ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ
ΛΟΓΙΣΤΙΚΗ ΚΑΙ ΕΛΕΓΚΤΙΚΗ

Διπλωματική Εργασία

Η Λογιστική Αντιμετώπιση των Κρυπτονομισμάτων

της

Βεροπλίδου Άννας

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος
στην
Εφαρμοσμένη Λογιστική και Ελεγκτική

2022

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας διπλωματικής είναι να εξετάσει τα κρυπτονομίσματα και τις τεχνολογίες που χρησιμοποιούν για τη δημιουργία τους, τη λειτουργία τους και την πραγματοποίηση συναλλαγών τους στο δίκτυο. Για την επίτευξη του παραπάνω στόχου, γίνεται λεπτομερής αναφορά στην δομή και στον τρόπο με τον οποίο αξιοποιείται η τεχνολογία του Blockchain στα κρυπτονομίσματα. Ακόμη μέσα από την εξέταση της περίπτωσης του Bitcoin, που αποτελεί και το πρώτο κρυπτονόμισμα που υπήρξε ποτέ στην διεθνή αγορά των κρυπτονομισμάτων διαπιστώνεται ότι έχει αρκετά οφέλη και σύντομα θα κατακτήσει τις διαδικτυακές συναλλαγές. Στο τέλος του εγγράφου ερευνάται η λογιστική και η φορολογική αντιμετώπιση των κρυπτονομισμάτων ως ένα καινούργιο γεγονός όπου οι κυβερνήσεις σε όλο τον κόσμο αντίστοιχα και στην Ελλάδα προσπαθούν είτε να το εντάξουν σ ένα θεσμικό πλαίσιο είτε να δημιουργήσουν ένα νέο λογιστικό πρότυπο.

Λέξεις κλειδιά: κρυπτονόμισμα, Blockchain, Bitcoin, λογιστικά πρότυπα, φορολογικό σύστημα.

ABSTRACT

The purpose of this dissertation is to examine cryptocurrencies and the technologies they use to create, operate and conduct transactions on the network. To achieve the above objective, a detailed discussion of the structure and how Blockchain technology is utilized in cryptocurrencies is provided. Further through the examination of the case of Bitcoin, which is the first cryptocurrency that ever existed in the international cryptocurrency market, it is found that it has several benefits and will soon conquer online transactions. At the end of the paper, the accounting and tax management of cryptocurrencies is investigated as a new event where governments all over the world and Greece respectively are trying to either incorporate it into an institutional framework or create a new accounting standard.

Keywords: cryptocurrency, Blockchain, Bitcoin, accounting standards, tax system.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγικές Παρατηρήσεις

Ζούμε σε έναν γρήγορο κόσμο, σε έναν καινοτόμο κόσμο που αναπτύσσεται με τεράστια ταχύτητα, όπου η τεχνολογία και το χρήμα συμβαδίζουν εδώ και αιώνες, ξεκινώντας με τον πρώτο άβακα. Στις αρχές του 17ου αιώνα ξεκίνησε να χρησιμοποιείται το χάρτινο χρήμα, μετά μεταβήκαμε στο τραπεζικό χρήμα, στη συνέχεια στα χαρτονομίσματα και στο πλαστό χρήμα. Κάθε μέρα είναι μια ευκαιρία για κάτι καινούργιο να δούμε και να μάθουμε και εκεί που νομίζουμε ότι αυτό ήταν, έρχονται κι άλλες αλλαγές. Μια από τις μεγαλύτερες αλλαγές της τεχνολογίας στον σύγχρονο κόσμο, που έχει προσελκύσει μεγάλη προσοχή του κοινού, είναι το φαινόμενο των κρυπτονομισμάτων. Σύμφωνα με ορισμένες απόψεις, πρόκειται για τη μεγαλύτερη τεχνολογική εφεύρεση των τελευταίων δέκα ετών. Έτσι, τα κρυπτονομίσματα έγιναν πολύ δημοφιλή μέσα σε πολύ σύντομο χρονικό διάστημα.

Τα κρυπτονομίσματα εμπίπτουν στην κατηγορία των ψηφιακών νομισμάτων, των εναλλακτικών νομισμάτων και των εικονικών νομισμάτων. Αρχικά σχεδιάστηκαν για να παρέχουν μια εναλλακτική μέθοδο πληρωμής για διαδικτυακές συναλλαγές. Ωστόσο, δεν έχουν γίνει ακόμη ευρέως αποδεκτά από τις επιχειρήσεις και τους καταναλωτές και επί του παρόντος είναι πολύ ασταθή για να είναι κατάλληλα ως μέθοδοι πληρωμής. Τα κρυπτονομίσματα διαφέρουν σημαντικά από τα παραδοσιακά νομίσματα, διότι χρησιμοποιούν κρυπτογραφία για την ασφάλεια των συναλλαγών και κάθε τι νέο που εμφανίζεται ελέγχεται από το δικό του σύστημα. Είναι δυνατόν να πούμε ότι το κρυπτονομίσματα είναι ένα υποσύνολο των ψηφιακών νομισμάτων. Παρ' όλα αυτά, μπορεί κανείς να τα αγοράσει και να τα πουλήσει όπως κάθε άλλο περιουσιακό στοιχείο.

Το πρώτο κρυπτονόμισμα που υπήρξε ποτέ ήταν το Bitcoin, που κυκλοφόρησε τον Ιανουάριο του 2009. Μετά από αυτό, πολλά άλλα κρυπτονομίσματα εμφανίστηκαν στην αγορά, αλλά ονομάστηκαν altcoins, καθώς αντιπροσώπευαν το μείγμα του

Bitcoin των εναλλακτικών νομισμάτων. Σήμερα υπάρχουν σχεδόν περίπου 6000 κρυπτονομίσματα διαθέσιμα στο διαδίκτυο.

1.2 Σκοπός της εργασίας

Σκοπός της παρούσας διπλωματικής εργασίας είναι η μελέτη όλων των θεωρητικών πτυχών των κρυπτονομισμάτων, εξετάζοντας ειδικότερα τον τρόπο με τον οποίο δημιουργήθηκαν και εξελίχθηκαν με βάση το θεωρητικό υπόβαθρο της διατριβής. Τα κρυπτονομίσματα είναι δύσκολο να γίνουν κατανοητά επειδή είναι νέα σε πολλά επίπεδα: είναι νέες τεχνολογίες πληροφορικής, μηχανικής και νέα εμπορεύσιμα μέσα, οπότε θα γίνει μια προσπάθεια να εξηγηθεί με σαφήνεια η έννοια, η προέλευση, ο σχεδιασμός, τα χαρακτηριστικά, η ιστορία και ο μηχανισμός των κρυπτονομισμάτων. Οι οικονομολόγοι και το ευρύ κοινό έχουν εξετάσει την οικονομία των κρυπτονομισμάτων ενός εικονικού περιουσιακού στοιχείου που έχει σχεδιαστεί για να ανταγωνίζεται τα νομίσματα όμως, η απουσία θεσμικών πλαισίων σχετικά με την λογιστική αντιμετώπιση τους, οδηγεί στην ανάγκη εξέτασης του παρόντος θέματος.

1.3 Ερευνητικά ερωτήματα

Έχοντας διευκρινίσει το στόχο της παρούσας διατριβής, θα παρατεθούν βασικά ερευνητικά ερωτήματα, οποία θα απαντηθούν μέσω της μελέτης.

Συγκεκριμένα , τι είναι η τεχνολογία blockchain;

Μπορούν τα κρυπτονομίσματα που διαθέτουν ισχυρή τεχνολογία και ανώνυμα χαρακτηριστικά να αποτελέσουν το χρήμα του μέλλοντος;

Ένα άλλο ζωτικής σημασίας ερώτημα που προκύπτει αφορά το θεσμικό πλαίσιο και πιο συγκεκριμένα ποια είναι η λογιστική αντιμετώπιση των κρυπτονομισμάτων;

1.4 Δομή της Εργασίας

Η δομή της εργασίας θα χωριστεί σε τέσσερα κεφάλαια. Στο πρώτο κεφάλαιο γίνεται μια ιστορική αναδρομή στην εξέλιξη του χρήματος και στο πως εμφανίστηκαν τα κρυπτονομίσματα. Στο ίδιο κεφάλαιο αναφέρεται και ο σκοπός που γίνεται η παρούσα μελέτη. Στο επόμενο κεφάλαιο παρατίθεται η επισκόπηση βιβλιογραφίας η οποία αποτελεί βασικό μέρος της διπλωματικής εργασίας διότι μέσα από την μελέτη αυτήν οι αναγνώστες θα γνωρίσουν την ιστορία, την εξέλιξη αλλά και το πώς δημιουργούνται τα κρυπτονομίσματα. Ακόμη θα αναλυθούν όροι όπως: η Κρυπτογραφία, το Bitcoin, Pow, Pos, η εξόρυξη (Mining) και η τεχνολογία Blockchain μαζί με τα πλεονεκτήματα και τα μειονεκτήματά της. Στο τρίτο κεφάλαιο που αποτελεί και το κύριο μέρος της διατριβής γίνεται μια προσπάθεια αποτύπωσης της λογιστικής και φορολογικής αντιμετώπιση των κρυπτονομισμάτων. Τέλος, παρατίθενται τα συμπεράσματα που προκύπτουν από την εργασία αλλά και οι προτάσεις για μελλοντική έρευνα.

ΚΕΦΑΛΑΙΟ 2

ΕΠΙΣΚΟΠΗΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑΣ

2.1 Εισαγωγή

Τα κρυπτονομίσματα είναι ένας τομέας αυξημένης νομισματικής, τεχνολογικής και επενδυτικού ενδιαφέροντος. Παρόλα αυτά η ολοκληρωμένη κατανόηση των θεωριών και των θεμελίων τους εξακολουθεί να λείπει από ορισμένους επαγγελματίες και ενδιαφερόμενους φορείς, ακόμη και όταν ο χώρος έχει αναπτυχθεί. Ο κόσμος των κρυπτονομισμάτων είναι και εικονικός και πραγματικός, δεδομένου ότι προσβλέπει σε υλικά κέρδη, ενώ ταυτόχρονα υποβιβάζεται σε μια αποκεντρωμένη ψηφιακή αρχιτεκτονική που βασίζεται σε κώδικα και υπολογιστές. Σήμερα υπάρχει ένα ιδιαίτερο ενδιαφέρον για τις έννοιες των εικονικών περιουσιακών στοιχείων με την ευρύτερη έννοια του όρου, στο πλαίσιο των οποίων τα κρυπτονομίσματα αποτελούν μια σημαντική κατηγορία, η οποία θα αναλυθεί εκτενώς στο κεφάλαιο αυτό.

2.2 Κρυπτονομίσματα

2.2.1 Γενικές πληροφορίες και Ιστορικό

Η ιστορία των εικονικών νομισμάτων ξεκινά με τον κρυπτογράφο David Chaum. Το 1983, ανέπτυξε ένα κρυπτογραφικό σύστημα με την ονομασία eCash. Δώδεκα χρόνια αργότερα, ανέπτυξε ένα άλλο σύστημα, το Digi Cash, το οποίο χρησιμοποιούσε κρυπτογραφία για να καταστήσει τις οικονομικές συναλλαγές εμπιστευτικές.

Ωστόσο, για πρώτη φορά η ιδέα ή ο όρος "κρυπτονόμισμα" επινοήθηκε το 1998. Εκείνη τη χρονιά, ο Wei Dai άρχισε να σκέφτεται την ανάπτυξη μιας νέας μεθόδου πληρωμών που χρησιμοποιούσε κρυπτογραφικό σύστημα και της οποίας το κύριο

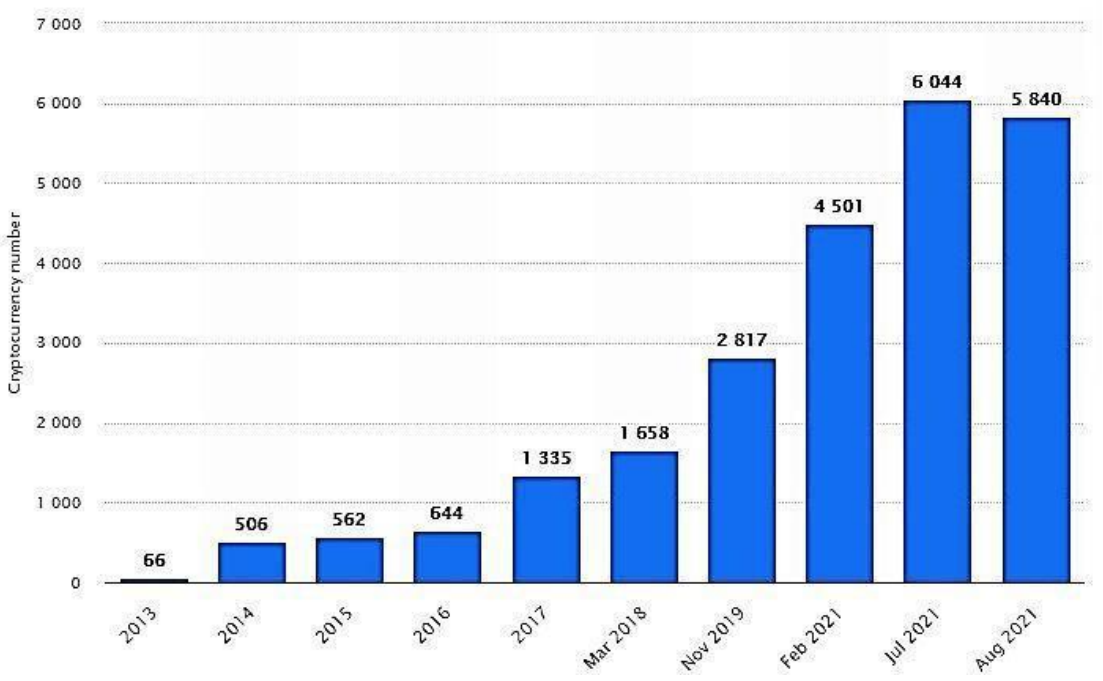
χαρακτηριστικό ήταν η αποκέντρωση[1]. Μετά από αυτό, ο Nick Szabo επινόησε το "bitgold". Θεωρείται ο άμεσος πρόδρομος για την κατασκευή του Bitcoin. Το "bitgold" αντιπροσώπευε έναν μηχανισμό που χρησιμοποιήθηκε για ένα αποκεντρωμένο ψηφιακό νόμισμα, αλλά δεν έγινε ποτέ πλήρως αποδεκτό και δεν εφαρμόστηκε. Η ιδέα ήταν οι συμμετέχοντες να λύνουν κρυπτογραφικούς γρίφους με τους υπολογιστές τους, και μέσω αυτού του δικτύου, όλοι οι γρίφοι που λύνονταν θα στέλνονταν σε ένα δημόσιο μητρώο που ονομάζεται "Byzantine-fault-tolerant" και θα εκχωρούσαν στον λύτη ένα δημόσιο κλειδί. Έτσι, κάθε λύση γίνεται απλώς μέρος της επόμενης πρόκλησης, αλλά αν η πλειοψηφία των συμμετεχόντων δεν συμφωνήσει να δεχτεί νέες λύσεις, ο επόμενος γρίφος δεν θα μπορούσε να ξεκινήσει.

Το 2009 κυκλοφόρησε μια πρόταση για το Bitcoin και πολλοί υποψιάστηκαν ότι ήταν ο Szabo που την έφτιαξε, αλλά αυτή τη φορά με το όνομα Satoshi Nakamoto. Ο ίδιος το αρνήθηκε κατηγορηματικά, αλλά υπήρξαν πολλές μελέτες και ερευνητές που προσπάθησαν να αποδείξουν ότι όντως είναι αυτός. Πρόθεσή του ήταν να δημιουργήσει έναν νέο τρόπο πληρωμής που θα μπορούσε να χρησιμοποιηθεί διεθνώς, αποκεντρωμένα (δηλαδή, ότι θα είναι απαραβίαστο από τρίτους, και διαθέσιμο σε οποιονδήποτε έχει πρόσβαση στο διαδίκτυο) και χωρίς να έχει πίσω του κάποιο χρηματοπιστωτικό ίδρυμα[2].

Τον Οκτώβριο του 2011 κυκλοφόρησε το Litecoin. Στα τέλη του 2012, το WordPress έγινε ο πρώτος μεγάλος έμπορος που δέχεται πληρωμές σε Bitcoin. Πολλές εταιρείες επιτρέπουν πλέον την πληρωμή των προϊόντων και υπηρεσιών με αυτά τα εικονικά νομίσματα και δημιούργησαν ακόμη και τα δικά τους. Τον Ιούνιο του 2021, το Ελ Σαλβαδόρ έγινε η πρώτη χώρα που αποδέχεται το Bitcoin ως νόμιμο χρήμα. Τον Αύγουστο του 2021, ακολούθησε η Κούβα με το ψήφισμα 215 για την αποδοχή του Bitcoin ως νόμιμο χρήμα. Τέλος από το 2013 μέχρι τον Αύγουστο του 2021 παρατηρήθηκε απότομη αύξηση του αριθμού των κρυπτονομισμάτων από 66 σε 5840.

[1]Bholane, K. P. (2021). Pros and Cons of Cryptocurrency: A Brief Overview. National Journal of Research in Marketing, Finance & HRM, 6(3), 71-78.

[2]Milutinović, M. (2018). Cryptocurrency.



Διάγραμμα 2.2: Αριθμός χαρτονομισμάτων παγκοσμίως από το 2013 έως τον Αύγουστο του 2021 (Πηγή: Bholane, K. P. (2021). Pros and Cons of Cryptocurrency: A Brief Overview)

2.2.2 Ορισμοί

Ο ορισμός των κρυπτονομισμάτων δεν είναι εύκολη υπόθεση, όπως και η αλυσίδα μπλοκ, έτσι και τα κρυπτονομίσματα έχουν γίνει μια "λέξη της μόδας" για να αναφερθούν σε ένα ευρύ φάσμα τεχνολογικών εξελίξεων που χρησιμοποιούν μια τεχνική πιο γνωστή ως κρυπτογραφία. Με απλά λόγια, η κρυπτογραφία είναι η τεχνική προστασία των πληροφοριών με τη μετατροπή τους (δηλαδή την κρυπτογράφησή τους) σε μια μη αναγνώσιμη μορφή που μπορεί να αποκρυπτογραφηθεί (ή να κρυπτογραφηθεί) μόνο από κάποιον που κατέχει ένα μυστικό κλειδί. Τα κρυπτονομίσματα, όπως το Bitcoin, εξασφαλίζονται μέσω αυτής της τεχνικής χρησιμοποιώντας ένα έξυπνο σύστημα δημόσιων και ιδιωτικών ψηφιακών κλειδιών.
Στη συνέχεια θα προσπαθήσουμε να δώσουμε έναν κατάλληλο ορισμό των κρυπτονομισμάτων βάσει μιας κριτικής ανάλυσης των ορισμών που έχουν ήδη αναπτυχθεί από διάφορους ενδιαφερόμενους φορείς χάραξης πολιτικής σε ευρωπαϊκό και διεθνές επίπεδο.

2.2.3 Οι υπεύθυνοι χάραξης πολιτικής

Από την εμφάνιση του Bitcoin το 2009, το θέμα των κρυπτονομισμάτων έχει εξεταστεί από διάφορους φορείς χάραξης πολιτικής, οι οποίοι έχουν αγγίξει το θέμα με διαφορετικό τρόπο.

Α) Ευρωπαϊκή Κεντρική Τράπεζα ("ΕΚΤ")

Η Ευρωπαϊκή Κεντρική Τράπεζα ("ΕΚΤ") έχει ταξινομήσει τα κρυπτονομίσματα ως υποσύνολο των εικονικών νομισμάτων. Σε έκθεσή της το 2012 σχετικά με τα συστήματα εικονικών νομισμάτων, όρισε τα εν λόγω νομίσματα ως μια μορφή μη ρυθμιζόμενου ψηφιακού χρήματος, τα οποία συνήθως εκδίδονται και ελέγχονται από τους προγραμματιστές του και χρησιμοποιούνται μεταξύ των μελών μιας συγκεκριμένης εικονικής κοινότητας. Περαιτέρω μπορούν να διακριθούν τρεις τύποι εικονικών νομισμάτων ανάλογα με την αλληλεπίδραση που έχουν με τα παραδοσιακά νομίσματα και την πραγματική οικονομία:

i. εικονικά νομίσματα που μπορούν να χρησιμοποιηθούν μόνο σε ένα κλειστό εικονικό σύστημα, συνήθως σε διαδικτυακά παιχνίδια (π.χ. World of Warcraft Gold),

ii. εικονικά νομίσματα που συνδέονται μονομερώς με την πραγματική οικονομία. Υπάρχει μια ισοτιμία μετατροπής για την αγορά του νομίσματος (με παραδοσιακό χρήμα) και το αγορασμένο νόμισμα μπορεί στη συνέχεια να χρησιμοποιηθεί για την αγορά εικονικών αγαθών και υπηρεσιών (κατ' εξαίρεση και για την αγορά πραγματικών αγαθών και υπηρεσιών) (π.χ. Facebook Credits),

iii. εικονικά νομίσματα που συνδέονται διμερώς με την πραγματική οικονομία. Δηλαδή υπάρχουν ισοτιμίες μετατροπής τόσο για την αγορά εικονικού νομίσματος όσο και για την πώληση του εν λόγω νομίσματος. Το αγορασμένο νόμισμα μπορεί να χρησιμοποιηθεί για την αγορά τόσο των εικονικών όσο και των πραγματικών αγαθών και υπηρεσιών

Τα κρυπτονομίσματα, όπως το Bitcoin, είναι εικονικά νομίσματα του τελευταίου τύπου: μπορούν τόσο να αγοραστούν με παραδοσιακό χρήμα όσο και να πωληθούν έναντι παραδοσιακού χρήματος. Ακόμη, μπορούν να χρησιμοποιηθούν για την αγορά τόσο ψηφιακών όσο και πραγματικών αγαθών και υπηρεσιών.

Σε μια πιο πρόσφατη έκθεση του 2015 με τίτλο "Virtual Currency Schemes - a further analysis", η "ΕΚΤ" πρότεινε έναν "δεύτερο" και σε μεγάλο βαθμό επικαιροποιημένο ορισμό των εικονικών νομισμάτων. Όρισε τα εικονικά νομίσματα ως ψηφιακές αναπαραστάσεις αξίας, οι οποίες δεν εκδίδονται από κεντρική τράπεζα, πιστωτικό ίδρυμα ή ίδρυμα ηλεκτρονικού χρήματος και οι οποίες σε ορισμένες περιπτώσεις μπορούν να χρησιμοποιηθούν ως εναλλακτική λύση σε σχέση με το χρήμα. Διευκρίνισε επίσης ότι τα χαρτονομίσματα, όπως το Bitcoin, αποτελούν ένα αποκεντρωμένο αμφίδρομο (δηλαδή διμερές) εικονικό νόμισμα.

Β) Διεθνές Νομισματικό Ταμείο ("ΔΝΤ")

Το Διεθνές Νομισματικό Ταμείο ("ΔΝΤ") έχει κατηγοριοποιήσει τα κρυπτονομίσματα ως υποσύνολο των εικονικών νομισμάτων, τα οποία ορίζει ως ψηφιακές αναπαραστάσεις αξίας, που εκδίδονται από ιδιώτες προγραμματιστές και εκφράζονται στη δική τους λογιστική μονάδα. Σύμφωνα με το ΔΝΤ, η έννοια των εικονικών νομισμάτων καλύπτει ένα ευρύτερο φάσμα "νομισμάτων", που κυμαίνεται από απλά "IOU"("ένα άτυπο πιστοποιητικό χρέους" ή "σου χρωστάω") από εκδότες (όπως κουπόνια διαδικτύου ή κινητής τηλεφωνίας και αεροπορικά μίλια).

