ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΤΜΗΜΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΠΜΣ ΟΙΚΟΝΟΜΙΚΗΣ ΕΠΙΣΤΗΜΗΣ

Αποκεντρωμένη Χρηματοοικονομική: Βασικές αρχές λειτουργίας και μελέτες περίπτωσης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χαράλαμπος-Παναγιώτης Γαλαθρής

Αθήνα, 2023

Τριμελής Επιτροπή

Νικόλαος Δασκαλάκης, Επίκουρος Καθηγητής Παντείου Πανεπιστημίου (Επιβλέπων)

Ιωάννης Φίλος, Καθηγητής Παντείου Πανεπιστημίου

Γρηγόριος Κόρδας, Επίκουρος Καθηγητής Παντείου Πανεπιστημίου

Αφιέρωση « Στην μητέρα μου και στην μνήμη του πατέρα μου, τους οποίους αγαπώ πολύ »

Περιεχόμενα

Περιεχόμενα

Πίνακες

Διαγράμματα

Σχήματα

Περίληψη

Η εργασία που ακολουθεί έχει ως σκοπό να ενημερώσει τον αναγνώστη σχετικά με τις ραγδαίες εξελίξεις που λαμβάνουν χώρα την τελευταία περίπου 15ετία στον χώρο της χρηματοοικονομικής επιστήμης. Αρχικά γίνεται λόγος για το παραδοσιακό χρηματοοικονομικό σύστημα αλλά και για τα μειονεκτήματα του, και στη συνέχεια παρατίθενται λύσεις στα προβλήματα αυτά μέσω της καινοτομίας του blockchain. Αφού αναλυθούν τα χαρακτηριστικά και ο τρόπος λειτουργίας του, γίνεται λόγος για έναν νέο τρόπο που φέρνει επανάσταση στον χώρο της χρηματοοικονομικής η οποία έχει ως βάση του την συνεχώς εξελισσόμενη πλατφόρμα του blockchain και η οποία ονομάζεται Αποκεντρωμένη Χρηματοοικονομική. Τέλος, παρουσιάζεται και αναλύεται μία από τις πλέον σημαντικές εφαρμογές της Αποκεντρωμένης Χρηματοοικονομικής.

Λέξεις-κλειδιά:Blockchain, Αποκεντρωμένη Χρηματοοικονομική, Μελέτη περίπτωσης, Uniswap

Abstract

The following thesis intends to inform the reader about the rapid developments that have taken place in the last 15 years in the field of Finance. Firstly, we talk about the traditional financial system as well as its disadvantages and then we propose solutions according to the innovation of blockchain technology. After analyzing its features and mode of operation, we talk about a new way that revolutionizes the field of finance which is based on the constantly evolving blockchain platform and which is called Decentralized Finance. Finally, the case of one of the most important applications of Decentralized Finance is presented and analyzed.

Keywords: Blockchain, Decentralized Finance, Case study, Uniswap

Εισαγωγή

Στο πρώτο κεφάλαιο της εργασίας παρουσιάζεται το κλασσικό χρηματοοικονομικό σύστημα μαζί με την δομή και τα χαρακτηριστικά του. Επίσης παρατίθενται τα μια σειρά από μειονεκτήματα-περιορισμούς του παραδοσιακού συστήματος.

Στο δεύτερο κεφάλαιο γίνεται εισαγωγή στην έννοια της τεχνολογίας του Blockchain. Δίνεται ο ορισμός και τα βασικά χαρακτηριστικά του καθώς και ο τρόπος λειτουργίας του. Τέλος αναφερόμαστε στην αναβάθμιση του δικτύου , δηλαδή στο Blockchain 2.0 καθώς και στο πολύ σημαντικό εργαλείο δηλαδή στα smart contracts.

Στο τρίτο κεφάλαιο παρατίθενται και αναλύονται τα ψηφιακά νομίσματα και πιο συγκεκριμένα τα κρυπτονομίσματα και τα tokens. Παρουσιάζονται τα βασικά χαρακτηριστικά τους, ο τρόπος λειτουργίας τους καθώς και διαδικασία των συναλλαγών τους. Τέλος, παρουσιάζεται και αναλύεται ο πιο διαδεδομένος τρόπος άντλησης κεφαλαίων στην κρυπτοοικονομία, ο οποίος πρόκειται για τις Αρχικές Προσφορές νομισμάτων (ICOs).

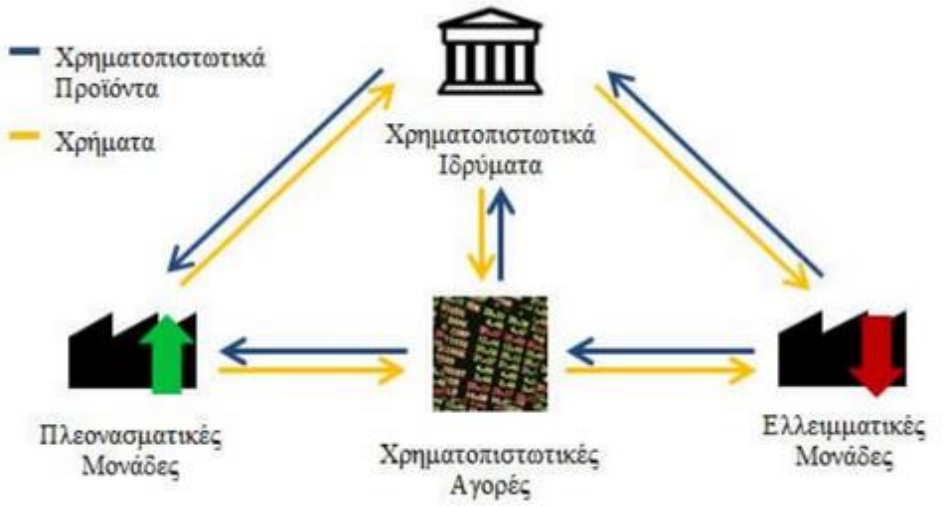
Στο τέταρτο κεφάλαιο δίνεται ο ορισμός της έννοιας και παρουσιάζονται τα χαρακτηριστικά της Αποκεντρωμένης Χρηματοοικονομικής, οι διαφορές της με την παραδοσιακή χρηματοοικονομική καθώς και η αρχιτεκτονική της. Τέλος, γίνεται μελέτη περίπτωσης για δύο εφαρμογές της Αποκεντρωμένης Χρηματοοικονομικής, το Uniswap και το Compound.

Κεφάλαιο 1: Το κλασσικό χρηματοοικονομικό σύστημα

1.1: Οι χρηματοοικονομικοί διαμεσολαβητές (Χρηματοπιστωτικά Ιδρύματα και αγορές) και οι βασικές τους λειτουργίες

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορούμε να ορίσουμε την έννοια του χρηματοοικονομικού (ή χρηματοπιστωτικού) συστήματος. Ένας αρκετά γενικός ορισμός είναι πως πρόκειται για ένα σύνολο δραστηριοτήτων και υπηρεσιών, οι οποίες συνδέονται μεταξύ τους αμφίδρομα, με σκοπό την διευκόλυνση της μεταφοράς κεφαλαίων από το σημείο στο οποίο βρίσκονται, στο σημείο όπου υπάρχει ανάγκη για αυτές. Ειδικότερα, για κάθε στιγμή μίας συγκεκριμένης χρονικής περιόδου, κάποιες οικονομικές μονάδες (νοικοκυριά, επιχειρήσεις, δημόσιο) εμφανίζουν έσοδα περισσότερα από τα έξοδα τους. Αντιθέτως, κάποιες άλλες οικονομικές μονάδες, έχουν μεγαλύτερα έξοδα από ότι έσοδα. Άρα, όπως φαίνεται και στο παρακάτω σχήμα (Σχήμα 1.1), το χρηματοοικονομικό σύστημα παρέχει τον τρόπο με τον οποίο, κεφάλαια από τις αρχικές πλεονασματικές οικονομικές μονάδες μπορούν να μεταφερθούν στις επόμενες ελλειμματικές οικονομικές μονάδες.

Σχήμα 1: Το παραδοσιακό χρηματοοικονομικό σύστημα



Σημείωση: Πηγή: https://www.dailyeconomics.gr/oikonomikoi-oroi/xrimatopistwtiko-sustima

Η δομή αυτού του χρηματοοικονομικού συστήματος περιέχει δύο βασικά μέρη: τις χρηματοπιστωτικές αγορές, οι οποίες αποτελούν την άμεση χρηματοδότηση, καθώς και τα χρηματοπιστωτικά ιδρύματα τα οποία δρουν ως διαμεσολαβητές, και απαρτίζουν την έμμεση χρηματοδότηση. Στην περίπτωση της άμεσης χρηματοδότησης, οι δανειστές διοχετεύουν τα κεφάλαια τους απευθείας σε δανειολήπτες, ενώ στην έμμεση χρηματοδότηση, οι δανειστές διοχετεύουν τα

κεφάλαια τους σε ένα ενδιάμεσο, ο οποίος με τη σειρά του αποφασίζει πώς θα παρέχει το σύνολο των χρημάτων που έχουν συγκεντρωθεί σε δανειολήπτες. Παράδειγμα άμεσης χρηματοδότησης, αποτελεί το Χρηματιστήριο Αθηνών, μέσω του οποίου, σε περίπτωση όπου ένας δανειστής αγοράσει μετοχές μίας εισηγημένης εταιρίας, γνωρίζει πως τα χρήματα του διοχετεύονται απευθείας σε αυτήν την εταιρία. Αντιθέτως, σύμφωνα με την έμμεση χρηματοδότηση, ένα χρηματοπιστωτικό ίδρυμα, όπως μια τράπεζα, θα χρησιμοποιήσει ένα σύνολο από τις καταθέσεις των πελατών της και με βάση αυτά τα χρήματα θα αποφασίσει στην συνέχεια το πώς ακριβώς θα δανείσει μία αντίστοιχη εταιρία.

Ζωτικής σημασίας προϋπόθεση για την εύρυθμη λειτουργία του χρηματοοικονομικού συστήματος είναι η ύπαρξη εμπιστοσύνης σε αυτό. Μέσω αυτής διασφαλίζεται η σταθερότητα και η αξιοπιστία του συστήματος. Σε περίπτωση όπου η εμπιστοσύνη χαθεί υπάρχει μεγάλος κίνδυνος να εμφανιστούν εντάσεις μέσα στο σύστημα οι οποίες μπορεί να έχουν καταστροφικές συνέπειες, όπως για παράδειγμα η Παγκόσμια Χρηματοπιστωτική Κρίση του 2008.

Καθοριστικό ρόλο επίσης σε ένα χρηματοοικονομικό σύστημα αποτελεί και η ύπαρξη ενός αποτελεσματικού συστήματος πληρωμών. Ως σύστημα πληρωμών ορίζεται ο μηχανισμός μεταφοράς και καταγραφής των χρηματικών ποσών. Έτσι, το σύστημα των πληρωμών αποτελεί το «κυκλοφορικό σύστημα» του χρηματοοικονομικού συστήματος. Η έννοια της πίστης που αναφέραμε νωρίτερα, αποτελεί προϋπόθεση για την λειτουργία του συστήματος πληρωμών και κατ' επέκταση όλου του χρηματοοικονομικού συστήματος. Τα συστήματα πληρωμών ανήκουν σε οργανισμούς τους οποίους συνήθως εποπτεύουν τράπεζες.

Στο παραδοσιακό χρηματοοικονομικό σύστημα υπάρχουν δύο κύριοι τρόποι χρηματοδότησης. Ο πρώτος έχει να κάνει με τα Ίδια Κεφάλαια, και γίνεται συνήθως μέσω αρχικών δημόσιων προσφορών ή με άλλα λόγια με την έκδοση νέων μετοχών με σκοπό την αύξηση του μετοχικού κεφαλαίου. Ο δεύτερος αναφέρεται στα Ξένα Κεφάλαια, με κύρια μέθοδο τον τραπεζικό δανεισμό.

1.2 Αδυναμίες και ευπάθειες του Κλασικού Χρηματοοικονομικού Συστήματος (περιορισμοί των κεντροποιημένων χρηματοπιστωτικών ιδρυμάτων)

Αφού αναλύσαμε την δομή και τον τρόπο λειτουργίας του παραδοσιακού χρηματοοικονομικού συστήματος, μπορούμε να διακρίνουμε μια σειρά από περιορισμούς τους οποίους αντιμετωπίζει το σύστημα λόγω της αρχιτεκτονικής στην οποία βασίζεται. Συγκεκριμένα θα αναφερθούμε στα μειονεκτήματα των χρηματοπιστωτικών ιδρυμάτων, τα οποία όπως αναφέραμε ήδη έχουν διαμεσολαβητικό ρόλο και υπόκεινται στον έλεγχο και την εποπτεία κεντρικών αρχών. Παρακάτω ακολουθεί μια σειρά από τους βασικούς περιορισμούς του κλασικού χρηματοοικονομικού συστήματος.

Ι) Κόστος συναλλαγής και προμήθεια. Ένα από τα κυριότερα μειονεκτήματα χρήσης του συμβατικού χρηματοοικονομικού συστήματος είναι η ύπαρξη κόστους ή

προμήθειας το οποίο πρέπει να καταβληθεί ώστε η οικονομική συναλλαγή να εκτελεσθεί. Για παράδειγμα στην περίπτωση της τράπεζας Alpha Bank[1], η προμήθεια για μια συναλλαγή από ΑΤΜ άλλης τράπεζας εκτός Ευρωπαϊκής Ένωσης, ανέρχεται στο 1% του συνολικού ποσού της συναλλαγής αυτής.

ΙΙ) Γεωγραφικοί περιορισμοί. Πολλές υπηρεσίες του παραδοσιακού συστήματος όπως οι τραπεζικές συναλλαγές υπόκεινται σε γεωγραφικούς περιορισμούς. Οι τράπεζες και αντίστοιχα ιδρύματα, δεν έχουν απεριόριστη εμβέλεια, δηλαδή δεν καλύπτουν όλες τις περιοχές σε παγκόσμιο επίπεδο. Αυτό οδηγεί τον εκάστοτε ενδιαφερόμενο ο οποίος θέλει να εκτελέσει μια συναλλαγή στο να χρησιμοποιήσει την αντίστοιχη υπηρεσία η οποία είναι διαθέσιμη στην περιοχή όπου εκείνος βρίσκεται. Αυτή η διαδικασία, πέρα από την δυσκολία που μπορεί να προκαλέσει, πιθανόν να έχει και ως αποτέλεσμα μεγαλύτερη χρονική διάρκεια για την εκτέλεση ή και την ολοκλήρωση της συναλλαγής. Υπάρχουν επίσης και περιοχές, όπως πολλές αφρικανικές και άλλες αναπτυσσόμενες χώρες[2] υπάρχει ακόμα και πλήρης έλλειψη ενός τραπεζικού συστήματος καθιστώντας έτσι συναλλαγές από και προς αυτές πρακτικά αδύνατες.

ΙΙΙ) Ταχύτητα εξυπηρέτησης και συναλλαγών. Οι τράπεζες παρέχουν μια σειρά από υπηρεσίες οι οποίες απαιτούν την φυσική αλληλεπίδραση μεταξύ ατόμων. Για παράδειγμα η μεταφορά μεγάλων κεφαλαίων απαιτεί μια πιο εξονυχιστική και λεπτομερείς διαδικασία, η οποία συνήθως προϋποθέτει την φυσική παρουσία του ενδιαφερομένου σε ένα κατάστημα της εκάστοτε τράπεζας.

ΙV) Έλλειψη διαφάνειας και διαλειτουργικότητας. Το τρέχων παραδοσιακό σύστημα δεν χαρακτηρίζεται από πλήρη διαφάνεια. Ο μέσος υποψήφιος πελάτης δεν γνωρίζει την πλήρη εικόνα της οικονομικής κατάστασης της τράπεζας αλλά ούτε και του εύρους της κρατικής προστασίας η οποία εκείνη δέχεται. Καλείται έτσι, να την εμπιστευτεί με αρκετούς ενδοιασμούς. Αυτή η αβεβαιότητα υπάρχει και στην περίπτωση διαδικασία αναζήτησης και λήψης κάποιου δανείου, όπου η εκάστοτε τράπεζα παρέχει τα δικά της σχέδια πληρωμών και επιτοκίων, περιορίζοντας έτσι την ικανότητα του πελάτη να επιλέξει το καλύτερο σχέδιο με βάση τα δικά τις δικές του ιδιαιτερότητες και δυνατότητες. Τέλος, λόγω της ύπαρξης αγορών και ιδρυμάτων διαφορετικού χαρακτήρα, όπως για παράδειγμα αγορές μετοχών, τράπεζες, ασφαλιστικές και συνταξιοδοτικών ταμείων, έγκειται η θέσπιση ενός κεντρικού συστήματος το οποίο θα ενώνει όλα αυτά τα ιδρύματα μεταξύ τους ικανοποιώντας έτσι και την ανάγκη για ένα σύστημα μεγαλύτερης διαλειτουργικότητας.

[1] https://www.alpha.gr/el/idiotes/support-center/atm-kas/kostos

[2] https://www.statista.com/chart/18497/countries-with-the-highest-share-of-adults-without-a-bank-account-in-2017/

Κεφάλαιο 2: Η τεχνολογία του Blockchain

2.1 Εισαγωγή στην έννοια της τεχνολογίας του Blockchain

Στο προηγούμενο κεφάλαιο έγινε μία σύντομη παρουσίαση του κλασσικού χρηματοοικονομικού συστήματος στα πλαίσια της οποίας αναπτύχθηκαν περιεκτικά τα βασικά του μέλη, χαρακτηριστικά καθώς και οι λειτουργίες. Στα επόμενα κεφάλαια θα αναφερθούμε την πρωτοποριακή τεχνολογία του Blockchain, η οποία μέσα στα λίγα χρόνια ύπαρξης της έχει καταφέρει να δημιουργήσει και να υποστηρίξει νέες και πιο αποτελεσματικές τεχνολογίες σε σχέση με το ήδη υπάρχων σύστημα εξαλείφοντας ταυτόχρονα και αδυναμίες του, όπως αυτές που αναφέρθηκαν στο Κεφάλαιο 1.

