



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

**ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ
ΕΠΙΧΕΙΡΗΣΕΩΝ**

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΤΟΥΡΙΣΜΟΥ

(πρώην Τμήμα Λογιστικής & Χρηματοοικονομικής – Μεσολόγγι)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**ΑΝΑΛΥΣΗ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΤΩΝ
ΔΥΝΑΤΟΤΗΤΩΝ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ
ΨΗΦΙΑΚΩΝ ΝΟΜΙΣΜΑΤΩΝ**

ΣΤΟΪΚΟΥ ΔΗΜΗΤΡΙΟΣ

**ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ
ΠΑΞΙΜΑΔΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ**

ΜΕΣΟΛΟΓΓΙ 2021

ΠΕΡΙΛΗΨΗ

Το θέμα της παρούσας πτυχιακής εργασίας είναι «Ανάλυση της Λειτουργιάς και των Δυνατοτήτων των Ηλεκτρονικών Ψηφιακών Νομισμάτων».

Στο 1^ο κεφάλαιο γίνεται μια σύντομη ιστορική παρουσίαση σε σχέση με τις ανάγκες που οδήγησαν στην δημιουργία των κρυπτονομισμάτων και την τεχνολογία που χρησιμοποιούν για την υλοποίησή τους. Γίνεται αναφορά στο πρώτο σημαντικό κρυπτονόμισμα το Bitcoin, καθώς και αναφέρονται τα σημαντικότερα που το ακολούθησαν. Επίσης, αναφέρονται οι επιπτώσεις που επέφερε ή προβλέπεται να επιφέρει η διάδοση της χρήσης των κρυπτονομισμάτων από το ευρύ κοινό.

Στο 2^ο κεφάλαιο αναλύονται οι τεχνολογίες που χρησιμοποιούνται και οι λειτουργίες που απαιτούνται για την λειτουργία των κρυπτονομισμάτων. Επίσης εξηγείται με ποιόν τρόπο ένας χρήστης μπορεί να συμμετέχει στον κύκλο λειτουργίας και να αμείβεται από αυτό.

Στο 3^ο κεφάλαιο αναλύονται οι κατηγορίες των κρυπτονομισμάτων σε σχέση με τον τρόπο που εξορύσσονται τα κρυπτονομίσματα.

Στο 4^ο κεφάλαιο αναφέρονται τα κυριότερα κρυπτονομίσματα που βρίσκονται σε λειτουργία και επιχειρείται μια προσπάθεια ταξινόμησης και ομαδοποίησης τους.

Στο 5^ο κεφάλαιο παρουσιάζεται η προσπάθεια της Ευρωπαϊκής Ένωσης να ελέγξει και να περιορίσει την χρήση των κρυπτονομισμάτων για παράνομες ενέργειες και να εντοπίσει πως χρησιμοποιούνται σε περιπτώσεις «ξεπλύματος χρήματος».

Λέξεις Κλειδιά: Κρυπτονομίσματα, blockchains, peer-to-peer, miners, DAO, cryptowallets, Proof of Work, Proof of Stake, Tokens, Stablecoins

ABSTRACT

The topic of this dissertation is "Analysis of the Function and Capabilities of Electronic Digital Currencies".

Chapter 1 provides a brief historical overview of the needs that led to the creation of cryptocurrencies and the technology they use to implement them. Reference is made to the first major cryptocurrency Bitcoin, as well as the most important that followed it. The effects of the use of cryptocurrencies by the general public are also reported.

Chapter 2 analyzes the technologies used and the functions required for the operation of cryptocurrencies. It also explains how a user can participate in the pay cycle and be paid by it.

Chapter 3 analyzes the categories of cryptocurrencies in relation to the way cryptocurrencies are mined.

Chapter 4 lists the main cryptocurrencies that are in operation and an attempt is made to classify and group them.

Chapter 5 presents the European Union's attempt to control and limit the use of cryptocurrencies for illegal activities and to identify how they are used in cases of "money laundering".

Keywords: Cryptocoins, blockchains, peer-to-peer, miners, DAO, cryptowallets, Proof of Work, Proof of Stake, Tokens, Stablecoins

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ.....	3
ABSTRACT	4
ΠΕΡΙΕΧΟΜΕΝΑ	5
ΕΙΣΑΓΩΓΗ.....	7
1 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ - ΣΥΝΤΟΜΗ ΙΣΤΟΡΙΑ	9
2 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ BLOCKCHAINS.....	13
2.1 ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN.....	13
2.2 ΙΔΙΩΤΙΚΑ ΚΛΕΙΔΙΑ	13
2.3 CRYPTOCURRENCY WALLETS - ΠΟΡΤΟΦΟΛΙΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ	14
2.4 MINERS - ΕΞΩΡΥΧΟΙ.....	15
2.5 FINITE SUPPLY - ΠΕΠΕΡΑΣΜΕΝΗ ΠΡΟΣΦΟΡΑ	16
2.6 CRYPTOCURRENCY EXCHANGES - ΑΝΤΑΛΛΑΓΕΣ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ	16
3 ΚΑΤΗΓΟΡΙΕΣ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ.....	18
3.1 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΜΕ ΑΠΟΔΕΙΚΤΙΚΟ ΕΡΓΑΣΙΑΣ (POW)	18
3.1.1 Πλεονεκτήματα των κρυπτονομισμάτων PoW	18
3.1.2 Μειονεκτήματα των κρυπτονομισμάτων PoW	19
3.1.3 Κρυπτονομίσματα που χρησιμοποιούν PoW.....	19
3.2 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΜΕ ΑΠΟΔΕΙΚΤΙΚΟ ΛΕΙΤΟΥΡΓΙΑΣ (POS)	20
3.2.1 Πλεονεκτήματα των κρυπτονομισμάτων PoS	21
3.2.2 Μειονεκτήματα των κρυπτονομισμάτων PoS.....	21
3.2.3 Κρυπτονομίσματα που χρησιμοποιούν PoS.....	21
3.3 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΤΟΚΕΝΣ - ΚΟΥΠΟΝΙΑ	22
3.3.1 Πλεονεκτήματα των κρυπτονομισμάτων κουπονιών	23
3.3.2 Μειονεκτήματα των κρυπτονομισμάτων κουπονιών	23
3.3.3 Σημαντικά κρυπτο-κουπόνια	23
3.4 STABLECOINS - ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΣΤΑΘΕΡΗΣ ΑΞΙΑΣ.....	24
3.4.1 Πλεονεκτήματα των κρυπτονομισμάτων Stablecoins.....	24
3.4.2 Μειονεκτήματα των κρυπτονομισμάτων Stablecoins	25
3.4.3 Σημαντικά Stablecoins	25
4 ΣΗΜΑΝΤΙΚΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ ΚΑΙΝΟΤΟΜΙΕΣ.....	27
4.1 BITCOIN (BTC)	27
4.2 ETHEREUM (ETH).....	28
4.3 RIPPLE (XRP)	29
4.4 BITCOIN CASH (BCH)	30
4.5 LITECOIN (LTC)	30
4.6 STELLAR (XLM).....	31
4.7 DASH (DASH).....	32
4.8 MONERO (XMR).....	33
4.9 ΤΑΞΙΝΟΜΗΣΗ – ΟΜΑΔΟΠΟΙΗΣΗ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ	35
5 ΕΥΡΩΠΑΙΚΟ ΠΛΑΙΣΙΟ ΛΕΙΤΟΥΡΓΙΑΣ.....	37
5.1 ΕΜΠΟΔΙΑ ΣΤΗΝ ΠΡΟΣΠΑΘΕΙΑ ΟΡΙΣΜΟΥ ΠΛΑΙΣΙΟΥ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΚΑΝΟΝΩΝ ΣΕ ΣΧΕΣΗ ΜΕ ΤΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ	37
5.1.1 Ανωνυμία	37
5.1.2 Διασυνοριακή φύση	37
5.1.3 Απουσία μεσάζοντα	38
5.2 ΤΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ «ΚΡΥΒΟΝΤΑΙ» ΠΙΣΩ ΑΠΟ ΤΗΝ ΑΝΩΝΥΜΙΑ ΤΟΥΣ.....	38
5.3 Η ΛΕΠΤΗ ΔΙΑΧΩΡΙΣΤΙΚΗ ΓΡΑΜΜΗ ΠΟΥ ΧΩΡΙΖΕΙ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ, ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΟ ΑΠΟΡΡΗΤΟ.....	38

5.4	ΤΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΣΤΟΝ ΝΟΜΟ AMLD4	39
5.5	Η ΣΥΜΠΕΡΙΛΗΨΗ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ ΣΤΟΝ ΝΟΜΟ AMLD5354	39
6	ΣΥΜΠΕΡΑΣΜΑΤΑ.....	41
7	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	44
7.1	ΒΙΒΛΙΑ – ΜΕΛΕΤΕΣ – ΕΡΓΑΣΙΕΣ.....	44
7.2	ΙΣΤΟΣΕΛΙΔΕΣ	45

ΕΙΣΑΓΩΓΗ

Κάθε χώρα λειτουργεί κάτω από συγκεκριμένα χαρακτηριστικά και συνήθειες, και με βάση αυτά δημιουργεί μέσα και πρότυπα για την διευκόλυνση της ζωής των κατοίκων της. Το χρήμα είναι ένα από αυτά τα μέσα. Ωστόσο, επειδή υπάρχουν πάρα πολλές χώρες που έχουν δημιουργήσει την δική τους εκδοχή χρήματος, προκύπτει το ζήτημα να καθοριστεί ποιες είναι οι ομοιότητες όλων αυτών πολυάριθμων μορφών χρήματος.

Το προφανές κοινό χαρακτηριστικό είναι ότι μπορούν να εκτιμώνται και να αναγνωρίζονται παντού. Η ιδιότητά τους είναι να χρησιμοποιούνται ως γενικό μέσο πληρωμής μέσα στην κοινότητα στην οποία παράγονται.

Βασική προϋπόθεση για την ύπαρξη ενός γενικού μέσου πληρωμής σε κάθε κοινότητα είναι ότι αυτή διαθέτει ένα σύστημα λογιστικής αξίας που περιλαμβάνει, ως συστατικό στοιχείο, μια νομισματική μονάδα. Μια μονάδα μέτρησης - όπως λίρα στερλίνα, δολάριο ΗΠΑ, ευρώ - με την οποία εκτιμάται η αξία όλων τα αγαθών, των υπηρεσιών και των περιουσιακών στοιχείων στην κοινότητα. Είναι σαφές ότι όλα τα χρηματικά ποσά πρέπει επίσης να εκφράζονται στις ίδιες νομισματικές μονάδες με τα χρέη, εάν τα χρήματα πρόκειται να χρησιμοποιηθούν για την εξόφλησή τους. Έτσι, η ίδια νομισματική μονάδα αποτελεί το βασικό χαρακτηριστικό ενός συστήματος υπολογισμού της αξίας.

Εάν η ονομαστική αξία οποιουδήποτε νομίσματος γίνεται αποδεκτή ως γενικό μέσο πληρωμής, τότε αυτό προστίθεται σαν μέρος του συστήματος λογιστικής αξίας της κοινότητας. Τα περισσότερα πράγματα (όχι μόνο το χρήμα) ενσωματώνονται, στην πραγματικότητα, στα κοινοτικά συστήματα ως διαδικασίες, μέσω της γενικής αποδοχής. Όλα τα κοινωνικά πράγματα διέπονται από σύνολα δικαιωμάτων και υποχρεώσεων που αναγνωρίζονται από την κοινότητα. Σαν παράδειγμα, αρκεί να σκεφτούμε τη δημιουργία και τις αποδεκτές χρήσεις μέσων μεταφοράς, αυτοκινητοδρόμων, χώρων στάθμευσης αυτοκινήτων, φωτεινών σηματοδοτών, διαβατηρίων, σχολείων, νοσοκομείων κ.λπ. Το χρήμα είναι απλώς μια άλλη μια έκφανση αυτής της γενικής διαδικασίας κοινωνικής αποδοχής.

Τα χρήματα αλλάζουν και εξελίσσονται από την πρώτη στιγμή της δημιουργίας τους, αλλά εξακολουθούν να εξυπηρετούν τις ίδιες βασικές λειτουργίες: μέσο ανταλλαγής, αποταμιευτικό μέσο και μονάδα μέτρησης αξίας.

Έτσι σήμερα, το χρήμα είναι ένα από τα πιο σημαντικά εργαλεία για κοινωνικές και οικονομικές αλληλεπιδράσεις. Είναι πολύ δύσκολο να φανταστούμε την καθημερινή μας ζωή χωρίς μετρητά. Όμως το άυλο χρήμα έχει κάνει την εμφάνιση του από καιρό και ο ρυθμός ανάπτυξης του είναι εξαιρετικά γρήγορος.

Αυτό οφείλεται στην ευκολία χρήσης του στα σύγχρονα συστήματα πληρωμών και την εξέλιξη του Διαδικτύου, η οποία καθιστά δυνατή την πραγματοποίηση ανέπαφων συναλλαγών μέσω τερματικών ή διαδικτυακών συναλλαγών μέσω Διαδικτύου.

Η εμφάνιση πλαστικών καρτών τον 20ο αιώνα μείωσε σημαντικά την κυκλοφορία μετρητών, επιτρέποντας στα άτομα να πληρώνουν για την απόκτηση αγαθών ή να πάρουν δάνειο χωρίς να φύγουν από το σπίτι τους.

Η περίοδος από τον 20ο έως τις αρχές του 21ου αιώνα χαρακτηρίζεται από την μεγάλη ανάπτυξη του παγκόσμιου χρηματοπιστωτικού τομέα. Τα χρηματοοικονομικά συστήματα αναπτύσσονται, εξελίσσονται, και προσαρμόζονται στις νέες οικονομικές και τεχνολογικές

απαιτήσεις, δημιουργώντας ένα καλύτερο περιβάλλον για την πιο αποτελεσματική κυκλοφορία του χρήματος, καθώς αποτελεί την κινητήρια δύναμη των παγκόσμιων οικονομιών.

Οι κύριοι παράγοντες που ευθύνονται για τις καινοτομίες στον χώρο της οικονομίας είναι η ανάπτυξη της παγκοσμιοποίησης και η ψηφιοποίηση των παγκόσμιων οικονομιών. Σε τέτοιες συνθήκες, επιβάλλονται αυξημένες κανονιστικές απαιτήσεις σε συστήματα και εργαλεία πληρωμών, καθώς οι κίνδυνοι, μεταξύ των παγκόσμιων οικονομιών, είναι κοινοί.

Αυτές οι συνθήκες και οι απαιτήσεις της σύγχρονης παγκοσμιοποιημένης οικονομίας δείχνουν να καλύπτονται από μια νέα μορφή χρήματος, **τα ψηφιακά νομίσματα ή κρυπτονομίσματα**. Αυτά φαίνονται ικανά να ξελιξουν τα υπάρχοντα συστήματα πληρωμών καθώς αντιπροσωπεύουν μια νέα μορφή χρήματος πιο αποκεντρωμένης και κατά συνέπεια πιο ασφαλούς.

Το κρυπτονομίσμα είναι ένα ψηφιακό - εικονικό νόμισμα που ασφαλίζεται με κρυπτογραφικές μεθόδους, πράγμα που καθιστά σχεδόν αδύνατη την παραποίηση του ή την διπλοχρησία του. Πολλά κρυπτονομίσματα είναι, ουσιαστικά, αποκεντρωμένα δίκτυα βασισμένα στην τεχνολογία **blockchain** (κατανεμημένο αρχείο καταγραφών συναλλαγών) που επιβλέπεται και ενημερώνεται από ένα εκτεταμένο δίκτυο υπολογιστών.

Ένα καθοριστικό χαρακτηριστικό των κρυπτονομισμάτων είναι ότι γενικά δεν εκδίδονται από κάποια κεντρική αρχή, καθιστώντας τα θεωρητικά απρόσβλητα από κυβερνητικές παρεμβάσεις και χειραγωγήσεις.

Χαρακτηριστικά, ο παγκόσμιος ηγέτης των χρηματοοικονομικών - οι Ηνωμένες Πολιτείες – ενεργούν έρευνα και κάνουν ενέργειες για την εισαγωγή κρυπτονομισμάτων στο εσωτερικό σύστημα πληρωμών της χώρας από το 2019.

Στο τέλος του 2019, το Κογκρέσο των ΗΠΑ ψήφισε νομοσχέδιο προς εξέταση που ονομάζεται «Crypto-Currency Act of 2020». Εξέτασε τη διαδικασία αναγνώρισης, αδειοδότησης και καταχώρησης ψηφιακών νομισμάτων ως τρόπο πληρωμής, και επίσης καθιέρωσε έναν κατάλογο κρατικών φορέων που είναι υπεύθυνοι για τον κανονισμό και έλεγχο του νέου νομίσματος.

Μπορούν τα κρυπτονομίσματα να γίνουν χρήματα:

Σήμερα είναι δύσκολο να εκτιμηθεί και να αξιολογηθεί η σημασία αυτής της τεχνολογίας και οι προοπτικές για την ανάπτυξή της. Ωστόσο, τα ψηφιακά νομίσματα μπορούν να γίνουν το νέο, παγκοσμίως αποδεκτό μέσο πληρωμής, αντικαθιστώντας τα συμβατικά χρήματα fiat¹. Σε αυτήν την περίπτωση, το πιο επιτυχημένο σύστημα κρυπτονομίσματος μιας συγκεκριμένης χώρας μπορεί να της δώσει ένα σημαντικό πλεονέκτημα στον παγκόσμιο χρηματοοικονομικό χώρο.

¹ **Παραστατικό χρήμα (fiat money)** ή αλλιώς χρήμα αναγκαστικής κυκλοφορίας είναι το μέσον πληρωμής το οποίο δεν καλύπτεται από αποθεματικό άλλων υλικών (π.χ. χρυσός) και επομένως στερείται κάποιας εσωτερικής αξίας έστω και έμμεσα. Επιβάλλεται στις συναλλαγές από κάποια αρχή (συνήθως το κράτος) τόσο στις πληρωμές όσο και στις εισπράξεις. Εκφράζεται με κάποια νομισματική μονάδα έχει την μορφή συνήθως χαρτονομισμάτων και κερμάτων, τα οποία μπορεί να έχουν ονομαστική αξία ίση, πολλαπλάσια ή υποπολλαπλάσια της νομισματικής μονάδας. (Από τη Βικιπαίδεια, την ελεύθερη εγκυκλοπαίδεια)

1 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ - ΣΥΝΤΟΜΗ ΙΣΤΟΡΙΑ

Πριν να εμφανιστούν οι σύγχρονες μορφές κρυπτονομισμάτων, έγιναν αρκετές απόπειρες να δημιουργηθεί κάτι αντίστοιχο, αλλά αυτά δεν απέκτησαν ευρεία αποδοχή. Οι προσπάθειες αυτές εντοπίζονται στις αρχές της δεκαετίας του 1980 στην Ολλανδία και τις Ηνωμένες Πολιτείες. Το πρώτο άξιο λόγου ψηφιακό νόμισμα είναι το DigiCash, το οποίο δημιουργήθηκε τη δεκαετία του 1990, αλλά δεν διαδόθηκε.

Το PayPal και οι ανταγωνιστές του εμφανίστηκαν αργότερα και υιοθέτησαν μια υβριδική προσέγγιση των ψηφιακών συναλλαγών χρησιμοποιώντας υπάρχοντα νομίσματα. Αυτές οι εταιρείες εξακολουθούν να διαδραματίζουν σημαντικό ρόλο στο διαδικτυακό και το διεθνές εμπόριο.

Άλλες προσπάθειες δημιουργίας κρυπτονομισμάτων περιλαμβάνουν τα B-Money, Hashcash, Flooz και Bit Gold. Ένα από τα μεγαλύτερα ονόματα στην αρχή της κρυπτογράφησης είναι ο David Chaum, ένας επιστήμονας υπολογιστών και μαθηματικός που δημιούργησε το DigiCash, το οποίο έπαιξε σημαντικό ρόλο στη μεταγενέστερη εξέλιξη των κρυπτονομισμάτων.

