



ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ: Η ΕΠΑΝΑΣΤΑΣΗ ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ

Πτυχιακή εργασία

Αβδέλαρου Κωνσταντίνα



Αθήνα, 2018 - 2019



ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

Τριμελής Εξεταστική Επιτροπή

Μιχαλακέλης Χρήστος (Επιβλέπων)

**Επίκουρος Καθηγητής, Τμήματος Πληροφορικής και Τηλεματικής, Χαροκόπειο
Πανεπιστήμιο**

Δημητρακόπουλος Γιώργος

**Επίκουρος Καθηγητής, Τμήματος Πληροφορικής και Τηλεματικής, Χαροκόπειο
Πανεπιστήμιο**

Βαμβακάρη Μαλβίνα

**Επίκουρος Καθηγητής, Τμήματος Πληροφορικής και Τηλεματικής, Χαροκόπειο
Πανεπιστήμιο**

Η Αβδέλαρου Κωνσταντίνα

δηλώνω υπεύθυνα ότι:

- 1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλλει τα πνευματικά δικαιώματα τρίτων.
- 2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία εκπονήθηκε στα πλαίσια του Προγράμματος Προπτυχιακών Σπουδών του Τμήματος Πληροφορικής και Τηλεματικής, του Χαροκοπείου Πανεπιστημίου.

Πρωτίστως, θα ήθελα να ευχαριστήσω τον κ. Μιχαλακέλη, επιβλέποντα καθηγητή, για την εμπιστοσύνη που μου έδειξε με την ανάθεση του συγκεκριμένου θέματος και τη συνεχή στήριξη, καθοδήγηση και τις επιστημονικές τους συμβουλές, καθ' όλη τη διάρκεια της συγγραφής της παρούσας πτυχιακής εργασίας, αλλά και για την άψογη συνεργασία μας όλα τα χρονιά των σπουδών μου.

Επιπροσθέτως, οφείλω να ευχαριστήσω και όλα τα μέλη του διδακτικού και ερευνητικού προσωπικού του Χαροκοπείου Πανεπιστημίου για τις γνώσεις τις οποίες μου μετέφεραν κατά τη διάρκεια της φοίτησής μου στο τμήμα Πληροφορικής και Τηλεματικής.

Το μεγαλύτερο «ευχαριστώ» το προσφέρω στην οικογένειά μου, για την αμέριστη ηθική και πνευματική συμπαράσταση σε όλα τα στάδια της συγκεκριμένης εργασίας αλλά και κατά τη διάρκεια των σπουδών μου, καθώς και τη στήριξή τους σε κάθε μου προσπάθεια.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ.....	7
ABSTRACT	9
ΚΕΦΑΛΑΙΟ 1: Η ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΟΥ ΧΡΗΜΑΤΟΣ.....	11
1.1. ΑΝΤΑΛΛΑΓΗ ΕΜΠΟΡΕΥΜΑΤΩΝ	11
1.2. ΕΜΦΑΝΙΣΗ ΤΟΥ ΜΕΤΑΛΛΟΥ.....	13
1.3. ΑΡΧΑΙΑ ΝΟΜΙΣΜΑΤΑ	14
1.4. ΧΡΥΣΟΣ – ΑΣΗΜΙ - ΧΑΛΚΟΣ.....	16
1.5. ΧΑΡΤΟΝΟΜΙΣΜΑΤΑ	17
1.6. ΣΥΓΧΡΟΝΑ ΧΡΗΜΑΤΑ	19
ΚΕΦΑΛΑΙΟ 2: Η ΕΝΝΟΙΑ ΤΟΥ ΧΡΗΜΑΤΟΣ.....	22
2.1. ΟΡΙΣΜΟΣ ΧΡΗΜΑΤΟΣ	22
2.2. ΛΕΙΤΟΥΡΓΙΕΣ ΧΡΗΜΑΤΟΣ	22
2.3. ΙΔΙΟΤΗΤΕΣ ΧΡΗΜΑΤΟΣ	23
2.4. ΜΟΡΦΕΣ ΧΡΗΜΑΤΟΣ	24
2.5. ΣΥΓΧΡΟΝΑ ΕΙΔΗ.....	25
ΚΕΦΑΛΑΙΟ 3: Η ΕΝΝΟΙΑ ΤΟΥ ΨΗΦΙΑΚΟΥ ΝΟΜΙΣΜΑΤΟΣ	28
3.1. ΟΡΙΣΜΟΣ ΨΗΦΙΑΚΟΥ ΝΟΜΙΣΜΑΤΟΣ	28
3.2. ΔΙΑΦΟΡΕΤΙΚΟΙ ΟΡΙΣΜΟΙ	29
3.3. ΡΥΘΜΙΣΗ ΚΑΙ ΕΛΕΓΧΟΣ ΨΗΦΙΑΚΟΥ ΝΟΜΙΣΜΑΤΟΣ	30
3.4. ΕΙΔΗ ΨΗΦΙΑΚΟΥ ΝΟΜΙΣΜΑΤΟΣ	32
3.5. ΚΑΤΗΓΟΡΙΕΣ ΕΙΚΟΝΙΚΩΝ ΝΟΜΙΣΜΑΤΩΝ.....	34
ΚΕΦΑΛΑΙΟ 4: Η ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ BLOCKCHAIN.....	37
4.1. ΟΡΙΣΜΟΣ ΤΗΣ BLOCKCHAIN.....	37
4.2. ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ.....	39
4.3. ΚΑΤΑΡΡΕΥΣΗ ΤΗΣ BLOCKCHAIN	45
4.4. ΚΑΝΟΝΕΣ ΤΗΣ BLOCKCHAIN	46
ΚΕΦΑΛΑΙΟ 5: ΤΟ ΠΡΩΤΟ ΚΡΥΠΤΟΝΟΜΙΣΜΑ.....	48
5.1. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ.....	48
5.2. ΕΙΣΑΓΩΓΗ ΣΤΟ BITCOIN	50
5.3. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΟΥ BITCOIN	51
5.4. SATOSHI NAKAMOTO	53
ΚΕΦΑΛΑΙΟ 6: ΑΠΟΚΤΗΣΗ ΚΑΙ ΑΠΟΘΗΚΕΥΣΗ BITCOIN.....	57
6.1. ΤΡΟΠΟΙ ΑΠΟΚΤΗΣΗΣ	57
6.2. Η ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΕΞΟΡΥΞΗΣ - MINING.....	59
6.3. ΑΓΟΡΑ ΝΟΜΙΣΜΑΤΩΝ BITCOIN.....	61
6.4. ΨΗΦΙΑΚΑ ΠΟΡΤΟΦΟΛΙΑ	63
ΚΕΦΑΛΑΙΟ 7: ΕΠΕΝΔΥΣΗ ΣΤΟ BITCOIN ΚΑΙ Η ΑΞΙΑ ΤΟΥ.....	66
7.1. ΕΠΕΝΔΥΣΗ ΣΤΟ BITCOIN.....	66
7.2. ΚΙΝΔΥΝΟΙ ΕΠΕΝΔΥΣΗΣ	67
7.3. Η ΑΞΙΑ ΤΟΥ BITCOIN	69
7.4. ΕΠΗΡΕΑΣΜΟΣ ΤΗΣ ΑΞΙΑΣ	73

ΚΕΦΑΛΑΙΟ 8: ΣΥΝΑΛΛΑΓΕΣ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ.....	77
8.1. ΕΠΙΤΕΥΞΗ ΣΥΝΑΛΛΑΓΩΝ ΜΕ BITCOIN	77
8.2. ΙΔΙΟΤΗΤΕΣ ΤΩΝ ΣΥΝΑΛΛΑΓΩΝ	80
ΚΕΦΑΛΑΙΟ 9: ALTCOINS	86
9.1. Η ΕΝΝΟΙΑ ΤΩΝ ALTCOINS	86
9.2. NAMECOIN	87
9.3. LITECOIN	89
9.4. RIPPLE	91
9.5. ETHEREUM	94
9.6. BITCOIN CASH.....	97
ΚΕΦΑΛΑΙΟ 10: ΤΑ ΥΠΕΡ ΚΑΙ ΤΑ ΚΑΤΑ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ	101
10.1. ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ.....	101
10.2. ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ	106
ΚΕΦΑΛΑΙΟ 11: ΚΑΝΟΝΕΣ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ	110
11.1. ΟΙΚΟΝΟΜΙΚΟΙ ΚΑΙ ΝΟΜΙΚΟΙ ΚΑΝΟΝΕΣ	110
11.2. ΦΟΡΟΛΟΓΙΚΑ ΚΑΙ ΝΟΜΟΘΕΤΙΚΑ ΠΛΑΙΣΙΑ ΧΩΡΩΝ	111
ΚΕΦΑΛΑΙΟ 12: ΕΠΙΛΟΓΟΣ.....	120
12.1. ΤΟ ΜΕΛΛΟΝ ΤΗΣ BLOCKCHAIN.....	120
12.2. ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ	122
ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ.....	126
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	129

ΠΕΡΙΛΗΨΗ

Η οικονομική δραστηριότητα στον σύγχρονο κόσμο αφορά κατά βάση τα χρήματα. Σκοπός της σύγχρονης οικονομικής αγοράς είναι να δημιουργεί χρήματα, να κερδίζει χρήματα, να διαχειρίζεται χρήματα, να σπαταλάει χρήματα, να εξοικονομεί χρήματα και ούτω καθεξής. Ο καθένας από εμάς χρησιμοποιεί χρήματα, όλοι τα θέλουμε, δουλεύουμε πολλές ώρες την ημέρα για την απόκτηση αυτών και τα σκεφτόμαστε. Σύμφωνα με τον Kulick Alex (2017) τα χρήματα αποτελούν τον τρόπο με τον οποίο αγοράζουμε και κατέχουμε τα πράγματα τα οποία χρειαζόμαστε και επιθυμούμε. Όμως τι είναι ουσιαστικά το χρήμα;

Είναι αλήθεια ότι σύμφωνα με τις συνεχόμενες αλλαγές στην τεχνολογία των ηλεκτρονικών υπολογιστών έχουμε οδηγηθεί σε συζητήσεις και ιδέες για μια κοινωνία χωρίς μετρητά όπου κυρίαρχο χρήμα θα είναι πλέον το ψηφιακό. Αν και θα μπορούσαμε εύκολα να αντιληφθούμε ότι ουσιαστικά δε μιλάμε για αλλαγή της ουσίας του χρήματος αλλά κυρίως για την μορφή του, όταν δηλαδή συζητάμε για μια κοινωνία χωρίς μετρητά εννοούμε μια τεχνολογία πληρωμών η οποία δεν κάνει χρήση χαρτιών και μικρών μεταλλικών δίσκων (Smithin John, 2000).

Φυσικά, αν κάτσουμε να το αναλύσουμε ακόμα περισσότερο θα δούμε ότι στην πραγματικότητα το χρήμα είναι μια αυθαίρετη έννοια, όλοι οι άνθρωποι δηλαδή έχουν συμφωνήσει ότι τα χαρτονομίσματα και τα κέρματα μπορούν να χρησιμοποιηθούν ευρέως στις συναλλαγές μας. Επομένως, αν μια μέρα άλλαζαν τα δεδομένα, αν για παράδειγμα αποφασίζαμε ότι ο χρυσός δεν έχει καμία αξία, αυτό θα είχε ως αποτέλεσμα να μη θέλει κανείς να τον αγοράσει και τότε η αξία του θα έπεφτε σταδιακά και στο τέλος θα κατέληγε σε μηδενική. Το ίδιο ισχύει και για οποιαδήποτε άλλη μορφή συναλλαγής.

Το χρήμα λοιπόν από μόνο του δεν είναι τίποτα και ανεξάρτητα από τη μορφή την οποία έχει, δεν είναι πολύτιμο για τον εαυτό του, αλλά για τα αγαθά και τις υπηρεσίες που μπορεί να αγοράσει. Μπορεί να είναι ένα κέλυφος, ένα μεταλλικό νόμισμα ή ένα κομμάτι χαρτί, αλλά η αξία που τοποθετούν οι άνθρωποι πάνω σε αυτό δεν έχει καμία σχέση με τη φυσική αξία των χρημάτων (Beattie Andrew, 2016). Επομένως, βλέπουμε ότι το χρήμα δημιουργήθηκε για να διευκολύνει τις συναλλαγές μεταξύ των ατόμων και αλλάζει συνεχώς μορφές. Αυτό το οποίο μένει να συνειδητοποιήσουμε είναι ότι το χρήμα είναι άυλο, δεν έχει δηλαδή κάποια υπόσταση, οπότε μπορεί κάλλιστα να είναι μόνο νούμερα σε υπολογιστές.

Στην παρούσα εργασία καλούμαστε να διερευνήσουμε και να εξηγήσουμε αυτήν την περίπτωση, πως δηλαδή από την απλή ανταλλαγή προϊόντων, τα χρυσά νομίσματα, τα δολάρια και το ευρώ έχουμε φτάσει πλέον στην έννοια του ψηφιακού νομίσματος και στην χρήση του στις καθημερινές μας συναλλαγές. Επιπρόσθετα, θα επικεντρωθούμε περισσότερο στην χρησιμότητα αυτού του καινοτόμου συστήματος πληρωμών και θα αναλύσουμε τα είδη του ψηφιακού νομίσματος, καθώς και τις λειτουργίες τους, τον τρόπο απόκτησής τους, τις επιρροές που έχουν στην εγχώρια και παγκόσμια οικονομία, τη συμβολή τους στη διάρθρωση της αγοράς και θα επισημάνουμε τόσο τα αρνητικά όσο και τα θετικά χαρακτηριστικά τους, αναλύοντας και αξιολογώντας τόσο τα οφέλη όσο και τους κινδύνους.

Λέξεις κλειδιά: Ψηφιακό Νόμισμα, Bitcoin, Blockchain, Κρυπτονόμισμα, Altcoins

ABSTRACT

In modern times the economic activity, as a whole, revolves around money. The main activities of the modern financial market are: generate money in all forms, raise more than the already existing money, use better management for the existing funds and lastly spent or save money. Each one of us uses and makes money on a daily basis, we all think about it and how to gain it, and our urge to raise more money for ourselves makes us work countless hours a day. According to Kulick Alex (2017) money is the key to buy or gain the things we need and truly desire.

It is well known that the continuous and rapid developments in computer technology have led us to a society where the virtual currency outmatches the physical currency (cash). Although we could easily understand that we are mainly not focusing on a change in the essence of money but instead we are interested in a change in its most commonly used form. With this in mind, when we look at a “cashless” society, we see a payment method that does not use paper and small metal discs (Smithin John, 2000).

In advance, if we investigate the matter deeper, we will come to a conclusion that the money is an arbitrary concept, meaning that all people have agreed upon using money bills and coins in their transactions. So, for example if one day the concept of buying what you want by spending currency such as gold ceased to exist, it would have as a result people not wanting to buy gold and its value would change to zero. Of course, the same principle would apply to any currency used as a payment method.

In conclusion, money regardless of its form is nothing without people determining its value. Currencies are not valued for their material substance but for the value we give them in order to buy goods and services to satisfy our saturation. The material of the money could be a shell, a metal coin or a piece of paper, but the value people place on it has nothing to do with the natural value of money (Beattie Andrew, 2016). Therefore, we understand that money was created to facilitate transactions between individuals and is constantly changing forms. What remains to be realized is that money is immaterial, and it is uncertain what would be its next form, hence it can easily take the form of just plain numbers in computers.

In this current thesis we study the case of how we have reached the concept of using digital currency in our daily transactions instead of the mere exchange of products, gold coins and currencies such as the US dollar and Euro. In addition, we focus more on the usefulness of this innovative payment system and we analyze the types of digital money that exist nowadays and their functions, how we can obtain them, their effects on the economic system, their contribution to the global economy market and we highlight equally their negative and their positive characteristics through assessing both the benefits and the risks of this new technology.

Keywords: Virtual Currency, Bitcoin, Money, Blockchain, Cryptocurrency, Altcoins

Κεφάλαιο 1: Η ιστορική αναδρομή του χρήματος

1.1. Ανταλλαγή εμπορευμάτων

Το χρήμα, όπως ορίζεται σήμερα, είναι αποτέλεσμα μιας μακροχρόνιας διαδικασίας στα βάθη των αιώνων. Στην αρχή του πολιτισμού, δεν υπήρχαν χρήματα και δεν υπήρχε ούτε η έννοια των χρημάτων, όπως είναι αντιληπτή στη σημερινή εποχή. Αντιθέτως, υπήρχε μόνο η έννοια της παλαιότερης μορφής εμπορίου, αυτή της ανταλλαγής εμπορευμάτων χωρίς ισοτιμία αξίας (Banco Central do Brasil, 2004). Εκείνη την εποχή, η αξία ενός προϊόντος ήταν η ανάγκη κατοχής του, για παράδειγμα, κάποιος γεωργός ο οποίος μπορούσε να καλλιεργεί περισσότερο σιτάρι στο χωράφι του από αυτό που θα χρειαζόταν για να ζήσει ο ίδιος και η οικογένειά του, είχε τη δυνατότητα να ανταλλάξει το περίσσειμα του με κάποιο αγαθό μεγαλύτερης χρησιμότητας για τον ίδιο, το οποίο παράλληλα θα αποτελούσε το πλεόνασμα ενός άλλου προσώπου. Σύμφωνα με το βιβλίο Αρχές Οικονομίας (2010, σελ. 21) ορίζεται ότι το είδος αυτό της ανταλλαγής ονομάζεται αντιπραγματισμός.

Το ανταλλακτικό εμπόριο επομένως στηρίζεται σε μια απλή ιδέα, δυο άτομα διαπραγματεύονται για να καθορίσουν και να συμφωνήσουν μεταξύ τους τη σχετική αξία των αγαθών και των υπηρεσιών τα οποία προσφέρουν και να ανταλλάξουν αυτά τα αγαθά ως προς μια ισοτιμία (Kulick Alex, 2003). Παραδείγματος χάριν, μια επιτυχής συναλλαγή θα μπορούσε να θεωρηθεί αν ο προαναφερθέντος γεωργός αντάλλαζε το σιτάρι του με έναν κτηνοτρόφο, ο οποίος από ένα μεγάλο κοπάδι αγελάδων θα είχε περίσσειμα γάλακτος. Όπως διακρίνεται, τα αγαθά τα οποία τα προμηθευόντουσαν



Εικ.2. Ανταλλακτικό εμπόριο μεταξύ κτηνοτρόφου και ιχθυοτρόφου

κατευθείαν από την γη, μέσα από την γεωργία, την κτηνοτροφία, την ιχθυοτροφία, το κυνήγι και τη συλλογή καρπών, αποτελούσαν και τα εμπορεύματα τα οποία αντάλλαζαν μεταξύ τους, μέσω αυτής της στοιχειώδους μορφής εμπορίου, οι άνθρωποι των πρωτόγονων οικονομιών.

Είναι εύκολα κατανοητό ότι το ανταλλακτικό εμπόριο ήταν έρμαιο κατά κύριο λόγο των περιβαντολλογικών συνθηκών. Το περιβάλλον αποτελούσε τον βασικότερο παράγοντα όσον αφορά τη φυσική κατάσταση των αγαθών τα οποία χρησιμοποιούνταν στην ανταλλαγή. Για

παράδειγμα, στις άσχημες καιρικές συνθήκες με κρύο και χιόνια, κυρίως κατά τους χειμερινούς μήνες, η γη δεν άνθιζε και δεν καρποφορούσε, πράγμα το οποίο είχε μεγάλο αρνητικό αντίκτυπο τόσο στο εμπόριο των γεωργών όσο και των κτηνοτρόφων, αφού η ποσότητα φαγητού των φυτοφάγων ζώων ελαττωνόταν, και έτσι έχαναν ένα μεγάλο κομμάτι της ανταλλακτικής τους δύναμης.

Επιπρόσθετα, ένας άλλος λόγος για τον οποίο αυτή η πρώιμη μορφή ανταλλαγής δεν μπορούσε πολλές φορές να καταστεί αποτελεσματική ήταν διότι δεν παρείχε τη δυνατότητα μεταβίβασης και διαίρεσης των αγαθών, αλλά και επειδή με τον αντιπραγματισμό οι ανταλλαγές ήταν σε γενικό πλαίσιο τυχαίες και ευκαιριακές. Ειδικότερα, για να πραγματοποιηθεί η παραπάνω συναλλαγή ανάμεσα στον γεωργό και στον κτηνοτρόφο, βασική προϋπόθεση θα ήταν και οι δυο να είχαν ανάγκη ο ένας το εμπόρευμα του άλλου, δηλαδή να υπήρχε ένα κοινό ενδιαφέρον για τα συναλλασσόμενα αγαθά και κατ' επέκταση μια οικονομική συναλλαγή. Με άλλα λόγια ο γεωργός δεν χρειάζεται απλά να βρει έναν κτηνοτρόφο για να του πουλήσει το γάλα του αλλά θα πρέπει και αντίστοιχα ο κτηνοτρόφος που θα βρει να έχει ως επιθυμία την απόκτηση σιταριού. Μόνο με αυτόν τον τρόπο θα μπορέσει να πραγματοποιηθεί η μεταξύ τους ανταλλαγή. Επομένως, μια επιτυχημένη ανταλλαγή προϋποθέτει σύμπτωση επιθυμιών καθώς και σύμπτωσή ανταλλασσόμενων ποσοτήτων (Αρχές Οικονομίας, 2010, σελ. 21), δηλαδή οι ποσότητες των ανταλλασσόμενων προϊόντων πρέπει να εκπληρούν συγχρόνως τις βλέψεις και των δυο συναλλασσόμενων.

Είναι σημαντικό να αναφερθεί ότι κάποια εμπορεύματα, εξαιτίας της χρησιμότητας τους, ήταν πιο επιδιωκόμενα από άλλα. Αυτά τα προϊόντα μεγαλύτερης ζήτησης χρησιμοποιήθηκαν ως στοιχεία ανταλλαγής και ως μονάδες σύγκρισης για να δώσουν αξία και σε άλλα εμπορεύματα. Από τα πιο διαδεδομένα ήταν τα βοοειδή, διότι είχαν το πλεονέκτημα να αναπαράγονται, να μετακινούνται μόνα τους και να παρέχουν τις υπηρεσίες τους στους ανθρώπους, αν και φυσικά υπήρχε πάντα κίνδυνος ασθένειας ή θανάτου. Αντίστοιχο χρηματικό προϊόν, με μεγάλη σημασία και ζήτηση ήταν το αλάτι το οποίο ήταν πολύ δύσκολο να αποκτηθεί, κυρίως στο εσωτερικό μέρος των ηπείρων, και πολλές φορές χρησιμοποιούνταν για συντηρητικό τροφίμων (Banco Central do Brasil, 2004).

Επιπροσθέτως, αξιοσημείωτο ήταν το εμπόριο το οποίο γινόταν στην νότια λατινική Αμερική και συγκεκριμένα στην περιοχή της Βραζιλίας όπου χρησιμοποιούσαν ως ανταλλακτικά αγαθά το ξύλο, τη ζάχαρη, το κακάο, τον καπνό και τα πανιά σε διάφορες μορφές νημάτων και υφασμάτων (Banco Central do Brasil, 2004). Επίσης, αξιόλογο ήταν και το εμπόριο

στην περιοχή της Αιγύπτου όπου χρησιμοποιούσαν ως μονάδα μέτρησης το σιτάρι και ως χρήματα δισκία στα οποία καταγράφονταν το χρέος. Ομοίως και το εμπόριο στη Βαβυλωνία όπου χρησιμοποιούσαν αντίστοιχα το κριθάρι, καθώς και το ζύθο. Με την πάροδο των χρόνων όμως, όλα αυτά τα προϊόντα τα οποία αναφέρθηκαν έγιναν ακατάλληλα για εμπορικές συναλλαγές. Το γεγονός ότι τα αγαθά αυτά ήταν εύκολα αλλοιωσίμα και δεν ήταν ανθεκτικά στη φυσική φθορά, καθώς και η αδυναμία τους να υποδιαιρεθούν σε μικρότερες μονάδες για να υπάρξει ένα μεγαλύτερο εύρος τιμών, οδήγησε στην ανάγκη δημιουργίας ενός καινούργιου μέσου συναλλαγής.

1.2. Εμφάνιση του μετάλλου

Όταν το μέταλλο εμφανίστηκε στην ζωή του ανθρώπου όλα άλλαξαν ριζικά. Η ανακάλυψη του μετάλλου αποτέλεσε μεγαλειώδες επίτευγμα και σημείο αναφοράς για ολόκληρη την οικονομία. Συγκεκριμένα, ο χαλκός και τα κράματά του χρησιμοποιήθηκαν από τον άνθρωπο για περισσότερα από 6.000 έτη. Στην αρχή ο χαλκός και τα κράματά με



Εικ. 3. Μεταλλικά αντικείμενα από χαλκό

αρσενικό και κασσίτερο βοήθησαν για την κατασκευή μεταλλικών σκευών, εργαλείων και όπλων τα οποία μέχρι πριν κατασκευάζονταν μόνο από πέτρινους λίθους. Είναι εύκολα αντιληπτό πως ο χαλκός από την 5η χιλιετία π. Χ. αποτέλεσε σημαντικό παράγοντα για τη μετάβαση του πολιτισμού από την εποχή του λίθου στην εποχή των μετάλλων (orykta.gr).



Εικ. 4. Χάλκινα ιατρικά εργαλεία από το ιερό του Ασκληπιού στην Επίδαυρο

φυσική του κατάσταση, αργότερα πήρε τη μορφή πλινθωμάτων και ύστερα μετατράπηκε σε αντικείμενα και κοσμήματα, όπως δαχτυλίδια ή βραχιόλια (Banco Central do Brasil, 2004). Από τότε και έπειτα, η χρήση μετάλλων και η ανάπτυξη της οικονομίας απέκτησαν μια ενιαία, παράλληλη πορεία (orykta.gr).

Σε κάθε συναλλαγή που γινόταν με τη βοήθεια μετάλλων ήταν απαραίτητη η μέτρηση του βάρους, αλλά και της καθαρότητας, του υλικού. Πολύ σύντομα όμως τα μεταλλικά αντικείμενα πήραν μια συγκεκριμένη μορφή και είχαν καθορισμένο βάρος, έχοντας το καθένα και ένα σήμα το οποίο υποδείκνυε την αξία του και τον υπεύθυνο για την έκδοση του. Αυτό το μέτρο έκανε τις συναλλαγές ακόμα πιο γρήγορες αφού έσωσε το πρόβλημα της ζύγισης και επέτρεψε την ταχεία αναγνώριση της ποσότητας μεταλλικού υλικού που προσφέρεται (Banco Central do Brasil, 2004).

Αναμενόμενη βεβαίως ήταν και η μετατροπή των χρημάτων σε μορφές αντικειμένων. Τα μεταλλικά αντικείμενα τα οποία δημιουργήθηκαν έγιναν πολύτιμα εμπορεύματα. Αυτό συνέβη διότι κάποιος δεν έπρεπε απλά να ξέρει να χειρίζεται σωστά το μέταλλο και να δημιουργεί κάτι καινούργιο από το μηδέν, αλλά έπρεπε να διαθέτει γνώσεις όσον αφορά την τήξη του μετάλλου και τα σημεία στα οποία μπορεί να βρεθεί το μέταλλο στην φύση. Συνεπώς, αυτό ήταν ένα έργο εφικτό για λίγους και όχι για όλους. Επομένως, η αυξημένη αξία αυτών των αντικειμένων οδήγησε στη χρησιμοποίησή τους ως χρήματα αλλά και στη δημιουργία και κυκλοφορία μικρότερων πανομοιότυπων αντικειμένων για να καλυφτεί ένα μεγαλύτερο εύρος τιμών (Banco Central do Brasil, 2004).

1.3. Αρχαία νομίσματα

Φημολογείται ότι γύρω στο 1.100 π. Χ. οι Κινέζοι σταμάτησαν τη χρήση ξύλινων εργαλείων και όπλων, ως μέσου ανταλλαγής, για να χρησιμοποιήσουν μικρότερα αντίγραφα των ίδιων εργαλείων φτιαγμένα πλέον από χαλκό. Αυτά τα αντικείμενα όμως αποδείχθηκαν ιδιαίτερα δύσχρηστα και με τη πάροδο του χρόνου, αυτά τα μικροσκοπικά μαχαίρια, σπαθιά και βέλη εγκαταλείφθηκαν για το καλύτερα σχηματισμένο σχήμα ενός κύκλου, το οποίο αποτέλεσε ένα από τα πρώτα νομίσματα. Παρόλο που η Κίνα πρωτοπόρησε και ήταν η πρώτη χώρα η οποία χρησιμοποίησε αναγνωρίσιμα νομίσματα, τα πρώτα ευρέως γνωστά νομίσματα θα κατασκευαστούν όχι πολύ μακριά, στην περιοχή της Λυδίας (Beattie Andrew, 2016).

Τον 7ο αιώνα, γύρω στο 600 π.Χ., τα πρώτα νομίσματα τα οποία μοιάζουν με τα σημερινά εμφανίστηκαν και εισήχθησαν ως μέθοδος πληρωμής. Η ανακάλυψη των νομισμάτων εξακολουθεί να περιβάλλεται από μυστήριο και η κληρονομιά των αρχαίων νομισμάτων είναι ένα θέμα το οποίο ενθουσιάζει τους μελετητές σε όλο τον κόσμο. Οι αριθμητικοί καθώς και αναφορές στα κείμενα του Έφορου και στο Πάριο χρονικό, θεωρούν ότι τα πρώτα νομίσματα

κόπηκαν στο ελληνικό νησί της Αίγινας, είτε από τους τοπικούς κυβερνήτες, είτε από τον βασιλιά Φείδων του Άργους (Jan van der Crabben, 2011). Συγκεκριμένα, η Αργολική Αρχαιακή Βιβλιοθήκη Ιστορίας και Πολιτισμού θεωρεί πως ο Φείδων ήταν ο πρώτος που εισήγαγε τη χρήση χάλκινων και αργυρών νομισμάτων, καθώς και μια νέα κλίμακα μέτρων και σταθμών.

Ωστόσο, σύμφωνα με τον Ηρόδοτο τα κέρματα κόπηκαν για πρώτη φορά από τους Λυδούς. Χαρακτηριστικά αναφέρει πως οι Λυδοί ήταν οι πρώτοι που χρησιμοποίησαν νομίσματα στις αρχές του 7ου αιώνα π.Χ., ενώ τα παλαιότερα Αιγινήτικα νομίσματα τα οποία διασώζονται χρονολογούνται στα μέσα του 6ου αιώνα, αρκετά αργότερα από τον Φείδων του 7ου αιώνα π. Χ. (Εγκυκλοπαίδεια Μπριτάνικα, 2016). Ο Αριστοτέλης με τη σειρά του υποστηρίζει ότι τα πρώτα νομίσματα κόπηκαν από τη Δημοδίκη της Κύμης, σύζυγο του βασιλιά Μίδα της Φρυγίας.



Εικ. 5. Στατήρ της Λυδίας, 6ος αιώνας π.Χ

Το παλαιότερο νόμισμα το οποίο διατίθεται σήμερα ανακαλύφθηκε στην Έφεσο, μια αρχαία ελληνική πόλη η οποία αποτελούσε εμπορικό κέντρο στις ακτές της Μικράς Ασίας. Είναι πάνω από 2.700 ετών, κατασκευασμένο από ήλεκτρο, ένα φυσικό κράμα 73% χρυσού και 27% άργυρου, και προέρχεται από την περιοχή της Λυδίας (Beattie Andrew, 2016). Επίσης, διαθέτει ένα σχέδιο μόνο από τη μια πλευρά, αποτέλεσμα της πρωτόγονης μεθόδου κατασκευής. Είναι φανερό, ότι πολλά από τα πρώτα νομίσματα κόπηκαν από τους εμπόρους της Λυδίας ως μάρκες οι οποίες χρησιμοποιούνται στις εμπορικές συναλλαγές και είχαν πάνω τους αποτυπωμένες παραστάσεις που συνδέονταν άμεσα με την πόλη και τους προστάτες θεούς, καθώς και με λιοντάρια, ταύρους και σύμβολα του βασιλείου. Επίσης, τα περισσότερα από τα νομίσματα που έκοψε το λυδικό κράτος αναφέρουν τον βασιλιά Αλυάττη της Λυδίας.

Αντίστοιχα, στην Αίγινα, στη Σάμο και στη Μίλητο κόπηκαν τα κέρματα για τους Αιγύπτιους και όταν η Λυδία κατακτήθηκε από τους Πέρσες το 546 π.Χ., είναι βέβαιο ότι εισήχθησαν νομίσματα και στην Περσία. Επίσης, οι Φοίνικες δεν έκοβαν νομίσματα μέχρι τα μέσα του πέμπτου αιώνα π.Χ., τα οποία έκτοτε εξαπλώθηκαν γρήγορα μέχρι τη Σικελία, ενώ οι Ρωμαίοι άρχισαν να κερδίζουν νομίσματα από το 326 π. Χ. Φημολογείται, πως στην Ινδία τα νομίσματα εισήχθησαν μέσω της Αχαιμενιδικής Αυτοκρατορίας καθώς και των διαδοχικών βασιλείων του Μεγάλου Αλεξάνδρου, ενώ τα ινδοελληνικά βασίλεια έκοψαν νομίσματα το 2ο

αιώνα π.Χ. Έπειτα, στην Κίνα, τα χρυσά νομίσματα τυποποιήθηκαν για πρώτη φορά κατά τη διάρκεια της δυναστείας Qin (221-207 π.Χ.) (Jan van der Crabben, 2011).

Αξιοπρόσεχτο είναι, ότι κάθε ένας από τους λαούς οι οποίοι αναφέρθηκαν πρωτίτερα έφτιαξε τα νομίσματα με το δικό του διαφορετικό τρόπο, αντικατοπτρίζοντας μέσα σε αυτά την νοοτροπία του. Επομένως, μέσω αυτών των νομισμάτων μπορούν να βρεθούν πολλές πολιτικές και οικονομικές πτυχές της ζωής του εκάστοτε πολιτισμού. Χαρακτηριστικό



Εικ. 6. Αργυρό τετράδραχμο του Μεγάλου Αλεξάνδρου, 323 π.Χ.

παράδειγμα αποτελούν οι διάφορες αποτυπώσεις προσώπων πάνω σε νομίσματα όπου μπορούν να αναγνωριστούν εικόνες προσωποτήτων που έζησαν αιώνες πριν. Άξιο αναφοράς αποτελεί το γεγονός ότι ο πρώτος ιστορικός χαρακτήρας ο οποίος έχει καταχωρηθεί σε ένα νόμισμα ήταν ο Μέγας Αλέξανδρος της Μακεδονίας, περίπου το έτος 330 π. Χ. (Banco Central do Brasil, 2004).

1.4. Χρυσός – Ασήμι - Χαλκός

Όπως έχει ήδη αναφερθεί, τα πρώτα νομίσματα ήταν φτιαγμένα από πολύ μικρά κομμάτια μετάλλου με σταθερό βάρος και αξία, στοιχεία τα οποία αναγράφονταν μέσω της επίσημης πλέον σφραγίδας, η οποία αποτελούσε την εγγύηση του νομίσματος. Ήταν κομμένα στο χέρι με πολύ χονδροειδή τρόπο γεγονός που είχε ως αποτέλεσμα να μην είναι απολύτως ίσια μεταξύ τους και να έχουν ακανόνιστες άκρες. Τα πρώτα μέταλλα τα οποία χρησιμοποιήθηκαν στη δημιουργία αυτών των νομισμάτων ήταν ο χρυσός και ο άργυρος. Οι λόγοι για τους οποίους χρησιμοποιήθηκαν αυτά τα μέταλλα ήταν η σπανιότητα τους, η ομορφιά τους αλλά και η ανοσία τους στη διάβρωση.

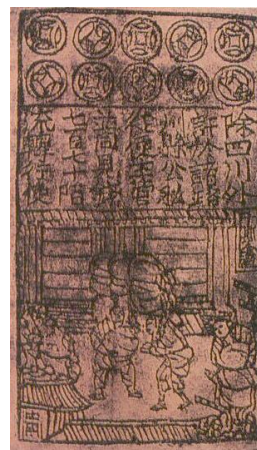
Επιπρόσθετα, πολλοί αρχέγονοι πολιτισμοί, ειδικά στην περιοχή της Βαβυλώνας, πίστευαν στη στενή και άρρηκτα δεμένη σχέση ανάμεσα στο χρυσό με τον ήλιο και στο ασήμι με το φεγγάρι. Αυτή η παλιά θρησκευτική συνήθεια την οποία οι ιερείς, όντας γνώστες της αστρονομίας, δίδαξαν στο λαό είχε ως αποτέλεσμα να οδηγήσει στην απόδοση μαγικών δυνάμεων τόσο στα συγκεκριμένα μέταλλα όσο και στα αντικείμενα που δημιουργήθηκαν βάση αυτών των μετάλλων.

Για πολλούς αιώνες, η κοπή των χρυσών και αργυρών νομισμάτων ήταν κοινή και η εγγύηση τους προέρχονταν από την εμπορική αξία του μετάλλου το οποίο χρησιμοποιήθηκε για την παράγωγή τους. Συγκεκριμένα, ο χρυσός αποτέλεσε το πιο σημαντικό μέταλλο της εποχής και γι' αυτό τον λόγο όλα τα αξιόλογα και μεγάλης αξίας κέρματα κόβονταν σε χρυσό. Αντιθέτως, τα ασημένια και τα χάλκινα νομίσματα απέκτησαν μικρότερη αξία. Η εύκολη υιοθέτηση των κερμάτων οφειλόταν στο γεγονός ότι εκτός από μέσο συναλλαγής και μονάδα μέτρησης ήταν μέταλλα φορητά, διατηρητέα, ανταλλάξιμα και μπορούσαν να αποθηκευτούν για μεγάλα χρονικά διαστήματα.

Αυτό το σύστημα διατηρήθηκε μέχρι τα τέλη του περασμένου αιώνα ενώ μετέπειτα χρησιμοποιήθηκαν άλλα μεταλλικά κράματα για την κατασκευή των κερμάτων και τα νομίσματα κυκλοφόρησαν για την ονομαστική τους αξία, ανεξάρτητα από το μέταλλο το οποίο χρησιμοποιήθηκε για την κατασκευή τους. Στη συνέχεια, με την εμφάνιση των χαρτονομισμάτων, τα μεταλλικά νομίσματα περιορίστηκαν σε ακόμα χαμηλότερες τιμές. Από τότε και έπειτα, σημαντικό και απαραίτητο ρόλο κατέχει η ανθεκτικότητα και η ποιότητα των χρήματων που χρησιμοποιούνται ως μέσο συναλλαγής και όχι το υλικό κατασκευής τους (Banco Central do Brasil, 2004).

1.5. Χαρτονομίσματα

Η Λυδία έμοιαζε να κατείχε το προβάδισμα στις νομισματικές εξελίξεις μέσα από την κοπή των πρώτων νομισμάτων. Την ίδια περίοδο όμως στην Κίνα, κατά τον 7ο αιώνα εμφανίστηκε η πρώτη καταγεγραμμένη χρήση χαρτονομίσματος (Beattie Andrew, 2016). Βασικός λόγος της εμφάνισης του χαρτονομίσματος ήταν η μείωση της ανάγκης μεταφοράς βαριών και δυσκίνητων μεταλλικών νομισμάτων για τη διεξαγωγή συναλλαγών.



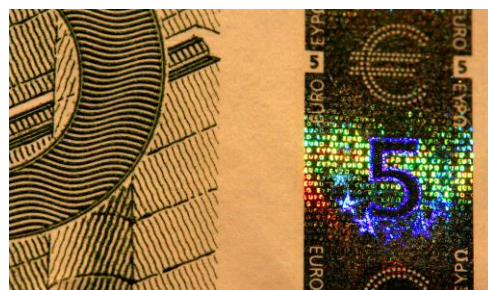
Εικ. 7. Πρώιμο Κινέζικο χαρτονόμισμα της περιόδου της δυναστείας Σονγκ

Παρόμοια με την κατάθεση σε μια σύγχρονη τράπεζα, τα άτομα μετέφεραν τα κέρματα τους σε ένα αξιόπιστο μέρος, όπου αποτελούσε την Κεντρική Τράπεζα της χώρας, και στη συνέχεια λάμβαναν ένα σημείωμα το οποίο ανέφερε πόσα χρήματα είχαν καταθέσει. Αυτά τα σημειώματα μπορούσαν να χρησιμοποιηθούν για την αγορά αγαθών και υπηρεσιών, και λειτουργούσαν όπως το σημερινό νόμισμα. Αργότερα, οι καταθέτες μπορούσαν να επισκεφτούν ξανά την τράπεζα

έχοντας το συγκεκριμένο σημείωμα και να εξαργυρώσουν το αναγραφόμενο ποσό (Beattie Andrew, 2016).

Στον Μεσαίωνα, οι χρυσοχόοι, τα άτομα δηλαδή τα οποία εμπορεύονταν με είδη χρυσού και άργυρου αποτελούσαν την εκάστοτε τράπεζα και οι συναλλαγές μαζί τους ήταν κοινές. Πιο συγκεκριμένα, ο χρυσοχόος, ως εγγυητής, έδινε μια απόδειξη με το αναγραφόμενο ποσό στον καταθέτη. Αυτές οι αποδείξεις έπειτα χρησιμοποιούνταν για την πραγματοποίηση πληρωμών περνώντας από το ένα χέρι στο άλλο προσθέτοντας με αυτόν τον τρόπο τα θεμέλια για την δημιουργία των χαρτονομισμάτων. Το 1810 από τη Banco de Brasil στη Βραζιλία, εκδόθηκαν και τα πρώτα τραπεζογραμμάτια, πρώιμες μορφές των σημερινών χαρτονομισμάτων, η αξία των οποίων εμφανίζονταν χειρόγραφη στο μπροστινό μέρος.

Με την πάροδο του χρόνου, όπως συνέβη με τα αρχαία νομίσματα, η κυβέρνηση έπρεπε να ανακαλύψει τρόπους να ελέγχει τα πλαστά χαρτονομίσματα και να εξασφαλίζει την αξία τους. Γι' αυτό το λόγο, ακόμα και σήμερα, όλες οι χώρες έχουν την Κεντρική Τράπεζα η οποία είναι υπεύθυνη για την έκδοση κερμάτων και χαρτονομισμάτων. Επιπρόσθετα, ένας άλλος τρόπος προστασίας των χρημάτων ήταν η εξέλιξη όσον αφορά την τεχνική η οποία χρησιμοποιείται στην εκτύπωση των χαρτονομισμάτων. Σήμερα στην εκτύπωση χρησιμοποιείται ειδικά επεξεργασμένο χαρτί και γίνονται πολλές διαδικασίες εκτύπωσης, συμπληρωματικές μεταξύ τους, εξασφαλίζοντας με αυτό το τρόπο μεγάλη ασφάλεια και ανθεκτικότητα.