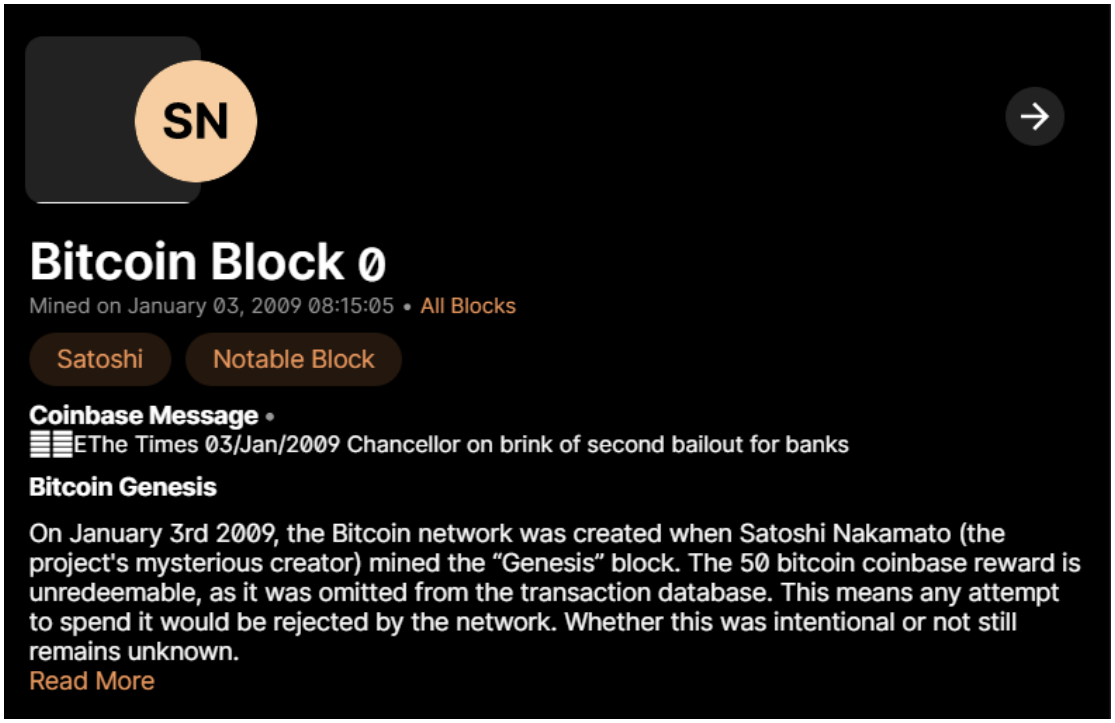
Η αρχή έγινε τον Οκτώβρη του 2008 όταν ένα άτομο ή μια ομάδα ατόμων χρησιμοποιώντας το ψευδώνυμο Satoshi Nakamoto, δημοσίευσε ένα επιστημονικό άρθρο (paper), με τον τίτλο ‘‘Bitcoin: A Peer-to-Peer Electronic Cash System’’[3], σύμφωνα με το οποίο το bitcoin ορίζεται ως: ‘‘A purely peer-to-peer version of electronic cash, that would allow online payments to be sent directly from one party to another without going through a financial institution.’’ Πρόκειται δηλαδή για μία νέα εκδοχή ηλεκτρονικού χρήματος το οποίο επιτρέπει την άμεση αποστολή διαδικτυακών πληρωμών μεταξύ δύο οντοτήτων χωρίς την χρήση ενός χρηματοπιστωτικού ιδρύματος ως μεσάζοντα. Η ιδέα ενός συστήματος πληρωμών χωρίς την ανάγκη ύπαρξης ενός χρηματοπιστωτικού οργανισμού που δρα ως διαμεσολαβητής σε αυτήν, είναι μια πραγματικά επαναστατική ιδέα στον κόσμο των χρηματοοικονομικών. Βέβαια, προσπάθειες για την υλοποίηση ενός τέτοιου ψηφιακού νομίσματος είχαν γίνει αρκετές δεκαετίες νωρίτερα. Πιο συγκεκριμένα ο David Chaum στις αρχές της δεκαετίας του 1980 δημιούργησε το ‘’e-cash’’, ενώ μετέπειτα το 1998, οι Nick Szabo και Wei Dai εισήγαγαν τα ‘‘Bit Gold’’ και ‘‘B-Money’’[4] αντίστοιχα. Βασικό πρόβλημα όλων αυτών των προσπαθειών αποτελούσε το πρόβλημα της διπλής δαπάνης, δηλαδή η δυσκολία της αποτροπής ένα νόμισμα να ξοδευτεί δύο φορές και κατ’ επέκταση πώς μπορούσε το σύστημα να σχεδιαστεί με τέτοιο τρόπο ώστε να μην καθίσταται δυνατή η αντιγραφή και η πλαστογράφηση του εκάστοτε νομίσματος. Παρόλα αυτά, η ιδέα που εξέφρασε ο Satoshi Nakamoto σχετικά με το σύστημα πληρωμών βασισμένο επάνω στην τεχνολογία του Blockchain, αποτέλεσε την λύση των προβλημάτων που αναφέρθηκαν παραπάνω. Η αρχή έγινε στις 3 Ιανουαρίου του 2009, όταν ο Satoshi Nakamoto ***εξόρυξε*** το πρώτο block, δημιουργώντας έτσι το δίκτυο του Bitcoin.[5] Όπως ειπώθηκε και στο πρώτο κεφάλαιο η έννοια της εμπιστοσύνης προς το σύστημα αποτελεί βασική προϋπόθεση για την ομαλή λειτουργία του. Επίσης, τα χρηματοπιστωτικά ιδρύματα φροντίζουν να καταγράφουν τις συναλλαγές με τέτοιο τρόπο ώστε το πρόβλημα της διπλής δαπάνης να εξαλείφεται. Διακρίνεται πως τεχνολογία του Blockchain, δημιουργήθηκε λαμβάνοντας υπόψιν αυτές τις δύο προϋποθέσεις.

Σχήμα 2: Η πρώτη συναλλαγή bitcoin

[3] https://bitcoin.org/bitcoin.pdf

[4] http://www.weidai.com/bmoney.txt

[5] https://www.blockchain.com/explorer/blocks/btc/0



Σημείωση: Πηγή: https://www.blockchain.com/explorer/blocks/btc/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

2.2 Ορισμός και βασικά χαρακτηριστικά

Σε κάθε παραδοσιακό δίκτυο ηλεκτρονικών πληρωμών υπάρχει ως απαραίτητη προϋπόθεση, η ύπαρξη ενός διαμεσολαβητή, όπως για παράδειγμα κάποιας τράπεζας, η οποία είναι υπεύθυνη για την καταγραφή όλων των συναλλαγών που εκτελούνται

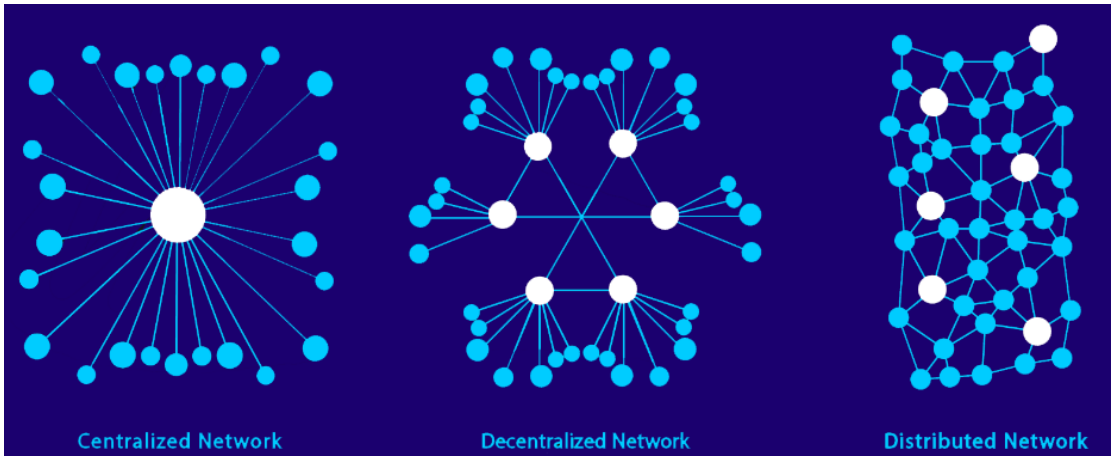
μέσω αυτής με σκοπό την αποφυγή της διπλής δαπάνης. Έτσι, σε αυτά τα συστήματα, η ύπαρξη ενός τρίτου (συνήθως μίας τράπεζας), καθώς και το αίσθημα της εμπιστοσύνης από όλους όσους συμμετέχουν, αποτελούν προϋπόθεση για την ορθή λειτουργία αυτού του είδους συστήματος. Όπως αναφέρθηκε και παραπάνω, το 2009, Ο Satoshi Nakamoto, παρουσίασε ένα καινοτόμο, αποκεντρωμένο σύστημα ηλεκτρονικών πληρωμών μέσω του οποίου οι χρήστες θα μπορούν να πραγματοποιούν ελεύθερα συναλλαγές μεταξύ τους χωρίς την ανάγκη κάποιου μεσάζοντα. Βάση αυτού του συστήματος αποτελεί η πλατφόρμα του Blockchain η οποία χρησιμοποιείται για την καταγραφή του κρυπτονομίσματος bitcoin. Γενικά, κρυπτονομίσματα ονομάζονται τα ψηφιακά νομίσματα τα οποία αντιμετωπίζονται ως ψηφιακή πληροφορία και δεν έχουν φυσική υπόσταση.

Άρα με βάση τα παραπάνω, το Blockchain αποτελεί μια ψηφιακή διανεμημένη βάση δεδομένων/ένα λογιστικό βιβλίο μέσα στο οποίο καταγράφονται όλες οι πληροφορίες, ενώ όλοι έχουν πρόσβαση σε αυτό. Μπορούμε να το παρομοιάσουμε με αντίστοιχο βιβλίο που διατηρούν οι τράπεζες το οποίο περιέχει το πλήρες ιστορικό των συναλλαγών τους, αλλά αντί να ανήκει σε μόνο σε μία τράπεζα, το δίκτυο του Blockchain είναι δημόσιο και προσβάσιμο σε όλους. Έτσι, οποιαδήποτε αλλαγή στην βάση δεδομένων/λογιστικό βιβλίο είναι άμεσα ορατή σε όλους ταυτόχρονα ενώ όλοι μπορούν να έχουν ένα αντίγραφο του βιβλίου. Ταυτόχρονα, τα προσωπικά δεδομένα των χρηστών είναι κρυπτογραφημένα. Οποιαδήποτε αλλαγή στη βάση δεδομένων, για να καταγραφεί πρέπει πρώτα να επικυρωθεί από το 51% των υπολογιστών του δικτύου. Έτσι, το Blockchain αποτελεί μια τεχνολογία καταγραφής και αποθήκευσης της πληροφορίας η οποία χρησιμοποιεί κρυπτογραφικές μεθόδους, επιτρέπει την μεταφορά πληροφοριών (και αξιών) χωρίς την παρουσία ενδιάμεσων, δεν μπορεί να πλαστογραφηθεί ή να αντιστραφεί και όπου όλο το ιστορικό των συναλλαγών μεταξύ των χρηστών του καταγράφεται, επαληθεύεται, αποθηκεύεται και είναι δημόσιο.

2.3 Πως λειτουργεί ένα δίκτυο Blockchain

Αρχικά πρέπει να αναφερθούμε στην φύση του δικτύου. Γενικά, τα δίκτυα μπορούν να διακριθούν σε συγκεντρωτικά (centralized), αποκεντρωμένα (decentralized) και σε διαμοιρασμένα (distributed), όπως αυτά παρουσιάζονται και στο παρακάτω σχήμα

Σχήμα 3: Τα είδη Δικτύων Blockchain

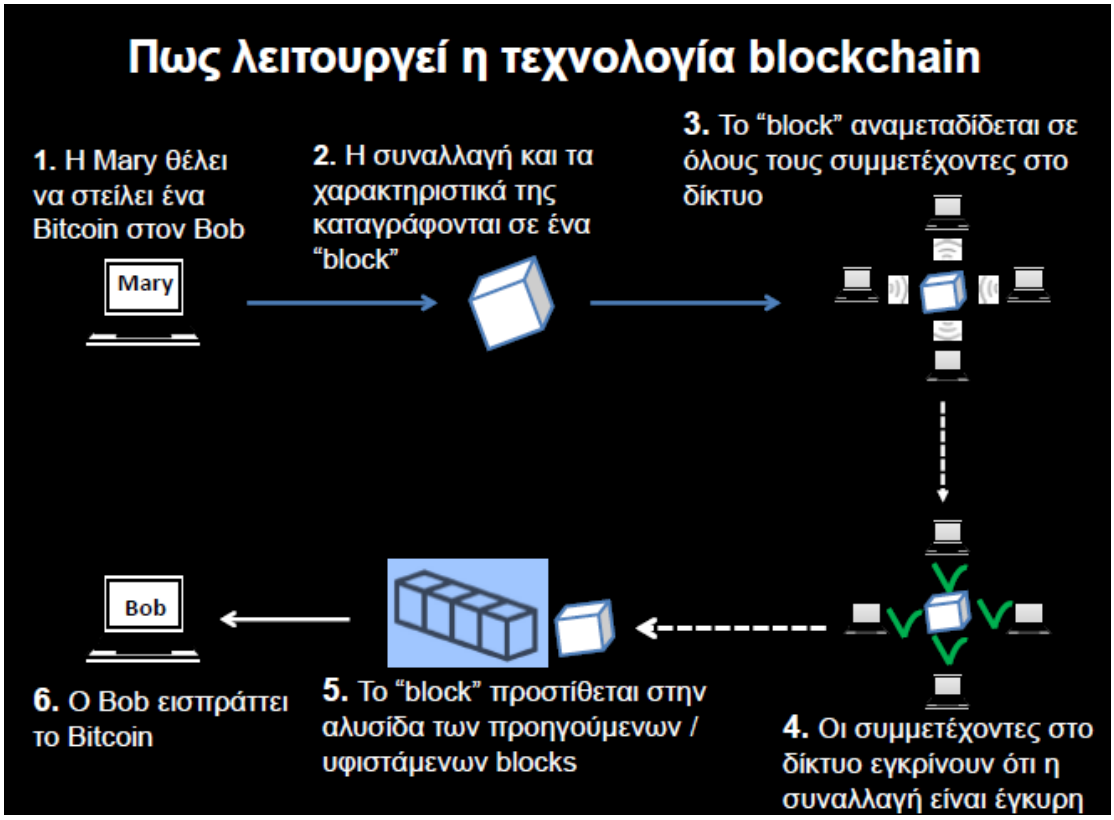


Σημείωση: Πηγή: https://blockchainengineer.com/centralized-vs-decentralized-vs-distributed-network/

Στα συγκεντρωτικά δίκτυα, έχουμε την ύπαρξη μίας Κεντρικής Οντότητας Ελέγχου (Central Control Entity), η οποία είναι υπεύθυνη για την πιστοποίηση των χρηστών (nodes) του δικτύου και για την διαχείριση της βάσης δεδομένων όπου τα δεδομένα/συναλλαγές αποθηκεύονται. Για την διασφάλιση των δεδομένων απαιτείται η χρήση ειδικού εξοπλισμού ασφαλείας. Στα αποκεντρωμένα δίκτυα δεν υπάρχει κεντρική οντότητα ελέγχου. Τα διαχειριστικά δικαιώματα είναι ισάξια διαμοιρασμένα σε αρκετές οντότητες/χρήστες του δικτύου. Αντίγραφα της βάσης δεδομένων διατηρούνται αυτούσια σε αρκετούς κόμβους του δικτύου με δικαίωμα πρόσβασης σε αυτά τα δεδομένα ανά πάσα στιγμή σε όποιον το θελήσει. Τα δίκτυα αυτά διαθέτουν υψηλού επιπέδου ασφάλεια έναντι κακόβουλων ενεργειών. Τέλος, στα διαμοιρασμένα δίκτυα δεν υπάρχει ούτε κεντρική οντότητα ελέγχου ούτε διαμοιρασμός διαχειριστικών δικαιωμάτων. Οι κόμβοι του δικτύου μπορούν ταυτόχρονα να είναι και μέλη άλλων δικτύων. Σκοπός κάθε κόμβου είναι η διασφάλιση των εγγράφων της Βάσης Δεδομένων και ακολουθείται ένα σύνολο κοινά αποδεκτών κανόνων για την επικύρωση των δεδομένων/συναλλαγών. Το Blockchain πρόκειται για ένα διαμοιρασμένο δίκτυο. Όλοι οι κόμβοι του δικτύου αυτού έχουν τα ίδια δικαιώματα και υποχρεώσεις, αποθηκεύουν την ίδια ποσότητα πληροφορίας και είναι συνδεδεμένα μεταξύ τους. Στο δίκτυο του Blockchain οποιοσδήποτε μπορεί να κάνει εγγραφές, αυτές όμως πρέπει να επικυρωθούν από άλλα μέλη για να προστεθούν στην αλυσίδα δεδομένων.

Αφού αναλύσαμε τα είδη των δικτύων και κατατάξαμε το δίκτυο του Blockchain ως διαμοιρασμένο, μπορούμε να προχωρήσουμε στο πώς το δίκτυο αυτό λειτουργεί. Συγκεκριμένα αυτό μπορεί να εύκολα να επιτευχθεί μέσω ενός απλού παραδείγματος μιας συναλλαγής στο Blockchain. Ας υποθέσουμε λοιπόν πως η Mary θέλει να στείλει ένα bitcoin στον Bob. Για να το κάνει αυτό, συνδέεται στο ηλεκτρονικό της πορτοφόλι όπου και φυλάσσει τα bitcoin της. Αφού διαλέξει την ποσότητα που επιθυμεί, στη συνέχεια πληκτρολογεί την διεύθυνση bitcoin του Bob, (η οποία αποτελείται από αριθμούς και γράμματα). Στην συνέχεια πατά αποστολή και η συναλλαγή εκτελείται.

Σχήμα 4: Παράδειγμα λειτουργίας blockchain



Σημείωση: Πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

Αυτή η συναλλαγή αναπαρίσταται ηλεκτρονικά ως ένα block το οποίο περιέχει κρυπτογραφημένες ψηφιακές πληροφορίες όπως για παράδειγμα τις διευθύνσεις του αποστολέα και του παραλήπτη καθώς και την ποσότητα που μεταφέρεται. Το block αυτό στη συνέχεια αναμεταδίδεται σε όλους τους συμμετέχοντες του δικτύου, οι οποίοι στη συνέχεια εγκρίνουν την συναλλαγή ως έγκυρη. Αφού συμβεί αυτό, το block προστίθεται στην αλυσίδα των προηγούμενων/υφιστάμενων blocks και τελικά ο Bob εισπράττει το bitcoin του. Αξίζει να σημειωθεί πως κάθε συμμετέχων στο δίκτυο διαθέτει προσωπικό αντίγραφο του λογιστικού βιβλίου, πλήρως ενημερωμένο με τις τελευταίες χρονικά συναλλαγές που συνέβησαν, αλλά κανείς δεν μπορεί να το αλλάξει.

Ο τρόπος με τον οποίο λειτουργεί το blockchain υποδεικνύει πως υπάρχουν 3 βασικά χαρακτηριστικά που διέπουν την τεχνολογία αυτή: η ασφάλεια, η διαφάνεια και η μη αναστρεψιμότητα των πράξεων.

Η ασφάλεια οφείλεται στο γεγονός πως από την στιγμή που κάθε κομμάτι πληροφορίας αποθηκεύεται ταυτόχρονα σε όλους τους υπολογιστές που συμμετέχουν στο δίκτυο, είναι τεχνικά αδύνατον για κακόβουλα στοιχεία να αλλάξουν οποιαδήποτε αποθηκευμένη πληροφορία μιας και για να το καταφέρουν αυτό θα πρέπει να αλλάξουν όλους τους υπολογιστές και μάλιστα ταυτόχρονα.

Η διαφάνεια πηγάζει από το γεγονός πως από την στιγμή όπου όλοι οι κόμβοι που συμμετέχουν στο δίκτυο έχουν ίδια δικαιώματα και υποχρεώσεις, όλη η πληροφορία αποθηκεύεται δημόσια, αναρτάται και επικυρώνεται από το σύνολο του

δικτύου, τότε δεν χρειάζεται και η συνδρομή κάποιου εγγυητή. Η διαφάνεια αποτελεί το κλειδί της δημιουργίας εμπιστοσύνης στο δίκτυο.

Τέλος, όταν μια συναλλαγή προστίθεται στο block, δεν μπορεί να τροποποιηθεί ούτε να διαγραφεί. Ο μόνος τρόπος διόρθωσης μίας λανθασμένης συναλλαγής είναι για τον παραλήπτη να πληρώσει πίσω την ποσότητα στον αρχικό αποστολέα, ώστε μια νέα συναλλαγή να εκτελεστεί ξανά. Έτσι η μη αναστρεψιμότητα των συναλλαγών αποτελεί σημαντικό στοιχείο της τεχνολογίας του Blockchain.

2.4 Blockchain 2.0: Το δίκτυο του Ethereum

2.4.1 Ορισμός και βασικά χαρακτηριστικ**ά.**

Η πρωτοποριακή ιδέα του Blockchain δοκιμάστηκε για πρώτη φορά με την κυκλοφορία του bitcoin. Τα αποτελέσματα της δοκιμασίας αυτής ήταν ενθαρρυντικά υπό την άποψη ότι κατάφερε να πραγματοποιήσει τους στόχους τους ήθελε, καταφέρνοντας έτσι να παρακινήσει πολλούς ανθρώπους όχι μόνο να ασχοληθούν αλλά και να εξελίξουν περαιτέρω την τεχνολογία αυτή. Το επόμενο μεγάλο βήμα έγινε το 2014, όταν ο Βιτάλικ Μπούτεριν (Vitalik Buterin), ένας νεαρός προγραμματιστής δημιούργησε την πλατφόρμα του Etherium. Ένα χρόνο νωρίτερα, το 2013, ο Μπούτεριν είχε δημοσιεύσει ένα άρθρο[6] στο οποίο περιέγραφε μια εναλλακτική πλατφόρμα η οποία θα αποτελούσε την βάση για οποιαδήποτε τύπο αποκεντρωμένης εφαρμογής την οποία θα ήθελαν να δημιουργήσουν προγραμματιστές.