Το κυριότερο στοιχείο για να επιτύχει ένα κρυπτονόμισμα είναι η αξιοπιστία, να υπάρχουν, δηλαδή, δικλίδες ασφαλείας που θα προστατεύουν τον κάτοχο από παραποιήσεις και υπεξαιρέσεις των νομισμάτων. Πρέπει να υπάρχει το ανάλογο της τραπεζικής θυρίδας και ο μηχανισμός για πληρωμές και εισπράξεις σε αυτό το νόμισμα.

Τα ψηφιακά περιουσιακά στοιχεία είναι δύσκολο να ασφαλιστούν. Στον ψηφιακό κόσμο είναι εύκολο να αντιγραφεί και να αναπαραχθεί μια πληροφορία, όπως αναπαράγεται μια φωτογραφία, για παράδειγμα, και αποστέλλεται μέσω ηλεκτρονικού ταχυδρομείου. Η δημιουργία ενός ψηφιακού νομίσματος απαιτεί την δημιουργία ενός ψηφιακού στοιχείου που δεν μπορεί να αναπαραχθεί και ανήκει σε έναν και μόνο, πιστοποιημένο κάτοχο.

Όσο η τράπεζα φυλάσσει τα μετρητά ενός πολίτη, αυτός δεν μπορεί να τα αντιγράψει και να χρησιμοποιήσει τα αντίγραφα. Είναι ασφαλή στην τράπεζα. Ο κάτοχος, η τράπεζα και η το κράτος συμφωνούν ότι σε έναν τραπεζικό λογαριασμό βρίσκονται το συγκεκριμένο ποσό χρημάτων. Για να γίνει χρήση των ψηφιακών νομισμάτων, θα πρέπει να δημιουργηθούν συστήματα ασφαλείας από το μηδέν.

Bitcoin

Και ξαφνικά δημιουργήθηκε το κρυπτονόμισμα Bitcoin. Η πραγματική προέλευση του παραμένει κάπως μυστηριώδης.

Το 2008, ο **Satoshi Nakamoto** - το οποίο πιθανώς είναι ψευδώνυμο είτε για ένα άτομο είτε για μια ομάδα ανθρώπων- δημοσίευσε την λευκή βίβλο, μια περιγραφή υλοποίησης ενός ψηφιακού νομίσματος με το όνομα **Bitcoin**. Το Bitcoin λειτουργεί μια τεχνολογία που ονομάζεται **Blockchain**², την οποία το πρότυπο του Bitcoin αποκαλεί σύστημα «τριπλής λογιστικής καταχώρησης». Κάθε φορά που γίνεται μια νέα συναλλαγή, ο αποστολέας, ο παραλήπτης και ένας τρίτος πρέπει να επιβεβαιώνουν και να συμφωνούν σχετικά με τη

² Blockchain (στα ελληνικά ο αγγλικός όρος αποδίδεται ποικιλοτρόπως, ως «αλυσίδα μπλοκ» ή «μπλοκ αλυσίδας», «αλυσίδα συστοιχιών», «τεχνολογία κατανεμημένης εγγραφής», «αλυσίδα ομάδων συναλλαγών», «αλυσίδα κοινοποιήσεων» είναι μια νέα τεχνολογία η οποία παρουσιάζεται ως μία δημόσια, μη δυνάμενη να τροποποιηθεί ως προς το ιστορικό της, διανεμημένη σειρά δεδομένων, ομαδοποιημένων σε χρονικά αριθμημένα «τμήματα», «συστοιχίες» (blocks). (Από τη Βικιπαίδεια, την ελεύθερη εγκυκλοπαίδεια)

συναλλαγή. Σε αυτό το διαμοιρασμένο αρχείο καταγραφής-blockchain βρίσκεται κάθε συναλλαγή Bitcoin που έχει πραγματοποιηθεί απαρχής.

Αυτό προσφέρει εμπιστοσύνη σε συνδυασμό με ορισμένου επιπέδου ανωνυμία, καθώς κάθε συναλλαγή σε ένα συγκεκριμένο πορτοφόλι Bitcoin μπορεί να εντοπιστεί, αλλά δεν είναι γνωστός απαραίτητα το ποιος κατέχει αυτό το πορτοφόλι.

Μετά από περισσότερο από μια δεκαετία, εκατοντάδες κρυπτονομίσματα και αμέτρητες άλλες εφαρμογές της τεχνολογίας Blockchain είναι διαθέσιμα.

Η συνολική αξία όλων των Bitcoin, γνωστή ως «market cap», ξεπέρασε το 1 τρισεκατομμύριο δολάρια τον Μάρτιο του 2021. Η εμπορική αξία του νομίσματος είναι εξαιρετικά ασταθής, συχνά αντιμετωπίζει σημαντικές μεταβολές σε σύντομες χρονικές περιόδους.

Άλλα κρυπτονομίσματα

Το Bitcoin δεν είναι ο μοναδικός παίκτης στο παιχνίδι των κρυπτονομισμάτων.

Καθώς η δημοτικότητα του άρχισε να αυξάνεται, άλλα νομίσματα κυκλοφόρησαν χρησιμοποιώντας την ίδια τεχνολογία blockchain. Η πιο αξιοσημείωτη εναλλακτική λύση Bitcoin είναι το Ethereum, το οποίο έχει το δεύτερο μεγαλύτερο μερίδιο αγοράς στα κρυπτονομίσματα. Υπάρχουν όμως πολλοί και άλλα. Η ακόλουθη λίστα εμφανίζει κρυπτονομίσματα με τις μεγαλύτερες διαθέσιμες κεφαλαιοποιήσεις για συναλλαγές στο δημοφιλές χρηματιστήριο Coinbase, στις 30 Μαρτίου 2021:

- Bitcoin
- Ethereum/Ethereum 2
- Binance Coin
- Tether
- Cardano
- Polkadot
- XRP
- Uniswap
- Litecoin
- THETA3

Αυτή η λίστα περιέχει νομίσματα που αλλάζουν σε αξία με τη ζήτηση της αγοράς, όπως το Bitcoin και νομίσματα που συνδέονται με το δολάριο ΗΠΑ. Το Tether και το USD Coin είναι δύο βασικά «stablecoins» που παρακολουθούν τα κύρια νομίσματα fiat.

Κρυπτονομίσματα και Αγορές

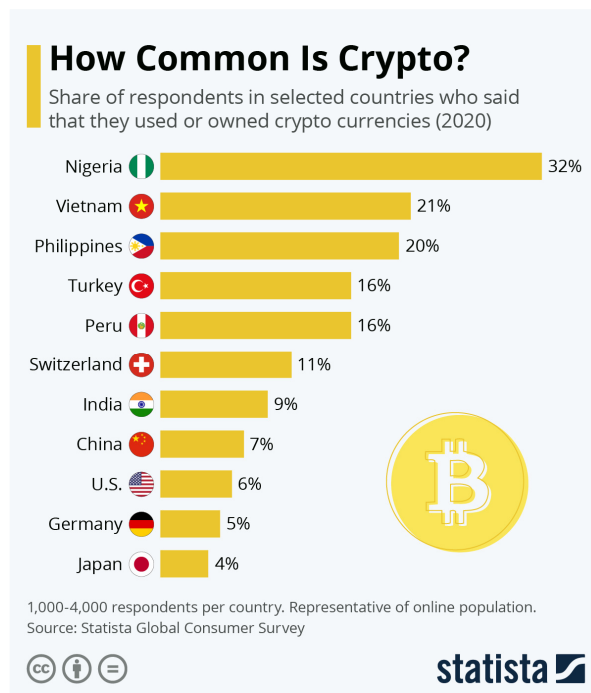
Η άνοδος των κρυπτονομισμάτων αποτελεί απειλή για τα συμβατικά νομίσματα και την παραδοσιακή οικονομία. Τα κρυπτονομίσματα υιοθετούν έναν μηχανισμό **peer-to-peer**³ (δίκτυο συνδεδεμένων - συνεργαζομένων υπολογιστών) που εξαλείφει την αναγκαιότητα ύπαρξης του μεσάζοντα, που συνήθως αποτελούν οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα, για την διεκπεραίωση χρηματοοικονομικών συναλλαγών.

Χαρακτηριστικά, δεν υπάρχει τραπεζικός λογαριασμός ή πιστωτική κάρτα στις συναλλαγές στον κόσμο των κρυπτονομισμάτων.

³ Ένα δίκτυο υπολογιστών peer-to-peer (ή P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισodύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα. (Από τη Βικιπαίδεια, την ελεύθερη εγκυκλοπαίδεια)

Πράγματι, ένα ηλεκτρονικό πορτοφόλι εκτελεί την ίδια λειτουργία με μια τραπεζική θυρίδα. Διοσεκατομμύρια χρήστες με έξυπνο τηλέφωνο με πρόσβαση στο Διαδίκτυο, μπορούν να εγκαταλείψουν τις τράπεζες και να εκτελούν οικονομικές συναλλαγές, αυτό είναι επαναστατικό. Η νέα τεχνολογία, προσφέρει την δυνατότητα για φτηνές, ασφαλείς και σχεδόν άμεσες συναλλαγές, επιτρέποντας διοσεκατομμύρια ανθρώπων για να ενταχθούν στον κόσμο του διαδικτυακού εμπορίου, να πληρώνουν και να πληρώνονται, για αγαθά ή υπηρεσίες, χωρίς να κάνουν χρήση της παραδοσιακής υποδομής τραπεζικών και πιστωτικών καρτών.

Είναι χαρακτηριστικό ότι οι μεγαλύτερη χρήση κρυπτονομισμάτων γίνεται από πολίτες χωρών που δεν έχουν αναπτυγμένο τραπεζικό τομέα ή οι οικονομίες τους βρίσκονται σε μεγάλη αστάθεια και παρουσιάζουν υψηλό πληθωρισμό.



Εικόνα 1 - Χώρες με την μεγαλύτερη χρήση κρυπτονομισμάτων

Οι συναλλαγές με κρυπτονομισμάτα επιτρέπουν πληρωμές σε πραγματικό χρόνο. Οι πιστωτικές κάρτες δεν έχουν σχεδιαστεί για χρέωση ενός λεπτού του ευρώ για λήψη, για παράδειγμα, ενός προϊόντος ή υπηρεσίας από το Διαδίκτυο. Τα κρυπτονομισμάτα υπόσχονται να κάνουν τις μικροπληρωμές απρόσκοπτες και να επιτρέπουν στις επιχειρήσεις να προσφέρουν σε πραγματικό χρόνο κατανάλωση ανά χρήση προϊόντα, όπως βίντεο, ήχος, υπηρεσία κινητού τηλεφώνου, βοηθητικά προγράμματα και άλλα.

Ένα κρυπτονομίσμα όπως το Bitcoin μπορεί να θεωρηθεί ως **Αποκεντρωμένος Αυτόνομος Οργανισμός (Decentralized Autonomous Organization DAO)** και ένα δίκτυο ανοιχτού κώδικα peer-to-peer που ελέγχει τις συναλλαγές είναι ο επιβλέπων φορέας. Σε αυτήν τη διαμόρφωση DAO, η προσφορά χρήματος ορίζεται από έναν αλγοριθμικό κανόνα και η αξιοπιστία του δικτύου αντικαθιστά την ανάγκη εμπιστοσύνης στον ανθρώπινο παράγοντα. Επομένως, η ανάπτυξη της τεχνολογίας κρυπτονομισμάτων αποτελεί πρόκληση για τις παραδοσιακές νομισματικές αρχές και τις κεντρικές τράπεζες, όπως υποδηλώνουν οι πρωτοβουλίες δημιουργίας εθνικών κρυπτονομισμάτων.

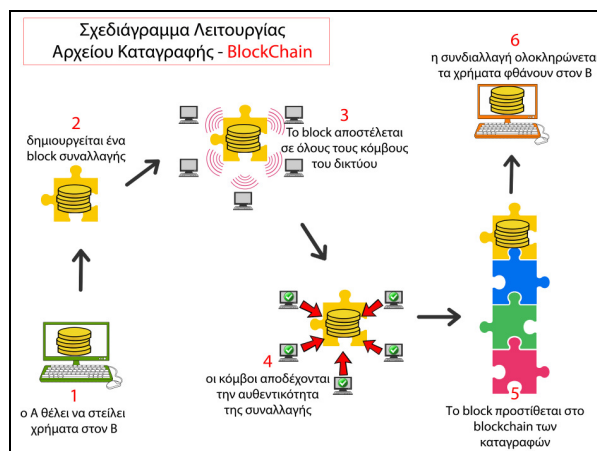
Όπως συμβαίνει μαζί με οποιαδήποτε νέα τεχνολογία, εμφανίζονται και κίνδυνοι. Στην νεοσύστατη αγορά κρυπτονομισμάτων, ένα ζήτημα ανησυχίας αφορά την ανώνυμη φύση των συναλλαγών σε ορισμένα κρυπτονομίσματα, το οποίο θα μπορούσε να επιτρέψει σε παράνομους φορείς να διεξάγουν παράνομες επιχειρήσεις, ή, χειρότερα, να δημιουργήσουν απειλή για την κοινωνία και τους θεσμούς της.

2 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ BLOCKCHAINS

2.1 Τεχνολογία Blockchain

Το **blockchain** ενός κρυπτονομίσματος είναι το κύριο δημόσιο καθολικό διαμοιρασμένο αρχείο που καταγράφει και αποθηκεύει όλες τις συναλλαγές και δραστηριότητες που έχουν διεξαχθεί στο παρελθόν, επικυρώνοντας την κυριότητα όλων των μονάδων του κρυπτονομίσματος σε οποιαδήποτε δεδομένη χρονική στιγμή. Ως το αρχείο ολόκληρου του ιστορικού συναλλαγών του κρυπτονομίσματος μέχρι σήμερα, ένα blockchain έχει ένα πεπερασμένο (finite) μήκος - που περιέχει έναν πεπερασμένο (finite) αριθμό συναλλαγών - που αυξάνεται με την πάροδο του χρόνου.

Πανομοιότυπα αντίγραφα του αρχείου blockchain αποθηκεύονται σε κάθε κόμβο του δικτύου του κρυπτονομίσματος, δηλαδή το δίκτυο αποκεντρωμένων διακομιστών, το οποίο διαχειρίζονται άτομα με γνώσεις υπολογιστών ή ομάδες ατόμων γνωστών ως miners (εξορύχων), τα οποία καταγράφουν και ελέγχουν συνεχώς τις συναλλαγές κρυπτογράφησης.



Σχεδιάγραμμα 1 - Λειτουργία Αρχείου Καταγραφής - Blockchain

Τεχνικά μια συναλλαγή κρυπτογράφησης δεν ολοκληρώνεται έως ότου προστεθεί στο blockchain, η οποία συμβαίνει συνήθως μέσα σε λίγα λεπτά. Μόλις ολοκληρωθεί η συναλλαγή, είναι συνήθως μη αναστρέψιμη. Σε αντίθεση με τους παραδοσιακούς επεξεργαστές πληρωμών, όπως το **PayPal** και τις πιστωτικές κάρτες, τα περισσότερα κρυπτονομίσματα δεν έχουν ενσωματωμένες λειτουργίες επιστροφής χρημάτων ή αντιστροφής χρέωσης, αν και ορισμένα νεότερα κρυπτονομίσματα έχουν κάποιες στοιχειώδεις δυνατότητες επιστροφής χρημάτων.

Κατά τη διάρκεια του κενού χρόνου μεταξύ της έναρξης και της οριστικοποίησης της συναλλαγής, οι μονάδες του νομίσματος δεν είναι διαθέσιμες για χρήση από κανένα μέρος. Αντ' αυτού, παραμένουν «παγωμένες». Έτσι, το blockchain αποτρέπει τη διπλή δαπάνη ή την χειραγώγηση του κώδικα ώστε να μην επιτρέπεται η αναπαραγωγή και αποστολή των ίδιων νομισματικών μονάδων σε πολλούς παραλήπτες.

2.2 Ιδιωτικά κλειδιά

Κάθε κάτοχος κρυπτογράφησης έχει ένα **ιδιωτικό κλειδί** που πιστοποιεί την ταυτότητά του και που του επιτρέπει να ανταλλάσσει μονάδες κρυπτονομίσματος. Οι χρήστες μπορούν να δημιουργήσουν τα δικά τους ιδιωτικά κλειδιά, τα οποία είναι μορφής ακέραιων αριθμών μεταξύ 1 και 78 ψηφίων, ή χρησιμοποιούν μια γεννήτρια τυχαίων αριθμών για να δημιουργήσουν ένα.

Μόλις αποκτήσουν ένα κλειδί, μπορούν να λάβουν και να δώσουν κρυπτονομίσματα. Χωρίς την χρήση του κλειδιού, ο κάτοχος δεν μπορεί να διενεργήσει συναλλαγές με τα κρυπτονομίσματα του.

Αν και αυτό κρίσιμο χαρακτηριστικό ασφαλείας είναι αυτό που περιορίζει την κλοπή και τη μη εξουσιοδοτημένη χρήση, είναι επίσης και καταστροφικό. Η απώλεια του ιδιωτικού κλειδιού είναι το ψηφιακό ισοδύναμο με ρίψη πραγματικών χρημάτων σε έναν αποτεφρωτήρα. Αν και υπάρχει η δυνατότητα να δημιουργηθεί ένα νέο ιδιωτικό κλειδί για την από την αρχή συγκέντρωση κρυπτονομισμάτων, δεν υπάρχει η δυνατότητα επανάκτησης του παλαιού κεφαλαίου. Επομένως, οι μεθοδικόι χρήστες κρυπτονομισμάτων φυλάσσουν με μανία τα ιδιωτικά τους κλειδιά, συνήθως τα αποθηκεύουν σε πολλαπλές ψηφιακές (αν και γενικά δεν είναι συνδεδεμένες στο Διαδίκτυο, για λόγους ασφαλείας) θέσεις, καθώς και σε αναλογικές (δηλαδή χαρτί).

2.3 Cryptocurrency Wallets - Πορτοφόλια Κρυπτονομισμάτων

Οι χρήστες κρυπτονομισμάτων διαθέτουν **Wallets** (πορτοφόλια) με μοναδικές πληροφορίες που τους καθιστούν ως προσωρινούς κατόχους των μονάδων κρυπτονομίσματος τους. Ενώ τα ιδιωτικά κλειδιά επιβεβαιώνουν την αυθεντικότητα μιας συναλλαγής κρυπτονομίσματος, τα πορτοφόλια μειώνουν τον κίνδυνο κλοπής για μονάδες κρυπτονομίσματος που δεν χρησιμοποιούνται. Τα πορτοφόλια που χρησιμοποιούνται για ανταλλαγές κρυπτονομισμάτων είναι κάπως ευάλωτα σε εισβολή. Για παράδειγμα, το ανταλλακτήριο bitcoin «**Mt. Gox**» με έδρα την Ιαπωνία έκλεισε και κήρυξε πτώχευση πριν λίγα χρόνια, όταν χάκερς υπεξαίρεσαν συστηματικά περισσότερα από 450 εκατομμύρια δολάρια σε bitcoin μέσω των διακομιστών της.



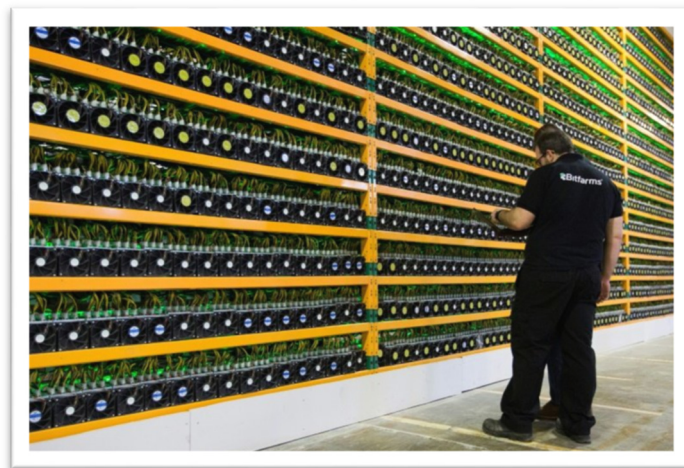
Εικόνα 2 - CryptoWallets

Τα πορτοφόλια μπορούν να αποθηκευτούν στο cloud, σε έναν εσωτερικό σκληρό δίσκο ή σε μια εξωτερική συσκευή αποθήκευσης. Ανεξάρτητα από τον τρόπο αποθήκευσης ενός πορτοφολιού, συνιστάται τουλάχιστον ένα αντίγραφο ασφαλείας. Λάβετε υπόψη ότι η δημιουργία αντιγράφων ασφαλείας ενός πορτοφολιού δεν αντιγράφει τις πραγματικές μονάδες κρυπτογράφησης, αλλά απλώς το αρχείο της ύπαρξης και της τρέχουσας ιδιοκτησίας τους.