Γ) Τράπεζας Διεθνών Διακανονισμών ("BIS")

Η Επιτροπή Πληρωμών και Υποδομών Αγοράς ("CPMI"), όργανο της Τράπεζας Διεθνών Διακανονισμών ("BIS"), έχει χαρακτηρίσει τα κρυπτονομίσματα ως ψηφιακά νομίσματα ή συστήματα ψηφιακών νομισμάτων.
Τα συστήματα αυτά λέγεται ότι παρουσιάζουν τα ακόλουθα βασικά χαρακτηριστικά:

i. είναι περιουσιακά στοιχεία, η αξία των οποίων καθορίζεται από την προσφορά και τη ζήτηση, παρόμοια στην έννοια με εμπορεύματα όπως ο χρυσός, αλλά με μηδενική εσωτερική αξία,

ii. χρησιμοποιούν κατανεμημένα λογιστικά βιβλία για να επιτρέπουν την εξ αποστάσεως ανταλλαγή ηλεκτρονικών αξιών μεταξύ ομότιμων, χωρίς να υπάρχει εμπιστοσύνη μεταξύ των μερών και χωρίς την ανάγκη διαμεσολαβητών.

iii. δεν λειτουργούν από κάποιο συγκεκριμένο άτομο ή ίδρυμα.

Δ) Ευρωπαϊκή Αρχή Τραπεζών ("ΕΑΤ")

Η Ευρωπαϊκή Αρχή Τραπεζών ("ΕΑΤ") πρότεινε να αναφέρονται τα κρυπτονομίσματα ως εικονικά νομίσματα, τα οποία ορίζει ως ψηφιακές αναπαραστάσεις αξίας που δεν εκδίδονται από κεντρική τράπεζα ή δημόσια αρχή ούτε συνδέονται απαραίτητα με ένα νόμισμα, αλλά χρησιμοποιούνται από φυσικά ή νομικά πρόσωπα ως μέσο ανταλλαγής και μπορούν να μεταφέρονται, να αποθηκεύονται ή να διαπραγματεύονται ηλεκτρονικά.

Ε) Η Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών ("ΕΑΚΑΑ")

Η Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών ("ΕΑΚΑΑ") αναφέρθηκε πρόσφατα επίσης στα κρυπτονομίσματα ως εικονικά νομίσματα, σε μια πανευρωπαϊκή προειδοποίηση που εκδόθηκε σε συνεργασία με την Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων ("ΕΑΑΕΣ") και την "ΕΑΤ". Σε πλήρη συμφωνία με τον ορισμό της "ΕΑΤ", τα εικονικά νομίσματα ορίζονται ως ψηφιακές αναπαραστάσεις αξίας που δεν εκδίδονται ούτε είναι εγγυημένες από κεντρική τράπεζα ή δημόσια αρχή και δεν έχουν το νομικό καθεστώς του νομίσματος ή του χρήματος.

ΣΤ) Παγκόσμια Τράπεζα

Η Παγκόσμια Τράπεζα έχει ταξινομήσει τα κρυπτονομίσματα ως ένα υποσύνολο των ψηφιακών νομισμάτων, τα οποία ορίζει ως ψηφιακές αναπαραστάσεις αξίας που εκφράζονται στη δική τους λογιστική μονάδα. Σε αντίθεση με το ηλεκτρονικό χρήμα το οποίο είναι απλώς ένας ψηφιακός μηχανισμός πληρωμών, που αντιπροσωπεύει και εκφράζεται σε πλαστό χρήμα. Σε αντιπαράθεση με τους περισσότερους φορείς χάραξης πολιτικής, η Παγκόσμια Τράπεζα έχει επίσης ορίσει τα ίδια τα κρυπτονομίσματα ως ψηφιακά νομίσματα που βασίζονται σε κρυπτογραφικές τεχνικές για την επίτευξη συναίνεσης

Ζ) Ομάδα Χρηματοοικονομικής Δράσης ("FATF")

Όπως και πολλοί άλλοι φορείς χάραξης πολιτικής, η Ομάδα Χρηματοοικονομικής Δράσης ("FATF") έχει προσεγγίσει τα κρυπτονομίσματα ως υποσύνολο των εικονικών νομισμάτων, τα οποία ορίζει ως ψηφιακές αναπαραστάσεις αξίας που μπορούν να διαπραγματεύονται ψηφιακά και να λειτουργούν: ως (1) μέσο ανταλλαγής ή/και (2) μονάδα λογαριασμού ή/και (3) αποθήκη αξίας. Όμως δεν έχουν καθεστώς νόμιμου χρήματος (δηλαδή, όταν προσφέρονται σε πιστωτή να αποτελούν έγκυρη και νόμιμη προσφορά πληρωμής) σε οποιαδήποτε δικαιοδοσία. Επίσης, προτείνει ότι τα εικονικά νομίσματα μπορούν να χωριστούν σε δύο βασικούς τύπους:

i. μετατρέψιμα εικονικά νομίσματα που έχουν ισοδύναμη αξία σε πραγματικό νόμισμα και μπορούν να ανταλλάσσονται εμπρός-πίσω με πραγματικό νόμισμα. Αυτά τα εικονικά νομίσματα μπορεί να έχουν συγκεντρωτικό ή αποκεντρωτικό χαρακτήρα (δηλαδή μπορεί να έχουν είτε μια κεντρική διαχειριστική αρχή που ελέγχει το σύστημα είτε καθόλου κεντρική εποπτεία) και

ii. μη μετατρέψιμα εικονικά νομίσματα που είναι ειδικά για ένα συγκεκριμένο εικονικό τομέα ή κόσμο (π.χ. ένα Massively Multiplayer Online Role-Playing Game όπως το World of Warcraft), και σύμφωνα με τους κανόνες που διέπουν τη χρήση του, δεν μπορούν να ανταλλαγούν με fiat νόμισμα. Τα κρυπτονομίσματα όπως το Bitcoin είναι εικονικά νομίσματα του πρώτου

τύπου, τα οποία μπορούν, σύμφωνα με την "FATF", να οριστούν ως μαθηματικά βασισμένα, αποκεντρωμένα μετατρέψιμα εικονικά νομίσματα που προστατεύονται από την κρυπτογραφία.

Το κύριο συμπέρασμα που μπορεί να εξαχθεί από τις διαφορετικές οπτικές γωνίες που παρατίθενται ανωτέρω, είναι ότι δεν υπάρχει γενικά αποδεκτός ορισμός του όρου κρυπτονομίσματα στον ρυθμιστικό χώρο. Ακόμη, οι περισσότεροι φορείς χάραξης πολιτικής απέφυγαν να ορίσουν συνολικά τον όρο. Μεταξύ των προαναφερθέντων, μόνο η Παγκόσμια Τράπεζα και η Ομάδα Χρηματοοικονομικής Δράσης ("FATF") έχουν διατυπώσει έναν σαφή ορισμό. Ωστόσο, είναι σαφές ότι οι περισσότεροι φορείς χάραξης πολιτικής προσεγγίζουν τα κρυπτονομίσματα ως υποσύνολο ή μορφή εικονικών ή ψηφιακών νομισμάτων.

Αν προσπαθήσουμε να συνοψίσουμε όλους τους παραπάνω ορισμούς, μια καλή περίληψη θα μπορούσε να είναι ότι ένα κρυπτονόμισμα είναι "μια ψηφιακή αναπαράσταση αξίας που:

i. προορίζεται να αποτελέσει μια εναλλακτική λύση από ομότιμους προς ομότιμους ("P2P") σε σχέση με το νόμιμο χρήμα που εκδίδεται από την κυβέρνηση,
ii. χρησιμοποιείται ως μέσο ανταλλαγής γενικής χρήσης (ανεξάρτητο από οποιαδήποτε κεντρική τράπεζα),
iii. διασφαλίζεται από έναν μηχανισμό γνωστό ως κρυπτογραφία και
iv. μπορεί να μετατραπεί σε νόμιμο χρήμα και αντίστροφα[3].

Στη συνέχεια θα ρίξουμε φως στην λειτουργία-μηχανισμό πίσω από τα κρυπτονομίσματα και πιο συγκεκριμένα με έννοιες, οι οποίες σχετίζονται άμεσα με τα κρυπτονομίσματα.

[3]Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain

2.3 Κρυπτογράφηση

2.3.1 Ιστορικά στοιχεία

Η κρυπτογραφία τοποθετεί την «κρυπτογράφηση» στο κρυπτονόμισμα. Υπήρχε πολύ πριν από την ψηφιακή εποχή μας και εξελίχθηκε όπως οι γλώσσες στους αιώνες. Η κρυπτογραφία είναι η επιστήμη της εξασφάλισης πληροφοριών με τη μετατροπή τους σε μια μορφή που μόνο οι παραλήπτες μπορούν να επεξεργαστούν και να διαβάσουν. Η πρώτη γνωστή χρήση χρονολογείται από το έτος 1900 π.Χ. ως ιερογλυφικά σε αιγυπτιακό τάφο. Ο ίδιος ο όρος προέρχεται από τις ελληνικές λέξεις κρύπτω και γράφω.

Μία από τις πιο διάσημες χρήσεις αναπτύχθηκε από τον Ιούλιο Καίσαρα γύρω στο 40 π.Χ. και ονομάστηκε εύστοχα η κρυπτογράφηση του Καίσαρα. Ένας κρυπτογράφος χρησιμοποιεί μια μυστική πληροφορία που σας λέει πώς να ανακατεύετε και επομένως να ξεμπερδεύετε ένα μήνυμα. Ο Καίσαρας χρησιμοποίησε μια κρυπτογράφηση αντικατάστασης, όπου κάθε γράμμα του αλφαβήτου αντικαταστάθηκε από ένα γράμμα σε διαφορετική σταθερή θέση πιο πάνω ή κάτω στο αλφάβητο. Για παράδειγμα, το αλφάβητο θα μπορούσε να μετακινηθεί πέντε θέσεις προς τα δεξιά, πράγμα που σημαίνει ότι το γράμμα «A» θα ήταν τώρα «F», το «B» θα ήταν τώρα «G» και ούτω καθεξής. Αυτό σήμαινε ότι μπορούσε να περάσει μηνύματα χωρίς να φοβάται ότι θα υποκλαπούν, γιατί μόνο οι αξιωματικοί του ήξεραν πώς να αποκωδικοποιήσουν το μήνυμα.

Ο Giovan Battista Bellaso, ένας κρυπτολόγος του 16ου αιώνα, σχεδίασε την κρυπτογράφηση Vigenere (που αποδίδεται ψευδώς στον διπλωμάτη Blaise de Vigenere), που πιστεύεται ότι ήταν ο πρώτος κρυπτογράφος που χρησιμοποίησε ένα κλειδί κρυπτογράφησης. Το αλφάβητο γράφτηκε σε 26 σειρές, με κάθε σειρά να αλλάζει ένα γράμμα για να δημιουργήσει ένα πλέγμα. Το κλειδί κρυπτογράφησης γράφτηκε για να ταιριάζει με το μήκος του μηνύματος. Στη συνέχεια, το πλέγμα χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος, γράμμα προς γράμμα. Τέλος, ο αποστολέας μοιράστηκε το κρυπτογραφημένο μήνυμα και τη μυστική λέξη - κλειδί στον παραλήπτη, ο οποίος θα είχε το ίδιο πλέγμα.

Στη συνέχεια ήρθαν οι υπολογιστές, οι οποίοι επέτρεψαν πολύ πιο εξελιγμένη κρυπτογραφία. Αλλά ο στόχος παραμένει ο ίδιος: να μεταφέρουμε ένα αναγνώσιμο

μήνυμα (απλό κείμενο) σε κάτι που ένας ακούσιος αναγνώστης δεν μπορεί να καταλάβει (κρυπτογράφηση κειμένου). Η διαδικασία είναι γνωστή ως κρυπτογράφηση και είναι ο τρόπος με τον οποίο οι πληροφορίες μπορούν να μοιραστούν σε δημόσιες συνδέσεις στο Διαδίκτυο. Η γνώση σχετικά με τον τρόπο αποκρυπτογράφησης – ή αποσυμπίεσης – των δεδομένων είναι γνωστή ως το κλειδί και μόνο τα ενδιαφερόμενα μέρη θα πρέπει να έχουν πρόσβαση σε αυτές τις πληροφορίες[4].

2.3.2 Τι είναι Κρυπτογραφία

Η κρυπτογραφία σχετίζεται με τη διαδικασία μετατροπής απλού κειμένου σε μη κατανοητό κείμενο και αντίστροφα. Είναι μια μέθοδος αποθήκευσης και μετάδοσης δεδομένων σε μια συγκεκριμένη μορφή[5]. Η κρυπτογραφία, με απλούστερους όρους, είναι να κάνεις τις επικοινωνίες μυστικές. Το "μυστικό" εδώ είναι ότι, ακόμη και με την παρουσία ενός υποκλοπέα που μπορεί να παρακολουθεί όλες τις επικοινωνίες, το προβλεπόμενο μήνυμα μπορεί να παραδοθεί στον παραλήπτη, ενώ παραμένει μυστικό για τους άλλους. Η διαδικασία που μετατρέπει το απλό κείμενο σε κρυπτογραφημένο κείμενο είναι γνωστό ως κρυπτογράφηση, ενώ η διαδικασία μετατροπής του κρυπτογραφημένου κειμένου σε απλό κείμενο ονομάζεται αποκρυπτογράφηση[6]. Ανάλογα με τη διαμόρφωση, η τεχνολογία κρυπτογραφίας μπορεί να εξασφαλίσει ψευδό- ή πλήρη ανωνυμία. Στο κρυπτονόμισμα, η κρυπτογραφία εγγυάται την ασφάλεια των συναλλαγών και των συμμετεχόντων, την ανεξαρτησία των λειτουργιών από μια κεντρική αρχή και επίσης μπορεί να χρησιμοποιηθεί για την πιστοποίηση της ταυτότητας του χρήστη.

2.3.3 Πως λειτουργεί η κρυπτογράφηση

Σκεφτείτε ότι λαμβάνετε ραδιοφωνικά σήματα στο ραδιόφωνο του αυτοκινήτου σας που σας επιτρέπει να ακούτε την εκπομπή. Αυτή η εκπομπή είναι δημόσια γνωστή και ανοιχτή σε όλους. Αντίθετα, σκεφτείτε τις επικοινωνίες αμυντικού επιπέδου, όπως αυτές μεταξύ στρατιωτών σε μια πολεμική αποστολή. Αυτή η επικοινωνία θα είναι

[4]https://www.basecoin.gr/kryptografia-orismos-leitoyrgia-kai-charaktiristika/
[5] https://economictimes.indiatimes.com/definition/cryptography
[6]https://crypto.com/university/what-is-cryptography

ασφαλής και κρυπτογραφημένη. Θα λαμβάνεται και θα είναι γνωστή μόνο στους προβλεπόμενους συμμετέχοντες αντί να είναι ανοιχτή σε όλο τον κόσμο. Η κρυπτογραφία των κρυπτονομισμάτων λειτουργεί με παρόμοιο τρόπο.

Με τους απλούστερους όρους, η κρυπτογραφία είναι μια τεχνική για την αποστολή ασφαλών μηνυμάτων μεταξύ δύο ή περισσότερων συμμετεχόντων. Ο αποστολέας κρυπτογραφεί/αποκρύπτει ένα μήνυμα χρησιμοποιώντας ένα είδος κλειδιού και στέλνει αυτή την κρυπτογραφημένη μορφή του μηνύματος στον παραλήπτη και ο παραλήπτης το αποκρυπτογραφεί για να δημιουργήσει το αρχικό μήνυμα. Τα κλειδιά κρυπτογράφησης είναι η πιο σημαντική πτυχή της κρυπτογραφίας. Κάνουν ένα μήνυμα, μια συναλλαγή ή μια τιμή δεδομένων μη αναγνώσιμη για έναν μη εξουσιοδοτημένο αναγνώστη ή παραλήπτη και μπορεί να διαβαστεί και να υποστεί επεξεργασία μόνο από τον προοριζόμενο παραλήπτη. Τα κλειδιά καθιστούν τις πληροφορίες "κρυπτογραφημένες" ή μυστικές.

Πολλά κρυπτονομίσματα, όπως το Bitcoin, μπορεί να μην χρησιμοποιούν ρητά τέτοια μυστικά, κρυπτογραφημένα μηνύματα, καθώς οι περισσότερες πληροφορίες που αφορούν συναλλαγές Bitcoin είναι σε μεγάλο βαθμό δημόσιες. Ωστόσο, υπάρχουν επίσης κρυπτονομίσματα με προσανατολισμό στην ιδιωτικότητα, όπως το ZCash και το Monero, που μπορούν να χρησιμοποιήσουν κρυπτογράφηση για να αποκρύψουν την αξία και τον παραλήπτη μιας συναλλαγής. Ορισμένα από τα εργαλεία που αναπτύχθηκαν ως μέρος της κρυπτογραφίας έχουν βρει σημαντική χρήση στα κρυπτονομίσματα. Περιλαμβάνουν λειτουργίες κατακερματισμού και ψηφιακών υπογραφών που αποτελούν αναπόσπαστο μέρος της επεξεργασίας του Bitcoin, ακόμη και αν το Bitcoin δεν χρησιμοποιεί άμεσα κρυφό μήνυμα[7].

2.3.4 Μέθοδοι κρυπτογραφίας που χρησιμοποιούνται στα κρυπτονομίσματα

Υπάρχουν πολλοί τρόποι κρυπτογράφησης και τα επίπεδα πολυπλοκότητας εξαρτώνται από τον βαθμό προστασίας που μπορεί να απαιτούν τα δεδομένα. Αλλά συνήθως βλέπουμε τρεις τύπους κρυπτογραφικών αλγορίθμων: η συμμετρική

[7]https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/#toc-how-does- cryptography-work

κρυπτογράφηση (ή κρυπτογράφηση ενός κλειδιού), η ασύμμετρη κρυπτογράφηση (κρυπτογράφηση δημόσιου κλειδιού) και οι λειτουργίες κατακερματισμού[8].

Συμμετρική κρυπτογράφηση

Η κρυπτογραφία συμμετρικού κλειδιού (ή συμμετρική κρυπτογράφηση) είναι ένας τύπος συστήματος κρυπτογράφησης στον οποίο το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση μηνυμάτων. Είναι σημαντικό ότι, χωρίς αυτό το κλειδί, το μήνυμα δεν μπορεί να αποκρυπτογραφηθεί και ταυτόχρονα, ο αλγόριθμος που χρησιμοποιείται (ως επί το πλείστον δημόσιος) να είναι τέτοιος ώστε να μπορούν να λάβουν το αντίστοιχο αρχικό κείμενο χρησιμοποιώντας αυτό το κλειδί[9].

Η διαδικασία της κρυπτογράφησης συνίσταται στην εκτέλεση ενός απλού κειμένου (είσοδος) μέσω ενός αλγορίθμου κρυπτογράφησης, ο οποίος με τη σειρά του παράγει ένα κρυπτογραφημένο κείμενο (έξοδος). Εάν το σύστημα κρυπτογράφησης είναι αρκετά ισχυρό, ο μόνος τρόπος για να διαβάσει ή να αποκτήσει πρόσβαση κάποιος στις πληροφορίες που περιέχονται στο κρυπτοκείμενο είναι να χρησιμοποιήσει το αντίστοιχο κλειδί για να το αποκρυπτογραφήσει. Η διαδικασία αποκρυπτογράφησης είναι ουσιαστικά η μετατροπή του κρυπτοκειμένου πίσω σε απλό κείμενο.

Η ασφάλεια των συμμετρικών συστημάτων κρυπτογράφησης βασίζεται στο πόσο δύσκολο είναι να μαντέψει κανείς τυχαία το αντίστοιχο κλειδί για να το καταστρέψει. Ένα κλειδί 128 bit, για παράδειγμα, θα χρειαζόταν δισεκατομμύρια χρόνια για να το μαντέψει κανείς χρησιμοποιώντας το κοινό υλικό υπολογιστών. Όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο πιο δύσκολη γίνεται η παραβίασή του. Τα κλειδιά που έχουν μήκος 256 bit θεωρούνται γενικά ιδιαίτερα ασφαλή και θεωρητικά ανθεκτικά στις επιθέσεις ωμής βίας κβαντικών υπολογιστών.

Δύο από τα πιο συνηθισμένα σχήματα συμμετρικής κρυπτογράφησης που χρησιμοποιούνται σήμερα βασίζονται σε κρυπτογράφηση "μπλοκ" και σε κρυπτογράφηση ροής. Οι "blockciphers" (κωδικοποιητές μπλοκ) ομαδοποιούν τα

[8]https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/cryptography/
[9]https://www.pwc.com/cz/en/assets/pdf/StaySecure/8_2019_StaySecure_Symmetric_Cryptography_EN_external_final.pdf

δεδομένα σε "μπλοκ" προκαθορισμένου μεγέθους και κάθε μπλοκ κρυπτογραφείται χρησιμοποιώντας το αντίστοιχο κλειδί και αλγόριθμο κρυπτογράφησης (π.χ., το απλό κείμενο των 128 bit κρυπτογραφείται σε κρυπτογράφημα των 128 bit). Από την άλλη πλευρά, οι κρυπτογράφοι ροής δεν κρυπτογραφούν τα δεδομένα απλού κειμένου ανά μπλοκ, αλλά με βήματα του 1 bit (1 bit απλό κείμενο κρυπτογραφείται σε 1 bit κρυπτοκείμενο κάθε φορά)[10].

Συγκεκριμένα ένας κρυπτογράφος μπλοκ είναι ένας αλγόριθμος κρυπτογράφησης που κρυπτογραφεί ένα σταθερό μέγεθος n-bit δεδομένων γνωστό ως μπλοκ σε μια στιγμή. Τα συνήθη μεγέθη κάθε μπλοκ είναι 64 bits, 128 bits και 256 bits. Έτσι, για παράδειγμα, ένας κρυπτογράφος μπλοκ 64 bit θα λάβει 64 bits απλού κειμένου και θα το κρυπτογραφήσει σε 64 bits κρυπτοκειμένου. Σε περιπτώσεις όπου τα bits του απλού κειμένου είναι μικρότερα από το μέγεθος του μπλοκ, χρησιμοποιούνται σχήματα συμπλήρωσης. Η πλειονότητα των συμμετρικών κρυπτογραφήσεων που χρησιμοποιούνται σήμερα είναι στην πραγματικότητα κρυπτογραφήσεις μπλοκ. Οι αλγόριθμοι κρυπτογράφησης DES, Triple DES, AES, IDEA και Blowfish είναι μερικοί από τους ευρέως χρησιμοποιούμενους αλγόριθμους κρυπτογράφησης που εμπίπτουν σε αυτή την ομάδα.

Αντίθετα ένας κρυπτογράφος ροής "streamcipher" είναι ένας αλγόριθμος κρυπτογράφησης που κρυπτογραφεί 1 bit ή byte απλού κειμένου κάθε φορά. Χρησιμοποιεί μια άπειρη ροή ψευδοτυχαίων bits ως κλειδί. Για να παραμείνει ασφαλής η υλοποίηση ενός κρυπτογραφήματος ροής, η γεννήτρια θα πρέπει να είναι απρόβλεπτη και το κλειδί δεν θα πρέπει ποτέ να επαναχρησιμοποιείται. Οι κρυπτογραφήσεις ροής έχουν σχεδιαστεί για να προσεγγίζουν μια εξιδανικευμένη κρυπτογράφηση, γνωστή ως "One-Time Pad" ένα μπλοκ μιας χρήσης.

Το "One-Time Pad", το οποίο υποτίθεται ότι χρησιμοποιεί ένα καθαρά τυχαίο κλειδί, μπορεί δυνητικά να επιτύχει "τέλεια μυστικότητα". Δηλαδή, υποτίθεται ότι είναι πλήρως απρόσβλητο σε επιθέσεις ωμής βίας. Το πρόβλημα με το "one-time pad" είναι ότι, προκειμένου να δημιουργηθεί μια τέτοια κρυπτογράφηση, το κλειδί της θα πρέπει να είναι το ίδιο μεγάλο ή και μεγαλύτερο από το απλό κείμενο. Με άλλα λόγια, αν έχετε

[10]https://academy.binance.com/en/articles/what-is-symmetric-key-cryptography

ένα αρχείο βίντεο 500 MegaByte που θέλετε να κρυπτογραφήσετε, θα χρειαστείτε ένα κλειδί μήκους τουλάχιστον 4 Gigabits.

Το RC4, το οποίο σημαίνει "Rivest Cipher 4", είναι ο πιο ευρέως χρησιμοποιούμενος από όλους τους κρυπτογράφους ροής, ιδίως στο λογισμικό. Είναι επίσης γνωστός ως "ARCFOUR" ή "ARC4" και έχουν χρησιμοποιηθεί σε διάφορα πρωτόκολλα όπως το WEP και το WPA (και τα δύο πρωτόκολλα ασφαλείας για ασύρματα δίκτυα) καθώς και στο TLS[11].

