
**SCHOOL OF ARCHITECTURE, COMPUTING &
ENGINEERING**

BSc in Computer Science

**Πτυχιακή Εργασία με τίτλο:
Τεχνολογία Blockchain για Authentication**

Μπάντης Χρήστος

2121211

**Επιβλέπων καθηγητής:
Μπουράκης Ανδρέας**

Θεσσαλονίκη, 20 Μαΐου 2022

Πίνακας Περιεχομένων

Περίληψη	- 2 -
Abstract	- 3 -
Χρονοπρογραμματισμός Έργου	- 4 -
1. Εισαγωγή	- 5 -
2. To Blockchain	- 7 -
2.1. Η δομή των Blockchain	- 9 -
2.2. Μηχανισμός Συναίνεσης (Consensus Mechanism)	- 12 -
2.3. Ethereum Blockchain	- 13 -
2.4. Αποκεντρωμένες Εφαρμογές (Decentralized Applications)	- 14 -
2.5. Έξυπνα συμβόλαια (Smart Contracts)	- 16 -
3. Η ψηφιακή ταυτότητα	- 18 -
3.1. Μέθοδοι Ταυτοποίησης	- 20 -
3.2. Συστήματα Διαχείρισης Ταυτότητας	- 22 -
3.3. Ασφάλεια και Ιδιωτικότητα	- 24 -
3.4. Η χρήση της τεχνολογίας των Blockchain στην ταυτοποίηση	- 27 -
4. Παρουσίαση της εφαρμογής ταυτοποίησης «IDEN»	- 29 -
4.1. Υφιστάμενο πρόβλημα	- 30 -
4.2. Σχεδιασμός και Μοντελοποίηση	- 32 -
4.3. Μεθοδολογία	- 41 -
4.3.1. Αναφορές	- 43 -
4.4. Ανάλυση δομής	- 56 -
4.5. Τεχνικά μέρη της εφαρμογής	- 59 -
4.5.1. Οδηγός εγκατάστασης απαραίτητων εφαρμογών (Windows)	- 60 -
4.5.2 Οδηγός εκτέλεσης της εφαρμογής	- 78 -
4.6. Περιγραφή περίπτωσης χρήσης	- 87 -
4.7. Διαδικασία δοκιμών (Testing)	- 102 -
5. Συμπεράσματα	- 107 -
5.1. Μελλοντικές ενέργειες	- 108 -
6. Παράτημα	- 109 -
6.1. Βιβλιογραφικές Αναφορές	- 109 -
6.2. Κατάλογος Εικόνων	- 113 -
6.3. Κατάλογος Πινάκων	- 116 -
6.4. Γλωσσάριο απόδοσης ξενόγλωσσων όρων	- 116 -

Περίληψη

Πλήθος δημοσίων και μη υπηρεσιών είναι πλέον διαθέσιμο σε ψηφιακή μορφή, τίθοντάς τες προσβάσιμες σε όλους τους πολίτες μέσω των έξυπνων συσκευών τους. Η ψηφιοποίηση των υπηρεσιών οδήγησε στην αύξηση του ρυθμού ανάπτυξης σχετικών εφαρμογών, οι οποίες συχνά χαρακτηρίζονται από το μικρό κόστος τους, που συνεπάγεται με ένα σύστημα ευάλωτο σε σφάλματα και απειλές. Οι υπηρεσίες που, μέχρι πρότινος, προσφέρουν οι πάροχοι, κάνουν χρήση της δομής AAA (Authentication, Authorization and Accounting Framework), που απευθύνεται στον έλεγχο ταυτότητας, την εξουσιοδότηση και την λογιστική και βασίζεται στο Μοντέλο Πελάτη - Εξυπηρετητή (Client - Server Model) (Vishnia and Peters, 2020). Κύριο γνώρισμα, αλλά και ευπάθεια του μοντέλου αυτού αποτελεί το γεγονός πως οι πάροχοι υπηρεσιών διατηρούν τον πλήρη έλεγχο των δεδομένων των πολιτών που επεξεργάζονται και κατά συνέπεια, αποτελούν συχνό στόχο κακόβουλων χρηστών. Η τεχνολογία του Blockchain, χάρη στις αρχές τις οποίες πρεσβεύει, ενδέχεται να επιφέρει σημαντικές αλλαγές στους τρόπους διαχείρισης των προσωπικών δεδομένων, αλλά και στον τρόπο λειτουργίας ολόκληρου του διαδικτύου, προσδίδοντας του έναν πιο αποκεντρωμένο χαρακτήρα. Παρόλο που υφίσταται στο χώρο εδώ και δεκαετίες, το Blockchain, απέκτησε τη φήμη του τα τελευταία χρόνια μέσω των κρυπτονομισμάτων (cryptocurrencies) και πιο συγκεκριμένα του Bitcoin, του πρώτου εξ αυτών. Ωστόσο, εξακολουθεί να βρίσκεται σε αρχικά στάδια ανάπτυξης. Μέσω της εκπόνησης της παρούσας πτυχιακής εργασίας, θα πραγματοποιηθεί εκτενής έρευνα στον ευρύτερο τομέα του Blockchain και της ψηφιακής ταυτότητας και θα αναπτυχθεί εφαρμογή που θα καθιστά εφικτή την αποκεντρωμένη ταυτοποίηση των πολιτών σε μια υπηρεσία μέσω Blockchain (Blockchain Authentication).

Λέξεις – Κλειδιά

Έξυπνες Συσκευές, Blockchain, Προσωπικά Δεδομένα, Διαδίκτυο, Κρυπτονομίσματα, Αποκεντρωμένη Ταυτοποίηση

Abstract

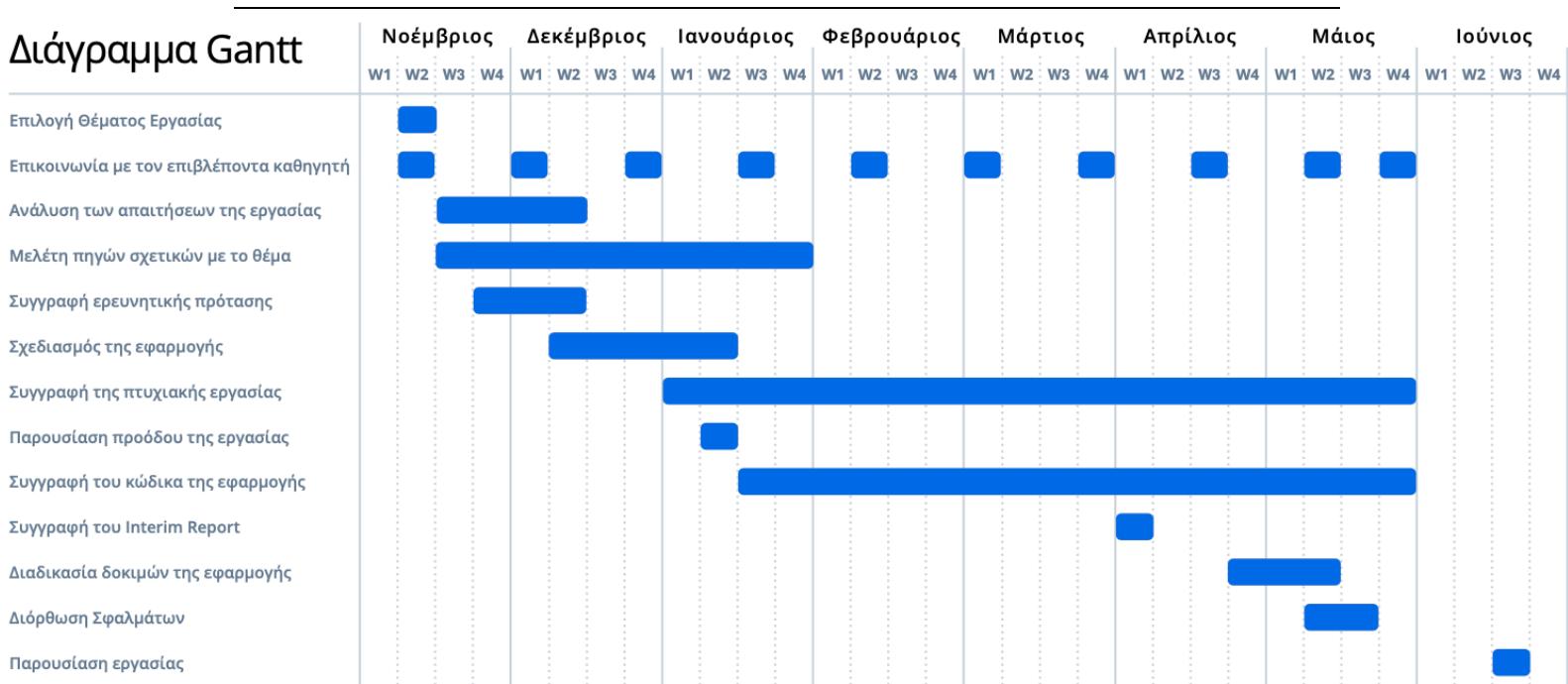
A multitude of public and non-public services are now available in digital form, making them accessible to all citizens through their smart devices. The digitization of services has led to an increase in the rate of development of relevant applications, which are often characterized by their low cost that comes with the downside of a system vulnerable to errors and threats. The services offered, until recently, by the providers, make use of the AAA (Authentication, Authorization and Accounting) Framework, which is based on the Client - Server Model (Vishnia and Peters, 2020). The main feature and vulnerability of this model is the fact that service providers maintain full control over the data of the citizens they process and are therefore a frequent target of malicious users. Blockchain technology, thanks to the principles it professes, may bring about significant changes in the ways personal data is managed, but also in the way the entire internet operates, giving it a more decentralized character. Although it has existed in the field for decades, Blockchain has gained its reputation in recent years through cryptocurrencies and more specifically Bitcoin, the first of them. However, it is still in the early stages of development. Through the elaboration of this thesis, an extensive research will be carried out in the wider field of Blockchain and digital identity and an application will be developed that will enable the decentralized identification of citizens in a Blockchain authentication service.

Keywords

Smart Devices, Blockchain, Personal Data, Internet, Cryptocurrencies, Decentralized Identification

Χρονοπρογραμματισμός Έργου

Διάγραμμα Gantt



Εικόνα 1 - Χρονοδιάγραμμα Gantt

Το παραπάνω χρονοδιάγραμμα «Gantt» παρουσιάζει την προβλεπόμενη χρονική έκταση του έργου, από την ανάθεση του θέματος, έως την παράδοσή του. Ο χρόνος μετράται σε εβδομάδες και ξεκινά την δεύτερη εβδομάδα του Νοεμβρίου, που πραγματοποιείται η επιλογή του θέματος της εργασίας. Η μέθοδος χρονικού διαμοιρασμού των δραστηριοτήτων αποσκοπεί στην αποδοτικότερη επιτέλεση του έργου. Παραδείγματος χάριν, η επικοινωνία με τον επιβλέποντα καθηγητή ορίστηκε να πραγματοποιείται κάθε τρεις εβδομάδες, ώστε να υπάρχουν επαρκή δεδομένα για παρουσίαση και ανατροφοδότηση. Αξίζει επίσης να αναφερθεί, πως για την ανάλυση των απαιτήσεων της εργασίας χρειάστηκε χρόνος ίσος με ένα μήνα, εξαιτίας της πολυπλοκότητας του θέματος. Η μελέτη των πηγών, που ξεκινά ταυτόχρονα με την ανάλυση των απαιτήσεων, διήρκησε οχτώ (8) εβδομάδες, καθώς προηγήθηκε έρευνα και αξιολόγηση του περιεχομένου τους. Ο χρόνος που αφιερώθηκε για τον σχεδιασμό της εφαρμογής δε ξεπέρασε τις πέντε (5) εβδομάδες, καθώς η απλότητα και συνάμα η χρηστικότητα της εφαρμογής αποτελούσαν βασικό κριτήριο για την υλοποίηση της. Τέλος, ο χρόνος που απέμεινε αφιερώθηκε στην συγγραφή της πτυχιακής εργασίας και του κώδικα της εφαρμογής. Στην τελευταία, συμπεριλαμβάνονται οι δοκιμές που υποβλήθηκε η εφαρμογή και η διόρθωση των σφαλμάτων που παρουσιάστηκαν, στις οποίες διατέθηκε αρκετός χρόνος ώστε να απαλειφθούν τυχόν ζητήματα και να καταστεί η εφαρμογή άρτια.

1. Εισαγωγή

Η ιστορία του Blockchain ξεκινά το 1991, όταν οι επιστήμονες Stuart Haber και W. Scott Stornetta παρουσίασαν μία τεχνολογία χρονοσήμανσης (timestamping) ψηφιοποιημένων αρχείων με σκοπό την επικύρωση της ακεραιότητας τους και την αποφυγή αλλοιώσεων των δεδομένων που περιείχαν. Η τεχνολογία αυτή αποτελείτο από ένα σύστημα που έκανε χρήση μιας κρυπτογραφημένης και, συνεπώς, ασφαλούς «αλυσίδας» (chain) συστοιχιών (blocks) στην οποία πραγματοποιούνταν αποθήκευση των αρχείων (Iredale, 2018).

Η τεχνολογία αυτή χρησιμοποιήθηκε, για πρώτη φορά, επτά (7) έτη αργότερα, το 1998, όταν ο πληροφορικός, και πρωτοπόρος στον τομέα του Blockchain, Nick Szabo παρουσίασε το «Bit Gold», τη πρώτη προσπάθεια δημιουργίας ενός αποκεντρωμένου ψηφιακού νομίσματος, το οποίο μέχρι και σήμερα θεωρείτο ο πρόγονος του Bitcoin (Hayes, 2022). Η ιδέα του BitGold όμως, δεν ευδοκίμησε, καθώς υπέκυψε σε μία σημαντική ευπάθεια του, γνωστή και ως «Double-Spending Problem», κατά την οποία οι κάτοχοι Bit Gold είχαν τη δυνατότητα να ξοδέψουν τον διπλάσιο αριθμό νομισμάτων από αυτόν που είχαν στην κατοχή τους. Έτσι, η εξέλιξη της τεχνολογίας του Blockchain έμεινε στάσιμη έως ότου, το 2008, ένας προγραμματιστής ή μία ομάδα προγραμματιστών υπό την επωνυμία «Satoshi Nakamoto» (η ταυτότητα του παραμένει άγνωστη μέχρι και σήμερα) παρουσίασε ένα έγγραφο που αφορούσε ένα νέο ψηφιακό νόμισμα, το Bitcoin, αντιμετωπίζοντας την αδυναμία του «προγόνου» του και κάνοντας ολοκληρωμένη χρήση της τεχνολογίας του Blockchain (Iredale, 2018).

Ως Blockchain ορίζεται η τεχνολογία κατά την οποία επαληθεύεται η κυριότητα πληροφοριών και δεδομένων που αφορούν τους τομείς της οικονομίας έχοντας όμως και πολιτικές, κοινωνικές και νομικές προεκτάσεις (Λογαράς, 2018). Βασικό χαρακτηριστικό της τεχνολογίας αυτής είναι, πως δημιουργείται μία συνεχής αλυσίδα δεδομένων, τα περιεχόμενα της οποίας αποθηκεύονται σε blocks, που είναι άρρηκτα συνδεδεμένα μεταξύ τους με χρονολογική σειρά. Μέσω του Bitcoin, η τεχνολογία του Blockchain αναπτύχθηκε σημαντικά και έγινε ευρέως γνωστή με αποτέλεσμα να χρησιμοποιείται με ολοένα και περισσότερους τρόπους (πχ. Μεταφορά Χρημάτων, Αποκεντρωμένες Εφαρμογές – Decentralized Applications, «Εξυπνα» συμβόλαια – Smart Contracts).

Στη σύγχρονη εποχή, που η χρήση του διαδικτύου αποτελεί βασικό κομμάτι της καθημερινότητας, δημιουργείται στους πολίτες η ανάγκη εξασφάλισης της προστασίας των προσωπικών τους δεδομένων. Η ταυτότητα, ίσως το σημαντικότερο από αυτά, αποτελεί τον ακρογωνιαίο λίθο της ανθρώπινης εξέλιξης και εμπλέκεται σε όλους τους τύπους συναλλαγών μεταξύ κράτους, πολιτών και οργανισμών-επιχειρήσεων, πράγμα που, σε συνδυασμό με τη μη ορθή χρήση του διαδικτύου, μπορεί να την μετατρέψει σε εργαλείο παρακολούθησης, καταπατώντας τις αρχές των ανθρωπίνων δικαιωμάτων. Τα παραπάνω αποτελούν την αφορμή που καθιστά αναγκαία την χρήση ενός νέου, ανθρωποκεντρικού προτύπου, στα συστήματα διαχείρισης ταυτότητας. Έτσι, κάθε πολίτης θα έχει ισχυρότερο έλεγχο της ταυτότητας του και σε μεγαλύτερο βαθμό, των προσωπικών του δεδομένων και θα δύναται να επιλέξει ο ίδιος ποιες οντότητες εμπιστεύεται, ώστε να δώσει πρόσβαση στα δεδομένα του. Η υλοποίηση ενός τέτοιου συστήματος προϋποθέτει την ύπαρξη ισχυρής κρυπτογραφικής τεχνολογίας, διαφάνειας και άμεσης προσβασιμότητας, χαρακτηριστικά που συναντώνται, μεταξύ άλλων, στη τεχνολογία του Blockchain. Καθ' ότι, όπως αναφέρει και ο Imran Bashir (2017) «Ο κώδικας του ηλεκτρονικού υπολογιστή γίνεται ο Νόμος».

Η παρούσα εργασία είναι κατανεμημένη σε κεφάλαια με τέτοιο τρόπο, ώστε να επιτευχθεί απόλυτη κατανόηση επί του θέματος, αναλύοντας όρους και τομείς όπως: η τεχνολογία του Blockchain και η «Ψηφιακή Ταυτότητα». Πιο συγκεκριμένα, εντός του επόμενου κεφαλαίου θα γίνει αναφορά στο Blockchain, στη δομή του, στο Ethereum Blockchain, στις Αποκεντρωμένες Εφαρμογές (Decentralized Applications) και στα Έξυπνα Συμβόλαια (Smart Contracts). Έπειτα, θα εξεταστούν τα στοιχεία της «Ψηφιακής Ταυτότητας», οι γνωστές μέθοδοι ταυτοποίησης, τα παρόντα συστήματα διαχείρισης ταυτότητας εν γένει, οι έννοιες της ασφάλειας και της ιδιωτικότητας και οι τρόποι με τους οποίους θα ωφεληθεί η ηλεκτρονική ταυτοποίηση από τις αρχές της τεχνολογίας του Blockchain. Τέλος, θα πραγματωθεί περιγραφή του πλάνου ανάπτυξης μιας πλήρως λειτουργικής αποκεντρωμένης εφαρμογής ταυτοποίησης μέσω Blockchain που αναπτύχθηκε για τις ανάγκες εκπόνησης της παρούσας πτυχιακής εργασίας, καθώς επίσης θα παρουσιαστεί η περίπτωση χρήσης στην οποία απευθύνεται η συγκεκριμένη υλοποίηση της εφαρμογής.

2. To Blockchain

Αρχικά, στην επιστήμη των υπολογιστών, ο όρος Blockchain αντιστοιχούσε σε μια μορφή δομής και διαμοιρασμού δεδομένων. Σύμφωνα με τα σημερινά δεδομένα, το Blockchain οποτελεί μια νέα προσέγγιση των κατανεμημένων βάσεων δεδομένων, οι οποίες ελέγχονται από ομάδες ατόμων και χρησιμοποιούνται για την αποθήκευση και τον διαμοιρασμό πληροφοριών. Πιο συγκεκριμένα, ως Blockchain ορίζεται μία δομή δεδομένων κατά την οποία καθίσταται δυνατή η δημιουργία ενός κοινόχρηστου, αμετάβλητου καθολικού (ledger) που διευκολύνει τη διαδικασία καταγραφής συναλλαγών και παρακολούθησης περιουσιακών στοιχείων (assets) σε ένα επιχειρηματικό δίκτυο (IBM, n.d.). Ένα περιουσιακό στοιχείο μπορεί να είναι από (σπίτι, αυτοκίνητο, μετρητά, γη) ή άνλο (πνευματική ιδιοκτησία, διπλώματα ευρεσιτεχνίας, πνευματικά δικαιώματα, επωνυμία). Σχεδόν οτιδήποτε αξίας μπορεί να εντοπιστεί και να αποτελέσει αντικείμενο διαπραγμάτευσης σε ένα Blockchain, μειώνοντας τον κίνδυνο και το κόστος για όλους τους εμπλεκόμενους (IBM, n.d.).

To Blockchain χωρίζεται σε τέσσερα είδη: τα Δημόσια (Public), τα Ελεγχόμενα (Permissioned), τα Ιδιωτικά (Private) και τα Κοινοπραξίας (Consortium):

- Τα δημόσια Blockchain, όπως αυτό του Bitcoin, είναι ευμεγέθη κατανεμημένα δίκτυα, ελεύθερα προς συμμετοχή για όλους, που απαιτείται η χρήση ενός εγγενούς διακριτικού (native token) για την λειτουργία τους και αποτελούνται από «ανοιχτού» τύπου κώδικα, ο οποίος διατηρείται από την αντίστοιχη κοινότητα. Αυτό το είδος Blockchain δεν ενδείκνυται για περιπτώσεις χρήσης επιχειρήσεων, καθώς χαρακτηρίζεται από την σημαντική υπολογιστική ισχύ που απαιτείται και την ελλιπή ιδιωτικότητα των συναλλαγών.
- Τα ελεγχόμενα Blockchain, όπως αυτό του Ripple, διαφέρουν εν μέρει από τα δημόσια, διότι στα συγκεκριμένα ελέγχονται οι ρόλοι των μονάδων που τα απαρτίζουν, αφού η συμμετοχή επιτρέπεται μόνο μετά πρόσκλησης. Ωστόσο, παραμένουν μεγάλα, κατανεμημένα συστήματα που η λειτουργία τους απαιτεί τη χρήση ενός εγγενούς διακριτικού. Όσον αφορά στον κώδικα τους, αυτός μπορεί να είναι είτε «ανοιχτού», είτε «κλειστού» τύπου.
- Τα ιδιωτικά Blockchain τείνουν να είναι μικρότερα από τα προαναφερθέντα και δεν κάνουν χρήση κάποιου διακριτικού. Διέπονται, συνήθως, από έναν οργανισμό ο οποίος ελέγχει ποιος θα συμμετάσχει και θα διατηρήσει το

καθολικό, ενισχύοντας έτσι την εμπιστοσύνη και την εμπιστευτικότητα μεταξύ των συμμετεχόντων. Ένα ιδιωτικό Blockchain μπορεί να λειτουργήσει πίσω από ένα εταιρικό τείχος προστασίας, ακόμη και να φιλοξενηθεί στις εγκαταστάσεις της εκάστοτε εταιρείας.

- Τα Blockchain κοινοπραξίας αποτελούνται από έναν αριθμό οργανισμών, οι οποίοι μοιράζονται τις ευθύνες διατήρησης των Blockchain. Αυτοί οι προεπιλεγέντες οργανισμοί καθορίζουν τις άδειες υποβολής συναλλαγών και πρόσβασης δεδομένων. Τέτοιου είδους Blockchain θεωρούνται ιδανικά για επιχειρήσεις που έχουν αξιόπιστα μέλη και επεξεργάζονται εμπιστευτικές πληροφορίες.

Καθένα από τα παραπάνω είδη, εκμεταλλευόμενα τα ισχυρά επίπεδα κρυπτογράφησης τους, όπως επίσης και την ασύμμετρη κρυπτογράφηση δημόσιου-ιδιωτικού κλειδιού, επιτρέπουν την ασφαλή διαχείριση του καθολικού από τους συμμετέχοντες, χωρίς την παρουσία κεντρικής αρχής για την επιβολή κανόνων. Η απομάκρυνση της κεντρικής αρχής από την επικρατούσα δομή των βάσεων δεδομένων αποτελεί μία από τις σημαντικότερες αλλαγές που επιφέρει η τεχνολογία του Blockchain (Laurence, 2017).

Το Blockchain πλέον, αποκαλείται ως η «πέμπτη εξέλιξη» της πληροφορικής ή αλλιώς «το χαμένο επίπεδο εμπιστοσύνης του διαδικτύου» (Laurence, 2017). Αποτελεί την ιδανική λύση για οργανισμούς που δεν έχουν την δυνατότητα να υποστούν ούτε ένα σημείο αποτυχίας, καθώς καθιστά πρακτικά αδύνατη την διακύβευση ευαίσθητων πληροφοριών από κακόβουλους χρήστες και εγκληματίες του κυβερνοχώρου.

Decentralized Ledger



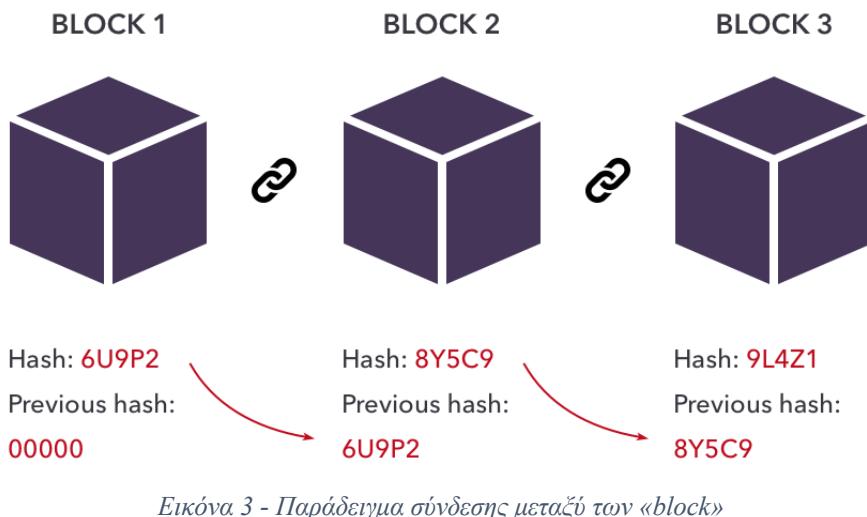
Eικόνα 2 - Αναπαράσταση ενός δικτύου Blockchain (CB Insights Research, 2018)

2.1. Η δομή του Blockchain

Η τεχνολογία του Blockchain δεν είναι κάτι νέο στην επιστήμη της πληροφορικής, καθώς βασίζεται σε μία ομάδα υφιστάμενων τεχνολογιών που χρησιμοποιούνται ευρέως σε ολόκληρο τον κλάδο. Ειδικότερα, το Blockchain είναι ένα ομότιμο (peer-to-peer) δίκτυο, δομημένο από blocks, τα οποία αποτελούν κατανεμημένα καθολικά (distributed ledgers) που περιέχουν τις καταγεγραμμένες συναλλαγές που έλαβαν μέρος μια ορισμένη χρονική στιγμή και ενημερώνονται από κάθε συμμετέχοντα στο Blockchain (Gupta, 2018). Έπειτα, τα blocks συνδέονται μεταξύ τους (chaining) μέσω μιας κρυπτογραφικής μαθηματικής παράστασης (hash). Αυτή η μαθηματική παράσταση είναι σχεδιασμένη με στόχο την προστασία της ακεραιότητας των δεδομένων, αφού κάθε νέο block περιέχει το «hash» του προηγούμενου και κατ' αυτό τον τρόπο κάνει άμεσα αντιληπτή την τροποποίηση ήδη καταχωρημένων δεδομένων. Τέλος, συγκροτείται από ένα δίκτυο ανεξάρτητων υπολογιστών που ονομάζονται «κόμβοι» (nodes) οι οποίοι διαχειρίζονται όλες τις συναλλαγές που λαμβάνουν χώρα εντός του Blockchain.

Αναλυτικότερα, ένα block είναι μια ενιαία μονάδα στο Blockchain που έχει τη μορφή δομής δεδομένων και απαρτίζεται από μεταδεδομένα (meta-data). Ένας miner (σε ελεύθερη μετάφραση «μεταλλωρύχος») συλλέγει τις έγκυρες συναλλαγές που καταγράφηκαν σε ένα συγκεκριμένο χρονικό διάστημα και σε συνδυασμό με το hash του προηγούμενου block, υπολογίζει το νέο hash που εξάγεται. Ωστόσο, το κάθε hash έχει μια αποκλειστική μορφή, για τον υπολογισμό της οποίας ο miner, έπειτα από συνεχείς προσπάθειες, πρέπει να ανακαλύψει έναν αυθαίρετο αριθμό που της αντιστοιχεί. Αυτός ο αριθμός αποκαλείται number used once ή number once (nonce) και διαχωρίζει τα blocks σε «signed» (υπογεγραμμένα - αυτά που έχουν nonce) και «unsigned» (ανυπόγραφα - αυτά που δεν έχουν nonce). Η διαδικασία ανακάλυψης του nonce ονομάζεται «Mining» (Εξόρυξη) (Shackelford and Myers, 2016).

Εάν πραγματοποιηθεί οποιαδήποτε παραποίηση στα δεδομένα ενός προϋπάρχοντος block, τα «hash» των επόμενων block, που συνδέονται διαδοχικά με αυτό, θα αλλάξουν, συνεπώς θα δημιουργηθεί ένα αμετάβλητο αρχείο καταγραφής που θα ενημερώνει τους συμμετέχοντες του Blockchain για το συμβάν. Δεδομένου αυτού, ένα προς ένα τα «hash» των block «οδηγούν» στο πρώτο εξ αυτών υπό την ονομασία «Genesis Block».



Όσον αφορά τη κρυπτογραφική συνάρτηση που δημιουργεί την μαθηματική παράσταση (hash), αποτελεί τον τρόπο εξαγωγής μιας αλφαριθμητικής ακολουθίας σταθερού μήκους από μία οποιουδήποτε δεδομένου μήκους συμβολοσειρά. Αυτή η ακολουθία που, εκτός από «hash», έχει την ονομασία «Message Digest», δεν μπορεί να αντιστραφεί ώστε να ληφθούν τα δεδομένα εισόδου και επομένως, μπορεί να χρησιμοποιηθεί για τον έλεγχο της ακεραιότητας των δεδομένων (Gauravaram, McCullagh and Dawson, 2006). Το «hash» που παράγεται από ένα σύνολο δεδομένων είναι πάντα το ίδιο, όσες φορές κι αν υπολογιστεί εκ νέου, ενώ μία μικρή αλλαγή έχει ως συνέπεια ένα παντελώς διαφορετικό αποτέλεσμα. Ως εκ τούτου, η κρυπτογραφική συνάρτηση είναι επίσης γνωστή με τον χαρακτηρισμό «One-way hash function» (Μονόδρομη κρυπτογραφική συνάρτηση).

Ένα «hash» έχει τρεις κύριες ιδιότητες: «άνευ σύγκρουσης» (collision free), απόκρυψη (hiding) και «φιλικό προς τα παζλ» (puzzle friendly). Άνευ σύγκρουσης σημαίνει, πως είναι εξαιρετικά απίθανο να βρεθούν δύο διαφορετικά δεδομένα εισόδου που έχουν το ίδιο hash. Παραδείγματος χάριν, το hash μιας συμβολοσειράς «x» και το hash μιας συμβολοσειράς «y» είναι πάντα διαφορετικά, παρά τον αριθμό των επανυπολογισμών. Με την ιδιότητα της απόκρυψης καθίσταται ανέφικτη η μετατροπή του hash στην αρχική του μορφή, δηλαδή στα δεδομένα εισόδου και η φράση «φιλικό προς τα παζλ» αντιπροσωπεύει την ευκολία υπολογισμού ενός hash δοθέντων δεδομένων (Treiblmaier, 2019).

Υπάρχουν διάφοροι τρόποι υπολογισμού ενός hash. Στον κόσμο των κρυπτονομισμάτων, με το Bitcoin να είναι ένα δημοφιλές παράδειγμα, ο αλγόριθμος

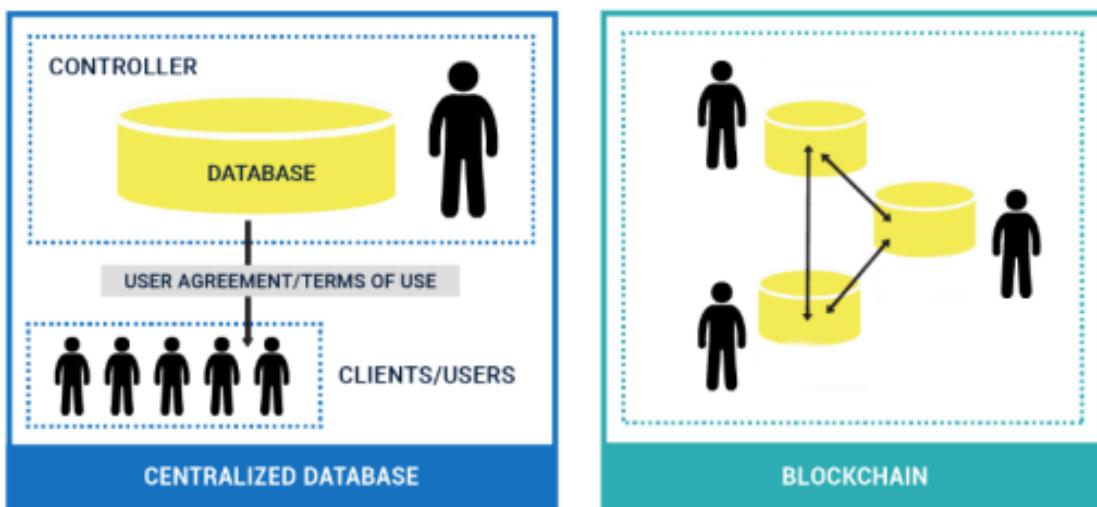
SHA-256 χρησιμοποιείται για την παραγωγή ενός 256-bit hash σταθερού μήκους σε κάθε μπλοκ.

Αξιο αναφοράς, επίσης, είναι το δέντρο κατακερματισμού ή αλλιώς «Merkle Tree». Ένα Merkle Tree είναι ένα δυαδικό δέντρο (binary tree), αποτελούμενο από δείκτες κατακερματισμού (hash pointers), το οποίο εξασφαλίζει πως κάθε κόμβος πρέπει να έχει τα ίδια, μη κατεστραμμένα, αναλλοίωτα και έγκυρα δεδομένα. Εάν υπάρξει τροποποίηση των δεδομένων σε έναν κόμβο, τότε οι αλλαγές πρέπει να μεταδοθούν στους υπόλοιπους. Το Merkle Tree συνίσταται από blocks που περιέχουν συναλλαγές και τοποθετούνται, σε ομάδες των δύο, στα φύλλα (leaves) του δέντρου. Κάθε ομάδα από block διαθέτει δείκτες κατακερματισμού, ο συνδυασμός των οποίων αντιστοιχεί στο επόμενο (κοντινότερο στη ρίζα) επίπεδο του δέντρου. Αυτή η διαδικασία επαναλαμβάνεται μέχρι να δημιουργηθεί ένα ενιαίο μπλοκ το οποίο ονομάζεται κατακερματισμός ρίζας (root hash) ή ρίζα του δέντρου (Jal, 2018).

Στα peer-to-peer δίκτυα, η επαλήθευση των δεδομένων κρίνεται χρονοβόρα και υπολογιστικά δαπανηρή. Με τη χρήση ενός Merkle Tree, στη θέση των δεδομένων, αποστέλλεται στον παραλήπτη μόνο το hash τους, ο οποίος εν συνεχείᾳ, το ελέγχει βασιζόμενος στη ρίζα του δέντρου. Κατ' αυτόν τον τρόπο, επιτρέπεται η ασφαλής και αποτελεσματική επαλήθευση μεγαλύτερων δομών δεδομένων, καθώς και η διασφάλιση της ακεραιότητας τους.

Εν κατακλείδι, στο μοντέλο πελάτη-εξυπηρετητή (client-server), που συναντάται σε πληθώρα εφαρμογών στο διαδίκτυο, τα δεδομένα των χρηστών αποθηκεύονται σε κεντρικούς (centralized) διακομιστές και βρίσκονται υπό τον αποκλειστικό έλεγχο των διαχειριστών τους, με αποτέλεσμα την τροποποίηση ή την διαγραφή των βάσεων δεδομένων, αν η ασφάλεια των διαχειριστών παραβιαστεί.

Στα ομότιμα δίκτυα, και κατά συνέπεια στο Blockchain, οι κόμβοι παρέχουν ένα μέρος των πόρων τους, όπως ένα ποσοστό της επεξεργαστικής τους ισχύος ή του χώρου αποθήκευσής τους, οι οποίοι είναι άμεσα διαθέσιμοι σε όλους τους συμμετέχοντες χωρίς την ανάγκη ύπαρξης ενός κεντρικού διακομιστή. Σε αντίθεση με τις προαναφερθείσες βάσεις δεδομένων, όλοι οι κόμβοι ενός Blockchain διατηρούν ένα αντίγραφο των δεδομένων, με αποτέλεσμα οι πληροφορίες να παραμείνουν διαθέσιμες, ακόμη και αν κάποιοι κόμβοι τεθούν εκτός λειτουργίας.



Εικόνα 4 - Σύγκριση μεταξύ συγκεντρωτικής (centralized) βάσης δεδομένων και Blockchain

2.2. Μηχανισμός Συναίνεσης (Consensus Mechanism)

Η δημοφιλία της τεχνολογίας τους Blockchain προέρχεται από τη δημιουργία του Bitcoin. Απόρροια της ραγδαίας αυτής ανάπτυξης είναι η απόδειξη, πως ένα σύνολο, αγνώστων μεταξύ τους, ατόμων μπορούσε να δραστηριοποιηθεί στο διαδίκτυο, σε ένα σύστημα που απευασθητοποιούσε τους συμμετέχοντες για θέματα εξαπάτησης ανάμεσα τους. Στον κόσμο του Blockchain, η συναίνεση είναι η διαδικασία ανάπτυξης μιας συμφωνίας μεταξύ μιας ομάδας ατόμων, συνήθως διακατεχόμενης από δυσπιστία, προκειμένου να διασφαλιστεί ότι όλα έχουν εξεταστεί πριν από την έναρξη της πραγματικής τους επικοινωνίας. Καθώς ο καθένας μπορεί να συμμετάσχει και να υποβάλει πληροφορίες, η αξιολόγηση των σκοπών του καθενός και η ομόφωνη απόφαση για μία επιθυμητή πολιτική αποτελούν επωφελείς τακτικές για την αποφυγή τυχόν προσπαθειών απάτης.

Κάθε Blockchain έχει τους δικούς του αλγορίθμους για τη δημιουργία συμφωνίας εντός του δικτύου του σχετικά με τις καταχωρήσεις που προστίθενται σε αυτό. Υπάρχουν διάφορα μοντέλα για δημιουργία συναίνεσης, διότι κάθε Blockchain χρησιμοποιείται για διαφορετικούς σκοπούς. Ορισμένα δραστηριοποιούνται με την συναλλαγή εμπορικής αξίας, άλλα διατίθενται για αποθήκευση δεδομένων και άλλα εντρυφούν στην ασφάλεια συστημάτων και συμβολαίων. Η αναμενόμενη απειλή και ο βαθμός εμπιστοσύνης που διαθέτει το δίκτυο στους κόμβους που συντρέχουν στη λειτουργεία του Blockchain, θα καθορίσουν τον τύπο του αλγόριθμου συναίνεσης που θα καταφύγουν για να διευθετήσουν το καθολικό τους. Επί παραδείγματι, το Bitcoin και το Ethereum υφίστανται απειλές υψηλού βαθμού επικινδυνότητας, επομένως

κάνουν χρήση ενός ισχυρού αλγορίθμου συναίνεσης που ονομάζεται Proof of Work (PoW). Μερικοί ακόμη αλγόριθμοι είναι οι: Proof of Stake (PoS), Delegated Proof of Stake (DPoS) και Proof of Burn (PoB).

Οι αλγόριθμοι συναίνεσης λόγουν το πρόβλημα του «Βυζαντινού Στρατηγού» (Byzantine Generals' Problem - Byzantine fault): «Πώς γνωρίζουμε ότι οι πληροφορίες που εξετάζουμε δεν έχουν αλλάξει εσωτερικά ή εξωτερικά;». Εξαιτίας της ανθρώπινης παρέμβασης στον χειρισμό των δεδομένων να είναι σχεδόν πάντα εφικτή, η αξιοπιστία τους αποτελεί ένα μεγάλο πρόβλημα για την επιστήμη των υπολογιστών.

2.3. Ethereum Blockchain

Το Ethereum είναι ένα από τα πιο ανεπτυγμένα και προσβάσιμα Blockchain στο οικοσύστημα. Θεωρείται ο «ηγέτης» του κλάδου στην καινοτομία και τις περιπτώσεις χρήσης της τεχνολογίας του Blockchain. Η κατανόηση αυτής της τεχνολογίας είναι σημαντική, διότι προπορεύεται στους τομείς των έξυπνων συμβολαίων (Smart Contracts) και των αποκεντρωμένων αυτόνομων οργανισμών (Decentralized Autonomous Organizations – DAOs).

Το Ethereum ίσως να είναι ένα από τα πιο σύνθετα Blockchain που κατασκευάστηκαν ποτέ. Διατηρεί την «παραδοσιακή» δομή ενός Blockchain ωστόσο, προσθέτει στον πυρήνα της μία «Turing-Complete» γλώσσα προγραμματισμού (πλήρης γλώσσα που επιτρέπει στους προγραμματιστές να λύσουν οποιοδήποτε υπολογιστικό πρόβλημα) και την «Εικονική Μηχανή Ethereum» (Ethereum Virtual Machine – EVM), που εξειδικεύεται στην εκτέλεση του κώδικα των έξυπνων συμβολαίων. Το πρωτόκολλο Ethereum μπορεί να ανταπεξέλθει σχεδόν σε οποιοδήποτε ζήτημα τεθεί στον μέσο όρο των γνωστών γλωσσών προγραμματισμού, με τη διαφοροποίηση πως συνοδεύεται από τα οφέλη και την ασφάλεια του Blockchain λόγω της ενσωμάτωσης του σε αυτό (Laurence, 2017).

Το πρωτόκολλο Ethereum έχει θεμελιώσει ένα εντελώς νέο είδος εφαρμογών, σύμφωνα με το οποίο οποιαδήποτε κυβέρνηση, επιχείρηση ή οργανισμός έχει τη δυνατότητα να αποκτήσει υπόσταση εντός του Ethereum. Επί του παρόντος, η πλατφόρμα του Ethereum διερευνάται για τη διαχείριση ψηφιακών περιουσιακών στοιχείων (μια νέα κατηγορία διαδικτυακών περιουσιακών στοιχείων που μπορεί να αντιπροσωπεύει ένα ολόκληρο ψηφιακό περιουσιακό στοιχείο, όπως ένα νόμισμα Bitcoin ή μια ψηφιακή αντιπροσώπευση ενός περιουσιακού στοιχείου του πραγματικού

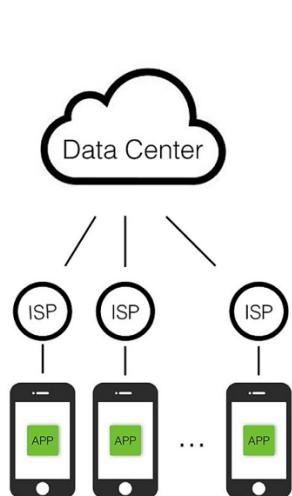
κόσμου, όπως ένα έργο τέχνης), χρηματοπιστωτικά μέσα (όπως χρεόγραφα που υποστηρίζονται από ενυπόθηκα δάνεια), καταγραφή της ιδιοκτησίας περιουσιακών στοιχείων, όπως γη και αποκεντρωμένων αυτόνομων οργανισμών (DAOs), ένα νέο τρόπο οργάνωσης μιας επιχείρησης, μη κερδοσκοπικού οργανισμού, κυβέρνησης ή οποιουδήποτε άλλου φορέα που χρειάζεται να καταλήξει σε συμφωνία και να συνεργαστεί για κοινό συμφέρον. Τέλος, χρησιμοποιείται επίσης για την ασφάλεια εφαρμογών Blockchain αλλά και μικρότερων Blockchain δικτύων (Laurence, 2017).

2.4. Αποκεντρωμένες Εφαρμογές (Decentralized Applications)

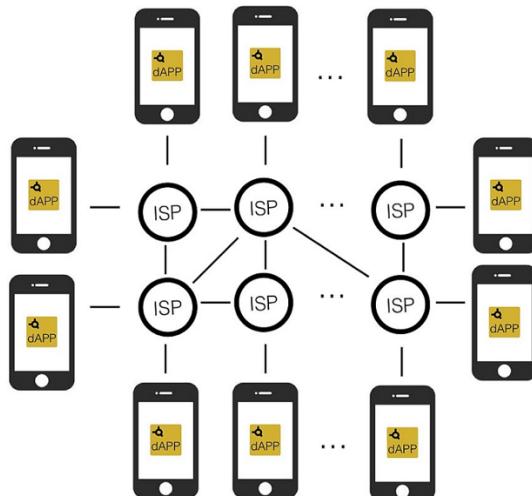
Οι αποκεντρωμένες εφαρμογές (Decentralized Applications - dApps) είναι ψηφιακές εφαρμογές ή προγράμματα που υπάρχουν και εκτελούνται σε ένα Blockchain, εν αντιθέσει με τις «παραδοσιακές» εφαρμογές που εκτελούνται σε έναν υπολογιστή-διακομιστή. Τα dApps βρίσκονται εκτός της δικαιοδοσίας και του ελέγχου μιας ενιαίας αρχής και χρησιμοποιούν «έξυπνα» συμβόλαια (smart contracts) για τη «λογική» τους (Frankenfield, 2021).

Μια κεντρική εφαρμογή ανήκει σε μία μόνο εταιρεία, ενώ το λογισμικό της βρίσκεται σε έναν ή περισσότερους διακομιστές που ελέγχονται από την ίδια. Η αλληλεπίδραση του χρήστη με την εφαρμογή επιτυγχάνεται με την αποστολή και τη λήψη δεδομένων από και προς τον διακομιστή της εταιρείας. Μόλις τα δεδομένα αποθηκευτούν στον διακομιστή, ο χρήστης αποστερείται του δικαιώματος του ελέγχου τους και δεν έχει πρόσβαση σε πληροφορίες σχετικά με τον τρόπο αποθήκευσης τους, ποια μέτρα πρόληψης ασφαλείας έχουν ληφθεί, ποιος μπορεί να τα διαβάσει και ούτω καθεξής. Στον αντίποδα, μια αποκεντρωμένη εφαρμογή εκτελείται σε ένα Blockchain και επιτρέπει στους χρήστες να προβαίνουν σε απευθείας συναλλαγές μεταξύ τους, αποφεύγοντας την εξάρτηση από μία οντότητα για την αποθήκευση και διαχείριση των προσωπικών και επιχειρηματικών τους δεδομένων, αποκτώντας τον πλήρη έλεγχο τους (Εικόνα 5). Ως επακόλουθο, διασφαλίζονται η ιδιωτικότητα των χρηστών και η έλλειψη λογοκρισίας.

Apps



dApps



Εικόνα 5 - Γραφική αναπαράσταση και σύγκριση των κεντρικών (centralized) και των αποκεντρωμένων (decentralized) εφαρμογών (Ray, 2021)

Το Ethereum είναι μια ευέλικτη πλατφόρμα δημιουργίας αποκεντρωμένων εφαρμογών, παρέχοντας την υποδομή που απαιτείται στους προγραμματιστές ώστε να εστιάσουν τις προσπάθειές τους στην εξεύρεση καινοτόμων χρήσεων των εφαρμογών. Έτσι, διευκολύνεται η ταχεία ανάπτυξη των dApps σε διάφορους κλάδους, συμπεριλαμβανομένων των τραπεζικών και χρηματοοικονομικών, των παιχνιδιών, των μέσων κοινωνικής δικτύωσης και των διαδικτυακών αγορών (Frankenfield, 2021).

Τα dApps, κατά κύριο λόγο, χρησιμοποιούν τη γλώσσα προγραμματισμού «Javascript» ως διεπαφή με έναν κόμβο στο Blockchain του Ethereum, με τον οποίο ακολούθως, επικοινωνούν μέσω ενός έξυπνου συμβολαίου. Επίσης, παρέχουν ένα περιβάλλον χρήστη με σκοπό την διευκόλυνση της διαχείρισης των συνδέσεων σε αυτές (Rajneesh Gupta, 2018).

Αξιοπρόσεκτη είναι η συντήρηση μιας αποκεντρωμένης εφαρμογής. Μόλις αναπτυχθεί, ένα dApp πιθανότατα θα χρειαστεί συνεχείς αλλαγές για σκοπούς βελτιστοποίησης ή για τη διόρθωση σφαλμάτων ή κινδύνων ασφαλείας. Σύμφωνα με το Ethereum, η ενημέρωση των dApp αποτελεί ένα δυσεπίλυτο πρόβλημα για τους προγραμματιστές, διότι τα δεδομένα και ο κώδικας που δημοσιεύονται στο Blockchain είναι δύσκολο να τροποποιηθούν.