2.4 Miners - Εξωρύχοι

Οι **miners-εξωρύχοι** χρησιμεύουν ως προστάτες αρχείων για τις κοινότητες κρυπτονομισμάτων και έμμεσοι επόπτες της αξίας των νομισμάτων. Χρησιμοποιώντας τεράστιες ποσότητες υπολογιστικής ισχύος, που συχνά συγκεντρώνονται σε φάρμες διακομιστών που ανήκουν σε συλλογικές εταιρείες εξόρυξης αποτελούμενες από δεκάδες άτομα, οι miners εξαιρετικά υψηλές τεχνολογικές μεθόδους για να επαληθεύσουν την πληρότητα, την ακρίβεια και την ασφάλεια των blockchain των νομισμάτων. Ο στόχος της διαδικασίας είναι η αναζήτηση νέων πρώτων αριθμών, η οποία απαιτεί τεράστια ποσά υπολογιστικής ισχύος.

Το έργο των miners είναι να δημιουργούνται περιοδικά νέα αντίγραφα του blockchain, προσθέτοντας πρόσφατες, προηγούμενες μη επαληθευμένες συναλλαγές που δεν περιλαμβάνονται σε κανένα προηγούμενο αντίγραφο blockchain - ολοκληρώνοντας αποτελεσματικά αυτές τις συναλλαγές. Κάθε προσθήκη είναι γνωστή ως block. Τα block αποτελούνται από όλες τις συναλλαγές που έχουν εκτελεστεί από τη δημιουργία του τελευταίου νέου αντιγράφου του blockchain.



Εικόνα 3 - Φάρμα Η/Υ για cryptomining

Ο όρος «miners» σχετίζεται με το γεγονός ότι η εργασία τους δημιουργεί κυριολεκτικά πλούτο με τη μορφή ολοκαίνουργιων μονάδων κρυπτονομίσματος. Στην πραγματικότητα, κάθε αντίγραφο blockchain που δημιουργήθηκε πρόσφατα συνοδεύεται από χρηματική επιβράβευση δύο μερών: έναν σταθερό αριθμό μονάδων κρυπτογράφησης ("mined") και έναν μεταβλητό αριθμό υπάρχουσων μονάδων που συλλέγονται από προαιρετικά τέλη συναλλαγής (συνήθως λιγότερο από 1% την αξία συναλλαγής) που πληρώνουν οι αγοραστές.

Αξίζει να σημειωθεί: Κάποτε, η εξόρυξη κρυπτονομισμάτων ήταν μια δυνητικά προσοδοφόρα δευτερεύουσα δραστηριότητα για όσους είχαν τους πόρους να επενδύσουν σε υψηλής ισχύος hardware. Σήμερα, αυτό είναι αδύνατο για τους χομπίστες. Απαιτούνται πολλά χρήματα για επένδυση σε εξοπλισμό εξόρυξης επαγγελματικής ποιότητας.

Παρόλο που οι πωλητές δεν χρεώνονται με τέλη συναλλαγής, οι miners επιτρέπεται να δίνουν προτεραιότητα στις συναλλαγές με χρέωση πριν από τις συναλλαγές χωρίς χρέωση κατά τη δημιουργία νέων blockchains, ακόμη και αν οι συναλλαγές χωρίς χρέωση ήταν πιο πρόσφατες. Αυτό δίνει στους πωλητές ένα κίνητρο να χρεώνουν τέλη συναλλαγής, καθώς πληρώνονται ταχύτερα με αυτόν τον τρόπο, οπότε είναι αρκετά συνηθισμένο οι συναλλαγές να συνοδεύονται από τέλη. Παρόλο που θεωρητικά είναι δυνατόν οι συναλλαγές ενός νέου blockchain να είναι εντελώς δωρεάν, αυτό σχεδόν ποτέ δεν συμβαίνει στην πράξη.

Μέσω των εντολών στον πηγαίο κώδικα τους, τα κρυπτονομίσματα προσαρμόζονται αυτόματα στο μέγεθος της εξορυκτικής ισχύος που λειτουργεί για τη δημιουργία νέων αντιγράφων blockchain - τα αντίγραφα γίνονται πιο δύσκολο να δημιουργηθούν καθώς η εξορυκτική ισχύς αυξάνεται και ευκολότερο να δημιουργηθεί καθώς η εξορυκτική ισχύς μειώνεται. Ο στόχος είναι να διατηρηθεί το μέσο διάστημα μεταξύ των νέων blockchain σταθερό σε ένα προκαθορισμένο επίπεδο. Για το Bitcoin, για παράδειγμα, ο χρόνος είναι 10 λεπτά.

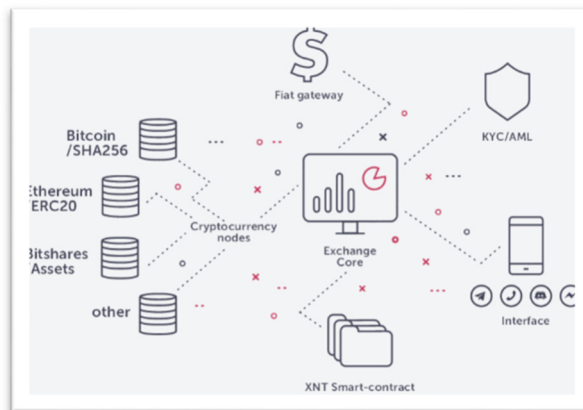
2.5 Finite Supply - Πεπερασμένη Προσφορά

Αν και η εξόρυξη παράγει περιοδικά νέες μονάδες κρυπτονομίσματος, τα περισσότερα κρυπτονομίσματα έχουν σχεδιαστεί για να έχουν μια πεπερασμένη προσφορά - βασικό εγγυητή της αξίας. Γενικά, αυτό σημαίνει ότι οι miners λαμβάνουν λιγότερες νέες μονάδες ανά νέο blockchain όσο περνά ο χρόνος. Προοδευτικά, οι miners θα λάμβανουν μόνο τα τέλη συναλλαγής για την εργασία τους, αν και αυτό δεν έχει συμβεί, ακόμα, στην πράξη και μπορεί να μην γίνει για κάποιο χρονικό διάστημα. Εάν συνεχιστούν οι τρέχουσες τάσεις, οι παρατηρητές προβλέπουν ότι η τελευταία μονάδα Bitcoin θα εξορύχθει κάποια στιγμή στα μέσα του 22ου αιώνα.

Τα κρυπτονομίσματα περιορισμένης προσφοράς είναι επομένως παρόμοια με τα πολύτιμα μέταλλα, όπως ο χρυσός, από τα νομίσματα fiat - εκ των οποίων, θεωρητικά, υπάρχουν απεριόριστα αποθέματα.

2.6 Cryptocurrency Exchanges - Ανταλλαγές Κρυπτονομισμάτων

Πολλά από τα κρυπτονομίσματα που χρησιμοποιούνται λιγότερο μπορούν να ανταλλαχθούν μόνο μέσω ιδιωτικών, peer-to-peer μεταφορών, που σημαίνει ότι είναι δύσκολο να εκτιμηθούν σε σχέση με άλλα νομίσματα τόσο crypto όσο και fiat.



Εικόνα 4 - Ανταλλαγή Κρυπτονομισμάτων

Τα πιο δημοφιλή κρυπτονομίσματα, όπως το Bitcoin και το Ripple, ανταλλάσσονται σε ειδικά ανταλλακτήρια παρόμοια με αυτά για τις ανταλλαγές συναλλάγματος για νομίσματα fiat. (Το μη υπάρχον πλέον Mt. Gox είναι ένα παράδειγμα.) Αυτές οι πλατφόρμες επιτρέπουν στους κατόχους να ανταλλάσσουν τα κρυπτονομίσματα τους με μεγάλα νομίσματα fiat, όπως το δολάριο ΗΠΑ και το ευρώ και άλλα κρυπτονομίσματα (συμπεριλαμβανομένων των λιγότερο δημοφιλών νομισμάτων). Σε αντάλλαγμα για τις υπηρεσίες τους, λαμβάνουν μια μικρή προμήθεια της αξίας κάθε συναλλαγής - συνήθως λιγότερο από 1%.

Η ανάγκη για ανταλλαγές κρυπτονομισμάτων οδήγησαν στην δημιουργία των liquid markets⁴ (ρευστών αγορών) για δημοφιλή κρυπτονομίσματα και στον καθορισμό της αξίας τους σε σχέση με τα παραδοσιακά νομίσματα. Ωστόσο, η τιμή συναλλάγματος μπορεί να εξακολουθεί να είναι εξαιρετικά ασταθής. Η συναλλαγματική ισοτιμία του δολαρίου ΗΠΑ του Bitcoin μειώθηκε κατά περισσότερο από 50% μετά την κατάρρευση του Mt Gox και, στη συνέχεια, αυξήθηκε περίπου δέκα φορές κατά τη διάρκεια του 2017 καθώς εξελίχθηκε η ζήτηση κρυπτονομισμάτων.

⁴ liquid market ονομάζεται ένα ανταλλακτήριο με πολλούς διαθέσιμους αγοραστές και πωλητές και συγκριτικά χαμηλό κόστος συναλλαγής. Σε μια liquid market, είναι εύκολο να εκτελέσετε μια συναλλαγή γρήγορα και σε επιθυμητή τιμή επειδή υπάρχουν πολλοί αγοραστές και πωλητές και το προϊόν που ανταλλάσσεται είναι τυποποιημένο και έχει υψηλή ζήτηση. Σε μια liquid market παρά τις καθημερινές αλλαγές στην προσφορά και τη ζήτηση, η διαφορά μεταξύ του τι ο αγοραστής θέλει να πληρώσει και του τι θα προσφέρουν οι πωλητές παραμένει σχετικά μικρό. (από την investopedia.com)

3 ΚΑΤΗΓΟΡΙΕΣ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

Σήμερα υπάρχει ένας μεγάλος αριθμός κρυπτονομισμάτων που η λειτουργία τους βασίζεται σε διαφορετικές εκδόσεις της αρχικής τεχνολογίας blockchain που εισήγαγε το Bitcoin. Για να γίνει κατανοητός ο τρόπος που λειτουργούν απαιτείται προσεκτική μελέτη και αρκετά εκτεταμένη κατανόηση του σχεδιασμού και της φιλοσοφίας τους.

Σε πρώτη προσέγγιση αυτά μπορούν να κατανεμηθούν σε τέσσερις βασικούς τύπους κρυπτογράφησης:

- Κρυπτονομίσματα με Αποδεικτικό εργασίας (Proof of Work - PoW)
- Κρυπτονομίσματα με Αποδεικτικό λειτουργίας (Proof of Stake - PoS)
- Κρυπτονομίσματα - Κουπόνια (Tokens)
- Κρυπτονομίσματα Σταθερής Αξίας (Stablecoins)

3.1 Κρυπτονομίσματα με Αποδεικτικό εργασίας (PoW)

Ο πρώτος τύπος κρυπτογράφησης είναι αυτός που ξεκίνησε με το Bitcoin και βασίζεται στην τεχνολογία blockchain που χρησιμοποιεί μια λειτουργία γνωστή ως αποδεικτικό εργασίας (PoW) για την επεξεργασία συναλλαγών. Για να γίνει αντιληπτός ο τρόπος λειτουργίας πρέπει αρχικά να ορισθεί το τι είναι το blockchain.

Με απλά λόγια, το blockchain είναι ένα κατανεμημένο αρχείο καταγραφής συναλλαγών. Σε ένα δίκτυο blockchain, κάθε υπολογιστής (κόμβος) διατηρεί ένα πλήρες αντίγραφο του κατανεμημένου αρχείου καταγραφής συναλλαγών. Είναι σαν να μοιράζεσαι ένα αντίγραφο ενός μητρώου επιταγών με πολλά άτομα - εκτός από το ότι κανένα μεμονωμένο μέλος δεν μπορεί να προσθέσει κάτι μόνο σε αυτό το μητρώο. Για να προστεθεί μια συναλλαγή, οι κόμβοι ανταγωνίζονται για την επίλυση ενός σύνθετου κρυπτογραφικού προβλήματος που αντιπροσωπεύει τα δεδομένα που θα προστεθούν. Ο πρώτος που λύνει το πρόβλημα μεταδίδει την απάντηση στο υπόλοιπο δίκτυο για επαλήθευση. Αυτή η διαδικασία είναι αυτό που έχει γίνει κοινώς γνωστό ως εξόρυξη (mining)⁵ επειδή ο κόμβος που παίρνει τη σωστή απάντηση παίρνει πρώτα μια ανταμοιβή από το δίκτυο. Είναι ένας ασφαλής και αυτοελεγχόμενος τρόπος τήρησης αξιόπιστων αρχείων.

Η ασφάλεια της τεχνολογίας blockchain, εκτός από τη εφαρμογή της στην λειτουργία κρυπτονομισμάτων, έχει εισαχθεί και σε άλλες βιομηχανίες άλλων ειδών. Η Walmart το χρησιμοποιεί για να διαχειριστεί την αλυσίδα εφοδιασμού προϊόντων της, η Maersk το χρησιμοποιεί για να παρακολουθεί εμπορευματοκιβώτια μεταφοράς καθώς ταξιδεύουν στον κόσμο, και ακόμη και η βιομηχανία διαμαντιών το έχει προσαρμόσει για να παρακολουθεί πολύτιμους λίθους καθώς κινούνται μέσω της αλυσίδας εμπορίου.

3.1.1 Πλεονεκτήματα των κρυπτονομισμάτων PoW

Αυτή η διαδικασία, όπως αναφέραμε, είναι το έργο που αντιστοιχεί στην απόδειξη της εργασίας. Η απόδειξη είναι η διαδικασία παρακολούθησης και επαλήθευσης από το υπόλοιπο δίκτυο. Αυτό διατηρεί το πλήρες καθολικό έγκυρο και συμφωνημένο από όλα τα μέρη. Είναι

⁵ Η εξόρυξη κρυπτονομισμάτων - cryptocoin mining είναι η διαδικασία με την οποία νέα κρυπτονομίσματα βγαίνουν σε κυκλοφορία, αλλά είναι επίσης ένα κρίσιμο συστατικό της συντήρησης και ανάπτυξης του blockchain. Εκτελείται χρησιμοποιώντας υπερσύγχρονους υπολογιστές που επιλύουν εξαιρετικά περίπλοκα υπολογιστικά μαθηματικά προβλήματα.

ένα σύστημα που είναι εγγενώς ασφαλές και ανθεκτικό, διότι ο μόνος γνωστός τρόπος παραβίασης θα ήταν μόνο αν κάποιος μπορούσε να ελέγχει περισσότερους από τους μισούς κόμβους (καθιστώντας δυνατή την πραγματοποίηση αλλαγών κατά βούληση).

3.1.2 Μειονεκτήματα των κρυπτονομισμάτων PoW

Ένα σημαντικό μειονέκτημα ενός συστήματος blockchain PoW είναι η μεγάλη υπολογιστική ισχύς που χρειάζεται για να λειτουργήσει. Δεδομένου ότι κάθε κόμβος πρέπει να λειτουργεί σε κάθε συναλλαγή, η απλή προσθήκη κόμβων δεν επηρεάζει τη συνολική ταχύτητα ή την απόδοση του δικτύου. Για αυτόν τον λόγο, τα συστήματα PoW δεν κλιμακώνονται ομαλά και είναι κάπως αναποτελεσματικά. Μία μελέτη διαπίστωσε ακόμη ότι το δίκτυο blockchain μόνο καταναλώνει την ίδια ποσότητα ηλεκτρικής ενέργειας με την πόλη του Λας Βέγκας, το οποίο μπορεί να αποτελεί εμπόδιο στη συνεχιζόμενη κυριαρχία της μεθόδου στην αγορά κρυπτογράφησης.

Ένα ακόμα μεγαλύτερο μειονέκτημα που ενέκυψε τα τελευταία χρόνια, πηγάζει από το γεγονός ότι προκειμένου να κερδίζουν περισσότερο, οι κόμβοι συνεργάζονται δημιουργώντας μεγάλες ομάδες εξόρυξης (mining pools)⁶, ώστε με την συνδυαστική υπολογιστική ισχύ τους να εκτελούν γρηγορότερα τις εργασίες mining και να κερδίζουν περισσότερο.

Με την τάση να δημιουργούνται όλο και μεγαλύτερα pools είναι πολύ εύκολο να υπάρξει στο μέλλον τέτοιο που να ελέγχει το 51% των κόμβων, άρα διακυβεύεται η αξιοπιστία των συναλλαγών.

3.1.3 Κρυπτονομίσματα που χρησιμοποιούν PoW


































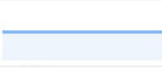




Αυτή τη στιγμή, τα δύο μεγάλα κρυπτονομίσματα που βασίζονται στην τεχνολογία POW είναι τα: Bitcoin και Ethereum. Τυγχάνει επίσης να έχουν την μεγαλύτερη εμπορική αξία.

Μαζί, αντιστοιχούν σε κεφαλαιοποίηση περίπου 150 δισεκατομμυρίων δολαρίων, αριθμός που επισκιάζει τον υπόλοιπο ανταγωνισμό. Ως η κληρονομιά της τεχνολογίας στον κόσμο της κρυπτογράφησης, το PoW έχει αποδειχθεί σταθερό και ανθεκτικό, οδηγώντας τα δύο προαναφερθέντα νομίσματα σε αστρονομικές τιμές τα τελευταία χρόνια.

Τα κυριότερα κρυπτονομίσματα που χρησιμοποιούν τεχνολογία PoW απεικονίζονται στο παρακάτω πίνακα. Απεικονίζονται επίσης το σύμβολο, η τρέχουσα αξία, η κεφαλαιοποίηση και άλλες πληροφορίες.

⁶ Mining Pool, Ορισμός: Δίκτυο συνεργαζόμενων κόμβων που συνδυάζουν την υπολογιστική ισχύ τους σε ένα δίκτυο, ώστε να κερδίζουν την ανταμοιβή από την επίλυση των γρίφων-ενημέρωσης των blocks. Τα «κέρδη» τα μοιράζονται ισόποσα όλοι οι συμμετέχοντες ανάλογα με το ποσό εργασίας που έχουν συνεισφέρει στην εύρεση του block. Τα Mining Pools άρχισαν να εμφανίζονται όταν η επίλυση γρίφων άρχισε να γίνεται πολύ δύσκολη για τους κόμβους με μικρή υπολογιστική ισχύ, σε σημείο που ποτέ δεν κέρδιζαν τίποτα από την συμμετοχή τους στο δίκτυο.