Αυτή η νέα πλατφόρμα έδινε την δυνατότητα τροποποίησης του κώδικα, πράγμα το οποίο άλλαζε την φύση των blocks στην αλυσίδα, δίνοντας έτσι την δυνατότητα στους προγραμματιστές να δημιουργούν διάφορους τύπους βάσεων δεδομένων, οι οποίες όχι μόνο θα μπορούσαν να αποθηκεύσουν περισσότερους τύπους πληροφορίας, όπως για παράδειγμα συμβόλαια/συμφωνίες, μετοχές ή ακόμα και εκλογικά αποτελέσματα αλλά επίσης και να εκτελέσουν μια σειρά από προκαθορισμένες πράξεις/εντολές υπό συγκεκριμένες προϋποθέσεις.

Σε αυτό το νέο πλαίσιο, δίνεται η δυνατότητα στους ενδιαφερόμενους να προγραμματίσουν συγκεκριμένες εφαρμογές οι οποίες μπορούν να λειτουργήσουν στην πλατφόρμα με τον προκαθορισμένο τρόπο τους και να εκτελεστούν αυτόματα χωρίς διακοπές ή παρεμβολές από οποιονδήποτε. Έτσι, η πλατφόρμα του Ethereum δεν αποτελεί απλώς ένα σύστημα πληρωμών όπως το bitcoin, αλλά ένα δίκτυο σχεδιασμένο για να επιτρέπει την ανάπτυξη οποιασδήποτε αποκεντρωμένης εφαρμογής.

Η φιλοσοφία και η τεχνολογία του Ethereum έχει ως βάση του το bitcoin, ιδιαίτερα υπό την άποψη ότι και αυτή εξαλείφει την ανάγκη της όποιας διαμεσολάβησης για την απόδειξη και την καταγραφή μίας συναλλαγής. Το Ethereum επίσης, δίνει μεγάλη βαρύτητα στα ακόλουθα δύο χαρακτηριστικά: πρώτον στην μεγαλύτερη ταχύτητα και στα μεγαλύτερα επίπεδα ασφάλειας των συναλλαγών και, δεύτερον στην αποδοτική λειτουργία των εφαρμογών πέρα από τα συστήματα που

[6] https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

χρησιμοποιούνται αποκλειστικά για πληρωμές. Τέλος, για να χρησιμοποιήσει κάποιος ενδιαφερόμενος την πλατφόρμα με σκοπό να χρησιμοποιήσει κάποια εφαρμογή της, θα πρέπει να χρησιμοποιήσει το κρυπτονόμισμα της πλατφόρμας, που ονομάζεται Αιθέρας (Ether).

2.4.2 Τα έξυπνα συμβόλαια (Smart Contracts).

Η μεγάλη καινοτομία της πλατφόρμας του ethereum είναι πως έδωσε την δυνατότητα προγραμματισμού εντολών οι οποίες ελέγχουν απευθείας την μεταφορά ηλεκτρονικών νομισμάτων ή περιουσιακών στοιχείων μεταξύ των εμπλεκόμενων μελών υπό συγκεκριμένους όρους. Αυτή η καινοτομία ονομάζεται ‘΄έξυπνα συμβόλαια’’. Ένα έξυπνο συμβόλαιο όχι μόνο ορίζει τους κανόνες σχετικά με μία συμφωνία με τον ίδιο τρόπο που το κάνει ένα παραδοσιακό συμβόλαιο, αλλά μπορεί επίσης να επιβάλλει αυτομάτως αυτές τις νομικές διατάξεις/υποχρεώσεις.

Η ιδέα των έξυπνων συμβολαίων είχε αρχικά προταθεί από τον Szabo[7], σχεδόν 20 χρόνια πριν την δημιουργία της πλατφόρμας του ethereum. Ο Szabo τα περιέγραψε ως ‘πρωτόκολλα υπολογιστών τα οποία εκτελούν τους όρους ενός συμβολαίου’. Είναι νομικές διατάξεις οι οποίες έχουν τυποποιηθεί σε υπολογιστικό κώδικα, έτσι ώστε όταν αυτές εκτελούνται να εφαρμόζεται αυτόματα η σχετική συμφωνία. Με άλλα λόγια, πρόκειται για υπολογιστικά πρωτόκολλα τα οποία πραγματοποιούν, επιβάλλουν και επαληθεύουν την εκτέλεση των όρων ενός συμβολαίου.

Οι όροι ενός συμβολαίου εισάγονται με την μορφή υπολογιστικών εντολών και εκτελούνται μέσω της τεχνολογίας του Blockchain. Χρησιμοποιώντας την τεχνολογία του Blockchain, οι όροι αυτοί δεν μπορούν να παραβιαστούν και κάθε συμβόλαιο καταγράφεται στην διαμοιρασμένη βάση δεδομένων. Όταν πληρούνται συγκεκριμένες προϋποθέσεις, όπως έχει προγραμματιστεί από τους όρους του συμβολαίου, τότε το συμβόλαιο εκτελείται αυτόματα χωρίς την παρέμβαση κάποιου διαμεσολαβητή.

Έξυπνα συμβόλαια μπορούν να σχεδιαστούν για το οτιδήποτε. Ένα απλό παράδειγμα των δυνατοτήτων των έξυπνων συμβολαίων, είναι η περίπτωση της αγοράς ακινήτων. Ας υποθέσουμε ότι ο Bob θέλει να αγοράσει ένα ακίνητο το οποίο ανήκει στην Mary. Στην πραγματική ζωή, θα χρειαζόταν να προσλάβει έναν δικηγόρο για να ελέγξει εάν όλα τα έγγραφα είναι νόμιμα, θα έπρεπε να κανονίσει πληρωμές με την τράπεζα και θα έπρεπε επίσης να ειδοποιήσει την αντίστοιχη κρατική αρχή σχετικά με την αγορά. Με την χρήση της τεχνολογίας του Blockchain, τα έγγραφα του ακινήτου μπορούν να φορτωθούν στο blockchain και κάθε διαδικασία στο ιστορικό του ακινήτου μπορεί να ενημερωθεί, έτσι ώστε ο Bob να έχει μια πλήρη και σαφή εικόνα του ιστορικού του ακινήτου. Ένα έξυπνο συμβόλαιο μπορεί να σχεδιαστεί έτσι ώστε όταν ο Μπομπ αποφασίσει να αγοράσει το σπίτι και μεταφέρει τα χρήματα, αυτό να ενεργοποιηθεί και, ταυτόχρονα, η Μαίρη να λάβει τα χρήματα, η ιδιοκτησία του ακινήτου να μεταφερθεί στον Μπομπ και το κράτος να ενημερωθεί. Υπάρχει ήδη μεγάλων αριθμός από πρωτοβουλίες που διερευνούν την εφαρμογή της τεχνολογίας

[7]https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

των έξυπνων συμβολαίων σε διάφορους τομείς. Για παράδειγμα, στον κλάδο της υγειονομικής περίθαλψης, τα αρχεία υγείας και το ιστορικό των ασθενών, μπορούν να διατηρηθούν σε ένα έξυπνο συμβόλαιο και να αποθηκευτούν στο blockchain, έτσι ώστε αυτές οι πληροφορίες να διατίθενται σε νοσοκομεία και ερευνητικά ιδρύματα παντού. Επίσης, οι εταιρείες θα μπορούσαν να χρησιμοποιούν τα έξυπνα συμβόλαια για οποιαδήποτε λειτουργική δαπάνη, όπως η πληρωμή των εργαζομένων τους, οι λογαριασμοί κοινής ωφελείας και οι εταιρικοί φόροι.

Κεφάλαιο 3: Κρυπτονομίσματα-Άντληση κεφαλαίων στην κρυπτοοικονομία, η περίπτωση των ICOs

3.1 Εισαγωγή και ταξινόμηση των ψηφιακών νομισμάτων, των υποκατηγοριών του και των tokens.

Ο προσδιορισμός ενός νέου πεδίου ή μίας νέας τεχνολογίας, όπως και στην περίπτωση του blockchain, δεν αποτελεί εύκολη υπόθεση. Ο προσδιορισμός αυτός, θα πρέπει να γίνει με τέτοιο σαφή τρόπο ώστε το ίδιο πράγμα να γίνεται κατανοητό από όλους, αλλά ταυτόχρονα θα πρέπει να είναι και αρκετά ευρύς ώστε να επιτρέπει την δημιουργία ενός ευρύτερου φάσματος, μέσα στο οποίο θα περιέχονται μία σειρά από διαφορετικά μεταξύ τους στοιχεία τα οποία παρουσιάζουν ορισμένες ομοιότητες αλλά και διαφορές, σε ένα ή σε περισσότερα από τα χαρακτηριστικά τους.

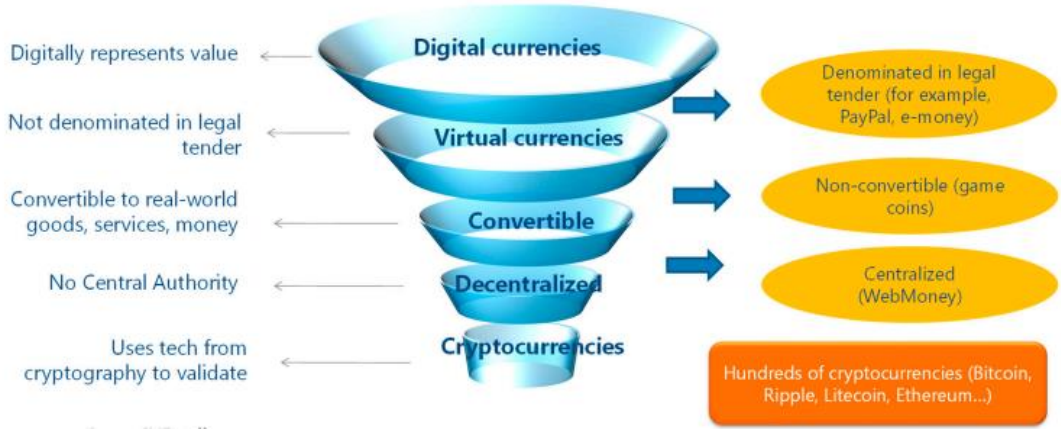
Έτσι και στην περίπτωση του blockchain, όντας μία ιδέα η οποία έχει δημιουργηθεί μόλις τα τελευταία 15 περίπου χρόνια, ο ορισμός και η κατηγοριοποίηση των εννοιών που έχουν δημιουργηθεί μέσω της τεχνολογίας του και των εφαρμογών της, αποτελεί ένα αρκετά δύσκολο έργο. Για παράδειγμα, πολλοί έχουμε πλέον ακούσει έννοιες όπως κρυπτονόμισμα, ψηφιακό νόμισμα ή εικονικό νόμισμα, οι οποίες συχνά χρησιμοποιούνται σαν να περιγράφουν το ίδιο πράγμα, αλλά κάτι τέτοιο δεν ισχύει. Παρομοίως και η έννοια της μάρκας (token), συχνά χρησιμοποιείται αντί του κρυπτονομίσματος, αλλά όπως θα δούμε και παρακάτω τα token προσφέρουν ένα μεγαλύτερο εύρος λειτουργιών, οι οποίες διαφέρουν από τις αντίστοιχες των κρυπτονομισμάτων.

Σε αυτό το κεφάλαιο θα εστιάσουμε στην ανάλυση των κρυπτονομισμάτων και των token, αλλά σε πρώτη φάση, ο προσδιορισμός τους, δεν μπορεί να γίνει χωρίς μια σύντομη αναφορά στα ψηφιακά και εικονικά νομίσματα, μιας και οι έννοιες που μας ενδιαφέρουν στην προκειμένη περίπτωση, αποτελούν μέρη ενός ευρύτερου συνόλου.

Στο σχήμα που ακολουθεί, παρουσιάζεται η συσχέτιση των εννοιών που μόλις αναφέραμε, σύμφωνα με την προσέγγιση του Διεθνούς Νομισματικού Ταμείου (ΔΝΤ). Όπως μπορούμε να διακρίνουμε, τα κρυπτονομίσματα (cryptocurrencies), αποτελούν

μια υποκατηγορία των εικονικών νομισμάτων (virtual currencies), τα οποία με την σειρά τους αποτελούν υποκατηγορία των ψηφιακών νομισμάτων (digital currencies).

Σχήμα 5: Ταξινόμηση των εικονικών νομισμάτων



Σημείωση: Πηγή: He et al., (2016).

Σύμφωνα με την Παγκόσμια Τράπεζα (World Bank)[8], τα ψηφιακά νομίσματα, ορίζονται ως ψηφιακές αναπαραστάσεις αξίας οι οποίες εκφράζονται στην δική τους λογιστική μονάδα, οι οποίες διαφέρουν από το ηλεκτρονικό χρήμα, το οποίο είναι απλώς ένας ψηφιακός μηχανισμός πληρωμών, που αντιπροσωπεύει και εκφράζεται σε συμβατικά χρήματα.

Η Εσωτερική Υπηρεσία Εσόδων (IRS)[9], των Ηνωμένων Πολιτειών, ορίζει τα εικονικά νομίσματα ως μία ψηφιακή αναπαράσταση της αξίας, εκτός από την αναπαράσταση του δολαρίου ΗΠΑ ή ενός ξένου νομίσματος ("πραγματικό νόμισμα"), που λειτουργεί ως λογιστική μονάδα, ως μέσο αποθήκευσης αξίας και ως μέσο ανταλλαγής. Ορισμένα εικονικά νομίσματα είναι μετατρέψιμα, πράγμα που σημαίνει ότι έχουν ισοδύναμη αξία σε ένα πραγματικό νόμισμα ή λειτουργούν ως υποκατάστατο για ένα πραγματικό νόμισμα.

3.1.1 Τα κρυπτονομίσματα.

Με βάση όλα όσα προηγήθηκαν, μπορούμε να προσδιορίσουμε με μεγαλύτερη ακρίβεια την έννοια των κρυπτονομισμάτων και των token. Αρχικά τα κρυπτονομίσματα διαφέρουν από τα εικονικά νομίσματα κυρίως λόγω ότι υπονοείται η χρήση κρυπτογραφικών μεθόδων στη λειτουργία τους. Αυτό είναι προφανές και στο λεξιλόγιο που χρησιμοποιείται και σε μια σειρά από επίσημα έγγραφα από διεθνείς ιδρύματα και οργανισμούς, όπως αυτά που αναφέρθηκαν προηγουμένως. Αρχικά, το ΔΝΤ (2016), αναφέρεται στην διαφορά των δύο εννοιών, λέγοντας πως τα πορτοφόλια εικονικών νομισμάτων χρησιμοποιούνται από τους ιδιοκτήτες τους για αποθήκευση και συναλλαγή σε όρους εικονικών νομισμάτων. Ενώ, τα κρυπτονομίσματα

[8] https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

[9] https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions

αποθηκεύονται λογισμικό ψηφιακών πορτοφολιών το οποίο συσχετίζεται με κλειδιά κρυπτογράφησης. Η Παγκόσμια Τράπεζα (2017), αναφέρει πως τα κρυπτονομίσματα αποτελούν ένα υποσύνολο των ψηφιακών νομισμάτων τα οποία βασίζονται σε κρυπτογραφικές μεθόδους για να επιτύχουν την συναίνεση, όπως για παράδειγμα το Bitcoin και ο Αιθέρας (Ether). Επίσης, μια αναφορά της Τράπεζας Διεθνών Διακανονισμών (BIS)[10], αναφέρει ξεκάθαρα πως τα συστήματα αυτά των εικονικών νομισμάτων, αναφέρονται συχνά ως κρυπτονομίσματα, αντικατοπτρίζοντας τη χρήση κρυπτογραφίας στην έκδοση τους και στην επικύρωση των συναλλαγών. Τέλος, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[11] , σε ένα άρθρο του, παρέχει τον ακόλουθο ορισμό: Τα κρυπτονομίσματα αναφέρονται σε ένα βασιζόμενο στα μαθηματικά, αποκεντρωμένο και μετατρέψιμο εικονικό νόμισμα το οποίο προστατεύεται από κρυπτογραφία, δηλαδή, ενσωματώνει αρχές κρυπτογραφίας για να εφαρμόσει μία διανεμημένη, αποκεντρωμένη και ασφαλής οικονομία της πληροφορίας.

Έτσι, αθροίζοντας τους παραπάνω ορισμούς, καταλήγουμε στο ότι τα κρυπτονομίσματα είναι ένα υποσύνολο των εικονικών νομισμάτων τα οποία χρησιμοποιούν κρυπτογραφία για να λειτουργήσουν σε ένα διανεμημένο, αποκεντρωμένο, και ασφαλές περιβάλλον.

3.1.2 Τα tokens.

Ο όρος ψηφιακές μάρκες (tokens), δεν συμπεριλαμβάνεται στο παραπάνω σχήμα, αλλά χρησιμοποιείται συχνά, εναλλακτικά με τον όρο των κρυπτονομισμάτων. Το γεγονός πως ο όρος αυτός, ο οποίος δεν είναι καθόλα ίδιος με τα κρυπτονομίσματα, αποτελεί βασική έννοια τόσο αυτού του κεφαλαίου όσο και του επόμενου, καθιστά απαραίτητο τον προσδιορισμό του και την εξερεύνηση των διαφορών του με τον όρο των κρυπτονομισμάτων.

Σύμφωνα με την Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών[12] ως ψηφιακό token ορίζεται κάθε ψηφιακή αναπαράσταση ενός ενδιαφέροντος, το οποίο μπορεί να είναι κάποιας αξίας, ένα δικαίωμα λήψης ενός οφέλους ή να εκτελέσει συγκεκριμένες λειτουργίες ή μπορεί και να μην έχει συγκεκριμένο σκοπό ή χρήση. Επίσης, η Ευρωπαϊκή Κεντρική Τράπεζα[13], αναφέρει πως τα tokens αποτελούν απλά ψηφιακές αναπαραστάσεις υπαρχόντων περιουσιακών στοιχείων, τα οποία επιτρέπουν την καταγραφή αυτών των στοιχείων χρησιμοποιώντας διαφορετική τεχνολογία.

Οι δύο ορισμοί που προηγήθηκαν υπονοούν πως η έννοια του token συμπεριλαμβάνει ένα ευρύτερο φάσμα λειτουργιών σε σχέση με τα κρυπτονομίσματα, από την στιγμή όπου αυτά περιορίζονται περισσότερο στο ρόλο του "νομίσματος", που εμπεριέχεται σε αυτούς. Πιο συγκεκριμένα, τα tokens όπως τα ψηφιακά νομίσματα και κατ' επέκταση τα κρυπτονομίσματα, εμπεριέχουν τις 3 βασικές λειτουργίες αυτών, όπως αναφέρονται παραπάνω, δηλαδή αποτελούν μέσο συναλλαγής, λογιστική μονάδα

[10] https://www.bis.org/cpmi/publ/d137.pdf

[11] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-opinion-paper-on-cryptocurrencies-in-the-eu

[12] https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

[13] https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

και μέσο αποθήκευσης της αξίας, αλλά ο ρόλος τους είναι ευρύτερος και δεν αποτελεί μόνο ένα νόμισμα. Αντιθέτως, τα tokens μπορούν να εκτελέσουν περισσότερες λειτουργίες από αυτές των κρυπτονομισμάτων που αναφέραμε πριν. Για παράδειγμα, μπορούν να παρέχουν προνομιακή πρόσβαση σε ένα συγκεκριμένο προϊόν ή υπηρεσία, σκοπό για τον οποίο μάλιστα και εκδίδονται, ή ακόμα και δυνατότητα συμμετοχής στην ανάπτυξη του προϊόντος ή της υπηρεσίας. Έτσι, αυτή η πολυπλοκότητα που διέπει τις λειτουργίες τους, αποτελούν την απάντηση στο ερώτημα γιατί κατά κύριο λόγο χαρακτηρίζονται ως ψηφιακές μάρκες (digital chips).

