



ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ
ΣΤΗ ΒΙΟΙΑΤΡΙΚΗ

Λύσεις Ασφαλείας για Web3 εφαρμογές

Παπαγεωργίου Κωνσταντίνος

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
Υπεύθυνος
Σπαθούλας Γεώργιος
Μέλος Ε.ΔΙ.Π.

Λαμία, 2024



**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ
ΒΙΟΙΑΤΡΙΚΗ**

Λύσεις Ασφαλείας για Web3 εφαρμογές

Παπαγεωργίου Κωνσταντίνος

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
Επιβλέπων
Σπαθούλας Γεώργιος
Μέλος Ε.ΔΙ.Π.**

Λαμία, 2024

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις (1), που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάστηκαν, χωρίς αναφορά στην πηγή.
2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.
3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια.
4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 3 Ιουνίου 2025

Ο – Η Δηλ.

(Υπογραφή)

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.

Λύσεις Ασφαλείας για Web3 εφαρμογές

Παπαγεωργίου Κωνσταντίνος

Τριμελής Επιτροπή:

Γεώργιος Σπαθούλας (επιβλέπων)

Αθανάσιος Κακαρούντας

Αθανάσιος Λουκόπουλος

Περίληψη

Η παρούσα εργασία διερευνά τις προκλήσεις ασφαλείας που εισάγουν οι αποκεντρωμένες εφαρμογές και η τεχνολογία αλυσίδας μπλοκ στο οικοσύστημα Web3. Επισημαίνονται ευπάθειες στα έξυπνα συμβόλαια, τα οποία μπορεί να οδηγήσουν σε οικονομικές απώλειες, και προτείνει την ανάπτυξη ενός συστήματος ασφαλείας που έχει σχεδιαστεί για να ανιχνεύει και να αποτρέπει συναλλαγές με δυνητικά ευάλωτες ή κακόβουλες αποκεντρωμένες εφαρμογές. Το προτεινόμενο σύστημα, που ονομάζεται «Παρατηρητήριο», στοχεύει να ενισχύσει την ασφάλεια αναλύοντας έξυπνα συμβόλαια και τις ιστοσελίδες που φιλοξενούν αποκεντρωμένες εφαρμογές που βασίζονται σε αυτά, παρέχοντας στους χρήστες και κυρίως στα ψηφιακά πορτοφόλια κρυπτονομισμάτων, αξιόπιστες πληροφορίες ασφαλείας. Με μια αρθρωτή αρχιτεκτονική, το σύστημα είναι προσαρμόσιμο και επεκτάσιμο, συμβάλλοντας στις συνεχείς προσπάθειες για τη βελτίωση της ασφάλειας και της αξιοπιστίας των αποκεντρωμένων εφαρμογών.

Abstract

Η άφιξη της Web3 τεχνολογίας και των αποκεντρωμένων εφαρμογών, εισήγαγε μια νέα εποχή ψηφιακής αλληλεπίδρασης, η οποία χαρακτηρίζεται από διαφάνεια, αυτονομία και ενδυνάμωση των χρηστών. Ωστόσο, ο αποκεντρωμένος χαρακτήρας αυτών των εφαρμογών, ιδίως εκείνων που βασίζονται στην τεχνολογία αλυσίδας μπλοκ, επιφέρει επίσης σημαντικές προκλήσεις στον τομέα της ασφάλειας. Τα έξυπνα συμβόλαια, τα οποία αποτελούν αναπόσπαστο μέρος των αποκεντρωμένων εφαρμογών, παρουσιάζουν συχνά ευπάθειες που μπορούν να οδηγήσουν σε σημαντικές οικονομικές απώλειες. Για την αντιμετώπιση αυτών των προκλήσεων, η παρούσα εργασία προτείνει την ανάπτυξη ενός συστήματος ασφαλείας που έχει σχεδιαστεί με απώτερο σκοπό την αποτροπή συναλλαγών με πιθανώς ευπαθή ή και κακόβουλες αποκεντρωμένες εφαρμογές, εντοπίζοντας ευπάθειες στα έξυπνα συμβόλαια και στις ιστοσελίδες που τα φιλοξενούν. Η ανάπτυξη αυτού του συστήματος στοχεύει στον μετριασμό των κινδύνων σε εφαρμογές Web3. Παρέχοντας στα ψηφιακά πορτοφόλια κρυπτονομισμάτων που αναλαμβάνουν τις συναλλαγές και κατ' επέκταση και στους χρήστες, αξιοποιήσιμες πληροφορίες σχετικά με την ασφάλεια των αποκεντρωμένων εφαρμογών. Το σύστημα ονόματι «Παρατηρητήριο» στοχεύει στην προώθηση ενός ασφαλέστερου και πιο αξιόπιστου αποκεντρωμένου οικοσυστήματος.

Περιεχόμενα

1	Εισαγωγή	8
2	Σχετικές εργασίες	11
3	Θέματα ασφάλειας στο Web3	17
1	Παρασκήνιο του οικοσυστήματος	17
1.1	Blockchain	17
2	Απειλές ασφαλείας στο Web3	21
2.1	Επίπεδο δεδομένων	21
2.2	Επίπεδο δικτύου	22
2.3	Επίπεδο συναίνεσης	23
2.4	Επίπεδο κινήτρου	26
2.5	Επίπεδο συμβολαίου	27
2.6	Επίπεδο εφαρμογής	31
4	Σχεδιασμός συστήματος	33
1	Επισκόπηση	33
2	Οντότητες	33
3	Αλληλεπιδράσεις στο σύστημα	35
5	Υλοποίηση συστήματος	38
1	Εργαλεία και τεχνολογίες	38
1.1	Ενορχήστρωση	38
1.2	Παρατηρητήριο - Watchtower	40
1.3	Βάση Δεδομένων	42

1.4	Εύρεση ευπαθειών	45
1.5	Επικοινωνία μεταξύ των στοιχείων του συστήματος	46
2	Δημιουργία πιστοποιητικού	46
3	Υπολογισμός βαθμού επικινδυνότητας	52
4	Διαδικασία επαλήθευσης πιστοποιητικού	57
6	Συμπεράσματα	62
	Βιβλιογραφία	64
	Ξενόγλωσση βιβλιογραφία	64

Κεφάλαιο 1

Εισαγωγή

Η ραγδαία εξέλιξη της τεχνολογίας αλυσίδας μπλοκ (blockchain) και των αποκεντρωμένων εφαρμογών (decentralized applications - dApps) έχει αποδώσει ένα νέο τρόπο με τον οποίο αλληλεπιδρούμε με τα ψηφιακά συστήματα. Με τη χρήση του Web3, έχει δημιουργηθεί η ανάγκη για ένα αποκεντρωμένο, χρηστοκεντρικό οικοσύστημα όπου τα άτομα έχουν μεγαλύτερο έλεγχο των δεδομένων και των συναλλαγών τους. Ωστόσο, αυτή η νέα τάση εισάγει επίσης μοναδικές προκλήσεις ασφαλείας, ιδίως στο πλαίσιο των έξυπνων συμβολαίων (smart contracts), των αποκεντρωμένων χρηματοοικονομικών εφαρμογών (DeFi) και γενικότερα οποιαδήποτε αποκεντρωμένη εφαρμογή που συναλλάσσεται χρηματοοικονομικά με τους χρήστες. Τα έξυπνα συμβόλαια, είναι ένας αυτοεκτελούμενος κώδικας που στον πυρήνα του εκτελεί συναλλαγές όταν πληρούνται κάποιες προκαθορισμένες συνθήκες. Ενώ τα έξυπνα συμβόλαια προσφέρουν διαφάνεια και αυτοματοποίηση, είναι επίσης επιρρεπείς σε ευπάθειες που μπορούν να οδηγήσουν σε σημαντικές οικονομικές απώλειες.

Το 2024, οι πλατφόρμες κρυπτονομισμάτων παρουσίασαν σημαντική αύξηση των περιστατικών παραβίασης, με το σύνολο των κλεμμένων κεφαλαίων να αυξάνεται κατά περίπου 21% σε ετήσια βάση σε 2,2 δισεκατομμύρια δολάρια [31]. Ο αριθμός των μεμονωμένων περιστατικών hacking αυξήθηκε επίσης από 282 το 2023 σε 303 το 2024. Βορειοκορεάτες χάκερς ήταν ιδιαίτερα δραστήριοι, κλέβοντας περίπου 1,34 δισεκατομμύρια δολάρια σε 47 περιστατικά, το οποίο αντιπροσωπεύει το 61% του συνολικού ποσού που εκλάπη για το έτος 2024.

Ένα αξιοσημείωτο περιστατικό συνέβη το 2023 όπου το MetaMask, ένα ευρέως χρησιμοποιούμενο ψηφιακό πορτοφόλι κρυπτονομισμάτων που ενσωματώνεται στην δίκτυο αλυσίδας μπλοκ Ethereum, υπήρξε στόχος επιθέσεων ψαρέματος με στόχο την κλοπή των φράσεων

με τις οποίες αποκτάται πρόσβαση στο ψηφιακό πορτοφόλι των χρηστών [23]. Σε αυτές τις επιθέσεις, οι επιτιθέμενοι δημιουργούσαν ψεύτικες ιστοσελίδες που μιμούνται το περιβάλλον εργασίας του MetaMask για να εξαπατήσουν τους χρήστες ώστε να αποκαλύψουν τις μυστικές φράσεις ανάκτησης. Οι φράσεις αυτές επέτρεπαν στους επιτιθέμενους να αποκτήσουν πρόσβαση στα ψηφιακά πορτοφόλια των θυμάτων και να κλέψουν τα χρήματά τους. Αξίζει να αναφερθεί ότι οι απατεώνες εκμεταλλεύτηκαν το Typeform, μια νόμιμη διαδικτυακή υπηρεσία δημιουργίας φορμών, για να ανακατευθύνουν τους χρήστες σε ιστοσελίδες phishing που έχουν σχεδιαστεί για τη σύλληψη φράσεων ανάκτησης πρόσβασης σε ψηφιακά πορτοφόλια κρυπτονομισμάτων. Ήταν μία διαφορετική τακτική σε σχέση με τις προηγούμενες τακτικές, όπου οι επιτιθέμενοι χρησιμοποιούσαν κυρίως κακόβουλες εφαρμογές Android και iOS για να στοχεύσουν χρήστες του MetaMask.

Σε αυτό το άρθρο με τίτλο «“Payzero” Scams and The Evolution of Asset Theft in Web3» [1], αναφέρει ένα απατηλό σχήμα στο οικοσύστημα Web3, γνωστό ως «Payzero». Σε αυτές τις απάτες, οι επιτιθέμενοι εξαπατούν τα θύματα ώστε να μεταβιβάσουν την κυριότητα των ψηφιακών περιουσιακών τους στοιχείων χωρίς να λάβουν καμία πληρωμή σε αντάλλαγμα. Αυτό επιτυγχάνεται συχνά εξαπατώντας τους χρήστες ώστε να υπογράψουν συναλλαγές που εξουσιοδοτούν τη μεταβίβαση περιουσιακών στοιχείων, εκμεταλλευόμενοι την πολυπλοκότητα των μηχανισμών ελέγχου ταυτότητας του Web3.

Τον Απρίλιο του 2018, το MyEtherWallet (MEW), ένα ευρέως χρησιμοποιούμενο ψηφιακό πορτοφόλι κρυπτονομισμάτων στο δίκτυο αλυσίδας μπλοκ στο Ethereum, υπέστη επίθεση πειρατείας στο Σύστημα Ονοματοδοσίας Διαδικτύου (Domain Name System - DNS). Οι επιτιθέμενοι παραβίασαν διακομιστές DNS, ανακατευθύνοντας τους χρήστες σε έναν ιστότοπο που μιμούταν τη διεπαφή του MEW. Παρά το γεγονός ότι τα προγράμματα περιήγησης εμφάνιζαν προειδοποιήσεις για άκυρα πιστοποιητικά στο Επίπεδο Ασφαλών Υποδοχών (Secure Sockets Layer - SSL), ορισμένοι χρήστες συνέχισαν, με αποτέλεσμα την κλοπή Ether αξίας περίπου 150,000 έως 365,000 δολαρίων. Οι επιτιθέμενοι εκμεταλλεύτηκαν ευπάθειες στο Πρωτόκολλο Πύλης Συνόρων (Border Gateway Protocol - BGP) για να ανακατευθύνουν την κυκλοφορία που προοριζόταν για την υπηρεσία DNS Route 53 της Amazon, την οποία χρησιμοποιούσε το MEW [8]. Το περιστατικό αυτό υπογραμμίζει τη σημασία της επαγρύπνησης των χρηστών σχετικά με τις προειδοποιήσεις SSL και την εξέταση της χρήσης υλικών πορτοφολιών (hardware wallets) ή μεθόδων εκτός σύνδεσης για συναλλαγές κρυπτονομισμάτων για την ενίσχυση της ασφάλειας.

Η υπόλοιπη εργασία οργανώνεται ως εξής: Στο Κεφάλαιο 3, παρουσιάζονται οι απειλές ασφαλείας που υπάρχουν στη τεχνολογία αλυσίδας μπλοκ στο οικοσύστημα Web3 και σε ποιο επίπεδο εμφανίζονται. Στο Κεφάλαιο 2 αναλύονται κάποια εργαλεία και μέθοδοι αντιμετώπισης ευπαθειών στο επίπεδο του έξυπνου συμβολαίου. Στο Κεφάλαιο 4 παρουσιάζεται ο σχεδιασμός του παρόν συστήματος – Παρατηρητηρίου (Watchtower). Στο Κεφάλαιο 5 παρουσιάζεται η υλοποίηση του συστήματος ενώ στο Κεφάλαιο 6 παρουσιάζονται τα συμπεράσματα της εργασίας και πιθανές βελτιώσεις του συστήματος που μπορούν να γίνουν στο μέλλον.

Κεφάλαιο 2

Σχετικές εργασίες

Τα περισσότερα προβλήματα που αντιμετωπίζει η τεχνολογία Web3 στο τομέα της ασφάλειας αφορούν κυρίως τον τρόπο με τον οποίο αναπτύσσονται τα έξυπνα συμβόλαια. Μια σημαντική πρόκληση που σχετίζεται με τα έξυπνες συμβόλαια είναι ο αμετάβλητος χαρακτήρας τους: αφού περαστούν στο δίκτυο αλυσίδας μπλοκ, δεν μπορούν να τροποποιηθούν ή να ενημερωθούν. Το γεγονός ότι είναι αμετάβλητο σημαίνει ότι εάν οι απαιτήσεις των χρηστών εξελιχθούν ή εάν ανακαλυφθούν σφάλματα μετά την ανάπτυξη, τα έξυπνα συμβόλαια δεν μπορούν να τροποποιηθούν με τον ίδιο τρόπο όπως οι παραδοσιακές εφαρμογές λογισμικού. Κατά συνέπεια, τυχόν ατέλειες ή σφάλματα που υπάρχουν στον κώδικα καθίστανται μόνιμα, οδηγώντας ενδεχομένως σε σημαντικές οικονομικές απώλειες. Για παράδειγμα, τα λογικά σφάλματα στον κώδικά τους μπορούν να αξιοποιηθούν από κακόβουλους φορείς, όπως αποδεικνύεται από τα περιστατικά που αναφέρθηκαν στην προηγούμενη ενότητα [27].

Επιπλέον, ο έλεγχος των έξυπνων συμβολαίων κατά τον χρόνο εκτέλεσής τους παρουσιάζει σημαντικές δυσκολίες. Αυτά τα έξυπνα συμβόλαια αλληλεπιδρούν συχνά με άλλα έξυπνα συμβόλαια και συχνά επικαλούνται εξωτερικές υπηρεσίες εκτός αλυσίδας, δημιουργώντας πολύπλοκες αλληλεξαρτήσεις. Αυτή η πολυπλοκότητα καθιστά δύσκολη τη διεξαγωγή ολοκληρωμένων δοκιμών, αυξάνοντας τον κίνδυνο να μην εντοπιστούν ευπάθειες. Οι επιτιθέμενοι έχουν ιδιαίτερο κίνητρο να εκμεταλλευτούν τέτοια σφάλματα, δεδομένου ότι τα έξυπνα συμβόλαια συχνά διαχειρίζονται σημαντικά ποσά περιουσιακών στοιχείων και κρυπτονομισμάτων. Τα δυνητικά οφέλη από την επιτυχή επίθεση σε ένα ευάλωτο έξυπνο συμβόλαιο μπορεί να είναι σημαντικά, δίνοντας κίνητρα για κακόβουλες δραστηριότητες.

Ένα από τα εργαλεία που στοχεύουν στην ανίχνευση ευπαθειών σε έξυπνα συμβόλαια είναι το ZEUS. Το ZEUS είναι ένα εργαλείο που έχει σχεδιαστεί για την ανάλυση της α-

σφάλειας και της προστασίας των έξυπνων συμβολαίων κάνοντας στατική ανάλυση. Στόχος του είναι να επαληθεύει την ορθότητα των έξυπνων συμβολαίων – εξασφαλίζοντας ότι ακολουθούν τις βέλτιστες πρακτικές προγραμματισμού – η οποία διασφαλίζει την τήρηση της επιχειρηματικής λογικής υψηλότερου επιπέδου. Για να το επιτύχει αυτό, το ZEUS χρησιμοποιεί αφηρημένη ερμηνεία και συμβολικό έλεγχο μοντέλου, μαζί με περιορισμένες ρήτρες Horn (Constrained Horn Clauses - CHCs), για να επαληθεύει γρήγορα τα έξυπνα συμβόλαια για ευπάθειες ασφαλείας. Μεταφράζει τα έξυπνες συμβόλαια από γλώσσες υψηλού επιπέδου όπως η Solidity σε μια ενδιάμεση αναπαράσταση όπως το bitcode LLVM, επιτρέποντας την ολοκληρωμένη στατική ανάλυση. Αυτή η μετάφραση επιτρέπει την ανίχνευση πιθανών αδυναμιών ασφαλείας πριν από την ανάπτυξη, καθώς τα έξυπνα συμβόλαια, αφού περάσουν στο δίκτυο αλυσίδας μπλοκ, δεν μπορούν να τροποποιηθούν ή να επιδιορθωθούν. Το ZEUS έχει υλοποιηθεί τόσο για τις πλατφόρμες αλυσίδας μπλοκ του Ethereum όσο και για το Hyperledger Fabric. Έχει αξιολογηθεί σε πάνω από 22.400 έξυπνα συμβόλαια, αποκαλύπτοντας ότι περίπου το 94,6% των έξυπνων συμβολαίων (που κατέχουν κρυπτονόμισμα αξίας άνω των 0,5 δισεκατομμυρίων δολαρίων) ήταν ευάλωτες σε τουλάχιστον ένα θέμα ασφαλείας. Ένα από τα βασικά πλεονεκτήματα του ZEUS είναι τα μηδενικά ψευδώς αρνητικά αποτελέσματα και το χαμηλό ποσοστό ψευδώς θετικών αποτελεσμάτων [20].

Ένα ακόμη εργαλείο στατικής ανάλυσης είναι το GASPER (συντομογραφία για Gas-costly Patterns checkER) είναι ένα εργαλείο που έχει σχεδιαστεί για να αναλύει το bytecode έξυπνων συμβολαίων και να εντοπίζει πρότυπα προγραμματισμού που προκαλούν κόστος καυσίμου και οδηγούν σε περιττά έξοδα κατά την εκτέλεση έξυπνων συμβολαίων στην πλατφόρμα του Ethereum. Το καύσιμο είναι μια θεμελιώδης μονάδα στο Ethereum, που αντιπροσωπεύει το υπολογιστικό κόστος που απαιτείται για την εκτέλεση λειτουργιών στην αλυσίδα μπλοκ. Δεδομένου ότι ο αναποτελεσματικός κώδικας έξυπνων συμβολαίων μπορεί να οδηγήσει σε υπερβολική κατανάλωση καυσίμου, το GASPER βοηθά τους προγραμματιστές να βελτιστοποιήσουν τα έξυπνα συμβόλαιά τους και να μειώσουν το κόστος. Το εργαλείο λειτουργεί αναλύοντας απευθείας το bytecode και δεν βασίζεται στον πηγαίο κώδικα, καθιστώντας το εφαρμόσιμο ακόμη και όταν ο πηγαίος κώδικας των έξυπνων συμβολαίων δεν είναι διαθέσιμος. Το GASPER αξιοποιεί τη συμβολική εκτέλεση για να διατρέξει όλες τις πιθανές διαδρομές εκτέλεσης σε ένα έξυπνο συμβόλαιο και να εντοπίσει τις αναποτελεσματικότητες. Συγκεκριμένα, εντοπίζει τρία αντιπροσωπευτικά μοτίβα που προκαλούν υψηλό κόστος: αχρειαστο κώδικα, αδιαφανείς προρρήσεις και ακριβές λειτουργίες μέσα σε βρό-

χους. Ο αχρείαστος κώδικας αναφέρεται σε τμήματα ενός έξυπνου συμβολαίου που δεν θα εκτελεστούν ποτέ, οδηγώντας σε περιττή κατανάλωση καυσίμου κατά την ανάπτυξη. Οι αδιαφανείς προρρήσεις είναι συνθήκες των οποίων τα αποτελέσματα είναι πάντα γνωστά εκ των προτέρων, αλλά εξακολουθούν να αξιολογούνται, σπαταλώντας καύσιμο. Οι ακριβές λειτουργίες μέσα σε βρόχους περιλαμβάνουν δαπανηρές λειτουργίες της Εικονικής Μηχανής Ethereum (Ethereum Virtual Machine - EVM), όπως ανάγνωση και εγγραφή στη μνήμη, οι οποίες θα πρέπει να βελτιστοποιούνται για την ελαχιστοποίηση του κόστους εκτέλεσης. Το GASPER λειτουργεί αποσυναρμολογώντας πρώτα το bytecode του έξυπνου συμβολαίου και κατασκευάζοντας ένα Γράφημα Ροής Ελέγχου (Control Flow Graph - CFG). Στη συνέχεια, εκτελεί συμβολική εκτέλεση για να διατρέξει όλες τις διαδρομές εκτέλεσης και να εντοπίσει μοτίβα με υψηλό κόστος καυσίμου. Για τον αχρησιμοποίητο κώδικα, το GASPER εντοπίζει τμήματα κώδικα που δεν εκτελούνται ποτέ. Για την αδιαφανή πρόρρηση, εντοπίζει διακλαδώσεις που δημιουργούνται από συνθήκες και δεν καταλήγει ποτέ σε κάποια απο αυτές. Για τον εντοπισμό ακριβών λειτουργιών σε βρόχους, το GASPER αναζητά δαπανηρές λειτουργίες που σχετίζονται με την αποθήκευση (όπως SLOAD και SSTORE) μέσα σε επαναλαμβανόμενες δομές [10].

