ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΚΑΙ ΣΥΝΑΛΛΑΓΕΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΙΣΤΟΥ ΚΑΙ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ

Διπλωματική Εργασία

του

Μπούτσκα Εμμανουήλ

Θεσσαλονίκη, Φεβρουάριος 2021

ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΚΑΙ ΣΥΝΑΛΛΑΓΕΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΙΣΤΟΥ ΚΑΙ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ

Μπούτσκας Εμμανουήλ

Πτυχίο Εφαρμοσμένης Πληροφορικής, Πανεπιστήμιο Μακεδονίας, 2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Γεωργιάδης Χρήστος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

Γεωργιάδης Χρήστος	Στειακάκης Εμμανουήλ	Δασίλας Απόστολος
.....	.....	.....

Μπούτσκας Εμμανουήλ

.....

Περίληψη

Η τεχνολογία Blockchain είναι έτοιμη να αλλάξει ριζικά τον διαδικτυακό κόσμο. Αν και είναι εξαιρετικά πρόσφατη σαν τεχνολογία, λειτούργησε άψογα και βρήκε ένα ευρύ φάσμα εφαρμογών τόσο στον οικονομικό όσο και στον μη χρηματοοικονομικό κόσμο. Η θεμελιώδης αλλαγή που αντιπροσωπεύει η τεχνολογία Blockchain είναι η απομάκρυνση της προσπάθειας να υπάρχει μια κεντρική αξιόπιστη αρχή σε ένα μαζικά κατανεμημένο δίκτυο. Αντιθέτως, προσφέρει πολλαπλάσιες πηγές εμπιστοσύνης που πρέπει όλες να συμφωνήσουν, με βάση έναν αλγόριθμο που υποδεικνύει ότι οι συναλλαγές μπορούν να θεωρηθούν αξιόπιστες και έγκυρες. Οι περισσότερες Blockchain λύσεις προσφέρουν μια αμετάβλητη και διαρκή καταγραφή των συναλλαγών καθιστώντας δύσκολο για οποιαδήποτε αξιόπιστη ή μη αξιόπιστη πηγή να τις αλλάξει ή να τις τροποποιήσει. Αυτό παρουσιάζει ένα εντελώς νέο επίπεδο ασφάλειας, απορρήτου και εμπιστοσύνης στον διαδικτυακό κόσμο. Σε αυτή την διπλωματική, παρουσιάζεται μια συστηματική έρευνα που καλύπτει ζητήματα λειτουργικότητας, ασφάλειας, απορρήτου, καθώς και αρχιτεκτονικών προσεγγίσεων της τεχνολογίας Blockchain. Στο πρώτα κεφάλαια παρουσιάζεται μια επισκόπηση της τεχνολογίας Blockchain και των βασικών αρχών της ως προς τη λειτουργικότητα και την αλληλεπίδραση τους μέσα στο δίκτυο. Το επόμενο κεφάλαιο αφιερώνεται στις αποκεντρωμένες εφαρμογές και συγκεκριμένα σε λεπτομέρειες και παραδείγματα γύρω από την περιοχή των αποκεντρωμένων οργανισμών (DAO). Στη συνέχεια τα επόμενα κεφάλαια εστιάζουν στις συναλλαγές καλύπτοντας το κύκλο ζωής τους, την αρχιτεκτονική και τη δομή τους. Συγκρίνονται οι διαφορές ανάμεσα στις συναλλαγές σε εφαρμογές ιστού και κινητών συσκευών παρουσιάζοντας τα χαρακτηριστικά και τις εκτεταμένες δυνατότητες τους. Το επόμενο κεφάλαιο επικεντρώνεται στα έξυπνα συμβόλαια και στη δύναμη τους να επιτρέπουν σε πολλαπλές πηγές αξίας και κανόνες να ενσωματώνονται σε συναλλαγές απευθείας. Τέλος, παρουσιάζονται τα σχετικά αποτελέσματα της έρευνας.

Λέξεις κλειδιά: Blockchain, Συναλλαγές, Κινητές Συσκευές, Αποκεντρωμένες Εφαρμογές, Έξυπνα Συμβόλαια

Abstract

Blockchain technology is ready to radically change the online world. Although extremely premature as a technology, it has worked flawlessly and found a wide range of applications in both the financial and non-financial worlds. The fundamental change represented by Blockchain technology is the removal of the attempt to have a central reliable authority in a distributed network. Instead, it offers various sources of trust that all have to agree, based on a protocol that indicates that transactions can be considered credible and valid. This offers an entire modern level of security, protection and trust within the online world. In this thesis, a systematic research is presented that covers issues of functionality, security, privacy, as well as architectural approaches to Blockchain technology. The first chapters provide an overview of Blockchain technology and its basic principles in terms of functionality and their interactions within the network. The next chapter is devoted to decentralized applications and specifically to details and examples around the area of decentralized agencies (DAOs). The following chapters focus on transactions, covering their life cycle, architecture and structure. Compare the differences between transactions in web applications and mobile devices by presenting their features and extensive capabilities. The next chapter focuses on smart contracts and their capabilities to allow different rules of execution to be applied in transactions. Finally, the relevant results of the research are presented.

Keywords: Blockchain, Transactions, Mobile Devices, Decentralized Applications, Smart Contracts

Ευχαριστίες

Θα ήθελα καταρχάς να ευχαριστήσω τον επιβλέπον καθηγητή μου, κ. Γεωργιάδη Χρήστο, για την υποστήριξη και την πολύτιμη καθοδήγηση του στην εκπλήρωση της διπλωματικής μου εργασίας. Τα διορατικά του σχόλιά με ώθησαν να οξύνω τη σκέψη μου και έφεραν τη δουλειά μου σε υψηλότερο επίπεδο. Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένεια μου για τη συμπαράσταση και την εμψύχωση προς το πρόσωπο μου σε ολόκληρη τη διάρκεια των μεταπτυχιακών μου σπουδών.

ΠΕΡΙΕΧΟΜΕΝΑ

Κατάλογος Εικόνων

Κατάλογος Πινάκων

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Το Blockchain είναι μια αναδυόμενη ψηφιακή τεχνολογία που συνδυάζει τη κρυπτογραφία μαζί με μηχανισμούς διαχείρισης δεδομένων και δικτύωσης, για την εκτέλεση και καταγραφή συναλλαγών μεταξύ μερών. Ένα Blockchain είναι μια λίστα («αλυσίδα») ομάδων («μπλοκ») συναλλαγών [8]. Κάθε φορά που υλοποιείται μια συναλλαγή προστίθεται σε ένα σύνολο συναλλαγών που προορίζονται να καταγραφούν στο καθολικό. Οι κόμβοι του συστήματος λαμβάνουν μερικές από αυτές τις συναλλαγές, ελέγχουν την ακεραιότητα τους και τις καταγράφουν σε νέα μπλοκ στο καθολικό. Το περιεχόμενο του Blockchain αναπαράγεται σε πολλούς γεωγραφικά κατανεμημένους κόμβους. Αυτοί οι κόμβοι λειτουργούν από κοινού το σύστημα Blockchain, χωρίς το κεντρικό έλεγχο οποιουδήποτε μεμονωμένου αξιόπιστου τρίτου μέρους. Συναλλαγές μεταξύ συμβαλλομένων μερών όπως πληρωμές, χρηματικές εγγυήσεις, συμβολαιογραφικές πράξεις και ψηφοφορίες, αποτελούν καθημερινό φαινόμενο για τους περισσότερους ανθρώπους. Παραδοσιακά, αυτές οι συναλλαγές υποστηρίζονται από αξιόπιστα τρίτα μέρη όπως κυβερνητικές υπηρεσίες, τράπεζες, νομικές και λογιστικές εταιρείες. Το Blockchain παρέχει έναν διαφορετικό τρόπο για να υποστηρίζει αυτές τις συναλλαγές. Αντί να εμπιστευόμαστε τρίτα μέρη, εμπιστευόμαστε από κοινού τη συλλογική λειτουργεία του και την ορθότητα της κοινής τεχνολογικής πλατφόρμας του [8].

Αρχικά σχεδιάστηκε ως βάση των κρυπτονομισμάτων, ωστόσο οι πτυχές της τεχνολογίας Blockchain έχουν ευρεία εμβέλεια και δυναμική σε πολλούς άλλους τομείς. Για να κατανοηθεί αυτή η δυναμική, είναι σημαντικό να διασαφηνιστούν δύο βασικά στοιχεία του Blockchain: τεχνολογία κατανεμημένου καθολικού (DLT) και έξυπνες συμβάσεις (smart contracts). Ένα κατανεμημένο καθολικό είναι μια αποκεντρωμένη, κοινόχρηστη και συγχρονισμένη καταγραφή συναλλαγών μεταξύ συμβαλλόμενων μερών που εξασφαλίζεται με χρήση κρυπτογραφικών μεθόδων [7]. Σε αντίθεση με μια κατανεμημένη βάση δεδομένων, οι κόμβοι ενός κατανεμημένου καθολικού δεν εμπιστεύονται άλλους κόμβους και ούτω καθεξής και πρέπει να επαληθεύουν ανεξάρτητα τις συναλλαγές πριν τις προσθέσουν σε μπλοκ. Τα

κατανεμημένα καθολικά χωρίζονται σε δύο ευρείες τάξεις: εκείνα που επιδιώκουν να ελαχιστοποιήσουν το ρόλο των αξιόπιστων και αναγνωρίσιμων τρίτων μερών (public Blockchains), και εκείνων που βασίζονται ρητά σε αναγνωρίσιμα τρίτα μέρη για κάποιο υποσύνολο του συστήματος (private/hybrid Blockchains). Δεν είναι όλα τα κατανεμημένα καθολικά Blockchains, αλλά όλα τα Blockchains είναι κατανεμημένα καθολικά [7].

Από την άλλη πλευρά, οι συναλλαγές που είναι αποθηκευμένες σε ένα Blockchain μπορεί να είναι κάτι παραπάνω από απλές εγγραφές ανταλλαγής περιουσιακών στοιχείων. Αρκετά συστήματα Blockchain επιτρέπουν επίσης προγράμματα υπολογιστών να αποθηκεύονται και να εκτελούνται ως μέρος των συναλλαγών στο καθολικό [31]. Αυτά τα προγράμματα ονομάζονται έξυπνα συμβόλαια. Το Blockchain του Bitcoin επιτρέπει μόνο πολύ απλές μορφές έξυπνων συμβάσεων, ωστόσο άλλα Blockchain όπως αυτό του Ethereum επιτρέπουν την εγγραφή πολύπλοκων και σύνθετων προγραμμάτων γενικού σκοπού. Ως αποτέλεσμα, τα Blockchains μπορεί να είναι περισσότεροο από μια απλή κατανεμημένη βάση δεδομένων, μπορεί να είναι γενικές υπολογιστικές πλατφόρμες, αν και επί του παρόντος με σοβαρούς πρακτικούς περιορισμούς στην υπολογιστική πολυπλοκότητα. Αυτή η ικανότητα επεκτείνει σημαντικά τη δύναμη των συστημάτων Blockchain και αυξάνει το εύρος χρήσης και τις δυνατότητες καινοτομίας που μπορούν να προσφέρουν. Αν και τα έξυπνα συμβόλαια δεν χρησιμοποιούνται πάντα για νομικές συμβάσεις, μερικές φορές μπορούν να χρησιμοποιηθούν για αυτοματοποίηση ή παρακολούθηση της εκτέλεσης βημάτων των νομικών συμβάσεων [47]. Τα έξυπνα συμβόλαια μπορούν επίσης να ορίσουν ένα πρωτόκολλο αλληλεπίδρασης μεταξύ διαφορετικών μερών, όπως σε μια συνεργατική επιχειρηματική διαδικασία μεταξύ εταιρειών.

Αναφορικά με τη δομή της διπλωματικής εργασίας, σε αυτό το κεφάλαιο παρουσιάσθηκε μια εισαγωγή του τι είναι και γιατί υπάρχει τόσο μεγάλο ενδιαφέρον γύρω από την τεχνολογία Blockchain. Για μεγαλύτερη σαφήνεια ορίστηκαν τα σημαντικότερα συστατικά στοιχεία που χρησιμοποιεί η τεχνολογία και ο ρόλος τους.

Στο δεύτερο κεφάλαιο ακολουθεί μια εκτενής αναφορά σε υψηλό επίπεδο των πιο σημαντικών πτυχών της τεχνολογίας Blockchain. Εξετάζονται οι τύποι Blockchain, οι μηχανισμοί συναίνεσης, η αρχιτεκτονική, κατανάλωση ενέργειας και οι κίνδυνοι επιθέσεων.

Στο τρίτο κεφάλαιο, παρουσιάστηκαν οι βασικοί τύποι αποκεντρωμένων εφαρμογών και μία σύγκριση μεταξύ αυτών και των εφαρμογών ιστού. Στη συνέχεια ακολούθησε παρουσίαση των δημοφιλέστερων Blockchain εφαρμογών με ιδιαίτερη έμφαση στο εγχείρημα των κοινωνικών δικτύων να εφαρμόσουν την τεχνολογία Blockchain στις δραστηριότητες τους.

Στο τέταρτο κεφάλαιο εξετάστηκε λεπτομερώς το κομμάτι των συναλλαγών και των επιμέρους συστατικών τους. Συγκεκριμένα, εξετάστηκε ο κύκλο ζωής των συναλλαγών, η δομή τους, ο ρόλος των δέντρων merkle καθώς και η ύπαρξη μικροσυναλλαγών στο δίκτυο Blockchain.

Στο πέμπτο κεφάλαιο αναλύεται ο τρόπος λειτουργίας των πορτοφολιών κρυπτονομισμάτων. Παρουσιάστηκαν οι διαθέσιμοι τύποι, οι στόχοι ασφάλειας, οι ευπάθειες και μια ταξινόμηση αυτών με βάση τον τρόπο σύνδεσης στο δίκτυο. Στη συνέχεια υλοποιήθηκαν τρεις συναλλαγές για κάθε ένα τύπο πορτοφολιού ξεχωριστά.

Στο έκτο κεφάλαιο περιγράφεται ο τρόπος λειτουργίας των έξυπνων συμβολαίων. Εξετάζεται η εφαρμογή τους, τα πλεονεκτήματα έναντι των παραδοσιακών συμβολαίων, τα νομικά ζητήματα και οι περιορισμοί. Στη συνέχεια παρουσιάζεται η υλοποίηση μιας συναλλαγής για απομακρυσμένη αγορά με χρήση έξυπνου συμβολαίου.

Τέλος, στο έβδομο κεφάλαιο διατυπώνονται τα συμπεράσματα γύρω από την υιοθέτηση της τεχνολογίας Blockchain σε περιβάλλοντα ιστού και κινητών εφαρμογών, και ακολουθούν οι βιβλιογραφικές πηγές που χρησιμοποιήθηκαν για τη παρούσα διπλωματική.

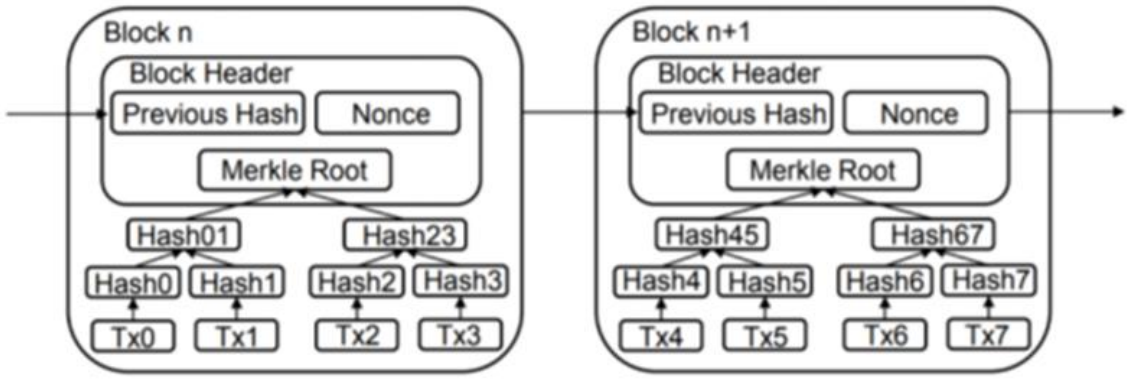
ΚΕΦΑΛΑΙΟ 2

Τεχνολογία Blockchain

Η τεχνολογία Blockchain είναι ένας τρόπος καταγραφής πληροφοριών σε πολλές συσκευές, ταυτόχρονα, μέσω του διαδικτύου. Ένα Blockchain είναι ένα τεράστιο αρχείο καταγραφής συναλλαγών που αναπαράγεται σε ένα σύνολο συμμετεχόντων κόμβων. Ουσιαστικά, μπορεί να θεωρηθεί ως ένα υπολογιστικό φύλλο που αντιγράφεται χιλιάδες φορές σε ένα παγκόσμιο δίκτυο υπολογιστών [8]. Αυτό το υπολογιστικό φύλλο ενημερώνεται τακτικά, έτσι ώστε νέες συναλλαγές να μπορούν να γίνουν μέρος του. Η αποκεντρωμένη φύση του Blockchain είναι συνέπεια του γεγονότος ότι το σύστημα αποτελείται από ένα παγκόσμιο δίκτυο peer-to-peer που αποτελείται από υπολογιστές, γνωστοί ως κόμβοι., με αποτέλεσμα πολλές τοποθεσίες να αποθηκεύουν τις ίδιες πληροφορίες. Αυτό διασφαλίζει ότι οι πληροφορίες είναι εύκολα επαληθεύσιμες και δημόσιες [8]. Το όνομα Blockchain στην πραγματικότητα προέρχεται από τον τρόπο αποθήκευσης των δεδομένων, διότι τα μπλοκ που διατηρούν πληροφορίες είναι πλήρως συνδεδεμένα με αλυσίδες.

Όταν πρόκειται να επισυναφθεί μια νέα συναλλαγή στο Blockchain, οι συμμετέχοντες κόμβοι ψηφίζουν εάν συμμορφώνεται με τους κανόνες του Blockchain και καταλήγουν σε συμφωνία σχετικά με την αποδοχή της ή όχι. Αυτή η συμφωνία είναι γνωστή ως συναίνεση και το πρωτόκολλο που την διασφαλίζει ονομάζεται πρωτόκολλο ασυναίνεσης, κάθε Blockchain χρησιμοποιεί δικό του πρωτόκολλο [20]. Αυτοί οι κόμβοι πρέπει να επαληθεύσουν τη νομιμότητα της συναλλαγής. Όλοι οι κόμβοι εκτελούν τις ίδιες δραστηριότητες και αποθηκεύουν ένα αντίγραφο του καθολικού. Μόλις επιτευχθεί συναίνεση μεταξύ των κόμβων, η συναλλαγή γίνεται μέρος ενός μπλοκ δεδομένων που περιέχει άλλες συναλλαγές. Αν το μπλοκ είναι πλήρες, ανταγωνίζεται με άλλα μπλοκ για να γίνει το επόμενο μπλοκ που θα προστεθεί στο υπάρχον Blockchain. Οποιοσδήποτε μπορεί να επαληθεύσει την εγκυρότητα των καταγεγραμμένων συναλλαγών, ενώ κανείς δεν μπορεί να παραβιάσει ή να διαγράψει προηγούμενες συναλλαγές.

Αυτό που κάνει το Blockchain μια ανατρεπτική τεχνολογία είναι ότι προσφέρει, για πρώτη φορά, μια ανθεκτική σε παραβίαση βάση δεδομένων όπου η εμπιστοσύνη προκύπτει μέσω της συνεργασίας ενός συνόλου υπολογιστών, αντί μέσω ενός ιδρύματος ή οργανισμού που επιβάλλει εμπιστοσύνη από τον εξωτερικό κόσμο πάνω στο σύστημα [20].



Εικόνα 1.1: Ένα κατανεμημένο σύστημα αποθήκευσης αποτελούμενο από block τα οποία είναι συνδεδεμένα μεταξύ τους με μία προσέγγιση προς τα πίσω.

Στα Blockchains, οι εγγραφές δεδομένων, δηλαδή οι συναλλαγές, ομαδοποιούνται σε ομάδες. Το πρώτο μπλοκ, γνωστό ως το μπλοκ γένεσης (genesis block), είναι ένα ειδικό μπλοκ που είναι γνωστό σε όλους [20]. Κάθε μπλοκ συνδέεται με το προηγούμενο μπλοκ του ενσωματώνοντας ένα κρυπτογραφικό κατακερματισμό του περιεχομένου του προηγούμενου μπλοκ, δημιουργώντας έτσι μια αλυσίδα από μπλοκ. Τα Blockchains ουσιαστικά αποτελούν κατανεμημένα καθολικά, γι' αυτό και η τεχνολογία Blockchain συχνά αναφέρεται ως Τεχνολογία Κατανεμημένων Καθολικών (Distributed Ledger Technology – DLT). Το καθολικό κοινοποιείται δημόσια σε όλους του συμμετέχοντες του δικτύου. Η αποθήκευση αποτελείται από πολλαπλά κομμάτια (blocks) δεδομένων συνδεδεμένα μεταξύ τους, όπως θα γινόταν από μία φυσική αλυσίδα. Όλες οι συναλλαγές που είναι αποθηκευμένες στο Blockchain θεωρούνται αμετάβλητες και έγκυρες [19].

Σκοπός του Blockchain

Αρχικός σκοπός του συστήματος Blockchain ήταν η υποστήριξη του ηλεκτρονικού συστήματος συναλλαγών που βασίζεται πάνω σε κρυπτογραφικά τεκμήρια αντί για πειστήρια εμπιστοσύνης. Ενώ το εύρος χρήσης της τεχνολογίας αυτής αυξήθηκε, οι πρωταρχικοί στόχοι παραμένουν σταθεροί. Ο πρώτος από αυτούς είναι η διαβεβαίωση της ανωνυμίας των χρηστών. Αυτό επιτεύχθηκε με την χρήση δημόσιου/ιδιωτικού ζεύγους κλειδιών, με έναν νέο τρόπο που δεν μπορούν να ξανά δημιουργηθούν, μέσω της τεχνολογίας του Blockchain [19]. Κάθε συμμετέχον ταυτοποιείται από το δημόσιο κλειδί και η επιβεβαίωση επιτυγχάνεται με την εισαγωγή του ιδιωτικού του κλειδιού. Ο δεύτερος πρωταρχικός στόχος είναι η παροχή μια δημόσιας καταγραφής του συνόλου των συναλλαγών οι οποίες δεν μπορούν να τροποποιηθούν μετά την επιβεβαίωση και συμφωνία τους. Η χρήση αυτής της καταγραφής αρχικά σχεδιάστηκε για να αποτρέπει τους χρήστες ηλεκτρονικών συναλλαγών από τις λανθασμένες διπλό συναλλαγές και να επιτρέπει δημόσιο έλεγχο όλων αυτών των συναλλαγών. Τρίτος και τελευταίος στόχος είναι η ανεξαρτησία από οποιαδήποτε κεντρική ή έμπιστη εξουσία. Αυτό οδηγεί στη δημιουργία ενός συστήματος στο οποίο καμία οντότητα δεν έχει περισσότερη ή λιγότερη εξουσία, ή αξιοπιστία από κάποια άλλη [19].

Δίκτυο και Κόμβοι

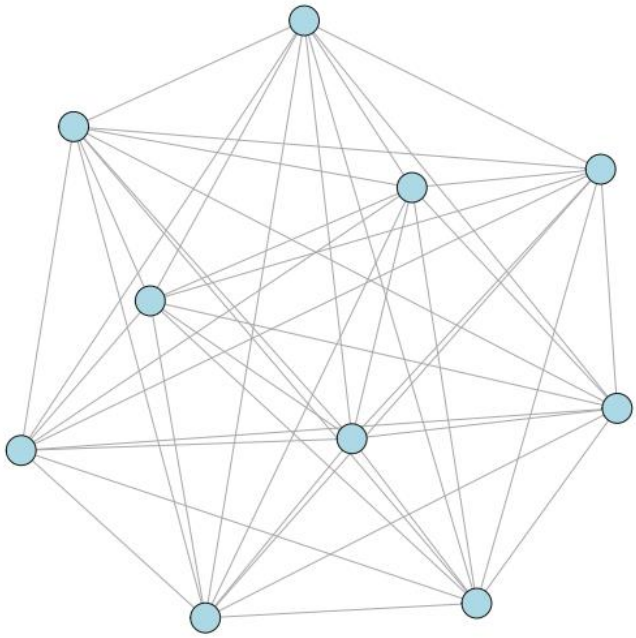
Το Blockchain λειτουργεί peer-to-peer, δεν υπάρχει καμία κεντρική αρχή εντός του δίκτυο. Οι πληροφορίες καταγράφονται συνεχώς και ανταλλάσσονται μεταξύ όλων των συμμετεχόντων. Οι χρήστες του δικτύου είναι η ραχοκοκαλιά ολόκληρου του συστήματος, και ανταλλάσσουν ένα μέρος των υπολογιστικών πόρων τους για να διατηρήσουν το δίκτυο σε λειτουργία. Σε ορισμένες περιπτώσεις οι συμμετέχοντες έχουν την ευκαιρία να εισπράξουν αμοιβές συναλλαγών (transaction fees) ή ανταμοιβές σε αντάλλαγμα την υπολογιστική ισχύ τους. Οι κόμβοι μπορούν να έχουν διαφορετικούς ρόλους στο δίκτυο. Οι πλήρεις κόμβοι ή οι ανθρακωρύχοι είναι μόνιμα συνδεδεμένοι και αποθηκεύουν ολόκληρο το Blockchain ενώ επαληθεύουν και διαδίδουν τις δραστηριότητες και τα μπλοκ στο δίκτυο [55]. Οι απλοί κόμβοι επαλήθευσης πληρωμής (SPV), από την άλλη πλευρά, δεν αποθηκεύουν ολόκληρο το Blockchain. Επομένως, βασίζονται σε πλήρεις κόμβους για τη λήψη και τη διάδοση

συναλλαγών σε όλο το δίκτυο. Οι κόμβοι SPV κατεβάζουν βασικά τις συναλλαγές που είναι σημαντικές για αυτούς [6].

Όλοι οι κόμβοι θεωρούνται ίσοι αν και μερικοί έχουν διαφορετικά καθήκοντα. Οι βασικές εργασίες ενός κόμβου είναι:

1. Να ελέγχουν την εγκυρότητα των συναλλαγών και να τις προσθέτουν σε υπάρχοντα μπλοκ ή απλά να τις απορρίπτουν.
2. Να αποθηκεύουν μπλοκ συναλλαγών.
3. Να μεταδίδουν το ιστορικό συναλλαγών σε άλλους κόμβους για να εξασφαλίσουν τον συγχρονισμό.

Ένας χρήστης που ενδιαφέρεται για πλήρη αυτονομία και εξουσία είναι προτιμότερο να εκτελεί έναν πλήρη κόμβο. Οι κόμβοι σχηματίζουν μεταξύ τους ένα τυχαίο γράφημα καθώς κάθε κόμβος συνδέεται σε άλλους τυχαίους κόμβους [11], όπως φαίνεται στη παρακάτω εικόνα. Όλοι οι κόμβοι διασυνδέονται μεταξύ τους για να επαληθεύσουν και να λάβουν τις συναλλαγές.



Εικόνα 1.2: Κατανεμημένο καθολικό

Οι κόμβοι μπορούν να εισέρχονται και να εξέρχονται στο. Ένας ενεργός (online) κόμβος που βγαίνει εκτός σύνδεσης, όταν επιστρέψει πρέπει να επανέλθει σε ταχύτητα.

Ο κόμβος θα πρέπει να κατεβάσει όλα τα μπλοκ που προστέθηκαν στο Blockchain όσο αυτός ήταν εκτός σύνδεσης. Θεωρητικά, ένας μόνο κόμβος μπορεί να διατηρήσει το Blockchain ζωντανό, ωστόσο, το δίκτυο θα ήταν τότε πολύ ευάλωτο στη διαφθορά. Μια νέα συναλλαγή διαδίδεται μέσω του δικτύου μετακινούμενη μεταξύ των συνδέσεων όλων των κόμβων. Κάθε κόμβος συνδέεται με όλους τους κόμβους στο δίκτυο χρησιμοποιώντας τους γείτονες του. Μόλις ένας κόμβος λάβει μια συναλλαγή, ελέγχει την εγκυρότητα του αποστολέα και αν τα χρήματα δεν έχουν ξοδευτεί ακόμη. Στη συνέχεια, στέλνει τις πληροφορίες στους υπόλοιπους κόμβους έως ότου όλο το δίκτυο γνωρίζει για τη συναλλαγή.

Βασικά χαρακτηριστικά του Blockchain

Τεχνικά, το Blockchain είναι μια αποκεντρωμένη και ασφαλής βάση δεδομένων συναλλαγών, που βασίζεται σε αποκεντρωμένους κόμβους. Το Blockchain χαρακτηρίζεται από αποκέντρωση, ανθεκτικότητα, ανωνυμία και δυνατότητα ελέγχου. [1][13]

Αποκέντρωση: Στον πραγματικό κόσμο, υπάρχουν δύο τύποι συναλλαγών: η κεντρική συναλλαγή και η αποκεντρωμένη συναλλαγή. Οι κεντρικές συναλλαγές είναι αυτές που ελέγχονται από τη μία κεντρική αρχή. Σε συμβατικά κεντρικά συστήματα συναλλαγών, κάθε συναλλαγή πρέπει να επικυρωθεί μέσω της κεντρικής αξιόπιστης εταιρείας (π.χ. της κεντρικής τράπεζας). Ο χρήστης πραγματοποιεί μια πληρωμή μέσω της πύλης πληρωμής της τράπεζας και στη συνέχεια η τράπεζα επεξεργάζεται το αίτημα και στέλνει την απάντηση για αυτό το αίτημα που είναι είτε αποτυχία είτε επιτυχία.

Από την άλλη πλευρά, στις αποκεντρωμένες συναλλαγές, η συναλλαγή δεν ελέγχεται ή εξουσιοδοτείται από μία αρχή, αλλά από όλα τα ομότιμα (peers) μέλη που είναι διαθέσιμα στο δίκτυο εκείνη τη στιγμή. Έτσι, σε αυτόν τον τύπο συναλλαγής, ο χρήστης στέλνει το αίτημα με τη μορφή μπλοκ. Στη συνέχεια, το μπλοκ μεταδίδεται σε κάθε μέρος του δικτύου το οποίο στη συνέχεια εγκρίνει τη συναλλαγή και μόνο τότε τα χρήματα μεταφέρονται στον λογαριασμό που πρέπει.

Characteristics	Centralised	Decentralised
Control	Central	Distributed
Design	Easy	Difficult
Maintenance	Easy	Difficult
Failures	Single point	No single point
Stability	Low	High
Vulnerable	Yes	No
Unethical Operation	Possible	Not possible
Scalability	Low	High

Εικόνα 1.3: Χαρακτηριστικά συγκεντρωτικού και αποκεντρωτικού συστήματος

Με αυτόν τον τρόπο, το Blockchain μπορεί να μειώσει σημαντικά το κόστος του διακομιστή, συμπεριλαμβανομένου του κόστους ανάπτυξης και του κόστους λειτουργίας, και να μειώσει την συμφόρηση που υπάρχει στον κεντρικό διακομιστή βελτιώνοντας την απόδοση του. Το καλύτερο παράδειγμα μιας αποκεντρωμένης συναλλαγής στον σημερινό κόσμο είναι οι συναλλαγές μέσω του δικτύου Bitcoin ή Ethereum. Όλες αυτές οι συναλλαγές πραγματοποιούνται με τη βοήθεια του Blockchain όπου οι ομότιμοι στο δίκτυο εξορύσσουν το μπλοκ με αποτέλεσμα την αποκεντρωμένη συναλλαγή.

Ανθεκτικότητα: Είναι σχεδόν αδύνατο να διαγραφούν ή να επαναφερθούν συναλλαγές μόλις συμπεριληφθούν στο Blockchain. Δεδομένου, ότι κάθε μία από τις συναλλαγές που διαδίδονται στο δίκτυο πρέπει να είναι επιβεβαιωμένες και καταγεγραμμένες σε μπλοκ, που διανέμονται σε ολόκληρο το δίκτυο, είναι σχεδόν αδύνατο να αλλοιωθούν. Μπορούν να εντοπιστούν αμέσως τα μπλοκ που περιέχουν μη έγκυρες συναλλαγές. Αυτό το όφελος κάνει την τεχνολογία Blockchain αναλλοίωτη και άφθαρτη. Οι χρήστες του Blockchain έχουν εξουσίες ελέγχου σε όλες τις συναλλαγές και πληροφορίες. Εάν το Blockchain αποτελείται από μικρό αριθμός υπολογιστών, η τεχνολογία είναι πιο εκτεθειμένη σε επιθέσεις ωστόσο εάν υπάρχουν πολλοί υπολογιστές το σύστημα γίνεται ασφαλέστερο και πιο διαφανές.

Ανωνυμία: Στο πλαίσιο των Blockchain, η ανωνυμία σημαίνει την ικανότητα των μερών να ανταλλάσσουν δεδομένα χωρίς να αποκαλύπτουν πληροφορίες ταυτότητας εκτός αλυσίδας. Κάθε χρήστης μπορεί να αλληλεπιδράσει με το Blockchain μέσω μιας δημιουργημένης διεύθυνσης, η οποία δεν αποκαλύπτει την πραγματική ταυτότητα του χρήστη. Ένα απλό παράδειγμα θα μπορούσε να είναι το Bitcoin, το οποίο είναι εν μέρει ανώνυμο, κάθε διεύθυνση δεν είναι τίποτα περισσότερο από το κατακερματισμό (hash) του δημόσιου κλειδιού του χρήστη, αλλά δεν είναι καθόλου ιδιωτική καθώς όλες οι συναλλαγές που πραγματοποιούνται από και προς αυτήν τη διεύθυνση είναι γνωστές. Αυτός ο μηχανισμός διατηρεί ένα συγκεκριμένο απόρρητο στις συναλλαγές που περιλαμβάνονται στο Blockchain.

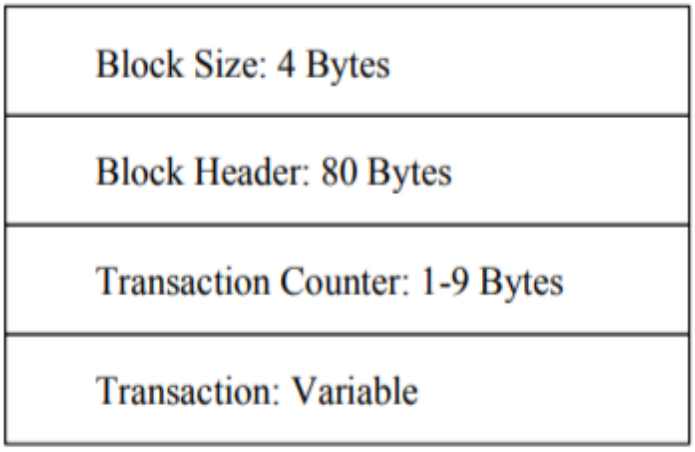
Δυνατότητα Ελέγχου: Δεδομένου ότι κάθε μία από τις συναλλαγές στο Blockchain επικυρώνεται και έχει καταγραφεί με χρονική σήμανση, οι χρήστες μπορούν εύκολα να επαληθεύσουν και να εντοπίσουν τις προηγούμενες εγγραφές μέσω της πρόσβασης σε οποιονδήποτε κόμβο στο κατανεμημένο δίκτυο. Επομένως, οι συναλλαγές μπορούν εύκολα να επαληθευτούν και να εντοπιστούν. Αυτός ο μηχανισμός βελτιώνει την ιχνηλασιμότητα και διαφάνεια των δεδομένων που είναι αποθηκευμένα στο Blockchain.

Συστατικά μέρη του Blockchain

Όπως υποδηλώνει το όνομά του, ένα Blockchain είναι μια ακολουθία από μπλοκ. Κάθε μπλοκ περιέχει ένα αριθμό συναλλαγών, καθώς και ένα κρυπτογραφημένο κατακερματισμό του προηγούμενου μπλοκ, το οποίο συνδέει δύο μπλοκ και σχηματίζει αποτελεσματικά μια αλυσίδα [19]. Ένα block αναγνωρίζεται από μία τιμή hash που παράγεται από την χρήση της συνάρτησης κατακερματισμού SHA256.

Η τιμή hash αποθηκεύεται στην επικεφαλίδα (header) του block. Το πεδίο της επικεφαλίδας (header) περιέχει την τιμή hash του προηγούμενου block ή του μητρικού block (parent block). Η ακολουθία της σύνδεσης των block με το προηγούμενο block δημιουργεί μία αλυσίδα που οδηγεί στο πρώτο block, γνωστό και ως genesis block. Μία επικεφαλίδα ενός block έχει σταθερό μέγεθός 80 bytes, ενώ το μέγεθος του πεδίου συναλλαγών δεν είναι σταθερό καθώς εξαρτάται από τον τύπο της εφαρμογής [19].

Εκτενέστερη ανάλυση των πεδίων που διέπουν ένα μπλοκ ακολουθεί στο κεφάλαιο των συναλλαγών



Εικόνα 1.4: Τα πεδία που αποτελούν ένα block

Η ενσωμάτωση της τεχνολογίας Blockchain αποτελείται από τρία κύρια συστατικά μέρη. Πρώτο και κυριότερο είναι το βιβλίο καταγραφών (ledger), το οποίο περιέχει τις δημόσιες εγγραφές των συναλλαγών και την σειρά με την οποία πραγματοποιήθηκαν. Δεύτερο συστατικό στοιχείο είναι το πρωτόκολλο γενικής συναίνεσης (consensus protocol), το οποίο επιτρέπει σε όλα τα μέλη της κοινότητας να συμφωνούν με τα δεδομένα που καταχωρούνται στο βιβλίο καταγραφών. Τέλος, υπάρχει το ψηφιακό συνάλλαγμα που δρα ως αμοιβή για αυτούς που είναι πρόθυμοι να κάνουν την εργασία προώθησης και εξέλιξης που χρειάζεται το βιβλίο καταγραφών. Η συνεργασία όλων των παραπάνω παρέχουν ένα σύστημα με ιδιότητες σταθερότητας και διαμοιραζόμενης εμπιστοσύνης που είναι και στόχος του συστήματος αυτού [19].

Καθολικό (Ledger)

Η τεχνολογία κατανεμημένου καθολικού (DLT) είναι ένα ψηφιακό σύστημα καταγραφής συναλλαγών κατά το οποίο οι συναλλαγές και τα στοιχεία τους καταγράφονται ταυτόχρονα σε πολλά μέρη. Σε αντίθεση με τις παραδοσιακές βάσεις δεδομένων, τα κατανεμημένα καθολικά δεν έχουν κεντρική λειτουργικότητα αποθήκευσης δεδομένων ή διαχείρισης.

Ένα κατανεμημένο καθολικό μπορεί να χρησιμοποιηθεί για την καταγραφή στατικών δεδομένων, όπως ένα μητρώο, και δυναμικών δεδομένων, δηλαδή συναλλαγών. Το καθολικό είναι μια ακολουθία μπλοκ, όπου κάθε μπλοκ είναι μια ταξινομημένη ακολουθία συναλλαγών ενός συμφωνημένου μεγέθους (αν και το πραγματικό μέγεθος διαφέρει από σύστημα σε σύστημα). Η πρώτη καταχώρηση σε ένα μπλοκ είναι ένα κρυπτογραφικός κατακερματισμός (όπως αυτά που παράγονται από τον αλγόριθμο SHA-256) του προηγούμενου μπλοκ. Η ύπαρξη αυτού του κατακερματισμού αποτρέπει την απόπειρα αλλαγών του περιεχομένου του προηγούμενου μπλοκ, καθώς οποιαδήποτε τέτοια αλλαγή θα αλλάξει το κρυπτογραφικό κατακερματισμό αυτού του μπλοκ και έτσι μπορεί να εντοπιστεί από την κοινότητα. Αυτοί οι κατακερματισμοί είναι εύκολο να υπολογιστούν αλλά αδύνατο να αντιστραφούν. Έτσι, μόλις δημοσιευτεί ο κατακερματισμός των περιεχομένων ενός μπλοκ, οποιοσδήποτε στην κοινότητα μπορεί εύκολα να ελέγξει ότι ο κατακερματισμός είναι σωστός. Αυτή η αρχιτεκτονική υπολογιστών αντιπροσωπεύει μια σημαντική επανάσταση στην τήρηση αρχείων αλλάζοντας τον τρόπο συλλογής και επικοινωνίας των πληροφοριών.

Πρωτόκολλο γενικής συναίνεσης (Consensus Protocol)

Το πρωτόκολλο γενικής συναίνεσης (consensus protocol) βρίσκεται ανάμεσα στις πιο μελετημένες διαστάσεις των κατανεμημένων συστημάτων. Στη τεχνολογία του Blockchain δεν υπάρχει κάποιος υπεύθυνος για τη διαχείριση, καθώς είναι ένα σύστημα χτισμένο πάνω στην εμπιστοσύνη [21]. Οι βασικές αρχές για τη λειτουργία των δικτύων Blockchain, είναι να έχουν κάποιο είδος συναίνεσης μεταξύ των συμμετεχόντων. Κατά την έναρξη της διάδοσης δεδομένων από τους κόμβους μέσω ενός δικτύου Blockchain, οι κόμβοι δεν έχουν κεντρικό μέρος που θα είναι υπεύθυνο για τη ρύθμιση και επίλυση διαφορών ή για προστασία από εισβολές. Επομένως, υπάρχει ανάγκη για έναν μηχανισμό που θα παρακολουθεί την κυκλοφορία των κεφαλαίων που μεταδίδονται μέσω των συναλλαγών και θα εγγυάται την αδιαμφισβήτητη ανταλλαγή τους αποτρέποντας περιπτώσεις απάτης, όπως επιθέσεις διπλών δαπανών. Μια συναίνεση γίνεται σε ένα δίκτυο peer to peer για να συμφωνηθεί η κατάσταση του δικτύου. Όλοι οι κόμβοι πρέπει να συναινέσουν σε ένα κοινό πρωτόκολλο ενημέρωσης περιεχομένου έτσι ώστε το καθολικό να διατηρεί μια συνεπή κατάσταση. Τα μπλοκ δεν πρέπει να γίνονται απλώς δεκτά ως μέρος του Blockchain

χωρίς τη συγκατάθεση της πλειοψηφίας. Αυτό ονομάζεται μηχανισμός συναίνεσης και αντιπροσωπεύει τον τρόπο με τον οποίο δημιουργούνται μπλοκ και προστίθενται στο υπάρχον καθολικό. Υπάρχουν διάφοροι μηχανισμοί συναίνεσης. Ωστόσο, οι πιο συνηθισμένοι μηχανισμοί συναίνεσης Blockchain είναι οι αλγόριθμοι Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA) και το πρακτικό Βυζαντινό σφάλμα ανοχής (PBFT) [4]. Η βασική διαφορά μεταξύ των διαφόρων μηχανισμών συναίνεσης είναι στον τρόπο με τον οποίο εκχωρούν και επιβραβεύουν την επαλήθευση των συναλλαγών [3].

Ψηφιακό νόμισμα (Digital Currency)

Κάθε νόμισμα αντιπροσωπεύει ένα αυθαίρετο χρηματικό ποσό. Ένα νόμισμα που δημιουργείται μέσω μιας συναλλαγής, είναι αμετάβλητο για ολόκληρη τη διάρκεια ζωής και μπορεί να ξοδευτεί μόνο μία φορά [21]. Ο λόγος για τον οποίο ένας ανθρακωρύχος (miner) πραγματοποιεί όλη αυτή την υπολογιστική εργασία για τον υπολογισμό του hash και του nonce ενός block είναι το μερίδιο που θα λάβει ως ανταμοιβή από ένα ψηφιακό νόμισμα. Αυτό ενθαρρύνει τους miners να αποδεχτούν ένα block όσο το δυνατόν πιο γρήγορα, έτσι ώστε να ξεκινήσουν να εργάζονται πάνω στο hash του επόμενου block.

Στη περίπτωση του Bitcoin, για την εξόρυξη (δηλαδή την δημιουργία) ενός μπλοκ που περιέχει πολλές συναλλαγές, ένας κόμβος πρέπει να λύσει ένα πρόβλημα που ονομάζεται Proof-of-Work (PoW). Η δυσκολία επίλυσης του PoW προσαρμόζεται αυτόματα κάθε δύο εβδομάδες, έτσι ώστε ένα μπλοκ να δημιουργείται κατά μέσο όρο κάθε 10 λεπτά [21]. Το Bitcoin ήταν το αρχικό νόμισμα του Blockchain και η ανταμοιβή για κάθε hashing που γινόταν σε κάποιο block ήταν 12 Bitcoins με τιμή περίπου τα $4.500. Αυτή η ανταμοιβή μειώνεται κατά το ήμισυ κάθε 210.000 blocks. Η τελευταία μείωση προήλθε στις 25 Μαΐου 2020, με την τιμή της ανταμοιβής να γίνεται 6,25 Bitcoin για κάθε block [21]. Μια συναλλαγή θεωρείται ως έγκυρη εάν όλες οι εισροές της υπάρχουν ως έξοδοι προηγούμενων συναλλαγών στο Blockchain και δεν έχουν ξοδευτεί ακόμη. Εμπλουτίζοντας αυτήν τη διαδικασία επαλήθευσης, οι κόμβοι παρακολουθούν τα μη εξαντλημένα νομίσματα σε μια τοπική δομή δεδομένων γνωστή ως μη δαπανημένα δεδομένα εξόδου (UTxO). Εκτενέστερη ανάλυση των αδαπάνητων δεδομένων εξόδου ακολουθεί στο κεφάλαιο των συναλλαγών.

Βασικές Έννοιες στο Blockchain

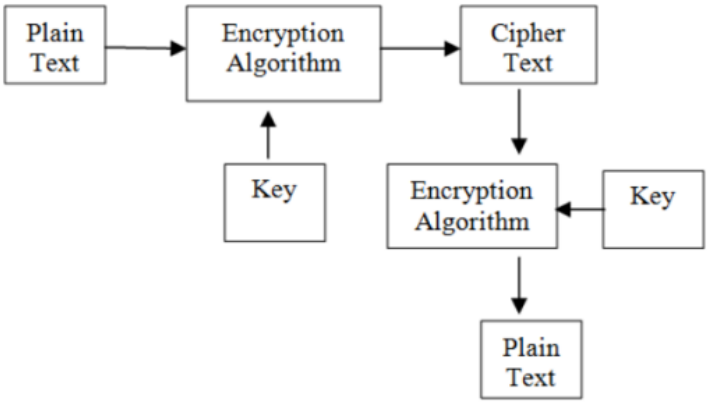
Το δίκτυο Blockchain λειτουργεί σύμφωνα με ορισμένες βασικές έννοιες που πρέπει να κατανοηθούν πλήρως προκειμένου να καταλάβουμε σε βάθος πως λειτουργούν. Αυτές οι έννοιες είναι:

Ασύμμετρη Κρυπτογραφία

Το δίκτυο Blockchain διασφαλίζει τη λειτουργία της αλυσίδας χρησιμοποιώντας κρυπτογράφηση ασύμμετρου κλειδιού. Η εκτέλεση οποιασδήποτε συναλλαγής απαιτεί από τους συμμετέχοντες να έχουν ψηφιακό πορτοφόλι το οποίο είναι ασφαλισμένο με το ιδιωτικό κλειδί τους. Η κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιείται για την υπογραφή συναλλαγών Bitcoin ή άλλων συναλλαγών Blockchain. Το Bitcoin χρησιμοποιεί ασύμμετρη κρυπτογράφηση για να βεβαιωθεί ότι μόνο ο ιδιοκτήτης ενός πορτοφολιού χρημάτων μπορεί να κάνει ανάληψη ή να μεταφέρει χρήματα σε αυτό.

Στην κρυπτογράφηση ασύμμετρου κλειδιού χρησιμοποιείται ζεύγος κλειδιών (key pair) για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Κάθε χρήστης παράγει το δικό του ζεύγος κλειδιών, δηλαδή τα κλειδιά δημόσιας κρυπτογράφησης (δημόσια διεύθυνση πορτοφολιού) και ιδιωτικής αποκρυπτογράφησης τα οποία είναι διαφορετικά μεταξύ τους [67]. Έπειτα, γνωστοποιεί σε όλους τους χρήστες το δημόσιο κλειδί κρυπτογράφησης προκειμένου να μπορούν να του αποστείλουν κρυπτογραφημένα μηνύματα. Οποιοσδήποτε κατέχει το δημόσιο κλειδί κρυπτογράφησης μπορεί να στείλει μηνύματα, αλλά μόνο ο κάτοχος του ιδιωτικού κλειδιού μπορεί να τα αποκωδικοποιήσει. Οι ποιο διαδεδομένοι αλγόριθμοι για ασύμμετρα κρυπτοσυστήματα είναι οι εξής:

- Αλγόριθμος RSA
- Αλγόριθμος Elliptic-Curve Cryptography (ECC).
- Αλγόριθμος των Diffie-Hellman
- Αλγόριθμος Digital Signature Standard (DSS)

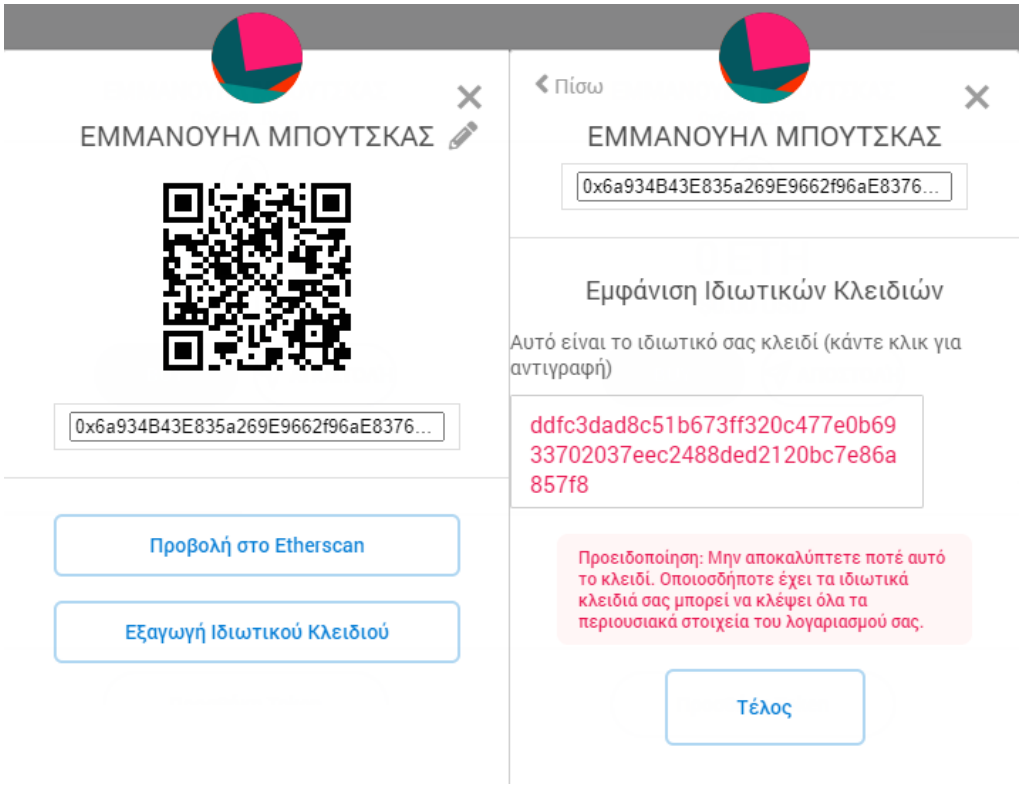


Εικόνα 1.5: Κρυπτογράφηση Ασύμμετρου Κλειδιού

Ο συνδυασμός και των δύο κλειδιών δημιουργεί μια ψηφιακή υπογραφή. Αυτή η ψηφιακή υπογραφή αποδεικνύει την ιδιοκτησία των κρυπτονομισμάτων και επιτρέπει τον έλεγχο τους μέσω ενός πορτοφολιού.

Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές αποδεικνύουν την κυριότητα των κρυπτονομισμάτων κάποιου χρήστη και επιτρέπουν σε αυτόν να ελέγχει τα χρήματα του. Συνδέοντας μια ψηφιακή υπογραφή σε μια συναλλαγή, κανείς δεν μπορεί να αμφισβητήσει ότι αυτή η συναλλαγή δεν είναι γνήσια και είναι προϊόν πλαστογραφίας. Το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή συναλλαγών, ενώ το δημόσιο κλειδί στη συνέχεια χρησιμοποιείται για την επαλήθευση της υπογραφής από τους υπολογιστές επικύρωσης. Όταν ένας χρήστης δημιουργήσει για πρώτη φορά ένα πορτοφόλι, δημιουργείται ένα ζεύγος κλειδιών που αποτελείται από ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί [67].



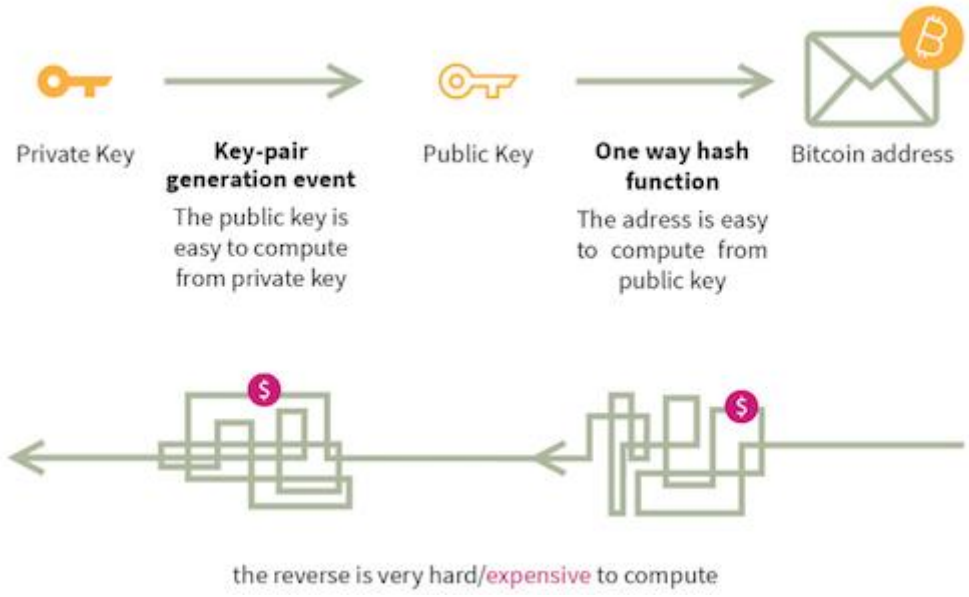
Εικόνα 1.6: Δημόσιο κλειδί σε web wallet

Εικόνα 1.7: Ιδιωτικό κλειδί σε web wallet

Εικόνα 1.8: Ψηφιακή Υπογραφή [67]

Σε ένα πρώτο βήμα, το ιδιωτικό κλειδί είναι ένας ακέραιος μήκους 128-256-bit που δημιουργείται τυχαία. Το δημόσιο κλειδί προκύπτει μαθηματικά, χρησιμοποιώντας κρυπτογράφηση ελλειπτικού κλειδιού, από το ιδιωτικό κλειδί. Αυτή η μαθηματική συνάρτηση λειτουργεί μονόδρομα, πράγμα που σημαίνει ότι είναι εύκολο να παραχθεί

ένα δημόσιο κλειδί από ένα ιδιωτικό κλειδί, αλλά η χρήση αντίστροφων μαθηματικών μηχανισμών για την εξαγωγή του ιδιωτικού κλειδιού από το δημόσιο κλειδί είναι πρακτικά αδύνατη [67].



Εικόνα 1.9: Δημιουργία κλειδιών και διευθύνσεων [67]

Σε ένα δεύτερο βήμα, η διεύθυνση Blockchain προέρχεται από το δημόσιο κλειδί, χρησιμοποιώντας έναν διαφορετικό τύπο κρυπτογραφικής συνάρτησης από αυτήν που χρησιμοποιήθηκε για την εξαγωγή του δημόσιου κλειδιού, προσθέτοντας μεταδεδομένα όπως αθροίσματα ελέγχου και προθέματα. Η χρήση διαφορετικού τύπου κρυπτογραφικής συνάρτησης για την εξαγωγή της διεύθυνσης προσθέτει ένα επιπλέον επίπεδο ασφάλειας καθώς αν το πρώτο επίπεδο ασφάλειας (κρυπτογράφηση ελλειπτικού κλειδιού) έχει σπάσει, τότε κάποιος που έχει το δημόσιο κλειδί θα μπορούσε ίσως να σπάσει το ιδιωτικό κλειδί. Βέβαια, κάτι τέτοιο θα μπορούσε να γίνει πραγματικότητα μόνο στην περίπτωση ύπαρξης κβαντικών υπολογιστών καθώς τότε η κρυπτογραφία ελλειπτικού κλειδιού θα ήταν ιδιαίτερα ευάλωτη στο να σπάσει. Αυτό σημαίνει ότι εάν κάποιος έχει τη διεύθυνση Blockchain και έχει σπάσει την κρυπτογράφηση ελλειπτικού κλειδιού, αυτό το άτομο θα πρέπει ακόμη να περάσει από το δεύτερο επίπεδο ασφάλειας, το οποίο χρησιμοποιήθηκε για την εξαγωγή της διεύθυνσης από το δημόσιο κλειδί. Ως αποτέλεσμα αυτού, η διεύθυνση λειτουργεί ως ψηφιακό δακτυλικό αποτύπωμα του δημόσιου κλειδιού [67].

Συναλλαγή

Η συναλλαγή σε ένα δίκτυο Blockchain θα μπορούσε να οριστεί ως μια μικρή μονάδα εργασίας αποθηκευμένη σε δημόσια αρχεία. Η εκτέλεση και η αποθήκευση αυτών των εγγραφών στο Blockchain απαιτούν προηγούμενη έγκριση από τους περισσότερους συμμετέχοντες που συμμετέχουν στο δίκτυο. Οποιαδήποτε προηγούμενη συναλλαγή μπορεί να υποβληθεί σε έλεγχο ανά πάσα στιγμή. Ωστόσο, δεν μπορεί να ενημερωθεί. Οι συναλλαγές που δημιουργούνται από κόμβους και συγκεντρώνονται σε μπλοκ αντιπροσωπεύουν την τρέχουσα κατάσταση του Blockchain [2].

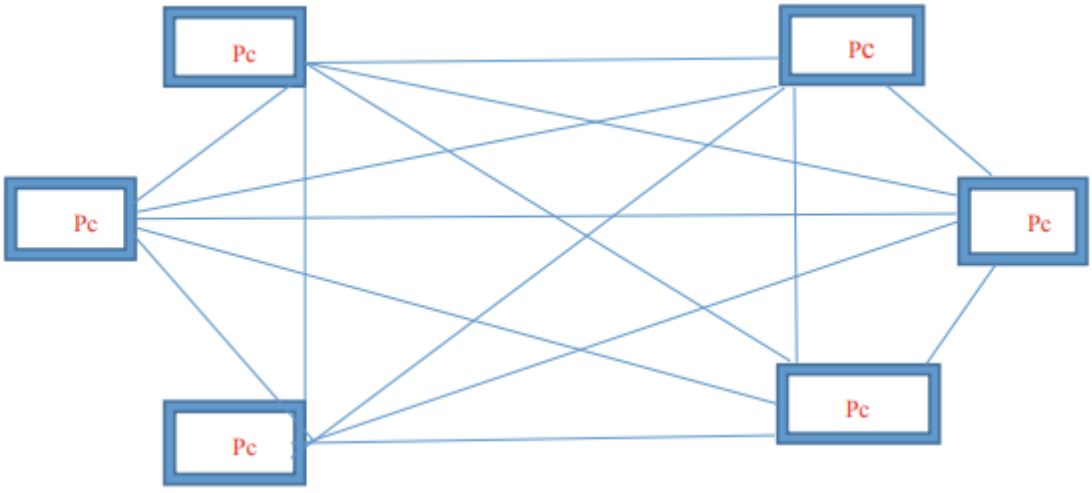
Κατακερματισμός

Οι κρυπτογραφικές λειτουργίες κατακερματισμού δημιουργούν μια συμβολοσειρά χαρακτήρων σταθερού μήκους από εγγραφές δεδομένων οποιουδήποτε μήκους. Μια εγγραφή δεδομένων μπορεί να είναι μια λέξη, μια πρόταση, ένα μεγάλο κείμενο ή ένα ολόκληρο αρχείο. Στο πλαίσιο των κρυπτονομισμάτων όπως το Bitcoin, οι συναλλαγές λαμβάνονται ως είσοδοι και εκτελούνται μέσω ενός αλγορίθμου κατακερματισμού (το Bitcoin χρησιμοποιεί τον αλγόριθμο SHA-256) που δίνει έξοδο σταθερού μήκους. Ο κατακερματισμός μιας συναλλαγής διευκολύνει τον εντοπισμό συναλλαγών στο Blockchain. Στο Blockchain, κάθε μπλοκ δεδομένων περιέχει την τιμή κατακερματισμού του προηγούμενου μπλοκ έτσι ώστε να μπορεί να επαληθευτεί η ακεραιότητα όλων των προηγούμενων δεδομένων, καθώς και να διατηρηθεί αναλλοίωτη η καταγραφή των συναλλαγών [12].

Τοπολογίες Blockchain

Μια βασική παράμετρος που λαμβάνεται υπόψη στο σχεδιασμό μιας πλατφόρμας Blockchain είναι η κατηγοριοποίηση των κόμβων που αποτελούν μέρος της. Η κύρια κατηγοριοποίηση των συστημάτων Blockchain διακρίνεται σε δημόσια (public), ιδιωτική (private), με κοινοπραξία (consortium), και υβριδική (hybrid).

***Public Blockchain*:** Δημόσια συστήματα Blockchain όπως το Bitcoin και το Ethereum επιτρέπουν σε οποιονδήποτε κόμβο να συμμετέχει στη διαδικασία συναίνεσης και οποιοσδήποτε κόμβος μπορεί να δημιουργήσει το επόμενο έγκυρο μπλοκ. Επομένως, εάν όλοι οι κόμβοι έχουν τους ίδιους πόρους, τότε κάθε κόμβος έχει την ίδια πιθανότητα της δημιουργίας ενός μπλοκ [4]. Τα δημόσια Blockchain λειτουργούν χωρίς κεντρικές αρχές και μεσάζοντες. Ένα από τα πρώτα δημόσια Blockchain που κυκλοφόρησαν στο κοινό ήταν το Bitcoin public Blockchain. Επέτρεψε σε οποιονδήποτε συνδεδεμένο στο διαδίκτυο να κάνει συναλλαγές με αποκεντρωμένο τρόπο. Η επαλήθευση των συναλλαγών γίνεται μέσω μεθόδων συναίνεσης όπως Proof-of-Work (PoW), Proof-of-Stake (PoS) και ούτω καθεξής. Στους πυρήνες, οι συμμετέχοντες κόμβοι αναλαμβάνουν την επικύρωση των συναλλαγών για να λειτουργήσει το κοινό Blockchain. Το μεγαλύτερο πλεονέκτημα αυτού του είδους Blockchain είναι ότι δεν μπορεί κανένας να ελέγξει το δίκτυο πλήρως.. Ως εκ τούτου, διασφαλίζει ότι τα δεδομένα είναι ασφαλή και βοηθά στο αμετάβλητο των εγγραφών. Τα Bitcoin, Ethereum και Litecoin είναι μερικά από τα παραδείγματα του Public Blockchain που χρησιμοποιούνται σε πραγματικά σενάρια.



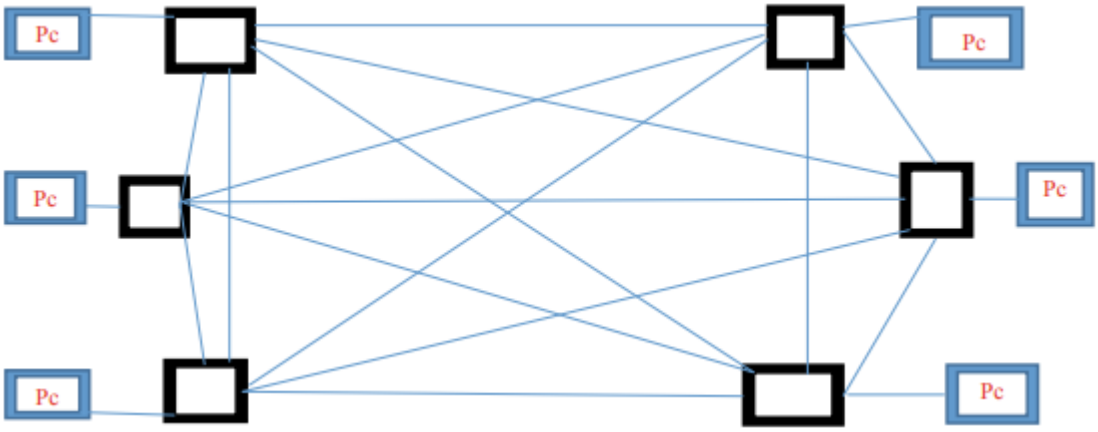
Εικόνα 1.10: Public Blockchain

Από την άλλη πλευρά, ένα από τα μειονεκτήματα τους είναι ότι υποφέρουν από έλλειψη ταχύτητας στις συναλλαγές [63]. Μπορεί να χρειαστούν μερικά λεπτά έως ώρες πριν ολοκληρωθεί μια συναλλαγή. Για παράδειγμα, το Bitcoin μπορεί να διαχειρίζεται μόνο επτά συναλλαγές ανά δευτερόλεπτο σε σύγκριση με 24.000 συναλλαγές ανά δευτερόλεπτο που πραγματοποιούνται από τη VISA [63].

Αυτό συμβαίνει επειδή χρειάζεται αρκετός χρόνος για την επίλυση των μαθηματικών προβλημάτων και στη συνέχεια της ολοκλήρωσης της συναλλαγής. Ένα άλλο πρόβλημα με το δημόσιο Blockchain είναι η επεκτασιμότητα. Όσο περισσότεροι κόμβοι υπάρχουν, τόσο πιο αδέξιο και αργό γίνεται το δίκτυο [63]. Έχουν ληφθεί μέτρα για την επίλυση αυτού του προβλήματος. Το Bitcoin για παράδειγμα υλοποιεί τις συναλλαγές εκτός αλυσίδας (off-chain transactions) για να κάνει το κύριο δίκτυο Bitcoin πιο γρήγορο και πιο επεκτάσιμο [65]. Το τελευταίο μειονέκτημα ενός δημόσιου Blockchain είναι η επιλογή της μεθόδου συναίνεσης. Το Bitcoin, χρησιμοποιεί το Proof-of-Work (PoW), το οποίο καταναλώνει πολλή ενέργεια γεγονός που έχει προκαλέσει περιβαλλοντικές ανησυχίες. Συγκεκριμένα, το Blockchain του Bitcoin καταναλώνει τόση ηλεκτρική ενέργεια όσο η Ιρλανδία, ή έως και το 5% της παγκόσμιας κατανάλωσης ενέργειας που χρησιμοποιείται για την κατασκευή αλουμινίου [64]. Ωστόσο, αυτό έχει επιλυθεί εν μέρει χρησιμοποιώντας πιο αποτελεσματικούς αλγόριθμους όπως το Proof-of-Stake (PoS).

