

---

**SCHOOL OF ARCHITECTURE, COMPUTING  
& ENGINEERING**

**MSc Information Security & Digital Forensics**

**Μεταπτυχιακή Διατριβή με τίτλο:**

Έρευνα για τη συνέργεια ιδιωτικών Blockchain και  
εφαρμογών Chain of Custody στην ηλεκτρονική  
εγκληματολογία: Ανάπτυξη ιδιωτικού Ethereum Blockchain  
και εφαρμογής Chain of Custody

**ΕΠΙΜΕΛΕΙΑ ΕΡΓΑΣΙΑΣ**

**ΜΠΑΝΤΗΣ ΧΡΗΣΤΟΣ**

**U2121211**

**ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ**

**Δρ. ΛΙΑΜΠΑΣ ΧΡΗΣΤΟΣ**

**ΙΔΡΥΜΑ**

**ΜΗΤΡΟΠΟΛΙΤΙΚΟ ΚΟΛΛΕΓΙΟ CAMPUS  
ΑΜΑΡΟΥΣΙΟΥ**

*Aύγουστος, 2023*

## Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες προς όλους όσους συνέβαλαν στην ολοκλήρωση αυτής της μεταπυχιακής διατριβής. Το ταξίδι της έρευνας και της δημιουργίας αυτού του έργου ήταν σημαντικό και χωρίς την υποστήριξη και τη βοήθεια των ακόλουθων ατόμων, αυτό το επίτευγμα δεν θα ήταν δυνατό.

Ευχαριστώ θερμά τον επιβλέποντα καθηγητή μου, κ. Λιάμπα Χρήστο, για τη συνεπή καθοδήγηση, εμπιστοσύνη και κίνητρό του καθ' όλη τη διάρκεια αυτής της διπλωματικής εργασίας. Οι ανεκτίμητες γνώσεις σας και η εποικοδομητική κριτική σας έχουν εμπλουτίσει σημαντικά τη δομή και το βάθος αυτής της μελέτης.

Τέλος, θα ήθελα να εκφράσω τις ευγνώμονες ευχαριστίες μου προς την οικογένειά μου και τους φίλους που με υποστήριξαν και με ενθάρρυναν κατά τη διάρκεια αυτής της πορείας.

## Περίληψη

---

Η ταχέως εξελισσόμενη φύση της τεχνολογίας και η ευρεία διάδοση ψηφιακών αποδεικτικών στοιχείων έχουν προκαλέσει μια επιτακτική ανάγκη για την εντατική αναθεώρηση και ισχυροποίηση των ψηφιακών εγκληματολογικών πρακτικών. Οι εξελίξεις στο τοπίο της Πληροφορικής τις τελευταίες δύο δεκαετίες έχουν καταστήσει τη συλλογή, διατήρηση και ανάλυση ψηφιακών αποδεικτικών στοιχείων ένα πολύτιμο εργαλείο για την επίλυση υποθέσεων και την απονομή δικαιοσύνης στα εμπλεκόμενα μέρη. Ως εκ τούτου, η προστασία αυτών των αποδεικτικών στοιχείων από οποιαδήποτε μορφή αλλοίωσης είναι υψίστης σημασίας. Σε αυτό το πλαίσιο, η ενσωμάτωση ιδιωτικών αλυσίδων συστοιχιών (εφεξής «blockchain») και εφαρμογών αλυσίδας επιτήρησης (εφεξής «chain of custody») αποτελεί μια πολλά υποσχόμενη οδό για την αντιμετώπιση των προκλήσεων που σχετίζονται με τη διατήρηση της ακεραιότητας και της αυθεντικότητας των ψηφιακών αποδεικτικών στοιχείων.

Ένα blockchain είναι ένα ψηφιακά κατανεμημένο καθολικό συναλλαγών που υπογράφεται μέσω μιας κρυπτογραφικής συνάρτησης με χρονολογική σειρά, το περιεχόμενό του ταξινομείται σε «block» και χαρακτηρίζεται από τη διαφάνεια που παρέχει σε όλους τους συμμετέχοντες του δικτύου (Sathyaprakasan et al., 2021). Αξιοποιώντας επομένως, την προαναφερθείσα διαφάνεια, αλλά και την εγγενή ασφάλεια που προσφέρει και αξιοποιώντας το «Ethereum» blockchain ως την θεμελιώδη πλατφόρμα ανάπτυξης, σχεδιάστηκε και αναπτύχθηκε ένα ιδιωτικό δίκτυο blockchain, με στόχο την ικανοποίηση των ιδιαίτερων απαιτήσεων των ψηφιακών εγκληματολογικών ερευνών. Πιο συγκεκριμένα, το ιδιωτικό δίκτυο παρέχει μια αποκεντρωμένη πλατφόρμα για τους συμμετέχοντες, οι οποίοι έχουν τη δυνατότητα να καταγράφουν, να επαληθεύουν και να παρακολουθούν με ασφάλεια τις κινήσεις των στοιχείων των εγκληματολογικών ερευνών. Η υλοποίηση αυτή αποσκοπεί στην εξασφάλιση ενισχυμένου απορρήτου, ελέγχου πρόσβασης και επεκτασιμότητας, διασφαλίζοντας παράλληλα, ένα υψηλό επίπεδο ακεραιότητας δεδομένων.

Ταυτόχρονα, αναπτύχθηκε μια αποκεντρωμένη εφαρμογή (Decentralized Application) chain of custody, με στόχο την ασφαλή καταγραφή της κίνησης και της διαχείρισης των ψηφιακών αποδεικτικών στοιχείων. Η εφαρμογή αξιοποιεί πλήρως τις δυνατότητες του ιδιωτικού blockchain, επιτρέποντας στους εξουσιοδοτημένους χρήστες να έχουν εύκολη πρόσβαση – σε πραγματικό χρόνο – σε πληροφορίες σχετικά με την ιδιοκτησία των πειστηρίων, το ιστορικό μεταφοράς και την ακεραιότητα τους,

μειώνοντας κινδύνους, όπως η αλλοίωση των αποδεικτικών στοιχείων και η μη εξουσιοδοτημένη πρόσβαση.

### **Λέξεις – Κλειδιά**

Ψηφιακά Αποδεικτικά Στοιχεία, Blockchain, Chain of Custody, Ethereum, Ιδιωτικό Δίκτυο, Αποκεντρωμένη Εφαρμογή

## Abstract

---

The rapidly evolving nature of technology and the widespread dissemination of digital evidence have created an urgent need to intensively review and strengthen digital forensic practices. Developments in the IT landscape over the past two decades have made the collection, preservation and analysis of digital evidence a valuable tool for resolving cases and administering justice to the parties involved. Therefore, protecting this evidence from any form of tampering is of paramount importance. In this context, the integration of private blockchains and chain of custody applications is a promising avenue to address the challenges related to maintaining the integrity and authenticity of digital evidence.

A blockchain is a digitally distributed ledger of transactions signed through a cryptographic function in chronological order. Its content is classified into a block and is characterized by the transparency it provides to all participants of the network (Sathyaprakasan et al., 2021). Therefore, taking advantage of the aforementioned transparency, but also the inherent security it offers and utilizing the "Ethereum" blockchain as the fundamental development platform, a private blockchain network was designed and developed, aiming to meet the particular requirements of digital forensic investigations. More specifically, the private network provides a decentralized platform for participants, who have the ability to securely record, verify and monitor the traffic of forensic investigations. This implementation aims to ensure enhanced privacy, access control and scalability, while ensuring a high level of data integrity.

At the same time, a decentralized chain of custody application was developed, aiming at the secure recording of traffic and management of digital evidence. The application takes full advantage of the capabilities of the private blockchain, allowing authorized users to easily access – in real time – information about the ownership of evidence, its transfer history and its integrity, reducing risks such as tampering with evidence and unauthorized access.

## Keywords

Digital Evidence, Blockchain, Chain of Custody, Ethereum, Private Network, Decentralized Application

## Πίνακας Περιεχομένων

---

<b>Ευχαριστίες .....</b>	<b>1</b>
<b>Περίληψη.....</b>	<b>2</b>
<b>Abstract.....</b>	<b>4</b>
<b>Πίνακας Περιεχομένων.....</b>	<b>5</b>
<b>Κατάλογος Εικόνων .....</b>	<b>7</b>
<b>Κατάλογος Πινάκων.....</b>	<b>11</b>
<b>Κεφάλαιο 1: Εισαγωγή.....</b>	<b>12</b>
<b>1.1. Ερευνητικό πλαίσιο.....</b>	<b>12</b>
<b>1.2. Υφιστάμενο Πρόβλημα .....</b>	<b>13</b>
<b>1.3. Στόχοι της εργασίας .....</b>	<b>14</b>
<b>Κεφάλαιο 2: To Blockchain .....</b>	<b>16</b>
<b>2.1. Δομή και είδη Blockchain.....</b>	<b>17</b>
<b>2.2. Ethereum Blockchain .....</b>	<b>23</b>
<b>2.3. Έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές.....</b>	<b>25</b>
<b>Κεφάλαιο 3: Ψηφιακή εγκληματολογία.....</b>	<b>28</b>
<b>3.1. Ιστορία της εγκληματολογίας .....</b>	<b>29</b>
<b>3.2. Μορφές και στόχος της ψηφιακής εγκληματολογίας .....</b>	<b>31</b>
<b>Κεφάλαιο 4: To Blockchain στην Ψηφιακή Εγκληματολογία.....</b>	<b>34</b>
<b>4.1. Κατανόηση της συνέργειας των ιδιωτικών Blockchain και των εφαρμογών Chain of Custody .....</b>	<b>35</b>
<b>4.2. Βιβλιογραφική Ανασκόπηση .....</b>	<b>38</b>
<b>Κεφάλαιο 5: Μεθοδολογία .....</b>	<b>40</b>
<b>5.1. Μοντελοποίηση .....</b>	<b>56</b>
<b>5.2. Σχεδιασμός.....</b>	<b>61</b>
<b>Κεφάλαιο 6: Ανάπτυξη του ιδιωτικού Ethereum Blockchain .....</b>	<b>66</b>
<b>6.1. Διαμόρφωση του δικτύου .....</b>	<b>68</b>

<b>Κεφάλαιο 7: Ανάπτυξη της εφαρμογής <i>Chain of Custody</i> .....</b>	<b>89</b>
7.1. Ανάλυση δομής .....	90
7.2. Τεχνικά μέρη .....	94
7.2.1. Οδηγός εγκατάστασης απαραίτητων εφαρμογών (Windows).....	96
7.3. Περιγραφή περίπτωσης χρήσης .....	109
7.4. Διαδικασία δοκιμών (Testing) .....	129
<b>Κεφάλαιο 8: Συμπεράσματα.....</b>	<b>145</b>
8.1. Μελλοντικές ενέργειες.....	146
<b>Κεφάλαιο 9: Παράρτημα.....</b>	<b>148</b>
9.1. Χρονοπρογραμματισμός έργου .....	148
9.2. Βιβλιογραφικές αναφορές .....	149
9.3. Γλωσσάριο απόδοσης ξενόγλωσσων όρων .....	153
9.4. Αρχείο genesis.json.....	155
9.5. Αρχείο static-nodes.json .....	156
9.6. Αρχείο geth.service.....	156
9.7. Αρχείο nodeθaccount.json .....	157
9.8. Κώδικας έξυπνων συμβολαίων .....	157
9.8.1. Έξυπνο συμβόλαιο Issued.sol .....	158
9.8.2. Έξυπνο συμβόλαιο Investigator.sol .....	159
9.8.3. Έξυπνο συμβόλαιο Case.sol .....	162
9.8.4. Έξυπνο συμβόλαιο Evidence.sol.....	168

## Κατάλογος Εικόνων

---

Εικόνα 1 - Σύνδεση των block σε ένα blockchain .....	17
Εικόνα 2 - Τρόπος σύνδεσης του genesis block με τα υπόλοιπα block (Oliveira et al., 2019) .....	18
Εικόνα 3 - Τρόπος λειτουργίας ενός αλγορίθμου κατακερματισμού (SHA-256) (Anand, 2020) .....	19
Εικόνα 4 - Αναπαράσταση ενός κατανεμημένου καθολικού (Majumder, 2022) .....	21
Εικόνα 5 - To Ethereum Virtual Machine (EVM) (coin98.net, 2022) .....	24
Εικόνα 6 - Παράδειγμα κώδικα σε γλώσσα προγραμματισμού «Solidity» .....	25
Εικόνα 7 - Σύγκριση κεντρικών και αποκεντρωμένων εφαρμογών (Goldmann, 2019)	
.....	27
Εικόνα 8 - Η τριάδα ασφαλείας «CIA» (Oliveira et al., 2020).....	35
Εικόνα 9 - Διαγράμματα περίπτωσης χρήσης δημιουργίας («ανοίγματος») μιας νέας υπόθεσης .....	43
Εικόνα 10 - Διαγράμματα περίπτωσης χρήσης διαχείρισης αποδεικτικών στοιχείων.	44
Εικόνα 11 - User Story Map (1/2).....	50
Εικόνα 12 - User Story Map (2/2) .....	50
Εικόνα 13 - Διάγραμμα Κλάσης (Class Diagram) .....	57
Εικόνα 14 - Διάγραμμα Αντικειμένου (Object Diagram) .....	57
Εικόνα 15 - Διάγραμμα Ροής δημιουργίας νέας υπόθεσης (Open new case Flowchart)	
.....	58
Εικόνα 16 - Διάγραμμα Ροής καταχώρισης νέου ερευνητή (Add new investigator Flowchart) .....	59
Εικόνα 17 - Διάγραμμα Ροής προσθήκης αποδεικτικού στοιχείου (Add evidence Flowchart) .....	59
Εικόνα 18 - Διάγραμμα Δραστηριότητας διαχείρισης υποθέσεων (Manage cases Activity Diagram) .....	60
Εικόνα 19 - Διάγραμμα Ακολουθίας προβολής ενεργών υποθέσεων (Active cases Sequence Diagram) .....	61
Εικόνα 20 – Προσχέδιο περιβάλλοντος χρήστη «Αναζήτηση αποδεικτικού στοιχείου» (Track Evidence Mockup) .....	62
Εικόνα 21 - Προσχέδιο περιβάλλοντος χρήστη «Δημιουργία νέας υπόθεσης» (Open a new Case Mockup) .....	63

Εικόνα 22 - Προσχέδιο περιβάλλοντος χρήστη «Διαχείριση υποθέσεων» (Manage Cases Mockup).....	64
Εικόνα 23 - Προσχέδιο περιβάλλοντος χρήστη «Προφίλ ερευνητή» (Investigator 's Profile Mockup) .....	64
Εικόνα 24 - Μακέτα περίπτωσης χρήσης «Προβολή του Chain of Custody ενός αποδεικτικού στοιχείου» (View Chain of Custody Wireframe) .....	65
Εικόνα 25 - Απλουστευμένη αρχιτεκτονική του δικτύου «ThemisChain».....	67
Εικόνα 26 - Δημιουργία λογαριασμού στο «AWS».....	68
Εικόνα 27 - Κουμπί δημιουργίας εικονικής μηχανής .....	69
Εικόνα 28 - Επιλογή δημιουργίας ενός «Key pair» .....	69
Εικόνα 29 - Φόρμα δημιουργίας ενός «Key pair» .....	70
Εικόνα 30 - Φόρμα δημιουργίας εικονικής μηχανής .....	71
Εικόνα 31 - Κανόνες του «Security Group» (1/2) .....	72
Εικόνα 32 - Κανόνες του «Security Group» (2/2) .....	73
Εικόνα 33 - Επιλογή χωρητικότητας εικονικής μηχανής.....	74
Εικόνα 34 - Τοποθεσία συνδέσμου «Elastic IPs» .....	75
Εικόνα 35 - Τα κουμπιά «Allocate Elastic Ip address» και «Associate this Elastic IP address».....	75
Εικόνα 36 - Η φόρμα ανάθεσης της «Elastic IP» διεύθυνσης .....	75
Εικόνα 37 - Η τελική μορφή της εικονικής μηχανής .....	76
Εικόνα 38 - Οδηγίες σύνδεσης με την εικονική μηχανή .....	76
Εικόνα 39 - Σύνδεση με την εικονική μηχανή μέσω τερματικού (1/2) .....	77
Εικόνα 40 - Σύνδεση με την εικονική μηχανή μέσω τερματικού (2/2) .....	77
Εικόνα 41 - Μεταφόρτωση του συμπιεσμένου αρχείου του Geth στην εικονική μηχανή .....	78
Εικόνα 42 - Η εντολή «geth version» .....	79
Εικόνα 43 - Βήματα δημιουργίας λογαριασμό κόμβου στο «geth» (1/2).....	80
Εικόνα 44 - Βήματα δημιουργίας λογαριασμό κόμβου στο «geth» (2/2).....	80
Εικόνα 45 - Το εργαλείο «puppeteth».....	81
Εικόνα 46 - Βήματα δημιουργίας του αρχείου «genesis» .....	82
Εικόνα 47 - Εξαγωγή των παραγόμενων αρχείων από τη διαδικασία δημιουργίας του αρχείου «genesis» .....	82
Εικόνα 48 - Διαγραφή του αρχείου «themischain-harmony.json».....	83
Εικόνα 49 - Αρχικοποίηση του blockchain βάσει του αρχείου «genesis.json» .....	84

Εικόνα 50 – Το «Geth Javascript Console» .....	85
Εικόνα 51 - Η εντολή admin.addPeer() .....	85
Εικόνα 52 - Η εντολή «systemctl status geth.service» .....	86
Εικόνα 53 - Το αρχείο που περιέχει το ιδιωτικό κλειδί του λογαριασμού του κόμβου .....	87
Εικόνα 54 - Παράθυρο διαχείρισης λογαριασμών στο «Metamask» .....	88
Εικόνα 55 - Παράθυρο εισαγωγής λογαριασμού στο «Metamask» .....	88
Εικόνα 56 - Η αρχική σελίδα της εφαρμογής «Themis» .....	90
Εικόνα 57 - Απλουστευμένη αρχιτεκτονική της εφαρμογής «Themis» .....	94
Εικόνα 58 - Ιστότοπος λήψης του «Node.js» .....	96
Εικόνα 59 - Απαραίτητη επιλογή κατά την εγκατάσταση του «Node.js» .....	97
Εικόνα 60 - Παράθυρο εγκατάστασης πρόσθετων εργαλείων του «Node.js» (1/2)....	98
Εικόνα 61 - Παράθυρο εγκατάστασης πρόσθετων εργαλείων του «Node.js» (2/2)....	98
Εικόνα 62 - Ολοκλήρωση της εγκατάστασης των πρόσθετων εργαλείων του «Node.js» .....	99
Εικόνα 63 - Επίσημος ιστότοπος του «Metamask» .....	100
Εικόνα 64 - Το «Metamask» στο ηλεκτρονικό κατάστημα του «Google Chrome»..	100
Εικόνα 65 - Επιλογή δημιουργίας νέου λογαριασμού πορτοφολιού «Metamask»....	101
Εικόνα 66 - Εισαγωγή κωδικού πρόσβασης νέου λογαριασμού πορτοφολιού «Metamask».....	102
Εικόνα 67 - Ασφάλιση του λογαριασμού κάνοντας χρήση μιας μοναδικής μυστικής φράσης .....	103
Εικόνα 68 - Η επιλογή «Ρυθμίσεις» (Settings) του μενού του «Metamask».....	104
Εικόνα 69 - Το κουμπί «Προσθήκη δικτύου» .....	104
Εικόνα 70 - Η επιλογή «Προσθήκη δικτύου χειροκίνητα» .....	105
Εικόνα 71 - Τα στοιχεία του δικτύου «ThemisChain» .....	106
Εικόνα 72 - Ο λογαριασμός του πρώτου κόμβου και το υπόλοιπο του σε «ETH» ...	107
Εικόνα 73 - Ο φάκελος «Application_files (Install)».....	108
Εικόνα 74 - Εκτέλεση της εντολής «npm install» .....	108
Εικόνα 75 - Τα αποτελέσματα της εντολής «npm install».....	109
Εικόνα 76 - Εκτέλεση της εντολής «npm run dev» .....	110
Εικόνα 77 - Ενεργοποίηση του τοπικού διακομιστή του module «lite-server».....	111
Εικόνα 78 - Η σελίδα που περιέχει το προφίλ του ερευνητή - διαχειριστή.....	112
Εικόνα 79 - Η σελίδα «Add a new Investigator».....	113

Εικόνα 80 - Επιβεβαίωση του μηδενικού κόστους συναλλαγών εντός της εφαρμογής	114
Εικόνα 81 - Η σελίδα «Manage Investigators» (1/2).....	115
Εικόνα 82 - Η σελίδα «Manage Investigators» (2/2).....	116
Εικόνα 83 - Η σελίδα «Open a new case» (1/2) .....	117
Εικόνα 84 - Η σελίδα «Open a new case» (2/2) .....	118
Εικόνα 85 - Η σελίδα «Active Cases» .....	119
Εικόνα 86 - Προβολή περιγραφής υπόθεσης.....	120
Εικόνα 87 - Η σελίδα «Manage Cases» (1/2) .....	121
Εικόνα 88 - Η σελίδα «Manage Cases» (2/2) .....	122
Εικόνα 89 - Προσθήκη επιπλέον ερευνητή στην υπόθεση .....	123
Εικόνα 90 - Το αποτέλεσμα της προσθήκης νέου ερευνητή στην υπόθεση .....	123
Εικόνα 91 - Η σελίδα «Add Case Evidence».....	124
Εικόνα 92 - Η σελίδα «Track Evidence» .....	125
Εικόνα 93 – Οι πλήρεις πληροφορίες του αποδεικτικού στοιχείου .....	126
Εικόνα 94 - Φόρμα μεταβίβασης κυριότητας αποδεικτικού στοιχείου .....	127
Εικόνα 95 - Το αποτέλεσμα της μεταβίβασης κυριότητας αποδεικτικού στοιχείου..	127
Εικόνα 96 – To chain of custody του αποδεικτικού στοιχείου .....	128
Εικόνα 97 - Η λίστα των επιτυχών «Unit Test» της εφαρμογής.....	131
Εικόνα 98 – Η εμφάνιση της σελίδας του προφίλ του ερευνητή σε συσκευή «iPhone 13» (smartphone) (Εργαλεία για προγραμματιστές - Google Chrome).....	138
Εικόνα 99 - Η εμφάνιση της σελίδας του προφίλ του ερευνητή σε συσκευή «iPad Air» (tablet) (Εργαλεία για προγραμματιστές - Google Chrome) .....	139
Εικόνα 100 - Η εμφάνιση της σελίδας «Add Case Evidence» στον περιηγητή ιστού «Google Chrome» .....	140
Εικόνα 101 - Η εμφάνιση της σελίδας «Add Case Evidence» στον περιηγητή ιστού «Safari».....	141
Εικόνα 102 - Διάγραμμα Gantt .....	148

## Κατάλογος Πινάκων

---

Πίνακας 1 - Τα σημαντικότερα γεγονότα στην ιστορίας της εγκληματολογίας (Prasad and Pandey, 2016).....	31
Πίνακας 2 - Αναφορά ιδιοκτήτη έργου .....	40
Πίνακας 3 - Αναφορά του Scrum Master.....	41
Πίνακας 4 - Αναφορά ομάδας Scrum.....	41
Πίνακας 5 - Ιεράρχηση περιπτώσεων χρήσης (Use Case Prioritization).....	46
Πίνακας 6 - Αναφορά των «Epics» .....	49
Πίνακας 7 - Ιεράρχηση ιστοριών χρήστη (User Stories Prioritization) .....	54
Πίνακας 8 - Παραδοτέα έργου (Project Deliverables).....	55
Πίνακας 9 - Κυκλοφορίες - Εκδόσεις έργου (Project Releases).....	56

## Κεφάλαιο 1: Εισαγωγή

---

### 1.1. Ερευνητικό πλαίσιο

Ο τομέας της ψηφιακής εγκληματολογίας έχει γνωρίσει αξιοσημείωτη ανάπτυξη και προβολή τα τελευταία χρόνια, που αποδίδεται σε μεγάλο βαθμό στις ταχείες εξελίξεις στην τεχνολογία και στην ευρεία χρήση ηλεκτρονικών συσκευών σε διάφορες πτυχές της σύγχρονης ζωής. Η ολοένα και μεγαλύτερη εξάρτηση των νομικών διαδικασιών από τα ψηφιακά αποδεικτικά στοιχεία και το συνεχώς διευρυνόμενο φάσμα εγκλημάτων στον κυβερνοχώρο, οδηγούν σε νέες προκλήσεις και πολυπλοκότητες για τους ερευνητές ψηφιακής εγκληματολογίας. Οι παραδοσιακές μέθοδοι χειρισμού ψηφιακών αποδεικτικών στοιχείων αντιμετωπίζουν συχνά περιορισμούς αναφορικά με τη διασφάλιση της ακεραιότητας, της επαληθευσιμότητας και της ιχνηλασιμότητας των δεδομένων, εγείροντας ανησυχίες σχετικά με την αξιοπιστία των ευρημάτων που παρουσιάζονται στο δικαστήριο.

Στην ψηφιακή εγκληματολογία, τα αποδεικτικά στοιχεία ακολουθούν μια ιεραρχία, περνώντας από διάφορα επίπεδα, ξεκινώντας από τον πρώτο ανταποκριτή και φτάνοντας στις ανώτερες αρχές που είναι υπεύθυνες για τη διαχείριση της διερεύνησης εγκλημάτων στον κυβερνοχώρο. Κατά τη διάρκεια αυτής της διαβίβασης των ψηφιακών αποδεικτικών στοιχείων, υπάρχει πάντα υψηλός κίνδυνος παραβίασης της ακεραιότητάς τους, καθιστώντας τα εγγενώς ευάλωτα σε διάφορα περιστατικά παραβίασης και πλαστογραφίας. Η παρουσία τέτοιων περιστατικών οφείλεται συνήθως στη συνεχή τεχνολογική εξέλιξη και την έλλειψη γνώσης και εμπειρογνωμοσύνης σε επίπεδο ερευνητών όπου, κατά την διαδικασία της διερεύνησης μιας συγκεκριμένης υπόθεσης κυβερνοεγκλήματος, πραγματοποιείται συλλογή, αποθήκευση και ανάλυση των ψηφιακών εγκληματολογικών στοιχείων (Lone and Mir, 2019).

Στον τομέα της ψηφιακής εγκληματολογίας, η διασφάλιση της ακεραιότητας και της γνησιότητας των αποδεικτικών στοιχείων είναι ζωτικής σημασίας για τις ερευνητικές και τις νομικές διαδικασίες. Σε νομικό πλαίσιο, η εξακρίβωση της γνησιότητας περιλαμβάνει την απόδειξη πως τα ψηφιακά αποδεικτικά στοιχεία προέρχονται από την υποτιθέμενη πηγή τους, δεν έχουν υποστεί αλλοιώσεις από τότε που αποκτήθηκαν, και οι σχετικές λεπτομέρειες, όπως η εμφανής ημερομηνία του αρχείου, είναι ακριβείς (Ćosić and Bača, 2010). Η διατήρηση των πληροφοριών προέλευσης των ψηφιακών αποδεικτικών στοιχείων αποτελεί μια ιδιαίτερα προκλητική διαδικασία, δεδομένης της ευκολίας με την οποία μπορούν να αντιγραφούν, να

τροποποιηθούν ή να καταστραφούν, καθώς ο αριθμός των μερών που μπορούν να τα επεξεργαστούν, αυξάνει τον κίνδυνο αλλοίωσης, είτε εκούσιας είτε ακούσιας.

Τη λύση στο παραπάνω πρόβλημα δίνει η διατήρηση ενός ισχυρού chain of custody, το οποίο καταγράφει το χρονολογικό ιστορικό και τον έλεγχο των αποδεικτικών στοιχείων, από τη στιγμή της απόκτησής τους μέχρι την παρουσίασή τους στο δικαστήριο (Giova, 2011). Ένα chain of custody περιλαμβάνει λεπτομέρειες σχετικά με το ποιος επεξεργάστηκε τα ψηφιακά αποδεικτικά στοιχεία, πότε, πού, πώς και συνήθως παρέχει έναν τρόπο επαλήθευσης της ακεραιότητάς τους. Ο συνηθέστερος τρόπος επαλήθευσης της ακεραιότητας των ψηφιακών αποδεικτικών στοιχείων είναι η χρήση μιας κρυπτογραφικής συνάρτησης κατακερματισμού (cryptographic hashing function), που επιτρέπει στον ενδιαφερόμενο να επαληθεύσει ότι τα αποδεικτικά στοιχεία δεν έχουν υποστεί οποιαδήποτε παραποίηση ή επεξεργασία μετά τη λήψη τους (Rasjid et al., 2017).

## 1.2. Υφιστάμενο Πρόβλημα

Οι παραδοσιακές μέθοδοι διατήρησης ενός chain of custody είναι επιρρεπείς σε προκλήσεις όπως η αλλοίωση δεδομένων, η έλλειψη διαφάνειας και η εξάρτηση από μία ή περισσότερες κεντρικές αρχές. Τα συστήματα βάσεων δεδομένων, που εμπλέκονται σε αυτές τις μεθόδους, δεν μπορούν επίσης να διατηρήσουν την ακεραιότητα, την πρωτοτυπία και την εμπιστευτικότητα των συλλεγόμενων αποδεικτικών στοιχείων, όπως επίσης και το ιστορικό των γεγονότων που συνέβησαν σε μια συγκεκριμένη σειρά κατά τη συλλογή, μεταφορά, αποθήκευση, ανάλυση και ερμηνεία των αποδεικτικών στοιχείων για την επίλυση μιας υπόθεσης (Rochmadi and Heksaputra, 2019).

Για να αντιμετωπίσουν αυτές τις προκλήσεις, πλήθος ερευνητών και επαγγελματιών έχουν στραφεί στην τεχνολογία του blockchain ως μια πολλά υποσχόμενη λύση. Το blockchain, ως κατανεμημένο καθολικό, παρέχει πολλαπλά οφέλη που το καθιστούν ιδανικό για τη διασφάλιση της ακεραιότητας και της διαφάνειας ενός chain of custody, αφού από το σχεδιασμό του, εγγυάται τη διαφάνεια, την αυθεντικότητα, την ασφάλεια και την ελεγξιμότητα, προσφέροντας τη δυνατότητα δημιουργίας ενός αμετάβλητου αρχείου όλων των ενεργειών και των κινήσεων που σχετίζονται με τα ψηφιακά αποδεικτικά στοιχεία. (Xu, Chen and Kou, 2019).

Αξιοποιώντας την τεχνολογία του blockchain, κάθε ενέργεια που πραγματοποιείται από έναν εγκληματολογικό ερευνητή κατά την επεξεργασία ψηφιακών αποδεικτικών στοιχείων, μπορεί να καταγραφεί και να αποθηκευτεί με ασφάλεια. Αυτό δημιουργεί μια σαφή και μόνιμη διαδρομή ελέγχου (audit trail), όπου κάθε προσπάθεια μεταφοράς και πρόσβασης σε δεδομένα καταγράφεται με αυτοματοποιημένο τρόπο, χάρη στα «έξυπνα» συμβόλαια (Guo et al., 2022). Αυτά τα «έξυπνα» συμβόλαια, που αναπτύσσονται και εκτελούνται σε πλατφόρμες blockchain όπως το Ethereum, διασφαλίζουν ότι το chain of custody διατηρείται και επιβάλλεται σύμφωνα με προκαθορισμένους κανόνες και πρωτόκολλα.

Η χρήση της τεχνολογίας του blockchain, σε συνδυασμό με το chain of custody, προσφέρει πολλά πλεονεκτήματα. Παρέχει ένα ασφαλές και αποκεντρωμένο μέσο παρακολούθησης της κίνησης και της διαχείρισης των ψηφιακών πειστηρίων, μειώνοντας τους κινδύνους παραποίησης δεδομένων και μη εξουσιοδοτημένης πρόσβασης. Επιπλέον, βελτιώνει τη διαφάνεια επιτρέποντας στα αρμόδια μέρη να εποπτεύουν και να επαληθεύουν εύκολα το ιστορικό των αποδεικτικών στοιχείων, μειώνοντας την ανάγκη εμπιστοσύνης προς τις κεντρικές αρχές.

Η παρούσα εργασία διερευνά τις συνδυασμένες δυνατότητες των ιδιωτικών blockchain και των εφαρμογών chain of custody στον τομέα της ψηφιακής εγκληματολογίας. Η μελέτη περιλαμβάνει μια ολοκληρωμένη έρευνα σχετικά με την τεχνολογία του blockchain, την ψηφιακή εγκληματολογία, την προσφορά των ιδιωτικών blockchain σε αυτήν, καθώς και τους τρόπους που μπορούν να συνεισφέρουν στη διατήρηση ενός chain of custody, οδηγώντας στην ανάπτυξη ενός ιδιωτικού blockchain βασιζόμενο στην πλατφόρμα του Ethereum και μιας αποκεντρωμένης εφαρμογής chain of custody.

### 1.3. Στόχοι της εργασίας

Το ταχέως εξελισσόμενο τοπίο της τεχνολογίας και η διάχυτη παρουσία ψηφιακών αποδεικτικών στοιχείων έχουν καταστήσει αναγκαία την εφαρμογή ισχυρών και ασφαλών μεθοδολογιών στον τομέα της ψηφιακής εγκληματολογίας. Καθώς ο όγκος και η πολυπλοκότητα των ψηφιακών δεδομένων συνεχίζουν να αυξάνονται, η ανάγκη για ενισχυμένη επαληθευσιμότητα, ιχνηλασιμότητα και ακεραιότητα των ψηφιακών αποδεικτικών στοιχείων έχει καταστεί πρωταρχικό μέλημα για τους εγκληματολογικούς ερευνητές και κατ' επέκταση, τις υπηρεσίες επιβολής του νόμου.

Η άνοδος της τεχνολογίας του blockchain, γνωστή για την ενισχυμένη προστασία της ιδιωτικής ζωής, την ακεραιότητα των δεδομένων και την - ανθεκτική στις παραβιάσεις - φύση της, σε συνδυασμό με την έννοια του chain of custody, η οποία διασφαλίζει την ασφαλή παρακολούθηση και διαχείριση ψηφιακών αποδεικτικών στοιχείων, παρουσιάζει μια πολλά υποσχόμενη οδό για την αντιμετώπιση των ελλείψεων των παραδοσιακών μεθόδων ψηφιακής εγκληματολογίας.

Ως απάντηση στις προαναφερθείσες προκλήσεις, η παρούσα διπλωματική εργασία, αξιοποιώντας την ευρωστία την τεχνολογίας του blockchain και πιο συγκεκριμένα, της πλατφόρμας blockchain «Ethereum», επιχειρεί να διερευνήσει τις πιθανές συνέργειες μεταξύ ιδιωτικών blockchain και εφαρμογών chain of custody, με στόχο την ανάπτυξη μιας καινοτόμου και αξιόπιστης λύσης για τις ψηφιακές εγκληματολογικές έρευνες. Η λύση αυτή περιλαμβάνει τη δημιουργία ενός ιδιωτικού blockchain, προσαρμοσμένο στις συγκεκριμένες απαιτήσεις των ψηφιακών εγκληματολογικών εφαρμογών, όπως και την ανάπτυξη μιας αποκεντρωμένης εφαρμογής chain of custody, σχεδιασμένη για την καταγραφή και την παρακολούθηση της κίνησης και της διαχείρισης ψηφιακών αποδεικτικών στοιχείων, καθ' όλη τη διάρκεια της διαδικασίας των ερευνών. Η ενσωμάτωση αυτών των δύο στοιχείων επιδιώκει να προσδώσει υψηλότερο βαθμό εμπιστοσύνης στα ψηφιακά εγκληματολογικά ευρήματα, ενισχύοντας το παραδεκτό και την αξιοπιστία των ψηφιακών αποδεικτικών στοιχείων σε νομικές διαδικασίες. Μέσω μιας εμπειρικής αξιολόγησης της αναπτυγμένης λύσης, η μελέτη αυτή στοχεύει να συμβάλει στην πρόοδο των πρακτικών ψηφιακής εγκληματολογίας, προάγοντας την εμπιστοσύνη και τη διαφάνεια στον συνεχώς εξελισσόμενο κόσμο της ψηφιακής τεχνολογίας.

## Κεφάλαιο 2: Το Blockchain

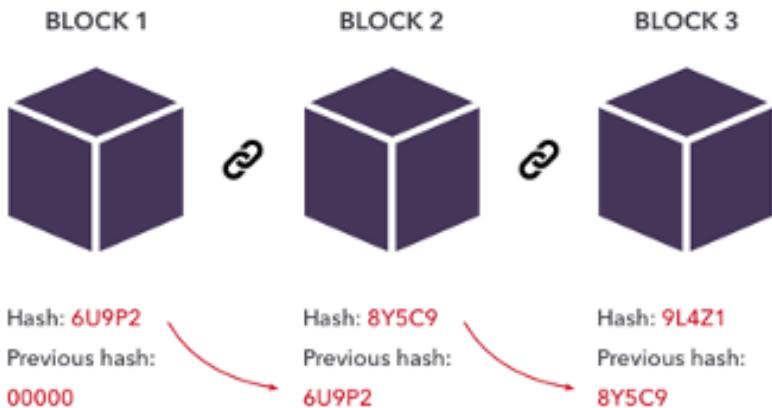
Το Blockchain είναι μια ταχέως αναπτυσσόμενη τεχνολογία κατανεμημένου καθολικού που έχει επεκταθεί από τις αρχικά αποκεντρωμένες οικονομικές συναλλαγές, σε περισσότερες εφαρμογές «πραγματικού κόσμου», όπως εμπόριο, υπηρεσίες εφοδιαστικής αλυσίδας, υπηρεσίες κατανομής πόρων, μεταφορά αγαθών, «IoT» κ.α. (Chen and Liang, 2022). Ακόμη, το blockchain έχει αρχίσει να έχει αντίκτυπο στο νομικό σύστημα και ιδιαίτερα στους κανόνες περί αποδείξεων. Αυτά τα σενάρια εφαρμογών έχουν φέρει νέες προκλήσεις στην αρχική τεχνολογία blockchain, ωθώντας τους προγραμματιστές και τους ερευνητές να διερευνούν συνεχώς καινοτόμες λύσεις για την αντιμετώπιση ζητημάτων επεκτασιμότητας, ασφάλειας, απορρήτου και διαλειτουργικότητας. Προκειμένου να πραγματοποιηθεί πλήρης κατανόηση της συγκεκριμένης αυτής τεχνολογίας, είναι απαραίτητο να παρατεθεί ο ορισμός της. Το blockchain μπορεί να οριστεί ως μια τεχνολογία κατανεμημένου καθολικού που μπορεί να καταγράφει μόνιμα και με ασφάλεια τις συναλλαγές μεταξύ των εκάστοτε μερών. Αυτό το αποκεντρωμένο καθολικό διατηρείται μέσω διαφόρων κόμβων που συνδέονται μεταξύ τους μέσω δικτύων, τα οποία είναι υπεύθυνα για την επικοινωνία και την καταγραφή των συναλλαγών (Umoren et al., 2022). Με την πάροδο των ετών η τεχνολογία του blockchain έχει εξελιχθεί και έχει ανοίξει το δρόμο για την ενσωμάτωση ή και τον συνδυασμό αποκεντρωμένων εφαρμογών με άλλες τεχνολογίες.

Με τις μεθόδους αποθήκευσης, ανταλλαγής και συγχρονισμού δεδομένων που χρησιμοποιούνται σε ένα δίκτυο απομακρυσμένων υπολογιστών, το αποκεντρωμένο και «μη αξιόπιστο» blockchain μπορεί να λύσει αποτελεσματικά τα προβλήματα απώλειας και πλαστογραφίας δεδομένων σε ένα κεντρικό σύστημα αποθήκευσης, μειώνοντας έτσι το κόστος διατήρησης των πληροφοριών και της εμπιστοσύνης και παρέχοντας μια πιο αξιόπιστη μέθοδο για τη δικαστική εξέταση των ηλεκτρονικών αποδεικτικών στοιχείων. Η τεχνολογία blockchain έχει φέρει επανάσταση στην ασφάλεια των δεδομένων με τον ασφαλή μηχανισμό αποθήκευσης που προσφέρει, ο οποίος περιλαμβάνει την καταγραφή συναλλαγών χρησιμοποιώντας αμετάβλητες κρυπτογραφικές υπογραφές (Umoren et al., 2022).

Με απλά λόγια, το blockchain είναι μια σειρά συνδεδεμένων δομών δεδομένων που ονομάζονται «μπλοκ» (block), τα οποία περιέχουν ή παρακολουθούν όλα όσα συμβαίνουν σε οποιαδήποτε κατανεμημένα (distributed) συστήματα σε ένα «peer to peer» δίκτυο. Κάθε μπλοκ συνδέεται με το προηγούμενο μέσω ενός ειδικού δείκτη που

ονομάζεται «δείκτης κατακερματισμού» (hash pointer), σχηματίζοντας μια αλυσίδα (Εικόνα 1), με αποτέλεσμα ένα σύστημα που τα δεδομένα του δεν επιδέχονται καμία επεξεργασία (Nakamoto, 2008).

Το Blockchain, εξ ορισμού, εγγυάται τη διαφάνεια, την αυθεντικότητα, την ασφάλεια και την ελεγξιμότητα των δεδομένων και, ως εκ τούτου, καθίσταται ως το πλέον κατάλληλο για τη διατήρηση των chain of custody των εγκληματολογικών ερευνών (Lone and Mir, 2019).



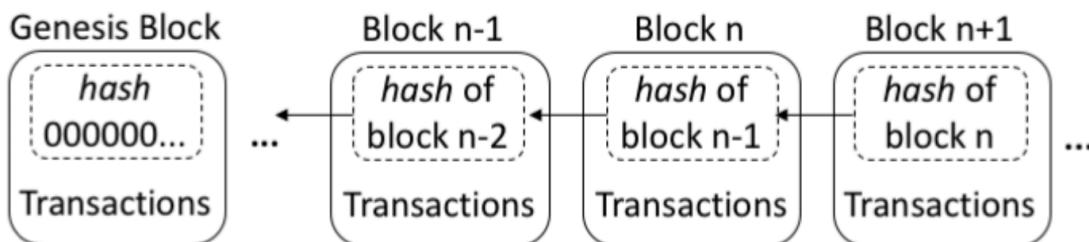
Εικόνα 1 - Σύνδεση των block σε ένα blockchain

## 2.1. Δομή και είδη Blockchain

Το blockchain είναι μια δομή δεδομένων που επιτρέπει τη δημιουργία ενός ψηφιακού καθολικού για την καταγραφή και την αποθήκευση συναλλαγών, τις οποίες μοιράζονται όλα τα συμμετέχοντα μέρη μέσω ενός κατανεμημένου δικτύου υπολογιστών, χρησιμοποιώντας την κρυπτογραφία για την προστασία τους, δημιουργώντας μια αδιάβλητη διαδρομή ελέγχου (audit trail) (Lone, 2017). Στον αντίποδα, τα υπάρχοντα συστήματα ακολουθούν την αρχιτεκτονική πελάτη-διακομιστή (client-server) και αποθηκεύουν τα δεδομένα τους εξ ολοκλήρου σε ένα σημείο-στόχο. Αποτέλεσμα αυτού είναι η δημιουργία ευπαθειών, οδηγώντας σε περιπτώσεις απώλειας δεδομένων, που και αυτές με την σειρά τους ενδέχεται να προκαλέσουν αστοχία ή κινδύνους κακόβουλης δραστηριότητας.

Ένα blockchain αποτελείται από πολλαπλά block και χρησιμοποιεί την συνάρτηση κατακερματισμού (hash) κάθε block για να το συνδέσει με το προηγούμενο. Έτσι, ένα block είναι σαν μια σελίδα ενός καθολικού ή ενός βιβλίου εγγραφών. Κάθε φορά που ένα block «ολοκληρώνεται», δίνει τη θέση του στο επόμενο block κ.ο.κ. Ένα

block είναι επομένως, μια μόνιμη τοποθεσία αποθήκευσης εγγραφών που, μόλις καταχωρηθούν, δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν. Αυτά τα block τοποθετούνται «το ένα πάνω στο άλλο», με το «Genesis» block να είναι το θεμέλιο. Το «Genesis» block, γνωστό και ως block 0, είναι το πρώτο block, βάσει του οποίου δημιουργούνται τα επιπλέον block σε ένα blockchain. Είναι ουσιαστικά ο «πρόγονος», στον οποίο κάθε άλλο block μπορεί να εντοπίσει τη καταγωγή του, αφού κάθε block αναφέρεται σε αυτό που προηγείται (Tardi, 2021) (Εικόνα 2).



Εικόνα 2 - Τρόπος σύνδεσης του genesis block με τα υπόλοιπα block (Oliveira et al., 2019)

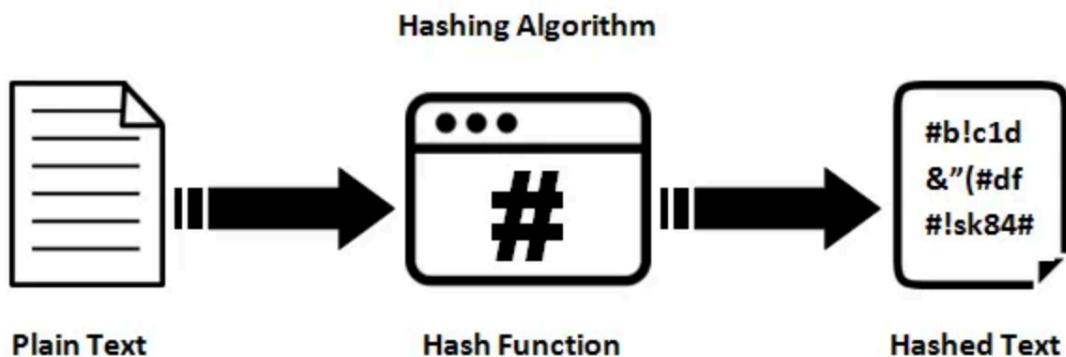
Στον πυρήνα του, ένα blockchain αποτελείται από τρία βασικά στοιχεία: τα block, στα οποία, όπως προαναφέρθηκε, αποθηκεύονται τα δεδομένα, την αλυσίδα (chain), η οποία συνδέει αυτά τα block μεταξύ τους μέσω της συνάρτησης κατακερματισμού (hash) και τον μηχανισμό συναίνεσης (consensus mechanism), που επιτρέπει σε πολλούς συμμετέχοντες να καταλήγουν σε συμφωνία σχετικά με την εγκυρότητα των νέων συναλλαγών και να διατηρούν την ακεραιότητα του δικτύου. Αναλυτικότερα, τα κύρια χαρακτηριστικά ενός blockchain είναι τα εξής:

- Κρυπτογραφική συνάρτηση κατακερματισμού (Cryptographic Hash Function)**

Οι συναρτήσεις κατακερματισμού είναι ένα από τα σημαντικότερα στοιχεία της τεχνολογίας του blockchain. Αποτελούν αλγορίθμους που χρησιμοποιούνται στην κρυπτογραφία για τη μετατροπή ήδη υπαρχόντων δεδομένων σε κρυπτογραφημένα δεδομένα σταθερού μήκους (Kahate, 2017) (Εικόνα 3). Οποιαδήποτε όμως, αλλαγή σε αυτά θα παράγει ένα αποτέλεσμα εντελώς διαφορετικό από το αρχικό.

Οι αλγόριθμοι κατακερματισμού όπως το «SHA-256» (Secure Hash Algorithm-256) ή το «Scrypt» χρησιμοποιούνται συνήθως από blockchain επειδή είναι εύκολο να ελεγχθούν, αλλά πραγματικά δύσκολο να πλαστογραφηθούν, επιτρέποντας έτσι τη δημιουργία ψηφιακών υπογραφών που χρειάζονται οι χρήστες των blockchain για να

πιστοποιήσουν τον εαυτό τους ή τις συναλλαγές τους (Fernandez-Carames and Fraga-Lamas, 2020). Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται επίσης από τα blockchain για τη σύνδεση των block τους. Τα block συνδέονται μεταξύ τους με χρονολογική σειρά, εμπειριέχοντας, το κάθε ένα από αυτά, το hash του προηγούμενου block.



Εικόνα 3 - Τρόπος λειτουργίας ενός αλγορίθμου κατακερματισμού (SHA-256) (Anand, 2020)

- **Ασύμμετρη κρυπτογράφηση / Κρυπτογράφηση δημοσίου κλειδιού (Asymmetric Cryptography / Public Key Cryptography)**

Ένα blockchain συνήθως, εκμεταλλεύεται την κρυπτογράφηση δημοσίου κλειδιού για τη διασφάλιση των συναλλαγών μεταξύ των μερών, ελέγχοντας τις συναλλαγές μέσω των ψηφιακών υπογραφών. Κάθε δημόσιο κλειδί συνοδεύεται από ένα ιδιωτικό κλειδί ενώ, η κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων πραγματοποιείται με τη χρήση αμφότερων. Έτσι, όταν ο αλγόριθμος, που είναι υπεύθυνος για την διαδικασία της υπογραφής, είναι ασφαλής, είναι αναμφισβήτητο ότι μόνο το άτομο με το συγκεκριμένο ιδιωτικό κλειδί θα μπορούσε να έχει δημιουργήσει την εν λόγω υπογραφή (Fernandez-Carames and Fraga-Lamas, 2020). Αυτή η μορφή κρυπτογραφίας δημιουργεί έναν παράγοντα εμπιστοσύνης μεταξύ των χρηστών, παρέχοντας έναν μηχανισμό που μπορεί να επικυρώσει την ακεραιότητα, καθώς και την αυθεντικότητα των δημόσιων συναλλαγών.

Η κρυπτογράφηση δημοσίου κλειδιού είναι επίσης απαραίτητη για τη λειτουργία των «πορτοφολιών». Σε ένα blockchain κάθε χρήστης έχει ένα πορτοφόλι που σχετίζεται με τουλάχιστον μια δημόσια διεύθυνση (συνήθως είναι το hash του δημόσιου κλειδιού του) και ένα ιδιωτικό κλειδί που χρειάζεται ο χρήστης για την υπογραφή των συναλλαγών (Fernandez-Carames and Fraga-Lamas, 2020).

- **Συναλλαγές (Transactions)**

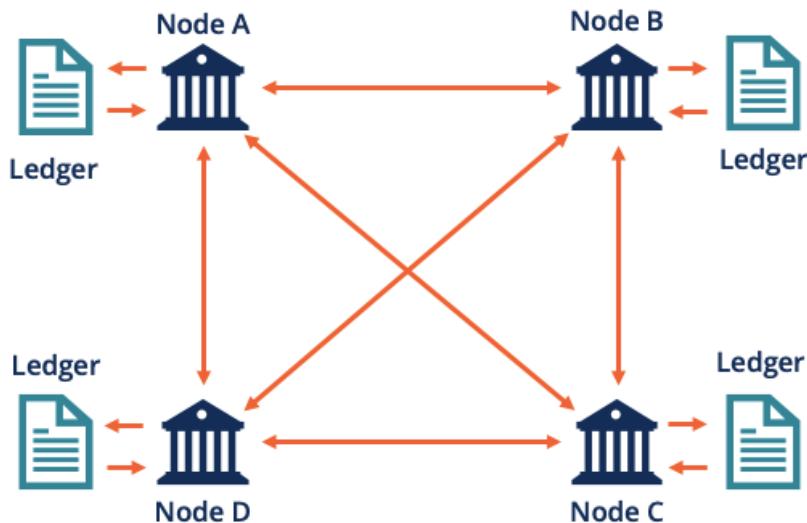
Ως συναλλαγή ορίζεται η αλληλεπίδραση μεταξύ δύο ατόμων, οργανισμών κ.λπ. Για παράδειγμα, η μεταφορά κρυπτονομισμάτων μεταξύ χρηστών «Bitcoin» αντιπροσωπεύει μια συναλλαγή (Kahate, 2017). Κάθε block μπορεί να περιέχει περισσότερες από μία ή ακόμη και μηδενικές συναλλαγές. Σε αρκετά blockchain, απαιτείται συνεχής δημιουργία νέων block, ανεξαρτήτως αν περιέχουν μηδενικές συναλλαγές, ώστε να διασφαλίζεται η προστασία του δικτύου από οποιαδήποτε αλλοίωση δύναται να προκαλέσουν τυχόν κακόβουλοι χρήστες.

- **Κατανεμημένο καθολικό (Distributed Ledger)**

Η τεχνολογία κατανεμημένου καθολικού αναφέρεται σε μια νέα και ταχέως εξελισσόμενη προσέγγιση για την καταγραφή και την ανταλλαγή δεδομένων σε πολλαπλούς χώρους αποθήκευσης (καθολικά), καθένας από τους οποίους έχει ακριβώς τα ίδια αρχεία και συντηρείται και ελέγχεται συλλογικά από ένα κατανεμημένο δίκτυο διακομιστών-υπολογιστών, οι οποίοι ονομάζονται «κόμβοι» (World Bank, 2017) (Εικόνα 4). Η τεχνολογία του blockchain, μία ιδιαίτερη μορφή τεχνολογίας κατανεμημένου καθολικού, χρησιμοποιεί κρυπτογραφικές και αλγορίθμικές μεθόδους για τη δημιουργία και την επαλήθευση μιας συνεχώς αναπτυσσόμενης δομής δεδομένων, η οποία λαμβάνει τη μορφή μιας αλυσίδας και λειτουργεί ως καθολικό.

Η διαδικασία της προσθήκης μιας εγγραφής στο blockchain ξεκινά από ένα από τα μέλη (κόμβους), το οποίο δημιουργεί ένα νέο block δεδομένων, που περιέχει το ιστορικό ορισμένων συναλλαγών. Στη συνέχεια, οι πληροφορίες σχετικά με αυτό το νέο block δεδομένων κοινοποιούνται σε ολόκληρο το δίκτυο, περιέχοντας κρυπτογραφημένα δεδομένα, ώστε να μην δημοσιοποιούνται τα στοιχεία της συναλλαγής και έπειτα, καθορίζεται η εγκυρότητα του block από τους συμμετέχοντες που διαθέτουν τα ανάλογα δικαιώματα, σύμφωνα με τον προκαθορισμένο μηχανισμό συναίνεσης. Μόνο μετά την επικύρωση, το σύνολο των συμμετεχόντων προσθέτει το νέο block στα αντίστοιχα καθολικά τους. Μέσω αυτού του μηχανισμού, κάθε αλλαγή στο καθολικό αναπαράγεται σε ολόκληρο το δίκτυο και κάθε μέλος του δικτύου διαθέτει ένα πλήρες, πανομοιότυπο αντίγραφο ολόκληρου του καθολικού ανά πάσα στιγμή (World Bank, 2017).

## Distributed Ledgers



Εικόνα 4 - Αναπαράσταση ενός κατανεμημένου καθολικού (Majumder, 2022)

- **Μηχανισμός συναίνεσης (Consensus Mechanism)**

Ένας κόμβος είναι μια υπολογιστική οντότητα ικανή να εκτελεί λειτουργίες στο blockchain. Αποτελεί συχνό φαινόμενο να πραγματοποιείται διάκριση μεταξύ των «κανονικών» κόμβων ενός blockchain, οι οποίοι αλληλεπιδρούν μόνο με το blockchain εκτελώντας συναλλαγές, και των «πλήρων» κόμβων, οι οποίοι διατηρούν ένα αντίγραφο του blockchain και συμβάλλουν σε αυτό επικυρώνοντας συναλλαγές. Ένας «miner» είναι ένας τρίτος τύπος κόμβου που υπάρχει σε πολλά blockchain, ο οποίος ακολουθώντας το εκάστοτε πρωτόκολλο συναίνεσης, συμβάλει στην επικύρωση των συναλλαγών (Wang et al., 2019). Καθώς η τεχνολογία του blockchain εξελίσσεται, παρουσιάζεται πληθώρα μηχανισμών συναίνεσης, ο καθένας αποβλέποντας και σε διαφορετικό σκοπό, με ορισμένους από τους πιο δημοφιλείς να είναι οι «Proof-of-Work (PoW)», «Proof-of-Stake (PoS)» και «Proof-of-Authority (PoA)»:

- **Proof-of-Work (PoW):** Είναι ο πρώτος μηχανισμός συναίνεσης που εφαρμόστηκε σε ένα δίκτυο blockchain. Στο πρωτόκολλο «PoW», οι «miners» ανταγωνίζονται μεταξύ τους εντός του δικτύου, με στόχο την επίλυση πολύπλοκων υπολογιστικών γρίφων. Όταν ένας «miner» βρει τη λύση του γρίφου, θα μεταδώσει το νέο-δημιουργηθέν block στο δίκτυο και στη συνέχεια, όλοι οι υπόλοιποι «miners» θα ελέγξουν τη λύση και θα επαληθεύσουν εάν είναι σωστή (Castor, 2017).

- **Proof-of-Stake (PoS):** Χρησιμοποιείται συνήθως αντί του πρωτοκόλλου «Proof-of-Work». Σε αυτό το πρωτόκολλο, ο ενδιαφερόμενος δύναται να επικυρώσει το block ανάλογα με τον αριθμό των κρυπτονομισμάτων που κατέχει. Όσο περισσότερα κρυπτονομίσματα έχει ένας επικυρωτής (validator) ή ένας «miner», τόσο περισσότερη «ισχύ» εξόρυξης και κατά συνέπεια πιθανότητες έχει ώστε να δημιουργήσει το block (Castor, 2017).
- **Proof-of-Authority (PoA):** Είναι ένας αλγόριθμος συναίνεσης που παρέχει μια αποτελεσματική λύση για ιδιωτικά blockchains. Ο όρος επινοήθηκε το 2017 από τον Gavin Wood, συνιδρυτή του blockchain «Ethereum». Η λειτουργία του αλγορίθμου βασίζεται στην εμπιστοσύνη προς την ταυτότητα του επικυρωτή (validator). Στο «Proof-of-Authority», οι κόμβοι αποκτούν το δικαίωμα δημιουργίας νέων block περνώντας μια αυστηρή διαδικασία ελέγχου, που υποβάλλεται από τους συντονιστές του συστήματος. Αυτοί οι συντονιστές είναι προεγκεκριμένοι συμμετέχοντες που ελέγχουν τα block και τις συναλλαγές. Ως αποτέλεσμα, τα «PoA» blockchains προστατεύονται μόνο από αξιόπιστους κόμβους επικύρωσης (Antolin, 2022).

Εν γένει, ένα blockchain μπορεί να είναι «ανοιχτό» (χωρίς άδεια) ή ελεγχόμενο (με άδεια), με θεμελιώδεις διαφορές να υφίστανται μεταξύ των δύο. Το «Bitcoin» και το «Ethereum» είναι τα πιο εξέχοντα παραδείγματα blockchain χωρίς άδεια, όπου οι συμμετέχοντες στο δίκτυο μπορούν να ενταχθούν ή να εγκαταλείψουν το δίκτυο κατά βιούληση, χωρίς να έχουν προεγκριθεί ή ελεγχθεί από κάποια οντότητα. Το μόνο που χρειάζεται για να συνδεθεί κάποιος στο δίκτυο και να προσθέσει συναλλαγές στο καθολικό είναι ένας υπολογιστής με το αντίστοιχο λογισμικό. Δεν υπάρχει κεντρικός ιδιοκτήτης, ενώ πανομοιότυπα αντίγραφα του καθολικού διανέμονται σε όλους τους συμμετέχοντες στο δίκτυο (World Bank, 2017).

Στα blockchain με άδεια τα μέλη προεπιλέγονται από τον κάτοχο ή τον διαχειριστή του blockchain, ο οποίος ελέγχει την πρόσβαση στο δίκτυο και ορίζει τους κανόνες του. Αυτό επιλύει μια σειρά ανησυχιών που έχουν οι κυβερνήσεις και οι ρυθμιστικές αρχές σχετικά με τα blockchain χωρίς άδεια, όπως είναι η επαλήθευση ταυτότητας των μελών του δικτύου και η καταγραφή της νόμιμης ιδιοκτησίας του καθολικού (World Bank, 2017). Στον αντίποδα, αναιρεί ένα βασικό πλεονέκτημα των blockchain χωρίς άδεια: την ικανότητα λειτουργίας χωρίς την ανάγκη οποιασδήποτε

μεμονωμένης οντότητας να διαδραματίζει συντονιστικό ρόλο, κάτι που απαιτεί αναγκαστικά από όλους τους συμμετέχοντες να εμπιστεύονται αυτήν την οντότητα.

Τα blockchain με άδεια, στα οποία η πρόσβαση στο δίκτυο είναι ρυθμιζόμενη, συνήθως δεν απαιτούν τον ενεργοβόρο αλγόριθμο συναίνεσης «Proof-of-Work» για την επαλήθευση των συναλλαγών, αλλά βασίζονται σε διαφορετικά πρωτόκολλα για τη δημιουργία συναίνεσης μεταξύ των μελών, όπως το «Proof-of-Authority». Στα blockchain χωρίς άδεια, τα οποία δεν ρυθμίζουν την πρόσβαση στο δίκτυο, δεν υπάρχει καμία απαίτηση εμπιστοσύνης μεταξύ των συμμετεχόντων και, ως εκ τούτου, χρησιμοποιείται ένας περίπλοκος αλγόριθμος «Proof-of-Work» για τη δημιουργία συναίνεσης ανάμεσα στους χρήστες (World Bank, 2017).

Στην πραγματικότητα, τα blockchain χωρίζονται σε τέσσερις (4) κατηγορίες: τα Δημόσια (Public), τα Ελεγχόμενα (Permissioned), τα Ιδιωτικά (Private) και τα Κοινοπραξίας (Consortium). Οι κατηγορίες αυτές μπορούν να διακριθούν σε «δημόσιο / ιδιωτικό» (όσον αφορά την πρόσβαση) και «ελεγχόμενο / χωρίς άδεια» (όσον αφορά τους ρόλους) blockchain. Το «Ripple», για παράδειγμα, είναι ένα ελεγχόμενο blockchain, αλλά τα δεδομένα επικυρώνονται από όλους τους συμμετέχοντες στο δίκτυο, επομένως το σύστημά τους μπορεί να χαρακτηριστεί ως «δημόσιο ελεγχόμενο» (World Bank, 2017). Από την άλλη, ένα ελεγχόμενο blockchain, όπου τα δεδομένα επικυρώνονται μόνο από ένα σύνολο συμμετεχόντων, θεωρείται «ιδιωτικό ελεγχόμενο». Τέλος, ένα blockchain κοινοπραξίας είναι ένας τύπος blockchain που συνδυάζει τα χαρακτηριστικά των δημόσιων και των ιδιωτικών blockchain. Χρησιμοποιείται συνήθως εντός εταιρειών ή ομίλων επιχειρήσεων, που μοιράζονται τον ίδιο στόχο ή σύνολο στόχων, οι οποίοι σχετίζονται με τη χρήση της τεχνολογίας του blockchain και συνεργάζονται για τη διαχείριση ενός κοινού δικτύου blockchain (Gondek, n.d.).

## 2.2. Ethereum Blockchain

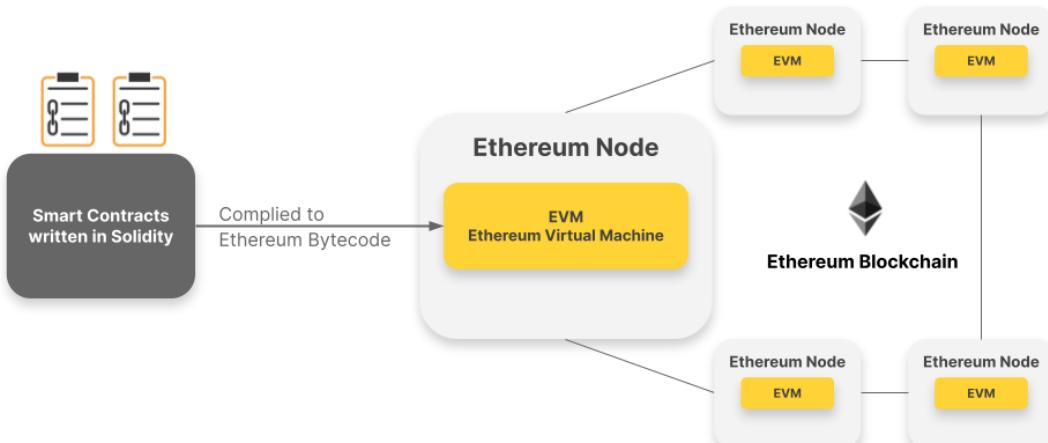
Το Ethereum, που ανακοινώθηκε το 2014 και κυκλοφόρησε το 2015, στοχεύει στη δημιουργία μιας καθολικής πλατφόρμας εφαρμογών που βασίζεται σε blockchain. Ενσωματώνει μια «Turing-Complete» γλώσσα προγραμματισμού (πλήρης γλώσσα που επιτρέπει στους προγραμματιστές να λύσουν οποιοδήποτε υπολογιστικό πρόβλημα), παρέχοντας στους χρήστες τη δυνατότητα να «γράφουν» «έξυπνα» συμβόλαια και

αποκεντρωμένες εφαρμογές, όπου καθορίζουν οι ίδιοι τους δικούς τους κανόνες αναφορικά με την ιδιοκτησία (Buterin, 2013).

