

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



IONIAN  
UNIVERSITY

- Πτυχιακή Εργασία -

Μελέτη Τεχνολογίας Blockchain και Προγραμματισμός  
αποκεντρωμένων εφαρμογών αξιοποιώντας έξυπνα συμβόλαια

Παναγιωτίδης Μιχαήλ Αχιλλέας

Επιβλέπων: Μάγκος Εμμανουήλ

March 31, 2023

## Επιβλέπων

Μάγκος Εμμανουήλ, Καθηγητής,  
*Ιόνιο Πανεπιστήμιο*

## Τριμελής Επιτροπή

Εμμανουήλ Μάγκος, Καθηγητής,  
*Ιόνιο Πανεπιστήμιο*

Νταντογιάν Χριστόφορος, Επίκουρος Καθηγητής,  
*Ιόνιο Πανεπιστήμιο*

Κουρουθανάσης Παναγιώτης, Καθηγητής,  
*Ιόνιο Πανεπιστήμιο*

# Πρόλογος

Στη σύγχρονη κοινωνία η οποία παίρνει όλο και περισσότερο ψηφιακή μορφή, οι οικονομικές συναλλαγές τόσο μεταξύ προσώπων όσο και μεταξύ οργανισμών ή εταιριών διενεργούνται μέσω του διαδικτύου, η ασφάλεια των συναλλαγών αναδεικνύεται σε ζήτημα πρωταρχικής σημασίας. Παραδοσιακά, για την τήρηση της ασφάλειας και της εγκυρότητας των συναλλαγών, είναι υπεύθυνες οι τράπεζες και οι μεγάλοι χρηματοπιστωτικοί οργανισμοί. Αυτό ωστόσο, αφενός έχει ένα σημαντικό κόστος, το οποίο καταβάλλουν οι συναλλασσόμενοι και, αφετέρου, επιτρέπει την πλήρη καταγραφή και τον έλεγχο όλων των συναλλαγών από τους φορείς που μεσολαβούν. Το ίδιο συμβαίνει και με κάθε είδους δεδομένα και τις πληροφορίες που είναι αποθηκευμένες στα ηλεκτρονικά συστήματα, τα οποία χρειάζονται έναν αξιόπιστο μηχανισμό που να εγγυάται την ιδιωτικότητα και την ασφάλειά τους.

Το 2008, ο Satoshi Nakamoto<sup>1</sup> στην προσπάθειά του να απαλλάξει τους συναλλασσόμενους από την εποπτεία του χρηματοοικονομικού συστήματος, παρουσίασε μια επαναστατική για την εποχή ιδέα βασισμένη στην κρυπτογραφία, η οποία εισήγαγε έναν νέο ψηφιακό τρόπο οργάνωσης αρχείων και ταυτόχρονα έναν τρόπο διασφάλισης της εγκυρότητας των συναλλαγών, με την μορφή του πρώτου ψηφιακού νομίσματος, του Bitcoin (Nakamoto, 2008).

Το Bitcoin, χρησιμοποιεί peer-to-peer (P2P) τεχνολογία κάτι που καθιστά τις συναλλαγές με αυτό ταυτόχρονα ελεγχόμενες από όλους τους συμμετέχοντες που βρίσκονται στο συγκεκριμένο δίκτυο. Η παραγωγή και η αξία του εξαρτάται από τους χρήστες του και έτσι η ανάγκη για κάποια κεντρική αρχή ή κυβέρνηση καθίσταται περιττή. Απλούστερα, ο ρόλος του διαμεσολαβητή που έχει η τράπεζα στις συνηθισμένες χρηματικές συναλλαγές, δεν υφίσταται πλέον. Η ιδέα ήταν τόσο ριζοσπαστική και ενδιαφέρουσα, που αποτέλεσε την έμπνευση και την αφετηρία για τη δημιουργία πολλών άλλων ψηφιακών νομισμάτων. Η τεχνολογία πίσω από όλα τα ψηφιακά νομίσματα βασίζεται στην κρυπτογραφία, από την οποία προκύπτει και ο

---

<sup>1</sup>Η ταυτότητα του Satoshi Nakamoto, παραμένει μέχρι και σήμερα άγνωστη. Ενδεχομένως δεν πρόκειται για φυσικό πρόσωπο, αλλά για ομάδα προγραμματιστών υπό αυτό το ψευδώνυμο

όρος κρυπτονομίσματα (cryptocurrency).

Τα κρυπτονομίσματα και η τεχνολογία στην οποία στηρίζονται, το Blockchain, είναι ένα από τα πιο πολλά υποσχόμενα τεχνολογικά εφευρήματα, κάτι που δικαιολογεί τις επενδύσεις δισεκατομμυρίων και την βιομηχανία κρυπτονομισμάτων που έχει δημιουργηθεί γύρω της τα τελευταία χρόνια. Τα οφέλη από την υιοθέτηση αυτής της τεχνολογίας είναι αναρίθμητα χάρη στην φιλοσοφία αλλά και την αρχιτεκτονική της. Το Blockchain είναι μία καινοτόμα τεχνολογία η οποία εξασφαλίζει στους χρήστες της υψηλότερα επίπεδα αυτονομίας και διαφάνειας. Ο ασφαλής και αμετάβλητος χαρακτήρας του, έχει προκαλέσει το ενδιαφέρον του ιδιωτικού τομέα αλλά και των κυβερνητικών αρχών. Οι δυνατότητες και οι χρήσεις της συγκεκριμένης τεχνολογίας είναι πολλές και διευρύνονται πέρα από την αγορά του συναλλαγών, συμπεριλαμβάνοντας ένα τεράστιο φάσμα εφαρμογών και πεδίων της οικονομίας και της κοινωνίας, όπως είναι για παράδειγμα οι κλάδος της ιατρικής, της εκπαίδευσης και της έρευνας, αλλά και τομείς όπως το ηλεκτρονικό εμπόριο, η ασφάλεια των τροφίμων, η διαχείριση της αλυσίδας των προϊόντων, οι ηλεκτρονικές ψηφοφορίες κ.ά.

Όπως είναι φυσικό, η εισαγωγή του blockchain, προκάλεσε μεγάλη διαμάχη μεταξύ των ειδικών του Διαδικτύου, καθώς πέρα από τα προφανή οφέλη τα οποία προσφέρει, ενδεχομένως κρύβει και κινδύνους. Ωστόσο, είναι αδιαμφισβήτητο, ότι πρόκειται για μία τεχνολογία ικανή να επιφέρει πολύ σημαντικές αλλαγές στα δεδομένα του κόσμου των συναλλαγών, αλλά και όπως περιγράφηκε νωρίτερα σε πολλούς άλλου τομείς της καθημερινής μας ψηφιακής πραγματικότητας.

Με την παρούσα πτυχιακή εργασία γίνεται προσπάθεια να αναλυθεί το Ethereum Blockchain και να κατασκευαστεί ένα έξυπνο συμβόλαιο το οποίο να δείχνει σε τεχνικό επίπεδο τον τρόπο λειτουργίας της τεχνολογίας Blockchain. Για το σκοπό αυτό, η εργασία διαρθρώνεται σε τέσσερα κεφάλαια. Στο πρώτο κεφάλαιο παρουσιάζεται τι είναι το Blockchain από τεχνολογική άποψη και η εξέλιξή του από τη στιγμή της δημιουργίας του μέχρι και σήμερα. Επίσης, αναλύονται τα blocks και πως αυτά συνδέονται άρρηκτα ώστε να δημιουργήσουν μια αλυσίδα. Στη συνέχεια, εξετάζονται τα χαρακτηριστικά ενός blockchain και πως αυτά το καθιστούν ικανό και ιδανικό για τη σημερινή εποχή. Τέλος, αναλύονται πεδία στα οποία το blockchain έχει ήδη υιοθετηθεί από τη σύγχρονη κοινωνία και πως χάρη στη χρήση αυτής της τεχνολογίας, τομείς όπως η εκπαίδευση και το εμπόριο επωφελούνται. Στο δεύτερο κεφάλαιο προσεγγίζονται τα κρυπτονομίσματα, ένα είδος ηλεκτρονικού νομίσματος προγραμματισμένο για συναλλαγές. Παρουσιάζονται διαφορετικοί τύποι κρυπτονομισμάτων και οι διαφορετικές εφαρμογές τους. Επίσης, γίνεται μια σύντομη αναφορά στα σημαντικότερα κρυπτονομίσματα και σύγκριση μεταξύ των δυο μεγαλύτερων, του Bitcoin και του Ethereum. Στο τρίτο κε-

φάλαιο αναλύεται συγκεκριμένα το Ethereum Blockchain. Η εργασία παίρνει μια πιο τεχνική προσέγγιση, εξετάζοντας τα accounts, τα contracts, τα transactions όπως επίσης το mining, το gas και τους αλγόριθμους συναίνεσης. Τέλος, στο τέταρτο κεφάλαιο, γίνεται ο προγραμματισμός μιας αποκεντρωμένης εφαρμογής, αποτελούμενης από 2 smart contracts, την προσομοίωση της συμπεριφοράς τους με στόχο τον μέγιστο έλεγχο και ασφάλειά τους, τη σύνδεση τους με ένα user interface και τέλος την αλληλεπίδραση ενός χρήστη με ολόκληρη την εφαρμογή. Κατά τη διαδικασία κατασκευής του προγράμματος, παρέχονται code snippets με σκοπό την εξήγηση του κώδικα.

### Ευχαριστήριο σημείωμα

Ευχαριστώ θερμά τον επιβλέποντα Καθηγητή μου κ. Μάγκο για τις γνώσεις, την πολύτιμη βοήθεια, καθώς και τη συνεχή καθοδήγηση που μου παρείχε καθ' όλη τη διαδικασία συγγραφής της πτυχιακής μου εργασίας. Θα ήθελα επιπλέον να ευχαριστήσω τα δύο μέλη της τριμελούς εξεταστικής επιτροπής, τον κ. Νταντογιάν και τον κ. Κουρουθανάση, καθηγητές μου στο Τμήμα Πληροφορικής του Ιονίου Πανεπιστημίου, για όλες τις γνώσεις που μου προσέφεραν κατά τη διάρκεια της φοίτησής μου. Επίσης, θα ήθελα να ευχαριστήσω τον ακαδημαϊκό υπότροφο Δρ. Καραγιάννη για τη συνεχή και άμεση βοήθεια που μου προσέφερε. Τέλος, ευχαριστώ την οικογένειά μου για την αμέριστη στήριξη αλλά και κατανόηση που υπέδειξαν και εξακολουθούν να υποδεικνύουν σε όλα μου τα ακαδημαϊκά -και μη- εγχειρήματα.

# Περιεχόμενα

|                                                           |    |
|-----------------------------------------------------------|----|
| Πρόλογος                                                  | i  |
| A Blockchain                                              | 4  |
| A.1 ΤΙ ΕΙΝΑΙ ΤΟ BLOCKCHAIN . . . . .                      | 5  |
| A.2 Η ΕΞΕΛΙΞΗ ΤΟΥ BLOCKCHAIN . . . . .                    | 6  |
| A.3 Ο ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ BLOCKCHAIN . . . . .         | 8  |
| A.4 Η ΔΟΜΗ ΤΟΥ BLOCK . . . . .                            | 10 |
| A.5 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ BLOCKCHAIN . . . . .               | 12 |
| A.6 ΠΕΔΙΑ ΕΦΑΡΜΟΓΗΣ ΤΟΥ BLOCKCHAIN . . . . .              | 14 |
| B Κρυπτονομίσματα                                         | 18 |
| B.1 ΤΥΠΟΙ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ . . . . .                      | 19 |
| B.2 ΕΠΙΡΡΟΗ ΚΑΙ ΑΝΤΙΚΤΥΠΟΣ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ . . . . . | 23 |
| B.3 ΤΑ ΣΗΜΑΝΤΙΚΟΤΕΡΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ . . . . .            | 25 |
| B.4 BITCOIN VS ETHEREUM . . . . .                         | 26 |
| C Ethereum Blockchain                                     | 30 |
| C.1 ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ ΤΟ ETHEREUM . . . . .                  | 31 |
| C.1.1 Δίκτυο Ethereum . . . . .                           | 31 |
| C.1.2 Λογαριασμοί . . . . .                               | 32 |
| C.1.3 Δημιουργία συμβολαίων . . . . .                     | 33 |
| C.1.4 Συναλλαγές και μηνύματα . . . . .                   | 35 |
| C.1.5 Gas . . . . .                                       | 37 |
| C.1.6 Εξόρυξη . . . . .                                   | 39 |

|       |                                                                                  |    |
|-------|----------------------------------------------------------------------------------|----|
| C.1.7 | Εκτέλεση συναλλαγών . . . . .                                                    | 40 |
| C.1.8 | Πορτοφόλια . . . . .                                                             | 43 |
| C.1.9 | Αλγόριθμοι συναίνεσης (Pow, PoS) . . . . .                                       | 44 |
| C.2   | SMART CONTRACTS . . . . .                                                        | 45 |
| C.2.1 | Τα δημοφιλέστερα smart contracts . . . . .                                       | 46 |
| C.3   | PROGRAMMING SMART CONTRACTS IN ETHEREUM . . . . .                                | 47 |
| D     | Προγραμματισμός smart contract για αγοραπωλησία ακίνητης<br>περιουσίας . . . . . | 48 |
| D.1   | CONTRACTS . . . . .                                                              | 51 |
| D.2   | TESTING . . . . .                                                                | 58 |
| D.3   | DEPLOYMENT . . . . .                                                             | 67 |
| D.4   | FRONT-END . . . . .                                                              | 70 |
| D.5   | ΑΛΛΗΛΕΠΙΔΡΩΝΤΑΣ ΜΕ ΤΟ SMART CONTRACT . . . . .                                   | 72 |
|       | Επίλογος . . . . .                                                               | 80 |
|       | Βιβλιογραφικές αναφορές . . . . .                                                | 82 |

# Κατάλογος Σχημάτων

|                                                                                                                                                                                                                                         |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| A.1 απεικόνιση τμήματος ενός blockchain. (Πηγή: HBH (Hellenic Blockchain Hub): <a href="https://www.blockchain.org.gr/home/mathe/">https://www.blockchain.org.gr/home/mathe/</a> ) . . . . .                                            | 10 |
| A.2 Ακολουθία blocks (Πηγή: Τίγκας, 2021) . . . . .                                                                                                                                                                                     | 11 |
| A.3 Horizen Academy <a href="https://www.horizen.io/blockchain-academy/technology/advanced/blockchain-as-a-data-structure/">https://www.horizen.io/blockchain-academy/technology/advanced/blockchain-as-a-data-structure/</a> . . . . . | 11 |
| B.4 Κεφαλαιοποίηση σημαντικότερων κρυπτονομισμάτων (Πηγή: CoinMarketCap, <a href="https://coinmarketcap.com/all/views/all/">https://coinmarketcap.com/all/views/all/</a> , 10/1/2023) . . . . .                                         | 26 |
| C.5 Ethereum Accounts (Kasireddy, 2017) . . . . .                                                                                                                                                                                       | 33 |
| C.6 Ethereum Transaction (Kasireddy, 2017) . . . . .                                                                                                                                                                                    | 36 |
| C.7 Gas calculation (Kasireddy, 2017) . . . . .                                                                                                                                                                                         | 37 |
| C.8 Gas calculation (Kasireddy, 2017) . . . . .                                                                                                                                                                                         | 38 |
| C.9 Gas calculation (Kasireddy, 2017) . . . . .                                                                                                                                                                                         | 38 |
| C.10 Gas calculation (Kasireddy, 2017) . . . . .                                                                                                                                                                                        | 39 |
| C.11 Gas calculation (Kasireddy, 2017) . . . . .                                                                                                                                                                                        | 41 |
| C.12 Gas calculation (Kasireddy, 2017) . . . . .                                                                                                                                                                                        | 41 |
| C.13 Gas calculation (Kasireddy, 2017) . . . . .                                                                                                                                                                                        | 42 |
| C.14 Top Ethereum applications, Source: <a href="https://dappradar.com/rankings/protocol/ethereum">https://dappradar.com/rankings/protocol/ethereum</a> . . . . .                                                                       | 46 |
| D.15 Διάγραμμα ενεργειών του έξυπνου συμβολαίου . . . . .                                                                                                                                                                               | 50 |
| D.16 Διάγραμμα συμμετεχόντων στο Smart Contract και η αλληλεπίδρασή τους με τα 2 συμβόλαια. . . . .                                                                                                                                     | 51 |
| D.17 Dummy accounts για testing που δίνει το Hardhat framework . . . . .                                                                                                                                                                | 61 |
| D.18 Έλεγχος για τα tests που γράφτηκαν μέχρι στιγμής περνάνε τον έλεγχο. . . .                                                                                                                                                         | 64 |

|                                                                                                                                                   |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----|
| D.19 Έλεγχος ορθότητας για τα τελικά tests των του Escrow Contract. . . . .                                                                       | 67 |
| D.20 Επικύρωση της εκτέλεσης του script. Τα συμβόλαια έγιναν deployed τοπικά. .                                                                   | 69 |
| D.21 Προσθήκη στο Metamsk του τοπικού blockchain που παρέχει το Hardhat. . .                                                                      | 70 |
| D.22 Προσθήκη των account που παρέχει το Hardhat ώστε να μπορεί ο χρήστης<br>να αλληλεπιδράσει με τα συμβόλαια υπο διαφορετικούς ρόλους . . . . . | 71 |
| D.23 Το User Interface όταν ο χρήστης με την ιδιότητα του αγοραστή επιλέξει να<br>αγοράσει ένα ακίνητο. . . . .                                   | 72 |
| D.24 Το User interface απο την πλευρά του πωλητή . . . . .                                                                                        | 75 |
| D.25 Το User interface απο την πλευρά του πωλητή . . . . .                                                                                        | 75 |
| D.26 Το User interface απο την πλευρά του Επιθεωρητή . . . . .                                                                                    | 76 |
| D.27 Το User interface απο την πλευρά του lender . . . . .                                                                                        | 76 |
| D.28 Το User Interface απο την πλευρά του πωλητή . . . . .                                                                                        | 77 |
| D.29 Το User Interface τη στιγμή ολοκλήρωσης της συναλλαγής. . . . .                                                                              | 77 |
| D.30 Διαφορά υπολοίπων στους λογαριασμούς του πωλητή και αγοραστή αντίσ-<br>τοιχα, στο ψηφιακό πορτοφόλι του Metamask. . . . .                    | 78 |

# Γλωσσάρι Ξενικών Όρων

|                             |                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Anonymity</b>            | Ανωνυμία                                                                                                             |
| <b>Auditability</b>         | Ανάλυση κώδικα με στόχο τον έλεγχο                                                                                   |
| <b>Block</b>                | Τα βασικά “δοχεία” πληροφοριών σε ένα blockchain                                                                     |
| <b>Blockchain</b>           | Ένα δίκτυο που αποτελείται από αλυσίδες με block                                                                     |
| <b>Centralization Issue</b> | Ζήτημα της συγκέντρωσης                                                                                              |
| <b>Consensus Mechanism</b>  | Αλγόριθμός συναίνεσης                                                                                                |
| <b>Cryptocurrency</b>       | Κρυπτονομίσματα                                                                                                      |
| <b>Cryptographic</b>        | Κρυπτογραφικός                                                                                                       |
| <b>Dapps</b>                | Decentralized Applications                                                                                           |
| <b>Data</b>                 | Δεδομένα                                                                                                             |
| <b>Decentralization</b>     | Αποκεντρωμένος                                                                                                       |
| <b>Defined Access Value</b> | Καθορισμένη αξία πρόσβασης                                                                                           |
| <b>Distributed Ledger</b>   | Κατανεμημένο αρχείο                                                                                                  |
| <b>Double Spending</b>      | Ελάττωμα σε ένα πρωτόκολλο στο οποίο το ίδιο μεμονωμένο ψηφιακό token μπορεί να δαπανηθεί περισσότερες από μία φορές |
| <b>EVM</b>                  | Ethereum Virtual Machine, Εικονική Μηχανή<br>Ethereum                                                                |
| <b>Execution</b>            | Εκτέλεση                                                                                                             |
| <b>Gas</b>                  | “Αέριο”. Χρησιμοποιείται σαν φόρος επιβάρυνσης κατά την εκτέλεση συναλλαγών στον Ethereum Blockchain                 |
| <b>GasLimit</b>             | Όριο gas                                                                                                             |
| <b>GasPrice</b>             | Τιμή gas                                                                                                             |
| <b>GHOST</b>                | Greedy Heaviest Observed Subtree                                                                                     |

|                                   |                                                                                                                                                 |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hash function</b>              | Συνάρτηση κατακερματισμού                                                                                                                       |
| <b>Init</b>                       | Initialize, εκκίνηση                                                                                                                            |
| <b>IoT</b>                        | Internet of things                                                                                                                              |
| <b>Issuance</b>                   | Έκδοση                                                                                                                                          |
| <b>Log series</b>                 | Σειρά καταγραφής                                                                                                                                |
| <b>loops</b>                      | Βρόχοι                                                                                                                                          |
| <b>Mainnet</b>                    | Το κύριο δίκτυο τους blockchain                                                                                                                 |
| <b>Metadata</b>                   | Μεταδεδομένα                                                                                                                                    |
| <b>Miner</b>                      | Ο χρήστης που κάνει mining                                                                                                                      |
| <b>Mining</b>                     | Διαδικασία δημιουργίας block                                                                                                                    |
| <b>native</b>                     | Εγγενής                                                                                                                                         |
| <b>NFT</b>                        | Non-Fungible Token                                                                                                                              |
| <b>Nodes</b>                      | Κόμβοι                                                                                                                                          |
| <b>Nonce</b>                      | Μετρητής που μετράει πόσες συναλλαγές έχουν διεκπεραιωθεί από έναν λογαριασμό                                                                   |
| <b>OOG</b>                        | Out-of-gas                                                                                                                                      |
| <b>P2P</b>                        | Peer-to-Peer                                                                                                                                    |
| <b>Proof of Stake</b>             | Αλγόριθμος συναίνεσης με βάση το staking                                                                                                        |
| <b>Proof of Work</b>              | Αλγόριθμος συναίνεσης με βάση το mining                                                                                                         |
| <b>Randomly Generated Address</b> | Τυχαία διεύθυνση                                                                                                                                |
| <b>Refund balance</b>             | Υπόλοιπο επιστροφής χρημάτων                                                                                                                    |
| <b>RLP</b>                        | Recursive Length Prefix                                                                                                                         |
| <b>Self-destruct set</b>          | Σετ αυτοκαταστροφής                                                                                                                             |
| <b>Server</b>                     | Διακομιστής                                                                                                                                     |
| <b>Solidity</b>                   | Γλώσσα προγραμματισμού των smart contracts                                                                                                      |
| <b>Stablecoins</b>                | Σταθερά νομίσματα                                                                                                                               |
| <b>Staking</b>                    | Το “ποντάρισμα” είναι μια διαδικασία κατά την οποία οι κάτοχοι κρυπτονομισμάτων συμμετέχουν εθελοντικά στην επικύρωση συναλλαγών στο blockchain |
| <b>Storage</b>                    | Αποθηκευτικός χώρος                                                                                                                             |
| <b>Testnet</b>                    | Δίκτυο για ελέγχους                                                                                                                             |
| <b>Timestamp</b>                  | Χρόνο-σφραγίδα                                                                                                                                  |
| <b>Tokens</b>                     | Ψηφιακές αναπαραστάσεις περιουσιακών στοιχείων που χρησιμοποιούνται για τη διευκόλυνση συναλλαγών                                               |

|                     |                    |
|---------------------|--------------------|
| <b>Transaction</b>  | Συναλλαγή          |
| <b>Transparency</b> | Διαφάνεια          |
| <b>Use cases</b>    | Περιπτώσεις χρήσης |
| <b>Validator</b>    | Επικυρωτής         |
| <b>Validator</b>    | Επικυρωτής         |
| <b>Wallets</b>      | Πορτοφόλι          |

## Κεφάλαιο Α

# Blockchain

Η ιδέα της δημιουργίας κρυπτονομισμάτων (cryptocurrency), προέκυψε ως λύση στην αποφυγή των περιορισμών στην κίνηση κεφαλαίων και έκανε για πρώτη φορά την εμφάνισή της μετά την κατάρρευση της εταιρίας Lehman Brothers το 2008 (Τίγκας, 2021). Το πρώτο κρυπτονόμισμα που κυκλοφόρησε ήταν το Bitcoin και στόχος του ήταν να δημιουργήσει έναν εναλλακτικό τρόπο ηλεκτρονικών συναλλαγών που να μην εξαρτάται από μεσάζοντες, αλλά να επιτρέπει ασφαλείς και αδιαμφησβήτητες απευθείας συναλλαγές ανάμεσα στους χρήστες του. Η δημιουργία του, αποδίδεται στον Satoshi Nakamoto -πιθανότατα ψευδώνυμο πίσω από το οποίο κρύβεται μια ομάδα ειδικών της πληροφορικής και της οικονομικής επιστήμης-, ο οποίος πρώτος στο άρθρο του “Bitcoin: A Peer-to-Peer Electronic Cash System” περιέγραψε τα βασικά της δημιουργίας ενός συστήματος ηλεκτρονικών συναλλαγών ανεξάρτητου από χρηματοπιστωτικά ιδρύματα και απρόσβλητου από κυβερνητικές παρεμβάσεις και χειρισμούς. Το σύστημα αυτό, βασισμένο σε ένα peer-to-peer δίκτυο, θα μπορούσε να εξασφαλίζει την διενέργεια ανώνυμων και ασφαλών συναλλαγών, χρησιμοποιώντας ένα μηχανισμό “proof-of-work” για την δημιουργία ενός δημόσιου ιστορικού των συναλλαγών αδύνατον να παραβιαστεί από έναν εισβολέα (Nakamoto, 2008). Σε ένα τέτοιο αποκεντρωμένο οικονομικό σύστημα, η προσφορά και η αξία των ψηφιακών νομισμάτων ελέγχονται από τους ίδιους τους χρήστες, μέσω πολύπλοκων πρωτοκόλλων που χρησιμοποιούν το δίκτυο P2P και έτσι, είναι απρόσβλητη από κυβερνητικές παρεμβάσεις και χειρισμούς.

Ωστόσο, η δημιουργία του Bitcoin, βασίστηκε επάνω στην προυπάρχουσα τεχνολογία Blockchain, η οποία δεν δημιουργήθηκε με αποκλειστικό στόχο την εφαρμογή στα κρυπτονομίσματα και στη βασική της μορφή είχε παρουσιαστεί το 1982 από τον D. Chaum ο οποίος

πρότεινε ένα παρόμοιο πρωτόκολλο μεταφοράς, το οποίο αργότερα, το 1991, εξέλιξαν οι S. Haber και W. Scott Stornetta περιγράφοντας τη δημιουργία μίας κρυπτογραφημένης αλυσίδας blocks δεδομένων (Bharathan, 2020). Θα πρέπει έτσι να είναι σαφές εξ αρχής, ότι το Bitcoin -και γενικά τα κρυπτονομίσματα- και το Blockchain, είναι δύο διαφορετικά πράγματα. Το κρυπτονόμισμα είναι το μέσο με το οποίο γίνονται οι συναλλαγές, και το Blockchain είναι το σύστημα το οποίο τις υποστηρίζει, τις επαληθεύει, τις εγκρίνει, τις καταγράφει και εξασφαλίζει την ασφάλεια και την εγκυρότητά τους.

## A.1 Τι είναι το blockchain

Το Blockchain<sup>1</sup> είναι μία “αλυσίδα” από ψηφιακά Blocs που περιέχουν δεδομένα. Η αλυσίδα αυτή των δεδομένων σχηματίζεται έτσι ώστε κάθε block να συνδέεται άρρηκτα με το προηγούμενο block, μέσω κρυπτογραφικών μεθόδων. Έτσι, αν κάποιος επιχειρήσει να κάνει μια αλλαγή σε κάποιο block, θα πρέπει να αλλάξει όλα τα blocks που ακολουθούν, ώστε να συνεχίσει να ισχύει η αλυσίδα, αλλιώς όλα τα blocks μετά από αυτό που αλλάχτηκε θα είναι άκυρα (Nofer et al, 2017).

Στην ουσία το Blockchain είναι ένα κατακεντρωμένο αρχείο (distributed ledger), ένα μητρώο δηλαδή, στο οποίο οι πληροφορίες αποθηκεύονται και επαληθεύονται (Salah et al, 2019). Το μητρώο αυτό είναι δημόσιο, και όπως προαναφέρθηκε δεν μπορεί να τροποποιηθεί, με συνέπεια να υπάρχει η εγγύηση ότι όλα τα δεδομένα και οι κινήσεις που έχουν καταγραφεί, είναι έγκυρα και αδιαμφισβήτητα. Ωστόσο, η θεμελιώδης διαφορά του από τα συνηθισμένα μητρώα και βάσεις δεδομένων, είναι ότι για την τήρησή του δεν είναι αρμόδια μία κεντρική αρχή, αλλά οι λεγόμενοι κόμβοι (nodes), δηλαδή χρήστες οι οποίοι, έχοντας εγκαταστήσει το απαιτούμενο λογισμικό ενημερώνουν, ταυτόχρονα όλοι, το μητρώο για τις αλλαγές σε αυτό, ώστε ανά πάσα στιγμή όλοι να έχουν την ίδια ακριβώς την ίδια κατάσταση του μητρώου (Λογαράς, 2018).

Οι συναλλαγές πραγματοποιούνται με αποκεντρωμένο τρόπο εξαλείφοντας την απαίτηση για μεσάζοντες για την επικύρωση και την επαλήθευση των συναλλαγών (Litke et al, 2019). Έτσι, όταν γίνεται για παράδειγμα μια μεταφορά χρημάτων, αυτή δεν επιβεβαιώνεται από κάποια κεντρική διαχείριση η οποία τηρεί το μητρώο συναλλαγών (πχ. Τράπεζα), αλλά επαληθεύεται από όλους τους κόμβους (χρήστες) οι οποίοι τηρούν το ίδιο μητρώο και το ενημερώνουν ταυτόχρονα. Κατά συνέπεια, το μητρώο σε μία πλατφόρμα blockchain δεν βρίσκεται σε

---

<sup>1</sup>Στα ελληνικά χρησιμοποιούνται για τον όρο blockchain διάφοροι όροι όπως αλυσίδα block, τεχνολογία κατακεντρωμένης εγγραφής, αλυσίδα ομάδων συναλλαγών ή αλυσίδα κοινοποιήσεων (Wikipedia, 2021).

ένα σημείο, αλλά είναι διανεμημένο (distributed) με αποτέλεσμα να τηρείται από όλους τους κόμβους και να συγχρονίζεται ταυτόχρονα, ώστε όλοι οι κόμβοι να έχουν το ίδιο ενημερωμένο μητρώο.

Με τον τρόπο αυτό, δεν είναι πια απαραίτητη η ύπαρξη ενός έμπιστου μεσάζοντα όπως οι τράπεζες, αφού η εμπιστοσύνη των χρηστών βασίζεται στην αυτόματη επιβεβαίωσή των συναλλαγών μέσα από το λογισμικό. Η ανταλλαγή των δεδομένων, πραγματοποιείται στο Peer2Peer (P2P) δίκτυο των συνδεδεμένων υπολογιστών (κόμβων - nodes), που, όσο περισσότεροι είναι, τόσο μεγαλύτερη ασφάλεια και εγκυρότητα προσδίδουν στο σύστημα (HBH, 2021). Αυτό το μοντέλο εξασφαλίζει ότι η ασφάλεια είναι ανώτερη ενός συστήματος client – server, αφού αν ένας κόμβος σταματήσει να λειτουργεί, το σύστημα δεν καταρρέει και τα δεδομένα είναι ασφαλή.