Private Blockchain: Ένα ιδιωτικό σύστημα Blockchain μπορεί να οριστεί καλύτερα ως το Blockchain που λειτουργεί σε περιοριστικό περιβάλλον, δηλαδή κλειστό δίκτυο, και βρίσκονται υπό τον έλεγχο μιας οντότητας. Ανήκουν στο άλλο άκρο του φάσματος, καθώς επιτρέπουν μόνο μερικοί κόμβοι να είναι μέρος της διαδικασίας συναίνεσης, και μόνο ένα υποσύνολο αυτών των κόμβων μπορεί να δημιουργήσει το επόμενο μπλοκ. Τα ιδιωτικά Blockchain συνήθως έχουν έναν διαχειριστή δικτύου που μπορεί να ορίζει τα δικαιώματα χρήστη και παραμέτρους του δικτύου, όπως προσβασιμότητα, εξουσιοδότηση και ούτω καθεξής [4]. Αυτά τα συστήματα θα μπορούσαν να χρησιμοποιηθούν μεταξύ τραπεζών για να σχηματίσουν ένα κατανεμημένο δίκτυο και να συναλλάσσονται μεταξύ τους. Αυτό προσφέρει το πλεονέκτημα μιας πιο απρόσκοπτης εμπορικής εμπειρίας, καθώς οι τράπεζες έχουν διαφορετικές τεχνολογίες οι οποίες πρέπει να επικοινωνούν μεταξύ τους για να πραγματοποιηθεί μια συναλλαγή με επιτυχία. Επιπλέον, τα ιδιωτικά Blockchain διατηρούν το απόρρητο των συμμετεχόντων και των δραστηριοτήτων τους, και έτσι, είναι η φυσική επιλογή για ιδρύματα που εκτιμούν την ιδιωτικότητα και την αποθήκευση ευαίσθητων πληροφοριών. Η κύρια διαφορά τους με τα δημόσια Blockchain εμφανίζεται στον τρόπο πρόσβασης και στην ταχύτητα. Τα ιδιωτικά Blockchain είναι γρηγορότερα. Αυτό συμβαίνει επειδή υπάρχουν λιγότεροι συμμετέχοντες σε σύγκριση με τα δημόσια

Blockchain [62]. Εν ολίγοις, απαιτείται λιγότερος χρόνος για το δίκτυο να επιτύχει συναίνεση με αποτέλεσμα γρηγορότερες συναλλαγές. Ταυτόχρονα, ιδιαίτερο πλεονέκτημα αποτελεί η επεκτασιμότητα τους. Η επεκτασιμότητα είναι δυνατή επειδή, σε ένα ιδιωτικό Blockchain, μόνο μερικοί κόμβοι έχουν εξουσιοδότηση για την επικύρωση των συναλλαγών [62]. Αυτό σημαίνει ότι δεν έχει σημασία αν το δίκτυο μεγαλώνει, το ιδιωτικό Blockchain θα λειτουργεί με την προηγούμενη ταχύτητα και αποτελεσματικότητά του. Το κλειδί εδώ είναι η κεντρική πτυχή της λήψης αποφάσεων. Πέραν αυτού, προσφέρουν το ίδιο σύνολο δυνατοτήτων με αυτό του δημόσιου Blockchain, παρέχοντας διαφάνεια, εμπιστοσύνη και ασφάλεια στους επιλεγμένους συμμετέχοντες.



Εικόνα 1.11: Private Blockchain [17]

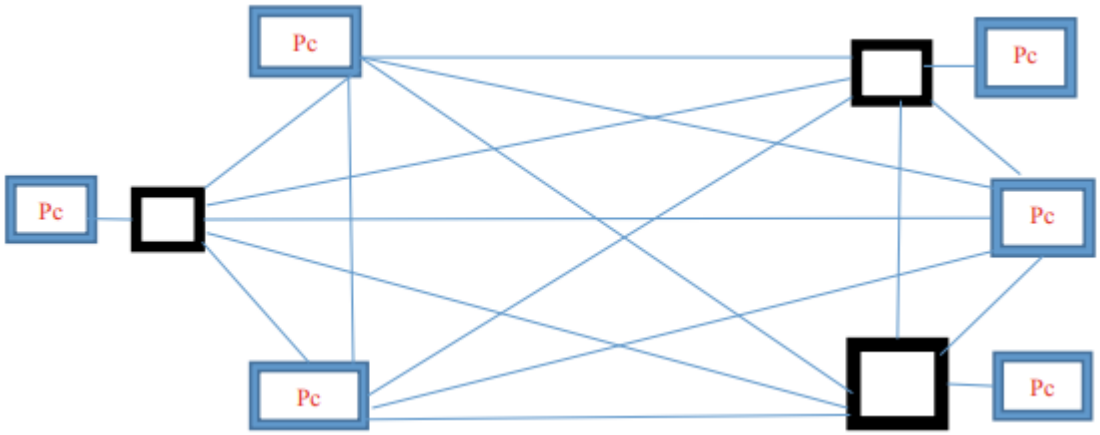
Ωστόσο, τα ιδιωτικά Blockchain δεν είναι πραγματικά αποκεντρωμένα [62]. Αυτό είναι ένα από τα μεγαλύτερα μειονεκτήματα τους και έρχεται σε αντίθεση με τη βασική φιλοσοφία της τεχνολογίας του κατανεμημένου καθολικού ή του Blockchain γενικά. Σε αντίθεση με τα Public Blockchain, τα οποία δεν απαιτούν από τους χρήστες να εμπιστεύονται κανέναν, δεδομένου ότι το δίκτυο είναι ανοιχτό στο κοινό, η ακεραιότητα του ιδιωτικού δικτύου Blockchain εξαρτάται από την αξιοπιστία των εξουσιοδοτημένων κόμβων, καθώς είναι απαραίτητη η εμπιστοσύνη στους κατόχους τους που υποτίθεται ότι επαληθεύουν και επικυρώνουν οι ίδιοι τις συναλλαγές. Ως αποτέλεσμα, η εγκυρότητα των εγγράφων δεν μπορεί να επαληθευτεί ανεξάρτητα. Τέλος, καθώς υπάρχουν μόνο μερικοί κόμβοι εδώ, η ασφάλεια δεν είναι τόσο καλή [62].

Είναι σημαντικό να κατανοηθεί ότι μπορεί να χαθεί η ασφάλεια εάν κάποιος κόμβος θέσει σε κίνδυνο τη μέθοδο συναίνεσης που χρησιμοποιείται από το ιδιωτικό δίκτυο. Με λιγότερους κόμβους, είναι πολύ πιο εύκολο για έναν επιτιθέμενο να πάρει τον έλεγχο του δικτύου και να χειριστεί τα δεδομένα σε αυτό.

Consortium Blockchain: Είναι ένας ημι-αποκεντρωμένος τύπος Blockchain όπου ένα δίκτυο Blockchain διαχειρίζεται από περισσότερους από έναν οργανισμούς. Είναι εν μέρει δημόσιο και εν μέρει ιδιωτικό και ως εκ τούτου ένας συνδυασμός τόσο δημόσιου όσο και ιδιωτικού Blockchain [17]. Ο διαχωρισμός μεταξύ δημόσιου και ιδιωτικού χαρακτήρα συμβαίνει βάσει της συναίνεσης. Σε μια κοινοπραξία Blockchain, μόνο λίγοι κόμβοι ή χρήστες έχουν το δικαίωμα να εξουσιοδοτούν συναλλαγές και να επιβλέπουν τη διαδικασία συναίνεσης. Τις περισσότερες φορές, οι κοινοπραξίες Blockchain συνδέονται με επιχειρηματική χρήση, όπου μια ομάδα οργανισμών συνεργάζεται για να αξιοποιήσει την τεχνολογία Blockchain για τη βελτίωση των επιχειρήσεων της. Ωστόσο, αυτός ο τύπος Blockchain μπορεί να επιτρέψει σε ορισμένους συμμετέχοντες να έχουν πρόσβαση ή να υιοθετήσουν μια υβριδική μέθοδο πρόσβασης. Για παράδειγμα, πηγές κατακερματισμού των μπλοκ και η διεπαφή προγράμματος εφαρμογής (API) ενδέχεται να είναι ανοιχτά στο κοινό [66]. Επομένως, οι εξωτερικές οντότητες μπορούν να χρησιμοποιήσουν το API για να κάνουν έναν συγκεκριμένο αριθμό ερευνών και να λάβουν ορισμένες πληροφορίες που σχετίζονται με την κατάσταση του Blockchain. Μερικά από τα τυπικά παραδείγματα κοινοπραξιών Blockchain είναι το Korum, το Corda, Energy Web Foundation και το Hyperledger.

Hybrid Blockchain: Τα υβριδικά συστήματα Blockchain βρίσκονται στην μέση μεταξύ των δύο προαναφερθέντων. Το υβριδικό Blockchain διακρίνεται από το γεγονός ότι δεν είναι ανοιχτό σε όλους, αλλά ταυτόχρονα προσφέρει χαρακτηριστικά Blockchain όπως ακεραιότητα, διαφάνεια και ασφάλεια [4]. Λειτουργεί σε κλειστό οικοσύστημα χωρίς να χρειάζεται να δημοσιοποιούνται τα πάντα, βέβαια οι κανόνες μπορούν να αλλάξουν ανάλογα με τις ανάγκες.

Αυτά τα συστήματα επιτρέπουν σε οποιονδήποτε κόμβο να αποτελεί μέρος στη διαδικασία της συναίνεσης, αλλά μόνο καθορισμένοι κόμβοι επιτρέπεται να σχηματίσουν το επόμενο μπλοκ.



Εικόνα 1.12: Hybrid Blockchain

Ως συνήθως, το υβριδικό Blockchain είναι εντελώς προσαρμόσιμο. Τα μέλη του υβριδικού Blockchain μπορούν να αποφασίσουν ποιος μπορεί να συμμετάσχει στο Blockchain ή ποιες συναλλαγές δημοσιοποιούνται. Μόλις ένας χρήστης λάβει την άδεια για πρόσβαση στο υβριδικό Blockchain, μπορεί να συμμετάσχει πλήρως στις δραστηριότητες του ίδιου του Blockchain [17]. Όπως να μοιράζεται ίσα δικαιώματα για να πραγματοποιεί συναλλαγές, να τις βλέπει ή ακόμα και να προσαρτά ή να τροποποιεί συναλλαγές. Ωστόσο, η ταυτότητα των χρηστών διατηρείται μυστική από τους άλλους συμμετέχοντες. Αυτό γίνεται για την προστασία του απορρήτου του χρήστη. Ουσιαστικά, το κύριο χαρακτηριστικό του υβριδικού μοντέλου είναι ότι προσφέρει ιδιωτικό απόρρητο ενώ εξακολουθεί να συνδέεται με δημόσιο δίκτυο. Το κρυπτονόμισμα Ripple υποστηρίζει μια παραλλαγή του υβριδικού μοντέλου, όπου ορισμένα δημόσια ιδρύματα μπορούν να λειτουργήσουν ως επικυρωτές συναλλαγών [18].

Χαρακτηριστικά	**Public Blockchain**	**Private Blockchain**	**Consortium/Hybrid Blockchain**
Πρόσβαση	Οποιοσδήποτε	Ένας οργανισμός	Πολλοί οργανισμοί
Ταυτότητα οντότητας	Ανώνυμη	Γνωστή	Γνωστή
Κατανάλωση ενέργειας	Μεγάλη	Μικρή	Μικρή
Τύπος Δικτύου	Αποκεντρωμένο	Μερικώς Αποκεντρωμένο	Αποκεντρωμένο (ένας συνδυασμός μεταξύ δημόσιου και ιδιωτικού)
Ταχύτητα συναλλαγών	Αργή	Γρήγορη	Γρήγορη
Χρήση	Μπορεί να χρησιμοποιηθεί σχεδόν σε κάθε κλάδο. Αρκετά καλό για δημόσια έργα, καθώς για τη δημιουργία κρυπτονομισμάτων για εμπορική χρήση.	Κατάλληλο για οργανισμούς που απαιτούν τον πλήρη έλεγχο της ροής εργασίας τους	Ταιριάζει καλύτερα σε έργα που δεν μπορούν να γίνουν ιδιωτικά ούτε δημόσια. Η αλυσίδα εφοδιασμού μπορεί να θεωρηθεί ένα εξαιρετικό παράδειγμα, ωστόσο είναι επίσης αποτελεσματικό στις τραπεζικές,

			χρηματοοικονομικές, IoT λειτουργίες.
Παραδείγματα	Bitcoin, Litecoin, Ethereum, Zcash, NXT	Monax, Ripple, MultiChain, Quorum	Hyperledger, Kadena, Korum, Corda, Energy Web Foundation
Αποκέντρωση	Ναι	Όχι	Μερική

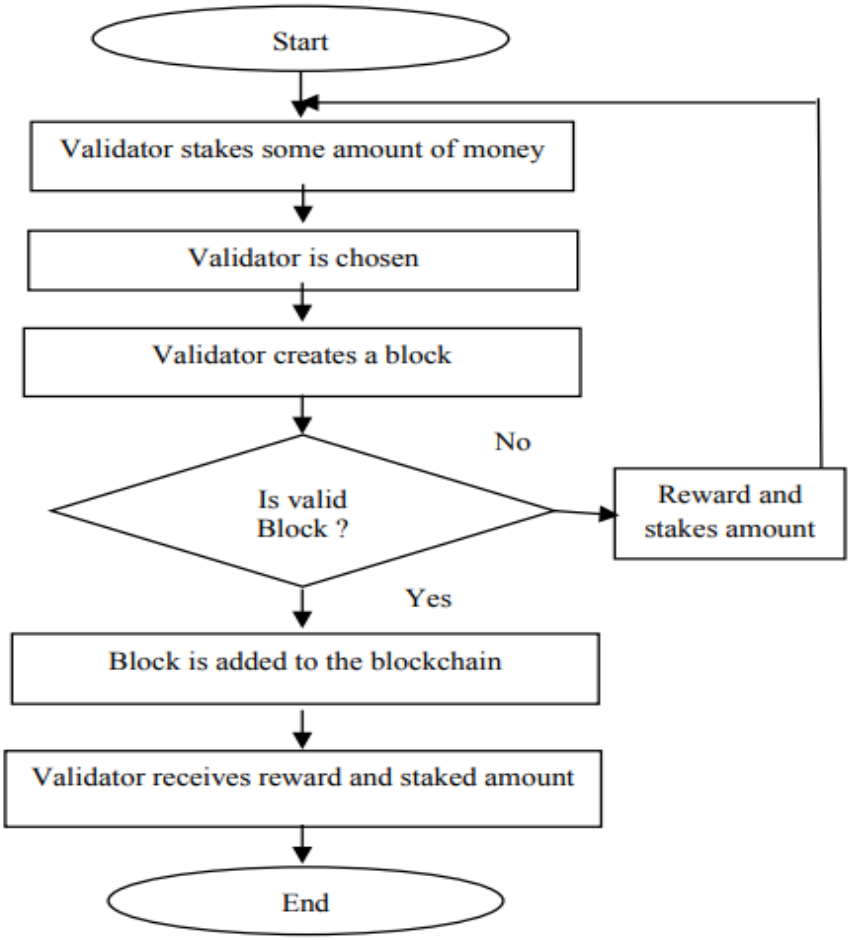
Πίνακας 1: Συγκεντρωτικός πίνακας διαφορών μεταξύ των παραπάνω τύπων

Αλγόριθμοι Συναίνεσης Blockchain

Ένας αλγόριθμος συναίνεσης είναι μια διαδικασία μέσω της οποίας όλοι οι κόμβοι του δικτύου Blockchain καταλήγουν σε μια κοινή συμφωνία σχετικά με την παρούσα κατάσταση του κατανεμημένου καθολικού. Με αυτόν τον τρόπο, οι αλγόριθμοι συναίνεσης επιτυγχάνουν αξιοπιστία στο δίκτυο και δημιουργούν εμπιστοσύνη σε ένα κατανεμημένο περιβάλλον υπολογιστών. Οι αλγόριθμοι συναίνεσης διασφαλίζουν ότι συγχρονίζονται όλοι οι κόμβοι στο δίκτυο. Αυτό σημαίνει ότι κάθε κόμβος πρέπει να επιλέξει αν θα συμπεριλάβει ή θα αποκλείσει μια νέα συναλλαγή στο αντίγραφο του καθολικού. Όταν η πλειονότητα των κόμβων επιλέξει να συμπεριλάβει τη συναλλαγή, επιτυγχάνεται συναίνεση και η συναλλαγή προστίθεται σε κάθε αντίγραφο του καθολικού. Ουσιαστικά, το πρωτόκολλο συναίνεσης διασφαλίζει ότι κάθε νέο μπλοκ που προστίθεται στο Blockchain συμφωνείται από όλους τους κόμβους του δικτύου. Ένα πρωτόκολλο συναίνεσης αποτελείται από ορισμένους συγκεκριμένους στόχους, όπως η επίτευξη συμφωνίας, η συνεργασία, τα ίσα δικαιώματα σε κάθε κόμβο και η υποχρεωτική συμμετοχή κάθε κόμβου στη διαδικασία συναίνεσης. Στο σημείο αυτό, θα δούμε διάφορους αλγόριθμους συναίνεσης και πώς λειτουργούν.

Ο αλγόριθμος Proof of Work

Όταν ξεκινά μια συναλλαγή, τα δεδομένα της συναλλαγής τοποθετούνται σε ένα μπλοκ με μέγιστη χωρητικότητα 1 megabyte και στη συνέχεια αντιγράφονται σε πολλούς υπολογιστές ή κόμβους στο δίκτυο. Οι κόμβοι είναι το διοικητικό σώμα του Blockchain και επαληθεύουν τη νομιμότητα των συναλλαγών σε κάθε μπλοκ. Για να πραγματοποιήσουν το βήμα επαλήθευσης, οι κόμβοι ή οι ανθρακωρύχοι (miners) θα πρέπει να λύσουν ένα υπολογιστικό πρόβλημα, γνωστό ως απόδειξη του προβλήματος εργασίας [8]. Η απόδειξη εργασίας (Proof of Work - POW) είναι μια στρατηγική συναίνεσης που χρησιμοποιείται στο δίκτυο του Bitcoin [6]. Ο αλγόριθμος αυτός απαιτεί μια περίπλοκη υπολογιστική διαδικασία για τον έλεγχο ταυτότητας. Σε Blockchain που χρησιμοποιούν τον POW, κάθε κόμβος του δικτύου υπολογίζει μια τιμή κατακερματισμού της συνεχώς μεταβαλλόμενης κεφαλίδας μπλοκ (block hash). Η συναίνεση απαιτεί ότι η υπολογισμένη τιμή πρέπει να είναι ίση ή μικρότερη από μια συγκεκριμένη δεδομένη τιμή. Στο αποκεντρωμένο δίκτυο, όλοι οι συμμετέχοντες πρέπει να υπολογίσουν την τιμή κατακερματισμού συνεχώς χρησιμοποιώντας διαφορετικά nonces (number only used once – μοναδικός αριθμός) έως ότου επιτευχθεί ο στόχος [1]. Όταν αποκτήσει ένας κόμβος τη σχετική τιμή, όλοι οι άλλοι κόμβοι πρέπει να επιβεβαιώνουν αμοιβαία την ορθότητα της τιμής. Οι κόμβοι που υπολογίζουν τους κατακερματισμούς καλούνται ανθρακωρύχοι (miners) και η διαδικασία του POW ονομάζεται εξόρυξη (mining) [6].

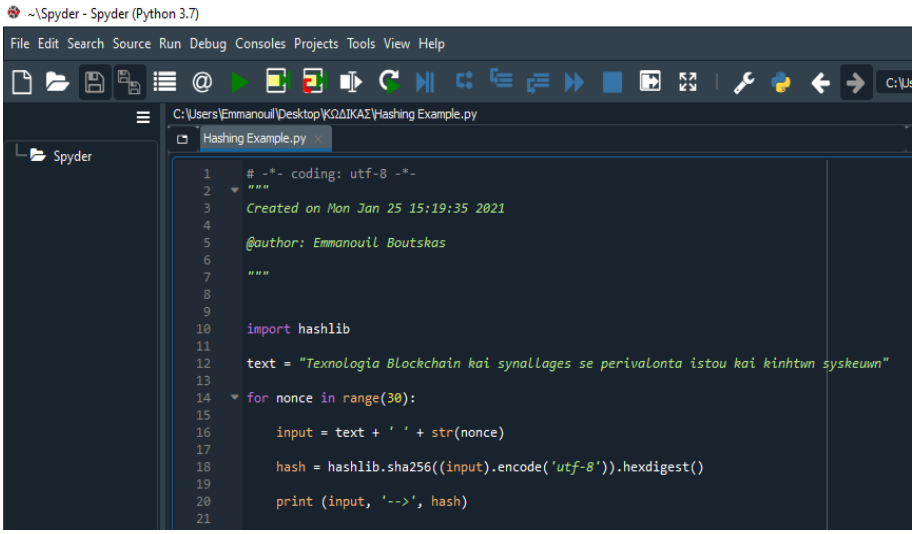


Εικόνα 1.13: Διάγραμμα ροής Proof of Work

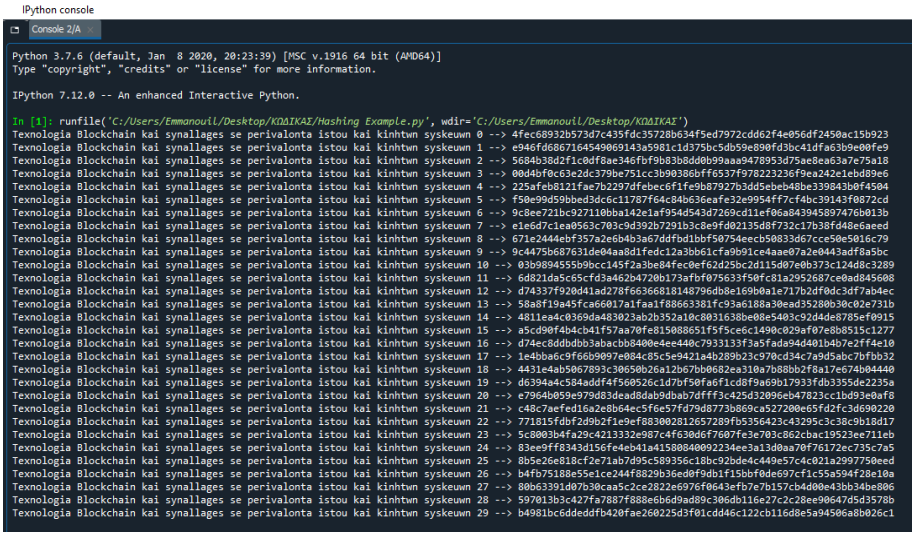
Ένα σύστημα απόδειξης εργασίας καταργεί τις επιθέσεις άρνησης εξυπηρέτησης και άλλες παραβιάσεις υπηρεσιών όπως το spam. Το βασικό χαρακτηριστικό αυτών των συστημάτων είναι η ασυμμετρία τους. Η εργασία θα πρέπει να είναι σχετικά δύσκολη (αλλά εφικτή) στην πλευρά του πελάτη, αλλά εύκολη στην επαλήθευση από την πλευρά του διακομιστή [7]. Μετά το λανσάρισμα του Bitcoin το 2009 και την εμφάνιση των κρυπτονομισμάτων ο όρος έγινε πολύ πιο γνωστός για τη χρήση του για την παροχή ασφάλειας στα νομισματικά συστήματα peer-to-peer. Το ευρύτερα χρησιμοποιούμενο σχήμα αποδείξεων εργασίας βασίζεται στον αλγόριθμο κατακερματισμού SHA-256 και εισήχθη ως μέρος του Bitcoin. Ορισμένοι άλλοι αλγόριθμοι κατακερματισμού που χρησιμοποιούνται για απόδειξη της εργασίας είναι οι Scrypt, Blake-256, Crypto Night, HEFTY1, Quark, SHA-3, scrypt-jane, scrypt-n και συνδυασμοί αυτών [5].

Η κρυπτογραφική συνάρτηση SHA-256 παράγει δεδομένα εξόδου μεγέθους 256 bit ανεξάρτητα από το μέγεθος των δεδομένων εισόδου. Στο παράδειγμα που ακολουθεί θα χρησιμοποιήσουμε την γλώσσα προγραμματισμού Python για να υπολογίσουμε το hash της φράσης «**Texnologia Blockchain kai synallages se perivalonta istou kai kinhtwn syskeuwn**»

Στο παρακάτω παράδειγμα θα υλοποιήσουμε ένα script για την παραγωγή πολλαπλών hashes με επαναλήψεις στην nonce τιμή. Όταν τρέξουμε το script παράγονται hashes αρκετών προτάσεων οι οποίες διαφοροποιούνται μεταξύ τους με την προσθήκη ενός αριθμού στο τέλος. Τα δεδομένα εξόδου θα είναι το παρακάτω:



Αποτέλεσμα:



Βλέπουμε ότι για κάθε πρόταση παράγεται εντελώς διαφορετικό hash διοτι αλλάζει η τιμή της μεταβλητής nonce. Η χρήση της nonce βοήθησε στο να παραχθούν διαφορετικά hashes, δηλαδή διαφορετικά δεδομένα εξόδου. Αν για παράδειγμα, θέλαμε να βρούμε μία φράση της οποίας το hash ξεκινά με έναν άσσο, τότε με βάση την παραπάνω εικόνα, βλέπουμε ότι χρειάστηκαν 17 προσπάθειες για να βρεθεί η φράση «**Texnologia Blockchain kai synallages se perivalonta istou kai kinhtwn syskeuwn 17**», η οποία παράγει ένα δεκαεξαδικό hash που ξεκινάει με έναν άσσο.

Υλοποίηση του Proof of Work

Το proof–of–work του Bitcoin μοιάζει αρκετά με το πρόβλημα που αναλύεται παραπάνω. Ο miner δημιουργεί ένα block το οποίο είναι γεμάτο με συναλλαγές. Εν συνεχεία προχωρά στον υπολογισμό του hash της επικεφαλίδας του block και εξετάζει αν αυτό είναι μικρότερο από τον στόχο. Αν είναι μικρότερο τότε ο miner τροποποιεί την τιμή της μεταβλητής nonce και προσπαθεί πάλι. Εξαιτίας της δυσκολίας του Bitcoin δικτύου πρέπει να γίνουν εκατομμύρια προσπάθειες από τους miners προκειμένου να βρουν ένα nonce από το οποίο θα προκύψει ένα μικρό hash για την επικεφαλίδα του μπλοκ. [7]

Παρακάτω παρουσιάζεται ένα παράδειγμα προσομοίωσης του proof-of-work στο οποίο ο αλγόριθμος χρησιμοποιώντας την συνάρτηση κατακερματισμού SHA-256 επιχειρεί να βρει ένα hash μικρότερο από τον αρχικό στόχο (target). Για την υλοποίηση του αλγορίθμου έχουμε εισάγει ένα δικό μας αρχικό block συναλλαγών.

Editor

C:\Users\Emmanouil\Desktop\ΚΩΔΙΚΑΣ\Proof-of-Work-Implementation.py

Proof-of-Work-Implementation.py*

```python
# -*- coding: utf-8 -*-
"""
Created on Mon Jan 25 15:19:35 2021

@author: https://github.com/subhan-nadeem/bitcoin-mining-python/blob/master/mining.py

"""

import hashlib

def get_sha_256_hash(input_value):
    return hashlib.sha256(input_value).hexdigest()

def block_hash_less_than_target(block_hash, given_target):
    return int(block_hash, 16) < int(given_target, 16)


# Arxiko Block me dedomena synallagwn
blockData = \
    '01000000000000000000000000000000000000000000000000000000000000000000000000000000' \
    '03ba3edfd7a7b12b27ac72c3e67768f617fc81bc3888a51323a9fb8aa4b1e5e4a29ab5f' \
    '49ffff001d1dac2b7c01010000000100000000000000000000000000000000000000000000000000' \
    '00000000000000000000000ffffffff4d04ffff001d0104455468652054696d65732030' \
    '332f4a616e2f323030392043686963616e63656c6c6f72206f6e20627266e6b206f66207365' \
    '636f6e64206261696c6f757420666f722062616e6b73ffffffff0100f2052a010000004' \
    '34104678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649' \
    'f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5fac00000000' \
        .encode()

# Arxikos Stoxos
target = '0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF'

solution_found = False
block_data_hexadecimal_value = int(blockData, 16)
nonce = 0

while not solution_found:
    block_data_with_nonce = block_data_hexadecimal_value + nonce


    first_hash = get_sha_256_hash(hex(block_data_with_nonce).encode())
    second_hash = get_sha_256_hash(first_hash.encode())

    print('Nonce: ' + str(nonce))

    print('Block hash:')
    print(second_hash)

    print('Einai to hash tis epikefalidas tou block mikrotero apo ton stoxo?')
    solution_found = block_hash_less_than_target(second_hash, target)
    print(solution_found)
    print(" ")
    if not solution_found:
        nonce += 1

```

Αποτέλεσμα:

```
Nonce: 43656

Block Hash:
e9ce0be8280618b4eabea75f562d9b0f8e91cb8f29bdc2ebed938c259ac92847

Einai to hash tis epikefalidas tou block mikrotero apo ton stoxo ?
False

Nonce: 43657

Block Hash:
b142eee7dd41d68a8650f0b1b209ebf39c49ac5fb900b2335348a77f2de78480

Einai to hash tis epikefalidas tou block mikrotero apo ton stoxo ?
False
```

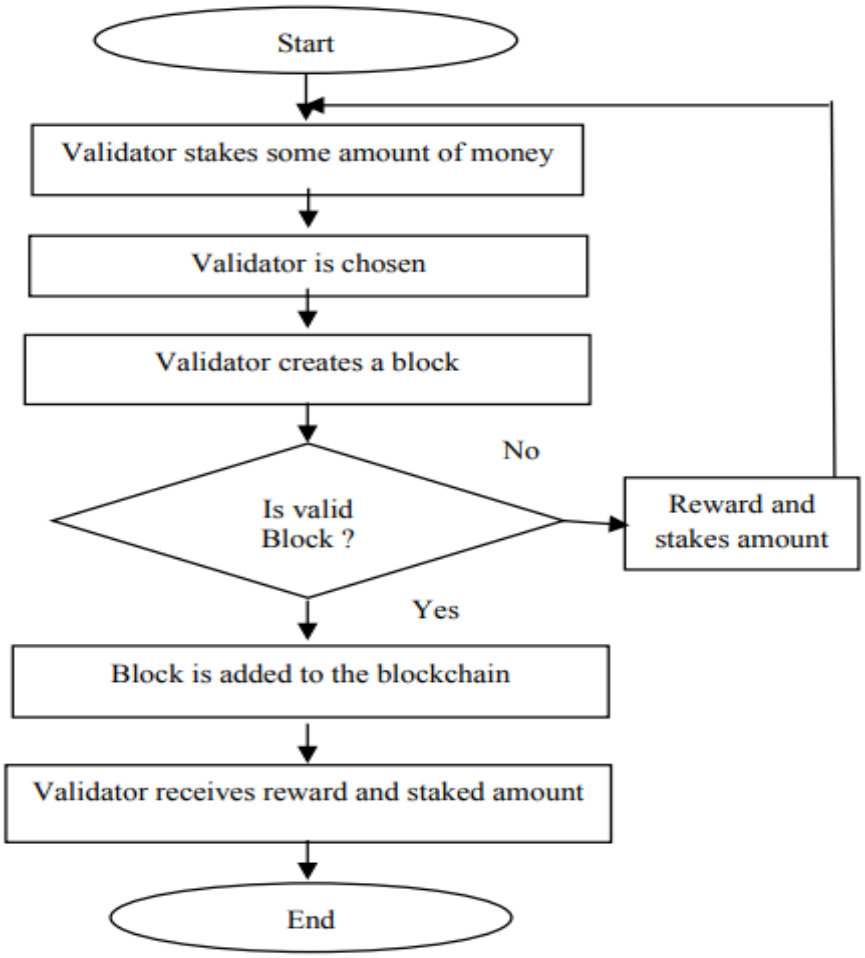
Και στις δύο εξόδους που εμφανίζονται στην παραπάνω εικόνα φαίνεται ότι ο αλγόριθμος δεν κατάφερε να βρει hash μικρότερο του αρχικού στόχου.

Ο αλγόριθμος Proof of Stake

Στοχεύει στη διατήρηση της αποκεντρωμένης φύσης του Blockchain δικτύου. Στον αλγόριθμο Proof-of-Stake ένας κόμβος με n% πόρους έχει n% πιθανότητες να δημιουργήσει ένα μπλοκ. Ως εκ τούτου, η βασική αρχή του Proof-of-Stake είναι ότι ο κόμβος με το υψηλότερο ποντάρισμα (stake) έχει μεγαλύτερη πιθανότητα για να επιλεγεί για τη δημιουργία του επόμενου μπλοκ [4]. Ο όρος “staking” (ποντάρισμα) ουσιαστικά αναφέρεται στην τοποθέτηση νομισμάτων ως εγγύηση [53]. Η διαδικασία του πονταρίσματος δεν συνεπάγεται με σχεδόν κανένα κόστος στον πραγματικό κόσμο, σε αντίθεση με την εξόρυξη όπου οι miners πρέπει να πληρώσουν για το υλικό (hardware), την ηλεκτρική ενέργεια και τη συντήρησή του. Σε περίπτωση που κάποιος επικυρωτής προσπαθήσει να προωθήσει μη έγκυρες συναλλαγές, όταν έρθει η σειρά του να επικυρώσει το επόμενο μπλοκ θα χάσει ένα μέρος του πονταρίσματος του. Αντ’ αυτού, οι έντιμοι χρήστες αποζημιώνονται με τα τέλη συναλλαγής που καταβάλλονται για τη χρήση του δικτύου. Επίσης, οι χρήστες που κατέχουν ένα μεγάλο ποσό νομισμάτων αποκλείονται από την προώθηση μη έγκυρων συναλλαγών, καθώς αυτό πιθανώς θα μειώσει την τιμή του εν λόγω κρυπτονομίσματος και θα μειώσει την αξία των νομισμάτων τους. Με την τοποθέτηση νομισμάτων ως εγγύηση, οι χρήστες αποκτάνε κάποια ισχύ αποφάσεων στο δίκτυο και τη δυνατότητα δημιουργίας εσόδων.

Αυτό μοιάζει αρκετά με τον τρόπο με τον οποίο κάποιος θα λάβει τόκους για την κατοχή χρημάτων σε τραπεζικό λογαριασμό ή την παράδοση στην τράπεζα για επένδυση.

Ο αλγόριθμος Proof of Stake δημιουργήθηκε ως εναλλακτική λύση του Proof-of-Work για την αντιμετώπιση εγγενών ζητημάτων, όπως αυτό της κατανάλωσης ενέργειας. Η εξόρυξη απαιτεί μεγάλη υπολογιστική ισχύ για την εκτέλεση των διάφορων κρυπτογραφικών υπολογισμών [10]. Η υπολογιστική ισχύς μεταφράζεται σε μεγάλη ποσότητα ηλεκτρισμού και ισχύος που απαιτείται από το Proof-of-Work. Το 2015, εκτιμήθηκε ότι μια συναλλαγή Bitcoin απαιτούσε την ποσότητα ηλεκτρικής ενέργειας που απαιτείται για την τροφοδοσία 1,57 αμερικανικών νοικοκυριών την ημέρα [52]. Ο αλγόριθμος Proof-of-Stake επιδιώκει να αντιμετωπίσει αυτό το ζήτημα αποδίδοντας εξορυκτική δύναμη στην αναλογία των κερμάτων που κατέχει ο εκάστοτε ανθρακωρύχος (miner). Με αυτόν τον τρόπο, αντί να χρησιμοποιεί ενέργεια για να λύνει υπολογιστικά προβλήματα, ένας miner περιορίζεται στην εξόρυξη ενός ποσοστού συναλλαγών που αντικατοπτρίζει το μερίδιο ιδιοκτησίας του. Για παράδειγμα, ένας ανθρακωρύχος που κατέχει το 3% του διαθέσιμου Bitcoin μπορεί θεωρητικά να εξορύξει μόνο το 3% των μπλοκ [52].



Εικόνα 1.14: Διάγραμμα Ροής Proof of Stake

Ωστόσο, προκειμένου η διαδικασία να μην ευνοεί μόνο τους πλουσιότερους κόμβους στο δίκτυο, προστίθενται πιο μοναδικές μέθοδοι στη διαδικασία επιλογής. Οι δύο πιο συχνά χρησιμοποιούμενες μέθοδοι είναι η «Τυχαιοποιημένη επιλογή μπλοκ» (Randomized Block Selection) και η «Επιλογή ηλικίας νομισμάτων» (Coin Age Selection) [51]. Στη μέθοδο Randomized Block Selection οι επικυρωτές επιλέγονται αναζητώντας κόμβους με συνδυασμό της χαμηλότερης τιμής κατακερματισμού και του υψηλότερου πονταρίσματος. Η μέθοδος Coin Age Selection επιλέγει τους επικυρωτές με βάση το χρονικό διάστημα για το οποίο τα στοιχήματά (stakes) τους έχουν τοποθετηθεί. Η ηλικία του νομίσματος υπολογίζεται πολλαπλασιάζοντας τον αριθμό των ημερών που κρατήθηκαν τα κέρματα ως στοίχημα με τον αριθμό των κερμάτων που στοιχηματίστηκαν. Μόλις ένας κόμβος εξορύξει ένα μπλοκ, η ηλικία των νομισμάτων του επαναφέρεται στο μηδέν και πρέπει να περιμένει μια συγκεκριμένη χρονική περίοδο για να μπορέσει να εξορύξει ένα άλλο μπλοκ, αυτό εμποδίζει τους

μεγάλους κόμβους πονταρίσματος να κυριαρχήσουν στο Blockchain. Ωστόσο, αυτές δεν είναι οι μόνες μέθοδοι επιλογής επικυρωτών. Ορισμένα νομίσματα συνδυάζουν τις προαναφερθείσες μεθόδους, ενώ άλλα πειραματίζονται με τις δικές τους.

Πλεονεκτήματα του Proof-Of-Stake

Το Proof-of-Stake θεωρείται ευρέως ως μία από τις καλύτερες επιλογές για αλγόριθμους συναίνεσης κρυπτονομισμάτων. Αυτό οφείλεται στους εξής λόγους:

Ενεργειακή απόδοση

Η υπολογιστική πολυπλοκότητα του Proof-of-Stake είναι μικρή και συνήθως δεν είναι ευαίσθητη στο μέγεθος του δικτύου. Αυτό συμβαίνει επειδή οι κόμβοι που συμμετέχουν στο δίκτυο δεν ανταγωνίζονται ο ένας τον άλλον για το ποιος θα φέρει το επόμενο μπλοκ στο Blockchain. Επομένως, ενεργειακά είναι πολύ αποδοτικό για συστήματα μεγάλης κλίμακας. Η κατανάλωση ενέργειας των Blockchains που χρησιμοποιούν το Proof-of-Stake είναι αρκετές τάξεις μεγέθους χαμηλότερη από αυτή του Proof-of-Work. Αυτός είναι και ο κύριος λόγος που η κοινότητα του κρυπτονομίσματος με τη δεύτερη υψηλότερη κεφαλαιοποίηση της αγοράς, το Ethereum, προσπαθεί να μεταβεί από το Proof-of-Work στο Proof-of-Stake. Άλλα κρυπτονομίσματα, όπως το EOS, Tezos και TRON τα οποία εμφανίζονται ανάμεσα στα 20 κορυφαία κρυπτονομίσματα όσον αφορά την κεφαλαιοποίηση της αγοράς χρησιμοποιούν ήδη με επιτυχία το Proof-of-Stake [10].

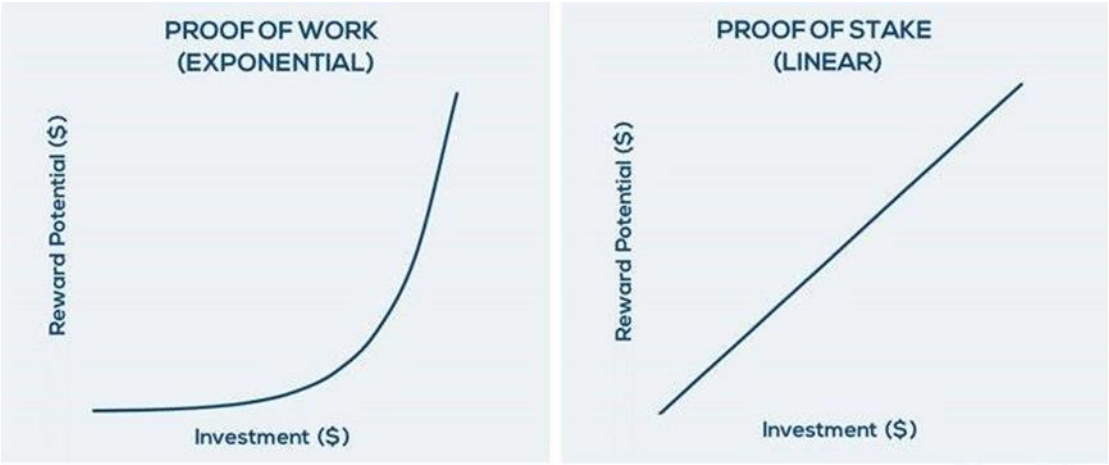
Ασφάλεια

Για τον αποτελεσματικό έλεγχο του δικτύου και την έγκριση δόλιων συναλλαγών, ένας κόμβος θα πρέπει να κατέχει το μεγαλύτερο ποσοστό στο δίκτυο, γνωστό και ως επίθεση 51%. Αν και θα ήταν δύσκολο και δαπανηρό να συγκεντρωθεί το 51% ενός αξιόπιστου ψηφιακού νομίσματος, ένας ανθρακωρύχος που έχει στην κατοχή του το 51% της κυκλοφορίας και τον έλεγχο του δικτύου, δεν θα είχε κανένα συμφέρον να επιτεθεί σε ένα δίκτυο στο οποίο κατέχει το μεγαλύτερο μέρος. Εάν η αξία του κρυπτονομίσματος πέσει, αυτόματα και η αξία των μετοχών του θα πέσει επίσης.

Συνεπώς, ο ιδιοκτήτης της πλειοψηφίας έχει περισσότερα κίνητρα να διατηρήσει ένα ασφαλές δίκτυο σε αντίθεση με ένα συστήματα που χρησιμοποιεί το Proof-of-Work όπου οι εισβολείς δεν χάνουν το υλικό τους όταν επιχειρούν επιθέσεις 51% [51][52].

Αποκέντρωση

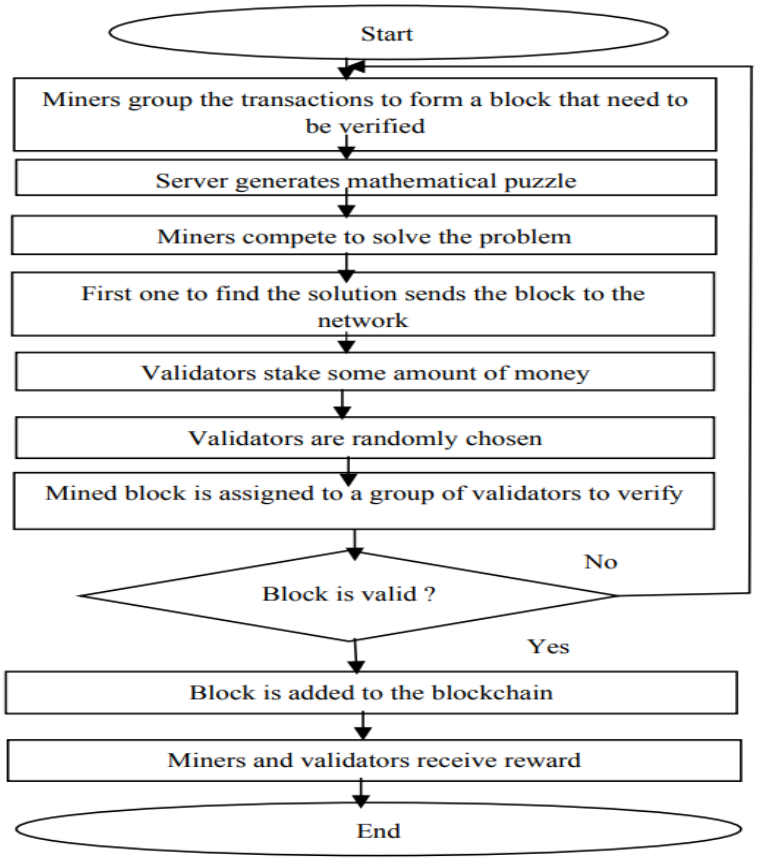
Το γεγονός ότι μεγάλες ομάδες ανθρακωρύχων (miners) μπορούν να συνδυάσουν τους πόρους τους με σκοπό να δημιουργήσουν δεξαμενές εξόρυξης (mining pools) προκειμένου να ελέγξουν πάνω από το 51% του δικτύου αποτελεί μια πραγματική απειλή που οδηγεί σε μια ποιο κεντροποιημένη μορφή του Blockchain. Αυτό οφείλεται στην εκθετική αύξηση της ανταμοιβής ανά επένδυση σε συστήματα που χρησιμοποιούν το Proof-of-Work, σε αντίθεση με τη γραμμική αύξηση στα συστήματα που κάνουν χρήση του Proof-of-Stake. Εάν ένας χρήστης σε δίκτυο που βασίζεται σε Proof-of-Stake επενδύει δύο φορές περισσότερο από έναν άλλο χρήστη, θα έχει διπλάσιο έλεγχο. Το ίδιο σενάριο για το Proof-of-Work θα έδινε στον χρήστη εκθετικά μεγαλύτερο έλεγχο [54].



Εικόνα 1.15: Εκθετική αύξηση ανταμοιβών και γραμμική αύξηση ανταμοιβών σε συστήματα που χρησιμοποιούν PoW και PoS

Ο αλγόριθμος Proof of Authority

Η βασική ιδέα του Proof of Authority (PoA) είναι να οριστεί ένα σύνολο κόμβων ως εξουσιάζοντες. Αυτοί οι κόμβοι αναλαμβάνουν το έργο της δημιουργίας νέων μπλοκ και της επικύρωσης των συναλλαγών [9]. Αναφέρονται ως "validators" (επικυρωτές) και εκτελούν λογισμικό που τους επιτρέπει να τοποθετούν συναλλαγές σε μπλοκ. Η διαδικασία είναι αυτοματοποιημένη και δεν απαιτεί οι επικυρωτές να παρακολουθούν συνεχώς τους υπολογιστές τους [48]. Οι κόμβοι επικύρωσης έχουν πλήρη ισχύ στο να αποφασίζουν για νέα μπλοκ. Αυτό σημαίνει, για παράδειγμα, ότι έχουν τη δυνατότητα να σταματήσουν συγκεκριμένες συναλλαγές, οι οποίες μπορούν να προκαλέσουν συγκρούσεις συμφερόντων ή και ακόμη να θέσουν σε κίνδυνο την ασφάλεια του δικτύου [9]. Ο αλγόριθμος συναίνεσης PoA αξιοποιεί την αξία των ταυτοτήτων, πράγμα που σημαίνει ότι οι επικυρωτές μπλοκ δεν ποντάρουν κρυπτονομίσματα αλλά αντ' αυτού τη φήμη τους. Είναι κατάλληλος τόσο για ιδιωτικά όσο και για δημόσια δίκτυα, όπως το POA Network, όπου η εμπιστοσύνη είναι κατανεμημένη [48].



Εικόνα 1.16: Διάγραμμα Ροής Proof of Authority [12]

Στο Proof of Authority ένα μπλοκ σηματοδοτείται ως τμήμα του Blockchain εάν έχει υπογραφεί από την πλειοψηφία των εγκεκριμένων κόμβων. Σε αντίθεση με τον μηχανισμό Proof-of-Work, που συνήθως αναφέρεται ως «εξόρυξη», δεν υπάρχει τεχνικός ανταγωνισμός μεταξύ των επικυρωτών εδώ. Αυτός ο μηχανισμός συναίνεσης δεν απαιτεί σχεδόν καθόλου υπολογιστική ισχύ και συνεπώς σχεδόν καθόλου ηλεκτρισμό για τη λειτουργία του. Δεδομένου ότι το PoA απαιτεί μόνο έναν περιορισμένο αριθμό εμπλεκόμενων, το δίκτυο έχει την οικονομική δυνατότητα να ενημερώνει το Blockchain πιο συχνά μειώνοντας το χρόνο μεταξύ κάθε μπλοκ (Blocktime) και να επεξεργάζεται περισσότερες συναλλαγές (Blocksize). Το Proof-of-Authority συχνά προτιμάται από ιδιωτικές Blockchain ή Blockchain κοινοπραξίας. Παράγοντες στον τραπεζικό τομέα, όπως η JP Morgan με το JPMCoin, χρησιμοποιούν αυτήν την τεχνολογία για να διευκολύνουν τον έλεγχο των κινήσεων κεφαλαίων τους, κυρίως για λογιστικούς σκοπούς, με μειωμένο κόστος [49].

Ο αλγόριθμος Practical Byzantine Fault Tolerance (PBFT)

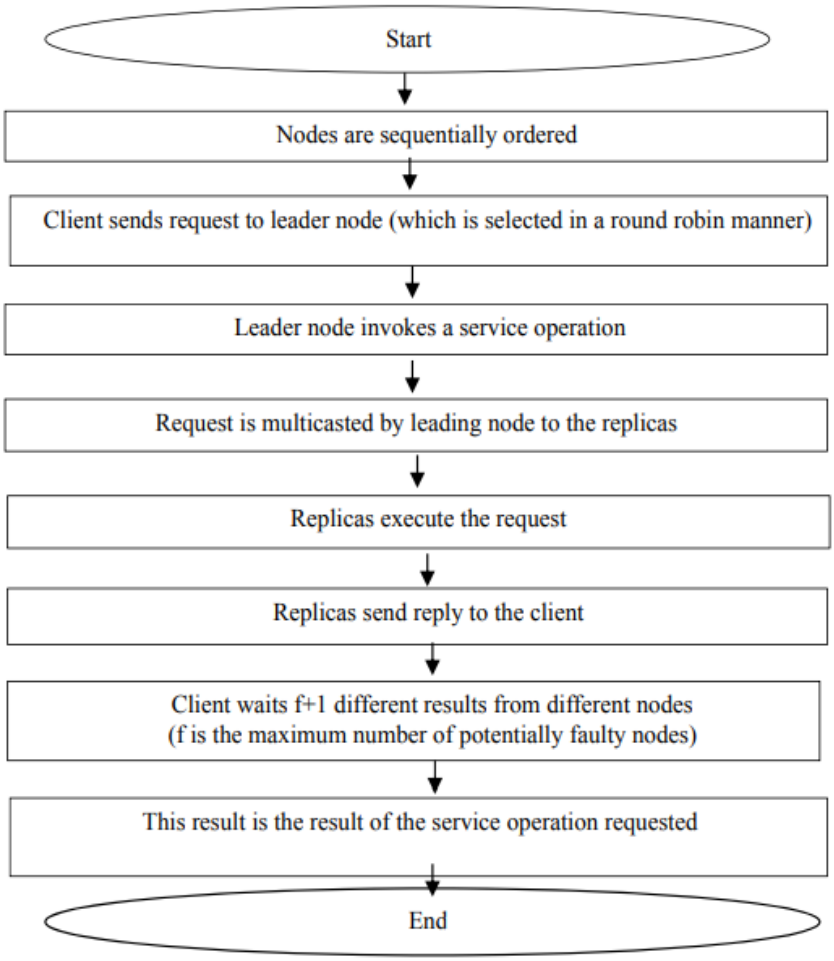
Η ανοχή βυζαντινού σφάλματος (Byzantine Fault Tolerance - BFT) είναι το χαρακτηριστικό ενός κατανεμημένου δικτύου για την επίτευξη συναίνεσης ακόμη και όταν ορισμένοι από τους κόμβους του δικτύου δεν ανταποκρίνονται ή ανταποκρίνονται με εσφαλμένες πληροφορίες. Ο στόχος ενός μηχανισμού BFT είναι η προστασία από τις αστοχίες του συστήματος χρησιμοποιώντας συλλογική λήψη αποφάσεων που στοχεύει στη μείωση της επιρροής των ελαττωματικών κόμβων. Το BFT προέρχεται από το πρόβλημα των Βυζαντινών στρατηγών [50].

Το Practical Byzantine Fault Tolerance (PBFT) είναι ένας αλγόριθμος που βελτιστοποιεί πτυχές του Byzantine Fault Tolerance και εφαρμόζεται σε πολλά σύγχρονα κατανεμημένα συστήματα υπολογιστών, συμπεριλαμβανομένων ορισμένων πλατφορμών Blockchain. Αυτές οι Blockchain χρησιμοποιούν συνήθως έναν συνδυασμό PBFT και άλλων μηχανισμών συναίνεσης [9]. Οι κόμβοι σε ένα σύστημα PBFT ταξινομούνται διαδοχικά με έναν κόμβο να είναι ο αρχηγός και άλλοι αναφέρονται ως εφεδρικοί κόμβοι.

Όλοι οι κόμβοι του συστήματος επικοινωνούν μεταξύ τους με στόχο να είναι όλοι οι ειλικρινείς κόμβοι σε συμφωνία για την κατάσταση του συστήματος χρησιμοποιώντας έναν κανόνα πλειοψηφίας. Η επικοινωνία μεταξύ κόμβων έχει δύο λειτουργίες: οι κόμβοι πρέπει να αποδεικνύουν ότι τα μηνύματα προέρχονται από έναν συγκεκριμένο κόμβο και πρέπει να επαληθεύσουν ότι το μήνυμα δεν τροποποιήθηκε κατά τη μετάδοση [9]. Ένα πρακτικό σύστημα βυζαντινού σφάλματος μπορεί να λειτουργήσει με την προϋπόθεση ότι ο μέγιστος αριθμός κακόβουλων κόμβων δεν πρέπει να είναι μεγαλύτερος ή ίσος με το ένα τρίτο όλων των κόμβων του συστήματος [50]. Καθώς ο αριθμός των κόμβων αυξάνεται, το σύστημα γίνεται πιο ασφαλές.

Οι γύροι συναίνεσης του PBFT χωρίζονται σε 4 φάσεις [50]:

1. Ένας πελάτης (client) στέλνει ένα αίτημα στον κύριο κόμβο (leader) για να επικαλεστεί μια λειτουργία υπηρεσίας.
2. Ο κύριος κόμβος (ηγέτης) μεταδίδει το αίτημα σε όλους τους δευτερεύοντες (εφεδρικούς) κόμβους.
3. Οι κόμβοι εκτελούν το αίτημα και στη συνέχεια στέλνουν μια απάντηση στον πελάτη.
4. Ο πελάτης περιμένει f + 1 απαντήσεις από διαφορετικούς κόμβους με το ίδιο αποτέλεσμα, όπου f αντιπροσωπεύει τον μέγιστο επιτρεπόμενο αριθμό ελαττωματικών κόμβων.



Εικόνα 1.17: Διάγραμμα Ροής Practical Byzantine Fault Tolerance

Ενεργειακή Κατανάλωση Blockchain

Η κύρια πρόκληση που αντιμετωπίζει η τεχνολογία του Blockchain είναι η υψηλή κατανάλωση ενέργειας. Ο κύριος λόγος για την υψηλή κατανάλωση ενέργειας των Blockchains οφείλεται σε μεγάλο βαθμό στην χρήση του Proof of Work και στη διαδικασία εκτέλεσης του. Έρευνες έχουν δείξει ότι τα Blockchains χρησιμοποιούν ετησίως ενέργεια που είναι περίπου ίση με την κατανάλωση ενέργειας ενός έθνους ετησίως [57]. Αυτό πηγάζει ως επί το πλείστων από την διαδικασία εξόρυξης των Bitcoins. Τα Bitcoins εξορύσσονται χρησιμοποιώντας ειδικό υλικό εξόρυξης που σχεδιάστηκε και βελτιώθηκε με την πάροδο του χρόνου για να μειώσει την κατανάλωση ενέργειας. Στα πρώτα στάδια της τεχνολογίας η εξόρυξη μπλοκ γίνονταν

μέσω επεξεργαστών (CPU) που ήταν αργοί και χρησιμοποιούσαν πάρα πολύ ενέργεια. Έτσι, άρχισαν να χρησιμοποιούνται τώρα οι κάρτες γραφικών (GPU), που υπολογίζεται ότι είναι σχεδόν 100 φορές γρηγορότερες από τους κλασσικούς επεξεργαστές και χρησιμοποιούν επίσης συγκριτικά λιγότερη ενέργεια. Αυτό βελτιώθηκε ακόμη περαιτέρω με την άφιξη των ASICS που είναι ταχύτερα και καταναλώνουν αρκετά λιγότερη ενέργεια συγκριτικά με τα FPGA, CPU ή GPU [56].

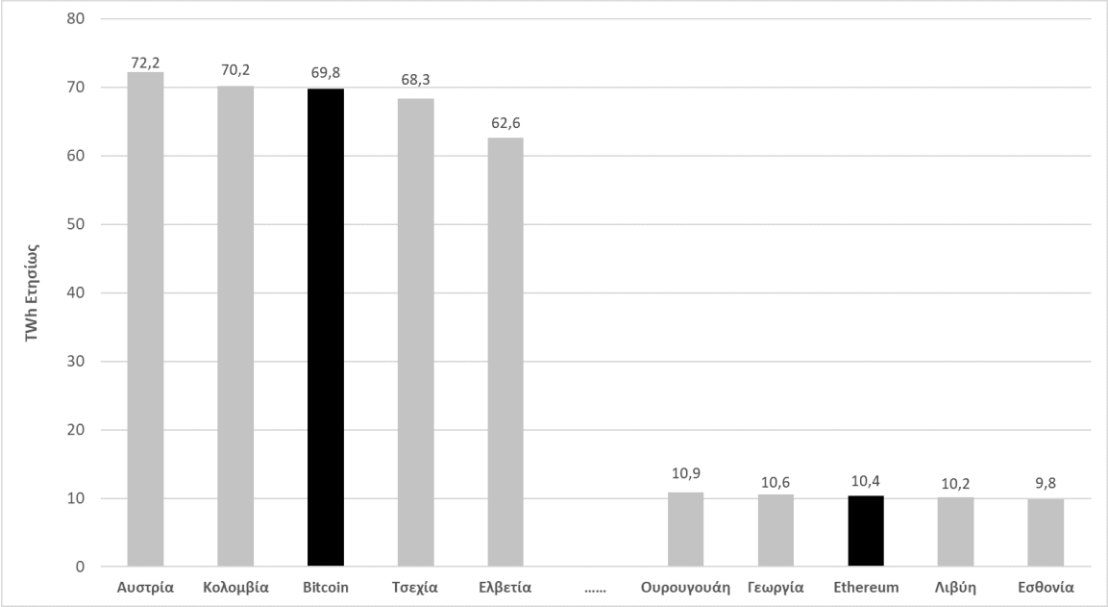
Πέραν αυτού, τα τελευταία χρόνια έχει αναπτυχθεί ένας σημαντικός αριθμός ενεργειακά αποδοτικών αλγόριθμων, όπως ο Proof-of-Stake,. Στο Proof-of-Stake, οι ιδιοκτήτες κερμάτων δημιουργούν μπλοκ και όχι οι miners, επομένως δεν απαιτούνται μηχανές που καταναλώνουν ενέργεια με σκοπό να παράγουν όσο το δυνατόν περισσότερα hash ανά δευτερόλεπτο. Εξαιτίας αυτού, η ενεργειακή κατανάλωση του Proof-of-Stake είναι αμελητέα σε σύγκριση με αυτή του Proof-of-Work. Το Bitcoin θα μπορούσε ενδεχομένως να μεταβεί σε έναν τέτοιο αλγόριθμο συναίνεσης, ο οποίος θα βελτιώσει σημαντικά τη βιωσιμότητα. Το μόνο μειονέκτημα είναι ότι υπάρχουν πολλές διαφορετικές εκδοχές του Proof-of-Stake και καμία από αυτές δεν έχει αποδειχθεί πλήρως.

Σύγκριση του Ethereum με το Bitcoin

Τα περισσότερα κρυπτονομίσματα δεν έχουν ακριβή εκτίμηση της κατανάλωσης ενέργειας των δικτύων τους, εξαιρουμένων των Bitcoin και Ethereum. Γι’ αυτό τον λόγο, στην συγκεκριμένη ενότητα θα συγκριθούν μόνο αυτά τα δύο νομίσματα. Δεδομένου ότι τόσο το Bitcoin όσο και το Ethereum χρησιμοποιούν επί του παρόντος το πρωτόκολλο συναίνεσης Proof of Work, μπορεί να θεωρηθεί με ασφάλεια ότι τα κρυπτονομίσματα που δεν χρησιμοποιούν το Proof of Work καταναλώνουν λιγότερη ισχύ ανά συναλλαγή.

Το παρακάτω γράφημα δείχνει την τρέχουσα κατανάλωση ενέργειας των δικτύων Bitcoin και Ethereum σε σύγκριση με επιλεγμένες χώρες. Ο άξονας Υ αντιπροσωπεύει την συνολική ενέργεια με την οποία τροφοδοτείται το δίκτυο του Bitcoin και Ethereum και ο άξονας Χ αντιπροσωπεύει τις διάφορες χώρες. Όπως φαίνεται ολόκληρο το δίκτυο του Bitcoin καταναλώνει λίγο περισσότερη ισχύ από τη Τσεχία και ελαφρώς μικρότερη από την Κολομβία και την Αυστρία. Ταυτόχρονα, ολόκληρο το δίκτυο του

Ethereum καταναλώνει περίπου 6,7 φορές λιγότερη ενέργεια από το δίκτυο του Bitcoin. Ωστόσο, παρουσιάζει ελαφρώς μεγαλύτερη ισχύ από την Λιβύη και την Εσθονία και ελαφρώς μικρότερη από την Γεωργία και την Ουρουγουάη.



Εικόνα 1.18: Σύγκριση της κατανάλωσης ενέργειας μεταξύ των δικτύων Bitcoin και Ethereum και επιλεγμένων χωρών σε TWh / έτος, με βάση τις [57] και [58], από το 2020-09-28

Στις 22 Ιανουαρίου 2019, Ο Δείκτης Κατανάλωσης Ενέργειας Bitcoin εκτιμούσε ότι το 100% των εσόδων από ανθρακωρύχους το οποίο ανέρχεται σε περίπου 2,3 δισεκατομμύρια δολάρια δαπανήθηκε για το κόστος ηλεκτρικής ενέργειας [57]. Αν το Bitcoin έπρεπε να χειριστεί τον απαιτούμενο αριθμό συναλλαγών από ένα παγκόσμιο σύστημα πληρωμών, οι σχετικές εκπομπές διοξειδίου του άνθρακα και μόνο θα οδηγούσαν σε παγκόσμια αύξηση της θερμοκρασίας κατά 2^{o} C τις επόμενες δεκαετίες.

Το ψηφιακό νόμισμα καταναλώνει 685 κιλοβατώρες ηλεκτρικής ενέργειας για μια μόνο συναλλαγή. Αυτό ισοδυναμεί με περίπου 460.000 συναλλαγές Visa, καθιστώντας το την πιο ενεργειακή μορφή ηλεκτρονικού εμπορίου που είναι γνωστή σήμερα [57]. Η ενέργεια που απαιτείται για την επεξεργασία των εξαιρετικά πολύπλοκων αλγορίθμων Blockchain για μια μόνο συναλλαγή θα ήταν αρκετή για να τροφοδοτήσει περίπου 20 νοικοκυριά των ΗΠΑ για μία μέρα.

Περιγραφή	Τιμές
Τρέχουσα εκτιμώμενη ετήσια κατανάλωση ηλεκτρικής ενέργειας (TWh)	77,78
Τρέχουσα ελάχιστη κατανάλωση ηλεκτρικής ενέργειας (TWh)	57,15
Ετήσιο αποτύπωμα άνθρακα (Mt co2)	36,95
Ηλεκτρική ενέργεια που καταναλώνεται ανά συναλλαγή (kWh)	684,51
Αποτύπωμα άνθρακα ανά συναλλαγή (kg co2)	325,14

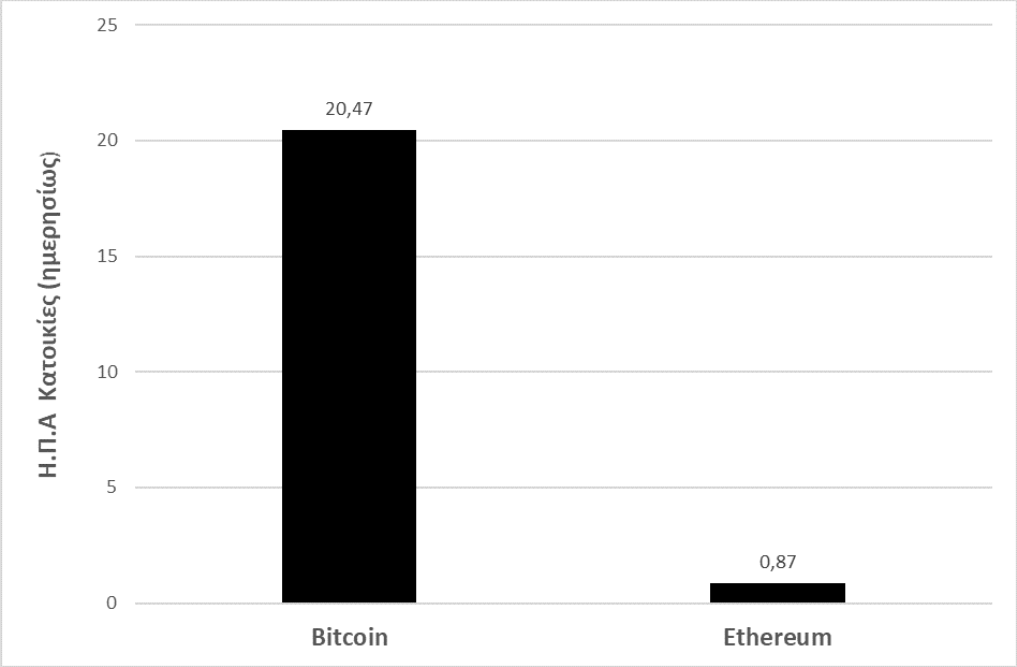
Πίνακας 2: Κατανάλωση ενέργειας Bitcoin [57]

Ο Πίνακας 2 δείχνει διαφορετικά υλικά (hardware) εξόρυξης Bitcoin και την αντίστοιχη απόδοση ισχύος.