2.5. Έξυπνα συμβόλαια (Smart Contracts)

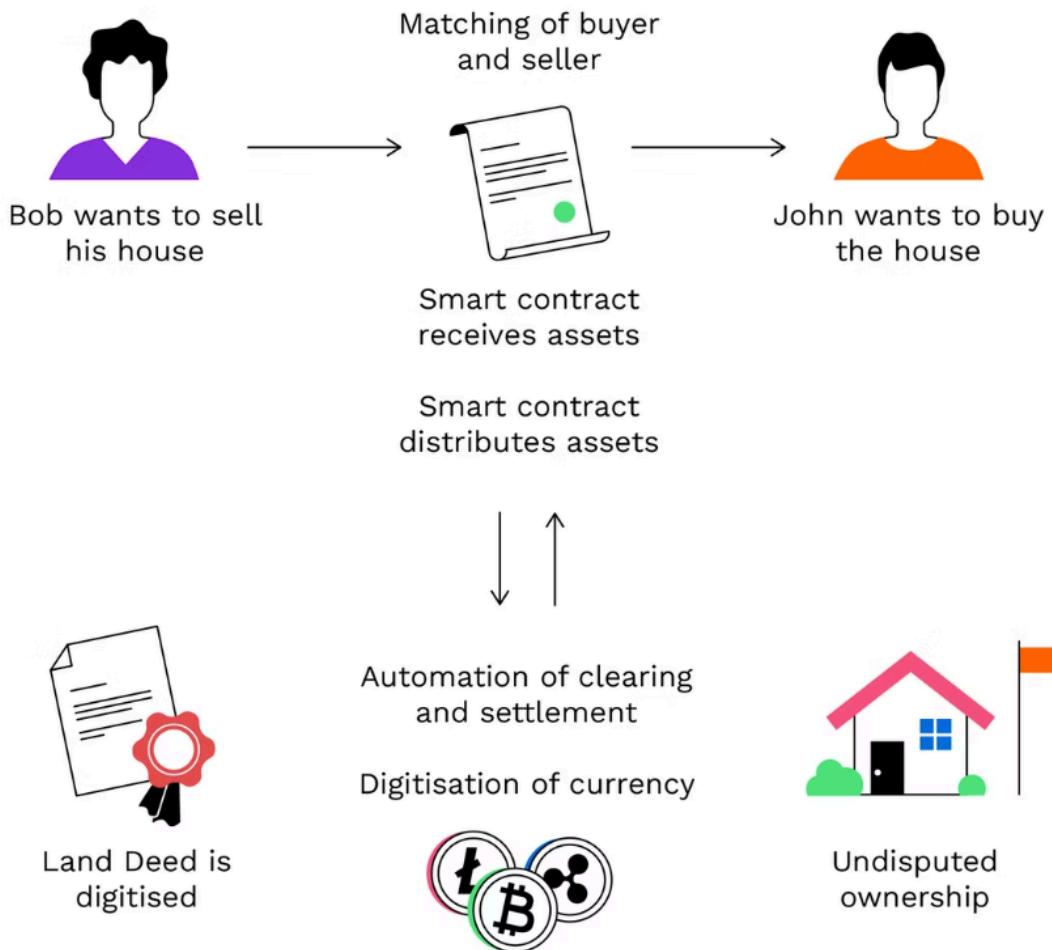
Τα έξυπνα συμβόλαια αποτελούν προγράμματα αποθηκευμένα σε μια αλυσίδα μπλοκ που εκτελούνται όταν πληρούνται προκαθορισμένες προϋποθέσεις. Συνήθως χρησιμοποιούνται για την αυτοματοποίηση της εκτέλεσης μιας συμφωνίας, έτσι ώστε όλοι οι συμμετέχοντες να μπορούν να είναι άμεσα βέβαιοι για το αποτέλεσμα, χωρίς τη συμμετοχή ή την απώλεια χρόνου από οποιονδήποτε μεσάζοντα. Μπορούν επίσης να αυτοματοποιήσουν μια ροή εργασίας, μεταβαίνοντας στην επόμενη ενέργεια όταν πληρούνται οι προϋποθέσεις (IBM, 2022). Ήδη από το 1990, ο Nick Szabo περιέγραψε τα συμβόλαια αυτά ως «ένα πρωτόκολλο υπολογιστικής συναλλαγής που εκτελεί τους όρους μιας σύμβασης-συμφωνίας». Γίνεται, επομένως, αντιληπτό ότι αυτού του τύπου τα συμβόλαια χαρακτηρίζονται από τρεις ιδιαιτερότητες: την αυτόματη εκτελεστικότητα, την δυνατότητα αυτοεπικύρωσης και την δυνατότητα να είναι κατανοητά, ασφαλή και αδιάληπτα (Bashir, 2017).

Παρά το γεγονός πως μπορούν να προγραμματιστούν για οποιονδήποτε υποστηριζόμενο τύπο Blockchain, το Ethereum είναι η ευρέως προτιμώμενη επιλογή, καθώς παρέχει δυνατότητες επεκτασιμότητας της επεξεργασίας. Στο Ethereum, κάθε συμβόλαιο αποκτά μια μοναδική διεύθυνση, για να μπορεί να ταυτοποιηθεί. Αυτή η διεύθυνση υπολογίζεται κατακερματίζοντας (hashing) τη διεύθυνση του δημιουργού του στο Blockchain και τον αριθμό των συναλλαγών που έχουν εκτελεστεί.

Η αποθήκευση δεδομένων σε ένα Blockchain χαρακτηρίζεται από την αμεταβλητότητα που παρουσιάζει, εντούτοις δεν ισχύει το ίδιο και για τα έξυπνα συμβόλαια. Κάθε έξυπνο συμβόλαιο που εκτελείται στο Ethereum διατηρεί τον δικό του μεταβλητό «χώρο» αποθήκευσης. Αυτός ο «χώρος» αποθήκευσης μπορεί να θεωρηθεί ως μια ευμεγέθης συστοιχία, αρχικά αποτελούμενη από μηδενικά. Κάθε τιμή στη συστοιχία έχει πλάτος 32 byte και υπάρχουν συνολικά 2^{256} τέτοιες τιμές. Ένα έξυπνο συμβόλαιο μπορεί να «διαβάσει» ή να «γράψει» σε μια τιμή που βρίσκεται σε οποιαδήποτε τοποθεσία του «χώρου» αποθήκευσης του (Marx , 2018).

Μέχρι στιγμής, τα έξυπνα συμβόλαια έχουν επεκταθεί σε πληθώρα τομέων. Η δυνατότητα έκδοσης και ελέγχου ψηφιακής ταυτότητας, η διεθνής μεταφορά αγαθών μέσω πιστωτικών μηχανισμών και η απλούστευση των διαδικασιών χωρίς περαιτέρω κόστος, η σαφήνεια στα χρηματοπιστωτικά συστήματα και τις συναλλαγές, καθώς και η αποδοτικότητα της σύνδεσης μεταξύ των μερών που τις απαρτίζουν είναι μερικές

από τις περιπτώσεις χρήσης που εξετάζονται πλέον, σε παγκόσμιο επίπεδο (Chamber of Digital Commerce, 2016).



Εικόνα 6 - Γραφική αναπαράσταση περίπτωσης χρήσης ενός «έξυπνου» συμβολαίου (Bitpanda, n.d.)

3. Η ψηφιακή ταυτότητα

Ως φυσική επέκταση του ορισμού της ταυτότητας, η ψηφιακή ταυτότητα χαρακτηρίζεται ότι είναι πεπερασμένο σύνολο χαρακτηριστικών που επιτρέπει σε ένα ατόμο, ένα ζώο, ένα πρόγμα ή μια διαδικασία να είναι μοναδικά αναγνωρίσιμα και η γνησιότητα τους να πιστοποιείται ηλεκτρονικά σε τρίτους (Allende López, 2020). Κάθε ψηφιακή ταυτότητα αντιπροσωπεύεται από ένα ή περισσότερα αναγνωριστικά στοιχεία και ένα σύνολο χαρακτηριστικών που είναι μοναδικά εντός ενός καθορισμένου περιβάλλοντος.

Η απόδειξη της ψηφιακής ταυτότητας ενός ατόμου αντιμετωπίζει αρκετές προκλήσεις. Λόγου χάριν, η επαλήθευση της ταυτότητας δεν εφαρμόζεται πλέον με την μορφή που ισχύει για τις φυσικές μορφές ταυτότητας. Ωστόσο, παρουσιάζει επίσης πολλά πλεονεκτήματα, καθώς προσφέρει πρόσβαση σε παγκόσμιες ψηφιακές υπηρεσίες χωρίς την ανάγκη φυσικής παρουσίας ή φυσικής μορφής ταυτότητας. Αυτό ωφελεί στην αλληλεπίδραση με ένα πλήθος δυνατοτήτων, επιτρέποντας την απομακρυσμένη παροχή υπηρεσιών, που υπό άλλες συνθήκες θεωρούνται απρόσιτες, σε πραγματικό χρόνο σε κοινότητες και πληθυσμούς με περιορισμένη εκ του σύνεγγυς πρόσβαση (Allende López, 2020).

Οι ψηφιακές ταυτότητες δημιουργούνται και χρησιμοποιούνται ως μέρος ενός κύκλου ζωής που περιλαμβάνει τέσσερα θεμελιώδη στάδια: α) εγγραφή, συμπεριλαμβανομένης της επικύρωσης, β) έκδοση εγγράφων ή διαπιστευτηρίων, γ) έλεγχος ταυτότητας και δ) ταυτοποίηση για διάθεση υπηρεσιών ή συναλλαγών (World Bank, 2018a).



Εικόνα 7 - Παραδείγματα ψηφιακής ταυτότητας σε τρεις διαφορετικές περιπτώσεις (Allende López, 2020)

Η ψηφιακή ταυτότητα δίνει τη δυνατότητα στον καθένα ξεχωριστά να παραμερίζει τους περιορισμούς του πραγματικού κόσμου, διευκολύνει την αμεσότητα και την αξιοπιστία των συνδέσεων και των συναλλαγών, όπως επίσης και την παροχή ψηφιακών υπηρεσιών. Σε μία πραγματικότητα που όλα ψηφιοποιούνται μέρα με τη μέρα, η ύπαρξη ισχυρών, χρήσιμων και κλιμακούμενων συστημάτων διαχείρισης ψηφιακής ταυτότητας κρίνεται ζωτικής σημασίας για την ηλεκτρονική ταυτοποίηση και την επίγνωση την ταυτότητας του τελικού αποδέκτη των κοινοποιηθέντων δεδομένων. Είναι σαφές πως λόγω αυτού, κάθε άτομο άρχει των δεδομένων του και κατά συνέπεια αποφασίζει με ποιον θα τα μοιραστεί και για ποιον σκοπό.

Σύμφωνα με το McKinsey (2019), «ένα πρότυπο ψηφιακής ταυτότητας είναι επαληθευμένο και πιστοποιημένο με υψηλό βαθμό διασφάλισης, μοναδικό, με ατομική συναίνεση, προστασία της ιδιωτικής ζωής των χρηστών και διασφάλιση του ελέγχου των προσωπικών τους δεδομένων. Κάτι τέτοιο μπορεί να προωθήσει την ένταξη, την επισημοποίηση και την ψηφιοποίηση. Για παράδειγμα:

- Το 45% των γυναικών ηλικίας 15 και άνω, σε χώρες χαμηλού εισοδήματος, στερείται ταυτότητας, κάτι που ισχύει μόνο για το 30% των ανδρών.
- Επιπλέον, 1,7 δισ. άνθρωποι θα δύναται να αποκτήσουν πρόσβαση σε υπηρεσίες οικονομικού χαρακτήρα.
- Το 90% του κόστους συμφωνίας με νέους πελάτες (customer onboarding) θα μπορούσε ενδεχομένως να μειωθεί.
- Η οικονομική αξία του ΑΕΠ (Ακαθάριστου Εγχώριου Προϊόντος) της εκάστοτε χώρας θα μπορούσε να κυμανθεί μεταξύ 3%-13% το 2030, λόγω της ψηφιακής ταυτότητας».

Είναι κοινά παραδεκτό ότι στον κοινωνικοπολιτικό τομέα, περιορίζεται ο οικονομικός αποκλεισμός. Είναι γεγονός πως στις αναπτυσσόμενες χώρες, λιγότερο από το 50% του πληθυσμού έχει στη κατοχή του λογαριασμό τραπέζης. Χάρη στην ηλεκτρονική ταυτοποίηση, τόσο οι γυναίκες όσο και τα παιδιά αποκτούν πρόσβαση σε διαδικασίες κοινωνικοπολιτικού και οικονομικού περιεχομένου, αλλά κυρίως τους παρέχεται η ευχέρεια άσκησης των πολιτικών τους δικαιωμάτων (Dahan and Hanmer, 2015). Εξάλλου, δεν πρέπει να λησμονηθεί ότι «σε αντίθεση με τον αντρικό, ο γυναικείος πληθυσμός, στις περισσότερες των περιπτώσεων, δεν έχει πρόσβαση στην προσωπική ταυτοποίηση» (Dahan and Hanmer, 2015). Ιδιαίτερα σημαντική θεωρείται η συμβολή της ηλεκτρονικής ταυτοποίησης στη διαχείριση του μεταναστευτικού

ζητήματος, λόγω της εκδούλευσης της ενάσκησης των δικαιωμάτων ασύλου και προστασίας κατά τη φιλοξενία σε μία ξένη χώρα ή κατά τη διάρκεια της μετακίνησης (Manby, 2016).

3.1. Μέθοδοι Ταυτοποίησης

Η ταυτοποίηση ορίζεται από τον John Hartley (2011) ως «μια διαδικασία που περιλαμβάνει τη διεκδίκηση των χαρακτηριστικών της ταυτότητας ενός ατόμου με σκοπό τη νοηματοδότηση του εαυτού». Το κυριότερο μέσο ταυτοποίησης για όλα τα κράτη είναι το «Δελτίο Ταυτότητας» ή «Κάρτα Ταυτότητας» (Identity Card). Πρόκειται για ένα απαραίτητο έγγραφο ταυτοποίησης, βασιζόμενο στα χαρακτηριστικά ενός ατόμου, που εκδίδεται από μία κρατική ή αστυνομική αρχή και διαθέτει ένα μοναδικό αναγνωριστικό, ενώ οι πληροφορίες που περιλαμβάνει φυλάσσονται σε μία κρατική βάση δεδομένων.

Εν γένει, για την ταυτοποίηση ενός ατόμου χρησιμοποιούνται Τεχνολογίες Πιστοποίησης (Credential Technologies), οι οποίες διαχωρίζονται σε: βιομετρική πληροφορία, κάρτες και κινητά τηλέφωνα (World Bank, 2018b).

Ο όρος βιομετρική πληροφορία περιλαμβάνει την αναγνώριση των μοναδικών φυσικών στοιχείων ενός ατόμου για την ταυτοποίηση και την επικύρωση της ταυτότητάς του (Das, 2016). Οι βιομετρικές πληροφορίες διαχωρίζονται σε πρωτεύουσες (πρόσωπο, δαχτυλικό αποτύπωμα κτλ.) και δευτερεύουσες (π.χ. υπογραφή) (World Bank, 2018b). Αναντίρρητα, η βιομετρική πληροφορία αποτελεί ένα καθολικό και ταυτόχρονα μοναδικό και αδιαίρετο στοιχείο (Das, 2016).

Όσον αφορά στις κάρτες, διακρίνονται σε τρεις κατηγορίες: απλές – ή μη ηλεκτρονικές, ψηφιακές και «έξυπνες». Εν πρώτοις, οι μη ηλεκτρονικές κάρτες, εκτός από το μοναδικό αναγνωριστικό τους, αναγράφουν τις βασικές δημογραφικές πληροφορίες του κατόχου, όπως ονοματεπώνυμο και ημερομηνία γεννήσεως. Επίσης, είναι πιθανό να φέρουν και φωτογραφία του. Σε αυτή τη κατηγορία εντάσσεται η προαναφερθείσα «Κάρτα Ταυτότητας». Έπειτα, οι ψηφιακές κάρτες (RFID) κάνουν χρήση ραδιοσυγχοντήτων για την αναγνώριση και την ταυτοποίησή των πληροφοριών που είναι αποθηκευμένες στην «RFID» ετικέτα που βρίσκεται στην επιφάνεια της εκάστοτε κάρτας (World Bank, 2018b). Η χρήση της κυρίως, περιορίζεται σε διαδικασίες όπως: το άνοιγμα μιας πόρτας με κλειδαριά αντίστοιχης τεχνολογίας, ανίχνευση προϊόντων, αλλά και στις ανέπαφες πληρωμές μέσω πιστωτικής και

χρεωστικής κάρτας. Στη συνέχεια, γίνεται λόγος για τις «έξυπνες» κάρτες, οι οποίες παίρνουν το όνομα τους από τις τεχνολογίες που διαθέτουν. Ενσωματώνουν στο εσωτερικό τους ένα μικροτσίπ και μία μονάδα επεξεργασίας, σχεδιασμένα με τέτοιο τρόπο, ώστε να ενεργοποιούνται όταν έρχονται σε επαφή με μία συσκευή ανάγνωσης. Είναι ευρέως χρησιμοποιούμενες ήδη σε πολλές χώρες, ιδίως για διαδικασίες ψήφου, ανοίγματος τραπεζικού λογαριασμού και αιτήσεων αδειών οδήγησης (World Bank, 2018b).

Η επόμενη και πιο προσφάτως αναπτυγμένη τεχνολογία ταυτοποίησης είναι η ταυτοποίηση μέσω κινητού τηλεφώνου (Εικόνα 8). Σε αυτή τη τεχνολογία περιλαμβάνεται πλήθος μεθόδων, κάποιες από τις οποίες είναι η μέθοδος Κωδικού Μιας Χρήστης (One Time Password – OTP), που αποστέλλεται στη συσκευή του χρήστη ένας μοναδικός κωδικός με συγκεκριμένη διάρκεια ενεργοποίησης και η μέθοδος Ταυτοποίησης Μέσω Εφαρμογής (Authenticator Mobile App), που συνδυάζοντας την λογική της μεθόδου OTP με τη χρήση ενός μυστικού κλειδιού, δημιουργείται ένας εξαψήφιος ή οκταψήφιος κωδικός, με εξαιρετικά μικρή διάρκεια ενεργοποίησης, απαραίτητος για τη ταυτοποίηση του χρήστη.



Εικόνα 8 - Μέθοδοι ταυτοποίησης μέσω κινητού τηλεφώνου (World Bank, 2018b)

3.2. Συστήματα Διαχείρισης Ταυτότητας

Ένα σύστημα διαχείρισης ταυτότητας απαρτίζεται από ένα σύνολο υπηρεσιών που αποσκοπούν στη διαχείριση των πληροφοριών της ταυτότητας ενός ατόμου· διαρθρώνεται σε τρία επίπεδα, καθένα από τα οποία είναι υπεύθυνο για την προσαρμογή των κανόνων επεξεργασίας δεδομένων και την πρόσβαση των κατόχων αυτών στο σύστημα. Ονομαστικά, τα επίπεδα αυτά είναι τα εξής: Βάση, Κύκλος Ζωής και Πρόσβαση και Χρήση.

Η Βάση ενός συστήματος διαχείρισης ταυτότητας είναι το επίπεδο που καθορίζει τους κανόνες πρόσβασης στα δεδομένα του συστήματος και συντάσσεται από τα παρακάτω μέρη (Pato and Rouault, 2003):

- Πάροχος Αυθεντικοποίησης (Authentication Provider): Είναι η υπεύθυνη οντότητα για την αρχική αυθεντικοποίηση ενός ατόμου που επιθυμεί να συνδεθεί με μια ταυτότητα. Στις τεχνικές αρχικής αυθεντικοποίησης περιλαμβάνονται μηχανισμοί όπως η επαλήθευση συνθηματικών, επαλήθευση έξυπνων καρτών, σαρώσεις βιομετρικών δεδομένων κ.α.
- Επόπτευση Πολιτικής (Policy Control): Η επεξεργασία των πληροφοριών που συνδέονται με μια ταυτότητα ρυθμίζεται από μια σειρά κανόνων που ελέγχουν τη διαχείριση των δεδομένων που διατηρούνται στο σύστημα καθώς και υπό ποιες προϋποθέσεις είναι δυνατόν να διαμοιραστούν.
- Έλεγχος (Auditing): Οι μέθοδοι ελέγχου αποτελούν ένα μηχανισμό για την καταγραφή της δημιουργίας, μεταβολής και χρήσης των δεδομένων.

Ο Κύκλος Ζωής είναι η σειρά ενεργειών που είναι υπεύθυνη για τη ρύθμιση των στοιχείων που αφορούν στην έκδοση ηλεκτρονικών ταυτοτήτων καθώς και στην διαχείριση των δεδομένων που περιλαμβάνουν. Τα χαρακτηριστικά του είναι τα εξής:

- Παροχή (Provisioning): Πρόκειται για την αυτοματοποίηση των διαδικασιών που επιτρέπουν τον συντονισμό του κύκλου ζωής μιας ταυτότητας (π.χ. τη δημιουργία ή τη κατάργηση της).
- Διάρκεια (Longevity): Η τήρηση του αρχείου τροποποιήσεων μιας ταυτότητας, καθ' όλη τη διάρκεια του κύκλου ζωής της.

Ολοκληρώνοντας, το επίπεδο Πρόσβασης και Χρήσης ορίζει τους τρόπους πρόσβασης και προσπέλασης των δεδομένων στο σύστημα και ενσωματώνει τις:

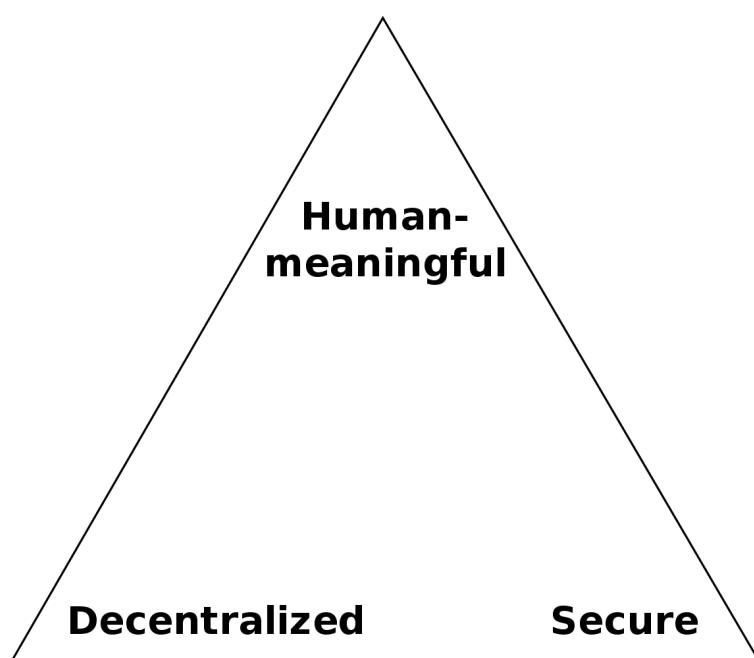
- Εφ' άπαξ Πρόσβαση (Single Sign-in): Ο κάτοχος της ταυτότητας αποκτά πρόσβαση στο σύνολο των διασυνδεμένων με το σύστημα υπηρεσιών, καθώς η

ταυτότητα του πιστοποιείται μονομιάς κατά τη πρώτη του σύνδεση στο σύστημα και δεν απαιτούνται περεταίρω ενέργειες.

- Εξατομίκευση (Personalization): Η παραχώρηση πληροφοριών σχετικά με της εφαρμογές που χρησιμοποιεί ο κάτοχος της ταυτότητας.
- Διαχείριση Πρόσβασης (Access Management): Διαχωρισμός των βαθμίδων πρόσβασης βάσει ήδη καθορισμένων προνομίων και κανόνων.

Στο μεγαλύτερο ποσοστό τους, τα συστήματα διαχείρισης ταυτότητας είναι συγκεντρωτικά (centralized), με αποτέλεσμα τα δεδομένα των ταυτοτήτων να ελέγχονται εξ ολοκλήρου από έναν ή περισσότερους οργανισμούς και όχι από τους κατόχους τους.

Η πρώτη προσπάθεια ανάπτυξης ενός συστήματος πλήρους αποκεντρωμένης (decentralized) ταυτοποίησης παρουσιάστηκε με την δημιουργία του «Namecoin». Το «Namecoin» ήρθε σε αντίθεση με τον τρόπο σκέψης που επικρατούσε εκείνη την εποχή, ο οποίος αντλούσε την επιρροή του από το άρθρο που δημοσίευσε ο Bryce Wilcox-O'Hearn το 2001 σχετικά με τον χώρο ονομάτων (namespace) στα συστήματα υπολογιστών. Σύμφωνα με αυτό, ήταν πρακτικά απίθανος ο σχεδιασμός ενός συστήματος ασφαλούς επιλογής διαπιστευτηρίων με κατανεμημένο τρόπο, που θα ήταν συγχρόνως αναγνώσιμα από τον άνθρωπο. Αυτή η δήλωση είναι ακόμη γνωστή ως «Τρίγωνο Zooko» (Zooko's Triangle) (Εικόνα 9).



Εικόνα 9 - Το τρίγωνο Zooko (Wikipedia, 2020)

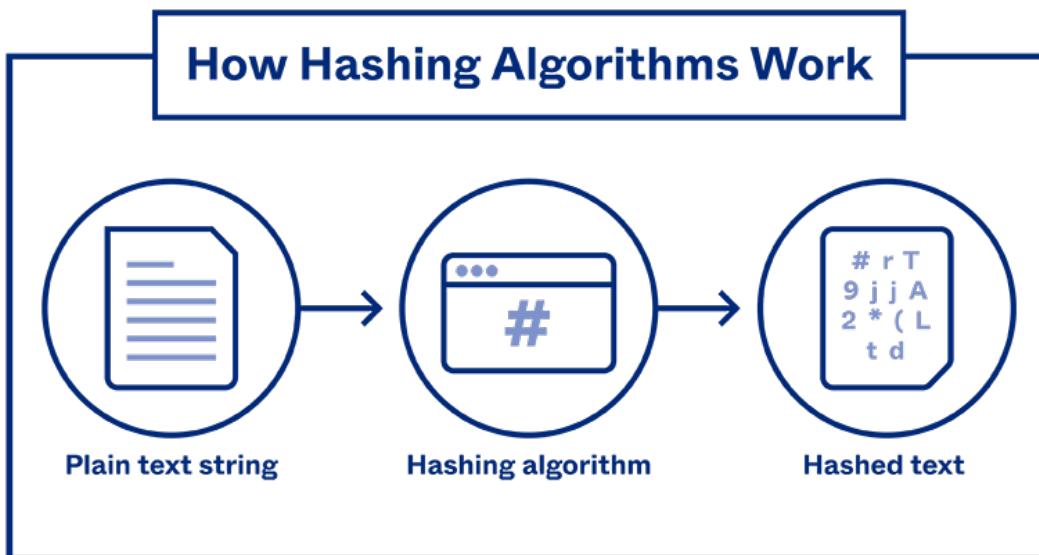
Με την τεχνολογία του Blockchain είναι εφικτή η επιλογή, με κατανεμημένο τρόπο, ενός αναγνώσιμου από τον άνθρωπο διαπιστευτηρίου, όπως επίσης και η αντιστοίχιση και επαλήθευση ζευγών ονομάτων-τιμών χωρίς την παρέμβαση μεσαζόντων.

3.3. Ασφάλεια και Ιδιωτικότητα

Λόγω της επιδίωξης για την εξασφάλιση της προστασίας των δεδομένων, της φορητότητας και της διαλειτουργικότητας, οι ψηφιακές ταυτότητες και τα αντίστοιχα συστήματα διαχείρισης εξελίσσονται και τείνουν όλο και περισσότερο προς πιο αποκεντρωμένες προσεγγίσεις, από τις πλήρως συγκεντρωτικές που τις χαρακτηρίζουν επί του παρόντος. Καθώς αναπτύσσονται νέες τεχνολογίες, οι ρυθμιστικές αρχές κατανοούν ορθότερα τον ψηφιακό κόσμο, οι κυβερνήσεις και οι ιδιωτικοί οργανισμοί ανακαλύπτουν καλύτερους τρόπους ηλεκτρονικής αλληλεπίδρασης και οι χρήστες αποκτούν μεγαλύτερη εμπιστοσύνη στα υφιστάμενα συστήματα διαχείρισης ψηφιακής ταυτότητας που εξακολουθούν να προτείνονται και να υιοθετούνται.

Σε ό,τι αφορά τον τομέα της ασφάλειας μιας ταυτότητας, αυτή επιτυγχάνεται μέσω των σταδίων της ίδιας της ταυτοποίησης του ατόμου με τα πραγματικά, ακριβή του στοιχεία. Αρχικά, πραγματοποιείται κρυπτογράφηση του αρχικού μηνύματος, με σκοπό τη μετατροπή του σε ακατανόητη για τον άνθρωπο μορφή, η οποία χρήζει αποκρυπτογράφησης για να αναγνωστεί. Σύμφωνα με την IBM (2019), κρυπτογράφηση ονομάζεται η διαδικασία μετατροπής ενός απλού, αναγνώσιμου κειμένου (plain text) σε μια μη αναγνώσιμη μορφή που λέγεται ciphertext (σε ελεύθερη μετάφραση «κρυπτοκείμενο»). Η κρυπτογραφία χρησιμοποιείται με σκοπό την επίτευξη ταυτοποίησης (identification), πιστοποίησης (authentication) και εξουσιοδότησης (authorization). Η ταυτοποίηση ανάγεται στον ισχυρισμό ότι κάποιο άτομο είναι αυτό που δηλώνει. Η πιστοποίηση αναφέρεται στην απόδειξη ότι πράγματι το άτομο είναι αυτό που ισχυρίζεται. Η εξουσιοδότηση αφορά στην πρόσβαση που αποκτά το άτομο σε συγκεκριμένους πόρους εξαιτίας της πιστοποίησης που έχει προηγηθεί. Κατόπιν, με τη χρήση της μεθόδου «σύνοψης μηνύματος» (Message Digest), το κρυπτογραφημένο κείμενο μετατρέπεται σε μία αριθμητική παράσταση η οποία, αμέσως μετά, κατακερματίζεται (hash) και επανακρυπτογραφείται, δημιουργώντας έτσι μια ψηφιακή υπογραφή. Τέλος, υφίσταται το σύστημα «Δομής Δημοσίου Κλειδιού» (Public Key Infrastructure – PKI) που σχετίζεται με

εγκαταστάσεις, πολιτικές και υπηρεσίες που υποστηρίζουν τη χρήση κρυπτογράφησης δημοσίου κλειδιού για τη πιστοποίηση των συμμετεχόντων μιας συναλλαγής (IBM, 2019a) αλλά και τα ψηφιακά πιστοποιητικά που εγγυόνται τη σωστή αντιστοίχιση ενός συγκεκριμένου δημοσίου κλειδιού με μία οντότητα.



okta

Εικόνα 10 - Τρόπος λειτουργίας των αλγόριθμου κατακερματισμού (Okta, n.d.)

Η έννοια της ιδιωτικότητας διαφέρει από τη προδιαγραφή ύπαρξης ασφάλειας στο σύστημα. Ορίζεται ως η ικανότητα ενός ατόμου ή μιας ομάδας να απομονώσει τις πληροφορίες που αφορούν στον εαυτό του και κατ' αυτόν τον τρόπο να ελέγχει τα όρια στα οποία μπορεί κάποιος τρίτος να αλληλεπιδράσει με αυτές. Υπάρχουν οι εξής τομείς ιδιωτικότητας: η πληροφοριακή ιδιωτικότητα που αναφέρεται σε δημόσια έγγραφα και μητρώα, η σωματική ιδιωτικότητα που αφορά τη ακεραιότητα του ανθρώπινου σώματος, η ιδιωτικότητα - απόρρητο των τηλεπικοινωνιών και η ιδιωτικότητα οικιακού και οικογενειακού ασύλου (The Public Voice, n.d.).

Στα συστήματα ηλεκτρονικής ταυτοποίησης, ο εκάστοτε οργανισμός, είτε κρατικός είτε ιδιωτικός, οφείλει να αναπτύξει ένα ευπρεπές πλαίσιο πολιτικής αναφορικά με την εμφύσηση της εμπιστοσύνης στα εμπλεκόμενα άτομα, την αποθήκευση των δεδομένων τους και την προστασία τους από απειλές, όπως επίσης και τους τρόπους διαχείρισης τους (World Bank, 2018b). Δίχως τις παραπάνω πολιτικές ιδιωτικότητας δε θα διαμορφωθεί η αίσθηση της εμπιστοσύνης ως προς το σύστημα.

Λόγω των προαναφερθέντων, στις 27 Απριλίου του 2016 η Ευρωπαϊκή Επιτροπή ανακοίνωσε τον «Γενικό Κανονισμό για την Προστασία των Δεδομένων» (General Data Protection Regulation - GDPR), ο οποίος αναφέρεται στα νέα δικαιώματα που αποκτούν οι πολίτες της Ευρωπαϊκής Ένωσης σχετικά με τα προσωπικά τους δεδομένα, με ένα από τα πιο σημαντικά από αυτά να είναι το δικαίωμα απόσυρσης της συγκατάθεσης τους. Αφορμή στάθηκε η συνεχής χρήση των προσωπικών δεδομένων των ατόμων από εταιρίες με απότερο σκοπό την παροχή υπηρεσιών, ιδίως στο διαδίκτυο, όπως είναι η υπηρεσίες στοχευμένων διαφημίσεων. Κύριο μέλημα της Ευρωπαϊκής Ένωσης με τον κανονισμό αυτό είναι να παράσχει στα φυσικά πρόσωπα τον έλεγχο των προσωπικών τους δεδομένων και να απλουστεύσει το ρυθμιστικό περιβάλλον για τις διεθνείς επιχειρήσεις με την εδραίωση του κανονισμού εντός της Ευρωπαϊκής Ένωσης (Pandit, O' Sullivan and Lewis, 2018).

Εξαιτίας ιστορικών και μη λόγων, η εμπειρία χρήσης της ψηφιακής ταυτότητας σήμερα είναι διφορούμενη, με ελλιπή πρότυπα ή διαλειτουργικότητα. Επίσης, περιβάλλεται από ανασφάλεια, όπως δηλώνουν οι σχεδόν καθημερινές αναφορές για επιθέσεις και παραβιάσεις δεδομένων (Lyons, Courcelas and Timsit, 2016). Παρά τις προσπάθειες των φορέων και των κυβερνήσεων ανά τα χρόνια, οι απειλές προς τα δεδομένα των χρηστών δεν έπαψαν να υπάρχουν. Χαρακτηριστικό παράδειγμα αποτελεί η υπόθεση με εμπλεκόμενους τη συμβουλευτική εταιρία «Cambridge Analytica» και το κοινωνικό δίκτυο «Facebook», όπου το δεύτερο έδωσε απεριόριστη πρόσβαση σε προσωπικά δεδομένα περισσότερων από 87 εκατομμυρίων χρηστών του χωρίς τη συγκατάθεσή τους. Κάποια ακόμη παραδείγματα απειλών – παραβιάσεων είναι: η υπόθεση παραβίασης δεδομένων του «Equifax» το 2017 (143 εκατομμύρια διαπιστευτήρια σε κίνδυνο), η υπόθεση «Adult Friend Finder» το 2016 (413 εκατομμύρια κλοπές λογαριασμών) και η υπόθεση «Anthem» το 2015 (78 εκατομμύρια λογαριασμοί παραβιάστηκαν). Καμία προληπτική προσέγγιση φαίνεται πως δεν είναι 100% ασφαλής, όμως η έγκαιρη ανακάλυψη του προβλήματος θα μπορούσε να αποτρέψει την κατάχρηση αυτών των λογαριασμών.

Types of Data Compromised

Personally Identifiable Information


ITRC | IDENTITY THEFT
RESOURCE CENTER

Number of Breaches/Exposures Containing PII

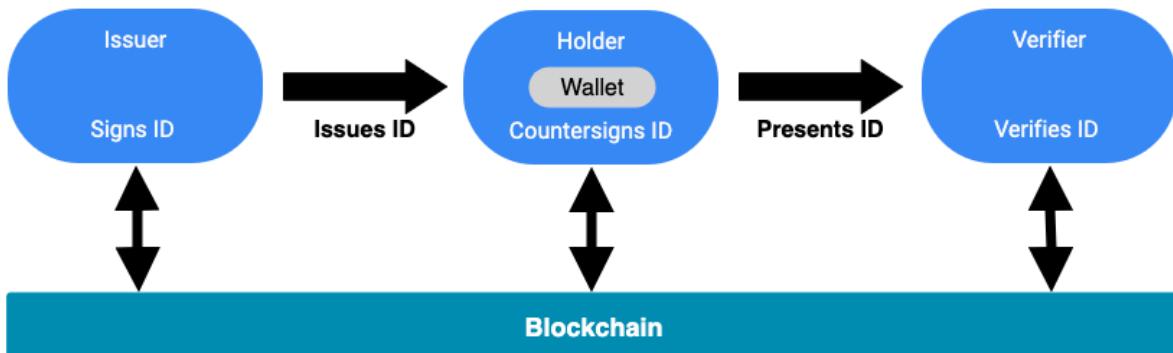
Εικόνα 11 - Γράφημα από την έκθεση του οργανισμού «Identity Theft Resource Center» για τις παραβιάσεις δεδομένων τη χρονιά 2021

3.4. Η χρήση της τεχνολογίας του Blockchain στην ταυτοποίηση

Η τεχνολογία του Blockchain μπορεί να θεωρηθεί ως ένας μηχανισμός για την επίτευξη ακεραιότητας σε κατανεμημένα συστήματα λογισμικού και δύναται να αντικαταστήσει τον ρόλο που αυτή τη στιγμή έχουν οι αναφερόμενες ως έμπιστες οντότητες (π.χ. κυβερνητικές υπηρεσίες, τράπεζες). Αυτό οφείλεται στην ιδιαιτερότητά της, δηλαδή στη μη απαίτηση ανάμειξης κάποιου τρίτου, κεντρικού μηχανισμού, κατά τη διάρκεια της επικοινωνίας μεταξύ δύο οντοτήτων. Σε ένα σύστημα ταυτοποίησης μέσω Blockchain, τα δεδομένα αποθηκεύονται εντός της αλυσίδας προσφέροντας έτσι, απόλυτη ασφάλεια. Κάθε χρήστης (εφ' εξής «κάτοχος») δημιουργεί ένα ψηφιακό πορτοφόλι, που αντιπροσωπεύεται από μία διεύθυνση στο Blockchain. Ένας οργανισμός αποκαλούμενος ως «εκδότης» (Issuer) εκτελεί τις απαραίτητες ενέργειες για τη καταχώριση μιας νέας ηλεκτρονικής ταυτότητας, οι πληροφορίες της οποίας «αποθηκεύονται» στο πορτοφόλι του κατόχου. Στη διαδικασία λαμβάνει μέρος και μια τρίτη οντότητα, ο «επαληθευτής» (Verifier), ο οποίος αλληλεπιδρά με τον κάτοχο, αιτώντας πληροφορίες της ταυτότητας του μέσω συναλλαγών. Ακολούθως, ο κάτοχος επιλέγει ποια δεδομένα της ταυτότητάς του επιθυμεί να μοιραστεί, ώστε στη συνέχεια, να επιβεβαιωθεί η γνησιότητα τους από τον επαληθευτή. Καθ' όλη τη διάρκεια της διαδικασίας διατηρείται εμπιστοσύνη στα μέρη της εκάστοτε συναλλαγής, λόγω της

κρυπτογράφησης δημόσιου και ιδιωτικού κλειδιού και της διαφάνειας που υφίσταται στον τρόπο δημιουργίας και επαλήθευσης των ταυτότητων.

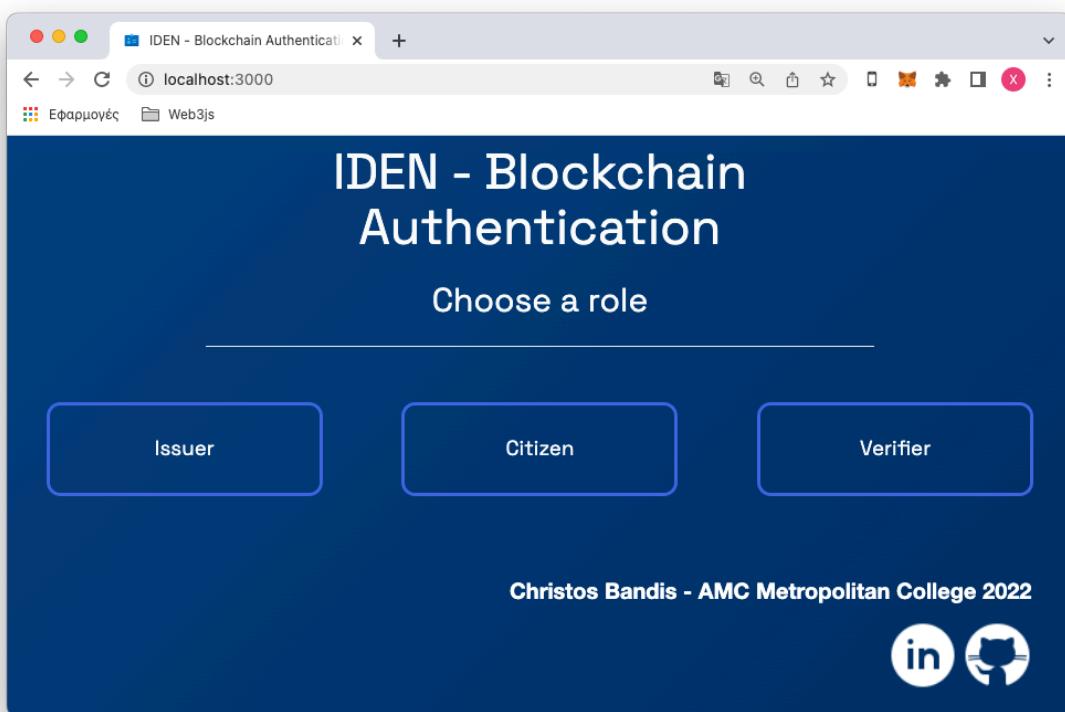
Αποτελεί όμως, κοινό τόπο ότι όλες οι τεχνολογίες, έτσι και το Blockchain, διαθέτουν και δυσμενή χαρακτηριστικά. Ένα από τα βασικότερα εξ αυτών είναι η έλλειψη της δυνατότητας ανάκτησης των κωδικών σύνδεσης ή του ιδιωτικού κλειδιού (Private Key) ενός πορτοφολιού σε περίπτωση απώλειάς τους, λόγω της απουσίας κεντρικού διακομιστή. Επίσης, σημαντικό μειονέκτημα θεωρείται το επίπεδο πολυπλοκότητας της τεχνολογίας, δεδομένου ότι η δομή του συστήματος δεν εξασφαλίζει πως ένας κάτοχος θα είναι ιδιοκτήτης ενός μόνο ιδιωτικού κλειδιού, κάτι που έχει ως αποτέλεσμα την πιθανότητα δημιουργίας πολλαπλών ταυτότητων για το ίδιο άτομο.



Εικόνα 12 - Τρόπος λειτουργίας ενός συστήματος ταυτοποίησης μέσω Blockchain

4. Παρουσίαση της εφαρμογής ταυτοποίησης «IDEN»

Η εφαρμογή «IDEN» (Identification Eden) είναι ένα σύστημα ταυτοποίησης που κάνει χρήση της τεχνολογίας του Blockchain. Αναπτύχθηκε στο Ethereum Blockchain και εκμεταλλεύεται οποιαδήποτε χαρακτηριστικά συνεπάγονται με αυτό. Εμπεριέχει τρεις ρόλους, τον «εκδότη» (Issuer), τον «πολίτη» (Citizen) και τον «επαληθευτή» (Verifier) και επωφελείται των έξυπνων συμβολαίων για την διεκπεραίωση των λειτουργιών της. Ο «εκδότης» είναι υπεύθυνος για την καταχώρηση των στοιχείων της ταυτότητας του «πολίτη» και του «επαληθευτή» στο Blockchain. Τα δεδομένα εισάγονται μέσω μίας φόρμας στο περιβάλλον εφαρμογής του «εκδότη» και στη συνέχεια «αποθηκεύονται» στο πορτοφόλι που αντιστοιχεί στη παρεχόμενη, από τον «πολίτη» ή τον «επαληθευτή», διεύθυνση. Έπειτα, ο «πολίτης» από το αντίστοιχο περιβάλλον, μπορεί να ελέγξει τα στοιχεία του και να «απαντήσει» σε εισερχόμενα αιτήματα κοινοποίησης των δεδομένων του. Τέλος, ο «επαληθευτής» έχει τη δυνατότητα, μέσω του δικού του περιβάλλοντος, να αιτηθεί των δεδομένων ενός «πολίτη», να επιβεβαιώσει την κυριότητα τους και να εκτελέσει τις επιθυμητές ενέργειες. Σε επίπεδο ασφάλειας, κληρονομεί όλα τα γνωρίσματα των έξυπνων συμβολαίων, συνεπώς όλα τα δεδομένα είναι κρυπτογραφημένα, με συνεχείς ελέγχους για την αποφυγή πιθανού σφάλματος.



Eικόνα 13 - Η αρχική σελίδα της εφαρμογής «IDEN»

4.1. Υφιστάμενο πρόβλημα

Μέχρι και σήμερα, η χρήση της ψηφιακής ταυτότητας διευκόλυνε τις τραπεζικές και τις μεταξύ πολιτών και κράτους συναλλαγές, καθώς περισσότεροι από 1,5 δισεκατομμύρια άνθρωποι σε όλο τον πλανήτη δεν έχουν στη κατοχή τους αστικές ταυτότητες (The World Bank Group, GSMA and Secure Identity Alliance, 2016). Ωστόσο, το σημαντικότερο μειονέκτημα αυτής της εξέλιξης, χωρίς αυτό να είναι αισθητό για το μεγαλύτερο ποσοστό των ανθρώπων, είναι ότι η διαχείριση της ταυτότητας και των δεδομένων της δεν γίνεται από τον ίδιο τον κάτοχο· αποτέλεσμα του οποίου είναι η έκθεση μερών αυτής της ταυτότητας σε κερδοσκοπικού χαρακτήρα οργανώσεις. Νομοθεσίες όπως ο «Γενικός Κανονισμός για την Προστασία των Δεδομένων» τέθηκαν αντιμέτωπες προς τέτοιου είδους προβλήματα απρεπούς διαχείρισης των προσωπικών δεδομένων. Παρ' όλα αυτά, η «έκρηξη» του διαδικτύου, η αύξηση της χρήσης κινητών συσκευών (π.χ. Smartphones, Tablets) και η εμμονή των οργανισμών να συλλέγουν δεδομένα έχουν επιδεινώσει την κατάσταση των ζητημάτων διαρροής δεδομένων.

Όπως αναφέρθηκε και στα προηγούμενα κεφάλαια, τα τελευταία έτη η τεχνολογία του Blockchain, παρά το γεγονός πως δεν είναι ένα νέο εγχείρημα στο χώρο της τεχνολογίας, αναπτύσσεται συνεχώς και θέτει τα θεμέλια για μία νέα εποχή τόσο στον χρηματοοικονομικό, όσο και στον κοινωνικοπολιτικό τομέα. Οι αλλαγές που πρόκειται να επιφέρει η συγκεκριμένη τεχνολογία είναι τόσο ριζικές, που πλήθος επιστημόνων του κλάδου -και μη, την αποκαλούν ως «το νέο διαδίκτυο».

Η χρήση της τεχνολογίας του Blockchain για την επαλήθευση των στοιχείων ψηφιακής ταυτότητας, αποτελεί σημαντική εξέλιξη αφού προστατεύει τα ευαίσθητα προσωπικά δεδομένα από μη αδειοδοτημένη «διαρροή», επιτρέποντας στους χρήστες να είναι οι μοναδικοί κάτοχοι των στοιχείων τους. Επίσης, δίνει λύση στο πρόβλημα που συναντάται κυρίως, στις απλές, υλικές ταυτότητες. Το πρόβλημα αυτό αφορά στις περιπτώσεις που απαιτείται η επαλήθευση ενός στοιχείου της ταυτότητας ενός ατόμου (λ.χ. επώνυμο), όμως τα υπόλοιπα στοιχεία (λ.χ. ημερομηνία γεννήσεως) παραμένουν ορατά στον «επαληθευτή», χωρίς την άδεια του κατόχου. Παραδείγματος χάριν, ένας υποψήφιος υπάλληλος μπορεί να μοιραστεί με τον υπεύθυνο προσωπικού της επιχείρησης τους βαθμούς επίδοσής του στο πανεπιστήμιο που φοίτησε, χωρίς να εκθέσει την υπηκοότητά του.

Βάσει των προαναφερθέντων, το κύριο πρόβλημα που καλείται να αντιμετωπίσει η εφαρμογή είναι η μη σωστή διαχείριση των προσωπικών δεδομένων από οργανισμούς που έχουν αποκτήσει πρόσβαση σε αυτά και οι τρόποι με τους οποίους η τεχνολογία του Blockchain μπορεί να ωφελήσει στην τήρηση της ακεραιότητας και της ασφάλειας τους. Για την ορθότερη επίλυσή του, είναι σημαντικό να διαχωριστεί σε μικρότερα υποπροβλήματα:

- Εύρεση της ιδανικότερης μεθόδου αυτοδιαχείρισης των δεδομένων.
- Έρευνα στον τομέα του Blockchain για τη δημιουργία της βέλτιστης υποδομής για την εφαρμογή.
- Αποκλειστικός έλεγχος των στοιχείων μιας ταυτότητας από τον κάτοχο της.
- Άμεση και έγκυρη επιβεβαίωση της κυριότητας μιας ταυτότητας απευθείας από τον επαληθευτή, χωρίς την επέμβαση τρίτου.

Απόρροια της παραπάνω ανάλυσης τους προβλήματος αποτελούν οι ακόλουθες απαιτήσεις προδιαγραφών που οφείλει να τηρεί η εφαρμογή, οι οποίες διαχωρίζονται σε λειτουργικές και μη λειτουργικές.

Στις λειτουργικές απαιτήσεις εντάσσονται οι εξής:

- Έλεγχος των δικαιωμάτων πρόσβασης του χρήστη που επιχειρεί να αλληλεπιδράσει με την εφαρμογή.
- Έλεγχος της, παρεχόμενης από τον κάτοχο, διεύθυνσης «πορτοφολιού» κατά την εγγραφή του στο Blockchain.
- Εγγραφή των στοιχείων ταυτότητας του κατόχου (πολίτης ή επαληθευτής) στον «χώρο» αποθήκευσης του «έξυπνου» συμβολαίου που του αντιστοιχεί.
- Δημιουργία αιτήματος κοινοποίησης στοιχείων ταυτότητας από τον επαληθευτή και συγκατάθεση από τον πολίτη που απευθύνεται.
- Ενημέρωση του πολίτη όταν ένα αίτημα «αναμένει» συγκατάθεση.
- Επαλήθευση των στοιχείων μιας ταυτότητας μέσω Blockchain συγκρίνοντας το «hash» των παρεχόμενων στοιχείων με το «hash» που αντιστοιχούν στο «έξυπνο» συμβόλαιο του εκδότη και ελέγχοντας την διεύθυνση «πορτοφολιού» του εκδότη της ταυτότητας, όταν αυτή ζητείται.
- Προσθήκη/Δημιουργία εγγραφής ιατρικού ιστορικού για τον πολίτη.
- Διατήρηση των στοιχείων ταυτότητας και του ιατρικού ιστορικού στο «πορτοφόλι» του πολίτη, για την ενίσχυση του απορρήτου του.

- Δυνατότητα δημιουργίας και «ανάγνωσης» του κωδικού QR που εξάγεται από την διεύθυνση «πορτοφολιού» του κατόχου.