Ασύμμετρη κρυπτογράφηση

Η δεύτερη μέθοδος είναι η κρυπτογραφία ασύμμετρης κρυπτογράφησης, η οποία χρησιμοποιεί δύο διαφορετικά κλειδιά το δημόσιο και το ιδιωτικό για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Το δημόσιο κλειδί δημοσιοποιείται χωρίς να μειώνεται η ασφάλεια της διαδικασίας, αλλά το ιδιωτικό κλειδί πρέπει να παραμείνει μυστικό για να διατηρήσουν τα δεδομένα την κρυπτογραφική τους προστασία. Παρόλο που υπάρχει σχέση μεταξύ των δύο κλειδιών, το ιδιωτικό κλειδί δεν μπορεί να προσδιοριστεί αποτελεσματικά με βάση τη γνώση του δημόσιου κλειδιού. Κάποιος μπορεί να κρυπτογραφήσει με ένα ιδιωτικό κλειδί και στη συνέχεια να αποκρυπτογραφήσει με το δημόσιο κλειδί. Εναλλακτικά, μπορεί κανείς να κρυπτογραφήσει με δημόσιο κλειδί και στη συνέχεια να αποκρυπτογραφήσει με ιδιωτικό κλειδί.

Η κρυπτογραφία ασύμμετρου κλειδιού επιτρέπει μια σχέση εμπιστοσύνης μεταξύ χρηστών που δεν γνωρίζουν ή δεν εμπιστεύονται ο ένας τον άλλον, παρέχοντας έναν μηχανισμό για την επαλήθευση της ακεραιότητας και της αυθεντικότητας των συναλλαγών, ενώ ταυτόχρονα επιτρέπει στις συναλλαγές να παραμένουν δημόσιες. Για να γίνει αυτό, οι συναλλαγές "υπογράφονται ψηφιακά". Αυτό σημαίνει ότι ένα ιδιωτικό κλειδί χρησιμοποιείται για την κρυπτογράφηση μιας συναλλαγής έτσι ώστε οποιοσδήποτε με το δημόσιο κλειδί να μπορεί να την αποκρυπτογραφήσει. Δεδομένου ότι το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο, η κρυπτογράφηση της συναλλαγής με το ιδιωτικό κλειδί αποδεικνύει ότι ο υπογράφων τη συναλλαγή, έχει πρόσβαση στο ιδιωτικό κλειδί. Εναλλακτικά, μπορεί κανείς να κρυπτογραφήσει δεδομένα με το

[11] https://www.jscape.com/blog/stream-cipher-vs-block-cipher

δημόσιο κλειδί ενός χρήστη, έτσι ώστε μόνο οι χρήστες με πρόσβαση στο ιδιωτικό κλειδί να μπορούν να το αποκρυπτογραφήσουν.

Ένα μειονέκτημα είναι ότι η κρυπτογραφία ασύμμετρου κλειδιού είναι συχνά αργή στον υπολογισμό. Εξαιτίας αυτού, όταν κάποιος ισχυρίζεται ότι κρυπτογραφεί κάτι χρησιμοποιώντας κρυπτογραφία ασύμμετρου κλειδιού, συχνά τα δεδομένα κρυπτογραφούνται με κρυπτογραφία συμμετρικού κλειδιού και στη συνέχεια το συμμετρικό κλειδί κρυπτογραφείται με κρυπτογραφία ασύμμετρου κλειδιού. Αυτό το "τέχνασμα" μπορεί να επιταχύνει σημαντικά την κρυπτογραφία ασύμμετρου κλειδιού[12].

Για παράδειγμα, ο Α θέλει να στείλει μήνυμα στον Β. Ακολουθούν τα εξής βήματα:

α) Ο Α και ο Β πρέπει να γνωρίζουν το δημόσιο κλειδί του άλλου, αλλά τα ιδιωτικά κλειδιά παραμένουν μυστικά.

β) Ο Α κρυπτογραφεί ένα μήνυμα απλού κειμένου για τον Β χρησιμοποιώντας το δημόσιο κλειδί του Β.

γ) Ο Α διαβιβάζει το κρυπτογραφημένο μήνυμα στον Β.

δ) Ο Β λαμβάνει το κρυπτογραφημένο κείμενο και το αποκρυπτογραφεί χρησιμοποιώντας το δικό του ιδιωτικό κλειδί.

ε) Ο Β λαμβάνει το μήνυμα απλού κειμένου.

Η χρήση δύο κλειδιών αντί για ένα παράγει επίσης μια σειρά λειτουργικών διαφορών μεταξύ συμμετρικής και ασύμμετρης κρυπτογράφησης. Τα αποτελέσματα των επιδόσεων δείχνουν ότι τα συμμετρικά συστήματα είναι υπολογιστικά ανέξοδα σε σύγκριση με τα ασύμμετρα συστήματα.. Επειδή τα δημόσια και τα ιδιωτικά κλειδιά που χρησιμοποιούνται στην ασύμμετρη κρυπτογράφηση σχετίζονται σε κάποιο βαθμό με μαθηματικά που είναι πιο πολύπλοκα. Επίσης τα ίδια τα κλειδιά πρέπει να είναι σημαντικά μεγαλύτερα για να παρέχουν παρόμοιο επίπεδο ασφάλειας που προσφέρουν τα μικρότερα συμμετρικά κλειδιά[13].

[12]Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Nistir 8202 blockchain technology overview.
[13] Maqsood, F., Ahmed, M., Ali, M. M., & Shah, M. A. (2017). Cryptography: a comparative analysis for modern techniques.

Hashing

Η τρίτη μέθοδος κρυπτογράφησης είναι η μέθοδος συνάρτηση κατακερματισμού "Hashing". Οι κρυπτογραφικές συναρτήσεις κατακερματισμού είναι αλγόριθμοι που δεν χρησιμοποιούν κλειδιά. Αντ' αυτού, τα δεδομένα καταγράφονται σε μια σταθερού μεγέθους (συνήθως μικρότερη) τιμή. Πρόκειται ουσιαστικά για κρυπτογράφηση μονής κατεύθυνσης που δημιουργεί ένα "δακτυλικό αποτύπωμα" των πληροφοριών που έχουν καταγραφεί και γίνεται έτσι ώστε τα περιεχόμενα του νέου, μικρότερου αρχείου να μην μπορούν να αλλοιωθούν[14]. Ο κατακερματισμός είναι μια μαθηματική συνάρτηση που μετατρέπει μια είσοδο αυθαίρετου μήκους σε μια κρυπτογραφημένη έξοδο σταθερού μήκους.

Χρησιμοποιείται για την αποτελεσματική επαλήθευση της ακεραιότητας των δεδομένων των συναλλαγών στο δίκτυο. Διατηρεί τη δομή των δεδομένων της αλυσίδας μπλοκ, κωδικοποιεί τις διευθύνσεις των λογαριασμών των ανθρώπων, αποτελεί αναπόσπαστο μέρος της διαδικασίας κρυπτογράφησης των συναλλαγών που πραγματοποιούνται μεταξύ λογαριασμών και καθιστά δυνατή την εξόρυξη μπλοκ. Επιπλέον, οι ψηφιακές υπογραφές συμπληρώνουν αυτές τις διάφορες διαδικασίες κρυπτογράφησης, επιτρέποντας στους γνήσιους συμμετέχοντες να αποδεικνύουν την ταυτότητά τους στο δίκτυο. Πολλαπλές παραλλαγές των παραπάνω μεθόδων με επιθυμητά επίπεδα προσαρμογής μπορούν να εφαρμοστούν σε διάφορα δίκτυα κρυπτονομισμάτων[15].

2.4 Blockchain

2.4.1 Τι είναι η "αλυσίδα μπλοκ"

Μια αλυσίδα μπλοκ, στην ουσία, είναι μια κατανεμημένη βάση δεδομένων. Καταγράφει κομμάτια πληροφοριών που είναι ομαδοποιημένα σε μπλοκ και τα οποία συνδέονται μέσω μιας κρυπτογραφικής διαδικασίας σε μια συνεχώς επεκτεινόμενη αλυσίδα. Δηλαδή χρησιμοποιεί (ένα σύνολο) συγκεκριμένων μαθηματικών αλγορίθμων για τη δημιουργία και την επαλήθευση μιας συνεχώς αυξανόμενης δομής

[14]https://www.ssl.com/el
[15]https://www.investopedia.com/terms/h/hash.asp

δεδομένων, στην οποία μπορούν να προστεθούν μόνο δεδομένα και από την οποία δεν μπορούν να αφαιρεθούν τα υπάρχοντα δεδομένα. Έχει τη μορφή μιας αλυσίδας "μπλοκ συναλλαγών" και λειτουργεί ως κατανεμημένο βιβλίο, -εξ ου και το όνομα. Η πρώτη εφαρμογή μιας αλυσίδας μπλοκ ήταν το Bitcoin, που ξεκίνησε τον Ιανουάριο του 2009. Στα κρυπτονομίσματα όπως το bitcoin ή το ethereum, τα απλούστερα κομμάτια πληροφοριών που αποθηκεύονται στις αντίστοιχες αλυσίδες μπλοκ είναι οι συναλλαγές κρυπτονομισμάτων μεταξύ δύο μερών. Ως εκ τούτου, ένα άτομο μπορεί να στείλει χρήματα σε ένα άλλο, όπως ακριβώς στέλνει ένα email, εξ ολοκλήρου εικονικά και ανεξάρτητα από τράπεζες ή σύνορα.

Όλο αυτό το σύστημα, φυσικά, εξαρτάται σε κρίσιμο βαθμό από την ορθότητα των πληροφοριών που είναι αποθηκευμένες στην αλυσίδα. Η καινοτόμος δύναμη της αλυσίδας μπλοκ έγκειται στο γεγονός ότι συνδυάζει την αποκέντρωση με τη μαθηματική επαλήθευση. Αυτό σημαίνει ότι δεν υπάρχει καμία ενιαία αρχή που να εγγυάται την αυθεντικότητα του βιβλίου που περιέχει τις πληροφορίες. Αντίθετα, ολόκληρη η αλυσίδα αποθηκεύεται σε πολλούς κόμβους, δηλαδή σε υπολογιστές χρηστών. Τα μπλοκ πληροφοριών προστίθενται συνεχώς στην αλυσίδα καθώς επεξεργάζονται νέες συναλλαγές[16]. Οποιαδήποτε αλλαγή γίνει στο ιστορικό θα σπάσει την αλυσίδα σε ένα συγκεκριμένο αντίγραφο της βάσης δεδομένων. Όταν μια αλυσίδα σπάσει, το δίκτυο την επιδιορθώνει αντικαθιστώντας κάθε κατεστραμμένο μπλοκ με ένα έγκυρο μπλοκ[17].

2.4.2 Η τεχνολογία πίσω από το Blockchain

Μια αλυσίδα μπλοκ αποτελείται από σύνολα δεδομένων τα οποία αποτελούνται από μια αλυσίδα πακέτων δεδομένων (μπλοκ) όπου ένα μπλοκ περιλαμβάνει πολλαπλές συναλλαγές. Η αλυσίδα μπλοκ επεκτείνεται με κάθε πρόσθετο μπλοκ και ως εκ τούτου αντιπροσωπεύει ένα πλήρες βιβλίο το ιστορικό των συναλλαγών. Τα μπλοκ μπορούν να επικυρωθούν από το δίκτυο με τη χρήση κρυπτογραφικών μέσων. Εκτός από τις συναλλαγές, κάθε μπλοκ περιέχει έναν τυχαίο αριθμό που χρησιμοποιείται για την

[16] Hacker, P., &Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. European Company and Financial Law Review,
[17]Härdle, W. K., Harvey, C. R., &Reule, R. C. (2020). Understanding cryptocurrencies. Journal of Financial Econometrics

επαλήθευση του κατακερματισμού. Αυτή η έννοια διασφαλίζει την ακεραιότητα ολόκληρης της αλυσίδας μπλοκ μέχρι το πρώτο μπλοκ ("genesis block"). Οι τιμές κατακερματισμού είναι μοναδικές και η απάτη μπορεί να αποτραπεί αποτελεσματικά αφού οι αλλαγές ενός μπλοκ στην αλυσίδα θα άλλαζαν αμέσως την αντίστοιχη τιμή κατακερματισμού. Εάν η πλειοψηφία των κόμβων του δικτύου συμφωνεί μέσω ενός μηχανισμού συναίνεσης για την εγκυρότητα των συναλλαγών σε ένα μπλοκ και για την εγκυρότητα του, το ίδιο το μπλοκ μπορεί να προστεθεί στην αλυσίδα[18]. Μια αλυσίδα μπλοκ μπορεί να ενταχθεί σε δύο κατηγορίες: μπορεί να είναι δημόσια (αλυσίδα μπλοκ χωρίς άδεια) ή ιδιωτική (αλυσίδα μπλοκ με άδεια), ανάλογα με το πεδίο χρήσης του, την τιμή κατακερματισμού του προηγούμενου μπλοκ ("γονέας") και ένα "nonce".

Δημόσιο Blockchain

Μια δημόσια αλυσίδα μπλοκ παρέχει μια ανοικτή πλατφόρμα για ανθρώπους από διάφορους οργανισμούς και υπόβαθρα για να συμμετάσχουν, να κάνουν συναλλαγές και να εξορύξουν. Δεν υπάρχουν περιορισμοί σε κανέναν από αυτούς τους παράγοντες. Σε κάθε συμμετέχοντα δίνεται πλήρης εξουσία να διαβάζει/γράφει συναλλαγές, να πραγματοποιεί ελέγχους στην αλυσίδα μπλοκ ή να εξετάζει οποιοδήποτε μέρος της αλυσίδας μπλοκ, ανά πάσα στιγμή. Η αλυσίδα μπλοκ είναι ανοικτή και διαφανής και δεν υπάρχουν συγκεκριμένοι "κόμβοι επικύρωσης". Όλοι οι χρήστες μπορούν να συλλέγουν συναλλαγές και να ξεκινούν με τη διαδικασία εξόρυξης για να κερδίζουν ανταμοιβές εξόρυξης. Η διαθεσιμότητα του αντιγράφου ολόκληρης της αλυσίδας μπλοκ συγχρονισμένης με όλους τους κόμβους την καθιστά αμετάβλητη. Με την πλήρη αποκέντρωση, την απεραντοσύνη των υφιστάμενων δικτύων και μια ανοιχτή πλατφόρμα για να συμμετάσχει ο καθένας, η συναίνεση επιτυγχάνεται με οποιονδήποτε από τους αποκεντρωμένους μηχανισμούς συναίνεσης, όπως το proof-of-work, proof-of-stake κ.λπ. Φυσικά, η δημόσια διαθεσιμότητα του λογιστικού βιβλίου σε ένα ιδιωτικό σύστημα blockchain το εκθέτει σε επιθέσεις. Ο ισχυρός μηχανισμός της απόδειξης εργασίας σε συνδυασμό με την κρυπτογραφική επικύρωση ολόκληρης της αλυσίδας μπλοκ κάθε φορά που προστίθεται ένα νέο μπλοκ αντισταθμίζει αυτή την έλλειψη.

[18]Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain.

Ιδιωτικό Blockchain

Πρόκειται για ένα είδος συστήματος blockchain το οποίο έχει ρυθμιστεί για να διευκολύνει τον ιδιωτικό διαμοιρασμό και την ανταλλαγή δεδομένων μεταξύ μιας ομάδας ατόμων (σε έναν οργανισμό) ή μεταξύ πολλαπλών οργανισμών με εξόρυξη που ελέγχεται από έναν οργανισμό ή επιλεκτικά άτομα. Επίσης, Ονομάζεται Blockchain με άδεια, καθώς άγνωστοι χρήστες δεν μπορούν να έχουν πρόσβαση σε αυτό, εκτός αν λάβουν ειδική πρόσκληση. Η συμμετοχή των κόμβων αποφασίζεται είτε από ένα σύνολο κανόνων είτε από τον υπεύθυνο του δικτύου, για τον έλεγχο της πρόσβασης. Αυτό τείνει το δίκτυο περισσότερο προς τον συγκεντρωτισμό, ενώ παρεκκλίνει από τα στοιχειώδη χαρακτηριστικά του Blockchain της πλήρους αποκέντρωσης και της ανοιχτότητας. Σε ένα ιδιωτικό σύστημα Blockchain, από τη στιγμή που οι κόμβοι γίνονται μέρος του δικτύου, συμβάλλουν στη λειτουργία ενός αποκεντρωμένου δικτύου, με κάθε κόμβο να διατηρεί ένα αντίγραφο του λογιστικού βιβλίου και να συνεργάζεται για την επίτευξη συναίνεσης, σε αντίθεση με το δημόσιο Blockchain που οι εγγραφές του είναι περιορισμένες.

2.4.3 Proof Of Work (POW)

Το Proof-of-work (μηχανισμός απόδειξης εργασίας) ήταν το πρώτο αποκεντρωμένο πρωτόκολλο συναίνεσης που πρότεινε ο Satoshi, για να επιτύχει συνέπεια και ασφάλεια στο δίκτυο bitcoin. Η μεταφορά συναλλάγματος γίνεται με εντελώς αποκεντρωμένο τρόπο, απαιτώντας έτσι συναίνεση για την πιστοποίηση και την επικύρωση μπλοκ. Οι κόμβοι του δικτύου ανταγωνίζονται για τον υπολογισμό της τιμής κατακερματισμού του επόμενου μπλοκ, η οποία υποτίθεται ότι πρέπει να είναι μικρότερη από μια δυναμικά μεταβαλλόμενη τιμή-στόχο, που καθορίζεται από τον κανόνα συναίνεσης. Οι κόμβοι που επιτυγχάνουν τη λύση, περιμένουν την αμοιβαία επιβεβαίωση από άλλους κόμβους, πριν προσθέσουν το μπλοκ στην υπάρχουσα αλυσίδα. Μπορεί να δημιουργηθούν περισσότερα από ένα έγκυρο μπλοκ. Εάν όμως βρεθούν πολλοί κόμβοι μαζί και οι οποίοι έχουν βρει την κατάλληλη λύση προκαλούν προσωρινή διακλάδωση (branch) στο δίκτυο. Σε τέτοια σενάρια, όλα είναι αποδεκτά και εγκρίνονται οι κόμβοι που βρίσκονται πιο κοντά στους ανθρακωρύχους. Η σύγκρουση σε μεταγενέστερο

στάδιο αποφεύγεται με την αποδοχή της "μακρύτερης έκδοσης" της αλυσίδας που είναι διαθέσιμη ανά πάσα στιγμή[19].

2.4.4 Proof-of-Stake (POS)

Τα πρωτόκολλα Proof-of-Stake (μηχανισμός απόδειξης συμμετοχής) αναπτύχθηκαν ως εναλλακτικές λύσεις εξοικονόμησης ενέργειας σε σχέση με το "PoW". Αντί για πόρους υπολογιστικής ισχύος, οι ηγέτες επιλέγονται με βάση τα στοιχήματά τους, δηλαδή τις συνεισφορές τους στο δίκτυο blockchain. Ειδικότερα στον μηχανισμό συναίνεσης "PoS", το μερίδιο ενός κόμβου είναι ο αριθμός των ψηφιακών tokens, π.χ. κουπόνια στα κρυπτονομίσματα, που κατέχει ή καταθέτει. Αντί να καταναλώνεται πολλή ενέργεια για τη διαδικασία αναζήτησης, όπως στο"PoW", ένας ηγέτης θα επιλέγεται με βάση τα μερίδια του για να εκτελέσει τη διαδικασία εξόρυξης και να προσθέσει ένα νέο μπλοκ στην αλυσίδα.

Η διαδικασία επιλογής ηγέτη γίνεται με βάση τον αλγόριθμο, το (FTS) που έχει υιοθετηθεί σε πολλά "PoS" δίκτυα του Blockchain, όπως το Cardano, και το Tezos. Σε αυτά τα δίκτυα, όλα τα κουπόνια είναι ευρετηριασμένα. Ο αλγόριθμος (FTS) είναι μια συνάρτηση κατακερματισμού που λαμβάνει έναν σπόρο (δηλαδή μια συμβολοσειρά αυθαίρετου μήκους, όπως η επικεφαλίδα του προηγούμενου μπλοκ ή μια τυχαία συμβολοσειρά που δημιουργείται από κάποιους άλλους επιλεγμένους κόμβους) ως είσοδο. Χρησιμοποιώντας το ευρετήριο, ο αλγόριθμος αναζητά το ιστορικό των συναλλαγών για να βρει και να επιλέξει τον τρέχοντα κάτοχο του συγκεκριμένου κουπονιού του για να είναι ο ηγέτης του. Αυτό σημαίνει ότι όσα περισσότερα μερίδια κατέχει ένας κόμβος, τόσο μεγαλύτερη πιθανότητα έχει να επιλεγεί ως ηγέτης.

Εκτός από το πλεονέκτημα της χαμηλής κατανάλωσης ενέργειας, ο μηχανισμός "PoS" έχουν γρηγορότερη ταχύτητα επιβεβαίωσης συναλλαγών από εκείνη του μηχανισμού "PoW". Όμως η δυσκολία ενός "POS" συστήματος είναι η ασφάλεια του υποκείμενου αλγορίθμου, ο οποίος πρέπει να είναι όσο το δυνατόν ασφαλέστερος από εγκληματίες. Στο πλαίσιο του "PoW" συστήματος, θα χρειαζόταν ένα τεράστιο ποσό χρημάτων για να επιτεθεί σε ολόκληρο το δίκτυο των

[19]Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain

ανθρακωρύχων που προσπαθούν να επικυρώσουν τις συναλλαγές έναντι μιας οντότητας στο σύστημα "POS"[20].

2.4.5 Πλεονεκτήματα Τεχνολογίας Blockchain

Η τεχνολογία Blockchain είναι ένας νέος τύπος βάσης δεδομένων που μας υπόσχεται ένα λαμπρό μέλλον. Αυτή η τεχνολογία είναι πολύ ενδιαφέρουσα για τους ανθρώπους, επειδή μπορεί να λύσει ένα από τα μεγάλα προβλήματα, τα οποία συνδέονται με τη χρηματοδότηση. Ακόμη, μπορεί να βοηθήσει ώστε να γίνουν οι επιχειρήσεις, η κυβέρνηση και τα συστήματα logistics πιο αξιόπιστα και ασφαλή. Επιπροσθέτως, η τεχνολογία αυτή έχει πολύ ισχυρά οφέλη, επειδή μπορεί να βοηθήσει στην επίτευξη των παραπάνω στόχων σε διάφορα συστήματα. Τα κύρια πλεονεκτήματα της τεχνολογίας Blockchain είναι το αποκεντρωμένο δίκτυο, η ανωνυμία, η συνέπεια, η ελεγξιμότητα, η διαφάνεια, η αξιοπιστία, και η ταχύτερη επεξεργασία.

- Αποκέντρωση

  Στα συμβατικά συγκεντρωτικά συστήματα συναλλαγών, κάθε συναλλαγή πρέπει να επικυρώνεται μέσω του κεντρικού έμπιστου φορέα (π.χ. της κεντρικής τράπεζας), με αποτέλεσμα να αυξάνεται το κόστος και τα σημεία συμφόρησης των επιδόσεων στους κεντρικούς διακομιστές. Διαφορετικά, μια συναλλαγή στο δίκτυο Blockchain μπορεί να πραγματοποιηθεί μεταξύ δύο οποιονδήποτε ομότιμων (P2P) χωρίς την επικύρωση από τον κεντρικό οργανισμό. Με αυτόν τον τρόπο η αλυσίδα μπλοκ μπορεί να μειώσει σημαντικά το κόστος του διακομιστή (συμπεριλαμβανομένου του κόστους ανάπτυξης και του κόστους λειτουργίας) και να αμβλύνει τα σημεία συμφόρησης των επιδόσεων στον κεντρικό διακομιστή.

[20]Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities.

- Ανωνυμία

Κάθε χρήστης μπορεί να αλληλοεπιδράσει με το δίκτυο Blockchain με μια παραγόμενη διεύθυνση. Περαιτέρω, ένας χρήστης θα μπορούσε να δημιουργήσει πολλές διευθύνσεις για να αποφύγει την έκθεση της ταυτότητάς του. Δεν υπάρχει πλέον κανένα κεντρικό μέρος που να διατηρεί τις ιδιωτικές πληροφορίες των χρηστών. Αυτός ο μηχανισμός διατηρεί ένα ορισμένο βαθμό ιδιωτικότητα στις συναλλαγές που περιλαμβάνονται στην αλυσίδα μπλοκ. Σημειώστε ότι η αλυσίδα μπλοκ δεν μπορεί να εγγυηθεί την τέλεια διατήρηση της ιδιωτικότητας λόγω του εγγενούς περιορισμού.