Εικ. 8. Ολόγραμμα σε χαρτονόμισμα των 5 ευρώ

Όσον αφορά τη φυσική τους όψη, τα χαρτονομίσματα έχουν ορθογώνιο σχήμα, αν και υπάρχει μεγάλη ποικιλία μεγεθών, και απεικονίζουν τον πολιτισμό της χώρας έκδοσής τους μέσα από μοτίβα όπως τοπία, ανθρώπους, μνημεία αρχαίας και σύγχρονης αρχιτεκτονικής, πολιτικούς ηγέτες, ιστορικές σκηνές και άλλα. Επιπρόσθετα, τα χαρτονομίσματα φέρουν επιγραφές, κατά κύριο λόγο στη γλώσσα της χώρας έκδοσής τους αν και αρκετά χαρτονομίσματα φέρουν τις ίδιες επιγραφές και σε άλλους ιδιωματισμούς, με κυρίαρχη την αγγλική γλώσσα, με σκοπό να επιτρέπουν σε μεγαλύτερο αριθμό ανθρώπων να διαβάσει τι αναγράφεται (Banco Central do Brasil, 2004).

1.6. Σύγχρονα χρήματα

Μεταφερόμενοι στην πιο σύγχρονη εποχή είναι γνωστό ότι κάθε χώρα έχει το δικό της νόμισμα, δηλαδή μια αποδεκτή μορφή χρήματος, τόσο κερμάτων όσο και χαρτονομισμάτων, τα οποία εκδίδονται από μια κυβέρνηση και κυκλοφορούν σε μια οικονομία. Για παράδειγμα, το επίσημο νόμισμα της Ελβετίας είναι το ελβετικό φράγκο και της Ιαπωνίας είναι το γιεν. Εξαίρεση φυσικά αποτελεί το ευρώ, το οποίο χρησιμοποιείται ως νόμισμα για τις περισσότερες χώρες της Ευρωπαϊκής Ένωσης. Πρέπει να τονίσουμε ότι τα σύγχρονα νομίσματα έχουν ως βασικό χαρακτηριστικό ότι το υλικό από το οποίο κατασκευάζονται είναι ουσιαστικά άχρηστο προκειμένου ολόκληρη η αξία του νομίσματος να αποδίδεται στην αξία του ως μέσο ανταλλαγής (Kenton Will, 2003).

Σχεδόν όλες οι χώρες χρησιμοποιούν ένα νομισματικό σύστημα στο οποίο οι υψηλότερες τιμές εκφράζονται σε χαρτονομίσματα ενώ οι μικρότερες τιμές αντιπροσωπεύονται από κέρματα. Παράλληλα, τα σύγχρονα μεταλλικά κέρματα επιτρέπουν στα κέρματα να είναι πιο ανθεκτικά από τα χαρτονομίσματα καθιστώντας τα κατάλληλα για πιο έντονη και συνεχή χρήση. Πλέον, η εκάστοτε χώρα μέσω των Κεντρικών Τραπεζών, οι οποίες στις περισσότερες περιπτώσεις έχουν και το μοναδικό δικαίωμα έκδοσης χρημάτων για κυκλοφορία, ελέγχει και εγγυάται την έκδοση χρημάτων και ανανεώνει συνεχώς το σύνολο αυτών, αντικαθιστώντας τυχόν φθορές. Εύκολα διακριτό είναι ότι έπειτα από την παύση της μετατροπής των νομισμάτων και των χαρτονομισμάτων σε πολύτιμα μέταλλα, τα χρήματα απέκτησαν μια ακόμα πιο άυλη και υποθετική υπόσταση (Banco Central do Brasil, 2004).

Στην Ευρώπη η έκδοση χαρτονομισμάτων οδήγησε σε μεγάλη αύξηση του διεθνούς εμπορίου. Πιο συγκεκριμένα, οι τράπεζες και οι διοικητικές τάξεις άρχισαν να αγοράζουν νομίσματα από άλλες χώρες δημιουργώντας με αυτό τον τρόπο την πρώτη συναλλαγματική αγορά. Φυσικά, σημαντικό ρολό κατείχε η σταθερότητα του πολιτεύματος σε μια χώρα που αναπόφευκτα επηρεάζει την αξία του νομίσματος της αλλά και την ικανότητα της να εμπορεύεται στη διεθνή αγορά. Ωστόσο, ταυτόχρονα, αναπτύχθηκε έντονο το αίσθημα του ανταγωνισμού ανάμεσα στις χώρες γεγονός που συχνά οδηγούσε σε νομισματικούς πολέμους, στους οποίους προσπαθώντας να επηρεάσουν την αξία του νομίσματος του ανταγωνιστή, πολλές χώρες μείωναν την αγοραστική δύναμη του εχθρού ή εξάλειφαν εντελώς το νόμισμά του (Beattie Andrew, 2016).

Σήμερα, ο 21ος αιώνας είναι γνωστός για τη δημιουργία δυο νέων μορφών νομισμάτων, τις κινητές πληρωμές και το ψηφιακό νόμισμα. Οι πρώτες κινητές πληρωμές, δηλαδή πληρωμές οι οποίες γίνονται μέσω κινητών φορητών συσκευών, έγιναν για πρώτη φορά δημοφιλείς στην Ασία και στην Ευρώπη και υστέρη στις Ηνωμένες Πολιτείες και τον Καναδά, όπου αποτελούν πλέον την πιο συνηθισμένη και διαδεδομένη μορφή πληρωμών.

Αρχικά, οι πληρωμές γίνονταν μέσω ενός κινητού τηλεφώνου και με την αποστολή ενός γραπτού μηνύματος κειμένου. Στη συνέχεια, η τεχνολογία επέτρεψε στη λήψη φωτογραφιών από επιταγές, μέσω της κάμερας του κινητού τηλεφώνου, και την αποστολή αυτών στον αποδέκτη της πληρωμής. Τελικά μέσω της εξέλιξης της τεχνολογίας υφίσταται ακόμα και η δυνατότητα κατάθεσης επιταγών μέσω των τραπεζικών εφαρμογών στα κινητά τηλέφωνα. Επιπλέον, πολλές τράπεζες έχουν υιοθετήσει στις εφαρμογές τους λειτουργίες οι οποίες επιτρέπουν στους πελάτες να στέλνουν χρήματα ανάμεσα σε φίλους και μέλη της οικογένειας απευθείας από τους τραπεζικούς τους λογαριασμούς.

Πρόσφατα, αναπτύχθηκαν επίσης εφαρμογές, όπως η PayPal και η Apple Pay, οι οποίες επιτρέπουν την άμεση αγορά προϊόντων από το χώρο των καταστημάτων απλά με τη σάρωση ενός γραμμωτού κώδικα (QR code) στην αντίστοιχη εφαρμογή. Το κόστος της αγοράς μπορεί να αφαιρεθεί από μια προκαταχωρισμένη ποσότητα χρημάτων στον λογαριασμό που σχετίζεται με το κατάστημα ή να πληρωθεί με πιστωτική ή χρεωστική κάρτα. Επειδή οι πληροφορίες κατά τη διάρκεια της συγκεκριμένης συναλλαγής είναι κρυπτογραφημένες θεωρείται ότι είναι η ασφαλέστερη μέθοδος πληρωμής σε σχέση με την απευθείας πληρωμή με χρεωστική ή πιστωτική κάρτα (investopedia.com, 2010).



Εικ. 9. QR code για την εφαρμογή PayPal

Η επόμενη καινοτόμα μορφή νομίσματος είναι το ψηφιακό νόμισμα, το οποίο αποτελεί ένα είδος νομίσματος χωρίς φυσική υπόσταση που βρίσκεται και εδρεύει μέσα σε έναν ηλεκτρονικό υπολογιστή. Χαρακτηριστικό παράδειγμα αποτελεί το κρυπτονόμισμα Bitcoin, το οποίο εφευρέθηκε το 2009 από ένα άτομο ή μια ομάδα ατόμων με το ψευδώνυμο



Εικ. 10. Το κρυπτονόμισμα Bitcoin

Satoshi Nakamoto και το οποίο έγινε το σημείο αναφοράς του ψηφιακού νομίσματος. Το κρυπτονόμισμα, μια συγκεκριμένη μορφή ψηφιακού νομίσματος, είναι ευρέως διαδεδομένη διότι υπόσχεται χαμηλότερα τέλη συναλλαγών έναντι των παραδοσιακών τρόπων ηλεκτρονικής πληρωμής.

Κεφάλαιο 2: Η έννοια του χρήματος

2.1. Ορισμός χρήματος

Ιστορικά πολλές οικονομίες στηρίζονταν στην ανταλλαγή αγαθών, όμως στις σύγχρονες κοινωνίες οι συναλλαγές δεν πραγματοποιούνται με την άμεση ανταλλαγή πράγματων ή υπηρεσιών αλλά γίνονται με τη μεσολάβηση του χρήματος, δηλαδή με χρηματικές μονάδες οι οποίες εκφράζουν τη τιμή του εκάστοτε εμπορεύματος. Αξίζει να τονισθεί ότι η ύπαρξη του χρήματος δεν ακυρώνει την σχέση ανταλλαγής μεταξύ των εμπορευμάτων, αν και την καθιστά λιγότερο ευδιάκριτη, από ότι θα ήταν στην περίπτωση που οι ανταλλαγές ήταν άμεσες (Αρχές Οικονομίας, 2010, σελ. 23). Ένας πιο συγκεκριμένος ορισμός του χρήματος είναι ο εξής: χρήμα ορίζεται ένα στοιχείο, ή επαληθεύσιμη εγγραφή, το οποίο είναι επίσημα αναγνωρισμένο καθώς και νομικά και κοινωνικά αποδεκτό και χρησιμοποιείται ως αντάλλαγμα και ως μέσο πληρωμής για οποιοδήποτε αγαθό ή υπηρεσία σε μια συγκεκριμένη χώρα ή ένα κοινωνικοοικονομικό πλαίσιο.

Έπειτα από την αναδρομή στην ιστορία του χρήματος η οποία περιγράφηκε αναλυτικά στο προηγούμενο κεφάλαιο κατέστη ορατό ότι μέσω του ανταλλακτικού εμπορίου υπήρχαν πολλές δυσκολίες, τόσο στην εύρεση του κατάλληλου συναλλασσόμενου που να ενδιαφέρεται για το εμπόρευμα κάποιου ατόμου καθώς και αντίστροφο, όσο και στην διαίρεση του εμπορεύματος σε επιμέρους τμήματα προκειμένου να επιτραπεί και να επιτευχθεί μια συναλλαγή. Χαρακτηριστική επίσης αποτελεί και η σύγχυση η οποία δημιουργούταν, μεταξύ των συναλλασσόμενων, εξαιτίας του πλήθους ανταλλακτικών αξιών που είχε το κάθε προϊόν σύμφωνα με τα υπόλοιπα εμπορεύματα. Όπως φαίνεται και στο βιβλίο Αρχές Οικονομικής Θεωρίας (2011, σελ.10) όλα αυτά τα προβλήματα τα οποία δυσκόλευαν τις εμπορευματικές ανταλλαγές επιλυθήκαν με τη βοήθεια του χρήματος το οποίο μετέτρεψε τις ανταλλαγές σε συναλλαγές και του οποίου η ύπαρξη διαδραματίζει καθοριστικό ρόλο στην οικονομία μέχρι σήμερα.

2.2. Λειτουργίες χρήματος

Είναι φανερό ότι η ύπαρξη του χρήματος καταργεί όλες τις προαναφερθέντες δυσκολίες, όμως πρέπει να ικανοποιεί και κάποια βασικά κριτήρια. Πολλά αγαθά έχουν μερικά από τα χαρακτηριστικά τα οποία θα αναφερθούν παρακάτω, εντούτοις κανένα αγαθό δεν είναι χρήμα εκτός αν μπορεί να ικανοποιήσει, σύμφωνα με τους Mankiw Gregory N. (2006, σελ. 22-32) και

Greco Thomas H. (2001), και τις τρεις κυρίες λειτουργίες του χρήματος οι οποίες διακρίνονται σε:

Μέσο συναλλαγής και ανταλλαγής

Το κόστος, τα προβλήματα και οι δυσκολίες οι οποίες προέκυπταν μέσα από την ανταλλαγή αγαθών και υπηρεσιών οδήγησαν στην σημερινή μορφή του χρήματος, δηλαδή στην δημιουργία χαρτονομισμάτων και κερμάτων, για να διευκολυνθούν οι εμπορικές συναλλαγές και οι επενδυτικές ενέργειες, με αξία την οποία όλοι εμπιστεύονται (Ευρωπαϊκή Κεντρική Τράπεζα, 2015 & Αρχές Οικονομικής Θεωρίας, 2011, σελ. 10). Το χρήμα ως μέσο ανταλλαγής επιτελεί μια σημαντικότερη λειτουργία αφού συμβάλει συγχρόνως και στη μείωση του κόστους των συναλλαγών καθώς και στην οικονομική ευημερία.

Μέτρο υπολογισμού των οικονομικών αξιών

Η σύγκριση και συσχέτιση των αγαθών μεταξύ τους ως προς την χρηματική τους τιμή βοηθάει να οριστεί ποιο αγαθό είναι μεγαλύτερης αξίας και ποιο μικρότερης. Η διαμόρφωση της ανταλλακτικής αξίας κάθε εμπορεύματος σε χρήμα το καθιστά ως μέτρο σύγκρισης της πραγματικής αξίας των εμπορευμάτων ώστε να υπάρξει μια σαφέστατη εικόνα της σχετικής σημασίας τους (Αρχές Οικονομίας, 2010, σελ. 26 & Αρχές Οικονομικής Θεωρίας, 2011, σελ. 10).

Μέσο πληρωμών και αποταμίευσης

Όλοι οι συναλλασσόμενοι δέχονται να αποκτήσουν το αντίτιμο του εμπορεύματος που προσφέρουν σε χρήμα διότι αποτελεί διαχρονική μονάδα μέτρησης (Αρχές Οικονομίας, 2010, σελ. 26). Η αξία των χρημάτων διατηρείται και επιτρέπεται να γίνει μελλοντική χρήση αυτών σε διαφορετικό χρόνο από τον χρόνο συναλλαγής. Επομένως, μπορεί κάποιος να έχει στη διάθεση του χρήματα αντί για αγαθά, τα οποία αποτελούν την περιουσία του και τα οποία μπορεί να χρησιμοποιήσει οποιαδήποτε στιγμή (Αρχές Οικονομικής Θεωρίας, 2011, σελ. 10).

2.3. Ιδιότητες χρήματος

Για να μπορεί το χρήμα να πληρεί όλες τις παραπάνω βασικές λειτουργίες πρέπει, όπως ορίζεται και στο βιβλίο Αρχές Οικονομίας (2010, σελ. 27), να έχει και τις εξής ιδιότητες:

- Πρέπει όλοι οι συναλλασσόμενοι, συνεπώς το σύνολο του κοινωνικού πληθυσμού, να το αποδεχτεί ως μέσο συναλλαγής.

- Το αντικείμενο που θα χρησιμοποιηθεί θα πρέπει να είναι σπάνιο αλλά όχι σπανιότατο, δηλαδή η ανταλλακτική του αξία θα πρέπει να είναι τόση, ώστε να καλύπτει τις συναλλαγές που γίνονται σε καθημερινή βάση.
- Θα πρέπει να μην αλλοιώνεται και να είναι ανθεκτικό στη φυσική φθορά με το πέρασμα του χρόνου.
- Τέλος, θα πρέπει να έχει ένα εύρος τιμών, ώστε να μπορεί να υποδιαιρεθεί σε μικρότερες μονάδες και να καλύπτει έτσι όλες τις πιθανές συναλλαγές.

2.4. Μορφές χρήματος

Στην αρχαιότητα μέσα από διάφορες πηγές συναντά κανείς πολλά είδη χρήματος τα οποία χρησιμοποιήθηκαν για τις συναλλαγές, όπως για παράδειγμα τα βοοειδή, τα πρόβατα, τα δέρματα, τα όστρακα, τα φτερά, το αλάτι, διάφορα μέταλλα, ακόμα και ανθρώπινα όντα μέσα από το δουλεμπόριο. Σε γενικές γραμμές, οποιαδήποτε απεικόνιση και αν έχει ένα μέσο ανταλλαγής, εάν γίνεται αποδεκτό από όλα τα μέλη μιας κοινωνίας σε αντάλλαγμα για οποιοδήποτε αγαθό ή υπηρεσία, αναλαμβάνει το ρόλο του χρήματος. Χρήμα, επομένως, ορίζεται καθετί χρησιμοποιείται ευρέως στις συναλλαγές.

Σύμφωνα με το βιβλίο Αρχές Οικονομίας (2010, σελ. 28), διακρίνονται τρεις βασικές κατηγορίες χρήματος:

- **Περιεκτικό**, δηλαδή το χρήμα το οποίο έχει αξία ίση με την εμπορευματική του αξία, για παράδειγμα είδη και προϊόντα τα οποία έχουν και άλλες χρήσεις εκτός από αυτές του χρήματος όπως ζώα, χρυσός, ασήμι, λάδι, αλάτι και οποιοδήποτε άλλο αντικείμενο κατανάλωσης.
- **Παραστατικό**, ή αλλιώς χρήμα αναγκαστικής κυκλοφορίας, δηλαδή το χρήμα του οποίου η αναγραφόμενη αξία αντιστοιχεί σε αξία μεγαλύτερη από την αξία του υλικού από το οποίο συντίθεται, για παράδειγμα κέρματα, χαρτονομίσματα, καταθέσεις όψεως.
- **Ψευδοπεριεκτικό**, ή αντιπροσωπευτικό χρήμα, δηλαδή τίτλοι κατοχής, αποδεικτικά δικαιώματα ή αξιόγραφα τα οποία δεν έχουν καμία εμπορευματική αξία αλλά αντιπροσωπεύουν αξία και μετατρέπονται αμέσως και πλήρως σε περιεκτικό χρήμα, για παράδειγμα τα χρεόγραφα τα οποία τυπώνανε ιδιώτες τραπεζίτες με την γραπτή διαβεβαίωση ότι ο ιδιοκτήτης του χρεογράφου θα αμειβόταν την αξία του σε χρυσό.

Σύμφωνα με τον Χρυσό Κανόνα, όταν το κράτος ανέλαβε ολοκληρωτικά το εκδοτικό δικαίωμα του χρήματος υποσχέθηκε ότι τα χαρτονομίσματα μπορούσαν να εξαργυρωθούν από

την εκδοτική τράπεζα σε χρυσό, γεγονός που σήμαινε ότι μπορούσε να κυκλοφορήσει τόση αξία σε χαρτονομίσματα όση η αξία των αποθεμάτων χρυσού στο θησαυροφυλάκιο της τράπεζας. Κυρίως εγγυητές αυτής της μετατρεψιμότητας ήταν η τράπεζα και το κράτος. Βέβαια, μετά την κρίση του δολαρίου το 1960 εγκαταλείφθηκε ο συγκεκριμένος κανόνας και επικρατέστερο χρήμα έγινε το παραστατικό (Αρχές Οικονομίας, 2010, σελ. 28). Πλέον, η ποσότητα των χαρτονομισμάτων τα οποία θέτει σε κυκλοφορία η Κεντρική Τράπεζα, προσδιορίζεται από τη νομισματική πολιτική κάθε χώρας με βάση γενικότερα οικονομικά κριτήρια (Αρχές Οικονομικής Θεωρίας, 2011, σελ. 10).

2.5. Σύγχρονα είδη

Πλέον τα είδη χρήματος τα οποία υπάρχουν στην σύγχρονη οικονομική αγορά είναι:

- Το **μεταλλικό χρήμα** το οποίο αποτελεί την πιο διαδεδομένη μορφή χρήματος. Χαρακτηριστικά πολύτιμα μέταλλα τα οποία χρησιμοποιούνταν από τη αρχαιότητα για την δημιουργία του μεταλλικού χρήματος είναι ο χαλκός στην Αρχαία Αίγυπτο, ο σίδηρος στη Σπάρτη και ο ορείχαλκος στη Ρώμη, διότι αποτελούν σπάνια και περιζήτητα προϊόντα τα οποία αντιπροσωπεύουν μεγάλη αξία σε μικρό μέγεθος και βάρος και δεν αλλοιώνονται. Παρομοίως, ο χρυσός και ο άργυρος επικράτησαν μέχρι το τέλος λόγω ορισμένων φυσικών ιδιοτήτων τους.

Στη σημερινή εποχή, τα μεταλλικά νομίσματα δεν περιέχουν ποσότητες πολύτιμων μεταλλευμάτων, και η αξία του κράματος το οποίο χρησιμοποιείτε για την κατασκευή τους είναι πολύ μικρότερη από αυτή που αντιπροσωπεύουν, πρόκειται επομένως για μια μορφή παραστατικού χρήματος. Στις μέρες μας, η χρήση του μεταλλικού χρήματος περιορίζεται ολοένα και περισσότερο καθώς εξυπηρετεί ένα πολύ μικρό εύρος των συναλλαγών (Αρχές Οικονομίας, 2010, σελ. 29).

- Τα **χαρτονομίσματα** αποτελούν το βασικό παράδειγμα παραστατικού χρήματος και είναι γνωστά και ως τραπεζογραμμάτια. Την σήμερα ημέρα, το κράτος έχει παραχωρήσει το δικαίωμα έκδοσης χρημάτων σε μια μόνο τράπεζα, την εκδοτική τράπεζα, προκειμένου να διατηρηθεί η ροή των κεφαλαίων σύμφωνα με τη νομισματική πολιτική (investopedia.com, 2007). Η εκδοτική τράπεζα, είναι υπεύθυνη τόσο για την έκδοση των χρημάτων όσο και για την κυκλοφορία τους, η οποία είναι υποχρεωτική, με την έννοια ότι όλοι οι συναλλασσόμενοι πρέπει να αποδέχονται το χαρτονόμισμα στις συναλλαγές τους (Αρχές Οικονομίας, 2010, σελ. 29).

Σήμερα, τα χαρτονομίσματα τείνουν να ενημερώνονται τακτικά και να κυκλοφορούν νέες εκδόσεις αυτών με μεγαλύτερα χαρακτηριστικά ασφαλείας ώστε να καθίσταται δυσκολότερη η δημιουργία παράνομων αντιγράφων (investopedia.com, 2007).

- Το **πιστωτικό χρήμα**, το οποίο ουσιαστικά πρόκειται για τις γνωστές επιταγές, δηλαδή εντολές προς την τράπεζα να εξαργυρώσει το αναγραφόμενο ποσό στον δικαιούχο της επιταγής από τον λογαριασμό του εκδότη της επιταγής. Το ποσό πρέπει να είναι ήδη κατατεθειμένο στο λογαριασμό αλλιώς η επιταγή χαρακτηρίζεται ως ακάλυπτη και ο εκδότης της αντιμετωπίζει κυρώσεις, τόσο οικονομικές όσο και ποινικές.

Άλλη μορφή πιστωτικού χρήματος είναι η συναλλαγματική, μια υπόσχεση πληρωμής στο μέλλον. Πρόκειται για μια ιδιωτική ρύθμιση, όπου ο οφειλέτης υπόσχεται ότι θα πληρώσει στο δικαιούχο το ποσό το οποίο αναγράφεται στην ημερομηνία που αναγράφεται. Συνήθως, εξαιτίας της δυνατότητας η οποία παρέχεται στον οφειλέτη να πληρώσει σε μεταγενέστερο χρόνο του προστίθεται ένα επιπλέον ποσό ως επιβάρυνση το οποίο ονομάζεται τόκος. Το πιστωτικό χρήμα πρέπει να τονιστεί ότι είναι προαιρετικός τρόπος συναλλαγής και οποιοσδήποτε μπορεί να αρνηθεί να τον αποδεχτεί ως μέσο πληρωμής και αντ' αυτού να απαιτήσει χαρτονομίσματα (Αρχές Οικονομίας, 2010, σελ. 29).

- Το **πλαστικό χρήμα**, δηλαδή οι πιστωτικές κάρτες τις οποίες εκδίδουν οι εμπορικές τράπεζες και των οποίων η χρήση αυξάνεται συνεχώς στις σημερινές κοινωνίες, αφού διευκολύνουν κατά πολύ τις συναλλαγές και αποτρέπουν κινδύνους κλοπής. Μέσω των πιστωτικών καρτών ο χρήστης της μπορεί να μην πληρώσει αμέσως με μετρητά αλλά να πληρώσει αργότερα στην τράπεζα το σύνολο της αξίας των αγορών του, συν τυχόν πρόσθετες συμφωνημένες χρεώσεις (investopedia.com, 2003).

Οι πιστωτικές κάρτες είναι πολύ διαδεδομένες μορφές πληρωμής για καταναλωτικά αγαθά και υπηρεσίες και χρησιμοποιούνται ευρέως σε πολλά καταστήματα, αφού σχεδόν κάθε επιχείρηση επιτρέπει την πληρωμή προϊόντων και υπηρεσιών μέσω πιστωτικών καρτών (Αρχές Οικονομίας, 2010, σελ. 29, Αρχές Οικονομικής Θεωρίας, 2011, σελ. 10 & investopedia.com, 2003).

- Το **ηλεκτρονικό χρήμα**. Με αυτόν τον όρο περιγράφεται κάθε μορφή μεταφοράς κεφαλαίου μεταξύ δυο ή περισσότερων μερών η οποία γίνεται με ψηφιακό τρόπο χωρίς τη μεσολάβηση

υλικού μέσου. Αποτελεί ουσιαστικά νομισματική αξία η οποία βρίσκεται αποθηκευμένη, για παράδειγμα, μέσα σε μια προπληρωμένη κάρτα ή σε ένα έξυπνο κινητό τηλέφωνο. Η άμεση χρέωση, η πληρωμή μέσω του διαδικτύου καθώς και η μεταφορά κεφαλαίων μέσω καρτών είναι ενέργειες που δεν χρησιμοποιούν μετρητά και αποτελούν ηλεκτρονικό τρόπο πληρωμής.

Εκτός από τους προαναφερθέντες τρόπους πληρωμής ήρθαν να ενταχθούν στην ίδια κατηγορία, και στην ζωή των ανθρώπων, τα νέα αποκεντρωμένα ψηφιακά νομίσματα, ένα καινοτόμο δίκτυο πληρωμών και ένα νέο είδος χρημάτων το οποίο δεν ελέγχεται από μια κεντρική αρχή. Βέβαια ακόμα και σήμερα σε νομικό και οικονομικό πλαίσιο το ψηφιακό νόμισμα δεν θεωρείται νόμιμο χρήμα (Ευρωπαϊκή Κεντρική Τράπεζα, 2015).

Κεφάλαιο 3: Η έννοια του ψηφιακού νομίσματος

3.1. Ορισμός ψηφιακού νομίσματος

Ψηφιακό νόμισμα ορίζεται ένα μέσο πληρωμής δίχως υλική υπόσταση το οποίο, σε αντίθεση με τα χαρτονομίσματα και τα κέρματα, υπάρχει μονάχα σε ψηφιακή μορφή διότι υπολογίζεται, αποθηκεύεται και μεταφέρεται αποκλειστικά μέσω ηλεκτρονικών υπολογιστών (Frankenfield Jake, Digital Money, 2011). Συγκεκριμένα, οποιοδήποτε νόμισμα βρίσκεται στη μορφή του δυαδικού συστήματος 0 και 1 αποτελεί ψηφιακό νόμισμα (Wagner Andrew, 2014).

Ένα από τα σημαντικότερα στοιχεία του ψηφιακού νομίσματος είναι ότι δεν έχει άμεση σχέση με το πραγματικό νόμισμα και ειδικότερα δεν επηρεάζει την τιμή του, αφού στην πραγματικότητα δεν αντιστοιχεί σε κανένα «αληθινό» νόμισμα (Wikoff Shawn, 2016). Όμως, παρόλο που δεν αλληλεξαρτάται από τα παραστατικά νομίσματα διαθέτει παρόμοιες ιδιότητες με αυτά. Στις ημέρες μας τα ψηφιακά νομίσματα αποτελούν μια πιο άμεση και αποδεκτή μέθοδο για την συναλλαγή αγαθών και υπηρεσιών μεταξύ πολιτών και επιχειρηματιών, τόσο στην εγχωρία όσο και στην παγκόσμια αγορά. Σημαντικό είναι να τονιστεί ότι είναι εφικτό τέτοιου είδους νομίσματα να χρησιμοποιηθούν και σε πιο συγκεκριμένες κοινότητες, όπως ένα παιχνίδι ή ένα κοινωνικό δίκτυο (Acheson Noelle, What is Bitcoin?, 2013).

Σε γενικό πλαίσιο, υπάρχει μεγάλη σύγχυση στον ευρύ κόσμο όσον αφορά τους όρους που χρησιμοποιούνται για την περιγραφή των νομισμάτων ηλεκτρονικής μορφής. Συχνά χρησιμοποιείται ο όρος εικονικό νόμισμα για να αποδοθούν οι έννοιες και οι λειτουργίες του ψηφιακού νομίσματος. Είναι σημαντικό λοιπόν να επισημανθεί ότι τα εικονικά νομίσματα δεν είναι παρα μια μορφή ψηφιακών νομισμάτων. Πιο συγκεκριμένα, όλα τα εικονικά νομίσματα είναι ψηφιακά νομίσματα χωρίς όμως να ισχύει και το αντίστροφο. Τα κρυπτονομίσματα είναι και αυτά με τη σειρά τους μια μορφή ψηφιακού νομίσματος, αλλά βρίσκονται σε κατηγορία διαφορετική από ότι τα εικονικά νομίσματα (Wagner Andrew, 2014). Μπορεί επομένως να γνωστοποιηθεί ότι τα ψηφιακά νομίσματα αποτελούν τη βασική κατηγορία νομισμάτων στην οποία εμπεριέχονται τόσο τα εικονικά νομίσματα όσο και τα κρυπτονομίσματα (Frankenfield Jake, Digital Currency, 2018).

Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι μπορούν και οι κεντρικές τράπεζες να εκδώσουν ψηφιακό νόμισμα το οποίο ονομάζεται Central Bank Digital Currency (CBDC) και αποτελεί ουσιαστικά την ψηφιακή μορφή των χρημάτων τα οποία τίθενται σε κυκλοφορία (Bank

for International Settlements, 2018). Είναι σημαντικό ωστόσο να μην συγχέεται το ψηφιακό νόμισμα της κεντρικής τράπεζας με το ψηφιακό νόμισμα το οποίο περιέχει τα εικονικά νομίσματα και τα κρυπτονομίσματα, διότι το τελευταίο δεν εκδίδεται από το κράτος και δεν αποτελεί, σύμφωνα με την κυβέρνηση, νόμιμο χρήμα.

3.2. Διαφορετικοί ορισμοί

Η Ευρωπαϊκή Κεντρική Τράπεζα (2012) όρισε το ψηφιακό νόμισμα ως *«ένα είδος εικονικού χρήματος το οποίο δεν διέπεται από κανονισμούς, εκδίδεται και ελέγχεται συνήθως από τους προγραμματιστές του και χρησιμοποιείται και γίνεται αποδεκτό μεταξύ των μελών μια συγκεκριμένης εικονικής κοινότητας»*.

Το Financial Crimes Enforcement Network (2013) όρισε το ψηφιακό νόμισμα ως *«ένα μέσο συναλλαγής που λειτουργεί ως συνάλλαγμα σε κάποια ορισμένα περιβάλλοντα, αλλά δεν έχει όλα τα χαρακτηριστικά του πραγματικού νομίσματος»*.

Η Ευρωπαϊκή Αρχή Τραπεζών (2014) όρισε το ψηφιακό νόμισμα ως *«μια εικονική αντιπροσώπευση της αξίας που δεν εκδίδεται ούτε από κάποια κεντρική τράπεζα, ούτε από κάποια δημόσια αρχή, καθώς και δεν συνδέεται υποχρεωτικά με ένα πραγματικό νόμισμα αλλά γίνεται δεκτό ως μέσω πληρωμής από φυσικά ή νομικά πρόσωπα και μπορεί να μεταφερθεί, να αποθηκευτεί και να ανταλλαχθεί ηλεκτρονικά»*.

Σύμφωνα με το Conference of State Bank Supervisors (2015) το ψηφιακό νόμισμα ορίζεται ως *«μια εικονική αντιπροσώπευση της αξίας και χρησιμοποιείται ως μέσο ανταλλαγής, ως λογιστική μονάδα ή ως αποθήκευση αξίας αλλά δεν είναι νόμιμο νόμισμα όπως αναγνωρίζεται από την κυβέρνηση των Ηνωμένων Πολιτειών. Το εικονικό νόμισμα δεν περιλαμβάνει το λογισμικό ή τα πρωτόκολλα για να μπορέσει να αποτελέσει την ψηφιακή αναπαράσταση της αξίας των πραγματικών νομισμάτων»*.

Όπως διακρίνεται στους παραπάνω ορισμούς γίνεται χρήση κυρίως της έννοιας του εικονικού νομίσματος και όχι του ψηφιακού. Η σωστή ορολογία για την αναφορά στις ηλεκτρονικές μορφές νομισμάτων είναι το ψηφιακό νόμισμα το οποίο συμπεριλαμβάνει τόσο τα εικονικά νομίσματα όσο και τα κρυπτονομίσματα, όμως η κυβέρνηση των Ηνωμένων Πολιτειών προτίμησε και υιοθέτησε τον όρο εικονικό νόμισμα. Το Financial Crimes Enforcement Network (2013) του Υπουργείου Οικονομικών των Ηνωμένων Πολιτειών ήταν το πρώτο που υιοθέτησε

την συγκεκριμένη ορολογία, ακολουθούμενο από το FBI (2012), καθώς και από άλλες κυβερνητικές υπηρεσίες. Αυτό συνέβη και συνεχίζει να συμβαίνει διότι, ενώ το εικονικό νόμισμα όπως φαίνεται και παραπάνω εμπεριέχεται στους νομούς αρκετών κρατών, δεν ισχύει το ίδιο και για το κρυπτονόμισμα, αφού το τελευταίο δεν είναι αποδεκτό ως νόμιμο νόμισμα συναλλαγής.

3.3. Ρύθμιση και έλεγχος ψηφιακού νομίσματος

Υπάρχουν δυο κατηγορίες ψηφιακών νομισμάτων ως προς τον τρόπο ρύθμισής τους, η πρώτη κατηγορία είναι το ψηφιακό νόμισμα να είναι ρυθμιζόμενο, δηλαδή να ελέγχεται και να ρυθμίζεται από κάποιον κεντρικό διαχειριστή. Αντιθέτως, η δεύτερη κατηγορία συνεπάγεται το ψηφιακό νόμισμα να μην είναι ρυθμιζόμενο, με άλλα λόγια να μην ελέγχεται και να μην επηρεάζεται από καμία κεντρική αρχή. Στην πρώτη περίπτωση του ρυθμιζόμενου ψηφιακού νομίσματος αντιστοιχεί το παράδειγμα της έκδοσης ψηφιακού νομίσματος από την Κεντρική Τράπεζα, το οποίο αποτελεί την ψηφιακή μορφή των πραγματικών χρημάτων που τίθενται σε κυκλοφορία. Στην δεύτερη περίπτωση στην οποία το ψηφιακό νόμισμα δεν είναι ρυθμιζόμενο αντιστοιχεί το εικονικό νόμισμα το οποίο τις περισσότερες φορές είναι ανεξέλεγκτο. Ομοίως, εξαιτίας της ανεξέλεγκτης φύσης τους τα κρυπτονόμισμα θεωρούνται ότι αποτελούν μέρος της ομάδας των εικονικών νομισμάτων (Frankenfield Jake, Virtual Currency, 2018).

Πιο αναλυτικά, ως προς τον έλεγχο των ψηφιακών νομισμάτων διακρίνονται δυο βασικές ιδιότητες, είτε να υπάρχει ένα κεντρικό σημείο ελέγχου είτε τα νομίσματα να είναι αποκεντρωμένα και ο έλεγχος να προέρχεται από διάφορες πηγές (Wikoff Shawn, 2016).

Κεντρικό σημείο ελέγχου

Σύμφωνα με το Financial Crimes Enforcement Network (2013) εικονικά νομίσματα με κεντρικό σημείο ελέγχου είναι εκείνα τα νομίσματα τα οποία έχουν ένα κεντρικό αποθετήριο, όπως μια Κεντρική Τράπεζα, και έναν κεντρικό διαχειριστή. Το ψηφιακό νόμισμα το οποίο έχει κεντρικό σημείο ελέγχου μπορεί να ανταλλαχθεί ηλεκτρονικά μέσα από χρεωστικές ή πιστωτικές κάρτες. Αυτή η ηλεκτρονική μεταφορά χρημάτων από τον ένα τραπεζικό λογαριασμό σε έναν άλλον χωρίς την άμεση μεσολάβηση της τράπεζας μπορεί να επιτευχθεί μέσω ενός ηλεκτρονικού τερματικού (POS), μέσω αυτομάτων μηχανημάτων ανάληψης μετρητών (ATM), μέσω κινητού τηλεφώνου ή μέσω ηλεκτρονικού υπολογιστή (Federal Reserve Board, 2008).

Αντίστοιχα, τα περισσότερα εικονικά νομίσματα σε κάποιο ηλεκτρονικό παιχνίδι έχουν ένα κεντρικό σημείο ελέγχου για την προσφορά του χρήματος το οποίο ρυθμίζεται συνήθως από τους αντίστοιχους προγραμματιστές του εικονικού κόσμου. Παραδείγματος χάριν, τα μαζικά διαδικτυακά παιχνίδια ρόλων για πολλαπλούς παίκτες (MMORPG) προσλαμβάνουν ειδικά εκπαιδευμένους οικονομολόγους για την διαχείριση των εκάστοτε εικονικών τους νομισμάτων. Επομένως, αν κριθεί απαραίτητο να αυξήσουν τα χρήματα τα οποία υπάρχουν μέσα στο παιχνίδι δημιουργούν κάποιες νέες αποστολές οι οποίες παρέχουν στους παίκτες ανταμοιβές σε εικονικά χρήματα. Από την άλλη, αν θελήσουν να μειώσουν τα εικονικά χρήματα του παιχνιδιού μπορούν να δημιουργήσουν νέα αντικείμενα, όπως οχήματα ή νέα αξεσουάρ χαρακτήρων τα οποία θα μπορούν να αγοράσουν οι παίκτες με τα εικονικά τους νομίσματα και έτσι να επιστρέφουν τα χρήματα πίσω στο παιχνίδι (Wagner Andrew, 2014).

Αποκεντρωμένα συστήματα

Ένα αποκεντρωμένο νόμισμα ορίστηκε από το Υπουργείο Οικονομικών των Ηνωμένων Πολιτειών της Αμερικής ως ένα νόμισμα το οποίο δεν έχει κεντρικό αποθετήριο και κανέναν διαχειριστή και τα άτομα μπορούν να το αποκτήσουν με δική τους υπολογιστική ή κατασκευαστική προσπάθεια (Financial Crimes Enforcement Network, 2013). Επομένως, το αποκεντρωμένο νόμισμα δεν στηρίζεται στην εμπιστοσύνη ως προς μια κεντρική αρχή, αλλά εξαρτάται από ένα συνολικό σύστημα εμπιστοσύνης (economist.com, 2013). Βασικό παράδειγμα αποκεντρωμένου συστήματος είναι το κρυπτονόμισμα, ένα είδος νομίσματος το οποίο βασίζεται στις αρχές της κρυπτογραφίας για την υλοποίησή του και επιτρέπει τις στιγμιαίες και χωρίς όρια συναλλαγές.

Έχοντας αναλύσει τους τρόπους ελέγχου του ψηφιακού νομίσματος διακρίνεται ότι στα αποκεντρωμένα συστήματα καμία κεντρική εξουσία δεν έχει τον έλεγχο για τον αριθμό των κρυπτονομισμάτων τα οποία υπάρχουν, σε αντίθεση με τα συστήματα με κεντρικό σημείο ελέγχου όπου, για παράδειγμα, μια ομάδα προγραμματιστών βιντεοπαιχνιδιών γνωρίζει ακριβώς τον αριθμό των εικονικών νομισμάτων που διαθέτει στους χρήστες. Δημοφιλή παιχνίδια όπως το World of Warcraft και το Second Life έχουν server τους οποίους διαχειρίζονται οι προγραμματιστές όπως επιθυμούν και θα μπορούσαν οποιαδήποτε στιγμή να τους κλείσουν τελείως. Αντιθέτως, το κρυπτονόμισμα εδρεύει σε ένα δίκτυο το οποίο απαρτίζεται από πολλούς υπολογιστές όπου όλοι έχουν συμφωνήσει σε συγκεκριμένους κανόνες και πρότυπα, γεγονός που καθιστά αδύνατη τη ξαφνική διακοπή λειτουργίας του (Wagner Andrew, 2014).

3.4. Είδη ψηφιακού νομίσματος

Όπως αναφέρθηκε και στην αρχή του κεφαλαίου το ψηφιακό νόμισμα εμπεριέχει δυο κατηγορίες νομισμάτων, το εικονικό νόμισμα και το κρυπτονόμισμα. Στην τρέχουσα ενότητα θα αναλυθούν πιο επεξηγηματικά οι δυο όροι προκειμένου να γίνουν καλύτερα κατανοητοί.

Εικονικό νόμισμα

Ονομάζεται το νόμισμα το οποίο ελέγχεται από τους προγραμματιστές, τον αντίστοιχο οργανισμό ίδρυσης του ή κάποιο πρωτόκολλο δικτύου (Frankenfield Jake, Digital Currency, 2018). Τα εικονικά νομίσματα υπάρχουν στις ζωές των ανθρώπων για πολύ περισσότερο καιρό από ότι υπάρχουν τα κρυπτονόμιστα και χρησιμοποιούνται κυρίως για την διαδικτυακή ψυχαγωγία και διασκέδαση σε εικονικούς κόσμους. Αυτή η μορφή ψηφιακού νομίσματος ονομάζεται εικονική διότι δεν βασίζεται στην πραγματικότητα, είναι κατά βάση δηλαδή πλασματική και τα συγκεκριμένα νομίσματα δεν προορίζονται για άμεση χρήση στην πραγματική ζωή αφού αποτελούν ουσιαστικά παιχνίδια.