To Ethereum είναι μια ανοιχτού κώδικα, αποκεντρωμένη υπολογιστική υποδομή, που συχνά περιγράφεται ως «ο παγκόσμιος υπολογιστής» (Antonopoulos and Wood, 2018), στην οποία εκτελούνται προγράμματα που ονομάζονται «έξυπνα συμβόλαια» (smart contracts). Χρησιμοποιεί ένα εγγενές κρυπτονόμισμα που ονομάζεται «Ether», ως μονάδα μέτρησης και περιορισμού του κόστους των πόρων εκτέλεσης των έξυπνων συμβολαίων σε μια εικονική μηχανή, που ονομάζεται «Ethereum Virtual Machine» (EVM) (Tikhomirov, 2018) (Εικόνα 5). Ακόμη, επιτρέπει στους προγραμματιστές να αναπτύσσουν αποκεντρωμένες εφαρμογές με ενσωματωμένες οικονομικές λειτουργίες.

Η νομισματική μονάδα του Ethereum, το ether, προσδιορίζεται επίσης ως «ETH» ή με τα σύμβολα «Ξ» και «♦» (π.χ. 1 Ether ή 1 ETH ή Ξ1 ή ♦1). To ether υποδιαιρείται σε μικρότερες μονάδες, με την μικρότερη αυτών να ονομάζεται «wei». Ένα ether αντιστοιχεί σε  $10^{18}$  ή 1,000,000,000,000,000,000 wei » (Antonopoulos and Wood, 2018).

To Ethereum ενσωματώνει έναν μηχανισμό τιμολόγησης, κατά τον οποίο κάθε υπολογιστικό βήμα στο «EVM» τιμολογείται σε μονάδες «gas» (Wood, 2014). Η αντιστοιχία μιας μονάδας gas σε ether καθορίζεται από την τιμή του στην αγορά. Για κάθε συναλλαγή, ο αποστολέας καθορίζει τη μέγιστη ποσότητα gas που αναμένεται να καταναλώσει το υπολογιστικό βήμα (gas limit) και την τιμή που επιθυμεί να πληρώσει ο αποστολέας ανά μονάδα gas (gas price). Το τελικό ποσό της συναλλαγής ισούται με το «gas limit» πολλαπλασιασμένο με το «gas price» τη δεδομένη χρονική στιγμή.



Εικόνα 5 - To Ethereum Virtual Machine (EVM) (coin98.net, 2022)

## 2.3. Έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές

Ο όρος έξυπνο συμβόλαιο έχει χρησιμοποιηθεί ανά τα χρόνια για να περιγράψει μια ποικιλία διαφορετικών πραγμάτων. Τη δεκαετία του 1990, ο κρυπτογράφος Nick Szabo επινόησε τον όρο και τον όρισε ως «ένα σύνολο υποσχέσεων, που ορίζονται σε ψηφιακή μορφή, συμπεριλαμβανομένων των πρωτοκόλλων, εντός των οποίων τα μέρη εκτελούν άλλες υποσχέσεις» (Antonopoulos and Wood, 2018). Στο πλαίσιο του Ethereum, ο όρος είναι στην πραγματικότητα λίγο εσφαλμένος, δεδομένου ότι τα έξυπνα συμβόλαια δεν είναι ούτε έξυπνα αλλά ούτε και νομικά συμβόλαια, παρά αμετάβλητα προγράμματα υπολογιστών που εκτελούνται ντετερμινιστικά στο πλαίσιο ενός «EVM», ως μέρος του πρωτοκόλλου δικτύου του Ethereum (Antonopoulos and Wood, 2018). Με άλλα λόγια, ένα έξυπνο συμβόλαιο είναι ένα κομμάτι κώδικα αποθηκευμένο στο blockchain, που μπορεί να εκτελεστεί ανεξάρτητα, με σκοπό την αυτοματοποίηση ορισμένων εργασιών (Christidis and Devetsikiotis, 2016).

Τα έξυπνα συμβόλαια συχνά εξισώνονται με τις εφαρμογές λογισμικού. Αντιθέτως, έχουν περισσότερο την μορφή των κλάσεων (classes) στον αντικειμενοστραφή προγραμματισμό. Όταν οι προγραμματιστές μιλούν για «ανάπτυξης έξυπνων συμβολαίων», συνήθως αναφέρονται στην πρακτική της συγγραφής κώδικα στη γλώσσα προγραμματισμού «Solidity» (Εικόνα 6), που έπειτα, θα εκτελεστεί στο δίκτυο Ethereum.