Όνομα	Hash Rate	Ενεργειακή Απόδοση (W)
DragonMint T1	16 TH/s	1480W
Antminer T9+	10.5 TH/s	1332W
Antminer R4	8.6 TH/s	845W
Avalon6	3.5 TH/s	1050W
Antminer S9	14 TH/s	1,372W
M3X	12 – 13 TH/s	2,100W

Πίνακας 3: Hardware Εξόρυξης Bitcoin [59]

Για να κατανοήσουμε καλύτερα την ενέργεια που καταναλώνεται από το δίκτυο του Ethereum και του Bitcoin θα προχωρήσουμε σε μία ακόμη σύγκριση μεταξύ τους. Το παρακάτω γράφημα δείχνει τη συνολική κατανάλωση ενέργειας για καθένα από τα δύο δίκτυα, μετρούμενη ως προς τον συνολικό αριθμό των νοικοκυριών των ΗΠΑ που θα μπορούσαν να τροφοδοτηθούν από αυτό. Ο υπολογισμός της ενέργειας υπολογίζεται ανά μία συναλλαγή. Το αποτέλεσμα του παρακάτω γραφήματος παρουσιάζει έναν αριθμό KWh που θα μπορούσε εύκολα να τροφοδοτήσει πολλαπλά νοικοκυριά των ΗΠΑ για μια ολόκληρη μέρα.



Εικόνα 1.19: Κατανάλωση ενέργειας ανα συναλλαγή [58]

Είναι προφανές, παρά το γεγονός ότι και τα δύο κρυπτονομίσματα χρησιμοποιούν το ίδιο πρωτόκολλο συναίνεσης, ότι το Ethereum είναι πολλές φορές πιο αποτελεσματικό από το Bitcoin. Προβλέπεται ότι, σε περίπτωση επιτυχούς μετάβασης του Ethereum πρωτόκολλο συναίνεσης Proof of Stake, ότι η διαφορά ισχύος μεταξύ των δύο νομισμάτων θα αυξηθεί ακόμη περισσότερο.

Επιθέσεις και Κίνδυνοι στο Blockchain

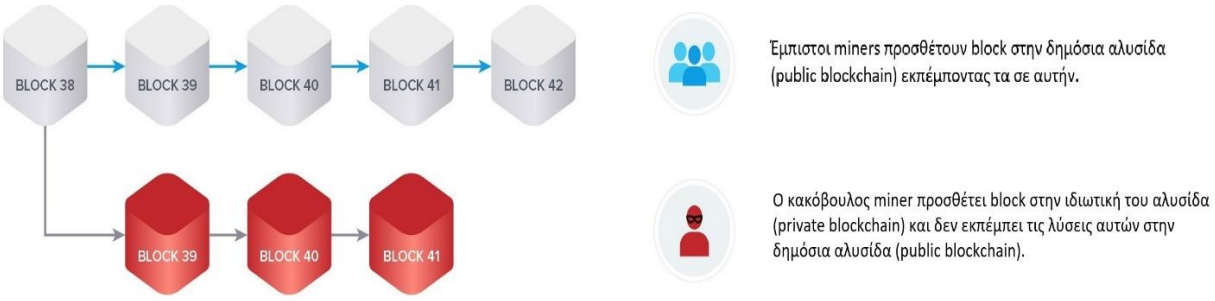
Παρόλο που η τεχνολογία Blockchain αποτρέπει διάφορους τύπους κακόβουλων επιθέσεων και μειώνει πολλούς σχετικούς κινδύνους, δεν εξαλείφει όλες τις επιθέσεις. Οι προληπτικοί μηχανισμοί του (π.χ. κατανεμημένη συναίνεση, κρυπτογραφία, ανωνυμία) μπορεί να επηρεάσουν την αντίστασή του σε άλλους τύπους απάτης και κακόβουλων λειτουργιών. Αυτές περιλαμβάνουν την επίθεση 51%, την ανάληψη λογαριασμού, την κλοπή ψηφιακής ταυτότητας, το ξέπλυμα χρημάτων και την εισβολή.

Επίθεση Πλειοψηφίας (51% Attack)

Με την χρήση του proof-of-work, η πιθανότητα εξόρυξης ενός μπλοκ εξαρτάται από την εργασία του miner (π.χ. CPU / GPU κύκλοι που δαπανώνται για τον έλεγχο των hashes). Λόγω αυτού του μηχανισμού, ο επιτιθέμενος ή οι επιτιθέμενοι προσπαθούν να εξορύξουν περισσότερα μπλοκ, και να γίνουν "δεξαμενές εξόρυξης" (mining pools) , με σκοπό να κατέχουν περισσότερη υπολογιστική ισχύ. Μόλις αποκτήσουν το 51% της συνολικής υπολογιστικής δύναμης, μπορούν να πάρουν τον έλεγχο αυτό του Blockchain. Προφανώς, αυτό προκαλεί ζητήματα ασφάλειας. Εάν κάποιος έχει περισσότερη από 51% υπολογιστική ισχύ, τότε μπορεί να βρει την τιμή της nonce μεταβλητής γρηγορότερα από άλλους [23].

Αυτό θα του έδινε την εξουσία να προχωρήσει σε:

1. Τροποποίηση των δεδομένων συναλλαγής έτσι ώστε να προκαλέσει επίθεση διπλής αποστολής (double spending).
2. Να σταματήσει τη συναλλαγή επαλήθευσης του μπλοκ.
3. Να σταματήσει την εξόρυξη οποιονδήποτε διαθέσιμων μπλοκ.



Εικόνα 1.20: 51% Attack

Μια επίθεση κατά πλειοψηφία ήταν πιο εφικτή στο παρελθόν όταν το ποσοστό hash του δικτύου (hash rate) ήταν πολύ χαμηλότερο και επιρρεπές στην αναδιοργάνωση με την εμφάνιση νέων τεχνολογιών εξόρυξης.

Mining Pools Επιθέσεις

Τα τελευταία χρόνια, οι επιθέσεις που εκμεταλλεύεται τις ευπάθειες των δεξαμενών εξόρυξης αυξάνεται διαρκώς. Ομάδες ανέντιμων ανθρακωρύχων (miners) εκτελούν ένα σύνολο εσωτερικών και εξωτερικών επιθέσεων σε μια "εξορυκτική πισίνα" (mining pool). Οι εσωτερικές επιθέσεις είναι εκείνες στις οποίες οι ανθρακωρύχοι ενεργούν κακόβουλα μέσα στην πισίνα για να αυξήσουν το μερίδιό τους στη συλλογική ανταμοιβή ή να διαταράξουν τη λειτουργικότητα της πισίνας, για να την απομακρύνουν από τις επιτυχείς προσπάθειες εξόρυξης. Αντιθέτως, στις εξωτερικές επιθέσεις, οι ανθρακωρύχοι χρησιμοποιούν την μέγιστη δύναμη κατακερματισμού που διαθέτει ο υπολογιστής ή το υλικό (hardware) τους, για να τρέξει και να λύσει διαφορετικούς αλγόριθμους κατακερματισμού. Με αυτόν τον τρόπο μπορούν να πραγματοποιήσουν επιθέσεις, όπως αυτές των διπλών δαπανών (double spending) [24].

Επίθεση Έκλειψης (Eclipse attack)

Πρόκειται για είδος επίθεσης σε αποκεντρωμένο δίκτυο (decentralized network) μέσω του οποίου ένας εισβολέας προσπαθεί να απομονώσει και να επιτεθεί σε συγκεκριμένους χρήστες, αντί να επιτεθεί σε ολόκληρο το δίκτυο (όπως γίνεται σε μια επίθεση Sybil). Μία επιτυχημένη Eclipse επίθεση επιτρέπει σε έναν εισβολέα να απομονώσει και στη συνέχεια να αποτρέψει το θύμα του να αποκτήσει τρέχουσα εικόνα της πραγματικής δραστηριότητας του δικτύου. Αυτή η επίθεση βρίσκει μεγάλη εφαρμογή, λόγω του ότι ένα αποκεντρωμένο δίκτυο δεν επιτρέπει σε όλους τους κόμβους να συνδέονται ταυτόχρονα με όλους τους άλλους κόμβους του δικτύου. Αντ' αυτού, για αποδοτικότητα, ένας κόμβος συνδέεται με μια επιλεγμένη ομάδα άλλων κόμβων, οι οποίοι με τη σειρά τους συνδέονται με μια δική τους επιλεγμένη ομάδα. Για παράδειγμα, ένας κόμβος Bitcoin έχει οκτώ εξερχόμενες συνδέσεις. Ένας κακόβουλος χρήστης έχει ως στόχο να τροποποιήσει όλες αυτές τις συνδέσεις. Η προσπάθεια που απαιτείται για να επιτευχθεί αυτό ποικίλλει ανάλογα με την κατασκευή, το μέγεθος και τη φύση ενός δικτύου, αλλά γενικά ένας εισβολέας θα πρέπει να ελέγξει ένα botnet των κεντρικών κόμβων (ο καθένας με τη δική του διεύθυνση IP) και να επεξεργαστεί (με την μέθοδο δοκιμής και σφάλματος) τους γειτονικούς κόμβους ενός προοριζόμενου θύματος. Την επόμενη φορά που ο κόμβος του θύματος αποσυνδεθεί και στη συνέχεια ξανασυνδεθεί στο δίκτυο (επαναφορά των συνδέσεών του και εύρεση νέου συνόλου

κόμβων για σύνδεση), ο εισβολέας θα είναι σε θέση να ελέγχει όλες τις συνδέσεις του θύματος [22].

Πώς κερδίζουν οι εισβολείς από μία τέτοια επίθεση

Μόλις ένας εισβολέας απομονώσει έναν χρήστη, λαμβάνοντας τον έλεγχο όλων των εξερχόμενων συνδέσεων, είναι σε θέση να τον εκμεταλλευτεί, για παράδειγμα, πραγματοποιώντας μια επίθεση διπλής δαπάνης μηδενικής επιβεβαίωσης (0-confirmation double spent). Εάν ο Χρήστης Α είναι ο κακόβουλος παράγοντας, ο Χρήστης Β είναι ο απομονωμένος κόμβος και ο Χρήστης Γ είναι μια άλλη οντότητα δικτύου, τότε ο Χρήστης Α θα μπορούσε να στείλει μια πληρωμή στον Χρήστη Γ και στη συνέχεια να στείλει την ίδια συναλλαγή στον Χρήστη Β. Ο Χρήστης Β δεν γνωρίζει ότι αυτά τα χρήματα έχουν ήδη δαπανηθεί καθώς όλες οι εξερχόμενες συνδέσεις τους περνάνε μέσω του Χρήστη Α, ο οποίος είναι σε θέση να καταστείλει και να χειριστεί τις πληροφορίες που λαμβάνει ο Χρήστης Β. Ο Χρήστης Β θα δεχτεί τα νομίσματα και μόνο αργότερα, όταν συνδεθούν με το «αληθινό» Blockchain, θα ανακαλύψει ότι έχει εξαπατηθεί και στην πραγματικότητα δεν έχει λάβει τίποτα.

Παράδειγμα:

Ένας πελάτης πληρώνει μια συναλλαγή σε έναν έμπορο ο οποίος με τη σειρά του απελευθερώνει τα αγαθά στον πελάτη πριν δει την επιβεβαίωση του μπλοκ, δηλαδή, τη συναλλαγή στο Blockchain. Αυτές οι συναλλαγές χρησιμοποιούνται όταν είναι ακατάλληλο να περιμένουμε τα 5-10 λεπτά που συνήθως χρειάζονται για να δούμε την συναλλαγή στο Blockchain, π.χ. σε συστήματα λιανικής πώλησης όπως το BitPay ή σε διαδικτυακούς ιστότοπους τζόγου όπως το Betcoin.

Κλοπή Ταυτότητας

Παρόλο που τα Blockchains διατηρούν την ανωνυμία και το απόρρητο, η ασφάλεια των στοιχείων εξαρτάται από την προστασία του ιδιωτικού κλειδιού του χρήστη. Αν το ιδιωτικό κλειδί κάποιου αποκτηθεί ή κλαπεί, κανένας τρίτος δεν μπορεί να το ανακτήσει.

Κατά συνέπεια, όλα τα περιουσιακά στοιχεία που κατέχει αυτό το άτομο και συνδέονται με το Blockchain θα εξαφανιστούν και θα είναι σχεδόν αδύνατο αναγνωριστεί ο κλέφτης. Πέραν αυτού, οι τρέχουσες τεχνικές κρυπτογραφίας αν και προσφέρουν υψηλά επίπεδα ασφάλειας μπορούν να διαπεραστούν [14]. Με την έλευση του κβαντικού υπολογισμού, δεν είναι αδύνατο να σπάσουν γρήγορα τα κρυπτογραφικά κλειδιά, καταστρέφοντας έτσι τα θεμέλια της τεχνολογία Blockchain [15].

Παραβίαση Συστήματος

Είναι δύσκολο να τροποποιηθούν τα αρχεία που είναι αποθηκευμένα σε Blockchain, αλλά όχι τόσο δύσκολο ο κώδικας των προγραμμάτων των συστημάτων που εφαρμόζουν αυτή την τεχνολογία. Το MtGox, κάποτε το μεγαλύτερο ανταλλακτήριο Bitcoin που έδρευε στο Τόκιο, έπεσε θύμα επίθεσης τον Μάρτιο του 2014 προκαλώντας τη κλοπή Bitcoin αξίας 700 εκατομμυρίων δολαρίων [60]. Οι κακοσυντηρημένοι και ξεπερασμένοι κώδικες επέτρεψαν στους εισβολείς να διπλασιάσουν τις δαπάνες τους. Ένα πιο πρόσφατο περιστατικό έπληξε έναν αποκεντρωμένο αυτόνομο οργανισμό (DAO) που κατέχει μεγάλες ποσότητες Ethereum [61]. Οι χάκερ εκμεταλλεύτηκαν ευπάθειες του λογισμικού κλέβοντας Ethereum αξίας 50 εκατομμυρίων δολαρίων

ΚΕΦΑΛΑΙΟ 2

Αποκεντρωμένες Εφαρμογές

Οι αποκεντρωμένες εφαρμογές (DApps) είναι ψηφιακές εφαρμογές ή προγράμματα που υπάρχουν και εκτελούνται σε δίκτυο υπολογιστών Blockchain ή peer-to-peer (P2P). Αυτές οι εφαρμογές διαδόθηκαν από κατανεμημένες τεχνολογίες καθολικών (Distributed Ledger Technology) όπως το Ethereum Blockchain και δεν εμπίπτουν στο πεδίο αρμοδιοτήτων και ελέγχου μιας μεμονωμένης αρχής. Εξαιτίας αυτού, δεν υπάρχει κάποιος κόμβος στο δίκτυο που να έχει τον πλήρη έλεγχο της εφαρμογής. Σε αντίθεση με τις εφαρμογές ιστού, τα DApps έχουν τα πρωτόκολλα και τα δεδομένα τους κρυπτογραφημένα και ταξινομημένα σε ένα Blockchain. Η πρώτη αποκεντρωμένη εφαρμογή που κυκλοφόρησε στην αγορά και αυτή που άνοιξε το δρόμο για μια επανάσταση αποκέντρωσης είναι, φυσικά, το Bitcoin. [27]

Προκειμένου μια εφαρμογή να χαρακτηριστεί ως αποκεντρωμένη, πρέπει να πληροί τα ακόλουθα κριτήρια: [26][69]

- Η εφαρμογή δεν πρέπει να έχει ελεγκτική οντότητα, πρέπει να λειτουργεί εντελώς αυτόνομα και να είναι εντελώς ανοιχτού κώδικα. Κάθε ενημέρωση της εφαρμογής πρέπει να συμφωνηθεί από το δίκτυο, πρέπει να αποφασιστεί με συναίνεση των χρηστών του.

- Η εφαρμογή πρέπει να λειτουργεί σε Blockchain. Όλα τα δεδομένα και τα αρχεία λειτουργίας της εφαρμογής πρέπει να αποθηκεύονται σε ένα δημόσιο αποκεντρωμένο Blockchain.

- Οι εφαρμογές πρέπει να χρησιμοποιούν ένα κρυπτογραφικό διακριτικό (token), ώστε να επιτρέπει την πρόσβαση στην εφαρμογή και να λειτουργεί ως συστήματα επιβράβευσης για τους ανθρακωρύχους (miners).

- Η εφαρμογή πρέπει να ακολουθεί έναν τυπικό αλγόριθμο κρυπτογράφησης και να δημιουργεί διακριτικά που λειτουργούν ως απόδειξη της αξίας που προσφέρουν οι κόμβοι στην εφαρμογή (π.χ. Αλγόριθμος Proof of Work).

Τύποι Αποκεντρωμένων Εφαρμογών

Υπάρχουν πολλά χαρακτηριστικά σύμφωνα με τα οποία μπορούν να ταξινομηθούν οι αποκεντρωμένες εφαρμογές. Για τους σκοπούς αυτής της διπλωματικής, θα ταξινομήσουμε τα DApps με βάση το εάν έχουν δικό τους Blockchain ή χρησιμοποιούν το Blockchain άλλου DApp. Με βάση αυτό το κριτήριο, υπάρχουν τρεις κύριοι τύποι.

Τύπος 1: Χρηματο*οικονομικές Εφαρμογές (Financial Applications)*

Οι χρήστες μπορούν να συναλλάσσονται μεταξύ τους σε ένα δίκτυο Blockchain, χρησιμοποιώντας το εγγενές νόμισμα του. Αυτές οι εφαρμογές έχουν συνήθως το δικό τους Blockchain και συχνά αποκαλούνται ως κρυπτονομίσματα (όπως το Bitcoin, Litecoin κλπ.). Οποιοδήποτε κρυπτονόμισμα έχει το δικό του Blockchain εμπίπτει σε αυτή την κατηγορία. [26]

Τύπος 2: Ημι-Χρηματο*οικονομικές Εφαρμογές (Semi-Financial Applications)*

Είναι αποκεντρωμένες εφαρμογές που χρησιμοποιούν το Blockchain του τύπου I. Αυτές οι εφαρμογές είναι πρωτόκολλα και διαθέτουν διακριτικά (tokens) απαραίτητα για τη λειτουργία τους. Η λειτουργικότητά τους μπορεί να συγκριθεί με εκείνη ενός προγράμματος λογισμικού γενικής χρήσης, όπως για παράδειγμα ένα υπολογιστικό φύλλο, το οποίο είναι μια εφαρμογή που χρειάζεται το λειτουργικό σύστημα πίσω από αυτό για να λειτουργήσει. [26]

Το πρωτόκολλο Omni είναι το καλύτερο παράδειγμα εφαρμογών τύπου 2. Το Omni είναι μια κατανεμημένη πλατφόρμα συναλλαγών που αναπτύχθηκε στην κορυφή του Blockchain του Bitcoin ως «στρώμα» για τη διευκόλυνση της ανταλλαγής περιουσιακών στοιχείων γρήγορα και χωρίς τη συμμετοχή μεσαζόντων.[29]

Τύπος 3: *Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (Decentralized Autonomous Organizations):*

Ένας Αποκεντρωμένος Αυτόνομος Οργανισμός είναι ένας οργανισμός που κατευθύνεται από κανόνες κωδικοποιημένους σε προγράμματα υπολογιστών που ονομάζονται έξυπνα συμβόλαια (smart contracts) [70]. Η εννοιολογική ουσία ενός

αποκεντρωμένου αυτόνομου οργανισμού έχει χαρακτηριστεί ως η ικανότητα της τεχνολογίας Blockchain να παρέχει ένα ασφαλές ψηφιακό καθολικό που παρακολουθεί τις οικονομικές αλληλεπιδράσεις μέσω του διαδικτύου, χωρίς παραβίαση χάρη στην αξιόπιστη χρονοσήμανση (trusted timestamp) και τη διάδοση μιας κατανεμημένης βάσης δεδομένων. Με απλά λόγια, ένα DAO αναφέρεται σε ένα συγκεκριμένο είδος οργανισμού που σε αντίθεση με τις συμβατικές εταιρείες, βασίζεται σε ανοικτό πηγαίο κώδικα και λειτουργεί εξ ολοκλήρου από την κοινότητά του. Επομένως, η υποκείμενη δομή και οι μηχανισμοί εργασίας ενός DAO δεν βασίζονται σε κανένα είδος ιεραρχικής διαχείρισης (που είναι αρκετά συνηθισμένο στις παραδοσιακές επιχειρήσεις). Αυτή η προσέγγιση εξαλείφει την ανάγκη συμμετοχής ενός αμοιβαία αποδεκτού αξιόπιστου τρίτου μέρους σε μια χρηματοοικονομική συναλλαγή, απλοποιώντας έτσι τη διαδικασία της υλοποίησης των συναλλαγών. [28]

Το δίκτυο SAFE (Secure Access For Everyone) είναι ένα παράδειγμα DApp τύπου 3. Είναι ένα αποκεντρωμένο δίκτυο αποθήκευσης δεδομένων και επικοινωνιών που αντικαθιστά τα κέντρα δεδομένων και τους διακομιστές με τους πρόσθετους υπολογιστικούς πόρους των χρηστών του. Αξιοποιεί το πρωτόκολλο Omni για την έκδοση διακριτικών SafeCoins τα οποία χρησιμοποιούνται για την απόκτηση κατανεμημένου χώρου αποθήκευσης αρχείων. Το δίκτυο SAFE αποτελείται από κόμβους που ονομάζονται Vaults. Συλλογικά, τα Vaults διαχειρίζονται την αποθήκευση όλων των δεδομένων στο δίκτυο διασφαλίζοντας ότι οι ενέργειες που συμβαίνουν σε αυτό είναι έγκυρες. Συγκεντρώνονται σε μικρές ομάδες, καθεμία από τις οποίες έχει την ευθύνη να φροντίζει τα δεδομένα που είναι αποθηκευμένα σε μια ενότητα (ένα συγκεκριμένο εύρος διευθύνσεων). Αυτές οι ομάδες κόμβων σχηματίζονται, συγχωνεύονται και χωρίζονται χωρίς ανθρώπινη επίβλεψη, καθώς το ίδιο το δίκτυο έχει τον πλήρη έλεγχο της διαδικασίας. Με τον ίδιο τρόπο, τα κρυπτογραφημένα κομμάτια δεδομένων κινούνται γύρω από το δίκτυο με έναν πλήρως αυτόνομο τρόπο. Δεν απαιτούνται κεντρικοί διακομιστές ή πράκτορες από το δίκτυο. Καμία κεντρική αρχή δεν επιβλέπει τη διαδικασία. [25][68]

Σύγκριση αποκεντρωμένων εφαρμογών και εφαρμογών ιστού

Προφανώς, κάθε σύστημα έχει κάποια πλεονεκτήματα και μειονεκτήματα. Προκειμένου, αυτά να γίνουν καλύτερα κατανοητά, ακολουθεί μια σύγκριση μεταξύ των αποκεντρωμένων εφαρμογών με τις παραδοσιακές εφαρμογές ιστού. Παρακάτω παρουσιάζονται ορισμένα από τα πλεονεκτήματα και μειονεκτήματα των δύο τύπων εφαρμογών [78][27][31][77].

Τα πλεονεκτήματα που ακολουθούν είναι τα εξής:

Αποκεντρωμένες Εφαρμογές (DApps)

- Αποτρέπουν περιστατικά καθαρής λογοκρισίας καθώς δεν υπάρχει κεντρική αρχή στην οποία μια κυβέρνηση μπορεί να πιέσει για την αφαίρεση κάποιου περιεχόμενου. Προφανώς, μια κυβέρνηση μπορεί να παρακολουθεί τους κόμβους στο δίκτυο από τη διεύθυνση IP τους και να τους κλείσει, αλλά εάν το δίκτυο είναι τεράστιο, τότε καθίσταται αδύνατο να τερματιστεί η εφαρμογή, ειδικά εάν οι κόμβοι κατανέμονται σε διάφορες χώρες.
- Είναι εφαρμογές ανοιχτού κώδικα. Οι προγραμματιστές μπορούν να κάνουν αλλαγές για να φέρουν αξία στην εφαρμογή προς όφελος όλων.
- Όλες οι τροποποιήσεις που εκτελέστηκαν στον κώδικα, καθώς και όλα τα δεδομένα που είναι αποθηκευμένα στο Blockchain, μπορούν να επαληθευτούν εύκολα και με ακρίβεια.
- Δεν μπορούν να «κρασάρουν» εντελώς από τεχνικά σφάλματα. Παραμένουν διαθέσιμα όλη την ώρα λόγω του peer-to-peer δικτύου τους.
- Επειδή χρησιμοποιούνται τεχνολογίες όπως το Blockchain, το Proof-of-Work και τα έξυπνα συμβόλαια καθίστανται αξιόπιστες και αδύνατο να παραβιαστούν από κακόβουλους χρήστες.

Εφαρμογές Ιστού (Web Apps)

- Φιλικά προς το χρήστη.
- Εύκολο να αναπτυχθούν καθώς λειτουργούν σε όλα τα προγράμματα περιήγησης. Είναι διαθέσιμα σε κάθε συσκευή και εύκολα προσβάσιμα.
- Μπορούν να σχεδιαστούν βάση συγκεκριμένων απαιτήσεων που ταιριάζουν με τις ανάγκες και τους στόχους των χρηστών. Αυτό επιτρέπει επίσης στους προγραμματιστές να είναι δημιουργικοί και να προσφέρουν καλύτερα προϊόντα.

Τα μειονεκτήματα που ακολουθούν είναι τα εξής:

Αποκεντρωμένες Εφαρμογές (DApps)

- Τα DApps είναι πολύ αργά και οι συναλλαγές χρειάζονται αρκετό χρόνο. Προς το παρόν, μπορούν να επεξεργαστούν με μια εκτίμηση περίπου 15 συναλλαγές ανά δευτερόλεπτο.
- Το Blockchain καθιστά αδύνατη την κατάργηση ενός DApp από ένα δίκτυο. Ο μόνος τρόπος για να επιτευχθεί αυτό είναι να κλείσει εντελώς το δίκτυο.
- Η επιδιόρθωση σφαλμάτων ή η ενημέρωση είναι δύσκολη, καθώς κάθε κόμβος στο δίκτυο πρέπει να ενημερώσει το λογισμικό του.
- Είναι δύσκολο να υλοποιηθούν επειδή χρησιμοποιούν πολύπλοκα πρωτόκολλα για να επιτύχουν συναίνεση και πρέπει να κατασκευαστούν για να κλιμακωθούν από την αρχή. Επομένως, δεν μπορούμε απλώς να εφαρμόσουμε μια ιδέα και στη συνέχεια να προσθέσουμε περισσότερα χαρακτηριστικά και να την κλιμακώσουμε.
- Ορισμένες εφαρμογές απαιτούν επαλήθευση της ταυτότητας χρήστη (δηλαδή, KYC) και καθώς δεν υπάρχει κεντρική αρχή για την επαλήθευση της ταυτότητας χρήστη, καθίσταται πρόβλημα κατά την ανάπτυξη τέτοιων εφαρμογών.

Εφαρμογές Ιστού (Web Apps)

- Δεν λειτουργούν σε ένα δίκτυο peer-to-peer. Τα δεδομένα αποθηκεύονται σε διακομιστές, δηλαδή κεντρικά σημεία. Ένα κεντρικό σημείο μπορεί να παραβιαστεί ευκολότερα, δημιουργώντας προβλήματα ασφάλειας σε ολόκληρη την εφαρμογή.
- Υψηλότεροι κίνδυνοι ασφάλειας και απορρήτου για τους χρήστες.
- Βασίζονται στο μοντέλο Client–Server. Αυτό σημαίνει ότι όταν ο διακομιστής που φιλοξενείται η εφαρμογή σταματήσει για οποιονδήποτε λόγο την λειτουργία του τότε αυτόματα αυτή καθιστάτε μη διαθέσιμη για χρήση. Αυτό δεν συμβαίνει με τις αποκεντρωμένες εφαρμογές όπου οι πόροι των δικτύων P2P διανέμονται συνήθως σε πολλούς κόμβους του δικτύου.

Δημοφιλής Αποκεντρωμένες Εφαρμογές

Ο κόσμος των αποκεντρωμένων εφαρμογών εξελίσσεται μέρα με τη μέρα, όχι μόνο μεταξύ προγραμματιστών, αλλά και μεταξύ μεγάλων οργανισμών και κυβερνήσεων που έχουν αντιληφθεί τα πλεονεκτήματα της ανάπτυξης τους. Μερικές από τις δημοφιλέστερες αποκεντρωμένες εφαρμογές είναι οι ακόλουθες.

Bitcoin

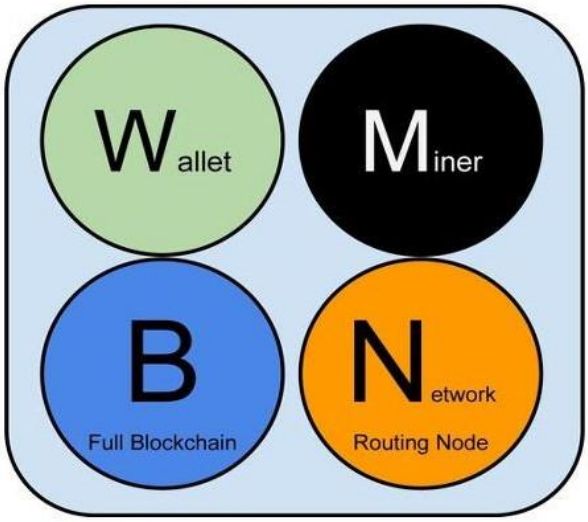
Ο Satoshi Nakamoto δημιούργησε το Bitcoin το 2008 για να διευκολύνει και να μειώσει το κόστος των ποσοστών χρέωσης των συναλλαγών, και έκτοτε αποτελεί το δημοφιλέστερο ψηφιακό νόμισμα. Μέσα σε 10 χρόνια, ως τον Οκτώβριο του 2018 η συνολική αξία του Bitcoin στην αγορά αυξήθηκε από μηδέν σε περισσότερα από 100 δισεκατομμύρια δολάρια [15]. Μεγάλοι κυβερνητικοί ηγέτες και σημαντικά άτομα του χώρου της τεχνολογίας όπως η Janet Yellen και ο Bill Gates, τόνισαν την σημαντικότητα του Bitcoin και γενικότερα της τεχνολογίας του Blockchain για το μέλλον της οικονομίας των Η.Π.Α. Το Bitcoin ως φυσική υπόσταση δεν υπάρχει αποθηκευμένο σε ένα αρχείο στον υπολογιστή. Στην πραγματικότητα είναι μία συλλογή από συναλλαγές ή ακόμα καλύτερα μία συνεχόμενη ομαδοποίηση συνδεδεμένων συναλλαγών που ξεκίνησαν από την αρχή της δημιουργίας του.

Για παράδειγμα, όταν κάποιος χρήστης Α έχει υπό την κατοχή του τρία BTC, αυτό που πραγματικά κατέχει είναι μία διεύθυνση που της ανατέθηκαν το σύνολο των τριών BTC από προηγούμενες συναλλαγές. Μία διεύθυνση στο Bitcoin είναι ένα μοναδικό αναγνωριστικό που βασίζεται στην κρυπτογράφηση δημόσιου κλειδιού. Αυτό που πραγματικά συμβαίνει είναι η δημιουργία ενός ζευγαριού κλειδιών από τον χρήστη του Bitcoin, ένα δημόσιο και ένα ιδιωτικό, χρησιμοποιώντας το δημόσιο ως διεύθυνση. Το ιδιωτικό κλειδί διατηρείται μυστικό και είναι το αποδεικτικό ως προς τους άλλους χρήστες Bitcoin ότι η διεύθυνση αυτή που χρησιμοποιήθηκε ανήκει πραγματικά στον ίδιο χρήστη [15]. Ο λογαριασμός ενός χρήστη μπορεί να αποτελείται από πολλές διαφορετικές διευθύνσεις, δυνατός είναι και ο συνδυασμός μεταξύ τους αν χρειαστεί, με σκοπό την επίτευξη μιας συναλλαγής. Για παράδειγμα, αν η διεύθυνση Α έχει 1 BTC και η διεύθυνση Β έχει 2 BTC, ο χρήστης μπορεί να συνδυάσει αυτές τις δύο διευθύνσεις μεταξύ τους για να πραγματοποιήσει μία συναλλαγή που απαιτεί 3 BTC. Από την στιγμή που οι χρήστες χρησιμοποιούν μόνο διευθύνσεις για τις συναλλαγές, το Bitcoin θεωρείται ότι είναι ανώνυμο, πράγμα που δεν αληθεύει εντελώς. Η διεύθυνση που χρησιμοποιείτε δεν συνδέεται με την πραγματική ταυτότητα του χρήστη, ωστόσο αν κάποιος θέλει να ανακαλύψει την ταυτότητα του μπορεί να το κάνει μέσω άλλων ενεργειών του χρήστη. Το υπόλοιπο, σε χρηματικό ποσό, κάθε διεύθυνσης μπορεί να επιβεβαιωθεί από οποιονδήποτε μέσα στο δίκτυο του Bitcoin, από τη στιγμή που όλοι οι χρήστες έχουν πρόσβαση στο συνολικό ιστορικό συναλλαγών του Blockchain, στο οποίο καταγράφονται όλες οι συναλλαγές που πραγματοποιούνται με Bitcoin [15].

Αρχιτεκτονική Δικτύου Bitcoin

Από πλευράς αρχιτεκτονικής το Bitcoin είναι ένα peer-to-peer δομημένο δίκτυο πάνω από το Internet. Με τον όρο peer-to-peer (P2P) εννοούμε ότι όλοι οι υπολογιστές που είναι μέρος του δικτύου είναι όλοι ομότιμοι και ίσοι μεταξύ τους. Όλοι οι κόμβοι του δικτύου μοιράζονται το βάρος, παρέχοντας τον ίδιο αριθμό υπηρεσιών σε αυτό. Η διασύνδεση τους στο δίκτυο γίνεται με την μορφή πλέγματος (Mesh Network), με επίπεδη τοπολογία [32]. Δεν υπάρχει κανένας εξυπηρετητής (server), ούτε κάποια κεντρικά σχεδιασμένη υπηρεσία και γενικώς καμιά ιεραρχία μέσα στο δίκτυο. Οι κόμβοι ενός peer-to-peer δικτύου παρέχουν και καταναλώνουν υπηρεσίες την ίδια στιγμή. Εκ φύσεως τα peer-to-peer δίκτυα είναι αποκεντρωμένα, ανθεκτικά και

ανοικτά. Χαρακτηριστικό παράδειγμα μιας peer-to-peer αρχιτεκτονικής δικτύου ήταν το διαδίκτυο, όταν βρίσκονταν στην πρώιμη του κατάσταση, καθώς όλοι οι κόμβοι στο IP δίκτυο ήταν ισότιμοι μεταξύ τους. Ωστόσο, αν και η τωρινή αρχιτεκτονική του διαδικτύου διατηρεί μία πιο ιεραρχική μορφή σε σχέση με το παρελθόν, το πρωτόκολλο του διαδικτύου συνεχίζει να διατηρεί την επίπεδη τοπολογία. Με βάση την λειτουργικότητα που υποστηρίζουν οι κόμβοι του P2P Bitcoin δικτύου, μπορούν να αναλάβουν διαφορετικούς ρόλους [7]. Ένας κόμβος Bitcoin είναι ένα σύνολο από επιμέρους λειτουργίες που σχετίζονται με την δρομολόγηση, την βάση δεδομένων Blockchain, την εξόρυξη και διάφορες υπηρεσίες πορτοφολιού. Η λειτουργία της δρομολόγησης περιλαμβάνεται σε όλους τους κόμβους, προκειμένου να συμμετέχουν στο δίκτυο, ωστόσο μπορεί να περιλαμβάνουν παράλληλα και κάποια άλλη λειτουργία. Όλοι οι κόμβοι ανακαλύπτουν και διατηρούν συνδέσεις με ομότιμους (peer) κόμβους ενώ ταυτόχρονα είναι σε θέση να εγκρίνουν και να διαδίδουν μπλοκ και συναλλαγές.



Εικόνα 2.1: Ένας κόμβος του δικτύου Bitcoin με όλες τις διαθέσιμες βασικές λειτουργίες.

Επιπλέον των προαναφερθέντων λειτουργιών, υπάρχουν και κόμβοι οι οποίοι μπορούν να διατηρούν ένα ολόκληρο και συνεχώς ενημερωμένο αντίγραφο του Blockchain. Αυτοί οι κόμβοι ονομάζονται “πλήρης” (full nodes) και μπορούν να επαληθεύουν αυτόνομα οποιαδήποτε συναλλαγή. Από την άλλη πλευρά, υπάρχουν και κόμβοι οι οποίοι διατηρούν μόνο ένα υποσύνολο του Blockchain και εγκρίνουν συναλλαγές μέσω μίας μεθόδου απλοποιημένης επαλήθευσης πληρωμών (Simplified Payment Verification - SPV) [32]. Η συγκεκριμένη μέθοδος βρίσκει χρήση στα mobile wallets καθώς τα κινητά τηλέφωνα δεν μπορούν να κατεβάσουν ολόκληρη την αλυσίδα των

μπλοκ. Οι κόμβοι αυτοί είναι γνωστοί ως “SPV κόμβοι” ή “ lightweight κόμβοι”. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι κόμβοι εξόρυξης οι οποίοι ανταγωνίζονται μεταξύ τους για τη δημιουργία νέων block. Για να το επιτύχουν αυτό, τρέχουν εξειδικευμένο υλικό που επιλύει τον αλγόριθμο της απόδειξης εργασίας (proof-of-work). Υπάρχουν κόμβοι εξόρυξης που είναι ταυτόχρονα και πλήρεις κόμβοι, καθώς διατηρούν ένα πλήρες αντίγραφο της Blockchain, ενώ άλλοι που είναι lightweight κόμβοι καθώς συμμετέχουν σε ομάδα εξόρυξης (mining pool). Τα wallet τα οποία είναι σχεδιασμένα να τρέχουν σε συσκευές με πρόσβαση σε περιορισμένους πόρους όπως είναι τα κινητά τηλέφωνα, είναι SPV κόμβοι [32]. Τέλος, εκτός των κύριων τύπων κόμβων του Bitcoin πρωτοκόλλου, υπάρχουν εξυπηρετητές και κόμβοι που χρησιμοποιούν πρωτόκολλα, όπως πρωτόκολλα πρόσβασης για lightweight πελάτες και συγκεκριμένα πρωτόκολλα ομάδων εξόρυξης (mining).

Ethereum

Το Ethereum είναι μια ανοιχτού τύπου, αποκεντρωμένη πλατφόρμα Blockchain με υπολογιστικές δυνατότητες που ξεπερνάνε τις στοιχειώδεις ανταλλαγές νομισμάτων, προσφέροντας λειτουργίες έξυπνων συμβολαίων. Η πλατφόρμα Ethereum επιτρέπει στους προγραμματιστές να δημιουργούν ισχυρές αποκεντρωμένες εφαρμογές με ενσωματωμένες οικονομικές λειτουργίες [31]. Το Ethereum αναγνωρίζεται ευρέως ως διάδοχος του πρωτοκόλλου Bitcoin, γενικεύοντας τις αρχικές ιδέες και επιτρέποντας τη δημιουργία μιας πιο ποικιλόμορφης σειράς εφαρμογών πάνω από την τεχνολογία Blockchain. Το Ethereum έχει δύο βασικά συστατικά. Το πρώτο είναι μια εικονική μηχανή που μπορεί να φορτώσει πόρους και να εκτελέσει σενάρια, που ονομάζεται Ethereum Virtual Machine (EVM). Το δεύτερο συστατικό είναι ένα διακριτικό που ονομάζεται Ether, και αποτελεί το νόμισμα του δικτύου που χρησιμοποιείται για συναλλαγές από χρήστη σε χρήστη ή αποζημιώσεις σε ανθρακωρύχους του δικτύου. Στο πρωτόκολλο Bitcoin, οι διευθύνσεις χαρτογραφούν τις συναλλαγές από τον αποστολέα στον παραλήπτη. Το μόνο πρόγραμμα που τρέχει στο Blockchain είναι το πρόγραμμα μεταφοράς. Το Ethereum γενικεύει αυτήν την ιδέα τοποθετώντας μία εικονική μηχανή (EVM) σε κάθε κόμβο έτσι ώστε να μπορεί να εκτελεστεί επαληθεύσιμος κώδικας στο Blockchain [31]. Ο σκοπός του Ethereum δεν είναι πρωτίστως να είναι ένα δίκτυο πληρωμών για ένα ψηφιακό νόμισμα, παρόλο που το ψηφιακό νόμισμα του Ether είναι αναπόσπαστο και απαραίτητο για τη λειτουργία του.

Σε αντίθεση με το Bitcoin, το οποίο έχει μια πολύ περιορισμένη γλώσσα σεναρίων, το Ethereum έχει σχεδιαστεί για να είναι ένα προγραμματιζόμενο Blockchain γενικής χρήσης που χρησιμοποιεί μια εικονική μηχανή για να εκτελεί κώδικα αυθαίρετης και απεριόριστης πολυπλοκότητας.

Namecoin

Το Namecoin ήταν το πρώτο fork (διακλάδωση αλυσίδας) του Bitcoin και ήταν το πρώτο που εφάρμοσε τη συγχωνευμένη εξόρυξη και ένα αποκεντρωμένο DNS. Επιλύει το πρόβλημα του τριγώνου του Zooko, δημιουργώντας έτσι ένα σύστημα ονομάτων τομέων (DNS) που είναι ταυτόχρονα ασφαλές και αποκεντρωμένο. Βασίζεται στην ίδια τεχνολογία με το Bitcoin με μικρές τροποποιήσεις και χρησιμοποιεί τον ίδιο αλγόριθμο κατακερματισμού SHA-256, αλλά διαθέτει δικό του λογισμικό Blockchain. Η αρχική ιδέα για το Namecoin ήταν να χρησιμοποιηθεί ως αποκεντρωμένο σύστημα DNS που θα χρησιμοποιεί απευθείας τη βάση δεδομένων του Bitcoin. Ωστόσο, στη πορεία προβλέποντας τις δυσκολίες κλιμάκωσης, αποφασίστηκε να δημιουργηθεί ένα νέο ψηφιακό νόμισμα ξεχωριστό από το Bitcoin εντελώς, στο οποίο οι ανθρακωρύχοι Bitcoin μπορούν να συμβάλλουν στην διατήρηση της ασφάλειά του χωρίς να χρειάζεται να αφιερώσουν επιπλέον πόρους. Σε αντίθεση με το Bitcoin, το Namecoin μπορεί να αποθηκεύει δεδομένα μέσα στο δικό του Blockchain. Η ιδέα του δεν βασίζεται στο να παρέχει ένα altcoin αλλά να παρέχει βελτιωμένη αποκέντρωση, απόρρητο, ασφάλεια και ταχύτητα. [71]

Litecoin

Το Litecoin ένα κατανεμημένο ηλεκτρονικό νόμισμα ανοιχτού κώδικα που δημοσιεύεται υπό την άδεια του MIT. Είναι εμπνευσμένο και πρακτικά πανομοιότυπο στην τεχνική του πτυχή με το Bitcoin (BTC). Το 2020, το δίκτυο του Litecoin είχε περισσότερους από 1.400 κόμβους. Καθένα από αυτά περιέχει ένα αντίγραφο όλων των δεδομένων συναλλαγών. Αυτό σημαίνει ότι τα δεδομένα δεν ελέγχονται από μία οντότητα, αλλά από ένα αποκεντρωμένο δίκτυο. Η δημιουργία και η μεταφορά του βασίζεται σε ένα κρυπτογραφικό πρωτόκολλο που δεν διαχειρίζεται καμία κεντρική αρχή και υποστηρίζεται από τη συναίνεση ενός δικτύου peer-to-peer. Το Litecoin θεωρήθηκε ως εναλλακτική λύση έναντι του Bitcoin για μεταφορές χαμηλής αξίας. Κάθε litecoin διαιρείται σε 100.000.000 μικρότερες μονάδες, που ορίζονται με οκτώ

δεκαδικά ψηφία. Παρόλο που είναι σχεδόν πανομοιότυπο με το Bitcoin (BTC) για τις τεχνικές πτυχές, το δίκτυο του Litecoin διαφέρει από αυτό σε ορισμένα σημεία όπως: [72][73]

Ταχύτητα συναλλαγής

- Το Bitcoin μπορεί να πραγματοποιήσει 4-7 συναλλαγές ανά δευτερόλεπτο, με χρόνο επιβεβαίωσης συναλλαγής 10 λεπτά. Το Litecoin μπορεί να πραγματοποιήσει 56 συναλλαγές ανά δευτερόλεπτο, με χρόνο επιβεβαίωσης συναλλαγής 2,5 λεπτών. Ωστόσο, εταιρείες πιστωτικών καρτών όπως η Visa μπορούν να χειριστούν έως και 4.000 συναλλαγές ανά δευτερόλεπτο.

Κεφαλαιοποίηση αγοράς

- Η συνολική αξία του Bitcoin στην αγορά ανέρχεται σε πάνω από στα 150 δισεκατομμύρια δολάρια, κατέχοντας την πρώτη θέση στον πίνακα κεφαλαιοποίησης της αγοράς. Το Litecoin βρίσκεται στην έκτη θέση, με την συνολική του αξία να φτάνει τα 3 δισεκατομμύρια δολάρια.

Αποδοχή νομισμάτων

- Το Bitcoin είναι αρκετά ευρέως αποδεκτό ως νόμισμα. Υπάρχει αυξανόμενος αριθμός λιανοπωλητών που επιτρέπει στους χρήστες τους χρησιμοποιούν Bitcoin απευθείας. Εταιρίες όπως η Microsoft, Expedia, PayPal, KFC και Subway, Virgin Galactic, AT&T, Amazon και Starbucks είναι μερικά από τα μεγάλα ονόματα που δέχονται πληρωμές σε Bitcoin. Το Litecoin αντιθέτως καθιστάτε δυνητικά πιο ελκυστικό για μικρότερες αγορές, με την λίστα των πωλητών λιανικής που το αποδέχονται να αυξάνεται γρήγορα.

Ανταμοιβή Εξόρυξης

- Επί του παρόντος, ένας ανθρακωρύχος κερδίζει 12,5 BTC για την ολοκλήρωση ενός μπλοκ - περίπου 300.000 δολάρια. Στον αντίποδα, ένας ανθρακωρύχος μπορεί επί του παρόντος να κερδίσει 12,5 Litecoin για την ολοκλήρωση ενός μπλοκ, περίπου 590,63 δολάρια.

- Χρησιμοποιεί τη λειτουργία scrypt στον αλγόριθμο Proof of Work καθιστώντας την εξόρυξη ευκολότερη, καθώς δεν απαιτεί εξελιγμένο εξοπλισμό όπως στην περίπτωση του Bitcoin.

Cardano (Ada)

Το Cardano είναι μία αποκεντρωμένη πλατφόρμα δημόσιου Blockchain με λειτουργικότητα ανοικτού κώδικα και έξυπνη σύμβασης (smart contracts). Επιδιώκει να εκτελεί οικονομικές εφαρμογές και να παρέχει στους χρήστες μεγαλύτερη ευελιξία από άλλα πρωτόκολλα Blockchain, μέσω μιας αρχιτεκτονικής με στρώσεις (layers). Το Cardano χρησιμεύει ως βάση για το κρυπτονόμισμα Ada, το οποίο τον Απρίλιο του 2018 ήταν το έβδομο πιο ισχυρό κρυπτονόμισμα από την άποψη της κεφαλαιοποίησης της αγοράς, με αξία 7.188.617.359 δολαρίων ΗΠΑ, με κόστος 0.27 δολάρια στις 26 Απριλίου. Την ίδια ημέρα υπήρχαν 25.927.070.538 ADA σε κυκλοφορία. Το έργο ξεκίνησε τον Σεπτέμβριο του 2017 από την εταιρεία Input Output Hong Kong (IOHK). Η ιεραρχική δομή του Cardano διασφαλίζει ότι μπορεί να χρησιμοποιηθεί ως μέσο ανταλλαγής καθώς και ως μέσο δημιουργίας έξυπνων συμβάσεων. Επιπλέον, η πλατφόρμα έχει φιλοδοξίες να είναι διαλειτουργική με το γενικό οικοσύστημα χρηματοδότησης. [76]

Η πλατφόρμα του Cardano αποτελείται από δύο επίπεδα. [20]

1. Το Cardano Settlement Layer (CSL) χρησιμοποιείται για τον διακανονισμό συναλλαγών που χρησιμοποιούν ADA. Ο διακανονισμός επιτρέπει στους χρήστες να ανταλλάσσουν νομίσματα ADA μεταξύ τους, λειτουργώντας με τρόπο παρόμοιο αυτού του Ethereum.
2. Το Cardano Control Layer (CCL) το οποίο είναι υπό ανάπτυξη, θα χρησιμοποιηθεί για έξυπνες συμβάσεις (smart contracts). Μέσω αυτής της λειτουργίας οι χρήστες θα μπορούν τόσο να δημιουργούν όσο και να υπογράφουν έξυπνα συμβόλαια.

Το Ada μπορεί να αποθηκευτεί στον Daedalus, το επίσημο πορτοφόλι της Cardano. Είναι διαθέσιμο για Windows, Mac και προγραμματισμένη έκδοση Linux. Το Daedalus επιτρέπει επίσης την αποθήκευση Bitcoin και Ethereum Classic. [75] Από τα τέλη Φεβρουαρίου, το Ada μπορεί επίσης να αποθηκευτεί στο πορτοφόλι Centra, ένα πορτοφόλι κρυπτογράφησης με μια συσχετισμένη χρεωστική κάρτα multi-Blockchain,

διαθέσιμη για iOS και Windows. Αυτό σημαίνει ότι μπορεί να χρησιμοποιηθεί τώρα με την κάρτα Centra που είχε πρόσβαση σε 36 εκατομμύρια τερματικά σε όλο τον κόσμο. [74]

Ωστόσο, αν και το ADA έχει ανοίξει τον δρόμο για το Blockchain 3.0 έχει ένα μεγάλο μειονέκτημα και αυτό είναι ότι δεν υπάρχουν ακόμη πολλές δυνατότητες, Υπάρχουν πολλά σχέδια για μελλοντικές λειτουργίες, αλλά όλα αυτά δεν έχουν ακόμη εφαρμοστεί, και αυτό οφείλεται στο γεγονός ότι το Blockchain του εξακολουθεί ακόμα να αναπτύσσεται. Άλλα Blockchains, όπως το Ripple, το Stellar Lumens και το NEO είναι ήδη σε θέση να επεξεργαστούν περισσότερες από 1.000 συναλλαγές ανά δευτερόλεπτο, σε αντίθεση με το ADA όπου η μέγιστη επεκτασιμότητα του αυτή τη στιγμή είναι μόνο 257 συναλλαγές ανά δευτερόλεπτο.

Αλγόριθμος Ouroboros

Η καρδιά της πλατφόρμας του Cardano είναι το Ouroboros, ένας αλγόριθμος που χρησιμοποιεί το πρωτόκολλο Proof of Stake για την εξόρυξη νομισμάτων. Ο αλγόριθμος έχει προσαρμοστεί για να μειώσει τη χρήση ενέργειας και το χρόνο δημιουργίας νέων νομισμάτων. Σε έναν τυπικό αλγόριθμο Proof of Stake, οι κόμβοι με το μέγιστο ποντάρισμα (ή τον μεγαλύτερο αριθμό νομισμάτων) δημιουργούν μπλοκ συναλλαγών σε ένα Blockchain. Ωστόσο, ο αλγόριθμος Ouroboros εφαρμόζει τον αλγόριθμο διαφορετικά.

Το Ouroboros συνδυάζει μοναδική τεχνολογία και μαθηματικά επαληθευμένους μηχανισμούς οι οποίοι, με τη σειρά τους, συνδυάζουν συμπεριφορική ψυχολογία και οικονομική φιλοσοφία για να διασφαλίσουν την ασφάλεια και τη βιωσιμότητα των Blockchain που εξαρτώνται από αυτόν. Αποτελεί, κρίσιμο μέρος της υποδομής του κρυπτονομίσματος ADA και γενικότερα σημαντική καινοτομία στην τεχνολογία Blockchain. Έχει αποδειχθεί μαθηματικά ότι είναι αποδεδειγμένα ασφαλές και ο πρώτος που έχει περάσει από ομότιμους κριτικούς μέσω της αποδοχής του στο Crypto 2017, το κορυφαίο συνέδριο κρυπτογράφησης. Το επίπεδο ασφάλειας που επιδεικνύει ο Ouroboros συγκρίνεται με αυτό του Blockchain του Bitcoin, το οποίο δεν έχει ποτέ παραβιαστεί. Το αποτέλεσμα είναι ένα πρωτόκολλο με αποδεδειγμένες εγγυήσεις ασφάλειας ικανές να διευκολύνουν τη διάδοση παγκόσμιων συναλλαγών με ελάχιστες ενεργειακές απαιτήσεις.[30]

Κρυπτονομίσματα και Κοινωνικά Δίκτυα: Facebook Libra

Το Facebook προσπάθησε να μπει στην αγορά των διαδικτυακών πληρωμών μέσω της εφαρμογής WhatsApp Pay το 2018 αφού είδε την τεράστια επιτυχία του Κινέζου ομολόγου του, WeChat. Περίπου το 90% των πληρωμών από Κινέζους που ζουν σε μεγάλες πόλεις χρησιμοποιούν είτε τον τρόπο πληρωμής του WeChat για κινητά είτε το Alipay (Mansoor, 2020). Ωστόσο, η εφαρμογή WhatsApp Pay δεν απογειώθηκε όπως αναμενόταν και η χρήση των πληρωμών μέσω κινητού σε πολλές δυτικές χώρες εξακολουθεί να υστερεί σε σχέση με την Κίνα και άλλες ασιατικές χώρες.

Παρόλο που η προσπάθεια του WhatsApp Pay δεν ανταποκρίθηκε στην αναμενόμενη επιτυχία, το Facebook επέστρεψε το 2019 με το Libra, που πλέον ονομάζεται Diem. Με βάση σχεδόν 3 δισεκατομμυρίων χρηστών (π.χ. Messenger, WhatsApp, Instagram και Facebook), το Facebook Libra προβλέπεται να κυριαρχεί στις καθημερινές συναλλαγές αγαθών / υπηρεσιών και μεταφοράς χρημάτων στο διαδίκτυο. Το Facebook στοχεύει να αξιοποιήσει περίπου 1,7 δισεκατομμύρια ενήλικες χωρίς τραπεζικούς λογαριασμούς. Σύμφωνα με την έρευνα FDIC του 2018, 8,4 εκατομμύρια νοικοκυριά (δηλαδή 48,9 εκατομμύρια ενήλικες και 15,4 εκατομμύρια παιδιά) στις Ηνωμένες Πολιτείες δεν είχαν κανένα τραπεζικό λογαριασμό το 2017.

Σύμφωνα με το White Paper του Libra (2019), το Libra θεωρείται ως ένα παγκόσμιο νόμισμα και μια χρηματοοικονομική υποδομή που αποτελείται από τρία μέρη.

- Πρώτον, το Libra είναι ένα ψηφιακό νόμισμα που βασίζεται στη τεχνολογία Blockchain.
- Δεύτερον, θα υποστηρίζεται από ένα αποθεματικό κεφάλαιο που έχει σχεδιαστεί για να διατηρεί την αξία του σταθερή, καταστώντας το ως ένα stable coin στην αγορά των ψηφιακών νομισμάτων.
- Τρίτον, θα διαχειρίζεται από έναν ανεξάρτητο οργανισμό (Libra Association) στον οποίο έχει ανατεθεί η ανάπτυξη του οικοσυστήματος του νομίσματος.

Παρόλο που η ομάδα του Facebook έπαιξε βασικό ρόλο στη δημιουργία αυτού του οργανισμού καθώς και του Libra Blockchain, δεν έχει κάποια ειδικά δικαιώματα εντός του οργανισμού.

Τα ιδρυτικά μέλη του οργανισμού απαρτίζουν 28 από τις μεγαλύτερες εταιρίες παγκοσμίως και στόχος τους είναι να φτάσουν τα 100 μέλη μέσα στα επόμενα χρόνια.

Εικόνα 2.2: Μέλη-Εταιρίες του Libra association

Το σύστημα πληρωμών του Libra είναι χτισμένο στο Libra Blockchain. Επειδή προορίζεται για ένα παγκόσμιου κοινό, το λογισμικό που εφαρμόζει το Libra Blockchain είναι ανοιχτού κώδικα - σχεδιασμένο έτσι ώστε ο καθένας να μπορεί να χτίσει πάνω του εφαρμογές, και δισεκατομμύρια άνθρωποι να μπορούν να το χρησιμοποιούν για τις οικονομικές τους ανάγκες. Πρόκειται ουσιαστικά για ένα ανοιχτό, διαλειτουργικό σύστημα πληρωμών που έχει δημιουργηθεί από προγραμματιστές και οργανισμούς για να βοηθήσουν τα άτομα και τις επιχειρήσεις να κρατήσουν και να μεταφέρουν τα νομίσματα Libra για καθημερινή χρήση. Ο στόχος του Libra Blockchain είναι να χρησιμεύσει ως βάση για χρηματοοικονομικές υπηρεσίες, συμπεριλαμβανομένου ενός νέου παγκόσμιου συστήματος πληρωμών που καλύπτει τις καθημερινές οικονομικές ανάγκες δισεκατομμυρίων ανθρώπων.

Το γεγονός ότι το Libra χρησιμοποιεί Blockchain ήταν ο λόγος που χαρακτηρίστηκε ως κρυπτονόμισμα ωστόσο είναι αρκετοί αυτοί που διαφωνούν. Αυτό οφείλεται στο λόγο ότι το σύστημα δεν είναι αποκεντρωμένο όπως γίνεται με τα κρυπτονομίσματα αλλά βασίζεται στη διακυβέρνηση ενός αξιόπιστου τρίτου μέρους (Libra Association), θεωρώντας το έτσι περισσότερο ως ψηφιακό νόμισμα παρά ως κρυπτονόμισμα.

Με την ραγδαία ανάπτυξη των smartphone και των ασύρματων δικτύων, είναι δεδομένο ότι όλο και περισσότεροι άνθρωποι θα συνδέονται στο διαδίκτυο και θα έχουν πρόσβαση και θα χρησιμοποιούν το σύστημα πληρωμών Libra. Για να επιτύχει το δίκτυο Libra αυτό το όραμα με την πάροδο του χρόνου, το Blockchain του έχει κατασκευαστεί δίνοντας προτεραιότητα στην επεκτασιμότητα, την ασφάλεια, την αποδοτικότητα στην αποθήκευση δεδομένων, καθώς και τη μελλοντική προσαρμοστικότητα.

Ενώ το White Paper του Libra και άλλες πληροφορίες που έχουν κυκλοφορήσει μέχρι στιγμής δεν παρέχουν αρκετές λεπτομέρειες σχετικά με όλες οι πτυχές της τελικής εφαρμογής, μερικά χαρακτηριστικά του προτεινόμενου νομίσματος και του οικοσυστήματος του θυμίζουν λειτουργίες υπαρχόντων ιδρυμάτων όπως τα διαπραγματεύσιμα αμοιβαία κεφάλαια (Exchange Traded Funds - ETF) και τα ειδικά τραβηκτικά δικαιώματα (Special Drawing Rights - SDRs) του Διεθνές Νομισματικού Ταμείου (IMF).

Ένα σημείο που αξίζει να αναφερθεί είναι πως το Libra δεν έχει ολοκληρωθεί ακόμη και δεν είναι έτοιμο. Όπως ανακοινώθηκε, η πρώτη έκδοση του αναμένεται να κυκλοφορήσει μέσα στο 2021, ωστόσο δεν έχει διευκρινιστεί ακόμα τι θα είναι ακριβώς το Libra και πως θα λειτουργεί. Από το white paper βγαίνει το συμπέρασμα ότι θα πρόκειται για ένα σύστημα πληρωμών που θα βασίζεται σε αμερικανικά ομόλογα και θα έχει ως βάση νομίσματα όπως το δολάριο ΗΠΑ, λίρα Βρετανίας, Ευρώ και γιέν Ιαπωνίας.

ΚΕΦΑΛΑΙΟ 3

Συναλλαγές

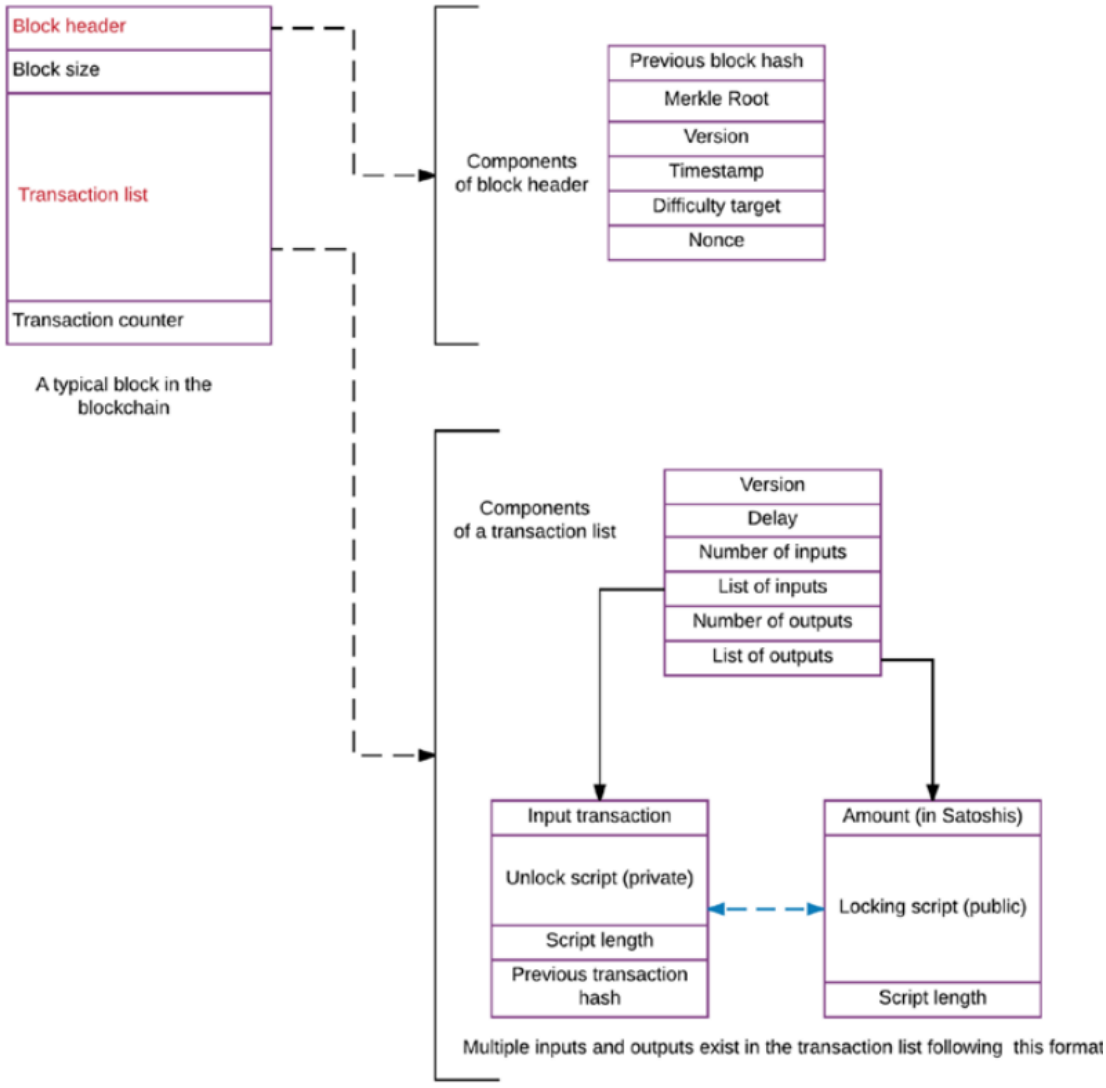
Μια συναλλαγή είναι μια δομή δεδομένων που κωδικοποιεί μια μεταφορά νομισμάτων από μια πηγή κεφαλαίων, που ονομάζεται είσοδος, σε έναν προορισμό που ονομάζεται έξοδος. Οι συναλλαγές μέσω της Blockchain τεχνολογίας επιτρέπουν τη μεταφορά κρυπτονομισμάτων όπως το Bitcoin και το Ethereum από ένα άτομο ή επιχείρηση σε άλλο χωρίς μεσάζοντα όπως μία τράπεζα. Αυτές οι συναλλαγές πραγματοποιούνται σε πραγματικό χρόνο σε αποκεντρωμένο δίκτυο για να διασφαλιστεί η ασφάλεια και η αξιοπιστία ολόκληρου του συστήματος. Μια συναλλαγή είναι ουσιαστικά μια δομή δεδομένων που μεταφέρεται και υπάρχει μέσα σε ένα μπλοκ [35].

Μπλοκ

Τα μπλοκ είναι το κύριο μέρος του Blockchain και αποτελούν το μέρος που αποθηκεύονται όλες οι συναλλαγές. Πρόκειται ουσιαστικά για αρχεία όπου καταγράφονται μόνιμα δεδομένα που σχετίζονται με το δίκτυο. Κάθε μπλοκ μπορεί να θεωρηθεί ως σελίδα στο καθολικό. Το δίκτυο Blockchain αποτελείται από εκατομμύρια μπλοκ που βρίσκονται σε συνεχή κατάσταση ροής. Ένα μπλοκ είναι επομένως μια μόνιμη αποθήκευση αρχείων που, μόλις γράφονται, δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν [7].

Κάθε μπλοκ έχει τουλάχιστον δύο μοναδικά στοιχεία. Το πρώτο είναι η κεφαλίδα του μπλοκ (block header), η οποία περιέχει ένα μοναδικό κατακερματισμό που ονομάζεται ρίζα merkle και προσδιορίζει μοναδικά το μπλοκ. Το δεύτερο είναι η λίστα συναλλαγών (transaction list) η οποία περιέχει νέες συναλλαγές. Σε αυτό το απλοποιημένο μοντέλο, υπάρχουν δύο επιπλέον στοιχεία ενός μπλοκ: το μέγεθος του μπλοκ (block size), το οποίο διατηρείται συνεπή για ολόκληρο το δίκτυο και τέλος ένας μετρητής (transaction counter) που χρησιμοποιείται για να μετράει τον αριθμό των συναλλαγών σε κάθε μπλοκ [35].