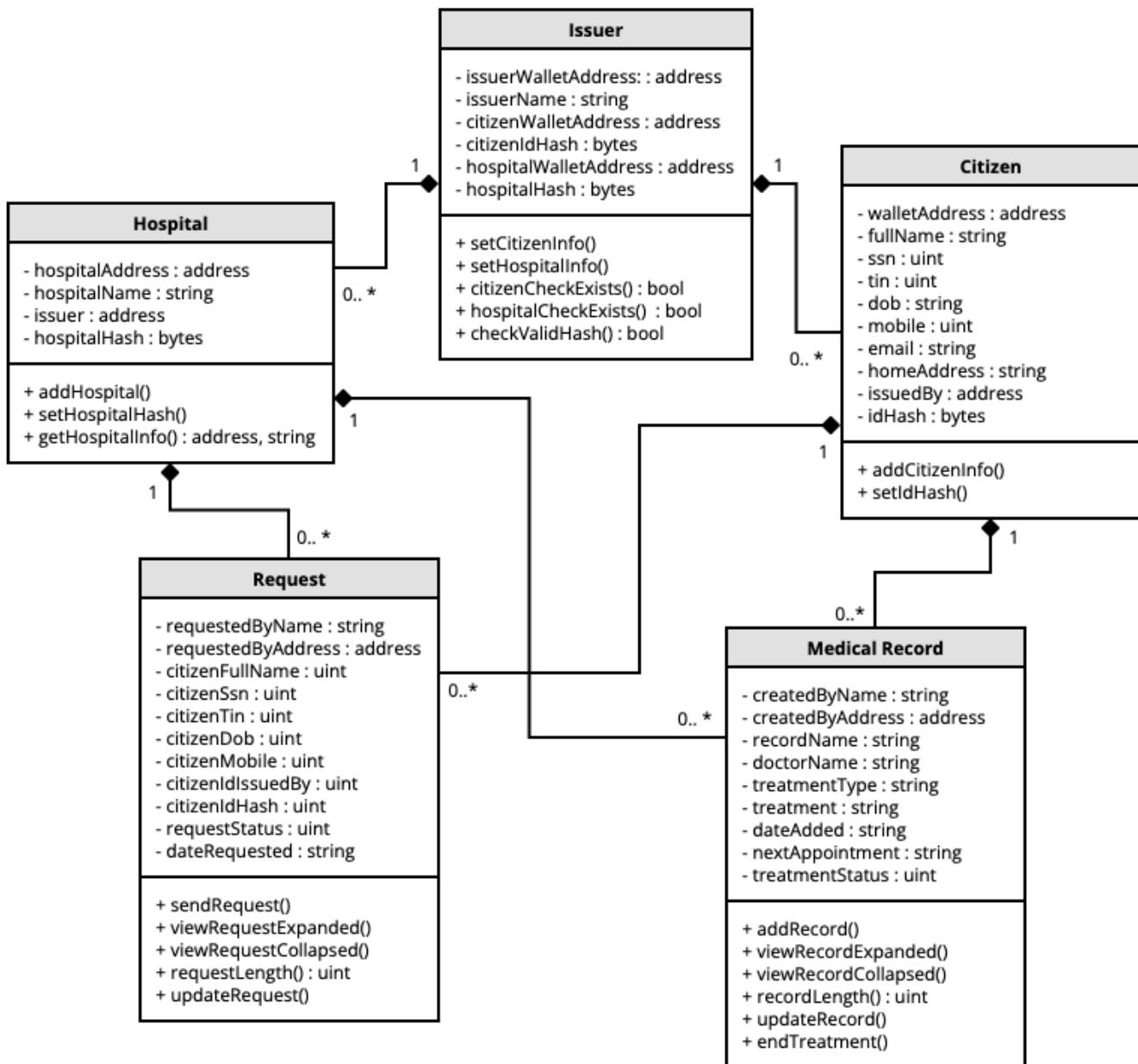
Ενώ, ως μη λειτουργικές απαιτήσεις χαρακτηρίζονται οι παρακάτω:

- Πλήρης αμεσότητα και διαθεσιμότητα της εφαρμογής.
- Υψηλή κρυπτογράφηση των δεδομένων, παρεχόμενη από το Blockchain και τα «έξυπνα» συμβόλαια.
- Υποστήριξη πληθώρας συσκευών (π.χ. ηλεκτρονικοί υπολογιστές, smartphones).
- Ταυτόχρονη εξυπηρέτηση πολλαπλών χρηστών.
- Φιλικό γραφικό περιβάλλον προς τους χρήστες, ανεξαρτήτως εμπειρίας.
- Ταχύτατες συναλλαγές (βασιζόμενες στο ποσοστό χρήσης του Ethereum Blockchain τη δεδομένη στιγμή).
- Χαμηλό κόστος συναλλαγών, αποστέλλοντας μόνο τα καίριας σημασίας δεδομένα μέσω συναλλαγών (εξαρτώμενο επίσης, από το ποσοστό χρήσης του Ethereum Blockchain τη δεδομένη στιγμή).
- Σωστή διαχείριση των δεδομένων εντός των «έξυπνων» συμβολαίων, με στόχο την ταχύτητα προσπέλασης τους και την αποφυγή σφαλμάτων.

4.2. Σχεδιασμός και Μοντελοποίηση

Τα παρακάτω διαγράμματα παρουσιάζουν την πλήρη δομή του συστήματος και τους αποδοτικότερους τρόπους εκμετάλλευσης της τεχνολογίας του Blockchain για την ανάπτυξη της εφαρμογής ταυτοποίησης. Στη συνέχεια, παρουσιάζονται οι ενέργειες που μπορεί να εκτελέσει ο κάθε ρόλος της εφαρμογής, καθώς και βασικά μέρη της εμφάνισης της. Για τη δημιουργία των διαγραμμάτων χρησιμοποιήθηκε η «Ενοποιημένη Γλώσσα Σχεδίασης Προτύπων» (Unified Modeling Language – UML).

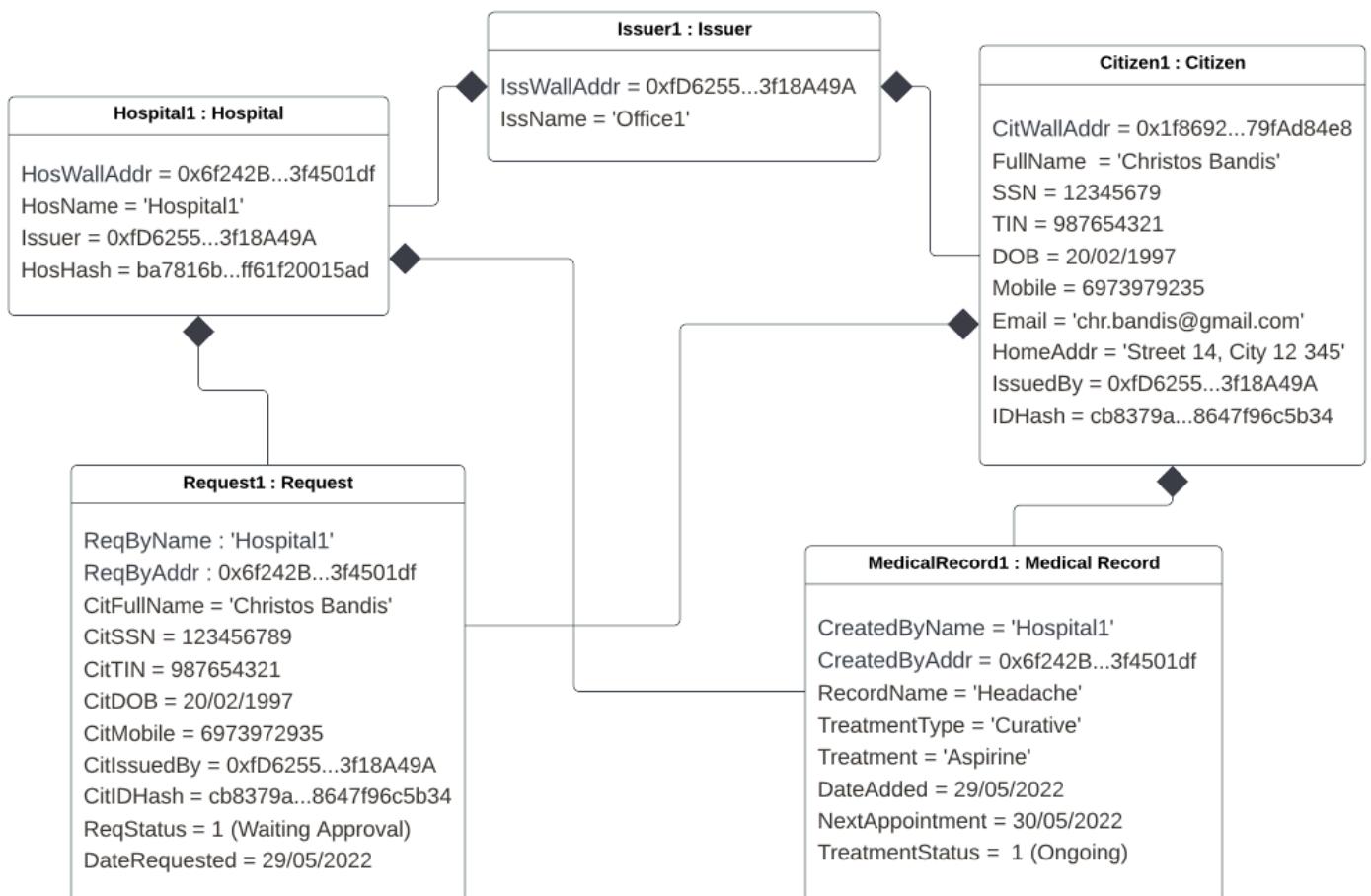
Σε επίπεδο κώδικα, οι κλάσεις που έχουν δημιουργηθεί αντιστοιχούν σε κάθε ένα ρόλο ξεχωριστά. Επίσης, υπάρχουν ακόμη δύο κλάσεις, μία για τα αιτήματα κοινοποίησης και μία για το ιατρικό ιστορικό. Κάθε κλάση, όπως διακρίνεται στο «Διάγραμμα Κλάσης» (Class Diagram) της Εικόνας 14, περιέχει τις απαραίτητες μεταβλητές και μεθόδους για τη λειτουργία της εφαρμογής. Επίσης, παρουσιάζεται η σύνδεση μεταξύ των κλάσεων, η μεταξύ τους σχέση, όπως και ο λόγος πληθικότητας τους.



Εικόνα 14 - Διάγραμμα Κλάσης (Class Diagram)

Ένα χαρακτηριστικό της γλώσσας προγραμματισμού «Solidity», που χρησιμοποιήθηκε για την συγγραφή των «έξυπνων» συμβολαίων, είναι πως δεν απαιτείται η δημιουργία «getter» (μέθοδος που επιστρέφει την τιμή μιας μεταβλητής) κατά τον προγραμματισμό, καθώς δημιουργείται αυτόματα. Παρομοίως, κρίθηκε μη απαραίτητη η δημιουργία «setter» (μέθοδος που θέτει ή ενημερώνει την τιμή μιας μεταβλητής), πλην μερικών εξαιρέσεων, διότι το μεγαλύτερο μέρος των μεταβλητών ενημερώνεται μέσω κατάλληλων μεθόδων. Οι παραπάνω παρατηρήσεις είναι ορατές στο διάγραμμα της Εικόνας 14 και στο «Διάγραμμα Αντικειμένου», ή αλλιώς

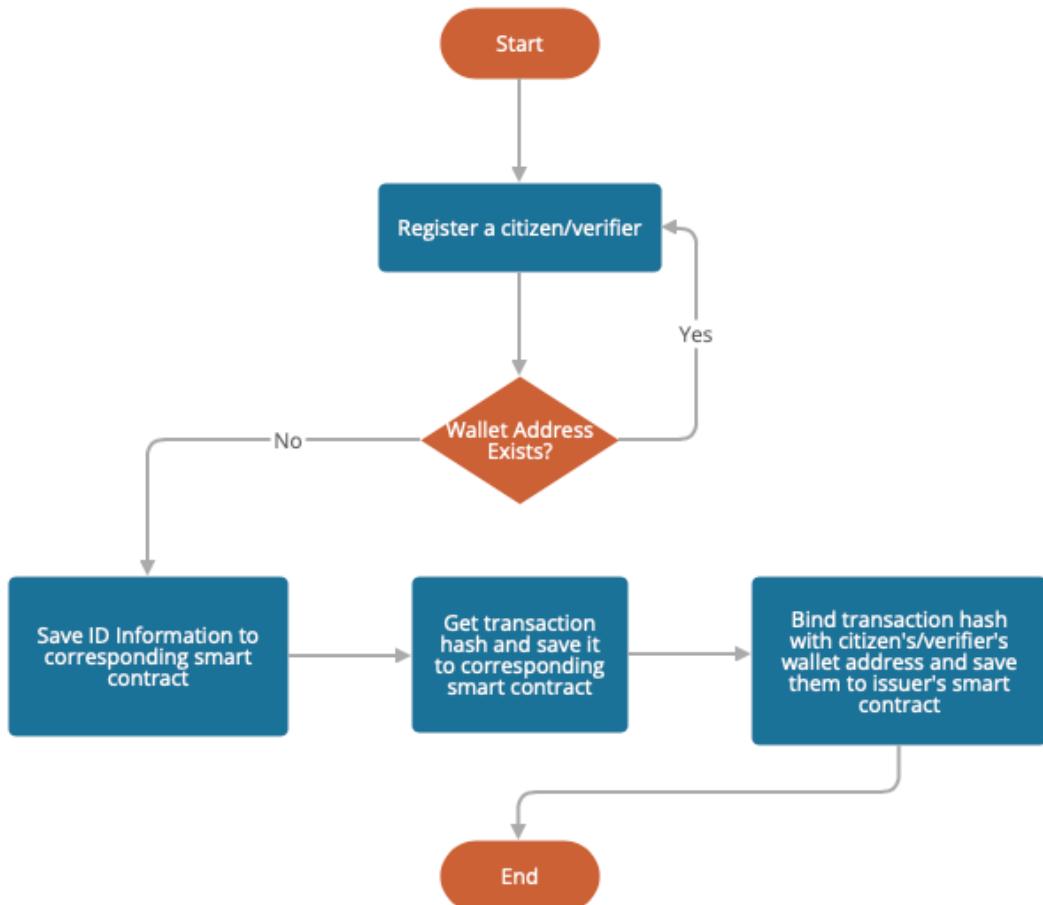
«Διάγραμμα Περίπτωσης», (Object Diagram / Instance Diagram) της Εικόνας 15, που παρουσιάζει διαγραμματικά, την εκτέλεση μιας πλήρους περίπτωσης χρήσης της εφαρμογής με πραγματικά δεδομένα (από την εγγραφή ενός χρήστη, έως την προσθήκη/δημιουργία ενός ιατρικού ιστορικού γι' αυτόν).



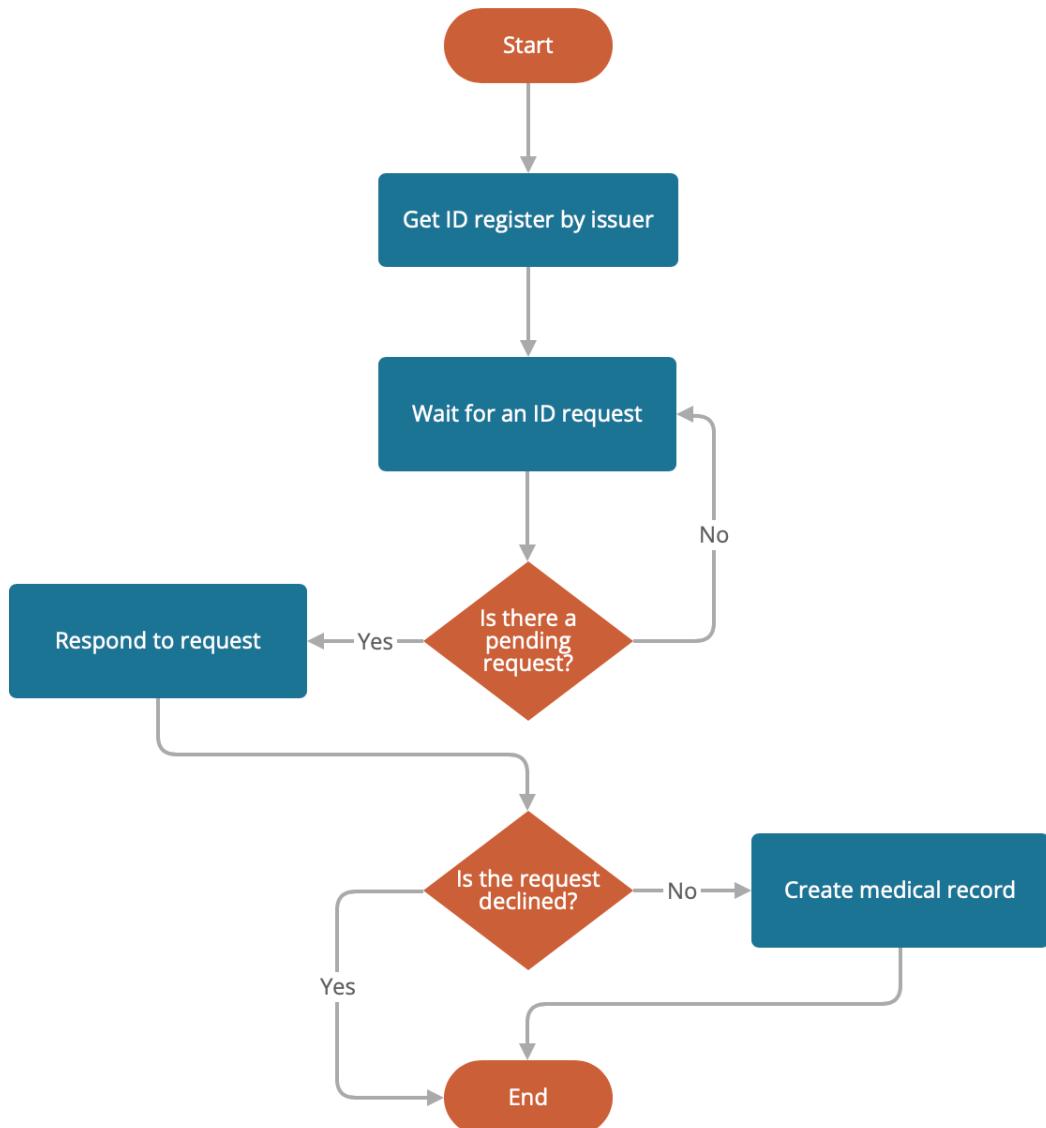
Εικόνα 15 - Διάγραμμα Αντικειμένου / Περίπτωσης (Object / Instance Diagram)

Η λειτουργία της εφαρμογής χαρακτηρίζεται από την απλότητα της δομής των υπολειτουργιών που τη συντελούν. Όπως γίνεται αντιληπτό στα παρακάτω «Διαγράμματα Ροής» (Flowcharts) (Εικόνες 16, 17, 18), τα βήματα των διαδικασιών που ακολουθούνται κατά την εκτέλεση της εφαρμογής, αναλόγως την περίπτωση χρήσης, έχουν συνταχθεί με τέτοιο τρόπο, ώστε να ωφελούν την σωστή ροή των δεδομένων καθ' όλη τη διάρκεια της λειτουργίας της. Ένα ακόμη χαρακτηριστικό των «Διαγραμμάτων Ροής» είναι πως οπτικοποιούν τις μεθόδους εκτέλεσης του κώδικα, παρουσιάζοντας τους τρόπους με τους οποίους έχει οργανωθεί. Τα προαναφερθέντα μπορούν να παρατηρηθούν και μέσω ενός «Διαγράμματος Δραστηριότητας» (Activity Diagram). Ενδεικτικά, στην Εικόνα 19, απεικονίζεται ένα διάγραμμα που

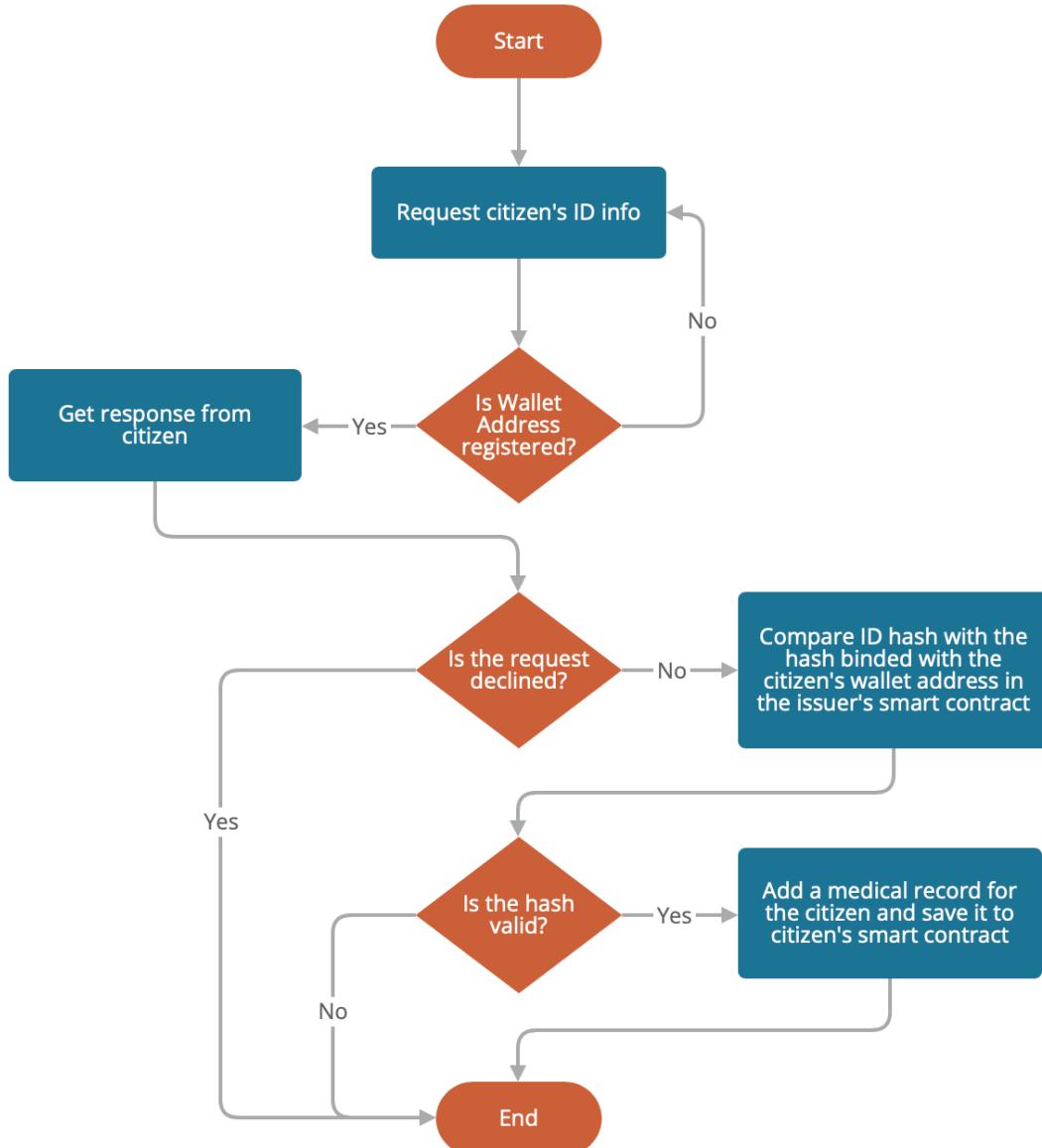
αντιπροσωπεύει το σύνολο των διαδικασιών και των βημάτων που εκτελούνται στην εφαρμογή από τους υπόλοιπους ρόλους και εμπεριέχει τη διαδικασία αιτήματος κοινοποίησης στοιχείων, επιβεβαίωσης κυριότητας και προσθήκης/δημιουργίας ιατρικού ιστορικού.



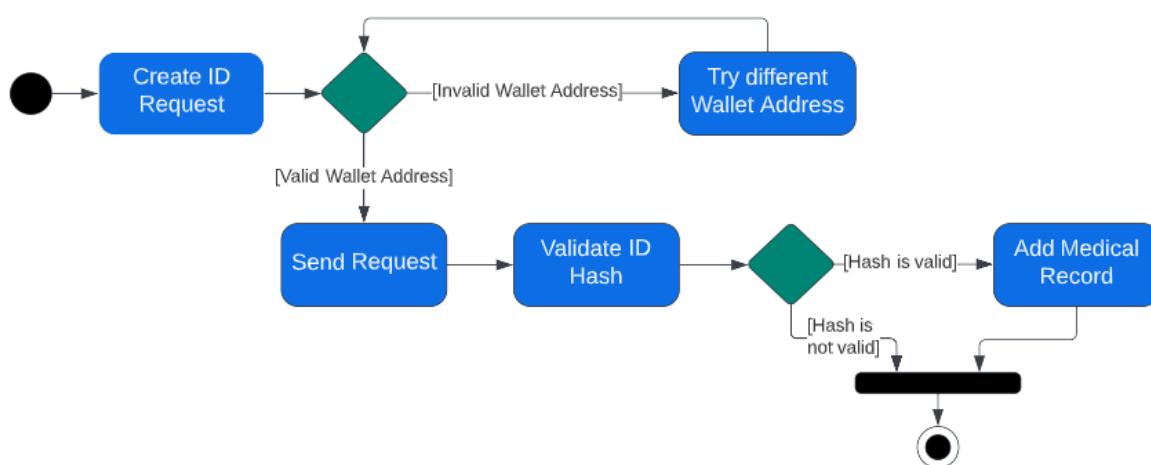
Εικόνα 16 - Διάγραμμα Ροής «Εκδότη» (Issuer Flowchart)



Εικόνα 17 - Διάγραμμα Ροής «Πολίτη» (Citizen Flowchart)

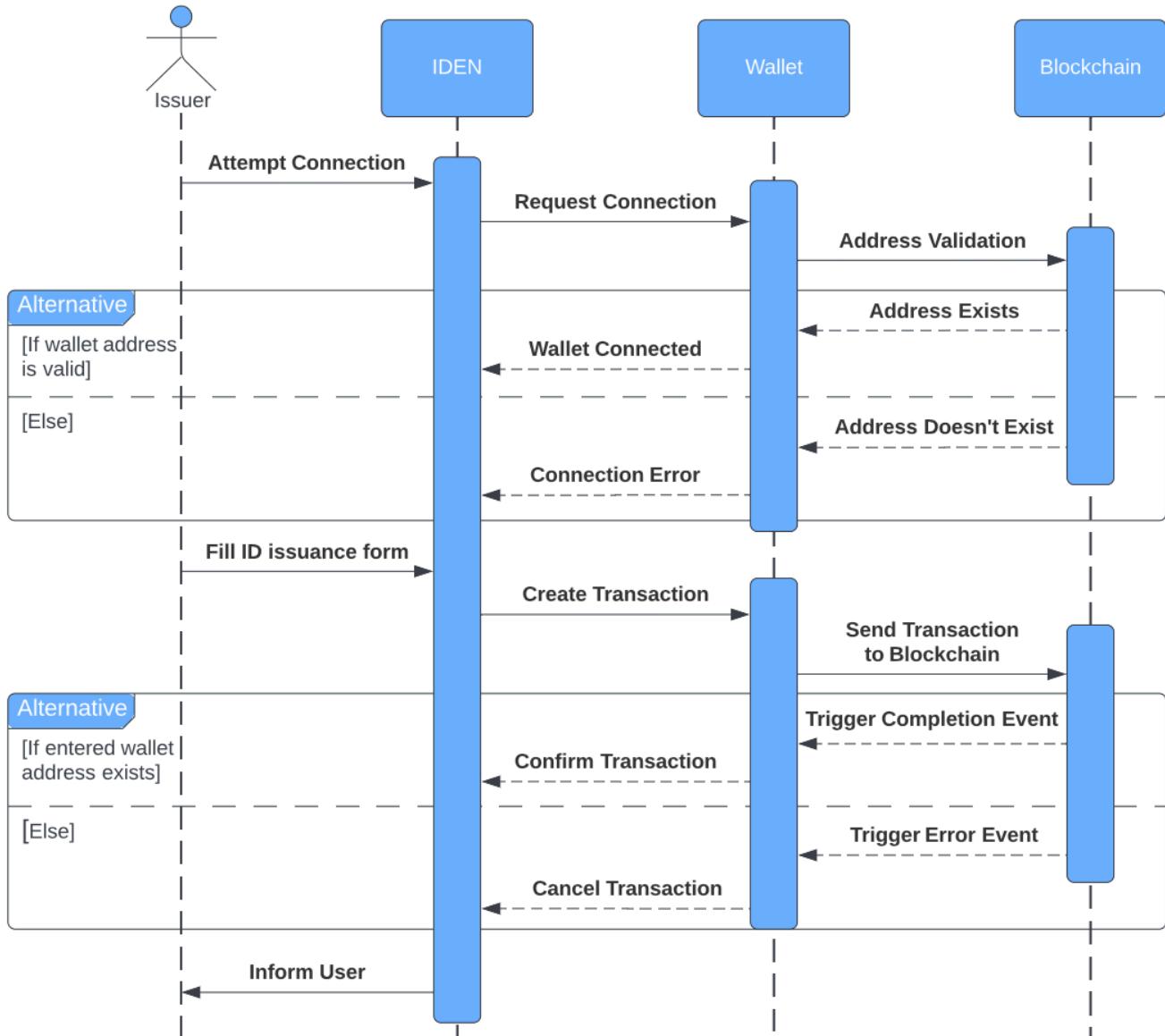


Εικόνα 18 - Διάγραμμα Ροής «Επαληθευτή» (Verifier Flowchart)



Εικόνα 19 - Διάγραμμα Δραστηριότητας «Επαληθευτή» (Verifier Activity Diagram)

Στην παρουσίαση του μοντέλου της εφαρμογής εντάσσεται και το «Διάγραμμα Ακολουθίας» (Sequence Diagram) (Εικόνα 20) που παρουσιάζει τον τρόπο και τη σειρά με την οποία ένας ρόλος, στη προκειμένη περίπτωση ο εκδότης, αλληλεπιδρά με τις βασικές λειτουργίες της εφαρμογής αλλά και το υπόβαθρο της («πορτοφόλι», δίκτυο Blockchain) σε βάθος χρόνου. Ομοίως με τον ρόλο του «Εκδότη», αλληλεπιδρούν και οι άλλοι δύο ρόλοι με τις βασικές λειτουργίες της εφαρμογής, συνεπώς αντιπροσωπεύονται από το παρακάτω διάγραμμα.



Εικόνα 20 - Διάγραμμα Ακολουθίας «Εκδότη» (Issuer Sequence Diagram)

Όσον αφορά στη σχεδίαση και την ανάπτυξη του περιβάλλοντος χρήστη, δόθηκε ιδιαίτερη έμφαση στην ευχρηστία της εφαρμογής και όχι στην εμφάνιση, καθώς απευθύνεται σε χρήστες όλων των επιπέδων. Όπως διακρίνεται και στις παρακάτω αντιπροσωπευτικές εικόνες (Εικόνα 21, 22, 23, 24), οι διαθέσιμες επιλογές της

εκάστοτε περίπτωσης είναι ευδιάκριτες, με σαφή βήματα για την ολοκλήρωση της επιθυμητής ενέργειας ενώ, σε περίπτωση σφάλματος ή παράλειψης ενός ή περισσότερων βημάτων, ο χρήστης ενημερώνεται μέσω μηνύματος που αποτρέπει τη συνέχεια εκτέλεσης της λειτουργίας. Αξίζει να σημειωθεί πως στην πραγματικότητα, τα μενού «Issuer» «Citizen» «Verifier» θα ήταν τρεις διαφορετικές διεπαφές της εφαρμογής, όμως για λόγους διευκόλυνσης της ανάπτυξης συμπεριλήφθηκαν σε μία.

IDEN

Issuer | **Citizen** | Verifier | Connected Wallet Address

ID Information

Full Name	name1
Mobile	mobile1
ID Issuer	address1
ID Hash	hash1

[Generate QR Code](#)

Notifications

Εικόνα 21 - Προσχέδιο σελίδας στοιχείων ταυτότητας "Πολίτη" (Citizen ID Page Mockup)

IDEN

Issuer | Citizen | **Verifier** | Connected Wallet Address

Citizen Wallet Address

QR Scanner

Citizen Information	
<input checked="" type="checkbox"/>	Full Name
<input checked="" type="checkbox"/>	Mobile
<input checked="" type="checkbox"/>	ID Issuer
<input checked="" type="checkbox"/>	ID Hash

[Submit](#)

Εικόνα 22 - Προσχέδιο σελίδας αίτησης στοιχείων ταυτότητας (ID Request Page Mockup)

IDEN

Issuer | Citizen | Verifier | Connected Wallet Address

Search Request by Wallet Address

Date Requested	Status	View Details
Date1	Approved	<input type="button" value="Button"/>
Date 2	Declined	<input type="button" value="Button"/>

Requested Information	
Full Name	name1
Mobile	mobile1
ID Issuer	address1
ID Hash	hash1

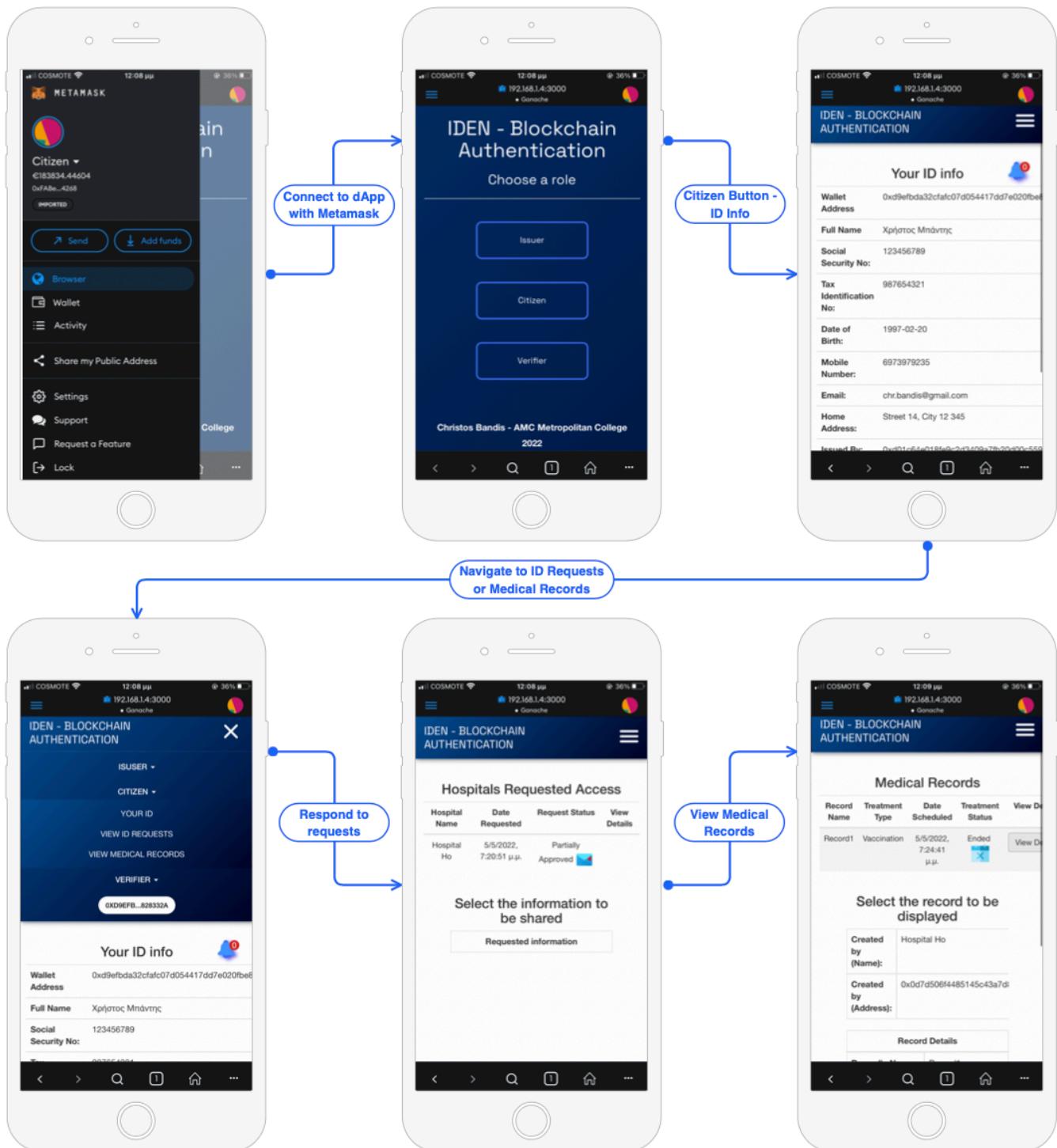
Εικόνα 23 - Προσχέδιο σελίδας διαχείρισης αιτημάτων ταυτότητας από τον "Επαληθευτή" (Verifier ID Request Management Page Mockup)

Record Information

Record Name	Placeholder
Treatment Type	Select ▾
Treatment	Placeholder
Doctor's Name	Placeholder
<input checked="" type="checkbox"/> Next Appointment	

Εικόνα 24 - Προσχέδιο παραθύρου καταχώρησης ιατρικού ιστορικού (Create medical record Window Mockup)

Όλα τα παραπάνω ισχύουν και για τις υπόλοιπες περιπτώσεις χρήσης της εφαρμογής, όπως είναι η εγγραφή ενός χρήστη και η απάντηση του πολίτη σε ένα αίτημα κοινοποίησης στοιχείων. Αξίζει να αναφερθεί η προσαρμογή της εμφάνισης της εφαρμογής σε όλους τους τύπους συσκευών, με χαρακτηριστικό παράδειγμα την Εικόνα 25, όπου παρουσιάζεται η «μακέτα» (Wireframe) της περίπτωσης χρήσης σύνδεσης του πολίτη στην εφαρμογή και της προβολής των αιτημάτων κοινοποίησης των στοιχείων του και του ιστορικού των ιατρικών του επισκέψεων.

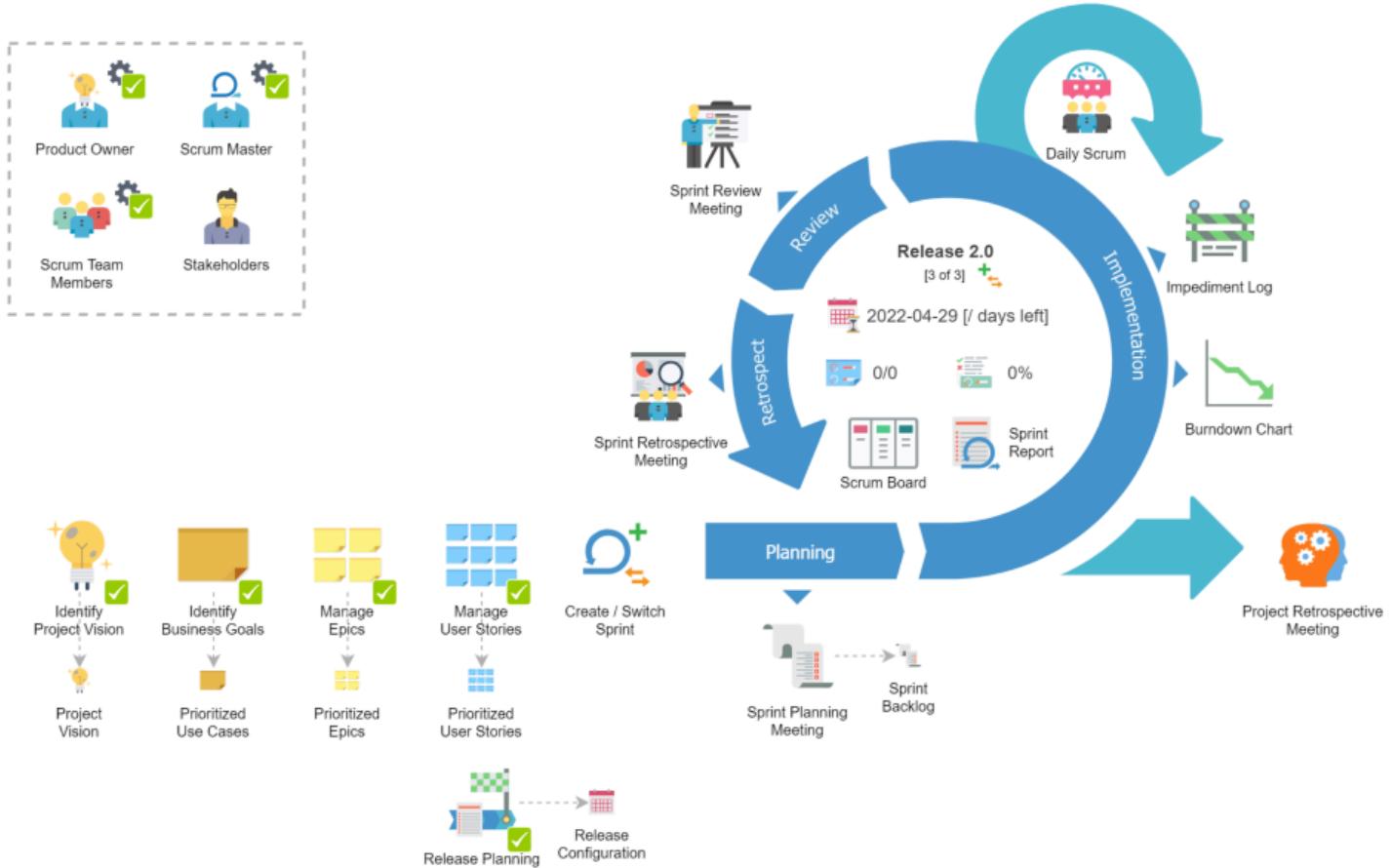


Εικόνα 25 – «Μακέτα» των περιπτώσεων χρήσης του «Πολίτη» σε κινητή συσκευή (Citizen Mobile Wireframe)

4.3. Μεθοδολογία

Προκειμένου να καταστεί δυνατή η εκπόνηση της παρούσας εργασίας, εφαρμόστηκε ένας ποιοτικός σχεδιασμός έρευνας που αφορά τη μελέτη και τη σύγκριση δημοσιευμένων εργασιών, βιβλίων, αλλά και επιστημονικών άρθρων γύρω από τον κλάδο του Blockchain και πιο συγκεκριμένα του Blockchain Authentication. Στη συνέχεια, εκμεταλλεύομενοι τις αξίες και τις αρχές της μεθοδολογίας «Agile», τέθηκε σε ισχύ η διαδικασία σταδιακής ανάπτυξης της εφαρμογής, η οποία χαρακτηρίστηκε από μία σειρά διηγεών ελέγχων και δοκιμών. Η μεθοδολογία αυτή επιλέχθηκε με γνώμονα την ευελιξία και τη συνεχή εξέλιξη που προσδίδει στη λήψη αποφάσεων αναφορικά με το μέλλον της ανάπτυξης της εφαρμογής και των λειτουργιών της.

Για την αντιμετώπιση των σύνθετων προβλημάτων που παρουσιάστηκαν κατά τη διαδικασία ανάπτυξης της εφαρμογής, έγινε χρήση του πλαισίου διαχείρισης «Scrum», που περιγράφει ένα σύνολο εργαλείων και ρόλων, στόχος των οποίων είναι η διευκόλυνση της δόμησης και της διαχείρισης έργων που επωφελούνται της μεθοδολογίας «Agile» (AppDividend, 2022). Τα διαγράμματα, οι αναφορές και οι πίνακες που ακολουθούν δημιουργήθηκαν μέσω της εφαρμογής «Visual Paradigm».



Εικόνα 26 - Εργαλείο διαχείρισης Scrum (Scrum Process Canvas)

4.3.1. Αναφορές

Product Owner Report

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

Πίνακας 1 - Αναφορά ιδιοκτήτη έργου

Scrum Master Report

Member	Χρήστος Μπάντης
Responsibilities	<ul style="list-style-type: none"> • Διευκολύνει τη δημιουργία των epics. • Συντονίζει τη δημιουργία του σχεδίου κυκλοφορίας. • Βοηθά στη διατήρηση του αρχείου καταγραφής αποτρεπτικών παραγόντων. • Διασφαλίζει ότι τα ζητήματα που επηρεάζουν την ανάπτυξη ανακαλύπτονται και επιλύονται.

Πίνακας 2 - Αναφορά "αρχηγού" των Scrum

Scrum Team Report

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

Πίνακας 3 - Αναφορά ομάδας Scrum

Project Charter

Ένα καταστατικό έργου (Project Charter) είναι ένα επίσημο, συνήθως σύντομο έγγραφο που περιγράφει το έργο στο σύνολό του (Wrike, 2019).

1. Project Vision

Το όραμα του έργου είναι η δημιουργία μιας εφαρμογής ταυτοποίησης μέσω της Τεχνολογίας Blockchain. Σε αντίθεση με τα ήδη υπάρχοντα συστήματα διαχείρισης ταυτότητας, η εφαρμογή θα παρέχει ασφαλή κρυπτογράφηση των δεδομένων και πλήρη διαχείριση των στοιχείων της ταυτότητας αποκλειστικά από τον κάτοχο της. Απευθύνεται σε όλους τους χρήστες που επιθυμούν να ασκήσουν το δικαίωμα τους στην ιδιωτικότητα και δεν επιθυμούν να βρίσκονται τα δεδομένα τους υπό τον έλεγχο δημόσιων ή ιδιωτικών οργανισμών.

2. Project Mission

Μέσω της τεχνολογίας του Blockchain, οι χρήστες της εφαρμογής θα έχουν τη δυνατότητα να διατηρούν τα προσωπικά τους δεδομένα εντός του ψηφιακού τους

«πορτοφολιού» στο Blockchain και θα έχουν τον πλήρη έλεγχο των στοιχείων που μοιράζονται στις περιπτώσεις που ζητείται επαλήθευση τους από μια άλλη οντότητα. Ονομαστικά, ορισμένοι από τους βασικούς στόχους της εφαρμογής είναι:

- Αποκεντρωποίηση των μεθόδων ταυτοποίησης.
- Κρυπτογράφηση των δεδομένων αλλά και των συναλλαγών μεταξύ πολιτών και οργανισμών.
- Αποφυγή της χρήσης προσωπικών δεδομένων για διαφημιστικούς σκοπούς.
- Διασφάλιση του απορρήτου των χρηστών.

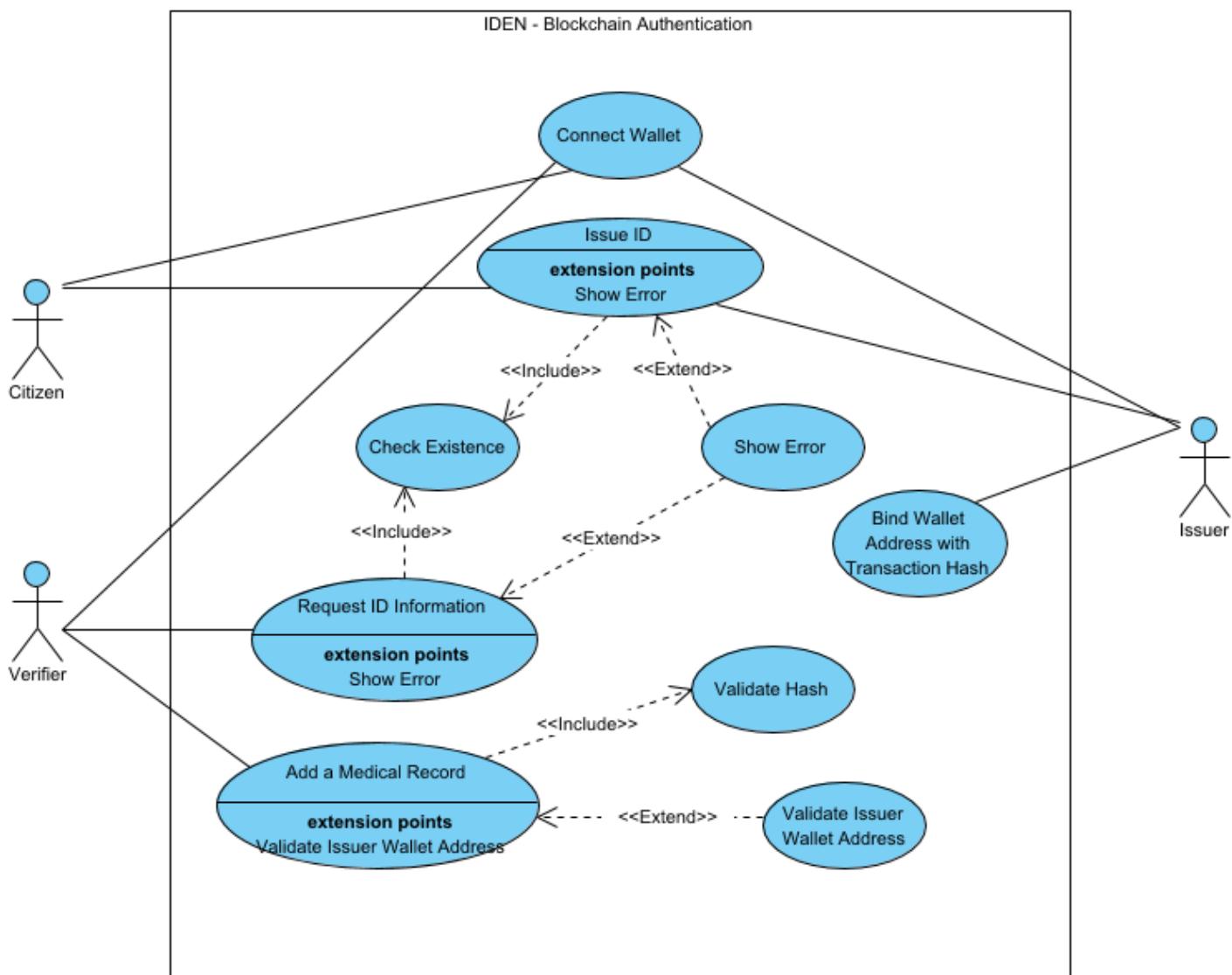
3. Project Success Criteria

Η επιτυχία της εφαρμογής θα εξαρτηθεί από τα κριτήρια της ασφάλειας και της ταχύτητας των συναλλαγών, αρχικά σε περιόδους δοκιμών και στη συνέχεια όταν δημοσιευτεί σε ένα δημόσιο Blockchain δοκιμών. Επίσης, καίριας σημασίας κριτήριο είναι η ευχρηστία της εφαρμογής από χρήστες κάθε επιπέδου εμπειρίας αλλά και η προσαρμοστικότητα του περιβάλλοντος χρήστη της σε πληθώρα συσκευών.

Use Case Report

1. Use Case Diagram

Στο παρακάτω διάγραμμα περίπτωσης χρήσης (Use Case Diagram) (Εικόνα 27) παρουσιάζεται μία γενική περίπτωση χρήσης που περιλαμβάνει όλες τις λειτουργίες της εφαρμογής, από τη σύνδεση του κάθε χρήστη στο σύστημα και τη δημιουργία της ταυτότητας του πολίτη και του επαληθευτή, μέχρι την αποστολή αιτήματος κοινοποίησης στοιχείων ταυτότητας, την επιβεβαίωση της κυριότητάς τους και την προσθήκη/δημιουργία ενός ιατρικού ιστορικού από τον επαληθευτή.



Εικόνα 27 - Διάγραμμα περίπτωσης χρήσης (Use Case Diagram)

2. Prioritized Use Cases

Η ιεράρχηση των περιπτώσεων χρήσης (Use Cases Prioritization) είναι μια μέθοδος με την οποία οι επιχειρήσεις μπορούν να εντοπίσουν πιθανές περιπτώσεις χρήσης, να αναλύσουν την επιχειρηματική αξία που προκύπτει από αυτές και να τις κατατάξουν με βάση τις επιπτώσεις που έχουν στους στρατηγικούς τους στόχους (Mishra, 2021). Στον παρακάτω πίνακα η στήλη «Priority» υποδηλώνει τη σημαντικότητα των περιπτώσεων σε σχέση με την παροχή μεγαλύτερων και αμεσότερων επιχειρηματικών οφελών, η στήλη «Size» περιέχει μια υποκειμενική αξιολόγηση της προσπάθειας που απαιτείται για την υποστήριξη της κάθε περίπτωσης και η στήλη «Complexity» περιλαμβάνει μια υποκειμενική αξιολόγηση της σχετικής δυσκολίας στην υποστήριξη της κάθε περίπτωσης.