- Συνέπεια

Δεδομένου ότι κάθε μία από τις συναλλαγές που διαδίδονται στο δίκτυο πρέπει να επιβεβαιώνεται και να καταγράφεται σε μπλοκ που κατανέμονται σε ολόκληρο το δίκτυο, είναι σχεδόν αδύνατη η αλλοίωσή τους. Επιπλέον, κάθε μπλοκ που μεταδίδεται θα επικυρώνεται από άλλους κόμβους και οι συναλλαγές θα ελέγχονται. Έτσι, οποιαδήποτε παραποίηση θα μπορούσε να εντοπιστεί εύκολα.

- Ελεγξιμότητα

Δεδομένου ότι κάθε συναλλαγή στην αλυσίδα μπλοκ επικυρώνεται και καταγράφεται με χρονοσφραγίδα, οι χρήστες μπορούν εύκολα να επαληθεύσουν και να εντοπίσουν τις προηγούμενες εγγραφές μέσω πρόσβασης σε οποιονδήποτε κόμβο του κατανεμημένου δικτύου. Στην αλυσίδα μπλοκ Bitcoin, κάθε συναλλαγή θα μπορούσε να ανιχνευθεί σε προηγούμενες συναλλαγές επαναληπτικά. Επιπλέον, βελτιώνει την ιχνηλασιμότητα και τη διαφάνεια των δεδομένων που είναι αποθηκευμένα στην αλυσίδα μπλοκ[21].

[21]Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey

- Διαφάνεια

Κάθε ενέργεια καταγράφεται στο Blockchain και τα δεδομένα των εγγραφών είναι διαθέσιμα σε κάθε συμμετέχοντα σε αυτό το Blockchain και δεν μπορούν να αλλάξουν ή να διαγραφούν. Η διαφάνεια του Blockchain επιτυγχάνεται στη διαδικασία αντιγραφής των συναλλαγών. Τα αποτελέσματα αυτής της καταγραφής προσδίδουν στο Blockchain διαφάνεια και αξιοπιστία.

- Αξιοπιστία

Η αξιοπιστία του Blockchain βασίζεται στην πίστη δύο ή περισσότερων συμμετεχόντων, οι οποίοι δεν γνωρίζονται μεταξύ τους. Η κύρια ιδέα είναι οι πραγματικές και όχι άχρηστες συναλλαγές μεταξύ αυτών των άγνωστων ανθρώπων. Η εμπιστοσύνη μπορεί να αυξηθεί περαιτέρω, επειδή μπορούν να υπάρχουν περισσότερες κοινές διαδικασίες και εγγραφές.

Η αξιοπιστία επιτυγχάνεται στις συναλλαγές που συμφωνούνται και μοιράζονται σε όλη την αλυσίδα μπλοκ. Όταν η συναλλαγή θα συνδεθεί στο Blockchain, δεν θα είναι δυνατή η αλλαγή ή η διαγραφή της. Οι χρήστες του Blockchain έχουν την εξουσία να ελέγχουν όλες τις συναλλαγές και τις πληροφορίες. Η αλλαγή ή η διαγραφή των πληροφοριών στο Blockchain είναι δυνατή όταν ο εισβολέας έχει τη φανταστική υπολογιστική ισχύ για να είναι σε θέση να αντικαταστήσει ή να διαγράψει τις πληροφορίες σε όλους τους υπολογιστές, οι οποίες περιλαμβάνονται στο Blockchain πριν από το επόμενο μπλοκ που καταγράφεται εδώ. Εάν το Blockchain αποτελείται από μικρό αριθμό υπολογιστών, η τεχνολογία είναι πιο εκτεθειμένη σε επιθέσεις, ενώ εάν υπάρχουν πολλοί υπολογιστές στο Blockchain, το σύστημα γίνεται ασφαλέστερο και πιο διαφανές.

- Ταχύτερη Επεξεργασία

Το τελευταίο πλεονέκτημα είναι η ταχύτερη επεξεργασία. Παραδοσιακά, η συναλλαγή απαιτεί πολύ χρόνο για την επεξεργασία και την πρωτοκόλληση στον

τραπεζικό οργανισμό. Η χρήση της τεχνολογίας Blockchain συμβάλλει στη μείωση του χρόνου επεξεργασίας και πρωτοκόλλησης από περίπου 3 ημέρες σε αρκετά λεπτά ή ακόμη και δευτερόλεπτα.

2.4.6 Μειονεκτήματα Τεχνολογίας Blockchain

Η αλυσίδα Blockchain ως ένας νέος τύπος βάσης δεδομένων μπορεί να έχει πολλά πλεονεκτήματα αλλά η τεχνολογία αυτή, έχει και κάποια μειονεκτήματα ή προκλήσεις τα οποία είναι: η υψηλή κατανάλωση ενέργειας, η δυνατότητα διάσπασης της αλυσίδας και το υψηλό κόστος.

- Υψηλή Κατανάλωση Ενέργειας

Η κατανάλωση ενέργειας απαιτείται για τη διατήρηση ενός λογιστικού βιβλίου σε πραγματικό χρόνο. Κάθε φορά δημιουργείται νέος κόμβος και ταυτόχρονα επικοινωνεί με κάθε άλλο κόμβο. Με αυτόν τον τρόπο δημιουργείται διαφάνεια. Οι ανθρακωρύχοι του δικτύου προσπαθούν να επιλύσουν πολλές λύσεις ανά δευτερόλεπτο στην προσπάθειά τους να επικυρώσουν τις συναλλαγές, χρησιμοποιούν σημαντικές ποσότητες ισχύος υπολογιστών. Κάθε κόμβος δίνει ακραία επίπεδα ανοχής σφαλμάτων, εξασφαλίζει μηδενικό χρόνο διακοπής λειτουργίας και καθιστά τα δεδομένα που είναι αποθηκευμένα στο Blockchain για πάντα αμετάβλητα και ανθεκτικά στη λογοκρισία. Αλλά αυτές οι ενέργειες καίνε ηλεκτρική ενέργεια και χρόνο που είναι σπατάλη, ειδικά όταν κάθε κόμβος επαναλαμβάνει την επίτευξη της Συναίνεσης.

- Δυνατότητα Διάσπασης της Αλυσίδας

Το επόμενο πρόβλημα του Blockchain είναι η δυνατότητα διάσπασης της αλυσίδας. Οι κόμβοι, οι οποίοι λειτουργούν με το παλιό λογισμικό, δεν θα δέχονται τις συναλλαγές στη νέα αλυσίδα. Αυτή η αλυσίδα δημιουργείται με το ίδιο ιστορικό με την αλυσίδα, η οποία βασίζεται στο παλιό λογισμικό και ονομάζεται

διχάλα. Υπάρχουν δύο είδη διακλαδώσεων το soft fork (απαλή διακλάδωση) και το hard fork (σκληρή διακλάδωση).

Το soft fork δημιουργεί το νέο σύνολο κανόνων στα μπλοκ του πρωτοκόλλου. Οι κόμβοι ενημερώνονται για να επιβάλλουν τους κανόνες του soft fork. Εάν το μπλοκ, το οποίο θεωρούνταν έγκυρο πριν, παραβιάζει τους νέους κανόνες του soft fork, το μπλοκ δεν θα θεωρείται έγκυρο μετά την ενεργοποίηση του soft fork. Για παράδειγμα, το soft fork περιορίζει το μέγεθος του μπλοκ μέχρι τα 500 kB, αλλά πριν ήταν το 1 MB. Αυτό σημαίνει ότι τα μπλοκ, τα οποία είναι μεγαλύτερα από 500 kB, δεν θα είναι έγκυρα στη νέα αλυσίδα μετά την αναβάθμιση.

Από την άλλη πλευρά η σκληρή διακλάδωση χαλαρώνει το σύνολο των κανόνων για τα μπλοκ στο πρωτόκολλο. Αυτή η διαδικασία είναι η ίδια με τη διαδικασία soft fork, αλλά η αξία και το αποτέλεσμά της είναι αντίθετα. Για παράδειγμα, το hard fork αυξάνει το μέγεθος των μπλοκ στα 2 MB από 1 MB. Εάν το μπλοκ έχει περάσει από όλους τους κανόνες του hard fork, το μπλοκ θα γίνει αποδεκτό, ακόμη και αν το μπλοκ δεν υπήρχε στην αλυσίδα πριν.

- Υψηλό Κόστος

Ένα άλλο πρόβλημα της αλυσίδας μπλοκ είναι η ισορροπία μεταξύ της ποσότητας των κόμβων και του ευνοϊκού κόστους για τους χρήστες. Αυτό σημαίνει ότι το Blockchain μεγαλώνει όταν τα νέα μπλοκ εντάσσονται στην αλυσίδα και οι υπολογιστικές απαιτήσεις αυξάνονται. Δεν μπορούν όμως όλοι οι κόμβοι να παρέχουν την απαραίτητη χωρητικότητα. Οπότε υπάρχουν δύο προβλήματα: το πρώτο είναι, το να δημιουργηθεί ένα μικρότερο βιβλίο επειδή οι κόμβοι δεν μπορούν να μεταφέρουν το πλήρες αντίγραφο της αλυσίδας μπλοκ. Ως αποτέλεσμα να σπάει το αμετάβλητο και διαφανές της αλυσίδας μπλοκ και δεύτερο είναι ότι το blockchain γίνεται ένα πιο συγκεντρωτικό σύστημα. Σε αυτή την περίπτωση, το κόστος είναι υψηλότερο, επειδή οι κόμβοι έλαβαν υψηλότερες ανταμοιβές αλλά οι συναλλαγές ολοκληρώνονται πιο αργά, επειδή οι κόμβοι δεν εργάζονται εντατικά. Το μέσο κόστος της συναλλαγής είναι μεταξύ 75 και 160

δολαρίων και το μεγαλύτερο μέρος του καλύπτεται από την κατανάλωση ενέργειας[22].

2.5 Bitcoin

2.5.1 Γενικές πληροφορίες και Ιστορικό

Το Bitcoin είναι ένα δημοφιλές κρυπτονόμισμα που καταγράφει όλες τις συναλλαγές σε ένα κατανεμημένο δημόσιο βιβλίο που ονομάζεται Blockchain. Η ασφάλεια του Bitcoin βασίζεται σε μεγάλο βαθμό στην απόδειξη εργασίας (PoW), η οποία εκτελείται από κόμβους του δικτύου που ονομάζονται ανθρακωρύχοι. Σε αντάλλαγμα για το κίνητρο, οι ανθρακωρύχοι αναμένεται να διατηρούν με ειλικρίνεια την αλυσίδα μπλοκ.

Από την έναρξή του το 2009, η οικονομία του Bitcoin έχει αναπτυχθεί με τεράστιο ρυθμό και σήμερα αξίζει περίπου 170 δισεκατομμύρια δολάρια. Τον Δεκέμβριο του 2017, είχε πάνω από 375.000 επιβεβαιωμένες συναλλαγές ανά ημέρα και η τρέχουσα συναλλαγματική ισοτιμία του Bitcoin ήταν περίπου 13 χιλ. δολάρια από περίπου 1000 δολάρια στις αρχές του 2016. Αυτή η εκθετική αύξηση της αγοραίας αξίας του Bitcoin παρακινεί τους αντιπάλους να εκμεταλλευτούν τις αδυναμίες για κέρδος και τους ερευνητές να ανακαλύψουν νέα τρωτά σημεία του συστήματος, να προτείνουν αντίμετρα και να προβλέψουν τις επερχόμενες τάσεις. Πράγματι, έχουν περιγράφει πολυάριθμες επιθέσεις που στοχεύουν σε διάφορες πτυχές του συστήματος, συμπεριλαμβανομένης της αλλοίωσης των συναλλαγών, των επιθέσεων δικτύωσης ή των επιθέσεων που στοχεύουν στην εξόρυξη και τις δεξαμενές εξόρυξης.

Παρόλο αυτά, οι κύριες τεχνολογίες του, όπως η αλυσίδα μπλοκ και τα πρωτόκολλα συναίνεσης κάνουν το Bitcoin να είναι το πιο επιτυχημένο κρυπτονόμισμα μέχρι σήμερα. Για τον λόγο αυτό πολλές εταιρείες οραματίζονται διάφορες εφαρμογές επόμενης γενιάς, όπως οι έξυπνες συναλλαγές σε έξυπνα δίκτυα, το Διαδίκτυο των πραγμάτων (IoT), τα δίκτυα οχημάτων, η διαχείριση δεδομένων υγειονομικής περίθαλψης και οι έξυπνες πόλεις. Καθώς η διάρκεια της δημοτικότητας εξαρτάται σε

[22] Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering.

μεγάλο βαθμό από το μέγεθος της ασφάλειας που έχει ενσωματωθεί στο σύστημα, το Bitcoin θα κατακτήσει σύντομα τις διαδικτυακές συναλλαγές.

2.5.2 Περιγραφή του Bitcoin

Το Bitcoin είναι ένα διεθνές αποκεντρωμένο ψηφιακό εικονικό νόμισμα που λειτουργεί χωρίς οικονομικό διαμεσολαβητή, κεντρική τράπεζα ή οποιοδήποτε τρίτο μέρος. Βασίζεται σε δίκτυο peer-to-peer (P2P) και σε ένα πιθανοτικό κατανεμημένο πρωτόκολλο συναίνεσης. Ειδικότερα, ένας ιδιοκτήτης έχει τον πλήρη έλεγχο των bitcoins του και μπορεί να τα ξοδέψει ανά πάσα στιγμή και οπουδήποτε χωρίς να εμπλέκεται καμία κεντρική αρχή. Ο σχεδιασμός του Bitcoin είναι ανοικτού κώδικα και κανείς δεν το κατέχει ή δεν το ελέγχει. Επιπλέον, είναι μια κρυπτογραφικά ασφαλής ηλεκτρονική πληρωμή και επιτρέπει συναλλαγές που αφορούν εικονικό νόμισμα με τη μορφή ψηφιακών tokens που ονομάζονται νομίσματα Bitcoin (BTC ή απλά bitcoins).

Οι ηλεκτρονικές πληρωμές του γίνονται με τη δημιουργία συναλλαγών που μεταφέρουν bitcoins μεταξύ των χρηστών. Η διεύθυνση προορισμού (που ονομάζεται επίσης διεύθυνση Bitcoin) δημιουργείται με την εκτέλεση μιας σειράς μη αναστρέψιμων κρυπτογραφικών πράξεων κατακερματισμού στο δημόσιο κλειδί του χρήστη. Στο Bitcoin, ένας χρήστης μπορεί να έχει πολλαπλές διευθύνσεις δημιουργώντας πολλαπλά δημόσια κλειδιά και οι διευθύνσεις αυτές θα μπορούσαν να συσχετιστούν με ένα ή περισσότερα πορτοφόλια του. Το ιδιωτικό κλειδί, του χρήστη απαιτείται για να ξοδέψει τα bitcoins που κατέχει με τη μορφή ψηφιακών υπογεγραμμένων συναλλαγών. Η χρήση του κατακερματισμού του δημόσιου κλειδιού ως διεύθυνση λήψης παρέχει στους χρήστες έναν ορισμένο βαθμό ανωνυμίας και συνιστάται η πρακτική να χρησιμοποιείται διαφορετική διεύθυνση Bitcoin για κάθε συναλλαγή λήψης.

Στο Bitcoin, οι συναλλαγές υποβάλλονται σε επεξεργασία για την επαλήθευση της ακεραιότητάς τους, γνησιότητα και την ορθότητά τους από μια ομάδα πολυμήχανων κόμβων του δικτύου που ονομάζονται miners "Εξ ορυκτές". Συγκεκριμένα, αντί να εξορύσσουν μια μεμονωμένη συναλλαγή, οι ανθρακωρύχοι ομαδοποιούν έναν αριθμό συναλλαγών που περιμένουν το δίκτυο να τις επεξεργαστεί σε μια ενιαία μονάδα που ονομάζεται "μπλοκ". Ο ανθρακωρύχος διαφημίζει ένα μπλοκ

σε ολόκληρο το δίκτυο και μόλις ολοκληρώσει την επεξεργασία του (ή την επικύρωσή του), διεκδικεί μια αμοιβή εξόρυξης. Αυτό το μπλοκ επαληθεύεται στη συνέχεια από την πλειοψηφία των εξορύξεων στο δίκτυο πριν προστεθεί επιτυχώς σε ένα κατανεμημένο δημόσιο βιβλίο που ονομάζεται "Blockchain". Ο ανθρακωρύχος που εξορύσσει ένα μπλοκ λαμβάνει ανταμοιβή όταν το εξορυσσόμενο μπλοκ προστεθεί επιτυχώς στο Blockchain. Στην συνέχεια θα παρουσιάσουμε τα λειτουργικά χαρακτηριστικά που είναι απαραίτητα για την πρακτική υλοποίηση του Bitcoin[23].

2.5.3 Ψηφιακό Πορτοφόλι

Το πορτοφόλι κρυπτονομισμάτων είναι ένα εργαλείο που επιτρέπει στους χρήστες να αλληλοεπιδρούν με δίκτυα Blockchain. Είναι απαραίτητα κατά την αποστολή και λήψη Bitcoin και άλλων ψηφιακών νομισμάτων. Τα πορτοφόλια κρυπτονομισμάτων μπορούν επίσης να χρησιμοποιηθούν για τη δημιουργία νέων διευθύνσεων Blockchain. Για να κατανοήσουμε το πορτοφόλι θα πρέπει λοιπόν να εξοικειωθούμε με την έννοια της διεύθυνσης.

Διεύθυνση

Μια διεύθυνση είναι ένα τυχαίο σύνολο αριθμών και γραμμάτων που αντιπροσωπεύουν έναν τύπο μοναδικού αριθμού παρόμοιου με έναν αριθμό τραπεζικού λογαριασμού και μάλιστα μπορούν να μοιραστούν ελεύθερα τη δημόσια διεύθυνσή τους με άλλους. Με αυτόν τον τρόπο, οι χρήστες μπορούν να στέλνουν κρυπτονομίσματα στη διεύθυνσή αυτήν.

Πώς λειτουργεί ένα πορτοφόλι bitcoin

Σε αντίθεση με τα παραδοσιακά πορτοφόλια που χρησιμοποιούμε στην καθημερινή μας ζωή, ένα ψηφιακό πορτοφόλι δεν αποθηκεύει πραγματικά τα χρήματά. Στην πραγματικότητα, τα κρυπτονομίσματα (ή τα Tokens) είναι απλά μέρος ενός συστήματος Blockchain ως κομμάτια δεδομένων και τα πορτοφόλια χρησιμεύουν ως

[23]Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin IEEE Communications Surveys & Tutorials.

μέσο πρόσβασης σε αυτά. Από τεχνικής απόψεως, τα περισσότερα πορτοφόλια κρυπτονομισμάτων μπορούν να δημιουργήσουν ένα ή περισσότερα ζεύγη δημόσιων και ιδιωτικών κλειδιών. Το δημόσιο κλειδί χρησιμοποιείται για τη δημιουργία διευθύνσεων πορτοφολιού, οι οποίες απαιτούνται για τη λήψη πληρωμών. Τα ιδιωτικά κλειδιά, από την άλλη πλευρά, χρησιμοποιούνται κατά τη δημιουργία ψηφιακών υπογραφών και την επαλήθευση συναλλαγών (τα ιδιωτικά κλειδιά είναι εμπιστευτικά και δεν πρέπει ποτέ να κοινοποιούνται σε κανέναν).

Είδη Πορτοφολιών

Υπάρχουν τρεις μεγάλες ομάδες πορτοφολιών κρυπτογράφησης: Software, hardware και πορτοφόλια Paper. Ωστόσο, μπορούν επίσης να οριστούν ως ζεστά πορτοφόλια ή κρύα πορτοφόλια ανάλογα με τον τρόπο λειτουργίας τους. Τα ζεστά πορτοφόλια είναι αυτά που κατά κάποιο τρόπο συνδέονται στο διαδίκτυο και, επομένως, είναι πιο ευαίσθητα σε επιθέσεις hacking. Τα κρύα πορτοφόλια είναι αυτά που δημιουργούν κλειδιά χωρίς σύνδεση στο Διαδίκτυο, τα οποία τα καθιστούν εξαιρετικά ανθεκτικά στις κυβερνοεπιθέσεις.

Software wallet

Οι πιο συνηθισμένοι τύποι πορτοφολιών λογισμικού περιλαμβάνουν πορτοφόλια ιστού, πορτοφόλια επιφάνειας και κινητά πορτοφόλια.

i. Πορτοφόλι Ιστού: αποτελείται από μια διεπαφή προγράμματος περιήγησης που δεν απαιτεί λήψη ή εγκατάσταση. Είναι πιο βολικό αλλά και πιο επικίνδυνο καθώς τα ιδιωτικά κλειδιά διαχειρίζονται συνήθως από τρίτους.

ii. Πορτοφόλι επιφάνειας εργασίας: είναι ένα λογισμικό που μπορεί να ληφθεί και να εκτελεστεί τοπικά. Λιγότερο βολικό από τα πορτοφόλια ιστού αλλά πιο ασφαλές επειδή τα ιδιωτικά κλειδιά αποθηκεύονται τοπικά και διαχειρίζονται από τους χρήστες. Τα πορτοφόλια πρέπει να χρησιμοποιούνται μόνο σε υπολογιστές που είναι καθαροί (χωρίς μολύνσεις από ιούς ή κακόβουλα προγράμματα).

iii. Πορτοφόλι για κινητά: είναι παρόμοια με τα πορτοφόλια για υπολογιστές, αλλά έχουν σχεδιαστεί για smartphone. Η χρήση κωδικών QR, τους καθιστά μια βολική εναλλακτική λύση για την αποστολή και τη λήψη κρυπτονομισμάτων.

Hardware wallet

Τα πορτοφόλια hardware αποτελούνται από φυσικές συσκευές που δημιουργούν και αποθηκεύουν κλειδιά χωρίς σύνδεση στο Διαδίκτυο και, ως εκ τούτου, εμπίπτουν στην κατηγορία των κρύων πορτοφολιών. Συνήθως, τα κλειδιά δημιουργούνται με βάση αλγόριθμους τυχαίας παραγωγής αριθμών (RNG) και αποθηκεύονται στην ίδια τη συσκευή (και πουθενά αλλού). Τέτοια πορτοφόλια χαρακτηρίζονται ως κρύα πορτοφόλια καθώς τα ιδιωτικά κλειδιά αποθηκεύονται στην συσκευή και βρίσκονται εκτός δικτύου.

Paper wallet

Ένα paper πορτοφόλι αποτελείται από ένα κομμάτι χαρτί με διεύθυνση Blockchain και το αντίστοιχο ιδιωτικό κλειδί του. Τα κλειδιά τυπώνονται συνήθως ως μεγάλες σειρές αριθμών και γραμμάτων μαζί με κωδικούς QR, οι οποίοι μπορούν να σαρωθούν για την εκτέλεση συναλλαγών με κρυπτονομίσματα. Εάν χρησιμοποιούνται paper πορτοφόλια για τη δημιουργία κλειδιών εκτός σύνδεσης, μπορούν επίσης να θεωρηθούν κρύα πορτοφόλια. Ωστόσο, η χρήση τους αποθαρρύνεται επειδή παρουσιάζουν πολλά ελαττώματα και πιθανό κίνδυνο για χρήστες που δεν διαθέτουν τεχνικές γνώσεις[24].

