# ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

**ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

**ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ «ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ»**

**Κατεύθυνση: Προηγμένα Πληροφοριακά Συστήματα**

## Μεταπτυχιακή Διπλωματική Εργασία

# «Δημιουργία Εφαρμογής Blockchain Ethereum και Κρυπτονομίσματος»

**Επιμέλεια: Στεφάνου Κύπρος**
**Α.Μ.: ΜΕ1626**

**Επιβλέπων: Καθηγητής Μαρίνος Θεμιστοκλέους**

**ΠΕΙΡΑΙΑΣ 2018**

## Ευχαριστίες

Κατ, αρχάς θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Θεμιστοκλέους Μαρίνο του Τμήματος Ψηφιακών Συστημάτων για την εμπιστοσύνη που μου έδειξε στην εκπόνηση της παρούσας διπλωματικής εργασίας. Επίσης θα ήθελα να τον ευχαριστήσω για όλες τις υποδείξεις και συμβουλές του, καθώς και για τις γνώσεις που αποκόμισα καθ, όλη την διάρκεια των φοιτητικών μου χρόνων.

Εν συνεχεία, θα ήθελα να ευχαριστήσω τον κ. Βασίλη Νικολόπουλο CEO & Co-founder της εταιρίας Intelen Inc. για την άψογη συνεργασία που είχαμε στα πλαίσια της διπλωματικής μου εργασίας.

Τέλος, ιδιαίτερα θερμές ευχαριστίες θέλω να δώσω στους γονείς μου Χαράλαμπο και Μαρία για την συνεχή συμπαράσταση τους, για τις πολύτιμες συμβουλές τους και για όλα όσα μου έχουν προσφέρει όλα αυτά τα χρόνια της ζωής μου αλλά και των σπουδών μου. Επίσης θέλω να ευχαριστήσω την αδερφή μου Χριστίνα καθώς και την Κατερίνα που με υπομονή και κουράγιο πρόσφεραν την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της μεταπτυχιακής μου εργασίας.

## Περίληψη

Σκοπός της παρούσας διπλωματικής εργασίας είναι η εξέταση της τεχνολογίας που κρύβεται πίσω από τα κρυπτονομίσματα. Η τεχνολογία αυτή είναι το Blockchain και συγκεκριμένα το Blockchain Ethereum, το οποίο είναι μια δημόσια αποκεντρωμένη και κατανεμημένη πλατφόρμα που επιτρέπει σε οποιονδήποτε να δημιουργεί και να χρησιμοποιεί αποκεντρωμένες εφαρμογές που λειτουργούν με αυτή την τεχνολογία.

Η καινοτομία της τεχνολογίας Blockchain δίνει λύση στο ζήτημα που αφορά την συγχρονισμένη καταγραφή δεδομένων σε ένα κατανεμημένο δίκτυο από ανεξάρτητους και άγνωστους μεταξύ τους κόμβους (υπολογιστές), συμφωνώντας ότι τα δεδομένα που αποθηκεύονται κάθε φορά είναι ακριβώς τα ίδια. Όλοι οι υπολογιστές που συμμετέχουν σε ένα δίκτυο Blockchain έχουν ακριβώς τα ίδια δεδομένα χωρίς να μπορούν να τα αλλάξουν ή να τα παραμετροποιήσουν, ενώ η ασφάλεια αυτών των δεδομένων επιτυγχάνεται μέσω της κρυπτογραφίας.

Χρησιμοποιώντας λοιπόν την τεχνολογία Ethereum Blockchain, επιχειρήθηκε η δημιουργία μιας αποκεντρωμένης κατανεμημένης εφαρμογής σε συνεργασία με την εταιρία Intelen Inc. Συγκεκριμένα, έγινε χρήση της τεχνολογίας Blockchain για να επιτευχθεί επικοινωνία μεταξύ έξυπνων οικιακών μπαταριών χωρίς να απαιτείται η παρέμβαση οποιασδήποτε κεντρικής αρχής. Με άλλα λόγια δημιουργήθηκε σχετική εφαρμογή όπου οι έξυπνες μπαταρίες είναι σε θέση να χρησιμοποιήσουν το προσωπικό τους ηλεκτρονικό πορτοφόλι για να ανταλλάζουν κρυπτονομίσματα και πληροφορίες χωρίς την παρέμβαση από τρίτα άτομα.



**Λέξεις Κλειδιά:** Blockchain, DLT, Bitcoin, Ethereum, Cryptocurrencies, Consensus Algorithms, Token ERC20, HD Wallet, testRPC, Solidity, Remix-IDE.

## Abstract

The purpose of this master thesis is to examine the technology behind cryptocurrencies. This technology is called “Blockchain”, and to be specific “Blockchain Ethereum”, which is a public decentralized and distributed platform that allows anyone to create and use decentralized Blockchain-based applications.

The innovation of Blockchain technology provides a solution to the issue of synchronous data logging in a distributed network of independent and unknown nodes (computers), agreeing that the data being stored is exactly the same. All computers participating in a Blockchain network have exactly the same data without being able to change or customize them and data security is accomplished through cryptography.

Using Ethereum Blockchain technology, a decentralized distributed application was developed in collaboration with Intelen Inc. Particularly, Blockchain technology was utilized to achieve communication between smart home batteries without the necessity of intervention of any central authority. In other words, I have developed an application where smart batteries are able to use their personal electronic wallet to exchange cryptocurrencies and information without the need of third-party intervention.

**Key Words:** Blockchain, DLT, Bitcoin, Ethereum, Cryptocurrencies, Consensus Algorithms, Token ERC20, HD Wallet, testRPC, Solidity, Remix-IDE.

## Περιεχόμενα

## Εισαγωγή

Η αλματώδης ανάπτυξη της πληροφορικής και της ψηφιοποίησης των δεδομένων συνέβαλε, μεταξύ άλλων, στην δημιουργία ενός νέου ψηφιακού κρυπτονομίσματος. Η ιδέα της δημιουργίας του ψηφιακού κρυπτονομίσματος με βάση την καινοτόμο τεχνολογία Blockchain προτάθηκε από ένα άτομο ή μια ομάδα ατόμων με το ψευδώνυμο Satoshi Nakamoto δημοσιεύοντας το 2008 σχετικό άρθρο (Nakamoto, S. 2017). Το 2009 υλοποιήθηκε το ψηφιακό κρυπτονόμισμα με ονομασία Bitcoin και άρχισε να χρησιμοποιείται σε όλο τον κόσμο ταράζοντας τα νερά της οικονομίας. Μετά από 6 χρόνια ένας νεαρός Καναδός προγραμματιστής με το όνομα Vitalik Buterin δημιούργησε ένα άλλο κρυπτονόμισμα με την ονομασία Ether, το οποίο έλαβε την ίδια αποδοχή από τον κόσμο όπως έγινε και με το Bitcoin (Antonopoulos, 2017).

Με αφορμή τα κρυπτονομίσματα bitcoin και ether έχει ξεκινήσει μια «μεγάλη τεχνολογική επανάσταση» στον κόσμο, η οποία βασίζεται στη χρήση της τεχνολογίας Blockchain, τεχνολογία η οποία έχει μετατραπεί σε ένα από τα πιο πολυσυζητημένα τεχνολογικά επιτεύγματα με επενδύσεις δισεκατομμυρίων ευρώ και μια ολόκληρη βιομηχανία να κτίζεται πάνω στις βάσεις της. Τα κύρια χαρακτηριστικά που καθιστούν το Blockchain ελκυστικό ως καινούργια τεχνολογία, είναι ο αποκεντρωμένος σχεδιασμός του και το γεγονός ότι δεν απαιτείται εμπιστοσύνη μεταξύ των χρηστών. Τα δεδομένα που ανταλλάζονται δεν βρίσκονται σε κεντρικό διακομιστή (Server), αλλά σε ένα κατανεμημένο δίκτυο από συνεργαζόμενους εθελοντές.

Σκοπός της παρούσας διπλωματικής εργασίας είναι η εξέταση της τεχνολογίας Blockchain, και συγκεκριμένα το Blockchain Ethereum. Πιο αναλυτικά επιχειρήθηκε η δημιουργία μιας αποκεντρωμένης κατανεμημένης εφαρμογής σε συνεργασία με την εταιρία Intelen Inc., η οποία ασχολείται με τη διαχείριση του ηλεκτρικού ρεύματος και συγκεκριμένα με τις έξυπνες οικιακές μπαταρίες. Αναλυτικότερα, έγινε χρήση της τεχνολογίας Blockchain για να επιτευχθεί η επικοινωνία μεταξύ έξυπνων οικιακών μπαταριών χωρίς να απαιτείται η παρέμβαση ενός τρίτου παράγοντα προκειμένου να επαληθεύει τα δεδομένα που ανταλλάζονται. Με άλλα λόγια οι έξυπνες μπαταρίες έχουν την δυνατότητα να ανταλλάξουν κρυπτονομίσματα και δεδομένα χωρίς την παρέμβαση οποιασδήποτε κεντρικής αρχής.

Πιο αναλυτικά στα πλαίσια της διπλωματικής μου εργασίας σχεδιάστηκαν και υλοποιήθηκαν τα ακόλουθα:

I. HD Wallet το οποίο είναι ένα από τα πιο προηγμένα και ασφαλή ηλεκτρονικά πορτοφόλια για διευθύνσεις (addresses) που αφορούν το Ethereum Blockchain.
II. Κρυπτονόμισμα με βάση το ERC20 standard και τη γλώσσα προγραμματισμού Solidity.
III. Smart Contract για την αποστολή και λήψη κρυπτονομισμάτων.
IV. Κώδικας ο οποίος θα επικοινωνεί με το δίκτυο Ethereum και με το Smart Contract έτσι ώστε να λαμβάνει πληροφορίες σχετικά με τις συναλλαγές των χρηστών και των έξυπνων οικιακών μπαταριών.

Αναφορικά με τη δομή της εργασίας, στο δεύτερο κεφάλαιο επιχειρήθηκε η αποσαφήνιση ορισμένων εννοιών οι οποίες χρησιμοποιούνται ευρέως στην παρούσα εργασία προκειμένου να καταστεί κατανοητό το περιεχόμενο της. Στο τρίτο κεφάλαιο πραγματοποιείται μια εκτενής αναφορά στο Bitcoin, αφού είναι το πρώτο κρυπτονόμισμα που χρησιμοποιεί την τεχνολογία Blockchain.

Στο τέταρτο κεφάλαιο εξετάζεται η τεχνολογία Blockchain, οι τύποι, η αρχιτεκτονική της αλλά και οι μηχανισμοί που είναι απαραίτητοι προκειμένου να διατηρηθεί η εμπιστοσύνη σε ένα Blockchain δίκτυο. Εν συνεχεία στο πέμπτο κεφάλαιο μελετάται η έννοια του έξυπνου συμβολαίου (Smart Contract) στον κόσμο του Blockchain.

Ακολουθεί το έκτο κεφάλαιο όπου παρουσιάζεται το «State of The Art», δηλαδή εξετάζονται και παρουσιάζονται οι πιο πρόσφατες υπηρεσίες που χρησιμοποιούν την τεχνολογία Blockchain για την αποστολή ρεύματος μεταξύ νοικοκυριών.

Έπειτα στο έβδομο κεφάλαιο παρουσιάζεται και αναλύεται το πρόβλημα που επιχειρήθηκε να επιλυθεί στο πλαίσιο της παρούσας διπλωματικής εργασίας καθώς και η λύση του προβλήματος. Στο όγδοο κεφάλαιο γίνεται αναφορά στις τεχνολογίες και τα εργαλεία που χρησιμοποιήθηκαν για την επίλυση του προβλήματος. Τέλος, στον επίλογο διατυπώνονται κάποιες συμπερασματικές σκέψεις για την τεχνολογία Blockchain και ακολουθεί η παράθεση των βιβλιογραφικών πηγών που αξιοποιήθηκαν.

## Εισαγωγικές έννοιες

Στο σημείο αυτό κρίνεται σκόπιμη η αποσαφήνιση ορισμένων εννοιών οι οποίες χρησιμοποιούνται ευρέως στην παρούσα εργασία προκειμένου να καταστεί κατανοητό το περιεχόμενο της.

- **Bitcoin**

  Το **B**itcoin χρησιμοποιείται όταν περιγράφουμε την έννοια του Bitcoin ή ολόκληρο το δίκτυο. π.χ. "Μάθατε για το πρωτόκολλο Bitcoin σήμερα."

- **bitcoin**

  Το **b**itcoin χρησιμοποιείται για να περιγράψει τα bitcoins ως μονάδα ενός λογαριασμού. π.χ. "Έστειλα δέκα bitcoins σήμερα."

- **Βιβλιάριο**

  -Το βιβλιάριο (ledger) είναι ένα ψηφιακό αρχείο καταγραφής δεδομένων, ένα σύνολο από πληροφορίες και χρησιμεύει ως "δοχείο" για την αποθήκευση της πληροφορίας.
  -Δημόσιο βιβλιάριο είναι το αρχείο στο οποίο όλοι έχουν πρόσβαση να διαβάσουν τα δεδομένα που περιέχει.
  -Κατανεμημένο βιβλιάριο είναι το βιβλιάριο το οποίο είναι αποθηκευμένο σε περισσότερους από ένα υπολογιστές. Στον κάθε υπολογιστή το βιβλιάριο περιέχει ακριβώς τα ίδια δεδομένα.

- **Συναλλαγή**

  Ο όρος συναλλαγή αναφέρεται στη συναλλακτική δραστηριότητα μεταξύ δύο ή περισσοτέρων προσώπων. Συναλλακτική δραστηριότητα είναι η συμφωνία των μερών για ανταλλαγή πληροφοριών-δεδομένων. Κάθε συναλλαγή καταγράφεται στο βιβλιάριο (ledger).

- **Κρυπτογραφία**

  Η κρυπτογραφία αναφέρεται στη «διαδικασία» την οποία χρησιμοποιούμε για να "μεταμφιέσουμε" μια πληροφορία (ένα κείμενο, έναν αριθμό, ένα αρχείο), έτσι ώστε να μην βγάζει κανένα απολύτως νόημα στα μάτια τρίτων προσώπων. Η αντίστροφη

διαδικασία περιλαμβάνει την εφαρμογή ενός αλγορίθμου στα κρυπτογραφημένα δεδομένα ώστε να πάρουμε ξανά τα αρχικά δεδομένα και ονομάζεται αποκρυπτογράφηση.

Στη μέθοδο της κρυπτογράφησης και της αποκρυπτογράφησης υπάρχουν δύο ζεύγη κλειδιών:

a. Το Public key, το οποίο είναι δημόσιο, όπως μια διεύθυνση ηλεκτρονικού ταχυδρομείου και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων.
b. Το Private Key το οποίο είναι μυστικό και συνδέεται μαθηματικά με το Public Key, είναι απαραίτητο για την αποκρυπτογράφηση των δεδομένων. Χαρακτηριστικό παράδειγμα ενός Private key αποτελεί ο κωδικός πρόσβασης που απαιτείται για την είσοδο σε μια διεύθυνση ηλεκτρονικού ταχυδρομείου.

- **Κόμβος (Node)**

  Ως Node ή αλλιώς Κόμβος μπορεί να χαρακτηριστεί οποιαδήποτε ενεργή ηλεκτρονική συσκευή που μπορεί να επικοινωνήσει με άλλες συσκευές μέσω διαδικτύου.

  Παραδείγματα συσκευών κόμβων αποτελούν τα modem, τα hub, τα switch, τα κινητά τηλέφωνα, οι εκτυπωτές, οι υπολογιστές και οι διακομιστές (Servers). Στην παρούσα εργασία ένας κόμβος είναι ένας ηλεκτρονικός υπολογιστής ο οποίος επικοινωνεί με άλλους υπολογιστές.

- **Bitcoin Δίκτυο ( Bitcoin Network )**

  Ο όρος Bitcoin Δίκτυο αναφέρεται σε ένα σύνολο από κόμβους οι οποίοι εκτελούν το πρωτόκολλο Bitcoin.

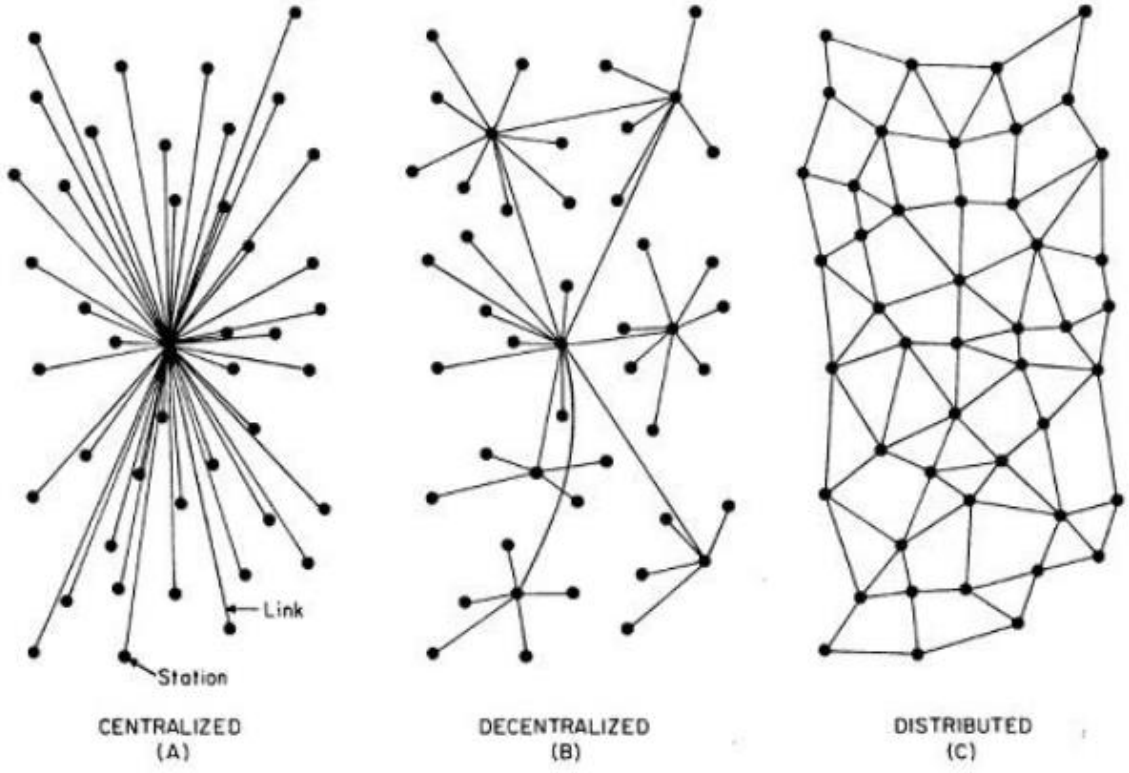
- **Hash**

  Το Hash είναι 64 αλφαριθμητικοί χαρακτήρες οι οποίοι προκύπτουν αφού εκτελέσουμε τον αλγόριθμο κρυπτογράφησης SHA-256 (Secure Hash Algorithm), ο οποίος κρυπτογραφεί τα δεδομένα και επιστρέφει πάντα ένα μοναδικό αλφαριθμητικό Hash 64 χαρακτήρων, το οποίο ισοδυναμεί με 32 byte. Η λειτουργία του αλγορίθμου χαρακτηρίζεται ως μη αντιστρέψιμη και λειτουργεί σαν ψηφιακό αποτύπωμα το οποίο είναι μοναδικό και δεν μπορεί να αποκρυπτογραφηθεί.

- **Μπλοκ (Block)**

  Το μπλοκ είναι ένα σύνολο (ή δέσμη) από δεδομένα.

- **Τύποι εφαρμογών λογισμικού**




Εικόνα 1: Παρουσίαση 3 τύπων εφαρμογών λογισμικού . Ανακτήθηκε από το βιβλίο: *Decentralized Applications* (Siraj Raval, 2016). Δεκέμβρης 3, 2017.

Στην πιο πάνω εικόνα οι τελείες αντιπροσωπεύουν τους κόμβους και οι γραμμές τις συνδέσεις μεταξύ των κόμβων.

**A. Centralized network**

Ο όρος κεντρικό δίκτυο αναφέρεται σε ένα κεντρικό σύστημα, όπου οι κόμβοι (ηλεκτρονικοί υπολογιστές) είναι όλοι συνδεδεμένοι με ένα κεντρικό υπολογιστή σε συγκεκριμένη τοποθεσία. Ο κεντρικός αυτός υπολογιστής χρησιμοποιείται ως μέσο επικοινωνίας μεταξύ των συνδεδεμένων υπολογιστών. Το πρόβλημα με αυτό το είδος υποδομής είναι ότι αν η κεντρική αρχή καταρρεύσει τότε ολόκληρο το σύστημα δεν θα λειτουργεί.

**B. Decentralized network**

Το αποκεντρωμένο δίκτυο παρουσιάζει ένα δίκτυο από πολλούς κεντρικούς κόμβους και διάφορους άλλους υπολογιστές συνδεδεμένους με αυτούς. Αν μερικοί από τους κύριους κόμβους καταρρεύσουν, τότε το σύστημα στο σύνολό του θα λειτουργεί κανονικά αφού τη θέση τους θα πάρουνε οι υπόλοιποι διαθέσιμοι κόμβοι και η επικοινωνία θα επιτυγχάνεται μέσω αυτών.

**C. Distributed network**

Το κατανεμημένο δίκτυο αποτελείται από κόμβους οι οποίοι είναι σχεδόν όλοι συνδεδεμένοι μεταξύ τους και η επικοινωνία επιτυγχάνεται χωρίς τη βοήθεια κεντρικού κόμβου. Αν μέρος του δικτύου καταρρεύσει το δίκτυο θα συνεχίσει να λειτουργεί κανονικά, αφού η επικοινωνία μπορεί να γίνεται μέσω των υπολοίπων κόμβων.

- **P2P:**

Ο όρος peer-to-peer ή P2P σημαίνει ότι οι υπολογιστές που συμμετέχουν στο δίκτυο είναι ομότιμοι μεταξύ τους, ότι είναι όλοι ίσοι, ότι δεν υπάρχουν ειδικοί κόμβοι και ότι όλοι οι κόμβοι μοιράζονται τις υπηρεσίες δικτύου. Οι κόμβοι δικτύου αλληλοσυνδέονται σε ένα δίκτυο πλέγματος με μια "επίπεδη" τοπολογία ενώ δεν υπάρχει καμία κεντρική υπηρεσία και καμία ιεραρχία εντός του δικτύου. Τα δίκτυα "peer-to-peer" είναι εγγενώς ανθεκτικά, αποκεντρωμένα και μπορεί ο οποιοσδήποτε να συμμετέχει. Το κύριο παράδειγμα μιας αρχιτεκτονικής δικτύου P2P ήταν το ίδιο το αρχικό Ίντερνετ, αλλά και το Bitcoin, όπου οι κόμβοι στο δίκτυο είναι ίσοι.

- **Κρυπτονόμισμα (Cryptocurrencies)**

  Ένα κρυπτο-νόμισμα είναι ένα ψηφιακό νόμισμα το οποίο έχει αξία και έχει σχεδιαστεί για να λειτουργεί ως μέσο συναλλαγής. Στα κρυπτονομίσματα χρησιμοποιείται κρυπτογραφία (εξίσου και το όνομα κρυπτονόμισμα) για να διασφαλιστούν οι συναλλαγές χωρίς να μπορεί κάποιος να αλλοιώσει τα δεδομένα αφού θα είναι κρυπτογραφημένα.

- **Tokens**

  Το Token μπορεί να χαρακτηριστεί ως ένα ψηφιακό αγαθό (digital asset). Είναι ένα κλειδί, που πιστοποιεί με μονοσήμαντο τρόπο, ότι το πρόσωπο που το κατέχει είναι και ο ιδιοκτήτης μιας αξίας. Τα Tokens μπορούν να αντιστοιχούν σε φυσικά assets τα οποία μπορούν να χρησιμοποιηθούν από τους ιδιοκτήτες τους ή να καταναλωθούν έναντι κάποιου προϊόντος υπηρεσίας ή πλατφόρμας. Μπορούν να χρησιμοποιούνται ως εσωτερικές μονάδες για την αγορά αγαθών ή υπηρεσιών. Η συμμετοχή σε μια τέτοια διαδικασία προϋποθέτει την αγορά των Tokens με χρήση fiat currency (π.χ ευρώ) ή με συμβατό κρυπτονόμισμα (π.χ bitcoin, ether). Τα **crypto-tokens** κατά βάση είναι διαθέσιμα σε μια κατανεμημένη βάση τύπου Blockchain ώστε να υποστηρίζονται οι προϋποθέσεις πιστοποίησης των συναλλαγών και ελέγχου από την κοινότητα των χρηστών.