Name	Description	Priority	Size	Complexity
Validate Hash	Σύγκριση και επικύρωση του «hash» των παρεχόμενων στοιχείων ταυτότητας του πολίτη με το «hash» αντιστοιχήθηκε με τη διεύθυνση του στο «έξυπνο» συμβόλαιο του εκδότη.	Must	Very Large	High
Validate Issuer Wallet Address	Επαλήθευση της διεύθυνσης του εκδότη στο Blockchain με στόχο την εγκυρότητα των κοινοποιηθέντων δεδομένων.	Should	Large	High
Check Existence	1) Ο εκδότης ελέγχει αν υφίσταται στο Blockchain η διεύθυνση που παρέχει ο πολίτης κατά την εγγραφή. 2) Ο επαληθευτής ελέγχει αν υφίσταται στο Blockchain η διεύθυνση που παρέχει ο πολίτης κατά το αίτημα κοινοποίησης στοιχείων ταυτότητας.	Must	Medium	Medium
Bind Wallet Address with Transaction Hash	Ο εκδότης αντιστοιχίζει την παρεχόμενη διεύθυνση πορτοφολιού του πολίτη με το «hash» της συναλλαγής δημιουργίας ταυτότητας και «αποθηκεύει» το αποτέλεσμα στο «χώρο» αποθήκευσης του «έξυπνου» συμβολαίου του.	Must	Medium	Medium
Add a Medical Record	Προσθήκη/Δημιουργία ιατρικού ιστορικού για τον πολίτη.	Should	Medium	Medium
Request ID Information	Ο επαληθευτής αποστέλλει στον πολίτη αίτημα κοινοποίησης των επιλεγμένων στοιχείων ταυτότητας.	Must	Small	Low
Issue ID	Έκδοση ταυτότητας για τον πολίτη ή τον επαληθευτή.	Must	Small	Low

Connect Wallet	Ο χρήστης συνδέεται στην εφαρμογή μέσω του ψηφιακού «πορτοφολιού» του.	Must	Very Small	Low
Show Error	Εμφάνιση σφάλματος αν η παρεχόμενη, από τον πολίτη, διεύθυνση δεν υφίσταται στο Blockchain.	Should	Very Small	Low

Πίνακας 4 - Ιεράρχηση περιπτώσεων χρήσης (Use Case Prioritization)

Epics Report

Τα «Epics» είναι υψηλού επιπέδου λειτουργικότητας ή γενικώς καθορισμένες απαιτήσεις. Μπορούν να χωριστούν σε μικρότερα κομμάτια, που ονομάζονται «User Stories». Στο παρακάτω πίνακα η στήλη «Priority» περιλαμβάνει τον βαθμό σημαντικότητας των «epics» αναφορικά με την παροχή μεγαλύτερων και αμεσότερων επιχειρηματικών οφελών ενώ, η στήλη «Risk» αντιπροσωπεύει το επίπεδο αβεβαιότητας γύρω από την επιτυχή ολοκλήρωση ενός «epic».

Name	Description	Parent Use Case	Priority	Risk
Προσθήκη/Δημιουργία ιατρικού ιστορικού	Εμφάνιση παραθύρου συναλλαγής προσθήκης/δημιουργίας ιατρικού ιστορικού και αποθήκευσης των δεδομένων στο «πορτοφόλι» του πολίτη	Add a Medical Record	Should	Low
Εμφάνιση σφάλματος	Εμφάνιση σφάλματος αν η παρεχόμενη, από τον πολίτη, διεύθυνση δεν υφίσταται στο Blockchain.	Show Error	Could	Low
Καταχώρηση στοιχείων ταυτότητας	Εμφάνιση παραθύρου συναλλαγής για την κατοχύρωση της ταυτότητας πολίτη ή επαληθευτή.	Issue ID	Must	High
Επαλήθευση παρεχόμενου «hash»	Σύγκριση του «hash» των παρεχόμενων στοιχείων ταυτότητας του πολίτη με το «hash» που έχει αντιστοιχηθεί με τη	Validate Hash	Must	Medium

	διεύθυνση του στο «έξυπνο» συμβόλαιο του εκδότη.			
Σύνδεση στην εφαρμογή	Εμφάνιση παραθύρου διαλόγου για τη σύνδεση του χρήστη από την εφαρμογή του «πορτοφολιού».	Connect Wallet	Must	Low
Επιλογή επιθυμητών στοιχείων	Μετά την επιβεβαίωση της ύπαρξης της παρεχόμενης διεύθυνσης του πολίτη, ο επαληθευτής επιλέγει τα στοιχεία της ταυτότητας του πολίτη που επιθυμεί να ελέγξει.	Request ID Information	Must	Medium
Αποστολή αιτήματος	Εμφάνιση παραθύρου συναλλαγής για την αποστολή του αιτήματος στον πολίτη.	Request ID Information	Must	Medium
Επαλήθευση διεύθυνσης εκδότη	Σύγκριση της διεύθυνσης του εκδότη της ταυτότητας με μία λίστα γνωστών διευθύνσεων, όταν αυτή ζητηθεί από το εκάστοτε αίτημα.	Validate Issuer Wallet Address	Should	Medium
Έλεγχος ύπαρξης διεύθυνσης	Έλεγχος αν η παρεχόμενη, κατά την εγγραφή ή το αίτημα κοινοποίησης, διεύθυνση πολίτη υφίσταται στο Blockchain.	Check Existence	Must	Low
Αντιστοίχιση διεύθυνσης με το «hash»	Αντιστοίχιση και «αποθήκευση» της διεύθυνσης του πολίτη με το «hash» της ταυτότητας του σε μορφή «κλειδιού-τιμής».	Bind Wallet Address with Transaction Hash	Must	Low

Πίνακας 5 - Αναφορά των «Epics»

Product Backlog

Το «Product Backlog» είναι ένας εξελισσόμενος, ταξινομημένος κατάλογος που περιέχει οτιδήποτε απαιτείται για τη βελτίωση του προϊόντος (Scrum.org, 2016).

1. User Story Map

Η χαρτογράφηση ιστοριών χρήστη (User Story Mapping) είναι μια λιτή, σχεδιαστική μέθοδος αντιστοίχισης που περιγράφει τις, αναμενόμενες από την ομάδα Scrum, ενέργειες που εκτελούν οι χρήστες, με σκοπό την ολοκλήρωση των στόχων τους σε ένα ψηφιακό προϊόν (Kaley, 2021).

General Activity	Connect Wallet	Issue ID	Bind Wallet Address with Transaction	Check Existence	Show Error	Request ID Information		Validate Hash	Validate Issuer Wallet Address	Add a Medical Record
General Epic	Σύνδεση στην εφαρμογή	Καταχώρηση στοιχείων ταυτότητας	Αντιστοίχιση διεύθυνσης με το "hash"	Ελεγχος ύπαρξης διεύθυνσης	Εμφάνιση σφαλμάτος	Επιλογή επιθυμητών στοιχείων	Αποστολή αιτήματος	Επαλήθευση παρεχόμενου "hash"	Επαλήθευση διεύθυνσης εκδότη	Δημιουργία ιατρικού συμβάντος

Release 1.0 04/15/2022



Release 2.0 04/29/2022



Unscheduled

Εικόνα 28 - User Story Map

2. Prioritized User Stories

Η ιεράρχηση των «User Stories» αναφέρεται στην ομόφωνη απόφαση των μελών της ομάδας Scrum ως προς την οργάνωση των χαρακτηριστικών του προϊόντος. Η οργάνωση των ιστοριών ξεκινά από τα πιο σημαντικά χαρακτηριστικά, ώστε το προϊόν να εξέλθει στην αγορά το συντομότερο δυνατό (CardBoard, 2020). Κάθε «User Story» έχει ένα σχετιζόμενο κριτήριο αποδοχής (Acceptance Criteria) που καθορίζει την ολοκλήρωση του. Τα κριτήρια αποδοχής παρέχουν σαφήνεια στην ομάδα σχετικά με τι αναμένεται από μια ιστορία χρήστη, «αφαιρούν» την ασάφεια από τις απαιτήσεις και βοηθούν στην διαμόρφωση των προσδοκιών. Οι «πόντοι» της ιστορίας (Story Points) είναι ένας αριθμός που αντιπροσωπεύει μια εκτίμηση του συνολικού μεγέθους μιας ιστορίας χρήστη. Το συνολικό μέγεθος μιας ιστορίας χρήστη αξιολογείται λαμβάνοντας υπόψη τον κίνδυνο, το ποσοστό της απαιτούμενης προσπάθειας και το επίπεδο πολυπλοκότητας της.

Name	Description	Epic	Status	Acceptance Criteria	Story Points	Priority	Risk
Σάρωση κωδικού QR διεύθυνσης	Ως εκδότης / επαληθευτής, επιθυμώ την επιλογή σάρωσης του κωδικού QR μιας διεύθυνσης «πορτοφολιού» πολίτη στο πλαίσιο πληκτρολόγησης της.	Καταχώρηση στοιχείων ταυτότητας	Approved	Ο εκδότης ή ο επαληθευτής θα πρέπει να έχουν την επιλογή σάρωσης κωδικού QR στο πλαίσιο εισαγωγής διεύθυνσης πολίτη.	2	Should	Low
Δημιουργία κωδικού QR διεύθυνσης	Ως κάτοχος ταυτότητας, επιθυμώ την εξαγωγή ενός κωδικού QR αποτελουμένου από τη διεύθυνση του «πορτοφολιού» μου.	General Epic	Approved	Ο κάτοχος θα πρέπει να έχει την επιλογή εξαγωγής κωδικού QR κάτω από το πλαίσιο που περιέχει τα στοιχεία ταυτότητας του.	2	Should	Low
Εμφάνιση ειδοποίησης στον πολίτη	Ως κάτοχος ταυτότητας, επιθυμώ να ενημερώνομαι όταν υπάρχει αίτημα κοινοποίησης στοιχείων που δεν έχει απαντηθεί.	Επιλογή επιθυμητών στοιχείων	Approved	Οι νέες ειδοποιήσεις θα πρέπει να φαίνονται στην αρχική σελίδα του πολίτη.	2	Should	Low
Βελτιστοποίηση κώδικα επαλήθευσης	Ως επαληθευτής, επιθυμώ να είμαι σίγουρος για τα στοιχεία ταυτότητας	Επαλήθευση παρεχόμενου «hash»	Approved	Χρήση κατάλληλης μεθόδου για την σύγκριση και	5	Must	High

	που κοινοποιεί σε μένα ένας πολίτης.			επαλήθευση του «hash» της ταυτότητας του πολίτη.			
Επιλογή επόμενης επίσκεψης	Ως πολίτης, επιθυμώ να έχω την επιλογή επόμενης επίσκεψης, όταν αυτή είναι απαραίτητη.	Προσθήκη/ Δημιουργία ιατρικού ιστορικού	Approved	Κατά τη προσθήκη/ δημιουργία ενός ιατρικού ιστορικού θα πρέπει να υπάρχει η επιλογή επόμενης επίσκεψης.	3	Should	Low
Προσθήκη τύπων θεραπείας	Ως πολίτης, επιθυμώ να υπάρχει κάλυψη πληθώρας περιπτώσεων από το νοσοκομείο που έχει αναλάβει την περίθαλψη μου.	Προσθήκη/ Δημιουργία ιατρικού ιστορικού	Approved	Κατά τη προσθήκη/ δημιουργία ενός ιατρικού ιστορικού θα πρέπει να υπάρχει λίστα με διαθέσιμες επιλογές θεραπείας.	3	Should	Low
Εμφάνιση παραθύρου σύνδεσης	Ως χρήστης, επιθυμώ να συνδέομαι άμεσα και εύκολα στην εφαρμογή.	Σύνδεση στην εφαρμογή	Approved	Κατά την επίσκεψη στην εφαρμογή θα πρέπει να εμφανίζεται αυτόμata το παράθυρο σύνδεσης στην εφαρμογή από	1	Must	Low

				την εφαρμογή του «πορτοφολιού».			
Δημιουργία σχέσης κλειδιού-τιμής	Ως εκδότης, επιθυμώ να διατηρήσω, για λόγους ασφαλείας, μια λίστα με τις διευθύνσεις και τα «hash» των εγγραφών που έχω πραγματοποιήσει.	Αντιστοίχιση διεύθυνσης με το «hash»	Approved	Διαμόρφωση του κώδικα του «έξυπνου» συμβολαίου του εκδότη, με σκοπό να υποστηρίζει μια τέτοια λειτουργία.	2	Must	Medium
Αναζήτηση στη «μνήμη» του «έξυπνου» συμβολαίου	Ως εκδότης / επαληθευτής επιθυμώ να πραγματοποιώ ενέργειες μόνο για υφιστάμενες διευθύνσεις πολιτών.	Έλεγχος ύπαρξης διεύθυνσης	Approved	Έλεγχος της διεύθυνσης που παρέχεται από τον πολίτη, προτού εκτελεστεί οποιαδήποτε ενέργεια.	2	Must	Medium
Χρήση μεθόδου alert της Javascript	Ως χρήστης της εφαρμογής, επιθυμώ να ενημερώνομαι για οποιοδήποτε συμβάν λαμβάνει χώρα κατά τη «παραμονή» μου σε αυτή.	Εμφάνιση σφάλματος	Approved	Εμφάνιση μηνύματος για οτιδήποτε συμβεί κατά τη χρήση της εφαρμογής.	1	Should	Low
Εμφάνιση παραθύρου συναλλαγής	Ως χρήστης της εφαρμογής, επιθυμώ να εμφανίζεται αυτόματα το παράθυρο	Αποστολή αιτήματος	Approved	Κατά την αίτηση μιας συναλλαγής θα πρέπει να εμφανίζεται αυτόματα το	1	Must	Low

	διεκπεραίωσης συναλλαγής.			αντίστοιχο παράθυρο διαλόγου.			
Σύγκριση διεύθυνσης με ήδη γνωστές	Ως επαληθευτής, επιθυμώ να επιβεβαιώνω την κυριότητα μιας ταυτότητας, όχι μόνο με την επαλήθευση του «hash» της, αλλά και με τη διεύθυνση του εκδότη της.	Επαλήθευση διεύθυνσης εκδότη	Approved	Έλεγχος της διεύθυνσης «πορτοφολιού» του εκδότη, όταν αυτή ζητείται, συγκρίνοντας την με αυτές που περιέχονται σε μία λίστα γνωστών διευθύνσεων.	4	Must	High

Πίνακας 6 - Ιεράρχηση ιστοριών χρήστη (User Stories Prioritization)

Release Plan

Ένα σχέδιο κυκλοφορίας (Release Plan) επιτρέπει στην ομάδα Scrum να έχει μια επισκόπηση των κυκλοφοριών και του χρονοδιαγράμματος παράδοσης για το προϊόν που αναπτύσσει, έτσι ώστε να μπορούν να συμμορφωθούν με τις προσδοκίες του ιδιοκτήτη του προϊόντος.

1. Project Deliverables

Ένα παραδοτέο (Deliverable) είναι ένα υλικό ή άνλο αγαθό ή υπηρεσία που πρόκειται να παραχθεί κατά τη διάρκεια ενός έργου.

Deliverable	Description	Planned Release Date	Priority	Status	Owner
Αρχικό μοντέλο της εφαρμογής αποκεντρωμένης ταυτοποίησης	Μοντέλο εφαρμογής που εκμεταλλεύεται τα οφέλη της τεχνολογίας του Blockchain με σκοπό την ορθότερη διαχείριση των προσωπικών δεδομένων και την αποφυγή κατάχρησής τους.	2022-04-01	High	Done	Χρήστος Μπάντης

Πίνακας 7 - Παραδοτέα έργου (Project Deliverables)

2. Release Configuration

Release	Description	Planned Release Date
Release 1.0	Πλήρως λειτουργική εφαρμογή, βασιζόμενη στο μοντέλο εφαρμογής που παρουσιάστηκε στο παραδοτέο.	2022-04-15
Release 2.0	Εμπλουτισμός της εφαρμογής με νέες λειτουργίες και μετονομασία της σε «IDEN - Blockchain Authentication»	2022-04-29

Πίνακας 8 - Κυκλοφορίες - Εκδόσεις έργου (Project Releases)

4.4. Ανάλυση δομής

Έπειτα από συνεχή μελέτη και δοκιμές, ορίστηκε η αποδοτικότερη μέθοδος περάτωσης του έργου και τα εργαλεία που συντέλεσαν στην υλοποίηση της εφαρμογής. Η ανάπτυξή της, βασίστηκε σε ένα τοπικό δίκτυο Blockchain, οι κόμβοι του οποίου επικοινωνούσαν με την εφαρμογή μέσω μιας «βιβλιοθήκης» της γλώσσας προγραμματισμού «Javascript» ενώ, για την συγγραφή των «έξυπνων» συμβολαίων έγινε χρήση της γλώσσας προγραμματισμού «Solidity». Για την εκτέλεση του κώδικα, κρίθηκε απαραίτητη η ύπαρξη του περιβάλλοντος εκτέλεσης «Node.js», το οποίο περιλάμβανε υποεφαρμογές που συντέλεσαν στη διευκόλυνση των απαιτούμενων διεργασιών.

Αναλυτικότερα, η σύνδεση στο Blockchain επιτυγχάνεται μέσω ενός «REST API» (μέθοδος επικοινωνίας μεταξύ συστημάτων), το οποίο «επιστρέφει» ένα αρχείο «JSON» (JavaScript Object Notation), που περιέχει όλα τα στοιχεία που συντελούν ένα «έξυπνο» συμβόλαιο. Κατά την ανάπτυξη των σύγχρονων αποκεντρωμένων εφαρμογών, είθισται να χρησιμοποιείται μια «βιβλιοθήκη» της εκάστοτε γλώσσας προγραμματισμού, η οποία περιέχει έτοιμες μεθόδους και διαδικασίες που διευκολύνουν την επικοινωνία με το Blockchain, εξυπηρετώντας κυρίως, στην κωδικοποίηση (encoding) και αποκωδικοποίηση (decoding) των αρχείων «JSON». Για την ανάπτυξη της παρούσας εργασίας έγινε χρήση της «βιβλιοθήκης» «Web3.js» της γλώσσας προγραμματισμού «Javascript».

Αναφορικά με τα «έξυπνα» συμβόλαια, πέραν της «Solidity» υπάρχουν κι άλλες γλώσσες για την ανάπτυξη τους, οι οποίες στο σύνολο τους «μεταγλωτίζονται» σε «bytecode» (τύπος δυαδικού κώδικα) που απευθύνεται σε «EVM» (Deol and Wiesner, 2021). Το «EVM» (Ethereum Virtual Machine), όπως αναφέρθηκε και στο Κεφάλαιο 2.3, είναι μία «εικονική μηχανή» (virtual machine) «τοποθετημένη» στον πυρήνα του Ethereum Blockchain, που σκοπός της είναι η ερμηνεία και η εκτέλεση του κώδικα των έξυπνων συμβολαίων. Ονομαστικά, ορισμένες γλώσσες προγραμματισμού «έξυπνων» συμβολαίων είναι οι: Solidity, Vyper, LLL και Mutan, με τη Solidity να είναι η δημοφιλέστερη εξ αυτών.

Η υποβόσκουσα αρχιτεκτονική του «μεταγλωτιστή» (compiler) της «Solidity» προέρχεται από το ECMAScript (European Computer Manufacturers Association Script) και λόγω αυτού πολλοί συγκρίνουν την εμφάνισή της με αυτή της «Javascript». Ο κώδικας ενός «έξυπνου» συμβολαίου ξεκινά με τη δήλωση του τύπου αδείας

πνευματικών δικαιωμάτων που τον χαρακτηρίζει. Έπειτα, συναντάται η φράση «*pragma solidity*» και η έκδοση του «μεταγλωττιστή». Αυτή η γραμμή κώδικα είναι ήδη «μεταγλωτισμένη» (pre compiled statement) και δεν χρήζει επαναμεταγλωττισης σε κάθε εκτέλεση. Σκοπός της είναι η κατοχύρωση της έκδοσης του «μεταγλωττιστή», χαρακτηριστικό που ενισχύει σημαντικά την ασφάλεια, διασφαλίζοντας πως ο κώδικας του «έξυπνου» συμβολαίου δε θα είναι ασταθής, παρά τις μελλοντικές αλλαγές που μπορεί να εφαρμοστούν στη δομή της γλώσσας (Deol and Wiesner, 2021). Κατά τη διάρκεια ανάπτυξης της εφαρμογής, η πιο πρόσφατη έκδοση της «Solidity» ήταν η «0.8.13» ενώ, το σύμβολο «^» που διακρίνεται στην Εικόνα 29, σημαίνει πως ο κώδικας του έξυπνου συμβολαίου μπορεί να επεξεργαστεί από «μεταγλωττιστές» της συγκεκριμένης έκδοσης και των μετέπειτα εκδόσεων. Ολοκληρώνοντας, συνεχίζεται με το όνομα του «έξυπνου» συμβολαίου, το οποίο ξεκινά με κεφαλαίο γράμμα και ακολουθείται από αγκύλες, που περιέχουν τον κύριο κώδικα του συμβολαίου.