[24]https://www.basecoin.gr/psifiako-portofoli-kryptonomismaton/

2.5.4 Συναλλαγές Bitcoin

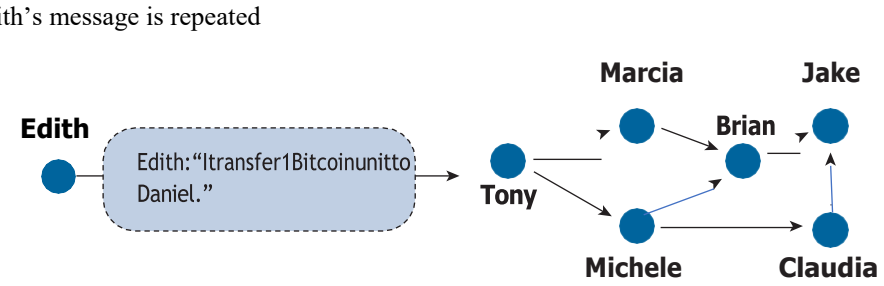
Οι συναλλαγές Bitcoin θεωρούνται συνήθως ως μεταφορά bitcoins από μια πηγή σε μια διεύθυνση προορισμού, κατά την οποία ο πρώτος μπορεί να αποδείξει την κυριότητα αυτών των bitcoins και συνεπώς, να τα ξοδέψει, παρέχοντας μια ψηφιακή υπογραφή[25]. Κάθε συναλλαγή περιέχει εισόδους και εξόδους. Μια είσοδος έχει την αναφορά στην έξοδο από την προηγούμενη συναλλαγή και η έξοδος μιας συναλλαγής περιέχει τη διεύθυνση λήψης και το αντίστοιχο ποσό. Γενικά, σε μια συναλλαγή, ένας συγκεκριμένος αριθμός bitcoin αποστέλλεται από ένα πορτοφόλι bitcoin, σε μια συγκεκριμένη διεύθυνση, εφόσον υπάρχει επαρκές υπόλοιπο στο πορτοφόλι από προηγούμενες συναλλαγές. Οι συναλλαγές δεν κρυπτογραφούνται και μπορούν να προβληθούν στην αλυσίδα μπλοκ με τις αντίστοιχες διευθύνσεις τους, αλλά η ταυτότητα του αποστολέα ή του παραλήπτη παραμένει ανώνυμη. Συνήθως, τα πορτοφόλια αυτά διαθέτουν ένα ιδιωτικό κλειδί που χρησιμοποιείται για την υπογραφή των συναλλαγών. Αυτό το ασφαλές κομμάτι δεδομένων παρέχει μια μαθηματική απόδειξη ότι τα νομίσματα της συναλλαγής προέρχονται από τον ιδιοκτήτη του πορτοφολιού. Με το ιδιωτικό κλειδί και την υπογραφή, ο λογαριασμός είναι προσβάσιμος μόνο από τον ιδιοκτήτη του και οι συναλλαγές δεν μπορούν να τροποποιηθούν από κάποιον άλλον χρήστη[26].

Ωστόσο, για να κατανοήσουμε το σύστημα Bitcoin, είναι απαραίτητο να συνδυάσουμε στοιχεία από τους τρεις κλάδους της οικονομίας, της κρυπτογραφίας και της επιστήμης των υπολογιστών. Έχοντας παρουσιάσει μια γενική επισκόπηση του συστήματος Bitcoin, θα εξηγήσουμε μερικά τεχνικά στοιχεία του συστήματος με περισσότερη λεπτομέρεια. Οι Berentsen και Schär (2017) υποστηρίζουν ότι η επεξεργασία συναλλαγών απαιτεί την ικανοποίηση τριών απαιτήσεων: (1) την ικανότητα συναλλαγής, (2) την νομιμότητα της συναλλαγής και (3) την συναίνεση της συναλλαγής. Αυτές οι τρεις απαιτήσεις θα εξεταστούν τώρα και θα γίνει μια προσπάθεια να εξηγηθούν για το πώς μπορούν να ικανοποιηθούν αυτές οι προϋποθέσεις ελλείψει μιας κεντρικής αρχής.

[25]Delgado-Segura, S., Pérez-Solà, C., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2020). A fair protocol for data trading based on Bitcoin transactions.
[26]Chuen, D. L. K., Guo, L., & Wang, Y. (2017). Cryptocurrency: A new investment opportunity.

- *Ικανότητα Συναλλαγής*

Αυτό που πρέπει να επιλυθεί είναι πώς μπορούν να ξεκινήσουν οι συναλλαγές εάν δεν υπάρχει κεντρική αρχή. Σε ένα κλασικό τραπεζικό σύστημα, ο πελάτης μιλάει με τον σύμβουλό του ή υποβάλλει τις εντολές πληρωμής του μέσω της ηλεκτρονικής τραπεζικής υπηρεσίας. Η υποδομή που παρέχεται από την εμπορική τράπεζα διασφαλίζει ότι η συναλλαγή θα κοινοποιηθεί προς εκτέλεση. Ελλείψει κεντρικής αρχής, η κοινοποίηση μιας εντολής πληρωμής με αυτή την παραδοσιακή έννοια δεν είναι δυνατή. Στο σύστημα Bitcoin, μια εντολή πληρωμής μπορεί να κοινοποιηθεί σε οποιονδήποτε αριθμό κόμβων του δικτύου. Οι κόμβοι του δικτύου συνδέονται μεταξύ τους σε ένα χαλαρό δίκτυο και προωθούν το μήνυμα μέχρι να ενημερωθούν όλοι οι κόμβοι για τη συναλλαγή (Σχήμα 2.5.4). Με τον τρόπο αυτόν πετυχαίνουμε την αποκέντρωση του συστήματος που δημιουργεί πολλά πλεονεκτήματα. Συγκεκριμένα, καθιστά το σύστημα εξαιρετικά εύρωστο. Δεν υπάρχει ούτε ένα κεντρικό σημείο αποτυχίας που μπορεί να δεχθεί επίθεση και ούτε κάποιοι κόμβοι που σχετίζονται με το σύστημα θα μπορούσαν να προκαλέσουν την κατάρρευση του συστήματος. Ως εκ τούτου, το σύστημα λειτουργεί ακόμη και όταν ορισμένοι κόμβοι του δικτύου δεν είναι προσβάσιμοι και μπορεί πάντα να δημιουργεί νέες συνδέσεις.



Σχήμα 2.5.4:Συναλλαγή Bitcoin που κοινοποιείται στους κόμβους του δικτύου. (Πηγή: Berentsen, A., & Schär, F. (2018). A short introduction to the world of cryptocurrencies.)

- *Νομιμότητα Συναλλαγής*

Κάθε συμμετέχων μπορεί να δημιουργήσει νέες εντολές πληρωμής και να τις διαδώσει στο δίκτυο. Αυτό το χαρακτηριστικό ενέχει τον κίνδυνο δόλιων μηνυμάτων. Εν προκειμένω, προκύπτουν δύο σημαντικά ερωτήματα:

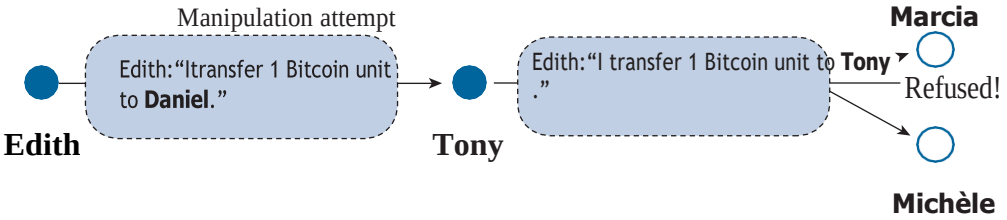
1. Πώς γνωρίζουν οι κόμβοι ότι ο ευκίνητής της συναλλαγής είναι ο νόμιμος ιδιοκτήτης και ότι αυτός ή αυτή δικαιούται έτσι να μεταβιβάσει τις μονάδες Bitcoin;

2. Πώς μπορεί κανείς να διασφαλίσει ότι το μήνυμα της συναλλαγής δεν θα αλλοιωθεί πριν περάσει από τον έναν κόμβο στον επόμενο;

Στο σύστημα Bitcoin, η νομιμότητα των συναλλαγών διασφαλίζεται με τη χρήση ασύμμετρης κρυπτογραφίας που έχουμε εξηγήσει πιο πάνω. Η ιδέα βασίζεται στη χρήση ζευγών κλειδιών που αποτελούνται από ένα ιδιωτικό και ένα δημόσιο κλειδί. Ένα ιδιωτικό κλειδί δεν πρέπει να μοιράζεται. Αντιστοιχεί σε μια τυχαία τιμή από ένα απίστευτα μεγάλο σύνολο αριθμών. Ένα δημόσιο κλειδί, από την άλλη πλευρά, προέρχεται από αυτόν τον αριθμό και μπορεί να διαμοιραστεί ελεύθερα. Χρησιμεύει ως ψευδώνυμο στο δίκτυο Bitcoin. Ένα ιδιωτικό κλειδί χρησιμοποιείται για την κρυπτογράφηση ενός μηνύματος που μπορεί να αποκρυπτογραφηθεί μόνο με τη χρήση του αντίστοιχου δημόσιου κλειδιού. Αυτός ο τύπος κρυπτογράφησης είναι επίσης γνωστός ως "υπογραφή". Η υπογραφή διευκρινίζει ότι η προσέγγιση αυτή δεν χρησιμοποιείται για την απόκρυψη οποιασδήποτε πληροφορίας στο κρυπτογραφημένο μήνυμα. Οποιοσδήποτε μπορεί απλώς να αποκρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του, αλλά η υπογραφή χρησιμεύει ως απόδειξη ότι το μήνυμα έχει προηγουμένως κρυπτογραφηθεί με το αντίστοιχο ιδιωτικό του κλειδί και είναι σαν μια χειρόγραφη υπογραφή αλλά πολύ πιο ασφαλής.

Για παράδειγμα, σκεφτείτε την Edith, η οποία θέλει να στείλει μια πληρωμή Bitcoin στον Daniel μέσω του δικτύου Bitcoin. Χρησιμοποιεί το ιδιωτικό της κλειδί για να κρυπτογραφήσει το μήνυμα. Οι άλλοι συμμετέχοντες στο δίκτυο μπορούν να αποκρυπτογραφήσουν το μήνυμα αυτό μόνο χρησιμοποιώντας το δημόσιο κλειδί της Edith. Εάν μια προσπάθεια είναι επιτυχής, εξασφαλίζει ότι το

μήνυμα κρυπτογραφήθηκε με τη χρήση του αντίστοιχου ιδιωτικού κλειδιού. Επειδή κανείς άλλος δεν έχει πρόσβαση στο ιδιωτικό κλειδί της Edith, η προσέγγιση αυτή μπορεί να χρησιμοποιηθεί για την επικύρωση της προέλευσης της συναλλαγής (Σχήμα 2.5.5).



Σχήμα 2.5.5: Απόπειρα χειραγώγησης συναλλαγής Bitcoin

Πηγή: Berentsen, A., &Schär, F. (2018). A short introduction to the world of cryptocurrencies.

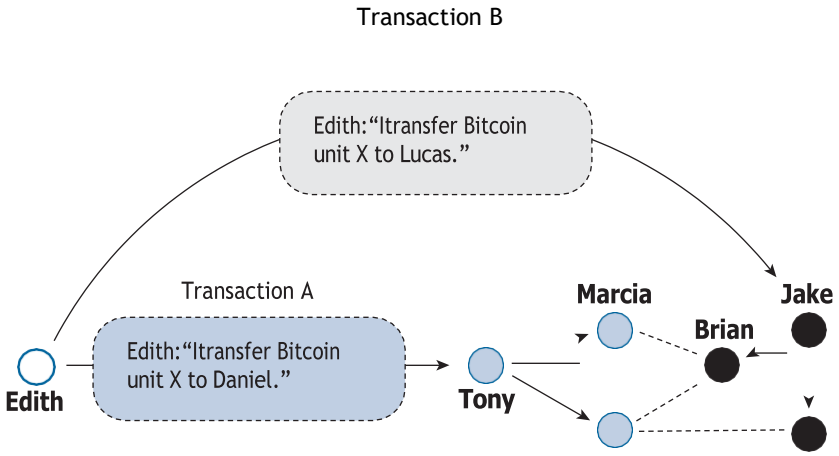
Όταν η συναλλαγή κυκλοφορεί στο δίκτυο, οποιοσδήποτε συμμετέχων του δικτύου μπορεί να αποκρυπτογραφήσει αυτό το μήνυμα και είναι σε θέση να αλλάξει στη συνέχεια τις οδηγίες πληρωμής. Ωστόσο, επειδή ο συμμετέχων δεν κατέχει το ιδιωτικό κλειδί της Edith, δεν μπορεί να αποκρυπτογραφήσει εκ νέου το παραποιημένο μήνυμα. Συνεπώς, η παραποιημένη συναλλαγή θα εντοπιστεί και θα απορριφθεί από το υπόλοιπο δίκτυο.

- *Συναλλαγή Συναίνεσης*

Συζητήσαμε ήδη παραπάνω πώς επικοινωνείτε ένα μήνυμα συναλλαγής και πώς μπορεί να επαληθευτεί η νομιμότητα και η προέλευσή του. Εξηγήσαμε επίσης πώς επιτυγχάνεται η συναίνεση σχετικά με την ιδιοκτησία των μονάδων Bitcoin στο δίκτυο Bitcoin με τη χρήση της συναίνεσης proof-of-work πρωτόκολλο. Τώρα θα εξηγήσουμε πως επιτυγχάνεται η συναλλαγή συναίνεσης με ένα παράδειγμα.

Η Edith ήταν σε θέση να δημιουργήσει δύο συναλλαγές που και οι δύο αναφέρονται στις ίδιες μονάδες Bitcoin. Και οι δύο συναλλαγές θα μπορούσαν να διαδοθούν ταυτόχρονα στο δίκτυο (ικανότητα συναλλαγής) και οι δύο θα

εμφάνιζαν έγκυρη προέλευση (νομιμότητα συναλλαγής). Λόγω των διαφορών στη διάδοση αυτών των δύο μηνυμάτων στο δίκτυο Bitcoin, ορισμένοι από τους κόμβους θα λάμβαναν πρώτα ένα μήνυμα για τη συναλλαγή Α, ενώ άλλοι θα λάμβαναν πρώτα ένα μήνυμα για τη συναλλαγή Β (Σχήμα 2.5.6). Προκειμένου να αποφευχθεί η διπλή δαπάνη, είναι σημαντικό μόνο η μία από τις δύο συναλλαγές να βρίσκει το δρόμο της στην αλυσίδα μπλοκ του Bitcoin. Επομένως, είναι απαραίτητος ένας μηχανισμός που αποφασίζει ποια από τις δύο συναλλαγές θα συμπεριληφθεί στο Blockchain.



Σχήμα 2.5.6: Επιβεβαίωση πρώτης συναλλαγής Bitcoin που προστίθεται σε ένα έγκυρο υποψήφιο μπλοκ. Πηγή: Berentsen, A., & Schär, F. (2018). A short introduction to the world of cryptocurrencies.

Το σύστημα Bitcoin επιλύει αυτό το πρόβλημα των διπλών δαπανών με έναν έξυπνο τρόπο. Η συναλλαγή που προστίθεται πρώτη σε ένα έγκυρο υποψήφιο μπλοκ, και εφόσον προστίθεται στο Blockchain, θεωρείται επιβεβαιωμένη. Το σύστημα παύει να επεξεργάζεται την άλλη συναλλαγή, έτσι οι ανθρακωρύχοι θα σταματήσουν να προσθέτουν τη συγκρουόμενη συναλλαγή στο υποψήφιο μπλοκ τους. Επιπλέον, δεν είναι δυνατόν για έναν ανθρακωρύχο να προσθέσει αντικρουόμενες συναλλαγές στο ίδιο υποψήφιο μπλοκ. Ένα τέτοιο μπλοκ θα ήταν παράνομο και συνεπώς θα απορρίπτονταν από όλους τους άλλους συμμετέχοντες στο δίκτυο[27].

[27] Berentsen, A., &Schär, F. (2018). A short introduction to the world of cryptocurrencies. FRB of St. Louis Working Review.

2.6 Mining

2.6.1 Περιγραφή της Εξόρυξης

Η εξόρυξη έχει εξελιχθεί σε σύντομο χρονικό διάστημα από ένα απλό χόμπι που εκτελούσαν οι πρώτοι χρήστες σε συνηθισμένους υπολογιστές σε μια βιομηχανία έντασης κεφαλαίου που χρησιμοποιεί προσαρμοσμένο εξοπλισμό υλικού και διαθέτει μια εξειδικευμένη αλυσίδα αξίας. Οι ανθρακωρύχοι (miners) διαδραματίζουν κρίσιμο ρόλο σε κάθε σύστημα κρυπτονομισμάτων, καθώς είναι υπεύθυνοι για την ομαδοποίηση ανεπιβεβαίωτων συναλλαγών σε νέα μπλοκ και την προσθήκη τους στο παγκόσμιο βιβλίο ("blockchain")[28]. Το παζλ στο οποίο εργάζονται οι ανθρακωρύχοι είναι ένα κρυπτογραφικό proof-of-work το οποίο απαιτεί σημαντική προσπάθεια σε υπολογιστικό χρόνο και ισχύ για την επίλυση. Ο γρίφος απόδειξης εργασίας βασίζεται στην απόδειξη εργασίας Hashcash. Η επίλυση του γρίφου απαιτεί την ολοκλήρωση ενός καθορισμένου αριθμού υπολογισμών. Το όριο αυτό καθορίζεται από το επίπεδο δυσκολίας του γρίφου, το οποίο καθορίζεται δυναμικά από το δίκτυο. Το επίπεδο δυσκολίας προσαρμόζεται κάθε 2016 μπλοκ σύμφωνα με έναν αλγόριθμο, έτσι ώστε ένα νέο μπλοκ συναλλαγών να προστίθεται στο δίκτυο κατά μέσο όρο κάθε 10 λεπτά. Εάν ο μέσος χρόνος για την προσθήκη των προηγούμενων μπλοκ 2016 πέσει κάτω από αυτόν, το επίπεδο δυσκολίας αυξάνεται για τα επόμενα μπλοκ 2016. Στην πράξη, αυτό σημαίνει ότι η δυσκολία προσαρμόζεται περίπου κάθε δύο εβδομάδες.

Επιπλέον, κάθε ανθρακωρύχος επιλέγει μια υπολογιστική τεχνολογία (κυρίως υλικό υπολογιστών) την οποία χρησιμοποιεί στην προσπάθειά του να λύσει τον γρίφο. Όσο μεγαλύτερη είναι η υπολογιστική τους ισχύς, τόσο μεγαλύτερος είναι ο αριθμός των υπολογισμών που μπορούν να υπολογίσουν μέσα σε ένα δεδομένο χρονικό διάστημα. Συνεπώς, η πιθανότητα να είναι ο πρώτος που θα λύσει το παζλ αυξάνεται με την ποσότητα της υπολογιστικής τεχνολογίας που διαθέτει ένας ανθρακωρύχος. Καθώς η συνάρτηση proof-of-work είναι μια τυχαία διαδικασία, η επίλυση του γρίφου περιλαμβάνει υπολογισμούς ωμής βίας με δοκιμές και σφάλματα. Ως αποτέλεσμα, δεν υπάρχει καμία εγγύηση ότι ο ανθρακωρύχος στο δίκτυο με την μεγαλύτερη υπολογιστική ισχύ θα είναι ο πρώτος που θα λύσει και τον γρίφο. Μόλις ένας

[28] Rauchs, M., & Hileman, G. (2017). Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance Reports.

ανθρακωρύχος προτείνει ότι έχει λύσει τον γρίφο, απαιτείται μόνο ένας υπολογισμός για να επαληθευτεί αν είναι σωστός. Η εργασία αυτή είναι ακριβή, ενώ η απόδειξη ότι έχει γίνει είναι φθηνή και αποτέλεσμα αυτού είναι να λαμβάνει ένα ισχυρό οικονομικό κίνητρο. Για κάθε μπλοκ που εξ ορύσσεται, ο εξ ορυκτής λαμβάνει μια ανταμοιβή μπλοκ καθώς και τα τέλη συναλλαγής των συναλλαγών στο μπλοκ.

Τα τέλη συναλλαγών παρέχουν παρόμοιο κίνητρο και προορίζονται να γίνουν πιο σημαντικά όσο μειώνεται ο ρυθμός έκδοσης bitcoin. Τα τέλη αυτά προσφέρονται από τους χρήστες όταν θέλουν να επηρεάσουν την ταχύτητα με την οποία επεξεργάζεται η συναλλαγή τους. Το κίνητρό τους είναι να δίνουν προτεραιότητα στις συναλλαγές με τη μεγαλύτερη αξία σύμφωνα με τις αμοιβές και αυτό είναι που καθορίζει την τιμή προτεραιότητας των χρηστών. Τα τέλη συναλλαγών έχουν γίνει πιο συνηθισμένα τον τελευταίο καιρό, καθώς η ζήτηση για συναλλαγές στο δίκτυο έχει αυξηθεί ραγδαία, προκαλώντας καθυστερήσεις στην επεξεργασία των συναλλαγών. Οι καθυστερήσεις αυτές είναι αποτέλεσμα του ορίου του 1 megabyte στο μέγεθος των μπλοκ. Όταν η ζήτηση για συναλλαγές στο δίκτυο αυξάνεται πάνω από το μέγεθος του 1 megabyte, ο χρόνος μεταξύ της πρότασης μιας συναλλαγής από έναν χρήστη και της συγκέντρωσής της σε ένα μπλοκ επιμηκύνεται. Έτσι, αυτές οι καθυστερήσεις συμβαίνουν ανεξάρτητα από το δίκτυο εξόρυξης Bitcoin, καθώς το πρωτόκολλο επιβάλλει ότι η επεξεργασία μιας συναλλαγής θα πρέπει να διαρκεί κατά μέσο όρο 10 λεπτά από τη στιγμή που θα έχει συν αρμολογηθεί σε μπλοκ μέσω των δυναμικών προσαρμογών του στη δυσκολία. Κατά συνέπεια, δεν υπάρχει κίνητρο για τους ανθρακωρύχους να επιβραδύνουν σκόπιμα τη δραστηριότητα εξόρυξης για να δημιουργήσουν καθυστέρηση και να κερδίσουν μακροπρόθεσμα πρόσθετες αμοιβές συναλλαγών λόγω της δυναμικής προσαρμογής της δυσκολίας του παζλ.

Αποτέλεσμα όλης αυτής της διαδικασίας είναι η καθαρή αμοιβή για τον νικητή ανθρακωρύχο δηλαδή η συνολική ανταμοιβή (νεοκοπα νομίσματα συν τα τέλη συναλλαγής) μείον το κόστος της υπολογιστικής τους τεχνολογίας. Οι ανθρακωρύχοι που αποτυγχάνουν στην επίλυση ενός υπολογιστικού γρίφου επιβαρύνονται με το κόστος της υπολογιστικής τους τεχνολογίας. Μόλις λυθεί ένας υπολογιστικός γρίφος και καταγραφεί το σχετικό μπλοκ συναλλαγών στο δίκτυο, οι ανθρακωρύχοι

συνεχίζουν να ανταγωνίζονται για την επεξεργασία του επόμενου μπλοκ συναλλαγών[29].

Τέλος, καθώς το bitcoin γίνεται όλο και πιο δημοφιλές, η προσπάθεια για την εξόρυξη bitcoin θα αυξηθεί. Δεδομένου ότι η εξόρυξη bitcoin είναι πολύ ανταγωνιστική, θα επιβιώσουν μόνο εκείνοι οι εξ ορυκτές που εφαρμόζουν το πιο ανταγωνιστικό υλικό εξόρυξης και επωφελούνται από το χαμηλότερο κόστος ηλεκτρικής ενέργειας. Επομένως, η βιωσιμότητα του bitcoin από μόνη της δεν κινδυνεύει άρα και οι εξ ορυκτές της[30].

[29] Ma, J., Gans, J. S., & Tourky, R. (2018). Market structure in bitcoin mining

[30]Vranken, H. (2017). Sustainability of bitcoin and blockchains. Current opinion in environmental sustainability,

ΚΕΦΑΛΑΙΟ 3

ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

3.1 Εισαγωγή

Η ραγδαία άνοδος των κρυπτονομισμάτων αλλάζει για πάντα το παγκόσμιο χρηματοπιστωτικό τοπίο, δημιουργώντας τόσο κινδύνους όσο και ευκαιρίες για νέους και υφιστάμενους παίκτες. Υποστηριζόμενη από την τεχνολογία Blockchain, η κρυπτογράφηση διαταράσσει τα παραδοσιακά επιχειρηματικά μοντέλα καταργώντας την ανάγκη για αξιόπιστους μεσάζοντες. Ως αποτέλεσμα, η εκρηκτική επέκταση των εφαρμογών κρυπτογράφησης που βρίσκεται τώρα σε εξέλιξη σηματοδοτεί την έναρξη μιας επανάστασης που κανένας οργανισμός δεν έχει την πολυτέλεια να αγνοήσει[31].