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.19;
3
4 contract Migrations {
5     address public owner;
6     uint public last_completed_migration;
7
8     constructor() public {
9         owner = msg.sender;
10    }

```

Εικόνα 6 - Παράδειγμα κώδικα σε γλώσσα προγραμματισμού «Solidity»

Οι προγραμματιστές συνήθως αναπτύσσουν έξυπνα συμβόλαια σε γλώσσες υψηλού επιπέδου (high-level) που στοχεύουν στο «EVM», με την πιο δημοφιλή να είναι η «Solidity». Ονομαστικά, μερικές από τις υπόλοιπες γλώσσες προγραμματισμού είναι: η «Serpent» (καταργήθηκε το 2017), η «Vyper» και η «LLL».

Ένα σημαντικό ζήτημα της αρχιτεκτονικής των έξυπνων συμβολαίων είναι η αδυναμία επεξεργασίας του κώδικα τους, μόλις αυτά εκτελεστούν στο blockchain. Ο μοναδικός τρόπος να διαγραφεί ένα έξυπνο συμβόλαιο είναι εάν προγραμματιστεί με έναν προσβάσιμο «SELFDESTRUCT» «opcode» (οδηγία σε γλώσσα μηχανής για μια συγκεκριμένη λειτουργία), το οποίο θα το αφαιρέσει πλήρως από το blockchain.

Μια Αποκεντρωμένη Εφαρμογή (Decentralized Application - dApp) είναι μια εφαρμογή που βασίζεται σε ένα αποκεντρωμένο δίκτυο και συνδυάζει ένα ή περισσότερα έξυπνα συμβόλαια με μια διεπαφή χρήστη (frontend) για τη λειτουργία της. Η βασική διαφορά της με μία κεντρική (centralized) εφαρμογή, είναι πως ο «backend» κώδικας της τελευταίας εκτελείται σε κεντρικούς διακομιστές (Ethereum.org, 2023).

Υπάρχουν πολλά πλεονεκτήματα στη δημιουργία ενός dApp, που μια τυπική κεντρική αρχιτεκτονική δεν μπορεί να προσφέρει (Antonopoulos and Wood, 2018):

- **Ανθεκτικότητα**

Επειδή η επιχειρηματική λογική (ο κώδικας) «πίσω» από μια αποκεντρωμένη εφαρμογή ελέγχεται από ένα έξυπνο συμβόλαιο, ο «backend» κώδικας του dApp θα διανεμηθεί και θα διαχειριστεί σε μια πλατφόρμα blockchain. Σε αντίθεση με μια εφαρμογή που αναπτύσσεται σε έναν κεντρικό διακομιστή, δε προβλέπεται διακοπή της λειτουργίας ενός dApp, έχοντας ως αποτέλεσμα να συνεχίσει να είναι διαθέσιμο όσο η εκάστοτε πλατφόρμα blockchain εξακολουθεί να λειτουργεί.

- **Διαφάνεια**

Η «on-chain» φύση ενός dApp επιτρέπει σε όλους να επιθεωρούν τον κώδικά του και να είναι πιο βέβαιοι για τη λειτουργία του. Οποιαδήποτε αλληλεπίδραση με το dApp θα αποθηκευτεί μόνιμα στο blockchain.

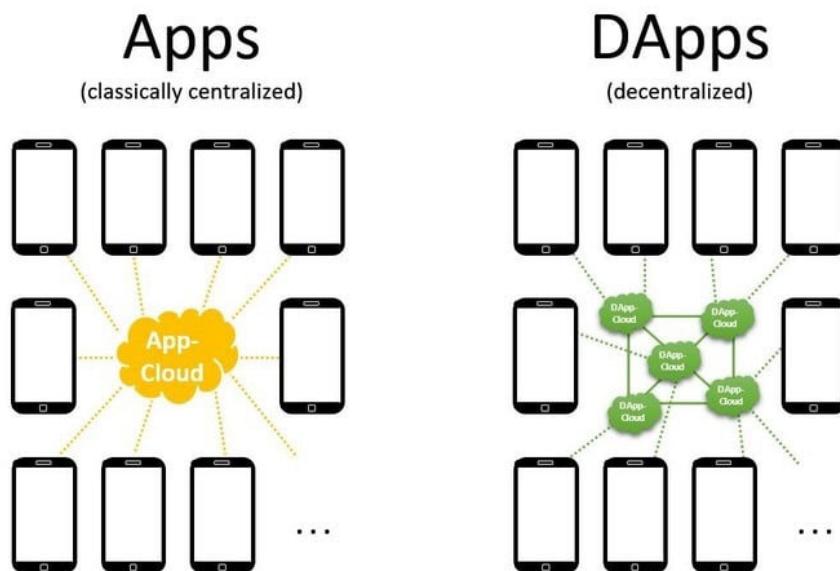
- **Αντίσταση στη λογοκρισία**

Όσο ένας χρήστης έχει πρόσβαση σε έναν κόμβο Ethereum (εκτελώντας έναν εάν είναι απαραίτητο), θα μπορεί πάντα να αλληλεπιδρά με ένα dApp χωρίς παρεμβολές από οποιαδήποτε κεντρική αρχή. Κανένας πάροχος υπηρεσιών, ή ακόμα και ο ιδιοκτήτης του έξυπνου συμβολαίου, δεν μπορεί να αλλάξει τον κώδικα μόλις εκτελεστεί στο δίκτυο.

Σε ένα dApp, τα έξυπνα συμβόλαια χρησιμοποιούνται για την αποθήκευση της επιχειρηματικής λογικής της εφαρμογής. Κατ' αυτόν τον τρόπο, με απλούς όρους, ένα

έξυπνο συμβόλαιο λειτουργεί πανομοιότυπα με ένα στοιχείο από την πλευρά του διακομιστή μιας κανονικής εφαρμογής. Μία από τις κύριες διαφορές τους είναι ότι κάθε υπολογισμός που εκτελείται σε ένα έξυπνο συμβόλαιο χαρακτηρίζεται από υψηλό κόστος και έτσι είναι σημαντικό να διατηρείται όσο το δυνατόν απλουστευμένος. Επομένως, είναι σημαντικό να προσδιοριστεί ποιες πτυχές της εφαρμογής χρειάζονται μια αξιόπιστη και αποκεντρωμένη πλατφόρμα εκτέλεσης και ποιες όχι, ώστε να ληφθούν τα κατάλληλα μέτρα κατά την συγγραφή του κώδικα.

Σε αντίθεση με την επιχειρηματική λογική των dApp, η οποία απαιτεί από έναν προγραμματιστή να κατανοήσει τον τρόπο λειτουργίας του «EVM», αλλά και νέες γλώσσες προγραμματισμού όπως η «Solidity», για τη διεπαφή χρήστη (user interface) ενός dApp μπορούν να χρησιμοποιηθούν τυπικές τεχνολογίες ιστού (HTML, CSS, JavaScript κ.λπ.) και βιβλιοθήκες, όπως το «Web3.js», για να συνδέεται το «frontend» της εφαρμογής, μέσω ενός «JavaScript API», στο «backend» της - το blockchain. Αυτό επιτρέπει σε έναν «παραδοσιακό» προγραμματιστή ιστού να χρησιμοποιεί οικεία εργαλεία, βιβλιοθήκες και πλαίσια (frameworks). Οι αλληλεπιδράσεις με το Ethereum, όπως η υπογραφή μηνυμάτων, η αποστολή συναλλαγών και η διαχείριση κλειδιών, πραγματοποιούνται συχνά μέσω του προγράμματος περιήγησης ιστού, με τη βοήθεια μιας επέκτασης-«πορτοφολιού», όπως το «Metamask».



Εικόνα 7 - Σύγκριση κεντρικών και αποκεντρωμένων εφαρμογών (Goldmann, 2019)

## Κεφάλαιο 3: Ψηφιακή εγκληματολογία

Η ψηφιακή εγκληματολογία (digital forensics) αντιπροσωπεύει έναν αναπτυσσόμενο κλάδο της πληροφορικής, που υπάγεται στο γενικότερο πλαίσιο της ασφάλειας πληροφοριών. Ειδικότερα, σχετίζεται με την απόκριση σε συμβάντα ασφάλειας μέσω κοινών πρακτικών και εργαλείων που επιτρέπουν την ανάλυση και την ερμηνεία των ψηφιακών αποδεικτικών στοιχείων (Μαυρίδης, 2015). Είναι δηλαδή, η πρακτική της συλλογής, ανάλυσης και αναφοράς ψηφιακών δεδομένων με τρόπο νομικά αποδεκτό, μέσω εξειδικευμένων τεχνικών ανάκτησης, αυθεντικοποίησης και ανάλυσης, όταν μια υπόθεση αφορά θέματα που σχετίζονται με την αναπαράσταση της χρήσης ηλεκτρονικού υπολογιστή, την εξέταση υπολειμμάτων δεδομένων και την ταυτοποίηση δεδομένων με τεχνική ανάλυση ή επεξήγηση των τεχνικών χαρακτηριστικών των δεδομένων και της χρήσης υπολογιστή (Prasad and Pandey, 2016). Μπορεί να χρησιμοποιηθεί για τον εντοπισμό και την πρόληψη εγκλημάτων, αλλά και κάθε διένεξης, όπου τα αποδεικτικά στοιχεία αποθηκεύονται ψηφιακά.

Ομοίως με πολλές άλλες εγκληματολογικές επιστήμες, η ψηφιακή εγκληματολογία περικλείει τη χρήση εξελιγμένων τεχνολογικών εργαλείων και διαδικασιών που πρέπει να ακολουθούνται για να διασφαλιστεί η ακεραιότητα των αποδεικτικών στοιχείων και η ακρίβεια των αποτελεσμάτων σχετικά με την επεξεργασία τους μέσω υπολογιστή (Prasad and Pandey, 2016). Η διαδικασία έρευνας ψηφιακής εγκληματολογίας ακολουθεί συνήθως προκαθορισμένες διεργασίες για την εξαγωγή πληροφοριών και τη συγγραφή μιας δομημένης έκθεσης αποδεικτικών στοιχείων (Khan et al., 2021):

- Συνλογή:** Απόκτηση ψηφιακού περιεχομένου που σχετίζεται με την υπό διερεύνηση υπόθεση από διάφορες συσκευές πολυμέσων.
- Ταυτοποίηση:** Προσδιορισμός της ιδιοκτησίας και των πιθανών πηγών των σημαντικότερων πληροφοριών και δεδομένων.
- Εξέταση και ανάλυση:** Διεξαγωγή λεπτομερούς συστηματικής εξέτασης των αποδεικτικών στοιχείων που σχετίζονται με το έγκλημα και εξαγωγή ουσιαστικών συμπερασμάτων.
- Αναφορά:** Συγγραφή μιας ολοκληρωμένης έκθεσης με βάση τα στοιχεία που εξετάστηκαν, χρησιμοποιώντας κατάλληλες εγκληματολογικές τεχνικές. Η

προκύπτουσα έκθεση παρουσιάζεται στο δικαστήριο ως ουσιαστικό αποδεικτικό στοιχείο κατά της υπό διερεύνηση υπόθεσης.

- **Διατήρηση:** Ηλεκτρονική διατήρηση των συλλεγόμενων αποδεικτικών στοιχείων, προστατεύοντας τις συσκευές πολυμέσων, τα αρχεία καταγραφής που σχετίζονται με τη συσκευή και τους χρήστες της και του φακέλου όλων των σχετικών αποδεικτικών στοιχείων με ασφαλή τρόπο.

Ο πρωταρχικός στόχος της ψηφιακής εγκληματολογίας έγκειται στη σχολαστική συλλογή των πληροφοριών, χωρίς τροποποίηση του αρχικού περιεχομένου και στη διεξαγωγή διεξοδικής έρευνας για την επικύρωση των ευρημάτων με συγκεκριμένες αποδείξεις, που αποκλείουν τυχόν διφορούμενες ερμηνείες. Οι διαδικασίες της συλλογής και της έρευνας ενδέχεται να περιλαμβάνουν μεθόδους όπως (Μαυρίδης, 2015):

- Ενδελεχής έρευνα για τη συλλογή δεδομένων από το πληροφοριακό σύστημα και από ποικίλους διαδικτυακούς πόρους.
- Ανάκτηση τροποποιημένων ή διαγραμμένων δεδομένων.
- Ανάκτηση κωδικών πρόσβασης μη εξουσιοδοτημένων χρηστών, για την πραγματοποίηση ή και την απόκρυψη των δραστηριοτήτων τους.
- Τεκμηρίωση των ενεργειών και των λειτουργιών των μη εξουσιοδοτημένων χρηστών.
- Αναλυτική εξέταση των συλλεχθέντων αποδεικτικών στοιχείων.
- Σύνταξη μιας λεπτομερούς ανάλυσης των αποτελεσμάτων της ερευνητικής διαδικασίας, με σκοπό τη χρήση της ως βάση των πορισμάτων που απευθύνεται στον αρμόδιο πραγματογνώμονα.

### 3.1. Ιστορία της εγκληματολογίας

Ο προσδιορισμός της ακριβούς διεξαγωγής της πρώτης έρευνας ψηφιακής εγκληματολογίας αντιμετωπίζει δυσκολίες. Ωστόσο, μια συναίνεση μεταξύ των εμπειρογνωμόνων αναγνωρίζει ότι ο τομέας αυτός ξεκίνησε την ανάπτυξή του πριν από περίπου τρεις δεκαετίες (Wheelbarger, 2009). Η προέλευσή του μπορεί να εντοπιστεί στις Ηνωμένες Πολιτείες, κυρίως όταν οι αρχές επιβολής του νόμου και οι στρατιωτικοί ερευνητές παρατήρησαν αύξηση των τεχνολογικά καταρτισμένων εγκληματιών. Το κυβερνητικό προσωπικό που ήταν επιφορτισμένο με τη διαφύλαξη ευαίσθητων,

εμπιστευτικών και απόρρητων δεδομένων διεξήγαγε εγκληματολογικές μελέτες ως απάντηση σε πιθανές παραβιάσεις ασφαλείας, με σκοπό όχι μόνο να διερευνήσει μια συγκεκριμένη παραβίαση αλλά και να συλλέξει πληροφορίες για την αποτροπή πιθανών μελλοντικών παραβιάσεων (Wheelbarger, 2009). Με την πάροδο του χρόνου, οι τομείς της ασφάλειας των πληροφοριών και της ψηφιακής εγκληματολογίας, άρχισαν σταδιακά να διαπλέκονται. Τα σημαντικότερα γεγονότα στην ιστορία της εγκληματολογίας συνοψίζονται στον παρακάτω πίνακα (Prasad and Pandey, 2016):

Έτος	Γεγονός
1835	Ο Henry Goddard της Scotland Yard έγινε ο πρώτος άνθρωπος που χρησιμοποίησε τη φυσική ανάλυση για να συνδέσει μια σφαίρα με το φονικό όπλο.
1836	Ο James Marsh ανέπτυξε ένα χημικό τεστ για την ανίχνευση αρσενικού, το οποίο χρησιμοποιήθηκε κατά τη διάρκεια μιας δίκης δολοφονίας.
1892	Ο Sir Francis Galton καθιέρωσε το πρώτο σύστημα χαρακτηρισμού των δακτυλικών αποτυπωμάτων ως απόρρητα δεδομένα.
1920	Ο Αμερικανός γιατρός Calvin Goddard δημιούργησε το «μικροσκόπιο σύγκρισης» για να βοηθήσει να προσδιοριστεί ποιες σφαίρες προήλθαν από ποιους κάλυκες.
1930	Ο Karl Landsteiner κέρδισε το βραβείο Νόμπελ για την κατηγοριοποίηση του ανθρώπινου αίματος στις διάφορες ομάδες του.
1970	Η Aerospace Corporation στην Καλιφόρνια ανέπτυξε μια μέθοδο για την ανίχνευση υπολειμμάτων πυροβολισμών χρησιμοποιώντας ηλεκτρονικά μικροσκόπια σάρωσης
1984	Δημιουργήθηκε το πρόγραμμα «Magnetic Media» του «FBI», το οποίο αργότερα μετονομάστηκε σε «Computer Analysis and Response Team» (CART) και πιστεύεται ότι είναι ο πρόγονος της ψηφιακής εγκληματολογίας.
1988	Ιδρύθηκε η «Διεθνής Ένωση Ειδικών Έρευνας Υπολογιστών» (International Association of Computer Investigative Specialists - IACIS).
1995	Ιδρύθηκε ο «Διεθνής Οργανισμός Ψηφιακών Αποδεικτικών Στοιχείων» (International Organization on Computer Evidence - IOCE).
1997	Τα μέλη της «G8» δήλωσαν ότι «το προσωπικό επιβολής του νόμου πρέπει να είναι εκπαιδευμένο και εξοπλισμένο για την αντιμετώπιση εγκλημάτων υψηλής τεχνολογίας».
1998	<ul style="list-style-type: none"> <li>• Η «G8» ανέθεσε στο «IICE» να δημιουργήσει διεθνείς αρχές, κατευθυντήριες γραμμές και διαδικασίες σχετικά με τα ψηφιακά αποδεικτικά στοιχεία.</li> <li>• Πραγματοποιήθηκε το 1ο Συμπόσιο Εγκληματολογικών Επιστημών της «INTERPOL».</li> </ul>

2000	Iδρύθηκε το πρώτο Περιφερειακό Εργαστήριο Ψηφιακής Εγκληματολογίας του FBI.
------	---

Πίνακας 1 - Τα σημαντικότερα γεγονότα στην ιστορίας της εγκληματολογίας (Prasad and Pandey, 2016)

Ο τομέας της ψηφιακής εγκληματολογίας αποτελεί έναν από τους πολλούς κλάδους της εγκληματολογικής επιστήμης, που εφαρμόζεται κυρίως σε συνδυασμό με αστικές δίκες ή ποινικές έρευνες. Σταδιακά, ο τομέας έχει υποστεί σημαντική ανάπτυξη τις τελευταίες δεκαετίες, συνεχίζοντας να εξελίσσεται μέχρι σήμερα. Τόσο οι κυβερνητικοί φορείς όσο και οι ιδιωτικές επιχειρήσεις έχουν υιοθετήσει αυτή την πορεία, εμπλέκοντας εσωτερικούς εμπειρογνόμονες ασφάλειας πληροφοριών και ψηφιακής εγκληματολογίας ή συνάπτοντας συμβάσεις με εξειδικευμένους επαγγελματίες ή εταιρείες όταν κρίνεται απαραίτητο. Συγκεκριμένα, ο ιδιωτικός νομικός τομέας έχει επίσης, αναγνωρίσει τη σημασία των αναλύσεων ψηφιακής εγκληματολογίας σε αστικές νομικές διαφορές, σημειώνοντας μια αξιοσημείωτη αύξηση ενδιαφέροντος στο πεδίο των ψηφιακών ερευνών.

### 3.2. Μορφές και στόχος της ψηφιακής εγκληματολογίας

Η ψηφιακή εγκληματολογία συνδέεται κατά κανόνα, με ποινικές ερευνητικές διαδικασίες, συχνά επικεντρωμένες σε διάφορες μορφές ψηφιακού εγκλήματος. Αυτού του είδους τα εγκλήματα διαιρούνται συνήθως, σε δύο διακριτές κατηγορίες: το ψηφιακό έγκλημα και το έγκλημα που εμπλέκονται ένας ή περισσότεροι υπολογιστές (Prasad and Pandey, 2016):

- **Ψηφιακό έγκλημα:** Ο όρος αναφέρεται σε παράνομες ενέργειες που πραγματοποιούνται αποκλειστικά μέσω υπολογιστών, όπως ο διαδικτυακός εκφοβισμός ή η ανεπιθύμητη αλληλογραφία (spamming). Εκτός από τα προσφάτως αναδυόμενα εγκλήματα που διευκολύνονται από την ψηφιακή εποχή, περιλαμβάνει επίσης συμβατικά εγκλήματα που εκτελούνται αποκλειστικά σε υπολογιστές, με παράδειγμα περιπτώσεις όπως η παιδική πορνογραφία.
- **Έγκλημα που εμπλέκεται ένας ή περισσότεροι υπολογιστές:** Πρόκειται για έγκλημα που διεξάγεται στον «πραγματικό κόσμο», αλλά διευκολύνεται από τη χρήση υπολογιστών. Ένα κλασικό παράδειγμα αυτού του είδους εγκλήματος είναι η απάτη, όπου οι υπολογιστές συχνά χρησιμεύουν ως μέσο επικοινωνίας μεταξύ των απατεώνων, καταγραφής (ή σχεδιασμού) δραστηριοτήτων ή δημιουργίας πλαστών εγγράφων.

Οι υπολογιστές μπορούν να αποτελέσουν «σκηνή εγκλήματος» σε δραστηριότητες όπως το «hacking» ή οι επιθέσεις άρνησης υπηρεσίας (Denial of Service – DoS) ή περιέχοντας κρίσιμα αποδεικτικά στοιχεία, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, ιστορικό διαδικτύου, έγγραφα ή άλλα σχετικά αρχεία που συνδέονται με εγκλήματα, όπως δολοφονία, απαγωγή, απάτη και διακίνηση ναρκωτικών. Ένας ερευνητής δεν ενδιαφέρεται μόνο για το περιεχόμενο των μηνυμάτων ηλεκτρονικού ταχυδρομείου, των εγγράφων και των αρχείων, αλλά και για τα «μεταδεδομένα» (Metadata), που σχετίζονται με αυτά. Μέσω της ψηφιακής εγκληματολογικής ανάλυσης, μπορούν να αποκαλυφθούν λεπτομέρειες, όπως η πρώτη εμφάνιση του εγγράφου σε μια συσκευή, η πιο πρόσφατη ημερομηνία που υπέστη επεξεργασία, η πιο πρόσφατη ημερομηνία αποθήκευσης ή εκτύπωσής του και ο χρήστης που πραγματοποίησε αυτές τις ενέργειες. Υπό μία ευρύτερη έννοια, ο στόχος της ψηφιακής εγκληματολογίας είναι να παρέχει κατευθυντήριες γραμμές για (Prasad and Pandey, 2016):

- Τήρηση του πρωτοκόλλου αρχικής απόκρισης και πρόσβασης στον υπολογιστή του θύματος μετά το περιστατικό.
- Διαμόρφωση πρωτοκόλλων σε μία ύποπτη σκηνή εγκλήματος για τη διασφάλιση ότι τα ψηφιακά αποδεικτικά στοιχεία που λαμβάνονται δεν είναι κατεστραμμένα.
- Απόκτηση και αντιγραφή δεδομένων.
- Ανάκτηση διαγραμμένων αρχείων και «διαμερισμάτων» από ψηφιακά μέσα για την εξαγωγή και την επικύρωση των αποδεικτικών στοιχείων.
- Ανάλυση ψηφιακών μέσων για τη διατήρηση των αποδεικτικών στοιχείων, ανάλυση αρχείων καταγραφής, εξαγωγή συμπερασμάτων, διερεύνηση της «κίνησης» του δικτύου και των αρχείων καταγραφής για τη δημιουργία συσχετισμών με το εκάστοτε συμβάν, εξέταση διαδικτυακών επιθέσεων και παρακολούθηση μηνυμάτων ηλεκτρονικού ταχυδρομείου για τη διερεύνηση εγκλημάτων που σχετίζονται με αυτό.
- Συγγραφή μιας ολοκληρωμένης εγκληματολογικής έκθεσης που περιγράφει λεπτομερώς ολόκληρη τη διαδικασία έρευνας.
- Διαφύλαξη των αποδεικτικών στοιχείων διατηρώντας ένα chain of custody.
- Εφαρμογή αυστηρών διαδικασιών με σκοπό την διασφάλιση πως τα αποτελέσματα των εγκληματολογικών ερευνών θα ανταπεξέλθουν στους αυστηρούς ελέγχους του δικαστηρίου.

- Παρουσίαση των αποτελεσμάτων των εγκληματολογικών ερευνών στο δικαστήριο.

## Κεφάλαιο 4: Το Blockchain στην Ψηφιακή Εγκληματολογία

Πολλοί ειδικοί στον τομέα της εγκληματολογίας χρησιμοποιούν όλο και περισσότερο την τεχνολογία του blockchain, εκμεταλλεύοντας την αποκεντρωμένη και κατανεμημένη αρχιτεκτονική της, η οποία ενισχύει την ανθεκτικότητα έναντι μιας σειράς κακόβουλων επιθέσεων, που συνήθως στοχεύουν σε κεντρικά συστήματα (Xiong and Du, 2019). Αξιοποιώντας επίσης, τις λειτουργίες κρυπτογράφησης και κατακερματισμού (hash), σε συνδυασμό με την ενσωμάτωση συστημάτων ανίχνευσης και πρόληψης εισβολών, τειχών προστασίας και εργαλείων και πολιτικών κατά της αποκάλυψης (anti-disclosure), αυξάνεται σημαντικά η άμυνα των αποκεντρωμένων κόμβων. Στην ψηφιακή εγκληματολογία, το blockchain μπορεί επίσης να διαδραματίσει κεντρικό ρόλο, κρυπτογραφώντας και αποθηκεύοντας τα αποδεικτικά στοιχεία και τις συναλλαγές που σχετίζονται με υποθέσεις σε ένα αμετάβλητο καθολικό, διευκολύνοντας τη διεκπεραίωση των εγκληματολογικών ερευνών.

Η τεχνολογία του blockchain έχει υιοθετηθεί ευρέως και χρησιμοποιείται σε ένα εκτεταμένο φάσμα εφαρμογών ασφαλείας, προσφέροντας λύσεις αμετάβλητου κατανεμημένου καθολικού, για την ασφάλεια και την προστασία των δεδομένων. Αυτό επιτυγχάνεται με την ιδιότητα που έχει κάθε block, να φέρει την κρυπτογραφημένη τιμή κατακερματισμού του προηγούμενου σε σειρά, αποθηκευμένου block. Με αυτόν τον τρόπο επιτρέπεται η αποθήκευση κατακερματισμένων κρυπτογραφημένων δεδομένων, διασφαλίζοντας έτσι την ακεραιότητα τους και αποτρέποντας μη εξουσιοδοτημένες παρεμβάσεις, καθώς οποιαδήποτε τροποποίηση πρέπει να συμφωνηθεί, να υπογραφεί και να εγκριθεί από όλους τους εξουσιοδοτημένους συμμετέχοντες σε ένα ελεγχόμενο (permissioned) δίκτυο blockchain, χρησιμοποιώντας προκαθορισμένους αλγορίθμους συναίνεσης (Ahmad et al., 2020). Επιπλέον, η επιχειρηματική λογική (κώδικας) διέπεται και ρυθμίζεται αποτελεσματικά μέσω των έξυπνων συμβολαίων, υλοποιώντας μια αποκεντρωμένη εφαρμογή έρευνας ψηφιακής εγκληματολογίας. Αυτό βοηθά στην επίτευξη ασφαλών, «διαφανών» και αμετάβλητων ψηφιακών ερευνών, καθιστώντας τες ανθεκτικές στην πλαστογραφία και την παραποίηση.

Η τεχνολογία blockchain παρουσιάζει αξιοσημείωτη συσχέτιση με την τριάδα ασφαλείας «CIA» (Confidentiality, Integrity, and Availability), η οποία περιλαμβάνει τις έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας (Gupta, 2018). Η αποκεντρωμένη και κρυπτογραφημένη φύση του blockchain διασφαλίζει την

εμπιστευτικότητα των ευαίσθητων δεδομένων, παρέχοντας πρόσβαση αποκλειστικά σε εξουσιοδοτημένα μέρη, μέσω κρυπτογραφικών κλειδιών. Η ιδιότητα της «μιας κατεύθυνσης» (one-way) της συνάρτησης κατακερματισμού διασφαλίζει ότι η ανάκτηση δεδομένων από το αποτέλεσμα κατακερματισμού είναι λογικά αδύνατη. Επιπλέον, η πρόβλεψη των αρχικών δεδομένων από το αποτέλεσμα του κατακερματισμού αποδεικνύεται δύσκολη, καθώς ακόμη και μικρές αλλαγές στο κείμενο της προέλευσης, οδηγούν σε σημαντικές διαφορές. Το χαρακτηριστικό της κατανομής του δικτύου εγγυάται τη διαθεσιμότητα, εξαλείφοντας τα μεμονωμένα σημεία αποτυχίας (single points of failure) και τις διακοπές λειτουργίας του. Ακόμα κι αν ένας κόμβος απενεργοποιηθεί, οι πληροφορίες παραμένουν προσβάσιμες στους υπόλοιπους, καθώς όλοι διατηρούν ένα ακριβές αντίγραφο του καθολικού, εξασφαλίζοντας συνεχείς ενημερώσεις. Η ενσωμάτωση των παραπάνω εννοιών ασφαλείας (CIA) στον κορμό της τεχνολογίας του blockchain, το καθιστά μια εξαιρετικά ευνοϊκή επιλογή για τη διατήρηση και τον εντοπισμό ενός chain of custody ψηφιακής εγκληματολογίας.



Εικόνα 8 - Η τριάδα ασφαλείας «CIA» (Oliveira et al., 2020)

#### **4.1. Κατανόηση της συνέργειας των ιδιωτικών Blockchain και των εφαρμογών Chain of Custody**

Οι έρευνες ψηφιακής εγκληματολογίας περιλαμβάνουν μια συστηματική και μεθοδολογική προσέγγιση για τον εντοπισμό, τη διατήρηση, τη συλλογή, την ανάλυση και την παρουσίαση ψηφιακών αποδεικτικών στοιχείων, με τρόπο αποδεκτό από ένα

δικαστήριο. Απαραίτητη προϋπόθεση για την επίτευξη αυτού του στόχου είναι η δημιουργία και η διατήρηση ενός chain of custody καθ' όλη τη διάρκεια της διαδικασίας της έρευνας. Το chain of custody είναι μια διαδικασία καταγραφής, τεκμηρίωσης και διατήρησης της χρονολογικής σειράς και του πλήρους ιστορικού χειρισμού και διατήρησης των ψηφιακών αποδεικτικών στοιχείων για την υπό διερεύνηση υπόθεση, ώστε να είναι παραδεκτή στο δικαστήριο (Khan et al., 2021). Η διαφύλαξη της ακεραιότητας του chain of custody έναντι οποιωνδήποτε αλλοιώσεων ή παραποίησεων είναι υψίστης σημασίας. Απώτερος στόχος του είναι να αποδειχθεί ότι τα συλλεχθέντα αποδεικτικά στοιχεία είναι αληθή, πραγματικά περιστατικά και συναφή με το υπό διερεύνηση έγκλημα.

Τα αποδεικτικά στοιχεία που λαμβάνονται από επαγγελματίες θεωρούνται αξιόπιστα από τα δικαστήρια. Ωστόσο, σε περιπτώσεις αμφισβήτησης, διεξάγεται εκτενέστερη εξέταση για την επαλήθευση της γνησιότητας και της ακεραιότητας των εκθέσεων. Η τιμή κατακερματισμού (hash value) των ψηφιακών αρχείων, η τοποθεσία της σκηνής του εγκλήματος και τα ονόματα των ερευνητών δεν αρκούν για να γίνουν δεκτά τα αποδεικτικά στοιχεία από τα δικαστήρια. Απαιτούνται πλέον, πρόσθετα δεδομένα, όπως η ψηφιακή υπογραφή κάθε αντικειμένου, οι ακριβείς τοποθεσίες επεξεργασίας κάθε ψηφιακού αποδεικτικού στοιχείου, η ταυτοποίηση όλων των ατόμων που εμπλέκονται στην εγκληματολογική έρευνα και των ατόμων που διατηρούσαν πρόσβαση στα αποδεικτικά στοιχεία, όπως επίσης και ένα αρχείο καταγραφής όλων των συναλλαγών που διεξήχθησαν (Lone and Mir, 2019). Επιπλέον, οι εγκληματολογικοί ερευνητές εξαρτώνται σε μεγάλο βαθμό από αυτοματοποιημένα εγκληματολογικά εργαλεία, επομένως η αξιοπιστία των αποτελεσμάτων της έρευνας εξαρτάται από την ακρίβεια αυτών των εργαλείων.

Χωρίς την εφαρμογή ενός ασφαλούς μηχανισμού πρόβλεψης παραβίασης, υπάρχει δυνητικός κίνδυνος τα ψηφιακά αποδεικτικά στοιχεία και η συσχετιζόμενη τιμή κατακερματισμού να παραπομούν από κακόβουλα άτομα. Ο ελεγκτής πληροφοριών μπορεί μόνο να εξακριβώσει ότι τα αποδεικτικά στοιχεία παραμένουν αμετάβλητα από τη στιγμή που υπολογίστηκε η τιμή κατακερματισμού. Κάνοντας χρήση της τεχνολογίας του blockchain, δεδομένου ότι αποτελείται από διαδοχικά block, τα οποία συνδέονται μεταξύ τους με χρονολογική σειρά, οποιαδήποτε προσπάθεια αλλοίωσης γίνεται εμφανής, καθώς τα δεδομένα που είναι αποθηκευμένα σε αυτό δεν μπορούν να τροποποιηθούν ή να διαγραφούν.

Τα δημόσια blockchain είναι αποκεντρωμένα, επιτρέποντας σε οποιονδήποτε να έχει πρόσβαση σε αυτά και στα αποθηκευμένα δεδομένα. Αντίθετα, ένα ιδιωτικό blockchain επιτρέπει την πρόσβαση αποκλειστικά σε αξιόπιστες οντότητες, καθιστώντας το ιδανικό για χρήση σε εγκληματολογικές υποθέσεις και άλλες περιπτώσεις που περιλαμβάνουν ευαίσθητες πληροφορίες. Ένα πρόσθετο επίπεδο ασφάλειας μπορεί να επιτευχθεί με την περιοδική καταγραφή της κατάστασης (state) του ιδιωτικού blockchain σε ένα δημόσιο, διασφαλίζοντας την ακεραιότητα του ίδιου του καθολικού (Lu, 2019). Τα δεδομένα που καταχωρούνται σε δημόσια blockchain δεν μπορούν να τροποποιηθούν, καθώς, όπως προαναφέρθηκε, είναι αποκεντρωμένα και ως εκ τούτου, όλοι οι συμμετέχοντες μπορούν να επαληθεύσουν την αυθεντικότητα τους. Έτσι, τα δημόσια blockchain μπορούν να επιτελέσουν αξιοσημείωτο ρόλο σε περιπτώσεις που απαιτείται ένα πιο ισχυρό chain of custody.

Σε ένα «παραδοσιακό» chain of custody, η μόνη επιλογή αναφορικά με τη διατήρηση των αποδεικτικών στοιχείων είναι η αποθήκευσή τους σε μία κεντρική τοποθεσία, αυξάνοντας τον κίνδυνο παραβίασης δεδομένων, εξαιτίας των κενών ασφαλείας που υφίστανται κατά τον χειρισμό τους. Μια τέτοια ρύθμιση στερείται ισχυρών μέτρων για την αντιμετώπιση κυβερνοεπιθέσεων, καθιστώντας την ευάλωτη σε αλλοίωση ή πλαστογραφία αποδεικτικών στοιχείων (Khan et al., 2021). Το κυριότερο ζήτημα που αντιμετωπίζουν οι μέθοδοι διατήρησης ενός chain of custody είναι η τεκμηρίωση και η σωστή καταγραφή των αλληλεπιδράσεων των ενδιαφερόμενων με τα αποδεικτικά στοιχεία. Ακόμη, όταν πολλά μέρη έχουν πρόσβαση στα αποδεικτικά στοιχεία, υπάρχει κίνδυνος αλλοίωσής τους.

Εκμεταλλεύοντας τις δυνατότητες ενός blockchain και ιδίως την συνάρτηση κατακερματισμού και την κρυπτογράφηση, διασφαλίζεται ότι μόλις τα αποδεικτικά στοιχεία κατακερματιστούν και αποθηκευτούν σε ένα block, η παραβίαση καθίσταται αδύνατη, εξορθολογίζοντας τη διαδικασία επαλήθευσης, καθώς μόνο εξουσιοδοτημένα μέρη έχουν την ευχέρεια αλληλεπίδρασης και πραγματοποίησης αλλαγών στα αποδεικτικά στοιχεία. Επίσης, παρέχεται «διαφάνεια» σε όλους τουν συμμετέχοντες, οι οποίοι μπορούν να ελέγξουν τις συναλλαγές μέσω των δημόσιων διευθύνσεων τους (Lone and Mir, 2019). Όλα τα παραπάνω οδηγούν στο συμπέρασμα, πως η τεχνολογία του blockchain καθίσταται ιδανική λύση για την διατήρηση της ακεραιότητας και της αμεταβλητότητας των δεδομένων, που αποτελεί ύψιστη πρόκληση κατά την εφαρμογή ενός chain of custody.

## 4.2. Βιβλιογραφική Ανασκόπηση

Το πλήθος των δημοσιεύσεων που έχουν προκύψει τα τελευταία χρόνια, αναφορικά με τα οφέλη της τεχνολογίας του blockchain στην ψηφιακή εγκληματολογία και πιο συγκεκριμένα, στη βελτίωση της διαδικασίας του chain of custody, αναδεικνύει το εύρος της έρευνας και τη δέσμευση της ερευνητικής κοινότητας να διερευνήσει τον τομέα αυτό. Καθώς η τεχνολογία συνεχίζει να αναπτύσσεται και οι εξελίξεις στο blockchain πληθαίνουν, αναμένεται πως η βιβλιογραφία θα συνεχίσει να επεκτείνεται, παρέχοντας περαιτέρω γνώσεις και καινοτομίες σε αυτόν τον συνεχώς εξελισσόμενο τομέα.

Αυτή η βιβλιογραφική ανασκόπηση στοχεύει στη διερεύνηση υφιστάμενων ερευνών και μελετών που σχετίζονται με ιδιωτικά δίκτυα blockchain και τη σχέση τους με εφαρμογές chain of custody. Εξετάζοντας την τρέχουσα κατάσταση των ερευνών, αυτή η ανασκόπηση θα παρέχει μια ολοκληρωμένη κατανόηση του θέματος και θα εντοπίσει τα ερευνητικά κενά που στοχεύει να αντιμετωπίσει η παρούσα διπλωματική εργασία.

Τα ιδιωτικά δίκτυα blockchain έχουν αποδειχθεί ως μια πολλά υποσχόμενη λύση για οργανισμούς που αναζητούν βελτιωμένη ασφάλεια και ιδιωτικότητα. Η μελέτη των Xu et al. (2017) υπογραμμίζει τα πλεονεκτήματα των ιδιωτικών blockchain, όπως η αυξημένη ταχύτητα συναλλαγών, η επεκτασιμότητα και η εποπτεία των συμμετεχόντων στο δίκτυο. Αυτά τα δίκτυα προσφέρουν ελεγχόμενη πρόσβαση, επιτρέποντας στους οργανισμούς να διατηρούν την εμπιστευτικότητα τους, αξιοποιώντας παράλληλα την αμετάβλητη και «διαφανή» φύση του blockchain.

Η ενσωμάτωση ιδιωτικών δικτύων blockchain σε εφαρμογές chain of custody έχει προσελκύσει μεγάλο ενδιαφέρον, ως μέσο ενίσχυσης της παρακολούθησης και της ασφάλειας περιουσιακών στοιχείων (assets). Οι Liu et al. (2020) προτείνουν πλαίσια (frameworks) για την ενσωμάτωση της τεχνολογίας blockchain στην αλυσίδα εφοδιασμού και στα συστήματα διαχείρισης περιουσιακών στοιχείων. Αυτές οι μελέτες υπογραμμίζουν τα οφέλη της χρήσης ενός ιδιωτικού δικτύου blockchain για τη ενίσχυση της διαφάνειας και της επαληθευσιμότητας ενός chain of custody. Οι Lone et al. (2019) προτάσουν ένα chain of custody για σκοπούς ψηφιακής εγκληματολογίας βασισμένο σε blockchain, για την παροχή ακεραιότητας και ανθεκτικότητας ενάντια σε παραβιάσεις κατά των ψηφιακών αποδεικτικών στοιχείων. Το μοντέλο λειτουργίας τους περιλαμβάνει τέσσερις ενέργειες αναφορικά με τα αποδεικτικά στοιχεία:

δημιουργία, μεταφορά, διαγραφή και εμφάνιση αποδεικτικών στοιχείων. Οι Jeong et al. (2020) παρουσιάζουν μια λύση για το σχεδιασμό και την υλοποίηση ενός ελεγχόμενου (permissioned) μοντέλου έρευνας εγκληματολογίας με χρήση του «Hyperledger Fabric», για τη προώθηση της αξιοπιστίας και της γνησιότητας των δεδομένων στις εγκληματολογικές υποθέσεις.

Το σύνολο της βιβλιογραφίας σχετικά με τα οφέλη της τεχνολογίας του blockchain στην ψηφιακή εγκληματολογία και πιο συγκεκριμένα, στη βελτίωση της διαδικασίας του chain of custody, προσφέρει πολύτιμες πληροφορίες για το πώς η τεχνολογία του blockchain μπορεί να ενισχύσει την ακεραιότητα και την ασφάλεια των ψηφιακών εγκληματολογικών στοιχείων. Η έρευνα σε αυτόν τον τομέα καταδεικνύει τις δυνατότητες του blockchain στη δημιουργία ενός αμετάβλητου και «διαφανούχου» chain of custody, αντιμετωπίζοντας έτσι τις προκλήσεις που σχετίζονται με την αλλοίωση των αποδεικτικών στοιχείων και τη χειραγώγηση των δεδομένων στις ψηφιακές εγκληματολογικές έρευνες.

Είναι σημαντικό να σημειωθεί, ότι η χρήση του blockchain στη διαδικασία του chain of custody μπορεί να αποφέρει σημαντική αξία στην κοινωνία. Παρέχοντας ένα αμετάβλητο αρχείο όλων των αλληλεπιδράσεων με τα ψηφιακά αποδεικτικά στοιχεία, η τεχνολογία blockchain διασφαλίζει την ακεραιότητα, την αυθεντικότητα και την ιχνηλασμότητά τους, καθ' όλη τη διάρκεια του κύκλου ζωής τους. Αυτό ενισχύει την εμπιστοσύνη στο σύστημα ποινικής δικαιοσύνης, αλλά και το παραδεκτό των ψηφιακών αποδεικτικών στοιχείων στο δικαστήριο, οδηγώντας τελικά, σε πιο αξιόπιστα και δίκαια αποτελέσματα στις νομικές διαδικασίες.

Παρά το αυξανόμενο ενδιαφέρον για τα δίκτυα blockchain και τις εφαρμογές chain of custody, οι υφιστάμενες έρευνες που επικεντρώνονται ειδικά στην ανάπτυξη ενός ιδιωτικού δικτύου blockchain και μιας αντίστοιχης εφαρμογής chain of custody, παρουσιάζονται ελλιπείς. Μολονότι οι υπάρχουσες μελέτες προσφέρουν πολύτιμες πληροφορίες, συχνά στερούνται της ολοκληρωμένης διερεύνησης της τεχνικής εφαρμογής και των πρακτικών επιπτώσεων ενός τέτοιου συστήματος. Αυτό το ερευνητικό κενό παρέχει ένα σαφές κίνητρο για την παρούσα διπλωματική εργασία, στόχος της οποίας είναι να καλύψει το προαναφερθέν κενό, αναπτύσσοντας ένα ιδιωτικό δίκτυο blockchain και μια φιλική προς το χρήστη εφαρμογή chain of custody.

## Κεφάλαιο 5: Μεθοδολογία

---

Για την επιτυχή πραγμάτωση της παρούσας διπλωματικής εργασίας, εφαρμόστηκε ένας ποιοτικός σχεδιασμός έρευνας που περιλαμβάνει μια διεξοδική βιβλιογραφική ανασκόπηση με στόχο τη δημιουργία μιας ισχυρής βάσης γνώσεων στους τομείς των ιδιωτικών blockchain, των εφαρμογών chain of custody και της ψηφιακής εγκληματολογίας. Κατόπιν, επωφελούμενοι από τις αρχές της μεθοδολογίας «Agile», εφαρμόστηκε η διαδικασία σταδιακής υλοποίησης του πρακτικού μέρους της εργασίας, ξεκινώντας από τον σχεδιασμό και την ανάπτυξη του ιδιωτικού Ethereum Blockchain. Έπειτα, σχεδιάστηκε και αναπτύχθηκε η αποκεντρωμένη εφαρμογή chain of custody, η οποία στη συνέχεια, ενσωματώθηκε στην υποδομή του ιδιωτικού blockchain.

Για την αντιμετώπιση των πολύπλοκων προβλημάτων που ανέκυψαν κατά τη διαδικασία ανάπτυξης της εφαρμογής, αξιοποιήθηκε το πλαίσιο διαχείρισης «Scrum», το οποίο περιλαμβάνει μια σειρά εργαλείων και ρόλων με στόχο τη διευκόλυνση της οργάνωσης και διαχείρισης έργων που εφαρμόζουν τη μεθοδολογία «Agile» (Scrum.org, n.d.). Τα διαγράμματα, οι αναφορές και οι πίνακες που ακολουθούν δημιουργήθηκαν μέσω της εφαρμογής «Visual Paradigm»:

### Product Owner Report

---

Member	Χρήστος Μπάντης
Responsibilities	<ul style="list-style-type: none"> <li>• Καθορισμός του οράματος του έργου.</li> <li>• Διαμόρφωση των epics (καθορισμένες απαιτήσεις).</li> <li>• Σχεδιασμός, προσδιορισμός και ιεράρχηση των user stories (οι υποδιεργασίες που δημιουργούνται από τα epics).</li> <li>• Δημιουργία και ενημέρωση του σχεδίου κυκλοφορίας (release plan).</li> <li>• Επιτήρηση της σειράς προτεραιότητας των ανεκτέλεστων προϊόντων (prioritized product backlog).</li> </ul>

Πίνακας 2 - Αναφορά ιδιοκτήτη έργου

## Scrum Master Report

Member	Χρήστος Μπάντης
Responsibilities	<ul style="list-style-type: none"> <li>• Υποστηρίζει την διαμόρφωση των epics.</li> <li>• Συντονίζει τη κατάρτιση του σχεδίου κυκλοφορίας.</li> <li>• Συμβάλλει στη διατήρηση των καταγεγραμμένων αποτρεπτικών παραγόντων.</li> <li>• Διασφαλίζει ότι τα ζητήματα που επηρεάζουν την ανάπτυξη εντοπίζονται και επιλύονται.</li> </ul>

Πίνακας 3 - Αναφορά του Scrum Master

## Scrum Team Report

Member	Χρήστος Μπάντης
Responsibilities	<ul style="list-style-type: none"> <li>• Δέσμευση πως τα user stories θα γίνονται εντός sprint (επαναλαμβανόμενο σταθερό χρονικό πλαίσιο).</li> <li>• Εντοπισμός κινδύνων και υλοποίηση δράσεων μετριασμού πιθανών σφαλμάτων.</li> <li>• Πλήρης ανάπτυξη του προϊόντος ή της υπηρεσίας.</li> <li>• Ανάπτυξη του ιδιωτικού δικτύου Blockchain.</li> <li>• Συγγραφή του κώδικα των «έξυπνων» συμβολαίων.</li> <li>• Σχεδίαση και ανάπτυξη του περιβάλλοντος χρήστη της εφαρμογής.</li> <li>• Συνεχής δοκιμή των λειτουργιών της εφαρμογής.</li> </ul>

Πίνακας 4 - Αναφορά ομάδας Scrum

## Project Charter

Ένα καταστατικό έργου (Project Charter) αναπαριστά ένα επίσημο, συνήθως σύντομο έγγραφο που προσδιορίζει το έργο στην πληρότητά του. (Wrike, 2019).

## 1. Project Vision

Το έργο οραματίζεται ότι θα μέλλον όπου η ενσωμάτωση ιδιωτικών blockchain και εφαρμογών chain of custody μεταμορφώνει το τοπίο της ψηφιακής εγκληματολογίας. Συνδυάζοντας άψογα την ασφάλεια και τη διαφάνεια του ιδιωτικού Ethereum Blockchain με τις σχολαστικές δυνατότητες παρακολούθησης που προσφέρουν οι εφαρμογές chain of custody, το έργο στοχεύει στη δημιουργία ενός νέου παραδείγματος εμπιστοσύνης στη διαχείριση ψηφιακών αποδεικτικών στοιχείων. Το όραμα αυτό περιλαμβάνει εξορθολογισμένες εγκληματολογικές διαδικασίες και αυξημένο επίπεδο εμπιστοσύνης στην αξιοπιστία και την αυθεντικότητα των ψηφιακών αποδεικτικών στοιχείων που παρουσιάζονται σε νομικά πλαίσια.

## 2. Project Mission

Μέσω της ανάπτυξης ενός ιδιωτικού Ethereum Blockchain και μιας αποκεντρωμένης εφαρμογής chain of custody, το έργο στοχεύει στην ενίσχυση της ακεραιότητας, της ιχνηλασμότητας και της ασφάλειας των ψηφιακών αποδεικτικών στοιχείων καθ' όλη τη διάρκεια του κύκλου ζωής του. Αξιοποιώντας την αμεταβλητότητα και τη διαφάνεια της τεχνολογίας blockchain, το έργο επιδιώκει να συμβάλει στην προώθηση ισχυρών ψηφιακών εγκληματολογικών πρακτικών, ενισχύοντας την αξιοπιστία των αποδεικτικών στοιχείων σε νομικές διαδικασίες και ενισχύοντας τη διαδικαστική συνεργασία μεταξύ των υπηρεσιών επιβολής του νόμου.

## 3. Project Success Criteria

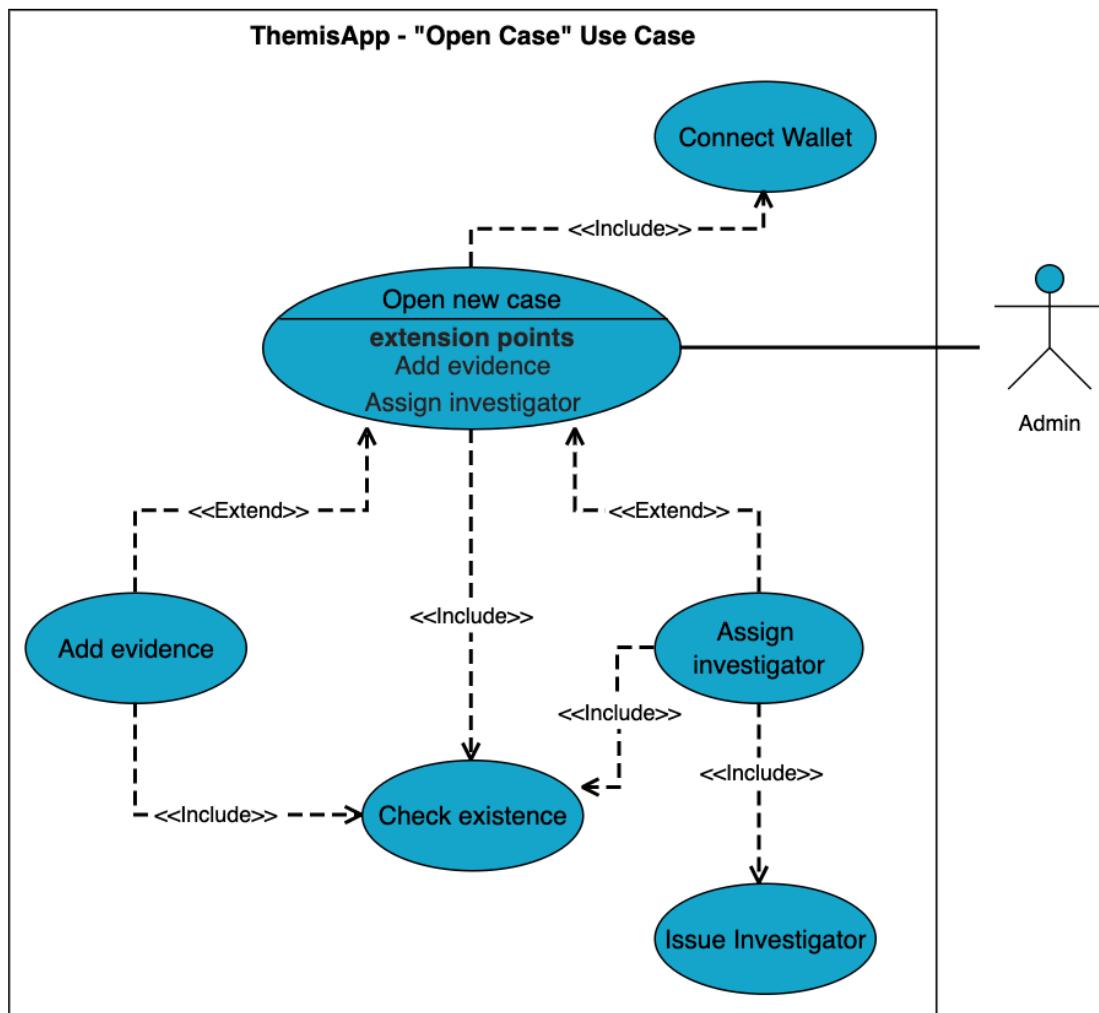
Η επιτυχία του έργου θα αξιολογηθεί με βάση ένα σύνολο προκαθορισμένων κριτηρίων. Αυτά περιλαμβάνουν την επιτυχή ανάπτυξη ενός ιδιωτικού Ethereum Blockchain, και μιας αποκεντρωμένης εφαρμογής Chain of Custody. Τα επιτεύγματα του έργου θα είναι εμφανή μέσω αποδεδειγμένων βελτιώσεων στην ακεραιότητα, τη διαφάνεια και την ασφάλεια της διαχείρισης ψηφιακών αποδεικτικών στοιχείων. Επιπλέον, η επιτυχής προσαρμογή των αναπτυγμένων λύσεων στις πρακτικές ροές εργασίας των επαγγελματιών ψηφιακής εγκληματολογίας και των υπηρεσιών επιβολής του νόμου θα αποτελέσει βασικό δείκτη επιτυχίας. Τέλος, η επιτυχία του έργου θα αντικατοπτρίζεται στη συμβολή του στην προώθηση της αξιοπιστίας των ψηφιακών αποδεικτικών στοιχείων σε νομικές διαδικασίες, στην προώθηση των συνεργατικών

προσπαθειών μεταξύ των ενδιαφερομένων και στην ενίσχυση της συνολικής αποτελεσματικότητας των πρακτικών ψηφιακής εγκληματολογίας.

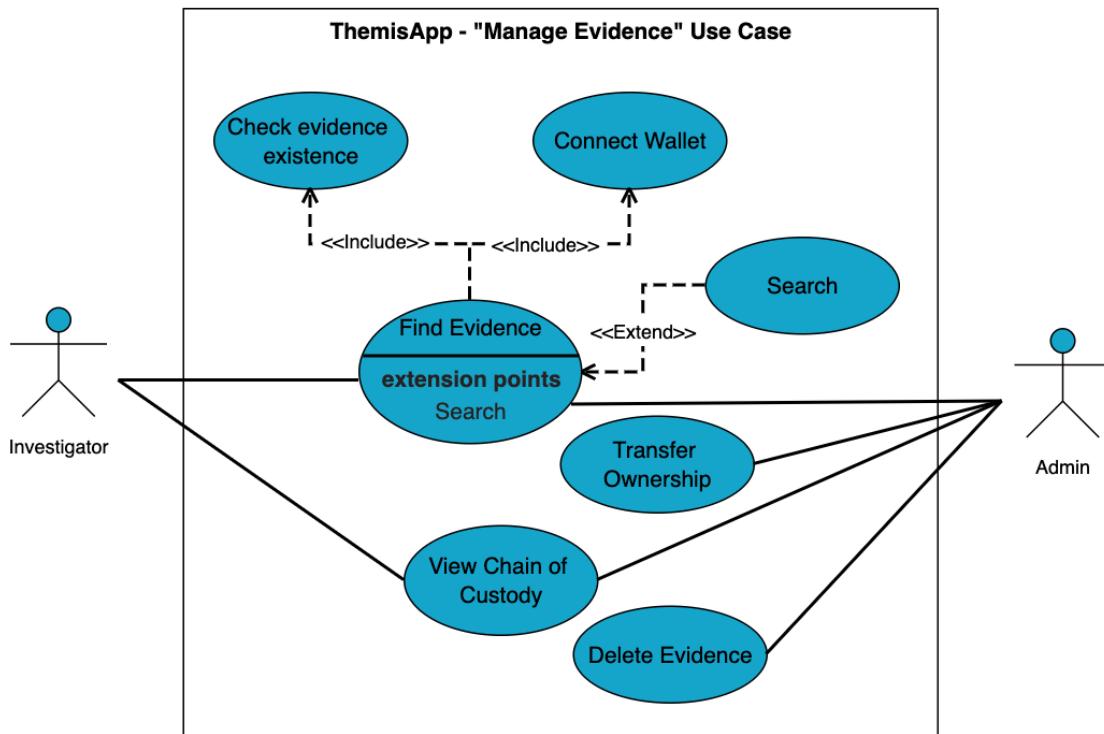
## Use Case Report

### 1. Use Case Diagram

Στα παρακάτω διαγράμματα περίπτωσης χρήσης (Use Case Diagrams) παρουσιάζονται ενδεικτικά, οι περιπτώσεις δημιουργίας («ανοίγματος») μιας νέας υπόθεσης (Εικόνα 9) και διαχείρισης αποδεικτικών στοιχείων (Εικόνα 10).



Εικόνα 9 - Διαγράμματα περίπτωσης χρήσης δημιουργίας («ανοίγματος») μιας νέας υπόθεσης



Εικόνα 10 - Διαγράμματα περίπτωσης χρήσης διαχείρισης αποδεικτικών στοιχείων

## 2. Prioritized Use Cases

Η ιεράρχηση περιπτώσεων χρήσης είναι μια προσέγγιση μέσω της οποίας οι οργανισμοί μπορούν να προσδιορίσουν πιθανά σενάρια χρήσης, να αξιολογήσουν την επιχειρηματική σημασία που προκύπτει από αυτά και να τα οργανώσουν κατά σειρά επιρροής στους στρατηγικούς τους στόχους (Mishra, 2021). Στον πίνακα που ακολουθεί, η στήλη «Priority» υποδηλώνει τη σημασία των σεναρίων για την παροχή ουσιαστικών και άμεσων επιχειρηματικών πλεονεκτημάτων. Η στήλη «Size» περιλαμβάνει μια υποκειμενική αξιολόγηση των πόρων που απαιτούνται για τη υποστήριξη κάθε σεναρίου, ενώ η στήλη «Complexity» περιλαμβάνει ένα υποκειμενικό μέτρο αξιολόγησης της πολυπλοκότητας που σχετίζεται με την υποστήριξη κάθε σεναρίου.

Name	Description	Priority	Size	Complexity
Connect Wallet	Ο χρήστης συνδέεται στην εφαρμογή μέσω του	Must	Very Small	Low

	ψηφιακού «πορτοφολιού» του.			
Find Evidence	Ο χρήστης (investigator / admin) διαχειρίζεται το αποδεικτικό στοιχείο που επιθυμεί.	Should	Medium	Medium
View Chain of Custody	Ο χρήστης (investigator / admin) αποκτά πρόσβαση στο chain of custody του αποδεικτικού στοιχείου.	Could	Medium	Medium
Add evidence	Ο admin προσθέτει ένα ή περισσότερα αποδεικτικά στοιχεία σε μία υπόθεση.	Must	Medium	Medium
Transfer ownership	Ο admin μεταβιβάζει την κυριότητα του αποδεικτικού στοιχείου σε άλλον ερευνητή.	Could	Small	Low
Close case	Ο admin κλείνει και διαγράφει μια υπόθεση.	Must	Medium	Low
Check evidence existence	Ο admin ελέγχει για την ύπαρξη ενός αποδεικτικού στοιχείου.	Must	Medium	Medium
Check existence	Ο admin ελέγχει αν υπάρχει εγγεγραμμένος ερευνητής με την ίδια διεύθυνση ή αν υπάρχει ήδη αυτός ο ερευνητής στην υπόθεση.	Must	Medium	Low
Remove investigator	Ο admin αφαιρεί έναν ερευνητή από το blockchain ή από μία υπόθεση.	Must	Small	Medium

Delete evidence	O admin διαγράφει ένα αποδεικτικό στοιχείο από μια υπόθεση.	Should	Medium	Medium
Issue investigator	O admin δημιουργεί μια ταυτότητα για έναν νέο ερευνητή.	Must	Medium	Low
Open new case	O admin ανοίγει μια νέα υπόθεση.	Must	Medium	Low
Assign case to investigator	O admin αναθέτει την υπόθεση σε έναν ή περισσότερους ερευνητές.	Must	Medium	Medium
Read case description	Εμφάνιση της περιγραφής μιας υπόθεσης.	Should	Small	Low
View active cases	Εμφάνιση της λίστας των υποθέσεων που έχουν ανατεθεί στον συνδεμένο ερευνητή / admin.	Should	Medium	Low
Manage investigators	Εμφάνιση της λίστας των εγγεγραμμένων ερευνητών.	Should	Small	Low

Πίνακας 5 - Ιεράρχηση περιπτώσεων χρήσης (Use Case Prioritization)

## Epics Report

Τα «Epics» αντιπροσωπεύουν ένα αυξημένο επίπεδο λειτουργικότητας ή γενικά περιγραφόμενες προϋποθέσεις, ενώ μπορούν να κατακερματιστούν σε πιο διαχειρίσιμες μονάδες που ονομάζονται «User Stories» (Sinha, 2023). Στον παρακάτω πίνακα, η στήλη «Priority» δείχνει τον βαθμό σημαντικότητας των «epics» σχετικά με την παροχή ουσιαστικών και άμεσων επιχειρηματικών οφελών, ενώ η στήλη «Risk» υποδηλώνει το επίπεδο αβεβαιότητας όσον αφορά την επιτυχή ολοκλήρωση ενός «epic».

Name	Description	Parent Use Case	Priority	Risk
Σύνδεση στην εφαρμογή	Εμφάνιση παραθύρου διαλόγου για τη σύνδεση του ερευνητή ή του admin μέσω της εφαρμογής «πορτοφολιού» που διαθέτει.	Connect Wallet	Must	Low
Προσθήκη αποδεικτικού στοιχείου σε υπόθεση	Εμφάνιση παραθύρου προσθήκης αποδεικτικού στοιχείου σε υπόθεση.	Add Evidence	Must	High
Προβολή περιγραφής υπόθεσης	Εμφάνιση παραθύρου περιγραφής υπόθεσης.	Read case description	Should	Low
Μεταβίβαση κυριότητας αποδεικτικού στοιχείου	Εμφάνιση παραθύρου μεταβίβασης κυριότητας αποδεικτικού στοιχείου.	Transfer ownership	Must	High
Κλείσιμο/Διαγραφή υπόθεσης	Εμφάνιση παραθύρου επιβεβαίωσης διαγραφής υπόθεσης.	Close case	Should	Medium
Καταχώριση νέου ερευνητή	Εμφάνιση παραθύρου συναλλαγής για την καταχώριση νέου ερευνητή.	Issue investigator	Must	High
Καταχώριση νέας υπόθεσης	Εμφάνιση παραθύρου συναλλαγής για την καταχώριση νέας υπόθεσης.	Open new case	Must	High

Εμφάνιση σφάλματος	Ενημέρωση του χρήστη σε περίπτωση σφάλματος κατά την εκτέλεση της εφαρμογής ή των συναλλαγών με το blockchain.	Show error	Should	Low
Εμφάνιση ενεργών υποθέσεων	Εμφάνιση λίστας ενεργών υποθέσεων συνδεμένου ερευνητή / admin.	View active cases	Should	Medium
Εμφάνιση chain of custody	Εμφάνιση του chain of custody ενός αποδεικτικού στοιχείου.	View Chain of Custody	Must	High
Διαχείριση καταχωρημένων ερευνητών	Εμφάνιση λίστας καταχωρημένων ερευνητών.	Manage investigators	Must	Medium
Διαχείριση αποδεικτικών στοιχείων	Αναζήτηση αποδεικτικών στοιχείων βάσει υπόθεσης.	Find evidence	Must	High
Διαγραφή αποδεικτικού στοιχείου	Διαγραφή του αποδεικτικού στοιχείου από την υπόθεση.	Delete evidence	Should	Medium
Αφαίρεση ερευνητή	Εμφάνιση παραθύρου πληκτρολόγησης διεύθυνσης ερευνητή προς αφαίρεση από το blockchain ή την υπόθεση.	Remove investigator	Must	Low

Ανάθεση υπόθεσης σε ερευνητή	Εμφάνιση παραθύρου πληκτρολόγησης διεύθυνσης ερευνητή για την ανάθεση της υπόθεσης.	Assign case to investigator	Should	Medium
Έλεγχος ύπαρξης ερευνητή / αποδεικτικού στοιχείου	Έλεγχος αν ο ερευνητής υπάρχει καταχωρημένος στο blockchain ή στην υπόθεση / Έλεγχος αν υπάρχει ήδη το αποδεικτικό στοιχείο στην υπόθεση.	Check existence	Must	Medium

Πίνακας 6 - Αναφορά των «Epics»

## Product Backlog

Το «Product Backlog» είναι ένας δυναμικός, οργανωμένος κατάλογος που περιλαμβάνει όλα τα στοιχεία που είναι απαραίτητα για τη βελτίωση ενός έργου (Scrum.org, n.d.).

### 1. User Story Map

Η χαρτογράφηση ιστοριών χρήστη (User Story Mapping) είναι μια απλή τεχνική σχεδιασμού, που περιγράφει τα – αναμενόμενα από την ομάδα «Scrum» – βήματα που ακολουθούν οι χρήστες για να επιτύχουν τους στόχους τους κατά τη χρήση ενός ψηφιακού προϊόντος (Kaley, 2021).

Connect Wallet	Find Evidence	Transfer ownership	View Chain of Custody	Delete evidence	Open new case	Add evidence	Assign case to investigator
Σύνδεση στην εφαρμογή	Διαχείριση αποδεικτικού στοιχείου	Μεταβίβαση κυριότητας από στοιχείου	Εμφάνιση chain of custody	Διαγραφή αποδεικτικού στοιχείου	Καταχώριση νέας υπόθεσης	Προσθήκη απ. στοιχείου σε υπόθεση	Ανάθεση υπόθεσης σε ερευνητή

Release 1 07/12/2023



Εμφάνιση πάραθυρου σύνδεσης

Ανάπτυξη μεθόδου διαγραφής

Ανάπτυξη μεθόδου καταχώρισης

Ανάπτυξη μεθόδου προσθήκης α.σ.

Προσθήκη ερευνητή βάσει διεύθυνσης

Release 2 07/19/2023



Ανάπτυξη μεθόδου εύρεσης απ.σ.

Ανάπτυξη μεθόδου μεταβίβασης

Ανάπτυξη μεθόδου συλλογής δεδ.

Eikόνα 11 - User Story Map (1/2)

Check existence	Issue investigator	View active cases	Read case description	Manage investigators	Remove investigator	Close case	Show error
Έλεγχος ύπαρξης ερευνητή - α.σ.	Καταχώριση νέου ερευνητή	Εμφάνιση ενεργών υπόθεσεων	Προβολή περιγραφής υπόθεσης	Διαχείριση εγγεγραμμένων ερευνητών	Αφαίρεση ερευνητή	Κλείσιμο ή διαγραφή υπόθεσης	Εμφάνιση σφάλματος

Αναζήτηση στην μνήμη του smart contract	Ανάπτυξη μεθόδου προσθήκης ερ.	Εμφάνιση πάραθυρου περιγραφής	Ανάπτυξη μεθόδου αφαίρεσης ερ.	Ανάπτυξη μεθόδου διαγραφής υπ.	Χρήση μεθόδου alert της Javascript
---	--------------------------------	-------------------------------	--------------------------------	--------------------------------	------------------------------------

Ανάπτυξη μεθόδου συλλογής υποθ

Ανάπτυξη μεθόδου συλλογής ερευ.

Eikόνα 12 - User Story Map (2/2)

## 2. Prioritized User Stories

Η ιεράρχηση των «User Stories» ακολουθεί τη συλλογική σύμβαση μεταξύ των μελών της ομάδας Scrum, σχετικά με τη οργάνωση των χαρακτηριστικών του έργου. Αυτή η οργάνωση ξεκινά με τα χαρακτηριστικά υψηλότερης προτεραιότητας, εξασφαλίζοντας την ταχεία κυκλοφορία του έργου στην αγορά (CardBoard, 2020).

Κάθε «User Story» συνοδεύεται από σχετικά κριτήρια αποδοχής (Acceptance Criteria), που χρησιμεύουν ως σημεία αναφοράς για την εκπλήρωσή του. Αυτά τα κριτήρια προσφέρουν σαφήνεια στην ομάδα σχετικά με τα αναμενόμενα αποτελέσματα ενός «user story», εξαλείφοντας τις αβεβαιότητες από τις απαιτήσεις και συμβάλλοντας στη διαμόρφωση σαφών προσδοκιών. Οι «πόντοι» της ιστορίας (Story Points) αποτελούν μια αριθμητική αναπαράσταση που υποδεικνύει το εκτιμώμενο «μέγεθος» μιας ιστορίας χρήστη. Η αξιολόγηση του μεγέθους μιας ιστορίας χρήστη λαμβάνει

υπόψη παράγοντες όπως ο κίνδυνος, η απαιτούμενη προσπάθεια και το επίπεδο πολυπλοκότητας.

Name	Description	Epic	Status	Acceptance Criteria	Story Points	Priority	Risk
Εμφάνιση παραθύρου σύνδεσης	Ως χρήστης, επιθυμώ να συνδέομαι αμέσα και εύκολα στην εφαρμογή.	Σύνδεση στην εφαρμογή	Approved	Κατά την επίσκεψη στην εφαρμογή θα πρέπει να εμφανίζεται αυτόματα το παράθυρο σύνδεσης στην εφαρμογή.	1	Must	Low
Ανάπτυξη μεθόδου εύρεσης αποδεικτικού στοιχείου	Ως χρήστης, επιθυμώ να αναζητώ το αποδεικτικό στοιχείο που με ενδιαφέρει, βάσει του αριθμού της υπόθεσης στην οποία ανήκει.	Διαχείριση αποδεικτικών στοιχείων	Approved	Ανάπτυξη μεθόδου κατά την οποία θα πραγματοποιείται αναζήτηση βάσει του αριθμού υπόθεσης και θα εμφανίζονται τα αποδεικτικά στοιχεία που ανήκουν σε αυτήν.	3	Must	High
Ανάπτυξη μεθόδου μεταβίβασης κυριότητας αποδεικτικών στοιχείων	Ως admin, επιθυμώ να μεταβιβάζω την κυριότητα ενός ή περισσοτέρων αποδεικτικών στοιχείων σε άλλους ερευνητές.	Μεταβίβαση κυριότητας αποδεικτικού στοιχείου	Approved	Ανάπτυξη μεθόδου κατά την οποία θα πραγματοποιείται μεταβίβαση της κυριότητας ενός ή περισσοτέρων αποδεικτικών στοιχείων, κάνοντας χρήση των διευθύνσεων των ερευνητών.	4	Must	High

Ανάπτυξη μεθόδου συλλογής δεδομένων αποδεικτικών στοιχείων	Ως χρήστης. επιθυμώ να ελέγχω το chain of custody ενός ή περισσοτέρων αποδεικτικών στοιχείων.	Εμφάνιση chain of custody	Approved	Ανάπτυξη μεθόδου κατά την οποία θα προβάλλεται το chain of custody των ζητούμενων αποδεικτικών στοιχείων.	4	Must	High
Ανάπτυξη μεθόδου διαγραφής αποδεικτικών στοιχείων	Ως admin, επιθυμώ να έχω τη δυνατότητα διαγραφής ενός ή περισσοτέρων αποδεικτικών στοιχείων.	Διαγραφή αποδεικτικού στοιχείου	Approved	Ανάπτυξη μεθόδου διαγραφής ενός ή περισσοτέρων αποδεικτικών στοιχείων από μία υπόθεση.	3	Must	Medium
Ανάπτυξη μεθόδου καταχώρισης νέας υπόθεσης	Ως admin, επιθυμώ να έχω τη δυνατότητα καταχώρισης μιας νέας υπόθεσης.	Καταχώριση νέας υπόθεσης	Approved	Ανάπτυξη μεθόδου καταχώρισης νέας υπόθεσης στο blockchain.	4	Must	High
Ανάπτυξη μεθόδου προσθήκης αποδεικτικών στοιχείων	Ως admin, επιθυμώ να έχω τη δυνατότητα να προσθέτω ένα ή περισσότερα αποδεικτικά στοιχεία σε μία υπόθεση.	Προσθήκη αποδεικτικού στοιχείου σε υπόθεση	Approved	Ανάπτυξη μεθόδου προσθήκης ενός ή περισσοτέρων αποδεικτικών στοιχείων σε μία υπόθεση.	4	Must	High
Προσθήκη ερευνητή βάσει διεύθυνσης	Ως admin, επιθυμώ να έχω τη δυνατότητα να προσθέτω	Ανάθεση υπόθεσης σε ερευνητή	Approved	Εμφάνιση επιλογής προσθήκης ερευνητή κατά την	3	Must	High

	έναν ερευνητή σε μία υπόθεση βάσει της διεύθυνσης πορτοφολιού του.			διαχείριση μιας υπόθεσης.			
Αναζήτηση στη μνήμη του «έξυπνου» συμβολαίου	Ως admin, επιθυμώ να ελέγχω την ύπαρξη ενός ερευνητή ή ενός αποδεικτικού στοιχείου πριν προβώ σε οποιαδήποτε σχετική ενέργεια.	Έλεγχος ύπαρξης ερευνητή / αποδεικτικού στοιχείου	Approved	Έλεγχος της διεύθυνσης του ερευνητή ή του hash του αποδεικτικού στοιχείου πριν εκτελεστεί οποιαδήποτε ενέργεια.	3	Must	Medium
Ανάπτυξη μεθόδου καταχώρησης νέου ερευνητή	Ως admin, επιθυμώ να έχω τη δυνατότητα να προσθέτω νέο ερευνητή στο blockchain.	Καταχώριση νέου ερευνητή	Approved	Ανάπτυξη μεθόδου καταχώρησης νέου ερευνητή στο blockchain.	4	Must	High
Ανάπτυξη μεθόδου συλλογής ενεργών υποθέσεων ανά ερευνητή	Ως χρήστης, επιθυμώ να ελέγχω τις ενεργές υποθέσεις που μου έχουν ανατεθεί.	Εμφάνιση ενεργών υποθέσεων	Approved	Ανάπτυξη μεθόδου εμφάνισης των ενεργών υποθέσεων ανά ερευνητή.	3	Should	Medium
Εμφάνιση παραθύρου	Ως χρήστης, επιθυμώ να προβάλω την	Προβολή περιγραφής υπόθεσης	Approved	Εμφάνιση επιλογής προβολής της	2	Should	Low

περιγραφής υπόθεσης	περιγραφή μιας υπόθεσης.			περιγραφής μιας υπόθεσης.			
Χρήση μεθόδου alert της Javascript	Ως χρήστης, επιθυμώ να ενημερώνομαι για οποιοδήποτε σφάλμα προκύπτει κατά τη χρήση της εφαρμογής ή κατά της εκτέλεση οποιασδήποτε συναλλαγής με το blockchain.	Εμφάνιση σφάλματος	Approved	Εμφάνιση μηνύματος για οποιουδήποτε είδους σφάλμα προκύψει.	1	Should	Low
Ανάπτυξη μεθόδου διαγραφής υπόθεσης	Ως admin, επιθυμώ να έχω τη δυνατότητα διαγραφής οποιασδήποτε υπόθεσης.	Κλείσιμο/Δια γραφή υπόθεσης	Approved	Εμφάνιση επιλογής διαγραφής υπόθεσης κατά την διαχείριση υποθέσεων.	3	Should	Medium
Ανάπτυξη μεθόδου αφαίρεσης ερευνητή	Ως admin, επιθυμώ να έχω τη δυνατότητα αφαίρεσης ερευνητή από μία υπόθεση ή από το blockchain.	Αφαίρεση ερευνητή	Approved	Εμφάνιση επιλογής αφαίρεσης ερευνητή κατά τη διαχείριση των διαθέσιμων ερευνητών ή κατά τη διαχείριση μιας υπόθεσης.	3	Must	Medium

Πίνακας 7 - Ιεράρχηση ιστοριών χρήστη (User Stories Prioritization)

## Release Plan

Ένα σχέδιο κυκλοφορίας παρέχει στην ομάδα «Scrum» μια ολοκληρωμένη άποψη για τις προγραμματισμένες κυκλοφορίες του έργου και το σχετικό χρονοδιάγραμμα παράδοσής του. Αυτό εξασφαλίζει την συμμόρφωση με τις προσδοκίες του ιδιοκτήτη του έργου και επιτρέπει την αποτελεσματικότερη ανάπτυξή του.

### 1. Project Deliverables

Ένα παραδοτέο (Deliverable) αναφέρεται σε ένα υλικό ή άνλο προϊόν ή υπηρεσία που προορίζεται για ανάπτυξη στο πλαίσιο ενός έργου.

Deliverable	Description	Planned Release Date	Priority	Status	Owner
Ιδιωτικό Ethereum Blockchain και αποκεντρωμένη εφαρμογή Chain of Custody	Μοντέλο ιδιωτικού blockchain και αποκεντρωμένης εφαρμογής chain of custody, με σκοπό την διαχείριση αποδεικτικών στοιχείων ψηφιακής εγκληματολογίας.	2023-06-25	High	Done	Χρήστος Μπάντης

Πίνακας 8 - Παραδοτέα έργου (Project Deliverables)

### 2. Release Configuration

Release	Description	Planned Release Date
Release 1	Πλήρως λειτουργικό ιδιωτικό Ethereum Blockchain, υπό την ονομασία «ThemisChain», ανεπτυγμένο στην πλατφόρμα cloud «AWS».	2023-07-05

Release 2	Πλήρως λειτουργική αποκεντρωμένη εφαρμογή chain of custody, βασιζόμενη στο ιδιωτικό δίκτυο «ThemisChain», σύμφωνα με το μοντέλο που παρουσιάστηκε στο παραδοτέο.	2023-07-12
Release 3	Εμπλουτισμός της εφαρμογής με νέες λειτουργίες και μετονομασία της σε «ThemisApp».	2023-07-19

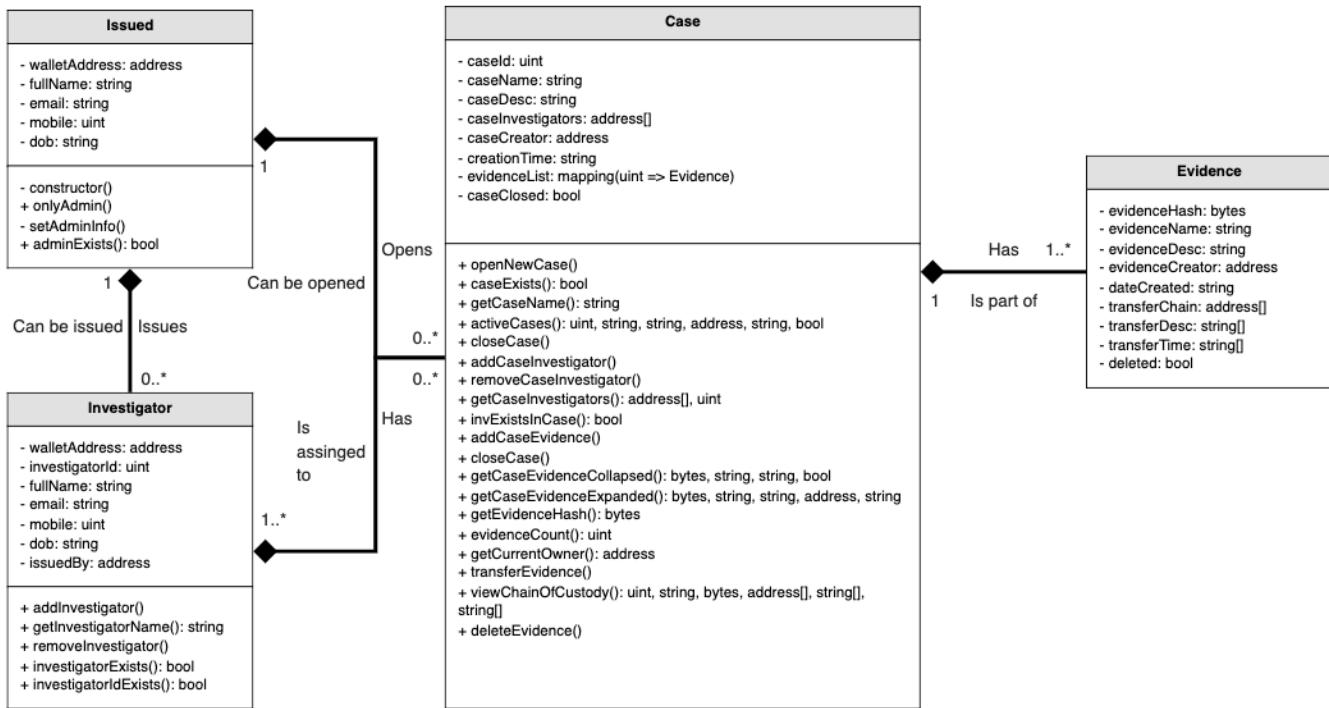
*Πίνακας 9 - Κυκλοφορίες - Εκδόσεις έργου (Project Releases)*

## 5.1. Μοντελοποίηση

Η μοντελοποίηση εφαρμογών είναι ένα κρίσιμο βήμα στον κύκλο ζωής ανάπτυξης λογισμικού, που χρησιμεύει ως γέφυρα μεταξύ σύλληψης και υλοποίησης. Τα διαγράμματα «UML» (Unified Modeling Language) παρέχουν έναν τυποποιημένο και οπτικό τρόπο αναπαράστασης των διαφόρων πτυχών της δομής, της συμπεριφοράς και των αλληλεπιδράσεων μιας εφαρμογής (Lucidchart, 2019). Μέσω των διαγραμμάτων «UML», οι προγραμματιστές μπορούν να δημιουργήσουν μια σταθερή βάση για τη δημιουργία επιτυχημένων και φιλικών προς το χρήστη εφαρμογών. Κάθε τύπος διαγράμματος «UML» διαδραματίζει μοναδικό ρόλο στη διασφάλιση μιας ολοκληρωμένης και καλά οργανωμένης διαδικασίας ανάπτυξης εφαρμογών.

### 1. Διάγραμμα Κλάσης (Class Diagram)

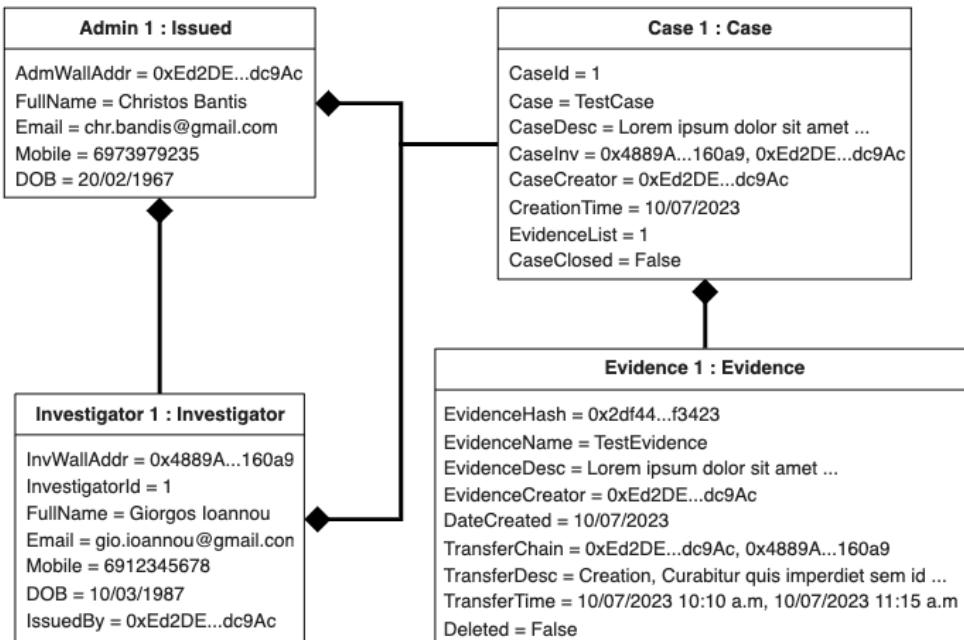
Στο παρακάτω διάγραμμα κλάσης (Εικόνα 13) παρουσιάζεται η δομή της εφαρμογής – κλάσεις, οι απαραίτητες μεταβλητές και μέθοδοι, όπως και η μεταξύ τους σχέση παράλληλα με τον λόγο πληθικότητάς τους. Να σημειωθεί πως, ένα θεμελιώδες γνώρισμα της γλώσσας προγραμματισμού «Solidity», που αξιοποιήθηκε για την ανάπτυξη των «έξυπνων» συμβόλαιών, είναι ότι δεν απαιτείται η υλοποίηση μεθόδων «getter» (μέθοδος που επιστρέφει την τιμή μιας μεταβλητής), καθώς θεωρούνται δεδομένες κατά τη δημιουργία μιας μεταβλητής.



Εικόνα 13 - Διάγραμμα Κλάσης (Class Diagram)

## 2. Διάγραμμα Αντικειμένου (Object Diagram)

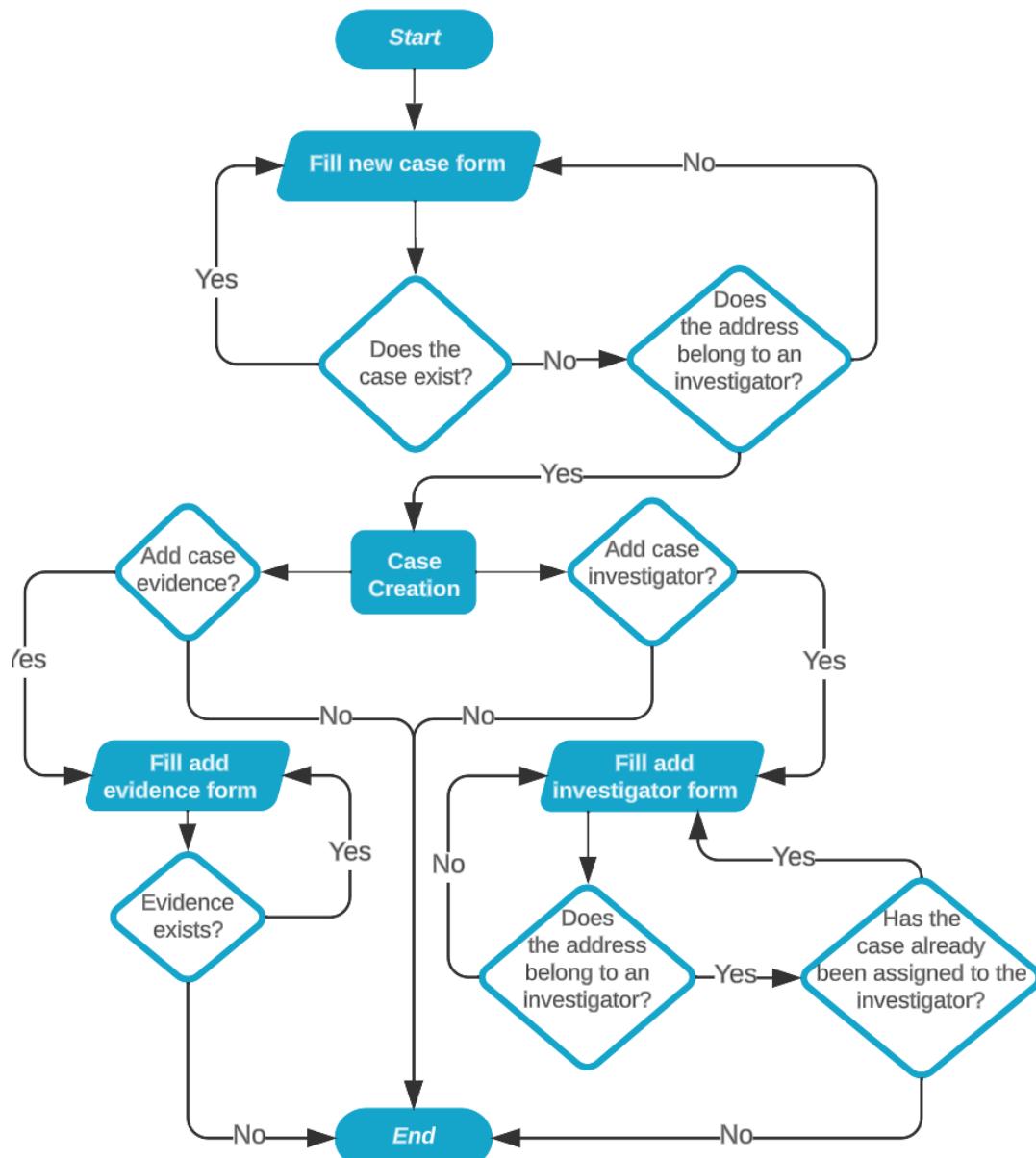
Όσα αναφέρονται στην παραπάνω παράγραφο, καθίστανται ορατά και στο διάγραμμα αντικειμένου της Εικόνας 14, το οποίο ενσωματώνει μια πλήρη περίπτωση χρήσης με πραγματικά δεδομένα, επαληθεύοντας την αρτιότητα του διαγράμματος κλάσης.



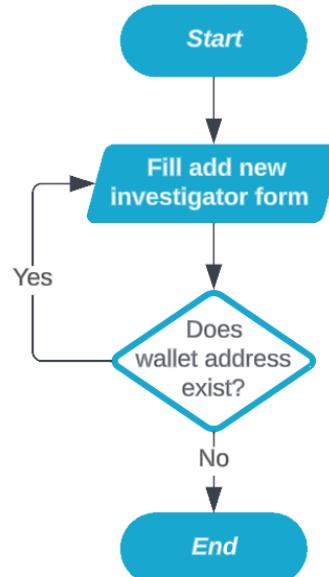
Εικόνα 14 - Διάγραμμα Αντικειμένου (Object Diagram)

### 3. Διαγράμματα Ροής (Flowcharts)

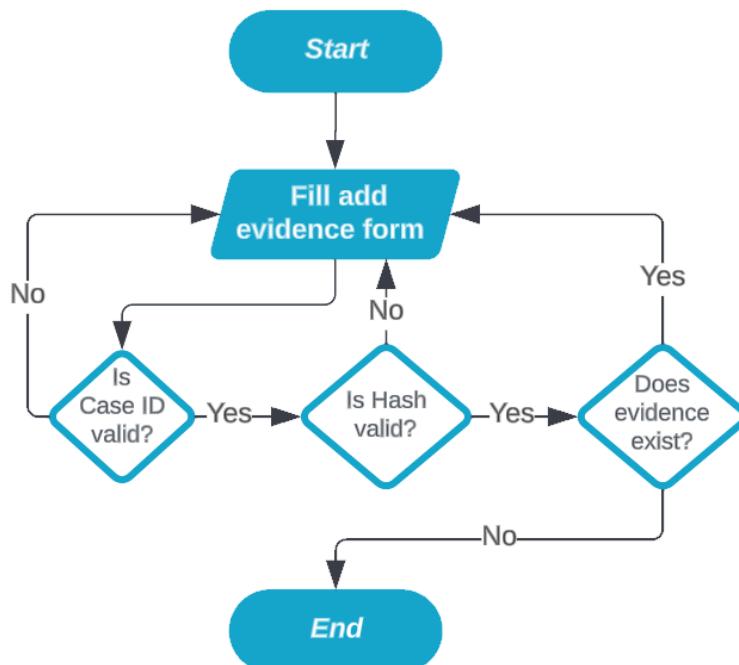
Τα διαγράμματα ροής που ακολουθούν, αντιπροσωπεύουν την απλότητα της σειράς των βημάτων και των αποφάσεων που λαμβάνονται κατά την εκτέλεση των διαδικασιών που απεικονίζουν. Αναλυτικότερα, το διάγραμμα ροής της Εικόνας 15 οπτικοποιεί τη ροή των δεδομένων και των ελέγχων κατά τη δημιουργία μιας νέας υπόθεσης, ενώ τα διαγράμματα ροής των Εικόνων 16 και 17 αφορούν τη καταχώριση ενός νέου ερευνητή και την προσθήκη ενός αποδεικτικού στοιχείου αντίστοιχα.



Εικόνα 15 - Διάγραμμα Ροής δημιουργίας νέας υπόθεσης (Open new case Flowchart)



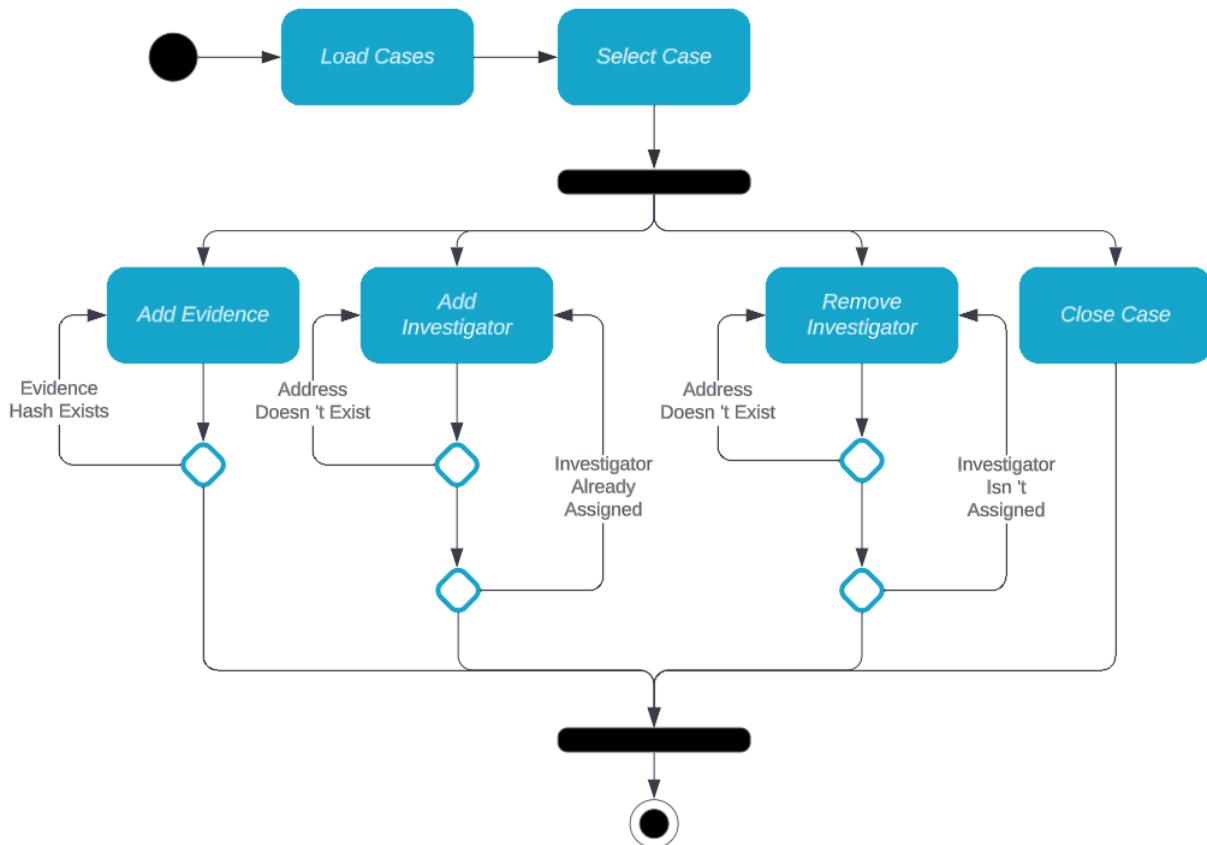
Εικόνα 16 - Διάγραμμα Ροής καταχώρισης νέου ερευνητή (Add new investigator Flowchart)



Εικόνα 17 - Διάγραμμα Ροής προσθήκης αποδεικτικού στοιχείου (Add evidence Flowchart)

#### 4. Διάγραμμα Δραστηριότητας (Activity Diagram)

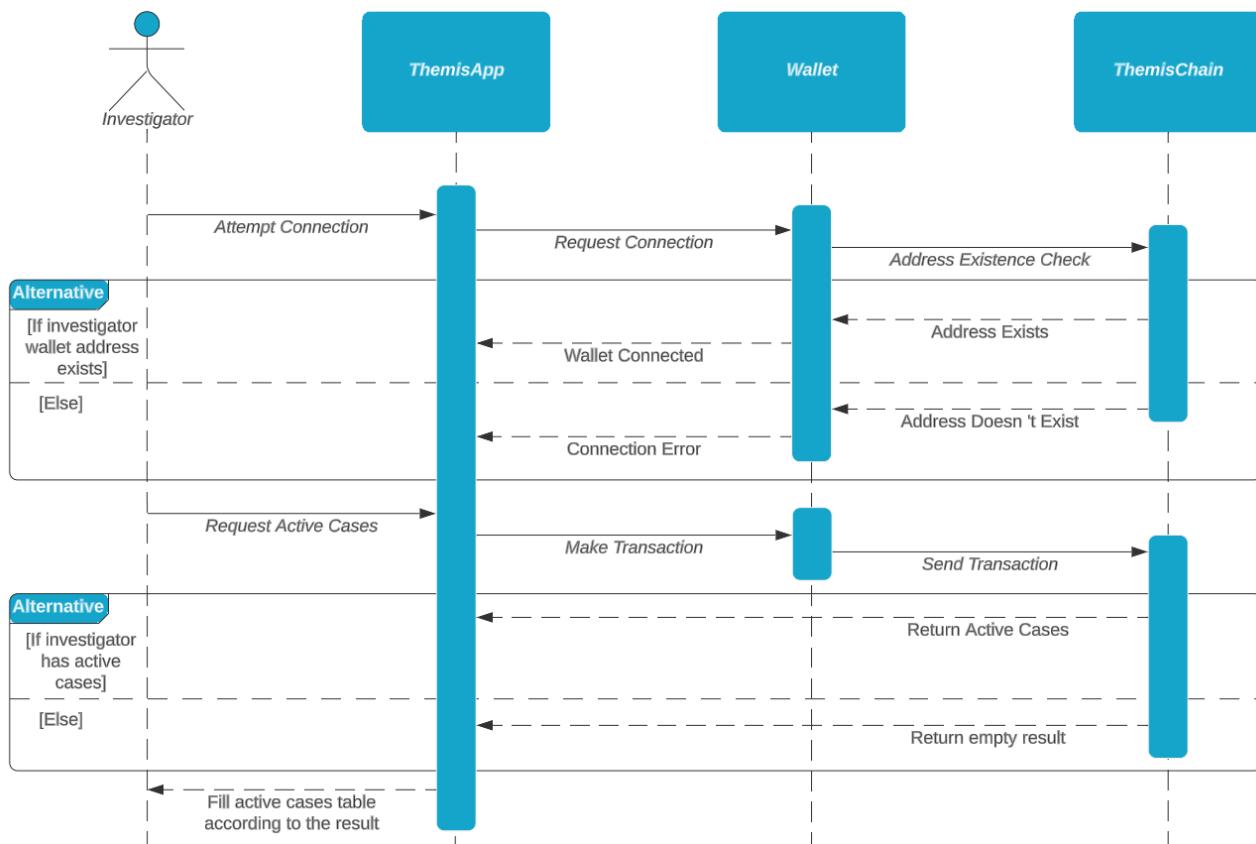
Το διάγραμμα δραστηριότητας της Εικόνας 18 παρουσιάζει ενδεικτικά, τον τρόπο σύνδεσης των δραστηριοτήτων και των ενεργειών που πραγματοποιούνται κατά τη διαδικασία διαχείρισης των υποθέσεων που είναι καταγεγραμμένες στο blockchain.



Εικόνα 18 - Διάγραμμα Δραστηριότητας διαχείρισης υποθέσεων (Manage cases Activity Diagram)

## 5. Διάγραμμα Ακολουθίας (Sequence Diagram)

Το παρακάτω διάγραμμα ακολουθίας (Εικόνα 19) παρέχει μια οπτική αναπαράσταση της διαδικασίας προβολής των ενεργών υποθέσεων του συνδεμένου ερευνητή και εξυπηρετεί στην κατανόηση της ροής των μηνυμάτων και της αλληλεπίδρασης μεταξύ των αντικειμένων που αποτελούν το υπόβαθρο της εφαρμογής. Ομοίως με την προαναφερθείσα διαδικασία, το παρόν διάγραμμα χαρακτηρίζει το σύνολο των περιπτώσεων χρήσης της εφαρμογής.



Εικόνα 19 - Διάγραμμα Ακολουθίας προβολής ενεργών υποθέσεων (Active cases Sequence Diagram)

## 5.2. Σχεδιασμός

Στο υποκεφάλαιο αυτό παρουσιάζεται ένας συνδυασμός προσχεδίων και μακετών, με σκοπό να αποτυπωθεί η προσχεδιασμένη διάταξη, ο τρόπος πλοήγησης και η συνολική αισθητική της εφαρμογής. Τα προσχέδια (mockups) παρουσιάζουν μια στατική αναπαράσταση μερικών από τα σημαντικότερα περιβάλλοντα χρήστη της εφαρμογής, τα οποία κατά σειρά είναι: Ανοιχτήση αποδεικτικού στοιχείου (Εικόνα 20), Δημιουργία νέας υπόθεσης (Εικόνα 21), Διαχείριση υποθέσεων (Εικόνα 22) και Προφίλ ερευνητή (Εικόνα 23). Κατ’ αυτόν τον τρόπο, επισημαίνονται τα βασικά στοιχεία σχεδίασης όπως είναι η διάταξη του περιεχομένου, τα κουμπιά και η τοποθέτηση του κειμένου. Ακολούθως, η μακέτα (wireframe) (Εικόνα 24) περιγράφει λεπτομερώς την τελική εμφάνιση και δομή της εφαρμογής, στην περίπτωση χρήσης «Προβολή του chain of custody ενός αποδεικτικού στοιχείου», εστιάζοντας στη διάταξη των στοιχείων και στη ροή μεταξύ των περιβαλλόντων χρήστη σε όλους τους τύπους συσκευών, εν προκειμένω, σε ένα «έξυπνο» κινητό (smartphone).

**Logo**

---

Active Cases

---

Track Evidence ►

---

Investigator's Profile

---

Open new Case

---

Add new Investigator

---

Add new Evidence

---

Manage Investigators

---

Manage Cases

## Track Evidence

Search

ID	Evidence Name	Evidence Hash	Date Created	Show More
				↗

Evidence ID	
Evidence Name	
Evidence Hash	
Evidence Description	
Date Created	
Evidence Creator	
Current Owner	

Transfer Ownership
View Chain of Custody
Delete Evidence

Wallet Address

Transfer Description

**Transfer Ownership**

Evidence Name      Evidence Hash  
Transferred To (Address) Transfer Date  
Transfer Description

Evidence Name      Evidence Hash  
Transferred To (Address) Transfer Date  
Transfer Description

Evidence Name      Evidence Hash  
Transferred To (Address) Transfer Date  
Transfer Description

Εικόνα 20 – Προσχέδιο περιβάλλοντος χρήστη «Αναζήτηση αποδεικτικού στοιχείου» (Track Evidence Mockup)

Logo

Active Cases

Track Evidence

Investigator 's Profile

Open new Case ►

Add new Investigator

Add new Evidence

Manage Investigators

Manage Cases

## Open a new Case

Case Name

Case Description

Case Investigator

**Open Case**

**Add Case Evidence**

**Add Case Investigator**

Evidence Hash

Evidence Name

Evidence Description

Wallet Address

**Add Investigator**

**Add Evidence**

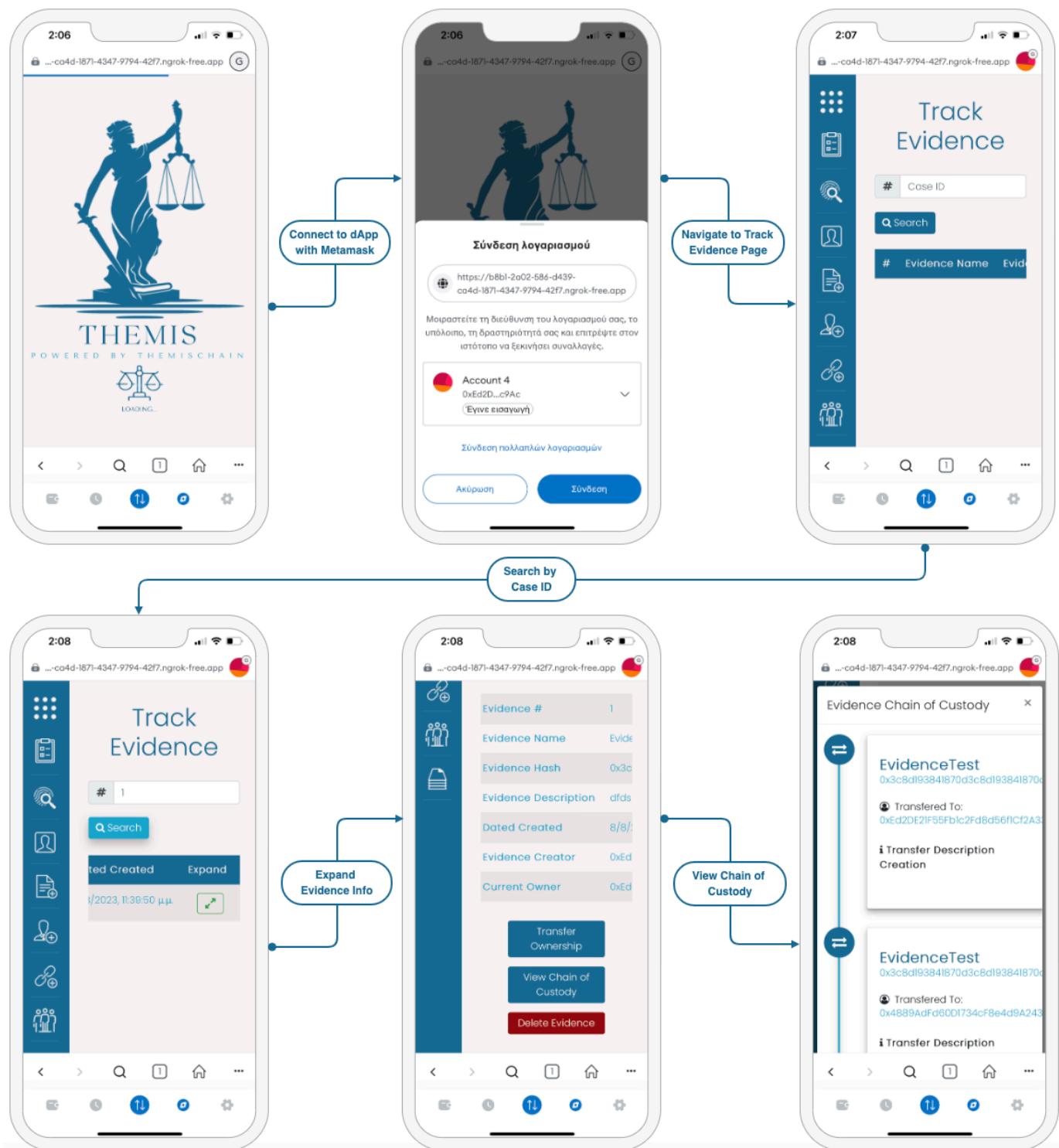
Εικόνα 21 - Προσχέδιο περιβάλλοντος χρήστη «Δημιουργία νέας υπόθεσης» (Open a new Case Mockup)

Logo		Manage Cases							
		ID	Case Name	Case Description	Case Investigators	Creation Date	Add Evidence	Add / Remove Investigator	Close Case
Active Cases				<input type="button" value="Read Description"/>			<input type="button" value="+"/>	<input type="button" value="+"/> <input type="button" value="+"/>	<input type="button" value="X"/>
Track Evidence				<input type="button" value="Read Description"/>			<input type="button" value="+"/>	<input type="button" value="+"/> <input type="button" value="+"/>	<input type="button" value="X"/>
Investigator 's Profile				<input type="button" value="Read Description"/>			<input type="button" value="+"/>	<input type="button" value="+"/> <input type="button" value="+"/>	<input type="button" value="X"/>
Open new Case									
Add new Investigator									
Add new Evidence									
Manage Investigators									
Manage Cases ►									

Εικόνα 22 - Προσχέδιο περιβάλλοντος χρήστη «Διαχείριση υποθέσεων» (Manage Cases Mockup)

Logo		Investigator 's Profile																				
Active Cases																						
Track Evidence																						
Investigator 's Profile ►		 Full Name ID Wallet Address <input type="button" value="Email"/> <input type="button" value="Call"/>		<table border="1"> <tr><td>Full Name</td><td></td></tr> <tr><td>Investigator ID</td><td></td></tr> <tr><td>Wallet Address</td><td></td></tr> <tr><td>Email</td><td></td></tr> <tr><td>Mobile</td><td></td></tr> <tr><td>Date of Birth</td><td></td></tr> <tr><td>Active Cases</td><td></td></tr> </table>					Full Name		Investigator ID		Wallet Address		Email		Mobile		Date of Birth		Active Cases	
Full Name																						
Investigator ID																						
Wallet Address																						
Email																						
Mobile																						
Date of Birth																						
Active Cases																						
Open new Case																						
Add new Investigator																						
Add new Evidence																						

Εικόνα 23 - Προσχέδιο περιβάλλοντος χρήστη «Προφίλ ερευνητή» (Investigator 's Profile Mockup)



Εικόνα 24 - Μακέτα περίπτωσης χρήσης «Προβολή του Chain of Custody ενός αποδεικτικού στοιχείου»  
(View Chain of Custody Wireframe)

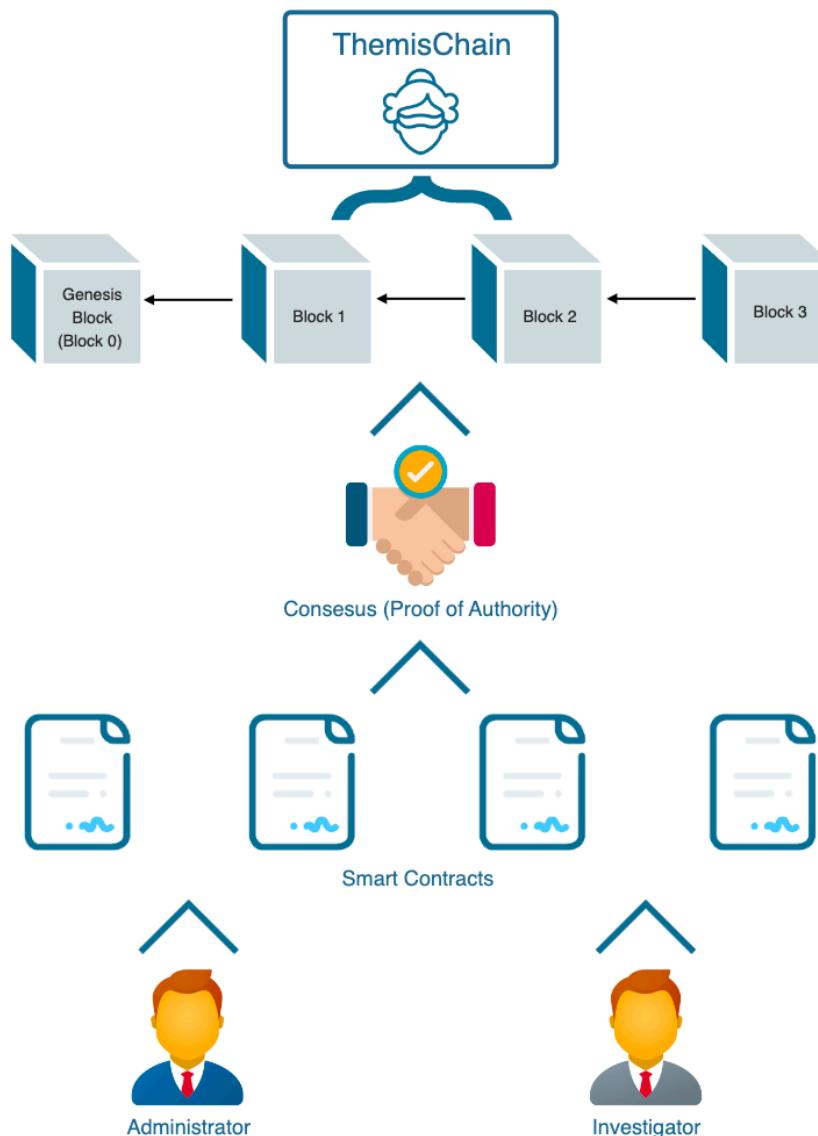
## Κεφάλαιο 6: Ανάπτυξη του ιδιωτικού Ethereum Blockchain

Όπως αναφέρθηκε στο Κεφάλαιο 2, ένα blockchain είναι ένα αποκεντρωμένο καθολικό που συνδέει μια συνεχώς αναπτυσσόμενη ακολουθία block μέσω κρυπτογραφικών κατακερματισμών. Αυτά τα μπλοκ περιέχουν μια ορισμένη ποσότητα συναλλαγών μεταξύ χρηστών και η δημιουργία καθενός από αυτά αποδίδεται σε έναν επιλεγμένο «miner», βάσει του αλγορίθμου συναίνεσης. Επίσης, οι πληροφορίες που περιέχονται σε ένα blockchain είναι διαθέσιμες για όλους, εξαλείφοντας την ανάγκη παρέμβασης τρίτων και προωθώντας την άμεση επικοινωνία μεταξύ οποιωνδήποτε δύο κόμβων, παρακάμπτοντας τα ενδιάμεσα έξοδα.

Η επιλογή του Ethereum ως πλατφόρμας ανάπτυξης, στην οποία θα βασιστεί η εφαρμογή chain of custody, συνεπάγεται μια σειρά επιτακτικών λόγων. Το Ethereum, γνωστό για τις δυνατότητες των «έξυπνων» συμβολαίων και την αποκεντρωμένη φύση του, προσφέρει ένα ιδανικό περιβάλλον για τη δημιουργία ασφαλών και «διαφανών» εφαρμογών. Η ενσωμάτωση της τεχνολογίας blockchain του Ethereum εγγυάται την αμεταβλητότητα των δεδομένων και αυξάνει την ακεραιότητά τους, δύο βασικές πτυχές στον τομέα της ψηφιακής εγκληματολογίας. Ακόμη, το Ethereum παρέχει την ευελιξία προσαρμογής πολλών καίριων χαρακτηριστικών του πρωτοκόλλου, συμπεριλαμβανομένης της επιλογής αλγορίθμων συναίνεσης και της δημιουργίας προσαρμοσμένων δημόσιων ή ιδιωτικών, ελεγχόμενων ή χωρίς άδεια δικτύων blockchain.

Για τις ανάγκες πραγμάτωσης του παρόντος έργου, αναπτύχθηκε ένα ιδιωτικό δίκτυο Ethereum, το «ThemisChain», στην υποδομή «AWS» (Amazon Web Services), παρέχοντας μια λύση που επιτρέπει τη διατήρηση του ελέγχου των δεδομένων, μειώνοντας παράλληλα τις οικονομικές δαπάνες και ενισχύοντας την ταχύτητα των συναλλαγών. Παρόλο που ένα ιδιωτικό blockchain δεν προσφέρει μια εντελώς αποκεντρωμένη δομή, όπως συμβαίνει με ένα αντίστοιχο δημόσιο, μπορεί ακόμα να κληρονομήσει βασικά χαρακτηριστικά, όπως ιχνηλασιμότητα, ακεραιότητα και εμπιστευτικότητα και επιτρέπει τη χρήση ενός κατανεμημένου καθολικού μεταξύ όλων των εμπλεκόμενων μερών, διασφαλίζοντας τον συγχρονισμό των αρχείων τους. Η υποδομή του blockchain υλοποιήθηκε μέσω του «Geth», μιας δημοφιλούς υλοποίησης του Ethereum, που μπορεί να μετατρέψει οποιονδήποτε υπολογιστή σε κόμβο ενός Ethereum blockchain. Το Geth παρέχει τη δυνατότητα δημιουργίας ενός ιδιωτικού δικτύου και επιτρέπει την προσαρμογή όλων των στοιχείων του blockchain, καθώς και

του μηχανισμού συναίνεσης που χρησιμοποιείται. Στο πλαίσιο του ιδιωτικού και ελεγχόμενου blockchain που αναπτύχθηκε, νιοθετήθηκε ο αλγόριθμος συναίνεσης «PoA» (Proof-of-Authority). Το δίκτυο αποτελείται από τρεις (3) κόμβους με την ιδιότητα του «validator» (επαληθευτής – το αντίστοιχο του «miner» στο «PoW»), οι οποίοι, λόγω του αλγορίθμου συναίνεσης, είναι οι μοναδικοί υπεύθυνοι για τον έλεγχο και την επικύρωση των συναλλαγών που πραγματοποιούνται. Ωστόσο, μελλοντικά είναι πιθανό να προστεθούν περισσότεροι «validators». Το κόστος των συναλλαγών έχει οριστεί να είναι μηδενικό, διότι το blockchain και κατ' επέκταση η εφαρμογή chain of custody, θα χρησιμοποιούνται από προκαθορισμένες έμπιστες οντότητες για σκοπούς ασφάλειας και διατήρησης αποδεικτικών στοιχείων, γεγονός που σημαίνει πως το μέγεθος των δεδομένων θα ανέρχεται σε μεγάλο αριθμό «MB» (Megabyte) και κατά συνέπεια, θα χαρακτηρίζονται από υψηλό κόστος.



Εικόνα 25 - Απλουστευμένη αρχιτεκτονική του δικτύου «ThemisChain»

## 6.1. Διαμόρφωση του δικτύου

Παρακάτω θα αναλυθούν τα βήματα που ακολουθήθηκαν για την διαμόρφωση του δικτύου, τα οποία θα διαχωριστούν σε τέσσερις (4) ενότητες: 1. Διαμόρφωση των Εικονικών Μηχανών (Virtual Machines), 2. Εγκατάσταση του Geth, 3. Δημιουργία του blockchain, 4. Προσθήκη των λογαριασμών των κόμβων στο πορτοφόλι «Metamask». Για την ορθότερη κατανόηση του περιεχομένου του τρέχοντος υποκεφαλαίου, παράλληλα με το τρίτο ενικό, θα χρησιμοποιηθεί και το πρώτο πληθυντικό πρόσωπο.

### 1. Διαμόρφωση της Εικονικής Μηχανής

Πρώτο βήμα για την διαμόρφωση της εικονικής μηχανής είναι η δημιουργία ενός λογαριασμού στον ιστότοπο «AWS» (<https://aws.amazon.com/>) (Εικόνα 26), που όπως προαναφέρθηκε, θα φιλοξενηθεί το blockchain. Στη συνέχεια, μέσω του μενού «Services», πλοηγούμαστε στην διαδρομή «EC2/Instances» και «πατάμε» το κουμπί «Launch Instances» (Εικόνα 27).



**Explore Free Tier products with a new AWS account.**

To learn more, visit [aws.amazon.com/free](https://aws.amazon.com/free).



### Sign up for AWS

#### Root user email address

Used for account recovery and some administrative functions

#### AWS account name

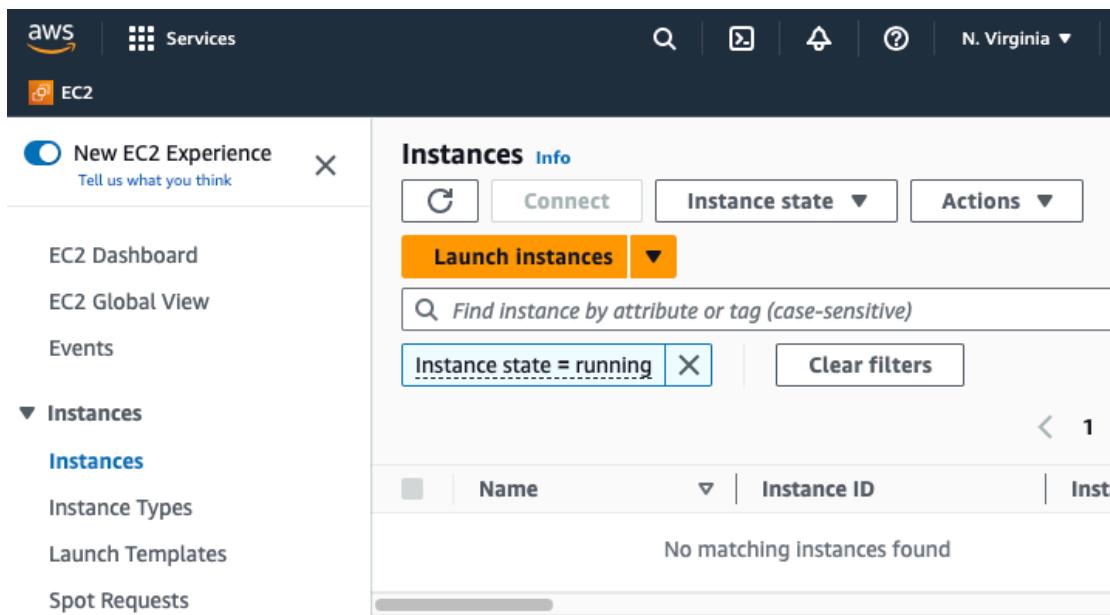
Choose a name for your account. You can change this name in your account settings after you sign up.

**Verify email address**

OR

**Sign in to an existing AWS account**

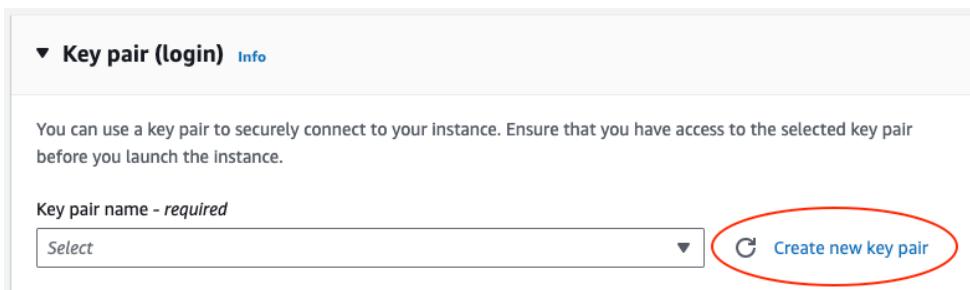
Εικόνα 26 - Δημιουργία λογαριασμού στο «AWS»



The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, there are links for 'Instances', 'Instance Types', 'Launch Templates', and 'Spot Requests'. The main area is titled 'Instances Info' and contains a search bar, a 'Launch instances' button (which is highlighted with a yellow box), and a filter bar set to 'Instance state = running'. Below this, a table header is visible with columns for 'Name', 'Instance ID', and 'Inst...'. A message 'No matching instances found' is displayed. At the top right of the main area, there are buttons for 'Actions' and 'Clear filters'.

*Εικόνα 27 - Κουμπί δημιουργίας εικονικής μηχανής*

Είναι σημαντικό, προτού ξεκινήσουμε τη διαδικασία, να δημιουργήσουμε ένα «Key pair», που χρησιμεύει στην ασφαλή σύνδεση με την εικονική μηχανή, μέσω της επιλογής που βρίσκεται στη φόρμα δημιουργίας της εικονικής μηχανής (Εικόνες 28 και 29).



The screenshot shows the 'Key pair (login)' configuration screen. It includes a note: 'You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.' Below this, there is a dropdown menu labeled 'Select' and a button labeled 'Create new key pair' which is circled in red.

*Εικόνα 28 - Επιλογή δημιουργίας ενός «Key pair»*

### Create key pair

**Key pair name**  
Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

**Key pair type**

- RSA  
RSA encrypted private and public key pair
- ED25519  
ED25519 encrypted private and public key pair

**Private key file format**

- .pem  
For use with OpenSSH
- .ppk  
For use with PuTTY

**⚠️** When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#) 

Cancel
Create key pair

Εικόνα 29 - Φόρμα δημιουργίας ενός «Key pair»

Αφού δημιουργηθεί το «Key pair» και αποθηκεύσουμε το αρχείο με κατάληξη «.pem» που παράγεται, μπορούμε να συνεχίσουμε την διαδικασία συμπληρώνοντας την φόρμα της Εικόνας 30. Όπως φαίνεται και στην εικόνα, η ονομασία της εικονικής μηχανής είναι «ThemisChain – Node0», καθώς πρόκειται για τον πρώτο κόμβο του blockchain, το λειτουργικό σύστημα είναι το «Ubuntu Server 22.04 LTS» και εκτελείται σε σύστημα με μονοπύρηνο επεξεργαστή και 1GiB (Gibibyte - 1GiB ≈ 1.074GB) μνήμη Ram.

### Name and tags Info

Name

[Add additional tags](#)

### ▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

**Quick Start**



Amazon Linux

**aws**



macOS

**Mac**



Ubuntu

**ubuntu®**



Windows



Red Hat



SUSE LI

**SUS**

🔍
[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

**Amazon Machine Image (AMI)**

<b>Ubuntu Server 22.04 LTS (HVM), SSD Volume Type</b>	<b>Free tier eligible</b>
<small>ami-053b0d53c279acc90 (64-bit (x86)) / ami-0a0c8eebcdd6dcdb0 (64-bit (Arm))            Virtualization: hvm ENA enabled: true Root device type: ebs</small>	

**Description**

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-05-16

<b>Architecture</b>	<b>AMI ID</b>	<b>Verified provider</b>
<b>64-bit (x86)</b>	ami-053b0d53c279acc90	<b>Verified provider</b>

### ▼ Instance type Info

**Instance type**

<b>t2.micro</b>	<b>Free tier eligible</b>
<small>Family: t2 1 vCPU 1 GiB Memory Current generation: true            On-Demand Windows pricing: 0.0162 USD per Hour            On-Demand SUSE pricing: 0.0116 USD per Hour            On-Demand RHEL pricing: 0.0716 USD per Hour            On-Demand Linux pricing: 0.0116 USD per Hour</small>	

All generations
[Compare instance types](#)

Εικόνα 30 - Φόρμα δημιουργίας εικονικής μηχανής

Εν συνεχεία, μέσω της φόρμας, είναι απαραίτητο να ορίσουμε ένα «Security Group», το οποίο αποτελεί ένα σύνολο κανόνων που ελέγχουν την «κίνηση» της εικονικής μηχανής ή απλούστερα, ποιος μπορεί να αποκτήσει πρόσβαση σε αυτήν. Στις Εικόνες 31 και 32, παρατίθενται οι κανόνες που εφαρμόστηκαν στο blockchain.

Ανάπτυξη του ιδιωτικού Ethereum Blockchain

71

#### Inbound Security Group Rules

- ▼ Security group rule 1 (TCP, 22, Multiple sources)

[Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh	TCP	22
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Custom	<input type="text" value="Add CIDR, prefix list or security"/> <a href="#">X</a>	e.g. SSH for admin desktop
	<input type="text" value="0.0.0.0"/> <a href="#">X</a> <input type="text" value="::/0"/> <a href="#">X</a>	

- ▼ Security group rule 2 (TCP, 80, Multiple sources)

[Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
HTTP	TCP	80
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Custom	<input type="text" value="Add CIDR, prefix list or security"/> <a href="#">X</a>	e.g. SSH for admin desktop
	<input type="text" value="0.0.0.0"/> <a href="#">X</a> <input type="text" value="::/0"/> <a href="#">X</a>	

- ▼ Security group rule 3 (TCP, 8545, Multiple sources)

[Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
Custom TCP	TCP	8545
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Custom	<input type="text" value="Add CIDR, prefix list or security"/> <a href="#">X</a>	e.g. SSH for admin desktop
	<input type="text" value="0.0.0.0"/> <a href="#">X</a> <input type="text" value="::/0"/> <a href="#">X</a>	

- ▼ Security group rule 4 (TCP, 30303, Multiple sources)

[Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
Custom TCP	TCP	30303
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Custom	<input type="text" value="Add CIDR, prefix list or security"/> <a href="#">X</a>	e.g. SSH for admin desktop
	<input type="text" value="0.0.0.0"/> <a href="#">X</a> <input type="text" value="::/0"/> <a href="#">X</a>	

Εικόνα 31 - Κανόνες του «Security Group» (1/2)

▼ Security group rule 5 (ICMP, N/A, Multiple sources) Remove

Type <a href="#">Info</a> Custom ICMP - IPv4	Protocol <a href="#">Info</a> Echo Reply	Port range <a href="#">Info</a> N/A
Source type <a href="#">Info</a> Custom	Source <a href="#">Info</a> <input type="text"/> Add CIDR, prefix list or security ξ	Description - optional <a href="#">Info</a> e.g. SSH for admin desktop <input type="text"/>
		<input type="button" value="0.0.0.0/0 X"/> <input type="button" value="::/0 X"/>

▼ Security group rule 6 (TCP, 443, Multiple sources) Remove

Type <a href="#">Info</a> HTTPS	Protocol <a href="#">Info</a> TCP	Port range <a href="#">Info</a> 443
Source type <a href="#">Info</a> Custom	Source <a href="#">Info</a> <input type="text"/> Add CIDR, prefix list or security ξ	Description - optional <a href="#">Info</a> e.g. SSH for admin desktop <input type="text"/>
		<input type="button" value="0.0.0.0/0 X"/> <input type="button" value="::/0 X"/>

▼ Security group rule 7 (TCP, 30301, Multiple sources) Remove

Type <a href="#">Info</a> Custom TCP	Protocol <a href="#">Info</a> TCP	Port range <a href="#">Info</a> 30301
Source type <a href="#">Info</a> Custom	Source <a href="#">Info</a> <input type="text"/> Add CIDR, prefix list or security ξ	Description - optional <a href="#">Info</a> e.g. SSH for admin desktop <input type="text"/>
		<input type="button" value="0.0.0.0/0 X"/> <input type="button" value="::/0 X"/>

▼ Security group rule 8 (All, All, Multiple sources) Remove

Type <a href="#">Info</a> All traffic	Protocol <a href="#">Info</a> All	Port range <a href="#">Info</a> All
Source type <a href="#">Info</a> Custom	Source <a href="#">Info</a> <input type="text"/> Add CIDR, prefix list or security ξ	Description - optional <a href="#">Info</a> e.g. SSH for admin desktop <input type="text"/>
		<input type="button" value="0.0.0.0/0 X"/> <input type="button" value="::/0 X"/>

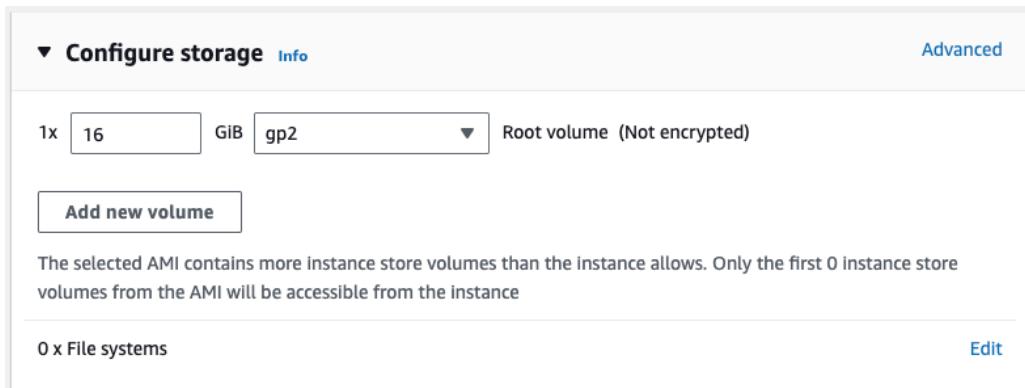
Εικόνα 32 - Κανόνες του «Security Group» (2/2)

Όπως παρατηρείται στις παραπάνω εικόνες, σε όλους τους κανόνες ορίστηκε να έχουν πρόσβαση όλες οι διευθύνσεις «IP» (λόγω των 0.0.0.0/0 και ::/0), διότι το blockchain δημιουργήθηκε και προορίζεται για την εκπόνηση της εργασίας και όχι για οποιονδήποτε άλλο σκοπό. Συνεπώς, δεν τίθεται θέμα διατήρησης κανόνων ασφαλείας

δεδομένων στον πραγματικό κόσμο. Επίσης, εκτός από τα προκαθορισμένα «ports», διακρίνονται και κάποια που έχουν προστεθεί χειροκίνητα:

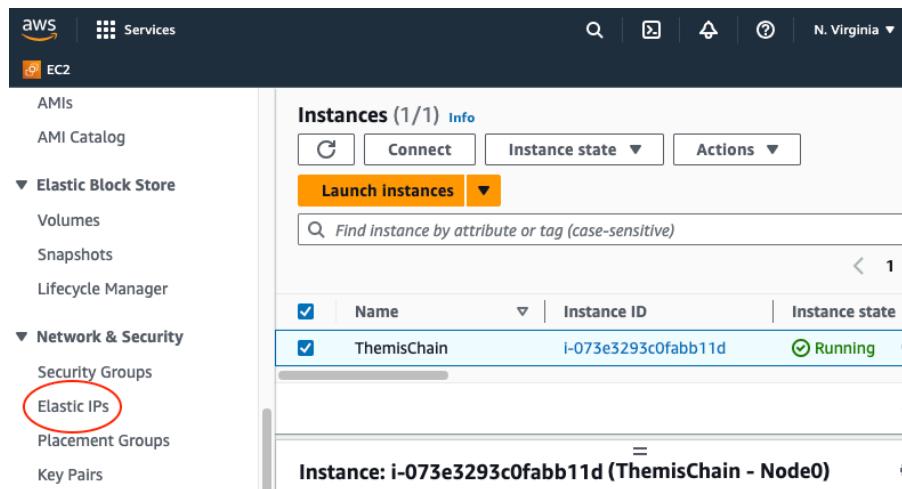
- **8545:** Το port του blockchain.
- **30303, 30301:** Ports που επιτρέπουν στους κόμβους να επικοινωνούν μεταξύ τους.

Ολοκληρώνοντας τη διαδικασία, μας ζητείται να επιλέξουμε την χωρητικότητα του συστήματος, η οποία στην προκειμένη περίπτωση είναι 16GiB (Εικόνα 33).



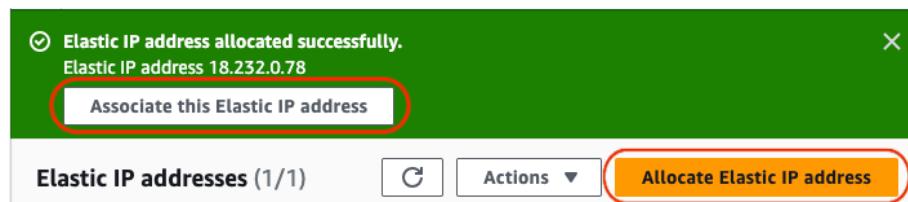
*Εικόνα 33 - Επιλογή χωρητικότητας εικονικής μηχανής*

Αφότου δημιουργήσουμε την εικονική μηχανή, αυτό που χρήζει ρύθμισης είναι η δημόσια διεύθυνση «IP» της, διότι μετά από κάθε επανεκκίνηση που θα πραγματοποιείται θα μεταβάλλεται, πράγμα που σημαίνει πως δε θα είναι δυνατή η σύνδεση με το blockchain. Κάτι τέτοιο επιτυγχάνεται με τη δημιουργία ενός «Elastic IP Address» και την μετέπειτα ανάθεση του στην εικονική μηχανή. Μεταβαίνοντας στον σύνδεσμο «Elastic IPs» στα αριστερά της σελίδας (Εικόνα 34) και πατώντας στο κουμπί «Allocate Elastic Ip address», δημιουργείται η διεύθυνση «IP» και εμφανίζεται στο πάνω μέρος της οθόνης το κουμπί «Associate this Elastic IP address» (Εικόνα 35). Αυτό το κουμπί μας μεταφέρει στη φόρμα ανάθεσης της «Elastic IP» διεύθυνσης (Εικόνα 36), στην οποία επιλέγουμε την εικονική μηχανή που επιθυμούμε και ολοκληρώνουμε την διαδικασία.



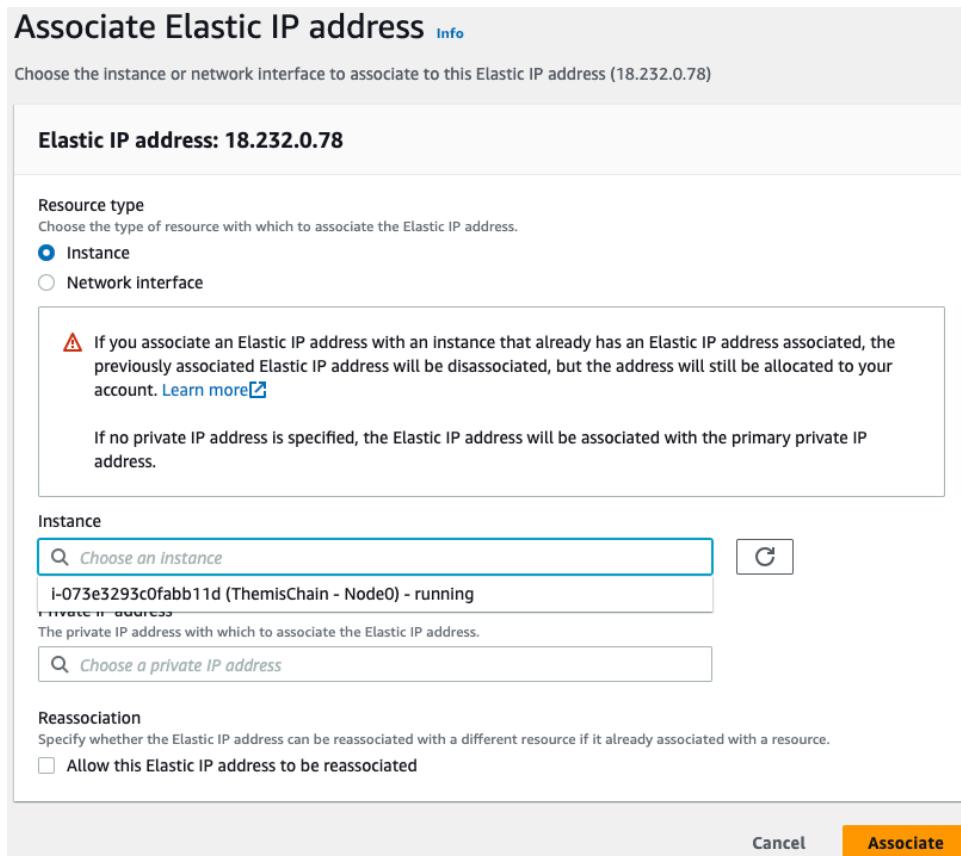
The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar has 'Elastic IPs' highlighted with a red circle. The main area displays 'Instances (1/1)' with one instance named 'ThemisChain' listed, which is currently 'Running'. Below the table is a note: 'Instance: i-073e3293c0fabb11d (ThemisChain - Node0)'

*Eikόνα 34 - Τοποθεσία συνδέσμου «Elastic IPs»*



The screenshot shows the 'Elastic IP addresses (1/1)' page. A green success message box contains the text: 'Elastic IP address allocated successfully. Elastic IP address 18.232.0.78' and a button labeled 'Associate this Elastic IP address'. Below the message is another button labeled 'Allocate Elastic IP address'.

*Eikόνα 35 - Τα κουμπιά «Allocate Elastic Ip address» και «Associate this Elastic IP address»*



The screenshot shows the 'Associate Elastic IP address' dialog. It starts with a note: 'Choose the instance or network interface to associate to this Elastic IP address (18.232.0.78)'. The 'Resource type' section shows 'Instance' selected. A warning message states: 'If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account.' Below this is a note: 'If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.' The 'Instance' section shows a dropdown menu with 'i-073e3293c0fabb11d (ThemisChain - Node0) - running' selected. The 'Reassociation' section has a checkbox 'Allow this Elastic IP address to be reassociated' checked. At the bottom are 'Cancel' and 'Associate' buttons.

*Eikόνα 36 - Η φόρμα ανάθεσης της «Elastic IP» διεύθυνσης*

Η τελική μορφή της εικονικής μηχανής είναι η παρακάτω:

Instance: i-073e3293c0fabb11d (ThemisChain - Node0)		
Instance ID <a href="#">i-073e3293c0fabb11d</a> (ThemisChain)	Public IPv4 address <a href="#">18.232.0.78</a>   <a href="#">open address</a>	Private IPv4 addresses <a href="#">172.31.83.3</a>
IPv6 address -	Instance state <span style="color: green;">Running</span>	Public IPv4 DNS <a href="#">ec2-18-232-0-78.compute-1.amazonaws.com</a>   <a href="#">open address</a>
Hostname type IP name: ip-172-31-83-3.ec2.internal	Private IP DNS name (IPv4 only) <a href="#">ip-172-31-83-3.ec2.internal</a>	
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	Elastic IP addresses <a href="#">18.232.0.78</a> [Public IP]

Εικόνα 37 - Η τελική μορφή της εικονικής μηχανής

## 2. Εγκατάσταση του Geth

Πρώτο βήμα για την εγκατάσταση του «Geth» είναι η σύνδεση με την εικονική μηχανή. Πατώντας το κουμπί «Connect» που βρίσκεται πάνω από την εικονική μηχανή, μεταβαίνουμε στην καρτέλα «SSH client», που περιέχει ορισμένες οδηγίες (Εικόνα 38). Αφού τις ακολουθήσουμε, αντιγράφουμε την εντολή που βρίσκεται στο κάτω μέρος (`ssh -i "ThemisChain_key_pair.pem" ubuntu@ec2-18-232-0-78.compute-1.amazonaws.com`) και την εκτελούμε σε ένα τερματικό (terminal), εντός του φακέλου που αποθηκεύσαμε το αρχείο με κατάληξη «.pem» (βλ. σελίδα 70) (Εικόνες 39 και 40).

**Connect to instance** [Info](#)

Connect to your instance i-073e3293c0fabb11d (ThemisChain - Node0) using any of these options

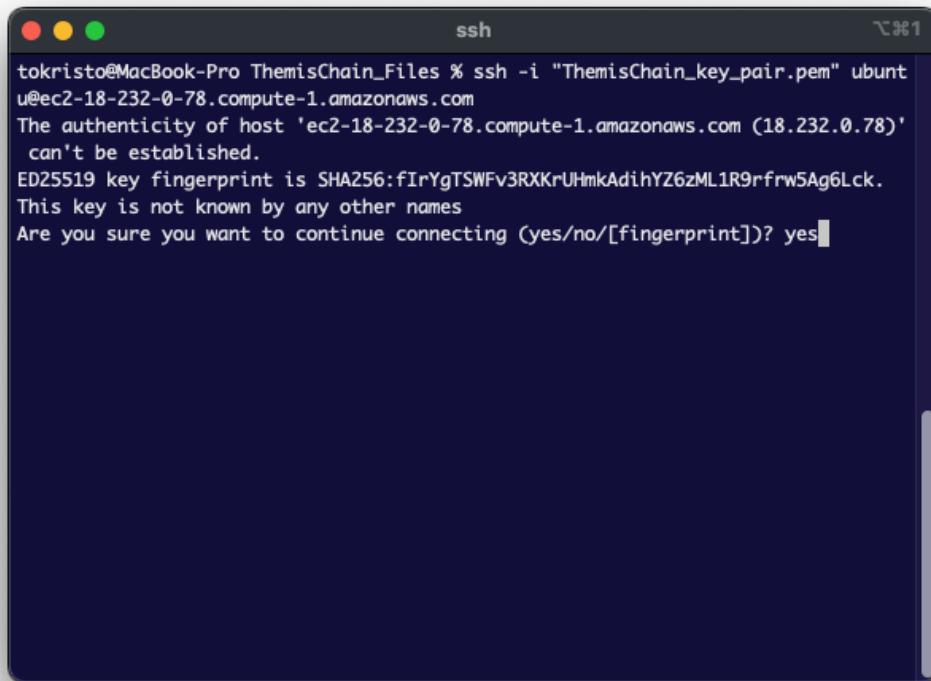
[EC2 Instance Connect](#)   [Session Manager](#)   **SSH client**   [EC2 serial console](#)

Instance ID  
[i-073e3293c0fabb11d](#) (ThemisChain - Node0)

1. Open an SSH client.  
 2. Locate your private key file. The key used to launch this instance is `ThemisChain_key_pair.pem`  
 3. Run this command, if necessary, to ensure your key is not publicly viewable.  
[chmod 400 ThemisChain\\_key\\_pair.pem](#)  
 4. Connect to your instance using its Public DNS:  
[ec2-18-232-0-78.compute-1.amazonaws.com](#)

Example:  
[ssh -i "ThemisChain\\_key\\_pair.pem" ubuntu@ec2-18-232-0-78.compute-1.amazonaws.com](#)

Εικόνα 38 - Οδηγίες σύνδεσης με την εικονική μηχανή