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.13;
3
4 contract Issuer {
5

```

Εικόνα 29 - Υπόδειγμα έναρξης κώδικα σε γλώσσα «Solidity»

Η διαδικασία συγγραφής των «έξυπνων» συμβολαίων διενεργήθηκε με τέτοιο τρόπο, ώστε να εκτελούνται στο Blockchain μόνο οι βασικές ενέργειες και μέθοδοι που είναι απαραίτητες για τη λειτουργία της εφαρμογής. Ο λόγος που επιλέχθηκε αυτή η μέθοδος, είναι πως η αποθήκευση μεγάλου όγκου δεδομένων σε ένα Blockchain, όπως το Ethereum, «έρχεται» σε συνδυασμό με μεγάλο χρηματικό κόστος. Όπως αναφέρθηκε στο Κεφάλαιο 2, η λειτουργία των δημόσιων Blockchain εξαρτάται από τη χρήση ενός εγγενούς διακριτικού (native token). Το «Yellow Paper» του Ethereum αναφέρει πως για την αποθήκευση μια λέξης αποτελούμενης από 256 bit καταναλώνονται 20.000 gas (το «καύσιμο» που χρησιμοποιείται για τις συναλλαγές εντός του Blockchain) (JAXenter, 2019). Μετατρέποντας αυτά τα bit σε byte (8 bits = 1 byte), συμπεραίνεται πως το μέγεθος της συγκεκριμένης λέξης είναι 32 bytes. Συνεπώς, για την αποθήκευση ενός (1) kilobyte ($1024 \text{ bytes} - 1024 / 32 = 32$ λέξεις) θα χρειαστούν $32 * 20.000 = 640.000$ gas. Καθώς η χρήση του Blockchain και η τιμή

του κρυπτονομίσματος του Ethereum μεταβάλλονται συνεχώς, δεν υφίσταται «οικονομικότερη» μέθοδος αποθήκευσης για το συγκεκριμένο δίκτυο. Λόγου χάριν, τη στιγμή συγγραφής του παρόντος κειμένου (Μάϊος 2022), η τιμή του «καυσίμου» κυμαίνεται στα 52 «gwei» (μικρότερη μονάδα μέτρησης του Ethereum), ή αλλιώς στα 0,0000000679 «ETH» (1 gwei αντιστοιχεί σε 0,00000000130 Ethereum – ETH). Βάσει αυτού, η αποθήκευση ενός kilobyte δεδομένων θα κόστιζε κατά μέσο όρο 640.000 * 0,0000000679 = 0,043456 ETH, ή 79,23€ με τη τρέχουσα ισοτιμία ETH/EUR.

Εν κατακλείδι, εκτός των ελέγχων που διεκπεραιώνονται με τη χρήση της γλώσσας «Javascript» σε επίπεδο περιηγητή (browser), οι μέθοδοι των «έξυπνων» συμβολαίων έχουν «σχεδιαστεί» με τέτοιο τρόπο, ώστε να εξετάζονται τα γνωρίσματα τους (function attributes), πριν την εκτέλεση οποιουδήποτε κώδικα και στη συνέχεια, να ενεργοποιείται ένα «συμβάν» (event) που αποστέλλει το κατάλληλο μήνυμα, όπου αυτό απαιτείται. Πιο συγκεκριμένα, στο επίπεδο των «έξυπνων» συμβολαίων πραγματοποιείται έλεγχος αντιστοίχισης μιας διεύθυνσης «πορτοφολιού» σε μία ήδη υπάρχουσα ταυτότητα «πολίτη» ή «επαληθευτή», διαδικασία καίριας σημασίας, καθώς οι διευθύνσεις των «πορτοφολιών» αποτελούν βασικό στοιχείο του κορμού της λειτουργίας της εφαρμογής. Ακόμη, στη δομή του έργου περιλαμβάνεται ένα «έξυπνο» συμβόλαιο με την ονομασία «Ownable», το οποίο αφορά τις διευθύνσεις «πορτοφολιών» των «εκδοτών». Βασικός σκοπός του είναι η εφαρμογή ενός κανόνα (modifier) στις μεθόδους (functions) των υπολοίπων «έξυπνων» συμβολαίων, που επιτρέπει την εκτέλεση τους μόνο από τον κάτοχο μίας εξ αυτών των διευθύνσεων. Κατ’ αυτόν τον τρόπο ενισχύεται η ασφάλεια του συστήματος, διότι σε περίπτωση που κάποιος κακόβουλος χρήστης εμπλακεί στη λειτουργία της εφαρμογής και επιχειρήσει να προβεί σε οποιαδήποτε ενέργεια, αυτομάτως οι εκκρεμείς συναλλαγές αποσύρονται (rollback) και δεν ολοκληρώνονται ποτέ. Στα αρχεία του έργου, που συνοδεύει την εργασία, έχει αφαιρεθεί ο κανόνας αυτός, όχι όμως το ίδιο το «έξυπνο» συμβόλαιο, καθώς κατά την εκκίνηση της εφαρμογής «Ganache» για τη ενεργοποίηση ενός τοπικού Blockchain, οι διευθύνσεις «πορτοφολιών» που θα «παραχθούν» θα είναι διαφορετικές από αυτές που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής, πράγμα που συνεπάγεται με την αλλομορφία της διεύθυνσης του «εκδότη» και τέλος, με την αδυναμία εκτέλεσης του συνόλου των ενεργειών.

4.5. Τεχνικά μέρη της εφαρμογής

Οι τεχνολογίες και οι εφαρμογές που χρησιμοποιήθηκαν κατά τη διάρκεια πραγμάτωσης της εφαρμογής είναι οι εξής:

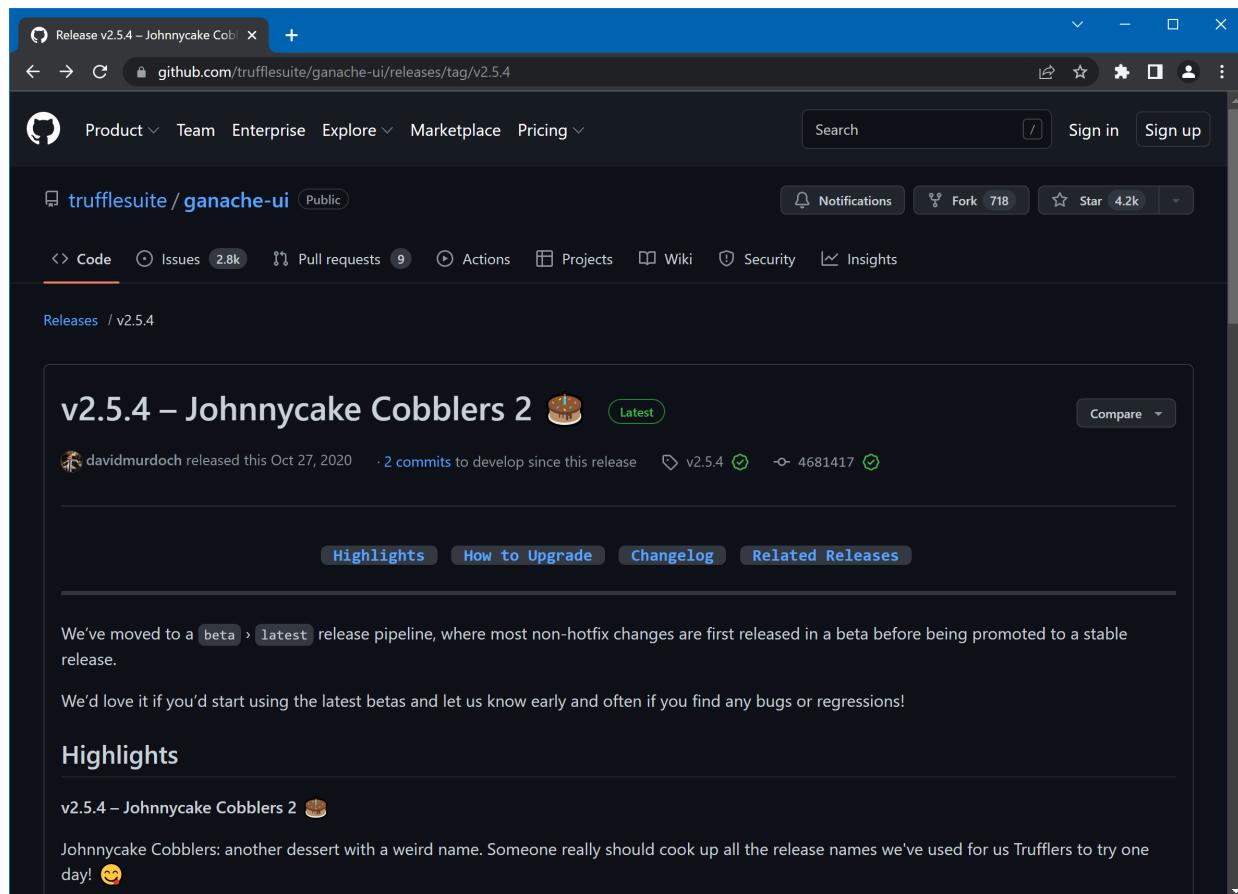
- **Ganache:** Εφαρμογή που παρέχει ένα τοπικό, προσωπικό Blockchain για ανάπτυξη εφαρμογών απευθυνόμενες στο Ethereum Blockchain.
- **Truffle:** Σουίτα εργαλείων ανάπτυξης «Web3» εφαρμογών.
- **Remix IDE:** Εργαλείο ανοιχτού κώδικα που εξειδικεύεται στην συγγραφή και την ανάπτυξη έξυπνων συμβολαίων σε γλώσσα προγραμματισμού «Solidity».
- **Solidity:** Αντικειμενοστραφής γλώσσα προγραμματισμού για την υλοποίηση έξυπνων συμβολαίων σε διάφορες πλατφόρμες Blockchain, κυρίως στο Ethereum.
- **Javascript:** Αντικειμενοστραφής γλώσσα προγραμματισμού για τον εμπλουτισμό και την αύξηση της δυναμικότητας του γραφικού περιβάλλοντος της εφαρμογής.
- **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).
- **Web3.js:** Συλλογή βιβλιοθηκών «Javascript» που επιτρέπουν την ανάπτυξη «Web3» εφαρμογών και την αλληλεπίδραση με έναν τοπικό ή απομακρυσμένο κόμβο Ethereum.
- **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) για το «Node.js» που λειτουργεί αποκλειστικά ως server (διακομιστής) για την ανάπτυξης μιας εφαρμογής.
- **QR Code Javascript Libraries:** Βιβλιοθήκες «Javascript» για την αλληλεπίδραση με κωδικούς γρήγορης ανταπόκρισης (Quick Response Code – QR Code).
- **Visual Studio Code:** Εφαρμογή επεξεργασίας κώδικα.
- **Metamask:** Πορτοφόλι λογισμικού σε μορφή «επέκτασης» για web browser, που χρησιμοποιείται για αλληλεπίδραση με Blockchain, όπως το Ethereum.
- **Infura:** Υποδομή ανάπτυξης και «μεταφοράς» «Web3» εφαρμογών σε δημόσια, κύρια Blockchain ή σε δημόσια Blockchain δοκιμών.
- **Visual Paradigm:** Εφαρμογή μοντελοποίησης και διαχείρισης έργου.
- **macOS:** Λειτουργικό σύστημα στο οποίο αναπτύχθηκε η εφαρμογή.

4.5.1. Οδηγός εγκατάστασης απαραίτητων εφαρμογών (Windows)

Το παρόν κεφάλαιο ανάγεται στην εγκατάσταση των τεχνικών μερών που απαιτούνται για την εκτέλεση του κώδικα της εφαρμογής. Πιο συγκεκριμένα, θα γίνει αναφορά στον τρόπο εγκατάστασης του τοπικού Blockchain «Ganache», του «πορτοφολιού» «Metamask» σε μορφή επέκτασης για τον περιηγητή «Google Chrome», του «Node.js», καθώς και των αναγκαίων, για τη λειτουργία της εφαρμογής, δομοστοιχείων του (εφ' εξής «modules»). Για την ορθότερη κατανόηση του περιεχομένου του τρέχοντος και του επόμενου κεφαλαίου, παράλληλα με το τρίτο ενικό, θα χρησιμοποιηθεί και το πρώτο πληθυντικό πρόσωπο.

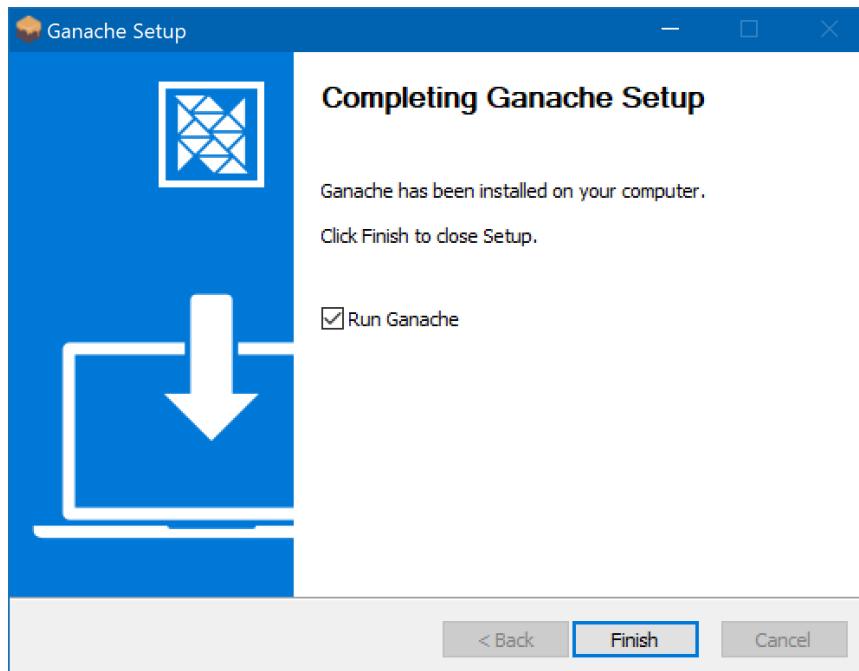
1. Ganache

Το «Ganache», όπως προαναφέρθηκε, είναι μια εφαρμογή προσομοίωσης ενός πλήρως λειτουργικού τοπικού Blockchain για ανάπτυξη εφαρμογών στο Ethereum Blockchain. Οι εκδόσεις της εφαρμογής είναι διαθέσιμες στο αποθετήριο (repository) «ganache-ui» στο «Github» (Εικόνα 30), ενώ μέσω του συνδέσμου <https://github.com/trufflesuite/ganache-ui/releases/download/v2.5.4/Ganache-2.5.4-win-setup.exe> πραγματοποιείται αυτόματα η λήψη του αρχείου εγκατάστασης.



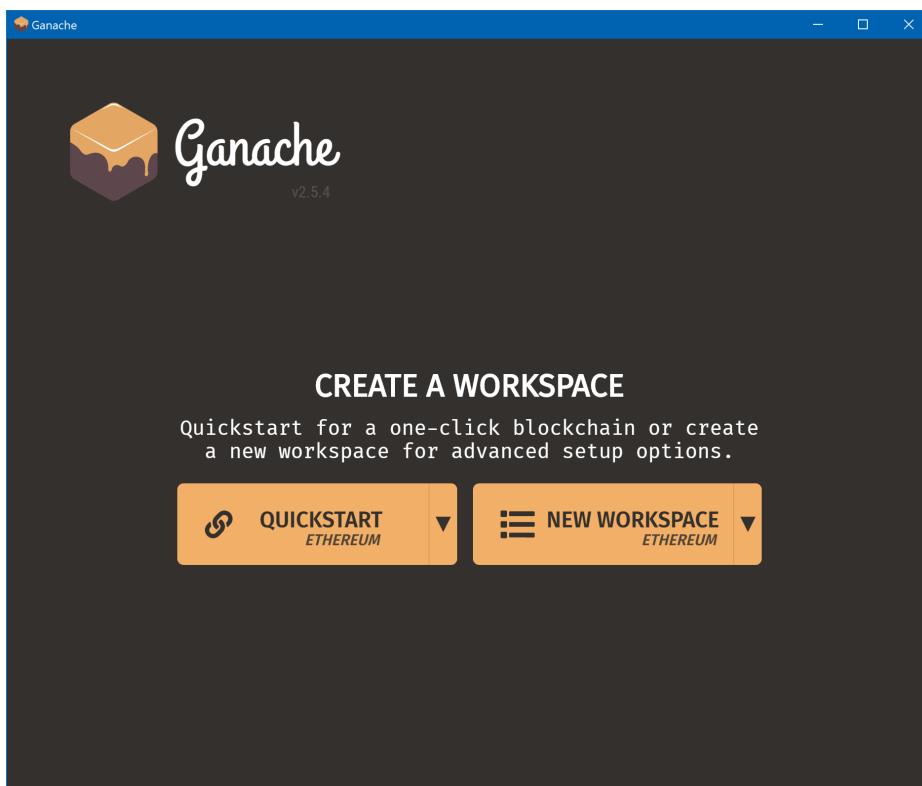
Εικόνα 30 - Το αποθετήριο (repository) του «Ganache» στο «Github»

Όλες οι επιλογές κατά τη διάρκεια της εγκατάστασης παραμένουν ως έχουν.
Κατόπιν ολοκλήρωσης της, επιλέγουμε το «κουτί» «Run Ganache» και «πατάμε» το κουμπί «Finish».



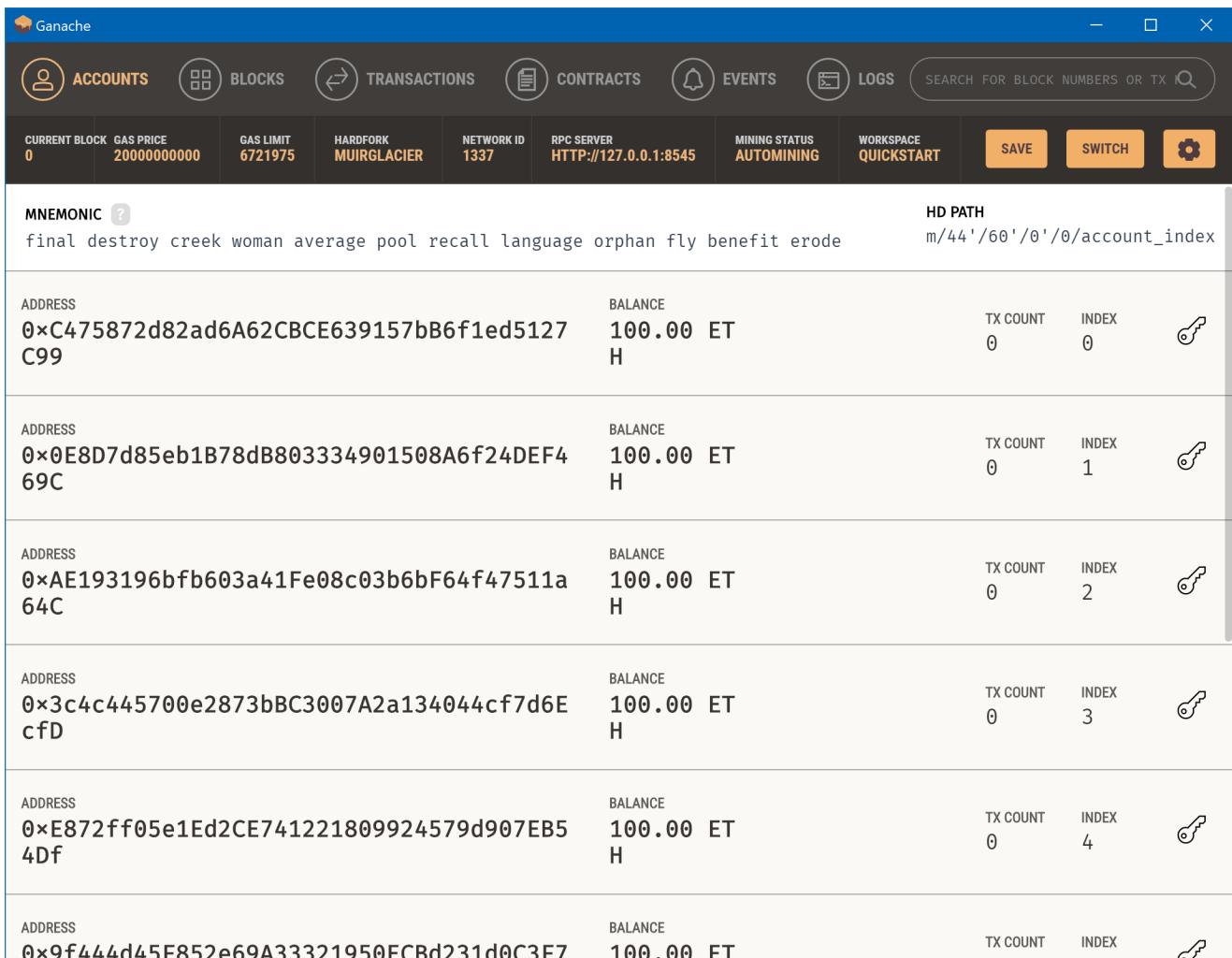
Εικόνα 31 - Ολοκλήρωση εγκατάστασης του «Ganache»

Μόλις εμφανιστεί το παράθυρο «πατάμε» στο κουμπί «QUICKSTART», ελέγχοντας πρώτα αν κάτω από αυτό αναγράφεται η λέξη «ETHEREUM» (Εικόνα 32).



Εικόνα 32 - Αρχική οθόνη του «Ganache»

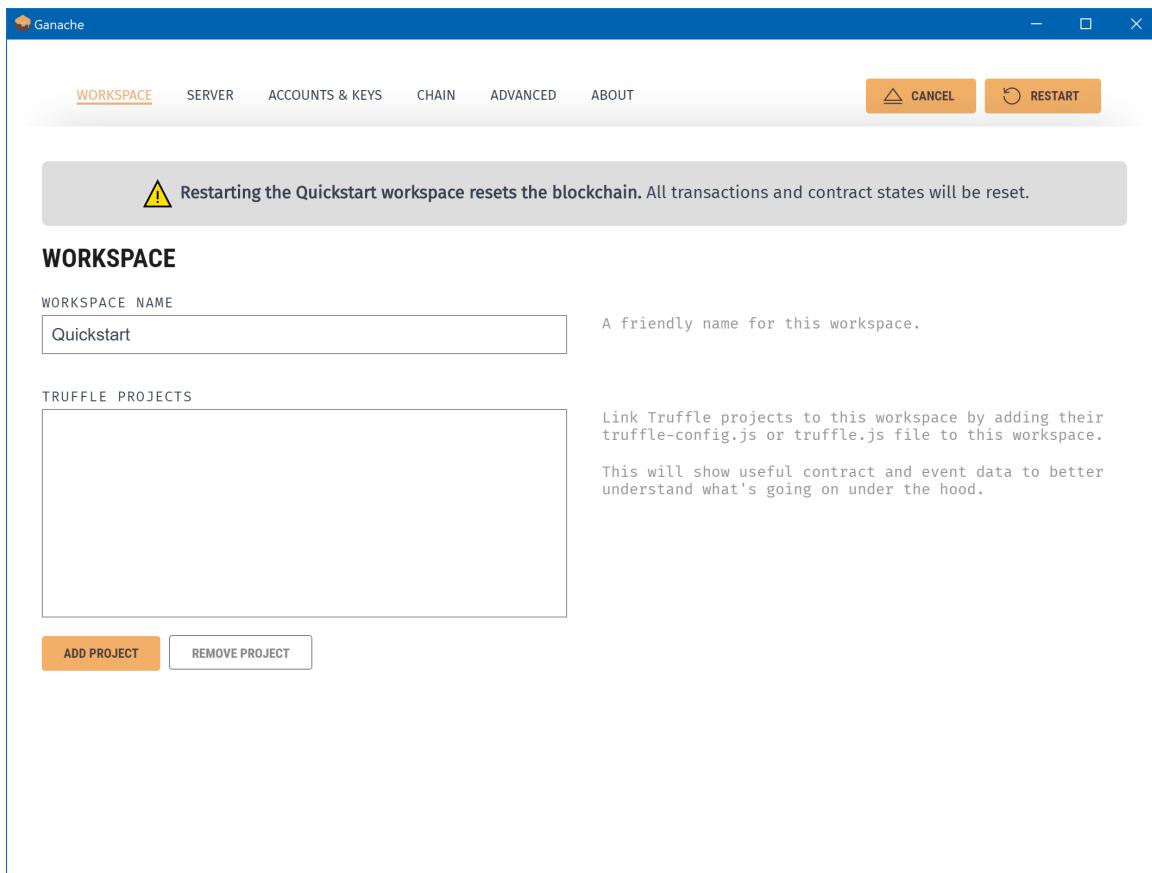
Αυτή η ενέργεια θα δημιουργήσει ένα νέο τοπικό Blockchain, που περιέχει δέκα (10) λογαριασμούς με υπόλοιπο 100 ETH ο καθένας (Εικόνα 33). Άλλα χαρακτηριστικά που διακρίνονται στο ενεργό παράθυρο είναι το «Mnemonic», μία φράση με δώδεκα (12) τυχαίες λέξεις που θα χρειαστούν στην εγκατάσταση του «Metamask», πληροφορίες σχετικά με το παρόν δίκτυο «Blockchain», όπως το τρέχον block, το αναγνωριστικό του δικτύου (Network ID) κ.α.



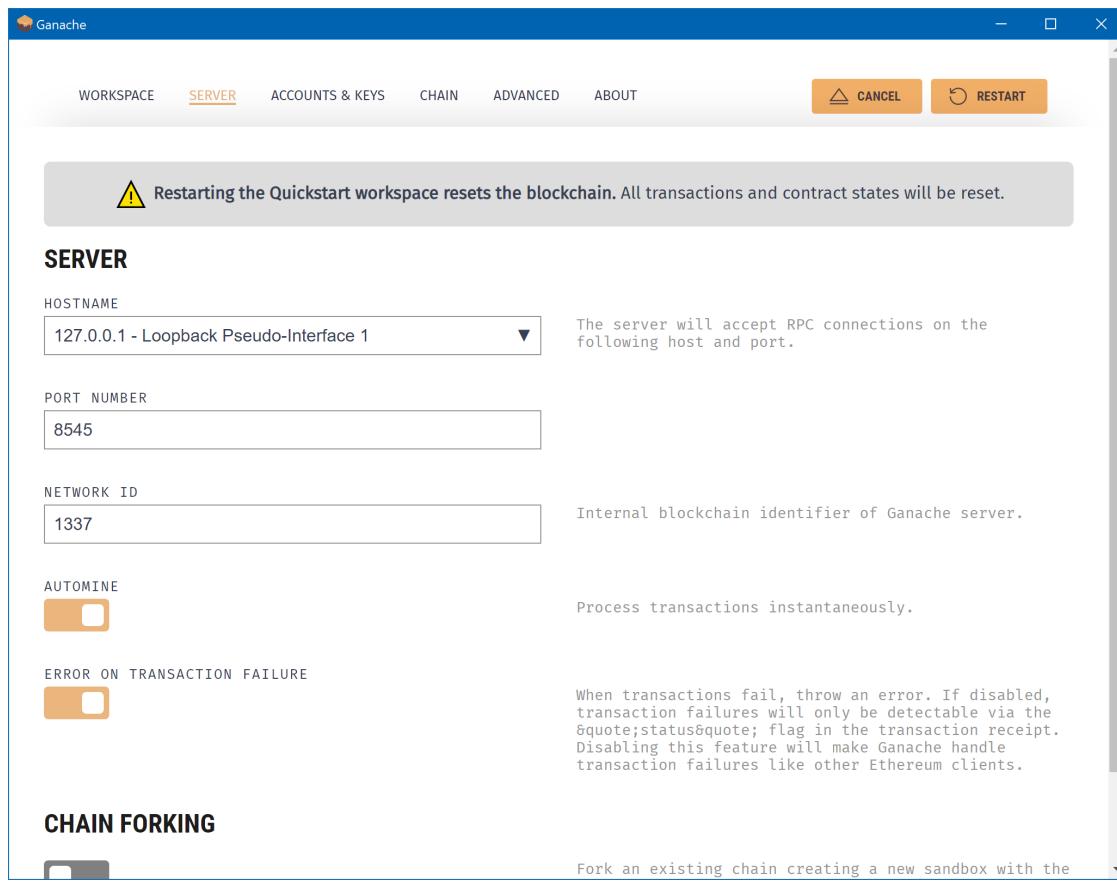
ADDRESS	BALANCE	TX COUNT	INDEX	
0xC475872d82ad6A62CBCE639157bB6f1ed5127C99	100.00 ET_H	0	0	
0xE8D7d85eb1B78dB803334901508A6f24DEF469C	100.00 ET_H	0	1	
0xAE193196bfb603a41Fe08c03b6bF64f47511a64C	100.00 ET_H	0	2	
0x3c4c445700e2873bBC3007A2a134044cf7d6Ecfd	100.00 ET_H	0	3	
0xE872ff05e1Ed2CE741221809924579d907EB54Df	100.00 ET_H	0	4	
0x9f444d45F852e69A33321950ECBd231d0C3F7	100.00 ET	0	5	

Εικόνα 33 - Παράθυρο διαχείρισης του Blockchain

«Πατώντας» στο γρανάζι, στο πάνω δεξιά μέρος του παραθύρου, μεταφερόμαστε στις ρυθμίσεις του δικτύου, όπου μπορούν να τροποποιηθούν στοιχεία, όπως η ονομασία του περιβάλλοντος εργασίας (Εικόνα 34), η διεύθυνση του διακομιστή (RPC Server) και ο αριθμός της θύρας (Port Number) (Εικόνα 35).



Εικόνα 34 - Παράθυρο τροποποίησης των περιβάλλοντος εργασίας

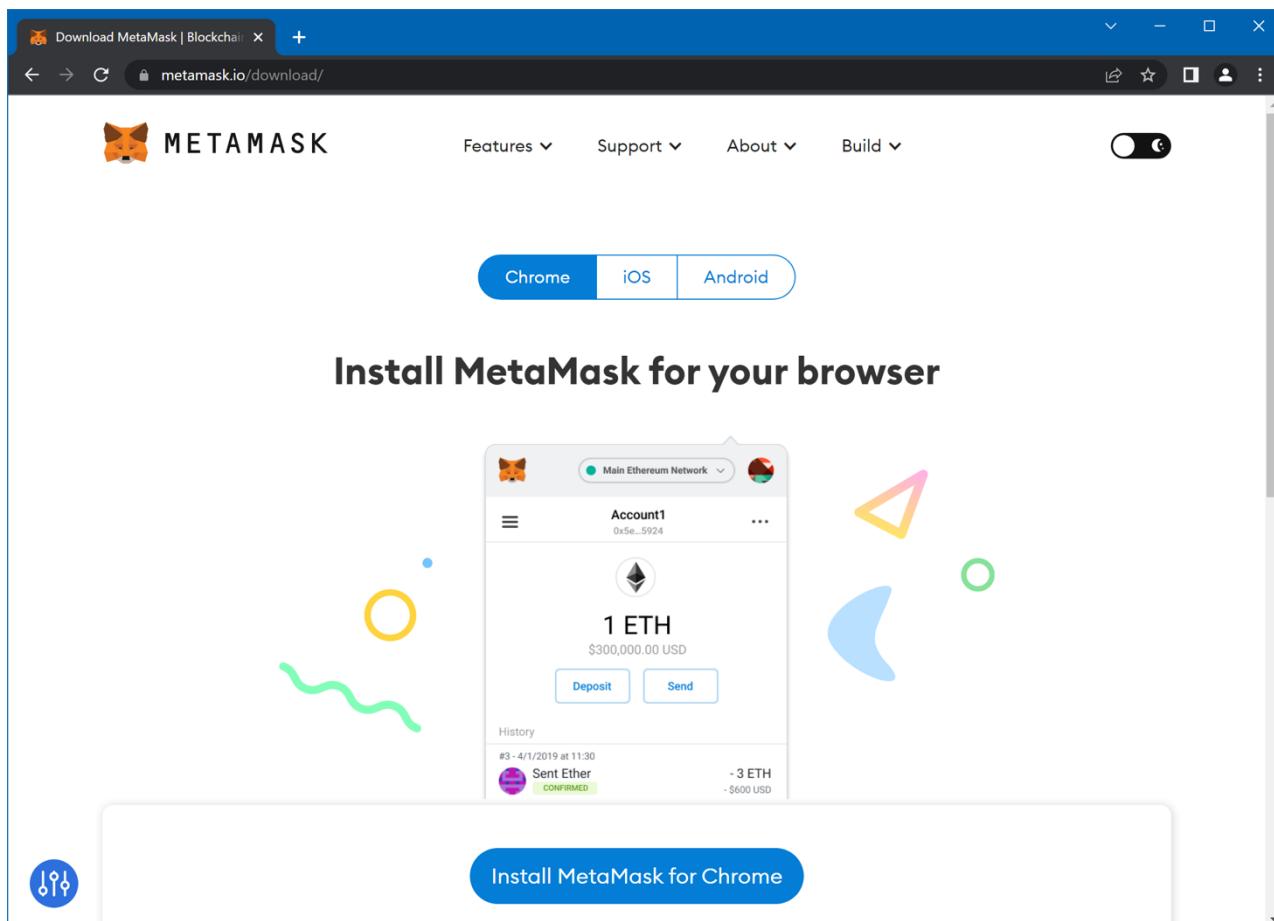


Εικόνα 35 - Παράθυρο τροποποίησης των διακομιστή

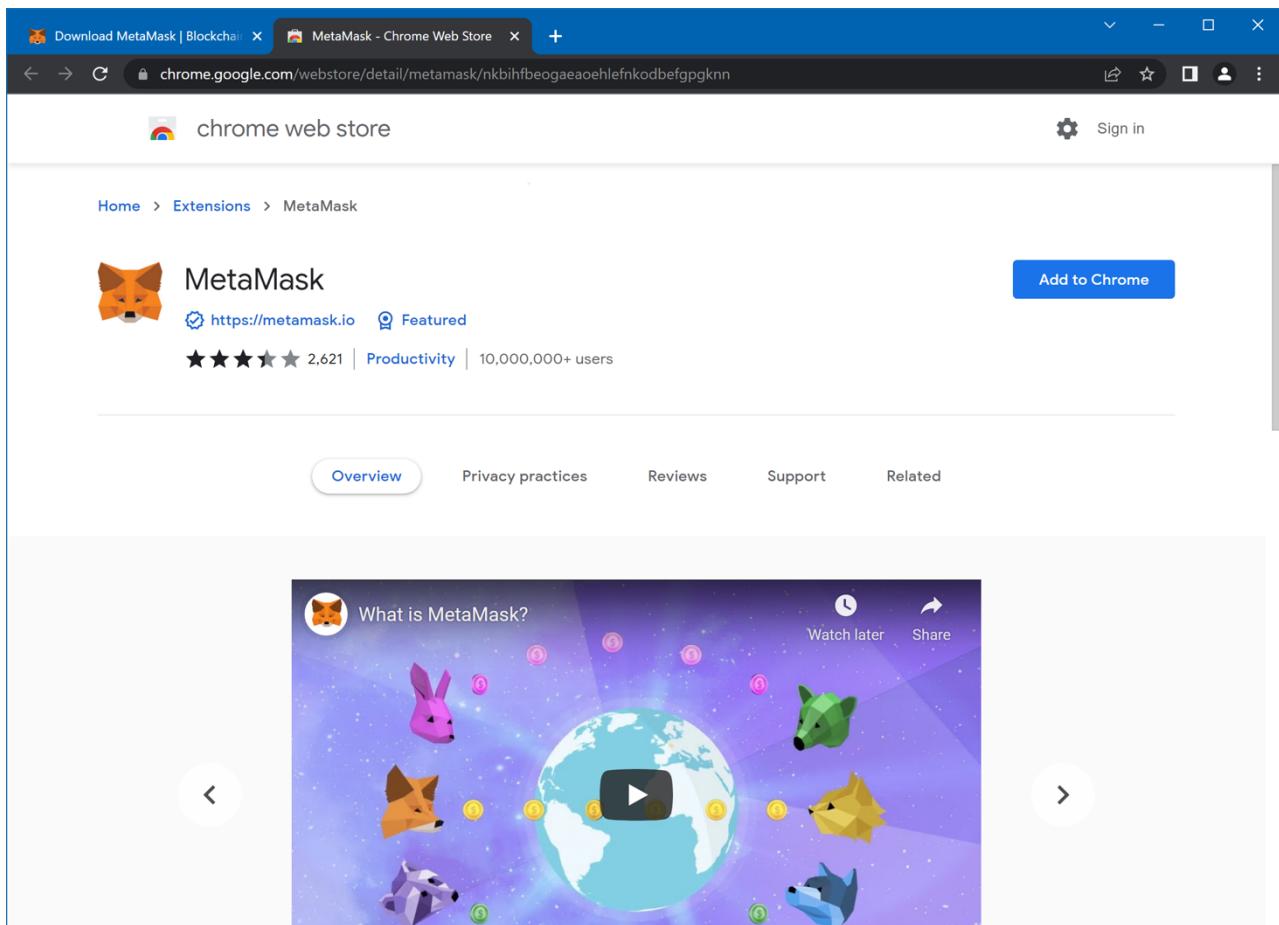
Για την επικοινωνία της εφαρμογής και του «Metamask» με το τοπικό δίκτυο Blockchain, απαιτείται συγκεκριμένο «Port Number» και «Network ID». Αναλυτικότερα, το «Port Number» πρέπει αντιστοιχεί σε «8545» και το «Network ID» σε «1337». Αν στις ρυθμίσεις δικτύου του «Ganache» υπάρχουν διαφορετικοί τετραγήφιοι, τότε θα πρέπει να τους τροποποιήσουμε και στη συνέχεια, να «πατήσουμε» «Save and Restart» στο πάνω δεξιά μέρος του παραθύρου, για να εφαρμοστούν οι αλλαγές.

2. Metamask

Η εφαρμογή «πορτοφολιού» «Metamask» είναι διαθέσιμη μέσω του επίσημου ιστοτόπου της: <https://metamask.io/download/> (Εικόνα 36), αλλά και μέσω του ηλεκτρονικού καταστήματος του προτιμώμενου περιηγητή, στη προκειμένη περίπτωση του «Google Chrome», στη διεύθυνση: https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefknkodbefgp_gknn (Εικόνα 37).

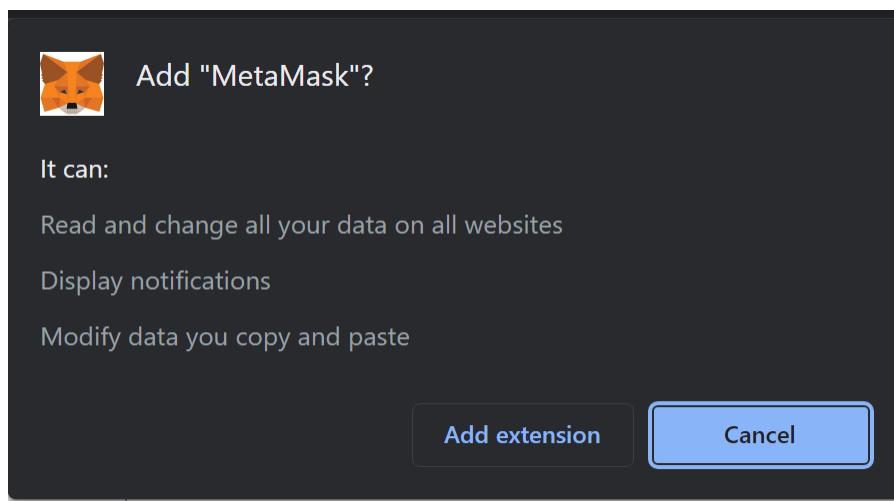


Εικόνα 36 - Επίσημος ιστότοπος του «Metamask»



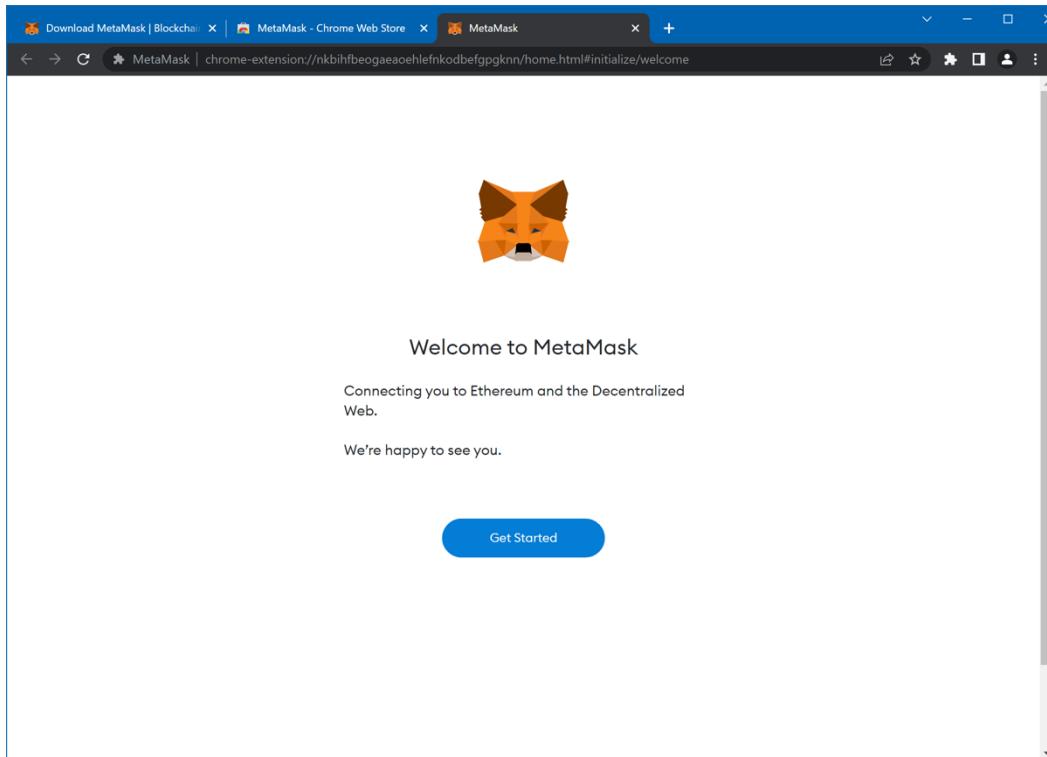
Εικόνα 37 - Ηλεκτρονικό κατάστημα των «Google Chrome»

Πριν ξεκινήσει η διαδικασία της λήψης, εμφανίζεται το μήνυμα της Εικόνας 38, στο οποίο ζητούνται από τον χρήστη ορισμένες άδειες. Κάνοντας «κλικ» στο κουμπί «Add extension» προστίθεται η επέκταση στον περιηγητή.

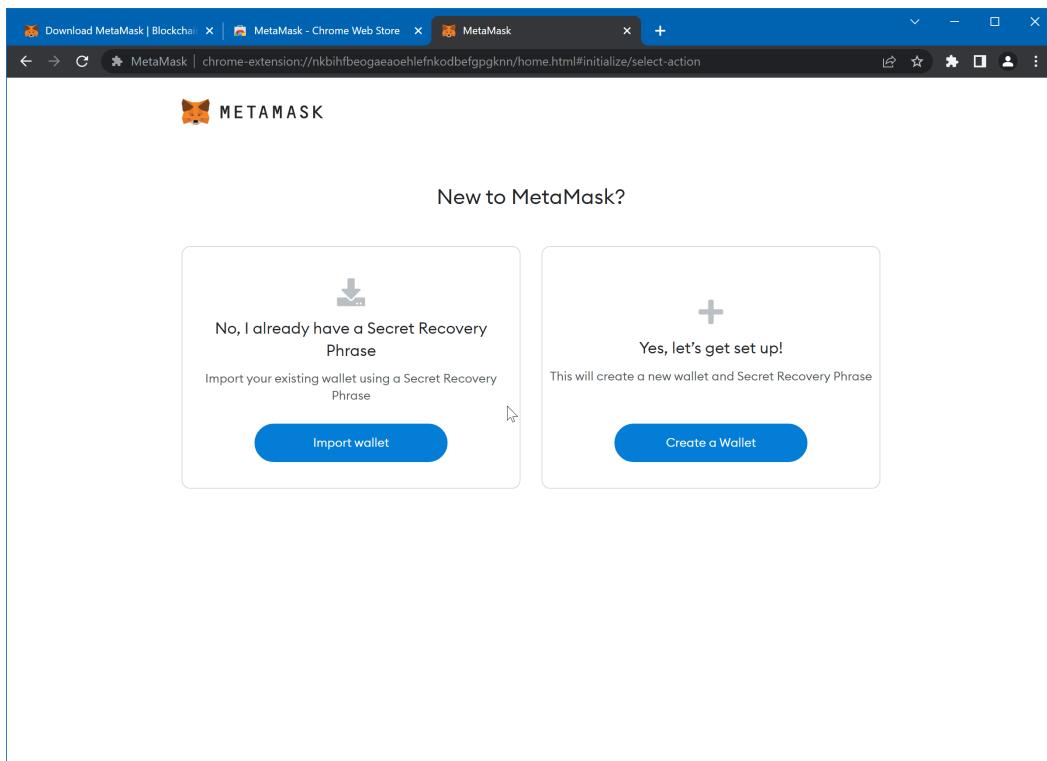


Εικόνα 38 - Μήνυμα έγκρισης προσθήκης της επέκτασης στο «Google Chrome»

Μόλις ολοκληρωθεί η εγκατάσταση, εμφανίζεται σε μία νέα καρτέλα η αρχική σελίδα του «Metamask» (Εικόνα 39), ενώ στη συνέχεια παρατίθενται οι επιλογές εισαγωγής ενός ήδη υπάρχοντος «πορτοφολιού» μέσω «Mnemonic» και δημιουργίας ενός νέου (Εικόνα 40).

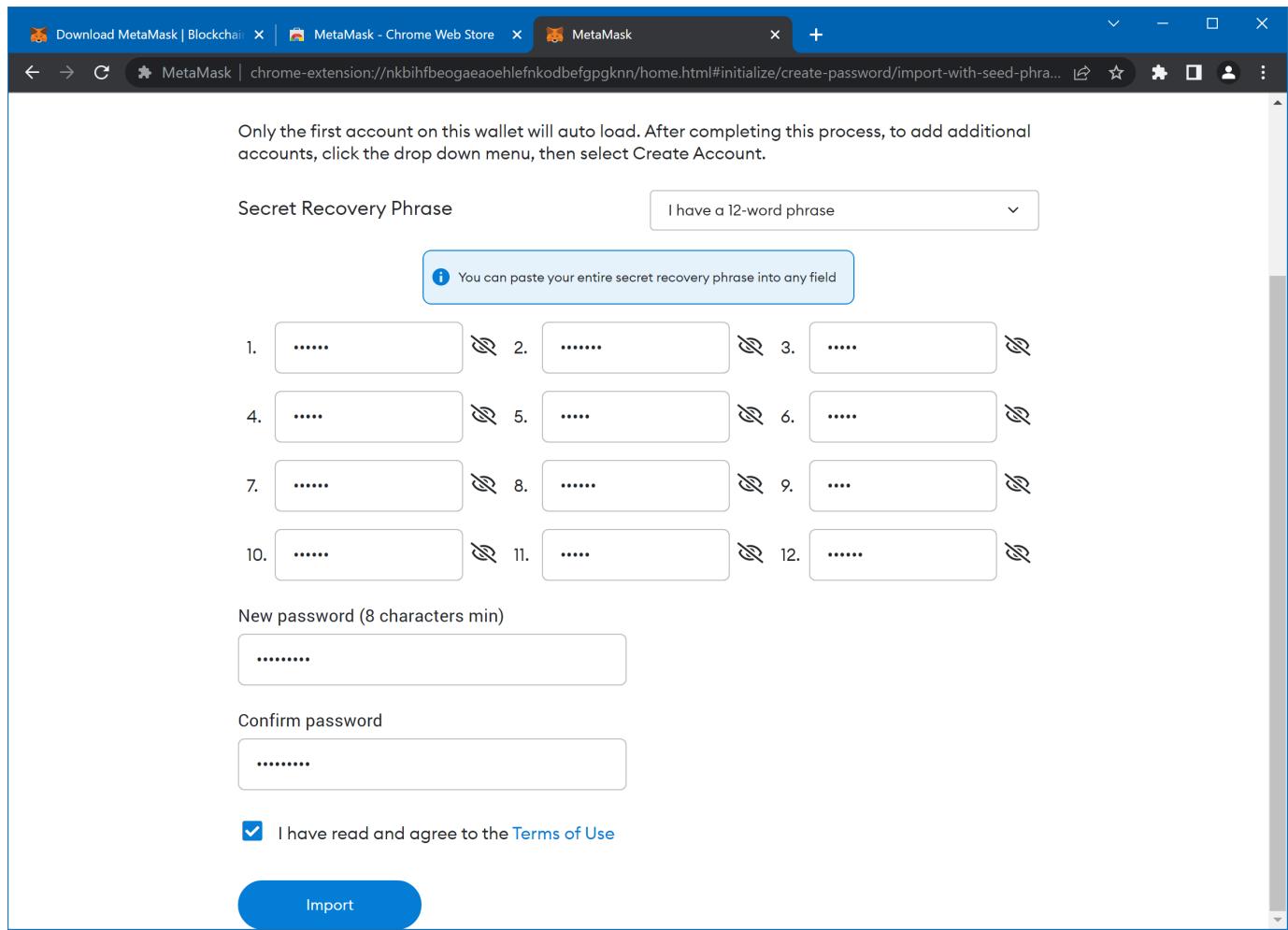


Εικόνα 39 - Αρχική σελίδα του «Metamask»



Εικόνα 40 - Επιλογές εισαγωγής ή δημιουργίας «πορτοφολιού»

Επιλέγοντας την εισαγωγή «πορτοφολιού», εμφανίζονται δώδεκα πλαίσια, ένα για κάθε λέξη του «Mnemonic» και από κάτω ένα πλαίσιο πληκτρολόγησης νέου κωδικού (Εικόνα 41). Σε αυτό το σημείο, «ανοίγουμε» το παράθυρο του Ganache και αντιγράφουμε το «Mnemonic», όπως αναφέρθηκε στην εγκατάσταση του «Ganache» (βλ. σελίδα 62) και πραγματοποιούμε επικόλληση σε οποιοδήποτε πεδίο, σύμφωνα με το μήνυμα στο μέσο του παραθύρου. Αφού πληκτρολογήσουμε και τον επιθυμητό κωδικό, προχωρούμε στην εισαγωγή (Import).

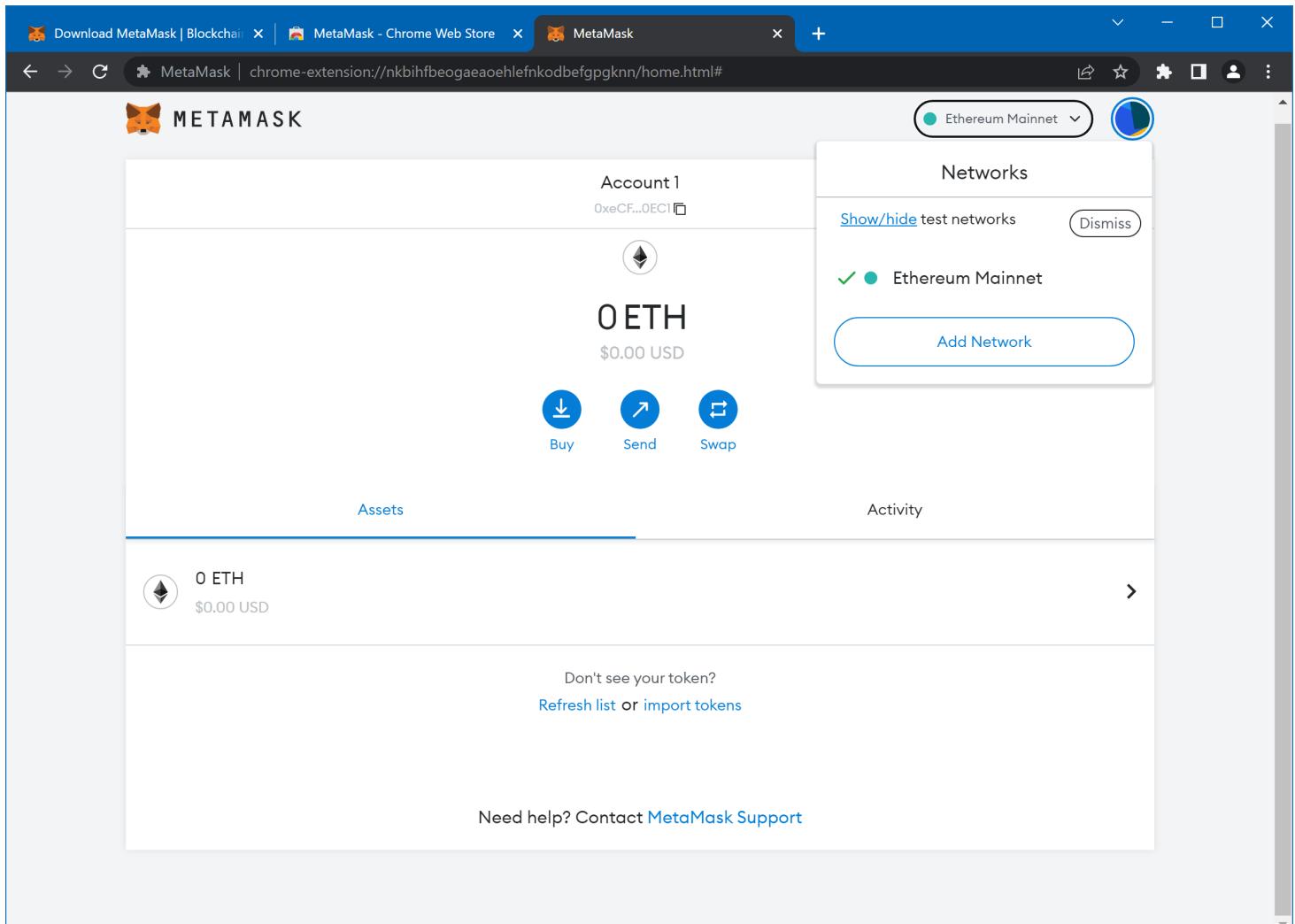


Εικόνα 41 - Εισαγωγή ήδη υπάρχοντος «πορτοφολιού»

Έπειτα, «μεταφερόμαστε» στο περιβάλλον διαχείρισης «πορτοφολιού», το οποίο περιέχει πληροφορίες για το υπόλοιπο του λογαριασμού σε «ETH» και σε άλλα κρυπτονομίσματα που βασίζονται στο «Ethereum», για τη δραστηριότητα του λογαριασμού κ.α.

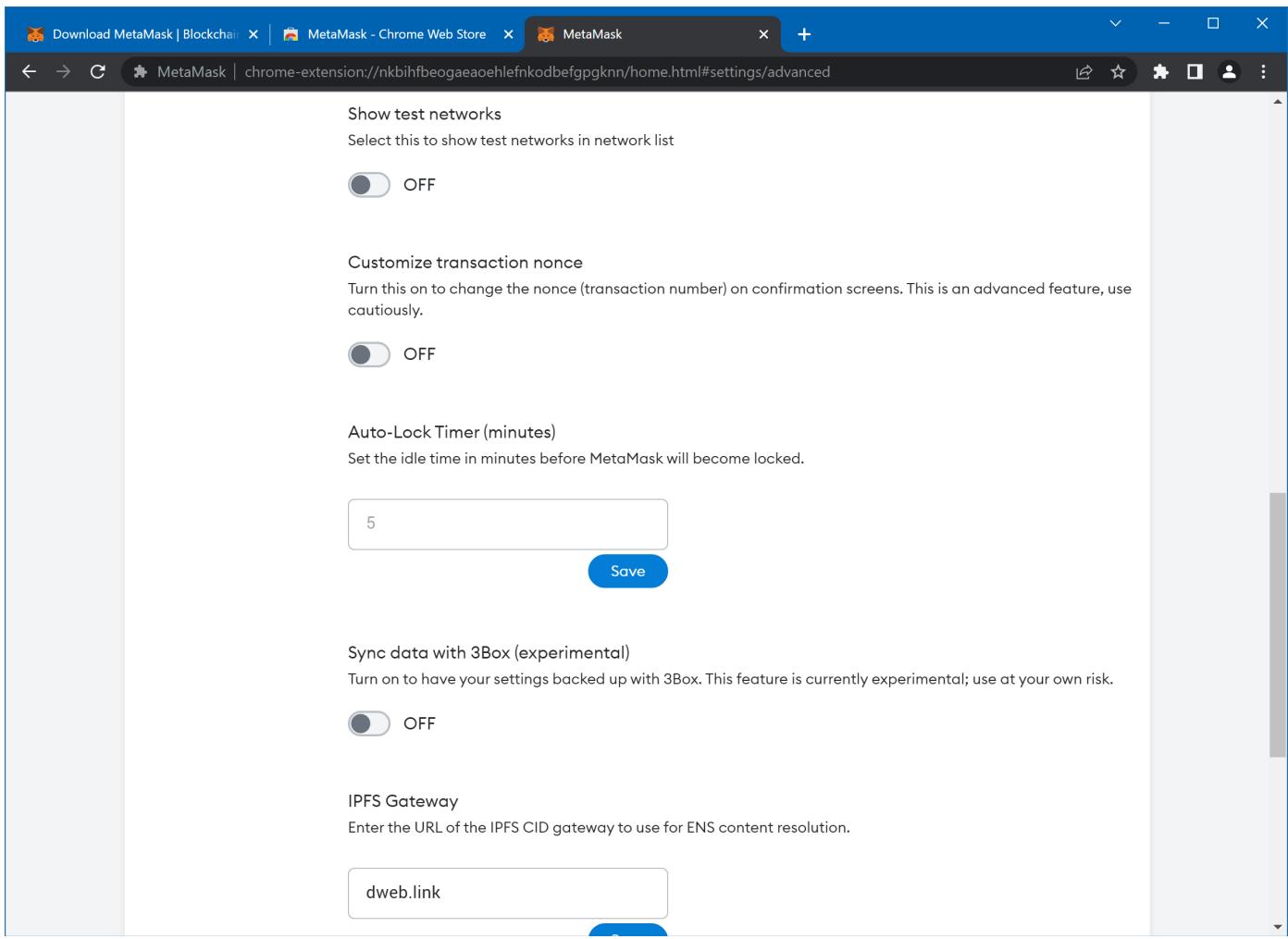
Για τη λειτουργία της εφαρμογής απαιτείται η προσθήκη του τοπικού δικτύου του «Ganache» στη λίστα των διαθέσιμων δικτύων του «Metamask». Αυτό

επιτυγχάνεται επιλέγοντας το «Ethereum Mainnet» στο πάνω δεξιό άκρο του παραθύρου και στη συνέχεια, κάνοντας «κλικ» στο «Show/hide test networks» (Εικόνα 42).

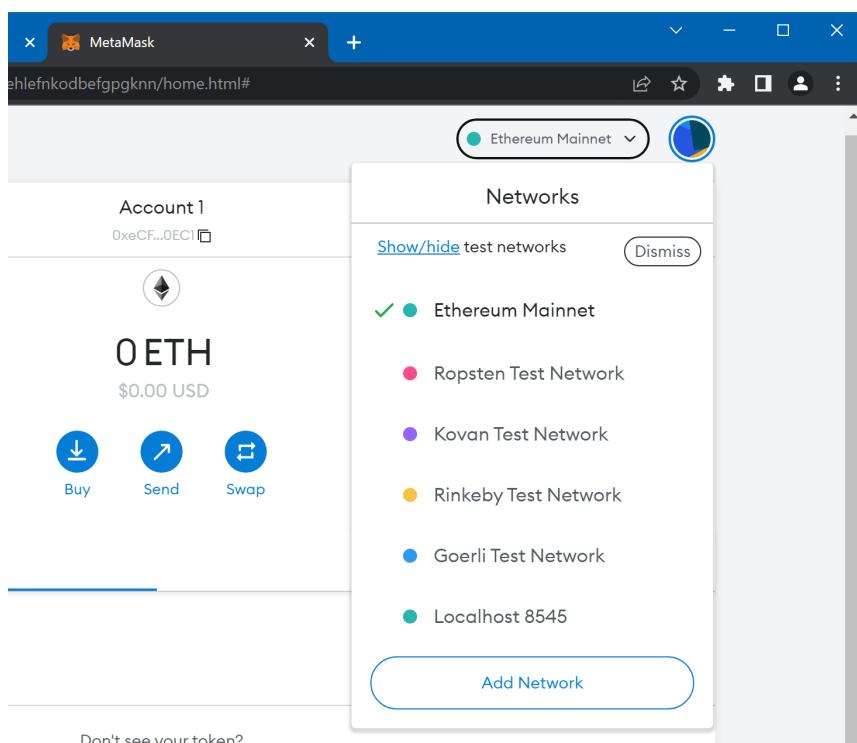


Εικόνα 42 - Περιβάλλον διαχείρισης «πορτοφολιού» του «Metamask»

Από εκεί, «ενεργοποιούμε» τον διακόπτη «Show test networks» στο πάνω μέρος του σημείου της σελίδας που θα μεταφερθούμε (Εικόνα 43). Μπορούμε να επιβεβαιώσουμε ότι τα δοκιμαστικά δίκτυα εμφανίζονται, επιστρέφοντας στο περιβάλλον διαχείρισης πορτοφολιού και κάνοντας «κλικ» στο «Ethereum Mainnet» (Εικόνα 44).



Εικόνα 43 - Διακόπτης ενεργοποίησης δοκιμαστικών δικτύων

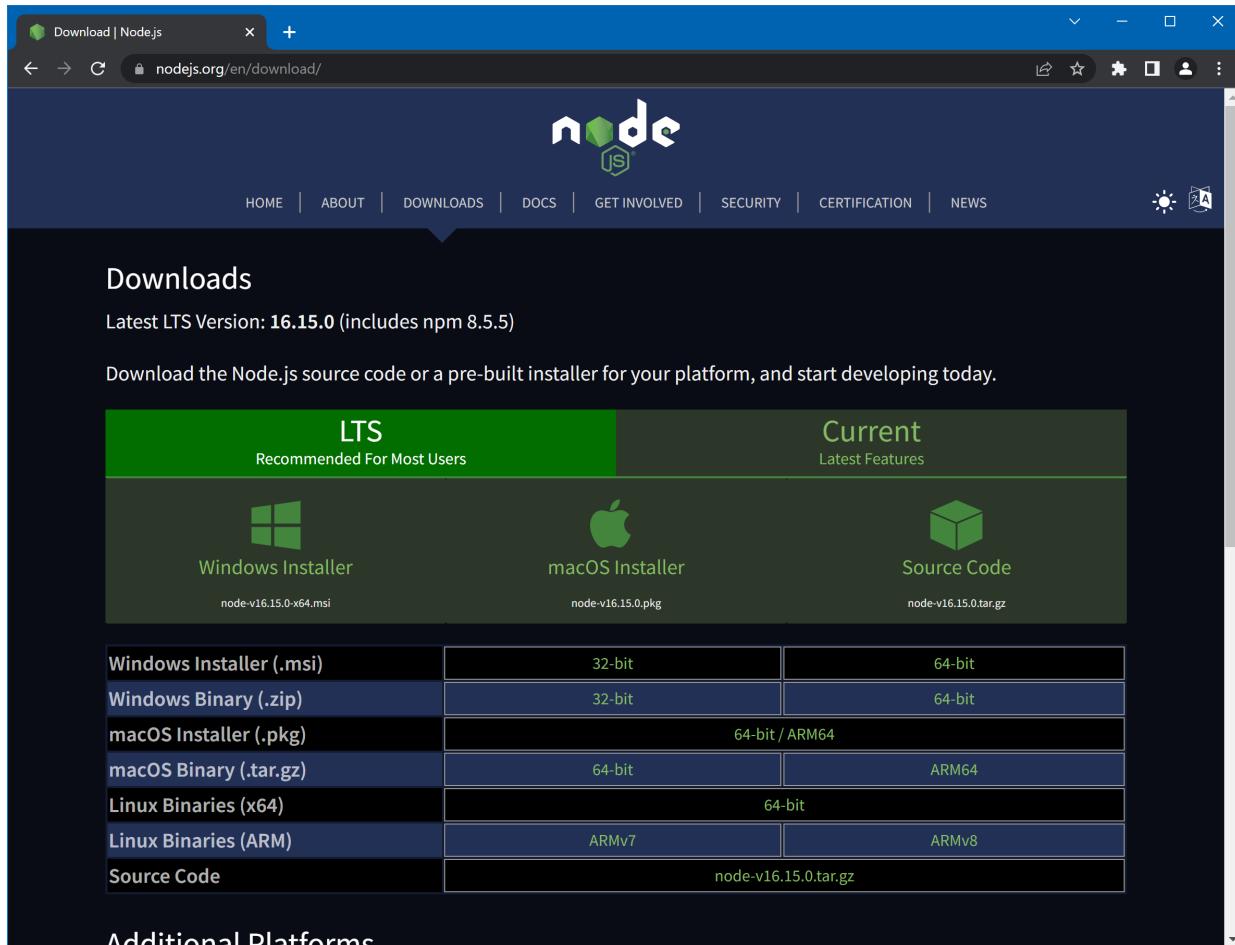


Εικόνα 44 - Τα προκαθορισμένα δοκιμαστικά δίκτυα που περιλαμβάνει το «Metamask»

Από το μενού της Εικόνας 44, επιλέγουμε το δίκτυο «localhost 8545». Θα παρατηρήσουμε ότι το υπόλοιπο του λογαριασμού από 0 ETH θα αλλάξει σε 100 ETH, πράγμα που συνεπάγεται με την επιτυχή σύνδεση στο τοπικό δίκτυο του «Ganache».

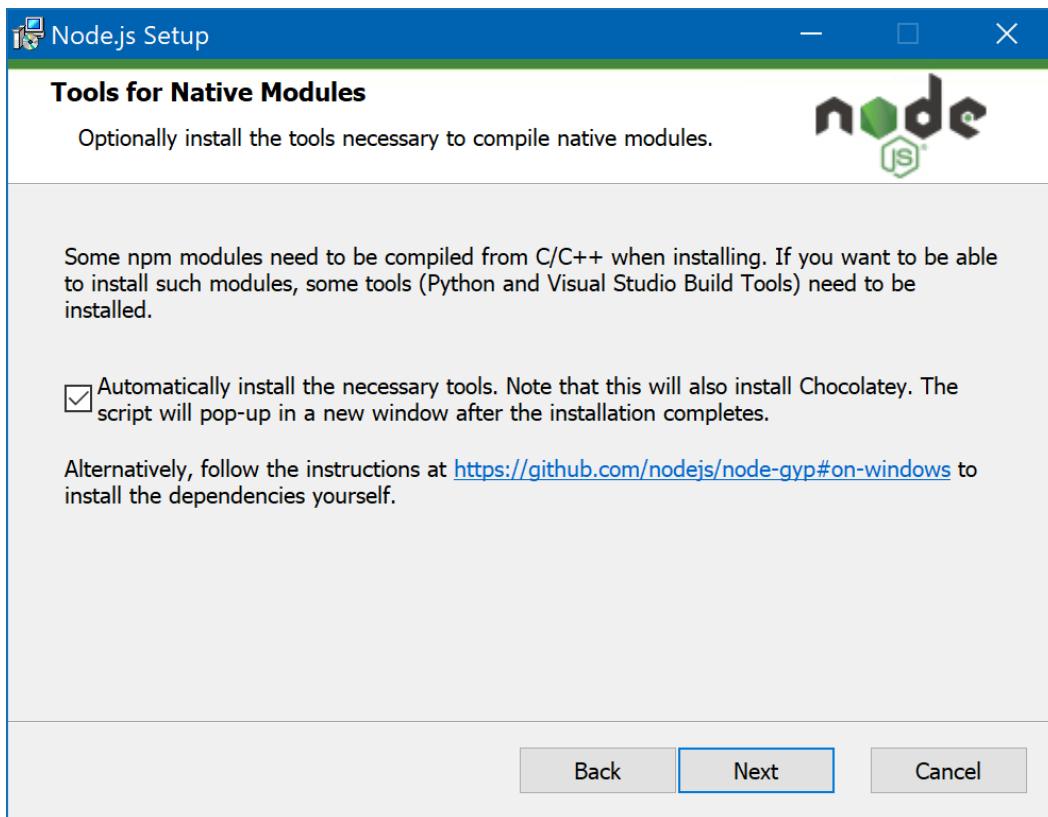
3. Node.js

Η εγκατάσταση του «Node.js» είναι εξίσου απλή. Η λήψη του πραγματοποιείται από τον επίσημο ιστότοπό του μέσω του συνδέσμου: <https://nodejs.org/en/download/> (Εικόνα 45).



Εικόνα 45 – Ιστότοπος λήψης του «Node.js»

Κατόπιν ολοκλήρωσης της λήψης, εκτελούμε το αρχείο εγκατάστασης και ξεκινούμε τη διαδικασία. Όλες οι επιλογές μένουν ως έχουν, ενώ χρήζει ιδιαίτερης σημασίας να αναφερθεί, πως το «κουτί» της Εικόνας 46, πρέπει να είναι επιλεγμένο, καθώς κρίνεται αναγκαία η εγκατάσταση επιπλέον εργαλείων για την εκτέλεση της εφαρμογής.



Εικόνα 46 - Απαραίτητη επιλογή κατά την εγκατάσταση του «Node.js»

Αφού ολοκληρωθεί η διαδικασία και «πατήσουμε» το κουμπί «Finish», αναδύονται δύο παράθυρα «CMD» (γραμμής εντολών). Αρχικά, εμφανίζεται το παράθυρο της Εικόνας 47. Για να εκτελεστεί το αρχείο μας ζητείται να «πατήσουμε» οποιοδήποτε πλήκτρο. Αμέσως, θα κλείσει αυτό το παράθυρο και θα εμφανιστεί το παράθυρο της Εικόνας 48, στο οποίο απαντείται η ίδια ενέργεια. Έπειτα, θα κάνει την εμφάνιση του ένα παράθυρο «Windows PowerShell», στο οποίο θα ολοκληρωθεί η εγκατάσταση των εργαλείων (Εικόνα 49).

```
Administrator: Install Additional Tools for Node.js
=====
Tools for Node.js Native Modules Installation Script
=====

This script will install Python and the Visual Studio Build Tools, necessary
to compile Node.js native modules. Note that Chocolatey and required Windows
updates will also be installed.

This will require about 3 Gb of free disk space, plus any space necessary to
install Windows updates. This will take a while to run.

Please close all open programs for the duration of the installation. If the
installation fails, please ensure Windows is fully updated, reboot your
computer and try to run this again. This script can be found in the
Start menu under Node.js.

You can close this window to stop now. Detailed instructions to install these
tools manually are available at https://github.com/nodejs/node-gyp#on-windows

Press any key to continue . . .
```

Εικόνα 47 - Πρώτο παράθυρο «CMD» εγκατάστασης πρόσθετων εργαλείων του «Node.js»

```
Administrator: Install Additional Tools for Node.js
-----
Using this script downloads third party software
-----

This script will direct to Chocolatey to install packages. By using
Chocolatey to install a package, you are accepting the license for the
application, executable(s), or other artifacts delivered to your machine as a
result of a Chocolatey install. This acceptance occurs whether you know the
license terms or not. Read and understand the license terms of the packages
being installed and their dependencies prior to installation:
- https://chocolatey.org/packages/chocolatey
- https://chocolatey.org/packages/python
- https://chocolatey.org/packages/visualstudio2019-workload-vctools

This script is provided AS-IS without any warranties of any kind
-----
Chocolatey has implemented security safeguards in their process to help
protect the community from malicious or pirated software, but any use of this
script is at your own risk. Please read the Chocolatey's legal terms of use
as well as how the community repository for Chocolatey.org is maintained.

Press any key to continue . . .
```

Εικόνα 48 - Δεύτερο παράθυρο «CMD» εγκατάστασης πρόσθετων εργαλείων του Node.js

```

Administrator: Windows PowerShell
Forcing web requests to allow TLS v1.2 (Required for requests to chocolatey.org)
Getting latest version of the chocolatey package for download.
Not using proxy.
Getting Chocolatey from https://community.chocolatey.org/api/v2/package/chocolatey/1.1.0.
Downloading https://community.chocolatey.org/api/v2/package/chocolatey/1.1.0 to C:\Users\ADMINI~1\AppData\Local\Temp\chocoInstall\chocolatey.zip
Not using proxy.
Extracting C:\Users\ADMINI~1\AppData\Local\Temp\chocolatey\chocoInstall\chocolatey.zip to C:\Users\ADMINI~1\AppData\Local\Temp\chocoInstall\chocolatey.
Installing ChocolateyInstall on the local machine
Creating ChocolateyInstall as an environment variable (targeting 'Machine')
    Setting ChocolateyInstall to 'C:\ProgramData\chocolatey'
WARNING: It's very likely you will need to close and reopen your shell
before you can use choco.
Restricting write permissions to Administrators
We are setting up the Chocolatey package repository.
The packages themselves go to 'C:\ProgramData\chocolatey\lib'
(i.e. C:\ProgramData\chocolatey\lib\yourPackageName).
A shim file for the command line goes to 'C:\ProgramData\chocolatey\bin'
and points to an executable in 'C:\ProgramData\chocolatey\lib\yourPackageName'.

Creating Chocolatey folders if they do not already exist.

WARNING: You can safely ignore errors related to missing log files when
upgrading from a version of Chocolatey less than 0.9.9.
'Batch file could not be found' is also safe to ignore.
'The system cannot find the file specified' - also safe.
chocolatey.nupkg file not installed in lib.
Attempting to locate it from bootstrapper.
PATH environment variable does not have C:\ProgramData\chocolatey\bin in it. Adding...
WARNING: Not setting tab completion: Profile file does not exist at
'C:\Users\Administrator\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1'.
Chocolatey (choco.exe) is now ready.
You can call choco from anywhere, command line or powershell by typing choco.
Run choco /? for a list of functions.
You may need to shut down and restart powershell and/or consoles
first prior to using choco.
Ensuring Chocolatey commands are on the path
Ensuring chocolatey.nupkg is in the lib folder
Chocolatey v1.1.0
Upgrading the following packages:
python;visualstudio2019-workload-vctools
By upgrading, you accept licenses for the packages.
python is not installed. Installing...
Progress: Downloading python3 3.10.4... 100%
Progress: Downloading python3 3.10.4... 100%
Progress: Downloading vcredist2015 14.0.24215.20170201... 100%
Progress: Downloading vcredist2015 14.0.24215.20170201... 100%

```

Εικόνα 49 - Έναρξη εγκατάστασης των πρόσθετων εργαλείων στο «Windows PowerShell»

Η εγκατάσταση θα διαρκέσει από δεκαπέντε (15) έως είκοσι (20) λεπτά, διότι, όπως αναφέρεται στην Εικόνα 47, το μέγεθος των αρχείων «αγγίζει» τα 3 GB. Μόλις ολοκληρωθεί η διαδικασία, το παράθυρο του «Microsoft PowerShell» θα μοιάζει όπως αυτό της Εικόνας 50.