3.2 Συναλλαγές με κρυπτονομίσματα και τα κύρια χαρακτηριστικά τους

3.2.1 Συναλλαγές κρυπτονομισμάτων με την χρήση crypto-wallets (δημόσιο και ιδιωτικό κλειδί).

Τα κρυπτονομίσματα λειτουργούν σε δίκτυα peer-to-peer, με πρωτόκολλα ανοιχτού κώδικα. Ένα δίκτυο με τα παραπάνω τεχνικά χαρακτηριστικά δεν υπόκειται σε κεντρική αρχή και δεν υπάρχει διαμεσολαβητής σε αυτό. Όλο το δίκτυο και οι συναλλαγές του ελέγχονται από τους ίδιους τους χρήστες, οι οποίοι είναι υπεύθυνοι τόσο για την επιβεβαίωση των συναλλαγών, όσο και για την ασφάλεια του δικτύου.

Τα κρυπτονομίσματα δεν υπάρχουν σε φυσική αλλά μόνο σε ψηφιακή μορφή. Ο μόνος τρόπος αποθήκευσης τους είναι σε ψηφιακά πορτοφόλια. Το ψηφιακό πορτοφόλι είναι ένα λογισμικό που στέλνει, λαμβάνει, και αποθηκεύει ψηφιακούς κωδικούς που αντιπροσωπεύουν και αντικατοπτρίζουν την αξία των κρυπτονομισμάτων. Υπάρχουν διαδικτυακές πλατφόρμες που προσφέρουν διαδικτυακά ψηφιακά πορτοφόλια, αλλά οι χρήστες μπορούν επίσης να χρησιμοποιούν συσκευές εκτός σύνδεσης που τους επιτρέπουν να αποθηκεύουν τα κρυπτονομίσματα τους εκτός δικτύου (hardware wallets). Τα ψηφιακά πορτοφόλια αποτελούνται από δύο κλειδιά (Σχήμα 6): (α) ένα δημόσιο κλειδί, που χρησιμοποιείται για τη λήψη κεφαλαίων και το οποίο προσδιορίζει τον λογαριασμό του μεμονωμένου χρήστη στο δίκτυο και είναι ορατό και γνωστό σε όλους, και (β) ένα ιδιωτικό κλειδί, το οποίο χρησιμοποιείται μόνο για την υπογραφή συναλλαγών και ως απόδειξη ότι ο μεμονωμένος χρήστης κατέχει τα σχετικό δημόσιο κλειδί, είναι γνωστό μόνο από τον χρήστη και δεν πρέπει να κοινοποιείται.

Αυτό το ζεύγος δημόσιου/ιδιωτικού κλειδιού δημιουργείται μέσω ενός συγκεκριμένου αλγόριθμου κρυπτογράφησης. Τα δύο κλειδιά έχουν τη μορφή συμβολοσειράς (περιέχουν λατινικούς χαρακτήρες, αριθμούς και σύμβολα) και έχουν μαθηματική σχέση μεταξύ τους. Συνήθως, όσο περισσότερους χαρακτήρες περιέχουν τόσο μεγαλύτερη είναι και η ασφάλειά τους. Τα σύμβολα και οι αριθμοί προκύπτουν τυχαία μετά την εφαρμογή μιας συνάρτησης κατακερματισμού (hash function).

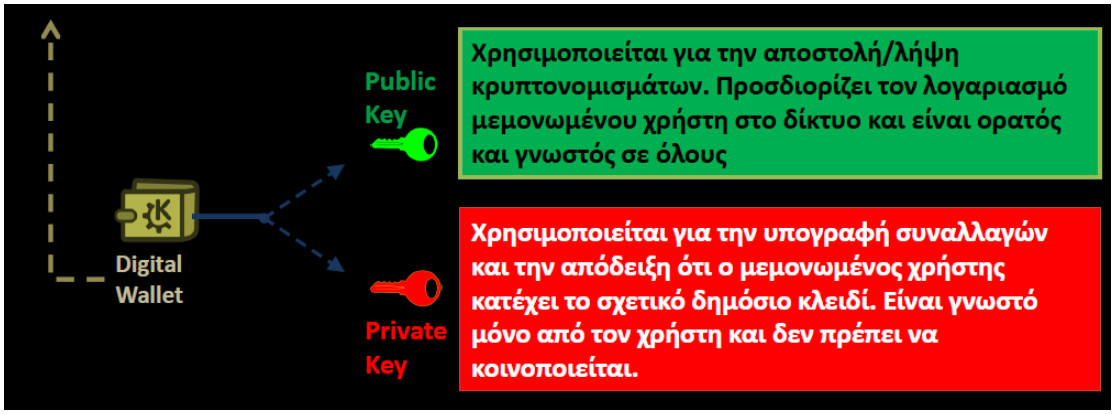
Σε αυτό το σημείο είναι εύλογο να αναφέρουμε πως το Blockchain χρησιμοποιεί την μέθοδο της κρυπτογραφίας, κατά την οποία πληροφορίες μπορούν να αποκρύπτονται και να αποκαλύπτονται μόνο σε εκείνους για τους οποίους αυτές προορίζονταν, μέσω της χρήσης πολύπλοκων μαθηματικών πράξεων. Η κρυπτογραφία

αξιοποιείται με 2 τρόπους. Αρχικά, μέσω αλγορίθμων (cryptographic hash functions), οι οποίοι δημιουργούν μία αλυσίδα μέσω της οποίας διαβεβαιώνεται πως τηρείται η σειρά με την οποία εκτελούνται οι συναλλαγές. Έχει ομοιότητες με το λογιστικό βιβλίο όπου χρησιμοποιεί το εκάστοτε ίδρυμα για να καταγράφει τις συναλλαγές αλλά με την ειδοποιό διαφορά πως στο αντίστοιχο βιβλίο του blockchain καταγράφονται όλες οι πληροφορίες και όλοι έχουν πρόσβαση σε αυτό. Ο 2ος τρόπος χρήσης της κρυπτογραφίας έχει να κάνει με την δημιουργία ηλεκτρονικών υπογραφών οι οποίες χρησιμοποιούνται για να διασφαλίσουν ότι τα δεδομένα που τοποθετούνται στο Blockchain είναι έγκυρα. Οι ηλεκτρονικές υπογραφές επίσης χρησιμοποιούνται για να επιβεβαιωθεί πως η σωστή ποσότητα πληροφορίας μεταφέρθηκε από ένα πορτοφόλι bitcoin σε ένα άλλο. Μέσω αυτών των 2 μεθόδων χρήσης της κρυπτογραφίας, η τεχνολογία του Blockchain διασφαλίζει το αίσθημα της εμπιστοσύνης και επιλύει το πρόβλημα της διπλής δαπάνης.

Τώρα, αφού παραθέσαμε την επεξήγηση της συνάρτησης κατακερματισμού, μπορούμε να συνεχίσουμε. Αυτά λοιπόν τα δύο κλειδιά αποθηκεύονται στο ψηφιακό πορτοφόλι του χρήστη. Κάθε κρυπτονόμισμα έχει το δικό του ψηφιακό πορτοφόλι και συνεπώς τα δικά του κλειδιά. Για παράδειγμα, κάποιος που έχει τρεις διαφορετικούς τύπους κρυπτονομισμάτων, θα έχει τρία διαφορετικά ψηφιακά πορτοφόλια με τα αντίστοιχα ψηφιακά κλειδιά τους. Να σημειωθεί, ωστόσο, πως υπάρχουν ήδη μικτά πορτοφόλια που επιτρέπουν την αποθήκευση περισσότερων του ενός είδους κρυπτονομισμάτων σε ένα πορτοφόλι, με διαφορετικές «τσέπες», δηλαδή διαφορετικά δημόσια κλειδιά.

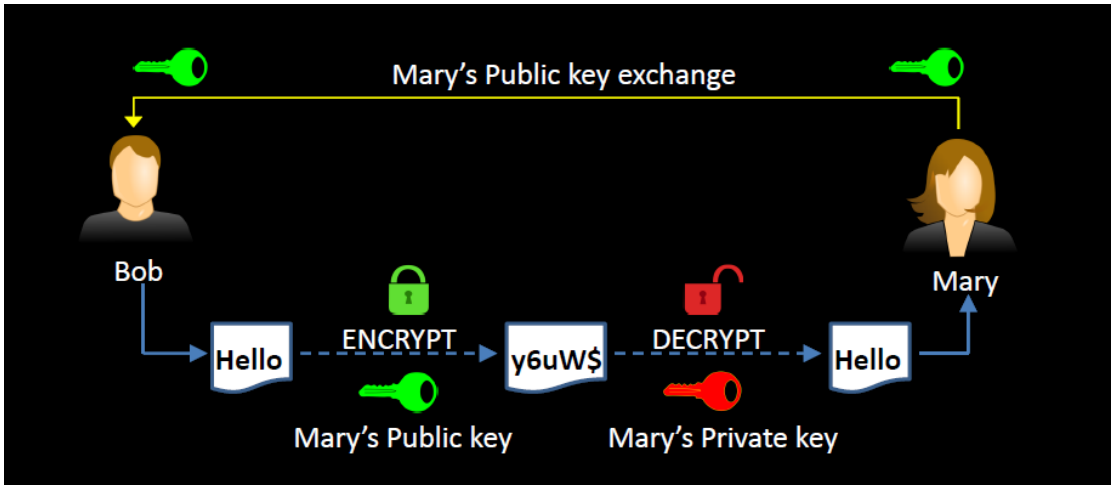
Ο ιδιοκτήτης ενός κρυπτονομίσματος είναι το άτομο που κατέχει το ιδιωτικό κλειδί. Αυτό το ιδιωτικό κλειδί είναι γνωστό μόνο στον κάτοχό του και είναι το πιο σημαντικό στοιχείο για τη λειτουργία του ψηφιακού πορτοφολιού. Το ιδιωτικό κλειδί δεν μπορεί να εκδοθεί ξανά. Εάν ο ιδιοκτήτης χάσει το ιδιωτικό κλειδί, χάνει και την πρόσβαση στο ψηφιακό του πορτοφόλι αλλά και σε όλα τα κρυπτονομίσματα που αυτό περιέχει. Το δημόσιο κλειδί από την άλλη πλευρά, είναι η δημόσια διεύθυνση του πορτοφολιού κάποιου, ορατό σε όλους τους χρήστες και όπου πραγματοποιούνται όλες οι συναλλαγές. Όμως, παρόλο που το δημόσιο κλειδί του χρήστη είναι δημόσια ορατό, είναι αδύνατο (τεχνικά και υπολογιστικά) να χρησιμοποιηθεί για να βρεθεί το αντίστοιχο ιδιωτικό κλειδί.

Σχήμα 6: Το δημόσιο και ιδιωτικό κλειδί



Σημείωση: πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

Σχήμα 7: Παράδειγμα συναλλαγής στο blockchain



Σημείωση: Πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

Για την καλύτερη κατανόηση της συνάρτησης των δύο κλειδιών, αυτή θα μπορούσε να συγκριθεί με τη συνάρτηση του ηλεκτρονικού ταχυδρομείου. Το δημόσιο κλειδί είναι σαν τη διεύθυνση email που είναι γνωστή σε κάποιον ο οποίος θέλει να στείλει ένα μήνυμα και το ιδιωτικό κλειδί είναι σαν τον κωδικό πρόσβασης του λογαριασμού email που απαιτείται για να συνδεθεί κάποιος και να διαβάσει το μήνυμα. Ένα παράδειγμα του πώς αυτό το ζεύγος κλειδιών λειτουργεί, ας υποθέσουμε ότι ο Bob θέλει να στείλει οποιοδήποτε είδος πληροφορίας (δηλαδή, ένα μήνυμα ή 1 bitcoin) στη Mary (Σχήμα 7). Ο Μπομπ χρησιμοποιεί το δημόσιο κλειδί της Mary (την διεύθυνση bitcoin της) για την κρυπτογράφηση των ψηφιακών πληροφοριών της συναλλαγής. Η Μαίρη τότε λαμβάνει το κρυπτογραφημένο μήνυμα και πρέπει να χρησιμοποιήσει το ιδιωτικό της κλειδί για να το αποκρυπτογραφήσει.

3.2.2 Κύρια χαρακτηριστικά κρυπτονομισμάτων

Τα κρυπτονομίσματα χρησιμοποιούν την τεχνολογία του blockchain, και έτσι εφαρμόζουν τις κύριες ιδιότητες της ασφάλειας, της διαφάνειας και της μη αναστρεψιμότητας που προσφέρει η τεχνολογία. Αυτές οι τρεις καθώς και μερικές επιπρόσθετες ιδιότητες των κρυπτονομισμάτων συζητούνται παρακάτω.

I) Αποκέντρωση. Τα κρυπτονομίσματα βασίζονται σε δίκτυα peer-to-peer και όχι σε κεντρικούς υπολογιστές (servers). Οι συναλλαγές επαληθεύονται από ολόκληρη την κοινότητα, δηλαδή από τους ίδιους τους χρήστες, και δεν υπάρχει ανάγκη για εξάρτηση από τρίτους. Αυτή η δυνατότητα αποκέντρωσης ισχύει στα περισσότερα κρυπτονομίσματα, αλλά υπάρχουν εξαιρέσεις όπου οι συναλλαγές επαληθεύονται είτε από μια κεντρική αρχή είτε από έναν αριθμό εξουσιοδοτημένων συμμετεχόντων. Η τεχνολογία του blockchain επιτρέπει την ύπαρξη αυτών των διαφοροποιήσεων και εξαρτάται από τον σχεδιαστή του έργου στο να αποφασίσει για το επίπεδο αποκέντρωσης.

II) Ασφάλεια. Η ασφάλεια είναι ένα εγγενές χαρακτηριστικό της τεχνολογίας του blockchain που χρησιμοποιεί κρυπτογράφηση. Όλες οι συναλλαγές είναι κρυπτογραφημένες και είναι πρακτικά αδύνατο να παραβιαστούν και να αλλάξει η αλυσίδα των συναλλαγών. Ορισμένες ανησυχίες προέκυψαν πρόσφατα μετά από τις εξελίξεις στον κβαντικό υπολογισμό, αλλά οι ειδικοί πληροφορικής πιστεύουν ότι οι πρακτικές κρυπτογράφησης στο Blockchain μπορούν να ενημερωθούν αντίστοιχα.

III) Διαφάνεια. Υπάρχουν τρία χαρακτηριστικά διαφάνειας στα κρυπτονομίσματα. Πρώτον, οι συναλλαγές επαληθεύονται από πολλούς κόμβους του δικτύου μέσω ενός μηχανισμού ομαδικής συναίνεσης. Δεύτερον, όλες οι συναλλαγές καταγράφονται σε δημόσιες βάσεις δεδομένων (δημόσια λογιστικά βιβλία). Τρίτον, όλοι οι χρήστες έχουν πρόσβαση σε αυτό το δημόσιο αρχείο/δημόσιο βιβλίο ανά πάσα στιγμή.

IV) Ανωνυμία. Οι συναλλαγές σε κρυπτονομίσματα πραγματοποιούνται με πιστοποίηση των ψηφιακών υπογραφών των συμμετεχόντων και δεν χρειάζονται άλλα προσωπικά στοιχεία. Αυτή το χαρακτηριστικό της ανωνυμίας, έχει εγείρει ανησυχίες σχετικά με τη χρήση της τεχνολογίας για κακόβουλες πρακτικές, (δηλαδή, ξέπλυμα χρήματος και χρηματοδότηση της τρομοκρατίας). Ωστόσο, από την στιγμή που τα σημεία εισόδου και εξόδου στο σύστημα (δηλαδή οι ανταλλαγές κρυπτονομισμάτων με συμβατικά νομίσματα) μπορούν να εντοπιστούν και αφού όλες οι συναλλαγές καταγράφονται και είναι δημόσια διαθέσιμες στο σύστημα, οι ρυθμιστικές αρχές θα πρέπει να είναι σε θέση να εντοπίζουν τυχόν κακόβουλες πρακτικές.

V) Μετατρεψιμότητα. Όλα τα κρυπτονομίσματα είναι άμεσα ή έμμεσα μετατρέψιμα σε συμβατικά νομίσματα. Μερικά κρυπτονομίσματα (π.χ. bitcoin, Ethereum, Litecoin) μπορούν να μετατραπούν απευθείας σε συμβατικά. Όλα τα άλλα πρέπει πρώτα να ανταλλάσσονται με τα πρώτα πριν εξαργυρωθούν σε συμβατικά νομίσματα.

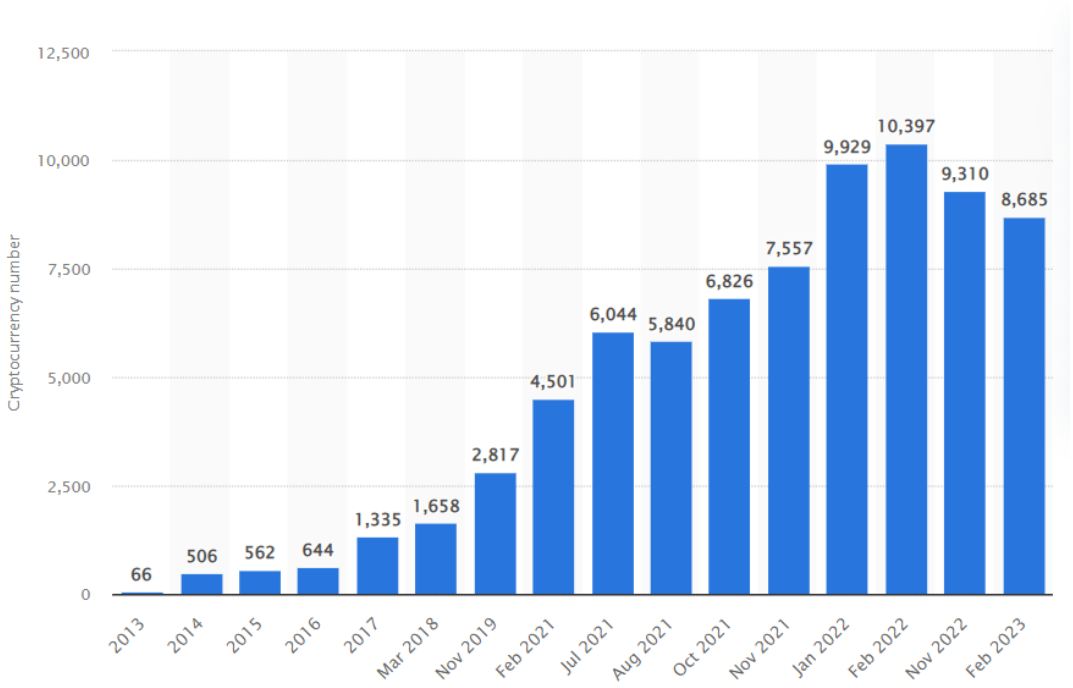
VI) Πεπερασμένη προσφορά. Τα περισσότερα κρυπτονομίσματα έχουν πεπερασμένη προσφορά. Ανάλογα με το έργο, η πεπερασμένη προσφορά μπορεί είτε να ασκηθεί από την αρχή, δηλαδή το έργο να παράγει και να προσφέρει όλα τα tokens (ψηφιακές μάρκες), ευθύς εξαρχής, ή μπορεί να φτάσει σταδιακά με την πάροδο του χρόνου, δηλαδή tokens θα συνεχίσουν να δημιουργούνται μέσω της διαδικασίας εξόρυξης έως ότου φτάσουν ένα συγκεκριμένο ανώτατο όριο προσφοράς κάποια στιγμή στο μέλλον. Ας σημειωθεί εδώ, ότι παρόλο που η πλειοψηφία των κρυπτονομισμάτων έχουν μια πεπερασμένη παροχή ενσωματωμένη στο πρωτόκολλο τους, οι προγραμματιστές μπορεί επίσης να δημιουργήσουν και κρυπτονομίσματα που έχουν άπειρη προσφορά. Το πιο εξέχον παράδειγμα εδώ είναι το Ethereum, το οποίο δεν έχει ακόμη δηλωμένο ανώτατο όριο ανεφοδιασμού, αλλά αυτό μπορεί και να αλλάξει από τους προγραμματιστές του έργου, εάν χρειαστεί.