Το απόσπασμα λήφθηκε από τον δικτυακό τόπο coincodex.com στις 13.05.2021

#	NAME	PRICE	24H CHANGE		MARKET CAP ↓	24H VOLUME	CIRCULATING SUPPLY	ACTIONS
2	 BTC Bitcoin	\$ 51,220	-10.25%		\$ 958.27B	\$ 142.20B	18.71M	...
3	 ETH Ethereum	\$ 4,006.02	-7.02%		\$ 464.11B	\$ 117.03B	115.85M	...
4	 DOGE Dogecoin	\$ 0.437580	-14.71%		\$ 56.70B	\$ 11.73B	129.57B	...
5	 BCH Bitcoin Cash	\$ 1,336.57	-12.11%		\$ 25.04B	\$ 7.84B	18.74M	...
6	 LTC Litecoin	\$ 330.78	-13.02%		\$ 22.08B	\$ 12.24B	66.75M	...
7	 ETC Ethereum Classic	\$ 93.13	-14.95%		\$ 10.83B	\$ 11.45B	116.31M	...
8	 XMR Monero	\$ 418.70	-7.05%		\$ 7.50B	\$ 603.37M	17.91M	...
9	 DASH Dash	\$ 382.00	-7.62%		\$ 3.87B	\$ 1.61B	10.13M	...
10	 ZEC Zcash	\$ 316.67	-5.68%		\$ 3.72B	\$ 3.57B	11.76M	...
11	 DCR Decred	\$ 206.10	-8.00%		\$ 2.66B	\$ 25.57M	12.92M	...
12	 DGB DigiByte	\$ 0.123978	-11.38%		\$ 1.77B	\$ 141.18M	14.30B	...
13	 SC Siacoin	\$ 0.032728	-12.87%		\$ 1.56B	\$ 183.83M	47.79B	...
14	 RVN Ravencoin	\$ 0.143163	-10.29%		\$ 1.25B	\$ 140.83M	8.76B	...
15	 ZEN Horizen	\$ 148.68	-2.64%		\$ 1.17B	\$ 371.95M	7.89M	...
16	 BCD Bitcoin Diamond	\$ 5.09	-17.54%		\$ 949.25M	\$ 60.31M	186.49M	...
17	 CKB Nervos Network	\$ 0.026786	-15.69%		\$ 704.17M	\$ 64.44M	26.29B	...
18	 BIXB BixbyCoin	\$ 126.25	0.00%		\$ 378.56M	\$ 0.00	3.00M	...
19	 KMD Komodo	\$ 2.63	-17.03%		\$ 330.82M	\$ 19.43M	125.79M	...
20	 BTM Bytom	\$ 0.215863	6.00%		\$ 308.56M	\$ 152.26M	1.43B	...

Πίνακας 1 Κρυπτονομίσματα Τεχνολογίας POW

3.2 Κρυπτονομίσματα με Αποδεικτικό λειτουργίας (PoS)

Το κύριο πρόβλημα με τα συστήματα PoW, όπως είδαμε, είναι το γεγονός ότι δεν αναπτύσσονται καλά. Για να ξεπεραστεί αυτό το πρόβλημα, αναπτύχθηκε ένα διαφορετικό μοντέλο συναίνεσης για το blockchain που επιτρέπει σε μικρότερες ομάδες κόμβων να επικυρώσουν τις συναλλαγές. Είναι γνωστό ως Αποδεικτικό λειτουργίας (PoS) και διασφαλίζει την ασφάλεια με θεμελιωδώς διαφορετικό τρόπο από το PoW.

Σε ένα σύστημα PoS, δεν χρειάζεται κάθε κόμβος να επικυρώνει κάθε συναλλαγή. Αντ' αυτού, οι συμμετέχοντες κόμβοι πρέπει να χρησιμοποιούν το δικό τους κεφάλαιο κρυπτονομισμάτων

ως εγγύηση για να συμμετάσχουν σε μια ομάδα επικύρωσης συναλλαγών. Αυτό το κεφάλαιο είναι απ' όπου η διαδικασία παίρνει το όνομά της. Κάθε κόμβος που προσπαθεί να εξαπατήσει ή να μεταβιάσει αναληθή δεδομένα στο σύστημα, χάνει αυτόματα το κεφάλαιό του ως ποινή. Όσοι παίζουν με τους κανόνες λαμβάνουν τόκους στις καταθέσεις τους ως ανταμοιβή για την εργασία τους. Σε ένα blockchain PoS, αυτό που κρατά τα πράγματα ασφαλή και δίκαια είναι το σύστημα κινήτρων.

3.2.1 Πλεονεκτήματα των κρυπτονομισμάτων PoS

το κύριο πλεονέκτημα του μπλοκ PoS είναι η ταχύτητα επεξεργασίας. Δεδομένου ότι οι συμμετέχοντες κόμβοι μπορούν να χωριστούν σε μικρότερες ομάδες για να εργαστούν σε μεμονωμένες συναλλαγές, τα κρυπτονομίσματα που το χρησιμοποιούν αποκτούν τη δυνατότητα να λειτουργούν χρησιμοποιώντας παράλληλες συναλλαγές που σημαίνει χαμηλότερο κόστος επεξεργασίας. Η αξία αυτής της πρακτικής είναι ανδιαμφισβήτητη.

Ακόμα και το Ethereum, ένας από τους κύριους πυλώνες του μπλοκ PoW, βρίσκεται ήδη στη διαδικασία της μετάβασης στο μπλοκ PoS. Θεωρείται ότι είναι ο μόνος τρόπος για να αποφευχθεί η συμφόρηση που θα φέρουν τα συνεχώς επεκτεινόμενα συστήματα PoW.

3.2.2 Μειονεκτήματα των κρυπτονομισμάτων PoS

Τα σημαντικότερα μειονεκτήματα των PoS blockchains είναι ότι θεωρητικά είναι λιγότερο ασφαλή από τα συστήματα PoW και διατρέχουν τον κίνδυνο να γίνουν πολύ λιγότερο αποκεντρωμένα με την πάροδο του χρόνου.

Από την πλευρά της ασφάλειας, η απειλή ενός συμμετέχοντα να χάσει το κεφάλαιο του λειτουργεί ως αποτρεπτικό μόνο εάν το κεφάλαιο του είναι μεγαλύτερο από αυτό που θα κέρδιζε παραβιάζοντας τους κανόνες. Εάν, για παράδειγμα, ένας κόμβος πετύχαινε να προσθέσει μια δόλια συναλλαγή στο blockchain με ένα μεγάλο ποσό το κίνητρο για να λειτουργήσει νόμιμα θα εξαφανιζόταν. Το άλλο πρόβλημα σχετίζεται με το πόσα κρυπτονομίσματα PoS ελέγχει κάθε κόμβος. Όσο μεγαλύτερες είναι οι συμμετοχές τους, σε τόσο περισσότερες συναλλαγές μπορούν να εμπλακούν και τόσο περισσότερο τόκο συλλέγουν. Αυτό θα μπορούσε να δημιουργήσει ένα αποτέλεσμα χιονοστιβάδας όπου οι πιο ισχυροί κόμβοι γίνονται ακόμη πιο ισχυροί με την πάροδο του χρόνου και τελικά να φθάσουν να κυριαρχήσουν στο ίδιο το δίκτυο. Δεδομένου ότι ένα από τα βασικά πλεονεκτήματα των κρυπτονομισμάτων είναι ότι δεν βρίσκονται υπό κεντρικό έλεγχο, αυτό θα μπορούσε να αποδειχθεί ότι είναι η αχίλλειος πτέρνα των κρυπτονομισμάτων PoS κάποια στιγμή στο μέλλον.












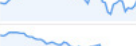





















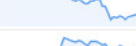



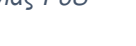
3.2.3 Κρυπτονομίσματα που χρησιμοποιούν PoS

Αυτήν τη στιγμή, υπάρχουν πολλά κρυπτονομίσματα που βασίζονται σε μπλοκ PoS. Τα πιο σημαντικά είναι τα Eos, Dash και Tron.

Αν και είναι μικρότερης αξίας σε σύγκριση με τα μεγάλα PoW, αυτό πρόκειται να αλλάξει σε μεγάλο βαθμό. Αυτό θα συμβεί επειδή, όπως αναφέρθηκε προηγουμένως, το Ethereum πρόκειται να ενταχθεί στις τάξεις τους μέσα στο 2021. Αξίζει επίσης να σημειωθεί ότι η συντριπτική πλειονότητα των νέων και προγραμματισμένων κρυπτονομισμάτων βασίζεται στο PoS, καθώς θεωρείται ως το μέλλον της τεχνολογίας blockchain.

Τα κυριότερα κρυπτονομίσματα που χρησιμοποιούν τεχνολογία PoS απεικονίζονται στο παρακάτω πίνακα. Απεικονίζονται επίσης το σύμβολο, η τρέχουσα αξία, η κεφαλοποίηση και άλλες πληροφορίες.

Το απόσπασμα λήφθηκε από τον δικτυακό τόπο [coincodex.com](https://www.coincodex.com) στις 13.05.2021

#	NAME	PRICE	24H CHANGE		MARKET CAP ↓	24H VOLUME	CIRCULATING SUPPLY	ACTIONS
2	 ADA Cardano	\$ 1.73	-3.42%		\$ 54.43B	\$ 5.37B	31.46B	...
3	 EOS EOS	\$ 11.44	-14.10%		\$ 10.91B	\$ 19.12B	953.34M	...
4	 TRX TRON	\$ 0.125807	-10.54%		\$ 8.39B	\$ 4.98B	66.67B	...
5	 ATOM Cosmos	\$ 25.01	-7.52%		\$ 5.27B	\$ 855.84M	210.77M	...
6	 XTZ Tezos	\$ 6.31	-10.82%		\$ 5.25B	\$ 804.25M	831.50M	...
7	 RUNE THORChain	\$ 18.24	-6.29%		\$ 4.38B	\$ 392.24M	239.90M	...
8	 ALGO Algorand	\$ 1.38	-5.78%		\$ 4.19B	\$ 470.31M	3.03B	...
9	 WAVES Waves	\$ 33.47	-6.48%		\$ 3.52B	\$ 736.09M	105.09M	...
10	 DCR Decred	\$ 205.42	-7.60%		\$ 2.65B	\$ 24.72M	12.92M	...
11	 QTUM Qtum	\$ 21.52	-14.45%		\$ 2.12B	\$ 1.25B	98.36M	...
12	 ONT Ontology	\$ 2.26	-11.56%		\$ 1.85B	\$ 1.20B	819.34M	...
13	 ICX iCIX	\$ 2.21	-11.92%		\$ 1.38B	\$ 231.39M	622.55M	...
14	 LSK Lisk	\$ 7.43	-14.82%		\$ 951.27M	\$ 114.42M	128.03M	...
15	 STEEM Steam	\$ 0.916794	-17.96%		\$ 341.75M	\$ 8.35M	372.76M	...
16	 ARDR Ardor	\$ 0.339751	-14.83%		\$ 339.41M	\$ 16.48M	999.00M	...
17	 WAN Wanchain	\$ 1.98	-10.00%		\$ 334.68M	\$ 22.59M	169.03M	...
18	 BTS BitShares	\$ 0.104237	-11.02%		\$ 312.18M	\$ 80.77M	2.99B	...
19	 ARK Ark	\$ 1.84	-18.32%		\$ 237.57M	\$ 7.56M	129.12M	...
20	 10SET Tenset	\$ 2.83	20.25%		\$ 232.10M	\$ 1.47M	82.02M	...

Πίνακας 2 Κρυπτονομίσματα Τεχνολογίας PoS

3.3 Κρυπτονομίσματα Tokens - Κουπόνια

Οι δύο τύποι κρυπτογράφησης που έχουμε καλύψει μέχρι στιγμής διακρίνονται μεταξύ τους από την τεχνολογία που χρησιμοποιούν. Υπάρχουν, όμως, επίσης διαφορές στους στόχους που είναι επιθυμητοί κατά την δημιουργία κάποιου κρυπτονομίσματος. Αυτό μας φέρνει στον επόμενο σημαντικό τύπο κρυπτογράφησης, τα κουπόνια. Τα κουπόνια διαφέρουν από τα παραδοσιακά κρυπτονομίσματα στο ότι δεν προορίζονται να χρησιμοποιηθούν ως νόμισμα γενικής χρήσης. Δημιουργούνται επίσης πάνω από υπάρχοντα blockchain, όπως το Ethereum, και δεν υπάρχουν ως αυτόνομα συστήματα. Είναι κάτι σαν τις μάρκες που χρησιμοποιείτε για να τοποθετήσετε στοιχήματα σε ένα καζίνο. Ενώ αντιπροσωπεύουν μετρητά ή άλλα περιουσιακά στοιχεία αξίας, μπορούν να χρησιμοποιηθούν μόνο στο συγκεκριμένο καζίνο που τα εξέδωσε.

Για παράδειγμα, η διαδικτυακή υπηρεσία ροής μουσικής Musicoin επιτρέπει την άμεση πληρωμή από ακροατές σε καλλιτέχνες χρησιμοποιώντας ένα νομισμα-κουπόνι που ονομάζεται Music που χρησιμοποιεί το Ethereum και δεν μπορεί να μετατραπεί απευθείας σε νόμισμα fiat. Αντ 'αυτού, οι καλλιτέχνες που πληρώνονται με αυτόν τον τρόπο πρέπει να μετατρέψουν τα νομίσματα τους σε τυπικά κρυπτονομίσματα όπως το Bitcoin ή το Ethereum προτού εξαργυρώσουν τα κέρδη τους.

3.3.1 Πλεονεκτήματα των κρυπτονομισμάτων κουπονιών

Το εύρος εφαρμογής τέτοιων νομισμάτων είναι πολύ μεγάλο. Δεδομένου ότι μπορούν να χρησιμοποιηθούν ως μονάδων αξίας, είναι ιδανικά για εφαρμογές σε περιπτώσεις που απαιτούνται πληρωμές χωρίς ρευστό.

Το real estate θα μπορούσε να είναι μια τέτοια εφαρμογή. Αν τα ποσοστά ιδιοκτησίας ακινήτων αντιστοιχηθούν με κρυπτο-κουπόνια, οι ιδιοκτήτες θα μπορούν να τα ανταλλάξουν σαν να ανταλλάσσουν μετοχές ή ομόλογα. Τα κρυπτο-κουπόνια χρησιμοποιούνται επίσης σε αγορές ενέργειας και άλλες.

3.3.2 Μειονεκτήματα των κρυπτονομισμάτων κουπονιών

Όταν τα κρυπτο-κουπόνια χρησιμοποιούνται ως απλό μέσο για συναλλαγή, λειτουργούν αρκετά καλά. Υπάρχει, όμως, πρόβλημα, στην μετατροπή τους σε πραγματική αξία. Όπως αναφέρθηκε προηγουμένως, δεν μπορούν να ανταλλαχθούν απευθείας με νόμισμα fiat, επομένως είναι δύσκολο να καθορισθεί η ακριβής αξία τους ανά πάσα στιγμή. Επιπλέον, είναι άρρηκτα συνδεδεμένα με το υποκείμενο blockchain στο οποίο βασίζονται. Εάν αυτό το blockchain καταρρεύσει, θα επηρεάσει και όλα τα αντίστοιχα κρυπτο-κουπόνια.

Επίσης, εάν το υποκείμενο blockchain κάνει μια τεχνική αλλαγή (όπως η προαναφερθείσα Ethereum μετάβαση σε PoS), μπορεί να έχει μεγάλες επιπτώσεις σε όλα τα σχετικά κρυπτο-κουπόνια.

3.3.3 Σημαντικά κρυπτο-κουπόνια

Δύο αξιοσημείωτα κρυπτο-κουπόνια είναι τα BAT και Tether.

Το BAT, το οποίο σημαίνει το Basic Attention Token, χρησιμοποιείται ως σύστημα πληρωμών στο πρόγραμμα περιήγησης Web Brave που κυκλοφόρησε πρόσφατα. Αποτελεί τρόπο αποζημίωσης των χρηστών για την παρακολούθηση διαδικτυακών διαφημίσεων.

Από την άλλη πλευρά, το Tether, είναι ένα κρυπτο-κουπόνι του οποίου η αξία παραμένει σε μια τιμή που είναι ισοδύναμη, ανά πάσα στιγμή, με το δολάριο ΗΠΑ. Είναι επίσης μέλος της επόμενης ομάδας κρυπτονομισμάτων τα stablecoins-κρυπτονομίσματα σταθερής αξίας.

Τα κυριότερα κρυπτονομίσματα που χρησιμοποιούν τεχνολογία Token απεικονίζονται στο παρακάτω πίνακα. Απεικονίζονται επίσης το σύμβολο, η τρέχουσα αξία, η κεφαλοποίηση και άλλες πληροφορίες.

Το απόσπασμα λήφθηκε από τον δικτυακό τόπο coinmarketcap.com στις 13.05.2021

#	Όνομα	Τιμή	24h %	7d %	Κεφαλαιοποίηση Αγοράς	Volume(24h)	Κυκλοφοριακή Προσφορά	Τελευταίος 7 Ημέρες
1	Tether USDT <small>Αγορά</small>	€0.8289	- 0.01%	- 0.01%	€47,878,177,547	€185,372,477,482 223,616,552,589 USDT	57,755,893,177 USDT	
2	Uniswap UNI	€31.65	- 10.05%	- 9.52%	€17,609,357,551	€1,345,289,466 42,749,077 UNI	559,570,115 UNI	
3	Chainlink LINK	€35.60	- 11.49%	- 9.25%	€15,072,447,212	€2,591,027,360 73,061,220 LINK	425,009,554 LINK	
4	USD Coin USDC	€0.8289	- 0.03%	- 0.01%	€11,921,436,806	€3,291,971,661 3,970,920,022 USDC	14,380,157,844 USDC	
5	Wrapped Bitcoin WBTC	€41,338.42	- 12.78%	- 12.81%	€7,207,790,283	€457,252,668 11,074 WBTC	174,565 WBTC	
6	Binance USD BUSD	€0.8291	- 0.02%	- 0.01%	€6,465,025,851	€10,338,345,364 12,471,246,520 BUSD	7,798,823,536 BUSD	
7	SHIBA INU SHIB	€0.00001527	- 40.86%	- 1016.51%	€6,004,957,758	€5,787,528,113 380,501,086,079,220 SHIB	394,796,000,000,000 SHIB	
8	Aave AAVE	€468.10	- 9.50%	- 22.47%	€5,923,559,737	€3,035,942,467 6,532,269 AAVE	12,745,395 AAVE	
9	Polygon MATIC	€0.8989	- 3.48%	- 38.15%	€5,428,288,683	€2,069,175,335 2,321,024,285 MATIC	6,088,990,937 MATIC	
10	Huobi Token HT	€28.54	- 3.27%	- 41.87%	€5,090,373,268	€2,582,761,405 90,966,363 HT	179,285,916 HT	
11	FTX Token FTT	€47.02	- 8.88%	- 1.34%	€4,418,906,272	€267,996,747 5,721,931 FTT	94,346,958 FTT	
12	PancakeSwap CAKE	€25.97	- 12.01%	- 16.33%	€4,282,058,769	€620,694,153 23,902,849 CAKE	164,900,129 CAKE	

Πίνακας 3 Κρυπτονομίσματα Τεχνολογίας Token

3.4 Stablecoins - Κρυπτονομίσματα σταθερής αξίας

Όπως υποδηλώνει το όνομα, τα stablecoins είναι κρυπτονομίσματα που δημιουργήθηκαν με σκοπό την παροχή αξιόπιστης αποταμίευσης. Δημιουργήθηκαν επειδή η αξία των εμπορικών κρυπτονομισμάτων όπως το Bitcoin και το Ether έχει μεγάλες μεταβολές σε μικρά διαστήματα, καθιστώντας τα δύσκολα στη διαχείριση. Αυτός είναι ο λόγος που ορισμένοι επενδυτές έχουν γίνει δισεκατομμυριούχοι σε μια νύχτα και μέχρι την άλλη μέρα τα κέρδη τους έχουν χαθεί.

Τα σταθερά νομίσματα αντιπροσωπεύουν κάτι υβριδικό μεταξύ των κρυπτοκουπονιών και των τυπικών κρυπτονομισμάτων, δεδομένου ότι βασίζονται σε υπάρχουσες blockchain, αλλά μπορούν να ανταλλαχθούν με νόμισμα fiat. Από κατασκευής επιτρέπουν καθημερινές, συνεχείς συναλλαγές που είναι απαλλαγμένες από μεταβολές της αξίας τους. Αυτό το επιτυγχάνουν συνδέοντας την αξία τους με ένα ή περισσότερα νομίσματα fiat και διατηρώντας αποθεματικά αυτών των νομισμάτων ως εγγύηση της αξίας τους.