## 1. Η ιστορία του Bitcoin

Το Bitcoin και η τεχνολογία Blockchain παρουσιάστηκαν στον κόσμο την Παρασκευή 31 Οκτωβρίου 2008 με τη δημοσίευση του άρθρου "Bitcoin: A Peer-to-Peer Electronic Cash System", το οποίο γράφτηκε από άγνωστο συγγραφέα που χρησιμοποίησε το ψευδώνυμο Satoshi Nakamoto (Nakamoto, 2008). Ο Nakamoto συνδυάζοντας αρκετές προγενέστερες εφευρέσεις και τεχνολογίες δημιούργησε για πρώτη φορά στην ιστορία ένα πλήρως αποκεντρωμένο ηλεκτρονικό σύστημα πληρωμών. Μέσα από αυτό το σύστημα μπορεί να μεταφερθεί αξία (bitcoins) μεταξύ 2 άγνωστων ανθρώπων χωρίς καμιά κεντρική αρχή για την επικύρωση των συναλλαγών (Antonopoulos, 2017, Laurence, 2017).

Το 2009 ο Nakamoto δημοσίευσε το Bitcoin ως λογισμικό ανοιχτού κώδικα και με την βοήθεια εθελοντών προγραμματιστών εξελίχθηκε ο κώδικας και το πρωτόκολλο (Antonopoulos, 2017). Τον Απρίλιο του 2011, ο Nakamoto αποσύρθηκε από το κοινό αφήνοντας την ευθύνη της ανάπτυξης του Bitcoin στους υπόλοιπους εθελοντές προγραμματιστές. Όμως η ταυτότητα του ατόμου ή της ομάδας των ανθρώπων που βρίσκονται πίσω από την αρχική δημιουργία του Bitcoin είναι ακόμα άγνωστη. (Antonopoulos, 2017). Θα πρέπει να διευκρινιστεί εντούτοις ότι κανείς δεν είναι ιδιοκτήτης του Bitcoin όπως ακριβώς και κανένας δεν είναι ιδιοκτήτης της τεχνολογίας του Internet.

Το λογισμικό και το πρωτόκολλο του Bitcoin εκδίδονται ανοιχτά προς όλους και οποιοσδήποτε μπορεί να επιθεωρήσει τον κώδικα. Οι προγραμματιστές οι οποίοι βελτιώνουν το λογισμικό, δεν μπορούν να εξαναγκάσουν καμία αλλαγή στο πρωτόκολλο Bitcoin γιατί αυτό θα μπορούσε να επηρεάσει ολόκληρο το σύστημα συναλλαγών bitcoin. Αναφορικά με το περιεχόμενο του πρωτοκόλλου, αυτό περιέχει τους κανόνες τους οποίους όλοι οι χρήστες Bitcoin πρέπει να ακολουθούν αλλά και το είδος των δεδομένων τα οποία δύνανται να ανταλλάζονται. Θα πρέπει να επισημανθεί ότι σε περίπτωση που κάποιος χρήστης Bitcoin διαφωνήσει με τους κανόνες λειτουργίας του, δεν έχει τη δυνατότητα να παρέμβει επιβάλλοντας τους δικούς του κανόνες στους υπόλοιπους χρήστες, διότι καθίσταται αδύνατη η αλλαγή του πρωτοκόλλου. Άλλωστε η αλλαγή του πρωτοκόλλου δύναται να επιτευχθεί μόνο με τη συνεργασία όλων των χρηστών , οι οποίοι επιλέγουν ποιο λογισμικό θα χρησιμοποιήσουν. Το λογισμικό, με τη σειρά του, συλλέγει τις συναλλαγές που

πραγματοποιούνται μεταξύ ομότιμων (peer-to-peer) μέσω του δικτύου και εκτελεί τις κατάλληλες λειτουργίες για να επεξεργαστεί και να επιβεβαιώσει τις συναλλαγές χρησιμοποιώντας το πρωτόκολλο Bitcoin.

Άξιο αναφοράς κρίνεται το γεγονός ότι το Bitcoin μπορεί να λειτουργήσει σωστά μόνο με την πλήρη συναίνεση όλων των χρηστών, αφού οι κανόνες λειτουργούν με μαθηματικές αρχές. Ως εκ τούτου, όλοι οι χρήστες και οι προγραμματιστές έχουν ισχυρό κίνητρο να προστατεύουν αυτήν την αρχή λειτουργίας (Antonopoulos, 2017).

Η βασική καινοτομία της τεχνολογίας Blockchain είναι ο συνδυασμός ενός κατανεμημένου δημόσιου βιβλιαρίου καταγραφής συναλλαγών (distributed ledger) μαζί με ένα έμπιστο μηχανισμό, ο οποίος επιβεβαιώνει την ακεραιότητα και την ορθότητα της κάθε συναλλαγής χωρίς να απαιτείται η παρέμβαση από κάποιο ενδιάμεσο ή κάποια κεντρική αρχή. Κάθε 10 λεπτά περίπου επικυρώνονται και καταγράφονται οι συναλλαγές στο δημόσιο βιβλιάριο στο οποίο τα δεδομένα δεν μπορούν να αλλάξουν, ούτε να διαγραφούν. Αυτό το βιβλιάριο περιέχει όλες τις συναλλαγές που πραγματοποιούνται και επιτρέπει στον υπολογιστή του χρήστη να εξακριβώνει την εγκυρότητα της κάθε συναλλαγής που πραγματοποιεί. Ο αλγόριθμος ο οποίος χρησιμοποιείται από το λογισμικό για την επιβεβαίωση και την έγκυρη καταγραφή των συναλλαγών στο βιβλιάριο ονομάζεται Proof-of-Work (PoW). Με βάση λοιπόν αυτόν τον αλγόριθμο και το κατανεμημένο βιβλιάριο οι χρήστες του συστήματος δεν μπορούν να ξοδέψουν τα ηλεκτρονικά τους νομίσματα (bitcoins) 2 φορές γιατί το βιβλιάριο είναι συγχρονισμένο με κάθε άλλο βιβλιάριο και έτσι υπάρχει εμπιστοσύνη ακόμη και μεταξύ ανώνυμων χρηστών. Μάλιστα, η αυθεντικότητα της κάθε συναλλαγής προστατεύεται από ψηφιακές υπογραφές, επιτρέποντας έτσι στους χρήστες να ελέγχουν πλήρως την αποστολή των bitcoins τους (Antonopoulos, 2017, Swan, 2015**,** Laurence, 2017).

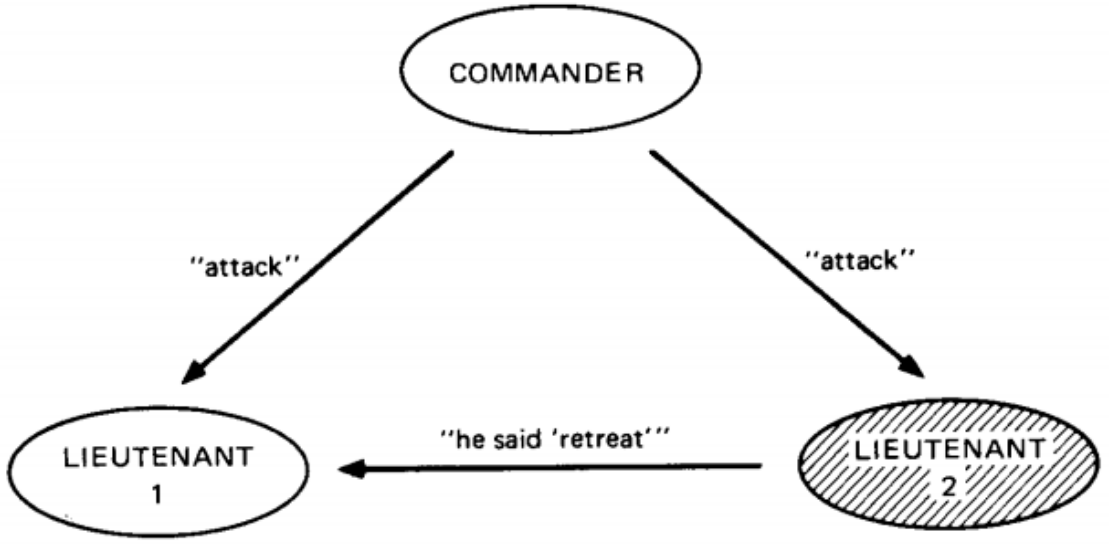
Η ιδέα του αλγορίθμου Proof-of-Work σε συνδυασμό με το κατανεμημένο βιβλιάριο έλυσε ένα ακόμη μεγάλο πρόβλημα στο χώρο της πληροφορικής γνωστό και ως «πρόβλημα των βυζαντινών στρατηγών», το οποίο έχει ως στόχο την επίτευξη του συγχρονισμού, της εμπιστοσύνης και της ακεραιότητας των πληροφοριών που ανταλλάζονται σε ένα αναξιόπιστο κατανεμημένο δίκτυο (Antonopoulos, 2017, Laurence, 2017).

Το «πρόβλημα των βυζαντινών στρατηγών» περιγράφηκε αρχικά από τους Marshall Pease, Robert Shostak και Leslie Lamport το 1982 και βασίστηκε στο σενάριο ότι τμήματα του Βυζαντινού στρατού που έχουν κατασκηνώσει έξω από τα τείχη μιας εχθρικής πόλης αντιμετωπίζουν προβλήματα με τη δημιουργία ενός κοινού σχεδίου δράσης λόγω της πιθανότητας μετάδοσης αναξιόπιστων πληροφοριών. Πιο αναλυτικά, το κάθε τμήμα διοικείται από το δικό του στρατηγό και έχει αποφασιστεί ότι μετά από μία συγκεκριμένη περίοδο παρακολούθησης των εχθρών θα πρέπει όλοι οι στρατηγοί να συμφωνήσουν σε ένα κοινό σχέδιο δράσης. Προκειμένου λοιπόν να επιτευχθεί η απαραίτητη επικοινωνία και ο συντονισμός όλων των στρατηγών είναι απαραίτητο να μεταφερθούν οι απαραίτητες πληροφορίες και ειδήσεις από το ένα τμήμα του στρατού στο άλλο. Στο σημείο αυτό θα πρέπει να αναφερθεί ότι στη δεδομένη ιστορική περίοδο η μετάδοση πληροφοριών γινόταν αποκλειστικά και μόνο με αγγελιαφόρους του κάθε στρατεύματος. Εντούτοις, αυτή η μέθοδος μετάδοσης των πληροφοριών δημιουργεί κινδύνους παραποίησης της πληροφορίας, διότι ορισμένοι πληροφοριοδότες οι οποίοι έχουν προδώσει το στράτευμά τους και έχουν συμμαχήσει με τους αντιπάλους, έχουν τη δυνατότητα να μεταδώσουν ψευδείς πληροφορίες, προκειμένου να εμποδίσουν τους (νομοταγείς) στρατηγούς να έρθουν σε συμφωνία.

Με βάση λοιπόν τα όσα προαναφέρθηκαν καθίσταται σαφές ότι οι στρατηγοί πρέπει να χρησιμοποιούν έναν αλγόριθμο ο οποίος να εγγυάται ότι :

I. Το σχέδιο δράσης που πρόκειται να υλοποιηθεί αποτελεί ομόφωνη απόφαση όλων των εμπλεκόμενων στρατηγών.
II. Η ενδεχόμενη ύπαρξη ενός περιορισμένου αριθμού πληροφοριοδοτών που έχουν προδώσει το στράτευμά τους δεν θα οδηγήσει στην παραποίηση των στοιχείων και ως εκ τούτου στην υιοθέτηση ενός επιβλαβούς σχεδίου δράσης.

Στην εικόνα 2 απεικονίζεται ένα παράδειγμα παραποίησης των εντολών που πρέπει να μεταφερθούν από ένα τμήμα του στρατού σε κάποιο άλλο. Αναλυτικότερα, ο στρατηγός (Commander) δίνει εντολή επίθεσης (attack) στους 2 λοχαγούς (Lieutenant) αλλά ο λοχαγός 2 (Lieutenant 2) είναι προδότης και παραποιεί την εντολή σε υποχώρηση (retreat).




Εικόνα **2:** . Παράδειγμα παραποίησης εντολών. Ανακτήθηκε από dl.acm.org: Άρθρο τους Marshall Pease, Robert Shostak και Leslie Lamport, Ανακτήθηκε Δεκέμβρης 3, 2017.

Καθίσταται λοιπόν φανερό ότι χωρίς την ύπαρξη συγχρονισμού και ακεραιότητας στις πληροφορίες που ανταλλάζονται, είναι αδύνατη η υλοποίηση ενός ομόφωνου και αξιόπιστου σχεδίου δράσης, διότι είναι πάντα υπαρκτός ο κίνδυνος μεταφοράς παραποιημένων εντολών από «προδότες» πληροφοριοδότες.

Λύση στο «Πρόβλημα των Βυζαντινών Στρατηγών» δόθηκε όπως προαναφέρθηκε με τη δημιουργία του αλγορίθμου Proof-of-Work, ο οποίος λειτουργεί σε συνδυασμό με το κατανεμημένο βιβλιάριο, συγχρονίζοντας τα δεδομένα και εμποδίζοντας την ανταλλαγή εσφαλμένων μηνυμάτων, συνθήκη απαραίτητη διότι στο κατανεμημένο σύστημα συμμετέχουν χιλιάδες ή και εκατομμύρια χρήστες.

# 2. Blockchain

Η τεχνολογία Blockchain έγινε αρχικά γνωστή μέσα από την λειτουργία του Bitcoin. Σύντομα όμως οι χρήστες της συγκεκριμένης τεχνολογίας συνειδητοποίησαν ότι το Blockchain έχει πολύ μεγαλύτερες δυνατότητες, μέσα από τις οποίες μπορεί να αλλάξει ολόκληρο το διαδίκτυο. Χαρακτηριστική είναι η δήλωση των Tapscott και Tapscott (2016) οι οποίοι χαρακτηρίζουν το Blockchain ως το "*έμπιστο πρωτόκολλο*" που τόσα χρόνια έλειπε από το διαδίκτυο. Επίσης, αναφέρουν ότι *τόσα χρόνια μέσα από το διαδίκτυο μπορούσαμε να μεταφέρουμε δεδομένα, ενώ τώρα μας δίνεται η δυνατότητα να μεταφέρουμε αξία* (Tapscott & Tapscott, 2016).

## 2.1. Εισαγωγή στο Blockchain

Το Blockchain είναι ένα αποκεντρωμένο και κατανεμημένο βιβλιάριο που χρησιμοποιείται για την καταγραφή δεδομένων σε ένα δίκτυο από ανεξάρτητους και άγνωστους μεταξύ τους χρήστες. Αυτό το κοινόχρηστο βιβλιάριο μπορεί να χρησιμοποιηθεί για την καταγραφή δεδομένων οποιασδήποτε μορφής. Στο σημείο αυτό θα πρέπει να διευκρινιστεί ότι τα δεδομένα διακρίνονται σε φυσικά και άυλα. Παραδείγματα φυσικών δεδομένων αποτελούν οι τίτλοι ιδιοκτησίας ενός σπιτιού ή ενός αυτοκινήτου ενώ ο όρος άυλο δεδομένο αναφέρεται στην πνευματική ιδιοκτησία (πνευματικά δικαιώματα και πατέντες). Στην πραγματικότητα, οτιδήποτε έχει αξία μπορεί να καταχωρηθεί και να διακινηθεί σε ένα δίκτυο Blockchain (Laurence, 2017 , Gupta, 2017 , Tapscott & Tapscott, 2016)

Το Blockchain οφείλει την ονομασία του στον τρόπο με τον οποίο αποθηκεύονται οι συναλλαγές δεδομένων σε αυτό. Πιο συγκεκριμένα, οι συναλλαγές, αφού ελεγχθούν με βάση τους κανόνες που έχουν προσυμφωνηθεί από τους συμμετέχοντες στο δίκτυο, τοποθετούνται με χρονολογική σειρά σε ομάδες που ονομάζονται **μπλοκ**. Τα μπλοκ συνδέονται μεταξύ τους όπως μια αλυσίδα.
Κάθε μπλοκ περιέχει το κλειδί του προηγούμενου μπλοκ και τις έγκυρες συναλλαγές, οι οποίες έχουν ελεγχθεί και καταχωρηθεί μέσα στο μπλοκ. Στο σημείο αυτό κρίνεται σκόπιμο να αναφερθεί ότι το κλειδί του κάθε μπλοκ μοιάζει με ψηφιακό δακτυλικό αποτύπωμα γιατί είναι μοναδικό. Επιπλέον, τα κλειδιά συνδέουν τα μπλοκ μεταξύ τους και εμποδίζουν την εισαγωγή ενός τρίτου μπλοκ μεταξύ δύο συνδεδεμένων μπλοκ, έτσι ώστε να μη διαταραχθεί η υπάρχουσα χρονική αλληλουχία της αλυσίδας και να εξασφαλιστεί η ασφάλεια των

δεδομένων. Έτσι, η εισαγωγή κάθε καινούριου μπλοκ διαδραματίζει σημαντικό ρόλο στη διατήρηση της ασφάλειας της αλυσίδας καθώς επαληθεύει τα προηγούμενα μπλοκ. Με βάση τα προαναφερθέντα, μπορούμε λοιπόν να κατανοήσουμε ότι ο τρόπος αποθήκευσης των δεδομένων σε μπλοκ, εξασφαλίζει την ασφάλεια των δεδομένων γιατί κανείς δεν μπορεί να τα παραποιήσει ή να τα διαγράψει (Gupta, 2017 **,** Swan, 2015).

Αναφορικά με τον τρόπο λειτουργίας του Blockchain, θα πρέπει να αναφερθεί ότι στη συγκεκριμένη τεχνολογία χρησιμοποιείται κρυπτογράφηση των δεδομένων, η οποία περιλαμβάνει την ύπαρξη ενός ζεύγους κλειδιών (ενός δημόσιου και ενός ιδιωτικού) επιτρέποντας σε κάθε συμμετέχοντα οποιουδήποτε δικτύου να διαχειρίζεται το τμήμα πληροφορίας που του ανήκει, με ασφαλή τρόπο, χωρίς δηλαδή την ανάγκη κεντρικής αρχής. Η απαλοιφή της κεντρικής αρχής αποτελεί θεμελιώδη αρχή στο Blockchain. Άξιο αναφοράς κρίνεται επίσης ότι τα δεδομένα που καταγράφονται σε ένα Blockchain είναι εξαιρετικά δύσκολο να αλλάξουν ή να αφαιρεθούν, στοιχείο που εμφανίζεται για πρώτη φορά στην πληροφορική.

Επίσης καινοτομία του Blockchain συνιστά η δυνατότητα διαχείρισης περιουσιακών στοιχείων χωρίς να χρειάζεται η παρέμβαση και πιστοποίηση από εξουσιοδοτημένες αρχές και οργανισμούς (Laurence, 2017 , Gupta, 2017). Στην περίπτωση που κάποιος θελήσει να προσθέσει μια εγγραφή (συναλλαγή ή καταχώρηση) σε ένα Blockchain, θα πρέπει τα δεδομένα να ελεγχθούν από έναν αλγόριθμο ο οποίος θα επιβεβαιώσει την ακεραιότητα και την ορθότητα της κάθε συναλλαγής, χωρίς να απαιτείται η περαιτέρω πιστοποίηση από κάποιον τρίτο οργανισμό (Laurence, 2017).

Επιπρόσθετα, το Blockchain μπορεί να χρησιμοποιηθεί σε όλες τις περιπτώσεις στις οποίες απαιτείται αποθήκευση δεδομένων. Εντούτοις, ευρύτερη και σπουδαιότερη είναι η εφαρμογή του σε αναξιόπιστα δίκτυα στα οποία θέλουμε να εξασφαλίσουμε ότι τα δεδομένα και τα αρχεία μας δεν πρόκειται να παραποιηθούν ή να διαγραφούν. Επομένως το Blockchain ενισχύει σε σημαντικό βαθμό την εμπιστοσύνη σε ένα δίκτυο (Gupta, 2017).

## 2.2. Οι τύποι του Blockchain

Το Blockchain αποτελείται από 3 διαφορετικούς τύπους. Η επιλογή του Blockchain τύπου που θα χρησιμοποιηθεί εξαρτάται από τους εξής παράγοντες:

- Αν το βιβλιάριο θα είναι κατανεμημένο ή όχι.
- Ποιοι χρήστες θα έχουν πρόσβαση σε αυτό.
- Ποιοι χρήστες θα επαληθεύουν και θα καταχωρούν τις συναλλαγές δεδομένων στο βιβλιάριο.

### 2.2.1. Public

Τα δημόσια Blockchains όπως είναι για παράδειγμα το Bitcoin και το Ethereum είναι από τα μεγαλύτερα σε αριθμό συμμετεχόντων κατανεμημένα δίκτυα. Ο κώδικας εκδίδεται ανοιχτά προς όλους και οποιοσδήποτε μπορεί να τον επιθεωρήσει. Ο κάθε χρήστης λοιπόν έχει πρόσβαση στο δίκτυο και χρησιμοποιώντας το εκάστοτε κρυπτονόμισμα δύναται να συμμετάσχει στο επίπεδο λειτουργιών που επιθυμεί. Για παράδειγμα μπορεί να συμμετέχει στο σύστημα σαν απλός χρήστης ή να λάβει μέρος σε πιο σύνθετες λειτουργίες όπως είναι η συμμετοχή στην επαλήθευση και επικύρωση των συναλλαγών. Επιπλέον το δίκτυο έχει συνήθως έναν μηχανισμό παροχής κινήτρων κατά τον οποίο οι χρήστες κερδίζουν κρυπτονομίσματα κατά την επαλήθευση και επικύρωση των συναλλαγών τους, προκειμένου να ενθαρρύνει περισσότερους συμμετέχοντες να ενταχθούν σε αυτό και να χρησιμοποιήσουν το κρυπτονόμισμα.

Αξιοσημείωτο κρίνεται και το γεγονός ότι τα δημόσια Blockchains τείνουν να είναι πιο ασφαλή από τους υπόλοιπους τύπους Blockchain λόγω του ότι κανένας οργανισμός ή κυβέρνηση δεν ελέγχει το δίκτυο και η συμμετοχή γίνεται ανώνυμα. Ο κώδικας με τη σειρά του ανανεώνεται αποκλειστικά από την κοινότητα του κάθε Blockchain δικτύου στην οποία συμμετέχουν εθελοντικά προγραμματιστές.

Εξετάζοντας τα μειονεκτήματα των δημόσιων Blockchains καθίσταται φανερό ότι απαιτείται σημαντικό ποσό υπολογιστικής ισχύος για να επιτευχθεί ο συγχρονισμός και η διατήρηση του κατανεμημένου βιβλιαρίου. Επίσης το δημόσιο Blockchain είναι συχνά πιο αργό από

τους υπόλοιπους τύπους Blockchain και με τη συνεχόμενη αύξηση των συναλλαγών αντιμετωπίζει προβλήματα αποθηκευτικού χώρου (Laurence, 2017).

### 2.2.2. Permissioned

Το εξουσιοδοτημένο Blockchain διατηρεί και αυτό ένα κατανεμημένο βιβλιάριο δεδομένων, όμως η συμμετοχή σε αυτό ελέγχεται από μια κεντρική αρχή. Η κεντρική αυτή αρχή γνωρίζει τους συμμετέχοντες και δίνει το δικαίωμα επικύρωσης των συναλλαγών σε έμπιστα προς αυτούς άτομα. Αυτό το χαρακτηριστικό διευκολύνει την αύξηση του όγκου των συναλλαγών που πραγματοποιούνται ημερησίως και ταυτόχρονα τα εξουσιοδοτημένα δίκτυα μπορούν να είναι πολύ γρήγορα με μεγαλύτερη αποθηκευτική χωρητικότητα. Επίσης ο βασικός κώδικας του κάθε εξουσιοδοτημένου Blockchain μπορεί να εκδίδεται ανοιχτά προς όλους για να τον επιθεωρήσουν ή και όχι (Laurence, 2017 **,** Gupta, 2017 **,** Tapscott & Tapscott, 2016).

### 2.2.3. Private

Τα ιδιωτικά Blockchains τείνουν να είναι πολύ πιο μικρά σε αριθμό συμμετεχόντων σε σχέση με τους υπόλοιπους τύπους Blockchain. Ενδέχεται μάλιστα ο κόσμος να μην γνωρίζει καν την ύπαρξή τους επειδή τις περισσότερες φορές δεν είναι ορατά στο κοινό . Η συμμετοχή κάθε χρήστη είναι ελεγχόμενη από μια κεντρική αρχή. Ως προς τα χαρακτηριστικά τους θα πρέπει να αναφερθεί ότι είναι πολύ πιο γρήγορα από τους υπόλοιπους τύπους και ενδέχεται να μην παρουσιάζουν καμία καθυστέρηση στο χρόνο επικύρωσης των δεδομένων. Έχουν επίσης χαμηλό κόστος λειτουργείας, απεριόριστη χωρητικότητα και μπορούν να κατασκευαστούν σε πολύ γρήγορο χρονικό διάστημα. Εντούτοις τα περισσότερα ιδιωτικά Blockchain δεν χρησιμοποιούν κρυπτονόμισμα και δεν έχουν την ίδια ασφάλεια που παρέχει ένα αποκεντρωμένο Blockchain δίκτυο (Gupta, 2017 **,** Tapscott & Tapscott, 2016).