VII) Μη αναστρεψιμότητα. Τη στιγμή που μια συναλλαγή επικυρώνεται και ένα μπλοκ δημιουργείται και καταγράφεται στο blockchain, δεν μπορεί να ακυρωθεί. Ο μόνος τρόπος για να αντιστραφεί μια συναλλαγή είναι να δημιουργηθεί μία νέα με αντίθετη κατεύθυνση.

3.3 Altcoins (εναλλακτικά κρυπτονομίσματα)

Το Bitcoin είναι το πρώτο πλήρως αποκεντρωμένο κρυπτονόμισμα και ίσως το πιο δημοφιλές, αλλά όχι το μοναδικό. Αυτή τη στιγμή (Φεβρουάριος 2023) υπάρχουν περισσότερα από 8.600 κρυπτονομίσματα (Διάγραμμα 1) συνολικής αγοραίας αξίας περίπου 1,08 τρισεκατομμυρίων δολαρίων (Φεβρουάριος 2023). Το bitcoin έχει ακόμα το μεγαλύτερο μερίδιο αγοράς, ακολουθούμενο από το Ethereum και το Tether (Σχήμα 8).

Διάγραμμα 1: Αριθμός κρυπτονομισμάτων παγκοσμίως από το 2013 έως Φεβρουάριο 2023



Σημείωση: Πηγή: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

Σχήμα 8: Κεφαλαιοποίηση αγοράς κρυπτονομισμάτων (Φεβρουάριος 2023) και το ποσοστό του συνόλου της αγοράς που καταλαμβάνει

Total Cryptocurrency Market Cap: $1,080,088,527,578

Rank	Name (Symbol)	Market Cap	Market Share	Price (USD)	24 Hr % Change
1	Bitcoin (BTC)	454,633,926,674	42.0923%	$23,580.6369945021	-1.78715345
2	Ethereum (ETH)	201,844,579,822	18.6878%	$1,649.40919218	-1.73262415
3	Tether (USDT)	68,038,310,544	6.2993%	$1.0001427817	-0.00551699
4	BNB (BNB)	51,490,867,942	4.7673%	$326.0956775036	1.73076292
5	USD Coin (USDC)	42,438,930,631	3.9292%	$0.9999333545	-0.00318099
6	XRP (XRP)	20,869,925,674	1.9322%	$0.4107961061	-0.58312322
7	Binance USD (BUSD)	16,084,725,461	1.4892%	$1.0000219127	-0.06334787
8	Cardano (ADA)	13,884,197,509	1.2855%	$0.4012760715	-0.45453827
9	Dogecoin (DOGE)	12,144,877,912	1.1244%	$0.0915414785	-3.64769435
10	Polygon (MATIC)	10,425,074,616	0.9652%	$1.1935763321	-3.14163239

Σημείωση: πηγή: https://www.slickcharts.com/currency

Όλα τα άλλα κρυπτονομίσματα (εκτός από το bitcoin) ονομάζονται "altcoins" (εναλλακτικά νομίσματα). Τα περισσότερα εμφανίστηκαν από το καλοκαίρι του 2017, κυρίως λόγω της ραγδαίας ανόδου της τιμής του bitcoin, που άρχισε να δημιουργεί προσδοκίες ότι τα κρυπτονομίσματα είναι μια ανερχόμενη αγορά που μπορεί να αποφέρει γρήγορα κέρδη. Ως κρυπτονομίσματα δεν εμπίπτουν σε καμία κεντρική αρχή ή συγκεκριμένο ρυθμιστικό πλαίσιο, και επειδή ο καθένας μπορεί να δημιουργήσει τα δικά του, αυτό είχε ως αποτέλεσμα, ότι όλο και περισσότερα altcoin άρχισαν να διεκδικούν το δικό τους μερίδιο στην αγορά.

Οι δημιουργοί των altcoins υιοθέτησαν τα βασικά χαρακτηριστικά της τεχνολογίας του blockchain και έκτοτε προσπάθησαν είτε να βελτιώσουν αυτά τα βασικά χαρακτηριστικά (κυρίως όσον αφορά την ταχύτητα και την ιδιωτικότητα), ή εφάρμοσαν αυτήν την τεχνολογία σε συγκεκριμένες επιχειρηματικές ιδέες. Και ενώ το bitcoin και μερικά από τα πρώτα altcoins δεν δημιουργήθηκαν ως επιχειρηματικές ιδέες για τη δημιουργία κερδών, η πλειοψηφία των altcoin δημιουργήθηκαν κυρίως για αυτό τον σκοπό, δηλαδή ως επιχειρηματικά έργα.

3.4 Τα Stablecoins

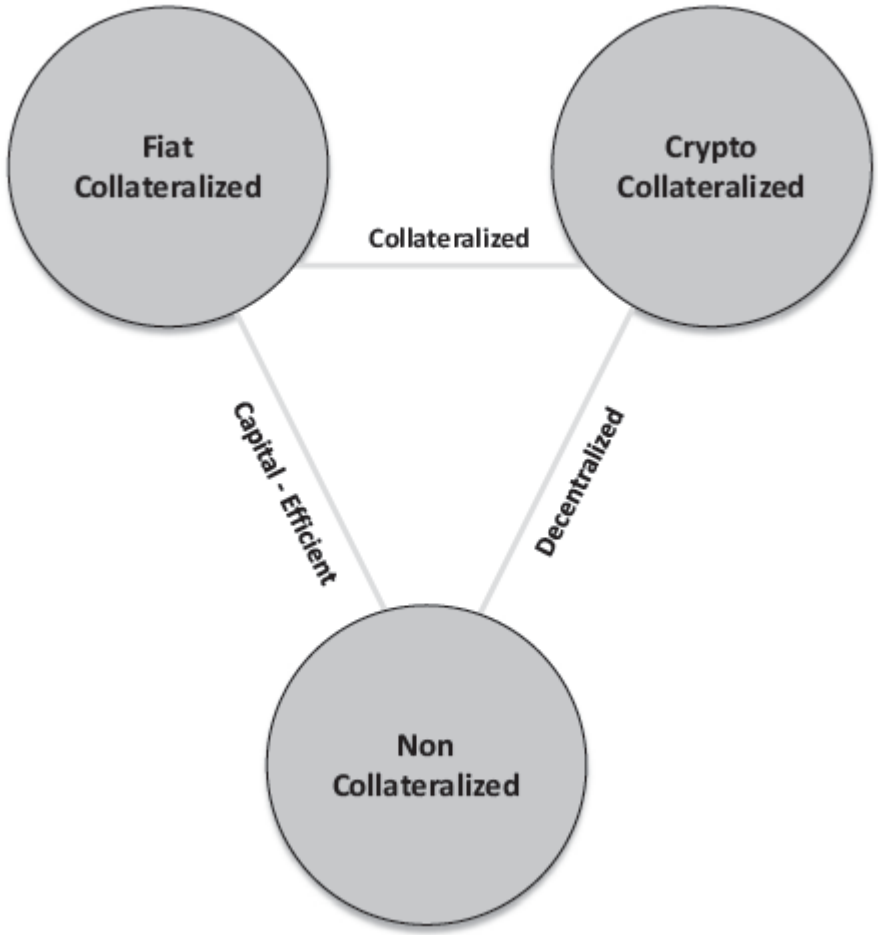
Ένα από τα πιο σημαντικά χαρακτηριστικά του όρου «νόμισμα» είναι η σταθερότητά της αξία του. Η ακραία αστάθεια της αγοράς κρυπτονομισμάτων έχει αψηφήσει έτσι το ίδιο το όνομα/τίτλο που έχει δοθεί σε αυτήν την αγορά, που περιέχει τον όρο «νόμισμα» στον τίτλο της. Από την άλλη πλευρά, η τεχνολογία blockchain φέρει

κάποια συγκεκριμένα χαρακτηριστικά, όπως η ασφάλεια, η ιδιωτικότητα και η ελαχιστοποίηση του κόστους συναλλαγής, πράγμα το οποίο θα μπορούσε να ενισχύσει σημαντικά τις συναλλαγές και να διευκολύνει τις πληρωμές παγκοσμίως, εάν αντιμετωπιστεί η περίπτωση της διακύμανσης των τιμών.

Στις αρχές του 2018, μετά την απότομη άνοδο και πτώση της αγοράς των κρυπτονομισμάτων, δημιουργήθηκε η ανάγκη για ένα «σταθερό νόμισμα» και έτσι, αυτά τα νομίσματα άρχισαν να εμφανίζονται στην αγορά. Τα "stablecoins" είναι ψηφιακά περιουσιακά στοιχεία (coins ή tokens) που έχουν σχεδιαστεί για να διατηρούν την αξία τους. Το επιτυγχάνουν αυτό, μέσω πολλών διαφορετικών μηχανισμών, όπως για παράδειγμα, με το να είναι συνδεδεμένα με άλλα περιουσιακό στοιχείο σχετικά σταθερής αξίας (δηλαδή, ένα συμβατικό νόμισμα ή ένα εμπόρευμα), μέσω μιας διαδικασίας υπερβολικής εξασφάλισης από άλλα πιο σταθερά κρυπτονομίσματα (π.χ. etherium, bitcoin) ή μέσω αλγοριθμικών μηχανισμών.

Τα stablecoins μοιράζονται όλα τα άλλα χαρακτηριστικά των κρυπτονομισμάτων εκτός από την αστάθεια. Αυτό τα καθιστά χρήσιμα στη διευκόλυνση των συναλλαγών σε ανταλλαγές κρυπτονομισμάτων και ως ένα μέσο εξασφάλισης κερδών από τις συναλλαγές κρυπτονομισμάτων, αλλά δεν είναι κατάλληλα για κερδοσκοπικές επενδύσεις δεδομένου ότι οι αποτιμήσεις τους δεν είναι ασταθείς. Τα σταθερά νομίσματα μπορούν να χρησιμοποιηθούν έτσι ως μέσο πληρωμής για καθημερινές συναλλαγές, ως μέσο αποθήκευσης ή ως μέσο ασφάλειας όταν οι επενδυτές αναμένουν πτώση της αξίας στις αγορές κρυπτονομισμάτων.

Σχήμα 9: Τα 3 είδη stablecoin



Σημείωση: Πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

Υπάρχουν τρεις κύριοι τύποι σταθερών (Σχήμα 9): (α) σταθερά νομίσματα με εξασφάλιση συμβατικού νομίσματος (fiat-collateralized), (β) σταθερά νομίσματα με εξασφάλιση κρυπτονομίσματος (crypto-collateralized) και (γ) σταθερά νομίσματα χωρίς εξασφαλίσεις.

3.4.1 σταθερά νομίσματα με εξασφάλιση συμβατικού νομίσματος.

Αυτή είναι η απλούστερη και πιο δημοφιλής κατηγορία stablecoin. Η ιδέα είναι ότι οποιοδήποτε εκδοθέν νόμισμα καλύπτεται από ένα ισοδύναμο συμβατικό νόμισμα, έτσι ώστε κάθε stablecoin να έχει την ίδια αξία με το αντίστοιχο συμβατικό νόμισμα. Σε αυτή την περίπτωση, συνήθως υπάρχει μία κεντρική αρχή, ο εκδότης των νομισμάτων, ο οποίος εκκαθαρίζει τις συναλλαγές (λαμβάνοντας το κόστος της συναλλαγής) και είναι υπεύθυνος για την προμήθεια και τη ρευστοποίηση του νομίσματος.

Το μοντέλο αυτό λειτουργεί ως εξής: Ένας καταθέτης καταθέτει ένα συγκεκριμένο ποσό σε συμβατικό νόμισμα (ας πούμε, δολάρια ΗΠΑ) σε έναν λογαριασμό, η εταιρεία έκδοσης νομισμάτων εκδίδει το αντίστοιχο ποσό των stablecoins και τα πληρώνει στον καταθέτη, ο οποίος είναι τώρα κάτοχος του stablecoin. Όταν εκείνος επιθυμεί να ρευστοποιήσει τα stablecoin του πίσω σε

συμβατικά νομίσματα, ο εκδότης τους επιστρέφει το ισόποσο ποσό σε δολάρια ΗΠΑ και ταυτόχρονα αφαιρεί από την κυκλοφορία ή καταστρέφει τα ισοδύναμα stablecoins.

Το κύριο πλεονέκτημα αυτού του τύπου stablecoin είναι ότι η διαδικασία είναι απλή. Αυτά τα σταθερά νομίσματα παρέχουν σταθερότητα καθώς υποστηρίζονται από συμβατικά νομίσματα, διατηρώντας παράλληλα τα τεχνολογικά πλεονεκτήματα του blockchain. Από την άλλη πλευρά, αυτό το μοντέλο απαιτεί κεντροποίηση/συγκέντρωση καθώς υπάρχει ανάγκη για έναν εκδότη νομισμάτων. Άρα, σε αυτή την περίπτωση απαιτείται ρύθμιση για τον τακτικό έλεγχο του εκδότη του κέρματος. Ένα άλλο μειονέκτημα είναι ότι υπάρχουν έξοδα συναλλαγής, αφού ο εκδότης θα πρέπει να πληρωθεί για τις υπηρεσίες που προσφέρει και δεν υπάρχει διαδικασία εξόρυξης για ανταμοιβές.

Παρομοίως με τα σταθερά νομίσματα εξασφάλισης συμβατικού νομίσματος, ορισμένα κρυπτονομίσματα έχουν υποστήριξη εμπορευμάτων, δηλαδή οι κάτοχοι μπορούν να εξαργυρώσουν τα stablecoins τους βάση την συναλλαγματική ισοτιμία για να λάβουν στην κατοχή τους εμπορεύματα.

3.4.2 σταθερά νομίσματα με εξασφάλιση κρυπτονομίσματος.

Σε αυτή τη περίπτωση τα σταθερά νομίσματα εξασφαλίζονται από κρυπτονομίσματα. Αυτό το γεγονός φέρνει ξανά στο προσκήνιο το θέμα της υπερβολικής μεταβλητότητας. Για να αποφευχθεί αυτό, πραγματοποιείται μία διαδικασία η οποία ονομάζεται «υπερβολική εξασφάλιση». Για παράδειγμα, ο Bob κλειδώνει (δεν πουλά/ανταλλάσσει bitcoin, τα κλειδώνει) bitcoin αξίας 100 δολαρίων και λαμβάνει stablecoins αξίας 50 δολαρίων. Εάν η τιμή του υποκείμενου περιουσιακού στοιχείου (bitcoin στην δική μας περίπτωση), μειώνεται, για παράδειγμα, κατά 10%, το stablecoin θα εξακολουθεί να διατηρεί σταθερή τιμή, καθώς θα εξακολουθεί να υπάρχει μια αξία 90 δολαρίων σε bitcoin που θα υποστηρίζει την αξία του κάθε stablecoin. Αυτή η πτώση της τιμής του υποκείμενου περιουσιακού στοιχείου (όχι του stablecoin) μπορεί να συνεχιστεί έως ότου επιτευχθεί ένα προκαθορισμένο όριο (ας πούμε στα 75 δολάρια), όπου στο όριο αυτό ενεργοποιείται μια διαδικασία τύπου δημοπρασίας όπου τα κλειδωμένα bitcoin του Bob απελευθερώνονται και προσφέρονται στην αγορά για την κάλυψη του δανείου του Bob. Με αυτόν τον τρόπο, η αγορά αγοράζει τα bitcoin του Bob, το δάνειό του διακανονίζεται και το υπόλοιπο ποσό επιστρέφεται σε αυτόν. Για να κατανοήσουμε καλύτερα αυτή τη διαδικασία, μπορούμε να παρομοιάσουμε το ίδρυμα που εκδίδει τα stablecoins ως μία τράπεζα, τα ίδια τα stablecoins ως δάνειο και η υποστήριξη από τα κρυπτονομίσματα ως εγγύηση. Στην πραγματικότητα, ο Μπομπ λαμβάνει ένα υπερ-εξασφαλισμένο δάνειο και όταν η τιμή της εγγύησης μειώνεται, το ίδρυμα ζητά να χρησιμοποιήσει την εγγύηση για τη ρύθμιση του δανείου.

Τα πλεονεκτήματα αυτής της μορφής stablecoin είναι τα ακόλουθα: (i) η αποκεντρωμένη τους δομή σε αντίθεση με την κεντροποιημένη δομή των stablecoins που εξασφαλίζονται από συμβατικά νομίσματα (ii) πλήρης διαφάνεια αφού όλες οι συναλλαγές καταγράφονται στο blockchain, και (iii) γρήγορη μετατροπή αφού τα stablecoins μετατρέπονται εύκολα σε όλα τα άλλα είδη κρυπτονομισμάτων. Μερικά από τα μειονεκτήματα είναι τα ακόλουθα: (i) τα υποκείμενα περιουσιακά στοιχεία

αυτής της κατηγορίας είναι κρυπτονομίσματα, τα οποία είναι πιο ασταθή σε σχέση με τα συμβατικά νομίσματα και (ii) το υποκείμενο κρυπτονόμισμα μπορεί να ρευστοποιηθεί άμεσα εάν η τιμή του πέσει κάτω από ένα ορισμένο όριο.

3.4.3 Σταθερά νομίσματα χωρίς κάποια εξασφάλιση.

Τα μη εξασφαλισμένα σταθερά νομίσματα δεν καλύπτονται από κανένα περιουσιακό στοιχείο, αλλά αναμένονται να διατηρήσουν την αξία τους μέσω ενός ελεγχόμενου μηχανισμού προσφοράς. Η ιδέα αυτής της έννοιας (που αναπτύχθηκε κυρίως από τον Robert Sams, 2014) είναι ο έλεγχος της νομισματικής προσφοράς και συνεπώς της τιμής διαπραγμάτευσης με τη σύναψη ενός έξυπνου συμβολαίου που παίζει το ρόλο της κεντρικής τράπεζας. Η νομισματική πολιτική εδώ, έχει μόνο ένα στόχο: να εκδόσει νομίσματα που θα διατηρήσουν την τιμή τους. Με άλλα λόγια, το δίκτυο καίει τα νομίσματα όταν η τιμή του stablecoin είναι πολύ χαμηλή και εκδίδει νέα νομίσματα όταν η τιμή του stablecoin είναι πολύ υψηλή. Αυτή η λειτουργία υποστηρίζεται από έναν αλγόριθμο και δεν υπάρχει ανάγκη για οποιαδήποτε εγγύηση. Στην πραγματικότητα, ο αλγόριθμος λειτουργεί ως κεντρική τράπεζα, αλλά με αποκεντρωμένο τρόπο, αφού στο παραδοσιακό σύστημα οι κεντρικές τράπεζες διατηρούν γενικά τη σταθερότητα των τιμών των συμβατικών νομισμάτων με παρόμοιους μηχανισμούς.

Πίνακας 1: Παρατίθενται παραδείγματα σταθερών νομισμάτων κάθε κατηγορίας

Fiat-collateralized stablecoins	*Crypto-collateralized stablecoins*	*Non-collateralized stablecoins*
• TrustToken • Tehter • Paxos • Digix • Gemini • Stably • Circle	• MakerDAO • Havven • Augmint • Sweetbridge	• Basis • Carbon • Kowala • Fragments

Σημείωση: πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

3.5 Μέθοδοι άντλησης κεφαλαίων στην κρυπτοοικονομία-Οι αρχικές προσφορές νομισμάτων (ICOs)

3.5.1. Εισαγωγή στην έννοια των ICOs.