Το είδος των δεδομένων καθώς και ο τρόπος με τον οποίο καταχωρούνται και επαληθεύονται τα δεδομένα, καθορίζεται από το λογισμικό της κάθε συγκεκριμένης πλατφόρμας blockchain.

Μια πλατφόρμα blockchain, μπορεί να είναι δημόσια (ανοιχτή) ή ιδιωτική (κλειστή). Σε ένα δημόσιο κατάλογο blockchain (πχ. Bitcoin) ο καθένας μπορεί να γράφει ή να διαβάσει. Αντίθετα, σε έναν ιδιωτικό κατάλογο, όλοι οι συμμετέχοντες στην αλυσίδα είναι γνωστοί και έμπιστοι (παράδειγμα παραγγελίες εσωτερικά σε μια εταιρεία ή ένα οργανισμό όπως μια Τράπεζα) και είναι οι μόνοι με πρόσβαση στον κατάλογο ενώ και η διαδικασία proof-of-work (βλέπε παρακάτω) είναι πιο απλή.

## A.2 Η εξέλιξη του Blockchain

Ήδη, από την πρώτη της εφαρμογή στο κρυπτονόμισμα Bitcoin, η τεχνολογία του Blockchain δεν έπαψε να εξελίσσεται και να βελτιώνεται από ειδικούς των υπολογιστών, μαθηματικούς, κρυπτογράφους και ειδικούς του χρηματοοικονομικού τομέα. Το Blockchain 1.0 χρησιμοποιήθηκε για κρυπτονομίσματα, συστήματα πληρωμών συναλλάγματος, και απλές οικονομικές συναλλαγές με μετρητά (Swan, 2015).

Μία πρώτη μεγάλη εξέλιξη, ήταν η εισαγωγή των έξυπνων συμβολαίων (smart contracts) που έγινε με το δεύτερης γενιάς blockchain system, Ethereum (Nofer et al, 2017). Τα Smart contracts είναι μικρές εφαρμογές υπολογιστών (προγράμματα) που θέτουν συγκεκριμένες συνθήκες και κριτήρια που πρέπει να ικανοποιηθούν προκειμένου να πραγματοποιηθεί μία

συναλλαγή πριν καταχωρηθεί στην αλυσίδα. Πιο συγκεκριμένα, τα smart contracts χρησιμοποιούν κώδικα της μορφής IFTTT (if-this-then-that) ο οποίος εκτελείται αυτόματα αν συντρέχουν οι προϋποθέσεις που έχουν τεθεί ή, σε άλλες περιπτώσεις, αν παραβιαστούν οι όροι χρηματοδότησης. Η διαδικασία αυτή εκτελείται χωρίς την μεσολάβηση κάποιου τρίτου μέρους (Alammery et al, 2019; Ezeudu et al, 2018). Αυτή η εξέλιξη, επέτρεψε στην τεχνολογία του blockchain να εφαρμοστεί και σε χρηματοοικονομικά εργαλεία όπως τα δάνεια, τα ομόλογα και οι υποθήκες αλλά και σε άλλες τραπεζικές συναλλαγές. Έτσι θα μπορούσε να ειπωθεί ότι το Blockchain 2.0 έχει να κάνει με συναλλαγές ιδιοκτησίας (properties), διαπραγμάτευση τίτλων (securities trading), smart contracts, και άλλες εφαρμογές του χρηματοοικονομικού τομέα (Bhaskar et al, 2020).

Μια άλλη πολύ σημαντική εξέλιξη, ήταν η σταδιακή εξέλιξη των μηχανισμών συναίνεσης (consensus mechanisms), από την διαδικασία proof-of-work, η οποία απαιτεί εξαιρετικά μεγάλη υπολογιστική ισχύ, στη διαδικασία proof-of-stake που εισήχθη από το Ethereum Blockchain και χρησιμοποιεί περισσότερο χρηματοοικονομικά εργαλεία για να προσφέρει το ίδιο επίπεδο ασφάλειας (βλ. παρακάτω κεφ. 3.1.9.).

Το ίδιο σημαντική ήταν και η μετάβαση στο blockchain scaling, που δεν χρησιμοποιεί πια όλους τους υπολογιστές για να επαληθεύσει τις συναλλαγές, αλλά μόνο όσους είναι απαραίτητοι για κάθε συναλλαγή, προφανώς προσφέροντας το ίδιο επίπεδο ασφάλειας, ενώ επιταχύνει δραστικά τη διαδικασία (Gupta, 2017).

Η επόμενη γενιά της τεχνολογίας, Blockchain 3.0, χρησιμοποιεί αποκεντρωμένη αποθήκευση των δεδομένων (decentralized storage) και επικοινωνία (decentralized communication) και εστιάζει στην ανάπτυξη εφαρμογών σε πεδία όπως η ηλεκτρονική διακυβέρνηση (e-government-, η υγεία, οι επιστήμες, αλλά και η ανταλλαγή έργων τέχνης (Swan, 2015; Alammery et al, 2019; Chen et al, 2018). Όπως το έθεσαν οι Efanov & Roshlin (2018) μπορούμε να αναγνωρίσουμε τρεις φάσεις ανάπτυξης: το Blockchain 1.0 σαν ψηφιακό νόμισμα, το Blockchain 2.0 ως ψηφιακή οικονομία και το Blockchain 3.0 σαν ψηφιακή κοινωνία.

Σήμερα, ο κύκλος εργασιών των εφαρμογών του blockchain γνωρίζει αλματώδη ανάπτυξη, ξεπερνώντας σε όγκο συναλλαγών τα 8 δισεκατομμύρια δολάρια το 2021<sup>2</sup>. Η έρευνα συνεχίζεται στην τέταρτη γενιά, το Blockchain 4.0, στο χώρο των επιχειρήσεων και της βιομηχανίας (Industry 4.0), με την αναζήτηση εφαρμογών σε τομείς όπως η διαχείριση εφοδιαστικής αλυσίδας (supply chain management), τα συστήματα οικονομικής διαχείρισης

---

<sup>2</sup>Στοιχεία από το Nasdaq Data Link, <https://data.nasdaq.com/data/BCHAIN/ETRVU-bitcoin-estimated-transaction-volume-usd>

(financial management systems), διαχείριση ροής εργασιών (workflow management) και η διαχείριση περιουσιακών στοιχείων (financial management systems) (Bhaskar et al, 2020).

### A.3 Ο τρόπος λειτουργίας του Blockchain

Όπως προαναφέρθηκε, το blockchain χρησιμοποιεί την τεχνολογία διασύνδεσης peer to peer, δηλαδή διασυνδεδεμένους κόμβους χρηστών. Ένας κόμβος (node) ξεκινά μια συναλλαγή σε ένα αποκεντρωμένο δίκτυο blockchain την οποία σφραγίζει με μια βασισμένη σε private key cryptography. Μια συναλλαγή μπορεί να θεωρηθεί ως μια δομή δεδομένων που αντιπροσωπεύει τη μεταφορά ψηφιακών στοιχείων μεταξύ χρηστών στο δίκτυο blockchain. Όλες οι συναλλαγές αποθηκεύονται σε μια ομάδα μη επιβεβαιωμένων συναλλαγών και διαδίδονται στο δίκτυο χρησιμοποιώντας ένα flooding protocol, γνωστό ως πρωτόκολλο Gossip. Στη συνέχεια, οι χρήστες πρέπει να επιλέξουν και να επικυρώσουν αυτές τις συναλλαγές με βάση ορισμένα προκαθορισμένα κριτήρια. Για παράδειγμα, οι κόμβοι προσπαθούν να επαληθεύσουν και να επικυρώσουν αυτές τις συναλλαγές ελέγχοντας εάν ο αποστολέας έχει αρκετό υπόλοιπο για να ενεργοποιήσει μια συναλλαγή ή προσπαθεί να ξεγελάσει το σύστημα με double spending. Το double spending αναφέρεται στη χρήση του ίδιου ποσού εισροής για δύο ή περισσότερες διαφορετικές συναλλαγές (Karame et al, 2012).

Στην περίπτωση μίας συναλλαγής, επιτυγχάνεται καταρχάς μία συμφωνία (consensus) μεταξύ των χρηστών (κόμβων), για την ορθότητα των στοιχείων που καταχωρούνται στο μητρώο. Οι χρήστες είναι ανώνυμοι, αφού οι λογαριασμοί τους (ψηφιακά πορτοφόλια - digital wallets) δεν περιλαμβάνουν κανένα προσωπικό στοιχείο, το περιεχόμενο όμως των λογαριασμών καθώς και το ιστορικό των συναλλαγών που έχουν πραγματοποιηθεί με αυτούς είναι ορατό σε όλους, το ίδιο και η διεύθυνσή τους, η οποία είναι προφανώς μοναδική.

Η κάθε συναλλαγή που πραγματοποιείται, καταχωρείται στο μητρώο του κάθε χρήστη, μαζί με τα καινούργια υπόλοιπα των λογαριασμών και κρυπτογραφείται με τη μέθοδο hashing μέσω της οποίας παράγεται ένας αριθμός-κλειδί (hash) που ενσωματώνει τα δεδομένα της συναλλαγής, μεταξύ των οποίων είναι το ιδιωτικό και δημόσιο κλειδί κάθε χρήστη. Όταν συμπληρωθεί ένας συγκεκριμένος αριθμός συναλλαγών, η ομάδα αυτή συναλλαγών (block) κλειδώνει, κρυπτογραφείται και πάλι με την ίδια μέθοδο, και της απονέμεται ένα μοναδικό κλειδί, με το οποίο το συγκεκριμένο block αρχειοθετείται, χωρίς πια να μπορεί να μεταβληθεί. Το τελικό αυτό κλειδί (hash) είναι ένας κρυπτογραφικά μοναδικός αριθμός ο οποίος παράγεται από μία συνάρτηση (hash function) η οποία λαμβάνει υπόψιν της το περιεχόμενο του block.

Έτσι, αν γίνει οποιαδήποτε αλλαγή εκ των υστέρων στο περιεχόμενο του block, η συνάρτηση θα δημιουργήσει έναν τελείως διαφορετικό αριθμό hash. Δεδομένου ότι κάθε block που παράγεται από το σύστημα περιέχει εξ ορισμού και τον έγκυρο αριθμό του προηγούμενου block, τυχόν επέμβαση θα παρατηρηθεί άμεσα, αφού το επόμενο block θα έχει διαφορετικό αριθμό από αυτόν που έχει πια το προηγούμενο. Έτσι η αλυσίδα θα σπάσει και δεν θα είναι πια έγκυρη.

Θα πρέπει εδώ να σημειωθεί, ότι για να κλειδώσει ένα block και να ενταχθεί στην αλυσίδα, πρέπει να λυθεί ένας μαθηματικός γρίφος μέσω μίας εξαιρετικά περίπλοκης μαθηματικής εργασίας (proof of work). Την εργασία αυτή (mining) αναλαμβάνουν οι λεγόμενοι «μεταλλωρύχοι» (miners), χρήστες που χρησιμοποιούν την υπολογιστική τους ισχύ για την εξόρυξη των blocks, οι οποίοι έχουν εγκατεστημένο το απαραίτητο λογισμικό (Kroll et al, 2013). Οι κόμβοι που είναι υπεύθυνοι για το mining οφείλουν να λύσουν έναν υπολογιστικό γρίφο, ξοδεύοντας αρκετούς από τους υπολογιστικούς πόρους τους για να δημοσιεύσουν ένα καινούριο block. Επειδή η λύση αυτού του γρίφου επιτυγχάνεται μόνο μέσω αλληπάλληλων δοκιμών τρισεκατομμυρίων διαφορετικών hashes ανά δευτερόλεπτο μέχρι να βρεθεί ο σωστός, απαιτεί εξαιρετικά μεγάλη υπολογιστική ισχύ ή ειδικές συσκευές mining (πχ. ASIC για το Bitcoin, GPU για το Ethereum κ.ά.). Ο miner που θα καταφέρει να λύσει πρώτος το παζλ ανακηρύσσεται νικητής και δημιουργεί ένα νέο block, και γι αυτό «ανταμείβεται» είτε με τη μορφή νέου νομίσματος που δημιουργείται για πρώτη φορά -με ένα ποσό από το αντίστοιχο κρυπτονόμισμα- ή/και με τέλη επί των συναλλαγών που περιλαμβάνονται στο block (Τίγκας, 2021).

Αφού κάποιος miner λύσει το γρίφο -βρει δηλαδή τον αριθμό στόχο, το hash του προσωρινού υπό έγκριση block-, τον στέλνει στο δίκτυο των κόμβων το οποίο επαληθεύει τη λύση χρησιμοποιώντας έναν consensus mechanism, δηλαδή μια τεχνική που βοηθά ένα αποκεντρωμένο δίκτυο να καταλήξει σε συμφωνία για το συγκεκριμένο θέμα. Μετά από αυτό, το νέο block θα προστεθεί στην υπάρχουσα αλυσίδα και στο τοπικό αντίγραφο του ledger που έχει ο κάθε peer. Σε αυτό το σημείο, η συναλλαγή επιβεβαιώνεται και το καινούριο block έρχεται να συνδεθεί με το τελευταίο της αλυσίδας, χρησιμοποιώντας έναν cryptographic hash. Τώρα το block λαμβάνει την πρώτη του επιβεβαίωση ενώ η συναλλαγή λαμβάνει τη δεύτερη επιβεβαίωση. Ομοίως, κάθε φορά που προστίθεται ένα νέο block στην αλυσίδα, η συναλλαγή θα επιβεβαιώνεται εκ νέου. Γενικά, μια συναλλαγή χρειάζεται έξι επιβεβαιώσεις στο δίκτυο για να θεωρηθεί οριστική (Del Castillo, 2017).

Με τον τρόπο αυτό δημιουργείται η αλυσίδα των blocks με τις συναλλαγές η οποία διαρκώς

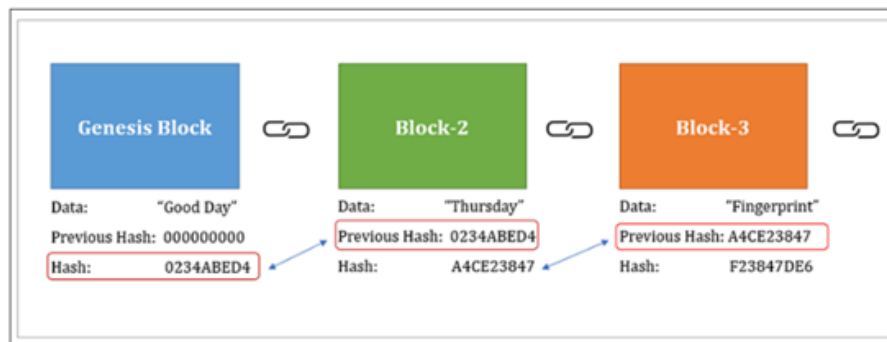
μεγαλώνει (ενδεικτικά στην πλατφόρμα blockchain του Bitcoin ένα block το οποίο περιέχει περίπου από 1.500 έως και 3.500 συναλλαγές, προστίθεται κάθε 12 λεπτά) (Λογαράς, 2018). Τα blocks αυτά είναι κρυπτογραφημένα με τον αλγόριθμό SHA-256 secure hash algorithm, ο οποίος κρυπτογραφεί μαθηματικά και κατακερματίζει την πληροφορία του block με τρόπο ο οποίος να μην μπορεί να είναι αναστρέψιμος (one way encryption) (HBH, 2021). Στην εικόνα που ακολουθεί, φαίνεται μια σχηματική απεικόνιση τμήματος ενός blockchain δηλαδή μια τυπική ακολουθία blocks και ο τρόπος διασύνδεσής τους με τους αριθμούς hash.



**Σχήμα Α.1:** απεικόνιση τμήματος ενός blockchain. (Πηγή: HBH (Hellenic Blockchain Hub): <https://www.blockchain.org.gr/home/mathe/>)

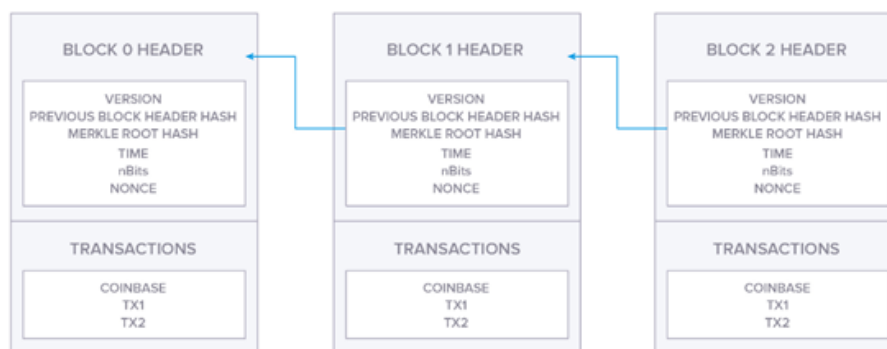
## Α.4 Η δομή του Block

Το Blockchain, όπως προδίδει και η ορολογία, περιλαμβάνει μια ακολουθία block, η οποία αποθηκεύει τις πληροφορίες όλων των συναλλαγών. Αυτά τα blocks συνδέονται μεταξύ τους μέσω ενός hash που ανήκει στο προηγούμενο block γνωστό ως parent block. Το αρχικό block -που δημιουργήθηκε με την γέννηση του bitcoin- ονομάζεται genesis block και δεν έχει κάποιο parent block.



**Σχήμα A.2:** Ακολουθία blocks (Πηγή: Τίγκας, 2021)

Όλα τα blocks, περιλαμβάνουν ένα header και το block body, το οποίο περιέχει την πληροφορία της συναλλαγής. Το header του block περιλαμβάνει metadata όπως η έκδοσή του, το hash του parent block, το Merkle root hash, ένα timestamp, nBits και nonce όπως φαίνεται στην επόμενη εικόνα. Το body του block αποτελείται από έναν counter που εκτελεί χρέη μετρητή συναλλαγών και τις ίδιες τις συναλλαγές που παρουσιάζονται στη μορφή μιας λίστας. Ο μέγιστος αριθμός συναλλαγών που μπορεί να περιέχει ένα block εξαρτάται από το μέγεθος του block και φυσικά από το μέγεθος κάθε συναλλαγής.



**Σχήμα A.3:** Horizen Academy <https://www.horizen.io/blockchain-academy/technology/advanced/blockchain-as-a-data-structure/>

Συνοψίζοντας, ένα block περιέχει:

- Το κρυπτογραφικό αποτύπωμα (hash) του προηγούμενου block στην αλυσίδα
- Το κρυπτογραφικό αποτύπωμα που προκύπτει από τη λειτουργία μιας συνάρτησης κατα-

ερματισμού πάνω στο σύνολο των εισαχθέντων και ξεχωριστών συναλλαγών (transactions) στο εν λόγω block, συμπεριλαμβανομένων και αυτών των συναλλαγών.

- Τη χρονική του σφραγίδα ή χρόνο-σφραγίδα (timestamp). Πρόκειται για τον αριθμό των δευτερολέπτων που έχουν μεσολαβήσει από την 1η Ιανουαρίου του 1970 μέχρι την στιγμή της παραγωγής της χρονο-σφραγίδας.
- Την απόδειξη εργασίας (proof-of-work)
- Το Κρυπτογραφικό αποτύπωμα (hash) του εν λόγω block. Αυτό το hash, θα αποτελέσει την ομάδα (A) του επόμενου από αυτό, block.

## A.5 Χαρακτηριστικά του Blockchain

Το Blockchain λειτουργεί σε ένα αποκεντρωμένο περιβάλλον που χρησιμοποιεί μια πληθώρα βασικών τεχνολογιών, όπως ψηφιακές υπογραφές (digital signatures), κρυπτογραφικοί κατακερματισμοί (cryptographic hashes) και κατανεμημένους αλγόριθμους συναίνεσης (distributed consensus algorithms). Καθ' όλη αυτή τη διαδικασία, κάθε συμμετέχων στο δίκτυο έχει ένα ζεύγος κλειδιών, ένα ιδιωτικό και ένα δημόσιο. Το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή ή την κρυπτογράφηση της συναλλαγής ενώ το δημόσιο κλειδί διανέμεται σε όλο το δίκτυο και είναι ορατό σε όλους, γεγονός απαραίτητο στην αποκρυπτογράφηση της ακόλουθης συναλλαγής (Liang et al, 2017).

Σύμφωνα με τους Monrat et al (2019), το blockchain έχει ορισμένα βασικά χαρακτηριστικά, όπως decentralization, transparency, anonymity and auditability.

### 1. Decentralization

Όπως ειπώθηκε νωρίτερα, στα συμβατικά κεντρικά συστήματα συναλλαγών κάθε συναλλαγή πρέπει να επικυρώνεται μέσω μιας κεντρικής αξιόπιστης υπηρεσίας (π.χ. της τράπεζας). Η αποκεντρωμένη λειτουργία του blockchain φαίνεται να υστερεί στον τομέα εμπιστοσύνης, αφού δεν υπάρχει μια κεντρική αρχή η οποία εγγυάται τις συναλλαγές, αλλά ακριβώς για αυτόν τον λόγο, εξασφαλίζει την δυνατότητα εκτέλεσης των συναλλαγών χωρίς απαραίτητα την έγκριση οποιουδήποτε μεσάζοντα.

Σε αντίθεση με ένα κεντρικό σύστημα, μια συναλλαγή στο δίκτυο blockchain μπορεί να πραγματοποιηθεί μεταξύ οποιωνδήποτε δύο peers (P2P) χωρίς τον έλεγχο ταυτότητας

από την κεντρική υπηρεσία. Το blockchain εξασφαλίζει την εγκυρότητα αντικαθιστώντας τον μεσάζοντα με διάφορα consensus mechanisms. Επιπλέον, μπορεί να μειώσει το κόστος του server, συμπεριλαμβανομένου του κόστους ανάπτυξης και του κόστους λειτουργίας, και να μετριάσει τα σημεία συμφόρησης απόδοσης στον κεντρικό server.

Το blockchain παρουσιάζει ωστόσο και κάποια μειονεκτήματα. Επειδή στην αρχιτεκτονική του bitcoin προβλέπονται ενεργοβόροι μηχανισμοί όπως ο PoW, η σπατάλη ενέργειας είναι πολύ υψηλή, ενώ και οι επιδόσεις είναι επίσης αρκετές τάξεις χαμηλότερες.

## **2. Transparency**

Το Blockchain παρέχει την υποδομή με την οποία μπορεί να μετρηθεί η “αλήθεια” των συναλλαγών και επιτρέπει στους παραγωγούς καθώς και στους καταναλωτές να αποδείξουν ότι τα δεδομένα τους είναι αυθεντικά και δεν έχουν αλλοιωθεί (Liang et al, 2017). Για παράδειγμα, εάν ένα Blockchain αποτελείται από 10 blocks, τότε το block αρ. 10 περιέχει το hash του προηγούμενου (parent) block και για τη δημιουργία ενός νέου block, χρησιμοποιούνται οι πληροφορίες του τρέχοντος block. Επομένως, όλα τα blocks είναι άρρηκτα συνδεδεμένα μεταξύ τους στην υπάρχουσα αλυσίδα. Το ίδιο ισχύει και για τις συναλλαγές οι οποίες ακολουθούν μια ροή. Σε περίπτωση ακόμα και της μικρότερης αλλαγής, μια απλή ενημέρωση θα αλλάξει σημαντικά το hash του block. Εάν κάποιος θέλει να τροποποιήσει οποιαδήποτε πληροφορία, πρέπει να αλλάξει όλα τα hash data του προηγούμενου block, κάτι που θεωρείται μαθηματικά απίθανο λαμβάνοντας υπόψη τον όγκο της δουλειάς που πρέπει να γίνει. Επιπλέον, μετά τη δημιουργία ενός block από έναν miner, αυτό θα πρέπει να επιβεβαιωθεί από άλλους χρήστες στο δίκτυο. Ως εκ τούτου, οποιαδήποτε παραποίηση δεδομένων θα εντοπιστεί κατευθείαν από το δίκτυο και για αυτόν τον λόγο, το blockchain θεωρείται ως ένα αμετάβλητο κατανεμημένο καθολικό (distributed ledger).

## **3. Anonymity**

Χάρη στην τεχνολογία του, το Blockchain δίνει τη δυνατότητα σε έναν οποιονδήποτε χρήστη να αλληλεπιδράσει με αυτό, χρησιμοποιώντας μια τυχαία διεύθυνση, (randomly generated address), που λειτουργεί ως ταυτότητα (Wang et al, 2018). Δεν υπάρχουν περιορισμοί στον αριθμό των διευθύνσεων που μπορεί να ανήκουν σε έναν χρήστη. Ουσιαστικά, το μόνο στοιχείο που συνδέει κάποιον χρήστη με το Blockchain, είναι μια κρυπτογραφημένη ταυτότητα, που αναπαρίσταται από εικοσιπέντε με τριάντα έξι

(25-36) αλφαριθμητικά ψηφία (Bodziony et al, 2021). Ακόμα και στην περίπτωση που οι ψηφιακές ταυτότητες δεν ήταν κρυπτογραφημένες, χάρη στην αποκεντροποίηση του συστήματος, δεν υπάρχει κάποια κεντρική αρχή να επικυρώσει τα στοιχεία που δήλωσε ο χρήστης με την πραγματική του ταυτότητα. Με λίγα λόγια, το Blockchain από τη φύση του προσφέρει ανωνυμία και μη ιχνηλασιμότητα, όσον αφορά έναν χρήστη και τα προσωπικά του στοιχεία.

## **2. Auditability**

Όπως προαναφέρθηκε, όλες οι συναλλαγές στο δίκτυο blockchain καταγράφονται και ταυτόχρονα επικυρώνονται από μια ψηφιακή χρόνο-σφραγίδα. Ως αποτέλεσμα, είναι δυνατό για έναν παρατηρητή, να ακολουθήσει χρονικά μια διεύθυνση και να δει όλες τις συναλλαγές που διεκπεραιώθηκαν από αυτήν. Αυτή είναι άλλωστε, μία εγγενής δυνατότητα της τεχνολογίας του blockchain: ο έλεγχος, η ανίχνευση και η επαλήθευση προηγούμενων εγγραφών, από οποιονδήποτε κόμβο στο δίκτυο (Yu et al, 2018). Χρειάστηκε δηλαδή η συνέπεια και η εγκυρότητα όλων των συναλλαγών μέχρι ενός σημείου, ώστε να διατηρηθεί η εγκυρότητα και διαφάνεια της κατάστασης δεδομένων στο blockchain. Ωστόσο, με τον συνεχόμενα επιταχυνόμενο ρυθμό συναλλαγών, ο εντοπισμός της προέλευσης τους γίνεται ολοένα και δυσκολότερος.

## **A.6 Πεδία εφαρμογής του Blockchain**

Μέσω των κρυπτονομισμάτων, οι διεθνείς μεταφορές κεφαλαίων, επιταχύνονται δραστικά (από μέρες σε λεπτά), ενώ παράλληλα γίνονται με πολύ χαμηλότερο κόστος. Έτσι, η τεχνολογία του blockchain, αναμένεται να επιφέρει ριζικές αλλαγές στον τρόπο λειτουργίας της οικονομίας, καθώς δημιουργεί την δυνατότητα γρήγορων, ασφαλών, έγκυρων και αδιαμφησβήτητων συναλλαγών έξω από το υπάρχον σύστημα, το οποίο μέχρι σήμερα αποτελούσε το μόνο σύστημα μέσω του οποίου μπορούσε να διακινείται χρήμα. Η καινοτομία του έγκειται στο ότι η ελεγκτική διαδικασία που μέχρι τώρα προσφερόταν από το παραδοσιακό τραπεζικό σύστημα, αντικαθίσταται από έναν εξίσου έμπιστο κατανεμημένο ελεγκτικό μηχανισμό, στον οποίο εξαλείφεται κάθε ενδεχόμενο παραβίασης, τόσο λόγω του ότι τα δεδομένα είναι δημόσια, όσο και γιατί ο τρόπος με τον οποίο κωδικοποιούνται και κρυπτογραφούνται είναι πρακτικά απαράβιαστος. Παράλληλα, απελευθερώνει τους χρήστες από τους περιορισμούς στην διακίνηση κεφαλαίων, μειώνει το χρόνο των συναλλαγών και επιτρέπει τις απευθείας συναλλαγές εξαφανίζοντας τους μεσάζοντες, μειώνοντας έτσι το κόστος χωρίς εκπώσεις στην ασφάλεια.

Παρότι η πρώτη εφαρμογή της τεχνολογίας blockchain αφορούσε τα ψηφιακά νομίσματα (Bitcoin), η χρησιμότητά της δεν περιορίζεται σε αυτά. Το blockchain αποτελείται όπως προαναφέρθηκε από blocks δεδομένων, τα οποία δεν είναι απαραίτητο να αφορούν χρηματοοικονομικές συναλλαγές, αλλά οποιονδήποτε άλλο τύπο δεδομένων ο οποίος χρειάζεται να καταγραφεί με ασφάλεια και να μην μπορεί να μεταβληθεί εκ των υστέρων. Για παράδειγμα όταν πωλείται ένα ψηφιακό έργο, το block πρέπει να έχει πληροφορίες σχετικά με το όνομα του έργου, τον καλλιτέχνη, τον προηγούμενο ιδιοκτήτη, τον νέο ιδιοκτήτη, την ώρα της πώλησης και της συναλλαγής. Δίπλα στα δεδομένα, κάθε block έχει ένα αναγνωρίσιμο κλειδί που χρησιμεύει ως δακτυλικό αποτύπωμα.

Αν και το Bitcoin είναι η πιο διάσημη εφαρμογή της τεχνολογίας του blockchain, αυτό μπορεί να χρησιμοποιηθεί σε διάφορες εφαρμογές πέρα από τα κρυπτονομίσματα. Δεδομένου ότι επιτρέπει την ολοκλήρωση των πληρωμών χωρίς κάποιον μεσολαβητή, το blockchain μπορεί να χρησιμοποιηθεί σε διάφορες χρηματοοικονομικές υπηρεσίες, όπως διαχείριση ψηφιακών περιουσιακών στοιχείων ή εμβάσματα και διαδικτυακές πληρωμές (Peters et al, 2015).

Αυτό που ουσιαστικά προσφέρει η τεχνολογία blockchain είναι έναν γρήγορο, ασφαλή, έγκυρο και αδιαμφισβήτητο τρόπο για την πραγματοποίηση συναλλαγών, καθώς και έναν αξιόπιστο κατανεμημένο μηχανισμό ελέγχου, που εξαλείφει κάθε πιθανή παραβίαση, τόσο επειδή τα δεδομένα είναι δημόσια όσο και επειδή η μέθοδος κρυπτογράφησης που χρησιμοποιείται είναι ουσιαστικά απαραβίαστη.

Για το λόγο αυτό, το blockchain υιοθετείται από την σύγχρονη κοινωνία ολοένα και περισσότερο καθώς έχει συμπεριληφθεί σε ένα ευρύ φάσμα εφαρμογών σε πολλούς κλάδους, όπως της χρηματοδότησης, της υγειονομικής περίθαλψης, της διακυβέρνησης, της κατασκευαστικής βιομηχανίας (manufacturing) και της διανομής (distribution) (Al-Jaroodi & Mohamed, 2019). Η υιοθέτηση του blockchain έχει τη δυνατότητα να μεταμορφώσει ένα ευρύ φάσμα εφαρμογών, συμπεριλαμβανομένης της μεταφοράς αγαθών (αλυσίδα εφοδιασμού), της ανταλλαγής ψηφιακών μέσων (πώληση τέχνης) και της παροχής υπηρεσιών εξ αποστάσεως (ταξίδια και τουρισμός) (Casino et al, 2019).