```
tokristo@MacBook-Pro ThemisChain_Files % ssh -i "ThemisChain_key_pair.pem" ubuntu
u@ec2-18-232-0-78.compute-1.amazonaws.com
The authenticity of host 'ec2-18-232-0-78.compute-1.amazonaws.com (18.232.0.78)'
can't be established.
ED25519 key fingerprint is SHA256:fIrYgTSWFv3RXKrUHmkAdihYZ6zML1R9rfrw5Ag6Lck.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

*Εικόνα 39 - Σύνδεση με την εικονική μηχανή μέσω τερματικού (1/2)*



```
ubuntu@ip-172-31-83-3: ~
Warning: Permanently added 'ec2-18-232-0-78.compute-1.amazonaws.com' (ED25519) to
o the list of known hosts.
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 System information as of Wed Jul 19 14:54:29 UTC 2023

 System load:  0.0          Processes:      96
 Usage of /:   10.2% of 15.32GB  Users logged in:   0
 Memory usage: 24%
 Swap usage:   0%
 IPv4 address for eth0: 172.31.83.3

Expanded Security Maintenance for Applications is not enabled.

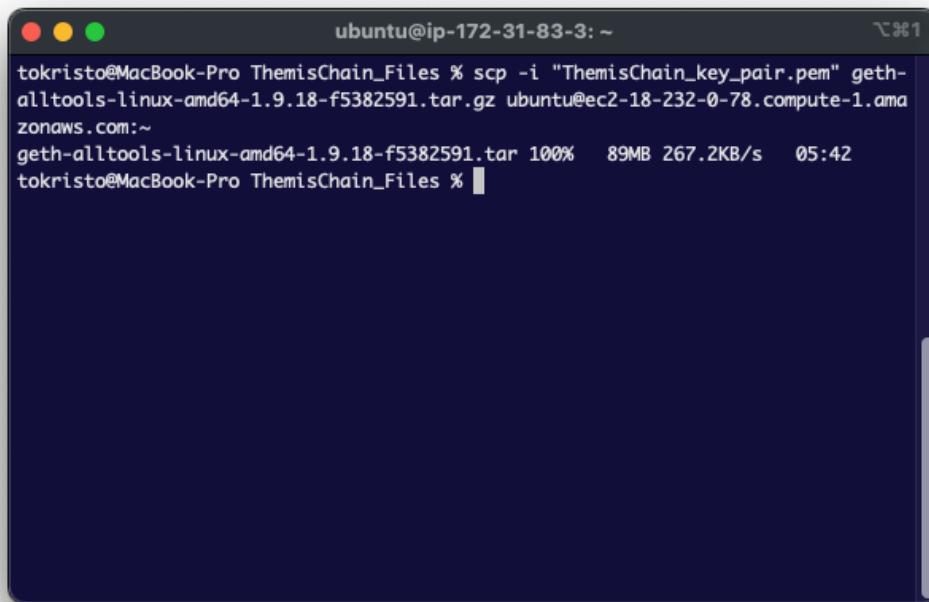
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

*Εικόνα 40 - Σύνδεση με την εικονική μηχανή μέσω τερματικού (2/2)*

Στη συνέχεια, μεταβαίνουμε στην διεύθυνση «<https://gethstore.blob.core.windows.net/builds/geth-alltools-linux-amd64-1.9.18-f5382591.tar.gz>» για να πραγματοποιήσουμε λήψη του συμπιεσμένου αρχείου που περιέχει την έκδοση 1.9.18 του «Geth», αλλά και κάποια συνοδευτικά εργαλεία που θα αξιοποιηθούν στη συνέχεια. Αφού ολοκληρωθεί η λήψη και το τοποθετήσουμε στον φάκελο που βρίσκεται το αρχείο με κατάληξη «.pem», εκτελούμε την παρακάτω εντολή για να το μεταφορτώσουμε στην εικονική μηχανή (Εικόνα 41):

```
scp -i "ThemisChain_key_pair.pem" geth-alltools-linux-amd64-1.9.18-f5382591.tar.gz
ubuntu@ec2-18-232-0-78.compute-1.amazonaws.com:~
```

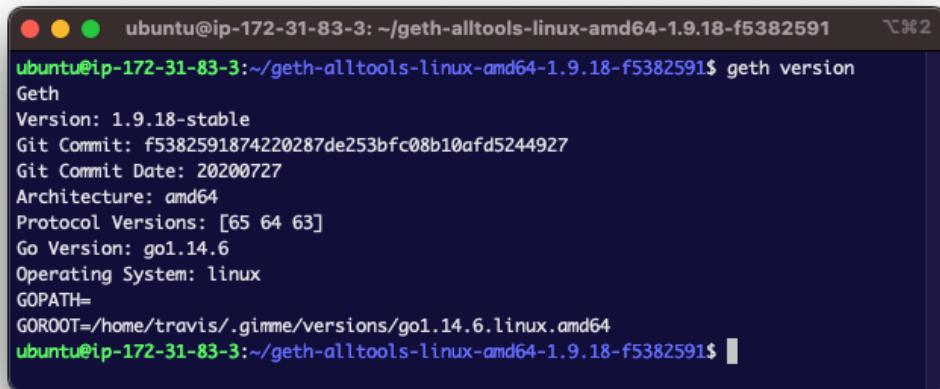


Εικόνα 41 - Μεταφόρτωση του συμπιεσμένου αρχείου του Geth στην εικονική μηχανή

Κατόπιν, αφού αποκτηθούν δικαιώματα διαχειριστή με την εντολή «*sudo -s*», ακολουθούμε μια σειρά εντολών ώστε: 1. Να αποσυμπιέσουμε το αρχείο που μεταφορτώσαμε, 2. Να παραχωρήσουμε άδεια εκτέλεσης στο αρχείο «Geth» και 3. Να μεταφέρουμε το σύνολο των αρχείων στην διαδρομή «/usr/local/bin» του συστήματος.

- 1a. *tar -xvf geth-alltools-linux-amd64-1.9.18-f5382591.tar.gz*
- 1β. *cd geth-alltools-linux-amd64-1.9.18-f5382591*
2. *chmod +x geth*
3. *cp \* /usr/local/bin/*

Τέλος, εκτελώντας την εντολή «*geth version*» μπορούμε να ελέγξουμε αν η παραπάνω διαδικασία ολοκληρώθηκε με επιτυχία (Εικόνα 42).



```
ubuntu@ip-172-31-83-3:~/geth-alltools-linux-amd64-1.9.18-f5382591$ geth version
Geth
Version: 1.9.18-stable
Git Commit: f5382591874220287de253bfc08b10af5244927
Git Commit Date: 20200727
Architecture: amd64
Protocol Versions: [65 64 63]
Go Version: go1.14.6
Operating System: linux
GOPATH=
GOROOT=/home/travis/.gimme/versions/go1.14.6.linux.amd64
ubuntu@ip-172-31-83-3:~/geth-alltools-linux-amd64-1.9.18-f5382591$
```

*Εικόνα 42 - Η εντολή «*geth version*»*

### 3. Δημιουργία του blockchain

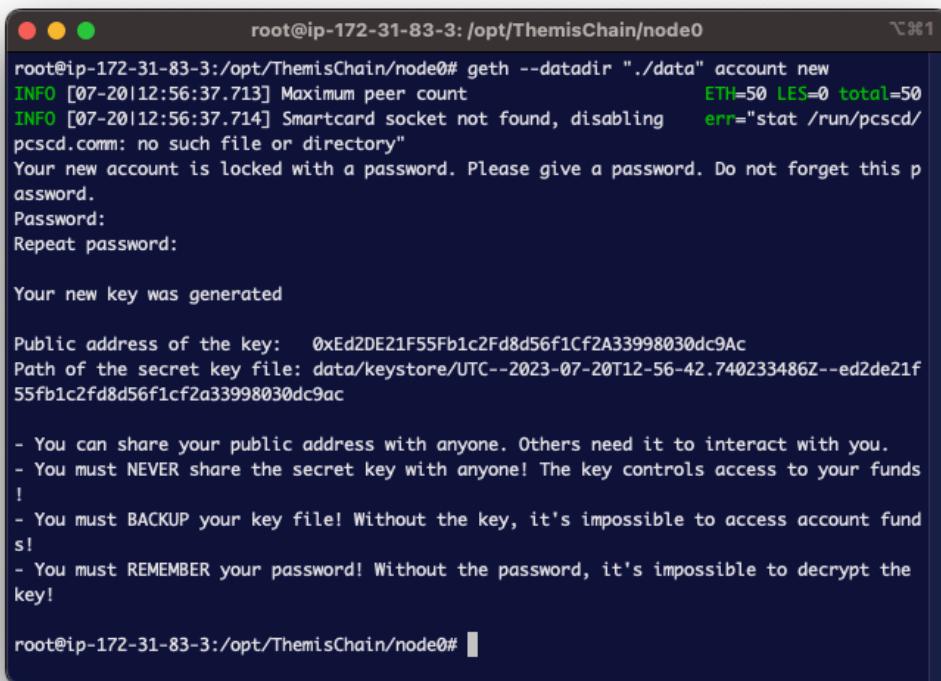
Αφού συνδεθούμε στην εικονική μηχανή (βλ. σελίδα 76), πρέπει να δημιουργήσουμε έναν λογαριασμό κόμβου στο «*geth*». Τα βήματα για τη δημιουργία ενός τέτοιου λογαριασμού είναι τα εξής (αφού αποκτηθούν δικαιώματα διαχειριστή με την εντολή «*sudo -s*») (Εικόνες 43 και 44): 1. Μετάβαση στη διαδρομή «*/opt*», που χρησιμοποιείται για την εγκατάσταση πακέτων λογισμικού στα λειτουργικά συστήματα «*Linux*», 2. Δημιουργία φακέλου που θα περιέχει τα απαραίτητα αρχεία του blockchain, 3. Δημιουργία φακέλου για τα αρχεία του κόμβου, 4. Δημιουργία του λογαριασμού, όπου μας ζητείται να εισάγουμε έναν κωδικό, ο οποίος είναι «12345» ομοίως και για τους τρεις κόμβους που δημιουργήθηκαν.

1. *cd /opt*
- 2α. *mkdir ThemisChain*
- 2β. *cd ThemisChain*
- 3α. *mkdir node0*
- 3β. *cd node0*
4. *geth --datadir "./data" account new*



```
root@ip-172-31-83-3:/home/ubuntu# cd /opt/
root@ip-172-31-83-3:/opt# mkdir ThemisChain
root@ip-172-31-83-3:/opt# cd ThemisChain
root@ip-172-31-83-3:/opt/ThemisChain# mkdir node0
root@ip-172-31-83-3:/opt/ThemisChain# cd node0
root@ip-172-31-83-3:/opt/ThemisChain/node0#
```

*Εικόνα 43 - Βήματα δημιουργίας λογαριασμού κόμβου στο «geth» (1/2)*



```
root@ip-172-31-83-3:/opt/ThemisChain/node0# geth --datadir "./data" account new
INFO [07-20|12:56:37.713] Maximum peer count                         ETH=50 LES=0 total=50
INFO [07-20|12:56:37.714] Smartcard socket not found, disabling      err="stat /run/pcscd/
pcscd.comm: no such file or directory"
Your new account is locked with a password. Please give a password. Do not forget this p
assword.
Password:
Repeat password:

Your new key was generated

Public address of the key: 0xED2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac
Path of the secret key file: data/keystore/UTC--2023-07-20T12-56-42.740233486Z--ed2de21f
55fb1c2fd8d56f1cf2a33998030dc9ac

- You can share your public address with anyone. Others need it to interact with you.
- You must NEVER share the secret key with anyone! The key controls access to your funds
!
- You must BACKUP your key file! Without the key, it's impossible to access account fund
s!
- You must REMEMBER your password! Without the password, it's impossible to decrypt the
key!
```

*Εικόνα 44 - Βήματα δημιουργίας λογαριασμού κόμβου στο «geth» (2/2)*

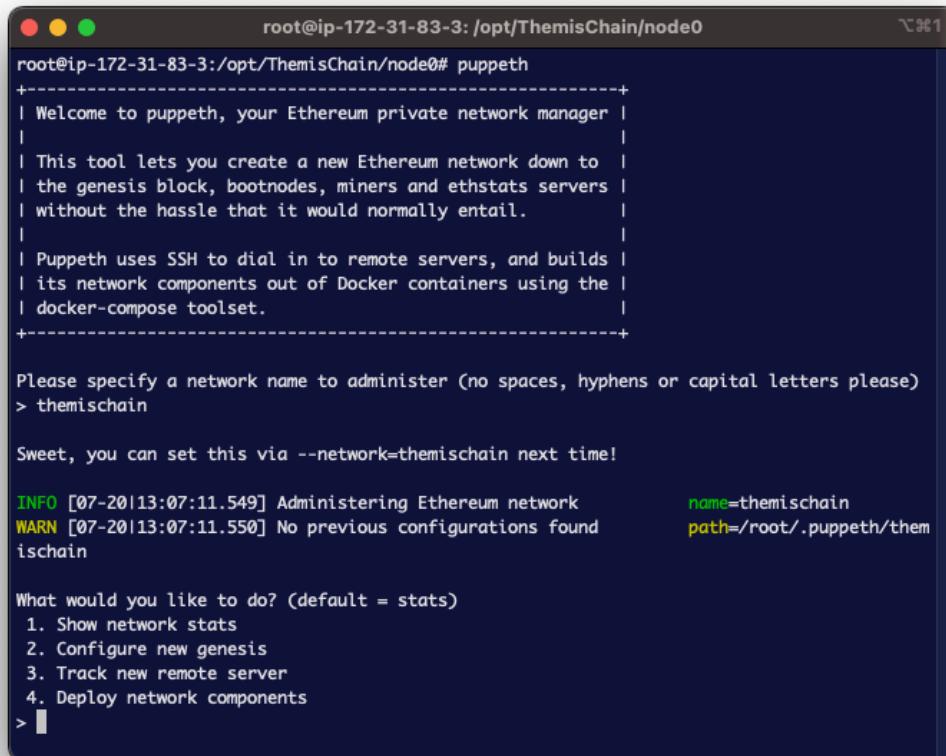
Από την παραπάνω εικόνα είναι σημαντικό να διαφυλάξουμε το «Public address of the key», στην προκειμένη περίπτωση το «0xED2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac», διότι θα χρειαστεί στη συνέχεια.

Προτού προχωρήσουμε στη δημιουργία του genesis block (βλ. σελίδα 18), είναι απαραίτητο να εκτελεστούν τα βήματα των παραπάνω δυο διαδικασιών (1. Διαμόρφωση της Εικονικής Μηχανής και 2. Εγκατάσταση του Geth), όπως και τα βήματα που παρουσιάστηκαν μέχρι στιγμής σε αυτή τη διαδικασία και για τους

υπόλοιπους δύο κόμβους του blockchain, καθώς για τη δημιουργία ενός PoA (proof of authority) blockchain είναι απαραίτητη η ύπαρξη τουλάχιστον ενός κόμβου (στην προκειμένη περίπτωση και των τριών).

Για τη δημιουργία του αρχείου genesis, που χρησιμοποιείται για την ανάπτυξη του genesis block, έγινε χρήση του εργαλείου «puppeth» του «geth» (Εικόνα 45), το οποίο ζητά από τον χρήστη να πληκτρολογήσει μόνο τα δεδομένα που χρειάζονται, διευκολύνοντας σε μεγάλο βαθμό τη διαδικασία. Τα δεδομένα αυτά, με τη σειρά που απεικονίζονται στην Εικόνα 46 είναι:

- Δημιουργία νέου αρχείου genesis.
- Επιλογή του αλγορίθμου συναίνεσης «Proof of Authority».
- Ορισμός του χρόνου δημιουργίας νέων block στα πέντε (5) δευτερόλεπτα.
- Ορισμός των λογαριασμών που μπορούν να επικυρώσουν μια συναλλαγή (validators) (βλ. σελίδα 67).
- Ορισμός των λογαριασμών προς πίστωση με το κρυπτονόμισμα «ETH».
- Ορισμός του αναγνωριστικού (ID) του blockchain.



```

root@ip-172-31-83-3:/opt/ThemisChain/node0#
root@ip-172-31-83-3:/opt/ThemisChain/node0# puppeth
+-----+
| Welcome to puppeth, your Ethereum private network manager |
|                                                               |
| This tool lets you create a new Ethereum network down to |
| the genesis block, bootnodes, miners and ethstats servers |
| without the hassle that it would normally entail.          |
|                                                               |
| Puppeth uses SSH to dial in to remote servers, and builds |
| its network components out of Docker containers using the |
| docker-compose toolset.                                     |
+-----+
Please specify a network name to administer (no spaces, hyphens or capital letters please)
> themischain

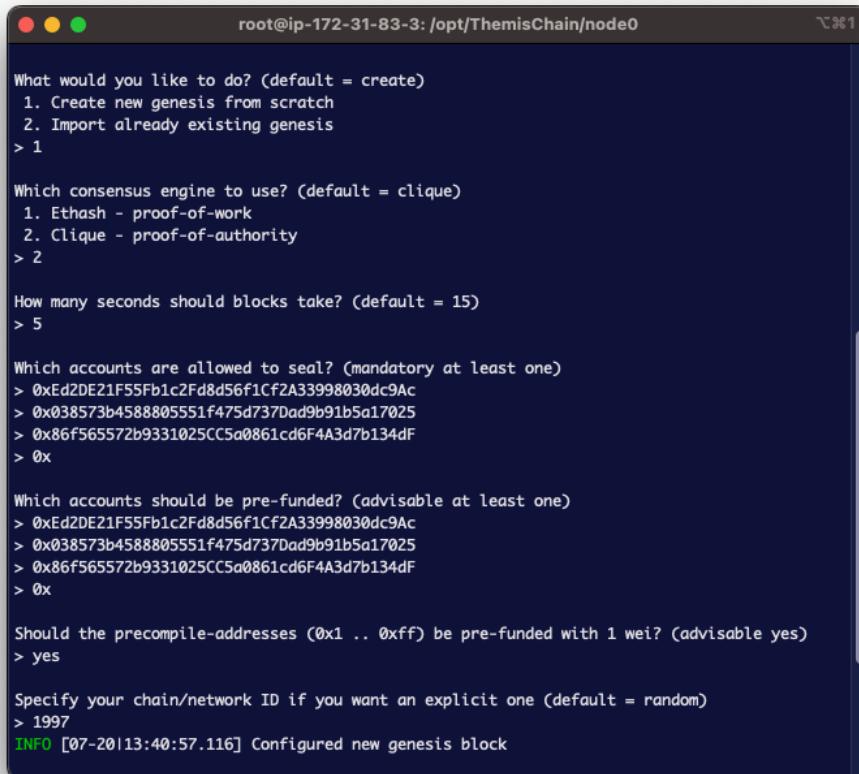
Sweet, you can set this via --network=themischain next time!

INFO [07-20|13:07:11.549] Administering Ethereum network           name=themischain
WARN [07-20|13:07:11.550] No previous configurations found         path=/root/.puppeth/them
ischain

What would you like to do? (default = stats)
1. Show network stats
2. Configure new genesis
3. Track new remote server
4. Deploy network components
> 1

```

Εικόνα 45 - Το εργαλείο «puppeth»



```

root@ip-172-31-83-3:/opt/ThemisChain/node0
What would you like to do? (default = create)
1. Create new genesis from scratch
2. Import already existing genesis
> 1

Which consensus engine to use? (default = clique)
1. Ethash - proof-of-work
2. Clique - proof-of-authority
> 2

How many seconds should blocks take? (default = 15)
> 5

Which accounts are allowed to seal? (mandatory at least one)
> 0xED2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac
> 0x038573b4588805551f475d737Dad9b91b5a17025
> 0x86f565572b9331025CC5a0861cd6F4A3d7b134dF
> 0x

Which accounts should be pre-funded? (advisable at least one)
> 0xED2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac
> 0x038573b4588805551f475d737Dad9b91b5a17025
> 0x86f565572b9331025CC5a0861cd6F4A3d7b134dF
> 0x

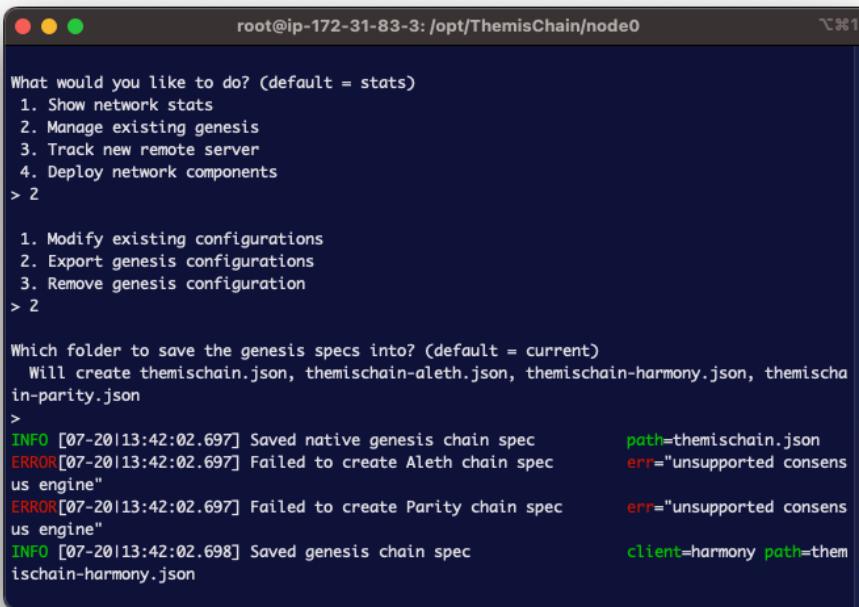
Should the precompile-addresses (0x1 .. 0xff) be pre-funded with 1 wei? (advisable yes)
> yes

Specify your chain/network ID if you want an explicit one (default = random)
> 1997
INFO [07-20|13:40:57.116] Configured new genesis block

```

*Eikόνα 46 - Βήματα δημιουργίας του αρχείου «genesis»*

Κατόπιν, εξάγουμε τα παραγόμενα αρχεία (Εικόνα 47) και διαγράφουμε το αρχείο «themischain-harmony.json», διότι δε θα χρειαστεί στη συνέχεια (Εικόνα 48).



```

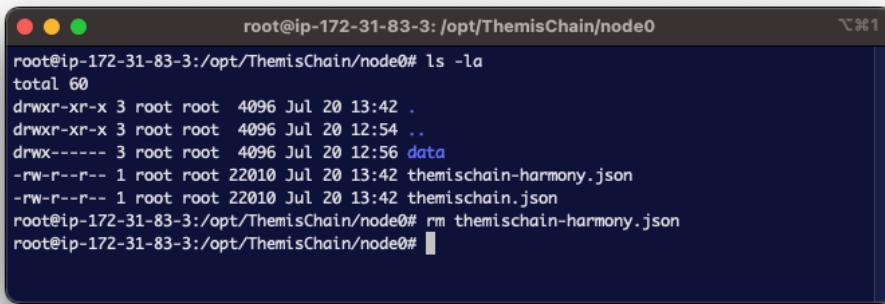
root@ip-172-31-83-3:/opt/ThemisChain/node0
What would you like to do? (default = stats)
1. Show network stats
2. Manage existing genesis
3. Track new remote server
4. Deploy network components
> 2

1. Modify existing configurations
2. Export genesis configurations
3. Remove genesis configuration
> 2

Which folder to save the genesis specs into? (default = current)
Will create themischain.json, themischain-aleth.json, themischain-harmony.json, themischain-parity.json
>
INFO [07-20|13:42:02.697] Saved native genesis chain spec
ERROR[07-20|13:42:02.697] Failed to create Aleth chain spec
path=themischain.json
err="unsupported consensus engine"
ERROR[07-20|13:42:02.697] Failed to create Parity chain spec
err="unsupported consensus engine"
INFO [07-20|13:42:02.698] Saved genesis chain spec
client=harmony path=themischain-harmony.json

```

*Eikόνα 47 - Εξαγωγή των παραγόμενων αρχείων από τη διαδικασία δημιουργίας του αρχείου «genesis»*

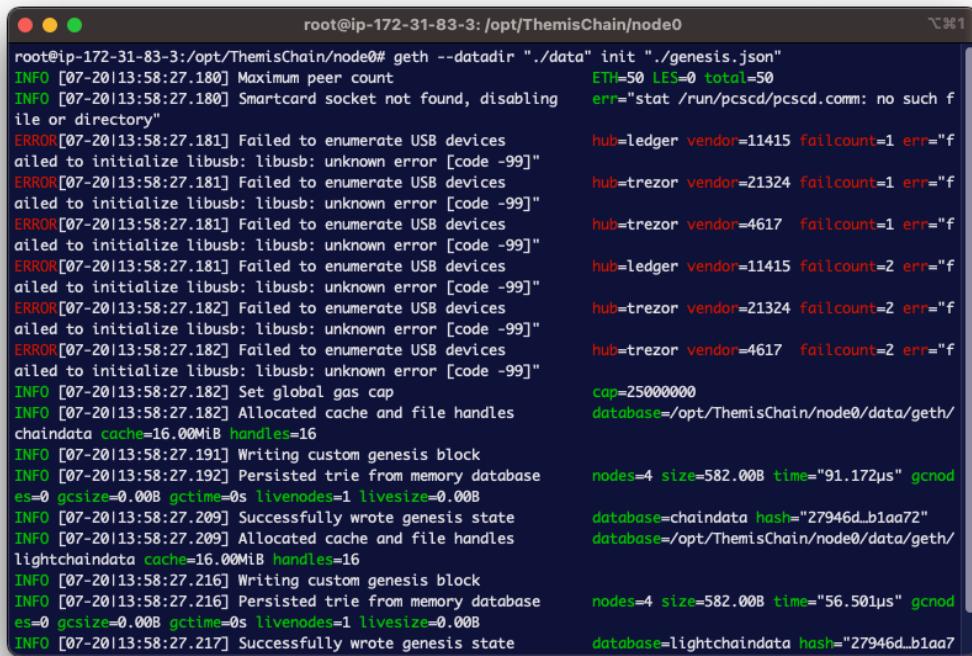


```
root@ip-172-31-83-3:/opt/ThemisChain/node0# ls -la
total 60
drwxr-xr-x 3 root root 4096 Jul 20 13:42 .
drwxr-xr-x 3 root root 4096 Jul 20 12:54 ..
drwx----- 3 root root 4096 Jul 20 12:56 data
-rw-r--r-- 1 root root 22010 Jul 20 13:42 themischain-harmony.json
-rw-r--r-- 1 root root 22010 Jul 20 13:42 themischain.json
root@ip-172-31-83-3:/opt/ThemisChain/node0# rm themischain-harmony.json
root@ip-172-31-83-3:/opt/ThemisChain/node0#
```

Εικόνα 48 - Διαγραφή του αρχείου «*themischain-harmony.json*»

Στη συνέχεια, πραγματοποιήθηκε επεξεργασία-σμίκρυνση του αρχείου «*themischain.json*» με τη χρήση της εφαρμογής «Visual Studio Code» και μετονομάστηκε σε «*genesis.json*». Για λόγους οικονομίας χώρου, το περιεχόμενο του αρχείου «*genesis.json*» παρουσιάζεται στο υποκεφάλαιο 9.4.

Τελευταίο βήμα είναι αρχικοποίηση του κόμβου, βάσει του αρχείου «*genesis.json*» με την εντολή «*geth --datadir "./data" account new*», ώστε να δημιουργηθεί το genesis block (Εικόνα 49). Για τους υπόλοιπους κόμβους η διαδικασία παραμένει η ίδια, ωστόσο δε χρειάζεται να δημιουργηθεί εξαρχής νέο αρχείο *genesis*, καθώς το αρχείο «*genesis.json*» που δημιουργήθηκε παραπάνω, είναι αυτό στο οποίο θα βασιστεί η αρχικοποίηση τους.



```

root@ip-172-31-83-3:/opt/ThemisChain/node0# geth --datadir "./data" init "./genesis.json"
INFO [07-20|13:58:27.180] Maximum peer count
INFO [07-20|13:58:27.180] Smartcard socket not found, disabling file or directory"
ERROR[07-20|13:58:27.181] Failed to enumerate USB devices ailed to initialize libusb: libusb: unknown error [code -99]
ERROR[07-20|13:58:27.181] Failed to enumerate USB devices ailed to initialize libusb: libusb: unknown error [code -99]
ERROR[07-20|13:58:27.181] Failed to enumerate USB devices ailed to initialize libusb: libusb: unknown error [code -99]
ERROR[07-20|13:58:27.181] Failed to enumerate USB devices ailed to initialize libusb: libusb: unknown error [code -99]
ERROR[07-20|13:58:27.181] Failed to enumerate USB devices ailed to initialize libusb: libusb: unknown error [code -99]
ERROR[07-20|13:58:27.182] Failed to enumerate USB devices ailed to initialize libusb: libusb: unknown error [code -99]
ERROR[07-20|13:58:27.182] Failed to enumerate USB devices ailed to initialize libusb: libusb: unknown error [code -99]
INFO [07-20|13:58:27.182] Set global gas cap
INFO [07-20|13:58:27.182] Allocated cache and file handles
chaindata cache=16.00MiB handles=16
INFO [07-20|13:58:27.191] Writing custom genesis block
INFO [07-20|13:58:27.192] Persisted trie from memory database es=0 gctime=0.00B livenodes=1 livesize=0.00B
INFO [07-20|13:58:27.209] Successfully wrote genesis state
INFO [07-20|13:58:27.209] Allocated cache and file handles
lightchaindata cache=16.00MiB handles=16
INFO [07-20|13:58:27.216] Writing custom genesis block
INFO [07-20|13:58:27.216] Persisted trie from memory database es=0 gctime=0s livenodes=1 livesize=0.00B
INFO [07-20|13:58:27.217] Successfully wrote genesis state

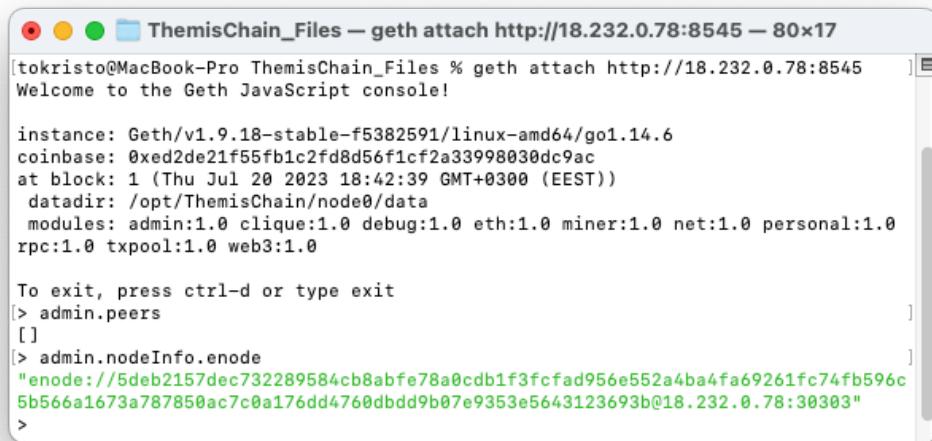
nodes=4 size=582.00B time="91.172µs" gcnode
database=chaindata hash="27946d...b1aa72"
database=/opt/ThemisChain/node0/data/geth/
nodes=4 size=582.00B time="56.501µs" gcnode
database=lightchaindata hash="27946d...b1aa72"

```

Εικόνα 49 - Αρχικοποίηση του blockchain βάσει του αρχείου «genesis.json»

### 3.1. Σύνδεση των κόμβων μεταξύ τους

Αφού πλέον έχουν δημιουργηθεί και οι τρεις κόμβοι, σειρά έχει η σύνδεση τους για τον σχηματισμό της τελικής μορφής του blockchain. Αρχικά, πρέπει να συνδεθούμε στον κάθε κόμβο μέσω του «Geth Javascript Console» πληκτρολογώντας την εντολή «*geth attach* (διεύθυνση IP του κόμβου)» (Εικόνα 50). Όπως φαίνεται στην εικόνα, ο κόμβος δεν είναι συνδεμένος με τους υπόλοιπους (*admin.peers -> []*). Το στοιχείο που χρειάζεται για να πραγματοποιηθεί η σύνδεση είναι το αναγνωριστικό κάθε κόμβου (*enode*), το οποίο εμφανίζεται μέσω της εντολής «*admin.nodeInfo.enode*». Συνεπώς, έχοντας τα «*enodes*» των κόμβων, συνδέομαστε στο «Geth Javascript Console» κάθε κόμβου και εκτελούμε την εντολή «*admin.addPeer(enode)*» για όσους κόμβους απομένουν (Εικόνα 51).



```
[tokristo@MacBook-Pro ThemisChain_Files % geth attach http://18.232.0.78:8545
Welcome to the Geth JavaScript console!

instance: Geth/v1.9.18-stable-f5382591/linux-amd64/go1.14.6
coinbase: 0xed2de21f55fb1c2fd8d56f1cf2a33998030dc9ac
at block: 1 (Thu Jul 20 2023 18:42:39 GMT+0300 (EEST))
datadir: /opt/ThemisChain/node0/data
modules: admin:1.0 clique:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0
rpc:1.0 txpool:1.0 web3:1.0

To exit, press ctrl-d or type exit
[> admin.peers
[]
[> admin.nodeInfo.enode
"enode://5deb2157dec732289584cb8abfe78a0cdb1f3fcfad956e552a4ba4fa69261fc74fb596c
5b566a1673a787850ac7c0a176dd4760dbdd9b07e9353e5643123693b@18.232.0.78:30303"
>
```

*Eικόνα 50 – To «Geth Javascript Console»*



```
[tokristo@MacBook-Pro ~ % geth attach http://52.73.112.80:8545
Welcome to the Geth JavaScript console!

instance: Geth/v1.9.18-stable-f5382591/linux-amd64/go1.14.6
coinbase: 0x038573b4588805551f475d737dad9b91b5a17025
at block: 6 (Thu Jul 20 2023 19:33:40 GMT+0300 (EEST))
datadir: /opt/Themischain/node1/data
modules: admin:1.0 clique:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0
rpc:1.0 txpool:1.0 web3:1.0

To exit, press ctrl-d or type exit
[> admin.addPeer("enode://5deb2157dec732289584cb8abfe78a0cdb1f3fcfad956e552a4ba4fa69261fc74fb596c5b566a1673a787850ac7c0a176dd4760dbdd9b07e9353e5643123693b@18.232.0.78:30303")
true
[> admin.addPeer("enode://45bfacf8f9a7b61f3a69cb8465b5de4655ae42062d760a21342a575691fec81363ddff20fe0f5c67daf40be31983612a4ec738da34e9da5248ba678f6949a22@52.20.6.247:30303")
true
>
```

*Eικόνα 51 - Η εντολή admin.addPeer()*

Έπειτα, μεταβαίνουμε στον υποφάκελο «data» του κάθε κόμβου (π.χ. /opt/ThemisChain/node0/data) και δημιουργούμε το αρχείο «static-nodes.json», το οποίο εξυπηρετεί στην αυτόματη επανασύνδεση των κόμβων, ακόμα κι αν ένας από αυτούς σταματήσει να λειτουργεί για ένα χρονικό διάστημα (για λόγους οικονομίας χώρου, το περιεχόμενο του αρχείου «static-nodes.json» παρατίθεται στο υποκεφάλαιο 9.5).

### 3.2. Δημιουργία του «geth.service»

Με τον τρόπο που είναι δομημένο μέχρι στιγμής το blockchain, κάθε φορά που θα πραγματοποιείται επανεκκίνηση των εικονικών μηχανών, θα πρέπει να πραγματοποιείται και εκ νέου εκκίνηση του blockchain, γεγονός που θα το έκρινε ακατάλληλο για τους σκοπούς τους οποίους αναπτύχθηκε. Αυτό αντιμετωπίζεται με τη δημιουργία μιας υπηρεσίας (service) στο λειτουργικό σύστημα της κάθε εικονικής μηχανής, που θα εκτελείται κάθε φορά που θα γίνεται εκκίνηση του συστήματος. Τα βήματα δημιουργίας αυτής της υπηρεσίας είναι τα εξής (αφού αποκτηθούν δικαιώματα διαχειριστή με την εντολή «*sudo -s*»): 1. Μετάβαση στη διαδρομή του φακέλου του συστήματος «*/etc/systemd/system*», 2. Δημιουργία του αρχείου-υπηρεσίας «*geth.service*» (για λόγους οικονομίας χώρου, το περιεχόμενο του αρχείου «*geth.service*» παρατίθεται στο υποκεφάλαιο 9.6), 3. Παραχώρηση άδειας εκτέλεσης στο αρχείο «*geth.service*», 4. Επαναφόρτωση του περιεχομένου του φακέλου, 5. Ενεργοποίηση της υπηρεσίας και 6. Εκκίνηση της υπηρεσίας.

1. *cd /etc/systemd/system*
2. *nano geth.service*
3. *chmod +x geth.service*
4. *systemctl daemon-reload*
5. *systemctl enable geth.service*
6. *systemctl start geth.service*

Επίσης, μπορούμε να ελέγχουμε την κατάσταση της υπηρεσίας μέσω της εντολής «*systemctl status geth.service*» (Εικόνα 52).