Ένα επίσης εργαλείο που αναλύει τα έξυπνα συμβόλαια με τη χρήση στατικής ανάλυσης είναι το Oyente. Το Oyente είναι ένα εργαλείο συμβολικής εκτέλεσης που έχει σχεδιαστεί για την ανάλυση έξυπνων συμβολαίων στη πλατφόρμα Ethereum και τον εντοπισμό ευπαθειών ασφαλείας πριν από την ανάρτησή τους στο δίκτυο αλυσίδας μπλοκ. Εξετάζει το bytecode της Εικονικής Μηχανής Ethereum για να αποκαλύψει ελαττώματα όπως η εξάρτηση από τη διάταξη των συναλλαγών (Transaction-Ordering Dependence - TOD), η εξάρτηση από τη χρονοσφραγίδα μπλοκ, η κακή διαχείριση σφαλμάτων και οι ευπάθειες επανειλημμένης εισόδου. Το Oyente λειτουργεί με συμβολική εκτέλεση έξυπνων συμβολαίων, δηλαδή διερευνά όλες τις πιθανές διαδρομές εκτέλεσης ενός έξυπνου συμβολαίου αντί να προσομοιώνει μόνο μερικές περιπτώσεις. Το εργαλείο λειτουργεί απευθείας με το bytecode της Εικονικής Μηχανής Ethereum, καθιστώντας το ιδιαίτερα χρήσιμο για τον έλεγχο έξυπνων συμβολαίων που έχουν ήδη αναρτηθεί στο δίκτυο αλυσίδας μπλοκ του Ethereum. Το μοντέλο εκτέλεσης ακολουθεί τη δομή του Ethereum: τα συμβόλαια αποθηκεύονται ως bytecode στην αλυσίδα μπλοκ και οι συναλλαγές ενεργοποιούν την εκτέλεσή τους. Οι εξορύκτες επεξεργάζονται τις συναλλαγές και η σειρά τους μπορεί να επηρεάσει τα αποτελέσματα των έξυπνων συμβολαίων, οδηγώντας σε ευπάθειες που το Oyente στοχεύει να εντοπίσει [21]. Τα βασικά στοιχεία

για την διαδοχική ανάλυση ενός έξυπνου συμβολαίου από το Oyente είναι τα εξής:

- Κατασκευαστής Γραφήματος Ροής Ελέγχου - Κατασκευάζει ένα γράφημα ροής ελέγχου από το bytecode, απεικονίζοντας τα μονοπάτια εκτέλεσης.
- Διερευνητής - Πραγματοποιεί συμβολική εκτέλεση, εντοπίζοντας αλλαγές κατάστασης και πιθανά προβλήματα.
- Ανάλυση Πυρήνα - Ανιχνεύει συγκεκριμένες ευπάθειες όπως:
 - Εξάρτηση από τη διάταξη συναλλαγών (TOD): Εξασφαλίζει ότι τα αποτελέσματα των έξυπνων συμβολαίων δεν αλλάζουν με βάση τη σειρά των συναλλαγών.
 - Εξάρτηση από χρονοσφραγίδα: Ελέγχει εάν τα έξυπνα συμβόλαια βασίζονται σε χρονοσφραγίδες μπλοκ, οι οποίες μπορούν να χειραγωγηθούν από τους εξορύκτες.
 - Λάθος χειρισμός σφαλμάτων: Μαρκάρει τα έξυπνα συμβόλαια που αποτυγχάνουν να χειριστούν σωστά τα σφάλματα κλήσης, τα οποία μπορεί να οδηγήσουν σε απώλεια κρυπτονομισμάτων.
 - Επιθέσεις επανειλημμένης εισόδου: Ανιχνεύει αν μια εξωτερική κλήση έξυπνου συμβολαίου μπορεί να γίνει αντικείμενο εκμετάλλευσης πριν από την ενημέρωση της κατάστασης.
- Επικυρωτής: Φιλτράρει τα ψευδώς θετικά αποτελέσματα, εξασφαλίζοντας ακριβή αποτελέσματα.

Το MAIAN είναι ένα εργαλείο που έχει σχεδιαστεί για τον εντοπισμό ευπαθειών σε έξυπνα συμβόλαια της πλατφόρμας Ethereum, επίσης με την χρήση του bytecode τους. Επικεντρώνεται στον εντοπισμό μιας συγκεκριμένης κατηγορίας ευπαθειών που είναι γνωστές ως ευπάθειες ίχνους, οι οποίες είναι ιδιότητες που εκδηλώνονται κατά τη διάρκεια πολλαπλών κλήσεων ενός συμβολαίου. Αυτές οι ευπάθειες μπορούν να οδηγήσουν σε έξυπνα συμβόλαια που είτε κλειδώνουν κεφάλαια επ' αόριστον (άπληστα συμβόλαια), είτε διαρρέουν κεφάλαια σε αυθαίρετους χρήστες (σπάταλα συμβόλαια), είτε μπορούν να καταστραφούν από οποιονδήποτε χρήστη (αυτοκτονικά συμβόλαια). Το MAIAN λειτουργεί σε δύο κύριες φάσεις: συμβολική ανάλυση και συγκεκριμένη επικύρωση. Στη φάση της συμβολικής ανάλυσης, το MAIAN χρησιμοποιεί μια προσαρμοσμένη εικονική μηχανή Ethereum για τη συμβολική εκτέλεση του bytecode του συμβολαίου. Ξεκινά με μια συγκεκριμένη κατάσταση blockchain και αντιμετωπίζει ορισμένες εισόδους, όπως τα δεδομένα συναλλαγών και οι παράμετροι μπλοκ, ως

συμβολικές μεταβλητές. Το εργαλείο διερευνά διάφορα μονοπάτια εκτέλεσης εντός του έξυπνου συμβολαίου, χρησιμοποιώντας μια στρατηγική αναζήτησης σε βάθος για τον εντοπισμό ιχνών που παραβιάζουν τις καθορισμένες ιδιότητες. Κατά τη διάρκεια αυτής της εξερεύνησης, το MAIAN διατηρεί τόσο συμβολικές όσο και συγκεκριμένες μνήμες για την παρακολούθηση της κατάστασης του έξυπνου συμβολαίου. Όταν συναντά μια διακλάδωση στον κώδικα, χρησιμοποιεί έναν επιλυτή ικανοποιησιμότητας θεωριών modulo (Satisfiability Modulo Theories - SMT) για να καθορίσει την ικανοποίηση των συνθηκών διακλάδωσης και να διερευνήσει όλα τα εφικτά μονοπάτια. Εάν το MAIAN βρει ένα μονοπάτι που παραβιάζει μια ιδιότητα ίχνους, επισημαίνει το έξυπνο συμβόλαιο ως πιθανώς ευπαθή και παράγει συγκεκριμένες τιμές εισόδου που προκαλούν την παραβίαση. Η συγκεκριμένη φάση επικύρωσης ακολουθεί τη συμβολική ανάλυση. Σε αυτή τη φάση, το MAIAN δημιουργεί μια ιδιωτική διακλάδωση της αλυσίδας μπλοκ του Ethereum για να ελέγξει τα έξυπνα συμβόλαια που έχουν επισημανθεί με τις συγκεκριμένες τιμές εισόδου που δημιουργήθηκαν στην προηγούμενη φάση. Αυτό το βήμα διασφαλίζει ότι τα τρωτά σημεία που εντοπίστηκαν κατά τη συμβολική ανάλυση είναι πραγματικά και όχι ψευδώς θετικά. Για τα σπάταλα συμβόλαια, η επικύρωση ελέγχει αν το συμβόλαιο διαρρέει Ether σε μια αυθαίρετη διεύθυνση. Για αυτοκτονικά συμβόλαια, ελέγχεται αν το έξυπνο συμβόλαιο μπορεί να καταστραφεί από οποιονδήποτε χρήστη. Για τα άπληστα συμβόλαια, η επικύρωση επιβεβαιώνει ότι το συμβόλαιο δέχεται Ether αλλά δεν έχει τις απαραίτητες οδηγίες για την απελευθέρωσή του. Αυτή η προσέγγιση δύο φάσεων επιτρέπει στο MAIAN να εντοπίζει αποτελεσματικά και με ακρίβεια τα ευάλωτα έξυπνα συμβόλαια, με υψηλό ποσοστό πραγματικών θετικών αποτελεσμάτων [25].

Τέλος, υπάρχει ακόμη ένα εργαλείο που χρησιμοποιεί την Μέθοδο Επίσημης Επαλήθευσης (Formal Verification Method), η οποία χρησιμοποιεί επίσημες μεθόδους των μαθηματικών για την απόδειξη συγκεκριμένων χαρακτηριστικών σε έναν κώδικα. Το πλαίσιο F* (F* Framework) είναι μια λειτουργική γλώσσα προγραμματισμού που έχει σχεδιαστεί για την επίσημη επαλήθευση προγραμμάτων. Το πλαίσιο επιτρέπει στους προγραμματιστές να αναλύουν και να επαληθεύουν τόσο την ασφάλεια κατά το χρόνο εκτέλεσης όσο και τη λειτουργική ορθότητα των έξυπνων συμβολαίων μεταφράζοντάς τα σε προγράμματα F*. Αυτή η μετάφραση επιτρέπει τη χρήση του πλούσιου συστήματος τύπων της F*, το οποίο περιλαμβάνει εξαρτημένους τύπους και μοναδιαίες επιδράσεις, για τη δημιουργία αυτοματοποιημένων ερωτημάτων για έναν επιλυτή ικανοποιησιμότητας θεωριών modulo. Αυτά τα ερωτήματα μπορούν στη συνέχεια να επαληθεύουν στατικά διάφορες ιδιότητες των έξυπνων συμβολαίων, όπως

η διασφάλιση ότι δεν περιέχουν σφάλματα χρόνου εκτέλεσης ή ότι πληρούν συγκεκριμένα κριτήρια λειτουργικής ορθότητας. Το πλαίσιο F* λειτουργεί μέσω μιας διττής προσέγγισης. Πρώτον, παρέχει ένα εργαλείο που ονομάζεται Solidity*, το οποίο μεταγλωττίζει τα έξυπνα συμβόλαια που έχουν γραφτεί σε Solidity, σε F*. Αυτό επιτρέπει την επαλήθευση υψηλού επιπέδου της λειτουργικής ορθότητας και ασφάλειας σε επίπεδο πηγαίου κώδικα. Δεύτερον, προσφέρει το EVM*, έναν αποσυμπιεστή που μεταφράζει το bytecode της εικονικής μηχανής Ethereum σε πιο συνοπτικό κώδικα F*. Αυτή η διαδικασία αποσυμπίεσης κρύβει τις πολυπλοκότητες και επιτρέπει την ανάλυση ιδιοτήτων χαμηλού επιπέδου, όπως τα όρια της ποσότητας καυσίμου που απαιτείται για την εκτέλεση ενός έξυπνου συμβολαίου. Το σύστημα τύπων του F* είναι ιδιαίτερα ισχυρό, επειδή μπορεί να επιβάλλει διάφορες συνθήκες ασφαλείας και να ανιχνεύει ευάλωτα μοτίβα σε έξυπνες συμβολαία. Για παράδειγμα, μπορεί να διασφαλίσει ότι ένα έξυπνο συμβόλαιο εμφανίζει πάντα μια εξαίρεση (exception) όταν αποτυγχάνει μια λειτουργία αποστολής ή ότι οι ενημερώσεις κατάστασης δεν εκτελούνται άνευ όρων μετά από εξωτερικές κλήσεις, γεγονός που θα μπορούσε να οδηγήσει σε επιθέσεις επανεισόδου. Το πλαίσιο χρησιμοποιεί μια συνδυασμένη μονάδα εξαίρεσης και κατάστασης για να παρακολουθεί την κατάσταση του συμβολαίου και την επιτυχία ή την αποτυχία των λειτουργιών, επιτρέποντάς του να επιβάλλει αυτές τις συνθήκες ασφαλείας μέσω ελέγχου τύπου [5].

Κεφάλαιο 3

Θέματα ασφάλειας στο Web3

1 Παρασκήνιο του οικοσυστήματος

Το Web3 σηματοδοτεί μια σημαντική αλλαγή στον τρόπο κατασκευής και λειτουργίας του διαδικτύου, εστιάζοντας στην αποκέντρωση και την ιδιοκτησία των δεδομένων με την αξιοποίηση των υπάρχουσων τεχνολογιών. Στο επίκεντρο του Web3 βρίσκονται βασικά στοιχεία όπως τα δίκτυα blockchain που αποτελούνται από αποκεντρωμένους αλλά διασυνδεδεμένους κόμβους, βιβλιοθήκες Web3, γλώσσες προγραμματισμού όπως η Solidity, ψηφιακά πορτοφόλια για την αποθήκευση ταυτότητας και κρυπτονομισμάτων, έξυπνα συμβόλαια και εξειδικευμένοι πάροχοι υπηρεσιών. Αυτά τα θεμελιώδη στοιχεία διαδραματίζουν κρίσιμο ρόλο στην ενεργοποίηση ενός πλήρως λειτουργικού οικοσυστήματος Web3, εξασφαλίζοντας ένα πιο ανοιχτό, ασφαλές και καθοδηγούμενο από τους χρήστες διαδίκτυο [29].

1.1 Blockchain

Η τεχνολογία της αλυσίδας μπλοκ αντιπροσωπεύει μια πρωτοποριακή εξέλιξη πέρα από τα παραδοσιακά κατακεντρωμένα συστήματα βάσεων δεδομένων. Σε αντίθεση με τις συμβατικές βάσεις δεδομένων, οι οποίες συχνά ελέγχονται από μια κεντρική αρχή, η αλυσίδα μπλοκ λειτουργεί ως ένα αποκεντρωμένο και συνεχώς επεκτεινόμενο έγγραφο καταγραφής συναλλαγών (ledger). Αυτό το έγγραφο – βασικό συστατικό των τεχνολογιών κατακεντρωμένων βιβλίων (DLTs) – επιτρέπει σε πολλούς χρήστες να έχουν πρόσβαση, να επαληθεύουν και να διαχειρίζονται με ασφάλεια τις συναλλαγές [4]. Τα DLTs έχουν σχεδιαστεί για να διανέμουν τα δεδομένα σε ένα δίκτυο, διασφαλίζοντας ότι καμία μεμονωμένη οντότητα δεν έχει τον πλήρη έλεγχο, μειώνοντας έτσι τους κινδύνους που συνδέονται με τον συγκεντρωτισμό, όπως η

αλλοίωση των δεδομένων ή οι μη εξουσιοδοτημένες τροποποιήσεις.

Στον πυρήνα της, η αλυσίδα μπλοκ λειτουργεί ως ένα ψηφιακό έγγραφο που καταγράφει τις συναλλαγές σε ένα δίκτυο υπολογιστών, γνωστών ως κόμβοι. Κάθε συναλλαγή επαληθεύεται μέσω ενός μηχανισμού συναίνεσης πριν καταγραφεί μόνιμα στην αλυσίδα μπλοκ. Μόλις καταγραφούν, οι συναλλαγές καθίστανται αμετάβλητες, πράγμα που σημαίνει ότι δεν μπορούν να τροποποιηθούν ή να διαγραφούν. Το γεγονός ότι είναι αμετάβλητο εξασφαλίζει ισχυρή ακεραιότητα δεδομένων και εξαλείφει την ανάγκη για μια τρίτη αρχή, όπως μια τράπεζα ή ένας κυβερνητικός οργανισμός, να επιβλέπει ή να πιστοποιεί τις συναλλαγές. Ως αποτέλεσμα, η αλυσίδα μπλοκ προωθεί ένα σύστημα, όπου οι συναλλαγές επικυρώνονται από το ίδιο το δίκτυο και όχι από μια κεντρική οντότητα.

Ένα από τα καθοριστικά χαρακτηριστικά της τεχνολογίας της αλυσίδας μπλοκ είναι η διαφάνειά της. Κάθε κόμβος του δικτύου έχει πρόσβαση στο έγγραφο καταγραφής συναλλαγών, διασφαλίζοντας ότι τα στοιχεία των συναλλαγών μοιράζονται ανοιχτά και είναι επαληθεύσιμα. Αυτή η διαφάνεια όχι μόνο ενισχύει τη λογοδοσία, αλλά και μετριάξει σημαντικά τον κίνδυνο απάτης. Δεδομένου ότι όλες οι συναλλαγές καταγράφονται με αμετάβλητο τρόπο και είναι ορατές στους συμμετέχοντες, κάθε απόπειρα απάτης ή χειραγώγησης είναι εύκολα ανιχνεύσιμη.

Μια άλλη αξιοσημείωτη πτυχή της τεχνολογίας της αλυσίδας μπλοκ είναι η ικανότητά της να φιλοξενεί ανώνυμους κόμβους. Ενώ η διαφάνεια αποτελεί βασικό χαρακτηριστικό, η αλυσίδα μπλοκ υποστηρίζει επίσης την ιδιωτικότητα μέσω κρυπτογραφικών τεχνικών που επιτρέπουν στους συμμετέχοντες να πραγματοποιούν συναλλαγές χωρίς να αποκαλύπτουν την ταυτότητά τους. Αυτή η ανωνυμία είναι ιδιαίτερα πολύτιμη σε σενάρια όπου η εμπιστευτικότητα είναι κρίσιμη, όπως οι προσωπικές, οικονομικές συναλλαγές και οι ασφαλείς επικοινωνίες. Αξιοποιώντας κρυπτογραφικά μέτρα ασφαλείας, η αλυσίδα μπλοκ επιτρέπει ασφαλείς και ιδιωτικές αλληλεπιδράσεις, διατηρώντας παράλληλα την ακεραιότητα του συνολικού συστήματος.

Παρά αυτές της δυνατότητες, η τεχνολογία της αλυσίδας μπλοκ αντιμετωπίζει κάποιες προκλήσεις. Πρέπει να αντιμετωπιστούν διάφορα τεχνικά εμπόδια για να επιτευχθεί ευρεία υιοθέτηση και απρόσκοπτη ενσωμάτωση σε όλους τους κλάδους. Η επεκτασιμότητα είναι μία από τις πρωταρχικές ανησυχίες, καθώς τα δίκτυα αλυσίδας μπλοκ μπορεί να συμφορηθούν όταν διαχειρίζονται μεγάλο όγκο συναλλαγών, οδηγώντας σε βραδύτερους χρόνους επεξεργασίας και αυξημένο κόστος. Οι περιορισμοί επιδόσεων, όπως η καθυστέρηση και η απόδο-

ση, πρέπει επίσης να βελτιστοποιηθούν για να διασφαλιστεί ότι τα δίκτυα αλυσίδας μπλοκ παραμένουν μια βιώσιμη λύση για εφαρμογές μεγάλης κλίμακας.

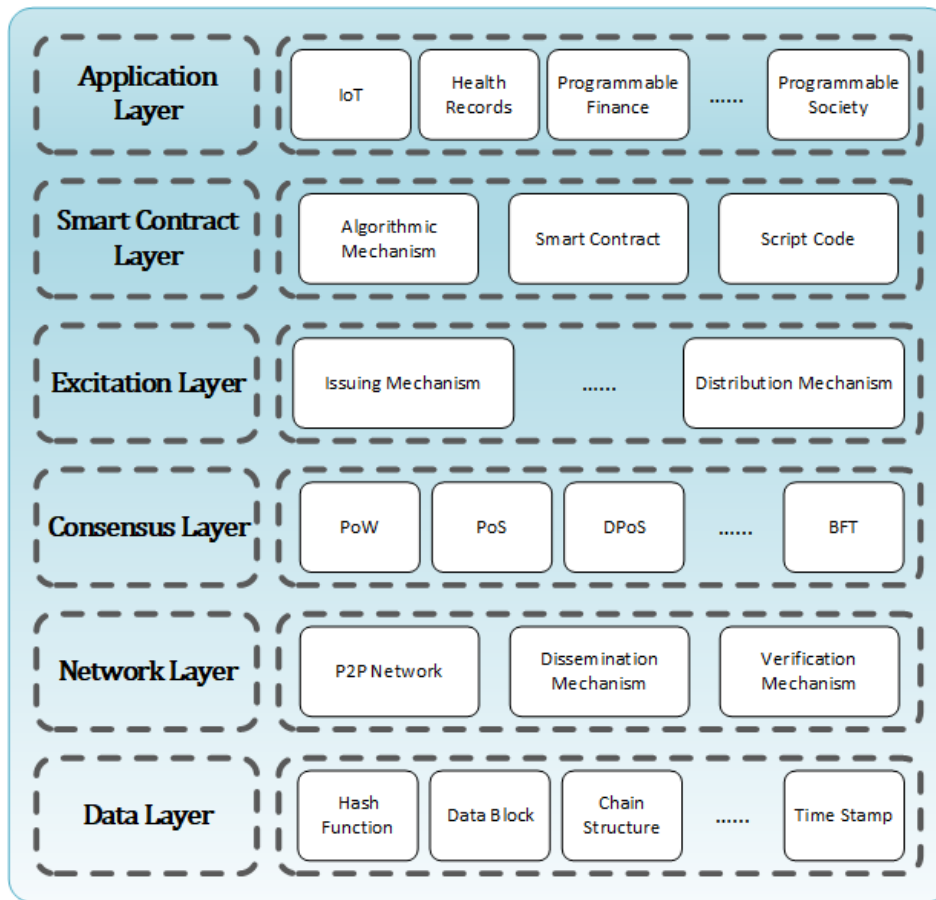
Η ασφάλεια είναι ένας άλλος κρίσιμος παράγοντας. Ενώ η ίδια η αλυσίδα μπλοκ είναι εξαιρετικά ασφαλής λόγω των κρυπτογραφικών της βάσεων, ευπάθειες μπορεί να προκύψουν στις σχετικές εφαρμογές, τα έξυπνα συμβόλαια (smart contracts) και τα πρωτόκολλα δικτύου. Η αντιμετώπιση αυτών των προβλημάτων ασφαλείας απαιτεί συνεχή καινοτομία στις μεθόδους κρυπτογράφησης, στους μηχανισμούς συναίνεσης και στις στρατηγικές πρόληψης κυβερνοεπιθέσεων.

Η διαλειτουργικότητα είναι μια άλλη πρόκληση, καθώς τα διάφορα δίκτυα αλυσίδας μπλοκ λειτουργούν συχνά απομονωμένα, γεγονός που καθιστά δύσκολη την αποτελεσματική επικοινωνία και ανταλλαγή δεδομένων. Οι προσπάθειες για τη δημιουργία λύσεων γεφύρωσης αλυσίδων (cross-chain) και τυποποιημένων πρωτοκόλλων αποσκοπούν στη γεφύρωση αυτού του χάσματος, επιτρέποντας την απρόσκοπτη αλληλεπίδραση μεταξύ των διαφόρων οικοσυστημάτων αλυσίδας μπλοκ.

Τέλος, η ευχρηστία παραμένει εμπόδιο για την ευρεία υιοθέτηση. Πολλές εφαρμογές αλυσίδας μπλοκ απαιτούν τεχνική εμπειρογνομosύνη και πρέπει να αναπτυχθούν φιλικές προς τον χρήστη διεπαφές, ώστε να καταστεί η τεχνολογία προσιτή σε ένα ευρύτερο κοινό.

Η τεχνολογία αλυσίδας μπλοκ λειτουργεί σε ένα αποκεντρωμένο και καταναμημένο πλαίσιο που έχει σχεδιαστεί για να παρέχει διαφάνεια, ασφάλεια και αντοχή στη μεταβλητότητα. Είναι δομημένη σε πολλαπλά επίπεδα, καθένα από τα οποία εξυπηρετεί μια ξεχωριστή λειτουργία, ενώ παράλληλα συνδέονται μεταξύ τους για να σχηματίσουν ένα ανθεκτικό σύστημα [34]. Η κατανόηση αυτών των επιπέδων είναι απαραίτητη για να αντιληφθούμε πώς λειτουργούν τα δίκτυα blockchain και τα βασικά στοιχεία που επιτρέπουν τη λειτουργία τους. Παρακάτω περιγράφονται τα θεμελιώδη επίπεδα της αρχιτεκτονικής της αλυσίδας μπλοκ ενώ απεικονίζονται και στο Σχήμα 3.1.

- **Επίπεδο δεδομένων (Data Layer):** Σε αυτό το επίπεδο δημιουργούνται μπλοκ με χρονοσφραγίδα. Η ασφάλεια διατηρείται με τη χρήση κρυπτογραφικών μεθόδων όπως συναρτήσεις κατακερματισμού και μια δομή αλυσίδας για την προστασία των δεδομένων.
- **Επίπεδο δικτύου (Network Layer):** Είναι υπεύθυνο για τη διανομή και την επικύρωση των δεδομένων στο δίκτυο, ενώ παράλληλα διασφαλίζει την ομαλή επικοινωνία μεταξύ των κόμβων.



Σχήμα 3.1: Τα βασικά επίπεδα της αρχιτεκτονικής της αλυσίδας μπλοκ.

- **Επίπεδο συναίνεσης (Consensus Layer):** Αυτό το επίπεδο είναι υπεύθυνο για την ομόφωνη συμφωνία μεταξύ των συμμετεχόντων στο δίκτυο μέσω διαφόρων αλγορίθμων συναίνεσης.
- **Επίπεδο κινήτρου (Excitation/Incentive Layer):** Είναι υπεύθυνο για την ανταμοιβή των κόμβων που συμμετέχουν στις λειτουργίες του δικτύου με βάση προκαθορισμένους μηχανισμούς κινήτρων.
- **Επίπεδο συμβολαίου (Contract Layer):** Λειτουργεί ως θεμέλιο για τις εφαρμογές του δικτύου, επιτρέποντας στα έξυπνα συμβόλαια να εκτελούν αυτόματα συναλλαγές όταν πληρούνται οι προϋποθέσεις.
- **Επίπεδο εφαρμογής (Application Layer):** Είναι το στρώμα που απευθύνεται στον χρήστη, όπου οι εφαρμογές αλληλεπιδρούν με το δίκτυο αλυσίδας μπλοκ για χρήση στον πραγματικό κόσμο.