Χαρακτηριστικό παράδειγμα αποτελεί το δημοφιλές ηλεκτρονικό παιχνίδι World of Warcraft, το οποίο είναι ιδιαίτερα αυστηρό όσον αφορά τα εικονικά του νομίσματα. Συγκεκριμένα, η Blizzard Entertainment, η εταιρεία η οποία δημιούργησε το συγκεκριμένο παιχνίδι είναι ιδιαίτερα προσεκτική στον συγκεκριμένο τομέα διότι δεν επιθυμεί νομικές παρεμβάσεις και φορολογήσεις οι οποίες θα προέλθουν αν αναγνωριστεί το εικονικό της νόμισμα ως νόμισμα με πραγματική αξία. Γι' αυτό το λόγο και προκειμένου να διατηρηθεί η αντίληψη ότι τα εικονικά της νομίσματα είναι ψεύτικα, η Blizzard Entertainment αναζητά συνεχώς λογαριασμούς οι οποίοι μπορεί να σχετίζονται με συναλλαγές πραγματικού χρήματος στην μαύρη αγορά και αν κάποιος παίκτης παραβιάσει τους συγκεκριμένους κανόνες τιμωρείται με μόνιμη απαγόρευση εισόδου στο παιχνίδι.



Εικ. 11. Η απογραφή των χρημάτων ενός παίκτη στο World of Warcraft

Ένα άλλο παράδειγμα αποτελεί ο εικονικός κόσμος του Second Life ο οποίος δημιουργήθηκε από την Linden Lab και λειτουργεί ως ένα προσομοιωτής της πραγματικής ζωής. Η Linden Lab αν και ελέγχει τον αριθμό των δολαρίων Linden (Linden Dollars) τα οποία υπάρχουν στο παιχνίδι, ανέχεται και την ανταλλαγή δολαρίων Linden με πραγματικά νομίσματα. Αυτό σημαίνει ότι ένας παίκτης μπορεί να ζήσει στην πραγματική του ζωή με το

εισόδημα που αποκτά μέσα από μια επιτυχημένη επιχείρηση στο παιχνίδι. Ωστόσο, τα δολάρια Linden εξακολουθούν να είναι μορφή εικονικού νομίσματος διότι δεν εξαργυρώνονται άμεσα για πραγματικά αγαθά ή υπηρεσίες. Δεν είναι δύσκολο να γίνει αντιληπτό όμως, πως κάποιοι παίκτες μπορεί να έχουν φτιάξει όλη τους την περιουσία στον πραγματικό κόσμο με τη βοήθεια του συγκεκριμένου παιχνιδιού, ωστόσο ακόμα και σήμερα το Second Life παραμένει απλά ένα παιχνίδι (Wagner Andrew, 2014 & Ευρωπαϊκή Κεντρική Τράπεζα, 2012).

Κρυπτονόμισμα

Το κρυπτονόμισμα είναι άλλο ένα είδος ψηφιακού νομίσματος το οποίο βασίζεται κυρίως στην επιστήμη των μαθηματικών και της κρυπτογραφίας και λειτουργεί ως μέσο ανταλλαγής. Πιο αναλυτικά, δημιουργείται μέσα από την επίλυση μαθηματικών προβλημάτων και με τη βοήθεια της κρυπτογραφίας, δηλαδή με την δημιουργία αλγορίθμων, κωδικών και μαθηματικών αποδείξεων, αποκρύπτει πληροφορίες, διασφαλίζει και επαληθεύει τις συναλλαγές, καθώς παράλληλα βοηθά στη διαχείριση και τον έλεγχο της δημιουργίας νέων νομισματικών μονάδων. Τα δίκτυα των κρυπτονομισμάτων είναι ανοικτά στο κοινό και οποιοσδήποτε μπορεί να ενταχθεί και να ξεκινήσει συναλλαγές με βάση αυτού του είδους τα ψηφιακά νομίσματα (Frankenfield Jake, Virtual Currency, 2018).

Το βασικό σκεπτικό πίσω από την έννοια του κρυπτονομίσματος είναι ότι λειτουργεί από μια αποκεντρωμένη αρχή, ώστε να είναι ανθεκτικό σε κάθε προσπάθεια για έλεγχο ή παρέμβαση και οι συναλλαγές γίνονται από τον ένα συναλλασσόμενο στον άλλον μέσω διαδικτύου χωρίς κάποιος ενδιάμεσος να πιστοποιεί την μεταξύ τους συναλλαγή, δηλαδή χωρίς τη συμμετοχή των συμβατικών τραπεζών (Frankenfield Jake, 2013). Εξαιτίας της μη ύπαρξης ενδιάμεσου πιστοποιητή δεν υπάρχει χρέωση επί της συναλλαγής, γι' αυτό το λόγο τα κρυπτονομίσματα προσφέρουν την υπόσχεση χαμηλότερων τελών συναλλαγών από ότι οι παραδοσιακοί μηχανισμοί ηλεκτρονικών πληρωμών (Frankenfield Jake, 2013). Αυτή η αποκεντρωμένη συναλλαγή μέσω διαδικτύου μεταξύ δυο διαφορετικών συναλλαζόμενων, οι οποίοι έρχονται σε συμφωνία μέσω ενός μοναδικού σημείου διαμεσολάβησης, ονομάζεται peer-to-peer και βασίζεται στις αρχές της κρυπτογραφίας τόσο για την ασφάλεια και την προστασία των συναλλαζόμενων αλλά και για τη σωστή επαλήθευση των συναλλαγών (Σπαθάς Βαγγέλης, 2017).

Αξιοσημείωτο είναι ότι οι λόγοι οι οποίοι οδήγησαν στην δημιουργία των κρυπτονομισμάτων δεν είναι άλλοι από την αβεβαιότητα και την έλλειψη εμπιστοσύνης και αξιοπιστίας των πολιτών τόσο ως προς τα χρηματοπιστωτικά ιδρύματα όσο και ως προς τις κυβερνήσεις για θέματα φερεγγυότητας και ρευστότητας. Συνάμα, οι συνεχείς μεταβολές στις χρηματοοικονομικές αγορές συνέβαλαν εξίσου στην ανάπτυξη τέτοιου είδους αρνητικών συναισθημάτων ως προς τον μέχρι τώρα γνωστό τρόπο συναλλαγών και οδήγησαν στην ανάγκη για ένα νέο καινοτόμο μέσο πληρωμών το οποίο μπορεί να αντικαθιστά τους μέχρι τώρα διαμεσολαβητές με την κρυπτογραφία.

Η λίστα των διαθέσιμων κρυπτονομισμάτων στις μέρες μας είναι μεγάλη, όμως τα πιο διάσημα κρυπτονομίσματα θεωρούνται το Bitcoin και το Ethereum (Frankenfield Jake, Digital Currency, 2018). Από τη στιγμή δημιουργίας του το Bitcoin ονομάστηκε το χρήμα του διαδικτύου και κέρδισε σημαντικό έδαφος στις ηλεκτρονικές αγορές, όμως στη σημερινή εποχή δύνανται να χρησιμοποιηθούν bitcoins και σε πραγματικές με φυσική υπόσταση επιχειρήσεις. Αυτό καθιστά τα κρυπτονομίσματα παρόμοια με τα παραδοσιακά χρήματα και πιο αληθινά, έναντι άλλων ψηφιακών νομισμάτων. Ούτως ή άλλως, τα κρυπτονομίσματα σχεδιάστηκαν με τέτοιο τρόπο ώστε κάποια στιγμή στο μέλλον να είναι σε θέση να αντικαταστήσουν τα μετρητά (Wagner Andrew, 2014).

3.5. Κατηγορίες εικονικών νομισμάτων

Το κρυπτονόμισμα είναι η βασική μορφή ψηφιακού νομίσματος με την οποία θα ασχοληθεί η παρούσα πτυχιακή εργασία, ωστόσο σωστή θα ήταν η αναφορά σε γενικό βαθμό και στις βασικές κατηγορίες των εικονικών νομισμάτων. Πρωτίστως, πρέπει να αναφερθεί πως υπάρχουν δυο βασικές κατηγορίες σύμφωνα με τον τρόπο με τον οποίο μπορεί κάποιος να αποκτήσει εικονικά νομίσματα. Αρχικά, ο πρώτος τρόπος είναι χρησιμοποιώντας παραστατικά χρήματα προκειμένου να αγοράσει ένα αντίστοιχο προσυμφωνημένο ποσό εικονικών νομισμάτων, ενώ αντίστοιχα ο δεύτερος τρόπος είναι η αύξηση του αποθέματος εικονικών νομισμάτων ενός ατόμου μέσα από διάφορες συγκεκριμένες δραστηριότητες όπως για παράδειγμα απαντώντας σε μια προσφορά ή κάποια διαφήμιση ή με τη συμπλήρωση κάποιας ηλεκτρονικής έρευνας (Ευρωπαϊκή Κεντρική Τράπεζα, 2012). Όμως, εκτός από τους τρόπους απόκτησης εικονικών νομισμάτων ιδιαίτερα μεγάλης σημασίας είναι και οι κατηγορίες αυτών των νομισμάτων που υπάρχουν στην σημερινή εποχή.

Κλειστά εικονικά νομίσματα

Τα εικονικά νομίσματα ονομάζονται κλειστά, φανταστικά ή ψεύτικα όταν δεν έχουν επίσημη σχέση με την πραγματική οικονομία και το παραστατικό χρήμα. Αυτή η μορφή εικονικών νομισμάτων ουσιαστικά δεν έχει καμία αξία εκτός του εκάστοτε ηλεκτρονικού παιχνιδιού αφού δεν μπορεί να αγορασθεί ή να πουληθεί (Korolon Maria, 2012). Τέτοια νομίσματα είναι τα εικονικά νομίσματα που εμφανίζονται σε μαζικά διαδικτυακά παιχνίδια ρόλων για πολλαπλούς παίκτες (MMORPG), όπως το World of Warcraft της Blizzard Entertainment, ή σε κάποιο οικογενειακό επιτραπέζιο παιχνίδι, όπως η Monopoly.

Συνήθως οι παίκτες πληρώνουν κάποια συνδρομή, όσον αφορά τα ηλεκτρονικά παιχνίδια, η οποία τους επιτρέπει να αγοράζουν προϊόντα και υπηρεσίες εντός του εικονικού κόσμου με τη βοήθεια των εικονικών νομισμάτων, χωρίς να επιτρέπουν την ανταλλαγή αυτών των νομισμάτων για νόμιμα χρήματα. Υπάρχει ωστόσο και μια πιο γκρίζα αγορά η οποία επιτρέπει την ανταλλαγή τέτοιων νομισμάτων, για παράδειγμα το παιχνίδι Second Life, καθώς και άλλων εικονικών περιουσιακών στοιχείων για περιουσιακά στοιχεία πραγματικού κόσμου, όμως συνήθως αυτό απαγορεύεται από τους όρους των παιχνιδιών.

Εικονικά νομίσματα κλειστού βρόχου

Αυτός ο τύπος νομισμάτων είναι γνωστός για πολύ μεγάλο χρονικό διάστημα με τη μορφή κουπονιών. Το πρώτο γνωστό κουπόνι στην ιστορία προέρχεται από τις Ηνωμένες Πολιτείες της Αμερικής και τον Asa Candler,

εφευρέτη της Coca-Cola, ο οποίος εξέδωσε κουπόνια για δωρεάν ποτά το 1887. Στη συνέχεια, σειρά έχει ο Charles William Post με τα κουπόνια στα κουτιά δημητριακών Grape-Nuts το 1895 (New York Magazine, 1992, σελ. 18). Τέτοιου είδους κουπόνια έμειναν στην αγορά για πάνω από 100 χρόνια μέχρι να εξελιχθεί η τεχνολογία και να κάνουν την εμφάνισή τους οι πιστωτικές κάρτες, τη δεκαετία του 1980, όποτε και δημιουργήθηκαν νέες μορφές επιβράβευσης των καταναλωτών μέσα από τη χρήση των πιστωτικών καρτών.



[α]



[β]

Εικ.12. Τα πρώτα κουπόνια της Coca-Cola

Οι πιστωτικές κάρτες οδήγησαν στην αύξηση του ηλεκτρονικού και διαδικτυακού εμπορίου, καθώς και των ηλεκτρονικών υπηρεσιών, των διαδικτυακών κοινοτήτων και των παιχνιδιών. Θα μπορούσε και σήμερα το εικονικό νόμισμα να παρουσιαστεί ως ένα κουπόνι,

με χαρακτηριστικά παραδείγματα τα Microsoft Points, τα Nintendo Points, τα Facebook Credits, τα Amazon Coins, τα αεροπορικά μίλια καθώς και οποιαδήποτε προπληρωμένη κάρτα μπορεί κάποιος να προμηθευτεί από ένα εστιατόριο ή ένα κατάστημα. Τα εικονικά νομίσματα κλειστού βρόχου δεν μπορούν να εξαργυρωθούν πάρα μόνο στην εταιρεία που τα εξέδωσε. Βέβαια, υπάρχει και μια μικρή ομάδα ατόμων που πουλάει τέτοιου είδους εικονικά νομίσματα μέσα σε διάφορες σελίδες αγοροπωλησίας, όπως το eBay (Korolov Maria, 2012).

Μετατρέψιμα εικονικά νομίσματα

Μετατρέψιμο είναι ένα εικονικό νόμισμα το οποίο λειτουργεί όπως ένα άλλο οποιοδήποτε νόμιμο νόμισμα και μπορεί να χρησιμοποιηθεί τόσο στην αγορά εικονικών αγαθών και υπηρεσιών, όσο και στην αγορά πραγματικών αγαθών και υπηρεσιών (Ευρωπαϊκή Κεντρική Τράπεζα, 2012). Χαρακτηριστικό παράδειγμα αποτελεί το OMC (Open Metaverse Currency) ένα νόμισμα το οποίο δημιουργήθηκε από τη VirWox και χρησιμοποιείται για την αγορά και πώληση εικονικών αγαθών και υπηρεσιών σε εικονικά περιβάλλοντα. Έχει γίνει αποδεκτό σε πολλούς εικονικούς κόσμους και λειτουργεί σε OpenSim HyperGrid περιβάλλοντα. Το OMC μπορεί να εξαργυρωθεί σε μετρητά ή να ανταλλαχθεί για διαφορά άλλα ψηφιακά νομίσματα, όπως Linden δολάρια και κρυπτονομίσματα, όπως Bitcoin (virwox.com).

Κεφάλαιο 4: Η τεχνολογία της Blockchain

4.1. Ορισμός της Blockchain

Προκειμένου να καταφέρει κάποιος να κατανοήσει την έννοια του κρυπτονομίσματος και να αντιληφθεί τους αλγορίθμους και τις διαδικασίες που το διέπουν θα πρέπει πρωτίστως να καταλάβει την βασική τεχνολογία πάνω στην οποία είναι χτισμένα όλα τα ευρέως γνωστά στην σημερινή εποχή κρυπτονομίσματα. Αυτή η επαναστατική τεχνολογία ονομάζεται blockchain και αποτελεί ένα από τα σημαντικότερα κομμάτια στην εξέλιξη της τεχνολογίας, διότι παρέχει μια νέα υποδομή για την κατασκευή καινοτόμων εφαρμογών, τόσο όσον αφορά τα κρυπτονομίσματα όσο και εκτός αυτών, οδηγώντας σε σημαντικές και θεμελιώδεις αλλαγές στις επιχειρήσεις, τις κοινότητες και την κοινωνία (accenture.com, Blockchain).

Σε επιστημονικό βαθμό η blockchain ορίζεται ως μια ψηφιακή έννοια και αποτελεί έναν νέο τρόπο αποθήκευσης δεδομένων σε έναν κατακευκτισμένο περιβάλλον, ο οποίος επιτρέπει σε πολλούς ενδιαφερόμενους να μοιράζονται με σιγουριά και ασφάλεια την πρόσβαση στις ίδιες πληροφορίες (accenture.com, Blockchain). Τα δεδομένα αυτά εμφανίζονται σε μορφή block τα οποία είναι αλυσοδεμένα μεταξύ τους, ιδιότητα που τα καθιστά αμετάβλητα. Πιο συγκεκριμένα τα δεδομένα από τη στιγμή που θα προστεθούν στη blockchain δεν μπορούν με κανέναν τρόπο να αλλάξουν ή να αφαιρεθούν από την αλυσίδα. Επιπρόσθετα, χαρακτηριστικό της blockchain των κρυπτονομισμάτων είναι πως όλες οι πληροφορίες παραμένουν πάντοτε δημόσιες και διαθέσιμες προς όλους. Με λίγα λόγια, οποιοσδήποτε μπορεί να ανατρέξει στις συγκεκριμένες πληροφορίες οποιαδήποτε στιγμή επιθυμεί.

Η ιδέα της δημιουργίας της blockchain καθώς και ο τρόπος λειτουργίας της αποτελούν ουσιαστική επανάσταση στον χώρο των τεχνολογικών εξελίξεων, διότι επιτρέπουν την αποθήκευση και την παρακολούθηση όλων των πληροφοριών των χρηστών χωρίς να υπάρχει κίνδυνος αυτά τα αρχεία να παραβιαστούν ή να μεταποιηθούν. Τέτοια αρχεία θα μπορούσαν να είναι ιατρικά έγγραφα, ταυτότητες, υπόλοιπα χρημάτων καθώς και δικαιώματα ιδιοκτησίας. Παραδείγματος χάριν, αν ένας χρήστης αποφάσιζε σήμερα να αγοράσει ένα σπίτι και έπειτα πρόσθετε τους τίτλους και τα δικαιώματα ιδιοκτησίας σε ένα block μέσα στη blockchain τότε θα ήταν σε θέση οποιαδήποτε στιγμή να ανατρέξει στο συγκεκριμένο block και να αποδείξει ότι εκείνη τη χρονική στιγμή είχε αυτά τα δικαιώματα. Συμπερασματικά, οι πληροφορίες οι οποίες υπάρχουν στη blockchain δεν μπορούν να τροποποιηθούν ποτέ ξανά έπειτα από την

καταχώρηση τους στα block. Αυτό δίνει τη δυνατότητα σε όλους του χρήστες να αποθηκεύουν δεδομένα τα οποία παραμένουν αμετάβλητα (S. Jimi, 2018).

Η κατανόηση όμως της blockchain είναι αρκετά δύσκολη και οι έννοιες που την αποτελούν είναι ιδιαίτερα δυσνόητες. Ωστόσο η βασική δυσκολία κατανόησης ανέρχεται στο γεγονός ότι δεν είναι ξεκάθαρο το πρόβλημα το οποίο επιλύει και ο λόγος ύπαρξης της. Μέσα από το επόμενο παράδειγμα απλοποιείται η ανάγκη της blockchain στις συναλλαγές. Στη σημερινή εποχή αν κάποιος αποφάσιζε να κάνει μια μεταφορά χρημάτων από τον τραπεζικό του λογαριασμό στον τραπεζικό λογαριασμό ενός συγγενικού του προσώπου, για παράδειγμα σε μια θεία του στην Αυστραλία, τότε θα ακολουθούσε την εξής διαδικασία:

- Πρωτίστως, θα επικοινωνούσε με την τράπεζα είτε τηλεφωνικά, είτε ηλεκτρονικά μέσω κάποιας ιστοσελίδας, είτε πηγαίνοντας αυτοπροσώπως σε κάποιο κατάστημα. Έπειτα, θα ζήτηγε να μεταφερθεί το Χ συμφωνημένο ποσό από τον δικό του τραπεζικό λογαριασμό στον τραπεζικό λογαριασμό της θείας του.
- Αυτό θα είχε ως αποτέλεσμα ο τραπεζικός υπάλληλος να ανατρέξει στον τραπεζικό του λογαριασμό, να ελέγξει αν ο αποστολέας διαθέτει αρκετά χρήματα ώστε να γίνει η επιθυμητή συναλλαγή και στη συνέχεια να πραγματοποιήσει τη συναλλαγή δίνοντας στη θεία άμεση πρόσβαση στα χρήματα τα οποία της έστειλε ο ανιψιός της.

Είναι προφανές πως μέσα από μια τέτοιου είδους συναλλαγή η εμπιστοσύνη μεταβιβάζεται εξολοκλήρου την τράπεζα προκειμένου να πραγματοποιηθεί σωστά και με ασφάλεια η μεταφορά των χρημάτων χρησιμοποιώντας το ηλεκτρονικό της τραπεζικό σύστημα. Ένα σύστημα στο οποίο ούτε ο αποστολέας αλλά ούτε και ο παραλήπτης μπορούν να αποκτήσουν πρόσβαση και εν τέλει δεν είναι σε θέση να διαχειριστούν.

Συνεπώς, το γεγονός ότι η εμπιστοσύνη μεταφέρεται σε ένα τρίτο πρόσωπο ή οργανισμό για να πραγματοποιηθούν οι προσωπικές συναλλαγές αποτελεί και το πρόβλημα το οποίο δημιουργείται μέσα από μια τέτοιου είδους συναλλαγή. Με άλλα λόγια όλοι οι άνθρωποι βασίζονται στην τράπεζα ότι ως μεσάζοντας δεν θα τους προδώσει, ότι ο τραπεζικός υπάλληλος θα σημειώσει το σωστό χρηματικό ποσό και δεν θα κάνει κάποιο αριθμητικό λάθος αλλά και ότι το σύστημα της τράπεζας δεν θα καταρρεύσει. Όμως δεν μπορεί να είναι ποτέ κανείς σίγουρος ότι όλα θα δουλεύουν σωστά και θα υπάρχει πάντοτε ένα αίσθημα ανασφάλειας από τη στιγμή που η όλη διαδικασία αναλαμβάνεται εξολοκλήρου από την τράπεζα. Σε αυτό το κομμάτι

εναντιώνεται η τεχνολογία της blockchain, η οποία δεν εξαρτάται από την παρέμβαση κάποιου τρίτου προσώπου ή οργανισμού ώστε να πραγματοποιηθεί μια συναλλαγή, αλλά βασίζεται εξολοκλήρου στους χρήστες του δικτύου της.

4.2. Τρόπος λειτουργίας

Έχοντας αποκτήσει τη βασική γνώση σχετικά με το πρόβλημα το οποίο επιλύει η χρήση της blockchain θα πρέπει να γίνει κατανοητό και το πως λειτουργεί αυτή η καινοτόμα τεχνολογία. Αρχικά, βασική προϋπόθεση αποτελεί να υπάρχουν αρκετοί άνθρωποι οι οποίοι έχουν την ίδια αντίληψη και επιθυμούν να κατέχουν τον πλήρη έλεγχο των συναλλαγών τους δίχως να εξαρτώνται από κάποιο μεσάζοντα για την πραγματοποίηση αυτών. Μόνο κατέχοντας ένα μεγάλο πλήθος μελών θα μπορέσει αυτή η ομάδα να διατηρήσει και να πραγματοποιήσει μονή της τις συναλλαγές της.

Σύμφωνα με τους Mamoria Mohit (2017), Dossman Jack (2018) και S. Jimi (2018) τα βήματα για τη δημιουργία της blockchain ενός κρυπτονομίσματος είναι ως εξής:

Δημιουργία των blocks

Υποθέτοντας πως δημιουργείται μια ομάδα 10 ατόμων τα οποία αποφάσισαν ότι δεν θέλουν πλέον να ελέγχονται και να εξαρτώνται από τράπεζες, χρηματοπιστωτικά ιδρύματα, κυβερνήσεις και ενδιάμεσους μεσολαβητές. Ως πρωταρχικό βήμα όλα τα μέλη της ομάδας θα πρέπει να συμφωνήσουν μεταξύ τους ώστε να αποκτήσουν όλοι πρόσβαση στις λεπτομέρειες των λογαριασμών όλων των υπολοίπων μελών χωρίς όμως να ανταλλάξουν τα προσωπικά τους στοιχεία. Αυτή η ομάδα που δημιουργείται αποτελεί πλέον το δίκτυο της blockchain.

Στη συνέχεια, θα δοθεί στο κάθε μέλος της ομάδας από ένας ηλεκτρονικός υπολογιστής ο οποίος θα περιέχει μόνο έναν άδειο φάκελο. Ο κάθε ηλεκτρονικός υπολογιστής ονομάζεται node και αποτελεί έναν κόμβο από το ενιαίο δίκτυο. Στους φακέλους που εμπεριέχονται σε αυτούς τους ηλεκτρονικούς υπολογιστές θα αρχίσουν σιγά σιγά τα μέλη τα αποθηκεύουν αρχεία στα οποία θα είναι καταγεγραμμένες όλες οι συναλλαγές οι οποίες θα γίνονται στο δίκτυο. Για να λειτουργήσει σωστά το δίκτυο θα πρέπει όλα τα μέλη της ομάδας να καταγράφουν όλες τις συναλλαγές που γίνονται τη χρονική στιγμή την οποία γίνονται.

Για να γίνει περισσότερο κατανοητό το συγκεκριμένο βήμα θα χρησιμοποιηθεί το ακόλουθο παράδειγμα. Έστω ότι το μέλος με τον αριθμό 3, ο Γιάννης θέλει να στείλει 100€ στο μέλος με τον αριθμό 6, τον Γιώργο. Για να πραγματοποιηθεί η συναλλαγή πρέπει ο Γιάννης να ενημερώσει όλα τα υπόλοιπα μέλη της ομάδας ότι επιθυμεί να μεταφέρει αυτό το χρηματικό ποσό στον Γιώργο. Όλα τα υπόλοιπα μέλη, πρέπει να ελέγξουν αν ο Γιάννης έχει αρκετό υπόλοιπο χρημάτων στο λογαριασμό του ώστε να ολοκληρωθεί η συναλλαγή. Αν το ποσό επαρκή, τότε όλοι σημειώνουν τη συναλλαγή στα αρχεία τους και η μεταφορά των χρημάτων πραγματοποιείται με επιτυχία.

Για μεγαλύτερη διευκόλυνση, αυτά τα αρχεία παρουσιάζονται με απλά έγγραφα κειμένου όπου σε κάθε σειρά αναγράφεται το όνομα του ατόμου το οποίο αποστέλλει το εκάστοτε χρηματικό ποσό, το όνομα του ατόμου το οποίο λαμβάνει το ποσό και στο τέλος το χρηματικό ποσό το οποίο μεταφέρθηκε από τον έναν συναλλασσόμενο στον άλλον. Για το παραπάνω παράδειγμα, η σειρά θα είχε την εξής μορφή:

Γιάννης → Γιώργος → 100€

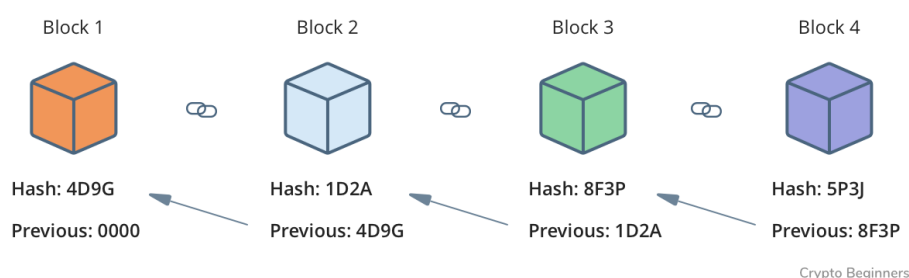
Οι συναλλαγές πρέπει να καταγράφονται με χρονολογική σειρά και το κάθε αρχείο περιέχει έναν συγκεκριμένο αριθμό συναλλαγών, για παράδειγμα έστω ότι σε κάθε αρχείο υπάρχει η δυνατότητα να σημειωθούν μέχρι 20 συναλλαγές, δηλαδή 20 σειρές, πριν γεμίσει ο χώρος. Όταν ολοκληρωθούν οι 20 συναλλαγές πρέπει το συγκεκριμένο αρχείο να αποθηκευτεί στο φάκελο του υπολογιστή και έπειτα να δημιουργηθεί ένα νέο αρχείο για να συνεχιστεί η καταγραφή των επομένων συναλλαγών. Οι συναλλαγές συνεχίζουν και κάθε φορά ακολουθείται η ίδια διαδικασία με όλο και περισσότερα άτομα να θέλουν να μεταφέρουν χρήματα σε άλλους. Αυτά τα αρχεία τα οποία αποθηκεύονται στον φάκελο αποτελούν τα blocks και το πρώτο αρχείο του φακέλου αποτελεί το genesis block της blockchain.

Η υπογραφή των blocks

Τα παραπάνω αρχεία τα οποία δημιουργήθηκαν είναι συνδεδεμένα – αλυσοδεμένα μεταξύ τους. Για να γίνει αυτό, κάθε block σφραγίζεται με μια ειδική υπογραφή η οποία αναφέρεται στα δεδομένα τα οποία υπάρχουν στο εκάστοτε block και στην οποία έχουν συμφωνήσει όσοι βρίσκονται μέσα στο δίκτυο. Αυτό συμβαίνει προκειμένου να διασφαλιστεί πως κανένας δεν θα μπορέσει να κάνει αλλαγές σε αυτό το αρχείο αφού

καθένα από τα μέλη της ομάδας θα έχει ένα αντίγραφο του. Αν για κάποιο λόγο κάτι αλλάξει μέσα στο block, έστω και ένα μόνο ψηφίο, τότε το block θα αποκτήσει μια καινούργια υπογραφή. Αυτή η υπογραφή αποτελεί και την ουσία της τεχνολογία της blockchain. Παρόμοια με το προηγούμενο παράδειγμα στο οποίο η τράπεζα παρείχε στον αποστολέα την σιγουριά ότι δεν θα αλλάξει ποτέ η συναλλαγή που πραγματοποιήθηκε έτσι και σε αυτό το αποκεντρωμένο σύστημα, η υπογραφή παρέχει αυτή την εμπιστοσύνη.

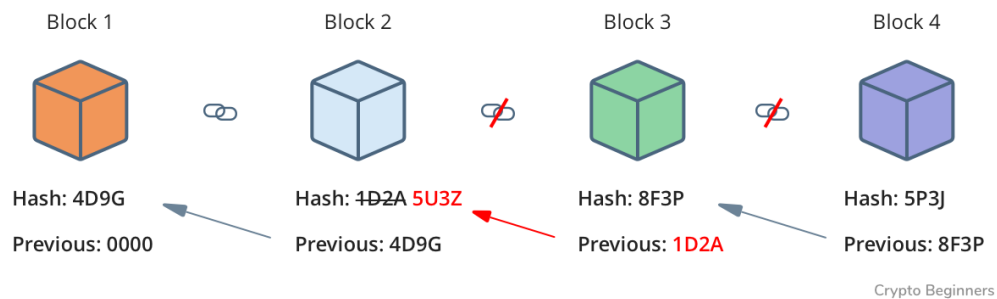
Επιστρέφοντας στο παράδειγμα της συναλλαγής μεταξύ του Γιάννη και του Γιώργου και θεωρώντας υποθετικά πως αυτή η συναλλαγή είναι η 20^η συναλλαγή του αρχείου τότε έχει φτάσει η στιγμή το αρχείο να δεχτεί μια υπογραφή και να αποθηκευτεί. Η υπογραφή που δέχεται το αρχείο είναι τυχαία και έχει τη μορφή Z89. Σύμφωνα με τους κανόνες της blockchain, το επόμενο αρχείο (block) που θα δημιουργηθεί πρέπει να είναι συνδεδεμένο με το προηγούμενο αρχείο. Αυτό επιτυγχάνεται με τη χρήση της υπογραφής του πρώτου αρχείου για την δημιουργία του δεύτερου αρχείου. Με άλλα λόγια, το δεύτερο αρχείο το οποίο θα δημιουργηθεί, εκτός από τις νέες συναλλαγές που θα πραγματοποιηθούν θα περιέχει στα δεδομένα του και την υπογραφή του πρώτου αρχείου. Επομένως, μετέπειτα η υπογραφή του αρχείου 2 θα βασίζεται και στην υπογραφή του αρχείου 1. Στη συνέχεια, το αρχείο 3 θα βασίζεται στην υπογραφή του αρχείου 2, το αρχείο 4 θα βασίζεται στην υπογραφή του αρχείου 3 και ούτω καθεξής. Με αυτόν τον τρόπο δημιουργείται η σύνδεση και η αλληλουχία μεταξύ των blocks ώστε να υλοποιηθεί τελικώς η αλυσίδα των blocks ονόματι blockchain.



Εικ.13. Η υπογραφή των blocks

Στην περίπτωση που τα δεδομένα στο αρχείο 1 τροποποιηθούν ψευδώς και αντί για 100€ ο Γιάννης υποτίθεται ότι έστειλε στον Γιώργο 500€, τότε αμέσως το σύστημα αντιλαμβάνεται ότι έχουν αλλάξει τα δεδομένα στο αρχείο 1 και όντας διαφορετικά από ότι πριν ζητάει από το block 1 να αποκτήσει μια καινούργια υπογραφή. Η καινούργια υπογραφή δεν θα είναι η Z89 όπως προηγουμένως αλλά θα αλλάξει και θα δημιουργηθεί μια νέα, για

παράδειγμα XT8. Αυτή η νέα υπογραφή δεν αντιστοιχεί πλέον στην υπογραφή που περιέχεται στο αρχείο 2 οπότε πλέον το block 1 και το block 2 δεν είναι συνδεδεμένα μεταξύ τους. Αυτό έχει ως αποτέλεσμα να ειδοποιηθούν όλα τα μέλη της ομάδας ότι τα δεδομένα στο αρχείο 1 έχουν αλλάξει και στη συνέχεια τα μέλη απορρίπτουν την αλλαγή και αντικαθιστούν το αρχείο 1 με την αρχική του μορφή, ώστε τελικά όλα τα blocks να είναι συνδεδεμένα μεταξύ τους.

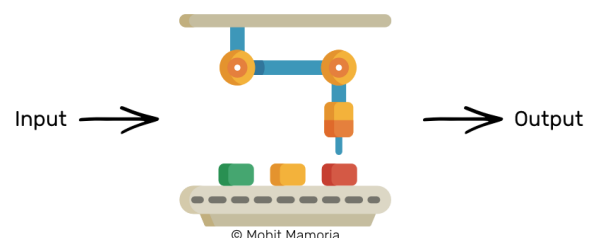


Εικ.14. Δημιουργία νέων υπογραφών με την τροποποίηση των δεδομένων στο Block 2

Ο μόνος τρόπος για να μην γίνει αντιληπτή η αλλαγή των δεδομένων στο αρχείο 1 είναι αν τα blocks παραμείνουν αλυσοδεμένα μεταξύ τους. Αυτό σημαίνει, ότι η υπογραφή του αρχείου 1 θα πρέπει να αντικαταστήσει την υπογραφή που υπάρχει μέσα στο αρχείο 2 και έτσι το αρχείο 2 θα αποκτήσει και αυτό με την σειρά του μια νέα υπογραφή. Όπως μπορεί να γίνει ευκολά αντιληπτό, αν αλλάξει η υπογραφή του αρχείου 2 θα πρέπει μετέπειτα να αλλάξει και η υπογραφή του αρχείου 3 και μετά του αρχείου 4 και ούτω καθεξής, πράγμα το οποίο θεωρείται ακατόρθωτο.

Δημιουργία της υπογραφής

Η υπογραφή με την οποία σφραγίζεται κάθε block της αλυσίδας δημιουργείται με μια κρυπτογραφική μέθοδο με το όνομα hash, δηλαδή κατακερματισμός. Η συγκεκριμένη μέθοδος αποτελείται από πολύ περίπλοκους αλγορίθμους οι οποίοι παίρνουν ένα κείμενο εισόδου και παράγουν ένα μοναδικό κείμενο εξόδου με 64 χαρακτήρες το οποίο αποτελεί κάτι τελείως καινούργιο που δεν έχει καμία σχέση με την είσοδο που δόθηκε.



Εικ.15. Η μέθοδος κατακερματισμού hash

Ως τυχαίο παράδειγμα, αν δοθεί στην μέθοδο αυτή ως είσοδος η λέξη «Κρυπτονόμισμα» το κείμενο εξόδου θα ήταν της μορφής:

H5D8IKRLOPS09J4HDFYURJ4MFYDKSOP3JRU7L2K4JD7JRSITJRH
B
FUWEBJF95H4D

Αν όμως αλλάξει ένα γράμμα από το κείμενο εισόδου, είτε αυτό είναι κάποιο κενό, είτε είναι η αλλαγή κάποιου γράμματος σε κεφαλαίο, είτε η προσθήκη κάποιας τελείας ή κάποιου κόμματος, τότε το κείμενο εξόδου θα έχει τελείως διαφορετική μορφή, για παράδειγμα έστω ότι η είσοδος μετατρέπεται σε «Κρυπτονόμισμα!!» τότε η έξοδος θα είναι της μορφής:

JDDUEJEH33I8YRBR32K2J3HDI84H DUH4R4EHFRHNDCNDCJEH2H3
HRJKFJKJRB3F

Αν η είσοδος γινόταν ίδια με πριν, δηλαδή «Κρυπτονόμισμα» τότε το αποτέλεσμα θα άλλαζε πάλι στο αρχικό:

H5D8IKRLOPS09J4HDFYURJ4MFYDKSOP3JRU7L2K4JD7JRSITJRH
B
FUWEBJF95H4D

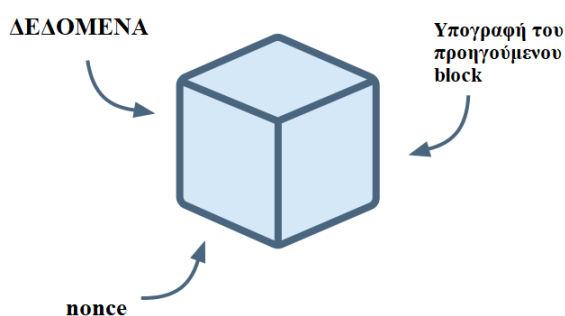
Διακρίνεται ότι αν δοθεί στην μέθοδο κατακερματισμού hash το ίδιο κείμενο εισόδου τότε το κείμενο εξόδου παραμένει το ίδιο κάθε φορά, ενώ μια διαφορετική είσοδος δίνει μια διαφορετική έξοδο. Με αυτή λοιπόν τη μέθοδο δίνεται σε κάθε block η υπογραφή του και ως είσοδο λαμβάνει τα δεδομένα του εκάστοτε αρχείου και ως έξοδο παράγει την αντίστοιχη υπογραφή που αναφέρεται σε αυτά.

Η σωστή υπογραφή

Μια υπογραφή η οποία δημιουργείται μέσα από τη μέθοδο κατακερματισμού δεν είναι πάντοτε η σωστή, και αυτό εξαρτάται ανάλογα από τις προϋποθέσεις της κάθε blockchain. Για παράδειγμα, στη blockchain που χρησιμοποιείται στο κρυπτονόμισμα Bitcoin ένα block μπορεί να γίνει δεκτό στην αλυσίδα των blocks μόνο αν η υπογραφή ξεκινάει από ένα συγκεκριμένο αριθμό μηδενικών. Παρόλα αυτά, όπως επισημάνθηκε προηγουμένως ένα συγκεκριμένο κείμενο εισόδου δίνει μια συγκεκριμένη έξοδο μέσα από την μέθοδο κατακερματισμού και αφού το κείμενο εισόδου απαγορεύεται να αλλάξει στοιχεία, φαίνεται ακατόρθωτο να δημιουργηθεί μια έξοδος η οποία να ξεκινάει με συγκεκριμένο αριθμό μηδενικών ψηφίων.

Σε αυτό το πρόβλημα βοηθάει ένα μικρό κομμάτι δεδομένων το οποίο προστίθεται σε κάθε block και δεν έχει κανέναν άλλο σκοπό εκτός από το να αλλάζει συνεχώς την υπογραφή του αρχείου που προκύπτει μέχρις ότου να βρεθεί μια υπογραφή η οποία να εξυπηρετεί τα δοσμένα κριτήρια. Αυτό το κομμάτι ονομάζεται nonce του block, το οποίο σημαίνει «number used once», δηλαδή αριθμός ο οποίος χρησιμοποιείται μόνο μια φορά. Αποτελεί έναν τελείως τυχαίο αριθμό ο οποίος μπορεί να περιλαμβάνει οποιονδήποτε αριθμό από το 0 μέχρι το 4,294,967,296 (Acheson Noelle, How Bitcoin mining works, 2013).

Εν κατακλείδι, ένα block περιέχει τρεις τύπους πληροφοριών:



Εικ.16. Τα στοιχεία που απαρτίζουν ένα block

Η διαδικασία κατά την οποία το nonce κομμάτι αλλάζει συνεχώς μέχρι να βρεθεί το σωστό το οποίο ταιριάζει στο συγκεκριμένο block ονομάζεται εξόρυξη (mining). Όσοι ασχολούνται με το mining δαπανούν ηλεκτρικό ρεύμα στη μορφή υπολογιστικής ενέργειας για να δοκιμάζουν συνεχώς νέα nonces. Όσο μεγαλύτερη είναι η υπολογιστική ισχύς τόσο πιο γρηγορά μπορούν να ελέγξουν περισσότερα nonces και είναι πιο πιθανό να βρουν μια λύση.

Ο πρώτος χρήστης ο οποίος βρίσκει την υπογραφή, που ανταποκρίνεται στις προϋποθέσεις, το ανακοινώνει στα υπόλοιπα μέλη της ομάδας τα οποία ελέγχουν αν αυτό το αποτέλεσμα είναι όντως το σωστό. Αυτός ο χρήστης που καταφέρνει να βρει πρώτος τη σωστή υπογραφή ανταμείβεται με δωρεάν χρήματα για την προσπάθειά του. Τα χρήματα με τα οποία ανταμείβεται πρέπει να σημειωθεί ότι απλά προστίθενται στο λογαριασμό του χρήστη και δεν αφαιρούνται από κάποιον άλλον χρήστη του δικτύου. Οι ανταμοιβές αυτές είναι που κάνουν τους χρήστες να συνεχίζουν να εργάζονται στο δίκτυο.

Οποιοσδήποτε χρήστης του δικτύου μπορεί να εμπλακεί στη συγκεκριμένη διαδικασία αρκεί να κατεβάσει το απαραίτητο λογισμικό εξόρυξης για τη συγκεκριμένη blockchain που

επιθυμεί. Όμως, το να βρει κάποιος το σωστό nonce για να δημιουργήσει τη σωστή υπογραφή χρειάζεται μεγάλη υπολογιστική ισχύ, ενέργεια, χρόνο και συγχρόνως πολύ τύχη. Υποστηρίζεται ότι υπάρχουν περισσότερες πιθανότητες κάποιος να κερδίσει σε κάποιο τυχερό λαχνό παρά να βρει πρώτος τη σωστή υπογραφή ενός block.