```
root@ip-172-31-83-3: /etc/systemd/system — ssh -i ThemisChain_key_pair.pem ubuntu@ec2-...
● geth.service - Go Ethereum Client
   Loaded: loaded (/etc/systemd/system/geth.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-08-18 13:44:09 UTC; 2min 32s ago
     Main PID: 426 (geth)
       Tasks: 8 (limit: 1130)
      Memory: 419.9M
        CPU: 6.037s
       CGroup: /system.slice/geth.service
           └─426 /usr/local/bin/geth --networkid 1997 --datadir /opt/ThemisChain/node0/data --port 30303 --ipcdisa

Aug 18 13:46:28 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:28.005] Imported new chain segment
Aug 18 13:46:28 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:28.006] ↘ block reached canonical chain
Aug 18 13:46:28 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:28.006] Commit new mining work
Aug 18 13:46:33 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:33.005] Imported new chain segment
Aug 18 13:46:33 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:33.006] Commit new mining work
Aug 18 13:46:38 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:38.001] Successfully sealed new block
Aug 18 13:46:38 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:38.001] ↗ mined potential block
Aug 18 13:46:38 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:38.001] Commit new mining work
Aug 18 13:46:38 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:38.001] Signed recently, must wait for others
Aug 18 13:46:38 ip-172-31-83-3 geth[426]: INFO [08-18|13:46:38.155] Looking for peers
blocks=>
number=>
blocks=>
number=>
blocks=>
number=>
blocks=>
number=>
peercou=>

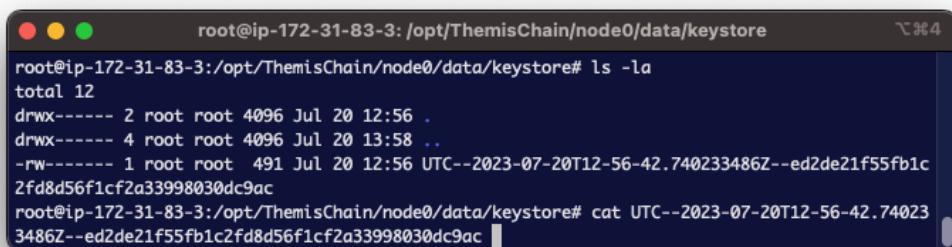
~
~
~
```

Lines 1-20/20 (END)

Εικόνα 52 - Η εντολή «*systemctl status geth.service*»

## 4. Προσθήκη των λογαριασμών των κόμβων στο πορτοφόλι «Metamask»

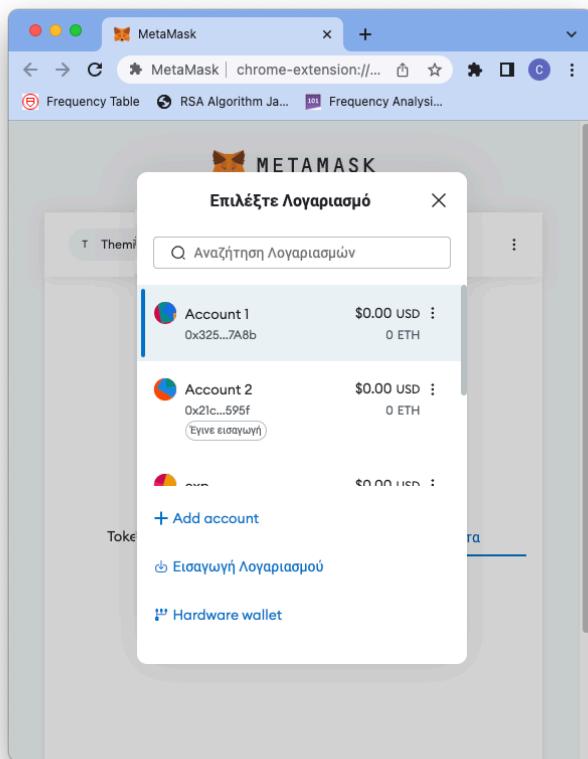
Η προσθήκη των λογαριασμών των κόμβων σε κάποιο πορτοφόλι είναι απαραίτητη για την διεκπεραίωση συναλλαγών κατά τη χρήση της εφαρμογής. Εξεινόντας θα πρέπει να πραγματοποιηθεί εξαγωγή του ιδιωτικού κλειδιού των λογαριασμών από τα αρχεία των κόμβων. Μεταβαίνοντας στον υποφάκελο «keystore» του κάθε κόμβου (π.χ. /opt/ThemisChain/node0/data/keystore), βρίσκουμε το αρχείο που περιέχει το ιδιωτικό κλειδί, το οποίο το «ανοίγουμε» με τη χρήση της εντολής «cat» (Εικόνα 53).



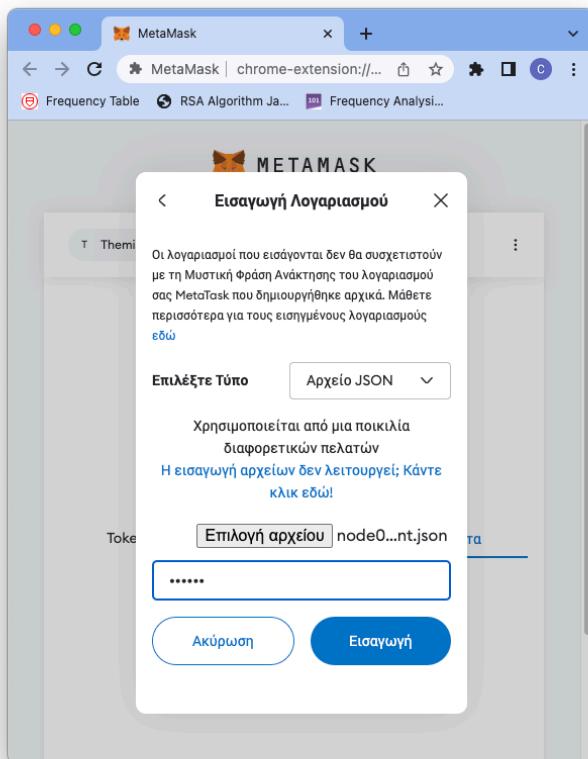
```
root@ip-172-31-83-3:/opt/ThemisChain/node0/data/keystore# ls -la
total 12
drwx----- 2 root root 4096 Jul 20 12:56 .
drwx----- 4 root root 4096 Jul 20 13:58 ..
-rw----- 1 root root 491 Jul 20 12:56 UTC--2023-07-20T12-56-42.740233486Z--ed2de21f55fb1c2fd8d56f1cf2a33998030dc9ac
root@ip-172-31-83-3:/opt/ThemisChain/node0/data/keystore# cat UTC--2023-07-20T12-56-42.740233486Z--ed2de21f55fb1c2fd8d56f1cf2a33998030dc9ac
```

Εικόνα 53 - Το αρχείο που περιέχει το ιδιωτικό κλειδί του λογαριασμού του κόμβου

Αφού αντιγράψουμε το περιεχόμενο του αρχείου και το αποθηκεύσουμε σε ένα νέο με κατάληξη «.json» (π.χ. node0account.json, βλ. υποκεφάλαιο 9.7), κάνουμε κλικ στην επιλογή «Εισαγωγή Λογαριασμού» του παραθύρου του «Metamask» (Εικόνα 54) και στη συνέχεια, επιλέγουμε το αρχείο που δημιουργήσαμε παραπάνω και πληκτρολογούμε τον κωδικό που εισαγάγαμε κατά τη δημιουργία του εκάστοτε λογαριασμού κόμβου (βλ. σελίδα 79) (Εικόνα 55).



Εικόνα 54 - Παράθυρο διαχείρισης λογαριασμών στο «Metamask»



Εικόνα 55 - Παράθυρο εισαγωγής λογαριασμού στο «Metamask»

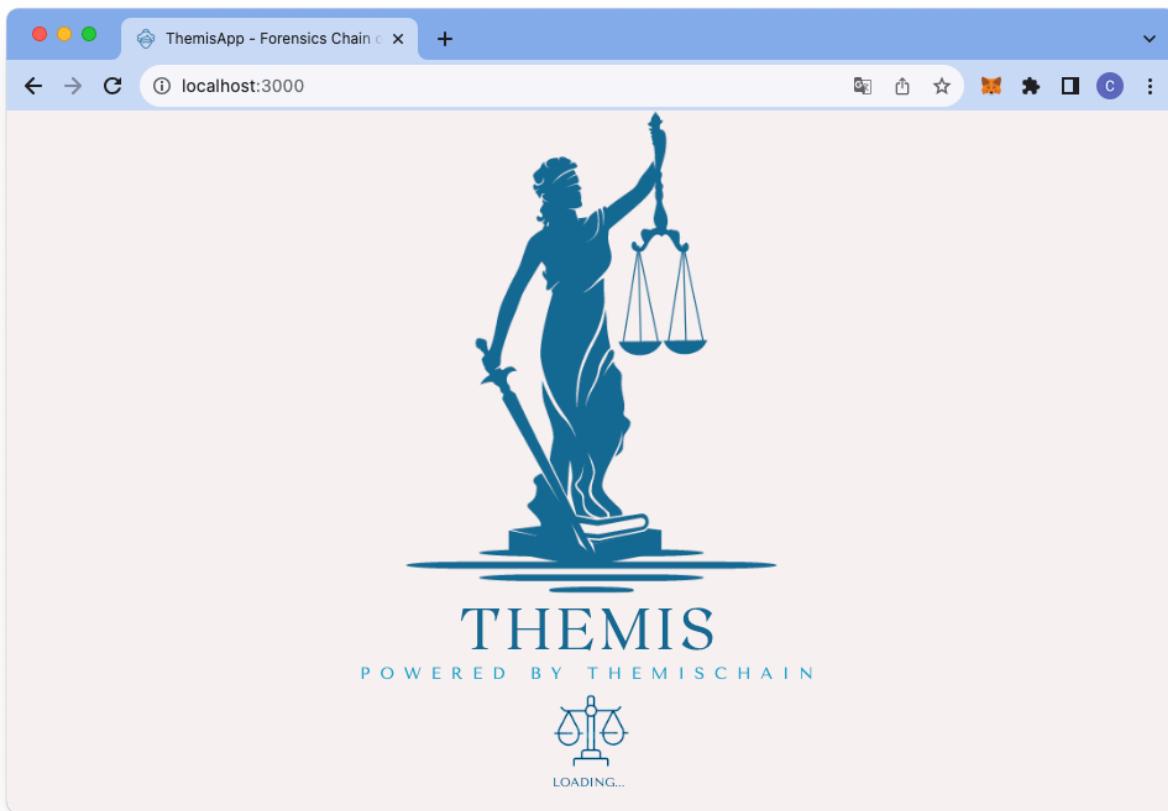
## Κεφάλαιο 7: Ανάπτυξη της εφαρμογής Chain of Custody

---

Η παρούσα διπλωματική εργασία παρουσιάζει το «Themis», ένα σύστημα διαχείρισης αποδεικτικών στοιχείων, που βασίζεται σε ένα εγγενές ιδιωτικό Ethereum blockchain. Αυτή η λύση στοχεύει στην ενίσχυση του ελέγχου και της εποπτείας των chain of custody των αποδεικτικών στοιχείων στο πλαίσιο της ψηφιακής εγκληματολογίας, προσφέροντας χαρακτηριστικά όπως η διαφάνεια, η αμεταβλητότητα και η επαληθευσιμότητα.

Το μοντέλο του παρόντος έργου (ThemisChain & ThemisApp) περικλείει δύο ρόλους: τον ερευνητή (investigator) και τον διαχειριστή (admin). Τα καθήκοντα ενός ερευνητή είναι η συλλογή των αποδεικτικών στοιχείων και ο υπολογισμός του hash τους, το οποίο στη συνέχεια, μεταβιβάζει εκτός σύνδεσης σε έναν admin, ώστε να το εισάγει στο blockchain. Με αυτόν τον τρόπο, οποιεσδήποτε ευαίσθητες πληροφορίες παραμένουν ασφαλείς και αναλλοίωτες. Ένας admin ουσιαστικά, είναι ένας ερευνητής με δικαιώματα επαληθευτή (validator) στο blockchain (βλ. Κεφάλαιο 6). Στα καθήκοντα ενός admin εντάσσονται αυτά του ερευνητή, παράλληλα με την προσθήκη ενός νέου ερευνητή, τη προσθήκη μιας νέας υπόθεσης και των αποδεικτικών στοιχείων αυτής, τη μεταφορά της κυριότητας ενός αποδεικτικού στοιχείου μεταξύ ερευνητών και την διαγραφή όλων των προαναφερθέντων δεδομένων από το blockchain. Συνοπτικά, ο ρόλος του admin είναι αυτός που έχει τον πλήρη έλεγχο του blockchain και των δεδομένων που καταχωρούνται σε αυτό.

Η διαδικασία δημιουργίας και μετέπειτα διαχείρισης του chain of custody ξεκινά με την προσθήκη του αποδεικτικού στοιχείου στο blockchain από τον admin. Η μοναδικότητα των αποδεικτικών στοιχείων παραμένει ανέπαφη, καθώς διατηρείται μεταξύ όλων των συμμετεχόντων στο δίκτυο. Δεδομένης της πιθανής συμπερίληψης εναίσθητων δεδομένων στα αποδεικτικά στοιχεία, τα πραγματικά αποδεικτικά στοιχεία προστατεύονται από την έκθεση στην εφαρμογή και κατ' επέκταση στο blockchain, ως εκ τούτου, αποθηκεύονται μόνο οι τιμές κατακερματισμού (hash values) τους. Κάθε διαχειριστής είναι σε θέση να ελέγξει τα δεδομένα στο blockchain, υπολογίζοντας μια τιμή κατακερματισμού του εκάστοτε αποδεικτικού στοιχείου και συγκρίνοντας την με την αντίστοιχη τιμή που είναι αποθηκευμένη στο blockchain. Αυτή η διαδικασία εγγυάται τη διασφάλιση της ακεραιότητας και της ελεγξιμότητας.



Εικόνα 56 - Η αρχική σελίδα της εφαρμογής «Themis»

## 7.1. Ανάλυση δομής

Το παρόν κεφάλαιο διερευνά την αρχιτεκτονική και οργανωτική δυναμική που σχετίζεται με την ανάπτυξη της αποκεντρωμένης εφαρμογής «Themis» και της απρόσκοπτης αλληλεπίδρασής της με το εγγενές ιδιωτικό Ethereum blockchain «ThemisChain». Πιο συγκεκριμένα, αναλύεται το δομικό πλαίσιο της εφαρμογής, αποκαλύπτοντας τον ρόλο της στη διατήρηση, παρακολούθηση και διαχείριση ψηφιακών αποδεικτικών στοιχείων καθ' όλη τη διάρκεια της ερευνητικής διαδικασίας.

Μέσω της εφαρμογής, καταγράφονται στο blockchain λεπτομέρειες όπως οι υπάρχοντες ερευνητές και τα στοιχεία τους, χαρακτηριστικά μιας υπόθεσης, όπως η ονομασία, οι υπεύθυνοι ερευνητές κ.λπ., αλλά και οι απαραίτητες πληροφορίες για κάθε αποδεικτικό στοιχείο. Κατά τη διάρκεια μιας έρευνας ψηφιακής εγκληματολογίας, οποιαδήποτε μεταφορά αποδεικτικών στοιχείων καταγράφεται αυτόματα στο blockchain μέσω των «έξυπνων» συμβολαίων, περιλαμβάνοντας

βασικές πληροφορίες, όπως η διεύθυνση του παραλήπτη και η ακριβής ημερομηνία και ώρα της μεταφοράς.

Τα κυριότερα χαρακτηριστικά της εφαρμογής που αφορούν τα αποδεικτικά στοιχεία μπορούν να αναλυθούν παρακάτω:

- **Δημιουργία αποδεικτικών στοιχείων**

Ο ρόλος του admin είναι ο αποκλειστικός υπεύθυνος για την προσθήκη των αποδεικτικών στοιχείων στο blockchain, ενισχύοντας την ασφάλεια και την αξιοπιστία της ψηφιακής εγκληματολογικής διαδικασίας. Για τη προσθήκη ενός αποδεικτικού στοιχείου, ο admin πρέπει να εισαγάγει τις απαιτούμενες λεπτομέρειες, δηλαδή το hash του που δημιουργήθηκε μέσω του αλγορίθμου SHA-256, την ονομασία του στοιχείου και μια σύντομη περιγραφή γι' αυτό. Αφού το αποδεικτικό στοιχείο προστεθεί, τότε ο admin μπορεί να μεταβιβάσει την κυριότητα του στον ερευνητή που το εντόπισε.

- **Μεταβίβαση κυριότητας αποδεικτικών στοιχείων**

Διευκολύνοντας την απρόσκοπη συνεργασία και ροή πληροφοριών μεταξύ των εμπλεκόμενων ενδιαφερόμενων μερών, το προτεινόμενο σύστημα υποστηρίζει την ασφαλή μεταφορά αποδεικτικών στοιχείων μεταξύ των ερευνητών. Αποτελεί επίσης, λειτουργία που μόνο ο ρόλος του admin έχει τη δυνατότητα να διεκπεραιώσει. Προκειμένου να μεταφερθεί ένα αποδεικτικό στοιχείο ζητείται από τον admin να πληκτρολογήσει τη διεύθυνση του παραλήπτη και μια σύντομη περιγραφή που θα αναφέρει τον σκοπό της μεταφοράς. Στη συνέχεια, το ενημερώνεται το ανάλογο «έξυπνο» συμβόλαιο και προσθέτει το γεγονός στο chain of custody του αποδεικτικού στοιχείου.

- **Πρόσβαση στα αποδεικτικά στοιχεία**

Πρόσβαση το εκάστοτε αποδεικτικό στοιχείο έχουν οι ερευνητές στους οποίους έχει ανατεθεί η υπόθεση στην οποία ανήκει το αποδεικτικό στοιχείο, είτε εμπλέκονται στο chain of custody του, είτε όχι. Ωστόσο, κανείς από αυτούς δεν έχει τη δυνατότητα να πραγματοποιήσει οποιαδήποτε αλλαγή.

Ομοίως με τα παραπάνω, μια σημαντική λειτουργία της εφαρμογής είναι πως, όλα τα εμπλεκόμενα μέρη (ερευνητές) που σχετίζονται άμεσα με τις υπό διερεύνηση υποθέσεις είναι καταχωρημένα στο ιδιωτικό δίκτυο blockchain από τους προκαθορισμένους admin-επαληθευτές. Οι επαληθευτές αυτοί αναλαμβάνουν τον

ρόλο της εποπτείας και του συντονισμού καθ' όλη τη διάρκεια μιας ερευνητικής διαδικασίας, αλλά και της ορθής λειτουργίας του συστήματος εν γένει.

Οι κυριότεροι σχεδιαστικοί στόχοι που επιδιώκει να επιτύχει η εφαρμογή «Themis» είναι οι εξής:

- **Απόρρητο:** Προστασία του απορρήτου των δεδομένων, περιορίζοντας ότι ένας ερευνητής δεν μπορεί να αποκτήσει πρόσβαση σε υποθέσεις και αποδεικτικά στοιχεία που είναι εκτός της δικαιοδοσίας του.
- **Έλεγχος πρόσβασης:** Μόνο ερευνητές που είναι εγγεγραμμένοι από τους προκαθορισμένους διαχειριστές έχουν πρόσβαση στην εφαρμογή.
- **Ακεραιότητα και Ελεγξιμότητα:** Εγγύηση της ακεραιότητας και της ελεγξιμότητας των δεδομένων στο blockchain, έτσι ώστε να αποτρέπεται η παραβίαση και να διευκολύνεται ο έλεγχος τους.
- **Ιχνηλασιμότητα:** Εντοπισμός της πηγής των αποδεικτικών στοιχείων, σε βαθμό όπου το αποδεικτικό στοιχείο προστέθηκε στην υπό διερεύνηση υπόθεση.
- **Αποδοτικότητα:** Εκμηδενισμός, εξ ορισμού, του κόστους συναλλαγών, ώστε να μην επιβαρύνονται οι ερευνητές που χρησιμοποιούν την εφαρμογή, καθώς βασικό μέλημα του συστήματος είναι η ορθότερη λειτουργία του, αποδίδοντας τα μέγιστα στη διαχείριση στοιχείων ψηφιακής εγκληματολογίας.
- **Εύχρηστο περιβάλλον χρήστη:** Στον τομέα της ψηφιακής εγκληματολογίας, όπου η ακρίβεια και η αποτελεσματικότητα είναι υψηστης σημασίας, ένα περιβάλλον χρήστη που είναι εύκολο στη διαχείριση, βελτιώνει την αφοσίωση των χρηστών, ελαχιστοποιεί το χρόνο εξοικείωσής τους σε αυτό και μειώνει τα σφάλματα. Επίσης, διασφαλίζει ότι οι χρήστες μπορούν να πλοηγηθούν στην εφαρμογή χωρίς κόπο, οδηγώντας σε ταχύτερη ολοκλήρωση εργασιών και λιγότερα λάθη.

Απόρροια των παραπάνω στόχων της εφαρμογής αποτελούν οι ακόλουθες «λειτουργικές» και «μη λειτουργικές» απαιτήσεις:

- **Λειτουργικές απαιτήσεις**
  - **Έλεγχος ταυτότητας και εξουσιοδότηση χρήστη:** Θα πρέπει να πραγματοποιείται ασφαλής σύνδεση του χρήστη χρησιμοποιώντας μηχανισμούς ελέγχου ταυτότητας. Οι χρήστες θα πρέπει να υπόκεινται

σε έλεγχο πρόσβασης βάσει δικαιωμάτων για την εκτέλεση εργασιών σύμφωνα με τους ρόλους τους.

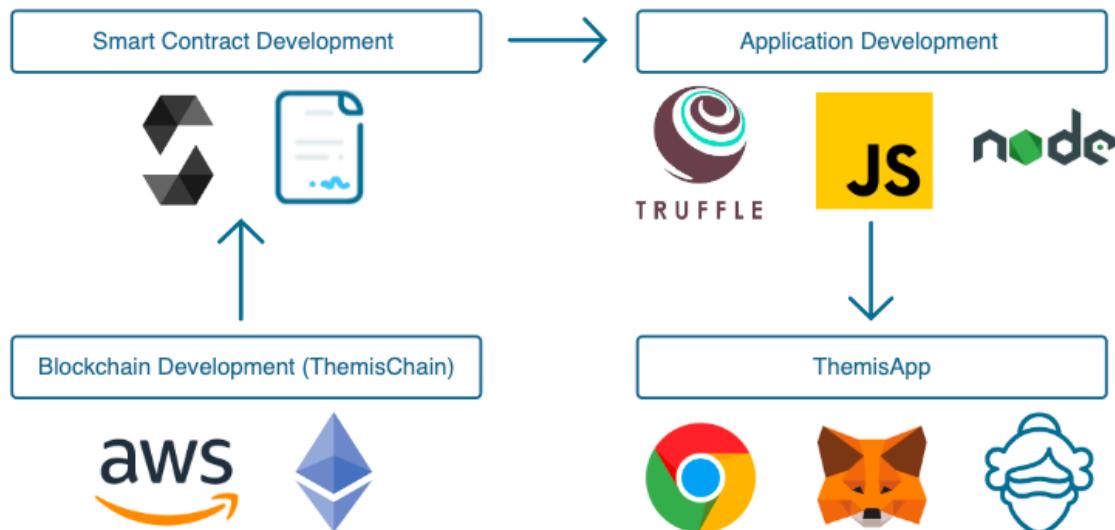
- **Δημιουργία και καταγραφή αποδεικτικών στοιχείων:** Θα πρέπει να επιτρέπεται μόνο στον διαχειριστή να δημιουργεί και να καταγράφει αποδεικτικά στοιχεία στο blockchain.
- **Μεταβίβαση αποδεικτικών στοιχείων:** Η εφαρμογή θα πρέπει να διευκολύνει την ασφαλή μεταβίβαση αποδεικτικών στοιχείων μεταξύ των ερευνητών.
- **Αμεταβλητότητα:** Όλα τα αποδεικτικά στοιχεία και οι συναλλαγές που καταγράφονται στο blockchain πρέπει να είναι αμετάβλητα και απαραβίαστα.
- **Παρακολούθηση του chain of custody:** Η εφαρμογή θα πρέπει, μέσω των «έξυπνων» συμβολαίων, να παρακολουθεί αυτόματα το chain of custody για κάθε αποδεικτικό στοιχείο, καταγράφοντας το ιστορικό των μεταβιβάσεων, των συμμετεχόντων και των χρονικών σημάνσεων.

- **Μη λειτουργικές απαιτήσεις**

- **Ασφάλεια και απόρρητο:** Η εφαρμογή θα πρέπει να διασφαλίζει την εμπιστευτικότητα και το απόρρητο των αποδεικτικών στοιχείων και των δεδομένων των ερευνητών μέσω μηχανισμών κρυπτογράφησης και ελέγχων πρόσβασης.
- **Επεκτασιμότητα:** Το σύστημα «Themis» (ThemisChain & ThemisApp) θα πρέπει να είναι επεκτάσιμο, για να φιλοξενεί έναν αυξανόμενο αριθμό ερευνητών, αποδεικτικών στοιχείων και συναλλαγών χωρίς αντίκτυπο στην απόδοση.
- **Αξιοπιστία:** Το σύστημα «Themis» θα πρέπει να διατηρεί υψηλή διαθεσιμότητα και αξιοπιστία, ελαχιστοποιώντας το χρόνο πιθανής διακοπής λειτουργίας και διασφαλίζοντας αδιάλειπτη πρόσβαση σε δεδομένα υποθέσεων και αποδεικτικά στοιχεία.
- **Ακεραιότητα δεδομένων:** Το σύστημα «Themis» θα πρέπει να διασφαλίζει την συνεχή ακεραιότητα των αποδεικτικών στοιχείων και των συναλλαγών, προστατεύοντας τα από την αλλοίωση ή την παραποίηση δεδομένων.

Σε επίπεδο κώδικα, η εφαρμογή, επικοινωνεί με τους κόμβους του ιδιωτικού blockchain χρησιμοποιώντας μια «βιβλιοθήκη» της γλώσσας προγραμματισμού «Javascript» ενώ, για την συγγραφή των «έξυπνων» συμβολαίων χρησιμοποιήθηκε η γλώσσα προγραμματισμού «Solidity». Το περιβάλλον εκτέλεσης «Node.js» έπαιξε κεντρικό ρόλο στην εκτέλεση του κώδικα και παρείχε υποεφαρμογές που εξορθολόγισαν τις απαιτούμενες διεργασίες.

Σε ένα πιο λεπτομερές πλαίσιο, η σύνδεση με το blockchain επιτυγχάνεται μέσω ενός «REST API», το οποίο αποδίδει ένα αρχείο «JSON» (JavaScript Object Notation), που περιλαμβάνει όλα τα στοιχεία που συντελούν ένα «έξυπνο» συμβόλαιο. Η ανάπτυξη σύγχρονων αποκεντρωμένων εφαρμογών συχνά περιλαμβάνει την αξιοποίηση συγκεκριμένων προγραμματιστικών «βιβλιοθηκών» που περιέχουν έτοιμες λειτουργίες και μεθόδους, διευκολύνοντας την επικοινωνία με το blockchain και ιδιαίτερα την κωδικοποίηση και αποκωδικοποίηση των αρχείων «JSON». Κατά τη διάρκεια της ανάπτυξης της εφαρμογής «Themis», αξιοποιήθηκε για το σκοπό αυτό η «βιβλιοθήκη» «Web3.js» της γλώσσας προγραμματισμού «Javascript».



Εικόνα 57 - Απλουστευμένη αρχιτεκτονική της εφαρμογής «Themis»

## 7.2. Τεχνικά μέρη

Οι τεχνολογίες και οι εφαρμογές που αξιοποιήθηκαν κατά τη διάρκεια ανάπτυξης του συστήματος «Themis» (ThemisChain & ThemisApp) είναι οι εξής:

- **AWS (Amazon Web Services):** Πλατφόρμα Cloud στην οποία φιλοξενείται το ιδιωτικό δίκτυο blockchain.

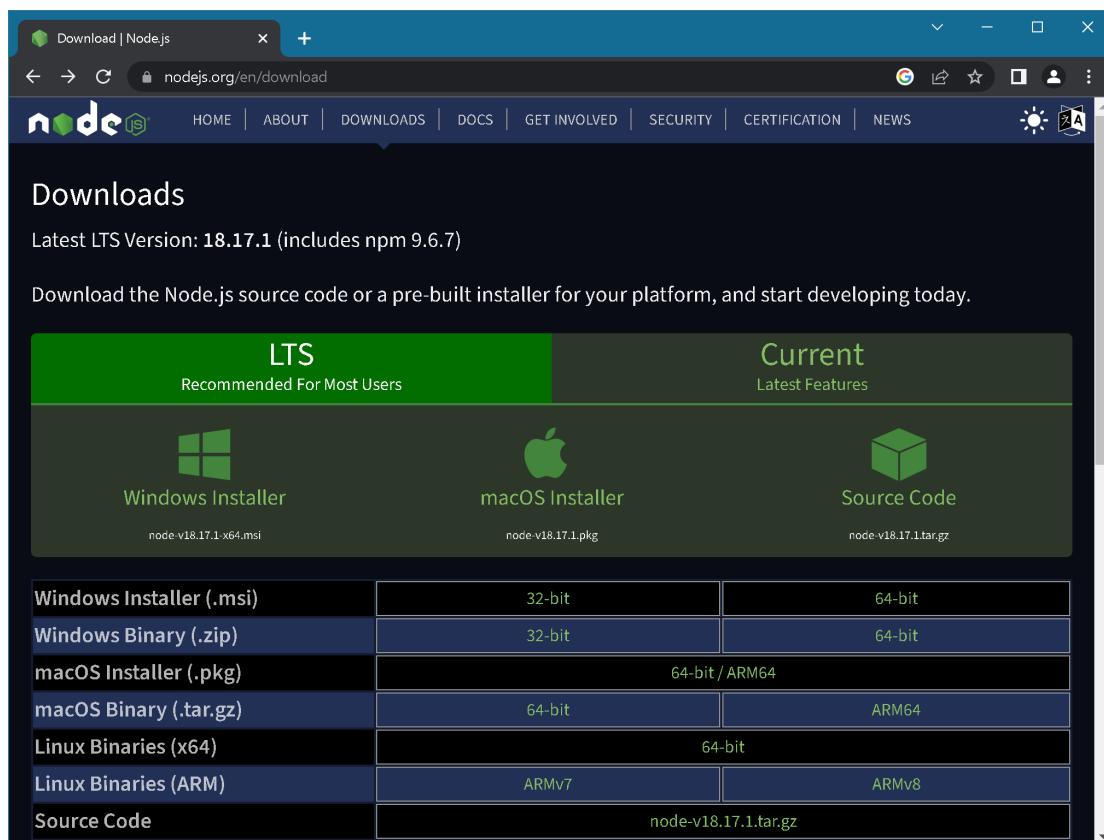
- **Geth (Go Ethereum):** Διεπαφή γραμμής εντολών (command-line interface) που επιτρέπει την εκτέλεση πλήρων κόμβων Ethereum, την εξόρυξη του κρυπτονομίσματος «Ethereum» και την εκτέλεση έξυπνων συμβολαίων.
- **Ganache:** Εφαρμογή που παρέχει ένα τοπικό Blockchain για ανάπτυξη εφαρμογών απευθυνόμενες στο Ethereum Blockchain.
- **Truffle:** Σουίτα εργαλείων ανάπτυξης «Web3» εφαρμογών.
- **Remix IDE:** Εργαλείο ανοιχτού κώδικα που εξειδικεύεται στην συγγραφή και την ανάπτυξη έξυπνων συμβολαίων σε γλώσσα προγραμματισμού «Solidity».
- **Solidity:** Αντικειμενοστραφής γλώσσα προγραμματισμού για την ανάπτυξη «έξυπνων» συμβολαίων στο Ethereum blockchain.
- **Javascript:** Αντικειμενοστραφής γλώσσα προγραμματισμού για τον εμπλουτισμό και την ενίσχυση της δυναμικότητας του γραφικού περιβάλλοντος της εφαρμογής.
- **Web3.js:** Συλλογή βιβλιοθηκών «Javascript» που επιτρέπουν την ανάπτυξη «Web3» εφαρμογών και την αλληλεπίδραση με έναν κόμβο Ethereum.
- **Bootstrap:** Πλαίσιο διασύνδεσης χρήστη (front-end framework) ανοιχτού κώδικα που χρησιμοποιείται για τη δημιουργία σύγχρονων ιστοτόπων και εφαρμογών ιστού.
- **Node.js:** Πλατφόρμα ανάπτυξης λογισμικού που επιτρέπει την εκτέλεση κώδικα «Javascript» εκτός του περιβάλλοντος ενός περιηγητή ιστού (web browser).
- **Chai:** Βιβλιοθήκη ανάπτυξης με γνώμονα τη συμπεριφορά και τις δοκιμές (Behavioral-Driven Development / Test-Driven Development - BDD/TDD) για το «Node.js», που μπορεί να συνδυαστεί με οποιοδήποτε πλαίσιο δοκιμών «Javascript».
- **Lite-server:** Δομοστοιχείο (module) του «Node.js» που λειτουργεί αποκλειστικά ως server (διακομιστής) για την ανάπτυξης μιας εφαρμογής.
- **Metamask:** Πορτοφόλι λογισμικού σε μορφή «επέκτασης» για web browser, που χρησιμοποιείται για την αλληλεπίδραση με blockchain.
- **Visual Studio Code:** Εφαρμογή επεξεργασίας κώδικα.
- **Visual Paradigm:** Εφαρμογή μοντελοποίησης και διαχείρισης έργου.
- **Ubuntu:** Λειτουργικό σύστημα στο οποίο αναπτύχθηκε και εκτελείται το ιδιωτικό δίκτυο blockchain.
- **macOS:** Λειτουργικό σύστημα στο οποίο αναπτύχθηκε η εφαρμογή.

## 7.2.1. Οδηγός εγκατάστασης απαραίτητων εφαρμογών (Windows)

Παρακάτω ακολουθούν οδηγίες εγκατάστασης των απαραίτητων τεχνικών μερών για την εκτέλεση του κώδικα εφαρμογής σε λειτουργικό σύστημα «Windows 10». Συγκεκριμένα, θα δοθούν διευκρινίσεις σχετικά με την διαδικασία εγκατάστασης του «Node.js» και των απαραίτητων, για την εκτέλεση της εφαρμογής, δομοστοιχείων του (εφεξής «modules») και της επέκτασης (extension) «Metamask» στον περιηγητή «Google Chrome». Για την ορθότερη κατανόηση του τρέχοντος και του επόμενου υποκεφαλαίου, θα χρησιμοποιηθεί τόσο το τρίτο ενικό όσο και το πρώτο πληθυντικό πρόσωπο.

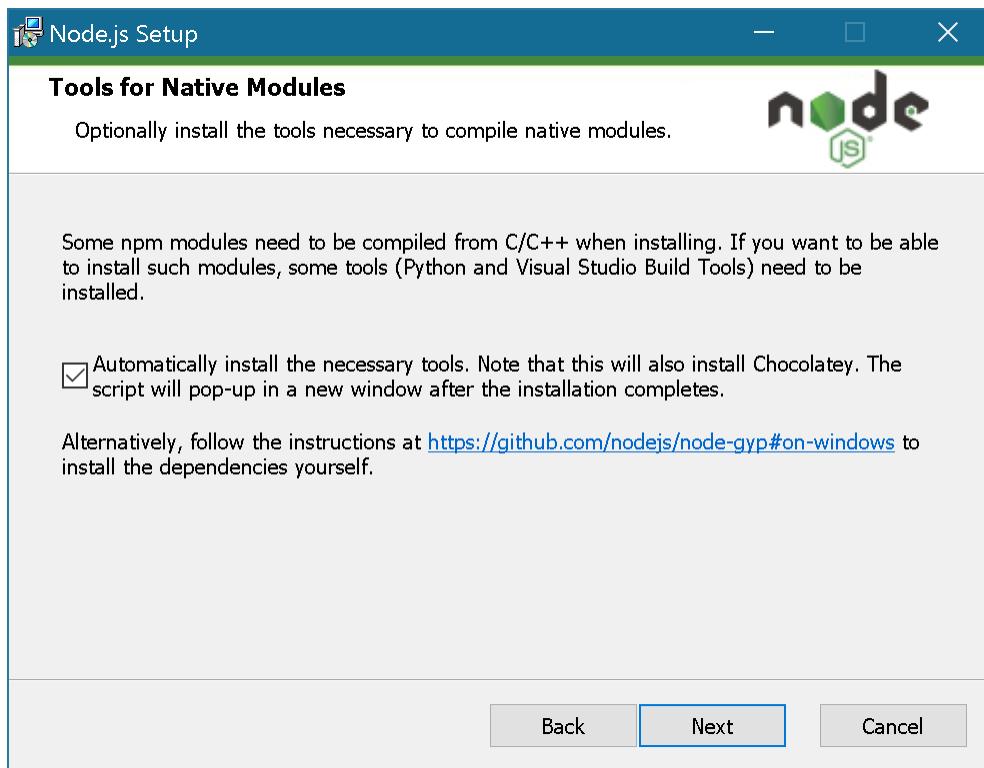
### 1. Node.js

Η λήψη του αρχείου εγκατάστασης του Node.js πραγματοποιείται από τον επίσημο ιστότοπό του μέσω του συνδέσμου: <https://nodejs.org/en/download/> (Εικόνα 58). Για τα βήματα αυτού το οδηγού, αλλά και για την επιτυχή εκτέλεση της εφαρμογής «Themis», έγινε λήψη της έκδοσης «18.17.1».



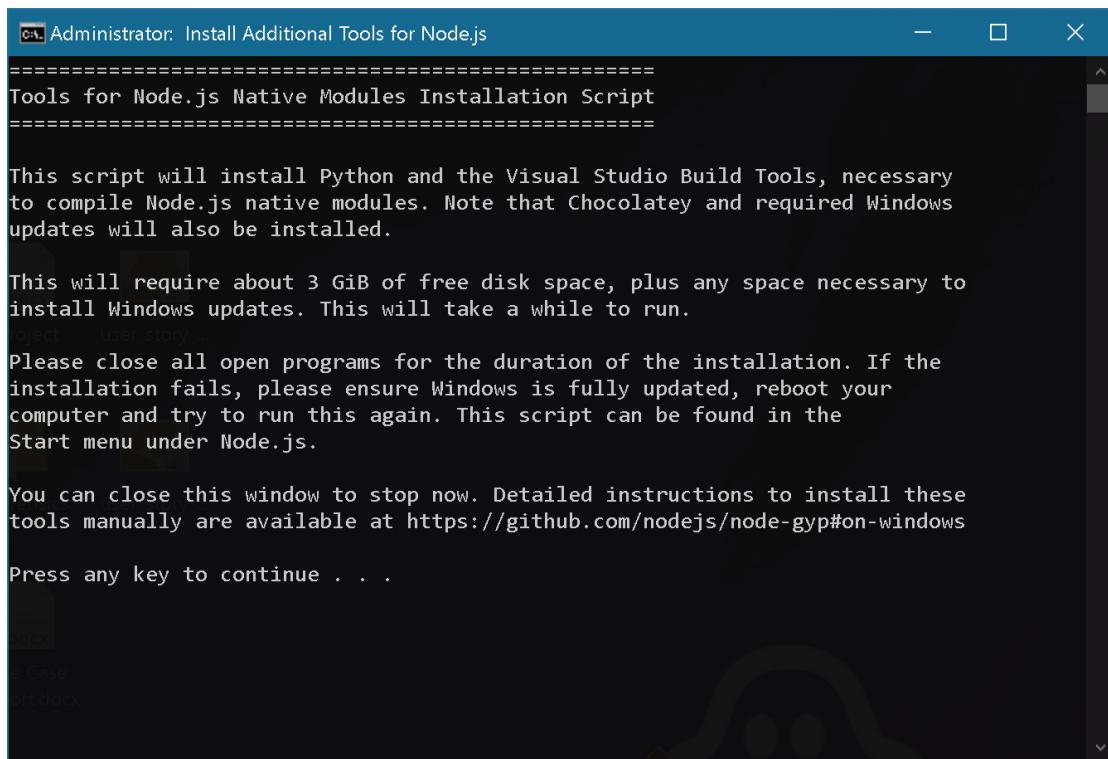
Εικόνα 58 - Ιστότοπος λήψης του «Node.js»

Αφού ολοκληρωθεί η λήψη, εκτελούμε το ληφθέν αρχείο και προχωρούμε στην διαδικασία της εγκατάστασης, ώστε ότου φτάσουμε στο βήμα της Εικόνας 59, όπου η επιλογή του πλαισίου ελέγχου (checkbox) κρίνεται αναγκαία για την εγκατάσταση πρόσθετων βασικών εργαλείων.

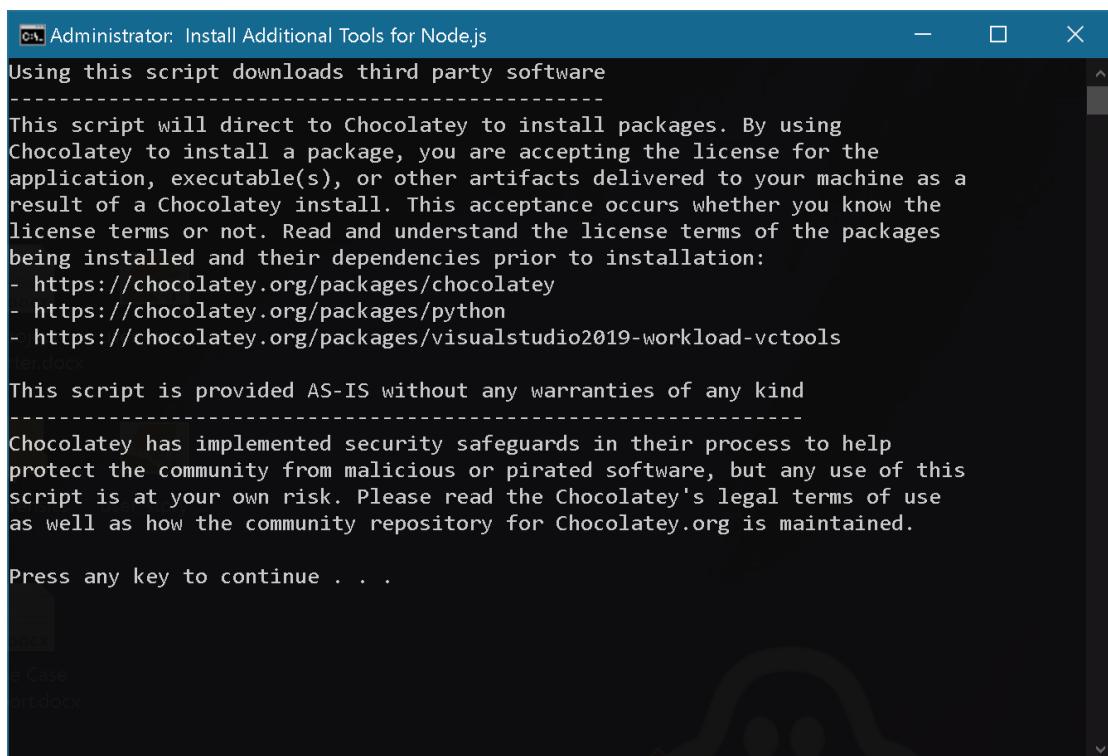


*Εικόνα 59 - Απαραίτητη επιλογή κατά την εγκατάσταση του «Node.js»*

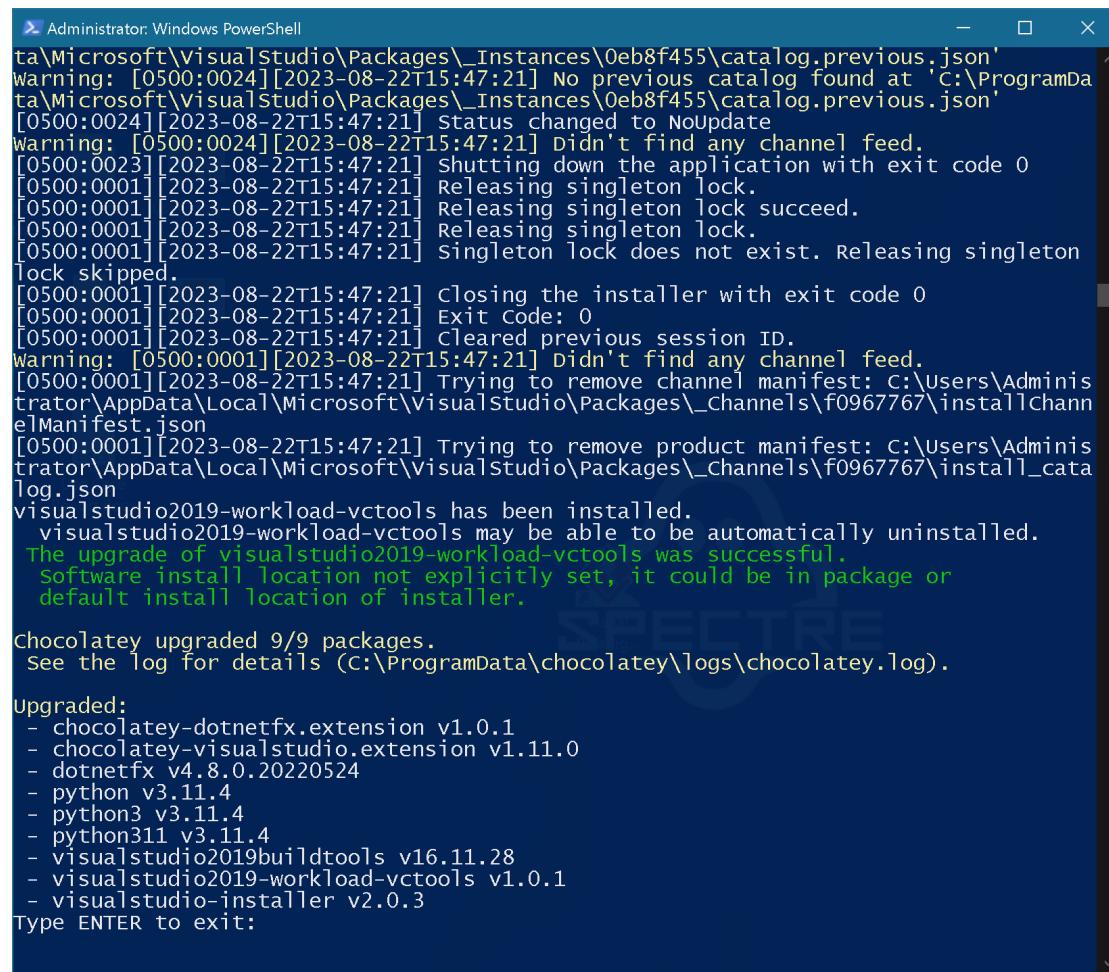
Αυτό το πλαίσιο ελέγχου, μετά το πέρας της διαδικασίας εγκατάστασης του Node.js, θα εμφανίσει δύο διαδοχικά παράθυρα γραμμής εντολών (CMD), που ζητούν από τον χρήστη να πατήσει οποιοδήποτε πλήκτρο για να συνεχίσει τη διαδικασία (Εικόνες 60 και 61). Αυτά τα παράθυρα θα αντικατασταθούν από ένα παράθυρο «Windows PowerShell», το οποίο ολοκληρώνοντας την αυτοποιημένη διαδικασία εγκατάστασης των εργαλείων, θα μοιάζει όπως αυτό της Εικόνας 62.



*Εικόνα 60 - Παράθυρο εγκατάστασης πρόσθετων εργαλείων του «Node.js» (1/2)*



*Εικόνα 61 - Παράθυρο εγκατάστασης πρόσθετων εργαλείων του «Node.js» (2/2)*



```

Administrator: Windows PowerShell
ta\Microsoft\VisualStudio\Packages\_Instances\0eb8f455\catalog.previous.json'
warning: [0500:0024][2023-08-22T15:47:21] No previous catalog found at 'C:\ProgramData\Microsoft\VisualStudio\Packages\_Instances\0eb8f455\catalog.previous.json'
[0500:0024][2023-08-22T15:47:21] Status changed to Noupdate
Warning: [0500:0024][2023-08-22T15:47:21] Didn't find any channel feed.
[0500:0023][2023-08-22T15:47:21] Shutting down the application with exit code 0
[0500:0001][2023-08-22T15:47:21] Releasing singleton lock.
[0500:0001][2023-08-22T15:47:21] Releasing singleton lock succeed.
[0500:0001][2023-08-22T15:47:21] Releasing singleton lock.
[0500:0001][2023-08-22T15:47:21] Singleton lock does not exist. Releasing singleton lock skipped.
[0500:0001][2023-08-22T15:47:21] Closing the installer with exit code 0
[0500:0001][2023-08-22T15:47:21] Exit Code: 0
[0500:0001][2023-08-22T15:47:21] Cleared previous session ID.
Warning: [0500:0001][2023-08-22T15:47:21] Didn't find any channel feed.
[0500:0001][2023-08-22T15:47:21] Trying to remove channel manifest: C:\Users\Administrator\AppData\Local\Microsoft\VisualStudio\Packages\_channels\f0967767\installManifest.json
[0500:0001][2023-08-22T15:47:21] Trying to remove product manifest: C:\Users\Administrator\AppData\Local\Microsoft\VisualStudio\Packages\_channels\f0967767\install_catalog.json
visualstudio2019-workload-vctools has been installed.
visualstudio2019-workload-vctools may be able to be automatically uninstalled.
The upgrade of visualstudio2019-workload-vctools was successful.
Software install location not explicitly set, it could be in package or default install location of installer.

Chocolatey upgraded 9/9 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Upgraded:
- chocolatey-dotnetfx.extension v1.0.1
- chocolatey-visualstudio.extension v1.11.0
- dotnetfx v4.8.0.20220524
- python v3.11.4
- python3 v3.11.4
- python311 v3.11.4
- visualstudio2019buildtools v16.11.28
- visualstudio2019-workload-vctools v1.0.1
- visualstudio-installer v2.0.3
Type ENTER to exit:

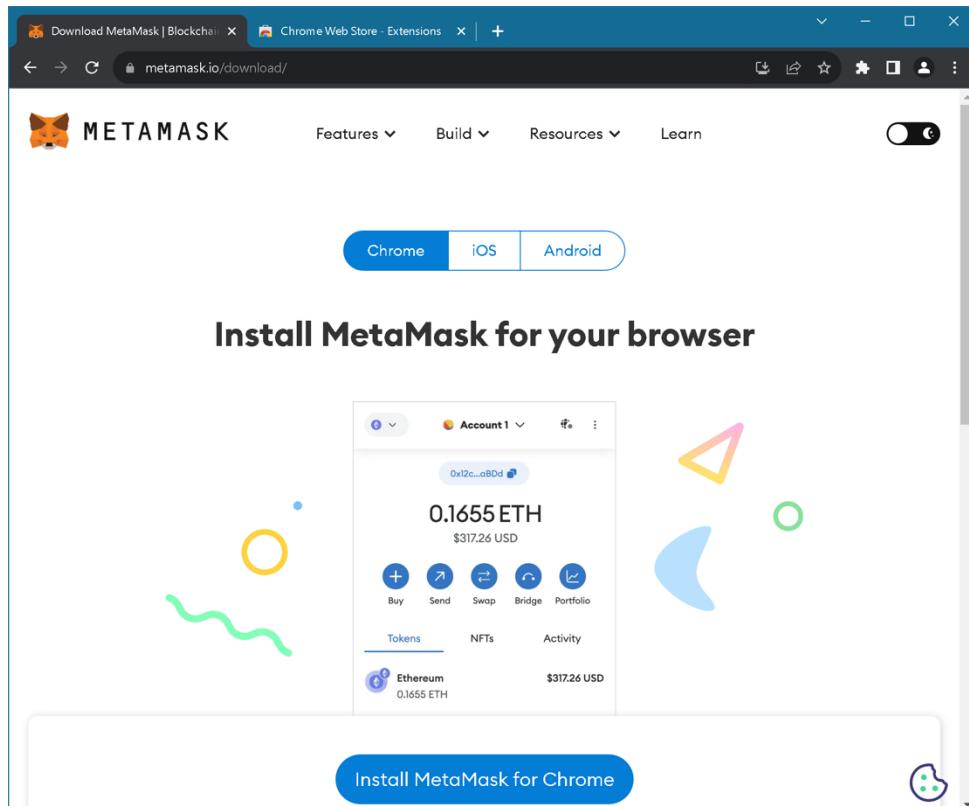
```

*Εικόνα 62 - Ολοκλήρωση της εγκατάστασης των πρόσθετων εργαλείων του «Node.js»*

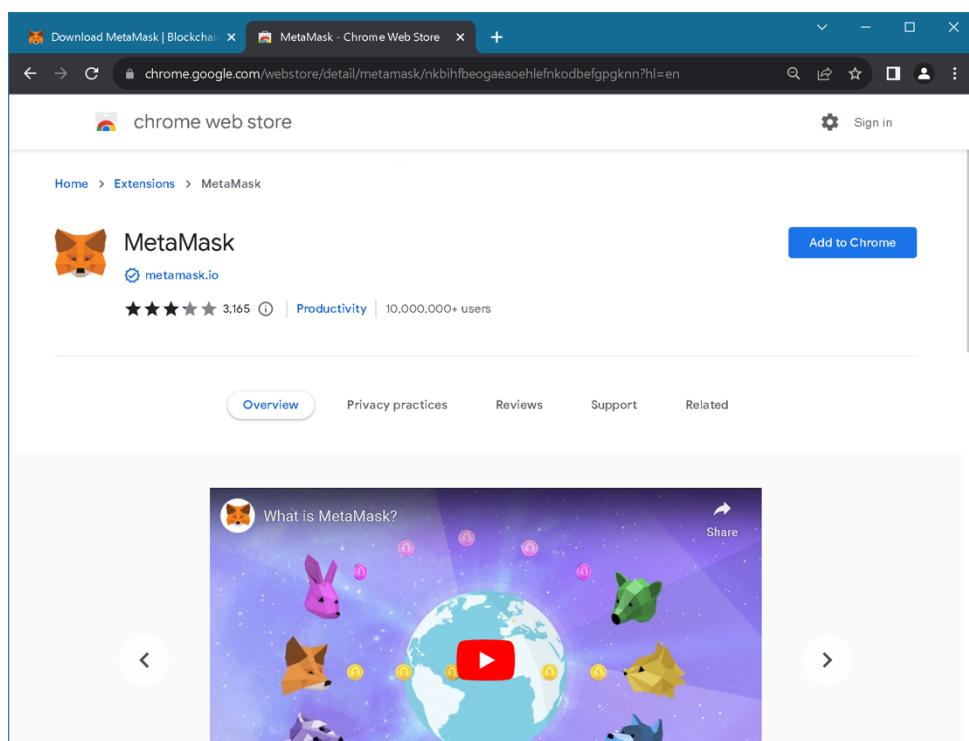
## 2. Metamask

Για την εγκατάσταση του Metamask χρειάζεται να δημιουργήσουμε έναν λογαριασμό πορτοφολιού, να προσθέσουμε το ιδιωτικό δίκτυο «ThemisChain» και τέλος, να εισάγουμε τον λογαριασμού του πρώτου κόμβου του δικτύου, μέσω του ιδιωτικού κλειδιού του.

Ξεκινώντας, κάνουμε λήψη του Metamask είτε μέσω του επίσημου ιστοτόπου του: <https://metamask.io/download/> (Εικόνα 63), είτε μέσω του ηλεκτρονικού καταστήματος του περιηγητή «Google Chrome» μεταβαίνοντας στη διεύθυνση: [https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefknkodbefgp\\_gknn](https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefknkodbefgp_gknn) (Εικόνα 64).

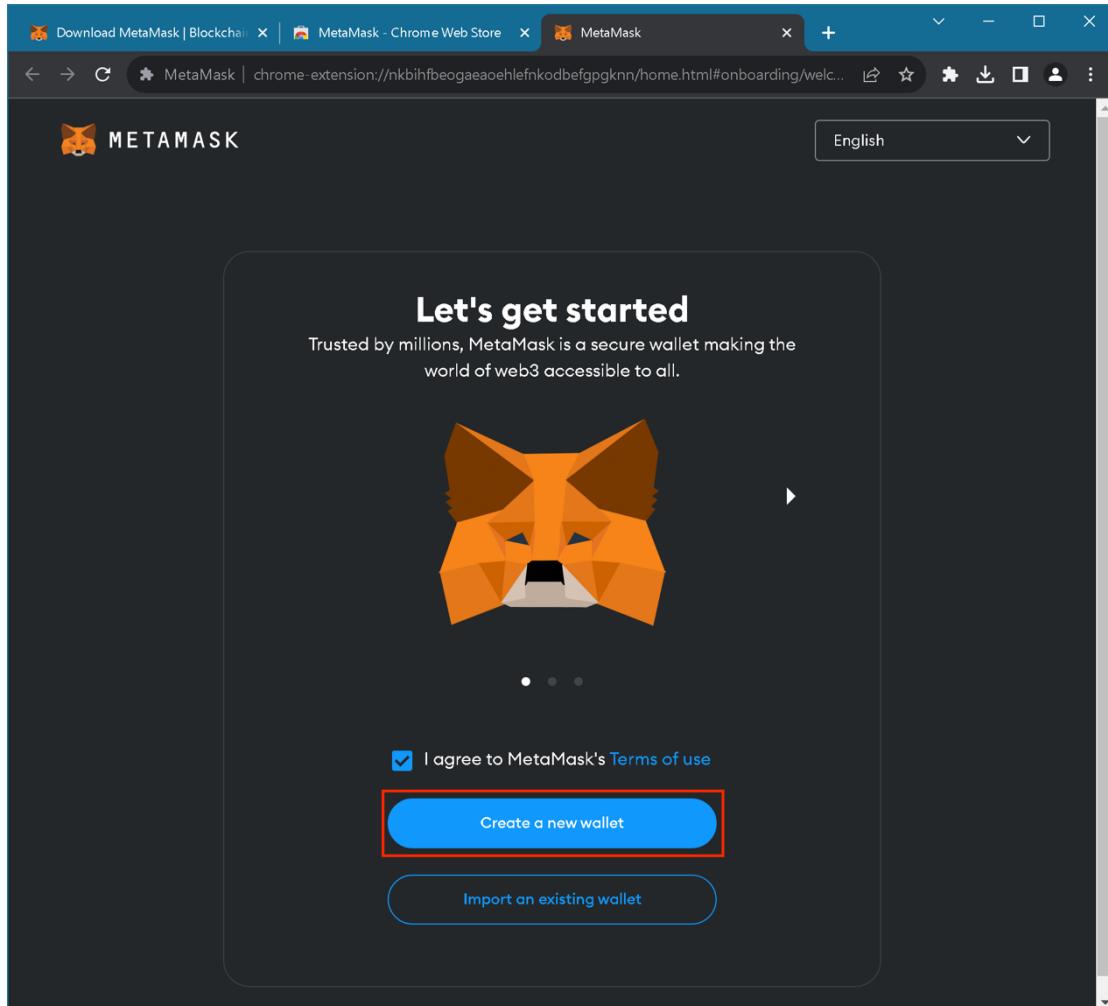


*Εικόνα 63 - Επίσημος ιστότοπος του «Metamask»*

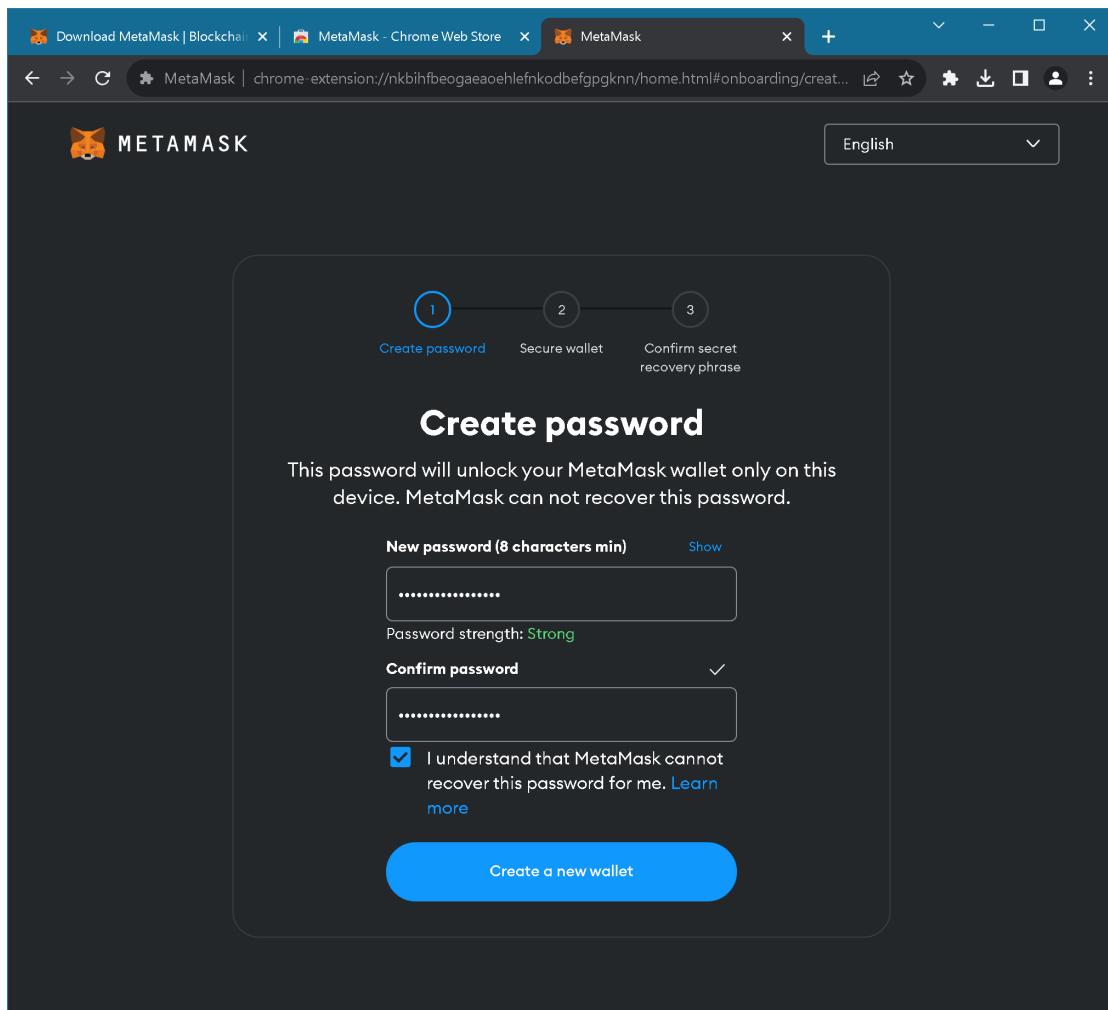


*Εικόνα 64 - Το «Metamask» στο ηλεκτρονικό κατάστημα του «Google Chrome»*

Μόλις ολοκληρωθεί η λήψη και η εγκατάσταση του Metamask, επιλέγουμε τη δημιουργία νέου λογαριασμού πορτοφολιού (Εικόνα 65) και πληκτρολογούμε τον επιθυμητό κωδικό πρόσβασης (Εικόνα 66).

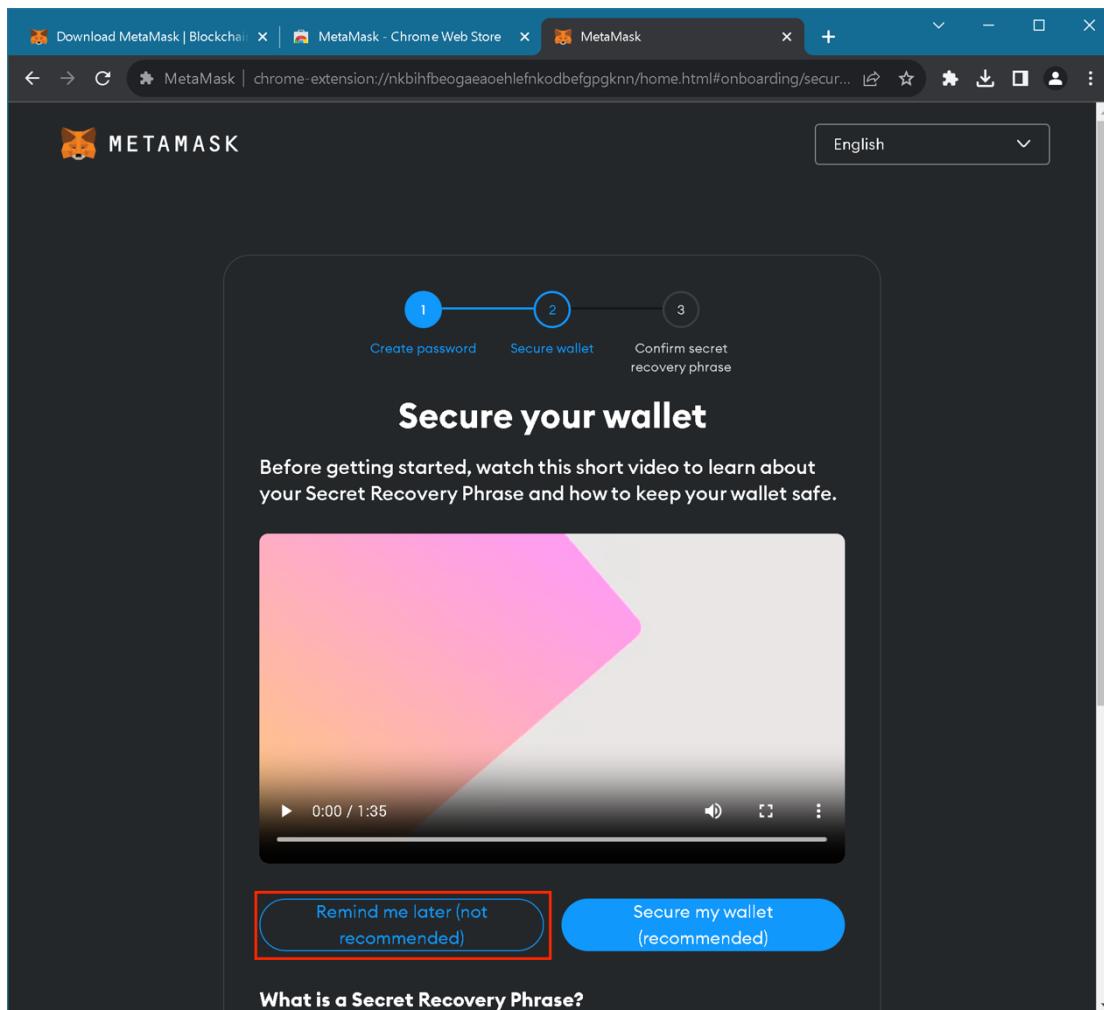


Εικόνα 65 - Επιλογή δημιουργίας νέου λογαριασμού πορτοφολιού «Metamask»



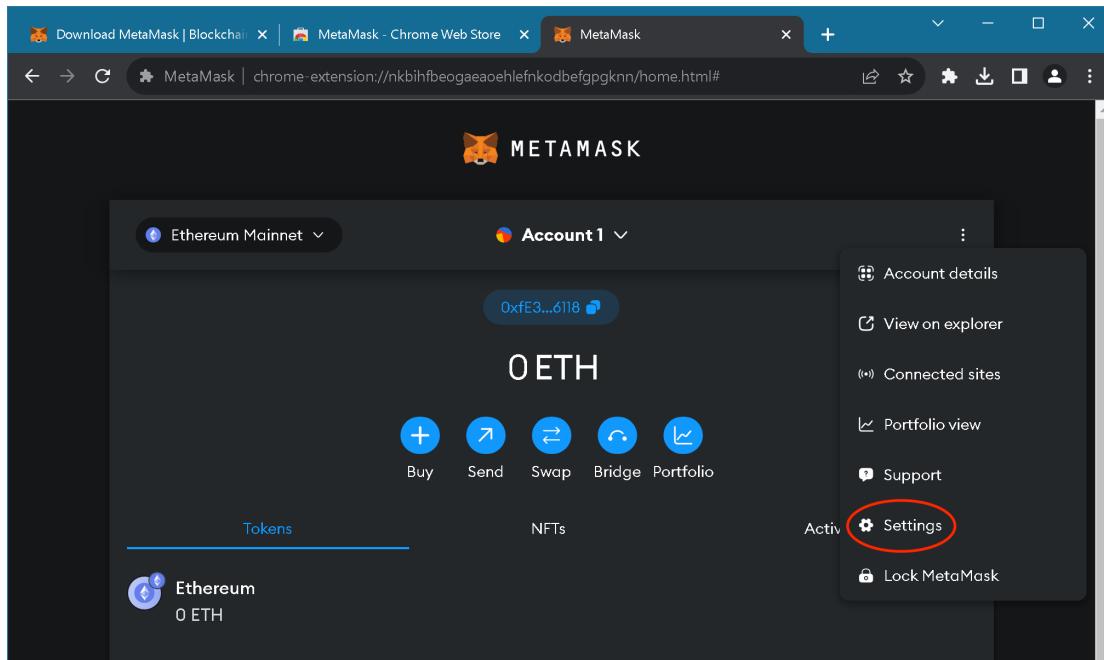
Εικόνα 66 - Εισαγωγή κωδικού πρόσβασης νέου λογαριασμού πορτοφολιού «Metamask»

Στο επόμενο βήμα, μας ζητείται να ασφαλίσουμε τον λογαριασμό μας κάνοντας χρήση μιας μοναδικής μυστικής φράσης. Καθώς όμως, ο οδηγός αυτός δημιουργήθηκε για λόγους επίδειξης, προσπερνάμε αυτό το βήμα (Εικόνα 67).

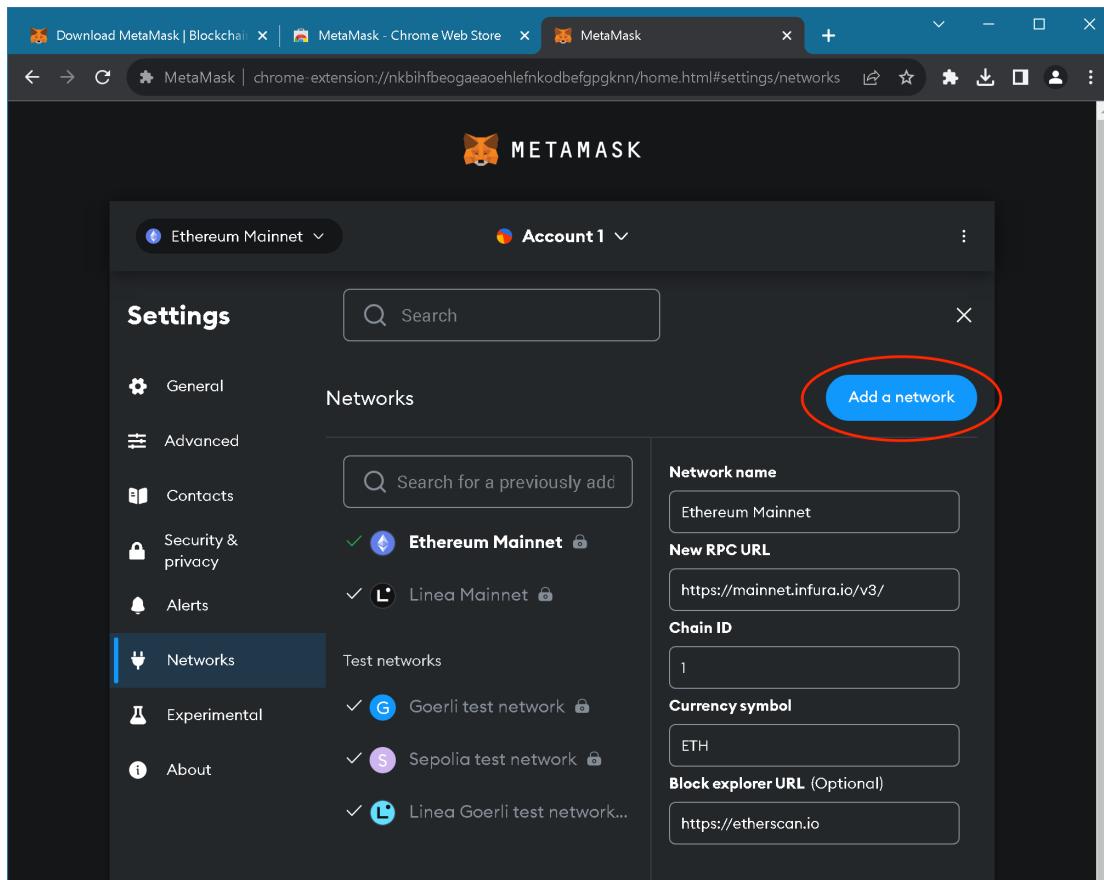


Εικόνα 67 - Ασφάλιση των λογαριασμού κάνοντας χρήση μιας μοναδικής μυστικής φράσης

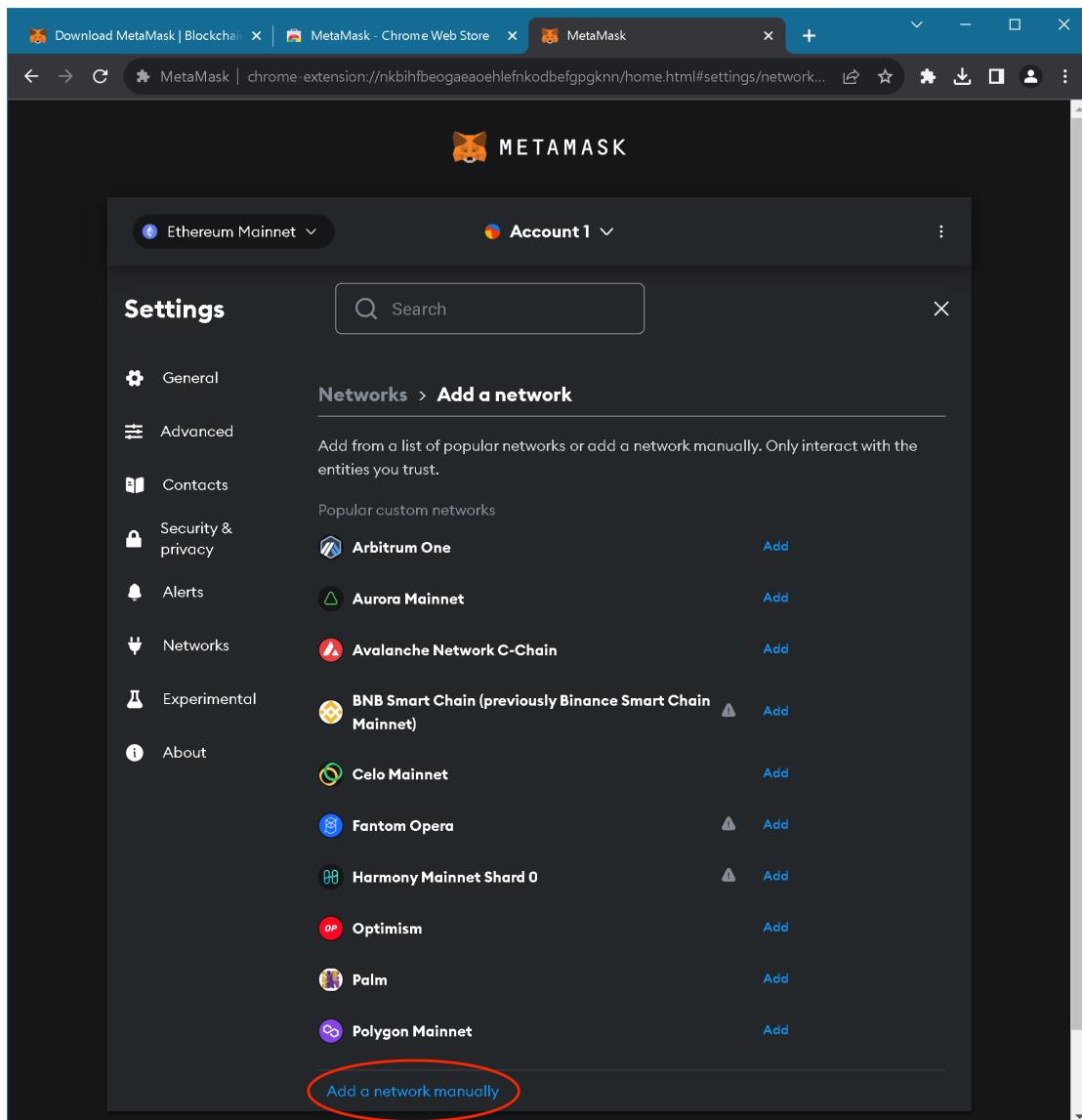
Κατόπιν διεκπεραίωσης της διαδικασίας, εμφανίζεται η αρχική σελίδα του πορτοφολιού μας, στην οποία μεταβαίνουμε στην επιλογή «Ρυθμίσεις» (Settings) του μενού (Εικόνα 68). Από εκεί, επιλέγουμε στο αριστερό μέρος την καρτέλα «Δίκτυα» (Networks), πατάμε στο κουμπί «Προσθήκη δικτύου» (Add a network) (Εικόνα 69) και στη συνέχεια, κάνουμε κλικ στην επιλογή «Προσθήκη δικτύου χειροκίνητα» (Add a network manually) (Εικόνα 70).



Εικόνα 68 - Η επιλογή «Ρυθμίσεις» (Settings) των μενού του «Metamask»



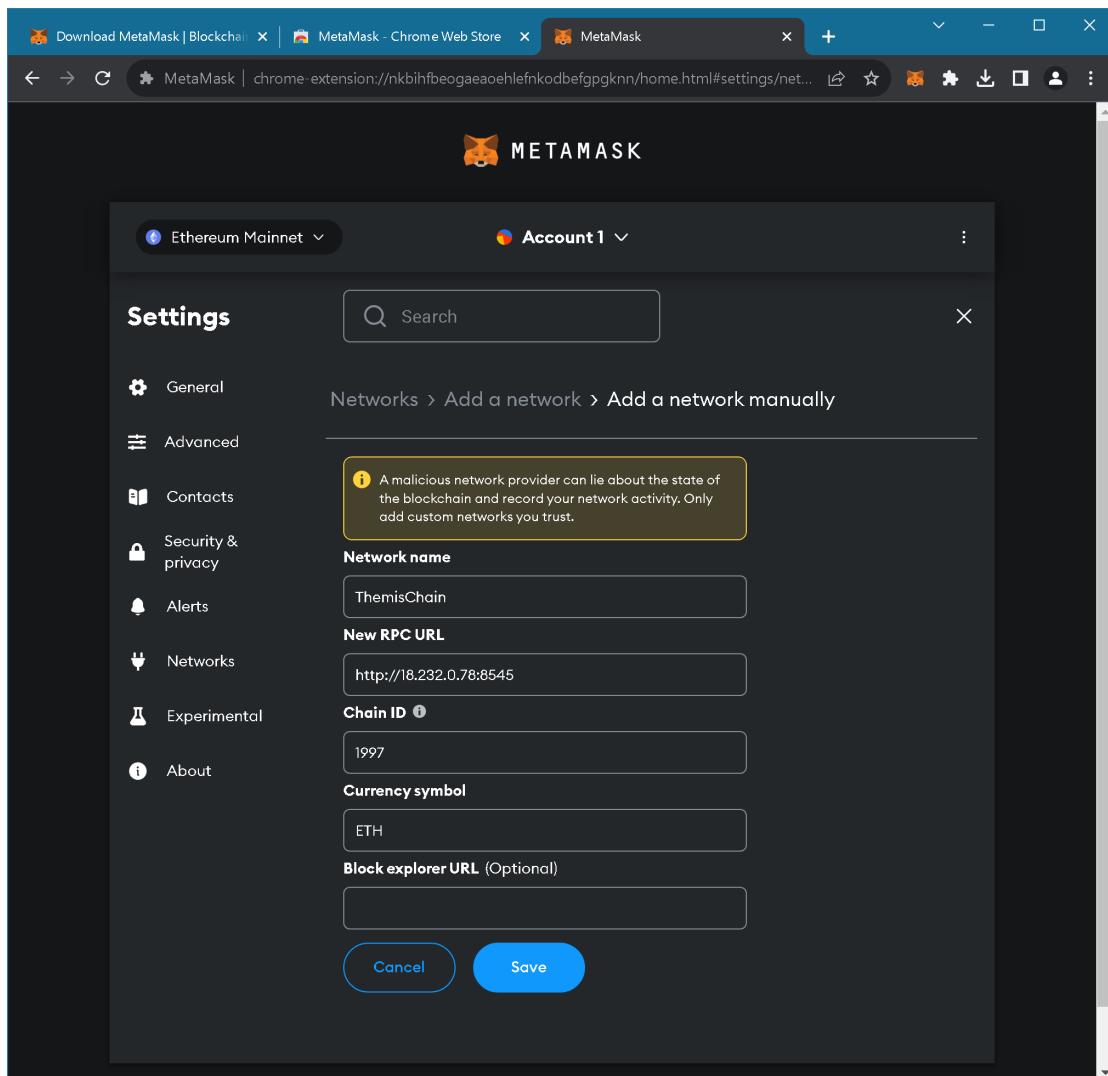
Εικόνα 69 - Το κουμπί «Προσθήκη δικτύου»



Εικόνα 70 - Η επιλογή «Προσθήκη δικτύου χειροκίνητα»

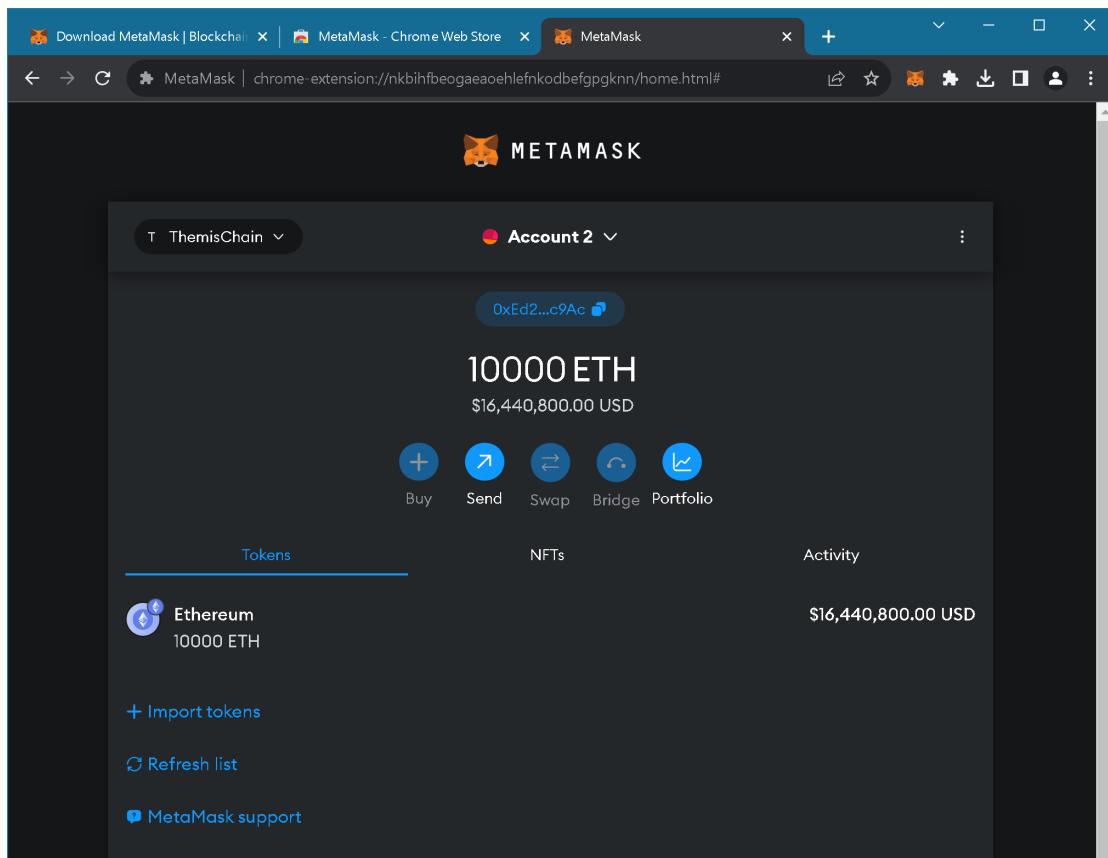
Έπειτα, πληκτρολογούμε τα παρακάτω στοιχεία του δικτύου «ThemisChain» (Εικόνα 71):

- **Network name:** ThemisChain
- **New RPC URL:** <http://18.232.0.78:8545>
- **Chain ID:** 1997
- **Currency symbol:** ETH



Εικόνα 71 - Τα στοιχεία του δικτύου «ThemisChain»

Για να εισάγουμε τον λογαριασμό του πρώτου κόμβου του δικτύου στο Metamask, ακολουθούμε τις οδηγίες που προαναφέρθηκαν στο υποκεφάλαιο 6.1 (βλ. σελίδα 87). Αν η σύνδεση με το δίκτυο και η εισαγωγή του λογαριασμού ήταν επιτυχείς, τότε θα εμφανιστεί στο Metamask ο λογαριασμός και το υπόλοιπο του σε «ETH» (Εικόνα 72).



Εικόνα 72 - Ο λογαριασμός του πρώτου κόμβου και το υπόλοιπο του σε «ETH»

### 3. Node.js Modules

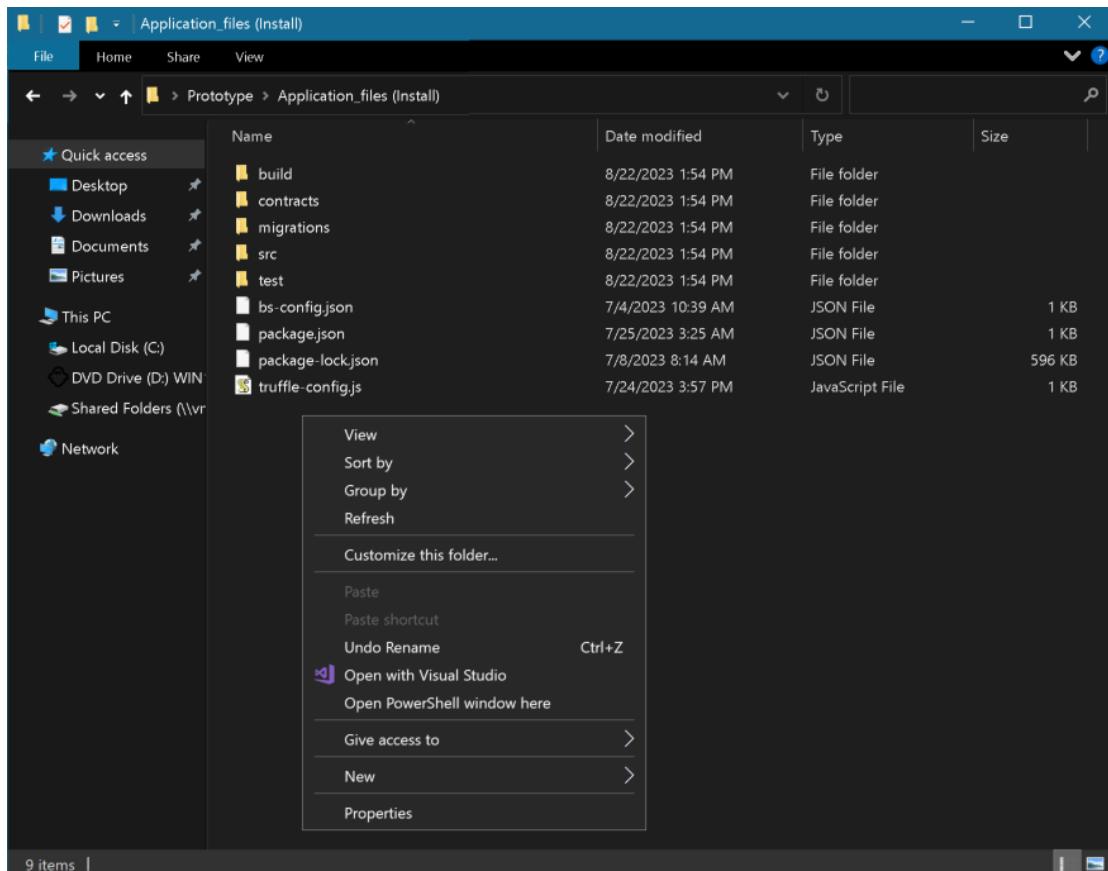
Η εγκατάσταση των modules του Node.js πραγματοποιείται με τη χρήση της εντολής «*npm install*», κατά την οποία τα modules εγκαθίστανται εκ νέου, βάσει του περιεχομένου του αρχείου «*package.json*», που βρίσκεται στον φάκελο της εφαρμογής.

Ομοίως με τον προαναφερθέν τρόπο εγκατάστασης, στα αρχεία που συνοδεύουν το έργο συμπεριλαμβάνεται ο φάκελος «*Application\_files (install)*», για τον οποίο, θα αναλυθεί παρακάτω ο τρόπος εγκατάστασής του.

#### 3.1. Η εντολή «*npm install*»

Εντός του φακέλου «*Application\_files (Install)*», χρησιμοποιούμε τον συνδυασμό πλήκτρων «Shift» + δεξί κλικ, προκειμένου να εμφανιστεί η επιλογή «Open PowerShell window here» (Εικόνα 73). Αφού το επιλέξουμε, εμφανίζεται ένα παράθυρο «Windows PowerShell», στο οποίο προβαίνουμε στην εισαγωγή της εντολής «*npm install*» (Εικόνα 74). Κατά τη διάρκεια της διεξαγωγής της διαδικασίας, αναμένεται ότι θα εμφανίζονται ποικίλα μηνύματα, τα οποία αγνοούμε. Ακόμη, μετά

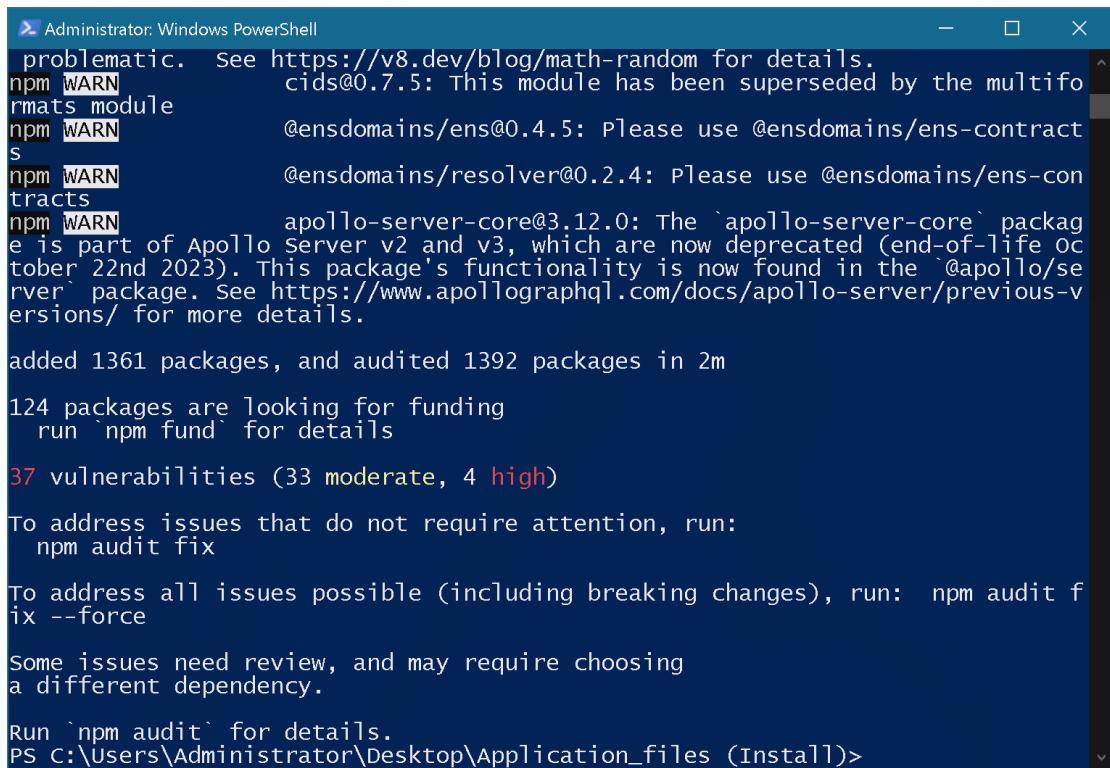
την ολοκλήρωσή της (Εικόνα 75), παρατηρείται η εμφάνιση ενός αριθμού ευπαθειών (vulnerabilities), τον οποίο επίσης αγνοούμε.



Εικόνα 73 - Ο φάκελος «Application\_files (Install)»

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\Application_files (Install)> npm install
```

