκευση δεδομένων. Περισσότερη δουλειά, όμως, στην κρυπτογραφικά ασφαλή αλυσίδα μπλοκ (blockchain) έγινε το 1991-92 [1] από τους Stuart Haber, Scott Storiette και Dave Bayer, οι οποίοι ήθελαν να εφαρμόσουν ένα σύστημα, στο οποίο οι χρονοσφραγίδες των εγγράφων δεν θα μπορούσαν να αλλοιωθούν, χρησιμοποιώντας την τεχνολογία αυτή.

Το πρώτο αποκεντρωμένο blockchain, όπως το γνωρίζουμε σήμερα, σχεδιάστηκε από ένα άτομο, γνωστό ως Satoshi Nakamoto, το 2008. [1] Ο Nakamoto βελτίωσε τον σχεδιασμό με σημαντικό τρόπο, χρησιμοποιώντας μια μέθοδο για τη χρονοσήμανση των μπλοκ χωρίς να απαιτείται η υπογραφή τους από ένα αξιόπιστο μέρος και εισάγοντας μια παράμετρο δυσκολίας για τη σταθεροποίηση του ρυθμού με τον οποίο προστίθενται μπλοκ στην αλυσίδα. Ο σχεδιασμός υλοποιήθηκε το επόμενο έτος από τον Nakamoto ως βασικό συστατικό του κρυπτονομίσματος bitcoin, ο οποίος χρησιμεύει ως ένα δημόσιο ψηφιακό βιβλίο για όλες τις συναλλαγές στο δίκτυο χρησιμοποιώντας τα κρυπτονομίσματα bitcoin.

Έκτοτε, το blockchain είναι μια τεχνολογία, η οποία χρησιμοποιείται όλο και περισσότερο με τα χρόνια, κυρίως για ασφαλείς και γρήγορες συναλλαγές. Ο αποκεντρωμένος χαρακτήρας του και η διαφάνεια που προσφέρει σε συνδυασμό με το ότι εξαλείφει την ανάγκη για κάποιον μεσάζοντα σε συναλλαγές, καθιστούν το blockchain μια τεχνολογία που χρησιμοποιείται από όλο και περισσότερο κόσμο.

Παρόλα αυτά, το blockchain δεν είναι άτρωτο όσον αφορά την ασφάλεια του. Αποτελείται από αρκετά επίπεδα, κάθε ένα από τα οποία μπορεί να δεχθεί επιθέσεις. Στην διπλωματική αυτή, αφού αναλυθούν τα βασικά χαρακτηριστικά της τεχνολογίας blockchain, θα αναλυθούν μια σειρά από τρωτότητες αλλά και επιθέσεις ανά "στρώμα" του blockchain, καθώς και ποιες είναι οι προϋποθέσεις για μια επίθεση αλλά και τι επιπτώσεις μπορεί να έχει. Εν συνεχεία, για κάθε επίθεση θα προταθούν διάφορα αντίμετρα που μπορούν να αντιμετωπίσουν ή να μετριάσουν τον κίνδυνο της εκάστοτε επίθεσης. Τέλος, στην διπλωματική παρατίθενται διάφορα κενά στην έρευνα για την αντιμετώπιση επιθέσεων στο blockchain και μερικές κατευθύνσεις ως προς την κάλυψή τους.

Σε αντίθεση με την υπάρχων βιβλιογραφία που παρέχει αυτές τις πληροφορίες μεμονωμένα, αυτή η διπλωματική παρέχει τις πληροφορίες αυτές συνδυαστικά ενώ προσπαθεί να είναι διεξοδική κατά μήκος όλων των πλευρών (ευπάθειες, επιθέσεις και αντίμετρα) ενώ αποσκοπεί τελικά σε μια εκτεταμένη και αναλυτική ενημέρωση του αναγνώστη σχετικά με την τεχνολογία blockchain και τα χαρακτηριστικά της, τα είδη επιθέσεων που μπορεί να συμβούν σε αυτό, καθώς και τρόπους για την αντιμετώπιση τους.

1.2 Δομή Διπλωματικής

Στην παρακάτω διπλωματική, μετά το πρώτο κεφάλαιο της εισαγωγής, ακολουθούν τα εξής κεφάλαια:

- Κεφάλαιο 2: Υπόβαθρο. Σε αυτό το κεφάλαιο αναφέρεται όλη η πληροφορία υπόβαθρου της τεχνολογίας blockchain. Περιλαμβάνει ορισμό, βασικά χαρακτηριστικά, εκδόσεις, τρόπο λειτουργίας, αρχιτεκτονική, μηχανισμούς συναίνεσης, έξυπνα συμβόλαια και εφαρμογές.
- Κεφάλαιο 3: Μεθοδολογία επιλογής άρθρων. Σε αυτό το κεφάλαιο γίνεται αναφορά στις βασικές ερωτήσεις που προσπαθεί να απαντήσει η διπλωματική, τι είδους πηγών εξετάστηκαν, τι κριτήρια αποδοχής/απόρριψης άρθρων χρησιμοποιήθηκαν καθώς και τα κριτήρια ποιότητας των άρθρων που εφαρμόστηκαν.
- Κεφάλαιο 4: Ζητήματα ασφάλειας. Σε αυτό το κεφάλαιο περιγράφονται οι τρωτότητες της τεχνολογίας blockchain. Επιπροσθέτως, γίνεται μια κατηγοριοποίηση των γνωστών ειδών επιθέσεων στην τεχνολογία, μαζί με τις απειλές αυτών καθώς και μερικές γνωστές επιθέσεις που έχουν γίνει στο παρελθόν.
- Κεφάλαιο 5: Αντίμετρα. Σε αυτό το κεφάλαιο παρουσιάζονται διάφορα αντίμετρα και λύσεις για κάθε μια επίθεση που αναλύθηκε στο προηγούμενο κεφάλαιο, οι οποίες μπορούν να αντιμετωπίσουν ή να μετριάσουν την επίθεση αυτή.
- Κεφάλαιο 6: Ερευνητικά κενά και κατευθύνσεις. Σε αυτό το κεφάλαιο παρουσιάζονται μια σειρά από ερευνητικά κενά που πρέπει να καλυφθούν και μερικές κατευθύνσεις για την αντιμετώπιση τους.
- Κεφάλαιο 7: Συμπεράσματα. Σε αυτό το κεφάλαιο γίνεται μια περίληψη της κύριας συνεισφοράς της αναφοράς καθώς και μια παροχή των πιο βασικών συμπερασμάτων και κρίσιμων ερευνητικών κατευθύνσεων που πρέπει να ακολουθηθούν.

2. Υπόβαθρο

2.1 Ορισμός

Ένα blockchain είναι ένα κοινό, αμετάβλητο, ψηφιακό λογιστικό βιβλίο (ledger) που διευκολύνει τη διαδικασία καταγραφής και διανομής συναλλαγών αλλά και εντοπισμού περιουσιακών στοιχείων (assets) σε όλο το επιχειρηματικό δίκτυο υπολογιστών που διαμοιράζεται το blockchain. Για αυτό το λόγο, το blockchain αναφέρεται και ως τεχνολογία κατανεμημένου ψηφιακού λογιστικού βιβλίου (distributed ledger technology ή DLT).

Με την χρήση της τεχνολογίας αυτής, η ιστορία οποιουδήποτε ψηφιακού περιουσιακού στοιχείου καθίσταται αναλλοίωτη και διαφανής μέσω της χρήσης ενός αποκεντρωμένου δικτύου και κρυπτογραφικού κατακερματισμού. Στην ουσία, κάθε μπλοκ που απαρτίζει την κατανεμημένη βάση της αυξανόμενης λίστας εγγραφών μέσα στο blockchain περιέχει έναν κρυπτογραφικό κατακερματισμό του προηγούμενου μπλοκ, μια χρονική σήμανση και τα δεδομένα συναλλαγών.

Το ιστορικό δεν μπορεί να τροποποιηθεί αναδρομικά χωρίς την αλλαγή όλων των επακόλουθων μπλοκ και τη συναίνεση του δικτύου. Επιπλέον, κάθε συναλλαγή στο παρόν ψηφιακό αρχείο εγκρίνεται με την ψηφιακή υπογραφή του ιδιοκτήτη των εκάστοτε περιουσιακών στοιχείων που πρόκειται να χρησιμοποιηθούν στην συναλλαγή, η οποία πιστοποιεί την συναλλαγή και την προστατεύει από τυχόν παραποίηση. Ως εκ τούτου, οι πληροφορίες που περιέχει το ψηφιακό αυτό αρχείο θεωρούνται ιδιαίτερα ασφαλείς.

Εκτός όλων των άλλων, το blockchain είναι η τεχνολογία που επιτρέπει την ύπαρξη των κρυπτονομισμάτων (cryptocurrency), δηλαδή των ψηφιακών νομισμάτων, ή πιο απλά των ψηφιακών χρημάτων. Το Bitcoin blockchain, για παράδειγμα, περιέχει μια καταγραφή κάθε φορά που κάποιος έστειλε ή έλαβε Bitcoin για λόγους διαφάνειας, έτσι ώστε να υπάρχουν καταγεγραμμένα όλα τα στοιχεία μεταξύ των ατόμων που αφορά η συναλλαγή. Τα κρυπτονομίσματα και η τεχνολογία blockchain που τους δίνει την εξουσία καθιστούν δυνατή τη μεταφορά αξίας στο διαδίκτυο χωρίς την ανάγκη για έναν μεσάζοντα, όπως μια τράπεζα ή εταιρεία πιστωτικών καρτών, μειώνοντας τον κίνδυνο και το κόστος για όλους τους εμπλεκόμενους. [2] [3] [4] [5] [6]

2.2 Βασικά Χαρακτηριστικά

- ***Αμετάβλητο*:** Το blockchain είναι ένα μόνιμο και αμετάβλητο δίκτυο όσον αφορά τα περιεχόμενα που καταγράφονται σε αυτό (δηλ. δεν μπορούν να αλλάξουν και είναι μόνιμα αποθηκευμένα). Αυτό είναι ένα από τα σημαντικότερα χαρακτηριστικά της τεχνολογίας αυτής. Η τεχνολογία blockchain λειτουργεί μέσω μιας συλλογής κόμβων. Κόμβος είναι κάθε μηχανή που εκτελεί το λογισμικό του blockchain για να επαληθεύει και να διατηρεί το σύνολο των αρχείων κάθε συναλλαγής που συμβαίνει στο δίκτυο (του blockchain). Για να προστεθεί μια συναλλαγή στο δίκτυο, πρέπει πρώτα κάθε κόμβος να ελέγξει την εγκυρότητα της συναλλαγής. Εφόσον η πλειοψηφία όλων των κόμβων πιστεύουν ότι είναι μια έγκυρη συναλλαγή, τότε προστίθεται στο δίκτυο. Οι επικυρωμένες εγγραφές είναι μη αναστρέψιμες και δεν είναι δυνατό να αλλάξουν. Αυτό σημαίνει ότι κάθε χρήστης στο δίκτυο δεν θα μπορεί να τις επεξεργαστεί, να τις αλλάξει ή να τις διαγράψει. Συνεπώς, με αυτόν τον τρόπο αποφεύγεται η παραποίηση δεδομένων. [7] [8]
- ***Διανεμημένο*:** Όλοι οι συμμετέχοντες στο δίκτυο έχουν ένα αντίγραφο του ψηφιακού λογιστικού βιβλίου για πλήρη διαφάνεια. Ένα ψηφιακό αρχείο θα παρέχει πλήρεις πληροφορίες σχετικά με όλους τους συμμετέχοντες στο δίκτυο και τις συναλλαγές, οπότε έτσι θα είναι διανεμημένο. Οποιοσδήποτε διαθέτει την απαραίτητη πρόσβαση μπορεί να δει το ψηφιακό λογιστικό βιβλίο, γεγονός που αυξάνει τη διαφάνεια και την αξιοπιστία της διαδικασίας. Κανείς από εκείνους που χρησιμοποιούν το δίκτυο δεν μπορεί να λάβει ειδική εύνοια ή να αντιμετωπίσει οποιαδήποτε μορφή προκατάληψης από τους κόμβους του δικτύου. Η διαδικασία για την προσθήκη μπλοκ είναι η ίδια για όλους. [7] [8]
- ***Αποκεντρωμένο*:** Η τεχνολογία blockchain είναι ένα αποκεντρωμένο σύστημα. Αυτό σημαίνει ότι δεν υπάρχει κεντρική αρχή που να ελέγχει ένα δίκτυο blockchain - βέβαια αυτό εξαρτάται από το είδος του blockchain. Αντίθετα, το δίκτυο αποτελείται από ένα μεγάλο αριθμό κόμβων που συνεργάζονται για την επαλήθευση και την επικύρωση των συναλλαγών. Έτσι, καθώς ένα δίκτυο blockchain δεν εξαρτάται από ανθρώπινους υπολογισμούς, είναι πλήρως οργανωμένο και ανθεκτικό σε σφάλματα, αφού οι λειτουργίες αυτοματοποιούνται και δεν απαιτούν ανθρώπινο έλεγχο. Ο αποκεντρωμένος χαρακτήρας του blockchain διευκολύνει τη δημιουργία ενός διαφανούς προφίλ για κάθε συμμετέχοντα στο δίκτυο, ο οποίος πλέον θα έχει τον έλεγχο των περιουσιακών του στοιχείων και δεν θα χρειάζεται να βασίζεται σε τρίτους για να τα διατηρήσουν και να τα διαχειριστούν. Έτσι, μέσω του blockchain, οι χρήστες βρίσκονται σε σαφή θέση εξουσίας. [7]
- ***Ασφαλές*:** Όλες οι εγγραφές στο blockchain είναι ξεχωριστά κρυπτογραφημένες. Η χρήση της κρυπτογράφησης προσθέτει ένα ακόμα επίπεδο ασφάλειας σε ολόκληρη τη διαδικασία στο δίκτυο blockchain. Κάθε πληροφορία στο blockchain είναι κρυπτογραφημένη, πράγμα που σημαίνει ότι κάθε κομμάτι των δεδομένων έχει μια μοναδική ταυτότητα στο δίκτυο. Όλα τα μπλοκ περιέχουν ένα μοναδικό κατακερματισμό του δικού τους (περιεχομένου) και τον κατακερματισμό του προηγούμενου μπλοκ. Λόγω αυτής της ιδιότητας, τα μπλοκ συνδέονται κρυπτογραφικά μεταξύ τους. Αρκετά blockchain κρυπτογραφούν τα δεδομένα χρησιμοποιώντας τον SHA-256, ο οποίος είναι ένας από τους πιο ισχυρούς αλγόριθμους κατακερματισμού. Αυτός ο αλγόριθμος δημιουργεί μια υπογραφή 256-bit για ένα σχεδόν μοναδικό κείμενο. Το blockchain χρησιμοποιεί, επίσης, ψηφιακές υπογραφές για την επαλήθευση των χρηστών. Ο τύπος κρυπτογράφησης που χρησιμοποιείται στις αρχιτεκτονικές blockchain είναι η κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού. Η κρυπτογραφία αυτή δημιουργεί ξεχωριστά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί κρυπτογράφησης είναι δημόσιο, ενώ το κλειδί αποκρυπτογράφησης είναι ιδιωτικό. Η κατακερματισμένη έκδοση του δημόσιου κλειδιού χρησιμεύει ως διεύθυνση πορτοφολιού που μοιράζεται κάποιος για να λάβει πληρωμή. Εν

τω μεταξύ, το ιδιωτικό κλειδί γίνεται ο κωδικός πρόσβασης που χρησιμοποιούν οι χρήστες του blockchain για να έχουν πρόσβαση και να ξοδέψουν τα χρήματά τους ή να εξουσιοδοτήσουν δράση σε ένα έξυπνο συμβόλαιο. Το μήνυμα του αποστολέα κατακερματίζεται ως μέρος της διαδικασίας και το αποτέλεσμα αποστέλλεται μέσω ενός αλγορίθμου υπογραφής με τη χρήση του ιδιωτικού κλειδιού του χρήστη για την παραγωγή της ψηφιακής υπογραφής του χρήστη. Το μήνυμα του χρήστη, η ψηφιακή υπογραφή και το δημόσιο κλειδί αποστέλλονται κατά τη διάρκεια της συναλλαγής. Αντιλαμβανόμαστε λοιπόν ότι το blockchain είναι ένα σύστημα αρκετά ασφαλές όπου όλες οι πληροφορίες είναι κρυπτογραφημένες, τα μπλοκ συνδέονται κρυπτογραφικά μεταξύ τους και ο κάθε χρήστης επαληθεύεται με ψηφιακή υπογραφή και έχει το δικό του σετ από δημόσια και ιδιωτικά κλειδιά. Παρόλα αυτά το σύστημα blockchain δεν είναι άτρωτο. Στο Κεφάλαιο 4 θα παρατηρηθούν μερικές ευπάθειες που μπορεί να έχει ένα τέτοιο σύστημα, καθώς και μερικές επιθέσεις που μπορούν να πραγματοποιηθούν σε αυτό. [7] [9]

- ***Συναίνεση*:** Κάθε blockchain εφαρμόζει έναν αλγόριθμο συναίνεσης για να βοηθήσει το δίκτυο να λάβει γρήγορες και αμερόληπτες αποφάσεις. Η συναίνεση είναι ένας αλγόριθμος λήψης αποφάσεων για την ομάδα των κόμβων που δραστηριοποιούνται στο δίκτυο για να επιτευχθεί συμφωνία γρήγορα και ταχύτερα και για την ομαλή λειτουργία του όλου συστήματος. Οι κόμβοι μπορεί να μην εμπιστεύονται ο ένας τον άλλο, αλλά μπορούν να εμπιστευτούν τον αλγόριθμο συναίνεσης που τρέχει στον πυρήνα του δικτύου για να λάβει αποφάσεις. Όταν εκατομμύρια κόμβοι επικυρώνουν μια συναλλαγή, η συναίνεση είναι απολύτως απαραίτητη για να εκτελεστεί ομαλά ένα σύστημα. Υπάρχουν πολλοί αλγόριθμοι συναίνεσης διαθέσιμοι. Κάθε blockchain πρέπει να έχει έναν αλγόριθμο συναίνεσης, διαφορετικά θα χάσει την αξία του. Στην Ενότητα 2.7 θα αναλυθούν περαιτέρω οι πιο σημαντικοί μηχανισμοί συναίνεσης. [7] [8]
- ***Ομοφωνία*:** Όλοι οι συμμετέχοντες στο δίκτυο συμφωνούν για την εγκυρότητα των εγγραφών πριν αυτές προστεθούν στο δίκτυο. Όταν ένας κόμβος θέλει να προσθέσει ένα εξορυγμένο μπλοκ στο δίκτυο, τότε πρέπει να πάρει την πλειοψηφία των ψήφων, διαφορετικά το μπλοκ δεν μπορεί να προστεθεί στο δίκτυο. Η ομόφωνη συμφωνία μεταξύ των κόμβων του δικτύου οδηγεί σε ένα blockchain που περιέχει επαληθευμένα δεδομένα (συναλλαγές) τα οποία το δίκτυο ισχυρίζεται ότι είναι σωστά. Οπότε, το blockchain λειτουργεί με την προσθήκη μπλοκ δεδομένων στην αλυσίδα και η ουσία της συναίνεσης είναι να εξασφαλιστεί ότι κάθε μπλοκ που προστίθεται στην αλυσίδα είναι η μία και μοναδική εκδοχή της αλήθειας στην οποία συμφωνούν όλοι οι κόμβοι του συστήματος. [7] [8]
- ***Ταχύτερη διευθέτηση*:** Το blockchain προσφέρει μια ταχύτερη διευθέτηση σε σύγκριση με τα παραδοσιακά τραπεζικά συστήματα σε μερικές περιπτώσεις, καθώς εξαλείφει τον μεσάζοντα και αυξάνει την αποτελεσματικότητα. Για παράδειγμα, σε παραδοσιακά τραπεζικά συστήματα υπάρχουν ωράρια λειτουργίας και μπορεί να υπάρχουν μέρες (κυρίως σαββατοκύριακα) που δεν ελέγχονται και επεξεργάζονται συναλλαγές, κάτι που δεν ισχύει στην περίπτωση του blockchain που λειτουργεί συνεχώς. Επίσης σε περιπτώσεις διασυνοριακών συναλλαγών, τα παραδοσιακά τραπεζικά συστήματα χρειάζονται αρκετές διευθετήσεις/διακανονισμούς που καθυστερούν την διενέργεια μιας συναλλαγής, σε αντίθεση με το blockchain. [7]
- ***Αυξημένη χωρητικότητα*:** Ένα άλλο χαρακτηριστικό είναι ότι αυξάνει την συνολική (υπολογιστική) χωρητικότητα όλου του συστήματος, λόγω του ότι υπάρχουν πολλοί υπολογιστές που εργάζονται μαζί. Έτσι παρέχεται ένα πιο μεγάλο και ισχυρό σύστημα σε σχέση με το να υπήρχε ένα μικρό σύστημα με λίγες συσκευές που θα είχαν μεμονωμένα όλη την υπολογιστική ισχύ. Έτσι παρέχεται και μεγαλύτερη ασφάλεια, επειδή το σύστημα είναι πιο δύσκολο να τερματιστεί (λόγω επίθεσης ή σφαλμάτων μηχανών) ή να ελεγχθεί. [8]

2.3 Εκδόσεις Blockchain

Blockchain 1.0: Currency

Η πρώτη έκδοση του blockchain είναι και η πιο γνωστή. Αφορά την χρήση των κρυπτονομισμάτων, η οποία είναι δυνατή με την τεχνολογία DLT (Distributed Ledger Technology). Η τεχνολογία αυτή εισήχθη το 2005 από τον Hall Finley [11]. Αυτό κάνει δυνατές χρηματικές συναλλαγές βάση την τεχνολογία blockchain. Ουσιαστικά, τα κρυπτονομίσματα παίζουν τον ρόλο των χρημάτων συναλλαγής.

Το Blockchain 1.0 αναπτύχθηκε πάνω στην ιδέα και τη δομή του Bitcoin. Επικεντρώθηκε κυρίως στην ανάπτυξη και τη δημιουργία νέων κρυπτονομισμάτων (κάθε ένα στο δικό του blockchain). Αυτή η έκδοση είναι και η πιο απλή μορφή ενός αποκεντρωμένου ψηφιακού λογιστικού βιβλίου (ledger) για καταγραφή συναλλαγών και αποθήκευση των δεδομένων σε πολλούς υπολογιστές. Ουσιαστικά, εισάγει ένα διαφανές, δημόσια προσβάσιμο, πλήρως αποκεντρωμένο, αμετάβλητο ψηφιακό λογιστικό βιβλίο και κατανεμημένο σύστημα συναλλαγών στην παγκόσμια χρηματοπιστωτική αγορά. [10]

Blockchain 2.0: Smart Contracts

Η νέα έκδοση του blockchain εισήχθη, καθώς θεωρήθηκε ότι στην έκδοση 1.0 υπήρχε έλλειψη κλιμακωσιμότητας του δικτύου, όπου γεμάτα πλήθος κόμβων δίκτυα κάποιες φορές οδηγούσαν σε μεγαλύτερους χρόνους συναλλαγών (οπότε η αύξηση των πόρων του δικτύου μείωνε την απόδοση), ενώ σε μερικές περιπτώσεις η εξόρυξη bitcoin θεωρούνταν σπατάλη, κάτι που συμβαίνει όταν δαπανάται περισσότερη ηλεκτρική ενέργεια (κατά την διάρκεια που ένας υπολογιστής εξορύσσει bitcoin) σε σχέση με το πόσο bitcoin κερδίζει ο ανθρακωρύχος. Ταυτόχρονα θεωρούνταν πως υπήρχε πρόβλημα επεκτασιμότητας καθώς η έκδοση 1.0 περιοριζόταν μόνο σε συναλλαγές κρυπτονομισμάτων. Σε αυτή την νέα έκδοση (την 2.0), λοιπόν, το blockchain δεν περιορίζεται μόνο στα κρυπτονομίσματα, αλλά επεκτείνεται μέχρι και τις έξυπνες συμβάσεις. Αυτές οι συμβάσεις επιτρέπουν σε δύο χρήστες ή οργανισμούς να κάνουν κάτι περισσότερο από απλές συναλλαγές κρυπτονομισμάτων. Το Ethereum, για παράδειγμα, περιέχει μια εικονική μηχανή με πολλαπλά επίπεδα πληροφοριών, λογαριασμούς χρηστών, συμβόλαια και λογιστική κόστους (μια μετρική γνωστή ως "αέριο" (gas)).

Τα έξυπνα συμβόλαια είναι υπολογιστικά προγράμματα μέσα στο blockchain που εκτελούνται αυτόματα όταν ορισμένες προκαθορισμένες συνθήκες συναντώνται. Στόχος του έξυπνου συμβολαίου είναι να παρέχει ασφάλεια κατά την επεξεργασία των συναλλαγών και να μειώσει το κόστος και το χρόνο των συναλλαγών. Η αυτοματοποιημένη εκτέλεση και επικύρωση των έξυπνων συμβολαίων μπορεί να οδηγήσει σε ταχύτερους χρόνους διακανονισμού συναλλαγών. Επίσης οι έξυπνες συμβάσεις μειώνουν την ανάγκη για μεσάζοντες, με αποτέλεσμα την εξοικονόμηση κόστους για τους συμμετέχοντες. Στα δίκτυα blockchain, όπου απαιτούνται τέλη για την εκτέλεση έξυπνων συμβάσεων (π.χ. Ethereum), το κόστος εκτέλεσης έξυπνων συμβάσεων είναι συνήθως χαμηλότερο από τα τέλη που σχετίζονται με τους παραδοσιακούς μεσάζοντες. Το μεγάλο πλεονέκτημα αυτής της τεχνολογίας είναι ότι το blockchain κάνει πολύ δύσκολο να παραβιαστούν οι έξυπνες συμβάσεις, καθώς λειτουργούν σε ένα αποκεντρωμένο δίκτυο, πράγμα που σημαίνει ότι δεν ελέγχονται από καμία μεμονωμένη οντότητα και ο κώδικάς τους είναι δημόσια ορατός και αμετάβλητος. Τέλος, οι έξυπνες συμβάσεις μπορούν να προσαρμοστούν ώστε να ανταποκρίνονται σε ένα ευρύ φάσμα περιπτώσεων χρήσης, από απλές συμφωνίες έως πολύπλοκες συμβάσεις πολλαπλών μερών. Αυτή η ευελιξία τα καθιστά ευέλικτα για διάφορους κλάδους και εφαρμογές. [10] [12]

Blockchain 3.0: DApps

Το DApp είναι συντόμευση του Decentralized Application, δηλαδή αποτελεί αποκεντρωμένη εφαρμογή. Χρησιμοποιεί αποκεντρωμένη αποθήκευση και επικοινωνία που υπάρχουν σαν χαρακτηριστικά στο blockchain, αλλά πλέον περνάει στο επίπεδο της εφαρμογής. Μπορούμε να πούμε ότι τα DApps είναι μέρος ενός λογισμικού που επικοινωνεί με το blockchain, το οποίο με την σειρά του διαχειρίζεται και ελέγχει την κατάσταση όλων των φορέων του δικτύου. Σε αντίθεση με κεντρικές εφαρμογές που εκτελούνται σε έναν μόνο υπολογιστή, οι εφαρμογές που βασίζονται στο blockchain εκτελούνται σε ένα δίκτυο P2P. Τα περισσότερα DApps έχουν το frontend τους γραμμένο σε οποιαδήποτε γλώσσα προγραμματισμού. Το frontend αυτό κάνει κλήσεις στο backend τους, του οποίου ο κώδικας (έξυπνο συμβόλαιο) τρέχει σε ένα αποκεντρωμένο peer-to-peer δίκτυο, ένα blockchain. [11] [12]

Blockchain 4.0: Making blockchain usable in industry

Πολλοί ειδικοί θεωρούν ότι το Blockchain 3.0 είναι η τελική εξέλιξη της τεχνολογίας blockchain. Παρόλα αυτά πολλοί άλλοι θεωρούν ότι για να αρχίσει το blockchain να χρησιμοποιείται σε επιχειρησιακές απαιτήσεις, και να προσδιορίζει λύσεις και προσεγγίσεις που κάνουν την τεχνολογία χρήσιμη σε αυτές, είναι απαραίτητη η δημιουργία μιας νέας έκδοσης του blockchain, της 4.0. Η διαχείριση της εφοδιαστικής αλυσίδας, οι ροές εργασιών έγκρισης, οι χρηματοπιστωτικές συναλλαγές και οι πληρωμές βάσει όρων, η συλλογή δεδομένων IoT, η διαχείριση της υγείας και η διαχείριση των περιουσιακών στοιχείων είναι μόνο μερικά παραδείγματα τομέων που μπορούν να ενισχυθούν από αυτή την νέα έκδοση της τεχνολογίας blockchain. Γενικά, το Blockchain 4.0 θα επικεντρώνεται στην καινοτομία. Η ταχύτητα, η εμπειρία του χρήστη και η χρηστικότητα από μεγαλύτερη και κοινή μάζα ανθρώπων θα είναι οι βασικοί τομείς εστίασης για το Blockchain 4.0. Σε αυτή τη γενιά θα περιμένουμε την εμφάνιση περισσότερων blockchains με επίκεντρο το Web 3.0 Το Web 3.0 στοχεύει στη δημιουργία ενός αυτόνομου, ανοιχτού και έξυπνου διαδικτύου, και θα στηριχθεί σε αποκεντρωμένα πρωτόκολλα, τα οποία μπορεί να παρέχει το Blockchain. Οι εφαρμογές Web 3.0 θα διαθέτουν συνεκτική διαλειτουργικότητα, αυτοματοποίηση μέσω έξυπνων συμβάσεων, καθώς και ενσωμάτωση και αποθήκευση αρχείων δεδομένων P2P. Τέλος, το Blockchain 4.0 θα επιτρέψει στις επιχειρήσεις να μεταφέρουν μέρος ή το σύνολο των σημερινών λειτουργιών τους σε ασφαλείς, αυτο-καταγραφόμενες εφαρμογές που βασίζονται σε αποκεντρωμένα, αξιόπιστα και κρυπτογραφημένα λογιστικά βιβλία. Οι επιχειρήσεις και τα ιδρύματα θα μπορούν εύκολα να απολαμβάνουν τα βασικά οφέλη του Blockchain. [12] [99]

2.4 Τρόπος Λειτουργίας Blockchain

Αρχικά παρέχουμε γενικές γνώσεις της λειτουργίας blockchain. Έπειτα, εξηγούμε με απλά λόγια την διαδικασία μιας συναλλαγής σε αυτό.

Τα δεδομένα που αποθηκεύονται μέσα σε κάθε μπλοκ εξαρτώνται από τον τύπο του blockchain. Για παράδειγμα, στη δομή blockchain του Bitcoin, το μπλοκ διατηρεί δεδομένα στα πλαίσια μιας συναλλαγής, σχετικά με τον παραλήπτη, τον αποστολέα και το ποσό των νομισμάτων.

Ένας κατακερματισμός (hash) είναι σαν ένα δακτυλικό αποτύπωμα (μακρύ αλφαριθμητικό που αποτελείται από ορισμένα ψηφία και γράμματα). Κάθε κατακερματισμός μπλοκ παράγεται με τη βοήθεια ενός κρυπτογραφικού αλγορίθμου κατακερματισμού (SHA 256 στο Bitcoin blockchain). Κατά συνέπεια, αυτό βοηθά στην εύκολη ταυτοποίηση κάθε μπλοκ σε μια δομή blockchain. Τη στιγμή που δημιουργείται ένα μπλοκ, επισυνάπτεται αυτόματα ένας κατακερματισμός, ενώ τυχόν αλλαγές που πραγματοποιούνται σε ένα μπλοκ επηρεάζουν και την αλλαγή του αντίστοιχου κατακερματισμού. Με απλά λόγια, οι κατακερματισμοί βοηθούν στον εντοπισμό τυχόν αλλαγών στα μπλοκ.

Το τελευταίο στοιχείο εντός του μπλοκ είναι ο κατακερματισμός από ένα προηγούμενο μπλοκ. Αυτό δημιουργεί μια αλυσίδα μπλοκ και είναι το κύριο στοιχείο πίσω από την ασφάλεια της αρχιτεκτονικής blockchain. Για παράδειγμα, το μπλοκ 44 δείχνει στο μπλοκ 45. Το πρώτο μπλοκ σε μια αλυσίδα είναι λίγο ιδιαίτερο καθώς όλα τα επιβεβαιωμένα και επικυρωμένα μπλοκ προέρχονται από αυτό το μπλοκ. Αυτό το μπλοκ ονομάζεται μπλοκ γένεσης (genesis block).

Τυχόν απόπειρες αλλοίωσης προκαλούν την αλλαγή των μπλοκ. Στη συνέχεια, όλα τα επόμενα μπλοκ μεταφέρουν εσφαλμένες πληροφορίες και καθιστούν άκυρο ολόκληρο το σύστημα blockchain. Παρόλα αυτά, η τεχνολογία blockchain έχει σχεδιαστεί για να είναι ανθεκτική στην παραποίηση, με την χρήση κατάλληλων μηχανισμών συναίνεσης αλλά και με την χρήση ισχυρών κρυπτογραφικών συναρτήσεων και ψηφιακών υπογραφών.

Όλοι οι κόμβοι στο εσωτερικό μιας αρχιτεκτονικής blockchain εφαρμόζουν ένα πρωτόκολλο συναίνεσης, χάρη στο οποίο λειτουργούν. Στο bitcoin, το πρωτόκολλο που χρησιμοποιείται είναι το proof-of-work (PoW). Αυτό επιτρέπει σε έναν χρήστη να "δουλεύει" με σκοπό τη δημιουργία νέων μπλοκ. Στην αρχιτεκτονική του blockchain του Bitcoin, χρειάζονται περίπου 10 λεπτά για να προσδιοριστεί η απαραίτητη απόδειξη εργασίας (proof-of-work) και να προστεθεί ένα νέο μπλοκ στην αλυσίδα. Η εργασία αυτή γίνεται από τους ανθρακωρύχους (miners) (ειδικούς κόμβους εντός της δομής της αλυσίδας μπλοκ του Bitcoin). Οι ανθρακωρύχοι μπορούν να κρατήσουν την αμοιβή του μπλοκ (ανάλογα με την δυσκολία εξόρυξης) καθώς και τα τέλη συναλλαγών που προστέθηκαν στο μπλοκ του, εφόσον αυτό επαληθευτεί από την πλειοψηφία των κόμβων (με βάση τον μηχανισμό συναίνεσης) ως ανταμοιβή.

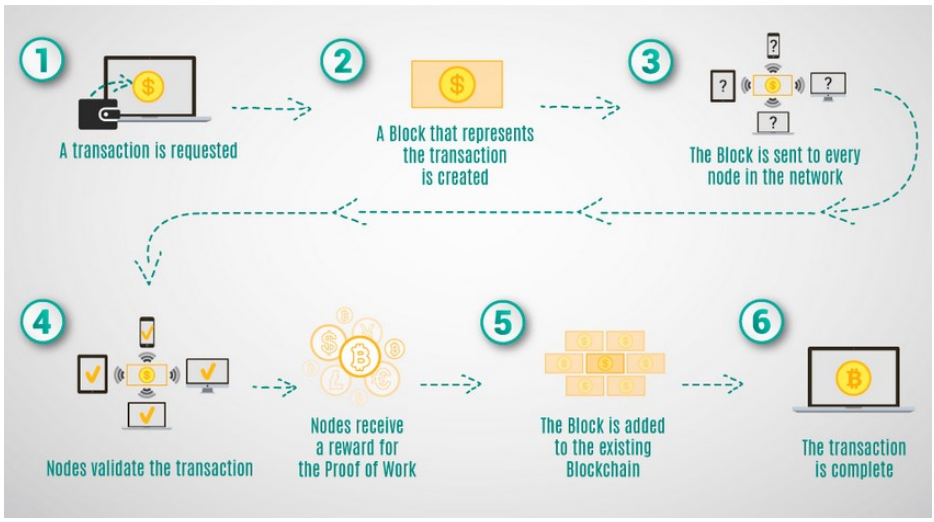
Κάθε νέος χρήστης (κόμβος) που εντάσσεται στο ομότιμο δίκτυο του blockchain, λαμβάνει ένα πλήρες αντίγραφο του συστήματος. Μόλις δημιουργηθεί ένα νέο μπλοκ, αποστέλλεται σε κάθε κόμβο εντός του συστήματος blockchain. Στη συνέχεια, κάθε κόμβος επαληθεύει το μπλοκ και ελέγχει αν οι πληροφορίες που δηλώνονται εκεί είναι σωστές, με βάση τον μηχανισμό συναίνεσης. Εάν όλα είναι εντάξει, σύμφωνα με την πλειοψηφία των κόμβων, το μπλοκ προστίθεται στην τοπική αλυσίδα μπλοκ (λογιστικό βιβλίο) σε κάθε κόμβο.

Ένα σύστημα συναίνεσης, εκτός από τον τρόπο λειτουργίας, περιέχει ένα σύνολο κανόνων δικτύου. Αν όλοι τους τηρούν, τότε οι κανόνες γίνονται αυτο-επιβαλλόμενοι στο εσωτερικό του blockchain.

Για παράδειγμα, το blockchain Bitcoin έχει έναν κανόνα συναίνεσης που ορίζει ότι το ποσό μιας συναλλαγής (πχ. 10 BTC (κρυπτονόμισμα του Bitcoin)) πρέπει να κόβεται στο μισό (5 BTC) μετά από κάθε 200.000 μπλοκ. Αυτό είναι το λεγόμενο halfing. [13]

Επίσης, μπορούν να απομείνουν μόνο 4 εκατομμύρια BTC προς εξόρυξη, καθώς υπάρχει ένα μέγιστο όριο 21 εκατομμυρίων BTC που έχει καθοριστεί στο σύστημα blockchain του Bitcoin από το πρωτόκολλο. Μόλις οι ανθρακωρύχοι ξεκλειδώσουν αυτό το ποσό των BTC, η προσφορά Bitcoins τελειώνει, εκτός κι αν αλλάξει το πρωτόκολλο.

Η διαδικασία μια συναλλαγής σε ένα blockchain, μπορεί να αναλυθεί σε απλά βήματα ως εξής, όπως φαίνονται και στην Εικόνα 1.: [13] [14]



Εικόνα 1. Τρόπος Λειτουργίας Blockchain

1. *Διευκόλυνση μιας συναλλαγής*: Μια νέα συναλλαγή εισέρχεται στο δίκτυο blockchain. Όλες οι πληροφορίες που πρέπει να μεταδοθούν κρυπτογραφούνται διπλά με τη χρήση δημόσιων και ιδιωτικών κλειδιών.

2. *Επαλήθευση της συναλλαγής*: Η συναλλαγή στη συνέχεια διαβιβάζεται στο δίκτυο ομότιμων υπολογιστών (του blockchain) που είναι κατανεμημένοι σε όλο τον κόσμο. Όλοι οι κόμβοι του δικτύου θα ελέγξουν την εγκυρότητα της συναλλαγής, όπως αν υπάρχει επαρκές υπόλοιπο για την πραγματοποίηση της συναλλαγής.

3. *Σχηματισμός νέου μπλοκ*: Σε ένα τυπικό δίκτυο blockchain υπάρχουν πολλοί κόμβοι και πολλές συναλλαγές επαληθεύονται ταυτόχρονα. Μόλις η συναλλαγή επαληθευτεί και δηλωθεί ως νόμιμη συναλλαγή, θα προστεθεί στο mempool (πισίνα μνήμης) ή αλλιώς transaction pool. Όλες οι επαληθευμένες συναλλαγές σε έναν συγκεκριμένο κόμβο σχηματίζουν ένα mempool (πισίνα μνήμης) ενώ πολλαπλές mempools σχηματίζουν ένα μπλοκ.

4. *Αλγόριθμος συναίνεσης*: Οι κόμβοι που σχηματίζουν ένα ολόκληρο μπλοκ θα προσπαθήσουν να προσθέσουν το μπλοκ στο δίκτυο blockchain για να το καταστήσουν μόνιμο. Αυτό θα γίνει εφόσον λύσουν τον μαθηματικό γρίφο (δηλαδή βρουν το nonce) και στην συνέχεια, το μπλοκ τους επαληθευτεί από την πλειοψηφία των κόμβων του δικτύου με βάση τον αλγόριθμο συναίνεσης.

Αλλά αν επιτραπεί σε κάθε κόμβο να προσθέτει μπλοκ με αυτόν τον τρόπο, τότε θα διαταραχθεί η λειτουργία του δικτύου blockchain, καθώς μπορεί να υπάρχουν περιπτώσεις που 2 ανθρακωρύχοι θα βρουν ταυτόχρονα την μαθηματική λύση και θα προσπαθήσουν να προσθέσουν το μπλοκ τους. Έτσι κάποιοι κόμβοι θα πάνε να επαληθεύσουν το μπλοκ του ενός και κάποιοι του άλλου. Για την επίλυση αυτού του προβλήματος, οι κόμβοι χρησιμοποιούν τον μηχανισμό συναίνεσης χάρη στον οποίο υπερισχύει ο κανόνας της μεγαλύτερης αλυσίδας (δηλαδή της αλυσίδας με την περισσότερη απόδειξη εργασίας). Στο τέλος, το μπλοκ που βρίσκεται σε αυτή την αλυσίδα επικυρώνεται και οι κόμβοι που επικύρωναν την άλλη αλυσίδα αρχίζουν και ακολουθούν και πάλι την κύρια.

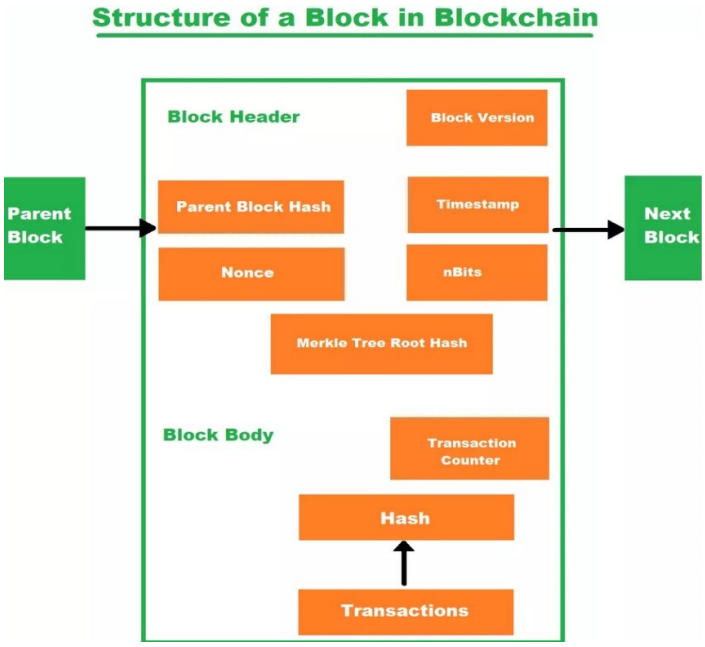
Έτσι διασφαλίζεται ότι κάθε νέο μπλοκ που προστίθεται στο Blockchain είναι η μία και μοναδική εκδοχή της αλήθειας που έχει συμφωνηθεί από όλους τους κόμβους στο Blockchain και μόνο ένα έγκυρο μπλοκ προσαρτάται με ασφάλεια στο blockchain. Ο κόμβος που τελικά κατορθώνει να προσθέσει ένα μπλοκ στο blockchain θα λάβει μια ανταμοιβή. Ως εκ τούτου αποκαλείται "ανθρακωρύχος" (miner). Ο αλγόριθμος συναίνεσης δημιουργεί έναν κωδικό κατακερματισμού για το συγκεκριμένο μπλοκ, ο οποίος απαιτείται για την προσθήκη του μπλοκ στο blockchain.

5. *Προσθήκη του νέου μπλοκ στην αλυσίδα μπλοκ (λογιστικό βιβλίο)*: Αφού το νέο δημιουργηθέν μπλοκ λάβει την τιμή κατακερματισμού του και πιστοποιηθεί, τώρα είναι έτοιμο να προστεθεί στην αλυσίδα μπλοκ. Σε κάθε μπλοκ υπάρχει η τιμή κατακερματισμού του προηγούμενου μπλοκ και με αυτόν τον τρόπο τα μπλοκ συνδέονται κρυπτογραφικά μεταξύ τους για να σχηματίσουν μια αλυσίδα μπλοκ. Ένα νέο μπλοκ προστίθεται στο ανοικτό άκρο του blockchain.

6. *Η συναλλαγή ολοκληρώθηκε*: Μόλις το μπλοκ προστεθεί στο blockchain, η συναλλαγή επιτέλους ολοκληρώνεται και τα στοιχεία αυτής της συναλλαγής αποθηκεύονται μόνιμα στην αλυσίδα μπλοκ. Οποιοσδήποτε μπορεί να αντλήσει τα στοιχεία της συναλλαγής και να επιβεβαιώσει τη συναλλαγή.

2.5 Αρχιτεκτονική Μπλοκ στο Blockchain

Η δομή ενός μπλοκ στο blockchain, όπως φαίνεται και στην Εικόνα 2. αποτελείται από τα εξής μέρη [15]:



Εικόνα 2. Αρχιτεκτονική Μπλοκ στο Blockchain

(Block Header) Επικεφαλίδα Μπλοκ: Χρησιμοποιείται για την αναγνώριση του συγκεκριμένου μπλοκ σε ολόκληρη την αλυσίδα μπλοκ. Μια επικεφαλίδα ενός νέου μπλοκ κατακερματίζεται περιοδικά από τους ανθρακωρύχους αλλάζοντας την τιμή του nonce (θα εξηγηθεί λίγο πιο κάτω) ως μέρος της κανονικής δραστηριότητας εξόρυξης μέχρι να ικανοποιηθεί μια συγκεκριμένη συνθήκη. Στην επικεφαλίδα μπλοκ περιέχονται τα παρακάτω σύνολα μεταδεδομένων: Τρεις ιδιότητες/σύνολα μεταδεδομένων

(Previous Block Address / Hash) Διεύθυνση προηγούμενου μπλοκ/κατακερματισμός: Χρησιμοποιείται για τη σύνδεση του i+1 μπλοκ με το i μπλοκ χρησιμοποιώντας κατακερματισμό. Εν ολίγοις, είναι μια αναφορά στον κατακερματισμό του αμέσως προηγούμενου μπλοκ στην αλυσίδα.

(Timestamp) Χρονοσήμανση: Είναι ένα σύστημα που επαληθεύει τα δεδομένα στο μπλοκ και αποδίδει χρόνο ή ημερομηνία δημιουργίας για το μπλοκ και άρα για τα ψηφιακά έγγραφα που αυτό περιέχει. Όταν ένας ανθρακωρύχος ή ένας επικυρωτής δημιουργεί ένα νέο μπλοκ, περιλαμβάνει μια χρονοσφραγίδα στην επικεφαλίδα του μπλοκ. Αυτή η χρονοσφραγίδα αντιπροσωπεύει την κατά προσέγγιση ώρα κατά την οποία ο ανθρακωρύχος άρχισε να εργάζεται στο μπλοκ.

(Nonce): Ένας αριθμός που χρησιμοποιείται μόνο μία φορά. Αποτελεί κεντρικό μέρος της απόδειξης της εργασίας (στο Proof of Work, σε περίπτωση άλλου μηχανισμού συναίνεσης το σχέδιο αλλάζει) στο μπλοκ. Οι ανθρακωρύχοι, δοκιμάζουν και εξαλείφουν πολλά Nonce ανά δευτερόλεπτο μέχρι να βρουν ένα Nonce με αξία που είναι έγκυρο. Το nonce είναι μια τιμή που οι ανθρακωρύχοι μπορούν να προσαρμόσουν και να συμπεριλάβουν στα δεδομένα του μπλοκ κατά τη διάρκεια της διαδικασίας εξόρυξης. Αλλάζουν επανειλημμένα το nonce και υπολογίζουν τον

κατακερματισμό των δεδομένων του μπλοκ μέχρι να βρουν έναν κατακερματισμό που πληροί τα προκαθορισμένα κριτήρια. Σκοπός του nonce είναι να τροποποιεί την είσοδο στη συνάρτηση κατακερματισμού μέχρι να επιτευχθεί η επιθυμητή έξοδος, λύνοντας ουσιαστικά το μαθηματικό πρόβλημα που χρειάζεται για την απόδειξη εργασίας. Το nonce είναι μέρος του μπλοκ στον μηχανισμό συναίνεσης Proof of Work, σε περίπτωση άλλου μηχανισμού συναίνεσης το σχέδιο αλλάζει, πχ. στο PoS υπάρχει η υπογραφή του επικυρωτή στην θέση αυτή.

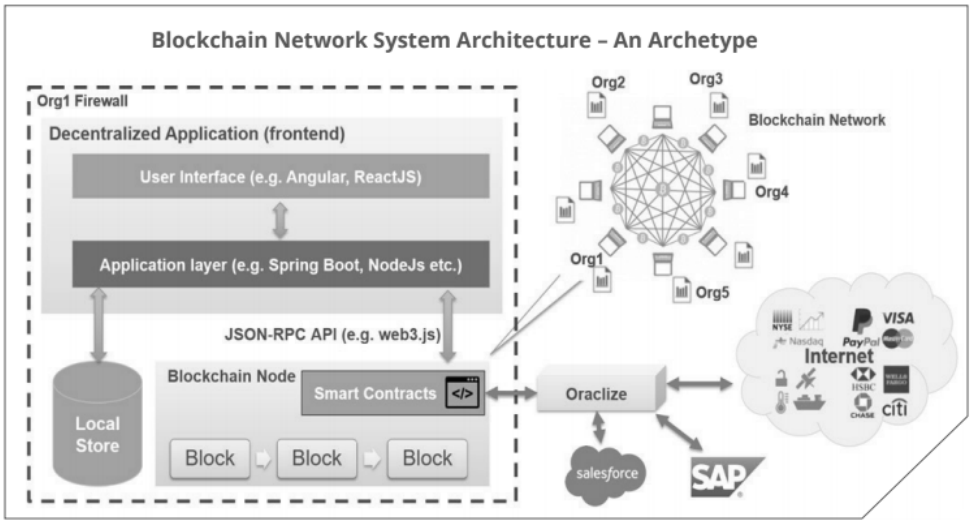
(Merkle Root): Μια ρίζα Merkle προέρχεται από ένα δέντρο Merkle, το οποίο είναι μια δομή δεδομένων που οργανώνει ένα σύνολο δεδομένων (όπως συναλλαγές) σε μια ιεραρχική δομή που μοιάζει με δέντρο. Ένα δέντρο Merkel αποθηκεύει όλες τις συναλλαγές σε ένα μπλοκ, παράγοντας ένα ψηφιακό αποτύπωμα όλων των συναλλαγών του μπλοκ. Επιτρέπει στους χρήστες να επαληθεύουν αν μια συναλλαγή μπορεί να συμπεριληφθεί σε ένα μπλοκ ή όχι. Συνοπτικά, είναι ένας κρυπτογραφικός κατακερματισμός που συνοψίζει όλες τις συναλλαγές εντός ενός μπλοκ του blockchain. Παρέχει έναν αποτελεσματικό και ασφαλή τρόπο για την επαλήθευση της ακεραιότητας και της συμπερίληψης των συναλλαγών χωρίς την ανάγκη επεξεργασίας κάθε συναλλαγής ξεχωριστά.