4.3. Κατάρρευση της Blockchain

Σε κάθε τεχνολογία είναι σωστό μαζί με τα θετικά της στοιχεία και τις καινοτομίες της, να αναγνωρίζονται και τα ευάλωτα σημεία της. Όπως παρουσιάστηκε προηγουμένως, εάν αλλάξει ένα στοιχείο σε ένα block τότε αναγκαστικά αλλάζει και η υπογραφή του, γεγονός που έχει ως συνέπεια να πρέπει να αλλάξουν και οι υπογραφές σε όλα τα αλλά block τα οποία υπάρχουν μετά από αυτό το οποίο τροποποιήθηκε, κάτι το οποίο, όπως τονίστηκε, θεωρείται ακατόρθωτο διότι είναι πολύ ακριβό και χρονοβόρο να πραγματοποιηθεί, όμως δεν είναι αδύνατον να γίνει.

Εικάζοντας ότι ένας διεφθαρμένος χρήστης του δικτύου αλλάζει ένα block συναλλαγών και προσπαθεί να υπολογίσει τις νέες υπογραφές για τα επόμενα blocks, έτσι ώστε όλο το δίκτυο να δεχτεί την αλλαγή την οποία πραγματοποίησε και να μην γίνει αντιληπτός. Ο συγκεκριμένος χρήστης επρόκειτο να αντιμετωπίσει μια πολύ σημαντική δυσκολία. Το πρόβλημα έγκειται στο γεγονός ότι ενώ εκείνος προσπαθεί να δημιουργήσει τις νέες υπογραφές των block που ήδη υπάρχουν στην αλυσίδα, όλοι οι υπόλοιποι χρήστες δημιουργούν υπογραφές για νέα blocks που δημιουργούνται. Επομένως, ο χρήστης θα πρέπει να καταφέρει να προφτάσει τους υπολοίπους χρήστες και να δημιουργήσει νέες υπογραφές και για τα νέα αυτά blocks τα οποία προστίθενται.

Μόνο αν ο χρήστης αυτός έχει περισσότερη υπολογιστική ισχύ από όλο το υπόλοιπο δίκτυο μαζί θα μπορέσει κάποια στιγμή να υπερβεί τις προσπάθειες των άλλων χρηστών. Ωστόσο, επειδή σήμερα στη τεχνολογία των blockchains οι χρήστες είναι εκατομμύρια σε αριθμό, υποτίθεται ότι ένας διεφθαρμένος χρήστης ή ένα μικρό πλήθος διεφθαρμένων χρηστών δεν θα αποκτήσουν ποτέ περισσότερη υπολογιστική ισχύ από όλο το υπόλοιπο δίκτυο μαζί, δηλαδή το δίκτυο δεν θα δεχτεί ποτέ αλλαγές στη blockchain και έτσι η blockchain θα παραμείνει αμετάβλητη.

Αν όμως έστω ότι κάποιος χρήστης αποκτήσει τεράστια υπολογιστική ισχύ, πολύ μεγαλύτερη από το υπόλοιπο δίκτυο, τότε θα υπάρξει 51% επίθεση στη blockchain. Στην πραγματικότητα, μια τέτοια επίθεση θα ήταν πολύ πιο δαπανηρή για να εκτελεστεί σε σχέση με το τι θα κέρδιζε ο χρήστης που θα την πραγματοποιούσε. Αυτό θα συνέβαινε γιατί εκτός από το ότι θα χρειαζόταν πάρα πολύ μεγάλο εξοπλισμό για να καταφέρει κάτι τέτοιο αφού ή θα έπρεπε

να αποκτήσει πρόσβαση σε πάνω από το 50% των υπολογιστών στο δίκτυο ή να δημιουργήσει έναν υπολογιστή με τόσο μεγάλη ισχύ, θα έπρεπε επίσης να αντιμετωπίσει κινδύνους διώξεων και το σημαντικότερο από όλα είναι ότι θα έπληττε την ίδια την blockchain αφού θα έπεφτε αισθητά η αξία της και θα αχρηστεύοταν μιας και η προσπάθεια του θα γινόταν αντιληπτή από το υπόλοιπο δίκτυο και όλοι οι υπόλοιποι χρήστες θα το εγκατέλειπαν. Γι' αυτό σημαντικός παράγοντας για την διασφάλιση της ασφάλειας της blockchain είναι να συμμετέχουν στη διαδικασία εξόρυξης όλο και περισσότεροι χρήστες.

4.4. Κανόνες της Blockchain

Η blockchain ακολουθεί το μοντέλο της δημοκρατίας και πάντα πιστεύει ως τεχνολογία αυτό που υποστηρίζει η πλειονότητα των χρηστών της. Η διαδικασία γίνεται αυτόματα αφού η blockchain λαμβάνει πάντοτε ως αληθή την μεγαλύτερη αλυσίδα των blocks που έχουν δημιουργηθεί θεωρώντας πως αυτή η αλυσίδα αντιπροσωπεύεται από την πλειοψηφία. Αυτό συμβαίνει διότι η μεγαλύτερη υπολογιστική ισχύς μπορεί να δημιουργήσει και τη μεγαλύτερη αλυσίδα blocks, και όσο περισσότεροι χρήστες τόσο μεγαλύτερη και η υπολογιστική ισχύς που διαθέτουν αρά και μεγαλύτερη η αλυσίδα blocks που δημιουργούν. Αυτός είναι και ο τρόπος με τον οποίο απορρίπτεται ένα τροποποιημένο block αυτόματα από το μεγαλύτερο μέρος του δικτύου, αφού το συγκεκριμένο block δεν θα είναι πλέον αλυσοδεμένο με την μεγάλη αλυσίδα.

Ένας άλλος σημαντικός κανόνας ο οποίος διέπει την τεχνολογία της blockchain είναι πως τα ιστορικά συναλλαγών καθώς και τα χρήματα τα οποία βρίσκονται σε κάθε λογαριασμό είναι πάντοτε δημόσια. Ο καθένας μπορεί οποιαδήποτε στιγμή να ανατρέξει σε μια συναλλαγή ή έναν λογαριασμό. Αν και όλες αυτές οι πληροφορίες είναι δημόσιες, τα προσωπικά στοιχεία των ιδιοκτητών των λογαριασμών καθώς και των συναλλαζόμενων σε κάθε συναλλαγή παραμένουν σε μεγάλο βαθμό άγνωστα. Παρακάτω παρουσιάζεται ένας λογαριασμός ενός χρήστη που περιέχει κοντά στα 70.000 bitcoins, τα οποία αξίζουν περίπου 250 εκατομμύρια δολάρια. Το ενδιαφέρον στη συγκεκριμένη περίπτωση είναι ότι ο συγκεκριμένος χρήστης συνεχίζει μέχρι και σήμερα να κάνει mining, όμως έχει να χρησιμοποιήσει ουσιαστικά bitcoins στις συναλλαγές του από το 2015.

Bitcoin Address 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx

Share:                             

block, address, transaction

69,370.12³⁶⁵¹⁶⁶ BTC
Balance: 247,337,948.99 USD
Received: 69,471.12³⁷ BTC (160 ins) first: 2013-04-10 00:03:36 last: 2018-12-31 12:59:23
Sent: 101 BTC (1 outs) first: 2015-04-23 17:10:25 last: 2015-04-23 17:10:25
Unspent outputs: 159



Εικ.17. Λογαριασμός χρήστη Bitcoin

Έχοντας στο νου όλα τα παραπάνω, υπάρχει ακόμα ένα ερώτημα το οποίο δεν έχει απαντηθεί και αφορά την εμπιστοσύνη που μπορούν να έχουν οι χρήστες στη blockchain. Αναφέρθηκε νωρίτερα ότι η blockchain είναι ένα αποκεντρωμένο σύστημα στο οποίο οποιοσδήποτε μπορεί να συμμετάσχει χωρίς να δώσει τα προσωπικά του στοιχεία. Για να μπορέσει η blockchain να χτίσει εμπιστοσύνη μεταξύ των χρηστών του δικτύου της δημιουργεί κάποια πρωτόκολλα για τους ηλεκτρονικούς υπολογιστές οι οποίοι θέλουν να λάβουν μέρος στην εξέλιξη της και να προσθέσουν αρχεία στην αλυσίδα. Τα πρωτόκολλα αυτά ονομάζονται πρωτόκολλα συναίνεσης και τα ευρέως γνωστά είναι δυο:

- **Proof of Work**, αποτελεί το πιο διαδεδομένο πρωτόκολλο και χρησιμοποιείται στα περισσότερα κρυπτονομίσματα. Με το Proof of Work, για να μπορεί ο κάθε κόμβος, δηλαδή ο κάθε ηλεκτρονικός υπολογιστής, να προσθέτει ένα block στην αλυσίδα πρέπει να αποδείξει ότι «εργάστηκε» λύνοντας ένα όλο και πιο δύσκολο υπολογιστικό παζλ. Αυτή η διαδικασία ονομάζεται εξόρυξη (mining), όπως τονίστηκε και πρωτύτερα, και χρησιμοποιεί πολλή μεγάλη υπολογιστική ισχύ. Σε αντάλλαγμα για το έργο τους, τα μέλη του δικτύου λαμβάνουν κάποιες ανταμοιβές, όπως για παράδειγμα bitcoins ή άλλα ψηφιακά στοιχεία – tokens (Murray Maryanne, 2018 & newgenapps.com, 2018).
- **Proof of Stake**, σε αυτήν την περίπτωση οι συμμετέχοντες αγοράζουν tokens ή bitcoins τα οποία τους επιτρέπουν να ενταχθούν στο δίκτυο. Όσο περισσότερα tokens ή bitcoins έχουν στην κατοχή τους τόσες περισσότερες πιθανότητες έχουν να επιλεγούν για να ανανεώσουν τη blockchain (Murray Maryanne, 2018). Αυτό το πρωτόκολλο μοιάζει με τους μέτοχους μιας επιχείρησης αφού έτσι δίνεται το προνόμιο στους πλουσίους να γίνονται ακόμα πιο πλούσιοι. Το Proof of Stake όμως δημιουργήθηκε εξ αρχής για να παρουσιάσει έναν λιγότερο δαπανηρό τρόπο για τη δημιουργία της blockchain με τον οποίο δεν χρειάζεται να καταναλωθούν υψηλές ποσότητες ενέργειας και ισχύος. Συγκεκριμένα, η χρήση ενέργειας περιορίζεται μόνο στην χρήση και στην έγκριση των χρηστών και όχι σε περίπλοκους υπολογισμούς (newgenapps.com, 2018).

Κεφάλαιο 5: Το πρώτο κρυπτονόμισμα

5.1. Ιστορική αναδρομή των κρυπτονομισμάτων

Το κρυπτονόμισμα, ενάντια στην κοινή αντίληψη, δεν αποτελεί έννοια της σημερινής εποχής αλλά υπάρχει και αναφέρεται σε κείμενα και έρευνες ήδη από τις αρχές του 20^{ου} αιώνα. Είναι σημαντικό να σημειωθεί ότι οι μείζονες επιστημονικές ανακαλύψεις, ανεξάρτητα με το πόσο πρωτότυπες φαίνονται, βασίζονται πάντα σε παλαιότερες και υπάρχουσες έρευνες. Μελετώντας το παρακάτω χρονοδιάγραμμα θα γίνει πιο εύκολα κατανοητό πως ξεκίνησε η αναφορά στα κρυπτονομίσματα και η δημιουργία αυτών.

- **1983:** ένας Αμερικανός κρυπτογράφος, ονόματι David Chaum, σε μια έρευνα του σχετικά με την κρυπτογραφία χρησιμοποιεί για πρώτη φορά τον όρο των κρυπτογραφημένων ψηφιακών νομισμάτων (Chaum David, 1983).
- **1990:** ο ίδιος Αμερικανός κρυπτογράφος ιδρύει τη DigiCash, μια εταιρεία ψηφιακών νομισμάτων, με έδρα το Άμστερνταμ, προκειμένου να εμπορευματοποιήσει τις ιδέες που είχε αναφέρει στην έρευνά του (Pitta Julie, 1999). Η DigiCash αποτελεί μια πρόιμη μορφή των κρυπτογραφημένων ηλεκτρονικών πληρωμών για την οποία απαιτείται ένα λογισμικό το οποίο λαμβάνει χρήματα από την τράπεζα και δημιουργεί συγκεκριμένα κρυπτογραφημένα κλειδιά για να μπορέσουν τα χρήματα αυτά να αποσταλούν σε έναν παραλήπτη χωρίς να είναι σε θέση η τράπεζα έκδοσης, η κυβέρνηση ή οποιοδήποτε τρίτο πρόσωπο να τα εντοπίσει.
- **1996:** Η πρεσβεία της Εθνικής Ασφάλειας (NSA) των Ηνωμένων Πολιτειών δημοσιεύει σε μια λίστα αλληλογραφίας του MIT ένα έγγραφο με τίτλο: «How to Make a Mint: the Cryptography of Anonymous Electronic Cash» περιγράφοντας ένα σύστημα κρυπτονομισμάτων (groups.csail.mit.edu, 1996). Την ίδια περίοδο δημιουργείται το e-gold, ένα ψηφιακό νόμισμα το οποίο αντιστοιχεί σε πραγματικό χρυσό.
- **1997:** η Coca Cola προσφέρει τη δυνατότητα αγοράς προϊόντων από αυτόματες μηχανές χρησιμοποιώντας κινητές πληρωμές (Wikoff Shawn, 2016).

- **1998:** Η εταιρεία DigiCash αποτυγχάνει και κηρύσσει πτώχευση, διότι εξαρτάται από τις υπάρχουσες υποδομές της κυβέρνησης και των εταιρειών έκδοσης πιστωτικών καρτών (Wikoff Shawn, 2016). Παράλληλα ο Wei Dai, μηχανικός ηλεκτρονικών υπολογιστών, δημοσιεύει μια περιγραφή του b-money, τον προκάτοχο του Bitcoin, το οποίο χαρακτηρίζεται ως ανώνυμο κατανεμημένο ηλεκτρονικό σύστημα μετρητών. Σε αυτό το έγγραφο, προτείνεται για πρώτη φορά το πρωτόκολλο Proof of Work ως μέσο για τη δημιουργία χρημάτων (weidai.com).

Την ίδια περίοδο ο Nick Szabo, επιστήμονας στον χώρο της πληροφορικής και της κρυπτογραφίας, σχεδιάζει ένα μηχανισμό για ένα αποκεντρωμένο ψηφιακό νόμισμα με το όνομα bit gold το οποίο όμως δεν εφαρμόστηκε ποτέ (Peck Morgen E., 2012). Το 1998 εμφανίζεται για πρώτη φορά η PayPal, ως ηλεκτρονική υπηρεσία πληρωμών βασισμένη στο παραδοσιακό νόμισμα. Διαθέτει ωστόσο περισσότερους περιορισμούς τηρώντας τους κανόνες της κυβέρνησης (Wikoff Shawn, 2016).

- **1999:** ο David Chaum εγκαταλείπει την εταιρεία DigiCash (Wikoff Shawn, 2016).
- **2006:** Δημιουργείται το Liberty Reserve, ένα σύστημα το οποίο μετατρέπει τα δολάρια και τα ευρώ σε Liberty Reserve δολάρια και Liberty Reserve ευρώ, επιτρέποντας την ανταλλαγή αυτών με χρέωση 1% σε κάθε συναλλαγή. Η δημιουργία του πραγματοποιήθηκε για λογούς ξεπλύματος χρημάτων και γι' αυτό καταργήθηκε αναπόφευκτα από την αμερικανική κυβέρνηση.
- **2008 – 2009:** Εμφανίζεται για πρώτη φορά το Bitcoin, ένα αποκεντρωμένο κρυπτονόμισμα το οποίο σηματοδοτεί την αρχή της εξέλιξης της τεχνολογίας των κρυπτονομισμάτων (Wikoff Shawn, 2016). Σχεδόν 10 χρόνια μετά τη περιγραφή του b-money από τον Wei Dai, ο Satoshi Nakamoto δημοσιεύει στην ίδια λίστα αλληλογραφίας της ομάδας ακτιβιστών Cypherpunks τις πρώτες προδιαγραφές του Bitcoin στο περίφημο πλέον white paper, όπου λίγο αργότερα κατατέθηκε και δημόσια. Είναι σημαντικό να σημειωθεί πως ως κρυπτογραφική μέθοδος κατακερματισμού, το Bitcoin χρησιμοποιεί τον αλγόριθμο SHA-256 (Brito Jerry and Castillo Andrea, 2013).
- **2011:** Τον Απρίλιο, το Namecoin εμφανίζεται ως μια προσπάθεια δημιουργίας ενός αποκεντρωμένου κατανεμημένου συστήματος ονοματοδοσίας (DNS), το οποίο σύστημα έχει

ως σκοπό να καταστήσει πολύ δύσκολη τη λογοκρισία στο διαδίκτυο. Το ίδιο έτος κυκλοφορεί και το Litecoin, το οποίο αποτελεί το πρώτο επιτυχές κρυπτονόμισμα που χρησιμοποιεί scrypt, δηλαδή μια συνάρτηση εξαγωγής κλειδιών με βάση τον κωδικό πρόσβασης, και όχι τη μέθοδο κατακερματισμού με βάση τον αλγόριθμο SHA-256 (Steadman Ian, 2013).

- **2012:** Εμφάνιση του Peercoin, το πρώτο υβριδικό κρυπτονόμισμα το οποίο χρησιμοποιεί το πρωτόκολλο Proof of Work μαζί με το πρωτόκολλο Proof of Stake (Steadman Ian, 2013).
- **2014:** Τον Αύγουστο το Ηνωμένο Βασίλειο ανακοίνωσε ότι ανατέθηκε στο Υπουργείο Οικονομικών του να μελετήσει τα κρυπτονόμισματα και πόσο μεγάλο ρόλο μπορούν να διαδραματίσουν στην οικονομία του Ηνωμένου Βασιλείου. Η μελέτη έπρεπε να αναφέρει επίσης αν χρειάζεται να ληφθεί υπόψη κάποια σχετική ρύθμιση (theuknews.com, 2014).
- **2018:** Σύμφωνα με την ιστοσελίδα capital.gr (2018), τον Οκτώβριο η παγκόσμια εποπτική αρχή για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες ανακοίνωσε ότι θα εφαρμόσει από το επόμενο έτος κανόνες σχετικά με τον τρόπο με τον οποίο οι κυβερνήσεις θα πρέπει να ρυθμίζουν τα ανταλλακτήρια κρυπτονομισμάτων σε μια προσπάθεια να εξαλειφθεί η εγκληματική χρήση bitcoin και άλλων ψηφιακών νομισμάτων.

5.2. Εισαγωγή στο Bitcoin

Ξεκινώντας θα πρέπει να ξεκαθαριστούν δυο βασικές έννοιες οι οποίες συγχέονται αρκετά συχνά όταν αναφερόμαστε στον όρο «Bitcoin». Από τη μια πλευρά, υπάρχει το bitcoin ως



Εικ.18. Επίσημο λογότυπο Bitcoin

νόμισμα, το οποίο αποτελεί ένα κομμάτι κώδικα που αντιπροσωπεύει την ιδιοκτησία μιας ψηφιακής ιδέας. Από την άλλη πλευρά, υπάρχει το Bitcoin ως πρωτόκολλο, το οποίο αποτελεί ένα κατανεμημένο δίκτυο το οποίο διατηρεί ένα λογιστικό βιβλίο για όλες τις συναλλαγές οι οποίες γίνονται με τα bitcoin νομίσματα (Acheson Noelle, What is Bitcoin?, 2013). Σύμφωνα με το επίσημο ίδρυμα Bitcoin Foundation, η

λέξη «Bitcoin» κεφαλαιοποιείται στο πλαίσιο αναφοράς στην οντότητα ή στην έννοια ως πρωτόκολλο, ενώ η λέξη «bitcoin» γράφεται με πεζά γράμματα όταν αναφερόμαστε σε μια ποσότητα του νομίσματος.

Το Bitcoin αποτελεί το πρώτο κρυπτονόμισμα το οποίο διαδόθηκε και αναπτύχθηκε σε ευρεία κλίμακα και στηρίζεται στην τεχνολογία της blockchain για την υλοποίηση του. Αυτό έχει ως αποτέλεσμα να επιτρέπει την αποστολή πληρωμών μεταξύ χρηστών χωρίς οι συναλλαγές να διέρχονται από κάποια κεντρική αρχή, όπως μια τράπεζα. Οι συναλλαγές πραγματοποιούνται και αποθηκεύονται ηλεκτρονικά, όπως ηλεκτρονικά είναι και τα νομίσματα, ονόματι bitcoins, τα οποία παράγονται ως ανταμοιβή για τους χρήστες οι οποίοι συμμετέχουν στη διαδικασία mining του Bitcoin. Τα bitcoins παράγονται σε υπολογιστές σε όλον τον κόσμο με τη χρήση ελεύθερου λογισμικού και έχουν ψηφιακή υπόσταση, δηλαδή δεν εκτυπώνονται όπως τα δολάρια ή το ευρώ και δεν εκδίδονται, ούτε υποστηρίζονται από τράπεζες ή κυβερνήσεις. Πάρα το γεγονός ότι τα bitcoins δεν είναι νόμιμο χρήμα είναι ευρέως διαδεδομένα στις συναλλαγές (Acheson Noelle, What is Bitcoin?, 2013).

Η ιστορία του Bitcoin αρχίζει ύστερα από τη Διεθνή Χρηματοπιστωτική Κρίση, δηλαδή μετά από μια παγκόσμια βαριά οικονομική ύφεση στον ευρύτερο χρηματοπιστωτικό και τραπεζικό τομέα με γενεσιουργό χώρα τις Ηνωμένες Πολιτείες της Αμερικής, η οποία διήρκησε από το καλοκαίρι του 2007 έως τα τέλη του 2008. Με την κατάρρευση της Lehman Brothers, η οποία ήταν μέχρι το 2008 η τέταρτη μεγαλύτερη επενδυτική τράπεζα στις Ηνωμένες Πολιτείες, ξεκίνησε η αναζήτηση ενός νέου οικονομικού συστήματος το οποίο δεν θα εξαρτιόνταν από κάποια κεντρική αρχή προκειμένου να εποπτεύει, να πιστοποιεί και τελικά να ελέγχει τις συναλλαγές, όπως γινόταν μέχρι τότε μέσω των τραπεζικών συστημάτων (Σπαθάς Βαγγέλης, 2017).

5.3. Ιστορική αναδρομή του Bitcoin

- Στις **18 Αυγούστου 2008** το bitcoin.org καταχωρήθηκε ως «όνομα διεύθυνσης» (domain name) στο διαδίκτυο. Μέχρι σήμερα, αυτή η ηλεκτρονική διεύθυνση είναι προστατευμένη, με την έννοια ότι η ταυτότητα του ατόμου που την έχει καταχωρήσει δεν αποτελεί δημοσιότητα (Frankenfield Jake, Bitcoin, 2011).
- Στις **31 Οκτωβρίου 2008** κάποιος με το όνομα Satoshi Nakamoto δημοσιεύει στην «Λίστα Αλληλογραφίας σχετικά με την Κρυπτογραφία» στο metzdowd.com: «Έχω δουλέψει σε ένα

νέο ηλεκτρονικό οικονομικό σύστημα το οποίο είναι πλήρως peer-to-peer, χωρίς τρίτο μεσολαβητή. Το έγγραφο διατίθεται στην ηλεκτρονική διεύθυνση bitcoin.org/bitcoin.pdf».

Ο συγκεκριμένος ηλεκτρονικός σύνδεσμος οδηγεί πλέον στο διάσημο white paper το οποίο δημοσιεύτηκε για πρώτη φορά στο bitcoin.org με τίτλο: «Bitcoin: Ένα σύστημα ηλεκτρονικών πληρωμών Peer-to-Peer» (Bitcoin: A Peer-to-Peer Electronic Cash System). Αυτό το έγγραφο θα γίνει το βασικό εγχειρίδιο για το πως λειτουργεί το Bitcoin μέχρι σήμερα, διότι περιέχει αναλυτικές μεθόδους για τη χρήση ενός peer-to-peer δικτύου προκειμένου να παραχθεί ένα «ηλεκτρονικό σύστημα συναλλαγών το οποίο δεν βασίζεται στην εμπιστοσύνη».

- Στις **3 Ιανουαρίου 2009** δημιουργείται το δίκτυο Bitcoin με τον Satoshi Nakamoto να εξορύσσει το genesis block, δηλαδή το πρώτο μπλοκ της Bitcoin Blockchain, το οποίο ονομάζεται Block 0 και είχε ως ανταμοιβή 50 bitcoins (Wallace Benjamin, 2011).

Εικ.19. Το genesis block της Bitcoin Blockchain

Block #0	
BlockHash 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f	
Summary	
Number Of Transactions	1
Height	0 (Mainchain)
Block Reward	50 BTC
Timestamp	Jan 3, 2009 8:15:05 PM
Mined by	
Merkle Root	4a5e1e4baab89f3a32518a88c31bc...
Difficulty	1
Bits	1d00ffff
Size (bytes)	285
Version	1
Nonce	2083236893
Next Block	1

Το Block 0 περιέχει το εξής κείμενο: «*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*» (Frankenfield Jack, Genesis Block, 2018). Το κείμενο αναφέρεται σε έναν τίτλο άρθρου των «The Times», Βρετανική ημερήσια ειδησεογραφική εφημερίδα με έδρα το Λονδίνο, το οποίο δημοσιεύθηκε **στις 3 Ιανουαρίου 2009** ([thetimes.co.uk](https://www.thetimes.co.uk), 2009). Αυτή η σημείωση έχει ερμηνευθεί ως χρονολογική σφραγίδα της ημερομηνίας δημιουργίας και έναρξης της Bitcoin Blockchain και ως πολιτικό σχόλιο.

- Στις **8 Ιανουαρίου 2009** η πρώτη έκδοση του λογισμικού Bitcoin ανακοινώνεται στην «Λίστα Αλληλογραφίας σχετικά με την Κρυπτογραφία».

- Στις **9 Ιανουαρίου 2009** το Block 1 εξορύσσεται και αρχίζει η πραγματική και σοβαρή εξόρυξη του Bitcoin. Ο πρώτος κώδικας ανοικτού λογισμικού δημοσιεύτηκε στις **9 Ιανουαρίου 2009** και φιλοξενήθηκε στην ηλεκτρονική ιστοσελίδα SourceForge (Nakamoto Satoshi, 2009 & sourceforge.net, 2009).
- Ο προγραμματιστής Hal Finney κατεβάζει και εγκαθιστά το Bitcoin λογισμικό την ημέρα έκδοσής του και δέχεται 10 bitcoins από τον Satoshi Nakamoto στην πρώτη συναλλαγή bitcoin στον κόσμο στις **12 Ιανουαρίου 2009** (Peterson Andrea, 2014 & Popper Nathaniel, 2014).
- Στις **6 Αυγούστου 2010** εντοπίζεται ένα τρωτό σημείο στο πρωτόκολλο Bitcoin. Οι συναλλαγές δεν επαληθευόντουσαν σωστά πριν συμπεριληφθούν στο ημερολόγιο συναλλαγών ή αλλιώς blockchain, επιτρέποντας έτσι στους χρήστες να παρακάμπτουν τους οικονομικούς περιορισμούς του Bitcoin και να δημιουργούν έναν απεριόριστο αριθμό bitcoins (nvd.nist.gov).
- Στις **15 Αυγούστου 2010**, γίνεται εκμετάλλευση αυτού του τρωτού σημείου με τη δημιουργία πάνω από 184 δισεκατομμύρια bitcoins σε μια συναλλαγή, τα οποία στάλθηκαν σε δυο διευθύνσεις στο δίκτυο. Μέσα σε λίγες ώρες η συναλλαγή εντοπίστηκε και το αρχείο διαγράφηκε από τη blockchain μετά την επιδιόρθωση του σφάλματος και ενημερώθηκε η έκδοση του πρωτοκόλλου (sourceforge.net, 2010). Αυτό αποτελεί και το μοναδικό μεγάλο ελάττωμα ασφαλείας που εντοπίστηκε στην ιστορία του Bitcoin (nvd.nist.gov).

5.4. Satoshi Nakamoto

Έχουν υπάρξει πολλές εικασίες ως προς την ταυτότητα του ατόμου το οποίο κρύβεται πίσω από το όνομα Satoshi Nakamoto, όμως το συγκεκριμένο όνομα δεν αποτελεί τίποτα άλλο παρά μόνο ένα ψευδώνυμο για το άτομο, ή ίσως και την ομάδα ατόμων, που σχεδίασε το πρωτότυπο πρωτόκολλο Bitcoin το 2008. Ο αυτοαποκαλούμενος Satoshi Nakamoto αποτελεί τον δημιουργό και σχεδιαστή της πλειοψηφίας του επίσημου λογισμικού Bitcoin και ο ίδιος ήταν ενεργός χρήστης και πραγματοποιούσε και δημοσίευε τροποποιήσεις και τεχνικές πληροφορίες σχετικά με τον κώδικα του λογισμικού στο Bitcoin Forum (Wallace Benjamin, 2011). Ωστόσο, πριν από τη δημιουργία του Bitcoin, δεν υπάρχει κανένα στοιχείο, όνομα ή αρχείο στο οποίο να αναφαίρετε στο όνομα Satoshi Nakamoto, καθώς δεν υπήρχε και κανένας προγραμματιστής γνωστός με αυτό το ονοματεπώνυμο. Επιπρόσθετα, η διεύθυνση ηλεκτρονικού ταχυδρομείου και

η διαδικτυακή ηλεκτρονική ιστοσελίδα που χρησιμοποίησε ο Satoshi, δεν μπορούν να εντοπιστούν.

Όσον αφορά το όνομα του έχουν γίνει διάφορες υποθέσεις από που προήλθε, όπως για παράδειγμα το Satoshi στα ιαπωνικά σημαίνει «σοφός» ή ότι όλο το ονοματεπώνυμο πήγασε από τα πρώτα συνθετικά τεσσάρων εταιρειών υψηλής τεχνολογίας «SAmsung, TOSHiba, NAKAmichi, MOTOrola». Όμως δεν είναι λίγες και οι εικασίες σχετικά με υποψήφιους που έχοντας τα κατάλληλα προσόντα ίσως να κρύβονται πίσω από την συγκεκριμένη επωνυμία όπως ο Wei Dai, ο οποίος εφηύρε τη τεχνολογία b-money, ο Nick Szabo ο οποίος εφηύρε το bit gold καθώς και υποθέσεις ως προς το πρόσωπο του Hal Finney, μιας και ήταν ο πρώτος χρήστης στον κόσμο ο οποίος κατέβασε το Bitcoin και εκτέλεσε την πρώτη συναλλαγή μαζί με τον Satoshi Nakamoto (likeinamirror, 2013). Τρανταχτό επιχείρημα όμως αποτελεί ότι στην ίδια πόλη στην οποία κατοικούσε ο Hal Finney, στην Καλιφόρνια, ζούσε και ένα φυσικός με το όνομα Dorian Prentice Satoshi Nakamoto, Αμερικάνος ιαπωνικής καταγωγής, ο οποίος όμως αρνήθηκε την εμπλοκή του στο Bitcoin δηλώνοντας ότι δεν είναι αυτός ο δημιουργός του (Greenberg Andy, 2014 & Goodman Leah McGrath, 2014).

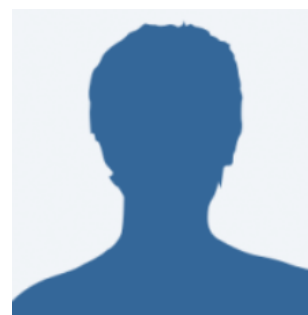
Είναι φανερό ότι μέχρι την σήμερα ημέρα ο εφευρέτης του Bitcoin έχει καταφέρει να διατηρήσει το μυστικό της ταυτότητας του, καθώς επιθυμεί πρωτίστως την ιδιωτικότητα του, μιας και το Bitcoin έχει κερδίσει μεγάλη δημοσιότητα αφού πλέον αποτελεί ένα παγκόσμιο φαινόμενο, επομένως και ο Satoshi Nakamoto, κατά πασα πιθανότητα αν αποκαλυφθεί θα συγκεντρώσει και αυτός τα βλέμματα της δημοσιότητας πάνω του κυρίως από τα μέσα μαζικής ενημέρωσης αλλά και από τις κυβερνήσεις. Από αυτή την δημοσιότητα απορρέει και ο δεύτερος λόγος για τον οποίο ο Satoshi Nakamoto δεν έχει γνωστοποιήσει τα πραγματικά του στοιχεία, και δεν είναι άλλος πέρα από την ασφάλεια.

Συγκεκριμένα, το 2009, στα πρώτα βήματα δηλαδή του Bitcoin, μόνο ο Satoshi και ίσως μερικοί άλλοι χρήστες εξόριζαν bitcoins. Επομένως ο Satoshi Nakamoto ως πρωταρχικός χρήστης μπορεί κάλλιστα να έχει συγκεντρώσει τόσα bitcoins ώστε να αντιστοιχούν σήμερα σε περίπου 900 εκατομμύρια δολάρια (McMillan Robert, 2013). Δεν είναι δύσκολο να αντιληφθεί κανείς ότι κάποιος ο οποίος έχει στην κατοχή του τόσα πολλά bitcoins θα μπορούσε να γίνει εύκολος στόχος των εγκληματιών μιας και τα bitcoins είναι λιγότερο σαν μετοχές και περισσότερο σαν μετρητά αφού τα ιδιωτικά κλειδιά τα οποία χρειάζονται για να πραγματοποιηθούν και να εγκριθούν οι συναλλαγές μπορούν να εκτυπωθούν σε οποιοδήποτε

χαρτί. Μπορεί βέβαια ο εφευρέτης του Bitcoin να πάρει προφυλάξεις για τυχόν εκβιασμούς και να καταφέρει εν τέλει να τους ανιχνεύσει, όμως η ανωνυμία είναι ένα κάλος τρόπος για να περιορίσει την ανεπιθύμητη δημοσιότητα (Frankenfield Jake, Bitcoin, 2011).

Παρόλα αυτά, άτομα τα οποία έχουν βάλει ως στόχο να μάθουν την πραγματική του ταυτότητα έχουν συγκεντρώσει κάποια στοιχεία ως προς το πρόσωπο του εφευρέτη του πρωτοκόλλου Bitcoin. Αρχικά, το πρωτόκολλο ζητάει από του χρήστες όταν πραγματοποιούν την εγγραφή τους να συμπληρώσουν την ημερομηνία των γενέθλιων τους. Εξαιτίας αυτού του πεδίου είναι γνωστό πως ένα άτομο το οποίο ονομάζεται Satoshi Nakamoto έκανε εγγραφή στο σύστημα με ημερομηνία γέννησης 5 Απρίλιου 1975 και τόπο διαμονής την Ιαπωνία. Αυτή είναι η μοναδική ουσιαστική πληροφορία που διατίθεται για την πραγματική ταυτότητα του Satoshi Nakamoto (Frankenfield Jake, Bitcoin, 2011 & p2pfoundation.ning.com).

Λόγω όμως κάποιων διαδικτυακών του κείμενων τα οποία είναι γραμμένα σε άπιαστα αγγλικά, καθώς και αναφερόμενοι στο γεγονός ότι το genesis block του Bitcoin Blockchain εμπεριέχει ένα κείμενο το οποίο παραθέτει έναν τίτλο βρετανικής εφημερίδας, υπάρχουν πολλοί υποστηρικτές τις βρετανικής καταγωγής του Satoshi Nakamoto. Επιπλέον, με κίνητρο το γεγονός ότι το λογισμικό Bitcoin δεν έχει τεκμηριωθεί στην ιαπωνική γλώσσα, ο Stefan Thomas, ένας Ελβετός



Satoshi Nakamoto
43, Male
Japan

προγραμματιστής, κατέγραψε σε ένα διάγραμμα τις ώρες τις οποίες ήταν ενεργός και δημοσίευε απαντήσεις ο Satoshi Nakamoto στο Bitcoin Forum. Τα αποτελέσματα του συγκεκριμένου διαγράμματος έδειξαν απότομη πτώση μεταξύ των ωρών 5 π.μ. και 11 μ.μ. ώρα Γκρίνουιτς. Οι ώρες αυτές στην Ιαπωνία αντιστοιχούν μεταξύ 2 μ.μ. και 8 μ.μ., υποδεικνύοντας ένα ασυνήθιστο μοτίβο ύπνου για κάποιον ο οποίος υποτίθεται πως ζει στην Ιαπωνία. Δεδομένου ότι αυτό το μοτίβο ίσχυε και τα Σάββατα και τις Κυριακές, ο Stefan Thomas πρότεινε ότι ο Nakamoto κοιμόταν εκείνες τις ώρες (Wallace Benjamin, 2011).

Εικ.20. Τα στοιχεία του λογαριασμού του Satoshi Nakamoto

Μεταξύ του έτους 2009 και του έτους 2010, ο Satoshi Nakamoto προσκάλεσε και άλλους προγραμματιστές να τον βοηθήσουν, ώστε να μπορέσει να βελτιώσει και να τελειοποιήσει τον κώδικα του, με αποτέλεσμα να συνομιλεί μαζί τους σε τακτά χρονικά διαστήματα χωρίς όμως και πάλι να αποκαλύπτει κάποια προσωπική πληροφορία. Τον Απρίλιο του 2011, ο ίδιος έστειλε ένα σημείωμα σε έναν από τους προγραμματιστές προκειμένου να γνωστοποιήσει ότι

«προχώρησε σε άλλα πράγματα» και από τότε μέχρι σήμερα δεν έχει επικοινωνήσει ποτέ κανείς μαζί του (Davis Joshua, 2011). Η εξαφάνιση του κλόνησε μεγάλο αριθμό ατόμων αφού ένιωσαν ότι ίσως όλα ήταν ένα είδους πλεκτάνης από την μεριά του Nakamoto. Όμως, το κίνητρο του Nakamoto δεν ήταν το έγκλημα αλλά η πολιτική και πριν εξαφανιστεί από οποιαδήποτε ανάμειξη σχετικά με το Bitcoin, παρέδωσε κατά μια έννοια τα ηνία στον προγραμματιστή Gavin Andresen, ο οποίος στη συνέχεια έγινε επικεφαλής στο Bitcoin Foundation (Bosker Bianca, 2013).

Τελικώς, φαίνεται πως δεν αξίζει η ανάλωση σκέψεων για την ανακάλυψη της μυστικής ταυτότητας του Satoshi Nakamoto και ποιος κρύβεται πίσω από την επωνυμία του, αλλά είναι ανάγκη να δοθεί περισσότερη σημασία στο σύστημα το οποίο δημιουργήθηκε, το οποίο επιτρέπει την ανεξαρτησία χωρίς να στηρίζεται η εμπιστοσύνη του χρήστη σε κάποιο άλλο άτομο, μια εταιρεία ή μια κυβέρνηση. Ένα σύστημα στο οποίο οποιοδήποτε μπορεί να συμμετέχει, οποιοσδήποτε μπορεί να ελέγξει τον κώδικα και του οποίου το δίκτυο δεν ελέγχεται από κάποια άλλη οντότητα. Ένα σύστημα το οποίο καθιστά δυνατή τη μεταβίβαση της εμπιστοσύνης από ένα πρόσωπο σε ένα ολόκληρο δίκτυο χρηστών. Ούτως ή άλλως, το Bitcoin άνθισε και εξακολουθεί να υπάρχει και να διαδίδεται στις μέρες μας, λόγω των πτυχών του που είναι εμφανείς αλλά και των πτυχών του που δεν είναι εμφανείς. Οι χρήστες είναι κρυφοί, οι συναλλαγές όμως όχι. Ο κώδικας είναι ορατός σε όλους, η προέλευση του όμως αποτελεί ένα μυστήριο. Το νόμισμα του είναι τόσο πραγματικό και τόσο αόριστο όπως είναι και ο ιδρυτής του (Davis Joshua, 2011).

Κεφάλαιο 6: Απόκτηση και αποθήκευση Bitcoin

6.1. Τρόποι απόκτησης

Το Bitcoin αποτελεί ένα κρυπτονόμισμα στο οποίο οι συναλλαγές καθώς και το σύνολο των bitcoins κάθε λογαριασμού βασίζονται στην κρυπτογραφία δημιουργώντας μέσω αυτής της τεχνολογίας τις ψηφιακές υπογραφές προκειμένου να παραχωρείται στους χρήστες ο πλήρης έλεγχος ιδιοκτησίας. Οι συγκεκριμένες υπογραφές αποτελούνται από δημοσιά και ιδιωτικά κλειδιά, τα οποία δημιουργούνται μέσα από την μέθοδο κατακερματισμού hashing που αναπτύχθηκε σε προηγούμενο κεφάλαιο, και αποτελούνται από ένα μεγάλο συνδυασμό αριθμών και γραμμάτων. Το δημόσιο κλειδί, μοιάζει με τον αριθμό ενός τραπεζικού λογαριασμού και αποτελεί την διεύθυνση η οποία είναι ορατή σε όλον το δίκτυο και στην οποία διεύθυνση μπορούν οι άλλοι χρήστες να αποστείλουν bitcoins. Το ιδιωτικό ή προσωπικό κλειδί θα μπορούσε να παρομοιαστεί με τον αριθμό PIN μιας τραπεζικής κάρτας και κατ' επέκταση πρέπει να φυλάσσεται πολύ καλά, διότι αποτελεί το μοναδικό στοιχείο με το οποίο επιτυγχάνεται η έγκριση των Bitcoin συναλλαγών.

Οι συναλλαγές μεταξύ δυο μερών στο Bitcoin γίνονται σε ένα δίκτυο διαμοιρασμού (Peer-to-Peer) χωρίς την εμπλοκή τρίτων μεσολαβητών, όπως χρηματοπιστωτικά ιδρύματα ή κυβερνήσεις, για τον έλεγχο και την πιστοποίηση της εκάστοτε συναλλαγής. Ο ρόλος του ενδιάμεσου μεσολαβητή αντικαθίσταται στο συγκεκριμένο σύστημα από τους χρηστές του δικτύου οι οποίοι μέσω των πόρων που διαθέτουν προκειμένου να συμμετέχουν στην διαδικασία της εξόρυξης επαληθεύουν και καταγράφουν ταυτόχρονα όλες τις συναλλαγές που πραγματοποιούνται στο δίκτυο. Ωστόσο αυτό το οποίο ελκύει τους χρήστες ώστε να παίρνουν μέρος στη διαδικασία εξόρυξης είναι φυσικά η ανταμοιβή για τις προσπάθειες τους σε νομίσματα bitcoin. Εντούτοις υπάρχουν και άλλοι τρόποι με τους οποίους μπορούν να αποκτηθούν τα ψηφιακής μορφής νομίσματα bitcoin και είναι οι εξής:

Ως μέσο πληρωμής

Τα bitcoins μπορούν να γίνουν αποδεκτά ως μέσο πληρωμής για τα προϊόντα τα οποία πωλούνται ή για υπηρεσίες οι οποίες παρέχονται. Για παράδειγμα, οποιοσδήποτε καταστηματάρχης μπορεί να προσθέσει μια ταμπέλα στο κατάστημα του λέγοντας «Δεχόμαστε bitcoins» και ως επακόλουθο πολλοί από τους πελάτες του θα ξεκινήσουν να πληρώνουν σε αυτή τη μορφή ψηφιακού νομίσματος. Οι συναλλαγές θα μπορέσουν να πραγματοποιηθούν με το αντίστοιχο απαραίτητο εξάρτημα τερματικού και μέσω μιας

διεύθυνσης πορτοφολιού η οποία μπορεί να γνωστοποιηθεί μέσω κωδικού QR μιας εφαρμογής. Αντίστοιχα μια επιχείρηση στο διαδίκτυο μπορεί ευκολά να δεχθεί ως μέσο πληρωμής το bitcoin αρκεί να προσθέσει αυτή την επιλογή πληρωμής μαζί με τις άλλες επιλογές οι οποίες προσφέρονται, όπως πιστωτικές κάρτες, PayPal κλπ.