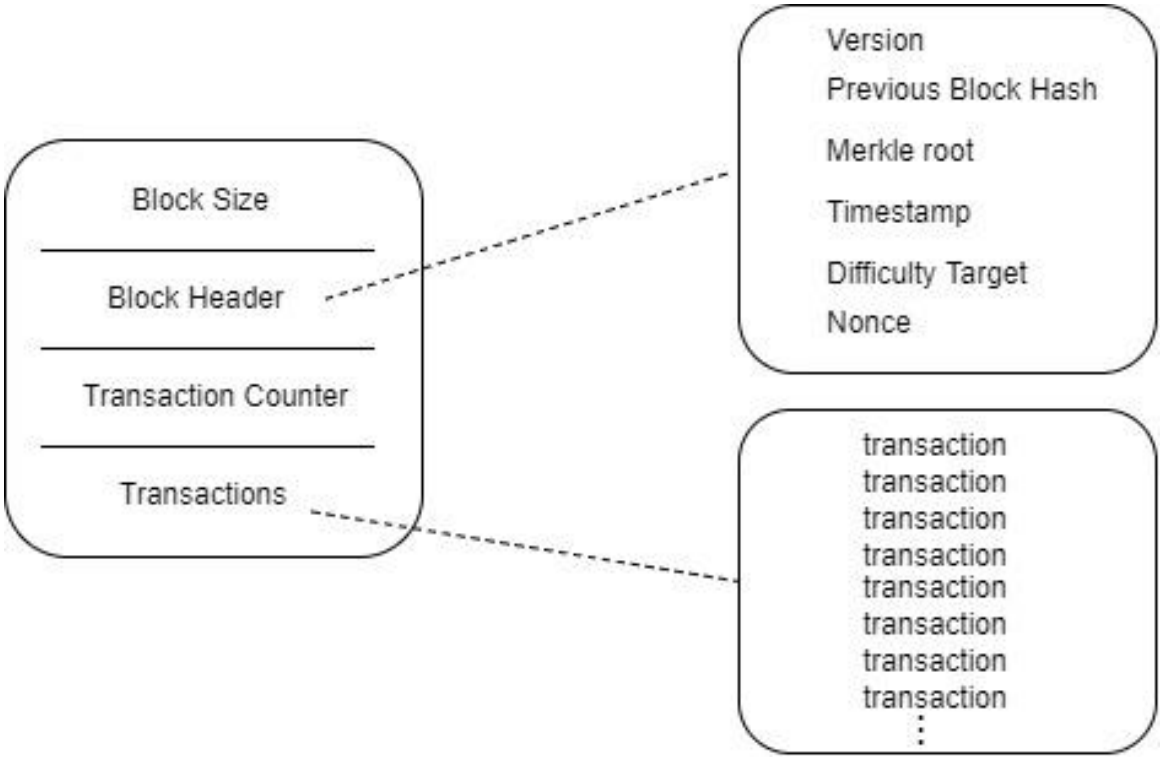
## 2.3. Αρχιτεκτονική του Blockchain

Η αρχιτεκτονική του Blockchain βασίζεται κυρίως σε 5 στοιχεία: το μπλοκ (Block), την αλυσίδα (Chain), τις ψηφιακές υπογραφές (Digital Signatures), το Peer-to-peer δίκτυο και τον έμπιστο μηχανισμό (Consensus Protocol).

### 2.3.1. Block

Σε ένα μπλοκ καταγράφονται οι πιο πρόσφατες συναλλαγές που έχουν γίνει σε ένα Blockchain δίκτυο. Συνεπώς, ένα μπλοκ είναι μια μόνιμη «αποθήκη δεδομένων», τα οποία, μόλις γραφτούν, δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν. Τα μπλοκ όμως διαφέρουνε από Blockchain σε Blockchain και εκτός από τις συναλλαγές περιέχουνε κι,άλλα δεδομένα όπως αυτά που εξετάζονται στο μπλοκ του Bitcoin δικτύου.

Παρακάτω παρουσιάζεται ένα παράδειγμα της δομής του μπλοκ στο Bitcoin δίκτυο το οποίο περιέχει τα εξής δεδομένα: το Block Size , το Block Header αποτελούμενο από 6 δεδομένα, το Transaction Counter και τις συναλλαγές (Transactions):




Εικόνα 3: Παράδειγμα της δομής του μπλοκ στο Bitcoin δίκτυο.

- **Block Size**: Είναι το μέγεθος του παρόν μπλοκ σε bytes (μονάδα μέτρησης ποσότητας πληροφορίας)
- Block Header: Είναι η κεφαλίδα του μπλοκ η οποία αποτελείται από το:

  **Version**: Είναι η έκδοσης του παρόν μπλοκ

  **Previous Block Hash**: Είναι το Hash του προηγούμενου μπλοκ

  **Merkle root**: Είναι ένα Hash το οποίο δημιουργείται από όλες τις συναλλαγές που περιλαμβάνονται σε αυτό το μπλοκ

  **Timestamp:** Είναι ο χρόνος που δημιουργήθηκε αυτό το μπλοκ

  **Difficulty target:** Είναι η δυσκολία που χρειάζεται για να επικυρωθεί αυτό το μπλοκ

  **Nonce:** Είναι ένας τυχαίος αριθμός ο οποίος χρησιμοποιείται από το τον αλγόριθμο Proof-of-Work (ο αλγόριθμος αυτός θα εξεταστεί στο υποκεφάλαιο 4.3.5.1)

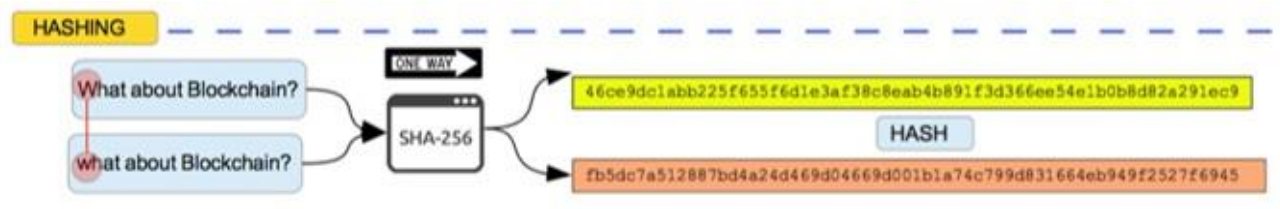
- **Transaction Counter:** Είναι ο συνολικός αριθμός των συναλλαγών στο μπλοκ
- **Transactions:** Είναι όλες οι συναλλαγές που έχουν καταχωρηθεί στο μπλοκ, οι οποίες είναι περίπου 500 (Gupta, 2017, Antonopoulos, 2017).

### 2.3.2. Chain

Ο όρος αλυσίδα (Chain) σχετίζεται με τον τρόπο που είναι ταξινομημένα τα μπλοκ σε ένα δίκτυο Blockchain. Σύμφωνα με τον Αντωνόπουλο (2017): "*Η δομή των δεδομένων στο Blockchain είναι μια ταξινομημένη λίστα από μπλοκ συνδεδεμένη προς τα πίσω*" (Antonopoulos, 2017). Αυτή η ταξινόμηση των μπλοκ σχηματίζει τελικά την αλυσίδα. Όπως προαναφέρθηκε, το Block Header αποτελείται από 6 δεδομένα και μέσα σε αυτά τα δεδομένα υπάρχει το Previous Block Hash το οποίο είναι αυτό που συνδέει αυτό το μπλοκ με το προηγούμενο μπλοκ στο Blockchain. Το Hash λοιπόν δημιουργείται πάντα από τα

δεδομένα του προηγούμενου μπλοκ. Όπως αναφέρει η Laurence "*Το Hash είναι η μαγική κόλλα που ενώνει τα μπλοκ μεταξύ τους και επιτρέπει εμπιστοσύνη με μαθηματική ακρίβεια*" (Laurence, 2017). Για τη δημιουργία του Hash χρησιμοποιείται ο αλγόριθμος κρυπτογράφησης SHA-256, ο οποίος όταν κρυπτογραφεί τα δεδομένα επιστρέφει σχεδόν πάντα ένα μοναδικό αλφαριθμητικό 64 χαρακτήρων Hash. Η λειτουργία του αλγορίθμου χαρακτηρίζεται ως μη αντιστρέψιμη και λειτουργεί σαν ψηφιακό αποτύπωμα το οποίο είναι μοναδικό και δεν μπορεί να αποκρυπτογραφηθεί (Laurence, 2017 **,** Antonopoulos, 2017).

Στην παρακάτω εικόνα παρουσιάζεται το αποτέλεσμα Hash που προκύπτει όταν εφαρμόσουμε τον αλγόριθμο SHA-256 σε 2 διαφορετικές προτάσεις.




Εικόνα **4:** Αλγόριθμος Κατακερματισμού SHA-256. Ανακτήθηκε από www.LinkedIn.com: Άρθρο από τον Peter van Emst, Ανακτήθηκε Οκτώβριος 30, 2017.

### 2.3.3. Digital Signatures

Η δημιουργία μιας συναλλαγής στο Blockchain απαιτεί ψηφιακή υπογραφή για τον έλεγχο και την εγκυρότητας της. Πιο αναλυτικά, για τη δημιουργία μιας ψηφιακής υπογραφής κάθε χρήστης χρησιμοποιεί ένα ζευγάρι κλειδιών, ένα ιδιωτικό και ένα δημόσιο.

Το ιδιωτικό κλειδί, το οποίο γνωρίζει μόνο ο χρήστης χρησιμοποιείται για τη δημιουργία της ψηφιακής υπογραφής.

Το δημόσιο κλειδί λειτουργεί σαν τις διευθύνσεις email, είναι δηλαδή ορατό προς όλους και χρησιμοποιείται για την επαλήθευση των δεδομένων.

Μια ψηφιακή υπογραφή περιλαμβάνει δύο φάσεις:

a) τη φάση υπογραφής και

b) τη φάση της επαλήθευσης.

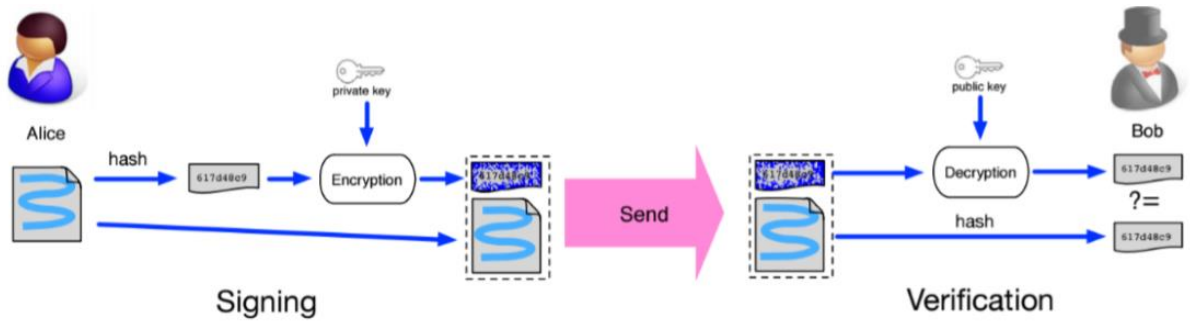
Στην παρακάτω εικόνα παρουσιάζεται ένα παράδειγμα ψηφιακής υπογραφής. Παρατηρούμε λοιπόν ότι για να υπογράψει ο χρήστης,,Alice,, μια συναλλαγή πρέπει να ακολουθήσει τα εξής βήματα:

i. Αρχικά δημιουργεί ένα Hash από τα δεδομένα της συναλλαγής χρησιμοποιώντας ένα αλγόριθμο κρυπτογράφησης.
ii. Έπειτα δημιουργεί μια ψηφιακή υπογραφή αφού κρυπτογραφήσει την τιμή Hash χρησιμοποιώντας το ιδιωτικό κλειδί.
iii. Τέλος αποστέλλει στον χρήστη "Bob" την ψηφιακή υπογραφή μαζί με τα αρχικά δεδομένα της συναλλαγής.

Ο Bob έχει τώρα στην κατοχή του τα δεδομένα της συναλλαγής και την ψηφιακή υπογραφή του χρήστη “Alice”. Για να ελέγξει την εγκυρότητα της συναλλαγής ο Bob χρειάζεται να κάνει 2 ενέργειες:

i. να αποκρυπτογραφήσει την ψηφιακή υπογραφή με το δημόσιο κλειδί της Alice για να αποκτήσει το Hash
ii. να δημιουργήσει ένα 2ο Hash από τα δεδομένα που του έχουνε σταλεί.

Αν αυτά τα 2 Hash είναι ίδια τότε η συναλλαγή είναι έγκυρη (Antonopoulos, 2017: 61).




Εικόνα 5: Digital Signature Used in Blockchain. Ανακτήθηκε από www.researchgate.net: Άρθρο από τον Zibin Zheng και άλλους, Ανακτήθηκε Οκτώβριος 30, 2017.

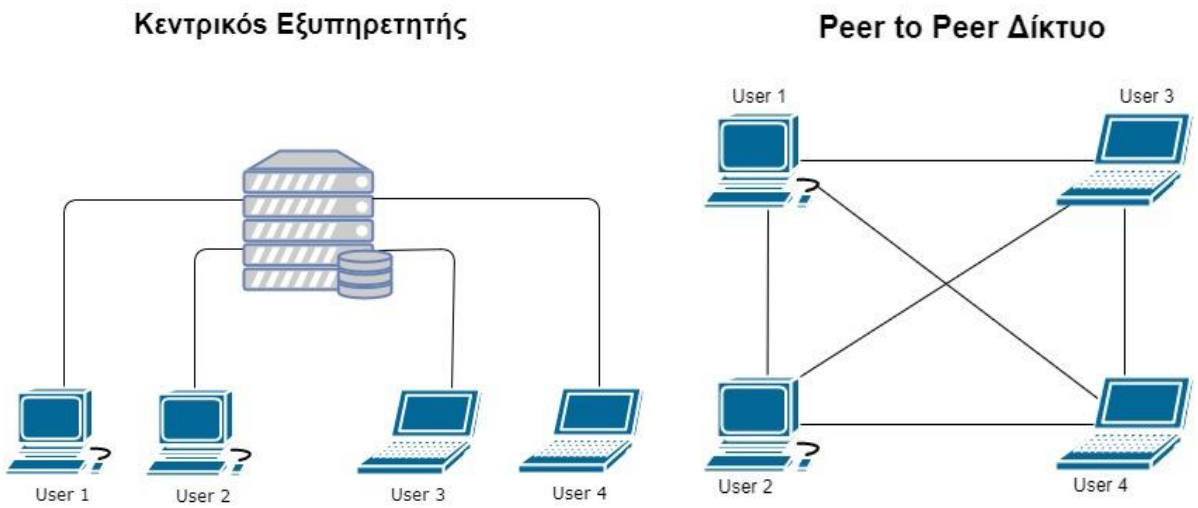
### 2.3.4. Peer-to-Peer Network

Οι χρήστες για να αλληλοεπιδράσουν με το Blockchain χρησιμοποιούν κατά κύριο λόγο ένα αποκεντρωμένο δίκτυο Peer-to-Peer (P2P) στο οποίο κάθε χρήστης αντιπροσωπεύει και έναν κόμβο. Για να θεωρείται όμως ο χρήστης κόμβος του δικτύου θα πρέπει να έχει ένα ηλεκτρονικό υπολογιστή με σχετικά μεγάλο αποθηκευτικό χώρο και συνδεδεμένο πάντα με το ίντερνετ. Επιπλέον οι χρήστες-κόμβοι του δικτύου προσφέρουν και λαμβάνουν υπηρεσίες μεταξύ τους αφού δεν υπάρχει κεντρικός εξυπηρετητής.

Όταν ένας χρήστης πραγματοποιεί συναλλαγή με ένα άλλο χρήστη ή όταν ένας κόμβος λαμβάνει δεδομένα από άλλο κόμβο, ελέγχετε η αυθεντικότητα των δεδομένων. Στη συνέχεια μεταδίδονται τα επικυρωμένα δεδομένα σε κάθε άλλο κόμβο που είναι συνδεδεμένος και σε πολύ μικρό χρονικό διάστημα τα δεδομένα διαδίδονται σε όλο το δίκτυο.

Το πλεονέκτημα της χρήσης ενός Peer-2-Peer δικτύου είναι ότι για την αποθήκευση και επιβεβαίωση της ορθότητας της κάθε συναλλαγής δεν χρειάζεται κάποιος ενδιάμεσος ή κάποια κεντρική αρχή, κάτι το οποίο κάνει το δίκτυο πιο ασφαλές από κακόβουλες επιθέσεις (Antonopoulos, 2017).

Στην παρακάτω εικόνα παρουσιάζεται στα αριστερά ένα δίκτυο με κεντρικό εξυπηρετητή και στα δεξιά ένα δίκτυο Peer-to-Peer:




Εικόνα 6: Παρουσίαση ενός δικτύου με κεντρικό Server και ενός Peer-to-Peer δικτύου:

Ο Server ή αλλιώς εξυπηρετητής, στην πιο απλή του μορφή είναι ένας ηλεκτρονικός υπολογιστής που έχει κατάλληλο λογισμικό ώστε να εξυπηρετεί τα αιτήματα των χρηστών που συνδέονται με αυτόν. Επίσης τα δεδομένα των χρηστών είναι αποθηκευμένα σ, αυτόν τον κεντρικό εξυπηρετητή και αν για κάποιο λόγο χάσει την συνδεσιμότητα του στο δίκτυο τότε και όλοι οι υπόλοιποι χρήστες θα χάσουν την πρόσβαση στα δεδομένα τους.

Αντίθετα, στο δίκτυο Peer-to-Peer όλοι οι χρήστες έχουν όλα τους τα δεδομένων σε όλους τους συνδεδεμένους υπολογιστές, μπορούν να συνεχίσουν να λειτουργούν και να ανταλλάζουν δεδομένα ακόμη και αν κάποιοι από τους κόμβους χάσουν τη συνδεσιμότητα τους με το υπόλοιπο δίκτυο. Επίσης, τα Peer-to-Peer δίκτυα είναι πιο ισχυρά, καθώς δεν υπάρχει κεντρικός διακομιστής, οπότε το να πάψει να λειτουργεί ένα τέτοιο δίκτυο είναι εξαιρετικά δύσκολο.

### 2.3.5. Consensus Protocol

Κάθε Peer-2-Peer δίκτυο βασισμένο σε Blockchain μπορεί να λειτουργήσει σωστά μόνο με την πλήρη συναίνεση όλων των χρηστών, αφού δεν υπάρχει κεντρική αρχή για να παρέχει εμπιστοσύνη και ακεραιότητα στις πληροφορίες που ανταλλάζονται. (Laurence, 2017 **,** Antonopoulos, 2017). Η συναίνεση σύμφωνα με τον Antonopoulo είναι : ”*ένα αναδυόμενο δημιούργημα της ασύγχρονης αλληλεπίδρασης χιλιάδων ανεξάρτητων κόμβων, ακολουθώντας απλούς κανόνες*” (Antonopoulos, 2017).

Για να υπάρξει λοιπόν συναίνεση, χρειάζεται ένας τρόπος για να αποφασιστεί ποια δεδομένα είναι έγκυρα και ποια όχι. Η διαδικασία της επικύρωσης των δεδομένων σε ένα δίκτυο Peer-to-Peer ονομάζεται εξόρυξη (mining) και απαιτεί τη χρήση σύνθετων αλγορίθμων όπως Proof-of-work, Proof of Stake και Practical Byzantine Fault Tolerance. Μέσω αυτής της διαδικασίας επιτυγχάνεται επίσης, η προσθήκη των επικυρωμένων μπλοκ από συναλλαγές στην αλυσίδα του Blockchain.

### 2.3.5.1. Proof of Work

Ο αλγόριθμος Proof-of-Work (PoW) έχει ως κύριο στόχο να διασφαλίσει την διαδικασία επικύρωσης των δεδομένων και την αποτροπή επιθέσεων στο δίκτυο.
Η ιδέα του αλγορίθμου αυτού υπήρχε και πριν από το Bitcoin, αλλά ο Satoshi Nakamoto εφάρμοσε για πρώτη φορά αυτήν την τεχνική στο ψηφιακό νόμισμά bitcoin. Στην πραγματικότητα, η ιδέα του αλγορίθμου PoW δημοσιεύθηκε αρχικά από τους Cynthia Dwork και Moni Naor το 1992 με τίτλο "Pricing via Processing or Combatting Junk Mail". Αργότερα μια παρόμοια πρόταση που ονομάζεται Hashcash προτάθηκε το 1997 από τον Adam Back αλλά ο όρος "Proof-of-Work" δημιουργήθηκε από τους Markus Jakobsson και Ari Juels σε έγγραφο με ονομασία «Proofs of Work and Bread Pudding Protocols (Extended Abstract)» που δημοσιεύθηκε το 1999. Ο αλγόριθμος αυτός είναι ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος στην τεχνολογία Blockchain.

Για να κατανοήσουμε τη λειτουργία του αλγορίθμου proof of work θα πρέπει να έχουμε υπόψη μας ότι κάθε φορά που πραγματοποιείται μια συναλλαγή στο δίκτυο Bitcoin, η συναλλαγή αυτή καταγράφεται και αποθηκεύεται σε ένα προσωρινό μπλοκ. Στη συνέχεια, μόλις το μπλοκ γεμίσει με συναλλαγές, μεταδίδεται σε όλους τους κόμβους που συμμετέχουν στο δίκτυο. Στην προκειμένη φάση όλοι οι κόμβοι θα πρέπει να ελέγξουν την εγκυρότητα ολόκληρου του μπλοκ. Σε αυτό το σημείο χρησιμοποιείται ο αλγόριθμος Proof-of-Work. Στη συνέχεια κάθε κόμβος προσθέτει ένα κομμάτι δεδομένου στο μπλοκ το οποίο ονομάζεται «nonce» και σχηματίζεται τελικά το «Block + nonce». Αυτό το «Block + nonce» τοποθετείται σε έναν αλγόριθμο κρυπτογράφησης με ονομασία SHA-256 (Secure Hash Algorithm). Με τη σειρά του αυτός ο αλγόριθμος παράγει ένα αλφαριθμητικό 64 χαρακτήρων το οποίο ονομάζεται Hash.

Το πρωτόκολλο του Bitcoin θέτει αυτόματα ένα στόχο (Difficulty target). Ο στόχος είναι το επίπεδο δυσκολίας που χρειάζεται ένας κόμβος για να επικυρώσει το μπλοκ. Όλοι οι κόμβοι στο δίκτυο συναγωνίζονται για το ποιος θα βρει πρώτος ένα αλφαριθμητικό Hash μικρότερο του στόχου. Το μόνο που μπορούν να κάνουν είναι κάθε φορά να αλλάζουν την τιμή του «nonce» και να τοποθετούνε το «Block + (καινούργιο)nonce» στον αλγόριθμο κρυπτογράφησης SHA256. Η διαδικασία της αλλαγής του «nonce» γίνεται αυτόματα και ο πρώτος κόμβος που θα βρει το σωστό αποτέλεσμα έχει επίσημα επικυρώσει τις συναλλαγές

στο μπλοκ και κερδίζει ένα ποσό bitcoins. Τότε αποστέλλεται σε όλους τους υπόλοιπους κόμβους το «Block+ nonce + Hash» και αφού πιστοποιήσουν οι υπόλοιποι κόμβοι ότι είναι σωστή η λύση, τότε προσκολλάτε στην αλυσίδα του Blockchain. Μόλις ολοκληρωθεί η διαδικασία αυτή η οποία διαρκεί περίπου 10 λεπτά, οι κόμβοι αμέσως μαζεύουνε τις καινούργιες συναλλαγές και συναγωνίζονται πάλι για να βρούνε το σωστό «nonce» (Antonopoulos, 2017 , Vincenzo Morabito).

### 2.3.5.2. Proof of Stake

Ο Proof-of-Stake (PoS) είναι ένας ακόμα αλγόριθμος, ο σκοπός του οποίου είναι ίδιος με τον αλγόριθμο Proof-of-Work. Εντούτοις η διαδικασία για την επικύρωση των συναλλαγών είναι αρκετά διαφορετική. Η πρώτη ιδέα του Proof-of-Stake προτάθηκε στο διαδικτυακό φόρουμ bitcointalk.org το 2011, αλλά το πρώτο κρυπτονόμισμα που έκανε χρήση αυτής της μεθόδου ήταν το Peercoin το 2012, μαζί με το ShadowCash, το Nxt, το BlackCoin, το NuShares/NuBits, το Qora και το NavCoin.