3.4.1 Πλεονεκτήματα των κρυπτονομισμάτων Stablecoins

Το σοβαρότερο εμπόδιο στην χρήση των κρυπτονομισμάτων στην ευρύτερη παγκόσμια οικονομία είναι η αστάθεια τους. Αυτό κατέστησε δύσκολο για τις τράπεζες να τα χρησιμοποιούν, για τους λιανοπωλητές να τα αποδεχθούν ως πληρωμή για αγαθά και υπηρεσίες και για τους ιδιώτες να τα χρησιμοποιήσουν ως αποταμιευτικό μέσο.

Τα σταθερά νομίσματα όπως το Tether (το οποίο είναι συνδεδεμένο με το Δολάριο ΗΠΑ) χρησιμοποιούνται πλέον ως αποταμιευτικό μέσο για τους επενδυτές – ακριβώς όπως ένα νόμισμα fiat. Χωρίς αυτά, θα ήταν πολύ δύσκολο για τους επενδυτές να αγοράσουν και να πουλήσουν κρυπτονομίσματα λόγω της ανάγκης να τα μετατρέπουν σε εμπορικό νόμισμα και να έχουν απώλειες.

3.4.2 Μειονεκτήματα των κρυπτονομισμάτων Stablecoins

Το σημαντικότερο μειονέκτημα των σταθερών νομισμάτων είναι το γεγονός ότι οι κάτοχοι τους πρέπει να βασίζονται στις εταιρείες που τα διαχειρίζονται και που διατηρούν τα ρευστά διαθέσιμα που εγγυόνται την αξία τους.

Εφόσον δεν υπάρχει κάποια κρατική εγγύηση κάτω από αυτούς, είναι πολύ επίφοβο να υπάρξει κατάρρευση του συστήματος λόγω κακής διαχείρισης ή ακόμα χειρότερα υπεξαίρεση κεφαλαίων.

3.4.3 Σημαντικά Stablecoins

Εκτός από το Tether, το οποίο αντιπροσωπεύει σχεδόν το 90% του όγκου συναλλαγών, υπάρχουν μερικά ακόμη stablecoins στην αγορά σήμερα.

Τα πιο γνωστά μεταξύ αυτών περιλαμβάνουν τα Paxos, Gemini και TrueUSD.

Υπάρχει, ωστόσο, ένα άλλο stablecoin που έχει τα φώτα της δημοσιότητας επάνω του τους τελευταίους μήνες. Είναι το Libra, το stablecoin που υποστηρίζεται από το Facebook που αν ξεπεράσει κάποια νομικά εμπόδια, θα μπορούσε να γίνει το κυρίαρχο stablecoin σχεδόν από την μια μέρα στην άλλη.

Λίγα λόγια για το Libra











Το Libra είναι ένα σταθερό κρυπτονόμισμα (StableCoin) που δημιουργήθηκε από το Facebook και προορίζεται να χρησιμοποιηθεί ως ένα απλό μέσο συναλλαγής χαμηλών χρεώσεων για χρήση σε όλο τον κόσμο.

Υποστηρίζεται από ένα απόθεμα με περιουσιακά στοιχεία, τα οποία περιλαμβάνουν σημαντικά νομίσματα και αριθμό κρατικών χρεογράφων που εγγυόνται την σταθερότητα του κρυπτονομίσματος.

Η κρυπτογράφηση και το σχετικό αποθεματικό της θα διαχειρίζονται η Libra Association, μια ανεξάρτητη μη κερδοσκοπική ένωση που αποτελείται από τους ιδρυτές του νομίσματος.

Τα κυριότερα κρυπτονομίσματα που χρησιμοποιούν τεχνολογία Stablecoins απεικονίζονται στο παρακάτω πίνακα. Απεικονίζονται επίσης το σύμβολο, η τρέχουσα αξία, η κεφαλοποίηση και άλλες πληροφορίες.

Το απόσπασμα λήφθηκε από τον δικτυακό τόπο cryptoslate.com στις 13.05.2021

#	Name	Marketcap	Price	24h Volume	Blockchain	Change 24h	Change 7d
1	 Tether #4 USDT	\$57.76B	\$1.00004	\$204,638,227,885	Omni	+0.01%	-0.02%
2	 USD Coin #14 USDC	\$14.38B	\$1.00013	\$3,639,769,151	Ethereum	+0.03%	+0.01%
3	 Binance USD #23 BUSD	\$7.8B	\$1.00005	\$11,053,323,976	Ethereum	+0.02%	-0.01%
4	 Dai #40 DAI	\$4.81B	\$1.00017	\$867,536,107	Ethereum	-0.08%	-0.03%
5	 TerraUSD #85 UST	\$2.09B	\$1.00141	\$75,191,842	Ethereum	+0.16%	+0.35%
6	 Paxos Standard #91 PAX	\$1.18B	\$0.99850	\$134,068,984	Ethereum	-0.02%	-0.03%
7	 TrueUSD #52 TUSD	\$1.12B	\$0.99884	\$232,484,798	Ethereum	-0.01%	-0.02%
8	 HUSD #112 HUSD	\$809.09M	\$1.00002	\$394,275,890	Ethereum	+0.11%	+0.13%
9	 Neutrino USD #138 USDN	\$438.82M	\$0.98849	\$33,388,244	Waves	-0.6%	-0.74%
10	 Vai #177 VAI	\$269.04M	\$0.88157	\$3,809,757	Binance Chain	-0.55%	-2.98%

Πίνακας 4 Κρυπτονομίσματα Τεχνολογίας Stablecoin

4 ΣΗΜΑΝΤΙΚΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ ΚΑΙΝΟΤΟΜΙΕΣ

4.1 Bitcoin (BTC)

Το Bitcoin (BTC) περιγράφεται ως ένα εικονικό, αποκεντρωμένο και ανώνυμο νόμισμα που δεν υποστηρίζεται από καμία κυβέρνηση ούτε από οποιαδήποτε άλλη νομική οντότητα και δεν μπορεί να ανταλλαχθεί σε χρυσό ή οποιοδήποτε άλλο είδος.

Η δημιουργία του Bitcoin βασίζεται στην εργασία του Satoshi Nakamoto “Bitcoin: ένα σύστημα ηλεκτρονικών μετρητών Peer-to-Peer”, που δημοσιεύθηκε στο Διαδίκτυο το 2008.

Το γεγονός ότι μέχρι τώρα παραμένει ασαφές εάν ο Satoshi Nakamoto είναι πραγματικό πρόσωπο, ψευδώνυμο, ή ίσως ακόμη και μια ομάδα χάκερ συμβάλλει στον μύθο του συγκεκριμένου κρυπτονομίσματος.

Ο εικονικός χαρακτήρας του Bitcoin υπονοεί ότι τα Bitcoins συνήθως δεν έχουν φυσική μορφή. Επομένως, μια καλή παρομοίωση ενός Bitcoin πιθανώς θα ήταν αυτή ενός αρχείου υπολογιστή που είναι αποθηκευμένο σε έναν προσωπικό υπολογιστή ή μέσω μιας ηλεκτρονικής υπηρεσίας, σε ένα ψηφιακό πορτοφόλι.

Για να γίνει αποδεκτό ως χρήμα το Bitcoin θα πρέπει να είναι χειροπιαστό. Υπάρχει η δυνατότητα για εκτύπωση του συνδυασμού χαρακτήρων που αντιπροσωπεύουν το κάθε Bitcoin και, στη συνέχεια, αυτή εκτύπωση να χρησιμοποιηθεί για συναλλαγές. Όμως δεν είναι αυτός ο λόγος που έχει δημιουργηθεί. Το Bitcoin δημιουργήθηκε ως άυλη μορφή χρήματος για χρήση σε οικονομικές συναλλαγές, παγκοσμίως, χωρίς μεσάζοντες και χωρίς σύνορα.

Το Bitcoin βασίζεται σε έναν μηχανισμό συναίνεσης PoW (βλέπε παραπάνω) και η δημιουργία νέων Bitcoin πραγματοποιείται μέσω μιας διαδικασίας που ονομάζεται «εξόρυξη» (βλέπε επίσης παραπάνω).

Ο συνολικός αριθμός των Bitcoin που μπορούν να δημιουργηθούν μέσω εξόρυξης είναι περιορισμένος: το σύστημα Bitcoin έχει σχεδιαστεί έτσι ώστε η εργασία ενημέρωσης του blockchain να ανταμείβεται, προοδευτικά στο χρόνο, με όλο και λιγότερο Bitcoins και ότι σε καμία στιγμή δεν θα υπάρχουν περισσότερα από 21 εκατομμύρια Bitcoins.

Το γεγονός ότι η δημιουργία και η αύξηση των bitcoins είναι αυτοματοποιημένη και περιορίζεται από το ίδιο το σύστημα χωρίς να χρειάζεται η παρέμβαση μιας κεντρικής οντότητας / αρχής να εκδίδει Bitcoins καθώς επίσης και ο περιορισμένος αριθμός Bitcoins, μαζί με το γεγονός ότι το ποσοστά μετατροπής Bitcoin καθορίζεται από την προσφορά και τη ζήτηση, χωρίς να μπορεί να παρέμβει κυβερνητικός φορέας (π.χ. εκτύπωση επιπλέον χρημάτων), οδηγεί σε υψηλή αστάθεια στις τιμές των Bitcoin.

Το Bitcoin blockchain είναι ένα τυπικό παράδειγμα ενός ανοιχτού, χωρίς άδεια blockchain. Οποιοσδήποτε μπορεί εγγραφεί ή να εγκαταλεί το δημόσιο Bitcoin κατά βούληση, χωρίς να απαιτείται έγκριση από οποιαδήποτε οντότητα.

Το Bitcoin μπορεί να αγοραστεί και να μετατραπεί απευθείας σε νόμισμα fiat και σε ένα ευρύ φάσμα άλλων κρυπτονομισμάτων.

Το Bitcoin είναι ένα από τα ευκολότερα νομίσματα από όλα κρυπτονομίσματα που κυκλοφορούν αυτήν τη στιγμή, για μετατροπή σε fiat νόμισμα.

Το Bitcoin (BTC) γίνεται αποδεκτό ως νόμισμα συναλλαγής από έναν σχετικά μεγάλο αριθμό (online) εμπόρων, μεταξύ των οποίων διάφορες μεγάλες εταιρείες (π.χ. Microsoft, Expedia, Playboy, Virgin, Galactic, κλπ)

Το Bitcoin είναι ένα ψευδο-ανώνυμο νόμισμα.

Το Bitcoin χαρακτηρίζεται συχνά ως ανώνυμο νόμισμα: αν και όλοι μπορούν να επαληθεύσουν την αλυσίδα του συναλλαγές με βάση το δημόσιο καθολικό, με την πρώτη ματιά τίποτα στο σύστημα δεν συνδέει τα Bitcoin σε άτομα. Ωστόσο, αυτός ο ανώνυμος χαρακτήρας απέχει πολύ από το να είναι απόλυτος. Είναι τεχνικά εφικτό - αν και πολύ περίπλοκο και δαπανηρό - για τον προσδιορισμό των συναλλασσομένων που βρίσκονται πίσω από μια συναλλαγή Bitcoin.

Με άλλα λόγια, το Bitcoin δεν είναι εντελώς ανώνυμο νόμισμα, αλλά μάλλον ψευδο-ανώνυμο.

4.2 Ethereum (ETH)

Το Ethereum, που κυκλοφόρησε τον Ιούλιο του 2015¹⁴⁸, είναι μια αποκεντρωμένη πλατφόρμα που τρέχει τα λεγόμενα «smart contracts -έξυπνα συμβόλαια».

Τα έξυπνα συμβόλαια είναι συμβάσεις ή εφαρμογές που εκτελούνται ακριβώς όπως έχουν προγραμματιστεί χωρίς καμία πιθανότητα διακοπής λειτουργίας (δηλαδή το blockchain δεν είναι ποτέ εκτός λειτουργίας), λογοκρισίας, απάτης ή παρέμβασης τρίτων.

Το Ethereum έχει μια ικανότητα που υπερβαίνει κατά πολύ ένα καθαρό ψηφιακό ισοδύναμο P2P όπως το Bitcoin. Με απλά λόγια, μοιάζει πολύ με ένα λειτουργικό σύστημα smartphone πάνω στο οποίο μπορεί να κατασκευαστούν εφαρμογές λογισμικού.

Από τεχνικής άποψης, η ίδια η πλατφόρμα Ethereum δεν περιέχει τεχνολογία κρυπτογράφησης. Ωστόσο, όπως και άλλα ανοιχτά, χωρίς άδεια blockchain, το Ethereum απαιτεί μια μορφή αξίας blockchain για να δώσει κίνητρα για να γίνουν συναλλαγές εντός του. Εδώ είναι που εμφανίζεται το κρυπτονόμισμα «Ether» (ETH) της Ethereum. Το ETH δεν επιτρέπει μόνο την κατασκευή έξυπνων συμβάσεων στην πλατφόρμα Ethereum, αλλά λειτουργεί επίσης ως γενικότερο νόμισμα συναλλαγής.

Όπως και το Bitcoin, το Ethereum χρησιμοποιεί επί του παρόντος έναν μηχανισμό ελέγχου PoW, αλλά προχωρά στην υιοθέτηση ενός μηχανισμού συναίνεσης PoS (βλέπε παραπάνω), γνωστό ως το πρωτόκολλο Casper.

Η ανάπτυξη του Ethereum προωθείται και υποστηρίζεται από το "Ethereum Foundation", μια ελβετική μη κερδοσκοπική οργάνωση, που ιδρύθηκε από τους εφευρέτες της Ethereum. Ένας μεγάλος όγκος αιθέρα «προ-εξορύχθηκε» (δηλαδή δημιουργήθηκε πριν από την κυκλοφορία του νομίσματος στο ευρύ κοινό) από τους εφευρέτες του και πωλήθηκε σε δημοπρασία για να πληρωθούν τα έξοδα ανάπτυξης και να χρηματοδοτηθεί το Ίδρυμα Ethereum.

Το Ethereum τρέχει σε ένα ανοιχτό, χωρίς άδεια blockchain. Όπως το Bitcoin, το Ethereum είναι ένα εξέχον παράδειγμα ανοιχτού blockchain χωρίς άδεια. Ο καθένας μπορεί να εγγραφεί ή να εγκαταλείψει το δίκτυο Ethereum κατά βούληση, χωρίς να χρειάζεται να εγκριθεί από οποιαδήποτε οντότητα.

Το Ether (ETH) μπορεί να αγοραστεί με και να μετατραπεί σε νόμισμα fiat και σε διάφορα κρυπτονομίσματα (π.χ. Coinbase, Kraken,...).

Όπως το Bitcoin, το Ether (ETH) γίνεται αποδεκτό ως μέσο πληρωμής από έναν μεγάλο αριθμό εμπόρων (π.χ. TapJets, Overstock κτλ).

Όπως και το Bitcoin, το Ether (ETH) μπορεί να κατηγοριοποιηθεί ως ψευδο-ανώνυμο ή ψευδώνυμο νόμισμα.

4.3 Ripple (XRP)

Το Ripple είναι μια πλατφόρμα ψηφιακής πληρωμής ανοικτού κώδικα, P2P που επιτρέπει σχεδόν στιγμιαίες μεταφορές χρημάτων ανεξάρτητα από τη μορφή τους (π.χ. Δολάριο ΗΠΑ, Γιεν, Bitcoin,...).

Ξεκίνησε το 2012 από την ιδιωτική εταιρεία Ripple (Labs), που είναι υπεύθυνη για την περαιτέρω εξέλιξη του πρωτοκόλλου Ripple, είναι η πρώτη εταιρεία που έχει λάβει «BitLicense» για πιστοποιημένη χρήση ψηφιακών στοιχείων από το Τμήμα Χρηματοοικονομικών Υπηρεσιών της Νέας Υόρκης.

Έχει την υποστήριξη διάφορων ισχυρών εταιρειών στον κλάδο των χρηματοοικονομικών υπηρεσιών, όπως η Bank of America, Merrill Lynch, Santander κ.λ.π.

Μετά την ίδρυση της Ripple, οι δημιουργοί της δημιούργησαν το κρυπτονόμισμα XRP. Το XRP δημιουργήθηκε σαν νόμισμα «γέφυρα» που επιτρέπει στα χρηματοπιστωτικά ιδρύματα να διευθετούν τις διασυνοριακές πληρωμές πολύ πιο γρήγορα και φθηνότερα από ό,τι μπορούν τα παγκόσμια δίκτυα πληρωμών που υπάρχουν σήμερα, το οποίο μπορεί να είναι αργό και να περιλαμβάνει πολλούς μεσάζοντες (δηλαδή τράπεζες).

Η πλατφόρμα πληρωμών του Ripple δεν έχει ανάγκη να χρησιμοποιήσει νόμισμα για να λειτουργήσει. Σύμφωνα με την Ripple, το XRP μπορεί να χειριστεί περισσότερες από 1.500 συναλλαγές ανά δευτερόλεπτο.

Ενώ αρχικά αναπτύχθηκε αποκλειστικά για επιχειρηματική χρήση, στο μεταξύ έχει υιοθετηθεί από μεγάλο αριθμό χρηστών κρυπτονομισμάτων. Το Ripple (XRP) δεν βασίζεται σε PoW ή PoS μηχανισμό για επικύρωση συναλλαγών, αλλά χρησιμοποιεί το δικό του ειδικό πρωτόκολλο επικύρωσης συναλλαγών.

Το XRP δεν εξορύσσεται. Ο συνολικός αριθμός των XRP έχει «προεξορυχθεί» πλήρως (ή καλύτερα: δημιουργήθηκε κατά την έναρξη του νομίσματος) από τους δημιουργούς του. Προς το παρόν, κατανέμεται ως εξής:

- 8.102.265.714 XRP κατέχει η Ripple (Labs), Inc.
- 39.189.968.239 XRP έχει διανεμηθεί
- 52.700.000.024 XRP έχουν κατατεθεί ως εγγύηση για της επάρκειας XRP σε οποιαδήποτε συναλλαγή

Σε αντίθεση με τους δημιουργούς της Ethereum, οι δημιουργούς του Ripple δεν πούλησαν ένα μέρος του XRP μέσω δημοπρασίας. Για την δημιουργία του XRP για τη χρηματοδότηση της Ripple (Labs), Inc., η εταιρεία χρηματοδοτήθηκε ιδιωτικά.

Προς το παρόν, δεν είναι απολύτως ξεκάθαρο πώς θα διανέμεται, περαιτέρω, στο μέλλον το XRP.

Το Ripple εκτελείται σε blockchain με δημόσια άδεια. Σε αντίθεση με το Bitcoin και το Ethereum, το Ripple τρέχει σε ένα εγκεκριμένο blockchain. Αυτό συμβαίνει επειδή η Ripple (Labs) Inc., η εταιρεία πίσω από το Ripple (XRP), ελέγχει και καθορίζει ποιος μπορεί να ενεργήσει ως επικυρωτής συναλλαγών στο δίκτυό της. Το ίδιο το blockchain θεωρείται δημόσιο, καθώς ο οποιοσδήποτε μπορεί να έχει πρόσβαση και να το δει.

Όπως το Bitcoin, το XRP μπορεί να μετατραπεί άμεσα σε νομίσματα σε διάφορα χρηματιστήρια κρυπτονομισμάτων (π.χ. Kraken, LiteBit, Anycoin Direct, Bitsane κτλ).

Το Ripple (XRP) είναι αποδεκτό ως μέσο πληρωμής από έναν μεγάλο αριθμό (online) εμπόρων για

διάφορα αγαθά και υπηρεσίες (π.χ. ηλεκτρονικά τσιγάρα, μέλι, καφέ κτλ). Υπάρχει ακόμη η φήμη ότι η Amazon είναι έτοιμη να υιοθετήσει το Ripple στο εγγύς μέλλον.

Το Ripple (XRP) είναι ένα ψευδο-ανώνυμο νόμισμα, όπως το Bitcoin.