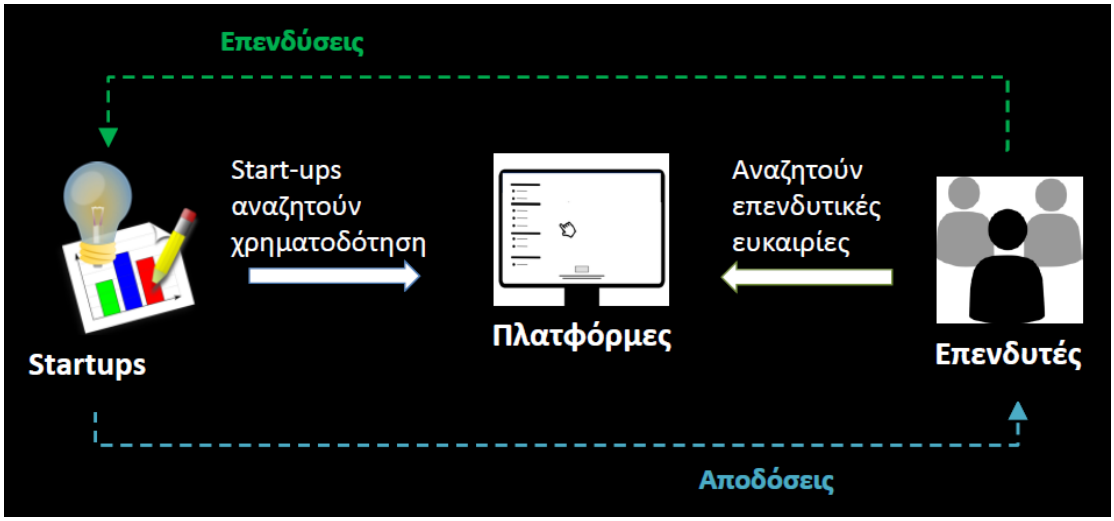
Οι αρχικές προσφορές νομισμάτων (ICOs) είναι ένας νέος και καινοτόμος τρόπος άντλησης κεφαλαίων ο οποίος βασίζεται στην τεχνολογία του blockchain. Οι ICO πραγματοποιούνται συνήθως στα αρχικά στάδια ενός έργου και στόχος τους είναι να συγκεντρώσουν κεφάλαια που θα καλύψουν τα λειτουργικά έξοδα από την έναρξη ενός έργου έως την υλοποίησή του. Η εταιρεία που διεξάγει μία αρχική προσφορά νομισμάτων, δημιουργεί tokens (ψηφιακά τσιπ) που στη συνέχεια πωλούνται απευθείας στο κοινό. Τα νεοεκδοθέντα token δεν μπορούν να αγοραστούν απευθείας

με συμβατικά νομίσματα (δηλαδή λίρες, ευρώ, κ.λπ.), και όσοι ενδιαφέρονται να αγοράσουν tokens χρησιμοποιούν τα κύρια κρυπτονομίσματα (δηλαδή Bitcoin, Ethereum). Έτσι, αν κάποιος ενδιαφερόμενος θέλει να αγοράσει 100 νέα tokens (έστω ΑΒΓΔ), πρέπει πρώτα να αγοράσει την αντίστοιχη αξία σε Ethereum και στη συνέχεια να ανταλλάξει το Ethereum του με τα ΑΒΓΔ tokens.

Οι ICO επιτρέπουν σε αυτούς που αναζητούν κεφάλαια να τα αντλούν απευθείας από το κοινό, σε παγκόσμια κλίμακα, χωρίς κόστος συναλλαγής και ακολουθώντας μια σχετικά εύκολη διαδικασία. Αυτά τα χαρακτηριστικά των ICO έχουν οδηγήσει σε εξαιρετικά γρήγορη και μεγάλης αξίας συγκέντρωση χρημάτων, όπου μπορούν να συγκεντρωθούν εκατομμύρια δολάρια μέσα σε λίγες ώρες. Μια ICO περιλαμβάνει τρία μέρη (Σχήμα 10): (i) νεοσύστατες επιχειρήσεις/έργα που χρησιμοποιούν την τεχνολογία blockchain, (ii) υποψήφιους επενδυτές και (iii) πάροχους ICO, οι οποίοι είναι κεντρικές πλατφόρμες στις οποίες πραγματοποιούνται οι ICO. Συγκρίνοντας αυτή τη διαδικασία με την αντίστοιχη διαδικασία των αρχικών δημόσιων προσφορών (IPOs)[14] στις πρωτογενείς κεφαλαιαγορές, και τα δύο άκρα (έργα και επενδυτές) είναι τα ίδια, και η ουσιαστική διαφορά είναι ότι ο διαμεσολαβητής συγκέντρωσης κεφαλαίων δεν είναι μια επενδυτική τράπεζα αλλά μια διαδικτυακή πλατφόρμα, η οποία κάνει χρήση της τεχνολογίας blockchain για την ολοκλήρωση της διαδικασίας συγκέντρωσης κεφαλαίων.

Από τις πιο διαδεδομένες και επιτυχημένες πλατφόρμες διεξαγωγής ICO είναι το αποκεντρωμένο δίκτυο του Ethereum. Αυτό το δίκτυο προσφέρει χρήση των smart contracts, τα οποία αναλύθηκαν παραπάνω, και προσφέρουν στους προγραμματιστές των έργων την δυνατότητα να δημιουργήσουν ορισμένα πρωτόκολλα υπολογιστή που εκτελούν, επιβάλλουν και επαληθεύουν την εκτέλεση των όρων μιας σύμβασης.

Σχήμα 10: Οι κύριοι συμμετέχοντες σε μια ICO



Σημείωση: πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

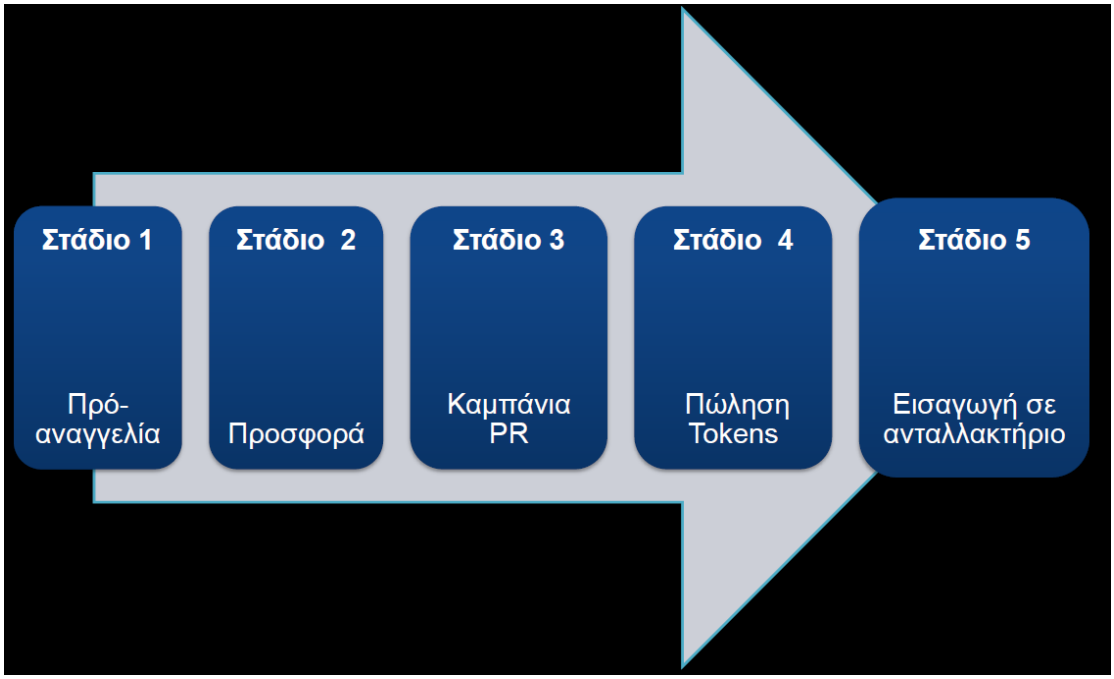
[14] Η αρχική δημόσια προσφορά (IPO) αναφέρεται στη διαδικασία προσφοράς μετοχών μιας ιδιωτικής εταιρείας στο κοινό μέσω της έκδοσης νέων μετοχών. Αυτή η διαδικασία επιτρέπει σε μια εταιρεία να αντλήσει μετοχικό κεφάλαιο από δημόσιους επενδυτές.

Οι επενδυτές προσελκύονται κυρίως από την προσδοκία της μελλοντικής επιτυχίας του έργου. Όταν επενδύουν, στοχεύουν κυρίως σε κεφαλαιακά κέρδη, αναμένοντας ότι η τιμή των tokens θα αυξηθεί. Λαμβάνοντας υπόψη ότι η μόνη πρόσβαση στην υπηρεσία/προϊόν που δημιουργεί το έργο είναι μέσω της κατοχής των tokens του έργου και ότι η προσφορά τους είναι συνήθως ένας προκαθορισμένος αριθμός, εάν το έργο είναι επιτυχές, η ζήτηση των tokens αναμένεται να αυξηθεί και επομένως θα αυξηθεί και η τιμή τους.

3.5.2. Πώς λειτουργούν οι ICOs.

Με βάση το γεγονός ότι οι ICOs αποτελούν ένα σχετικά πρόσφατο φαινόμενο, υπάρχουν συχνές και ουσιώδεις διαφορές κατά περίπτωση στον τρόπο διεξαγωγής τους και δεν υπάρχει κάποια σταθερή διαδικασία που να ακολουθείται παγκοσμίως. Ωστόσο, υπάρχουν συγκεκριμένα βήματα που φαίνεται να ακολουθεί η πλειοψηφία των ICO που διεξάγονται, (Σχήμα 11).

Σχήμα 11: Κύρια στάδια σε μια ICO



Σημείωση: πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

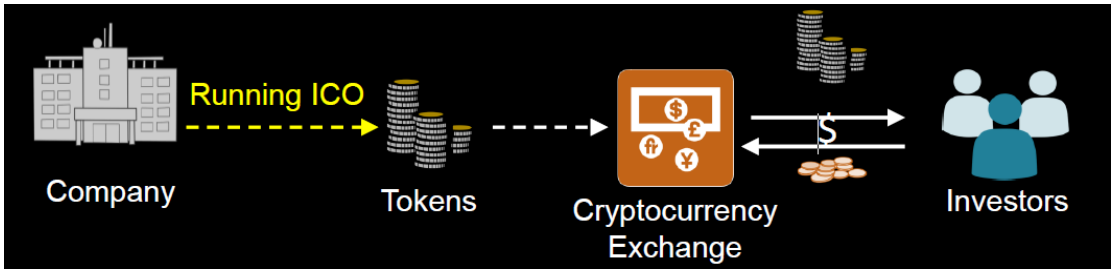
Το πρώτο στάδιο είναι αυτό της προ-αναγγελίας, το οποίο έχει ως βασικό στόχο την ενημέρωση του ευρύτερου κοινού σχετικά με το έργο. Αυτό επιτυγχάνεται συνήθως μέσω ανακοινώσεων σε ιστοσελίδες και διαδικτυακά forums, που σχετίζονται με την τεχνολογία του blockchain και την αγορά των κρυπτονομισμάτων, όπως για παράδειγμα το Reddit και το Twitter. Μέσα στην προαναγγελία περιέχεται μία σύντομη επισκόπηση του έργου, αναφορικά με την ιδέα, τον σκοπό και τα βήματα της υλοποίησης του καθώς και πληροφορίες για τα άτομα που απαρτίζουν την ομάδα που ευθύνεται για το project αυτό. Με βάση αυτές τις αρχικές πληροφορίες, το κοινό αρχίζει να παρέχει ανατροφοδότηση στην ομάδα. Αυτή η διαδικασία είναι πολύ σημαντική κατά την διεξαγωγή των αρχικών βημάτων, αρχικά επειδή δείχνει την

αντίδραση του κοινού στην ιδέα, άρα συνεπώς και στο ίδιο το έργο, και επίσης επειδή τα σχόλια του κοινού βοηθούν την ομάδα να βελτιώσει το έργο της πριν την έναρξη του επόμενου σταδίου, δηλαδή της προσφοράς. Η προσφορά είναι η τελική έκδοση του έργου, η οποία παρουσιάζεται και προσφέρεται στο κοινό. Βασικό στοιχείο της προσφοράς αποτελεί το whitepaper. Το whitepaper αποτελεί ένα υπόμνημα/σημείωμα κατανόησης του έργου, το οποίο περιέχει με κάθε λεπτομέρεια το έργο. Η συνήθης δομή του whitepaper περιλαμβάνει μια περίληψη των κυριότερων σημείων του έργου, το κίνητρο, την κύρια ιδέα, πληροφορίες που έχουν να κάνουν με την εμπορευσιμότητα του έργου, πληροφορίες που απευθύνονται στους επενδυτές όπως σχέδια διανομής των tokens, πληροφορίες σχετικά με την ομάδα και τους συμβούλους και τέλος ένα σχέδιο της υλοποίησης του έργου. Άλλο ένα αξιοσημείωτο μέρος του σταδίου της προσφοράς είναι η παρουσίαση όλων των τεχνικών χαρακτηριστικών του έργου, παρέχοντας δωρεάν για όλους τον υπολογιστικό κώδικα της σχεδιασθείσας εφαρμογής, ώστε να δώσει την δυνατότητα σε ειδικούς να ελέγξουν για τυχόν λάθη ή κενά στον κώδικα.

Μόλις η προσφορά δημοσιοποιηθεί, η ομάδα επικεντρώνεται στην εκστρατεία των δημοσίων σχέσεων της. Από την στιγμή όπου τα ICOs έχουν ως στόχο ευρύ κοινό, η διάδοση των πληροφοριών αποτελεί ζωτικής σημασίας ρόλο καθ' όλη την διάρκεια της διαδικασίας μιας ICO. Για την ακρίβεια, οι δημόσιες σχέσεις και οι στρατηγικές για τις εκστρατείες αποτελούν παράγοντες κλειδιά για την επιτυχία της ICO. Ακόμα και από το πρώτο στάδιο της προαναγγελίας, οι ιδιοκτήτες των έργων πρέπει να βεβαιωθούν πως χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης όσο πιο αποτελεσματικά γίνεται με σκοπό να παρακολουθούν και να ελέγχουν τις ροές πληροφοριών προς το κοινό και να χρησιμοποιούν τα σχόλια που λαμβάνουν. Ειδικά, μετά τη δημοσιοποίηση της προσφοράς, η καμπάνια των δημοσίων σχέσεων αναλαμβάνει κεντρικό ρόλο στην διαδικασία της ICO. Οι ιδιοκτήτες των έργων προσλαμβάνουν συνήθως ειδικούς επικοινωνίας οι οποίοι διαφημίζουν την επερχόμενη ICO, μέσω ομιλιών σε συνέδρια και διαδικτυακές παρουσιάσεις με σκοπό την προσέλκυση επενδυτών. Μέρος της καμπάνιας είναι η χρήση συγκεκριμένων στρατηγικών μάρκετινγκ, από τις οποίες μία από τις δημοφιλέστερες είναι τα λεγόμενα AirDrops. Τα AirDrops είναι ουσιαστικά δωρεάν tokens τα οποία μοιράζονται από αυτούς που αναπτύσσουν το έργο σε ηλεκτρονικά πορτοφόλια του κοινού.

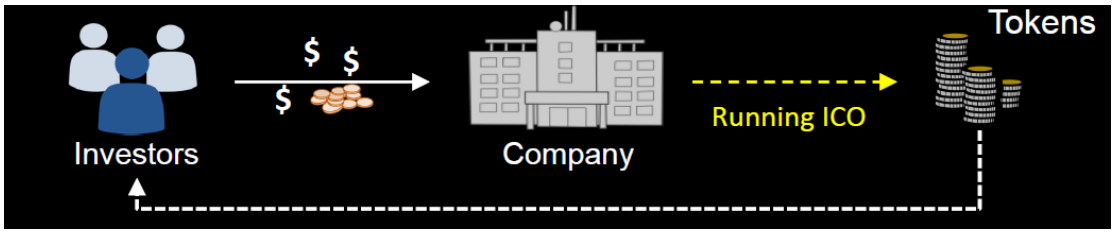
Το επόμενο στάδιο είναι η πώληση των tokens. Υπάρχουν δύο διαφορετικές προσεγγίσεις για το πως μπορούν να διεξαχθούν αυτές οι πωλήσεις. Στην πρώτη περίπτωση, (Σχήμα 12), οι ιδιοκτήτες του έργου απελευθερώνουν τα tokens στην αγορά σε μία συγκεκριμένη ημερομηνία και οι επενδυτές έχουν την δυνατότητα να τα αγοράσουν ανταλλάσσοντας τα κύρια κρυπτονομίσματα τους, όπως Bitcoin ή Ethereum, με τον αντίστοιχο αριθμό tokens βασισμένοι στην σχετική τιμή των token με το βασικό κρυπτονόμισμα. Στην δεύτερη περίπτωση, (Σχήμα 13), οι ιδιοκτήτες του έργου χρηματοδοτούνται πρώτα από τους επενδυτές οι οποίοι λαμβάνουν τα tokens τους αργότερα, αφού το έργο έχει ήδη αναπτυχθεί μέχρι ένα ορισμένο σημείο.

Σχήμα 12: Άντληση κεφαλαίων παράλληλα με τον απελευθέρωση των tokens



Σημείωση: πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

Σχήμα 13: Άντληση κεφαλαίων πριν την απελευθέρωση των tokens



Σημείωση: πηγή: An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Daskalakis and Georgitseas (2020)

Η πώληση tokens αποτελεί ένα ευαίσθητο στάδιο στην όλη διαδικασία, από την στιγμή που πρόκειται για το βασικό βήμα στην άντληση κεφαλαίων. Πολλές ICOs χρησιμοποιούν υπηρεσίες μεσεγγύησης ή ακόμα τους στόχους που βασίζονται σε μεσεγγύηση, με σκοπό την αύξηση της εμπιστοσύνης και της διαφάνειας. Η μεσεγγύηση αποτελεί μία χρηματοοικονομική συμφωνία η οποία περιλαμβάνει ένα τρίτο πρόσωπο το οποίο είναι υπεύθυνο για τις πληρωμές, τις συναλλαγές και την ρύθμιση της εκταμίευσης των κεφαλαίων. Αυτά τα τρίτα μέρη συλλέγουν και αποθηκεύουν τα κεφάλαια που συγκεντρώθηκαν από τους επενδυτές σε ένα λογαριασμό μεσεγγύησης και στη συνέχεια εκταμιεύουν αυτά τα κεφάλαια στον εκδότη αμέσως αφού εκπληρωθεί ένα σύνολο προσυμφωνημένων όρων, οι οποίοι είναι γνωστοί στους επενδυτές. Αυτή η διαδικασία αυξάνει την εμπιστοσύνη μεταξύ της ομάδας του έργου και των χρηματοδοτών, αυξάνοντας έτσι και την πιθανότητα επιτυχίας της ICO. Οι στόχοι/επιτεύγματα που βασίζονται στη μεσεγγύηση σημαίνουν πως η ομάδα του έργου δεν αποκτά πρόσβαση σε όλο το κεφάλαιο που συγκεντρώθηκε μονομιάς, αλλά αυτά τα κεφάλαια αποδεσμεύονται τμηματικά και σύμφωνα με συγκεκριμένα ορόσημα που ορίσει οι ίδιοι οι εκδότες. Αυτή η διαδικασία αυξάνει περαιτέρω την εμπιστοσύνη από την στιγμή που οι επενδυτές βλέπουν τα ορόσημα που βασίζονται σε μεσεγγύηση ως ένα τρόπο για την αύξηση της παραγωγικότητας και της εκπλήρωσης των στόχων που περιγράφονται στο whitepaper διότι, η ομάδα του έργου μπορεί να αποκτήσει πρόσβαση στα κεφάλαια που συγκεντρώθηκαν μόνο όταν επιτευχθούν αυτά τα ορόσημα.

Το τελευταίο βήμα είναι η καταχώρηση του νεοεκδοθέντος κέρματος σε ένα ανταλλακτήριο. Υπάρχουν σχεδόν 600[15] ανταλλακτήρια παγκοσμίως μέχρι και τις μέρες μας (Φεβρουάριος 2023), με ποικίλες χρεώσεις καταχώρισης και προϋποθέσεις.