Σε αντίθεση με το Proof-of-Work όπου επικυρώνει τις συναλλαγές ο γρηγορότερος κόμβος, στο Proof-of-Stake, ο κόμβος που θα επικυρώσει τις συναλλαγές επιλέγεται με ντετερμινιστικό τρόπο. Οι κόμβοι δηλαδή, καταθέτουν στο δίκτυο ένα ποσό από τα κρυπτονομίσματα τους ως εγγύησή ότι θα επικυρώσουν τις συναλλαγές σε ένα μπλοκ. Το ποιος κόμβος τελικά θα επιλεγεί, καθορίζεται από το ποσό που έχει καταθέσει. Για παράδειγμα, εάν η Μαρία καταθέσει 60 κρυπτονομίσματα, η Άννα 30 και η Κατερίνα 10, η Μαρία έχει 60% πιθανότητα να επικυρώσει το μπλοκ, η Άννα έχει 30% και η Κατερίνα 10%. Έτσι στο PoS εμπιστευόμαστε την αλυσίδα με την υψηλότερη εγγύηση. Επίσης δεν υπάρχει ανταμοιβή για την επικύρωση του κάθε μπλοκ, όμως ο κόμβος που θα επικυρώσει το μπλοκ λαμβάνει ένα ποσό από την κάθε συναλλαγή (Ethan Buchman, 2016).

### 2.3.5.3. Practical Byzantine Fault Tolerance

Το 1999, οι Miguel Castro και Barbara Liskov εισήγαγαν τον αλγόριθμο "Practical Byzantine Fault Tolerance" (PBFT), που αποτέλεσε την πρώτη πρακτική λύση απέναντι στο πρόβλημα των Βυζαντινών Στρατηγών, η οποία έγινε αποδεκτή από όλους. Θα πρέπει να διευκρινιστεί στο σημείο αυτό ότι το πρόβλημα των Βυζαντινών Στρατηγών παρουσιάζεται όταν διαφορετικοί κόμβοι σε ένα αναξιόπιστο δίκτυο πρέπει να καταλήξουν σε μια τελική απόφαση, ελέγχοντας τα δεδομένα που ανταλλάζονται. Παράλληλα ο αλγόριθμος «PBFT» θεωρήθηκε ως ο πρώτος πρακτικός αλγόριθμος που είναι κατάλληλος για χρήση σε ασύγχρονα δίκτυα.

Ο συγκεκριμένος αλγόριθμος χρησιμοποιείται από εξουσιοδοτημένα Blockchain δίκτυα όπως το Hyperledger Fabric, Ripple, Stellar και απαιτεί ο κάθε κόμβος να είναι γνωστός στο δίκτυο. Κάθε φορά που πραγματοποιείται μια συναλλαγή, επικυρώνεται μέσω μιας συγκεκριμένης διαδικασίας. Πιο αναλυτικά, σε κάθε φάση της διαδικασίας, επιλέγεται με βάση ορισμένους κανόνες ένας κύριος εισηγητής κόμβος, ο οποίος είναι υπεύθυνος να εξετάσει αν τα δεδομένα είναι σωστά. Αφού εξετάσει τα δεδομένα στέλνει τα αποτελέσματα σε όλους τους υπόλοιπους κόμβους του δικτύου. Ο εισηγητής θα περάσει στην επόμενη φάση εξέτασης των δεδομένων, αν τα 2/3 όλων των κόμβων έχουν ψηφίσει ότι συμφωνούν μαζί του. Αν οι ψήφοι είναι λιγότεροι, τότε εκλέγεται ένας καινούργιος εισηγητής. Η διαδικασία ολοκληρώνεται σε 3 φάσεις, όπου κάθε φάση ακολουθείται η ίδια διαδικασία (Ethan Buchman, 2016)

## 3. Smart Contract

Ένα συμβόλαιο με την παραδοσιακή του έννοια, είναι μια γραπτή συμφωνία με την οποία τα συμβαλλόμενα μέρη αναλαμβάνουν συγκεκριμένες δεσμεύσεις το ένα απέναντι στο άλλο. Κάθε συμβαλλόμενο μέρος πρέπει να εμπιστεύεται το άλλο μέρος ότι θα εκπληρώσει τις υποχρεώσεις του συμβολαίου. Τα έξυπνα συμβόλαια διαθέτουν το ίδιο είδος συμφωνίας, αλλά καταργούν την ανάγκη για εμπιστοσύνη μεταξύ των διαφόρων μερών. Αυτό οφείλεται στο γεγονός ότι ένα έξυπνο συμβόλαιο είναι ένα κομμάτι κώδικα που αποθηκεύεται σε ηλεκτρονικό υπολογιστή χωρίς να μπορεί κάποιος να το παραβιάσει και είναι σε θέση να εκτελέσει ή να επιβάλει μια προκαθορισμένη συμφωνία χρησιμοποιώντας ένα δίκτυο Blockchain, όταν και αν πληρούνται συγκεκριμένες προϋποθέσεις. Δηλαδή ο κώδικας περιέχει τη συμφωνία μεταξύ των διαφόρων μερών και καταργεί την ανάγκη εμπιστοσύνης, αφού κανείς δεν θα μπορεί να αλλάξει ή τροποποιήσει την συμφωνία και θα εκτελεστεί όταν θα πληρούνται οι προϋποθέσεις που έχουν συμφωνήσει.

Ένα έξυπνο συμβόλαιο χαρακτηρίζεται από τρία βασικά στοιχεία: την αυτονομία, την αυτάρκεια και την αποκέντρωση. Αυτονομία σημαίνει ότι μετά τη δρομολόγησή και τη λειτουργία του, το συμβόλαιο και τα συμβαλλόμενα μέρη δεν χρειάζεται να βρίσκονται σε περαιτέρω επαφή. Ο όρος αυτάρκεια αναφέρεται, με τη σειρά του, στη δυνατότητα των έξυπνων συμβολαίων να είναι αυτάρκη, να είναι δηλαδή ικανά να εκτελούν τις εσωτερικές τους λειτουργίες ανάλογα με τους πόρους που διαθέτουν. Τέλος, τα έξυπνα συμβόλαια είναι αποκεντρωμένα, δεδομένου ότι δεν έχουν έναν κεντρικό εξυπηρετητή αλλά εκτελούνται σε διάφορους κόμβους του Blockchain δικτύου.

Κύριος στόχος του έξυπνου συμβολαίου σε ένα Blockchain δίκτυο, είναι να επιτρέψει σε δύο ή περισσότερα μέρη να πραγματοποιήσουν μια αξιόπιστη συναλλαγή χωρίς να έχουν ανάγκη από μεσάζοντες. Το συμβόλαιο ενεργοποιείται αυτόματα όταν πληροί κάποιες προϋποθέσεις που έχουν προσυμφωνεί από τα εμπλεκόμενα μέρη. Ένα παράδειγμα θα μπορούσε να ήταν: μόλις ένας άνθρωπος γίνει 18 ετών θα μεταφερθεί στο λογαριασμό του ένα ποσό που έχει συμφωνηθεί προηγουμένως στο συμβόλαιο. Όταν τα συμβόλαια ενεργοποιηθούν δεν μπορεί να διακοπεί η λειτουργία τους από τρίτα άτομα ούτε να αλλάξει η εκάστοτε συμφωνία. Τέλος ένα μικρό λάθος στον κώδικα μπορεί να έχει ως αποτέλεσμα την απώλεια των κρυπτονομισμάτων του έξυπνου συμβολαίου (Melanie Swan, 2015).

## 4. State of The Art

Μέχρι σήμερα, η ηλεκτρική ενέργεια προέρχεται κυρίως από μεγάλους κεντρικούς σταθμούς ηλεκτροπαραγωγής που λειτουργούν με μη ανανεώσιμα ορυκτά καύσιμα. Αυτό προκαλεί άμεσα τον περιβαλλοντικό εκφυλισμό κατά τη μετάδοση της ενέργειας, λόγω των μεγάλων φυσικών αποστάσεων μεταξύ των τόπων παραγωγής και κατανάλωσης. Η αυξανόμενη έτσι ενσωμάτωση των ανανεώσιμων πηγών ενέργειας (ΑΠΕ) στο ενεργειακό σύστημα παρέχει μια λύση σε αυτό το περιβαλλοντικό ενεργειακό πρόβλημα. Στο σημείο αυτό θα πρέπει να διευκρινιστεί ότι η έννοια «ενεργειακό σύστημα» αναφέρεται συνήθως στην ενεργειακή υποδομή που αποτελείται από την παραγωγή, μετατροπή, μεταφορά, διανομή και κατανάλωση ενέργειας.

Οι αγορές ενέργειας Microgrid επιτρέπουν στους συμμετέχοντες μικρής κλίμακας, δηλαδή τους consumer (καταναλωτές) και τους prosumer (καταναλωτές που παράγουν ενέργεια), να εμπορεύονται ενεργά μέσα στην κοινότητά τους (σχεδόν) σε πραγματικό χρόνο. Ένα Microgrid είναι ένα τοπικό ενεργειακό δίκτυο με δυνατότητα ελέγχου, γεγονός που σημαίνει ότι μπορεί να αποσυνδεθεί από το παραδοσιακό δίκτυο και να λειτουργήσει αυτόνομα. Έτσι, καθίσταται εφικτή η επίτευξη ισορροπίας ανάμεσα στην παραγωγή και την κατανάλωση. Ως εκ τούτου, αυτό αποτελεί μια βιώσιμη επιλογή για την ενσωμάτωση των κατανεμημένων ΑΠΕ στο σημερινό ενεργειακό σύστημα με οικονομικό τρόπο.
Η μετάβαση σε περισσότερες νέες ανανεώσιμες πηγές ενέργειας, όπως ανεμογεννήτριες, ηλιακά πάρκα σημαίνει ότι η παραγωγή ενέργειας θα εξαρτάται όλο και περισσότερο από τον καιρό γιατί αν κάποιες μέρες δεν φυσάει και δεν έχει ήλιο τότε δεν θα έχουμε ούτε και ηλεκτρικό ρεύμα. Ταυτόχρονα, το ενεργειακό σύστημα γίνεται πιο αποκεντρωμένο και τα ευέλικτα πάρκα ανεμογεννητριών και οι οικιακοί ηλιακοί συλλέκτες αποτελούν μια αυξανόμενη τάση στην παραγωγή ηλεκτρικής ενέργειας. Αυτό απαιτεί ένα πιο ευέλικτο ενεργειακό σύστημα όπως ευέλικτη παραγωγή και κατανάλωση σε επίπεδο νοικοκυριού, καθώς και καινοτόμες λύσεις αποθήκευσης ενέργειας, όπως οικιακές μπαταρίες.

Ως εκ τούτου, ένας στόχος θα μπορούσε να είναι: κάθε νοικοκυριό να κατανείμει αυτόνομα ηλεκτρική ενέργεια μεταξύ άλλων νοικοκυριών, έτσι ώστε η κατανομή να είναι αποδοτική, αυτοσυντηρούμενη και να μην ελέγχεται από εξωτερικούς παράγοντες.
Υπάρχουν περιπτώσεις χρήσης που επικεντρώνονται στην κατανομή διανεμημένων

ανανεώσιμων πηγών ενέργειας μεταξύ γειτονικών νοικοκυριών χρησιμοποιώντας την τεχνολογία Blockchain. Η υλοποίηση των αγορών αυτών απαιτεί καινοτόμα, ασφαλή και έξυπνα συστήματα πληροφοριών, τα οποία αποτελούν βασικό παράγοντα για την επιτυχή λειτουργία τους.

Το Blockchain, ως αναδυόμενη τεχνολογία, προσφέρει νέες ευκαιρίες για τη δημιουργία αποκεντρωμένης αγοράς και παρέχει φιλικές προς το χρήστη εφαρμογές που επιτρέπουν στους καταναλωτές ενέργειας να συμμετέχουν στην απόφαση σχετικά με το ποιος παράγει την ενέργειά τους και με ποια τεχνολογία παράγεται.

## Χαρακτηριστικά Παραδείγματα P2P

Η ανταλλαγή ενέργειας Peer-to-Peer (P2P) είναι ένα καινοτόμο παράδειγμα της τεχνολογίας Blockchain, όπου οι άνθρωποι παράγοντας δική τους ενέργεια από ανανεώσιμες πηγές ενέργειας σε κατοικίες, γραφεία, εργοστάσια μπορούν να την μοιράζονται μεταξύ τους τοπικά κερδίζοντας παράλληλα χρήματα.

Παρακάτω παρουσιάζονται παραδείγματα ανταλλαγής ενέργειας peer-to-peer:

### Piclo

Η Piclo ιδρύθηκε στο Ηνωμένο Βασίλειο. Ήταν μια συνεργασία μεταξύ μιας καινοτόμου τεχνολογικής εταιρείας που ονομάζεται "Open Utility" και ενός προμηθευτή ανανεώσιμης ενέργειας "Good Energy", όπου οι καταναλωτές των επιχειρήσεων θα μπορούσαν να αγοράσουν ηλεκτρική ενέργεια απευθείας από τις τοπικές ανεμογεννήτριες. Οι «έξυπνες» ανεμογεννήτριες ελέγχουν και «βλέπουν» ποιος αγοράζει ηλεκτρισμό από αυτές. Οι καταναλωτές μπορούν να επιλέξουν και να δώσουν προτεραιότητα από ποιες γεννήτριες θα αγοράσουν ηλεκτρική ενέργεια. Η Piclo εξετάζει τα δεδομένα των μετρητών ρεύματος, την τιμολόγηση της κάθε ανεμογεννήτριας και τις πληροφορίες σχετικά με τις προτιμήσεις των καταναλωτών. Έτσι ανάλογα με τις προτιμήσεις και την τοποθεσία, του κάθε πελάτη, τους προσφέρει διάφορα δεδομένα και αναλύσεις σχετικά με την παραγωγή

και κατανάλωση της ηλεκτρικής ενέργειας (Local renewable energy for businesses,2018 , Introducing Piclo, 2018).

## SonnenCommunity

Η sonnenCommunity αναπτύχθηκε από την sonnenBatterie, η οποία είναι κατασκευαστής αποθήκευσης ηλεκτρικής ενέργειας στη Γερμανία. Είναι μια κοινότητα στην οποία οι κάτοχοι sonnenBatterie μπορούν να μοιράζονται την ίδια ενέργεια με άλλους. Ως αποτέλεσμα, δεν υπάρχει πλέον ανάγκη για κεντρικό προμηθευτή ενέργειας.
Με ένα sonnenBatterie και ένα φωτοβολταϊκό σύστημα, τα μέλη μπορούν να καλύψουν πλήρως τις δικές τους ενεργειακές ανάγκες κατά τη διάρκεια των ηλιόλουστων ημερών. Τις περισσότερες φορές δημιουργείται πλεόνασμα, το οποίο δεν μεταφέρεται στο συμβατικό ηλεκτρικό δίκτυο αλλά σε μια ενεργειακή δεξαμενή που εξυπηρετεί άλλα μέλη σε στιγμές που δεν μπορεί να παραχθεί αρκετή ενέργεια λόγω κακοκαιρίας. Ένα κεντρικό λογισμικό συνδέει και παρακολουθεί όλα τα μέλη του συστήματος, ενώ καθορίζει την προσφορά και την ζήτηση ενέργειας (Sonnen Batterie, 2018).

## Brooklyn Microgrid

Το έργο Brooklyn Microgrid αναπτύσσεται στις ΗΠΑ από την TransactiveGrid, μια κοινοπραξία μεταξύ της LO3 Energy και της ConsenSys.
Στόχος του έργου είναι να δοκιμάσει πώς η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για να πραγματοποιήσει άμεσες πωλήσεις ηλιακής ενέργειας από γειτονικές χώρες. Η τεχνολογία που χρησιμοποιείται στο σχέδιο βασίζεται στο Blockchain του Ethereum. Η δοκιμαστική υλοποίηση ξεκίνησε στο Brooklyn τον Απρίλιο του 2016 ενσωματώνοντας φωτοβολταϊκά συστήματα σε πέντε από τα κτίρια που συμμετέχουν στο έργο παράγοντας ηλιακή ενέργεια. Όλη η ενέργεια που δεν χρησιμοποιείται από τα ίδια τα κτίρια πωλείται σε πέντε γειτονικά νοικοκυριά. Όλα τα κτίρια διασυνδέονται μέσω του συμβατικού ηλεκτρικού δικτύου ενώ η διαχείριση και η αποθήκευση των συναλλαγών γίνεται μέσω του Blockchain του Ethereum.

Η υλοποίηση του έργου απαιτεί να υπάρχουν έξυπνοι μετρητές για την καταγραφή της ποσότητας ενέργειας που παράγεται και τεχνολογία Blockchain για την πραγματοποίηση συναλλαγών μεταξύ των γειτόνων καθώς απαιτούνται έξυπνες συμβάσεις (smart contracts) για την εκτέλεση και καταγραφεί αυτών των συναλλαγών αυτόματα και με ασφάλεια. Οι συναλλαγές που γίνονται στο πλαίσιο του πιλοτικού σχεδίου εκτελούνται χειροκίνητα. Μελλοντικά, ενδέχεται το κάθε νοικοκυριό να μπορεί μέσα από μια εφαρμογή να καθορίζει διάφορες συνθήκες όπως για παράδειγμα σε ποιες τιμές θα αγοραστεί η ηλεκτρική ενέργεια από τους γείτονες. Τελικός στόχος θα είναι όλες οι συναλλαγές να πραγματοποιούνται πλήρως αυτόματα σύμφωνα με τους προκαθορισμένους κανόνες (Brooklyn Microgrid, 2018).

## Oneup: POWR

Η ολλανδική εταιρία (startup) "Oneup" (πρώην BigData.Company) έχει αναπτύξει ένα πρωτότυπο αποκεντρωμένο σύστημα ενεργειακών συναλλαγών και το εφάρμοσε χρησιμοποιώντας τα ενεργειακά δεδομένα δέκα νοικοκυριών. Όπως και στην περίπτωση Brooklyn, τα νοικοκυριά που βρίσκονται στην ίδια γειτονιά παράγουν ηλιακή ενέργεια. Όση ενέργεια δεν καταναλώνεται από ένα νοικοκυριό παραδίδεται στους γείτονές του και τιμολογείται χρησιμοποιώντας το δίκτυο Blockchain Ethereum.
Όλες οι συναλλαγές γίνονται βάσει έξυπνων συμβολαίων. Κάθε κτίριο διαθέτει έναν έξυπνο μετρητή που συνδέεται με ένα Raspberry Pi ( έναν μίνι υπολογιστή ) ο οποίος με τη σειρά του συνδέεται με ένα δίκτυο. Το Raspberry Pi επικοινωνεί με ένα έξυπνο συμβόλαιο (smart contract) που ελέγχει σε πραγματικό χρόνο αν πληρούνται οι όροι σύμβασης και υποδεικνύει στο σύστημα εάν ένα νοικοκυριό είναι σε θέση να παρέχει ενέργεια ή εάν χρειάζεται ενέργεια. Το λογισμικό πραγματοποιεί αυτόματα τη μεταφορά ενέργειας και τις αντίστοιχες πληρωμές (oneup.company, 2018).

SolarChange- SolarCoin

Το έργο SolarChange δημιουργήθηκε για να επιβραβεύσει οικονομικά τους παραγωγούς ηλιακής ενέργειας μέσω δικής τους τεχνολογίας Blockchain. Για κάθε μεγαβάτ ηλιακής ενέργειας που τροφοδοτείται στο δίκτυο, ο παραγωγός κερδίζει ένα SolarCoin, το οποίο μπορεί είτε να αποθηκεύσει στο ηλεκτρονικό πορτοφόλι του, είτε να μετατραπεί σε bitcoins. Το έργο ξεκίνησε από την εταιρεία SolarCoin (SolarChange, 2018 , solarCoin, 2018).

# 5. Παρουσίαση προβλήματος

Αφού στην παραπάνω ενότητα εξετάστηκαν οι προσπάθειες για τη δημιουργία πληροφοριακών συστημάτων για συναλλαγές ενέργειας μέσα από αποκεντρωμένα ενεργειακά συστήματα, στη συνέχεια θα επιχειρηθεί η διατύπωση μιας νέας περίπτωσης χρήσης, η οποία υλοποιήθηκε σε συνεργασία με την εταιρία Intelen Inc.

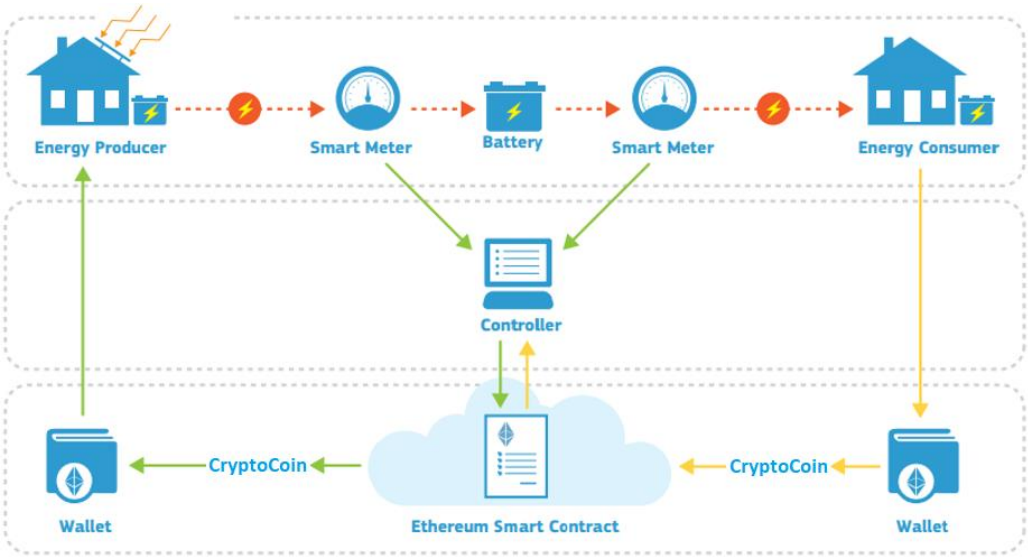
Πιο αναλυτικά θα εξεταστεί η περίπτωση χρήσης για συναλλαγές μεταξύ συσκευών και συγκεκριμένα οι συναλλαγές μεταξύ έξυπνων οικιακών μπαταριών. Στόχος είναι η δημιουργία μιας κατανεμημένης αγοράς που να βασίζεται στο Blockchain του Ethereum και η δημιουργία έξυπνων μπαταριών οι οποίες θα έχουν τη δυνατότητα να ενεργούν ως αγοραστές ή πωλητές ηλεκτρικού ρεύματος, σύμφωνα με τις προϋποθέσεις που έχει θέση ο κάθε ιδιοκτήτης οικιακής μπαταρίας.

## 5.1. Σενάριο Προβλήματος

Καθώς ο ήλιος ανατέλλει, φωτοβολταϊκά συστήματα εγκατεστημένα στην οροφή ενός σπιτιού αρχίζουν να παράγουν ηλεκτρική ενέργεια. Τα φωτοβολταϊκά έχουν εγκατασταθεί από μια εταιρεία υπό την προϋπόθεση ότι ο ιδιοκτήτης διατηρεί το δικαίωμα να πουλάει την ηλεκτρική ενέργεια που παράγει. Τα φωτοβολταϊκά είναι συνδεδεμένα με μια έξυπνη μπαταρία και ένα μετρητή ρεύματος. Η κάθε μπαταρία είναι συνδεδεμένη στο διαδίκτυο και

ο κάθε ιδιοκτήτης της μπορεί μέσα από εφαρμογή κινητού τηλεφώνου ή ηλεκτρονικού υπολογιστή να δει τα επίπεδα φόρτισης της μπαταρίας.