Το Blockchain, ειδικά στην τρίτη γενιά του (blockchain 3.0) έχει πλέον πολλές εφαρμογές στους παρακάτω τομείς:

- στην ηλεκτρονική διακυβέρνηση (e-government), στις ηλεκτρονικές ψηφοφορίες (e-voting) και σε εκλογές, αλλά και στις ψηφιακές ταυτότητες (digital identities) για προφανείς λόγους ασφάλειας και αποφυγής παραβίασης ή αλλαγής,

- στον τομέα της υγείας, για την ασφαλή τήρηση και ανταλλαγή ιατρικών αρχείων,
- στη βιομηχανία τροφίμων και στην παρακολούθηση της αλυσίδας εφοδιασμού για την καταγραφή όλων των πληροφοριών σχετικά με ένα ζώο ή ένα τρόφιμο, από την ανα- παραγωγή / παραγωγή έως την τελική πώληση,
- στις μεταφορές, για την οργάνωση και την παρακολούθηση δεδομένων και προϊόντων,
- στον τομέα των ασφαλειών, για την ασφαλή τήρηση μητρώων και αρχείων,
- Στην τήρηση ασφαλών και αμετάβλητων μητρώων και αρχείων, όπως το κτηματολόγιο, το περιουσιολόγιο, το ληξιαρχείο,
- στην εφορία και στα λογιστήρια εταιρειών,
- στην πιστοποίηση διαφόρων προϊόντων και υπηρεσιών,
- στην αυτόνομη οδήγηση, στην πληρωμή διοδίων, στον ανεφοδιασμό και στις πτήσεις drones για την ασφαλή προσγείωση (Gupta, 2017).,
- στη βιομηχανία ροής ήχου (audio streaming) για την ακριβή καταγραφή της κίνησης κάθε τραγουδιού και μέσω έξυπνων συμβολαίων, αλλά και στην απόδοση πνευματικών δικαιωμάτων σε καλλιτέχνες (Τίγκας, 2021),
- στην διαχείριση θεμάτων πνευματικής ιδιοκτησίας όπως η διανομή τελών ή δικαιωμάτων χρήσης αλλά και η άμεση καταβολή των σχετικών τελών απευθείας από τους χρήστες,
- στην αγορά ψηφιακής τέχνης για την πιστοποίηση της γνησιότητας των ψηφιακών έργων. Η τεχνολογία NFT (Non-Fungible Token) , μια μορφή διακριτικού που χρησι- μοποιείται στο blockchain Ethereum, έχει αναπτυχθεί προς αυτή την κατεύθυνση και,
- στην εκπαίδευση.

Όπως είναι φανερό, το φάσμα των δραστηριοτήτων της ανθρώπινης δραστηριότητας στο οποίο θα μπορούσε να αξιοποιηθεί η τεχνολογία blockchain, είναι ευρύτατο. Η έρευνα πάνω στις προοπτικές που δίνει η τεχνολογία του blockchain είναι παγκόσμια. Η Ευρωπαϊκή Επιτροπή από τον Φεβρουάριο του 2018 έχει συστήσει το EU Blockchain Observatory and Forum, με σκοπό την παρακολούθηση των εξελίξεων, την προώθησή της νέας τεχνολογίας και την έρευνα σε θέματα κρυπτονομισμάτων (European Commission, 2018). Πράγματι, οι

νέες τεχνολογικές εξελίξεις όπως τα δίκτυα 5G, οι έξυπνες και διασυνδεδεμένες συσκευές και η ανάπτυξη του Internet of Things (IoT), οδηγούν σε μία νέα πραγματικότητα στην οποία η ασφαλής διακίνηση των δεδομένων είναι αδιαπραγμάτευτη. Σε αυτήν την νέα πραγματικότητα, η τεχνολογία blockchain, μπορεί να έχει κυρίαρχο ρόλο, καθώς έχει τη δυνατότητα να εξασφαλίσει το απαραίτητο υπόβαθρο για την ασφαλή και απαραβίαστη λειτουργία των συστημάτων μειώνοντας ταυτόχρονα το κόστος και παρέχοντας αυξημένη ταχύτητα στις συναλλαγές (Horwitz & Rosencrance, 2021).

## Κεφάλαιο Β

# Κρυπτονομίσματα

Ενώ το Bitcoin ήταν το πρώτο λειτουργικό δημόσιο κρυπτονόμισμα, δεν είναι ο μόνος τύπος καθώς υπάρχουν στην αγορά πολλά ακόμη κρυπτονομίσματα. Σύμφωνα με το CoinMarketCap, αυτή τη στιγμή ο συνολικός αριθμός κρυπτονομισμάτων σε λειτουργία ξεπερνά τις 22.000, με το συνολικό όγκο συναλλαγών να αγγίζει τα 800 δις. δολάρια. Πολλά ψηφιακά νομίσματα δεν αντιπροσωπεύουν κάποια λογιστική μονάδα, αλλά ένα μέσο ανταλλαγής ή κάποιο περιουσιακό στοιχείο. Έτσι, ο όρος κρυπτονομίσματα, παρότι χρησιμοποιείται για να ορίσει όλους τους διαφορετικούς τύπους ψηφιακών νομισμάτων, συνήθως συσχετίζεται με τα νομίσματα που έχουν χρηματική αξία

Θα πρέπει εξ αρχής να γίνει αντιληπτό, ότι ένα κρυπτονόμισμα δεν λειτουργεί ως κανονικό νόμισμα, αλλά είναι μια κατανεμημένη ηλεκτρονική μορφή χρήματος, ένα ψηφιακό περιουσιακό στοιχείο, η αξία του οποίου είναι συνδεδεμένη και υπάρχει μόνο μέσα στο οικοσύστημα λειτουργίας μιας συγκεκριμένης πλατφόρμας blockchain (Λογαράς, 2018). Η αξία συνεπώς ενός κρυπτονομίσματος, καθορίζεται από την πλατφόρμα, τις λειτουργικές του δυνατότητες και φυσικά, από την απήχυσή του στο παγκόσμιο κοινό. Οι όροι λειτουργίας κάθε κρυπτονομίσματος, είναι ενσωματωμένοι στο πρωτόκολλο (whitepaper) κάθε πλατφόρμας και είναι διαθέσιμοι στο κοινό.

Τα κρυπτονομίσματα, εκτός από τα εγγενή χαρακτηριστικά του blockchain όπως η απουσία κεντρικής αρχής ελέγχου των συναλλαγών και η δυνατότητα χρήσης χωρίς την υποβολή προσωπικών στοιχείων τα οποία υιοθετούν, παρουσιάζουν και μερικά ακόμη κοινά χαρακτηριστικά όπως η δυνατότητα χρήσης σε οποιονδήποτε χώρο και χρόνο, η δυνατότητα εκτέλεσης πολύ μικρών αλλά και πολύ μεγάλων συναλλαγών με πολύ μικρό κόστος και η δυνατότητα

συμμετοχής στην έκδοση νομίσματος (mining).

## B.1 Τύποι κρυπτονομισμάτων

Σε κάποια blockchains (όπως το Ethereum) χρησιμοποιείται ένας τύπος κρυπτονομισμάτων, τα tokens.

- Τα tokens είναι μια υποκατηγορία κρυπτονομίσματος που έχουν φτιαχτεί μέσα σε ένα blockchain.
- Αντιπροσωπεύουν μια αξία ή ένα περιουσιακό στοιχείο σε ένα blockchain.
- Κάθε συναλλαγή με token καταγράφεται στο blockchain και δίνει στους αγοραστές απόδειξη γνησιότητας και ιδιοκτησίας.

Μπορούμε να αναγνωρίσουμε τουλάχιστον τέσσερις τύπους tokens, ανάλογα με τον σχεδιασμό του κώδικά τους, την εφαρμογή ή την περίπτωση χρήσης τους. Οι τέσσερις κύριοι τύποι περιλαμβάνουν χρησιμότητα (utility tokens), πληρωμή (payment tokens), ασφάλεια (security tokens) και σταθερά νομίσματα (stablecoins). Υπάρχουν επίσης Exchange Tokens, DeFi Tokens, NFT (Non fungible tokens) και tokens που υποστηρίζονται από περιουσιακά στοιχεία (asset-backed). Από όλα τα κρυπτονομίσματα, τα πιο κοινά είναι τα utility και τα payment tokens<sup>1</sup>.

### Utility Tokens

Τα utility tokens μεταφράζονται καλύτερα ως “κουπόνια”, αλλά ουσιαστικά είναι ψηφιακές μονάδες που αντιπροσωπεύουν μια αξία στο blockchain. Με άλλα λόγια, το token παρέχει συγκεκριμένη πρόσβαση σε ένα προϊόν ή υπηρεσία που διαχειρίζεται ή λειτουργεί ο εκδότης του token. Ένας χρήστης, έχοντας στην κατοχή του ένα αντίστοιχο token, μπορεί να το εξαργυρώσει για μια καθορισμένη αξία πρόσβασης (defined access value) στο προϊόν ή την υπηρεσία. Να σημειωθεί ότι τα utility tokens δεν είναι επενδυτικά προϊόντα και μπορούν να χάσουν εντελώς την αξία τους σε βάρος του κατόχου. Αυτό που αντιπροσωπεύουν είναι προκαθορισμένο και υφίσταται μόνο στο blockchain στο οποίο έχει δημιουργηθεί το token. Οι εφαρμογές περιλαμβάνουν πρόσβαση σε αποκεντρωμένη αποθήκευση, χρηματική ανταμοιβή και ανταλλαγή με νομίσματα στο αντίστοιχο blockchain. Παραδείγματα utility token αποτελούν τα Funfair, Basic Attention Token, Brickblock, Timicoin, Sirin Labs Token και Golem.

---

<sup>1</sup>Software Testing Help, <https://www.softwaretestinghelp.com/>

## Security Tokens

Πρόκειται είναι χρηματοοικονομικά μέσα που αντιπροσωπεύουν συμφέροντα ιδιοκτησίας, δηλαδή για κρυπτονομίσματα που αντλούν αξία από ένα εξωτερικό περιουσιακό στοιχείο και έχουν ως απώτερο σκοπό την παροχή ασφάλειας, βάσει ενός χρηματοοικονομικού κανονισμού. Ως εκ τούτου, χρησιμοποιούνται για τιτλοποιημένο (securitized) συμβολισμό ακινήτων, ομολόγων, μετοχών και νομισμάτων του πραγματικού κόσμου (Di Angelo et al, 2020).

είναι χρηματοοικονομικά μέσα που αντιπροσωπεύουν συμφέροντα ιδιοκτησίας σε ένα περιουσιακό στοιχείο – μόνο που έχουν δημιουργηθεί ψηφιακά (τοκενοποιημένα) για να ξεκλειδώσουν τη δύναμη του blockchain. Τα παραδοσιακά περιουσιακά στοιχεία κάνουν δημοφιλείς χρήσεις για χρεόγραφα με διακριτικά.

Επομένως, λόγω της φύσης των συναλλαγών, η ανταλλαγή, η έκδοση, η αξία, οι πληρωμές, η υποστήριξη και η διαπραγμάτευση πρέπει να ελέγχονται και να διεκπεραιώνονται από χρηματοοικονομικές ρυθμιστικές αρχές για την προστασία των επενδύσεων των χρηστών. Ο κανονισμός, σε μια τέτοια περίπτωση, υπάρχει για να εγγυάται τα κεφάλαια και τις επενδύσεις των χρηστών και να καθιστά υπεύθυνους τους ιδρυτές (Di Angelo et al, 2020).

Τα security tokens μπορούν επίσης να αντιπροσωπεύουν ένα μερίδιο σε μετοχές ή σε κάποιο κεφάλαιο, δικαιώματα ψήφου και δικαίωμα στο μέρισμα στο περιουσιακό στοιχείο που αντιπροσωπεύεται. Χρησιμοποιούνται αποκλειστικά σε περιπτώσεις κατά τις οποίες οι επενδυτές χρειάζονται άμεσο διακανονισμό, διαφάνεια στη διαχείριση και διαχωρισμό σε περιουσιακά στοιχεία.

## Payment Tokens

Όπως υποδηλώνει το όνομα, τα payment tokens είναι αυτά που χρησιμοποιούνται για την αγορά και πώληση αγαθών και υπηρεσιών σε ψηφιακές πλατφόρμες χωρίς μεσάζοντα. Φυσικά, η πλειονότητα των κρυπτονομισμάτων εντάσσεται σε αυτήν την κατηγορία, είτε πρόκειται για ασφάλεια (security tokens) είτε για χρησιμότητα (utility tokens). Σε αντίθεση με τα security tokens, τα payment tokens δεν αντιπροσωπεύουν περιουσιακά στοιχεία και δεν μπορούν να χρησιμοποιηθούν για επενδύσεις. Τα πιο γνωστά παραδείγματα token πληρωμής είναι το Bitcoin και το Ethereum.

## Stable Coins

Όπως υποδηλώνει το όνομά τους, πρόκειται για coins μιας σταθερής αξίας. Είναι προγραμματισμένα με τέτοιο τρόπο ώστε η αξία τους να είναι προβλέψιμη, με την έννοια ότι

δεν μπορεί να μεταβάλλεται. Τα stablecoins όπως ονομάζονται κυρίως, υποστηρίζονται από ένα σταθερό ή αρκετά σταθερό σε αξία περιουσιακό στοιχείο ή νόμισμα fiat<sup>2</sup>. Έτσι, έχουμε σταθερά νομίσματα των οποίων η αξία κυμαίνεται σε αυτήν του δολαρίου.

Τα stable coins βοηθούν τους χρήστες του blockchain να προφυλαχτούν από την αστάθεια στα περιουσιακά στοιχεία ή στα ψηφιακά νομίσματα.

Όσον αφορά τον προγραμματισμό τους, το περιουσιακό στοιχείο που τα υποστηρίζει πρέπει να διατηρείται σε μεγάλα αποθέματα σύμφωνα με την προκαθορισμένη αναλογία. Στην κορυφή των stable tokens, βρίσκεται το Tether, το οποίο υποστηρίζεται σε αναλογία 1:1 με το δολάριο. Υπάρχουν πολλά ακόμη ίδιας φύσης νομίσματα, όπως το TruSD, το Gemi Dollar και το USD Coin, τα οποία υποστηρίζονται από χρυσό.

### **Exchange Tokens**

Αυτό το είδος των tokens αντιπροσωπεύει ένα ψηφιακό περιουσιακό στοιχείο που υφίσταται στα ανταλλακτήρια κρυπτονομισμάτων, τα οποία είναι διαδικτυακά marketplaces για αγοραπωλησίες κρυπτονομισμάτων και ανταλλαγή tokens.

Παρόλο που μπορούν να χρησιμοποιηθούν εκτός των εγγενών (native) περιβαλλόντων ανταλλαγής τους, χρησιμοποιούνται κυρίως για τη διευκόλυνση ανταλλαγής μεταξύ άλλων tokens. Τα exchange tokens μπορούν να εκδοθούν και από κεντρικά ανταλλακτήρια με ή χωρίς αποκεντρωμένες πλατφόρμες. Συνήθως τα χρηματιστήρια τα χρησιμοποιούν για να παρασύρουν τους χρήστες να συμμετάσχουν σε μεγάλα έργα ή projects, με απώτερο σκοπό την αύξηση της ρευστότητας (liquidity).

Κάποια από τα μεγαλύτερα exchange tokens είναι τα BNB, Gemini, FTX και CRO.

### **Non-fungible Tokens (NFT)**

Πρόκειται για μια μορφή token που χρησιμοποιείται στο Ethereum blockchain. Ο όρος Non-Fungible σημαίνει ότι το token δεν μπορεί να ανταλλαχθεί με κάτι παρόμοιας αξίας, άρα είναι εξ ορισμού μοναδικό (PTTL, 2021). Ένα NFT δηλαδή, αντιπροσωπεύει μια συγκεκριμένη αξία και έναν μοναδικό κάτοχο. Αξίες σαν το bitcoin είναι fungible, με την έννοια ότι όλα τα κρυπτονομίσματα (πχ τα BTC, ETH) είναι ίδια και, άρα, ανταλλάξιμα μεταξύ τους.

---

<sup>2</sup>Ο όρος Fiat ή νόμισμα Fiat (Fiat money) αναφέρεται σε ένα νόμισμα που εκδίδεται από την κυβέρνηση και δεν υποστηρίζεται από ένα φυσικό εμπόρευμα, όπως ο χρυσός ή το ασήμι, αλλά από την κυβέρνηση που το εξέδωσε. Είναι δηλαδή χρήματα που ελέγχονται από την κυβέρνηση, όπως το δολάριο ΗΠΑ και άλλα εθνικά νομίσματα.<https://www.investopedia.com/terms/f/fiatmoney.asp>

Ένα NFT, όπως και κάθε token, έχει τη δική του διεύθυνση, κάτι που το καθιστά μοναδικό και μπορεί να αντιστοιχεί σε κάτι συγκεκριμένο (υλικό ή ψηφιακό), όπως ένα έργο τέχνης, ένα τραγούδι, ένα αυτοκίνητο κ.ά. Το NFT ισχύει μόνο για το συγκεκριμένο αντικείμενο ενώ δεν γίνεται δύο NFT να αντιστοιχούν στο ίδιο αντικείμενο. Επειδή τα NFT «ζουν» στο blockchain, μπορούν να εξαργυρωθούν με κρυπτονομίσματα. Τα NFTs δηλαδή, μπορούν να αγοραστούν, να πωληθούν ή να μεταβιβαστούν.

Αν ένα NFT αντιστοιχεί σε κάτι υλικό, ο κάτοχός του μπορεί να το ανταλλάξει με το αντικείμενο, ενώ αν αντιστοιχεί σε κάτι ψηφιακό, ο κάτοχος του NFT είναι και ο μοναδικός ιδιοκτήτης του αντικειμένου.

Οι αγορές NFT υπάρχουν εντός του blockchain, το οποίο απαιτεί την αγορά κρυπτονομισμάτων. Αυτό σημαίνει ότι το για να αγοράσει κάποιος ένα NFT θα χρειαστεί ένα νόμισμα αντίστοιχο με το blockchain στο οποίο «ζει» το NFT. Υπάρχουν αρκετές αγορές NFT αλλά οι μεγαλύτερες είναι οι OpenSea<sup>3</sup>, Bitski<sup>4</sup> και KnownOrigin<sup>5</sup>.

Τα NFTs βρίσκουν ιδιαίτερη εφαρμογή στην αγορά έργων τέχνης. Η φύση τους τα καθιστά κατάλληλα για την αγορά έργων τέχνης, αφού μπορούν να εξασφαλίσουν την αντιστοίχιση ενός έργου τέχνης με έναν μοναδικό ιδιοκτήτη, κάτι που επιτρέπει την διάκριση ενός πρωτότυπου ψηφιακού έργου από τα αντίγραφα του. Αυτό για παράδειγμα επιτρέπει την κατοχή μιας πρωτότυπης ψηφιακής φωτογραφίας -και όχι ενός αντιγράφου που μπορεί κάποιος να κατεβάσει από το internet και να την αποθηκεύσει στον Η/Υ του- και ταυτόχρονα την απόδειξη γνησιότητας και μοναδικότητας. Σε ότι αφορά τα πνευματικά δικαιώματα, ο δημιουργός του έργου παραμένει ο ιδιοκτήτης του (εκτός αν τα έχει παραχωρήσει στον αγοραστή).

Η δημιουργία ενός NFT για κάποιο έργο τέχνης, χρειάζεται ένα Crypto wallet (ψηφιακό πορτοφόλι)<sup>6</sup>, ένα Ethereum Cryptocurrency (Eth, “Ξ”) και ένα Marketplace (πλατφόρμα αγοροπωλησίας)

## DeFi Tokens

Η αποκεντρωμένη χρηματοδότηση (DeFi - Decentralized Finance) αναφέρεται σε οικονομικές εφαρμογές ή dApps που έχουν δημιουργηθεί στο blockchain. Κάθε εφαρμογή DeFi τρο-

---

<sup>3</sup>Opensea NFT market: <https://opensea.io/>

<sup>4</sup>Bitski: <https://bitski.com>

<sup>5</sup>KnownOrigin: <https://knownorigin.io/>

<sup>6</sup>Υπάρχουν τεσσάρων ειδών wallets: Hardware wallet (NanoX), Desktop wallet (Atomic), Mobile wallet (Trust Wallet), Web wallets (Metamask)

φοδοτείται από μια οικονομία γεμάτη tokens, πίσω από την οποία υπάρχει ένα εγγενές (native) token (Amler et al, 2021). Τα DeFi tokens είναι μια μορφή προγραμματιζόμενων χρημάτων, στην οποία οι προγραμματιστές μπορούν να προγραμματίσουν και να ρυθμίσουν τη λογική όσον αφορά τις πληρωμές και τις ροές των συναλλαγών. Μέσω αυτών των tokens, οι κάτοχοι μπορούν να κερδίζουν, να δανείζουν ή να δανείζονται, να αποθηκεύουν ή να επενδύουν μέρος του κεφαλαίου τους.

Τα περισσότερα από τα DeFi tokens βασίζονται επί του παρόντος στο Ethereum Blockchain, το οποίο υποστηρίζει την αποκεντρωμένη χρηματοδότηση με περισσότερη ασφάλεια από ότι οι ανταγωνιστές του (Stellar, Polygon κ.κ.).

Το πιο ισχυρό χαρακτηριστικό των DeFi tokens, είναι η σύνδεσή τους με τα έξυπνα συμβόλαια (smart contracts). Τα τελευταία, είναι ψηφιακά προγράμματα που επιτρέπουν στον δημιουργό τους να ορίζει κανόνες και προϋποθέσεις που πρέπει να πληρούνται ώστε να διεκπεραιώνονται οι συναλλαγές.

Στις διάφορες κατηγορίες εφαρμογών DeFi περιλαμβάνονται αποκεντρωμένες εφαρμογές δανεισμού, αποκεντρωμένα χρηματιστήρια, αποκεντρωμένη κοινή χρήση αποθηκευτικού χώρου, κ.ά. Οι πιο γνωστές εφαρμογές αυτής της κατηγορίας είναι οι Solana, Chainlink, Uniswap, Polkadot και Aave.

## B.2 Επιρροή και αντίκτυπος των κρυπτονομισμάτων

Όσον αφορά τον αντίκτυπο των κρυπτονομισμάτων στην οικονομία, παρόλο που οι όγκοι συναλλαγών και οι αξίες των κρυπτονομισμάτων αυξάνονται συνεχώς, δεν μπορεί να ειπωθεί ότι επί του παρόντος έχουν μεγάλη επίδραση στις νομισματικές πολιτικές. Αυτό συμβαίνει διότι η χρήση τους εξακολουθεί να βρίσκεται σε πολύ χαμηλά επίπεδα, λόγω της πολυπλοκότητας της τεχνολογίας που στέκεται εμπόδιο μεταξύ αυτών και του αγοραστικού κοινού. Σύμφωνα με τους Srokosz et al (2015), για να φτάσουν τα κρυπτονομίσματα στον όγκο που θα επηρεάσει τις χρηματοπιστωτικές αγορές, πρέπει να χρησιμοποιούνται ως υποκατάστατο του επίσημου νομίσματος.

Ένας τομέας που προτιμούνται τα κρυπτονομίσματα από το κοινό, είναι ο χώρος των οικονομικών επενδύσεων. Τεχνολογικά από τη φύση τους, τα κρυπτονομίσματα αποσκοπούν στη διασφάλιση ότι οι συναλλαγές μπορούν να πραγματοποιούνται χωρίς την ανάγκη διμεσολαβητικών αρχών ή ιδρυμάτων εκκαθάρισης, χάρη στην κρυπτογράφηση και στην τεχνολογία

δικτύου peer-to-peer. Επιπλέον, τα χρηματοοικονομικά περιουσιακά στοιχεία που αποκτώνται με κρυπτονομίσματα δεν μπορούν να αγοραστούν από παραδοσιακά ιδρύματα χρησιμοποιώντας το εγγενές (native) νόμισμα. Παρόλα αυτά, το γεγονός ότι τα κρυπτονομίσματα μπορούν να φορολογηθούν είναι πραγματικά ένα μεγάλο βήμα για το οικοσύστημα των blockchain, διότι με αυτόν τον τρόπο ένας απλός χρήστης που δεν κατανοεί σε βάθος την τεχνολογία, μπορεί να επενδύσει με ασφάλεια σε κρυπτονομίσματα υπό την εγγύηση της κυβέρνησης (Solodan et al, 2019).

Η σχέση μεταξύ των κρυπτονομισμάτων και της παραδοσιακής οικονομίας είναι ορατή σε πολλούς τομείς, παρόλο που ο αντίκτυπος είναι μικρός. Για παράδειγμα, η εκπαίδευση είναι ένας τομέας όπου η πιθανή χρήση της τεχνολογίας κρυπτονομισμάτων αυξάνεται ραγδαία. Πρόσφατα, ορισμένα πανεπιστήμια στην Κύπρο, την Ελβετία, τις ΗΠΑ και τη Γερμανία δέχονται κρυπτονομίσματα ως δίδακτρα εκπαίδευσης στους ιστότοπούς τους και ορισμένα δι-αδικτυακά εκπαιδευτικά ιδρύματα λαμβάνουν πληρωμές μέσω Bitcoin. Αρκετές ταξιδιωτικές επιχειρήσεις επιτρέπουν επίσης τη χρήση κρυπτονομισμάτων, καθώς η δυνατότητα αγοράς αεροπορικών εισιτηρίων, κρατήσεων ξενοδοχείων, ενοικιάσεων αυτοκινήτων και κρουαζιέρων με αυτά τα χρήματα επιταχύνει βοηθά στην αύξηση της κίνησης και των συναλλαγών (Fedorova et al, 2020).

Ο τομέας της στέγασης και των ακινήτων είναι ένας άλλος τομέας όπου τα κρυπτονομίσματα αρχίζουν να χρησιμοποιούνται ολοένα και περισσότερο. Με την αύξηση του αριθμού των εταιρειών που δέχονται πληρωμές με κρυπτονομίσματα, πιστεύεται ότι οι επενδύσεις σε αυτόν τον τομέα θα αυξηθούν. Ένα ακόμα παράδειγμα αποδοχής κρυπτονομισμάτων είναι το λιανικό εμπόριο, το οποίο αποτελεί προφανώς έναν πολύ κρίσιμο πεδίο αξιοποίησης της τεχνολογίας των κρυπτονομισμάτων. Το πρώτο παράδειγμα αξιοποίησης στο πεδίο αυτό, ήταν η ιστοσελίδα Overstock.com, η οποία παρέχει υπηρεσίες στον τομέα των επίπλων, δεχόμενη Bitcoin ως μέσο πληρωμής. Μετά από αυτό, αρκετές πύλες λιανικής πώλησης, συμπεριλαμβανομένων μεγάλων εμπόρων λιανικής όπως οι Crate and Barrel, Nordstrom και Whole Foods, ξεκίνησαν επίσης να προσφέρουν την ευκαιρία αγοράς προϊόντων με κρυπτονομίσματα (Chakrabarti et al, 2017).

Τέλος, τα κρυπτονομίσματα έχουν δημιουργήσει νέες δυνατότητες για εκδότες και προγραμματιστές παιχνιδιών. Ορισμένα διαδικτυακά παιχνίδια έχουν ήδη ξεκινήσει να δέχονται κρυπτονομίσματα. Ένα χαρακτηριστικό παράδειγμα αυτής της πρακτικής είναι το Project Big ORB, ένα παιχνίδι που επιτρέπει τους συμμετέχοντες να μετατρέψουν τα χρήματά τους μέσα στο παιχνίδι σε άλλα περιουσιακά στοιχεία, συμπεριλαμβανομένων άλλων κρυπτονομισμάτων,

και στη συνέχεια να τα ανταλλάζουν με πραγματικά νομίσματα.

Ενώ η εισαγωγή των κρυπτονομισμάτων στην κοινωνία είναι σχετικά νέα, ο οικονομικός αντίκτυπος του Bitcoin και άλλων νομισμάτων είναι ήδη σημαντικός, καθώς μέσα σε λίγα χρόνια απο την ίδρυσή του bitcoin, δημιουργήθηκε μια επιτυχημένη εναλλακτική λύση στο παγκόσμιο χρηματοπιστωτικό σύστημα. Κανείς δε μπορεί ακόμη να πει με βεβαιότητα εάν η αυξανόμενη δυναμική των κρυπτονομισμάτων μπορεί να ωφελήσει ή να βλάψει ολόκληρο το χρηματοπιστωτικό σύστημα και αν μπορεί πραγματικά να επηρεάσει την ισορροπία που επικρατεί μεταξύ των παγκόσμιων δυνάμεων στον τομέα της οικονομίας. Είναι ωστόσο σίγουρο, ότι η επιβράδυνση της επέκτασης των κρυπτονομισμάτων είναι προς το παρόν αδιανόητη. Από την άλλη πλευρά, η ολοένα και πιο διαδεδομένη χρήση τους, από μεμονωμένους πολίτες μέχρι κυβερνήσεις σε όλο τον κόσμο, θα συνεισφέρει στην πρόοδο της αποκεντρωμένης οικονομίας, καθιστώντας τα κρυπτονομίσματα μια ακόμα μεγαλύτερη και ευεργετική για την κοινωνία τεχνολογία.

### **B.3 Τα σημαντικότερα κρυπτονομίσματα**

Στην εικόνα 2.1, παρουσιάζονται τα δέκα σημαντικότερα κρυπτονομίσματα με βάση την κεφαλαιοποίηση αγοράς τους.

| Cryptocurrencies ▾ Exchanges ▾ Watchlist |                                                                                               |        |                   |             |
|------------------------------------------|-----------------------------------------------------------------------------------------------|--------|-------------------|-------------|
| Rank                                     | Name                                                                                          | Symbol | Market Cap        | Price       |
| 1                                        |  Bitcoin     | BTC    | \$333,590,658,558 | \$17,322.03 |
| 2                                        |  Ethereum    | ETH    | \$163,017,263,975 | \$1,332.12  |
| 3                                        |  Tether      | USDT   | \$66,271,433,350  | \$0.9999    |
| 4                                        |  BNB         | BNB    | \$44,061,863,966  | \$275.45    |
| 5                                        |  USD Coin    | USDC   | \$43,937,592,527  | \$0.9999    |
| 6                                        |  XRP         | XRP    | \$17,701,748,609  | \$0.3497    |
| 7                                        |  Binance USD | BUSD   | \$16,347,206,064  | \$1.00      |
| 8                                        |  Cardano     | ADA    | \$11,007,016,908  | \$0.3188    |
| 9                                        |  Dogecoin    | DOGE   | \$10,149,189,291  | \$0.0765    |
| 10                                       |  Polygon   | MATIC  | \$7,393,256,590   | \$0.8465    |

**Σχήμα Β.4:** Κεφαλαιοποίηση σημαντικότερων κρυπτονομισμάτων (Πηγή: CoinMarketCap, <https://coinmarketcap.com/all/views/all/> , 10/1/2023)

## B.4 Bitcoin vs Ethereum

Αυτή τη στιγμή, το Bitcoin (BTC) και το Ethereum (ETH) είναι τα πιο δημοφιλή κρυπτονομίσματα στον κόσμο. Και τα δυο έχουν καταφέρει να συγκεντρώσουν και να υποστηρίξουν ψηφιακά περιουσιακά στοιχεία πολλών δισεκατομμυρίων δολαρίων (βλ. παρακάτω, MarketCap) με αποτέλεσμα να γίνονται ανταγωνιστικά προς τα παραδοσιακά οικονομικά συστήματα. Η συζήτηση για το πιο από τα δύο υπερτερεί έναντι του άλλου, διχάζει την κοινότητα και τους οπαδούς της τεχνολογίας του Blockchain. Η απάντηση είναι περίπλοκη, καθώς τα δυο αυτά κρυπτονομίσματα όσο και να μοιάζουν φαινομενικά στη φιλοσοφία τους, διαφέρουν κατά πολύ.