4.4 Bitcoin Cash (BCH)

Το Bitcoin Cash (BCH) είναι αποκεντρωμένο κρυπτονόμισμα. Δημιουργήθηκε την 1η Αυγούστου 2017 και βασίζεται στον αρχικό αλγόριθμο SHA-256 PoW του Bitcoin, αλλά με κάποιες αλλαγές στον υποκείμενο κώδικα. Το Bitcoin Cash είναι γνωστό στην κρυπτοκοινότητα ως το «σκληρό αντίγραφο» του Bitcoin

Η δημιουργία του προέκυψε από το αποτέλεσμα δύο πολύ διαφορετικών οραμάτων για το μέλλον του Bitcoin και του Bitcoin blockchain, που με αυτόν τον τρόπο ακολουθεί δύο διαφορετικές διαδρομές προς το μέλλον.

Αυτό που έγινε ήταν ότι κάποιοι προγραμματιστές Bitcoin ήθελαν να αυξηθεί το όριο μεγέθους μπλοκ από 1MB σε 8MB, για να μειωθούν τα τέλη συναλλαγών και να βελτιωθεί ο χρόνος επιβεβαίωσης των συναλλαγών, ενώ άλλοι διαφωνούσαν. Επειδή η κοινότητα δεν μπορούσε να φτάσει σε συμφωνία, δημιουργήθηκε ένα νέο Bitcoin, το Cash Bitcoin.

Όπως και το Bitcoin, το Bitcoin Cash χρησιμοποιεί τον μηχανισμό PoW, που σημαίνει ότι μπορεί να εξορύσσεται. Αυτό που είναι αξιοσημείωτο είναι ότι επειδή το Bitcoin Cash είναι αντίγραφο του Bitcoin, ο καθένας που είχε στην κατοχή του Bitcoins κατά τη δημιουργία του Bitcoin Cash (δηλαδή την 1η Αυγούστου 2017 - 13:16 UTC) έγινε επίσης κάτοχος του ίδιου ποσού Bitcoin Cash. Κάθε Bitcoin που αποκτήθηκε μετά τη συγκεκριμένη στιγμή ακολουθεί τον αρχικό σχέδιασμο και δεν περιλαμβάνει το Bitcoin Cash.

Το Bitcoin Cash λειτουργεί σε ένα ανοιχτό blockchain χωρίς άδεια, όπως το Bitcoin και μπορεί εύκολα να μετατραπεί σε νόμισμα fiat και αντίστροφα μέσω ενός αριθμού κρυπτονομισμάτων (π.χ. Coinbase, Kraken, LiteBit, κτλ).

Το Bitcoin Cash μπορεί να χρησιμοποιηθεί για την πληρωμή ενός αυξανόμενου φάσματος αγαθών και υπηρεσιών (π.χ. κοσμήματα, τρόφιμα, παιχνίδια, τηλεπικοινωνίες, κτλ) σε μια σειρά διαδικτυακών αγορών και πλατφορμών (π.χ. OpenBazaar).

Το Bitcoin Cash είναι ένα ψευδο-ανώνυμο νόμισμα.

4.5 Litecoin (LTC)

Όπως το Bitcoin, το Litecoin (LTC) είναι ένα αποκεντρωμένο κρυπτονόμισμα P2P ανοιχτού κώδικα. Ξεκίνησε τον Οκτώβριο του 2011 και βασίζεται σε αυτό που είναι γνωστό ως αλγόριθμος Scrypt PoW, ο οποίος χρησιμοποιεί τον αρχικό αλγόριθμο SHA-256 PoW του Bitcoin.

Το Litecoin περιγράφεται συχνά ως «ασήμι» σε αντιπαράθεση με το χρυσό Bitcoin, από το γεγονός ότι χρησιμοποιεί διαφορετικό αλγόριθμο.

Διαφέρει από το Bitcoin σε δύο τρόπους:

Πρώτον, και αυτό προκύπτει από τη χρήση του αλγορίθμου Scrypt PoW, το Litecoin παρέχει πολύ πιο γρήγορη ταχύτητα συναλλαγής από το Bitcoin. Ο χρόνος που απαιτείται για τη

δημιουργία ενός μπλοκ στο Bitcoin BC είναι περίπου δέκα λεπτά, ενώ ο μέσος χρόνος δημιουργίας μπλοκ στο blockchain του Litecoin είναι περίπου 2,5 λεπτά.

Δεύτερον, το συνολικό όριο προσφοράς του Litecoin είναι 84 εκατομμύρια νομίσματα, πολύ υψηλότερα από τα 21 εκατομμύρια όριο προσφοράς του Bitcoin.

Ακριβώς όπως το Bitcoin, το Litecoin runons σε ένα ανοιχτό blockchain χωρίς άδεια. Το μόνο που χρειάζεται για να εγγραφεί κανείς στο δίκτυο είναι να κάνει λήψη του λογισμικού ανοιχτού κώδικα.

Το Litecoin μπορεί να μετατραπεί σε νόμισμα fiat σε διάφορα χρηματιστήρια κρυπτονομισμάτων, καθώς και σε άλλα κρυπτονομίσματα (π.χ. BTC, Direct200, LiteBit, Coinbase, Anycoin Direct κτλ.)

Το Litecoin είναι αποδεκτό, όπως το Bitcoin, ως μέσο πληρωμής από έναν μεγάλο αριθμό διαδικτυακών εμπόρων.

Όπως το Bitcoin, το Litecoin είναι ένα ψευδο-άνωνυμο νόμισμα. Ο καθένας μπορεί να έχει πρόσβαση στο blockchain του LTC, πράγμα που θα καθιστούσε τεχνικά δυνατό τον προσδιορισμό του αποστολέα και του παραλήπτη μιας συναλλαγής.

Πρέπει να σημειωθεί ότι η κοινότητα Litecoin εισήγαγε πρόσφατα μια καινούργια τεχνολογία στον κόσμο των κρυπτονομισμάτων που αναφέρεται ως «atomic swap - ατομική ανταλλαγή». Αυτό που γίνεται είναι ότι μια ατομική ανταλλαγή επιτρέπει μια P2P ανταλλαγή μεταξύ blockchains δηλαδή ανταλλαγή ενός κρυπτονομίσματος με άλλο κρυπτονόμισμα, χωρίς την ανάγκη ύπαρξης ενδιάμεσου

Στην πράξη αυτό δεν είναι φυσικά και τόσο εύκολο. Πρώτα απ' όλα, δεδομένου ότι αυτή τη στιγμή βρίσκεται ακόμη στα σπάργανα, η εφαρμογή της τεχνολογίας atomic swap απαιτεί πολλές γνώσεις πληροφορικής. Για παράδειγμα, πρέπει να δημιουργηθεί ένας σύνδεσμος μεταξύ των δύο blockchains που απαιτεί την υλοποίηση ενός πρωτοκόλλου IT γνωστού ως "Lightning Protocol". Επί πλέον, για να ολοκληρωθεί η συναλλαγή, τα δύο blockchains πρέπει να μοιραστούν την ίδια κρυπτογραφική ρουτίνα (πχ την SHA-256).

Αν και αυτή η καινοτομία έχει δρόμο να διανύσει, αφήνει να δημιουργηθεί προοπτική για νέες προκλήσεις στον κόσμο των κρυπτονομισμάτων.

4.6 Stellar (XLM)

Το Stellar είναι μια υποδομή κατανεμημένων πληρωμών ανοιχτού κώδικα, όπως το Ripple.

Το Stellar δημιουργήθηκε το 2014 από έναν από τους ιδρυτές της Ripple. Στόχος του είναι να προσφέρει οικονομικές υπηρεσίες χαμηλού κόστους για την καταπολέμηση της φτώχειας και την ανάπτυξη του ατομικού δυναμικού.²⁰⁸ Το Stellar μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία έξυπνων συμβάσεων.

Δεν βασίζεται σε μηχανισμό συναίνεσης PoW ή PoS, αλλά έχει το δικό του ειδικό πρωτόκολλο πιστοποίησης συναλλαγών.

Το Stellar χρησιμοποιεί το κρυπτονόμισμα Lumen (XLM) για την υλοποίηση των συναλλαγών στο δίκτυο του. Προσφέρει την δυνατότητα μεταφοράς χρημάτων σε όλο τον κόσμο και την διεξαγωγή συναλλαγών μεταξύ διαφορετικών νομισμάτων γρήγορα και με ασφάλεια.

Η ανάπτυξη του Stellar υποστηρίζεται από τον μη κερδοσκοπικό οργανισμό Stellar.org (ιδρύθηκε το 2014 ως μια μη κερδοσκοπική μη κερδοσκοπική εταιρεία στην πολιτεία του Delaware των ΗΠΑ), ο οποίος εργάζεται για την ανάπτυξη εργαλείων και κοινωνικών πρωτοβουλιών στο δίκτυο Stellar.

Οι υπάλληλοι εισάγουν ουν κώδικα στο δίκτυο, αλλά το ίδιο το δίκτυο ισχυρίζονται ότι είναι εντελώς ανεξάρτητο από τον οργανισμό.

Παρόμοια με το XRP κρυπτογράφησης της Ripple, η συνολική προσφορά των Lumens είναι προεξοργυμένη. Διατηρείται από το Stellar.org που του έχει ανατεθεί η δωρεάν διανομή Lumens, με τον ακόλουθο τρόπο:

- Το 50% θα δοθεί σε άτομα (μέσω προγράμματος άμεσης εγγραφής)
- Το 25% θα δοθεί στους συνεργάτες (μέσω ενός ειδικού προγράμματος εταιρικής σχέσης)
- Το 20% χορηγείται στους κατόχους Bitcoin και XRP
- Το 5% προορίζεται για τα λειτουργικά έξοδα του Stellar.org

Η τελική διανομή δεν πραγματοποιείται ταυτόχρονα, αλλά με την πάροδο του χρόνου σε αρκετούς κύκλους.

Σε αντίθεση με το Ripple, το Stellar τρέχει σε ένα blockchain χωρίς άδεια. Οποιοσδήποτε μπορεί να συμμετάσχει στο δίκτυο κατά βούληση και, εάν πληρούνται ορισμένες προϋποθέσεις, επικυρώνει τις συναλλαγές χωρίς να χρειάζεται να έχει προεγκριθεί ή να ελεγχθεί από κανένα κεντρικό διαχειριστή.

Το Lumens (XLM) μπορεί να μετατραπεί άμεσα σε νόμισμα fiat μέσω ανταλλαγών κρυπτονομισμάτων όπως το LiteBit (έως το μέγιστο ποσό των 500 ευρώ (ανά συναλλαγή)) ή Kraken. Τα Lumens (XLM) ΔΕΝ είναι ακόμα ένα πραγματικό μέσο συναλλαγής. Προς το παρόν, όπως φαίνεται, τα Lumens (XLM) μπορούν να χρησιμοποιηθούν μόνο για να αγοραστούν διαφημιστικά αυτοκόλλητα Stellar και πρωινό σε ένα τοπικό μπαρ πρωινού στο Arkansas. Έτσι δεν αποτελεί ακόμη ένα πραγματικό μέσο ανταλλαγής.

Τα Lumens (XLM) είναι ψευδο-ανώνυμα νομίσματα. Όλες οι συναλλαγές στο δίκτυο Stellar είναι δημόσιες, αλλά δεν μπορούν να συνδεθούν εύκολα με τις ταυτότητες των χρηστών τους. Ως αποτέλεσμα, οι Stellar Lumens (XLM) μπορούν να χαρακτηριστούν ως ψευδο-ανώνυμα νομίσματα.

4.7 DASH (DASH)

Το Dash (DASH), παλαιότερα γνωστό ως Darkcoin, είναι ένα κρυπτονομίσμα με συναλλαγές P2P.

Κυκλοφόρησε για πρώτη φορά τον Ιανουάριο του 2014 και βασίζεται σε αυτό που είναι γνωστό ως αλγόριθμος X11 PoW.

Αυτό που είναι ιδιαίτερο για το Dash, και το κάνει διαφορετικό από τα άλλα κρυπτονομίσματα, είναι ότι διαθέτει δίκτυο δύο επιπέδων. Το blockchain του Dash προστατεύεται μέσω των λεγόμενων "masternodes – βασικών κόμβων" εκτός από το PoW που γίνεται από τους miners.

Με λίγα λόγια, ένας masternode είναι ένας server συνδεδεμένος στο δίκτυο Dash που εγγυάται ένα συγκεκριμένο ελάχιστο επίπεδο απόδοσης και λειτουργικότητας για την εκτέλεση ορισμένων εργασιών που σχετίζονται με PrivateSend και InstantSend (λειτουργίες του Dash για ιδιωτική και άμεση συναλλαγή) .

Οι συναλλαγές με παραδοσιακά κρυπτονομίσματα μπορεί να είναι πολύ χρονοβόρες (δηλαδή μπορεί να απαιτηθούν οτιδήποτε μεταξύ λίγων λεπτών και περισσότερο από μία ώρα). Αυτό οφείλεται στο γεγονός ότι αρκετά μπλοκ πρέπει να προστεθούν για να διασφαλιστεί ότι μια συναλλαγή είναι μη αναστρέψιμη και ταυτόχρονα όχι απόπειρα διπλοεγγραφής. Η Dash

αντιμετωπίζει αυτό το ζήτημα χρησιμοποιώντας το masternode δίκτυο. Οι Masternodes μπορούν να κληθούν να οργανώσουν ψηφοφορίες για να ελέγξουν εάν ή όχι η υποβληθείσα συναλλαγή είναι έγκυρη και εάν είναι «κλειδώνουν» τις εισόδους για τη συναλλαγή και μεταδίδουν αυτές τις πληροφορίες στο δίκτυο, υπόσχομενοι ουσιαστικά ότι η συναλλαγή θα συμπεριληφθεί στο

επόμενο μπλοκ και δεν επιτρέπουν άλλες δαπάνες αυτών των εισροών κατά τη διάρκεια της χρονικής περιόδου της επιβεβαίωσης. Ως αποτέλεσμα, το Dash λέγεται ότι μπορεί να ανταγωνιστεί με σχεδόν στιγμιαία συναλλαγή συστήματα, όπως οι πιστωτικές κάρτες.

Το Dash τρέχει σε ένα ανοιχτό, χωρίς άδεια blockchain όπως το Monero, το Dash τρέχει σε ένα blockchain χωρίς άδεια. Οποιοσδήποτε μπορεί να εγγραφεί στο δίκτυο κατά βούληση, χωρίς να χρειάζεται να προεγκριθεί ή να ελεγχθεί από οποιονδήποτε κεντρικό διαχειριστή.

Το Dash (DASH) μπορεί να μετατραπεί απευθείας σε νόμισμα fiat μέσω διαφόρων ανταλλαγών κρυπτονομισμάτων (π.χ. Anycoin Direct, Kraken, κλπ).

Όπως και το Monero, το Dash γίνεται αποδεκτό ως μέσο πληρωμής από έναν σταθερά αυξανόμενο αριθμό διαδικτυακών έμπορων.

Όπως το blockchain του Bitcoin, το blockchain του Dash είναι από επιλογή διάφανο, πράγμα που σημαίνει γενικά ότι οι συναλλαγές είναι πάντα επαληθεύσιμες και ανιχνεύσιμες στο blockchain. Για να δώσει στους χρήστες του πραγματικό οικονομικό απόρρητο, το Dash προσφέρει την επιλογή να χρησιμοποιήσουν μια λειτουργία που ονομάζεται PrivateSend. Το PrivateSend αποκρύπτει την προέλευση των χρημάτων ενός χρήστη μέσω μιας διαδικασίας που είναι γνωστή ως «mixing».

4.8 Monero (XMR)

Το Monero (XMR) είναι ένα κρυπτονομίσμα P2P ανοιχτού κώδικα «επικεντρωμένο στις ιδιωτικές και απαραβίαστες συναλλαγές». Ξεκίνησε τον Απρίλιο του 2014 και βασίζεται σε αυτό που είναι γνωστό ως CryptoNote Αλγόριθμος PoW.

Το Monero έχει αναπτυχθεί ειδικά για να επιτρέψει στους χρήστες του να εκτελούν συναλλαγές με πλήρη ανωνυμία. Είναι κρυπτογραφικά ιδιωτικό από την δημιουργία του. Συγκεκριμένα, χρησιμοποιεί κρυπτογραφία για να προστατεύσει τις διευθύνσεις αποστολής και λήψης (δηλαδή τα λεγόμενα «κλειδιά»), καθώς και τα ποσά συναλλαγής.

Το Monero (XMR) χαρακτηρίζεται ως τελείως ελεύθερο. Αυτό σημαίνει ότι δύο συναλλασσόμενοι XMR μπορούν πάντα να εκτελούν συναλλαγές, χωρίς να υπάρχει μαύρη λίστα XMR από προμηθευτές ή συναλλαγές λόγω συσχέτισης με προηγούμενες συναλλαγές.

Το Bitcoin και το Litecoin, θεωρητικά μπορεί να έχουν μαύρη λίστα, εάν έχουν χρησιμοποιηθεί για παράνομο σκοπό στο παρελθόν, αυτό θα είναι καταγεγραμμένο στο blockchain και μάλιστα για πάντα.

Σε αντίθεση με ορισμένα άλλα κρυπτονομίσματα, το Monero (XMR) δεν έχει προ-εξορυχθεί.

Το Monero τρέχει σε ένα ελεύθερο σε πρόσβαση blockchain και ο οποιοσδήποτε μπορεί να ενταχθεί χωρίς να χρειάζεται να προεγκριθεί ή να ελεγχθεί από οποιονδήποτε κεντρικό διαχειριστή.

Το Monero (XMR) μπορεί να μετατραπεί άμεσα σε νόμισμα fiat και σε μια σειρά κρυπτονομισμάτων

(π.χ. LiteBit, Anycoin Direct, Kraken κλπ)

Το Monero γίνεται αποδεκτό ως μέσο πληρωμής από έναν σταδιακά αυξανόμενο αριθμό διαδικτυακών εμπορών.

Το Monero είναι ένα ανώνυμο νόμισμα. Σε ένα πλήρως διαφανές blockchain, όπως το Bitcoin ή το Ethereum blockchain, οι συναλλαγές είναι πάντα ελεύθερα επαληθεύσιμες και ανιχνεύσιμες από οποιονδήποτε. Στην πράξη - αν και αυτό δεν θα είναι εύκολο έργο - η αποστολή και η λήψη διευθύνσεων για τέτοιες συναλλαγές θα μπορούσε να συνδεθεί με την πραγματική ταυτότητα ενός ατόμου. Εδώ βρίσκεται η διαφοροποίηση του Monero από τα άλλα κρυπτονομίσματα ώστε να χαρακτηρίζεται ως ασφαλές, ιδιωτικό και μη ανιχνεύσιμο κρυπτονόμισμα.

Αυτό το υψηλό επίπεδο ανωνυμίας επιτυγχάνεται χρησιμοποιώντας δύο διαφορετικές τεχνικές:

- Εμπιστευτικές συναλλαγές δακτυλίου ("RingCT")
- Διευθύνσεις Stealth

Εμπιστευτικές συναλλαγές δακτυλίου (RingCT)

Το RingCT συνδυάζει την τεχνική Ring signatures και αυτό που αναφέρεται στην κρυπτοκοινότητα ως εμπιστευτικές συναλλαγές:

Οι Ring signatures συνδυάζουν κλειδιά λογαριασμού του χρήστη με δημόσια κλειδιά που λαμβάνονται από το blockchain του Monero για την δημιουργία, αυτού που θα μπορούσε να ονομαστεί κύκλος πιθανών υπογραφών, πράγμα που σημαίνει ότι οι

εξωτερικοί παρατηρητές δεν μπορούν να συνδέσουν μια υπογραφή με έναν συγκεκριμένο χρήστη. Σε συνδυασμό με διευθύνσεις stealth (βλέπε παρακάτω) αποκρύπτουν πλήρως την ταυτότητα τόσο των αποστολέων όσο και των παραληπτών του XMR;

Οι εμπιστευτικές συναλλαγές προσθέτουν ένα άλλο επίπεδο απορρήτου στο «μείγμα», αποκρύπτοντας επίσης το ποσό κάθε συναλλαγής. Χωρίς να αποκαλυφθούν οι πραγματικοί αριθμοί, περιλαμβάνουν μια κρυπτογραφημένη απόδειξη ότι το άθροισμα των ποσών εισόδου είναι το ίδιο με το άθροισμα της εξόδου

Διευθύνσεις Stealth

Επίσης, εκτός από το RingCT, η Monero χρησιμοποιεί επίσης διευθύνσεις Stealth (αόρατες). Αυτές είναι προσωρινές διευθύνσεις που δημιουργούνται τυχαία και εφάπαξ για κάθε συναλλαγή που πραγματοποιείται από τον αποστολέα προς τον παραλήπτη. Όλες οι πληρωμές που αποστέλλονται στον παραλήπτη δρομολογούνται μέσω αυτών των διευθύνσεων, διασφαλίζοντας ότι δεν υπάρχουν σύνδεσμοι στο blockchain μεταξύ της διεύθυνσης του αποστολέα και του παραλήπτη. Με άλλα λόγια, οι διευθύνσεις stealth αποτρέπουν τη δυνατότητα σύνδεσης στο blockchain. Ωστόσο, χωρίς τη χρήση του RingCT, ο αρχικός αποστολέας θα εξακολουθούσε να είναι σε θέση να εντοπίσει τα ποσά που θα μετακινηθούν από τον παραλήπτη αναγνωρίζοντας τις εξόδους στο blockchain. Το RingCT καλύπτει αυτές τις εξόδους, κάνοντας την συναλλαγή εντελώς μη ανιχνεύσιμη.