[15] https://www.forbes.com/advisor/investing/cryptocurrency/best-crypto-exchanges/

Η καταχώρηση ενός νέου νομίσματος σε ένα ανταλλακτήριο προϋποθέτει την συμπλήρωση μιας εκτενούς φόρμας καταχώρησης, με πληροφορίες σχετικά με το έργο και την ομάδα, καθώς και τεχνικές λεπτομέρειες σχετικά με το κέρμα/token. Τα κορυφαία ανταλλακτήρια απαιτούν νομική μορφή (δηλαδή, ο εκδότης πρέπει να είναι νομική οντότητα) επιπλέον μίας επιστολής νομικής γνώμης γραμμένη από δικηγορικό γραφείο, η οποία περιγράφει τα νομικά χαρακτηριστικά του νομίσματος, εστιάζοντας κυρίως στο εάν το νόμισμα ελέγχεται από μία αρχή και εάν ισχύει η αδειοδότηση. Ορισμένα ανταλλακτήρια επίσης ζητούν έλεγχο ασφαλείας από έξυπνο συμβόλαιο, το οποίο μπορεί να διαρκέσει μέχρι και μήνα. Μόλις η αίτηση και όλα τα απαιτούμενα έγγραφα είναι έτοιμα, χρειάζονται μερικές εβδομάδες μέχρι το ανταλλακτήριο να ελέξει τα έγγραφα και να καταχωρήσει το token.

Κεφάλαιο 4: Αποκεντρωμένη Χρηματοοικονομική-Μελέτες Περίπτωσης

4.1 Ορισμός και εισαγωγή στην έννοια της Αποκεντρωμένης Χρηματοοικονομικής

Σύμφωνα με τον Schär[16] (2021), ως αποκεντρωμένη χρηματοοικονομική (Decentralized Finance ή απλώς DeFi), ορίζουμε το χρηματοοικονομικό οικοσύστημα το οποίο βασίζεται στην τεχνολογία του blockchain. Κύρια γνωρίσματα αυτού του όρου αποτελούν η εύκολη και ελεύθερη πρόσβαση σε αυτή καθώς και η διαλειτουργική δομή της, η οποία έχει ως βάση δημόσιες πλατφόρμες έξυπνων συμβολαίων όπως για παράδειγμα αυτή του Ethereum. Έχει την ικανότητα να παράγει το ίδιο αποτέλεσμα με τις υπάρχουσες χρηματοοικονομικές υπηρεσίες συνεισφέροντας παράλληλα στην καλύτερη προσβασιμότητα και διαφάνεια της όλης διαδικασίας. Έχει αντικαταστήσει τους διαμεσολαβητές και τα κεντροποιημένα ιδρύματα με ανοιχτά πρωτόκολλα και αποκεντρωμένες εφαρμογές. Παραδείγματα τέτοιων εφαρμογών αποτελούν τα αποκεντρωμένα ανταλλακτήρια (DEXs), όπως το Uniswap, οι πλατφόρμες δανεισμού με στρατηγικές μεγιστοποίησης απόδοσης, όπως το Compound, οι πλατφόρμες προβλέψεων/στοιχηματισμού γεγονότων όπως το Gnosis και τέλος εφαρμογές δημιουργίας και ανταλλαγής παραγώγων νομισμάτων, πολύτιμων μετάλλων και άλλων πραγματικών περιουσιακών στοιχείων όπως το Synthetix. Όλες οι συμφωνίες τηρούνται βάση κώδικα, οι συναλλαγές εκτελούνται με ασφαλέστερους και πιο αποδεδειγμένους τρόπους σε σχέση με το παραδοσιακό σύστημα και όλες οι αλλαγές καταγράφονται στο blockchain, το οποίο όντας δημόσιο είναι προσβάσιμο από όλους. Έτσι χάρη στην αρχιτεκτονική της, η αποκεντρωμένη χρηματοοικονομική έχει προοπτικές να αποτελέσει ένα χρηματοοικονομικό σύστημα υψηλών προδιαγραφών και πρωτοποριακών χαρακτηριστικών όπως η διαφάνεια και η αξιοπιστία, χωρίς την

[16] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571335

εποπτεία και την εξάρτηση από τρίτους αφού τους αντίστοιχους ρόλους, μπορούν να αναλάβουν και να υπερκαλύψουν τα smart contracts.

4.2 Διαφορές Αποκεντρωμένης Χρηματοοικονομικής και Κλασσικής Χρηματοοικονομικής

Σύμφωνα με τους (Qin et al., 2021)[17] η αποκεντρωμένη χρηματοοικονομική προσφέρει μία σειρά από αποκλειστικά χαρακτηριστικά τα οποία δεν απαντώνται στο κλασσικό κεντροποιημένο χρηματοοικονομικό σύστημα. Συγκεκριμένα:

Ι) Διαφάνεια. Στην αποκεντρωμένη χρηματοοικονομική δίνεται η δυνατότητα σε όλους τους χρήστες να ελέγχουν τους ακριβείς κανόνες οι οποίοι καθορίζουν πώς λειτουργούν τα χρηματοοικονομικά περιουσιακά στοιχεία και τα προϊόντα. Το μέτρο διαφάνειας της κλασικής χρηματοοικονομικής περιορίζεται αρκετά από μία σειρά παραγόντων όπως: οι ιδιωτικές συμφωνίες, οι αποχωρήσεις από συμφωνίες που έχουν ήδη κανονιστεί καθώς και το χαρακτηριστικό της κεντροποίησης. Η αποκεντρωμένη χρηματοοικονομική, επιχειρεί ενεργά την αποφυγή αυτών των καταστάσεων.

ΙΙ) Έλεγχος. Η αποκεντρωμένη χρηματοοικονομική προσδίδει το χαρακτηριστικό του ελέγχου στους χρήστες της, μέσω της δυνατότητας που τους παρέχει να διατηρούν την κυριότητα των περιουσιακών τους στοιχείων. Δηλαδή, για παράδειγμα, η λογοκρισία, η μετακίνηση ή η καταστροφή των περιουσιακών στοιχείων ενός χρήστη, δεν μπορούν να γίνουν, χωρίς την σύμφωνη γνώμη του.

ΙΙΙ) Προσβασιμότητα. Η αποκεντρωμένη χρηματοοικονομική προσφέρει την δυνατότητα σε όλους όσους διαθέτουν τα ελαχίστως απαραίτητα, όπως ένα μέτριο υπολογιστή, διαδικτυακή σύνδεση και γνώση πάνω στο αντικείμενο, να δημιουργήσουν και να παράξουν προϊόντα DeFi. Ταυτόχρονα, το blockchain και το διαμοιρασμένο του δίκτυο από χρήστες (miners) αναλαμβάνει την λειτουργία της εκάστοτε εφαρμογής αποκεντρωμένης χρηματοοικονομικής.

Επίσης, σύμφωνα με τους (Makarov and Schoar, 2022)[18], διαφορές μεταξύ της παραδοσιακής και της αποκεντρωμένης χρηματοοικονομικής εντοπίζονται και σε τομείς, όπως στο κόστος των συναλλαγών, στην διακυβέρνηση καθώς και στον συστημικό κίνδυνο.

Αρχικά, όσον αφορά το κόστος των συναλλαγών, το παραδοσιακό σύστημα εμφανίζει, όπως αναλύθηκε και στο 1ο κεφάλαιο μία σειρά από χαρακτηριστικά που το καθιστούν αναποτελεσματικό σε πολλές περιπτώσεις. Αποτέλεσμα αυτών, μεταξύ άλλων αποτελούν το υψηλό κόστος για τραπεζικές υπηρεσίες και η απαίτηση σχετικά μεγάλου χρονικού διαστήματος για την ολοκλήρωση των συναλλαγών. Ένα ουσιώδες μέρος από τα κόστη αυτά, πηγάζει από την ανάγκη της κάλυψης των λειτουργικών εξόδων των φυσικών καταστημάτων των παραδοσιακών τραπεζών και της ξεπερασμένης πλέον δομής τους. Η αποκεντρωμένη χρηματοοικονομική μειώνει δραστικά, ουσιαστικά εξαλείφει την ανάγκη ύπαρξης φυσικών καταστημάτων, έχοντας

[17] https://arxiv.org/pdf/2106.08157.pdf
[18] https://www.nber.org/papers/w30006

έτσι μία πιο αποδοτική αρχιτεκτονική δομή, με αποτέλεσμα μειωμένα κόστη συναλλαγών καθώς και την πιο σύντομη περάτωση τους σε σχέση με το παραδοσιακό σύστημα.

Η διακυβέρνηση στην κλασική χρηματοοικονομική αποτελεί έναν τομέα με συχνές αναταραχές και διαφωνίες, όπου για την επίλυση τους συχνά χρειαζόταν να συνδράμει το νομικό σύστημα το οποίο βοηθούσε με αυτόν τον τρόπο στην εύρυθμη λειτουργία του χρηματοοικονομικού συστήματος. Η αποκεντρωμένη χρηματοοικονομική αντιμετωπίζει τα προβλήματα διακυβέρνησης, και μάλιστα χωρίς την ανάγκη συνδρομής ενός ενδιάμεσου φορέα, εισάγοντας μία νέα μορφή διακυβέρνησης η οποία ονομάζεται Αποκεντρωμένος Αυτόνομος Οργανισμός (Decentralized Autonomous Organization ή DAO)[19]. Η βασική ιδέα του DAO είναι ο διαμοιρασμός του ελέγχου σχετικά με την λήψη των αποφάσεων σε όλους τους ενδιαφερόμενους/συμμετέχοντες. Αυτό γίνεται μέσω της ειδικών tokens τα οποία δίνουν την δυνατότητα σε αυτούς που τα κατέχουν, να προτείνουν αλλαγές στο πρωτόκολλο και να μπορούν να τις ψηφίζουν. Όλη αυτή η διαδικασία διέπεται από έξυπνα συμβόλαια και καταγράφεται στο blockchain.

Τέλος, όσον αφορά τον συστημικό κίνδυνο, ένας από τους κύριους λόγους ύπαρξης του στην παραδοσιακή χρηματοοικονομική είναι η ευρεία χρήση του συστήματος των κλασματικών αποθεμάτων, κατά το οποίο η εκάστοτε τράπεζα διατηρεί μόνο ένα κομμάτι από τις καταθέσεις ενός πελάτη ενώ το υπόλοιπο προσφέρεται ως δάνειο σε άλλους πελάτες. Αυτή η μέθοδος έχει ως πιθανό ρίσκο να θέσει σε κίνδυνο το τραπεζικό σύστημα σε περίπτωση επιβολής δεσμεύσεων και περιορισμών καθώς και στην περίπτωση όπου η εκάστοτε τράπεζα χάσει την εμπιστοσύνη των πελατών της, οι οποίοι θεωρώντας την πλέον αναξιόπιστη προχωρήσουν σε απόσυρση των καταθέσεων τους. Η αποκεντρωμένη χρηματοοικονομική λειτουργεί με βάση ένα μοντέλο ‘‘στενής’’ τραπεζικής, όπου κάθε δάνειο είναι υπερ-εξασφαλισμένο, μειώνοντας έτσι τον συνολικό κίνδυνο του συστήματος.

4.3 Η αρχιτεκτονική πυλώνων των εφαρμογών-συστημάτων της Αποκεντρωμένης Χρηματοοικονομικής

Σύμφωνα με τον Schär[20] (2021), η αρχιτεκτονική της Αποκεντρωμένης Χρηματοοικονομικής αποτελείται από ένα σύνολο πυλώνων (layers). Κάθε πυλώνας έχει ένα συγκεκριμένο σκοπό. Κάθε πυλώνας βασίζεται σε έναν άλλο και ακολουθούν ιεραρχική δομή. Έτσι, δημιουργούν μία ανοιχτή και προσβάσιμη υποδομή η οποία επιτρέπει σε όλους τους ενδιαφερόμενους να χτίσουν πάνω σε αυτή ή να χρησιμοποιήσουν επιμέρους κομμάτια της. Η ιεραρχική δομή, αποτελεί κρίσιμης σημασίας καθώς υποδηλώνει πως η ασφάλεια του κάθε πυλώνα εξαρτάται άμεσα από τον προηγούμενο. Δηλαδή, για παράδειγμα, εάν παραβιαστεί το blockchain που βρίσκεται στον 1ο πυλώνα, ο οποίος και αποτελεί την βάση όλης της αρχιτεκτονικής,

[19] https://ethereum.org/en/dao/

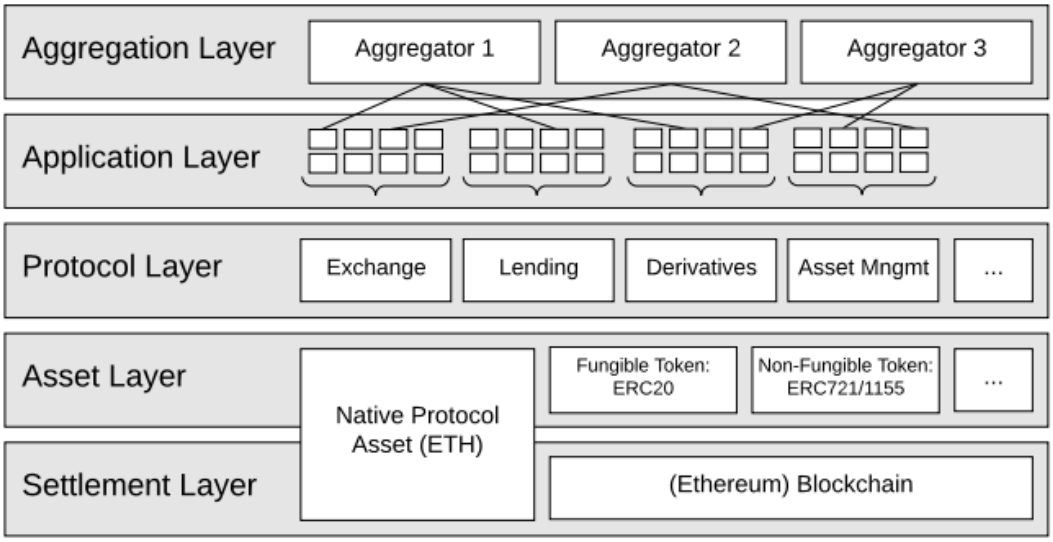
[20] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571335

τότε και όλοι οι υπόλοιποι πυλώνες θα βρίσκονται σε κίνδυνο και δεν θα είναι ασφαλείς.

Παρακάτω παρουσιάζεται η αρχιτεκτονική των συστημάτων DeFi, η οποία αποτελείται από 5 πυλώνες στο σύνολο της.

I) Πυλώνας 1 (Layer 1 ή settlement layer), ο οποίος αποτελείται από το εκάστοτε blockchain και το αντίστοιχο στοιχείο του πρωτοκόλλου του, δηλαδή το blockchain του Bitcoin και το Bitcoin [BTC] καθώς και το blockchain του Ethereum και το ETH. Δίνει την δυνατότητα στο δίκτυο να αποθηκεύσει με ασφάλεια, πληροφορίες σχετικά με ιδιοκτησία και διαβεβαιώνει πως οποιαδήποτε αλλαγή συμβεί, αυτή είναι σύμφωνη με τους κανόνες. Το blockchain αποτελεί την βάση για την αυτόματη εκτέλεση εντολών χωρίς την ανάγκη εμπιστοσύνης και λειτουργεί ως ο πυλώνας για την διευθέτηση και την επίλυση διαφορών που ενδέχεται να προκύψουν.
II) Πυλώνας 2 (Layer 2 ή asset layer), στον οποίο εμπεριέχονται όλα τα στοιχεία τα οποία εκδίδονται πάνω από τον πυλώνα 1, δηλαδή εκτός από τα στοιχεία πρωτοκόλλου του εκάστοτε blockchain που αναφέραμε πριν, (BTC και ETH), αλλά και τα επιπρόσθετα στοιχεία που εκδίδονται σε αυτό το blockchain, τα οποία συχνά αναφέρονται ως, τα γνωστά σε όλους μας, tokens.
III) Πυλώνας 3 (Layer 3 ή protocol layer), ο οποίος παρέχει τα βασικά για μία πληθώρα περιπτώσεων, όπως αποκεντρωμένα ανταλλακτήρια, αγορές ομολόγων, παράγωγα και διαχείριση στοιχείων εντός της αλυσίδας. Αυτά τα βασικά πρότυπα, συνήθως εφαρμόζονται σε ένα σετ από έξυπνα συμβόλαια, στα οποία έχουν πρόσβαση όλοι οι χρήστες και όλες οι DeFi εφαρμογές, έτσι τα πρωτόκολλα αυτά χαρακτηρίζονται από μεγάλη διαλειτουργικότητα.
IV) Πυλώνας 4 (Layer 4 ή application layer), ο οποίος δημιουργεί εφαρμογές για χρήστες, οι οποίες συνδέονται σε επιμέρους πρωτόκολλα. Για την αλληλεπίδραση με τα smart contracts συνήθως χρησιμοποιείται μία ιστοσελίδα, η οποία διευκολύνει την χρήση των πρωτοκόλλων.
V) Πυλώνας 5 (Layer 5 ή aggregation layer), ο οποίος πρόκειται για μία επέκταση του πυλώνα 4. Οι συσσωρευτές, πρόκεινται για ιστοσελίδες ή προγράμματα που δημιουργούν πλατφόρμες σχεδιασμένες για χρήστες οι οποίες συνδέονται σε διάφορες εφαρμογές και πρωτόκολλα. Οι συσσωρευτές συνήθως, παρέχουν εργαλεία για την σύγκριση και την αξιολόγηση υπηρεσιών, επιτρέπουν στους χρήστες να εκτελέσουν διεργασίες οι οποίες σε άλλες περιπτώσεις θα ήταν αρκετά περίπλοκες, μέσω της σύνδεσης με πολλά πρωτόκολλα ταυτόχρονα και συνδυάζοντας σχετικές πληροφορίες με τρόπο σαφή και περιεκτικό.

Σχήμα 14: Η αρχιτεκτονική των DeFi συστημάτων



Σημείωση: Πηγή: Schär Fabian (2021), Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets.

4.4 Μελέτη περίπτωσης Uniswap (Αποκεντρωμένο Ανταλλακτήριο)

4.4.1 Εισαγωγή στην έννοια των Αποκεντρωμένων Ανταλλακτηρίων (Decentralized Exchanges ή DEXs)

Πριν προχωρήσουμε στην μελέτη περίπτωσης του Uniswap, πρέπει πρώτα να εισάγουμε την έννοια και τα βασικά χαρακτηριστικά των Αποκεντρωμένων Ανταλλακτηρίων (DEXs). Τα DEXs αποτελούν ουσιαστικά μία κατηγορία από αποκεντρωμένες εφαρμογές οι οποίες επιτρέπουν τις ανταλλαγές κρυπτονομισμάτων μεταξύ χρηστών peer-to-peer, χωρίς την ανάγκη για μεσολάβηση τρίτου. Στην περίπτωση των DEXs, τα smart contracts είναι αυτά που αναλαμβάνουν τον ρόλο του διαμεσολαβητή και επιτρέπουν στους χρήστες να εκτελούν ανταλλαγές κρυπτονομισμάτων απευθείας από τα ηλεκτρονικά τους πορτοφόλια (e-wallets), σε αντίθεση με τα παραδοσιακά κεντροποιημένα ανταλλακτήρια, όπου το ίδιο το ανταλλακτήριο έχει πρόσβαση στα e-wallets των χρηστών.

Η διαδικασία λειτουργίας των DEXs μπορεί να συνοψιστεί ως εξής:

1. Για την χρήση ενός DEX, ένας χρήστης πρέπει αρχικά, να διαθέτει ένα συμβατό e-wallet (π.χ. το MetaMask). Με τον όρο συμβατό εννοούμε πως μέσω ενός smart contract το εκάστοτε DEX έχει την δυνατότητα να "διαβάζει'' τα περιεχόμενα του πορτοφολιού και πραγματοποιεί συναλλαγές με βάση τους περιορισμούς (π.χ. όρια ποσού) που έχει θέσει ο χρήστης.
2. Έπειτα ο χρήστης επιλέγει το ζεύγος συναλλαγής (π.χ. BTC/ETH) και στη συνέχεια ορίζει το αντίστοιχο ποσό πώλησης/αγοράς.