### Ομοιότητες

Αρχικά, σύμφωνα με το CoinMarketCap, το Bitcoin και το Ethereum πρωταγωνιστούν όσον αφορά την κεφαλαιοποίηση της αγοράς, τους κατόχους πορτοφολιών (wallets) και τον όγκο συναλλαγών.

Όπως προαναφέρθηκε και τα δυο έχουν αποκεντρωμένο χαρακτήρα, που σημαίνει ότι δεν τα ελέγχει, ούτε και τα διαχειρίζεται κάποια κεντρική αρχή όπως η κυβέρνηση. Και τα δύο έχουν τις δικές τους αποκεντρωμένες αλυσίδες block με εγγενή (native) κρυπτονομίσματα, παρέχοντας υπηρεσίες κρυπτογραφικού πορτοφολιού για ψηφιακή αποθήκευση και χρησιμοποιώντας hashes και κρυπτογραφία για την εξασφάλιση της διαφάνειας και της ασφάλειας των συναλλαγών.

### **Διαφορές**

Εκτός από τη λειτουργία σε αποκεντρωμένες αλυσίδες block, τη χρήση open source λογισμικού, την κρυπτογράφηση και τα εγγενή νομίσματα, το Bitcoin και το Ethereum διαφέρουν σημαντικά ως προς τη λειτουργικότητα.

**Use Cases:** Το Bitcoin ως νόμισμα, εστιάζει αποκλειστικά στο να είναι η κυρίαρχη μορφή χρημάτων, ενώ δεν διαθέτει την πρόσθετη λειτουργικότητα έξυπνων συμβολαίων και tokens που υπάρχουν στο Ethereum.

Ενώ και τα δύο δίκτυα επιτρέπουν στους προγραμματιστές να χτίσουν πάνω τους αξιολογώντας τις αλυσίδες block για αποθήκευση δεδομένων, στο Ethereum, οι προγραμματιστές εφαρμογών μπορούν να δημιουργήσουν τα δικά τους tokens για χρήση στις εφαρμογές τους. Αυτά περιλαμβάνουν “πρότυπα” (“standards”), όπως τα ERC-20 και ERC-721, τα οποία χαρακτηρίζουν το είδος και την μορφή των tokens όπως τα DAI, τα UNI και τα NFT αντίστοιχα.

Όπως προαναφέρθηκε, το Ethereum επιτρέπει προγραμματισμό έξυπνων συμβολαίων. Οι προγραμματιστές προγραμματίζουν αυτές τις εφαρμογές με τρόπο ώστε να χρησιμοποιούν το Ethereum σαν έναν παγκόσμιο υπολογιστή, προγραμματίζοντας συμβόλαια που εκτελούνται αυτόματα χωρίς ένα κεντρικό μέρος ή έναν διαχειριστή. Αυτό επιτρέπει πολλές ασύγχρονες περιπτώσεις χρήσης που προηγουμένως απαιτούσαν κεντρικούς μεσάζοντες.

Οι υποστηρικτές του Bitcoin ισχυρίζονται ότι όλη αυτή η επιπλέον λειτουργικότητα είναι περιττή και μειώνει την πραγματική καινοτομία των κρυπτονομισμάτων ως «καλύτερων χρημάτων», ενώ θέτουν σε κίνδυνο και την ακεραιότητα του blockchain. Απο την άλλη πλευρά, οι υποστηρικτές του Ethereum θεωρούν πως το δίκτυο τους, είναι κάτι πολύ παραπάνω από ένα ανταλλακτήριο και ότι μπορεί να συνεισφέρει σε πολλούς τομείς τόσο σήμερα όσο και στο μέλλον.

**MarketCap:** Η κεφαλαιοποίηση αγοράς (Market Capitalization)<sup>7</sup> είναι μια μέτρηση που χρησιμοποιείται για να αξιολογήσει πόσο δημοφιλές ή πολύτιμο είναι ένα κρυπτονομίσμα στην αγορά κρυπτονομισμάτων. Αφορά την συνολική αξία (αγοράς) των κρυπτονομισμάτων που κυκλοφορούν, και προκύπτει από τον πολλαπλασιασμό της τρέχουσας τιμής ενός κρυπτονομίσματος επί τον αριθμό των συνολικών νομισμάτων που βρίσκονται σε κυκλοφορία παγκοσμίως.

Κατά τη στιγμή συγγραφής αυτής της έρευνας, το όγκος κεφαλαίου του Bitcoin ήταν περίπου 324 δισεκατομμύρια δολάρια, με περισσότερα από 19 εκατομμύρια νομίσματα σε κυκλοφορία, ενώ του Ethereum είναι περίπου 152 δισεκατομμύρια δολάρια, με σχεδόν 122 εκατομμύρια Ether σε παγκόσμια κυκλοφορία <sup>8</sup>.

**Issuance:** Η έκδοση (Issuance) αναφέρεται στη δημιουργία νέων νομισμάτων. Για την έκδοση κρυπτονομισμάτων χρησιμοποιούνται διάφορες μέθοδοι, ανάλογα με τις συνθήκες και τα πρωτόκολλα που περιγράφονται από τον προγραμματιστή ενός κρυπτονομίσματος.

Τοσο το Bitcoin, όσο και το Ethereum ανταμείβουν τους συμμετέχοντες στο ίδιο τους το νόμισμα, για την εγγύηση της ασφάλειας του δικτύου. Ωστόσο, το ποσό που λαμβάνουν οι χρήστες και το αν κάποιο ποσό κρυπτονομίσματος καταστρέφεται ή όχι, διαφέρει. Στο Bitcoin, οι miners λαμβάνουν ένα σταθερό ποσό για κάθε block. Αυτό το ποσό μειώνεται στο μισό περίπου κάθε τέσσερα χρόνια, οδηγώντας σε μέγιστη δυνητική προσφορά 21 εκατομμυρίων.

Μέχρι πρόσφατα, το μοντέλο έκδοσης του Ethereum ήταν πιο περίπλοκο, με την ανταμοιβή ανά επαλήθευση να διαφέρει ανάλογα με τις μαθηματικές εξισώσεις που χρειάζονταν για την εξόρυξη ενός καινούργιου block. Το Ethereum καίει (burn) ή καταστρέφει επίσης μέρος του νομίσματός του σε κάθε συναλλαγή μετά από μια πρόσφατη αναβάθμιση.

**Consensus Mechanism:** Ο μηχανισμός συναίνεσης είναι μια διαδικασία που διασφαλίζει ότι όλοι οι peers σε ένα blockchain «παραμένουν ειλικρινείς» με τις ενέργειες επικύρωσης κατά την επαλήθευση των συναλλαγών. Πλέον το Bitcoin χρησιμοποιεί το PoW (Proof of Work), ενώ το Ethereum χρησιμοποιεί το PoS (Proof of Stake) (Βλ. παρακάτω, 3.1.9). Η κύρια διαφορά σε αυτούς τους μηχανισμούς είναι ότι το Proof of Stake (POS) χρησιμοποιεί τυχαία επιλεγμένους επικυρωτές για την επιβεβαίωση συναλλαγών και τη δημιουργία νέων

---

<sup>7</sup>Κεφαλαιοποίηση αγοράς (Market Capitalization): η συνολική δηλαδή αξία των μεριδίων και των μετοχών μιας εταιρίας

<sup>8</sup>CoinMarketCap, <https://coinmarketcap.com/all/views/all/>

block, ενώ το Proof of Work (POW) χρησιμοποιεί μια ανταγωνιστική μέθοδο επικύρωσης για την επιβεβαίωση συναλλαγών και την προσθήκη νέων block στο blockchain. Αξίζει να σημειωθεί ότι το PoW καταναλώνει εξαιρετικά μεγάλη ποσότητα ηλεκτρικής ενέργειας. Μετά από έρευνες τον Ιούνιο του 2021 από ειδικούς, οι εκτιμήσεις ανεβάζουν την κατανάλωση ενέργειας Bitcoin σε 110 Terrawatt ώρες ετησίως, παρόμοια με την κατανάλωση ενέργειας στην Ολλανδία (111TWh) (Sedlmeir et al, 2020).

**Decentralization:** Η αποκέντρωση εξαλείφει την επίβλεψη μιας κεντρικής αρχής ή ενός μεσάζοντα. Επομένως δεν υπάρχει οντότητα που να ρυθμίζει ή να διαχειρίζεται το blockchain και τις ενέργειες των χρηστών του. Παρόλο που το Bitcoin και το Ethereum λειτουργούν και τα δύο σε αποκεντρωμένες αλυσίδες block, ορισμένοι ισχυρίζονται ότι το Bitcoin είναι περισσότερο αποκεντρωμένο από το Ethereum, κυρίως λόγω της εισβολής DAO στο blockchain του Ethereum το 2016<sup>9</sup>.

---

<sup>9</sup>Μια από τις πρώτες μεγάλες εφαρμογές στο Ethereum με το όνομα "The DAO", συγκέντρωσε 150 εκατομμύρια δολάρια σε ETH μέσω μιας πώλησης που προοριζόταν να διαρκέσει 28 ημέρες. Ωστόσο, το DAO παραβιάστηκε λόγω των σφαλμάτων στον πηγαίο κώδικα, με τον hacker να κλέβει περισσότερο από το ένα τρίτο των κεφαλαίων (Ghaleb et al, 2018).

## Κεφάλαιο C

# Ethereum Blockchain

Το Ethereum Blockchain παρουσιάστηκε πρώτη φορά από τον Vitalik Buterin (2014) και είχε ως στόχο να αντιμετωπίσει αρκετούς περιορισμούς στον προγραμματισμό του Bitcoin. Τα κύρια σημεία τα οποία έθιξε, ήταν η πληρότητα Turing (Turing completeness), που σημαίνει ότι το Ethereum υποστηρίζει όλους τους τύπους υπολογισμών, συμπεριλαμβανομένων των βρόχων (loops). Επίσης, το Ethereum υποστηρίζει την κατάσταση των συναλλαγών (transaction state), καθώς και αρκετές άλλες βελτιώσεις στη δομή του blockchain.

Το Ethereum αντιπροσωπεύει ένα blockchain με μια ενσωματωμένη γλώσσα προγραμματισμού που είναι “Turing complete”. Παρέχει ένα αφηρημένο επίπεδο που επιτρέπει σε οποιονδήποτε να δημιουργήσει τους δικούς του κανόνες για την ιδιοκτησία, τις μορφές συναλλαγών και τις συναρτήσεις μετάβασης κατάστασης (state transition functions). Αυτό γίνεται με τη χρήση των smart contracts, ενός συνόλου κρυπτογραφικών κανόνων που εκτελούνται μόνο εάν πληρούνται ορισμένες προϋποθέσεις (Buterin, 2014).

Η συναίνεση στο δίκτυο Ethereum βασίζεται στο τροποποιημένο πρωτόκολλο GHOST (Greedy Heaviest Observed Subtree) (Sompolinsky et al, 2015). Δημιουργήθηκε για να αντιμετωπίσει το ζήτημα των stale<sup>1</sup> block στο δίκτυο. Τα stale blocks μπορεί να προκύψουν εάν μια ομάδα από miners έχει μεγαλύτερη υπολογιστική ισχύ από τις άλλες, πράγμα που σημαίνει ότι τα block από την πρώτη ομάδα θα συνεισφέρουν περισσότερο στο δίκτυο, δημιουργώντας έτσι το ζήτημα της συγκέντρωσης (centralization issue). Το πρωτόκολλο GHOST περιλαμβάνει αυτά τα stale blocks στους υπολογισμούς της μεγαλύτερης αλυσίδας. Το πρόβλημα

---

<sup>1</sup>Τα “μπαγιάτικα” block είναι καλά διαμορφωμένα block που δεν αποτελούν πλέον μέρος της μεγαλύτερης (από άποψη πολυπλοκότητας) και της επικρατούσας αλυσίδας block

συγκέντρωσης εξαλείφεται μέσω της παροχής ανταμοιβών ακόμα και στα stale blocks, όπου αυτά ανταμείβονται το 87,5% της ανταμοιβής, ενώ τα υπόλοιπα που ακολουθούν λαμβάνουν το υπόλοιπο 12,5%. Με αυτόν τον τρόπο, οι miners εξακολουθούν να ανταμείβονται ακόμη και αν το block τους δεν έγινε μέρος του κύριου blockchain (αυτά τα block ονομάζονται uncle blocks) (Buterin, 2014).

## C.1 Πως λειτουργεί το Ethereum

### C.1.1 Δίκτυο Ethereum

Το Ethereum Blockchain είναι παρόμοιο με το Bitcoin Blockchain. Η κύρια διαφορά είναι ότι τα block Ethereum δεν περιέχουν μόνο τον αριθμό block, τη δυσκολία, το nonce<sup>2</sup>, κ.λπ., αλλά και τη λίστα συναλλαγών και την πιο πρόσφατη κατάσταση. Για κάθε συναλλαγή στη λίστα συναλλαγών, η νέα κατάσταση δημιουργείται εφαρμόζοντας την προηγούμενη κατάσταση. Το Block Header στο Ethereum Blockchain αποτελείται από το Keccak 256-bit hash του header του parent block, τη διεύθυνση του παραλήπτη του τέλους εξόρυξης, hashes των ριζών κατάστασης του block, τις συναλλαγές, τη δυσκολία εξόρυξης του block, το gas limit του block -έναν αριθμό που αντιπροσωπεύει το συνολικό gas που χρησιμοποιήθηκε για όλες τις συναλλαγές στο block-, τη χρονική σήμανση, το nonce και πολλά επιπλέον hashes για σκοπούς επαλήθευσης (Wood, 2014).

Σε κάθε κόμβο στο δίκτυο Ethereum λειτουργεί το EVM (Ethereum Virtual Machine)<sup>3</sup>. Τα έξυπνα συμβόλαια μεταφράζονται σε κώδικα EVM και στη συνέχεια εκτελούνται από τους κόμβους (Wood, 2014). Μία από τις πιο δημοφιλείς γλώσσες προγραμματισμού για τη σύνταξη έξυπνων συμβολαίων είναι η Solidity.

Σύμφωνα με το Etherscan (February 16, 2023), ο χρόνος δημιουργίας νέων block στο Ethereum είναι περίπου 12 δευτερόλεπτα, ωστόσο ορισμένες φορές καθυστερεί έως και 30 δευτερόλεπτα. Χρησιμοποιώντας το blockchain Client “Geth” με γρήγορο συγχρονισμό, το μέγεθος της αλυσίδας block Ethereum είναι 881,53841 GB.

Αν και υπάρχουν ανησυχίες σχετικά με την επεκτασιμότητα του Ethereum, υπάρχουν

---

<sup>2</sup>το nonce ενός λογαριασμού είναι ένας μετρητής που δείχνει το πλήθος συναλλαγών που αποστέλλονται από αυτόν τον λογαριασμό. Για να είναι έγκυρη μια συναλλαγή, το nonce της πρέπει να είναι ίσο με το nonce του λογαριασμού του αποστολέα.

<sup>3</sup>Όλο το δίκτυο του Ethereum χαρακτηρίζεται και

καταγραφές ότι το δίκτυο Ethereum διαχειρίστηκε με επιτυχία περισσότερες από ένα εκατομμύριο μοναδικές συναλλαγές σε 24 ώρες, με μέσο όρο περίπου 11 συναλλαγές ανά δευτερόλεπτο (Filiba, 2017). Πλέον, η έκδοση “Serenity” της πλατφόρμας Ethereum -γνωστή και ως Ethereum 2.0- που βασίζεται στον αλγόριθμο συναίνεσης Casper, επέτρεψε τη μετάβαση στο proof-of-stake consensus mechanism, κατά το οποίο η ανταμοιβή δίνεται στους miners, όχι με βάση τους υπολογισμούς τους, αλλά στο αποθεματικό νομισμάτων τους -όσα περισσότερα νομίσματα έχει ο χρήστης, τόσο μεγαλύτερο είναι και το κέρδος ανταμοιβής-. (Silva, 2018).

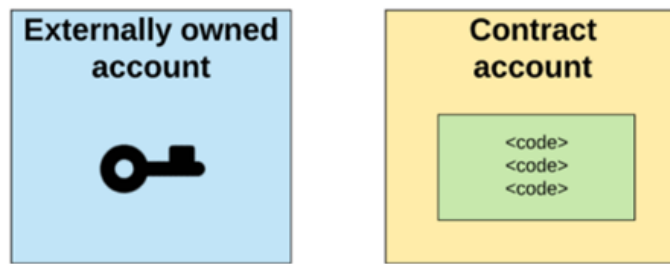
Οι πιθανές χρήσεις του Ethereum περιλαμβάνουν token systems, χρηματοοικονομικά παράγωγα, συστήματα ταυτότητας και φήμης (reputation), αποθήκευση αρχείων, ασφάλιση, υπολογιστικό νέφος, κ.λπ. (Buterin, 2014). Η πιο σημαντική περίπτωση χρήσης του Ethereum είναι οι αποκεντρωμένες εφαρμογές (Dapps), οι οποίες θα αναλυθούν στη συνέχεια.

### C.1.2 Λογαριασμοί

Η παγκόσμια “κοινή κατάσταση” (mutual state) του Ethereum αποτελείται από πολλούς λογαριασμούς που είναι σε θέση να αλληλεπιδρούν μεταξύ τους μέσω ενός πλαισίου διέλευσης μηνυμάτων (message passing framework). Κάθε λογαριασμός έχει μια κατάσταση (state) που σχετίζεται με αυτόν και μια διεύθυνση μεγέθους 20 byte. Μια διεύθυνση στο Ethereum έχει ένα αναγνωριστικό μεγέθους 160 bit που χρησιμοποιείται για την αναγνώριση οποιουδήποτε λογαριασμού.

Υπάρχουν δύο τύποι λογαριασμών:

- Λογαριασμοί εξωτερικής ιδιοκτησίας (Externally Owned Accounts), οι οποίοι ελέγχονται με ιδιωτικά κλειδιά και δεν έχουν κανένα κώδικα που να σχετίζεται με αυτά.
- Λογαριασμοί συμβολαίων (Contract Accounts), οι οποίοι ελέγχονται από τον κώδικα συμβολαίου τους και έχουν κώδικα που σχετίζεται με αυτά.



**Σχήμα C.5:** *Ethereum Accounts (Kasireddy, 2017)*

Είναι σημαντικό να γίνει κατανοητή μια θεμελιώδης διαφορά μεταξύ αυτών των δυο τύπων λογαριασμών. Ένας externally owned account μπορεί να στέλνει μηνύματα σε άλλους λογαριασμούς ίδιου τύπου ή ακόμα και σε contract accounts, δημιουργώντας και υπογράφοντας μια συναλλαγή χρησιμοποιώντας το ιδιωτικό του κλειδί. Ένα μήνυμα μεταξύ δύο externally owned accounts είναι απλώς μια μεταφορά αξίας. Ωστόσο, ένα μήνυμα από ένα externally owned account σε ένα contract account ενεργοποιεί τον κώδικα του contract account, επιτρέποντάς του να εκτελεί διάφορες ενέργειες (π.χ. μεταφορά tokens, εγγραφή σε εσωτερικό χώρο αποθήκευσης, δημιουργία νέων συμβολαίων κ.λπ.).

Από την άλλη πλευρά, τα contract accounts δεν μπορούν να ξεκινήσουν από μόνα τους νέες συναλλαγές. Εξαιτίας του προγραμματισμού τους, μπορούν να ενεργοποιούνται και να εκτελούν συναλλαγές μόνο ως απόκριση σε άλλες συναλλαγές που έχουν λάβει -από λογαριασμό εξωτερικού ή από άλλο λογαριασμό συμβολαίου-. Επομένως, οποιαδήποτε ενέργεια λαμβάνει χώρα στο blockchain Ethereum τίθεται πάντα σε κίνηση από συναλλαγές που ενεργοποιούνται από εξωτερικά ελεγχόμενους λογαριασμούς (Kasireddy, 2017).

### **C.1.3 Δημιουργία συμβολαίων**

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, στο Ethereum υπάρχουν δύο τύποι λογαριασμών: contract accounts and externally owned accounts. Όταν λέμε ότι ένα transaction αποσκοπεί στη δημιουργία ενός contract, εννοούμε ότι ο σκοπός της συναλλαγής είναι η δημιουργία ενός νέου contract account. Για να δημιουργηθεί έναν νέο contract account, απαιτείται αρχικά η δήλωση της διεύθυνσης του νέου λογαριασμού χρησιμοποιώντας μια ειδική φόρμουλα-εξίσωση. Στη συνέχεια η αρχικοποίηση του νέου λογαριασμού γίνεται ως εξής:

- Ο μετρητής του nonce ρυθμίζεται στο μηδέν
- Εάν ο αποστολέας έστειλε κάποια ποσότητα Ether με τη συναλλαγή, το υπόλοιπο του λογαριασμού ορίζεται σε αυτήν την τιμή
- Η αξία που προστίθεται στο υπόλοιπο αυτού του νέου λογαριασμού, αφαιρείται από το υπόλοιπο του αποστολέα
- Ο αποθηκευτικός χώρος (storage) ορίζεται ως κενός
- Το codeHash του contract παίρνει τη μορφή του hash ενός κενού string.

Εφόσον τα κριτήρια πληρούνται, μπορεί να δημιουργηθεί το νέο account, χρησιμοποιώντας τον πηγαίο κώδικα που αποστέλλεται με τη συναλλαγή (βλ. παρακάτω 3.1.4). Αυτό που συμβαίνει κατά την εκτέλεση αυτού του αρχικού κώδικα ποικίλλει. Ο προγραμματιστής του συμβολαίου μπορεί να ενημερώσει το χώρο αποθήκευσης του λογαριασμού, να δημιουργήσει άλλους λογαριασμούς συμβολαίου κ.λπ. Καθώς εκτελείται ο κώδικας για την προετοιμασία ενός contract, χρησιμοποιείται gas<sup>4</sup>. Η συναλλαγή δεν επιτρέπεται να καταναλώνει περισσότερο gas από το υπολειπόμενο. Εάν συμβεί αυτό, η εκτέλεση θα εμφανίσει ένα out-of-gas (OOG) exception και θα τερματίσει. Στην περίπτωση αυτή, η κατάσταση επανέρχεται στο σημείο αμέσως πριν από τη συναλλαγή και το gas που ξοδεύτηκε από τον αποστολέα δεν επιστρέφεται πίσω. Ωστόσο, εάν ο αποστολέας έστειλε οποιαδήποτε τιμή Ether με τη συναλλαγή, αυτό θα επιστραφεί ακόμη και αν η δημιουργία του συμβολαίου αποτύχει.

Στην περίπτωση που ο κώδικας εκκίνησης εκτελεστεί με επιτυχία, καταβάλλεται ένα τελικό κόστος δημιουργίας του συμβολαίου. Αυτό είναι ένα κόστος αποθήκευσης και είναι ανάλογο με το μέγεθος του κώδικα του contract που δημιουργήθηκε. Εάν δεν απομένει αρκετό gas για την πληρωμή αυτού του τελικού κόστους, τότε η συναλλαγή δηλώνει ξανά το out-of-gas exception και ματαιώνεται.

Τέλος, αν όλες οι συνθήκες πληρούνται, τότε το τυχόν αχρησιμοποίητο gas που έχει απομείνει επιστρέφεται στον αρχικό αποστολέα της συναλλαγής και η τροποποιημένη κατάσταση επιτρέπεται πλέον να εκτελεστεί.

---

<sup>4</sup>Μία μορφή φόρου (βλ. παρακάτω C.1.5)

### C.1.4 Συναλλαγές και μηνύματα

Σημειώσαμε προηγουμένως ότι το Ethereum είναι ένα δίκτυο του οποίου η κατάσταση μεταβάλλεται ανάλογα με τις συναλλαγές. Με την πιο βασική έννοια, μια συναλλαγή είναι ένα κρυπτογραφικά υπογεγραμμένο κομμάτι εντολής που δημιουργείται από έναν εξωτερικό λογαριασμό που ανήκει στο blockchain, η οποία πραγματοποιείται σειριακά και στη συνέχεια υποβάλλεται στο blockchain.

Υπάρχουν δύο τύποι συναλλαγών: κλήσεις μηνυμάτων και δημιουργίες συμβολαίων (δηλαδή συναλλαγές που δημιουργούν νέα συμβόλαια Ethereum). Σύμφωνα με τον δημιουργό του Ethereum, (Buterin, 2014) όλες οι συναλλαγές περιέχουν τα ακόλουθα στοιχεία, ανεξάρτητα από τον τύπο τους:

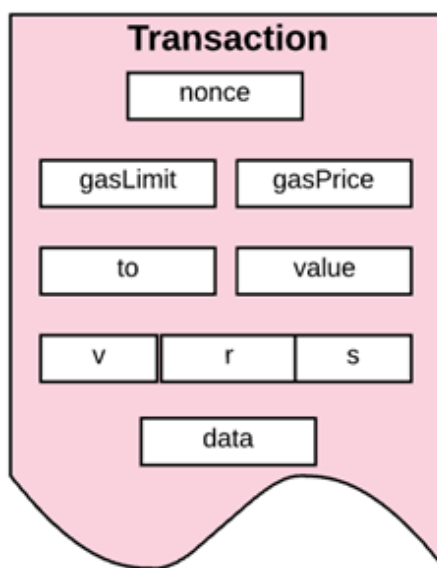
- **nonce:** ο αριθμός συναλλαγής, μια καταμέτρηση του αριθμού των συναλλαγών που αποστέλλονται από τον αποστολέα.
- **gasPrice:**<sup>5</sup> ο αριθμός Wei που είναι διατεθειμένος να πληρώσει ο αποστολέας ανά μονάδα Ether που απαιτείται για την εκτέλεση της συναλλαγής.
- **gasLimit:** η μέγιστη ποσότητα gas που είναι διατεθειμένος να πληρώσει ο αποστολέας για την εκτέλεση αυτής της συναλλαγής. Αυτό το ποσό ορίζεται και καταβάλλεται εκ των προτέρων, πριν γίνει οποιοσδήποτε υπολογισμός.
- **to:** η διεύθυνση του παραλήπτη. Σε μια συναλλαγή δημιουργίας συμβολαίου, η διεύθυνση του λογαριασμού του συμβολαίου δεν υπάρχει ακόμη και επομένως χρησιμοποιείται μια κενή τιμή.
- **value:** το ποσό του Wei που θα μεταφερθεί από τον αποστολέα στον παραλήπτη. Σε μια συναλλαγή για τη δημιουργία συμβολαίου, αυτή η τιμή χρησιμεύει ως το αρχικό υπόλοιπο στον νέο λογαριασμό συμβολαίου.
- **v, r, s:** χρησιμοποιείται για τη δημιουργία της υπογραφής που προσδιορίζει τον αποστολέα της συναλλαγής.
- **init** (υπάρχει μόνο για συναλλαγές που δημιουργούν συμβόλαια): Ένα τμήμα κώδικα EVM που χρησιμοποιείται για την προετοιμασία του νέου λογαριασμού συμβολαίου. Το init εκτελείται μόνο μία φορά και, στη συνέχεια, απορρίπτεται. Όταν το init εκτελείται

---

<sup>5</sup>Το “Wei” είναι η μικρότερη μονάδα του Ether, όπου το Wei είναι  $10^{-18}$  ETH

για πρώτη φορά, επιστρέφει το κύριο μέρος από τον κώδικα του contract, το οποίο σχετίζεται μόνιμα με τον contract account.

- **data** (προαιρετικό πεδίο που υπάρχει μόνο για message calls): τα δεδομένα εισόδου (δηλαδή οι παράμετροι) της κλήσης μηνυμάτων. Για παράδειγμα, εάν ένα έξυπνο συμβόλαιο χρησιμεύει ως υπηρεσία καταχώρισης domain, μια κλήση σε αυτό το συμβόλαιο ενδέχεται να περιμένει πεδία εισαγωγής όπως ο τομέας και η διεύθυνση IP.



**Σχήμα C.6:** *Ethereum Transaction (Kasireddy, 2017)*

Όπως αναφέρθηκε νωρίτερα στην ενότητα C.1.2, οι συναλλαγές -τόσο οι κλήσεις μηνυμάτων όσο και οι συναλλαγές που δημιουργούν συμβόλαια- πραγματοποιούνται πάντα από εξωτερικούς λογαριασμούς και υποβάλλονται στο blockchain. Υπό μια άλλη έννοια, οι συναλλαγές είναι αυτές που γεφυρώνουν τον εξωτερικό κόσμο με την εσωτερική κατάσταση του Ethereum (Vujičić et al, 2018). Ωστόσο, αυτό δεν σημαίνει ότι τα συμβόλαια δεν μπορούν να “επικοινωνήσουν” με άλλα συμβόλαια. Τα συμβόλαια που υπάρχουν εντός του παγκόσμιου εύρους της κατάστασης του Ethereum μπορούν να συνομιλούν με άλλα συμβόλαια εντός του ίδιου πεδίου. Ο τρόπος με τον οποίο το κάνουν αυτό είναι μέσω “μηνυμάτων” ή “εσωτερικών συναλλαγών” σε άλλα συμβόλαια. Αυτά τα μηνύματα ή οι εσωτερικές συναλλαγές είναι παρόμοια με τις κανονικές συναλλαγές, με τη βασική διαφορά ότι δεν δημιουργούνται από externally owned accounts. Αντίθετα, δημιουργούνται από τα συμβόλαια. Όταν ένα συμβόλαιο αποσ-

τέλλει μια εσωτερική συναλλαγή σε άλλο συμβόλαιο, εκτελείται ο συσχετισμένος κωδικός που υπάρχει στο contract account του παραλήπτη.