(Block Version): Αυτό το πεδίο αποθηκεύει τον αριθμό έκδοσης του μπλοκ για την εμφάνιση αναβαθμίσεων λογισμικού.

(nBits): Η δυσκολία εξόρυξης κατά τη στιγμή της δημιουργίας του μπλοκ.

Τέλος, υπάρχει και το σώμα του μπλοκ (Block Body), στο οποίο αποθηκεύονται οι συναλλαγές μαζί με τον κατακερματισμό τους, καθώς και ένας μετρητής για τις συναλλαγές που περιέχονται στο μπλοκ.

2.6 Αρχιτεκτονική Blockchain



Εικόνα 3. Αρχιτεκτονική Blockchain

2.6.1 Αρχιτεκτονικά Στοιχεία

Η αρχιτεκτονική blockchain είναι ένα είδος τεχνολογικής ορχήστρας (technological orchestra), όπως βλέπουμε και στην Εικόνα 3. [101]. Έχει πολλά στοιχεία/συστατικά που πρέπει να συνεργάζονται αρμονικά. Τα ακόλουθα είναι τα πιο βασικά συστατικά σε αυτή την αρχιτεκτονική [17]:

- *Κόμβοι*: Ένας κόμβος θεωρείται πως είναι ένα μηχάνημα στο δίκτυο P2P του blockchain. Είναι συνδεδεμένος στο διαδίκτυο και έχει εγκαταστήσει το βασικό λογισμικό του blockchain (σημ.: το λογισμικό αλλάζει ανάλογα με το είδος του blockchain), επιτρέποντάς του να συνεργάζεται με άλλους κόμβους στο δίκτυο του blockchain. Οι (βασικές) λειτουργίες των κόμβων (που επιτρέπονται από το προαναφερόμενο λογισμικό) περιλαμβάνουν την ενημέρωση του κοινού ψηφιακού λογιστικού βιβλίου, την αποθήκευση του αρχείου αυτού και τη διαβίβαση δεδομένων σε άλλους κόμβους του δικτύου. Ένα μπλοκ εκπέμπεται σε όλους τους κόμβους του δικτύου όταν ένας ανθρακωρύχος επιδιώκει να προσθέσει ένα νέο μπλοκ με συναλλαγές στην αλυσίδα μπλοκ.

  Υπάρχουν διάφορα είδη κόμβων, τα πιο σημαντικά από τα οποία είναι [100]:

  1. Πλήρεις κόμβοι (full nodes): Αυτοί οι κόμβοι αποθηκεύουν ένα πλήρες αντίγραφο ολόκληρου του blockchain και επικυρώνουν όλες τις συναλλαγές και τα μπλοκ. Συμμετέχουν στον μηχανισμό συναίνεσης, διασφαλίζοντας ότι κάθε συναλλαγή ακολουθεί τους κανόνες του πρωτοκόλλου. Με λίγα λόγια είναι υπεύθυνοι για τη διατήρηση του συνόλου των αρχείων συναλλαγών σε ένα δίκτυο blockchain. Θεωρούνται ως οι διακομιστές όπου αποθηκεύονται και διατηρούνται τα δεδομένα. Εάν υπάρχουν βελτιώσεις που πρέπει να γίνουν σε ένα blockchain, η πλειοψηφία των πλήρων κόμβων πρέπει να είναι έτοιμη γι' αυτές. Έτσι, μπορεί να συναχθεί το

συμπέρασμα ότι οι πλήρεις κόμβοι έχουν δικαίωμα ψήφου προκειμένου να γίνουν οποιεσδήποτε αλλαγές σε μια αλυσίδα μπλοκ. Υπάρχουν δύο είδη πλήρων κόμβων:

(α) Μειωμένοι - Κλαδεμένοι κόμβοι (Pruned Nodes): Σε αυτούς δίνεται συγκεκριμένη χωρητικότητα μνήμης για την αποθήκευση δεδομένων. Αυτό σημαίνει ότι μπορεί να προστεθεί μπλοκ μέχρι ένα συγκεκριμένο όριο διότι δεν μπορούμε να ξεπεράσουμε τη διαθέσιμη χωρητικότητα.
Για τη διατήρηση του λογιστικού βιβλίου, οι κλαδεμένοι κόμβοι μπορούν να αποθηκεύουν μπλοκ μέχρι να φτάσουν το καθορισμένο όριο. Μόλις επιτευχθεί το όριο, ο κόμβος αρχίζει να διαγράφει τα παλαιότερα μπλοκ και να δημιουργεί χώρο για νέα, προκειμένου να διατηρηθεί το μέγεθος του blockchain. Παρ' όλα αυτά, δεν διαγράφει εντελώς τα παλιά μπλοκ, καθώς η ακολουθία και τα μετα-δεδομένα τους εξακολουθούν να καταγράφονται στο blockchain, τηρώντας τις βασικές αρχές της τεχνολογίας.

(β) Πλήρεις κόμβοι αρχειοθέτησης (Archival Full Nodes): Οι πλήρεις κόμβοι αυτού του τύπου συναντώνται συνήθως σε ένα δίκτυο blockchain. Οι πλήρεις κόμβοι αρχειοθέτησης διατηρούν την πλήρη αλυσίδα μπλοκ και διαφέρουν από τους περικομμένους πλήρεις κόμβους όσον αφορά τη χωρητικότητα μνήμης. Αυτοί οι κόμβοι είναι διαφόρων τύπων:

- Κόμβοι ανθρακωρύχων (Mining Nodes): Για την επαλήθευση των εγγραφών και την προσθήκη συναλλαγών στο blockchain χρειάζονται ορισμένοι κόμβοι για υψηλούς υπολογισμούς και την επίλυση πολύπλοκων μαθηματικών συναρτήσεων. Αυτό απαιτεί μεγάλη υπολογιστική ισχύ και καταναλώνει μεγάλη ποσότητα ενέργειας κατά τη διαδικασία. Οι κόμβοι εξόρυξης είναι ιδανικοί για τη διαδικασία εξόρυξης, που είναι ο τρόπος με τον οποίο δημιουργούνται και προστίθενται νέα μπλοκ στο blockchain και η οποία περιλαμβάνει αλγορίθμους συναίνεσης, όπως τον Proof of Work.
- Κόμβοι εξουσίας (Authority Nodes): Οι κόμβοι εξουσίας χρησιμοποιούνται για την εξουσιοδότηση άλλων κόμβων που θέλουν να ενταχθούν σε ένα δίκτυο blockchain. Μπορούν επίσης να καθορίσουν τα δικαιώματα πρόσβασης άλλων κόμβων εάν θέλουν να έχουν πρόσβαση σε ένα συγκεκριμένο κανάλι δεδομένων.
- Κύριοι κόμβοι (Masternodes): Είναι πλήρεις κόμβοι που δεν έχουν τη δυνατότητα εξόρυξης ενός νέου μπλοκ στο δίκτυο. Χρησιμοποιούνται για τη διατήρηση του λογιστικού βιβλίου και την επαλήθευση των συναλλαγών.
- Κόμβοι ανατοκισμού (Staking Nodes): Αυτοί οι κόμβοι επικυρώνουν τις συναλλαγές σε ένα δίκτυο blockchain και είναι υπεύθυνοι για τη διατήρηση του αλγορίθμου συναίνεσης. Στον μηχανισμό συναίνεσης PoS, οι κόμβοι ανατοκισμού χρησιμοποιούνται για να κλειδώσουν - επενδύσουν τα κρυπτονομίσματα τους ως εγγύηση και να επαληθεύσουν τη συναλλαγή.

2. Ελαφροί κόμβοι (Light Nodes): Οι ελαφροί κόμβοι, γνωστοί και ως κόμβοι απλοποιημένης επαλήθευσης πληρωμών, δεν αποθηκεύουν ολόκληρο το blockchain. Αντ' αυτού, κατεβάζουν και επικυρώνουν μόνο τις επικεφαλίδες των μπλοκ, βασιζόμενοι στους πλήρεις κόμβους για την επαλήθευση των συναλλαγών. Αυτοί οι κόμβοι είναι επίσης γνωστοί ως κόμβοι απλοποιημένης επαλήθευσης πληρωμών (SPV). Οι ελαφροί κόμβοι χρησιμοποιούνται συνήθως σε πορτοφόλια

κρυπτονομισμάτων για τη γρήγορη επαλήθευση συναλλαγών χωρίς την ανάγκη αποθήκευσης ολόκληρου του blockchain.

3. Οι υπερ-κόμβοι (Super Nodes): χρησιμοποιούνται για την εκτέλεση ορισμένων ειδικών εργασιών και εφαρμόζονται σε ορισμένα blockchain. Μπορούν να χρησιμοποιηθούν για τον καθορισμό ή τη διατήρηση των κανόνων ενός blockchain, την εφαρμογή μιας αλλαγής στο πρωτόκολλο κ.λπ.
4. Αστραπιαίοι Κόμβοι (Lightning Nodes): Οι κόμβοι αυτοί διευκολύνουν τις συναλλαγές, επιτρέποντας στους χρήστες να πραγματοποιούν γρήγορες και χαμηλού κόστους μεταφορές. Αντί να καταγράφουν κάθε συναλλαγή στο κύριο δίκτυο, αυτοί οι κόμβοι δημιουργούν ένα ασφαλές κανάλι πληρωμών μεταξύ δύο μερών. Αυτό το κανάλι τους επιτρέπει να πραγματοποιούν πολλαπλές συναλλαγές χωρίς να μεταδίδουν κάθε συναλλαγή στο blockchain. Ως αποτέλεσμα, το δίκτυο Lightning ανακουφίζει σημαντικά τα προβλήματα συμφόρησης και κλιμάκωσης που αντιμετωπίζουν τα συμβατικά δίκτυα blockchain.
   Οι lightning nodes δημιουργούν ένα άτομο με έναν χρήστη, προωθώντας όλες τις συναλλαγές στο κύριο blockchain. Αυτό διευκολύνει τις στιγμιαίες συναλλαγές, ενώ παράλληλα μειώνει το κόστος που συνεπάγεται η συναλλαγή, καθώς μειώνεται ο φόρτος του δικτύου.

- *Συναλλαγές*: Μια συναλλαγή αντιστοιχεί σε μια καταχώρηση στο κοινό ψηφιακό λογιστικό βιβλίο του blockchain. Θα μπορούσε να είναι μια μεταφορά ψηφιακής αξίας, όπως κρυπτονομίσματα, από μια διεύθυνση σε μια άλλη, ή μια αλλαγή κατάστασης σε ένα έξυπνο συμβόλαιο. Το δίκτυο υπολογιστών στο blockchain αποθηκεύει τα δεδομένα της συναλλαγής ως αντίγραφο στο ψηφιακό λογιστικό βιβλίο.
- *Μπλοκ*: Στον τομέα των κρυπτονομισμάτων, τα μπλοκ είναι σαν αρχεία που αποθηκεύουν τις συναλλαγές π.χ. με την μορφή ενός βιβλίου εγγραφών. Τα μπλοκ αυτά είναι κρυπτογραφημένα σε ένα δέντρο κατακερματισμού. Πρόκειται δηλαδή για ένα σύμπλεγμα ή μια παρτίδα συναλλαγών που το δίκτυο P2P επεξεργάζεται και εγκρίνει ταυτόχρονα στο κοινόχρηστο ψηφιακό λογιστικό βιβλίο. Για παράδειγμα, στο Bitcoin blockchain, όλες οι συναλλαγές που ξεκινούν μέσα σε περίπου δέκα λεπτά εγκρίνονται και καταγράφονται ως νέο μπλοκ.
- *Αλυσίδα*: Πρόκειται για μια αλυσίδα από μπλοκ που συνδέονται από το πρώτο μπλοκ (το μπλοκ γένεσης) μέχρι το τρέχον μπλοκ. Κάθε μπλοκ συνδέεται με το προηγούμενο μέσω κατακερματισμού και μοναδικών μετα-δεδομένων (metadata), δημιουργώντας μια ασφαλή δομή αλυσίδας. Από τη σύνδεση των μπλοκ για τη δημιουργία μιας αλυσίδας προέρχεται το όνομα blockchain.
- *Miners*: Η λέξη "ανθρακωρύχος" αναφέρεται στο πρόσωπο που αποκτά, εγκαθιστά και λειτουργεί έναν κόμβο εξόρυξης (mining node) για να κερδίσει την ανταμοιβή που εκδίδει το πρωτόκολλο.
- *Πρωτόκολλο συναίνεσης*: Πρόκειται για ένα σύνολο κανόνων που καθοδηγούν τους υπολογιστές στο δίκτυο P2P για να αλληλεπιδρούν και, το σημαντικότερο, να διαμορφώνουν συναίνεση σχετικά με τον τρόπο επεξεργασίας και αποθήκευσης των συναλλαγών σε ένα κοινόχρηστο ψηφιακό αρχείο ή τον τρόπο εκτέλεσης των έξυπνων συμβάσεων. Το πρωτόκολλο διεξάγεται και υλοποιείται στο βασικό λογισμικό που πρέπει να εγκαταστήσει και να εκτελέσει κάθε υπολογιστής στο δίκτυο.
- *Έξυπνα συμβόλαια:* Τα έξυπνα συμβόλαια, είναι αυτό-εκτελούμενα προγράμματα υπολογιστή αποθηκευμένα στο blockchain, και εισήχθησαν στην γενιά 2.0 του blockchain. (Δείτε Ενότητα 2.3 και Ενότητα 2.8 για περισσότερες λεπτομέρειες).

- *dApps:* Τα DApps (αποκεντρωμένες εφαρμογές), είναι ένας τύπος εφαρμογής λογισμικού που εκτελείται σε μια τεχνολογία blockchain και εισήχθη στην γενιά 3.0 του blockchain.(Δείτε Ενότητα 2.3 για περισσότερες λεπτομέρειες).

2.6.2 Τύποι Αρχιτεκτονικών Blockchain

Υπάρχουν έξι κύριοι τύποι αρχιτεκτονικών blockchain, οι οποίοι θα αναλυθούν στην συνέχεια.

Δημόσια ή Χωρίς Άδεια (Public or Permissionless) Blockchain

Στη δημόσια αρχιτεκτονική blockchain, οποιοσδήποτε μπορεί να δημιουργήσει έναν κόμβο και να γίνει μέλος του δικτύου P2P καθώς και να συμμετάσχει στις βασικές δραστηριότητες του, χωρίς να ζητήσει άδεια από κανέναν. Έτσι τα δεδομένα και η πρόσβαση στο σύστημα είναι διαθέσιμα σε οποιονδήποτε είναι πρόθυμος να συμμετάσχει.
Οποιοσδήποτε μπορεί να διαβάσει, να αποθηκεύσει και να ελέγξει τις τρέχουσες δραστηριότητες σε ένα δημόσιο δίκτυο blockchain, γεγονός που βοηθά στην επίτευξη του αυτό-καθοριζόμενου, αποκεντρωμένου χαρακτήρα που συνήθως αποδίδεται στο blockchain όταν αυτό συζητείται.

Επίσης, όσοι συμμετέχουν στο δίκτυο συχνά παραμένουν με ψευδώνυμα. Παρ' όλα αυτά, η δημόσια αρχιτεκτονική blockchain παρέχει κίνητρα στα ενδιαφερόμενα μέρη (stakeholders) να ενεργούν με ειλικρίνεια μέσω των ανταμοιβών, όπως είναι αυτές της εξόρυξης (mining) ή ανατοκισμού (staking). [17] Για ανταμοιβές ανατοκισμού θα μιλήσουμε στην Ενότητα 2.7, όπου θα αναλυθεί ο μηχανισμός συναίνεσης Proof of Stake (PoS).

Στα πλεονεκτήματα της δημόσιας αρχιτεκτονικής blockchain είναι ότι το δημόσιο δίκτυο λειτουργεί με ένα σύστημα κινήτρων που παρακινεί νέους χρήστες να εγγραφούν και διατηρεί την ευελιξία του δικτύου. Επίσης, πολύ ελκυστική στους χρήστες φαίνεται να είναι η αποκεντρωμένη και εκδημοκρατισμένη λειτουργία της αρχιτεκτονικής αυτής, εφόσον δεν υπάρχει κάποιος οργανισμός ή φορέας που να την ελέγχει. Αυτό κάνει τους χρήστες να νιώθουν μεγαλύτερη ασφάλεια.

Το μειονέκτημα είναι ότι μπορεί αυτή η μορφή του blockchain να είναι άκαμπτη αφού έχει ένα σταθερό μηχανισμό συναίνεσης και μπορεί να καταστεί δύσκολη η προσαρμογή στις εξελισσόμενες τεχνολογικές ανάγκες ή τη βελτιστοποίηση της κατανάλωσης ενέργειας, ενώ οι αναβαθμίσεις συχνά αντιμετωπίζουν αμφιλεγόμενες διαδικασίες διακυβέρνησης. Ακόμη, πολλές φορές χρειάζεται αρκετή ενέργεια για να διατηρηθεί σε λειτουργία. Το πρόβλημα προκαλείται επειδή οι χρήστες αναγκάζονται να ανταγωνίζονται για ανταμοιβές ώστε να παραχωρούν στο δίκτυο πρόσβαση στην υπολογιστική τους ισχύ. [16]

Παραδείγματα δημοσίων blockchain είναι τα blockchain Bitcoin[1], Ethereum[2], Dogecoin[3], & Litecoin[4].

[1] https://bitcoin.org/el/

[2] https://ethereum.org/en/

[3] https://dogecoin.com/

Ιδιωτικά (Private) Blockchain

Σε αυτή την περίπτωση, ένα άτομο, μια επιχείρηση ή ένα ίδρυμα ελέγχει όλους τους κόμβους στο δίκτυο P2P. Σε ένα τέτοιο περιβάλλον, μόνο ο ιδιοκτήτης του blockchain μπορεί να επιτρέψει σε άλλο πρόσωπο ή οντότητα να ενταχθεί στο δίκτυο, οπότε η συμμετοχή σε αυτό είναι περιορισμένη. Προφανώς, μόνο οι οντότητες που συμμετέχουν στο blockchain θα έχουν γνώσεις για τις συναλλαγές που συμβαίνουν σε αυτό.

Το πλεονέκτημα ενός ιδιωτικού blockchain είναι ότι ο ιδιοκτήτης μπορεί να το προσαρμόσει στον βαθμό που επιθυμεί. Επίσης, οι αναβαθμίσεις είναι εύκολο να εφαρμοστούν, καθώς υπάρχουν λίγα ενδιαφερόμενα μέρη που πρέπει να πειστούν για αυτές, ιδιαίτερα εφόσον αυτές δεν επιβάλλονται από τον φορέα. Θετικό είναι επίσης ότι οι χρήστες εντάσσονται στο δίκτυο χρησιμοποιώντας προσκλήσεις και έτσι όλοι επαληθεύονται.

Οι συναλλαγές σε ιδιωτικά blockchain μπορούν συχνά να είναι ταχύτερες σε σύγκριση με τα δημόσια, αλλά η ταχύτητα εξακολουθεί να εξαρτάται από διάφορους παράγοντες, όπως ο μηχανισμός συναίνεσης και το μέγεθος και η καθυστέρηση του δικτύου. Τα ιδιωτικά blockchain συνήθως σχεδιάζονται με γνώμονα συγκεκριμένες περιπτώσεις χρήσης (ότι χρειάζεται ο οργανισμός στην εκάστοτε περίπτωση) και μπορούν να βελτιστοποιηθούν για απόδοση και ταχύτητα μέσα σε ένα ελεγχόμενο περιβάλλον.

Από την άλλη πλευρά, στα ιδιωτικά blockchain είναι πιο πιθανό να υπάρχει λογοκρισία από τον φορέα, καθώς η πρόσβαση, ο έλεγχος και το είδος των συναλλαγών είναι περιορισμένα σε ένα επιλεγμένο από τον φορέα γκρουπ συμμετεχόντων. Επιπλέον, πρέπει να είναι έμπιστη η επιχείρηση που ελέγχει το blockchain για να συμμετάσχει κάποιος σε αυτήν. Ιδιαίτερα διότι υπάρχει κίνδυνος ακούσιας αλλαγής των συναλλαγών ή της αλυσίδας του blockchain προς όφελος του ιδιοκτήτη/φορέα. Επίσης, δεν είναι αμετάβλητα καθώς ο ιδιοκτήτης μπορεί εύκολα να αλλάξει τους κανόνες.

Παραδείγματα ιδιωτικών blockchain είναι τα Energy Web Chain[5], Everledger[6], CargoX[7].

[4] https://litecoin.org/

[5] https://www.energyweb.org/

[6] https://everledger.io/

[7] https://cargox.io/

Blockchain Κοινοπραξίας ή Με Άδεια (Consortium or Permissioned Blockchain)

Μια αρχιτεκτονική blockchain κοινοπραξίας αποτελεί μια συνεργασία πολλών οργανισμών. Κάθε ένας από αυτούς μπορεί να έχει έναν κόμβο στο δίκτυο, να συμμετέχει στη λήψη αποφάσεων και να κατέχει μετοχές στην κοινοπραξία (δηλ. στο blockchain). Στην ουσία, τα blockchain κοινοπραξίας μοιάζουν με τα ιδιωτικά blockchain αλλά αντί να υπάρχει ένας οργανισμός/εταιρεία που να ελέγχει το blockchain και να αποφασίζει για το ποιός θα ενσωματωθεί σε αυτό και ποιος οχι, πολλοί οργανισμοί/εταιρείες κατέχουν ποσοστά και ελέγχουν το blockchain από κοινού.

Τα blockchain κοινοπραξίας βρίσκονται μεταξύ των δημόσιων και των ιδιωτικών blockchain. Σχεδιάζονται από οργανισμούς και κανένα άτομο εκτός των οργανισμών δεν μπορεί να αποκτήσει πρόσβαση σε αυτά. Στα blockchain κοινοπραξίας υπάρχει ισότιμη συνεργασία μεταξύ όλων των οργανισμών που συμμετέχουν σε αυτό.

Τα ενδιαφερόμενα μέρη σε αρχιτεκτονικές blockchain κοινοπραξιών πρέπει συχνά να ταυτοποιούνται. Επίσης, όσοι θέλουν να ενταχθούν στο δίκτυο και την κοινοπραξία πρέπει να πληρούν καθορισμένες απαιτήσεις. Αυτό μπορεί να περιλαμβάνει την καταβολή ενός χρηματικού ποσού. [17]

Πλεονεκτήματα που έχει αυτή η αρχιτεκτονική είναι ότι οι πάροχοι αυτών των blockchain θα προσπαθούν πάντα να δίνουν την ταχύτερη απόδοση σε σύγκριση με τα δημόσια blockchain, καθώς υπάρχουν λιγότεροι κόμβοι και είναι πιο εύκολο για το δίκτυο να λειτουργεί πιο γρήγορα. Προφανώς παίζουν ρόλο και άλλοι παράγοντες, όπως ο μηχανισμός συναίνεσης. Ο καθένας που ανήκει στους οργανισμούς του blockchain μπορεί να συνδεθεί στο δίκτυο με μια κατάλληλη διαδικασία επαλήθευσης.

Οι συμμετέχοντες σε ένα blockchain κοινοπραξίας έχουν συνήθως καθιερωμένες σχέσεις και κοινά συμφέροντα για την επιτυχία του δικτύου. Αυτή η αμοιβαία εμπιστοσύνη συμβάλλει στη συνολική ασφάλεια των συναλλαγών, καθώς οι συμμετέχοντες είναι πιο πιθανό να ενεργούν υπεύθυνα και να τηρούν τους συμφωνημένους κανόνες. Επίσης, με τον περιορισμένο αριθμό γνωστών συμμετεχόντων, ο έλεγχος των συναλλαγών και η επίλυση των προβλημάτων είναι συχνά πιο αποτελεσματικός. Επιπλέον, τα μέλη μιας κοινοπραξίας blockchain μοιράζονται συνήθως τις ευθύνες και τα έξοδα που σχετίζονται με τη δημιουργία, τη λειτουργία και τη συντήρηση του δικτύου. Τέλος, οι συμμετέχοντες οργανισμοί ελέγχουν συλλογικά το δίκτυο, καθιστώντας πιο δύσκολο για οποιαδήποτε μεμονωμένη οντότητα να αποκτήσει τον έλεγχο της πλειοψηφίας.

Στα μειονεκτήματα, η διαχείριση της διαδικασίας διακυβέρνησης και λήψης αποφάσεων στο πλαίσιο μιας κοινοπραξίας μπορεί να είναι πολύπλοκη. Διαφορετικοί συμμετέχοντες μπορεί να έχουν διαφορετικά συμφέροντα και προτεραιότητες, με αποτέλεσμα την πρόκληση της επίτευξης συναίνεσης σχετικά με την αναβάθμιση του δικτύου, τις αλλαγές κανόνων και άλλες αποφάσεις.

Οι Hyperledger Fabric[8], R3 Corda[9] και B3i[10] είναι παραδείγματα κοινοπρακτικών αλυσίδων μπλοκ.

[8] https://www.hyperledger.org/projects/fabric

[9] https://corda.net/

[10] https://home.treasury.gov/system/files/311/May2018FACI_B3i.pdf

Υβριδικό (Hybrid) Blockchain

Ένα υβριδικό blockchain μπορεί να οριστεί ως ένα ειδικό είδος τεχνολογίας blockchain που συνδυάζει στοιχεία τόσο ιδιωτικών όσο και δημόσιων blockchain, ή ακόμα και αυτά των blockchain κοινοπραξίας, και στοχεύει στη χρήση των καλύτερων χαρακτηριστικών από όλους αυτούς τους τύπους blockchain. [18]

Τα δημόσια τμήματα ενός υβριδικού blockchain μπορούν να είναι προσβάσιμα από οποιονδήποτε, επιτρέποντας τη διαφάνεια και την αποκεντρωμένη συμμετοχή, ενώ τα ιδιωτικά τμήματα περιορίζονται σε εξουσιοδοτημένους συμμετέχοντες, προσφέροντας ενισχυμένη ιδιωτικότητα και έλεγχο.

Τα υβριδικά blockchain έχουν την ευελιξία ως πλεονέκτημα διότι επιτρέπουν στους οργανισμούς (που συμμετέχουν σε αυτό) να σχεδιάσουν μια λύση blockchain που ταιριάζει καλύτερα στις ανάγκες τους. Μπορούν να αξιοποιήσουν τη διαφάνεια και την αποκέντρωση των δημόσιων blockchain, διατηρώντας παράλληλα την ιδιωτικότητα και τον έλεγχο με ιδιωτικά blockchain για άλλες. Επίσης, μπορούν να επιτύχουν καλύτερη επεκτασιμότητα, κατανέμοντας λειτουργίες ή τύπους δεδομένων μεταξύ δημόσιων και ιδιωτικών blockchain. Οι συναλλαγές με μη ευαίσθητα δεδομένα μπορούν να υποβάλλονται σε επεξεργασία σε δημόσια blockchain, ενώ οι συναλλαγές που σχετίζονται με ευαίσθητα δεδομένα μπορούν να διαχειρίζονται σε ιδιωτικά. Έτσι έχουν και αποδοτικότητα κόστους καθώς εστιάζονται περισσότεροι πόροι στα ιδιωτικά τμήματα όπου ο έλεγχος και η ασφάλεια είναι υψίστης σημασίας και χρησιμοποιούν δημόσια blockchain για μη ευαίσθητες πληροφορίες.

Στα αρνητικά, η διαχείριση και η συντήρηση τόσο των δημόσιων όσο και των ιδιωτικών τμημάτων μπορεί να είναι πολύπλοκη και να απαιτεί εξειδικευμένη τεχνογνωσία ενώ η ενσωμάτωση διαφορετικών μηχανισμών συναίνεσης μεταξύ δημόσιων και ιδιωτικών τμημάτων μπορεί να είναι δύσκολη.

Παραδείγματα πλατφορμών με υβριδικές αρχιτεκτονικές blockchain περιλαμβάνουν το Polkadot[11] και το Kusama[12].

[11] https://www.polkadot.network/

[12] https://kusama.network/

2.7 Μηχανισμοί Συναίνεσης

Proof of Work (PoW)

Τα blockchain υιοθετούν διάφορες συναρτήσεις κατακερματισμού για την απόδειξη εργασίας τους στα πλαίσια των μηχανισμών συναίνεσης που μπορούν να χρησιμοποιηθούν. Ο μηχανισμός Proof of Work επιβραβεύει όποιον ανακαλύπτει πρώτος έναν έγκυρο nonce μεταξύ των ανθρακωρύχων κατά την εξόρυξη ενός νέου μπλοκ. Επίσης, είναι ένας τρόπος για την επίτευξη συναίνεσης χρησιμοποιώντας υψηλή υπολογιστική ισχύ.

Ο PoW είναι από τους πρώτους μηχανισμούς συναίνεσης και ο πιο δημοφιλής, ενώ χρησιμοποιείται από τα δίκτυα Bitcoin και Litecoin. Χρησιμοποιούνταν αρχικά και από το Ethereum (πριν το τελευταίο πάει στην νέα του έκδοση όπου χρησιμοποιεί το PoS). Στον μηχανισμό αυτό, οι ανθρακωρύχοι (ή block adders) πρέπει να κάνουν μαθηματικούς υπολογισμούς για να βρουν ένα σωστό κατακερματισμό για την επικεφαλίδα του μπλοκ που θα προσθέσουν, αλλάζοντας συνεχώς το nonce του μπλοκ (αυτή η διαδικασία ονομάζεται εξόρυξη). Το nonce είναι μια τιμή που τροποποιεί την είσοδο στη συνάρτηση κατακερματισμού μέχρι να επιτευχθεί η επιθυμητή έξοδος, λύνοντας ουσιαστικά το μαθηματικό πρόβλημα που χρειάζεται για την απόδειξη εργασίας.

Ο ανθρακωρύχος που βρίσκει πρώτος τον κατακερματισμό σύμφωνα με το επίπεδο δυσκολίας (κατακερματισμού) που έχει τεθεί, αδράζει την ευκαιρία να προσθέσει το μπλοκ του στο δίκτυο. Ως εκ τούτου, παίρνει την αντίστοιχη ανταμοιβή. Η δυσκολία εύρεσης κατάλληλου κατακερματισμού ελέγχεται από το πρωτόκολλο του δικτύου blockchain. Όσο υψηλότερη είναι η δυσκολία, τόσο περισσότεροι υπολογισμοί απαιτούνται για την εύρεση ενός έγκυρου nonce και, επομένως, τόσο περισσότερη υπολογιστική εργασία άρα και ισχύ απαιτείται για την εξόρυξη ενός μπλοκ. Ο ανθρακωρύχος εκτός από την ανταμοιβή του μπλοκ (η οποία εξαρτάται από την δυσκολία της εύρεσης του nonce), θα πάρει και τα τέλη εκείνων των συναλλαγών που θα εισαχθούν στο μπλοκ του.

Μόλις ο ανθρακωρύχος εξορύξει ένα νέο μπλοκ, το συναρμολογεί χρησιμοποιώντας συναλλαγές από μια πισίνα συναλλαγών (transaction pool), η οποία περιέχει συναλλαγές που έχουν υποβληθεί από χρήστες και περιμένουν να προστεθούν στο επόμενο μπλοκ. Ο ανθρακωρύχος θα επιλέγει συναλλαγές με βάση τα τέλη των συναλλαγών (συνήθως επιλέγει τα πιο υψηλά τέλη, καθώς αυτός θα επωφεληθεί από αυτά) αλλά και την χωρητικότητα του μπλοκ.

Στην συνέχεια, πριν προσθέσει το μπλοκ, ο ανθρακωρύχος θα επαληθεύσει την εγκυρότητα των συναλλαγών (κοιτώντας αν είναι έγκυρες οι υπογραφές, αν υπάρχουν αρκετά κεφάλαια, και αν η συναλλαγή ακολουθεί τους κανόνες του πρωτοκόλλου).

Αφού ο ανθρακωρύχος μεταδώσει το μπλοκ στους υπόλοιπους κόμβους του δικτύου (άλλοι ανθρακωρύχοι και απλοί συμμετέχοντες), αυτοί μπορούν να αποδεχτούν την εγκυρότητά του μπλοκ ή να την αμφισβητήσουν σύμφωνα με τον μηχανισμό συναίνεσης. Ειδικότερα, οι κόμβοι μπορούν εύκολα να επαληθεύσουν ότι ο ανθρακωρύχος έχει εκτελέσει την απαιτούμενη υπολογιστική εργασία, κατακερματίζοντας την επικεφαλίδα του μπλοκ με το δεδομένο nonce για να επιβεβαιώσουν ότι ο κατακερματισμός πληροί τα καθορισμένα κριτήρια. Μόλις το μπλοκ προστεθεί στο blockchain, οι συναλλαγές που περιέχει ολοκληρώνονται.

Πλεονεκτήματα:

Δομή κινήτρων: Το PoW παρέχει στους ανθρακωρύχους οικονομικά κίνητρα για να συμμετέχουν με ειλικρίνεια στο δίκτυο, καθώς ανταμείβονται με κρυπτονόμισμα για τις προσπάθειές τους. Αυτή η δομή κινήτρων ευθυγραμμίζει τα συμφέροντα των συμμετεχόντων με την ασφάλεια και την ακεραιότητα του blockchain.

Δικαιοσύνη: Το PoW επιτρέπει μια δίκαιη και ανταγωνιστική διαδικασία επικύρωσης μπλοκ. Οι ανθρακωρύχοι ανταγωνίζονται για την επίλυση κρυπτογραφικών γρίφων και ο πρώτος που θα βρει μια έγκυρη λύση θα δημιουργήσει ένα νέο μπλοκ. Αυτός ο δίκαιος ανταγωνισμός συμβάλλει στην ασφάλεια και την ακεραιότητα του δικτύου.

Μειονεκτήματα:

Εντατική ενέργεια: Το PoW απαιτεί σημαντική υπολογιστική ισχύ, καθιστώντας το ενεργοβόρο και μη φιλικό προς το περιβάλλον.

Κόστος υλικού: Το υλικό εξόρυξης μπορεί να είναι ακριβό, καθιστώντας δύσκολη τη συμμετοχή μεμονωμένων ατόμων.

Proof of Stake (PoS)

Το Proof of Stake είναι ένας αλγόριθμος συναίνεσης που λειτουργεί με έναν μηχανισμό ανατοκισμού (staking), όπου οι επικυρωτές (ονομάζονται έτσι διότι δεν εξορύσσουν όπως οι ανθρακωρύχοι στο PoW αλλά απλώς επικυρώνουν νέα μπλοκ) κλειδώνουν για κάποιο χρονικό διάστημα συγκεκριμένο ποσό περιουσιακών τους στοιχείων (δηλ. το stake) τόσο για να προστατεύσουν το blockchain όσο και για να επιλεγούν για την προσθήκη ενός μπλοκ. Μάλιστα σε κάποια blockchain ο ανατοκισμός σημαίνει δέσμευση περιουσιακών στοιχείων για να λάβει κανείς ανταμοιβές με την πάροδο του χρόνου. Έτσι, οι επικυρωτές επιλέγονται για να δημιουργήσουν νέα μπλοκ και να επικυρώσουν συναλλαγές με βάση το ποσό του κρυπτονομίσματος που κλειδώνουν και κατέχουν ως εγγύηση (stake). Η τοποθέτηση περιλαμβάνει τη δέσμευση ενός συγκεκριμένου ποσού κρυπτονομίσματος σε ένα πορτοφόλι ως μια μορφή κατάθεσης ασφαλείας, η οποία αποδεικνύει τη δέσμευση του επικυρωτή να διατηρήσει την ακεραιότητα του δικτύου. Όσο μεγαλύτερο είναι το ποντάρισμα που κατέχει ένας επικυρωτής, τόσο μεγαλύτερες είναι οι πιθανότητες να επιλεγεί για τη δημιουργία του επόμενου μπλοκ και να κερδίσει ανταμοιβές. Οι επικυρωτές έχουν κίνητρο να ενεργούν με ειλικρίνεια επειδή έχουν κάτι να χάσουν (τα κρυπτονομίσματα που έχουν κλειδώσει) αν συμπεριφερθούν κακόβουλα.

Πολλά δίκτυα PoS (πχ. Tezos) εφαρμόζουν μηχανισμούς για την προσαρμογή της πιθανότητας επιλογής των επικυρωτών με βάση τη συμπεριφορά τους. Για παράδειγμα, ένας επικυρωτής που συμπεριφέρεται συστηματικά ανέντιμα μπορεί να δει την πιθανότητα επιλογής του να μειώνεται με την πάροδο του χρόνου, ενώ επικυρωτές με ισχυρό ιστορικό ειλικρινούς συμμετοχής μπορεί να δουν την πιθανότητα τους να αυξάνεται. Η συναίνεση PoS εξαλείφει την υψηλή κατανάλωση ενέργειας από το PoW - αναπτύχθηκε ως μια καλύτερη επιλογή για το PoW. Μπορεί να εφαρμοστεί μόνο αφού ένα δίκτυο αποκτήσει έναν καλό αριθμό συμμετεχόντων (ή κόμβων).

Πλεονεκτήματα:

Ενεργειακή απόδοση: Το PoS είναι σημαντικά πιο ενεργειακά αποδοτικό σε σύγκριση με το Proof of Work (PoW), καθώς δεν απαιτεί από τους ανθρακωρύχους να εκτελούν ενεργοβόρους υπολογισμούς.

Ασφάλεια: Το PoS έχει σχεδιαστεί για να είναι ασφαλές, καθώς οι επικυρωτές έχουν οικονομικό συμφέρον να διατηρήσουν την ακεραιότητα του δικτύου. Μπορούν να χάσουν τις μάρκες/κρυπτονομίσματα που έχουν ποντάρει αν ενεργήσουν κακόβουλα.

Μειονεκτήματα:

Συγκέντρωση πλούτου: Οι κάτοχοι περισσότερων tokens (μαρκών) έχουν μεγαλύτερη επιρροή στο δίκτυο.

"Nothing-at-stake": Το πρόβλημα του "τίποτα δεν διακυβεύεται" εμφανίζεται όταν οι επικυρωτές δεν έχουν κόστος που συνδέεται με την επικύρωση πολλαπλών αντικρουόμενων μπλοκ, προκαλώντας ενδεχομένως ή βοηθώντας σε διακλαδώσεις.

Delegated Proof of Stake (DPoS)

Το DPoS βελτιώνει τον μηχανισμό PoS με την εισαγωγή ψηφοφορίας από τους συμμετέχοντες στο δίκτυο, οι οποίοι, χρησιμοποιώντας τα νομίσματά τους, εκλέγουν τους έμπιστους αντιπροσώπους (delegates) τους. Στη συνέχεια, με βάση μια τυχαία επιλογή, ένας από τους ψηφίσαντες αντιπροσώπους έχει την ευκαιρία να προσθέσει το μπλοκ του στην αλυσίδα. Οι αντιπρόσωποι, επίσης, εκτελούν τη λήψη αποφάσεων, όπως την επαλήθευση συναλλαγών ή αναβαθμίσεις του δικτύου και αλλαγές στο πρωτόκολλο για λογαριασμό των υπολοίπων. Οι αντιπρόσωποι επιλέγονται συνήθως για μια συγκεκριμένη περίοδο, η οποία μπορεί να διαφέρει από blockchain σε blockchain. Μετά την καθορισμένη περίοδο, πραγματοποιείται νέος γύρος ψηφοφορίας, επιτρέποντας στους κατόχους κρυπτονομισμάτων του δικτύου να αντικαταστήσουν ενδεχομένως τους υπάρχοντες αντιπροσώπους με νέους. Αυτή η εναλλαγή των αντιπροσώπων συμβάλει στη διασφάλιση της αποκέντρωσης και αποτρέπει τη συγκέντρωση της εξουσίας μεταξύ μιας μικρής ομάδας αντιπροσώπων. Επίσης, εάν ένας αντιπρόσωπος συμπεριφέρεται κακόβουλα ή δεν εκπληρώνει σωστά τα καθήκοντά του, οι κάτοχοι κρυπτονομισμάτων του δικτύου μπορούν να ψηφίσουν για την αντικατάστασή του. Το DPoS έχει δημοκρατική προοπτική και σχεδιασμό.

Πλεονεκτήματα:

Ταχύτητα: Το DPoS είναι γνωστό για την ικανότητά του να επεξεργάζεται γρήγορα τις συναλλαγές και να διαχειρίζεται μεγάλο όγκο συναλλαγών. Οι εξουσιοδοτημένοι επικυρωτές μπορούν να επιβεβαιώνουν αποτελεσματικά τις συναλλαγές, οδηγώντας σε χαμηλούς χρόνους επιβεβαίωσης.

Δημοκρατικότητα: Οι κάτοχοι token μπορούν να ψηφίζουν για αντιπροσώπους και να προτείνουν αναβαθμίσεις του δικτύου. Αυτό επιτρέπει την πιο δημοκρατική λήψη αποφάσεων και την προσαρμοστικότητα.

Μειονεκτήματα:

Απάθεια ψήφου: Πολλοί κάτοχοι token ενδέχεται να μην συμμετέχουν στη διαδικασία ψηφοφορίας, οδηγώντας σε έλλειψη αποκέντρωσης.

Πιθανή συμπαιγνία: Οι αντιπρόσωποι μπορεί να συνεννοηθούν ή να συμμετάσχουν σε εξαγορά ψήφων, υπονομεύοντας την ακεραιότητα του συστήματος.

Proof of Importance (PoI)

Το PoI χρησιμοποιεί βαθμολογίες σημαντικότητας για να επιλέξει ένα λογαριασμό ενός χρήστη από όλους τους συμμετέχοντες με στόχο αυτός να δημιουργήσει και να επικυρώσει καινούργια μπλοκ. Στοχεύει στην εξάλειψη των ευνοϊκών συμπεριφορών προς τους πλούσιους ενδιαφερόμενους στη συναίνεση PoS, όπου όποιος έχει κλειδώσει περισσότερα κρυπτονομίσματα έχει περισσότερες πιθανότητες να δημιουργήσει ένα μπλοκ.

Η βαθμολογία σημαντικότητας εξαρτάται από την ποιότητα των συναλλαγών και τη φήμη ενός κόμβου-χρήστη στο δίκτυο. Συγκεκριμένα, ο μηχανισμός βαθμολογεί έναν κόμβο με βάση 3 μεταβλητές: (α) πόσα χρήματα υπάρχουν σε έναν λογαριασμό, (β) πόσο συχνά ο λογαριασμός πραγματοποιεί συναλλαγές με άλλους εντός του πρωτοκόλλου και (γ) ποιος είναι ο όγκος κάθε συναλλαγής αλλά και τι σχέσεις έχει ο λογαριασμός με άλλους στο δίκτυο. Όσο πιο μεγάλο είναι το "σκορ" του χρήστη σε κάθε μια μεταβλητή, τόσο μεγαλύτερες είναι οι πιθανότητες του να είναι αυτός που θα επιλεχθεί. Το PoI χρησιμοποιεί τη θεωρία δικτύου (network theory) για να αποδώσει μια βαθμολογία για τη σημασία κάθε κόμβου στο δίκτυο. Επίσης, οι κόμβοι πρέπει να κατοχυρώσουν έναν αριθμό νομισμάτων προτού να είναι επιλέξιμοι για την εξόρυξη μπλοκ ανάλογα με τη βαθμολογία που υποδηλώνει τη συμβολή τους στο δίκτυο.

Πλεονέκτημα είναι ότι ο μηχανισμός PoI ενθαρρύνει τους συμμετέχοντες στο δίκτυο να κατέχουν περιουσιακά στοιχεία και να πραγματοποιούν συναλλαγές με αυτά. Επίσης στο PoI η βαθμολογία σημαντικότητας κάθε κόμβου βασίζεται στη δραστηριότητα του δικτύου και είναι δυναμική. Έτσι, αυτό αποθαρρύνει τις διακλαδώσεις του blockchain, καθώς ο νέος χρήστης πρέπει να δαπανήσει πόρους και στα δύο διακλαδωμένα δίκτυα για να παραμείνει ενεργός ώστε να διατηρήσει τη βαθμολογία του.

Πλεονεκτήματα:

Δίκαιη διανομή: Το PoI μπορεί να συμβάλει σε μια πιο δίκαιη κατανομή των κρυπτονομισμάτων, επειδή ανταμείβει τους χρήστες με βάση τη δραστηριότητα και τη συμμετοχή τους και όχι με βάση την υπολογιστική ισχύ ή την ιδιοκτησία υλικού.

Ασφάλεια μέσω της φήμης: Το PoI ενσωματώνει ένα σύστημα φήμης, όπου λαμβάνονται υπόψη η αξιοπιστία και το ιστορικό των συμμετεχόντων. Αυτό ενισχύει την ασφάλεια του δικτύου αποθαρρύνοντας την κακόβουλη συμπεριφορά.

Μειονεκτήματα:

Πολυπλοκότητα: Ο υπολογισμός της βαθμολογίας σημαντικότητας μπορεί να είναι πολύπλοκος και μπορεί να περιλαμβάνει υποκειμενικά στοιχεία, όπως η αξιολόγηση της συμπεριφοράς των χρηστών.

Proof of Capacity (PoC)

Το PoC αλλιώς γνωστό και ως PoSpace χρησιμοποιεί τη χωρητικότητα του δίσκου ή της αποθήκευσης ενός ανθρακωρύχου για την εξόρυξη ενός μπλοκ σε ένα αποκεντρωμένο δίκτυο. Ανταλλάσσει τον συντελεστή υπολογισμού με το χώρο στο δίσκο. Οι ανθρακωρύχοι πρέπει να αποδείξουν ότι διαθέτουν την αποθηκευτική ικανότητα για την εξόρυξη. Στο PoC οι ανθρακωρύχοι συλλέγουν έναν κατάλογο με όλους τους πιθανούς nonce για κατακερματισμό μπλοκ πριν από την πραγματική εξόρυξη. Κατά τη στιγμή αυτή, ο ανθρακωρύχος απλώς ανεβάζει τα υπολογισμένα αρχεία των πιθανών κατακερματισμών στο δίκτυο. Ένας ανθρακωρύχος μπορεί να αποθηκεύσει μόνο τόσα nonces για όσα έχει χώρο. Η διαδικασία αυτή του "προ-υπολογισμού" ονομάζεται "plot". Μόλις δημιουργηθεί το plot, οι ανθρακωρύχοι μπορούν να συμμετέχουν στη διαδικασία εξόρυξης. Κατά τη διάρκεια της εξόρυξης, το δίκτυο blockchain επιλέγει μια "πρόκληση" - γρίφο, η οποία είναι συνήθως μια τιμή κατακερματισμού. Οι ανθρακωρύχοι αναζητούν μέσω των προ-υπολογισμένων plot τους για να βρουν μια λύση που να ταιριάζει με την πρόκληση. Οι ανθρακωρύχοι με μεγαλύτερα plot έχουν περισσότερες πιθανότητες να βρουν έγκυρη λύση.

Πλεονεκτήματα:

Αποδοτικότητα: Το PoC μειώνει το χρόνο που απαιτείται για την προσθήκη και την επικύρωση του μπλοκ συναλλαγών.

Ενεργειακή απόδοση: Το PoC είναι ενεργειακά αποδοτικό σε σύγκριση με το PoW επειδή βασίζεται στον αποθηκευτικό χώρο και όχι στην υπολογιστική ισχύ. Αυτό τον καθιστά πιο φιλικό προς το περιβάλλον μηχανισμό συναίνεσης.

Αξιοποίηση πόρων: Το PoC κάνει αποτελεσματική χρήση του αχρησιμοποίητου χώρου του σκληρού δίσκου, θέτοντάς τον σε παραγωγική χρήση για την εξασφάλιση του δικτύου blockchain. Αυτή η επαναχρησιμοποίηση των πόρων μπορεί να θεωρηθεί ως μια μορφή ανακύκλωσης και βιωσιμότητας.

Μειονεκτήματα:

Υψηλές απαιτήσεις αποθήκευσης: Το PoC απαιτεί από τους συμμετέχοντες να διαθέσουν σημαντική ποσότητα αποθηκευτικού χώρου για τα αρχεία του plot, γεγονός που μπορεί να είναι εντατικό σε πόρους και δαπανηρό, ιδίως για άτομα με περιορισμένη αποθηκευτική ικανότητα.

Αρχική πολυπλοκότητα σχεδίασης: Η δημιουργία των αρχικών αρχείων σχεδίασης μπορεί να είναι πολύπλοκη και χρονοβόρα, απαιτώντας από τους συμμετέχοντες να κατανοήσουν και να ρυθμίσουν σωστά το λογισμικό σχεδίασης.

Proof of Elapsed Time (PoET)

Ο μηχανισμός PoET χρησιμοποιεί έννοιες βασισμένες στη χρονική λοταρία. Διανέμει τυχαίους χρόνους αναμονής σε κάθε ανθρακωρύχο, χάρη σε αξιόπιστα περιβάλλοντα εκτέλεσης (Trusted Execution Environments - TEEs). Τα TEEs παρέχουν ένα ασφαλές και απομονωμένο περιβάλλον εντός ενός συστήματος υπολογιστών, όπου ορισμένοι υπολογισμοί και διαδικασίες μπορούν να εκτελεστούν με υψηλό βαθμό εμπιστευτικότητας και ακεραιότητας. Κατά την διάρκεια του χρόνου αναμονής, ο κόμβος εξόρυξης πρέπει να είναι αδρανής (κοιμάται). Με αυτό τον τρόπο, ο

πρώτος κόμβος που ξυπνάει, δηλαδή με τον μικρότερο χρόνο αναμονής έχει την ευκαιρία να προσθέσει το μπλοκ του στο δίκτυο. Στη συνέχεια, πραγματοποιείται η επαλήθευση του μπλοκ από τους επικυρωτές του δικτύου ώστε να προστεθεί στο blockchain.

Πλεονεκτήματα:

Δικαιοσύνη: Το PoET επιτυγχάνει δικαιοσύνη στην επικύρωση μπλοκ αναθέτοντας επικυρωτές τυχαία με βάση έναν προκαθορισμένο χρόνο αναμονής. Αυτό διασφαλίζει ότι κανένας συμμετέχων δεν έχει αθέμιτο πλεονέκτημα στη δημιουργία μπλοκ.

Επεκτασιμότητα: Το PoET έχει σχεδιαστεί για να κλιμακώνεται καλά, καθιστώντας το κατάλληλο για δίκτυα με μεγάλο αριθμό συμμετεχόντων. Η διαδικασία τυχαίας επιλογής του επιτρέπει την αποτελεσματική συμμετοχή ακόμη και σε μεγάλα δίκτυα.

Μειονεκτήματα:

Πολυπλοκότητα και εξάρτηση από το υλικό: Η υλοποίηση PoET με TEEs μπορεί να είναι πολύπλοκη και η ασφάλεια του δικτύου εξαρτάται σε μεγάλο βαθμό από τη σωστή λειτουργία αυτών των στοιχείων υλικού. Τυχόν ευπάθειες στα TEEs μπορούν να θέσουν σε κίνδυνο το δίκτυο blockchain.