```
Administrator: Windows PowerShell
Version '10.0.19041.0' is not in the supported version range '[6.1,6.3]'.
[048c:0027][2022-05-22T14:41:26] Package Microsoft.VisualStudio.Debugger.Remote.DbgHelp.Win8 is not applicable: The current OS Version '10.0.19041.0' is not in the supported version range '[6.1,6.3]'.
[048c:0027][2022-05-22T14:41:26] Package Microsoft.VisualStudio.Debugger.Remote.DbgHelp.Win8 is not applicable: The current OS Version '10.0.19041.0' is not in the supported version range '[6.1,6.3]'.
[048c:0027][2022-05-22T14:41:26] Package Microsoft.Net.4.8.FullRedist is not applicable: The current OS Version '10.0.19041.0' is not in the supported version range '[6.1,10.0.17763]'.
[048c:0027][2022-05-22T14:41:26] Package Microsoft.VisualStudio.NuGet.PowerShellBindingRedirect is not applicable: The current OS Version '10.0.19041.0' is not in the supported version range '[6.1,6.2)'.
[048c:0027][2022-05-22T14:41:27] shutting down the application with exit code 0
[048c:0001][2022-05-22T14:41:27] Releasing singleton lock.
[048c:0001][2022-05-22T14:41:27] Releasing singleton lock succeed.
[048c:0001][2022-05-22T14:41:27] Releasing singleton lock.
[048c:0001][2022-05-22T14:41:27] Singleton lock does not exist. Releasing singleton lock skipped.
[048c:0001][2022-05-22T14:41:27] Closing the installer with exit code 0
[048c:0001][2022-05-22T14:41:27] Exit Code: 0
[048c:0001][2022-05-22T14:41:27] Cleared previous session ID.
[048c:0001][2022-05-22T14:41:28] Trying to remove channel manifest: c:\Users\Administrator\AppData\Local\Microsoft\VisualStudio\Packages\_channels\A0FE1051\install\ChannelManifest.json
[048c:0001][2022-05-22T14:41:28] Trying to remove product manifest: c:\Users\Administrator\AppData\Local\Microsoft\VisualStudio\Packages\_channels\A0FE1051\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 18/18 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Upgraded:
- kb2919355 v1.0.20160915
- python v3.10.4
- kb3033929 v1.0.5
- chocolatey-core.extension v1.4.0
- kb2999226 v1.0.20181019
- python3 v3.10.4
- visualstudio2019-workload-vctools v1.0.1
- dotnetfx v4.8.0.20190930
- chocolatey-visualstudio.extension v1.10.2
- visualstudio2019buildtools v16.11.15.0
- vcredist2015 v14.0.24215.20170201
- kb2919442 v1.0.20160915
- visualstudio-installer v2.0.3
- vcredist140 v14.32.31326
- chocolatey-compatibility.extension v1.0.0
- chocolatey-dotnetfx.extension v1.0.1
- kb3035131 v1.0.3
- chocolatey-windowsupdate.extension v1.0.4
Type ENTER to exit:
```

Εικόνα 50 - Ολοκλήρωση της εγκατάστασης των πρόσθετων εργαλείων του «Node.js»

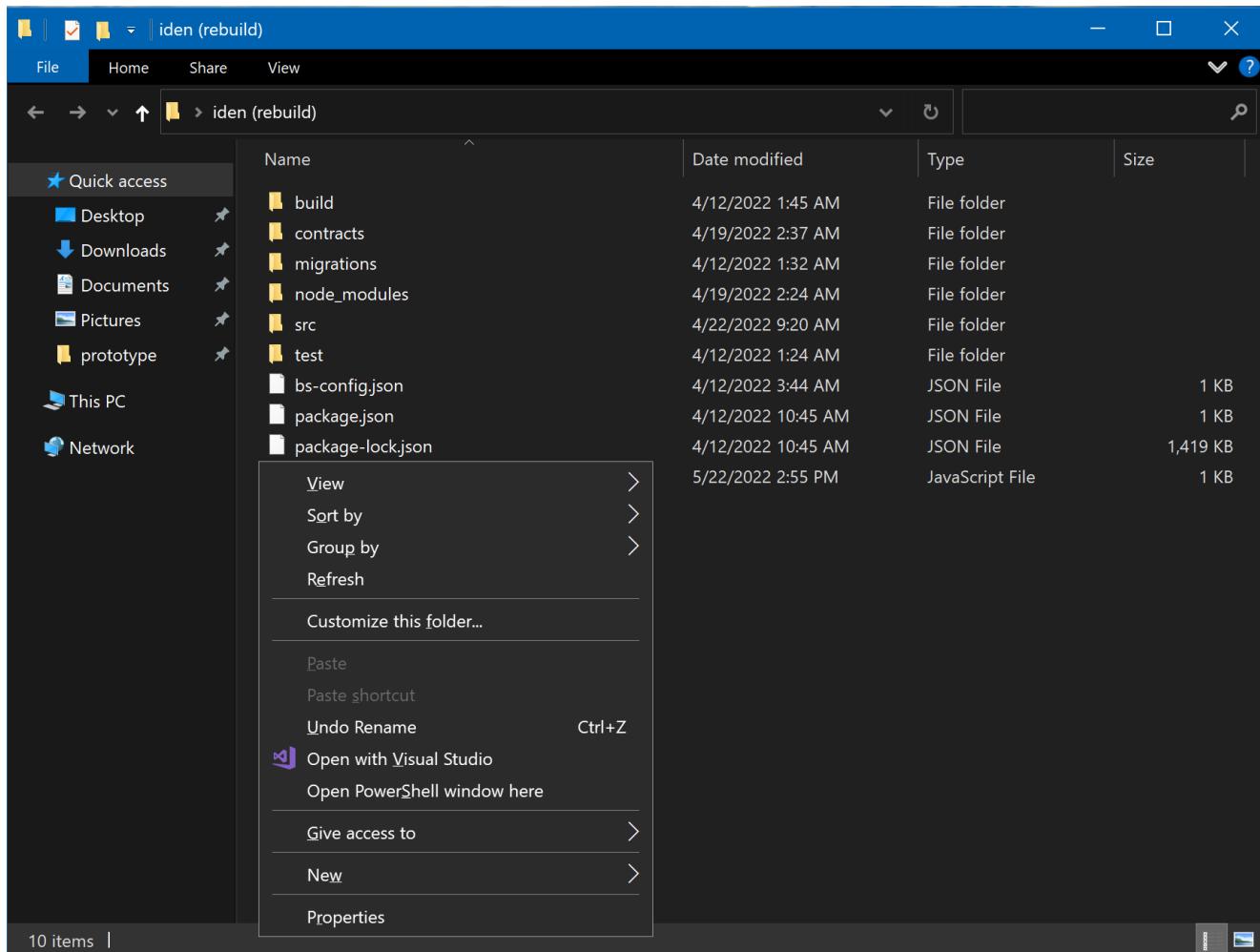
4. Node.js Modules

Η εγκατάσταση των modules μπορεί να πραγματοποιηθεί με δύο τρόπους: με τη χρήση της εντολής «npm rebuild» ή της εντολής «npm install». Με την εντολή «npm rebuild» τα modules «ανακατασκευάζονται», με σκοπό να είναι συμβατά με την τρέχουσα έκδοση του «Node.js» που είναι εγκατεστημένη στο σύστημα. Η διάρκεια της ενέργειας αυτής υπολογίζεται στα δύο (2) με πέντε (5) λεπτά. Από την άλλη, χρησιμοποιώντας την «npm install», τα modules εγκαθίστανται εκ νέου, βάσει του περιεχομένου του αρχείου «package.json», που βρίσκεται μέσα στον φάκελο της εφαρμογής. Αυτή η διαδικασία εκτιμάται να διαρκέσει επίσης, από δύο (2) έως πέντε (5) λεπτά. Εκ των δύο αυτών εντολών, συνίσταται η «npm install», διότι πραγματοποιείται «καθαρή» εγκατάσταση (clean installation) των modules και κατά συνέπεια μειώνεται η πιθανότητα σφάλματος.

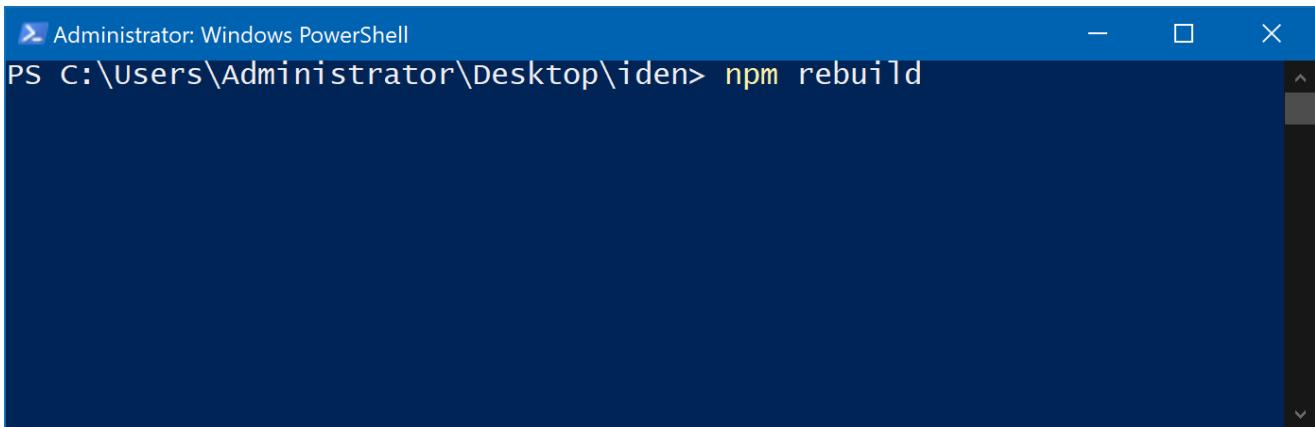
Ομοίως με τους προαναφερθέντες τρόπους εγκατάστασης, στα αρχεία του έργου συμπεριλαμβάνονται δύο φάκελοι: ο «Prototype (rebuild)» και ο «Prototype (install)». Παρακάτω, θα αναλυθούν και οι δύο τρόποι εγκατάστασης στους φακέλους που αντιστοιχούν.

4.1. Εντολή «npm rebuild»

Εντός του φακέλου «Prototype (rebuild)» χρησιμοποιούμε τον συνδυασμό πλήκτρων «Shift» + δεξί «κλικ», ώστε να εμφανιστεί η επιλογή «Open PowerShell window here» (Εικόνα 51). Αφού το επιλέξουμε, αναδύεται ένα παράθυρο «Windows PowerShell» στο οποίο πληκτρολογούμε την εντολή «npm rebuild» (Εικόνα 52). Όπως προαναφέρθηκε, η διαδικασία διαρκεί από δύο (2) έως πέντε (5) λεπτά και από τα αποτελέσματά της, που διακρίνονται στην Εικόνα 53, αγνοούμε τις γραμμές που ξεκινούν με «npm notice».

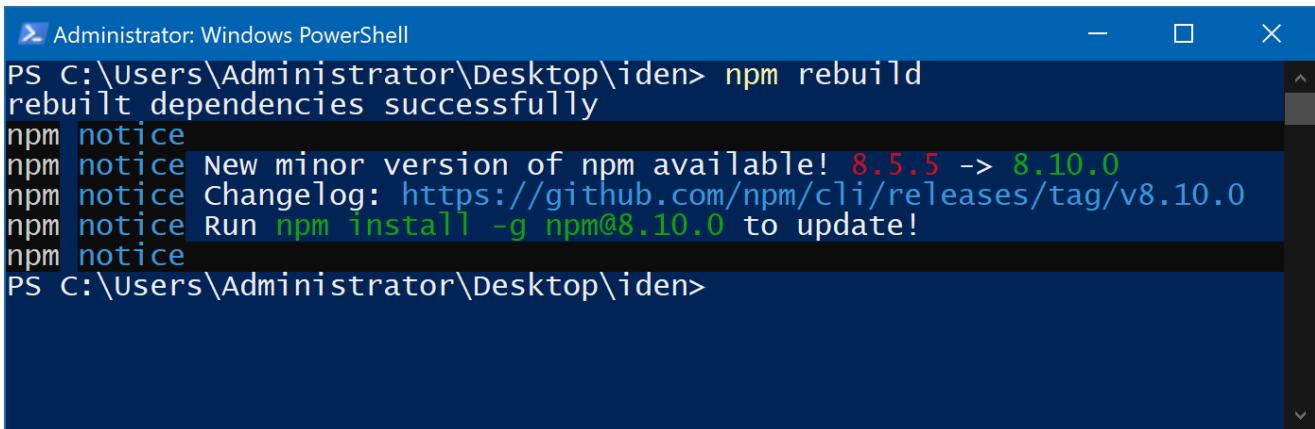


Εικόνα 51 - Ο φάκελος «Prototype (rebuild)»



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\iden> npm rebuild
```

Εικόνα 52 - Εκτέλεση της εντολής «*npm rebuild*»

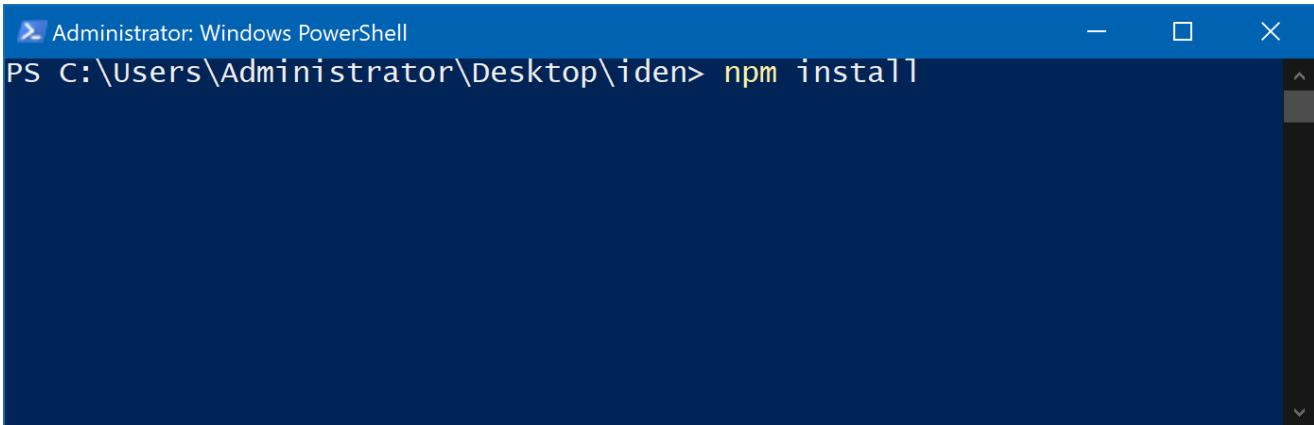


```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\iden> npm rebuild
rebuilt dependencies successfully
npm notice
npm notice New minor version of npm available! 8.5.5 => 8.10.0
npm notice Changelog: https://github.com/npm/cli/releases/tag/v8.10.0
npm notice Run npm install -g npm@8.10.0 to update!
npm notice
PS C:\Users\Administrator\Desktop\iden>
```

Εικόνα 53 - Αποτελέσματα της εντολής «*npm rebuild*»

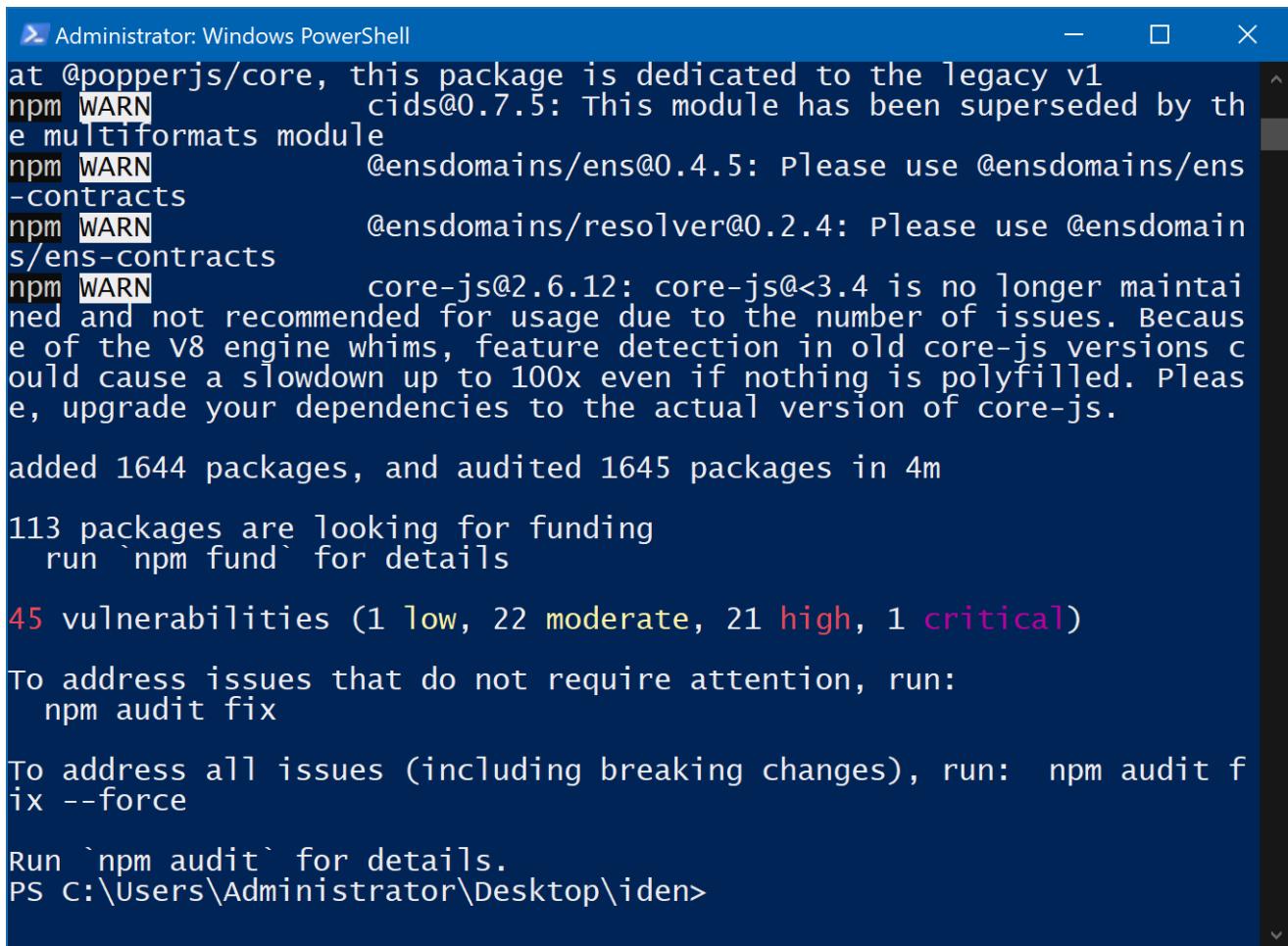
4.2. Εντολή «*npm install*»

Κατά τον ίδιο τρόπο εκτελείται και η εντολή «*npm install*». Κάνοντας χρήση του συνδυασμού πλήκτρων «Shift» + δεξί «κλικ» εντός του φακέλου «Prototype (install)», εμφανίζεται το μενού, στο οποίο επιλέγουμε το «Open PowerShell window here». Στο νέο παράθυρο «Windows PowerShell» πληκτρολογούμε την εντολή «*npm install*» (Εικόνα 54). Κατά τη διάρκεια της εκτέλεσης θα εμφανιστούν αρκετά μηνύματα τα οποία αγνοούμε. Επίσης, μόλις ολοκληρωθεί η διαδικασία (Εικόνα 55) αναγράφεται ένας αριθμός ευπαθειών (vulnerabilities), τον οποίο ομοίως αγνοούμε.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\iden> npm install
```

Εικόνα 54 - Εκτέλεση της εντολής «npm install»



```
Administrator: Windows PowerShell
at @popperjs/core, this package is dedicated to the legacy v1
npm WARN                               cids@0.7.5: This module has been superseded by th
e multiformats module
npm WARN                               @ensdomains/ens@0.4.5: Please use @ensdomains/ens
-contracts
npm WARN                               @ensdomains/resolver@0.2.4: Please use @ensdomain
s/ens-contracts
npm WARN                               core-js@2.6.12: core-js@<3.4 is no longer maintai
ned and not recommended for usage due to the number of issues. Becaus
e of the V8 engine whims, feature detection in old core-js versions c
ould cause a slowdown up to 100x even if nothing is polyfilled. Pleas
e, upgrade your dependencies to the actual version of core-js.

added 1644 packages, and audited 1645 packages in 4m
113 packages are looking for funding
  run `npm fund` for details
45 vulnerabilities (1 low, 22 moderate, 21 high, 1 critical)

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

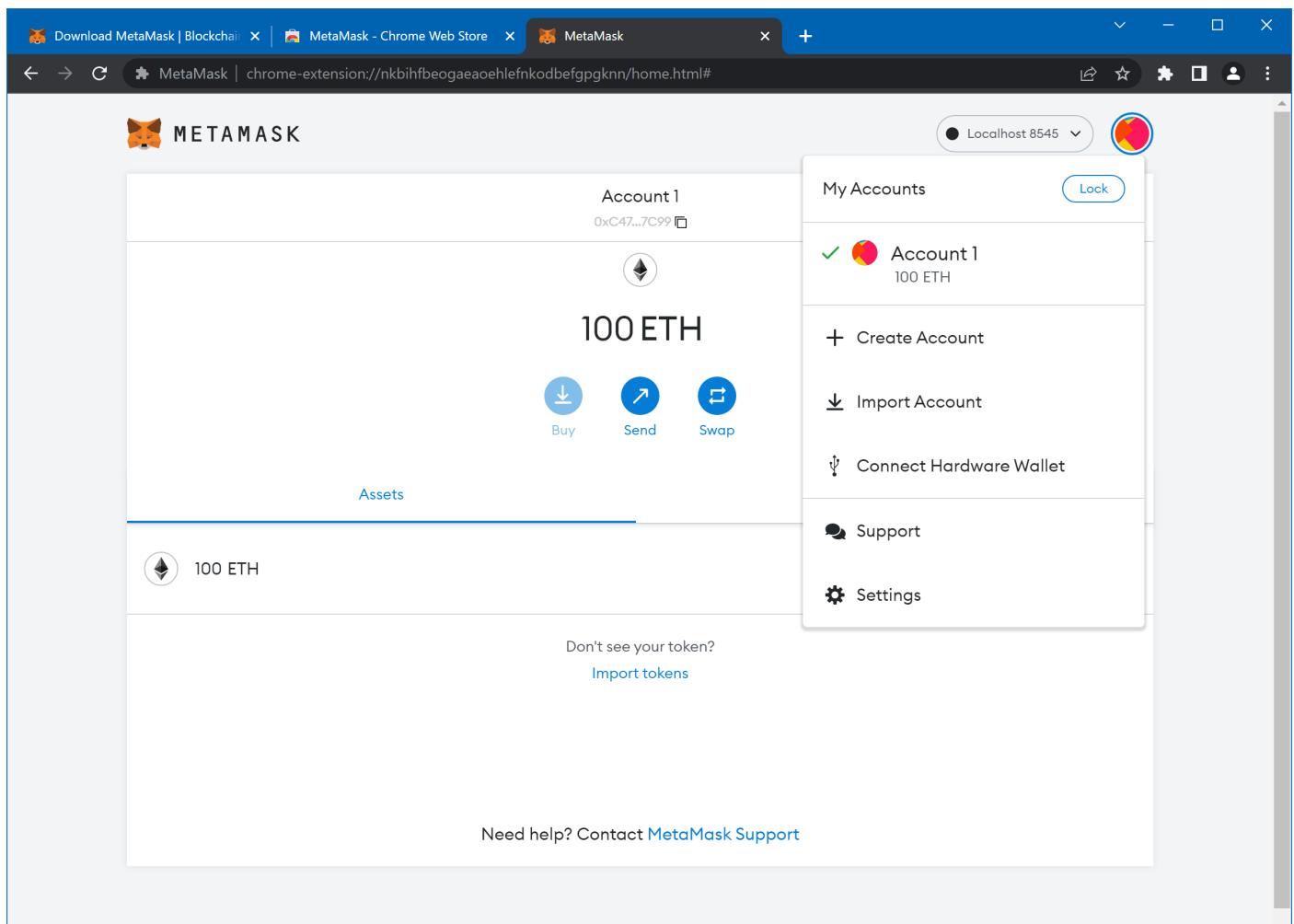
To address all issues (including breaking changes), run:
  npm audit fix --force

Run `npm audit` for details.
PS C:\Users\Administrator\Desktop\iden>
```

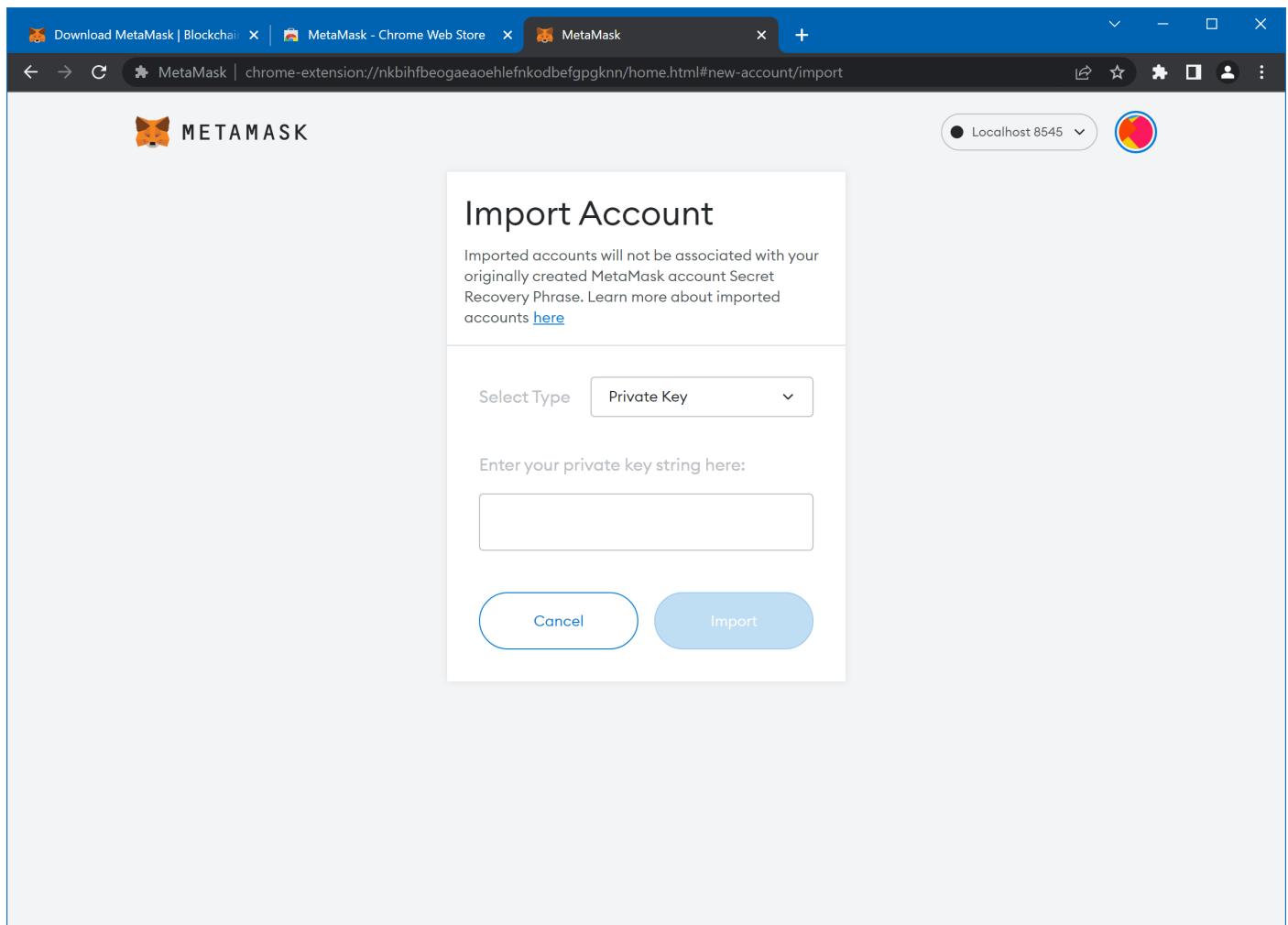
Εικόνα 55 - Αποτελέσματα της εντολής «npm install»

4.5.2 Οδηγός εκτέλεσης της εφαρμογής

Καθώς η εφαρμογή αποτελείται από τρεις ρόλους (εκδότη, πολίτη και επαληθευτή), είναι απαραίτητη η προσθήκη των αντίστοιχων λογαριασμών «πορτοφολιού» στο «Metamask». Λόγω της εισαγωγής ενός υπάρχοντος «πορτοφολιού» με τη χρήση του «Mnemonic» που παρέχει το «Ganache» (βλ. σελίδα 67), έχει προστεθεί αυτόματα ο πρώτος από τους δέκα λογαριασμούς που δημιουργήθηκαν κατά την εγκατάστασή του. Συνεπώς, πρέπει να γίνει προσθήκη ακόμη δύο λογαριασμών «πορτοφολιού» στο «Metamask». Αφού έχουμε συνδεθεί στο τοπικό δίκτυο του «Ganache» μέσω του «Metamask» (βλ. σελίδες 68, 69, 70), κάνουμε «κλικ» στον κύκλο με το μπλε περίγραμμα στο πάνω δεξί άκρο του περιβάλλοντος διαχείρισης πορτοφολιού και στη συνέχεια, στην επιλογή «Import Account» (Εικόνα 56). Ακολούθως, εμφανίζεται η σελίδα εισαγωγής λογαριασμού μέσω «ιδιωτικού κλειδιού» (Private Key) (Εικόνα 57).

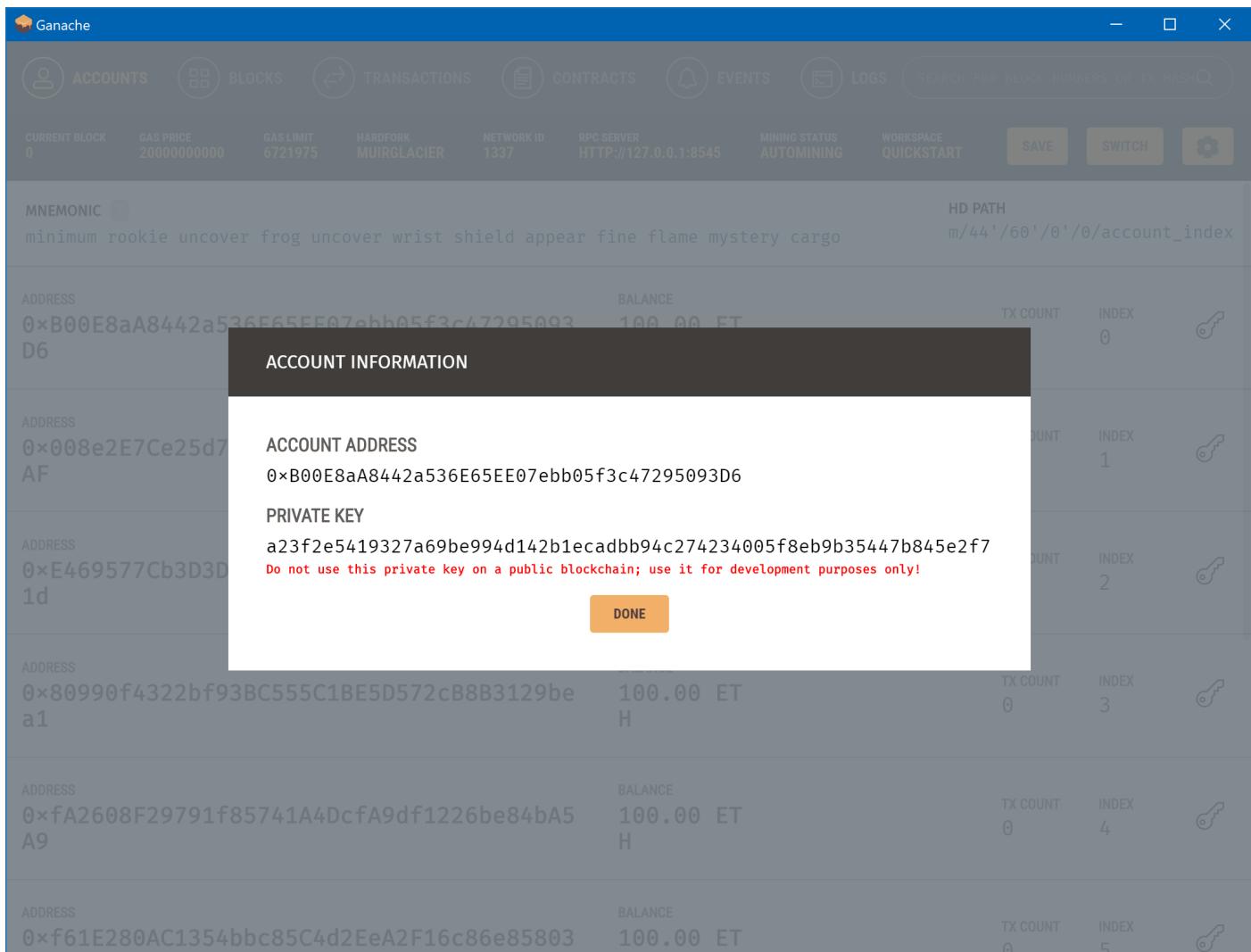


Εικόνα 56 - Μενού διαχείρισης λογαριασμού «πορτοφολιού» στο «Metamask»



Εικόνα 57 - Σελίδα εισαγωγής λογαριασμού μέσω «ιδιωτικού κλειδιού»

Έπειτα, επιστρέφουμε στο παράθυρο διαχείρισης του Blockchain του «Ganache» (βλ. σελίδα 62) και «πατάμε» στο εικονίδιο του κλειδιού που βρίσκεται στα δεξιά του λογαριασμού με «Index» 1 (ο πρώτος λογαριασμός που προστέθηκε αυτόματα έχει «Index» 0). Κατόπιν, εμφανίζεται το παράθυρο πληροφοριών λογαριασμού (Εικόνα 58), από το οποίο αντιγράφουμε το αλφαριθμητικό που αντιστοιχεί στο «Private Key», το επικολλούμε στο κενό πεδίο της Εικόνας 57 και κάνουμε «κλικ» στο κουμπί «Import».



The screenshot shows the Ganache interface with the following details:

ADDRESS	BALANCE	TX COUNT	INDEX
0xB00E8aA8442a536E65EE07ebb05f3c47295093D6	100.00 ET	0	0
0x008e2E7Ce25d7AF	100.00 ET	0	1
0xE469577Cb3D3D1d	100.00 ET	0	2
0x80990f4322bf93BC555C1BE5D572cB8B3129bea1	100.00 ET	0	3
0xfA2608F29791f85741A4DcfA9df1226be84bA5A9	100.00 ET	0	4
0xf61E280AC1354bbc85C4d2EeA2F16c86e85803	100.00 ET	0	5

A modal window titled "ACCOUNT INFORMATION" is open for the account at index 2, showing the account address and a warning about the private key:

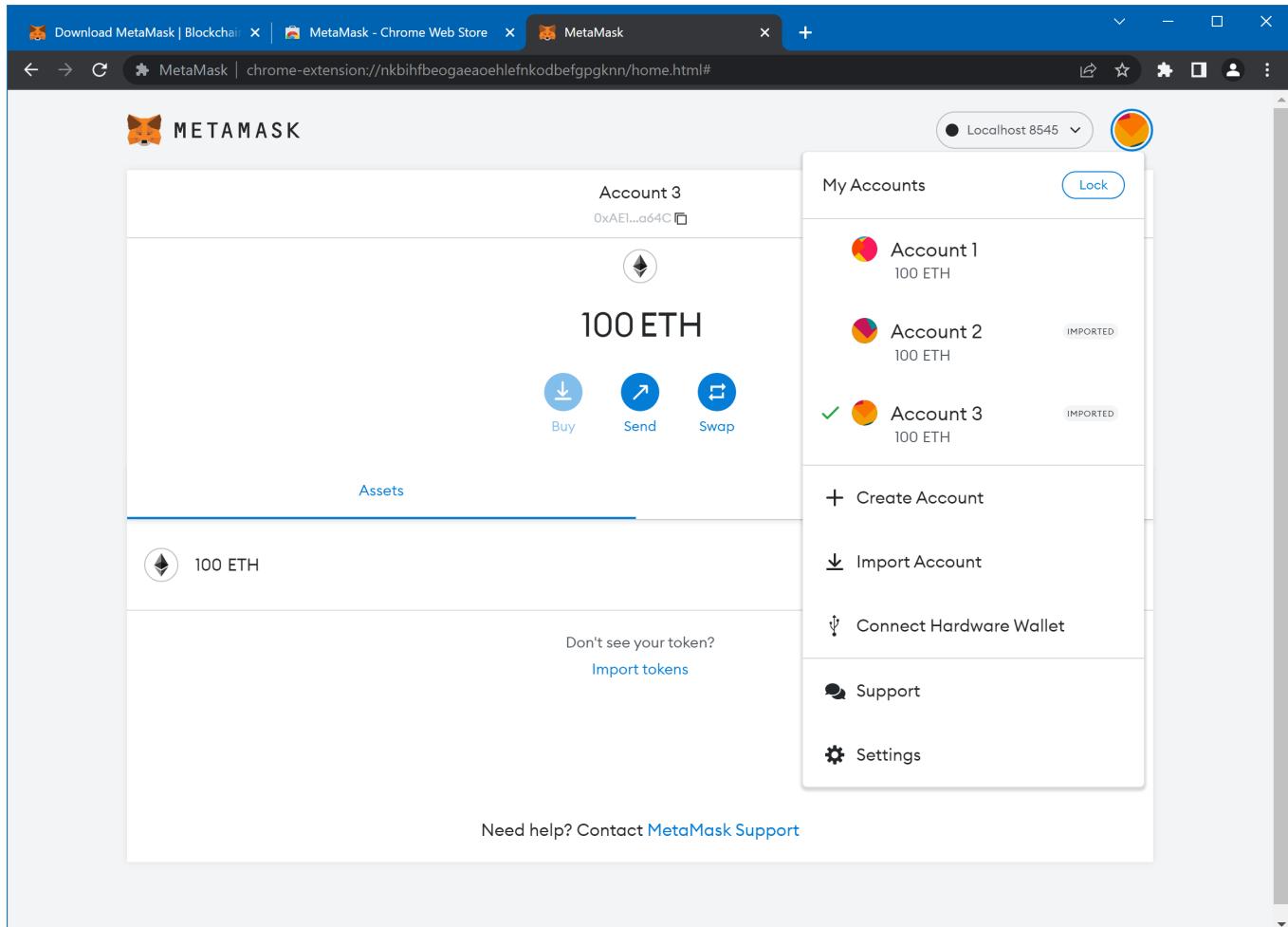
ACCOUNT ADDRESS
0xB00E8aA8442a536E65EE07ebb05f3c47295093D6

PRIVATE KEY
a23f2e5419327a69be994d142b1ecadbb94c274234005f8eb9b35447b845e2f7
Do not use this private key on a public blockchain; use it for development purposes only!

DONE

Εικόνα 58 - Παράθυρο πληροφοριών λογαριασμού στο «Ganache»

Ακολουθούμε την ίδια διαδικασία και για τον επόμενο λογαριασμό του «Ganache» (με «Index» 2), ούτως ώστε το μενού διαχείρισης λογαριασμού του «Metamask» να μοιάζει όπως αντό της Εικόνας 59.



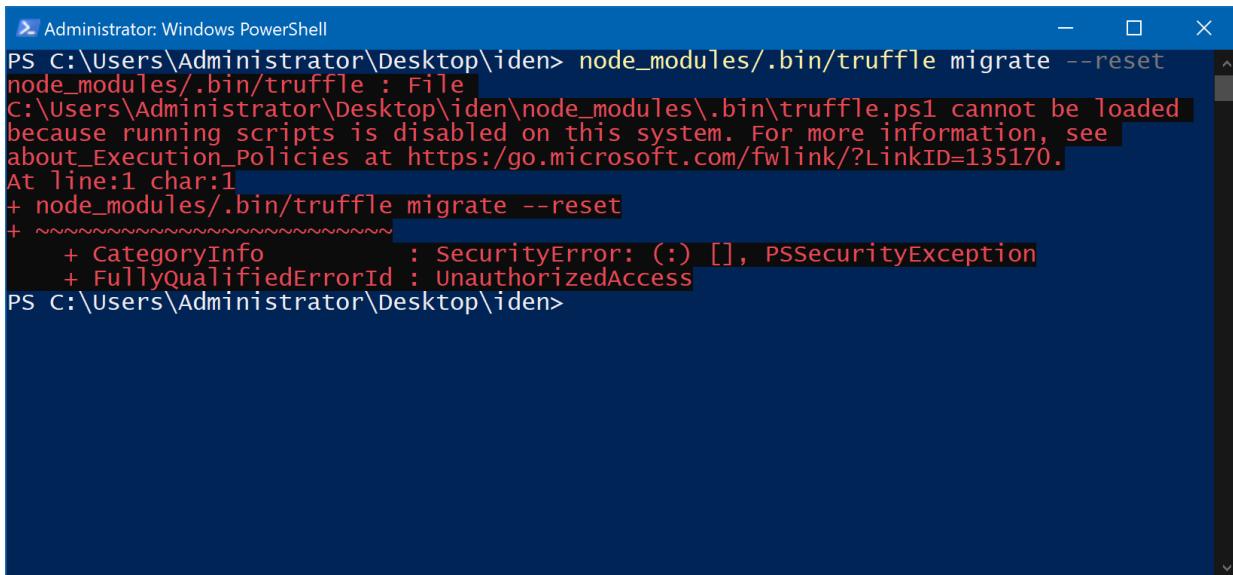
Εικόνα 59 - Μενού διαχείρισης λογαριασμού «πορτοφολιού» στο «Metamask» με τους τρεις λογαριασμούς συνδεμένους

Στη συνέχεια, «ανοίγουμε» ένα παράθυρο «Windows PowerShell» στον φάκελο της εφαρμογής (βλ. σελίδα 75), αφού πρώτα έχει ολοκληρωθεί η διαδικασία μιας εκ των δύο εντολών: «npm rebuild» και «npm install» (βλ. σελίδες 75, 76, 77). Όπως διακρίνεται στην Εικόνα 60, πληκτρολογούμε την εντολή «node_modules/.bin/truffle migrate --reset» για να αποθηκευτεί ο κώδικας των «έξυπνων» συμβολαίων στο τοπικό Blockchain και να τεθεί έτοιμος προς εκτέλεση.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\iden> node_modules/.bin/truffle migrate --reset
```

Εικόνα 60 - Εκτέλεση της εντολής «node_modules/.bin/truffle migrate --reset»

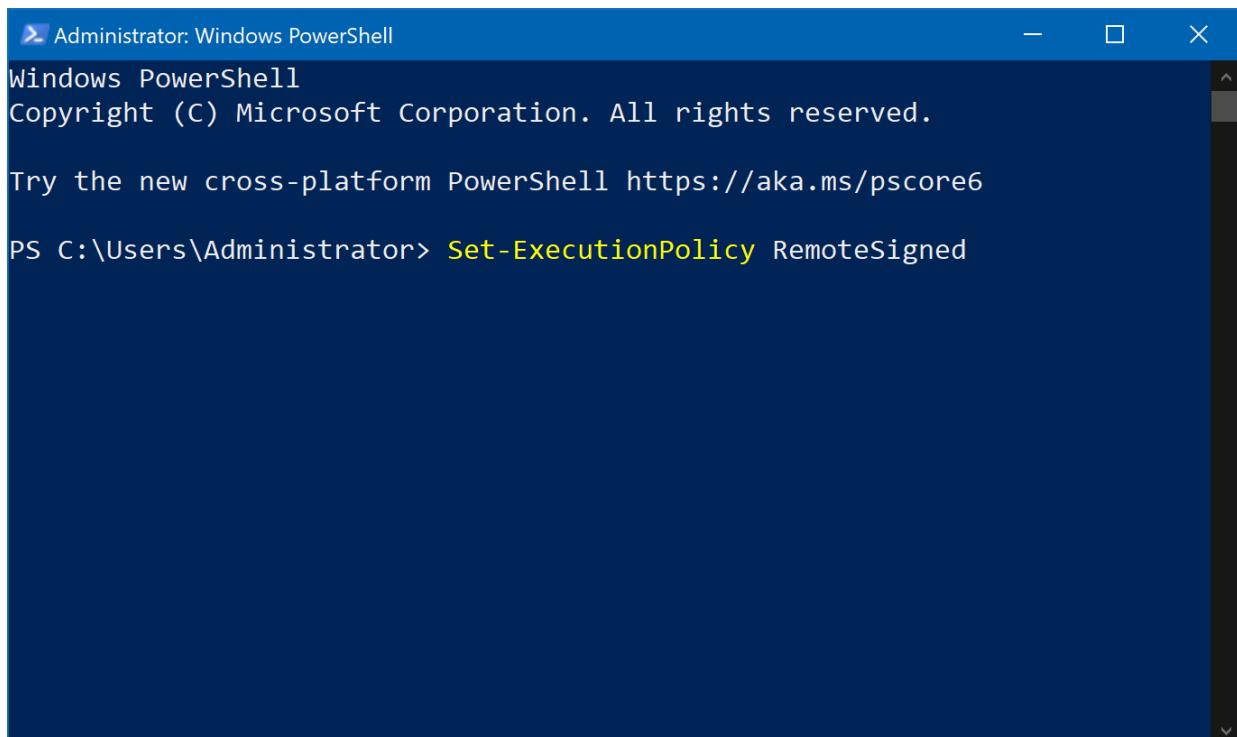
Σε περίπτωση που παρουσιαστεί το σφάλμα της Εικόνας 61, μεταβαίνουμε στην αναζήτηση των «Windows» και «ανοίγουμε» ένα νέο παράθυρο «Windows PowerShell» με δικαιώματα διαχειριστή. Εκεί, εισάγουμε και εκτελούμε την εντολή «Set-ExecutionPolicy RemoteSigned» (Εικόνα 62) και στη συνέχεια, πληκτρολογούμε τον χαρακτήρα «A», όπως ζητείται (Εικόνα 63).



```

Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\iden> node_modules/.bin/truffle migrate --reset
node_modules/.bin/truffle : File
C:\users\Administrator\Desktop\iden\node_modules\.bin\truffle.ps1 cannot be loaded
because running scripts is disabled on this system. For more information, see
about_Execution_Policies at https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ node_modules/.bin/truffle migrate --reset
+ ~~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\Administrator\Desktop\iden>
  
```

Εικόνα 61 - Σφάλμα κατά την εκτέλεση της εντολής «node_modules/.bin/truffle migrate --reset»



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Administrator> Set-ExecutionPolicy RemoteSigned
  
```

Εικόνα 62 - Εκτέλεση της εντολής «Set-ExecutionPolicy RemoteSigned»

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell <https://aka.ms/pscore6>

PS C:\Users\Administrator> **Set-ExecutionPolicy RemoteSigned**

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the **about_Execution_Policies** help topic at <https://go.microsoft.com/fwlink/?LinkID=135170>. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):A

Εικόνα 63 - Συνέχεια της εκτέλεσης της εντολής «*Set-ExecutionPolicy RemoteSigned*»

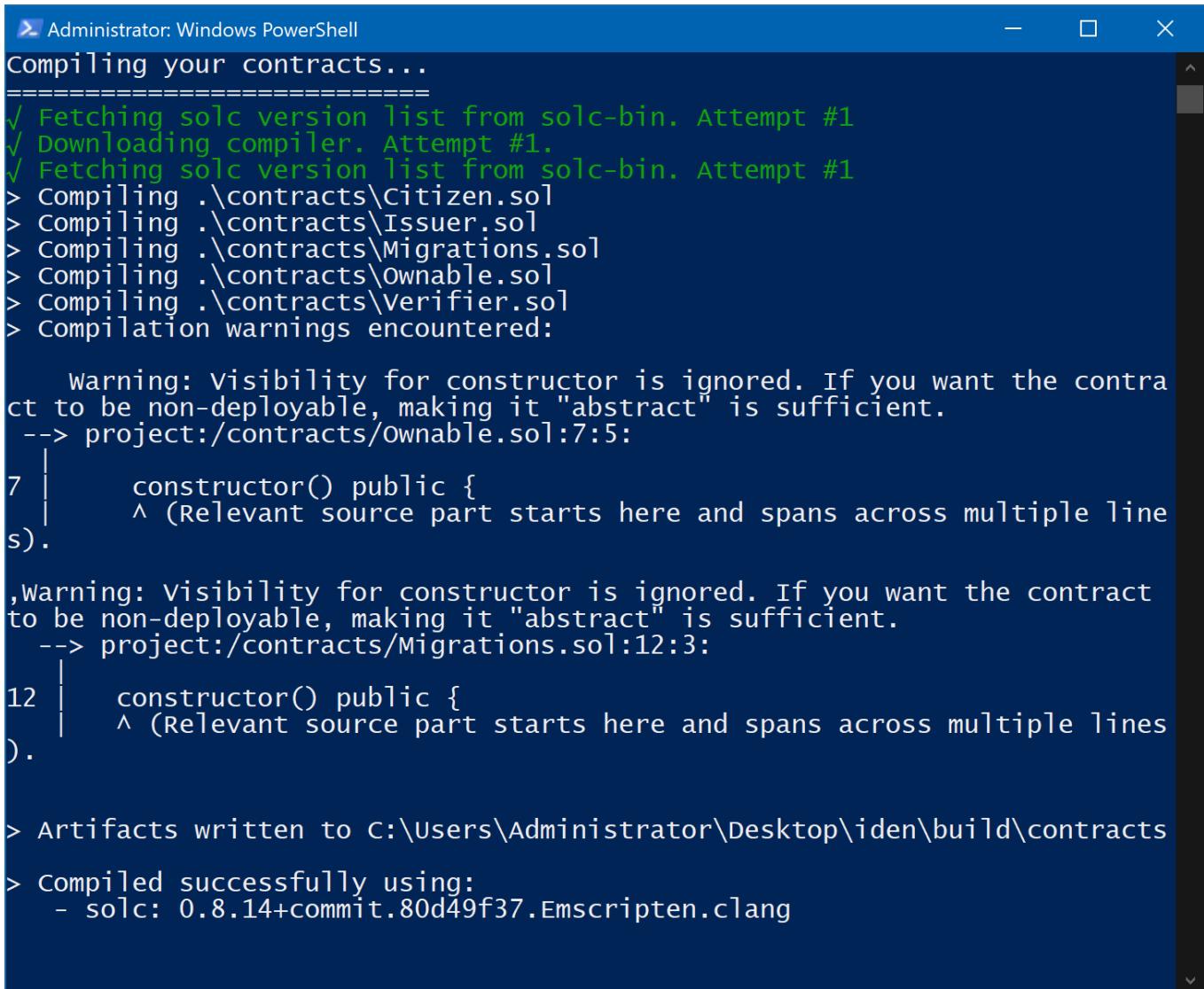
Αφού ολοκληρωθεί η διαδικασία, επιστρέφουμε στο προηγούμενο παράθυρο «Windows PowerShell» και εκτελούμε ξανά την εντολή «node_modules/.bin/truffle migrate --reset» (Εικόνα 64).

Administrator: Windows PowerShell

PS C:\Users\Administrator\Desktop\iden> node_modules/.bin/truffle migrate --reset
node_modules/.bin/truffle : File
c:\Users\Administrator\Desktop\iden\node_modules\.bin\truffle.ps1 cannot be loaded
because running scripts is disabled on this system. For more information, see
about_Execution_Policies at <https://go.microsoft.com/fwlink/?LinkID=135170>.
At line:1 char:1
+ node_modules/.bin/truffle migrate --reset
+ ~~~~~~
+ CategoryInfo : SecurityError: () [], PSInvalidOperationException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\Administrator\Desktop\iden> node_modules/.bin/truffle migrate --reset

Εικόνα 64 - Επανεκτέλεση της εντολής «*node_modules/.bin/truffle migrate --reset*»

Μόλις εκτελέσουμε την παραπάνω εντολή, ξεκινά η μεταγλώττιση του κώδικα των «έξυπνων» συμβολαίων σε «bytecode» (βλ. σελίδες 56, 57) (Εικόνα 65), ενώ αφού διεκπεραιωθεί η διεργασία, αναγράφονται, για κάθε «έξυπνο» συμβόλαιο που αποθηκεύτηκε στο Blockchain, πληροφορίες όπως η διεύθυνση του, ο λογαριασμός που χρεώθηκε τη συναλλαγή (στο «Ganache» είναι ο λογαριασμός με «Index» 0), το υπόλοιπό του λογαριασμού, καθώς και το συνολικό κόστος για να πραγματοποιηθεί η συναλλαγή (βλ. σελίδες 57, 58) (Εικόνα 66).



```

Administrator: Windows PowerShell
Compiling your contracts...
=====
✓ Fetching solc version list from solc-bin. Attempt #1
✓ Downloading compiler. Attempt #1.
✓ Fetching solc version list from solc-bin. Attempt #1
> Compiling .\contracts\Citizen.sol
> Compiling .\contracts\Issuer.sol
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Ownable.sol
> Compiling .\contracts\Verifier.sol
> Compilation warnings encountered:

    Warning: visibility for constructor is ignored. If you want the contract to be non-deployable, making it "abstract" is sufficient.
    --> project:/contracts/Ownable.sol:7:5:
    7 |     constructor() public {
    |         ^
    |         (Relevant source part starts here and spans across multiple lines).
    ,Warning: visibility for constructor is ignored. If you want the contract to be non-deployable, making it "abstract" is sufficient.
    --> project:/contracts/Migrations.sol:12:3:
    12 |     constructor() public {
    |         ^
    |         (Relevant source part starts here and spans across multiple lines).

> Artifacts written to C:\Users\Administrator\Desktop\iden\build\contracts
> Compiled successfully using:
  - solc: 0.8.14+commit.80d49f37.Emscripten clang

```

Εικόνα 65 - Η διαδικασία μεταγλώττισης του κώδικα των «έξυπνων» συμβολαίων σε «bytecode»

```
Administrator: Windows PowerShell
=====
Replacing 'Issuer'
-----
> transaction hash: 0x89a718707d36af4df802e127cc8992c1387cd9b3a48bdf
a17b6d793993979ac0
> Blocks: 0
> contract address: 0x8Df8823b40229B7E9eB42405f9EC4818b890069d
> block number: 3
> block timestamp: 1653256943
> account: 0xB00E8aA8442a536E65EE07ebb05f3c47295093D6
> balance: 99.98717918
> gas used: 469353 (0x72969)
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.00938706 ETH

Replacing 'Citizen'
-----
> transaction hash: 0xe054df83db4ebfacaf6dad42db14aeeecfa5895605fc820
b39cbcbecc267315d
> Blocks: 0
> contract address: 0x39c4663B2866AD0851aB514D9B4F6ED0f4d43093
> block number: 4
> block timestamp: 1653256943
> account: 0xB00E8aA8442a536E65EE07ebb05f3c47295093D6
> balance: 99.9518425
> gas used: 1766834 (0x1af5b2)
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.03533668 ETH

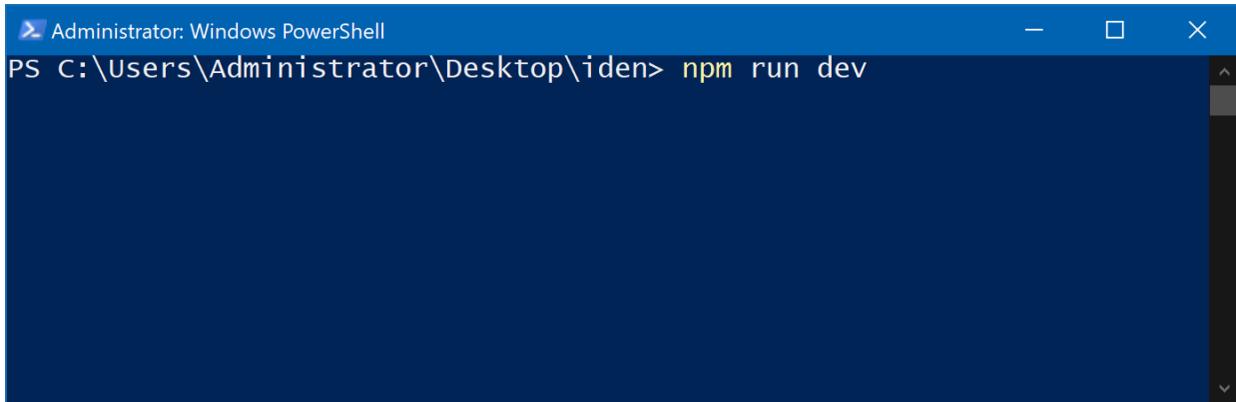
Replacing 'Verifier'
-----
> transaction hash: 0x173d560d868c31b8a296672da28d87e53b72299d3bf14d
5aabf5a987a5836055
> Blocks: 0
> contract address: 0x39B1246811daB08e13a808AEd172D748673Af742
> block number: 5
> block timestamp: 1653256944
> account: 0xB00E8aA8442a536E65EE07ebb05f3c47295093D6
> balance: 99.92437064
> gas used: 1373593 (0x14f599)
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.02747186 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost: 0.0721956 ETH

Summary
=====
> Total deployments: 4
> Final cost: 0.0747834 ETH
```