Παράλληλα, υπάρχει η δυνατότητα πώλησης της ηλεκτρικής ενέργειας που έχει παραχθεί καθώς και η αγορά ηλεκτρικής ενέργειας από άλλα νοικοκυριά. Η μπαταρία θα μπορεί να σαρώσει τη βάση δεδομένων με τις παραγγελίες ηλεκτρικής ενέργειας ψάχνοντας για την υψηλότερη προσφορά**.** Στην συνέχεια θα συγκρίνει την προσφορά με τα επενδυτικά και λειτουργικά της έξοδα, καθώς και με όλες τις παραμέτρους τιμών που έχει καθορίσει ο ιδιοκτήτης μπαταρίας. Αν υπάρξει κάποια προσφορά που πληροί τις προϋποθέσεις, τότε ο χρήστης χρησιμοποιώντας ένα ψηφιακό «έξυπνο συμβόλαιο» αγοράζει ή πουλάει ηλεκτρική ενέργεια. Επίσης θα υπάρχει η δυνατότητα η μπαταρία να τεθεί σε αυτόματη λειτουργία, διεξάγοντας αυτόματες αναλύσεις τάσεων σχετικά με τη ζήτηση, την προσφορά και την τιμή αγοράς της ηλεκτρικής ενέργειας. Βάσει τις αναλύσεις της, σχετικά με την τρέχουσα κατάσταση της αγοράς, η μπαταρία αποφασίζει να αγοράσει ηλεκτρική ενέργεια για να επαναφορτίσει, να πουλήσει το υπόλοιπο φορτίο στο δίκτυο ( ή σε άλλη μπαταρία) ή αν δεν θα προβεί σε καμία απολύτως ενέργεια αναμένοντας την περαιτέρω εξέλιξη της κατάστασης στην αγορά. Η αγοραπωλησία ηλεκτρικής ενέργειας θα επιτυγχάνεται μέσο έξυπνων ψηφιακών συμβολαίων που θα αποθηκεύονται στο Ethereum Blockchain καθώς και οι συναλλαγές θα επικυρώνονται μέσα από αυτό.

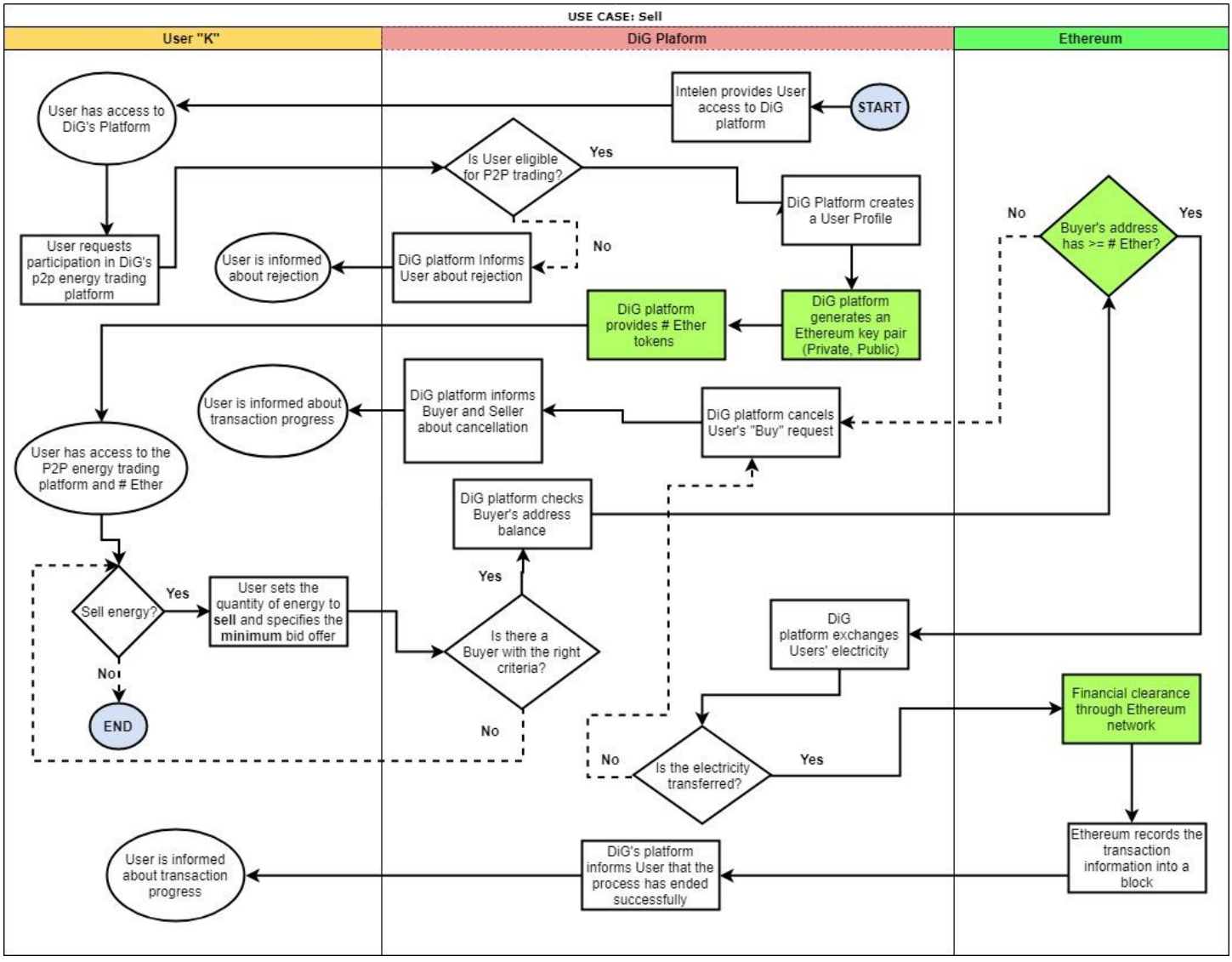


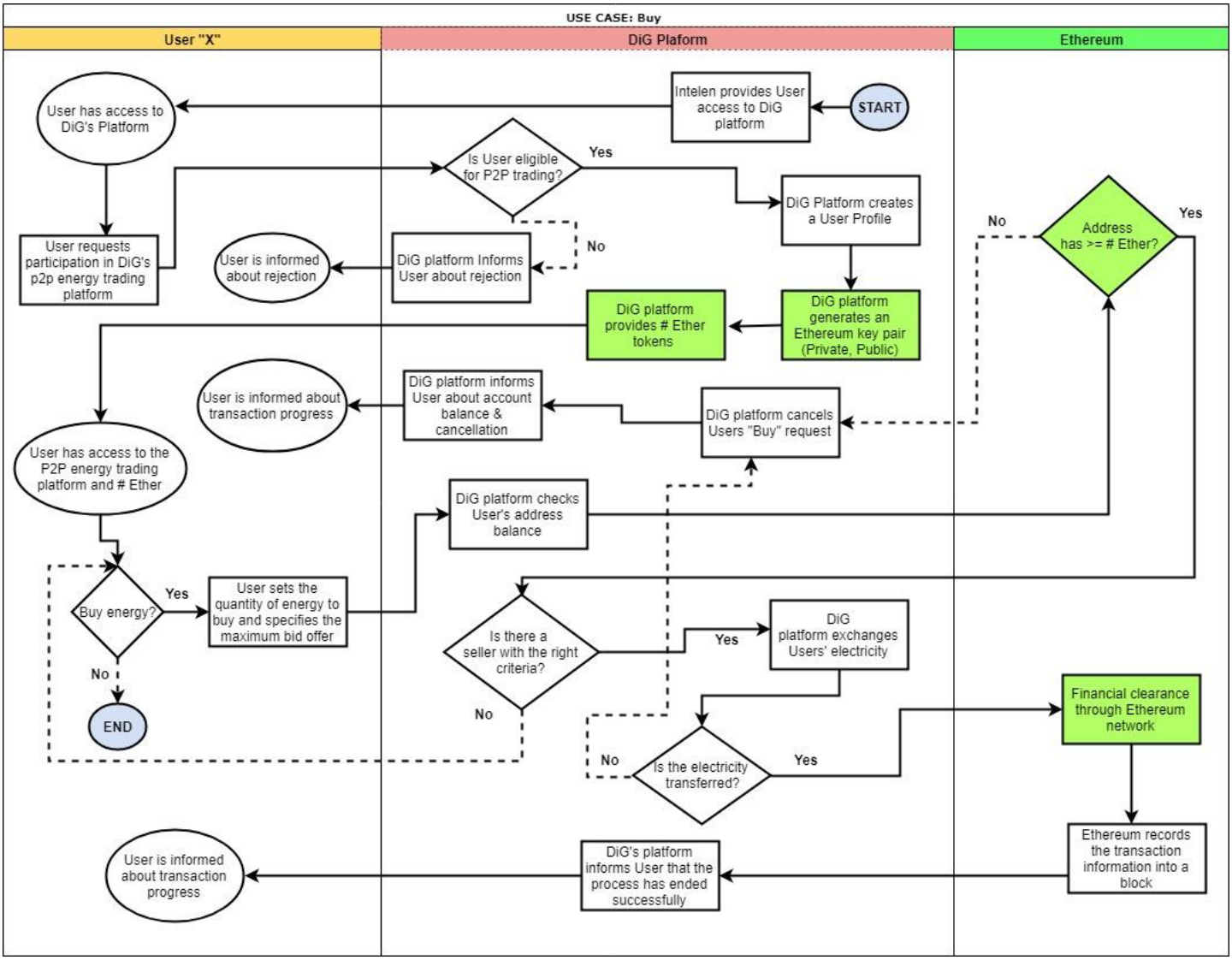

Εικόνα 7: Παρουσίαση αγοραπωλησία ηλεκτρικής ενέργειας:

## 5.2. Μελέτη περίπτωσης

Η μελέτη περίπτωσης έγινε σε συνεργασία με την εταιρία Intelen Inc., όπου καταλήξαμε στα εξής 2 σενάρια : a) Πώληση ηλεκτρικής Ενέργειας και b) Αγορά ηλεκτρικής Ενέργειας.

Στις δύο εικόνες που ακολουθούν παρουσιάζεται η ροή με την οποία οι χρήστες χρησιμοποιώντας την πλατφόρμα DiG της εταιρίας Intelen θα έχουν τη δυνατότητα να αγοράσουν ή να πουλήσουν την ηλεκτρική τους ενέργεια. Πιο αναλυτικά οι χρήστες μέσω της πλατφόρμας θα προμηθεύονται μια διεύθυνση Ethereum η οποία θα περιέχει ένα συγκεκριμένο αριθμό από κρυπτονομίσματα και οι συναλλαγές θα πραγματοποιούνται μέσα από το δίκτυο του Ethereum. Τα κουτάκια με πράσινο χρώμα αφορούν την αλληλεπίδραση των χρηστών με το Ethereum Blockchain.






## 5.3. Περιγραφή περιορισμών

Με βάση τις περιπτώσεις Buy και Sell η μεταφορά και αποθήκευση του ηλεκτρικού ρεύματος θα γίνει αρχικά σε πειραματικό στάδιο σε ψηφιακή μορφή σε συνεργασία με την εταιρεία Intelen. Επίσης η εταιρεία θα καθορίσει και θα υλοποιήσει τους αλγόριθμους τεχνητής νοημοσύνης για την οικιακή μπαταρία, έτσι ώστε να μπορεί η μπαταρία να τεθεί σε αυτόματη λειτουργία, διεξάγοντας αυτόματες αναλύσεις τάσεων σχετικά με τη ζήτηση, την προσφορά και την τιμή της ηλεκτρικής ενέργειας. Επίσης, με βάσει τις αναλύσεις της, η μπαταρία θα αποφασίζει να αγοράσει ή να πουλήσει ηλεκτρική ενέργεια.

## 5.4. Προτεινόμενη Λύση

Η λύση του προβλήματος όπως προαναφέρθηκε έχει χωριστεί σε 2 υποθέσεις :

a. αγορά ηλεκτρικής ενέργειας και
b. πώληση ηλεκτρικής ενέργειας.

Για να γίνει εφικτή λοιπόν η αποστολή και λήψη ηλεκτρικής ενέργειας καθώς και η αμοιβή ή χρέωση των χρηστών να πραγματοποιείται σε πραγματικό χρόνο θα πρέπει στα πλαίσια της διπλωματικής μου εργασίας να σχεδιαστούν και υλοποιηθούν τα ακόλουθα :

- HD Wallet το οποίο είναι ένα από τα πιο προηγμένα και ασφαλή ηλεκτρονικά πορτοφόλια για διευθύνσεις (addresses) που αφορούν το Ethereum Blockchain.
- Δημιουργία κρυπτονομίσματος με βάση το ERC20 standard και χρήση της γλώσσας προγραμματισμού Solidity.
- Smart Contract για την αποστολή και λήψη κρυπτονομισμάτων.
- Κώδικας ο οποίος θα επικοινωνεί με το δίκτυο Ethereum και με το Smart Contract έτσι ώστε να λαμβάνει πληροφορίες σχετικά με τις συναλλαγές των χρηστών και των έξυπνων οικιακών μπαταριών.

# 6. Τεχνολογίες και Εργαλεία

Οι τεχνολογίες που έχουν χρησιμοποιηθεί στην παρούσα διπλωματική εργασία αφορούν το δίκτυο Blockchain Ethereum.

## 6.1. Ethereum

Το Ethereum είναι μια ανοικτή Blockchain πλατφόρμα που επιτρέπει σε οποιονδήποτε να δημιουργεί και να χρησιμοποιεί αποκεντρωμένες εφαρμογές που λειτουργούν με τεχνολογία Blockchain. Προτάθηκε το 2013 από τον Vitalik Buterin πρώην προγραμματιστεί του Bitcoin και δόθηκε στη δημοσιότητα στις 30 Ιουλίου 2015. Όπως και στην περίπτωση του Bitcoin, έτσι και το Ethereum δεν ελέγχεται από κάποια κεντρική αρχή. Είναι μια πλατφόρμα ανοιχτού κώδικα που κατασκευάστηκε από πολλούς ανθρώπους σε όλο τον κόσμο. Αντίθετα με το πρωτόκολλο Bitcoin, το Ethereum σχεδιάστηκε για να είναι προσαρμόσιμο και ευέλικτο.

Το Ethereum είναι ένα προγραμματιζόμενο Blockchain. Αντί να δίνει στους χρήστες ένα σύνολο προκαθορισμένων λειτουργιών (π.χ. συναλλαγές bitcoin), το Ethereum επιτρέπει στους χρήστες να δημιουργούν τις δικές τους λειτουργίες οι οποίες ποικίλουν σε βαθμό δυσκολίας. Με τον τρόπο αυτό, χρησιμεύει ως πλατφόρμα για πολλούς διαφορετικούς τύπους αποκεντρωμένων εφαρμογών Blockchain, συμπεριλαμβανομένων, μεταξύ άλλων, των κρυπτονομισμάτων.

Το Ethereum αναφέρεται σε μια σειρά πρωτοκόλλων που δημιουργούν τελικά μια πλατφόρμα για αποκεντρωμένες εφαρμογές. Στην καρδιά του Ethereum βρίσκεται η εικονική μηχανή Ethereum Virtual Machine, η οποία μπορεί να εκτελέσει κώδικα οποιασδήποτε αλγοριθμικής πολυπλοκότητας. Στον τομέα της πληροφορικής, το Ethereum ονομάζεται "Turing complete", γεγονός που καταδεικνύει ότι θα μπορούσε να χρησιμοποιηθεί για την επίλυση οποιουδήποτε υπολογιστικού προβλήματος. Επίσης η εικονική μηχανή Ethereum ή EVM είναι εντελώς απομονωμένη, πράγμα που σημαίνει ότι ο κώδικας που τρέχει μέσα στο EVM δεν έχει πρόσβαση σε κανένα δίκτυο. Συνεπώς, ο κώδικας είναι απόλυτα ασφαλής.

Όπως κάθε Blockchain, το Ethereum περιλαμβάνει επίσης ένα πρωτόκολλο δικτύου Peer-2-Peer. Κάθε μπλοκ στο Ethereum διατηρείται και ενημερώνεται από πολλούς κόμβους που είναι συνδεδεμένοι στο δίκτυο. Κάθε κόμβος του δικτύου χρησιμοποιεί το EVM και εκτελεί ακριβώς τις ίδιες οδηγίες με τους υπόλοιπους κόμβους. Για το λόγο αυτό, το Ethereum μερικές φορές περιγράφεται με την έννοια του «παγκόσμιου υπολογιστή». Όμως δεν φτιάχτηκε για να αντικαταστήσει τους υπολογιστές και την επεξεργαστική τους ισχύ. Στην πραγματικότητα, το Ethereum είναι πολύ πιο αργό και πιο ακριβό από τον παραδοσιακό «υπολογιστή». Αυτό συμβαίνει διότι όλοι οι κόμβοι στο Ethereum επεξεργάζονται όλα τα δεδομένα που εισέρχονται σε αυτό και εκτελούν τις απαραίτητες διαδικασίες στο EVM προκειμένου να μην υπάρξει περιθώριο λάθους. Η επεξεργασία κάθε εισερχόμενου δεδομένου απ, όλους τους κόμβους δίνει στο Ethereum ακραία επίπεδα ανοχής σε σφάλματα, εξασφαλίζει μηδενικό χρόνο διακοπής λειτουργίας και καθιστά τα δεδομένα που είναι αποθηκευμένα στο Blockchain για πάντα αμετάβλητα (Laurence, 2017 , Antonopoulos, 2017).

## 6.2. Η λειτουργία του Ethereum

Το Ethereum ενσωματώνει πολλά χαρακτηριστικά και τεχνολογίες από το Bitcoin, ενώ ταυτόχρονα εισάγει πολλές δικές του τροποποιήσεις και καινοτομίες. Έτσι ενώ στην αλυσίδα Bitcoin το κάθε μπλοκ αποτελεί έναν κατάλογο συναλλαγών, η βασική ιδέα του Ethereum είναι η ανταλλαγή «δεδομένων» μεταξύ λογαριασμών (accounts). Δηλαδή το κάθε μπλοκ στο Ethereum παρακολουθεί την κατάσταση κάθε λογαριασμού και όλες οι μεταβολές που γίνονται στο Ethereum αφορούν μεταφορά «αξίας», δηλαδή κρυπτονομισμάτων και πληροφοριών μεταξύ λογαριασμών.

Υπάρχουν δύο τύποι λογαριασμών:

a. Externally Owned Accounts (EOA), οι οποίοι ελέγχονται από ιδιωτικά κλειδιά
b. Contract Accounts, οι οποίοι ελέγχονται από τον εσωτερικό τους κώδικα και μπορούν να «ενεργοποιηθούν» μόνο από έναν EOA

Η βασική διαφορά μεταξύ αυτών, είναι ότι ένας λογαριασμός EOA ελέγχεται από τους ίδιους τους χρήστες, καθώς μπορούν να ελέγχουν τα ιδιωτικά κλειδιά, τα οποία είναι απαραίτητα

για την ανάληψη του ελέγχου σε ένα τέτοιο λογαριασμό. Από την άλλη πλευρά οι λογαριασμοί Contract Accounts, ελέγχονται από τον εσωτερικό κώδικα τους. Εάν ελέγχονται από έναν συγκεκριμένο χρήστη (EOA), είναι επειδή έχουν προγραμματιστεί να ελέγχονται από αυτόν με μια συγκεκριμένη διεύθυνση, η οποία με τη σειρά της ελέγχεται από όποιον κατέχει τα ιδιωτικά κλειδιά.

Ο δημοφιλής όρος «Smart Contract» αναφέρεται σε κώδικα ο οποίος υπάρχει μέσα σε έναν λογαριασμό (Contract Account). Ο κώδικας εκτελείται όταν μια συναλλαγή αποστέλλεται στον λογαριασμό αυτό.

Όπως και στο Bitcoin, οι χρήστες πρέπει να πληρώνουν μικρά τέλη σε κάθε τους συναλλαγή στο δίκτυο και αυτό γίνεται για να προστατεύεται το Blockchain Ethereum από επιθέσεις. Εάν μια συναλλαγή αφορά λογαριασμό Contract Account τότε ο αποστολέας της συναλλαγής πρέπει να πληρώσει για κάθε βήμα του "κώδικα-προγράμματος" που ενεργοποίησε. Αυτά τα τέλη συναλλαγών συλλέγονται από τους κόμβους που επικυρώνουν τα δεδομένα στο δίκτυο. Το Ethereum Blockchain χρησιμοποιεί για τις συναλλαγές μεταξύ χρηστών ένα κρυπτονόμισμα το οποίο ονομάζεται «ether». Συνεπώς οι κόμβοι ανταμείβονται με ether για κάθε μπλοκ που επικυρώνουν.

Ο αλγόριθμος που χρησιμοποιείται για την επικύρωση των καινούργιων μπλοκ όπως και στο δίκτυο Bitcoin ονομάζεται Proof-of-Work. Οι κόμβοι καλούνται να επιλύσουν ένα πολύπλοκο μαθηματικό πρόβλημα προκειμένου να επικυρώσουν ένα μπλοκ. Στο δίκτυο Bitcoin, χρησιμοποιούνται από μερικούς κόμβους πολύ ακριβά εξειδικευμένα εργαλεία τα οποία παρέχουν μεγάλη επεξεργαστική ισχύ για την γρήγορη επεξεργασία των δεδομένων. Το Ethereum θέλοντας λοιπόν όλοι οι κόμβοι να είναι ίσοι, επέλεξε ένα μαθηματικό πρόβλημα το οποίο χρησιμοποιεί την μνήμη RAM του υπολογιστή αλλά ταυτόχρονα και το σκληρό του ηλεκτρονικού υπολογιστή. Με αυτόν τον τρόπο δεν μπορούν τα ισχυρά εργαλεία που χρησιμοποιούνται στο Bitcoin να χρησιμοποιηθούν και στο Ethereum διότι δεν χρησιμοποιούν την μνήμη RAM.

Όπως προαναφέρθηκε το ether είναι το όνομα του κρυπτονομίσματος που χρησιμοποιείται στο Blockchain Ethereum. Η μικρότερη ονομασία ως μονάδα μέτρησης του ether ονομάζεται Wei (Ethereum Homestead, 2018).

Παρακάτω είναι μια λίστα με τις υποδιαιρέσεις του ether και την αξία τους με βάση το Wei. Το ether αποτελείται από 18 δεκαδικά ψηφία.

| Unit | Wei Value | Wei |
|---|---|---|
| wei | 1 wei | 1 |
| Kwei (babbage) | 1e3 wei | 1,000 |
| Mwei (lovelace) | 1e6 wei | 1,000,000 |
| Gwei (shannon) | 1e9 wei | 1,000,000,000 |
| microether (szabo) | 1e12 wei | 1,000,000,000,000 |
| milliether (finney) | 1e15 wei | 1,000,000,000,000,000 |
| ether | 1e18 wei | 1,000,000,000,000,000,000 |

Εικόνα 8: Πίνακας υποκατηγοριών ether. Ανακτήθηκε από Ethereum Homestead (2018): Ιστοσελίδα http://ethdocs.org/en/latest/ether.html, Ανακτήθηκε Δεκέμβρης 24, 2017.

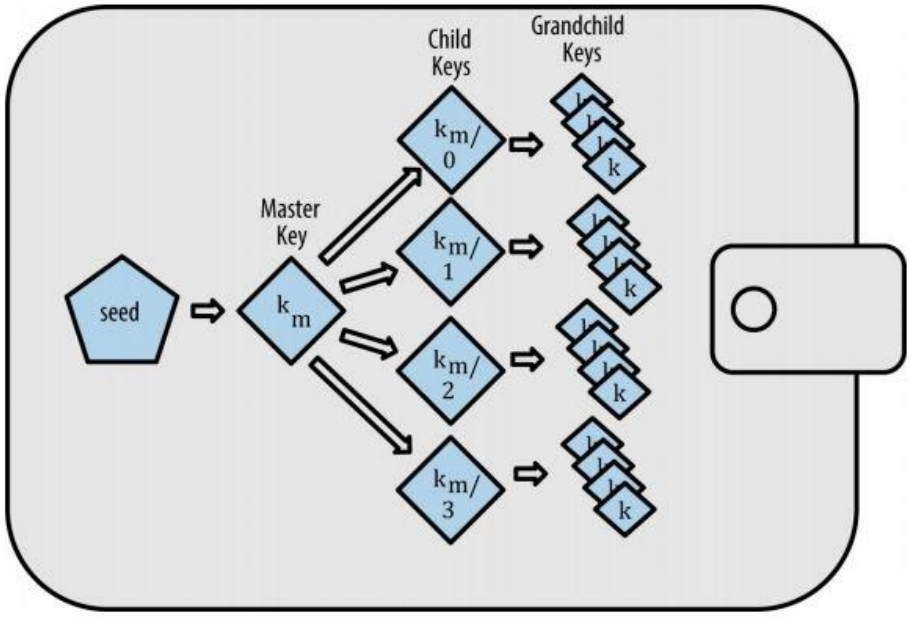
## 6.3. HD Wallet

Τα Hierarchical Deterministic ή «seeded» πορτοφόλια είναι τα πορτοφόλια που περιέχουν ιδιωτικά κλειδιά τα οποία προέρχονται όλα από ένα κοινό «σπόρο» (seed), και έχουν δημιουργηθεί μέσω της χρήσης μιας μονόδρομης λειτουργίας κατακερματισμού Hash. Το ψηφιακό πορτοφόλι HD είναι η πιο προηγμένη μορφή πορτοφολιού και ορίζεται συγκεκριμένα από το πρότυπο BIP-32.