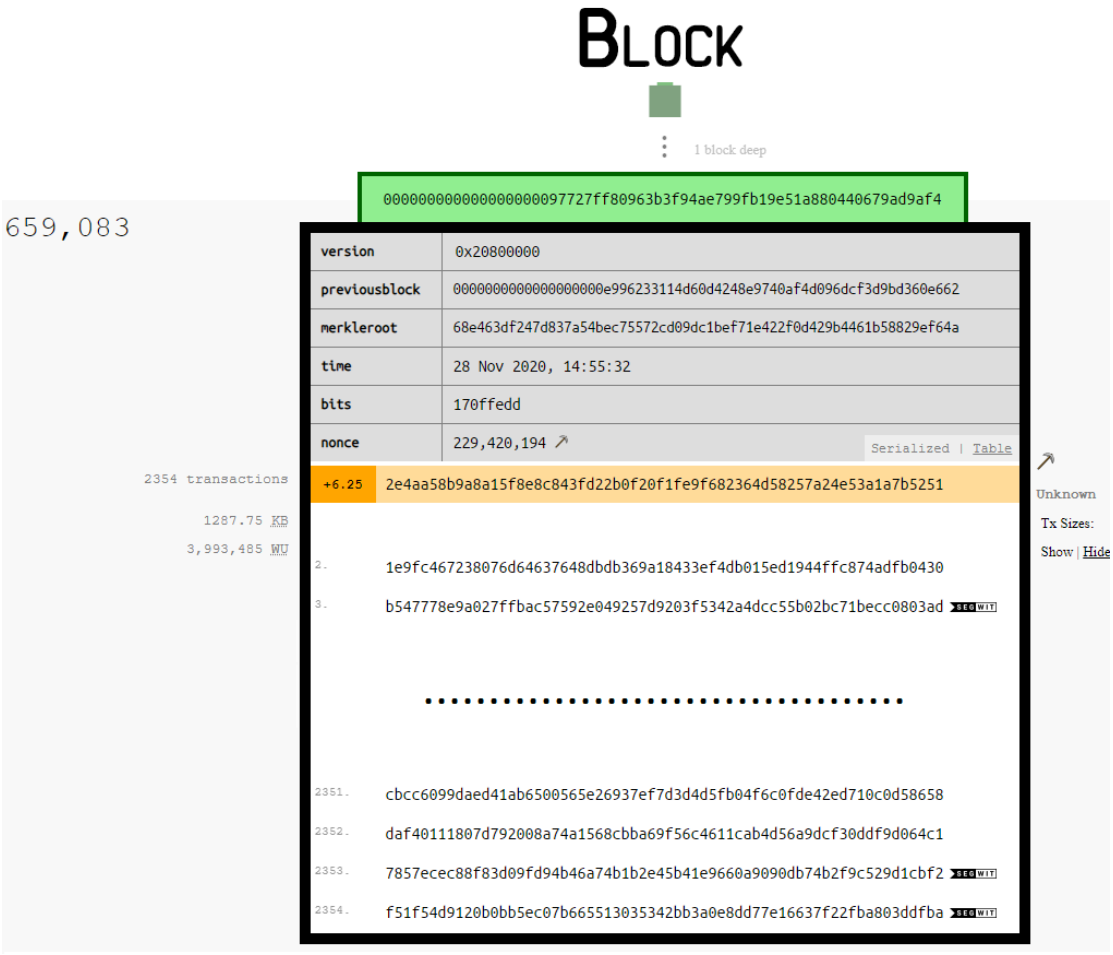
Η κεφαλίδα του μπλοκ περιέχει μερικά τυπικά στοιχεία, όπως ο στόχος δυσκολίας και το nonce. Περιέχει επίσης την χρονική σήμανση (timestamp) που είναι ένα μοναδικό χαρακτηριστικό κάθε μπλοκ, καθώς αναγνωρίζει αναμφίβολα ένα συγκεκριμένο μπλοκ στο δίκτυο. Ακόμη, διαθέτει έναν κατακερματισμό από το προηγούμενο μπλοκ της αλυσίδας, και τον ειδικό κατακερματισμό που προσδιορίζει αυτό το μπλοκ, που ονομάζεται ρίζα merkle [35].



Εικόνα 3.1: Πλήρης δομή ενός μπλοκ [35]

Κάθε μπλοκ περιέχει επίσης μια λίστα συναλλαγών. Εκτός από τις πραγματικές συναλλαγές, η λίστα συναλλαγών περιέχει επίσης μερικά στοιχεία που είναι ζωτικής σημασίας για το πώς ένα μπλοκ θα δεχτεί μια συναλλαγή.

Για παράδειγμα, η καθυστέρηση χρόνου κλειδώματος (delay) υπαγορεύει πότε μια συναλλαγή μπορεί να γίνει αποδεκτή σε ένα μπλοκ. Ουσιαστικά, αναφέρεται στον χρόνο μετά τον οποίο μια συναλλαγή μπορεί να γίνει δεκτή σε ένα μπλοκ. Τέλος, η λίστα περιέχει όλες τις συναλλαγές που γίνονται δεκτές στο μπλοκ ως μια σειρά υπογεγραμμένων εισόδων (inputs) και εξόδων (outputs) που διασφαλίζουν τη μεταφορά του ποσού από τον αποστολέα στον παραλήπτη [35].

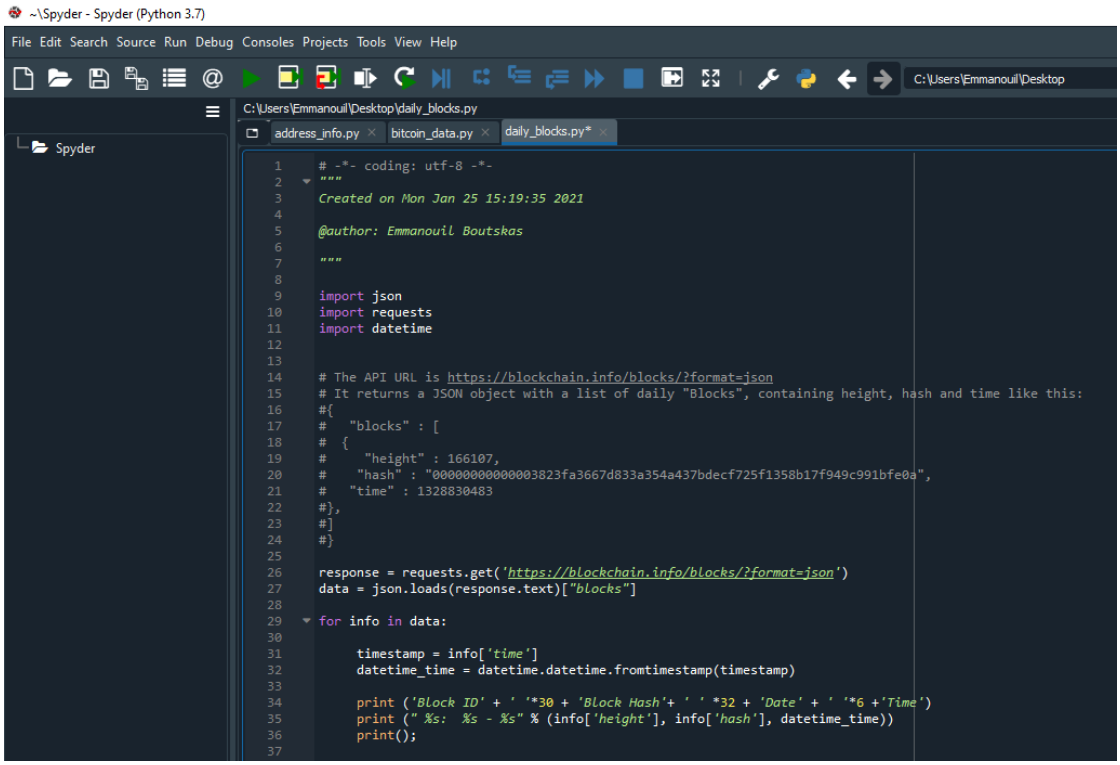


Εικόνα 3.2: Αναπαράσταση πληροφοριών block # 659083, το οποίο περιέχει 2354 συναλλαγές [82]

Όλες οι συναλλαγές αφού κατακερματιστούν κατά μήκος ενός δέντρου Merkle σχηματίζουν τη ρίζα Merkle (merkleroot) [7]. Στη συνέχεια, η κεφαλίδα του μπλοκ που περιέχει τον αριθμό έκδοσης, τον κατακερματισμό του προηγούμενου μπλοκ, τον χρόνο, τη δυσκολία και τη ρίζα Merkle κατακερματίζεται, με αποτέλεσμα τη δημιουργία του κατακερματισμού του μπλοκ (πράσινο πλαίσιο).

Κάθε συναλλαγή που εκτελείται στο δίκτυο συνδυάζεται για να σχηματίσει ένα μπλοκ. Όταν σχηματιστεί ένα μπλοκ, αμέσως, θα προστεθεί στο Blockchain. Αυτά τα μπλοκ είναι αμετάβλητα και απαραβίαστα για όλες τις συναλλαγές που πραγματοποιούνται στο δίκτυο. Κάθε μπλοκ πρέπει να περιέχει μία ή περισσότερες συναλλαγές και η πρώτη συναλλαγή στο μπλοκ ονομάζεται συναλλαγή coinbase [7]. Αυτή η συναλλαγή δημιουργείται από τον κόμβο εξόρυξης και αποτελεί την ανταμοιβή για την εξόρυξη του μπλοκ. Το ποσό της συνολικής ανταμοιβής που συλλέγει ο κόμβος εξόρυξης είναι το άθροισμα όλων των κόμιστρων των συναλλαγών που περιέχονται στο μπλοκ συν την coinbase ανταμοιβή.

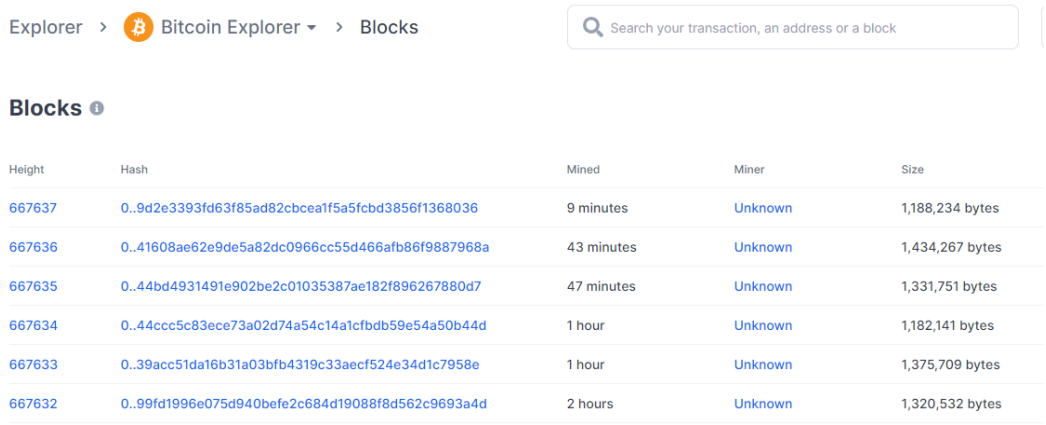
Στο παρακάτω παράδειγμα θα χρησιμοποιήσουμε τη βιβλιοθήκη αιτημάτων (requests), json και datetime της Python σε συνδυασμό με το Blockchain Data API για να βρούμε τα block που έχουν προστεθεί στο Blockchain του Bitcoin το τελευταίο 24ώρο.



Αποτέλεσμα:

```
Block ID                          Block Hash                                  Date       Time
 667631:  00000000000000000000c6a143abbedd7a57cd41c605a0d387c2e00bb0e4dd12b - 2021-01-25 19:40:49

Block ID                          Block Hash                                  Date       Time
 667632:  00000000000000000000099fd1996e075d940befe2c684d19088f8d562c9693a4d - 2021-01-25 19:43:39

Block ID                          Block Hash                                  Date       Time
 667633:  00000000000000000000039acc51da16b31a03bfb4319c33aecf524e34d1c7958e - 2021-01-25 19:58:52

Block ID                          Block Hash                                  Date       Time
 667634:  00000000000000000000044ccc5c83ece73a02d74a54c14a1cfbdb59e54a50b44d - 2021-01-25 20:05:20

Block ID                          Block Hash                                  Date       Time
 667635:  00000000000000000000044bd4931491e902be2c01035387ae182f896267880d7 - 2021-01-25 20:41:01

Block ID                          Block Hash                                  Date       Time
 667636:  00000000000000000000041608ae62e9de5a82dc0966cc55d466afb86f9887968a - 2021-01-25 20:44:51

Block ID                          Block Hash                                  Date       Time
 667637:  00000000000000000000009d2e3393fd63f85ad82cbcea1f5a5fcbd3856f1368036 - 2021-01-25 21:19:08
```

Για να δούμε ωστόσο αν ο κώδικας τραβάει τα σωστά δεδομένα θα ελέγξουμε αν το αποτέλεσμα είναι ίδιο με αυτό που υπάρχει στο Blockchain.com. Παρατηρούμε ότι η παρακάτω εικόνα εμφανίζει όντως το ίδιο αποτέλεσμα με αυτό του κώδικα.

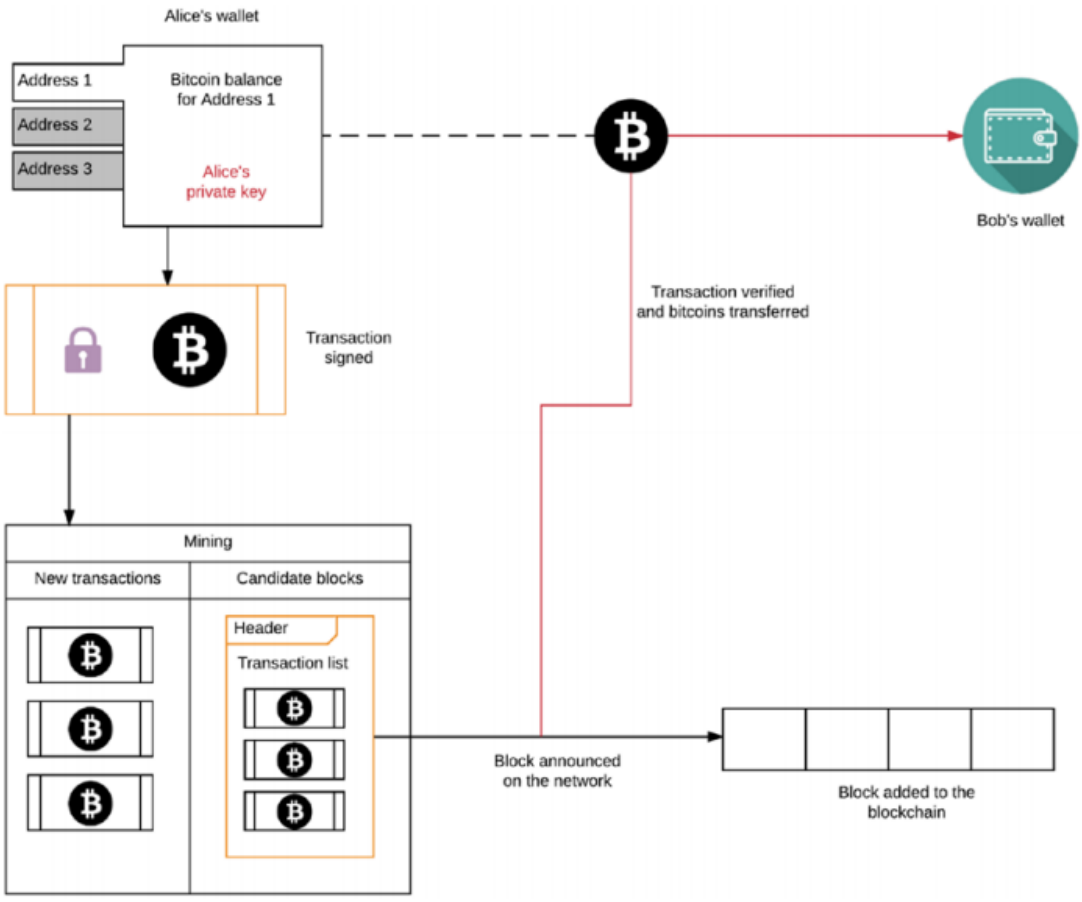


Εικόνα 3.2.1: Blockchain explorer - Blocks

Κύκλος Ζωής Συναλλαγών

Η αρχική δημιουργία μιας συναλλαγής ξεκινά συνήθως από κάποια εφαρμογή πορτοφόλι (wallet). Εν συνεχεία, υπογράφεται με την ψηφιακή υπογραφή του δημιουργού προκειμένου να ξεκλειδωθεί η χρηματική αξία των κρυπτονομισμάτων που θέλει να μεταφέρει. Έπειτα διαδίδεται σε ολόκληρο το δίκτυο μέχρι να φτάσει σε όλους τους κόμβους. Στο τελευταίο στάδιο θα επικυρωθεί από κάποιον mining κόμβο και θα συμπεριληφθεί σε ένα μπλοκ συναλλαγών το οποίο θα καταγραφεί στο Blockchain [7].

Στο παρακάτω σχήμα ακολουθεί ένα παράδειγμα στο οποίο η Alice ξεκινά μια συναλλαγή από το πορτοφόλι της, το οποίο περιέχει πολλές διευθύνσεις. Ένας χρήστης μπορεί να δημιουργήσει όσες διευθύνσεις θέλει [35]. Όπως φαίνεται και στο παρακάτω σχήμα η Alice είχε τρεις διευθύνσεις στο πορτοφόλι της και καθεμία από τις διευθύνσεις μπορεί να λειτουργήσει μαζί με το ιδιωτικό της κλειδί. Κάθε διεύθυνση έχει ένα συγκεκριμένο ποσό υπολοίπου Bitcoin (το άθροισμα όλων των UTXO που σχετίζονται με αυτήν τη διεύθυνση) που μπορεί να χρησιμοποιηθεί για τη δημιουργία νέων συναλλαγών [35]. Στη συνέχεια, η συναλλαγή υπογράφεται χρησιμοποιώντας το ιδιωτικό κλειδί της Alice και εισέρχεται στη φάση εξόρυξης, όπου θα καταχωρηθεί σε υποψήφιο μπλοκ. Καθώς ολοκληρώνεται η εξόρυξη, ο νικητής ανθρακωρύχος ανακοινώνει το μπλοκ στο δίκτυο και το μπλοκ συμπεριλαμβάνεται στο Blockchain. Η συναλλαγή διαδίδεται στον Μπομπ, ο οποίος μπορεί τώρα να χρησιμοποιήσει το ιδιωτικό κλειδί του για να ξεκλειδώσει το ποσό εξόδου συναλλαγής και να το χρησιμοποιήσει [35]. Οι ιδέες των UTXO, η υπογραφή, και το κλείδωμα και το ξεκλείδωμα σεναρίων παρέχουν βαθύτερες πληροφορίες για το πώς το Blockchain παραμένει εσωτερικά συνεπή ως αποκεντρωμένο καθολικό.



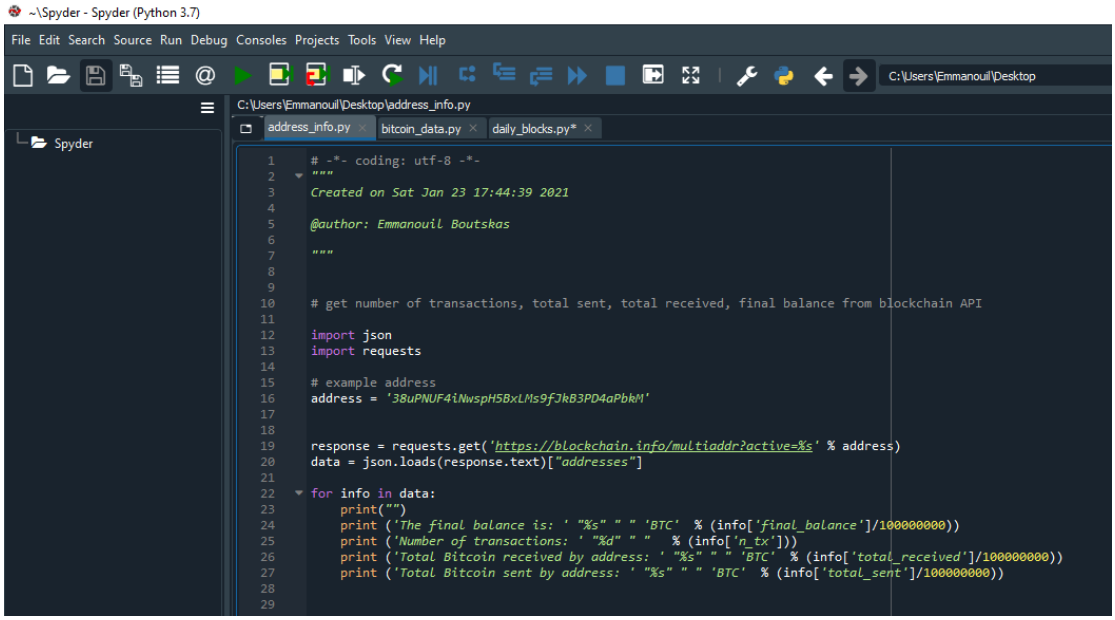
Εικόνα 3.3: Κύκλος ζωής μίας συναλλαγής στο δίκτυο [35]

Μετάδοση Συναλλαγών στο Δίκτυο

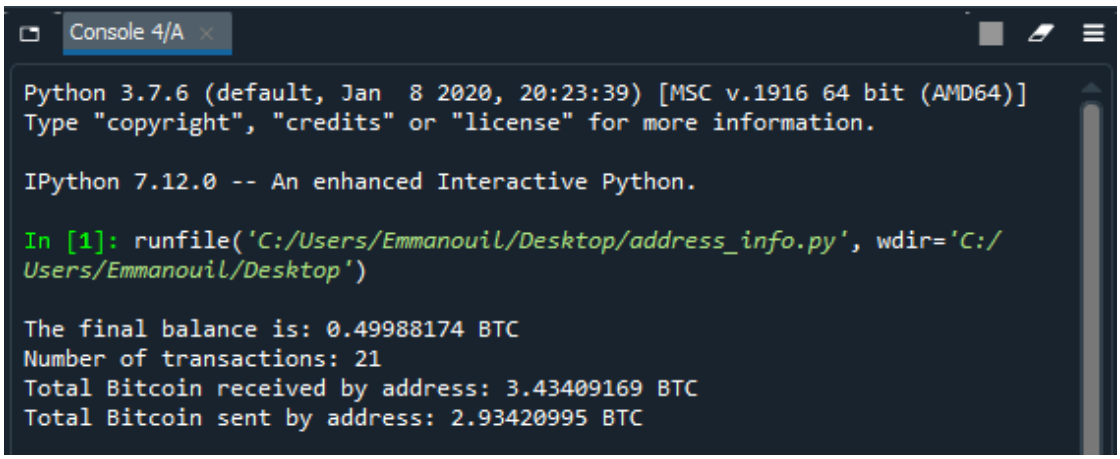
Προκειμένου μία συναλλαγή να συμπεριληφθεί και να διαδοθεί στο Blockchain πρέπει πρώτα να φτάσει στο δίκτυο. Κάθε συναλλαγή έχει μέγεθος περίπου 300 - 400 byte δεδομένων τα οποία πρέπει να φτάσουν σε κάποιον από τους κόμβους του δικτύου του [7]. Οι κόμβοι από την πλευρά τους δεν χρειάζεται να γνωρίζουν την ταυτότητα του αποστολέα. Από την στιγμή που η συναλλαγή υπογράφεται και δεν περιέχει ευαίσθητες πληροφορίες όπως ιδιωτικά κλειδιά του αποστολέα τότε είναι έτοιμη να μεταδοθεί δημοσίως. Οι συναλλαγές με Bitcoin μπορούν να σταλούν μέσα από οποιοδήποτε δίκτυο, σε αντίθεση με τις συναλλαγές που πραγματοποιούνται μέσα από πιστωτικές και χρεωστικές κάρτες οι οποίες μεταδίδονται μόνο μέσω κρυπτογραφημένων δικτύων γιατί περιέχουν ευαίσθητα δεδομένα και πληροφορίες [7].

Το μόνο που αρκεί είναι η συναλλαγή να φτάσει σε έναν κόμβο του δικτύου και στη συνέχεια θα αναλάβει αυτός την διάδοση της σε ολόκληρο το δίκτυο, δεν έχει σημασία το πώς θα φτάσει στον κόμβο. Ως αποτέλεσμα, οι συναλλαγές είναι σε θέση να διαδοθούν στο δίκτυο μέσω όχι τόσο ασφαλών δικτύων όπως Bluetooth, WiFi, NFC, Barcode κλπ.

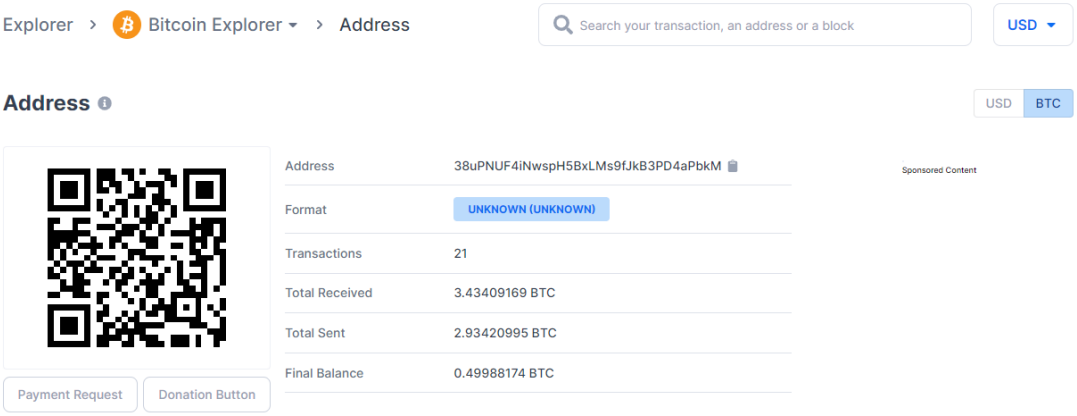
Στο παρακάτω παράδειγμα θα χρησιμοποιήσουμε τη βιβλιοθήκη αιτημάτων (requests) και json της Python και το Blockchain Data API για να αντλήσουμε πληροφορίες σχετικά με το διαθέσιμο υπόλοιπο μιας διεύθυνσης Bitcoin και το συνολικό αριθμό συναλλαγών που έχει εκτελέσει. Το API είναι δωρεάν και δεν απαιτεί έλεγχο ταυτότητας.



Αποτέλεσμα:



Για να δούμε ωστόσο αν ο κώδικας τραβάει τα σωστά δεδομένα θα ελέγξουμε αν το αποτέλεσμα είναι ίδιο με αυτό που υπάρχει στο Blockchain.com. Παρατηρούμε ότι η παρακάτω εικόνα εμφανίζει όντως το ίδιο αποτέλεσμα με αυτό του κώδικα.



Εικόνα 3.3.1: Blockchain explorer - Address

Διάδοση Συναλλαγών στο Δίκτυο

Από την στιγμή που μια συναλλαγή σταλεί σε κάποιον κόμβο του δικτύου, επικυρώνεται από αυτόν και στην συνέχεια ο ίδιος κόμβος αναλαμβάνει να την διαβιβάσει στους κόμβους με τους όποιους συνδέεται. Αν η συναλλαγή είναι έγκυρη τότε αποστέλλει ένα μήνυμα επιτυχίας πίσω στον δημιουργό της αλλιώς σε περίπτωση που δεν είναι έγκυρη την απορρίπτει και στέλνει μήνυμα αντιστοίχως. Κάθε κόμβος ανακαλύπτει τους υπόλοιπους κόμβους με τους οποίους θα συνδεθεί κατά τη διάρκεια της εκκίνησης της συναλλαγής, μέσω του πρωτοκόλλου peer to peer [7]. Όλοι οι κόμβοι είναι ισάξιοι μεταξύ τους και δεν υπάρχει καμία προκαθορισμένη τοπολογία στο δίκτυο. Τα block, οι συναλλαγές και τα μηνύματα διαβιβάζονται από τον κάθε κόμβο στους κόμβους με τους οποίους συνδέεται. Όταν μία συναλλαγή σταλθεί σε κάποιον κόμβο αυτός με την σειρά του θα την στείλει σε 4 με 5 γειτονικούς κόμβους όπου με την σειρά τους ο καθένας θα την στείλει σε άλλους 4 με 5 κόμβους κ.ο.κ. [7]. Μέσα σε λίγα δευτερόλεπτα η συναλλαγή μεταβιβάζεται με έναν εκθετικά αυξανόμενο ρυθμό σε ολόκληρο το δίκτυο μέχρι να την λάβουν όλοι οι συνδεδεμένοι κόμβοι. Το Bitcoin δίκτυο είναι σχεδιασμένο με τέτοιο τρόπο ώστε να είναι ανθεκτικό σε πιέσεις.

Επιθέσεις DDoS και Spamming μπορούν και αποτρέπονται χάρις στην δυνατότητα που έχουν οι κόμβοι να επικυρώνουν ανεξάρτητα ο καθένας κάθε συναλλαγή, προτού την διαβιβάσουν σε άλλον κόμβο [7]. Όταν μία συναλλαγή είναι διαμορφωμένη λάθος τότε δεν μπορεί να προχωρήσει πέραν του αρχικού κόμβου.

Κύκλος Ζωής Συναλλαγών στο δίκτυο του Ethereum

Μόλις ένας χρήστης στείλει μια συναλλαγή στο δίκτυο, δημιουργείται ένας κατακερματισμός αυτής της συναλλαγής π.χ. *0x97d99bc7729211111a21b12c933c949d4f31684f1d6954ff477d0477538ff017*. Στη συνέχεια, η συναλλαγή μεταδίδεται στο δίκτυο. Το δίκτυο του Ethereum χρησιμοποιεί ένα πρωτόκολλο «δρομολόγησης πλημμύρας» (flood routing) [31]. Κάθε πελάτης στο δίκτυο ενεργεί ως ένας κόμβος σε δίκτυο peer-to-peer (P2P), το οποίο ιδανικά σχηματίζει ένα δίκτυο πλέγματος (mesh network). Όλοι οι κόμβοι του δικτύου ενεργούν ως ίσοι μεταξύ τους. Η διάδοση των συναλλαγών ξεκινά από έναν κόμβο του δικτύου που δημιουργεί μια υπογεγραμμένη συναλλαγή. Η συναλλαγή επικυρώνεται και στη συνέχεια μεταδίδεται σε όλους τους άλλους κόμβους του δικτύου που συνδέονται άμεσα με τον αρχικό κόμβο που δημιούργησε την συναλλαγή. Κατά μέσο όρο, κάθε κόμβος στο δίκτυο του Ethereum διατηρεί συνδέσεις με τουλάχιστον 13 άλλους κόμβους, που ονομάζονται γείτονες του [31]. Κάθε γειτονικός κόμβος επικυρώνει τη συναλλαγή μόλις την λάβει. Εφόσον η συναλλαγή είναι έγκυρη οι κόμβοι αποθηκεύουν ένα αντίγραφο της και το διαδίδουν σε όλους τους γείτονες τους (εκτός από αυτόν που προήλθε). Ως αποτέλεσμα, η συναλλαγή διαδίδεται σε όλο το δίκτυο, μέχρις ότου όλοι οι κόμβοι στο δίκτυο να έχουν ένα αντίγραφο της. Μέσα σε λίγα δευτερόλεπτα, μια συναλλαγή στο Ethereum διαδίδεται σε όλους τους κόμβους του δικτύου σε ολόκληρο τον κόσμο.

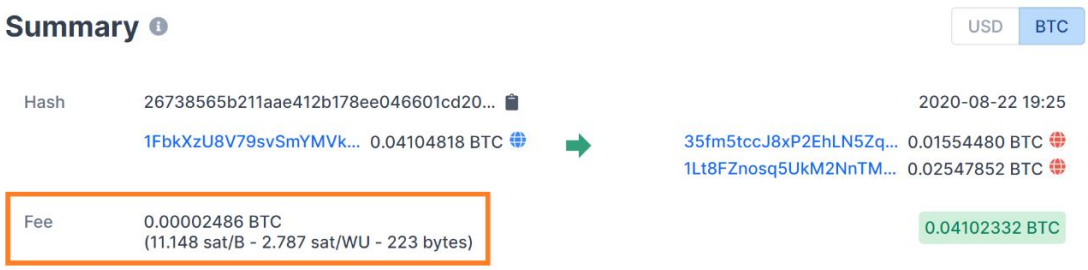
Από την πλευρά κάθε κόμβου, δεν είναι δυνατή η διάκριση σχετικά με την προέλευση της συναλλαγής. Ο κόμβος που έστειλε στον γειτονικό του κόμβο την συναλλαγή μπορεί να είναι ο εντολέας της συναλλαγής ή μπορεί να την έχει λάβει από έναν άλλο γείτονα. Για να μπορέσει να παρακολουθήσει την προέλευση των συναλλαγών ή να παρέμβει στη διάδοση τους στο δίκτυο, ένας εισβολέας θα έπρεπε να ελέγξει ένα σημαντικό ποσοστό όλων των κόμβων [31]. Αυτό είναι εξαιρετικά δύσκολο και αποτελεί μέρος της ασφάλειας και του σχεδιασμού απορρήτου των δικτύων P2P, ειδικά

όπως εφαρμόζονται σε δίκτυα Blockchain. Στη συνέχεια, η συναλλαγή περιλαμβάνεται σε μια ομάδα με πολλές άλλες συναλλαγές.

Ένας ανθρακωρύχος πρέπει να επιλέξει τη συναλλαγή και να τη συμπεριλάβει σε ένα μπλοκ για να επαληθεύσει την εγκυρότητα της. Οι ανθρακωρύχοι δίνουν πάντα προτεραιότητα στις συναλλαγές με υψηλότερο GASPRICE επειδή λαμβάνουν υψηλότερα τέλη [31]. Για να γίνει αυτό ο ανθρακωρύχος πρέπει να βρει την τιμή nonce που αντιπροσωπεύει μια σωστή λύση σε ένα κρυπτογραφικό πρόβλημα. Ο πρώτος ανθρακωρύχος που βρίσκει μια λύση για το μπλοκ του, μεταδίδει τη λύση σε όλους τους άλλους κόμβους. Οι κόμβοι που έλαβαν τη λύση, επαληθεύουν αν αντιστοιχεί στο πρόβλημα του μπλοκ του αποστολέα. Εάν η λύση είναι σωστή, οι άλλοι κόμβοι μπορούν να επιβεβαιώσουν ότι το μπλοκ μπορεί να προστεθεί στο Blockchain. Όταν η πλειονότητα των κόμβων καταλήξει σε συναίνεση, το μπλοκ προστίθεται στο Blockchain. Όσο μεγαλύτερος είναι ο αριθμός των μπλοκ που επιβεβαιώνουν την λύση, τόσο πιο αμετάβλητη είναι η συναλλαγή. Επομένως, για συναλλαγές υψηλότερης αξίας, ενδέχεται να απαιτούνται περισσότερες επιβεβαιώσεις μπλοκ.

Κόμιστρα των Συναλλαγών

Σχεδόν όλες οι συναλλαγές περιέχουν κόμιστρα τα οποία αποζημιώνουν τους miners για την εξόρυξη του μπλοκ, το οποίο αναλαμβάνει την καταγραφή της συναλλαγής στο Blockchain. Στη περίπτωση του Bitcoin, η αξία των κόμιστρων υπολογίζεται με βάση το μέγεθος σε kilobytes της συναλλαγής και όχι με βάση την αξία της σε Bitcoin [7]. Συγκεκριμένα, υπολογίζεται ως η διαφορά μεταξύ των συνολικών δεδομένων εισόδου και των συνολικών δεδομένων εξόδου. Το αποτέλεσμα που απομένει από αυτή την διαφορά είναι το κόμιστρο που θα λάβει ο miner [7].



Εικόνα 3.4: Χρέωση συναλλαγής Bitcoin

Εικόνα 3.5: Χρέωση συναλλαγής Ethereum

Συναλλαγές με ικανοποιητικά κόμιστρα έχουν περισσότερες πιθανότητες να συμπεριληφθούν στο αμέσως επόμενο μπλοκ που θα προστεθεί στο Blockchain. Αντιθέτως, αυτές που δεν έχουν τόσο ικανοποιητικά κόμιστρα ή και μηδενικά μπορεί να επεξεργαστούν μετά από κάποια μπλοκ ή και καθόλου. Υπάρχουν βέβαια και περιπτώσεις όπου οι miners επεξεργάζονται συναλλαγές δωρεάν υπό συγκεκριμένες συνθήκες. Δεν είναι υποχρεωτικό κάποια συναλλαγή να έχει κόμιστρο, ωστόσο το γεγονός ότι συμπεριλαμβάνεται σε αυτήν δίνει μεγαλύτερο κίνητρο στους miners να την επεξεργαστούν με μεγαλύτερη προτεραιότητα. Τα τέλη συναλλαγής σε συναλλαγές με Bitcoin και Ethereum είναι εντελώς προαιρετικά. Η ελάχιστη χρέωση ανά συναλλαγή ορίζεται στα 0,0001 Bitcoin ανά kilobyte [7]. Οι περισσότερες συναλλαγές έχουν μέγεθος μικρότερο του ενός kilobyte εκτός και αν έχουν περισσότερες από μία εισόδους και εξόδους, οπότε μπορεί να έχουν μεγαλύτερο μέγεθος. Τα κόμιστρα που προσφέρονται σε συναλλαγές με Ethereum μετατρέπονται σε μία μονάδα που ονομάζεται gas [31]. Τα πορτοφόλια μπορούν να προσαρμόσουν το gasPrice στις συναλλαγές που προέρχονται από αυτά για να επιτύχουν ταχύτερη επιβεβαίωση συναλλαγών. Όσο μεγαλύτερο είναι το gasPrice, τόσο πιο γρήγορα είναι πιθανό η συναλλαγή να επιβεβαιωθεί. Αντίθετα, οι συναλλαγές χαμηλότερης προτεραιότητας μπορούν να έχουν μειωμένο gasPrice, με αποτέλεσμα πιο αργή επιβεβαίωση [31]. Η ελάχιστη τιμή στην οποία μπορεί να οριστεί το gasPrice είναι μηδέν, που σημαίνει μια συναλλαγή χωρίς χρέωση.

Δομή Συναλλαγών

Μια συναλλαγή αποτελείται από έξι πεδία. Το πρώτο περιέχει το αριθμός έκδοσης, που δηλώνει τους κανόνες που ακολουθούνται από τη συναλλαγή για επικύρωση. Το δεύτερο περιέχει τον αριθμό των εισόδων μέσα στη συναλλαγή ακολουθούμενο από μια λίστα εισόδων που προέρχονται από προηγούμενες εξόδους άλλων συναλλαγών. Το τέταρτο πεδίο περιέχει τον αριθμό των εξόδων και το πέμπτο πεδίο περιέχει τη λίστα με τις εξόδους, τουλάχιστον μία έξοδος είναι απαραίτητη. Το τελευταίο πεδίο περιέχει το χρόνο κλειδώματος της συναλλαγής και αναφέρεται στην πρώτη φορά που η συναλλαγή θεωρείται έγκυρη και μπορεί πλέον να μεταδοθεί σε όλο το δίκτυο ή να προστεθεί στο Blockchain [7]. Στις περισσότερες συναλλαγές παίρνει την τιμή μηδέν για να υποδείξει ότι η συναλλαγή μπορεί να διαδοθεί και να εκτελεστεί άμεσα. Αν η τιμή του χρόνο κλειδώματος δεν είναι μηδέν και κυμαίνεται σε μία κλίμακα μέχρι 500 εκατομμύρια μεταφράζεται ως ύψος του μπλοκ κάτι που σημαίνει ότι η συναλλαγή δεν είναι έγκυρη και δεν διαδίδεται στο δίκτυο [7].

Size	Field	Description
4 bytes	Version	Specifies which rules this transaction follows
1–9 bytes (VarInt)	Input Counter	How many inputs are included
Variable	Inputs	One or more transaction inputs
1–9 bytes (VarInt)	Output Counter	How many outputs are included
Variable	Outputs	One or more transaction outputs
4 bytes	Locktime	A Unix timestamp or block number

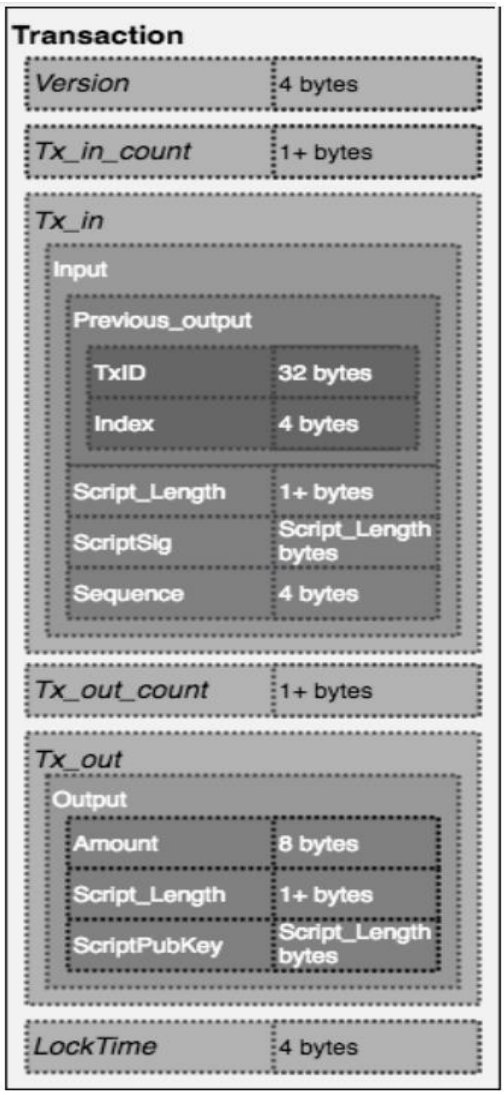
Εικόνα 3.6: Δομή συναλλαγής [7]

Hash	Inputs #	Outputs #	Input (BTC)	Output (BTC)	Version [int]	Lock time
0c...00	1	1	0.00012050	0.00003026	1	0
7d...fd	1	10	1.14160609	1.14120540	2	658968
f4...db	1	2	0.00488077	0.00469402	1	0
25...da	1	2	0.20364813	0.20346055	1	0
0b...d2	1	2	0.00370250	0.00351492	1	0
f1...d0	1	2	0.01324822	0.01307558	1	0
3b...bb	1	2	0.04142260	0.04123751	1	0

Εικόνα 3.7: Πεδία Συναλλαγών Bitcoin, https://blockchair.com/

Όπως προαναφέρθηκε οι συναλλαγές αποτελούνται από μια λίστα εισόδων (Tx_in) και μια λίστα εξόδων (Tx_out). Η είσοδος είναι αναφορά σε έξοδο προηγούμενης συναλλαγής. Μία συναλλαγή μπορεί να περιέχει πολλαπλές εισόδους. Αυτές οι τιμές εισόδου συνδυάζονται για να δώσουν ένα σύνολο που αντιπροσωπεύει το υπόλοιπό του λογαριασμού. Πρόκειται ουσιαστικά για το προστιθέμενο ποσό των μη χρησιμοποιημένων (προηγούμενων) εξόδων συναλλαγών, το άθροισμα των οποίων δείχνει το υπόλοιπο. Η έξοδος της συναλλαγής ορίζεται ως το άθροισμα των δεδομένων εισόδων μείον τα κόμιστρα συναλλαγών [36].

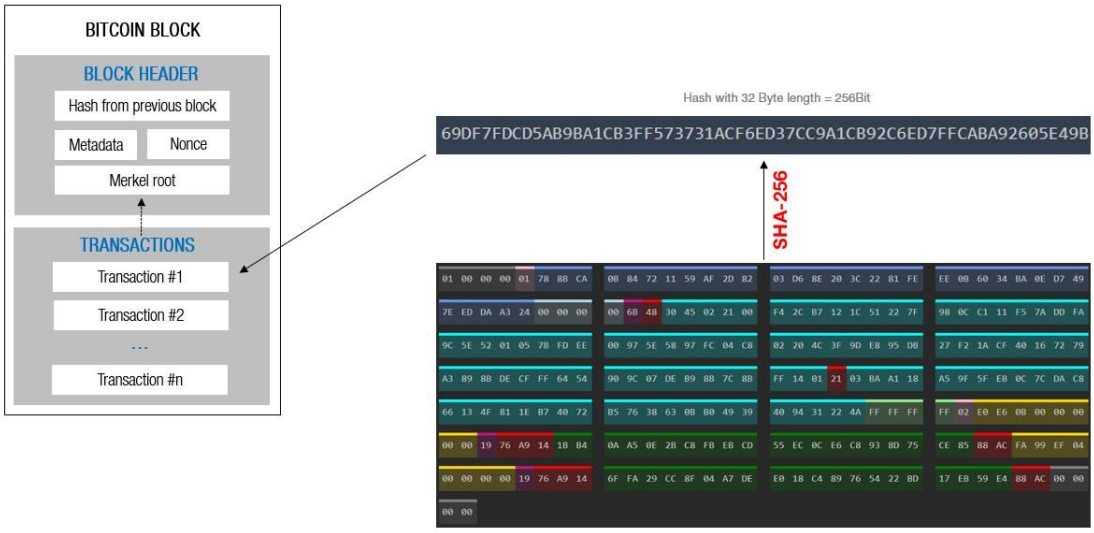
Μια είσοδος (Tx_in) αποτελείται από 4 πεδία. Το πρώτο περιέχει μια αναφορά σε προηγούμενη έξοδο (Previous_output). Το δεύτερο περιέχει πληροφορίες σχετικά με το μήκος του ScriptSig (Script_Length) με μέγεθος από 1 byte έως 10.000 byte. Το επόμενο πεδίο περιέχει το ScriptSig, που χρησιμοποιείται για να αποδείξει την ιδιοκτησία της προηγούμενης εξόδου. Το τελευταίο πεδίο περιέχει τον αριθμό ακολουθίας (Sequence) που χρησιμοποιείται για την επαλήθευση του χρόνου κλειδώματος (LockTime) με προεπιλεγμένη τιμή 0xFFFFFFFF [36].



Εικόνα 3.8: Δεδομένα συναλλαγών, σε αυτό το παράδειγμα υπάρχει μόνο μία είσοδος και μία έξοδος [36]

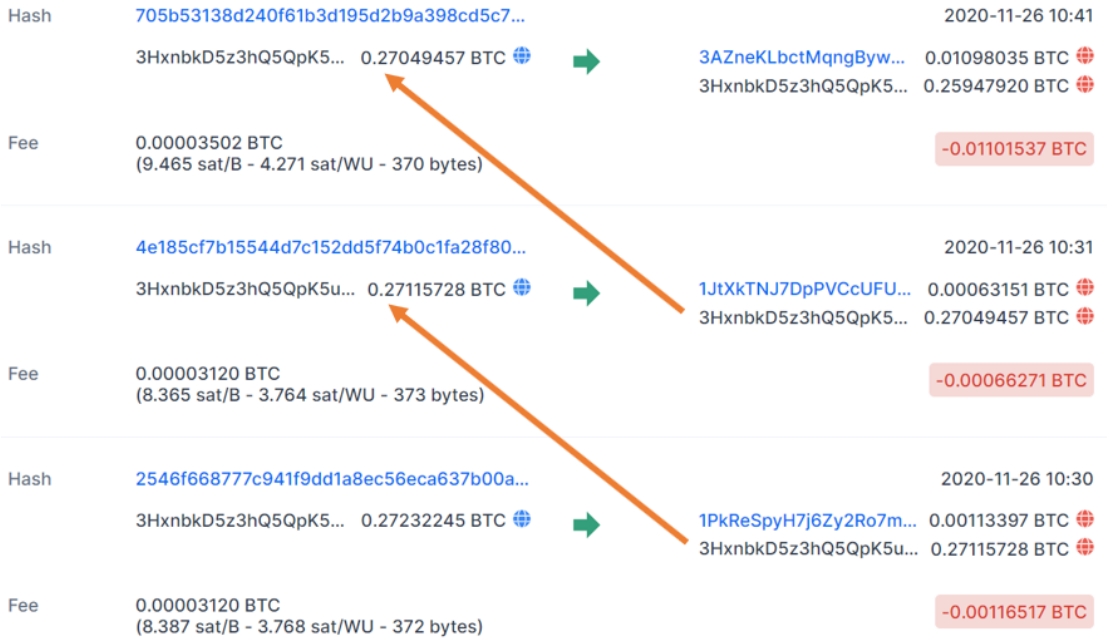
Η προηγούμενη έξοδος αποτελείται από τη ταυτότητα (TxID) της προηγούμενης συναλλαγής και αποθηκεύεται εντός του UTxO. Το TxID είναι ο κατακερματισμός της συναλλαγής. Τέλος, ακολουθεί ο δείκτης της εξόδου εντός της συναλλαγής.

Η έξοδος αποτελείται από 3 πεδία. Το πρώτο περιέχει το ποσό (Amount) Bitcoin σε satoshi της εξόδου. Το δεύτερο περιέχει πληροφορίες σχετικά με το μήκος του ScriptPubKey (Script_Length) με μέγεθος που κυμαίνεται από 1 byte έως 10.000 byte. Ακολουθεί το ScriptPubKey, το οποίο καθορίζει ποιος μπορεί ξοδέψει την έξοδο [36].



Εικόνα 3.9: Στα δεξιά της εικόνας εμφανίζονται τα δεδομένα της δομής της συναλλαγής, κάθε ένα με διαφορετικό χρώμα. Στο πάνω μέρος εμφανίζεται ο κατακερματισμός (hash) όλων των δεδομένων που προθέτεται στο block [81]

Για να κατανοήσουμε καλύτερα πως λειτουργούν όλα αυτά στον πραγματικό κόσμο ας δούμε για παράδειγμα το στιγμιότυπο κάποιων συναλλαγών που ανακτήθηκαν από το *Blockchain.com*



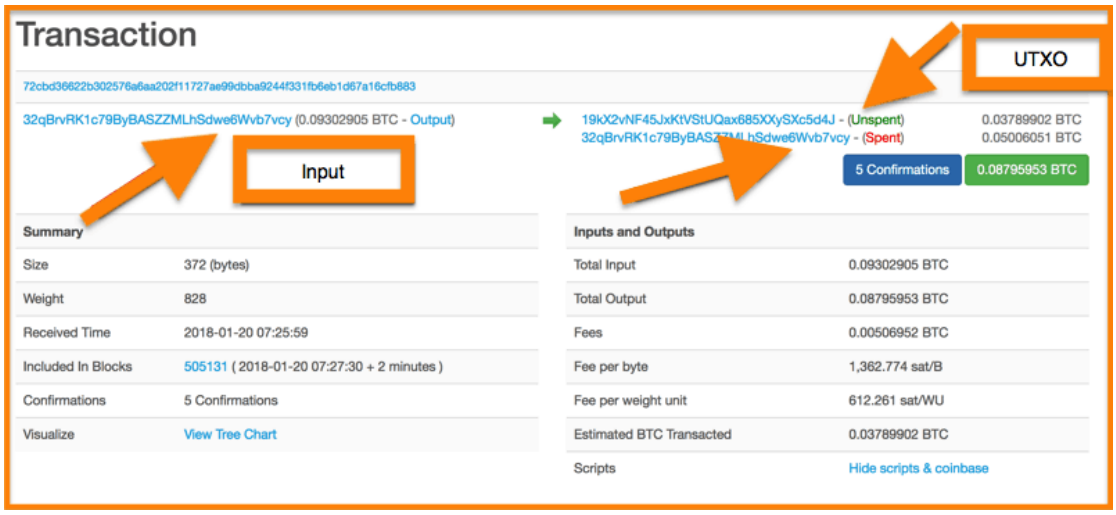
Εικόνα 3.9.1: Στιγμιότυπο συναλλαγών

Όπως φαίνεται στην παρακάτω εικόνα ο χρήστης με διεύθυνση **3HxnbkD5z3hQ5QpK5uNKaPdc7VbZ6AZ7qW** στέλνει **0.00063151** BTC σε έναν άλλο χρήστη με διεύθυνση **1JtXkTNJ7DpPVCcUFUGrr9H4967hwp1T9S** και χρησιμοποιεί μια προηγούμενη έξοδο **0.27115728** BTC. Η συναλλαγή αποτελείται από μία έξοδο **0.00063151** BTC και άλλη μια **0.27049457** BTC ως UTXO πίσω στον αρχικό αποστολέα. Μια καλή πρακτική ασφάλειας είναι να χρησιμοποιείται ένα νέο ζεύγος κλειδιών για κάθε νέα συναλλαγή.

Αδαπάνητα Δεδομένα Εξόδου

Το σημαντικότερο στοιχείο μιας συναλλαγής είναι τα αδαπάνητα δεδομένα εξόδου (Unspent Transaction Output). Το Bitcoin διατηρεί κάποια αδιαίρετα κομμάτια τα οποία είναι κλειδωμένα σε κάποιον συγκεκριμένο ιδιοκτήτη. Αυτά τα κομμάτια ονομάζονται UTXO και είναι καταγεγραμμένα σε ολόκληρο το Blockchain, και αναγνωρισμένα από ολόκληρο το δίκτυο ως νομισματικές μονάδες [7]. Όταν ένας χρήστης λάβει Bitcoin (π.χ. αγορά, μεταφορά από άλλο λογαριασμό) τότε το ποσό αυτό καταγράφεται στο Blockchain σαν UTXO [34]. Με αυτόν τον τρόπο τα Bitcoin των χρηστών μοιράζονται ως UTXO ανάμεσα σε χιλιάδες block και χιλιάδες συναλλαγές. Στην πραγματικότητα το υπόλοιπο των λογαριασμών των χρηστών δεν είναι αποθηκευμένο κάπου. Αυτό που υπάρχει μόνο, είναι διάσπαρτα UTXO κλειδωμένα σε διάφορους ιδιοκτήτες. Το υπόλοιπο που εμφανίζεται στα πορτοφόλια κρυπτονομισμάτων είναι ουσιαστικά το άθροισμα των UTXO που υπάρχουν στο Blockchain που ανήκουν στον συγκεκριμένο χρήστη [7]. Σε περίπτωση που ένα UTXO είναι μεγαλύτερο της αξίας της συναλλαγής τότε αυτό πρέπει να καταναλωθεί όλο και εκ νέου να δημιουργηθούν τα ρέστα της συναλλαγής [34]. Έστω ότι έχουμε ένα UTXO των 30 Bitcoin και θέλουμε να πραγματοποιήσουμε μία συναλλαγή αξίας 5 Bitcoin. Η συναλλαγή αναγκαστικά θα καταναλώσει και τα 30 Bitcoin του UTXO και δημιουργήσει ως αποτέλεσμα δύο δεδομένα εξόδου. Το πρώτο δεδομένο θα πληρώνει 5 Bitcoin στον αντίστοιχο παραλήπτη και το δεύτερο δεδομένο θα πληρώνει 25 Bitcoin στο πορτοφόλι του χρήστη ως ρέστα.

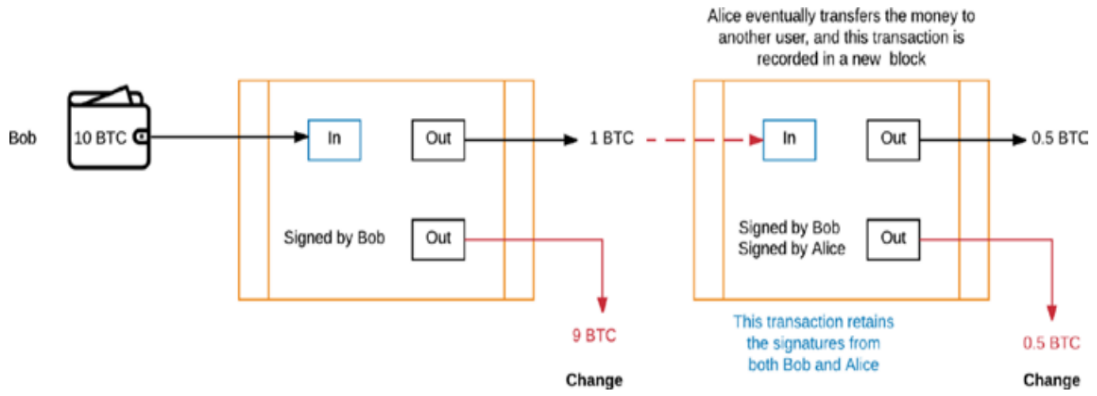
Τα UTXO μπορούν να ονομαστούν ως δεδομένα εισόδου αν καταναλώνονται από κάποια συναλλαγή, και ως δεδομένα εξόδου αν δημιουργούνται από κάποια συναλλαγή [7]. Τέλος, τα UTXO που καταναλώνονται από τις συναλλαγές ξεκλειδώνονται με την υπογραφή του ιδιοκτήτη, ενώ αυτά που δημιουργούνται από τις συναλλαγές κλειδώνονται στην διεύθυνση του νέου ιδιοκτήτη.



Εικόνα 3.10: Πληροφορίες συναλλαγής Bitcoin. Στην αριστερή πλευρά εμφανίζονται τα δεδομένα εισόδου και εξόδου και UTXO [80].

Στο παρακάτω παράδειγμα περιγράφετε η διαδικασία με την οποία διαδίδονται οι συναλλαγές σε όλο το δίκτυο. Σε αυτό το παράδειγμα, ο Bob ξεκινάει για πρώτη φορά μία συναλλαγή στέλνοντας στην Alice 1 BTC και λαμβάνει πίσω ως αδαπάνητα δεδομένα εξόδου 9 BTC. Η Alice με τη σειρά της στέλνει περαιτέρω 0,5 BTC σε έναν άλλο χρήστη και λαμβάνει πίσω ως αδαπάνητα δεδομένα εξόδου 0,5 BTC Όπως παρατηρούμε η πρώτη συναλλαγή υπογράφηκε από τον Bob, ο οποίος ξεκίνησε τη συναλλαγή και στη συνέχεια η Alice υπέγραψε τη δεύτερη συναλλαγή. Κατά μία έννοια, η έξοδος από την πρώτη συναλλαγή έγινε είσοδος για τη δεύτερη, έτσι η υπογραφή του Bob διατηρήθηκε ως απόδειξη της πρώτης συναλλαγής και η υπογραφή της Alice χρησιμεύει πλέον ως μηχανισμός ξεκλειδώματος. Με αυτόν τον τρόπο μπορούν οι συναλλαγές να παρακολουθούνται σε ολόκληρο το δίκτυο Bitcoin από την προέλευση έως τον τελικό κάτοχο (τελική διεύθυνση).

Ένα σενάριο (script) επισυνάπτεται σε κάθε συναλλαγή και περιέχει οδηγίες σχετικά με το πώς μπορεί να έχει πρόσβαση ο χρήστης στα Bitcoin που λαμβάνει [35]. Ουσιαστικά, ο αποστολέας πρέπει να παρέχει ένα δημόσιο κλειδί που οποιοσδήποτε στο δίκτυο μπορεί να χρησιμοποιήσει για να προσδιορίσει ότι η συναλλαγή προήλθε πράγματι από τη διεύθυνση που περιέχεται μέσα στο σενάριο, και μια υπογραφή που δείχνει ότι η συναλλαγή υπογράφηκε χρησιμοποιώντας το ιδιωτικό κλειδί του αποστολέα [35]. Χωρίς την εξουσιοδότηση ενός ζεύγους ιδιωτικού - δημόσιου κλειδιού, δεν θα ήταν δυνατή η πραγματοποίηση συναλλαγών μεταξύ χρηστών.



Εικόνα 3.10.1: Συναλλαγή στο Blockchain [35]

Στο παρακάτω παράδειγμα θα χρησιμοποιήσουμε τη βιβλιοθήκη αιτημάτων (requests) και json της Python και το Blockchain Data API για να αντλήσουμε πληροφορίες σχετικά με τα αδαπάνητα δεδομένα εξόδου (UTXO) που σχετίζονται με μία διεύθυνση.

Editor

C:\Users\Emmanouil\Desktop\ΚΩΔΙΚΑΣ\UTXO.py

UTXO.py*

```
# -*- coding: utf-8 -*-
"""
Created on Mon Jan 25 15:19:35 2021

@author: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html

"""

# get unspent outputs from blockchain API

import json
import requests

# example address
address = '1Dorian4RoXcnBv9hnQ4Y2C1an6NJ4UrjX'

# The API URL is https://blockchain.info/unspent?active=<address>
# It returns a JSON object with a list "unspent_outputs", containing UTXO, like this:
#{      "unspent_outputs":[
#   {
#     "tx_hash":"ebadfaa92f1fd29e2fe296eda702c48bd11ffd52313e986e99ddad9084062167",
#     "tx_index":51919767,
#     "tx_output_n": 1,
#     "script":"76a9148c7e252f8d64b0b6e313985915110fcfefcf4a2d88ac",
#     "value": 8000000,
#     "value_hex": "7a1200",
#     "confirmations":28691
#   },
# ...
#]}

resp = requests.get('https://blockchain.info/unspent?active=%s' % address)
utxo_set = json.loads(resp.text)["unspent_outputs"]

for utxo in utxo_set:
    print ("%s:%d - %g Bitcoin" % (utxo['tx_hash'], utxo['tx_output_n'], utxo['value']/100000000))

```

Με την εκτέλεση του script, βλέπουμε μια λίστα με αναγνωριστικά συναλλαγών, τον αριθμοδείκτη του UTXO και την τιμή αυτού του UTXO σε Bitcoins.

Console 4/A

```
Python 3.7.6 (default, Jan  8 2020, 20:23:39) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.12.0 -- An enhanced Interactive Python.

In [1]: runfile('C:/Users/Emmanouil/.spyder-py3/temp.py', wdir='C:/Users/Emmanouil/.spyder-
py3')
dbb3853afdb127cb7555bf44a033fa69b57335720132b8c016239ca80e4e570b:0 - 0.0010101 Bitcoin
b28ed2d746ea50e4b915d4ecaa9584da693c7785ab2fd33959e0eb21d9845bd8:0 - 0.0006 Bitcoin
4f0ecbba0264e890ab750d532151bae324c451a6bb8eb4405d6f9a8d16186b73:0 - 0.00154 Bitcoin
```

Δέντρα Merkle

Μέχρι στιγμής, μιλήσαμε για τη δομή των μπλοκ, τις λίστες συναλλαγών, τον τρόπο με τον οποίο πραγματοποιούνται οι συναλλαγές από τους χρήστες και πώς καταγράφονται στο Blockchain. Τα μπλοκ είναι ουσιαστικά δομές δεδομένων που συνδέονται με το Blockchain και οι συναλλαγές μπορούν να θεωρηθούν ως ιδιοκτησία αυτής της δομής δεδομένων. Πιο συγκεκριμένα, στην περίπτωση των Blockchains, οι συναλλαγές αντιπροσωπεύονται ως φύλλα ενός δέντρου merkle [7].

Αυτό που παρέχει ένα δέντρο merkle είναι ταχύτητα και απόδοση, και χρησιμοποιείται για επαλήθευση των συναλλαγών. Επειδή ο έλεγχος ενός N αριθμού αντικειμένων σε μια λίστα είναι μία αναποτελεσματική μέθοδος, δεν μπορούμε απλά να ελέγξουμε αν μία συναλλαγή ανήκει σε ένα Blockchain που περιέχει εκατομμύρια μπλοκ για επαλήθευση. Ένα δέντρο merkle είναι κατασκευασμένο από τις συναλλαγές ενός μπλοκ για να επιτρέψει γρήγορη πρόσβαση για λόγους επαλήθευσης [7]. Στο παρακάτω σχήμα ακολουθεί η απεικόνιση ενός δέντρου merkle. Σε αυτήν την περίπτωση, υπάρχουν τέσσερις συναλλαγές που συλλέχθηκαν σε ένα μπλοκ και απεικονίστηκαν σε ένα δέντρο merkle.

Ας υποθέσουμε ότι πραγματοποιήθηκαν τέσσερις συναλλαγές σε ένα μπλοκ: A, B, C και D. Οι συναλλαγές βρίσκονται πάντα στο χαμηλότερο επίπεδο του δέντρου. Κάθε συναλλαγή στη συνέχεια κατακερματίζεται, αφήνοντας:

Hash A, Hash B, Hash C, Hash D

Οι κατακερματισμοί συνδυάζονται μαζί με αποτέλεσμα την δημιουργία δύο νέων κατακερματισμών:

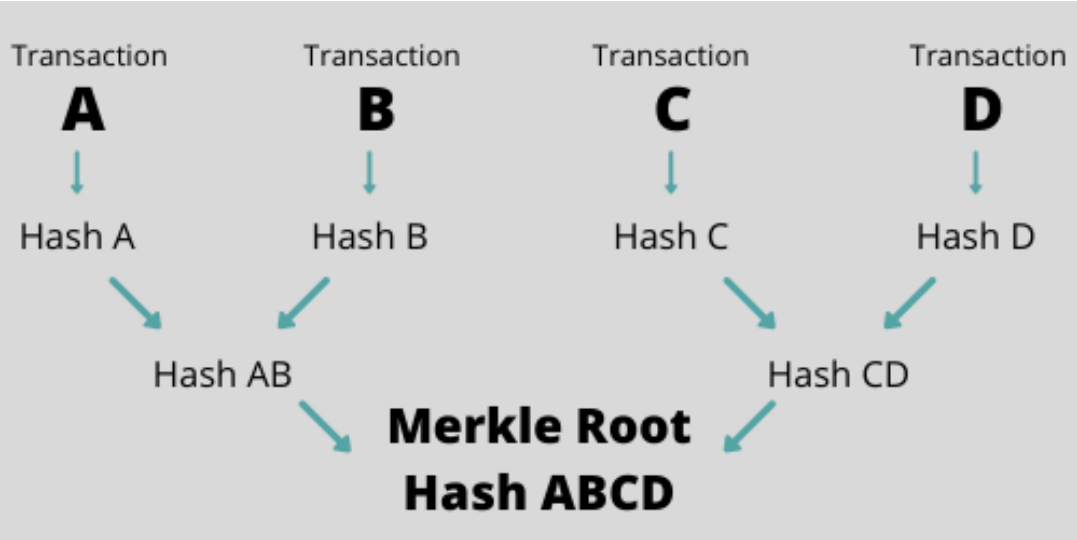
Hash AB και ***Hash CD***

Αυτοί οι δύο κατακερματισμοί κατακερματίζονται μαζί για να μας δώσουν την ρίζα του δέντρου merkle:

Hash ABCD

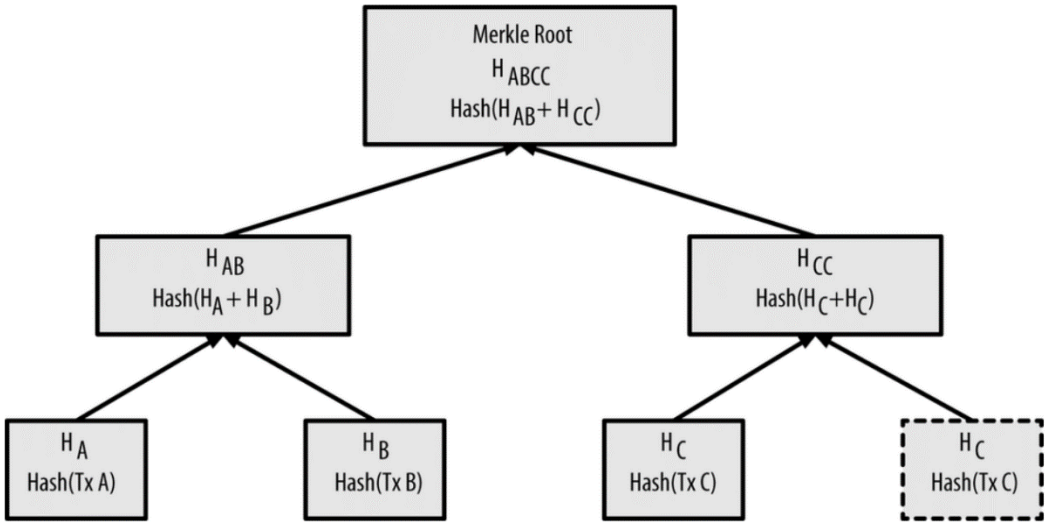
Η ρίζα merkle αποτελεί το υψηλότερο επίπεδο και διατηρεί ένα κατακερματισμό με πληροφορίες από ολόκληρο το δέντρο.