Εικόνα 74 - Εκτέλεση της εντολής «npm install»



```

Administrator: Windows PowerShell
problematic. See https://v8.dev/blog/math-random for details.
npm WARN cids@0.7.5: This module has been superseded by the multifo
rmats module
npm WARN @ensdomains/ens@0.4.5: Please use @ensdomains/ens-contract
s
npm WARN @ensdomains/resolver@0.2.4: Please use @ensdomains/ens-con
tracts
npm WARN apollo-server-core@3.12.0: The `apollo-server-core` packag
e is part of Apollo Server v2 and v3, which are now deprecated (end-of-life o
ctober 22nd 2023). This package's functionality is now found in the `@apollo/se
rver` package. See https://www.apollographql.com/docs/apollo-server/previous-v
ersions/ for more details.

added 1361 packages, and audited 1392 packages in 2m

124 packages are looking for funding
  run `npm fund` for details

37 vulnerabilities (33 moderate, 4 high)

To address issues that do not require attention, run:
  npm audit fix

To address all issues possible (including breaking changes), run:
  npm audit fix --force

Some issues need review, and may require choosing
a different dependency.

Run `npm audit` for details.
PS C:\Users\Administrator\Desktop\Application_files (Install)>

```

*Εικόνα 75 - Τα αποτελέσματα της εντολής «npm install»*

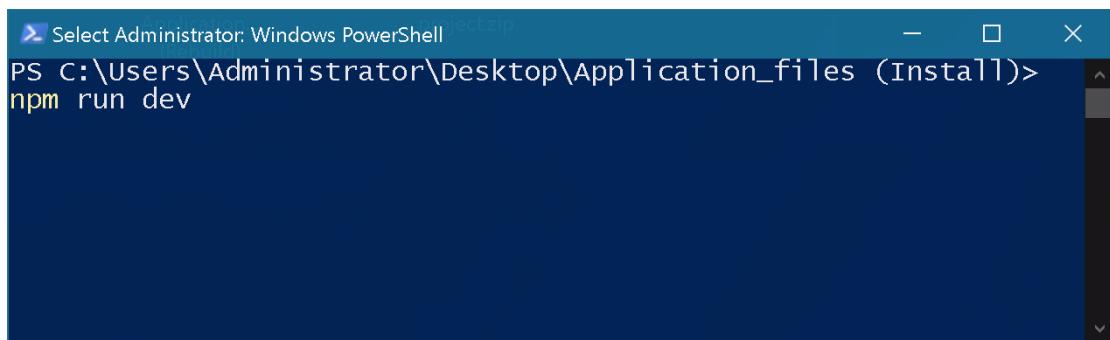
### 7.3. Περιγραφή περίπτωσης χρήσης

Η περίπτωση χρήσης που θα παρουσιαστεί παρακάτω αφορά τον ρόλο του διαχειριστή (admin) και την αλληλεπίδρασή του με το σύνολο των λειτουργιών της εφαρμογής. Οι λειτουργίες αυτές περιλαμβάνουν:

- Την προβολή του προφίλ του ερευνητή
- Την προσθήκη ενός νέου ερευνητή
- Την διαχείριση του συνόλου των ερευνητών που έχουν καταχωρηθεί στο blockchain
- Το «άνοιγμα» μιας νέας υπόθεσης
- Την προβολή των ενεργών υποθέσεων που έχουν ανατεθεί σε έναν ερευνητή
- Την διαχείριση του συνόλου των υποθέσεων που έχουν καταχωρηθεί στο blockchain
- Την προσθήκη ενός αποδεικτικού στοιχείου σε μια την υπόθεση
- Την αναζήτηση των αποδεικτικών στοιχείων μιας υπόθεσης
- Την μεταβίβαση της κυριότητας ενός αποδεικτικού στοιχείου

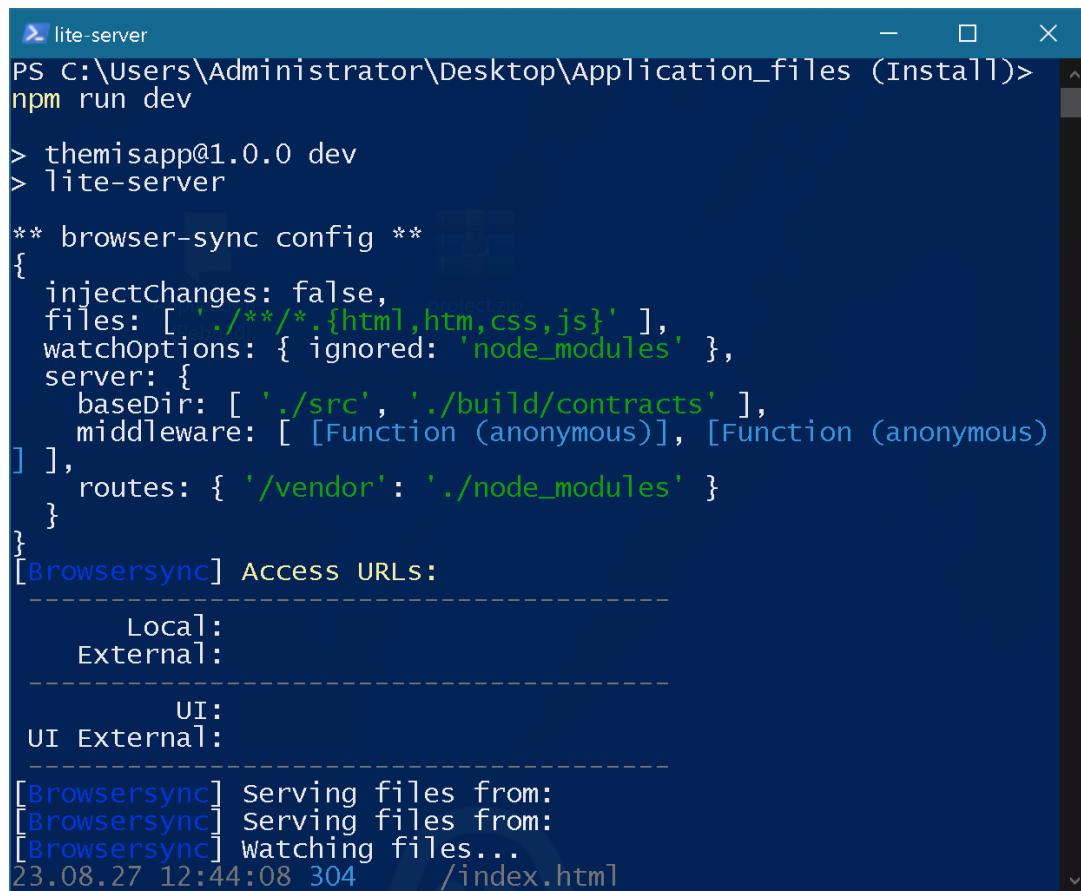
- Την προβολή του chain of custody ενός αποδεικτικού στοιχείου

Έχοντας προσθέσει στο «Metamask» τον λογαριασμό του πρώτου κόμβου – που αντιστοιχεί σε έναν από τους τρεις διαχειριστές (βλ. σελίδες 79, 87) – σειρά έχει η ενεργοποίηση ενός τοπικού διακομιστή, κάνοντας χρήση του module «lite-server» του Node.js, στον οποίο θα εκτελεστεί ο κώδικας της εφαρμογής ώστε να είναι προσβάσιμη από τον περιηγητή ιστού, μέσω της διεύθυνσης «<http://localhost:3000/>». Εκτελώντας ένα παράθυρο «Windows PowerShell» εντός του φακέλου που περιέχει τα αρχεία της εφαρμογής (βλ. σελίδα 108), πληκτρολογούμε την εντολή «`npm run dev`» (Εικόνα 76). Ο διακομιστής ο οποίος ενεργοποιείται (Εικόνα 77), θα πρέπει να παραμείνει ενεργός καθ' όλη τη διάρκεια εκτέλεσης της εφαρμογής.



```
PS C:\Users\Administrator\Desktop\Application_files (Install)> npm run dev
```

Εικόνα 76 - Εκτέλεση της εντολής «`npm run dev`»



```

lite-server
PS C:\Users\Administrator\Desktop\Application_files (Install)> npm run dev

> themisapp@1.0.0 dev
> lite-server

** browser-sync config **

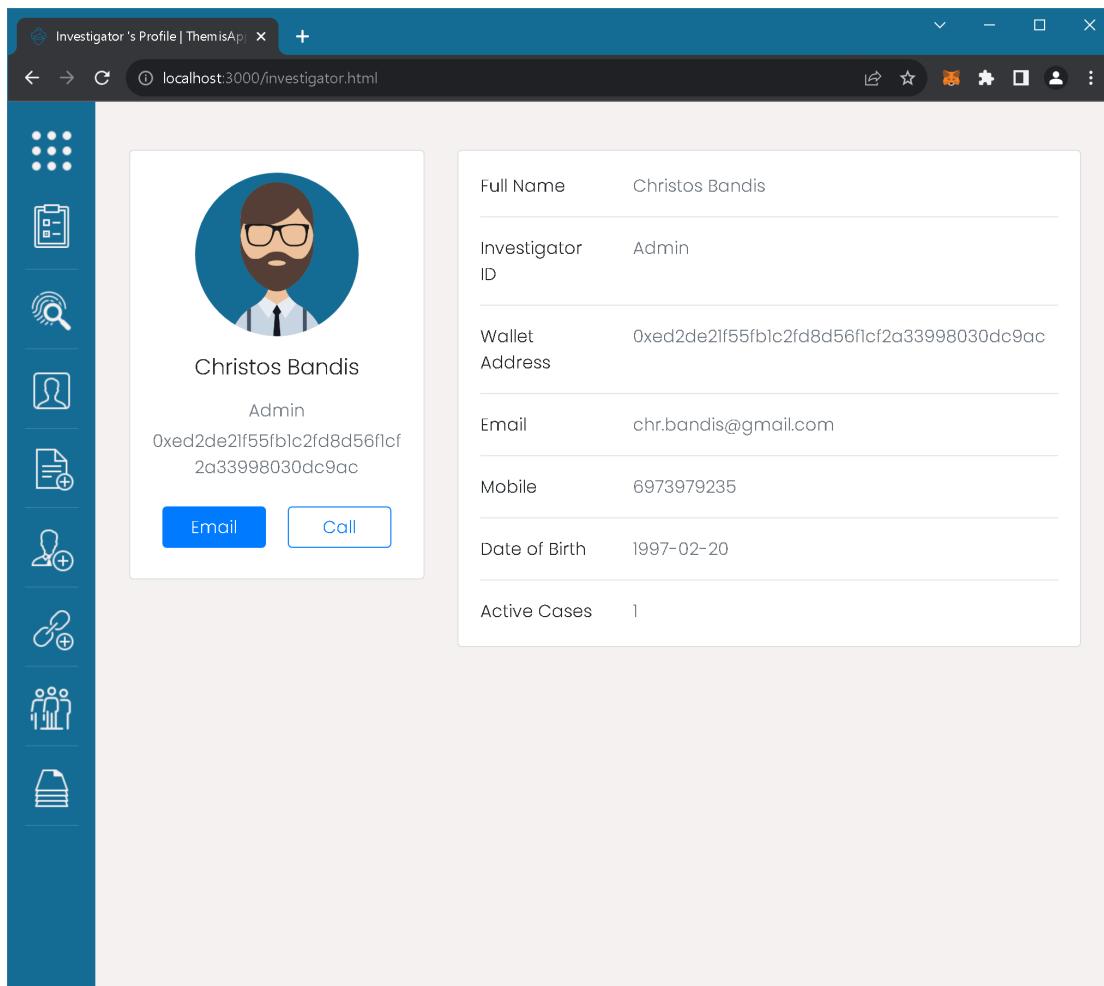
{
  injectChanges: false,
  files: ['./**/*.{html,htm,css,js}'],
  watchOptions: { ignored: 'node_modules' },
  server: {
    baseDir: ['./src', './build/contracts'],
    middleware: [ [Function (anonymous)], [Function (anonymous)] ],
    routes: { '/vendor': './node_modules' }
  }
}
[Browsersync] Access URLs:
-----[redacted]
  Local: [redacted]
  External: [redacted]
-----[redacted]
  UI: [redacted]
  UI External: [redacted]
-----[redacted]
[Browsersync] Serving files from:
[Browsersync] Serving files from:
[Browsersync] Watching files...
23.08.27 12:44:08 304      /index.html

```

*Εικόνα 77 - Ενεργοποίηση του τοπικού διακομιστή του module «lite-server»*

## • Προβολή του προφίλ του ερευνητή

Μόλις ο χρήστης μεταβεί στην αρχική σελίδα της εφαρμογής (βλ. σελίδα 90) και συνδεθεί επιτυχώς με τον λογαριασμό πορτοφολιού του, μέσω του αναδυόμενου παραθύρου του «Metamask», ανακατευθύνεται στη σελίδα που περιέχει το προφίλ του ερευνητή – είτε είναι απλός ερευνητής, είτε ερευνητής με δικαιώματα διαχειριστή – η οποία περιέχει στοιχεία της ταυτότητάς του, όπως: το ονοματεπώνυμο, το email, τη διεύθυνση του πορτοφολιού του στο blockchain και τις ενεργές υποθέσεις του (Εικόνα 78).

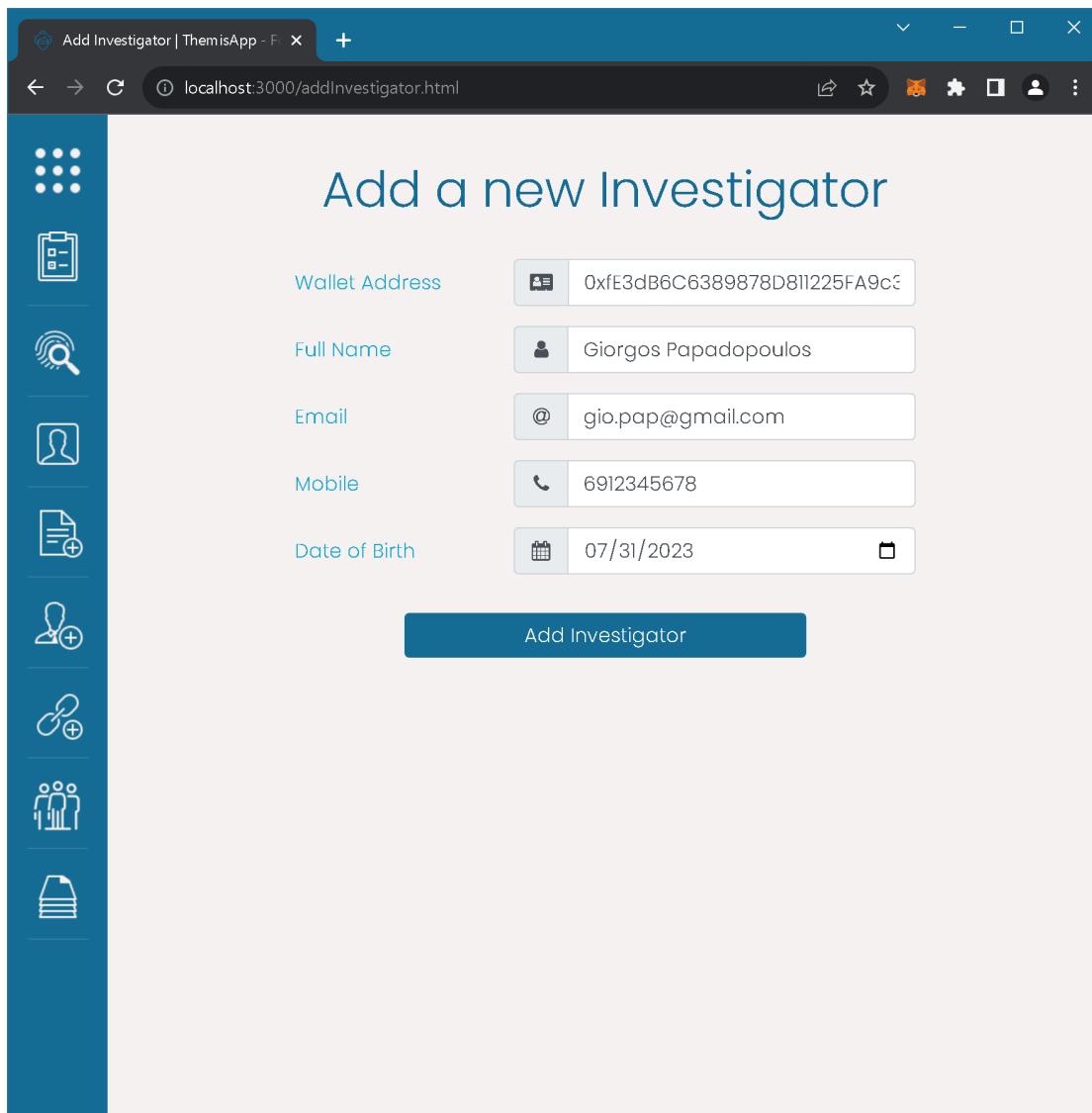


Full Name	Christos Bandis
Investigator ID	Admin
Wallet Address	0xed2de21f55fb1c2fd8d56f1cf2a33998030dc9ac
Email	chr.bandis@gmail.com
Mobile	6973979235
Date of Birth	1997-02-20
Active Cases	1

Εικόνα 78 - Η σελίδα που περιέχει το προφίλ του ερευνητή - διαχειριστή

### • Προσθήκη ενός νέου ερευνητή

Επόμενη λειτουργία της εφαρμογής προς παρουσίαση, είναι η προσθήκη ενός νέου ερευνητή στην εφαρμογή και κατ' επέκταση στο blockchain. Μέσω του μενού στα αριστερά της εφαρμογής, ο διαχειριστής μεταβαίνει στη σελίδα «Add a new Investigator», στην οποία συμπληρώνει τη φόρμα με τα κατάλληλα στοιχεία ταυτότητας του νέου ερευνητή (Εικόνα 79).



Add Investigator | ThermisApp - F X +

localhost:3000/addInvestigator.html

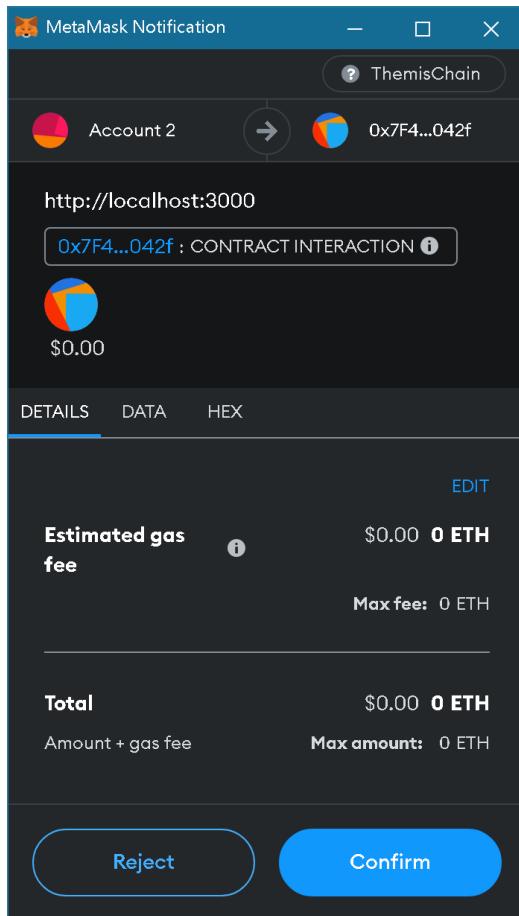
## Add a new Investigator

Wallet Address	<input type="text" value="0xfE3dB6C6389878D811225FA9c3"/>
Full Name	<input type="text" value="Giorgos Papadopoulos"/>
Email	<input type="text" value="gio.pap@gmail.com"/>
Mobile	<input type="text" value="6912345678"/>
Date of Birth	<input type="text" value="07/31/2023"/> <input type="button" value=""/>

Add Investigator

Εικόνα 79 - Η σελίδα «Add a new Investigator»

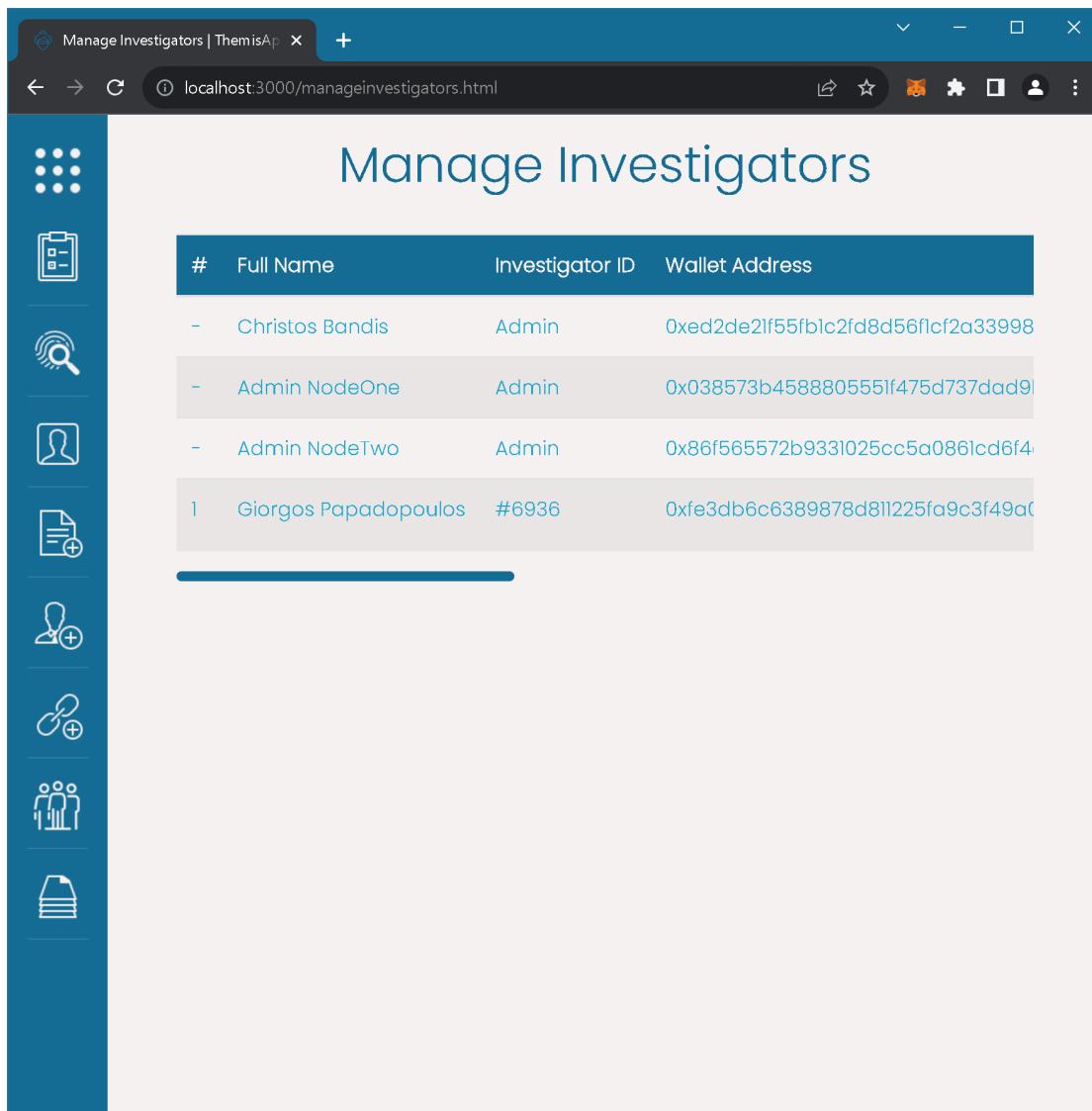
Πατώντας στο κουμπί «Add Investigator», εμφανίζεται το παράθυρο έγκρισης συναλλαγής του «Metamask», το οποίο επιβεβαιώνει αυτό που αναφέρθηκε στο Κεφάλαιο 6 (βλ. σελίδα 67), πως οι διεκπεραίωση συναλλαγών έχει μηδενικό κόστος, εξαιτίας του μεγάλου μεγέθους των δεδομένων που περιέχουν (Εικόνα 80). Το ίδιο ισχύει για όλο το φάσμα των συναλλαγών εντός της εφαρμογής.



Εικόνα 80 - Επιβεβαίωση του μηδενικού κόστους συναλλαγών εντός της εφαρμογής

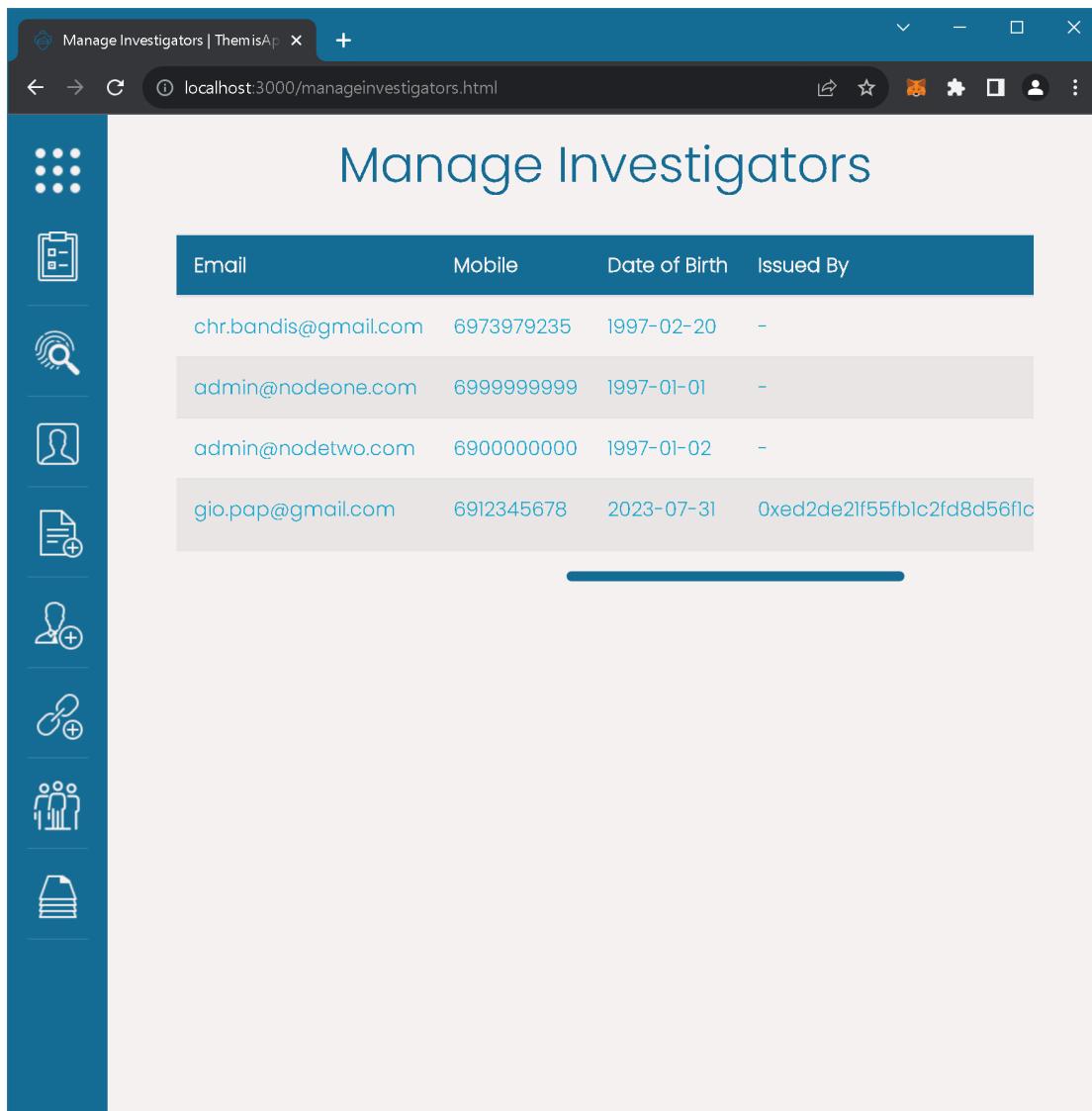
- **Διαχείριση των συνόλου των ερευνητών που έχουν καταχωρηθεί στο blockchain**

Ένας διαχειριστής έχει δικαίωμα να ελέγξει όλους τους ερευνητές που έχουν καταχωρηθεί στο blockchain, από τη σελίδα «Manage Investigators» (Εικόνες 81 και 82). Στον πίνακα που παρουσιάζεται εντός της σελίδας, περιέχονται στοιχεία της ταυτότητας των ερευνητών, όπως: το ονοματεπώνυμο, το αναγνωριστικό (για τους διαχειριστές είναι «Admin», ενώ για τους ερευνητές είναι ένας τυχαίος τετραψήφιος αριθμός) και η διεύθυνση πορτοφολιού του διαχειριστή που καταχώρησε την ταυτότητα.



#	Full Name	Investigator ID	Wallet Address
-	Christos Bandis	Admin	0xed2de21f55fb1c2fd8d56f1cf2a33998
-	Admin NodeOne	Admin	0x038573b4588805551f475d737dad91
-	Admin NodeTwo	Admin	0x86f565572b9331025cc5a0861cd6f4
1	Giorgos Papadopoulos	#6936	0xfe3db6c6389878d811225fa9c3f49a0...

Εικόνα 81 - Η σελίδα «Manage Investigators» (1/2)

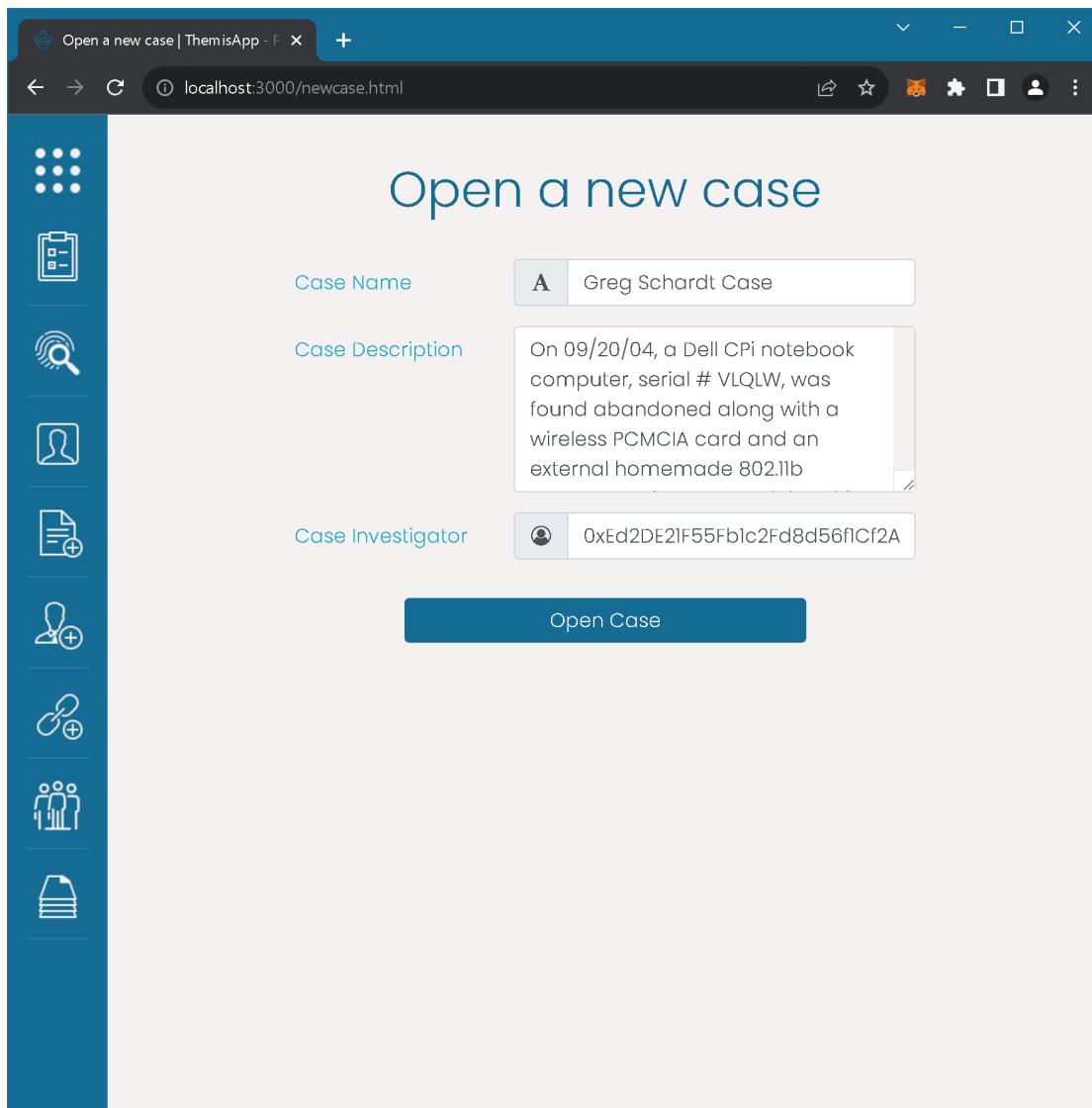


Email	Mobile	Date of Birth	Issued By
chr.bandis@gmail.com	6973979235	1997-02-20	-
admin@nodeone.com	69999999999	1997-01-01	-
admin@nodeltwo.com	69000000000	1997-01-02	-
gio.pap@gmail.com	6912345678	2023-07-31	0xed2de21f55fb1c2fd8d56fc

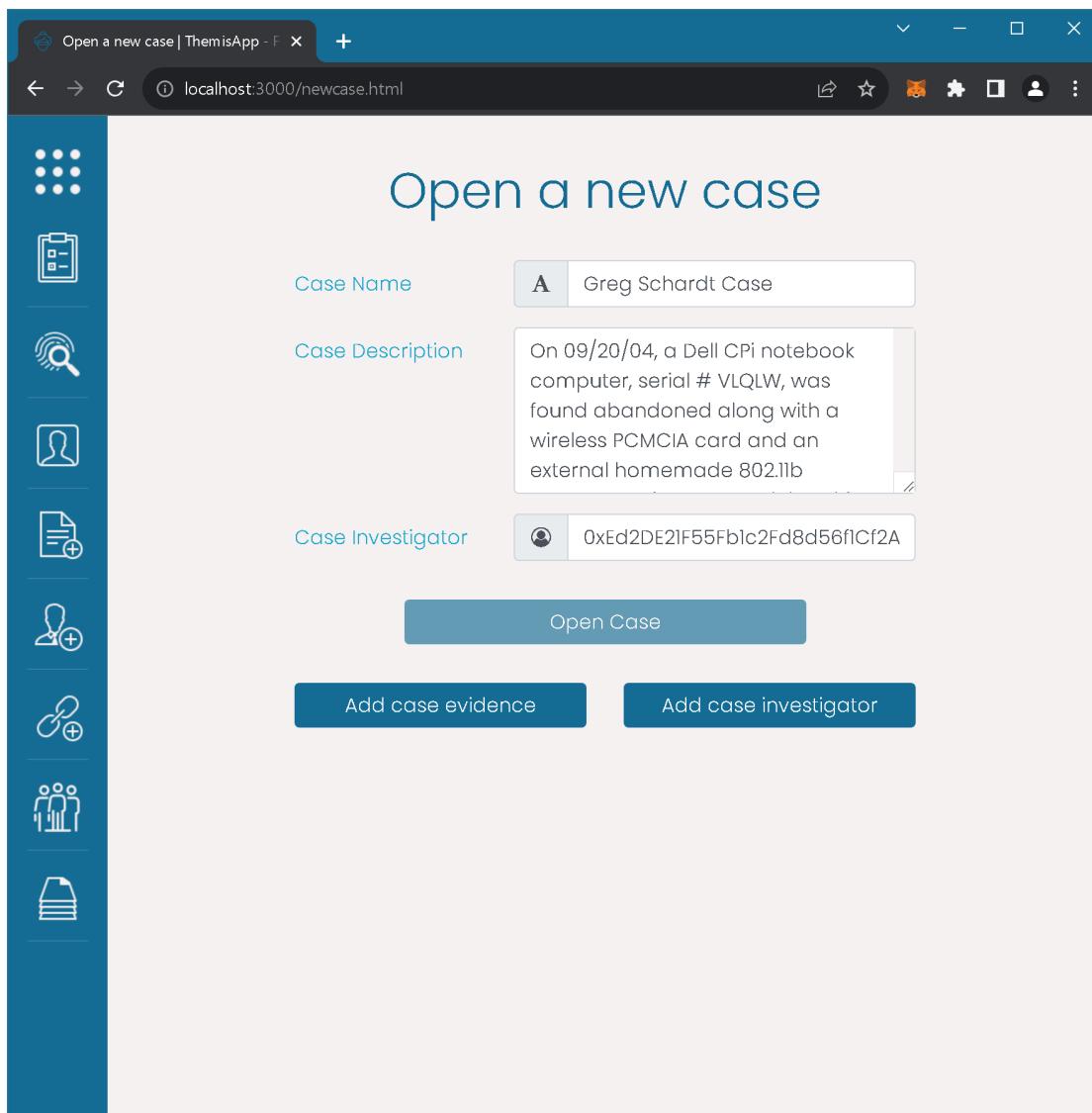
Εικόνα 82 - Η σελίδα «Manage Investigators» (2/2)

- **«Άνοιγμα» μιας νέας υπόθεσης**

Το «άνοιγμα» μιας νέας υπόθεσης πραγματοποιείται μέσω της φόρμας που βρίσκεται στη σελίδα «Open a new case», στην οποία ζητούνται το όνομα, η περιγραφή και η διεύθυνση πορτοφολιού του ερευνητή, στον οποίο θα ανατεθεί η υπόθεση (Εικόνα 83). Αφού ολοκληρωθεί η διαδικασία, εμφανίζονται ακριβώς κάτω από το κομπί «Open Case», δύο επιπλέον κουμπιά: τα «Add case evidence» και «Add case investigator» (Εικόνα 84). Στην προκειμένη χρονική στιγμή δε θα εκτελεστεί καμία από τις δύο ενέργειες, καθώς θα εκτελεστούν μεμονωμένα στη συνέχεια.

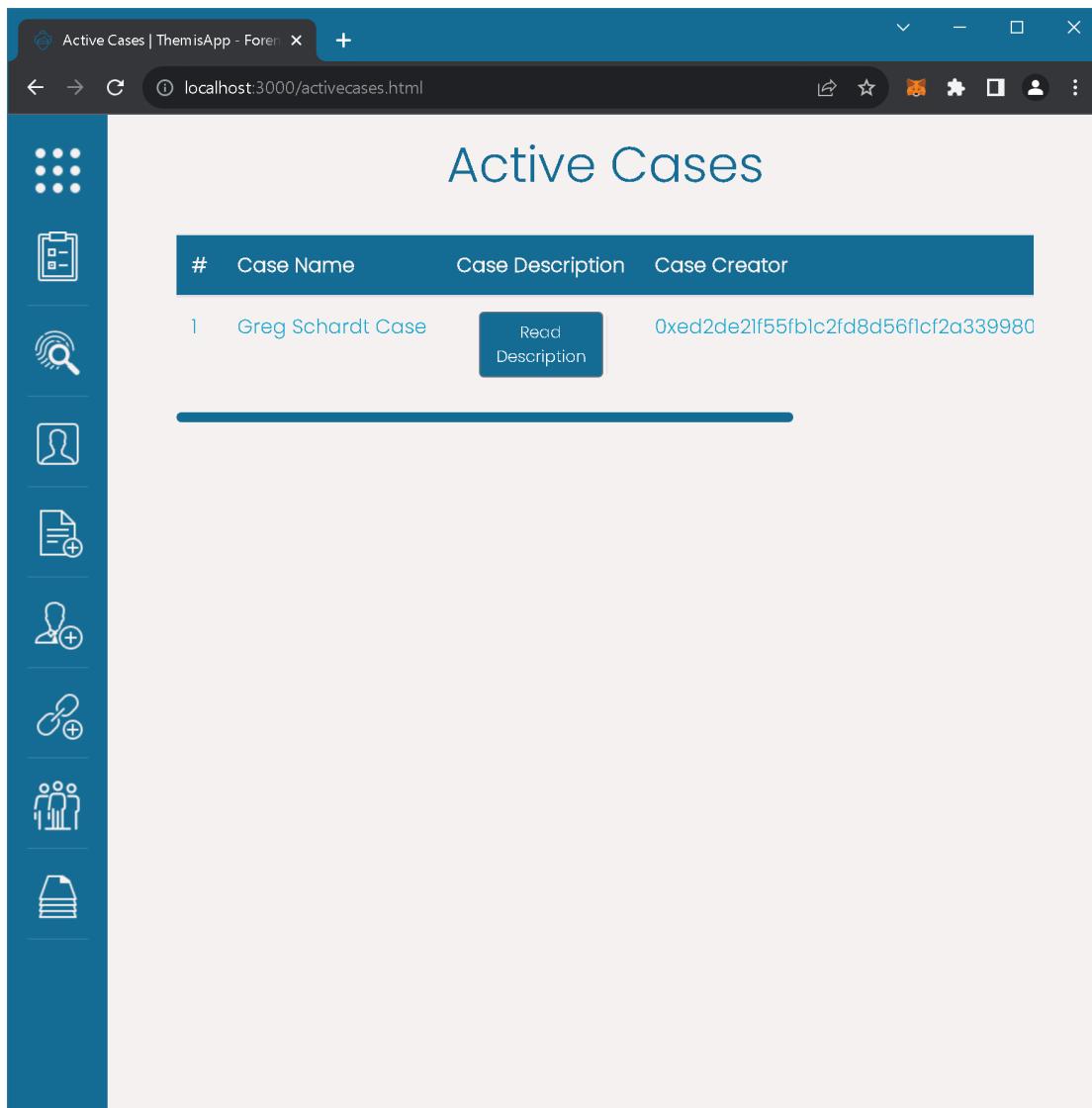


Εικόνα 83 - Η σελίδα «Open a new case» (1/2)



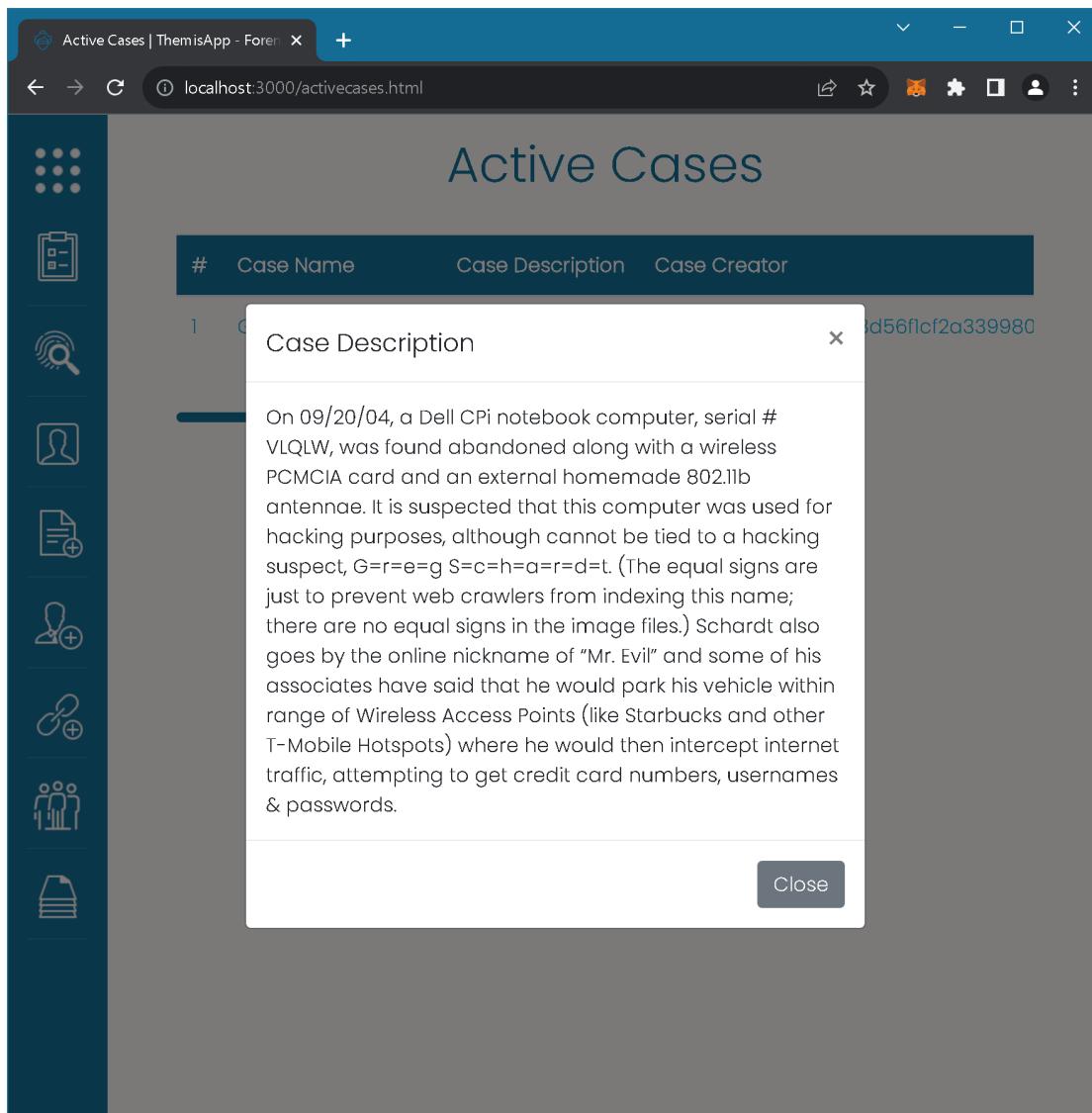
Εικόνα 84 - Η σελίδα «Open a new case» (2/2)

- **Προβολή των ενεργών υποθέσεων που έχουν ανατεθεί σε έναν ερευνητή**  
Ένας ερευνητής - διαχειριστής έχει τη δυνατότητα να παρακολουθεί τις ενεργές υποθέσεις του στη σελίδα «Active Cases» (Εικόνα 85 και 86).