Τα HD πορτοφόλια αναπτύχθηκαν για να καταστήσουν εύκολη την εξαγωγή πολλών κλειδιών από έναν ενιαίο «σπόρο» ο οποίος είναι συνήθως 12 τυχαίες Αγγλικές λέξεις. Επίσης σε ένα τέτοιο ντετερμινιστικό πορτοφόλι, ο «σπόρος» μπορεί να ανακτήσει όλα τα παράγωγα κλειδιά που έχουν ήδη δημιουργηθεί και να εξάγει ή να εισαγάγει ένα πορτοφόλι, επιτρέποντας την εύκολη μετακίνηση όλων των κλειδιών του χρήστη μεταξύ διαφορετικών υλοποιήσεων πορτοφολιού.

Στην εικόνα που ακολουθεί βλέπουμε ένα HD πορτοφόλι να περιέχει κλειδιά που παράγονται σε μια δομή δέντρου, έτσι ώστε ένα γονικό κλειδί (Master Key) να μπορεί να

παράγει μια σειρά από κλειδιά (Chilled keys), καθένα από τα οποία μπορεί να δημιουργήσει μια σειρά από καινούργια κλειδιά (Grand chilled Keys).




Εικόνα 9: Hierarchical Deterministic Wallet . Ανακτήθηκε από Mastering Bitcoin (2015): Βιβλίο από τον Andreas Antonopoulos, Ανακτήθηκε Δεκέμβρης 26, 2017.

Τα πορτοφόλια HD προσφέρουν δύο σημαντικά πλεονεκτήματα σε σχέση με τα τυχαία (μη ντετερμινιστικά) κλειδιά.

Πρώτον, η δομή του «δέντρου» κλειδιών μας επιτρέπει να χρησιμοποιήσουμε κάθε κλειδί για διαφορετικό σκοπό, όπως για παράδειγμα σε μια εταιρεία κάθε κλειδί θα μπορούσε να ανήκει σε κάθε τμήμα που ασχολείται με τις συναλλαγές. Έχοντας πάντα τον έλεγχο όλων των κλειδιών μέσα από τον κύριο μοναδικό «σπόρο».

Το δεύτερο πλεονέκτημα των πορτοφολιών HD είναι ότι οι χρήστες μπορούν να δημιουργήσουν μια σειρά δημόσιων κλειδιών χωρίς να έχουν πρόσβαση στα αντίστοιχα ιδιωτικά κλειδιά. Αυτό επιτρέπει στα πορτοφόλια HD να χρησιμοποιούνται σε ένα μη ασφαλές διακομιστή, εκδίδοντας για κάθε συναλλαγή ένα διαφορετικό δημόσιο κλειδί (Antonopoulos, 2017).

## 6.4. Token ERC20

Το 2015, το δίκτυο Ethereum Blockchain εξέδωσε τις τεχνικές προδιαγραφές για τα Tokens που ανταλλάζονται μέσα στο δίκτυο. Τα Tokens που συμμορφώνονται με αυτές τις προδιαγραφές είναι γνωστά ως Tokens ERC20. Το ERC σημαίνει Ethereum Request for Comments και το,20, είναι ο αριθμός αναγνωριστικού της πρότασης.

Στην ουσία, τα Tokens ERC20 είναι έξυπνα συμβόλαια (Smart Contracts) στο Blockchain του Ethereum. Μάλιστα, ενώ οι προδιαγραφές των Tokens ERC20 λειτουργούν με βάση κανόνες, οι προγραμματιστές που προτείνανε αυτή την προδιαγραφή, επιτρέπουν στους υπόλοιπους προγραμματιστές να διαμορφώσουν τη λειτουργία των Tokens.

Δεδομένου ότι τα περισσότερα Tokens που δημιουργούνται στο Ethereum είναι συμβατά με το πρότυπο ERC20, κρίνεται σκόπιμη η μελέτη του συγκεκριμένου τύπου Tokens. Το πρότυπο ERC20 διαθέτει 6 λειτουργίες (functions) και 2 event. Το πρότυπο δημιουργήθηκε για να επιτρέπει τη διαλειτουργικότητα μεταξύ εφαρμογών. Οι 6 λειτουργίες περιγράφουν τον τρόπο με τον οποίο τα Tokens μπορούν να σταλούν και τον τρόπο με τον οποίο μπορούν να αποκτήσουν πρόσβαση οι χρήστες στα δεδομένα που σχετίζονται με τα εκάστοτε Token. Τα event περιλαμβάνουν ενημερώσεις σχετικά με τις ενέργειες που έχουν γίνει σε μια λειτουργία του Token (ERC20 Token Standard, 2018 , Nathan, 2017).

Στην κάτω εικόνα παρουσιάζεται το πρότυπο ERC20 το οποίο αποτελείται από τις 6 λειτουργίες και τα 2 event:

```
// ----------------------------------------------------------------------------
// ERC Token Standard #20 Interface
// https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md
// ----------------------------------------------------------------------------
contract ERC20Interface {
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint balance);
    function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool success);
    function transferFrom(address from, address to, uint tokens) public returns (bool success);

    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

Εικόνα 10: ERC20 Standard. Ανακτήθηκε από www.github.com/Ethereum/EIPs: Ανακτήθηκε Γενάρης 10, 2018.

## 6.5. Solidity

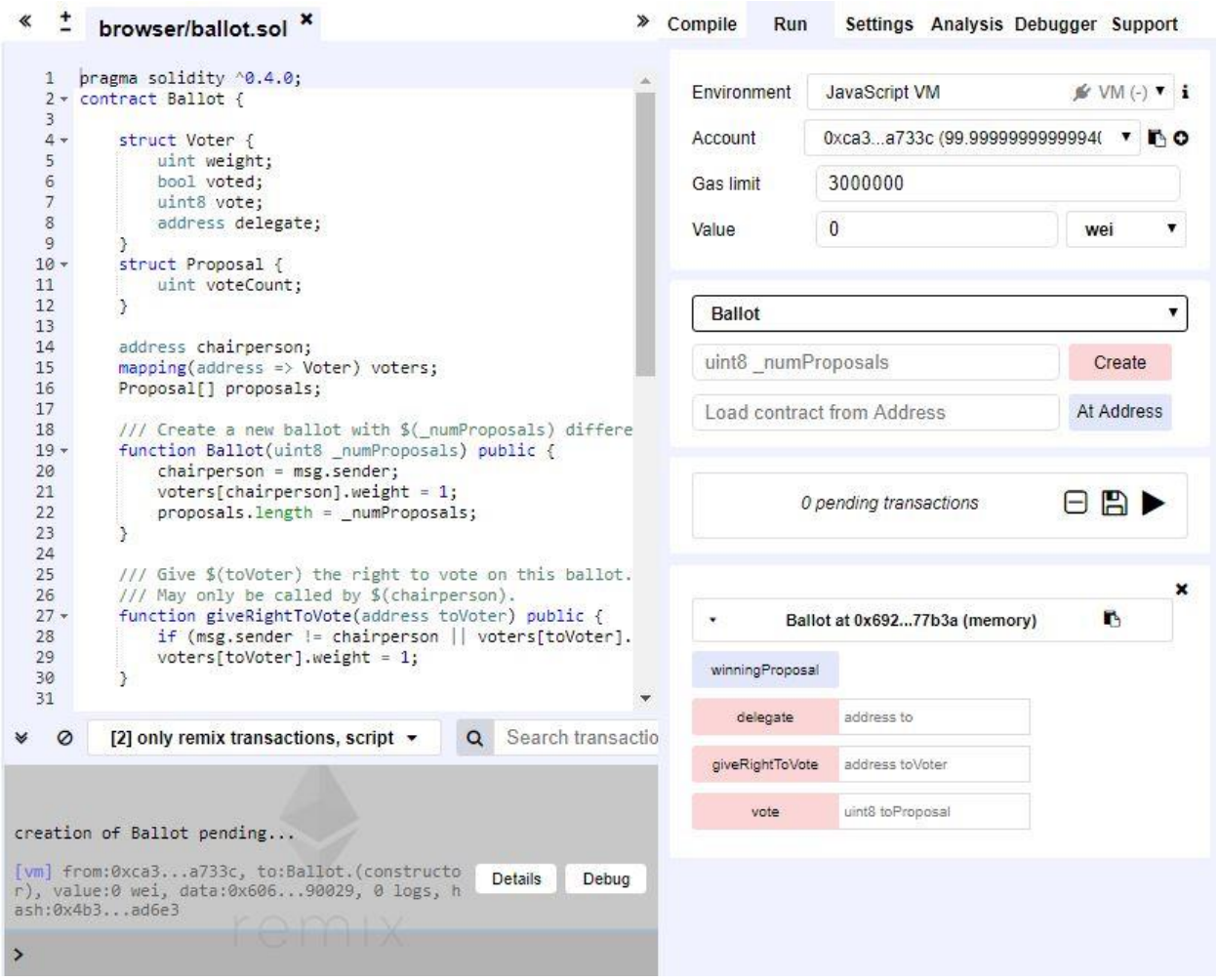
Η γλώσσα προγραμματισμού Solidity προτάθηκε αρχικά τον Αύγουστο του 2014 από τον Gavin Wood. Η γλώσσα αναπτύχθηκε αργότερα από την ομάδα Solidity του Ethereum, με επικεφαλής τον Christian Reitwiessner. Είναι μία από τις τέσσερις γλώσσες που έχουν σχεδιαστεί για να εκτελούνται με βάση την εικονική μηχανή (EVM) του Ethereum και είναι η πιο γνωστή και ευρέως χρησιμοποιούμενη γλώσσα για το συγκεκριμένο δίκτυο.

Η Solidity είναι γνωστή ως γλώσσα προγραμματισμού υψηλού επιπέδου. Είναι επίσης μια στατική γλώσσα προγραμματισμού σχεδιασμένη για την ανάπτυξη έξυπνων συμβολαίων (Smart Contracts) που εκτελούνται στο EVM. Τα αρχεία Solidity (.sol) για να μπορούν να διαβαστούν και να εκτελεστούν μέσα από την εικονική μηχανή (EVM) του Ethereum θα πρέπει να μετατραπούν σε γλώσσα μηχανής (bytecode). Ακόμη η Solidity επιτρέπει στους προγραμματιστές να γράψουν κώδικα οποιασδήποτε αλγοριθμικής πολυπλοκότητας (Solidity, 2018).

## 6.6. Remix-IDE

Το Remix-IDE, γνωστό στο παρελθόν με την ονομασία "Browser Solidity", είναι ένα διαδικτυακό ολοκληρωμένο περιβάλλον ανάπτυξης κώδικα (Integrated Development Environment, IDE), το οποίο επιτρέπει στους χρήστες να δημιουργούν Smart Contracts στο Blockchain του Ethereum με τη γλώσσα προγραμματισμού Solidity. Το Remix-IDE επίσης προσφέρει στους προγραμματιστές την δυνατότητα να εντοπίζουν σφάλματα στο κώδικα και στις συναλλαγές αφού συνδέεται με ένα εικονικό δίκτυο Ethereum. Το Remix-IDE βρίσκεται στην ιστοσελίδα: https://remix.ethereum.org (Ethereum, 2018).

Στην παρακάτω εικόνα βλέπουμε ένα παράδειγμα του περιβάλλοντος Remix-IDE:



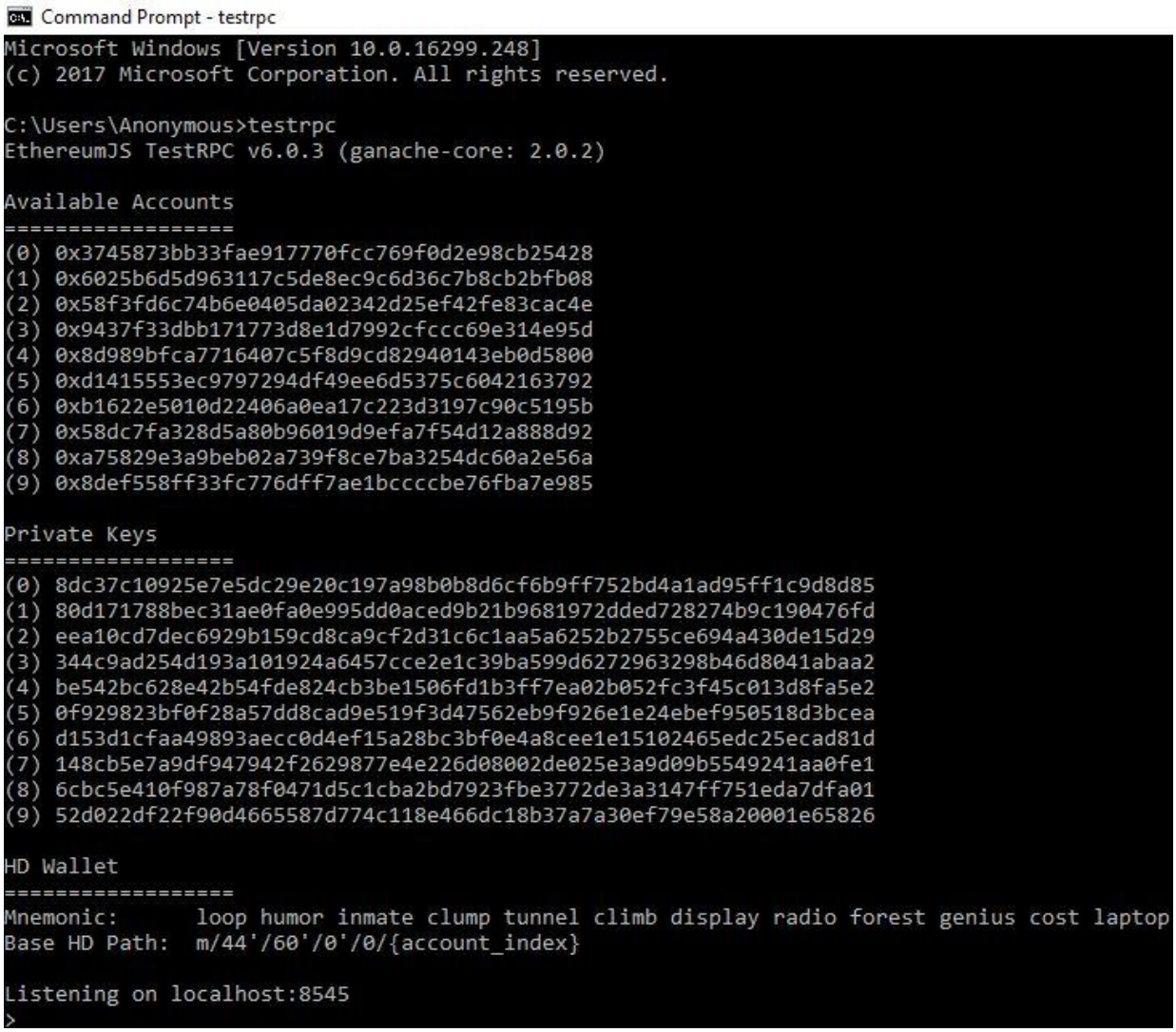

Εικόνα 11: Remix_IDE. Ανακτήθηκε από https://remix.ethereum.org/:

Ανακτήθηκε Φεβρουάριος 07, 2018.

## 6.7. TestRPC

Το TestRPC δημιουργεί ένα εικονικό δίκτυο Ethereum στον υπολογιστή, το οποίο κληρονομεί όλα τα χαρακτηριστικά του πραγματικού δικτύου Ethereum. Ταυτόχρονα μας παρέχει 10 διευθύνσεις (addresses) Ethereum μαζί με τα ιδιωτικά τους κλειδιά. Όλες οι διευθύνσεις έχουν δημιουργηθεί μέσα από ένα HD Wallet με κοινό «σπόρο» (seed). Ο συγκεκριμένος σπόρος είναι οι 12 Αγγλικές λέξεις που εμφανίζονται στο κάτω μέρος της εικόνας. Η κάθε διεύθυνση έχει ενσωματωμένα 100 Ether. Το Remix-IDE έχει τη δυνατότητα να συνδεθεί με το TestRPC (ethereumjs-testrpc, 2018).

Στην παρακάτω εικόνα βλέπουμε ένα παράδειγμα TestRPC :




Εικόνα 12: testRPC Ethereum network. Φεβρουάριος 07, 2018.

# 7. Υλοποίηση

Στα πλαίσια της παρούσας διπλωματικής εργασίας έχει δημιουργηθεί ένα HD Wallet για την δημιουργία λογαριασμών Ethereum, κρυπτονόμισμα με βάση το ERC20 standard, Smart Contract για την αποστολή και λήψη κρυπτονομισμάτων και τέλος μια ιστοσελίδα η οποία επικοινωνεί με το Smart Contract.

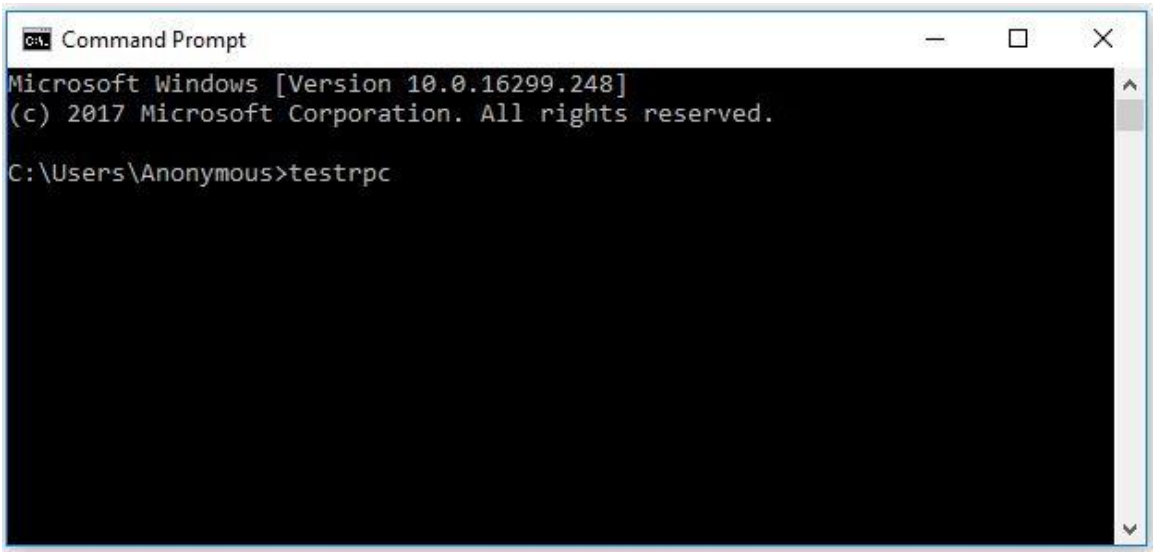
Αρχικά θα γίνει περιγραφή και επεξήγηση του εργαλείου TestRPC, όπου στη συνέχεια μέσα από την ιστοσελίδα θα δημιουργηθούν διευθύνσεις Ethereum χρησιμοποιώντας το HD Wallet. Σε περίπτωση που ο χρήστης ξεχάσει τις διευθύνσεις και τα Private Keys υπάρχει η δυνατότητα για την επανάκτηση τους χρησιμοποιώντας τον «σπόρο» (seed). Στην συνέχεια με τη βοήθεια των διευθύνσεων από το TestRPC θα σταλούν μερικά ether στην δικιά μου διεύθυνση Ethereum. Μέσα από την ιστοσελίδα, θα έχω τη δυνατότητα να δημιουργήσω το δικό μου κρυπτονόμισμα αφού πρώτα γίνει επεξήγηση του Smart Contract του Token.

Τέλος, έχοντας δημιουργήσει το δικό μου κρυπτονόμισμα θα αγοράσω μερικά Tokens χρησιμοποιώντας τις υπόλοιπες διευθύνσεις από το TestRPC. Μέσα από την δημιουργία του Smart Contract θα μπορούνε οι έξυπνες οικιακές μπαταρίες να συναλλάσσονται χωρίς καμία παρέμβασή από κάποια κεντρική αρχή.

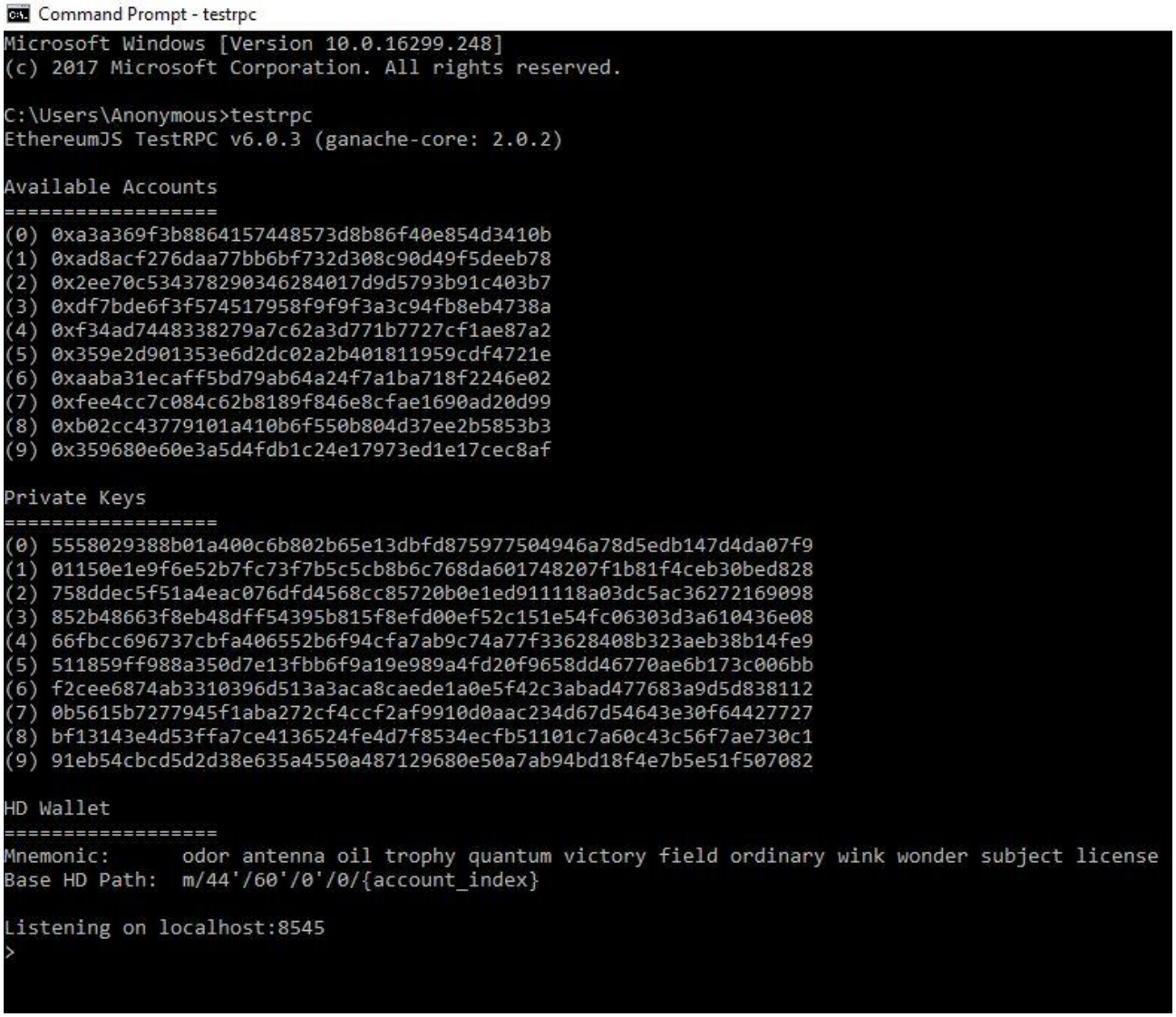
**TestRPC**

Αρχικά θα πρέπει να χρησιμοποιηθεί το εργαλείο TestRPC, έτσι ώστε να δημιουργηθεί ένα εικονικό δίκτυο Ethereum τοπικά στον υπολογιστή. Το εικονικό δίκτυο κληρονομεί όλα τα χαρακτηριστικά του πραγματικού δικτύου Ethereum και υπάρχει η δυνατότητα παρακολούθησης όλων των συναλλαγών του δικτύου. Ταυτόχρονα μας παρέχει 10 διευθύνσεις (addresses) Ethereum μαζί με τα ιδιωτικά τους κλειδιά. Η κάθε διεύθυνση έχει στην κατοχή της 100 εικονικά ETH και αυτό θα μας βοηθήσει να δημιουργήσουμε τις δικές μας συναλλαγές χρησιμοποιώντας το HD Wallet.

Μέσα από το Command Prompt καλούμε το εργαλείο testrpc:

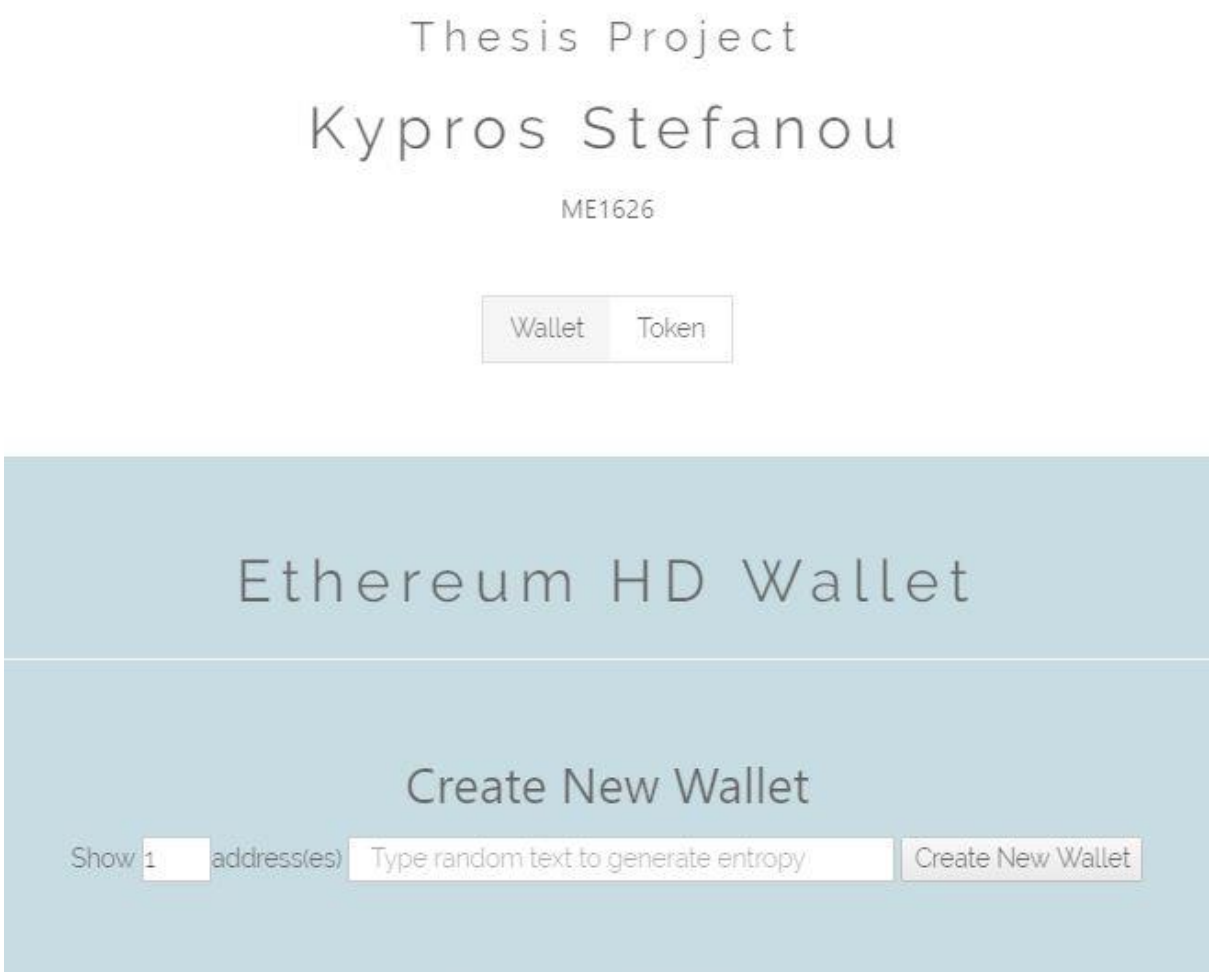



Στην παρακάτω εικόνα παρουσιάζεται το εικονικό δίκτυο Ethereum με τις 10 διευθύνσεις:

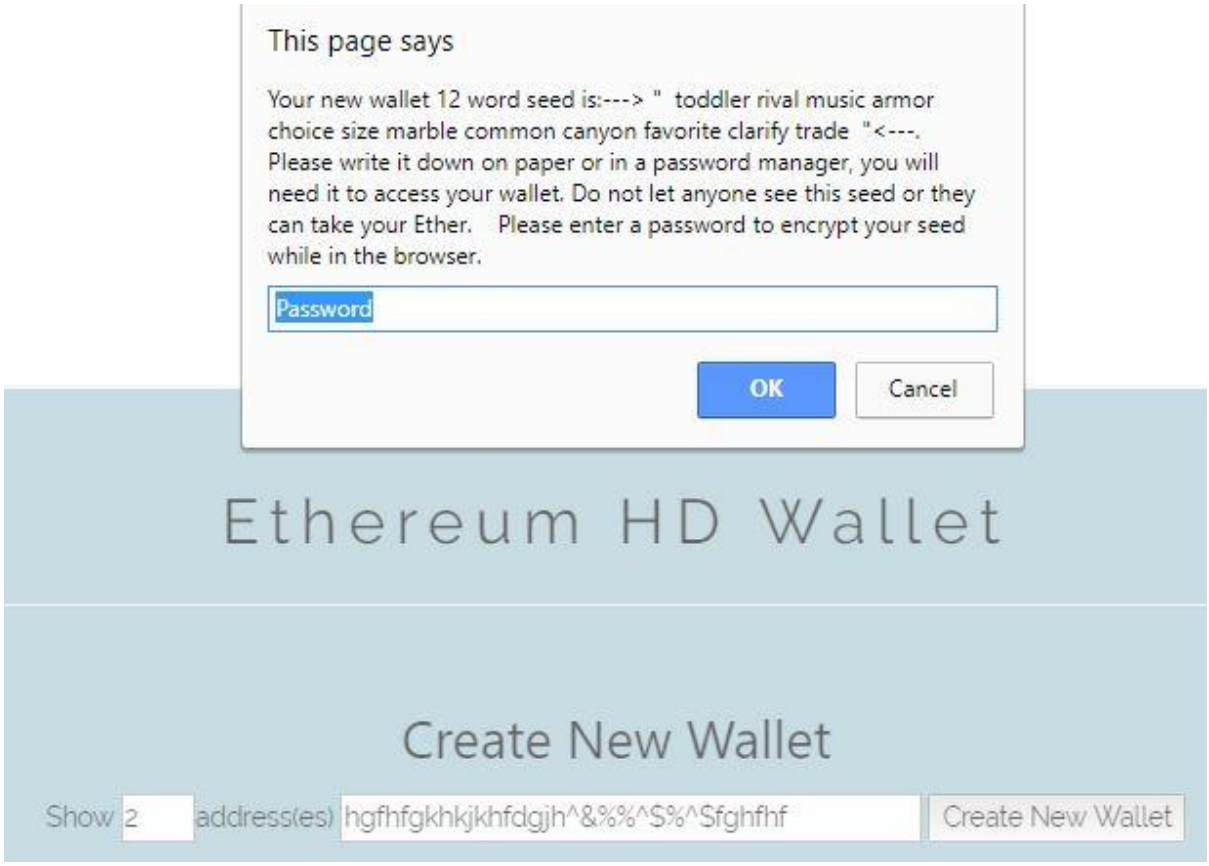


## 7.1. Ιστοσελίδα-Wallet

Στην παρακάτω εικόνα παρουσιάζεται το HD Wallet :




Όπως παρουσιάζεται στην παραπάνω εικόνα μπορούμε να εισάγουμε στο πρώτο κουτί τον αριθμό των διευθύνσεων που επιθυμούμε να δημιουργηθούνε και στο αμέσως επόμενο κουτί πληκτρολογούμε τυχαία γράμματα, αριθμούς και σύμβολα. Με αυτό τον τρόπο γίνεται ακόμη πιο μικρή η πιθανότητα να δημιουργηθούνε 2 ίδιες διευθύνσεις Ethereum. Στη συνέχεια πατάμε το κουμπί Create New Wallet:




Μόλις πατήσουμε το κουμπί για τη δημιουργία του πορτοφολιού, όπως φαίνεται στην παραπάνω εικόνα, εμφανίζεται ένα μήνυμα το οποίο μας δίνει τον «σπόρο» (seed) που χρησιμοποιήθηκε για την δημιουργία των 2 διευθύνσεων. Ο «σπόρος» όπως φαίνεται στο μήνυμα μας δίνει τις εξής 12 Αγγλικές λέξεις: toddler rival music armor choice size marble common canyon favorite clarify trade. Στη συνέχεια μας ζητάει να εισάγουμε ένα κωδικό με τον οποίο θα κρυπτογραφήσουμε τον «σπόρο». Δηλαδή αν κάποιος καταφέρει να κλέψει από εμάς το «σπόρο» και προσπαθήσει να επαναφέρει το πορτοφόλι για να μας κλέψει τα κρυπτονομίσματα, θα του ζητηθεί ο κωδικός που χρησιμοποιήθηκε για την κρυπτογράφηση του. Άρα ο κωδικός μας παρέχει μια έξτρα ασφάλεια.

Μόλις πατήσουμε το κουμπί OK μας εμφανίζονται στην οθόνη  οι 2 διευθύνσεις Ethereum όπως φαίνεται στην παρακάτω εικόνα:

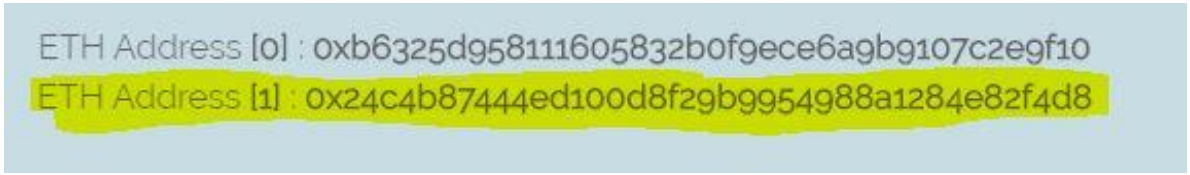

Αν χρειαστεί να γίνει επαναφορά του πορτοφολιού, θα πρέπει να γίνει η εισαγωγή των 12 Αγγλικών λέξεων, όπως φαίνεται στην παρακάτω εικόνα με κίτρινο χρώμα, οι οποίες αποτελούνε το σπόρο των διευθύνσεων μας. Μόλις πατήσουμε το κουμπί Restore για ανάκτηση του πορτοφολιού, εμφανίζεται ένα μήνυμα στο οποίο θα πρέπει να εισάγουμε τον κωδικό με τον οποίο έγινε η κρυπτογράφηση του «σπόρου».

Μόλις πατήσουμε το κουμπί OK μας εμφανίζονται στην οθόνη οι 2 διευθύνσεις Ethereum όπως παρουσιάζεται στην παρακάτω εικόνα:


Σε επόμενο βήμα θα γίνει αποστολή μερικών ether από την 1η διεύθυνση του TestRPC στην διεύθυνση που δημιουργήσαμε παραπάνω. Στην παρακάτω εικόνα παρατηρούμε 4 πεδία για εισαγωγή δεδομένων και ένα κουμπί send ether. Το πρώτο πεδίο είναι το «From», από πια διεύθυνση δηλαδή θα σταλούν τα ether, αμέσως δεξιά είναι το πεδίο για να εισάγουμε το Private Key της εκάστοτε διεύθυνσης. Στο πεδίο «To» θα εισάγουμε τη διεύθυνση που θα λάβει τα ether και τέλος στο πεδίο «Ether» εισάγουμε το ποσό που θα στείλουμε.

Η πρώτη διεύθυνση στο TestRPC είναι η :


Και από τις διευθύνσεις μου θα επιλέξω την 2η :




Στην παρακάτω εικόνα έγινε η εισαγωγή των διευθύνσεων που προανέφερα για την αποστολή 6 Ether στην διεύθυνση μας. Για την αποστολή των ether δεν χρειάστηκε να εισάγουμε το Private Key της διεύθυνσης του TestRPC και ο λόγος είναι ότι το εικονικό δίκτυο μας επιτρέπει να μην εισάγουμε το ιδιωτικό κλειδί για να γίνεται η διαδικασία πιο γρήγορα. Αν όμως χρησιμοποιήσουμε τη δική μας διεύθυνση Ethereum θα χρειαστεί να εισάγουμε το Private key μας.

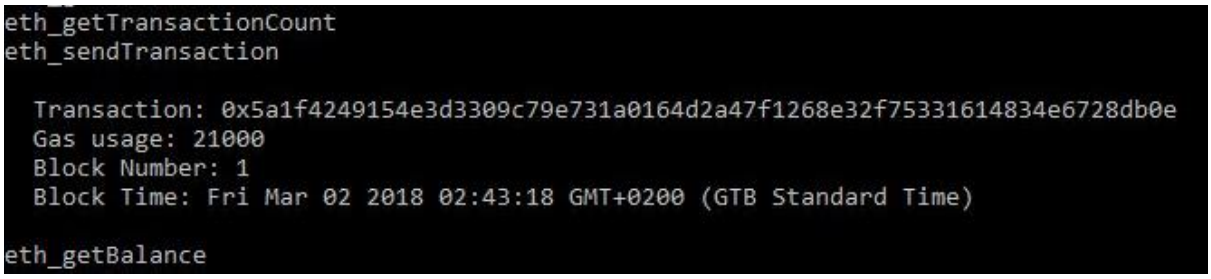
Μετά την ολοκλήρωση της αποστολής ether μπορούμε να δούμε στην πιο κάτω εικόνα τα δεδομένα που αποθηκεύονται στο Blockchain μέσα από το εικονικό δίκτυο Ethereum τα οποία είναι:

Transaction: είναι η απόδειξη της συναλλαγής.

Gas usage: είναι η συνολική τιμή σε μονάδα μέτρησης Wei που έχει πληρώσει ο χρήστης για την επικύρωση της συναλλαγής.

Block Number: είναι ο αριθμός μπλοκ που έχει αποθηκευτεί η συναλλαγή.

Block Time: είναι η ημερομηνία που έχει δημιουργηθεί η συναλλαγή.

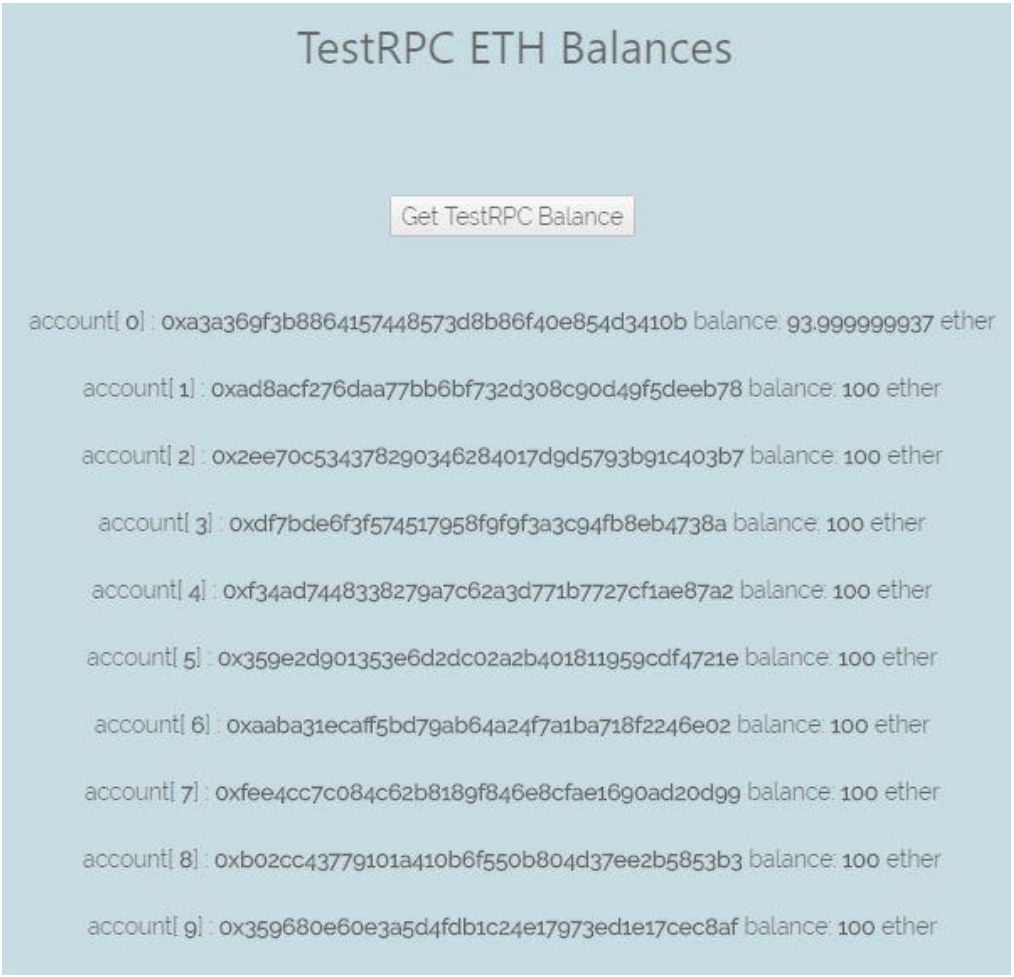



Εν συνεχεία μπορούμε να δούμε το υπόλοιπο κάθε διεύθυνσης όπως παρουσιάζεται στις 2 πιο κάτω εικόνες:

Η διεύθυνση μας

Διεύθυνση TestRPC


Στην παραπάνω εικόνα παρατηρούμε ότι το υπόλοιπο από τη διεύθυνση TestRPC είναι 93.9 ενώ θα έπρεπε να έχουν απομείνει 94 ether (100-6). Ο λόγος είναι ότι για να μπορεί να γίνει η μεταφορά των κρυπτονομισμάτων από τη μια διεύθυνση στην άλλη θα πρέπει ο αποστολέας να πληρώσει κάποια «τέλη» (gas) στον κόμβο που θα επικυρώσει την συναλλαγή. Τέλος μέσα από την ιστοσελίδα μας δίνεται η δυνατότητα να παρακολουθούμε το υπόλοιπο όλων των διευθύνσεων TestRPC:



## 7.2. Smart Contract - Token

Το Smart Contract υλοποιήθηκε μέσα από το διαδικτυακό εργαλείο Remix-IDE και δεν είναι τίποτα περισσότερο από ένα αρχείο υπολογιστή στο οποίο δίνουμε ένα περιγραφικό όνομα και την κατάληξη « .sol ». Η γλώσσα προγραμματισμού που χρησιμοποιήθηκε είναι η Solidity.

Για την υλοποίηση του Token αλλά και της ανταλλαγής των κρυπτονομισμάτων κρίνεται σκόπιμη η δημιουργία μιας μαθηματικής ψηφιακής βιβλιοθήκης εντός του Smart Contract. Σε κάθε σημείο του Smart Contract που απαιτεί μαθηματικές πράξεις θα γίνεται αναφορά στη μαθηματική βιβλιοθήκη για να μειώσουμε την πιθανότητα λάθους κατά τις προσαφαιρέσεις των κρυπτονομισμάτων από τους διάφορους λογαριασμούς. Στην παρακάτω εικόνα παρουσιάζεται η μαθηματική βιβλιοθήκη με ονομασία SafeMath:

browser/KypCoin.sol