Έκθεση σε ελαττωματικό υλικό: Τα δίκτυα PoET είναι ευάλωτα στους ίδιους κινδύνους που σχετίζονται με το υλικό, όπως και η υποκείμενη τεχνολογία TEE. Εάν το υλικό αποτύχει ή υποστεί βλάβη, μπορεί να διαταράξει τη λειτουργία του δικτύου.

Proof of Authority (PoAuth)

Η συναίνεση με απόδειξη αρχής (Proof of Authority - PoAuth) χρησιμοποιείται από ιδιωτικά ή εξουσιοδοτημένα δίκτυα blockchain. Η PoAuth εξαρτάται σε μεγάλο βαθμό από τη φήμη του ανθρακωρύχου ή του συμμετέχοντος στο δίκτυο που επιθυμεί να προσθέσει ένα νέο μπλοκ συναλλαγών. Εδώ, οι ανθρακωρύχοι ποντάρουν τη φήμη τους και κρυπτονομίσματα. Για να αυξηθεί η φήμη τους, οι επικυρωτές πρέπει να επιβεβαιώνουν την πραγματική τους ταυτότητα και να είναι πρόθυμοι να επενδύσουν χρήματα. Αφού εξακριβωθεί η πραγματική ταυτότητα ενός χρήστη, αυτός θα επιλεγεί από συμμετέχοντες του δικτύου ως επικυρωτής αλλά πλέον θα είναι γνωστός στο δίκτυο (σε αντίθεση με τα PoS συστήματα). Επομένως, έτσι θα ποντάρεται η φήμη του, μαζί με το γεγονός ότι οι υπόλοιποι συμμετέχοντες θα περιμένουν από αυτόν να επενδύσει σημαντικά και σε οικονομικό επίπεδο στο δίκτυο. Επίσης, θα πρέπει να διατηρεί την τυποποιημένη διαδικασία για την απομάκρυνση των ύποπτων επικυρωτών και τη διασφάλιση της μακροπρόθεσμης δέσμευσης.

Πλεονεκτήματα:

Αυξημένη αξιοπιστία: Η πραγματική ταυτότητα κάθε επικυρωτή εξακριβώνεται στο πλαίσιο ενός τέτοιου μοντέλου συναίνεσης, και οι διαχειριστές του δικτύου ελέγχουν πόσο αξιόπιστος είναι ο υποψήφιος επικυρωτής.

Προσαρμοστικότητα: Τα δίκτυα PoAuth προσαρμόζονται εύκολα, καθώς οι επικυρωτές μπορούν να αλλάζουν ανάλογα με τις ανάγκες του δικτύου και οι κανόνες για την επικύρωση των συναλλαγών μπορούν να προσαρμόζονται ανάλογα με τις αντίστοιχες ανάγκες.

Μειονεκτήματα:

Συγκέντρωση: Μόνο ένας περιορισμένος αριθμός αρχών είναι υπεύθυνος για την επικύρωση των συναλλαγών.

Έλλειψη αποκέντρωσης: Το επίπεδο αποκέντρωσης στα δίκτυα PoA είναι συχνά χαμηλό, γεγονός που μπορεί να επηρεάσει την ασφάλεια και την αντίσταση στη λογοκρισία.

Proof of Activity (PoA)

Η απόδειξη δραστηριότητας (PoA) συνδυάζει τους μηχανισμούς PoW και PoS με τρόπο που να επιτρέπει στους συμμετέχοντες να εξορύσσουν και να ανατοκίζουν (staking) τα token τους για να επικυρώνουν μπλοκ. Οι συμμετέχοντες ασχολούνται αρχικά με την παραδοσιακή εξόρυξη PoW, ανταγωνιζόμενοι για την επίλυση πολύπλοκων μαθηματικών γρίφων για την επικύρωση συναλλαγών και τη δημιουργία νέων μπλοκ με πληροφορίες επικεφαλίδας αλλά πλέον και με διεύθυνση ανταμοιβής. Όταν βρεθεί (ή εξορυχθεί) ένα νέο μπλοκ, το σύστημα μεταβαίνει σε PoS, σε μια φάση που ονομάζεται minting με το εξορυγμένο μπλοκ να περιέχει μόνο μια επικεφαλίδα και τη διεύθυνση ανταμοιβής του ανθρακωρύχου, οπότε θα πρέπει να επικυρωθεί. Με βάση τα στοιχεία της επικεφαλίδας, επιλέγεται μια νέα, τυχαία ομάδα επικυρωτών από το δίκτυο που καλούνται να επικυρώσουν ή να υπογράψουν το νέο μπλοκ. Όσο περισσότερα νομίσματα κατέχει ένας επικυρωτής, τόσο περισσότερες πιθανότητες έχει να επιλεγεί ως υπογράφων (όπως και στο PoS). Μόλις όλοι οι επικυρωτές υπογράψουν το νεοαποκτηθέν μπλοκ, αυτό αποκτά την ιδιότητα ενός πλήρους μπλοκ, ταυτοποιείται και προστίθεται στο δίκτυο blockchain. Στην ουσία, ο μηχανισμός PoA είναι μια υβριδική μέθοδος που προσπαθεί να αντλήσει τα θετικά από τους PoW και PoS.

Πλεονεκτήματα:

Ενισχυμένη ασφάλεια: Το PoA παρέχει ενισχυμένη ασφάλεια ενσωματώνοντας την αρχική φάση εξόρυξης PoW. Αυτό καθιστά δαπανηρή και δύσκολη την επίθεση κακόβουλων φορέων στο δίκτυο κατά τη διάρκεια αυτής της φάσης.

Ενεργειακή απόδοση: Το PoA μειώνει σημαντικά την κατανάλωση ενέργειας σε σύγκριση με τις παραδοσιακές αλυσίδες μπλοκ PoW, επειδή βασίζεται στο PoS κατά τη φάση του minting, η οποία δεν απαιτεί δραστηριότητες εξόρυξης.

Ενεργή συμμετοχή: Το PoA παρέχει κίνητρα τόσο για τους miners όσο και για τους stakers, ενθαρρύνοντας την ενεργό συμμετοχή στο δίκτυο. Οι ανθρακωρύχοι ανταμείβονται για την εξασφάλιση του δικτύου κατά τη φάση PoW, ενώ οι stakers κερδίζουν ανταμοιβές για το minting του μπλοκ κατά τη φάση PoS.

Μειονεκτήματα:

Πολυπλοκότητα: μπορεί να καταστήσει το πρωτόκολλο πιο πολύπλοκο στην κατανόηση και την υλοποίηση σε σύγκριση με απλούστερους μηχανισμούς συναίνεσης. Επίσης, η μετάβαση μεταξύ της φάσης εξόρυξης PoW και της φάσης minting PoS μπορεί να είναι πολύπλοκη. Απαιτείται προσεκτική διαχείριση κατά τη διάρκεια αυτών των μεταβάσεων.

Proof of Burn (PoB)

Το PoB επιτρέπει στους ανθρακωρύχους να προσθέσουν το μπλοκ τους στέλνοντας μερικά από τα νομίσματά τους σε έναν λογαριασμό που δεν μπορεί να τα δαπανήσει. Αυτή η διαδικασία της αποστολής των κερδισμένων νομισμάτων σε ένα λογαριασμό καταθέσεων ονομάζεται "κάψιμο" των νομισμάτων. Το PoB εξαλείφει μόνιμα τα "καμένα" νομίσματα από τις κανονικές συναλλαγές. Ως εκ τούτου, καθίστανται αδιάθετα ακόμη και από τον ιδιοκτήτη τους.

Όσο περισσότερα νομίσματα καίει ένας ανθρακωρύχος, τόσο μεγαλύτερες είναι οι πιθανότητές του να προσθέσει το νέο μπλοκ συναλλαγών του στο δίκτυο. Δηλαδή το πόσα νομίσματα καίει ένας ανθρακωρύχος αποδεικνύει την εικονική ισχύ εξόρυξής του. Επομένως, όσο περισσότερα νομίσματα, τόσο μεγαλύτερη η ισχύς και το αντίστροφο. Οπότε, η καύση νομισμάτων αποφέρει εικονικά δικαιώματα εξόρυξης στον ανθρακωρύχο. Επιδεικνύοντας την αφοσίωσή τους στο δίκτυο μέσω της σκόπιμης καταστροφής tokens (κρυπτονομισμάτων) αντί της δαπάνης υπολογιστικών πόρων και της αξιοποίησης ισχυρού υλικού εξόρυξης, οι ανθρακωρύχοι σε μια ρύθμιση PoB είναι σε θέση να λειτουργούν με πολύ λιγότερη ενέργεια από ό,τι συχνά απαιτούν τα κλασικά συστήματα PoW.

Πλεονεκτήματα:

Καλύτερη αποκέντρωση: Το PoB επιτρέπει την αποκεντρωμένη και δίκαιη έναρξη ενός δικτύου blockchain. Οι συμμετέχοντες καίνε τα υπάρχοντα κρυπτονομίσματα για να λάβουν τις νέες εγγενείς μάρκες, γεγονός που συμβάλλει στην αποφυγή ζητημάτων προ-εξόρυξης και συγκέντρωσης τους.

Μείωση της κερδοσκοπίας: Το PoB ενθαρρύνει τους συμμετέχοντες να αποδείξουν τη δέσμευσή τους στην επιτυχία του δικτύου καίγοντας τα υπάρχοντα token. Αυτό μπορεί να μειώσει την κερδοσκοπική συμπεριφορά και να ευθυγραμμίσει τα συμφέροντα των συμμετεχόντων με τους μακροπρόθεσμους στόχους του δικτύου.

Μειονεκτήματα:

Καταστροφή μαρκών (tokens): Το PoB απαιτεί από τους συμμετέχοντες να καταστρέψουν τα υπάρχοντα κρυπτονομίσματα για να αποκτήσουν δικαιώματα εξόρυξης ή άλλα προνόμια στο δίκτυο. Αυτό μπορεί να οδηγήσει σε μείωση της κυκλοφοριακής προσφοράς του εγγενούς κρυπτονομίσματος, επηρεάζοντας δυνητικά την αγοραία αξία και τη ρευστότητά του.

Περιβαλλοντικές επιπτώσεις: Παρόλο που το PoB δεν καταναλώνει ενέργεια όπως το PoW, εξακολουθεί να έχει περιβαλλοντικό αντίκτυπο όσον αφορά την καταστροφή των μαρκών, καθώς αυτές αντιπροσωπεύουν πραγματική οικονομική αξία.

Practical Byzantine Fault Tolerance (PBFT)

Το pBFT στοχεύει στην επίλυση του γρίφου των Βυζαντινών Στρατηγών για την λήψη αποφάσεων. Βασίζεται στο πρόβλημα επικοινωνίας που μπορεί να έχουν οι στρατηγοί διαφορετικών στρατών που πρέπει να αποφασίσουν αν θα επιτεθούν ή θα υποχωρήσουν

ταυτόχρονα. Ουσιαστικά περιγράφει την πολυπλοκότητα της επίτευξης συμφωνίας εάν υπάρχουν άπιστοι στρατηγοί.

Ο μηχανισμός PBFT ρυθμίζει την επικοινωνία μεταξύ των κόμβων χρησιμοποιώντας κατακερματισμούς, ψηφιακές υπογραφές και μετα-δεδομένα. Επιτυγχάνει συναίνεση όταν υπάρχει συμφωνία ⅔ από τους ειλικρινείς κόμβους. Ωστόσο, η ασφάλεια του PBFT θα παραβιαστεί εάν οι ανέντιμοι/ελαττωματικοί κόμβοι είναι περισσότεροι από το ⅓ όλων των κόμβων του δικτύου. Οι κόμβοι στο PBFT χωρίζονται σε πρωτεύοντες και δευτερεύοντες κόμβους. Οι πρωτεύοντες κόμβοι είναι οι κόμβοι-ηγέτες, ενώ οι δευτερεύοντες κόμβοι είναι οι εφεδρικοί κόμβοι. Οι πρωτεύοντες κόμβοι αλλάζουν σε κάθε γύρο συναίνεσης. Ο πρωτεύων κόμβος για τον επόμενο γύρο επιλέγεται συνήθως κυκλικά, διασφαλίζοντας ότι κάθε κύριος κόμβος έχει σειρά να ενεργήσει ως πρωτεύων κόμβος. [19] [20] [21]

Πλεονεκτήματα:

Χαμηλή καθυστέρηση επιβεβαίωσης: Ο PBFT παρέχει ταχύτερους χρόνους επιβεβαίωσης συναλλαγών σε σύγκριση με τον PoW και ορισμένους άλλους μηχανισμούς συναίνεσης, καθιστώντας τον κατάλληλο για εφαρμογές που απαιτούν ταχεία οριστικοποίηση συναλλαγών.

Ανθεκτικότητα σε βυζαντινά σφάλματα: Ο PBFT έχει σχεδιαστεί για να ανέχεται έως και το ένα τρίτο των κόμβων να συμπεριφέρονται κακόβουλα ή να αποτυγχάνουν, ενώ εξακολουθεί να επιτυγχάνει συναίνεση (όσο βρίσκεται στο προκαθορισμένο όριο). Αυτή η ανοχή σε σφάλματα τον καθιστά μια στιβαρή επιλογή για δίκτυα όπου η αξιοπιστία είναι ζωτικής σημασίας.

Μειονεκτήματα:

Πιθανή αποτυχία συστήματος: Εάν ο αριθμός των ελαττωματικών κόμβων υπερβαίνει ένα ορισμένο όριο, το PBFT ενδέχεται να μην είναι σε θέση να επιτύχει συναίνεση, οδηγώντας σε αποτυχίες του συστήματος.

Μη κλιμακωσιμότητα: Το PBFT είναι αποδοτικό για μικρό έως μεσαίο αριθμό κόμβων, η απόδοσή του μπορεί να υποβαθμιστεί καθώς αυξάνεται ο αριθμός των κόμβων.

Πίνακας 1. Είδος Αρχιτεκτονικής/Μηχανισμοί Συναίνεσης

Public	PoW, PoS, DPoS, PoAuth, PoC, PoI, PoB
Private	PoS, PoAuth, PBFT
Consortium	PoAuth, PBFT, PoET, PoB
Hybrid	PoS, DPoS, PoAuth

Παραπάνω παρατίθεται ένας πίνακας (Πίνακας 1) που δείχνει τι είδος μηχανισμού συναίνεσης χρησιμοποιείται συνήθως από την εκάστοτε αρχιτεκτονική blockchain.

Με βάση τον πίνακα παρατηρούμε ότι ο μηχανισμός συναίνεσης PoAuth μπορεί να χρησιμοποιηθεί συχνά για όλες τις αρχιτεκτονικές blockchain, ενώ επίσης ότι ο μηχανισμός συναίνεσης PoS χρησιμοποιείτε συχνά σε όλες τις αρχιτεκτονικές εκτός από τα Consortium blockchain.

2.8 Έξυπνα Συμβόλαια

Τα έξυπνα συμβόλαια ή έξυπνες συμβάσεις, είναι αυτό-εκτελούμενα προγράμματα υπολογιστή αποθηκευμένα στο blockchain. Συγκεκριμένα, όταν αναπτύσσεται ένα έξυπνο συμβόλαιο, ο κώδικας και τα αρχικά δεδομένα του συσκευάζονται σε μια συναλλαγή και περιλαμβάνονται σε ένα μπλοκ από έναν ανθρακωρύχο ή επικυρωτή. Αυτή η αρχική συναλλαγή ανάπτυξης καταγράφεται στο blockchain.

Τα έξυπνα συμβόλαια μπορούν να εφαρμοστούν σε ένα ευρύ φάσμα περιπτώσεων χρήσης πέραν των χρηματοπιστωτικών συναλλαγών, όπως συστήματα ψηφοφορίας, οι συναλλαγές ακινήτων, οι ασφαλιστικές απαιτήσεις και άλλα. Οποιοδήποτε σενάριο όπου πρέπει να ικανοποιηθεί ένα προκαθορισμένο σύνολο συνθηκών για να πραγματοποιηθεί μια ενέργεια μπορεί δυνητικά να επωφεληθεί από τις έξυπνες συμβάσεις. Τα έξυπνα συμβόλαια ελέγχουν, μεταξύ άλλων, άμεσα και αυτόματα τη μεταφορά ψηφιακών περιουσιακών στοιχείων μεταξύ των μερών, και εκτελούνται όταν πληρούνται προκαθορισμένες συνθήκες. Συνήθως χρησιμοποιούνται για την αυτοματοποίηση της εκτέλεσης μιας συμφωνίας, έτσι ώστε όλοι οι συμμετέχοντες να είναι άμεσα βέβαιοι για το αποτέλεσμα, χωρίς την εμπλοκή οποιουδήποτε ενδιάμεσου ή την απώλεια χρόνου. Μόλις ολοκληρωθεί, μια τέτοια συναλλαγή είναι ανιχνεύσιμη και μη αναστρέψιμη. Ένα έξυπνο συμβόλαιο μπορεί να είναι σχεδιασμένο να εκτελεί μια σειρά από συναλλαγές και όχι μόνο μια.

Ένα έξυπνο συμβόλαιο είναι απλώς ένα ψηφιακό συμβόλαιο με την κωδικοποίηση ασφάλειας του blockchain και με την διεύθυνση του μέσα σε αυτή. Η κρυπτογράφηση παρέχει ασφαλή αυθεντικοποίηση και μεταφορά μηνυμάτων μεταξύ των μερών που σχετίζονται με τις έξυπνες συμβάσεις. Ένα έξυπνο συμβόλαιο συνήθως λειτουργεί ακολουθώντας απλές δηλώσεις "AN/TOTE" ("IF/THEN") που είναι γραμμένες σε κώδικα στο blockchain. Τέτοιου είδους δηλώσεις χρησιμοποιούνται πιο συχνά και κυρίως για βασικές ενέργειες, αλλά μπορεί να χρησιμοποιηθούν και πιο πολύπλοκες δηλώσεις για χειρισμό πιο σύνθετων σεναρίων. Ένα δίκτυο υπολογιστών εκτελεί τις ενέργειες όταν πληρούνται και επαληθεύονται προκαθορισμένες συνθήκες. Στη συνέχεια, το blockchain ενημερώνεται όταν ολοκληρωθεί η συναλλαγή. Αυτό σημαίνει ότι η συναλλαγή δεν μπορεί να αλλάξει και μόνο τα μέρη στα οποία έχει χορηγηθεί άδεια μπορούν να δουν τα αποτελέσματα.

Στο πλαίσιο ενός έξυπνου συμβολαίου, μπορούν να υπάρχουν όσοι όροι χρειάζονται για να ικανοποιήσουν τους συμμετέχοντες ότι η εργασία θα ολοκληρωθεί ικανοποιητικά. Για τον προσδιορισμό των όρων, οι συμμετέχοντες πρέπει να καθορίσουν τον τρόπο με τον οποίο οι συναλλαγές και τα δεδομένα τους αναπαρίστανται στο blockchain, να συμφωνήσουν στους κανόνες "AN/TOTE" που διέπουν τις εν λόγω συναλλαγές, να διερευνήσουν όλες τις πιθανές εξαιρέσεις και να ορίσουν ένα πλαίσιο για την επίλυση των διαφορών. Παράδειγμα προϋπόθεσης θα μπορούσε να είναι ο έλεγχος αν το ποσό της αξίας που πρόκειται να μεταφερθεί είναι πράγματι διαθέσιμο στον λογαριασμό του αποστολέα. Τέλος, μπορεί επίσης να περιλαμβάνει τους χρονικούς περιορισμούς που μπορούν να εισάγουν προθεσμίες στο συμβόλαιο. Σε αυτή την περίπτωση οι συνθήκες είναι της μορφής "ΟΤΑΝ/TOTE" ("WHEN/THEN"). Σε τέτοιου είδους συνθήκες θα μπορούσαν να υφίστανται συναλλαγές που θα χρειάζεται να περάσει κάποιος προκαθορισμένος χρόνος για να ολοκληρωθούν (πχ. κάποια πληρωμή να γίνει σε μια συγκεκριμένη μέρα) ή εξαιρέσεις, όπως ποινές, εφόσον δεν ολοκληρωθεί η απαιτούμενη συναλλαγή μέσα σε κάποιο προκαθορισμένο διάστημα.

Το έξυπνο συμβόλαιο μπορεί να αναπτυχθεί από έναν προγραμματιστή - αν και όλο και περισσότερο, οι οργανισμοί που χρησιμοποιούν το blockchain για επιχειρήσεις παρέχουν

πρότυπα, διεπαφές ιστού και άλλα διαδικτυακά εργαλεία για την απλοποίηση της δόμησης των έξυπνων συμβολαίων.

Μόλις ολοκληρωθεί μια προϋπόθεση, η σύμβαση εκτελείται αμέσως. Επειδή οι έξυπνες συμβάσεις είναι ψηφιακές και αυτοματοποιημένες, δεν υπάρχει γραφειοκρατία προς επεξεργασία και δεν δαπανάται χρόνος για τη διόρθωση σφαλμάτων που συχνά προκύπτουν από τη χειροκίνητη συμπλήρωση εγγράφων.

Γίνεται κατανοητό, λοιπόν, ότι τα έξυπνα συμβόλαια έχουν προϋποθέσεις έναρξης αλλά και προϋποθέσεις εκτέλεσης ενεργειών. Για παράδειγμα, αν θεωρηθεί ένα απλό έξυπνο συμβόλαιο καταθέσεων για μια αγορά ψηφιακών αγαθών, οι συνθήκες εκκίνησης μπορεί να περιλαμβάνουν την αρχικοποίηση της σύμβασης με τις διευθύνσεις του αγοραστή και του πωλητή και τη συμφωνηθείσα τιμή. Οι συνθήκες εκτέλεσης θα μπορούσαν να περιλαμβάνουν την αποδέσμευση της πληρωμής στον πωλητή όταν ο αγοραστής επιβεβαιώσει την παραλαβή των ψηφιακών αγαθών ή την επιστροφή της πληρωμής στον αγοραστή εάν ο πωλητής δεν παραδώσει.

Επειδή δεν εμπλέκεται κανένας τρίτος και επειδή τα κρυπτογραφημένα αρχεία των συναλλαγών μοιράζονται μεταξύ των συμμετεχόντων, δεν υπάρχει λόγος να αμφισβητείται αν οι πληροφορίες έχουν αλλοιωθεί για προσωπικό όφελος. Επίσης, όλοι στο δίκτυο έχουν εγγυημένα ένα αντίγραφο όλων των όρων του έξυπνου συμβολαίου. Ένα έξυπνο συμβόλαιο αναπαράγεται και διανέμεται από όλους τους κόμβους που είναι συνδεδεμένοι στο δίκτυο.

Όλες οι συναλλαγές της σύμβασης αποθηκεύονται με χρονολογική σειρά στο blockchain και είναι προσβάσιμες μαζί με την πλήρη διαδρομή ελέγχου. Ωστόσο, τα εμπλεκόμενα μέρη μπορούν να διασφαλίσουν κρυπτογραφικά την ταυτότητα τους για πλήρη ιδιωτικότητα.

Επειδή οι έξυπνες συμβάσεις εκτελούν συμφωνίες, μπορούν να χρησιμοποιηθούν για πολλούς διαφορετικούς σκοπούς. Μία από τις απλούστερες χρήσεις είναι η διασφάλιση της πραγματοποίησης συναλλαγών μεταξύ δύο μερών, όπως η αγορά και η παράδοση αγαθών. Για παράδειγμα, ένας κατασκευαστής που χρειάζεται πρώτες ύλες μπορεί να ρυθμίσει τις πληρωμές και ο προμηθευτής μπορεί να ρυθμίσει τις αποστολές χρησιμοποιώντας μια έξυπνη σύμβαση. Στη συνέχεια, ανάλογα με τη συμφωνία μεταξύ των δύο επιχειρήσεων, τα κεφάλαια θα μπορούσαν να μεταφερθούν αυτόματα στον προμηθευτή κατά την αποστολή ή την παράδοση. [22] [23]

2.9 Εφαρμογές

Η δημοτικότητα της τεχνολογίας blockchain έχει αυξηθεί πάρα πολύ την τελευταία δεκαετία. Καθώς αλλάζει τα δεδομένα στην τεχνολογία, θεωρείται ως η επόμενη μεγάλη επανάσταση μετά τη γέννηση του διαδικτύου.

Ένα blockchain αποθηκεύει πληροφορίες σε ψηφιακή μορφή ηλεκτρονικά, όπως μια βάση δεδομένων. Τα blockchain είναι ευρέως αναγνωρισμένα επειδή παίζουν σημαντικό ρόλο στα δίκτυα κρυπτονομισμάτων, όπως το Bitcoin, όπου διατηρούν ένα ασφαλές και αποκεντρωμένο αρχείο συναλλαγών. Παρόλα αυτά, τα κρυπτονομίσματα, αν και πολύ σημαντικός, δεν είναι ο μόνος τομέας στον οποίο μπορεί να χρησιμοποιηθεί η τεχνολογία blockchain. Παρακάτω θα παρουσιαστούν μερικές εφαρμογές της τεχνολογίας συμπεριλαμβανομένου των κρυπτονομισμάτων:

- Κρυπτονόμισμα

  Ίσως μία από τις πιο δημοφιλείς εφαρμογές της Blockchain είναι το κρυπτονόμισμα. Τα κρυπτονομίσματα μπορούν να χρησιμοποιηθούν για συναλλαγές σε όλο τον κόσμο. Αυτή η επιλογή είναι πολύ καλύτερη από τις περιφερειακές εφαρμογές πληρωμών, οι οποίες είναι σχετικές μόνο σε μια συγκεκριμένη χώρα ή γεωγραφική περιοχή και δεν μπορούν να χρησιμοποιηθούν για την πληρωμή χρημάτων σε άτομα σε άλλες χώρες. Επιπλέον, δεν χρειάζεται μεσάζοντας στην συναλλαγή. Επομένως, οι συναλλαγές γίνονται πολύ γρήγορα από οπουδήποτε με την χρήση κρυπτονομισμάτων.

- Διαχείριση περιουσιακών στοιχείων

  Το blockchain παίζει μεγάλο ρόλο στον χρηματοπιστωτικό κόσμο και στη διαχείριση περιουσιακών στοιχείων. Σε γενικές γραμμές, η διαχείριση περιουσιακών στοιχείων περιλαμβάνει τον χειρισμό και την ανταλλαγή διαφόρων περιουσιακών στοιχείων που μπορεί να κατέχει ένα άτομο, όπως σταθερό εισόδημα, ακίνητα, μετοχές, αμοιβαία κεφάλαια, εμπορεύματα και άλλες εναλλακτικές επενδύσεις. Οι συνήθεις διαδικασίες συναλλαγών στη διαχείριση περιουσιακών στοιχείων μπορεί να είναι πολύ δαπανηρές, ιδίως εάν οι συναλλαγές αφορούν πολλές χώρες και διασυνοριακές πληρωμές. Σε τέτοιες περιπτώσεις, το Blockchain μπορεί να προσφέρει μεγάλη βοήθεια, καθώς καταργεί τις ανάγκες για οποιουσδήποτε μεσάζοντες, όπως χρηματιστές, θεματοφύλακες, μεσίτες, διαχειριστές διακανονισμών κλπ.

- Υγειονομική περίθαλψη

  Το blockchain μπορεί να έχει μεγάλο αντίκτυπο στην υγειονομική περίθαλψη με τη χρήση έξυπνων συμβάσεων. Αυτές οι έξυπνες συμβάσεις σημαίνουν ότι μια σύμβαση γίνεται μεταξύ 2 μερών χωρίς να χρειάζεται κάποιος μεσάζων. Όλα τα μέρη που εμπλέκονται στη σύμβαση γνωρίζουν τις λεπτομέρειες της σύμβασης και η σύμβαση υλοποιείται αυτόματα όταν πληρούνται οι όροι της σύμβασης. Αυτό μπορεί να είναι πολύ χρήσιμο στην υγειονομική περίθαλψη, όπου τα προσωπικά αρχεία υγείας μπορούν να κωδικοποιηθούν μέσω Blockchain, ώστε να είναι προσβάσιμα μόνο σε παρόχους πρωτοβάθμιας υγειονομικής περίθαλψης με ένα κλειδί. Σε περίπτωση χρήσης των ιδιωτικών blockchain μάλιστα μπορεί να τηρηθεί και ο κανόνας προστασίας προσωπικών δεδομένων HIPAA, ο οποίος διασφαλίζει ότι οι πληροφορίες των ασθενών είναι εμπιστευτικές και δεν είναι προσβάσιμες σε όλους. Επίσης, το blockchain χρησιμοποιείται για την παρακολούθηση

και τον εντοπισμό συνταγογραφούμενων φαρμάκων σε όλα τα δίκτυα εφοδιασμού. Με τη χρήση αυτού του εργαλείου, είναι δυνατή η απλή και ταχεία πρόληψη και ρύθμιση της διανομής πλαστών φαρμάκων καθώς και η ανάκληση αναποτελεσματικών και μη ασφαλών φαρμάκων.

- Διαδικτυακή επαλήθευση ταυτότητας

  Δεν είναι δυνατή η ολοκλήρωση οποιασδήποτε οικονομικής συναλλαγής στο διαδίκτυο χωρίς διαδικτυακή επαλήθευση και ταυτοποίηση. Και αυτό ισχύει για όλους τους πιθανούς παρόχους υπηρεσιών που μπορεί να έχει κάθε χρήστης στον χρηματοπιστωτικό και τραπεζικό τομέα. Αυτό σημαίνει πως η διαδικασία επαλήθευσης θα επαναλαμβάνεται για κάθε πάροχο υπηρεσίας. Ωστόσο, το blockchain μπορεί να συγκεντρώσει τη διαδικασία διαδικτυακής επαλήθευσης ταυτότητας, ώστε οι χρήστες να χρειάζεται να επαληθεύσουν την ταυτότητά τους μόνο μία φορά χρησιμοποιώντας το blockchain και στη συνέχεια να μπορούν να μοιραστούν αυτή την ταυτότητα με όποιον πάροχο υπηρεσιών επιθυμούν. Οι χρήστες έχουν, επίσης, τη δυνατότητα να επιλέξουν τις μεθόδους επαλήθευσης της ταυτότητάς τους, όπως η πιστοποίηση ταυτότητας χρήστη, η αναγνώριση προσώπου κ.λ.π.

- Διαδίκτυο των πραγμάτων

  Το Διαδίκτυο των πραγμάτων είναι ένα δίκτυο διασυνδεδεμένων συσκευών που μπορούν να αλληλοεπιδρούν μεταξύ τους και να συλλέγουν δεδομένα που μπορούν να χρησιμοποιηθούν για την απόκτηση χρήσιμων πληροφοριών. Οποιοδήποτε σύστημα "πραγμάτων" γίνεται ένα σύστημα IoT μόλις διασυνδεθεί. Ένα συνηθισμένο παράδειγμα ενός IoT συστήματος είναι το έξυπνο σπίτι, όπου όλες οι οικιακές συσκευές, όπως τα φώτα, ο θερμοστάτης, το κλιματιστικό, ο συναγερμός καπνού κ.λ.π., μπορούν να συνδεθούν μεταξύ τους σε μια ενιαία πλατφόρμα. Το Διαδίκτυο των Πραγμάτων (IoT) κάνει τη ζωή μας ευκολότερη, αλλά ανοίγει επίσης την πόρτα σε κακόβουλους φορείς να αποκτήσουν πρόσβαση στα δεδομένα μας ή να πάρουν τον έλεγχο σημαντικών συστημάτων. Η τεχνολογία blockchain και κυρίως τα ιδιωτικά αλλά και σε ορισμένες περιπτώσεις τα blockchain κοινοπραξίας και τα υβριδικά (που έχουν χαρακτηριστικά των ιδιωτικών) μπορεί να παρέχει μεγαλύτερη ασφάλεια, αποθηκεύοντας κωδικούς πρόσβασης και άλλα δεδομένα (όπως αρχεία συντήρησης και δεδομένα αισθητήρων) σε ένα αποκεντρωμένο δίκτυο αντί για έναν κεντρικό διακομιστή. Επιπλέον, προσφέρει προστασία από την αλλοίωση των δεδομένων, καθώς ένα blockchain είναι πρακτικά αμετάβλητο.

- Πνευματικά δικαιώματα και NFTs

  Τα πνευματικά δικαιώματα είναι ένα μεγάλο ζήτημα στους δημιουργικούς τομείς, όπως η μουσική, οι ταινίες κ.λ.π. Τα τελευταία είναι καλλιτεχνικά μέσα και δεν φαίνεται να έχουν κάποια σχέση με το Blockchain. Όμως, η τεχνολογία του Blockchain είναι αρκετά σημαντική για τη διασφάλιση της ασφάλειας και της διαφάνειας στις δημιουργικές βιομηχανίες. Υπάρχουν πολλές περιπτώσεις όπου τα καλλιτεχνικά μέρη μπορούν να αποτελέσουν προϊόν λογοκλοπής. Αυτό μπορεί να διορθωθεί με τη χρήση του Blockchain, το οποίο μπορεί να διαθέτει ένα λεπτομερές ψηφιακό (λογιστικό) βιβλίο με τα δικαιώματα των καλλιτεχνών. Αυτό μπορεί να αποτελέσει πολύτιμο αποδεικτικό στοιχείο σε διαφορές πνευματικών δικαιωμάτων, αποδεικνύοντας την κυριότητά και την πρωτοτυπία του έργου κάποιου καλλιτέχνη. Η πληρωμή των δικαιωμάτων μπορεί, επίσης, να διαχειριστεί με τη χρήση ψηφιακών νομισμάτων. Είναι σημαντικό να σημειωθεί ότι, ενώ η τεχνολογία blockchain μπορεί να ενισχύσει την προστασία των πνευματικών δικαιωμάτων, δεν

αντικαθιστά τους παραδοσιακούς νομικούς μηχανισμούς, όπως η καταχώρηση πνευματικών δικαιωμάτων ή οι νόμοι περί πνευματικής ιδιοκτησίας. Για να προστατεύσει κάποιος πλήρως τα πνευματικά του δικαιώματα, είναι σκόπιμο να συνδυάσει λύσεις που βασίζονται στην τεχνολογία blockchain με νομικά μέτρα και να συμβουλευτεί νομικούς εμπειρογνώμονες που ειδικεύονται στη νομοθεσία περί πνευματικής ιδιοκτησίας και πνευματικών δικαιωμάτων.

Τα non-fungible tokens, ή NFTs, θεωρούνται συνήθως ως τρόποι κατοχής των δικαιωμάτων της ψηφιακής τέχνης. Δεδομένου ότι το blockchain αποτρέπει την κατοχή ενός asset από πολλαπλούς χρήστες, η τοποθέτηση ενός NFT σε αυτό εγγυάται ότι υπάρχει μόνο ένα αντίγραφο ενός έργου ψηφιακής τέχνης. Αυτό μπορεί να μοιάζει σαν επένδυση σε φυσική τέχνη, αλλά χωρίς τα μειονεκτήματα της αποθήκευσης και της συντήρησης. Χάρη στην τεχνολογία blockchain, οι καταναλωτές μπορούν πλέον να διεκδικήσουν την αποκλειστική κυριότητα ορισμένων από τα πιο επιθυμητά ψηφιακά περιουσιακά στοιχεία που υπάρχουν.

Τα NFTs μπορούν να έχουν ποικίλες εφαρμογές. Τελικά, αποτελούν ένα τρόπο να μεταφέρεται η ιδιοκτησία σε οτιδήποτε μπορεί να αναπαρασταθεί με δεδομένα. Αυτό θα μπορούσε να είναι ο τίτλος ιδιοκτησίας ενός σπιτιού, τα δικαιώματα μετάδοσης ενός βίντεο ή ένα εισιτήριο εκδήλωσης. Οτιδήποτε εξ αποστάσεως μοναδικό θα μπορούσε να είναι ένα NFT.

- Ψηφοφορία

Το blockchain έχει αναδειχθεί σε βασικό θέμα στις συζητήσεις για την ασφαλή ψηφοφορία. Παρόλο που η ηλεκτρονική ψηφοφορία λύνει τις περισσότερες από τις δυσκολίες που σχετίζονται με την παλιά χειρόγραφη ψηφοφορία, ζητήματα όπως το απόρρητο των ψηφοφόρων, η απάτη των ψηφοφόρων και το υψηλό κόστος των παλαιών τεχνολογιών ψηφιακής ψηφοφορίας παραμένουν βασικές ανησυχίες.

Η χρήση της τεχνολογίας blockchain μπορεί να διασφαλίσει ότι κανείς δεν ψηφίζει δύο φορές, ότι μόνο οι δικαιούχοι ψηφοφόροι μπορούν να ψηφίσουν και ότι οι ψήφοι δεν μπορούν να αλλοιωθούν. Επιπλέον, μπορεί να αυξήσει την πρόσβαση στην ψηφοφορία, καθιστώντας την τόσο απλή όσο το πάτημα μερικών κουμπιών σε ένα smartphone. Ταυτόχρονα, το κόστος διεξαγωγής των εκλογών θα μειωθεί σημαντικά.

Μέσω των έξυπνων συμβάσεων και της κρυπτογράφησης, το blockchain μπορεί να καταστήσει την ψηφοφορία ασφαλέστερη, πιο διαφανή και πιο ιδιωτική για τους ψηφοφόρους. Το blockchain μπορεί να εκπληρώσει αυτούς τους στόχους, καθώς και να επιτρέψει την προσαρμογή της διαδικασίας ψηφοφορίας μέσω της χρήσης πολλαπλών τύπων ψηφοδελτίων και ψηφοφορίας με βάση τη λογική. [24] [25] [26]

3. Μεθοδολογία Επιλογής Άρθρων

Οι βασικές ερωτήσεις που θέλει να απαντήσει η συγκεκριμένη διπλωματική εργασία είναι:

- Ποια είναι τα ζητήματα ασφάλειας και οι πιθανές επιθέσεις που μπορούν να γίνουν στο blockchain;
- Τι αντίμετρα μπορούν να χρησιμοποιηθούν για την αντιμετώπιση ή τον μετριασμό της εκάστοτε επίθεσης;

Στην παρούσα διπλωματική εργασία έγινε συστηματική μελέτη της βιβλιογραφίας με βάση κατάλληλη επιλογή άρθρων για την ανάλυση των πιθανών επιθέσεων που μπορούν να γίνουν στο blockchain, αλλά και των πιθανών αντίμετρων για τις επιθέσεις αυτές.

Η στρατηγική αναζήτησης που εφαρμόστηκε ήταν με την χρήση λέξεων-κλειδιών, προκειμένου να αναζητηθεί σχετική βιβλιογραφία στο Google και Google Scholar. Επίσης, πολλά άρθρα της βιβλιογραφίας που χρησιμοποιήθηκαν υπήρχαν ως παραπομπές (μέθοδος snowball) σε άρθρα που βρέθηκαν με την αρχική μέθοδο αναζήτησης. Οι λέξεις κλειδιά που χρησιμοποιήθηκαν κυρίως είναι: “Blockchain && (Consensus Mechanism | Network | Transaction | Smart Contract)? && (Security | Attacks | Countermeasures).

Εξετάστηκαν αρκετά άρθρα καθώς και μελέτες που εμφανίστηκαν με τις παραπάνω λέξεις κλειδιά. Προκειμένου να διαχωριστούν οι μελέτες, εφαρμόστηκαν κριτήρια επιλογής, απόρριψης και ποιότητας, για να καθοριστεί αν θα συμπεριληφθούν ή όχι στην μετέπειτα ανάλυση.

Τα κριτήρια επιλογής ήταν τα εξής:

- Άρθρα που αναλύουν επιθέσεις ανά “στρώμα”, όπου τα στρώματα είναι τα εξής: στρώμα μηχανισμού συναίνεσης, συναλλαγών, δικτύου και έξυπνων συμβολαίων.
- Άρθρα που περιέχουν αντίμετρα άμυνας ή συγκεκριμένα εργαλεία αντιμετώπισης επιθέσεων στο blockchain.
- Πρόσφατα άρθρα που έχουν δημοσιευθεί από το 2014 και έπειτα.

Τα κριτήρια απόρριψης ήταν τα εξής:

- Αποκλεισμός άρθρων με αδυναμία πρόσβασης στο περιεχόμενό τους (λόγω σχετικών περιορισμών).
- Αποκλεισμός άρθρων σε γλώσσα εκτός των Αγγλικών.

Τα κριτήρια ποιότητας ήταν τα εξής:

- Άρθρα με δύσκολη ανάγνωση περιεχομένου.

- Άρθρα χωρίς αξιολόγηση της συνεισφοράς τους.
- Άρθρα χωρίς κάποια αξιόλογη συνεισφορά.
- Άρθρα με λιγοστές και απλοϊκές πληροφορίες.

Οι πηγές που αρχικά εντοπίστηκαν ήταν 167 και αυτές που διατηρήθηκαν και χρησιμοποιήθηκαν στην Διπλωματική εργασία ήταν 106.

Από τις 106, οι 51 ήταν ερευνητικά επιστημονικά άρθρα και οι 55 τεχνικά άρθρα από ιστότοπους (sites).

4. Ζητήματα Ασφαλείας

Στο κεφάλαιο αυτό αναλύονται αρχικά μερικές γενικές ευπάθειες των συστημάτων blockchain, καθώς και μερικές γενικές ευπάθειες για μερικούς βασικούς μηχανισμούς συναίνεσης του blockchain (Ενότητα 4.1.4). Στην συνέχεια παρατίθεται μια ανάλυση (Ενότητα 4.2) των βασικών επιθέσεων που μπορούν να γίνουν στο blockchain, χωρισμένες σε ορισμένες βασικές κατηγορίες.

4.1 Τρωτότητες Blockchain

4.1.1 Blockchain Forks

Ένα Blockchain Fork (διακλάδωση του blockchain) αποτελεί την διάσπαση της τρέχουσας αλυσίδας σε διάφορα μέρη που ονομάζονται διακλαδώσεις (forks). Οι διακλαδώσεις που προκύπτουν εμπεριέχουν το τρέχων περιεχόμενο της αλυσίδας (από το τρέχων μπλοκ έως πίσω στο αρχικό μπλοκ genesis) και μπορεί να διαφοροποιούνται από αυτήν, ανάλογα με το είδος τους, από εκείνο το σημείο και έπειτα. Υπάρχουν πολλοί λόγοι για την δημιουργία διακλαδώσεων σε ένα blockchain, όπως μια αναβάθμιση που απλώνεται πάνω στο δίκτυο και υιοθετείται από κόμβους σε διαφορετικές ταχύτητες. Αν και οι περισσότερες απόπειρες για διακλάδωση δεν είναι κακόβουλες, πολλές φορές αντιπροσωπεύουν μια ασυνεπή κατάσταση που μπορεί να αξιοποιηθεί για να προκαλέσει σύγχυση, δόλιες συναλλαγές και δυσπιστία εντός του δικτύου.

Υπάρχουν δύο τύποι διακλάδωσης, η σκληρή διακλάδωση (hard fork) και η μαλακή διακλάδωση (soft fork). Μια σκληρή διακλάδωση είναι αυτό που γενικά κατανοούμε ως διακλάδωση του blockchain. Το ένα blockchain διαχωρίζεται και γίνεται ασύμβατο με το άλλο στέλεχος, οδηγώντας σε δύο εντελώς ξεχωριστά νέα blockchain. Αυτό συμβαίνει όταν τα πρόσφατα εισηγμένα μπλοκ στην αλυσίδα, ενώ φαίνεται πως η επικύρωσή τους είναι η σωστή, δεν συμφωνούν με τα νέα μπλοκ (πχ. τα νέα μπλοκ μπορεί να δείχνουν σε άλλα παλαιά μπλοκ). Αυτό σημαίνει ότι οι αλλαγές που εισάγονται στη διακλάδωση δεν είναι συμβατές με τους παλιούς κανόνες του blockchain. Αυτό έχει ως αποτέλεσμα μια μόνιμη διάσπαση. Τόσο η παλιά όσο και η νέα αλυσίδα συνεχίζουν να υπάρχουν ανεξάρτητα και έχουν διαφορετικό ιστορικό συναλλαγών από το σημείο της διακλάδωσης. Οι χρήστες, οι κόμβοι και οι ανθρακωρύχοι στο δίκτυο πρέπει να αναβαθμίσουν σε νέο λογισμικό για να παραμείνουν στη νέα αλυσίδα μπλοκ. Όσοι δεν αναβαθμίσουν, παραμένουν στο παλιό blockchain. Μια σκληρή διακλάδωση γίνεται πραγματικότητα όταν η επαλήθευση κόμβου της παλαιότερης έκδοσης είναι πιο περιοριστική από το νέο σύστημα ή όταν υπάρχουν διαφωνίες μέσα στην κοινότητα του blockchain [27], [28].

Έτσι η σκληρή διακλάδωση είναι μόνιμη και έχει πλήρη απόκλιση από τις προηγούμενες εκδόσεις του blockchain. Οι κόμβοι που εκτελούν τις παλαιότερες εκδόσεις δεν είναι πλέον αποδεκτοί από την πιο πρόσφατη έκδοση. Οι συναλλαγές στη διχαλωτή/νέα αλυσίδα δεν είναι έγκυρες στην παλαιότερη αλυσίδα. Οι κόμβοι και οι ανθρακωρύχοι πρέπει να αναβαθμίσουν την έκδοση λογισμικού τους στην τελευταία, αν θέλουν να βρίσκονται στην διχαλωτή αλυσίδα. Ένα διάσημο παράδειγμα είναι το 2017 Bitcoin Hard Fork, που είχε ως αποτέλεσμα τη δημιουργία ενός νέου κρυπτονομίσματος, το Bitcoin Cash, στην διχαλωτή αλυσίδα. [29]

Μια μαλακή διακλάδωση συμβαίνει με παρόμοιο τρόπο, αλλά αντί τα παλιά μπλοκ να αναγκάζουν την διάσπαση της αλυσίδας, παραμένουν στην ίδια αλυσίδα. Αυτό επιτρέπει στους κόμβους που εκτελούν το νέο λογισμικό να συνεχίσουν να συμμετέχουν στο παλιό δίκτυο χωρίς προβλήματα και άρα οι αναβαθμισμένοι κόμβοι μπορούν να συνυπάρχουν με τους μη αναβαθμισμένους κόμβους στο ίδιο δίκτυο. Η νέα διχαλωτή αλυσίδα θα συνεχίσει να ακολουθεί τους νέους κανόνες τιμώντας τους παλιούς. Η μαλακή διακλάδωση απαιτεί μόνο από την πλειοψηφία των ανθρακωρύχων να αναβαθμίσουν την έκδοσή τους για να επιβάλουν τους νέους κανόνες. Οι χρήστες στο δίκτυο δεν υποχρεούνται να αναβαθμίσουν στο νέο λογισμικό. Όσοι δεν αναβαθμίσουν μπορούν να συνεχίσουν να συμμετέχουν στο δίκτυο, αλλά ενδέχεται να μην είναι σε θέση να χρησιμοποιήσουν τα νέα χαρακτηριστικά που εισάγει η μαλακή διακλάδωση.[29]

Αν συμβεί μια μαλακή διακλάδωση, οι παλιοί κόμβοι μπορούν να ενημερωθούν σταδιακά, έως ότου όλοι οι κόμβοι φτάσουν τελικά στην ίδια κατάσταση και πάλι. Μια μαλακή διακλάδωση συμβαίνει αν οι νεότερες απαιτήσεις κόμβων είναι πιο περιοριστικές από τις παλιές [27], [28].

Για να επιτραπεί η χρήση διακλαδώσεων τακτικά σε λειτουργίες blockchain, είναι πολύ πιθανό ότι το blockchain φτιάχνει νέα μπλοκ με πιθανολογικό τρόπο, όπου πολλαπλοί κόμβοι μπορούν να φέρουν ένα έγκυρο μπλοκ ταυτόχρονα, με αποτέλεσμα μια κατάσταση σύγκρουσης. Συστήματα όπου υπάρχει μόνο μία οντότητα που να παράγει και να προσαρτά νέα μπλοκ δεν θα υποφέρουν από το πρόβλημα της διακλάδωσης υπό κανονικές συνθήκες.

Οι διακλαδώσεις που γίνονται για λόγους αναβάθμισης είναι γενικότερα προγραμματισμένες και συνήθως έχουν ψηφιστεί από την πλειοψηφία των κόμβων του εκάστοτε blockchain. Μια διακλάδωση πάντως μπορεί να δημιουργηθεί και κατά την διάρκεια μιας συνθήκης αγώνα δύο μπλοκ, όπου δύο ανθρακωρύχοι βρίσκουν το nonce ταυτόχρονα και άρα προωθούν το μπλοκ τους ταυτόχρονα για επικύρωση τους στο blockchain. Σε αυτή την περίπτωση, το blockchain διασπάται και μερικοί κόμβοι επικυρώνουν το ένα μπλοκ και μερικοί το άλλο. Στο τέλος, ο μηχανισμός συναίνεσης κρατάει την έγκυρη αλυσίδα και το μπλοκ που δεν μπήκε σε αυτή μένει ως έωλο (4.1.2) έξω από το blockchain. Οπότε θεωρητικά μια διακλάδωση μπορεί να δημιουργηθεί από τον οποιοδήποτε. Οι προϋποθέσεις μιας προγραμματισμένης διακλάδωσης είναι η πρόταση για αλλαγές και βελτιώσεις του δικτύου από κόμβους του και στην συνέχεια η ψηφοφορία με σκοπό η πλειοψηφία να συμφωνεί με αυτές τις αλλαγές.

4.1.2 Έωλα (Stale) και Ορφανά (Orphan) Μπλοκ

Τα έωλα και ορφανά μπλοκ είναι επικυρωμένα μπλοκ που καταλήγουν έξω από το κύριο blockchain. Είναι συνήθως ένα φαινόμενο στα δημόσια blockchain, όπου οι ανθρακωρύχοι προσπαθούν να ξεπεράσουν τους άλλους στη δημιουργία νέων μπλοκ.

Τα έωλα μπλοκ είναι το αποτέλεσμα μιας συνθήκης αγώνα, η οποία συμβαίνει όταν τα μπλοκ δημιουργούνται από δύο ανθρακωρύχους ταυτόχρονα. Καθώς μόνο ένα από αυτά μπορεί να προστεθεί στην αλυσίδα, το άλλο τελειώνει ως μια έωλη επέκταση. Επιπλέον, τονίζεται πως ένα έωλο μπλοκ θα μπορούσε να είναι το προϊόν κακόβουλης συμπεριφοράς. Ένα έωλο μπλοκ συνδέεται συνήθως απευθείας με την κύρια αλυσίδα (δηλ. υπάρχει ένα πιθανότατα τελευταίο μπλοκ στην αλυσίδα στο οποίο το έωλο μπλοκ δείχνει).