#	Case Name	Case Description	Case Creator
1	Greg Schardt Case	<a href="#">Read Description</a>	0xed2de2lf55fb1c2fd8d56f1cf2a339980

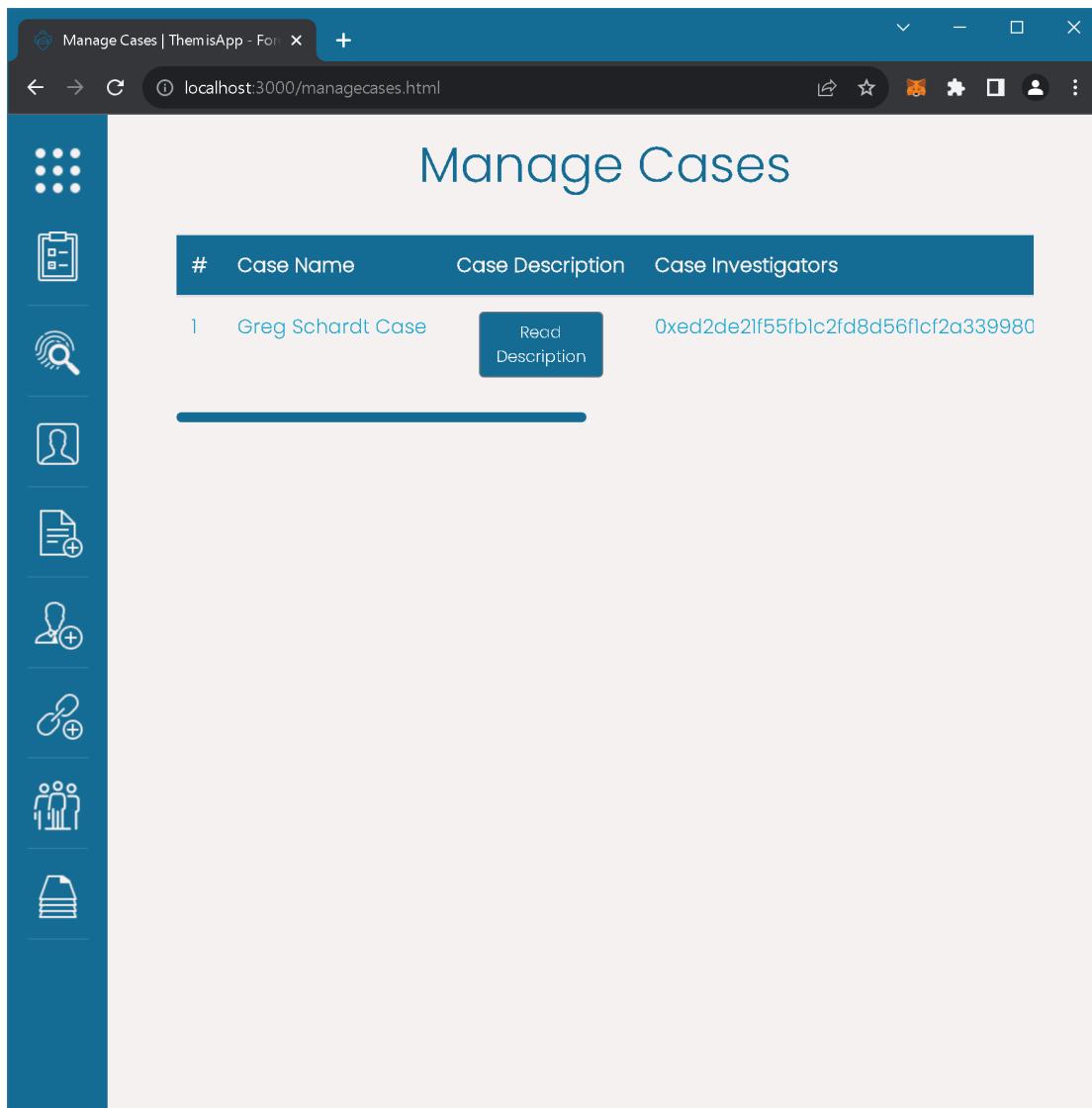
*Eikόνα 85 - Η σελίδα «Active Cases»*



Εικόνα 86 - Προβολή περιγραφής υπόθεσης

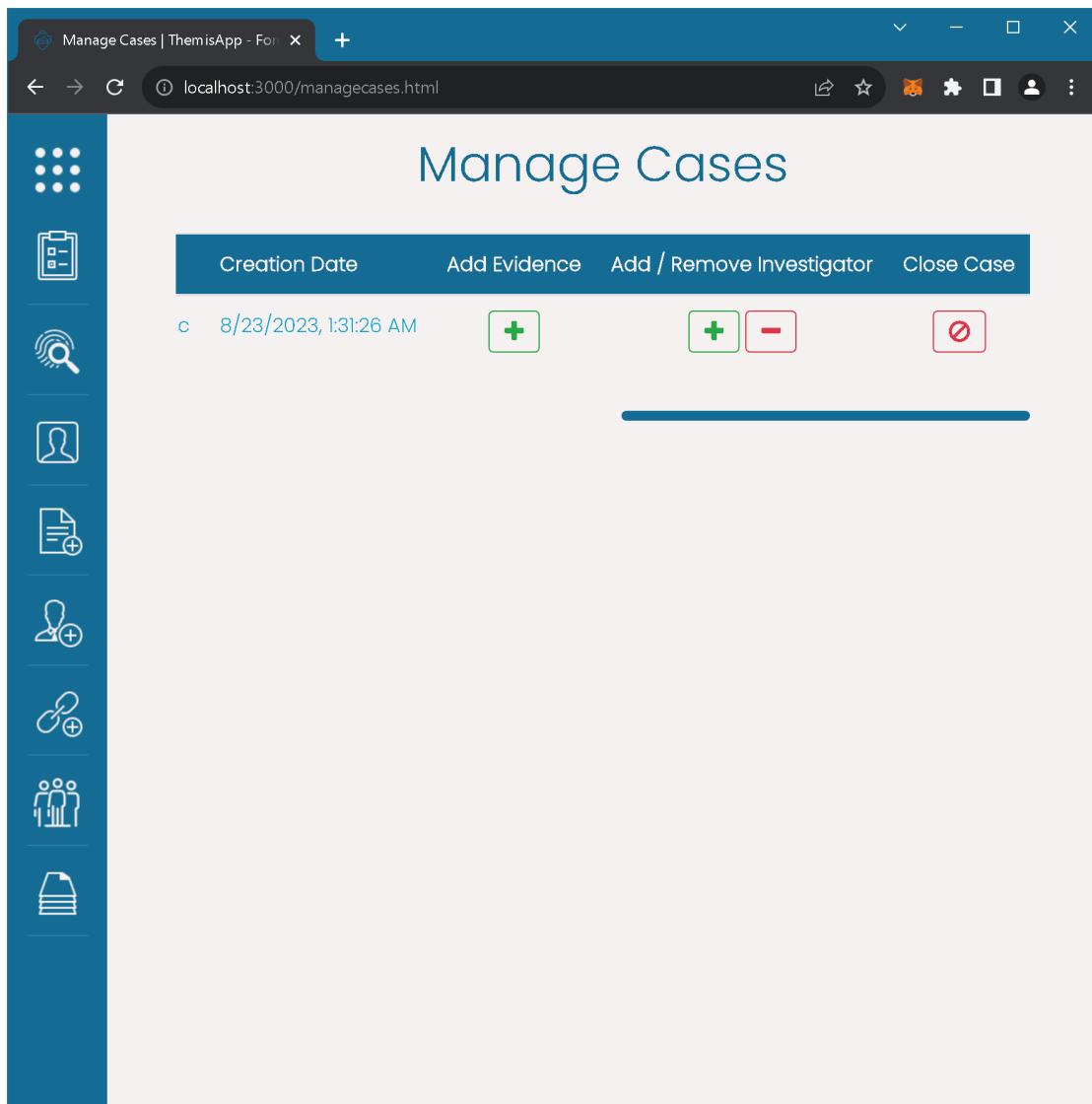
- Διαχείριση του συνόλου των υποθέσεων που έχουν καταχωρηθεί στο blockchain**

Ομοίως με τη διαχείριση του συνόλου των ερευνητών, ένας διαχειριστής έχει δικαίωμα να ελέγχει όλες τις υποθέσεις που έχουν καταχωρηθεί στο blockchain. Αυτό επιτυγχάνεται μέσω της σελίδα «Manage Cases» (Εικόνες 87 και 88). Ο πίνακας που περιέχεται στη σελίδα, παρουσιάζει πληροφορίες για την εκάστοτε υπόθεση, αλλά παρέχει και μια σειρά ενεργειών που μπορούν να εφαρμοστούν σε κάθε μία από αυτές. Στην Εικόνα 89, απεικονίζεται η διαδικασία προσθήκης ενός επιπλέον ερευνητή στην υπόθεση χρησιμοποιώντας τη διεύθυνση του πορτοφολιού του, ενώ στην Εικόνα 90 γίνεται ορατό το αποτέλεσμα της, με την υπόθεση να έχει ανατεθεί πλέον σε δύο ερευνητές.



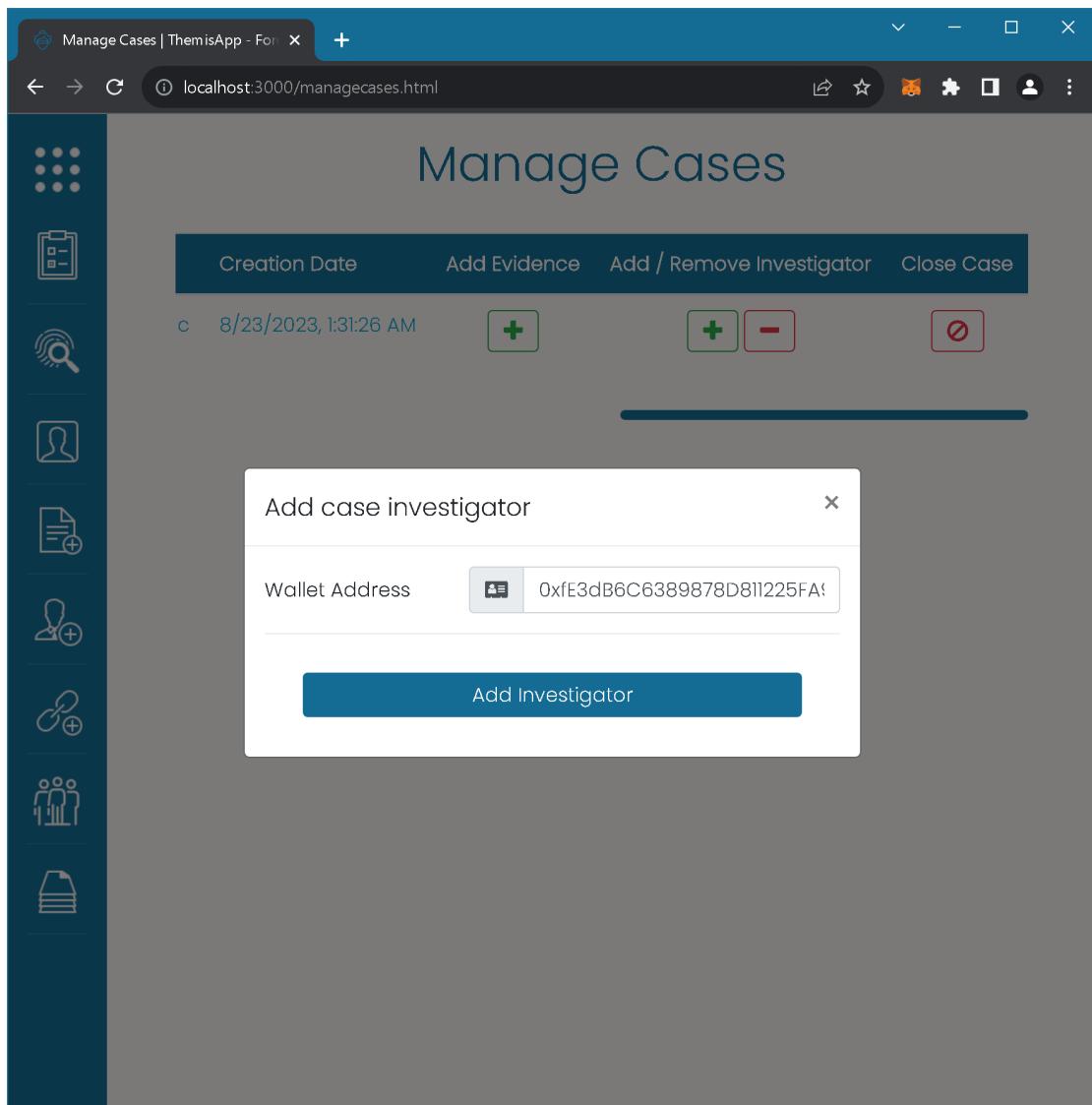
The screenshot shows a web-based application titled "Manage Cases". The interface includes a sidebar with various icons for navigation, such as a grid, a clipboard, a magnifying glass, a user profile, a document with a plus sign, a person with a plus sign, a gear, and a stack of papers. The main content area has a header with columns: "#", "Case Name", "Case Description", and "Case Investigators". A single row of data is displayed, showing entry #1, the case name "Greg Schardt Case", a placeholder for the case description, and the investigator identifier "0xed2de2lf55fb1c2fd8d56f1cf2a339980". A blue button labeled "Read Description" is visible next to the description field.

Εικόνα 87 - Η σελίδα «Manage Cases» (1/2)



The screenshot shows a web-based application titled "Manage Cases". On the left is a vertical sidebar with eight icons: a grid, a clipboard, a magnifying glass, a user profile, a document with a plus sign, a user with a plus sign, a gear, and a stack of papers. The main area has a blue header bar with buttons for "Manage Cases | ThemisApp - For" (with a dropdown arrow), a search icon, a refresh icon, a "+" icon, and a close button. Below the header is a URL bar showing "localhost:3000/managecases.html". The main content area has a title "Manage Cases" and a sub-header with four buttons: "Creation Date" (blue), "Add Evidence" (green), "Add / Remove Investigator" (grey), and "Close Case" (red). Below these buttons is a timestamp "c 8/23/2023, 1:31:26 AM" and three small buttons: a green one with a plus sign, a red one with a minus sign, and a red one with a zero symbol.

Εικόνα 88 - Η σελίδα «Manage Cases» (2/2)



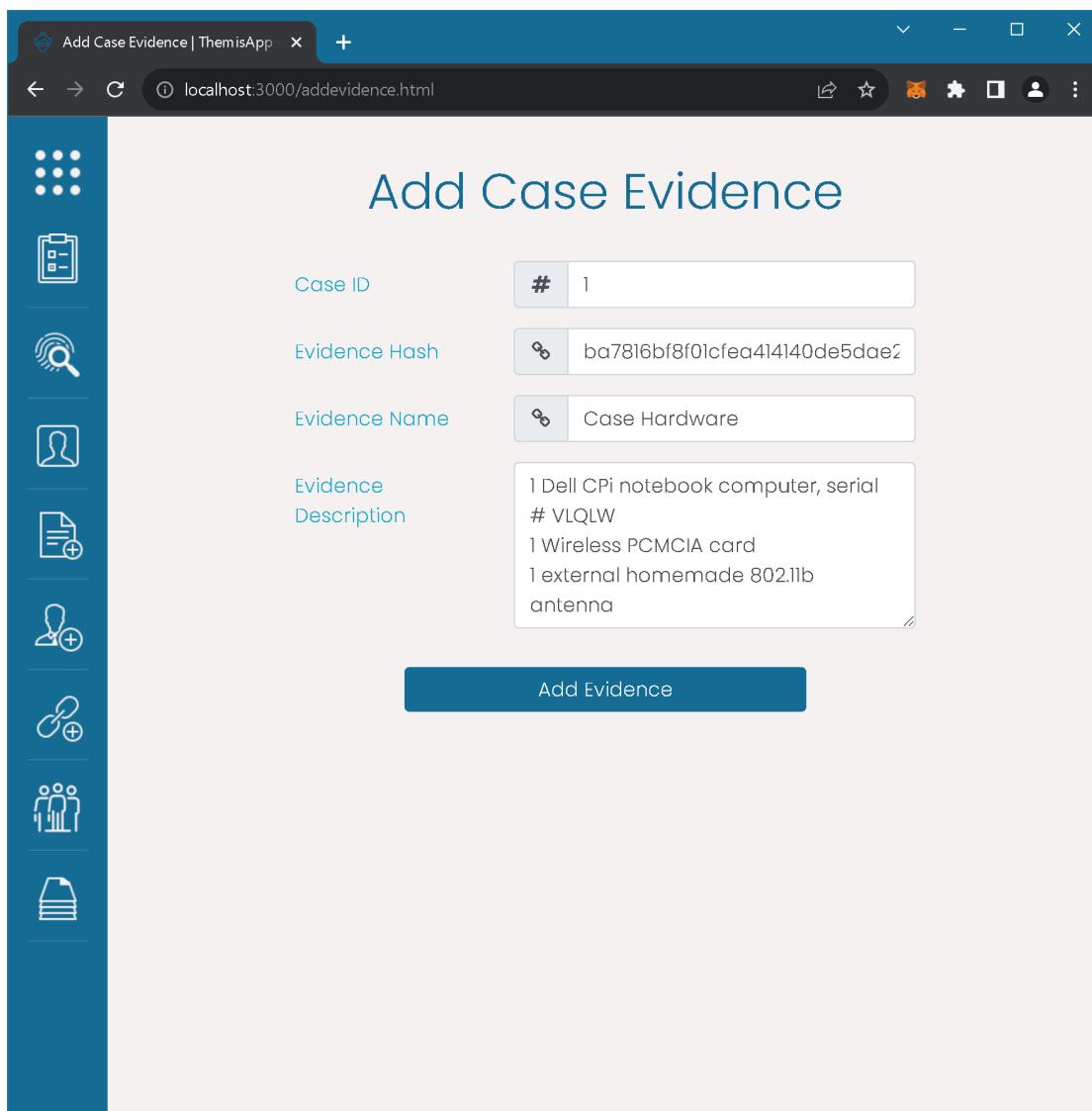
*Εικόνα 89 - Προσθήκη επιπλέον ερευνητή στην υπόθεση*

#	Case Name	Case Description	Case Investigators
1	Greg Schardt Case	<a href="#">Read Description</a>	0xed2de21f55fb1c2fd8d56fcf2a339980 0xfe3db6c6389878d811225fa9c3f49a0c

*Εικόνα 90 - Το αποτέλεσμα της προσθήκης νέου ερευνητή στην υπόθεση*

- Προσθήκη ενός αποδεικτικού στοιχείου σε μια υπόθεση**

Εκτός από την περίπτωση «ανοίγματος» μια νέας υπόθεσης, η προσθήκη ενός αποδεικτικού στοιχείου μπορεί να πραγματοποιηθεί και σε δευτερεύοντα χρόνο, συμπληρώνοντας τη φόρμα της σελίδας «Add Case Evidence» (Εικόνα 91). Για την προσθήκη ενός αποδεικτικού στοιχείου, απαιτείται από τον διαχειριστή να γνωρίζει το αναγνωριστικό (ID) της υπόθεσης που επιθυμεί, το οποίο μπορεί να το αναζητήσει στη σελίδα «Manage Cases» και το hash του αποδεικτικού στοιχείου σε μορφή «SHA-256», καθώς επίσης και να γνωρίζει περί τίνος πρόκειται ώστε να μπορεί να του προσδώσει μια ονομασία και μια περιγραφή.



Add Case Evidence

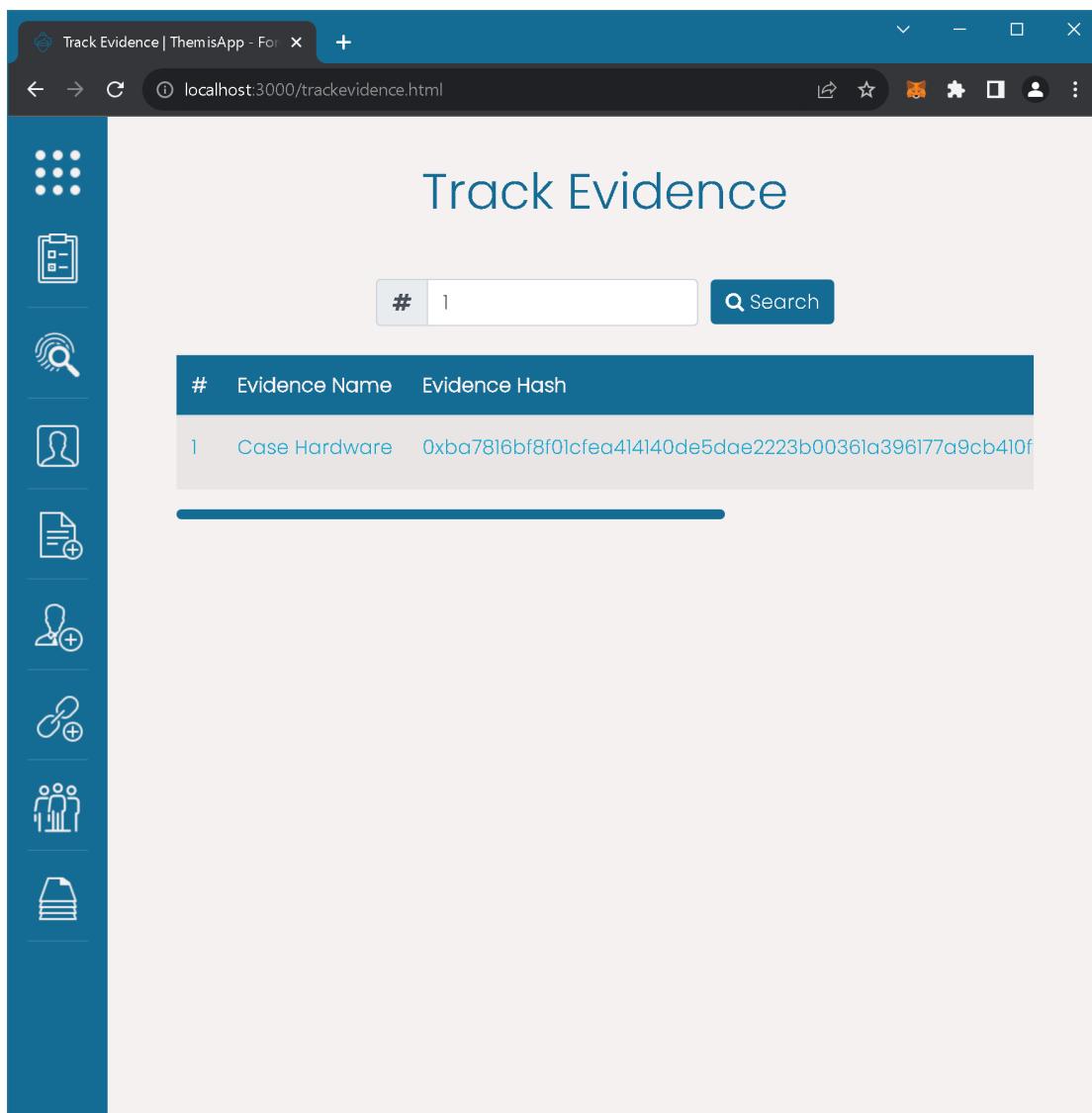
Case ID	# 1
Evidence Hash	ba7816bf8f01cfea414140de5dae2
Evidence Name	Case Hardware
Evidence Description	1 Dell CPi notebook computer, serial # VLQLW 1 Wireless PCMCIA card 1 external homemade 802.11b antenna

Add Evidence

Εικόνα 91 - Η σελίδα «Add Case Evidence»

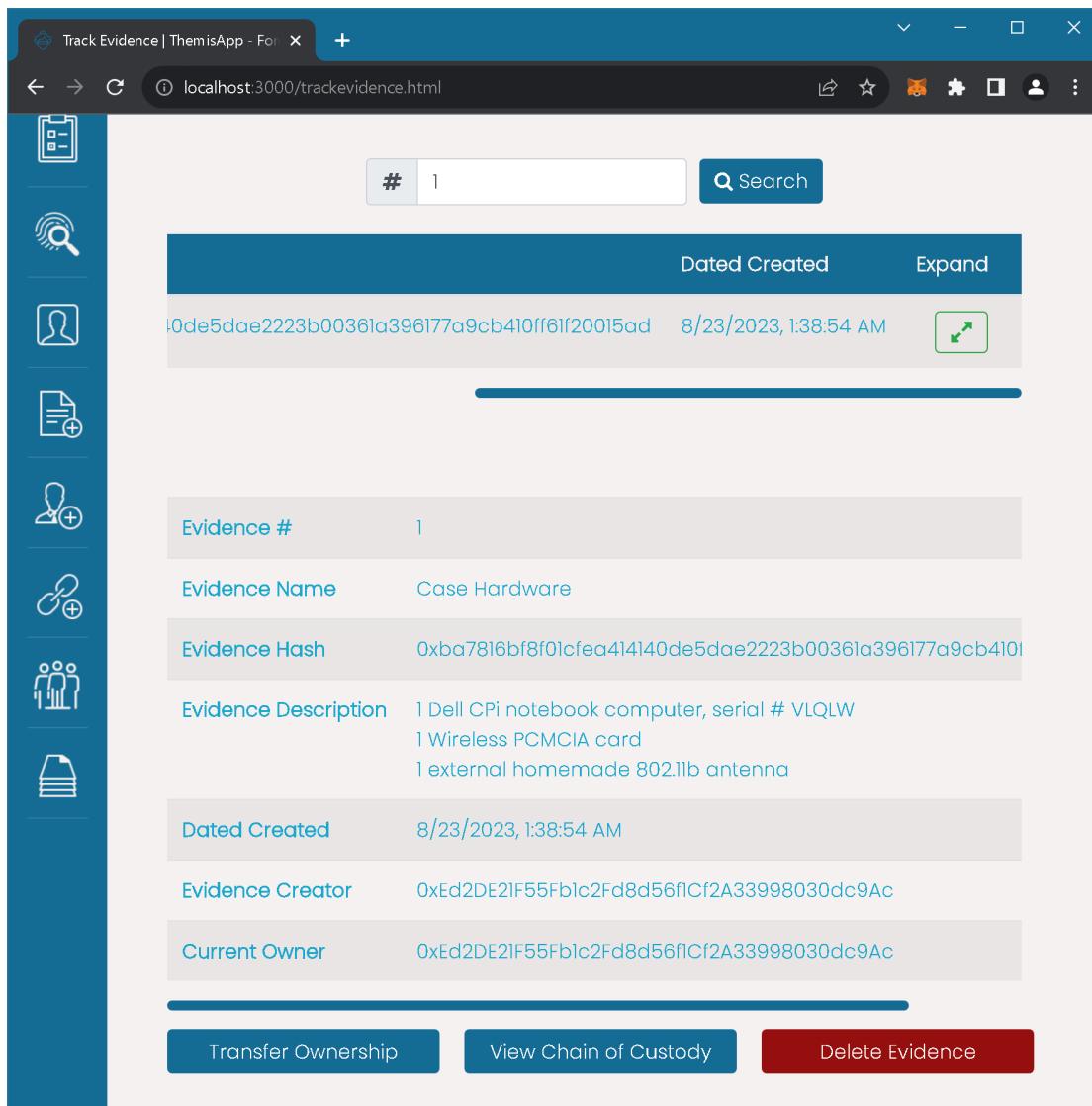
- Αναζήτηση των αποδεικτικών στοιχείων μιας υπόθεσης**

Μια κοινή λειτουργία της εφαρμογής για τους ερευνητές και τους διαχειριστές είναι η αναζήτηση ενός αποδεικτικού στοιχείου. Για να πραγματοποιήσει οποιαδήποτε ενέργεια, ένας από τους δύο ρόλους του συστήματος, θα πρέπει να έγκειται στους ερευνητές της υπόθεσης που ανήκει το αποδεικτικό στοιχείο που αναζητούν. Έτσι, πληκτρολογώντας το αναγνωριστικό (ID) της υπόθεσης στην αναζήτηση, εμφανίζονται ως αποτελέσματα τα αποδεικτικά στοιχεία της (Εικόνα 92), από τα οποία στη συνέχεια, μπορεί να επιλέξει αυτό που επιθυμεί για να προβάλλει τις πλήρεις πληροφορίες του (Εικόνα 93).



#	Evidence Name	Evidence Hash
1	Case Hardware	0xba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410f

Εικόνα 92 - Η σελίδα «Track Evidence»



The screenshot shows a web-based application for tracking evidence. On the left is a vertical sidebar with icons for different functions: a clipboard, magnifying glass, user profile, file, person, and document. The main area has a header with a search bar (# 1) and a 'Search' button. Below the header is a table with columns 'Dated Created' and 'Expand'. A single row is shown with the hash value '0de5dae2223b00361a396177a9cb410ff61f20015ad' and the date '8/23/2023, 1:38:54 AM'. There is also a green 'Expand' button with a double arrow icon. The detailed view below shows the following information:

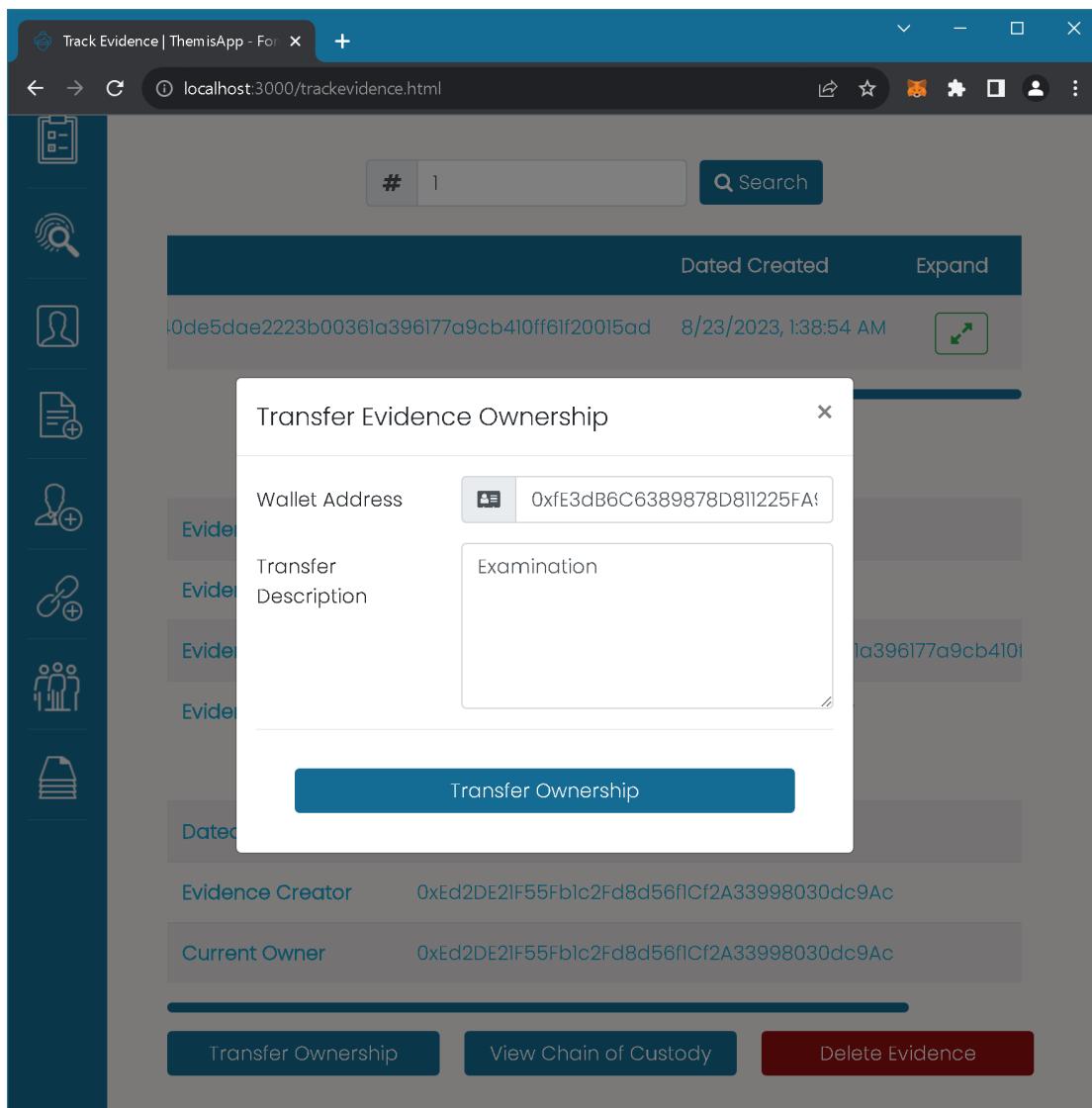
Evidence #	1
Evidence Name	Case Hardware
Evidence Hash	0xba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410f
Evidence Description	<ul style="list-style-type: none"> <li>1 Dell CPi notebook computer, serial # VLQLW</li> <li>1 Wireless PCMCIA card</li> <li>1 external homemade 802.11b antenna</li> </ul>
Dated Created	8/23/2023, 1:38:54 AM
Evidence Creator	0xED2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac
Current Owner	0xED2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac

At the bottom are three buttons: 'Transfer Ownership' (blue), 'View Chain of Custody' (blue), and 'Delete Evidence' (red).

Εικόνα 93 – Οι πλήρεις πληροφορίες του αποδεικτικού στοιχείου

### • Μεταβίβαση της κυριότητας ενός αποδεικτικού στοιχείου

Προβάλλοντας τις πλήρεις πληροφορίες ενός αποδεικτικού στοιχείου, εμφανίζονται στο κάτω μέρος της σελίδας τρία κουμπιά. Όπως φαίνονται στην παραπάνω εικόνα, αυτά είναι: «Transfer Ownership», «View Chain of Custody» και «Delete Evidence». Πατώντας στο κουμπί «Transfer Ownership», ο διαχειριστής έχει τη δυνατότητα, πληκτρολογώντας τη διεύθυνση του παραλήπτη και την αιτιολογία – περιγραφή της πράξης, να μεταβιβάσει την κυριότητα του αποδεικτικού στοιχείου σε κάποιον άλλο ερευνητή (Εικόνα 94). Το αποτέλεσμα αυτής της ενέργειας φαίνεται στην Εικόνα 95, όπου η διεύθυνση του «Δημιουργού του Αποδεικτικού Στοιχείου» (Evidence Creator) είναι πλέον, διαφορετική από αυτή του «Τρέχοντος Ιδιοκτήτη» (Current Owner).



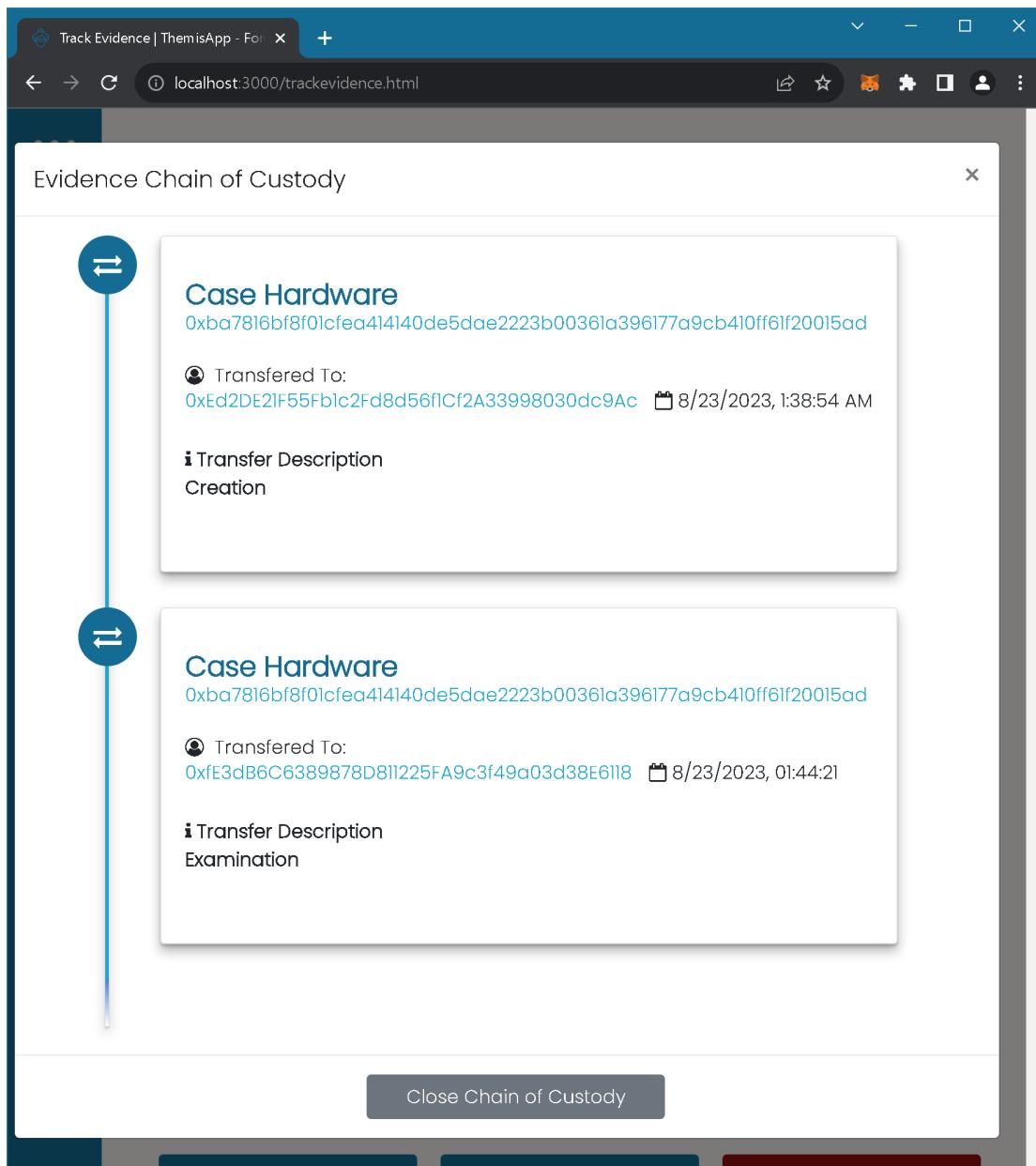
Εικόνα 94 - Φόρμα μεταβίβασης κυριότητας αποδεικτικού στοιχείου

Evidence Creator	0xED2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac
Current Owner	0xE3dB6C6389878D811225FA9c3f49a03d38E6118

Εικόνα 95 - Το αποτέλεσμα της μεταβίβασης κυριότητας αποδεικτικού στοιχείου

- **Προβολή του chain of custody ενός αποδεικτικού στοιχείου**

Αφού ολοκληρωθεί η μεταβίβαση κυριότητας του αποδεικτικού στοιχείου, το chain of custody του ενημερώνεται, περιλαμβάνοντας όλα τα απαραίτητα δεδομένα που συνεπάγονται με αυτή, όπως είναι το hash του αποδεικτικού στοιχείου, η ημέρα και ώρα διεκπεραίωσης της πράξης και η διεύθυνση πορτοφολιού του παραλήπτη (Εικόνα 96).



Εικόνα 96 – Το chain of custody του αποδεικτικού στοιχείου

## 7.4. Διαδικασία δοκιμών (Testing)

Η διεκπεραίωση δοκιμών αποτελεί μέρος της διαδικασίας ανάπτυξης μιας εφαρμογής, και ωφελεί στην επαλήθευση της ορθότητας και την επικύρωση των λειτουργικών χαρακτηριστικών της (Pedamkar, 2019). Οι διαδικασίες δοκιμών που ακολουθούν είναι ονομαστικά οι εξής: 1. Δοκιμές Μονάδας (Unit Testing), 2. Δοκιμή Ενσωμάτωσης (Integration Testing), 3. Δοκιμή Λειτουργιών (Functional Testing), 4. Δοκιμή Ασφάλειας (Security Testing), 5. Δοκιμές Συμβατότητας (Compatibility Testing) και 6. Δοκιμές Παλινδρόμησης (Regression Testing). Κάθε μία από αυτές παρουσιάζει ένα σενάριο δοκιμής, το οποίο αποτελείται από τα βήματα εκτέλεσης του σεναρίου, τα προσδοκόμενα και τα τελικά αποτελέσματα.

### 1. Unit Testing

Το «Unit Testing», αποτελεί μια μεθοδολογία δοκιμής που στοχεύει σε διακριτές μονάδες λογισμικού. Ο σκοπός της είναι να εξακριβωθεί ότι κάθε μονάδα του κώδικα λογισμικού αποδίδει όπως αναμένεται. Εκτελείται στη φάση ανάπτυξης του κώδικα, ώστε να εξακριβωθεί η ακρίβειά του. Οι μονάδες υπό έλεγχο μπορεί να περιλαμβάνουν συναρτήσεις, μεθόδους, διαδικασίες, modules ή αντικείμενα. (Hamilton, 2019a). Για τη παρούσα διαδικασία δοκιμών έγινε χρήση της γλώσσας προγραμματισμού «Javascript» και του module «chai» του «Node.js». Τα αρχεία που περιέχουν τον κώδικα των δοκιμών βρίσκονται εντός του φακέλου «test», στα αρχεία της εφαρμογής.

**Σενάριο:** Δοκιμές των μεθόδων των έξυπνων συμβολαίων

**Στόχος:** Εκτέλεση δοκιμών μονάδων σε μεμονωμένες μεθόδους των έξυπνων συμβολαίων (εφεξής «smart contracts») εντός του ιδιωτικού Ethereum blockchain «ThemisChain» και της αποκεντρωμένης εφαρμογής chian of custody «Themis».

**Βήματα εκτέλεσης του σεναρίου:**

#### 1. Προετοιμασία:

- Δημιουργία ενός τοπικού περιβάλλοντος δοκιμών για το ιδιωτικό blockchain.
- Ανάπτυξη των smart contracts στο τοπικό blockchain.

## 2. Case Smart Contract:

- Δοκιμή των μεθόδων που αφορούν τις υποθέσεις και τα αποδεικτικά στοιχεία.
- Παροχή δειγματοληπτικών δεδομένων υποθέσεων και αποδεικτικών στοιχείων και προσομοίωση της προσθήκης τους στο blockchain.
- Βεβαίωση ότι οι μέθοδοι επιστρέφουν την αναμενόμενη «απάντηση».

## 3. Investigator Smart Contract:

- Δοκιμή των μεθόδων που αφορούν τους ερευνητές.
- Παροχή δειγματοληπτικών στοιχείων ταυτότητας ερευνητών.
- Βεβαίωση ότι οι μέθοδοι επιστρέφουν την αναμενόμενη «απάντηση».

## 4. Issued Smart Contract:

- Δοκιμή των λειτουργιών ελέγχου πρόσβασης που διασφαλίζουν ότι μόνο εξουσιοδοτημένοι συμμετέχοντες μπορούν να αλληλεπιδράσουν με τα smart contracts.
- Επαλήθευση ότι το smart contract αρνείται την πρόσβαση σε μη εξουσιοδοτημένους χρήστες.

## 5. Ενσωμάτωση στην εφαρμογή chain of custody:

- Βεβαίωση ότι η εφαρμογή διασυνδέεται σωστά με τα smart contracts.
- Βεβαίωση ότι η διεπαφή χρήστη της εφαρμογής αντικατοπτρίζει τα αποτελέσματα των λειτουργιών των smart contracts.

### Αναμενόμενα αποτελέσματα:

- Οι λειτουργίες των smart contracts εκτελούνται χωρίς σφάλματα.
- Τα δεδομένα των αποδεικτικών στοιχείων μεταφορτώνονται στο blockchain με τις απαραίτητες λεπτομέρειες.
- Οι μεταβιβάσεις κυριότητας των αποδεικτικών στοιχείων ενημερώνουν αυτόματα το chain of custody.
- Οι λειτουργίες ελέγχου πρόσβασης περιορίζουν σωστά τη μη εξουσιοδοτημένη πρόσβαση.
- Η ενσωμάτωση των λειτουργιών των smart contracts στην εφαρμογή chain of custody είναι απρόσκοπτη και ακριβής.

### Τελικά αποτελέσματα:

Όπως διακρίνεται στην Εικόνα 97, όλα τα παραπάνω αναμενόμενα αποτελέσματα καλύπτονται πλήρως.

#### Contract: Case

- ✓ Should successfully add a Case to caseList mapping (313ms)
- ✓ Should successfully show if a Case exists
- ✓ Should successfully get the name of a Case
- ✓ Should successfully show info about the active cases of an investigator
- ✓ Should successfully close a case (59ms)
- ✓ Should successfully assign a case to an investigator
- ✓ Should successfully remove an investigator from a case (49ms)
- ✓ Should successfully show the investigators of a case
- ✓ Should successfully show if an investigators exists in a case
- ✓ Should successfully add evidence to a case (313ms)
- ✓ Should successfully get collapsed info of an evidence
- ✓ Should successfully get expanded info of an evidence
- ✓ Should successfully get the hash of an evidence
- ✓ Should successfully count the evidences of a case
- ✓ Should successfully get the current owner of an evidence
- ✓ Should successfully transfer the evidence (50ms)
- ✓ Should successfully show the chain of custody of an evidence
- ✓ Should successfully delete an evidence (92ms)

#### Contract: Investigator

- ✓ Should successfully add a new investigator (83ms)
- ✓ Should successfully show investigator 's name
- ✓ Should successfully remove an investigator (74ms)
- ✓ Should successfully check if an investigator with the same wallet address exists
- ✓ Should successfully check if an investigator with the same id exists

#### Contract: Issued

- ✓ Should successfully check if an admin exists

#### Contract: Issued

- ✓ Contract "Issued" successfully deployed

#### Contract: Investigator

- ✓ Contract "Investigator" successfully deployed

#### Contract: Case

- ✓ Contract "Case" successfully deployed

#### Contract: Evidence

- ✓ Contract "Evidence" successfully deployed

28 passing (2s)

Εικόνα 97 - Η λίστα των επιτυχών «Unit Test» της εφαρμογής

## 2. Integration Testing

To «Integration Testing» ομαδοποιεί και ελέγχει τις διάφορες ξεχωριστές ενότητες ενός λογισμικού (Hamilton, 2019b).

**Σενάριο:** Αλληλεπίδραση μεταξύ του ιδιωτικού blockchain «ThemisChain» και της αποκεντρωμένης εφαρμογής chain of custody «Themis».

**Στόχος:** Διασφάλιση της απρόσκοπτης ενσωμάτωσης και σωστής λειτουργίας της εφαρμογής chain of custody με το ιδιωτικό blockchain. Αντή η δοκιμή επικυρώνει ότι τα στοιχεία της εφαρμογής αλληλεπιδρούν σωστά με τα smart contracts και την αποθήκευση δεδομένων εντός του blockchain.

### Βήματα εκτέλεσης του σεναρίου:

#### 1. Προετοιμασία:

- Επιβεβαίωση ότι το ιδιωτικό δίκτυο blockchain και η εφαρμογή chain of custody είναι λειτουργικά.

#### 2. Αλληλεπίδραση έξυπνων συμβολαίων:

- Πρόσβαση στη διεπαφή της εφαρμογής και δημιουργήστε μιας νέας καταχώρισης αποδεικτικών στοιχείων.
- Έλεγχος της αλληλεπίδρασης μεταξύ του «frontend» της εφαρμογής και του αντίστοιχου smart contract.
- Επαλήθευση ότι τα στοιχεία που εισάγονται στην εφαρμογή καταγράφονται με ακρίβεια και αποθηκεύονται στη «μνήμη» του smart contract.

#### 3. Μεταβίβαση κυριότητας αποδεικτικού στοιχείου:

- Επιλογή ενός αποδεικτικού στοιχείου που δημιουργήθηκε προηγουμένως και εκκίνηση μιας διαδικασίας μεταβίβασης κυριότητας σε άλλο ερευνητή.
- Παρακολούθηση της επικοινωνίας μεταξύ της εφαρμογής και του smart contract κατά τη διαδικασία μεταβίβασης.
- Επιβεβαίωση ότι το smart contract ενημερώνει την κατάσταση ιδιοκτησίας του αποδεικτικού στοιχείου και καταγράφει το συμβάν της μεταβίβασης.

#### 4. Συνέπεια δεδομένων:

- Δημιουργία μιας νέας καταχώριση αποδεικτικών στοιχείων απευθείας μέσω του smart contract στο blockchain.
- Πρόσβαση στη διεπαφή της εφαρμογής και αυτόματος συγχρονισμός των δεδομένων της με το blockchain.
- Επιβεβαίωση ότι η εφαρμογή λαμβάνει τα στοιχεία που προστέθηκαν πρόσφατα και τα εμφανίζει με ακρίβεια.

### Αναμενόμενα αποτελέσματα:

- **Αλληλεπίδραση έξυπνων συμβολαίων:** Η εφαρμογή θα πρέπει να επικοινωνεί με επιτυχία με το smart contract και να ενημερώνει τα δεδομένα των αποδεικτικών στοιχείων στο blockchain.
- **Μεταβίβαση κυριότητας αποδεικτικού στοιχείου:** Η εφαρμογή και το αντίστοιχο smart contract θα πρέπει να αλληλεπιδρούν για να διευκολύνουν τη μεταβίβαση κυριότητας αποδεικτικών στοιχείων και να επικαιροποιούν το καθεστώς ιδιοκτησίας.
- **Συνέπεια δεδομένων:** Η άμεση προσθήκη αποδεικτικών στοιχείων στο blockchain θα πρέπει να αντικατοπτρίζεται στα δεδομένα της εφαρμογής μετά το συγχρονισμό.

### Τελικά αποτελέσματα:

Τα τελικά αποτελέσματα του παραπάνω σεναρίου δοκιμών επικυρώνουν την απρόσκοπτη αλληλεπίδραση μεταξύ της εφαρμογής «Themis» και του ιδιωτικού blockchain «ThemisChain» και διασφαλίζουν ότι τα στοιχεία της εφαρμογής, όπως τα smart contracts και η διατήρηση των δεδομένων, λειτουργούν αρμονικά, παρέχοντας μια λειτουργική και αξιόπιστη λύση για τη διαχείριση των αποδεικτικών στοιχείων. Επίσης, η επιτυχής ολοκλήρωση αυτής της δοκιμής συμβάλλει στον στόχο της έρευνας να αποδείξει την αποτελεσματική συνέργεια μεταξύ ιδιωτικών blockchain και εφαρμογών chain of custody.

### 3. Functional Testing

Το «Functional Testing» διενεργείται για να ελεγχθεί εάν η εφαρμογή πληροί τις λειτουργικές απαιτήσεις που αναφέρονται κατά την ανάλυση της δομής της (βλ σελίδες 91 και 92).

**Σενάριο:** Δοκιμή λειτουργιών της αποκεντρωμένης εφαρμογής chain of custody «Themis».

**Στόχος:** Επικύρωση των βασικών λειτουργιών της εφαρμογής chain of custody. Αυτή η δοκιμή διασφαλίζει ότι τα χαρακτηριστικά και οι λειτουργίες της εφαρμογής λειτουργούν όπως προβλέπεται, ικανοποιώντας τις απαιτήσεις που περιγράφονται στην ανάλυση της δομής της.

## Βήματα εκτέλεσης του σεναρίου:

### 1. Προετοιμασία:

- Επιβεβαίωση ότι το ιδιωτικό δίκτυο blockchain και η εφαρμογή chain of custody είναι λειτουργικά.

### 2. Έλεγχος ταυτότητας και εξουσιοδότηση χρήστη:

- Δοκιμή του ελέγχου πρόσβασης χρήστη πραγματοποιώντας ενέργειες που περιορίζονται για εκτέλεση από συγκεκριμένους ρόλους του συστήματος.
- Επιβεβαίωση ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να εκτελέσουν ενέργειες όπως μεταβίβαση κυριότητας αποδεικτικών στοιχείων.
- Επιβεβαίωση ότι οι μη εξουσιοδοτημένοι χρήστες λαμβάνουν τα κατάλληλα μηνύματα σφάλματος όταν επιχειρούν περιορισμένες ενέργειες.

### 3. Δημιουργία και καταγραφή αποδεικτικών στοιχείων:

- Σύνδεση ως διαχειριστής και μετάβαση στη σελίδα «Add Case Evidence».
- Δημιουργία μιας νέας καταχώρισης αποδεικτικού στοιχείου, παρέχοντας ακριβείς πληροφορίες.
- Επαλήθευση ότι η εφαρμογή καταγράφει τα στοιχεία του αποδεικτικού στοιχείου.

### 4. Μεταβίβαση κυριότητας αποδεικτικών στοιχείων - Παρακολούθηση του chain of custody:

- Εκκίνηση της διαδικασίας μεταβίβασης της κυριότητας ενός αποδεικτικού στοιχείου από έναν ερευνητή σε άλλο.
- Επιβεβαίωση ότι η εφαρμογή ενημερώνει τα στοιχεία ιδιοκτησίας και δημιουργεί μια καρτέλα μεταφοράς.
- Επιβεβαίωση ότι η διαδικασία μεταβίβασης περιλαμβάνει τις κατάλληλες πληροφορίες αποστολέα, παραλήπτη και κατακερματισμού του αποδεικτικού στοιχείου.

### 5. Αμεταβλητότητα:

- Επιβεβαίωση ότι τα στοιχεία που έχουν καταχωρηθεί στο blockchain δε μπορούν να παραποιηθούν.

- Έλεγχος των δικαιωμάτων πρόσβασης και επεξεργασίας των χρηστών που διαθέτουν ρόλο «ερευνητή».
- Επιβεβαίωση ότι τα χαρακτηριστικά των αποδεικτικών στοιχείων παραμένουν ακριβή και όμοια με το αρχικό φυσικό αντίγραφο.

#### Αναμενόμενα αποτελέσματα:

- **Έλεγχος ταυτότητας και εξουσιοδότηση χρήστη:** Επιτυχής εκτέλεση καίριων ενεργειών από εξουσιοδοτημένους χρήστες και αντίστοιχη απόρριψη για μη εξουσιοδοτημένους χρήστες.
- **Δημιουργία και καταγραφή αποδεικτικών στοιχείων:** Ακριβής καταγραφή των λεπτομερειών των αποδεικτικών στοιχείων.
- **Μεταβίβαση κυριότητας αποδεικτικών στοιχείων - Παρακολούθηση του chain of custody:** Σωστή ενημέρωση των στοιχείων ιδιοκτησίας και διατήρηση ιστορικού μεταβίβασης.
- **Αμεταβλητότητα:** Διαφύλαξη της αμεταβλητότητας των δεδομένων που καταγράφονται στο blockchain.

#### Τελικά αποτελέσματα:

Το παρόν σενάριο δοκιμής λειτουργικών επαληθεύει ότι οι βασικές λειτουργίες της εφαρμογής chain of custody λειτουργούν όπως προβλέπεται, ευθυγραμμιζόμενες με τις περιγραφόμενες απαιτήσεις. Η επιτυχής ολοκλήρωση αυτού του ελέγχου αποδεικνύει ότι η εφαρμογή διευκολύνει αποτελεσματικά τη διαχείριση των αποδεικτικών στοιχείων και διασφαλίζει την ακεραιότητα του chain of custody των αποδεικτικών στοιχείων.

## 4. Security Testing

«Security Testing» ονομάζεται ο έλεγχος μιας εφαρμογής ως προς την προστασίας της από εξωτερικές και εσωτερικές απειλές (Acharya, 2022).

**Σενάριο:** Δοκιμή ασφαλείας της αποκεντρωμένης εφαρμογής chain of custody «Themis».

**Στόχος:** Αξιολόγηση των πτυχών ασφάλειας της εφαρμογής chain of custody, διασφαλίζοντας ότι τα ευαίσθητα δεδομένα παραμένουν προστατευμένα και η εφαρμογή είναι ανθεκτική έναντι κοινών τρωτών σημείων ασφαλείας.

Όπως αναφέρθηκε στο υποκεφάλαιο 6.1 (βλ. σελίδα 73), το blockchain «ThemisChain» και κατ' επέκταση η εφαρμογή «Themis» δημιουργήθηκαν και προορίζονται για ακαδημαϊκούς σκοπούς και όχι για πραγματικές περιπτώσεις χρήσεις. Συνεπώς, δεν δόθηκε έμφαση στη προσπάθεια διατήρησης κανόνων ασφαλείας δεδομένων και προστασίας από κυβερνοεπιθέσεις. Ωστόσο, μία θεωρητική προσέγγιση σε ένα σενάριο «Security Testing» θα περιλάμβανε τα παρακάτω βήματα:

#### **Βήματα εκτέλεσης του σεναρίου:**

##### **1. Προετοιμασία:**

- Επιβεβαίωση ότι το ιδιωτικό δίκτυο blockchain και η εφαρμογή chain of custody είναι λειτουργικά.

##### **2. Προσπάθεια παράκαμψης ελέγχου ταυτότητας:**

- Προσπάθεια παράκαμψης του μηχανισμού ελέγχου ταυτότητας εισβάλλοντας σε περιοχές περιορισμένης πρόσβασης χωρίς έγκυρα διαπιστευτήρια.

##### **3. Επιθέσεις «XSS» (Cross-Site Scripting):**

- Προσπάθεια εισαγωγής «script» κακόβουλων ενεργειών μέσω των πεδίων μιας φόρμας.

##### **4. Ασφάλεια του blockchain:**

- Αξιολόγηση της ασφάλειας του ιδιωτικού blockchain επιχειρώντας μη εξουσιοδοτημένες συναλλαγές ή παραβιάζοντας τα αρχεία του blockchain.
- Επιβεβαίωση ότι το δίκτυο blockchain διατηρεί την ακεραιότητα των δεδομένων του και αποτρέπει μη εξουσιοδοτημένες αλλαγές.

#### **Αναμενόμενα αποτελέσματα:**

- **Προσπάθεια παράκαμψης ελέγχου ταυτότητας:** Η μη εξουσιοδοτημένη πρόσβαση θα πρέπει να αποκλειστεί και θα πρέπει να επιβληθεί ο κατάλληλος έλεγχος ταυτότητας.

- **Επιθέσεις «XSS» (Cross-Site Scripting):** Η εφαρμογή θα πρέπει να φιλτράρει και διαφεύγει (escape) την είσοδο δεδομένων από το χρήστη για να αποτρέψει επιθέσεις «XSS».
- **Ασφάλεια του blockchain:** Οι μη εξουσιοδοτημένες συναλλαγές ή οι προσπάθειες παραβίασης θα πρέπει να αποτρέπονται από το blockchain.

## 5. Compatibility Testing

Ο τύπος δοκιμής που αξιολογεί τον τρόπο εκτέλεσης και συμπεριφοράς μιας εφαρμογής σε διαφορετικές πλατφόρμες, διακομιστές, περιβάλλοντα δικτύου και ρυθμίσεις παραμέτρων υλικού ονομάζεται «Compatibility Testing». Σκοπός του είναι να διασφαλίσει ότι μια εφαρμογή λειτουργεί ομαλά με βέλτιστη απόδοση σε διαφορετικά προγράμματα περιήγησης, διαμορφώσεις, βάσεις δεδομένων και εκδόσεις λογισμικού (Acharya, 2022).

**Σενάριο:** Έλεγχος συμβατότητας της αποκεντρωμένης εφαρμογής chain of custody «Themis».

**Στόχος:** Διασφάλιση πως η εφαρμογή chain of custody είναι συμβατή με διάφορες συσκευές και προγράμματα περιήγησης, παρέχοντας μια συνεπή εμπειρία χρήστη σε διαφορετικές πλατφόρμες.

**Βήματα εκτέλεσης του σεναρίου:**

### 1. Προετοιμασία:

- Επιβεβαίωση ότι η εφαρμογή chain of custody είναι λειτουργική.
- Ρύθμιση ενός περιβάλλοντος δοκιμής με διάφορες συσκευές και προγράμματα περιήγησης.

### 2. Συμβατότητα συσκευών:

- Δοκιμή της εφαρμογής σε διαφορετικές συσκευές, όπως επιτραπέζιους και φορητούς υπολογιστές, tablets και smartphones.

### 3. Συμβατότητα περιηγητών ιστού:

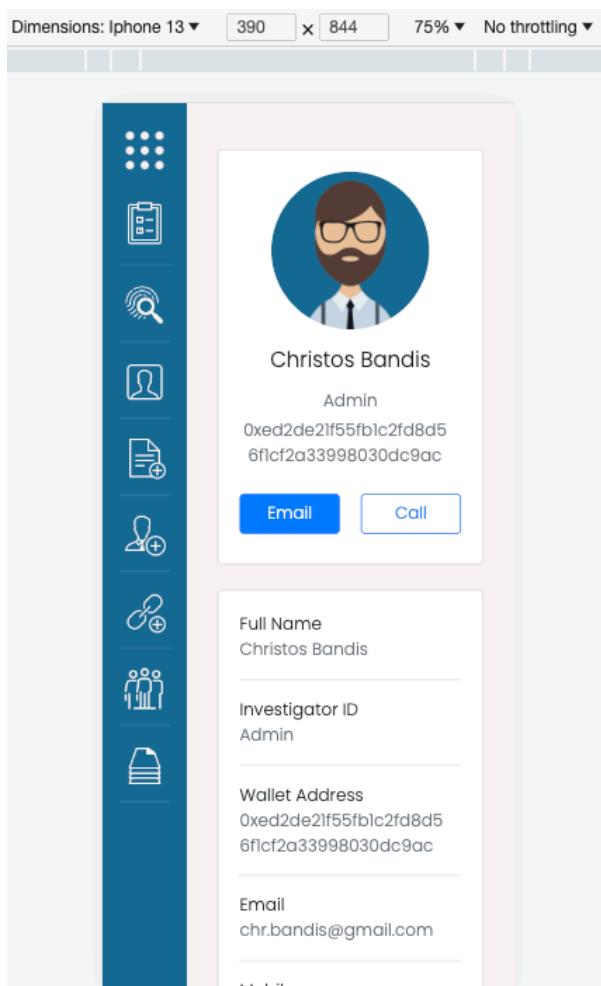
- Πρόσβαση στην εφαρμογή μέσω διαφορετικών περιηγητών ιστού, συμπεριλαμβανομένων των «Google Chrome», «Mozilla Firefox», «Microsoft Edge» και «Safari».

### **Αναμενόμενα αποτελέσματα:**

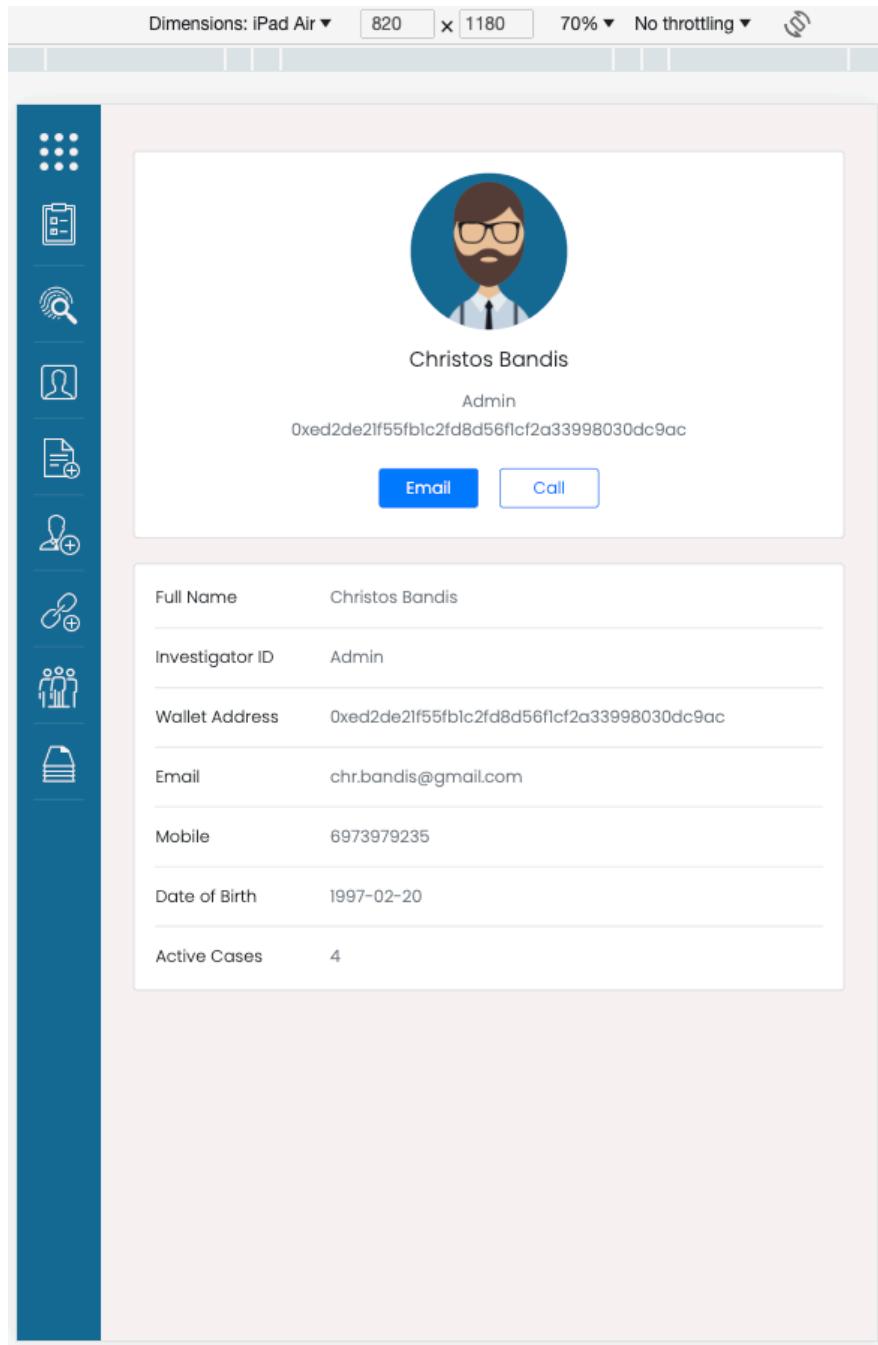
- **Συμβατότητα συσκευών:** Η εφαρμογή θα πρέπει να προσαρμόζεται ανταποκρινόμενη σε διαφορετικές συσκευές και μεγέθη οθόνης.
- **Συμβατότητα περιηγητών ιστού:** Η εφαρμογή θα πρέπει να λειτουργεί με συνέπεια και να εμφανίζεται σωστά σε διάφορους περιηγητές ιστού.