```
pragma solidity ^0.4.16;

library SafeMath {
  /**
  * @dev Multiplies two numbers, throws on overflow.
  */
  function mul(uint256 a, uint256 b) internal pure returns (uint256) {
    if (a == 0) {
      return 0;
    }
    uint256 c = a * b;
    assert(c / a == b);
    return c;
  }
  /**
  * @dev Integer division of two numbers, truncating the quotient.
  */
  function div(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a / b;
    return c;
  }
  /**
  * @dev Substracts two numbers, throws on overflow
  */
  function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    assert(b <= a);
    return a - b;
  }
  /**
  * @dev Adds two numbers, throws on overflow.
  */
  function add(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a + b;
    assert(c >= a);
    return c;
  }
}
```

Ακολούθως όπως φαίνεται στην παρακάτω εικόνα γίνεται χρήση του ERC20 Standard. Όπως προανέφερα στο κεφάλαιο 8.4, το ERC20 μας επιτρέπει να χρησιμοποιήσουμε 6 λειτουργίες και στα πλαίσια της διπλωματικής μου εργασίας θα γίνει χρήση 3 λειτουργιών και ενός event τα οποία είναι :

TotalSypply: επιστρέφει το συνολικό ποσό του κρυπτονομίσματος που έχει δημιουργηθεί.

balanceOf: επιστρέφει το ποσό Tokens που ένας λογαριασμός διαθέτει.

transfer: γίνεται μεταφορά κρυπτονομισμάτων από ένα λογαριασμό σε ένα άλλο.

Και τέλος το event Transfer μας επιστρέφει τα δεδομένα που αφορούν μια συναλλαγή.

```
contract ERC20Basic {

  function totalSupply() public view returns (uint256);
  function balanceOf(address who) public view returns (uint256);
  function transfer(address _to, uint256 _value) public returns (bool);

  event Transfer(address indexed from, address indexed to, uint256 value);
}
```

Έπειτα, ακολουθεί ο κεντρικός κώδικας του Smart Contract, όπου μέσα από διάφορες εντολές δημιουργείτε το κρυπτονόμισμα με τα χαρακτηριστικά που επιθυμούμε, καθώς και οι λειτουργίες που επιτρέπουν σε ένα λογαριασμό Ethereum να αγοράσει και να ξοδέψει το συγκεκριμένο κρυπτονόμισμα.

Στην παρακάτω εικόνα παρουσιάζεται ένα μέρος του κώδικα του κρυπτονομίσματος, το οποίο είναι και το σημαντικότερο. Αφορά τα χαρακτηριστικά που ένα Token θα πρέπει να έχει:

```
function myCoin() public{

    owner= msg.sender;

    balanceOf[owner]= totalSupply= 10000 * 10 ** uint256(decimals);

    name="KypCoin";
    symbol="KYP";
    decimals=18;