Στην πραγματικότητα, ένα δέντρο merkle είναι πολύ πιο περίπλοκο από αυτό, ειδικά όταν θεωρείτε ότι κάθε αναγνωριστικό συναλλαγής (transaction id) έχει μήκος 64 χαρακτήρων (π.χ.36ac415402e5076079944373408b789b5849d44e86f807b3683eac71e1dc106b).



Εικόνα 3.11: Κατασκευή μιας ρίζας merkle [79]

Επειδή ένα δέντρο merkle είναι ένα δυαδικό δέντρο απαιτεί ζυγό αριθμό φύλλων. Αν ο αριθμός των συναλλαγών που πρέπει να συναθροίσει είναι μονός, τότε ο κατακερματισμός της τελευταίας συναλλαγής θα αναπαραχθεί ξανά για να δημιουργήσει ένα ζυγό αριθμό από φύλλα δημιουργώντας ένα ισορροπημένο δέντρο (balanced tree) [7].



Εικόνα 3.12: Αναπαραγωγή κατακερματισμού συναλλαγής C, για επίτευξη ζυγού αριθμού φύλλων. [7]

Ένα μπλοκ συνήθως περιέχει εκατοντάδες έως και χιλιάδες συναλλαγές. Η μέθοδος που εφαρμόστηκε για την κατασκευή ενός δέντρου τεσσάρων συναλλαγών μπορεί να εφαρμοστεί για την κατασκευή δέντρων οποιουδήποτε μεγέθους. Για να αποδειχθεί ότι μια συγκεκριμένη συναλλαγή συμπεριλαμβάνεται σε ένα μπλοκ, ένας κόμβος χρειάζεται μόνο να παράγει log2(N) κατακερματισμούς, που αποτελούν μια διαδρομή ελέγχου ταυτότητας που συνδέει τη συγκεκριμένη συναλλαγή με τη ρίζα του δέντρου [7]. Αυτό είναι ιδιαίτερα σημαντικό καθώς όσο ο αριθμός των συναλλαγών μεγαλώνει τόσο πιο αργά αυξάνεται ο λογάριθμος του αριθμού των συναλλαγών.

Πλεονεκτήματα δέντρων Merkle

Ένα δέντρο merkle μπορεί να μειώσει σημαντικά τον όγκο των δεδομένων που πρέπει να διατηρηθούν για λόγους επαλήθευσης. Στην ουσία διαχωρίζει την επικύρωση των δεδομένων από τα ίδια τα δεδομένα. Τα δέντρα merkle έχουν τέσσερα σημαντικά οφέλη [79]:

1. Παρέχουν έναν τρόπο για την απόδειξη τόσο της ακεραιότητας όσο και της εγκυρότητας των δεδομένων
2. Η απαιτούμενη απόδειξη και διαχείριση χρειάζεται μόνο μικρές ποσότητες πληροφοριών για μετάδοση στο δίκτυο
3. Προσφέρει απλοποιημένη επαλήθευση πληρωμής (SPV) - ένας τρόπος επαλήθευσης συναλλαγών σε ένα μπλοκ χωρίς λήψη ολόκληρου του μπλοκ. Συχνά χρησιμοποιείται από ελαφρούς πελάτες (light client) Bitcoin.
4. Εξασφαλίζουν ότι όλα τα δεδομένα καταγράφονται και παρουσιάζονται με χρονολογική σειρά.

Τα δέντρα merkle ωφελούν τόσο τους χρήστες όσο και τους ανθρακωρύχους σε ένα Blockchain. Οι χρήστες μπορούν να επαληθεύσουν μεμονωμένα τμήματα των μπλοκ και μπορούν επίσης να ελέγξουν συναλλαγές χρησιμοποιώντας κατακερματισμούς από άλλα κλαδιά του δέντρου. Οι ανθρακωρύχοι μπορούν να υπολογίσουν κατακερματισμούς προοδευτικά καθώς λαμβάνουν συναλλαγές από τους συναδέλφους τους.

Οφέλη δέντρων Merkle για το Blockchain

Για να γίνει κατανοητό πόσο σημαντικά είναι τα δέντρα merkle για την τεχνολογία Blockchain, θα αναφερθούμε κυρίως στο κρυπτονόμισμα Bitcoin. Για παράδειγμα, εάν το Bitcoin δεν είχε δέντρα merkle, κάθε κόμβος στο δίκτυο θα έπρεπε να διατηρεί ένα πλήρες αντίγραφο κάθε συναλλαγής που έχει συμβεί ποτέ στο Bitcoin [79]. Ο κόμβος θα πρέπει να συγκρίνει κάθε γραμμή εισόδου ανά γραμμή για να βεβαιωθεί ότι οι δικές του εγγραφές και οι εγγραφές δικτύου ταιριάζουν ακριβώς. Εάν υπήρχε ασυμφωνία μεταξύ των καθολικών, θα μπορούσε να θέσει σε κίνδυνο την ασφάλεια του δικτύου.

Κάθε αίτημα επαλήθευσης στο Bitcoin θα απαιτούσε την αποστολή υπερβολικά μεγάλων πακέτων πληροφοριών μέσω του δικτύου, επειδή για να επικυρώσει ένας χρήστης τα δεδομένα θα πρέπει να έχει τα ίδια τα δεδομένα. Ο υπολογιστής που χρησιμοποιείται για επικύρωση θα πρέπει να εφαρμόσει μεγάλη ποσότητα επεξεργαστικής ισχύς για να συγκρίνει τα καθολικά για να διασφαλίσει ότι δεν υπήρξαν αλλαγές. Τα δέντρα merkle λύνουν αυτό το πρόβλημα. Κατακερματίζουν τις εγγραφές στο καθολικό, κάτι που διαχωρίζει αποτελεσματικά την απόδειξη των δεδομένων από τα ίδια τα δεδομένα. Το Ethereum χρησιμοποιεί επίσης δέντρα, ωστόσο, χρησιμοποιεί μια πιο περίπλοκη μέθοδο. Ονομάζεται Merkle Patricia Tree και χρησιμοποιεί τρεις διαφορετικές ρίζες merkle για κάθε μπλοκ [79].

Αν και δεν είναι η πιο συναρπαστική πτυχή της τεχνολογίας Blockchain, τα δέντρα Merkle είναι θεμελιώδη για την εσωτερική λειτουργία των έργων Blockchain. Χάρη στα δέντρα Merkle τα πορτοφόλια κρυπτονομισμάτων είναι σε θέση να εκτελούν ασφαλή επικύρωση συναλλαγών αποτελεσματικά σε συσκευές όπως τα κινητά τηλέφωνα, όπου οι πόροι υλικού και δικτύωσης είναι πολύ περιορισμένοι.

Μικροσυναλλαγές

Μια ξεχωριστή κατηγορία συναλλαγών στο οικοσύστημα του Blockchain είναι οι μικροσυναλλαγές. Οι μικροσυναλλαγές είναι συναλλαγές πολύ μικρών ποσών που δεν είναι βιώσιμες χρησιμοποιώντας υπάρχουσες μεθόδους πληρωμής, όπως πιστωτικές κάρτες, επειδή τα τέλη συναλλαγής θα αντιπροσώπευαν ένα μεγάλο μέρος της μεταφερόμενης αξίας [33]. Τα κρυπτονομίσματα καθιστούν τις μικροσυναλλαγές βιώσιμες, δεδομένων των χαμηλών χρεώσεων τους. Οι μικροσυναλλαγές συχνά συνδέονται με τις συναλλαγές εκτός αλυσίδας (off – chain transaction). Μια συναλλαγή εκτός αλυσίδας είναι μια συναλλαγή που είναι έγκυρη, αλλά δεν έχει δημοσιευτεί ακόμα στο Blockchain [33]. Οι συναλλαγές εκτός αλυσίδας μπορούν να χρησιμοποιηθούν για συχνές μικροπληρωμές με τον ακόλουθο τρόπο. Έστω ότι ένας χρήστης συνάπτει μια σχέση με έναν πάροχο υπηρεσιών όπως μια ηλεκτρονική εφημερίδα. Η εφημερίδα επιθυμεί να χρεώσει τον χρήστη μια μικρή χρέωση για κάθε άρθρο που διαβάζει. Την πρώτη φορά που ο χρήστης θέλει να διαβάσει ένα άρθρο, δημιουργεί μια κύρια συναλλαγή με τη μικρή τιμή του άρθρου, υπογράφει τη συναλλαγή και τη στέλνει στην διεύθυνση του πορτοφολιού της εφημερίδας. Ωστόσο, η εφημερίδα δεν την δημοσιεύει ακόμη στο Blockchain επειδή αναμένει από τον χρήστη να διαβάσει περισσότερα άρθρα και έτσι να αυξήσει το ποσό της συναλλαγής. Όταν ο χρήστης επιθυμεί να διαβάσει ένα άλλο άρθρο, η εφημερίδα στέλνει στον πελάτη την κύρια συναλλαγή με ένα ενημερωμένο ποσό που ο πελάτης υπογράφει με το ιδιωτικό του κλειδί και στέλνει πίσω στην εφημερίδα. Το πλεονέκτημα της χρήσης συναλλαγών εκτός σύνδεσης για μικροπληρωμές είναι ότι μπορούν να μεταβληθούν και να αλλάξουν την τρέχουσα κατάσταση τους.

ΚΕΦΑΛΑΙΟ 4

Πορτοφόλια Κρυπτονομισμάτων

Τα κρυπτονομίσματα είναι ένα μέσο ανταλλαγής που βασίζεται στο διαδίκτυο και χρησιμοποιεί κρυπτογραφικές λειτουργίες για τη διεξαγωγή χρηματοοικονομικών συναλλαγών. Τα κρυπτονομίσματα αξιοποιούν την τεχνολογία Blockchain για αποκέντρωση και διαφάνεια. Το πιο σημαντικό χαρακτηριστικό των περισσότερων κρυπτονομισμάτων είναι ότι δεν ελέγχονται από καμία κεντρική αρχή. Η αποκεντρωμένη φύση του Blockchain καθιστά τα κρυπτονομίσματα θεωρητικά άνοσα στους παλιούς τρόπους κυβερνητικού ελέγχου και παρέμβασης. Οι μεταφορά κρυπτονομισμάτων μπορεί να γίνει απευθείας μεταξύ των συναλλασσόμενων με τη χρήση ενός ζεύγους δημόσιου και ιδιωτικού κλειδιού. Αυτές οι μεταφορές μπορούν να γίνουν με ελάχιστα τέλη επεξεργασίας, επιτρέποντας στους χρήστες να αποφεύγουν τις μεγαλύτερες χρεώσεις που χρεώνουν τα παραδοσιακά χρηματοπιστωτικά ιδρύματα. Σήμερα, τα κρυπτονομίσματα έχουν γίνει παγκόσμιο φαινόμενο και η έννοια τους είναι γνωστή στους περισσότερους ανθρώπους. Σε αυτό το κεφάλαιο, θα αναλύσουμε τον τρόπο διαχείρισης τους μέσα από τα πορτοφόλια κρυπτονομισμάτων, τους διάφορους τύπους αυτών και το πώς αλληλοεπιδρά το καθένα με τη τεχνολογία του Blockchain.

Αγορά Κρυπτονομισμάτων

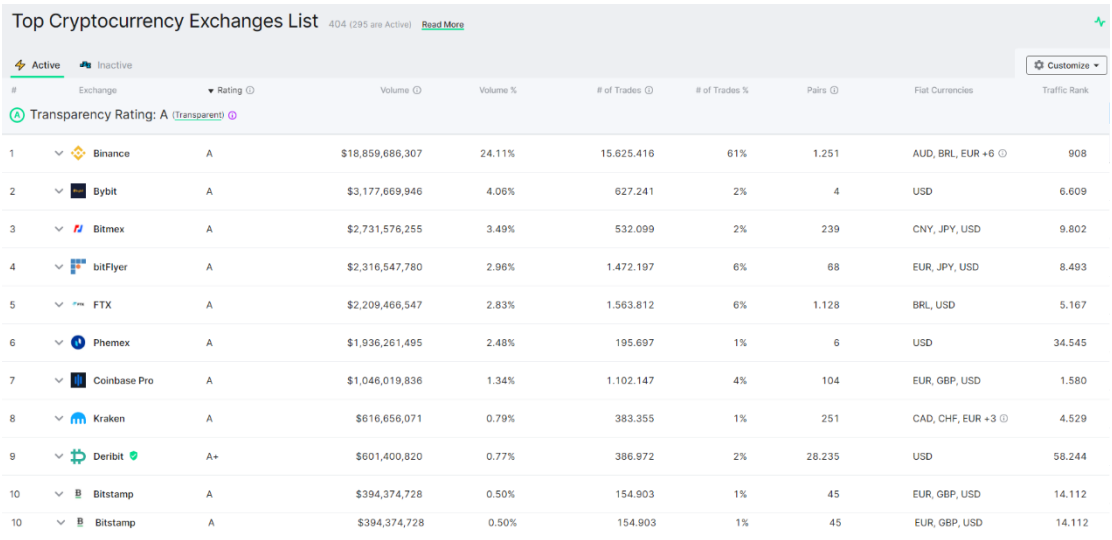
Η απόκτηση κρυπτονομισμάτων δεν μπορεί να γίνει μέσω τραπεζών ή αγορών ξένου συναλλάγματος. Ακόμη, και σήμερα εν έτη 2021 η απόκτηση τους εξακολουθεί να είναι μία δύσκολη διαδικασία σε αρκετές χώρες. Το πρόβλημα της αγοράς το οποίο δεν μπορούν να λύσουν τα χρηματοοικονομικά κέντρα καλύπτεται από συγκεκριμένα ανταλλακτήρια νομισμάτων, μέσα από τα οποία οι χρήστες μπορούν να αγοράσουν και να πωλήσουν κρυπτονομίσματα έναντι τοπικού νομίσματος. Παραδείγματα τέτοιων διαδικτυακών αγορών συναλλάγματος είναι:

Bitstamp

Το Bitstamp είναι μία πλατφόρμα ανταλλαγής συναλλάγματος με έδρα το Λουξεμβούργο. Επιτρέπει τη διαπραγμάτευση μεταξύ νομισμάτων: Ευρώ (EUR) και δολαρίων ΗΠΑ (USD) και ορισμένων κρυπτονομισμάτων, όπως Bitcoin, Litecoin, Ethereum, Ripple ή Bitcoin Cash, καθώς και ορισμένες ενέργειες όπως η κατάθεση και η ανάληψη. Το Bitstamp προσφέρει ένα API που επιτρέπει στους πελάτες να χρησιμοποιούν προσαρμοσμένο λογισμικό για την πρόσβαση και τον έλεγχο των λογαριασμών τους.

Coinbase

Η Coinbase Inc. είναι μια πλατφόρμα συναλλαγών κρυπτονομισμάτων με βάση το Σαν Φρανσίσκο των ΗΠΑ, η οποία προσφέρει υπηρεσίες αγοράς και ανταλλαγής νομισμάτων σε περίπου 32 χώρες, καθώς και αποθήκευση και διαχείριση ψηφιακών περιουσιακών στοιχείων σε 190 χώρες παγκοσμίως. Μεταξύ των νομισμάτων που υποστηρίζονται από αυτήν την πλατφόρμα είναι τα Bitcoin , Bitcoin Cash, Ethereum, Ethereum Classic και Litecoin τα διαπραγματεύονται και ανταλλάσσονται σε επίσημα νομίσματα, συμπεριλαμβανομένων των δολαρίων (USD) και του ευρώ.



Top Cryptocurrency Exchanges List 404 (295 are Active) Read More

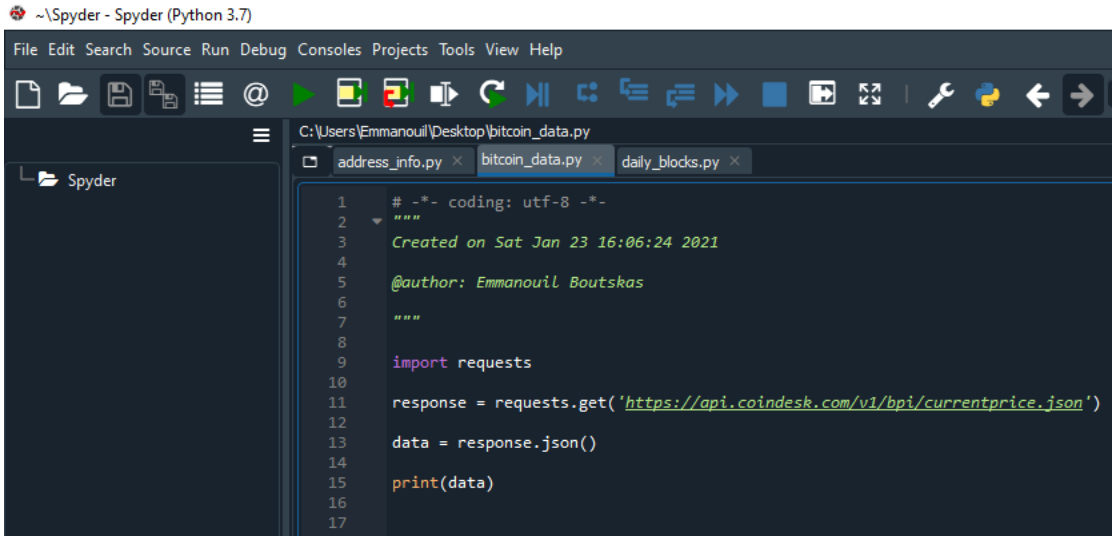
Active Inactive Customize

Transparency Rating: A (Transparent)

#	Exchange	Rating	Volume	Volume %	# of Trades	# of Trades %	Pairs	Fiat Currencies	Traffic Rank
1	Binance	A	$18,859,686,307	24.11%	15.625.416	61%	1.251	AUD, BRL, EUR +6	908
2	Bybit	A	$3,177,669,946	4.06%	627.241	2%	4	USD	6.609
3	Bitmex	A	$2,731,576,255	3.49%	532.099	2%	239	CNY, JPY, USD	9.802
4	bitFlyer	A	$2,316,547,780	2.96%	1.472.197	6%	68	EUR, JPY, USD	8.493
5	FTX	A	$2,209,466,547	2.83%	1.563.812	6%	1.128	BRL, USD	5.167
6	Phemex	A	$1,936,261,495	2.48%	195.697	1%	6	USD	34.545
7	Coinbase Pro	A	$1,046,019,836	1.34%	1.102.147	4%	104	EUR, GBP, USD	1.580
8	Kraken	A	$616,656,071	0.79%	383.355	1%	251	CAD, CHF, EUR +3	4.529
9	Deribit	A+	$601,400,820	0.77%	386.972	2%	28.235	USD	58.244
10	Bitstamp	A	$394,374,728	0.50%	154.903	1%	45	EUR, GBP, USD	14.112
10	Bitstamp	A	$394,374,728	0.50%	154.903	1%	45	EUR, GBP, USD	14.112

Εικόνα 4.1: Top 10 ανταλλακτηρίων κρυπτονομισμάτων με βάση τη κεφαλαιοποίηση αγοράς [89].

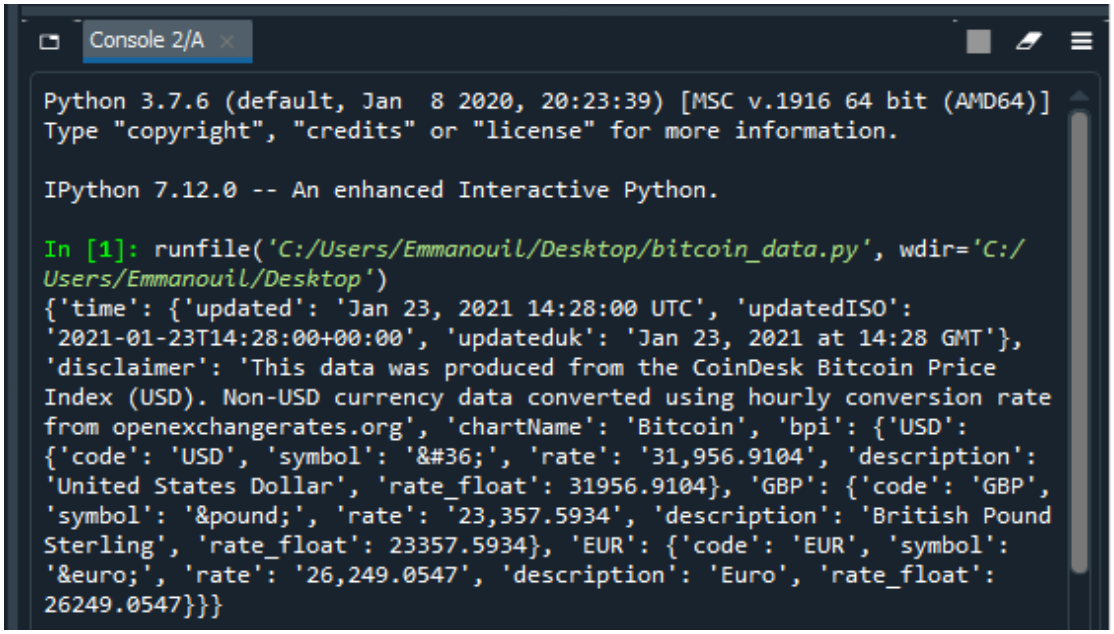
Η λειτουργία αυτών των ανταλλακτηρίων βασίζεται στην διασταύρωση των κρυπτονομισμάτων με τα εθνικά νομίσματα. Αυτό έχει ως αποτέλεσμα, να υπόκεινται σε διεθνείς και εθνικούς κανονισμούς, ενώ πολλές φορές λειτουργούν μόνο σε συγκεκριμένες οικονομικές ζώνες και χώρες. Η επιλογή του εκάστοτε ανταλλακτηρίου πρέπει να γίνεται με βάση το εθνικό νόμισμα του χρήστη και πρέπει να συμβαδίζει με τις νομοθετικές διατάξεις της χώρας. Το άνοιγμα ενός λογαριασμού σε αυτές τις υπηρεσίες είναι παρόμοιο με το άνοιγμα ενός τραπεζικού λογαριασμού, ως προς το χρονικό διάστημα, καθώς απαιτούνται αρκετές μέρες ή και εβδομάδες για την δημιουργία του. Αυτό, συμβαίνει συνήθως γιατί απαιτείται ένα είδος συμμόρφωσης με τις τραπεζικές ρυθμίσεις σχετικά με το ξέπλυμα μαύρου χρήματος (AML - Anti-Money Laundering). Στο παρακάτω παράδειγμα θα χρησιμοποιήσουμε τη βιβλιοθήκη αιτημάτων (requests) της Python και το Coindesk API για να αντλήσουμε πληροφορίες για την τρέχουσα τιμή του Bitcoin σε συναλλάγματα USD, GDB, EUR. Το API είναι δωρεάν και δεν απαιτεί έλεγχο ταυτότητας. Για να αποκτήσουμε πρόσβαση στο API του Coindesk θα χρησιμοποιήσουμε τον εξής κώδικα.



- **Γραμμή 9**: Εισαγωγή της βιβλιοθήκης αιτημάτων.
- **Γραμμή 11**: Κλήση της συνάρτησης get στη βιβλιοθήκη αιτημάτων και πέρασμα της διεύθυνσης URL του API ως παράμετρο. Εκχώρηση αυτού που επιστρέφεται σε μια μεταβλητή που ονομάζεται response
- **Γραμμή 13**: Κλήση της μεθόδου json() στη μεταβλητή response που μόλις δημιουργήσαμε. Αυτή η μέθοδος επιστρέφει το JSON που λάβαμε στην κλήση του API και εκχωρεί τα αποτελέσματα σε μια μεταβλητή που ονομάζεται data.

- **Γραμμή 15**: Εκτύπωση των δεδομένων JSON.

Αποτέλεσμα:



Μετά από μία μορφοποίηση της παραπάνω εικόνας το τελικό αποτέλεσμα έχει την εξής μορφή:


```
{
   "time":{
      "updated":" Jan 23, 2021 14:28:00 UTC",
      "updatedISO":" 2021-01-23T14:28:00+00:00",
      "updateduk":" Jan 23, 2021 at 14:28 GMT"
   },

   "disclaimer":'This data was produced from the CoinDesk Bitcoin Price Index (USD).
   'Non-USD currency data converted using hourly conversion rate from openexchangerates.org',

   "chartName":"Bitcoin",
   "bpi":{

      "USD":{
         "code":"USD",
         "symbol":"&#36;",
         "rate":"31,956.9104",
         "description":"United States Dollar",
         "rate_float":31956.9104
      },
      "GBP":{
         "code":"GBP",
         "symbol":"&pound;",
         "rate":"23,357.5934",
         "description":"British Pound Sterling",
         "rate_float":23357.5934
      },
      "EUR":{
         "code":"EUR",
         "symbol":"&euro;",
         "rate":"26,249.0547",
         "description":"Euro",
         "rate_float":26249.0547
      }
   }
}
```

Πορτοφόλια Κρυπτονομισμάτων

Τα πορτοφόλια κρυπτονομισμάτων είναι ψηφιακά πορτοφόλια που χρησιμοποιούνται για τη λήψη, αποστολή και αποθήκευση ψηφιακών νομισμάτων όπως το Bitcoin ή το Ethereum, μεταξύ άλλων νομισμάτων. Χρησιμοποιούν μηχανισμούς κρυπτογράφησης για την εξασφάλιση των συναλλαγών και γι' αυτό τον λόγο, περιλαμβάνουν τη χρήση ιδιωτικών και δημόσιων κλειδιών [88]. Ένα δημόσιο κλειδί ενεργεί όπως ένα αναγνωριστικό λογαριασμού για ένα άτομο (π.χ. όνομα διεύθυνσης email), ενώ ένα ιδιωτικό κλειδί ενεργεί ως κωδικός πρόσβασης που απαιτείται για τη χρήση του κρυπτονομίσματος (π.χ. pin κάρτας για χρήση ATM). Ένας αποστολέας θα απαιτήσει τη δημόσια διεύθυνση (δημόσιο κλειδί) του παραλήπτη για να του στείλει κρυπτονομίσματα και ο παραλήπτης θα μπορεί να έχει πρόσβαση και να χρησιμοποιεί αυτά τα κρυπτονομίσματα χρησιμοποιώντας το ιδιωτικό του κλειδί [41]. Παρόλο, που τα κλειδιά είναι συνδεδεμένα μεταξύ τους δεν μπορεί να προκύψει το ένα από το άλλο. Με άλλα λόγια, αν ο αποστολέας γνωρίζει το δημόσιο κλειδί του παραλήπτη, δεν μπορεί να προσδιορίσει το ιδιωτικό του κλειδί. Δεδομένου, ότι τα ιδιωτικά κλειδιά χρησιμοποιούνται για την απόκτηση πρόσβασης στα κρυπτονομίσματα είναι απολύτως απαραίτητο να διατηρούνται ασφαλή και μυστικά για την αποφυγή τυχών εισβολής, κλοπής και άλλων επιθέσεων [41].

Τρόπος Λειτουργίας Πορτοφολιών

Σε αντίθεση με τα ανταλλακτήρια κρυπτονομισμάτων που επιτρέπουν την αγορά και πώληση κρυπτονομισμάτων με πραγματικά χρήματα όπως δολάρια (US) και ευρώ (EUR), οι εφαρμογές πορτοφολιών χρησιμοποιούνται για την αποθήκευση, την αποστολή και τη λήψη κρυπτονομισμάτων (ορισμένα πορτοφόλια ενδέχεται να έχουν ενσωματωμένες λειτουργίες για τη μετατροπή κρυπτονομισμάτων σε πραγματικά χρήματα και το αντίστροφο) [88]. Μόλις ένας χρήστης αγοράσει κρυπτονομίσματα από ένα ανταλλακτήριο, αποθηκεύονται στον λογαριασμό του σε αυτό. Η αποθήκευση των κρυπτονομισμάτων στο πορτοφόλι που παρέχεται από το ανταλλακτήριο ωστόσο δεν συνιστάται, λόγω του γεγονότος ότι σε αυτήν την περίπτωση, το ανταλλακτήριο θα κατέχει το ιδιωτικό κλειδί του χρήστη και όχι ο ίδιος. Ως εκ τούτου, είναι προτιμότερο η μεταφορά και η αποθήκευση τους να γίνεται σε κάποια εξειδικευμένη εφαρμογή

πορτοφολιού προκειμένου ο χρήστης να έχει τον πλήρη έλεγχο των κρυπτονομισμάτων του [88]. Για να γίνει αυτό, πρέπει πρώτα να δημιουργήσει ένα δημόσιο κλειδί (δημόσια διεύθυνση) και ένα ιδιωτικό κλειδί στο πορτοφόλι του. Εν συνεχεία, μπορεί να μεταφέρει τα κρυπτονομίσματα από το ανταλλακτήριο στο πορτοφόλι του χρησιμοποιώντας τη διεύθυνση δημόσιου κλειδιού. Μόλις γίνει αυτό, μπορεί εύκολα να εκτελέσει συναλλαγές και να στείλει κρυπτονομίσματα σε άλλους λογαριασμούς χρησιμοποιώντας τα δημόσια κλειδιά τους και να λάβει κρυπτονομίσματα στον λογαριασμό του κοινοποιώντας το δημόσιο κλειδί του στον αποστολέα. Η ύπαρξη δημόσιου και ιδιωτικού κλειδιού βασίζεται στην τεχνική της ασύμμετρης κρυπτογραφίας [41].

Τύποι Πορτοφολιών

Τα πορτοφόλια κρυπτονομισμάτων χωρίζονται ως επί πρωτίστως σε «Ζεστά» (διαδικτυακά πορτοφόλια) και «Κρύα» (μη συνδεδεμένα στο διαδίκτυο). Τα πορτοφόλια που είναι αποθηκευμένα σε οποιονδήποτε ιστότοπο/βάση δεδομένων ονομάζονται διαδικτυακά πορτοφόλια (online wallets). Τα πορτοφόλια αυτά ονομάζονται επίσης πορτοφόλια ιστού (web wallets) ή φιλοξενούμενα πορτοφόλια (hosted wallets) [33]. Τα διαδικτυακά πορτοφόλια δεν συνίστανται για την αποθήκευση μεγάλων ποσοτήτων κρυπτονομισμάτων ή την αποθήκευση κρυπτονομισμάτων για μεγάλο χρονικό διάστημα επειδή είναι ριψοκίνδυνα. Επίσης, ανάλογα με τον τόπο αποθήκευσης του πορτοφολιού, ενδέχεται να απαιτείται εμπιστοσύνη σε τρίτο μέρος [24]. Για παράδειγμα, οι περισσότερες από τις δημοφιλείς υπηρεσίες πορτοφολιού αποθηκεύουν τα ιδιωτικά κλειδιά των πορτοφολιών και επιτρέπουν στους χρήστες να έχουν πρόσβαση στο πορτοφόλι τους μέσω e-mail και κωδικού πρόσβασης. Αυτό βασικά σημαίνει, ότι οι χρήστες δεν έχουν πραγματική πρόσβαση και πλήρη έλεγχο του πορτοφολιού τους, διότι αν θέλουν μπορούν να κλέψουν τα χρήματα από το πορτοφόλι τους.

Από την άλλη πλευρά, ένα πορτοφόλι λέγεται ότι είναι ένα πορτοφόλι χωρίς σύνδεση (offline wallet) όταν δεν είναι συνδεδεμένο στο Διαδίκτυο. Για παράδειγμα, πορτοφόλια που είναι αποθηκευμένα σε μονάδες usb, χαρτιά, αρχεία κειμένου και ούτω καθεξής. Τα offline wallets ονομάζονται επίσης «κρύα» πορτοφόλια (cold wallets) [33]. Τα πορτοφόλια αυτά είναι πιο ασφαλή από τα διαδικτυακά πορτοφόλια, επειδή

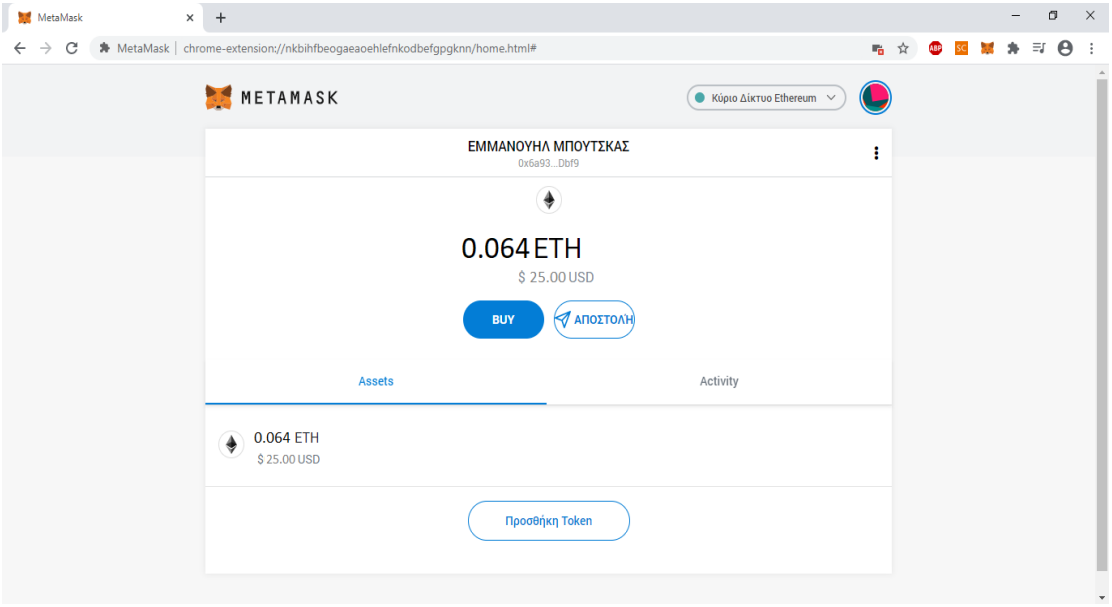
για να υπάρξει κλοπή χρήματων, κάποιος θα χρειαστεί φυσική πρόσβαση στον χώρο αποθήκευσης. Οι προκλήσεις με τα offline πορτοφόλια είναι ότι χρειάζεται να είναι αποθηκευμένα σε ασφαλές μέρος που δεν πρόκειται να χαθεί η πρόσβαση σε αυτό. Πολλοί χρήστες αποθηκεύουν το πορτοφόλι τους σε χαρτί (paper wallets) και διατηρούν αυτό το χαρτί σε ένα ασφαλές συρτάρι, θυρίδα ασφαλείας κλπ., εάν θέλουν να κρατήσουν κάποια χρήματα με ασφάλεια για πολύ καιρό [33]. Σε περίπτωση που η αποθήκευση γίνεται σε ψηφιακή συσκευή οι χρήστες πρέπει να είναι περισσότερο προσεκτικοί, καθώς οι ψηφιακές συσκευές μπορεί να καταστραφούν οποιαδήποτε στιγμή και έτσι να χάσουν την πρόσβαση στο πορτοφόλι τους. Η καλύτερη λύση για την επιλογή offline πορτοφολιού γίνεται ανάλογα με τις ανάγκες του εκάστοτε χρήστη, αφού πρώτα βεβαιωθεί ότι είναι ασφαλές και δεν θα χαθεί η πρόσβαση σε αυτό.

Πορτοφόλια Ιστού (Web wallets)

Τα πορτοφόλια ιστού λειτουργούν ως διαδικτυακές πλατφόρμες για συναλλαγές κρυπτονομισμάτων και είναι προσβάσιμα μέσω προγραμμάτων περιήγησης ιστού όπως το Google Chrome, το Mozilla Firefox, το Opera κ.λπ [88]. Παρέχουν μια εμπειρία παρόμοια με τις διαδικτυακές τραπεζικές υπηρεσίες και μπορούν να συνδεθούν αυτόματα στον τραπεζικό λογαριασμό του χρήστη. Οι χρήστες έχουν τη δυνατότητα πρόσβασης στο πορτοφόλι τους από οποιαδήποτε συσκευή, ενώ οι συναλλαγές ολοκληρώνονται σε σύντομο χρονικό διάστημα. Εκτός αυτού, υπάρχουν πρόσθετα πλεονεκτήματα, όπως χαμηλές προμήθειες για συναλλαγές ή δυνατότητα διευθέτησης συναλλαγών μεταξύ των χρηστών της ίδιας υπηρεσίας άμεσα και με μηδενικά τέλη [33].

Ωστόσο, η χρήση διαδικτυακών πορτοφολιών έχει επιπτώσεις στο απόρρητο. Το γεγονός ότι ο πλήρης έλεγχος του ψηφιακού πορτοφολιού δεν βρίσκεται στο χέρι του χρήστη αποτελεί ένα μεγάλο μειονέκτημα. Υπάρχει μειωμένη ανωνυμία από την πλευρά του χρήστη, επειδή ο πάροχος του διαδικτυακού πορτοφολιού διατηρεί συνήθως αρχείο των συναλλαγών και προσωπικών πληροφοριών των χρηστών του [33]. Παρόλο, που είναι πιο βολικά στην πρόσβαση, τα διαδικτυακά πορτοφόλια αποθηκεύουν τα ιδιωτικά κλειδιά στο διαδίκτυο και ελέγχονται από τρίτο μέρος (πάροχο του πορτοφολιού) που τα καθιστά πιο ευάλωτα και επιρρεπή σε hacking και

online επιθέσεις. Μερικά από τα διαθέσιμα πορτοφόλια Ιστού στην αγορά είναι τα Coinbase, BitGo, Copay κ.λπ [88].



Εικόνα 4.2: MetaMask web wallet. Υπόλοιπο λογαριασμού

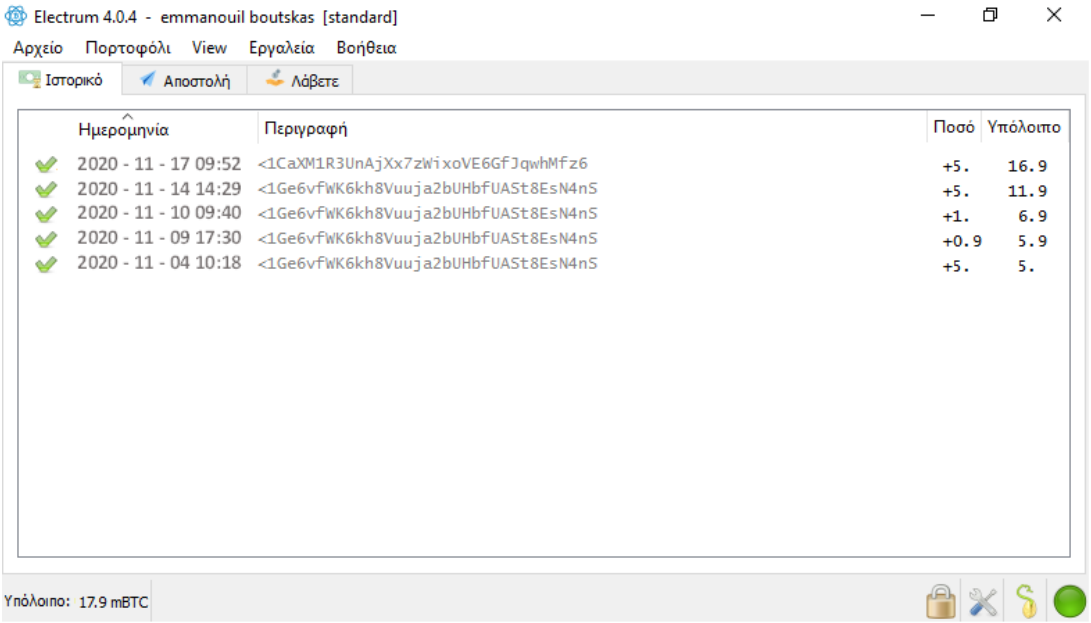
- **Υβριδικά πορτοφόλια ιστού (Hybrid web wallets)**

  Μετά την παραβίαση αρκετών διαδικτυακών πορτοφολιών, ένα δεύτερο κύμα διαδικτυακών πορτοφολιών μπήκε στην αγορά. Τα υβριδικά πορτοφόλια χρησιμοποιούν Javascript στο πρόγραμμα περιήγησης του χρήστη για τη διαχείριση ιδιωτικών κλειδιών και τη δημιουργία πληρωμών [83]. Αυτά τα πορτοφόλια διαφέρουν από τις παραδοσιακές διαδικτυακές υπηρεσίες πορτοφολιών επειδή τα ιδιωτικά κλειδιά αποθηκεύονται τοπικά στον υπολογιστή του χρήστη ενώ ο πάροχος του πορτοφολιού αναλαμβάνει την διαχείριση του λογισμικού. Οι συναλλαγές δημοσιεύονται στο Blockchain από τον πάροχο του πορτοφολιού. Αυτή η προσέγγιση δίνει το πλεονέκτημα στον χρήστη να αναζητήσει το υπόλοιπο του λογαριασμού του στο Blockchain, κάτι που εγγυάται ότι το υπόλοιπο του λογαριασμού του είναι όντως σωστό [83].

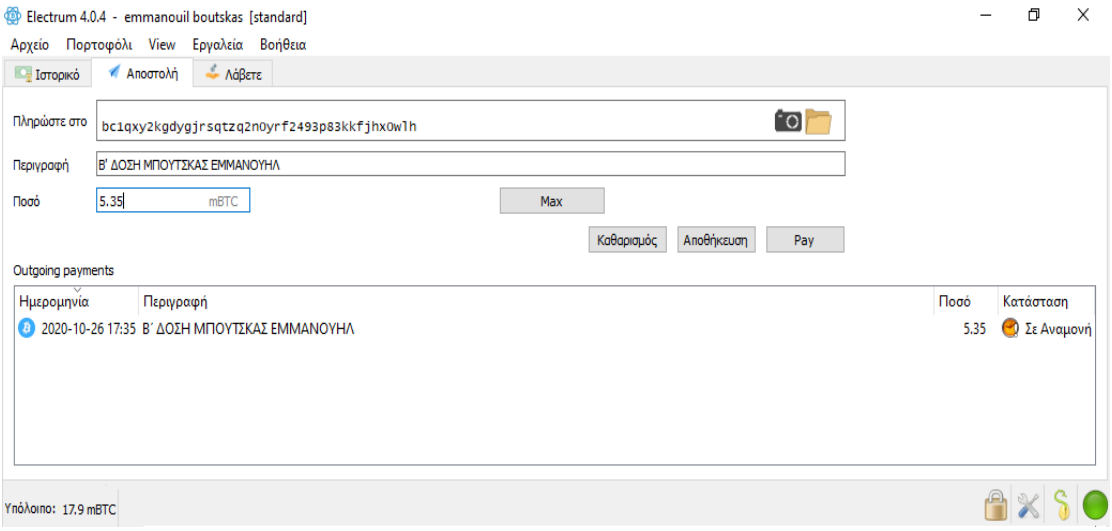
Πορτοφόλια Επιφάνειας Εργασίας (Desktop Wallets)

Τα πορτοφόλια υπολογιστή θεωρούνται ασφαλέστερα σε σύγκριση με τα διαδικτυακά και κινητά πορτοφόλια και σε γενικές γραμμές, προσφέρουν έναν καλό συνδυασμό ασφάλειας και ευκολίας. Ο βαθμός ασφάλειας ωστόσο, σχετίζεται άμεσα με την ποιότητα της προστασίας του υπολογιστή από διαδικτυακές απειλές, όπως ιούς υπολογιστών και κακόβουλο λογισμικό. Ένα πορτοφόλι υπολογιστή διαθέτει ένα χαρακτηριστικό που μπορεί να το αναγνωρίσει ως «κρύο» πορτοφόλι [42]. Όταν ο υπολογιστής δεν είναι συνδεδεμένος στο διαδίκτυο, είναι αδιαπέραστο από διαδικτυακές απειλές όπως χάκερ, ιούς κ.λπ. Το κύριο πλεονέκτημα τους πηγάζει από την διαχείριση των ιδιωτικών κλειδιών, καθώς δεν αποθηκεύονται σε διακομιστή τρίτου μέρους αλλά στον ίδιο τον υπολογιστή, εξαλείφοντας την ανάγκη να βασίζονται σε τρίτους [42]. Επειδή οι χρήστες έχουν τον έλεγχο των ιδιωτικών κλειδιών τους μπορούν να κρυπτογραφήσουν το πορτοφόλι τους για να αποφύγουν απόπειρες εισβολής.

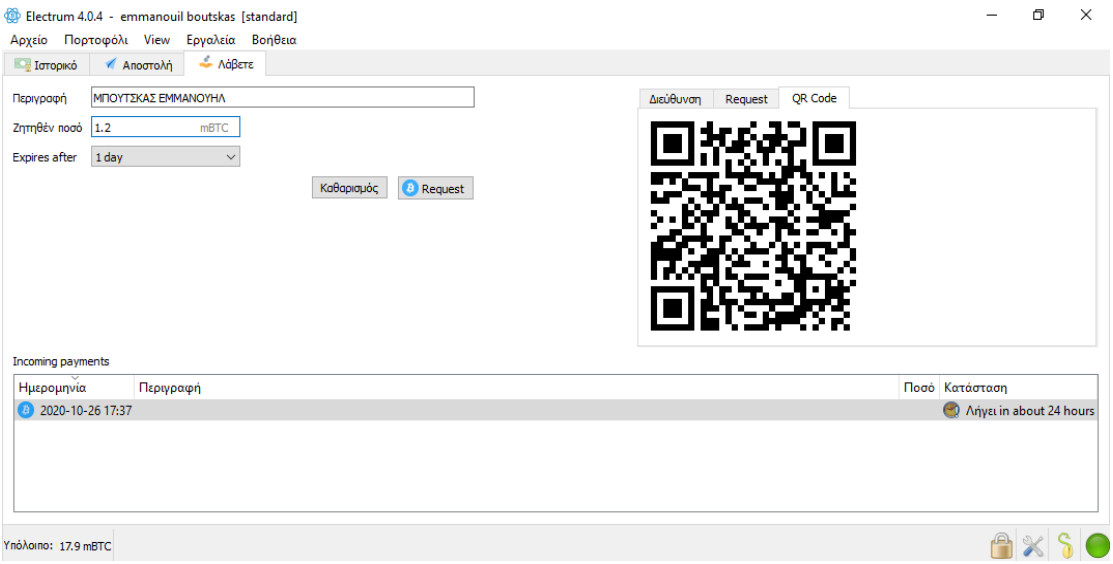
Το μοναδικό μειονέκτημα τους εμφανίζεται στην περίπτωση που ο υπολογιστής είναι συνδεδεμένος στο διαδίκτυο. Τα επιτραπέζια πορτοφόλια τότε διατρέχουν τον κίνδυνο να επηρεαστούν από έναν ιό ή κακόβουλο λογισμικό υπολογιστή. [42] Υπήρξαν πολλές περιπτώσεις κλοπής σε desktop πορτοφόλια όπου μερικοί χάκερ κατάφεραν να κλέψουν Bitcoin αξίας εκατομμυρίων δολαρίων. Τα desktop πορτοφόλια είναι ιδανικά για την αποθήκευση μικρών ποσοτήτων κρυπτονομισμάτων. Δεν ενδείκνυται για αποθήκευση μεγάλου αριθμού κρυπτονομισμάτων, και είναι καλύτερο να μεταφέρονται σε αποθηκευτικό χώρο εκτός σύνδεσης ή κρύα πορτοφόλια. Γι’ αυτό τον λόγο, είναι απαραίτητη η τακτική δημιουργία αντιγράφων ασφαλείας γιατί σε κάποιο σημείο το σύστημα μπορεί να καταρρεύσει ή να κλαπεί και να χαθούν όλα τα περιουσιακά στοιχεία του χρήστη. Παραδείγματα επιτραπέζιων πορτοφολιών είναι εφαρμογές για επιτραπέζιους υπολογιστές, όπως Exodus, Multibit, Armory, και Bitcoin Core.



Εικόνα 4.2.1: Electrum wallet, στην αριστερή πλευρά εμφανίζεται το ιστορικό των συναλλαγών, ενώ στην δεξιά πλευρά το διαθέσιμο υπόλοιπο σε mBTC



Εικόνα 4.2.2: Συναλλαγή αποστολής mBTC



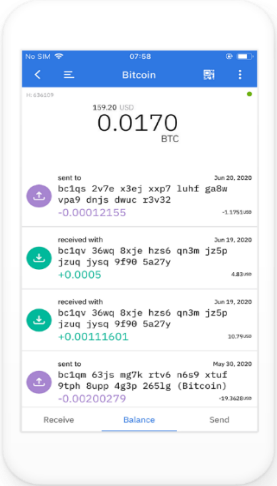
Εικόνα 4.2.3: Συναλλαγή λήψης mBTC.

Πορτοφόλια Κινητών Συσκευών (Mobile Wallets)

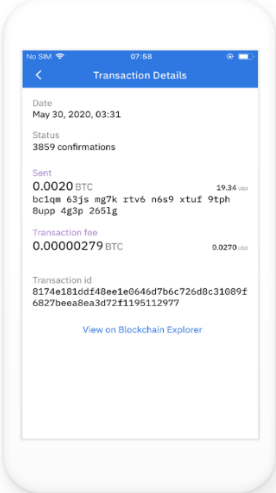
Τα κινητά πορτοφόλια λειτουργούν ακριβώς όπως τα πορτοφόλια επιτραπέζιων υπολογιστών, αλλά είναι εφαρμογές ειδικά σχεδιασμένες για κινητά τηλέφωνα. Αυτές οι εφαρμογές είναι πολύ βολικές και εύχρηστες καθώς επιτρέπουν την αποστολή και λήψη ψηφιακών νομισμάτων μέσω της χρήσης κωδικών QR [44]. Ως εκ τούτου, τα κινητά πορτοφόλια είναι ιδιαίτερα κατάλληλα για την ολοκλήρωση καθημερινών συναλλαγών και πληρωμών, καθιστώντας τα μια βιώσιμη επιλογή για περιπτώσεις όπου οι χρήστες βρίσκονται σε εξωτερικούς χώρους, προσπαθώντας να υλοποιήσουν μία συναλλαγή σε κάποιο φυσικό κατάστημα. Τρέχουν εύκολα σε Android και iOS λειτουργικά συστήματα ως εγγενής (native) εφαρμογές αποθηκεύοντας τα ιδιωτικά κλειδιά και τις διευθύνσεις των κρυπτονομισμάτων, επιτρέποντας την άμεση πληρωμή μέσα από το κινητό εύκολα και γρήγορα. Ένα άλλο κοινό χαρακτηριστικό των mobile wallets είναι ότι δεν είναι πλήρεις πελάτες (full clients) [7]. Οι πλήρεις clients είναι σε θέση να κατεβάζουν ολόκληρο το Blockchain το οποίο έχει χωρητικότητα αρκετά gigabyte. Ως εκ τούτου, ένα κινητό τηλέφωνο δεν είναι σε θέση να φέρει εις πέρας κάτι τέτοιο, καθώς αυτό θα οδηγήσει στην εμφάνιση προβλημάτων ως προς την λειτουργικότητα και την χωρητικότητα του. Αυτός είναι και ο λόγος που η σχεδίαση

τους βασίζεται σε απλή επαλήθευση πληρωμής (Simple Payment Verification – SPV) [43].

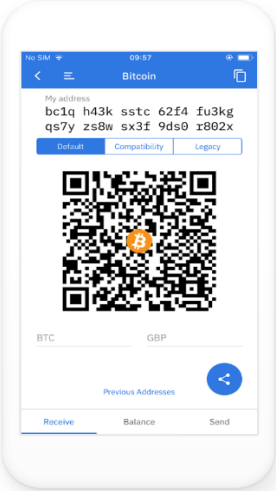
Κατεβάζουν μόνο ένα μικρό κομμάτι του Blockchain. Για να το επιτύχουν αυτό βασίζονται σε έμπιστους κόμβους του δικτύου, με αυτό τον τρόπο σιγουρεύονται ότι έχουν τις σωστές πληροφορίες που χρειάζονται [43]. Ορισμένα παραδείγματα mobile wallets android λειτουργικού συστήματος είναι τα: Blockchain, Bitcoin wallet, Xapo, Coinbase, Coinomi, Mycelium και το Aegis Bitcoin wallet που μπορεί να υποστηρίξει android smart watches. Ωστόσο, υπάρχουν επιπλέων τύποι πορτοφολιών που μπορούν να χρησιμοποιηθούν από ένα smartphone, όπως η web εφαρμογή Coinpunk.



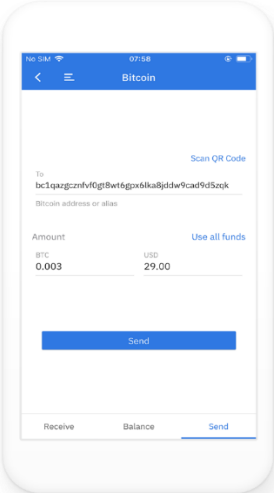
Εικόνα 4.2.4: Συναλλαγές και υπόλοιπο πορτοφολιού Coinomi



Εικόνα 4.2.5: Λεπτομέρειες συναλλαγής που υλοποιήθηκε



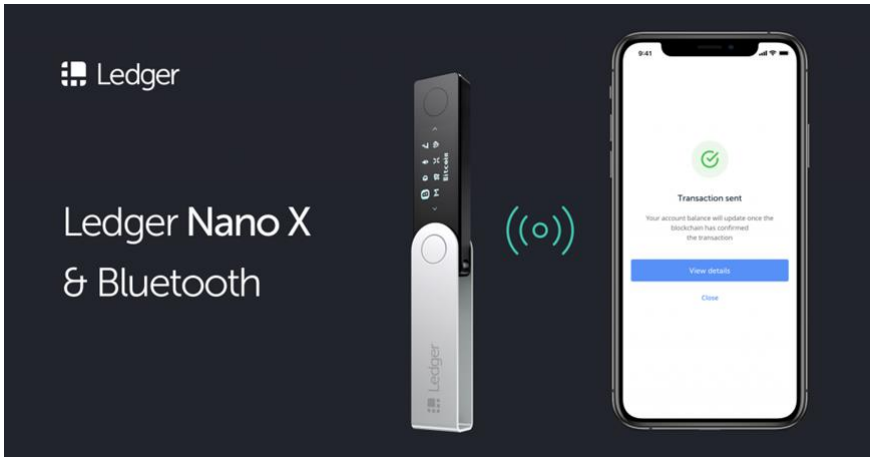
Εικόνα 4.2.6: Διεύθυνση λήψης Bitcoin



Εικόνα 4.2.7: Λεπτομέρειες αποστολής Bitcoin

Πορτοφόλια Υλικού (Hardware Wallets)

Τα πορτοφόλια υλικού είναι συσκευές που αποθηκεύουν ιδιωτικά κλειδιά και υπογράφουν συναλλαγές με αυτά τα ιδιωτικά κλειδιά. Τα ιδιωτικά κλειδιά δεν φεύγουν ποτέ από τη συσκευή, επομένως δεν μπορούν να δεχτούν επίθεση και να υποκλαπούν από κακόβουλο λογισμικό εγκατεστημένο στον υπολογιστή του χρήστη [33]. Τα πορτοφόλια αυτά μπορούν να συνδεθούν μέσω υπολογιστών και να χρησιμοποιηθούν με διαδικτυακά λογισμικά, όπως ένα πορτοφόλι ιστού που εκτελείται μέσα σε ένα πρόγραμμα περιήγησης ιστού. Ο ρόλος αυτών των λογισμικών είναι να ενεργούν ως μεσάζων μεταξύ του πορτοφολιού υλικού και του Blockchain, μεταδίδοντας απλώς τις συναλλαγές που υπογράφονται μέσα στο πορτοφόλι υλικού. Οι συναλλαγές υπογράφονται μέσα σε ένα αξιόπιστο υπολογιστικό περιβάλλον στο υλικό (π.χ. το ARM TrustZone) και τα ιδιωτικά κλειδιά δεν είναι εκτεθειμένο στον κεντρικό υπολογιστή [33]. Όλες οι διαδικασίες που απαιτούνται για την διεκπεραίωση μιας συναλλαγής γίνονται μέσα στο πορτοφόλι και όχι στον υπολογιστή στον οποίο είναι συνδεδεμένο. Επομένως, ακόμη και αν ο υπολογιστής παραβιαστεί, οι εισβολείς δεν θα μπορούν να κλέψουν τα κλειδιά του χρήστη. Τα πορτοφόλια υλικού έχουν συνήθως μια μικρή οθόνη για εμφάνιση των πληροφοριών του χρήστη σχετικά με τη συναλλαγή και ορισμένα κουμπιά που επιτρέπουν στον χρήστη να αποφασίσει εάν θα υπογράψει τη συναλλαγή ή θα την απορρίψει. Επιπρόσθετα, ένα κοινό χαρακτηριστικό τους είναι ότι απαιτείται εισαγωγή κωδικού πρόσβασης (PIN) για επιβεβαίωση συναλλαγών [33]. Επειδή, τα ιδιωτικά και δημόσια κλειδιά αποθηκεύονται φυσικά σε κάποια συσκευή υλικού, παρέχουν υψηλότερο επίπεδο ασφάλειας, καθώς είναι λιγότερο ευάλωτα σε διαδικτυακές επιθέσεις και ως εκ τούτου χαρακτηρίζονται ως η ασφαλέστερη επιλογή**.**



Εικόνα 4.2.8: Πορτοφόλι υλικού Ledger Nano X. Διαθέτει συνδεσιμότητα Bluetooth χαμηλής ενέργειας (Bluetooth Low Energy - BLE) που επιτρέπει τη χρήση του με συσκευές Android ή iOS χωρίς την ανάγκη καλωδίου.

Πορτοφόλια Χαρτιού (Paper Wallets)

Τα πορτοφόλια χαρτιού αναφέρονται σε ένα φυσικό αντίγραφο των δημόσιων και ιδιωτικών κλειδιών που είναι απλώς ένα κομμάτι χαρτί. Θεωρείται ένας από τους ασφαλέστερους τύπους πορτοφολιών καθώς δεν είναι επιρρεπές σε διαδικτυακούς κινδύνους απώλειας του ιδιωτικού κλειδιού. Επομένως, δεν είναι εκτεθειμένο σε μεγάλο βαθμό σε απειλές στον κυβερνοχώρο. Το ιδιωτικό κλειδί και η δημόσια διεύθυνση αναπαρίστανται σε κωδικούς QR, και χρησιμοποιούνται κατά την εκτέλεση οποιωνδήποτε συναλλαγών, καθιστώντας την διαδικασία λιγότερο επιρρεπής σε σφάλματα πληκτρολόγησης. Υπάρχουν διαδικτυακοί ιστότοποι που δημιουργούν εκτυπώσιμα πορτοφόλια (π.χ. www.bitaddress.org) [33].

Εικόνα 4.2.9: Χάρτινο πορτοφόλι: Στα αριστερά της εικόνας εμφανίζεται η διεύθυνση μαζί με την αναπαράσταση του κωδικού QR. Στη δεξιά πλευρά εμφανίζεται το ιδιωτικό κλειδί, κωδικοποιημένο σε μορφή WIF, και ο σχετικός κωδικός QR.

Ταξινόμηση Πορτοφολιών με Βάση τον Τρόπο Σύνδεσης στο Δίκτυο

Όπως αναφέραμε νωρίτερα, οι υπολογιστές και τα κινητά τηλέφωνα που συνδέονται με το δίκτυο Blockchain είναι γνωστοί ως κόμβοι. Αυτοί οι κόμβοι ανάλογα με τον τρόπο που αλληλοεπιδρούν με το δίκτυο χωρίζονται σε δύο κατηγορίες: πλήρης κόμβος και ελαφρύς κόμβος.

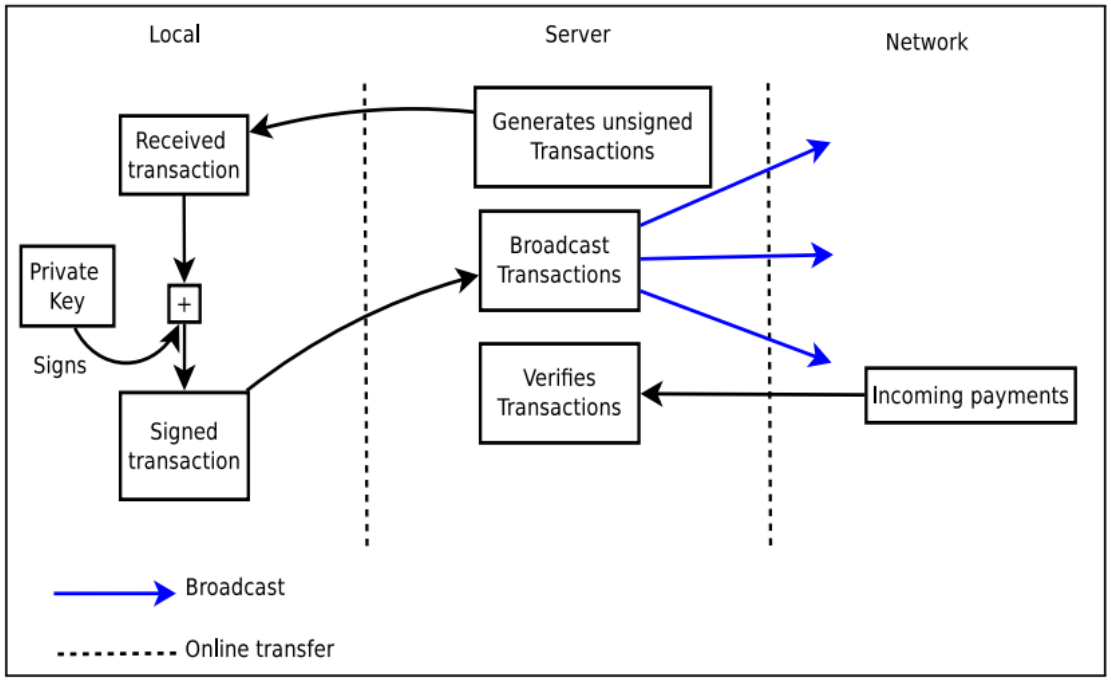
Πλήρης Κόμβος (Full Node)

Τα πορτοφόλια που διατηρούν ένα πλήρες αντίγραφο του Blockchain ονομάζονται πλήρεις κόμβοι [38]. Αυτά τα πορτοφόλια έχουν το πλεονέκτημα ότι δεν χρειάζεται να βασίζονται σε οποιονδήποτε τρίτο διακομιστή, αντιθέτως αποθηκεύουν και επεξεργάζονται ολόκληρη τη βάση δεδομένων των συναλλαγών, καθιστώντας τα περισσότερο ασφαλή σε σχέση με τα ελαφριά πορτοφόλια [33]. Επειδή δεν εξαρτώνται από κανέναν τρίτο προσφέρουν ταυτόχρονα και καλύτερο απόρρητο από την πλευρά του χρήστη. Ένας πλήρης κόμβος ουσιαστικά είναι ένα πρόγραμμα που επικυρώνει πλήρως τις συναλλαγές και τα μπλοκ [7]. Οι περισσότεροι πλήρεις κόμβοι εξυπηρετούν επίσης ελαφρούς πελάτες (lightweight clients) επιτρέποντάς τους να μεταδίδουν τις συναλλαγές τους στο δίκτυο και ειδοποιώντας τους όταν μια συναλλαγή πρόκειται να λάβει δράση από το πορτοφόλι τους.

Ωστόσο, καταναλώνουν αρκετούς πόρους καθώς καταλαμβάνουν τεράστιο χώρο στον δίσκο του υπολογιστή. Αυτό συμβαίνει επειδή κατεβάζουν ολόκληρο το ιστορικό συναλλαγών που συνέβη ποτέ στο Blockchain. Για παράδειγμα, το μέγεθος του Blockchain του Bitcoin είναι πάνω από 300 GB, πράγμα που σημαίνει ότι μόλις δημιουργηθεί το πορτοφόλι πρέπει να κατεβάσει όλο το ποσό αυτών των δεδομένων [90]. Αυτός είναι και ο λόγος που η εγκατάσταση τους αργεί τόσο πολύ συγκριτικά με τα ελαφριά πορτοφόλια, όπου κατεβάζουν μόνο τις κεφαλίδες των block απαιτώντας ελάχιστο χώρο και χρόνο.

Ελαφρύς Κόμβος (Lightweight Node)

Εκτός από τους πλήρεις κόμβους, υπάρχουν επίσης και οι ελαφριοί κόμβοι. Οι ελαφριοί κόμβοι βοηθούν στην επαλήθευση συναλλαγών χρησιμοποιώντας μια μέθοδο που ονομάζεται απλοποιημένη επαλήθευση πληρωμής (Simplified Payment Verification - SPV) [39]. Αυτή η μέθοδος επιτρέπει σε έναν κόμβο να επαληθεύσει εάν μια συναλλαγή έχει συμπεριληφθεί σε ένα μπλοκ, χωρίς να χρειάζεται να κάνει λήψη ολόκληρου του Blockchain. Χρησιμοποιώντας την απλοποιημένη επαλήθευση πληρωμής, οι ελαφριοί κόμβοι συνδέονται σε πλήρεις κόμβους και μεταδίδουν συναλλαγές σε αυτούς για επαληθεύσεις. Οι ελαφριοί κόμβοι αποθηκεύουν μόνο τις κεφαλίδες όλων των μπλοκ του Blockchain. Ένα παράδειγμα ενός ελαφριού κόμβου είναι η εφαρμογή Coinbase για κινητά iOS και Android. Χρησιμοποιώντας ένα κινητό πορτοφόλι, ένας χρήστης μπορεί να εκτελεί συναλλαγές στην κινητή συσκευή [40].