2 Απειλές ασφαλείας στο Web3

Σε αυτή την ενότητα θα αναλυθούν κάποιες από τις κύριες απειλές ασφαλείας που αντιμετωπίζει η τεχνολογία αλυσίδας μπλοκ για κάθε επίπεδο που αναφέρθηκε παραπάνω.

2.1 Επίπεδο δεδομένων

Αυτό το επίπεδο αποτελείται από μπλοκ δεδομένων που συνδέονται μεταξύ τους με χρονολογική σειρά χρησιμοποιώντας κρυπτογραφικές συναρτήσεις κατακερματισμού. Αυτά τα μπλοκ είναι συνήθως οργανωμένα σε μια δομή Merkle Tree, η οποία επιτρέπει την αποτελεσματική και ασφαλή επαλήθευση δεδομένων. Τα σημαντικότερα δίκτυα αλυσίδας μπλοκ, συμπεριλαμβανομένου του Bitcoin, χρησιμοποιούν τον αλγόριθμο κατακερματισμού SHA-256 για την κρυπτογράφηση μπλοκ δεδομένων και τη δημιουργία μοναδικών υπογραφών. Ενώ ο SHA-256 παραμένει ασφαλής σήμερα, οι εξελίξεις στην τεχνολογία θα μπορούσαν τελικά να τον καταστήσουν ανεπαρκή. Η συνεχιζόμενη έρευνα και οι αναδυόμενες μέθοδοι επίθεσης δημιουργούν πιθανούς κινδύνους, ορισμένοι από τους οποίους βρίσκονται ακόμη υπό ανάπτυξη.

- *Επίθεση Κβαντικής Σύγκρουσης (Quantum Collision Attack)*: Μια επίθεση κβαντικής σύγκρουσης συμβαίνει όταν ένας κακόβουλος φορέας προσπαθεί να εντοπίσει μια διαφορετική είσοδο που παράγει την ίδια τιμή κατακερματισμού με την αρχική. Ο ερευνητής Mendel F. παρουσίασε έναν βελτιωμένο αλγόριθμο που απέδειξε με επιτυχία μια επίθεση σύγκρουσης 31 βημάτων στον SHA-256 [6]. Κοιτάζοντας μπροστά, η πρόοδος της κβαντικής πληροφορικής θα μπορούσε να αυξήσει σημαντικά τη δυνατότητα πραγματοποίησης τέτοιων επιθέσεων, καθιστώντας ενδεχομένως τον SHA-256 ανεπαρκή για τη διασφάλιση της κρυπτογραφικής ασφάλειας.
- *Επίθεση Επέκτασης Μήκους (Length Extension Attack)*: Μια επίθεση επέκτασης μήκους εκμεταλλεύεται τον τρόπο με τον οποίο ορισμένες συναρτήσεις κατακερματισμού επεξεργάζονται δεδομένα. Αυτές οι συναρτήσεις παράγουν μια έξοδο σταθερού μεγέθους που αντικατοπτρίζει την εσωτερική τους κατάσταση κατά την ολοκλήρωση. Σε αυτή την επίθεση, ένας κακόβουλος δράστης λαμβάνει την έξοδο κατακερματισμού (digest) ενός μηνύματος και, εκτιμώντας το μήκος του αρχικού μηνύματος, προσθέτει επιπλέον δεδομένα για να δημιουργήσει ένα νέο μήνυμα. Χωρίς να γνωρίζει το αρχικό μυστικό κλειδί,

ο επιτιθέμενος μπορεί να επεκτείνει τη διαδικασία κατακερματισμού και να δημιουργήσει έναν έγκυρο Κωδικό Ελέγχου Ταυτότητας Μηνύματος (Message Authentication Code - MAC) για το τροποποιημένο μήνυμά του, θέτοντας ουσιαστικά σε κίνδυνο την ακεραιότητα του συστήματος [12].

2.2 Επίπεδο δικτύου

Το επίπεδο δικτύου, που συχνά αναφέρεται ως επίπεδο διάδοσης (Propagation Layer), διαδραματίζει κρίσιμο ρόλο στο οικοσύστημα της αλυσίδας μπλοκ διασφαλίζοντας την αποκεντρωμένη και κατανεμημένη δομή του. Το επίπεδο αυτό είναι υπεύθυνο για τη διαχείριση των πρωτοκόλλων δικτύωσης, των μηχανισμών διάδοσης μηνυμάτων και των διαδικασιών ελέγχου ταυτότητας που χρησιμοποιούνται εντός της αλυσίδας μπλοκ. Βασικές λειτουργίες όπως η ανακάλυψη κόμβων, η διαχείριση συναλλαγών και η διάδοση των μπλοκ διαχειρίζεται επίσης από το επίπεδο δικτύου. Παρ' όλα αυτά, λόγω της θεμελιώδους φύσης του και του κεντρικού του ρόλου στη διευκόλυνση της ανταλλαγής δεδομένων, το στρώμα δικτύου είναι εκτεθειμένο σε ένα ευρύ φάσμα πιθανών απειλών και επιθέσεων ασφαλείας.

- *Επίθεση Sybil (Sybil Attack)*: Μια επίθεση Sybil στα συστήματα αλυσίδας μπλοκ μπορεί να έχει σοβαρές επιπτώσεις, επιτρέποντας ενδεχομένως διάφορες άλλες επιθέσεις, όπως Άρνηση Παροχής Υπηρεσιών (Denial of Service - DoS), Κατανεμημένη Άρνηση Παροχής Υπηρεσιών (Distributed Denial of Service - DDoS), επιθέσεις πλειοψηφίας και επιθέσεις σε δεξαμενές εξόρυξης (mining pools). Αυτός ο τύπος επίθεσης απειλεί την ακεραιότητα των αποκεντρωμένων μηχανισμών συναίνεσης, επιτρέποντας στον επιτιθέμενο να κυριαρχήσει δυνητικά σε ένα σημαντικό μέρος των κόμβων του δικτύου [14]. Στις αλυσίδες μπλοκ Proof-of-Work (PoW), αυτό είναι ιδιαίτερα επικίνδυνο, καθώς ο έλεγχος της πλειοψηφίας των κόμβων θα μπορούσε να οδηγήσει σε επίθεση 51%. Όταν οι νόμιμοι κόμβοι προσπαθούν να συνδεθούν στο δίκτυο, μπορεί να συναντήσουν μια χειραγωγημένη διακλάδωση που αποτελείται από ψεύτικα μπλοκ που συνδέονται με τον κόμβο του επιτιθέμενου. Ως αποτέλεσμα, ο επιτιθέμενος μπορεί να αναλάβει τον έλεγχο ολόκληρου του δικτύου, εμποδίζοντας τους γνήσιους εξορύκτες μπλοκ (blockchain miners) να επεξεργάζονται αποτελεσματικά τις συναλλαγές. Αυτό μπορεί να υποβαθμίσει σοβαρά τη συνολική απόδοση του συστήματος και την απόδοση των συναλλαγών.
- *Επίθεση Eclipse (Eclipse Attack)*: Αυτή η επίθεση είναι μια μορφή κυβερνοεπίθεσης που

αποσκοπεί στη διατάραξη του μηχανισμού συναίνεσης ενός δικτύου αλυσίδας μπλοκ. Σε αυτό το σενάριο, ένας κακόβουλος δράστης εξασφαλίζει στρατηγικά έναν μεγάλο αριθμό διευθύνσεων IP για να αποκτήσει τον έλεγχο της διαδικασίας συναίνεσης του δικτύου. Ο επιτιθέμενος απομονώνει έναν συγκεκριμένο κόμβο από το υπόλοιπο δίκτυο διακόπτοντας την επικοινωνία του με άλλους κόμβους. Αυτό επιτυγχάνεται με μεθόδους όπως ο κατακλυσμός του κόμβου με υπερβολική κίνηση ή η χρήση παραποίησης διευθύνσεων δικτύου. Μόλις απομονωθεί ο κόμβος-στόχος, ο επιτιθέμενος μπορεί να τον τροφοδοτήσει με ψευδείς ή παραπλανητικές πληροφορίες σχετικά με την κατάσταση της αλυσίδας μπλοκ. Αυτή η παραπλάνηση μπορεί να χρησιμοποιηθεί για να χειραγωγήσει τη δύναμη ψήφου του κόμβου ή να τον εξαπατήσει ώστε να αποδεχθεί δόλιες συναλλαγές [19]. Η επιτυχία μιας τέτοιας επίθεσης εξαρτάται από την ικανότητα του επιτιθέμενου να εκμεταλλευτεί τη δομή του δικτύου και να θέσει σε κίνδυνο την αξιοπιστία των κόμβων που συνδέονται με το θύμα.

- *Επίθεση άρνησης παροχής υπηρεσιών εξάντλησης καυσίμου (Gas Exhaustion Denial of Service (DoS) Attack)* Αυτός ο τύπος επίθεσης παρατηρείται συνήθως σε έξυπνα συμβόλαια που βασίζονται στη γλώσσα προγραμματισμού Solidity και εκτελούνται στην εικονική μηχανή του Ethereum. Σε αυτά τα συμβόλαια, κάθε λειτουργία χρεώνει ένα τέλος καυσίμου για την εκτέλεσή της. Παρόλο που μπορούν να διεκπεραιωθούν πολλαπλές πράξεις μέσα σε ένα μπλοκ, το συνολικό καύσιμο που καταναλώνεται από όλες τις συναλλαγές σε αυτό το μπλοκ περιορίζεται από ένα προκαθορισμένο όριο. Εάν το όριο αυτό ξεπεραστεί, όλες οι εκκρεμείς συναλλαγές αποτυγχάνουν. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτόν τον περιορισμό με την ταυτόχρονη υποβολή πολυάριθμων συναλλαγών, καθεμία από τις οποίες έχει οριστεί στη μέγιστη τιμή καυσίμου. Αυτή η προσέγγιση έχει σχεδιαστεί για να εξαντλήσει το όριο καυσίμου των μπλοκ του Ethereum, εξαντλώντας τους διαθέσιμους πόρους καυσίμων και καθιστώντας το συμβόλαιο μη λειτουργικό. Ως αποτέλεσμα, οι νόμιμοι χρήστες δεν έχουν πρόσβαση στην υπηρεσία [15].

2.3 Επίπεδο συναίνεσης

Για να εξασφαλιστεί ότι όλοι οι κόμβοι του δικτύου συμφωνούν σχετικά με την κατάσταση του κατανεμημένου εγγράφου καταγραφής συναλλαγών, είναι απαραίτητος ένας μηχανισμός

συναίνεσης [3]. Ωστόσο, αυτοί οι μηχανισμοί συναίνεσης μπορεί να είναι ευάλωτοι σε ευπάθειες και μπορούν να αντιμετωπίσουν διάφορες προκλήσεις ασφαλείας. Παρακάτω περιγράφονται ορισμένοι από τους συνήθεις αλγόριθμους συναίνεσης και τους πιθανούς κινδύνους ασφαλείας που συνδέονται με αυτούς.

Proof-of-Work (PoW)

Αυτός ο μηχανισμός συναίνεσης συγκαταλέγεται μεταξύ των πρώτων αλγορίθμων συναίνεσης και χρησιμοποιείται από δίκτυα αλυσίδας μπλοκ όπως το Bitcoin. Σε αυτό το πρωτόκολλο, ένα μπλοκ δημιουργείται με τον υπολογισμό ενός κατακερματισμού, ο οποίος απαιτεί τον προσδιορισμό μιας συγκεκριμένης τιμής (nonce). Η πρόκληση της εύρεσης αυτής της τιμής εξαρτάται από τις συγκεκριμένες συνθήκες που πρέπει να ικανοποιεί ο κατακερματισμός (hash). Μόλις υπολογιστεί το σωστό hash, η δημιουργία του μπλοκ ανακοινώνεται σε όλους τους κόμβους του δικτύου. Συνήθως, οι κόμβοι δίνουν προτεραιότητα στη μεγαλύτερη αλυσίδα για να συνεχίσουν τη δημιουργία νέων μπλοκ [36]. Η επίλυση αυτού του υπολογιστικού γρίφου απαιτεί σημαντική επεξεργαστική ισχύ, ιδίως καθώς το επίπεδο δυσκολίας αυξάνεται με την πάροδο του χρόνου.

Η ασφάλεια αυτού του μηχανισμού συναίνεσης βασίζεται σημαντικά στην προϋπόθεση ότι καμία οντότητα δεν ελέγχει περισσότερο από το 50% της συνολικής υπολογιστικής ισχύος του δικτύου. Εάν μια οντότητα αποκτήσει τον έλεγχο του 51% ή περισσότερο αυτής της υπολογιστικής ισχύος, μπορεί να κυριαρχήσει στο δίκτυο διατηρώντας τη μεγαλύτερη αλυσίδα. Αυτό δημιουργεί μια κρίσιμη ευπάθεια, που επιτρέπει στην οντότητα να πραγματοποιεί επιβλαβείς επιθέσεις στο δίκτυο. Παρακάτω παρατίθενται ορισμένα παραδείγματα γνωστών επιθέσεων που μπορούν να εκτελεστούν υπό αυτές τις συνθήκες.

- *Επίθεση Εγωιστικής Εξόρυξης (Selfish Mining Attack)*: Σε αυτό το είδος επίθεσης, ένας ανέντιμος εξορύχος που επιλύει επιτυχώς το παζλ κατακερματισμού και δημιουργεί ένα νέο μπλοκ μπορεί να επιλέξει να μην το μοιραστεί με το δίκτυο, οδηγώντας στη δημιουργία μιας διακλάδωσης στην αλυσίδα των μπλοκ. Ο κακόβουλος εξορύχος μπορεί στη συνέχεια να συνεχίσει την εξόρυξη επόμενων μπλοκ κρυφά για να δημιουργήσει μια μεγαλύτερη ιδιωτική αλυσίδα. Όταν το δίκτυο υιοθετήσει τελικά τη μακρύτερη αλυσίδα – η οποία, στην προκειμένη περίπτωση, είναι αυτή που δημιούργησε ο εγωιστής εξορύχος – ο επιτιθέμενος εξασφαλίζει τις ανταμοιβές των μπλοκ. Ενώ οι έντιμοι εξορύκτες μένουν με μια μικρότερη, άκυρη αλυσίδα, σπαταλώνοντας ουσιαστικά τις προσπάθειες και

τους πόρους τους [7].

- *Επίθεση Διπλών Δαπανών (Double-Spending Attack)*: Όταν ένας κακόβουλος φορέας διαθέτει σημαντική υπολογιστική (κατακερματιστική) ισχύ, μπορεί να εκμεταλλευτεί το σύστημα αλυσίδας μπλοκ δαπανώντας τις ίδιες μονάδες κρυπτονομισμάτων σε πολλαπλές συναλλαγές. Με αυτόν τον τρόπο, μπορούν να δημιουργήσουν μια εναλλακτική αλυσίδα μπλοκ που γίνεται μεγαλύτερη από τη νόμιμη αλυσίδα. Αυτή η μεγαλύτερη, απατηλή αλυσίδα μπορεί να αντικαταστήσει την αρχική αλυσίδα, επιτρέποντας στον επιτιθέμενο να ακυρώσει προηγούμενες συναλλαγές και να ξοδέψει ουσιαστικά τα ίδια κεφάλαια περισσότερες από μία φορές [32].

Proof-of-Stake (PoS)

Ενώ ο μηχανισμός Proof-of-Work (PoW) βασίζεται στην υπολογιστική ισχύ, έχει ως αποτέλεσμα σημαντική κατανάλωση ενέργειας. Ο μηχανισμός Proof-of-Stake (PoS) αντιμετωπίζει αυτό το πρόβλημα υιοθετώντας μια διαφορετική μεθοδολογία. Στον PoS, οι συμμετέχοντες στην αλυσίδα μπλοκ είναι γνωστοί ως «επικυρωτές». Οι επικυρωτές μπορούν να κλειδώσουν, ή να «ποντάρουν», ένα μέρος από τις μάρκες τους (token) για να αποκτήσουν την ευκαιρία να επικυρώνουν νέες συναλλαγές. Εάν ένας επικυρωτής εγκρίνει μια δόλια συναλλαγή, όχι μόνο χάνει την ανταμοιβή για τη σωστή επικύρωση αλλά και τις μάρκες που είχε ποντάρει. Ενώ αυτό το σύστημα αποθαρρύνει τους κακόβουλους φορείς από το να επιτίθενται στο δίκτυο λόγω του κινδύνου οικονομικής απώλειας, υπάρχουν και σε αυτό ορισμένες ευπάθειες.

- *Επίθεση Nothing-at-Stake (Nothing-at-Stake Attack)*: Αυτό το είδος επίθεσης συμβαίνει όταν οι επικυρωτές, κατά τη διάρκεια μιας διαδικασίας συναίνεσης, δεν έχουν οικονομικό κίνητρο για να δεσμευτούν σε έναν μόνο κλάδο μιας διακλάδωσης αλυσίδας μπλοκ. Ως αποτέλεσμα, οι επικυρωτές μπορούν να επιλέξουν να εξορύξουν σε πολλαπλούς κλάδους ταυτόχρονα, δημιουργώντας αντικρουόμενα μπλοκ χωρίς να αντιμετωπίσουν σημαντικές οικονομικές κυρώσεις. Αυτή η συμπεριφορά μπορεί να υπονομεύσει τη σταθερότητα του δικτύου και να εισάγει σημαντικά τρωτά σημεία ασφαλείας [17].
- *Επίθεση Συσσώρευσης Ηλικίας Νομισμάτων (Coin Age Accumulation Attack)*: Στην πρώτη έκδοση του πρωτοκόλλου, η επιρροή του πονταρίσματος ενός χρήστη αυξανόταν όσο περισσότερο παρέμενε ανέγγιχτο, χωρίς να υπάρχουν χρονικοί περιορισμοί. Αυτή η

έλλειψη περιορισμών επέτρεπε σε έναν επιτιθέμενο να συσσωρεύσει σταδιακά ένα σημαντικό μερίδιο με την πάροδο του χρόνου, το οποίο θα μπορούσε τελικά να του δώσει τον έλεγχο του δικτύου. Ο μηχανισμός ηλικίας νομισμάτων λειτουργούσε ως πλασιστής, ενισχύοντας τη βαρύτητα των συμμετοχών των επικυρωτών στο σύστημα [13].

- *Επίθεση Μεγάλου Βεληνεκούς (Long-Range Attack)*: Αυτό το είδος επίθεσης στοχεύει στον έλεγχο ενός δικτύου αλυσίδας μπλοκ. Εάν ένας επιτιθέμενος κατέχει ένα σημαντικό ποσό πονταρισμένων μαρκών, μπορεί να ξεκινήσει από το αρχικό μπλοκ της αλυσίδας (Genesis block). Πείθοντας τους κόμβους του δικτύου να υποστηρίξουν έναν νέο κλάδο αλυσίδας που ευθυγραμμίζεται με τα συμφέροντα του επιτιθέμενου, δημιουργώντας μια εναλλακτική αλυσίδα που αντικατοπτρίζει τη νόμιμη. Αυτός ο χειραγωγημένος κλάδος, αν και πανομοιότυπος ως προς τη δομή, επιτρέπει στον επιτιθέμενο να διαταράξει δυνητικά ή να καταλάβει το δίκτυο [2].

2.4 Επίπεδο κινήτρου

Το επίπεδο κινήτρου στην αλυσίδα μπλοκ είναι ένα ζωτικό στοιχείο που κινεί τη δραστηριότητα του δικτύου και υποστηρίζει τους μηχανισμούς συναίνεσης. Είναι απαραίτητο για τη διατήρηση της ασφάλειας και της ακεραιότητας της αλυσίδας μπλοκ, παρακινώντας τους συμμετέχοντες με ανταμοιβές, ενθαρρύνοντας μια δυναμική κοινότητα επικυρωτών και ενισχύοντας την ανθεκτικότητα των αποκεντρωμένων συστημάτων. Παρά τη σημασία του, υπάρχουν σημαντικές απειλές, όπως περιγράφονται παρακάτω, που θα μπορούσαν να διαταράξουν την κανονική λειτουργία του.

- *Επίθεση Εναλλαγής Ομάδων Εξόρυξης (Pool Hopping Attack)*: Αυτή η επίθεση αναφέρεται σε μια στρατηγική όπου οι εξορύκτες εναλλάσσονται συχνά μεταξύ των ομάδων εξόρυξης για να μεγιστοποιήσουν τα κέρδη τους με βάση την τρέχουσα κερδοφορία της κάθε ομάδας. Ενώ αυτή η πρακτική ωφελεί μεμονωμένους εξορύκτες, έχει ευρύτερες αρνητικές συνέπειες για τη σταθερότητα και την ασφάλεια του δικτύου αλυσίδας μπλοκ. Ενθαρρύνοντας τη συγκέντρωση της δύναμης εξόρυξης σε συγκεκριμένες ομάδες, η εναλλαγή των ομάδων εξόρυξης αυξάνει την ευπάθεια του δικτύου σε επιθέσεις, ιδίως σε εκείνες που στοχεύουν σε μηχανισμούς συναίνεσης όπως το Proof-of-Work (PoW). Αυτή η συγκέντρωση της δύναμης εξόρυξης διευκολύνει τους κακόβουλους φορείς να

αποκτήσουν τον έλεγχο ενός σημαντικού μέρους του ρυθμού κατακερματισμού του δικτύου. Ως αποτέλεσμα, το δίκτυο γίνεται πιο εκτεθειμένο σε απειλές όπως οι επιθέσεις 51% ή οι επιθέσεις εγωιστικής εξόρυξης, υπονομεύοντας τη συνολική ακεραιότητά του.

- *Επίθεση Άρνησης Υπηρεσίας Αλυσίδας Μπλοκ (Blockchain Denial of Service - BDoS Attack)*: Πρόκειται για μια επίθεση που βασίζεται σε κίνητρα, όπου ένας κακόβουλος δράστης χειραγωγεί το σύστημα ανταμοιβής της αλυσίδας μπλοκ για να διαταράξει τις λειτουργίες. Ο επιτιθέμενος επενδύει πόρους για τη δημιουργία ενός μπλοκ, αλλά αποκάλυπτε μόνο την απόδειξη εξόρυξης, αποκρύπτοντας σκόπιμα τη δημοσίευση του πλήρους μπλοκ. Οι έντιμοι εξορύκτες ερμηνεύουν αυτή τη μερική αποκάλυψη ως στρατηγική κίνηση του επιτιθέμενου, μειώνοντας το κίνητρό τους να συνεχίσουν την εξόρυξη. Ως αποτέλεσμα, οι εξορύκτες μπορεί να αποσυρθούν από τη διαδικασία εξόρυξης, οδηγώντας ενδεχομένως το δίκτυο αλυσίδας μπλοκ σε παύση. Τέτοιες επιθέσεις με κίνητρα μπορούν επίσης να επιβάλουν μια συγκεκριμένη σειρά συναλλαγών ή να προκαλέσουν τον αποκλεισμό ορισμένων συναλλαγών από την αλυσίδα μπλοκ [24].

2.5 Επίπεδο συμβολαίου

Ένα έξυπνο συμβόλαιο είναι ένα αυτο εκτελούμενο πρόγραμμα σχεδιασμένο να εκτελεί αυτόματα μια συναλλαγή μόλις ικανοποιηθούν συγκεκριμένες προκαθορισμένες συνθήκες. Επιβάλλει τους όρους μιας συμφωνίας χωρίς να απαιτείται ανθρώπινη παρέμβαση ή επίβλεψη. Αυτό μπορεί να περιλαμβάνει ενέργειες όπως η μεταφορά κεφαλαίων, η παροχή υπηρεσιών ή άλλες συμφωνημένες εργασίες. Τα έξυπνα συμβόλαια αναπτύσσονται σε ένα δίκτυο αλυσίδας μπλοκ και μπορούν να ενσωματωθούν σε διάφορα συστήματα πληρωμών, συμπεριλαμβανομένων κρυπτονομισμάτων όπως το Bitcoin.

Η κύρια λειτουργία τους είναι η αυτοματοποίηση προκαθορισμένων ενεργειών, διαδικασιών ή συναλλαγών που ενεργοποιούνται από συγκεκριμένα κριτήρια. Ωστόσο, όπως κάθε λογισμικό, τα έξυπνα συμβόλαια μπορεί να έχουν σφάλματα στην λογική του κώδικα ή ευπάθειες. Εάν αξιοποιηθούν από κακόβουλους φορείς, αυτές οι αδυναμίες θα μπορούσαν να οδηγήσουν σε οικονομικές απώλειες για τους χρήστες ή παραβιάσεις της ιδιωτικότητας των δεδομένων. Οι πιο συνηθισμένες ευπάθειες που σχετίζονται με τα έξυπνα συμβόλαια περιγράφονται παρακάτω.