Το project Kovri












Πρέπει να σημειωθεί ότι η κοινότητα των προγραμματιστών και ειδικών κρυπτογραφίας που βρίσκονται πίσω από το Monero εργάζονται επί του παρόντος σε ένα έργο για την προσθήκη ενός ακόμη επιπέδου απορρήτου στο σύστημα, δρομολογώντας και κρυπτογραφώντας συναλλαγές XMR μέσω κόμβων **Invisible Internet Project I2P**. Η χρήση του I2P θα αποκρύψει μια διεύθυνση IP ενός κόμβου και θα παρέχει περαιτέρω προστασία του δικτύου έναντι της παρακολούθησης.

Αυτό το έργο, του οποίου βρίσκεται σε εξέλιξη μια έκδοση άλφα, είναι πιο γνωστό στους θιασώτες των κρυπτονομισμάτων ως Kovri.

4.9 Ταξινόμηση – Ομαδοποίηση Κρυπτονομισμάτων

Είναι φανερό, όπως είδαμε και από την επισκόπηση των κυρίων κρυπτονομισμάτων ότι η ομαδοποίησή τους δεν είναι εφικτή. Αν και μερικά είναι παρόμοια, υπάρχει μεγάλη παραλλαγή ως προς το πώς είναι δομημένα, με ποια τεχνολογία λειτουργούν, θέματα ανωνυμίας κ.λπ.

Αυτό φαίνεται στον παρακάτω πίνακα:

ΟΝΟΜΑ	ΣΥΜΒΟΛΟ	ΔΗΜΙΟΥΡΓΗΜΕΝΟ ΑΠΟ ΑΤΟΜΟ Η ΟΝΤΟΤΗΤΑ	ΑΝΤΑΛΑΣΣΟΜΕΝΟ ΗΛΕΚΤΡΟΝΙΚΑ	ΑΜΕΣΑ ΜΕΤΑΤΡΕΨΙΜΟ ΣΕ ΝΟΜΙΣΜΑ FIAΤ	ΜΕΣΟ ΣΥΝΑΛΛΑΓΗΣ	ΨΕΥΔΟΑΝΩΝΥΜΟ/ ΑΝΩΝΥΜΟ
Bitcoin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
Ethereum		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
Ripple		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
Bitcoin Cash		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
Litecoin		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
Stellar		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
Cardano		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
IOTA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
NEO		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΨΕΥΔΟΑΝΩΝΥΜΟ
Monero		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΑΝΩΝΥΜΟ
Dash		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ΑΝΩΝΥΜΟ

ναι όχι ✓ ως ένα σημείο

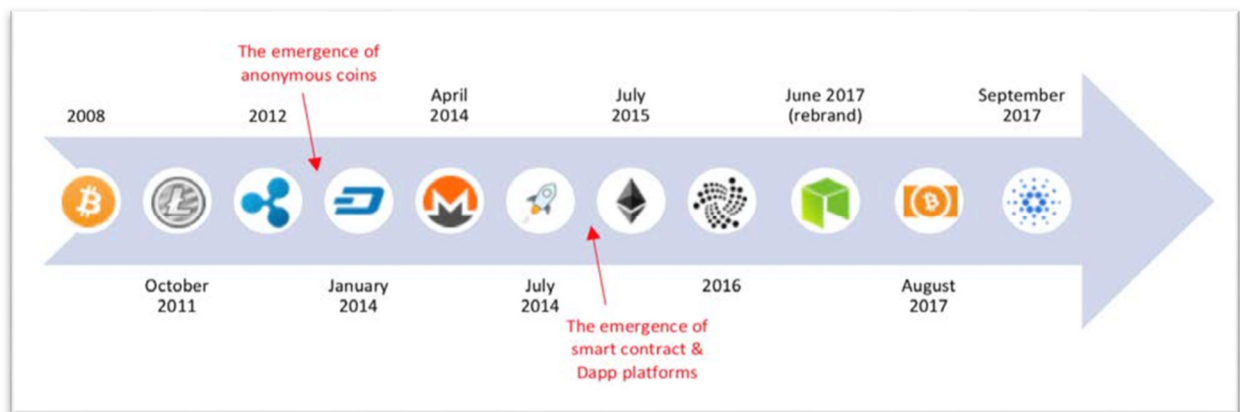
Πίνακας 5 - Χαρακτηριστικά βασικών κρυπτονομισμάτων

Τα κρυπτονομίσματα μπορούν να κατηγοριοποιηθούν με βάση διάφορες παραμέτρους: αν λειτουργούν με τεχνολογία με ή χωρίς άδεια, την αποκεντρωμένη τους φύση, αν προσφέρθηκαν αρχικά από συγκεκριμένο υπαρκτό άτομο ή οντότητα, αν είναι διαπραγματεύσιμα ηλεκτρονικά, αν είναι άμεσα μετατρέψιμα σε νόμισμα fiat, αν

χρησιμοποιούνται σαν μέσο συναλλαγής και αν είναι ψευδο-ανώνυμο ή πλήρως ανώνυμο. Αυτές οι παράμετροι μπορούν να βοηθήσουν στην εκτίμηση αν και σε ποιο βαθμό τα κρυπτονομίσματα υπάγονται στον νόμο AMLD5 του ευρωκοινοβουλίου, αν οι ίδιοι οι κάτοχοι κρυπτονομισμάτων περιλαμβάνονται στο πεδίο εφαρμογής του AMLD5 κ.λ.π.

Όπως φαίνεται στον πίνακα, οι διαφορές, μεταξύ των κρυπτονομισμάτων, δεν είναι καθόλου ξεκάθαρες. Επίσης αυτό που κάνει δυσκολότερη την κατηγοριοποίηση τους είναι μεταξύ άλλων, η ανεπάρκεια των διαθέσιμων τεχνικών πληροφοριών σε σχέση με την τεχνολογία που χρησιμοποιούν και η κινητικότητα τους, δηλαδή ένα κρυπτόνμισμα που δεν χρησιμοποιείται ως μέσο συναλλαγής τώρα, μπορεί να χρησιμοποιείται ένα αύριο.

Χρησιμοποιώντας ένα χρονοδιάγραμμα κρυπτονομισμάτων, μπορούμε να προχωρήσουμε σε καλύτερη κατανόηση αυτών των νομισμάτων, με στόχο να τα ταξινομήσουμε.



Σχεδιάγραμμα 2 - Εξέλιξη κρυπτονομισμάτων στον χρόνο

Αυτό που μπορούμε να πούμε είναι ότι τα πρώτα κρυπτονομίσματα αναπτύχθηκαν ως καθαρά ψηφιακά ισοδύναμα μετρητών P2P, αλλά προοδευτικά εμφανίστηκαν νέες μορφές κρυπτονομισμάτων για να εξυπηρετούν διαφορετικούς ή επιπρόσθετους σκοπούς.

Το 2014 είδαμε ότι η εμφανίζονται κρυπτονομίσματα που είναι πλήρως ανώνυμα. Το 2015 έγινε ένα σημαντικό βήμα, η δημιουργία της πλατφόρμας Ethereum, η οποία ξεκίνησε την ανάπτυξη εντελώς νέων συστημάτων ή πλατφορμών πάνω στις οποίες γίνονται έξυπνες συμβάσεις και μπορούν να εκτελεστούν αποκεντρωμένες εφαρμογές (Dapps) που τροφοδοτούνται από μια νέα γενιά

κρυπτονομισμάτων. Αυτή η συνεχώς αυξανόμενη τεχνολογική πολυπλοκότητα και η εξελισσόμενη φύση των κρυπτονομισμάτων, πρέπει να ληφθούν υπόψη κατά την περαιτέρω κατάταξη των κρυπτονομισμάτων στο μέλλον.

5 ΕΥΡΩΠΑΙΚΟ ΠΛΑΙΣΙΟ ΛΕΙΤΟΥΡΓΙΑΣ

Ορισμός πλαισίου λειτουργίας και κανόνων στον αγώνα εναντίον νομιμοποίησης εσόδων από «ξέπλυμα» χρημάτων, χρηματοδότησης της τρομοκρατίας και φοροδιαφυγής μέσω κρυπτονομισμάτων

5.1 Εμπόδια στην προσπάθεια ορισμού πλαισίου λειτουργίας και κανόνων σε σχέση με τα κρυπτονομίσματα

5.1.1 Αωνυμία

Το βασικό ζήτημα που πρέπει να επιλυθεί για την επαρκή παρακολούθηση των κρυπτονομισμάτων, των ιδιοκτητών τους και της νόμιμης διαχείρισής τους είναι η δημιουργία νομοθεσίας που θα καταργήσει την ανωνυμία που τα περιβάλλει. Η ανωνυμία αποτρέπει από το να παρακολουθούνται επαρκώς οι συναλλαγές κρυπτονομισμάτων, επιτρέποντας την εκτέλεση «σκοτεινών» συναλλαγών εκτός νομικού ελέγχου, επιτρέποντας σε εγκληματικές οργανώσεις να χρησιμοποιούν κρυπτονομίσματα για απόκτηση εύκολης πρόσβασης σε «ξεπλυμένο χρήμα».

Η ανωνυμία είναι επίσης το σημαντικότερο σημείο σε σχέση με την φοροδιαφυγή. Αγορά κρυπτονομισμάτων χωρίς πληρωμή φόρων είναι φοροδιαφυγή. Όμως, όταν η φορολογική αρχή δεν γνωρίζει ποιος είναι πίσω από την κάθε συναλλαγή, λόγω της σχετικής ανωνυμίας, δεν μπορεί ούτε να εντοπίσει τους συναλλασσόμενους, ούτε να επιβάλει φόρο. Αυτό καθιστά τα κρυπτονομίσματα ένα πολύ ελκυστικό μέσο για τους φοροφυγάδες .

Πάντως, πρέπει να σημειωθεί ότι ορισμένα κρυπτονομίσματα είναι ψευδο-ανώνυμα, πράγμα που ουσιαστικά σημαίνει ότι εάν καταβληθεί μεγάλη προσπάθεια και χρησιμοποιηθούν πολύπλοκες τεχνικές, οι αρχές μπορούν να ανακαλύψουν τις ταυτότητες των χρηστών που τα κατέχουν.

Αν και αυτό μπορεί να βοηθήσει στην καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, της χρηματοδότησης της τρομοκρατίας και της φορολογίας σε ορισμένες περιπτώσεις, δεν αποτελεί μια δυνητικά τυποποιημένη μέθοδο για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, της χρηματοδότησης της τρομοκρατίας και της φοροδιαφυγής. Η ανακάλυψη ταυτοτήτων με αυτόν τον τρόπο είναι πολύ περίπλοκη και δαπανηρή ώστε να γίνει ο κανόνας για την αντιμετώπιση αυτού του ζητήματος.

Σε κάθε περίπτωση, είναι επιθυμητή μια πιο διαρθρωτική ρυθμιστική προσέγγιση.

5.1.2 Διασυνοριακή φύση

Εκτός από την ανωνυμία, η εγγενώς ασυνοριακή φύση των κρυπτονομισμάτων, των αγορών κρυπτογράφησης και των crypto -παίκτην είναι μια μεγάλη πρόκληση για τους νομικούς.

Ένα από τα ζητήματα είναι π.χ. ότι οι αγορές κρυπτογράφησης και οι crypto -παίκτες μπορούν να βρίσκονται σε χώρες που δεν έχουν μεθόδους ελέγχου ξεπλύματος χρήματος ή χρηματοδότησης τρομοκρατίας. Ο διασυνοριακός χαρακτήρας των κρυπτονομισμάτων και των αγορών κρυπτογράφησης σημαίνει ότι η σχετική νομοθεσία θα είναι επαρκής μόνο όταν λαμβάνεται σε διεθνές επίπεδο.

5.1.3 Απουσία μεσάζοντα

Ένας άλλος σημαντικός παράγοντας που δυσκολεύει την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες συναλλαγές και ενέργειες μέσω κρυπτονομισμάτων είναι ότι συχνά δεν υπάρχει κεντρικός μεσολαβητής, που θα μπορούσε να ήταν το σημείο εστίασης της νομοθεσίας. Επομένως, ένα σημαντικό ερώτημα είναι σε ποιο σημείο στην αγορά κρυπτογράφησης πρέπει να εστιάσει η νομοθεσία.

5.2 Τα κρυπτονομίσματα «κρύβονται» πίσω από την ανωνυμία τους

Το υφιστάμενο ευρωπαϊκό νομικό πλαίσιο δεν μπορεί να αντιμετωπίσει τα προαναφερθέντα ζητήματα, επειδή ακριβώς δεν υπάρχουν κανόνες που να αποκαλύπτουν την ανωνυμία που σχετίζεται με τα κρυπτονομίσματα, κάνοντας το ερώτημα είτε έχουν ληφθεί στο σωστό επίπεδο είτε σε ποιον εφαρμόζουν περιπτώ.

Λόγω της απουσίας κανόνων που αποκαλύπτουν την ανωνυμία, δεν μπορεί να εφαρμοστεί το νομικό πλαίσιο για την ανταλλαγή πληροφοριών στον τομέα της φορολογίας, επειδή για να εφαρμοστεί η ανταλλαγή πληροφοριών, οι αρχές πρέπει να τις έχουν στην διάθεσή τους. Για τους ίδιους λόγους, το ισχύον πλαίσιο της ΕΕ για τη φοροδιαφυγή, που αφορά, την αποφυγή φορολόγησης περιουσιακών στοιχείων δεν μπορεί να εφαρμοστεί στην περίπτωση των κρυπτονομισμάτων, λόγω της ανωνυμίας τους και την εύκολη στην απόκρυψη φύση τους.

Για να είναι σε θέση να φορολογήσει, η φορολογική διοίκηση πρέπει να γνωρίζει τη φορολογητέα βάση και όταν πρόκειται για κρυπτονομίσματα, αυτό είναι εξαιρετικά δύσκολο.

Ένα άλλο παράδειγμα σχετίζεται με το πάγωμα και τη δήμευση περιουσιακών στοιχείων. Είναι αναμφισβήτητο ότι τα κρυπτονομίσματα εμπίπτουν στο πλαίσιο εφαρμογής των σχετικών ευρωπαϊκών κανόνων. Αυτοί οι κανόνες εφαρμόζονται σε κάθε φύσης ιδιοκτησία, κινητή ή ακίνητη, νομικά έγγραφα ή έγγραφα που αποδεικνύουν τίτλο ιδιοκτησίας. Τα κρυπτονομίσματα, φυσικά, εμπίπτουν στο πεδίο εφαρμογής αυτής της νομοθεσίας και: θα μπορούσαν να θεωρηθούν ως ασυνήθιστα κινητή ιδιοκτησία. Ωστόσο για να μπορείς να παγώσεις και να δημεύσεις κρυπτονομίσματα, είναι απαραίτητο να γνωρίζεις ότι τα κατέχει ένας παρανομούντας και αυτό είναι κάτι που αποτρέπεται από την ανωνυμία των κρυπτονομισμάτων.

Έτσι, η ουσία του θέματος είναι πώς μπορεί να αρθεί η ανωνυμία που σχετίζεται με κρυπτονομίσματα ώστε να ελεγχθούν οι παράνομες συναλλαγές.

5.3 Η λεπτή διαχωριστική γραμμή που χωρίζει την ασφάλεια στον κυβερνοχώρο, την προστασία δεδομένων και το απόρρητο.

Είναι αλήθεια ότι η κρυπτογράφηση, η οποία εφαρμόζεται στο πλαίσιο των κρυπτονομισμάτων, είναι ένας αποτελεσματικός τρόπος για τους πολίτες και τις επιχειρήσεις να αμυνθούν ενάντια στο ηλεκτρονικό έγκλημα, όπως είναι η κλοπή ταυτότητας και προσωπικών δεδομένων, η απάτη και η αποκάλυψη εμπιστευτικών πληροφοριών. Όμως, η κρυπτογράφηση μπορεί επίσης να χρησιμοποιηθεί από εγκληματίες, επομένως, είναι μια λεπτή γραμμή μεταξύ της διατήρησης της ισχυρής κρυπτογράφησης για την προστασία της κυβερνοασφάλειας, της προστασίας δεδομένων και του απορρήτου από τη μία πλευρά και της χρήσης για του εγκληματικούς σκοπούς, από την άλλη.

Τα κρυπτονομίσματα λειτουργούν με έξυπνη τεχνολογία. Για να επιβληθεί ο νόμος, θα πρέπει να αποτραπεί η χρήση αυτής της τεχνολογίας για κακόβουλους σκοπούς, αλλά ταυτόχρονα να μην εμποδίζει την ύπαρξη τεχνολογικής καινοτομίας. Επομένως, η νομοθετική δράση πρέπει πάντα να είναι αναλογική ώστε να αντιμετωπίζει το παράνομη συμπεριφορά, αλλά ταυτόχρονα να μην εμποδίζει την τεχνολογική καινοτομία.

Τα κρυπτονομίσματα εκτελούνται σε τεχνολογία blockchain. Αυτή η τεχνολογία είναι απολύτως νόμιμη και προσφέρει πολλά πλεονεκτήματα στην λειτουργία πολλών υπηρεσιών, συμπεριλαμβανομένων των ιδιωτικών και του δημόσιου τομέα.

Εάν τα κρυπτονομίσματα χρησιμοποιούνται για εγκληματικούς σκοπούς, δεν είναι επομένως η τεχνολογία που πρέπει να περιοριστεί, αλλά η παράνομη χρήση της.

Αυτό έγινε από την Ευρωπαϊκή Επιτροπή με την πρότασή για τροποποίηση του νόμου AMLD4315.

Τα προτεινόμενα μέτρα δεν έχουν αρνητικές επιπτώσεις στις τεχνολογικές εξελίξεις που παρουσιάζονται από την τεχνολογία κρυπτονομισμάτων, όμως προτείνουν καινοτόμους τρόπους για τη μείωση της απάτης, της διαφθοράς.

Ευρωπαϊκοί νόμοι για την καταπολέμηση εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας. Νόμος AMLD4

Η βασική αρχή του AMLD4 είναι η απαγόρευση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας μέσω του ξέπλυματος χρήματος.

5.4 Τα κρυπτονομίσματα στον νόμο AMLD4

Περιλαμβάνονται οι συναλλαγές σε κρυπτονομίσματα στο πεδίο εφαρμογής του AMLD4;

Αν και με πρώτη ματιά η παρακολούθηση των κρυπτονομισμάτων μπορεί να ενταχθεί κάτω από τον AMLD4, υπάρχει το εμπόδιο είναι η σύνδεση παράγοντας «ιδιοκτησία» ή «περιουσιακά στοιχεία»

Ορίζεται ως περιουσιακό στοιχείο οποιοδήποτε είδος περιουσία, κινητή ή ακίνητη, απτή ή άυλη, και

Με νομικά έγγραφα ή σε οποιαδήποτε μορφή, συμπεριλαμβανομένων ηλεκτρονικών ή ψηφιακών, αποδεικτικών τίτλων. Αν και δεν είναι προορισμένος για κρυπτονομίσματα, αυτός ο ορισμός είναι αρκετά ευρύς ώστε να περιλαμβάνει επίσης κρυπτονομίσματα, καθώς θα μπορούσαν να θεωρηθούν ως άυλα περιουσιακά στοιχεία.