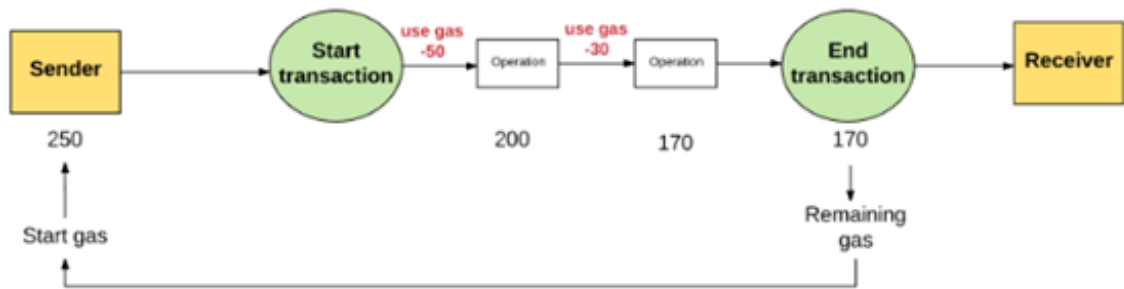
### C.1.5 Gas

Μια πολύ σημαντική έννοια στο Ethereum είναι η έννοια των φόρων (fees). Κάθε υπολογισμός που προκύπτει ως αποτέλεσμα μιας συναλλαγής στο δίκτυο Ethereum, επιβαρύνεται με μια χρέωση. Αυτό το τέλος καταβάλλεται σε μια ονομαστική αξία που ονομάζεται “αέριο” (gas). Το gas είναι η μονάδα που χρησιμοποιείται για τη μέτρηση των τελών που απαιτούνται για έναν συγκεκριμένο υπολογισμό. Η τιμή του gas (Gas price) είναι η ποσότητα του Ether που ένας αποστολέας είναι διατεθειμένος να ξοδέψει σε κάθε μονάδα gas και μετριέται σε “gwei”. Το “Wei” είναι η μικρότερη μονάδα του Ether, όπου το  $10^{18}$  Wei αντιπροσωπεύει 1 Ether. Ένα gwei είναι 1.000.000.000 Wei. Με κάθε συναλλαγή, ένας αποστολέας ορίζει ένα όριο αερίου (gas limit) και την τιμή του αερίου (gas price). Το γινόμενο gas price και του gas limit αντιπροσωπεύει το μέγιστο ποσό Wei που είναι διατεθειμένος να πληρώσει ο αποστολέας για την εκτέλεση μιας συναλλαγής (Buterin, 2014). Για παράδειγμα, υποθέτοντας ότι ένας αποστολέας θέτει το gas limit σε 50.000 gwei και το gas price στα 20 gwei, αυτός είναι διατεθειμένος να ξοδέψει το πολύ  $50.000 \times 20 \text{ gwei} = 1.000.000.000.000.000 \text{ Wei} = 0,001 \text{ Ether}$  για να εκτελέσει αυτήν τη συναλλαγή.

|                            |          |                             |          |                                           |
|----------------------------|----------|-----------------------------|----------|-------------------------------------------|
| Gas Limit<br><b>50,000</b> | <b>X</b> | Gas Price<br><b>20 gwei</b> | <b>=</b> | Max transaction fee<br><b>0.001 Ether</b> |
|----------------------------|----------|-----------------------------|----------|-------------------------------------------|

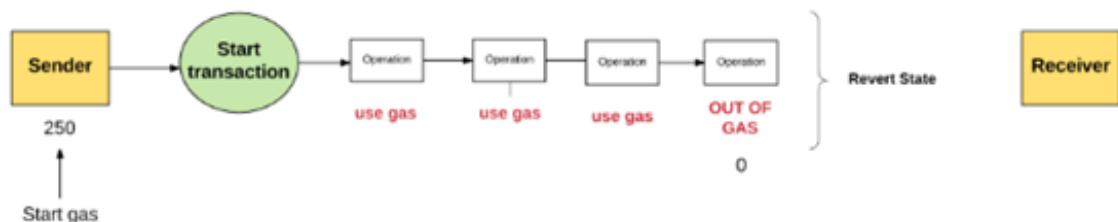
Σχήμα C.7: Gas calculation (Kasireddy, 2017)

Δεδομένου ότι το gas limit αντιπροσωπεύει το μέγιστο gas στο οποίο ο αποστολέας είναι διατεθειμένος να ξοδέψει χρήματα. Εάν υπάρχει αρκετό Ether στο υπόλοιπο του λογαριασμού του για να καλύψει αυτό το μέγιστο, μπορεί να προχωρήσει με τη συναλλαγή. Ταυτόχρονα, στον αποστολέα επιστρέφεται το αχρησιμοποίητο gas στο τέλος της συναλλαγής, και αντλλάσσεται στην αρχική τιμή Ether.



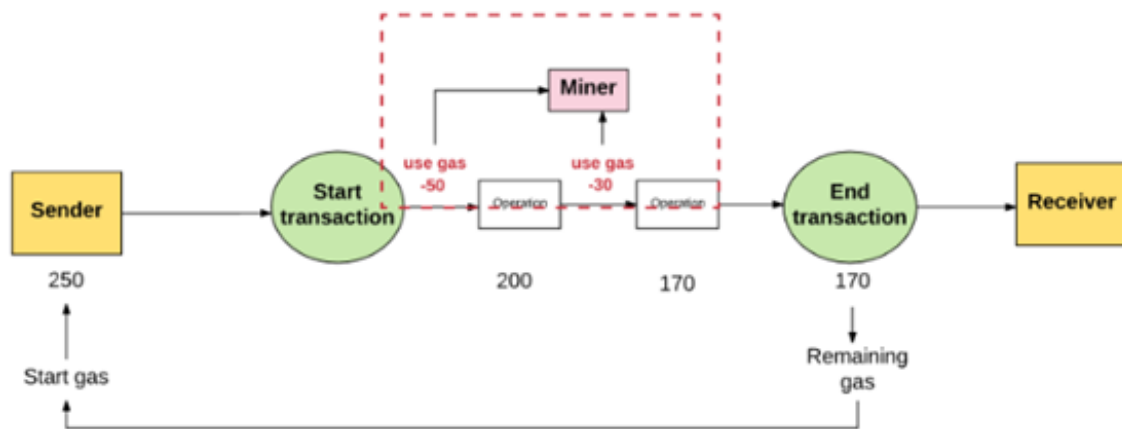
Σχήμα C.8: Gas calculation (Kasireddy, 2017)

Σε περίπτωση που ο αποστολέας δεν διαθέτει το απαραίτητο gas για την εκτέλεση της συναλλαγής, η συναλλαγή ακυρώνεται. Σε αυτήν την περίπτωση, η επεξεργασία των συναλλαγών ματαιώνεται και τυχόν αλλαγές κατάστασης που συνέβησαν αντιστρέφονται, έτσι ώστε η τελική κατάσταση του Ethereum να παραμείνει αμετάβλητη. Επιπλέον, καταγράφεται ένα αρχείο αποτυχίας της συναλλαγής, το οποίο δείχνει ποια συναλλαγή επιχειρήθηκε και πού απέτυχε. Όπως είναι επίσης φυσικό, έχει ήδη καταβληθεί προσπάθεια για την εκτέλεση των υπολογισμών πριν τελειώσει το gas, οπότε δεν επιστρέφεται gas στον αποστολέα.



Σχήμα C.9: Gas calculation (Kasireddy, 2017)

Μια συχνή απορία είναι που καταλήγουν όλα τα χρήματα σε μορφή gas όταν χάνονται. Όλα τα χρήματα που ξοδεύονται για gas από τον αποστολέα, αποστέλλονται στη διεύθυνση του «δικαιούχου», η οποία είναι συνήθως η διεύθυνση του miner. Δεδομένου ότι οι miners καταβάλλουν την προσπάθεια για την εκτέλεση υπολογισμών και την επικύρωση συναλλαγών, είναι και αυτοί που λαμβάνουν το gas ως ανταμοιβή.



**Σχήμα C.10:** *Gas calculation (Kasireddy, 2017)*

Συνήθως, όσο υψηλότερο είναι το gas price που είναι διατεθειμένος να πληρώσει ο αποστολέας, τόσο μεγαλύτερη είναι η αξία που αντλεί ο miner από τη συναλλαγή. Έτσι, όπως είναι φυσικό, ο ανταγωνισμός επικύρωσης συναλλαγών υψηλής αξίας είναι αυξημένος. Με αυτόν τον τρόπο, οι miners είναι ελεύθεροι να επιλέξουν ποιες συναλλαγές θέλουν να επικυρώσουν ή να αγνοήσουν. Προκειμένου να καθοδηγήσουν τους αποστολείς σχετικά με το ποσό του gas price που θα ορίσουν, οι miners έχουν τη δυνατότητα να διαφημίσουν το ελάχιστο gas price για το οποίο θα εκτελέσουν συναλλαγές.

### C.1.6 Εξόρυξη

Ένα πολύ σημαντικός μηχανισμός όχι μόνο του Ethereum, αλλά όλων των blockchain, είναι το mining. Το mining είναι η διαδικασία δημιουργίας ενός νέου block συναλλαγών που στη συνέχεια θα προστεθεί στο εκάστοτε blockchain αφότου πρώτα επικυρωθεί. Για την επιτυχή εξόρυξη ενός νέου block, χρησιμοποιούνται διάφοροι μηχανισμοί συναίνεσης, όπως το PoW, PoS κ.α. Συγκεκριμένα, το Ethereum έκανε πρόσφατα τη μετάβασή του στο Proof of Stake, και χρησιμοποιεί αυτήν την αρχιτεκτονική για την επικύρωση των νέων block που προστίθενται στην αλυσίδα (Siim, 2017).

Ο όρος mining προέρχεται από τη διαδικασία εξόρυξης χρυσού, και ταιριάζει απόλυτα με τα κρυπτονομίσματα, για τον λόγο ότι αυτά είναι σπάνια, όπως ο χρυσός και τα υπόλοιπα πολύτιμα μέταλλα, και ο μόνος τρόπος για να αυξηθεί ο συνολικός όγκος τους είναι μέσω της

εξόρυξης. Στο Ethereum που μέχρι πρόσφατα δούλευε με το proof-of-work, ο μόνος τρόπος έκδοσης ήταν μέσω εξόρυξης. Ωστόσο, σε αντίθεση με τον χρυσό ή τα πολύτιμα μέταλλα, η εξόρυξη Ethereum ήταν επίσης ο τρόπος για να ασφαλιστεί το δίκτυο δημιουργώντας, επαληθεύοντας, δημοσιεύοντας και διαδίδοντας καινούργια blocks στην αλυσίδα. Ουσιαστικά, η εξόρυξη του Ether συνδέεται άρρηκτα με την ασφάλιση του δικτύου του Ethereum. Η εξόρυξη είναι η κινητήρια δύναμη του κάθε blockchain που λειτουργεί με τον μηχανισμό του Proof-of-Work. Οι miners του Ethereum, οι οποίοι είναι απλά χρήστες που εκτελούν λογισμικό από τον υπολογιστή τους, χρησιμοποιούσαν το χρόνο και την υπολογιστική τους ισχύ για να επεξεργαστούν συναλλαγές και να δημιουργήσουν blocks, μέχρι και την μετάβαση στο μηχανισμό του Proof-of-Stake (Siim, 2017).

Όπως έχει προαναφερθεί, σε αποκεντρωμένα συστήματα όπως το Ethereum, πρέπει να διασφαλίζεται ότι όλοι οι κόμβοι συμφωνούν για τη σειρά και την εγκυρότητα των συναλλαγών. Οι miners συνεισφέρουν σε αυτό λύνοντας υπολογιστικά δύσκολους γρίφους για την παραγωγή block, προστατεύοντας το δίκτυο από επιθέσεις.

Το Ethereum, όντας ένα peer-to-peer δίκτυο, επέτρεπε σε όλους τους συμμετέχοντες τη δυνατότητα εξόρυξης. Ωστόσο, δεν ήταν εφικτό σε όλους να εξορύξουν Ether επικερδώς. Αυτό οφείλεται στο γεγονός ότι το mining επέφερε μεγάλη οικονομική επιβάρυνση στον χρήστη. Στις περισσότερες περιπτώσεις, οι miners έπρεπε να αγοράσουν hardware για αποκλειστική χρήση και να έχουν πρόσβαση σε φθηνές πηγές ενέργειας. Ο μέσος υπολογιστής ήταν απίθανο να κερδίσει αρκετές ανταμοιβές από τα block για να καλύψει το σχετικό κόστος της εξόρυξης. Επιπλέον, ο miner επιβαρυνόταν με το κόστος του ηλεκτρικού ρεύματος για την τροφοδοσία του εξοπλισμού του, καθώς επίσης και για επιπλέον εξοπλισμό για την υποστήριξη εξόρυξης, όπως ο εξερισμός, η ψύξη, η παρακολούθηση ενέργειας, η ηλεκτρική καλωδίωση κ.ά. (Grunspan et al, 2020)

### C.1.7 Εκτέλεση συναλλαγών

Ένα από τα πιο βασικά αλλά ταυτόχρονα περίπλοκα μέρη του πρωτοκόλλου του Ethereum, είναι η εκτέλεση των συναλλαγών. Παρακάτω θα αναλυθεί το τι ακριβώς συμβαίνει με την κατάσταση του Ethereum και πως αυτή μεταβάλλεται, από τι στιγμή που μια συναλλαγή αποστέλλεται στο δίκτυο για επεξεργασία (Vujčić et al, 2018). Καταρχάς, όλες οι συναλλαγές πρέπει να πληρούν το παρακάτω αρχικό σύνολο απαιτήσεων για να εκτελεστούν.

- Η συναλλαγή πρέπει να είναι διαμορφωμένη σε μορφή RLP. Το RLP (Recursive Length

Prefix) είναι μια μορφή δεδομένων που χρειάζεται για την κωδικοποίηση δυαδικών δεδομένων (binary data) και χρησιμοποιείται από το Ethereum για τη σειριοποίηση αντικειμένων.

- Να υπάρχει έγκυρη υπογραφή συναλλαγής.
- Να υπάρχει μετρητής (nonce) έγκυρης συναλλαγής.
- Το gas limit της συναλλαγής πρέπει να είναι ίσο ή μεγαλύτερο από το gas που χρησιμοποιείται από τη συναλλαγή. Αυτό το “ενδογενές” gas περιλαμβάνει:
- προκαθορισμένο κόστος 21.000 gas για την εκτέλεση της συναλλαγής
- έναν “φόρο” gas για τα δεδομένα που αποστέλλονται με τη συναλλαγή (4 gas για κάθε byte των δεδομένων και 68 gas για κάθε μη μηδενικό byte δεδομένων.
- εάν η συναλλαγή είναι συναλλαγή που δημιουργεί ένα contract, απαιτείται πρόσθετο 32.000 gas.

$$\text{Intrinsic gas} = \begin{array}{|c|} \hline \text{Predefined gas fee} \\ \hline \mathbf{21,000} \\ \hline \end{array} + \begin{array}{|c|} \hline \text{Storage fee} \\ \hline \mathbf{4(X) + 68(Y)} \\ \hline \end{array} + \begin{array}{|c|} \hline \text{Contract creation} \\ \hline \mathbf{32,000} \\ \hline \end{array}$$

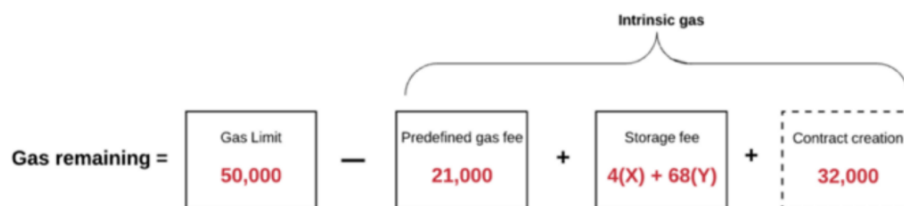
**Σχήμα C.11:** Gas calculation (Kasireddy, 2017)

Το υπόλοιπο του λογαριασμού του αποστολέα πρέπει να έχει αρκετό Ether για να καλύψει το «προκαταβολικό» κόστος gas που πρέπει να πληρώσει ο αποστολέας. Ο υπολογισμός για το αρχικό κόστος φυσικού αερίου είναι ο εξής: Πρώτον, το gas limit της συναλλαγής πολλαπλασιάζεται με την τιμή του gas της συναλλαγής για να προσδιοριστεί το μέγιστο κόστος του τελικού gas. Στη συνέχεια, αυτό το μέγιστο κόστος προστίθεται στη συνολική αξία που μεταφέρεται από τον αποστολέα στον παραλήπτη.

$$\text{Upfront cost} = \begin{array}{|c|} \hline \text{Gas Limit} \\ \hline \mathbf{50,000} \\ \hline \end{array} \times \begin{array}{|c|} \hline \text{Gas Price} \\ \hline \mathbf{20 \text{ gwei}} \\ \hline \end{array} + \begin{array}{|c|} \hline \text{Value} \\ \hline \mathbf{0.05 \text{ Ether}} \\ \hline \end{array}$$

**Σχήμα C.12:** Gas calculation (Kasireddy, 2017)

Εάν η συναλλαγή πληροί όλες τις παραπάνω απαιτήσεις εγκυρότητας, μεταβαίνει στο επόμενο στάδιο. Κατά αυτό, αφαιρείται το προκαταβολικό κόστος εκτέλεσης από το υπόλοιπο του αποστολέα και αυξάνεται το μηδενικό του λογαριασμού του κατά 1 για να λογιστικοποιηθεί (to account for) η τρέχουσα συναλλαγή. Σε αυτό το σημείο, υπολογίζεται το gas που απομένει ως το συνολικό gas limit για τη συναλλαγή μείον το ενδογενές αέριο που χρησιμοποιείται.



**Σχήμα C.13:** Gas calculation (Kasireddy, 2017)

Στη συνέχεια, η συναλλαγή αρχίζει να εκτελείται. Καθ' όλη τη διάρκεια της εκτέλεσης μιας συναλλαγής, το Ethereum παρακολουθεί την “υποκατάσταση”. Η υποκατάσταση είναι ένας τρόπος καταγραφής πληροφοριών που συγκεντρώθηκαν κατά τη διάρκεια της συναλλαγής και θα χρειαστούν αμέσως μετά την ολοκλήρωσή της. Συγκεκριμένα περιέχει (Kasireddy, 2017):

- Σετ αυτοκαταστροφής (Self-destruct set): ένα σύνολο λογαριασμών (εάν υπάρχουν) που θα απορριφθούν μετά την ολοκλήρωση της συναλλαγής.
- Σειρά καταγραφής (Log series): αρχειοθετημένα και ευρετηριάσιμα (indexable) σημεία ελέγχου της εκτέλεσης κώδικα της εικονικής μηχανής.
- Υπόλοιπο επιστροφής χρημάτων (Refund balance): το ποσό που πρέπει να επιστραφεί στον λογαριασμό αποστολέα μετά τη συναλλαγή <sup>6</sup>.

Στη συνέχεια, οι διάφοροι υπολογισμοί που απαιτούνται από τη συναλλαγή υποβάλλονται σε επεξεργασία. Μόλις ολοκληρωθούν όλα τα βήματα που απαιτούνται από τη συναλλαγή, και υποθέτοντας ότι δεν υπάρχει κάποιο σφάλμα, η κατάσταση καθορίζεται προσδιορίζοντας την ποσότητα του αχρησιμοποίητου gas που πρέπει να επιστραφεί στον αποστολέα. Εκτός από το αχρησιμοποίητο gas, στον αποστολέα επιστρέφεται και κάποιο επίδομα από το «υπόλοιπο επιστροφής χρημάτων» που περιγράφηκε προηγουμένως.

<sup>6</sup>Η αποθήκευση στο Ethereum κοστίζει χρήματα και βάση πρωτοκόλλου, ο αποστολέας αποζημιώνεται για την εκκαθάριση αποθηκευτικού χώρου. Το Ethereum παρακολουθεί όλες τις

Μόλις επιστραφούν τα χρήματα στον αποστολέα, το Ether για το gas δίνεται στον miner, το gas που χρησιμοποιείται από τη συναλλαγή προστίθεται στον μετρητή gas που έχει κάθε block -ο οποίος παρακολουθεί το συνολικό gas που χρησιμοποιείται από όλες τις συναλλαγές στο block και είναι χρήσιμο κατά την επικύρωση block- και διαγράφονται όλοι οι λογαριασμοί στο self-destruct set (αν υπάρχουν). Τέλος, απομένει η νέα κατάσταση και ένα σύνολο από τα αρχεία καταγραφής που δημιουργήθηκαν από τη συναλλαγή.

### C.1.8 Πορτοφόλια

Τα Crypto Wallets αναφέρονται σε ένα φυσικό μέσο, συσκευή, υπηρεσία ή εφαρμογή που διατηρεί public και private keys για συναλλαγές στο blockchain. Εκτός από τον βασικό σκοπό της αποθήκευσης κλειδιών, δίνουν τη δυνατότητα στον ιδιοκτήτη τους να παραμένει ανώνυμος (Moniruzzaman et al, 2020)

Τα Crypto Wallets υπάρχουν σε διάφορες μορφές υπό δυο κατηγορίες, Hardware και Software, που μπορεί να είναι συσκευές όπως το Ledger, που μοιάζει με USB stick, έως εφαρμογές σε κινητές συσκευές που επιτρέπουν την αγορά και την κατοχή ψηφιακών περιουσιακών στοιχείων, όπως κρυπτονομίσματα.

Όταν πρόκειται για κρυπτονομίσματα, η βασική διαφορά είναι ότι το ψηφιακό περιουσιακό στοιχείο στην πραγματικότητα δεν κατέχεται ποτέ από τον ιδιοκτήτη, αλλά παραμένει στο blockchain.

Ένα ψηφιακό πορτοφόλι, σε οποιαδήποτε μορφή, δεν αποθηκεύει τα νομίσματα, αλλά διατηρεί τα ιδιωτικά κλειδιά του χρήστη, τα οποία δημιουργούνται ταυτόχρονα με τους λογαριασμούς. Εφόσον δεν υπάρχει αντίγραφο ασφαλείας του ιδιωτικού κλειδιού σε διακομιστή, δεν μπορεί να ανακτηθεί εάν χαθεί. Στις περισσότερες περιπτώσεις αυτό είναι χρήσιμο, καθώς εάν ένα τρίτο μέλος αποκτήσει πρόσβαση στο ιδιωτικό κλειδί, αποκτά αυτόματα πρόσβαση σε όλους τους λογαριασμούς και τα περιουσιακά τους στοιχεία.

Κάθε ψηφιακό πορτοφόλι έχει επίσης ένα δημόσιο κλειδί, το οποίο είναι μια αλφαριθμητική auto-generated σειρά ψηφίων. Αυτό το κλειδί είναι μια διεύθυνση που θα εμφανίζεται μέσα στο blockchain κάθε φορά που θα διεκπεραιώνεται μια συναλλαγή. Το Public και Private key, μπορούν να παρομοιαστούν ως ένα email και ο κωδικός πρόσβασης αντίστοιχα (Moniruzzaman et al, 2020).

Υπάρχουν τεσσάρων ειδών wallets:

- Hardware wallet (ledger)
- Desktop wallet (Atomic)
- Mobile wallet (Trust Wallet)
- Web wallets (Metamask)

### C.1.9 Αλγόριθμοι συναίνεσης (Pow, PoS)

Όπως αναφέρθηκε νωρίτερα, δυο είναι οι κύριοι μηχανισμοί που έχουν χρησιμοποιηθεί στο Ethereum Blockchain:

- Proof-of-Work (PoW): Είναι μια μέθοδος επαλήθευσης συναλλαγών σε ένα blockchain στο οποίο ένας αλγόριθμος παρέχει ένα μαθηματικό πρόβλημα που πρέπει να λυθεί για να επαληθευτεί μια ομάδα συναλλαγών - που αναφέρεται ως block - (Ashford & Schmidt, 2020). Κάθε συμμετέχων υπολογιστής, ο οποίος αναφέρεται ως “μεταλλωρύχος” (miner), προσπαθεί να λύσει το πρόβλημα και, αν το καταφέρει, στη συνέχεια τις προσθέτει στο blockchain. Ο πρώτος υπολογιστής που το κάνει με επιτυχία ανταμείβεται με ένα μικρό ποσό κρυπτονομίσματος για τις προσπάθειές του. Η διαδικασία PoW απαιτεί μεγάλη ποσότητα ισχύος και ηλεκτρικής ενέργειας από τον υπολογιστή, η αξία της οποία μπορεί στην πράξη, να ξεπεράσει την αξία του κρυπτονομίσματος που λαμβάνουν οι miners για την επικύρωση των συναλλαγών, αν αφαιρεθεί το κόστος ισχύος και υπολογιστικών πόρων.
- Proof-of-Stake (PoS): Proof-of-stake: Για να μειωθεί η ποσότητα ενέργειας που απαιτείται για τον έλεγχο συναλλαγών, ορισμένα κρυπτονομίσματα χρησιμοποιούν μια μέθοδο επαλήθευσης που ονομάζεται proof-of-stake. Με αυτή τη μέθοδο, ο αριθμός των συναλλαγών που μπορεί να επαληθεύσει κάθε χρήστης, περιορίζεται από το ποσό του κρυπτονομίσματος που είναι διατεθειμένος να «ποντάρει» ή να κλειδώσει προσωρινά σε ένα κοινόχρηστο χρηματοκιβώτιο, για να έχει την ευκαιρία να συμμετάσχει στη διαδικασία. Κάθε χρήστης που «ποντάρει» κρυπτονομίσματα είναι επιλέξιμος για επαλήθευση συναλλαγών, αλλά οι πιθανότητες που έχει να επιλεγεί τελικά, να γίνει δηλαδή «επικυρωτής» (validator), αυξάνονται με το ποσό που «ποντάρει».

## C.2 Smart Contracts

Τα έξυπνα συμβόλαια (Smart Contracts) είναι απλά προγράμματα που δημιουργούνται και αποθηκεύονται στο blockchain και εκτελούνται όταν πληρούνται προκαθορισμένες προϋποθέσεις. Συνήθως χρησιμοποιούνται για την αυτοματοποίηση της εκτέλεσης μιας συμφωνίας, έτσι ώστε όλοι οι συμμετέχοντες να μπορούν να είναι αμέσως σίγουροι για το αποτέλεσμα, χωρίς την ανάμειξη κάποιου μεσάζοντα ή την απώλεια χρόνου. Τα έξυπνα συμβόλαια αυτοματοποιούν επίσης τη ροή εργασίας, ενεργοποιώντας με τη σειρά όλες τις εντολές, εφόσον πληρούνται οι προϋποθέσεις που έθεσε ο δημιουργός τους (Zheng et al, 2020).

Τα έξυπνα συμβόλαια λειτουργούν κυρίως ακολουθώντας απλές δηλώσεις «αν/όταν... τότε...», που είναι γραμμένες σε κώδικα με μια ειδική γλώσσα προγραμματισμού (βλ. παρακάτω). Από τη στιγμή που ένα smart contract εκτελεστεί, το blockchain ενημερώνεται όταν ολοκληρωθούν όλες οι συναλλαγές και αυτές παραμένουν για πάντα αμετάβλητες (Kolvar et al, 2016).

Μέσα σε ένα smart contract, μπορεί να υπάρχουν τόσες προϋποθέσεις όσες χρειάζονται για να ικανοποιηθούν οι συμμετέχοντες ότι η εργασία θα ολοκληρωθεί ικανοποιητικά. Για να καταλήξουν στους όρους, οι συμμετέχοντες πρέπει να καθορίσουν τον τρόπο με τον οποίο αντιπροσωπεύονται οι συναλλαγές και τα δεδομένα τους στο blockchain, να συμφωνήσουν στους κανόνες «αν/όταν...τότε...» που διέπουν αυτές τις συναλλαγές και να διερευνήσουν όλες τις πιθανές εξαιρέσεις.

Παραδοσιακά, το έξυπνο συμβόλαιο προγραμματίζεται από έναν ειδικό, αν και όλο και περισσότερο, οι οργανισμοί που χρησιμοποιούν blockchain για επιχειρήσεις, παρέχουν πρότυπα, διεπαφές ιστού (web interfaces) και άλλα διαδικτυακά εργαλεία για την απλοποίηση της δόμησης των έξυπνων συμβολαίων (Zheng et al, 2020).

Δεδομένων των δυνατοτήτων τους και των υπηρεσιών που προσφέρουν τα Smart Contracts, έχουν πολλά οφέλη έναντι των παραδοσιακών προγραμμάτων.

- Ταχύτητα, αποτελεσματικότητα και ακρίβεια: Μόλις εκπληρωθούν οι όροι ενός smart contract, αυτό εκτελείται αμέσως. Επειδή τα έξυπνα συμβόλαια είναι ψηφιακά και αυτοματοποιημένα, δεν υπάρχει καμία γραφειοκρατία για επεξεργασία και δεν δαπανάται χρόνος για τη συμφωνία σφαλμάτων που συχνά προκύπτουν από τη μη-αυτόματη συμπλήρωση εγγράφων.
- Εμπιστοσύνη και διαφάνεια: Επειδή δεν εμπλέκεται κανένα τρίτο μέρος και επειδή τα κρυπτογραφημένα αρχεία συναλλαγών μοιράζονται μεταξύ των συμμετεχόντων, δεν υπ-

άρχει λόγος να αμφισβητηθεί εάν οι πληροφορίες έχουν τροποποιηθεί για προσωπικό όφελος.

- Ασφάλεια: Τα αρχεία συναλλαγών στο Blockchain είναι κρυπτογραφημένα, γεγονός που το καθιστά πολύ δύσκολο να παραβιαστούν. Επιπλέον, επειδή κάθε εγγραφή συνδέεται με τις προηγούμενες και τις επόμενες εγγραφές σε ένα distributed ledger, οποιοσδήποτε με κακόβουλες προθέσεις, αναγκάζεται να αλλάξει ολόκληρη την αλυσίδα για να τροποποιήσει έστω και μία μόνο εγγραφή.
- Εξοικονόμηση πόρων: Τα έξυπνα συμβόλαια καταργούν την ανάγκη διαμεσολαβητών και, κατ' επέκταση, τις σχετικές χρονικές καθυστερήσεις και οικονομικές χρεώσεις.

### C.2.1 Τα δημοφιλέστερα smart contracts

Στην παρακάτω εικόνα παρουσιάζονται τα έντεκα πιο δημοφιλή Smart Contracts με βάση τους ενεργούς χρήστες Top Ethereum applications (OpenSea, Uniswap, DxDy, etc)

|    |                                                                                                            |              |           |                   |           |                                                                                       |
|----|------------------------------------------------------------------------------------------------------------|--------------|-----------|-------------------|-----------|---------------------------------------------------------------------------------------|
| 1  |  Uniswap V3             | Exchanges    | \$2.37B   | 30.75k<br>-13.29% | \$4.93B   |  |
| 2  |  Uniswap NFT Aggregator | Marketplaces | \$0       | 28.28k<br>-13.56% | \$206.69M |  |
| 3  |  Blur                   | Marketplaces | \$125.73M | 17.37k<br>-34.56% | \$68.4M   |  |
| 4  |  OpenSea                | Marketplaces | \$73.96k  | 17.25k<br>-3.25%  | \$9.79M   |  |
| 5  |  Uniswap V2             | Exchanges    | \$871.97M | 10.92k<br>-0.46%  | \$116.14M |  |
| 6  |  MetaMask Swap          | DeFi         | \$79.62M  | 7.55k<br>-14.36%  | \$7.25M   |  |
| 7  |  Tinch Network          | DeFi         | \$26.38k  | 6.01k<br>-3.12%   | \$239.47M |  |
| 8  |  Manifold               | Marketplaces | \$237.31k | 5.42k<br>+16.77%  | \$554.17k |  |
| 9  |  LIDO                   | DeFi         | \$399.82M | 3.37k<br>+877.68% | \$5.32M   |  |
| 10 |  Sushi                  | DeFi         | \$329.08M | 2.05k<br>-8.94%   | \$68.72M  |  |
| 11 |  Dx Protocol            | Exchanges    | \$18M     | 1.83k<br>-6.53%   | \$76.14M  |  |

Σχήμα C.14: Top Ethereum applications, Source: <https://dappradar.com/rankings/protocol/ethereum>

### C.3 Programming Smart Contracts in Ethereum

Ενώ τα περισσότερα έξυπνα συμβόλαια είναι χτισμένα στο Ethereum, υπάρχουν και άλλα blockchain που υποστηρίζουν έξυπνα συμβόλαια. Μερικά από τα πιο δημοφιλή είναι τα Solana (SOL), Polkadot (DOT), BNB Chain και άλλα. Ωστόσο, το Ethereum παραμένει η κυρίαρχη πλατφόρμα ανάπτυξης έξυπνων συμβολαίων.