Η εφεύρεση της τεχνολογίας blockchain άλλαξε ριζικά την αντίληψη για το πώς μπορούν να δομηθούν και να λειτουργήσουν τα νομισματικά συστήματα. Οι κεντρικές τράπεζες και οι κρατικές αρχές αρνούνται ως επί το πλείστον να αναγνωρίσουν ότι τα κρυπτονομίσματα είναι χρήμα. Ωστόσο ο αριθμός των συναλλαγών πληρωμών και υπηρεσιών με την χρήση των κρυπτονομισμάτων να αυξάνεται και τα κρυπτονομίσματα να αποτελούν ένα μη αμελητέο μερίδιο του πλούτου. Όπως και με άλλα οικονομικά φαινόμενα, τα κρυπτονομίσματα θα πρέπει να αντιμετωπίζονται στις οικονομικές καταστάσεις των οντοτήτων που να τα χρησιμοποιούν, παρ' όλου που δεν υπάρχει καμία λογιστική καθοδήγηση στα ισχύοντα πρότυπα χρηματοοικονομικής αναφοράς.

Η επαγγελματική βιβλιογραφία και οι δημόσιες γνώμες σχετικά με τα κρυπτονομίσματα περιστρέφονται κυρίως γύρω από τα τεχνικά χαρακτηριστικά τους, ενώ η ανάλυση των λογιστικών χειρισμών της εργασίας αξιολογείται σε σχέση με τα οικονομικά χαρακτηριστικά τους. Η προσέγγιση αυτή, που σέβεται τη θεμελιώδη αρχή "(οικονομική) ουσία έναντι (νομικής) μορφής", παράγει ενδιαφέροντα αποτελέσματα. Σε ορισμένα σενάρια, μια συναλλαγή που αφορά ένα κρυπτονόμισμα πρέπει να λογιστικοποιείται ως συναλλαγή σε ξένο νόμισμα, παρά τον ισχυρισμό των κεντρικών

[31] https://www.pwc.com/gx/en/about/new-ventures/crypto-center.html

τραπεζιτών ότι τα κρυπτονομίσματα δεν είναι χρήμα. Κατά τον ίδιο τρόπο, αποδεικνύεται ότι τα κρυπτονομίσματα δεν μπορούν να αναγνωριστούν και να καταγραφούν ως άυλα περιουσιακά στοιχεία, παρά το γεγονός ότι έχουν ψηφιακή (εικονική) μορφή και οι ρυθμιστικές αρχές προτρέπουν για μια τέτοια αντιμετώπιση. Η εργασία υποστηρίζει ότι η πιστή απεικόνιση ποικίλλει ανάλογα με τις οντότητες που υποβάλλουν στοιχεία και εξαρτάται από το πραγματικό επιχειρηματικό τους μοντέλο μαζί με την οικονομική πραγματικότητα της υποκείμενης συναλλαγής[32].

Σκοπός της παρούσας εργασίας είναι να εξετάσει τόσο τους πιθανούς λογιστικούς χειρισμούς βάσει του IFRS όσο και την παρουσίαση των κρυπτονομισμάτων εντός των οικονομικών καταστάσεων. Θα πρέπει να σημειωθεί ότι πρόκειται για έναν αναδυόμενο τομέα και η πρακτική θα εξελιχθεί αναμφίβολα με την πάροδο του χρόνου[33].

3.2 Λογιστική Μεταχείριση

Τα κρυπτονομίσματα όπως τα bitcoin, ethereum, ripple και άλλα altcoins έχουν μπει κανονικά μέσα στο συναλλακτικό κύκλο αρκετών Ελληνικών επιχειρήσεων που δέχονται πληρωμές ή αγοράζουν προϊόντα και υπηρεσίες με κρυπτοχρήμα. Ένα θέμα που δημιουργείται από τη χρήση τους είναι η λογιστική απεικόνιση στα βιβλία της επιχείρησης και η φορολογική αντιμετώπιση των εσόδων. Αναφορικά με τη λογιστική αντιμετώπιση του ζητήματος, το Συμβούλιο Λογιστικής Τυποποίησης (ΣΛΟΤ), το εποπτικό συμβούλιο της Επιτροπής Λογιστικής Τυποποίησης και Ελέγχων (ΕΛΤΕ), εξέδωσε την υπ' αριθ. πρωτ.: 104 ΕΞ 27.2.2018 εγκύκλιο.

Η εγκύκλιος του ΣΛΟΤ παρέχει μία γενική κατεύθυνση για τον λογιστικό χειρισμό των κρυπτονομισμάτων, ο οποίος βασίζεται κυρίως στους σκοπούς της επιχείρησης και στα πραγματικά γεγονότα. Τα κρυπτονομίσματα χαρακτηρίζονται ως απόθεμα, στην περίπτωση που η εμπορία τους εμπίπτει στις συνήθεις δραστηριότητες της επιχείρησης, και ως άυλο περιουσιακό στοιχείο στις υπόλοιπες περιπτώσεις κατοχής, και κυρίως στην διακράτηση ως επένδυση. Παρόλο που υπάρχει μία

[32] Procházka, D. (2018). Accounting for bitcoin and other cryptocurrencies under IFRS: A comparison and assessment of competing models. The International Journal of Digital Accounting Research,

[33] https://www.icaew.com/technical/tas-helpsheets/financial-reporting/accounting-for-cryptocurrencies-under-frs-102

προσπάθεια τα κρυπτονομίσματα να ενταχθούν σε μία μορφή κανονιστικού πλαισίου, θεωρούμε ότι θα πρέπει να υπάρξει ένα σαφές και συγκεκριμένο κανονιστικό πλαίσιο που να ρυθμίζει όλα τα θέματα που προκύπτουν από τον τρόπο λειτουργίας των κρυπτονομισμάτων. Αυτό θεωρούμε ότι είναι και η απαίτηση όσων θέλουν να επενδύσουν στην εν λόγω αγορά και επιθυμούν να υπάρξει κανονιστικό πλαίσιο για τα κρυπτονομίσματα που θα τα αποσυνδέει από οποιαδήποτε σχέση με παραβατικές πρακτικές (ξέπλυμα μαύρου χρήματος κλπ.)[34]. Στην συνέχεια θα δοθούν οι βασικές κατευθύνσεις και θα εξεταστούν όλες οι πιθανές περιπτώσεις περιουσιακών στοιχείων, στις οποίες θα μπορούσε να ενταχθεί το κρυπτονόμισμα.

3.2.1 Χρηματοοικονομικό Περιουσιακό Στοιχείο

Η κατοχή κρυπτονομισμάτων, εμφανώς, δεν αποτελεί συμμετοχή και δεν δημιουργεί κάποια συμβατική απαίτηση. Συνεπώς, 'τα χρηματικά διαθέσιμα και ισοδύναμα' είναι η μόνη κατηγορία κυκλοφορούντος ενεργητικού στην οποία θα μπορούσαν να ενταχθούν τα κρυπτονομίσματα. Το ΣΛΟΤ, παρόλα αυτά, θεωρεί ότι μία τέτοια κατηγοριοποίηση δεν συμβαδίζει με την ορθή λογιστική απεικόνιση, καθώς το κρυπτονόμισμα:

- Δεν εκδίδεται από κεντρική τράπεζα ή κράτος, με συνέπεια να μην απολαμβάνει τις σχετικές εγγυήσεις,
- Δεν είναι επένδυση υψηλής ρευστότητας,
- Δεν είναι άμεσα μετατρέψιμο σε γνωστά ποσά μετρητών και
- Υπόκειται σε σημαντικό κίνδυνο μεταβολής της αξίας του.

Παρόλα αυτά, η ίδια εγκύκλιος αναφέρει ότι «τα κρυπτονομίσματα χρησιμοποιούνται για την πληρωμή υποχρεώσεων από προμήθεια αγαθών ή υπηρεσιών, για την πληρωμή των εργαζόμενων και για επενδυτικούς σκοπούς». Συνεπώς, από τη στιγμή που αποτελούν μέσο πληρωμών, αποδεκτό μεταξύ των συναλλασσόμενων, διαδραματίζουν το ρόλο του χρήματος.

Κατά τη γνώμη μας, τα κρυπτονομίσματα αποτελούν 'επένδυση' υψηλής ρευστότητας διότι μπορούν να ανταλλαχθούν άμεσα για την αγορά περιουσιακών

[34] https://www.capital.gr/arthra/3590867/i-logistiki-kai-forologiki-metaxeirisi-ton-kruptonomismaton

στοιχείων και μπορούν να μετατραπούν εύκολα σε μετρητά μέσω αναγνωρισμένων ανταλλακτηρίων. Η έντονη μεταβλητότητα των τιμών των κρυπτονομισμάτων, η οποία οφείλεται στην αποκεντρωμένη και αναποτελεσματική από χρηματοοικονομικής άποψης αγοράς τους, δεν αποτελεί χαρακτηριστικό μόνο των κρυπτονομισμάτων αλλά και επίσημων νομισμάτων, τα οποία υφίστανται πληθωριστικές και κερδοσκοπικές πιέσεις στις διεθνείς αγορές.

Συνεπώς, ο σημαντικότερος ίσως παράγοντας είναι η αβεβαιότητα λόγω της αφερεγγυότητας των κρυπτονομισμάτων σε διεθνές επίπεδο. Η αβεβαιότητα αποτελεί ευρύτερη έννοια από τον κίνδυνο υποτίμησης, ο οποίος σε γενικές γραμμές είναι αποδεκτός από τους συναλλασσόμενους και πηγάζει από τις απαγορεύσεις κυκλοφορίας ή την επιβολή αυστηρού ρυθμιστικού πλαισίου για τα κρυπτονομίσματα.

3.2.2 Απόθεμα

Καταρχήν, η εγκύκλιος του ΣΛΟΤ αποδέχεται ότι δεν είναι απαραίτητο τα αποθέματα να έχουν φυσική υπόσταση. Έπειτα, οι οδηγίες προκαταλαμβάνουν ότι «τα κρυπτονομίσματα δεν μπορεί να αποτελούν αντικείμενο συχνών συναλλαγών, έτσι ώστε οι πωλήσεις κρυπτονομισμάτων να αντιπροσωπεύουν τη συνήθη δραστηριότητα της οικονομικής οντότητας». Παρόλα αυτά, ο χειρισμός ως απόθεμα θεωρείται πρόσφορος όταν η πώληση κρυπτονομισμάτων αντιπροσωπεύει τεκμηριωμένα τη συνήθη δραστηριότητα της επιχείρησης.

Σε αυτή την περίπτωση, προκύπτουν δύο καίρια ζητήματα. Πρώτον, πώς μπορεί να αποδείξει η εταιρεία ότι δραστηριοποιείται στην παραγωγή νομισμάτων τη στιγμή που δεν υπάρχει σχετικός Κωδικός Δραστηριότητας (ΚΑΔ). Δεύτερον, πώς πραγματοποιείται η αποτίμηση του αποθέματος κατά την απογραφή τέλους χρήσης. Βάσει των ΕΛΠ και των ΔΠΧΑ, η αποτίμηση των αποθεμάτων γίνεται στο κόστος (κόστος κτήσης μείον σωρευμένες ζημιές απομείωσης). Προβλέπεται όμως και η δυνατότητα αποτίμησης στο κόστος παραγωγής, ήτοι ενσωματωμένη ενέργεια και αποσβέσεις εξοπλισμού? Ο εν λόγω χειρισμός ενδέχεται να υποεκτιμά την πραγματική χρηματοοικονομική κατάσταση της εταιρείας εξαιτίας της μεγάλης διαφοράς μεταξύ κόστους παραγωγής και αγοραίας αξίας.

3.2.3 Άυλο περιουσιακό στοιχείο

Βάσει των οδηγιών του ΣΛΟΤ, το κρυπτονόμισμα μπορεί να αντιμετωπιστεί ως άυλο περιουσιακό στοιχείο, εφόσον έχει χαρακτηριστεί ως επενδυτικό προϊόν της επιχείρησης. Σε αυτή την περίπτωση, ο λογιστικός χειρισμός εξαρτάται από τα πρότυπα που εφαρμόζονται από την πλευρά της επιχείρησης. Πιο συγκεκριμένα στο πλαίσιο των Δ.Π.Χ.Α. μπορεί να αποτιμάται, είτε στο αποσβέσιμο κόστος (κόστος κτήσεως μείον σωρευμένες αποσβέσεις και ζημίες απομείωσης), είτε στην εύλογη αξία ενώ στο πλαίσιο των Ε.Λ.Π. αποτιμάται στο αποσβέσιμο κόστος.

Πάντως, η εγκύκλιος σημειώνει ότι «η αποτίμηση στην εύλογη αξία φαίνεται να είναι η πλέον κατάλληλη βάση αποτίμησης του κρυπτονομίσματος, επειδή αυτό χρησιμοποιείται ως ταμειακό υποκατάστατο ή ως εναλλακτικό επενδυτικό μέσο». Παρόλα αυτά, η αποτίμηση στην εύλογη αξία προϋποθέτει την ύπαρξη ενεργούς αγοράς. Βάσει των ΕΛΠ (ν. 4308/14 όπως ισχύει), «ενεργός αγορά (active market) είναι μια αγορά στην οποία λαμβάνουν χώρα συναλλαγές για ένα περιουσιακό στοιχείο ή μια υποχρέωση, με επαρκή συχνότητα και όγκο ώστε να παρέχουν πληροφορίες για τιμές σε συνεχή βάση». Συνεπώς, απαιτείται να προσδιοριστεί η έννοια της ενεργούς αγοράς κρυπτονομισμάτων, τη στιγμή που οι αγοραπωλησίες διενεργούνται από κατακερματισμένα ανταλλακτήρια σε διαφορετικές τιμές.

Η εγκύκλιος του ΣΛΟΤ (104/27.02.2018) παρέχει μία γενική κατεύθυνση για το λογιστικό χειρισμό των κρυπτονομισμάτων, ο οποίος βασίζεται κυρίως στους σκοπούς της επιχείρησης και στα πραγματικά γεγονότα. Συνοπτικά, τα κρυπτονομίσματα χαρακτηρίζονται ως απόθεμα, στην περίπτωση που η εμπορία τους εμπίπτει στις συνήθεις δραστηριότητες της επιχείρησης, και ως άυλο περιουσιακό στοιχείο στις υπόλοιπες περιπτώσεις κατοχής, και κυρίως στην διακράτηση ως επένδυση[35].

[35] https://www.taxexperts.gr/αρθρογραφία/κρυπτονομίσματα-λογιστικός-χειρισμός-της-παραγωγής-και-εμπορίας-τους

3.2.4 Εφαρμογή των Λογιστικών Προτύπων (ΔΛΠ-ΔΠΧΑ)

Αρχικά, μπορεί να φαίνεται ότι τα κρυπτονομίσματα θα πρέπει να λογιστικοποιούνται ως μετρητά, επειδή είναι μια μορφή ψηφιακού χρήματος. Ωστόσο, τα κρυπτονομίσματα δεν μπορούν να θεωρηθούν ισοδύναμα με μετρητά (νόμισμα) όπως ορίζεται στο ΔΛΠ 7 και στο ΔΛΠ 32, επειδή δεν μπορούν εύκολα να ανταλλαγούν με οποιοδήποτε αγαθό ή υπηρεσία. Αν και ένας αυξανόμενος αριθμός οντοτήτων δέχεται ψηφιακά νομίσματα ως πληρωμή, τα ψηφιακά νομίσματα δεν είναι ακόμη ευρέως αποδεκτά ως μέσο συναλλαγής και δεν αποτελούν νόμιμο χρήμα. Οι οντότητες μπορούν να επιλέξουν να αποδέχονται ψηφιακά νομίσματα ως μέσο πληρωμής, αλλά δεν υπάρχει απαίτηση να το κάνουν. Το ΔΛΠ 7 ορίζει τα ταμειακά ισοδύναμα ως "βραχυπρόθεσμες, υψηλής ρευστότητας επενδύσεις που είναι άμεσα μετατρέψιμες σε γνωστά ποσά μετρητών και οι οποίες υπόκεινται σε ασήμαντο κίνδυνο μεταβολών της αξίας τους". Συνεπώς, τα κρυπτονομίσματα δεν μπορούν να ταξινομηθούν ως ταμειακά ισοδύναμα επειδή υπόκεινται σε σημαντική μεταβλητότητα των τιμών τους. Ως εκ τούτου, δεν φαίνεται ότι τα ψηφιακά νομίσματα αντιπροσωπεύουν μετρητά ή ταμειακά ισοδύναμα που μπορούν να λογιστικοποιηθούν σύμφωνα με το ΔΛΠ 7.

Διαισθητικά, μπορεί να φαίνεται ότι τα κρυπτονομίσματα θα πρέπει να λογιστικοποιούνται ως χρηματοοικονομικά περιουσιακά στοιχεία στην εύλογη αξία μέσω των αποτελεσμάτων (FVTPL) σύμφωνα με το ΔΠΧΑ 9. Εντούτοις, δεν φαίνεται να πληροί τον ορισμό του χρηματοοικονομικού μέσου, διότι δεν αντιπροσωπεύει μετρητά, συμμετοχή σε μια οικονομική οντότητα ή σύμβαση που δημιουργεί δικαίωμα ή υποχρέωση να παραδώσει ή να λάβει μετρητά ή άλλο χρηματοοικονομικό μέσο. Το κρυπτονόμισμα δεν είναι χρεωστικός τίτλος, ούτε συμμετοχικός τίτλος (αν και ένα ψηφιακό περιουσιακό στοιχείο θα μπορούσε να έχει τη μορφή συμμετοχικού τίτλου) επειδή δεν αντιπροσωπεύει συμφέρον ιδιοκτησίας σε μια οικονομική οντότητα. Ως εκ τούτου, φαίνεται ότι το κρυπτονόμισμα δεν πρέπει να λογιστικοποιείται ως χρηματοοικονομικό περιουσιακό στοιχείο.

Ωστόσο, τα ψηφιακά νομίσματα φαίνεται να πληρούν τον ορισμό ενός άυλου περιουσιακού στοιχείου σύμφωνα με το ΔΛΠ 38, (άυλα περιουσιακά στοιχεία). Αυτό το πρότυπο ορίζει ένα άυλο περιουσιακό στοιχείο ως ένα αναγνωρίσιμο μη νομισματικό περιουσιακό στοιχείο χωρίς φυσική υπόσταση. Το ΔΛΠ 38 αναφέρει ότι ένα περιουσιακό στοιχείο είναι αναγνωρίσιμο εάν είναι διαχωρίσιμο ή προκύπτει από

συμβατικά ή άλλα νομικά δικαιώματα. Ένα περιουσιακό στοιχείο είναι διαχωρίσιμο εάν είναι ικανό να διαχωριστεί ή να διαιρεθεί από την οντότητα και να πωληθεί, μεταβιβαστεί, παραχωρηθεί, ενοικιαστεί ή ανταλλαγεί, είτε μεμονωμένα είτε μαζί με μια σχετική σύμβαση, ένα αναγνωρίσιμο περιουσιακό στοιχείο ή μια υποχρέωση. Αυτό αντιστοιχεί επίσης με το ΔΛΠ 21. Οι επιδράσεις των μεταβολών των συναλλαγματικών ισοτιμιών, το οποίο αναφέρει ότι ένα βασικό χαρακτηριστικό ενός μη νομισματικού περιουσιακού στοιχείου είναι η απουσία δικαιώματος λήψης (ή υποχρέωσης παράδοσης) ενός σταθερού ή προσδιορίσιμου αριθμού μονάδων νομίσματος. Έτσι, φαίνεται ότι το κρυπτονόμισμα πληροί τον ορισμό του άυλου περιουσιακού στοιχείου του ΔΛΠ 38, καθώς μπορεί να διαχωριστεί από τον κάτοχό του και να πωληθεί ή να μεταβιβαστεί μεμονωμένα και, σύμφωνα με το ΔΛΠ 21, δεν παρέχει στον κάτοχό του δικαίωμα να λάβει σταθερό ή προσδιορίσιμο αριθμό μονάδων νομισμάτων. Οι συμμετοχές σε κρυπτονομίσματα μπορούν να διαπραγματεύονται σε ένα χρηματιστήριο και επομένως, υπάρχει η προσδοκία ότι η οικονομική οντότητα θα λάβει εισροή οικονομικών ωφελειών. Όμως, το κρυπτονόμισμα υπόκειται σε μεγάλες διακυμάνσεις της αξίας του και ως εκ τούτου είναι μη νομισματικής φύσης. Τα κρυπτονομίσματα είναι μια μορφή ψηφιακού χρήματος και δεν έχουν φυσική υπόσταση οπότε, η καταλληλότερη ταξινόμηση τους είναι ως άυλο.

Επιπλέον, το ΔΛΠ 38 επιτρέπει την επιμέτρηση των άυλων περιουσιακών στοιχείων στο κόστος ή στην αναπροσαρμογή. Χρησιμοποιώντας το μοντέλο του κόστους, τα άυλα περιουσιακά στοιχεία επιμετρώνται στο κόστος κατά την αρχική αναγνώριση και μεταγενέστερα επιμετρούνται στο κόστος μείον συσσωρευμένες αποσβέσεις και ζημίες απομείωσης. Χρησιμοποιώντας το μοντέλο της αναπροσαρμογής, τα άυλα περιουσιακά στοιχεία μπορούν να αποτιμηθούν σε αναπροσαρμοσμένη αξία εάν υπάρχει ενεργός αγορά γι' αυτά αλλά, αυτό μπορεί να μην ισχύει για όλα τα κρυπτονομίσματα. Το ίδιο μοντέλο επιμέτρησης θα πρέπει να χρησιμοποιείται για όλα τα περιουσιακά στοιχεία μιας συγκεκριμένης κατηγορίας περιουσιακών στοιχείων. Εάν υπάρχουν περιουσιακά στοιχεία για τα οποία δεν υπάρχει ενεργός αγορά σε μια κατηγορία περιουσιακών στοιχείων που επιμετρώνται με το υπόδειγμα αναπροσαρμογής, τότε αυτά τα περιουσιακά στοιχεία θα πρέπει να επιμετρούνται με το υπόδειγμα κόστους.

Ακόμη, το ΔΛΠ 38 ορίζει ότι μια αύξηση αναπροσαρμογής θα πρέπει να αναγνωρίζεται στα λοιπά συνολικά έσοδα και να συσσωρεύεται στα ίδια κεφάλαια.

Ωστόσο, μια αύξηση αναπροσαρμογής θα πρέπει να αναγνωρίζεται στα αποτελέσματα στο βαθμό που αντιστρέφει μια μείωση αναπροσαρμογής του ίδιου περιουσιακού στοιχείου που είχε προηγουμένως αναγνωριστεί στα αποτελέσματα. Μια ζημία αναπροσαρμογής θα πρέπει να αναγνωρίζεται στα αποτελέσματα. Η μείωση θα πρέπει να αναγνωρίζεται στα λοιπά συνολικά έσοδα στην έκταση οποιουδήποτε πιστωτικού υπολοίπου στο πλεόνασμα αναπροσαρμογής σε σχέση με το εν λόγω περιουσιακό στοιχείο. Είναι ασυνήθιστο για τα άυλα περιουσιακά στοιχεία να έχουν ενεργές αγορές. Παρά ταύτα, τα κρυπτονομίσματα συχνά αποτελούν αντικείμενο διαπραγμάτευσης σε ένα χρηματιστήριο και, ως εκ τούτου, μπορεί να είναι δυνατή η εφαρμογή του μοντέλου αναπροσαρμογής.

Το μοντέλο αναπροσαρμογής μπορεί να εφαρμοστεί σύμφωνα με το ΔΠΧΑ 13, (επιμέτρηση εύλογης αξίας) και θα πρέπει να χρησιμοποιείται για τον προσδιορισμό της εύλογης αξίας του κρυπτονομίσματος. Το ΔΠΧΑ 13 ορίζει την ενεργό αγορά και πρέπει να εφαρμόζεται κρίση για να καθοριστεί εάν υπάρχει ενεργός αγορά για τα συγκεκριμένα κρυπτονομίσματα. Καθώς υπάρχει καθημερινή διαπραγμάτευση του Bitcoin, είναι εύκολο να αποδειχθεί ότι υπάρχει τέτοια αγορά. Μια χρηματιστηριακή τιμή σε ενεργό αγορά παρέχει την πιο αξιόπιστη απόδειξη της εύλογης αξίας και χρησιμοποιείται χωρίς προσαρμογή για την επιμέτρηση της εύλογης αξίας, όποτε είναι διαθέσιμη. Επιπλέον, η οντότητα θα πρέπει να προσδιορίσει την κύρια ή την πιο συμφέρουσα αγορά για τα κρυπτονομίσματα.