Όμως πουθενά δεν υπάρχει καταγεγραμμένη η πράξη ιδιοκτησίας τους, ούτε καν η ανταλλαγή τους.

Αυτό υπέπεσε στην προσοχή της Ευρωπαϊκής Επιτροπής το 2016, η οποία κίνησε νομοθετική δράση να προσαρμόσει τις εικονικές πλατφόρμες ανταλλαγής κρυπτονομισμάτων και τους παρόχους πορτοφολιών στο πεδίο εφαρμογής του.

5.5 Η συμπερίληψη των κρυπτονομισμάτων στον νόμο AMLD5354

Στο μεγαλύτερο μέρος της τεκμηρίωσης της νομοθετικής πολιτικής χρησιμοποιείται ο όρος "εικονικά νομίσματα" αντί για κρυπτονομίσματα.

Σημαντικό είναι ότι τα κρυπτονομίσματα είναι μια υποκατηγορία εικονικών νομισμάτων, περισσότερο ιδιαίτερα αυτού του είδους τα εικονικά νομίσματα που έχουν αμφίδρομη σύνδεση με την πραγματική οικονομία.

Επομένως, όταν σε όλη αυτή την ανάλυση του κανονιστικού πλαισίου αναφερόμαστε σε εικονικά νομίσματα, αυτό περιλαμβάνει τα κρυπτονομίσματα. Επιπλέον, όταν εξετάζουμε το ακριβές πεδίο εφαρμογής των ορισμών που περιλαμβάνονται στα διάφορα έγγραφα πολιτικής, υπάρχει σαφής στόχευση προς τα κρυπτονομίσματα.

6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Το φαινόμενο των κρυπτονομισμάτων βρίσκεται, αναμφισβήτητα, στο κέντρο του παγκόσμιου ενδιαφέροντος τα τελευταία χρόνια. Αποτελούν, όμως, μια νέα τεχνολογία και πρέπει να μάθουμε πολλά για αυτήν. Υπάρχουν πολλές ανησυχίες ότι η διάδοση και η χρήση κρυπτονομισμάτων θα κλονίσει τα παραδοσιακά χρηματοοικονομικά συστήματα.

Στην αρχή της εποχής των κρυπτονομισμάτων, το Bitcoin φάνηκε να είναι ο αναμφισβήτητος ηγέτης. Στη συνέχεια, το Ethereum, το Ripple και άλλα νομίσματα άρχισαν να καλύπτουν την διαφορά. Οι αναλυτές άρχισαν να συζητούν εάν τα κρυπτονομίσματα είναι πραγματικά νομίσματα. Μερικοί προέβλεπαν ακόμη μεγαλύτερες αλλαγές. Η ιδέα ότι τα κρυπτονομίσματα θα μπορούσαν να αντικαταστήσουν πλήρως τα μετρητά, άρχισε να πλανάται στην ατμόσφαιρα.

Ένα σημαντικό θέμα είναι ότι τα κρυπτονομίσματα δεν μπορούν να χειραγωγηθούν τόσο εύκολα όσο το νόμισμα fiat, κυρίως λόγω της αποκεντρωμένης και μη ελεγχόμενης κατάστασής τους. Πέρα από αυτό, τα κρυπτονομίσματα θα μπορούσαν να υποστηρίξουν καλύτερα την ιδέα ενός παγκόσμιου βασικού εισοδήματος από ότι τα νομίσματα fiat. Επιπλέον, τα κρυπτονομίσματα θα μπορούσαν να βοηθήσουν να απαλλαγούμε από τους μεσάζοντες στις καθημερινές συναλλαγές. Αυτό θα μπορούσε να μειώσει το κόστος για τις επιχειρήσεις και να βοηθήσει τους καταναλωτές.

Φυσικά, υπάρχουν επίσης πολλές σκέψεις και ανησυχίες σχετικά με αυτό το σενάριο. Εάν τα κρυπτονομίσματα ξεπεράσουν τα συμβατικά χρήματα ως προς τη χρήση, τα παραδοσιακά νομίσματα θα χάσουν μέρος από την αξία τους. Εάν τα κρυπτονομίσματα κυριαρχήσουν εξ ολοκλήρου, θα πρέπει να αναπτυχθούν συνθήκες ώστε ο κόσμος να μπορέσει να προσαρμοστεί. Αναπόφευκτα θα υπάρξουν δυσκολίες στην μετάβαση, καθώς τα μετρητά θα μπορούσαν να καταστούν άχρηστα αρκετά γρήγορα, αφήνοντας πίσω πολίτες με χαμένες περιουσίες. Τα χρηματοπιστωτικά ιδρύματα, επίσης, θα πρέπει να σπεύσουν για να αλλάξουν την οργάνωση και τον τρόπο λειτουργίας τους.

Πέρα από τον αντίκτυπο που θα φέρει ένα μέλλον με κυρίαρχα τα κρυπτονομίσματα στους απλούς πολίτες και στα χρηματοπιστωτικά ιδρύματα, οι ίδιες οι κυβερνήσεις θα υποφέρουν. Ο κυβερνητικός έλεγχος στα κεντρικά νομίσματα είναι το κλειδί για τον έλεγχο πολλών άλλων τομέων και τα κρυπτονομίσματα λειτουργούν με πολύ λιγότερες παρεμβάσεις από τις κυβερνήσεις. Οι κυβερνήσεις δεν θα μπορούσαν πλέον, για παράδειγμα, να εκτυπώσουν χρήματα ως αντίδραση σε εξωτερικές και εσωτερικές πιέσεις. Αντίθετα, η παραγωγή νέων νομισμάτων θα εξαρτάται από ανεξάρτητες δραστηριότητες εξόρυξης κρυπτονομισμάτων.

Οι υποστηρικτές του Bitcoin και άλλων κρυπτονομισμάτων ισχυρίζονται ότι οι κρύπτο-χρηματοοικονομικές πλατφόρμες είναι εντελώς αξιόπιστα συστήματα ακριβώς επειδή δεν συνδέονται άμεσα με κανένα κράτος, κυβέρνηση ή οργανισμό.

Από την άλλη πλευρά, οι αναλυτές αναφέρουν ότι αυτό δεν είναι απολύτως ακριβές. Η υποτιθέμενη αξιοπιστία του κάθε κρυπτονομίσματος βασίζεται στο παγκοσμίως διαμερισμένο δίκτυο των κόμβων που διαχειρίζεται το blockchain του. Όμως αυτό δεν είναι πραγματικά αξιόπιστο. Για παράδειγμα, πολλοί από τους κόμβους που στηρίζουν κρυπτονομίσματα όπως το Bitcoin, βρίσκονται στην Κίνα. Η κινεζική κυβέρνηση θα μπορούσε θεωρητικά να κάνει αλλαγές στα κρυπτονομίσματα σε θεμελιώδες επίπεδο επιβάλλοντας τη βούλησή της στους miners που τα κρατούν σε λειτουργία.

Η συμβολή του Facebook στον κόσμο της κρυπτογράφησης με το κρυπτονομίσμα Libra, θεωρείται από κάποιους η λύση σε διάφορα οικονομικά ζητήματα. Συγκεκριμένα, η πλατφόρμα

σχεδιάστηκε για να διευκολύνει τις διεθνείς πληρωμές και να εξαλείφει τα περιττά κόστη και τις χρεώσεις συναλλαγών.

Η προσέγγιση των αναλυτών, σε αυτό, είναι ότι ο στόχος είναι αξιοθαύμαστος, αλλά η προσέγγιση είναι λανθασμένη. Δεν είναι κατανοητό πως η εισαγωγή ακόμα ενός κρυπτονομίσματος είναι η σωστή λύση για την ελαχιστοποίηση των συναλλαγών πληρωμής και γιατί το Facebook προσπαθεί να παρακάμψει πλήρως τα παραδοσιακά τραπεζικά συστήματα.

Μια καλύτερη προσέγγιση από το Facebook θα ήταν, ενδεχομένως, να δημιουργήσει την δική του τράπεζα που θα μπορούσε να λειτουργήσει ως βασικό χρηματοπιστωτικό ίδρυμα για τους χρήστες του. Η εταιρεία θα μπορούσε να επικεντρωθεί στην οικοδόμηση τραπεζικών συστημάτων προσαρμοσμένων σε κάθε κράτος ή περιοχή, στην αντιμετώπιση κανονιστικών απαιτήσεων και στη μείωση του κόστους. Μόλις αυτά θα είχαν καθιερωθεί και θα είχε εδραιωθεί η εμπιστοσύνη του κοινού, τότε θα ήταν λογικό να συνδεθούν όλα σε ένα παγκόσμιο δίκτυο.

Μια άλλη προσέγγιση είναι αυτή των κρυπτονομισμάτων σταθερής αξίας. Τα σταθερά κρυπτονομίσματα έχουν δει αύξηση της δημοτικότητας τους, επειδή έχουν σαν χαρακτηριστικό τους την στήριξη της αξίας του κρυπτονομίσματος με περιουσιακά στοιχεία που κατέχουν πραγματική αξία, όπως και το νόμισμα των ΗΠΑ στο παρελθόν. Αυτά τα περιουσιακά στοιχεία θα μπορούσαν να είναι άλλα νομίσματα ή εμπορεύματα, σχεδόν οτιδήποτε αντικείμενο αξίας.

Υπάρχουν μερικά ζητήματα που προκύπτουν από αυτήν την προσέγγιση. Πρώτον, δημιουργεί ουσιαστικά ένα σύστημα που υπάρχει ήδη. Το άλλο ζήτημα είναι ότι θα μπορούσε να διευκολύνει τους ανθρώπους να διαπράξουν απάτη, καθώς δεν είναι τόσο εύκολο να ελεγχθούν και να παρακολουθηθούν όσο τα παραδοσιακά νομίσματα.

Όμως, οι προβλέψεις είναι πάντα δύσκολες και τα κρυπτονομίσματα, αυτή τη στιγμή, αποτελούν μια πραγματικότητα, όσο και αν κάποιοι δεν θέλουν να το πιστέψουν. Τα πράγματα χρειάζονται χρόνο, αλλά η αντίστροφη μέτρηση έχει ξεκινήσει. Τα κρυπτονομίσματα έχουν γίνει πιο δημοφιλή από ό, τι ο περισσότερος κόσμος. Σύμφωνα με μια έρευνα, περίπου το 18% των φοιτητών που βρίσκονται στις ΗΠΑ είτε έχουν τουλάχιστον ένα ψηφιακό νόμισμα στην κατοχή τους, είτε είχαν ένα στο παρελθόν.

Αυτό που είναι ακόμη πιο αξιοσημείωτο είναι ότι ίσως βρισκόμαστε κοντά στο τέλος των χρημάτων fiat. Αυτό θα είναι κάτι πολύ «βαρύ» για το χώρο της οικονομίας. Οι συνέπειες θα είναι εντελώς απρόβλεπτες. Αυτό το γνωρίζουν, εδώ και καιρό, οι άνθρωποι που ανήκουν στην κοινότητα των κρυπτονομισμάτων, όμως οι τράπεζες αρχίζουν, τώρα, να το συνειδητοποιούν.

Το πραγματικό θύμα της κρυπτογράφησης μπορεί να μην είναι, τελικά, τα νομίσματα fiat, αλλά οι πλαστικές κάρτες. Για δεκαετίες τώρα, σταδιακά καταργούμε τα μετρητά. Τα μετρητά, οι πιστωτικές και χρεωστικές κάρτες καθίστανται ξεπερασμένα και θα συνεχίσουν να είναι, καθώς αυξάνεται η αποδοχή των κρυπτονομισμάτων.

Ας σκεφτούμε την εξέλιξη, περάσαμε από τα χαρτονομίσματα και τα κέρματα σε διαδικτυακές συναλλαγές με χρεωστικές και πιστωτικές κάρτες. Η αύξηση των πληρωμών μέσω κινητού μέσω των WeChat Pay, AliPay και Paypal ήδη καθιστά περιττές τις πλαστικές κάρτες. Το Blockchain προσφέρει πολλά πλεονεκτήματα σε σχέση με τις πλαστικές κάρτες, αλλά η βασική διαφορά μεταξύ των δύο είναι ότι όλες οι πληρωμές και οι μεταφορές γίνονται με την πλήρη συναίνεση του χρήστη. Η Deutsche Bank πιστεύει ότι οι πλαστικές κάρτες θα μπορούσαν να πεθάνουν. Καθώς αυξάνεται η υιοθέτηση κρυπτονομισμάτων, είναι λογικό να υποθέσουμε ότι οι πιστωτικές κάρτες θα εξαφανιστούν, επειδή απλά δεν θα τις χρειαζόμαστε.

Αυτό που τελικά μπορούμε να πούμε είναι ότι παρόλο τους κινδύνους υπάρχουν ορισμένες εφαρμογές όπου τα κρυπτονομίσματα είναι μια βιώσιμη λύση. Καθώς θα ξεπερνούν τα νομικά εμπόδια, τα κρυπτονομίσματα μπορεί να γίνουν νόμιμα υποκατάστατα του νομίσματος. Αλλά αυτό θα γίνει με σχετικό κρατικό έλεγχο, όπως με τις σχετικές προσπάθειες που καταβάλλει η Ευρωπαϊκή Ένωση.

Η ρύθμιση της λειτουργίας των κρυπτονομισμάτων και η επίσημη ένταξη τους στο παγκόσμιο χρηματοπιστωτικό σύστημα, ίσως να είναι πολύ κοντά. Καθώς ξεπερνούνται τα ρυθμιστικά εμπόδια, τα κρυπτονομίσματα μπορεί να γίνουν νόμιμα υποκατάστατα του νομίσματος. Οι κυβερνήσεις, φυσικά, δεν θα καθίσουν να χάσουν τον έλεγχο του χρήματος χωρίς σκληρό αγώνα. Θα προσπαθήσουν να μπουν στο παιχνίδι είτε με έλεγχο, είτε με συνσυμμετοχή, είτε με δημιουργία κρατικά ελεγχόμενων κρυπτονομισμάτων⁷.

Τα κρυπτονομίσματα μπορεί να είναι κάτι καλό ή κακό, όπως όλα τα πράγματα στη ζωή. Πολλοί άνθρωποι δεν καταλαβαίνουν την πραγματική αξία του κρυπτονομίσματος, επειδή επικεντρώνονται μόνο σε κερδοσκοπικές συναλλαγές, λόγω της μεταβλητότητας της τιμής τους.

Τα κρυπτονομίσματα προσφέρουν μια μοναδική πρόταση που καθιστά τα νόμισματα fiat ξεπερασμένα. Τα κρυπτονομίσματα δίνουν τη δυνατότητα στους ανθρώπους να είναι η δική τους ιδιωτική τράπεζα με ιδιωτικούς τρόπους πληρωμής. Αν και τα σημαντικότερα εμπόδια στην γενικότερη αποδοχή τους είναι ρυθμιστικής και λειτουργικής φύσης, τελικά ο αποφασιστικός παράγοντας για το αν θα αντικαταστήσουν τα μετρητά είναι η υιοθέτηση τους από την μεριά του χρήστη. Όμως, μόλις ολοκληρωθεί η πρώτη δύσκολη φάση και ενταχθούν στη ζωή μας, τα κρυπτονομίσματα θα κάνουν τον κόσμο να φαίνεται εντελώς διαφορετικός, με τρόπους που μόλις αρχίσαμε να καταλαβαίνουμε.

⁷ Ορισμένα από τα νησιά της Ανατολικής Καραϊβικής, συμπεριλαμβανομένων της Γρενάδας και του Σεντ Κιτς και Νέβις, έχουν ήδη εκδώσει το δικό τους ψηφιακό νόμισμα, το οποίο βρίσκεται τώρα σε δοκιμαστική φάση. Η πρώτη μεγάλη κεντρική τράπεζα που θα εκδώσει νόμισμα σε μεγάλη κλίμακα θα είναι πιθανότατα η Λαϊκή Τράπεζα της Κίνας. Μετά από πέντε χρόνια έρευνας, η PBOC δήλωσε τον Αύγουστο ότι το ψηφιακό της νόμισμα πλησιάζει. Η σουηδική Riksbank διερευνά ένα νόμισμα e-krona, η Ουρουγουάη έχει προχωρήσει σε ένα πιλοτικό πρόγραμμα που ονομάζεται e-Peso και οι κεντρικές τράπεζες της Νότιας Αφρικής και της Ελβετίας διερευνούν ήδη τη δημιουργία ψηφιακού νομίσματος (πηγή capital.gr)

7 ΒΙΒΛΙΟΓΡΑΦΙΑ

7.1 ΒΙΒΛΙΑ – ΜΕΛΕΤΕΣ – ΕΡΓΑΣΙΕΣ

The Economics of Cryptocurrencies - Bitcoin and Beyond*

Jonathan Chiu - Bank of Canada - Victoria University of Wellington
Thorsten Koeppl = Queen's University
April, 2017

Understanding Cryptocurrencies

Wolfgang Karl Härdle - Campbell R. Harvey - Raphael C. G. Reule
IRTG 1792 Discussion Paper 2018-44
<http://irtg1792.hu-berlin.de>
ISSN 2568-5619

Analysis of Data Management in Blockchain-based Systems: From Architecture to Governance

HYE-YOUNG PAIK - XIWEI XU - HMN DILUM BANDARA - SUNG UNE LEE - SIN KUANG LO
First version: March, 2017 This version: September, 2018
https://www.bis.org/events/eopix_1810/chiu_paper.pdf

BITCOIN AND ETHEREUM EVOLUTION

Egor Zmaznev
Thesis
CENTRIA UNIVERSITY OF APPLIED SCIENCES
Business Management
November 2017

Cryptocurrency Market Analysis from the Open Innovation Perspective

Alexey Mikhaylov
Research Center of Monetary Relations, Financial University under the Government of the Russian Federation, 124167 Moscow, Russia; ayumihajlov@fa.ru
Received: 27 October 2020; Accepted: 14 December 2020; Published: 17 December 2020

Virtual Money: How Much do Cryptocurrencies Alter the Fundamental Functions of Money?

Requested by the ECON committee
Authors: Eddie GERBA and Margarita RUBIO
Requested by the TAX3 committee – European Parliament
PE 642.360 - November 2019

Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion (STUDY)

Policy Department for Economic, Scientific and Quality of Life Policies
Authors: Prof. Dr. Robby HOUBEN, Alexander SNYERS
Directorate-General for Internal Policies – European Parliament
PE 619.024 - July 2018

7.2 ΙΣΤΟΣΕΛΙΔΕΣ

What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives By Brian Martucci

<https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/>

What Is Blockchain? Blockchain Explained By Jeffrey M Green

<https://www.thebalance.com/what-is-blockchain-5088260>

History of Cryptocurrency By Eric Rosenberg

<https://www.thebalance.com/history-of-cryptocurrency-5119511>

A short history of cryptocurrencies by Davies

<https://www.daviescoin.io/blog/a-short-history-of-cryptocurrencies>

4 Major Types of Cryptocurrency (+What They're Good For)

<https://learn.g2.com/types-of-cryptocurrency>

PI White Paper

<https://minepi.com/white-paper>

Could Cryptocurrencies Replace Cash?

<https://www.investopedia.com/news/could-cryptocurrencies-replace-cash-bitcoin-flipping/>

Is Cryptocurrency the Future of Money?

by Ilias Louis Hatzis

https://www.finyear.com/Is-Cryptocurrency-the-Future-of-Money_a41914.html

What Does the Future Hold for Cryptocurrency?

<https://online.stanford.edu/future-for-cryptocurrency>