Όπως έχει αναφερθεί προηγουμένως, από τη στιγμή που κάτι ενσωματωθεί στο blockchain παραμένει αμετάβλητο. Επιπλέον, λόγω της αρχιτεκτονικής του κατασκευής, κάθε φορά που ένα συμβόλαιο προγραμματίζεται, ή όταν προστίθεται στην αλυσίδα ένα καινούργιο block, χρησιμοποιείται gas. Για τους παραπάνω λόγους, σε συνδυασμό με το ότι το Blockchain και συγκεκριμένα το Ethereum είναι σχετικά καινούργια και πρωτοφανή, όλοι οι συμμετέχοντες -επενδυτές, προγραμματιστές κ.α.- δίνουν ιδιαίτερη προσοχή και μελέτη στις πράξεις τους, καθώς οποιοδήποτε λάθος μπορεί να τους κοστίσει. Όπως είναι φυσικό, δε θα ήταν καθόλου πρακτικό για κάποιον ενδιαφερόμενο να πειραματιστεί απευθείας στο Mainnet.

Εκτός από το Mainnet, υπάρχουν δημόσια δοκιμαστικά δίκτυα. Τα λεγόμενα testnets είναι δίκτυα που χρησιμοποιούνται από προγραμματιστές πρωτοκόλλων ή προγραμματιστές smart contracts για να δοκιμάσουν τόσο τις αναβαθμίσεις πρωτοκόλλων όσο και τις αποκεντρωμένες εφαρμογές τους, σε περιβάλλον παρόμοιο με το Mainnet. Καθώς ένας μεγάλος αριθμός των smart contracts αλληλεπιδρούν μεταξύ τους, τα περισσότερα μεγάλα έργα έχουν αντίγραφα που έχουν αναπτυχθεί σε δοκιμαστικά δίκτυα ακριβώς για λόγους testing.

Τα περισσότερα testnets ξεκίνησαν χρησιμοποιώντας το Proof-of-Authority, έναν διαφορετικό μηχανισμό συναίνεσης. Αυτό σημαίνει ότι επιλέγεται ένας μικρός αριθμός κόμβων για την επικύρωση των συναλλαγών και τη δημιουργία νέων μπλοκ - ποντάροντας την ταυτότητά τους στη διαδικασία. Εναλλακτικά, ορισμένα testnets διαθέτουν μια ελαφρώς παραποιημένη εκδοχή του Proof-of-Stake, όπου όλοι μπορούν να δοκιμάσουν την εκτέλεση ενός validator, όπως ακριβώς στο Ethereum Mainnet.

Το Ether στα δοκιμαστικά δίκτυα δεν έχει πραγματική αξία. Επομένως, δεν υπάρχουν αγορές για το testnet Ether. Δεδομένου ότι οποιοσδήποτε χρειάζεται ETH για να αλληλεπιδράσει πραγματικά με το Ethereum, υπάρχουν ειδικές εφαρμογές ιστού, τα faucets, που χτίστηκαν ειδικά για να δίνουν “ψεύτικα” νομίσματα, ώστε να μπορούν οι προγραμματιστές να αλληλεπιδρούν με τα testnets. Τα πιο δημοφιλή είναι τα Goerli, Sepolia και Rinkeby.

## Κεφάλαιο D

# Προγραμματισμός smart contract για αγοραπωλησία ακίνητης περιουσίας

Όπως αναφέρθηκε στο πρώτο κεφάλαιο (A.5), η τεχνολογία Blockchain έχει αμέτρητα πεδία εφαρμογής και αναμένεται να φέρει ριζικές αλλαγές στους περισσότερους επιστημονικούς τομείς. Με τη σωστή χρήση και ασφάλεια, καθίσταται ικανή να βελτιστοποιήσει τον τρόπο με τον οποίο λειτουργούν οι περισσότεροι βιομηχανικοί κλάδοι. Ένα παράδειγμα τέτοιου κλάδου αποτελεί το πεδίο αγοραπωλησίας ακινήτων (Real Estate Industry), το οποίο φαίνεται να μπορεί να εκμεταλλευτεί σε μέγιστο βαθμό τα χαρακτηριστικά και τα προτερήματα που παρέχει το δίκτυο Ethereum.

- Δυνατότητα των ακινήτων να μετατραπούν και να συναλλαχθούν ως tokens.
- Μειωμένο κόστος από την αυτοματοποίηση των διαδικασιών.
- Γρηγορότερες συναλλαγές λόγω έλλειψης γραφειοκρατίας.
- Πρόσβαση σε ευρύτερες ομάδες επενδυτών λόγω κλασματοποίησης ιδιοκτησίας.
- Προσβασιμότητα δεδομένων για αύξηση της διαφάνειας και εγκυρότητας.

Σε αυτό το κεφάλαιο, θα παρουσιαστεί ο προγραμματισμός ενός smart contract που έχει ως στόχο την αγοραπωλησία ακίνητης περιουσίας (Real Estate) στο Ethereum Blockchain,

χρησιμοποιώντας Ether. Για την υλοποίηση του προγράμματος, θα χρησιμοποιηθούν τα παρακάτω εργαλεία:

**Solidity:** Ειδική γλώσσα προγραμματισμού, προορισμένη για την κατασκευή smart contracts στο Ethereum Blockchain. Η Solidity είναι μια Object-oriented γλώσσα προγραμματισμού, παρόμοια με την Javascript.

**Metamask:** Ένα software cryptocurrency wallet που χρησιμοποιείται για την αλληλεπίδραση με το Ethereum Blockchain. Επιτρέπει στους χρήστες να έχουν πρόσβαση στο Ethereum wallet μέσω ενός browser extension ή ενός mobile app, το οποίο στη συνέχεια μπορεί να χρησιμοποιηθεί για αλληλεπίδραση με αποκεντρωμένες εφαρμογές.

**Hardhat:** Ένα περιβάλλον ανάπτυξης που βοηθά τους προγραμματιστές στη δοκιμή, τη μεταγλώττιση, την ανάπτυξη και τον εντοπισμό σφαλμάτων των εφαρμογών στο Ethereum.

**React:** Μια δωρεάν open-source βιβλιοθήκη της Javascript. Χρησιμοποιείται για το front-end κομμάτι των εφαρμογών. Αποσκοπεί δηλαδή στη δημιουργία ενός περιβάλλοντος διεπαφής για τον χρήστη.

**Node.js:** Ένα back-end JavaScript runtime environment

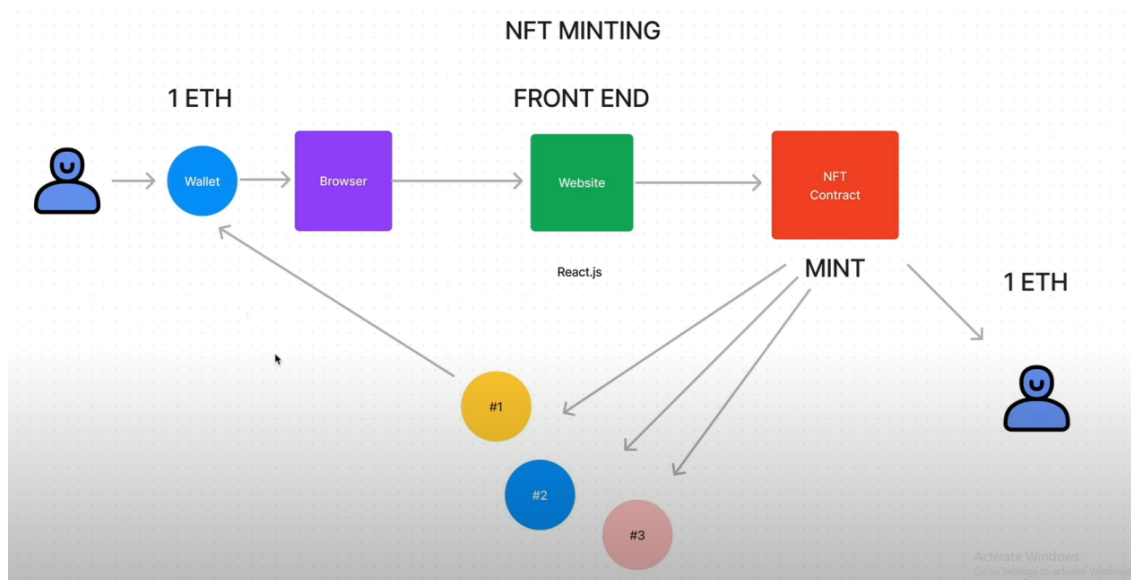
**Ethers.js:** Μια βιβλιοθήκη της Javascript που παρέχει στον χρήστη πολλά εργαλεία που βοηθούν στην αλληλεπίδραση με δίκτυα blockchain.

**OpenZeppelin:** Μια βιβλιοθήκη που θα χρησιμοποιηθεί για τη δημιουργία ενός αρχικού template για τα NFT.

**IPFS:** Αποκεντρωμένο σύστημα αποθήκευσης αρχείων

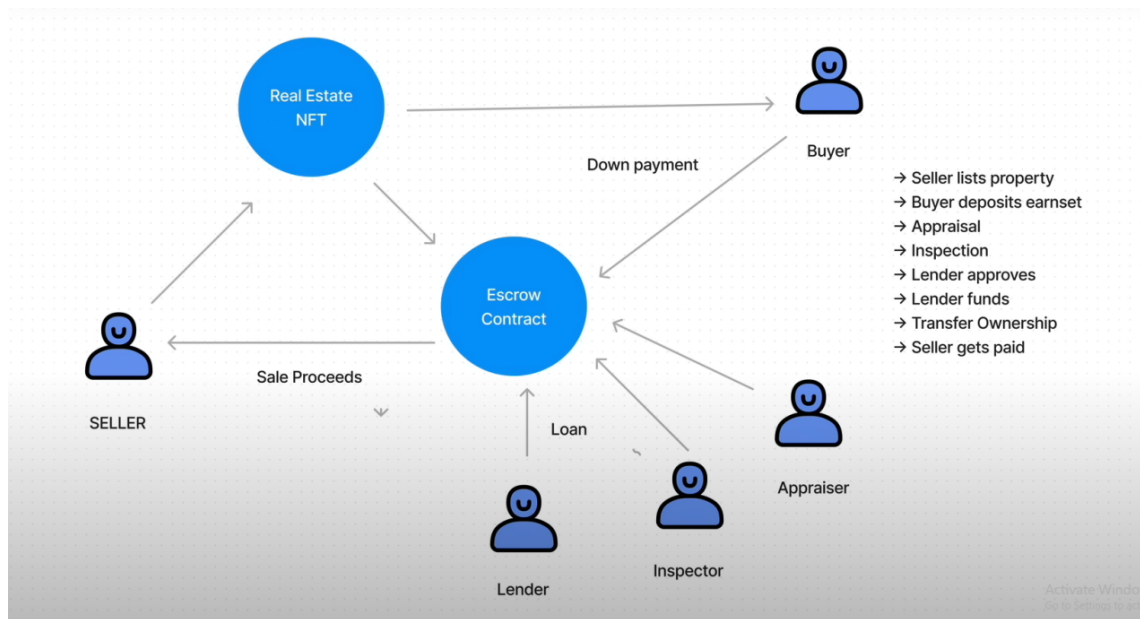
Σε πρώτο στάδιο (Σχήμα D.15), ο χρήστης συνδέεται στο πορτοφόλι του με τη χρήση του Metamask, από έναν διακομιστή όπως το Google Chrome. Στη συνέχεια, ο χρήστης αλληλεπιδρά μέσω της ιστοσελίδας με το έξυπνο συμβόλαιο, το οποίο θα έχει όλες τις ακίνητες

περιουσίες σε μορφή NFT. Τα παραπάνω NFT θα έχουν δημιουργηθεί χειροκίνητα, καλώντας τη συνάρτηση MINT.



**Σχήμα D.15:** Διάγραμμα ενεργειών του έξυπνου συμβολαίου

Ο αγοραστής αλληλεπιδρά με το έξυπνο συμβόλαιο το οποίο είναι υπεύθυνο για όλα τα ακίνητα. Στη συνέχεια, όταν επιλέξει ποιο ακίνητο θα αγοράσει, θα συμμετάσχουν και άλλοι χρήστες που θα είναι υπεύθυνοι για την εκτίμηση και την επιθεώρηση της εγκυρότητας του ακινήτου, όπως επίσης και για ένα ενδεχόμενο δάνειο, εάν χρειαστεί. Ο ρόλος τους είναι να επικυρώσουν ότι η συναλλαγή είναι έγκυρη και ασφαλής, πριν ο κάτοχος και πωλητής του ακινήτου μεταφέρει την ιδιοκτησία του NFT (Σχήμα D.16).



**Σχήμα D.16:** Διάγραμμα συμμετεχόντων στο Smart Contract και η αλληλεπίδρασή τους με τα 2 συμβόλαια.

## D.1 Contracts

Όσον αφορά τα εργαλεία για την ανάπτυξη της εφαρμογής, αρχικά θα γίνει η εγκατάσταση και χρήση της έκδοσης των Node.js (v16.14.0), Hardhat, Ethers.js και React.js.

Το πρώτο έξυπνο συμβόλαιο είναι υπεύθυνο για τα Real Estate NFT (Listing D.1).

**Listing D.1:** Χρήση βιβλιοθηκών για τη συμπεριφορά του NFT, σύνταξη της συνάρτησης `mint()` για τα νέα ακίνητα, και της `totalSupply()` για καταγραφής των ήδη υπαρχόντων.

```

1 //SPDX-License-Identifier: Unlicense
2 pragma solidity ^0.8.0;
3
4 import "@openzeppelin/contracts/utils/Counters.sol";
5 import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
6 import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
7

```

```

8 contract RealEstate is ERC721URIStorage {
9     using Counters for Counters.Counter;
10    Counters.Counter private _tokenIds;
11
12    constructor() ERC721("Real Estate", "REAL") {}
13
14    function mint(string memory tokenURI) public returns (uint256) {
15        _tokenIds.increment();
16
17        uint256 newItemId = _tokenIds.current();
18        _mint(msg.sender, newItemId);
19        _setTokenURI(newItemId, tokenURI);
20
21        return newItemId;
22    }
23
24    function totalSupply() public view returns (uint256) {
25        return _tokenIds.current();
26    }
27 }

```

---

- Οι βιβλιοθήκες που εισάγονται, χάρη στη διαδικασία της κληρονομικότητας προσδίδουν έτοιμες ιδιότητες και μεθόδους που είναι υπεύθυνες για την ορθότητα και έλεγχο του κώδικα των NFT.
- Το Mint() function χρησιμοποιείται για την δημιουργία νέων ακινήτων, ενώ το totalSupply() function λειτουργεί σαν μετρητής για τα ήδη υπάρχοντα.

Το δεύτερο συμβόλαιο (Listing D.2). είναι αυτό που έχει όλη τη λειτουργικότητα όσον αφορά τις αγοροπωλησίες των ακινήτων.

**Listing D.2:** Δήλωση μεταβλητών για την συνάρτηση *transferFrom()*, δημιουργία του *Escrow Contract* και αρχικοποίηση όλων των διευθύνσεων των συμμετεχόντων.

---

```

1 //SPDX-License-Identifier: Unlicense
2 pragma solidity ^0.8.0;
3
4 interface IERC721 {

```

```

5     function transferFrom(
6         address _from,
7         address _to,
8         uint256 _id
9     ) external;
10 }
11
12 contract Escrow {
13     address public nftAddress;
14     address payable public seller;
15     address public inspector;
16     address public lender;

```

---

**Στο πρώτο στάδιο**, δηλώνονται ως μεταβλητές ο πωλητής (seller), επιθεωρητής (inspector), ο δανειστής (lender) και η διεύθυνση του NFT της ακίνητης περιουσίας στο blockchain (nftAddress).

Στο Interface, το οποίο λειτουργεί ως “σκελετός” για ένα smart contract -με την έννοια ότι εκεί μπορούν να δηλωθούν χρήσιμες συναρτήσεις που θα χρειαστούν στη συνέχεια-, δηλώνεται η συνάρτηση transferFrom(), η οποία καλείται από την πλευρά του buyer. Το interface είναι χρήσιμο στην προκειμένη περίπτωση επειδή ο χρήστης μπορεί να καλέσει κατευθείαν αυτή τη συνάρτηση, αντί να κάνει import συνέχεια το προηγούμενο contract που περιέχει το NFT.

Στη συνέχεια, στον Constructor, ο οποίος είναι μια συνάρτηση που τρέχει μια μοναδική φορά όταν ένα smart contract γίνεται deploy στο blockchain, αυτές οι μεταβλητές θα πάρουν μια τιμή, η οποία κάθε φορά θα εξαρτάται από τον χρήστη που καλεί το συγκεκριμένο contract.

Να σημειωθεί πως μερικές λέξεις όπως το public, payable λέγονται modifiers και δίνουν ιδιότητες στις μεταβλητές και στις συναρτήσεις. Στην προκειμένη περίπτωση, το public αφορά την ορατότητα (visibility) της μεταβλητής, καθιστώντας τη δημόσια και ορατή από όλους τους χρήστες του blockchain. Το address payable, δηλώνει πως η συγκεκριμένη διεύθυνση μπορεί να δεχτεί Ether ως πληρωμή.

**Στο δεύτερο στάδιο**, θα προστεθεί μια νέα συνάρτηση, η οποία θα είναι υπεύθυνη για την καταχώρηση (listing) ενός NFT. Κατά αυτή τη διαδικασία, η ακίνητη περιουσία θα μεταφερθεί από το πορτοφόλι του πωλητή στο συμβόλαιο Escrow.

Για να ελαχιστοποιηθεί το περιθώριο λάθους ή εκμετάλλευσης του έξυπνου συμβολαίου, στην συνάρτηση `list()` θα γραφτεί ως προϋπόθεση, να είναι δυνατή η κλήση της μόνο από αυτόν που καλεί το έξυπνο συμβόλαιο ως αγοραστή. Επίσης, πρέπει να ελεγχθούν η διεύθυνση του αγοραστή, η τιμή του ακινήτου, μια αρχική τιμή σαν προκαταβολή (down payment) και εάν το ακίνητο είναι ήδη προς πώληση. Για να κρατηθούν αυτές οι πληροφορίες, χρησιμοποιούνται mappings (Listing D.3), μια διεργασία που συσχετίζει 2 στοιχεία. Το mapping είναι σαν ένας πίνακας που συνδέει ένα κλειδί με μια αξία.

**Listing D.3:** *mappings που συνδέουν τα ακίνητα με χρήσιμες τιμές, όπως τον αγοραστή τους, την κατάσταση του ακινήτου και χρηματικά ποσά.*

---

```
1     modifier onlySeller() {
2         require(msg.sender == seller, "Only seller can call this ←
           method");
3     }
4
5     mapping(uint256 => bool) public isListed;
6     mapping(uint256 => uint256) public purchasePrice;
7     mapping(uint256 => uint256) public escrowAmount;
8     mapping(uint256 => address) public buyer;
9     mapping(uint256 => bool) public inspectionPassed;
```

---

Η συνάρτηση `list()` (Listing D.4) χρειάζεται το ID του NFT, τη διεύθυνση του αγοραστή και τις τιμές του ακινήτου και του escrow. Στη συνέχεια, μεταφέρεται από τον `msg.sender` στον αγοραστή. Ο modifier `msg.sender` αναφέρεται στη διεύθυνση του χρήστη που καλεί το συμβόλαιο, ενώ το `this`, αναφέρεται στη διεύθυνση του παρόντος συμβολαίου.

**Listing D.4:** *Δημιουργία της συνάρτησης `list()`, που είναι υπεύθυνη για την πώληση μια ακίνητης περιουσίας.*

---

```
1     function list(
2         uint256 _nftID,
3         address _buyer,
4         uint256 _purchasePrice,
5         uint256 _escrowAmount
6     ) public payable onlySeller {
7         // Transfer NFT from seller to this contract
8         IERC721(nftAddress).transferFrom(msg.sender, address(this), ←
           _nftID);
```

```
9
10     isListed[_nftID] = true;
11     purchasePrice[_nftID] = _purchasePrice;
12     escrowAmount[_nftID] = _escrowAmount;
13     buyer[_nftID] = _buyer;
14 }
```

---

Μια ακόμα αναγκαία προσθήκη είναι η συναρτήσεις `depositEarnest()` και `getBalance()` (Listing D.5).

- Με την `depositEarnest()`, ο αγοραστής στέλνει ένα ποσό Ether στο contract ώστε να αγοράσει το ακίνητο. Το ποσό αυτό βρίσκεται και αποθηκεύεται πλέον μέσα στο contract. Η μόνη προϋπόθεση είναι το ποσό να είναι μεγαλύτερο από την τιμή του ακινήτου.
- Με την `getBalance()`, ο αγοραστής μπορεί να δει πόσα funds έχουν μαζευτεί στο contract και να υπολογίσει έτσι πόσα ακόμα του απομένουν ώστε να αγοράσει το ακίνητο.

**Listing D.5:** Δημιουργία της `depositEaarnest()` και της `getBalance()`. Συναρτήσεις υπεύθυνες για την "προκαταβολή" και την προβολή του υπολοίπου για την ακίνητη περιουσία αντίστοιχα.

---

```
1 // Put Under Contract (only buyer — payable escrow)
2 function depositEarnest(uint256 _nftID) public payable onlyBuyer(←
   _nftID) {
3     require(msg.value >= escrowAmount[_nftID]);
4 }
5 function getBalance() public view returns (uint256) {
6     return address(this).balance;
7 }
```

---

Όπως έχει γίνει αντιληπτό μέχρι στιγμής, το συγκεκριμένο έξυπνο συμβόλαιο, μπορεί να κληθεί από διάφορους χρήστες. Τον αγοραστή, τον πωλητή, αυτού που δίνει ενδεχομένως το δάνειο, αυτού που κάνει επιθεώρηση, και αυτού που δίνει μια εκτίμηση της αξίας. Για το λόγο αυτό, πριν δημιουργηθεί η επόμενη συνάρτηση, θα χρειαστεί ο παρακάτω modifier που θα προστεθεί στην αντίστοιχη συνάρτηση (Listing D.6). Έτσι, κανένας άλλος δε θα είναι σε θέση να την καλέσει και να κρίνει αν η ακίνητη περιουσία είναι έγκυρη ή όχι.

**Listing D.6:** *Modifier για μια συνάρτηση που επιτρέπει μόνο στον επιθεωρητή να την καλέσει.*

---

```
1     modifier onlyInspector() {
2         require(msg.sender == inspector, "Only inspector can call ↵
           this method");
3     };
4 }
```

---

Παρόμοια με την `depositEarnest()`, γράφεται και η `updateInspectionStatus()`. Αυτή η συνάρτηση όπως και η `list()` θα χρησιμοποιήσει έναν ειδικό modifier ώστε μόνο ο χρήστης που έχει το ρόλο του επιθεωρητή να μπορεί να την καλέσει (Listing D.7).

**Listing D.7:** *Συνάρτηση με για τον επιθεωρητή, ο οποίος μπορεί να χαρακτηρίσει την ακίνητη περιουσία ως "Passed"*

---

```
1     // Update Inspection Status (only inspector)
2     function updateInspectionStatus(uint256 _nftID, bool _passed)
3     public
4     onlyInspector
5     {
6         inspectionPassed[_nftID] = _passed;
7     }
8 }
```

---

Ακολουθώντας την παραπάνω λογική, θα προστεθούν μερικές ακόμα συναρτήσεις ώστε η αγοραπωλησία να είναι όσο πιο ασφαλής γίνεται.

Οποιοσδήποτε από τον δανειστή, επιθεωρητή και του χρήστη που εκτιμά την περιουσία, μετά την εκπλήρωση του ρόλου τους, πρέπει να έχουν τη δυνατότητα να δώσουν την έγκρισή τους για τη συναλλαγή. Για αυτό το λόγο ορίζουμε την συνάρτηση `approveSale()`, η οποία θα δρασει ως μια θετική ψήφος για την εγκυρότητα της συναλλαγής (Listing D.8).

**Listing D.8:** *Συνάρτηση που δίνει δικαίωμα στους συμμετέχοντες να εγκρίνουν την αγοραπωλησία*

---

```
1     // Approve Sale
2     function approveSale(uint256 _nftID) public {
3         approval[_nftID][msg.sender] = true;
4     }
```

---

Για να οριστικοποιηθεί η αγοραπωλησία, πρέπει να υπάρξει ακόμη μια συνάρτηση η οποία να πληροί τα παρακάτω κριτήρια (Listing D.9):

- Να έχει μια θετική κατάσταση επιθεώρησης.
- Να εγκρίνεται η πώληση.
- Το NFT να μην είναι ήδη προς πώληση.
- Το NFT να μεταφέρεται στον αγοραστή.
- Το ποσό των Eth να είναι αρκετό ώστε να ολοκληρωθεί η πώληση
- Το ποσό των Eth να μεταφέρεται στον πωλητή.

**Listing D.9:** *Σύνταξη της `finalizeSale()`. Εάν πληρούνται οι προϋποθέσεις μέσα στα `require()`, αυτή η συνάρτηση μεταφέρει την ακίνητη περιουσία από τον πωλητή στον αγοραστή και το πληρωταίο ποσό από τον αγοραστή στον πωλητή.*

---

```
1      function finalizeSale(uint256 _nftID) public {
2          require(inspectionPassed[_nftID]);
3          require(approval[_nftID][buyer[_nftID]]);
4          require(approval[_nftID][seller]);
5          require(approval[_nftID][lender]);
6          require(address(this).balance >= purchasePrice[_nftID]);
7
8          isListed[_nftID] = false;
9
10         (bool success, ) = payable(seller).call{value: address(this).↵
            balance}(
11             ""
12         );
13         require(success);
14
15         IERC721(nftAddress).transferFrom(address(this), buyer[_nftID]↵
            , _nftID);
16     }
```

---

Τέλος, θα πρέπει να υπάρχει η επιλογή ακύρωσης την αγοραπωλησίας, εάν η επιθεώρηση δεν είναι σωστή. Στην περίπτωση αυτή, το NFT επιστρέφει στην κατοχή του πωλητή (Listing D.10).

**Listing D.10:** *Συνάρτηση που ακυρώνει την συναλλαγή εάν ο επιθεωρητής δεν εγκρίνει την αγοραπωλησία*

---

```
1      function cancelSale(uint256 _nftID) public {
2          if (inspectionPassed[_nftID] == false) {
3              payable(buyer[_nftID]).transfer(address(this).balance);
4          } else {
5              payable(seller).transfer(address(this).balance);
6          }
7      }
```

---

## D.2 Testing

Επειδή τα έξυπνα συμβόλαια επεξεργάζονται κυρίως οικονομικές συναλλαγές, είναι πολύ σημαντικό να είναι όσο πιο ασφαλή γίνεται. Για το λόγο αυτό, οι προγραμματιστές μέσω κάποιων frameworks όπως το Truffle, Foundry, Hardhat κ.α., γράφουν ένα επιπλέον κομμάτι κώδικα στο οποίο προσομοιώνουν και προσπαθούν να αναπαραστήσουν διάφορα σενάρια αλληλεπίδρασης με τα smart contracts. Είναι αποδεδειγμένο πως όσο περισσότερο testing γίνει σε ένα πρόγραμμα, τόσο πιο ασφαλές θα είναι.

Στο συγκεκριμένο Real Estate έξυπνο συμβόλαιο, θα αναπτυχθούν τα tests σε ένα συγκεκριμένο αρχείο που παρέχει το Hardhat framework. Αυτά είναι γραμμένα σε Javascript και χρησιμοποιούν ασύγχρονες συναρτήσεις, καθώς όλες οι συναλλαγές στο blockchain λειτουργούν με διαφορά φάσης.

Αρχικά, δημιουργείται ο σκελετός για το testing. Σε αυτό το σημείο, ζητάμε τις λειτουργίες δυο βιβλιοθηκών που βοηθούν στον έλεγχο της συμπεριφοράς του smart contract. Επίσης υπάρχει η βοηθητική συνάρτηση tokens(), η οποία βοηθάει στη μετατροπή Ether σε tokens. Όσον αφορά τη συνάρτηση describe(), όπως υποδεικνύει και το όνομα, εκεί θα γραφτούν τα διάφορα σενάρια συμπεριφοράς του smart contract (Listing D.11).

**Listing D.11:** *Δημιουργία σκελετού για το testing. Εισαγωγή βιβλιοθηκών και δημιουργία*

*βοηθητικής συνάρτησης για τη μετατροπή Ether σε tokens.*

---

```
1 const { expect } = require('chai');
2 const { ethers } = require('hardhat');
3
4 const tokens = (n) => {
5     return ethers.utils.parseUnits(n.toString(), 'ether')
6 }
7
8 describe('Escrow', () => {
9 })
```

---

Στη συνέχεια, τα tests παίρνουν την εξής μορφή (Listing D.12):

**Listing D.12:** Περιγραφή μιας συμπεριφοράς του smart contract. Το συγκεκριμένο test εκτυπώνει ασύγχρονα τη διεύθυνση του Real Estate contract

---

```
1 const { expect } = require('chai');
2 const { ethers } = require('hardhat');
3
4 const tokens = (n) => {
5     return ethers.utils.parseUnits(n.toString(), 'ether')
6 }
7
8 describe('Escrow', () => {
9     it('saves the addresses', async () => {
10         const RealEstate = await ethers.getContractFactory('RealEstate')
11         realEstate = await RealEstate.deploy()
12         console.log(realEstate.address)
13     })
```

---

Η συνάρτηση `it()` όπως φαίνεται στην εικόνα, θα περιγράψει μια ενέργεια. Μετά καλείται το contract για το οποίο γίνεται το testing, αυτό γίνεται `deploy` τοπικά με στόχο να εμφανιστεί το επιθυμητό αποτέλεσμα. Στην προκειμένη περίπτωση, καλείται το πρώτο contract που παρουσιάστηκε και έχει ως στόχο να εμφανίζει τη σωστή διεύθυνση ώστε να είναι σίγουρο πως η αλληλεπίδραση γίνεται με το σωστό contract.

Το Hardhat προσφέρει μια προσομοίωση του blockchain, και δίνει τη δυνατότητα στον προγραμματιστή να αλληλεπιδράσει με διαφορά accounts. Το κάθε ένα από αυτά έχει ένα address και ένα private key. Έτσι είναι εφικτό μέσα από τα tests, ένας χρήστης να υποδυθεί

πολλούς ρόλους, όπως αυτούς του αγοραστή, πωλητή, δανειστή, επιθεωρητή κ.α.

Επειδή σε κάθε συμβόλαιο γίνονται πολλά tests, και ένα κομμάτι του κώδικα θα ανακαλείται, χρησιμοποιείται η `beforeEach()` συνάρτηση. Κατά αυτήν, με τη βοήθεια της βιβλιοθήκης `ethers.js`, συνδέεται σε κάθε ένα από τα “dummy” accounts που δίνει το `hardhat`, μια ιδιότητα. Στην προκειμένη περίπτωση, ενδεικτικά τα πρώτα τέσσερα accounts παίρνουν τη μορφή του αγοραστή, πωλητή, επιθεωρητή και δανειστή. Μετά όπως φαίνεται στο Listing D.13, αφού κληθεί το συμβόλαιο, γίνεται έλεγχος για τις διευθύνσεις των συμμετεχόντων.