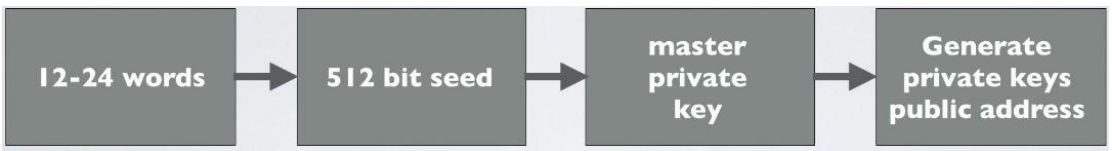
Εικόνα 4.3: Λειτουργιές light node πορτοφολιού [40]

Από την άποψη της δικτύωσης, τα περισσότερα ελαφριά πορτοφόλια, ειδικά αυτά των κινητών τηλεφώνων, δεν συνδέονται σε P2P δίκτυο. Αντ' αυτού, στέλνουν συναλλαγές στον διακομιστή του παρόχου του πορτοφολιού μέσω του πρωτοκόλλου TLS, ο οποίος με τη σειρά του τις μεταδίδει το δίκτυο P2P [39].

Αυτό αποτελεί αναμφισβήτητα μια σοβαρή απειλή απορρήτου επειδή ο πάροχος του πορτοφολιού μπορεί να καταγράψει όλες τις συναλλαγές των χρηστών και να τις συνδέσει με τη διεύθυνση IP τους. Τα ελαφριά πορτοφόλια επιτρέπουν στον τελικό χρήστη να αλληλοεπιδρά με το Blockchain και να πραγματοποιεί και να επιβεβαιώνει συναλλαγές χωρίς να δεσμεύει σημαντικούς πόρους της συσκευής. Καταλαμβάνουν μικρότερο χώρο αποθήκευσης επειδή κατεβάζουν μόνο τις κεφαλίδες των μπλοκ καθώς και μικρότερο εύρος ζώνης ενώ παράλληλα είναι ευκολότερα στην ρύθμιση τους. [39]

Ντετερμινιστικά και Μη-ντετερμινιστικά πορτοφόλια

Εάν η κατηγοριοποίηση γίνεται σύμφωνα με τις μεθόδους δημιουργίας κλειδιών, τα πορτοφόλια κατηγοριοποιούνται σε ντετερμινιστικά και μη ντετερμινιστικά [7]. Τα πιο σύγχρονα πορτοφόλια ονομάζονται ντετερμινιστικά πορτοφόλια. Σε αυτά τα πορτοφόλια όλα τα ιδιωτικά κλειδιά συνδέονται με έναν σπόρο (seed) που καλείται ως μοναδικό κλειδί ή βασικό κλειδί [7]. Μία μονόδρομη λειτουργία κατακερματισμού εφαρμόζεται στον σπόρο για τη δημιουργία όλων των ιδιωτικών κλειδιών. Ο σπόρος επιτρέπει στον χρήστη να δημιουργεί εύκολα αντίγραφα ασφαλείας και να επαναφέρει ένα πορτοφόλι χωρίς να χρειάζεται άλλες πληροφορίες. Ένα ντετερμινιστικό πορτοφόλι χρησιμοποιεί 12-24 λέξεις για να δημιουργήσει ένα σπόρο 512 bit. Αυτές οι λέξεις ονομάζονται μνημονικές λέξεις, επειδή είναι πιο εύκολο για έναν χρήστη να θυμάται λέξεις με τη σειρά, όπως «***cherry you receive shuffle ski wise youth roof shield private shaft shield***» αντί για ένα δεκαεξαδικό όπως «***331d1e7724a2784fa4d75c96da9d68f23321e1cd0b55a4d2377192bdae2f10fc***». Στη συνέχεια, ο σπόρος των 512 bit χρησιμοποιείται για τη δημιουργία ενός κύριου ιδιωτικού κλειδιού (master private key). Τέλος, αυτό το κύριο κλειδί με τη σειρά του χρησιμοποιείται για τη δημιουργία ιδιωτικών κλειδιών και αντίστοιχης δημόσιας διεύθυνσης [84].



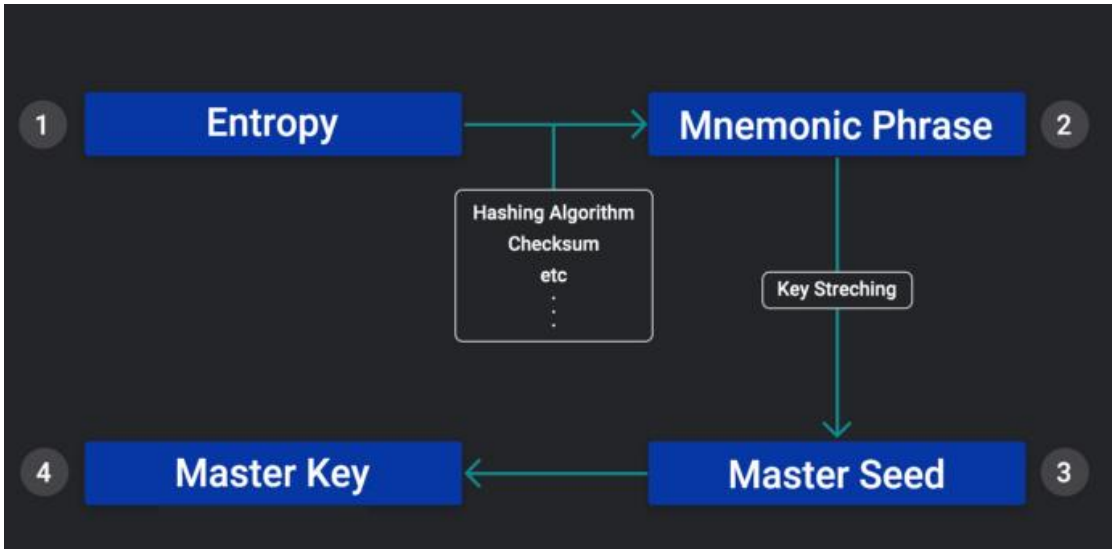
Εικόνα 4.4: Δημιουργία ιδιωτικών κλειδιών και αντίστοιχης δημόσιας διεύθυνσης σε ντετερμινιστικό πορτοφόλι.[84]

Τα μη ντετερμινιστικά πορτοφόλια αποτελούν μια πιο παραδοσιακή προσέγγιση πορτοφολιών. Σε αυτά τα πορτοφόλια κάθε κλειδί δημιουργείται ανεξάρτητα από έναν τυχαίο αριθμό. Οι πρώτες εφαρμογές πορτοφολιών Bitcoin ήταν μη ντετερμινιστικά πορτοφόλια επιτραπέζιων υπολογιστών, τα οποία δημιουργούσαν ένα τυχαίο σύνολο διευθύνσεων Bitcoin και αντίστοιχων ιδιωτικών κλειδιών (ζεύγη κλειδιών). Οι χρήστες έπρεπε να δημιουργήσουν αντίγραφα ασφαλείας των βασικών ζευγών τους μετά από κάθε συναλλαγή, ώστε να είναι 100% σίγουροι ότι δεν θα χάσουν χρήματα [7].

Σχέση μεταξύ μνημονικής φράσης και ιδιωτικού κλειδιού.

Υπάρχει μια παρεξήγηση όσον αφορά τη σχέση μεταξύ μνημονικής φράσης και ιδιωτικού κλειδιού. Όπως φαίνεται από τα παρακάτω βήματα, το ιδιωτικό κλειδί δημιουργείται από μια μνημονική φράση και όχι το αντίστροφο. Η διαδικασία κατά την οποία δημιουργείται ένα ιδιωτικό κλειδί σε ένα πορτοφόλι είναι η εξής:

- Δημιουργία εντροπίας (ένα κλειδί με 128 128, 160, 192, 224 ή 256 δυαδικά bit)
- Δημιουργία μνημονικής φράσης από την εντροπία
- Δημιουργία ενός κύριου σπόρου (master seed) από τη μνημονική φράση
- Δημιουργία ιδιωτικού κλειδιού από τον κύριο σπόρο

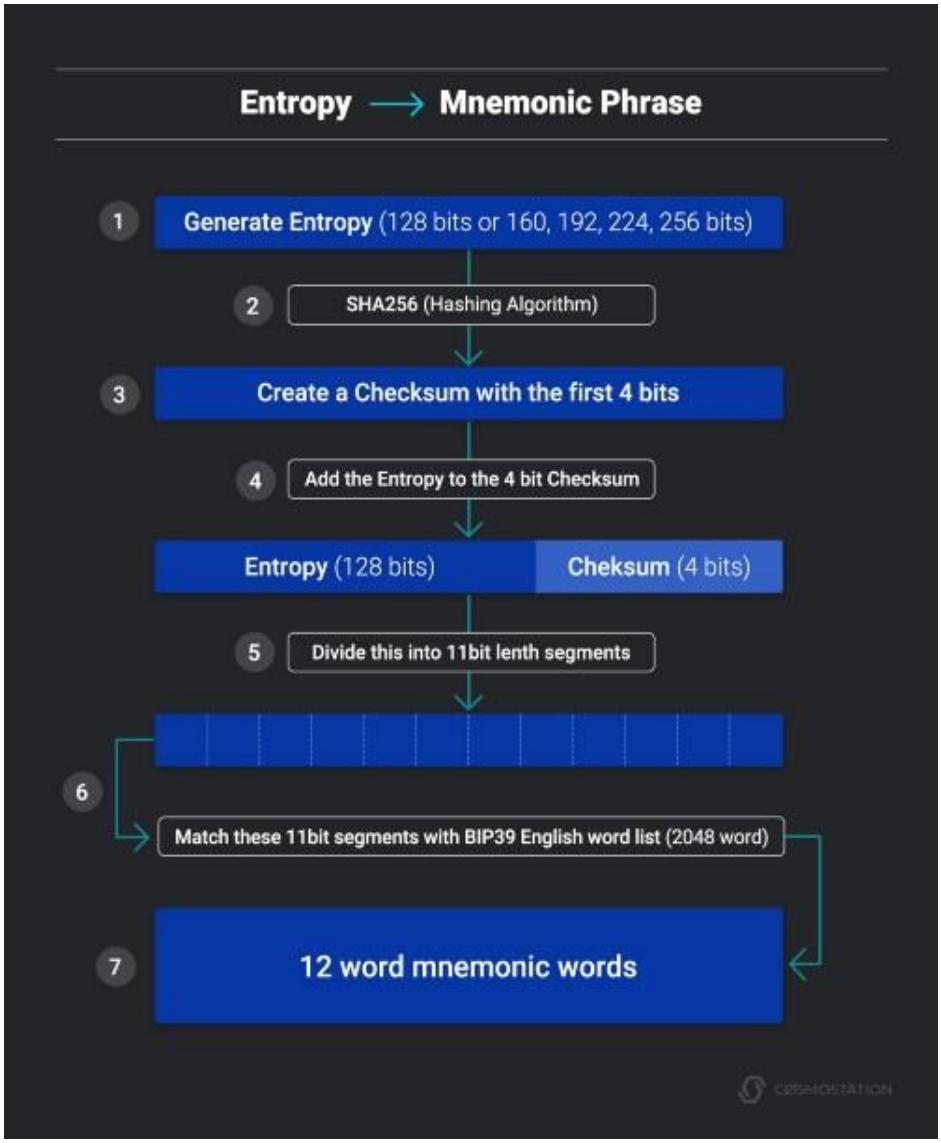


Εικόνα 4.5: Διαδικασία δημιουργίας ιδιωτικού κλειδιού [85]

Τα περισσότερα κρυπτονομίσματα δεν διαχειρίζονται ή λειτουργούν από κεντρικούς οργανισμούς. Ο τελικός χρήστης πρέπει πάντα να είναι προσεκτικός και να λαμβάνει κάθε μέτρο για την καλύτερη προστασία των περιουσιακών του στοιχείων. Για να επιτευχθεί αυτό, πρέπει να υπάρχει μια πλήρη κατανόηση του πορτοφολιού που χρησιμοποιείτε και του μηχανισμού πίσω από τη διαχείριση κλειδιών.

Δημιουργία μνημονικής φράσης

Ακολουθεί βήμα προς βήμα εξήγηση για το πώς δημιουργείται μια μνημονική φράση από ένα κλειδί με 128 δυαδικά bit (από εδώ κ πέρα το συγκεκριμένο κλειδί θα ονομάζεται εντροπία) [85] .

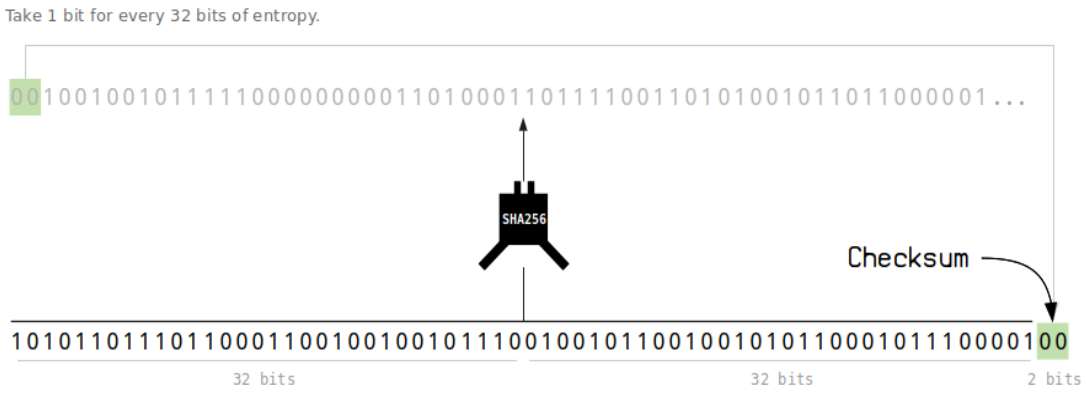


Εικόνα 4.6: Δημιουργία μνημονικής φράσης [85]

Βήμα 1: Η δημιουργία μνημονικής φράσης ξεκινά με τη δημιουργία εντροπίας μεγέθους 128, 160, 192, 224 ή 256 bits.

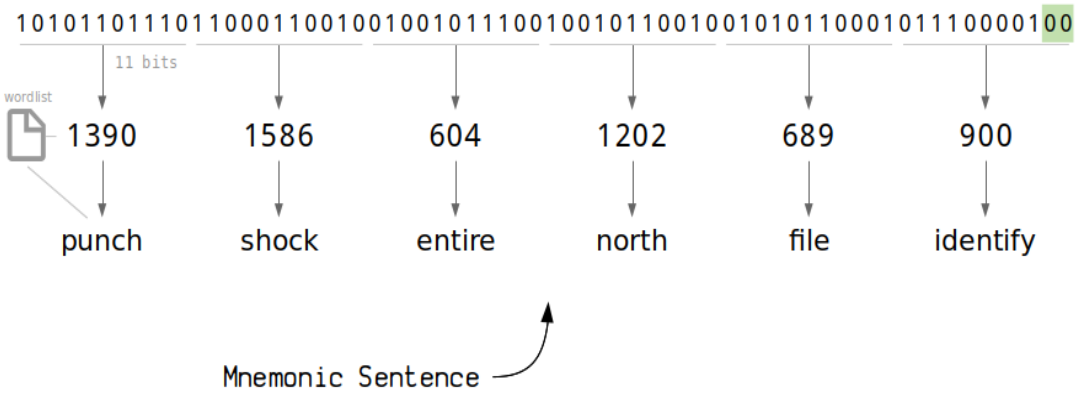
Βήμα 2: Ο αλγόριθμος κατακερματισμού SHA256 εφαρμόζεται στην εντροπία και δημιουργείται ένα άθροισμα ελέγχου (checksum) μήκους 4 bit.

Βήμα 3: Το άθροισμα ελέγχου προστίθεται στο τέλος της εντροπίας, το οποίο στη συνέχεια χωρίζεται σε τμήματα μήκους 11 bit.



Εικόνα 4.7: Πρόσθεση Checksum στο τέλος της εντροπίας [86]

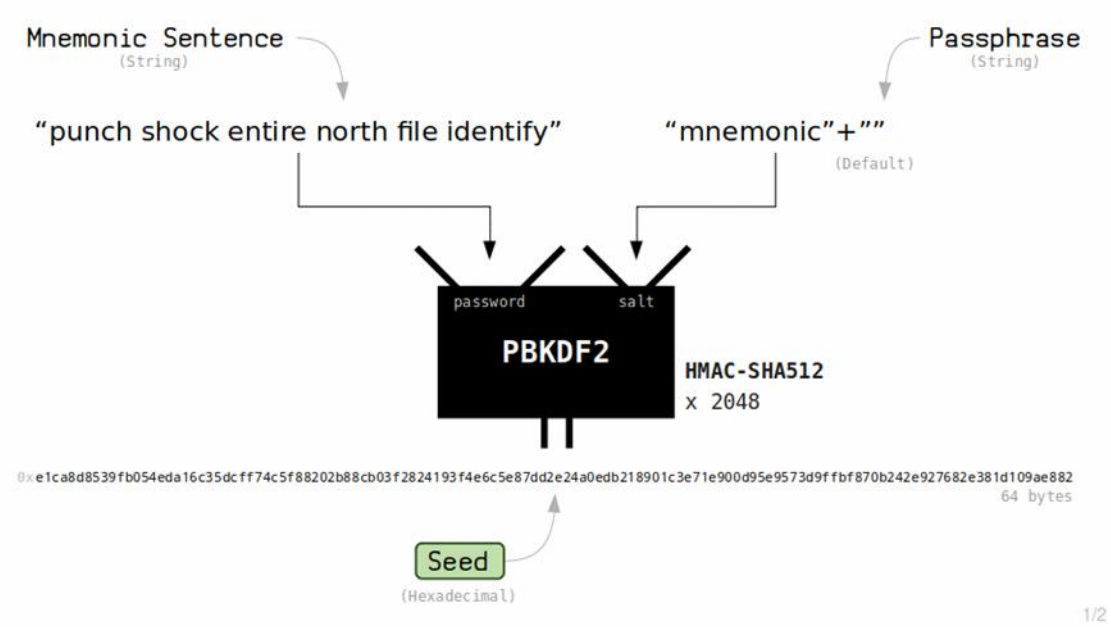
Βήμα 4: Τέλος, τα τμήματα των 11 bit μετατρέπονται σε δεκαδικά ψηφία και οι αριθμοί που προκύπτουν χρησιμοποιούνται για την επιλογή των αντίστοιχων λέξεων, από τη λίστα λέξεων BIP39 μεγέθους 2048 λέξεων.



Εικόνα 4.8: Μετατροπή δυαδικών τμημάτων μεγέθους 11 bit σε δεκαδικό, και εκ νέου μετατροπή δεκαδικού σε λέξεις [86]

Δημιουργία κύριου σπόρου από τη μνημονική φράση

Εφόσον έχει δημιουργηθεί η μνημονική φράση, μπορεί πλέον να μετατραπεί στον τελικό σπόρο. Για τη δημιουργία του σπόρου, η μνημονική φράση εισάγετε στην συνάρτηση κατακερματισμού PBKDF2. Έπειτα η φράση κατακερματίζεται πολλές φορές έως ότου παραχθεί ένα τελικό αποτέλεσμα μεγέθους 64 byte. Η συγκεκριμένη διαδικασία είναι γνωστή ως «τέντωμα» (key stretching) [86].



Εικόνα 4.9: Δημιουργία σπόρου (master seed) [86]

Στο τελευταίο στάδιο, ο σπόρος χρησιμοποιείται για τη δημιουργία του ιδιωτικού κλειδιού του πορτοφολιού.

Στόχοι Ασφαλείας των Πορτοφολιών

Οι στόχοι ασφαλείας των πορτοφολιών συμβαδίζουν με τους στόχους των περισσότερων συστημάτων ασφαλείας, κυρίως ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα [37].

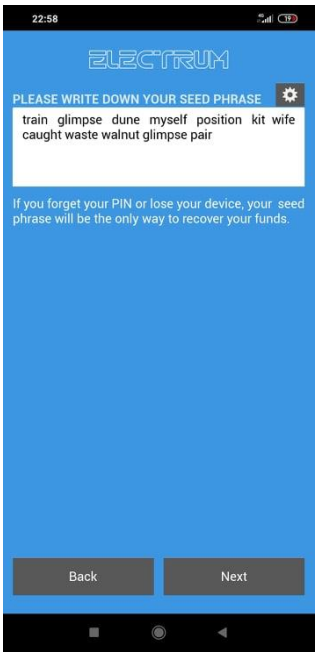
Εμπιστευτικότητα: Η εμπιστευτικότητα είναι η αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε εμπιστευτικές πληροφορίες. Για έναν λογαριασμό που κατέχει κρυπτονομίσματα, το ιδιωτικό κλειδί του σημαίνει τον πλήρη έλεγχο όλων των ψηφιακών περιουσιακών στοιχείων στο λογαριασμό. Επομένως, η θεμελιώδης αρχή του πορτοφολιού είναι να εξασφαλίσει ότι το ιδιωτικό κλειδί δεν μπορεί να προσπελαστεί με μη εξουσιοδοτημένους τρόπους. Οι πληροφορίες συναλλαγών ωστόσο δεν θεωρούνται εμπιστευτικές λόγω του γεγονότος ότι όλα τα δεδομένα αποθηκεύονται στο Blockchain που είναι προσβάσιμο στο κοινό. Οι εμπιστευτικές συναλλαγές διατηρούν το ποσό και τον τύπο των περιουσιακών στοιχείων που μεταφέρονται ορατά μόνο στους συμμετέχοντες της συναλλαγής, ενώ ταυτόχρονα εγγυούνται κρυπτογραφικά ότι δεν μπορούν να δαπανηθούν περισσότερα νομίσματα από όσα είναι διαθέσιμα.

Ακεραιότητα: Η ακεραιότητα είναι η αποτροπή της τροποποίησης πληροφοριών από μη εξουσιοδοτημένες οντότητες για να εξασφαλιστεί η ακρίβεια και η πληρότητα αυτών. Όσον αφορά τα πορτοφόλια κρυπτονομισμάτων, αποτελεί υψίστης σημασίας η εγγύηση της ακεραιότητας του ιδιωτικού κλειδιού. Εάν το ιδιωτικό κλειδί που είναι αποθηκευμένο στο πορτοφόλι τροποποιηθεί ή διαγραφεί παράνομα, ο χρήστης θα χάσει τον έλεγχο του λογαριασμού του, χάνοντας έτσι τα περιουσιακά στοιχεία του. Για δεδομένα συναλλαγών που έχουν σταλθεί στο Blockchain, το Blockchain χρησιμοποιεί κρυπτογραφικές μεθόδους όπως ψηφιακές υπογραφές και κατακερματισμούς για να διασφαλιστεί ότι τα δεδομένα συναλλαγών δεν έχουν παραποιηθεί. Ωστόσο, εάν οι πληροφορίες μιας συναλλαγής αλλοιωθούν με οποιονδήποτε τρόπο πριν ο χρήστης την υπογράψει με το ιδιωτικό του κλειδί, η συναλλαγή θα αναγνωριστεί από το Blockchain ως έγκυρη επειδή έχει την νόμιμη υπογραφή του κατόχου.

Διαθεσιμότητα: Η διαθεσιμότητα αναφέρεται στη διασφάλιση της νόμιμης χρήσης των πληροφοριών, πράγμα που σημαίνει ότι οι πληροφορίες θα πρέπει να είναι προσβάσιμες και να μπορούν να χρησιμοποιηθούν κατόπιν αιτήματος από εξουσιοδοτημένη οντότητα. Για εφαρμογές πορτοφολιού, είναι απαραίτητο να διασφαλιστεί ότι τα κλειδιά μπορούν να δημιουργηθούν, να αποθηκευτούν και να προσπελαστούν σωστά. Επίσης, οι συναλλαγές πρέπει να υπογράφονται, να αποστέλλονται και να εμφανίζονται σωστά μετά από αιτήματα των χρηστών.

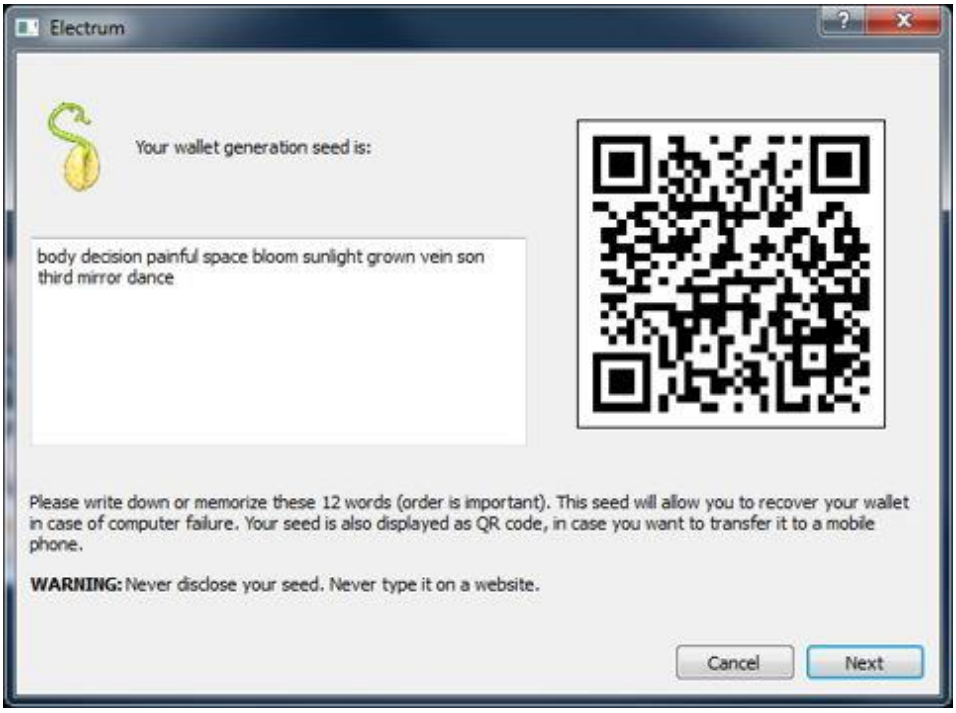
Ασφάλεια Πορτοφολιών

Τα πορτοφόλια που χρησιμοποιούνται για την αποθήκευση κρυπτονομισμάτων είναι ένα κομμάτι λογισμικού (software) ή υλικού (hardware) που μπορεί να δημιουργήσει, να αποθηκεύσει και να διαχειριστεί ιδιωτικά κλειδιά των λογαριασμών που περιέχουν κρυπτονομίσματα. Τα πορτοφόλια λογισμικού, όπως τα πορτοφόλια κινητών συσκευών, επιτρέπουν στους χρήστες να έχουν πλήρη πρόσβαση στο ιστορικό συναλλαγών, το υπόλοιπο του λογαριασμού καθώς και τη δημιουργία, υπογραφή και αποστολή νέων συναλλαγών στο κατανεμημένο δίκτυο. Η διαχείριση του ιδιωτικού κλειδιού είναι ιδιαίτερα σημαντική από τη πλευρά της ασφάλειας, επειδή η κατοχή του ισοδυναμεί με τον πλήρη έλεγχο του εκάστοτε λογαριασμού. Τα ιδιωτικά κλειδιά πρέπει να κρυπτογραφηθούν πριν αποθηκευτούν στο πορτοφόλι και εν συνεχεία να αποκρυπτογραφηθούν σε μορφή απλού κειμένου όταν πρόκειται να χρησιμοποιηθούν. Λαμβάνοντας ως παράδειγμα το Ethereum, το ιδιωτικό κλειδί σε μορφή απλού κειμένου (μη κρυπτογραφημένο) είναι ένας δυαδικός αριθμός μήκους 256-bit, ο οποίος κωδικοποιείται ως ένας δεκαεξαδικός αριθμός για παρουσίαση [37]. Ωστόσο, επειδή η απομνημόνευση ενός δεκαεξαδικού αριθμού είναι ένας ενοχλητικός τρόπος πρόσβασης στο πορτοφόλι, οι προγραμματιστές βρήκαν έναν τρόπο να μεταφράσουν το ιδιωτικό κλειδί σε μια πιο ευανάγνωστη και εύκολα αναγνωρίσιμη μορφή. Αυτή ονομάζεται BIP-0039 και είναι μια μνημονική φράση (mnemonic phrase) που αποτελείται από 12 (128-bit ιδιωτικό κλειδί) έως 24 (256-bit ιδιωτικό κλειδί) ευανάγνωστες λέξεις [7].



Εικόνα 4.10: Electrum mobile wallet. Δημιουργία μνημονικης φράσης ανάκτησης πορτοφολιού

Εικόνα 4.10.1: Electrum mobile wallet. Επαλήθευση φράσης ανάκτησης.



Εικόνα 4.11: Electrum desktop wallet. Δημιουργία μνημονικης φράσης ανάκτησης πορτοφολιού. Στην αριστερή πλευρά η μνημονική φράση απεικονίζεται σε μορφή QR code για δυνατότητα απευθείας αποθήκευσης στη κινητή συσκευή του χρήστη.

Με αυτόν τον τρόπο ένας χρήστης μπορεί πολύ εύκολα να αποκτήσει πρόσβαση στο πορτοφόλι, δεδομένου ότι μπορεί να γράψει ή να απομνημονεύσει αυτές τις λέξεις. Επειδή κανένα πορτοφόλι δεν έχει πρόσβαση στη φράση ανάκτησης συμβουλεύει πάντοτε τους χρήστες να την αποθηκεύσουν, καθώς σε περίπτωση που ο χρήστης χάσει την κινητή συσκευή του ή εγκαταστήσει ξανά την εφαρμογή μετά από μία απεγκατάσταση της, δεν θα μπορεί να έχει πρόσβαση στον λογαριασμό του και συνεπώς στην ανάκτηση των κεφαλαίων του.

Ευπάθειες Πορτοφολιών

Τα πορτοφόλια κρυπτονομισμάτων φέρουν γενικά τις βασικές λειτουργίες της διαχείρισης ιδιωτικών κλειδιών και της διαχείρισης συναλλαγών. Η διαχείριση των κλειδιών περιλαμβάνει τη δημιουργία, την αποθήκευση, την εισαγωγή και την εξαγωγή ενός ιδιωτικού κλειδιού, ενώ η διαχείριση συναλλαγών περιλαμβάνει τη μεταφορά και τη συλλογή διακριτικών (tokens), καθώς και την διατήρηση του ιστορικού των συναλλαγών. Η ακατάλληλη εφαρμογή αυτών των λειτουργιών μπορεί να εισαγάγει σημεία ευπάθειας στην "επιφάνεια επίθεσης" [37]. Εκτός αυτού, επειδή το πορτοφόλι φιλοξενείται σε ένα λειτουργικό σύστημα, τα χαρακτηριστικά που παρέχονται από το λειτουργικό σύστημα μπορούν επίσης να αξιοποιηθούν από τον εισβολέα, θέτοντας έτσι μια επιπλέον απειλή για την ασφάλεια του ψηφιακού πορτοφολιού. Παρακάτω, ακολουθεί μια ανάλυση των σημείων επίθεσης, από τις πτυχές του ίδιου του πορτοφολιού κρυπτονομισμάτων και του υποκείμενου λειτουργικού συστήματος.

Διαχείριση κλειδιών

Όταν ένας χρήστης δημιουργήσει λογαριασμό σε μία εφαρμογή πορτοφολιού, ένα ζευγάρι δημόσιων και ιδιωτικών κλειδιών για το νέο λογαριασμό θα δημιουργηθεί τοπικά στη συσκευή μέσω του πορτοφολιού. Εάν ο χρήστης έχει ήδη λογαριασμό, το ιδιωτικό κλειδί που αντιστοιχεί στον λογαριασμό μπορεί να εισαχθεί στο πορτοφόλι έτσι ώστε ο χρήστης να μπορεί να διαχειριστεί τον λογαριασμό χρησιμοποιώντας αυτό το πορτοφόλι. Σε περίπτωση που το ιδιωτικό κλειδί κλαπεί ή διαγραφεί από κάποιον τρίτο, τότε ο χρήστης αυτομάτως θα χάσει τον έλεγχο του λογαριασμού του, κάτι που αποτελεί απειλή για την ακεραιότητα και τη διαθεσιμότητα του λογαριασμού.

Κατά την εισαγωγή ενός ιδιωτικού κλειδιού στο πορτοφόλι, ένας χρήστης ενδεχομένως να χρειαστεί να εισάγει χειροκίνητα το ιδιωτικό κλειδί του χρησιμοποιώντας το πληκτρολόγιο, ή αντιγράφοντας και επικολλώντας, αυτό μπορεί να λειτουργήσει ως πόρτα εισόδου για τα κακόβουλα λογισμικά [37].

Τα τελευταία χρόνια τα κακόβουλα λογισμικά (π.χ. Anubis) αυξάνονται όλο και περισσότερο στην κοινότητα των κρυπτονομισμάτων [87]. Υπάρχει ένας αυξανόμενος αριθμός κακόβουλων λογισμικών που στοχεύουν υπολογιστές χρηστών που κατέχουν κρυπτονομίσματα, και εξειδικεύονται στην καταγραφή/κλοπή κωδικών πρόσβασης του συστήματος του χρήστη. Οι έμπειροι κάτοχοι κρυπτονομισμάτων που γνωρίζουν πως λειτουργεί η τεχνολογία του Blockchain χρησιμοποιούν συνήθως πορτοφόλια υλικού και αποθηκεύουν εκεί τα ιδιωτικά κλειδιά τους εκτός σύνδεσης. Οι λιγότερο έμπειροι χρήστες, ωστόσο, λόγω του φόβου της απώλειας των ιδιωτικών κλειδιών τους, ενδέχεται να τα διατηρήσουν αποθηκευμένα στον υπολογιστή τους. Ακόμα κι αν το αρχείο πορτοφολιού που είναι εγκατεστημένο στον υπολογιστή έχει κωδικό πρόσβασης, εάν το κακόβουλο λογισμικό περιλαμβάνει καταγραφέα πληκτρολόγησης (keylogger), μπορεί να συλλάβει εύκολα οτιδήποτε πληκτρολογήσει ο χρήστης στον υπολογιστή συμπεριλαμβανομένου και του ιδιωτικού κλειδιού [87].

Διαχείριση συναλλαγών

Όταν ένας χρήστης χρειάζεται να μεταφέρει χρήματα από τον λογαριασμό του, το πορτοφόλι δημιουργεί την αντίστοιχη συναλλαγή και την υπογράφει με το ιδιωτικό κλειδί του χρήστη. Στη συνέχεια μεταδίδει την υπογεγραμμένη συναλλαγή στο δίκτυο του Blockchain, και περιμένει την επιβεβαίωση για την ολοκλήρωση της μεταφοράς. Κατά τη αποστολή και λήψη χρημάτων, τα στοιχεία της συναλλαγής που εισήχθησαν από τον χρήστη μπορούν να παραβιαστούν, γεγονός που αποτελεί απειλή για την ακεραιότητα, και μπορεί να οδηγήσει σε υπεξαίρεση χρημάτων από τον λογαριασμό του χρήστη προς όφελος του εισβολέα. Επιπλέον, εάν ένας εισβολέας καταφέρει και διακόψει τη ροή της συναλλαγής διακόπτοντας τη σύνδεση μεταξύ του πορτοφολιού και του δικτύου Blockchain ή του διακομιστή που στέλνεται η συναλλαγή, θα δημιουργηθεί απειλή για τη διαθεσιμότητα. Αυτή η απειλή ενδέχεται να οδηγήσει σε ευαίσθητες ενέργειες όπως η εξαγωγή του ιδιωτικού κλειδιού του χρήστη και της ανάκτησης του ελέγχου του λογαριασμού, με αποτέλεσμα περαιτέρω ζημιά.

Εκτός αυτού, εάν το πληκτρολόγιο και η οθόνη εισαγωγής του κωδικού πρόσβασης παρακολουθούνται, ο κρυπτογραφημένος κωδικός πρόσβασης του χρήστη μπορεί να κλαπεί, απειλώντας την εμπιστευτικότητα [37].

Υλοποίηση Συναλλαγής μέσω Desktop Wallet

Σε αυτό το σημείο θα διερευνήσουμε τον τρόπο μεταφοράς χρημάτων μεταξύ πορτοφολιών στο δίκτυο του Bitcoin. Θα εξετάσουμε πρώτα πώς λειτουργεί το πορτοφόλι και θα πάρουμε μία ιδέα για το τέλη συναλλαγής. Τέλος, θα δούμε πως αποθηκεύεται η συναλλαγή στο κατανεμημένο καθολικό.

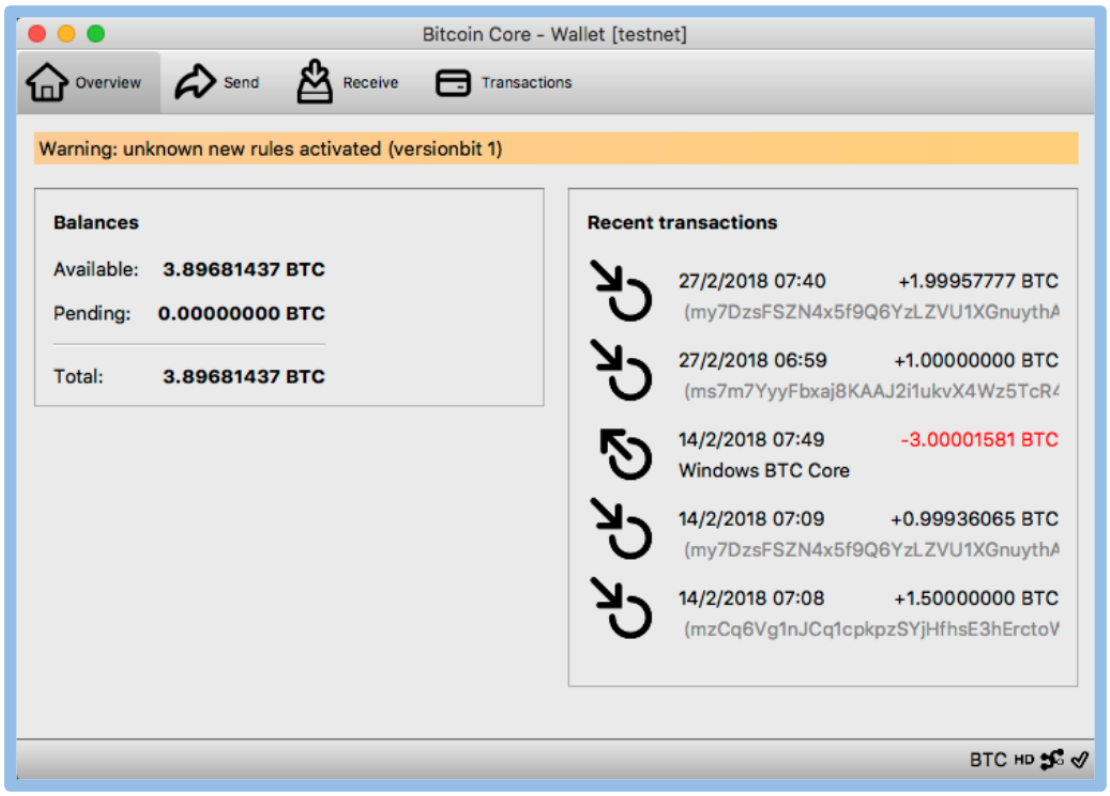
Για την ανάγκη αυτή θα χρησιμοποιήσουμε το Bitcoin-Qt Wallet το οποίο λειτουργεί ως πλήρης κόμβος και προσφέρει μια εύκολη σε χρήση διεπαφή χρήστη.

Ρύθμιση

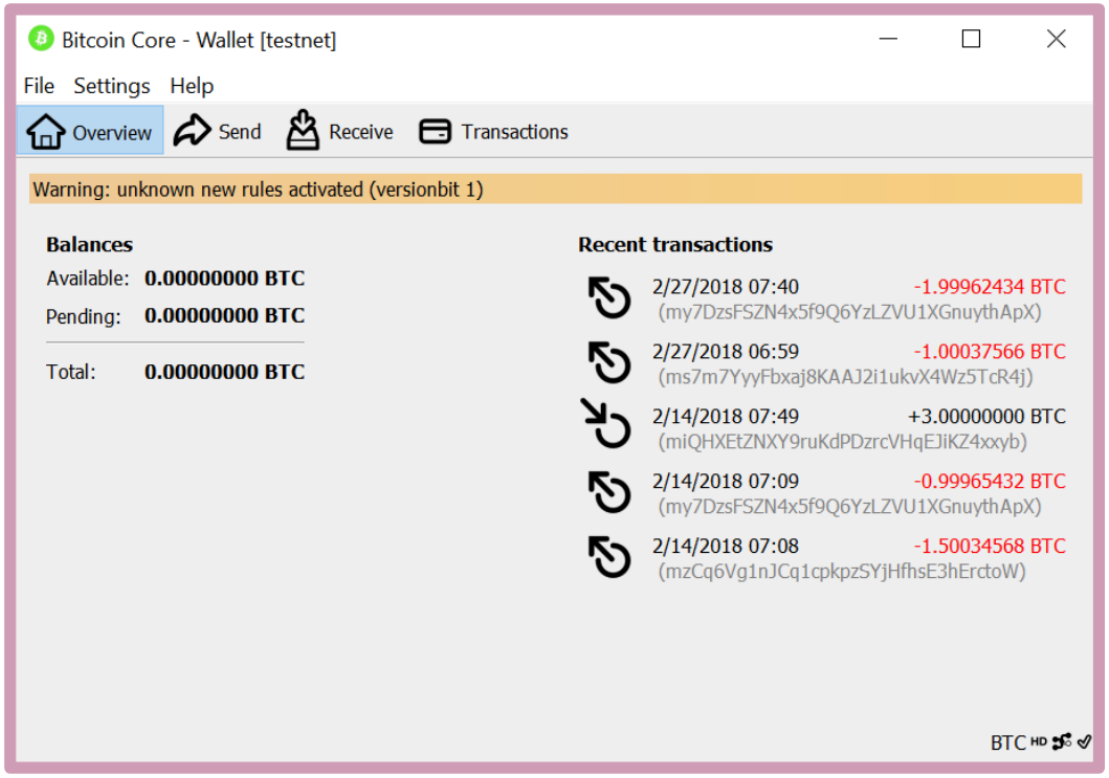
Σε αυτό το σημείο υπάρχουν δύο υπολογιστές, καθένας από τους οποίους έχει εγκατεστημένο το Bitcoin-Qt Wallet. Ορίζουμε τον πρώτο υπολογιστή ως Πορτοφόλι Α και τον δεύτερο ως Πορτοφόλι Β. Σημειώστε ότι μπορεί κανείς να δημιουργήσει όσες διευθύνσεις Bitcoin θέλει σε ένα πορτοφόλι κατόπιν επιθυμίας του.

Μεταφορά Χρημάτων

Πριν ξεκινήσει η μεταφορά χρημάτων από το ένα πορτοφόλι στο άλλο βλέπουμε ότι το Πορτοφόλι Α κατέχει το χρηματικό ποσό 3.89681437 BTC, ενώ το Πορτοφόλι Β διατηρείται άδειο. Εδώ βλέπουμε και τα δύο πορτοφόλια.

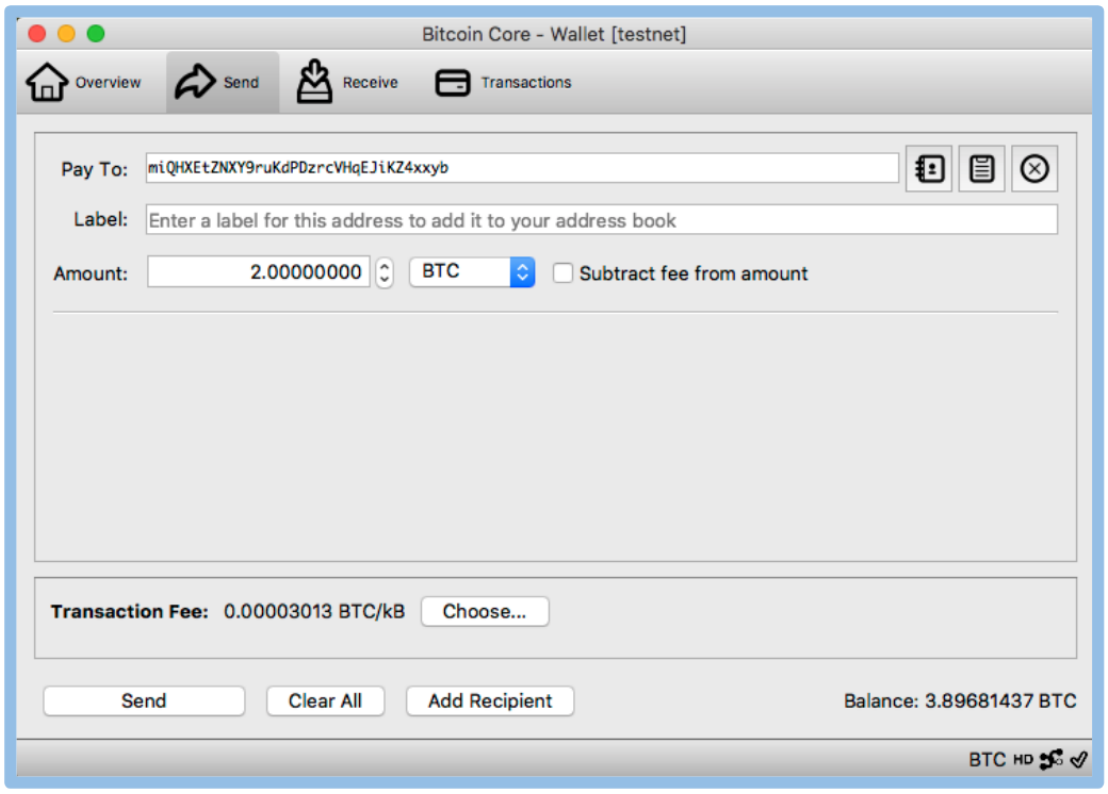


Εικόνα 4.12: Πορτοφόλι Α



Εικόνα 4.13: Πορτοφόλι Β

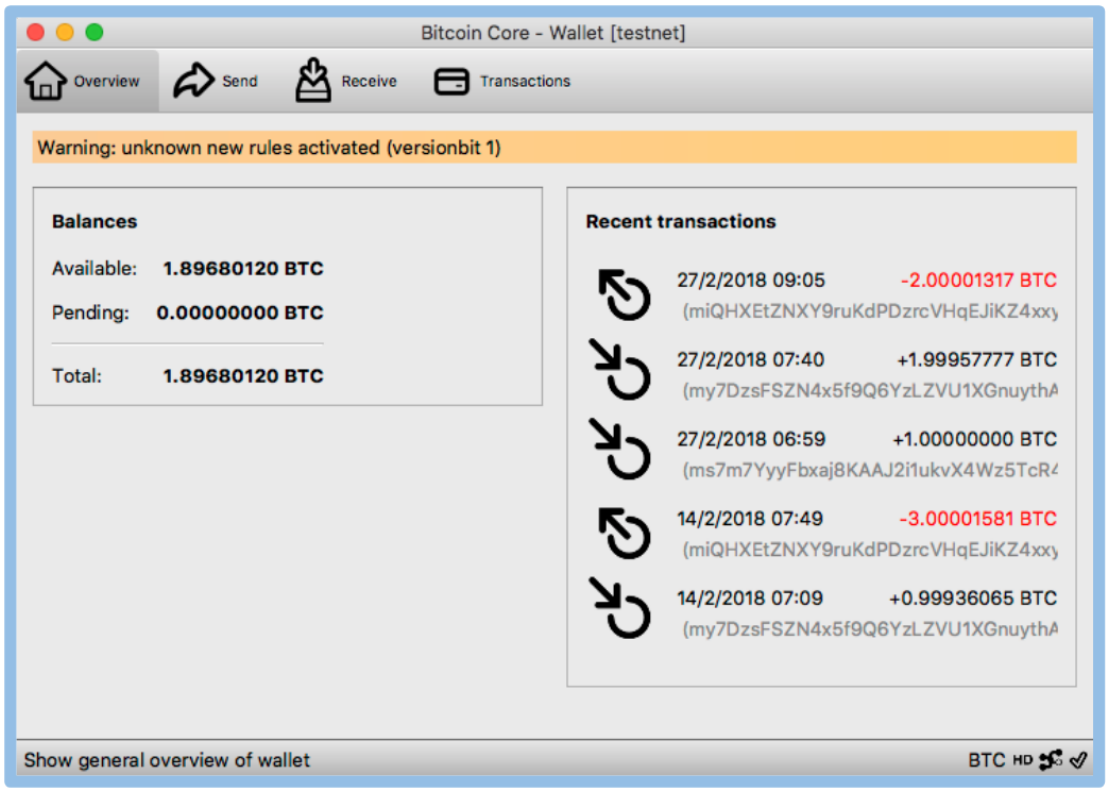
Στο Πορτοφόλι Α, εισάγουμε τη διεύθυνση του Πορτοφολιού Β και μεταφέρουμε 2 BTC. Όπως βλέπουμε υπάρχει μια επιλογή "Αφαίρεση αμοιβής από το ποσό". Εάν αυτό το πλαίσιο δεν είναι επιλεγμένο, η χρέωση συναλλαγής καταβάλλεται πάνω από τα 2 BTC. Ως αποτέλεσμα, το Πορτοφόλι Β θα λάβει 2 BTC, ενώ το Πορτοφόλι Α ξοδεύει περισσότερα από 2 BTC.



Εικόνα 4.14: Πορτοφόλι Α

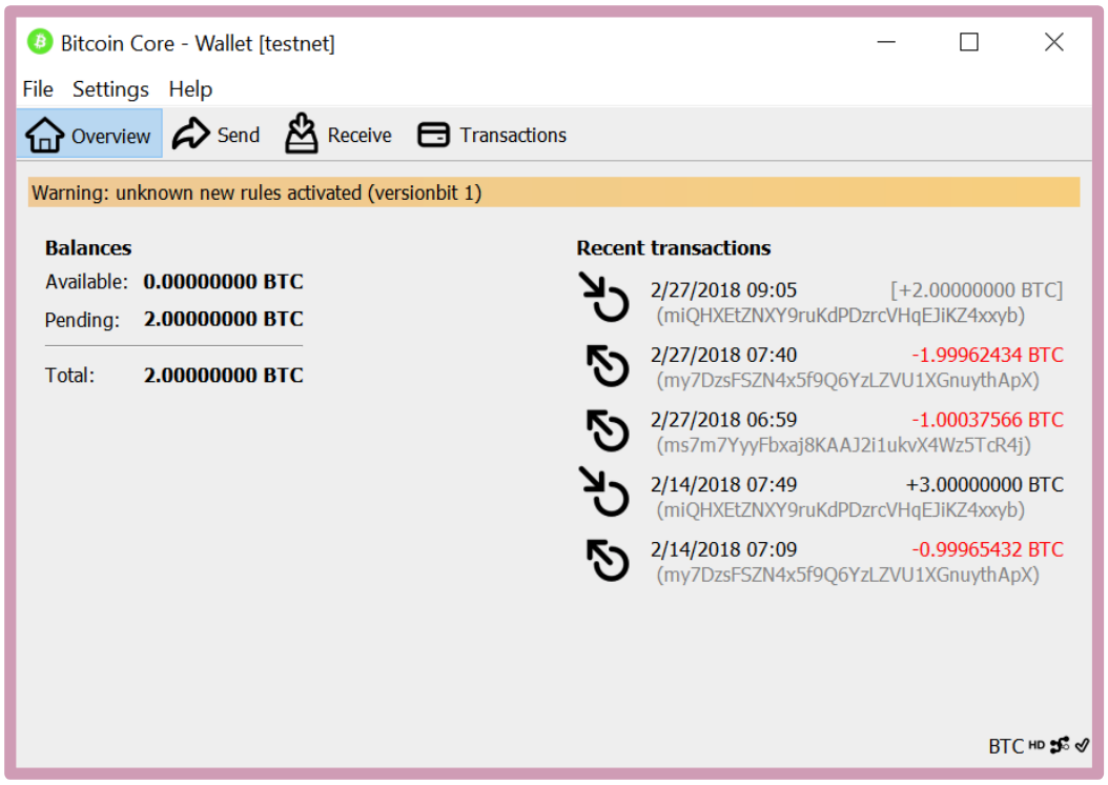
Επιβεβαίωση Συναλλαγής

Μετά την αποστολή του ποσού στο Πορτοφόλι Α βλέπουμε αλλαγές και στα δύο πορτοφόλια. Αυτό είναι το Πορτοφόλι Α μετά την αποστολή του κεφαλαίου.



Εικόνα 4.15: Πορτοφόλι Α

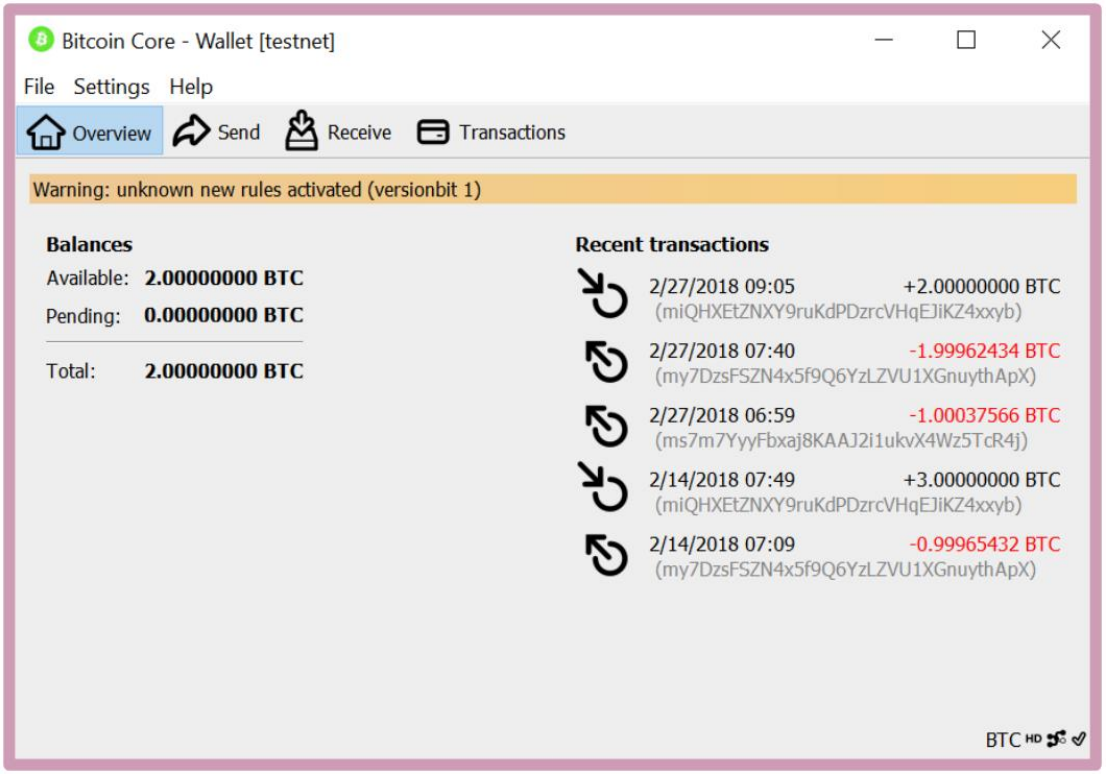
Παρατηρούμε ότι στο Πορτοφόλι Α καταγράφεται μια νέα συναλλαγή, πρώτη καταχώρηση στις πρόσφατες συναλλαγές, που δείχνει ότι αποστέλλονται 2.00001317 BTC. Το διαθέσιμο υπόλοιπο γίνεται αμέσως 1.89680120 BTC, αντικατοπτρίζοντας τη μείωση από το ποσό 2.00001317 BTC.



Εικόνα 4.16: Πορτοφόλι Β

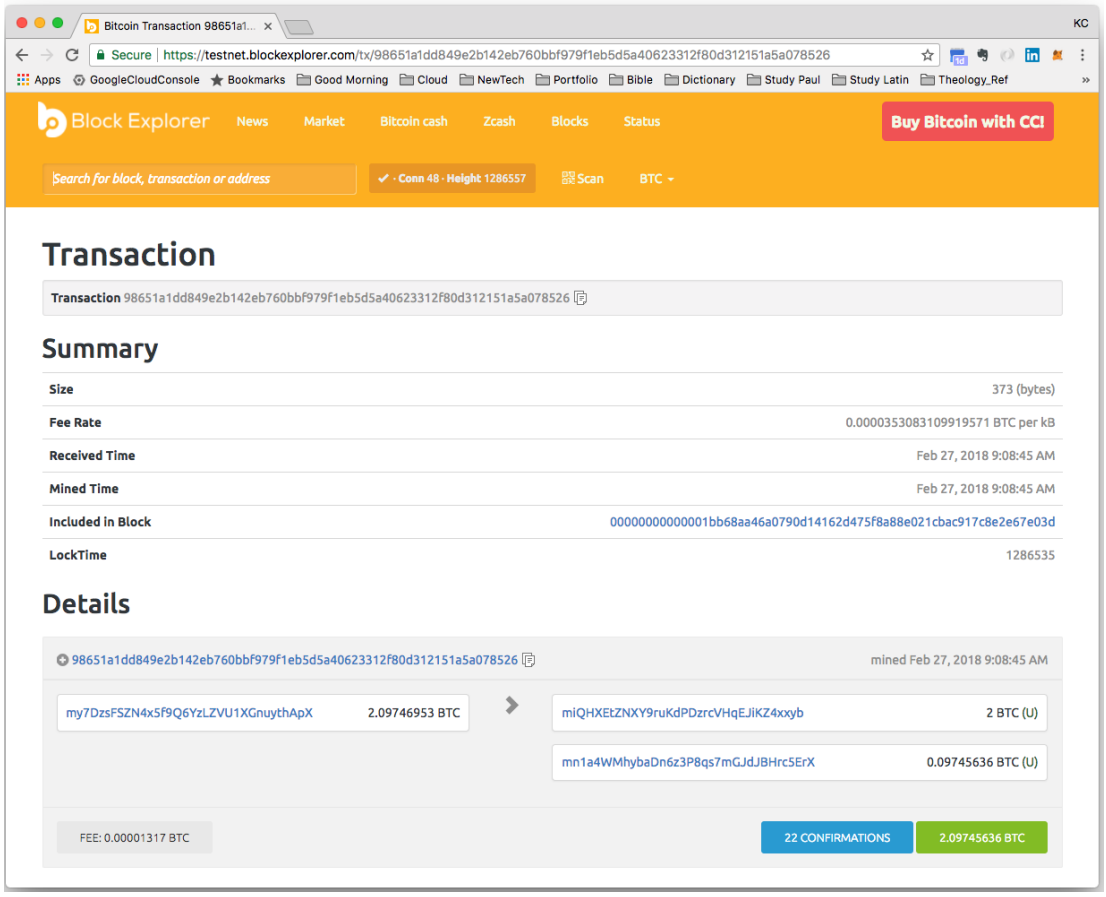
Παρατηρούμε ότι στο Πορτοφόλι Β καταγράφεται μια νέα συναλλαγή που δείχνει ότι λαμβάνονται 2.00000000 BTC. Όπως βλέπουμε το ποσό των 2.00000000 BTC είναι μέσα σε αγκύλες σε αντίθεση με τις προηγούμενες συναλλαγές. Αυτό συμβαίνει επειδή αυτή η συναλλαγή δεν έχει επιβεβαιωθεί ακόμη, δηλαδή εκκρεμεί επιβεβαίωση. Παρόλο που το υπόλοιπο γίνεται αμέσως 2.00000000 BTC, δεν είναι ακόμη διαθέσιμο.

Μετά από λίγο αυτή η συναλλαγή επιβεβαιώνεται και το ποσό γίνεται πλέον διαθέσιμο για χρήση



Εικόνα 4.17: Πορτοφόλι Β

Αυτή η συναλλαγή είναι ήδη διαθέσιμη στο Blockchain του Bitcoin, όπως όλες οι συναλλαγές, και είναι ορατή στο κοινό. Μπορούμε να χρησιμοποιήσουμε το txid για να εντοπίσουμε αυτήν τη συναλλαγή σε οποιονδήποτε Bitcoin Explorer. Εδώ είναι ένα παράδειγμα.



Εικόνα 4.18: Block Explorer

Αυτή είναι η πλήρης εικόνα της συναλλαγής. Η αριστερή πλευρά είναι η είσοδος (input), όπου χρηματοδοτείται η συναλλαγή. Η δεξιά πλευρά είναι η έξοδος (output), μία στο Πορτοφόλι Β και μία πίσω στο Πορτοφόλι Α. Η έξοδος πίσω στο Πορτοφόλι Α έχει ένα (U) δίπλα, που σημαίνει ότι πρόκειται για έξοδο συναλλαγής που δεν έχει δαπανηθεί και μπορεί να χρησιμοποιηθεί αργότερα ως είσοδος μιας νέας συναλλαγής. Είναι το λεγόμενο UTXO που αναφερθήκαμε νωρίτερα στο κεφάλαιο 3.

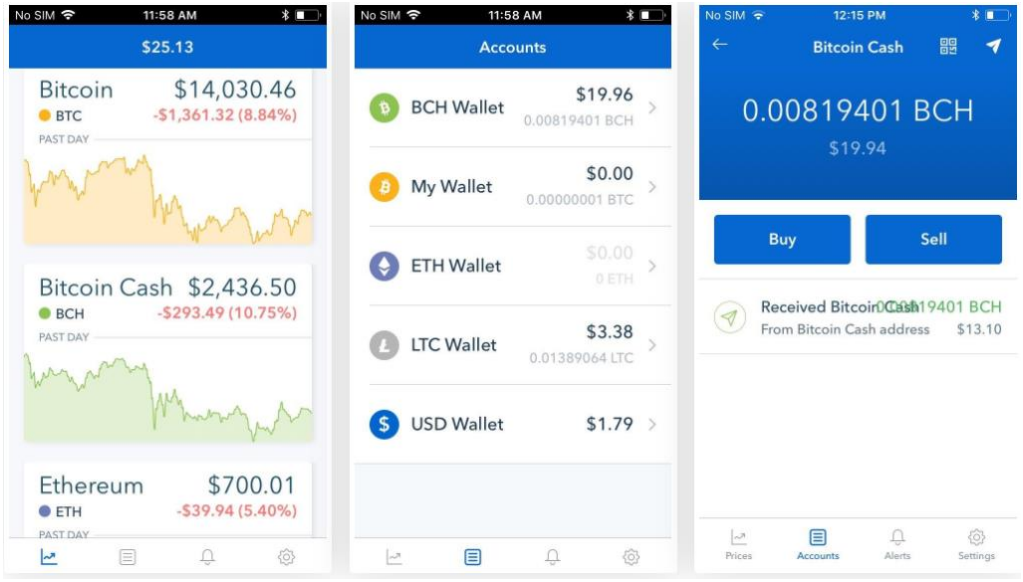
Υλοποίηση Συναλλαγής μέσω Mobile Wallet

Σε αυτό το σημείο θα διερευνήσουμε τον τρόπο μεταφοράς χρημάτων μεταξύ πορτοφολιών σε κινητές συσκευές. Για την ανάγκη αυτή θα χρησιμοποιήσουμε το πορτοφόλι Coibase. Σε αντίθεση με την αγορά και πώληση κρυπτονομισμάτων, το Coinbase δεν χρεώνει τέλη συναλλαγής για την αποστολή και τη λήψη κρυπτονομισμάτων. Η αποστολή και λήψη ψηφιακών νομισμάτων στο Coinbase είναι εύκολη διαδικασία μόλις ρυθμιστεί ο λογαριασμός και είναι η ίδια ανεξάρτητα από το αν χρησιμοποιείτε συσκευή iPhone ή Android.

Αποστολή Bitcoin

Βήμα 1

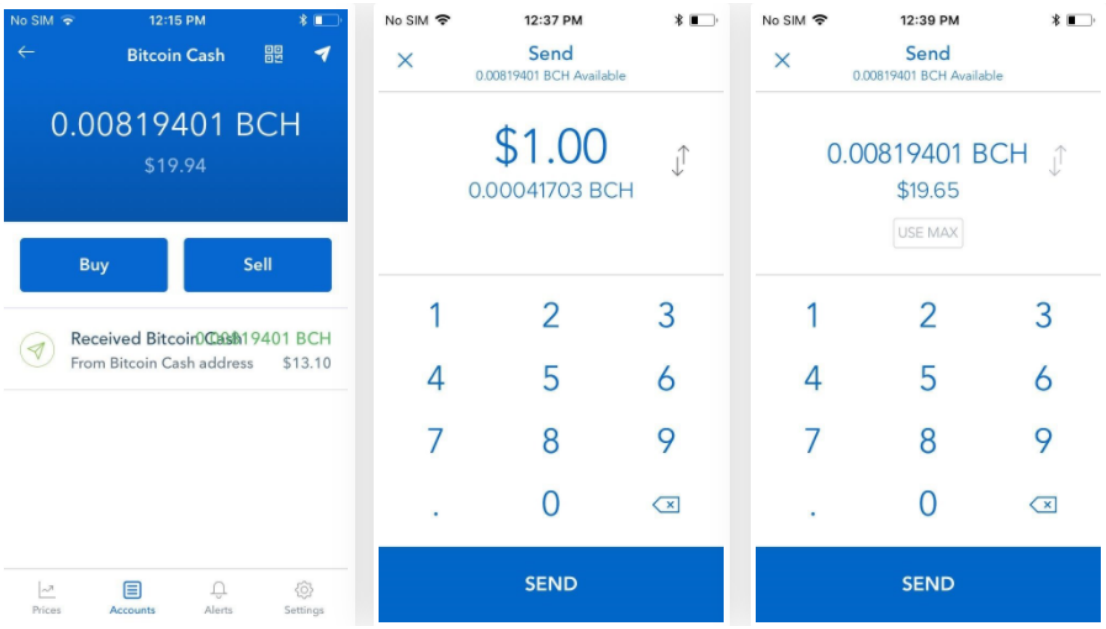
Εφόσον έχουμε δημιουργήσει το λογαριασμό ανοίγουμε το Coinbase και αποκτάμε πρόσβαση στα πορτοφόλια μας πατώντας "Λογαριασμοί" στο κάτω μέρος της οθόνης σας. Από εκεί, επιλέγουμε το πορτοφόλι με το οποίο θέλουμε να πραγματοποιήσουμε τη συναλλαγή. Μεταφερόμαστε τώρα στο πορτοφόλι του συγκεκριμένου νομίσματος, το οποίο δείχνει το ιστορικό συναλλαγών και το διαθέσιμο υπόλοιπο. Για την παρούσα συναλλαγή θα χρησιμοποιήσουμε το Bitcoin Cash (BCH), αλλά τα βήματα είναι ακριβώς τα ίδια ανεξάρτητα από το ποιο κρυπτονόμισμα θα επιλέξουμε.