### **Τελικά αποτελέσματα:**

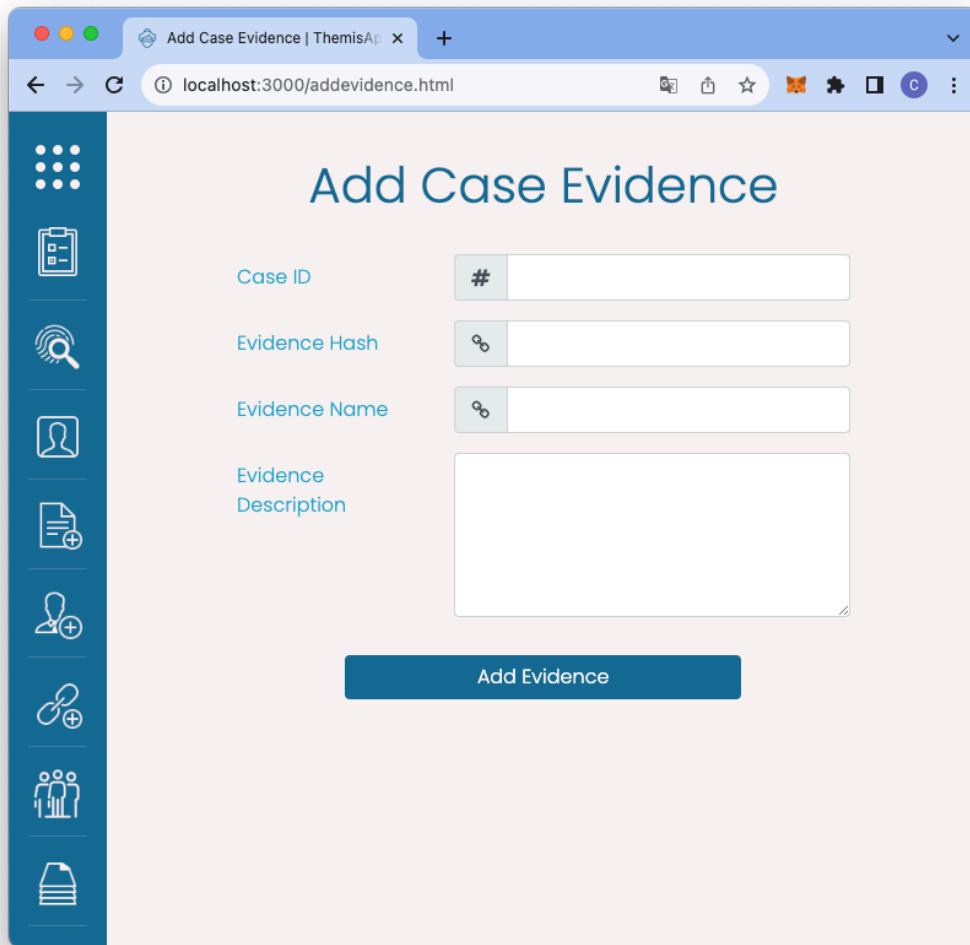
Η επιτυχία του σεναρίου δοκιμών συμβατότητας διασφαλίζει ότι η εφαρμογή chain of custody προσφέρει μια συνεπή και αξιόπιστη εμπειρία χρήστη σε μια σειρά συσκευών (Εικόνες 98 και 99) και περιηγητών ιστού (Εικόνες 100 και 101). Αυτή η συμβατότητα εξασφαλίζει ευρύτερη προσβασιμότητα και χρηστικότητα γι' αυτούς που ασχολούνται με ψηφιακές εγκληματολογικές διαδικασίες.



Εικόνα 98 – Η εμφάνιση της σελίδας του προφίλ του ερευνητή σε συσκευή «iPhone 13» (smartphone)  
(Εργαλεία για προγραμματιστές - Google Chrome)

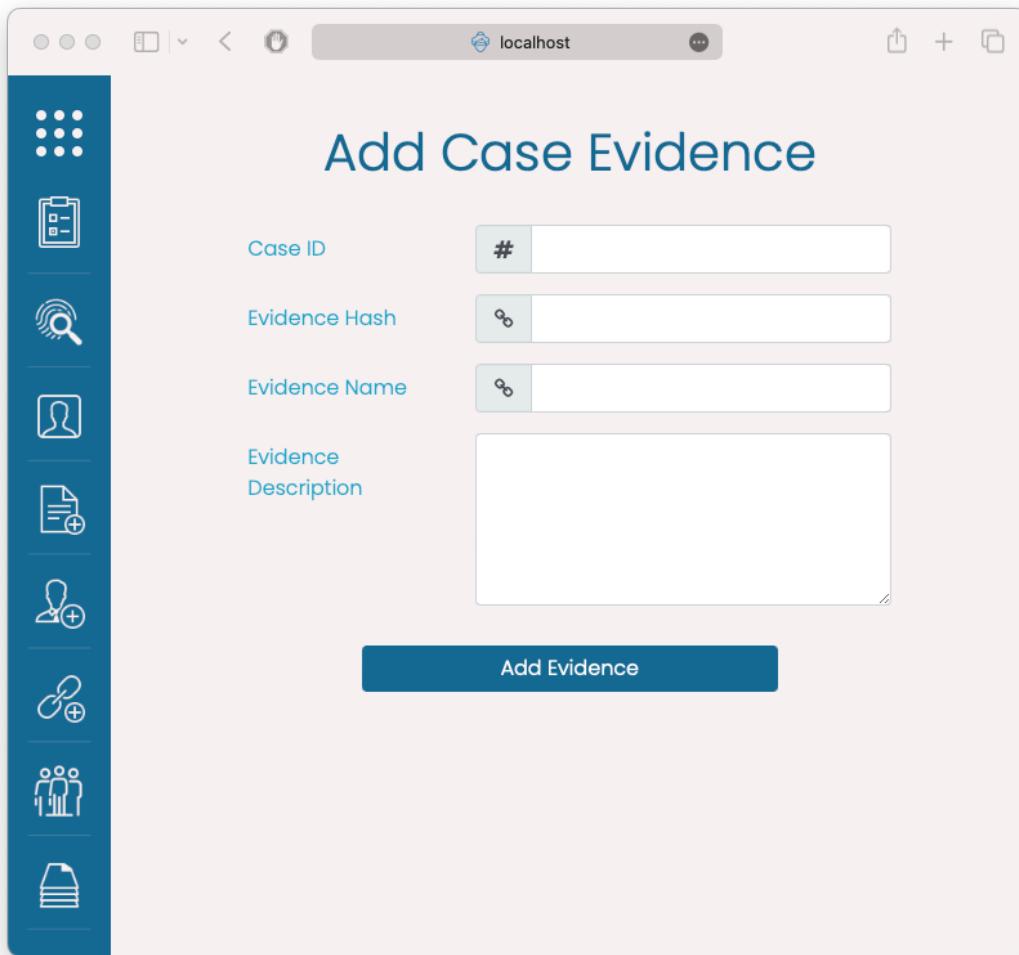


Εικόνα 99 - Η εμφάνιση της σελίδας του προφίλ του ερευνητή σε συσκευή «iPad Air» (tablet) (Εργαλεία για προγραμματιστές - Google Chrome)



The screenshot shows a web application window titled "Add Case Evidence | ThemisAp" with the URL "localhost:3000/addevidence.html". The main content area is titled "Add Case Evidence". It contains four input fields: "Case ID" with placeholder "#", "Evidence Hash" with placeholder "hash", "Evidence Name" with placeholder "name", and "Evidence Description" with a large text area. Below these fields is a blue button labeled "Add Evidence". To the left of the main content is a vertical sidebar with eight icons, each with a horizontal line underneath, representing different application features.

Εικόνα 100 - Η εμφάνιση της σελίδας «Add Case Evidence» στον περιηγητή ιστού «Google Chrome»



*Eikόνα 101 - Η εμφάνιση της σελίδας «Add Case Evidence» στον περιηγητή ιστού «Safari»*

## 6. Regression Testing

To «Regression Testing» ορίζεται ως ο έλεγχος του τρόπου λειτουργίας μιας ολοκληρωμένης εφαρμογής, μετά την τροποποίηση οποιασδήποτε λειτουργικότητας, στοιχείου ή module. Στόχος του είναι να διασφαλίσει ότι οι υπάρχουσες λειτουργίες της εφαρμογής παραμένουν ανεπηρέαστες μετά τις νέες τροποποιήσεις.

**Σενάριο:** Δοκιμή παλινδρόμησης της αποκεντρωμένης εφαρμογής chain of custody «Themis».

**Στόχος:** Διασφάλιση ότι οι πιο πρόσφατες τροποποιήσεις και βελτιώσεις που έγιναν στην εφαρμογή chain of custody δεν επηρεάζουν αρνητικά την υπάρχουσα λειτουργικότητα ή προσθέτουν νέα ελαττώματα.

## Βήματα εκτέλεσης του σεναρίου:

### 1. Προετοιμασία:

- Επιβεβαίωση ότι η εφαρμογή chain of custody είναι λειτουργική.
- Παρακολούθηση των πρόσφατων αλλαγών, βελτιώσεων ή διορθώσεων σφαλμάτων που έχουν εφαρμοστεί.

### 2. Σημείο αναφοράς δοκιμής:

- Δημιουργία ενός σημείου αναφοράς διεξάγοντας μια πλήρη δοκιμή της υπάρχουσας λειτουργικότητας της εφαρμογής.

### 3. Εφαρμογή τροποποιήσεων:

- Εφαρμογή των πρόσφατων αλλαγών, βελτιώσεων ή διορθώσεων σφαλμάτων.

### 4. Δοκιμή παλινδρόμησης:

- Δοκιμή όλων των δυνατοτήτων, των ροών εργασίας και των σεναρίων που είχαν δοκιμαστεί προηγουμένως και καλύφθηκαν σε προηγούμενες φάσεις δοκιμών.
- Επιβεβαίωση ότι οι πρόσφατες αλλαγές δεν έχουν προκαλέσει ανεπιθύμητες παρενέργειες ή παλινδρομήσεις.

### 5. Δοκιμή ακεραιότητας δεδομένων:

- Επαλήθευση ότι οι πρόσφατες αλλαγές δεν έχουν επηρεάσει την ακεραιότητα των δεδομένων, στις περιπτώσεις αποθήκευσης, ανάκτησης και χειρισμού δεδομένων.

### 6. Δοκιμή διεπαφής χρήστη:

- Επιβεβαίωση ότι τα στοιχεία της διεπαφής χρήστη και τα στοιχεία σχεδίασης παραμένουν συνεπή και λειτουργικά.

### 7. Δοκιμή συμβατότητας:

- Επαλήθευση ότι οι πρόσφατες αλλαγές δεν έχουν επηρεάσει τη συμβατότητα με διαφορετικές συσκευές και προγράμματα περιήγησης.

### 8. Δοκιμή επίδοσης:

- Μέτρηση των επιδόσεων της εφαρμογής πριν και μετά τις αλλαγές για την εύρεση τυχόν υποβαθμίσεων των επιδόσεων.

### 9. Δοκιμή ασφάλειας:

- Επιβεβαίωση ότι οι αλλαγές δεν έχουν εισαγάγει νέες ευπάθειες ή αδυναμίες ασφαλείας.

### Αναμενόμενα αποτελέσματα:

- Όλες οι δυνατότητες και οι ροές εργασίας που έχουν δοκιμαστεί προηγουμένως θα πρέπει να συνεχίσουν να λειτουργούν όπως αναμένεται.
- Η ακεραιότητα των δεδομένων θα πρέπει να διατηρείται χωρίς αποκλίσεις.
- Τα στοιχεία διεπαφής χρήστη πρέπει να παραμένουν ανέπαφα.
- Η συμβατότητα με συσκευές και προγράμματα περιήγησης δεν πρέπει να διακυβεύεται.
- Οι μετρήσεις επίδοσης θα πρέπει να παραμείνουν σταθερές ή να βελτιωθούν.
- Δεν πρέπει να εισαχθούν νέα τρωτά σημεία ασφαλείας.

### Τελικά αποτελέσματα:

Το «Regression Testing» διασφαλίζει ότι οι πρόσφατες τροποποιήσεις και βελτιώσεις που έγιναν στην εφαρμογή chain of custody δεν έχουν επηρεάσει αρνητικά την υπάρχουσα λειτουργικότητά της. Επιβεβαιώνοντας ότι οι πρόσφατες αλλαγές δεν εισάγουν παλινδρομήσεις ή ελαττώματα, διατηρείται η συνολική ποιότητα και αξιοπιστία της εφαρμογής, παρέχοντας μια ισχυρή λύση για τις διαδικασίες ψηφιακής εγκληματολογίας.

## 7. Λοιπές παρατηρήσεις

Κατά τη διάρκεια της συγγραφής του κώδικα της εφαρμογής, παρουσιάστηκαν δύο σφάλματα (bugs), τα οποία δεν επηρεάζουν τη σωστή λειτουργία της εφαρμογής κι έτσι, η λύση τους θα προσεγγιστεί θεωρητικά. Τα σφάλματα αυτά είναι:

1. Κατά τη διαδικασία της μεταβίβασης της κυριότητας ενός αποδεικτικού στοιχείου σε έναν ερευνητή ο οποίος δεν είναι καταχωρημένος στην υπόθεση που ανήκει το αποδεικτικό στοιχείο, παρόλο που ολοκληρώνεται η διαδικασία, ο αριθμός των ενεργών υποθέσεων του ερευνητή παραμένει ίδιος (δεν αυξάνεται). Βέβαια, με αυτόν τον τρόπο διακυβεύεται η ασφάλεια και η ακεραιότητα του αποδεικτικού στοιχείου, καθώς μπορεί η μεταβίβαση αυτή να είναι αποτέλεσμα μιας κακόβουλης ενέργειας. Συνεπώς, η ορθότερη λύση στο πρόβλημα θα ήταν ο έλεγχος των ερευνητών στους οποίους έχει ανατεθεί η υπόθεση, ούτως ώστε αν δεν ανήκει σε αυτούς ο παραλήπτης της κυριότητας, να ακυρώνεται άμεσα η διαδικασία.

2. Μετά τη διαγραφή ενός ερευνητή, που έχει μία η περισσότερες ενεργές υποθέσεις, από το blockchain, η διεύθυνσή του παραμένει στη λίστα των ερευνητών που έχει ανατεθεί η υπόθεση. Αυτό το σφάλμα μπορεί να αντιμετωπιστεί με δύο τρόπους: είτε να μην επιτρέπεται εξαρχής η διαγραφή και να εμφανίζει το κατάλληλο μήνυμα στον χρήστη, είτε να διαγράφεται ο ερευνητής αυτόματα και από την υπόθεση.

## Κεφάλαιο 8: Συμπεράσματα

---

Η έρευνα που διεξήχθη στο πλαίσιο αυτής της διπλωματικής εργασίας ανέδειξε τις δυνατότητες συνέργειας των ιδιωτικών blockchain και των εφαρμογών chain of custody στον τομέα της ψηφιακής εγκληματολογίας. Οι σύγχρονες εξελίξεις στον τεχνολογικό τομέα έχουν τονίσει την κρισιμότητα της αποτελεσματικής συλλογής, της ασφαλούς αποθήκευσης, της σχολαστικής διατήρησης και της μεθοδικής ανάλυσης των ψηφιακών εγκληματολογικών στοιχείων, ένα βασικό εργαλείο για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο και την παρουσίαση τεκμηριωμένων αποδεικτικών στοιχείων στο πλαίσιο νομικών διαδικασιών. Στον τομέα των ερευνών στον κυβερνοχώρο, η διαχείριση των ψηφιακών αποδεικτικών στοιχείων και του chain of custody τους αποκτά αυξημένη σημασία, χρησιμεύοντας ως θεμελιώδης ανησυχία, που ασκεί βαθύ αντίκτυπο στην αποτελεσματικότητα των ερευνών για εγκλήματα στον κυβερνοχώρο, καθώς συνδέουν διακριτά γεγονότα και δραστηριότητες που διευκολύνουν τη διεξαγωγή ολοκληρωμένων ποινικών ερευνών.

Τα εγγενή χαρακτηριστικά της τεχνολογίας blockchain διασφαλίζουν ιδιότητες όπως η ακεραιότητα, η διαφάνεια, η αυθεντικότητα, η ασφάλεια και η δυνατότητα ελέγχου των δεδομένων, καθιστώντας την ενδεχομένως, την καλύτερη επιλογή για τη δημιουργία και τη σχολαστική παρακολούθηση του chain of custody στον τομέα των ψηφιακών εγκληματολογικών διαδικασιών. Η διατήρηση του chain of custody αναδεικνύεται ως καίριας σημασίας, καθώς έχει τη δυνατότητα να τεκμηριώσει την ακρίβεια των αποδεικτικών στοιχείων υποδεικνύοντας την πιθανότητα παραποίησης κατά τα στάδια της συλλογής και της επακόλουθης ανάλυσης τους.

Μέσω της ανάπτυξης του ιδιωτικού Ethereum Blockchain «ThemisChain» και της αποκεντρωμένης εφαρμογής chain of custody «Themis», επιτεύχθηκε μια ολοκληρωμένη διερεύνηση της αλληλένδετης δυναμικής τους. Η σύγκλιση των τεχνολογιών αυτών έχει χαράξει μια πορεία προς την αυξημένη ακεραιότητα και την ενισχυμένη διαφάνεια και ασφάλεια των δεδομένων στο τοπίο των ψηφιακών εγκληματολογικών διαδικασιών.

Η διερεύνηση της δομής, του σχεδιασμού και της υλοποίησης του ιδιωτικού Ethereum Blockchain και της εφαρμογής chain of custody αποκάλυψε ένα ανθεκτικό πλαίσιο που όχι μόνο βελτιστοποιεί τη διαχείριση αποδεικτικών στοιχείων αλλά και αντιμετωπίζει τις προκλήσεις που συνδέονται με τη διασφάλιση της ιχνηλασιμότητας και της μη αποκήρυξης (non-repudiation) των αποδεικτικών στοιχείων. Η χρήση των

χαρακτηριστικών της τεχνολογίας του blockchain έχει σφυρηλατήσει ένα αξιόπιστο και ανθεκτικό στην παραβίαση αποθετήριο αποδεικτικών στοιχείων, προωθώντας ένα ασφαλές chain of custody, καθ' όλη τη διάρκεια του κύκλου ζωής της έρευνας.

Τα ευρήματα αυτής της μελέτης σηματοδοτούν ένα σημαντικό βήμα προς την προσπάθεια μετασχηματισμού της σφαίρας των ψηφιακών εγκληματολογικών διαδικασιών. Η συνεργασία μεταξύ ιδιωτικών blockchain και εφαρμογών chain of custody προσφέρει μια μετασχηματιστική αλλαγή στον τρόπο με τον οποίο οργανώνονται, διατηρούνται και παρουσιάζονται τα αποδεικτικά στοιχεία.

Εν κατακλείδι, αυτή η εργασία υπογραμμίζει τη σημασία της συνεργατικής καινοτομίας μεταξύ της τεχνολογίας blockchain και των ερευνητικών μεθοδολογιών, θέτοντας τις βάσεις για μια επερχόμενη εποχή αυξημένης ασφάλειας, διαφάνειας και ευθύνης στην ψηφιακή εγκληματολογία. Τα αποτελέσματα που παρουσιάστηκαν υπογραμμίζουν την επιτακτική ανάγκη για συνεχή έρευνα και βελτίωση παρόμοιων λύσεων στο εξελισσόμενο τοπίο της διαχείρισης ψηφιακών αποδεικτικών στοιχείων. Καθώς η τεχνολογία εξελίσσεται, οι δυνατότητες ενίσχυσης της ακεραιότητας και της αξιοπιστίας της ψηφιακής εγκληματολογίας μέσω νέων εφαρμογών της τεχνολογίας blockchain παραμένουν απεριόριστες.

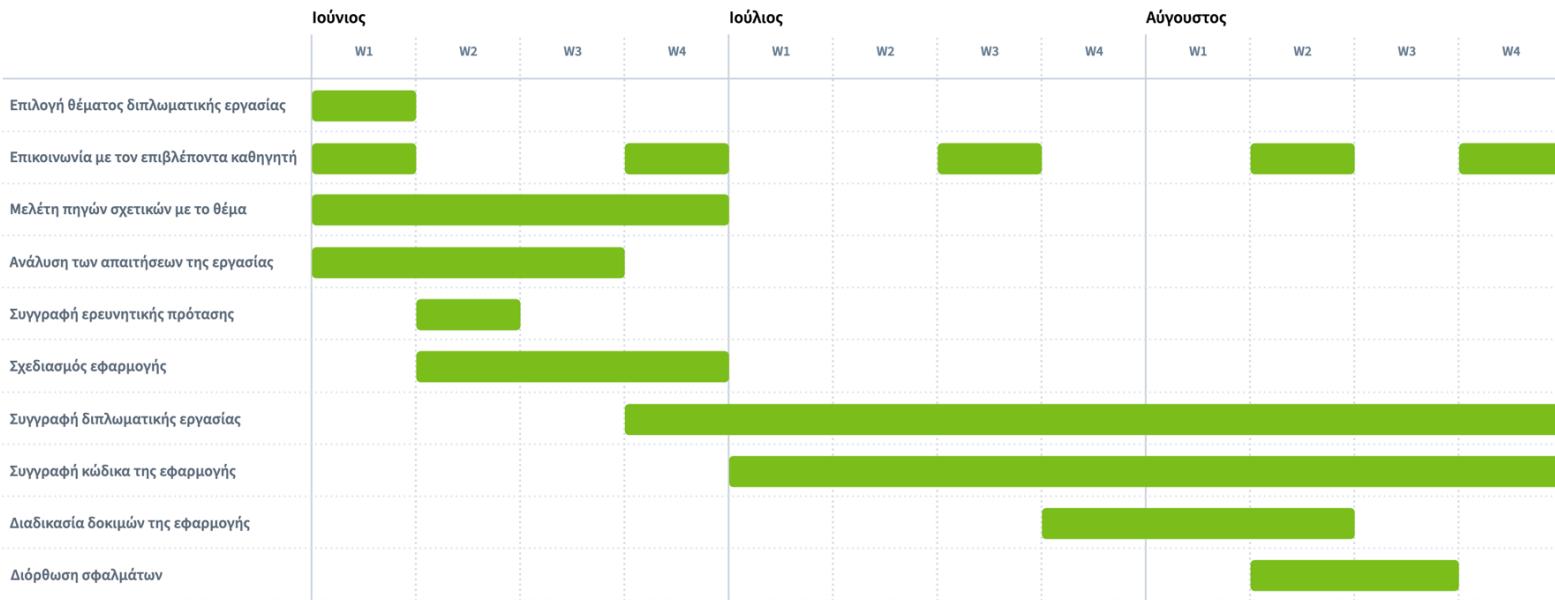
## 8.1. Μελλοντικές ενέργειες

Στον απόηχο αυτής της έρευνας, αναδύεται μια σειρά από πιθανές οδούς για επακόλουθη εξερεύνηση και ανάπτυξη, παρουσιάζοντας προοπτικές για σχολαστική ενίσχυση και επέκταση της αρμονικής συγχώνευσης ιδιωτικών blockchain και εφαρμογών chain of custody στον τομέα της ψηφιακής εγκληματολογίας. Αρχικά, στους μελλοντικούς στόχους ανάπτυξης περιλαμβάνεται η ενσωμάτωση του αναπτυχθέντος μοντέλου (ThemisChain & ThemisApp) σε κάποιο πιθανό δικαστικό σύστημα, στο οποίο θα έχουν πρόσβαση τα στελέχη του εκάστοτε δικαστηρίου (π.χ. δικηγόροι και δικαστές), ώστε να ελέγχουν και να επαληθεύουν οι ίδιοι την ακεραιότητα των αποδεικτικών στοιχείων. Έπειτα, σε επίπεδο κώδικα τα σχέδια μελλοντικής ανάπτυξης της εφαρμογής περιλαμβάνουν δύο στόχους. Ο πρώτος από αυτούς είναι η διαδικασία ενίσχυσης του hash των αποδεικτικών στοιχείων με την προσθήκη τυχαίων χαρακτήρων (salting) σε κάθε ένα από αυτά, αυξάνοντας την πολυπλοκότητά τους. Ο δεύτερος, όπως αναφέρθηκε και στο υποκεφάλαιο 4.1 (βλ. σελίδα 37), είναι η περιοδική καταγραφή της κατάστασης (state) του ιδιωτικού

blockchain σε ένα δημόσιο, διασφαλίζοντας την ακεραιότητα του ίδιου του καθολικού. Ένας ακόμη μελλοντικός στόχος είναι η μετατροπή του ιδιωτικού blockchain, που όπως σημειώνεται στο υποκεφάλαιο 6.1 (βλ. σελίδα 73) βάσει των κανόνων σύνδεσής του, προορίζεται για ακαδημαϊκή χρήση, σε ένα δίκτυο ικανό να διαχειριστεί πραγματικά δεδομένα εγκληματολογίας. Επιπλέον, η επικύρωση της εφαρμογής σε ένα φάσμα πραγματικών εγκληματολογικών σεναρίων θα μπορούσε να δημιουργήσει μια σταθερή βάση για εκτεταμένες μελέτες περιπτώσεων και εμπειρικές αξιολογήσεις. Ακόμη, η εμβάθυνση στην ενσωμάτωση προηγμένων κρυπτογραφικών τεχνικών, όπως οι αποδείξεις μηδενικής γνώσης (zero-knowledge proofs) ή η ομομορφική κρυπτογράφηση (homomorphic encryption), έχει την ικανότητα να αυξήσει τις διαστάσεις απορρήτου και εμπιστευτικότητας της εφαρμογής, διασφαλίζοντας το απόρθητο των ευαίσθητων πληροφοριών κατά τη διάρκεια της ερευνητικής διαδικασίας. Αυτές οι επερχόμενες τροχιές διαθέτουν συλλογικά τη δύναμη να ενισχύσουν τις συνεισφορές της έρευνας και να κατευθύνουν τον τομέα της ψηφιακής εγκληματολογίας προς την αυξημένη αποτελεσματικότητα, αξιοπιστία και τεχνολογική πρόοδο.

## Κεφάλαιο 9: Παράρτημα

### 9.1. Χρονοπρογραμματισμός έργου



Εικόνα 102 - Διάγραμμα Gantt

Το παραπάνω διάγραμμα Gantt παρουσιάζει την αναμενόμενη χρονική έκταση του έργου, από την επιλογή του θέματος, έως την παράδοσή του. Ο χρόνος μετράται σε εβδομάδες, ξεκινώντας από την πρώτη εβδομάδα του Ιουνίου, που πραγματοποιείται η επιλογή του θέματος της εργασίας. Η χρονολόγηση της κατανομής των δραστηριοτήτων αποσκοπεί στην αποδοτικότερη επιτέλεση του έργου. Ενδεικτικά, η επικοινωνία με τον επιβλέποντα καθηγητή ορίστηκε να πραγματοποιείται κάθε τρεις εβδομάδες, ώστε να εξασφαλιστούν επαρκή δεδομένα για παρουσίαση και ανατροφοδότηση. Αξίζει επίσης να αναφερθεί, πως για την μελέτη των πηγών χρειάστηκε χρόνος ίσος με τέσσερις (4) εβδομάδες, καθώς προηγήθηκε έρευνα και αξιολόγηση του περιεχομένου τους. Η ανάλυση των απαιτήσεων της εργασίας, που ξεκίνησε ταυτόχρονα με την μελέτη των πηγών, διήρκησε τρεις (3) εβδομάδες, λόγω της πολυπλοκότητας του θέματος. Ο χρόνος που αφιερώθηκε για τον σχεδιασμό της εφαρμογής δεν ξεπέρασε τις τρεις (3) εβδομάδες, καθώς η απλότητα και ταυτόχρονα η χρηστικότητα της εφαρμογής αποτέλεσαν βασικό κριτήριο για την υλοποίησή της. Τέλος, ο χρόνος που απέμεινε διατέθηκε στην συγγραφή της διατριβής και του κώδικα της εφαρμογής. Στην τελευταία, συμπεριλήφθηκαν οι δοκιμές που υποβλήθηκε η εφαρμογή και η διόρθωση των σφαλμάτων που παρουσιάστηκαν, στις οποίες

αφιερώθηκε αρκετός χρόνος ώστε να αντιμετωπιστούν πιθανά ζητήματα και να καταστεί η εφαρμογή άρτια.

## 9.2. Βιβλιογραφικές αναφορές

Acharya, D.P. (2022). Understanding Different Types of Application Testing. [online] Geekflare. Available at: <https://geekflare.com/understanding-application-testing/> [Accessed 2 Aug. 2023].

Ahmad, L., Khanji, S., Iqbal, F. and Kamoun, F. (2020). Blockchain-based chain of custody. Proceedings of the 15th International Conference on Availability, Reliability and Security. doi:<https://doi.org/10.1145/3407023.3409199>

Anand, A. (2020). Breaking Down : SHA-256 Algorithm. [online] Medium. Available at: <https://infosecwriteups.com/breaking-down-sha-256-algorithm-2ce61d86f7a3> [Accessed 23 Jul. 2023].

Antolin, M. (2022). What Is Proof-of-Authority? [online] CoinDesk. Available at: <https://www.coindesk.com/learn/what-is-proof-of-authority/> [Accessed 24 Jul. 2023].

Antonopoulos, A. and Wood, G. (2018). Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media.

Buterin, V. (2013). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. [online] Available at: <https://github.com/ethereum/wiki/wiki/White-Paper> [Accessed 25 Jul. 2023].

CardBoard. (2020). How to Prioritize Agile Stories. [online] Available at: <https://cardboardit.com/2020/08/how-to-prioritize-agile-stories/> [Accessed 26 Jul. 2023].

Castor, A. (2017). A (Short) Guide to Blockchain Consensus Protocols. [online] CoinDesk. Available at: <https://www.coindesk.com/markets/2017/03/04/a-short-guide-to-blockchain-consensus-protocols/> [Accessed 24 Jul. 2023].

Chen, H. and Liang, D. (2022). Adaptive Spatio-Temporal Query Strategies in Blockchain. ISPRS International Journal of Geo-Information, 11(7), p.409. doi:<https://doi.org/10.3390/ijgi11070409>.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, [online] 4(4), pp.2292–2303. doi:<https://doi.org/10.1109/access.2016.2566339>.

coin98.net. (2022). What Is EVM (Ethereum Virtual Machine)? How Does EVM Work? [online] Available at: <https://coin98.net/what-is-evm> [Accessed 25 Jul. 2023].

Ćosić, J. and Bača, M. (2010). (Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. The 33rd International Convention MIPRO, pp.1226–1230.

Ethereum.org (2023). Introduction to dapps. [online] Ethereum.org. Available at: <https://ethereum.org/en/developers/docs/dapps/> [Accessed 25 Jul. 2023].

Fernandez-Carames, T.M. and Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access, 8, pp.21091–21116.  
doi:<https://doi.org/10.1109/access.2020.2968985>.

Giova, G. (2011). Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems. International Journal of Computer Science and Network Security, Vol. 11, pp.1–9.

Goldmann, M. (2019). App Vs. dApp. [online] Cryptopolitan. Available at: <https://www.cryptopolitan.com/app-vs-dapp/> [Accessed 25 Jul. 2023].

Gondek, C. (n.d.). What is a Consortium Blockchain? [online] originstamp.com. Available at: <https://originstamp.com/blog/what-is-a-consortium-blockchain/#what-is-consortium-blockchain> [Accessed 25 Jul. 2023].

Guo, J., Wei, X., Zhang, Y., Ma, J., Gao, H., Wang, L. and Liu, Z. (2022). Antitampering Scheme of Evidence Transfer Information in Judicial System Based on Blockchain. 2022, pp.1–19. doi:<https://doi.org/10.1155/2022/5804109>.

Gupta, R. (2018). Hands-on cybersecurity with blockchain : implement DDoS protection, PKI-based identity, 2FA, and DNS security using blockchain. Birmingham ; Mumbai: Packt.

Hamilton, T. (2019a). Unit Testing Tutorial: What is, Types, Tools, EXAMPLE. [online] Guru99.com. Available at: <https://www.guru99.com/unit-testing-guide.html> [Accessed 2 Aug. 2023].

Hamilton, T. (2019b). Integration Testing: What is, Types, Top Down & Bottom Up Example. [online] Guru99.com. Available at: <https://www.guru99.com/integration-testing.html> [Accessed 2 Aug. 2023].

Jeong, J., Kim, D., Lee, B. and Son, Y. (2020). Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric. J. Inf. Process. Syst., 16, pp.760–773. doi:<https://doi.org/10.3745/JIPS.04.0178>.

Kahate, A. (2017). Cryptography and Network Security. 3rd ed. McGraw Hill Education India Pvt Ltd.

Kaley, A. (2021). Mapping User Stories in Agile. [online] Nielsen Norman Group. Available at: <https://www.nngroup.com/articles/user-story-mapping/> [Accessed 26 Jul. 2023].

Khan, A.A., Uddin, M., Shaikh, A., Laghari, A.A. and Rajput, A. (2021). MF-Ledger: Blockchain Hyperledger Sawtooth-enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture. *IEEE Access*, pp.1–1.  
doi:<https://doi.org/10.1109/access.2021.3099037>.

Liu, B., Si, X. and Kang, H. (2022). A Literature Review of Blockchain-Based Applications in Supply Chain. *Sustainability*, 14(22), p.15210.  
doi:<https://doi.org/10.3390/su142215210>.

Lone, A. (2017). Forensic-chain: Ethereum blockchain based digital forensics chain of custody. *Scientific and practical cyber security journal*, Vol. 1.

Lone, A.H. and Mir, R.N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, 28, pp.44–55. doi:<https://doi.org/10.1016/j.diin.2019.01.002>.

Lozupone, V. (2018). Analyze encryption and public key infrastructure (PKI). *International Journal of Information Management*, 38(1), pp.42–44.  
doi:<https://doi.org/10.1016/j.ijinfomgt.2017.08.004>.

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*, [online] 15, pp.80–90.  
doi:<https://doi.org/10.1016/j.jiii.2019.04.002>.

Lucidchart (2019). Introducing Types of UML Diagrams | Lucidchart Blog. [online] Lucidchart.com. Available at: <https://www.lucidchart.com/blog/types-of-UML-diagrams> [Accessed 27 Jul. 2023].

Majumder, P. (2022). Understanding Distributed Ledger Technology. [online] Analytics Vidhya. Available at: <https://www.analyticsvidhya.com/blog/2022/07/understanding-distributed-ledger-technology/> [Accessed 24 Jul. 2023].

Mishra, D. (2021). API Use-Case Prioritization Approach and Methodology. [online] Available at: <https://www.linkedin.com/pulse/api-use-case-prioritization-approach-methodology-debasisa-mishra/> [Accessed 26 Jul. 2023].

Nakamoto, S. (2008). Bitcoin: a Peer-to-Peer Electronic Cash System. [online] Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 23 Jul 2023].

Oliveira, J., Rosado, M. and Faria P.M. (2020). Zeroconf Network Retail Kiosk for Fish Products Traceability. doi:<https://doi.org/10.23919/cisti49556.2020.9141069>.

Oliveira, M.T., Carrara, G.R., Fernandes, N.C., Albuquerque, C.V.N., Carrano, R.C., Medeiros, D.S.V. and Mattos, D.M.F. (2019). Towards a Performance Evaluation of Private Blockchain Frameworks using a Realistic Workload. *2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*.  
doi:<https://doi.org/10.1109/icin.2019.8685888>.

Pedamkar, P. (2019). Application Testing | Complete Guide to Application Testing. [online] Available at: <https://www.educba.com/application-testing/> [Accessed 2 Aug. 2023].

Prasad, A. and Pandey, J. (2016). Digital Forensics. Uttrakhand Open University.

Rasjid, Z.E., Soewito, B., Witjaksono, G. and Abdurachman, E. (2017). A review of collisions in cryptographic hash function used in digital forensic tools. Procedia Computer Science, 116, pp.381–392. doi:<https://doi.org/10.1016/j.procs.2017.10.072>.

Rochmadi, T. and Heksaputra, D. (2019). Forensic Analysis in Cloud Storage with Live Forensics in Windows (Adrive Case Study). International Journal of Cyber-Security and Digital Forensics, Vol. 8(4).

Sathyaprakasan, R., Govindan, P., Alvi, S., Sadath, L., Philip, S. and Singh, N. (2021). An Implementation of Blockchain Technology in Forensic Evidence Management. 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). doi:<https://doi.org/10.1109/iccike51210.2021.9410791>.

Scrum.org (n.d.). What is Scrum? [online] Scrum.org. Available at: <https://www.scrum.org/resources/what-scrum-module> [Accessed 26 Jul. 2023].

Sinha, D. (2023). What is an Epic in Agile? examples and Differences. [online] knowledgehut.com. Available at: <https://www.knowledgehut.com/blog/agile/what-is-an-epic-agile> [Accessed 26 Jul. 2023].

Tardi, C. (2021). Genesis Block Definition. [online] Investopedia. Available at: <https://www.investopedia.com/terms/g/genesis-block.asp> [Accessed 23 Jul 2023].

Tikhomirov, S. (2018). Ethereum: State of Knowledge and Research Perspectives. Foundations and Practice of Security, pp.206–221. doi:[https://doi.org/10.1007/978-3-319-75650-9\\_14](https://doi.org/10.1007/978-3-319-75650-9_14).

Umoren, O., Singh, R., Awan, S., Pervez, Z. and Dahal, K. (2022). Blockchain-Based Secure Authentication with Improved Performance for Fog Computing. Sensors, 22(22), p.8969. doi:<https://doi.org/10.3390/s22228969>.

Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y. and Kim, D.I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access, [online] 7, pp.22328–22370. doi:<https://doi.org/10.1109/access.2019.2896108>.

Wheelbarger, S. (2009). History of Computer Forensics. [online] Criminal Justice Collaboratory. Available at: <http://colbycriminaljustice.wikidot.com/cyberforensics> [Accessed 26 Jul. 2023].

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper. [online] Available at: <https://ethereum.github.io/yellowpaper/paper.pdf> [Accessed 25 Jul. 2023].

World Bank (2017). International Bank for Reconstruction and Development / the World Bank. In: FinTech Note | No. 1. [online] Washington, DC: World Bank Group. Available at:

<https://openknowledge.worldbank.org/server/api/core/bitstreams/5166f335-35db-57d7-9c7e-110f7d018f79/content> [Accessed 24 Jul. 2023].

Wrike (2019). What is a Project Charter in Project Management? [online] Wrike.com. Available at: <https://www.wrike.com/project-management-guide/faq/what-is-a-project-charter-in-project-management/> [Accessed 26 Jul. 2023].

Xiong, Y. and Du, J. (2019). Electronic evidence preservation model based on blockchain. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19. doi:<https://doi.org/10.1145/3309074.3309075>.

Xu, M., Chen, X. and Kou, G. (2019). A systematic review of blockchain. Financial Innovation, [online] 5(1). doi:<https://doi.org/10.1186/s40854-019-0147-z>.

Μαυρίδης, Ι. (2015). Ασφάλεια Πληροφοριών στο Διαδίκτυο. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών.

### 9.3. Γλωσσάριο απόδοσης ξενόγλωσσων όρων

**Admin:** Διαχειριστής

**Agile:** Μεθοδολογία ανάπτυξης

**Amazon Web Services (AWS):** Πλατφόρμα παροχής υπηρεσιών «cloud» της Amazon

**API:** Μέθοδος επικοινωνίας μεταξύ συστημάτων

**Audit trail:** Διαδρομή ελέγχου

**Blockchain:** Αλυσίδα συστοιχιών

**Chain of custody:** Αλυσίδα επιτήρησης

**Consensus mechanism:** Μηχανισμός Συναίνεσης

**Cryptographic hashing function:** Κρυπτογραφική συνάρτηση κατακερματισμού

**Decentralized Application:** Αποκεντρωμένη Εφαρμογή

**Denial of Service (DoS):** Επίθεση άρνησης υπηρεσιών digital forensics

**Distributed Ledger:** Κατανεμημένα Καθολικό

**ETH:** Το νόμισμα του Ethereum Blockchain

**Ethereum Virtual Machine (EVM):** Εικονική Μηχανή Ethereum

**Ethereum:** Πρωτόκολλο Blockchain

**Gas limit:** Το όριο του «καυσίμου» στο Ethereum Blockchain

**Gas price:** Η τιμή του «καυσίμου» στο Ethereum Blockchain

**Gas:** Το «καύσιμο» του Ethereum Blockchain

**Genesis block:** Το πρώτο block σε ένα blockchain

**Geth Javascript Console:** Περιβάλλον ανάπτυξης και αλληλεπίδρασης με έναν κόμβο «Geth»

**Geth:** Υλοποίηση του Ethereum σε γλώσσα προγραμματισμού «Go»

**Hash pointer:** Δείκτης κατακερματισμού

**Hyperledger Fabric:** Πλατφόρμα Blockchain

**HyperText Markup Language (HTML):** Γλώσσα σήμανσης ιστοσελίδων

**Internet of Things (IoT):** Διαδίκτυο των Πραγμάτων

**Investigator:** Ερευνητής

**Javascript:** Γλώσσα προγραμματισμού

**MetaMask:** Λογισμικό πορτοφόλι για την αλληλεπίδραση με το Ethereum blockchain

**Miner:** «Μεταλλωρύχος»

**Mockup:** Προσχέδιο εφαρμογής

**Node:** Κόμβος

**On-chain:** Κάτι που βρίσκεται στο blockchain

**Opcode:** Τμήμα μιας εντολής γλώσσας μηχανής που καθορίζει τη λειτουργία που πρέπει να εκτελεστεί

**Peer-to-Peer Network:** Ομότιμο Δίκτυο

**Permissioned blockchain:** Ελεγχόμενο blockchain

**Port:** Θύρα

**Scrum:** Πλαίσιο (Framework) της μεθοδολογίας «Agile»

**Scrypt:** Αλγόριθμο κατακερματισμού

**Secure Hash Algorithm-256 (SHA-256):** Αλγόριθμο κατακερματισμού

**Single point of failure:** Ένα μέρος ενός συστήματος που, εάν αποτύχει, θα σταματήσει να λειτουργεί ολόκληρο το σύστημα.

**Solidity:** Γλώσσα προγραμματισμού «έξυπνων» συμβολαίων

**Turing-Complete:** Υπολογιστικά πλήρες σύστημα

**Unified Modeling Language (UML):** Ενοποιημένη Γλώσσα Σχεδίασης Προτύπων

**Validator:** Επαληθευτής στον αλγόριθμο συναίνεσης «PoA»

**Wireframe:** «Μακέτα» εφαρμογής

## 9.4. Αρχείο genesis.json

## 9.5. Αρχείο static-nodes.json

```
[

"enode://5deb2157dec732289584cb8abfe78a0cdb1f3fcfad956e552a4ba4fa69261fc74fb
596c5b566a1673a787850ac7c0a176dd4760dbdd9b07e9353e5643123693b@18.232.0.78:30
303",

"enode://5b8af4884487c73faeb298558d73efc2f31c3f50486199206d9108b012001e89f0c
d6deb10694d2294222fbd2a6dc2e2e0a02a72faeb9d1b5c1e472ebe1c6f64@52.73.112.80:3
0303",

"enode://45bfacf8f9a7b61f3a69cb8465b5de4655ae42062d760a21342a575691fec81363
ddff20fe0f5c67daf40be31983612a4ec738da34e9da5248ba678f6949a22@52.20.6.247:30
303"
]
```

## 9.6. Αρχείο geth.service

```
//Geth Service Node0
[Unit]
Description=Go Ethereum Client

[Service]
User=root
Type=simple
Restart=always
ExecStart=/usr/local/bin/geth --networkid 1997 --datadir
/opt/ThemisChain/node0/data --port 30303 --ipcdisable --syncmode full --rpc
--allow-insecure-unlock --rpccorsdomain "*" --rpcport 8545 --rpcaddr
"172.31.83.3" --unlock 0xED2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac --password
/opt/ThemisChain/node0/password.txt --mine --rpcapi
personal,admin,db,eth,net,web3,miner,ssh,txpool,debug,cliique --ws --wsaddr
172.31.83.3 --wsport 8546 --wsorigins "*" --wsapi
personal,admin,db,eth,net,web3,miner,ssh,txpool,debug,cliique --maxpeers 25 --
etherbase 0 --gasprice 0 --targetgaslimit 99999999

[Install]
WantedBy=default.target

//Geth Service Node1
[Unit]
Description=Go Ethereum Client

[Service]
User=root
Type=simple
Restart=always
ExecStart=/usr/local/bin/geth --networkid 1997 --datadir
/opt/Themischain/node1/data --port 30303 --ipcdisable --syncmode full --rpc
--allow-insecure-unlock --rpccorsdomain "*" --rpcport 8545 --rpcaddr
```

```
"172.31.89.21" --unlock 0x038573b4588805551f475d737Dad9b91b5a17025 --
password /opt/Themischain/node1/password.txt --mine --rpcapi
personal,admin,db,eth,net,web3,miner,ssh,txpool,debug,cliique --ws --wsaddr
172.31.89.21 --wsport 8546 --wsorigins "*" --wsapi
personal,admin,db,eth,net,web3,miner,ssh,txpool,debug,cliique --maxpeers 25 --
etherbase 0 --gasprice 0 --targetgaslimit 99999999

[Install]
WantedBy=default.target

//Geth Service Node2
[Unit]
Description=Go Ethereum Client

[Service]
User=root
Type=simple
Restart=always
ExecStart=/usr/local/bin/geth --networkid 1997 --datadir
/opt/ThemisChain/node2/data --port 30303 --ipcdisable --syncmode full --rpc
--allow-insecure-unlock --rpccorsdomain "*" --rpcport 8545 --rpcaddr
"172.31.80.130" --unlock 0x86f565572b9331025CC5a0861cd6F4A3d7b134dF --
password /opt/ThemisChain/node2/password.txt --mine --rpcapi
personal,admin,db,eth,net,web3,miner,ssh,txpool,debug,cliique --ws --wsaddr
172.31.80.130 --wsport 8546 --wsorigins "*" --wsapi
personal,admin,db,eth,net,web3,miner,ssh,txpool,debug,cliique --maxpeers 25 --
etherbase 0 --gasprice 0 --targetgaslimit 99999999

[Install]
WantedBy=default.target
```

## 9.7. Αρχείο node0account.json

```
{"address":"ed2de21f55fb1c2fd8d56f1cf2a33998030dc9ac","crypto":{"cipher":"aes-128-ctr","ciphertext":"771ed23a278df5cf495095332f465c146113d607e06c64f6e037396b80961191","cipherparams":{"iv":"a26f7150dd843146361d4c2e267baf27"},"kdf":"scrypt","kdfparams":{"dklen":32,"n":262144,"p":1,"r":8,"salt":"773be3df3310212f13902908ee597517a2285d8e996d386c9303a803897f460a"},"mac":"c15e509cecd4fdfc02fc8e84c07c46d921f82c36341a26431fd684212739d7b0"},"id":"632a7b3c-f2e3-4e6f-99d4-b03160024bb3","version":3}
```

## 9.8. Κώδικας έξυπνων συμβολαίων

### 9.8.1. Έξυπνο συμβόλαιο Issued.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

contract Issued {

    //Administrator counter
    uint public adminCounter;

    //Administrator info struct
    struct AdminInfo {
        address walletAddress;
        string fullName;
        string email;
        uint mobile;
        string dob;
    }

    //Administrator lists
    mapping(address => AdminInfo) public adminList;
    mapping(uint => AdminInfo) public adminCountList; //This list is used by
the admins to render every administrator info

    //Constructor used to create three administrators with the
setAdminInfo() function. These addresses correspond to the authorized nodes
of the private blockchain (ThemisChain)
    constructor() {
        setAdminInfo(0xEd2DE21F55Fb1c2Fd8d56f1Cf2A33998030dc9Ac, "Christos
Bandis", "chr.bandis@gmail.com", 6973979235, "1997-02-20"); //Node 0
        setAdminInfo(0x038573b458805551f475d737Dad9b91b5a17025, "Admin
NodeOne", "admin@nodeone.com", 6999999999, "1997-01-01"); //Node 1
        setAdminInfo(0x86f565572b9331025CC5a0861cd6F4A3d7b134dF, "Admin
NodeTwo", "admin@nodetwo.com", 6900000000, "1997-01-02"); //Node 2
    }

    //onlyAdmin modifier used in "Investigator" and "Case" smart contracts
    modifier onlyAdmin() {
        require(adminList[msg.sender].walletAddress == msg.sender, "You are
not allowed");
        _;
    }

    //Private function to add an administrator (can be called only within
this smart contract)
    function setAdminInfo (address _walletAddress, string memory _fullname,
string memory _email, uint _mobile, string memory _dob) private {
        adminList[_walletAddress].walletAddress = _walletAddress;
        adminList[_walletAddress].fullName = _fullname;
        adminList[_walletAddress].email = _email;
        adminList[_walletAddress].mobile = _mobile;
    }
}
```

```

adminList[_walletAddress].dob = _dob;

adminCountList[adminCounter].walletAddress = _walletAddress;
adminCountList[adminCounter].fullName = _fullname;
adminCountList[adminCounter].email = _email;
adminCountList[adminCounter].mobile = _mobile;
adminCountList[adminCounter].dob = _dob;

adminCounter++;
}

//Function to check if an administrator exists
function adminExists (address _walletAddress) public view returns (bool)
{
    if (adminList[_walletAddress].walletAddress == _walletAddress) {
        return true;
    } else {
        return false;
    }
}
}

```

### 9.8.2. Έξυπνο συμβόλαιο Investigator.sol

```

// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

import "./Issued.sol";

contract Investigator is Issued {

    //Investigator counter
    uint public investigatorCounter;

    //Array that keeps a history of the IDs assigned to investigators
    uint[] public investigatorIdArray;

    //Investigator info struct
    struct InvestigatorInfo {
        address walletAddress;
        uint invId;
        string fullName;
        string email;
        uint mobile;
        string dob;
        address issuedBy;
    }

    //Investigator lists
    mapping (address => InvestigatorInfo) public investigatorList;
}

```

```

mapping (uint => InvestigatorInfo) public adminInvestigatorList; //This
list is used by the admins to render every investigator info

//Events
event IsSuccessful(bool result);
event AddressExists(bool exists);

//Function to add an investigator, with the "onlyAdmin" modifier from
"Issued" smart contract, which means that only an admin can interact with it
function addInvestigator (address _walletAddress, uint _invId, string
memory _fullName, string memory _email, uint _mobile, string memory _dob,
address _issuer) public onlyAdmin {
    investigatorCounter++; //Investigator counter starts with 1

    if (investigatorList[_walletAddress].walletAddress != _walletAddress) { //Investigator existence check by wallet address
        emit AddressExists(false);
        investigatorList[_walletAddress].walletAddress = _walletAddress;
        investigatorList[_walletAddress].invId = _invId;
        investigatorList[_walletAddress].fullName = _fullName;
        investigatorList[_walletAddress].email = _email;
        investigatorList[_walletAddress].mobile = _mobile;
        investigatorList[_walletAddress].dob = _dob;
        investigatorList[_walletAddress].issuedBy = _issuer;

        adminInvestigatorList[investigatorCounter].walletAddress =
_walletAddress;
        adminInvestigatorList[investigatorCounter].invId = _invId;
        adminInvestigatorList[investigatorCounter].fullName = _fullName;
        adminInvestigatorList[investigatorCounter].email = _email;
        adminInvestigatorList[investigatorCounter].mobile = _mobile;
        adminInvestigatorList[investigatorCounter].dob = _dob;
        adminInvestigatorList[investigatorCounter].issuedBy = _issuer;

        investigatorIdArray.push(_invId); //Push investigator ID to
the idArray
        emit IsSuccessful(true);
    } else {
        emit AddressExists(true);
    }
}

//Function which returns the name of a certain investigator
function getInvestigatorName (address _walletAddress) public view
returns (string memory) {
    return investigatorList[_walletAddress].fullName;
}

//Function to delete an investigator, with the "onlyAdmin" modifier from
"Issued" smart contract, which means that only an admin can interact with it

```

```

        function removeInvestigator(address _walletAddress, uint _invId) public
onlyAdmin {
    investigatorList[_walletAddress].walletAddress =
0x0000000000000000000000000000000000000000000000000000000;
    investigatorList[_walletAddress].invId = 0;
    investigatorList[_walletAddress].fullName = "";
//In blockchain is impossible to delete something permanently, like in a
traditional
    investigatorList[_walletAddress].email = "";
//databases. Instead, delete means to assign the default value in a
variable. For example,
    investigatorList[_walletAddress].mobile = 0;
//the default value of a string variable is "" (empty) and of a uint is 0
    investigatorList[_walletAddress].dob = "";
    investigatorList[_walletAddress].issuedBy =
0x0000000000000000000000000000000000000000000000000000000;

    adminInvestigatorList[_invId].walletAddress =
0x0000000000000000000000000000000000000000000000000000000;
    adminInvestigatorList[_invId].invId = 0;
    adminInvestigatorList[_invId].fullName = "";
    adminInvestigatorList[_invId].email = "";
    adminInvestigatorList[_invId].mobile = 0;
    adminInvestigatorList[_invId].dob = "";
    adminInvestigatorList[_invId].issuedBy =
0x0000000000000000000000000000000000000000000000000000000;

    emit IsSuccessful(true);
}

//Function to check if an investigator exists
function investigatorExists (address _walletAddress) public view returns
(bool) {
    if (investigatorList[_walletAddress].walletAddress ==
_walletAddress) {
        return true;
    } else {
        return false;
    }
}

//Function to check if an investigator 's ID in the IdArray
function invIdExists (uint _invId) public view returns (bool) {
    for (uint i = 0; i < investigatorIdArray.length; i++) {
        if (investigatorIdArray[i] == _invId) {
            return true;
        }
    }
    return false;
}
}

```

### 9.8.3. Έξυπνο συμβόλαιο Case.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

import "./Evidence.sol";
import "./Issued.sol";

contract Case is Evidence, Issued {

    //Case ID counter
    uint public caseId;

    //Case info struct
    struct CaseInfo {
        uint caseNum;
        string caseName;
        string caseDesc;
        address[] caseInvestigators;
        address creator;
        string creationTime;
        mapping (uint => Evidence.EvidenceInfo[]) evidenceList;
        bool closed; //default false
    }

    //((Not used) Modifier to check if an evidence was deleted
    /* modifier evidenceNotDeleted(uint _caseId, uint _evidenceId) {
        bool isDeleted =
    caseList[_caseId].evidenceList[_caseId][_evidenceId].deleted;
        require (isDeleted == false, "There is no such evidence");
        _;
    } */

    //Case List
    mapping (uint => CaseInfo) public caseList;

    //Events
    event CaseExists(bool result);
    event IsSuccessful(bool result, uint id);
    event IsSuccessful_Evidence(bool result);
    event IsSuccessful_Investigator(bool result);

    //Function to open a new case, with the "onlyAdmin" modifier from
    "Issued" smart contract, which means that only an admin can interact with it
    function openNewCase (string memory _caseName, string memory _caseDesc,
address _caseInvestigator, address _caseCreator, string memory
_creationTime) public onlyAdmin {
        caseId++; //Case Id starts with 1
    }
}
```

```

        if (caseList[caseId].caseNum != caseId) { //Case Id existence check
            emit CaseExists(false);
            caseList[caseId].caseNum = caseId;
            caseList[caseId].caseName = _caseName;
            caseList[caseId].caseDesc = _caseDesc;
            caseList[caseId].caseInvestigators.push(_caseInvestigator);
            caseList[caseId].creator = _caseCreator;
            caseList[caseId].creationTime = _creationTime;
            caseList[caseId].closed = false;

            emit IsSuccessful(true, caseId);
        } else {
            emit CaseExists(true);
        }
    }

    //Function to check if a case exists based on its ID
    function caseExists (uint _caseId) public view returns (bool) {
        if (caseList[_caseId].caseNum == _caseId) {
            return true;
        }
    }

    //Function which returns the name of a case based on its ID
    function getCaseName (uint _caseId) public view returns (string memory)
    {
        return caseList[_caseId].caseName;
    }

    //Function which returns the active cases of a certain investigator
    function activeCases (uint _caseId, address _walletAddress) public view
returns (uint, string memory, string memory, address, string memory, bool) {
        CaseInfo storage thisCase = caseList[_caseId];

        address[] memory caseInvestigatorsArray =
caseList[_caseId].caseInvestigators;
        uint len = caseInvestigatorsArray.length;

        for (uint i = 0 ; i < len; i++){
            if (caseList[_caseId].caseInvestigators[i] == _walletAddress) {
                return (thisCase.caseNum, thisCase.caseName,
thisCase.caseDesc, thisCase.creator, thisCase.creationTime,
thisCase.closed);
            }
        }
    }

    //Function to close a case based on its ID and delete its evidence, with
    //the "onlyAdmin" modifier from "Issued" smart contract, which means that only
    //an admin can interact with it

```

```

function closeCase (uint _caseId) public onlyAdmin {
    caseList[_caseId].caseNum = 0;
//In blockchain is impossible to delete something permanently, like in a traditional database. Instead, delete means to assign the default value in a variable. For example,
    caseList[_caseId].caseName = "";
//the default value of a string variable is "" (empty) and of a uint is 0
    caseList[_caseId].creator =
0x0000000000000000000000000000000000000000000000000000000000000000;
    caseList[_caseId].creationTime = "";
    caseList[_caseId].closed = true;

    uint caseLen = caseList[_caseId].caseInvestigators.length;
    for (uint i = 0 ; i < caseLen; i++){
        delete caseList[_caseId].caseInvestigators[i];
    }

    Evidence.EvidenceInfo[] storage thisEvidence =
caseList[_caseId].evidenceList[_caseId];

    uint evidLen = thisEvidence.length;
    for (uint j = 0 ; j < evidLen; j++){
        delete thisEvidence[j]; //Delete doesn't actually delete the element but it assigns the default value to it (see comment above)
    }
}

//Function to assign an investigator to a case, with the "onlyAdmin" modifier from "Issued" smart contract, which means that only an admin can interact with it
function addCaseInvestigator (uint _caseId, address _investigator)
public onlyAdmin {
    caseList[_caseId].caseInvestigators.push(_investigator);
    emit IsSuccessful_Investigator(true);
}

//Function to remove an investigator from a case, with the "onlyAdmin" modifier from "Issued" smart contract, which means that only an admin can interact with it
function removeCaseInvestigator (uint _caseId, address _investigator)
public onlyAdmin {
    caseList[_caseId].caseInvestigators.push(_investigator);

    uint caseLen = caseList[_caseId].caseInvestigators.length;
    for (uint i = 0 ; i < caseLen; i++){
        if (caseList[_caseId].caseInvestigators[i] == _investigator) {
            delete caseList[_caseId].caseInvestigators[i];
        }
    }
}

```

```

        }

        emit IsSuccessful_Investigator(true);
    }

    //Function which returns the investigators of a particular case and the total number of them
    function getCaseInvestigators (uint _caseId) public view returns (address[] memory, uint) {
        address[] memory CaseInvestigators =
caseList[_caseId].caseInvestigators;
        uint len = CaseInvestigators.length;
        address[] memory investigatorResult = new address[](len);

        for (uint i = 0 ; i < len; i++){
            investigatorResult[i] = CaseInvestigators[i];
        }
        return (investigatorResult, len);
    }

    //Function to check if a case has already been assigned to an investigator
    function invExistsInCase (uint _caseId, address _walletAddress) public view returns (bool) {
        address[] memory CaseInvestigators =
caseList[_caseId].caseInvestigators;
        uint len = CaseInvestigators.length;

        for (uint i = 0 ; i < len; i++){
            if (CaseInvestigators[i] == _walletAddress) {
                return true;
            }
        }
    }

    //Function to add evidence to a case, with the "onlyAdmin" modifier from "Issued" smart contract, which means that only an admin can interact with it
    function addCaseEvidence (uint _caseId, bytes memory _evidenceHash, string memory _evidenceName, string memory _evidenceDesc, address _creator, string memory _dateCreated) public onlyAdmin {
        Evidence.EvidenceInfo[] storage thisEvidence =
caseList[_caseId].evidenceList[_caseId];
        Evidence.EvidenceInfo storage singleEvidence = thisEvidence.push();

        singleEvidence.evidenceHash = _evidenceHash;
        singleEvidence.evidenceName = _evidenceName;
        singleEvidence.evidenceDesc = _evidenceDesc;
        singleEvidence.creator = _creator;
        singleEvidence.dateCreated = _dateCreated;
        singleEvidence.transferChain.push(_creator);
        singleEvidence.transferDesc.push("Creation");
        singleEvidence.transferTime.push(_dateCreated);
    }
}

```

```

singleEvidence.deleted = false;

emit IsSuccessful_Evidence(true);
}

//Function which returns evidence 's info
function getCaseEvidenceCollapsed(uint _caseId, uint _evidenceId) public
view returns (bytes memory, string memory, string memory, bool) {
    Evidence.EvidenceInfo memory thisEvidence =
caseList[_caseId].evidenceList[_caseId][_evidenceId];
    return (thisEvidence.evidenceHash, thisEvidence.evidenceName,
thisEvidence.dateCreated, thisEvidence.deleted);
}

//Function which returns evidence 's info
function getCaseEvidenceExpanded(uint _caseId, uint _evidenceId) public
view returns (bytes memory, string memory, string memory, address, string
memory) {
    Evidence.EvidenceInfo memory thisEvidence =
caseList[_caseId].evidenceList[_caseId][_evidenceId];
    return (thisEvidence.evidenceHash, thisEvidence.evidenceName,
thisEvidence.evidenceDesc, thisEvidence.creator, thisEvidence.dateCreated);
}

//Function which returns evidence 's hash
function getEvidenceHash(uint _caseId, uint _evidenceId) public view
returns (bytes memory) {
    Evidence.EvidenceInfo memory thisEvidence =
caseList[_caseId].evidenceList[_caseId][_evidenceId];
    return (thisEvidence.evidenceHash);
}

//Function which returns the total number of the evidences in a case
function evidenceCount (uint _caseId) public view returns (uint){
    Evidence.EvidenceInfo[] storage thisEvidence =
caseList[_caseId].evidenceList[_caseId];
    return thisEvidence.length;
}

//Function which returns the current owner of an evidence
function getCurrentOwner (uint _caseId, uint _evidenceId) public view
returns (address) {
    Evidence.EvidenceInfo memory thisEvidence =
caseList[_caseId].evidenceList[_caseId][_evidenceId];
    address[] memory chain = thisEvidence.transferChain;
    return chain[chain.length - 1];
}

//Function to transfer an evidence from one investigator to another,
with the "onlyAdmin" modifier from "Issued" smart contract, which means that
only an admin can interact with it

```

```

        function transferEvidence (uint _caseId, uint _evidenceId, address _transferTo, string memory _transferDesc, string memory _transferTime)
public onlyAdmin {
    Evidence.EvidenceInfo storage thisEvidence =
caseList[_caseId].evidenceList[_caseId][_evidenceId];

    thisEvidence.transferChain.push(_transferTo);
    thisEvidence.transferDesc.push(_transferDesc);
    thisEvidence.transferTime.push(_transferTime);

    emit IsSuccessful_Evidence(true);
}

//Function which returns the chain of custody of an evidence
function viewChainOfCustody (uint _caseId, uint _evidenceId) public view
returns (uint, string memory, bytes memory, address[] memory, string[]
memory, string[] memory) {
    Evidence.EvidenceInfo memory thisEvidence =
caseList[_caseId].evidenceList[_caseId][_evidenceId];

    address[] memory transfChain = thisEvidence.transferChain;
    uint transfArrayLen = transfChain.length;           //transfArrayLen is
the same as the length of timeChain and descChain
    address[] memory transfResult = new address[](transfArrayLen);

    string[] memory timeChain = thisEvidence.transferTime;
    string[] memory timeResult = new string[](transfArrayLen);

    string[] memory descChain = thisEvidence.transferDesc;
    string[] memory descResult = new string[](transfArrayLen);

    for (uint i = 0 ; i < transfArrayLen; i++){
        transfResult[i] = transfChain[i];
        timeResult[i] = timeChain[i];
        descResult[i] = descChain[i];
    }
    return (transfArrayLen, thisEvidence.evidenceName,
thisEvidence.evidenceHash, transfChain, timeChain, descChain);
}

//Function to delete a certain evidence, with the "onlyAdmin" modifier
from "Issued" smart contract, which means that only an admin can interact
with it
function deleteEvidence (uint _caseId, uint _evidenceId) public
onlyAdmin {
    Evidence.EvidenceInfo storage thisEvidence =
caseList[_caseId].evidenceList[_caseId][_evidenceId];

    thisEvidence.evidenceHash =
"0x0000000000000000000000000000000000000000000000000000000000000000";
    thisEvidence.evidenceName = "";
}

```

```

thisEvidence.evidenceDesc = "";
thisEvidence.creator = 0x000000000000000000000000000000000000000000000000000000000000000;
thisEvidence.dateCreated = "";

uint transfArrayLen = thisEvidence.transferChain.length;
for (uint i = 0 ; i < transfArrayLen; i++){
    thisEvidence.transferChain[i] =
0x000000000000000000000000000000000000000000000000000000000000000;
    thisEvidence.transferDesc[i] = "";
    thisEvidence.transferTime[i] = "";
}
thisEvidence.deleted = true;

emit IsSuccessful_Evidence(true);
}
}

```

#### 9.8.4. Έξυπνο συμβόλαιο Evidence.sol

```

// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

contract Evidence {

    //Evidence info struct (used in "Case" smart contract)
    struct EvidenceInfo {
        bytes evidenceHash;
        string evidenceName;
        string evidenceDesc;
        address creator;
        string dateCreated;
        address[] transferChain;
        string[] transferDesc;
        string[] transferTime;
        bool deleted; //default false
    }
}

```