**Listing D.13:** Έλεγχος για το αν το *smart contract* επιστρέφει σωστά τις διευθύνσεις του *NFT*, πωλητή, δανειστή και επιθεωρητή.

---

```
1 describe('Escrow', () => {
2     let buyer, seller, inspector, lender
3     let realEstate, escrow
4
5     beforeEach(async () => {
6         // Setup accounts
7         [buyer, seller, inspector, lender] = await ethers.getSigners()
8
9         // Deploy Real Estate
10        const RealEstate = await ethers.getContractFactory('RealEstate')
11        realEstate = await RealEstate.deploy()
12
13        // Mint
14        let transaction = await realEstate.connect(seller).mint("https://ipfs.io/ipfs/QmTudSYeM7mz3PkYEWXWqPjomRPHogcMFSq7XAvsosgAPS")
15        await transaction.wait()
16        // Deploy Escrow
17        const Escrow = await ethers.getContractFactory('Escrow')
18        escrow = await Escrow.deploy(
19            realEstate.address,
20            seller.address,
21            inspector.address,
22            lender.address
```

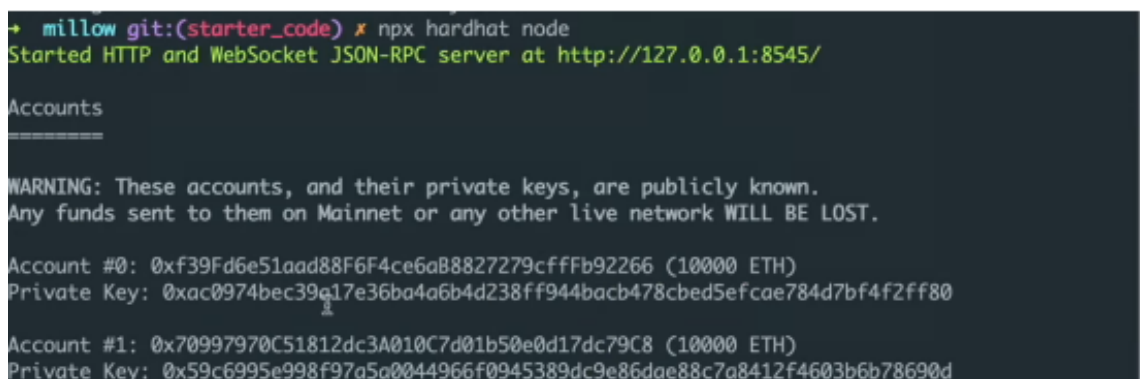
```

23     )
24     describe('Deployment', () => {
25         it('Returns NFT address', async () => {
26             const result = await escrow.nftAddress()
27             expect(result).to.be.equal(realEstate.address)
28         })
29
30         it('Returns seller', async () => {
31             const result = await escrow.seller()
32             expect(result).to.be.equal(seller.address)
33         })
34
35         it('Returns inspector', async () => {
36             const result = await escrow.inspector()
37             expect(result).to.be.equal(inspector.address)
38         })
39
40         it('Returns lender', async () => {
41             const result = await escrow.lender()
42             expect(result).to.be.equal(lender.address)
43         })

```

---

Τα “dummy accounts” που τρέχουν τοπικά, βρίσκονται στη γραμμή εντολών και έχουν τη μορφή της εικόνας Σχήμα D.17.



```

→ millow git:(starter_code) x npx hardhat node
Started HTTP and WebSocket JSON-RPC server at http://127.0.0.1:8545/

Accounts
=====

WARNING: These accounts, and their private keys, are publicly known.
Any funds sent to them on Mainnet or any other live network WILL BE LOST.

Account #0: 0xf39Fd6e51aad88F6F4ce6aB8827279cFfFb92266 (10000 ETH)
Private Key: 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf4f2ff80
Account #1: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8 (10000 ETH)
Private Key: 0x59c6995e998f97a5a0044966f0945389dc9e86dae88c7a8412f4603b6b78690d

```

Σχήμα D.17: *Dummy accounts για testing που δίνει το Hardhat framework*

Με την ίδια λογική, θα εξεταστεί αν λειτουργεί σωστά και η συνάρτηση `listing()`. Στο Listing D.14, καλούνται μερικές συναρτήσεις όπως οι `isListed()`, `ownerOf()`, `buyer()`, `purchasePrice()`, `escrowAmount()`. Αυτές παίρνουν την τιμή ένα (1), η οποία αναφέρεται στο πρώτο NFT από τη λίστα ακινήτων. Παρομοίως, δίνονται ενδεικτικές τιμές `tokens`, που χρησιμοποιούνται ως το ποσό πληρωμής. Πρέπει να εξεταστεί εάν οι διευθύνσεις και οι τιμές του ακινήτου που τίθεται προς πώληση είναι οι σωστές και εάν συνδέονται με τη διεύθυνση του χρήστη που αγοράζει ή πουλάει.

**Listing D.14:** Συνάρτηση που ελέγχει αν μετά απο ένα *listing* μιας περιουσίας, εκτυπώνονται σωστά η κατάσταση `isListed()`, ο αγοραστής, η τιμή αγοράς, η τιμή `escrow` και αν ενημερώνεται σωστά η ιδιοκτησία στον καινούργιο χρήστη.

---

```
1 describe('Listing', () => {
2     it('Updates as listed', async () => {
3         const result = await escrow.isListed(1)
4         expect(result).to.be.equal(true)
5     })
6
7     it('Returns buyer', async () => {
8         const result = await escrow.buyer(1)
9         expect(result).to.be.equal(buyer.address)
10    })
11
12    it('Returns purchase price', async () => {
13        const result = await escrow.purchasePrice(1)
14        expect(result).to.be.equal(tokens(10))
15    })
16
17    it('Returns escrow amount', async () => {
18        const result = await escrow.escrowAmount(1)
19        expect(result).to.be.equal(tokens(5))
20    })
}
```

---

Να σημειωθεί ότι σε ένα ξεχωριστό αρχείο, έχουν περαστεί χειροκίνητα μεταδεδομένα που σχετίζονται με τα ακίνητα. Αυτά παρέχουν πληροφορίες όπως το όνομα του ακινήτου, η διεύθυνση του, χαρακτηριστικά όσον αφορά τα δωμάτια και γενικές πληροφορίες όπως τα τετραγωνικά μέτρα και η χρονολογία κατασκευής του (Listing D.15).

**Listing D.15:** Δεδομένα που αναπαριστούν μια ακίνητη περιουσία.

---

```
1 {
2   "name": "Luxury NYC Penthouse",
3   "address": "157 W 57th St APT 49B, New York, NY 10019",
4   "description": "Luxury Penthouse located in the heart of NYC",
5   "image": "https://ipfs.io/ipfs/↵
        QmQUozrHLAusXDxrvsESJ3PYB3rUeUuBAvVWw6nop2uu7c/1.png",
6   "id": "1",
7   "attributes": [
8     {
9       "trait_type": "Purchase Price",
10      "value": 20
11    },
12    {
13      "trait_type": "Type of Residence",
14      "value": "Condo"
15    },
16    {
17      "trait_type": "Bed Rooms",
18      "value": 2
19    },
20    {
21      "trait_type": "Bathrooms",
22      "value": 3
23    },
24    {
25      "trait_type": "Square Feet",
26      "value": 2200
27    },
28    {
29      "trait_type": "Year Built",
30      "value": 2013
31    }
32  ]
33 }
```

---

Με τη χρήση της εντολής `npx hardhat test` γίνεται έλεγχος της συμπεριφοράς των tests (Σχήμα D.18).



**Σχήμα D.18:** Έλεγχος για τα tests που γράφτηκαν μέχρι στιγμής περνάνε τον έλεγχο.

Περνώντας στο δεύτερο συμβόλαιο, με την ίδια λογική θα εξεταστούν οι καταθέσεις στο Escrow συμβόλαιο, το Inspection και το Approval (Listing D.16 και Listing D.17).

**Listing D.16:** Συναρτήσεις που ελέγχουν αν οι τιμές στο contract αλλάζουν όταν κάποιος προσπαθήσει να βάλει χρήματα ως προκαταβολή ή αν η κατάσταση επιθεώρησης ενημερώνεται επιτυχώς.

```
1 describe('Deposits', () => {
2     beforeEach(async () => {
3         const transaction = await escrow.connect(buyer).↵
4             depositEarnest(1, { value: tokens(5) })
5         await transaction.wait()
6     })
7     it('Updates contract balance', async () => {
8         const result = await escrow.getBalance()
9         expect(result).to.be.equal(tokens(5))
10    })
11 })
12
13 describe('Inspection', () => {
14     beforeEach(async () => {
15         const transaction = await escrow.connect(inspector).↵
16             updateInspectionStatus(1, true)
17         await transaction.wait()
```

```

17     })
18
19     it('Updates inspection status', async () => {
20         const result = await escrow.inspectionPassed(1)
21         expect(result).to.be.equal(true)
22     })
23 })

```

---

**Listing D.17:** Έλεγχος για το αν η κατάσταση "έγκρισης" ενημερώνεται σωστά απο την πλευρά του αγοραστή, του πωλητή και του δανειστή

---

```

1 describe('Approval', () => {
2     beforeEach(async () => {
3         let transaction = await escrow.connect(buyer).approveSale(
4             1)
5         await transaction.wait()
6
7         transaction = await escrow.connect(seller).approveSale(1)
8         await transaction.wait()
9
10        transaction = await escrow.connect(lender).approveSale(1)
11        await transaction.wait()
12    })
13
14    it('Updates approval status', async () => {
15        expect(await escrow.approval(1, buyer.address)).to.be(
16            equal(true)
17        )
18        expect(await escrow.approval(1, seller.address)).to.be(
19            equal(true)
20        )
21        expect(await escrow.approval(1, lender.address)).to.be(
22            equal(true)
23        )
24    })
25 })

```

---

Τέλος, θα γίνει έλεγχος για την πιο σημαντική συνάρτηση, την `finalizeSale()` (Listing D.18 και Listing D.19) και θα εκτελεστούν τα τελευταία tests (Σχήμα D.19).

**Listing D.18:** Έλεγχος των προϋποθέσεων της συνάρτησης `finalizeSale()` (βλ. Σχήμα

25). Η συνάρτησή ελέγχει εάν η αγοραπωλησία έχει πάρει την έγκρισή όλων των συμμετεχόντων, εάν μεταφέρεται σωστά το χρηματικό ποσό από τον lender και αν η συναλλαγή ολοκληρώνεται σωστά από την πλευρά του seller.

---

```
1 describe('Sale', () => {
2     beforeEach(async () => {
3         let transaction = await escrow.connect(buyer).↵
4             depositEarnest(1, { value: tokens(5) })
5         await transaction.wait()
6
7         transaction = await escrow.connect(escrow).↵
8             updateInspectionStatus(1, true)
9         await transaction.wait()
10
11        transaction = await escrow.connect(buyer).approveSale(1)
12        await transaction.wait()
13
14        transaction = await escrow.connect(seller).approveSale(1)
15        await transaction.wait()
16
17        transaction = await escrow.connect(lender).approveSale(1)
18        await transaction.wait()
19
20        await lender.sendTransaction({ to: escrow.address, value:↵
21            tokens(5) })
22    })
```

---

**Listing D.19:** Τελευταία tests που δείχνουν εάν έχει αλλάξει κατοχή η ακίνητη περιουσία και εάν έχει μεταφερθεί σωστά το ποσό χρημάτων.

---

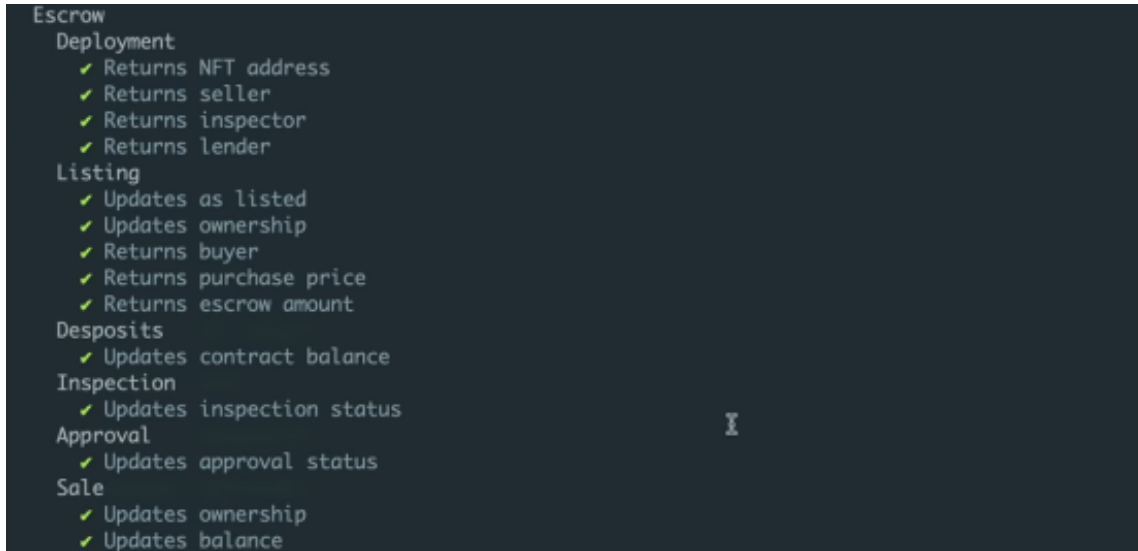
```
1 it('Updates ownership', async () => {
2     expect(await realEstate.ownerOf(1)).to.be.equal(buyer.↵
3         address)
4 })
```

```

5         it('Updates balance', async () => {
6             expect(await escrow.getBalance()).to.be.equal(0)
7         })

```

---



**Σχήμα D.19:** Έλεγχος ορθότητας για τα τελικά tests των του Escrow Contract.

### D.3 Deployment

Σε αυτό το στάδιο, το έξυπνο συμβόλαιο είναι λειτουργικό και ασφαλές. Επόμενος στόχος είναι να γίνει deployment. Για λόγους ευκολίας, θα προστεθεί ένα ακόμα αρχείο σε μορφή script, που έχει ως σκοπό την αυτοματοποιημένη ανάρτηση σε ένα Ethereum Blockchain, που τρέχει τοπικά χάρη στο Hardhat framework (Listing D.20).

**Listing D.20:** Το script δίνει ένα account σε κάθε έναν απο τους αγοραστή, πωλητή, επιθεωρητή, δανειστή, Φορτώνει τα συμβόλαια και στη συνέχεια τα μεταδεδομένα για τις ακίνητες περιουσίες.

---

```

1 const hre = require("hardhat");
2
3 const tokens = (n) => {
4     return ethers.utils.parseUnits(n.toString(), 'ether')
5 }

```

```

6
7 async function main() {
8   // Setup accounts
9   const [buyer, seller, inspector, lender] = await ethers.getSigners↵
    ()
10
11   // Deploy Real Estate
12   const RealEstate = await ethers.getContractFactory('RealEstate')
13   const realEstate = await RealEstate.deploy()
14   await realEstate.deployed()
15
16   console.log(`Deployed Real Estate Contract at: ${realEstate.address↵
    }`)
17   console.log(`Minting 3 properties...\n`)
18
19   for (let i = 0; i < 3; i++) {
20     const transaction = await realEstate.connect(seller).mint(`https↵
        ://ipfs.io/ipfs/↵
        QmQVcpsjrA6cr1iJjZAodYwmPekYgbnXGo4DFubJiLc2EB/${i + 1}.json↵
        `)
21     await transaction.wait()
22   }
23
24   // Deploy Escrow
25   const Escrow = await ethers.getContractFactory('Escrow')
26   const escrow = await Escrow.deploy(
27     realEstate.address,
28     seller.address,
29     inspector.address,
30     lender.address
31   )
32   await escrow.deployed()
33
34   console.log(`Deployed Escrow Contract at: ${escrow.address}`)
35   console.log(`Listing 3 properties...\n`)
36
37   for (let i = 0; i < 3; i++) {
38     // Approve properties...

```

```

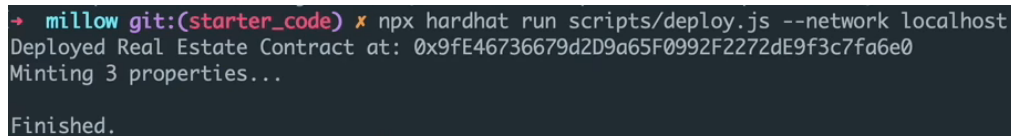
39     let transaction = await realEstate.connect(seller).approve(escrow↵
        .address, i + 1)
40     await transaction.wait()
41 }
42
43 // Listing properties...
44 transaction = await escrow.connect(seller).list(1, buyer.address, ↵
        tokens(20), tokens(10))
45 await transaction.wait()
46
47 transaction = await escrow.connect(seller).list(2, buyer.address, ↵
        tokens(15), tokens(5))
48 await transaction.wait()
49
50 transaction = await escrow.connect(seller).list(3, buyer.address, ↵
        tokens(10), tokens(5))
51 await transaction.wait()
52
53 console.log(`Finished.`)
54 }

```

---

Στο Listing D.20, το script επιχειρεί να κάνει deploy τα δυο(2) συμβόλαια, και καταχωρεί τις ακίνητες περιουσίες ως NFT.

Το Script εκτελείται με την εντολή `npx hardhat run scripts/deploy.js --network localhost` (Σχήμα D.20).



```

→ millow git:(starter_code) ✗ npx hardhat run scripts/deploy.js --network localhost
Deployed Real Estate Contract at: 0x9fE46736679d2D9a65F0992F2272dE9f3c7fa6e0
Minting 3 properties...
Finished.

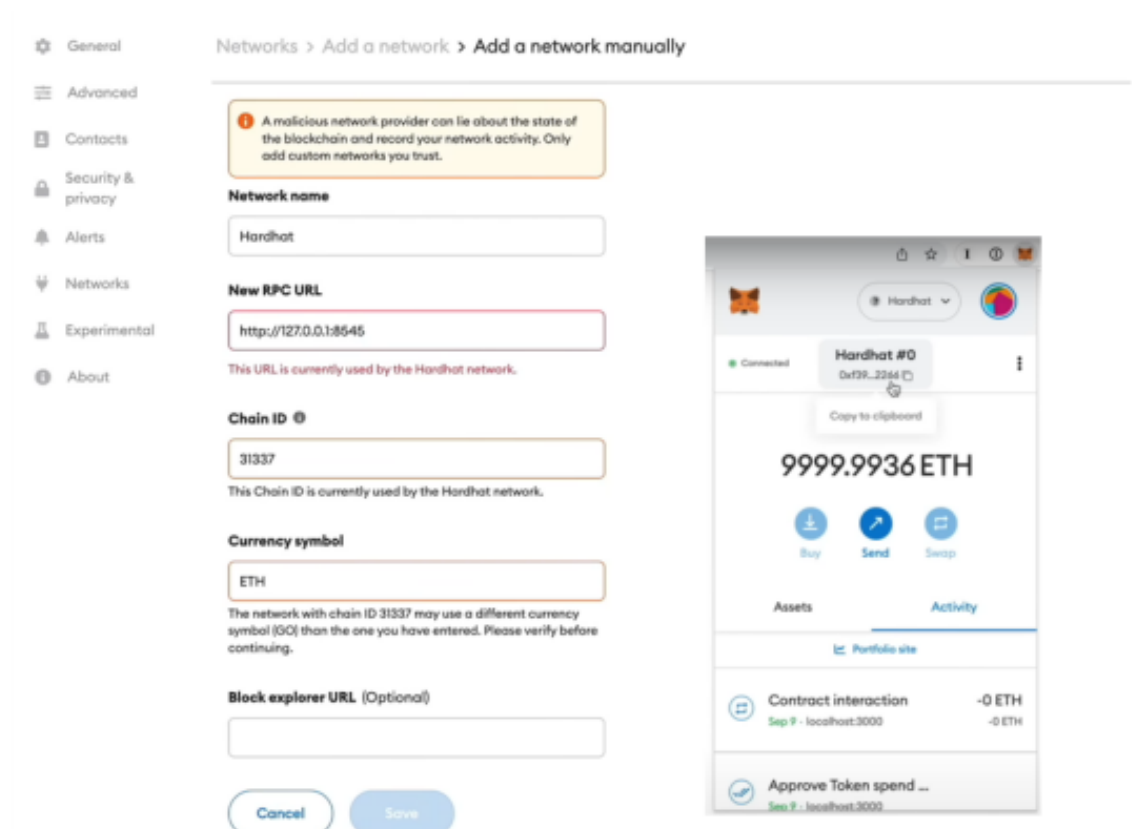
```

**Σχήμα D.20:** Επικύρωση της εκτέλεσης του script. Τα συμβόλαια έγιναν deployed τοπικά.

## D.4 Front-end

Για το Front-end κομμάτι, χρησιμοποιείται ένα έτοιμο προτότυπο (template) από το Real Estate site, Zillow.com<sup>1</sup>

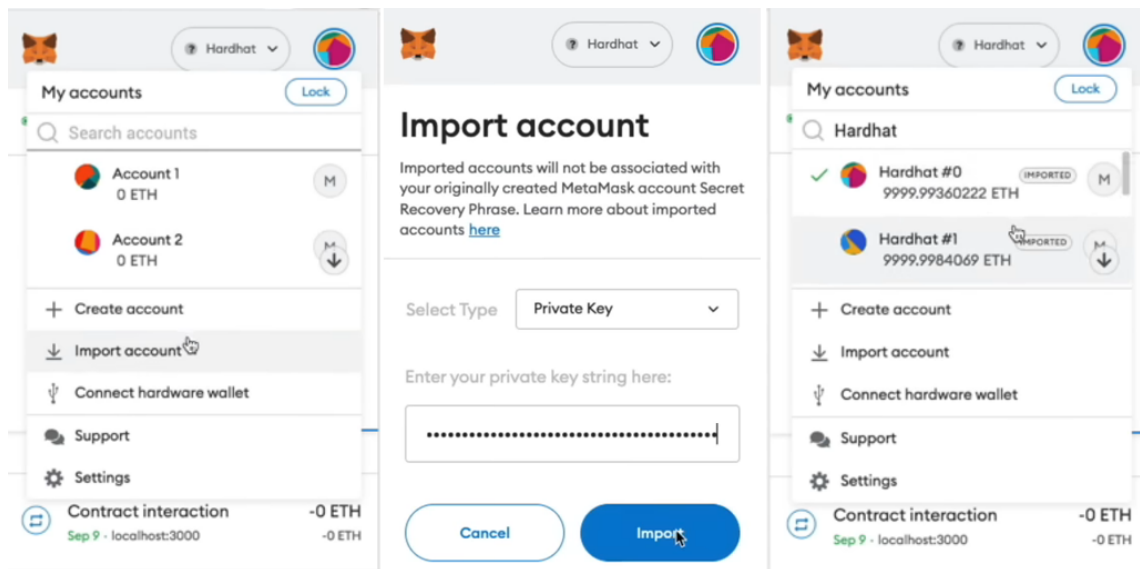
Ο χρήστης συνδέεται με το Metamask στο τοπικό blockchain (Σχήμα D.21).



**Σχήμα D.21:** Προσθήκη στο Metamask του τοπικού blockchain που παρέχει το Hardhat.

Στη συνέχεια, πρέπει να εισαχθούν στο Metamask τα dummy accounts που τρέχουν τοπικά, ώστε να μπορέσει ο χρήστης να αλληλεπιδράσει με το site, με όλους τους διαφορετικούς ρόλους που έχουν δηλωθεί στο έξυπνο συμβόλαιο. Όπως φαίνεται και στην εικόνα Σχήμα D.22, εισάγονται πολλοί διαφορετικοί λογαριασμοί.

<sup>1</sup>Κώδικας από το site <https://www.zillow.com/>



**Σχήμα D.22:** Προσθήκη των *account* που παρέχει το *Hardhat* ώστε να μπορεί ο χρήστης να αλληλεπιδράσει με τα συμβόλαια υπο διαφορετικούς ρόλους

Τέλος, για να γίνει η σύνδεση του προγράμματος με το blockchain που τρέχει τοπικά, πρέπει να προστεθεί στον κώδικα του front-end αυτό το κομμάτι (Listing D.21). Ουσιαστικά, είναι μια συνάρτηση που συνδέει το πρόγραμμα με το παράθυρο. Επίσης, συνδέει όλα τα accounts που συνδέσαμε στο Metamask και τους επιτρέπει να αλληλεπιδράσουν με το site.

**Listing D.21:** Συνάρτηση που συνδέει τα δεδομένα που υπάρχουν στο τοπικό blockchain με το user interface.

```

1 // Components
2 import Navigation from './components/Navigation';
3 import Search from './components/Search';
4 import Home from './components/Home';
5
6 // ABIs
7 import RealEstate from './abis/RealEstate.json';
8 import Escrow from './abis/Escrow.json';
9
10 // Config
11 import config from './config.json';

```

```

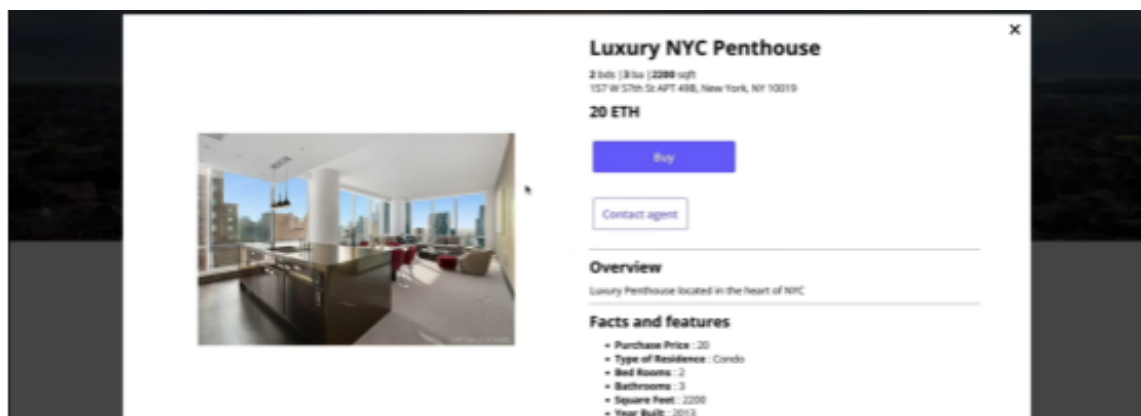
12
13 function App() {
14
15     const [account, setAccount] = useState(null)
16
17     const loadBlockchainData = async () => {
18         const provider = new ethers.providers.Web3Provider(window.↵
            ethereum)
19         const accounts = await window.ethereum.request({ method: '↵
            eth_requestAccounts' })
20         setAccounts(accounts[0])
21         console.log(accounts)
22     }
23     useEffect(() => {
24         loadBlockchainData()
25     }, [])

```

---

## D.5 Αλληλεπιδρώντας με το smart contract

Ο χρήστης έχει τη δυνατότητα να αλληλεπιδράσει τοπικά με το smart contract και να συμμετάσχει σε αγοραπωλησίες (Σχήμα D.23).



**Σχήμα D.23:** *To User Interface όταν ο χρήστης με την ιδιότητα του αγοραστή επιλέξει να αγοράσει ένα ακίνητο.*

Η μόνη προγραμματιστική δυσκολία εμφανίζεται όταν πολλά διαφορετικά accounts, επιθυμούν να υποδυθούν διαφορετικό ρόλο, όπως του αγοραστή, πωλητή, επιθεωρητή κ.α. (Listing D.22).

**Listing D.22:** Συνάρτηση που δίνει διαφορετικό ρόλο σε κάθε account που έγινε import στο Metamask. Λογαριασμός 1 -> Αγοραστής, Λογαριασμός 2 -> Πωλητής, κλπ.

---

```
1 const Home = ({ home, provider, account, escrow, togglePop }) => {
2   const [hasBought, setHasBought] = useState(false)
3   const [hasLended, setHasLended] = useState(false)
4   const [hasInspected, setHasInspected] = useState(false)
5   const [hasSold, setHasSold] = useState(false)
6
7   const [buyer, setBuyer] = useState(null)
8   const [lender, setLender] = useState(null)
9   const [inspector, setInspector] = useState(null)
10  const [seller, setSeller] = useState(null)
11
12  const [owner, setOwner] = useState(null)
13
14  const fetchDetails = async () => {
15    // — Buyer
16
17    const buyer = await escrow.buyer(home.id)
18    setBuyer(buyer)
19
20    const hasBought = await escrow.approval(home.id, buyer)
21    setHasBought(hasBought)
```

---

Εδώ δηλώνονται τα διαφορετικά accounts και στη συνέχεια γίνεται μετατροπή στο αρχείο που είναι υπεύθυνο για το front-end, ώστε ανάλογα με το ποιο account προσπαθεί να αλληλεπιδράσει με την εφαρμογή, να εμφανίζεται και η αντίστοιχη ενέργεια (Listing D.23).

**Listing D.23:** Συνάρτηση που θα αλλάζει τις επιλογές του χρήστη στο user interface ανάλογα με το ποιο account αλληλεπιδρά. Για παράδειγμα, εάν ο χρήστης είναι συνδεδεμένος με το account του lender, η επιλογή πρέπει να δείχνει "Approve and Lend"

---

```
1 {owner ? (
2   <div className='home__owned'>
```

```

3          Owned by {owner.slice(0, 6) + '...' + owner.slice(38,↵
          42)}}
4      </div>
5      ) : (
6      <div>
7          {(account === inspector) ? (
8              <button className='home__buy' onClick={inspectHandler↵
              } disabled={hasInspected}>
9              Approve Inspection
10             </button>
11             ) : (account === lender) ? (
12                 <button className='home__buy' onClick={lendHandler} ↵
                 disabled={hasLended}>
13                 Approve & Lend
14                 </button>
15                 ) : (account === seller) ? (
16                     <button className='home__buy' onClick={sellHandler} ↵
                     disabled={hasSold}>
17                     Approve & Sell
18                     </button>
19                     ) : (
20                         <button className='home__buy' onClick={buyHandler} ↵
                         disabled={hasBought}>
21                         Buy
22                         </button>
23                     )}
24
25                     <button className='home__contact '>
26                         Contact agent
27                     </button>
28                 </div>
29             )}

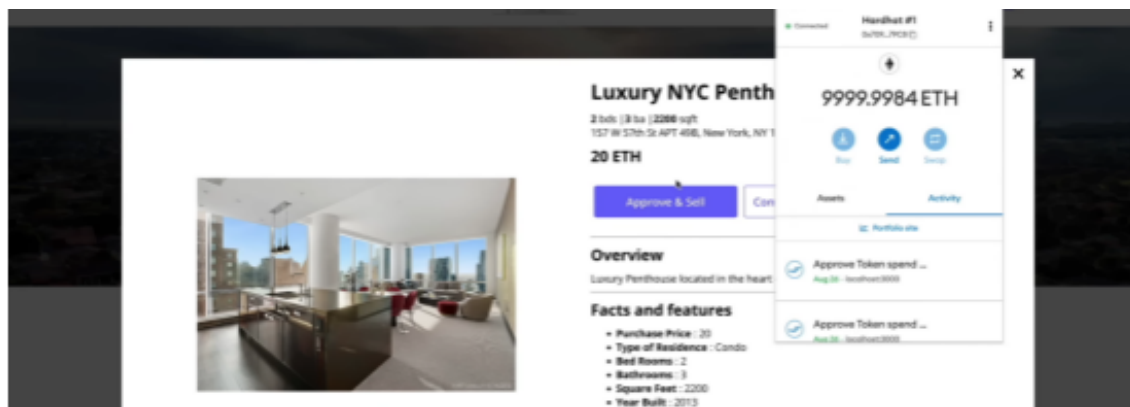
```

---

Τελικά, ο στόχος πρέπει να είναι ο εξής: Ο χρήστης χρησιμοποιώντας το Metamask, το οποίο είναι το ψηφιακό πορτοφόλι με το οποίο θα επικυρώνει συναλλαγές στο τοπικό blockchain, να υποδυθεί τους παρακάτω ρόλους.