- *Επίθεση με Κλήση Επικίνδυνου Εντολοδόχου Έξυπνου Συμβολαίου (Dangerous Delegate*

Call Attack): Στη γλώσσα προγραμματισμού Solidity, που χρησιμοποιείται για την ανάπτυξη έξυπνων συμβολαίων, περιλαμβάνει μια χαμηλού επιπέδου συνάρτηση που ονομάζεται «delegatecall» και επιτρέπει την αλληλεπίδραση μεταξύ συμβολαίων. Όταν χρησιμοποιείται η delegatecall, η εκτέλεση πραγματοποιείται στο πλαίσιο του έξυπνου συμβολαίου που καλεί. Για παράδειγμα, εάν το έξυπνο συμβόλαιο "A" χρησιμοποιεί την delegatecall για να καλέσει μια συνάρτηση στο έξυπνο συμβόλαιο "B", η κατάσταση του έξυπνου συμβολαίου "A" μεταβάλλεται με βάση τη λογική του έξυπνου συμβολαίου "B". Αυτός ο μηχανισμός ενέχει σημαντικό κίνδυνο: εάν το έξυπνο συμβόλαιο "B" είναι κακόβουλο, θα μπορούσε να χειραγωγήσει την κατάσταση του συμβολαίου "A" με επιβλαβείς τρόπους ή ακόμη και να επιτρέψει σε έναν εισβολέα να αποκτήσει τον έλεγχο του συμβολαίου "A". Αυτή η ευπάθεια αναδεικνύει τους κινδύνους από τη χρήση της delegatecall χωρίς τις κατάλληλες διασφαλίσεις. Αυτό φαίνεται στο παράδειγμα του Κώδικα 3.1.

```
1 contract Delegate {
2     address public owner;
3
4     constructor(address _owner) public {
5         owner = _owner;
6     }
7
8     function pwn() public {
9         owner = msg.sender;
10    }
11 }
12
13 contract Delegation {
14     address public owner;
15     Delegate delegate;
16
17     constructor(address _delegateAddress) public {
18         delegate = Delegate(_delegateAddress);
19         owner = msg.sender;
20     }
21
22     fallback() external {
23         (bool result,) = address(delegate).delegatecall(msg.data);
24         if (result) {
25             this;
26         }
27     }
28 }
```

Κώδικας 3.1: Παράδειγμα επίθεσης delegatecall

Στο παραπάνω παράδειγμα:

1. Ο επιτιθέμενος δημιουργεί ένα έξυπνο συμβόλαιο που καλεί το Delegation και περνάει τον επιλογέα της συνάρτησης `own()` στα `calldata`. Δεδομένου ότι καμία συνάρτηση στην Delegation δεν ταιριάζει με την `own()`, πιάνει το σφάλμα χρησιμοποιώντας τη συνάρτηση `fallback` και προωθεί την κλήση στην Delegate. Η `own()` υπάρχει στην Delegate, οπότε η κλήση – η οποία λέει στην Delegate να ενημερώσει τον ιδιοκτήτη στην `msg.sender` – μπορεί να εκτελεστεί.
 2. Η Delegate εκτελεί την κλήση χρησιμοποιώντας τις αρχικές τιμές των `msg.sender` και `msg.data` και ενημερώνει τη μεταβλητή `owner` στην Delegation στην τιμή του `msg.sender` (δηλαδή τη διεύθυνση συμβολαίου του επιτιθέμενου). Ο επιτιθέμενος αποκτά τον έλεγχο του Delegation και προχωρά στην ενεργοποίηση κακόβουλων λειτουργιών, όπως η αποστράγγιση των κεφαλαίων που είναι αποθηκευμένα στο έξυπνο συμβόλαιο.
- *Παγωμένο Ether (Ether Frozen)*: Αυτή η ευπάθεια εμφανίζεται σε έξυπνα συμβόλαια που έχουν σχεδιαστεί για να λαμβάνουν μάρκες Ether, αλλά δεν διαθέτουν μηχανισμό για να τα ανακτήσουν οι χρήστες. Εάν το έξυπνο συμβόλαιο περιλαμβάνει μια εφεδρική λειτουργία που αποτρέπει τις αναλήψεις, τα Ether που αποστέλλεται στο έξυπνο συμβόλαιο παγιδεύονται μόνιμα, χωρίς οι χρήστες να μπορούν να τα ανακτήσουν. Αυτό έχει ως αποτέλεσμα τα κεφάλαια να κλειδώνονται επ' αόριστον εντός του έξυπνου συμβολαίου.
 - *Υπερχείλιση/Υπορροή Ακεραίαου (Integer Over/Underflow)*: Αυτή η ευπάθεια προκύπτει όταν μια τιμή υπερβαίνει το μέγιστο όριο (υπερχείλιση) ή πέφτει κάτω από το ελάχιστο όριο (υπορροή) που μπορεί να διαχειριστεί ένας καταχωρητής αποθήκευσης. Για παράδειγμα, εάν ένας αριθμός είναι πολύ μεγάλος για να χωρέσει στο καθορισμένο εύρος, υπερχειλίζει, ενώ εάν είναι πολύ μικρός (συμπεριλαμβανομένων των αρνητικών αριθμών), υπορρέει. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτή την αδυναμία για να χειραγωγήσουν έξυπνα συμβόλαια, αποσπώντας δυνητικά σημαντικές ποσότητες μαρκών. Ένα αξιοσημείωτο παράδειγμα είναι η παραβίαση του έξυπνου συμβολαίου

BeautyChain, όπου ένας επιτιθέμενος εκμεταλλεύτηκε μια υπερχείλιση ακέραιου αριθμού για να παρακάμψει τα μέτρα ασφαλείας και να κλέψει μια σημαντική ποσότητα μαρκών BEC [26].

- *Μη ελεγμένη Εξωτερική Κλήση (Unchecked External Call)*: Αυτή η ευπάθεια προκύπτει όταν η τιμή επιστροφής μιας κλήσης εξωτερικού μηνύματος δεν ελέγχεται. Σε τέτοια σε-νάρια, ακόμη και αν το καλούμενο έξυπνο συμβόλαιο αντιμετωπίσει σφάλμα, το έξυπνο συμβόλαιο που έκανε την κλήση συνεχίζει να εκτελείται χωρίς διακοπή. Είτε η αποτυχία συμβαίνει τυχαία είτε προκαλείται σκόπιμα από έναν εισβολέα, η μη ελεγχόμενη κλήση μπορεί να οδηγήσει σε απροσδόκητα και δυνητικά επιβλαβή αποτελέσματα. Η Solidity παρέχει αρκετές συναρτήσεις κλήσης χαμηλού επιπέδου, όπως οι `call`, `callcode`, `send` και `delegatecall`, οι οποίες λειτουργούν σε ακατέργαστες διευθύνσεις. Αξίζει να σημειωθεί ότι αυτές οι μέθοδοι δεν εμφανίζουν αυτομάτως εξαιρέσεις όταν προκύπτουν σφάλματα – αντίθετα, επιστρέφουν `false` αν η κλήση αποτύχει, αφήνοντας στον προγραμματιστή να χειριστεί κατάλληλα το σφάλμα. Η αποτυχία ελέγχου αυτών των τιμών επιστροφής μπορεί να οδηγήσει σε εσφαλμένη λογική του προγράμματος και σε κινδύνους ασφάλειας.
- *Ευπάθεια Εξάρτησης Χρονοσφραγίδας (Timestamp Dependency Vulnerability)*: Αυτό το ζήτημα προκύπτει όταν ένα έξυπνο συμβόλαιο εξαρτάται από τη συνάρτηση `block.timestamp` για κρίσιμες λειτουργίες, όπως η ενεργοποίηση συναλλαγών ή η δημιουργία τυχαίων αριθμών για συγκεκριμένες διεργασίες. Η τιμή της χρονοσφραγίδας καθορίζεται από τον κόμβο που δημιουργεί το μπλοκ που περιέχει τη συναλλαγή που εκτελεί το έξυπνο συμβόλαιο. Δεδομένου ότι οι χρονοσφραγίδες μπλοκ δεν είναι αυστηρά σταθερές και μπορούν να ποικίλλουν εντός ενός συγκεκριμένου εύρους, είναι επιρρεπείς σε χειραγώγηση. Κακόβουλοι φορείς, ιδίως οι εξορύκτες, μπορούν να το εκμεταλλευτούν αυτό προσαρμόζοντας τις χρονοσφραγίδες μπλοκ όταν ένα έξυπνο συμβόλαιο βασίζεται στο `block.timestamp` για τις συναλλαγές στο δίκτυο Ethereum. Χειραγωγώντας αυτές τις χρονοσφραγίδες, μπορούν να δημιουργήσουν συνθήκες που ευνοούν τα δικά τους συμφέροντα, θέτοντας ενδεχομένως σε κίνδυνο την ακεραιότητα του έξυπνου συμβολαίου.
- *Επίθεση Επανεισόδου (Reentrancy Attack)*: Πρόκειται για ένα θέμα ασφαλείας στα έξυπνα συμβόλαια που επιτρέπει την εκτέλεση εξωτερικού, μη αξιόπιστου κώδικα. Η ευπάθεια προκύπτει όταν ένα έξυπνο συμβόλαιο αλληλεπιδρά με ένα εξωτερικό έξυπνο

συμβόλαιο, το οποίο στη συνέχεια καλεί με τη σειρά του το αρχικό έξυπνο συμβόλαιο. Αυτή η αλληλεπίδραση μπορεί να δημιουργήσει έναν ατελείωτο βρόχο. Ένας εισβολέας εκμεταλλεύεται αυτήν την αδυναμία ενεργοποιώντας επανειλημμένα μια λειτουργία εντός του έξυπνου συμβολαίου, οδηγώντας σε έναν κύκλο συνεχών κλήσεων. Αυτός ο ατελείωτος βρόχος μπορεί ενδεχομένως να επιτρέψει στον εισβολέα να αποστραγγίσει χρήματα από το έξυπνο συμβόλαιο, θέτοντας σημαντικό κίνδυνο οικονομικής απώλειας.

2.6 Επίπεδο εφαρμογής

Το επίπεδο εφαρμογής, τοποθετημένο στην κορυφή της αρχιτεκτονικής της αλυσίδας μπλοκ, λειτουργεί ως η κρίσιμη διεπαφή που γεφυρώνει τους τελικούς χρήστες με το βασικό λογισμικό, επιτρέποντας την αλληλεπίδραση σε όλο το δίκτυο αλυσίδας μπλοκ. Αυτό το επίπεδο περιλαμβάνει στοιχεία όπως τις διεπαφές χρήστη (UI), τις διεπαφές προγραμματισμού εφαρμογών (API) και τις αποκεντρωμένες εφαρμογές, για τα οποία υπάρχουν διάφορα είδη επιθέσεων. Παραβιάσεις στην ασφάλεια των πλατφορμών συναλλαγών και των λογαριασμών χρηστών απειλούν σημαντικά την ασφάλεια των περιουσιακών στοιχείων που είναι αποθηκευμένα σε ψηφιακά πορτοφόλια κρυπτονομισμάτων. Παρακάτω, περιγράφονται ορισμένοι από τους βασικούς κινδύνους που συνδέονται με αυτά τα τρωτά σημεία.

- *Επίθεση Ψευδής Συμπλήρωσης (False Top-Up Attack)*: Στα συστήματα αλυσίδας μπλοκ, το αποτέλεσμα μιας συναλλαγής υποδεικνύεται συχνά από ένα πεδίο κατάστασης, το οποίο λειτουργεί ως μεταβλητή διακριτού τύπου (Boolean). Αυτό το πεδίο ορίζεται σε «Αληθής» (True) ή «Ψευδής» (False) ανάλογα με το αν υπάρχει κάποιο σφάλμα κατά τη διάρκεια της συναλλαγής. Διαφορετικές πλατφόρμες, όπως ανταλλακτήρια και ψηφιακά πορτοφόλια κρυπτονομισμάτων, χειρίζονται τις αποτυχίες συναλλαγών με διάφορους τρόπους. Ωστόσο, εάν υπάρχουν ελαττώματα στον τρόπο με τον οποίο επαληθεύεται μια επιτυχημένη μεταφορά κρυπτονομισμάτων, μπορεί να γίνει εκμετάλλευση ενός κενού ασφαλείας που ονομάζεται ψευδής συμπλήρωση. Αυτή η επίθεση μπορεί δυνητικά να αποστραγγίσει όλα τα χρήματα από μία αλυσίδα μπλοκ. Για παράδειγμα, στο δίκτυο αλυσίδας μπλοκ Ethereum, εάν το υπόλοιπο του αποστολέα είναι ανεπαρκές για τη συναλλαγή, το σύστημα επιστρέφει μια "ψευδή" τιμή αντί να εμφανίσει κάποιο σφάλμα, δημιουργώντας έτσι, μια ευκαιρία για εκμετάλλευση [15].
- *Επίθεση σε Εξάρτηση Σειράς Συναλλαγών (Transaction Order Dependency Attack)*: Αυ-

τή η επίθεση εκμεταλλεύεται μια ευπάθεια αγωνιστικής κατάστασης (race condition) σε έξυπνα συμβόλαια. Ένα έξυπνο συμβόλαιο δίνει κίνητρο στους εξορύκτες να λύσουν ένα υπολογιστικό πρόβλημα πριν ολοκληρωθεί η συναλλαγή στο blockchain με αντάλλαγμα ένα τέλος καυσίμου (gas fee). Μόλις υποβληθεί η λύση, η συναλλαγή τοποθετείται σε μία ομάδα αναμονής (mempool), περιμένοντας να προστεθεί στο επόμενο μπλοκ. Κατά τη διάρκεια αυτής της περιόδου αναμονής, ένας κακόβουλος παράγοντας που παρακολουθεί την ομάδα αναμονής μπορεί να υποκλέψει τις λεπτομέρειες της συναλλαγής, συμπεριλαμβανομένης της λύσης. Ο εισβολέας μπορεί στη συνέχεια να υποβάλει εκ νέου τη συναλλαγή με τα ίδια δεδομένα αλλά με υψηλότερη τιμή καυσίμου. Δεδομένου ότι οι συναλλαγές με υψηλότερες χρεώσεις καυσίμου έχουν συνήθως προτεραιότητα, η συναλλαγή του εισβολέα είναι πιο πιθανό να υποβληθεί σε επεξεργασία πρώτα, επιτρέποντάς του να διεκδικήσει την ανταμοιβή. Αυτή η χειραγώγηση μπορεί να οδηγήσει σε διάφορα ζητήματα και διαταραχές στα έξυπνα συμβόλαια [15].

- *Επίθεση Επανάληψης (Replay Attack)*: Ένας νόμιμος χρήστης ξεκινά μια συναλλαγή στο δίκτυο blockchain, παρέχοντας όλες τις απαραίτητες λεπτομέρειες, όπως τη διεύθυνση του αποστολέα, τη διεύθυνση του παραλήπτη και το ποσό του κρυπτονομίσματος που πρόκειται να μεταφερθεί, χρησιμοποιώντας τη συνάρτηση transferProxy όπως απεικονίζεται στο Κώδικα 3.2. Στη συνέχεια, ένας κακόβουλος φορέας θα μπορούσε να στείλει ξανά τα ίδια ακριβώς δεδομένα συναλλαγής στο δίκτυο για επικύρωση. Χωρίς διασφαλίσεις όπως ένα μοναδικό αναγνωριστικό συναλλαγής ή μία χρονοσφραγίδα, οι επικυρωτές δεν έχουν αξιόπιστο τρόπο να εντοπίσουν εάν η συναλλαγή έχει ήδη υποβληθεί σε επεξεργασία. Αυτό επιτρέπει στον εισβολέα να αντιγράψει τη συναλλαγή, προκαλώντας συνέπειες, όπως διπλές δαπάνες ή μη εξουσιοδοτημένες μεταφορές [15].

```
1 function transferProxy(address _from, address _to, uint256 _value, uint256 _fee) {
2     require(balances[_from] >= _fee + _value);
3     require(balances[_to] + _value >= balances[_to]);
4     require(balances[msg.sender] + _fee >= balances[msg.sender]);
5     balances[_to] += _value;
6     balances[msg.sender] += _fee;
7     balances[_from] -= _value + _fee;
8 }
```

Κώδικας 3.2: Συνάρτηση transferProxy του Ethereum

Κεφάλαιο 4

Σχεδιασμός συστήματος

Στην παρούσα ενότητα γίνεται μια συνοπτική περιγραφή του συστήματος, των οντοτήτων, των συστατικών και των διαφόρων διεργασιών που λαμβάνουν χώρα.

1 Επισκόπηση

Η παρούσα εργασία αφορά την ανάπτυξη ενός συστήματος με το όνομα «Παρατηρητήριο» (Watchtower) που θα επιτρέπει την ασφαλή αλληλεπίδραση των ανθρώπων με αποκεντρωμένες εφαρμογές οι οποίες βασίζονται στην τεχνολογία των έξυπνων συμβολαίων και γενικότερα την τεχνολογία της αλυσίδας των μπλοκ. Οι διαδικασίες που έχουν αναπτυχθεί στο πλαίσιο του συστήματος αυτού έχουν ως στόχο την μείωση των απατών που μπορούν να υπάρχουν σε ένα αποκεντρωμένο σύστημα οι οποίες αφορούν κυρίως χρηματικές απώλειες εις βάρος των χρηστών. Ο κύριος σκοπός του συστήματος αυτού βασίζεται στην ιδέα ότι τα ψηφιακά πορτοφόλια κρυπτονομισμάτων (crypto-wallets) θα πρέπει να αποτρέπουν τις πιθανών κακόβουλες συναλλαγές που μπορεί να εκτελέσει κάποιος χρήστης ή να παρέχουν τη δυνατότητα επιλογής στο χρήστη αν θέλει να εκτελέσει την συναλλαγή παρέχοντας του απαραίτητες πληροφορίες για το επίπεδο ασφαλείας της εκάστοτε συναλλαγής.

2 Οντότητες

Το Παρατηρητήριο έχει σχεδιαστεί προκειμένου να εξυπηρετεί πολλαπλές οντότητες με ξεχωριστούς σκοπούς. Οι κύριες οντότητες/ρόλοι του συστήματος είναι οι εξής:

- **Παρατηρητήριο – Watchtower:** Είναι η βασική υπηρεσία που παρέχει πληροφορίες σχετικά με την ασφάλεια των αποκεντρωμένων εφαρμογών. Το Παρατηρητήριο είναι

υπεύθυνο για τον έλεγχο και την εύρεση ευπαθειών σε έξυπνα συμβόλαια καθώς επίσης και στις ιστοσελίδες που φιλοξενούν αυτές τις αποκεντρωμένες εφαρμογές που επικοινωνούν με αυτά τα έξυπνα συμβόλαια. Αυτή η υπηρεσία, μπορεί να αλληλεπιδράσει με τον χρήστη και να του παρέχει πληροφορίες σχετικά με την εγκυρότητα των πιστοποιητικών των αποκεντρωμένων εφαρμογών. Επικοινωνεί με το ψηφιακό πορτοφόλι κρυπτονομισμάτων του χρήστη προκειμένου να εξυπηρετήσει τα αιτήματά του. Επιπρόσθετα, επικοινωνεί με τα δίκτυα αλυσίδων μπλοκ προκειμένου να ελέγξει έξυπνα συμβόλαια που υπάρχουν ήδη στο εκάστοτε δίκτυο. Τέλος μπορεί επίσης να αλληλεπιδράσει με τον υπεύθυνο-διαχειριστή της αποκεντρωμένης εφαρμογής προκειμένου να δημιουργήσει πιστοποιητικά σε περίπτωση που η αποκεντρωμένη εφαρμογή θεωρηθεί ασφαλής.

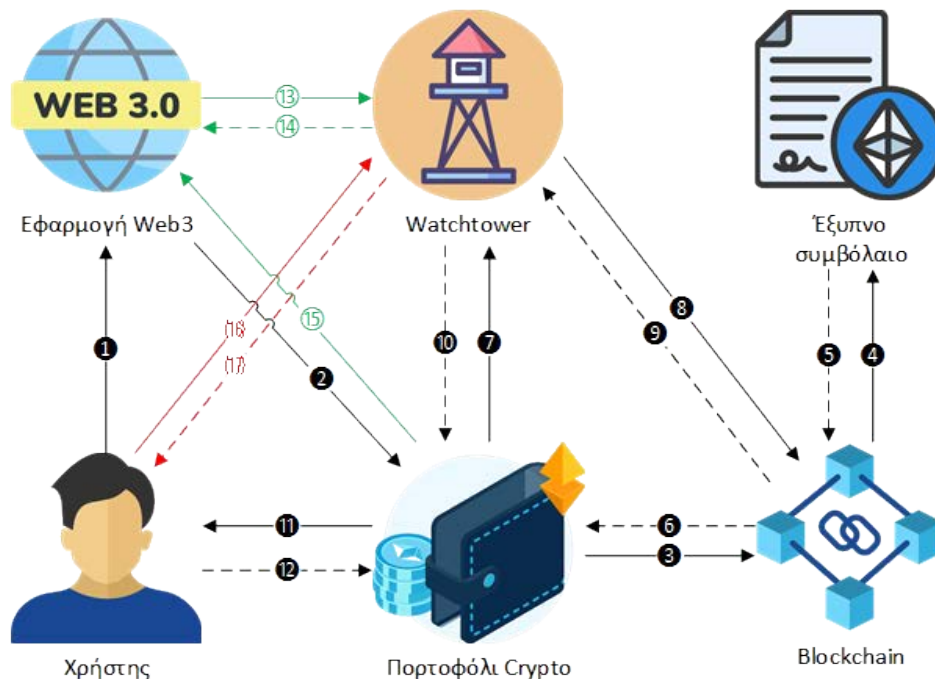
- **Χρήστης:** Ο χρήστης είναι αυτός που μπορεί να ξεκινήσει τις διαδικασίες στο σύστημα. Είναι αυτός που αλληλεπιδρά με την αποκεντρωμένη εφαρμογή σε μία ιστοσελίδα και εκτελεί χρηματικές συναλλαγές με το εκάστοτε κρυπτονόμισμα. Ο χρήστης μπορεί κατά κύριο λόγο να αλληλεπιδράσει άμεσα με την αποκεντρωμένη εφαρμογή όπως επίσης και με το ψηφιακό του πορτοφόλι κρυπτονομισμάτων προκειμένου να εκτελέσει χρηματικές συναλλαγές που αφορούν την αποκεντρωμένη εφαρμογή. Υπάρχει και μία ακόμη αλληλεπίδραση που μπορεί να έχει – με το Παρατηρητήριο – η οποία είναι κατόπιν αιτήματος και εκτελείται αυτοβούλως χειροκίνητα από τον χρήστη. Ο χρήστης μπορεί να καλέσει το Παρατηρητήριο ούτως ώστε να ελέγξει αν το πιστοποιητικό της αποκεντρωμένης εφαρμογής είναι έγκυρο ή όχι.
- **Αποκεντρωμένη εφαρμογή:** Είναι αυτή που αλληλεπιδρά με τον χρήστη και πάνω σε αυτή εκτελούνται συναλλαγές. Επίσης, επικοινωνεί με τον ψηφιακό πορτοφόλι του χρήστη σε περίπτωση που ο χρήστης θέλει να εκτελέσει κάποια χρηματική συναλλαγή.
- **Δίκτυο αλυσίδας μπλοκ:** Είναι το αποκεντρωμένο δίκτυο με το οποίο μπορεί να συνδεθεί το ψηφιακό πορτοφόλι του χρήστη προκειμένου να εκτελέσει την χρηματική συναλλαγή μεταξύ του χρήστη και του έξυπνου συμβολαίου.
- **Ψηφιακό πορτοφόλι κρυπτονομισμάτων:** Είναι το ψηφιακό πορτοφόλι του χρήστη που συνδέεται με τα δίκτυα αλυσίδων μπλοκ και έχει πρόσβαση στο ποσό των κρυπτονομισμάτων που ανήκουν στον χρήστη. Είναι υπεύθυνο να εκτελεί τις χρηματικές συναλλαγές, καθώς επίσης να επικοινωνεί με το Παρατηρητήριο προκειμένου να επιβε-

βαιώνει ότι οι συναλλαγές που θα εκτελεστούν, πρόκειται να λαμβάνουν χώρα σε ένα ασφαλές περιβάλλον.