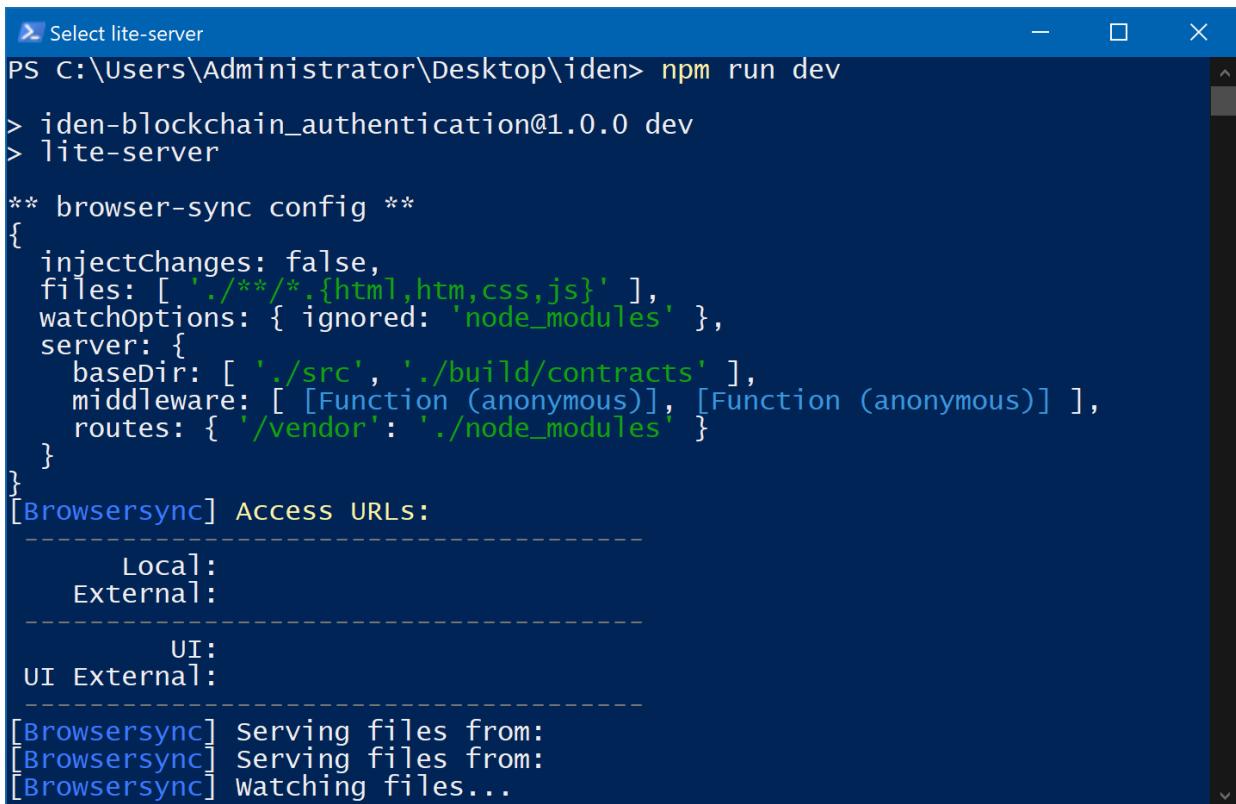
Εικόνα 66 - Ολοκλήρωση της διαδικασίας μεταγλώττισης και παρουσίαση πληροφοριών για κάθε «έξυπνο» συμβόλαιο

Ολοκληρώνοντας, για να εκτελεστεί η εφαρμογή και να είναι προσβάσιμη από τον περιηγητή ιστού απαιτείται η εκτέλεση ακόμη μίας εντολής εντός του φακέλου της εφαρμογής με τη χρήση του «Windows PowerShell» (βλ. σελίδα 75). Η εντολή αυτή είναι η «npm run dev» (Εικόνα 67) και σκοπός της είναι η εκκίνηση ενός τοπικού διακομιστή στον οποίο θα εκτελεστεί ο κώδικας της εφαρμογής παράλληλα με το Node.js και τα modules του. Στην Εικόνα 68 παρουσιάζεται ο διακομιστής που εκτελείται, με τη χρήση του Node.js module «lite-server», ο οποίος θα πρέπει να μείνει ενεργός καθ' όλη τη διάρκεια εκτέλεσης της εφαρμογής.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\iden> npm run dev
```

Εικόνα 67 - Εκτέλεση της εντολής «npm run dev»



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\iden> npm run dev
> iden-blockchain_authentication@1.0.0 dev
> lite-server

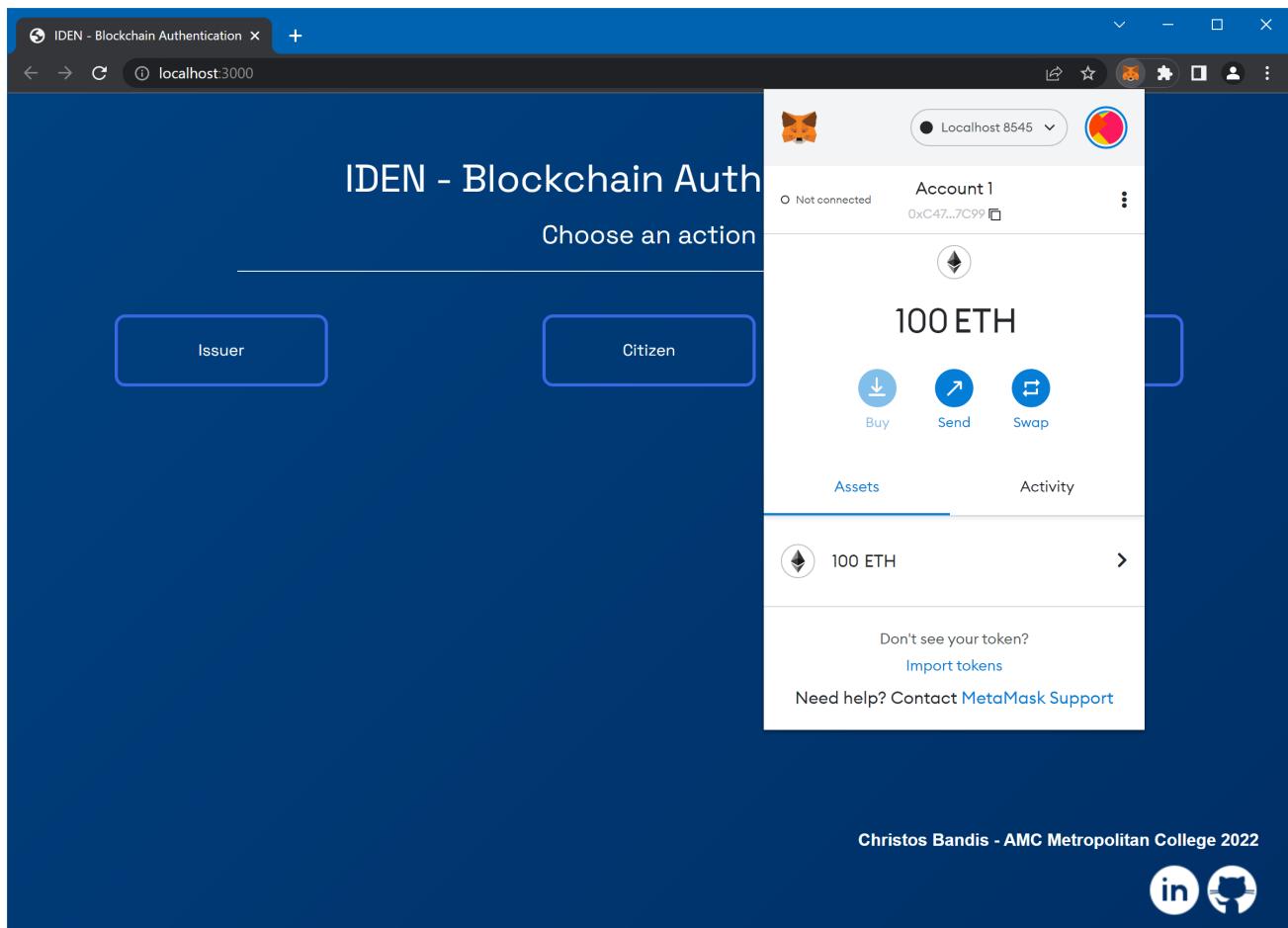
** browser-sync config **
{
  injectChanges: false,
  files: [ './**/*.{html,htm,css,js}' ],
  watchOptions: { ignored: 'node_modules' },
  server: {
    baseDir: [ './src', './build/contracts' ],
    middleware: [ [Function (anonymous)], [Function (anonymous)] ],
    routes: { '/vendor': './node_modules' }
  }
}
[Browsersync] Access URLs:
-----
  Local: http://127.0.0.1:3001
  External: http://192.168.1.7:3001
-----
  UI: http://127.0.0.1:3002
  External: http://192.168.1.7:3002
-----
[Browsersync] Serving files from: ./src
[Browsersync] Serving files from: ./build/contracts
[Browsersync] Watching files...
```

Εικόνα 68 - Παράδειγμα λειτουργίας του module «lite-server»

4.6. Περιγραφή περίπτωσης χρήσης

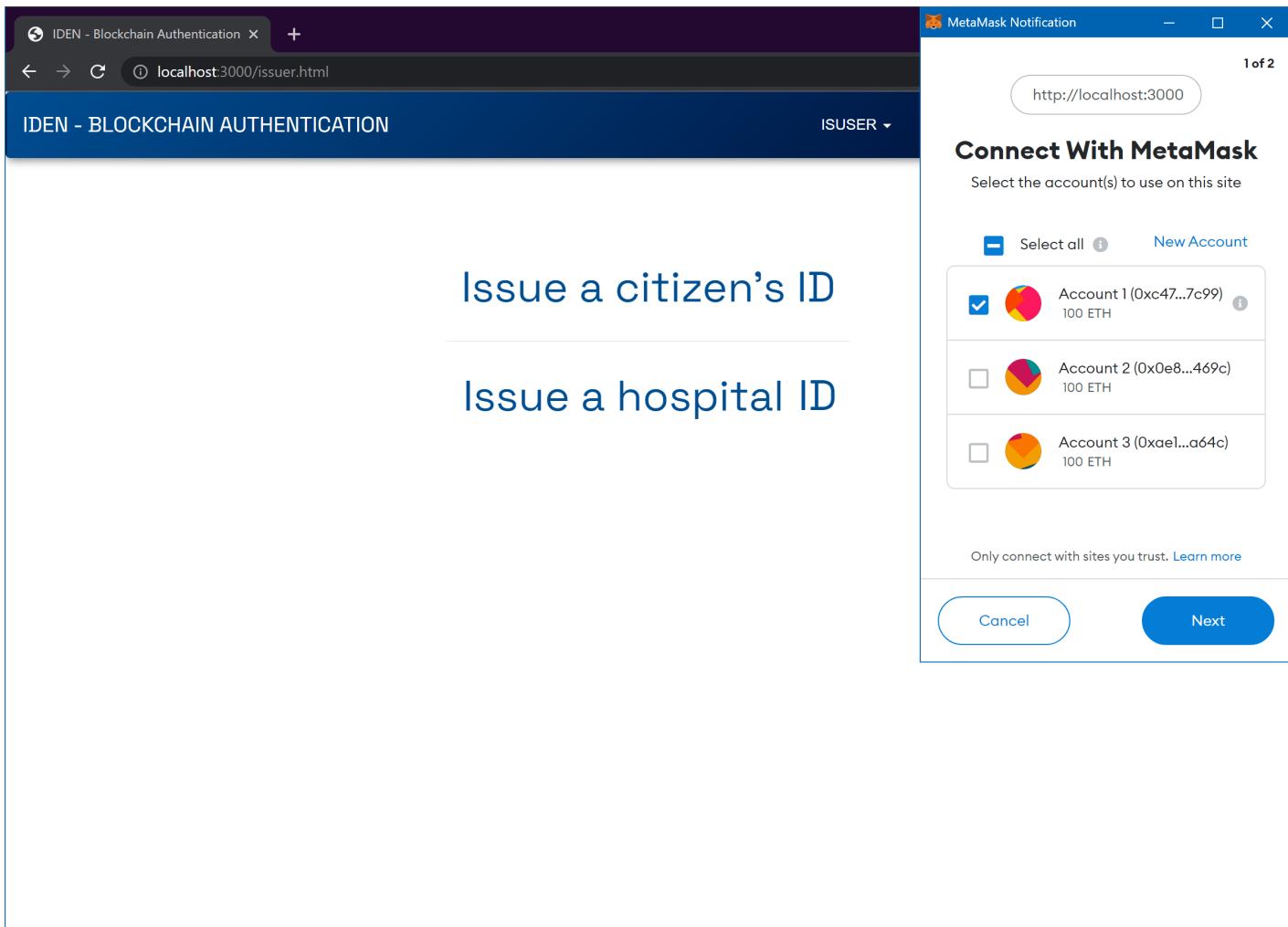
Όπως γίνεται αντιληπτό από τα διαγράμματα του Κεφαλαίου 4.2. Σχεδιασμός και Μοντελοποίηση, η εφαρμογή βασίζεται στην περίπτωση χρήσης στην οποία ένας πολίτης, μετά την καταχώριση της ταυτότητας του στο Blockchain από έναν εκδότη, πραγματοποιεί επίσκεψη σε ένα νοσοκομείο για εξέταση. Παρακάτω θα παρουσιαστεί το σύνολο των σταδίων της περίπτωσης χρήσης, τα οποία επιγραμματικά είναι: η καταχώριση της ταυτότητας του πολίτη και του νοσοκομείου στο Blockchain, η αποστολή ενός αιτήματος κοινοποίησης στοιχείων ταυτότητας από το νοσοκομείο προς τον πολίτη, η προβολή του αιτήματος και η απάντηση του από τον πολίτη, η επαλήθευση των στοιχείων του πολίτη από το νοσοκομείο, μέσω του «έξυπνου» συμβολαίου του εκδότη και τέλος, η προσθήκη/δημιουργία ενός ιατρικού ιστορικού για τον πολίτη από το νοσοκομείο. Για την ορθότερη κατανόηση του περιεχομένου του τρέχοντος κεφαλαίου, παράλληλα με το τρίτο ενικό, θα χρησιμοποιηθεί και το πρώτο πληθυντικό πρόσωπο.

Έχοντας προσθέσει τους υπόλοιπους λογαριασμούς «πορτοφολιών» στο «Metamask» (βλ. σελίδες 78, 79, 80, 81) και ενεργοποιήσει τον τοπικό διακομιστή (βλ. σελίδα 86), η πρόσβαση στην εφαρμογή πραγματοποιείται μέσω της διεύθυνσης [«http://localhost:3000/»](http://localhost:3000/). Βασική αποτελεί η επιβεβαίωση πως ο επιλεγμένος λογαριασμός είναι αυτός με την ονομασία «Account 1» (εφ' εξής «εκδότης») (Εικόνα 69), καθώς οι λογαριασμοί «Account 2» (εφ' εξής «πολίτης») και «Account 3» (εφ' εξής «νοσοκομείο») θα χρησιμοποιηθούν για τους υπόλοιπους δύο ρόλους.



Εικόνα 69 - Επιβεβαίωση πως ο επιλεγμένος λογαριασμός είναι ο «Account 1»

Αρχικά, κάνοντας «κλικ» στο κουμπί «Issuer» εμφανίζεται η σελίδα επιλογής του τύπου της ταυτότητας προς καταχώριση. Μόλις ολοκληρωθεί η φόρτωση της σελίδας, αναδύεται το παράθυρο του «Metamask», το οποίο ζητά τη σύνδεση του λογαριασμού στην εφαρμογή (Εικόνα 70). Αφού συνδεθούμε, «πατάμε» τον σύνδεσμο «Issue a citizen's ID».



Εικόνα 70 - Παράθυρο του «Metamask» για τη σύνδεση λογαριασμού στην εφαρμογή

Αρχικά, από το παράθυρο διαχείρισης του «Ganache» (βλ. σελίδα 62), αντιγράφουμε το αλφαριθμητικό που αντιστοιχεί στο «Address» του λογαριασμού με «Index» 1, δηλαδή του πολίτη και το επικολλούμε στο πρώτο πεδίο της φόρμας της Εικόνας 71. Έπειτα, συμπληρώνουμε τα υπόλοιπα πεδία με τα στοιχεία ταυτότητας του πολίτη και «πατάμε» το κουμπί «Submit».

IDEN - Blockchain Authentication X +

localhost:3000/issuerCitizen.html

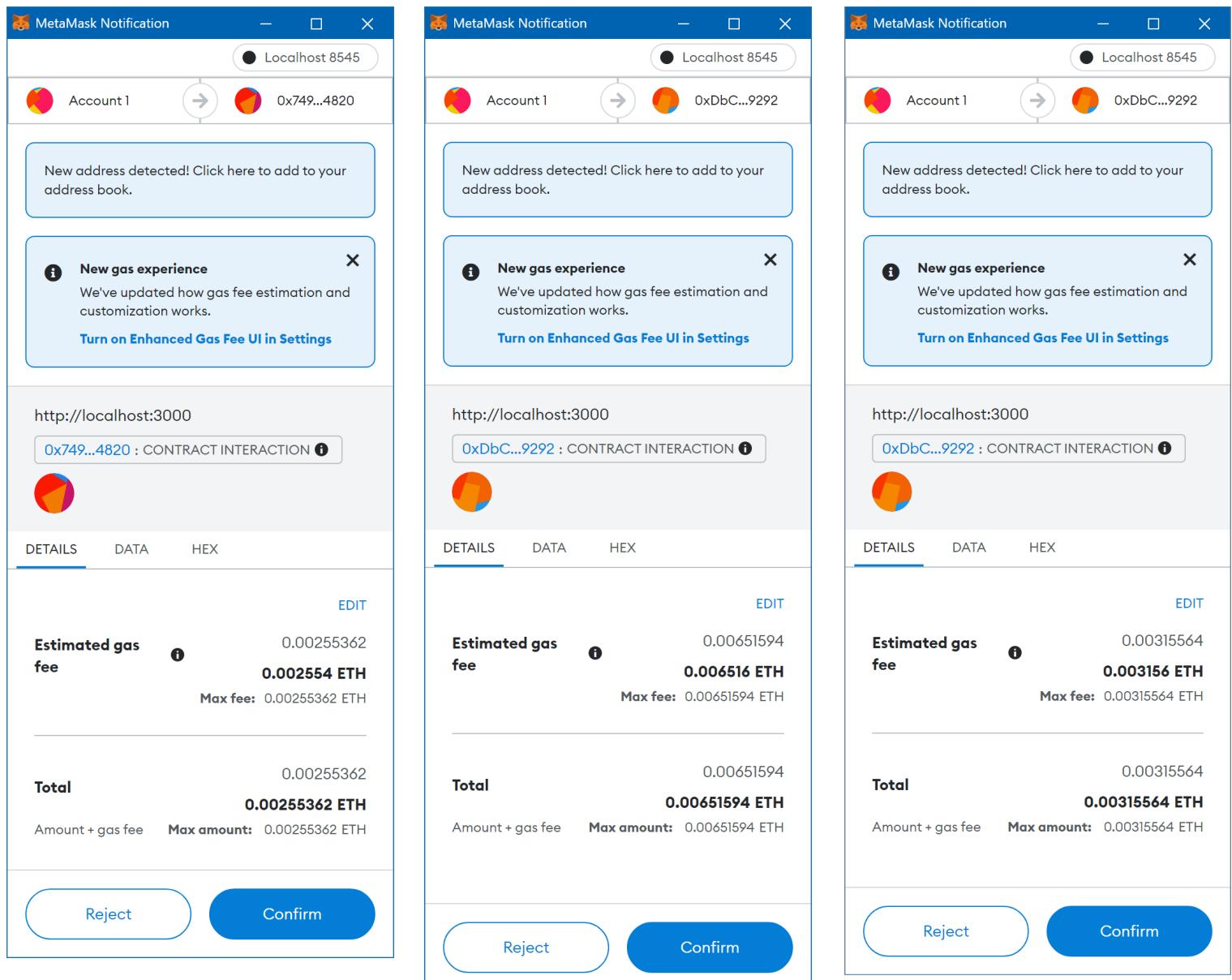
IDEN - BLOCKCHAIN AUTHENTICATION ISUSER CITIZEN VERIFIER 0XC4758...5127C99

Enter ID information

Wallet Address:	0x0E8D7d85eb1B78dB803334901508A6f24DEF469C	QR Scanner
Full Name:	Χρήστος Μπάντης	
Social Security No:	12345678	
Tax Identification No:	87654321	
Date of birth:	02/20/1997	<input type="button" value=""/>
Mobile Number:	6973979235	
Email:	chr.bandis@gmail.com	
Home Address:	Street 14, City 123 45	
<input type="button" value="Submit"/>		

Eikόνα 71 - Φόρμα καταχώρισης ταυτότητας πολίτη

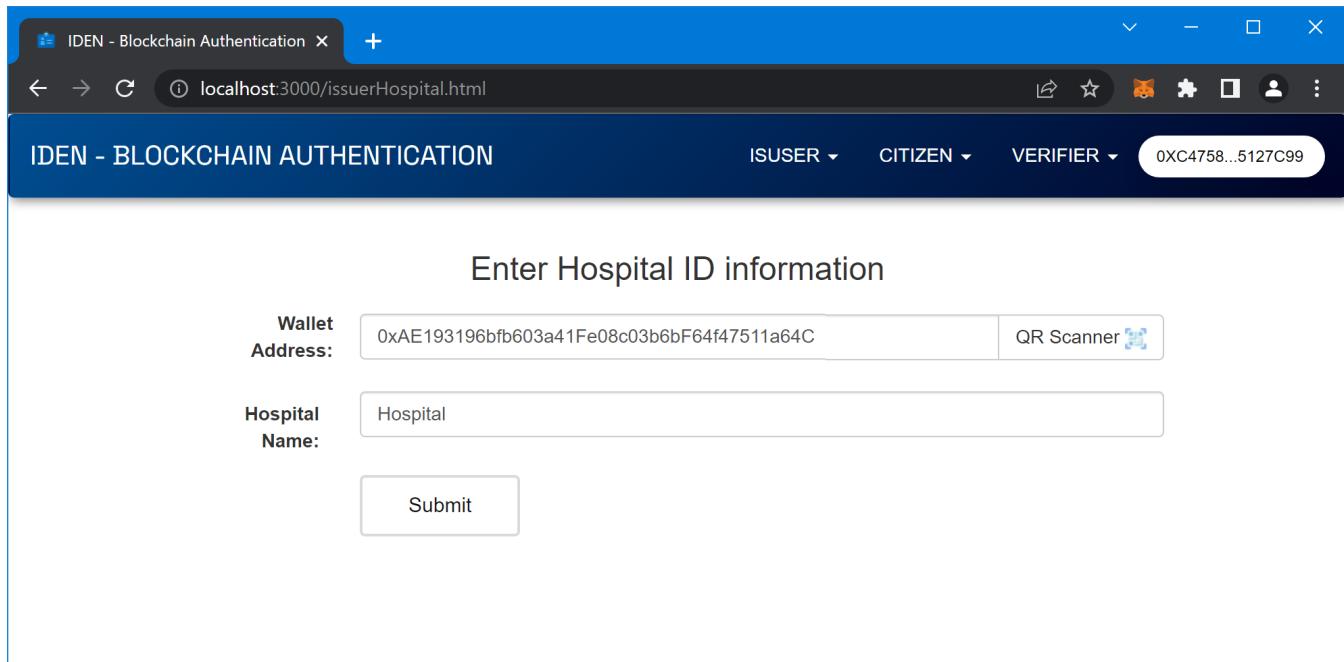
Αφότου κάνουμε «κλικ» στο κουμπί «Submit» εμφανίζονται κατά σειρά τρία παράθυρα έγκρισης συναλλαγής (Εικόνα 72), κάθε ένα για διαφορετικό σκοπό. Η πρώτη συναλλαγή αφορά την αποθήκευση των δεδομένων στο «έξυπνο» συμβόλαιο του πολίτη και την αντιστοίχισή τους με τη διεύθυνση του, με τη δεύτερη συναλλαγή αποθηκεύεται, στα στοιχεία της ταυτότητας του πολίτη, το «hash» (βλ. σελίδα 10) της πρώτης συναλλαγής (αυτό πραγματοποιείται σε δεύτερο χρόνο, καθώς πρέπει πρώτα να εκτελεστεί η πρώτη συναλλαγή και μετά να υπολογιστεί το «hash» της) και τέλος, ο λόγος ύπαρξης της τρίτης συναλλαγής είναι η αντιστοίχιση της διεύθυνσης του πολίτη με το παραγόμενο «hash» της συναλλαγής καταχώρισης της ταυτότητας και η αποθήκευση τους στο «έξυπνο» συμβόλαιο του εκδότη, για τον έλεγχο της εγκυρότητας της ταυτότητας του πολίτη από τον επαληθευτή.



Εικόνα 72 - Παράθυρα έγκρισης συναλλαγής κατά την καταχώριση ταυτότητας στο Blockchain

Η ίδια ακριβώς διαδικασία συναντάται και κατά τη καταχώριση της ταυτότητας του νοσοκομείου. Επιστρέφοντας στη σελίδα επιλογής του τύπου της ταυτότητας προς καταχώριση (Εικόνα 70) «πατάμε» τον σύνδεσμο «Issue a hospital ID». Από το παράθυρο διαχείρισης του «Ganache», αντιγράφουμε το αλφαριθμητικό που αντιστοιχεί στο «Address» του λογαριασμού με «Index» 2, δηλαδή του νοσοκομείου και το επικολλούμε στο πρώτο πεδίο της φόρμας της Εικόνας 73. Στη συνέχεια, πληκτρολογούμε το όνομα του νοσοκομείου και «πατάμε» το κουμπί «Submit». Όπως στη καταχώριση ταυτότητας πολίτη, έτσι και στη καταχώριση ταυτότητας

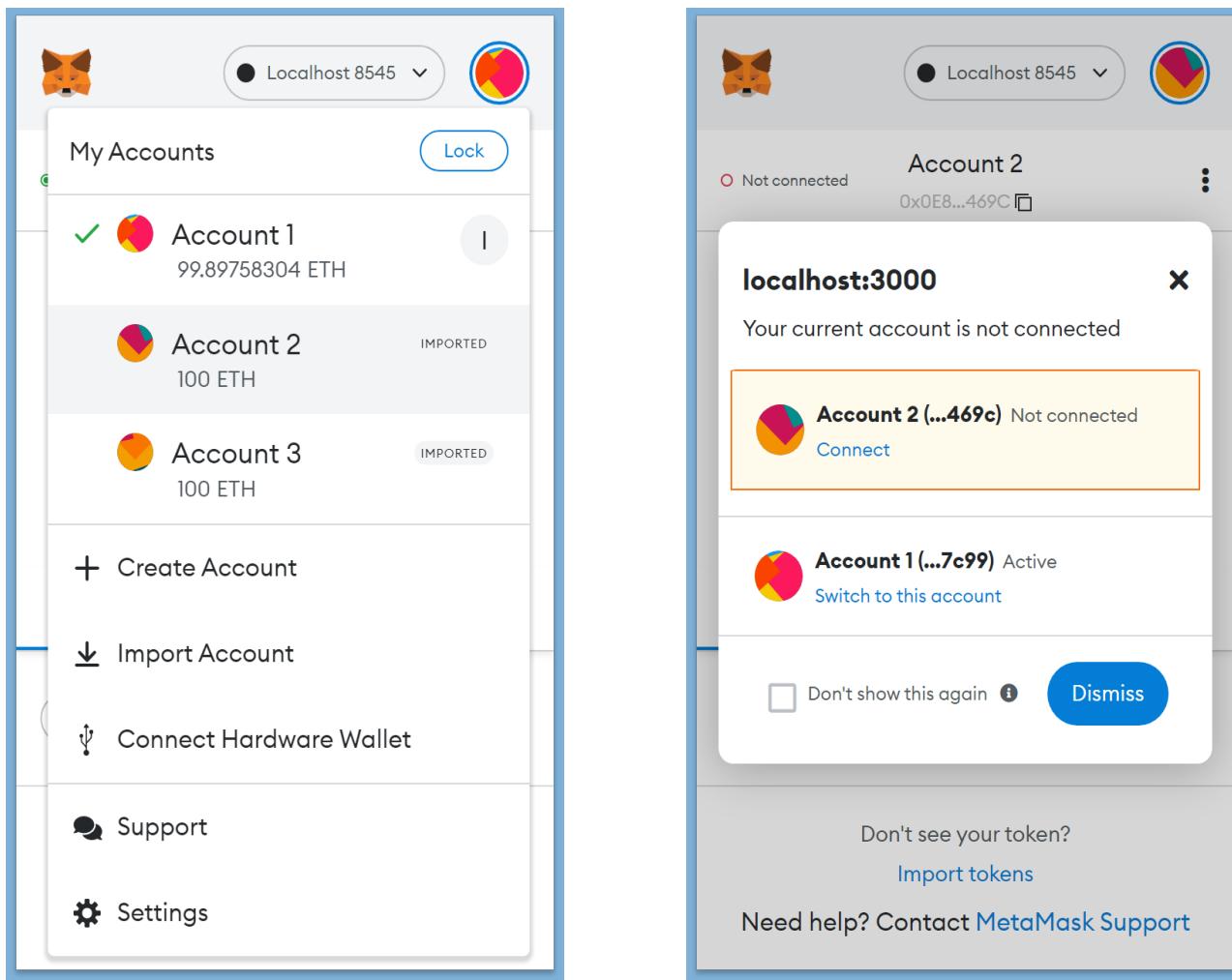
νοσοκομείου, εμφανίζονται τα τρία παράθυρα έγκρισης συναλλαγής, τα οποία επιτελούν τις αντίστοιχες ενέργειες.



The screenshot shows a web browser window titled "IDEN - Blockchain Authentication". The address bar displays "localhost:3000/issuerHospital.html". The main content area has a dark blue header with the text "IDEN - BLOCKCHAIN AUTHENTICATION" and three dropdown menus: "ISUSER", "CITIZEN", and "VERIFIER", followed by a wallet address "0XC4758...5127C99". Below the header, the text "Enter Hospital ID information" is centered. There are two input fields: "Wallet Address:" containing the value "0xAE193196bfb603a41Fe08c03b6bF64f47511a64C" and "Hospital Name:" containing the value "Hospital". A "Submit" button is located below the input fields. On the right side of the input fields, there is a "QR Scanner" icon.

Εικόνα 73 - Φόρμα καταχώρισης ταυτότητας νοσοκομείου

Προχωρώντας στον ρόλο του πολίτη, επιστρέφουμε στην αρχική σελίδα της εφαρμογής «πατώντας» στο λογότυπο στην πάνω αριστερή γωνία, επιλέγοντας τον δεύτερο λογαριασμό (πολίτη) στο «Metamask» και «πατάμε» «Connect» (Εικόνα 74). Αφού συνδεθούμε, κάνουμε «κλικ» στο κουμπί «Citizen» της αρχικής σελίδας για να μεταφερθούμε στη σελίδα με τα στοιχεία της ταυτότητας που αντιστοιχούν σε αυτόν τον λογαριασμό (Εικόνα 75).



Εικόνα 74 - Σύνδεση των δεύτερου λογαριασμού (πολίτη) στην εφαρμογή

IDEN - Blockchain Authentication X +

localhost:3000/citizen.html

IDEN - BLOCKCHAIN AUTHENTICATION ISUSER CITIZEN VERIFIER 0X0E8D7...DEF469C

Your ID info

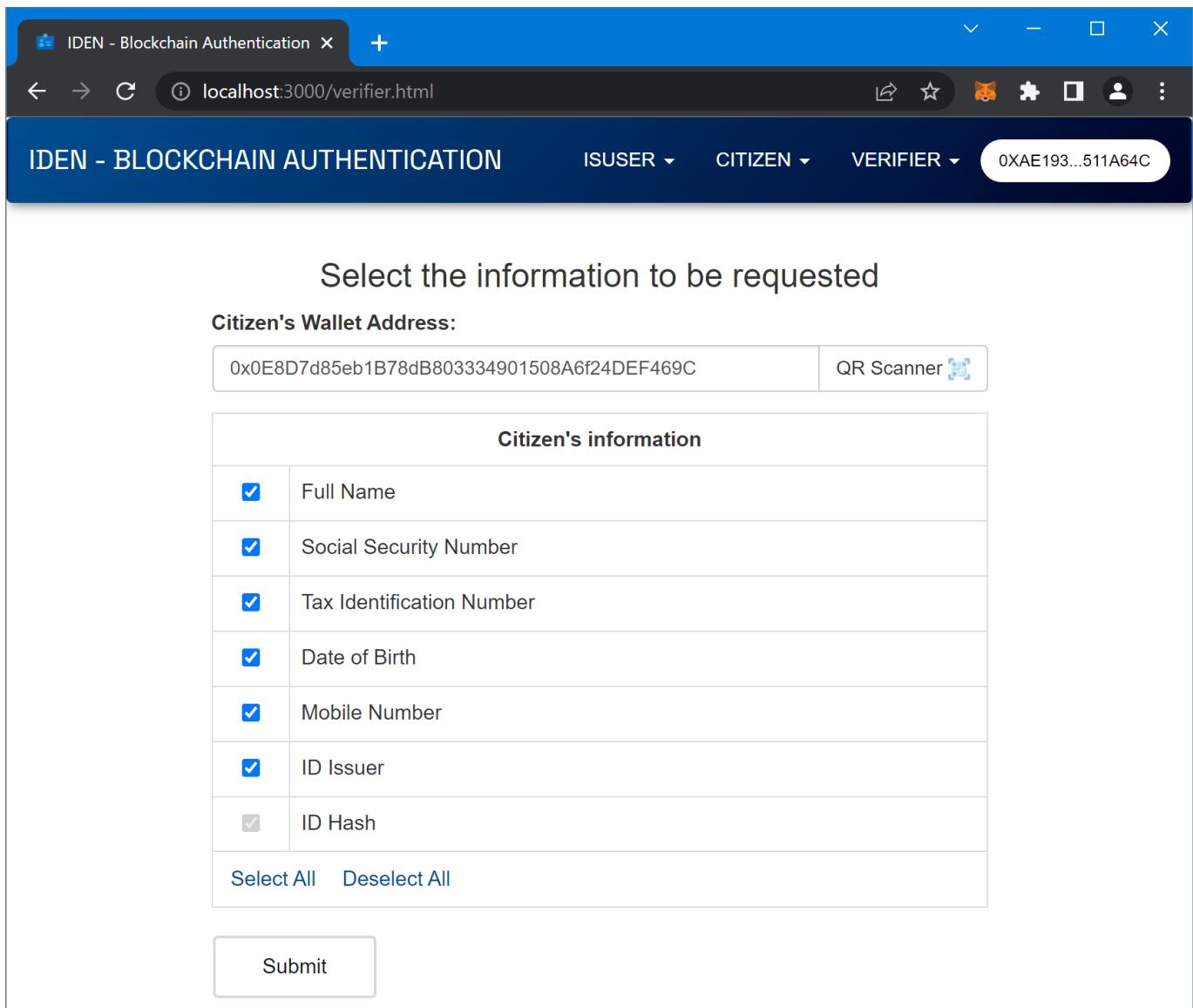
Wallet Address	0x0e8d7d85eb1b78db803334901508a6f24def469c
Full Name	Χρήστος Μπάντης
Social Security No:	12345678
Tax Identification No:	87654321
Date of Birth:	1997-02-20
Mobile Number:	6973979235
Email:	chr.bandis@gmail.com
Home Address:	Street 14, City 123 45
Issued By:	0xc475872d82ad6a62cbce639157bb6f1ed5127c99
ID Hash:	0xbcafb41f28ad034f6ae35cae1c2f82693e31606c94ed88a912fb0b36cb41c26c

Generate QR Code

Εικόνα 75 - Σελίδα με τις πληροφορίες ταυτότητας του πολίτη

Στη σελίδα που απεικονίζεται παραπάνω, εκτός από τα στοιχεία του πολίτη, διακρίνουμε και τη διεύθυνση του λογαριασμού του εκδότη που καταχώρησε την ταυτότητα (Issued By), αλλά και το «hash» της συναλλαγής (ID Hash). Στο κάτω μέρος της σελίδας βρίσκεται το κουμπί «Generate QR Code», το οποίο χρησιμεύει στη δημιουργία ενός κωδικού «QR», που αντιστοιχεί στη διεύθυνση του πολίτη, για χρήση κατά τη προσθήκη/δημιουργία ενός ιατρικού ιστορικού, όταν απαιτείται η εισαγωγή της διεύθυνσης. Επίσης, στο άνω δεξιά άκρο της σελίδας, υπάρχει ένα εικονίδιο σε σχήμα «καμπάνας», σκοπός του οποίου είναι η εμφάνιση του αριθμού των αιτημάτων κοινοποίησης ταυτότητας που βρίσκονται σε αναμονή.

Συνεχίζοντας στον ρόλο του επαληθευτή – νοσοκομείου, η διαδικασία σύνδεσης του λογαριασμού (Account 3) είναι ίδια με αυτή του πολίτη (βλ. σελίδες 92, 93). Αφού επιστρέψουμε στην αρχική σελίδα της εφαρμογής, «πατάμε» στο κουμπί «Verifier» και μεταφερόμαστε στην σελίδα αίτησης κοινοποίησης στοιχείων ταυτότητας πολίτη (Εικόνα 76). Εδώ, ο χρήστης του λογαριασμού του νοσοκομείου, εισάγει στο πρώτο πεδίο τη διεύθυνση, είτε πληκτρολογώντας τη, είτε σαρώνοντας τον κωδικό «QR» που θα υποδείξει ο πολίτης. Κατόπιν, επιλέγει τα στοιχεία που επιθυμεί να επαληθεύσει και αποστέλλει το αίτημα στον πολίτη μέσω συναλλαγής. Αξίζει να σημειωθεί πως το πλαίσιο «ID Hash» παραμένει επιλεγμένο, χωρίς δυνατότητα αποεπιλογής, καθώς αποτελεί το στοιχείο στο οποίο βασίζεται η επικύρωση της γνησιότητας των στοιχείων.



The screenshot shows a web browser window titled "IDEN - Blockchain Authentication". The address bar displays "localhost:3000/verifier.html". The main content area has a dark blue header with the text "IDEN - BLOCKCHAIN AUTHENTICATION" and three dropdown menus: "ISUSER", "CITIZEN", and "VERIFIER". The "VERIFIER" menu is currently selected, showing the hex value "0XAE193...511A64C". Below the header, the text "Select the information to be requested" is displayed. A section titled "Citizen's Wallet Address:" contains a text input field with the value "0x0E8D7d85eb1B78dB803334901508A6f24DEF469C" and a "QR Scanner" button. A table titled "Citizen's information" lists several items, each with a checked checkbox. The items are: Full Name, Social Security Number, Tax Identification Number, Date of Birth, Mobile Number, ID Issuer, and ID Hash. At the bottom of this table are two buttons: "Select All" and "Deselect All". A large "Submit" button is located at the bottom left of the form.

Εικόνα 76 - Σελίδα αίτησης κοινοποίησης στοιχείων ταυτότητας πολίτη

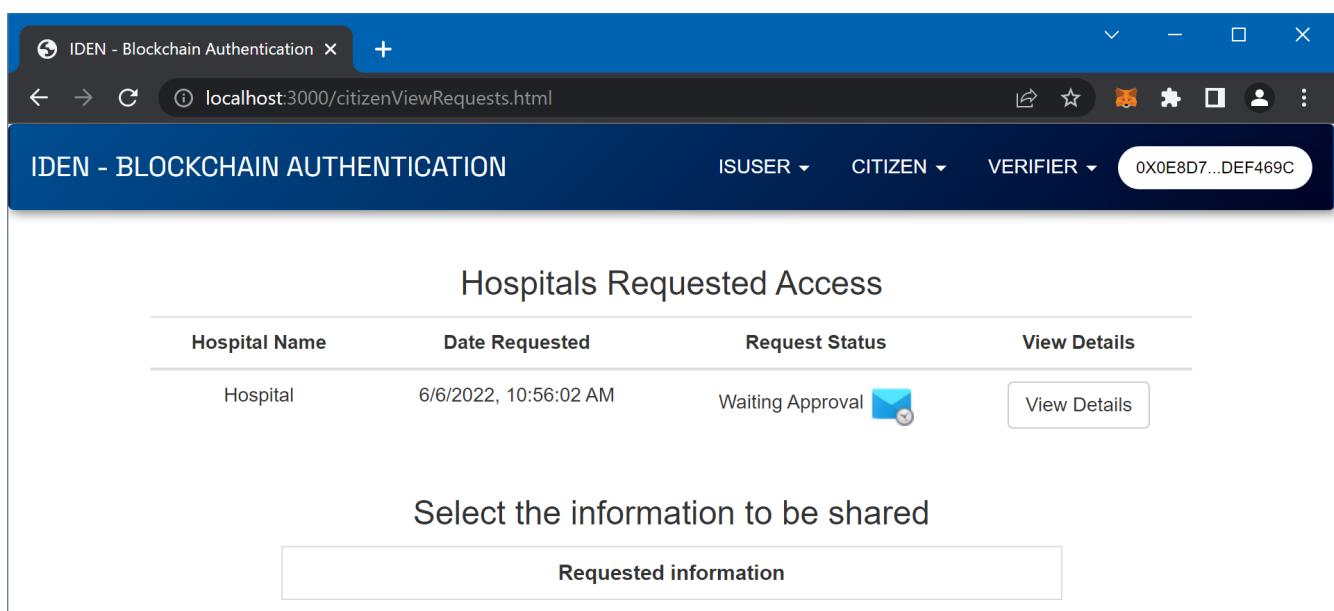
Αμέσως μόλις ολοκληρωθεί η συναλλαγή, το εικονίδιο των ειδοποιήσεων στη σελίδα του πολίτη τον ενημερώνει για το αναπάντητο αίτημα (Εικόνα 77). Κάνοντας «κλικ» επάνω του ή κάνοντας χρήση του μενού της εφαρμογής, ο πολίτης μεταβαίνει στη σελίδα των αιτημάτων (Εικόνα 78), που περιέχει όλα τα αιτήματα που έχει δεχτεί.

Your ID info



Wallet Address 0x0e8d7d85eb1b78db803334901508a6f24def469c

Εικόνα 77 - Ενημέρωση του πολίτη για το αναπάντητο αίτημα μέσω του εικονιδίου ειδοποίησης



The screenshot shows a web browser window titled "IDEN - Blockchain Authentication". The URL is "localhost:3000/citizenViewRequests.html". The top navigation bar includes links for "ISUSER", "CITIZEN", "VERIFIER", and a wallet address "0X0E8D7...DEF469C". Below the navigation, the title "IDEN - BLOCKCHAIN AUTHENTICATION" is displayed. The main content area is titled "Hospitals Requested Access" and lists one request:

Hospital Name	Date Requested	Request Status	Action
Hospital	6/6/2022, 10:56:02 AM	Waiting Approval 	View Details

Below this, a section titled "Select the information to be shared" contains a button labeled "Requested information".

Εικόνα 78 - Σελίδα των αιτημάτων του πολίτη

Τα περιεχόμενα των αιτήματος εμφανίζονται «πατώντας» το κουμπί «View Details». Στην αρχή των λεπτομερειών του αιτήματος αναγράφονται το όνομα και η διεύθυνση του αιτούντα. Τα πλαίσια που βρίσκονται μπροστά από κάθε αιτούμενο στοιχείο αποτελούν την «απάντηση» του πολίτη, καθώς η επιλογή οποιουδήποτε πλαισίου συνεπάγεται με την κοινοποίηση της αντίστοιχης πληροφορίας στο νοσοκομείο (Εικόνα 79). Αφού ο πολίτης επιλέξει τα στοιχεία που θέλει να μοιραστεί, τα αποστέλλει μέσω νέας συναλλαγής.

IDEN - Blockchain Authentication X +

localhost:3000/citizenViewRequests.html

IDEN - BLOCKCHAIN AUTHENTICATION ISUSER CITIZEN VERIFIER 0X0E8D7...DEF469C

Hospitals Requested Access

Hospital Name	Date Requested	Request Status	View Details
Hospital	6/6/2022, 10:56:02 AM	Waiting Approval 	View Details

Select the information to be shared

Requested by (Name):	Hospital
Requested by (Address):	0xae193196bf603a41fe08c03b6bf64f47511a64c

Requested information	
<input checked="" type="checkbox"/>	Full Name
<input checked="" type="checkbox"/>	Social Security Number
<input checked="" type="checkbox"/>	Tax Identification Number
<input checked="" type="checkbox"/>	Date of Birth
<input checked="" type="checkbox"/>	Mobile Number
<input checked="" type="checkbox"/>	ID Issuer
<input type="checkbox"/>	ID Hash
Select All Deselect All	

[Send](#)

Εικόνα 79 - Επιλογή των στοιχείων ταυτότητας προς κοινοποίηση από τον πολίτη

Ο χρήστης του λογαριασμού του νοσοκομείου με τη σειρά του, πλοηγείται μέσω του μενού στη σελίδα «View Requests», όπου εισάγει στο πλαίσιο αναζήτησης τη διεύθυνση, για την οποία επιθυμεί να εντοπίσει τα αιτήματα και «πατώντας» το κουμπί «View Details» αντικρίζει τα στοιχεία που κοινοποίησε ο πολίτης (Εικόνα 80).

IDEN - Blockchain Authentication X +

localhost:3000/verifierViewRequests.html

IDEN - BLOCKCHAIN AUTHENTICATION ISUSER CITIZEN VERIFIER 0XAE193...511A64C

Search Requests by Wallet Address

Wallet Address: 0xE8D7d85eb1B78dB803334901508A6f24DEF469C

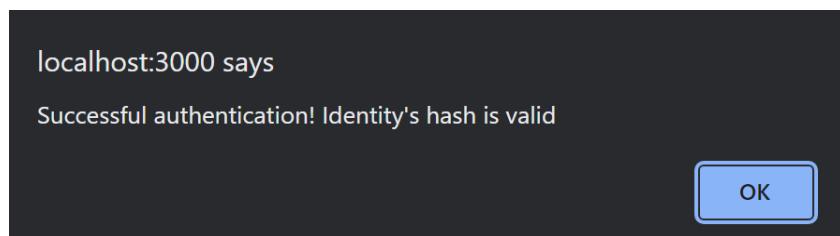
Date Requested	Request Status	View Details
6/6/2022, 10:56:02 AM	Approved 	View Details

Requested information		
✓ Full Name	Χρήστος Μπάντης	
✓ Social Security Number	12345678	
✓ Tax Identification Number	87654321	
✓ Date of Birth	1997-02-20	
✓ Mobile Number	6973979235	
✓ ID Issuer	0xc475872d82ad6a62cbce639157bb6f1ed5127c99	
✓ ID Hash	0xbcaf841f28ad034f6ae35cae1c2f82693e31606c94ed88a912fb0b36cb41c26c	

[Validate Identity](#) [Add a record](#)

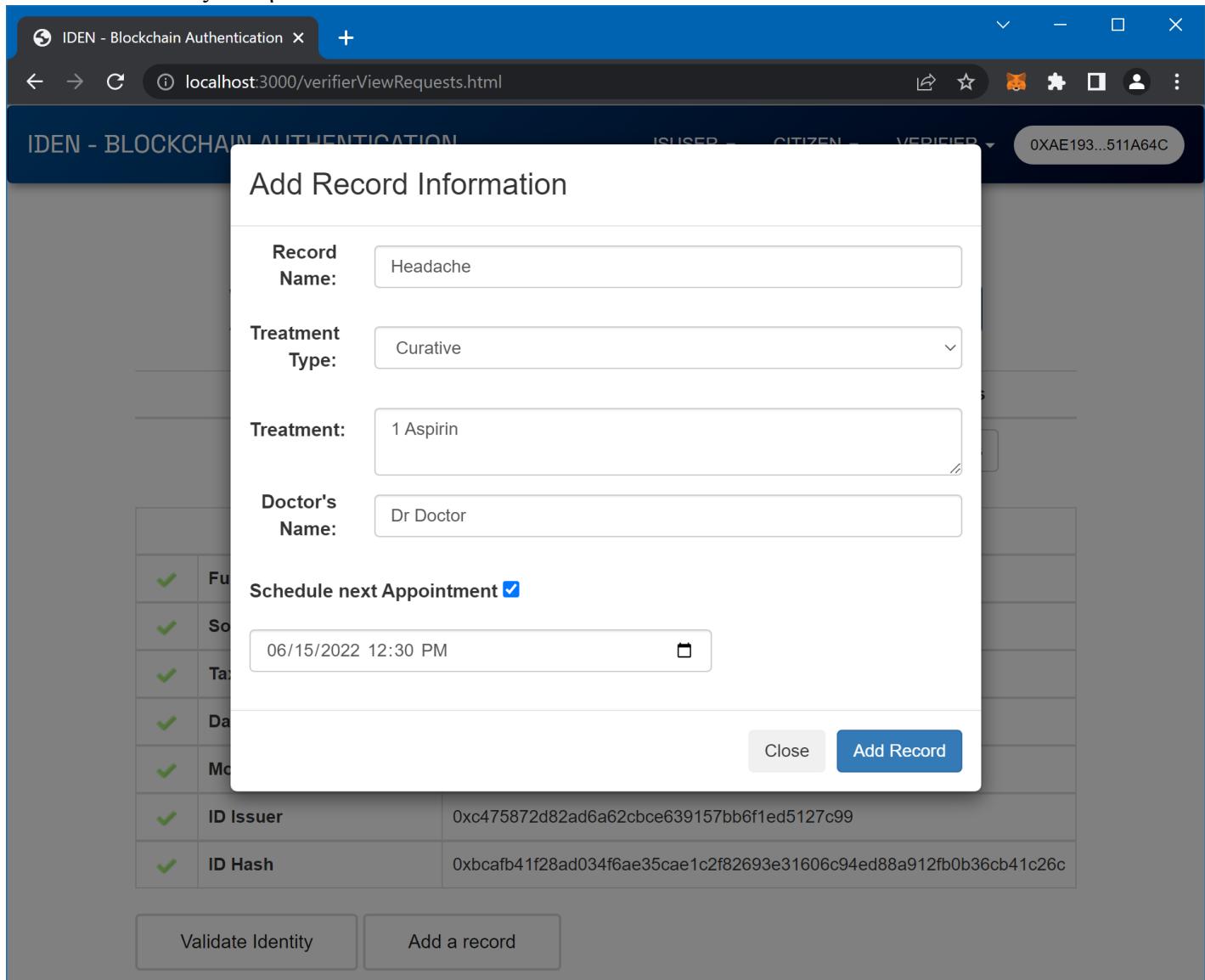
Εικόνα 80 - Λεπτομέρειες ενός αποδεκτού αιτήματος κοινοποίησης στοιχείων ταυτότητας

Στη παραπάνω εικόνα, γίνεται εύκολα αντιληπτό πως το κουμπί «Add a record» είναι απενεργοποιημένο. Αυτό συμβαίνει, διότι δεν είναι δυνατόν να πραγματοποιηθεί οποιαδήποτε ενέργεια αν το νοσοκομείο δεν επαληθεύσει την εγκυρότητα των στοιχείων. Η επαλήθευση των στοιχείων γίνεται με το κουμπί «Validate Identity» και το αποτέλεσμα της εμφανίζεται ως μήνυμα στο επάνω μέρος της σελίδας (Εικόνα 81).



Εικόνα 81 - Μήνυμα επιτυχούς επικύρωσης στοιχείων ταυτότητας πολίτη

Στη συνέχεια, ο χρήστης του λογαριασμού του νοσοκομείου δύναται να προσθέσει/δημιουργήσει ένα νέο ιατρικό ιστορικό μέσω του κουμπιού «Add a record». Κάνοντας «κλικ» σε αυτό το κουμπί αναδύεται ένα παράθυρο, που περιέχει μια φόρμα εισαγωγής όλων των απαραίτητων στοιχείων (Εικόνα 82). Μέσα από αυτή τη φόρμα, ο χρήστης μπορεί να ονομάσει την εγγραφή, να επιλέξει τον τύπο της θεραπείας μέσα από μια λίστα θεραπειών, να πληκτρολογήσει την συνταγή και το όνομα του επιβλέποντα γιατρού, όπως επίσης και να καταχωρίσει μια νέα συνάντηση για επανεξέταση.