Ως ανταμοιβή για παροχή εργασίας

Οι ελεύθεροι επαγγελματίες μπορούν να πληρωθούν για μια δουλειά την οποία θα αναλάβουν σε bitcoins. Πιο συγκεκριμένα υπάρχουν αρκετές διαδικτυακές ιστοσελίδες για εύρεση εργασίας όπου η ανταμοιβή παρέχεται σε bitcoin νομίσματα. Κάποιες από αυτές τις ιστοσελίδες είναι:

- **Working for Bitcoins** - workingforbitcoins.com, οι αιτούντες εργασία αλλά και οι υποψήφιοι εργοδότες μπορούν να έρθουν σε επαφή μέσω διάφορων αγγελιών και η πληρωμή φυσικά γίνεται μέσω bitcoins.
- **Coinality** - coinality.com, στην συγκεκριμένη ιστοσελίδα διατίθενται θέσεις εργασίας τόσο μερικής όσο και πλήρους απασχόλησης. Επιπλέον είναι δυνατή η πληρωμή όχι μόνο σε bitcoins αλλά και σε άλλα κρυπτονομίσματα όπως dogecoins και litecoins.
- **Jobs4Bitcoins** - reddit.com/r/Jobs4Bitcoins, μια λίστα δημοσιεύσεων στην ιστοσελίδα reddit.com στην οποία οποιοσδήποτε μπορεί να ζητήσει ή να προσφέρει εργασία με αμοιβή σε bitcoin νομίσματα.
- **Bitgigs** - bitgigs.com, μια ιστοσελίδα όπου ο καθένας μπορεί να προσφέρει οποιαδήποτε υπηρεσία επιθυμεί για αμοιβή σε bitcoins.

Ως δάνειο

Ένας άλλος ενδιαφέρον τρόπος για να κερδίσει κάποιος bitcoins είναι με τον δανεισμό τους και την μετέπειτα εξόφληση τους. Αυτή η δανειοδότηση μπορεί να γίνει με τους εξής τρόπους, είτε απευθείας με τον δανεισμό σε κάποιο γνωστό πρόσωπο, είτε μέσω μιας ιστοσελίδας η οποία διευκολύνει τέτοιου είδους συναλλαγές, είτε με την κατάθεση σε κάποια εικονική τράπεζα η οποία προσφέρει ένα συγκεκριμένο επιτόκιο για τους λογαριασμούς Bitcoin. Τέτοιες ιστοσελίδες είναι η Bitbond και η BTCjam. Προφανώς, για ευνόητους λογούς η επιλογή κάποιου οργανισμού ως τρίτο μεσολαβητή πρέπει να γίνεται πολύ προσεκτικά.

Ως κέρδη σε τυχερά παιχνίδια

Υπάρχουν καζίνο για τους λάτρεις του Bitcoin με επιλογές όπως το τζακπότερ, διαδικτυακές λαχειοφόρες αγορές, τα στοιχήματα και άλλα παρόμοια παιχνίδια. Φυσικά, τα υπέρ και τα κατά καθώς και όσοι κίνδυνοι υπάρχουν και ισχύουν για οποιοδήποτε τέτοιου είδους τυχερό παιχνίδι με παραστατικά χρήματα, ισχύουν και στην συγκεκριμένη περίπτωση των bitcoins.

6.2. Η διαδικασία της εξόρυξης - Mining

Στο συγκεκριμένο κεφάλαιο θα προσπαθήσει να γίνει πιο κατανοητή η διαδικασία εξόρυξης στο Bitcoin πρωτόκολλο και τον τρόπο με τον οποίο τελικά μπορεί κάποιος χρήστης να ανταμειφθεί με bitcoins για τη συμμετοχή του. Αρχικά, η οικονομία του Bitcoin βασίζεται στο δίκτυο των υπολογιστών οι οποίοι συμμετέχουν στις διαδικασίες εξόρυξης. Όπως έχει αναφερθεί, η διαδικασία εξόρυξης πρόκειται ουσιαστικά για την επίλυση δύσκολων μαθηματικών και αλγοριθμικών προβλημάτων μέσω υπολογιστικής ισχύς. Όταν καταφέρει κάποιος να επιλύσει τον αλγόριθμο που έχει δοθεί τότε ανταμείβεται με bitcoins για την ενέργεια και τον χρόνο που ξόδεψε, και με αυτόν τον τρόπο δημιουργούνται τα νέα bitcoins στο δίκτυο. Δε θα πρέπει ωστόσο να παραλείπεται το γεγονός ότι μέσω της εξόρυξης επιτυγχάνεται συγχρόνως και η επαλήθευση των συναλλαγών και η προσθήκη τους στην blockchain, αλλά και η διασφάλιση των συναλλαγών και των bitcoins τα οποία έχει ο κάθε χρήστης στην κατοχή του.

Ένα από τα θετικά στοιχεία της εξόρυξης είναι ότι κάθε άνθρωπος ο οποίος έχει πρόσβαση στο διαδίκτυο, καταλληλά μηχανήματα υπολογιστών και εξαρτήματα μπορεί να συμμετέχει στην διαδικασία. Οι συμμετέχοντες προσπαθούν ταυτόχρονα να λύσουν τα δύσκολα μαθηματικά προβλήματα τα οποία προκύπτουν και ο συμμετέχων ο οποίος καταφέρνει να επιλύσει πρώτος το πρόβλημα προσθέτει το επόμενο block στην blockchain και ανταμείβεται για την εργασία του. Οι ανταμοιβές είναι ουσιαστικά αυτές οι οποίες ενθαρρύνουν την όλη διαδικασία της εξόρυξης. Ο αλγόριθμος ξεκίνησε το 2009 δίνοντας για κάθε αλγοριθμική λύση 50 bitcoins και ο αριθμός των bitcoins που δίνονται μειώνεται σταδιακά. Υπολογίζεται πως η όλη διαδικασία θα διαρκέσει μέχρι το έτος 2140 περίπου. Συγκεκριμένα, η ανταμοιβή μειώνεται κατά το ήμισυ σε κάθε 210.000 block, ή περίπου κάθε 4 χρόνια, με την ανταμοιβή του block σήμερα, το έτος 2019 να είναι στα 12,5 bitcoins. Ο αυτοματοποιημένος αυτός ρυθμός έχει σκοπό να εξασφαλίζει μια τακτική αύξηση της προσφοράς νομισμάτων με τελικό στόχο τα 21 εκατομμύρια bitcoins, χωρίς παρεμβολές από τρίτους μεσολαβητές, όπως η τράπεζα, γεγονός που θα μπορούσε να οδηγήσει σε υπερπληθωρισμό (Acheson Noelle, How Bitcoin mining works, 2013).

Οι αλγόριθμοι τους οποίους καλούνται να επιλύσουν οι χρήστες ωστόσο δεν είναι τόσο εύκολοι όσο φαντάζουν και η δυσκολία τους εξαρτάται από την γενική προσπάθεια επίλυσης τους η οποία καταβάλλεται στο δίκτυο. Η δυσκολία της εξόρυξης τροποποιείται από το πρωτόκολλο σε κάθε 2016 blocks ή περίπου κάθε 2 εβδομάδες. Ο λόγος που αλλάζει η δυσκολία και προσαρμόζεται είναι προκειμένου να διατηρηθεί σταθερός ο ρυθμός με τον οποίον λύνονται τα μαθηματικά αυτά προβλήματα. Επομένως, όσο περισσότερη υπολογιστική ισχύ χρησιμοποιείται για την εξόρυξη, τόσο θα μεγαλώνει και η δυσκολία επίλυσης του μαθηματικού προβλήματος το οποίο προκύπτει, ενώ αν αφαιρεθεί υπολογιστική ισχύς από το δίκτυο τότε θα συμβεί το αντίθετο προκειμένου να διευκολυνθεί η εξόρυξη. Η δυσκολία ξεκίνησε στο 1.0 στα πρώτα στάδια του Bitcoin το έτος 2009 και στο τέλος του ιδίου χρόνου είχε φτάσει στο 1.18. Τον Απρίλιο του 2017 η δυσκολία της εξόρυξης είχε φτάσει τα 4.24 δισεκατομμύρια.

Εκτός όμως από τη δημιουργία νέων bitcoins, η εξόρυξη είναι ο τρόπος με τον οποίο δημιουργείται ουσιαστικά και ολόκληρη η blockchain αφού μέσω αυτής της διαδικασίας επαληθεύονται οι συναλλαγές οι οποίες γίνονται με τα ψηφιακής υπόστασης bitcoins. Η ανταμοιβή του χρήστη ολοκληρώνεται όταν θα τοποθετήσει το νέο block στην blockchain το οποίο θα περιέχει και την δικιά του ανταμοιβή ως τελευταία συναλλαγή. Με αυτόν τον τρόπο καθίσταται δυνατή η ασφάλεια της blockchain αλλά και των bitcoins ως νομίσματα δίχως σχετικές ρυθμίσεις από κάποια τράπεζα ή κυβέρνηση.

Στα αρχικά βήματα του Bitcoin, η εξόρυξη μπορούσε να πραγματοποιηθεί από έναν κανονικό επιτραπέζιο υπολογιστή με τις κάρτες γραφικών και τις μονάδες επεξεργασίας γραφικών (GPU) να είναι πιο αποτελεσματικές στην εξόρυξη από της κεντρικές μονάδες επεξεργασίας (CPU). Ωστόσο, με την άνοδο της δημοτικότητας του Bitcoin οι GPUs κυριάρχησαν απέναντι στις απλές κάρτες γραφικών και στις CPUs. Πολύ σύντομα, το 2013, δημιουργήθηκε και κυκλοφόρησε το πρώτο ολοκληρωμένο κύκλωμα εξειδικευμένης χρήσης για Bitcoin Mining, τα επονομαζόμενα Application Specific Integrated Circuits (ASICs). Η εξόρυξη είναι ιδιαίτερα ανταγωνιστικό κομμάτι του Bitcoin πρωτοκόλλου και σήμερα μπορεί να πραγματοποιηθεί μόνο με τα τελευταία και πιο εξελιγμένα μοντέλα ASICs.

Στην σημερινή εποχή, αν γίνει προσπάθεια συμμετοχής στην εξόρυξη με CPUs, GPUs ή ακόμα και με παλαιότερα ASICs, το κόστος της ενέργειας που θα καταναλωθεί είναι πολύ μεγαλύτερο από το εισόδημα το οποίο θα παραχθεί στο τέλος. Επομένως, επειδή ο χρόνος

εύρεσης ενός block είναι μεγάλος και η δυνατότητα ενός μεμονωμένου χρήστη να λύσει τον αλγόριθμο είναι ιδιαίτερα δύσκολη έως ακατόρθωτη, έχουν δημιουργηθεί πολλά mining pools, όπου οι χρήστες ενώνουν όλοι μαζί τις δυνάμεις τους για την εύρεση του block και έπειτα μοιράζονται την αμοιβή ανάλογα με τη συνεισφορά του καθενός. Ωστόσο, τα mining pools πρέπει να είναι ιδιαίτερα προσεκτικά με τον αριθμό των ατόμων που θα τα απαρτίζει καθώς και με την συνολική υπολογιστική ισχύ την οποία θα κατέχουν ώστε να μην προκαλέσουν την λεγόμενη 51% επίθεση στη blockchain (coindesk.com, What are Bitcoin mining pools?, 2014).

6.3. Αγορά νομισμάτων bitcoin

Έχοντας αναφέρει τους βασικούς τρόπους με τους οποίους μπορεί κάποιος να αποκτήσει bitcoin νομίσματα και έχοντας επεξηγήσει περεταίρω την διαδικασία της εξόρυξης (mining) και τον τρόπο ανταμοιβής των χρηστών μέσω αυτής, είναι η στιγμή να επισημανθεί ότι υπάρχει η δυνατότητα οποιοσδήποτε να αγοράσει bitcoins είτε από ιστοσελίδες ανταλλαγής νομισμάτων ή απευθείας από άλλους χρήστες μέσω συγκεκριμένων αγορών. Είναι σημαντικό ωστόσο να σημειωθεί ότι δεν πρέπει κάποιος να επενδύει και να αγοράζει bitcoins αν δεν έχει το οικονομικό περιθώριο να χάσει αυτά τα χρήματα, διότι η τιμή των κρυπτονομισμάτων δεν είναι σταθερή και μεταβάλλεται συνεχώς, με άλλα λόγια όσο εύκολα μπορεί να αυξηθεί τόσο εύκολα μπορεί και να μειωθεί.

Συνεχίζοντας, όπως έχει ήδη τονισθεί οποιοσδήποτε χρήστης του διαδικτύου μπορεί με πολύ εύκολο τρόπο να αγοράσει και να κατέχει τα δικά του bitcoins. Η αγορά αυτή πραγματοποιείται είτε με μετρητά, δηλαδή με τη χρήση παραστατικού χρήματος, είτε με πιστωτικές ή χρεωστικές κάρτες, είτε ακόμα και με τη χρήση άλλων κρυπτονομισμάτων. Ο τρόπος αλλά και η μέθοδος η οποία θα χρησιμοποιηθεί για να αγοραστούν τα bitcoin νομίσματα εξαρτάται από τον πωλητή των κρυπτονομισμάτων αλλά και από τον τόπο διαμονής τόσο του πωλητή όσο και του αγοραστή.

Η διαδικασία την οποία μπορεί να ακολουθήσει κάποιος προκειμένου να αγοράσει bitcoins είναι η εξής, αρχικά το πρώτο βήμα είναι να δημιουργήσει ένα ψηφιακό πορτοφόλι στο οποίο θα μπορέσει να αποθηκεύσει τα bitcoin νομίσματα του με οποιονδήποτε τρόπο τα συλλέξει, περεταίρω ανάλυση των ψηφιακών πορτοφολιών θα γίνει στο επόμενο κεφάλαιο. Το δεύτερο βήμα είναι να ανοίξει έναν λογαριασμό σε κάποια ιστοσελίδα ανταλλαγής. Αυτές οι ιστοσελίδες λειτουργούν για να βοηθούν του χρήστες, αγοράζοντας και πουλώντας τα κρυπτονομίσματα αυτών ευκολά και γρηγορά. Είναι αναμενόμενο ότι υπάρχουν εκατοντάδες τέτοιες επιχειρήσεις

οι οποίες λειτουργούν με διαφορετικούς βαθμούς ρευστότητας και ασφάλειας καθώς νέες συνεχίζουν συνεχώς να εμφανίζονται, κάποιες από αυτές αναφορικά είναι η Coinbase, η Coingate, η Poloniex και η Bitstamp. Όσον αφορά τα πορτοφόλια καθώς και τις ιστοσελίδες ανταλλαγής κρυπτονομισμάτων θα πρέπει να διεξαχθεί σωστή ερευνά, ώστε να μην πέσει κάποιος θύμα απάτης ή κλοπής.

Στο τέλος της διαδικασίας, η ιστοσελίδα ανταλλαγής θα πρέπει να παρέχει στον χρήστη αρκετές και επαρκείς λεπτομέρειες για την εκτέλεση της αγοράς, Αν όχι θα πρέπει ο χρήστης να συλλογιστεί ώστε να αλλάξει πάροχο υπηρεσιών. Αφού γίνει η πληρωμή για την ανταλλαγή, η ιστοσελίδα θα αγοράσει το αντίστοιχο ποσό bitcoin για λογαριασμό του χρήστη και θα δημιουργήσει αυτόματα ένα ψηφιακό πορτοφόλι γι' αυτόν με το τέλος της συναλλαγής. Η όλη διαδικασία μπορεί να διαρκέσει από μερικά λεπτά έως μερικές ώρες ανάλογα με την κατάσταση του δικτύου. Συνήθως συνίσταται οι χρήστες να μεταφέρουν τα bitcoins ή οποιοδήποτε άλλο κρυπτονόμισμα ανταλλάξουν σε ένα εξωτερικό ψηφιακό πορτοφόλι για μεγαλύτερη ασφάλεια.

Το δεύτερο βήμα μπορεί να τροποποιηθεί αν ο χρήστης δεν θέλει να πραγματοποιήσει αγορά bitcoins μέσω διαδικτύου και επιθυμεί να ανταλλάξει bitcoins για μετρητά. Υπάρχουν πλατφόρμες, όπως η LocalBitcoins, οι οποίες βοηθάνε του χρήστες να βρουν άτομα στην περιοχή στην οποία διαμένουν και τα οποία είναι πρόθυμα να ανταλλάξουν bitcoins για παραστατικά χρήματα. Επίσης, η LibertyX προσφέρει μια λίστα με καταστήματα λιανικής σε όλες τις Ηνωμένες Πολιτείες όπου μπορεί κάποιος να ανταλλάξει μετρητά για bitcoins. Η WallofCoins, η Paxful και η BitQuick είναι κάποιες από τις ιστοσελίδες οι οποίες μπορούν να κατευθύνουν τους χρήστες σε κάποιο κατάστημα τράπεζας για να κάνουν μια απλή κατάθεση μετρητών και να λάβουν το αντίστοιχο ποσό σε bitcoins λίγες ώρες αργότερα.

Υπάρχουν και μηχανήματα ATM τα οποία μπορούν στείλουν bitcoins απευθείας στο ψηφιακό πορτοφόλι του χρήστη σε αντάλλαγμα για μετρητά. Λειτουργούν με παρόμοιο τρόπο όπως τα τραπεζικά ATM. Με λίγα λόγια εισάγει ο χρήστης τα μετρητά που επιθυμεί στο ATM, εισάγει τον κωδικό QR για το ψηφιακό του πορτοφόλι και ο αριθμός bitcoin ο οποίος αντιστοιχεί στο χρηματικό ποσό το οποίο κατατέθηκε προστίθεται στο ψηφιακό του πορτοφόλι. Η ιστοσελίδα Coinatmradar μπορεί να βοηθήσει ορισμένους χρήστες να βρουν κάποιο ATM σε κοντινή τους περιοχή (Acheson Noelle, How can I buy bitcoin?, 2013).

6.4. Ψηφιακά πορτοφόλια

Τα bitcoins ενός χρήστη μπορούν να αποθηκευτούν σε πολλά διαφορετικά μέρη, είτε σε κάποιο ψηφιακό πορτοφόλι σε κάποιον υπολογιστή ή σε κάποιο κινητό τηλέφωνο, είτε σε κάποια διαδικτυακή πλατφόρμα, είτε σε κάποια συσκευή μη συνδεδεμένη στο διαδίκτυο, είτε ακόμα και στο cloud. Επειδή υπάρχει μια ευρεία γκάμα επιλογής για τον τρόπο και το μέρος που θα αποθηκεύσει κάποιος τα bitcoin νομίσματα του θα πρέπει να γίνεται μια σωστή και ολοκληρωμένη ερευνά ώστε να επιλεγθεί η σωστή λύση η οποία θα βολεύει καλύτερα τον κάθε χρήστη.

Η σημαντικότερη λειτουργία ουσιαστικά ενός πορτοφολιού κρυπτονομισμάτων είναι να συλλεγεί και να διαφυλάσσει τα ιδιωτικά και τα δημόσια κλειδιά του κάθε χρήστη ασφαλής. Στην περίπτωση που κάποιος χρήστης χάσει ένα από αυτά τα δυο στοιχεία ή και τα δυο, τότε χάνει και την πρόσβαση στα bitcoins τα οποία έχουν αποθηκευτεί στο πορτοφόλι του. Στην πραγματικότητα ωστόσο, ένα πορτοφόλι συνήθως κατέχει πολλά ιδιωτικά κλειδιά, και είναι σύνηθες πολλοί επενδυτές να έχουν πολλά πορτοφόλια.

Γενικά, τα πορτοφόλια μπορούν να βρίσκονται είτε σε κάποιον υπολογιστή ή κινητό τηλέφωνο, σε κάποια συσκευή αποθήκευσης ή και σε ένα κομμάτι χαρτί. Τα είδη επομένως των πορτοφολιών τα οποία μπορούμε να συναντήσουμε σύμφωνα με την Acheson Noelle (How to store your bitcoin, 2013) και την ιστοσελίδα buybitcoinworldwide.com (Which is the best Bitcoin wallet?) έχουν ως εξής:

- Τα **computer-based / desktop πορτοφόλια** τα οποία μπορούν να ληφθούν και να εγκατασταθούν ως λογισμικό σε κάποιον υπολογιστή. Πρόκειται ουσιαστικά για πορτοφόλια στην μορφή ενός αρχείου το οποίο βρίσκεται σε κάποιον υπολογιστή ή κάποια άλλη ηλεκτρονική συσκευή και διευκολύνει τις συναλλαγές παρέχοντας σε κάθε χρήστη τη δυνατότητα να ελέγχει και να κρατάει ασφαλή τα κλειδιά του. Τα πορτοφόλια αυτής της μορφής έχουν μια σχετικά εύκολη διαμόρφωση και είναι δωρεάν. Τέτοια πορτοφόλια είναι το Bitcoin Core, το Armory, το Electrum, το Exodus, το Jaxx και το Copay.

Το μειονέκτημα των computer-based πορτοφολιών είναι ότι απαιτούν περισσότερη συντήρηση και ανάγκη ύπαρξης πολλών αντιγράφων για την διασφάλιση της ασφάλειας, διότι αν υπολογιστής ή η συσκευή στην οποία βρίσκεται το πορτοφόλι του χρήστη κλαπεί ή

καταστραφεί και δεν υπάρχουν κάπου αλλού αποθηκευμένα τα ιδιωτικά κλειδιά τότε χάνονται τα bitcoin τα οποία είναι αποθηκευμένα στο εκάστοτε πορτοφόλι. Επιπρόσθετα, απαιτούν μεγαλύτερες προφυλάξεις ασφάλειας, διότι εάν κάποιος εισέλθει παράνομα στον υπολογιστή του χρήστη και καταφέρει να αποκλέψει τα ιδιωτικά του κλειδιά, τότε θα αποκτήσει πρόσβαση και στα bitcoin νομίσματά του.

- Τα **cloud-based πορτοφόλια** τα οποία συνδέονται απευθείας με το cloud, είναι δωρεάν και προσφέρουν αυξημένη ευκολία αφού μπορεί ο χρήστης να έχει πρόσβαση στα bitcoins του από οποιαδήποτε συσκευή επιθυμεί αρκεί να έχει τους σωστούς κωδικούς πρόσβασης. Επιπλέον, είναι πιο φιλικά προς το χρήστη σε σχέση με τα computer-based πορτοφόλια, αφού ο χρήστης μπορεί να τα ρυθμίσει πολύ πιο ευκολά μέσα από εφαρμογές είτε για τον υπολογιστή, είτε για το κινητό τηλέφωνο και μπορεί μέσα από αυτές τις εφαρμογές να λαμβάνει και να ξοδεύει τα bitcoin νομίσματά του. Τέτοια πορτοφόλια είναι το Coinbase και το Blockchain. Το Coinbase και το Xapo δίνουν επίσης την δυνατότητα στους χρήστες να αποθηκεύουν τα bitcoins τους εκτός δικτύου.

Ωστόσο με τη χρήση των cloud-based πορτοφολιών η εμπιστοσύνη μεταβιβάζεται πάλι σε κάποιο τρίτο μεσολαβητή ο οποίος θα διασφαλίσει τα κλειδιά του κάθε χρήστη και με αυτόν τρόπο αναγκαστικά παρέχεται χαμηλότερη ασφάλεια. Πρέπει ο χρήστης να εμπιστευτεί τα μετρά ασφαλείας του κεντρικού υπολογιστή καθώς και την ίδια την εταιρεία παροχής του πορτοφολιού πως δεν θα εξαφανιστεί με τα χρήματά του, πως δεν θα σταματήσει η λειτουργία της υπηρεσίας και πως δεν θα του αρνηθεί κάποια στιγμή πρόσβαση στις υπηρεσίες της.

- Τα **mobile πορτοφόλια** τα οποία είναι διαθέσιμα ως εφαρμογές στα έξυπνα ηλεκτρονικά κινητά τηλεφώνια και είναι ιδιαίτερα χρήσιμα αν ο χρήστης επιθυμεί να πληρώσει σε ένα κατάστημα με bitcoins, ή αν θέλει να αγοράσει, να πουλήσει ή να στείλει bitcoins καθώς βρίσκεται εν κίνηση. Τα περισσότερα cloud-based πορτοφόλια έχουν αντίστοιχες τέτοιες εφαρμογές για τα κινητά τηλεφώνια, ενώ άλλα πορτοφόλια όπως το Abra, το Airbitz και το Bread δημιουργήθηκαν με γνώμονα τα κινητά τηλεφώνια. Επιπροσθέτως, κάποια διαθέτουν ως επιπλέον χαρακτηριστικό πληρωμής την τεχνολογία NFC ή υποστηρίζουν έξυπνα ρολόγια με λειτουργικό Android. Είναι καλή πρακτική κάποιος να διαθέτει ένα μικρό αριθμό των bitcoins του σε ένα mobile πορτοφόλι και τα υπόλοιπα να τα έχει προστατευμένα μέσω κάποιας άλλης πιο ασφαλούς επιλογής πορτοφολιού.

- Τα **hardware πορτοφόλια** τα οποία είναι μικρές συσκευές χωρίς σύνδεση στο διαδίκτυο, οι οποίες συνδέονται σε αυτό μόνο για να ενεργοποιήσουν τις bitcoin συναλλαγές. Είναι εξαιρετικά ασφαλή πορτοφόλια, καθώς βρίσκονται γενικά εκτός σύνδεσης επομένως δεν μπορούν να προσπελαστούν ή να χακαριστούν μέσω διαδικτύου. Ωστόσο, υπάρχει η πιθανότητα να κλαπούν και να προσπελαστούν αν δεν έχουν κλειδωθεί – ασφαλιστεί με κάποιον κωδικό πρόσβασης ή απλά να χαθούν μαζί με τα bitcoins τα οποία είναι αποθηκευμένα στο εσωτερικό τους. Μερικοί από τους μεγαλύτερης επενδυτές διατηρούν τα hardware πορτοφόλια τους σε ασφαλείς τοποθεσίες όπως τραπεζικές θυρίδες. Παράδειγμα τέτοιων πορτοφολιών είναι το Trezor, το Keepkey, το Ledger και το Case.
- Τα **paper πορτοφόλια** είναι η πιο απλή, εύκολη και οικονομική μορφή ενός πορτοφολιού. Πρόκειται για κομμάτια χαρτιού στα οποία τυπώνονται τα ιδιωτικά και τα δημοσιά κλειδιά μιας διεύθυνσης Bitcoin. Ωστόσο, είναι ιδανικά για την μακροπρόθεσμη αποθήκευση των bitcoin εξαιρώντας την περίπτωση φωτιάς ή νερού. Επίσης, είναι κατάλληλα για την παροχή των bitcoins ως δώρο. Αυτά τα πορτοφόλια είναι τα πιο ασφαλή διότι δεν είναι συνδεδεμένα στο δίκτυο, όμως είναι πολύ πιο εύκολο να χαθούν. Υπάρχουν ιστοσελίδες, οι οποίες για διευκόλυνση του χρήστη παράγουν εικόνες και κωδικούς QR με τα κλειδιά και τις διευθύνσεις του. Τέτοιες ιστοσελίδες είναι το WalletGenerator και το BitcoinPaperWallet.

Κεφάλαιο 7: Επένδυση στο Bitcoin και η αξία του

7.1. Επένδυση στο Bitcoin

Δεν είναι λίγοι οι υποστηρικτές του Bitcoin οι οποίοι πιστεύουν ότι το συγκεκριμένο ψηφιακό νόμισμα είναι το μέλλον της οικονομίας. Ατράνταχτα επιχειρήματα τους αποτελούν η μεγαλύτερη διευκόλυνση των χρηστών στο πέρας των συναλλαγών τους καθώς και μια ταχύτερη συνολική διαδικασία. Επίσης, υποστηρίζουν ακράδαντα τις χωρίς αμοιβές συναλλαγές, οι οποίες μπορούν να γίνουν από οποιονδήποτε σημείο της γης σε οποιοδήποτε άλλο σημείο χωρίς να υπάρχει κάποιος τρίτος μεσολαβητής.

Αν και το Bitcoin δεν υποστηρίζεται από καμία κυβέρνηση και κανένα χρηματοπιστωτικό ίδρυμα, μπορεί ωστόσο να ανταλλαχθεί για παραστατικά χρήματα και στην πραγματικότητα αυτή η συναλλαγματική ισοτιμία έναντι στο δολάριο, το ευρώ ή οποιοδήποτε άλλο νόμισμα είναι πολλές φορές ο λόγος που προσελκύει επενδυτές και εμπόρους ώστε να ενδιαφερθούν για το συγκεκριμένο νόμισμα. Παρατηρείται λοιπόν, ότι ενώ το Bitcoin δεν δημιουργήθηκε έχοντας ιδιότητες ίδιες με αυτές των μετοχών, ορισμένοι κερδοσκόποι επενδυτές το αντιμετωπίζουν ως μετοχή και όχι ως μέσο ανταλλαγής λόγω της αξίας του. Πολλοί χρήστες του Bitcoin ακολουθούν αυτό το παράδειγμα και πλέον αγοράζουν bitcoins εξαιτίας της τιμής του και της αξίας του ως επένδυση.

Φαίνεται επομένως, ότι η έντονη ανάπτυξη του κρυπτονομίσματος Bitcoin οφείλεται σε έναν μεγάλο βαθμό και στην ικανότητα του να μπορεί να λειτουργήσει ως εναλλακτική λύση για τα εθνικά χρήματα αλλά και για παραδοσιακά προϊόντα, όπως ο χρυσός. Ωστόσο, η αξία των bitcoins δεν είναι εγγυημένη γεγονός που σημαίνει ότι η αγορά και η χρήση τους επιφέρει πολλούς κινδύνους. Πολλοί φορείς έχουν κάνει δηλώσεις για να προειδοποιήσουν τον κόσμο για τέτοιους κινδύνους, όπως η Επιτροπή Κεφαλαιαγοράς των Ηνωμένων Πολιτειών της Αμερικής (SEC), η Χρηματοοικονομική Ρυθμιστική Αρχή Βιομηχανιών (FINRA) και το Γραφείο Προστασίας Χρηματοοικονομικών Καταναλωτών (CFPB).

Δεν θα πρέπει να αμελείται ότι το κρυπτονόμισμα εξακολουθεί να είναι μια καινοτόμα τεχνολογία η οποία δεν κατέχει μακροπρόθεσμο ιστορικό ή ιστορικό αξιοπιστίας για να μπορεί να υποστηρίξει μια σταθερή τιμή και αξία, σε σύγκριση με τις παραδοσιακές επενδύσεις. Παρόλα αυτά με την αυξανόμενη χρήση τους, τα κρυπτονομίσματα δεν βρίσκονται πλέον σε

πειραματικό στάδιο. Ωστόσο, ακόμα και μετά από δέκα σχεδόν χρονιά από την εμφάνιση τους συνεχίζουν να βρίσκονται σε φάση ανάπτυξης, βελτίωσης και εξέλιξης.

7.2. Κίνδυνοι επένδυσης

Όπως έχει επισημανθεί ήδη υπάρχουν πολλές διακινδυνεύσεις που διέπουν τα κρυπτονομίσματα, και αν κάποιος επιθυμεί να επενδύσει σε κάποιο κρυπτονόμισμα, όπως για παράδειγμα το Bitcoin, θα πρέπει να έχει μελετήσει και να έχει κατανοήσει όλους τους κινδύνους και τα ρίσκα που θα χρειαστεί να αντιμετωπίσει. Αναφορικά αυτοί οι κίνδυνοι είναι οι εξής:

Κίνδυνος Ρύθμισης

Τα bitcoins βρίσκονται σε συνεχή αντιπαλότητα με τα κρατικά νομίσματα. Παρόμοια με οποιοδήποτε άλλο νόμισμα μπορούν να χρησιμοποιηθούν σε συναλλαγές στην μαύρη αγορά, σε ξέπλυμα χρήματων, σε παράνομες δραστηριότητες καθώς και σε φοροδιαφυγή. Αυτό έχει ως αποτέλεσμα πολλές κυβερνήσεις να επιθυμούν να ελέγξουν, να ρυθμίσουν, να περιορίσουν ακόμα και να απαγορεύσουν τόσο τη χρήση όσο και την πώληση και αγορά των bitcoins, με μερικές κυβερνήσεις να το έχουν ήδη καταφέρει ενώ άλλες να έχουν δημιουργήσει διάφορους κανόνες για να μπορέσουν ως ένα βαθμό να εκπληρώσουν την επιθυμία τους.

Κίνδυνος Ασφάλειας

Οι συναλλαγές οι οποίες πραγματοποιούνται μέσα από το Bitcoin πρωτόκολλο είναι εξολοκλήρου ψηφιακές και επομένως, όπως και οποιοδήποτε άλλο ψηφιακό σύστημα, διατρέχουν κινδύνους από κακόβουλα λογισμικά και προγράμματα, από χάκερς καθώς και από λειτουργικές δυσλειτουργίες. Αν κάποιος εισβάλει στον σκληρό δίσκο ενός υπολογιστή, ο χρήστης του οποίου διαθέτει στην κατοχή του bitcoins, και κλέψει το ιδιωτικό του κλειδί, τότε θα μπορέσει πολύ ευκολά να αποκτήσει πρόσβαση σε αυτά τα ψηφιακά νομίσματα καθώς και να τα μεταφέρει σε κάποιον άλλο λογαριασμό.

Ωστόσο, σε προηγούμενο κεφάλαιο κατέστη ορατό ότι μια τέτοια επίθεση μπορεί να αποτραπεί μόνο αν ο χρήστης αποθηκεύσει τα bitcoins του σε κάποια άλλη ηλεκτρονική συσκευή ή ηλεκτρονικό υπολογιστή που δεν είναι συνδεδεμένα στο διαδίκτυο ή αν επιλέξει να χρησιμοποιήσει ένα paper πορτοφόλι, εκτυπώνοντας τα ιδιωτικά κλειδιά και τις δημοσιές

διευθύνσεις σε κομμάτια χαρτιού αποφεύγοντας εξολοκλήρου την αποθήκευση τους σε κάποιο ηλεκτρονικό μέσο.

Κίνδυνος Ασφάλισης

Ορισμένες επενδύσεις ασφαλίζονται μέσω της Ασφαλιστικής Προστασίας Ομίλου Επενδυτών καθώς και οι κανονικοί τραπεζικοί λογαριασμοί είναι ασφαλισμένοι μέσω της Ομοσπονδιακής Εταιρείας Ασφάλισης Καταθέσεων (FDIC) μέχρι ένα ποσό ανάλογα με τη δικαιοδοσία. Αντίθετα, οι συναλλαγές Bitcoin καθώς και οι λογαριασμοί Bitcoin των χρηστών δεν είναι ασφαλισμένοι από κανένα τύπο ομοσπονδιακού ή κυβερνητικού προγράμματος.

Κίνδυνος Απάτης

Μπορεί το Bitcoin πρωτόκολλο να χρησιμοποιεί την τεχνολογία της κρυπτογραφίας για τη δημιουργία των ιδιωτικών κλειδιών τα οποία χρησιμοποιούνται για να επαληθεύσουν τις συναλλαγές των ιδιοκτητών τους και για να καταχωρήσουν αυτές τις συναλλαγές στην blockchain, ωστόσο υπάρχουν πολλοί απατεώνες οι οποίοι μπορεί να επιχειρήσουν να πουλήσουν ψευδή bitcoins σε ανυποψίαστους αγοραστές.

Κίνδυνος Αγοράς

Όπως και με οποιαδήποτε άλλη επένδυση, με τον ίδιο τρόπο και οι τιμές του Bitcoin μπορούν να κυμανθούν είτε σε πολύ χαμηλές, είτε σε πολύ υψηλές. Τα τελευταία χρόνια, έχουν παρατηρηθεί πράγματι τεράστιες μεταβολές στην τιμή του συγκεκριμένου κρυπτονομίσματος εξαιτίας κυρίως της σύντομης ύπαρξης του στο χώρο της οικονομίας. Επίσης, πρέπει να σημειωθεί πως αν όλο και λιγότεροι άνθρωποι αρχίσουν να αποδέχονται το Bitcoin ως νομίσματα τότε ενδέχεται να χάσει τελείως την αξία του.

Ο χώρος των κρυπτονομισμάτων είναι ένα πολύ ανταγωνιστικό πεδίο, και παρόλο που το Bitcoin έχει τεράστιο προβάδισμα έναντι όλων των άλλων κρυπτονομισμάτων που έχουν εμφανιστεί, χάρη στην επωνυμία του και στα κεφάλαια τα οποία έχουν κατατεθεί σε αυτό, η εμφάνιση ενός νέου καλύτερου και πιο εξελιγμένου κρυπτονομίσματος αποτελεί μια συνεχής απειλή.

Κίνδυνος Φορολογίας

Δεδομένου ότι το Bitcoin έχει κριθεί ως ακατάλληλο νόμισμα προκειμένου να συμπεριληφθεί σε οποιοδήποτε φορολογικό λογαριασμό, δεν υπάρχουν καλές νομικές επιλογές για να προστατευτούν οι επενδύσεις των χρηστών από την φορολογία.

7.3. Η αξία του Bitcoin

Στη σημερινή εποχή το Bitcoin ως πρωτόκολλο αλλά και τα bitcoin νομίσματα του αποτελούν ένα παγκόσμιο φαινόμενο. Το κάθε bitcoin σήμερα αντιστοιχίζεται και πωλείται για χιλιάδες δολάρια. Κατά τη συγγραφή της συγκεκριμένης πτυχιακής εργασίας η τιμή ενός bitcoin αντιστοιχεί σε 3.626,58 δολάρια ή σε 3.179,40 ευρώ. Το 2017 η τιμή του Bitcoin ήταν λίγο χαμηλότερη από τα 1.000 δολάρια στην αρχή του έτους, και αυξήθηκε περίπου 1.400% φτάνοντας κοντά στις 19.000 δολάρια τον Δεκέμβριο του ίδιου χρόνου σημειώνοντας την υψηλότερη τιμή σε όλα τα χρόνια ύπαρξής του, ενώ μετέπειτα η τιμή του έπεσε απότομα (Finley Klint, 2018). Σύμφωνα με έρευνες μέχρι το Ιανουάριο του 2019, πάνω από 17,5 εκατομμύρια bitcoin βρίσκονται σε κυκλοφορία τα οποία αντιστοιχούν σε αξία άνω των 64 δισεκατομμυρίων δολαρίων (buybitcoinworldwide.com, How many bitcoins are there?).



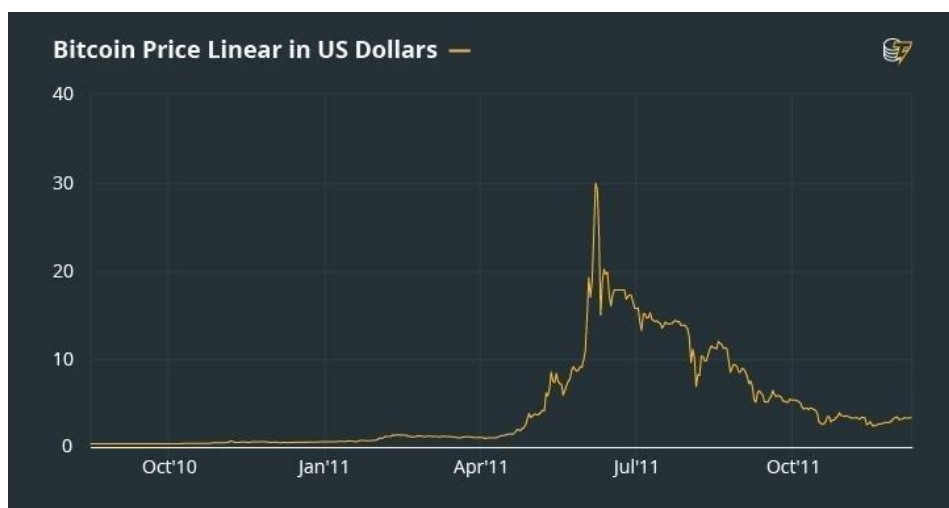
Εικ.21. Αντιστοιχία ενός bitcoin νομίσματος σε δολάρια και ευρώ, 26/01/2019

Στο ξεκίνημα του πάντως το Bitcoin δεν είχε την ίδια αξία και φήμη που φαίνεται να έχει σήμερα. Μέχρι το 2009 και τις αρχές του 2010, τα bitcoins δεν είχαν καθόλου αξία και για τους πρώτους έξι μήνες κυκλοφορίας τους μέχρι και τον Απρίλιο του 2010, η αξία ενός bitcoin παρέμεινε κάτω από 14 σεντς. Στη συνέχεια καθώς το νόμισμα ξεκίνησε να αποκτά κάποια στοιχειώδη φήμη και ζήτηση άρχισε να υπάρχει κινητικότητα και στην τιμή του. Στις αρχές του Νοέμβριου, η τιμή του αυξήθηκε σε 36 σεντς πριν σταθεροποιηθεί περίπου στα 29 σεντς. Έπειτα, τον Φεβρουάριο του 2011 αυξήθηκε ξανά η τιμή του επιτυγχάνοντας ισοτιμία με το δολάριο στα 1.06 δολάρια πριν σταθεροποιηθεί πάλι στα 87 σεντς (Wallace Benjamin, 2011).