3. Το DEX από την πλευρά του, προσφέρει ένα εκτιμώμενο ποσό για το σε ποια τιμή θα αγοράσει, ενώ ταυτόχρονα δίνεται η δυνατότητα και στους χρήστες να ορίσουν τις δικές τους επιθυμητές τιμές.
4. Τέλος, όταν ο χρήστης αποδεχθεί τους προσφερόμενους όρους, η συναλλαγή πραγματοποιείται στο blockchain (Layer 1)

4.4.2 Η περίπτωση του Uniswap

4.4.2.1 Τί είναι το Uniswap; Ορισμός και ανάλυση των πτυχών του

Αρχικά, με σκοπό την καλύτερη κατανόηση του, πρέπει να επεξηγήσουμε τις διάφορες πτυχές του Uniswap. Το Uniswap αναλύεται στις επιμέρους 4 υποκατηγορίες.

- **Uniswap Labs**: Πρόκειται για την εταιρία η οποία ανέπτυξε το πρωτόκολλο Uniswap (Uniswap protocol), μαζί με την ιστοσελίδα.
- **Το Uniswap Protocol**: Ένα σύνολο από μη αναβαθμίσιμα smart contracts τα οποία δημιουργούν μαζί έναν αυτοματοποιημένο διαπραγματευτή αγοράς (Automated Market Maker ή AMM), ο οποίος αποτελεί ένα σύνολο από αλγοριθμικούς παράγοντες που παρέχουν ρευστότητα στις αγορές, μέσω διατήρησης αποθεμάτων ενός ζεύγους token. Στην περίπτωση του Uniswap, υπάρχει peer-to-peer ανταλλαγή ERC-20[21] tokens στο Ethereum blockchain.
- **Το Uniswap Interface**: Μία διεπαφή ιστοσελίδας η οποία επιτρέπει την εύκολη αλληλεπίδραση με το πρωτόκολλο του Uniswap. Η διεπαφή αυτή αποτελεί μόνο έναν από τους πολλούς τρόπους με τους οποίους ένας χρήστης μπορεί να αλληλοεπιδράσει με το πρωτόκολλο του Uniswap.
- **Το Uniswap Governance**: Ένα σύστημα διακυβέρνησης για την διακυβέρνηση του Uniswap πρωτοκόλλου, το οποίο καθίσταται εφικτό με την βοήθεια του UNI token.

4.4.2.2. Το πρωτόκολλο του Uniswap

Το πρωτόκολλο του Uniswap είναι ένα peer-to-peer σύστημα το οποίο σχεδιάστηκε για την ανταλλαγή κρυπτονομισμάτων (ERC-20 Tokens), πάνω στο Ethereum blockchain. Το πρωτόκολλο εφαρμόζεται ως ένα σύνολο από μη αναβαθμιζόμενα smart contracts, το οποίο είναι σχεδιασμένο να δίνει προτεραιότητα στην ασφάλεια, στην αυτοεπιμέλεια, στην αντίσταση κατά της λογοκρισίας και στην λειτουργία του χωρίς την ύπαρξη εμπιστεύσιμων ενδιάμεσων οι οποίοι ενδέχεται να απαγορεύσουν επιλεκτικά την πρόσβαση.

Αυτή τη στιγμή υπάρχουν 3 εκδόσεις του πρωτόκολλου Uniswap. Οι εκδόσεις 1 και 2 είναι ανοιχτού κώδικα (open source), και έχουν γενική άδεια δημόσιας χρήσης (General Public License). Η 3η έκδοση είναι και εκείνη ανοιχτού κώδικα, αλλά με κάποιες παραμετροποιήσεις. Κάθε έκδοση του Uniswap, αφού τεθεί σε λειτουργία, θα

[21] Το ERC-20 πρόκειται για ένα πρότυπο για ανταλλάξιμα tokens, το οποίο καθιστά κάθε token παρόμοιο, σε τύπο και αξία, με ένα άλλο. Π.χ. το ERC-20 Token δρα ακριβώς όπως το ETH, δηλαδή 1 token είναι και πάντα θα είναι ίσο με όλα τα άλλα Tokens.
https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

λειτουργεί για πάντα, αδιάκοπα, δεδομένου βέβαια ότι το Ethereum blockchain θα συνεχίσει να υφίσταται.

4.4.4.3 Πώς συγκρίνεται το πρωτόκολλο του Uniswap σε σχέση με την παραδοσιακή αγορά;

Για την καλύτερη κατανόηση του πως διαφοροποιείται το πρωτοκόλλου του Uniswap σε σχέση με ένα κεντροποιημένο ανταλλακτήριο, θα εστιάσουμε αρχικά σε 2 θέματα: αρχικά, πως η σχεδίαση των AMMs αποκλίνει από τις παραδοσιακές συναλλαγές του βιβλίου παραγγελιών (order-book), και δεύτερον πως τα συστήματα που δεν απαιτούν εξουσιοδότηση (permissionless systems) απομακρύνονται από τα συμβατικά συστήματα όπου απαιτείται εξουσιοδότηση (permissioned systems).

Order Book VS AMM

Οι περισσότερες δημόσια προσβάσιμες αγορές χρησιμοποιούν το βιβλίο παραγγελιών ως μέθοδο ανταλλαγών, όπου οι αγοραστές και οι πωλητές δημιουργούν παραγγελίες που οργανώνονται ανά επίπεδο τιμών όπου καλύπτονται σταδιακά καθώς μετατοπίζεται η ζήτηση. Όποιος έχει διαπραγματευτεί μετοχές μέσω χρηματιστηριακών εταιρειών θα είναι εξοικειωμένος με ένα σύστημα βιβλίου παραγγελιών.

Το πρωτόκολλο του Uniswap ακολουθεί μια διαφορετική προσέγγιση, χρησιμοποιώντας έναν Αυτοματοποιημένο Διαπραγματευτή Αγοράς (AMM), ο οποίος μερικές φορές αναφέρεται ως Διαπραγματευτής σταθερής λειτουργίας, αντί ενός βιβλίου παραγγελιών.

Σε πολύ υψηλό επίπεδο, ένας Αυτοματοποιημένο Διαπραγματευτή Αγοράς αντικαθιστά τις εντολές αγοράς και πώλησης σε μια αγορά βιβλίου παραγγελιών με μια ομάδα ρευστότητας (liquidity pool ή LP), δύο περιουσιακών στοιχείων, τα οποία αποτιμώνται μεταξύ τους. Καθώς το ένα περιουσιακό στοιχείο ανταλλάσσεται με το άλλο, οι σχετικές τιμές των δύο περιουσιακών στοιχείων μετατοπίζονται και καθορίζεται μια νέα τιμή αγοράς και για τα δύο. Σε αυτή τη δυναμική, ένας αγοραστής ή ένας πωλητής συναλλάσσεται απευθείας με το liquidity pool , αντί για συγκεκριμένες παραγγελίες που αφήνουν άλλα άτομα/ομάδες ατόμων.

Συστήματα χωρίς ανάγκη εξουσιοδότησης (Permissionless Systems)

Η δεύτερη απόκλιση από τις παραδοσιακές αγορές είναι ο χωρίς ανάγκη εξουσιοδότησης και αμετάβλητος σχεδιασμός του Uniswap πρωτοκόλλου.

Σύμφωνα με τους δημιουργούς του πρωτοκόλλου, εμπνεύστηκαν αυτές τις σχεδιαστικές αποφάσεις από τις βασικές αρχές του Ethereum και αποτελεί δέσμευσή τους στα ιδανικά της πρόσβασης χωρίς ανάγκη εξουσιοδότησης καθώς και του αμετάβλητου σχεδιασμού του Uniswap, ως στοιχεία ενός μέλλοντος στο οποίο οποιοσδήποτε στον κόσμο μπορεί να έχει πρόσβαση σε χρηματοοικονομικές υπηρεσίες χωρίς φόβο διακρίσεων ή κινδύνου κάποιου αντισυμβαλλόμενου προσώπου ή ομάδας.

Ο σχεδιασμός χωρίς εξουσιοδότηση, σημαίνει ότι οι υπηρεσίες του πρωτοκόλλου είναι εξ ολοκλήρου ανοιχτές για δημόσια χρήση, χωρίς την δυνατότητα επιλεκτικού περιορισμού του ποιος μπορεί ή δεν μπορεί να τις χρησιμοποιήσει. Ο

καθένας μπορεί να ανταλλάξει, να παρέχει ρευστότητα ή να δημιουργήσει νέες αγορές όπως και όποτε αυτός επιθυμεί. Πρόκειται για μια απομάκρυνση από τις παραδοσιακές χρηματοοικονομικές υπηρεσίες, οι οποίες συνήθως περιορίζουν την πρόσβαση με βάση τη γεωγραφία, την περιουσία και την ηλικία.

Το πρωτόκολλο είναι επίσης αμετάβλητο, με άλλα λόγια δεν μπορεί να αναβαθμιστεί. Κανένα μέρος δεν είναι σε θέση να διακόψει τις συμβάσεις, να αντιστρέψει την εκτέλεση συναλλαγών ή να αλλάξει με οποιονδήποτε τρόπο τη συμπεριφορά του πρωτοκόλλου. Αξίζει να σημειωθεί ότι ο τρόπος Διακυβέρνησης του Uniswap, έχει το δικαίωμα (αλλά όχι υποχρέωση) να εκτρέψει ένα ποσοστό των προμηθειών ανταλλαγής σε οποιαδήποτε ομάδα ρευστότητας (LP) σε μια καθορισμένη διεύθυνση. Ωστόσο, αυτή η ικανότητα είναι γνωστή σε όλους τους συμμετέχοντες εκ των προτέρων και για να αποφευχθεί η κατάχρηση, το ποσοστό περιορίζεται μεταξύ 10% και 25%.

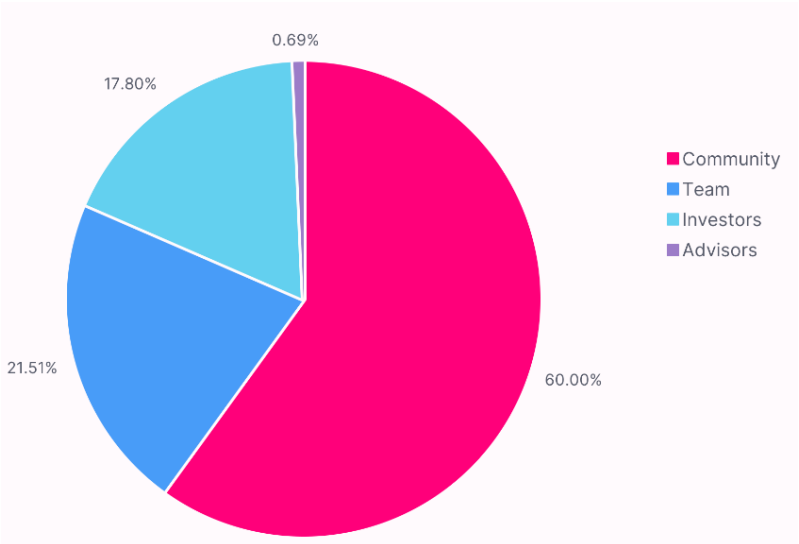
4.4.4.4 Διακυβέρνηση

Το πρωτόκολλο του Uniswap αποτελεί δημόσιο αγαθό του οποίου η ιδιοκτησία και η διακυβέρνηση ανήκει/γίνεται από τους κατόχους των UNI tokens. Το UNI αποτελεί το token του Uniswap πρωτοκόλλου. Συνολικά έχουν δημιουργηθεί 1 δισεκατομμύριο UNI και θα γίνουν προσβάσιμα κατά τη διάρκεια της επόμενης 4ετίας. Η αρχική τετραετής κατανομή έχει ως εξής:

- 60,00% στα μέλη της κοινότητας Uniswap (600 εκατ. UNI)
- 21,266% σε μέλη της ομάδας και μελλοντικούς υπαλλήλους με 4ετή κατοχύρωση (212,66 εκατ. UNI)
- 18,044% σε επενδυτές με 4ετή κατοχύρωση (180,44 εκατ. UNI)
- 0,69% σε συμβούλους με 4ετή κατοχύρωση (6.9 εκατ. UNI)

Να σημειωθεί πως, ένα διαρκές ποσοστό πληθωρισμού 2% ετησίως θα ξεκινήσει μετά από 4 χρόνια, διασφαλίζοντας τη συνεχή συμμετοχή και συνεισφορά στο Uniswap σε βάρος των παθητικών κατόχων UNI.

Σχήμα 15: Η κατανομή των UNI tokens



Πηγή: https://uniswap.org/

Με το 15% των tokens να είναι ήδη διαθέσιμα για διεκδίκηση από ιστορικούς χρήστες και πάροχους ρευστότητας, το ταμείο διακυβέρνησης θα διατηρήσει το 43% (430.000.000 UNI) της προσφοράς UNI για διανομή σε συνεχή βάση μέσω επιχορηγήσεων συντελεστών, κοινοτικών πρωτοβουλιών, εξόρυξης ρευστότητας και άλλων προγραμμάτων .

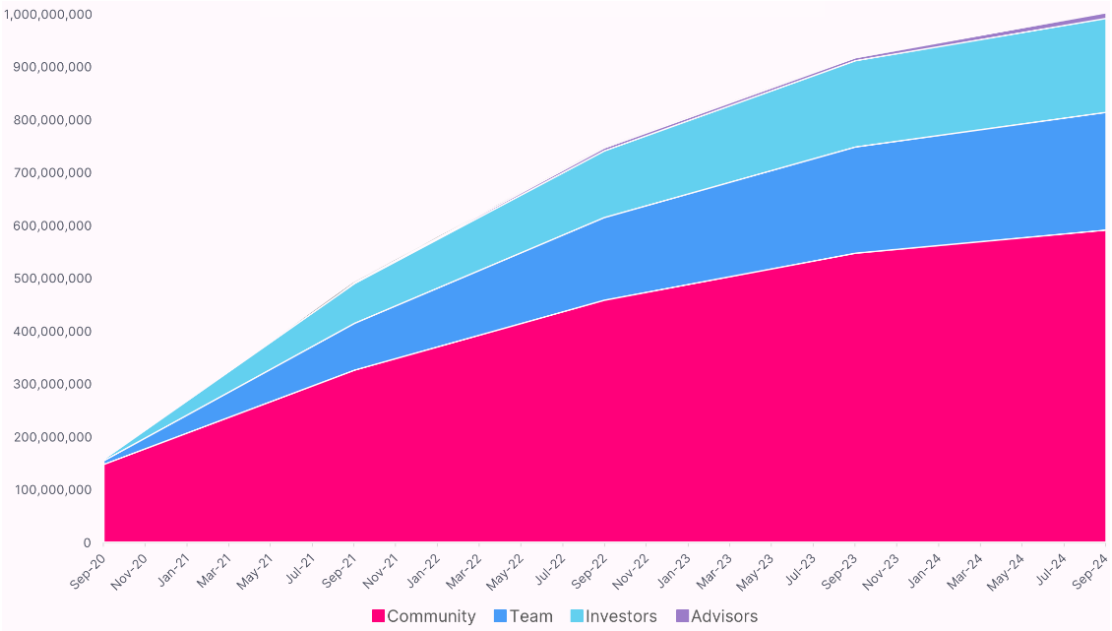
Το UNI θα κατοχυρώσει στο ταμείο διακυβέρνησης σε συνεχή βάση σύμφωνα με το ακόλουθο χρονοδιάγραμμα. Η διακυβέρνηση έχει πρόσβαση στο κατοχυρωμένο UNI από τις 18 Οκτωβρίου 2020 στις 12:00 π.μ. UTC.

Πίνακας 2: Κατανομή UNI tokens στην κοινότητα[22] κατά τη διάρκεια της 4ετίας

Year	Community Treasury	Distribution %
Year 1	172,000,000 UNI	40%
Year 2	129,000,000 UNI	30%
Year 3	86,000,000 UNI	20%
Year 4	43,000,000 UNI	10%

Πηγή: https://uniswap.org/

Σχήμα 16: Πρόγραμμα κατανομής UNI ανά ομάδα για την περίοδο Σεπτέμβριος 2020-Σεπτεμβριος 2024



Πηγή: https://uniswap.org/

[22] Οι κατανομές ομάδας, επενδυτών και συμβούλων UNI θα έχουν tokens κλειδωμένα με το ίδιο χρονοδιάγραμμα.

Συμπεράσματα

Με το τέλος αυτής της εργασίας μπορούμε να αναλογιστούμε την πληθώρα καινοτομιών που έφεραν το blockchain αρχικά στο τρόπο με τον οποίο γίνονται οι συναλλαγές και κατ' επέκταση η Αποκεντρωμένη Χρηματοοικονομική σε πολλές πτυχές της καθημερινότητάς μας εκτός από τον τομέα των συναλλαγών. Με την μελέτη περίπτωσης των 2 εφαρμογών μπορούμε να αναλογιστούμε το μας επιφυλάσσει το μέλλον για τις άπειρες δυνατότητες των εφαρμογών που δημιουργούνται με βάση την πλατφόρμα του Ethereum.

Πηγές-Βιβλιογραφία

Πηγές

Uniswap Website: https://uniswap.org/

Uniswap Whitepaper: https://uniswap.org/whitepaper-v3.pdf

Ορισμός tokens από την ΕΚΤ: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

Ορισμός tokens από την Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

Ορισμός κρυπτονομισμάτων από τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-opinion-paper-on-cryptocurrencies-in-the-eu

Τράπεζα Διεθνών Διακανονισμών σχετικά με τα κρυπτονομίσματα: https://www.bis.org/cpmi/publ/d137.pdf

Σχήμα παραδοσιακού χρηματοοικονομικού συστήματος:

https://www.dailyeconomics.gr/oikonomikoi-oroi/xrimatopistwtiko-sustima

Το πρώτο block του blockchain:

https://www.blockchain.com/explorer/blocks/btc/0

Bitcoin Whitepaper:

https://bitcoin.org/bitcoin.pdf

Ιδέα των smart contracts από τον Szabo:

www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Ethereum Whitepaper: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

B Money Whitepaper: http://www.weidai.com/bmoney.txt

Είδη δικτύων: https://blockchainengineer.com/centralized-vs-decentralized-vs-distributed-network/

Αριθμός κρυπτονομισμάτων 2013- Φεβρουάριος 2023

https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

Προμήθειες Alpha Bank: https://www.alpha.gr/el/idiotes/support-center/atm-kas/kostos

Χώρες χωρίς τραπεζικό σύστημα: https://www.statista.com/chart/18497/countries-with-the-highest-share-of-adults-without-a-bank-account-in-2017/

Ορισμός ψηφιακών νομισμάτων από την Παγκόσμια Τράπεζα: https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

Ορισμός εικονικών νομισμάτων από την Εσωτερική Υπηρεσία Εσόδων των ΗΠΑ: https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions

Κεφαλαιοποίηση των κρυπτονομισμάτων (Φεβρουάριος 2023): https://www.slickcharts.com/currency

Αριθμός ανταλλακτηρίων (Φεβρουάριος 2023):

https://www.forbes.com/advisor/investing/cryptocurrency/best-crypto-exchanges/

Σχετικά με τους Αποκεντρωμένους Αυτόνομους Οργανισμούς: https://ethereum.org/en/dao/

Σχετικά με το πρότυπο ERC-20 : https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

Βιβλιογραφία

Daskalakis, N. and Georgitseas, P. (2020). An Introduction to Cryptocurrencies: The Crypto Market Ecosystem, Routledge Taylor&Francis Group.

Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets. Federal Reserve Bank of St. Louis Review, 103(2), pp. 153-74.

Makarov, I. and Schoar, A. (2022). CRYPTOCURRENCIES AND DECENTRALIZED FINANCE (DEFI), NBER Working paper 30006.

He et al. (2016) Virtual Currencies and Beyond: Initial Considerations, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

Qin et al. (2021) CeFi vs. DeFi — Comparing Centralized to Decentralized Finance, https://arxiv.org/pdf/2106.08157.pdf