Ένα ορφανό μπλοκ έχει το γονικό του έωλο επομένως δεν έχει άμεση σύνδεση επόμενου μπλοκ με το κύριο blockchain. Είναι απολύτως πιθανό ότι ένα ορφανό μπλοκ ξεκίνησε ως μέρος του κανονικού blockchain, αλλά η συναίνεση έσπρωξε το γονικό του έξω για να γίνει έωλο, καθιστώντας το ίδιο το μπλοκ ένα ορφανό μπλοκ. Υπολογιστική δύναμη που δαπανάται σε μπλοκ που γίνονται έωλα ή ορφανά ουσιαστικά χάνεται και συνήθως δεν ανταμείβεται [28].

4.1.3 Αμοιβή για τα Θειικά Μπλοκ (Uncle Blocks)

Οι ανταμοιβές για τα θειικά μπλοκ αναφέρεται ως μια ευπάθεια του μηχανισμού ανταμοιβής του Ethereum που υποκίνησε σε εγωιστική εξόρυξη (δείτε επίθεση στην Ενότητα 4.2.1.2 στα είδη επιθέσεων) [34]. Το Ethereum έχει ένα επιπλέον χαρακτηριστικό ανταμοιβής εκτός των τακτικών ανταμοιβών μπλοκ, που ονομάζονται uncle and nephew (θείος και ανιψιός) ανταμοιβές.

Ένα θειικό μπλοκ είναι ένα έωλο μπλοκ έξω από την κύρια αλυσίδα, το οποίο αναφέρεται απευθείας σε ένα κανονικό μπλοκ στην αλυσίδα. Με άλλα λόγια, τα έωλα μπλοκ, που βρίσκονται πιο κοντά στην κύρια αλυσίδα, μπορούν να γίνουν θειικά μπλοκ. Αν ένα μελλοντικό μπλοκ αρχίζει να αναφέρεται σε αυτό το έωλο θειικό μπλοκ, το νέο μπλοκ στη συνέχεια ονομάζεται ένα μπλοκ ανιψιός (nephew block) και ο δημιουργός του θειικού μπλοκ παίρνει την θειική ανταμοιβή (uncle reward). Το ποσό που επιβραβεύεται καθορίζεται από την απόσταση μεταξύ του θείου και του ανιψιού. Ένας θείος μπορεί να κερδίσει μέχρι 7/8 από το ποσό της ανταμοιβής ενός κανονικού μπλοκ ενώ οι ανιψιοί θα κερδίζουν πάντα το 1/32 [35].

Καθώς τα θειικά μπλοκ είναι μοναδικά στο Ethereum, δεν υπάρχει απειλή για άλλες λύσεις blockchain που δεν χρησιμοποιούν αυτό το σύστημα ανταμοιβής. Στο Bitcoin, δεν υπάρχει μηχανισμός ανταμοιβής για τα έωλα μπλοκ και ο σταθερός ρυθμός μπλοκ είναι 0,41%. Το Ethereum από την άλλη πλευρά με το μηχανισμό του θείου μπλοκ έχει σταθερό ποσοστό μπλοκ 6,8%. Ο μηχανισμός αυτός μειώνει τη συνολική ασφάλεια του blockchain, καθώς χάνει τη σταθερότητα λόγω της ποσότητας των έωλων μπλοκ που πρέπει να χειριστεί. Ειδικότερα, κάθε εγωιστής ανθρακωρύχος μπορεί να παράγει μια αφθονία μπλοκ στην ελπίδα για κέρδος [30] [36].

4.1.4 Τρωτά Σημεία Βασικών Μηχανισμών Συναίνεσης

4.1.4.1 Τρωτά Σημεία Απόδειξης Εργασίας (PoW)

Το PoW είναι ένας κοινά χρησιμοποιούμενος μηχανισμός συναίνεσης στα δημόσια blockchain. Οι ανθρακωρύχοι πρέπει να καταβάλλουν προσπάθεια (εργασίας) για την παροχή μαθηματικής απόδειξης κατά τη διάρκεια της δημιουργίας ενός νέου έγκυρου μπλοκ.

Τα blockchain που υπάρχουν για μεγάλο χρονικό διάστημα, παρουσιάζουν αύξηση της αθροιστικής ισχύος κατακερματισμού στο δίκτυο. Αυτό σημαίνει ότι οι υπολογιστικοί κατακερματισμοί γίνονται όλο και πιο ακριβοί στον κάθε ανθρακωρύχο καθώς το επίπεδο της δυσκολίας αυξάνεται.

Επιπλέον, ο υπολογισμός κατακερματισμού έχει συνήθως ένα στενό χρονικό πλαίσιο μέχρι να ολοκληρωθεί, το οποίο θα μπορούσε να καταστήσει δύσκολο για κάποιον ανθρακωρύχο να μπει στην διαδικασία. Εφόσον οι ανταμοιβές για αυτές τις προσπάθειες συνήθως δίνονται μόνο σε όσους δημιουργούν πραγματικά το νέο επικυρωμένο μπλοκ, αυτό σημαίνει ότι όλοι οι άλλοι ανθρακωρύχοι δεν θα ανταμειφθούν για τις προσπάθειες που δαπανήθηκαν.

Για να αντιμετωπίσουν αυτό το πρόβλημα, οι ανθρακωρύχοι άρχισαν να αυξάνουν τους ρυθμούς κατακερματισμού με τη χρήση εξειδικευμένου υλικού. Όλα αυτά οδηγούν στη σπατάλη μεγάλων ποσοτήτων ενέργειας χωρίς αποτέλεσμα.

Ένα άλλο μέτρο για την αντιμετώπιση της δαπανηρής διαδικασίας κατακερματισμού είναι οι πισίνες εξόρυξης. Στις λεγόμενες αυτές πισίνες, οι ανθρακωρύχοι συγκεντρώνουν την υπολογιστική δύναμή τους, κάτι που τους οδηγεί στο να «κατέχουν» όλοι μαζί ορισμένα τμήματα του δικτύου, καθώς λειτουργούν σαν ένας ανθρακωρύχος με πολύ μεγάλη δύναμη εξόρυξης. Τα κέρδη μεταξύ των ανθρακωρύχων σε μια πισίνα εξόρυξης μοιράζονται ανάλογα με την υπολογιστική δύναμη που προσθέτει ο κάθε ανθρακωρύχος στην πισίνα εξόρυξης. Αν αυτές οι πισίνες γίνουν πολύ μεγάλες, θα μπορούσαν να χρησιμοποιηθούν ως μέσο για πιθανές επιθέσεις, όπως επιθέσεις κατά πλειοψηφία (majority attacks) (δείτε Ενότητα 4.2.1.1 στα είδη επιθέσεων) και διπλές δαπάνες (double spending) (δείτε Ενότητα 4.2.2.1 στα είδη επιθέσεων). [28] [30]

4.1.4.2 Τρωτά Σημεία Απόδειξης Συμμετοχής (PoS)

Η απόδειξη συμμετοχής (PoS) εισήχθη για να ξεπεραστούν τα προφανή προβλήματα της απόδειξης εργασίας (PoW). Η κατανάλωση ενέργειας μειώνεται, γεγονός που την καθιστά πιο βιώσιμη λύση. Επιπλέον, αυξάνονται τα όρια για επιθέσεις κατά πλειοψηφία (majority attacks).

Ενώ η απόδειξη εργασίας χρησιμοποιεί μια πιθανολογική προσέγγιση, όπου οι ανθρακωρύχοι εγκρίνονται «τυχαία», η απόδειξη συμμετοχής χρησιμοποιεί μια ντετερμινιστική προσέγγιση. Οι επικυρωτές (validators) επιλέγονται με τη χρήση μιας διεργασίας που ονομάζεται bidding, δηλαδή υποβολή προσφοράς. Εκεί θα πρέπει να υποβάλουν τις προσφορές τους, που είναι το υπόλοιπο τους σε νομίσματα, και ο υποψήφιος με το μεγαλύτερο μερίδιο (stake) επιλέγεται να είναι ο επόμενος επικυρωτής.

Η κακόβουλη συμπεριφορά θα οδηγήσει στην απώλεια του μεριδίου. Το PoS είναι πιο ανθεκτικό στις επιθέσεις κατά πλειοψηφία από ό,τι το PoW. Δεν είναι πλέον η υπολογιστική δύναμη του δικτύου, αλλά αντίθετα ο επιτιθέμενος θα πρέπει να έχει εκ των προτέρων στην κατοχή του το μισό από το υπόλοιπο από τα μερίδια, για να ξεκινήσει την επίθεση.

Από την άλλη πλευρά, το μειονέκτημα της απόδειξης συμμετοχής είναι ότι οι πλούσιοι επικυρωτές συνεχίζουν να κερδίζουν την προσφορά, η οποία με τη σειρά της τους δίνει την ανταμοιβή μπλοκ, οδηγώντας σε μερικούς επικυρωτές να γίνονται πλουσιότεροι κάθε φορά, ενώ οι νέοι υποψήφιοι δεν έχουν σχεδόν καμία πιθανότητα να κερδίσουν μια προσφορά. Αυτό με τη

σειρά του οδηγεί σε ένα ψευδο-κεντρικό σύστημα και ανατρέπει τον σκοπό ενός αποκεντρωμένου δημόσιου blockchain [28] [31] [32].

Επιπλέον, υπάρχει το πρόβλημα του "Nothing-at-Stake". Οι επικυρωτές PoS δεν χρειάζεται να καταναλώνουν υπολογιστική ισχύ όπως οι ανθρακωρύχοι στο PoW, καθιστώντας ευκολότερη την ταυτόχρονη επικύρωση πολλαπλών μπλοκ και άρα την δημιουργία διακλαδώσεων. Αυτό δημιουργεί το πρόβλημα "nothing-at-stake", όπου οι επικυρωτές δεν έχουν κανένα αντικίνητρο να επικυρώσουν πολλαπλές εκδόσεις του blockchain, δηλαδή διακλαδώσεις που δεν είναι η κύρια αλυσίδα του blockchain. Μάλιστα η πολλαπλή επικύρωση δεν σχετίζεται με κάποιο υπολογιστικό κόστος για τους επικυρωτές, καθιστώντας εν τέλει τη συναίνεση ασθενέστερη.

4.1.4.3 Τρωτά Σημεία Delegated Proof of Stake (DPoS)

Το Delegated Proof of Stake (DPoS) είναι μια παραλλαγή του PoS που στοχεύει στην επίτευξη ισορροπίας μεταξύ αποκέντρωσης και επεκτασιμότητας. Το DPoS βασίζεται σε εκλεγμένους αντιπροσώπους, συχνά έναν μικρό αριθμό αξιόπιστων ατόμων ή οντοτήτων, για την επικύρωση συναλλαγών και τη δημιουργία μπλοκ. Ενώ προσφέρει επεκτασιμότητα, συνοδεύεται από το δικό του σύνολο ευπαθειών.

Χειραγώγηση ψηφοφορίας: Τα συστήματα DPoS βασίζονται στη δημοκρατική διαδικασία της ψηφοφορίας για την επιλογή των αντιπροσώπων. Εάν ένας επιτιθέμενος μπορεί να συγκεντρώσει αρκετή δύναμη ψήφου, μπορεί να ελέγξει αποτελεσματικά το δίκτυο επιλέγοντας κακόβουλους αντιπροσώπους. Αυτό θέτει σε κίνδυνο την ακεραιότητα του blockchain και συγκεντρώνει την εξουσία σε λίγες οντότητες.

Δωροδοκία: Οι επιτιθέμενοι μπορεί να επιχειρήσουν να δωροδοκήσουν αντιπροσώπους για να αποκτήσουν τον έλεγχο του δικτύου. Αυτό εισάγει τον κίνδυνο συνεννόησης και διαφθοράς στο σύστημα DPoS, υπονομεύοντας την αξιοπιστία του.

Συμβιβασμοί: Το DPoS εισάγει συμβιβασμούς μεταξύ αποκέντρωσης και αποτελεσματικότητας. Ενώ μπορεί να επεξεργάζεται γρήγορα τις συναλλαγές, η εξάρτηση από έναν περιορισμένο αριθμό αντιπροσώπων μπορεί να θέσει σε κίνδυνο την αξιοπιστία του δικτύου. [98]

4.1.4.4 Τρωτά Σημεία Practical Byzantine Fault Tolerance (PBFT)

Το Πρακτικό Βυζαντινό Πρωτόκολλο Ανοχής Σφαλμάτων (PBFT) χρησιμοποιείται περισσότερο σε ιδιωτικά εγκεκριμένα blockchain. Σε αυτό το αξιόπιστο περιβάλλον, το δίκτυο είναι ομαδοποιημένο σε ενεργητικές και παθητικές αντιγραφές (replicas). Οι ενεργές αντιγραφές είναι αυτές που συμμετέχουν ενεργά στο πρωτόκολλο συναίνεσης. Διαδραματίζουν δυναμικό και κρίσιμο ρόλο στη διαδικασία συναίνεσης, προτείνοντας μπλοκ, επικυρώνοντας μπλοκ που προτείνονται από τους πρωτεύοντες κόμβους και ψηφίζοντας μια αντιγραφή που αναλαμβάνει τον ρόλο του πρωτεύον κόμβου, ο οποίος προτείνει ένα νέο μπλοκ ή δέσμη συναλλαγών στα άλλα αντίγραφα του δικτύου. Γενικά οι ενεργές αντιγραφές συμμετέχουν άμεσα στην επίτευξη συναίνεσης συμβάλλοντας στη διαδικασία λήψης αποφάσεων.

Οι παθητικές αντιγραφές, από την άλλη πλευρά, δεν συμμετέχουν ενεργά στο πρωτόκολλο συναίνεσης. Χρησιμεύουν κυρίως ως εφεδρικές αντιγραφές των ενεργών και χρησιμοποιούνται συχνά για τη διατήρηση της διαθεσιμότητας και του πλεονασμού του συστήματος. Ενώ οι παθητικές αντιγραφές δεν συμμετέχουν στην πρόταση μπλοκ ή στην ψηφοφορία στη διαδικασία συναίνεσης, διατηρούν ένα αντίγραφο του blockchain και μπορούν να παρέμβουν για να αντικαταστήσουν ένα ενεργό αντίγραφο σε περίπτωση που αυτό καταστεί ελαττωματικό ή συμπεριφερθεί κακόβουλα.

Από όλες τις ενεργές ρέπλικες, επιλέγεται μία ως πρωτεύων κόμβος. Αυτός ο κόμβος είναι αυτός που λαμβάνει όλες τις συναλλαγές και τις σπρώχνει έξω στις ενεργές ρέπλικες, ώστε να μπορούν να υπογράψουν τις συναλλαγές και να τις μοιραστούν με όλες τις άλλες αντιγραφές. Τα αποτελέσματα στη συνέχεια μεταδίδονται πίσω στον πρωτεύοντα κόμβο, ο οποίος τα συλλέγει και φτιάχνει ένα νέο μπλοκ με όλες τις υπογεγραμμένες συναλλαγές. Αυτό το νέο μπλοκ μεταδίδεται στη συνέχεια μέσω του δικτύου.

Ολόκληρο το πρωτόκολλο βασίζεται στο γεγονός ότι ο πρωτεύων κόμβος είναι αξιόπιστος και δεν τίθεται σε κίνδυνο. Υπάρχει ένας αριθμός ενεργειών που μπορεί να πραγματοποιήσει μια ρέπλικα του πρωτεύον κόμβου που είναι εκτεθειμένη, όπως η απόρριψη ορθών εγκρίσεων και διακοπή της εκτέλεσης της συναλλαγής, ανάμειξη με την εντολή συναλλαγής για την ενεργή δημιουργία καθυστέρησης σε ολόκληρη τη διαδικασία δημιουργίας μπλοκ, απόκρυψη μπλοκ και συναλλαγών καθώς και πλαστογράφηση εγκρίσεων συναλλαγής.

Τα μέλη σε ένα ιδιωτικό δίκτυο blockchain είναι συνήθως γνωστά και ως εκ τούτου είναι σχετικά εύκολο να εντοπιστούν κακόβουλες δραστηριότητες σε ορισμένα μέλη. Ωστόσο, αν προκληθεί βλάβη, ο εντοπισμός του κακόβουλου μέλους είναι απλώς ένα αντιδραστικό ή διορθωτικό μέτρο.

Μια άλλη αδυναμία του PBFT είναι η επεκτασιμότητα. Τα μεγαλύτερα δίκτυα θα υποστούν επιβάρυνση από την επικοινωνία μεταξύ των ρεπλίκων και οι επιδόσεις θα μειωθούν. Μία από τις βασικές αδυναμίες του PBFT είναι ότι έχει συγκριτικά μικρή ανοχή στους κακόβουλους κόμβους του δικτύου με μόλις 33% σε σύγκριση με το 50% του PoW και του PoS. Αυτή η χαμηλή ανοχή σφαλμάτων είναι ένα σημαντικό πρόβλημα, ειδικότερα δεδομένου ότι τα ιδιωτικά δίκτυα είναι συνήθως πολύ μικρότερα σε μέγεθος από τα δημόσια δίκτυα, γεγονός που μειώνει επιπλέον τον πραγματικό αριθμό των κόμβων που απαιτούνται [28] [33].

4.2 Είδη Επιθέσεων Blockchain

Ο χωρισμός των ειδών επιθέσεων στο Blockchain χωρίζεται ως εξής:

- Επιθέσεις στον Μηχανισμό Συναίνεσης
- Επιθέσεις στην Συναλλαγή
- Επιθέσεις στο Ομότιμο Σύστημα
- Επιθέσεις σε Έξυπνα Συμβόλαια
- Κλασικές Επιθέσεις Ασφάλειας

Όλα τα προαναφερόμενα είδη επιθέσεων αναλύονται στις ακόλουθες υπο-ενότητες της Ενότητας 4.2.

4.2.1 Επιθέσεις στον Μηχανισμό Συναίνεσης

4.2.1.1 51% Επίθεση

Η 51% επίθεση, γνωστή και ως πειρατεία συναίνεσης (consensus hijacking), αποτελεί επίθεση στον αλγόριθμο συναίνεσης μιας εφαρμογής blockchain. Ο επιτιθέμενος επιχειρεί να καταλάβει το δίκτυο ελέγχοντας την πλειοψηφία των κόμβων, ή περισσότερο από το 50% της συνολικής υπολογιστικής ισχύος στο δίκτυο. Βασικά αυτή η επίθεση μπορεί να επιτευχθεί όταν ένας μόνο εισβολέας, μια ομάδα κόμβων Sybil (δείτε Ενότητα 4.2.3.2), ή μια δεξαμενή εξόρυξης στο δίκτυο επιτυγχάνει την πλειοψηφία του ποσοστού κατακερματισμού του δικτύου για να χειριστεί το Blockchain [28]. Με το μεγαλύτερο ποσοστό κατακερματισμού του δικτύου, οι επιτιθέμενοι είναι σε θέση [37]:

- Να αποτρέψουν την επαλήθευση συναλλαγών ή μπλοκ (καθιστώντας τα έτσι άκυρα)
- Να αντιστρέψουν συναλλαγές που ελέγχουν κατά τη διάρκεια του χρόνου για να επιτρέψουν τη διπλή δαπάνη (double spending) (δείτε Ενότητα 4.2.2.1)
- Να διακλαδώσουν (fork) το κύριο blockchain και να διαιρέσουν το δίκτυο
- Να αποτρέψουν άλλους ανθρακωρύχους (ελεγκτές) από την εύρεση οποιονδήποτε μπλοκ για ένα σύντομο χρονικό διάστημα.
- Υπό συνθήκες αγώνα (race), οι επιτιθέμενοι με πάνω από 50% ποσοστό κατακερματισμού είναι εγγυημένο πως θα προσπεράσουν άλλους ανθρακωρύχους και θα προσαρτήσουν το δικό τους μπλοκ με μεγάλη πιθανότητα.

Τα ειδικά χαρακτηριστικά μιας τέτοιας επίθεσης εξαρτώνται σε μεγάλο βαθμό από τον εφαρμοζόμενο αλγόριθμο συναίνεσης και τον τύπο του blockchain. Η πλειοψηφική "εξαγορά" ενός δικτύου blockchain, ακόμη και αν ήταν μόνο για ένα μικρό χρονικό διάστημα, θα μπορούσε να χρησιμοποιηθεί από τον επιτιθέμενο για να επιτύχει πιο εξελιγμένους στόχους και να επιτρέψει μια ποικιλία από άλλες επιθέσεις, όπως η διπλή δαπάνη. Η 51% επίθεση μπορεί να αποτελέσει κρίσιμη απειλή για την ακεραιότητα και τη διαθεσιμότητα. [27] [38].

Στα επιτρεπόμενα blockchain (permissioned blockchain), η κατάσταση απειλής όσον αφορά τις 51% επιθέσεις είναι διαφορετική [10], καθώς υπάρχει ένα αυξημένο επίπεδο εμπιστοσύνης μεταξύ των μελών με βάση το εμπόδιο της πιστοποίησης. Επίσης, υπάρχει περιορισμένη πρόσβαση στο δίκτυο και γενικότερα στο blockchain. Με την κεντρική αρχή να χορηγεί άδειες, αυτό το είδος επίθεσης είναι πιο ρεαλιστικό να αποτελεί απειλή εκ των έσω, όπου μια κεντρική αρχή θα μπορούσε να αναλάβει και να ελέγξει το blockchain.

Η κύρια απειλή των 51% επιθέσεων προέρχεται από δημόσια, χωρίς άδειες blockchain (permissionless blockchains) που χρησιμοποιούν Proof-of-X μηχανισμούς συναίνεσης [34], καθώς δεν υπάρχει ρυθμιστική ή ελεγκτική αρχή και κάθε αντίπαλος είναι άγνωστος ο ένας στον άλλο.

Στα blockchain με απόδειξη της εργασίας (PoW) [39], πολλές φορές οι ανθρακωρύχοι θέλουν να ενωθούν για να εξορύξουν περισσότερα μπλοκ ταυτόχρονα και έτσι δημιουργούν μια «πισίνα εξόρυξης», που είναι μια συγκεντρωμένη ομάδα ανθρακωρύχων με πολύ υψηλή υπολογιστική δύναμη. Εάν επιτύχουν το 51% της υπολογιστικής ισχύος, θα μπορούσαν να πάρουν τον έλεγχο ολόκληρου του blockchain. Αυτό γίνεται γιατί αν κάποιος αποκτήσει περισσότερο από το 51% της υπολογιστικής ισχύς, θα μπορέσει να βρει την τιμή Nonce γρηγορότερα από τους άλλους, πράγμα που σημαίνει ότι έχει την εξουσία να αποφασίζει για τα επιτρεπόμενα μπλοκ. Αυτό επιτρέπει και τις προαναφερθέντες επιθέσεις.

Τα προαπαιτούμενα μιας επίθεσης 51% ποικίλλουν ανάλογα με την επηρεαζόμενη δομή blockchain, τους χρησιμοποιημένους αλγορίθμους συναίνεσης και τα πρωτόκολλα:

- PoW: περισσότερο από το 50% της ακατέργαστης υπολογιστικής ισχύος του δικτύου.
- PoS: πάνω από το 50% του δεσμευμένου μεριδίου.
- DPoS: πάνω από το 50% των αντιπροσώπων.
- PoI: πάνω από το 50% του συνολικού σκορ φήμης του δικτύου. Δηλαδή των κόμβων με το μεγαλύτερο σκορ φήμης.
- PoC: περισσότερο από το 50% της συνολικής χωρητικότητας αποθήκευσης.
- PBFT: πάνω από το 33% όλων των ρεπλικών θεωρητικά για την εισροή του δικτύου, στην πράξη αρκεί να αναλάβει τον μοναδικό πρωτεύοντα κόμβο.

Πάντως, όταν το σύνολο των καλών κόμβων ελέγχει τουλάχιστον το 51% της ισχύος εξόρυξης του δικτύου, ένα blockchain μπορεί τότε να θεωρηθεί προστατευμένο από τέτοιου είδους επιθέσεις. Σε αυτήν την περίπτωση, το κόστος ελέγχου ενός σημαντικού ποσοστού του δικτύου θα μπορούσε να είναι μεγαλύτερο από το κόστος απόκτησης σημαντικής ισχύος εξόρυξης, αυξάνοντας έτσι το κόστος των επιθέσεων.

Τον Ιανουάριο του 2014 [29] η δεξαμενή εξόρυξης "ghash.io" έφτασε το 42% της συνολικής υπολογιστικής ισχύος του Bitcoin, ενώ τον Ιούνιο του 2014 το hashrate της ίδιας δεξαμενής εξόρυξης κυμαινόταν μεταξύ 40% και 50% της συνολικής ισχύος του δικτύου κατά τη διάρκεια μιας εβδομάδας. Αυτό ανάγκασε ορισμένους ανθρακωρύχους να εγκαταλείψουν οικειοθελώς τη δεξαμενή εξόρυξης "ghash.io" για να μειώσουν την υπολογιστική ισχύ και να εξαλείψουν το φόβο της επίθεσης 51%.

Μακράν το πιο διαβόητο παράδειγμα 51% επίθεσης έγινε στο Bitcoin Gold (σκληρή διακλάδωση-hard fork του Bitcoin), το οποίο πραγματοποιήθηκε μεταξύ 16 και 19 Μαΐου 2018 [66]. Οι επιτιθέμενοι αφού απέκτησαν πάνω από το 51% της κατακερματικής δύναμης του δικτύου, άρχισαν να κάνουν διπλές δαπάνες σε ανταλλακτήρια και απέσπασαν κρυπτονομίσματα αξίας 18 εκατομμυρίων δολαρίων. Αυτό ήταν καταστροφικό για το hard fork του Bitcoin και οδήγησε στη

διαγραφή του από τα εν λόγω ανταλλακτήρια, τα οποία ήταν δικαιολογημένως απογοητευμένα με το αποτέλεσμα.

4.2.1.2 Επίθεση Εγωιστικής Εξόρυξης (Selfish Mining Attack)

Ένα blockchain στο οποίο τα νέα μπλοκ του δημιουργούνται από ανθρακωρύχους, είναι ευάλωτο σε εγωιστικές επιθέσεις εξόρυξης. Κατά την κανονική διαδικασία εξόρυξης, ένα νέο μπλοκ προσαρτάται μόλις παραχθεί.

Ένας εγωιστής ανθρακωρύχος, όμως, θέλει να παράγει όσο το δυνατόν περισσότερα έσοδα ανταμοιβής με την εξόρυξη νέων μπλοκ χωρίς να ενημερώνει την κύρια αλυσίδα. Αυτά τα σιωπηλά δημιουργημένα μπλοκ στο προσωπικό "micro blockchain" του εγωιστή ανθρακωρύχου στη συνέχεια απελευθερώνονται όλα μαζί, γεγονός που κάνει τον εγωιστή ανθρακωρύχο να κερδίσει τους άλλους ανθρακωρύχους. Αυτό θα είχε ως αποτέλεσμα τα νέα του μπλοκ να γίνουν αποδεκτά πάνω από αυτά που άλλοι ανθρακωρύχοι δημιουργούν στο blockchain. Έτσι υφίσταται η απώλεια των προηγουμένως εξορυσσόμενων μπλοκ από άλλους ανθρακωρύχους για αυτήν τη διάρκεια. Αυτό περιγράφεται επίσης ως κούρσα μπλοκ (block race), στην οποία τα δύο μέρη, έντιμοι και εγωιστές ανθρακωρύχοι, προσπαθούν να είναι αυτοί που θα επιβάλλουν τα νέα έγκυρα μπλοκ. Παρακάτω αναλύουμε περισσότερο αυτό το είδος επίθεσης για να γίνει πιο κατανοητό.

Ο επιτιθέμενος, λοιπόν, κρατά τα μπλοκ που ανακαλύφθηκαν ιδιωτικά και στη συνέχεια προσπαθεί να δημιουργήσει μια δική του ιδιωτική αλυσίδα/διακλάδωση, συνεχίζοντας την εξόρυξη πάνω σε αυτά. Έπειτα, ο εγωιστής ανθρακωρύχος θα εξορύσσει σε αυτήν την ιδιωτική αλυσίδα και θα προσπαθήσει να διατηρήσει ένα μεγαλύτερο ιδιωτικό τμήμα από το δημόσιο. Εν τω μεταξύ, οι τίμιοι ανθρακωρύχοι συνεχίζουν την εξόρυξη στη δημόσια αλυσίδα. Νέα μπλοκ που εξορύσσονται από τον επιτιθέμενο θα αποκαλυφθούν όταν το δημόσιο παράρτημα προσεγγίσει το μήκος του ιδιωτικού, έτσι ώστε οι έντιμοι ανθρακωρύχοι να καταλήξουν να χάνουν υπολογιστική ισχύ και να μην κερδίζουν ανταμοιβή, επειδή οι εγωιστές ανθρακωρύχοι δημοσιεύουν τα νέα τους μπλοκ λίγο πριν τους έντιμους. Ως αποτέλεσμα, ο εγωιστής ανθρακωρύχος αποκτά ανταγωνιστικό πλεονέκτημα και οι τίμιοι ανθρακωρύχοι θα ενθαρρυνθούν να ενταχθούν στο υποκατάστημα που διατηρείται από εγωιστές ανθρακωρύχους. Μέσω της περαιτέρω εδραίωσης της εξορυκτικής δύναμης υπέρ του επιτιθέμενου, αυτή η επίθεση υπονομεύει τη φύση της αποκέντρωσης του blockchain [44].

Η επιτυχία ενός εγωιστή ανθρακωρύχου μπορεί να βελτιωθεί σημαντικά με την αύξηση της χρησιμοποιούμενης υπολογιστικής ισχύος. Σε αυτή την περίπτωση, οι τίμιοι ανθρακωρύχοι μπορούν να στερηθούν αυτό που θα ήταν η ανταμοιβή τους. Επιπλέον, η υπολογιστική ισχύς που δαπανάται χάνεται και ο αριθμός των έωλων μπλοκ (ένα άλλο πρόβλημα στο blockchain), αυξάνεται. Αν δύο ή περισσότεροι εγωιστές ανθρακωρύχοι ανταγωνίζονται ιδιωτικά τα συσσωρευμένα μπλοκ τους, αυτό θα οδηγήσει πιθανώς σε μια μεγαλύτερη διακλάδωση, το οποίο θα καθυστερήσει ολόκληρο το δίκτυο και θα ανοίξει την πόρτα για μια σειρά από περαιτέρω επιθέσεις [28], [45].

Για να διεξαχθεί μια εγωιστική εξόρυξη, ένας επιτιθέμενος πρέπει να είναι σε θέση να σφυρηλατήσει νέα μπλοκ σε ένα ταχύτερο ρυθμό από ό, τι οι άλλοι κόμβοι. Αυτό γίνεται συνήθως με το συνδυασμό δύναμης κατακερματισμού σε μια πισίνα εξόρυξης. Για τα ιδιωτικά blockchain, ο επιτιθέμενος πρέπει συνήθως να αναλάβει ή να επηρεάσει τον κύριο/πρωτεύοντα κόμβο του δικτύου για να είναι επιτυχής.

Είναι σημαντικό να σημειωθεί ότι οι πρακτικές περιπτώσεις επιτυχημένων επιθέσεων εγωιστικής εξόρυξης είναι δύσκολο να εντοπιστούν λόγω της πολύπλοκης φύσης αυτών των επιθέσεων, οι οποίες καθιστούν δύσκολο να ελεγχθεί αν πρόκειται για κανονική ή κακόβουλη δραστηριότητα.

4.2.1.3 Επίθεση από Μακριά (Attack from afar ή Long-Range)

Σε ένα σύστημα απόδειξης συμμετοχής (PoS), ένας επιτιθέμενος με αρκετή υπολογιστική ισχύ μπορεί να προσπαθήσει να οικοδομήσει ένα εναλλακτικό blockchain, ξεκινώντας από το πρώτο μπλοκ (μπλοκ γένεσης). Κατά κάποιο τρόπο, οι επιθέσεις από μακριά στα πρωτόκολλα PoS σχετίζονται με τις επιθέσεις εγωιστικής εξόρυξης των πρωτοκόλλων PoW, καθώς ο επιτιθέμενος και στις δύο περιπτώσεις προσθέτει μπλοκ που κρατά κρυφά. Είναι προφανές ότι οι επιθέσεις εγωιστικής εξόρυξης δεν μπορούν να επιστρέψουν στο μπλοκ γένεσης των πρωτοκόλλων PoW, καθώς η υπολογιστική προσπάθεια που απαιτείται είναι απαγορευτική.

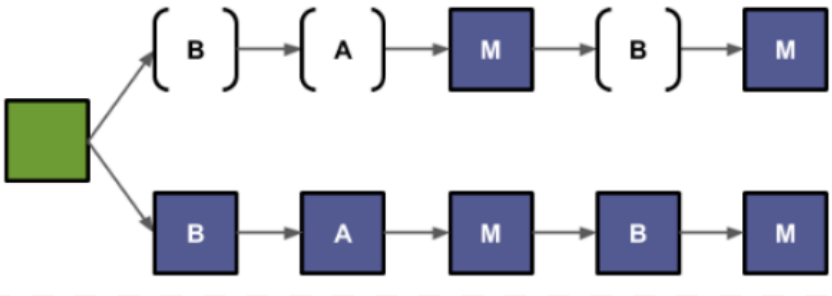
Μια επίθεση από μακριά (Long-Range) είναι ένα σενάριο επίθεσης όπου ο επιτιθέμενος πηγαίνει πίσω στο μπλοκ γένεσης και διακλαδώνει το blockchain [40]. Η νέα διακλάδωση έχει ένα μερικώς ή και εντελώς διαφορετικό ιστορικό από την κύρια αλυσίδα. Η επίθεση πετυχαίνει όταν η διακλάδωση που είναι κατασκευασμένη από τον επιτιθέμενο γίνεται μεγαλύτερη από την κύρια αλυσίδα, και ως εκ τούτου την ξεπερνά. Οι επιθέσεις από μακριά εμπίπτουν σε τρεις διαφορετικές κατηγορίες: Απλή, Μεταγενέστερη Διαφθορά (Posterior Corruption) και Αιμορραγία μεριδίου (Stake Bleeding).

Σε απλές επιθέσεις, εξετάζουμε μια αφελή εφαρμογή του πρωτοκόλλου PoS, στο οποίο οι κόμβοι δεν ελέγχουν τις χρονικές σφραγίδες των μπλοκ. Συνεπώς, όταν εκτελείται το πρωτόκολλο PoS, κάθε επικυρωτής θα έχει τη δυνατότητα να επικυρώσει το μπλοκ του (για τις αλυσίδες που είναι εν γνώση του).

Παράδειγμα Απλής Επίθεσης από μακριά:

Θα θεωρήσουμε μια πισίνα με 3 επικυρωτές (validators), τους A,B και M, όπου ο καθένας έχει το 1/3 του μεριδίου του δικτύου.

Όταν ο M ξεκινήσει την επίθεση από μακριά, θα δημιουργήσει ένα εναλλακτικό κλάδο του blockchain, ξεκινώντας τη διακλάδωση από το μπλοκ γένεσης και εισάγοντας διαφορετικές συναλλαγές.



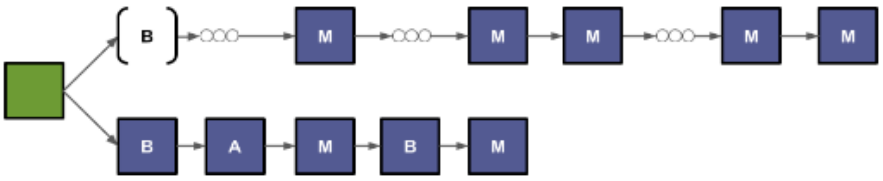
Εικόνα 4. Αρχή Απλής Επίθεσης από Μακριά

Όπως φαίνεται, έχουμε ένα snapshot του blockchain μέχρι ένα σημείο για να δείξει πως θα είναι η διαφορά των δύο κλάδων. Ο κάτω κλάδος είναι ο κύριος, και ο πάνω είναι του M. Ο M έχει την ίδια πιθανότητα να εκλεγεί και στους 2 κλάδους. Τα μπλοκ με παρένθεση είναι τα μπλοκ που

χάνονται καθώς παρόλο που μπορεί να εκλέγονται οι επικυρωτές Α και Β για επικυρωτές μπλοκ, δεν γνωρίζουν για αυτή την αλυσίδα. Άρα το μήκος της πάνω είναι μικρότερο (2 μπλοκ πάνω και 5 κάτω).

Επειδή η πληροφορία του επικυρωτή βρίσκεται στο μπλοκ γένεσης, ο Μ δεν θα μπορεί να παράγει μπλοκ γρηγορότερα από την κύρια αλυσίδα και έτσι θα τα δημιουργεί με τον ίδιο ρυθμό. Για να προσπεράσει, όμως, ο κλάδος του Μ την κύρια αλυσίδα, θα πρέπει να παράγει μπλοκ πιο γρήγορα.

Για αυτό το σκοπό, ο Μ θα πρέπει να πλαστογραφήσει χρονοσφραγίδες (timestamps). Αφού ο Μ είναι ο μόνος ενεργός stakeholder στον κλάδο που διακλάδωσε, μπορεί να τις διαχειριστεί όπως θέλει. Έτσι, σε υλοποιήσεις που οι κόμβοι δεν λαμβάνουν υπόψη χρονοσφραγίδες, και οι 2 κλάδοι θα είναι έγκυροι και έτσι οι κόμβοι δεν θα εντοπίσουν την πλαστογραφία του Μ.



Εικόνα 5. Συνέχεια Απλής Επίθεσης από Μακριά

Με τις τριπλές τελείες φαίνονται πολλαπλά παρατημένα μπλοκ. Στην προσπάθεια του Μ να ανταγωνιστεί την κύρια αλυσίδα, φτιάχνει πιο γρήγορα μπλοκ. Στην Εικόνα 5. φαίνεται ότι οι 2 αλυσίδες έχουν το ίδιο μήκος αλλά στην αλυσίδα του Μ, όλα τα μπλοκ ανήκουν στον Μ.

Στην μεταγενέστερη διαφθορά (posterior corruption), έχουμε το σενάριο όπου ο Μ δεν μπορεί να πλαστογραφήσει τις χρονικές σφραγίδες των μπλοκ. Για να αλλάξει το ιστορικό της κύριας αλυσίδας, πρέπει να δημιουργήσει ένα μεγαλύτερο αριθμό δημιουργούμενων (minted) μπλοκ παράλληλα με την κύρια αλυσίδα. Ωστόσο δεσμεύεται από το γεγονός ότι έχει μια σταθερή πιθανότητα να παράγει μπλοκ.

Για να αυξήσει τις πιθανότητές του να ανταγωνιστεί με την κύρια αλυσίδα, θα πρέπει να είναι σε θέση να πλαστογραφήσει τα μπλοκ ενός άλλου επικυρωτή. Αν, για παράδειγμα, ο Β συμφωνεί να επιτεθεί στην κύρια αλυσίδα, τότε η επίθεση είναι μάλλον ξεκάθαρη, καθώς και οι δύο θα είχαν πολύ περισσότερο από το 50% του μεριδίου. Ωστόσο, αυτό δεν συμβαίνει απαραίτητα.

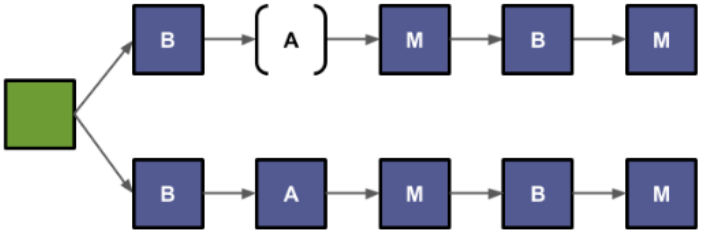
Οι επικυρωτές πρέπει να εναλλάσσονται για να έχουν ένα δίκαιο σύστημα όπως επίσης θα πρέπει να έχουν τη δυνατότητα να αποσυρθούν. Μάλιστα το σύστημα θα πρέπει να τους εναλλάσσει ή να τους αφαιρεί υπό ορισμένες συνθήκες, όπως μια καθορισμένη χρονική περίοδο ή μια ανέντιμη συμπεριφορά.

Για λόγους απλότητας, θεωρούμε ότι ο Β αποφασίζει να αποσυρθεί, αφού επικυρώσει τα πρώτα *n* μπλοκ της κύριας αλυσίδας. Ο Β αφαιρεί το μερίδιο του, βγάζει χρήματα, άρα δεν είναι πια μέλος της αλυσίδας, αλλά τα μπλοκ του είναι.

Αν και ο Β δεν μπορεί να υπογράψει νέα μπλοκ, αφού δεν είναι πλέον επικυρωτής, αυτός (ή όποιος έχει πρόσβαση στα κλειδιά του) μπορεί να υπογράψει τα πρώτα *n* μπλοκ από οποιοδήποτε κλάδο αυτού του blockchain. Πρακτικά, αυτό σημαίνει ότι έχοντας πρόσβαση στα κλειδιά του Β,

μπορεί κανείς να πλαστογραφήσει τα μπλοκ που επικύρωσε. Ο Β δεν είναι πλέον μέρος του συστήματος και ως εκ τούτου δεν υπάρχει τίποτα σε κίνδυνο για τον Β (nothing at stake). Επομένως, δεν έχει κανένα αντικίνητρο να μην επιτεθεί στο blockchain. Στην πράξη, μια επίθεση από τον Β θα ήταν να υπογράψει τα πρώτα *n* μπλοκ σε μια άλλη αλυσίδα του blockchain για ή με έναν εισβολέα.

Με βάση τα παραπάνω, υπάρχουν δύο πιθανά σενάρια για την επίθεση που ονομάζουμε μεταγενέστερη διαφθορά. Είτε ο Μ χακάρει τον Β και κλέβει το ιδιωτικό του κλειδί, ή ο Μ δωροδοκεί τον Β, και αυτός συμμετέχει στην επίθεση. Σε κάθε περίπτωση, το ιδιωτικό κλειδί του Β είναι γνωστό στον Μ, ο οποίος μπορεί να υπογράψει έγκυρα μπλοκ, μεταμφιεσμένος ως Β, αυξάνοντας τις πιθανότητές του να ξεπεράσει την κύρια αλυσίδα.

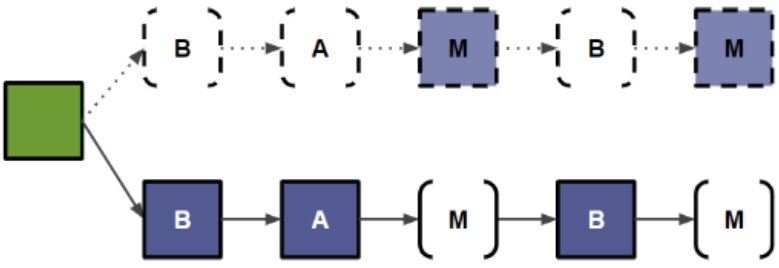


Εικόνα 6. Επίθεση απο Μακριά - Μεταγενέστερη Διαφθορά

Αιμορραγία μεριδίου (stake bleeding): Ας υποθέσουμε και πάλι ότι ο Μ, ως επικυρωτής θέλει να προσχηματίσει ένα άλλο είδος επίθεσης. Όπως και στις προηγούμενες περιπτώσεις, ο Μ έχει διακλαδωσει την κύρια αλυσίδα, έχει κρύψει τον (ιδιωτικό) κλάδο της και σχεδιάζει να τον δημοσιεύσει όταν ξεπεράσει την κύρια αλυσίδα. Σαφώς, όταν ο κλάδος αυτός δημιουργείται, ο Μ έχει τις ίδιες πιθανότητες να εκλεγεί ως ηγέτης σε όλους τους κλάδους του blockchain.

Ο Μ, για να αυξήσει τις πιθανότητές του να πετύχει αυτήν την επίθεση, αρχίζει να καθυστερεί την κύρια αλυσίδα. Η ιδέα είναι ότι παρακολουθώντας την κύρια αλυσίδα, θα έχει τον απαραίτητο χρόνο για να παράγει μπλοκ και να ξεπεράσει την κύρια αλυσίδα.

Για να ξεκινήσει την επίθεση, κάθε φορά που ο Μ εκλέγεται ως επικυρωτής της κύριας αλυσίδας, παραλείπει τη σειρά του, χάνοντας τη θέση του, όπως φαίνεται στην Εικόνα 7. Ωστόσο, αυτό δεν σημαίνει ότι ένας άλλος επικυρωτής θα πάρει τη θέση του, αντίθετα δεν θα προστεθεί νέο μπλοκ στο blockchain για εκείνη την περίοδο.

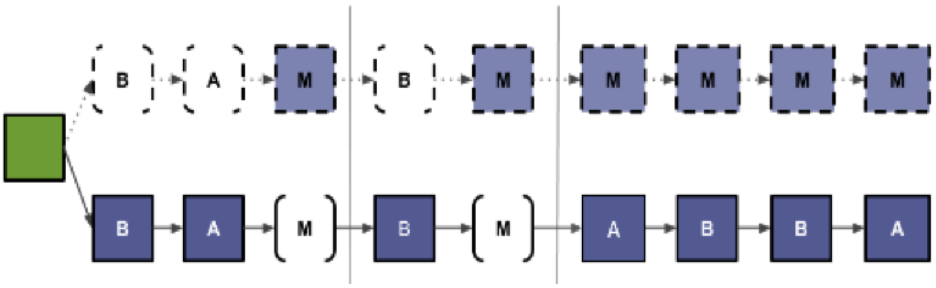


Εικόνα 7. Αρχή Επίθεσης από Μακριά Αιμορραγίας Μεριδίου

Ως αποτέλεσμα, ο Μ δεν θα λάβει ανταμοιβές από το σύστημα και το μερίδιό του θα μειωθεί σταδιακά. Τελικά, όλοι οι άλλοι επικυρωτές θα δημοσιεύσουν μπλοκ και θα πάρουν τις αμοιβές μπλοκ.

Ταυτόχρονα, στο δικό του κλάδο, ο Μ θα είναι ο μόνος επικυρωτής μπλοκ δημοσίευσης. Ως εκ τούτου, ο Μ θα δημοσιεύσει ένα μπλοκ, κάθε φορά που του δίνεται η ευκαιρία. Σε αυτήν την επίθεση, ο Μ θα προσπαθήσει να αυξήσει το μερίδιό του με κάθε δυνατό τρόπο. Κατά την εκτέλεση αυτής της επίθεσης, ο Μ βρίσκεται πίσω από την κύρια αλυσίδα, και έτσι είναι σε θέση να παρακολουθεί τις ενέργειες της κύριας αλυσίδας, π.χ. ποια συναλλαγή επιλέγει να προσθέσει σε κάθε μπλοκ. Εκτός από αυτό, ο Μ έχει πρόσβαση στο πεδίο συναλλαγών από το οποίο μπορεί να επιλέξει οποιαδήποτε συναλλαγή που βρίσκεται σε αυτό για να την προσθέσει στο μπλοκ του, εφόσον αυτές οι συναλλαγές είναι έγκυρες στο πλαίσιο του κλάδου του. Για το σκοπό αυτό, θα αντιγράψει τις συναλλαγές από την κύρια αλυσίδα και θα τις δημοσιεύσει στο δικό του κλάδο. Ο στόχος του είναι να μεγιστοποιήσει τον αριθμό των τελών συναλλαγών (transaction fees) που θα πάρει και να τα χρησιμοποιήσει για να αυξήσει το προσωπικό του μερίδιο. Ο Μ μπορεί να προτιμά να αντιγράφει συναλλαγές που βρίσκονται ήδη στην κύρια αλυσίδα για να μειώσει τις υποψίες του δικτύου.

Στην Εικόνα 8. βλέπουμε πως το μερίδιο του Μ αυξάνεται σταδιακά στην δικιά του αλυσίδα, ενώ μειώνεται στην κύρια:



Εικόνα 8. Επίθεση από Μακριά Αιμορραγία Μεριδίου

Με την καθυστέρηση της κύριας αλυσίδας και τη δημοσίευση όσο το δυνατόν περισσότερων μπλοκ στην εναλλακτική αλυσίδα που έφτιαξε, ο Μ θα πάρει τελικά το μεγαλύτερο μέρος του μεριδίου στον κλάδο του. Ως εκ τούτου, το μερίδιο του Μ θα αρχίσει να επεκτείνεται ταχύτερα από ό,τι η κύρια αλυσίδα, όπως απεικονίζεται στο σχήμα. Μόλις ο κλάδος του ξεπεράσει την κύρια αλυσίδα, ο Μ θα κάνει μια τελευταία συναλλαγή στην οποία αναδιανέμει το μερίδιο σε άλλους επικυρωτές για να τους μεταφέρει στην δική του αλυσίδα αφού έχει ξεπεράσει την κύρια, και στη συνέχεια θα δημοσιεύσει τον πλαστό κλάδο του. Το μερίδιο που αναδιανέμει στους άλλους επικυρωτές θα είναι μικρότερο από ότι αυτό που είχαν στην κύρια αλυσίδα.

Πρέπει να τονιστεί ότι η επίθεση είναι αρκετά αργή. Για να εκτελεστεί αυτή η επίθεση με επιτυχία, χρειάζεται περίπου μια εξαετής ιστορία blockchain για έναν εισβολέα με ποσοστό 30% του blockchain [41]. Για αυτό το λόγο δεν έχει καταγραφεί επίσημα κάποια πραγματική επίθεση αυτού του είδους.

4.2.1.4 Επίθεση Δωροδοκίας (Bribe Attack)

Ένας επιτιθέμενος [75] μπορεί να αγοράσει ισχύ εξόρυξης για σύντομο χρονικό διάστημα μέσω δωροδοκίας. Ο επιτιθέμενος επιχειρεί να δωροδοκήσει χρησιμοποιώντας το ίδιο το κρυπτονόμισμα, δημιουργώντας μια διακλάδωση (fork) που περιέχει τα χρήματα της δωροδοκίας και είναι διαθέσιμη για τον ανθρακωρύχο που την υιοθετεί. Αυτό ονομάζεται πληρωμή εντός ζώνης. Εκτός από την πληρωμή εντός ζώνης, υπάρχει και η πληρωμή εκτός ζώνης, κατά την οποία ο επιτιθέμενος θα πληρώσει απευθείας για να νοικιάσει την υπολογιστική του ισχύ, ή μέσω του Negative-Fee mining pool, κατά το οποίο ο επιτιθέμενος σχηματίζει μια πισίνα πληρώνοντας υψηλότερη απόδοση. Αυτή η επίθεση θα μπορούσε να οδηγήσει σε επίθεση πλειοψηφίας (51%), ή σε επίθεση κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS) με σκοπό τη διακοπή της λειτουργίας ολόκληρου του δικτύου.

Με λίγα λόγια η επίθεση βασίζεται στη δωροδοκία ανθρακωρύχων για να εργαστούν σε συγκεκριμένα μπλοκ ή διακλαδώσεις. Με αυτόν τον τρόπο, ο επιτιθέμενος μπορεί να παρουσιάσει αυθαίρετες συναλλαγές ως έγκυρες και να έχει ανέντιμους κόμβους που πληρώνονται για να τις επαληθεύσουν. Πληρώνοντάς τους ένα ποσό ίσο ή μεγαλύτερο από από τις ανταμοιβές του μπλοκ (σε περίπτωση που το μπλοκ ανακληθεί από το δίκτυο), παρέχει ένα κίνητρο αρκετά υψηλό για τους ανθρακωρύχους για να εργαστούν στα μπλοκ ή την αλυσίδα του επιτιθέμενου.