Η οικονομική οντότητα θα πρέπει επίσης, να εκτιμήσει εάν η ωφέλιμη ζωή του κρυπτονομίσματος είναι πεπερασμένη ή αόριστη. Αόριστη ωφέλιμη ζωή είναι όταν δεν υπάρχει προβλέψιμο όριο στην περίοδο κατά την οποία το περιουσιακό στοιχείο αναμένεται να δημιουργεί καθαρές ταμειακές εισροές για την οικονομική οντότητα. Φαίνεται ότι τα κρυπτονομίσματα θα πρέπει να θεωρούνται ότι έχουν απεριόριστη ωφέλιμη ζωή για τους σκοπούς του ΔΛΠ 38. Ένα άυλο περιουσιακό στοιχείο με απεριόριστη ωφέλιμη ζωή δεν αποσβένεται αλλά πρέπει να ελέγχεται ετησίως για απομείωση. Σε ορισμένες περιπτώσεις, και ανάλογα με το επιχειρηματικό μοντέλο μιας οικονομικής οντότητας, θα μπορούσε να είναι σκόπιμο να λογιστικοποιηθούν τα κρυπτονομίσματα σύμφωνα με το ΔΛΠ 2 (αποθέματα), επειδή το ΔΛΠ 2 εφαρμόζεται στα αποθέματα άυλων περιουσιακών στοιχείων. Το ΔΛΠ 2 ορίζει τα αποθέματα ως περιουσιακά στοιχεία:

- που κατέχονται προς πώληση κατά τη συνήθη πορεία της επιχείρησης
- κατά τη διαδικασία παραγωγής για την πώληση αυτή, ή
- με τη μορφή υλικών ή προμηθειών που πρόκειται να καταναλωθούν στην παραγωγική διαδικασία ή στην παροχή υπηρεσιών.

Για παράδειγμα, μια οντότητα μπορεί να κατέχει κρυπτονομίσματα προς πώληση στο πλαίσιο της συνήθους επιχειρηματικής δραστηριότητας και, εάν αυτό συμβαίνει, τότε τα κρυπτονομίσματα θα μπορούσαν να αντιμετωπίζονται ως αποθέματα. Κανονικά, αυτό θα σήμαινε την αναγνώριση των αποθεμάτων στη χαμηλότερη τιμή μεταξύ κόστους και καθαρής ρευστοποιήσιμης αξίας. Εάν όμως, η οικονομική οντότητα ενεργεί ως μεσίτης-διακινητής κρυπτονομισμάτων, τότε το ΔΛΠ 2 ορίζει ότι τα αποθέματά της θα πρέπει να αποτιμώνται στην εύλογη αξία μείον το κόστος πώλησης. Αυτού του είδους τα αποθέματα αποκτώνται κυρίως με σκοπό να πωληθούν στο εγγύς μέλλον και να προκύψει κέρδος από τις διακυμάνσεις της τιμής ή του περιθωρίου κέρδους των broker-traders. Κατ' ακολουθίαν, αυτή η μέθοδος αποτίμησης θα μπορούσε να εφαρμοστεί μόνο σε πολύ στενές περιπτώσεις όπου το επιχειρηματικό μοντέλο είναι η πώληση κρυπτονομισμάτων στο εγγύς μέλλον με σκοπό την επίτευξη κέρδους από τις διακυμάνσεις της τιμής.

Καθώς η αναγνώριση και η επιμέτρηση των κρυπτονομισμάτων εμπεριέχει τόσο μεγάλη κρίση και αβεβαιότητα, απαιτείται ορισμένη πληροφόρηση για την ενημέρωση των χρηστών κατά τη λήψη οικονομικών αποφάσεων. Το ΔΛΠ 1 (Παρουσίαση των οικονομικών καταστάσεων), απαιτεί από την οικονομική οντότητα να γνωστοποιεί τις κρίσεις που έχει κάνει η διοίκησή της σχετικά με τη λογιστική αντιμετώπιση της κατοχής περιουσιακών στοιχείων, στην προκειμένη περίπτωση εάν αυτές αποτελούν μέρος των κρίσεων που είχαν τη σημαντικότερη επίδραση στα ποσά που αναγνωρίζονται στις οικονομικές καταστάσεις. Επίσης, το ΔΛΠ 10, Γεγονότα μετά την περίοδο αναφοράς απαιτεί από την οικονομική οντότητα να γνωστοποιεί όλα τα σημαντικά μη διορθωτικά γεγονότα. Αυτό θα περιλάμβανε το κατά πόσον οι μεταβολές στην εύλογη αξία των κρυπτονομισμάτων μετά την περίοδο αναφοράς είναι τόσο σημαντικές ώστε η μη γνωστοποίηση θα μπορούσε να επηρεάσει τις οικονομικές αποφάσεις που λαμβάνουν οι χρήστες των οικονομικών καταστάσεων βάσει των οικονομικών καταστάσεων.

Έτσι, η λογιστική των κρυπτονομισμάτων δεν είναι τόσο απλή όσο φαίνεται αρχικά. Καθώς δεν υπάρχει επί του παρόντος κανένα πρότυπο ΔΠΧΑ που να μπορεί να εφαρμοστεί πλήρως για τα κρυπτονομίσματα και θα πρέπει να γίνει αναφορά στα υφιστάμενα λογιστικά πρότυπα[36].

3.2.5 Εφαρμογή των Λογιστικών Προτύπων (US GAAP)

Παρά την αυξημένη προσοχή που λαμβάνουν τα ψηφιακά περιουσιακά στοιχεία, η χρηματοοικονομική πληροφόρηση για αυτά τα περιουσιακά στοιχεία δεν εντάσσεται με σαφήνεια στις υφιστάμενες λογιστικές οδηγίες σύμφωνα με τις γενικά αποδεκτές λογιστικές αρχές των ΗΠΑ (GAAP). Ως αποτέλεσμα, πολλοί ορκωτοί λογιστές (CPAs) και λογιστικές εταιρείες ζήτησαν από το Συμβούλιο Λογιστικών Προτύπων (FASB) να αντιμετωπίσει αυτή την αυξανόμενη ανησυχία και να εξετάσει το ενδεχόμενο έκδοσης επικαιροποιημένων οδηγιών πιο προσαρμοσμένων σε αυτή τη νέα κατηγορία περιουσιακών στοιχείων. Τον Ιούνιο του 2021, το FASB εξέδωσε πρόσκληση υποβολής σχολίων, όπου τα ενδιαφερόμενα μέρη μπορούν να εκφράσουν τη γνώμη τους σχετικά με την επερχόμενη τεχνική ατζέντα του. Ενώ παραμένει ασαφές αν τα κρυπτονομίσματα και τα ψηφιακά περιουσιακά στοιχεία θα εμφανιστούν στην επίσημη ατζέντα του FASB. Παρακάτω παρατίθεται μια επισκόπηση της ισχύουσας σήμερα λογιστικής αντιμετώπισης όσον αφορά:

- Μεταβολές στην αξία

Δυστυχώς, δεν μπορείτε να λογιστικοποιήσετε ένα περιουσιακό στοιχείο κρυπτογράφησης χρησιμοποιώντας τα ίδια πρότυπα που ισχύουν για τα μετρητά ή τα ισοδύναμα μετρητών. Με την πρώτη ματιά, θα φαινόταν ο πιο προφανής τρόπος λογιστικής αντιμετώπισης των κρυπτονομισμάτων, αλλά δημιουργεί ορισμένα προβλήματα. Το πιο σημαντικό είναι ότι, σε αντίθεση με τα μετρητά ή ένα ισοδύναμο μετρητών, τα ψηφιακά περιουσιακά στοιχεία υφίστανται τακτικά σημαντικές

[36] https://www.accaglobal.com/in/en/student/exam-support-resources/professional-exams-study-resources/strategic-business-reporting/technical-articles/cryptocurrencies.html

διακυμάνσεις στην αξία τους. Τα μετρητά, ή ένα ισοδύναμο μετρητών, πρέπει εξ ορισμού να έχουν ασήμαντο κίνδυνο μεταβολής της εύλογης αξίας τους.

- Ως άυλο περιουσιακό στοιχείο

Ένα εναλλακτικό λογιστικό μοντέλο για τα ψηφιακά περιουσιακά στοιχεία είναι να ακολουθηθεί η καθοδήγηση για τα αποθέματα ή τα χρηματοοικονομικά μέσα. Ενώ αυτά παρουσιάζουν ορισμένα ελκυστικά χαρακτηριστικά, και πάλι δεν είναι τέλεια και εγείρουν ορισμένες προκλήσεις. Επί του παρόντος, οι δημόσιες εταιρείες πρέπει να λογιστικοποιούν ένα ψηφιακό νόμισμα ως άυλο περιουσιακό στοιχείο με απεριόριστη διάρκεια ζωής σύμφωνα με τα GAAP στις Ηνωμένες Πολιτείες και τα διεθνή πρότυπα χρηματοοικονομικής αναφοράς (ΔΠΧΑ) στο εξωτερικό. Και στις δύο περιπτώσεις, οι εταιρείες θα αναγνωρίζουν αρχικά τα κρυπτονομίσματα στον ισολογισμό στη βάση κόστους τους. Δεν υπάρχει ανάγκη απόσβεσής τους ως άυλο περιουσιακό στοιχείο με απεριόριστη διάρκεια ζωής, αλλά μάλλον πρέπει να αναγνωριστεί ζημία σε περίπτωση που το περιουσιακό στοιχείο απομειωθεί ποτέ. Τα κρυπτονομίσματα απομειώνονται κάθε φορά που η τιμή τους πέφτει κάτω από τη βάση κόστους, και λόγω της προαναφερθείσας μεταβλητότητάς τους, αυτό συμβαίνει αρκετά συχνά.

- Ως Καταγεγραμμένες ζημίες, όχι κέρδη

Δυστυχώς, στις Ηνωμένες Πολιτείες καταγράφονται μόνο οι μη πραγματοποιθείσες ζημίες και όχι τα κέρδη. Οι λογιστικοί κανόνες των GAAP για τα άυλα περιουσιακά στοιχεία δεν επιτρέπουν τη μεταγενέστερη αναστροφή μιας ζημίας απομείωσης, ακόμη και αν το περιουσιακό στοιχείο ανακτήσει ή ξεπεράσει τα προηγούμενα επίπεδα τιμών. Εάν η επιχείρησή σας αγοράσει Bitcoin αξίας 500.000 δολαρίων, και στη συνέχεια η εύλογη αξία του πέσει στα 400.000 δολάρια, θα πρέπει να αναγνωριστεί ζημία 100.000 δολαρίων και να μειώσει τις συμμετοχές σε Bitcoin για να αντανάκλαση τη μείωση της αξίας. Ακόμη και αν η αγοραία αξία αυξηθεί αργότερα σε 600.000 δολάρια, δεν επιτρέπεται να αντιστρέψετε τη ζημία ή να αυξήσετε την αξία του στον ισολογισμό. Παραμένει στην απομειωμένη αξία των 400.000 δολαρίων σύμφωνα με τα GAAP. Αυτή η λογιστική αντιμετώπιση δεν είναι μόνο δυσμενής για τις επιχειρήσεις που

επενδύουν σε εικονικό νόμισμα, αλλά έχει επίσης τη δυνατότητα να δημιουργήσει παραπλανητικές πληροφορίες για τους αναγνώστες των οικονομικών καταστάσεων.

Για παράδειγμα, η MicroStrategy Incorporated, επί του παρόντος η δημόσια εταιρεία με τις περισσότερες συμμετοχές σε Bitcoin, κατείχε 70.469 BTC στις 31 Δεκεμβρίου 2020. Οι συμμετοχές της είχαν εύλογη αγοραία αξία 2 δισεκατομμυρίων δολαρίων εκείνη τη στιγμή, αλλά ο ισολογισμός της έδειχνε μόνο 1,1 δισεκατομμύρια δολάρια στο τέλος του έτους, επειδή είχαν καταγραφεί μόνο μη πραγματοποιθείσες ζημίες. Αυτό δημιουργεί μια σαφή αναντιστοιχία μεταξύ της οικονομικής πραγματικότητας των συμμετοχών μιας εταιρείας και του τρόπου με τον οποίο τα λογιστικά πρότυπα αντικατοπτρίζουν αυτές τις συμμετοχές. Αυτά τα ζητήματα είναι οι κύριοι λόγοι για τους οποίους τόσοι πολλοί ζητούν από το FASB να εκδώσει νέα πρότυπα ειδικά για το κρυπτονόμισμα και άλλα ψηφιακά περιουσιακά στοιχεία.

3.2.6 Παραδείγματα Λογιστικής Μεταχείρισης Κρυπτονομισμάτων Σύμφωνα με τα (US GAAP)

Ερώτημα 1: Πώς θα πρέπει η επιχείρησή σας να καταγράφει τα κρυπτονομίσματα και άλλα ψηφιακά περιουσιακά στοιχεία στο λογιστικό της βιβλίο;

Ενώ οι συναλλαγές με κρυπτονομίσματα παρουσιάζουν πολλές μοναδικές επιπλοκές, εξακολουθούν να αποτελούν περιουσιακό στοιχείο και ισχύουν οι θεμελιώδεις λογιστικές αρχές.

Όταν η επιχείρησή σας αγοράζει κρυπτονόμισμα, θα πρέπει να αναγνωρίζετε το περιουσιακό στοιχείο στον ισολογισμό σας στην εύλογη αγοραία αξία του κατά την ημερομηνία αγοράς. Αυτό γίνεται με την καταγραφή μιας χρέωσης στο λογαριασμό του περιουσιακού στοιχείου. Αν υποθέσουμε ότι η επιχείρησή σας αγόρασε το εικονικό νόμισμα χρησιμοποιώντας νόμισμα Fiat, θα πιστώνατε τον λογαριασμό μετρητών σας με το ίδιο ποσό.

Όταν η επιχείρησή σας πουλήσει αργότερα το περιουσιακό στοιχείο, κάνετε το αντίθετο. Πιστώνετε το περιουσιακό στοιχείο για να το αφαιρέσετε από τον ισολογισμό σας στη λογιστική του αξία, και χρεώνετε τα μετρητά σας με το ποσό των εσόδων σας

ή άλλου ανταλλάγματος που λάβατε. Επειδή τα έσοδα θα μπορούσαν να είναι πολύ υψηλότερα από την τρέχουσα λογιστική αξία του περιουσιακού στοιχείου -είτε λόγω απομείωσης, είτε λόγω ανατίμησης, είτε λόγω και των δύο- θα μπορούσαν επίσης να αναγνωρίσουν πίστωση σε λογαριασμό κεφαλαιακού κέρδους που να αντανακλά τη διαφορά μεταξύ της λογιστικής αξίας και των εισπραχθέντων εσόδων.

Ερώτημα 2: Πώς πρέπει να καταγράψει η επιχείρησή σας τις πληρωμές προς τους προμηθευτές της;

Όταν χρησιμοποιείτε κρυπτονόμισμα για να πληρώσετε έναν πωλητή, πρέπει να καταγράψετε τη συναλλαγή με τον ίδιο τρόπο όπως αν είχατε αποφασίσει να το πουλήσετε. Είτε έτσι είτε αλλιώς, λογίζεται ως διάθεση, οπότε θα αναγνωρίσετε κεφαλαιακό κέρδος για τη διαφορά μεταξύ της δαπάνης και της λογιστικής αξίας του ψηφιακού περιουσιακού στοιχείου.

Φανταστείτε ότι έχετε 100 BTC στον ισολογισμό σας με αξία $300.000. Από τότε που αποκτήσατε το νόμισμα, η δίκαιη αξία του έχει αυξηθεί σε 400.000 δολάρια. Η επιχείρησή σας πληρώνει στην εταιρεία CPA που είναι υπεύθυνη για τον έλεγχό σας 400.000 δολάρια χρησιμοποιώντας το άυλο περιουσιακό στοιχείο ως μέσο πληρωμής αντί για μετρητά. Θα καταγράφατε μια χρέωση 400.000 δολαρίων στον λογαριασμό εξόδων επαγγελματικών υπηρεσιών, θα πιστώνατε τον λογαριασμό περιουσιακών στοιχείων Bitcoin για 300.000 δολάρια και θα πιστώνατε το υπόλοιπο 100.000 δολάρια σε έναν λογαριασμό κεφαλαιακών κερδών.

Σημειώστε, εάν η εύλογη αξία του περιουσιακού στοιχείου μειωθεί σε 200.000 δολάρια σε κάποιο σημείο ενώ βρίσκεται στον ισολογισμό σας, πριν ανακτήσει την τρέχουσα αξία του ύψους 400.000 δολαρίων, πιθανότατα δεν θα υπήρχε κεφαλαιακή ζημία κατά τη διάθεση, επειδή έχετε ήδη καταγράψει απομείωση όταν συνέβη η μείωση της αξίας. Σε αυτό το σενάριο, στην πραγματικότητα θα πιστώνατε ένα ακόμη πιο σημαντικό κεφαλαιακό κέρδος ύψους 200.000 δολαρίων για να υπολογίσετε τη διαφορά μεταξύ της λογιστικής αξίας του περιουσιακού στοιχείου ύψους 200.000 δολαρίων και της δαπάνης 400.000 δολαρίων και της τρέχουσας εύλογης αξίας.

Ερώτημα 3: Πώς αντιμετωπίζεται η διαπραγμάτευση ψηφιακών περιουσιακών στοιχείων στο λογιστικό σας βιβλίο;

Θα πρέπει να καταγράφετε τις δραστηριότητες διαπραγμάτευσης κρυπτονομισμάτων σας παρόμοια με τον τρόπο που θα καταγράφατε τις συναλλαγές σε μετοχές. Όταν αγοράζετε ένα κρυπτογραφικό περιουσιακό στοιχείο με τη χρήση Fiat currency, καταχωρίστε την επένδυση στα βιβλία σας με πίστωση του λογαριασμού μετρητών σας και χρέωση του λογαριασμού του νεοαποκτηθέντος κρυπτογραφικού περιουσιακού στοιχείου. Θα πρέπει να κάνετε τις απαραίτητες ημερολογιακές εγγραφές για να λογιστικοποιήσετε τυχόν απομειώσεις καθώς προκύπτουν, χρεώνοντας τον λογαριασμό ζημιών σας και πιστώνοντας τον λογαριασμό περιουσιακών στοιχείων σας.

Όταν διαθέτετε την επένδυση κρυπτογράφησης, διαγράψτε το περιουσιακό στοιχείο από τα βιβλία σας με πίστωση του λογαριασμού του περιουσιακού στοιχείου στη λογιστική του αξία και χρέωση του λογαριασμού που αντιπροσωπεύει το αντίτιμο που λάβατε ως αντάλλαγμα για την ανταλλαγή του ψηφιακού σας περιουσιακού στοιχείου.

Εάν πουλήσατε το κρυπτονόμισμα σας για νόμισμα Fiat, χρεώστε τον λογαριασμό μετρητών σας. Αν το ανταλλάξατε με ένα άλλο ψηφιακό περιουσιακό στοιχείο, χρεώστε τον νέο λογαριασμό κρυπτογράφησης. Στη συνέχεια, βάλτε τη διαφορά σε έναν λογαριασμό κεφαλαιακού κέρδους ή ζημίας για να εξισορροπήσετε τη συναλλαγή ανάλογα με τις ανάγκες.

Ερώτημα 4: Πώς πρέπει να καταγράφει η επιχείρησή όσον αφορά τις δραστηριότητες εξόρυξης κρυπτογράφησης;

Η εξόρυξη αποτελεί θεμελιώδες συστατικό της τεχνολογίας Blockchain και φέρνει σε κυκλοφορία νέα ψηφιακά περιουσιακά στοιχεία. Εάν η επιχείρησή σας ασχολείται με δραστηριότητες εξόρυξης, αυτές θα πρέπει να εμφανίζονται στο λογιστικό σας βιβλίο, όπως κάθε άλλη δραστηριότητα που δημιουργεί εισόδημα. Θα πιστώσετε τον λογαριασμό εσόδων εξόρυξης και θα χρεώσετε το νέο δημιουργηθέν περιουσιακό στοιχείο κρυπτονομίσματος στα βιβλία σας στην εύλογη αγοραία αξία του. Επειδή

αναπόφευκτα θα προκύψουν έξοδα κατά τη διαδικασία, θα πρέπει να τα λογιστικοποιήσετε και αυτά.

Υποθέτοντας ότι χρησιμοποιείτε μετρητά για να πληρώσετε για αυτές τις δραστηριότητες, θα πιστώσετε τον λογαριασμό μετρητών και θα χρεώσετε είτε ένα περιουσιακό στοιχείο -εάν αγοράζετε εξοπλισμό εξόρυξης που πρέπει να κεφαλαιοποιηθεί και στη συνέχεια να αποσβεστεί- είτε ένα έξοδο για πράγματα όπως οι υπηρεσίες κοινής ωφέλειας και οι προμήθειες. Σε γενικές γραμμές, οποιαδήποτε έσοδα από τις εξορυκτικές σας δραστηριότητες θα πρέπει να αναγνωρίζονται ως έσοδα τη στιγμή που τα έσοδα αποκτώνται[37].

Ερώτημα 5: Απόκτηση σε συνένωση επιχειρήσεων ή απόκτηση περιουσιακών στοιχείων

Ένα άυλο περιουσιακό στοιχείο κρυπτογράφησης που αποκτάται σε μια συνένωση επιχειρήσεων αναγνωρίζεται και επιμετράται με τον ίδιο τρόπο όπως κάθε άλλο περιουσιακό στοιχείο που αποκτάται σε μια συνένωση επιχειρήσεων σύμφωνα με το θέμα (Συνενώσεις επιχειρήσεων). Αυτό σημαίνει ότι ένα κρυπτογραφικό άυλο περιουσιακό στοιχείο που αποκτάται σε μια συνένωση επιχειρήσεων επιμετράται στην εύλογη αξία.

Αντίθετα, ένα άυλο περιουσιακό στοιχείο κρυπτογράφησης που αποκτάται σε μια απόκτηση περιουσιακών στοιχείων αναγνωρίζεται και επιμετράται με τον ίδιο τρόπο όπως ένα περιουσιακό στοιχείο κρυπτογράφησης που αποκτάται με μετρητά. Ωστόσο, επειδή μια οικονομική οντότητα δεν αναγνωρίζει υπεραξία ή κέρδος από αγορά σε τιμή ευκαιρίας σε μια απόκτηση περιουσιακών στοιχείων, το ποσό που καταχωρείται για ένα αποκτώμενο κρυπτογραφικό περιουσιακό στοιχείο μπορεί, μαζί με άλλα αποκτώμενα περιουσιακά στοιχεία, να προσαρμοστεί στη σχετική εύλογη αξία του.

Συνεπώς, επειδή δεν υπάρχουν ρητά US GAAP για τα κρυπτογραφημένα περιουσιακά στοιχεία, η παρουσίαση και η γνωστοποίηση των κρυπτογραφημένων περιουσιακών στοιχείων και των συναλλαγών κρυπτογραφημένων περιουσιακών

[37] https://taxbit.com/blog/a-quick-guide-to-accounting-for-cryptocurrency

στοιχείων θα πρέπει να ακολουθεί το συμπέρασμα της οντότητας σχετικά με το λογιστικό μοντέλο που θα εφαρμοστεί στο κρυπτογραφημένο περιουσιακό στοιχείο, δηλαδή ως άυλο περιουσιακό στοιχείο ή ως χρηματοοικονομικό περιουσιακό στοιχείο[38].