Εικόνα 4.19: Coinbase Mobile Wallet

Βήμα 2

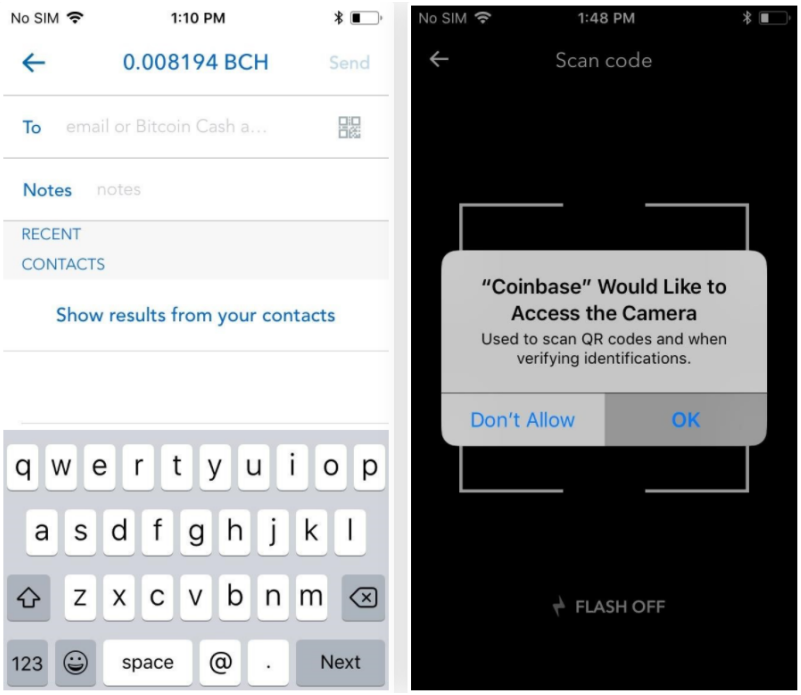
Για να στείλουμε Bitcoin, πατάμε πρώτα το κουμπί σε σχήμα αεροπλάνου στην επάνω δεξιά γωνία της οθόνης. Μέσα από τη σελίδα "Αποστολή", επιλέγουμε το ποσό BCH που θέλουμε να στείλουμε. Μπορείτε να επιλέξουμε μεταξύ BCH ή USD πατώντας στα βέλη δίπλα στην ονομασία για περιστροφή μεταξύ των δύο. Εάν επιλέξουμε το BCH, υπάρχει πρόσθετη επιλογή αποστολής ολόκληρου του περιεχομένου του πορτοφολιού πατώντας στο κουμπί "Use Max" κάτω από το ποσό BCH.



Εικόνα 4.20: Coinbase Mobile Wallet

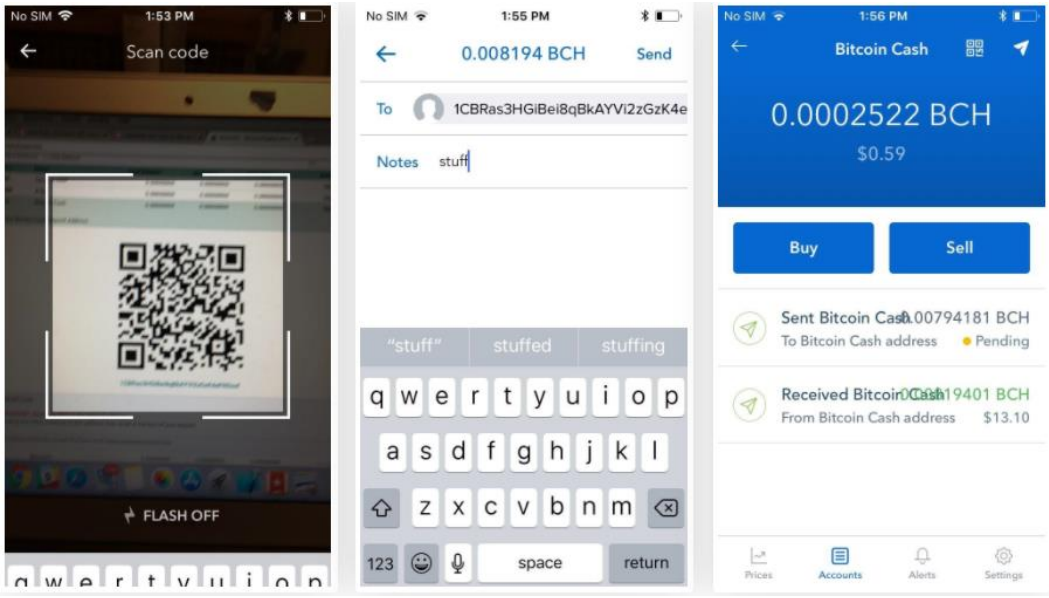
Μόλις πατήσουμε το μπλε κουμπί "Αποστολή" θα μεταφερθούμε τώρα σε μια σελίδα επιβεβαίωσης για να εισαγάγουμε τη διεύθυνση του παραλήπτη και τυχόν επιπλέον σημειώσεις που ενδέχεται να έχουμε. Εάν ο παραλήπτης διαθέτει λογαριασμό Coinbase, μπορούμε απλά να εισάγουμε τη διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με τον λογαριασμό του.

Εάν στέλνουμε σε ένα πορτοφόλι που δεν είναι συνδεδεμένο στο Coinbase, θα πρέπει είτε να εισάγουμε την ακριβή διεύθυνση του πορτοφολιού ή να χρησιμοποιήσουμε την κάμερα του τηλεφώνου μας για να σαρώσετε το QR code του παραλήπτη. Για να χρησιμοποιήσουμε το τελευταίο, πατάμε το κουμπί QR στα δεξιά της διεύθυνσης του παραλήπτη και, στη συνέχεια, παραχωρούμε στο Coinbase πρόσβαση στην κάμερα του τηλεφώνου.



Εικόνα 4.21: Coinbase Mobile Wallet

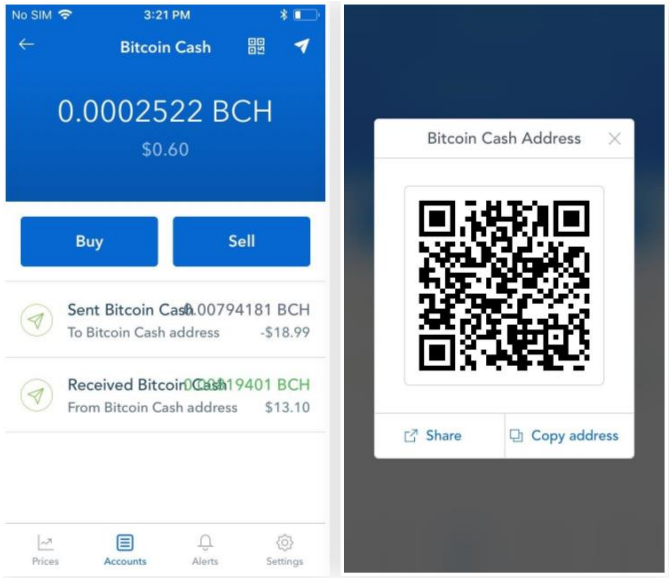
Τώρα, χρησιμοποιούμε την κάμερα του τηλεφώνου για να σαρώσουμε τον κωδικό QR του πορτοφολιού στο οποίο θα στείλουμε BCH και η διεύθυνσή θα συμπληρώσει αυτόματα στη καρτέλα διευθύνσεων του παραλήπτη. Πατώντας "Αποστολή" το Coinbase θα στείλει τα χρήματα και θα μας μεταφέρει στη σελίδα του πορτοφολιού, δείχνοντας την πιο πρόσφατη συναλλαγή στο κάτω μέρος.



Εικόνα 4.22: Coinbase Mobile Wallet

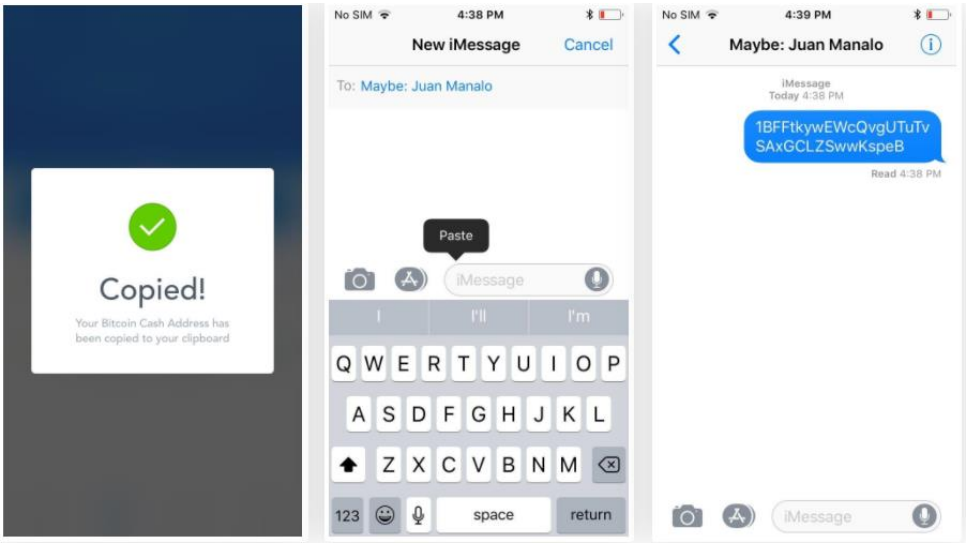
Λήψη Bitcoin

Για να λάβουμε BCH, ξεκινάμε πατώντας το κουμπί QR που βρίσκεται στην επάνω δεξιά γωνία της οθόνης στη σελίδα του πορτοφολιού. Η διεύθυνση θα εμφανιστεί σε μορφή QR, οπότε αν κάνουμε μια συναλλαγή πρόσωπο με πρόσωπο, απλώς ζητάμε από τον αποστολέα να το σαρώσει χρησιμοποιώντας την ίδια μέθοδο που περιγράφεται στο Βήμα 2 παραπάνω.



Εικόνα 4.23: Coinbase Mobile Wallet

Εάν ο αποστολέας βρίσκεται μακριά, πατάμε "Κοινοποίηση" για να κοινοποιηθεί η διεύθυνσή μας στον αποστολέα μέσω email ή γραπτού μηνύματος.



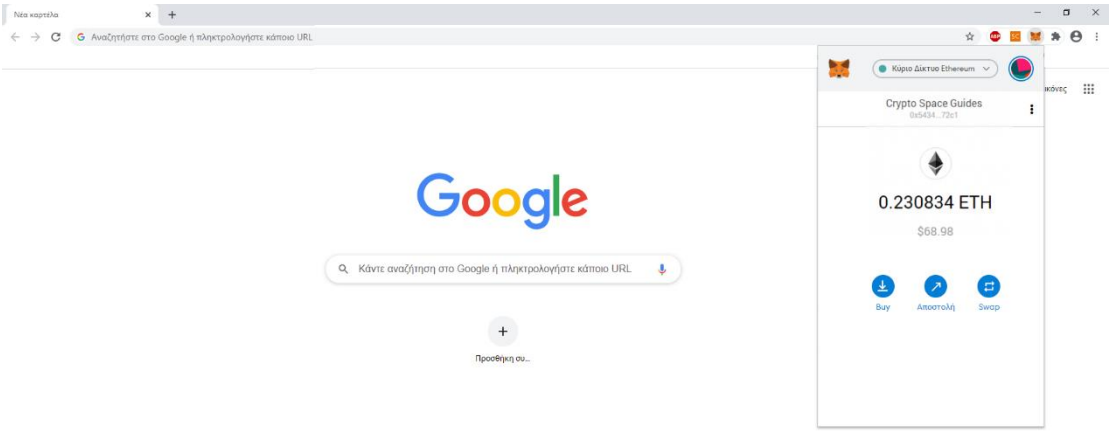
Εικόνα 4.24: Coinbase Mobile Wallet

Μόλις ο αποστολέας στείλει το ποσό εκκρεμεί η καταγραφεί της συναλλαγή η οποία γίνεται συνήθως μέσα σε λίγα λεπτά, στο αντίστοιχο πορτοφόλι του παραλήπτη. νομίσματος κάτω από την καρτέλα ιστορικού συναλλαγών στο κάτω μισό του πορτοφολιού σας. Όταν η συναλλαγή επιβεβαιωθεί το ποσό θα προστεθεί στο υπόλοιπο του πορτοφολιού.

Εικόνα 4.25: Αναμονή Επιβεβαίωσης Συναλλαγής

Υλοποίηση Συναλλαγής μέσω Web Wallet

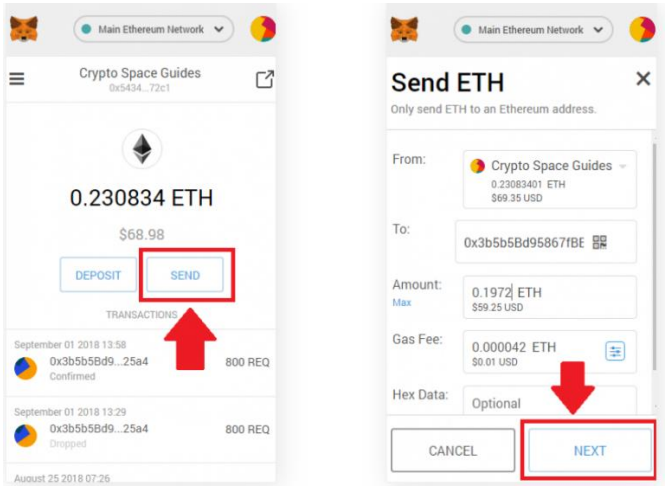
Σε αυτό το σημείο θα διερευνήσουμε τον τρόπο μεταφοράς χρημάτων μεταξύ πορτοφολιών στο δίκτυο του Ethereum.Υπάρχουν πολλά πορτοφόλια διαθέσιμα για το Ethereum τα οποία είναι παρόμοια σε βασική λειτουργικότητα με κάποιες μικρές διαφορές. Το "MetaMask" είναι ένα από τα δημοφιλέστερα, ασφαλή και υψηλού επιπέδου πορτοφόλια στην κοινότητα των κρυπτονομισμάτων. Είναι διαθέσιμο ως επέκταση προγράμματος περιήγησης και ως εφαρμογή για κινητά. Προτού εγκαταστήσουμε το Metamask, πρέπει να γνωρίζουμε ότι υποστηρίζει μόνο μερικά προγράμματα περιήγησης. Συγκεκριμένα υποστηρίζει τα ακόλουθα προγράμματα περιήγησης: Google Chrome, Mozilla Firefox και Opera.



Εικόνα 4.26: MetaMask Web Wallet

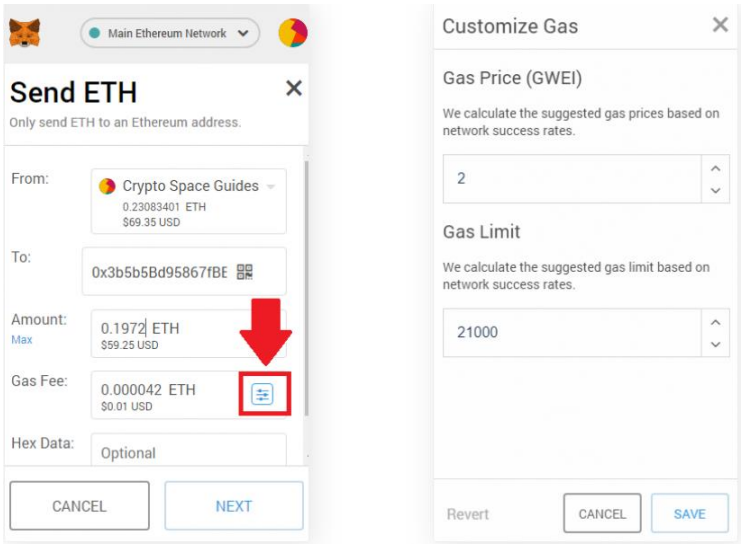
Αποστολή Ethereum

Ας δούμε τον τρόπο αποστολής ETH με το Metamask. Επιλέγουμε πρώτα το κουμπί αποστολής. Στη συνέχεια, εισαγάγετε το ποσό ETH για αποστολή και τη διεύθυνση ethereum του παραλήπτη. Επιλέγουμε το κουμπί "NEXT" για να συνεχίσουμε τη συναλλαγή.



Εικόνα 4.27: Αποστολή Ethereum

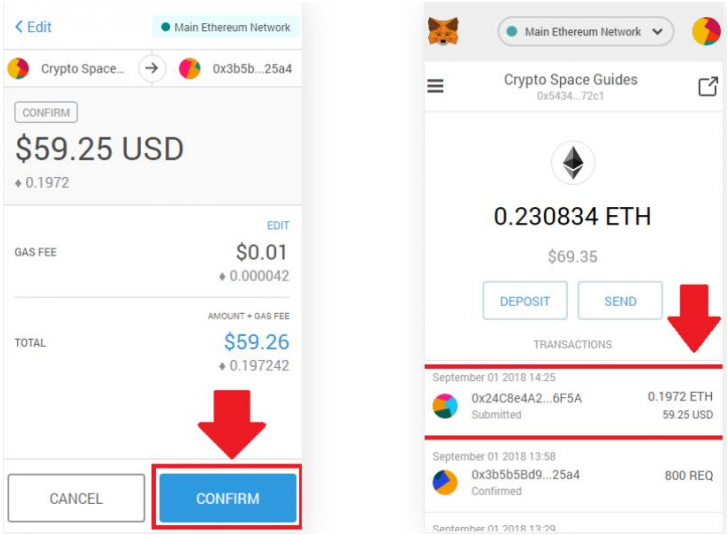
Το Metamask ορίζει δυναμικά ένα GASPRICE και ένα GASLIMIT που πρέπει να πληρώσει ο αποστολέας για να στείλει ETH. Ωστόσο, οι χρήστες μπορούν επίσης να εισαγάγουν μια προσαρμοσμένη τιμή gas, εάν θέλουν μια συναλλαγή να κοστίζει λιγότερο ή να προχωρήσει γρηγορότερα.



Εικόνα 4.28: Προσαρμογή GASPRICE και GASLIMIT για αποστολή ETH

Επιβεβαίωση Αποστολής

Το Metamask θα εμφανίσει μια τελική επιβεβαίωση στους χρήστες για να επανεξετάσουν τις συναλλαγές τους για τελευταία φορά. Ελέγξτε τη συναλλαγή και επιλέξτε επιβεβαίωση για να την επεξεργαστείτε. Με το που επιλέξει "CONFIRM" η συναλλαγή εμφανίζεται αμέσως στη λίστα συναλλαγών ως "υποβληθείσα". Όταν το Blockchain του Ethereum επιβεβαιώσει τη συναλλαγή τότε θα εμφανιστεί στη λίστα συναλλαγών ως “επιβεβαιωμένη”.

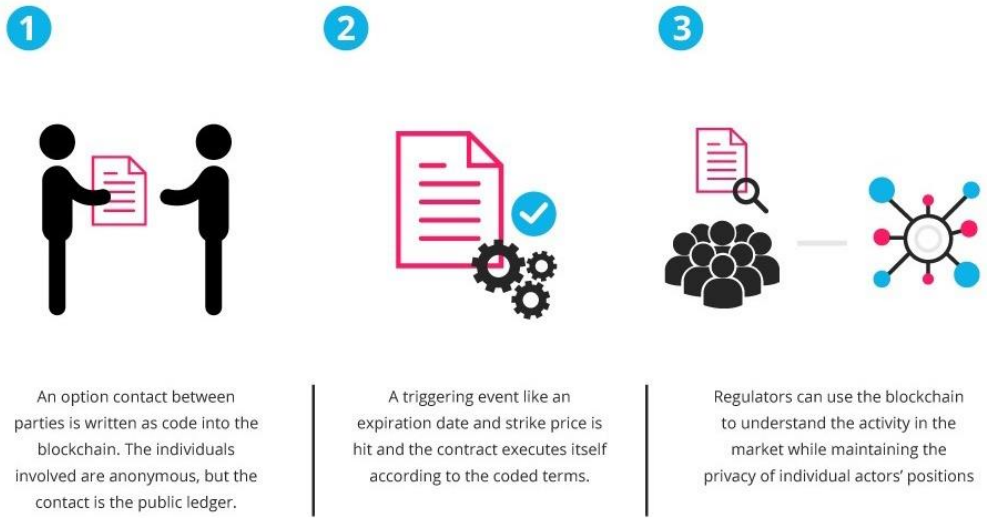


Εικόνα 4.29: Επιβεβαίωση Αποστολής

ΚΕΦΑΛΑΙΟ 5

Έξυπνα Συμβόλαια

Ο όρος «έξυπνα συμβόλαια» επινοήθηκε από τον επιστήμονα υπολογιστών Nick Szabo το 1994 για να τονίσει τη σύνδεση μεταξύ του πολύ ανεπτυγμένου δικαίου των συμβάσεων και των σχετικών επιστημονικών κλάδων, με το σχεδιασμό πρωτοκόλλων ηλεκτρονικού εμπορίου [45]. Τα έξυπνα συμβόλαια είναι γραμμές κώδικα που αποθηκεύονται σε ένα Blockchain και εκτελούνται αυτόματα όταν πληρούνται κάποιοι προκαθορισμένοι όροι και προϋποθέσεις [91]. Ο κώδικας περιέχει ένα σύνολο κανόνων βάσει των οποίων τα μέρη αυτού του συμβολαίου συμφωνούν να αλληλοεπιδρούν μεταξύ τους. Εάν και όταν πληρούνται οι προκαθορισμένοι κανόνες, η συμφωνία εφαρμόζεται αυτόματα. Τα έξυπνα συμβόλαια παρέχουν μηχανισμούς για την αποτελεσματική διαχείριση των διακριτικών στοιχείων και των δικαιωμάτων πρόσβασης μεταξύ δύο ή περισσότερων μερών. Κάποιος μπορεί να το σκεφτεί σαν ένα κρυπτογραφικό πλαίσιο που ξεκλειδώνει αξία ή πρόσβαση, εάν και όταν πληρούνται συγκεκριμένες προκαθορισμένες συνθήκες. Οι υποκείμενες τιμές και τα δικαιώματα πρόσβασης που διαχειρίζονται αποθηκεύονται σε ένα Blockchain, το οποίο είναι ένα διαφανές κοινόχρηστο καθολικό. Επομένως, παρέχουν έναν δημόσιο και επαληθεύσιμο τρόπο ενσωμάτωσης κανόνων διακυβέρνησης και επιχειρηματικής λογικής σε μερικές γραμμές κώδικα, οι οποίοι μπορούν να ελεγχθούν και να επιβληθούν με την πλειοψηφία συναίνεσης ενός δικτύου P2P [91].



Εικόνα 5.1 : Εκτέλεση έξυπνου συμβολαίου [94]

Τα οφέλη των έξυπνων συμβολαίων είναι πιο εμφανή στις επιχειρηματικές συνεργασίες, στις οποίες χρησιμοποιούνται συνήθως για την επιβολή κάποιου είδους συμφωνίας, έτσι ώστε όλοι οι συμμετέχοντες να μπορούν να είναι σίγουροι για το αποτέλεσμα χωρίς τη συμμετοχή ενός διαμεσολαβητή. Στόχος τους είναι να παρέχουν ασφάλεια, ανώτερη από την παραδοσιακή νομοθεσία περί συμβάσεων και να μειώσουν το κόστος συναλλαγής που σχετίζεται με τη σύμβαση. Μπορούν να πραγματοποιηθούν σε οποιαδήποτε συναλλαγή που απαιτεί καταχωρημένη συμφωνία μεταξύ των μερών, όπως, για παράδειγμα, τη σύναψη χρηματοοικονομικών ή ασφαλιστικών συμφωνιών, εγγυητικές καταθέσεις, την αγορά και πώληση χρηματοοικονομικών μέσων στα χρηματιστήρια, κοινοπρακτικά δάνεια, αγορά πώλησης δικαιωμάτων κ.ο.κ.

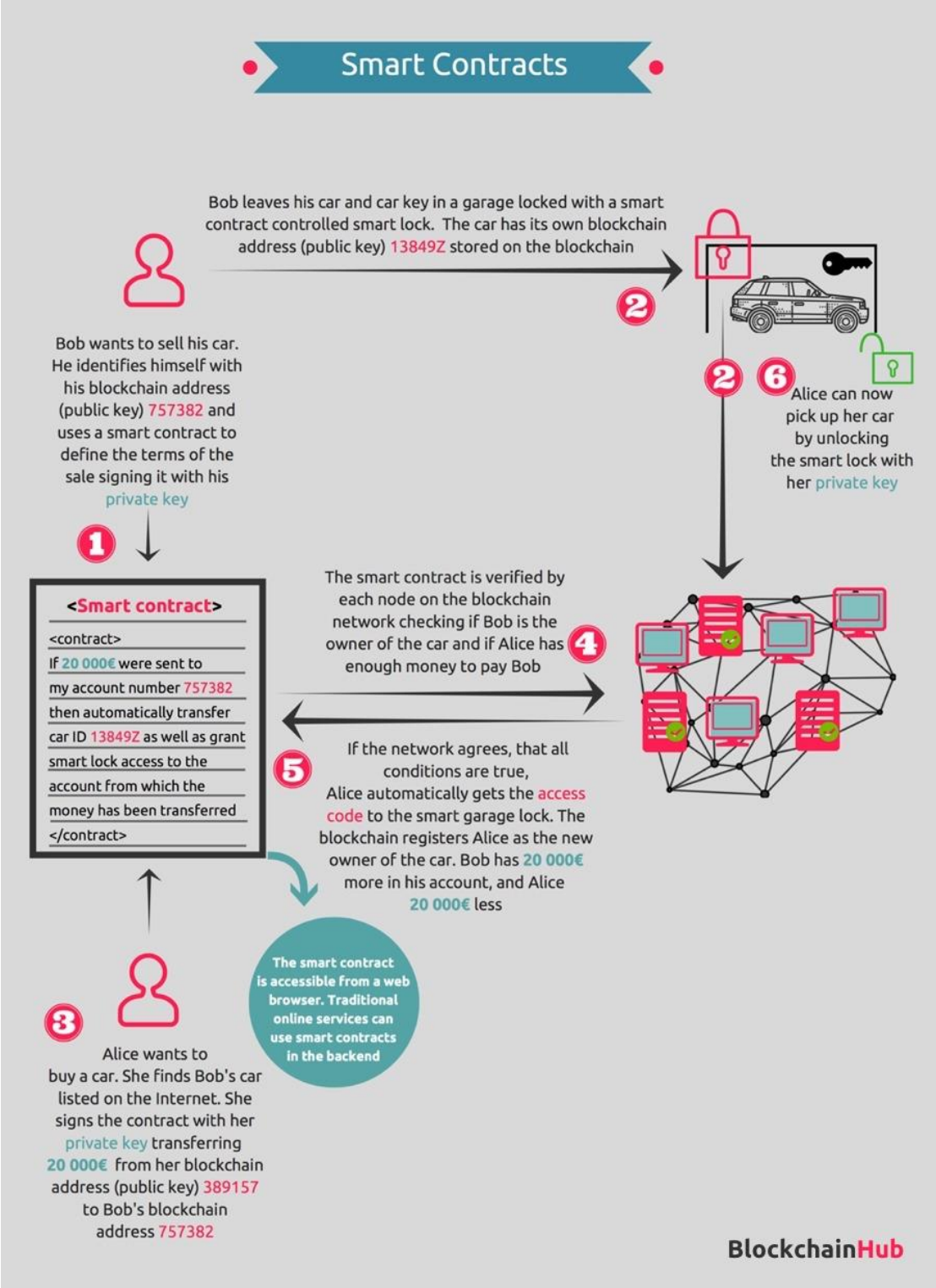
Οι περιπτώσεις χρήσης μπορούν να βρεθούν στον τραπεζικό τομέα, την ασφάλιση, την ενέργεια, την ηλεκτρονική διακυβέρνηση, τις τηλεπικοινωνίες, τη βιομηχανία μουσικής και κινηματογράφου, τον κόσμο της τέχνης, την εκπαίδευση και πολλά άλλα. Η χρήση τους κυμαίνεται από απλή ως πολύπλοκη. Ως απλές περιπτώσεις μπορούν να θεωρηθούν υπηρεσίες που σχετίζονται με κυβερνητικά μητρώα όπως πιστοποιητικά γέννησης, τίτλοι ιδιοκτησίας γης, σχολικά και πανεπιστημιακά πτυχία. Ενώ ως πιο σύνθετες περιπτώσεις χρήσης μπορούν να θεωρηθούν οι αποκεντρωμένοι αυτόνομοι οργανισμοί (DAO) [91].

Πώς λειτουργούν τα έξυπνα συμβόλαια

Τα έξυπνα συμβόλαια εκτελούνται στο Blockchain, ακριβώς όπως έχουν προγραμματιστεί, χωρίς δυνατότητα λογοκρισίας, διακοπή λειτουργίας, απάτη ή παρέμβαση τρίτων [92]. Λειτουργούν εκτελώντας εντολές «if…then…else» που είναι γραμμένες σε κώδικα σε ένα Blockchain. Το δίκτυο υπολογιστών του Blockchain μπορεί να εκτελέσει ενέργειες όπως: αποδέσμευση χρημάτων στα κατάλληλα μέρη, αποστολή ειδοποιήσεων, έκδοση εισιτηρίων κλπ., μόνο όταν πληρούνται και έχουν επαληθευτεί οι προκαθορισμένες προϋποθέσεις που έχουν οριστεί στο συμβόλαιο. Στη συνέχεια, το Blockchain ενημερώνεται όταν ολοκληρωθεί η συναλλαγή [92].

Έστω ότι ο Νίκος θέλει να αγοράσει ένα αυτοκίνητο από τον Μανώλη. Για να προχωρήσει αυτή η αγορά απαιτείται μια σειρά από αξιόπιστα τρίτα μέρη για την επαλήθευση και την επικύρωση της συμφωνίας. Η διαδικασία διαφέρει από χώρα σε χώρα, αλλά συνήθως περιλαμβάνει περισσότερα από ένα αξιόπιστα τρίτα μέρη όπως εφορία, υπουργείο μεταφορών, συμβολαιογράφοι και ασφαλιστικές εταιρείες. Είναι μια περίπλοκη και χρονοβόρα διαδικασία και ισχύουν σημαντικές χρεώσεις για όλα αυτά.

Εφόσον, όλες οι εμπλεκόμενες αρχές αποφασίσουν να προχωρήσουν σε μία λύση μέσω Blockchain, θα μπορούσε να χρησιμοποιηθεί ένα έξυπνο συμβόλαιο για τον καθορισμό όλων των κανόνων μιας έγκυρης αγοραπωλησίας. Εάν ο Νίκος θέλει να αγοράσει το αυτοκίνητο από τον Μανώλη χρησιμοποιώντας ένα έξυπνο συμβόλαιο στο Blockchain, η συναλλαγή θα πρέπει επαληθευτεί από κάθε κόμβο του δικτύου, για να ελεγχθεί αν ο Μανώλης είναι όντως ο ιδιοκτήτης του αυτοκινήτου και αν ο Νίκος έχει αρκετά χρήματα για να πληρώσει τον Μανώλη.



Εικόνα 5.2: Αγορά αυτοκινήτου με χρήση έξυπνου συμβολαίου [93]

Όταν το δίκτυο επαληθεύσει ότι ισχύουν και οι δύο προϋποθέσεις, ο Νίκος λαμβάνει αυτόματα τον κωδικό πρόσβασης που ανοίγει το γκαράζ που είναι τοποθετημένο το αυτοκίνητο. Το Blockchain καταγράφει τον Νίκο ως νέο ιδιοκτήτη του αυτοκινήτου. Ο λογαριασμός του Μανώλη πιστώνεται με το ποσό πώλησης του αυτοκινήτου, ενώ ο λογαριασμός του Νίκου χρεώνεται με το ποσό αγοράς. Η διαδικασία εκτέλεσης του του έξυπνου συμβολαίου παρουσιάζεται στη παρακάτω εικόνα.

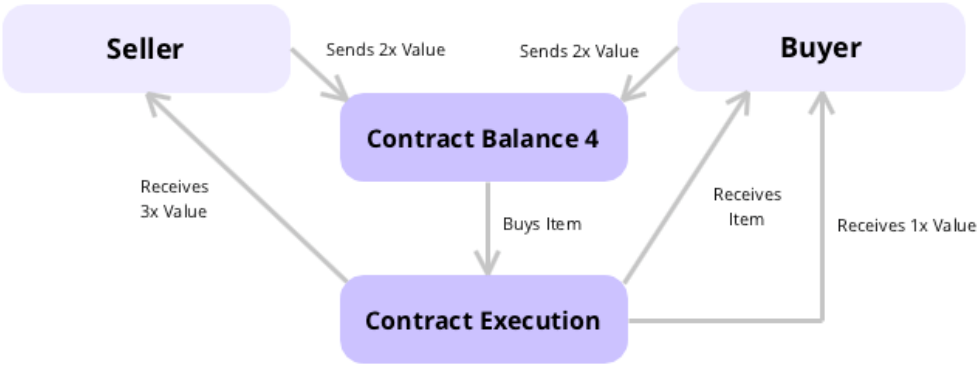
Πλατφόρμα Ethereum

Σήμερα, η δημοφιλέστερη πλατφόρμα έξυπνων συμβολαίων είναι η Ethereum Virtual Machine (EVM). Πρόκειται, για μία αποκεντρωμένη εικονική μηχανή που παρέχεται από το Ethereum ως περιβάλλον για εκτέλεση έξυπνων συμβολαίων. Η EVM μπορεί να θεωρηθεί ως ένας παγκόσμιος αποκεντρωμένος υπολογιστής στον οποίο εκτελούνται όλα τα έξυπνα συμβόλαια. Ένα έξυπνο συμβόλαιο στην EVM γράφετε σε γλώσσα προγραμματισμού Solidity (παρόμοια με την JavaScript) και ανεβαίνει στο Blockchain [46]. Μόλις προστεθεί στο Blockchain, στο έξυπνο συμβόλαιο εκχωρείται μια διεύθυνση, η οποία αποτελεί μοναδικό αναγνωριστικό του. Για να εξασφαλιστεί η σωστή διαχείριση πόρων της εικονικής μηχανής, κάθε εντολή που εκτελεί η EVM έχει ένα κόστος που σχετίζεται με αυτό, μετρούμενο σε μονάδες αερίου – «gas». Το gas είναι μονάδα που μετρά το ποσό της υπολογιστικής προσπάθειας που θα χρειαστεί για την εκτέλεση ορισμένων λειτουργιών (π.χ. εκτέλεση συναρτήσεων). Λειτουργίες που απαιτούν περισσότερο υπολογιστικό κόστος απαιτούν περισσότερες μονάδες αερίου συγκριτικά με λειτουργίες που απαιτούν λιγότερους υπολογιστικούς πόρους [46]. Αυτό εξασφαλίζει ότι το σύστημα δεν θα μπλοκαριστεί από επιθέσεις άρνησης υπηρεσίας, όπου οι χρήστες προσπαθούν να κατακλύσουν το δίκτυο με χρονοβόρους υπολογισμούς.

Παράδειγμα Ασφαλής απομακρυσμένης αγοράς με χρήση έξυπνου συμβολαίου

Σε αυτό το μέρος, παρουσιάζεται η υλοποίηση ενός έξυπνου συμβολαίου, ως συμφωνία μεταξύ ενός πωλητή και ενός αγοραστή για τον προγραμματισμό μιας απομακρυσμένης αγοράς.

Η κύρια ιδέα είναι ότι τόσο ο πωλητής όσο και ο αγοραστής στέλνουν διπλάσια την αξία του αντικειμένου σε Ether. Όταν ο αγοραστής το παραλάβει, παίρνει το ήμισυ της αξίας του Ether που κατέβαλε. Το άλλο μισό αποστέλλεται στον πωλητή ως πληρωμή. Ως εκ τούτου, ο πωλητής λαμβάνει τριπλή αξία της πώλησης του, καθώς λαμβάνει πίσω και την συνολική αξία σε Ether που κατέβαλε αρχικώς [95].



Εικόνα 5.3: Λειτουργία έξυπνου συμβολαίου [95]

Αναλυτική παρουσίαση υλοποίησης

```
pragma solidity >=0.4.22 <0.7.0;

contract Purchase {
    uint public value;
    address payable public seller;
    address payable public buyer;

    enum State { Created, Locked, Release, Inactive }
    // The state variable has a default value of the first member, `State
    State public state;

    modifier condition(bool _condition) {
        require(_condition);
        _;
    }

    modifier onlyBuyer() {
        require(
            msg.sender == buyer,
            "Only buyer can call this."
        );
        _;
    }
    modifier onlySeller() {
        require(
            msg.sender == seller,
            "Only seller can call this."
        );
        _;
    }

    modifier inState(State _state) {
        require(
            state == _state,
            "Invalid state."
        );
        _;
    }

    event Aborted();
    event PurchaseConfirmed();
    event ItemReceived();
    event SellerRefunded();

    // Ensure that `msg.value` is an even number.
    // Division will truncate if it is an odd number.
    // Check via multiplication that it wasn't an odd number.
    constructor() public payable {
        seller = msg.sender;
        value = msg.value / 2;
        require((2 * value) == msg.value, "Value has to be even.");
    }

    /// Abort the purchase and reclaim the ether.
    /// Can only be called by the seller before
    /// the contract is locked.
    function abort()
        public
        onlySeller
        inState(State.Created)
    {
        emit Aborted();
        state = State.Inactive;
        // We use transfer here directly. It is
        // reentrancy-safe, because it is the
        // last call in this function and we
        // already changed the state.
        seller.transfer(address(this).balance);
    }

    /// Confirm the purchase as buyer.
    /// Transaction has to include `2 * value` ether.
    /// The ether will be locked until confirmReceived
    /// is called.
    function confirmPurchase()
        public
        inState(State.Created)
        condition(msg.value == (2 * value))
        payable
    {
        emit PurchaseConfirmed();
        buyer = msg.sender;
        state = State.Locked;
    }

    /// Confirm that you (the buyer) received the item.
    /// This will release the locked ether.
    function confirmReceived()
        public
        onlyBuyer
        inState(State.Locked)
    {
        emit ItemReceived();
        // It is important to change the state first because
        // otherwise, the contracts called using `send` below
        // can call in again here.
        state = State.Release;

        buyer.transfer(value);
    }

    /// This function refunds the seller, i.e.
    /// pays back the locked funds of the seller.
    function refundSeller()
        public
        onlySeller
        inState(State.Release)
    {
        emit SellerRefunded();
        // It is important to change the state first because
        // otherwise, the contracts called using `send` below
        // can call in again here.
        state = State.Inactive;

        seller.transfer(3 * value);
    }
}
```

Εικόνα 5.4: Κώδικας υλοποίησης σε γλώσσα Solidity [96]

```
pragma solidity ^0.7.0;
```

- Έκδοση της Solidity

```
uint public value;
address payable public seller;
address payable public buyer;
```

Μεταβλητές του συμβολαίου

- **address payable**: είναι μια διεύθυνση στην οποία μπορούν να στείλουν Ether ο πωλητής και ο αγοραστής.

```
constructor() payable {
    seller = msg.sender;
    value = msg.value / 2;
    require((2 * value) == msg.value, "Value has to be even.");
  }
```

Κατασκευαστής (constructor) του συμβολαίου Purchase. Όταν το συμβόλαιο ενεργοποιηθεί στο Blockchain εκτελείται αυτόματα. Περιλαμβάνει, αρχικοποιήσεις των μεταβλητών seller και value.

- **msg.value** περιέχει το ποσό σε wei (1 wei = 0.000000000000000001 Ether) που αποστέλλεται στη συναλλαγή.

- **msg.sender** είναι η διεύθυνση του αποστολέα της συναλλαγής

Σε περίπτωση που η συνθήκη μέσα στο **require** δεν ισχύει τότε σταματάει η εκτέλεση του συμβολαίου και η συναλλαγή ακυρώνεται.

```
modifier onlyBuyer() {
    require(
      msg.sender == buyer,
      "Only buyer can call this."
    );
    _;
  }
```

Τροποποιητής (modifier) που ελέγχει εάν η διεύθυνση (**msg.sender**) είναι ίδια με τη διεύθυνση του αγοραστή που ορίζεται στο συμβόλαιο. Σε περίπτωση που η συνθήκη μέσα στο **require** δεν ισχύει τότε σταματάει η εκτέλεση του συμβολαίου και η συναλλαγή ακυρώνεται.

```
modifier onlySeller() {
    require(
        msg.sender == seller,
        "Only seller can call this."
    );
    _;
}
```

Τροποποιητής (modifier) που ελέγχει εάν η διεύθυνση (**msg.sender**) είναι ίδια με τη διεύθυνση του πωλητή που ορίζεται στο συμβόλαιο. Σε περίπτωση που η συνθήκη μέσα στο **require** δεν ισχύει τότε σταματάει η εκτέλεση του συμβολαίου και η συναλλαγή ακυρώνεται.

```
event Aborted();
```

- Ένα event που ονομάζεται Aborted. Θα ενεργοποιηθεί εάν κάποιο μέρος ακυρώσει την αγορά.

```
event PurchaseConfirmed();
```

- Ένα event που ονομάζεται PurchaseConfirmed. Θα ενεργοποιηθεί όταν ο αγοραστής επιβεβαιώσει την αγορά.

```
event ItemReceived();
```

- Ένα event που ονομάζεται ItemReceived. Θα ενεργοποιηθεί όταν ο αγοραστής λάβει το αντικείμενο που αγόρασε.

```
event SellerRefunded();
```

- Ένα event που ονομάζεται SellerRefunded. Θα ενεργοποιηθεί όταν ο αγοραστής λάβει τα κλειδωμένα χρήματα του.

```
function abort()
    public
    onlySeller
    inState(State.Created)
{
    emit Aborted();
    state = State.Inactive;
    seller.transfer(address(this).balance);
}
```

Η συνάρτηση **abort()** προκαλεί ακύρωση της αγοράς και ανάκτηση των Ether. Μπορεί να κληθεί μόνο από τον πωλητή πριν από το κλείδωμα του συμβολαίου.

```
function confirmPurchase()
    public
    inState(State.Created)
    condition(msg.value == (2 * value))
    payable
{
    emit PurchaseConfirmed();
    buyer = msg.sender;
    state = State.Locked;
}
```

Για να επιβεβαιώσει την πώληση, ο αγοραστής καλεί την **confirmPurchase()**. Η συναλλαγή τους πρέπει να περιλαμβάνει την διπλάσια αξία του αντικειμένου σε Ether (2 * value)

```
function confirmReceived()
    public
    onlyBuyer
    inState(State.Locked)
{
    emit ItemReceived();
    state = State.Release;

    buyer.transfer(value);
}
```

Το συμβόλαιο κρατάει τα Ether κλειδωμένα έως ότου ο αγοραστής καλέσει την **confirmReceived()**. Κάνοντας αυτό και επιβεβαιώνοντας ότι παρέλαβε το αγορασμένο αντικείμενο, τα κλειδωμένα Ether του αγοραστή απελευθερώνονται.

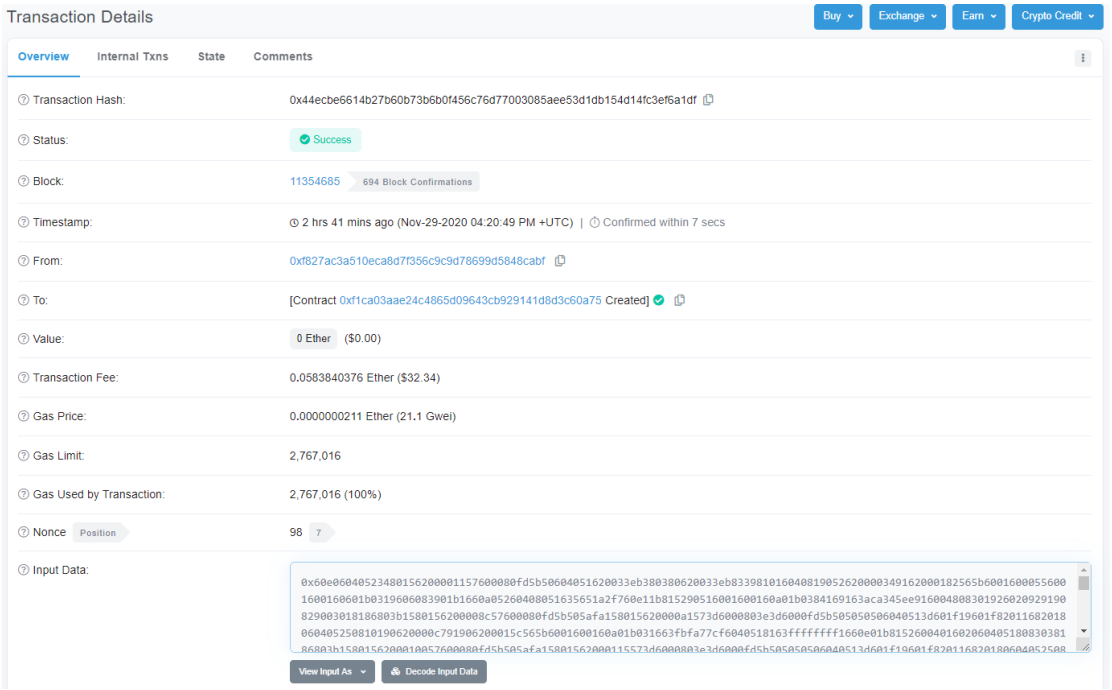
```
function refundSeller()
    public
    onlySeller
    inState(State.Release)
{
    emit SellerRefunded();
    state = State.Inactive;

    seller.transfer(3 * value);

}
```

Η συνάρτηση refundSeller() επιστρέφει τον πωλητή τα κλειδωμένα χρήματα του.

Συναλλαγή Δημιουργίας Συμβολαίου

Μια ειδική περίπτωση που πρέπει να αναφέρουμε είναι μια συναλλαγή που δημιουργεί ένα νέο συμβόλαιο στο Blockchain, αναπτύσσοντας το για μελλοντική χρήση. Οι συναλλαγές δημιουργίας συμβολαίου αποστέλλονται σε μια ειδική διεύθυνση προορισμού που ονομάζεται «μηδενική διεύθυνση» [31]. Το πεδίο παραλήπτη σε μια συναλλαγή δημιουργίας συμβολαίου περιέχει τη διεύθυνση 0x0. Δεν υπάρχει κανένα αντίστοιχο ζεύγος ιδιωτικού-δημόσιου κλειδιού, όπως γίνεται με μία κανονική συναλλαγή. Αυτή η συναλλαγή είναι μηδενική και δεν περιέχει καμία ποσότητα Ether.

Ενώ η μηδενική διεύθυνση προορίζεται μόνο για τη δημιουργία συμβολαίου, μερικές φορές λαμβάνει πληρωμές από διάφορες διευθύνσεις [31]. Υπάρχουν δύο εξηγήσεις για αυτό: είτε είναι από ατύχημα, με αποτέλεσμα την απώλεια Ether, ή είναι σκόπιμο για την καταστροφή Ether στέλνοντάς τα σε μια διεύθυνση από την οποία δεν μπορούν ποτέ να ξοδευτούν. Κάθε Ether που αποστέλλεται σε αυτή τη διεύθυνση θα γίνει αχρησιμοποίητο και θα χαθεί για πάντα [31].



Εικόνα 5.5: Επιτυχής δημιουργία συμβολαίου

Μια συναλλαγή δημιουργίας συμβολαίου πρέπει να περιέχει το μεταγλωττισμένο bytecode που θα δημιουργήσει το συμβόλαιο [31]. Όπως φαίνεται στη παραπάνω εικόνα αυτό εμφανίζεται στο πεδίο Input Data. Το μόνο αποτέλεσμα αυτής της συναλλαγής είναι η δημιουργία του συμβολαίου και τίποτα παραπάνω.

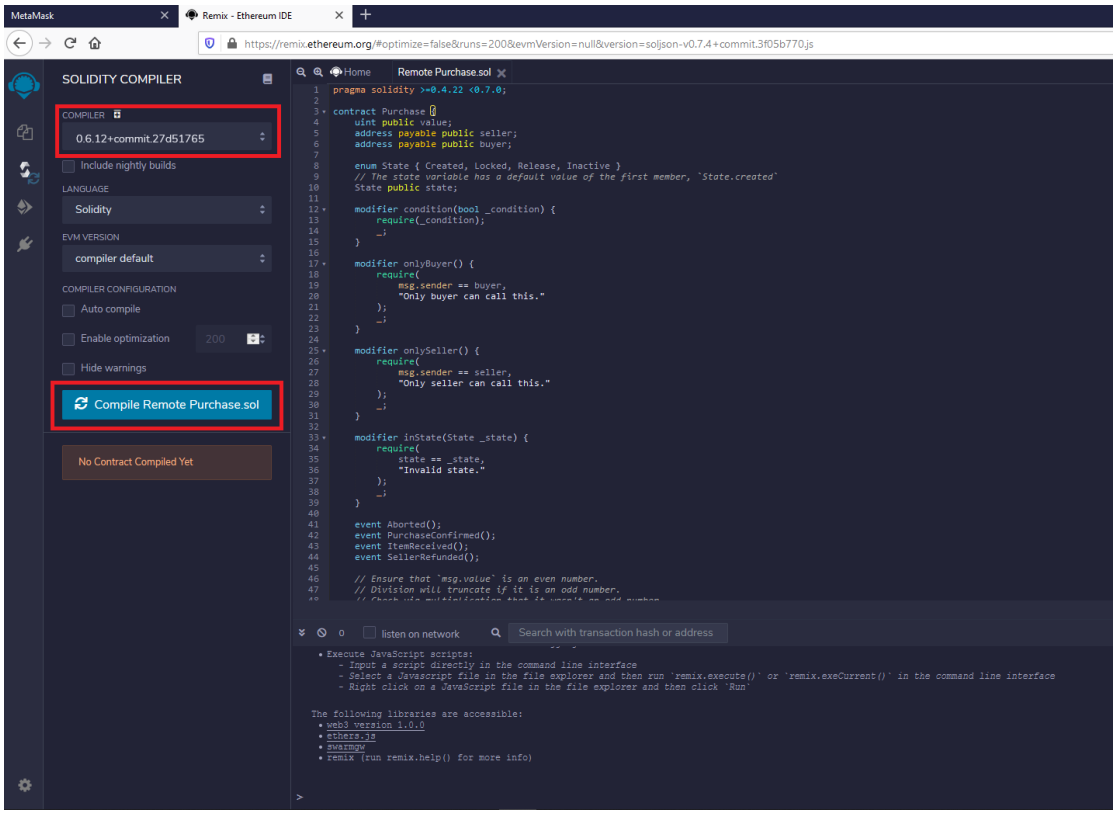
Σύνταξη και Ανάπτυξη Remote Purchase Συμβολαίου

Στο παρακάτω παράδειγμα θα υλοποιήσουμε την συναλλαγή δημιουργίας του συμβολαίου remote purchase που περιεγράφηκε παραπάνω. Για την ανάγκη αυτή θα χρησιμοποιήσουμε το Remix IDE. Το Remix IDE (Integrated Development Environment) είναι μια διαδικτυακή εφαρμογή που μπορεί να χρησιμοποιηθεί για τη σύνταξη, τον εντοπισμό σφαλμάτων στο κώδικα και την ανάπτυξη Smart Contracts. Η πρόσβαση στο Remix IDE μπορεί να γίνει με διαφορετικούς τρόπους: online μέσω προγράμματος περιήγησης ιστού όπως το Google Chrome, από ένα τοπικά εγκατεστημένο αντίγραφο ή από το Mist (το πρόγραμμα περιήγησης Ethereum Dapp). Για την ανάγκη της παρούσας διπλωματικής θα γίνει χρήση του IDE Remix In-Browser.

Μπορούμε να αποκτήσομε πρόσβαση στο Remix IDE από το πρόγραμμα περιήγησης ιστού που χρησιμοποιούμε χωρίς καμία ειδική εγκατάσταση. Εφόσον επισκεφθούμε τη διεύθυνση https://remix.ethereum.org θα παρουσιαστεί ένα πλήρες IDE με έναν επεξεργαστή κώδικα και διάφορα πάνελ για τη σύνταξη, την εκτέλεση και τον εντοπισμό σφαλμάτων των έξυπνων συμβολαίων.

Μεταγλώττιση συμβολαίου

Αφού γράψουμε το έξυπνο συμβόλαιο, θα πρέπει να γίνει μεταγλώττιση του κώδικα για να ελέγξουμε εάν υπάρχουν σφάλματα ή προειδοποιήσεις. Εάν δεν υπάρχουν σφάλματα, το έξυπνο συμβόλαιο είναι έτοιμο για ανάπτυξη. Για να συντάξουμε το έξυπνο συμβόλαιο, θα μεταβούμε στην καρτέλα "SOLIDITY COMPILER" και θα επιλέξουμε την έκδοση του μεταγλωττιστή. Η έκδοση πρέπει να συμφωνεί με αυτή που έχουμε ορίσει στην 1η γραμμή του κώδικα (στο παράδειγμα μας, θα χρησιμοποιήσουμε 0.6.12 + commit.27d51765).

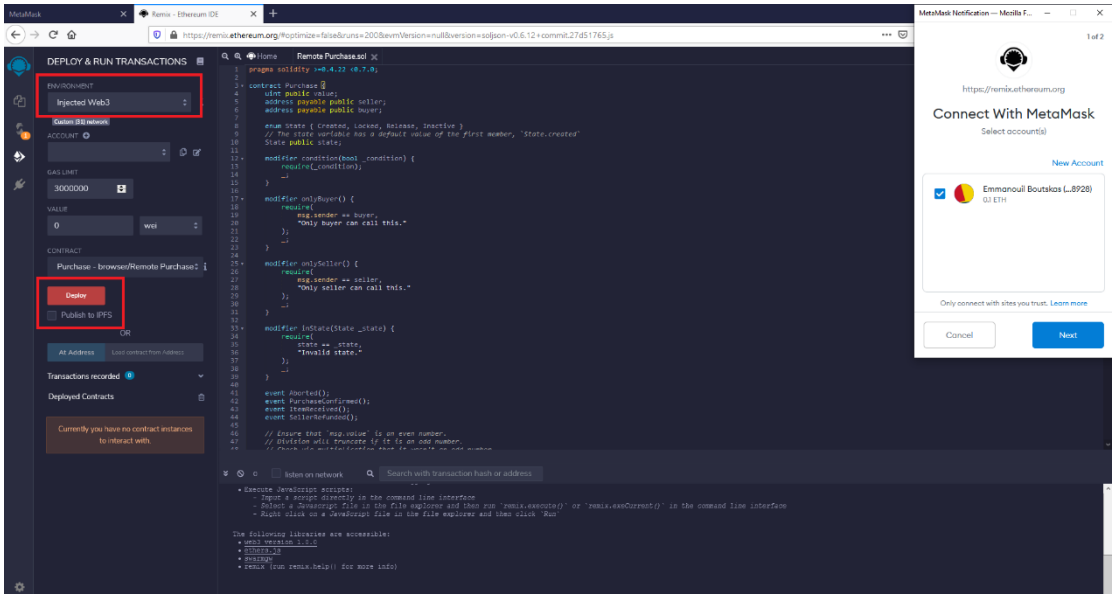


Εικόνα 5.6: Μεταγλώττιση συμβολαίου

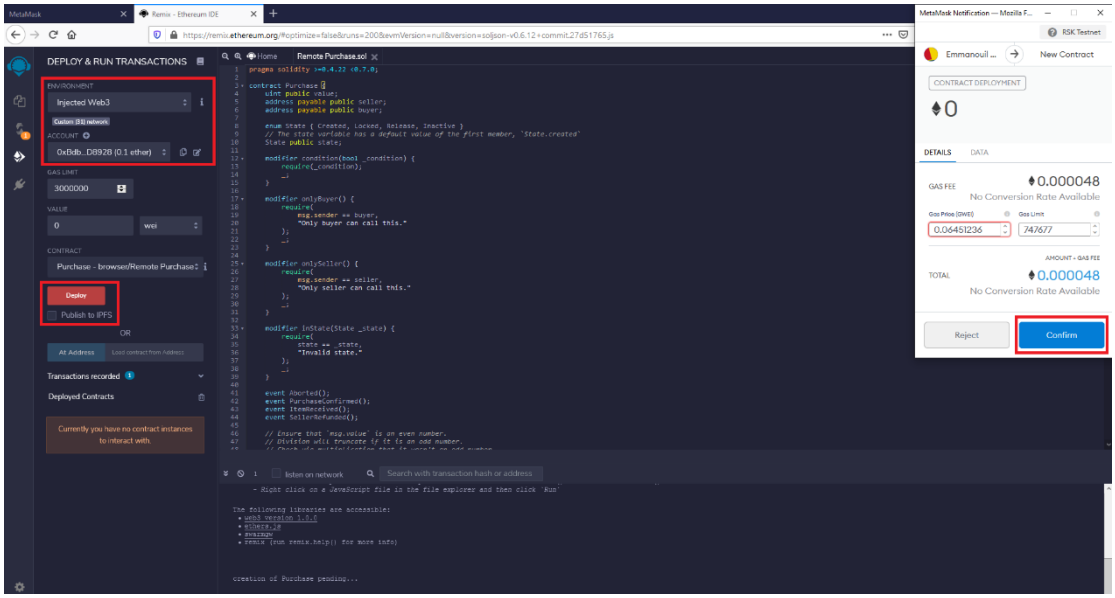
Ανάπτυξη συμβολαίου

Μετά την επιτυχή σύνταξη του συμβολαίου, μπορούμε πλέον να το αναπτύξουμε (deploy). Η ανάπτυξη το συμβολαίου θα μας επιτρέψει να το δοκιμάσουμε και να το χρησιμοποιήσουμε οπουδήποτε θέλουμε. Θα μεταβούμε στην καρτέλα “DEPLOY & RUN TRANSACTIONS” και θα ορίσουμε τις εξής παραμέτρους:

Εφόσον θα χρησιμοποιήσουμε το Metamask για να αναπτύξουμε το συμβόλαιό μας, θα επιλέξουμε το Injected Provider για το ENVIROMENT και στο πεδίο ACCOUNT θα συμπληρωθεί αυτόματα η διεύθυνση του λογαριασμού μας. Θα αφήσουμε τις άλλες επιλογές σε προεπιλογή. Στη συνέχεια, κάνουμε κλικ στο κουμπί “Deploy” για να αναπτύξουμε το συμβόλαιο. Θα εμφανιστεί ένα παράθυρο Metamask όπου θα πρέπει να επιβεβαιώσουμε την ανάπτυξη του συμβολαίου.

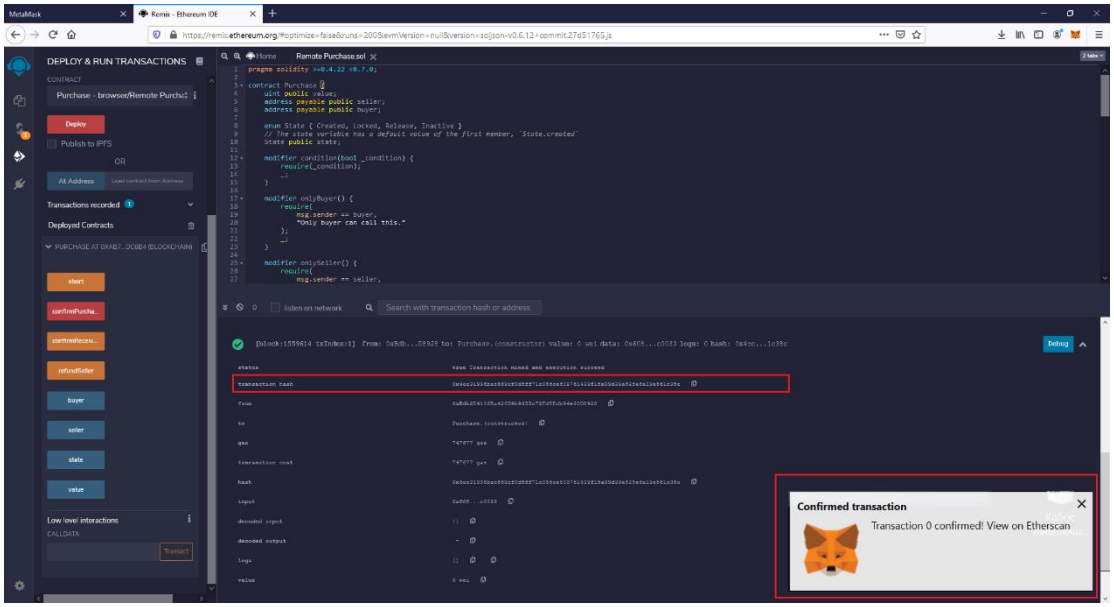


Εικόνα 5.7: Ανάπτυξη συμβολαίου



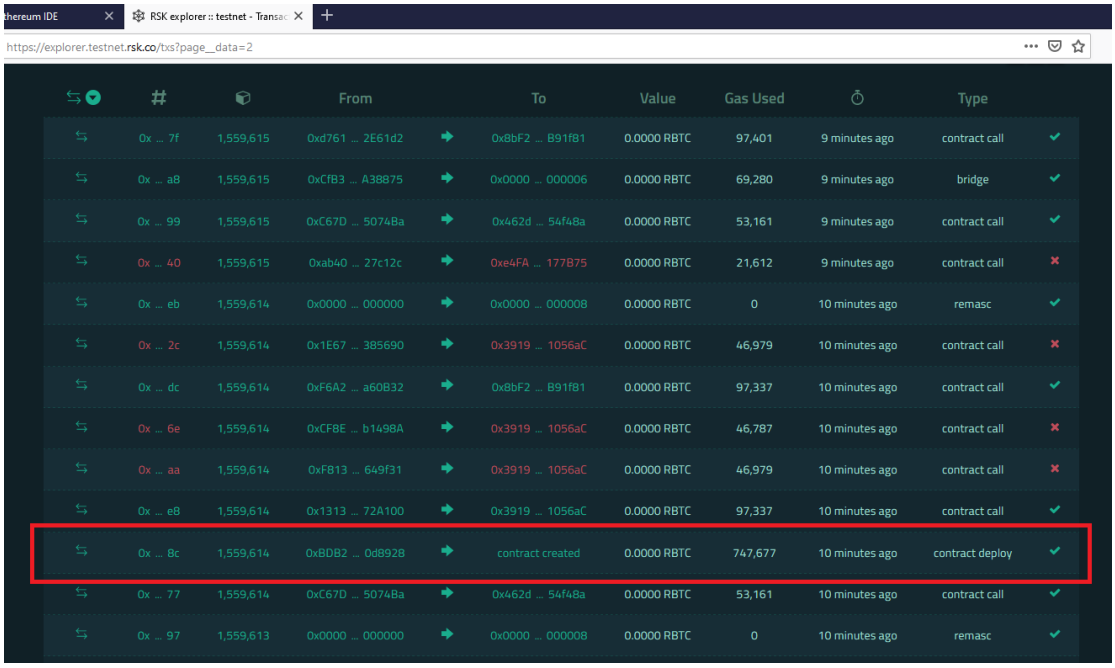
Εικόνα 5.8: Σύνδεση συμβολαίου με λογαριασμό

Μετά από κάποια λεπτά η συναλλαγή γίνεται επιτυχής και προστίθεται στο Blockchain. Αυτό φαίνεται στο μήνυμα που εμφανίζεται στο κάτω μέρος του παραθύρου.



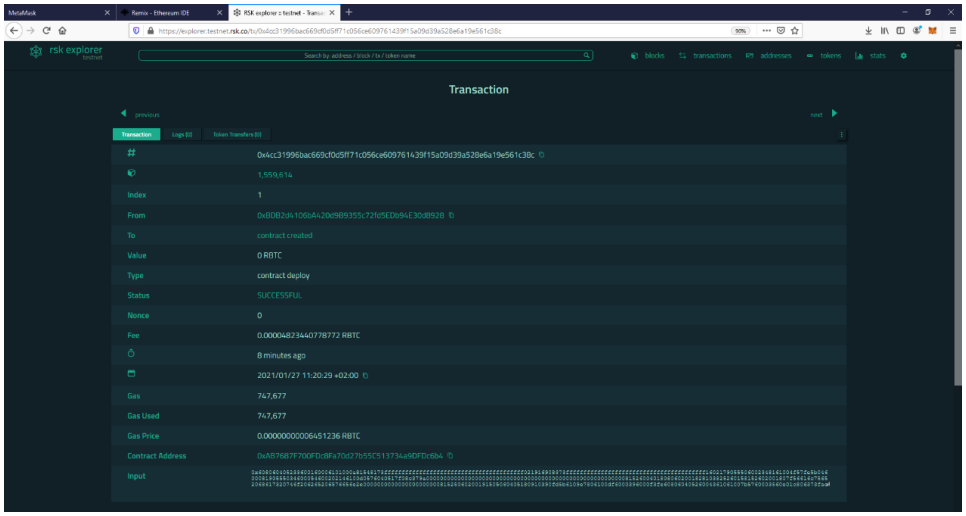
Εικόνα 5.9: Επιβεβαίωση συναλλαγής δημιουργίας του συμβολαίου

Ωστόσο για να ήμαστε επιπλέον σίγουροι για την επιτυχή εκτέλεση της συναλλαγής θα ελέγξουμε το Blockchain explorer του δικτύου RSK, το οποίο χρησιμοποιεί Bitcoin για την ανάπτυξη συμβολαίων σε αντίθεση με το δίκτυο του Ethereum που χρησιμοποιεί Ether. Παρατηρούμε ότι η συναλλαγή δημιουργίας του συμβολαίου μας εμφανίζεται όντως στον rsk explorer.

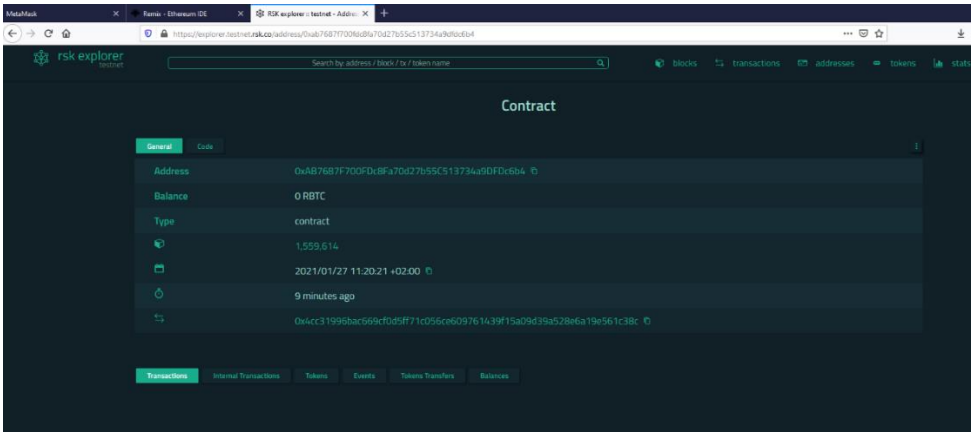


Εικόνα 5.10: Επιτυχής προσθήκη όπως συναλλαγής στον RSK Explorer

Με ένα κλικ πάνω όπως *https://explorer.testnet.rsk.co/tx/0x4cc31996bac669cf0d5ff71c056ce609761439f15a09d39a528e6a19e561c38c* μπορούμε να δούμε περισσότερες πληροφορίες όπως το input, contract address, gas used κλπ. Το συμβόλαιο είναι πλέον έτοιμο για χρήση.