Παράδειγμα επίθεσης δωροδοκίας [42]:

Ας υποθέσουμε ότι ο επιτιθέμενος Α, ο οποίος ελέγχει μια μειοψηφία της υπολογιστικής ισχύος στο δίκτυο Bitcoin, επιχειρεί να εξαπολύσει επίθεση διπλής δαπάνης εναντίον ενός πωλητή Β. Πρώτον, ο Α πραγματοποιεί μια μεγάλη συναλλαγή με τον Β. Αφού η συναλλαγή συμπεριληφθεί στην αλυσίδα, ο Α αρχίζει να εργάζεται σε μια διακλάδωση, δημιουργώντας ένα μπλοκ που δεν περιλαμβάνει αυτή τη συναλλαγή, αλλά κρατάει το θέμα αυτό ιδιωτικό. Ο Α πρέπει να δημιουργήσει τουλάχιστον ένα μπλοκ στην αλυσίδα του πριν επιβεβαιωθεί η συναλλαγή. Αυτό το μπλοκ έχει κάποιες ειδικές συναλλαγές στις οποίες ο Α μεταφέρει κάποια BTC σε νέες διευθύνσεις που έχει δημιουργήσει προηγουμένως. Αφού επιβεβαιωθεί η συναλλαγή του Α προς τον Β (γενικά, σε χρόνο 6 μπλοκ), ο Β στέλνει στον Α τα αγαθά που αγόρασε και ο Α απελευθερώνει το μπλοκ του (τα μπλοκ) ενώ προσπαθεί να "δωροδοκήσει" άλλους ανθρακωρύχους για να εξορύξουν στη διακλάδωση του. Για να το κάνει αυτό, ο Α αποκαλύπτει το ιδιωτικό κλειδί (ή τα ιδιωτικά κλειδιά) (ενός ή περισσοτέρων) του λογαριασμού (ή των λογαριασμών) στον οποίο (στους οποίους) έχει μεταφέρει τα χρήματα στο μπλοκ (ή στα μπλοκ) που μόλις δημιούργησε. Οι ορθολογικοί ανθρακωρύχοι που βλέπουν το(α) ιδιωτικό(α) κλειδί(α), μπορούν να αποφασίσουν να εργαστούν στη διακλάδωση του Α. Θα δημιουργήσουν μια νέα συναλλαγή για να στείλουν τα BTC από τον αποκαλυπτόμενο λογαριασμό στους λογαριασμούς τους και στη συνέχεια θα προσπαθήσουν να δημιουργήσουν νέα μπλοκ στη διακλάδωση του Α. Μόλις ένας ανθρακωρύχος βρει μια λύση, ο Α την επιβεβαιώνει αποκαλύπτοντας το επόμενο ιδιωτικό κλειδί. Αν καταφέρει να δώσει επαρκή κίνητρα για να προσελκύσει αρκετή δύναμη εξόρυξης στη διακλάδωση του, η διακλάδωση αυτή θα αναλάβει τον κύριο κλάδο/αλυσίδα και η συναλλαγή μεταξύ του Α και του Β θα αναιρεθεί.

Αν ο Α δεν ενθαρρύνει άλλους ανθρακωρύχους να εργαστούν στην διακλάδωση του, δεν μπορεί να ελπίζει ότι η επίθεσή του θα είναι επιτυχής, επειδή έχει ένα μικρό κλάσμα της υπολογιστικής ισχύος του δικτύου. Αν η εξόρυξη στη διακλάδωση του Α θεωρείται πιο κερδοφόρα από τους ορθολογικούς ανθρακωρύχους, θα ενταχθούν σε αυτήν. Ο Α πρέπει να συνεχίζει να πείθει τους ανθρακωρύχους να κάνουν εξόρυξη στη δική του διακλάδωση, διασφαλίζοντας παράλληλα ότι η επίθεση παραμένει κερδοφόρα για εκείνον στο τέλος.

Για να ξεκινήσει την επίθεση, ο Α χρειάζεται τουλάχιστον ένα μπλοκ στη διακλάδωση του που περιέχει συναλλαγές στα αναγνωριστικά λογαριασμών που πρέπει να δημοσιευθούν. Υποθέτοντας ότι μια συναλλαγή χρειάζεται έξι μπλοκ για να επιβεβαιωθεί, ο επιτιθέμενος θα πρέπει να έχει τουλάχιστον το 14,28% της υπολογιστικής ισχύος του δικτύου. Με μια τέτοια ισχύ, ο επιτιθέμενος μπορεί (κατά μέσο όρο) να δημιουργήσει ένα μπλοκ σε 70 λεπτά, δηλαδή το χρόνο που απαιτείται για τη δημιουργία 6 μπλοκ από άλλους ανθρακωρύχους, (με το 85,72% της ισχύος) στο κύριο fork [42].

Στο [67] αναφέρεται ότι στην πράξη, είναι δύσκολο να εντοπιστεί αν τα κρυπτογραφικά περιουσιακά στοιχεία που αποστέλλονται στους ανθρακωρύχους είναι δωροδοκίες. Παρόλα αυτά αναφέρεται ότι με συλλογή δεδομένων Ethereum από την 1η Ιανουαρίου 2019 έως την 1η Μαρτίου 2022, φιλτράρονται 982.116 συναλλαγές και 19.601 μπλοκ, και εμπλέκονται 150 ανθρακωρύχοι και 829 πιθανοί δωροδοκητές (bribers). Το μέγιστο των πιθανών δωροδοκιών είναι 7.620 ETH, και η μέγιστη μεταφερόμενη αξία (σε δολάρια ΗΠΑ) υπερβαίνει τα 12,5 εκατομμύρια δολάρια.

4.2.2 Επιθέσεις στην Συναλλαγή

4.2.2.1 Διπλή Δαπάνη (Double Spending)

Στα κρυπτονομίσματα, η διπλή δαπάνη αναφέρεται στη χρήση των ίδιων κρυπτονομισμάτων δύο ή περισσότερες φορές (δηλαδή σε δύο ή παραπάνω συναλλαγές). Στις λειτουργίες κρυπτονομισμάτων, μια συναλλαγή μεταφέρει την ιδιοκτησία ενός περιουσιακού στοιχείου από τη διεύθυνση του αποστολέα στη δημόσια διεύθυνση του παραλήπτη και η αξία της συναλλαγής υπογράφεται από τον αποστολέα με ιδιωτικό κλειδί [28]. Μόλις υπογραφεί η συναλλαγή, μεταδίδεται στο δίκτυο πάνω στο οποίο ο δέκτης επικυρώνει τη συναλλαγή. Η επικύρωση, στο τέλος, του παραλήπτη πραγματοποιείται όταν ο παραλήπτης αναζητά την έξοδο της μη αποθηκευμένης συναλλαγής του αποστολέα, επαληθεύει την υπογραφή του αποστολέα και περιμένει την εξόρυξη της συναλλαγής σε ένα έγκυρο μπλοκ. Η διαδικασία αυτή διαρκεί μερικά λεπτά ανάλογα με το μέγεθος του transaction mempool, την ταχύτητα του δικτύου, τον παράγοντα προτεραιότητας της συναλλαγής και τον χρόνο υπολογισμού μπλοκ του κρυπτονομίσματος. Στο Bitcoin, για παράδειγμα, ο μέσος χρόνος εξόρυξης μπλοκ είναι 10 λεπτά [28].

Για μια επιτυχημένη επίθεση διπλής δαπάνης υπό κανονικές συνθήκες, απαιτείται η ολοκλήρωση δύο επιτυχημένων ξεχωριστών συναλλαγών ταχύτερα από ό,τι χρειάζεται για την επαλήθευση μιας από αυτές και άρα την ανίχνευση του προβλήματος. Το βασικό πρόβλημα, λοιπόν, προκύπτει από το γεγονός ότι οι επιβεβαιώσεις των συναλλαγών χρειάζονται χρόνο. Υπάρχουν διαφορετικές τεχνικές, οι οποίες μπορούν να χρησιμοποιηθούν από έναν επιτιθέμενο.

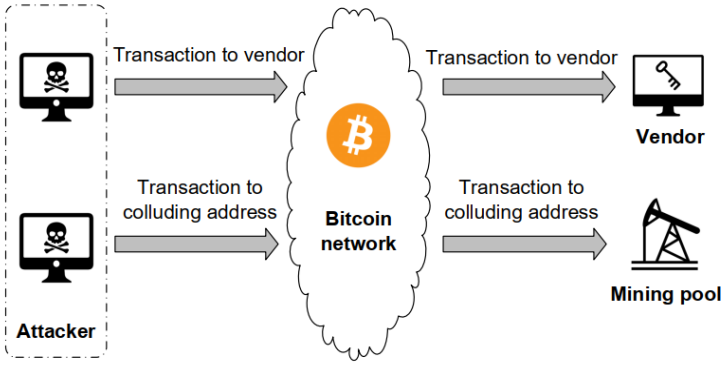
Στην έρευνα του [46], διεξάγεται μια ανάλυση των διπλών δαπανών κατά των ταχέων πληρωμών στο Bitcoin, και προτείνεται ένα μοντέλο επίθεσης, όπως φαίνεται στην Εικόνα 9. Υποθέτοντας ότι ο επιτιθέμενος γνωρίζει τη διεύθυνση του θύματος πριν από την επίθεση, για να εκτελέσει διπλή δαπάνη, ο επιτιθέμενος θα στείλει δύο συναλλαγές, TXv και TXa και θα επιλέξει τα ίδια BTCs (κρυπτονόμισμα στο Bitcoin) ως εισροές για τις TXv και TXa. Η διεύθυνση παραλήπτη του TXv ορίζεται στη διεύθυνση του στοχευόμενου θύματος και η διεύθυνση παραλήπτη του TXa ορίζεται στη διεύθυνση που ελέγχεται από τον επιτιθέμενο. Αν πληρούνται οι ακόλουθες τρεις προϋποθέσεις, η διπλή δαπάνη θα είναι επιτυχής:

(1) η TXv προστίθεται στο πορτοφόλι του στοχευόμενου θύματος

(2) η TXa εξορύσσεται ως έγκυρη στο blockchain

(3) Ο επιτιθέμενος παίρνει έξοδο TXv πριν το θύμα εντοπίσει ανάρμοστη συμπεριφορά.

Αν η επίθεση είναι επιτυχής, το TXv θα επαληθευθεί τελικά ως μη έγκυρη συναλλαγή και τα BTCs πραγματικά ξοδεύονται από την TXa. Ο δράστης της επίθεσης έλαβε έξοδο TXv, που είναι η συνήθης υπηρεσία του θύματος. Εφόσον η διεύθυνση παραλήπτη της TXa ελέγχεται από τον επιτιθέμενο, τα εν λόγω BTC εξακολουθούν να ανήκουν στον ίδιο τον επιτιθέμενο. Σε αυτό το μοντέλο διπλής δαπάνης, ο επιτιθέμενος απολαμβάνει την υπηρεσία χωρίς να πληρώσει BTC.



Εικόνα 9. Επίθεση Διπλής Δαπάνης

Στις περισσότερες περιπτώσεις επιτυχών 51% επιθέσεων, οι επιτιθέμενοι καταλήγουν να μπορέσουν αποτελεσματικά με την δύναμη αυτή να εκτελέσουν διπλή δαπάνη. Στην πιο μεγάλη 51% επίθεση που αναφέρθηκε στο 4.1.1 και έγινε στο Bitcoin Gold [66] χρησιμοποιήθηκε διπλή δαπάνη. Μια άλλη περίπτωση επιτυχής τέτοιας επίθεσης ήταν η διπλή δαπάνη στο Ethereum Classic (διακλάδωση του Ethereum) όπου μετά από την 51% επίθεση, ο επιτιθέμενος προσπάθησε να κάνει διπλή δαπάνη σε 465.444 ethereum classic (ETC), αξίας περίπου 3,3 εκατομμυρίων δολαρίων, αλλά τελικά κατάφερε να κάνει σε 238.306 ETC, αξίας 1,68 εκατομμυρίων δολαρίων. [71]

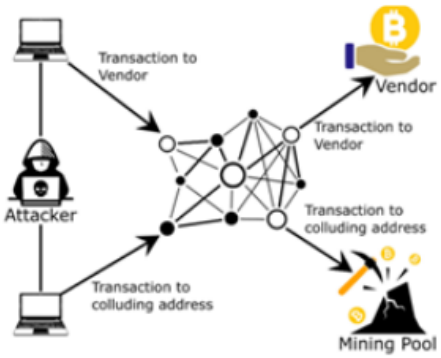
Υπάρχουν τρεις σημαντικές παραλλαγές της διπλής δαπάνης, για τις οποίες θα μιλήσουμε παρακάτω. Αυτές είναι οι: Race attack, Finney attack και Vector76 attack.

4.2.2.1.1 Επίθεση Αγώνα (Race Attack)

Η επίθεση αγώνα, που απεικονίζεται στην παρακάτω εικόνα [38], επιτρέπει μια κατάσταση στην οποία ένας εισβολέας δημιουργεί δύο συναλλαγές, μία γνήσια και μία δόλια (προσπάθεια διπλής σπατάλης). Ο στόχος είναι οποιοσδήποτε κόμβος που δέχεται συναλλαγές με μη επιβεβαιωμένη κατάσταση, δηλαδή ορατές συναλλαγές που έχουν περάσει στο transaction pool αλλά δεν έχουν μπει σε κάποιο μπλοκ και δεν έχουν πάρει κάποια επιβεβαίωση από κάποιον ανθρακωρύχο. Ο επιτιθέμενος προσπαθεί, να συνδεθεί στενά ή απευθείας με το transaction pool και χρονομετρά τη μετάδοση των συναλλαγών για να εκμεταλλευτεί τον μικρότερο χρόνο επιβεβαίωσης της πρώτης συναλλαγής (της νόμιμης). Με την αποστολή της δόλιας συναλλαγής στον στόχο και της νόμιμης συναλλαγής στην πισίνα εξόρυξης, η επίθεση μπορεί να επιτύχει αν ο στόχος αποδεχτεί την δόλια συναλλαγή και παρέχει ορισμένα αγαθά ή υπηρεσίες προτού δει ποτέ τη νόμιμη συναλλαγή. Ως αποτέλεσμα, η δόλια συναλλαγή επιβεβαιώνεται και προστίθεται στο blockchain, ενώ η αντικρουόμενη συναλλαγή (που είναι η νόμιμη) παραμένει ανεπιβεβαίωτη και απορρίπτεται (προκαλώντας διπλή δαπάνη). Η διαφορά με την απλή επίθεση διπλής δαπάνης είναι ότι η διπλή δαπάνη αποσκοπεί στο να δαπανηθούν τα ίδια κεφάλαια δύο φορές, ενώ η επίθεση αγώνα αποσκοπεί στην αντικατάσταση μιας νόμιμης συναλλαγής με μια νέα, αντικρουόμενη, εκμεταλλευόμενη τη σειρά επιβεβαίωσης της συναλλαγής.

Αυτός είναι ο λόγος για τον οποίο συνιστάται να περιμένει κάποιος για κάποιο ελάχιστο αριθμό επιβεβαιώσεων πριν θεωρήσει μια συναλλαγή έγκυρη. Σε μια επίθεση αγώνα, ο επιτιθέμενος

εκμεταλλεύεται τη διαφορά στους χρόνους επιβεβαίωσης για διαφορετικούς τύπους συναλλαγών για να εξαπατήσει το δίκτυο ώστε να αποδεχτεί τη νόμιμη συναλλαγή (όπου στέλνονται χρήματα στον εαυτό του) και να αγνοήσει την απόπειρα διπλής δαπάνης.



Εικόνα 10. Επίθεση Αγώνα

Μια επίθεση αγώνα [40], βασίζεται στην ύπαρξη πιθανότητας τερματισμού. Σε περιβάλλοντα blockchain, όπου ο τερματισμός δεν είναι απόλυτος, πρέπει να επιτευχθεί ένας αριθμός επιβεβαιώσεων πριν θεωρηθεί μια συναλλαγή ότι ολοκληρώθηκε. Σημειώνουμε η προσθήκη του μπλοκ, όπου έχει ενταχθεί μια συναλλαγή, στο blockchain θεωρείται πως είναι η πρώτη επιβεβαίωση ενώ οι προσθήκες έξτρα μπλοκ μετά από αυτό (στο blockchain) αντιστοιχούν έκαστη σε επόμενες επιβεβαιώσεις.

Συνήθως είναι γνωστός στο δίκτυο ένας συνιστώμενος αριθμός επιβεβαίωσης (στο Bitcoin για παράδειγμα συνιστώνται έξι επιβεβαιώσεις για να θεωρείται μια συναλλαγή πλήρως ασφαλής γιατί η πιθανότητα αντιστροφής μιας συναλλαγής λόγω επιτυχούς επίθεσης διπλής δαπάνης γίνεται εξαιρετικά χαμηλή). Επομένως, για να αποφύγουν αυτές τις επιθέσεις, οι χρήστες θα πρέπει πάντα να περιμένουν να προστεθούν μερικά μπλοκ στην αλυσίδα πάνω από το μπλοκ της συναλλαγής τους πριν θεωρήσουν ότι η συναλλαγή είναι έγκυρη. Συναλλαγές που χειρίζονται σημαντικό ποσό χρημάτων ενδέχεται να απαιτούν μεγαλύτερο αριθμό επιβεβαιώσεων προτού γίνουν αποδεκτές ως έγκυρες. Είναι πιθανό πως μια υπηρεσία ενδέχεται να μην είναι σωστά μελετημένη/σχεδιασμένη/υλοποιημένη και δεν περιμένει τον συνιστώμενο αριθμό αποδοχών για ένα συγκεκριμένο blockchain μέσω του οποίου προσφέρετε. Σε αυτήν την περίπτωση, μια επίθεση διπλής δαπάνης είναι δυνατή.

Οι επιθέσεις διπλής δαπάνης, όπως είναι οι επιθέσεις αγώνα αλλά και Finney (4.2.1.2), βασίζονται στο γεγονός ότι οι χρήστες αποδέχονται συναλλαγές πριν αυτές επικυρωθούν ή επιβεβαιωθούν.

4.2.2.1.2 Επίθεση Finney

Η επίθεση Finney είναι μια παραλλαγή της επίθεσης διπλής δαπάνης στην οποία ένας ανθρακωρύχος καθυστερεί τη διάδοση μπλοκ για να επιτύχει διπλή δαπάνη ως προς τη συναλλαγή του [47]. Ο ανθρακωρύχος δημιουργεί μια συναλλαγή, υπολογίζει ένα μπλοκ, και επιλέγει να μην αναμεταδώσει το μπλοκ. Εν τω μεταξύ, παράγει ένα αντίγραφο της προηγούμενης συναλλαγής του και το στέλνει σε έναν παραλήπτη. Αφού ο παραλήπτης αποδεχτεί τη συναλλαγή και παραδώσει το προϊόν, ο ανθρακωρύχος δημοσιεύει το προηγούμενο μπλοκ του με την αρχική συναλλαγή σε αυτό. Επομένως, η συναλλαγή που στάλθηκε στον παραλήπτη καθίσταται άκυρη και ο ανθρακωρύχος επιτυχώς πραγματοποίησε επίθεση διπλής δαπάνης [28].

Με λίγα λόγια η επίθεση Finney είναι μια επίθεση διπλής δαπάνης που απαιτεί ένα μπλοκ να έχει προ-εξορυχθεί, δηλαδή θα έχει εξορυχθεί αλλά δεν θα έχει μεταδοθεί ακόμα για επιβεβαίωση. Αυτό το μπλοκ θα πραγματοποιήσει μια δόλια συναλλαγή, αλλά δεν θα μεταδοθεί ακόμα. Τα ίδια κέρματα που χρησιμοποιούνται στην δόλια συναλλαγή θα χρησιμοποιούνται εν τω μεταξύ ως πληρωμή στον κόμβο-στόχο. Μετά τη λήψη ορισμένων αγαθών ή υπηρεσιών, το δόλιο μπλοκ θα μεταδοθεί στη συνέχεια στο υπόλοιπο δίκτυο, ακυρώνοντας έτσι τη συναλλαγή που στάλθηκε στο στόχο. Και πάλι, η αναμονή για πρόσθετες επιβεβαιώσεις πριν από την αποδοχή μιας συναλλαγής μπορεί να υπερνικήσει αυτήν την επίθεση. [38]

Η επίθεση Finney έχει χαμηλή πιθανότητα επιτυχίας λόγω των σύντομων χρονικών διαστημάτων δημιουργίας μπλοκ και της διαδικασίας επίθεσης που είναι χρονικά ευαίσθητη. Αν ένας επιτιθέμενος επιχειρήσει να ξεκινήσει αυτήν την επίθεση, είναι δύσκολο ότι θα είναι σε θέση να επιτύχει τα εξής: να δημιουργήσει μια συναλλαγή διπλής δαπάνης, να εξαπατήσει έναν αισιόδοξο δέκτη, να λάβει το προϊόν πριν από την επιβεβαίωση, και να δημοσιεύσει ένα μπλοκ πριν από οποιοδήποτε άλλο ανθρακωρύχο, εντός του χρόνου που χρειάζεται για ένα μπλοκ να δημιουργηθεί (ανάλογα με το blockchain).

Για παράδειγμα, ο χρόνος εξόρυξης ενός μπλοκ στο Ethereum είναι 15 δευτερόλεπτα [28], κάτι που σημαίνει ότι είναι αδύνατο ένας επιτιθέμενος να πραγματοποιήσει μια τέτοια επίθεση σε αυτό (το blockchain). Δεδομένου ότι η διαδικασία επίθεσης είναι πιο χρονοβόρα από το χρονικό διάστημα δημιουργίας μπλοκ, η επίθεση Finney είναι ιδιαίτερα δύσκολο να είναι επιτυχής, και δεν έχουν καταγραφεί σοβαρές & επιτυχείς τέτοιες επιθέσεις (στο παρελθόν).

4.2.2.1.3 Επίθεση Vector76

Το Vector76 είναι ένας συνδυασμός της επίθεσης Finney και της επίθεσης αγώνα [48]. Σε αυτήν την περίπτωση, ένας κακόβουλος ανθρακωρύχος δημιουργεί δύο κόμβους, ο ένας από τους οποίους συνδέεται μόνο με τον κόμβο ανταλλαγής και ο άλλος συνδέεται με καλά συνδεδεμένους ομότιμους στο δίκτυο blockchain. Μετά από αυτό, ο ανθρακωρύχος δημιουργεί δύο συναλλαγές, μία υψηλής αξίας και μία χαμηλής αξίας. Στη συνέχεια, ο επιτιθέμενος προ-εξορύσσει και παρακρατεί ένα μπλοκ με μια συναλλαγή υψηλής αξίας. Μετά από μια ανακοίνωση μπλοκ (επικύρωση ενός μπλοκ από τους κόμβους), στέλνει γρήγορα το προ-εξορυγμένο μπλοκ απευθείας στην υπηρεσία ανταλλαγής κρυπτονομισμάτων (exchange service). Μαζί με μερικούς ανθρακωρύχους θα θεωρήσουν το προ-εξορυγμένο μπλοκ ως μέρος της κύρια αλυσίδα και θα επιβεβαιώσουν αυτήν τη συναλλαγή. Έτσι, αυτή η επίθεση εκμεταλλεύεται το γεγονός ότι ένα μέρος του δικτύου βλέπει τη συναλλαγή που ο επιτιθέμενος έχει συμπεριλάβει σε ένα μπλοκ ενώ το άλλο μέρος του δικτύου δεν βλέπει αυτήν την συναλλαγή. Αφού η υπηρεσία ανταλλαγής επιβεβαιώσει τη συναλλαγή υψηλής αξίας, ο επιτιθέμενος στέλνει μια συναλλαγή χαμηλής αξίας στο κύριο δίκτυο που τελικά απορρίπτει τη συναλλαγή υψηλής αξίας. Ως αποτέλεσμα, στον λογαριασμό του δράστη επιστρέφει το ποσό της συναλλαγής υψηλής αξίας. Αν και υπάρχει μεγάλη πιθανότητα επιτυχίας με αυτήν την επίθεση, δεν είναι κοινή γιατί απαιτεί ένα φιλοξενούμενο ηλεκτρονικό πορτοφόλι που τρέχει ένα κόμβο με μια εισερχόμενη συναλλαγή που δέχεται την πληρωμή μετά από μία μόνο επιβεβαίωση [49].

4.2.2.2 Επιθέσεις Επανάληψης

Μια επίθεση επανάληψης μπορεί να λάβει χώρα, αν υπάρχει μια σκληρή διακλάδωση ενός blockchain [43]. Αυτό σημαίνει ότι δύο χωριστές αλυσίδες blockchain προέρχονται από μια κοινή αρχική αλυσίδα.

Στους χρήστες θα χορηγηθεί ίση ποσότητα περιουσιακών στοιχείων και για τα δύο αυτά νέα στελέχη, αν κατέχουν κάποια πριν από τον χωρισμό. Δηλαδή εάν είχε κάποιος Χ ποσό του αρχικού κρυπτονομίσματος πριν από τη διακλάδωση, συνήθως θα λάβει ίσο ποσό του νέου κρυπτονομίσματος που σχετίζεται με τη διακλάδωση. Αυτό αναφέρεται συχνά ως "διαχωρισμός νομισμάτων" ή "airdrop". Οι συγκεκριμένες λεπτομέρειες και οι μηχανισμοί της διάσπασης νομίσματος εξαρτώνται από τους κανόνες και τις πολιτικές που θέτουν οι προγραμματιστές ή η κοινότητα πίσω από τη διακλάδωση.

Οι συναλλαγές μπορούν τώρα να πραγματοποιηθούν και στις δύο αλυσίδες ξεχωριστά. Δεδομένου ότι τα ψηφιακά αρχεία είναι δημόσια, ο επιτιθέμενος μπορεί να δει μια συναλλαγή στη μια διακλάδωση και να την αναπαράγει στην άλλη, αν δεν ληφθούν αντίμετρα. Αυτό έχει ως αποτέλεσμα την ίση απώλεια των περιουσιακών στοιχείων και για τα δύο διχαλωτά στελέχη/διακλαδώσεις αντί για το ένα.

Αυτό ήταν δυνατό στο Ethereum πριν εισαγάγει το chainID (αναγνωριστικό αλυσίδας) για να προσδιορίσει το προβλεπόμενο blockchain για μια δεδομένη συναλλαγή, αλλά αυτό το χαρακτηριστικό δεν είναι ενεργοποιημένο από προεπιλογή και ορισμένοι χρήστες εξακολουθούν να είναι ευάλωτοι.

Κάθε φορά που γίνεται μια διακλάδωση, είναι ευθύνη των προγραμματιστών του blockchain να συμπεριλάβουν τα κατάλληλα μέτρα μετριασμού για τις επιθέσεις επανάληψης μέσω της δημιουργίας και χρήσης ανανεώσεων (updates). Οι έξυπνες συμβάσεις μπορούν να περιέχουν παρόμοιες τρωτότητες.

Για μια επιτυχημένη επίθεση επανάληψης, λοιπόν, ένας κακόβουλος χρήστης πρέπει να βρει το blockchain σε μια κατάσταση που επιτρέπει μια τέτοια επίθεση, όπως μια κατάσταση διακλάδωσης (αλυσίδας) ή κακώς γραμμένες έξυπνες συμβάσεις. Αν το blockchain έχει διαχωριστεί (forked), ο δράστης απαιτεί πρόσβαση σε μια συναλλαγή με το ένα στέλεχος για να την επαναλάβει στο άλλο, πράγμα που θα έχει ως αποτέλεσμα τη μετακίνηση κεφαλαίων και από τα δύο στελέχη/διακλαδώσεις.

4.2.3 Επιθέσεις στο Ομότιμο Σύστημα

4.2.3.1 Επίθεση Έκλειψης (Eclipse Attack)

Ο στόχος της επίθεσης έκλειψης είναι να απομονωθεί ένα θύμα από ένα νόμιμο δίκτυο, κάνοντας το να είναι συνδεδεμένο αποκλειστικά μόνο με κόμβους που βρίσκονται υπό τον έλεγχο του επιτιθέμενου μέχρι να επιτευχθεί το μέγιστο όριο σύνδεσης . Στη συνέχεια είναι πολύ πιο εύκολο να ξεκινήσουν περαιτέρω επιθέσεις. Η ακριβής διαδικασία διαφέρει ανάλογα με την υλοποίηση του δικτύου P2P. Σημαντικοί παράγοντες είναι, μεταξύ άλλων, το όριο σύνδεσης και ο αριθμός των κόμβων που μπορούν να ξεκινήσουν ταυτόχρονα σε μια συσκευή με συγκεκριμένη IP. Επίσης, παίζουν ρόλο το πόσο συχνά αλλάζουν οι ομότιμοι με τους οποίους συνδέεται ένας κόμβος (και πόσο διαφορετικοί είναι αυτοί) καθώς και τι μεθόδους ασφάλειας ως προς αυτές τις επιθέσεις χρησιμοποιεί το εκάστοτε blockchain [43]. Παρακάτω εξηγούμε πόσο ευάλωτα είναι συγκεκριμένα διάσημα blockchains σε αυτό το είδος επίθεσης.

Bitcoin: Ο πελάτης (client) Bitcoin που εκτελείται σε ένα μηχάνημα ενός χρήστη/κόμβου του δικτύου χρησιμοποιεί ένα τυχαίο πρωτόκολλο για την αναζήτηση 8 ομότιμων. Επιπλέον, γίνεται δέκτης 117 εισερχόμενων συνδέσεων (αυτό είναι το άνω όριο). Ένας επιτιθέμενος θα μπορούσε τώρα να προσπαθήσει να μπλοκάρει και τις 117 συνδέσεις και να στείλει κακόβουλη κυκλοφορία (garbage traffic) στο θύμα, ελπίζοντας να επανεκκινήσει τον Bitcoin client. Γενικότερα ο επιτιθέμενος προσδοκά την επανεκκίνηση του Bitcoin client. Αυτό θα μπορούσε να συμβεί και με κάποια διακοπή ρεύματος ή ακόμα και με κάποια προγραμματισμένη αναβάθμιση στο σύστημα (την οποία θα γνωρίζει και μπορεί να εκμεταλλευτεί ο επιτιθέμενος). Δεδομένου ότι απαιτούνται πολλοί κόμβοι για να επιτευχθεί το μπλοκάρισμα όλων των συνδέσεων (στην προκειμένη περίπτωση 117), είναι συνήθως απαραίτητο να χρησιμοποιηθεί ένα botnet για αυτό το είδος της επίθεσης.

Ο όρος botnet προέρχεται από τις λέξεις “robot” και “network”. Είναι ένα δίκτυο υπολογιστών υπό τον έλεγχο ενός μοναδικού επιτιθέμενου, ο οποίος μπορεί να δώσει εντολή σε κάθε υπολογιστή του botnet να εκτελέσει ταυτόχρονα μια συντονισμένη εγκληματική/κακόβουλη ενέργεια. [50]

Κατά την επανεκκίνηση του Bitcoin πελάτη, διαγράφονται οι υπάρχοντες ομότιμοι και δημιουργούνται νέοι. Η πιθανότητα οι νέοι ομότιμοι να ελέγχονται από τον επιτιθέμενο είναι τώρα πολύ υψηλή, καθώς ο επιτιθέμενος θα φροντίσει οι κακόβουλοι κόμβοι του να διαθέτουν συχνά μεγάλο αριθμό συνδέσεων και να είναι στρατηγικά τοποθετημένοι ώστε να κυριαρχούν στις εισερχόμενες και εξερχόμενες συνδέσεις του στόχου. Αυτό θα γίνει με ανάλυση δικτύου από τον επιτιθέμενο για να εντοπίσει τις διευθύνσεις IP διαφόρων κόμβων στο δίκτυο blockchain και άρα και του κόμβου θύματος. Αυτή η ανάλυση μπορεί να περιλαμβάνει την παρακολούθηση της κυκλοφορίας του δικτύου, τη συμμετοχή στο δίκτυο ή τη συλλογή δημοσίως διαθέσιμων δεδομένων σχετικά με τους κόμβους. Ο επιτιθέμενος θα μπορούσε επίσης να χρησιμοποιήσει τεχνικές όπως το "sniffing" ή η ακρόαση πακέτων δικτύου για τη συλλογή πληροφοριών. Το κόστος μιας τέτοιας επίθεσης μπορεί να είναι δαπανηρό καθώς χρειάζεται ένας σημαντικός αριθμός πόρων από τον επιτιθέμενο, ενώ ταυτόχρονα όσο πιο μεγάλο και ποικιλόμορφο είναι το δίκτυο του blockchain στο οποίο γίνεται η επίθεση τόσο πιο δαπανηρή είναι για τον επιτιθέμενο.

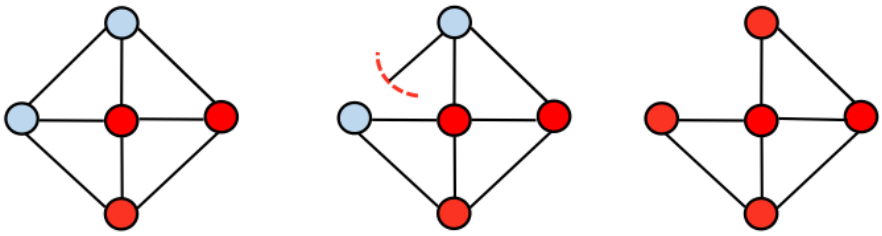
Αν ένας διακομιστής εκλείψει με επιτυχία, αυτό μπορεί να οδηγήσει σε κάποια προβλήματα και περαιτέρω επιθέσεις, καθώς το θύμα θα είναι συνδεδεμένο μόνο με κόμβους του botnet, το οποίο θα ενεργεί ως ένα κακόβουλο blockchain που θα προσομοιώνει το νόμιμο. Έτσι το θύμα δεν θα

είναι πλέον σε θέση να εντοπίσει τη διαφορά μεταξύ μιας έγκυρης συναλλαγής και κακόβουλων πράξεων [51].

Ethereum: Το Ethereum είναι επίσης ευάλωτο σε επιθέσεις Έκλειψης. Το μέγιστο για εξερχόμενες συνδέσεις είναι 13 αντί για 8 που έχει το Bitcoin, γεγονός που καθιστά την επίθεση πιο δύσκολη (από αυτή την πλευρά). Όμως, ως αναγνωριστικό για έναν πελάτη χρησιμοποιείται ένα δημόσιο κλειδί ECDSA και όχι η IP διεύθυνση. Αυτό σημαίνει ότι οποιοσδήποτε αριθμός κόμβων θα μπορούσε να εκτελεστεί σε έναν υπολογιστή (δηλαδή δεν υπάρχει συγκεκριμένο όριο συνδέσεων). Αυτό εξάλειψε την ανάγκη για ένα botnet και επέτρεψε να πραγματοποιούνται τέτοιες επιθέσεις με ένα κλάσμα των αρχικά απαιτούμενων πόρων (πχ. ένα μόνο μηχάνημα) [52].

Μια ομάδα κακόβουλων κόμβων απομονώνει τους γειτονικούς της κόμβους χρησιμοποιώντας διευθύνσεις IP, θέτοντας έτσι σε κίνδυνο την εισερχόμενη και εξερχόμενη κυκλοφορία τους. Στο Bitcoin, ένας κόμβος μπορεί να συνδεθεί ενεργά με όλους τους άλλους κόμβους του δικτύου, σχηματίζοντας μια συστάδα κόμβων. Στη συστάδα κόμβων, κάθε ομότιμος γνωρίζει τη διεύθυνση IP όλων των άλλων ομότιμων. Με αρκετούς εκτεθειμένους κόμβους σε μια συστάδα, ο επιτιθέμενος μπορεί να απομονώσει τους τίμιους κόμβους και να αλλάξει την προβολή του Blockchain τους. Μπορεί να ελέγχει την εισερχόμενη και εξερχόμενη κυκλοφορία τους και να τους τροφοδοτεί με ψεύτικες πληροφορίες σχετικά με το Blockchain και τις συναλλαγές.

Στην Εικόνα 11 βλέπουμε μια επίθεση έκλειψης σε ένα δίκτυο κρυπτονομισμάτων. Οι μπλε κόμβοι είναι οι ειλικρινείς κόμβοι που ακολουθούν την πραγματική κατάσταση του blockchain, ενώ οι κόκκινοι είναι οι κακόβουλοι κόμβοι που προσπαθούν να φτιάξουν μια συστάδα κόμβων γύρω από τους μπλε. [28]



Εικόνα 11. Επίθεση Έκλειψης

Εφόσον ένας έντιμος κόμβος κρατάει σύνδεση με έναν άλλο έντιμο κόμβο, είναι πιθανό να λάβει τις σωστές πληροφορίες για την κατάσταση του blockchain. Αν η σύνδεση μεταξύ τους διακυβεύεται (πχ. λόγω επανεκκινήσεων), οι δύο αυτοί έντιμοι κόμβοι θα περικυκλωθούν με κακόβουλους κόμβους και θα γίνουν άθελά τους μέρος της κακόβουλης συστάδας κόμβων.

Επιθέσεις που ακολουθούν (Follow-Up Attacks): Αν ένας επιτιθέμενος έχει καταφέρει να απομονώσει ένα θύμα, μπορεί να χρησιμοποιήσει διάφορες τεχνικές για να προκαλέσει περαιτέρω ζημιά. Αν, για παράδειγμα, δύο διακομιστές θέλουν να εκπληρώσουν και να μεταδώσουν ένα μπλοκ την ίδια στιγμή, δημιουργείται μια συνθήκη αγώνα. Στην περίπτωση αυτή, το δίκτυο για λίγο διακλαδώνεται και στην συνέχεια γίνεται δεκτό μόνο το ένα αποτέλεσμα και απορρίπτεται το άλλο, οπότε το ένα μπλοκ θα εισαχθεί στο blockchain και το άλλο θα μείνει έωλο έξω από αυτό. Ο επιτιθέμενος θα μπορούσε πλέον να δημιουργήσει τεχνητά αυτό το πρόβλημα συγκρατώντας τα αποτελέσματα, έως ότου να εξορυχθεί ένα άλλο μπλοκ και να δημιουργήσει αυτή τη συνθήκη αγώνα. Αυτό προκαλεί μεγάλη υπολογιστική προσπάθεια χωρίς όφελος.

Ένας απομονωμένος διακομιστής επίσης δεν αποτελεί πλέον μέρος του δικτύου και δεν συμβάλλει στην ολοκλήρωση των εργασιών (tasks). Επειδή ορισμένοι συμμετέχοντες μπορούν να αποκλειστούν από το δίκτυο με αυτόν τον τρόπο, αυτό μπορεί να διευκολύνει επιθέσεις 51%. Πολλές επιθέσεις στοχεύουν, επίσης, συγκεκριμένα σε κρυπτονομίσματα. Προσπαθούν να χειραγωγήσουν το σύστημα με τέτοιο τρόπο ώστε τα κέρδη να αποκομίζονται με την παρακράτηση της πραγματικής κατάστασης των συναλλαγών από το θύμα. Αυτό συμβαίνει σε περιπτώσεις που ο επιτιθέμενος ανακατευθύνει τα κεφάλαια σε δικές του διευθύνσεις ή κάνοντας νόμιμες συναλλαγές να αποτύχουν. Το ότι το θύμα βρίσκεται κάτω από την επιρροή του επιτιθέμενου μπορεί να οδηγήσει και σε διπλή δαπάνη, καθώς ο επιτιθέμενος μπορεί να ξεκινήσει μια νόμιμη συναλλαγή με τα ίδια κρυπτονομίσματα που μπορεί να χρησιμοποιήσει το θύμα για μια δικιά του. Καθώς οι πληροφορίες που παρέχονται από τους κακόβουλους κόμβους του επιτιθέμενου, δεν ενημερώνουν το θύμα για κάποια νόμιμη συναλλαγή που έρχεται σε σύγκρουση με την δική του, προκαλείται διπλή δαπάνη [28].

4.2.3.2 Sybil Attack

Μια επίθεση Sybil είναι μια επίθεση που βασίζεται στην ταυτότητα και απειλεί το δίκτυο peer-to-peer του blockchain [38] [43]. Η επικοινωνία μεταξύ των ομότιμων σε ένα δίκτυο blockchain λειτουργεί έτσι ώστε ένας κόμβος να παίρνει τις πληροφορίες του από τους υπόλοιπους κόμβους. Ένας επιτιθέμενος μπορεί να δημιουργήσει πολλές πλαστές ταυτότητες (sybil nodes), τις οποίες χρησιμοποιεί για να αποκτήσει μεγάλη επιρροή χειραγωγώντας λειτουργίες του δικτύου (όπως η δύναμη ψήφου) με αποτέλεσμα να υπονομεύεται η ακεραιότητα και η αξιοπιστία του δικτύου καθώς το θύμα θα παίρνει πληροφορίες μόνο από τους κόμβους sybil [53]. Όταν το θύμα τελικά περικυκλωθεί και αποκοπεί από άλλους κόμβους, ένας επιτιθέμενος μπορεί να τροφοδοτήσει το θύμα με παραπλανητικές πληροφορίες, οι οποίες θα οδηγήσουν σε επιθέσεις.

Για παράδειγμα, ο επιτιθέμενος μπορεί να αρνηθεί να αναμεταδώσει συναλλαγές και μπλοκ από τον κόμβο-στόχο, να πραγματοποιήσει διάφορες μορφές επιθέσεων διπλής δαπάνης, (δημιουργεί μια συναλλαγή, την επιβεβαιώσει με τους κόμβους Sybil και στη συνέχεια εκτελεί μια αντικρουόμενη συναλλαγή στο τίμιο τμήμα του δικτύου, ξοδεύοντας ουσιαστικά τα ίδια κεφάλαια δύο φορές), να φιλτράρει συγκεκριμένα συναλλαγές για τη διενέργεια διπλών δαπανών στην περίπτωση που ο στόχος δέχεται 0 επιβεβαιώσεις για τις συναλλαγές του, ή να νικήσει πρωτόκολλα ανωνυμοποίησης (αποκωδικοποιώντας την προσφερόμενη ανωνυμία εφόσον ελέγχεται το δίκτυο), όπως το Tor και το JAP, και να εκθέσει ευαίσθητα δεδομένα των προηγουμένως ανώνυμων χρηστών. [38]

Το πρωτόκολλο του Bitcoin θεωρείται ανθεκτικό στις επιθέσεις Sybil, επειδή θεωρεί ότι η αληθινή αλυσίδα είναι αυτή με τις περισσότερες αθροιστικές αποδείξεις εργασίας. Αποτέλεσμα είναι ένας νέος ομότιμος που εντάσσεται στο δίκτυο να χρειάζεται να συνδεθεί μόνο με έναν ειλικρινή ομότιμο για να βρει την αληθινή αλυσίδα. Αυτό είναι, επίσης, γνωστό ως αντίσταση Sybil, που σημαίνει ότι δεν είναι δυνατό για κάποιον να εξαπολύσει επίθεση εναντίον ενός κόμβου, δημιουργώντας πολλούς ανέντιμους ομότιμους που παρέχουν τις ψευδείς πληροφορίες. Εφόσον ένας μόνο τίμιος κόμβος μεταβιβάζει τα αληθινά δεδομένα σε έναν τίμιο κόμβο που δέχεται επίθεση Sybil, ο τελευταίος θα αγνοήσει όλες τις προσπάθειες (επίθεσης Sybil) από τους κόμβους του επιτιθέμενου.

Αν και η επίθεση Sybil έχει πολλές ομοιότητες με την επίθεση της Έκλειψης, εξακολουθούν να υπάρχουν διαφορές, ειδικά καθώς η πρώτη (Sybil) εστιάζει μόνο στην ταυτότητα με σκοπό να

ελέγξει το δίκτυο και να αρχίσει να αποκόπτει πληροφορίες από κόμβους, ενώ η επίθεση έκλειψης εστιάζει στην αποκοπή ενός συγκεκριμένου κόμβου-στόχου από το υπόλοιπο δίκτυο. Ένας εισβολέας χρειάζεται τη δυνατότητα να ελέγχει ή να δημιουργεί αρκετούς κόμβους Sybil (και σε αυτή την περίπτωση μπορεί να χρησιμοποιηθεί ένα botnet από τον επιτιθέμενο) για να παρακάμψει το εκλογικό αποτέλεσμα των ειλικρινών κόμβων, να ελέγξει το δίκτυο και να αποκλείσει τους ειλικρινείς κόμβους αργά από το πραγματικό δίκτυο.

4.2.3.3 Χρονοκλοπή (Timejacking)

Η χρονοκλοπή είναι μια επίθεση που επιχειρεί να διαστρεβλώσει το χρονισμό ενός κόμβου-στόχου άρα και της χρησιμοποιούμενες χρονοσφραγίδες του (timestamps), συνδέοντας έναν στόχο με πολλούς ομότιμους που ελέγχονται από τον επιτιθέμενο (πχ. με μια επίθεση έκλειψης) και αναφέροντας μια λανθασμένη ώρα στον στόχο ως την σωστή [38]. Επομένως, η επίθεση αυτή λογικά απαιτεί την επιτυχή διενέργεια μιας άλλης προγενέστερης επίθεσης ως βασική προϋπόθεση για να πραγματοποιηθεί. Ο στόχος μιας επίθεσης timejacking είναι να εξαπατήσει τον κόμβο κάνοντάς τον να πιστέψει ότι ορισμένες συναλλαγές ή μπλοκ δημιουργήθηκαν σε διαφορετικό χρόνο από ό,τι στην πραγματικότητα. Ένας κόμβος χρησιμοποιεί τον χρόνο του δικτύου για την επικύρωση νέων μπλοκ. Με τη διαστρέβλωση της άποψης ενός κόμβου για τον χρόνο δικτύου, θα απορρίψει νέα μπλοκ με χρονοσφραγίδα μεγαλύτερη από μια προκαθορισμένη διάρκεια. Όπως οι επιθέσεις Sybil και Eclipse, αυτό θα επέτρεπε στους κακόβουλους κόμβους να απομονώσουν ουσιαστικά τον κόμβο-στόχο από το υπόλοιπο δίκτυο, καθώς έχει λανθασμένη εικόνα για το blockchain.

Με την απομόνωση ενός κόμβου-στόχου, θα μπορούσαν να δημιουργηθούν και να σταλούν στον κόμβο-στόχο δόλιες συναλλαγές. Με τη συνέχιση της επίθεσης, θα μπορούσαν να σταλούν στον στόχο δόλιες επιβεβαιώσεις, έως ότου ο στόχος αποδεχτεί τη συναλλαγή ως επιβεβαιωμένη. Ακόμη πιο προηγμένες επιθέσεις θα μπορούσαν να διεξαχθούν σε πολλαπλούς στόχους για να επιταχύνουν τα ρολόγια μιας πισίνας εξόρυξης, αυξάνοντας έτσι τη διαφορά χρόνου μεταξύ της πισίνας εξόρυξης και ενός κόμβου-στόχου. Εάν ο κόμβος-στόχος είναι ανθρακωρύχος, θα κάνει τον ανθρακωρύχο να απομονωθεί από ολόκληρο το δίκτυο, και η υπολογιστική ισχύς του ανθρακωρύχου θα σπαταληθεί για μεγάλο χρονικό διάστημα.

Στο Bitcoin οι πλήρεις κόμβοι διατηρούν ένα εσωτερικό μετρητή που δηλώνει το χρόνο του δικτύου. Ο χρόνος αυτός λαμβάνεται τακτικά με τη λήψη ενός μηνύματος από τους γειτονικούς ομότιμους και τον υπολογισμό της διάμεσης τιμής του κατά την διάρκεια της φάσης εκκίνησης. Αν ο διάμεσος χρόνος όλων αυτών των κόμβων υπερβαίνει τα 70 λεπτά, ο μετρητής χρόνου δικτύου επανέρχεται στον χρόνο συστήματος του κόμβου καθώς θεωρείται πολύ μεγάλος και συνεπώς "παράνομος". Αν οι γειτονικοί κόμβοι ελέγχονται από έναν επιτιθέμενο, μπορούν να χρησιμοποιηθούν για να στείλουν διαφορετικές χρονικές σφραγίδες με αποτέλεσμα να στέλνουν διάμεσο χρόνο μικρότερο από 70 λεπτά. Επιπλέον, ένα μπλοκ απορρίπτεται από ένα κόμβο αν η χρονοσφραγίδα του υπερβαίνει το χρόνο δικτύου κατά 70 λεπτά, καθώς έτσι φαίνεται παράνομο στον κόμβο-στόχο και θα απορριφθεί από αυτόν. [28] [43].

4.2.3.4 Επιθέσεις DNS

Όταν ένας κόμβος εισέρχεται στο δίκτυο blockchain για πρώτη φορά, δεν γνωρίζει τους ενεργούς ομότιμους στο δίκτυο. Για να εντοπίσει τους ενεργούς ομότιμους (που προσδιορίζονται από τις διευθύνσεις IP τους) στο δίκτυο, απαιτείται ένας μηχανισμός εκκίνησης (bootstrapping). Το σύστημα ονοματοδοσίας τομέα (Domain Name System) μπορεί να χρησιμοποιηθεί ως μηχανισμός εκκίνησης. Ειδικότερα, DNS seeds υποβάλλονται σε ερώτημα από κόμβους κατά τη σύνδεση στο δίκτυο για τη λήψη περαιτέρω πληροφοριών σχετικά με άλλους ενεργούς ομότιμους. Το αρχικό ερώτημα DNS επιστρέφει μία ή περισσότερες εγγραφές μαζί με τις αντίστοιχες διευθύνσεις IP των υπολογιστών που δέχονται εισερχόμενες συνδέσεις. Μόλις ο νέος κόμβος δημιουργήσει συνδέσεις με τους ομότιμους, μπορεί να στείλει την εντολή addr με αριθμούς θύρας για να δημιουργήσει συνδέσεις με άλλους ομότιμους [28].

Έχει αναφερθεί στον οδηγό προγραμματιστών συστημάτων Bitcoin [54] ότι το DNS ανοίγει εν γένει μια ευρεία επιφάνεια επίθεσης στα δίκτυα Bitcoin, καθώς γίνεται ανακατεύθυνση του κόμβου σε κακόβουλους κόμβους και προετοιμάζει το έδαφος για άλλες επιθέσεις όπως αυτή της έκλειψης. Ειδικότερα, η επίλυση DNS (DNS resolution) είναι ευάλωτη σε επιθέσεις man-in-the-middle (ενδιάμεσου), δηλητηρίαση κρυφής μνήμης (cache poisoning), πλημμύρας DNS (DNS flooding) και DNS hijacking μεταξύ πολλών άλλων.

DNS MitM (man-in-the-middle): Σε μια επίθεση DNS MitM, ένας επιτιθέμενος τοποθετείται μεταξύ των κόμβων του blockchain και του DNS Server, και "κρυφακούει" τα δεδομένα που ανταλλάσσονται μεταξύ των μερών. Αυτό μπορεί να εκθέσει λεπτομέρειες συναλλαγών, ιδιωτικά κλειδιά και άλλες ευαίσθητες πληροφορίες, καθώς ο επιτιθέμενος παρεμβάλλεται μεταξύ του διακομιστή DNS και των κόμβων και μπορεί να τους παραπλανήσει ώστε να συνδεθούν με κακόβουλους κόμβους. Ουσιαστικά πλαστογραφεί την ταυτότητα ενός μέρους της επικοινωνίας ώστε να ξεγελάσει ή να κλέψει πληροφορίες από κάποιον κόμβο.