    BuyRate=200; // 1 ether = 200 KypCoin

}
```

Στην πρώτη γραμμή υπάρχει το **owner=msg.sender;** . Γίνεται δήλωση ότι ο ιδιοκτήτης (owner) του κρυπτονομίσματος είναι αυτός που θα το δημιουργήσει. Σε αυτή την περίπτωση, θα αποθηκευτεί στη μεταβλητή owner η διεύθυνση Ethereum που θα δημιουργήσει αυτό το Smart Contract. Θα μπορούσαμε βέβαια να θέσουμε μια άλλη διεύθυνση.

Στην επόμενη γραμμή υπάρχει το :

**balanceOf [owner] = totalSupply = 10000 * 10 ** uint256(decimals);** όπου σε αυτό το σημείο τοποθετούνται στην διεύθυνση owner 10000 Tokens, τα οποία θα έχουνε μέχρι 18 δεκαδικά ψηφία.

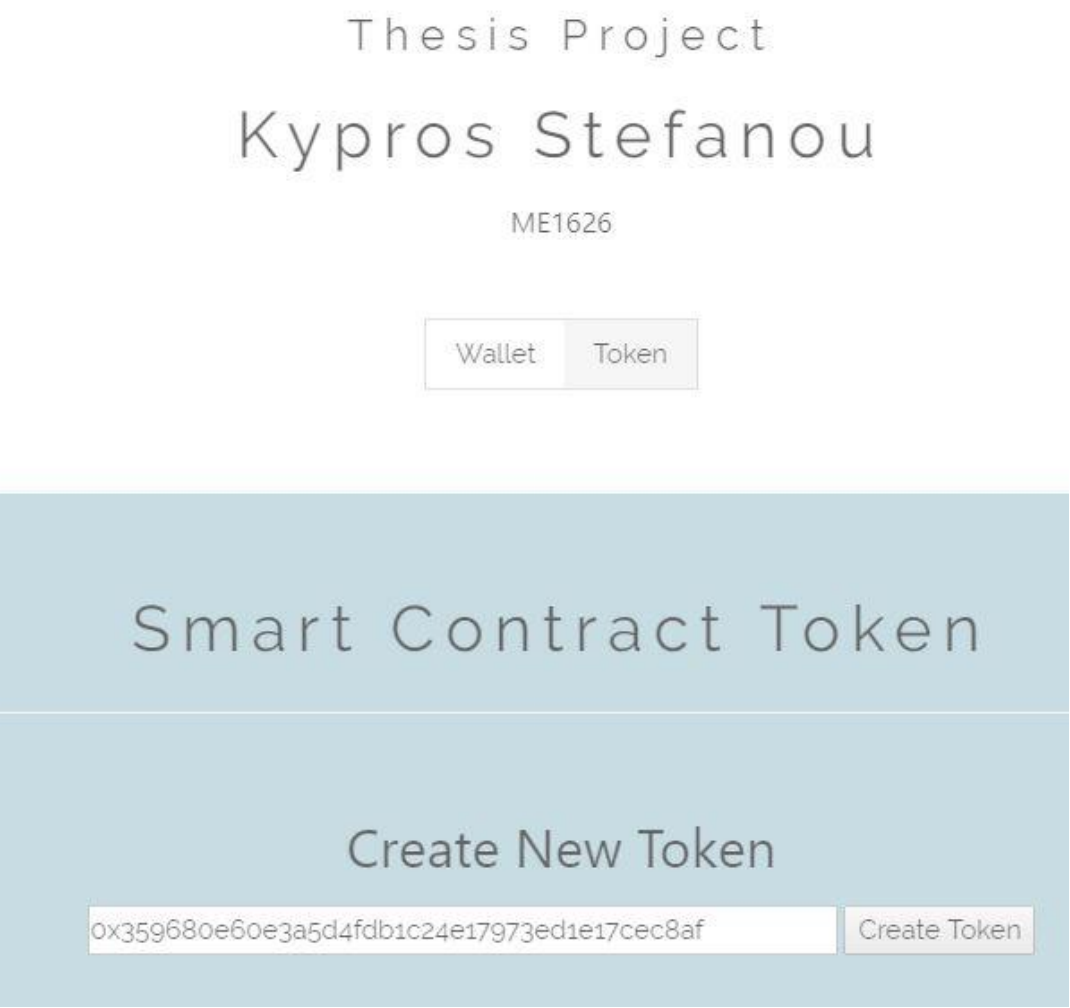
Στη συνέχεια γίνεται δήλωση του ονόματος του κρυπτονομίσματος **name="KypCoin";** , του συμβόλου **symbol="KYP";** , των δεκαδικών ψηφίων **decimals=18;** Και τέλος γίνεται αναφορά στο Buy Rate, στο οποίο καθορίζουμε την ισοτιμία ether και Token **BuyRate=200; // 1 ether = 200 KypCoin** . Στην συγκεκριμένη περίπτωση έχω θέση την ισοτιμία ως εξής: 1 ether = 200 kypCoin.

Αξίζει να σημειωθεί ότι όταν ένας λογαριασμός αγοράσει ένα ποσό από το κρυπτονόμισμα KypCoin τα ether θα μεταφερθούνε στην διεύθυνση αυτού που δημιούργησε το Smart Contract.

Αφού προηγήθηκε η περιγραφή του Smart Contract θα ακολουθήσει η περιγραφή του τρόπου με τον οποίο ένας λογαριασμός Ethereum μπορεί να «ανεβάσει» το συγκεκριμένο Smart Contract για πάντα στο Blockahin του Ethereum.

Αρχικά επιλέγουμε ένα λογαριασμό από το testRPC όπως φαίνεται στην παρακάτω εικόνα:


και τοποθετούμε την συγκεκριμένη διεύθυνση στην ιστοσελίδα :

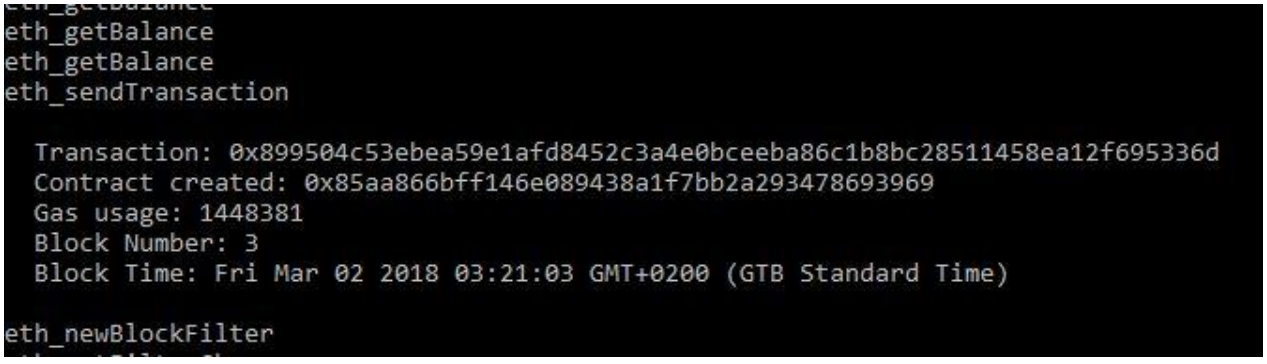


Πατώντας λοιπόν το κουμπί Create Token η διεύθυνση που φαίνεται στην πιο πάνω εικόνα γίνεται ο **owner** του Token. Με το που πατήσουμε το κουμπί το αρχείο του Smart Contract μετατρέπεται σε γλώσσα μηχανής bytecode για να μπορεί το EVM του Ethereum να το διαβάσει και να το καταχωρήσει μέσα στο Blockchain. Ο αποστολέας (owner) του Smart Contract πληρώνει από τον λογαριασμό του ένα μικρό ποσό (gas) για την επικύρωση του συμβολαίου. Μόλις το συμβόλαιο επικυρωθεί αυτόματα δημιουργείται και μια διεύθυνση Ethereum για το συγκεκριμένο Smart Contract.

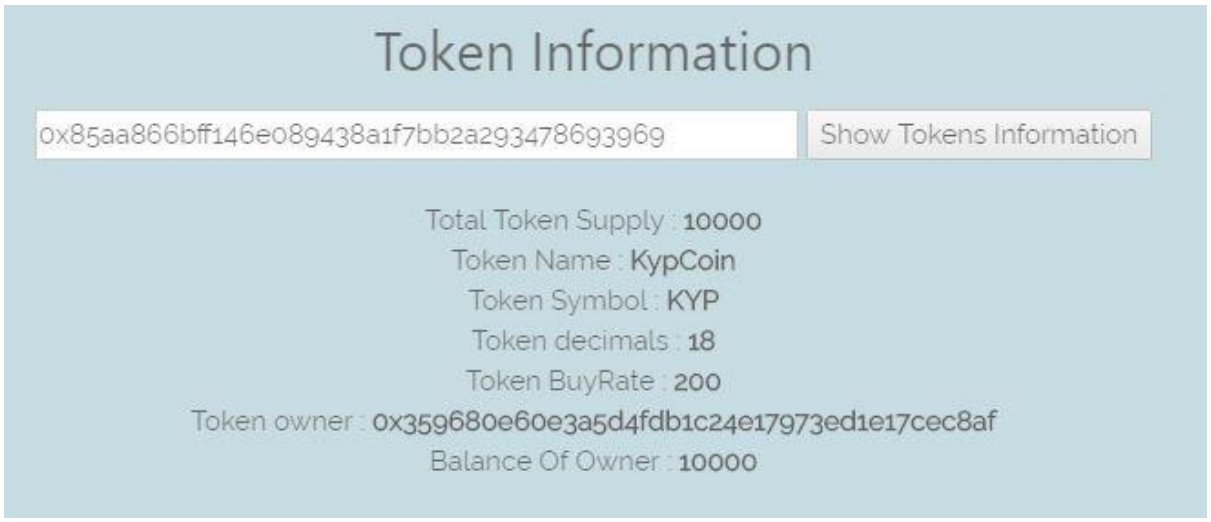
Στην πιο κάτω εικόνα παρατηρούμε το αποτέλεσμα αφού πατήσουμε το κουμπί Create Token, όπου δημιουργείται η διεύθυνση του Smart Contract και μια απόδειξη της συναλλαγής (Transaction Hash):


Παρατηρώντας και το δίκτυο Ethereum στην πιο κάτω εικόνα βλέπουμε τα δεδομένα που αφορούν το Smart Contract:

Αυτό που έχει προστεθεί σε αυτή τη συναλλαγή είναι η δημιουργία της διεύθυνσης του Smart Contract ( Contract Created: διεύθυνση του συμβολαίου):



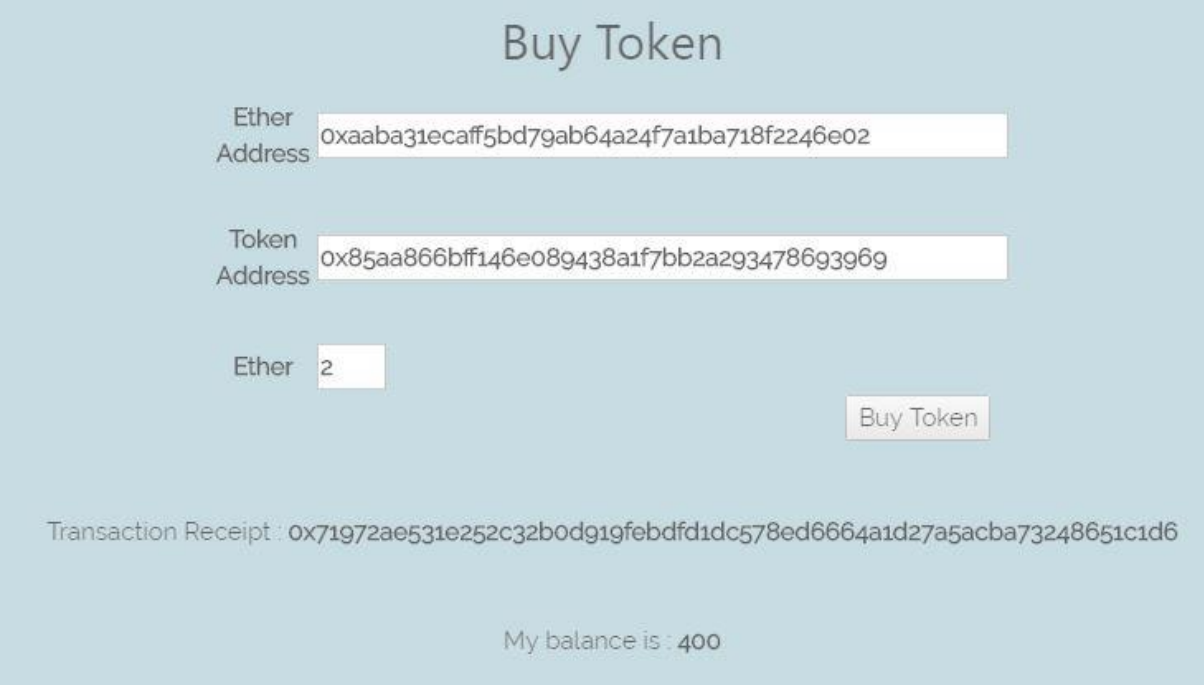
Έπειτα στην πιο κάτω εικόνα επικοινωνούμε με το ήδη δημιουργημένο Smart Contract και βλέπουμε τις πληροφορίες που μας επιστρέφει:



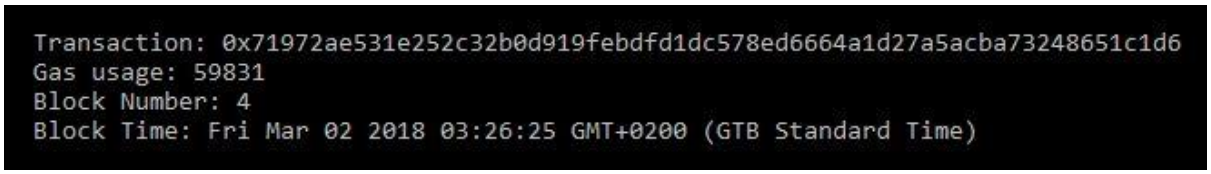

Εν συνεχεία χρησιμοποιώντας την διεύθυνση account[6]:


θα αγοράσω ένα ποσό KypCoin δίνοντας 2 Ether όπως φαίνεται και στην πιο κάτω εικόνα εισάγοντας την διεύθυνση μου και τη διεύθυνση του Smart Contract, καθώς και το ποσό σε ether :

Μόλις πατήσουμε το κουμπί Buy Token δημιουργείτε μια απόδειξη της συναλλαγής και παρουσιάζεται το Balance της διεύθυνσης μας. Η ισοτιμία είναι 1 ether=200 KypCoin άρα πληρώνοντας 2 ether θα αποκτήσω 400 KypCoin :

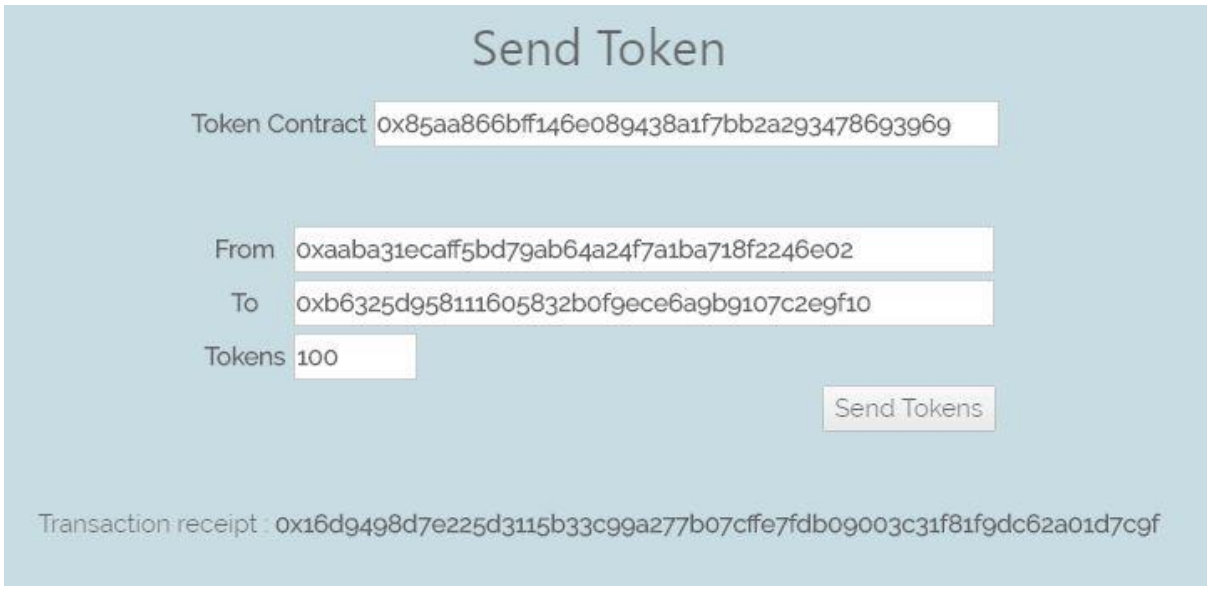


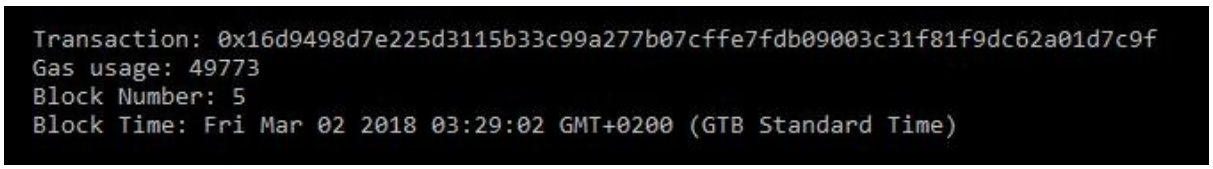

Επίσης παρατηρώντας την παρακάτω εικόνα, βλέπουμε το δίκτυο Ethereum και συγκεκριμένα το «Transaction» πιστοποιώντας ότι πράγματι έγινε η συναλλαγή:



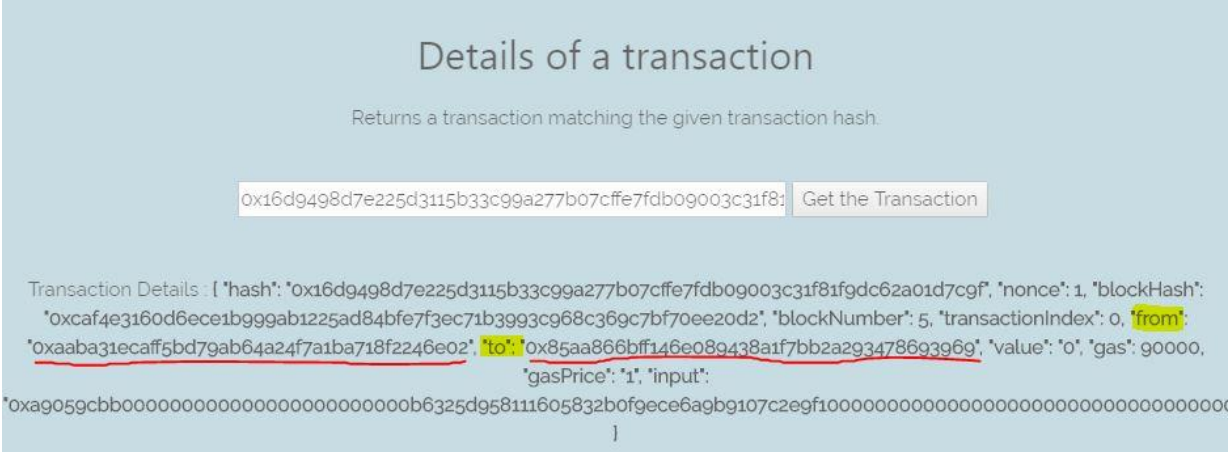
Στο επόμενο στάδιο μπορούμε να στείλουμε μερικά kypCoin σε ένα άλλο λογαριασμό όπως παρουσιάζεται στην πιο κάτω εικόνα:


Αμέσως μετά την αποστολή των 100 KypCoin δημιουργείται η απόδειξη συναλλαγής όπως βλέπουμε στις επόμενες 2 εικόνες:



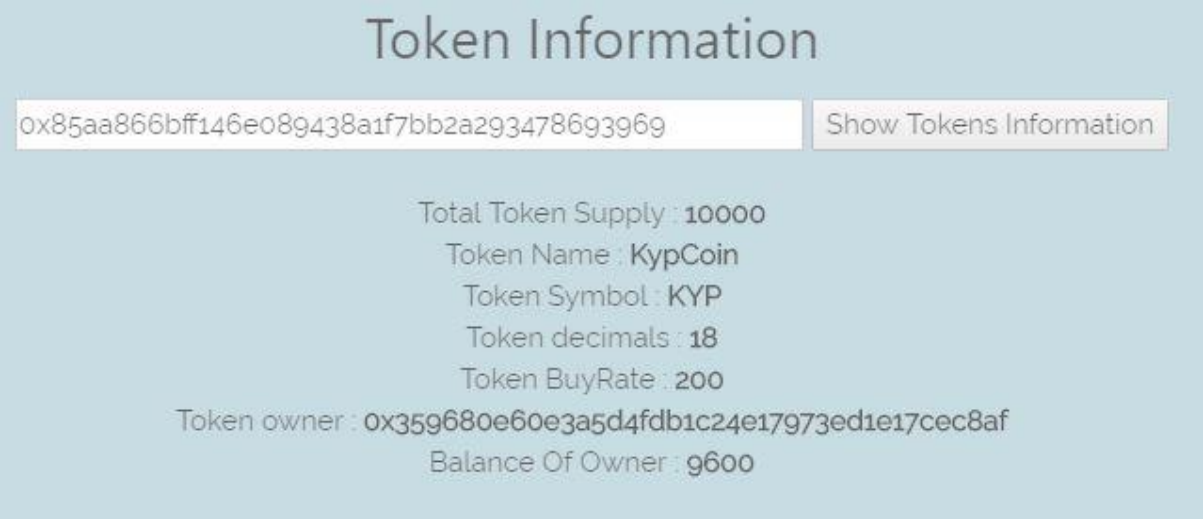



Εν συνεχεία μέσα από την ιστοσελίδα μπορούμε να εξάγουμε πληροφορίες από το Transaction (απόδειξη συναλλαγής) όπως ακριβώς φαίνεται στην πιο κάτω εικόνα:




Τέλος, παρατηρούμε ότι μετά την αγορά των 400 KypCoin ο λογαριασμός του ιδιοκτήτη του Smart Contract μειώθηκε από 10000 KypCoin σε 9600 KypCoin αλλά αυξήθηκε το ποσό του λογαριασμού Ethereum κατά 2 ether.

Στις επόμενες 2 εικόνες παρουσιάζονται αυτά τα αποτελέσματα:




# 8. Επίλογος

Η εκπόνηση της παρούσας διπλωματικής εργασίας είχε ως προαπαιτούμενο την έρευνα και ενδελεχή μελέτη του Bitcoin, του Ethereum και της συναρπαστικής τεχνολογίας που βρίσκεται πίσω από αυτά, η οποία δεν είναι άλλη από την τεχνολογία Blockchain. Η ιδέα του Bitcoin και του Ethereum υιοθετήθηκε από τον κόσμο και διατάραξε τα νερά της οικονομίας με αποτέλεσμα μεγάλες τράπεζες και κυβερνήσεις να πολεμούν αυτά τα κρυπτονομίσματα. Ανήμπορες όμως οι τράπεζες και κυβερνήσεις να πάψουν την λειτουργία των κρυπτονομισμάτων άρχισαν να υποστηρίζουν την τεχνολογία Blockchain φτιάχνοντας τα δικά τους κρυπτονομίσματα και τις δικές τους υπηρεσίες βασισμένα σε αυτά. Καθίσταται έτσι φανερή η σπουδαιότητα και σοβαρότητα της νέας αυτής τεχνολογίας.

Ταυτόχρονα, κατά τη διεξαγωγή της έρευνάς μου κατανόησα απόλυτα ότι το Bitcoin και το Ethereum αποτελούν ένα μικρό μόνο δείγμα των δυνατοτήτων της τεχνολογίας Blockhain. Συνδυάζοντας λοιπόν παλιές και καινούργιες τεχνολογίες δημιουργήθηκε το Blockchain, το οποίο αποτελεί το έμπιστο πρωτόκολλο του Internet που τόσα χρόνια απουσίαζε αλλά ήταν τόσο αναγκαίο. Θα μπορούσε να υποστηριχθεί ότι η δημιουργία της τεχνολογίας Blockchain είναι αντίστοιχης σπουδαιότητας με τη δημιουργία του Παγκόσμιου Ιστού (γνωστό με τα αρχικά www), τον οποίο δημιούργησε  ο Τιμ Μπέρνερς Λι στις 12 Νοεμβρίου του 1990. Το έμπιστο λοιπόν Blockchain μας δίνει την δυνατότητα να κοιτάξουμε το μέλλον και να δημιουργήσουμε τις επόμενες εφαρμογές οι οποίες θα βασίζονται σε αυτό, αλλάζοντας ριζικά τον τρόπο που λειτουργεί ο κόσμος, όπως ακριβώς είχε γίνει και με την δημιουργία του Internet.

## Βιβλιογραφία


Antonopoulos, A.M. (2015). *Mastering Bitcoin.* United States of America: O,Reilly Media Inc.

Antonopoulos, A.M. (2017). *Mastering Bitcoin (2nd Edition).* United States of America: O,Reilly Media Inc.

Brooklyn Microgrid. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://www.brooklyn.energy/

Ethereum Homestead. (2018, Φεβρουάριος 27). Ανακτήθηκε από http://ethdocs.org/en/latest/introduction/index.html

ethereumjs-testrpc. (2018, Φεβρουάριος 26). Ανακτήθηκε από https://www.npmjs.com/package/ethereumjs-testrpc

ethereum/remix-ide. (2018, Φεβρουάριος 26). Ανακτήθηκε από https://github.com/ethereum/remix-ide

Introducing Piclo. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://www.openutility.com/piclo/

Gupta, M. (2017). *Blockchain IBM Limited Edition.* United States of America: John Wiley & Sons, Inc.

Laurence, T. (2017). *Blockchain*. Canada: John Wiley & Sons, Inc.

Local renewable energy for businesses. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://piclo.uk/

Nathan Reiff. (2017). what is ERC-20 and what Does it Mean for Ethereum? Ανακτήθηκε Φεβρουάριος 24, 2018 από https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

Nakamoto, S. (2017). Bitcoin P2P e-cash paper. Ανακτήθηκε Οκτώβρη 16, 2017 από article.gmane.org/gmane.comp.encryption.general/12588/

oneup.company. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://www.oneup.company/pdf/oneup-what-we-do.pdf

Remix - Solidity IDE. (2018, Φεβρουάριος 27). Ανακτήθηκε από http://remix.readthedocs.io/en/latest/

Solar Change. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://solarchange.co/

SolarCoin. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://solarcoin.org/

Solidity. Ανακτήθηκε Φεβρουάριος 24, 2018 από https://en.wikipedia.org/wiki/Solidity

Swan, M. (2015). *Blockchain Blueprint for a new economy*. United States of America: O,Reilly Media, Inc.

Sonnen Batterie. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://www.sonnenbatterie.de

Tapscott, D. & Tapscott, A. (2016). *Blockchain Revolution*. Great Britain: Clays Ltd, St Ives plc

Vincenzo Morabito (2017). *Business Innovation Through Blockchain.* Cham, Switzerland Springer International Publishing AG.

Web3 JavaScript app API for 0.2x.x. (2018, Φεβρουάριος 27). Ανακτήθηκε από https://github.com/ethereum/wiki/wiki/JavaScript-API