- **Έξυπνο συμβόλαιο – Smart Contract:** Είναι ο κώδικας που εκτελείται και διαχειρίζεται τα κρυπτονομίσματα από τις συναλλαγές που γίνονται κατά την αλληλεπίδραση μεταξύ του χρήστη και της αποκεντρωμένης εφαρμογής. Το έξυπνο συμβόλαιο θα πρέπει να υπάρχει στο δίκτυο αλυσίδας μπλοκ προκειμένου να μπορεί να κληθεί.

3 Αλληλεπιδράσεις στο σύστημα

Τα κύρια βήματα των αλληλεπιδράσεων μεταξύ των οντοτήτων που αναφέρθηκαν προηγουμένως, απεικονίζονται στο Σχήμα 4.1. Η πιο απλή ροή που μπορεί να υπάρξει μέσα στο σύστημα είναι:



Σχήμα 4.1: Αλληλεπίδραση μέσα στο σύστημα

- (1) Ο χρήστης αλληλεπιδρά με την αποκεντρωμένη εφαρμογή που φιλοξενείται σε μια ιστοσελίδα στο διαδίκτυο, και ξεκινάει μία χρηματική συναλλαγή. Παραδείγματος χάρι, η αποκεντρωμένη εφαρμογή μπορεί να είναι ένα ηλεκτρονικό παιχνίδι με ψηφιακούς χαρακτήρες, όπου ο χρήστης θα θέλει να αγοράσει κάποια ψηφιακά αντικείμενα για τον χαρακτήρα του.

- (2) Η αποκεντρωμένη εφαρμογή επικοινωνεί με το ψηφιακό πορτοφόλι του χρήστη προκειμένου να εκτελέσει την συναλλαγή. Σε αυτό το σημείο η εφαρμογή δίνει κάποιες πληροφορίες που χρειάζονται για την εκτέλεση της συναλλαγής όπως το κόστος της αγοράς, η διεύθυνση του έξυπνου συμβολαίου η οποία είναι σε κατακερματισμένη μορφή και μοναδική σε όλο το δίκτυο αλυσίδας μπλοκ. Υπάρχουν και κάποιες ακόμη πληροφορίες που αντλούνται από το ψηφιακό πορτοφόλι κατά την είσοδο του χρήστη στην αποκεντρωμένη εφαρμογή όπως είναι το μοναδικό αναγνωριστικό του δικτύου αλυσίδας μπλοκ στο οποίο συναλλάσσεται η εκάστοτε αποκεντρωμένη εφαρμογή, το όνομα του δικτύου, τον σύνδεσμο που χρησιμοποιείται για κλήσεις απομακρυσμένων διαδικασιών (Remote Procedure Call - RPC) κ.α.
- (3) – (6) Το ψηφιακό πορτοφόλι επικοινωνεί με το δίκτυο αλυσίδας μπλοκ προκειμένου να αλληλεπιδράσει με το έξυπνο συμβόλαιο.
- (7) Το ψηφιακό πορτοφόλι στέλνει ένα αίτημα στο Παρατηρητήριο προκειμένου να ελέγξει αν η συναλλαγή που πρόκειται να γίνει, θα εκτελεστεί σε ένα ασφαλές περιβάλλον. Το αίτημα αυτό θα περιλαμβάνει (α) το όνομα τομέα (domain name) της ιστοσελίδας που φιλοξενεί την αποκεντρωμένη εφαρμογή, (β) τη διεύθυνση του έξυπνου συμβολαίου σε κατακερματισμένη μορφή δεκαεξαδικού τύπου και (γ) το αναγνωριστικό του δικτύου αλυσίδας μπλοκ στο οποίο υπάρχει το έξυπνο συμβόλαιο.
- (8) – (9) Το Παρατηρητήριο θα ελέγξει στη βάση δεδομένων του αν έχει γίνει ήδη ο έλεγχος για το συγκεκριμένο έξυπνο συμβόλαιο. Αν δεν έχει γίνει, τότε θα πρέπει να επικοινωνήσει με το δίκτυο αλυσίδας μπλοκ και να αντλήσει το έξυπνο συμβόλαιο προκειμένου να το ελέγξει για ευπάθειες. Επιπροσθέτως θα ελεγχθεί αν η ιστοσελίδα που φιλοξενεί την αποκεντρωμένη εφαρμογή, έχει ευπάθειες ή είναι κακόβουλη.
- (10) Όταν το Παρατηρητήριο εκτελέσει τα παραπάνω βήματα, θα επιστρέψει ένα ποσοστό εμπιστοσύνης σχετικά με το πόσο ανασφαλές είναι το περιβάλλον στο οποίο συναλλάσσεται ο χρήστης.
- (11) Σε τελικό βήμα της διαδικασίας αυτής, το ψηφιακό πορτοφόλι θα ενημερώσει τον χρήστη για το πόσο ασφαλής είναι το περιβάλλον στο οποίο θα εκτελεστεί η συναλλαγή ή θα αποτρέψει τελείως τον χρήστη όταν πρόκειται για μία σίγουρα κακόβουλη/ευπαθή αποκεντρωμένη εφαρμογή.

- (12) Σε περίπτωση που το ψηφιακό πορτοφόλι ενημερώσει τον χρήστη, τότε αυτός είναι υπεύθυνος για το αν θα εκτελέσει την συναλλαγή ή όχι.

Το Παρατηρητήριο υποστηρίζει επίσης και την έκδοση πιστοποιητικών για τις αποκεντρωμένες εφαρμογές, προσθέτοντας μία ακόμη διαδικασία στο σύστημα. Η διαδικασία αυτή είναι η ακόλουθη:

- (13) Ο υπεύθυνος/προγραμματιστής της αποκεντρωμένης εφαρμογής επικοινωνεί απευθείας με το Παρατηρητήριο, στέλνοντας ένα αίτημα που περιέχει (α) την διεύθυνση του έξυπνου συμβολαίου σε κατακερματισμένη μορφή δεκαεξαδικού τύπου, (β) το μοναδικό αναγνωριστικό του δικτύου αλυσίδας μπλοκ, (γ) τον σύνδεσμο που χρησιμοποιείται για κλήσεις απομακρυσμένων διαδικασιών και (δ) η διεύθυνση ηλεκτρονικού ταχυδρομείου.

- (14) Λόγω του ότι η αναζήτηση ευπαθειών από το Παρατηρητήριο ενδέχεται να χρειάζεται αρκετό χρόνο, η απάντηση στο αίτημα του υπεύθυνου της αποκεντρωμένης εφαρμογής θα γίνει μέσω ηλεκτρονικού ταχυδρομείου που αναφέρθηκε στο βήμα (13). Σε αυτή την διεύθυνση θα σταλούν τα ευρήματα ή το πιστοποιητικό, σε περίπτωση που η αποκεντρωμένη εφαρμογή θεωρηθεί μη ασφαλής ή κριθεί ότι είναι ασφαλής αντίστοιχα. Σε περίπτωση που σταλθεί το πιστοποιητικό, τότε ο υπεύθυνος/προγραμματιστής μπορεί να το εγκαταστήσει στην ιστοσελίδα του και να είναι ορατό προς όλους.

- (15) Με αυτό τον τρόπο το ψηφιακό πορτοφόλι, μπορεί να ελέγξει απευθείας στην ιστοσελίδα που φιλοξενεί την αποκεντρωμένη εφαρμογή, το πιστοποιητικό και να επαληθεύσει αν έχει εκδοθεί από το Παρατηρητήριο και δεν έχει περάσει η ημερομηνία λήξης του.

Σε περίπτωση που υπάρχει το πιστοποιητικό στην ιστοσελίδα που φιλοξενεί την αποκεντρωμένη εφαρμογή, ο χρήστης μπορεί να εκκινήσει μία χειροκίνητη διαδικασία εντός του συστήματος:

- (16) Ο χρήστης μπορεί να στείλει σε αίτημα το πιστοποιητικό της ιστοσελίδας απευθείας στο Παρατηρητήριο προκειμένου να ελέγξει αν το πιστοποιητικό έχει εκδοθεί από το Παρατηρητήριο και είναι έγκυρο.

- (17) Λόγω του ότι το έγγραφο είναι υπογεγραμμένο ψηφιακά, το Παρατηρητήριο θα ελέγξει την υπογραφή, αν το πιστοποιητικό είναι έγκυρο και αν είναι ακόμη σε ισχύ.

Κεφάλαιο 5

Υλοποίηση συστήματος

Σε αυτό το κεφάλαιο θα γίνει καλύτερη κατανόηση της υλοποίησης και θα περιγραφούν λεπτομερώς τα τεχνικά χαρακτηριστικά του συστήματος καθώς και τα εργαλεία που χρησιμοποιήθηκαν για την δημιουργία του συστήματος. Πιο συγκεκριμένα θα αναλυθούν σε υποενότητες τα παρακάτω:

- Τεχνική ανάλυση των εργαλείων και τεχνολογιών που χρησιμοποιήθηκαν καθώς και της εσωτερικής υποδομής.
- Τεχνική περιγραφή της δημιουργίας πιστοποιητικού.
- Τεχνική περιγραφή της διαδικασίας υπολογισμού βαθμού επικινδυνότητας.
- Περιγραφή της διαδικασίας επαλήθευσης πιστοποιητικού.

1 Εργαλεία και τεχνολογίες

1.1 Ενορχήστρωση

Όσον αφορά την εσωτερική υποδομή, έγινε χρήση του εργαλείου Docker [35] σε συνδυασμό με το πρόσθετο Docker Compose. Το Docker είναι μια πλατφόρμα που έχει σχεδιαστεί για να απλοποιεί την ανάπτυξη και τη διαχείριση εφαρμογών με τη χρήση της τεχνολογίας ονόματι "Δοχειοποίηση" (Containerization). Παρέχει ένα συνεπές περιβάλλον για την εκτέλεση λογισμικού σε διαφορετικά συστήματα με την ενθυλάκωση εφαρμογών και των εξαρτήσεών τους σε ελαφριές, φορητές μονάδες που ονομάζονται δοχεία (Containers). Τα δοχεία αυτά είναι ουσιαστικά απομονωμένα περιβάλλοντα που περιλαμβάνουν όλα όσα απαιτούνται

Κάποια από τα βασικά χαρακτηριστικά του Docker:

- Σε συνδυασμό με το Docker, το Docker Compose προσθέτει τα ακόλουθα χαρακτηριστικά:

- 39

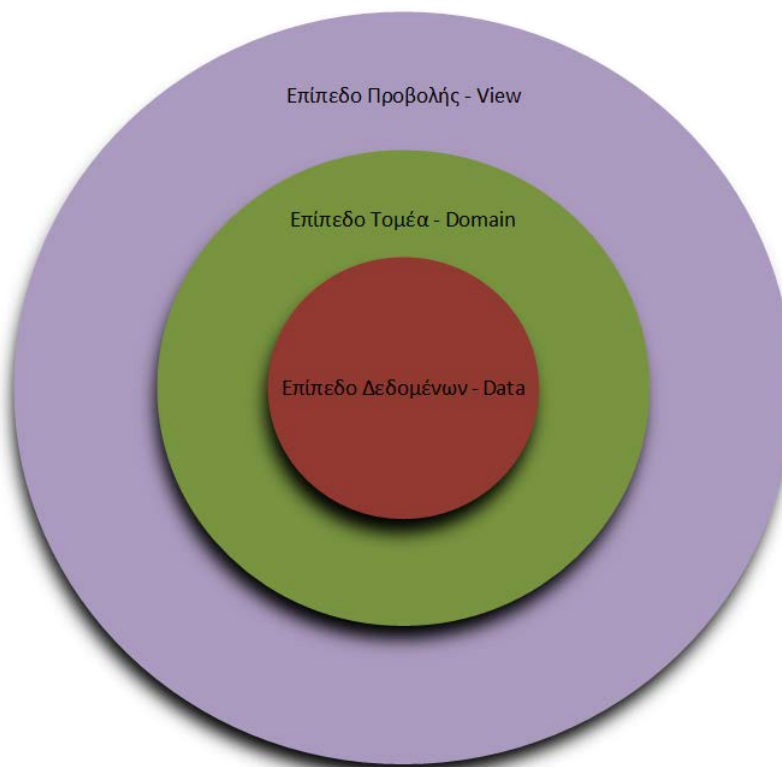
- Την εικόνα (image) του δοχείου που θα χρησιμοποιηθεί.
 - Τους κανόνες δικτύωσης.
 - Τις μεταβλητές περιβάλλοντος.
 - Τους τόμους για τη μόνιμη αποθήκευση δεδομένων.
- **Ενορχήστρωση:** Το Docker Compose εκκινεί και διαχειρίζεται τα δοχεία ως ενιαία εφαρμογή, διασφαλίζοντας ότι οι υπηρεσίες εκκινούνται με τη σωστή σειρά και είναι σωστά δικτυωμένες μεταξύ τους.
 - **Κλιμάκωση:** Το Docker Compose επιτρέπει την κλιμάκωση μεμονωμένων υπηρεσιών προς τα πάνω ή προς τα κάτω (π.χ. εκτέλεση πολλαπλών οντοτήτων ενός διακομιστή ιστού για εξισορρόπηση φορτίου) με απλές εντολές.
 - **Δικτύωση:** Δημιουργείται αυτόματα ένα αποκλειστικό δίκτυο για τα δοχεία, επιτρέποντας την απρόσκοπτη επικοινωνία μεταξύ τους χωρίς επιπλέον ρυθμίσεις.
 - **Επαναχρησιμοποιήσιμες διαμορφώσεις:** Ένα ενιαίο δηλωτικό αρχείο τύπου YAML μπορεί να επαναχρησιμοποιηθεί και να προσαρμοστεί για διαφορετικά έργα ή περιβάλλοντα με ελάχιστες αλλαγές.

1.2 Παρατηρητήριο - Watchtower

Η βασική υπηρεσία του προτεινόμενου συστήματος είναι το Παρατηρητήριο (Watchtower). Είναι η υπηρεσία που είναι υπεύθυνη για τον έλεγχο ευπαθειών σε ιστοσελίδες που φιλοξενούν αποκεντρωμένες εφαρμογές καθώς επίσης και των ελέγχων των έξυπνων συμβολαίων που εκτελούνται στο παρασκήνιο στο δίκτυο αλυσίδας μπλοκ, κατά την διαδικασία των συναλλαγών στις εκάστοτε αποκεντρωμένες εφαρμογές. Το Παρατηρητήριο έχει υλοποιηθεί με την υψηλού-επιπέδου γλώσσα προγραμματισμού Python έκδοση: 3.12. Ουσιαστικά, το Παρατηρητήριο είναι μία υπηρεσία που υλοποιεί μία Διεπαφή Προγραμματισμού Εφαρμογής (Application Programming Interface - API) που συμμορφώνεται με τις αρχές σχεδιασμού του αρχιτεκτονικού μοντέλου Μεταφοράς Κατάστασης Αναπαράστασης (Representational State Transfer - ReST) κάνοντας χρήση του πλαισίου ονόματι FastAPI [16]. Το δοχείο που είναι υπεύθυνο για αυτή την υπηρεσία, εκτελεί μια Ασύγχρονη Διεπαφή Πύλης Διακομιστή (Asynchronous Server Gateway Interface - ASGI) δικτύου που την υλοποιεί το εργαλείο Unicorn [33].

Το Παρατηρητήριο έχει υλοποιηθεί με πολύ συγκεκριμένη αρχιτεκτονική προκειμένου να είναι ευέλικτος και ανεξάρτητος από εξωτερικά εργαλεία και βιβλιοθήκες. Πιο συγκεκριμένα έχει ακολουθηθεί η «Καθαρή Αρχιτεκτονική» (Clean Architecture) [22] που προτάθηκε από τον Robert C. Martin. Η Καθαρή Αρχιτεκτονική είναι μια φιλοσοφία σχεδιασμού λογισμικού που δίνει έμφαση στη δημιουργία συστημάτων τα οποία είναι εύρωστα, συντηρήσιμα, επεκτάσιμα, ελέγξιμα και ανεξάρτητα από εξωτερικές βιβλιοθήκες και τεχνολογίες. Η βασική ιδέα είναι να δομηθεί η βάση του κώδικα με τρόπο που να επιτρέπει στην επιχειρησιακή λογική να μην έχει εξαρτήσεις. Αυτό διασφαλίζει ότι οι αλλαγές σε ένα μέρος του συστήματος έχουν ελάχιστες επιπτώσεις σε άλλα μέρη.

Η Καθαρή Αρχιτεκτονική το επιτυγχάνει αυτό με την οργάνωση του κώδικα σε επίπεδα, όπου κάθε επίπεδο έχει συγκεκριμένη ευθύνη και σαφή όρια. Επιβάλλει έναν κανόνα εξάρτησης σύμφωνα με τον οποίο η κατεύθυνση της εξάρτησης πρέπει πάντα να δείχνει προς τα μέσα. Οι ενότητες υψηλότερου επιπέδου (βασική επιχειρησιακή λογική) δεν θα πρέπει να εξαρτώνται από ενότητες χαμηλότερου επιπέδου (εργαλεία, βάσεις δεδομένων).



Σχήμα 5.1: Καθαρή Αρχιτεκτονική - Clean Architecture

Όπως φαίνεται και στο Σχήμα 5.1, Το πρώτο επίπεδο που συναντάμε είναι το **επίπεδο προβολής (View)**. Σε αυτό το επίπεδο υπάρχουν οι Ελεγκτές (Controllers) που είναι υπεύθυνοι

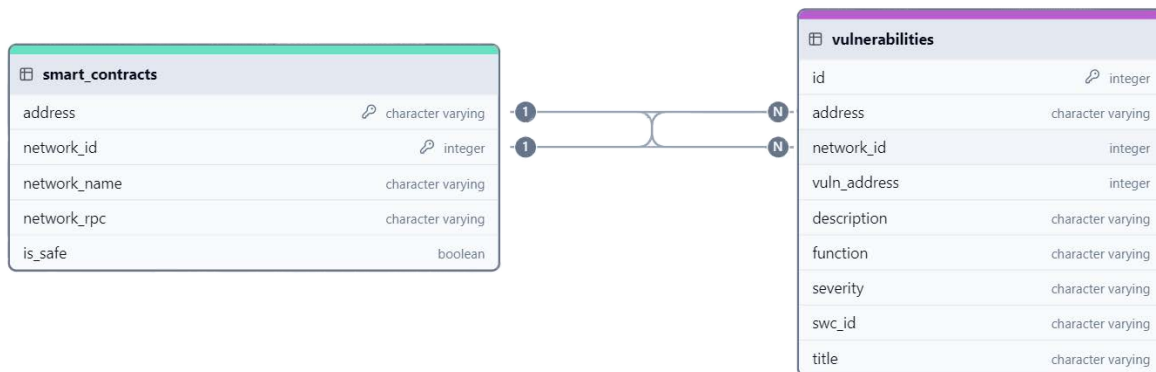
για την διαχείριση των αιτημάτων των χρηστών και την αποστολή των αντίστοιχων απαντήσεων. Σε αυτό το επίπεδο γίνονται έλεγχοι εγκυρότητας των δεδομένων που λαμβάνονται από το κάθε αίτημα πριν αυτά περάσουν στο επόμενο επίπεδο στο οποίο και βασίζονται. Το επόμενο επίπεδο είναι το **επίπεδο τομέα (Domain)**. Σε αυτό το επίπεδο υπάρχει η λογική που απαιτείται για την εκτέλεση συγκεκριμένων διαδικασιών. Αυτή η λογική υλοποιείται σε Περιπτώσεις Χρήσης (Use Cases) οι οποίες εννοχρηστρώνουν τον τρόπο με τον οποίο οι οντότητες αλληλεπιδρούν μεταξύ τους. Το επόμενο και τελευταίο επίπεδο είναι το **επίπεδο δεδομένων (Data)**. Σε αυτό το επίπεδο υπάρχουν οι οντότητες που αντιπροσωπεύουν τα δεδομένα της εφαρμογής. Αυτές οι οντότητες αντιπροσωπεύουν τον πυρήνα της εφαρμογής. Έχουν την πιο αφηρημένη μορφή και είναι τα πιο σταθερά κομμάτια του συστήματος και αποθηκεύονται/αντλούνται σε/από αποθετήρια (Repositories). Π.χ. σε ένα σύστημα διαχείρισης βιβλιοθήκης οι οντότητες μπορεί να είναι τα βιβλία τα οποία Έχουν γράψει οι συγγραφείς. Παρατηρείται δηλαδή, ότι ο πυρήνας της εφαρμογής έχει τα πιο σταθερά και ανεξάρτητα κομμάτια του συστήματος, ενώ όσο προχωράμε προς τα εξωτερικά επίπεδα, υπάρχουν πιο συγκεκριμένα και εξαρτημένα κομμάτια που έχουν την τάση να μεταβάλλονται με μεγαλύτερη συχνότητα.

1.3 Βάση Δεδομένων

Το Παρατηρητήριο χρησιμοποιεί μια σχεσιακή βάση δεδομένων. Ορίζει, διαχειρίζεται και αναζητά δεδομένα με τη Δομημένη Γλώσσα Ερωτήσεων (SQL). Οι πίνακες, που έχουν γραμμές και στήλες, αποθηκεύουν δεδομένα με οργανωμένο τρόπο. Αυτοί οι πίνακες, μπορούν να συνδέονται μεταξύ τους μέσω σχέσεων.

Στην προτεινόμενη λύση, χρησιμοποιείται η CockroachDB. Είναι μια κατανεμημένη βάση δεδομένων SQL. Έχει ενσωματωμένη υψηλή διαθεσιμότητα και επεκτασιμότητα καθώς επίσης κλιμακώνεται ομαλά και αντιγράφει δεδομένα σε πολλούς κόμβους. Αυτή η ικανότητα την καθιστά ανθεκτική σε σφάλματα. Είναι ιδανική για κατανεμημένες, παγκόσμιες εφαρμογές καθώς εξασφαλίζει ότι τα δεδομένα είναι πάντα διαθέσιμα.

Το σχήμα της βάση δεδομένων του συστήματος αποτελείται από δύο βασικούς πίνακες όπως αποτυπώνεται και στο Σχήμα 5.2:



Σχήμα 5.2: Σχήμα βάσης δεδομένων του Watchtower

- Πίνακας **smart_contracts**: Αυτός ο πίνακας περιέχει τα συνολικά έξυπνα συμβόλαια που έχουν ελεγχθεί από το Παρατηρητήριο. Περιέχει τα εξής πεδία:
 - **address**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων. Είναι η διεύθυνση του έξυπνου συμβολαίου σε κατακερματισμένη μορφή δεκαεξαδικού τύπου.
 - **network_id**: Πεδίο τύπου Ακεραίου. Είναι το μοναδικό αναγνωριστικό του δικτύου αλυσίδας μπλοκ στο οποίο υπάρχει το έξυπνο συμβόλαιο.
 - **network_name**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων. Είναι το όνομα του δικτύου αλυσίδας μπλοκ.
 - **network_rpc**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων. Είναι ο σύνδεσμος που χρησιμοποιείται για κλήσεις απομακρυσμένων διαδικασιών στο δίκτυο αλυσίδας μπλοκ.
 - **is_safe**: Πεδίο τύπου Διάκρισης. Είναι το αποτέλεσμα του ελέγχου του έξυπνου συμβολαίου. Σε περίπτωση που το έξυπνο συμβόλαιο είναι ασφαλές, το πεδίο παίρνει την τιμή «Αληθής» (True), αλλιώς παίρνει την τιμή «Ψευδής» (False).
- Πίνακας **vulnerabilities**: Αυτός ο πίνακας περιέχει τις ευπάθειες που εντοπίστηκαν κατά τον έλεγχο των έξυπνων συμβολαίων. Περιέχει τα εξής πεδία:
 - **id**: Πεδίο τύπου Ακεραίου. Είναι το μοναδικό αναγνωριστικό της εγγραφής στον πίνακα.
 - **address**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων.

Είναι η διεύθυνση του έξυπνου συμβολαίου σε κατακερματισμένη μορφή δεκαεξάδικού τύπου στην οποία βρέθηκε η εκάστοτε ευπάθεια.