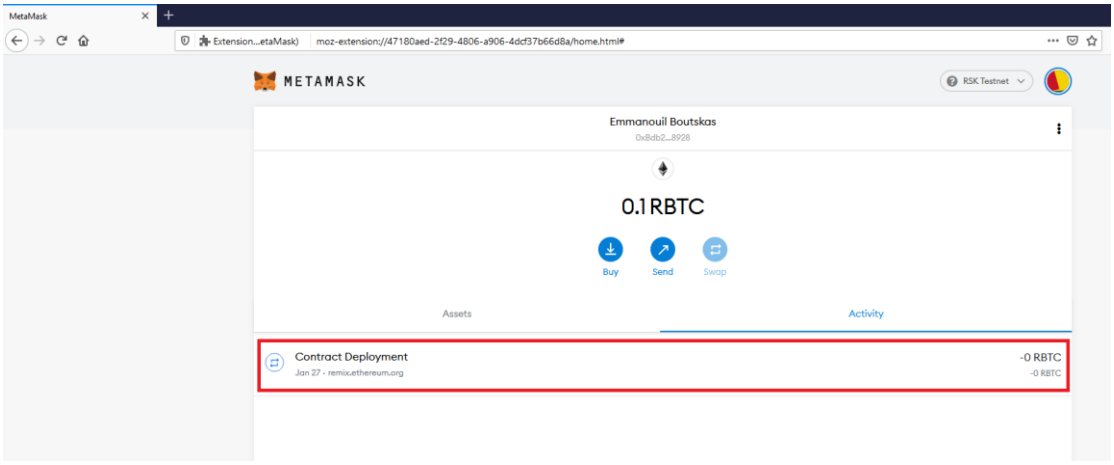


Εικόνα 5.11: Λεπτομέρειες συναλλαγής

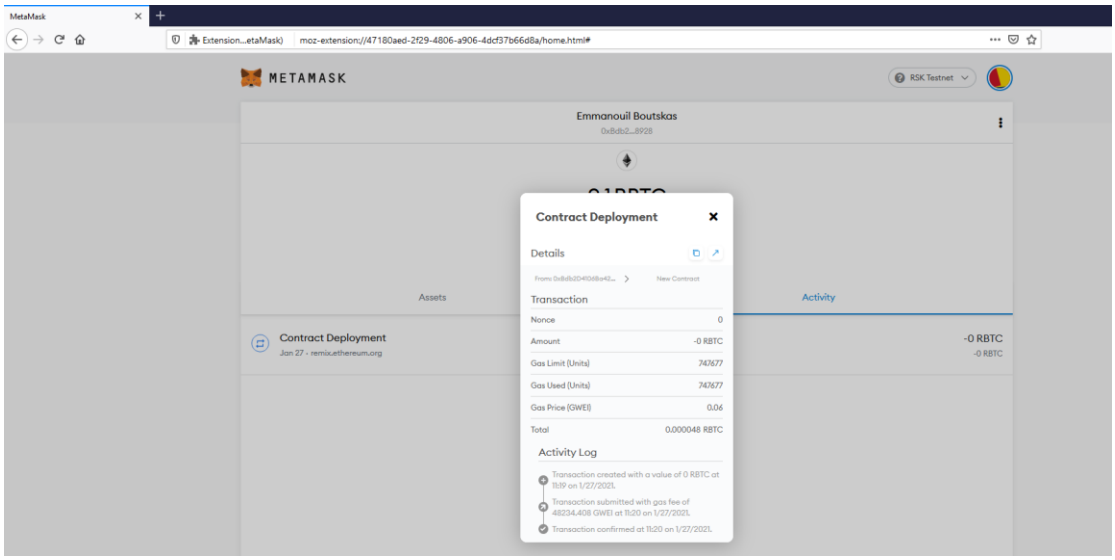


Εικόνα 5.12: Λεπτομέρειες συμβολαίου

Επιστρέφοντας στο Metamask μπορούμε να δούμε στην καρτέλα “Activity” το αποδεικτικό της δημιουργίας του συμβόλαιο.



Εικόνα 5.13: Αποδεικτικό δημιουργίας συμβολαίου



Εικόνα 5.14: Πληροφορίες ανάπτυξης συμβολαίου

Πλεονεκτήματα έξυπνων συμβολαίων

Τα έξυπνα συμβόλαια έχουν ήδη πολλαπλά πλεονεκτήματα έναντι των παραδοσιακών συμβολαίων. Αυτός ο αριθμός είναι πιθανόν να αυξηθεί στο μέλλον όσο βελτιώνεται η τεχνολογία [92].

Ταχύτητα: Τα έξυπνα συμβόλαια είναι ψηφιακά και αυτοματοποιημένα, επομένως δεν χρειάζεται επιπλέων χρόνος επεξεργασίας εγγράφων και διόρθωσης σφαλμάτων που συχνά παρατηρούνται σε έγγραφα που έχουν συμπληρωθεί με μη αυτόματο τρόπο. Από επιχειρηματική άποψη, η αυτοματοποίησή τους μπορεί να συμβάλει στον εξ ορθολογισμό των επιχειρηματικών δραστηριοτήτων και στην ενίσχυση της αποτελεσματικότητας, επιτρέποντας στους υπαλλήλους να επικεντρώνονται σε άλλες εργασίες.

Εμπιστοσύνη: Τα έξυπνα συμβόλαια εκτελούν αυτόματα συναλλαγές σύμφωνα με προκαθορισμένους κανόνες και οι κρυπτογραφημένες εγγραφές αυτών των συναλλαγών κοινοποιούνται σε όλους τους συμμετέχοντες. Επομένως, κανείς δεν μπορεί να αμφισβητεί ότι έχουν αλλάξει πληροφορίες για προσωπικό όφελος.

Ασφάλεια: Τα αρχεία συναλλαγών Blockchain είναι κρυπτογραφημένα και αυτό τα καθιστά πολύ δύσκολο να τροποποιηθούν από κακόβουλους χρήστες. Επειδή κάθε μεμονωμένη εγγραφή συνδέεται με προηγούμενες και επόμενες εγγραφές σε ένα κατανεμημένο καθολικό, ολόκληρη η αλυσίδα θα πρέπει να αλλάξει για να μεταβληθεί μία μόνο εγγραφή.

Εξοικονόμηση: Τα έξυπνα συμβόλαια αφαιρούν την ανάγκη για μεσάζοντες. Δεν υπάρχει ανάγκη για ένα επιπλέον άτομο να επικυρώσει και να επαληθεύσει τους όρους μιας συμφωνίας, επειδή είναι ήδη ενσωματωμένοι στον κώδικα.

Νομικά Ζητήματα και Περιορισμοί

Υπάρχουν ακόμη δυνητικά ζητήματα που πρέπει να επιλυθούν ώστε να διαδοθεί ευρέως η υιοθεσία των έξυπνων συμβολαίων. Δεδομένου ότι κάθε κόμβος πρέπει να επεξεργάζεται κάθε συναλλαγή, κάτι τέτοιο θα ήταν ανέφικτο με τον αριθμό των συμβολαίων και των χρηστών να μεγαλώνει καθημερινά. Το δεύτερο είναι η ορθότητα του κώδικα, καθώς τόσο οι προγραμματιστές όσο και οι χρήστες των έξυπνων συμβολαίων πρέπει να είναι σίγουροι ότι τα συμβόλαια εκτελούν τη προοριζόμενη χρήση τους και δεν εκτελούν άσκοπους υπολογισμούς αυξάνοντας τα τέλη συναλλαγής.

Από την άλλη πλευρά, υπάρχει και το ζήτημα της σχέσης μεταξύ ενός ηλεκτρονικού έξυπνου συμβολαίου και του νομικού ομολόγου του. Μέχρι στιγμής, τα έξυπνα συμβόλαια δεν είναι νομικά εκτελεστέα, αν και έχουν γίνει προσπάθειες προς αυτή την κατεύθυνση. Συγκεκριμένα, η ειδική επιτροπή για θέματα δικαιοδοσίας του Ηνωμένου Βασιλείου (UK Jurisdiction Taskforce) δημοσίευσε νομική δήλωση σχετικά με το καθεστώς των κρυπτονομισμάτωνν και των έξυπνων συμβάσεων, σύμφωνα με το δίκαιο της Αγγλίας και της Ουαλίας [47]. Εν ολίγοις, η νομική της δήλωση καταλήγει στο συμπέρασμα ότι τα κρυπτονομίσματα μπορούν να αποτελέσουν νομική μορφή ιδιοκτησίας και ότι τα έξυπνα συμβόλαια μπορούν, ανάλογα με τα γεγονότα, να πληρούν τις προϋποθέσεις για έγκυρη σύναψη δεσμευτικής και εκτελεστής σύμβασης μεταξύ των μερών.

Επιπρόσθετα, καταλήγει στο συμπέρασμα ότι οι συνήθεις κανόνες του αγγλικού δικαίου των συμβάσεων θα πρέπει να εφαρμόζονται στα έξυπνα συμβόλαια. Δεν υπάρχει λόγος να διακρίνονται από τα παραδοσιακά συμβόλαια, εφόσον υπάρχουν τα τρία βασικά χαρακτηριστικά της σύναψης παραδοσιακών συμβολαίων [47]. Εξηγεί ότι εάν ένα έξυπνο συμβόλαιο είναι σε θέση να δημιουργήσει δεσμευτικές νομικές υποχρεώσεις θα εξαρτηθεί από το κατά πόσον τα συμβαλλόμενα μέρη της έξυπνης σύμβασης ήταν σε θέση:

- Να επιτύχουν αντικειμενική συμφωνία ως προς τους όρους του συμβολαίου.
- Να αναπτύξουν μια νομικά δεσμευτική σχέση μεταξύ τους.
- Να παρέχουν κάτι ως αντάλλαγμα ο ένας στον άλλο, προκειμένου να καταστεί το συμβόλαιο εκτελεστέο.

Παρά τους περιορισμούς που υπάρχουν, η Gartner εκτιμά ότι έως το 2022, τα έξυπνα συμβόλαια θα χρησιμοποιούνται σε περισσότερο από το 25% των παγκόσμιων οργανισμών, επηρεάζοντας το παγκόσμιο εμπόριο [97]. Ο στόχος είναι να αφαιρεθεί η ασάφεια όσο το δυνατόν περισσότερο, προκειμένου ένα έξυπνο συμβόλαιο να αντικατοπτρίζει με ακρίβεια τη γραπτή νομική σύμβαση, έτσι ώστε να μπορεί να εφαρμοστεί στον πραγματικό κόσμο.

ΚΕΦΑΛΑΙΟ 7

Συμπεράσματα

Ο προσωπικός υπολογιστής (υλικό και λογισμικό), τα tablet και τα κινητά τηλέφωνα έχουν επηρεάσει σημαντικά τη ζωή των ανθρώπων έχοντας τεράστιο αντίκτυπο στην παγκόσμια αγορά και στην ανάπτυξη του οικονομικού συστήματος. Η αφοσίωση στο σχεδιασμό και τη δημιουργία μιας καλής εφαρμογής έχει αυξηθεί, λόγω της ζήτησης στην αγορά και της ταχύτητας ανάπτυξης της τεχνολογίας πληροφοριών. Η χρηματοοικονομική αγορά παρουσιάζει νέες τεχνολογίες κάθε μέρα, αλλά οι περισσότερες από αυτές δεν μπορούν να επιτύχουν ή να επιβιώσουν. Το Blockchain βρίσκεται στην παγκόσμια αγορά για περισσότερα από δέκα χρόνια και έχει εισβάλλει στη χρηματοοικονομική αγορά με σκοπό να αλλάξει τον τρόπο με τον οποίο υλοποιούνται οι ψηφιακές συναλλαγές. Πολλοί ειδικοί στην τεχνολογία του Blockchain εξετάζουν τα μοναδικά χαρακτηριστικά και τη μοναδική δομή αυτής της τεχνολογίας. Από τη σκοπιά του χρήστη, η νομοθεσία και η νομιμότητα είναι η πρώτη αξιωματική ανησυχία, ακολουθούμενη από περιβαλλοντικές μεταβλητές όπως η κοινωνική επίδραση, ο σχεδιασμός της τεχνολογίας και οι εμπειρίες των χρηστών [1]. Επιπλέον, πρέπει να ληφθούν υπόψη η εμπιστοσύνη και ο κίνδυνος. Οι πελάτες θεωρούν ότι το ρίσκο που υπάρχει γύρω από τα κρυπτονομίσματα είναι ο μεγαλύτερος κίνδυνος που σχετίζεται με τη τεχνολογία Blockchain. Για να αποφευχθεί αυτό, η τεχνολογία θα πρέπει να αποκτήσει αρκετή εμπιστοσύνη για να προχωρήσει στην εξαιρετικά ανταγωνιστική αγορά [12]. Πρόσφατα, η τεχνολογία Blockchain έχει γίνει το επίκεντρο για πολλές νέες πλατφόρμες, ειδικά για οικονομικές εφαρμογές. Ωστόσο, παρά την αύξηση της υιοθέτησης της, όσον αφορά τη χρήση των πελατών, το επίπεδο ήταν χαμηλότερο από το αναμενόμενο [12]. Αυτό οφείλεται στο ότι οι περισσότεροι άνθρωποι δεν είναι ακόμα εξοικειωμένοι με την ιδέα των κρυπτονομισμάτων προτιμώντας να χρησιμοποιούν τις παραδοσιακές υπηρεσίες τραπεζικών συναλλαγών, οι οποίες τους προκαλούν υψηλό κόστος λόγο της επιβάρυνσης των εξόδων συναλλαγής, χωρίς ιδιωτικό απόρρητο ή έλεγχο [2].

Τα τελευταία χρόνια σημειώθηκε σημαντική αλλαγή στη ρητορική που αναδύθηκε από το στρατόπεδο του Blockchain. Ενώ υπάρχουν ακόμα, και πιθανότατα θα υπάρξουν, βασικές ομάδες ενθουσιωδών υποστηρικτών που πιστεύουν στη τεχνολογία με μια ένταση που ταιριάζει μόνο με το κίνημα του ελεύθερου λογισμικού, το Blockchain δεν ανταποκρίνεται στις προσδοκίες ορισμένων χρηστών. Ένα ανώνυμο και αποκεντρωμένο σύστημα πληρωμών όπως αυτό του Bitcoin θα μπορούσε πράγματι να φέρει επανάσταση στην οικονομία, να βοηθήσει στον τερματισμό της δυσανάλογης ισχύος ορισμένων τραπεζικών συστημάτων και να εκδημοκρατίσει τη νομισματική ανταλλαγή. Ωστόσο, διάφορα σκάνδαλα και ισχυρισμοί απάτης σε συνδυασμό με τη σχετική δυσκολία στην απόκτηση και τη δαπάνη του, έχουν αποτρέψει αποφασιστικά την αντίληψη ότι το Bitcoin είναι το νόμισμα του μέλλοντος [8]. Το Blockchain σαν τεχνολογία είναι μια επαναστατική ιδέα για την επίτευξη αποκέντρωσης, αλλά η τρέχουσα εφαρμογή πάσχει από φιλελεύθερο οικονομικό δόγμα και κρίσιμα λάθη, όπως η πιθανότητα μιας οντότητας με πρόσβαση σε μεγάλη υπολογιστική ισχύ να αποκτήσει τον έλεγχο περιουσιακών στοιχείων. Τα κρυπτονομίσματα εξακολουθούν να εμφανίζουν σημαντικά εμπόδια που πρέπει να ξεπεραστούν προτού μπορέσουν να αντικαταστήσουν πλήρως τα τρέχοντα νομισματικά συστήματα. Το μεγαλύτερο όλων είναι η αντίθεση των υφιστάμενων χρηματοπιστωτικών ιδρυμάτων, τα οποία ασκούν μεγάλη δύναμη και έχουν κίνητρα για να αποθαρρύνουν τον πολλαπλασιασμό των κρυπτονομισμάτων [2]. Εκτός από την καταπολέμηση του τρέχοντος οικονομικού συστήματος, τα κρυπτονομίσματα έχουν κάποιες εσωτερικές προκλήσεις που πρέπει να ξεπεράσουν. Εξακολουθεί να μην είναι σαφές εάν η τεχνολογία Blockchain θα μπορούσε να προσαρμοστεί επιτυχώς σε περιπτώσεις που απαιτούνται πολύ υψηλές ταχύτητες με υψηλούς όγκους, κατά σειρά δευτερολέπτων αντί λεπτών. Ταυτόχρονα, λόγω του σημαντικού ενεργειακού κόστους και των μειωμένων ανταμοιβών με την πάροδο του χρόνου που σχετίζονται με τη διαδικασία της «εξόρυξης», οι χρήστες ενδέχεται τελικά να αναγκαστούν να υποστούν όλο και υψηλότερα και παράλογα κόμιστρα συναλλαγών.

Στο μακρινό μέλλον, τα παγκόσμια και εκδημοκρατισμένα κρυπτονομίσματα ίσως έχουν τη δυνατότητα να αντικαταστήσουν τα κλασσικά νομίσματα που υποστηρίζονται από τις κυβερνήσεις ως το κύριο μέσο διεξαγωγής χρηματοοικονομικών συναλλαγών. Έχοντας αυτό κατά νου, η Microsoft άρχισε να υλοποιεί δοκιμές προσομοίωσης μεγάλης κλίμακας για λογαριασμούς τραπεζών και άλλων μεγάλων εταιρειών που

ενδιαφέρονται να κατανοήσουν τις πιθανές συνέπειες για μια τόσο μεγάλη αλλαγή στην παγκόσμια οικονομία [98]. Προφανώς, είμαστε ακόμα στην αρχή της κατανόησης των δυνατοτήτων του Blockchain και γι’ αυτό τον λόγο είναι πολύ νωρίς να εκτιμηθούν όλες οι πτυχές και οι πλήρεις δυνατότητές του. Η έρευνα με προσανατολισμό τα οικονομικά και τα πληροφοριακά συστήματα σε συνδυασμό με την επιστήμη των υπολογιστών μπορεί να συνεισφέρει σημαντικές γνώσεις στη κατασκευή και διάδοση λύσεων Blockchain που θα αποτελέσουν την πύλη για συναλλαγές μεγάλης κλίμακας σε καθημερινή βάση.

Βιβλιογραφία

1. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.
2. Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through Blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking beyond banks and money* (pp. 239-278). Springer, Cham
3. Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied energy*, *195*, 234-246.
4. Gupta, S., & Sadoghi, M. (2019). Blockchain Transaction Processing.
5. Sukheja, D., Indira, L., Sharma, P. and Chirgaiya, S., 2019. Blockchain Technology: A Comprehensive Survey. Journal of Advanced Research in Dynamical and Control Systems, 11(0009-SPECIAL ISSUE), pp.1187-1203.
6. Nakamoto, S. (2019). *Bitcoin: A peer-to-peer electronic cash system*. Manubot.
7. Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.".
8. Van der Auwera, E., Schoutens, W., Giudici, M. P., & Alessi, L. (2020). Financial Risk Management for Cryptocurrencies.
9. Yadav, A. K., & Singh, K. (2020). Comparative Analysis of Consensus Algorithms of Blockchain Technology. In *Ambient Communications and Computer Systems* (pp. 205-218). Springer, Singapore.
10. Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of Blockchain technology: beyond myth. *Business & Information Systems Engineering*, 1-10.
11. Javarone, M. A., & Wright, C. S. (2018, June). From Bitcoin to Bitcoin Cash: a network analysis. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (pp. 77-81).

12. Gao, W., Hatcher, W. G., & Yu, W. (2018, July). A survey of Blockchain: techniques, applications, and challenges. In *2018 27th international conference on computer communication and networks (ICCCN)* (pp. 1-11). IEEE.
13. Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the Blockchain technology. In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.
14. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".
15. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin. *Applied Innovation*, *2*(6-10), 71.
16. Siddiqui, S. T., Ahmad, R., Shuaib, M., & Alam, S. (2020). Blockchain Security Threats, Attacks and Countermeasures. In *Ambient Communications and Computer Systems* (pp. 51-62). Springer, Singapore.
17. Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. (2018). Decentralized applications: The Blockchain-empowered software system. *IEEE Access*, *6*, 53019-53033.
18. Schwartz, D., Youngs, N., & Britto, A. (2014). The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, *5*(8).
19. Khan, M. A., Algarni, F., & Quasim, M. T. (2020). Decentralised Internet of Things. In *Decentralised Internet of Things* (pp. 3-20). Springer, Cham.
20. Voulgaris, S., Fotiou, N., Siris, V. A., Polyzos, G. C., Jaatinen, M., & Oikonomidis, Y. (2019). Blockchain Technology for Intelligent Environments. *Future Internet*, *11*(10), 213.
21. Waldo, J. (2019). A hitchhiker's guide to the Blockchain universe. *Communications of the ACM*, *62*(3), 38-42.
22. Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on Bitcoin's peer-to-peer network. In *24th {USENIX} Security Symposium ({USENIX} Security 15)* (pp. 129-144).
23. Lin, I. C., & Liao, T. C. (2017). A survey of Blockchain security issues and challenges. *IJ Network Security*, *19*(5), 653-659.

24. Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416-3452.
25. Lambert, N., & Bollen, B. (2014). The SAFE Network: a New, Decentralised Internet.
26. Johnston, D., Yilmaz, S. O., Kandah, J., Bentenitis, N., Hashemi, F., Gross, R., ... & Mason, S. (2014). The General Theory of Decentralized Applications, DApps.
27. Prusty, N. (2017). Building Blockchain projects. Packt Publishing Ltd.
28. Wright, A., & De Filippi, P. (2015). Decentralized Blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664.
29. Willett, J. R., Hidskes, M., Johnston, D., Gross, R., & Schneider, M. (2016). Omni Protocol Specification (formerly Mastercoin). white paper), accessed January, 28.
30. Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake Blockchain protocol. In *Annual International Cryptology Conference* (pp. 357-388). Springer, Cham.
31. Antonopoulos, A. M., & Wood, G. (2018). Mastering ethereum: building smart contracts and dapps. O'reilly Media.
32. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
33. Franco, P. (2014). Understanding Bitcoin: Cryptography, engineering and economics. John Wiley & Sons
34. Frey, D., Makkes, M. X., Roman, P. L., Taïani, F., & Voulgaris, S. (2016, December). Bringing secure Bitcoin transactions to your smartphone. In Proceedings of the 15th International Workshop on Adaptive and Reflective Middleware (pp. 1-6).
35. Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain enabled applications: understand the Blockchain ecosystem and how to make it work for you. Apress.
36. Vallois, V., & Guenane, F. A. (2017, October). Bitcoin transaction: From the creation to validation, a protocol overview. In 2017 1st Cyber Security in Networking Conference (CSNet) (pp. 1-7). IEEE.

37. He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., & Guizani, N. (2020). Security Analysis of Cryptocurrency Wallets in Android-based Applications. IEEE Network.
38. Lee, W. M. Beginning Ethereum Smart Contracts Programming. With Examples in Python, Solidity and JavaScript.
39. Biryukov, A., & Tikhomirov, S. (2019, April). Transaction clustering using network traffic analysis for Bitcoin and derived Blockchains. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 204-209). IEEE.
40. Dumas, J., Sygnet, P., & Xuereb, V. Bitcoin a Peer-to-Peer payment solution
41. Bulut, Y. E. (2019). Secure hardware cryptocurrency wallet within common criteria framework (Doctoral dissertation).
42. Gregory, D. (2018). Cryptocurrency and its forensic significance (Doctoral dissertation, Murdoch University).
43. Karame, G. O., & Androulaki, E. (2016). Bitcoin and Blockchain security. Artech House.
44. Jokić, S., Cvetković, A. S., Adamović, S., Ristić, N., & Spalević, P. (2019). Comparative analysis of cryptocurrency wallets vs traditional wallets. Ekonomika, 65(3), 65-75.
45. Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. arXiv preprint arXiv:1710.06372.
46. Wohrer, M., & Zdun, U. (2018, March). Smart contracts: security patterns in the ethereum ecosystem and solidity. In 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE) (pp. 2-8). IEEE.
47. Earls, J., Smith, M., & Smith, R. (2018). Smart Contracts: Is the Law Ready. Chamber of Digital Commerce.

Ιστοσελίδες

48. https://www.geeksforgeeks.org/proof-of-authority-consensus/
49. https://www.coinhouse.com/coinhouse-academy/Blockchain/what-is-proof-of-authority/
50. https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/
51. https://proofofstake.com/
52. https://www.investopedia.com/terms/p/proof-stake-pos.asp
53. https://coincodex.com/article/9961/ethereum-based-decentralized-advertising-project-adex-launches-governance-system/
54. https://maxthake.medium.com/what-is-proof-of-stake-pos-479a04581f3a
55. https://medium.com/coinmonks/Blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f
56. https://www.Bitcoinmining.com/
57. https://digiconomist.net/Bitcoin-energy-consumption
58. https://digiconomist.net/ethereum-energy-consumption
59. https://www.bitdegree.org/crypto/tutorials/Bitcoin-mining-hardware
60. https://www.investopedia.com/terms/m/mt-gox.asp
61. https://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6?r=UK&IR=T
62. https://data-flair.training/blogs/types-of-Blockchain/
63. https://selfkey.org/understanding-public-vs-private-Blockchain/
64. https://medium.com/@Equisafe/easily-understand-the-difference-between-private-Blockchain-and-public-Blockchain-2c4f9b2111b
65. https://en.Bitcoin.it/wiki/Off-Chain_Transactions
66. https://medium.com/swlh/everything-you-need-to-know-about-public-private-and-consortium-Blockchain-54821c159c7a
67. https://Blockchainhub.net/blog/blog/cryptography-Blockchain-Bitcoin/
68. https://wiredelta.com/decentralized-apps-vs-web-apps/
69. https://www.leewayhertz.com/what-are-dapps/
70. https://ethereum.org/en/whitepaper/#applications
71. https://www.namecoin.org/
72. https://litecoin.org/

73. https://currency.com/what-is-better-litecoin-or-Bitcoin
74. https://cryptocurrencynews.com/info/what-is-centra-ctr/
75. https://daedaluswallet.io/
76. https://cardano.org/
77. https://ethereum.org/en/developers/docs/dapps/
78. https://wiredelta.com/decentralized-apps-vs-web-apps/
79. https://selfkey.org/what-is-a-merkle-tree-and-how-does-it-affect-Blockchain-technology/
80. https://coinsutra.com/unspent-transaction-outputs-utxos/
81. https://marcsteiner.tech/blog/description-of-Bitcoin-blocks-and-transactions
82. https://learnmeaBitcoin.com/explorer/block/00000000000000000097727ff80963b3f94ae799fb19e51a880440679ad9af4
83. https://en.Bitcoin.it/wiki/Browser-based_wallet
84. https://www.ntirawen.com/2019/04/Bitcoin-deterministic-wallet-and-non.html
85. https://medium.com/cosmostation/the-magic-behind-a-mnemonic-phrase-and-hd-wallets-let-us-explain-43d9c97f6098
86. https://learnmeaBitcoin.com/technical/mnemonic#bip39-wordlist
87. https://www.coindesk.com/malware-anubis-cryptocurrency-wallets
88. https://blog.quantinsti.com/cryptocurrency-wallets-beginners-guide/
89. https://nomics.com/exchanges
90. https://www.Blockchain.com/charts/blocks-size
91. https://Blockchainhub.net/smart-contracts/
92. https://www.ibm.com/blogs/Blockchain/2018/07/what-are-smart-contracts-on-Blockchain/
93. https://qtronex.com/blockedu/Blockchain/what-is-Blockchain/
94. https://digital.hbs.edu/platform-digit/submission/ethereum-fueling-the-hype-around-Blockchain/
95. https://www.bitdegree.org/learn/solidity-examples#simple-auction
96. https://docs.soliditylang.org/en/v0.4.24/solidity-by-example.html#safe-remote-purchase
97. https://www.gartner.com/smarterwithgartner/why-Blockchains-smart-contracts-arent-ready-for-the-business-world/
98. https://news.Bitcoin.com/microsoft-cryptocurrency-system

Παράρτημα : Εγχειρίδιο εγκατάστασης πορτοφολιών

Σε αυτό το παράρτημα θα γίνει μια παρουσίαση των οδηγιών εγκατάστασης και χρήσης των πορτοφολιών που χρησιμοποιήθηκαν στο Κεφάλαιο 4.

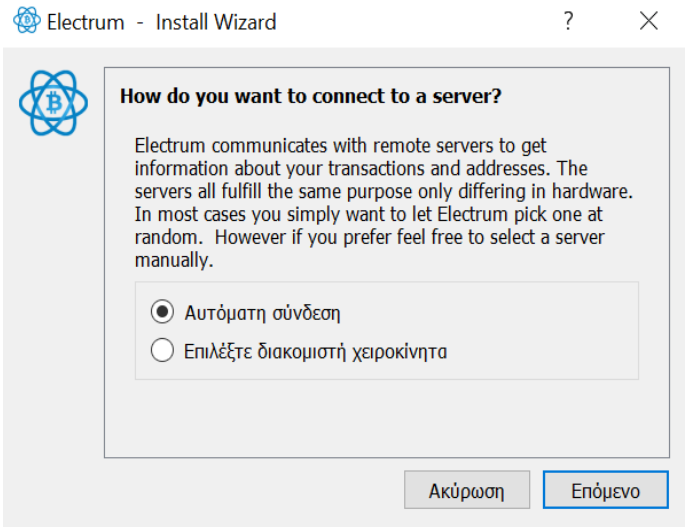
Τα βήματα που ακολουθούν παρακάτω πραγματοποιήθηκαν σε περιβάλλον Windows 10 Enterprise.

Electrum Bitcoin Wallet

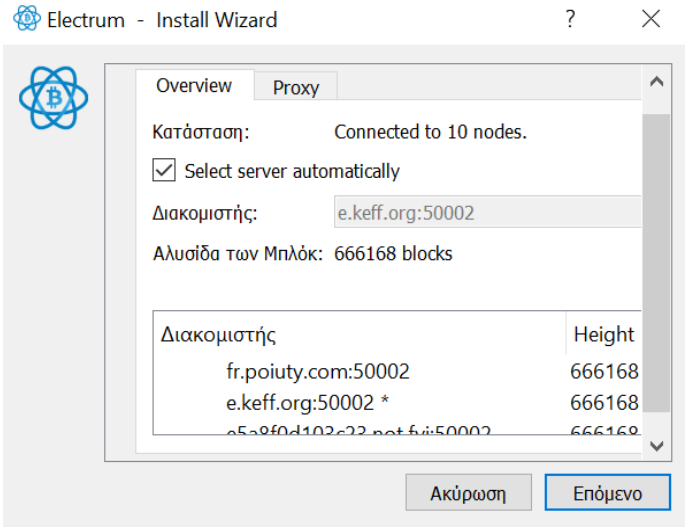
Το Electrum εστιάζει στη ταχύτητα, με χαμηλή χρήση πόρων και απλοποίηση της υλοποίησης των συναλλαγών. Από προεπιλογή, το Electrum προσπαθεί να διατηρήσει συνδέσεις με ~10 διακομιστές. Οι χρόνοι εκκίνησης είναι στιγμιαίοι επειδή λειτουργούν σε συνδυασμό με διακομιστές υψηλής απόδοσης που χειρίζονται τα πιο περίπλοκα μέρη του συστήματος Bitcoin. Λειτουργεί ως light client και δεν στέλνει ποτέ ιδιωτικά κλειδιά στους διακομιστές. Επιπλέον, επαληθεύει τις πληροφορίες που αναφέρονται από διακομιστές, χρησιμοποιώντας μια τεχνική που ονομάζεται απλή επαλήθευση πληρωμής (Simple Payment Verification).

Βήμα 1: Θα χρειαστεί το εκτελέσιμο αρχείο της εφαρμογής (electrum-4.0.9-setup.exe) το οποίο βρίσκεται εδώ: https://electrum.org/#download.

Βήμα 2: Θα πρέπει να επιλεχθεί ο server με τον οποίο θα επικοινωνεί το Electrum. Ο χρήστης έχει 2 επιλογές: **i)** *Αυτόματη σύνδεση* όπου το Electrum διαλέγει έναν server τυχαία και **ii)** *Χειροκίνητη επιλογή* όπου ο χρήστης διαλέγει τον server που θέλει από τη λίστα που προσφέρει το Electrum.

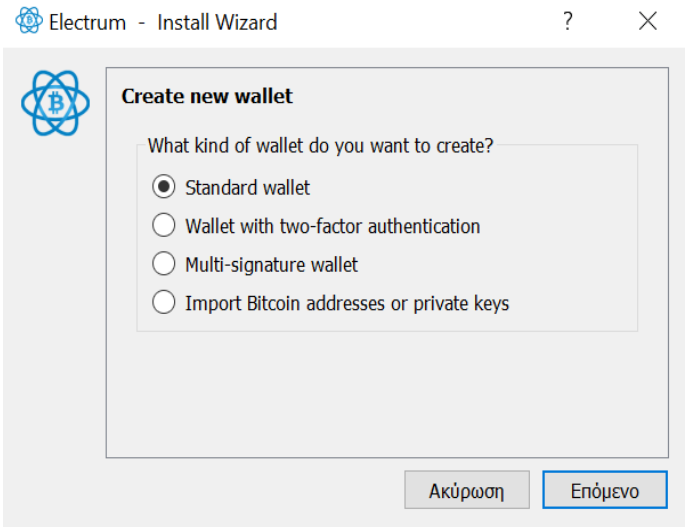


Εικόνα 1: Αυτόματη σύνδεση σε server

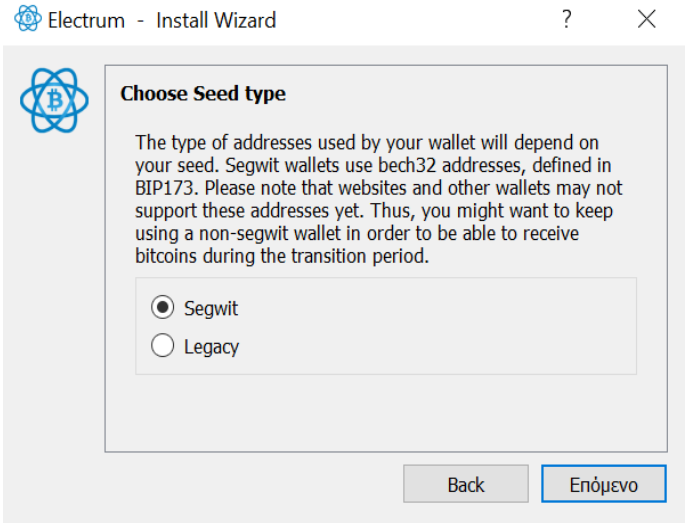


Εικόνα 2: Χειροκίνητη επιλογή server

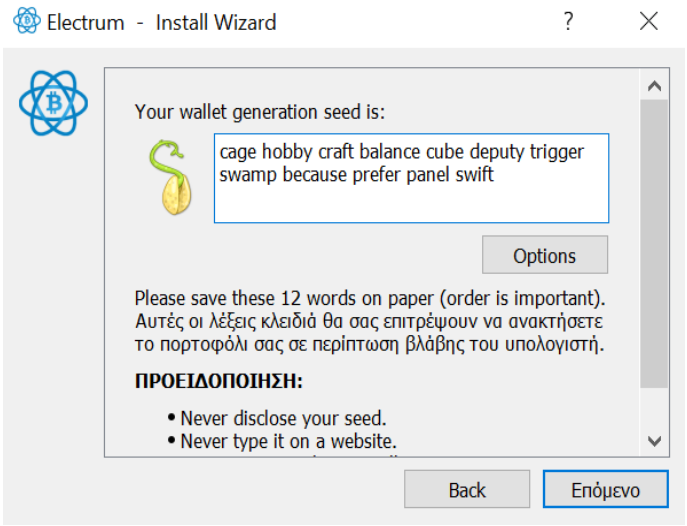
Βήμα 3: Θα χρειαστεί να επιλεχθεί ο τύπος πορτοφολιού που θέλουμε να δημιουργήσουμε καθώς και ο τύπος της μνημονικής φράσης που θέλουμε να παραχθεί. Η μνημονική φράση μπορεί να βασίζεται στο πρότυπο BIP173 (Segwit) ή όχι (Legacy). Το Electrum δίνει της εξής επιλογές.



Εικόνα 3: Τύπος πορτοφολιού

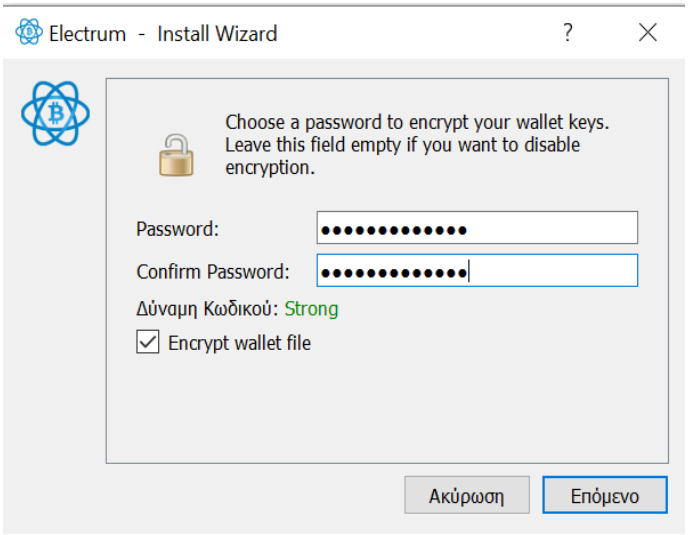


Εικόνα 4: Τύπος μνημονικής φράσης



Εικόνα 5: Μνημονική φράση τύπου Segwit

Βήμα 4: Θα χρειαστεί να εισάγουμε ένα κωδικό πρόσβασης στο πορτοφόλι τον οποίο θα χρησιμοποιούμε κάθε φορά που θα συνδεόμαστε σε αυτό. Μετά από αυτό το βήμα έχει τελειώσει η παραμετροποίηση του πορτοφολιού και είναι έτοιμο προς χρήση.



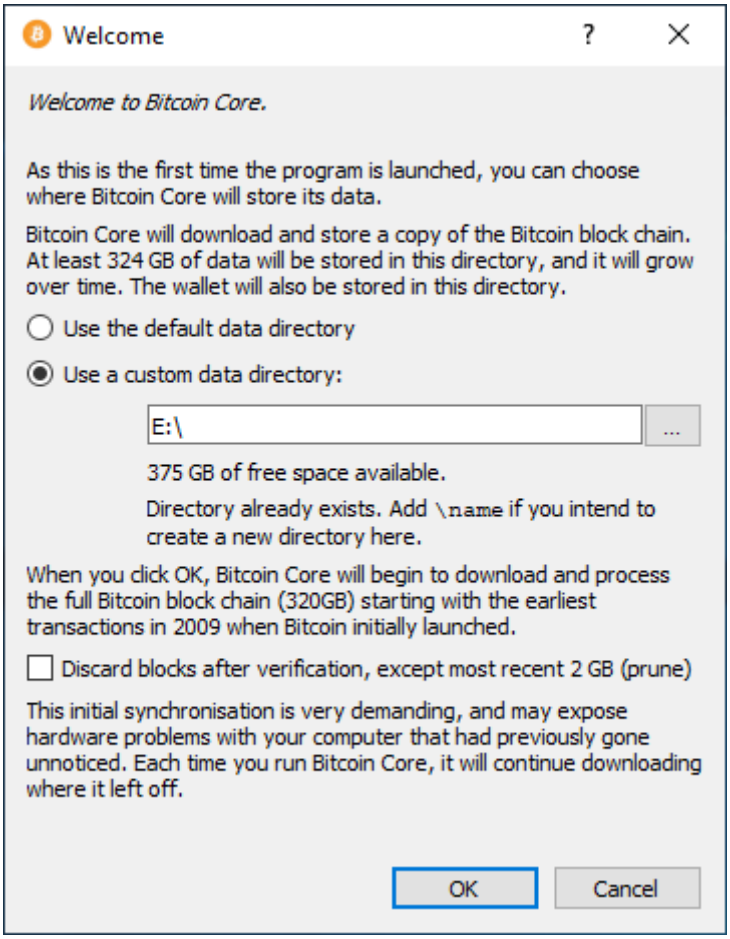
Εικόνα 6: Επιλογή κωδικού πρόσβασης

Bitcoin Core Wallet

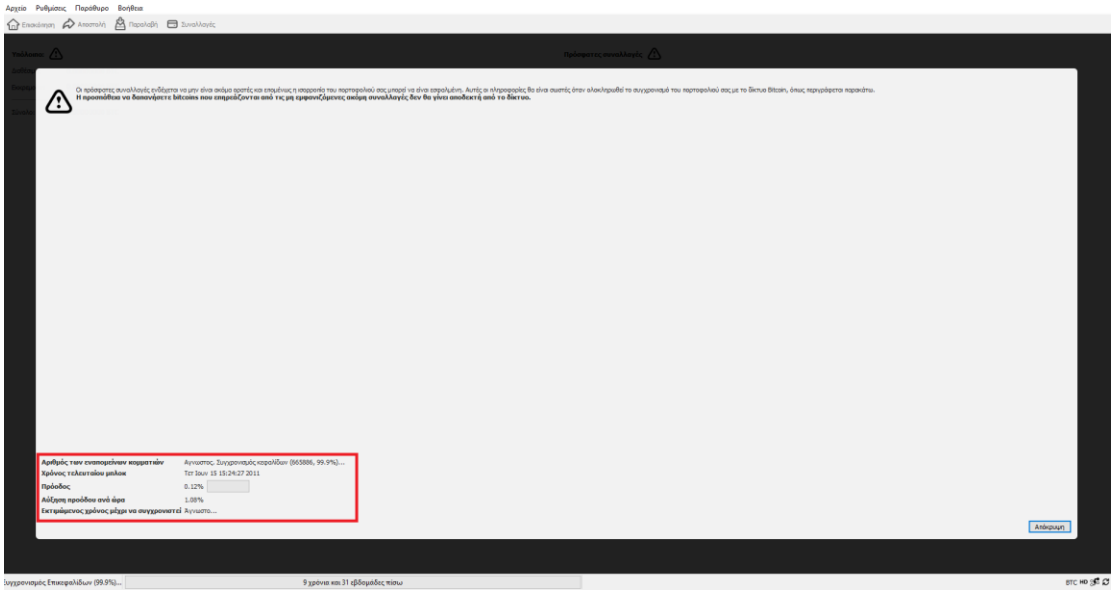
Το Bitcoin Core είναι ένας πλήρης πελάτης (full client). Αυτό το πορτοφόλι είναι ένας πλήρης κόμβος που επικυρώνει και μεταδίδει συναλλαγές στο δίκτυο του Bitcoin. Αυτό σημαίνει ότι δεν απαιτείται εμπιστοσύνη σε τρίτο μέρος κατά την επαλήθευση πληρωμών. Οι πλήρεις κόμβοι παρέχουν το υψηλότερο επίπεδο ασφάλειας και είναι απαραίτητοι για την προστασία του δικτύου. Ωστόσο, απαιτούν περισσότερο χώρο (πάνω από 350 GB), εύρος ζώνης και μεγαλύτερο αρχικό χρόνο συγχρονισμού.Το Bitcoin Core ως ένας τέτοιος κόμβος προσφέρει υψηλά επίπεδα ασφάλειας, απορρήτου και σταθερότητας.

Βήμα 1: Θα χρειαστεί το εκτελέσιμο αρχείο της εφαρμογής (Bitcoin-0.21.0-win64-setup.exe) το οποίο βρίσκεται εδώ: https://Bitcoin.org/en/download.

Βήμα 2: Μετά την εγκατάσταση του πορτοφολιού θα χρειαστεί να γίνει συγχρονισμός με το Blockchain του Bitcoin έτσι ώστε να κατεβάσει όλα τα block που υπάρχουν στο δίκτυο, ξεκινώντας από το genesis block μέχρι και το πιο πρόσφατο. Η λήψη του Blockchain απαιτεί χώρο μεγαλύτερο των 300 GB.

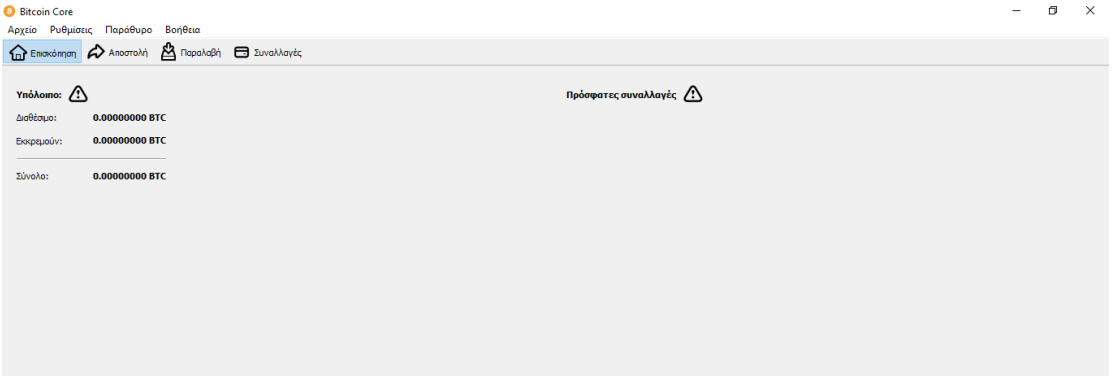


Εικόνα 7: Επιλογή path αποθήκευσης του Blockchain



Εικόνα 8: Λήψη Blockchain Bitcoin

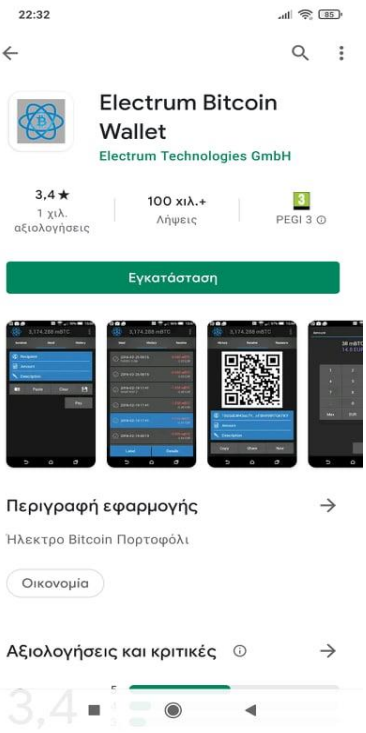
Βήμα 3: Μετά το τέλος του συγχρονισμού το πορτοφόλι είναι έτοιμο για χρήση



Εικόνα 9: Bitcoin core wallet διεπαφή χρήστη

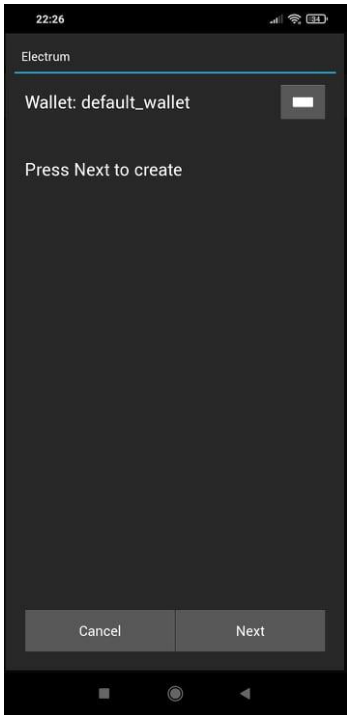
Electrum Bitcoin Mobile Wallet

Βήμα 1: Σε αυτό το βήμα απαιτείται αρχικά η λήψη και εγκατάσταση της εφαρμογής από το Google Play Store.

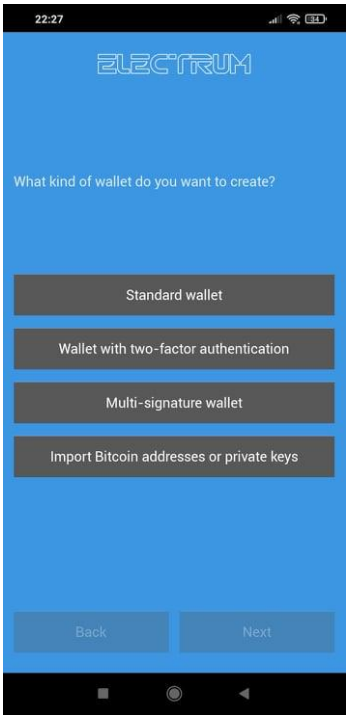


Εικόνα 10: Electrum Mobile Wallet Google Play Store

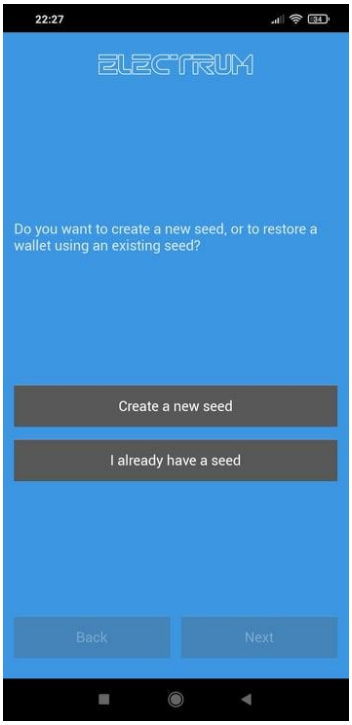
Βήμα 2: Εφόσον έχει εγκατασταθεί η εφαρμογή, ξεκινά η δημιουργία και παραμετροποίηση του πορτοφολιού. Η παρακάτω παραμετροποίηση βασίζεται σε δημιουργία πορτοφολιού με έλεγχο ταυτότητας δύο παραγόντων (2FA). Η συγκεκριμένη τεχνική προσθέτει ένα επιπλέον επίπεδο ασφάλειας στο λογαριασμό του χρήστη. Πέρα από τον κωδικό πρόσβασης το πορτοφόλι θα προστατεύεται επιπλέον με έναν κωδικό που θα είναι σε μορφή κειμένου.



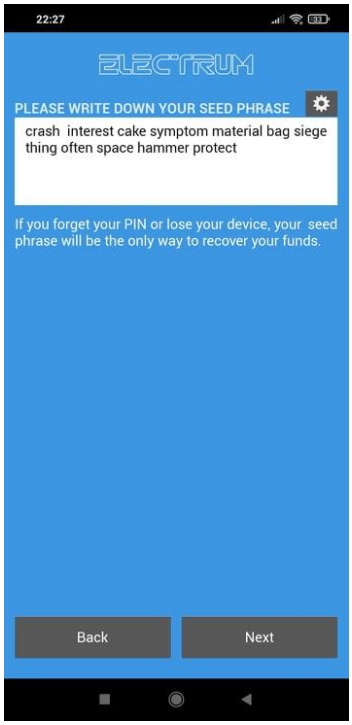
Εικόνα 11: Δημιουργία νέου πορτοφολιού



Εικόνα 12: Διαθέσιμοι τύποι πορτοφολιών

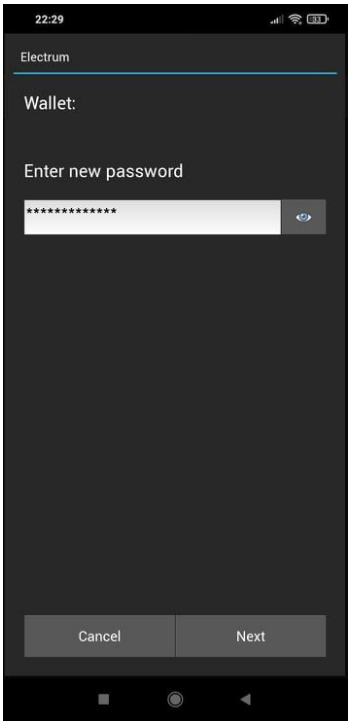


Εικόνα 13: Δημιουργία νέας ή χρήση υπάρχουσας μνημονικής φράσης

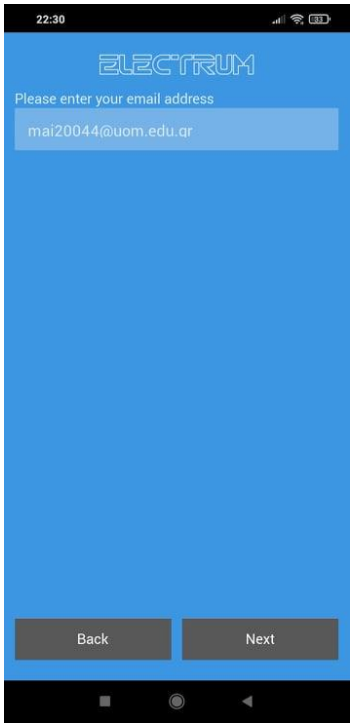


Εικόνα 14: Μνημονική φράση

Εικόνα 15: Επιβεβαίωση μνημονικής φράσης

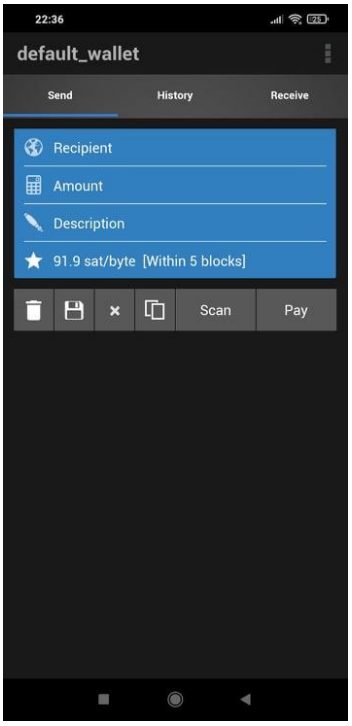


Εικόνα 16: Εισαγωγή κωδικού ασφαλείας



Εικόνα 17: Email με το οποίο θα συνδεθεί το πορτοφόλι

Εικόνα 18: Ανάκτηση κωδικού ασφαλείας μέσω σκαναρίσματος QR Code. Ο παρών κωδικός απαιτείται γα την δημιουργία του πορτοφολιού

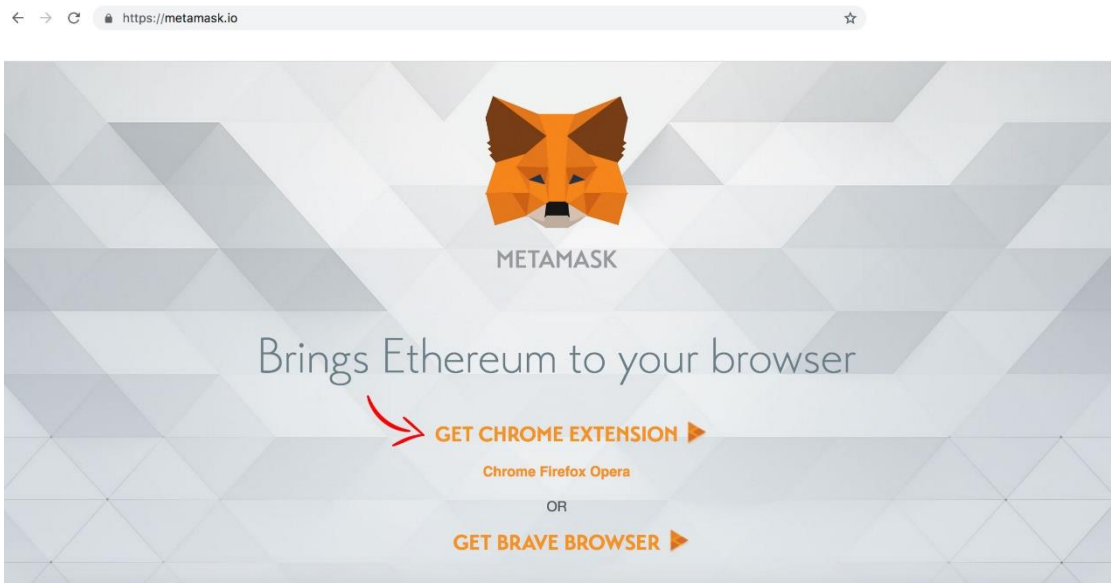


Εικόνα 19: Διεπαφή χρήστη μετα την δημιουργία του electrum mobile wallet.

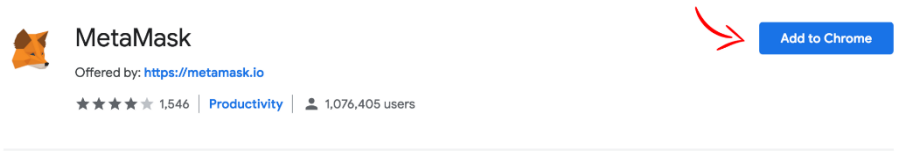
MetaMask Wallet

Το MataMask είναι ένα διαδικτυακό πορτοφόλι κρυπτονομισμάτων που λειτουργεί ως επέκταση σε προγράμματα περιήγησης Firefox, Chrome και Brave. Το πορτοφόλι επιτρέπει επίσης στους χρήστες να αλληλεπιδρούν με έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές (DApps). Τα κλειδιά του MetaMask αποθηκεύονται στο πρόγραμμα περιήγησης του χρήστη και όχι σε απομακρυσμένους διακομιστές. Ορισμένοι πάροχοι πορτοφολιών αποθηκεύουν τα κλειδιά των χρηστών σε δικούς τους διακομιστές. Αυτό είναι κοινό σε ανταλλακτήρια που παρέχουν πορτοφόλια, όπως το Coinbase.. Αυτό δίνει στον χρήστη μεγαλύτερο έλεγχο στα δημόσια και ιδιωτικά του κλειδιά.

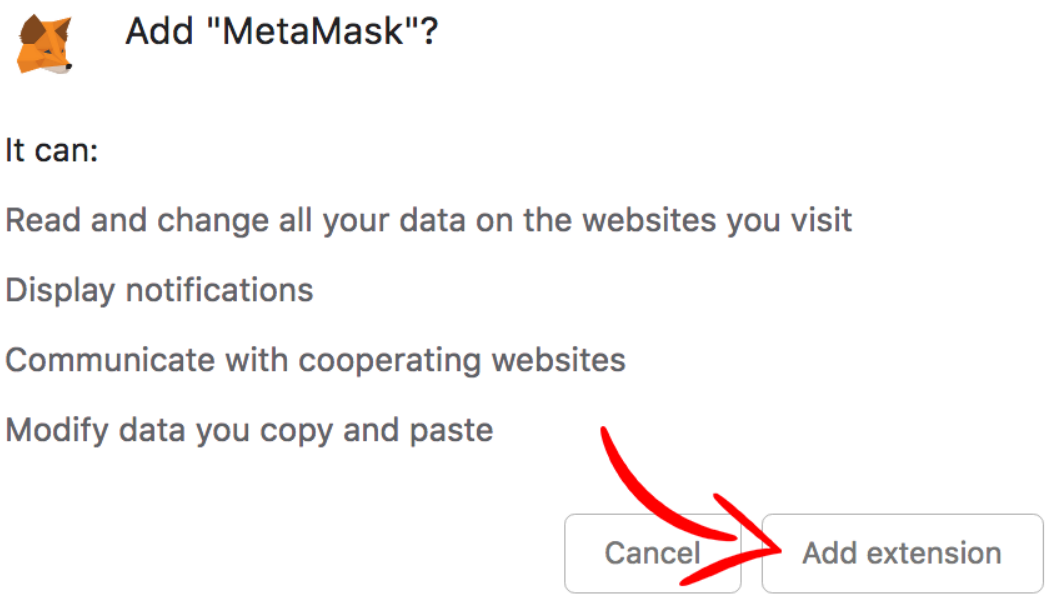
Βήμα 1: Επισκεφθείτε τη διεύθυνση https://metamask.io/. Επιλέξτε το πρόγραμμα περιήγησής σας. Θα προχωρήσουμε με το Chrome. Κάντε κλικ στην επιλογή "Λήψη επέκτασης Chrome".



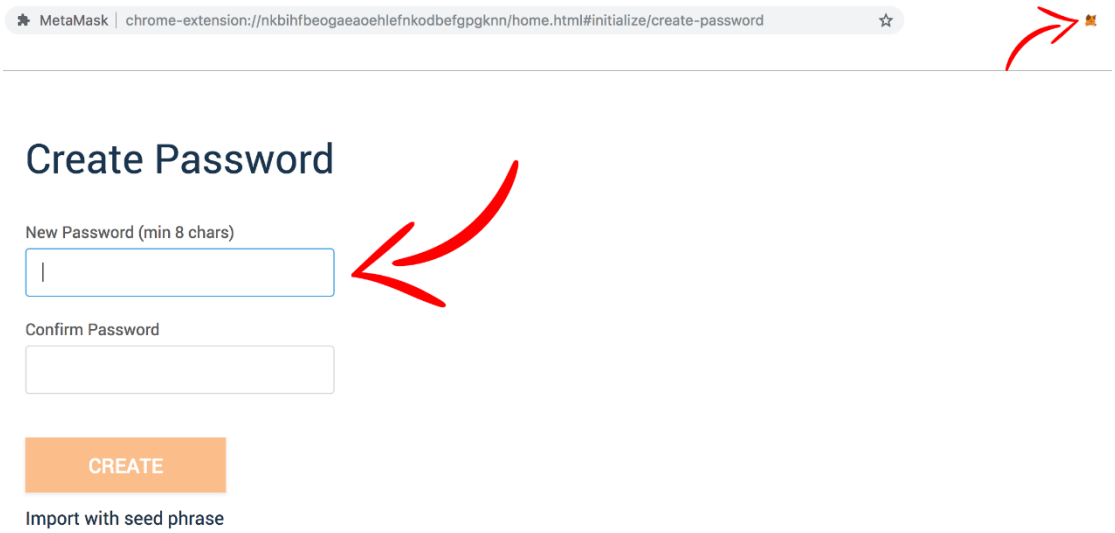
Βήμα 2: Θα κατευθυνθείτε στο Chrome web store. Κάντε κλικ στην επιλογή "Προσθήκη στο Chrome".



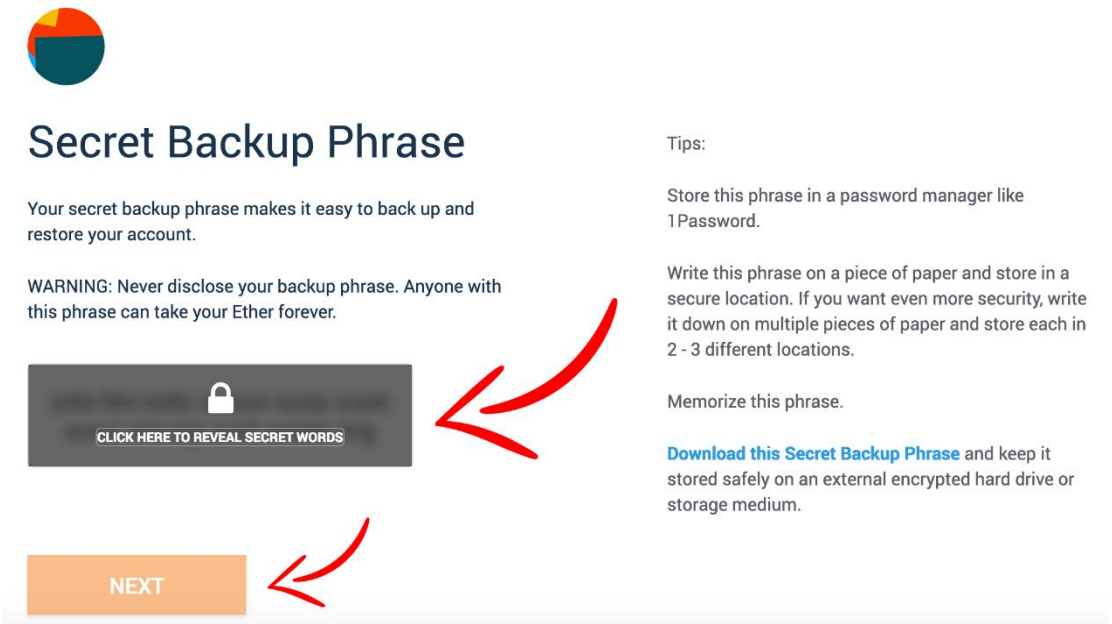
Βήμα 3: Κάντε κλικ στην επιλογή "Προσθήκη επέκτασης". Το εικονίδιο MetaMask θα εμφανιστεί στην επάνω δεξιά γωνία του προγράμματος περιήγησης Chrome.



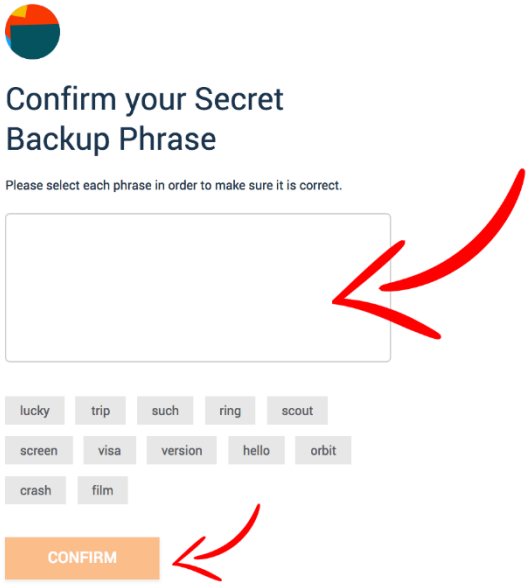
Βήμα 4: Κάντε κλικ στην επέκταση Metamask στην επάνω δεξιά γωνία του προγράμματος περιήγησης Chrome. Θα σας ζητηθεί να δημιουργήσετε έναν νέο κωδικό πρόσβασης. Δημιουργήστε έναν κωδικό πρόσβασης, επιβεβαιώστε τον και κάντε κλικ στη «Δημιουργία».



Βήμα 5: Το MetaMask θα δημιουργήσει μια μυστική εφεδρική φράση. Πρέπει να την αποθηκεύστε σε ασφαλές μέρος. Στη συνέχεια κάντε κλικ στο επόμενο.



Βήμα 6: Επιβεβαιώστε τη μυστική εφεδρική φράση. Μετά από αυτό το βήμα το πορτοφόλι είναι πλέον έτοιμο για χρήση.



Βήμα 7: Αν θέλετε να προσθέσετε token στο πορτοφόλι, κάντε κλικ στο "Προσθήκη token" από τον κύριο πίνακα ελέγχου.