DNS cache poisoning: Επίσης γνωστή ως DNS spoofing είναι ένας τύπος επίθεσης στην οποία ένας εισβολέας εισάγει ψευδείς πληροφορίες DNS στην cache (κρυφή μνήμη) ενός DNS resolver (αναλυτή). Ο στόχος είναι να παραπλανήσει τον επιλυτή DNS ώστε να αποθηκεύσει λανθασμένα δεδομένα DNS. Όταν οι χρήστες ρωτούν τον επιλυτή DNS για τις ίδιες πληροφορίες, τους παρέχονται τα "δηλητηριασμένα" δεδομένα, τα οποία μπορούν να τους ανακατευθύνουν σε κακόβουλους ιστότοπους ή διευθύνσεις IP. Η δηλητηρίαση της κρυφής μνήμης DNS μπορεί να επηρεάσει πολλούς χρήστες και συσκευές που βασίζονται στον εκτεθειμένο επιλυτή DNS.

DNS flooding: Μια επίθεση πλημμύρας DNS, γίνεται συχνά με τη μορφή άρνησης υπηρεσίας DDoS (επίθεση 4.3.5), και περιλαμβάνει τη υπερφόρτωση των διακομιστών DNS ή των επιλυτών με υπερβολικό όγκο ερωτημάτων DNS. Ο στόχος μιας τέτοιας επίθεσης είναι να καταναλώσει τους πόρους της υποδομής DNS, καθιστώντας την ανίκανη να ανταποκριθεί σε νόμιμα αιτήματα DNS. Αυτό οδηγεί τους χρήστες να μην μπορούν να έχουν πρόσβαση σε ιστότοπους, κόμβους ή άλλες υπηρεσίες blockchain, ή έστω να έχουν μια βραδύτερη πρόσβαση - γενικότερα προκαλεί αστάθεια στο δίκτυο.

DNS hijacking: Το DNS hijacking, γνωστό και ως ανακατεύθυνση DNS, περιλαμβάνει την τροποποίηση των εγγραφών DNS του κόμβου/μηχανήματος ενός χρήστη για την ανακατεύθυνση του χρήστη από νόμιμες ιστοσελίδες ή υπηρεσίες σε κακόβουλες. Στο DNS hijacking, ο επιτιθέμενος χειρίζεται απευθείας τις εγγραφές DNS για να αλλάξει τον προορισμό ενός τομέα. Αυτός ο τύπος επίθεσης επικεντρώνεται συνήθως σε έναν συγκεκριμένο χρήστη σε αντίθεση με

το DNS cache poisoning που έχει ευρύτερο αντίκτυπο και μπορεί να επηρεάσει πολλούς χρήστες ταυτόχρονα.

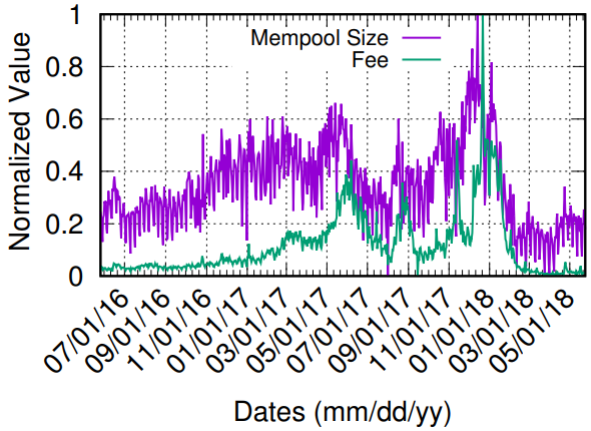
4.2.3.5 Επιθέσεις DDoS

Μία από τις πιο κοινές επιθέσεις σε επίπεδο δικτύου είναι η επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS) [28]. Οι DDoS επιθέσεις σε επίπεδο δικτύου προκαλούν κορεσμό του δικτύου, καταναλώνοντας μεγάλο μέρος του διαθέσιμου εύρους ζώνης του δικτύου. Η τεχνολογία blockchain με το σύστημα peer-to-peer, είναι επιρρεπής σε επιθέσεις DDoS. Οι επιθέσεις DDoS εκδηλώνονται με διάφορους τρόπους, ανάλογα με τη φύση της εφαρμογής, την αρχιτεκτονική του δικτύου και τη συμπεριφορά των ομότιμων. Σε αυτό το είδος επίθεσης, ο επιτιθέμενος συνήθως χρησιμοποιεί ένα σύνολο συσκευών που έχουν πέσει θύματα πειρατείας (πχ. botnet) για να πλημμυρίσει το δίκτυο blockchain με ένα υπερβολικό αριθμό αιτημάτων που καταστρέφουν την ικανότητα του δικτύου να εξυπηρετήσει την κίνηση των υπολοίπων/νόμιμων [38]. Πολλές φορές η άρνηση υπηρεσίας είναι εφικτή μετά από μια επιτυχημένη επίθεση Sybil, καθώς ο επιτιθέμενος που έχει γεμίσει το δίκτυο με πολλούς κακόβουλους κόμβους (ταυτότητες) μπορεί να γεμίσει το δίκτυο με αιτήματα από τους κόμβους αυτούς ή και να επηρεάσει ειλικρινείς κόμβους στην προώθηση αιτημάτων με τελικό σκοπό την άρνηση υπηρεσίας.

Μια επίθεση DDoS μπορεί να προκληθεί και μετά από μια επίθεση 51%. Όταν ένα δίκτυο blockchain δέχεται επίθεση 51%, απαιτούνται σημαντικοί υπολογιστικοί πόροι για τη διατήρηση και την ασφάλεια του δικτύου. Οι κόμβοι, οι ανθρακωρύχοι και οι επικυρωτές του δικτύου πρέπει να διαθέσουν περισσότερους πόρους για την επαλήθευση και την επικύρωση των συναλλαγών, γεγονός που μπορεί να οδηγήσει σε αυξημένη συμφόρηση του δικτύου και εν τέλει σε άρνηση υπηρεσίας. Σε ορισμένες περιπτώσεις, στην αντίθετη κατεύθυνση, οι επιτιθέμενοι μπορεί να εξαπολύσουν επίθεση DDoS στο blockchain ώστε να διευκολύνουν την διεξαγωγή και την επιτυχίας μιας επίθεσης 51%. Η επίθεση DDoS χρησιμεύει ως αντιπερισπασμός, κατακλύζοντας το δίκτυο ή τους διακομιστές του στόχου με τεράστιο όγκο παράνομης κυκλοφορίας. Κατά τη διάρκεια αυτού του χάους, ο επιτιθέμενος μπορεί να εκμεταλλευτεί περαιτέρω τα τρωτά σημεία και να εκτελέσει πιο αποτελεσματικά την επίθεση 51%.

Πλημμύρες στην πισίνα μνήμης (Mempool): Μια άλλη μορφή επίθεσης DDoS πραγματοποιείται στις πισίνες μνήμης (mempools) των κρυπτονομισμάτων. Ειδικότερα, τα mempool γεμίζονται με ανεπιβεβαίωτες συναλλαγές από τον επιτιθέμενο με σκοπό να αυξηθεί το τέλος των συναλλαγών των συμμετεχόντων. Επομένως, ορισμένοι χρήστες μπορεί να πληρώσουν το αυξημένο τέλος για να εξυπηρετηθούν ενώ άλλοι χρήστες μπορεί να μην έχουν την ευχέρεια ή να μην επιθυμούν να πληρώσουν το τέλος αυτό. Επομένως, για τους τελευταίους χρήστες έχει συντελεστεί ένα είδος άρνησης υπηρεσίας διότι εν τέλει δεν μπορούν να επικυρώσουν και να αποθηκεύσουν τις συναλλαγές τους στο δίκτυο..

Τα mempools λειτουργούν ως μια κρυφή μνήμη των ανεπιβεβαίωτων συναλλαγών. Αν και το μέγεθος μπλοκ είναι περιορισμένο στα κρυπτονομίσματα, μια mempool δεν έχει όριο μεγέθους. Ωστόσο, οι χρήστες εκτιμούν το μέγεθος των mempools για να δώσουν προτεραιότητα στις συναλλαγές τους. Αν υπάρχουν περισσότερες συναλλαγές στο mempool, τότε ο ανταγωνισμός για την εξόρυξη γίνεται υψηλός. Προκειμένου να δώσουν προτεραιότητα στις συναλλαγές τους, οι χρήστες αρχίζουν να πληρώνουν περισσότερα τέλη εξόρυξης ως κίνητρο για τους ανθρακωρύχους.



Εικόνα 12. Γράφημα Τέλους Συναλλαγών - Μεγέθους Mempool

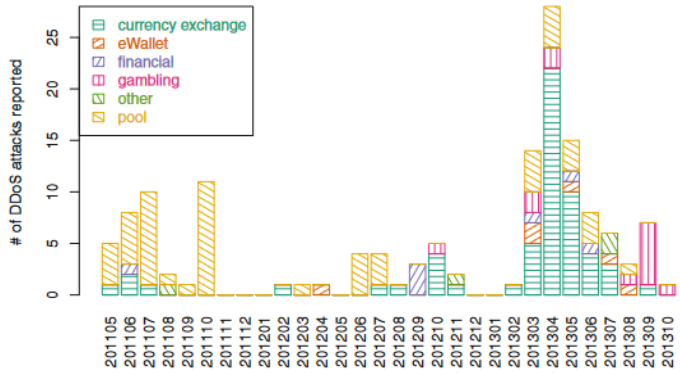
Στην Εικόνα 12 φαίνεται πως όσο το μέγεθος του mempool μεγαλώνει, το τέλος που πληρώνεται στους ανθρακωρύχους μεγαλώνει επίσης.

Στο [55], εντοπίστηκε μια επίθεση χαμηλού κόστους DDoS σε εφαρμογές Blockchain στην οποία ο αντίπαλος μαζί με τους κόμβους Sybil (οπότε θα πρέπει να έχει προηγηθεί μια επίθεση Sybil) μπορεί να πλημμυρίσει τα mempools με ανεπιβεβαίωτες συναλλαγές. Μια τέτοια επίθεση δημιουργεί πανικό στους νόμιμους χρήστες που μπαίνουν στον πειρασμό να πληρώσουν υψηλότερα τέλη εξόρυξης για να δώσουν προτεραιότητα στις συναλλαγές τους, οπότε κάποιοι χρήστες πληρώνουν παραπάνω και κάποιοι άλλοι δεν έχουν γρήγορη εξυπηρέτηση (το οποίο είναι ένα σύμπτωμα επίθεσης άρνησης υπηρεσίας). Παράλληλα οι συναλλαγές του επιτιθέμενου δεν εξορύσσονται και έχουν πολύ μικρό τέλος εξόρυξης.

Επιθέσεις DDoS σε δημόσια blockchain: Σε δημόσια blockchain η έναρξη μιας τέτοιας επίθεσης μπορεί να είναι δαπανηρή. Ο επιτιθέμενος πρέπει να έχει είτε την πλειοψηφία του συνολικού ποσοστού κατακερματισμού, την πλειοψηφία των μετοχών (stake), ή τον έλεγχο πάνω από 50% ομοτίμων δικτύου. Λαμβάνοντας υπόψη ότι οι δημόσιες εφαρμογές Blockchain, όπως το Bitcoin έχουν περισσότερους από 10.000 ενεργούς πλήρεις κόμβους [57], είναι ανέφικτο για τον επιτιθέμενο να ξεκινήσει μια τέτοια επιτυχημένη επίθεση.

Επιθέσεις DDoS σε ιδιωτικά blockchain: Σε ιδιωτικά blockchain που βασίζονται στο PBFT, μια επίθεση DDoS μπορεί να ξεκινήσει αν ο αντίπαλος ελέγχει 33% από τις ρέπλικες [56]. Στα ιδιωτικά Blockchain, το μέγεθος του δικτύου είναι γνωστό στους εν μέρει συμμετέχοντες κόμβους, το οποίο επιτρέπει στον επιτιθέμενο να υπολογίσει τον αριθμό των sybil κόμβων που χρειάζεται να εισάγει στο δίκτυο για μια επίθεση. Αν υποθέσουμε ότι ο επιτιθέμενος ελέγχει f sybil κόμβους έτσι ώστε το συνολικό μέγεθος του δικτύου να είναι $n < 3f + 1$, τότε ο επιτιθέμενος θα μπορεί να ξεκινήσει μια επίθεση DDoS για να σταματήσει τη διαδικασία επαλήθευσης. Για κάθε συναλλαγή που αποστέλλεται από τον πρωτεύοντα, οι sybil ρεπλίκες δεν απαντούν με τις εγκρίσεις τους. Δεδομένου ότι ο πρωτεύον κόμβος θα χρειαστεί εγκρίσεις από τουλάχιστον $3f + 1$ ρεπλίκες, δεν θα είναι σε θέση να επεξεργαστεί οποιαδήποτε συναλλαγή και οι δραστηριότητες του συστήματος θα σταματήσουν. Αυτό είναι ιδανικό επακόλουθο για τον επιτιθέμενο για μια επίθεση DDoS.

Στο [96] πραγματοποιήθηκε μια εμπειρική μελέτη των επιθέσεων DDoS και καταγράφηκαν 142 μοναδικές επιθέσεις DDoS στο Bitcoin μεταξύ Μαΐου 2011 και Οκτωβρίου 2013.



Εικόνα 13. Επιθέσεις DDoS ανά Κατηγορία Χρησιμοποίησης

Στην Εικόνα 13 παρατηρείται ο αριθμός των επιθέσεων DDoS σε διάφορες κατηγορίες χρήσης του Bitcoin Blockchain ανάμεσα στον Μάιο 2011 και Οκτώβρη 2013. Οι κατηγορίες κατά σειρά είναι οι εξής: συναλλαγές νομισμάτων, ηλεκτρονικό πορτοφόλι, οικονομικά, στοιχηματισμός, άλλο και mempool.

4.2.3.6 BGP (Border Gateway Protocol) Hijack Attack

Το BGP (Border Gateway Protocol) είναι ένα πρωτόκολλο δρομολόγησης που ρυθμίζει τον τρόπο προώθησης των πακέτων IP στον προορισμό τους. Για την παρακολούθηση της δικτυακής κίνησης του blockchain, οι επιτιθέμενοι είτε εκμεταλλεύονται είτε χειρίζονται τη δρομολόγηση BGP. Η πειρατεία στο BGP συνήθως απαιτεί τον έλεγχο των χειριστών δικτύου, οι οποίοι θα μπορούσαν δυνητικά να χρησιμοποιηθούν για να καθυστερήσουν τα μηνύματα δικτύου. Παρόλα αυτά μια τέτοιου είδους επίθεση είναι πολύ σπάνιο καθώς πρέπει ο επιτιθέμενος να έχει πολύ μεγάλο επίπεδο γνώσεων δικτύου καθώς και πρόσβαση στην υποδομή ενός παρόχου υπηρεσιών διαδικτύου (ISP) ή ενός αυτόνομου συστήματος (AS). [44]

Στις περισσότερες εφαρμογές Blockchain, υπάρχουν δύο τύποι κόμβων, οι πλήρεις κόμβοι (full nodes) και ελαφρείς κόμβοι (lightweight nodes) [28]. Δεδομένου ότι οι ελαφρείς κόμβοι αντλούν την άποψή τους για την αλυσίδα Blockchain από τους πλήρεις κόμβους, όταν ένας πλήρης κόμβος είναι σε κίνδυνο, όλοι οι σχετιζόμενοι ελαφρείς κόμβοι είναι επίσης σε κίνδυνο. Οι πλήρεις κόμβοι σε ένα δίκτυο Blockchain είναι χωρικά κατανεμημένοι σε όλο το Διαδίκτυο. Η ροή της κυκλοφορίας στο Διαδίκτυο ελέγχεται από Παρόχους Υπηρεσιών Διαδικτύου (Internet Service Providers ή ISPs), οι οποίοι είναι ιδιοκτήτες ενός ή περισσότερων Αυτόνομων Συστημάτων (Autonomous Systems ή ASes), υπεύθυνων για τη διαχείριση της δρομολόγησης της κυκλοφορίας. [58].

Η χωρική συγκέντρωση των κόμβων σε ένα AS ή έναν ISP τους καθιστά ευάλωτους σε επιθέσεις δρομολόγησης, όπως το BGP Hijacking. Συνήθως, σε περίπτωση μιας τέτοιας επίθεσης, ένας ISP (ο οποίος μπορεί να είναι υπό τον έλεγχο ενός επιτιθέμενου, είτε σκόπιμα είτε λόγω λανθασμένης ρύθμισης, ή να είναι κακόβουλος), εκτρέπει την κυκλοφορία του διαδικτύου διαφημίζοντας μια ψεύτικη ανακοίνωση στο σύστημα δρομολόγησης του διαδικτύου. Ένα επιτιθέμενο AS μπορεί να διαχειριστεί και να υποκλέψει την κυκλοφορία (από ένα AS που φιλοξενεί την πλειοψηφία των κόμβων ενός Blockchain). Αυτό μπορεί να διαταράξει τη ροή πολύτιμων πληροφοριών, συμπεριλαμβανομένων των συναλλαγών και των μπλοκ, προς τους κόμβους που φιλοξενούνται από το σύστημα-στόχο. Όταν οι κόμβοι του θύματος είναι ανθρακωρύχοι ή δεξαμενές εξόρυξης, ο

επιτιθέμενος μπορεί να μειώσει σημαντικά το ποσοστό κατακερματισμού της εφαρμογής Blockchain, επηρεάζοντας έτσι τις δραστηριότητες του συστήματος επειδή ουσιαστικά αυτοί οι κόμβοι απομονώνονται.

Στο [59] μελετήθηκε ότι με την πειρατεία λιγότερων από 100 προθεμάτων του πρωτοκόλλου συνοριακής πύλης (Border Gateway Protocol) στο Bitcoin, ένας επιτιθέμενος μπορεί να απομονώσει έως και το 50% του ρυθμού κατακερματισμού του δικτύου. Διερεύνησαν περαιτέρω ότι το 60% του συνόλου της κυκλοφορίας Bitcoin διασχίζει μόνο τρεις παρόχους υπηρεσιών Διαδικτύου (ISPs). Έτσι, κάθε μήνα, πάνω από 100 κόμβοι Bitcoin υποφέρουν από επιθέσεις δρομολόγησης και BGP hijacks. Επιπλέον, οι ερευνητές εκτίμησαν ότι οι επιθέσεις δρομολόγησης μπορούν να καθυστερήσουν τη μετάδοση μπλοκ μέχρι και 20 λεπτά. Συνεπώς, οι επιθέσεις δρομολόγησης μπορούν να καθυστερήσουν τη μετάδοση δύο ή περισσότερων μπλοκ σε μια ομάδα κόμβων.

Τέτοιες καθυστερήσεις αυξάνουν την πιθανότητα άλλων ευπαθειών και επιθέσεων, όπως η διακλάδωση (fork) ενός Blockchain, η καθυστέρηση συναίνεσης και η διπλή δαπάνη.

Στις 3 Φεβρουαρίου 2022 χάκερς έκλεψαν περίπου 1,9 εκατομμύρια δολάρια από τη νοτιοκορεατική πλατφόρμα κρυπτονομισμάτων KLAYswap, αφού πραγματοποίησαν μια πειρατεία BGP εναντίον της υποδομής διακομιστή ενός από τους παρόχους της πλατφόρμας [68].

4.2.4 Επιθέσεις στα Έξυπνα Συμβόλαια

4.2.4.1 Επιθέσεις Επανεισαγωγής (Reentrancy Attacks)

Σε μια περίπτωση που αφορά ειδικά το Ethereum, είναι δυνατόν για έναν εισβολέα να διεκδικήσει ολόκληρο το υπόλοιπο ενός χρήστη καλώντας αναδρομικά μια λειτουργία των ERC20 μαρκών (tokens) του. Το ERC-20 είναι ένα τεχνικό πρότυπο που χρησιμοποιείται για έξυπνα συμβόλαια στο Ethereum Blockchain. Το πρότυπο ERC-20 ορίζει ένα σύνολο κανόνων που μπορούν να ακολουθήσουν οι προγραμματιστές για να δημιουργήσουν τις δικές τους μάρκες (tokens) (δηλαδή κρυπτονομίσματα) στο Ethereum Blockchain. Τα token που έχουν δημιουργηθεί με βάση το πρότυπο ERC-20 είναι συμβατά μεταξύ τους και μπορούν να διαπραγματεύονται σε αποκεντρωμένα χρηματιστήρια (DEX) που βασίζονται στο Ethereum, όπως το Uniswap και το Sushiswap. [60]

Οι επιθέσεις επανεμφάνισης περιλαμβάνουν την επαναλαμβανόμενη κλήση ενός ευάλωτου έξυπνου συμβολαίου, το οποίο δεν διασφαλίζει σωστά την κατάσταση ή δεν ελέγχει τις συνθήκες. Καθώς συμβαίνει αυτό, η κατάσταση του λογαριασμού του συμβολαίου αλλάζει μετά την κλήση της λειτουργίας και πριν από την ολοκλήρωση του συμβολαίου. [61]

Πιο συγκεκριμένα, το συμβόλαιο καλείται αναδρομικά με την μέθοδο call.value(), κάτι που όμως μπορεί να δουλέψει μόνο εφόσον ένας μη προσεκτικός χρήστης δεν ενημερώσει το υπόλοιπο του πριν στείλει το ether του [28]. Η μέθοδος αυτή καλείται μέσω ενός έξυπνου συμβολαίου που έχει φτιάξει ένας κακόβουλος χρήστης για τις συγκεκριμένες περιπτώσεις.

Αυτό αξιοποιείται από έναν επιτιθέμενο χρησιμοποιώντας την ενδιάμεση κατάσταση για να καλέσει επανειλημμένα το έξυπνο συμβόλαιο. Αν το συμβόλαιο που επικαλείται περιλαμβάνει πολύτιμα δεδομένα όπως κρυπτονομίσματα, αυτό θα μπορούσε να οδηγήσει σε παράνομη κλοπή κρυπτονομισμάτων και έτσι απώλεια χρημάτων [62].

Παράδειγμα εκτέλεσης της επίθεσης με βήματα: [63]

1. Ο επιτιθέμενος βρίσκει ένα ευάλωτο έξυπνο συμβόλαιο που διαθέτει μια λειτουργία που επιτρέπει στους χρήστες να αποσύρουν το υπόλοιπο ETH τους.
2. Στην συνέχεια ο επιτιθέμενος αναπτύσσει το δικό του κακόβουλο συμβόλαιο.
3. Το συμβόλαιο του επιτιθέμενου αλληλοεπιδρά με το ευάλωτο συμβόλαιο και ξεκινά μια ανάληψη, στέλνοντας ένα αίτημα στο ευάλωτο συμβόλαιο για τη μεταφορά ETH.
4. Επίθεση επανεισαγωγής: Το συμβόλαιο του επιτιθέμενου περιλαμβάνει μια συνάρτηση επανάκλησης που καλείται από το ευάλωτο συμβόλαιο ως μέρος της διαδικασίας απόσυρσης. Αντί να ενημερώνει απλώς τη δική του κατάσταση, το ευάλωτο συμβόλαιο πραγματοποιεί μια εξωτερική κλήση στο συμβόλαιο του επιτιθέμενου.
5. Το συμβόλαιο του επιτιθέμενου καλεί επανειλημμένα πίσω το ευάλωτο συμβόλαιο, προκαλώντας την απόσυρση περισσότερων ETH με κάθε κλήση. Οι αναδρομικές κλήσεις συνεχίζονται μέχρι να εξαντληθεί το υπόλοιπο ETH του ευάλωτου συμβολαίου.
6. Ο επιτιθέμενος αποσύρει επιτυχώς περισσότερα ETH από το ευάλωτο συμβόλαιο από όσα θα έπρεπε να του επιτραπούν, κλέβοντας ουσιαστικά ETH από το συμβόλαιο.

4.2.4.2 Επιθέσεις Υπερχείλισης (Overflow Attacks)

Οι έξυπνες συμβάσεις συχνά περιλαμβάνουν αριθμητικές πράξεις, όπως η πρόσθεση και η αφαίρεση, για διάφορους σκοπούς, όπως ο υπολογισμός υπολοίπων, ο χειρισμός συναλλαγών και η ενημέρωση των καταστάσεων των συμβάσεων. Η υπερχείλιση ακεραίων αριθμών συμβαίνει όταν το αποτέλεσμα μιας αριθμητικής πράξης υπερβαίνει τη μέγιστη αναπαραγώγιμη τιμή για έναν συγκεκριμένο τύπο δεδομένων. Στο Ethereum, η μέγιστη ποσότητα του Ether σε μια μεταβλητή μπορεί να είναι 2^256. [63]

Σε ορισμένες περιπτώσεις, μια επίθεση υπερχείλισης μπορεί να διαταράξει την κανονική λογική και λειτουργία ενός έξυπνου συμβολαίου, καθιστώντας το μη λειτουργικό ή απρόβλεπτο. Επιπλέον μπορεί να προκαλέσει ακούσιες αλλαγές στις μεταβλητές κατάστασης του συμβολαίου, οδηγώντας σε αλλοίωση δεδομένων ή ανακρίβειες στις εγγραφές του συμβολαίου. Εάν μια επίθεση υπερχείλισης χειραγωγήσει το υπόλοιπο ενός συμβολαίου, ένας εισβολέας μπορεί δυνητικά να αποσύρει περισσότερα χρήματα από όσα κατέθεσε. Αυτό έχει ως αποτέλεσμα άμεση οικονομική απώλεια για το συμβόλαιο και τους χρήστες του.

Για παράδειγμα, για ένα έξυπνο συμβόλαιο για online στοιχήματα, αν κάποιος στείλει ether αξίας μεγαλύτερης από 2^256, τότε το στοίχημα θα ρυθμιστεί σε 0. Η εκμετάλλευση αυτής της ευπάθειας είναι εξαιρετικά απίθανη, επειδή απαιτεί από τον αποστολέα να στείλει ένα ποσό μεγαλύτερο από το μέγιστο, το οποίο στη συνέχεια θα μηδενιστεί [28], πράγμα που προφανώς δεν συμφέρει τον αποστολέα.

4.2.4.3 Επιθέσεις με Σύντομες Διευθύνσεις (Short Address Attacks)

Η "επίθεση σύντομης διεύθυνσης" στο πλαίσιο των έξυπνων συμβολαίων είναι ένας τύπος ευπάθειας που εμφανίζεται όταν ένα συμβόλαιο δεν επικυρώνει σωστά το μήκος των δεδομένων εισόδου που λαμβάνει. Συγκεκριμένα, αναφέρεται στην περίπτωση κατά την οποία ένα έξυπνο συμβόλαιο εμπιστεύεται μια διεύθυνση εισόδου ώστε να έχει ένα συγκεκριμένο μήκος και ένας επιτιθέμενος παρέχει μια διεύθυνση με ανεπαρκείς χαρακτήρες, εκμεταλλευόμενος αυτή την ευπάθεια.

Η πιο συχνή επίπτωση μιας επίθεσης σύντομης διεύθυνσης μπορεί να προκαλέσει αποτυχία της εκτέλεσης μιας συνάρτησης εντός του συμβολαίου. Αυτό μπορεί να οδηγήσει στην αλλαγή διεύθυνσης μεταφοράς περιουσιακών στοιχείων.

Διαδικασία εκτέλεσης της επίθεσης:

1. Ένα έξυπνο συμβόλαιο αναμένει από έναν χρήστη να παραδώσει μια διεύθυνση ως είσοδο και υποθέτει ότι η διεύθυνση θα έχει ένα συγκεκριμένο μήκος (π.χ. 40 χαρακτήρες στην περίπτωση των διευθύνσεων του Ethereum). Αυτός είναι ένας κοινός μηχανισμός επικύρωσης σε πολλές συμβάσεις.
2. Ένας επιτιθέμενος στέλνει μια συναλλαγή στο συμβόλαιο και παρέχει μια διεύθυνση που είναι μικρότερη από το αναμενόμενο μήκος.
3. Το έξυπνο συμβόλαιο, χωρίς κατάλληλη επικύρωση, αποδέχεται τη διεύθυνση εισόδου και προχωρά στην προβλεπόμενη λειτουργία. Αυτή η λειτουργία μπορεί να περιλαμβάνει τη μεταφορά περιουσιακών στοιχείων ή την ενημέρωση της κατάστασης.
4. Επειδή η διεύθυνση του επιτιθέμενου είναι μικρότερη από την αναμενόμενη, ενδέχεται να επικαλύπτεται με άλλα τμήματα των δεδομένων εισόδου. Αυτό μπορεί να οδηγήσει σε απρόβλεπτες συνέπειες, όπως η μεταφορά περιουσιακών στοιχείων σε μη προβλεπόμενη

διεύθυνση (η οποία προκύπτει από τη μικρότερη διεύθυνση και τους υπολειπόμενους χαρακτήρες που αφορούν μια άλλη είσοδο).

4.2.5 Κλασικές Επιθέσεις Ασφάλειας

4.2.5.1 Κρυπτοκλοπή (Cryptojacking)

Η κρυπτοκλοπή είναι μια μορφή επίθεσης που εξαπολύεται σε διαδικτυακές και cloud-based (βασισμένες στο νέφος) υπηρεσίες για την παράνομη εκτέλεση PoW για κρυπτονομίσματα που βασίζονται σε Blockchain, χωρίς συγκατάθεση.

Λόγω της αυξανόμενης ζήτησης υπολογιστικής ισχύος, η εξόρυξη γίνεται όλο και λιγότερο κερδοφόρα για το άτομο. Αυτό οδηγεί σε περιπτώσεις κρυπτοκλοπής, όπου ένας εισβολέας, ορμώμενος λόγω της δίψας του για περισσότερο κέρδος, χρησιμοποιεί την υποδομή του θύματος για να εξορύξει συγκαλυμμένα νέα μπλοκ.

Οι δύο πιο συνηθισμένοι τύποι είναι οι βασισμένη σε νέφος (cloud-based) και βασισμένη στο διαδίκτυο (web-based) κρυπτοκλοπή.

Στον τύπο που είναι βασισμένος σε νέφος, οι κακόβουλοι ανθρακωρύχοι έχουν βρει έναν τρόπο να επεκτείνουν τη δύναμη κατακερματισμού τους, καταλαμβάνοντας επεξεργαστές απομακρυσμένων μηχανημάτων/συσκευών για εξόρυξη. Αυτή η επίθεση είναι γνωστή ως κρυφή εξόρυξη ή επίθεση κρυπτοκλοπής και περιλαμβάνει την πειρατεία μιας συσκευής-στόχου από τον επιτιθέμενο για την εκτέλεση υπολογισμών PoW. Αρχικά, οι επιθέσεις αυτές εξαπολύθηκαν εναντίον παρόχων υπηρεσιών νέφους (cloud), όπου κακόβουλοι χρήστες εκτελούσαν κρυφές εργασίες εξόρυξης σε εικονικές μηχανές και εξαντλούσαν τους πόρους του νέφους. Οι επιτιθέμενοι συνήθως παίρνουν τον έλεγχο των εικονικών μηχανών με ευπάθειες του τύπου: μη ενημερωμένο λογισμικό του λειτουργικού τους συστήματος, αδύναμη ταυτοποίηση και προεπιλεγμένοι κωδικοί (ή αδύναμοι γενικά κωδικοί) ή εσφαλμένα διαμορφωμένος έλεγχο πρόσβασης (δηλαδή υπερβολικά επιτρεπτά δικαιώματα).

Όμως η πιο πρόσφατη καθώς και η πιο διαδεδομένη μορφή της επίθεσης κρυπτοκλοπής είναι αυτή εντός του προγράμματος περιήγησης / φυλλομετρητή (web browser), η οποία μετατρέπει ιστότοπους σε δεξαμενές εξόρυξης. Η κρυπτοκλοπή βασισμένη στο διαδίκτυο, εγχέει κακόβουλο κώδικα JavaScript σε ιστοσελίδες, ο οποίος εκτελείται όταν φορτώνονται οι ιστοσελίδες και στέλνει μάρκες εξόρυξης σε όλους τους επισκέπτες των ιστοσελίδων αυτών χωρίς τη συγκατάθεσή τους. Ως αποτέλεσμα, οι φυλλομετρητές των επισκεπτών αυτών υπολογίζουν και στέλνουν πίσω τους κατακερματισμούς.

Ένας επιτιθέμενος πρέπει να εισάγει τον κακόβουλο κώδικα JavaScript στην ιστοσελίδα (πχ. κατά την εισαγωγή δεδομένων από μια φόρμα που δεν ελέγχονται). Όταν αυτή φορτωθεί από τον φυλλομετρητή (web browser) του θύματος, ο κώδικας Javascript θα εκτελεστεί με αποτέλεσμα την αύξηση της χρήσης της CPU και την κρυφή εξόρυξη μαρκών χωρίς τη συγκατάθεση του θύματος. Ειδικότερα, ο φυλλομετρητής στη συσκευή του θύματος εκτελεί κώδικα JavaScript που εγκαθιστά μια σύνδεση WebSocket με έναν απομακρυσμένο διακομιστή. Στη συνέχεια, ο διακομιστής στέλνει τον στόχο στον κακόβουλο κώδικα, ο οποίος υπολογίζει κατακερματισμούς για PoW και τους μεταδίδει πίσω στον διακομιστή. Κατά τη διάρκεια αυτής της διαδικασίας, ο ιδιοκτήτης της συσκευής, δηλαδή το θύμα, δεν γνωρίζει τίποτα για αυτή τη δραστηριότητα (που εκτελείται στο παρασκήνιο) και συνεχίζει απρόσκοπτα την περιήγηση στον ιστότοπο.

Η κρυπτοκλοπή εντός του προγράμματος περιήγησης/φυλλομετρητή δεν αποτελεί μόνο μια σημαντική απειλή για την ιδιωτικότητα, αλλά βλάπτει επίσης τις επιδόσεις της τοπικής συσκευής

(φιλοξενίας), καθώς οι υπολογισμοί κατακερματισμού με βάση το PoW είναι ενεργοβόροι επεξεργαστικά και μπορεί να οδηγήσουν σε υπερβολική χρήση της CPU και αποφόρτιση της μπαταρίας. Συνήθως, για να φέρει σημαντικά αποτελέσματα μια κρυπτοκλοπή αυτού του είδους, θα πρέπει ο χρήστης να παραμείνει σε μια συγκεκριμένη σελίδα για μεγάλο χρονικό διάστημα (πχ. ιστοσελίδες streaming). [28], [64].

4.2.5.2 Επίθεση Ηλεκτρονικού Ψαρέματος (Phishing Attack)

Γενικότερα το Phishing είναι μια δόλια προσπάθεια απόκτησης ευαίσθητων πληροφοριών, όπως τα ονόματα χρηστών, κωδικοί πρόσβασης κτλ., με την μεταμφίεση του επιτιθέμενου ως μια αξιόπιστη οντότητα στην ηλεκτρονική επικοινωνία. Συνήθως πραγματοποιείται μέσω πλαστογράφησης ηλεκτρονικού ταχυδρομείου ή ανταλλαγής άμεσων μηνυμάτων και συχνά κατευθύνει τους χρήστες να εισάγουν προσωπικές πληροφορίες σε έναν ψεύτικο ιστότοπο, η εμφάνιση και η αίσθηση του οποίου είναι ταυτόσημη με τον αντίστοιχο νόμιμο (ιστότοπο) [49]. Έτσι λοιπόν, σε αυτή την επίθεση, ο επιτιθέμενος εξαπατά το θύμα ώστε να ανοίξει μια κακόβουλη ιστοσελίδα, συνδέεται στην θύρα RPC (Remote Procedure Call) (η οποία κατανέμεται δυναμικά σε εφαρμογές διακομιστών και σε εφαρμογές απομακρυσμένης διαχείρισης) του πορτοφολιού κρυπτονομισμάτων του θύματος μέσω ενός Cross-Domain αιτήματος και στην συνέχεια κλέβει περιουσιακά στοιχεία κρυπτογράφησης του θύματος (συνήθως κρυπτονομίσματα). Ένα cross-domain αίτημα είναι ένα χαρακτηριστικό της HTML5 που επιτρέπει σε έναν ιστότοπο να έχει πρόσβαση στους πόρους ενός άλλου ιστότοπου χρησιμοποιώντας JavaScript μέσα στο πρόγραμμα περιήγησης. [65]

5. Αντίμετρα

Στο παρακάτω κεφάλαιο παρατίθενται μερικά αντίμετρα για κάθε επίθεση που αναλύθηκε στο Κεφάλαιο 4. Τα αντίμετρα είναι προτάσεις βασισμένες στην βιβλιογραφία και σε προσωπική συνεισφορά. Στο τέλος των αντίμετρων κάθε επίθεσης προστίθεται και ένας πίνακας που αναλύει κάθε αντίμετρο που αποσκοπεί στην εκάστοτε επίθεση. Τα αντίμετρα που προτείνονται προσπαθούν να καλύψουν τις εξής κατηγορίες:

- Πρόληψη, δηλαδή την εφαρμογή του αντίμετρου με σκοπό να μην φτάσουμε στο σημείο να γίνει μια επίθεση.
- Ανίχνευση/Παρακολούθηση, δηλαδή την εφαρμογή του αντίμετρου για τον εντοπισμό της επίθεσης.
- Μετριασμός, δηλαδή την μερική αντιμετώπιση της επίθεσης.
- Αντιμετώπιση, δηλαδή την πλήρη αντιμετώπιση της επίθεσης.

5.1 Αντίμετρα για Επιθέσεις στον Μηχανισμό Συναίνεσης

5.1.1 Επίθεση 51%

[69][70]

- Σε πολλά blockchain η επιλογή μηχανισμού συναίνεσης αποτελεί από μόνη της μια προσέγγιση που μειώνει την πιθανότητα αυτών των επιθέσεων. Στο PoW υπάρχει μεγάλη πιθανότητα εμφάνισης αυτής της επίθεσης λόγω του κινδύνου συγκέντρωσης της εξόρυξης. Αντίθετα στο PoS είναι δύσκολο και πολύ ακριβό κάποιος να συγκεντρώσει παραπάνω από το 50% των μεριδίων (stake) ενός ολόκληρου δικτύου.
- *Καθυστέρηση των επιβεβαιώσεων blockchain*. Αυτή η μέθοδος κερδίζει χρόνο για το δίκτυο να ανιχνεύσει και ενδεχομένως να αποκρούσει μια επίθεση 51%. Με την παράταση του χρόνου επιβεβαίωσης της συναλλαγής, οι επιτιθέμενοι θα πρέπει να διατηρήσουν τον έλεγχο του 51% του δικτύου για μια πιο παρατεταμένη περίοδο, αυξάνοντας δραματικά το κόστος και τη δυσκολία μιας τέτοιας επίθεσης.
- Η καθιέρωση ενός συστήματος ποινών χρησιμεύει ως μια άλλη βιώσιμη αμυντική στρατηγική. Για παράδειγμα, η εφαρμογή των όρων slashing στα PoS blockchain τιμωρεί τους κακόβουλους φορείς με την κατάσχεση μέρους ή του συνόλου των token που έχουν ποντάρει (stake), εάν διαπιστωθεί ότι ενεργούν ενάντια στους κανόνες του δικτύου. Αυτό το τιμωρητικό μέτρο αυξάνει σημαντικά το διακύβευμα για τυχόν επίδοξους επιτιθέμενους και μπορεί να λειτουργήσει ως ισχυρό αποτρεπτικό μέσο.
- *Αύξηση του ρυθμού κατακερματισμού*: Ένας τρόπος για να αποτραπεί μια επίθεση 51% είναι να αυξηθεί ο ρυθμός κατακερματισμού του δικτύου. Αυτό μπορεί να γίνει με την ενθάρρυνση περισσότερων ανθρακωρύχων να ενταχθούν στο δίκτυο ή με τη χρήση ισχυρότερου εξοπλισμού εξόρυξης. Αυτό βέβαια μπορεί να οδηγήσει σε υψηλότερη κατανάλωση ενέργειας στην περίπτωση χρησιμοποίησης ισχυρότερου εξοπλισμού εξόρυξης, ενώ η ενθάρρυνση περισσότερων ανθρακωρύχων να ενταχθούν στο δίκτυο θα αυξήσει τον ανταγωνισμό εξόρυξης και θα μειώσει την ανταμοιβή εξόρυξης, κάτι που δεν κάνει το συγκεκριμένο αντίμετρο και το ιδανικό.
- *Εφαρμογή υπολογισμού πολλαπλών μερών (MPC)*: Το MPC είναι μια κρυπτογραφική τεχνική που επιτρέπει σε πολλαπλά μέρη να υπολογίζουν από κοινού μια συνάρτηση χωρίς να αποκαλύπτουν τις εισόδους τους. Αυτό μπορεί να χρησιμοποιηθεί για την ασφάλεια του δικτύου έναντι επιθέσεων 51% με τον διαχωρισμό της διαδικασίας επικύρωσης σε πολλαπλούς κόμβους.
- *Αναδιοργάνωση δικτύου ή επαναφορά (rollback)*: Σε ακραίες περιπτώσεις, το δίκτυο μπορεί να επιλέξει να πραγματοποιήσει αναδιοργάνωση του blockchain ή επαναφορά σε ένα σημείο πριν από την επίθεση. Αυτή είναι μια αμφιλεγόμενη και πολύπλοκη απόφαση και θα πρέπει να λαμβάνεται με συναίνεση της κοινότητας.
- Προσωρινή διακοπή συναλλαγών για την αποτροπή περαιτέρω ζημιών.
- *Τυχαιοποιημένες δεξαμενές εξόρυξης*: Δημιουργία συστήματος όπου οι ανθρακωρύχοι κατανέμονται τυχαία σε δεξαμενές εξόρυξης και δεν μπορούν να ελέγχουν την επιλογή της δεξαμενής τους. Έτσι θα δημιουργούνται δεξαμενές εξόρυξης που θα έχουν προκαθορισμένο μέγεθος που είναι αρκετά μικρό της συνολικής δύναμης του δικτύου.

Πίνακας 2. Αντίμετρα Επίθεσης 51%

Αντίμετρα για την Επίθεση 51%	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Επιλογή Σωστού Μηχανισμού Συναίνεσης	x			
Καθυστέρηση Επιβεβαιώσεων	x	x	x	
Σύστημα Ποινών	x			
Αύξηση Ρυθμού Κατακερματισμού	x		x	
Υπολογισμός Πολλαπλών Μερών (MPC)	x		x	
Αναδιοργάνωση/Επαναφορά				x
Προσωρινή Διακοπή Συναλλαγών			x	
Τυχαιοποιημένες Δεξαμενές Εξόρυξης	x			x

5.1.2 Επίθεση Εγωιστικής Εξόρυξης

Το να αναγνωριστεί μια εξόρυξη ως εγωιστική μέσα σε ένα blockchain δεν είναι απλή υπόθεση καθώς είναι δύσκολο να ελεγχθεί αν πρόκειται για κανονική ή κακόβουλη δραστηριότητα. Έχουν γίνει μερικές έρευνες στις οποίες προτείνονται διάφοροι αλγόριθμοι που θα προβλέπουν αν κάποια κανονική φαινομενικά δραστηριότητα είναι δραστηριότητα εγωιστικής εξόρυξης, όπως το σύστημα ForkDec στην [72]. Παρόλα αυτά, δεν έχει υπάρχει κάποιος αλγόριθμος αρκετά γνωστός που να λειτουργεί γενικά για όλα τα PoW blockchain.

Το [73] πρότεινε μια λύση που ονομάζεται Freshness Preferred (FP), στην οποία το μπλοκ με την πιο πρόσφατη χρονοσφραγίδα επιλέγεται. Το FP χρησιμοποιεί μη παραχαράξιμες χρονοσφραγίδες στα μπλοκ εκτός από τη χρονοσφραγίδα που υπάρχει ήδη στην επικεφαλίδα κάθε μπλοκ. Η μη παραχαράξιμη χρονοσφραγίδα μπορεί να αποδείξει ότι ένα μπλοκ εξορύχθηκε πρόσφατα. Στην περίπτωση της εγωιστικής εξόρυξης, ο επιτιθέμενος παρακρατεί ένα μπλοκ, οπότε με τη χρήση αυτής της προσέγγισης θα μειωθούν τα κίνητρα για εγωιστική εξόρυξη, επειδή τα

παρακρατηθέντα μπλοκ θα χάσουν τον αγώνα μπλοκ έναντι των νεων δημιουργηθέντων μπλοκ (τα οποία θα έχουν πιο πρόσφατη χρονοσφραγίδα). Έτσι, εάν ο ανέντιμος ανθρακωρύχος απελευθερώσει έναν μακρύ κατάλογο μπλοκ (ιδιωτική αλυσίδα), τότε οι υπόλοιποι έντιμοι ανθρακωρύχοι, κατά την διαδικασία επικύρωσης των μπλοκ, θα σταθμίσουν την εγκυρότητά τους με βάση τη χρονοσφραγίδα με την οποία κατακερματίστηκαν και τη χρονοσφραγίδα που αναφέρθηκαν στο δίκτυο.

Οι μηχανισμοί τυχαιοποίησης μπορούν να χρησιμοποιηθούν για να διαταράξουν την προβλεψιμότητα των ανταμοιβών εξόρυξης και να καταστήσουν πιο δύσκολο για τους εγωιστές ανθρακωρύχους να επωφεληθούν από την παρακράτηση μπλοκ και άρα από την εγωιστική εξόρυξη. Τέτοιοι μηχανισμοί τυχαιοποίησης μπορεί να είναι:

Τυχαία έκδοση Block: Εισαγωγή μιας τυχαία καθυστέρησης στη δημοσίευση των εξορυγμένων μπλοκ, καθιστώντας δύσκολο για τους εγωιστές ανθρακωρύχους να προβλέψουν πότε θα πρέπει να δημοσιεύσουν τα μπλοκ τους.
Τυχαιοποιημένες δεξαμενές εξόρυξης: Δημιουργία συστήματος όπου οι ανθρακωρύχοι κατανέμονται τυχαία σε δεξαμενές εξόρυξης και δεν μπορούν να ελέγχουν την επιλογή της δεξαμενής τους. Αυτό μπορεί να μειώσει την ικανότητα μιας εγωιστικής ομάδας εξόρυξης να συντονίζει αποτελεσματικά τις επιθέσεις.

Πίνακας 3. Αντίμετρα Επίθεσης Εγωιστικής Εξόρυξης

Αντίμετρα για τη Επίθεση Εγωιστικής Εξόρυξης	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
ForkDec	x	x	x	
Freshness Preferred	x	x		x
Μηχανισμοί Τυχαιοποίησης	x			x

5.1.3 Επίθεση από Μακριά

[40][74]

- *Μετακίνηση σημείων ελέγχου*: Η ιδέα πίσω από τη μετακίνηση των σημείων ελέγχου είναι ότι υπάρχει μια ποσόστωση στον τελευταίο αριθμό *n* μπλοκ της αλυσίδας που μπορεί να αναδιοργανωθεί. Ανάλογα με το πρωτόκολλο, η ποσόστωση μπλοκ μπορεί να αλλάξει. Στο Peercoin, για παράδειγμα, η ποσόστωση αυτή είναι ίση με τα μπλοκ ενός μήνα. Αυτός ο αμυντικός μηχανισμός μετριάζει εν μέρει τις μακράς εμβέλειας επιθέσεις καθώς επιτρέπει την αναδιοργάνωση κάποιου μπλοκ. Παρ' όλα αυτά, με κινούμενα σημεία ελέγχου, οι επιθέσεις μεγάλης εμβέλειας υποβαθμίζονται και πλέον εμπίπτουν στην κατηγορία των μικρής εμβέλειας, καθώς η αναδιοργάνωση δεν ξεκινά από το μπλοκ

γένεσης. Με τη χρήση κινούμενων σημείων ελέγχου, η κύρια αλυσίδα γίνεται πραγματικά αμετάβλητη μέχρι τα τελευταία *n* μπλοκ.

- Χρησιμοποιώντας κρυπτογραφία με εξελισσόμενο κλειδί και πιο συγκεκριμένα key-evolving signatures (KES), η διάρκεια ζωής του κλειδιού χωρίζεται σε εποχές για τις οποίες χρησιμοποιείται διαφορετικό ιδιωτικό κλειδί, αλλά το δημόσιο παραμένει το ίδιο. Από την άποψη αυτή, υπάρχει ένας αλγόριθμος ανανέωσης κλειδιού για την εξαγωγή του νέου ιδιωτικού κλειδιού από το προηγούμενο. Επομένως, η εποχή που η υπογραφή εκδίδεται γίνεται αναπόσπαστο μέρος ολόκληρης της υπογραφής. Ως αποτέλεσμα, ακόμη και αν ένα κλειδί διαρρεύσει, δεν μπορεί να χρησιμοποιηθεί για την εκ νέου / επόμενη εποχή. Η χρήση συνεχώς εξελισσόμενων κλειδιών και χωρίς τη δυνατότητα ανάκτησης παλαιότερης έκδοσης του κλειδιού υπογραφής καθιστά την επίθεση δύσκολη, καθώς εάν ο επιτιθέμενος αποφασίσει να υπογράψει παλιά μπλοκ ενός διαφορετικού κλάδου, δεν θα είναι σε θέση να χρησιμοποιήσει το κλειδί που είχε πίσω στο μπλοκ Genesis, αφού θα έχει ήδη εξελιχθεί από το δικό του υπογράφοντας για έναν άλλο κλάδο.
- Κατά την επίθεση από μακριά στα πρωτόκολλα PoS, υπάρχει μια περίοδος κατά την οποία η πυκνότητα ενός κακόβουλου κλάδου του blockchain είναι πιο αραιή, δηλαδή υπάρχουν παραπάνω μέρη που δεν είναι απευθείας σε σύνδεση με το blockchain όλη την ώρα. Αυτό επιτρέπει σε μερικά πρωτόκολλα, όπως το KRDO17, να εντοπίζουν και να εξαλείφουν τους κλάδους αυτούς λόγω της έλλειψης που τους διακρίνει σε σχέση με το σωστό blockchain (δηλ. την κύρια αλυσίδα) που παράγεται από έντιμα μέρη.
- Ένα θεμελιώδες χαρακτηριστικό μιας επίθεσης stake bleeding είναι η ανάληψη μιας συναλλαγής "εκτός από το πλαίσιο", δηλαδή, αντιγράφοντας την από το ειλικρινά διατηρούμενο blockchain στο ιδιωτικό blockchain που διατηρείται από τον επιτιθέμενο. Ένας πολύ απλός και αποτελεσματικός τρόπος για την αποτροπή να συμβεί αυτό είναι να συμπεριληφθεί ο κατακερματισμός ενός πρόσφατου μπλοκ, σε κάθε συναλλαγή. Η εγκυρότητα μιας συναλλαγής θα απαιτούσε την παρουσία αυτού του κατακερματισμού στο blockchain. Αυτό θα επέτρεπε μόνο σε αντιφατικά παραγόμενες συναλλαγές να είναι μεταβιβάσιμες στο ιδιωτικό blockchain. Συνεπώς, αυτός ο τρόπος/μηχανισμός εξουδετερώνει εντελώς την επίθεση.