- **network_id**: Πεδίο τύπου Ακεραίου. Είναι το μοναδικό αναγνωριστικό του δικτύου αλυσίδας μπλοκ στο οποίο υπάρχει το έξυπνο συμβόλαιο που βρέθηκε η εκάστοτε ευπάθεια.
- **vuln_address**: Πεδίο τύπου Ακεραίου. Είναι η διεύθυνση του κώδικα πράξης (opcode) όπου βρέθηκε η ευπάθεια.
- **description**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων. Είναι η περιγραφή της ευπάθειας που εντοπίστηκε.
- **function**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων. Είναι η συνάρτηση του έξυπνου συμβολαίου στην οποία βρέθηκε η ευπάθεια.
- **severity**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων. Είναι το επίπεδο καταστροφικότητας της ευπάθειας που εντοπίστηκε. Χωρίζεται σε τρία επίπεδα: «Χαμηλή» (Low), «Μέτρια» (Medium) και «Υψηλή» (High).
- **swc_id**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων. Είναι το μοναδικό αναγνωριστικό της Ταξινόμησης Αδυναμιών Έξυπνου Συμβολαίου (Smart Contract Weakness Classification - SWC) [30] που αντιστοιχεί στην ευπάθεια.
- **title**: Πεδίο τύπου Μεταβλητού Χαρακτήρα μέγιστου μήκους 256 χαρακτήρων. Είναι ο τίτλος της ευπάθειας που εντοπίστηκε.

Όπως φαίνεται και στο Σχήμα 5.2, το πεδίο **address** και το πεδίο **network_id** του πίνακα **smart_contracts**, σε συνδυασμό, αποτελούν το πρωτεύον κλειδί (primary key) του πίνακα. Αυτό σημαίνει ότι στον πίνακα μπορεί να υπάρχει μόνο μία διεύθυνση έξυπνου συμβολαίου για κάθε δίκτυο αλυσίδας μπλοκ. Αντίστοιχα, αυτά τα δύο πεδία αποτελούν το δευτερεύον κλειδί (foreign key) του πίνακα **vulnerabilities**. Τέλος, Παρατηρούμε ότι η σχέση μεταξύ του πίνακα **smart_contracts** και του πίνακα **vulnerabilities** είναι μία-προς-πολλά (one-to-many). Αυτό σημαίνει ότι ένα έξυπνο συμβόλαιο σε κάποιο δίκτυο μπορεί να έχει παραπάνω από μία ευπάθειες.

1.4 Εύρεση ευπαθειών

Ο έλεγχος ευπαθειών γίνεται σε δύο επίπεδα. Το πρώτο επίπεδο είναι η εύρεση ευπαθειών στον κώδικα του έξυπνου συμβολαίου. Στην παρούσα υλοποίηση, η εύρεση ευπαθειών στα έξυπνα συμβόλαια γίνεται με τη χρήση του εργαλείου ονόματι Mythril [11]. Το Mythril είναι ένα εργαλείο ανάλυσης ασφαλείας που έχει σχεδιαστεί για τον εντοπισμό ευπαθειών σε έξυπνα συμβόλαια. Χρησιμοποιεί τεχνικές συμβολικής εκτέλεσης, ανάλυσης ροής ελέγχου και ανάλυσης μολύνσεων για τον εντοπισμό πιθανών προβλημάτων στον κώδικα μηχανής (bytecode). Το Mythril είναι ένα εργαλείο ανοιχτού κώδικα, που χρησιμοποιείται για τον έλεγχο της αξιοπιστίας των έξυπνων συμβολαίων πριν από την ανάπτυξή τους σε κάποιο δίκτυο αλυσίδας μπλοκ.

Το Mythril πραγματοποιεί μια εις βάθος ανάλυση των έξυπνων συμβολαίων προσομοιώνοντας τη συμπεριφορά τους και ελέγχοντας για τρωτά σημεία ασφαλείας. Κάποια χαρακτηριστικά του εργαλείου:

- Μπορεί να εκτελέσει έλεγχο σε κώδικα μηχανής ή σε πηγαίο κώδικα.
- Χρησιμοποιεί συμβολική εκτέλεση, μια τεχνική που εξερευνά όλες τις πιθανές διαδρομές εκτέλεσης ενός προγράμματος. Αναθέτει συμβολικές τιμές στις εισόδους και αξιολογεί τη λογική του έξυπνου συμβολαίου υπό διαφορετικές συνθήκες, εντοπίζοντας ακραίες περιπτώσεις που ενδέχεται να οδηγήσουν σε ευπάθειες.
- Αναλύει τη ροή ελέγχου του έξυπνου συμβολαίου για τον εντοπισμό λογικών ατελειών ή συνθηκών που θα μπορούσαν να οδηγήσουν σε μη προβλεπόμενη συμπεριφορά.
- Εκτελεί ανάλυση μολύνσεων με την οποία παρακολουθεί τη ροή δυνητικά επικίνδυνων εισροών (όπως οι εισροές χρηστών) μέσω του έξυπνου συμβολαίου. Βοηθά στον εντοπισμό ευπαθειών όπου αυτές οι εισροές ενδέχεται να αξιοποιηθούν, όπως επιθέσεις Επανεισόδου (Reentrancy attack).

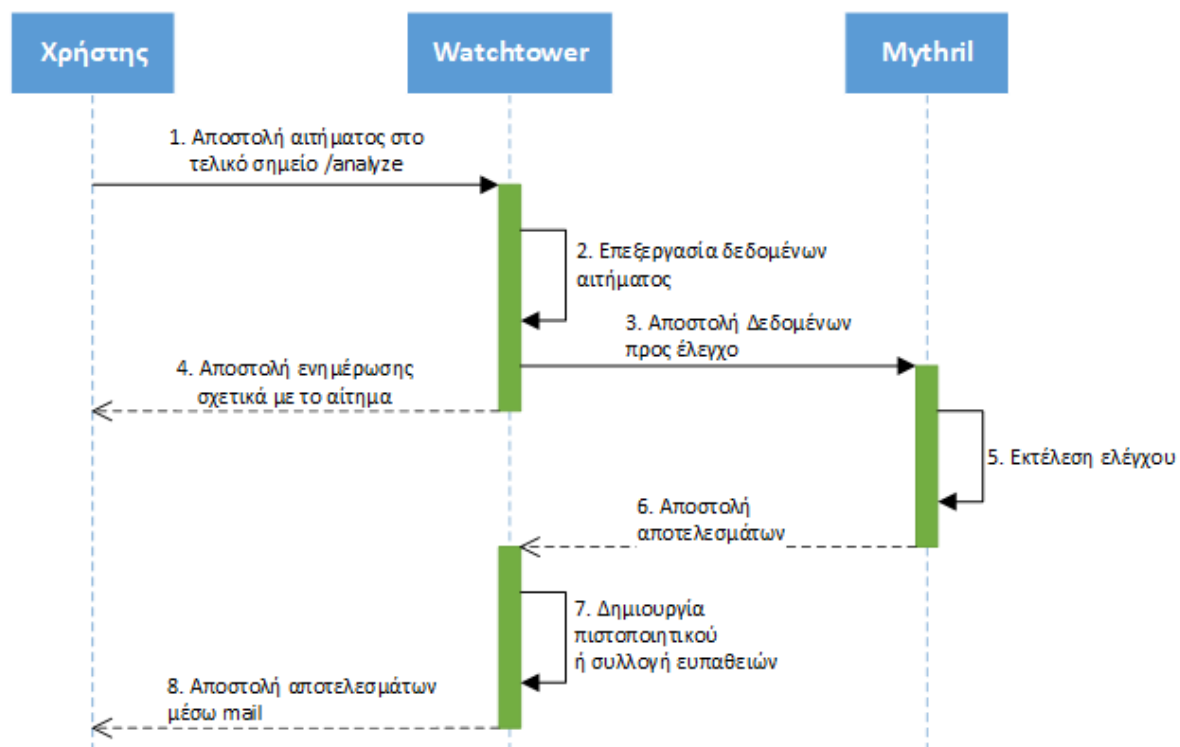
Στο δεύτερο επίπεδο γίνεται έλεγχος στην ιστοσελίδα που φιλοξενεί την αποκεντρωμένη εφαρμογή, για το αν έχει αναφερθεί ως κακόβουλη. Στην παρούσα υλοποίηση αυτός ο έλεγχος γίνεται με την χρήση της εξωτερικής υπηρεσίας ChainPatrol [9]. Η υπηρεσία αυτή παρέχει μια Διεπαφή Προγραμματισμού Εφαρμογής μέσω της οποίας το Παρατηρητήριο μπορεί να ελέγξει αν μια ιστοσελίδα έχει αναφερθεί ως κακόβουλη.

1.5 Επικοινωνία μεταξύ των στοιχείων του συστήματος

Προκειμένου να μπορούν τα εργαλεία εύρεσης ευπαθειών να επικοινωνούν με το Παρατηρητήριο εντός του συστήματος, χρησιμοποιείται το RabbitMQ [28]. Το RabbitMQ είναι ένας διαμεσολαβητής μηνυμάτων που διευκολύνει την επικοινωνία μεταξύ διαφορετικών τμημάτων ενός κατανεμημένου συστήματος υλοποιώντας το Προηγμένο Πρωτόκολλο Ουράς Μηνυμάτων (Advanced Message Queuing Protocol - AMQP), μαζί με άλλα πρωτόκολλα ανταλλαγής μηνυμάτων όπως είναι η Ουρά Μηνυμάτων Μεταφοράς Τηλεμετρίας (MQTT) και το Πρωτόκολλο Ανταλλαγής Μηνυμάτων Προσανατολισμένο σε Κείμενο Συνεχούς Ροής (Streaming Text Orientated Messaging Protocol - STOMP). Επιτρέπει την ασύγχρονη επικοινωνία, όπου οι παραγωγοί και οι καταναλωτές μηνυμάτων μπορούν να λειτουργούν ανεξάρτητα χωρίς να περιμένουν ο ένας τον άλλον.

2 Δημιουργία πιστοποιητικού

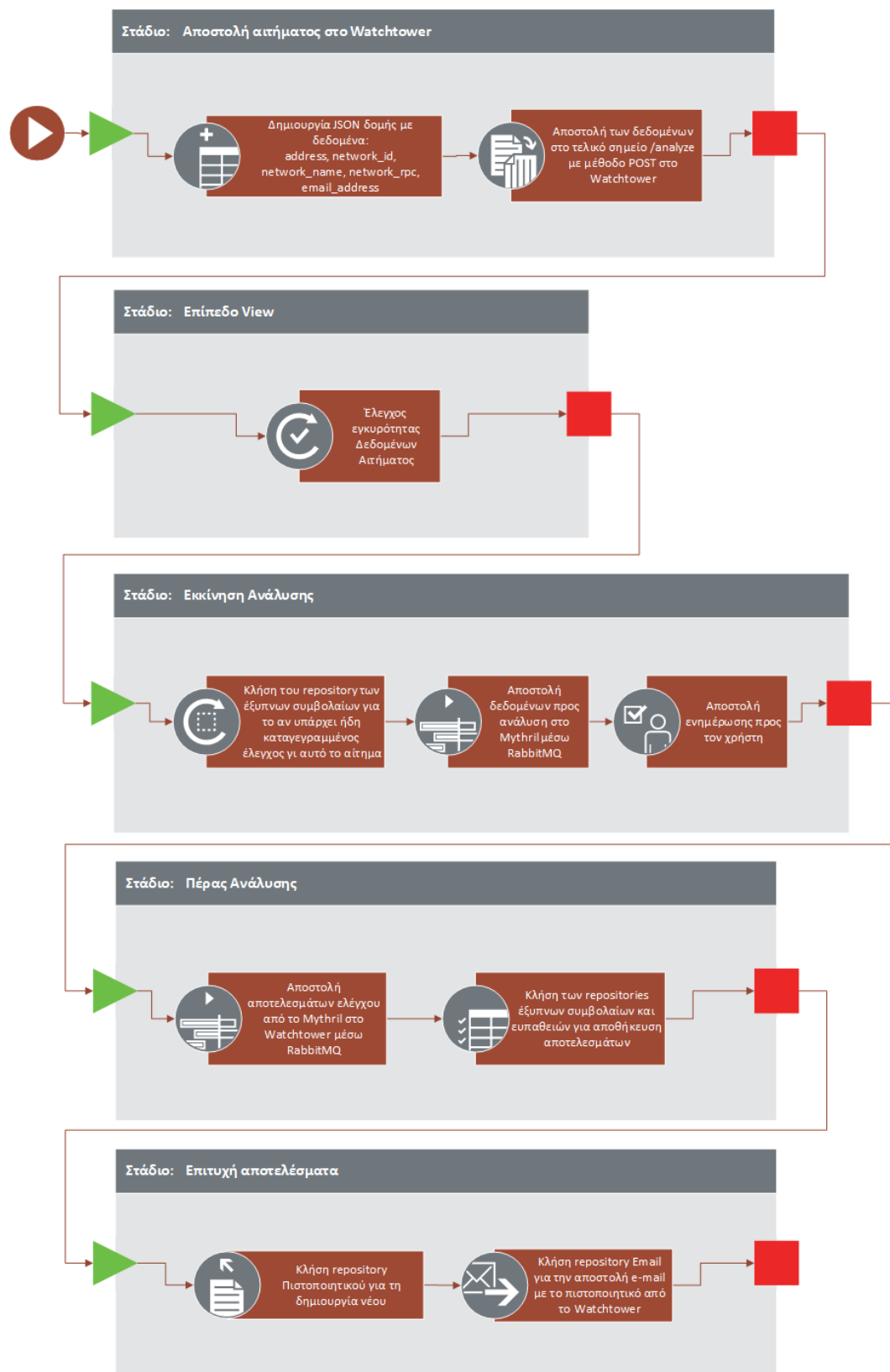
Στο παρακάτω Σχήμα 5.3 παρουσιάζεται το διάγραμμα ακολουθίας για τη δημιουργία ενός πιστοποιητικού.



Σχήμα 5.3: Διάγραμμα ακολουθίας δημιουργίας πιστοποιητικού

Πιο αναλυτικά η διαδικασία δημιουργίας πιστοποιητικού φαίνεται στο παρακάτω διάγραμμα-

μα ροής (Σχήμα 5.4), το οποίο και θα αναλυθεί.



Σχήμα 5.4: Διάγραμμα ροής διαδικασίας δημιουργίας πιστοποιητικού

Όπως μπορούμε να δούμε στο διάγραμμα, η διαδικασία ξεκινάει όταν ο προγραμματιστής του έξυπνου συμβολαίου αποφασίζει να δημιουργήσει ένα πιστοποιητικό για το έξυπνο συμβόλαιο του. Στέλνει ένα αίτημα στο Παρατηρητήριο και πιο συγκεκριμένα, στέλνει αίτημα τύπου POST στο τελικό σημείο «/v1/address/analyze» με το σώμα του αιτήματος να περιέχει: τη διεύθυνση του έξυπνου συμβολαίου (address), το αναγνωριστικό του δικτύου αλυσίδας μπλοκ (network_id), το όνομα του δικτύου (network_name), το σύνδεσμο Κλήσης Απομακρυσμένων Διαδικασιών του δικτύου αλυσίδας μπλοκ (network_rpc) και τη διεύθυνση mail (email_address) όπου θα σταλθούν τα αποτελέσματα ελέγχου ή το πιστοποιητικό. Τα στοιχεία αυτά φαίνονται στο Σχήμα 5.5.

Address Analysis Smart Contract vulnerability analysis based on address

POST /v1/address/analyze Analyze Address

Parameters

No parameters

Request body required

application/json

Example Value | Schema

```
{
  "address": "string",
  "network_id": 0,
  "network_name": "string",
  "network_rpc": "string",
  "email_address": "user@example.com"
}
```

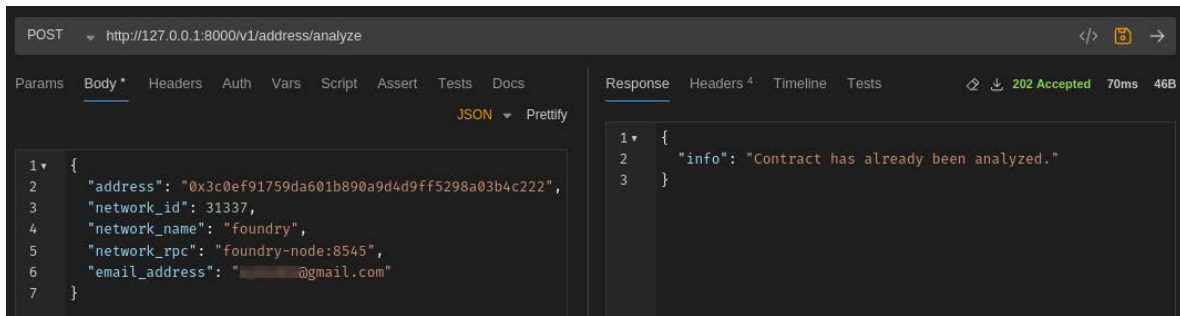
Responses

Code	Description	Links
202	Successful Response	No links
422	Validation Error	No links

Σχήμα 5.5: Στοιχεία του τελικού σημείου «/v1/address/analyze»

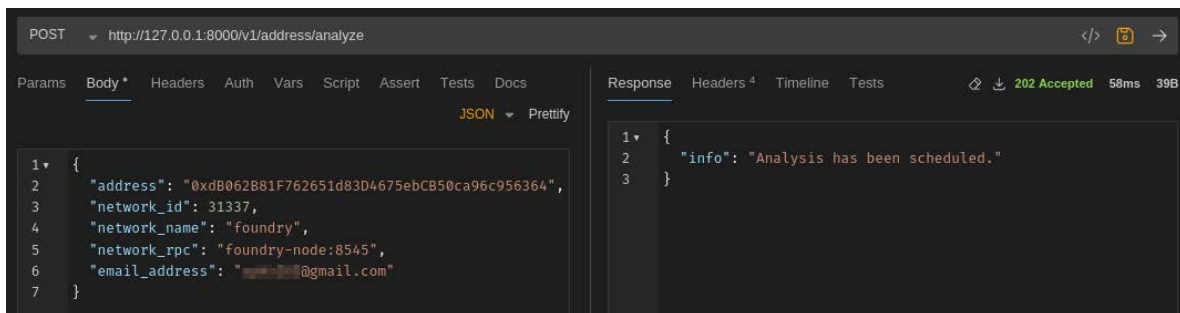
Μόλις το αίτημα φτάσει στο Παρατηρητήριο, αυτομάτως θα περάσει από το επίπεδο Προβολής (View) όπου θα γίνουν οι απαραίτητοι έλεγχοι για την ορθότητα των δεδομένων του αιτήματος, όπως π.χ. αν η διεύθυνση του έξυπνου συμβολαίου ακολουθεί το σωστό μορφωτικό πρότυπο.

Το αίτημα θα περάσει στο στάδιο του τομέα (Domain), όπου θα κληθεί το αποθετήριο των έξυπνων συμβολαίων (επίπεδο Δεδομένων) για να ελεγχθεί αν ο αιτούμενος έλεγχος έχει εκτελεστεί ήδη και τα αποτελέσματά του υπάρχουν ήδη στην βάση δεδομένων. Αν υπάρχουν τότε στέλνεται σχετική ενημέρωση στον χρήστη (Σχήμα 5.6) και τελειώνει η διαδικασία.



Σχήμα 5.6: Περίπτωση που η ανάλυση έχει ήδη πραγματοποιηθεί στο παρελθόν

Αν δεν υπάρχουν, τότε αποστέλνεται ένα μήνυμα στο εργαλείο Mythril μέσω της ουράς με όνομα «mythril_queue», όπου περιέχει την ενέργεια (action): «Ανάλυση» (analyze) και τις λεπτομέρειες (details) όπως: τη διεύθυνση του έξυπνου συμβολαίου (address) και το σύνδεσμο Κλήσης Απομακρυσμένων Διαδικασιών του δικτύου αλυσίδας μπλοκ (network_rpc). Λόγω του ότι η διαδικασία μπορεί να είναι χρονοβόρα, το Παρατηρητήριο θα απαντήσει στον χρήστη ενημερώνοντάς τον ότι η διαδικασία έχει ξεκινήσει (Σχήμα 5.7).



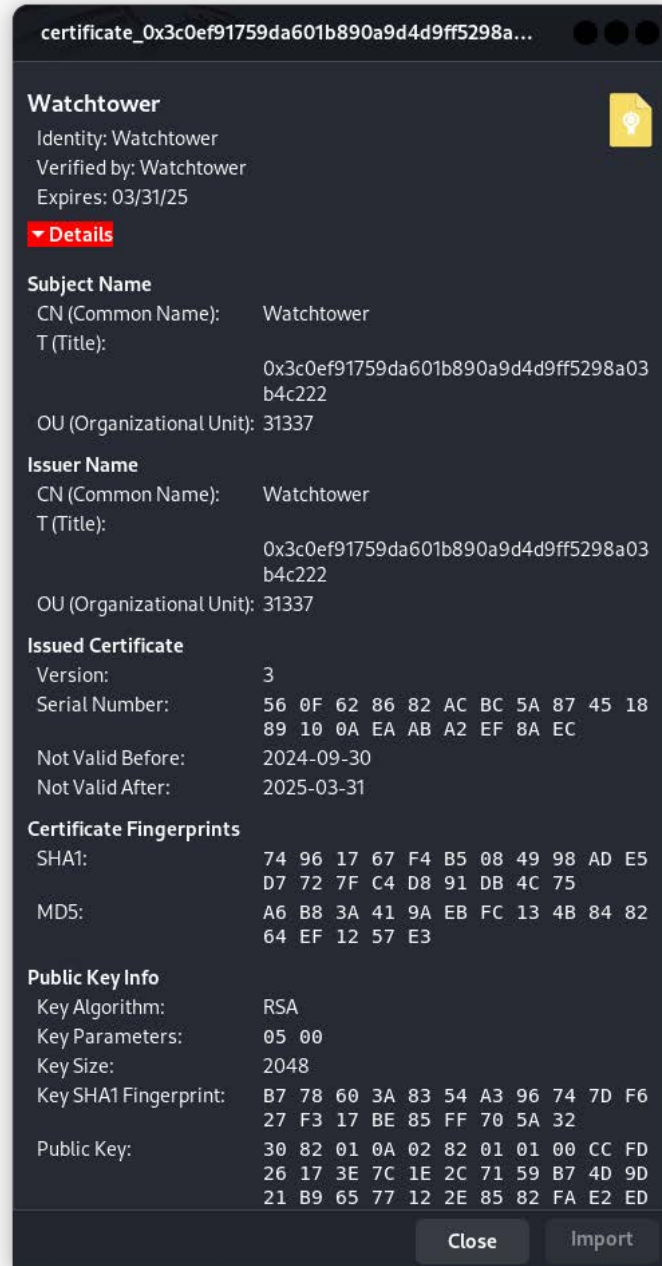
Σχήμα 5.7: Περίπτωση που η ανάλυση έχει προγραμματιστεί να εκτελεστεί

Το εργαλείο Mythril θα εκτελέσει τον έλεγχο του έξυπνου συμβολαίου και θα επιστρέψει τα αποτελέσματα της ανάλυσης μέσω της ουράς με όνομα «result_queue». Το Παρατηρητήριο αυτομάτως θα λάβει την απάντηση και θα καλέσει τα αποθετήρια των έξυπνων συμβολαίων και ευπαθειών προκειμένου να αποθηκεύσει τα αποτελέσματα της ανάλυσης στη βάση δεδομένων.

Στο τελικό στάδιο, αν τα αποτελέσματα της ανάλυσης δεν περιέχουν ευπάθειες, το Παρατηρητήριο θα κάνει κλήση του αποθετηρίου που είναι υπεύθυνο για τα πιστοποιητικά. Θα δημιουργήσει ένα νέο πιστοποιητικό όπου τα δεδομένα που θα έχει είναι:

- Το όνομα της υπηρεσίας «Watchtower» στο πεδίο του Εκδότη.