Ο μικρός αριθμός των πρώτων χρηστών αντιμετώπιζε το Bitcoin ως μια μικρή κοινότητα φτιαγμένη από ένα πρόγραμμα με λογισμικό ανοικτού κώδικα. Ο Gavin Andresen, ένας προγραμματιστής από την Αγγλία ο οποίος στη συνέχεια έγινε επικεφαλής στο Bitcoin Foundation, αγόρασε τότε 10.000 bitcoins για 50 δολάρια και δημιούργησε μια ιστοσελίδα με το όνομα Bitcoin Faucet, μέσω της οποίας δώρισε αυτά τα bitcoins απλόχερα στον κόσμο. Ο Laszlo

Hanyecz, ένας προγραμματιστής από τη Φλόριντα, πραγματοποίησε την πρώτη πραγματική συναλλαγή bitcoin με παραστατικά χρήματα στον κόσμο, πληρώνοντας 10.000 bitcoins για να πάρει δυο πίτσες από μια αλυσίδα καταστημάτων (bitcointalk.org, 2010). Ουσιαστικά έδωσε τα bitcoins σε έναν εθελοντή στην Αγγλία, ο οποίος έπειτα πραγματοποίησε την συναλλαγή μέσω της χρεωστικής του κάρτα, ωστόσο θεωρείται ευρέως ως η πρώτη φορά που το ψηφιακό νόμισμα εκπληρώνει τον σκοπό του, δηλαδή την αγορά αγαθών. Ένας αγρότης στη Μασαχουσέτη ο οποίος ονομαζόταν David Forster άρχισε να δέχεται bitcoins ως μέσο πληρωμής για κάλτσες από αλπακά (Wallace Benjamin, 2011).

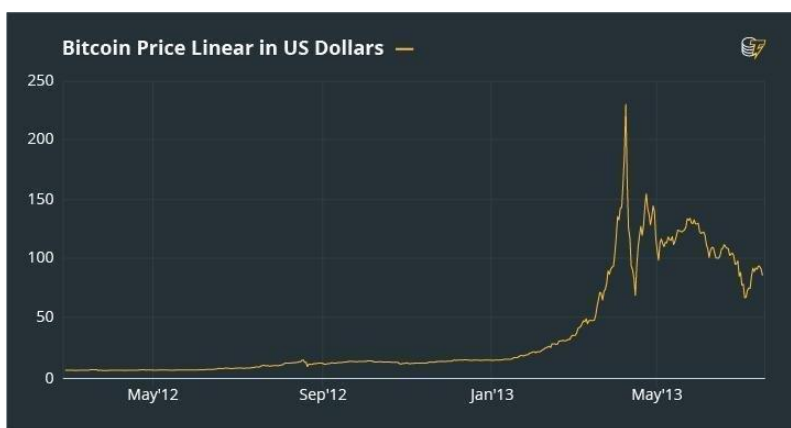
Την άνοιξη του 2011, έπειτα από μια ιστορία η οποία δημοσιεύθηκε στο περιοδικό Forbes με θέμα τα κρυπτονομίσματα η τιμή αυξήθηκε σημαντικά (Greenberg Andy, 2011). Από τις αρχές του Απριλίου έως τα τέλη του Μαΐου η τιμή ενός bitcoin αυξήθηκε από 86 σεντς στα 8,89 δολάρια. Στη συνέχεια, αφού ο Gawker δημοσίευσε τον Ιούνιο μια ιστορία σχετικά με τη δημοτικότητα του νομίσματος μεταξύ του διαδικτυακού υποκόσμου, όπως τους εμπόρους ναρκωτικών, η τιμή του bitcoin τριπλασιάστηκε σε περίπου μια εβδομάδα και έφτασε τα 27 δολάρια (Chen Adrian, 2011). Η αξία όλων των bitcoins τα οποία είχαν κυκλοφορήσει μέχρι τότε πλησίαζε τα 130 εκατομμύρια δολάρια συνολικά. Ένας κάτοικος του Τενεσί ο οποίος ονομάστηκε KnightMB, κατείχε 371.000 bitcoins, δηλαδή αξία άνω των 10 εκατομμυρίων δολαρίων, και αποτέλεσε τον πλουσιότερο άνθρωπο στο δίκτυο του Bitcoin. Η αξία των 10.000 bitcoins τα οποία είχε δώσει ο Laszlo Hanyecz για να αγοράσει τις δυο πίτσες είχε φτάσει τα 272.329 δολάρια.



Εικ.22. Η πορεία του Bitcoin από τον Οκτώβριο του 2010 έως τον Οκτώβριο του 2011

Στη συνέχεια, μετά τις δηλώσεις της Mt. Gox, της μεγαλύτερης αγοράς συναλλάγματος bitcoin προτού πτωχεύσει το 2014, πως υπάρχει κίνδυνος διαρροής πληροφοριών ξεκίνησε

πτώση της τιμής φτάνοντας τα 2.05 δολάρια τον Νοέμβριο του 2011. Από αυτό το σημείο και μετά, η αύξηση της τιμής του Bitcoin γίνεται με πολύ αργούς ρυθμούς φτάνοντας τα 13.30 δολάρια όπου σταθεροποιείται για λίγα χρόνια. Στις 9 Απρίλιου του 2013 η τιμή εκτοξεύεται στα 230 δολάρια και στις 16 Απρίλιου του 2013, μόλις 6 μέρες μετά, η τιμή πέφτει στα 68.36 δολάρια. Πρόκειται για 61% μείωση της τιμής σε μόλις μια μέρα.



Εικ.23. Η πορεία του Bitcoin από τον Μάιο του 2012 έως τον Μάιο του 2013

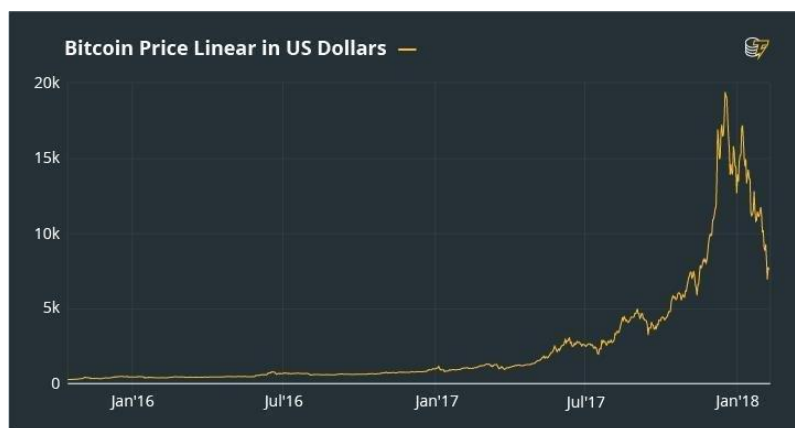
Έπειτα από σκαμπανεβάσματα καθ' όλη τη διάρκεια του συγκεκριμένου έτους, η τιμή καταφέρνει και φτάνει τα 200 δολάρια όπου σταθεροποιείται μέχρι τον Νοέμβριο, ενώ το Δεκέμβριο έχοντας τραβήξει την προσοχή των μέσων μαζικής ενημέρωσης, πολλοί οργανισμοί σε όλο τον κόσμο ανακοινώνουν ότι αρχίσαν να δέχονται πληρωμές σε Bitcoin και η τιμή εκτοξεύεται στα 1.147,25 δολάρια. Τον Απρίλιο του 2014 η τιμή μειώθηκε κατά 80% και έφτασε τα 360.84 δολάρια στην οποία τιμή σταθεροποιείται για τα επόμενα τουλάχιστον τρία χρόνια (capital.gr, 2018).



Εικ.24. Η πορεία του Bitcoin από τα τέλη του 2013 έως τα μέσα του 2015

Συνεχίζοντας, η Mt. Gox το 2014 χρεωκοπεί μιας και υπέστη θύμα επίθεσης από χάκερς οι οποίοι κατάφεραν να κλέψουν περίπου 850.000 bitcoins, αντιστοιχούμενα σε περίπου μισό

δισεκατομμύριο δολάρια, κάτι που ανάγκασε την τιμή του Bitcoin να μειωθεί κατά 30%. Αυτή αποτελεί και την μεγαλύτερη κλοπή στον κόσμο των ψηφιακών νομισμάτων αναδεικνύοντας τις αδυναμίες του πρωτοκόλλου και τους κινδύνους. Τον Αύγουστο του 2017 ο κώδικας του Bitcoin διασπάται για να δημιουργηθεί το Bitcoin Cash, ένας κλώνος του bitcoin και πάρα την δυσαρέσκεια πολλών χρηστών για αυτή την κίνηση, τον Δεκέμβριο του 2017 η τιμή του Bitcoin εκτοξεύεται στο ιστορικό νούμερο των 19.666 δολαρίων, αύξηση άνω του 1300% της τιμής του σε διάστημα μόλις ενός έτους.



Εικ.25. Η πορεία του Bitcoin από τις αρχές του 2016 έως τις αρχές του 2018

Με την αύξηση της τιμής πολλοί μικροεπενδυτές έσπευσαν να αγοράσουν bitcoins, όμως τον Ιούνιο του 2018 η τιμή φαίνεται πως κυμάνθηκε σε πολύ χαμηλότερο επίπεδο από την τιμή του Δεκεμβρίου του 2017, αφού το Bitcoin στεκόταν λαβωμένο από την αυστηρότερη κανονιστική εποπτεία σε όλο τον κόσμο και από τη μείωση του ενδιαφέροντος των μικροεπενδυτών. Τον Οκτώβριο του 2018 η παγκόσμια εποπτική αρχή για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες ανακοίνωσε ότι θα εφαρμόσει από το επόμενο έτος κανόνες σχετικά με τον τρόπο με τον οποίο οι κυβερνήσεις θα πρέπει να ρυθμίζουν τα ανταλλακτήρια κρυπτονομισμάτων σε μια προσπάθεια να εξαλειφθεί η εγκληματική χρήση bitcoin και άλλων ψηφιακών νομισμάτων (capital.gr, 2018).



Εικ.26. Η πορεία του Bitcoin από τις αρχές του 2018 έως τις αρχές του 2019

7.4. Επηρεασμός της αξίας

Μελετώντας τα στοιχεία που δόθηκαν στο προηγούμενο κεφάλαιο και παρατηρώντας την συνολική πορεία του Bitcoin από το ξεκίνημά του έως τις μέρες μας είναι ιδιαίτερα εμφανής η αστάθεια της τιμής του μέσω μεγάλων διακυμάνσεων, χωρίς κάποια αλληλουχία στο μέγεθος τους, ιδιαίτερα εν καιρώ ραγδαίων διεθνών πολιτικοοικονομικών μεταβολών. Μπορεί εύκολα να διαπιστωθεί πως έχουν υπάρξει διακυμάνσεις οι οποίες ήταν πολύ μικρές σε μεγάλα χρονικά διαστήματα, όπως το διάστημα ενός χρόνου, ενώ αντίθετα άλλες οι οποίες ήταν πολύ μεγάλες σε μικρά χρονικά διαστήματα, για παράδειγμα λίγες ημέρες ή μήνες.

Η τιμή του Bitcoin όπως έχει προαναφερθεί εξαρτάται πολύ από μεταβλητές τεχνικής φύσεως, όπως η υπολογιστική ισχύς και το μέγεθος του δικτύου εξόρυξης. Πιο αναλυτικά, όσο μεγαλύτερο είναι το δίκτυο των χρηστών που ασχολείται με το mining και αντίστοιχα όσο μεγαλύτερη είναι η υπολογιστική ισχύς που χρησιμοποιείται σε αυτό, τόσο πιο δύσκολη και δαπανηρή καθίσταται η διαδικασία της εξόρυξης και επομένως η διαδικασία της παραγωγής νέων bitcoins. Αντίθετα όσο ευκολότερη και γρηγορότερη είναι η διάθεση των bitcoins τόσο μικρότερη είναι και η τιμή του. Αυτό έχει ως αποτέλεσμα, η τιμή του bitcoin να πρέπει να αυξηθεί καθώς αυξάνεται και το κόστος παραγωγής του (Cronimund Christoph, 2014). Ωστόσο, υπάρχουν και άλλοι παράγοντες που επηρεάζουν την τιμή του κρυπτονομίσματος οι οποίοι είναι οι εξής:

Προσφορά

Είναι ευρέως γνωστό ότι το Bitcoin έχει κατά πολύ μεγαλύτερη κεφαλαιοποίηση αγοράς έναντι των υπολοίπων κρυπτονομισμάτων. Η προσφορά του ωστόσο έχει άμεση σχέση με το αποθεματικό του σε κυκλοφορία. Το σύνολο των bitcoins που μπορούν να δημιουργηθούν είναι ήδη γνωστό και όπως έχει αναφερθεί δεν ξεπερνά τα 21.000.000 bitcoins σε αριθμό. Συγκεκριμένα, η προσφορά αυξάνεται κάθε δέκα λεπτά με την προσθήκη καινούργιων block στην blockchain. Η ανταμοιβή κάθε block ξεκίνησε στα 50 bitcoins και ο αριθμός των bitcoins που δίνονται για κάθε νέο block που δημιουργείται μειώνεται σταδιακά. Ειδικότερα, η ανταμοιβή μειώνεται κατά το ήμισυ κάθε 210.000 block ή περίπου κάθε 4 χρόνια. Επίσης, θα πρέπει να ληφθεί υπόψιν ότι η προσφορά μειώνεται και μέσα από την απώλεια ή καταστροφή κάποιων ιδιωτικών κλειδιών, και συνεπώς των bitcoins που αντιστοιχούν σε αυτά, καθώς και από την αποταμίευση κάποιων άλλων bitcoin.

Ζήτηση

Η μελλοντική τιμή του Bitcoin είναι ένα βασικός παράγοντας που επηρεάζει την ζήτηση του συγκεκριμένου κρυπτονομίσματος. Όσο περισσότερο αυξάνει η τιμή του Bitcoin τόσο θα αυξάνει και η ζήτηση του, αντιθέτως με τη μείωση της τιμής θα μειώνεται και η ζήτηση διότι οι χρήστες δεν θα θέλουν να επενδύσουν σε ένα κρυπτονόμισμα δίχως μέλλον. Για παράδειγμα, δεν είναι λίγες οι περιπτώσεις όπου ο κόσμος προμηθεύεται το Bitcoin όχι για να το ανταλλάξει με αγαθά και υπηρεσίες αλλά για την υπερτιμημένη αξία του έχοντας ως σκεπτικό ότι η πώληση του θα επιφέρει περισσότερο κέρδος. Με άλλα λόγια, η τιμή του Bitcoin ανεβαίνει, από τις εικασίες ότι θα αυξηθεί και άλλο η αξία του (Μπαλάς Φώτης, 2017).

Επίσης, η φορολόγηση, τα έξοδα συναλλαγών καθώς και οι οροί ανταλλαγής των bitcoins με το παραστατικό χρήμα μπορούν να επηρεάσουν το βαθμό ζήτησης του. Επιπλέον, τα πλεονεκτήματα και τα οφέλη που προσφέρει στους χρήστες, όπως η ανωνυμία, η διαφάνεια, η αμεσότητα, η πραγματοποίηση συναλλαγών παγκοσμίως είναι λίγα από τα θετικά στοιχεία που μπορούν να αυξήσουν την ζήτηση του. Αντιθέτως, τα μειονεκτήματα και οι κίνδυνοι που το διέπουν όπως η κλοπή, η απάτη ακόμα και η αστάθεια της τιμής του, καθώς και η ανάγκη χρήσης ψηφιακών πορτοφολιών μπορούν να μειώσουν το βαθμό ζήτησης του.

Τέλος, είναι μείζονος σημασίας να σημειωθεί πως το Bitcoin έχει ιδιότητες που το καθιστούν όμοιο με το χρυσό, με άλλα λόγια η παραγωγή των bitcoin νομισμάτων είναι συγκεκριμένη, 21 εκατομμύρια bitcoins, το οποίο αποτελεί σημαντικό περιορισμό σε σύγκριση με τα παραστατικά χρήματα και αποτελεί έναν σημαντικό λόγο επηρεασμού της τιμής του. Επιπλέον, η δημιουργία νέων bitcoins με μειωμένο και προβλέψιμο ρυθμό συνεπάγεται ότι η ζήτηση θα πρέπει να ακολουθεί το επίπεδο του πληθωρισμού για να κρατήσει σταθερή την τιμή.

Δημοφιλία και Ελκυστικότητα

Ένας άλλος παράγοντας επηρεασμού της τιμής και της αξίας του Bitcoin είναι το πόσο ελκυστικό και το πόσο δημοφιλές είναι στον χώρο των κρυπτονομισμάτων. Τα μέσα κοινωνικής δικτύωσης καθώς και τα μέσα μαζικής ενημέρωσης και σε γενικό πλαίσιο το διαδίκτυο μπορούν πολύ εύκολα να επηρεάσουν την τιμή ενός κρυπτονομίσματος, είτε θετικά είτε αρνητικά, αφού έχουν άμεση επιρροή στους χρήστες και ως ένα βαθμό

συμβάλλουν στην λήψη των αποφάσεων τους. Παραδείγματος χάριν, όπως τονίστηκε νωρίτερα, οι δηλώσεις της Mt. Gox, ότι υπάρχει κίνδυνος διαρροής πληροφοριών μέσα από τη χρήση του Bitcoin επηρέασε πολύ αρνητικά την τιμή του κρυπτονομίσματος, ενώ αντίθετα ένα ευνοϊκό ως προς το Bitcoin άρθρο το οποίο δημοσιεύθηκε στο περιοδικό Forbes βοήθησε στην άνοδο της τιμής του.

Ωστόσο, ο κίνδυνος και η αβεβαιότητα του συστήματος επηρεάζουν σε μεγάλο βαθμό την δημοφιλία και την ελκυστικότητα του κρυπτονομίσματος. Στο παρελθόν έχουν γίνει πολλές προσπάθειες επιθέσεων από χάκερς έναντι των κρυπτονομισμάτων, κάποιες από τις οποίες ήταν ατελέσφορες αλλά και άλλες με σημαντικά και αξιοσημείωτα αποτελέσματα, όπως για παράδειγμα η επίθεση στην εταιρεία Mt. Gox, όπου το 2014 οι χάκερς κατάφεραν να κλέψουν περίπου 850.000 bitcoins, αντιστοιχούμενα σε περίπου μισό δισεκατομμύριο δολάρια.

Επιπρόσθετα, ενώ ένα μεγάλο πλήθος νέων κρυπτονομισμάτων έχει δημιουργηθεί προσπαθώντας να αντικαταστήσουν το Bitcoin, κανένα από αυτά τα κρυπτονομίσματα δεν έχει καταφέρει να προσελκύσει τόσο μεγάλο ενδιαφέρον από τους χρήστες και τους επενδυτές όσο αυτό, γεγονός το οποίο υπόκειται στην αυξημένη ζήτηση του Bitcoin αλλά και στην θέση την οποία κατέχει στην επικαιρότητα, κάτι που αναμφισβήτητα βοηθά στην ένταξη του ως πρώτη επιλογή στις αποφάσεις των χρηστών, διότι ο περισσότερος κόσμος δεν επιθυμεί να ξοδέψει χρόνο και χρήμα ώστε να ανακαλύψει κάποια άλλη πιθανή επενδυτική ευκαιρία και κατ' επέκταση ακολουθεί την δημοφιλέστερη επιλογή.

Πολιτικές εξελίξεις και οικονομικές μεταβολές

Σήμερα, στην εποχή της παγκοσμιοποίησης, οι αποφάσεις σε μια μόνο χώρα μπορούν να επηρεάσουν ολόκληρο τον κόσμο, για παράδειγμα, το γεγονός ότι η Ιαπωνία δέχτηκε το Bitcoin ως μέσο πληρωμής αποτέλεσε τρανταχτή είδηση και αδιαμφισβήτητα επηρέασε την τιμή και την αξία του κρυπτονομίσματος (Tar Andrew, 2017). Αντίστοιχα, οι ανακοινώσεις από την εφορία των Ηνωμένων Πολιτειών, οι οποίες δηλώνουν το κρυπτονόμισμα ως «περιουσιακό στοιχείο» για φορολογικούς λόγους είχαν μικτές επιδράσεις στην μεταβλητότητα της τιμής του Bitcoin.

Από τη θετική πλευρά, οποιαδήποτε δήλωση πραγματοποιείται η οποία αναγνωρίζει με οποιονδήποτε τρόπο το κρυπτονόμισμα επιδρά θετικά στην αποτίμηση της αγοράς του

νομίσματος. Αντίθετα, η απόφαση να θεωρηθεί «περιουσιακό στοιχείο» είχε δυο αρνητικές επιπτώσεις. Η πρώτη ήταν η προσθετή πολυπλοκότητα για τους χρήστες οι οποίοι επιθυμούν να πληρώσουν με τη χρήση κρυπτονομισμάτων μιας και πλέον θα πρέπει να καταγράφουν την αξία του νομίσματος κατά τη στιγμή της κάθε συναλλαγής ανεξάρτητα από το πόσο που θα ξοδέψουν. Δεύτερον, η απόφαση να θεωρηθεί το νόμισμα ως «περιουσιακό στοιχείο» για φορολογικούς σκοπούς, αντιλαμβάνεται από κάποιους ως μήνυμα ότι η εφορία ετοιμάζεται να επιβάλει ισχυρότερους κανονισμούς και περιορισμούς στο μέλλον (Barker Jonathan Todd, 2014).

Επιπρόσθετα, η τιμή του Bitcoin εξαρτάται και επηρεάζεται από τη συναλλαγματική του ισοτιμία έναντι σε άλλα νομίσματα, όπως το δολάριο ή το ευρώ αλλά και από χρηματοοικονομικούς δείκτες, όπως η τιμή του χρυσού και του πετρελαίου, οι οποίοι αντανακλούν την εξέλιξη της παγκόσμιας οικονομίας.

Κεφάλαιο 8: Συναλλαγές κρυπτονομισμάτων

8.1. Επίτευξη συναλλαγών με Bitcoin

Στις προηγούμενες ενότητες μελετήθηκε η ιστορία των κρυπτονομισμάτων, το πρώτο κρυπτονόμισμα και ο δημιουργός του, οι τρόποι με τους οποίους μπορεί κάποιος να αποκτήσει και να αποθηκεύσει τα κρυπτονομίσματα, η τιμή και η αξία του πρώτου κρυπτονομίσματος που εμφανίστηκε στην αγορά και εν τέλει έγινε προσπάθεια κατανόησης για το αν αξίζει ή όχι κάποια επένδυση σε αυτό. Στο παρόν κεφάλαιο θα πραγματοποιηθεί μεγαλύτερη εμβάθυνση ως προς τις συναλλαγές των κρυπτονομισμάτων, έχοντας ως παράδειγμα το δημοφιλέστερο στις μέρες μας Bitcoin κρυπτονόμισμα, και χρησιμοποιώντας όλα τα στοιχεία τα οποία μελετήθηκαν θα γίνει περισσότερο κατανοητός ο τρόπος με τον οποίο αυτές επιτυγχάνονται, με την χρήση πάντοτε της καινοτόμα τεχνολογίας blockchain.

Ως πρώτο βήμα για να ξεκινήσει μια συναλλαγή θα πρέπει και ο αποστολέας αλλά και ο παραλήπτης, οι οποίοι θα λάβουν μέρος στη συναλλαγή, να διαθέτουν το απαραίτητο λογισμικό για τη δημιουργία ψηφιακών πορτοφολιών. Μέσα από αυτό το λογισμικό θα δημιουργηθεί για τον καθένα ξεχωριστά μια μοναδική σειρά από γράμματα και αριθμούς η οποία θα αποτελέσει τη Bitcoin διεύθυνση του κάθε χρήστη και θα εμπεριέχει το σύνολο των bitcoins του και το ιστορικό των συναλλαγών του. Τονίζεται πως αυτή η διεύθυνση δεν συνδέεται με το όνομα του χρήστη ή με άλλα προσωπικά του δεδομένα, και είναι ο μόνος τρόπος αναγνώρισής του μέσα σε ολόκληρο το δίκτυο. Τα ψηφιακά πορτοφόλια των χρηστών παρέχουν πρόσβαση σε πολλαπλές διευθύνσεις Bitcoin, επομένως ένας χρήστης μπορεί να δημιουργήσει όσες διευθύνσεις επιθυμεί και μάλιστα θεωρείται καλύτερη και σωστότερη πρακτική να δημιουργείται μια νέα διεύθυνση για κάθε συναλλαγή η οποία πραγματοποιείται, ώστε να παρέχεται μεγαλύτερη ασφάλεια και ιδιωτικότητα.

Η δημιουργία μιας νέας διεύθυνσης στην πραγματικότητα σημαίνει δημιουργία ενός νέου κρυπτογραφικού ζεύγους, το οποίο αποτελείται από ένα δημόσιο και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί είναι η διεύθυνσή Bitcoin που αναφέρθηκε νωρίτερα η οποία είναι γνωστή προς όλους και η οποία δίνεται σε κάποιον άλλον χρήστη προκειμένου να στείλει κάποια πληρωμή. Από την άλλη, το ιδιωτικό κλειδί είναι ένα άλλο σύνολο αλφαριθμητικών χαρακτήρων το οποίο είναι προσωπικό για κάθε χρήστη, κάνεις άλλος δεν το γνωρίζει και χρησιμοποιείται για την υπογραφή των συναλλαγών. Όλες οι συναλλαγές υπογράφονται με το ιδιωτικό κλειδί και μαζί με τον αριθμό bitcoins κάθε συναλλαγής ταξιδεύουν σε όλο το δίκτυο με τη μορφή της

ψηφιακής υπογραφής. Τα δυο κλειδιά σχετίζονται μεταξύ τους, αφού το λογισμικό Bitcoin μπορεί να επαληθεύσει συναλλαγές μόνο αν η υπογραφή η οποία δημιουργήθηκε με ένα ιδιωτικό κλειδί αντιστοιχεί στη εκάστοτε δημόσια διεύθυνση, χωρίς ωστόσο να γνωρίζει ποιο είναι αυτό το ιδιωτικό κλειδί. Τονίζεται, πως δεν υπάρχει τρόπος να ανακαλύψει κάποιος το ιδιωτικό κλειδί ενός χρήστη γνωρίζοντας μόνο τη δημόσια διεύθυνσή του.

Σύμφωνα με τις διαδικασίες της blockchain, όταν ο αποστολέας αποφασίσει πως θέλει να πραγματοποιήσει μια συναλλαγή, θα πρέπει να γνωστοποιήσει αυτήν του την επιθυμία σε ολόκληρο το δίκτυο. Το λογισμικό σε αυτήν την περίπτωση καταγραφεί το αίτημα για τη συναλλαγή με τη χρήση ενός από τα ιδιωτικά κλειδιά του αποστολέα με το οποίο υπογράφεται η συναλλαγή που επιθυμεί. Έπειτα ο αποστολέας προσθέτει μια από τις δημοσιές διευθύνσεις του παραλήπτη στην οποία θα αποσταλούν τα νομίσματα bitcoin και περιμένει την επιβεβαίωση από το δίκτυο. Σε αυτό το σημείο όλοι οι χρήστες του δικτύου θα πρέπει να επαληθεύσουν αρχικά ότι ο αποστολέας έχει τον απαιτούμενο αριθμό bitcoins ώστε να πραγματοποιηθεί η συναλλαγή και δεύτερον ότι τα bitcoins δεν έχουν ήδη αποσταλεί σε κάποιον άλλον χρήστη. Αυτό επιτυγχάνεται όταν ο καθένας στο δίκτυο χρησιμοποιήσει το δημόσιο κλειδί για να επαληθεύσει ότι το αίτημα συναλλαγής έρχεται από τον νόμιμο ιδιοκτήτη του λογαριασμού. Στη συνέχεια, το δίκτυο μέσα από το ιστορικό συναλλαγών, στο οποίο έχουν όλοι πρόσβαση εξαιτίας της δημοσίας διεύθυνσης, επαληθεύει ότι ο χρήστης δεν έχει ξοδέψει κάπου αλλού τα νομίσματα του.

Μόλις αυτές οι πληροφορίες επαληθευτούν και καταστούν έγκυρες τότε η συναλλαγή συμπεριλαμβάνεται στο νέο block που δημιουργείται μαζί με άλλες συναλλαγές. Για να δημιουργηθεί το νέο block και να συμπεριληφθούν οι συναλλαγές σε αυτό, κάποιοι χρήστες του δικτύου οι οποίοι λαμβάνουν μέρος στη διαδικασία της εξόρυξης και ονομάζονται miners χρησιμοποιούν τους καταλληλά εξοπλισμένους ηλεκτρονικούς τους υπολογιστές. Η δουλειά των miners είναι αρχικά μέσω της υπολογιστικής τους ισχύος να υπολογίσουν κρυπτογραφημένες συναρτήσεις κατακερματισμού και να επικυρώσουν τις νέες συναλλαγές με την καταγραφή τους στην blockchain.

Η μέθοδος κατακερματισμού ουσιαστικά μετατρέπει μια συλλογή δεδομένων σε ένα αλφαριθμητικό σύνολο χαρακτήρων συγκεκριμένου σταθερού μήκους το οποίο ονομάζεται τιμή κατακερματισμού. Οποιαδήποτε αλλαγή πραγματοποιηθεί στα αρχικά δεδομένα, όσο μικρή και αν είναι, θα αλλάξει την τελική τιμή κατακερματισμού. Είναι αδύνατο επομένως, να προβλέψει

κάποιος ποιο ήταν το αρχικό σύνολο δεδομένων που δημιούργησε μια συγκεκριμένη τιμή κατακερματισμού. Με τη βοήθεια του nonce, ενός τυχαίου αριθμού ο οποίος προστίθεται στα δεδομένα πριν το κατακερματισμό, καταφέρνει το σύστημα να δημιουργήσει διαφορετικές τιμές κατακερματισμού για τα ίδια δεδομένα, αφού αλλάζοντας αυτόν τον αριθμό προκύπτει μια τελείως διαφορετική τιμή κατακερματισμού.

Το σύστημα του Bitcoin ωστόσο, απαιτεί η νέα τιμή να έχει μια συγκεκριμένη μορφή και να ξεκινάει με έναν ορισμένο αριθμό μηδενικών. Για να επιτευχθεί κάτι τέτοιο, υπάρχει ένας μοναδικός συνδυασμός μεταξύ των αρχικών δεδομένων και του nonce. Οι miners δεν μπορούν να προβλέψουν ποιος αριθμός nonce μπορεί να παράγει το επιθυμητό αποτέλεσμα οπότε αναγκάζονται να δημιουργούν πολλές τιμές κατακερματισμού μέχρι να το πετύχουν. Κάθε νέο block το οποίο δημιουργείται περιλαμβάνει μια νέα συναλλαγή με bitcoins η οποία αντιστοιχεί στην ανταμοιβή του συμμετέχον ο οποίος καταφέρνει να βρει τη λύση. Ο «νικητής» μπορεί να βρει τα νέα του νομίσματα σε μια νέα διεύθυνσή η οποία δημιουργείται αυτόματα στο ψηφιακό του πορτοφόλι. Όπως έχει αναφερθεί, η ανταμοιβή υποδιπλασιάζεται ανά 210.000 block, ή περίπου κάθε 4 χρόνια, με την ανταμοιβή του block σήμερα, το έτος 2019 να είναι στα 12,5 bitcoins.

Με τη πάροδο του χρόνου η κάθε συναλλαγή η οποία πραγματοποιείται θάβεται κάτω από άλλες πιο πρόσφατες συναλλαγές. Το ιστορικό των συναλλαγών είναι άμεσα διαθέσιμο, αφού είναι δημόσιο και το γνωρίζουν όλα τα μέλη του δικτύου, διότι ο καθένας διαθέτει το δικό του αντίγραφο της blockchain. Αν τύχει και κάποιος θέλει να τροποποιήσει ή να καταργήσει μια συναλλαγή θα πρέπει να επαναλάβει όλη τη διαδικασία που έκαναν οι miners, διότι οι αλλαγές απαιτούν ένα τελείως διαφορετικό nonce από το προηγούμενο. Ωστόσο θα πρέπει να αλλάξουν και όλα τα blocks τα οποία δημιουργήθηκαν μετέπειτα από αυτό, καθότι κάθε block περιέχει και την υπογραφή του προηγούμενου του με το οποίο είναι συνδεδεμένο στη blockchain. Όμως, μέχρι ένας χρήστης να καταφέρει να επιλύσει κάτι τόσο δύσκολο θα έχουν ήδη δημιουργηθεί κάποια άλλα blocks τα οποία θα πρέπει επίσης να τροποποιήσει. Αυτή η διαδικασία είναι δύσκολο να πραγματοποιηθεί και είναι απίθανο να γίνει, όχι όμως ακατόρθωτο (Acheson Noelle, How do Bitcoin transactions work?, 2013).

Τέλος, αν εμφανιστεί κάποιος χρήστης ο οποίος προσπαθήσει να δημιουργήσει μια συναλλαγή η οποία δεν είναι εφικτό να πιστοποιηθεί από τη πλειοψηφία των μελών του δικτύου, τότε αυτή θεωρείται ψευδής και απορρίπτεται από το σύστημα. Αυτή είναι και η αρχή του

Bitcoin πρωτοκόλλου, με λίγα λόγια μια συναλλαγή πρέπει να πιστοποιείται από όλους για να είναι έγκυρη. Επομένως, όσο πιο πολλοί χρήστες συμμετέχουν στο δίκτυο τόσο πιο δύσκολο είναι να πλαστογραφηθούν συναλλαγές από κακόβουλους χρήστες (Σπαθάς Βαγγέλης, 2017).

8.2. Ιδιότητες των συναλλαγών

Το Bitcoin είναι ένα κρυπτονόμισμα το οποίο αναπτύχθηκε και εξελίχθηκε εξαιτίας κάποιων ιδιαίτερων ιδιοτήτων που παρέχει στις συναλλαγές του, όπως η ελάχιστη χρέωση μεταξύ των συναλλαγών, η ανωνυμία και το επίπεδο ασφάλειας που προσφέρει. Πιο αναλυτικά αυτές οι ιδιότητες είναι οι εξής:

Μικρότερα τέλη συναλλαγών

Σύμφωνα με την ιστοσελίδα bitcoin.org οι περισσότερες συναλλαγές μπορούν να επεξεργαστούν χωρίς τέλη, όμως οι χρήστες ενθαρρύνονται να πληρώνουν εθελοντικά ένα μικρό ποσό ως τέλος συναλλαγής για ταχύτερη επιβεβαίωση των συναλλαγών. Τα τέλη συναλλαγών περιλαμβάνονται στη συναλλαγή bitcoin νομισμάτων προκειμένου η συναλλαγή να επεξεργαστεί από κάποιο χρήστη ο οποίος συμμετέχει στη διαδικασία της εξόρυξης και να επικυρωθεί από το δίκτυο. Ο διαθέσιμος χώρος για συναλλαγές σε ένα block του Bitcoin είναι αυτή τη στιγμή περιορισμένος και προς το παρόν δεν ξεπερνάει το 1 MB. Αυτό σημαίνει ότι αν κάποιος επιθυμεί να γίνει πιο γρήγορη η επεξεργασία της συναλλαγής του θα πρέπει να δώσει περισσότερα χρήματα από ότι οι άλλοι χρήστες (bitcoinfees.info).

Τονίζεται, πως το τέλος συναλλαγής επηρεάζει μόνο το χρόνο αναμονής για την πρώτη επιβεβαίωση και πως συνήθως στις συναλλαγές Bitcoin οι παραλήπτες απαιτούν μεταξύ 2 έως 6 επιβεβαιώσεων προκειμένου να θεωρηθεί μια συναλλαγή έγκυρη. Με την απόκτηση της πρώτης επιβεβαίωσης η συναλλαγή συμπεριλαμβάνεται σε ένα block και ο χρόνος αναμονής για κάθε επιπλέον επιβεβαίωση είναι συνήθως δέκα λεπτά και είναι ανεξάρτητος από το τέλος συναλλαγής που δόθηκε.

Σύμφωνα με υποθέσεις τις ιστοσελίδας bitcoinfees.info για να συμπεριληφθεί μια συναλλαγή στο επόμενο block σε 10 λεπτά χρειάζονται περίπου 0.12 δολάρια. Αντίστοιχα για να συμπεριληφθεί σε ένα από τα επόμενα τρία block με εκτιμώμενο χρόνο 30 λεπτά θα χρειαστούν περίπου 0.10 δολάρια, ενώ για να συμπεριληφθεί σε ένα από τα επόμενα έξι

block με εκτιμώμενο χρόνο μια ώρα θα χρειαστούν περίπου 0.04 δολάρια. Ωστόσο, ο ακριβής τρόπος με τον οποίο λειτουργούν και υπολογίζονται τα τέλη είναι ακόμα σε διαδικασίες εξέλιξης και ενδέχεται να αλλάξει με την πάροδο του χρόνου. Τα τέλη συναλλαγών δεν σχετίζονται με το ποσό των bitcoins που αποστέλλεται με αποτέλεσμα κάποιες φορές να είναι πολύ χαμηλά για παράδειγμα 0.00005 bitcoins για μεταφορά 1.000 bitcoins, ή να είναι πολύ υψηλά για παράδειγμα 0.00004 bitcoins για μεταφορά 0.02 bitcoins. Επομένως, το τέλος συναλλαγής ορίζεται από τα δεδομένα της συναλλαγής και την περιοδικότητα της (bitcoin.org).

Ανωνυμία και διαφάνεια συναλλαγών

Ένα βασικό χαρακτηριστικό του Bitcoin είναι η ανωνυμία μιας και είναι ένα κρυπτονόμισμα που χρησιμοποιεί την τεχνολογία της κρυπτογραφίας για τη δημιουργία τόσο της δημοσίας διεύθυνσης του κάθε χρήστη όσο και του ιδιωτικού του κλειδιού. Δυο Ιρλανδοί επιστήμονες οι οποίοι ειδικεύονται στην ανάλυση δικτύων απέδειξαν, έπειτα από έρευνες, ότι το Bitcoin δεν είναι τόσο ανώνυμο όσο πιστεύεται αφού κατάφεραν να αναγνωρίσουν συναλλαγές πολλών ανθρώπων οι οποίοι είχαν δωρίσει bitcoins στο Wikileaks, δωρεές που ο οργανισμός αρνήθηκε ότι δέχτηκε τον Ιούνιο του 2011 (Wallace Benjamin, 2011).

Προκύπτει επομένως, ότι στην πραγματικότητα το Bitcoin δεν πρόκειται για ένα ανώνυμο κρυπτονόμισμα και ότι στ' αλήθεια μπορεί να προσφέρει το ίδιο επίπεδο προστασίας προσωπικών δεδομένων όπως τα μετρητά. Ωστόσο είναι το πιο διάφανες δίκτυο πληρωμών στο κόσμο, αφού δεν επιτρέπει την αντιγραφή και χρήση πάνω από δυο φορές του ιδίου νομίσματος και ο ανοικτός κώδικάς του παρέχει τη δυνατότητα ελέγχου από οποιονδήποτε προγραμματιστή οποιαδήποτε στιγμή. Παρόλα αυτά, με τη προϋπόθεση ότι το Bitcoin χρησιμοποιείται σωστά μπορεί να προσφέρει αρκετά αποδεκτά επίπεδα προστασίας των προσωπικών δεδομένων των χρηστών του, αν και η διασφάλιση της ανωνυμίας έγκειται περισσότερο στα χεριά του εκάστοτε χρήστη και όχι τόσο στο ίδιο το πρωτόκολλο (bitcoin.org).

Προκειμένου να ληφθεί το λογισμικό και να δημιουργηθεί ένα ψηφιακό πορτοφόλι του χρήστη, το οποίο δεν αντιστοιχεί σε κάποιον τραπεζικό του λογαριασμό, δεν απαιτούνται προσωπικά δεδομένα, όπως το όνομα του άλλα ούτε και κάποιο άλλο προσωπικό έγγραφο, όπως για παράδειγμα αστυνομική ταυτότητα ή εκκαθαριστικό εφορίας. Μπορεί ωστόσο η ταυτότητα του χρήστη να παραμένει άγνωστη και μια συναλλαγή μπορεί να

πραγματοποιηθεί χωρίς να γνωρίζει ο αποστολέας ποιος είναι ο παραλήπτης, όμως οι ανώνυμες αυτές συναλλαγές δεν προσφέρουν πλήρη απόκρυψη των ψηφιακών ιχνών μιας και παραμένουν για πάντα καταγεγραμμένες στο δίκτυο του Bitcoin. Με την προσθήκη μιας συναλλαγής στο δίκτυο καταγράφονται τα δημόσια κλειδιά του αποστολέα και του παραλήπτη και η χρονική περίοδος που ολοκληρώθηκε η συναλλαγή και από τη στιγμή που μια συναλλαγή προστεθεί στη blockchain του πρωτοκόλλου δεν μπορεί να αναιρεθεί ή να διαγραφεί από αυτή (trssllc.com, 2013).

Οι διευθύνσεις Bitcoin είναι η μονή πληροφορία η οποία χρησιμοποιείται για να δηλωθεί από ποιον λογαριασμό αποστέλλονται bitcoins και σε ποιον λογαριασμό εκχωρούνται. Αυτές οι διευθύνσεις όμως εμπεριέχουν όλο το ιστορικό των συναλλαγών στο οποίο εμπλέκονται και επομένως καθένας μπορεί να δει το υπόλοιπο αριθμό bitcoins κάθε διεύθυνσης άλλα και όλες τις συναλλαγές της. Για πιο ασφαλή και ανώνυμη χρήση του λογισμικού συνίσταται η χρήση πολλαπλών πορτοφολιών για διαφορετικούς σκοπούς ώστε να μην μπορούν να συσχετιστούν οι συναλλαγές μεταξύ τους. Το σημείο κλειδί στο πρωτόκολλο βρίσκεται σε αυτήν ακριβώς την πρακτική, διότι αφού δεν υπάρχει μια μοναδική διεύθυνσή για κάθε χρήστη δεν μπορεί να βρεθεί η ταυτότητα του έχοντας ως γνώση μόνο το ιστορικό των συναλλαγών.

Βέβαια, οι χρήστες συνήθως αποκαλύπτουν την ταυτότητα τους προκειμένου να λάβουν υπηρεσίες και αγαθά, οπότε οι διευθύνσεις δεν μπορούν να μείνουν πλήρως ανώνυμες. Προκειμένου να προστατευτούν τα προσωπικά δεδομένα του κάθε χρήστη, προτείνεται να γίνεται χρήση των διευθύνσεων μόνο μια φορά και έπειτα να δημιουργούνται καινούργιες διευθύνσεις κάθε φορά που επρόκειτο να πραγματοποιηθεί μια συναλλαγή. Ούτως ή άλλως, οι χρήστες με τους οποίους γίνονται οι συναλλαγές δεν μπορούν να δούνε ποιες άλλες διευθύνσεις έχει ο κάθε χρήστης και τι κάνει με αυτές (bitcoin.org).