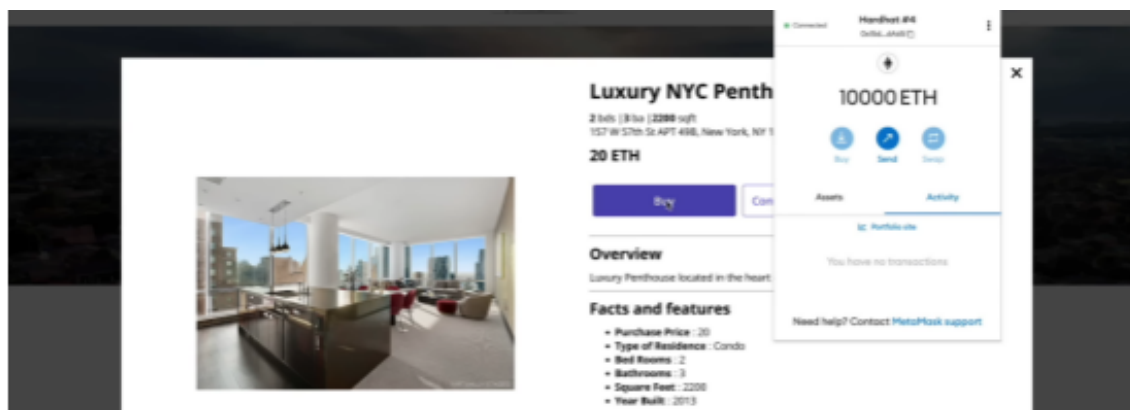
Αυτόν του πωλητή, ο οποίος είναι σε θέση να θέσει ένα ακίνητο προς πώληση και να

κάνει approve την πώληση.



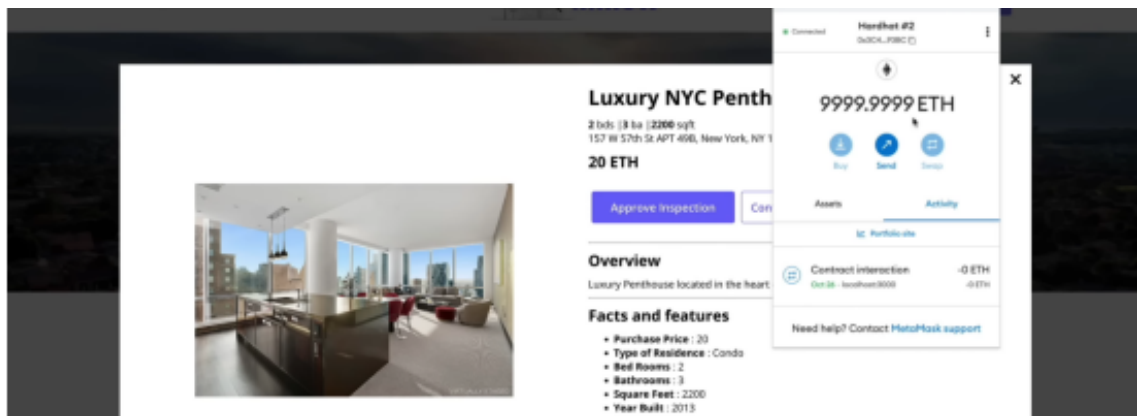
Σχήμα D.24: To User interface απο την πλευρά του πωλητή

Αυτόν του αγοραστή, ο οποίος είναι σε θέση να αγοράσει το NFT που αντιπροσωπεύει την ακίνητη περιουσία. Τη στιγμή που ο buyer επιλέξει να αγοράσει ένα ακίνητο, οι υπόλοιποι χρήστες οφείλουν να κάνουν approve τη συναλλαγή. Στην περίπτωση αυτή, η αξία του NFT, θα αφαιρεθεί απο το υπόλοιπό του και αυτό θα περάσει στην κατοχή του.



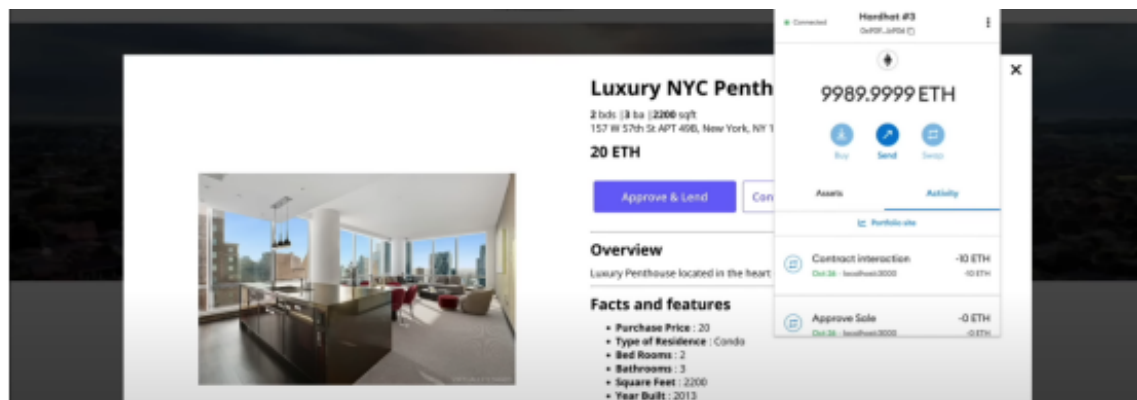
Σχήμα D.25: To User interface απο την πλευρά του πωλητή

Αυτόν του δανειστή, ο οποίος είναι σε θέση να μπορεί να εγκρίνει την επιθεώρηση.



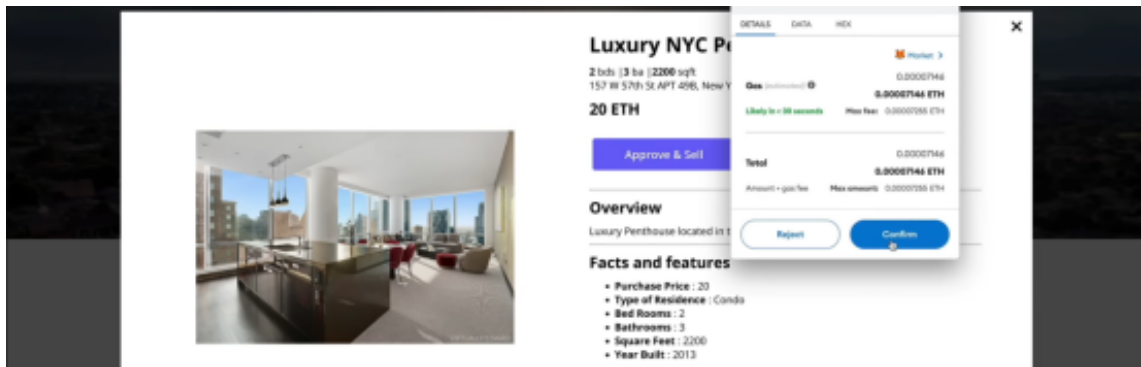
Σχήμα D.26: To User interface απο την πλευρά του Επιθεωρητή

Αυτόν του δανειστή, ο οποίος είναι σε θέση να εγκρίνει τη συναλλαγή και να δανείσει ένα ποσό Ether. Όπως αναφέρθηκε προηγουμένως, εάν ο πωλητής δεν έχει το ακριβές ποσό για την ολοκλήρωση της αγοραπωλησίας, ο δανειστής θα δώσει ένα ποσό ώστε το συνολικό να φτάσει την τιμή πώλησης του ακινήτου.



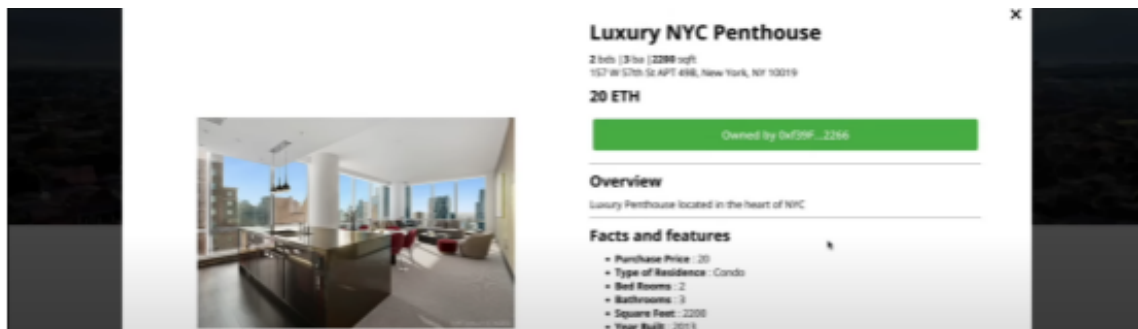
Σχήμα D.27: To User interface απο την πλευρά του lender

Αυτό που απομένει είναι ο πωλητής να εγκρίνει την ιδιοκτησία και να επικυρώσει τη συναλλαγή.



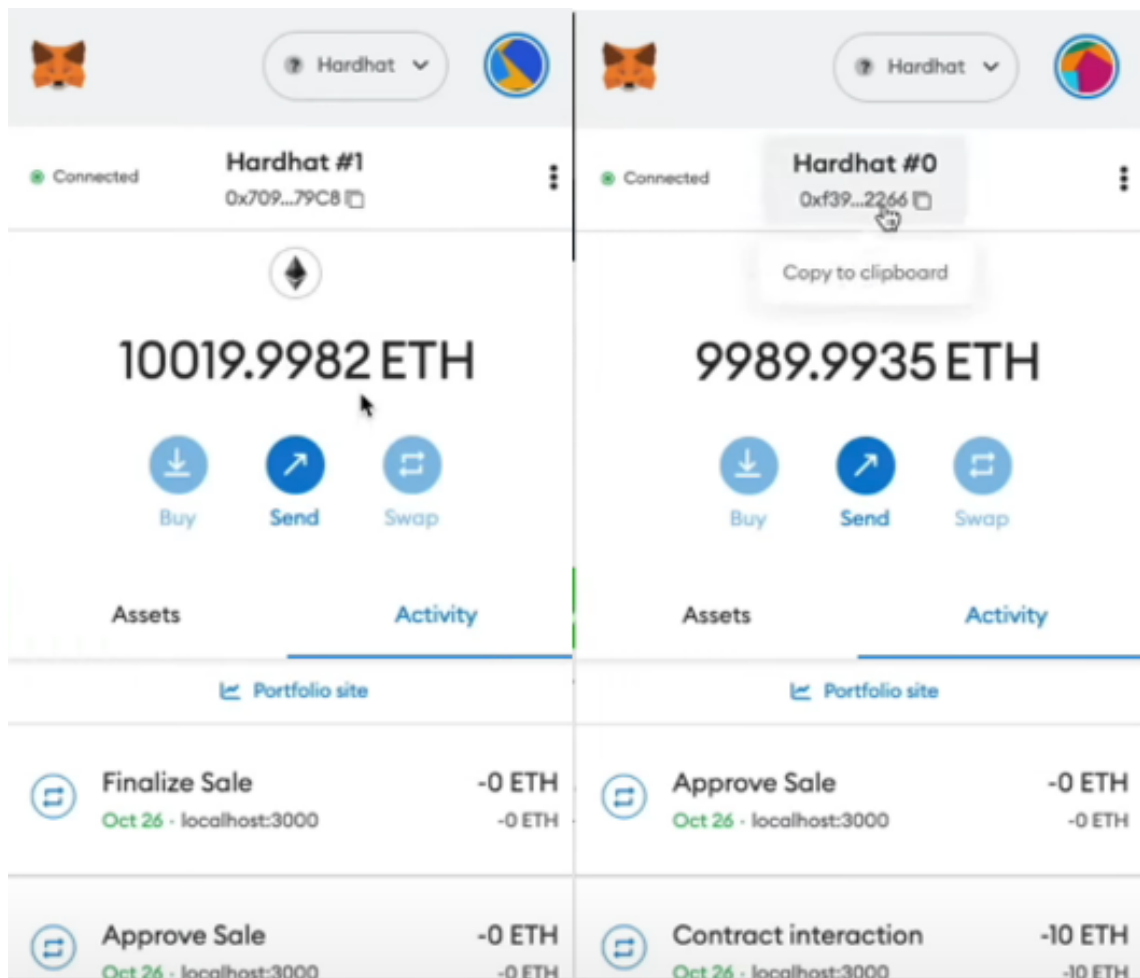
**Σχήμα D.28:** *To User Interface* από την πλευρά του πωλητή

Εάν η ιδιοκτησία μεταφερθεί από τον λογαριασμό του πωλητή και περάσει στο λογαριασμό του αγοραστή, και αν η χρηματική διαφορά είναι ορθή, τότε η συναλλαγή ολοκληρώνεται και το έξυπνο συμβόλαιο είναι πλήρως λειτουργικό.



**Σχήμα D.29:** *To User Interface* τη στιγμή ολοκλήρωσης της συναλλαγής.

Κατά το πέρας της αγοραπωλησίας, εκτός από τη μεταφορά του NFT από τον λογαριασμό του seller, σε αυτόν του buyer, μεταφέρεται και το ποσό του Ether που δαπανήθηκε. Η παρακάτω εικόνα δείχνει το Metamask ψηφιακό πορτοφόλι του πωλητή και του αγοραστή. Οι λογαριασμοί που παρέχονται από το hardhat έχουν υπόλοιπο 100 ETH. Μετά την ολοκλήρωση όμως της συναλλαγής, φαίνεται η διαφορά στα υπόλοιπα των δυο λογαριασμών. Η αξία της ακίνητης περιουσίας μεταφέρθηκε από τον buyer στον seller και επομένως το smart contract λειτούργησε όπως ήταν προγραμματισμένο.



**Σχήμα D.30:** Διαφορά υπολοίπων στους λογαριασμούς του πωλητή και αγοραστή αντίστοιχα, στο ψηφιακό πορτοφόλι του Metamask.

Το πρόγραμμα που υλοποιήθηκε σε αυτήν την πτυχιακή εργασία είναι μια προσομοίωση, με σκοπό την επίδειξη των δυνατοτήτων της τεχνολογίας Blockchain. Παρόλο που η εφαρμογή αναπτύχθηκε τοπικά και χωρίς πραγματικό κόστος υλοποίησης ή επιβάρυνση με φόρους κατά τις συναλλαγές, δεν αποκλίνει από την πραγματικότητα. Όσον αφορά τις αγοραπωλησίες ακινήτων, φάνηκε πως η λειτουργικότητα της τεχνολογίας μπορεί να επωφεληθεί αυτόν τον τομέα. Οι αγοραπωλησίες ακινήτων επιτυγχάνονται γρήγορα χάρη στην αυτοματοποίηση των συμβολαίων και στην έλλειψη κάποιου μεσάζοντα, όπως η τράπεζα, και υπάρχει διαφάνεια καθώς οποιοσδήποτε μπορεί να δει και να εξετάσει αναλυτικά τα έξυπνα συμβόλαια τα οποία

πλέον ζουν αμετάβλητα μέσα στο Blockchain. Το συγκεκριμένο πρόγραμμα μπορεί κάλλιστα να χρησιμοποιηθεί ως θεμέλιο για οποιαδήποτε εφαρμογή που ασχολείται με αγοραπωλησία αγαθών. Αποτελεί μια βάση που χρήζει βελτίωσης και ανάπτυξης, που όμως με το σωστό όραμα και την κατάλληλη δόμηση, έχει τη δυνατότητα να εξελιχθεί σε μια πολλά υποσχόμενη και καινοτόμα εφαρμογή.

## Επίλογος

Από τη στιγμή της εμφάνισης του και του με το Bitcoin, η τεχνολογία όντας πρωτότυπη και διαφορετική από τα δεδομένα της εποχής, εξετάστηκε με πολύ ενδιαφέρον. Το blockchain αρχικά χαρακτηρίστηκε ως μία αποκεντρωμένη τεχνολογία για ψηφιακές συναλλαγές. Με την ανάπτυξη του Ethereum, το blockchain έχει εξελιχθεί σε μια πλατφόρμα που μπορεί να χρησιμοποιηθεί για την υλοποίηση ενός τεράστιου εύρους εφαρμογών. Από τις απλούστερες διεργασίες όπως μια χρηματική συναλλαγή, μέχρι και τις πιο σύνθετες όπως η υποστήριξη της εφοδιαστικής αλυσίδας ή της ηλεκτρονικής ψηφοφορίας.

Αν και η τεχνολογία που υποστηρίζει το Ethereum Blockchain είναι σχετικά καινούργια και για τους περισσότερους πολύπλοκη, η χρήση ποικίλων αποκεντρωμένων εφαρμογών, ο υπερμεγέθης όγκος συναλλαγών και το ενδιαφέρον για συμμετοχή και εξερεύνηση της τεχνολογίας, καθιστούν το Ethereum ένα πολύ χρήσιμο για το παρόν και πολλά υποσχόμενο οικοσύστημα για το μέλλον. Αυτό οφείλεται στο γεγονός ότι εκ κατασκευής, το Ethereum Blockchain προσφέρει εγκυρότητα, διαφάνεια και διαύγεια στις συναλλαγές που καταγράφονται σε αυτό, και ως αποτέλεσμα πολύ μεγαλύτερη ασφάλεια. Οι περισσότεροι χρήστες στρέφονται προς αυτό, διότι αφαιρεί από την εξίσωση τον μεσολαβητή και επιφέρει οικονομικά οφέλη, αλλά και ταχύτητα διεκπεραίωσης των συναλλαγών λόγω της αυτοματοποίησής τους.

Στην εργασία αυτή στο πρώτο -θεωρητικό- μέρος, παρουσιάστηκε το Blockchain, ο τρόπος λειτουργίας του και οι εφαρμογές του, έγινε σύγκριση μεταξύ των κυριότερων κρυπτονομισμάτων και αναλύθηκαν τα χαρακτηριστικά του Ethereum blockchain, και ιδιαίτερα τα έξυπνα συμβόλαια. Στο δεύτερο -πρακτικό- μέρος, σχεδιάστηκε και παρουσιάστηκε μια εφαρμογή αγοραπωλησίας ακίνητων περιουσιών. Ο προγραμματισμός μια εφαρμογής αυτού του είδους, η λογική πίσω από την αρχιτεκτονική της καθώς και οι συναρτήσεις που χρησιμοποιούνται είναι σχετικά απλά. Ωστόσο, η σύνδεση όλων των τμημάτων του κώδικα ώστε η εφαρμογή να είναι πλήρως λειτουργική, διαφέρει από αυτόν μιας συνηθισμένης εφαρμογής.

Λόγω του αμετάβλητου χαρακτήρα του Blockchain, τα smart contracts πρέπει να ελέγχονται εξονυχιστικά ώστε να ελαχιστοποιείται κάθε περιθώριο λάθους. Επίσης, όπως αναλύθηκε στο κεφάλαιο 3.1.5., η χρήση του gas επιβαρύνει κάθε προσπάθεια για συναλλαγή ή deployment. Στον προγραμματισμό της συγκεκριμένης εφαρμογής, δόθηκε ιδιαίτερη έμφαση στον έλεγχο όλης της λειτουργικότητας και της συμπεριφοράς του smart contract. Χάρη στα προηγμένα frameworks που χρησιμοποιήθηκαν, η εφαρμογή αναρτάται σε ένα αντίγραφο του blockchain που λειτουργεί τοπικά και τελικά γίνεται μια ολοκληρωμένη παρουσίαση της αλληλεπίδρασης του χρήστη υπό διαφορετικούς ρόλους.

Η τεχνολογία Blockchain είναι σίγουρα πολλά υποσχόμενη και με εξαιρετικά ευρύ πεδίο εφαρμογών. Ήδη βρίσκεται σε ένα προχωρημένο στάδιο, όμως συνεχίζει να μελετάται σε καθημερινή βάση, έχοντας την υποστήριξη μεγάλου μέρους των ισχυρών της βιομηχανίας. Έχει σίγουρα πτυχές που χρειάζονται βελτίωση και σίγουρα κάποιες που ακόμα δεν έχουν εξερευνηθεί αρκετά. Η χρησιμότητά της ωστόσο στη σύγχρονη κοινωνία είναι πλέον αδιαμφισβήτητη, καθώς τα πάντα ψηφιοποιούνται και το μεγαλύτερο μέρος της ανθρώπινης δραστηριότητας τόσο σε ότι αφορά την εργασία όσο και την καθημερινότητα εκτελείται μέσω του διαδικτύου. Σε ένα τέτοιο περιβάλλον, η ασφάλεια των συναλλαγών καθίσταται ζήτημα πρωταρχικής σημασίας και οι τεχνολογίες που μπορούν να την εξασφαλίσουν, τομέας υψηλής προτεραιότητας για την έρευνα.

Σε αυτό το σημείο, είναι σκόπιμο να σημειωθεί η σημασία και η ανάγκη για περαιτέρω έρευνα και μελέτη τόσο του πεδίου εφαρμογής της τεχνολογίας blockchain, όσο και των κρυπτονομισμάτων. Ήδη θεωρείται ως η τεχνολογία του μέλλοντος λόγω της ασφάλειας και της διαφάνειας που προσφέρει, ειδικά στην σημερινή εποχή που τα περισσότερα δεδομένα αποθηκεύονται ψηφιακά. Όσον αφορά τη συγκεκριμένη πτυχιακή εργασία και το πρόγραμμα που αναπτύχθηκε κατά τη συγγραφή της, μια πιθανή επέκταση θα ήταν η προσθήκη ενός μηχανισμού δημοπρασίας. Κατά αυτή τη διαδικασία, περισσότεροι πιθανοί αγοραστές θα είχαν τη δυνατότητα δήλωσης ενδιαφέροντος για μια ακίνητη περιουσία και μέσω πλειστηριασμού, ως νέος κάτοχος θα ανακηρυσσόταν ο χρήστης με το πιο ανταγωνιστικό ποσό.

## Βιβλιογραφία

All cryptocurrencies | coinmarketcap. <https://coinmarketcap.com/all/views/all/>. (Accessed on 03/07/2023).

Bitcoin energy consumption and sustainability of pow - dec 10, 2021. <https://www.minima.global/post/bitcoin-energy-consumption-and-sustainability-of-pow>. (Accessed on 03/07/2023).

Blockchain - Βικιπαίδεια. <https://el.wikipedia.org/wiki/Blockchain>. (Accessed on 03/07/2023).

Cryptocurrency prices, charts and market capitalizations | coinmarketcap. <https://coinmarketcap.com/>. (Accessed on 03/07/2023).

European commission launches the eu blockchain observatory and forum | shaping europe's digital future. <https://digital-strategy.ec.europa.eu/en/news/european-commission-launches-eu-blockchain-observatory-and-forum>. (Accessed on 03/07/2023).

Top ethereum dapps | dappradar. <https://dappradar.com/rankings/protocol/ethereum>. (Accessed on 03/07/2023).

Types of cryptocurrency and tokens with examples. <https://www.softwaretestinghelp.com/types-of-cryptocurrency/>. (Accessed on 03/07/2023).

What affects the cryptocurrency market? | trading education. <https://trading-education.com/what-affects-the-cryptocurrency-market>. (Accessed on 03/07/2023).

Etherscan. <https://etherscan.io>.

Nasdaq data link. <https://data.nasdaq.com/data/BCHAIN/ETRVU-bitcoin-estimated-transaction-volume-usd>. (Accessed on 03/07/2023).

Αυτό το κολλάζ πωλήθηκε σε ψηφιακή μορφή nft (jpeg) για 69.3 εκατομμύρια δολάρια! | pttl.gr.  
<https://www.pttl.gr/nft-jpeg-sold-for-record-price-at-christies-auction/?fbclid=IwAR11C7eHrcPczfgzzUeW8sZbFwi2hDfpm5f4G9czyNnzCITARDHK82XdU8M>.  
(Accessed on 03/07/2023).

Τι είναι η τεχνολογία blockchain – HBH. <https://www.blockchain.org.gr/home/mathe/>.  
(Accessed on 03/07/2023).

Jameela Al-Jaroodi and Nader Mohamed. Blockchain in industries: A survey. *IEEE Access*, 7:36500–36515, 2019.

Ali Alammery, Samah Alhazmi, Marwah Almasri, and Saira Gillani. Blockchain-based applications in education: A systematic review. *Applied Sciences*, 9(12):2400, 2019.

Hendrik Amler, Lisa Eckey, Sebastian Faust, Marcel Kaiser, Philipp Sandner, and Benjamin Schlosser. Defi-ning defi: Challenges & pathway. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 181–184. IEEE, 2021.

K. Ashford and J. Schmidt. What is cryptocurrency? Forbes Advisor (online), Dec 2020. URL <https://www.forbes.com/advisor/investing/what-is-cryptocurrency/>.

V Bharathan. Blockchain was born 20 years before bitcoin. forbes, 2020.

Preeti Bhaskar, Chandan Kumar Tiwari, and Amit Joshi. Blockchain in education management: present and future applications. *Interactive Technology and Smart Education*, 18(1):1–17, 2021.

Norbert Bodziony, Paweł Jemioło, Krzysztof Kluza, and Marek R Ogiela. Blockchain-based address alias system. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(5):1280–1296, 2021.

Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.

- Fran Casino, Thomas K Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, 36:55–81, 2019.
- Arijit Chakrabarti and Ashesh Kumar Chaudhuri. Blockchain and its scope in retail. *International Research Journal of Engineering and Technology*, 4(7):3053–3056, 2017.
- Guang Chen, Bing Xu, Manli Lu, and Nian-Shing Chen. Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, 5(1):1–10, 2018.
- Michael del Castillo. Chain is now working on six ‘citi-sized’ blockchain networks, 2017.
- Monika Di Angelo and Gernot Salzer. Tokens, types, and standards: identification and utilization in ethereum. In *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, pages 1–10. IEEE, 2020.
- Dmitry Efanov and Pavel Roschin. The all-pervasiveness of the blockchain technology. *Procedia computer science*, 123:116–121, 2018.
- Florence O Ezeudu, Ngozi M Eya, and Hope I Nworgi. Application of blockchain-based technology in chemistry education students’ data management. *International Journal of Database Theory and Application*, 11(2):11–22, 2018.
- Elena P Fedorova and Ella I Skobleva. Application of blockchain technology in higher education. *European Journal of Contemporary Education*, 9(3):552–571, 2020.
- K. Gardner. Introduction to cryptocurrency. Kevin Gardner (online), Nov 2019. URL <https://kevgardner83.medium.com/introduction-to-cryptocurrency-be9bd0c9545e>.
- Baraq Ghaleb, Ahmed Al-Dubai, Elias Ekonomou, Mamoun Qasem, Imed Romdhani, and Lewis Mackenzie. Addressing the dao insider attack in rpl’s internet of things networks. *IEEE Communications Letters*, 23(1):68–71, 2018.
- Cyril Grunspan and Ricardo Pérez-Marco. Selfish mining in ethereum. In *Mathematical Research for Blockchain Economy: 2nd International Conference MARBLE 2020, Vilamoura, Portugal*, pages 65–90. Springer, 2020.

- V. Gupta. A brief history of blockchain. Harvard Business Review (online), Feb 2017. URL <https://hbr.org/2017/02/a-brief-history-of-blockchain>.
- L. Horwitz and L. Rosencrance. How blockchain technology can benefit the internet of things. IoT World Today (online), May 2021. URL <https://www.iotworldtoday.com/2021/05/31/how-blockchain-technology-can-benefit-the-internet-of-things/>.
- Ghassan O Karame, Elli Androulaki, and Srdjan Capkun. Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. *Cryptology EPrint Archive*, 2012.
- Preethi Kasireddy. How does ethereum work, anyway. *published on Medium*, 2017.
- M Kőlvart, M Poola, and A Rull. Smart contracts. the future of law and etechnologies, 133–147, 2016.
- Mahtab Kouhizadeh and Joseph Sarkis. Blockchain practices, potentials, and perspectives in greening supply chains. *Sustainability*, 10(10):3652, 2018.
- Joshua A Kroll, Ian C Davey, and Edward W Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Proceedings of WEIS*, volume 2013. Citeseer, 2013.
- Κωνσταντίνος Λογαράς. Η τεχνολογία blockchain, οι εφαρμογές της και οι νομικές πτυχές της. *naftemporiki. gr, Διαθέσιμο στο Internet: https://www.naftemporiki. gr/story/1363055/i-ternologiablockchain-oi-efarmoges-tis-kai-oi-nomikes-ptures-tis (πρόσβαση στις 21/06/2018)*, 2018.
- Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pages 468–477. IEEE, 2017.
- Antonios Litke, Dimosthenis Anagnostopoulos, and Theodora Varvarigou. Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment. *Logistics*, 3(1):5, 2019.

- Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. Examining usability issues in blockchain-based cryptocurrency wallets. In *Cyber Security and Computer Science: Second EAI International Conference, ICONCS 2020, Dhaka, Bangladesh, February 15-16, 2020, Proceedings 2*, pages 631–643. Springer, 2020.
- Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7:117134–117151, 2019.
- Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, page 21260, 2008.
- Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. *Business & Information Systems Engineering*, 59:183–187, 2017.
- Gareth W Peters, Efstathios Panayi, and Ariane Chapelle. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. *arXiv preprint arXiv:1508.04364*, 2015.
- J. Royal and K. VoigtJun. What is cryptocurrency? here’s what you should know. Nerd-Wallet (online), Jun 2021. URL <https://www.nerdwallet.com/article/investing/cryptocurrency-7-things-to-know#1.-what-is-cryptocurrency>.
- Khaled Salah, M Habib Ur Rehman, Nishara Nizamuddin, and Ala Al-Fuqaha. Blockchain for ai: Review and open research challenges. *IEEE Access*, 7:10127–10149, 2019.
- Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, 62(6):599–608, 2020.
- Janno Siim. Proof-of-stake. In *Research seminar in cryptography*, 2017.
- Kateryna Solodan et al. Legal regulation of cryptocurrency taxation in european countries. *European Journal of Law and Public Administration*, 6(1):64–74, 2019.
- Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In *Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers 19*, pages 507–527. Springer, 2015.

- Witold Srokosz and T Kopciaski. Legal and economic analysis of the cryptocurrencies impact on the financial system stability. *Journal of Teaching and Education*, 4(2):619–627, 2015.
- Melanie Swan. Blockchain: Blueprint for a new economy.—o’reill media. *Inc., Sebastopol, CA*, 2015.
- Dejan Vujičić, Dijana Jagodić, and Siniša Randić. Blockchain technology, bitcoin, and ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)*, pages 1–6. IEEE, 2018.
- Qi Wang, Xiangxue Li, and Yu Yu. Anonymity for bitcoin from secure escrow address. *IEEE Access*, 6:12336–12341, 2017.
- Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.
- Haiyang Yu, Zhen Yang, and Richard O Sinnott. Decentralized big data auditing for smart city environments leveraging blockchain technology. *IEEE Access*, 7:6288–6296, 2018.
- Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105:475–491, 2020.
- A. Τίγκας. Τι Είναι η blockchain: Όλη η Αλήθεια για τις Αμέτρητες Εφαρμογές Της. PC Steps (Online), Μάιος 2021. URL <https://www.pcsteps.gr/214154>.