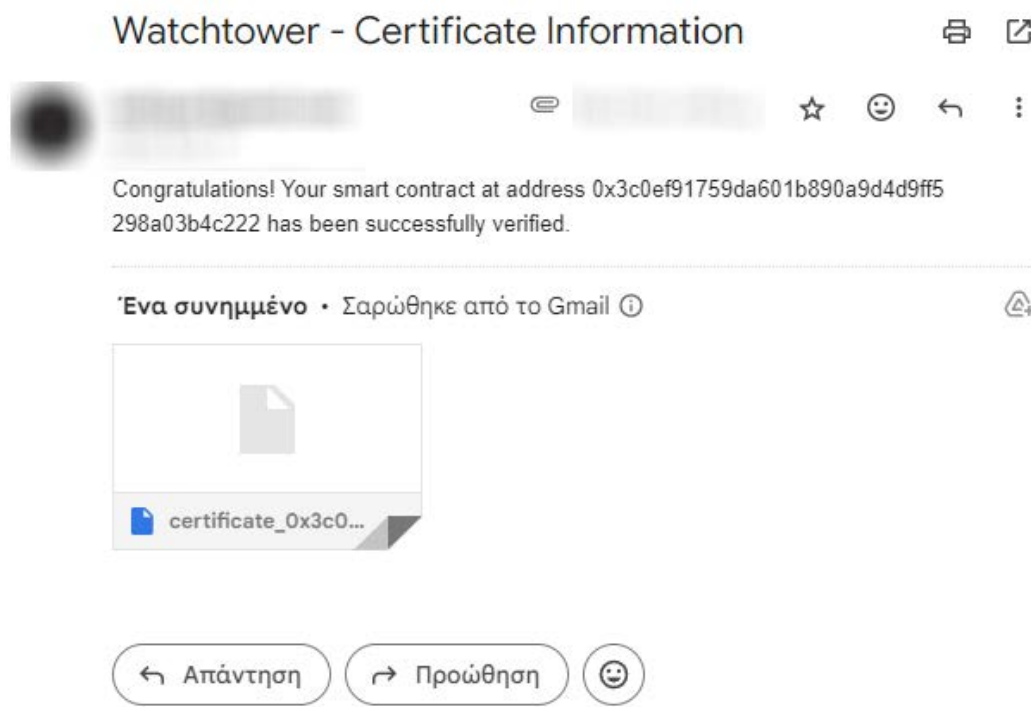
- Τη διεύθυνση του έξυπνου συμβολαίου στο πεδίο του Τίτλου,
- Το αναγνωριστικό δικτύου της αλυσίδας μπλοκ στο πεδίο του Ονόματος της Οργανωτικής Μονάδας.



Σχήμα 5.8: Δεδομένα πιστοποιητικού

Το πιστοποιητικό θα υπογραφεί με τη χρήση του ιδιωτικού ασύμμετρου κλειδιού (RSA)

που ανήκει στο Παρατηρητήριο, και θα έχει ισχύ για έξι μήνες. Τέλος θα κληθεί το αποθετήριο που είναι υπεύθυνο για την αποστολή των μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου και θα σταλεί το πιστοποιητικό στη διεύθυνση Email που είχε δηλώσει ο προγραμματιστής κατά το αρχικό αίτημα όπως φαίνεται στο Σχήμα 5.9. Τα δεδομένα που περιέχει το πιστοποιητικό απεικονίζονται στο Σχήμα 5.8.



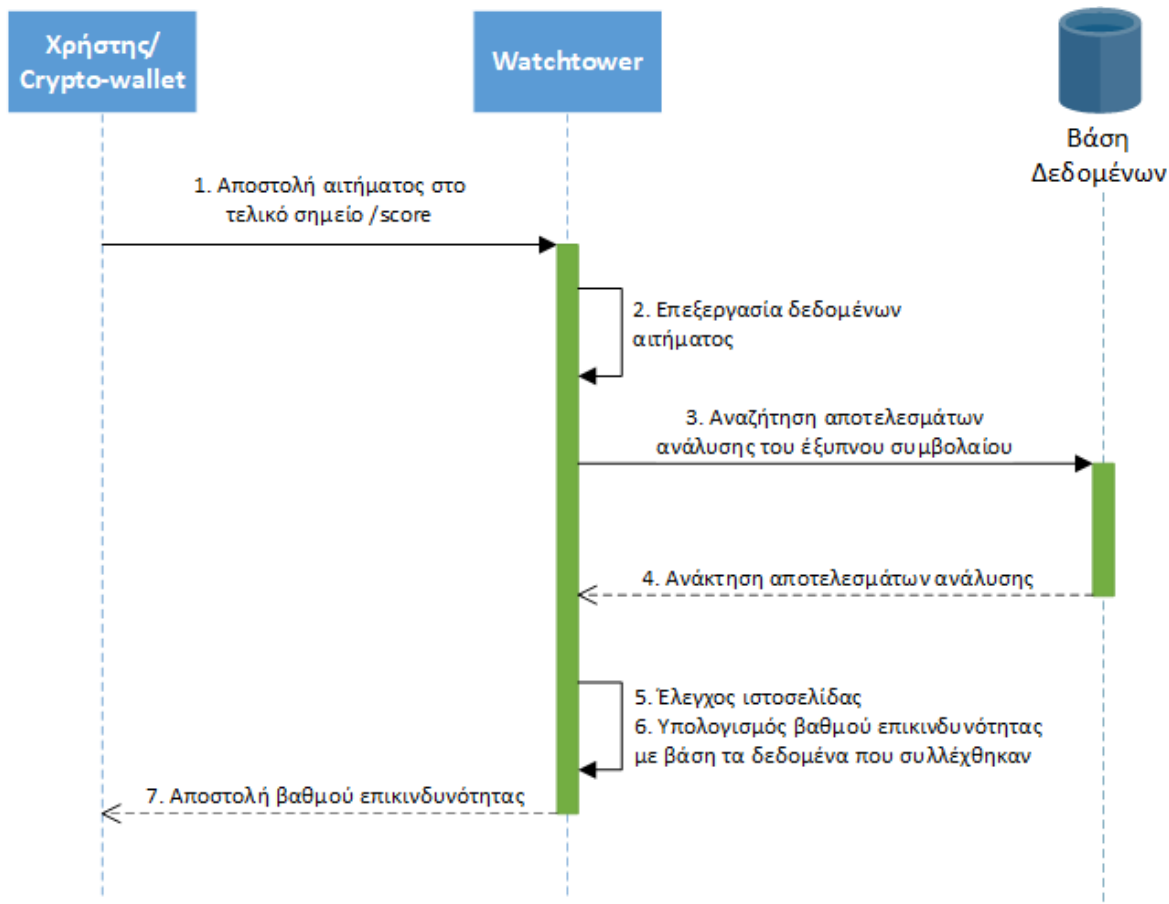
Σχήμα 5.9: Μήνυμα ηλεκτρονικού ταχυδρομείου με το πιστοποιητικό

Σε περίπτωση που τα αποτελέσματα της ανάλυσης περιέχουν ευπάθειες, το Παρατηρητήριο θα ενημερώσει τον χρήστη για την ύπαρξή τους μέσω e-mail, όπως φαίνεται και στο Σχήμα 5.10.

vuln_address	description	function	severity	swc_id	title
240	Any sender can cause the contract to self-destruct. Any sender can trigger execution of the SELFDESTRUCT instruction to destroy this contract account and withdraw its balance to an arbitrary address. Review the transaction trace generated for this issue and make sure that appropriate security controls are in place to prevent unrestricted access.	_function_0x7c11da20	High	106	Unprotected Selfdestruct



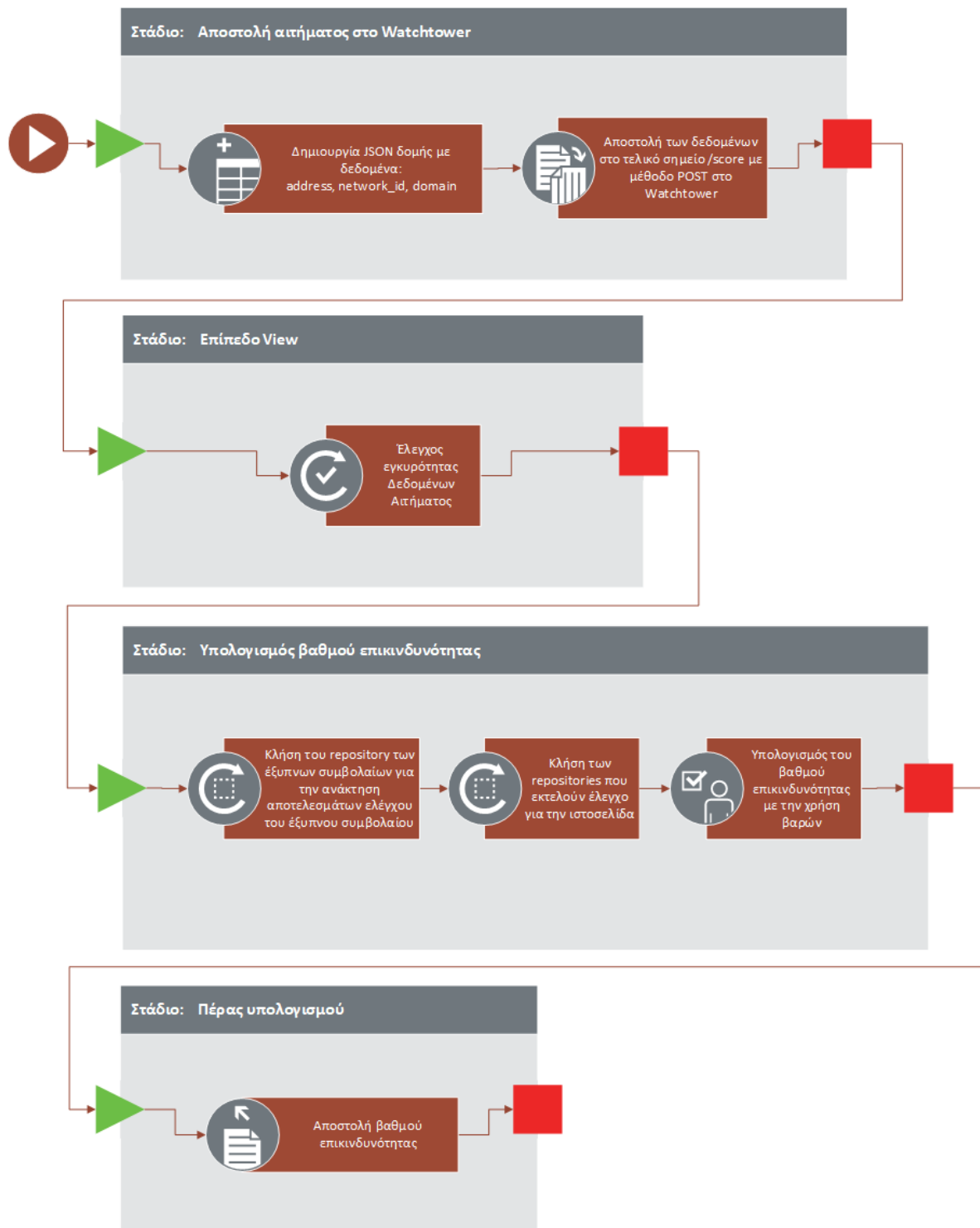


Σχήμα 5.11: Διάγραμμα ακολουθίας υπολογισμού βαθμού επικινδυνότητας

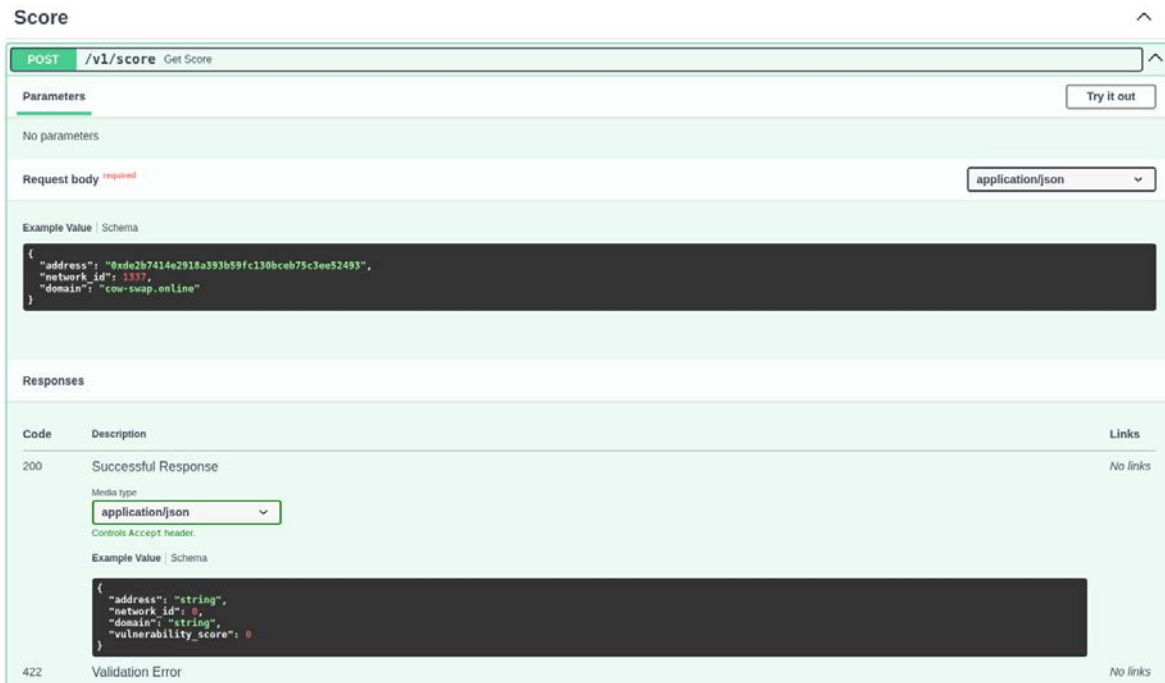
να τα συλλέξει. Για λόγους απλότητας θα χρησιμοποιηθεί το σενάριο στο οποίο το ψηφιακό πορτοφόλι κρυπτονομισμάτων ξεκινάει τη διαδικασία. Στέλνει ένα αίτημα τύπου POST στο τελικό σημείο «/v1/score» του Παρατηρητηρίου με το σώμα του αιτήματος να περιέχει: τη διεύθυνση του έξυπνου συμβολαίου (address), το αναγνωριστικό του δικτύου αλυσίδας μπλοκ (network_id) και τον τομέα της ιστοσελίδας (domain). Τα στοιχεία αυτά φαίνονται και στο Σχήμα 5.13.

Αφού το αίτημα ληφθεί από το Παρατηρητήριο, θα εκτελεστούν οι απαραίτητοι έλεγχοι για την ορθότητα των δεδομένων του αιτήματος στο επίπεδο της Προβολής (View). Όπως για το αν η διεύθυνση έξυπνου συμβολαίου ακολουθεί το σωστό μορφωτικό πρότυπο ή αν το όνομα τομέα της ιστοσελίδας είναι έγκυρο.

Το αίτημα θα περάσει στο στάδιο του Τομέα (Domain), όπου θα γίνει αρχικά η κλήση του αποθετηρίου των έξυπνων συμβολαίων (επίπεδο Δεδομένων) προκειμένου να γίνει ανάκτηση των αποτελεσμάτων από την ανάλυση του ζητούμενου έξυπνου συμβολαίου. Έπειτα, θα γίνει κλήση στο αποθετήριο που είναι υπεύθυνο για τον έλεγχο της ιστοσελίδας. Στην παρούσα



Σχήμα 5.12: Διάγραμμα ροής υπολογισμού βαθμού επικινδυνότητας



Σχήμα 5.13: Στοιχεία τελικού σημείου «/v1/score»

εργασία έχει γίνει χρήση της υπηρεσίας ChainPatrol. Ωστόσο η υλοποίηση του συστήματος του Παρατηρητηρίου έχει δομηθεί με τέτοιο τρόπο ώστε να μπορεί να φιλοξενήσει παραπάνω από μία υπηρεσίες με ελάχιστες αλλαγές στην υλοποίηση. Έστερα, αφού και τα δεδομένα για την ιστοσελίδα συλλεχθούν, θα κληθεί το αποθετήριο που είναι υπεύθυνο για τον υπολογισμό του βαθμού επικινδυνότητας. Σε αυτό το στάδιο ανατίθενται δύο βάρη για τον υπολογισμό, το βάρος της ανάλυσης του έξυπνου συμβολαίου και το βάρος της ανάλυσης της ιστοσελίδας. Στη παρούσα εργασία το βάρος της ανάλυσης του έξυπνου συμβολαίου έχει τεθεί στο 0.6 και το βάρος της ανάλυσης της ιστοσελίδας στο 0.4. Στη συνέχεια, ανατίθενται πόντοι για κάθε ευπάθεια με την φόρμουλα:

$$\text{πόντοι ανά ευπάθεια} = \frac{1}{\text{πλήθος ευπαθειών}} \quad (5.1)$$

Για κάθε μία ευπάθεια από την ανάλυση, υπολογίζεται το ποσοστό των πόντων που αντιστοιχούν σε αυτήν, με βάση το επίπεδο καταστροφικότητας (Severity):

- Χαμηλό (Low): $\frac{\text{Πόντοι ανά ευπάθεια}}{3}$
- Μεσαίο (Medium): $\frac{\text{Πόντοι ανά ευπάθεια}}{2}$
- Υψηλό (High): Πόντοι ανά ευπάθεια

Τα αποτελέσματα αυτά αθροίζονται και πολλαπλασιάζονται με το βάρος της ανάλυσης του έξυπνου συμβολαίου.

$$\text{σκορ ανάλυσης έξυπνου συμβολαίου} = \sum (\text{ποσοστό πόντων ευπάθειας}) \times 0.6 \quad (5.2)$$

Στη συνέχεια υπολογίζεται το σκορ ανάλυσης της ιστοσελίδας με παρόμοιο τρόπο. Αρχικά ανατίθενται πόντοι για τον κάθε έλεγχο που έχει πραγματοποιηθεί για την εκάστοτε ιστοσελίδα (στην παρούσα εργασία – όπως αναφέρθηκε προηγουμένως – έχει χρησιμοποιηθεί μόνο μία υπηρεσία για τον έλεγχο της ιστοσελίδας):

$$\text{πόντοι ανά έλεγχο} = \frac{1}{\text{πλήθος ελέγχων από υπηρεσίες}} \quad (5.3)$$

Για κάθε μία από τις αναλύσεις που έχουν πραγματοποιηθεί, υπολογίζεται το ποσοστό των πόντων που αντιστοιχούν σε αυτήν με βάση τη κατάσταση τους (Status):

- Ασφαλής (Safe): 0
- Ανασφαλής (Unsafe): Πόντοι ανά έλεγχο
- Άγνωστο (Unknown): $\frac{\text{Πόντοι ανά έλεγχο}}{3}$

Τα αποτελέσματα αυτά αθροίζονται και πολλαπλασιάζονται με το βάρος της ανάλυσης της ιστοσελίδας.

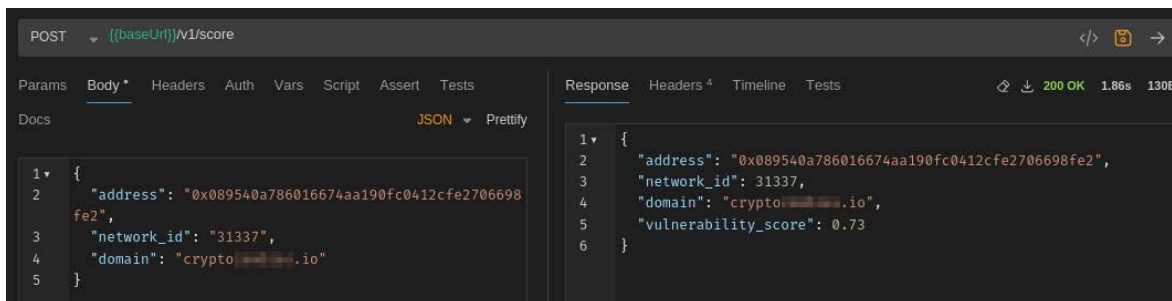
$$\text{σκορ ανάλυσης ιστοσελίδας} = \sum (\text{ποσοστό πόντων ελέγχου}) \times 0.4 \quad (5.4)$$

Σε τελικό στάδιο, τα δύο σκορ αθροίζονται και το αποτέλεσμα στρογγυλοποιείται ούτως ώστε να έχει δύο δεκαδικά ψηφία. Η τιμή του αποτελέσματος ανήκει στο διάστημα $[0, 1]$.

Για παράδειγμα. Αν ένα έξυπνο συμβόλαιο έχει τεσσereis ευπάθειες: δύο υψηλές, δύο μεσαίες και η ιστοσελίδα έχει δύο ελέγχους με κατάσταση: μία ανασφαλής και μία άγνωστη, τότε ο βαθμός επικινδυνότητας θα είναι:

$$\text{Βαθμός επικινδυνότητας} = 0.6 \times \left[\frac{1}{4} \times \left(1 + 1 + \frac{1}{2} + \frac{1}{2} \right) \right] + 0.4 \times \left[\frac{1}{2} \times \left(1 + \frac{1}{3} \right) \right] = 0.72 \quad (5.5)$$

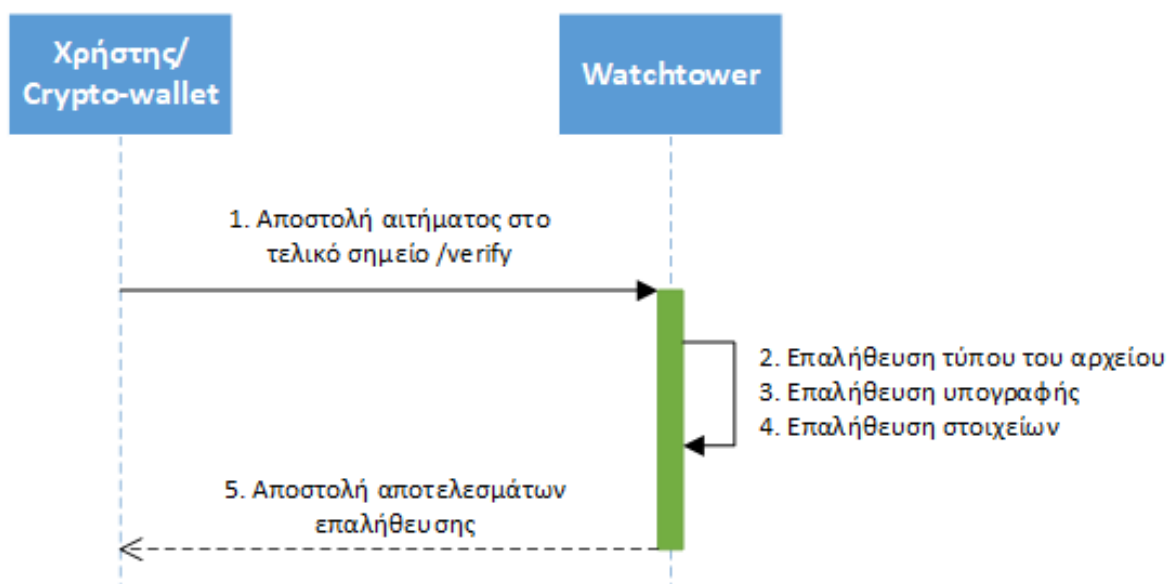
Τέλος, το αριθμητικό αποτέλεσμα αποστέλλεται σαν απάντηση στο ψηφιακό πορτοφόλι κρυπτονομισμάτων.