3.3 Φορολογική Μεταχείριση των Κρυπτονομισμάτων

Τα τελευταία χρόνια έχει αυξηθεί η χρήση των κρυπτονομισμάτων, είτε ως μέσο πληρωμής είτε ως επενδυτικό αγαθό. Ιδιώτες επενδυτές αλλά και νομικές οντότητες αποκτούν κρυπτονομίσματα προσβλέποντας στο άμεσο ή μελλοντικό κέρδος. Ο νόμος δεν απαγορεύει τη χρήση των κρυπτονομισμάτων, όπως και δεν υπάρχει έως τώρα στην Ελληνική Φορολογική Νομοθεσία συγκεκριμένο φορολογικό καθεστώς που να διέπει τα κέρδη που αποκτούν οι φορολογούμενοι από υπεραξία πώλησης κρυπτονομισμάτων. Ωστόσο, η έλλειψη ρητών φορολογικών διατάξεων δεν αποτελεί άλλοθι προκειμένου να μη δηλωθούν και φορολογηθούν τα παραπάνω κέρδη, τα οποία θα πρέπει να θεωρηθούν από τον κάθε αποκτώντα επενδυτή ως φορολογητέο εισόδημα. Οι βασικές κατηγορίες εισοδημάτων από κρυπτονομίσματα είναι:

- Η αγορά τους ως επενδυτικό αγαθό, είτε από φυσικά είτε από νομικά πρόσωπα.
- Αυτών που τα παράγουν (miners) με σκοπό την πώλησή τους.

Η Ανεξάρτητη Αρχή Δημοσίων Εσόδων, στο επιχειρησιακό της σχέδιο το 2019, κάνει μία πρώτη προσέγγιση αντιμετωπίζοντας τη θεσμοθέτηση της φορολόγησης των κρυπτονομισμάτων ως επένδυση χαρτοφυλακίου.

Με δεδομένη την πρόθεση της ΑΑΔΕ και ελλείψει ρητών νομοθετικών διατάξεων, θεωρούμε ότι τα παραπάνω εισοδήματα είναι κέρδη από υπεραξία μεταβίβασης κεφαλαίου και θα φορολογηθούν σύμφωνα με το άρθρο 43 του ΚΦΕ με συντελεστή 15%. Αξίζει να σημειωθεί ότι τα εισοδήματα αυτά υπόκεινται και σε εισφορά αλληλεγγύης. Με τις παραγράφους 3 και 4 του άρθρου 42 του Νόμου 4172, προσδιορίζεται η υπεραξία (Καθαρή αξία πώλησης - Κόστος αγοράς) που αποκτά φυσικό πρόσωπο, η οποία προκύπτει από τη διαφορά μεταξύ της τιμής πώλησης που εισέπραξε κατά την πώληση και την τιμή κτήσης που κατέβαλε ο φορολογούμενος -

[38] https://frv.kpmg.us/reference-library/2022/crypto-asset-executive-summary.html

επενδυτής για αγορά. Δαπάνες που συνδέονται άμεσα με την αγορά ή την πώληση των κρυπτονομισμάτων συμπεριλαμβάνονται στην αξία κτήσης ή πώλησης, επομένως έξοδα προμήθειας των ψηφιακών πλατφορμών στα οποία γίνονται οι αγοραπωλησίες διαμορφώνουν το τελικό αποτέλεσμα με το οποίο θα φορολογηθεί.

Στην περίπτωση νομικών προσώπων που έχουν αγοράσει ως επενδυτικό προϊόν κρυπτονομίσματα και στο μέλλον τα ρευστοποιήσουν, η τυχόν υπεραξία - κέρδος που θα προκύψει, θα φορολογηθεί με τις γενικές διατάξεις φορολογίας νομικών προσώπων και τον ισχύον φορολογικό συντελεστή κατά την υποβολή της φορολογικής δήλωσης. Παρακάτω θα δούμε μερικά παραδείγματα:

Παράδειγμα 1^0

Αν φυσικό πρόσωπο αγοράσει κρυπτονομίσματα αξίας 2.000 ευρώ και καταβάλει δαπάνες που συνδέονται άμεσα με την αγορά τους (π.χ. προμήθεια ανταλλακτηρίου) 20 ευρώ και στη συνέχεια πουλήσει τα άνω κρυπτονομίσματα 2.500 ευρώ κα ταυτόχρονα θα επιβαρυνθεί με δαπάνες ύψους 30 ευρώ, το τελικό ποσό της υπεραξίας επί του οποίου οφείλεται φόρος 15% ανέρχεται στο ποσό των 450 ευρώ (2.000+20 =2.020) Κόστος κτήσης, (2.500-30 = 2470) Καθαρή αξία πώλησης.

Εάν το φυσικό πρόσωπο έχει προβεί σε διαδοχικές αποκτήσεις κρυπτονομισμάτων και στη συνέχεια πωλήσει το σύνολο ή μέρος αυτών, ως τιμή κτήσης των πωλούμενων κρυπτονομισμάτων λαμβάνεται η μέση τιμή κτήσης που προκύπτει από τη συνολική αξία κτήσης των κρυπτονομισμάτων δια της ποσότητας αυτών. (πολ. 1032/2015 και πολ.1082/2018).

Παράδειγμα 2^0

Αν φυσικό πρόσωπο είχε κάνει διαδοχικές αγορές Bitcoin το έτος 2020, σύμφωνα με τον παρακάτω πίνακα:

Πίνακας 3.3: Αγορές Bitcoin

ΜΗΝΑΣ ΑΓΟΡΑ	ΤΙΜΗ BITCOIN €	ΠΟΣΟ ΑΓΟΡΑΣ €	ΠΟΣΟΤΗΤΑ BITCOIN	ΕΞΟΔΑ	ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΚΤΗΣΗΣ
ΑΠΡΙΛΙΟΣ	7.000,00	1.400,00	0,2	10,00€	1.410,00€
ΜΑΪΟΣ	10.000,00	3.000,00	0,3	30,00€	3.030,00€
ΝΟΕΜΒΡΙΟΣ	15.000,00	3.000,00	0,2	30,00€	3.030,00€
ΣΥΝΟΛΑ			**0,7**		**7.470,00€**

Ο επενδυτής έχει δαπανήσει 7.470,00 για να αποκτήσει 0,7 ενός Bitcoin. Άρα η μέση τιμή κτήσης των κρυπτονομισμάτων που αγόρασε είναι: 7.470,00 / 0,7 = **10.671,43.** Τον Δεκέμβριο, όπου η τιμή του Bitcoin ήταν 28.000,00 €, πουλάει 0,5 από τα Bitcoin που κατέχει και εισπράττει (14.000€ μείον 50 € έξοδα) 13.950 €.

Πίνακας 3.4: Πώληση Bitcoin

ΜΗΝΑΣ	ΤΙΜΗ BITCOIN	ΠΩΛΗΣΗΣ BITCOIN	ΠΟΣΟ ΠΩΛΗΣΗΣ	ΕΞΟΔΑ ΠΩΛΗΣΗΣ	ΜΕΣΗ ΤΙΜΗ ΚΤΗΣΗΣ	ΥΠΕΡΑΞΙΑ
					(0,5 χ 10.671,43)	(13.950-5.335,72)
ΔΕΚΕΜΒΡΙΟΣ	28.000,00	0,5	14.000,00	50,00€	5.335,72	**8.614,28**

Η υπεραξία που θα φορολογηθεί με συντελεστή 15% του 8.614,28. Ως χρόνος φορολόγησης των κερδών της υπεραξίας λαμβάνεται ο χρόνος πώλησης των κρυπτονομισμάτων και όχι η μεταφορά των κερδών προς τους τραπεζικούς λογαριασμούς. Π.χ. εάν πραγματοποιήθηκε μία πώληση με κέρδος τον Δεκέμβριο του 2020, το κέρδος αυτό θα φορολογηθεί με την υποβολή της δήλωσης του 2020, ανεξάρτητα εάν αυτά παραμένουν στην ψηφιακή πλατφόρμα και μεταφερθούν στον τραπεζικό λογαριασμό του επενδυτή σε μεταγενέστερο χρόνο, είτε συνολικά είτε με διαδοχικά εμβάσματα.

3.3.1 Τεκμήρια - κάλυψη - κωδικοί

Ιδιαίτερη προσοχή πρέπει να δίνεται στα ποσά που καταβάλλονται για την απόκτηση των κρυπτονομισμάτων τα οποία αποτελούν τεκμήριο και θα πρέπει να δικαιολογούνται. Τα ποσά αυτά θα αναγραφούν στον κωδικό 743 του πίνακα 5 του εντύπου Ε1 της φορολογικής δήλωσης το έτος αγοράς τους. Σε περίπτωση πώλησης, το ποσό του κεφαλαίου που εισπράχθηκε μειωμένο με τα έξοδα συναλλαγής, θα αναγραφεί στον κωδικό 781 του πίνακα 6 του εντύπου Ε1 της φορολογικής δήλωσης, στο έτος της πώλησής τους. Όσον αφορά τυχόν υπεραξία που προκύψει από την πώληση των κρυπτονομισμάτων, θα αναγραφεί στον κωδικό 865 του πίνακα 4 Ε του εντύπου Ε1 της φορολογικής δήλωσης (κέρδος από μεταβίβαση τίτλων αλλοδαπής). Σημαντικό είναι ότι εάν προκύψει ζημία από την πώληση των κρυπτονομισμάτων, μπορεί να συμψηφιστεί με μελλοντικά κέρδη από την ίδια κατηγορία εισοδήματος μέσα στα επόμενα 5 έτη (πολ.1032/2015). Σε αυτή την περίπτωση συμπληρώνεται ο κωδικός 871 του εντύπου Ε1 της φορολογικής δήλωσης.

Ο φορολογούμενος πρέπει να τηρεί αναλυτικές καταστάσεις συνοδευόμενες από τα παραστατικά έγγραφα της ψηφιακής πλατφόρμας που έγιναν οι αγοραπωλησίες και να είναι σε θέση να αποδείξει πώς προκύπτουν τα ποσά που συμπληρώθηκαν στους κωδικούς της φορολογικής δήλωσης. Να σημειωθεί ότι οι ψηφιακές πλατφόρμες αγοραπωλησίας κρυπτονομισμάτων κατέχουν τα προσωπικά στοιχεία του κάθε συναλλασσόμενου και δεν προσφέρουν ανωνυμία.

Επίσης ιδιαίτερη προσοχή πρέπει να δίνεται στα εισερχόμενα εμβάσματα στους τραπεζικούς λογαριασμούς από τις ψηφιακές πλατφόρμες, τα οποία είναι προϊόν ρευστοποίησης των κρυπτονομισμάτων. Τα ποσά αυτά για να μπορέσουν να δικαιολογηθούν φορολογικά θα πρέπει να έχουν δηλωθεί κατά την πώλησή τους.

3.3.2 Φορολογία παραγωγού κρυπτονομισμάτων (Miner)

Δυστυχώς και στην περίπτωση του παραγωγού κρυπτονομισμάτων δεν υπάρχουν έως τώρα φορολογικοί και λογιστικοί κανόνες που να δίνουν κατευθύνσεις, πλην μιας γνωμοδότησης του Σ.ΛΟ.Τ. με αριθμό 104/27.02.2018. Ο κάθε παραγωγός που ασχολείται με το συγκεκριμένο αντικείμενο με σκοπό την πραγματοποίηση εσόδων

από πώληση, πρέπει να προσεγγίσει το θέμα προσεκτικά και πάντα με γνώμονα ότι οποιοδήποτε κέρδος αποκομίζεται, αποτελεί φορολογητέο εισόδημα από εμπορικές επιχειρήσεις.

Το φορολογητέο εισόδημα του παραγωγού κρυπτονομισμάτων θα εξευρεθεί από τα συνολικά έσοδα που πραγματοποιεί από την πώληση των κρυπτονομισμάτων, αφαιρώντας όλα τα λειτουργικά έξοδα που μπορεί να έχει η εν λόγω επιχείρηση, π.χ. λογαριασμοί ΔΕΚΟ, ενοίκια, αποσβέσεις πάγιου εξοπλισμού, ηλεκτρονικών υπολογιστών, λοιπών μηχανημάτων. Κατόπιν θα φορολογηθεί με τους ισχύοντες φορολογικούς συντελεστές. Τέλος, δεδομένης της εξαιρετικά μεγάλης διάστασης που έχει πάρει η συναλλαγή μέσω κρυπτονομισμάτων θεωρούμε βέβαιο ότι θα υπάρξει μια ενιαία διεθνής προσέγγιση για το πώς θα αντιμετωπίζεται από τις φορολογικές αρχές[39].

[39] https://www.euro2day.gr/investments/crypto/article/2072143/pos-forologoyntai-ta-kryptonomismata-sthn-ellada.html

ΚΕΦΑΛΑΙΟ 4

ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Τα κρυπτονομίσματα είναι μια ενδιαφέρουσα χρηματοοικονομική καινοτομία και προσφέρουν πολλούς πιθανούς ερευνητικούς δρόμους. Όπως συμβαίνει με πολλές νέες τεχνολογίες, υπάρχει σημαντική σύγχυση τόσο για την υποκείμενη έννοια των κρυπτονομισμάτων όσο και τις προσεγγίσεις για την λογιστική αντιμετώπισή τους. Ο πρώτος στόχος αυτού του έγγραφου ήταν να δοθεί μια υψηλού επιπέδου ερμηνεία του όρου κρυπτονομίσματος και της κρυπτογραφίας που συνδέεται άμεσα με την τεχνολογία blockchain. Στη συνέχεια ο δεύτερος στόχος ήταν να γίνει η περιγραφή των χαρακτηριστικών του Bitcoin και ο τρόπος με τον οποίο δημιουργούνται οι συναλλαγές του, καθώς και ο τρόπος με τον οποίο επιτυγχάνεται η τεχνολογία της εξόρυξης. Στο τέλος της παρούσας εργασίας διερευνήθηκε η δυσκολία που αντιμετωπίζουν τα φυσικά, νομικά αλλά και τα χρηματοπιστωτικά ιδρύματα όσον αφορά την λογιστική και τη φορολογική αντιμετώπιση των κρυπτονομισμάτων. Τα συμπεράσματα στα οποία κατέληξε είναι τα εξής.

Τα κρυπτονομίσματα αποτελούν μια εξαιρετική τεχνολογική καινοτομία της δεκαετίας. Στον πυρήνα τους, τα κρυπτονομίσματα αποτελούν μια διαταραχή του χρήματος. Αποσυνδέουν το χρήμα από την κρατική εξουσία μέσω της αποκέντρωσης και αποσυνδέουν το χρήμα από την κοινωνική εμπιστοσύνη μέσω της διαφάνειας. Ωστόσο, η αλυσίδα μπλοκ είναι αυτή στην οποία μπορεί να τρέξει ένα κρυπτονόμισμα και το πεδίο εφαρμογής της είναι πολύ ευρύτερο από αυτό των κρυπτονομισμάτων.

Η τεχνολογία Blockchain είναι χρήσιμη και ευέλικτη για τον κόσμο μας, επειδή έλυσε ορισμένα από τα προβλήματα του κεντρικού συστήματος, όπως οι συναλλαγές χωρίς μεσάζοντα, ο χρόνος που δαπανάται για κάθε συναλλαγή, η ακούσια ή ειδική διαγραφή κ.τ.λ. Με τα πλεονεκτήματα της τεχνολογίας, όπως η διαφάνεια, η αξιοπιστία, η πολλαπλή αντιγραφή των συναλλαγών και το αποκεντρωμένο ψηφιακό βιβλίο, η τεχνολογία Blockchain είναι αξιόπιστη και μη καταστρέψιμη. Συνεπώς, η

εφεύρεση της αλυσίδας μπλοκ μπορεί να θεωρηθεί ότι αποτελεί ένα ζωτικής σημασίας και πολύ αναγκαίο πρόσθετο στοιχείο του διαδικτύου, το οποίο στερούνταν ασφάλειας και εμπιστοσύνης. Επιπλέον, η τεχνολογία Blockchain μας υπόσχεται ένα λαμπρό μέλλον χωρίς απάτες και εξαπατήσεις λόγω των πλεονεκτημάτων της τεχνολογίας της. Επιπροσθέτως, η αλυσίδα μπλοκ μπορεί να εφαρμοστεί σε μια μεγάλη ποικιλία τομέων (π.χ. εμπόριο, εμπορικές συναλλαγές, υγειονομική περίθαλψη, διακυβέρνηση, κτλ.).

Από την άλλη πλευρά, η πρόθεση των δημιουργών του Bitcoin ήταν να αναπτύξουν μια αποκεντρωμένη ηλεκτρονική πληρωμή που να μοιάζει με μετρητά. Κατά τη διαδικασία αυτή, αντιμετώπισαν τη θεμελιώδη πρόκληση του τρόπου θέσπισης και μεταβίβασης των ψηφιακών δικαιωμάτων ιδιοκτησίας μιας νομισματικής μονάδας χωρίς κεντρική αρχή. Έλυσαν αυτή την πρόκληση εφευρίσκοντας την αλυσίδα μπλοκ Bitcoin. Αυτή η νέα τεχνολογία μας επιτρέπει να αποθηκεύουμε και να μεταφέρουμε μια νομισματική μονάδα χωρίς την ανάγκη ύπαρξης κεντρικής αρχής. Η αστάθεια όμως των τιμών και τα ζητήματα κλιμάκωσης εγείρουν συχνά ανησυχίες σχετικά με την καταλληλότητα του Bitcoin ως μέσο πληρωμής. Αυτό μπορεί να οδηγήσει στη δημιουργία μιας νέας κατηγορίας περιουσιακών στοιχείων που μπορεί να ωριμάσει σε ένα πολύτιμο μέσο διαφοροποίησης χαρτοφυλακίου.

Τώρα όσον αφορά τον λογιστικό χειρισμό των κρυπτονομισμάτων επί του παρόντος, ούτε τα ΔΠΧΑ ούτε τα UK GAAP κάνουν ειδική αναφορά στη λογιστική των κρυπτονομισμάτων (τα οποία αποτελούν υποσύνολο των κρυπτογραφημένων περιουσιακών στοιχείων), τα οποία περιλαμβάνουν το Bitcoin, το Ethereum και το Ripple, καθώς και μια σειρά από νεότερα κρυπτονομίσματα που κυκλοφορούν με ταχείς ρυθμούς. Σκοπός του παρόντος βοηθητικού φύλλου είναι να εξετάσει τόσο τους πιθανούς λογιστικούς χειρισμούς βάσει του IFRS και UK GAAP όσο και την παρουσίαση των κρυπτονομισμάτων εντός των οικονομικών καταστάσεων. Θα πρέπει να σημειωθεί ότι πρόκειται ακόμη για έναν αναδυόμενο τομέα και η πρακτική θα εξελιχθεί αναμφίβολα με την πάροδο του χρόνου.

Κλείνοντας, θα γίνει μια σύντομη αναφορά στις πιθανές επεκτάσεις που μπορεί να λάβει η μελέτη αυτή. Αρχικά να τονιστεί ότι υπάρχουν πολλά που πρέπει να γίνουν σε αυτό το νέο πεδίο της οικονομίας. Πρώτα τα από όλα θεωρούμε ότι πρέπει, έστω και καθυστερημένα, η εγκύκλιος του ΣΛΟΤ να παρέχει μία γενική κατεύθυνση για τον λογιστικό χειρισμό των κρυπτονομισμάτων. Δεύτερον να θεσπιστούν κανόνες

αδειοδότησης και εποπτείας των παραγωγών και εμπόρων κρυπτονομισμάτων και τρίτον να δοθεί ο φορολογικός χειρισμός των κερδών και ζημιών σε επίπεδο φυσικών και νομικών προσώπων. Επιπροσθέτως, μια άλλη σημαντική πρόταση για διερεύνηση είναι κατά πόσο η άνοδος ή η κάθοδος των κρυπτονομισμάτων θα μπορούσε να επηρεάσει την παγκόσμια οικονομία. Τέλος, μια άλλη πρόταση για μελλοντική έρευνα είναι, για το πως η χρήση της τεχνολογία Blockchain θα μπορούσε να βοηθήσει στην αντιμετώπιση της φοροδιαφυγής.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Bholane, K. P. (2021). "Pros and Cons of Cryptocurrency: A Brief Overview". *National Journal of Research in Marketing, Finance & HRM, 6*(3), 71-78.
2. Milutinović, M. (2018). "Cryptocurrency". *Ekonomika, 64*(1), 105-122.
3. Houben, R., and Snyers, A. (2018). "*Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion"*.
4. Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2019). "Blockchain technology overview". *arXiv preprint arXiv:1906.11078*.
5. Maqsood, F., Ahmed, M., Ali, M. M., and Shah, M. A. (2017). Cryptography: a comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications, 8*(6).
6. Hacker, P., and Thomale, C. (2018). "Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law". *European Company and Financial Law Review, 15*(4), 645-696.
7. Härdle, W. K., Harvey, C. R., and Reule, R. C. (2020). "Understanding cryptocurrencies". *Journal of Financial Econometrics, 18*(2), 181-208.
8. Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. (2017). "Blockchain". *Business & Information Systems Engineering, 59*(3), 183-187.
9. Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., and Das, G. (2018). "Everything you wanted to know about the blockchain: Its promise,

components, processes, and problems". *IEEE Consumer Electronics Magazine*, *7*(4), 6-14.

10. Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., and Dutkiewicz, E. (2019). "Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities". *IEEE Access, 7*, 85727-85745.
11. Zheng, Z., Xie, S., Dai, H. N., Chen, X., and Wang, H. (2018). "Blockchain challenges and opportunities: A survey". *International journal of web and grid services, 14*(4), 352-375.
12. Golosova, J., and Romanovs, A. (2018, November). "The advantages and disadvantages of the blockchain technology". In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.
13. Conti, M., Kumar, E. S., Lal, C., and Ruj, S. (2018). "A survey on security and privacy issues of bitcoin". *IEEE Communications Surveys & Tutorials*, *20*(4), 3416-3452.
14. Delgado-Segura, S., Pérez-Solà, C., Navarro-Arribas, G., and Herrera-Joancomartí, J. (2020). "A fair protocol for data trading based on Bitcoin transactions". *Future Generation Computer Systems*, *107*, 832-840.
15. Chuen, D. L. K., Guo, L., and Wang, Y. (2017). "Cryptocurrency: A new investment opportunity?". *The journal of alternative investments*, *20*(3), 16-40.
16. Berentsen, A., and Schär, F. (2018). "A short introduction to the world of cryptocurrencies". *FRB of St. Louis Working Review*.
17. Rauchs, M., and Hileman, G. (2017). "Global cryptocurrency benchmarking study". *Cambridge Centre for Alternative Finance Reports*.
18. Ma, J., Gans, J. S., and Tourky, R. (2018). "*Market structure in bitcoin mining"* (No. w24242). National Bureau of Economic Research.
19. Vranken, H. (2017). "Sustainability of bitcoin and blockchains". *Current opinion in environmental sustainability*, *28*, 1-9.
20. Procházka, D. (2018). "Accounting for bitcoin and other cryptocurrencies under IFRS: A comparison and assessment of competing models". *The International Journal of Digital Accounting Research*, *18*(24), 161-188.

Διαδικτυακές Πηγές:

1. https://www.basecoin.gr/kryptografia-orismos-leitoyrgia-kai-charaktiristika/
2. https://economictimes.indiatimes.com/definition/cryptography
3. https://crypto.com/university/what-is-cryptography
4. https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/
5. https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/cryptography/
6. https://www.pwc.com/cz/en/assets/pdf/StaySecure/8_2019_StaySecure_Symmetric_Cryptography_EN_external_final.pdf
7. https://academy.binance.com/en/articles/what-is-symmetric-key-cryptography
8. https://www.jscape.com/blog/stream-cipher-vs-block-cipher
9. https://www.ssl.com/el
10. https://www.investopedia.com/terms/h/hash.asp
11. https://www.basecoin.gr/psifiako-portofoli-kryptonomismaton/
12. https://www.pwc.com/gx/en/about/new-ventures/crypto-center.html
13. https://www.icaew.com/technical/tas-helpsheets/financial-reporting/accounting-for-cryptocurrencies-under-frs-102
14. https://www.capital.gr/arthra/3590867/i-logistiki-kai-forologiki-metaxeirisi-ton-kruptonomismaton
15. https://www.taxexperts.gr/αρθρογραφία/κρυπτονομίσματα-λογιστικός-χειρισμός-της-παραγωγής-και-εμπορίας-τους
16. https://www.accaglobal.com/in/en/student/exam-support-resources/professional-exams-study-resources/strategic-business-reporting/technical-articles/cryptocurrencies.html
17. https://taxbit.com/blog/a-quick-guide-to-accounting-for-cryptocurrency
18. https://frv.kpmg.us/reference-library/2022/crypto-asset-executive-summary.html
19. https://www.euro2day.gr/investments/crypto/article/2072143/pos-forologoyntai-ta-kryptonomismata-sthn-ellada.html