Πίνακας 4. Αντίμετρα Επίθεσης από Μακριά

Αντίμετρα για την Επίθεση Από Μακριά	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Μετακίνηση Σημείων Ελέγχου			x	
Key-evolving Signatures			x	
KRDO17		x		x

Συμπερίληψη Κατακερματισμού Πρόσφατου Μπλοκ στην Συναλλαγή				x

5.1.4 Επίθεση Δωροδοκίας

Ο μηχανισμός PoW μπορεί να αποτρέψει καλά τις επιθέσεις δωροδοκίας, διότι οι επιτιθέμενοι χρειάζονται μεγάλο κόστος για να δωροδοκήσουν έναν ή παραπάνω ανθρακωρύχους και να πραγματοποιήσουν μια επιτυχημένη επίθεση. Το κόστος της επίθεσης θα είναι πολύ μεγαλύτερο από τη συναλλαγή της, οπότε η επιλογή του μηχανισμού συναίνεσης είναι ένας τρόπος πρόληψης της επίθεσης.

Υπάρχουν αρκετοί παράγοντες, οι οποίοι θα μπορούσαν να μετριάσουν την επίθεση δωροδοκίας. Πρώτον, η αναγνώριση ή η αποδοχή δωροδοκιών δεν είναι τόσο απλή για τους ανθρακωρύχους και οι επιτιθέμενοι απαιτούν σημαντικό κεφάλαιο και ανοχή στον κίνδυνο, επειδή ο επιτιθέμενος δεν θα μπορούσε να ανακτήσει τις δωροδοκίες εάν η επίθεση αποτύχει. Επιπλέον, οι πωλητές μπορεί να απαιτούν περισσότερες επιβεβαιώσεις για μια μεγάλη συναλλαγή, γεγονός που αυξάνει γραμμικά το κόστος δωροδοκίας των επιτιθέμενων. [75]

Σύμφωνα με το [42], μια λύση για να ξεπεραστεί αυτή η επίθεση είναι ο περιορισμός της ποσότητας κρυπτονομισμάτων που μπορεί να μεταφέρει ένας χρήστης. Ο περιορισμός σχετίζεται στενά με το ποσό της ανταμοιβής μπλοκ. Εάν ο προϋπολογισμός του επιτιθέμενου παραμένει σταθερός, η μείωση της ανταμοιβής αυξάνει την πιθανότητα επιτυχίας επίθεσης. Έτσι, σε ορισμένα κρυπτονομίσματα όπως το Bitcoin, ο αλγόριθμος εξόρυξης θα πρέπει να είναι εξοπλισμένος με έναν μηχανισμό που προσαρμόζει το όριο κάθε 4 χρόνια (όταν η ανταμοιβή πέφτει).

Επίσης, θα μπορούσαν να υπάρχουν κίνητρα για τους πληροφοριοδότες, δηλαδή την ενθάρρυνση των συμμετεχόντων στο δίκτυο να αναφέρουν τυχόν απόπειρες δωροδοκίας ή ύποπτη συμπεριφορά. Δημιουργία με προγράμματα κινήτρων ή ανταμοιβές για άτομα που αποκαλύπτουν κακόβουλες δραστηριότητες, καθιστώντας πιο δαπανηρό για τους επιτιθέμενους να λειτουργούν κρυφά.

Επιπλέον, η διασφάλιση ότι τα οικονομικά κίνητρα για τους συμμετέχοντες ευθυγραμμίζονται με τους μακροπρόθεσμους στόχους και την ασφάλεια του δικτύου, βοηθάει στην ακεραιότητα του δικτύου και μπορεί να αποθαρρύνει τους συμμετέχοντες από τη δωροδοκία. Αυτό γίνεται με την χρήση ανταμοιβών και ποινών.

Πίνακας 5. Αντίμετρα Επίθεσης Δωροδοκίας

Αντίμετρα για την Επίθεση Δωροδοκίας	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Επιλογή Μηχανισμού Συναίνεσης	x			
Περισσότερες Επιβεβαιώσεις για Μεγάλες Συναλλαγές	x		x	
Περιορισμός Ποσότητας Μεταφοράς Κρυπτονομισμάτων	x		x	
Κίνητρα Πληροφοριοδοτών	x	x		
Οικονομικά Κίνητρα	x			

5.2 Αντίμετρα για Επιθέσεις στην Συναλλαγή

5.2.1 Διπλή Δαπάνη και Παραλλαγές

- Στο [76] προτείνονται 3 τεχνικές για την ανίχνευση διπλών δαπανών, κυρίως στο Bitcoin:
  1) Μια "περίοδος ακρόασης" όπου ο πωλητής παρακολουθεί όλες τις συναλλαγές λήψης (πχ. πώλησης αγαθού, παροχής υπηρεσίας, κρυπτονομισμάτων) κατά τη διάρκεια αυτής της περιόδου. Ο πωλητής παραδίδει το προϊόν, ή παρέχει την υπηρεσία, μόνο εάν δεν δει καμία προσπάθεια διπλής δαπάνης κατά τη διάρκεια της περιόδου ακρόασης. Η περίοδος αυτή εξαρτάται κυρίως από τον αριθμό των επιβεβαιώσεων που έχει λάβει μια συναλλαγή. Στο Bitcoin συνίσταται να περιμένει κανείς 6 επιβεβαιώσεις, αλλά οι περισσότερες καθημερινές συναλλαγές μπορούν να γίνουν με ασφαλή τρόπο μετά από 3. Η αναμονή για πολλαπλές επιβεβαιώσεις, δεν θα αποτρέψει την επίθεση διπλής δαπάνης, αλλά θα μετριάσει τον κίνδυνο και θα καταστήσει δυσκολότερο για τον επιτιθέμενο να δαπανήσει τα ίδια νομίσματα περισσότερες από μία φορές. Η μείωση από 6 σε 3 επιβεβαιώσεις επίσης μειώνει την επίδραση του αντιμέτρου ως προς τον βαθμό ικανοποίησης των πελατών από την συναλλαγή (πχ. όσον αφορά την απόδοσή της).
  2) "Εισαγωγή παρατηρητών", κατά την οποία ο πωλητής εισάγει έναν κόμβο (ή ένα ζευγάρι κόμβων) που ονομάζεται "παρατηρητής", ο οποίος θα αναμεταδίδει απευθείας όλες τις συναλλαγές που λαμβάνει από τον πωλητή. Αυτό βοηθά τον πωλητή να εντοπίσει μια προσπάθεια διπλής δαπάνης μέσα σε λίγα δευτερόλεπτα από τον ίδιο ή από τους παρατηρητές του.
  3) Η τρίτη τεχνική είναι η "κοινοποίηση ειδοποιήσεων για διπλές δαπάνες μεταξύ ομότιμων". Αυτή η τεχνική θεωρείται ένα αποτελεσματικό αντίμετρο για την καταπολέμηση της διπλής δαπάνης στη γρήγορη πληρωμή Bitcoin. Σε αυτή την τεχνική, οι ομότιμοι του δικτύου Bitcoin διαδίδουν ειδοποιήσεις κάθε φορά που λαμβάνουν δύο συναλλαγές που μοιράζονται κοινές εισόδους και διαφορετικές εξόδους (απόπειρα διπλής δαπάνης).

- Στο [77] τονίζεται ένα αντίμετρο που μοιάζει με το τελευταίο του προηγούμενου bullet και εξηγεί ότι οι κοντινοί ομότιμοι θα πρέπει να ειδοποιήσουν τον έμπορο/πωλητή για την απόπειρα διπλής δαπάνης των ίδιων νομισμάτων στο δίκτυο. Συγκεκριμένα, κάθε φορά που ένας ομότιμος λαμβάνει μια νέα συναλλαγή, ελέγχει αν η συναλλαγή χρησιμοποιεί νομίσματα που δεν έχουν δαπανηθεί σε οποιαδήποτε άλλη συναλλαγή που υπάρχει στο blockchain και στη δεξαμενή μνήμης τους (mempool). Εάν η συναλλαγή δεν ξοδεύει νομίσματα που έχουν ήδη δαπανηθεί, οι ομότιμοι προσθέτουν τη συναλλαγή στη δεξαμενή μνήμης τους και την προωθούν στο δίκτυο. Από την άλλη πλευρά, εάν οι ομότιμοι εντοπίσουν ότι υπάρχει άλλη συναλλαγή στη δεξαμενή μνήμης που ξοδεύει τα ίδια νομίσματα σε διαφορετικούς παραλήπτες (διεύθυνση), τότε οι ομότιμοι προωθούν αυτή τη συναλλαγή διπλής δαπάνης στους γείτονές τους (χωρίς να την προσθέσουν στη δεξαμενή μνήμης τους). Η πρωταρχική πρόθεση πίσω από αυτή την τεχνική δεν είναι να αποτρέψει την επίθεση διπλής δαπάνης, αλλά να την εντοπίσει και να ενημερώσει τον πωλητή ώστε να μπορεί να εντοπίσει τη συναλλαγή διπλής δαπάνης πριν από την αποστολή ή την παροχή υπηρεσιών στον επιτιθέμενο.
- Στο [78] η προηγούμενη ιδέα επεκτάθηκε και προτάθηκε μια λύση με την ονομασία Enhanced Observers (ENHOBS) (ενισχυμένοι παρατηρητές), ένα υβριδικό μοντέλο παρατηρητών (observers) και του συστήματος συναγερμού από ομότιμους (peer alert

system). Σε αυτό το σύστημα, οι ENHOBS θα κάνουν πιο εμπεριστατωμένες επιθεωρήσεις όλων των συναλλαγών που λαμβάνουν και θα συγκρίνουν τις εξόδους και τις εισόδους τους. Μόλις εντοπιστεί μια επίθεση διπλής δαπάνης, ένα μήνυμα συναγερμού αποστέλλεται, το οποίο περιέχει επίσης τις συναλλαγές διπλής δαπάνης ως απόδειξη μέσω του δικτύου P2P. Μόλις ληφθεί η ειδοποίηση και επαληθευτεί, όλες οι συναλλαγές που αντιστοιχούν στις ίδιες εισόδους απορρίπτονται από τη δεξαμενή μνήμης αμέσως.

- Ένα άλλο αντίμετρο είναι το ακόλουθο. Ο έμπορος θα πρέπει να συνδεθεί με έναν αρκετά μεγάλο τυχαίο αριθμό κόμβων στο δίκτυο. Αυτό θα καταστήσει δυσκολότερο για τον επιτιθέμενο να εισάγει εσφαλμένες πληροφορίες συναλλαγής ή συναλλαγή διπλής δαπάνης, επειδή ο επιτιθέμενος δεν γνωρίζει μέσω ποιων κόμβων επικοινωνεί ο έμπορος. Επιπλέον, ο έμπορος δεν θα πρέπει να δέχεται απευθείας εισερχόμενες συνδέσεις. Έτσι, ο επιτιθέμενος δεν μπορεί να στείλει απευθείας μια συναλλαγή στον έμπορο και να τον αναγκάσει να τη μεταδώσει στο δίκτυο. Οι κόμβοι που θα προωθήσουν αυτή τη συναλλαγή θα την εξετάσουν και θα ανιχνεύσουν αν η συναλλαγή έχει προσπάθεια διπλής δαπάνης. Οι επόμενες συναλλαγές που χρησιμοποιούν την ίδια είσοδο (διεύθυνση) από τον επιτιθέμενο θα αγνοηθούν από τους εν λόγω κόμβους και θα καταστήσουν δυσκολότερο για τον επιτιθέμενο να κάνει διπλές δαπάνες. [79]
- Χρησιμοποίηση πορτοφολιών πολλαπλών υπογραφών που απαιτούν πολλαπλά ιδιωτικά κλειδιά για την εξουσιοδότηση μιας συναλλαγής. Αυτό προσθέτει ένα επιπλέον επίπεδο ασφάλειας απαιτώντας συναίνεση μεταξύ πολλών μερών. Μερικά πορτοφόλια αυτού του είδους είναι: Electrum, Trezor, Coinbase.

Πίνακας 6. Αντίμετρα Επιθέσεων Διπλής Δαπάνης

Αντίμετρα για τις Επιθέσεις Διπλής Δαπάνης	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Περίοδος Ακρόασης				x
Εισαγωγή Παρατηρητών	x	x		
Ειδοποιήσεις Μεταξύ Ομότιμων για Διπλές Δαπάνες	x	x		x
ENHOBS	x	x		x
Σύνδεση με Πολλούς Τυχαίους Κόμβους	x		x	
Πορτοφόλια Πολλαπλών Υπογραφών	x		x	

5.2.2 Επιθέσεις Επανάληψης

[95]

- Χαρακτηριστικά αναγνώρισης στο διακλαδωμένο δίκτυο, όπως οι χρονοσφραγίδες ή τα μοναδικά αναγνωριστικά αλυσίδας, διασφαλίζουν ότι δεν μπορούν να υποβληθούν διπλές συναλλαγές σε ένα δίκτυο, αποφεύγοντας την πιθανότητα εμφάνισης επιθέσεων επανάληψης.
- Η ισχυρή προστασία επανάληψης (strong replay protection) περιλαμβάνει την τοποθέτηση ενός σελιδοδείκτη στο νέο ψηφιακό λογιστικό βιβλίο που δημιουργείται μετά από μια σκληρή διακλάδωση. Με αυτόν τον σελιδοδείκτη στη θέση του, κάθε υπάρχουσα/καταγεγραμμένη συναλλαγή που πραγματοποιείται σε αυτή την έκδοση του blockchain καθίσταται άκυρη. Αυτός ο τύπος προστασίας προστέθηκε στο Bitcoin Cash όταν διαμορφώθηκε για πρώτη φορά από το Bitcoin. Ο σελιδοδείκτης επέτρεπε στους κόμβους του Bitcoin Cash να διακρίνουν τις συναλλαγές που είχαν πραγματοποιηθεί στο τυπικό Bitcoin από εκείνες που πραγματοποιήθηκαν στο Bitcoin Cash.
- Υπάρχει και η opt-in προστασία επανάληψης, η οποία χρησιμοποιείται κυρίως όταν προκύπτει μια σκληρή διακλάδωση μετά την ενημέρωση του ψηφιακού λογιστικού βιβλίου ενός κρυπτονομίσματος, σε αντίθεση με τη διάσπασή του στα δύο. Μόλις εφαρμοστεί αυτή η προστασία, οι χρήστες πρέπει να κάνουν χειροκίνητες αλλαγές στις συναλλαγές για να διασφαλίσουν ότι δεν θα επαναληφθούν. Το αντίμετρο αυτό δεν είναι το ιδανικό αλλά προτείνεται σε περίπτωση που κατά την διακλάδωση δεν υπάρχει ισχυρή προστασία επανάληψης ή δεν υπάρχουν καλά χαρακτηριστικά αναγνώρισης.
- Η αναδιοργάνωση μιας αλυσίδας περιλαμβάνει το συντονισμό με την κοινότητα και τους συμμετέχοντες στο δίκτυο προς αυτό τον σκοπό. Αυτό μπορεί να σημαίνει την ανακύκλωση συναλλαγών ή την πραγματοποίηση αλλαγών στο ιστορικό της "κακής" αλυσίδας ώστε να ακυρωθούν οι συναλλαγές που μπορούν να αναπαραχθούν. Πρόκειται για μια πολύπλοκη και αμφιλεγόμενη προσέγγιση και θα πρέπει να επιδιώκεται μόνο εάν υπάρχει ισχυρή συναίνεση εντός της κοινότητας.

Πίνακας 7. Αντίμετρα Επίθεσης Επανάληψης

Αντίμετρα για την Επίθεση Replay	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Χαρακτηριστικά Αναγνώρισης	x			x
Ισχυρή Προστασία Επανάληψης	x			x
Opt-in Προστασία Επανάληψης	x		x	

Αναδιοργάνωση Αλυσίδας				x

5.3 Αντίμετρα για Επιθέσεις Δικτύου

5.3.1 Επιθέσεις Έκλειψης

[80][81]

- Τυχαία επιλογή κόμβων: Με τη δόμηση ενός ομότιμου δικτύου κατά τέτοιο τρόπο ώστε κάθε κόμβος να συνδέεται σε ένα τυχαίο σύνολο διευθύνσεων IP κάθε φορά που συγχρονίζεται με το δίκτυο αντί να ακολουθεί ένα επαναλαμβανόμενο, εκμεταλλεύσιμο σύνολο κριτηρίων για τους κόμβους. Έτσι μπορεί να μειωθούν σημαντικά οι πιθανότητες ένας κόμβος να συνδεθεί με έναν ελεγχόμενο από επιτιθέμενο κόμβο, ακόμη και αν είχε συνδεθεί πρόσφατα.
- Ντετερμινιστική επιλογή κόμβων: Σε μια προσέγγιση διαφορετική από την τυχαία επιλογή κόμβων, η ντετερμινιστική επιλογή κόμβων περιλαμβάνει την εισαγωγή συγκεκριμένων διευθύνσεων IP των κόμβων στις αντίστοιχες προκαθορισμένες σταθερές θέσεις κάθε φορά που συνδέονται με το δίκτυο. Καθορίζοντας τις συνδέσεις των κόμβων του δικτύου, ένας επιτιθέμενος θα δυσκολευτεί περισσότερο να ελιχθεί με κακόβουλους κόμβους μέσω του δικτύου και να συγκλίνει γύρω από έναν στόχο, ενώ η επαναλαμβανόμενη εισαγωγή διευθύνσεων που ελέγχονται από τον επιτιθέμενο δεν θα συμβάλλει απαραίτητα στην επιτυχία μιας απόπειρας επίθεσης έκλειψης. Αυτό βέβαια προϋποθέτει πως δεν είναι μολυσμένοι/ελεγχόμενοι όλοι οι κόμβοι με τους οποίους συνδέεται ένας κόμβος. Με παρόμοιο τρόπο, ένα blockchain θα μπορούσε να ενσωματώσει αναγνωριστικά κόμβων στα κριτήρια σύνδεσης στο δίκτυο για να διευκολύνει την επανασύνδεση με νόμιμους ομότιμους με υψηλότερες βαθμολογίες εμπιστοσύνης, οι οποίες θα προκύπτουν με συστάσεις από κόμβους της κοινότητας, που θα εχουν συνδεθεί και θα γνωρίζουν την αξιοπιστία κάποιου κόμβου. Με την καθιέρωση συνδέσεων κόμβων με τη χρήση πληροφοριών αναγνώρισης και όχι περιστασιακών δεδομένων, όπως οι χρονοσφραγίδες και η διαθεσιμότητα, το δίκτυο θα είναι πιο ασφαλές και λιγότερο επιρρεπές σε επιρροές τρίτων που αποκλίνουν από τη νόμιμη δραστηριότητα του δικτύου.
- Αυξημένες συνδέσεις κόμβων: Αυξάνοντας τον απαιτούμενο αριθμό συνδέσεων μεταξύ κόμβων, ένα δίκτυο θα μπορούσε να αυξήσει την πιθανότητα ένας κόμβος να συνδεθεί με έναν νόμιμο χρήστη. Ωστόσο, υπάρχουν περιορισμοί στους κόμβους και στο εύρος ζώνης (ανάλογα με το είδος blockchain) που περιορίζουν την σχετική ευελιξία αύξησης ως προς τον αριθμό των συνδέσεων κόμβων χωρίς να θυσιαστεί η απόδοση και η αποτελεσματικότητα.
- Νέοι περιορισμοί κόμβων: Κάνοντας το πιο ακριβό ή δύσκολο να προστεθούν καινούργιοι κόμβοι σε ένα δίκτυο, το blockchain μπορεί να θέσει έναν υψηλότερο πήχη για τους κακόβουλους φορείς να πλημμυρίσουν το δίκτυο με κόμβους που ελέγχονται από επιτιθέμενους. Συχνά αυτή η προσέγγιση περιλαμβάνει τον περιορισμό του αριθμού των κόμβων ανά διεύθυνση IP ή συσκευή, αν και αυτό το αμυντικό μέτρο μπορεί να παρακαμφθεί από έναν επιτιθέμενο που αναπτύσσει ένα botnet αποτελούμενο από συσκευές που έχουν τις δικές τους μοναδικές διευθύνσεις IP. Εν γένει, μπορεί να ειπωθεί πως το ζητούμενο πια για έναν επιτιθέμενο είναι να μπορέσει να ελέγξει υπάρχοντες

κόμβους, πράγμα το οποίο είναι περισσότερο δύσκολο σε σχέση με την εισαγωγή πολλαπλών νέων κόμβων, η οποία περιορίζεται.

- Ασφαλής επικοινωνία: Οι κόμβοι του δικτύου θα πρέπει να χρησιμοποιούν ασφαλή πρωτόκολλα επικοινωνίας, όπως SSL/TLS, για την κρυπτογράφηση των δεδομένων που μεταδίδονται μεταξύ τους. Αυτό αποτρέπει τους επιτιθέμενους από το να κρυφακούσουν την επικοινωνία και να αποκτήσουν πληροφορίες που μπορούν να χρησιμοποιηθούν για την εξαπόλυση μιας επίθεσης έκλειψης.
- Χρήση τειχών προστασίας (firewalls): Τα τείχη προστασίας μπορούν να χρησιμοποιηθούν για το φιλτράρισμα της κυκλοφορίας από και προς κάθε κόμβο του δικτύου. Αυτό συμβάλλει στην αποτροπή των επιτιθέμενων από το να στέλνουν κακόβουλη κυκλοφορία (garbage traffic) στον κόμβο-στόχο και επίσης βοηθά στην αποτροπή του κόμβου-στόχου από το να αναπέμπει κακόβουλη κυκλοφορία σε άλλους κόμβους του δικτύου.
- Χρησιμοποίηση εργαλείων παρακολούθησης δικτύου όπως το wireshark που είναι ένας αναλυτής πρωτοκόλλων δικτύου και χρησιμεύει στην ανίχνευση μη φυσιολογικών δραστηριοτήτων ή ασυνήθιστης επικοινωνίας μεταξύ ομότιμων. Επίσης, συστήματα ανίχνευσης εισβολών (IDS), όπως το Suricata μπορούν να εντοπίσουν ύποπτες δραστηριότητες, όπως επαναλαμβανόμενες προσπάθειες σύνδεσης ή ασυνήθιστη συμπεριφορά δικτύου, που μπορεί να συνδέονται με επίθεσης έκλειψης.
- Αφού βρεθεί ένας παραβιασμένος κόμβος, αποσυνδέεται από το blockchain χειροκίνητα από το δίκτυο και κατά την επαναρρύθμιση του, γίνεται σύνδεση με γνωστούς αξιόπιστους κόμβους, κάτι που θα του επιτρέψει την σωστή επανένταξη του στο δίκτυο. Το αντίμετρο αυτό είναι ευθύνη του κάθε χρήστη που αντιλαμβάνεται ότι γίνεται θύμα μιας τέτοιας επίθεσης.

Πίνακας 8. Αντίμετρα Επίθεσης Έκλειψης

Αντίμετρα για την Επίθεση Έκλειψης	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Τυχαία Επιλογή Κόμβων	x		x	
Ντετερμινιστική Επιλογή Κόμβων	x		x	
Αυξημένες Συνδέσεις Κόμβων	x			
Περιορισμοί Κόμβων	x			
Ασφαλής Επικοινωνία	x		x	
Εισαγωγή Τειχών Προστασίας	x		x	
Εργαλεία παρακολούθησης/IDS		x		x

Αποσύνδεση κόμβου				x

5.3.2 Επιθέσεις Sybil

[82][83]

- Κόστος για τη δημιουργία μιας ταυτότητας: Για να αποτραπεί η ύπαρξη πολλαπλών πλαστών ταυτοτήτων στο δίκτυο, μπορεί να υπάρξει ένα κόστος για κάθε ταυτότητα που θέλει να ενταχθεί στο δίκτυο και να τρέξει ένα κόμβο. Το κόστος αυτό είναι για τους χρήστες που θέλουν να τρέξουν ένα κόμβο στο σύστημα και θα θεωρήσουν ότι η πληρωμή του αντίστοιχου ποσού αξίζει για την αποτροπή αυτών των επιθέσεων.

  Στο Ethereum, για παράδειγμα, οποιοσδήποτε χρειάζεται να ποντάρει 32 ETH για να τρέξει έναν κόμβο Ethereum. 32 ETH αντιστοιχούν σε περίπου 48.000 ευρώ (Αύγουστος 2023). Επομένως, η λειτουργία πολλαπλών κόμβων για μια επίθεση Sybil δεν αξίζει οικονομικά.

  Μια άλλη προσέγγιση θα μπορούσε να είναι η δωρεάν δημιουργία μιας ταυτότητας στο δίκτυο για την χρήση ενός κόμβου, αλλά η πληρωμή του χρήστη για κάθε παραπάνω κόμβο που θα ήθελε υπό τον έλεγχο του.

- Επικύρωση των ταυτοτήτων πριν από την ένταξη στο δίκτυο, πιο συγκεκριμένα: *Άμεση επικύρωση*: ένα ήδη εγκατεστημένο μέλος επαληθεύει τον νέο συμμετέχοντα στο δίκτυο. Για να μπορεί κάποιος κόμβος να το κάνει αυτό, θα μπορούσε να επαληθεύσει για παράδειγμα στο δίκτυο την πραγματική του ταυτότητα με σκοπό να αποκτήσει την απαραίτητη εμπιστοσύνη. Η εμπιστοσύνη αυτή θα μπορούσε να προκύψει και από την κοινότητα μέσω ενός συστήματος φήμης.

  Έμμεση επικύρωση: Ένα καθιερωμένο μέλος επαληθεύει κάποια άλλα μέλη, τα οποία μπορούν, με τη σειρά τους, να επαληθεύσουν άλλους νέους συμμετέχοντες στο δίκτυο. Καθώς τα μέλη που επαληθεύουν τους νέους συμμετέχοντες επαληθεύονται και επικυρώνονται από μια καθιερωμένη οντότητα, οι νέοι συμμετέχοντες θεωρούνται ειλικρινείς. Θα πρέπει να υπάρχει μια διαδικασία εκλογής και επανεκλογής του κόμβου με βάση ενός συστήματος υπολογισμού φήμης/εμπιστοσύνης με σκοπό να παραμένει ο κόμβος ενεργός και έμπιστος στο δίκτυο.

- Ρύθμιση ενός ιεραρχικού δυναμικού συστήματος εμπιστοσύνης: Σύστημα κατά το οποίο θα αλλάζει ο βαθμός εμπιστοσύνης κάθε κόμβου ανάλογα με τον χρόνο που βρίσκεται στο δίκτυο, αλλά και την συμπεριφορά του, για ανίχνευση πιθανών κόμβων sybil.
- Αναδιοργάνωση δικτύου ή επαναφορά (rollback): Σε περίπτωση που το δίκτυο υποστεί αρκετές ζημιές από μια επίθεση sybil, μπορεί να επιλέξει να πραγματοποιήσει αναδιοργάνωση του blockchain ή επαναφορά σε ένα σημείο πριν από την επίθεση. Αυτή

είναι μια αμφιλεγόμενη και πολύπλοκη απόφαση και θα πρέπει να λαμβάνεται με συναίνεση της κοινότητας.

Πίνακας 9. Αντίμετρα Επίθεσης Sybil

Αντίμετρα για την Επίθεση Sybil	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Κόστος Ταυτότητας	x			
Επικύρωση Ταυτότητας	x			
Δυναμικό Ιεραρχικό Σύστημα	x	x	x	
Αναδιοργάνωση/Rollback				x

5.3.3 Επιθέσεις Timejacking

- Η χρήση της ώρας του συστήματος του κόμβου να χρησιμοποιείται τόσο κατά τη δημιουργία ενός νέου μπλοκ (όπως πριν) όσο και κατά τη σύγκριση των χρονοσφραγίδων μεταξύ των μπλοκ. [84]
- Στο Bitcoin, το αποδεκτό χρονικό εύρος ώρας μέχρι την οποία ο κόμβος θα επιστρέψει στον χρόνο συστήματος θα μπορούσε να αυστηροποιηθεί από 70 λεπτά σε 30 λεπτά οδηγώντας σε περιορισμένο παράθυρο επίθεσης, αλλά αυτό εκθέτει το δίκτυο σε προβλήματα σε περίπτωση που ορισμένοι κόμβοι δεν χειρίζονται σωστά τη θερινή ώρα. [85]
- Στο [84] προτείνεται ένα σύστημα αξιόπιστης αρχής χρονοσφραγίδας (TSA) που είναι μια διαδικασία που θα μπορούσε να παρακολουθεί με ασφάλεια τους χρόνους δημιουργίας και τροποποίησης των ψηφιακών δεδομένων, και θα εγγυάται την ύπαρξη και την ακεραιότητα των δεδομένων. Ο πελάτης (client) στέλνει τον κατακερματισμό ενός ψηφιακού αρχείου στην TSA, όπου το αρχείο υπογράφεται με την τρέχουσα ώρα. Οι επικοινωνίες μεταξύ των κόμβων και του TSA θα πρέπει να χρησιμοποιούν σύστημα κρυπτογραφίας δημόσιου κλειδιού για την προστασία της ασφάλειας των δεδομένων. Στον μηχανισμό αυτό, η χρονοσφραγίδα όλων των κόμβων συγχρονίζεται συχνά με την TSA. Ακόμη και αν ο επιτιθέμενος αλλάξει τη χρονοσήμανση του στόχου, ο στόχος θα επανέλθει σε μια κανονική χρονοσήμανση με βάση την TSA όταν δημιουργείται κάθε νέο μπλοκ. Οι διαφορές των χρονοσφραγίδων μεταξύ όλων των κόμβων γίνονται μικρότερες

και μπορούν να περιορίσουν τα αποδεκτά χρονικά εύρη, γεγονός που μπορεί να μειώσει το παράθυρο επίθεσης timejacking.

- Το Πρωτόκολλο Χρόνου Δικτύου (NTP) χρησιμοποιείται για το συγχρονισμό των ρολογιών των διαφόρων συσκευών σε ένα δίκτυο. Εξασφαλίζοντας ότι όλοι οι κόμβοι έχουν λογικά συγχρονισμένα ρολόγια, τα δίκτυα blockchain μπορούν να αποτρέψουν μεγάλες αποκλίσεις στις χρονοσφραγίδες. Γενικά υπάρχει ένας φόβος για επίθεση ενδιάμεσου στο NTP, κάτι που είναι τεχνικά δυνατό για έναν επιτιθέμενο να επιχειρήσει και να προσποιηθεί έναν διακομιστή NTP, για να συγχρονίσει λάθος τα ρολόγια των κόμβων. Αυτό όμως δεν είναι τόσο εύκολο και πολλοί διακομιστές NTP χρησιμοποιούν μηχανισμούς ελέγχου ταυτότητας και ασφάλειας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.
- Εφαρμογή σημείων ελέγχου (checkpoints), όπου έμπιστοι κόμβοι ή αρχές επιβεβαιώνουν την εγκυρότητα ορισμένων μπλοκ. Τα σημεία ελέγχου είναι συνήθως προκαθορισμένα μπλοκ σε συγκεκριμένα χρονικά διαστήματα στο blockchain. Αυτά τα μπλοκ θεωρούνται αξιόπιστα και χρησιμοποιούνται ως σημεία αναφοράς για άλλους κόμβους στο δίκτυο. Συγκρίνοντας το τοπικό τους αντίγραφο του blockchain με τα σημεία ελέγχου, οι κόμβοι μπορούν να ανιχνεύσουν αν έχουν υποστεί επίθεση timejacking. Εάν το τοπικό blockchain ενός κόμβου είναι πολύ μακριά από τον συγχρονισμό με τα σημεία ελέγχου, αυτό μπορεί να αποτελεί ένδειξη επίθεσης timejacking.
- Οι εξερευνητές μπλοκ (block explorers), όπως είναι οι Blockstream Explorer και Etherscan, είναι διαδικτυακά εργαλεία που επιτρέπουν στους χρήστες να επιθεωρούν το ιστορικό συναλλαγών του blockchain, συμπεριλαμβανομένων των χρονοσφραγίδων. Οι ανωμαλίες στις χρονοσφραγίδες μπλοκ μπορούν να εντοπιστούν χειροκίνητα με τη χρήση των εξερευνητών μπλοκ.

Πίνακας 10. Αντίμετρα Επίθεσης Timejacking

Αντίμετρα για την Επίθεση Timejacking	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Χρήση Ώρας Συστήματος στην Σύγκριση Χρονοσφραγίδων	x		x	
Μείωση Αποδεκτού Εύρους Ώρας	x		x	
TSA	x		x	
NTP	x		x	
Checkpoints	x	x		
Block Explorers	x	x		

5.3.4 Επιθέσεις DNS

- Οι επεκτάσεις ασφαλείας DNS (DNSSEC) χρησιμοποιούνται για να προσθέσουν ένα πρόσθετο επίπεδο ασφάλειας στη διαδικασία επίλυσης DNS για την αποτροπή απειλών ασφαλείας, δηλητηρίαση της κρυφής μνήμης του DNS, DNS MitM και DNS Hijacking. Το DNSSEC προστατεύει από τέτοιου είδους επιθέσεις με την ψηφιακή "υπογραφή" των δεδομένων, για τη διασφάλιση της αυθεντικότητας και της ακεραιότητας των εγγραφών DNS. Το DNSSEC διασφαλίζει ότι οι απαντήσεις DNS προστατεύονται από παραποίηση καθ' όλη τη διάρκεια της διαδικασίας επίλυσης DNS. Όμως, Το DNSSEC μπορεί να μην υποστηρίζεται καθολικά από όλους τους επιλύτες DNS. [86]
- Εφαρμογή ελέγχου ταυτότητας πηγής: Η αυθεντικοποίηση πηγής μπορεί να χρησιμοποιηθεί για να επαληθεύσει ότι η ταυτότητα του προορισμού ή της πηγής των απαντήσεων σε αιτήματα DNS είναι νόμιμη. Αυτό μπορεί να επιτευχθεί με τη χρήση τεχνικών όπως το IPsec ή το TLS για την αυθεντικοποίηση του αιτούντος και τη διασφάλιση ότι το αίτημα δεν έχει αλλοιωθεί κατά τη μεταφορά. Έτσι παρέχεται ασφάλεια εναντίων DNS Hijacking (Spoofing) καθώς ο έλεγχος ταυτότητας πηγής επαληθεύει τη νομιμότητα της απάντησης DNS, καθιστώντας δύσκολη για τους επιτιθέμενους την παραποίηση των απαντήσεων με ανακατεύθυνση. [86]
- Χρήση περιορισμού ποσοστού απόκρισης: Είναι μια τεχνική που περιορίζει το ρυθμό με τον οποίο ένας διακομιστής DNS απαντά σε ερωτήματα καθώς και των απαντήσεων για το κάθε ερώτημα, βοηθώντας στην αποτροπή επιθέσεων ενίσχυσης DNS . Επίσης, με την χρήση ορίων ρυθμού στα ερωτήματα DNS αποτρέπεται μια μεμονωμένη πηγή από τη δημιουργία υπερβολικού αριθμού αιτήσεων σε σύντομο χρονικό διάστημα.
- Μπορεί να χρησιμοποιηθεί φιλτράρισμα DNS για τον αποκλεισμό της κυκλοφορίας σε γνωστούς κακόβουλους τομείς ή διευθύνσεις IP. Αυτό μπορεί να γίνει χρησιμοποιώντας λίστες DNS που ενημερώνονται τακτικά με γνωστούς κακόβουλους ή νόμιμους τομείς.
- Οι ανιχνευτές πακέτων, όπως το Wireshark ή το tcpdump, μπορούν να αναλύσουν την κυκλοφορία του δικτύου, συμπεριλαμβανομένων των πακέτων DNS. Χρησιμοποιούνται για την ανίχνευση παρατυπιών και ενδείξεις επιθέσεων DNS.

Πίνακας 11. Αντίμετρα Επίθεσης DNS

Αντίμετρα για την Επίθεση DNS	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
DNSSEC	x	x		x
Έλεγχος ταυτότητας πηγής	x			x

Χρήση Περιορισμού Ποσοστού Απόκρισης	x		x	
Φιλτράρισμα DNS	x		x	
Ανιχνευτές Πακέτων		x		

5.3.5 Επιθέσεις DDoS

[87][88]

- Ο πρωταρχικός τρόπος για την προστασία από DDoS στο blockchain είναι να διασφαλιστεί ότι όλοι οι κόμβοι διαθέτουν αρκετή επεξεργαστική ισχύ, επαρκή αποθηκευτικό χώρο και εύρος ζώνης δικτύου.
- Κρυπτογράφηση και πιστοποίηση της επικοινωνίας μεταξύ των κόμβων και των πελατών με πρωτόκολλα, όπως το TLS.
- Φιλτράρισμα και αποκλεισμός της κακόβουλης κυκλοφορίας με τείχη προστασίας.
- Χρησιμοποίηση δικτύων παράδοσης περιεχομένου (CDN) για διανομή της κίνησης των συναλλαγών σε πολλαπλά σημεία παρουσίας, καθιστώντας πιο δύσκολο για τις επιθέσεις DDoS να στοχεύσουν ένα μόνο mempool. Οι CDN διανέμουν την εισερχόμενη δικτυακή κίνηση, η οποία περιλαμβάνει συναλλαγές, συνδέσεις ομότιμων χρηστών και άλλες επικοινωνίες, σε ένα κατανεμημένο δίκτυο διακομιστών άκρων. Αυτή η κατανομή συμβάλλει στην εξισορρόπηση του φορτίου του δικτύου και αποτρέπει τη συμφόρηση πριν και κατά τη διάρκεια μιας επίθεσης DDoS.
- Διάφορες υπηρεσίες anti-DDoS διατίθενται στην αγορά, οι οποίες θα μπορούσαν να προστατεύσουν το δίκτυο blockchain από επιθέσεις DDoS, όπως το CloudFlare. Το CloudFlare μπορεί να φιλτράρει και να επιθεωρεί την εισερχόμενη κίνηση δικτύου, εντοπίζοντας και αποκλείοντας την κακόβουλη κίνηση επιθέσεων DDoS πριν φτάσει στους κόμβους blockchain. Το CloudFlare μπορεί να παρέχει τα παραπάνω αντίμετρα, δηλαδή πρωτόκολλο TLS για επικοινωνία μεταξύ των κόμβων, τείχος προστασίας για έλεγχο ρυθμού εισερχόμενων αιτήσεων και CDN για διανομή της κίνησης των συναλλαγών. Επίσης, παρέχει παρακολούθηση και ανάλυση της κίνησης σε πραγματικό χρόνο, επιτρέποντάς την παρακολούθηση για ασυνήθιστα μοτίβα ή περιστατικά.
- Εφαρμογή μηχανισμών περιορισμού ρυθμού για τις εισερχόμενες συναλλαγές. Περιορισμός του αριθμού των συναλλαγών που μπορούν να προστεθούν στο transaction mempool ανά δευτερόλεπτο για αποτροπή υπερφόρτωσης του από μια ξαφνική εισροή συναλλαγών που θα οδηγήσει σε άρνηση υπηρεσίας.
- Επιβολή ορίων για το μέγεθος των μεμονωμένων συναλλαγών, καθώς οι μεγάλες συναλλαγές μπορούν να καταναλώσουν σημαντικό ποσό πόρων στο mempool, καθιστώντας το πιο ευάλωτο σε επιθέσεις DDoS.
- Προτεραιότητα σε συναλλαγές με υψηλότερες χρεώσεις ή συγκεκριμένα χαρακτηριστικά που υποδηλώνουν τη σπουδαιότητά τους. Αυτό μπορεί να βοηθήσει να διασφαλιστεί ότι οι σημαντικές συναλλαγές επεξεργάζονται ακόμη και κατά τη διάρκεια μιας επίθεσης DDoS.

Πίνακας 12. Αντίμετρα Επίθεσης DDoS

Αντίμετρα για την Επίθεση DDoS	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Επαρκή επεξεργαστική ισχύ, αποθηκευτικός χώρος και εύρος ζώνης δικτύου.	x			
TLS/Firewall/CDN	x		x	
Anti-DDoS	x	x		x
Περιορισμός Ρυθμού Συναλλαγών	x			
Όρια Μεγέθους Συναλλαγών	x			
Προτεραιότητα Συναλλαγών	x		x	

5.3.6 Επιθέσεις BGP Hijack

- Για τους οργανισμούς που δεν διατηρούν τη δική τους υποδομή δρομολόγησης AS, η άμυνα κατά της πειρατείας BGP είναι θέμα επιλογής παρόχων υπηρεσιών που αμύνονται ενεργά κατά τέτοιων επιθέσεων.
- Χρήση φιλτραρίσματος προθέματος διεύθυνσης IP για τον αποκλεισμό της εισερχόμενης δικτυακής κίνησης από δίκτυα που είναι γνωστό ότι ελέγχονται από κακόβουλους φορείς.
- Ανάπτυξη στρατηγικών ανίχνευσης BGP hijack σε επίπεδο AS, όπου οι φορείς εκμετάλλευσης μπορούν να παρακολουθούν την καθυστέρηση του δικτύου, τις επιδόσεις και τις αποτυχημένες παραδόσεις πακέτων για τον εντοπισμό προσπαθειών BGP hijack.
- Αύξηση της ποικιλομορφίας των συνδέσεων των κόμβων. Δηλαδή, όσο πιο συνδεδεμένο είναι ένα AS, τόσο πιο δύσκολη είναι η επίθεση σε αυτό. Έτσι, είναι καλύτερα, οι κόμβοι να είναι πολλαπλά συνδεδεμένοι. [59]
- Παρακολούθηση του round-trip (RTT). Ο RTT είναι ο συνολικός χρόνος που χρειάζεται το αίτημα για να ταξιδέψει στο δίκτυο και η απάντηση για να ταξιδέψει πίσω. Το RTT αυξάνεται κατά τη διάρκεια της επίθεσης, οπότε παρατηρώντας το RTT προς τους ομότιμους κόμβους του, ένας κόμβος θα μπορούσε να ανιχνεύσει ξαφνικές αλλαγές και να δημιουργήσει επιπλέον τυχαίες συνδέσεις ως μηχανισμό προστασίας.

- Το Border Gateway Protocol Security (BGPsec) είναι μια επέκταση του πρωτοκόλλου BGP που προορίζεται να προσθέσει κρυπτογραφική επαλήθευση για τις διαφημιζόμενες διαδρομές BGP. Το BGPsec, ένα πρωτόκολλο που παρακολουθεί τα πρότυπα του διαδικτύου, παρέχει έναν μηχανισμό για τους δρομολογητές κορμού να εφαρμόζουν ψηφιακές υπογραφές στις ανακοινώσεις των ενημερώσεων διαδρομών τους, καθιστώντας δυσκολότερη τη μη εξουσιοδοτημένη ανακοίνωση διαδρομών για AS από μη εξουσιοδοτημένους επιτιθέμενους. Το BGPsec μπορεί επίσης να συμβάλει στη μείωση της πιθανότητας επιπλοκών όταν οι διαδρομές BGP διαφημίζονται εσφαλμένα λόγω λανθασμένων ρυθμίσεων. [89]

Πίνακας 13. Αντίμετρα Επίθεσης BGP Hijack

Αντίμετρα για την Επίθεση BGP Hijack	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Επιλογή Καλού Παρόχου Υπηρεσιών	x			
Φιλτράρισμα Προθέματος IP	x			
Ανίχνευση Επίθεσης σε Επίπεδο AS		x		
Πολλαπλή Σύνδεση Κόμβων	x			
Παρακολούθηση RTT	x	x	x	
BGPsec				x

5.4 Αντίμετρα για Επιθέσεις σε Έξυπνα Συμβόλαια

5.4.1 Επιθέσεις Επανεισαγωγής (Reentrancy)

[90][91]

- Χρήση ενός Mutex ή Mutual Exclusion Lock: Η κλειδαριά mutex χρησιμοποιείται για να αποτρέψει την ταυτόχρονη πραγματοποίηση πολλαπλών κλήσεων στην ίδια συνάρτηση. Όταν καλείται μια συνάρτηση, το κλείδωμα mutex τίθεται και άλλες κλήσεις στην ίδια συνάρτηση θα μπλοκαριστούν μέχρι να απελευθερωθεί το κλείδωμα. Παρόλα αυτά η χρήση mutex σε πολλά έξυπνα συμβόλαια μπορεί να οδηγήσει και σε deadlock (κόλλημα ή κλείδωμα) μεταξύ των συμβολαίων.
- Χρήση μιας συνθήκης φύλαξης (Guard Condition): Μια συνθήκη φύλαξης είναι μια σημαία που τίθεται πριν από την κλήση εξωτερικών συναρτήσεων και ελέγχεται μετά. Εάν η σημαία είναι ρυθμισμένη, το συμβόλαιο δεν θα εκτελέσει την εξωτερική κλήση και θα αποτρέψει την επανεμφάνιση.
- Ο έλεγχος του βάθους της στοίβας κλήσεων είναι ένας τρόπος για να διασφαλιστεί ότι η σύμβαση δεν καλείται αναδρομικά. Εάν το βάθος της στοίβας κλήσεων υπερβεί ένα ορισμένο όριο, η σύμβαση θα σταματήσει να εκτελείται.
- Ορισμός των ορίων αερίου (gas) για τις συναλλαγές. Αυτό το όριο αερίου θα πρέπει να καθορίζεται προσεκτικά με βάση τις αναμενόμενες υπολογιστικές απαιτήσεις της καλούμενης συνάρτησης και θα πρέπει να τίθεται σε επίπεδο που να επιτρέπει στη συνάρτηση να εκτελείται με επιτυχία, ενώ δεν αφήνει υπερβολικό αέριο για πιθανές επαναληπτικές κλήσεις. Ο καθορισμός ενός κατάλληλου ορίου αερίου συμβάλλει στην αποτροπή επιθέσεων επανεισαγωγής, διασφαλίζοντας ότι η εκτέλεση της καλούμενης συνάρτησης μπορεί να ολοκληρωθεί χωρίς να προκληθεί περαιτέρω απροσδόκητη εκτέλεση κώδικα.
- Θα πρέπει να ακολουθείται το μοτίβο “checks-effects-interactions” στις συναρτήσεις του έξυπνου συμβολαίου. Δηλαδή:

  (α) Εκτέλεση όλων των ελέγχων και επικύρωσης για να διασφαλιστεί ότι πληρούνται οι προϋποθέσεις για την προβλεπόμενη λειτουργία.

  (β) Ενημέρωση των μεταβλητών κατάστασης, αλλάζοντας την εσωτερική κατάσταση του συμβολαίου.

  (γ) Αλληλεπίδραση με εξωτερικές συμβάσεις

  Αυτή η σειρά λειτουργιών διασφαλίζει ότι η κατάσταση ενημερώνεται πριν από οποιαδήποτε εξωτερική αλληλεπίδραση, καθιστώντας την πιο ανθεκτική σε επιθέσεις επανεισαγωγής.

- Χρήση εργαλείων στατικής ανάλυσης ανοικτού κώδικα, όπως το Oyente, που έχουν σχεδιαστεί κυρίως για τον εντοπισμό τρωτών σημείων επανεισαγωγής σε έξυπνες συμβάσεις Ethereum.

Πίνακας 14. Αντίμετρα Επίθεσης Επανεισαγωγής

Αντίμετρα για την Επίθεση Επανεισαγωγής	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Mutual Exclusion Lock				x
Guard Condition				x
Έλεγχος Βάθους Στοίβας Κλήσεων	x		x	x
Ορισμός Ορίου Gas	x		x	x
Μοτίβο checks-effects-interactions	x		x	
Εργαλεία Στατικής Ανάλυσης		x		x

5.4.2 Επιθέσεις Υπερχείλισης (Overflow)

- Βιβλιοθήκη SafeMath[13]: Για να αποτρέψουν μια επίθεση υπερχείλισης, οι προγραμματιστές θα πρέπει να βεβαιώνονται ότι χρησιμοποιούν ασφαλείς βιβλιοθήκες μαθηματικών ή κατάλληλους τύπους που παρέχουν ανίχνευση υπερχείλισης. Η βιβλιοθήκη SafeMath παρέχει τις βασικές αριθμητικές πράξεις, αλλά μπορεί επίσης να ελέγξει τις προ- και μετα-προϋποθέσεις για να διαπιστώσει αν έχει συμβεί υπερχείλιση ή όχι. Σε περίπτωση σφάλματος, η βιβλιοθήκη αποτυγχάνει τη συναλλαγή και ενημερώνει την κατάσταση της συναλλαγής σε 'Reverted'. [92]
- Εφαρμογή ελέγχων για διασφάλιση ότι οι αριθμητικές πράξεις δεν θα οδηγήσουν σε υπερχειλίσεις. Για παράδειγμα, πριν από μια μεταφορά μαρκών, μπορεί να υπάρξει μια βεβαίωση ότι η πηγή έχει επαρκές υπόλοιπο πριν εκτελεστεί η λειτουργία.
- Στο [93] προτάθηκε το Easyflow, ένα εργαλείο που εντοπίζει έξυπνα συμβόλαια με πιθανή υπερχείλιση.

Πίνακας 15. Αντίμετρα Επίθεσης Υπερχείλισης

Αντίμετρα για την Επίθεση Υπερχείλισης	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Βιβλιοθήκη SafeMath	x	x		x
Εφαρμογή Ελέγχων	x			
EasyFlow		x		

[13] https://docs.openzeppelin.com/contracts/2.x/api/math

5.4.3 Επιθέσεις με Σύντομη Διεύθυνση (Short-Address)

- Χρησιμοποίηση δηλώσεων require για έλεγχο του μήκους δεδομένων εισόδου. Θα πρέπει να καθοριστεί το ελάχιστον αναμενόμενο μήκος και να διασφαλιστεί ότι τα δεδομένα εισόδου δεν είναι μικρότερα.
- Χρήση βιβλιοθηκών όπως η "ethereum-address" που είναι ειδικά σχεδιασμένες για την επικύρωση διευθύνσεων Ethereum και μήκους δεδομένων. Αυτές οι βιβλιοθήκες μπορούν να βοηθήσουν να διασφαλιστεί ότι η παρεχόμενη είσοδος τηρεί την αναμενόμενη μορφή.
- Στην αλληλεπίδραση με εξωτερικές συμβάσεις πρέπει να χρησιμοποιείται η σωστή υπογραφή συνάρτησης και μορφή δεδομένων. Η απαίτηση να έχουν τα δεδομένα της κλήσης της συνάρτησης ένα συγκεκριμένο μήκος και η επαλήθευση της υπογραφής της συνάρτησης μπορεί να βοηθήσει στην αποτροπή επιθέσεων σύντομης διεύθυνσης.
- Η σκληρή διακλάδωση Constantinople του δικτύου Ethereum εισήγαγε αλλαγές που απορρίπτουν αυτόματα συναλλαγές με εσφαλμένα κωδικοποιημένα δεδομένα εισόδου, μειώνοντας τον κίνδυνο επιθέσεων με σύντομες διευθύνσεις.
- Το Slither είναι ένα δημοφιλές εργαλείο στατικής ανάλυσης για έξυπνα συμβόλαια Ethereum. Διαθέτει έναν έλεγχο με την ονομασία "Short Address Attack" που εντοπίζει συγκεκριμένα ευπάθειες που σχετίζονται με επιθέσεις σε σύντομες διευθύνσεις.