Επιπρόσθετα, οι χρήστες από πλευράς τους πρέπει να είναι ιδιαίτερα προσεκτικοί ώστε να μην αποκαλύπτουν τις διευθύνσεις τους σε ιστοσελίδες ή μέσα κοινωνικής δικτύωσης και να μην δημοσιεύουν πληροφορίες σχετικές με τις συναλλαγές και τις αγορές τους οι οποίες θα μπορούσαν να επιτρέψουν σε κάποιον να τους ταυτοποιήσει. Μια άλλη πρόταση είναι η απόκρυψη της διεύθυνσης IP του υπολογιστή, χρησιμοποιώντας έναν πρόγραμμα ανώνυμης περιήγησης όπως το Tor, ώστε να μην θεωρηθεί κάποιος χρήστης λανθασμένα ως η πηγή μιας συναλλαγής ενώ δεν είναι στην πραγματικότητα. Τελικώς, θα πρέπει όλοι οι χρήστες να

είναι πολύ προσεκτικοί όταν χρησιμοποιούν ένα κρυπτονόμισμα, διότι ένα ανώνυμο νόμισμα διακατέχεται από σημαντικό κίνδυνο εξαπάτησης. Με λίγα λόγια, άμα κάποιος καταφέρει να κλέψει τα χρήματά ενός χρήστη δεν υπάρχει κανένας τρόπος να αποδείξει ότι ήταν δικά του (bitcoin.org).

Ασφάλεια συναλλαγών

Μια άλλη σημαντική ιδιότητα του κρυπτονομίσματος είναι η μεγάλη ασφάλεια που προσφέρει στις συναλλαγές του λόγω των τεχνολογιών της κρυπτογραφίας και της blockchain που χρησιμοποιεί. Το Bitcoin είναι το μεγαλύτερο διαμοιρασμένο πρωτόκολλο σε όλον τον κόσμο και η μονή του αδυναμία έγκειται στο λάθος του χρήστη. Τα bitcoin νομίσματα βρίσκονται αποθηκευμένα σε διευθύνσεις και μέσω της κρυπτογραφίας παραμένουν απροσπέλαστα από οποιονδήποτε άλλο εκτός του κάτοχου του ειδικού ιδιωτικού κλειδιού. Μόνο ο κάτοχος έχοντας το ιδιωτικό του κλειδί μπορεί να πραγματοποιήσει συναλλαγές μέσω της αντίστοιχης διεύθυνσης.

Ωστόσο τα ψηφιακά πορτοφόλια στα οποία είναι αποθηκευμένα τα ιδιωτικά κλειδιά των χρηστών είναι πολύ εύκολο να διαγράψουν, να χαθούν ή να κλαπούν, αλλά όπως έχει γνωστοποιηθεί υπάρχουν πολλοί τρόποι ώστε οι χρήστες να ασφαλίσουν και να προστατεύσουν όσο το δυνατό περισσότερο και καλύτερα τα χρήματά τους. Ως παράδειγμα για την μεγάλη ανάγκη προστασίας των πορτοφολιών αποτελεί ο Stefan Thomas ο οποίος είχε δημιουργήσει τρία αντίγραφα του ψηφιακού του πορτοφολιού. Εντούτοις κατάφερε κατά λάθος να διαγράψει τα δυο από αυτά και παράλληλα να χάσει τον κωδικό του για το τρίτο και έτσι έχασε γύρω στα 7.000 bitcoins (Wallace Benjamin, 2011).

Το πρωτόκολλο λειτουργεί και χρησιμοποιείται εδώ και δέκα χρόνια από χρήστες σε ολόκληρο τον κόσμο, γεγονός που αποτελεί ένδειξη ότι πρόκειται για μια ιδέα καλά δομημένη και σχεδιασμένη. Ωστόσο, οι συναλλαγές του Bitcoin γίνονται ηλεκτρονικά χρησιμοποιώντας το διαδίκτυο, και όπως συμβαίνει και με οποιοδήποτε άλλο ηλεκτρονικό σύστημα, κινδυνεύουν από χάκερς, κακόβουλά πρόγραμμα και λειτουργικές δυσλειτουργίες. Σε διάφορες χρονικές περιόδους έχουν εντοπιστεί και έχουν διορθωθεί διαφορές κενά ασφαλείας, γεγονός που «ωριμάζει» το Bitcoin ως τεχνολογία. Συχνά όμως, οι χάκερς δεν βάζουν στο στόχαστρο το Bitcoin αλλά συγκεκριμένες συναλλαγές ατόμων και πολλές φορές έχουν αποκτήσει πρόσβαση σε λογαριασμούς και ψηφιακά πορτοφόλια με αποθέματα

νομισμάτων. Το Cryptoaware.org εκτιμά ότι τουλάχιστον 2.3 δισεκατομμύρια δολάρια έχουν χαθεί σε απάτες και κλοπές από το 2011 μέχρι τον Αύγουστο του 2018.

Μια κλοπή αποτελεί ιδιαίτερο πρόβλημα αφού οι συναλλαγές είναι μόνιμες και δεν μπορούν να τροποποιηθούν, να ακυρωθούν ή να διαγραφτούν. Αν ένας κλέφτης καταφέρει και εισχωρήσει στο Bitcoin λογαριασμό κάποιου χρήστη ή αποκτήσει πρόσβαση στον σκληρό του δίσκο και καταφέρει να κλέψει το ιδιωτικό του κλειδί τότε θα έχει τη δυνατότητα να κλέψει τα bitcoins του και να τα μεταφέρει σε κάποιον άλλον δικό του λογαριασμό. Παρόλα αυτά, στην περίπτωση που ένας χρήστης ακολουθήσει σωστές πρακτικές, όπως πορτοφόλια εκτός σύνδεσης και συναλλαγές με πολλαπλές διευθύνσεις, τότε καταφέρνει να προστατεύει τα χρήματά του και συνάμα μειώνει τον κίνδυνο απώλειας και κλοπής.

Επιπρόσθετα, σημαντικό ρόλο στην ασφάλεια παίζει το γεγονός ότι δεν υπάρχει τρίτος μεσολαβητής να ενισχύει την εμπιστοσύνη του κόσμου ως προς το πρωτόκολλο. Με λίγα λόγια, δεν υπάρχει κανείς ο οποίος να είναι σε θέση να προσφέρει κάποιου είδους επιπλέον ασφάλεια στο σύστημα, γεγονός το οποίο έχει ως αποτέλεσμα στην περίπτωση που υπάρξει κάποιο πρόβλημα ο χρήστης να βρίσκεται μόνος του ενάντια σε ολόκληρο το δίκτυο χωρίς να μπορεί κανείς να τον βοηθήσει (cryptobeginners.info, Common crypto scams and how to avoid them).

Υπάρχουν πολλά παραδείγματα κλοπών και διαρροών ασφαλείας τα οποία συνέβησαν σε συναλλαγές και σε επιχειρήσεις, ωστόσο πριν γίνει αναφορά σε κάποια από αυτά τα γεγονότα πρέπει να τονιστεί ότι αυτά τα ατυχή περιστατικά δεν σχετίζονται με την απόκτηση παράνομης πρόσβασης στο ίδιο το πρωτόκολλο Bitcoin και επομένως δεν αποδεικνύουν τυχόν ελαττώματα του ιδίου του λογισμικού. Τον Ιούλιο του 2013, η Επιτροπή Κεφαλαιαγοράς (SEC) άσκησε νομική αγωγή εις βάρος ενός φορέα ο οποίος φαίνεται να είχε οργανώσει ένα σχέδιο Ponzi σχετιζόμενο με Bitcoins (cryptobeginners.info, Common crypto scams and how to avoid them).

Με λίγα λόγια, ενθάρρυνε επενδυτές να δώσουν τα χρήματά τους στην επιχείρηση και υστέρα απέδιδε κέρδη στους παλαιότερους επενδυτές χρησιμοποιώντας χρήματα τα οποία προέρχονταν από τους πιο προσφάτους επενδυτές. Μια άλλη νομισματική πλεκτάνη σχετιζόμενη με bitcoins ήταν όταν η Bitomat της Πολωνίας, η τρίτη μεγαλύτερη εταιρεία

συναλλαγής, αποκάλυψε ότι κατά λάθος αντικατέστησε ολόκληρο το πορτοφόλι της. Οι ερευνητές ασφαλείας ανίχνευσαν πολλαπλά κακόβουλα λογισμικά και ιούς στην ιστοσελίδα που προορίζονταν για χρήστες του Bitcoin. Κάποιοι από αυτούς τους ιούς είχαν σχεδιαστεί για να κλέβουν bitcoins μέσα από τα πορτοφόλια των χρηστών και κάποιοι άλλοι για να δέχονται υπολογιστική ισχύ από τους χρήστες εν αγνοία τους για την εξόρυξη νέων νομισμάτων (Wallace Benjamin, 2011).

Άλλες σημαντικές περιπτώσεις επιθέσεων είναι αρχικά η MyBitcoin, η παλαιότερη υπηρεσία πορτοφολιών η οποία σταμάτησε να ανταποκρίνεται στα μηνύματα ηλεκτρονικού ταχυδρομείου μέχρι που αποδείχτηκε ότι οποίος και αν ήταν αυτός ο οποίος διαχειριζόταν την υπηρεσία είχε κλέψει τα χρήματα όλων. Ωστόσο, ο υποτιθέμενος ιδιοκτήτης επανεμφανίστηκε αργότερα υποστηρίζοντας ότι ο ισότοπος του είχε χακαριστεί (Wallace Benjamin, 2011). Τον Ιούνιο του 2014 κάποιος ο οποίος ονομάζεται Allinvain ανέφερε ότι 25.000 bitcoins αξίας τότε άνω των 500.000 δολαρίων είχαν κλαπεί από τον υπολογιστή του, ισχυρισμοί οι οποίοι δεν έχει αποκαλυφθεί αν τελικά ισχύουν ή όχι (Κυρίτσης Άγγελος, 2014). Μια εβδομάδα αργότερα ωστόσο πραγματοποιήθηκε η σημαντικότερη ίσως επίθεση η οποία έχει καταγραφεί ως σήμερα στην ιστορία του κρυπτονομίσματος η οποία επηρέασε για αρκετά χρονιά ολόκληρο το δίκτυο του Bitcoin.

Συγκεκριμένα ένας χάκερ πραγματοποίησε μια επιτυχημένη επίθεση στην Mt. Gox, η οποία τότε χειριζόταν το 90% περίπου όλων των συναλλαγών bitcoin. Εκείνη την περίοδο η εταιρεία είχε περιορίσει τις αναλήψεις των λογαριασμών στα 1.000 δολάρια που αντιστοιχούσε τότε γύρω στα 35 bitcoins, και από πολλούς θεωρείται ότι αυτό το γεγονός πυροδότησε την επίθεση. Ο χάκερ αφού επιτέθηκε στο σύστημα έκλεψε δεκάδες χιλιάδες bitcoins άλλων ανθρώπων και οδήγησε τη συναλλαγματική ισοτιμία στο μηδέν. Με την δημοσίευση της συγκεκριμένης είδησης οι δυνάμεις της αγοράς έσπευσαν να αντιμετωπίσουν τον χάκερ και κατάφεραν να περιορίσουν την κλοπή του στα 2.000 bitcoins.

Ωστόσο, η τιμή του Bitcoin έπεσε κατακόρυφα δίχως να ανεβεί πάνω από τα 17 δολάρια για αρκετό καιρό και η εταιρεία έπαψε να λειτουργεί για μια περίπου εβδομάδα. Όμως, η ζημιά είχε ήδη γίνει και μέσα σε ένα μήνα η Mt. Gox έχασε το 10% του μεριδίου της αγοράς από μια άλλη εταιρεία από τη Χιλή με το όνομα TradeHill και εν τέλει κήρυξε πτώχευση. Δυστυχώς, αυτή η επίθεση μετέτρεψε, για αρκετό καιρό, το Bitcoin από το νόμισμα του μέλλοντος σε ένα δυστοπικό αστείο (Wallace Benjamin, 2011).

Κεφάλαιο 9: AltCoins

9.1. Η έννοια των AltCoins

Πριν γίνει αναφορά στα πλεονεκτήματα και στα μειονεκτήματα των κρυπτονομισμάτων θα πρέπει να μην παραληφθεί και η γνωστοποίηση κάποιων νέων κρυπτονομισμάτων, εκτός από το Bitcoin, τα οποία έχουν ξεκινήσει να εμφανίζονται και να εδραιώνονται στο χώρο της οικονομίας και της τεχνολογίας έχοντας το καθένα κάποιο δικό του ιδιαίτερο χαρακτηριστικό. Φυσικά, σε κάποιες περιπτώσεις τα νέα κρυπτονομίσματα αποτελούν απλά μια παραλλαγή ή απομίμηση των αρχικών ψηφιακών νομισμάτων χωρίς πραγματικές βελτιώσεις (Frankenfield Jake, 2013).

Η δημιουργία και κυκλοφορία αυτών των νέων ανταγωνιστικών κρυπτονομισμάτων, τα οποία στο σύνολο τους ονομάζονται AltCoins, οφείλεται στην επιτυχία του Bitcoin αλλά και στην ανοικτή φύση του λογισμικού του, η οποία επέτρεψε σε πολλούς προγραμματιστές να πειραματιστούν με τον κώδικα του και να τον τροποποιήσουν. Το αποτέλεσμα ήταν να δημιουργηθεί μια νέα γκάμα κρυπτονομισμάτων με κύριο στόχο την βελτιστοποίηση του ήδη υπάρχον κώδικα και την προσθήκη νέων δυνατοτήτων και λειτουργιών, όπως μεγαλύτερη ανωνυμία και ταχύτερες συναλλαγές (Finley Klint, 2018).

Από την ετυμολογία του ονόματος των AltCoins, alternative δηλαδή εναλλακτικό και coins δηλαδή νομίσματα, φαίνεται ο διαχωρισμός των AltCoins ως μια κατηγορία διαφορετική από αυτή του κρυπτονομίσματος Bitcoin. Αν και το Bitcoin έχει εξέχουσα θέση και ξεχωρίζει των υπολοίπων, αφού αποτελεί το πρώτο αποκεντρωμένο κρυπτονόμισμα στην ιστορία, πλέον είναι ένα από τα εκατοντάδες κρυπτονομίσματα που υπάρχουν στον κόσμο, με έρευνες να δηλώνουν ότι μέχρι το Μάιο του 2018 πάνω από 1500 κρυπτονομίσματα έχουν τεθεί σε κυκλοφορία, τα οποία αποτελούν απλά παραλλαγές ή βελτιώσεις του Bitcoin και βασίζονται σε έναν μεγάλο βαθμό σε ιδέες και καινοτομίες τις οποίες εισήγαγε αυτό (Frankenfield Jake, 2014).

Για παράδειγμα, τα περισσότερα από τα AltCoins χρησιμοποιούν peer-to-peer τεχνολογίες, διαθέτουν διαδικασίες εξόρυξης στις οποίες ο χρήστης χρειάζεται να λύσει δύσκολα προβλήματα για να ξεκλειδώσει blocks και προσφέρουν αποδοτικούς και φθηνούς τρόπους συναλλαγής στο διαδίκτυο. Ωστόσο, τα AltCoins μπορεί να μοιάζουν με το Bitcoin όμως διαφέρουν σε αρκετά σημεία από αυτό αφού διαθέτουν διαδικαστικές παραλλαγές, για

παράδειγμα διαφορετικούς Proof of Work αλγορίθμους, διαφορετικά μέσα με τα οποία οι χρήστες λαμβάνουν μέρος στην εξόρυξη και βελτιώσεις για αυξημένη ανωνυμία των χρηστών.

Τα σημαντικότερα κρυπτονομίσματα αυτή τη στιγμή στην κεφαλαιαγορά, πέρα από το Bitcoin το οποίο βρίσκεται στην κορυφή έχοντας την μεγαλύτερη τιμή της αγοράς, και με τα οποία θα ασχοληθούμε περιληπτικά στη συγκεκριμένη ενότητα είναι το Ethereum, το Litecoin, το Namecoin, το Ripple και το Bitcoin Cash των οποίων οι τιμές ακολουθούν ταυτόχρονα τιμή στατική προς καθοδική. Παρόλα αυτά, τα κρυπτονομίσματα όπως το Ethereum και το Ripple αρχίζουν και χρησιμοποιούνται περισσότερο από το κόσμο μιας και προσφέρουν ταυτόχρονα και επιχειρησιακές λύσεις εκτός από νομίσματα.

9.2. Namecoin

Το πρώτο κρυπτονόμισμα το οποίο δημιουργήθηκε τον Απρίλιο του 2011 μετά την εμφάνιση του Bitcoin ονομάζεται Namecoin, και βασίστηκε ως επί το πλείστον στην τεχνολογία την οποία εισήγαγε ο προκάτοχος του. Βασικό χαρακτηριστικό και των δυο κρυπτονομισμάτων είναι πως χρησιμοποιούν τον ίδιο αλγόριθμο Proof of Work και διαθέτουν τον ίδιο περιορισμένο και συγκεκριμένο αριθμό νομισμάτων που μπορούν να παραχθούν, δηλαδή τα 21 εκατομμύρια.



Εικ.27. Το επίσημο λογότυπο του Namecoin

Μάλιστα, στην αρχή ο κώδικας για την διαδικασία της εξόρυξης των δυο πρωτοκόλλων ήταν συγχωνευμένος, με την έννοια ότι επιτρεπόταν το mining και στο Bitcoin και στο Namecoin ταυτόχρονα ώστε να μη χρειάζεται οι χρήστες να μεταβαίνουν από το ένα κρυπτονόμισμα στο άλλο και αποφεύγοντας με αυτόν τον τρόπο τον κίνδυνο να ακολουθήσουν εν τέλει το πιο κερδοφόρο. Ωστόσο, η διαφορά των κρυπτονομισμάτων προκύπτει από τον τρόπο διαχείρισης της ανωνυμίας των χρηστών. Το Namecoin κάνει τους λογαριασμούς των χρηστών λιγότερο ορατούς στο διαδίκτυο αφού αφήνει τους χρήστες να καταχωρούν ένα δικό τους .bit domain μέσα από το οποίο μπορούν να συμμετέχουν και στη διαδικασία της εξόρυξης. Είναι φανερό επομένως, πως ως απώτερο σκοπό το Namecoin έχει να αυξήσει την ανωνυμία και να μειώσει τη λογοκρισία στο διαδίκτυο.

Οι δημιουργοί του Namecoin κρυπτονομίσματος το έχουν χαρακτηρίσει ως «μια πειραματική τεχνολογία ανοικτού κώδικα που βελτιώνει τις ιδιότητες του αποκεντρωμένου συστήματος, την ασφάλεια, τη λογοκρισία, την ιδιωτικότητα και την ταχύτητα ορισμένων στοιχείων υποδομής όπως DNS και ταυτότητες». Πράγματι, το Namecoin άνοιξε το δρόμο για διάφορα άλλα πρωτόκολλα κρυπτονομισμάτων και διάφορά νέα χαρακτηριστικά αυτών, όπως η συγχωνευμένη εξόρυξη και τα αποκεντρωμένα DNS. Το DNS, αποτελεί το σύστημα με το οποίο οι σύνδεσμοι ηλεκτρονικών ιστοσελίδων, τα λεγόμενα domains, συνδέονται με αριθμητικές διευθύνσεις IP σε όλον τον κόσμο. Με αυτόν τον τρόπο το κρυπτονόμισμα στοχεύει στην ενίσχυση της ασφάλειας και της ιδιωτικότητας.

Ωστόσο, μια από τις κυρίες ιδιότητες του Namecoin, κάτι για το οποίο οι δημιουργοί είναι ιδιαίτερα περήφανοι, είναι η προστασία των δικαιωμάτων της διαδικτυακής ελευθερίας του λόγου που καθιστά ολόκληρο το διαδίκτυο ανθεκτικό στη λογοκρισία. Επιπρόσθετα, είναι ένα κρυπτονόμισμα, το οποίο από τον Ιούνιο του 2013, μπορεί να χρησιμοποιηθεί για την επισύναψη πληροφοριών ταυτοποίησης, όπως για παράδειγμα διευθύνσεις ηλεκτρονικού ταχυδρομείου ή διευθύνσεις bitcoin σε διάφορες ταυτότητες που καθορίζονται από τον χρήστη, ιδιότητα η οποία τελικώς σημαίνει πως το κρυπτονόμισμα είναι σε θέση να αποθηκεύει πληροφορίες μέσα στη blockchain. Τελικώς, μπορεί να χρησιμοποιηθεί ως μέσο παροχής αποκεντρωμένου TLS (HTTPS) πιστοποιητικού.

Από τον Μάρτιο του 2018, το Namecoin έχει χαθεί από το επίκεντρο της κεφαλαιαγοράς. Η τιμή ενός Namecoin νομίσματος έφτασε το ανώτατο όριο των περίπου 12 δολαρίων και έκτοτε παραμένει κάτω από τα 3 δολάρια, με τη σημερινή του τιμή να κυμαίνεται στα 0.783 δολάρια. Επειδή το ανώτατο όριο της αντιστοιχίας του νομίσματος είναι κάτω από 40 εκατομμύρια δολάρια, δεν καταφέρνει να βρίσκεται πλέον στα 200 κορυφαία κρυπτονομίσματα. Ανεξάρτητα όμως από την οικονομική του επιτυχία, υπάρχουν μελλοντικά σχέδια για το κρυπτονόμισμα και οι βλέψεις του στρέφονται προς τις διαδικασίες ψηφοφορίας, την υπογραφή αρχείων και τις συμβολαιογραφικές υπηρεσίες ακόμα και σε υπηρεσίες απόδειξης της ύπαρξης ατόμων και οντοτήτων (namecoin.org).

9.3. Litecoin

Το 2011, την ίδια περίοδο εμφάνισης του κρυπτονομίσματος Namecoin δημιουργήθηκε και κυκλοφόρησε ακόμα ένα κρυπτονόμισμα με το όνομα Litecoin. Ο δημιουργός του, ονόματι Charlie Lee, ο οποίος είναι απόφοιτος του MIT, πρώην μηχανικός της Google (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017) και πλέον εργάζεται για τη Coinbase, μια από τις μεγαλύτερες ιστοσελίδες ψηφιακών πορτοφολιών, στηρίχτηκε στο πρωτόκολλο του Bitcoin για τη κατασκευή του νέου του κρυπτονομίσματος (coindesk.com, What is the difference between Litecoin and Bitcoin?, 2014).



Εικ.28. Το επίσημο λογότυπο του Litecoin

Το Litecoin εμφανίστηκε ως ένα εναλλακτικό κρυπτονόμισμα και αποσκοπούσε στη βελτίωση της υποτιθέμενης αναποτελεσματικότητας του Bitcoin (Wikoff Shawn, 2016). Μέχρι σήμερα αποτελεί τον κύριο ανταγωνιστή του πρώτου κρυπτονομίσματος, κυρίως σε άποψη πρωτοκόλλου γεγονός το οποίο έχει καταφέρει να κερδίσει μεγάλη δημοτικότητα για το κρυπτονόμισμα από την εποχή της κυκλοφορίας του μέχρι σήμερα. Ο ίδιος ο Charlie Lee έχει δηλώσει πως «η δημιουργία του Litecoin ξεκίνησε με στόχο να γίνει το ασήμι στο χρυσό του Bitcoin» (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017 & coindesk.com, What is the difference between Litecoin and Bitcoin?, 2014 & cryptobeginners.info, The top 10 cryptos explained).

Το Litecoin πρόκειται για ένα παγκόσμιο πλήρως αποκεντρωμένο δίκτυο πληρωμών ανοικτού κώδικα το οποίο δεν ελέγχεται από κάποιον τρίτο μεσολαβητή και καμία κεντρική αρχή. Δεδομένου ότι βασίζεται στο πρωτόκολλο του Bitcoin διαθέτει και αυτό διαδικασία εξόρυξης για την επιβεβαίωση των συναλλαγών του, ωστόσο στο συγκεκριμένο κρυπτονόμισμα ως Proof of Work δεν χρησιμοποιείται ο αλγόριθμος SHA-256 ο οποίος απαιτεί μεγάλη υπολογιστική ισχύ με τη χρήση CPUs ή ASICs για την επίλυση δύσκολων υπολογιστικών προβλημάτων και είναι η αίτια που υπάρχει τόσο μεγάλη αύξηση στη δυσκολία εξόρυξης των bitcoins (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017). Αντ' αυτού χρησιμοποιείται ο αλγόριθμος scrypt ο οποίος συμπεριλαμβάνει τον SHA-256 αλλά διαθέτει πιο συνεχή υπολογισμούς και δεν χρειάζεται τόσο μεγάλη υπολογιστή ισχύ για την εκτέλεση της διαδικασίας, απαιτούνται όμως μεγαλύτερες ποσότητες μνήμης RAM. Η χρήση

του αλγορίθμου scrypt ως Proof of Work κάνει το Litecoin πιο προσιτό στους χρήστες οι οποίοι θέλουν να λάβουν μέρος στο δίκτυο ως miners, ωστόσο αντίστοιχη τεχνολογία ASIC για το συγκεκριμένο κρυπτονόμισμα έχει ξεκινήσει να κατασκευάζεται από την εταιρεία Alpha Technology (coindesk.com, What is the difference between Litecoin and Bitcoin?, 2014).

Η χρήση του scrypt ως Proof of Work καθιστά πολύ πιο δύσκολη τη δημιουργία νομισμάτων καθώς απαιτεί μεγάλο χώρο μνήμης και με αυτόν τον τρόπο μειώνεται η ταχύτητα εξόρυξης δυσκολεύοντας ταυτόχρονα τον οποιονδήποτε χρήστη, ή ομάδα χρηστών, να κυριαρχήσει στην blockchain. Συνεχίζοντας, παρόλο που το Litecoin μοιάζει σε πολλά χαρακτηριστικά του με το Bitcoin, έχει σχεδιαστεί για να εστιάζει σε μικρότερες και συχνότερες συναλλαγές (cryptobeginners.info, The top 10 cryptos explained). Γι' αυτό το λόγο διαθέτει ταχύτερο ρυθμό παραγωγής των blocks σε σύγκριση με το κυρίαρχο κρυπτονόμισμα. Σύμφωνα με δεδομένα από την ιστοσελίδα Blockchain.info, η παραγωγή ενός block στο Bitcoin γίνεται σε 10 λεπτά, αν και ο χρόνος μπορεί να αλλάξει αν υπάρχουν πολλές συναλλαγές οι οποίες πρέπει να επικυρωθούν, ενώ στο Litecoin η παραγωγή γίνεται σε διάστημα 2.5 λεπτών.

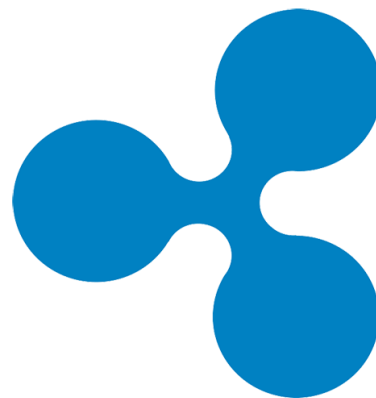
Με λίγα λόγια το κρυπτονόμισμα έχει σχεδιαστεί για να παράγει τέσσερις φορές περισσότερα block από το Bitcoin και ως εκ τούτου προσφέρει πιο γρήγορη επιβεβαίωση συναλλαγών και μειώνει το ρίσκο των διπλών δαπανών (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017 & coindesk.com, What is the difference between Litecoin and Bitcoin?, 2014). Αν για παράδειγμα ένας έμπορος πουλούσε το εμπόρευμα του για Bitcoins θα έπρεπε να περιμένει τετραπλάσιο χρόνο για να επιβεβαιωθεί η συναλλαγή του σε σύγκριση με την πώληση του ίδιου προϊόντος για Litecoins. Επίσης, εκτός από την καλύτερη ταχύτητα και την ευκολία απόκτησης του, το Litecoin προσφέρει και μικρότερες χρεώσεις στα τέλη των συναλλαγών (cryptobeginners.info, The top 10 cryptos explained).

Σήμερα το Litecoin διαθέτει περισσότερα από 60 εκατομμύρια κέρματα σε κυκλοφορία, ωστόσο αν και θεωρείται ένα από τα μεγαλύτερα κρυπτονομίσματα εξακολουθεί να έχει τιμή χαμηλότερη από το Bitcoin φτάνοντας περίπου στα 32.94 δολάρια. Όπως έχει γνωστοποιηθεί, για την εξάλειψη του πληθωρισμού έχει σχεδιαστεί μια ακολουθία καθυστέρησης της παραγωγής για τα περισσότερα ψηφιακά νομίσματα και αυτή η παραγωγή θα τερματιστεί σε ένα προαποφασισμένο απόθεμα. Το τελικό απόθεμα litecoins το οποίο θα παραχθεί είναι 4 φορές μεγαλύτερο από το τελικό απόθεμα του Bitcoin με συνολική παραγωγή 84.000.000 LCT (Μπαλάς Φώτης, 2016).

Τελικώς, ο χειρισμός μεγάλου όγκου συναλλαγών που πραγματοποιεί το Litecoin εξαιτίας της ταχύτερης παραγωγής των block του οδηγεί σε υψηλό όγκο blocks και γενικά σε μεγάλα ζητήματα κλιμάκωσης μόλις το δίκτυο φτάσει σε ένα ορισμένο μέγεθος (coindesk.com, What is the difference between Litecoin and Bitcoin?, 2014). Ωστόσο, η κοινότητα του κρυπτονομίσματος προσπαθεί να προετοιμαστεί για τέτοια ζητήματα εφαρμόζοντας έγκαιρα λύσεις κλιμάκωσης, όπως το Lightning Network, ένα αποκεντρωμένο δίκτυο που χρησιμοποιεί έξυπνες λειτουργικότητες στην blockchain για να επιτρέπει τις άμεσες πληρωμές μέσα σε ένα δίκτυο συμμετεχόντων (cryptobeginners.info, The top 10 cryptos explained & lightning.network).

9.4. Ripple

Το Ripple ή αλλιώς XRP είναι μια τεχνολογία η οποία διαθέτει δυο διαφορετικές ιδιότητες, από την μια είναι ένα πρωτόκολλο πληρωμών για χρηματοπιστωτικές συναλλαγές και από την άλλη είναι ένα ψηφιακό νόμισμα με την ονομασία XRP (Μπαλάς Φώτης, 2016). Πρόκειται για ένα νομισματικό σύστημα το οποίο δημιουργήθηκε και προορίζεται ώστε να χρησιμοποιηθεί από τις τράπεζες και τους παρόχους πληρωμών για ταχείες και άμεσες διασυννοριακές πληρωμές με υψηλή ασφάλεια και χαμηλά τέλη. Πιο συγκεκριμένα «δίνει τη δυνατότητα στις τράπεζες να διακανονίζουν τις διασυννοριακές πληρωμές σε πραγματικό χρόνο, με διαφάνεια και με χαμηλότερο κόστος» (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017).



Εικ.29. Το επίσημο λογότυπο του Ripple

Το Ripple κυκλοφόρησε το 2012 από τους Chris Larsen και Jed McCaleb και φαίνεται πως είναι πιο διαδομένο για το πρωτόκολλο ψηφιακής πληρωμής το οποίο διαθέτει και όχι τόσο ως κρυπτονόμισμα. Το πρωτόκολλο ξεχωρίζει από το Bitcoin άλλα και από πολλά άλλα AltCoins διότι δεν λειτουργεί με αλγορίθμους Proof of Work ή Proof of Stake και δεν υποστηρίζει την διαδικασία της εξόρυξης ως τρόπο επιβεβαίωσης των συναλλαγών (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017 & Μπαλάς Φώτης, 2016). Αντίθετα, βασίζεται σε δίκτυα εμπιστοσύνης, χρησιμοποιώντας έναν αλγόριθμο ομοφωνίας μεταξύ των μελών του δικτύου, προκειμένου να επικυρωθούν τα υπόλοιπα των λογαριασμών και οι

συναλλαγές του συστήματος (Wikoff Shawn, 2016). Με αυτόν τον τρόπο επιτυγχάνεται η βελτίωση της ακεραιότητας του συστήματος και εμποδίζονται οι δίπλες δαπάνες.

Επιπλέον, επειδή δεν πραγματοποιείται στο συγκεκριμένο πρωτόκολλο mining για τις επικυρώσεις των συναλλαγών, μειώνεται απευθείας η υπολογιστικής ισχύς η οποία χρησιμοποιείται, γεγονός το οποίο εκτός των άλλων ελαχιστοποιεί και την καθυστέρηση του δικτύου κάνοντας τις επιβεβαιώσεις στιγμιαίες, με χρόνο περίπου 5 δευτερόλεπτων, παρόλο που το δίκτυο διαχειρίζεται ταυτόχρονα εκατομμύρια συναλλαγές. Επίσης, με αυτόν τον τρόπο τα τέλη για τη διεξαγωγή των συναλλαγών παραμένουν πολύ μικρά σε σχέση με άλλα πρωτόκολλα με το ελάχιστο κόστος να αγγίζει τα 0.00001 XRP. Ωστόσο, υπάρχει μια σημαντική ομοιότητα του Ripple με το Bitcoin, και έγκειται στην ύπαρξη ενός συγκεκριμένου αριθμού αποθεματικού του νομίσματος το οποίο θα φτάσει περίπου τα 100.000.000.000 XRPs. Έχει δηλωθεί όμως πως όταν συμπληρωθεί αυτό το ποσό ένα ποσοστό θα διαμοιραστεί με τη μέθοδο ομοφωνίας σε όλους τους χρήστες (Μπαλάς Φώτης, 2016).

Το Ripple ως σύστημα πληρωμών λειτουργεί σε μια αποκεντρωμένη peer-to-peer πλατφόρμα ανοικτού κώδικα και επιτρέπει την ανεμπόδιστη μεταφορά χρημάτων σε οποιαδήποτε μορφή, είτε δολάρια, είτε ευρώ, είτε γιεν, είτε bitcoin χωρίς να κάνει διακρίσεις μεταξύ παραστατικών νομισμάτων και κρυπτονομισμάτων. Με αυτόν τον τρόπο, καθίσταται πιο εύκολη η ανταλλαγή οποιουδήποτε νομίσματος με άλλο νόμισμα. Ωστόσο, η ασφάλεια του δικτύου δεν είναι διαφορετική από αυτή που διέπει τα άλλα κρυπτονομίσματα. Όπως ακριβώς στο Bitcoin όλο το ιστορικό των συναλλαγών είναι δημόσιο, έτσι συμβαίνει και στο Ripple χωρίς τα δεδομένα να συνδέονται άμεσα με την ταυτότητά ή τον λογαριασμό κάποιου ατόμου ή επιχείρησης, όμως οι πληροφορίες παραμένουν ευαίσθητες σε μέτρα γνωστοποίησης και ταυτοποίησης χρηστών.

Αναφερόμενοι στις συναλλαγές ο τρόπος με τον οποίο αυτές επιτυγχάνονται στο συγκεκριμένο σύστημα είναι ο εξής, οι χρήστες δημιουργούν διασυνδέσεις με άλλους χρήστες τους οποίους εμπιστεύονται και στη συνέχεια μέσα από την δημιουργία αλυσίδων με τους έμπιστους χρήστες αποστέλλουν χρήματα για πληρωμές (Reiff Nathan, What is the biggest security threat to ripple cryptocurrency?, 2017). Οι αλυσίδες δημιουργούνται μέχρις ότου τα χρήματα να φτάσουν στον επιθυμητό παραλήπτη και για τη δημιουργία τους χρησιμοποιείται ένα μέσο γνωστό ως Gateway το οποίο χρησιμεύει ως σύνδεσμος εμπιστοσύνης αναμεσά στα δυο μέρη τα οποία επιθυμούν να πραγματοποιήσουν μια συναλλαγή. Τονίζεται, ότι κάθε

νόμισμα έχει το δικό του Gateway, για παράδειγμα το bitcoin έχει το BTCbitstamp και το αμερικανικό δολάριο έχει το USDsnapswap.

Στην περίπτωση που κάποιος χρήστης επιθυμεί να πληρωθεί σε ένα νόμισμα το οποίο ο αποστολέας δεν κατέχει τότε ο αποστολέας μπορεί πολύ απλά να μπει στο αντίστοιχο Gateway και να στείλει το χρηματικό ποσό της πληρωμής στο νόμισμα το οποίο διαθέτει και ο παραλήπτης θα λάβει το αντίστοιχο χρηματικό ποσό στο νόμισμα που εκείνος επιθυμεί. Δεν είναι απαραίτητη όμως, η χρήση μιας μόνο Gateway για να ολοκληρωθεί μια συναλλαγή αλλά μπορούν να χρησιμοποιηθούν πολλές Gateways δημιουργώντας έτσι μια μεγαλύτερη αλυσίδα εμπιστοσύνης ανάμεσα στους χρήστες. Ωστόσο, στην περίπτωση που ένας κακόβουλος χρήστης ξεκινήσει μια συναλλαγή σε πολλαπλά Gateways στέλνοντας όμως τα ίδια 100 νομίσματα θέλοντας να κοροϊδέψει το πρωτόκολλο, τότε το σύστημα των Gateways θα διαγράψει όλες τις συναλλαγές εκτός από την πρώτη για να αποφευχθεί η διπλή δαπάνη. Αυτό θα συμβεί σύμφωνα με το πρωτόκολλο συναίνεσης όπου ο κάθε χρήστης θα αποφασίσει ποια συναλλαγή έγινε πρώτη και μέσα από δημοσκόπηση θα επιλεγεί η επιλογή η οποία υποστηρίζεται από την πλειοψηφία των χρηστών.

Πλέον, υπάρχουν πολλοί υποστηρικτές της άποψης ότι το XRP δεν θα πρέπει να θεωρείται αποκεντρωμένο κρυπτονόμισμα αφού η ίδια η εταιρεία διαθέτει πάνω από το 50% όλων των XRP νομισμάτων όπως επίσης και την πλειοψηφία των κόμβων επικύρωσης στο δίκτυο (cryptobeginners.info, The top 10 cryptos explained). Ωστόσο, πρόκειται για μια επιτυχημένη τεχνολογία και παραμένει ένα από τα πιο δελεαστικά πρωτόκολλα μεταξύ των παραδοσιακών χρηματοπιστωτικών ιδρυμάτων που αναζητούν τρόπους επανάστασης στις διασυνοριακές πληρωμές. Μάλιστα, τον Ιούνιο του 2017, ήταν το τρίτο μεγαλύτερο κρυπτονόμισμα στην κεφαλαιαγορά με αξία 11.94 δισεκατομμυρίων δολαρίων, μετά από το Bitcoin με αξία 45,26 δισεκατομμύρια δολάρια και το Ethereum με 31,53 δισεκατομμύρια δολάρια. Τον Οκτώβριο του 2018 είχε ανώτατο όριο αγοράς 20.07 δισεκατομμύρια δολάρια και μια συμβολική αξία 0.518 δολάρια (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017). Ενώ σήμερα στις αρχές του 2019 η τιμή του έχει πέσει στα 0.311 δολάρια Αμερικής. Συμπερασματικά, το μόνο βέβαιο είναι πως το Ripple έχει πολύ δρόμο ακόμα ώστε να αποδείξει ότι είναι μια αξιόπιστη πλατφόρμα για διεθνές πληρωμές (cryptobeginners.info, The top 10 cryptos explained).

9.5. Ethereum

Το 2015 δημιουργήθηκε και κυκλοφόρησε ένα νέο κρυπτονόμισμα με το όνομα Ethereum το οποίο στις μέρες μας θεωρείται από πολλούς το μέλλον τόσο για τον κόσμο των κρυπτονομισμάτων αλλά και για τον κόσμο του διαδικτύου. Ο Vitalik Buterin, ο δημιουργός του Ethereum, κατάφερε να οραματιστεί και να εφεύρει ένα νέο κρυπτονόμισμα το οποίο παράλληλα λειτουργεί και ως μια νέα αποκεντρωμένη πλατφόρμα λογισμικού η οποία καθιστά δυνατή την κατασκευή smart contracts και τη δημιουργία και χρήση κατανεμημένων εφαρμογών (DApps) χωρίς διακοπές, απάτες, ελέγχους ή παρεμβολές από τρίτους. Παράλληλα, το ίδιο το Ethereum δηλώνει πως *«μπορεί να χρησιμοποιηθεί για την κωδικοποίηση, αποκέντρωση, ασφάλεια και εμπορία για σχεδόν οτιδήποτε»* (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017 & Frankenfield Jake, 2016).



Εικ.30. Το επίσημο λογότυπο του Ethereum

Όταν γίνεται αναφορά στον όρο smart contracts ή αλλιώς έξυπνες συμβάσεις εννοείται ένα νέο πρωτόκολλο το οποίο διευκολύνει ψηφιακά την επαλήθευση ή επιβολή μιας διαπραγματεύσεως καθώς και την εκτέλεση μιας συμβάσης. Με λίγα λόγια τα smart contracts επιτρέπουν την εκτέλεση αξιόπιστων συναλλαγών χωρίς τρίτους μεσολαβητές και καθιστούν τις συναλλαγές ανιχνεύσιμες, διαφανείς και μη αναστρέψιμες. Μέσω των smart contracts μπορεί κάποιος να στείλει χρήματα σε κάποιον άλλον αυτόματα αλλά μόνο όταν πληρούνται ορισμένες προϋποθέσεις, για παράδειγμα στη διαδικασία πώλησης ενός σπιτιού, ο αγοραστής και ο πωλητής θα μπορούσαν να συνάψουν ένα smart contract το οποίο θα μεταβιβάσει την κυριότητα στον αγοραστή και τα χρήματα στον πωλητή αυτόματα μόλις επιτευχθεί μια συμφωνία (cryptobeginners.info, The top 10 cryptos explained). Τα smart contracts είναι σημαντικά για τη διατήρηση της αποκεντρωμένης λειτουργικότητας του Ethereum καθώς λειτουργούν με δικό τους κώδικα χωρίς καμία πιθανότητα λογοκρισίας, απάτης, διακοπής ή παρέμβασης από τρίτους (Shobhit Seth, All about Ethereum, 2018).

Το άλλο σημαντικό πλεονέκτημα το οποίο διαθέτει το Ethereum είναι η ιδιότητα του να επιτρέπει τη χρήση της blockchain του από άλλους προγραμματιστές για την κατασκευή αποκεντρωμένων εφαρμογών γνωστές ως Dapps (cryptobeginners.info, The top 10 cryptos explained & Frankenfield Jake, 2016). Η γλώσσα προγραμματισμού η οποία σχεδιάστηκε από

την ομάδα του Ethereum και χρησιμοποιείται για τη δημιουργία των διάφορων αυτών εφαρμογών ονομάζεται Solidity. Ωστόσο, για να αναπτυχθεί κάποια εφαρμογή και για να μπορέσει το δίκτυο να την φιλοξενήσει πρέπει να πληρωθεί ένα αντίτιμο είτε με κάποιο ανταλλακτικό νόμισμα, είτε με το νόμισμα του Ethereum το οποίο ονομάζεται ether.