Σχήμα 5.14: Παράδειγμα αποτελέσματος βαθμού επικινδυνότητας (0.73)

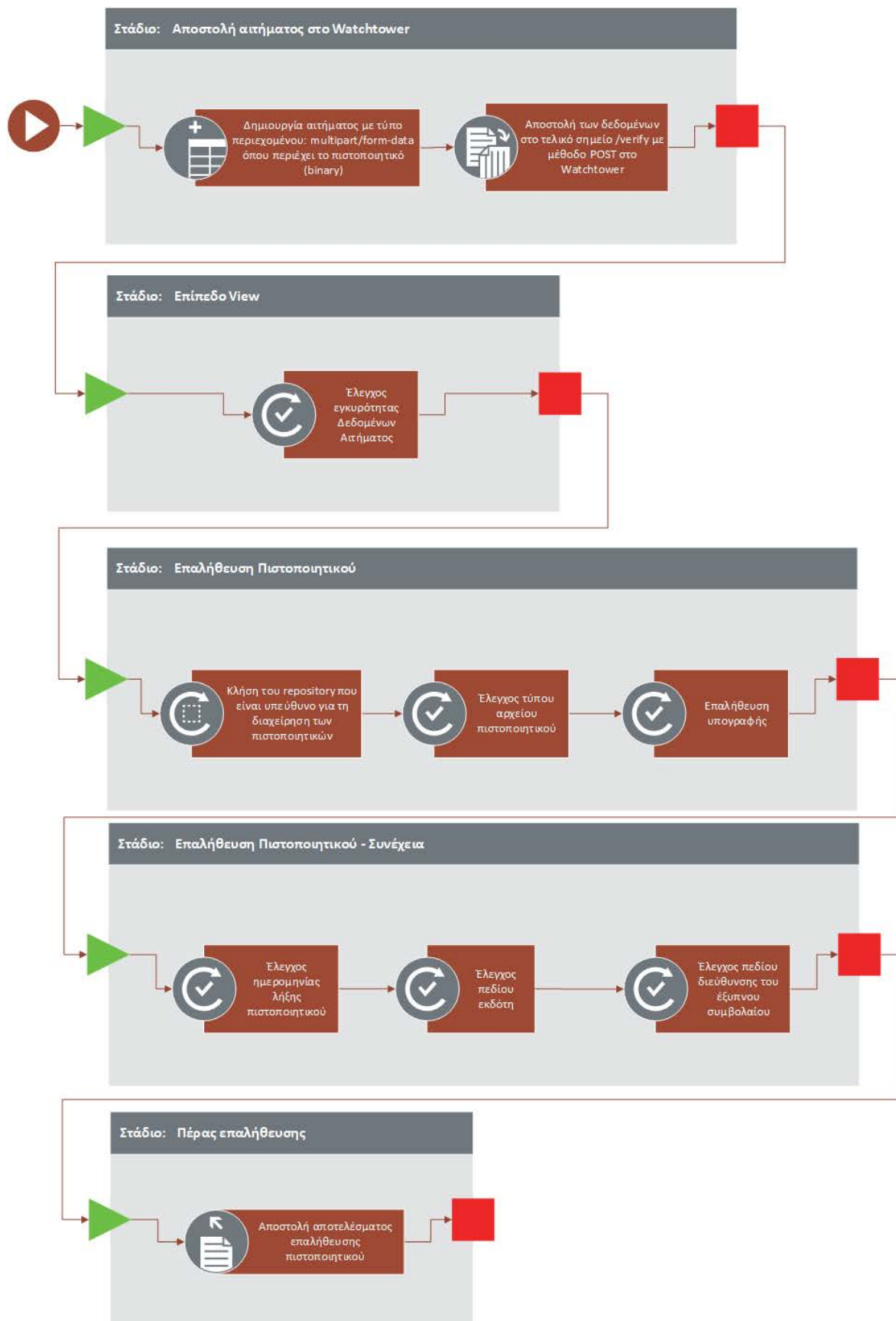
4 Διαδικασία επαλήθευσης πιστοποιητικού

Όταν ο προγραμματιστής ή ο υπεύθυνος της ιστοσελίδας που φιλοξενεί την αποκεντρωμένη εφαρμογή λάβει πιστοποιητικό από το Παρατηρητήριο, μπορεί να το εναποθέσει στην ιστοσελίδα του, ώστε να είναι προσβάσιμο από τους χρήστες ή από το ψηφιακό πορτοφόλι κρυπτονομισμάτων. Έτσι οι χρήστες μπορούν να εκκινήσουν την διαδικασία της επαλήθευσης του πιστοποιητικού χειροκίνητα, καθώς και τα ψηφιακά πορτοφόλια, προκειμένου να έχουν ένα γρηγορότερο τρόπο επαλήθευσης για τις συναλλαγές εντός της αποκεντρωμένης εφαρμογής. Στο Σχήμα 5.15 φαίνεται το διάγραμμα ακολουθίας που απεικονίζει τη διαδικασία της επαλήθευσης ενός πιστοποιητικού σε υψηλό επίπεδο.



Σχήμα 5.15: Διάγραμμα ακολουθίας επαλήθευσης πιστοποιητικών

Πιο αναλυτικά, η διαδικασία της επαλήθευσης ενός πιστοποιητικού φαίνεται στο διάγραμμα ροής του Σχήματος 5.16.



Σχήμα 5.16: Διάγραμμα ροής επαλήθευσης πιστοποιητικού

Η διαδικασία ξεκινάει όταν ένας χρήστης ή ένα ψηφιακό πορτοφόλι κρυπτονομισμάτων αποφασίζει να επαληθεύσει το πιστοποιητικό που υπάρχει στην ιστοσελίδα που φιλοξενεί μια αποκεντρωμένη εφαρμογή. Στέλνει ένα αίτημα τύπου POST στο τελικό σημείο «/v1/verify» του Παρατηρητηρίου έχοντας στις κεφαλές (Headers) του αιτήματος το πεδίο «Content-Type» ορισμένο με τιμή: «multipart/form-data». Αυτό θα σηματοδοτήσει ότι τα δεδομένα που θα σταλθούν μέσω του αιτήματος, θα είναι αρχεία. Το σώμα του αιτήματος θα πρέπει να περιέχει το πιστοποιητικό που θέλει να επαληθεύσει, το οποίο είναι ένα αρχείο σε δυαδική μορφή (binary). Τα παραπάνω χαρακτηριστικά φαίνονται στο Σχήμα 5.17.

The screenshot displays a REST client interface with two tabs: 'Score' and 'Certificate'. The 'Certificate' tab is active, showing a POST request to '/v1/verify'. The request body is configured as 'multipart/form-data' with a required field 'file' of type 'string(\$binary)'. The 'Responses' section shows a 200 status code with a 'Successful Response' in 'application/json' format. The example response is a JSON object: { "verified": true, "failed_reason": "string" }. A 422 status code is also listed for 'Validation Error'.

Σχήμα 5.17: Στοιχεία τελικού σημείου «/v1/verify»

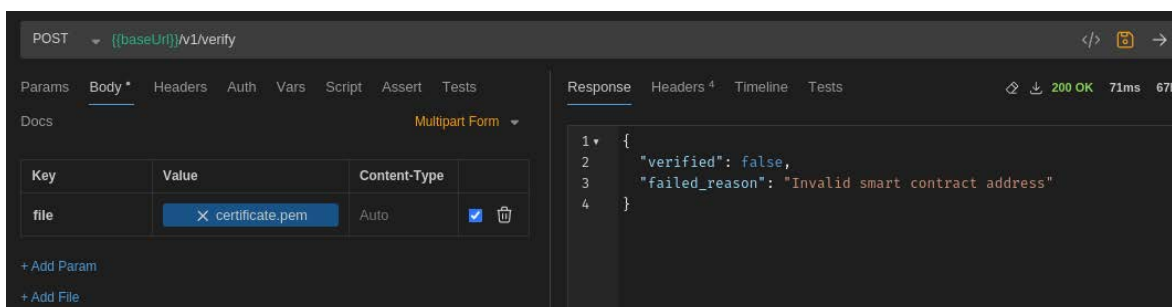
Όταν το αίτημα ληφθεί από το Παρατηρητήριο, θα κληθεί το επίπεδο Τομέα (Domain) στο οποίο θα χρησιμοποιηθεί το αποθετήριο που είναι υπεύθυνο για την διαχείριση των πιστοποιητικών. Αρχικά, θα γίνει έλεγχος αν το αρχείο που δόθηκε στο αίτημα είναι ένα έγκυρο X.509 (πρότυπο Διεθνής Ένωσης Τηλεπικοινωνιών που ορίζει τα πιστοποιητικά δημοσίου κλειδιού [18]) με κωδικοποίηση σύμφωνα με τους Διακεκριμένους Κανόνες Κωδικοποίησης (DER). Αν το αρχείο δεν είναι έγκυρο, το Παρατηρητήριο θα επιστρέψει ένα μήνυμα ενημέρωσης σχετικά με το σφάλμα. Αν το αρχείο είναι έγκυρο, θα ελεγχθεί αν το πιστοποιητικό είναι υπογεγραμμένο από το Παρατηρητήριο. Χρησιμοποιώντας το δημόσιο κλειδί του. Αν η υπογραφή είναι έγκυρη, το Παρατηρητήριο θα προχωρήσει στην επιβεβαίωση των δεδο-

μένων που περιέχει το πιστοποιητικό. Ο πρώτος έλεγχος που γίνεται, αφορά την ημερομηνία λήξης του πιστοποιητικού. Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, τα πιστοποιητικά είναι έγκυρα από τη στιγμή που εκδίδονται μέχρι και 6 μήνες μετά. Αν το πιστοποιητικό έχει λήξει, το Παρατηρητήριο θα επιστρέψει ένα μήνυμα ενημέρωσης σχετικά με το σφάλμα. Ο δεύτερος έλεγχος που γίνεται είναι για το αν υπάρχει τιμή στο πεδίο του εκδότη (Issuer) του πιστοποιητικού και αν υπάρχει, θα πρέπει να ταυτίζεται με το Παρατηρητήριο. Αν ο έλεγχος δεν ολοκληρωθεί επιτυχώς, επιστρέφεται σαν απάντηση το αντίστοιχο μήνυμα σφάλματος. Τέλος, γίνεται έλεγχος αν υπάρχει τιμή στο πεδίο του Τίτλου (Title). Αν υπάρχει θα πρέπει να είναι μία έγκυρη διεύθυνση έξυπνου συμβολαίου σε κατακερματισμένη μορφή δεκαεξαδικού τύπου. Αν ο έλεγχος δεν περάσει επιτυχώς, θα σταλθεί σαν απάντηση το αντίστοιχο μήνυμα σφάλματος.

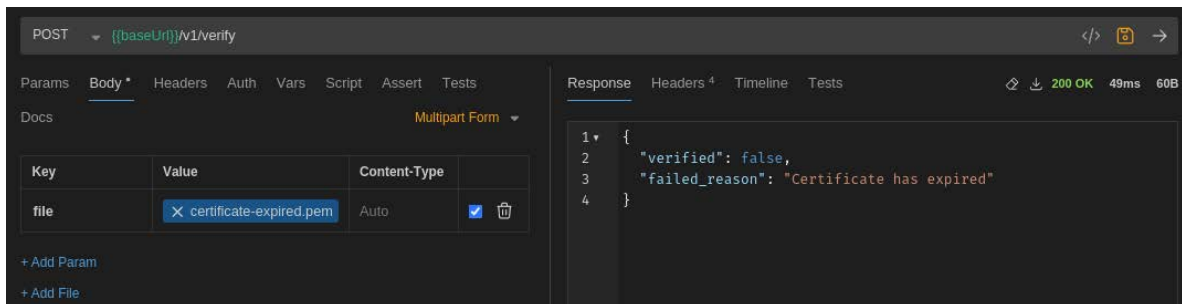
Μετά την ολοκλήρωση των παραπάνω ελέγχων, θα σταλθεί μία απάντηση που το σώμα (body) της θα περιέχει σε μορφή JSON τα πεδία:

- **verified:** Πεδίο τύπου Διάκρισης (Boolean). Για το αν το πιστοποιητικό είναι έγκυρο ή όχι.
- **failed_reason:** Πεδίο τύπου Συμβολοσειράς (String). Αν το πιστοποιητικό δεν είναι έγκυρο, θα περιέχει τον λόγο της αποτυχίας.

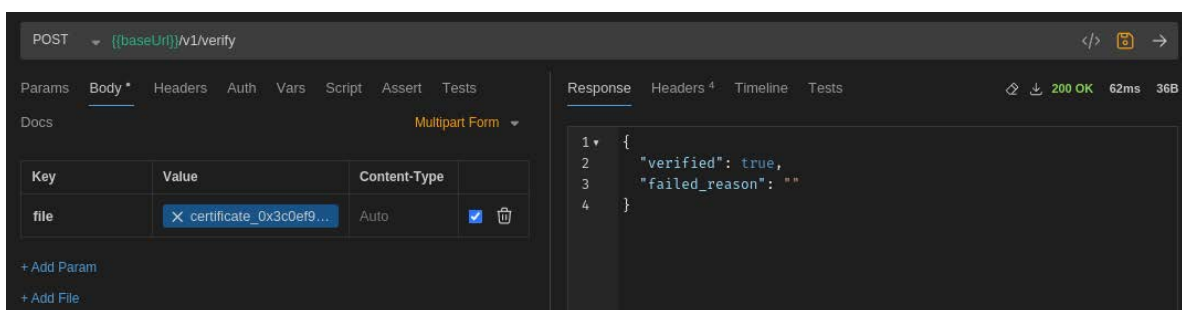
Ακολουθούν παραδείγματα απαντήσεων από επαληθεύσεις πιστοποιητικών στα επόμενα σχήματα.



Σχήμα 5.18: Αποτέλεσμα επαλήθευσης πιστοποιητικού με εσφαλμένη διεύθυνση Έξυπνου Συμβολαίου



Σχήμα 5.19: Αποτέλεσμα επαλήθευσης πιστοποιητικού που έχει λήξει



Σχήμα 5.20: Αποτέλεσμα επαλήθευσης πιστοποιητικού που είναι έγκυρο

Κεφάλαιο 6

Συμπεράσματα

Η παρούσα εργασία είχε ως στόχο την δημιουργία ενός συστήματος που θα μπορεί να προλαμβάνει κινδύνους που μπορεί να υπάρχουν σε αποκεντρωμένες Web3 εφαρμογές που οι χρήστες αλληλεπιδρούν. Λόγω του ότι ευπάθειες μπορούν να υπάρχουν σε οποιαδήποτε επίπεδο (βλ. Κεφάλαιο 3), το Παρατηρητήριο υλοποιήθηκε για να καλύψει ευπάθειες που μπορούν να υπάρξουν στα επίπεδα του Έξυπνου Συμβολαίου και της Εφαρμογής.

Το σύστημα που αναπτύχθηκε στα πλαίσια αυτής της εργασίας είναι σε ένα πρώιμο στάδιο και μπορεί να δεχθεί αρκετές βελτιστοποιήσεις και επεκτάσεις, ώστε να είναι πιο εύελκτο, και γρήγορο. Η αρχιτεκτονική που έχει υλοποιηθεί το σύστημα, βοηθάει στην εύκολη προσθήκη επεκτάσεων με ελάχιστες αλλαγές. Κάποιες από τις βελτιώσεις που μπορεί να δεχθεί είναι:

- Προσθήκη εργαλείων για την ανίχνευση ευπαθειών σε έξυπνα συμβόλαια. Αυτή η αρχική έκδοση χρησιμοποιεί μόνο ένα εργαλείο για την ανίχνευση ευπαθειών στον κώδικα των έξυπνο συμβολαίων.
- Ρύθμιση των παραμέτρων στα που χρησιμοποιούνται για την εύρεση ευπαθειών. Αυτή τη στιγμή το χρησιμοποιούμενο εργαλείο έχει ρυθμιστεί με παραμέτρους που το καθιστούν πιο γρήγορο στην ανίχνευση ευπαθειών, θυσιάζοντας την πιο εις βάθος ανάλυση και εύρεση περισσότερων ευπαθειών. Εναλλακτικά μπορούν αυτές οι παράμετροι να εξαχθούν προς τον εντολέα και να ρυθμίζονται ένα βήμα πριν την εκτέλεση του ελέγχου.
- Προσθήκη εργαλείων για την ανίχνευση ευπαθειών σε επίπεδο εφαρμογής. Αυτή τη στιγμή το σύστημα χρησιμοποιεί ένα εργαλείο για την ανίχνευση θεμάτων ασφαλείας σε ιστοσελίδες.

- Προσθήκη μηχανισμού προσωρινής μνήμης. Με αυτό τον τρόπο αποτελέσματα που ζητούνται επανειλημμένα δεν θα χρειάζεται να υπολογίζονται κάθε φορά από την αρχή. Αυτό θα μειώσει τον χρόνο που χρειάζεται για να εξυπηρετηθεί ένα αίτημα.

Βιβλιογραφία

Ξενόγλωσση βιβλιογραφία

- [1] “Payzero” Scams and The Evolution of Asset Theft in Web3. Jan. 2023. URL: https://www.trendmicro.com/en_us/research/23/a/payzero-scams-and-the-evolution-of-asset-theft-in-web3.html.
- [2] Sarah Azouvi, George Danezis, and Valeria Nikolaenko. “Winkle: Foiling Long-Range Attacks in Proof-of-Stake Systems”. In: *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. New York NY USA: ACM, Oct. 2020, pp. 189–201. ISBN: 978-1-4503-8139-0. DOI: [10.1145/3419614.3423260](https://doi.org/10.1145/3419614.3423260).
- [3] L. M. Bach, B. Mihaljevic και M. Zagar. «Comparative Analysis of Blockchain Consensus Algorithms». Στο: *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Opatija: IEEE, Μάι. 2018, σσ. 1545–1550. ISBN: 978-953-233-095-3. DOI: [10.23919/MIPRO.2018.8400278](https://doi.org/10.23919/MIPRO.2018.8400278).
- [4] Marianna Belotti et al. “A Vademecum on Blockchain Technologies: When, Which, and How”. In: *IEEE Communications Surveys & Tutorials* 21.4 (2019), pp. 3796–3838. ISSN: 1553-877X, 2373-745X. DOI: [10.1109/COMST.2019.2928178](https://doi.org/10.1109/COMST.2019.2928178).
- [5] Karthikeyan Bhargavan et al. “Formal Verification of Smart Contracts: Short Paper”. In: *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*. Vienna Austria: ACM, Oct. 2016, pp. 91–96. ISBN: 978-1-4503-4574-3. DOI: [10.1145/2993600.2993611](https://doi.org/10.1145/2993600.2993611). (Visited on 02/08/2025).
- [6] Alexandra Boldyreva and Daniele Micciancio, eds. *Advances in Cryptology – CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I*. Vol. 11692. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019. ISBN: 978-3-030-26947-0 978-3-030-26948-7. DOI: [10.1007/978-3-030-26948-7](https://doi.org/10.1007/978-3-030-26948-7).
- [7] Joseph Bonneau and Nadia Heninger, eds. *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers*. Vol. 12059. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020. ISBN: 978-3-030-51279-8 978-3-030-51280-4. DOI: [10.1007/978-3-030-51280-4](https://doi.org/10.1007/978-3-030-51280-4).
- [8] Amy Castor. *Popular Ether Wallet MEW Is Hijacked in DNS Attack*. Apr. 2018. URL: <https://bitcoinmagazine.com/culture/popular-ether-wallet-mew-hijacked-dns-attack>.

- [9] *ChainPatrol*. URL: <https://chainpatrol.io/>.
- [10] Ting Chen et al. “Under-Optimized Smart Contracts Devour Your Money”. In: *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*. Klagenfurt, Austria: IEEE, Feb. 2017, pp. 442–446. ISBN: 978-1-5090-5501-2. DOI: [10.1109/SANER.2017.7884650](https://doi.org/10.1109/SANER.2017.7884650). (Visited on 02/08/2025).
- [11] *Consensys/Mythril*. Consensys. Δεκ. 2024. URL: <https://github.com/Consensys/mythril>.
- [12] Dan Michael Cortez, Ariel Sison και Ruji Medina. «Cryptographic Randomness Test of the Modified Hashing Function of SHA256 to Address Length Extension Attack». Στο: Απρ. 2020, σσ. 24–28. DOI: [10.1145/3390525.3390540](https://doi.org/10.1145/3390525.3390540).
- [13] Evangelos Deirmentzoglou, Georgios Papakyriakopoulos, and Constantinos Patsakis. “A Survey on Long-Range Attacks for Proof of Stake Protocols”. In: *IEEE Access* 7 (2019), pp. 28712–28725. ISSN: 2169-3536. DOI: [10.1109/ACCESS.2019.2901858](https://doi.org/10.1109/ACCESS.2019.2901858).
- [14] John R. Douceur. «The Sybil Attack». Στο: *International Workshop on Peer-to-Peer Systems*. 2002. URL: <https://api.semanticscholar.org/CorpusID:5310675>.
- [15] Li Duan et al. “Multiple-Layer Security Threats on the Ethereum Blockchain and Their Countermeasures”. In: *Security and Communication Networks* 2022 (Feb. 2022), e5307697. ISSN: 1939-0114. DOI: [10.1155/2022/5307697](https://doi.org/10.1155/2022/5307697).
- [16] *FastAPI*. URL: <https://fastapi.tiangolo.com/>.
- [17] Joaquin Garcia-Alfaro et al., eds. *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14-15, 2017, Proceedings*. Vol. 10436. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. ISBN: 978-3-319-67815-3 978-3-319-67816-0. DOI: [10.1007/978-3-319-67816-0](https://doi.org/10.1007/978-3-319-67816-0).
- [18] E Gerck and E Gerck. “Overview of Certification Systems: X.509, CA, PGP and SKIP”. In: ().
- [19] Ethan Heilman and Alison Kendler. “Eclipse Attacks on Bitcoin’s Peer-to-Peer Network”. In: ().
- [20] Sukrit Kalra et al. “ZEUS: Analyzing Safety of Smart Contracts”. In: *Proceedings 2018 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society, 2018. ISBN: 978-1-891562-49-5. DOI: [10.14722/ndss.2018.23082](https://doi.org/10.14722/ndss.2018.23082). (Visited on 02/08/2025).
- [21] Loi Luu et al. “Making Smart Contracts Smarter”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. Vienna Austria: ACM, Oct. 2016, pp. 254–269. ISBN: 978-1-4503-4139-4. DOI: [10.1145/2976749.2978309](https://doi.org/10.1145/2976749.2978309). (Visited on 02/08/2025).
- [22] Robert C. Martin et al. *Clean Architecture: A Craftsman’s Guide to Software Structure and Design*. Robert C. Martin Series. Prentice Hall, 2018. ISBN: 978-0-13-449416-6.
- [23] *MetaMask Phishing Attacks Put Crypto Users At Risk*. Feb. 2023. URL: <https://thecyberexpress.com/metamask-phishing-attacks-crypto-users-at-risk/>.

- [24] Michael Mirkin et al. “BDoS: Blockchain Denial-of-Service”. In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. Virtual Event USA: ACM, Oct. 2020, pp. 601–619. ISBN: 978-1-4503-7089-9. DOI: [10.1145/3372297.3417247](https://doi.org/10.1145/3372297.3417247).
- [25] Ivica Nikolic et al. *Finding The Greedy, Prodigal, and Suicidal Contracts at Scale*. Mar. 2018. DOI: [10.48550/arXiv.1802.06038](https://doi.org/10.48550/arXiv.1802.06038). arXiv: [1802.06038](https://arxiv.org/abs/1802.06038) [cs]. (Visited on 02/08/2025).
- [26] *NVD - Cve-2018-10299*. URL: <https://nvd.nist.gov/vuln/detail/cve-2018-10299>.
- [27] Purathani Praitheeshan et al. *Security Analysis Methods on Ethereum Smart Contract Vulnerabilities: A Survey*. Sept. 2020. DOI: [10.48550/arXiv.1908.08605](https://doi.org/10.48550/arXiv.1908.08605). arXiv: [1908.08605](https://arxiv.org/abs/1908.08605) [cs]. (Visited on 02/08/2025).
- [28] *RabbitMQ: One Broker to Queue Them All | RabbitMQ*. URL: <https://www.rabbitmq.com/>.
- [29] Dan Sheridan et al. *Web3 Challenges and Opportunities for the Market*. Sept. 2022. DOI: [10.48550/arXiv.2209.02446](https://doi.org/10.48550/arXiv.2209.02446). arXiv: [2209.02446](https://arxiv.org/abs/2209.02446) [cs].
- [30] *Smart Contract Weakness Classification (SWC)*. URL: <https://swcregistry.io/>.
- [31] Chainalysis Team. *\$2.2 Billion Stolen in Crypto in 2024 but Hacked Volumes Stagnate*. Dec. 2024. URL: <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/>.
- [32] Deepak K. Tosh et al. “Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack”. In: *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CC-GRID)*. Madrid, Spain: IEEE, May 2017, pp. 458–467. ISBN: 978-1-5090-6611-7. DOI: [10.1109/CCGRID.2017.111](https://doi.org/10.1109/CCGRID.2017.111).
- [33] *Uvicorn*. URL: <https://www.uvicorn.org/>.
- [34] Xianhua Wei, Aiya Li, and Zhou He. “Impacts of Consensus Protocols and Trade Network Topologies on Blockchain System Performance”. In: *Journal of Artificial Societies and Social Simulation* 23.3 (2020), p. 2. ISSN: 1460-7425. DOI: [10.18564/jasss.4289](https://doi.org/10.18564/jasss.4289).
- [35] *What Is Docker?* URL: <https://docs.docker.com/get-started/docker-overview/>.
- [36] Xinle Yang, Yang Chen, and Xiaohu Chen. “Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information”. In: *2019 IEEE International Conference on Blockchain (Blockchain)*. Atlanta, GA, USA: IEEE, July 2019, pp. 261–265. ISBN: 978-1-7281-4693-5. DOI: [10.1109/Blockchain.2019.00041](https://doi.org/10.1109/Blockchain.2019.00041).