Πίνακας 16. Αντίμετρα Επίθεσης Σύντομης Διεύθυνσης

Αντίμετρα για την Επίθεση Σύντομης Διεύθυνσης	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Δήλωση require		x		x
Βιβλιοθήκη ethereum-address	x	x		x
Υπογραφή Συνάρτησης	x		x	
Διακλάδωση Constantinople		x		x
Slither		x		

5.5 Αντίμετρα για Κλασικές Επιθέσεις

5.5.1 Επιθέσεις Κρυπτοκλοπής

- Περιορισμός της εκτέλεσης κώδικα (scripting) από την πλευρά των πελατών κάτι το οποίο γίνεται με έλεγχο των δεδομένων που αποθηκεύονται στον διακομιστή και τον αποκλεισμό της εκτέλεσης κώδικα που παρέχεται από διαφορετικό τομέα από αυτό του διακομιστή (single-domain scripting).
- Εργαλεία ανίχνευσης συμπεριφοράς εξόρυξης, όπως το MineGuard, ένα εργαλείο που προτείνεται στο [97] και μπορεί να ανιχνεύσει τη συμπεριφορά εξόρυξης σε πραγματικό χρόνο σε πισίνες εξόρυξης και VMs. Αυτό γίνεται με παρακολούθηση της κυκλοφορίας του δικτύου για μοτίβα και ανωμαλίες που σχετίζονται με την εξόρυξη σε γνωστές δεξαμενές εξόρυξης. Η ανίχνευση δραστηριοτήτων εξόρυξης συχνά περιλαμβάνει την παρακολούθηση των πόρων του συστήματος, ιδίως της χρήσης CPU και GPU.
- Χρησιμοποίηση αξιόπιστου λογισμικού προστασίας από ιούς και κακόβουλο λογισμικό που μπορεί να ανιχνεύσει και να αποκλείσει τα σενάρια κρυπτοκλοπής. Για παράδειγμα, το Norton 360 παρέχει ολοκληρωμένη ασφάλεια από κακόβουλο λογισμικό και διαδικτυακές απειλές. Περιλαμβάνει λειτουργίες για τον εντοπισμό και τον αποκλεισμό προσπαθειών κρυπτοπειρατείας.
- Χρησιμοποίηση επεκτάσεων και πρόσθετων του προγράμματος περιήγησης που μπορούν να βοηθήσουν στον αποκλεισμό των σεναρίων κρυπτοκλοπής. Το NoCoin[14]μπλοκάρει τα σενάρια εξόρυξης κρυπτονομισμάτων σε ιστότοπους, εμποδίζοντας τα να χρησιμοποιούν την ισχύ της CPU, παρέχει τη δυνατότητα μπλοκαρίσματος συγκεκριμένων ιστότοπων και προσφέρει στατιστικά στοιχεία σχετικά με τον αριθμό των μπλοκαρισμένων προσπαθειών εξόρυξης. Άλλο ένα παράδειγμα είναι το minerBlock που αποκλείει την εκτέλεση script κρυπτοκλοπής στο πρόγραμμα περιήγησής, εμφανίζει πληροφορίες σχετικά με τον αριθμό των μπλοκαρισμένων αιτήσεων και την εξοικονόμηση CPU ενώ προσφέρει φιλική προς το χρήστη διεπαφή με λεπτομερή στατιστικά στοιχεία.
- Τα προγράμματα αποκλεισμού διαφημίσεων μπορούν μερικές φορές να μπλοκάρουν τα σενάρια κρυπτοκλοπής, καθώς τα τελευταία συχνά παρέχονται μέσω διαδικτυακών διαφημίσεων όπου αν κάποιος πατήσει πάνω στη διαφήμιση ενεργοποιείται το αντίστοιχο σενάριο. Το uBlock Origin[15] είναι ένας ανοιχτού κώδικα, ελαφρύς και εξαιρετικά προσαρμόσιμος αποκλειστής διαφημίσεων (ad blocker). Είναι γνωστό για την αποτελεσματικότητά του στο μπλοκάρισμα όχι μόνο των διαφημίσεων αλλά και των σεναρίων κρυπτοκλοπής.
- Εφαρμογή μιας ισχυρής πολιτικής ασφάλειας περιεχομένου (CSP) για να γίνεται έλεγχος ποια σενάρια μπορούν να εκτελούνται στην ιστοσελίδα και από πού μπορούν να φορτώνονται πόροι. Απαγόρευση της εκτέλεσης inline σεναρίων και τη φόρτωση εξωτερικών σεναρίων από μη αξιόπιστες πηγές.
- Ορισμός HttpOnly στα cookies για αποτροπή της εκτέλεσης scripts στην μεριά του πελάτη, οπότε ο επιτιθέμενος δεν θα μπορεί να εισάγει κακόβουλα script κατά την διάρκεια της συνεδρίας του χρήστη σε κάποια ιστοσελίδα.

[14] https://github.com/keraf/NoCoin

[15] https://ublockorigin.com/

- Ο καθαρισμός δεδομένων σε ιστοσελίδες και εφαρμογές ιστού (web applications) μπορεί να βοηθήσει σε ορισμένες περιπτώσεις αφαιρώντας αποθηκευμένα σενάρια (scripts) ή προσωρινά αρχεία που μπορεί να σχετίζονται με μια πιθανή επίθεση cryptojacking.

Πίνακας 17. Αντίμετρα Επίθεσης Κρυπτοκλοπής

Αντίμετρα για την Επίθεση Κρυπτοκλοπής	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Περιορισμός scripting	x			
Εργαλεία ανίχνευσης συμπεριφοράς εξόρυξης		x		
Λογισμικό Προστασίας	x	x		x
Επεκτάσεις και Πρόσθετα Φυλλομετρητή	x	x		x
Προγράμματα Αποκλεισμού Διαφημίσεων	x			x
Πολιτική Ασφάλειας Περιεχομένου	x			x
Ρύθμιση HttpOnly	x			x
Καθαρισμός Δεδομένων	x		x	

5.5.2 Επίθεση Phishing

[94]

- Επαλήθευση διευθύνσεων URL ιστότοπου: Πριν την εισαγωγή ευαίσθητων πληροφοριών ή εκτέλεσης συναλλαγών, πρέπει να γίνεται έλεγχος της διεύθυνσης URL του ιστότοπου, για την βεβαίωση ότι πρόκειται για τον επίσημο και νόμιμο ιστότοπο. Αυτό γίνεται με έλεγχο ονομάτων τομέων (Domain Names), εφαρμογή λευκών λιστών με αξιόπιστους τομείς ή υπηρεσίες και χρήση δημόσιων APIs (Application Programming Interface), που διαθέτουν πολλά blockchain και επιτρέπουν να την ανάκτηση πληροφοριών σχετικά με συναλλαγές. Τα API μπορούν να χρησιμοποιηθούν για επιθεώρηση των συναλλαγών που σχετίζονται με μια διεύθυνση URL και να προσδιοριστεί αν είναι νόμιμες. Επίσης, συνίσταται προσοχή σε ιστότοπους με μικρές παραλλαγές στη διεύθυνση URL ή στο όνομα τομέα, καθώς οι επιτιθέμενοι συχνά δημιουργούν τομείς που μοιάζουν με τους νόμιμους.
- Εγκατάσταση λογισμικού anti-phishing: παραδείγματα περιλαμβάνουν την ενσωματωμένη ανίχνευση phishing του MetaMask[16] (που είναι ηλεκτρονικό πορτοφόλι για κρυπτονομίσματα) και επεκτάσεις του προγράμματος περιήγησης, όπως το MetaCert[17].
- Χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων: Ενεργοποίηση 2FA όπου είναι δυνατόν, ειδικά για ανταλλαγές, πορτοφόλια και λογαριασμούς που σχετίζονται με τα περιουσιακά στοιχεία blockchain.
- Σύνθετοι κωδικοί πρόσβασης (τουλάχιστον 14 σύμβολα), καθώς στην επίθεση phishing, ο επιτιθέμενος προσπαθεί να πάρει πρόσβαση στον λογαριασμό κάποιου χρήστη ξεγελώντας τον παίρνοντας πληροφορίες από αυτόν. Ένας σύνθετος κωδικός πρόσβασης, κάνει πιο δύσκολο για τον επιτιθέμενο να βρει ή να μαντέψει τον κωδικό του θύματος και να πάρει πρόσβαση στον λογαριασμό του.
- Η εκπαίδευση των χρηστών και η ενημέρωση τους σχετικά με τις επιθέσεις phishing, μπορεί να βοηθήσει στην αποτροπή λαθών από τους χρήστες που μπορεί να οδηγήσει σε επιτυχημένες επιθέσεις phishing.

Πίνακας 18. Αντίμετρα Επίθεσης Phishing

Αντίμετρα για την Επίθεση Phishing	**Πρόληψη**	**Ανίχνευση/ Παρακολούθηση**	**Μετριασμός Επίθεσης**	**Αντιμετώπιση Επίθεσης**
Επαλήθευση Διευθύνσεων URL	x			
Anti-Phishing Software		x		x
2FA Authentication	x		x	
Σύνθετοι Κωδικοί Πρόσβασης	x			

[16] https://metamask.io/

[17] https://metacert.com/

Εκπαίδευση χρηστών	x			x

6. Ερευνητικά Κενά και Κατευθύνσεις

Στο παρακάτω κεφάλαιο παρατίθενται μερικά ερευνητικά κενά που δεν έχουν επιλυθεί για τις βασικές επιθέσεις blockchain καθώς και μερικές (ερευνητικές) κατευθύνσεις-προτάσεις που μπορεί να οδηγήσουν στην επίλυση ή βελτίωση των κενών αυτών.

6.1 Επίθεση 51%

6.1.1 Κενά

- Ένα από τα κύρια τρωτά σημεία που οδηγούν σε επιθέσεις 51% είναι η συγκέντρωση της εξορυκτικής δύναμης. Στα blockchain με απόδειξη εργασίας (PoW) όπως το Bitcoin, οι ανθρακωρύχοι με σημαντικούς υπολογιστικούς πόρους έχουν πλεονέκτημα. Οι μεγάλες δεξαμενές εξόρυξης μπορούν δυνητικά να ενοποιήσουν την ισχύ τους, καθιστώντας ευκολότερο για αυτούς να εξαπολύσουν επίθεση 51%. Ένας επιτιθέμενος μπορεί να το βρει ευκολότερο να στοχεύσει έναν μικρό αριθμό αυτών των δεξαμενών για να συγκεντρώσει αρκετή ισχύ εξόρυξης για μια επίθεση.

- Όπως φάνηκε στο κεφάλαιο των αντίμετρων η παρακολούθηση/ανίχνευση των επιθέσεων 51% μπορεί να συμβεί μόνο με την καθυστέρηση επιβεβαιώσεων για να μπορέσει να ανιχνεύσει την επίθεση. Πολλά δίκτυα blockchain δεν διαθέτουν ολοκληρωμένα συστήματα παρακολούθησης και επιτήρησης για τον εντοπισμό και την απόκριση σε πιθανές επιθέσεις 51% σε πραγματικό χρόνο.

6.1.2 Κατευθύνσεις

- Σχεδίαση με δομές κινήτρων που αποθαρρύνουν τους ανθρακωρύχους να συμμετέχουν σε μεγάλες πισίνες και ενθαρρύνουν τη συμμετοχή σε μικρότερες, αποκεντρωμένες δεξαμενές. Αυτό μπορεί να περιλαμβάνει προσαρμογή ανταμοιβών μπλοκ, χρεώσεις συναλλαγών και άλλα κίνητρα για να ευνοηθούν μικρότερες ομάδες ή επιβολή κυρώσεων για τους εξορύκτες που συμβάλλουν στον υπερβολικό συγκεντρωτισμό μιας πισίνας εξόρυξης.

- Οι μελλοντικές κατευθύνσεις θα μπορούσαν να περιλαμβάνουν την ανάπτυξη προηγμένων εργαλείων παρακολούθησης δικτύου, αλγορίθμων ανίχνευσης και συνεργασία μεταξύ των συμμετεχόντων στο δίκτυο για τον γρήγορο εντοπισμό και τον μετριασμό πιθανών

επιθέσεων 51%. Σκοπός θα είναι η παρακολούθηση της κατανομής της ισχύος εξόρυξης και η ανίχνευση τυχόν ανωμαλιών ή ύποπτης δραστηριότητας που θα μπορούσε να υποδεικνύει μια πιθανή επίθεση 51%.

6.2 Επίθεση Εγωιστικής Εξόρυξης

6.2.1 Κενά

- Η ανίχνευση επιθέσεων εγωιστικής εξόρυξης μπορεί να είναι δύσκολη, επειδή οι περισσότεροι, αν όχι όλοι, ανθρακωρύχοι αποκρύπτουν στρατηγικά τα μπλοκ τους από το δημόσιο δίκτυο. Αυτή η μυστική συμπεριφορά καθιστά δύσκολο για το δίκτυο να εντοπίσει πότε γίνεται εγωιστική εξόρυξη, και τις περισσότερες φορές η εξόρυξη αυτή φαίνεται σαν κανονική εργασία. Αυτό το κενό στους μηχανισμούς ανίχνευσης πρέπει να αντιμετωπιστεί για να ενισχυθεί η ασφάλεια των δικτύων blockchain.

- Οι επιθέσεις εγωιστικής εξόρυξης μπορούν να είναι πιο επιτυχείς σε δίκτυα με μεγαλύτερη καθυστέρηση και προβλήματα συγχρονισμού.

6.2.2 Κατευθύνσεις

- Εφαρμογή ισχυρότερων εργαλείων παρακολούθησης και ανάλυσης του δικτύου για τον εντοπισμό ανώμαλης συμπεριφοράς εξόρυξης, που θα μπορούν να εκτελεστούν σε οποιοδήποτε blockchain. Με τη συνεχή ανάλυση των χρόνων διάδοσης των μπλοκ, των ποσοστών ορφανών μπλοκ και της συμπεριφοράς των εξορύξεων, τα δίκτυα blockchain μπορούν να εντοπίζουν πιθανές εγωιστικές προσπάθειες εξόρυξης. Στην διπλωματική αυτή προτείνονται μέσα από έρευνες δύο εργαλεία για την ανίχνευση αυτών των επιθέσεων, τα ForkDec και Freshness Preferred [106], τα οποία όμως προκύπτουν σαν προτάσεις και δεν είναι ευρέως γνωστά και κοινώς αποδεκτά για την πλειοψηφία των blockchain. Η επέκταση τους για χρήση σε όλα τα PoW blockchain είναι μια κατεύθυνση για την αντιμετώπιση αυτού του κενού στο μέλλον.

- Οι μελλοντικές κατευθύνσεις μπορεί να περιλαμβάνουν τη βελτιστοποίηση των πρωτοκόλλων δικτύου, τη μείωση της καθυστέρησης και τη βελτίωση των μηχανισμών συγχρονισμού, ώστε να είναι πιο δύσκολο για τους επιτιθέμενους να χειραγωγούν τη διάδοση των μπλοκ και να εκτελούν με επιτυχία στρατηγικές εγωιστικής εξόρυξης. Τα κανάλια κατάστασης (state channels) και οι δευτερεύουσες αλυσίδες (side chains), μπορούν να βοηθήσουν στην ανακούφιση της συμφόρησης και τη μείωση της καθυστέρησης στο κύριο blockchain, επεξεργάζοντας συναλλαγές εκτός αλυσίδας και στη συνέχεια διακανονίζοντάς τις περιοδικά στην αλυσίδα. [102]

6.3 Επίθεση από Μακριά

6.3.1 Κενά

Η ανίχνευση επιθέσεων μεγάλης εμβέλειας σε πραγματικό χρόνο μπορεί να αποτελέσει πρόκληση λόγω της μυστικής φύσης αυτών των επιθέσεων, οι οποίες μπορεί να περιλαμβάνουν τη μυστική συσσώρευση ενός σημαντικού ποσοστού μπλοκ για μεγάλο χρονικό διάστημα.

6.3.2 Κατευθύνσεις

Διερεύνηση προηγμένων μηχανισμών παρακολούθησης και ανίχνευσης για τον εντοπισμό ύποπτων μοτίβων συμπεριφοράς που μπορεί να υποδηλώνουν επίθεση μεγάλης εμβέλειας. Αυτό θα μπορούσε να περιλαμβάνει τη χρήση αλγορίθμων μηχανικής μάθησης και τεχνικών ανίχνευσης ανωμαλιών για την αναγνώριση μη φυσιολογικών κινήσεων μεριδίων ή μοτίβων ψηφοφορίας. Πιο συγκεκριμένα, τα μοντέλα μηχανικής μάθησης μπορούν να εκπαιδευτούν για την αναγνώριση μοτίβων που σχετίζονται με επιθέσεις μεγάλης εμβέλειας με βάση ιστορικά δεδομένα blockchain. Αναλύοντας χαρακτηριστικά, όπως η συμπεριφορά των επικυρωτών, η κατανομή των συμμετοχών, ο όγκος των συναλλαγών και η δραστηριότητα του δικτύου, αυτά τα μοντέλα μπορούν να μάθουν να αναγνωρίζουν ύποπτη δραστηριότητα ενδεικτική μιας επίθεσης μεγάλης εμβέλειας. [103]

6.4 Επίθεση Δωροδοκίας

6.4.1 Κενά

Πολλές συναλλαγές blockchain έχουν σχεδιαστεί για να είναι διαφανείς και ανιχνεύσιμες, κάτι που μπορεί να είναι επωφελές, ωστόσο, αυτή η διαφάνεια μπορεί να εμποδίσει το απόρρητο, καθιστώντας ευκολότερο για τους κακόβουλους παράγοντες να εντοπίσουν πιθανούς στόχους για επιθέσεις δωροδοκίας.

6.4.2 Κατευθύνσεις

Τα μελλοντικά συστήματα blockchain μπορεί να χρειαστεί να επιτύχουν μια καλύτερη ισορροπία μεταξύ διαφάνειας και ιδιωτικότητας. Αυτό θα μπορούσε να περιλαμβάνει την ανάπτυξη τεχνολογιών με επίκεντρο το απόρρητο, όπως αποδείξεις μηδενικής γνώσης ή κρυπτογραφικές τεχνικές διατήρησης της ιδιωτικής ζωής για την ενίσχυση του απορρήτου των συναλλαγών, διατηρώντας παράλληλα την ακεραιότητα του συνολικού συστήματος.

6.5 Επίθεση Διπλής Δαπάνης

6.5.1 Κενά

Πολλές υπάρχουσες μελέτες επικεντρώνονται σε στατικές στρατηγικές για την αποτροπή επιθέσεων διπλής δαπάνης, όπως εισαγωγή παρατηρητών και ειδοποιήσεις μεταξύ ομότιμων. Ωστόσο, υπάρχει ανάγκη για έρευνα σχετικά με δυναμικές στρατηγικές που μπορούν να προσαρμόζονται στα εξελισσόμενα μέσα και τις τακτικές των επιθέσεων. Αυτό περιλαμβάνει τη διερεύνηση προληπτικών αντιμέτρων που μπορούν να ανιχνεύουν και να μετριάζουν τις διπλές δαπάνες σε πραγματικό χρόνο.

6.5.2 Κατευθύνσεις

Εφαρμογή αλγορίθμων μηχανικής μάθησης που μπορούν να αναλύουν μοτίβα συναλλαγών σε πραγματικό χρόνο για τον εντοπισμό ύποπτης συμπεριφοράς που υποδηλώνει διπλές δαπάνες. Αυτοί οι αλγόριθμοι μπορούν να μαθαίνουν συνεχώς από νέα δεδομένα για να βελτιώνουν την ακρίβειά τους και να προσαρμόζονται στις εξελισσόμενες τεχνικές διπλών δαπανών. [104]

6.6 Επίθεση Επανάληψης

6.6.1 Κενά

- Ένα σημαντικό κενό στην πρόληψη επιθέσεων επανάληψης στα blockchain είναι η έλλειψη τυποποιημένων λύσεων για τη συμβατότητα μεταξύ αλυσίδων. Καθώς εμφανίζονται διαφορετικά δίκτυα blockchain με διάφορους μηχανισμούς συναίνεσης και διαφορετικές πλατφόρμες έξυπνων συμβολαίων, υπάρχει ανάγκη για πρωτόκολλα και πρότυπα που αποτρέπουν τις επιθέσεις επανάληψης κατά τη διάρκεια συναλλαγών κατά μήκος αλυσίδων.

- Οι επιθέσεις αναπαραγωγής μπορεί να είναι δύσκολο να εντοπιστούν σε πραγματικό χρόνο, εφόσον δεν έχουν παρθεί αντίμετρα κατά την διακλάδωση του blockchain για αυτές. Αυτό ισχύει κυρίως στα δίκτυα blockchain που αυξάνονται σε μέγεθος και όγκο συναλλαγών.

6.6.2 Κατευθύνσεις

- Οι μελλοντικές εργασίες θα πρέπει να στοχεύουν στη δημιουργία μηχανισμών και προτύπων πρόληψης επιθέσεων επανάληψης, όπως έχει κάνει το Ethereum με το ChainID (αναγνωριστικό αλυσίδας), το οποίο όμως δεν ενεργοποιημένο στους χρήστες από προεπιλογή.

- Θα πρέπει να αναπτυχθούν εργαλεία εντοπισμού αυτών των επιθέσεων, για παράδειγμα με την βοήθεια μηχανικής μάθησης, ιδιαίτερα για τα blockchain που δεν έχουν λάβει κατάλληλα αντίμετρα κατά των επιθέσεων επανάληψης μετά την διακλάδωση. Αυτό θα είναι χρήσιμο σε περιπτώσεις που αν ο εντοπισμός γίνει έγκαιρα, δεν θα χρειαστεί η αναδιοργάνωση της αλυσίδας για να αντιμετωπιστεί το πρόβλημα αλλά η ακύρωση ενός μικρού αριθμού συναλλαγών.

6.7 Επίθεση Έκλειψης

6.7.1 Κενά

Η ανίχνευση των επιθέσεων έκλειψης μπορεί να είναι δύσκολη, και έχει διεξαχθεί περιορισμένη έρευνα σχετικά με την ανάλυση της συμπεριφοράς των επιτιθέμενων που εκτελούν τέτοιες επιθέσεις. Η κατανόηση των κινήτρων, των στρατηγικών και των μοτίβων των επιτιθέμενων των επιθέσεων έκλειψης μπορεί να προσφέρει πολύτιμες πληροφορίες για την ανάπτυξη αποτελεσματικότερων τεχνικών ανίχνευσης και μετριασμού.

6.7.2 Κατευθύνσεις

Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στην ανάλυση της συμπεριφοράς των κακόβουλων κόμβων πριν και κατά τη διάρκεια των επιθέσεων έκλειψης για τον εντοπισμό έγκαιρων προειδοποιητικών σημάτων και την πρόβλεψη πιθανών φορέων επίθεσης. Συγκεκριμένα, η εφαρμογή αρχών από τη θεωρία γραφημάτων και την ανάλυση δικτύων για τη μελέτη της συνδεσιμότητας και των αλληλεπιδράσεων μεταξύ των κόμβων σε ένα δίκτυο blockchain θα μπορούσε να προσφέρει πληροφορίες σχετικά με πιθανούς φορείς επιθέσεων και ύποπτη συμπεριφορά κόμβων. Η μελλοντική έρευνα θα μπορούσε να διερευνήσει αλγορίθμους και τεχνικές για τον εντοπισμό ανώμαλων δομών δικτύου και την ανίχνευση κόμβων με ανώμαλα μοτίβα επικοινωνίας ενδεικτικά επιθέσεων έκλειψης. [104]

6.8 Επίθεση Sybil

6.8.1 Κενά

Η υπάρχουσα έρευνα σχετικά με τις επιθέσεις Sybil συχνά παραβλέπει τις προκλήσεις της κλιμάκωσης, ιδίως σε μεγάλης κλίμακας δίκτυα blockchain με εκατομμύρια κόμβους. Οι παραδοσιακοί μηχανισμοί ανίχνευσης Sybil μπορεί να καταστούν υπολογιστικά μη πρακτικοί σε τέτοια περιβάλλοντα, οδηγώντας σε προβλήματα κλιμάκωσης.

6.8.2 Κατευθύνσεις

Η μελλοντική έρευνα θα πρέπει να διερευνήσει κλιμακούμενους και αποτελεσματικούς αλγορίθμους ανίχνευσης Sybil που μπορούν να χειριστούν το αυξανόμενο μέγεθος και την πολυπλοκότητα των δικτύων blockchain χωρίς να διακυβεύεται η ακρίβεια ή η απόδοση της ανίχνευσης. Αυτό θα μπορούσε να γίνει με εξερεύνηση τεχνικών κλιμακούμενου διαμερισμού του δικτύου που διαιρούν το δίκτυο blockchain σε μικρότερα, πιο διαχειρίσιμα τμήματα, διατηρώντας παράλληλα τη συνδεσιμότητα και την επικοινωνία μεταξύ των διαμερισμάτων. Αυτή η προσέγγιση μπορεί να διευκολύνει την αποτελεσματικότερη ανίχνευση Sybil, εστιάζοντας τις προσπάθειες ανίχνευσης σε μικρότερα τμήματα του δικτύου και μειώνοντας την υπολογιστική επιβάρυνση.

6.9 Επίθεση Χρονοκλοπής

6.9.1 Κενά

Τα δίκτυα blockchain συχνά βασίζονται σε εξωτερικές πηγές χρόνου για συγχρονισμό. Ωστόσο, τα πιθανά τρωτά σημεία που εισάγονται από την αλληλεπίδραση μεταξύ των πρωτοκόλλων blockchain και των εξωτερικών πηγών ώρας δεν έχουν διερευνηθεί επαρκώς.

6.9.2 Κατευθύνσεις

Θα πρέπει να διερευνηθούν οι εξαρτήσεις μεταξύ των δικτύων blockchain και των εξωτερικών πηγών χρόνου, αξιολογώντας πώς οι ευπάθειες στα εξωτερικά πρωτόκολλα χρόνου μπορεί να επηρεάσουν την ασφάλεια blockchain. Θα πρέπει να πραγματοποιηθεί ανάπτυξη στρατηγικών για την ενίσχυση της ασφάλειας και της ανθεκτικότητας των δικτύων blockchain με την αντιμετώπιση πιθανών αδυναμιών στην ενσωμάτωση με εξωτερικές πηγές χρόνου. Οι μελλοντικές κατευθύνσεις θα μπορούσαν να βασιστούν σε πολλαπλές εξωτερικές πηγές χρόνου, όπως δορυφόρους GPS, ατομικά ρολόγια και αξιόπιστους διακομιστές NTP (Πρωτόκολλο Χρόνου Δικτύου). Με τη διασταύρωση των χρονοσφραγίδων από διαφορετικές πηγές, το δίκτυο μπορεί να ανιχνεύσει και να μετριάσει τις ασυμφωνίες ή τις επιθέσεις σε μία μόνο πηγή ώρας.

6.10 Επίθεση DNS

6.10.1 Κενά

Οι συναλλαγές blockchain θεωρούνται συχνά αμετάβλητες, γεγονός που εγείρει ανησυχίες σχετικά με την ιδιωτικότητα και την εμπιστευτικότητα των δεδομένων DNS που είναι αποθηκευμένα σε ένα blockchain.

6.10.2 Κατευθύνσεις

Απαιτείται έρευνα για την ανάπτυξη τεχνικών για τη διατήρηση της ιδιωτικότητας, ενώ παράλληλα διασφαλίζεται η ακεραιότητα των εγγραφών DNS που είναι αποθηκευμένες σε ένα blockchain. Οι αποδείξεις μηδενικής γνώσης (Zero-Knowledge Proofs ή ZKP) επιτρέπουν σε ένα μέρος (αυτόν που θέλει να αποδείξει) να αποδείξει σε ένα άλλο μέρος (τον επαληθευτή) ότι μια δήλωση είναι αληθής χωρίς να αποκαλύπτει καμία πληροφορία πέρα από την εγκυρότητα της ίδιας της δήλωσης. Η έρευνα μπορεί να επικεντρωθεί στην ενσωμάτωση τεχνικών ZKP σε συστήματα blockchain DNS, ώστε να επιτρέπονται επαληθεύσιμες συναλλαγές χωρίς να αποκαλύπτονται ευαίσθητες λεπτομέρειες εγγραφής DNS. [105]

6.11 Επίθεση DDoS

6.11.1 Κενά

Οι παραδοσιακές τεχνικές ανίχνευσης και μετριασμού DDoS ενδέχεται να μην είναι άμεσα εφαρμόσιμες σε συστήματα blockchain λόγω της αποκεντρωμένης φύσης τους. Απαιτείται έρευνα για την ανάπτυξη εξειδικευμένων τεχνικών ανίχνευσης και μετριασμού που είναι προσαρμοσμένες στα δίκτυα blockchain, λαμβάνοντας υπόψη παράγοντες όπως οι μηχανισμοί συναίνεσης, η ομότιμη επικοινωνία και η εκτέλεση έξυπνων συμβολαίων.

6.11.2 Κατευθύνσεις

Τα δίκτυα blockchain διαθέτουν συχνά περιορισμένους πόρους, όπως εύρος ζώνης και υπολογιστική ισχύ. Η μελλοντική έρευνα μπορεί να διερευνήσει την ανάπτυξη αλγορίθμων δυναμικής κατανομής πόρων που κατανέμουν προσαρμοστικά τους πόρους με βάση τις τρέχουσες συνθήκες του δικτύου και τις πιθανές απειλές επιθέσεων DDoS. Αυτοί οι αλγόριθμοι θα μπορούσαν να δώσουν προτεραιότητα στις κρίσιμες λειτουργίες του δικτύου κατά τη διάρκεια επιθέσεων DDoS, ενώ θα μπορούσαν να αποπροσανατολίσουν προσωρινά τις λιγότερο κρίσιμες εργασίες.

6.12 Επίθεση σε Έξυπνες Συμβάσεις

6.12.1 Κενά

Ενώ έχει σημειωθεί πρόοδος στις τεχνικές τυπικής επαλήθευσης για έξυπνα συμβόλαια, εξακολουθεί να υπάρχει κενό σε ευρέως εφαρμόσιμες και φιλικές προς τον χρήστη μεθόδους για την τυπική επαλήθευση της ορθότητας και των ιδιοτήτων ασφάλειας των έξυπνων συμβολαίων. Η γεφύρωση αυτού του κενού θα βοηθούσε στον εντοπισμό τρωτών σημείων και στην πρόληψη πιθανών επιθέσεων πριν από την ανάπτυξη.

6.12.2 Κατευθύνσεις

- Ανάπτυξη διαισθητικών εργαλείων GUI που επιτρέπουν στους χρήστες να καθορίζουν διαδραστικά τις ιδιότητες που θέλουν να επαληθεύσουν και να απεικονίζουν τα αποτελέσματα της διαδικασίας επαλήθευσης. Αυτές οι γραφικές διεπαφές θα πρέπει να κρύβουν την πολυπλοκότητα των τεχνικών τυπικής επαλήθευσης πίσω από φιλικές προς το χρήστη διεπαφές, επιτρέποντας σε μη ειδικούς να τις χρησιμοποιούν εύκολα.

- Δημιουργία προκαθορισμένων προτύπων για έξυπνα συμβόλαια και ιδιότητες ασφαλείας. Οι χρήστες μπορούν να επιλέξουν ένα πρότυπο που αντιστοιχεί στον σχεδιασμό της σύμβασής τους και να καθορίσουν απαιτήσεις ασφαλείας υψηλού επιπέδου, επιτρέποντας στο εργαλείο επαλήθευσης να παράγει αυτόματα τις απαραίτητες τυπικές προδιαγραφές και να διεξάγει τη διαδικασία επαλήθευσης.

7. Συμπεράσματα

Μέσα από την εκπόνηση της παρούσας διπλωματικής εργασίας ο αναγνώστης καταλαβαίνει την καινοτομία και την συνεισφορά της τεχνολογίας Blockchain και ότι είναι μια τεχνολογία με πολλές πτυχές χρησιμότητας και με καλό μέλλον. Γίνεται όμως επίσης κατανοητό ότι δεν είναι μια άτρωτη τεχνολογία και σίγουρα υπάρχουν πολλές επιθέσεις που μπορούν να συμβούν και να δημιουργήσουν προβλήματα, σε διάφορα στρώματα της, τα κύρια εκ των οποίων είναι ο μηχανισμός συναίνεσης, η συναλλαγή, το δίκτυο και τα έξυπνα συμβόλαια. Στην πλειοψηφία των επιθέσεων αυτών όμως υπάρχουν τρόποι είτε πρόληψης, είτε ανίχνευσης, είτε αντιμετώπισης για τους οποίους θα πρέπει οι χρήστες να είναι ενημερωμένοι.

Όσο το Blockchain αρχίζει να χρησιμοποιείται όλο και περισσότερο στις ζωές μας, γίνεται κατανοητό ότι πέραν από την ενημέρωση των χρηστών, θα πρέπει να βελτιωθούν και οι τρόποι αντιμετώπισης των επιθέσεων, έτσι ώστε οι τελευταίες να μειωθούν σε όσο το δυνατόν μεγαλύτερο βαθμό, κάτι που θα οδηγήσει σε ακόμα μεγαλύτερη εμπιστοσύνη των χρηστών στην τεχνολογία.

Βιβλιογραφία

[1] Blockchain. (2024). Στο Wikipedia. https://en.wikipedia.org/w/index.php?title=Blockchain&oldid=1211228500

[2] What Is Blockchain? | IBM. (χ.χ.). Ανακτήθηκε 15 Σεπτέμβρη 2023, από https://www.ibm.com/topics/blockchain

[3] What Is Blockchain Technology? How Does It Work? | Built In. (χ.χ.). Ανακτήθηκε 17 Ιουνίου 2023, από https://builtin.com/blockchain

[4] What Is Blockchain and How Does It Work? | Synopsys. (χ.χ.). Ανακτήθηκε 17 Ιουνίου 2023, από https://www.synopsys.com/glossary/what-is-blockchain.html

[5] What is Blockchain Technology? How Does Blockchain Work? [Updated]. (χ.χ.). Simplilearn.Com. Ανακτήθηκε 17 Ιουνίου 2023, από https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology

[6] What is a blockchain? | Coinbase. (χ.χ.). Ανακτήθηκε 17 Ιουνίου 2023, από https://www.coinbase.com/learn/crypto-basics/what-is-a-blockchain

[7] What is a blockchain? | Coinbase. (χ.χ.). Ανακτήθηκε 17 Ιουνίου 2023, από https://www.coinbase.com/learn/crypto-basics/what-is-a-blockchain

[8]Team, S. C. (2022, Αύγουστος 4). 11 Features of Blockchain Technology | Shardeum. Shardeum | EVM Based Sharded Layer 1 Blockchain. https://shardeum.org/blog/what-are-the-features-of-blockchain/

[9] Blockchain App Development | Important Features of Blockchain. (χ.χ.). Ανακτήθηκε 21 Ιουνίου 2023, από https://dashtechinc.com/the-important-features-of-blockchain-technology

[10] Blockchain Versions Difference. (χ.χ.). Ανακτήθηκε 21 Ιουνίου 2023, από https://originstamp.com/blog/blockchain-1-vs-2-vs-3-whats-the-difference/

[11] Different Version of BlockChain. (2021, Μάρτιος 10). GeeksforGeeks. https://www.geeksforgeeks.org/different-version-of-blockchain/

[12] Bhalla, A. (2021, Μάιος 17). Blockchain Versions Explained: A Guide for Beginners. https://www.blockchain-council.org/blockchain/blockchain-versions-explained-a-guide-for-beginners/

[13] Blockchain Architecture Explained: How It Works & How to Build. (χ.χ.). Ανακτήθηκε 24 Ιουνίου 2023, από https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

[14] How Does the Blockchain Work? (2018, Αύγουστος 14). GeeksforGeeks. https://www.geeksforgeeks.org/how-does-the-blockchain-work/

[15] Richard Davis. (2021, Ιούνιος 21). Structure of a Block in Blockchain—The Engineering Projects. https://www.theengineeringprojects.com/2021/06/structure-of-a-block-in-blockchain.html

[16] What is Blockchain Architecture—Types & Components. (χ.χ.). Ανακτήθηκε 25 Ιουνίου 2023, από https://intellipaat.com/blog/blockchain-architecture/?US

[17] Blockchain Architecture—How It Works | Casper Network. (χ.χ.). Ανακτήθηκε 25 Ιουνίου 2023, από https://casper.network/en-us/web3/blockchain/a-guide-to-blockchain-architecture/

[18] Hybrid Blockchains: Everything You Need to Know About. (2022, Νοέμβριος 16). https://www.zenledger.io/blog/hybrid-blockchain/

[19] Consensus Mechanisms in Blockchain—Shiksha Online. (χ.χ.). Ανακτήθηκε 27 Ιουνίου 2023, από https://www.shiksha.com/online-courses/articles/consensus-mechanisms-in-blockchain/

[20] Types Of Consensus Mechanisms In Blockchain—Hacken. (χ.χ.). Ανακτήθηκε 27 Ιουνίου 2023, από https://hacken.io/discover/consensus-mechanisms/

[21] Consensus Algorithm/Consensus Mechanism Innovations. (χ.χ.). Gemini. Ανακτήθηκε 27 Ιουνίου 2023, από https://www.gemini.com/cryptopedia/blockchain-consensus-mechanism-types-of-algorithm

[22] What Are Smart Contracts on Blockchain? | IBM. (χ.χ.). Ανακτήθηκε 29 Ιουνίου 2023, από https://www.ibm.com/topics/smart-contracts

[23] Smart Contracts in Blockchain. (2019, Ιανουάριος 7). GeeksforGeeks. https://www.geeksforgeeks.org/smart-contracts-in-blockchain/

[24] Levy, A. 15 Applications for Blockchain Technology. The Motley Fool. (χ.χ.). Ανακτήθηκε 3 Ιουλίου 2023, από https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/blockchain-applications/

[25] Top Applications of Blockchain in the Real World. (2021, Φεβρουάριος 27). GeeksforGeeks. https://www.geeksforgeeks.org/top-applications-of-blockchain-in-the-real-world/

[26] Top 10 Blockchain Applications in 2024. (χ.χ.). upGrad Blog. Ανακτήθηκε 3 Ιουλίου 2023, από https://www.upgrad.com/blog/top-blockchain-applications/

[27] I.-C. Lin and T.-C. Liao. "A survey of blockchain security issues and challenges. *International Journal of Network Security"*, September 2017.

[28] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen. "Exploring the attack surface of blockchain: A systematic overview", April 2019.

[29] H. Hasanova, U.-J. Baek, M.-G. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures", Jun. 2019.

[30] A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, and S. Capkun. "On the security and performance of proof of work blockchains", October 2016.

[31] P. Gazi, A. Kiayias, and A. Russell. "Stake-bleeding attacks on proof-of-stake blockchains", June 2018.

[32] W. Li, S. Andreina, J.-M. Bohli, and G. Karame. "Securing proof-of-stake blockchain protocols", September 2017.

[33] M. Castro and B. Liskov. "Practical byzantine fault tolerance and proactive recovery", November 2002.

[34] Huashan Chen, Marcus Pendleton, Laurent Njilla, "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defences", August 2019

[35] J. Niu and C. Feng. "Selfish mining in ethereum", July 2019.

[36] F. Ritz and A. Zugenmaier. "The impact of uncle rewards on selfish mining in ethereum", April 2018.

[37] 51% Attack. (χ.χ.). Privacy Canada. Ανακτήθηκε 11 Αυγούστου 2023, από https://privacycanada.net/cryptocurrency/51-attack/

[38] D. Dasgupta, J. M. Shrein, and K. D. Gupta. "A survey of blockchain from security perspective", April 2019.

[39] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," April 2018

[40] Evangelos Deirmentzoglou, Georgios Papakyriakopoulos, and Konstantinos Patsakis, "A Survey on Long-Range Attacks for Proof of Stake Protocols", February 2019

[41] P. Gaži, A. A. Kiayias. "Stake-Bleeding Attacks on Proof-of-Stake Blockchains" January 2019.

[42] Ghader Ebrahimpour, Mohammad Sayad Haghighi, "Analysis of Bitcoin Vulnerability to Bribery Attacks Launched Through Large Transactions" January 2021

[43] Lukas Konig, Stefan Unger, Peter Kieseberg and Simon Tjoa "The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks" 2020

[44] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen. "A survey on the security of blockchain systems", June 2020.

[45] Q. Bai, X. Zhou, X. Wang, Y. Xu, X. Wang, and Q. Kong. "A deep dive into blockchain selfish mining", May 2019.

[46] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin" Oct. 2012

[47] Finney Attack. (χ.χ.). Ανακτήθηκε 21 Αυγούστου 2023, από https://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack

[48] Averin A., Averina O., "Review of Blockchain Technology Vulnerabilities and Blockchain-System Attacks", October 2019

[49] Blockchain Attack Vectors: Vulnerabilities of Secure Technology | Apriorit. (χ.χ.). Ανακτήθηκε 23 Αυγούστου 2023, από https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors

[50] Botnet. (2024). Στο Wikipedia. https://en.wikipedia.org/w/index.php?title=Botnet&oldid=1200010008

[51] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. "Eclipse attacks on bitcoin's peer-to-peer network", August 2015.

[52] Y. Marcus, E. Heilman, and S. Goldberg. "Low-resource eclipse attacks on ethereum's peer-to-peer network", February 2018.

[53] J. H. Mosakheil. "Security threats classification in blockchains". May 2018.

[54] "Bitcoin developer guide" (χ.χ.). Ανακτήθηκε 25 Αυγούστου 2023, από https://bitcoin.org/en/developer-guidepeer-discovery

[55] M. Saad, M. T. Thai, and A. Mohaisen, "POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization" Jun 2018

[56] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," November 2002

[57] Bitnodes, "Global bitcoin nodes distribution". (χ.χ.). Ανακτήθηκε 25 Αυγούστου 2023, από https://bitnodes.earn.com/

[58] M. Kumar and S. Kumar, "Improving routing in large networks inside autonomous system," September 2014

[59] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," May 2017

[60] Beginner's Guide: What is ERC20? [UPDATED]—Blockchain Council. (χ.χ.). Ανακτήθηκε 25 Αυγούστου 2023, από , από https://www.blockchain-council.org/ethereum/beginners-guide-what-is-erc20/

[61] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," April 2017

[62] Kevin Jonathan, Annie Kartika Sari, "Security Issues and Vulnerabilities On A Blockchain System: A Review", December 2019

[63] P. Zhang, F. Xiao, and X. Luo. "Solidityсheck: Quickly detecting smart contract problems through regular expressions", November 2019.

[64] S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark. "A first look at browser-based cryptojacking", April 2018

[65] Setting Up Cross-Domain Request Enforcement. (χ.χ.). Ανακτήθηκε 27 Αυγούστου 2023, από https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-12-1-0/17.html

[66] Viewnodes. (2019, Μάιος 7). The history of 51% attacks and the implications for Bitcoin. HackerNoon.Com. https://medium.com/hackernoon/the-history-of-51-attacks-and-the-implications-for-bitcoin-ec1aa0f20b94

[67] Xiaotong Sun, Bribes to Miners: Evidence from Ethereum, March 2022

[68] Viewnodes. (2019, Μάιος 7). The history of 51% attacks and the implications for Bitcoin. HackerNoon.Com. https://medium.com/hackernoon/the-history-of-51-attacks-and-the-implications-for-bitcoin-ec1aa0f20b94

[69] Barwikowski, H., Bartosz. (2023, Ιούνιος 29). 51% Attack: The Concept, Risks & Prevention. Hacken. https://hacken.io/discover/51-percent-attack/

[70] Understanding the 51% Attack in Crypto: Risks and Prevention Measures—WazirX Blog. (χ.χ.). Ανακτήθηκε 2 Σεπτεμβρίου 2023, από https://wazirx.com/blog/understanding-the-51-attack-in-crypto-risks-and-prevention-measures/

[71] Ethereum Classic Attacker Double-Spends $1.68M: Report—CoinDesk. (χ.χ.). Ανακτήθηκε 2 Σεπτεμβρίου 2023, από https://www.coindesk.com/markets/2020/08/07/ethereum-classic-attacker-successfully-double-spends-168m-in-second-attack-report/

[72] Zhaojie Wang, Qingzhe Lv, Zhaobo Lu, "ForkDec: Accurate Detection for Selfish Mining" November 2021

[73] Ethan Heilman, "One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner", January 2014

[74] Peter Gazi, Aggelos Kiayias, Alexander Russell, "Stake-Bleeding Attacks on Proof-of-Stake Blockchains" June 2018

[75] Joseph Bonneau, Edward W. Felten, Steven Goldfeder, Joshua A. Kroll, and Arvind Narayanan, "Why buy when you can rent? Bribery attacks on Bitcoin consensus", February 2016

[76] Ghassan O. Karame, Elli Androulaki, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin" 2012

[77] Ghassan O. Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, "Misbehavior in Bitcoin: A Study of Double-Spending and Accountability" May 2015

[78] John P. Podolanko, Jiang Ming, Matthew Wright, "Countering Double-Spend Attacks on Bitcoin Fast-Pay Transactions" 2017

[79] Tobias Bamert, Christian Decker, Lennart Elsen, Roger Wattenhofer, Samuel Welten, "Have a Snack, Pay with Bitcoins" September 2013

[80] Eclipse Attacks Explained: What Are They? (χ.χ.). Gemini. Ανακτήθηκε 4 Σεπτεμβρίου 2023, από https://www.gemini.com/cryptopedia/eclipse-attacks-defense-bitcoin, https://www.gemini.com/cryptopedia/eclipse-attacks-defense-bitcoin

[81] What is an Eclipse Attack? (2022, Φεβρουάριος 21). GeeksforGeeks. https://www.geeksforgeeks.org/what-is-an-eclipse-attack/

[82] Sybil Attack. (2019, Ιανουάριος 10). GeeksforGeeks. https://www.geeksforgeeks.org/sybil-attack/

[83] Sybil Attack in Blockchain: Examples & Prevention—Hacken. (χ.χ.). Ανακτήθηκε 5 Σεπτεμβρίου 2023, από https://hacken.io/insights/sybil-attacks/

[84] Guangkai Ma, Chunpeng Ge, Lu Zhou, "Achieving reliable timestamp in the bitcoin platform" May 2020

[85] Sigurdsson, Gudmundur Giaretta, Alberto Dragoni, Nicola "Vulnerabilities and Security Breaches in Cryptocurrencies", March 2019

[86] DNS Spoofing or DNS Cache poisoning. (2018, Ιανουάριος 12). GeeksforGeeks. https://www.geeksforgeeks.org/dns-spoofing-or-dns-cache-poisoning/

[87] How do you protect your blockchain network from DDoS attacks? (χ.χ.). Ανακτήθηκε 7 Σεπτεμβρίου 2023, από https://www.linkedin.com/advice/0/how-do-you-protect-your-blockchain-network-from

[88] DDoS in Blockchain. (2022, Αύγουστος 13). GeeksforGeeks. https://www.geeksforgeeks.org/ddos-in-blockchain/

[89] How does BGP hijacking work and what are the risks? | TechTarget. (χ.χ.). Ανακτήθηκε 8 Σεπτεμβρίου 2023, από https://www.techtarget.com/searchsecurity/tip/How-does-BGP-hijacking-work-and-what-are-the-risks

[90] Michael Rodler, Wenting Li, Ghassan O. Karame, Lucas Davi Sereum: "Protecting Existing Smart Contracts Against Re-Entrancy Attacks" December 2018

[91] Reentrancy Attack in Smart Contracts. (2023, Ιανουάριος 30). GeeksforGeeks. https://www.geeksforgeeks.org/reentrancy-attack-in-smart-contracts/

[92] Overflow and Underflow Attacks on Smart Contracts. (2022, Δεκέμβριος 31). GeeksforGeeks. https://www.geeksforgeeks.org/overflow-and-underflow-attacks-on-smart-contracts/

[93] Jianbo Gao, Han Liu, Chao Liu, Qingshan Li, "EASYFLOW : Keep Ethereum Away From Overflow" May 2019

[94] A.A. Andryukhin, "Phishing Attacks and Preventions in Blockchain Based Projects" March 2019

[95] What Is a Replay Attack & How Does It Affect Blockchains? | Bybit Learn. (χ.χ.). Ανακτήθηκε 9 Σεπτεμβρίου 2023, από https://learn.bybit.com/blockchain/what-is-a-replay-attack/

[96] Marie Vasek, Micah Thornton, Tyler Moore, "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem" January 2014

[97] Rashid Tahir, Muhammad Huzaifa, Anupam Das, Mohammad Ahmad,
Carl Gunter, Fareed Zaffar, Matthew Caesar, and Nikita Borisov, "Mining on Someone Else's Dime: Mitigating Covert Mining Operations in Clouds and Enterprises", October 2017

[98] KiranmaiBalijepalli. (2023, Σεπτέμβριος 25). Vulnerabilities in Consensus Mechanisms: What You Need to Know. Coinmonks. https://medium.com/coinmonks/vulnerabilities-in-consensus-mechanisms-what-you-need-to-know-3db69b4af7a6

[99] Technological evolution up to Blockchain 4.0 |OpenMind. (χ.χ.). Ανακτήθηκε 10 Σεπτεμβρίου 2023, από https://www.bbvaopenmind.com/en/technology/digital-world/blockchain-4-0/

[100] Acharya, D. P. (2022, Μάιος 12). An In-Depth Guide on the Types of Blockchain Nodes. Geekflare. https://geekflare.com/blockchain-nodes-guide/

[101] Blockchain Reference Architecture – A Smarter way to implement Agile and Effective Blockchain Solutions. (χ.χ.). Ανακτήθηκε 12 Σεπτεμβρίου 2023, από https://www.coforge.com/resource-library/white-papers/blockchain-reference-architecture-a-smarter-way-to-implement-agile-and-effective-blockchain-solutions

[102] A Comprehensive Guide On Blockchain Layer 2 Scaling Solutions | by Annabelle Darcie | NFT Daily Dose | Medium. (χ.χ.). Ανακτήθηκε 12 Σεπτεμβρίου 2023, από https://medium.com/nftdailydose/a-comprehensive-guide-on-blockchain-layer-2-scaling-solutions-27957657a5b4

[103] Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen, "Anomaly Detection in Blockchain Networks: A Comprehensive Survey", September 2022

[104] K. Venkatesan & Syarifah Bahiyah Rahayu, "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques", January 2024

[105] Takyar, A. (2021, Σεπτέμβριος 6). What is Zero Knowledge Proof and its role in blockchain? LeewayHertz - AI Development Company. https://www.leewayhertz.com/zero-knowledge-proof-and-blockchain/

[106] Zhaojie Wang, Qingzhe Lv,Zhaobo Lu,**Yilei Wang** and Shengjie Yue, "ForkDec: Accurate Detection for Selfish Mining Attacks", November 2021