The screenshot shows the 'Add Record Information' dialog box. It includes fields for Record Name (Headache), Treatment Type (Curative), Treatment (1 Aspirin), Doctor's Name (Dr Doctor), and a checkbox for scheduling the next appointment with a date and time set to 06/15/2022 12:30 PM. At the bottom right are 'Close' and 'Add Record' buttons.

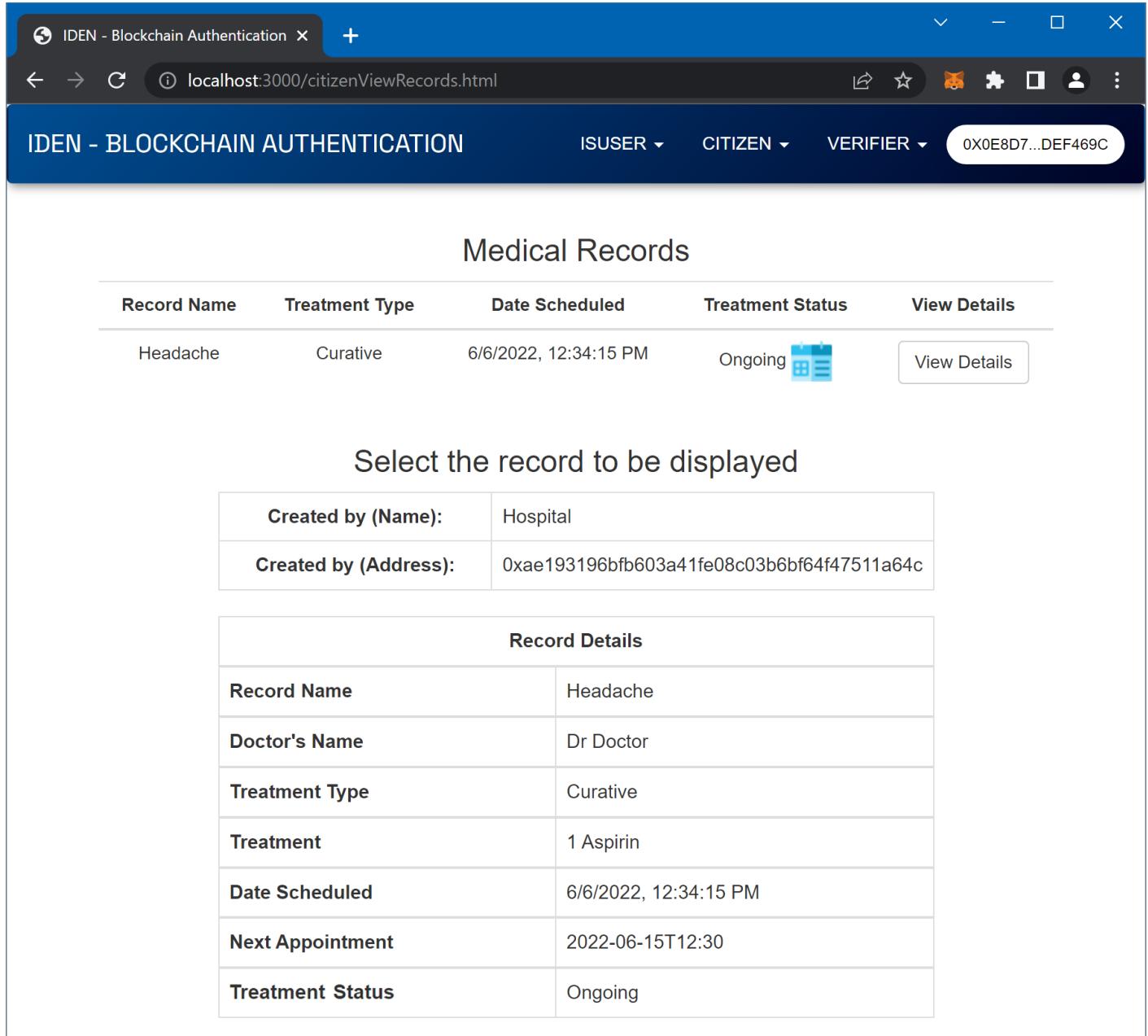
	ID Issuer	ID Hash
✓	0xc475872d82ad6a62cbce639157bb6f1ed5127c99	0xbcaf841f28ad034f6ae35cae1c2f82693e31606c94ed88a912fb0b36cb41c26c

Validate Identity **Add a record**

Εικόνα 82 – Προσθήκη/Δημιουργία ιατρικού ιστορικού

Ολοκληρώνοντας, το νέο ιατρικό ιστορικό είναι ορατό μέσα από τη σελίδα «View Medical Records» του μενού του πολίτη (Εικόνα 83), αλλά και από την αντίστοιχη σελίδα στο μενού του επαληθευτή – νοσοκομείου, κατόπιν αναζήτησης της επιθυμητής διεύθυνσης πολίτη (Εικόνα 84). Η σελίδα ιατρικού ιστορικού που είναι

ορατή στο νοσοκομείο διαθέτει δύο επιπλέον επιλογές, την ενημέρωση του ιστορικού (Update Record) και την ολοκλήρωση της θεραπείας.



The screenshot shows a web browser window titled "IDEN - Blockchain Authentication". The URL is "localhost:3000/citizenViewRecords.html". The page header includes "IDEN - BLOCKCHAIN AUTHENTICATION", "ISUSER", "CITIZEN", "VERIFIER", and a user ID "0X0E8D7...DEF469C". Below the header, a section titled "Medical Records" displays a table with one row:

Record Name	Treatment Type	Date Scheduled	Treatment Status	View Details
Headache	Curative	6/6/2022, 12:34:15 PM	Ongoing 	View Details

Below the table, a message says "Select the record to be displayed" and shows two dropdown menus:

Created by (Name):	Hospital
Created by (Address):	0xae193196bfb603a41fe08c03b6bf64f47511a64c

Finally, a "Record Details" table is shown with the following data:

Record Details	
Record Name	Headache
Doctor's Name	Dr Doctor
Treatment Type	Curative
Treatment	1 Aspirin
Date Scheduled	6/6/2022, 12:34:15 PM
Next Appointment	2022-06-15T12:30
Treatment Status	Ongoing

Εικόνα 83 - Σελίδα ιατρικού ιστορικού από τον λογαριασμό του πολίτη

IDEN - Blockchain Authentication x +

localhost:3000/verifierViewRecords.html

IDEN - BLOCKCHAIN AUTHENTICATION ISUSER CITIZEN VERIFIER 0XAE193...511A64C

Search Medical Records by Wallet Address

Wallet Address: 0x0E8D7d85eb1B78dB803334901508A6f24DEF469C

Record Name	Treatment Type	Date Scheduled	Treatment Status	View Details
Headache	Curative	6/6/2022, 12:34:15 PM	Ongoing 	<button>View Details</button>

Record Details	
Record Name	Headache
Doctor's Name	Dr Doctor
Treatment Type	Curative
Treatment	1 Aspirin
Date Scheduled	6/6/2022, 12:34:15 PM
Next Appointment	2022-06-15T12:30
Treatment Status	Ongoing

Update Record End Treatment

Εικόνα 84 - Σελίδα ιατρικού ιστορικού από τον λογαριασμό του επαληθευτή - νοσοκομείου

Αξίζει να σημειωθεί πως τα «έξυπνα» συμβόλαια της εφαρμογής, εκτός από το τοπικό Blockchain του «Ganache», είναι διαθέσιμα και στα δημόσια δοκιμαστικά δίκτυα Blockchain «Ropsten» και «Rinkeby». Πράγμα που σημαίνει πως οι συναλλαγές και εν γένει η παραπάνω περίπτωση χρήσης, μπορούν να πραγματοποιηθούν από οποιοδήποτε σύστημα έχει πρόσβαση στην εφαρμογή, χωρίς την ύπαρξη, τοπικά, των «έξυπνων» συμβολαίων, με την προϋπόθεση πως υπάρχει διαθέσιμο υπόλοιπο σε ETH σε ένα από τα δύο δίκτυα.

4.7. Διαδικασία δοκιμών (Testing)

Ως διαδικασία δοκιμών ορίζεται η διαδικασία αξιολόγησης και επαλήθευσης πως ένα προϊόν λογισμικού ή μια εφαρμογή κάνει αυτό που υποτίθεται ότι πρέπει να κάνει. Τα οφέλη των δοκιμών περιλαμβάνουν την πρόληψη σφαλμάτων, τη μείωση του κόστους ανάπτυξης και τη βελτίωση της απόδοσης (IBM, 2019b).

Παρακάτω παρουσιάζονται οι δοκιμές στις οποίες υποβλήθηκε η εφαρμογή. Ονομαστικά, αυτές είναι οι εξής: Δοκιμές Μονάδας (Unit Testing), Δοκιμές Απόδοσης (Performance Testing), Δοκιμές Γραφικού Περιβάλλοντος (GUI Testing), Δοκιμές μεταξύ Περιηγητών Ιστού (Cross-Browser Testing), Δοκιμές «Παλινδρόμησης» (Regression Testing) και Δοκιμές Λογικής (Sanity Testing).

1. Unit Testing

Το «Unit Testing» είναι ένας τύπος δοκιμής λογισμικού όπου ελέγχονται μεμονωμένες μονάδες ή στοιχεία του. Σκοπός του είναι να επικυρωθεί ότι κάθε μονάδα του κώδικα λογισμικού αποδίδει όπως αναμένεται (Hamilton, 2019a). Στο παρόν έργο, ο κώδικας των δοκιμών είναι «γραμμένος» σε γλώσσα προγραμματισμού «Javascript», και γίνεται χρήση του module «chai» του «Node.js». Το σύνολο των αρχείων δοκιμών βρίσκεται εντός του φακέλου «test» του έργου και είναι της μορφής «(όνομα).test.js». Στο παρακάτω παράδειγμα κώδικα «Unit Testing» (Εικόνα 85), δημιουργείται ένα αντίγραφο του αναπτυχθέντος, στο Blockchain, «έξυπνου» συμβολαίου και στη συνέχεια, πραγματοποιείται έλεγχος για την ύπαρξη πολίτη με τη συγκεκριμένη διεύθυνση «πορτοφολιού».

```
JS Issuer.test.js > ...
1  const { assert } = require("chai");
2
3  const Issuer = artifacts.require('./Issuer.sol');
4
5  contract('Issuer', (accounts) => {
6    before(async () => {
7      this.Issuer = await Issuer.deployed()
8    })
9
10   it('Should check if a Citizen exists', async () => {
11     const citizenExists = await this.Issuer.checkExists('0xFABeceBf00E1EA7A835d01f86412A3fA472E4268');
12     assert.equal(citizenExists, true);
13   });
14 })
```

Εικόνα 85 - Παράδειγμα κώδικα «Unit Testing» του αρχείου «Issuer.test.js»

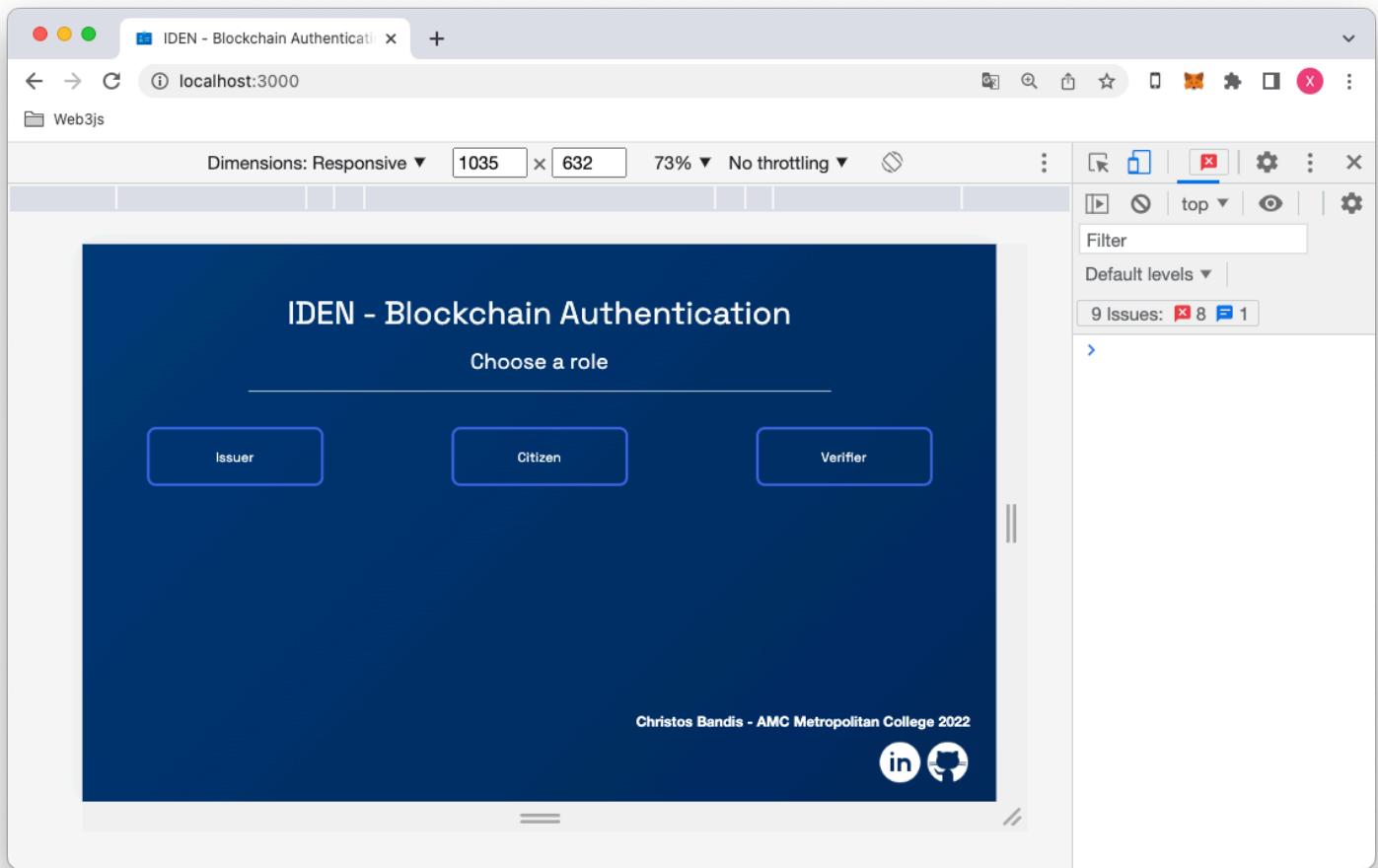
2. Performance Testing

Το «Performance Testing» είναι ένα μέτρο δοκιμής που αξιολογεί την ταχύτητα, την απόκριση και τη σταθερότητα ενός υπολογιστή, δικτύου, λογισμικού ή συσκευής κάτω από ευμεγέθη φόρτο εργασίας (Gillis, n.d.). Λόγω της άμεσης εξάρτησης της εφαρμογής από το Ethereum Blockchain και όχι από μία κεντρική βάση δεδομένων, δε μπορεί να πραγματοποιηθεί δοκιμή της ταχύτητας και της σταθερότητάς της υπό αντίξοες συνθήκες. Προσεγγίζοντας θεωρητικά το θέμα, όσο το Ethereum Blockchain βρίσκεται σε λειτουργία και υποστηρίζεται από τους κόμβους του, τόσο αποκρίσιμη και προσβάσιμη θα είναι η εφαρμογή, ανεξαρτήτως το πλήθος των ταυτόχρονων χρηστών.

3. Graphical User Interface (GUI) Testing

Το «Graphical User Interface Testing» είναι ένας τύπος δοκιμής λογισμικού που ελέγχει το γραφικό περιβάλλον εργασίας χρήστη. Σκοπός των δοκιμών αυτών είναι να διασφαλιστεί ότι οι λειτουργίες της εφαρμογής εκτελούνται σύμφωνα με τις προδιαγραφές, ελέγχοντας οθόνες και στοιχεία όπως μενού, κουμπιά, εικονίδια κ.λπ. (Hamilton, 2019a).

Για τον έλεγχο του γραφικού περιβάλλοντος της εφαρμογής, έγινε χρήση των «Εργαλείων για προγραμματιστές» του περιηγητή «Google Chrome» και πιο συγκεκριμένα της επιλογής «Γραμμή εργαλείων συσκευής» (Device Toolbar) (Εικόνα 86). Έτσι, κατέστη δυνατή η δοκιμή της εμφάνισης και της σωστής λειτουργίας όλων των γραφικών στοιχείων της εφαρμογής σε πληθώρα αναλύσεων (οθόνης) και συσκευών.



Εικόνα 86 - Γραμμή εργαλείων συσκευής (Εργαλεία για προγραμματιστές - Google Chrome)

4. Cross-Browser Testing

Το «Cross Browser Testing» είναι ένας τύπος δοκιμής για την παρακολούθηση της λειτουργίας της εφαρμογής σε διαφορετικά προγράμματα περιήγησης (Rungta, 2020). Για τη δοκιμή έγινε χρήση των μοντέρνων περιηγητών: «Google Chrome», «Mozilla Firefox», «Brave», «Microsoft Edge» και «Safari». Το αποτέλεσμα της δοκιμής ήταν πως σε όλους τους περιηγητές η εφαρμογή έχει την ίδια συμπεριφορά και εμφάνιση (πεδία φορμών, κουμπιά, γραμματοσειρές), με τη μόνη διαφορά της εμφάνισης του ημερολογίου στα πεδία εισαγωγής ημερομηνίας και αυτό εξαιτίας της ιδιαιτερότητας του, να είναι δημιουργημένο εξ ολοκλήρου από κώδικα «HTML», χωρίς κάποια πρόσθετη παραμετροποίηση. Πιο συγκεκριμένα, η εμφάνιση του παρουσιάζεται πανομοιότυπη στους περιηγητές που βασίζονται στην «ανοιχτού» κώδικα «μηχανή» «Chromium» (Chrome, Brave, Edge) και διαφορετική στο «Firefox» και στο «Safari». Επίσης, στους περιηγητές για τους οποίους δεν έχει αναπτυχθεί

κάποιο «πορτοφόλι» σε μορφή επέκτασης (π.χ. Safari), οι λειτουργίες της εφαρμογής δεν εκτελούνται, μετατρέποντας την σε έναν απλό ιστότοπο.

5. Regression Testing

Το «Regression Testing» ορίζεται ως ένας τύπος δοκιμής λογισμικού με σκοπό την επιβεβαίωση πως μια πρόσφατη αλλαγή στον κώδικα της εφαρμογής δεν έχει επηρεάσει αρνητικά τις υπάρχουσες λειτουργίες (IBM, 2019b). Καθ' όλη τη διάρκεια ανάπτυξης της εφαρμογής πραγματοποιήθηκαν δοκιμές «παλινδρόμησης», καθώς σε οποιαδήποτε κρίσιμη τροποποίηση στον κώδικα ήταν απαραίτητος ο έλεγχος για την ύπαρξη οποιουδήποτε σφάλματος. Επιπλέον, οι δοκιμές αυτές ωφέλησαν στην επιδιόρθωση ελαττωμάτων και ζητημάτων απόδοσης.

6. Sanity Testing

Το «Sanity Testing» είναι ένα υποσύνολο δοκιμών παλινδρόμησης. Μόλις αναπτυχθεί (build) μια έκδοση του λογισμικού, εκτελούνται δοκιμές λογικής για να διασφαλιστεί ότι οι αλλαγές που εισάγονται στο σύνολο του κώδικα λειτουργούν όπως αναμένεται. Αυτή η δοκιμή είναι ένα σημείο ελέγχου για τον προσδιορισμό της συνέχειας των δοκιμών για την τρέχουσα έκδοση. Στην ανάπτυξη του έργου, οι δοκιμές λογικής εφαρμόστηκαν πριν από κάθε διενέργεια ενός «Regression Testing», αποσκοπώντας στην εξοικονόμηση χρόνου από περιττές δοκιμές.

7. Λοιπές παρατηρήσεις

Με την περίπτωση χρήσης που παρουσιάστηκε στο Κεφάλαιο 4.6, γίνεται αντιληπτό πως μια διεύθυνση χρήστη μπορεί χρησιμοποιηθεί και στην περίπτωση καταχώρισης ταυτότητας νοσοκομείου και το αντίστροφο. Αυτό συμβαίνει, εξαιτίας της ιδιαιτερότητας του «Ganache» να δημιουργεί διαφορετική δεκάδα λογαριασμών σε κάθε εκκίνηση του συνεπώς, δεν ήταν δυνατή η καταχώρηση συγκεκριμένων διευθύνσεων σε λίστα, με σκοπό τον έλεγχο τους (βλ. σελίδα 58).

Αξια αναφοράς είναι, επίσης η διαδικασία έγκρισης των τριών συναλλαγών που δημιουργούνται όταν πραγματοποιείται καταχώριση μιας ταυτότητας. Εξαιτίας της «σύνδεσης» αυτών των συναλλαγών (βλ. σελίδες 90, 91), παρατηρείται πως αν μία εκ των δύο τελευταίων ακυρωθεί, ενώ θα εμφανιστεί το αντίστοιχο μήνυμα σφάλματος, η

συναλλαγή(-ες) που προηγήθηκαν δεν είναι δυνατόν να αναιρεθούν, λόγω της ιδιαιτερότητας του Blockchain να είναι μη αναστρέψιμο.

5. Συμπεράσματα

Στην παρούσα εργασία πραγματοποιήθηκε εκτενής έρευνα γύρω από τη τεχνολογία του Blockchain, την ψηφιακή ταυτοποίηση, καθώς επίσης παρουσιάστηκε η εφαρμογή ταυτοποίησης «IDEN», βασιζόμενη στο Ethereum Blockchain, που κάνει χρήση «έξυπνων» συμβολαίων για την διεκπεραίωση των λειτουργειών της.

Οι μέχρι πρότινος τεχνολογίες ψηφιακής ταυτότητας, παρά τα οφέλη που παρέχουν στην κοινωνία, αποτελούν νούμερο ένα στόχο για κακόβουλους χρήστες και υπηρεσίες κερδοσκοπικού χαρακτήρα, λόγω της ανορθόδοξης διαχείρισης των δεδομένων από τρίτους. Ενώ έχουν οριστεί νομοθεσίες προστασίας των προσωπικών δεδομένων, το γεγονός αυτό ενισχύεται από την άνευ προηγουμένου χρήση του διαδικτύου και των κινητών συσκευών.

Εν γένει, η τεχνολογία του Blockchain θεμελιώνεται από διαφάνεια, ισχυρή κρυπτογράφηση και άμεση προσβασιμότητα· χαρακτηριστικά που, εκτός των άλλων, φέρεται να είναι ζωτικής σημασίας για πληθώρα καθημερινών δραστηριοτήτων, όπως τραπεζικές συναλλαγές, συστήματα ψηφοφορίας, διαχείριση αλυσίδων ανεφοδιασμού και επικύρωση εγγράφων. Βάσει αυτών, οτιδήποτε βρίσκεται σε αναλογική μορφή, όπως μια αξία ενός αγαθού ή τα στοιχεία ταυτότητας ενός ατόμου ή αντικειμένου, πλέον δύναται να καταχωρηθεί και να διατηρηθεί στο διαδίκτυο (Laurence, 2017). Χάρη στη τεχνολογία αυτή είναι εφικτός ο σχεδιασμός ενός αποκεντρωμένου συστήματος ασφαλούς διαχείρισης δεδομένων.

Η ψηφιοποίηση της διαδικασίας ταυτοποίησης φαίνεται πως είναι πια δυνατή μέσω του Blockchain. Τα αποκεντρωμένα συστήματα διαχείρισης ταυτότητας, σε συνδυασμό με τα «έξυπνα» συμβόλαια, προσδίδουν ακεραιότητα και εμπιστοσύνη στις συναλλαγές μεταξύ οντοτήτων. Ο κάτοχος της ταυτότητας είναι ο μόνος με πρόσβαση στα προσωπικά του δεδομένα, αποκαθιστώντας την ασφάλεια που δε του παρείχαν τα «παραδοσιακά» συστήματα διαχείρισης ταυτότητας, ενώ ο «επαληθευτής» που ζητά να ελέγξει ορισμένα από αυτά τα δεδομένα, παύει να ανησυχεί για πιθανώς παραποτημένα στοιχεία ταυτότητας.

Αποτελεί κοινό τόπο πως η τεχνολογία του Blockchain βρίσκεται ακόμη σε αρχικά στάδια ανάπτυξης, περιβαλλόμενη από ελλιπείς νομοθετικές ρυθμίσεις. Όμως, καθώς «ωριμάζει» παρουσιάζονται ολοένα και πιο αποδοτικές και ασφαλείς επιλογές, που «απαντάνε» στα κοινωνικά, πολιτικά και οικονομικά ζητήματα που υφίστανται

ανά τον κόσμο. Σύμφωνα με τον Schwab (2016), «Βρισκόμαστε στα πρόθυρα μιας τεχνολογικής επανάστασης που θα αλλάξει ριζικά τον τρόπο που ζούμε, εργαζόμαστε και συσχετιζόμαστε μεταξύ μας. Στην κλίμακα, το πεδίο εφαρμογής και την πολυπλοκότητά του, ο μετασχηματισμός αυτός δεν θα μοιάζει με τίποτα από αυτά που έχει βιώσει η ανθρωπότητα στο παρελθόν. Δεν γνωρίζουμε ακόμη πώς θα εξελιχθεί, αλλά ένα πράγμα είναι σαφές: η απάντηση σε αυτό πρέπει να είναι εμπεριστατωμένη, με τη συμμετοχή όλων των ενδιαφερόμενων μερών της παγκόσμιας πολιτικής, από τον δημόσιο και τον ιδιωτικό τομέα έως τον ακαδημαϊκό χώρο και την κοινωνία».

5.1. Μελλοντικές ενέργειες

Η αποκεντρωμένη εφαρμογή ταυτοποίησης «IDEN», που αναπτύχθηκε για τις ανάγκες εκπόνησης της παρούσας εργασίας, είναι μία πλήρως λειτουργική προσέγγιση στις απαιτήσεις του θέματος που ανατέθηκε, χωρίς όμως, αυτό να την καθιστά ολοκληρωμένη. Στους μελλοντικούς στόχους ανάπτυξης της περιλαμβάνεται η ένταξη περισσότερων περιπτώσεων χρήσης, όπως η χρήση της εφαρμογής για την επαλήθευση στοιχείων σε κάποιο κρατικό μηχανισμό, σε ιδιωτικούς οργανισμούς κ.α. Ακόμη, εντός των στόχων τάσσεται και η έρευνα για άλλους τύπους Blockchain, όπως είναι τα «Solana», «Cardano» και «Holochain», με σκοπό την ευρύτερη υποστήριξη της εφαρμογής.

6. Παράρτημα

6.1. Βιβλιογραφικές Αναφορές

Λογαράς, Κ. (2018). Η τεχνολογία Blockchain, οι εφαρμογές της και οι νομικές πτυχές της. [online] Available at: <https://www.nafemporiki.gr/story/1363055/i-texnologia-blockchain-oi-efarmoges-tis-kai-oi-nomikes-ptuxes-tis> [Accessed 17 Apr. 2022].

Allende López, M. (2020). *Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain*. Inter-American Development Bank. doi:10.18235/0002635.

AppDividend. (2022). *What is Agile Scrum Master and How Scrum Process Works*. [online] Available at: <https://appdividend.com/2022/01/11/what-is-agile-scrum-master/> [Accessed 30 Apr. 2022].

Bashir, I. (2017). Mastering blockchain : distributed ledger technology, decentralization, and smart contracts explained. Birmingham - Mumbai Packt March.

Bitpanda (n.d.). *What are Smart Contracts and how do they work?* [online] www.bitpanda.com. Available at: <https://www.bitpanda.com/academy/en/lessons/what-are-smart-contracts-and-how-do-they-work/> [Accessed 20 Apr. 2022].

CardBoard. (2020). *How to Prioritize Agile Stories*. [online] Available at: <https://cardboardit.com/2020/08/how-to-prioritize-agile-stories/> [Accessed 30 Apr. 2022].

CB Insights Research. (2018). *What is Blockchain Technology?* [online] Available at: <https://www.cbinsights.com/research/what-is-blockchain-technology/> [Accessed 18 Apr. 2022].

Chamber of Digital Commerce (2016). *Smart Contracts: 12 Use Cases for Business & Beyond A Technology, Legal & Regulatory Introduction — Foreword by Nick Szabo*. Washington, D.C.

Dahan, M. and Hanmer, L. (2015). *The Identification for Development Agenda : Its Potential for Empowering Women and Girls*. [online] Washington, DC: World Bank. Available at: <https://openknowledge.worldbank.org/handle/10986/22795> [Accessed 24 Apr. 2022].

Das, R. (2016). *Adopting Biometric Technology Challenges and Solutions*. CRC Press.

Deol, R. and Wiesner, T. (2021) ‘Ethereum Blockchain Developer Bootcamp With Solidity (2022)’ [Recorded lecture], *Udemy*. Available at:

<https://www.udemy.com/course/blockchain-developer/learn/lecture/17026898#overview> [Accessed: 17 March 2021].

Frankenfield, J. (2021). *Decentralized Applications – dApps*. [online] Investopedia. Available at: <https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp> [Accessed 20 Apr. 2022].

Gauravaram, P., McCullagh, A. and Dawson, E. (2006). The legal and practical implications of recent attacks on 128-bit cryptographic hash function. *First Monday*, 11(1). doi:10.5210/fm.v11i1.1306.

Gillis, A.S. (n.d.). *What is Performance Testing?* [online] Available at: <https://www.techtarget.com/searchsoftwarequality/definition/performance-testing> [Accessed 5 May 2022].

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 5 May 2022].

Hamilton, T. (2019b). *GUI Testing Tutorial: User Interface (UI) TestCases with Examples*. [online] Available at: <https://www.guru99.com/gui-testing.html> [Accessed 5 May 2022].

Hartley, J. (2011). *Communication, Cultural and Media Studies The Key Concepts*. London: Routledge.

Hayes, A. (2022). Blockchain Explained. [online] Investopedia. Available at: <https://www.investopedia.com/terms/b/blockchain.asp> [Accessed 17 Apr. 2022].

IBM (2019b). *What is software testing?* [online] Ibm.com. Available at: <https://www.ibm.com/topics/software-testing> [Accessed 5 May 2022].

IBM (2022). *What are smart contracts on blockchain?* [online] www.ibm.com. Available at: <https://www.ibm.com/topics/smart-contracts> [Accessed 20 Apr. 2022].

IBM (n.d.). *What is blockchain technology? - IBM Blockchain*. [online] www.ibm.com. Available at: <https://www.ibm.com/topics/what-is-blockchain> [Accessed 18 Apr. 2022].

IBM. (2019a). *Cryptographic concepts*. [online] Available at: <https://www.ibm.com/docs/en/ibm-mq/9.0?topic=mechanisms-cryptographic-concepts> [Accessed 26 Apr. 2022].

Iredale, G. (2018). The History of Blockchain Technology: Must Know Timeline. [online] 101 Blockchains. Available at: <https://101blockchains.com/history-of-blockchain-timeline/> [Accessed 17 Apr. 2022].

Jal, A. (2018). Secure The Data In Multi Cloud Using Erasure Code And Merkle Hash Tree Algorithm. *International Journal of Recent Trends in Engineering and Research*, 4(4). doi:10.23883/ijrter.2018.4198.w12zv.

JAXenter. (2019). *No, you don't store data on the blockchain - here's why*. [online] Available at: <https://jaxenter.com/blockchain-data-164727.html> [Accessed 1 May 2022].

Kaley, A. (2021). *Mapping User Stories in Agile*. [online] Nielsen Norman Group. Available at: <https://www.nngroup.com/articles/user-story-mapping/> [Accessed 30 Apr. 2022].

Laurence, T. (2017). *Blockchain for dummies*. Hoboken, Nj: John Wiley & Sons.

Lyons, T., Courcelas, L. and Timsit, K. (2016). *The European Union Blockchain Observatory and Forum*. [online] European Union. Available at: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf [Accessed 26 Apr. 2022].

Manby, B. (2016). *Identification in the Context of Forced Displacement : Identification for Development*. [online] Washington, DC: World Bank. Available at: <https://openknowledge.worldbank.org/handle/10986/24941> [Accessed 24 Apr. 2022].

Marx, S. (2018). *Understanding Ethereum Smart Contract Storage*. [online] Available at: <https://programtheblockchain.com/posts/2018/03/09/understanding-ethereum-smart-contract-storage/> [Accessed 20 Apr. 2022].

McKinsey (2019). *Infographic: What is good digital ID?* | McKinsey. [online] Available at: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/infographic-what-is-good-digital-id> [Accessed 24 Apr. 2022].

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 30 Apr. 2022].

Okta. (n.d.). *Hashing Algorithm Overview: Types, Methodologies & Usage* | Okta. [online] Available at: <https://www.okta.com/identity-101/hashing-algorithms/> [Accessed 26 Apr. 2022].

Pandit, H.J., O' Sullivan, D. and Lewis, D. (2018). Queryable Provenance Metadata For GDPR Compliance. In: *Procedia Computer Science*. SEMANTiCS 2018 – 14th International Conference on Semantic Systems.

Pato, J. and Rouault, J. (2003). *Identity management: The drive to federation*. Technical White Papers.

Ray, S. (2021). *What is a DAPP?* [online] Medium. Available at: <https://towardsdatascience.com/what-is-a-dapp-a455ac5f7def> [Accessed 20 Apr. 2022].

- Rungta, K. (2020). *Cross Browser Testing using Selenium WebDriver*. [online] www.guru99.com. Available at: <https://www.guru99.com/cross-browser-testing-using-selenium.html> [Accessed 5 May 2022].
- Schwab, K. (2016). *The Fourth Industrial Revolution: what it means, how to respond*. [online] World Economic Forum. Available at: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> [Accessed 6 May 2022].
- Scrum.org (2016). *What is Scrum?* [online] Scrum.org. Available at: <https://www.scrum.org/resources/what-is-scrum> [Accessed 30 Apr. 2022].
- Shackelford, S. and Myers, S. (2016). Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace. *SSRN Electronic Journal*. doi:10.2139/ssrn.2874090.
- The Public Voice, (n.d.). *Privacy: Background – thepublicvoice.org*. [online] Available at: https://thepublicvoice.org/issues_and_resources/privacy-background/ [Accessed 26 Apr. 2022].
- The World Bank Group, GSMA and Secure Identity Alliance (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. [online] Washington, DC: World Bank. Available at: <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf> [Accessed 28 Apr. 2022].
- Treiblmaier, H. (2019). Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies. *Frontiers in Blockchain*, 2. doi:10.3389/fbloc.2019.00003.
- Vishnia, G.R. and Peters, G.W. (2020). AuditChain: A Trading Audit Platform Over Blockchain. *Frontiers in Blockchain*, 3. doi:10.3389/fbloc.2020.00009.
- Wikipedia (2020). *Zooko's triangle*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Zooko%27s_triangle [Accessed 26 Apr. 2022].
- World Bank (2018a). *Catalog of Technical Standards for Digital Identification Systems (English)*. Washington, D.C. : World Bank.
- World Bank (2018b). *Technology Landscape for Digital Identification*. [online] Washington, DC: World Bank. Available at: <https://openknowledge.worldbank.org/handle/10986/31825> [Accessed 25 Apr. 2022].
- 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 30 Apr. 2022].

6.2. Κατάλογος Εικόνων

Εικόνα 1 - Χρονοδιάγραμμα Gantt.....	- 4 -
Εικόνα 2 - Αναπαράσταση ενός δικτύου Blockchain (CB Insights Research, 2018)	- 8 -
Εικόνα 3 - Παράδειγμα σύνδεσης μεταξύ των «block»	- 10 -
Εικόνα 4 - Σύγκριση μεταξύ συγκεντρωτικής (centralized) βάσης δεδομένων και Blockchain	- 12 -
Εικόνα 5 - Γραφική αναπαράσταση και σύγκριση μιας κεντρικής (centralized) και μιας αποκεντρωμένης (decentralized) εφαρμογής (Ray, 2021).....	- 15 -
Εικόνα 6 - Γραφική αναπαράσταση περίπτωσης χρήσης ενός «έξυπνου» συμβολαίου (Bitpanda, n.d.)	- 17 -
Εικόνα 7 - Παραδείγματα ψηφιακής ταυτότητας σε τρεις διαφορετικές περιπτώσεις (Allende López, 2020)	- 18 -
Εικόνα 8 - Μέθοδοι ταυτοποίησης μέσω κινητού τηλεφώνου (World Bank, 2018b)..	- 21 -
Εικόνα 9 - Το τρίγωνο Zooko (Wikipedia, 2020).....	- 23 -
Εικόνα 10 - Τρόπος λειτουργίας του αλγόριθμου κατακερματισμού (Okta, n.d.)	- 25 -
Εικόνα 11 - Γράφημα από την έκθεση του οργανισμού «Identity Theft Resource Center» για τις παραβιάσεις δεδομένων τη χρονιά 2021	- 27 -
Εικόνα 12 - Τρόπος λειτουργίας ενός συστήματος ταυτοποίησης μέσω Blockchain ..	- 28 -
Εικόνα 13 - Η αρχική σελίδα της εφαρμογής «IDEN»	- 29 -
Εικόνα 14 - Διάγραμμα Κλάσης (Class Diagram).....	- 33 -
Εικόνα 15 - Διάγραμμα Αντικειμένου / Περίπτωσης (Object / Instance Diagram)	- 34 -
Εικόνα 16 - Διάγραμμα Ροής «Εκδότη» (Issuer Flowchart)	- 35 -
Εικόνα 17 - Διάγραμμα Ροής «Πολίτη» (Citizen Flowchart).....	- 36 -
Εικόνα 18 - Διάγραμμα Ροής «Επαληθευτή» (Verifier Flowchart)	- 37 -
Εικόνα 19 - Διάγραμμα Δραστηριότητας «Επαληθευτή» (Verifier Activity Diagram)-	37 -
Εικόνα 20 - Διάγραμμα Ακολουθίας «Εκδότη» (Issuer Sequence Diagram).....	- 38 -
Εικόνα 21 - Προσχέδιο σελίδας στοιχείων ταυτότητας "Πολίτη" (Citizen ID Page Mockup)	- 39 -
Εικόνα 22 - Προσχέδιο σελίδας αίτησης στοιχείων ταυτότητας (ID Request Page Mockup).....	- 39 -
Εικόνα 23 - Προσχέδιο σελίδας διαχείρισης αιτημάτων ταυτότητας από τον "Επαληθευτή" (Verifier ID Request Management Page Mockup)	- 40 -
Εικόνα 24 - Προσχέδιο παραθύρου καταχώρησης ιατρικού ιστορικού (Create medical record Window Mockup).....	- 40 -

Εικόνα 25 – «Μακέτα» των περιπτώσεων χρήσης του «Πολίτη» σε κινητή συσκευή (Citizen Mobile Wireframe)	- 41 -
Εικόνα 26 - Εργαλείο διαχείρισης Scrum (Scrum Process Canvas).....	- 42 -
Εικόνα 27 - Διάγραμμα περίπτωσης χρήσης (Use Case Diagram)	- 46 -
Εικόνα 28 - User Story Map	- 50 -
Εικόνα 29 - Υπόδειγμα έναρξης κώδικα σε γλώσσα «Solidity»	- 57 -
Εικόνα 30 - Το αποθετήριο (repository) του «Ganache» στο «Github»	- 60 -
Εικόνα 31 - Ολοκλήρωση εγκατάστασης του «Ganache»	- 61 -
Εικόνα 32 - Αρχική οθόνη του «Ganache»	- 61 -
Εικόνα 33 - Παράθυρο διαχείρισης του Blockchain	- 62 -
Εικόνα 34 - Παράθυρο τροποποίησης του περιβάλλοντος εργασίας	- 63 -
Εικόνα 35 - Παράθυρο τροποποίησης του διακομιστή	- 63 -
Εικόνα 36 - Επίσημος ιστότοπος του «Metamask».....	- 64 -
Εικόνα 37 - Ηλεκτρονικό κατάστημα του «Google Chrome»	- 65 -
Εικόνα 38 - Μήνυμα έγκρισης προσθήκης της επέκτασης στο «Google Chrome»	- 65 -
Εικόνα 39 - Αρχική σελίδα του «Metamask».....	- 66 -
Εικόνα 40 - Επιλογές εισαγωγής ή δημιουργίας «πορτοφολιού».....	- 66 -
Εικόνα 41 - Εισαγωγή ήδη υπάρχοντος «πορτοφολιού».....	- 67 -
Εικόνα 42 - Περιβάλλον διαχείρισης «πορτοφολιού» του «Metamask».....	- 68 -
Εικόνα 43 - Διακόπτης ενεργοποίησης δοκιμαστικών δικτύων	- 69 -
Εικόνα 44 - Τα προκαθορισμένα δοκιμαστικά δίκτυα που περιλαμβάνει το «Metamask» -	
69 -	
Εικόνα 45 – Ιστότοπος λήψης του «Node.js».....	- 70 -
Εικόνα 46 - Απαραίτητη επιλογή κατά την εγκατάσταση του «Node.js»	- 71 -
Εικόνα 47 - Πρώτο παράθυρο «CMD» εγκατάστασης πρόσθετων εργαλείων του «Node.js»	- 72 -
Εικόνα 48 - Δεύτερο παράθυρο «CMD» εγκατάστασης πρόσθετων εργαλείων του Node.js	- 72 -
Εικόνα 49 - Έναρξη εγκατάστασης των πρόσθετων εργαλείων στο «Windows PowerShell»	- 73 -
Εικόνα 50 - Ολοκλήρωση της εγκατάστασης των πρόσθετων εργαλείων του «Node.js» ..	
74 -	
Εικόνα 51 - Ο φάκελος «Prototype (rebuild)».....	- 75 -
Εικόνα 52 - Εκτέλεση της εντολής «npm rebuild».....	- 76 -
Εικόνα 53 - Αποτελέσματα της εντολής «npm rebuild»	- 76 -

Εικόνα 54 - Εκτέλεση της εντολής «npm install»	- 77 -
Εικόνα 55 - Αποτελέσματα της εντολής «npm install»	- 77 -
Εικόνα 56 - Μενού διαχείρισης λογαριασμού «πορτοφολιού» στο «Metamask».....	- 78 -
Εικόνα 57 - Σελίδα εισαγωγής λογαριασμού μέσω «ιδιωτικού κλειδιού»	- 79 -
Εικόνα 58 - Παράθυρο πληροφοριών λογαριασμού στο «Ganache».....	- 80 -
Εικόνα 59 - Μενού διαχείρισης λογαριασμού «πορτοφολιού» στο «Metamask» με τους τρεις λογαριασμούς συνδεμένους	- 81 -
Εικόνα 60 - Εκτέλεση της εντολής «node_modules/.bin/truffle migrate --reset»	- 81 -
Εικόνα 61 - Σφάλμα κατά την εκτέλεση της εντολής «node_modules/.bin/truffle migrate --reset».....	- 82 -
Εικόνα 62 - Εκτέλεση της εντολής «Set-ExecutionPolicy RemoteSigned».....	- 82 -
Εικόνα 63 - Συνέχεια της εκτέλεσης της εντολής «Set-ExecutionPolicy RemoteSigned» .	-
Εικόνα 64 - Επανεκτέλεση της εντολής «node_modules/.bin/truffle migrate --reset»	- 83 -
Εικόνα 65 - Η διαδικασία μεταγλώττισης του κώδικα των «έξυπνων» συμβολαίων σε «bytecode»	- 84 -
Εικόνα 66 - Ολοκλήρωση της διαδικασίας μεταγλώττισης και παρουσίαση πληροφοριών για κάθε «έξυπνο» συμβόλαιο	- 85 -
Εικόνα 67 - Εκτέλεση της εντολής «npm run dev»	- 86 -
Εικόνα 68 - Παράδειγμα λειτουργίας του module lite-server	- 86 -
Εικόνα 69 - Επιβεβαίωση πως ο ενεργός λογαριασμός είναι ο «Account 1»	- 88 -
Εικόνα 70 - Παράθυρο του «Metamask» για τη σύνδεση λογαριασμού στην εφαρμογή ...	-
Εικόνα 71 - Φόρμα καταχώρισης ταυτότητας πολίτη	- 89 -
Εικόνα 72 - Παράθυρα έγκρισης συναλλαγής κατά την καταχώριση ταυτότητας στο Blockchain	- 90 -
Εικόνα 73 - Φόρμα καταχώρισης ταυτότητας νοσοκομείου	- 91 -
Εικόνα 74 - Σύνδεση του δεύτερου λογαριασμού (πολίτη) στην εφαρμογή	- 92 -
Εικόνα 75 - Σελίδα με τις πληροφορίες ταυτότητας του πολίτη	- 93 -
Εικόνα 76 - Σελίδα αίτησης κοινοποίησης στοιχείων ταυτότητας πολίτη	- 94 -
Εικόνα 77 - Ενημέρωση του πολίτη για το αναπάντητο αίτημα μέσω του εικονιδίου ειδοποίησης.....	- 95 -
Εικόνα 78 - Σελίδα των αιτημάτων του πολίτη	- 96 -
Εικόνα 79 - Επιλογή των στοιχείων ταυτότητας προς κοινοποίηση από τον πολίτη ...	- 97 -

Εικόνα 80 - Λεπτομέρειες ενός αποδεκτού αιτήματος κοινοποίησης στοιχείων ταυτότητας	- 98 -
Εικόνα 81 - Μήνυμα επιτυχούς επικύρωσης στοιχείων ταυτότητας πολίτη	- 98 -
Εικόνα 82 – Προσθήκη/Δημιουργία ιατρικού ιστορικού	- 99 -
Εικόνα 83 - Σελίδα ιατρικού ιστορικού από τον λογαριασμό του πολίτη.....	- 100 -
Εικόνα 84 - Σελίδα ιατρικού ιστορικού από τον λογαριασμό του επαληθευτή - νοσοκομείου.....	- 101 -
Εικόνα 85 - Παράδειγμα κώδικα «Unit Testing» του αρχείου «Issuer.test.js»	- 102 -
Εικόνα 86 - Γραμμή εργαλείων συσκευής (Εργαλεία για προγραμματιστές - Google Chrome)	- 104 -

6.3. Κατάλογος Πινάκων

Πίνακας 1 - Αναφορά ιδιοκτήτη έργου	- 43 -
Πίνακας 2 - Αναφορά "αρχηγού" του Scrum	- 43 -
Πίνακας 3 - Αναφορά ομάδας Scrum	- 44 -
Πίνακας 4 - Ιεράρχηση περιπτώσεων χρήστης (Use Case Prioritization).	- 48 -
Πίνακας 5 - Αναφορά των «Epics»	- 49 -
Πίνακας 6 - Ιεράρχηση ιστοριών χρήστη (User Stories Prioritization).....	- 54 -
Πίνακας 7 - Παραδοτέα έργου (Project Deliverables).....	- 55 -
Πίνακας 8 - Κυκλοφορίες - Εκδόσεις έργου (Project Releases).....	- 55 -

6.4. Γλωσσάριο απόδοσης ξενόγλωσσων όρων

Agile: Μεθοδολογία ανάπτυξης

Authentication, Authorization and Accounting Framework: Δομή που απευθύνεται στον έλεγχο ταυτότητας, την εξουσιοδότηση και την λογιστική

Authenticator Mobile App: Εφαρμογή Ταυτοποίησης

Blockchain: Αλυσίδα μπλοκ

Byte: Μονάδα μέτρησης ποσότητας πληροφορίας

Bytecode: Τύπος δυαδικού κώδικα

Centralized: Κεντρικός/Συγκεντρωτικός

Ciphertext: Κρυπτοείμενο

Citizen: Πολίτης

Client - Server Model: Μοντέλο Πελάτη – Εξυπηρετητή

Compiler: «Μεταγλωττιστής»

Consensus Mechanism: Μηχανισμός Συναίνεσης

Credential Technologies: Τεχνολογίες Πιστοποίησης

Cryptocurrencies: Κρυπτονομίσματα

Decentralized Applications: Αποκεντρωμένες Εφαρμογές

Decentralized Autonomous Organizations – DAOs: Αποκεντρωμένοι Αυτόνομοι Οργανισμοί

Decoding: Αποκωδικοποίηση

Distributed Ledgers: Κατανεμημένα Καθολικό

ECMAScript: Πρότυπο «Javascript» για τη διασφάλιση της διαλειτουργικότητας ιστοσελίδων

Encoding: Κωδικοποίηση

ETH: Το νόμισμα του Ethereum Blockchain

Ethereum Virtual Machine – EVM: Εικονική Μηχανή Ethereum

Ethereum: Πρωτόκολλο Blockchain

Gas: Το «καύσιμο» του Ethereum Blockchain

General Data Protection Regulation – GDPR: Γενικός Κανονισμός για την Προστασία των Δεδομένων

Gwei: Μικρότερη μονάδα μέτρησης του Ethereum (ETH)

Hash pointers: Δείκτες κατακερματισμού

Hash: Κρυπτογραφική Μαθηματική Παράσταση

HyperText Markup Language – HTML: Γλώσσα σήμανσης ιστοσελίδων

Identity Card: Κάρτα Ταυτότητας

Issuer: Εκδότης

JavaScript Object Notation – JSON: Αρχείο σε μορφή κειμένου για μετάδοση δεδομένων

Javascript: Γλώσσα προγραμματισμού

Merkle Tree: Δέντρο κατακερματισμού

Message Digest: Σύνοψη Μηνύματος

Meta-data: Μεταδεδομένα

Miner: «Μεταλλωρύχος»

Mining: Εξόρυξη

Mnemonic: Μνημονικός κανόνας

Mockup: Προσχέδιο εφαρμογής

Namespace: Χώρος ονομάτων

Native Token: Εγγενές Διακριτικό

Node: Κόμβος

Node.js: Περιβάλλον εκτέλεσης κώδικα «Javascript»

One Time Password – OTP: Κωδικός Μιας Χρήσης

One-way hash function: Μονόδρομη κρυπτογραφική συνάρτηση

Peer-to-Peer Network: Ομότιμο Δίκτυο

Plain text: Απλό κείμενο

Private key: Ιδιωτικό κλειδί

Public Key Infrastructure – PKI: Δομή Δημοσίου Κλειδιού

Quick Response Code – QR Code: Κωδικός γρήγορης ανταπόκρισης

Radio Frequency Identification – RFID: Ταυτοποίηση Μέσω Ραδιοσυγχονούμενων

REST API: Μέθοδος επικοινωνίας μεταξύ συστημάτων

Smart Contracts: «Εξυπνα» συμβόλαια

Solidity: Γλώσσα προγραμματισμού «έξυπνων» συμβολαίων

Timestamping: Χρονοσήμανση

Turing-Complete: Υπολογιστικά πλήρες σύστημα

Unified Modeling Language – UML: Ενοποιημένη Γλώσσα Σχεδίασης Προτύπων

Verifier: Επαληθευτής

Wireframe: «Μακέτα» εφαρμογής

Yellow Paper: Έγγραφο έρευνας που δεν έχει ακόμη δημοσιευτεί ακαδημαϊκά

Assets: Περιουσιακά Στοιχεία