Το ether χρησιμοποιείται για δυο συνολικά σκοπούς, αρχικά διατίθεται ως κρυπτονόμισμα για ανταλλαγή με αλλά παραστατικά νομίσματα ή κρυπτονομίσματα και δεύτερον χρησιμοποιείται στο εσωτερικό του δικτύου για να εκτελέσει εφαρμογές και για την αποκόμιση κέρδους από εργασίες (Frankenfield Jake, 2016). Όπως έχει αναφερθεί, ένας προγραμματιστής εφαρμογών θα πρέπει αρκετές φορές να πληρώνει τέλη για τη φιλοξενία της εφαρμογής του στο δίκτυο σε ether, και αντίστοιχα ο ίδιος θα πληρώνεται από τους χρήστες της εφαρμογής του στο ίδιο κρυπτονόμισμα. Βέβαια, αυτός δεν είναι ο μοναδικός τρόπος απόκτησης των ether νομισμάτων. Όπως και στο Bitcoin έτσι και στο Ethereum οι συμμετέχοντες σε διαδικασίες εξόρυξης και επαλήθευσης συναλλαγών ανταμείβονται για τους πόρους του οποίους διαθέτουν στο δίκτυο, και τελικώς είναι αυτοί που διατηρούν ευέλικτο και λειτουργικό το δίκτυο του Ethereum (Shobhit Seth, All about Ethereum, 2018).

Το ether θα μπορούσε να παρομοιαστεί με ένα όχημα το οποίο επιτρέπει την μετακίνηση μέσα στο δίκτυο του Ethereum, αφού χρησιμοποιείται για να πληρώσει ο κάθε χρήστης την εκτέλεση μια εφαρμογής ή ενός προγράμματος ανάλογα με την ενέργεια και το χρόνο που απαιτείται για να εκτελεστεί αυτό. Η πληρωμή ενός ποσού για οποιαδήποτε ενέργεια πραγματοποιείται μέσα στο σύστημα δεν είναι καθόλου δελεαστική, ωστόσο η απόκτηση ενός ether είναι πολύ πιο γρήγορη σε σύγκριση με την απόκτηση ενός bitcoin, αν και έχει ξεπεραστεί κατά πολύ ο απλός υπολογιστής, διότι το πρώτο αποκτάται σε χρονικό διάστημα 14 ή 15 δευτερολέπτων ενώ το δεύτερο σε διάστημα 10 λεπτών, γεγονός το οποίο συνεπάγεται την κυκλοφορία περισσότερων ether νομισμάτων από ότι bitcoin (Frankenfield Jake, 2016). Συγκεκριμένα, 18 εκατομμύρια ethers δημιουργούνται ετησίως με 5 ethers να δημιουργούνται περίπου κάθε 12 δευτερόλεπτα. Φαίνεται επομένως, πως οι κανόνες του Ethereum για την οικονομία είναι πιο ανοικτοί και δεν διαθέτει όριο νομισμάτων που θα τεθούν σε κυκλοφορία (Hertig Alyssa and Palmer Daniel, 2017).

Μπορεί να μην έχουν ανακαλυφθεί ακόμα οι πλήρεις δυνατότητες του Ethereum, ωστόσο με βάση την συνολική αξία του αποθέματος του, είναι το δεύτερο πιο ισχυρό ψηφιακό νόμισμα μετά το Bitcoin (Frankenfield Jake, 2016). Το 2014, 60 εκατομμύρια από τα ether νομίσματα τα

οποία υπάρχουν σήμερα αγοράστηκαν από χρήστες σε έναν έρανο για την αύξηση της δημοτικότητας του κρυπτονομίσματος (Bajpai Prableen, The 10 most important cryptocurrencies other than Bitcoin, 2017). Αντίστοιχα, 12 εκατομμύρια ethers δοθήκαν στο Ethereum Foundation, μια ομάδα ερευνητών και προγραμματιστών οι οποίοι εργάζονταν πάνω στην υποκείμενη τεχνολογία (Hertig Alyssa and Palmer Daniel, 2017). Σήμερα, στις αρχές του 2019 η τιμή του Ethereum είναι στα 114.44 δολάρια, μεγαλύτερη δηλαδή από το Ripple και το Litecoin αλλά πολύ μικρή σε σχέση με το Bitcoin, γεγονός το οποίο καθιστά εμφανές πως το κρυπτονόμισμα έχει βραδύτερη από την αναμενόμενη ανάπτυξη μιας και ο κόσμος δεν δείχνει ιδιαίτερο ενδιαφέρον για τις Dapps (cryptobeginners.info, The top 10 cryptos explained). Οι τιμές ωστόσο των κρυπτονομισμάτων είναι πάντα σχετικές, για παράδειγμα έπειτα από ψεύτικη είδηση για το θάνατο του ιδρυτή του Ethereum το νόμισμα έχασε πάνω από 4 δισεκατομμύρια δολάρια από τη συνολική του αξία.

Ωστόσο, το Ethereum δεν δημιουργήθηκε για να γίνει ένα ακόμα ψηφιακό νόμισμα, αλλά για να προσφέρει στους χρήστες του την δυνατότητα να κατασκευάζουν αποκεντρωμένες εφαρμογές στο δίκτυο του. Συγκεκριμένα, πολλές νέες επιχειρήσεις θέλουν να υλοποιήσουν τα σχέδια τους μέσα στο δίκτυο του Ethereum και αξιοσημείωτη είναι η συνεργασία του κρυπτονομίσματος με τη Microsoft η οποία προσφέρει το Ethereum blockchain ως υπηρεσία (EBaaS) στο Microsoft Azure προκειμένου οι χρήστες και οι προγραμματιστές να έχουν με το πάτημα ενός κουμπιού ένα cloud-based blockchain προγραμματιστικό περιβάλλον (Frankenfield Jake, 2016). Το Ethereum πιστεύεται πως έχει τις δυνατότητες να χρησιμοποιηθεί σε αποκεντρωμένες οργανώσεις, στοιχήματα και διαδικτυακά τυχερά παιχνίδια καθώς και σε προβλέψεις αγορών, χρηματιστηριακές αγορές ή ακόμα και στη ασφαλιστική βιομηχανία. Όμως, όπως και το Bitcoin αντιμετωπίζει προβλήματα κλιμάκωσης λόγω του μεγέθους της χωρητικότητας των συναλλαγών και επίσης υπάρχουν και άλλες πλατφόρμες οι οποίες δημιουργούν παρόμοια τεχνολογία και είναι πιο απλές στην χρήση, γεγονός το οποίο ασκεί πίεση στο Ethereum (cryptobeginners.info, The top 10 cryptos explained).

Επιπρόσθετα, με τη χρήση του Ethereum δημιουργήθηκαν οι Αποκεντρωμένες Αυτόνομες Οργανώσεις γνωστές ως DAO, δηλαδή οργανώσεις οι οποίες χρησιμοποιώντας ένα συνδυασμό smart contracts, αλλάζουν τους κανόνες και τη δομή του Ethereum για να λειτουργήσει μια εταιρεία χωρίς ηγέτες (Shobhit Seth, All about Ethereum, 2018). Το 2016, ένα έργο DAO με τίτλο «The DAO» συγκέντρωσε επιτυχώς 150 εκατομμύρια δολάρια μέσα από την πώληση smart contracts και τον Ιουνίου του ιδίου έτους μπήκε στο στόχαστρο ενός χάκερ ο οποίος

κατάφερε να αποκλέψει το 1/3 των ethers τα οποία ισοδυναμούσαν εκείνο το διάστημα σε 50 εκατομμύρια δολάρια. Αν και ανακτήθηκαν ethers αντιστοιχίας 48 εκατομμυρίων δολαρίων το πλήγμα ήταν τεράστιο τόσο για το DAO όσο και για το Ethereum του οποίου η συναλλαγματική αξία καταρράγησε. Παρόλο που δεν υπήρχαν προβλήματα στο δίκτυο του Ethereum αλλά έφταιξε ένα τεχνικό ελάττωμα στον κώδικα του «The DAO» (Shobhit Seth, All about Ethereum, 2018), μετά από αυτήν την επίθεση το Ethereum χωρίστηκε σε δυο κρυπτονομίσματα, στο Ethereum, όπως είναι γνωστό σήμερα με αλλαγές στην ασφάλεια για παρόμοιες τέτοιες επιθέσεις κακόβουλων λογισμικών και το Ethereum Classic (Μπαλάς Φώτης, 2016 & Frankenfield Jake, 2016).

9.6. Bitcoin Cash

Τον Αύγουστο του 2017 ένα συγκλονιστικό γεγονός για τον κόσμο των κρυπτονομισμάτων έλαβε μέρος. Το Bitcoin διασπάστηκε σε δυο διαφορετικά κρυπτονομίσματα, στο Bitcoin όπως είναι ευρέως γνωστό στην σημερινή εποχή και στο Bitcoin Cash, ένα νέο αποκεντρωμένο σύστημα ηλεκτρονικών πληρωμών. Ο λόγος που οδήγησε στη



Εικ.31. Το επίσημο λογότυπο του Bitcoin Cash

διάσπαση του κρυπτονομίσματος ήταν καθαρά βασισμένος στις τεχνικές του υποδομές. Πολλοί χρήστες και miners είχαν εκφράσει από πολύ νωρίς την δυσαρέσκεια τους έναντι στους χαμηλούς χρόνους διεκπεραίωσης των συναλλαγών, διότι στην αρχή της κυκλοφορίας του το Bitcoin πραγματοποιούσε 3 συναλλαγές ανά δευτερόλεπτο με την χωρητικότητα των block του να είναι μόνο 1MB (Bajpai Prableen, What's Bitcoin Cash and where did it come from?, 2017). Αυτό το χαρακτηριστικό του Bitcoin οφειλόταν στο γεγονός ότι ο αρχικός του σχεδιασμός έδινε περισσότερο βάση στην ασφάλεια των συναλλαγών που γίνονταν στο δίκτυο και όχι τόσο στην σωστή λειτουργικότητα του δικτύου, γεγονός το οποίο στις αρχές εξαιτίας του μικρού αριθμού χρηστών στο δίκτυο δεν αποτελούσε ιδιαίτερο πρόβλημα.

Εντούτοις, στη σημερινή εποχή είναι αναγνωρισμένο το πόσο διάσημο και διαδεδομένο είναι το κρυπτόνμισμα Bitcoin κάτι που συνεπάγεται την χρήση του από πληθώρα ατόμων και ταυτόχρονα την ύπαρξη ακόμα περισσότερων συναλλαγών. Οι χρόνοι επομένως των συναλλαγών ήταν ανεπίτρεπτοι για ένα τόσο μεγάλο και σημαντικό πλέον κρυπτόνμισμα γι' αυτό και εμφανίστηκε η πρώτη πρόταση για επίλυση του προβλήματος η οποία ονομάστηκε SegWit αναβάθμιση και άλλαξε την χωρητικότητα ενός block αναδιαμορφώνοντας τον τρόπο

αποθήκευσης των δεδομένων των συναλλαγών χωρίς ωστόσο να αλλάζει το μέγεθος του (Acheson Noelle, 2018).

Η αναδιαμόρφωση του τρόπο αποθήκευσης των πληροφοριών αφορούσε κυρίως τις υπογραφές που περιλαμβάνονται στα blocks, οι οποίες με τη νέα πρόταση μετακινούνταν σε μια ξεχωριστή σελίδα η οποία γέμιζε παράλληλα με την κλασσική που περιέχει τις συναλλαγές, ώστε να υπάρχει περισσότερος χώρος διαθέσιμος για την καταγραφή μεγαλύτερου αριθμού συναλλαγών. Αντίστοιχα, η μη τροποποίηση του μεγέθους ενός block οφείλεται στην πλειοψηφία των προγραμματιστών οι οποίοι πίστευαν ότι με αυτόν τον τρόπο προσφέρεται περισσότερη ασφάλεια ενάντια σε πιθανές επιθέσεις hacking. Με την νέα αυτή πρόταση η οποία εν τέλει υιοθετήθηκε από το Bitcoin, αναβάθμισε το κρυπτονόμισμα ώστε να πραγματοποιεί 6-7 συναλλαγές ανά δευτερόλεπτο με την κάθε συναλλαγή να χρειάζεται 10 λεπτά μέχρι την ολοκλήρωσή της, χρόνος ο οποίος εξαρτάται και από το πλήθος των συναλλαγών που πρέπει να επιβεβαιωθούν.

Ωστόσο, μια μικρή κοινότητα χρηστών και προγραμματιστών, με ηγέτη τον Amaury Séchet, πρώην προγραμματιστή του Facebook, πίστευαν ότι η αναβάθμιση SegWit δεν ήταν τίποτα άλλο παρά μια προσωρινή λύση στο πρόβλημα της κλιμάκωσης (Acheson Noelle, 2018). Δεδομένης αυτής τους της άποψης αποφάσισαν να σχεδιάσουν μια νέα δικιά τους έκδοση του κρυπτονομίσματος που σύμφωνα με αυτούς είναι πιο κοντά στην ιδεολογία και το όραμα του Satoshi Nakamoto (Sharma Rakesh, 2017). Η νέα έκδοση ονομάστηκε Bitcoin Cash και όμοια με τον πρόγονό του είναι ένα αποκεντρωμένο, peer-to-peer ψηφιακό νόμισμα το οποίο μπορεί να χρησιμοποιηθεί για οικονομικές συναλλαγές στο διαδίκτυο. Συγκεκριμένα το ίδιο το Bitcoin Cash ορίζει τον εαυτό του ως *«ένα peer-to-peer ηλεκτρονικό χρήμα του διαδικτύου, το οποίο αποτελεί τη συνέχιση του Bitcoin εγχειρήματος. Είναι μια διακλάδωση της Bitcoin blockchain, με αναβαθμισμένους κανόνες ως προς τη συναίνεση, ιδιότητα που του επιτρέπει να μεγαλώνει και να κλιμακώνεται»* (Bajpai Prableen, What's Bitcoin Cash and where did it come from?, 2017).

Επομένως είναι εμφανές ότι το Bitcoin Cash αποσχίστηκε από την ήδη υπάρχουσα blockchain σε ένα προκαθορισμένο χρόνο και από εκεί και έπειτα ξεκίνησε να λειτουργεί η νέα έκδοση ως παρακλάδι του Bitcoin με αρκετές τροποποιήσεις. Η απόσχιση από τη blockchain του Bitcoin το καθιστά διαφορετικό από όλα τα υπόλοιπα AltCoins μιας και δεν αντιγράφει μόνο τον κώδικα του πρωτοκόλλου αλλά αντιγράφει και όλη τη blockchain μέχρι το σημείο απόσχισης. Με λίγα λόγια με τη δημιουργία του Bitcoin Cash όσοι είχαν στη διάθεση τους bitcoins είχαν

θεωρητικά και τον ίδιο αριθμό bitcoin cash. Η σχετική δήλωση των δημιουργών του Bitcoin Cash είναι η εξής, «όλοι οι κάτοχοι από το block 478.558 είναι τώρα ιδιοκτήτες bitcoin cash. Όλοι οι χρήστες του Bitcoin είναι ευπρόσδεκτοι να συμμετέχουν στην κοινότητα του Bitcoin Cash καθώς προχωράμε μπροστά στη δημιουργία χρημάτων προσβάσιμα σε ολόκληρο τον κόσμο» (Bajpai Prableen, What's Bitcoin Cash and where did it come from?, 2017).

Το Bitcoin Cash αν και βασίζεται και αντιγράφει ως ένα μεγάλο βαθμό τον κώδικα του Bitcoin, διαφέρει σημαντικά από αυτό διότι αρχικά δεν περιέχει την αναβάθμιση SegWit, μιας και οι προγραμματιστές του θεώρησαν πως ο διαχωρισμός των συναλλαγών με τις υπογραφές μείωνε την ασφάλεια ενάντια σε τυχόν επιθέσεις, και δεύτερον προσφέρει αύξηση του μεγέθους κάθε block στα 8MB, δηλαδή οκτώ φορές μεγαλύτερο από το μέγεθος του Bitcoin το οποίο περιορίζεται στο 1MB για κάθε block (Acheson Noelle, 2018). Συγκεκριμένα, το πρώτο block το οποίο δημιουργήθηκε στην Bitcoin Cash blockchain τον Αύγουστο του 2017, περιείχε 6.985 συναλλαγές με συνολικό μέγεθος του block 1.915MB, δηλαδή σχεδόν διπλάσιο από το όριο της Bitcoin blockchain. Ειδικότερα, το Bitcoin Cash μπορεί να διαχειριστεί 60 συναλλαγές το δευτερόλεπτο σε σύγκριση με τις 7 συναλλαγές τις οποίες μπορεί να διαχειριστεί πλέον το Bitcoin (cryptobeginners.info, The top 10 cryptos explained).

Επιπρόσθετα το Bitcoin Cash δημιούργησε νέους μεθόδους υπογραφής των συναλλαγών με σκοπό διάφορες βελτιώσεις ώστε να ταιριάζουν καλύτερα και με συγκεκριμένους τύπους εξαρτημάτων οι οποίοι χρησιμοποιούνται για την αποθήκευση των νομισμάτων. Επιπλέον, φαίνεται ότι διαθέτει διαφορές και ως προς την διαδικασία εξόρυξης μιας και έχει διαφορετικές διαδικασίες για την προσαρμογή της δυσκολίας εύρεσης των αριθμών nonce που παράγουν ένα hash. Στο Bitcoin, ο κώδικας επιθυμεί την διατήρηση μιας σχετικά ομαλής ροής των block και γι' αυτό ρυθμίζει τη δυσκολία της εξόρυξης σε κάθε 2016 block. Αντίθετα, το Bitcoin Cash θέλοντας να είναι κερδοφόρο έπρεπε με κάποιον τρόπο να διαφοροποιηθεί από το Bitcoin, γι' αυτό και στο συγκεκριμένο πρωτόκολλο η δυσκολία είναι πιο ευέλικτη και αλλάζει κάθε 600 δευτερόλεπτα ανάλογα με τη υπολογιστική ισχύ στο δίκτυο. Αν δεν καταφέρει να δημιουργηθεί ένα block μέσα σε αυτό το χρονικό διάστημα τότε η δυσκολία λιγοστεύει κάνοντας πιο εύκολη την εξόρυξη και επομένως πιο εύκολη την απόκτηση των αντίστοιχων νομισμάτων. Σε σύγκριση επομένως με το Bitcoin, η τιμή του Bitcoin Cash είναι σαφώς χαμηλότερη και σήμερα αγγίζει τα 123.70 δολάρια, όμως ένας miner μπορεί πιο συχνά να βρίσκει το σωστό nonce και να δημιουργεί ένα block και επομένως να καταφέρνει να συλλέξει περισσότερα bitcoin cash νομίσματα σε πιο λίγο χρονικό διάστημα (Acheson Noelle, 2018).

Το μέλλον του Bitcoin Cash όπως και οποιουδήποτε άλλου κρυπτονομίσματος φαντάζει αβέβαιο όμως η αποδοχή του έχει αυξηθεί από την στιγμή δημιουργίας του μέχρι σήμερα (Acheson Noelle, 2018). Συγκεκριμένα, η εταιρεία εξόρυξης ViaBTC στο Πεκίνο αν και παράγει το 4% της υπολογιστικής ισχύς του Bitcoin παράλληλα προωθεί και το Bitcoin Cash. Επίσης, το 2017 ο Emil Oldenburg, συνιδρυτής του bitcoin.com αποκάλυψε ότι επιθυμεί να πουλήσει όλα του τα bitcoins για bitcoin Cash, διότι όπως αναφέρει τα τέλη των συναλλαγών αλλά και οι ώρες που διαρκεί μια συναλλαγή σε bitcoin είναι αρκετά υψηλά. Σύμφωνα με τον ίδιο μια συναλλαγή που του κόστισε 50 δολάρια σε τέλη και κράτησε περίπου 12 ώρες, τον έκανε να αναθεωρήσει σχετικά με το Bitcoin και αποφάσισε ότι είναι ένα άχρηστο κρυπτόνμισμα σύμφωνα με τον τρόπο σχεδιασμού του (Sharma Rakesh, 2017). Συμπερασματικά, δεν είναι λίγοι οι χρήστες που ενδιαφέρονται για το μέγεθος των block στα κρυπτονομίσματα που χρησιμοποιούν και οι οποίοι τάσσονται υπέρ της αύξηση του μεγέθους. Μάλιστα το Bitcoin Cash επιθυμεί μελλοντικά να αυξήσει το μέγεθος των 8MB σε 32MB εισάγοντας νέους πιο έξυπνους τρόπους δημιουργίας πληροφοριών, διαχείρισης δικαιωμάτων και ελέγχου του χρόνου διεκπεραίωσης των συναλλαγών (Acheson Noelle, 2018). Σήμερα, και άλλα κρυπτονομίσματα έχουν εμφανιστεί με βάση το Bitcoin Cash, όπως το Bitcoin Classic και το Bitcoin Unlimited (Φυτίλης Γιάννης, 2017).

Κεφάλαιο 10: Τα υπέρ και τα κατά των κρυπτονομισμάτων

10.1. Πλεονεκτήματα των κρυπτονομισμάτων

Στις μέρες μας πολλοί άνθρωποι ελπίζουν στην ύπαρξη ενός νομίσματος το οποίο να καταφέρνει να διατηρεί την αξία του ανεξαρτήτως πολιτικών και οικονομικών συνθήκων, να διευκολύνει κατά κύριο λόγο τις συναλλαγές, να πραγματοποιείται εύκολα η μεταφορά του, αλλά ταυτόχρονα να μην εξαρτάται από κεντρικές τράπεζες ή άλλα χρηματοπιστωτικά ιδρύματα και να μην επηρεάζεται από την εκάστοτε κυβέρνηση (Frankenfield Jake, 2013). Ένα τέτοιο νόμισμα αυτή τη δεδομένη χρονική περίοδο δεν υφίσταται και ενδεχομένως να μην παρουσιαστεί για αρκετό καιρό ακόμα, όμως προς στιγμήν υπάρχουν κάποια νομίσματα τα οποία έχουν μερικά από τα ανωτέρω χαρακτηριστικά.

Τα κρυπτονομίσματα προσφέρουν πολλά πλεονεκτήματα στις σημερινές συναλλαγές έχοντας ταχύτερους χρόνους διεκπεραίωσης των συναλλαγών, χαμηλά ή και μηδαμινά τέλη και επιτρέποντας τις συναλλαγές σε ολόκληρο το κόσμο με ασφάλεια και διαφάνεια. Ωστόσο, κάθε πλεονέκτημα, θέλοντας και μη, έχει και το αντίστοιχο μειονέκτημά του είτε για λόγους ηθικής είτε για λόγους τεχνικής φύσεως, όπως για παράδειγμα η ανωνυμία η οποία προσφέρεται στο δίκτυο μπορεί να οδηγήσει και στην διευκόλυνση των παρανομιών, καθώς και το γεγονός ότι τα προσωπικά δεδομένα του εκάστοτε χρήστη δεν υπάρχουν αποθηκευμένα στο δίκτυο καθιστά αδύνατη την αντιστρεψιμότητα των συναλλαγών. Είναι ορθότερο όμως, να γνωστοποιήσουμε και τα αρνητικά και τα θετικά στοιχεία ενός νομίσματος ή μιας τεχνολογίας ώστε να διευκολυνθεί η δημιουργία απόψεων επί του θέματος.

Είναι άξιο αναφοράς πως τα κρυπτονομίσματα αν και βρίσκονται λίγα χρόνια στην αγορά και δεν επεκτείνονται με ιδιαίτερα ταχείς ρυθμούς, αποτελούν πιο ελκυστικά μέσα πληρωμής σε σύγκριση με τις υπόλοιπες παραδοσιακές μεθόδους. Αυτό συμβαίνει κυρίως λόγω της πληθώρας θετικών χαρακτηριστικών που διαθέτουν. Το κρυπτονόμισμα, εμπνευσμένο από τον χρυσό, δημιουργήθηκε για να μπορέσουν να ξεπεραστούν οι περιορισμοί οι οποίοι προέρχονταν από το μονοπώλιο των κεντρικών τραπεζών. Μερικά από τα βασικότερα πλεονεκτήματά του είναι τα εξής:

Ελευθέρια πληρωμών

Με τη χρήση των κρυπτονομισμάτων τα σύνορα μεταξύ των χωρών εξαφανίζονται αφού ο κάθε χρήστης μπορεί οποιαδήποτε στιγμή να στείλει, ή να λάβει, οποιοδήποτε χρηματικό

ποσό επιθυμεί σε οποιοδήποτε μέρος του κόσμου. Τα κρυπτονομίσματα δεν έχουν όρια, δεν έχουν αργίες και γιορτές, όπως οι τράπεζες, και δεν γνωρίζουν χιλιομετρικές αποστάσεις (bitcoin.org & coinreport.net, 2014).

Αποκεντρώση

Ένα κρυπτονόμισμα πρόκειται για ένα αποκεντρωμένο σύστημα το οποίο δεν βασίζεται σε καμία τράπεζα, σε κανένα χρηματοπιστωτικό ίδρυμα και σε καμία κυβέρνηση. Αντιθέτως, οι χρήστες είναι αυτοί οι οποίοι διαθέτουν τον πλήρη έλεγχο των χρημάτων τους χωρίς να χρειάζεται να εμπιστευτούν κάποιον τρίτο πάροχο υπηρεσιών (coinreport.net, 2014 & blogbucket.org, 2017). Ως κεντρική αρχή του συστήματος μετατρέπονται πλέον οι ίδιοι οι χρήστες οι οποίοι εκτελούν όλες τις απαραίτητες εργασίες για τη σωστή λειτουργία του, επαληθεύουν συναλλαγές και παρέχουν ασφάλεια στο δίκτυο όλο το εικοσιτετράωρο, μειώνοντας έτσι τις πιθανότητες να πέσουν θύματα ανεπιθύμητων ή απαρατήρητων χρεώσεων, όπως μπορεί να συμβεί με άλλες μεθόδους πληρωμής (bitcoin.org).

Παράλληλα, η απουσία κεντρικής εξουσίας συνεπάγεται την έλλειψη γραφειοκρατίας, νομοθεσίας και φορολόγησης. Κάνεις δεν είναι σε θέση να δεσμεύσει ή να κατασχέσει τα χρήματα των χρηστών ή ακόμα και να «παγώσει» τους λογαριασμούς τους (weacceptbitcoin.gr). Επίσης, δεν υπάρχει κανένας φορέας ο οποίος να μπορεί να περιορίσει το όριο των συναλλαγών ή να επιβάλλει συγκεκριμένους κανόνες και ειδικότερα από τη στιγμή που δεν ισχύουν φόροι στο δίκτυο δεν απαιτείται αντίστοιχο σύστημα φορολόγησης (Ευρωπαϊκή Κεντρική Τράπεζα, 2012). Επομένως, δίνεται στον κάθε χρήστη η ελευθέρια να χρησιμοποιεί τα χρήματά του με όποιον τρόπο εκείνος επιθυμεί (Pal Kaushik, 2016).

Χαμηλά τέλη

Μέχρι σήμερα οι συναλλαγές των κρυπτονομισμάτων γίνονται με μηδενικά ή με χαμηλά τέλη. Το Bitcoin συγκεκριμένα, σύμφωνα με την υλοποίηση του δεν διαθέτει κόστος συναλλαγής αφού το λογισμικό ενεργεί μονάχα για να διατηρεί συνδεδεμένους τον αποστολέα και τον παραλήπτη αναλαμβάνοντας όλο το φορτίο της εξουσιοδότησης κάθε συναλλαγής στο δίκτυο (Pal Kaushik, 2016). Ωστόσο, οι χρήστες αν το επιθυμούν μπορούν να δώσουν οικειοθελώς ένα μικρό επιπλέον ποσό προκειμένου να αποκτήσουν προτεραιότητα στην διαδικασία επικύρωσης των συναλλαγών τους (Frankenfield Jake, 2013).

Τα χαμηλά τέλη συναλλαγών δίνουν στους χρήστες τη δυνατότητα να αποφεύγουν τις χρεώσεις των τραπεζών και των χρηματοπιστωτικών ιδρυμάτων για τις τραπεζικές μεταφορές κεφαλαίων και για τις διεξαγωγές πληρωμών (blogbucket.org, 2017). Ακόμα και αν κάποιος χρήστης επιλέξει να διαθέσει ένα ποσό για να πάρει προβάδισμα στην αλυσίδα διεκπεραίωσης συναλλαγών, το τελικό ποσό παραμένει πολύ χαμηλό σε σύγκριση με άλλες νομισματικές συναλλαγές που γίνονται σε απευθείας σύνδεση όπως οι συναλλαγές οι οποίες πραγματοποιούνται από την PayPal, την Pioneer ή κάποιο άλλο δίκτυο πιστωτικών καρτών (bitcoin.org & Frankenfield Jake, 2013 & coinreport.net, 2014). Εξαίρεση αποτελεί το Bitcoin το οποίο λόγω προβλημάτων κλιμάκωσης έχει οδηγηθεί σε αυξανόμενα τέλη συναλλαγών, φτάνοντας μέχρι και 50 δολάρια (cryptobeginners.info, The top 10 cryptos explained & Medema Todd, 2018).

Μειωμένοι κίνδυνοι για τους εμπόρους

Οι συναλλαγές οι οποίες πραγματοποιούνται με την χρήση κρυπτονομισμάτων είναι ιδιαίτερα ασφαλείς μέσω της κρυπτογραφίας και της ανωνυμίας που τις διέπουν και δεν μπορούν να ακυρωθούν, να διαγραφτούν ή να τροποποιηθούν. Μόλις μιας συναλλαγή ολοκληρωθεί και τα χρήματα σταλούν σε μια διεύθυνση του δικτύου δεν γίνεται με κανένα τρόπο τα νομίσματα να επιστραφούν στον αποστολέα. Πλέον, ο μονός ο οποίος μπορεί να έχει πρόσβαση στα χρήματα αυτά είναι ο παραλήπτης (Pal Kaushik, 2016).

Με τον τρόπο αυτό δεν μπορεί να γίνει ακύρωση χρέωσης, όπως γίνεται για παράδειγμα με τις πιστωτικές κάρτες, και ως αποτέλεσμα οι πιθανότητες απάτης ή πολλαπλών χρεώσεων λιγοστεύουν (blogbucket.org, 2017). Ταυτόχρονα, πληθαίνουν οι πιθανότητες κάποιος έμπορος να επεκταθεί σε νέες αγορές στις οποίες μέχρι τώρα δεν μπορούσε είτε διότι δεν διαθέτουν δυνατότητα εκτέλεσης συναλλαγών μέσω πιστωτικών καρτών, είτε επειδή είναι ιδιαίτερα επικίνδυνες μιας και τα ποσοστά απάτης είναι πολύ υψηλά (bitcoin.org & coinreport.net, 2014).

Ανωνυμία και ασφάλεια

Ένα βασικό θετικό χαρακτηριστικό το οποίο διαθέτουν τα κρυπτονομίσματα είναι τα αυξημένα επίπεδα ασφαλείας που προσφέρουν στους χρήστες τους τα οποία επιτυγχάνονται μέσω της ανωνυμίας των συναλλαγών και της κρυπτογράφησης. Όπως έχει αναφερθεί, το λογισμικό ενός κρυπτονομίσματος δεν απαιτεί κατά την εγγραφή του χρήστη κάποιο προσωπικό του στοιχείο, όπως ταυτότητα ή εκκαθαριστικό εφορίας.

Αντιθέτως, το ίδιο το σύστημα για λόγους ασφαλείας δημιουργεί για κάθε χρήστη ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού, τα οποία του προσφέρουν την ανωνυμία που χρειάζεται εντός και εκτός του συστήματος και με τα οποία μπορεί να λάβει μέρος στις συναλλαγές (Frankenfield Jake, 2013). Με αυτόν τον τρόπο, οι συναλλαγές διεξάγονται χωρίς προσωπικές πληροφορίες γεγονός που προσφέρει ισχυρή προστασία της ιδιωτικής ζωής και προφύλαξη απέναντι σε κακόβουλες κλοπές δεδομένων (bitcoin.org).

Επίσης, το ίδιο το λογισμικό προτρέπει τους χρήστες του να χρησιμοποιούν ψηφιακά πορτοφόλια για την αποθήκευση των νομισμάτων τους προκειμένου να αποφευχθούν απάτες και κλοπές. Ωστόσο, οι χρήστες πρέπει να προστατεύουν τα ψηφιακά πορτοφόλια τους με αντίγραφα ασφαλείας, κωδικούς πρόσβασης και επιπλέον κρυπτογράφηση. Στην περίπτωση που ένας χρήστης έχει προστατευτεί επαρκώς, ο μόνος τρόπος για να μπορέσει κάποιος να αποκτήσει πρόσβαση στον λογαριασμό του και στα χρήματά του είναι να έχει φυσική πρόσβαση στον υπολογιστή του (Pal Kaushik, 2016).

Διαφάνεια

Όλες οι πληροφορίες των συναλλαγών των κρυπτονομισμάτων είναι άμεσα διαθέσιμες στο blockchain και οποιοσδήποτε μπορεί να ανατρέξει σε αυτές και να τις επιβεβαιώσει οποιαδήποτε στιγμή. Το ιστορικό των συναλλαγών από την πρώτη συναλλαγή μέχρι την τελευταία δεν μπορεί να διαγραφεί, ωστόσο κανείς δεν μπορεί να παρακολουθήσει μια συναλλαγή, διότι εξαιτίας της ανωνυμίας δεν είναι εφικτό να γνωρίζει τα στοιχεία των συναλλασσόμενων. Συγκεκριμένα μπορούν να πραγματοποιηθούν συναλλαγές που ο αποστολές και ο παραλήπτης δεν γνωρίζουν ο ένας τον άλλον (bitcoin.org).

Επιπρόσθετα, παρότι ο κώδικας είναι ανοικτός για ελέγχους διεκπεραίωσης συναλλαγών από προγραμματιστές κανείς δεν μπορεί να πλαστογραφήσει ή να τροποποιήσει το πρωτόκολλο του εκάστοτε νομίσματος διότι είναι κρυπτογραφικά ασφαλές (coinreport.net, 2014). Αυτό επιτρέπει στα κρυπτονομίσματα να παραμένουν αξιόπιστα αφού είναι απολύτως ουδέτερα και διαφανή. Ο μόνος τρόπος για να υπάρξει παρακολούθηση χρηστών και ανίχνευση συναλλαγών στο σύστημα είναι αν οι ίδιοι οι χρήστες έχουν δημοσιοποιήσει τη διεύθυνση του πορτοφολιού τους. Ωστόσο, είναι πολύ εύκολο να δημιουργηθεί μια νέα διεύθυνση πορτοφολιού προκειμένου να αποκρυφτούν τα ίχνη συναλλαγών και να αυξηθεί η ιδιωτικότητα (Pal Kaushik, 2016).

Ταχύτητα

Τα κρυπτονομίσματα διαθέτουν πολύ γρήγορες συναλλαγές μεταξύ των χρηστών τους μιας και πραγματοποιούν πληρωμές χωρίς να χρειάζεται κάποιο επιπλέον μέσο, όπως για παράδειγμα η χρήση μιας πιστωτικής κάρτας ή κάποιο έγγραφο για υπογραφή. Το μόνο που πρέπει να γνωρίζει ένας χρήστης για να πραγματοποιήσει μια πληρωμή είναι η διεύθυνση πορτοφολιού του ατόμου ή του οργανισμού στο οποίο θέλει να μεταφέρει τα χρήματα. Στη συνέχεια, η επεξεργασία των πληρωμών είναι πολύ γρήγορη και από τη στιγμή επιβεβαίωσης της συναλλαγής οι παραλήπτες λαμβάνουν τα χρήματα σε διάστημα μερικών λεπτών (blogbucket.org, 2017).

Ευκολία χρήσης και μεταφοράς

Τα κρυπτονομίσματα, όπως επισημάνθηκε και νωρίτερα, πρέπει να αποθηκεύονται σε ψηφιακά πορτοφόλια προκειμένου να επιτευχθούν υψηλά επίπεδα ασφάλειας. Ωστόσο, στα πορτοφόλια δεν αποθηκεύονται αυτούσια χρήματα αλλά το περιεχόμενο των ψηφιακών πορτοφολιών αντιστοιχεί στη δημόσια διεύθυνση και στο ιδιωτικό κλειδί που δημιουργεί ο κάθε χρήστης. Αυτά τα δυο στοιχεία είναι τα μόνο που χρειάζεται ο χρήστης ώστε να πραγματοποιήσει μια συναλλαγή στο δίκτυο. Είναι φανερό, πως αφού τα νομίσματα δεν είναι απτά μπορούν να μεταφέρονται πολύ πιο ευκολά από ότι τα παραστατικά χρήματα, για παράδειγμα μέσα σε ένα κινητό τηλέφωνο ή ένα ψηφιακό μέσο, μειώνοντας έτσι κίνδυνους κλοπής. Επιπλέον με αυτόν τον τρόπο καθίσταται πιο εύκολη η χρήση τους στις συναλλαγές, διότι τα χρήματα είναι άμεσα διαθέσιμα με το πάτημα ενός κουμπιού (techopedia.com).

Συγκεκριμένος αριθμός παραγωγής νομισμάτων

Ένα ακόμα πλεονέκτημα υπέρ των περισσότερων κρυπτονομισμάτων είναι η τροφοδοσία των νομισμάτων η οποία ελέγχεται αυστηρά από έναν αλγόριθμο. Ένας μικρός αριθμός νέων κρυπτονομισμάτων διαρρέει κάθε ώρα και θα συνεχίσει να το κάνει με μειωμένο ρυθμό έως ότου φθάσουν ένα συγκεκριμένο ποσό, για παράδειγμα στο Bitcoin τα 21 εκατομμύρια bitcoins. Με αυτόν τον τρόπο ελέγχεται ο πληθωρισμός και το κρυπτονόμισμα γίνεται πιο ελκυστικό, διότι θεωρητικά αν η ζήτηση μεγαλώσει και η προσφορά παραμένει η ίδια, τότε η αξία του κρυπτονομίσματος θα αυξηθεί. Αντίθετα, τα παραδοσιακά νομίσματα, όπως τα δολάρια, έχουν απεριόριστη προσφορά και οι τράπεζες μπορούν να εκδώσουν όσα χρήματα θέλουν προσπαθώντας να χειραγωγήσουν την αξία ενός νομίσματος σε σχέση με άλλα (Acheson Noelle, What is Bitcoin?, 2013).

10.2. Μειονεκτήματα των κρυπτονομισμάτων

Κάθε τεχνολογία αναπόφευκτα χρειάζεται να αντιμετωπίσει διάφορες προκλήσεις, δυσκολίες και μειονεκτήματα τόσο στην αρχή της δημιουργίας της όσο και κατά τη διάρκεια χρήσης της. Ωστόσο, κάθε εμπόδιο το οποίο εμφανίζεται βοηθάει αν μην τι άλλο στην εξέλιξη ενός έργου και στη βελτιστοποίηση του ώστε να καταφέρει να οδηγηθεί όσο το δυνατόν στο πιο τέλειο αποτέλεσμα. Παραπάνω, αναπτύσσοντας τα πλεονεκτήματα των κρυπτονομισμάτων έγινε φανερό ότι μπορούν να προσφέρουν αρκετά διαφορετικά προνόμια σε σύγκριση με τα παραστατικά χρήματα. Όμως το τέλειο δεν υπάρχει σε καμία τεχνολογία, σε κανένα πρωτόκολλο και σε κανένα κρυπτονόμισμα. Αντιθέτως, όσο υπάρχουν πλεονεκτήματα άλλα τόσα μειονεκτήματα θα βγαίνουν στο φως, είτε λόγο τεχνικών υποδομών είτε λόγω ηθικών φραγμών.

Με την αναφορά ωστόσο στα αρνητικά χαρακτηριστικά των κρυπτονομισμάτων θα γίνει αντιληπτό ότι πολλά από αυτά πηγάζουν από την πρώιμη μορφή των κρυπτονομισμάτων, διότι επρόκειτο για μια καινούργια τεχνολογία, ξεχωριστή, η οποία δεν μοιάζει με καμία άλλη ως τώρα, και η οποία υπάρχει, χρησιμοποιείται και ανθίζει τα τελευταία δέκα χρόνια, διάστημα αρκετά μικρό για να προσδώσει σιγουριά και σταθερότητα. Ωστόσο, είναι σημαντικό να δημιουργηθεί μια ολοκληρωμένη άποψη γύρω από το επίμαχο θέμα των κρυπτονομισμάτων, η οποία εν τέλει θα παραχθεί μέσα από την παρουσίαση και των εξής μειονεκτημάτων:

Αποκέντρωση

Τα κρυπτονομίσματα είναι αποκεντρωμένα συστήματα τα οποία δεν διαθέτουν κάποιον τρίτο μεσολαβητή, όπως για παράδειγμα κάποια τράπεζα ή κάποιο άλλο χρηματοπιστωτικό ίδρυμα για την διεκπεραίωση των συναλλαγών τους, καθώς συγχρόνως δεν διαθέτουν και κάποιο κεντρικό αποθετήριο για τα νομίσματα που παράγονται στο σύστημα. Αυτή η ιδιότητα των κρυπτονομισμάτων καταφέρει να είναι ταυτόχρονα και πλεονέκτημα και μειονέκτημα των ψηφιακών νομισμάτων. Πολλοί είναι αυτοί που στρέφονται στα κρυπτονομίσματα εξαιτίας της αποκέντρωσης που προσφέρουν ενώ ταυτόχρονα διακινδυνεύουν τα χρήματά τους (Frankenfield Jake, 2013).

Πιο αναλυτικά, όμοια με τα παραστατικά χρήματα, αν το ψηφιακό πορτοφόλι ενός χρήστη διαγραφεί, κλαπεί ή καταστραφεί, είτε από φυσική φθορά είτε από ιούς και κακόβουλα προγράμματα, και δεν υπάρχει κάποιο αντίγραφο ασφαλείας τότε ο ιδιοκτήτης

του πορτοφολιού έχει χάσει μέσα σε πολύ λίγα δευτερόλεπτα όλα του τα χρήματα και δεν υπάρχει κανένας τρόπος να τα ανακτήσει. Επιπρόσθετα, ο χρήστης δεν έχει ούτε νομική προστασία μήτε τη δυνατότητα να ζητήσει βοήθεια από κάποιον άλλο φορέα, όπως η αστυνομία, αλλά ούτε και από οποιονδήποτε άλλο χρήστη στο δίκτυο διότι κανείς δεν μπορεί να κάνει τίποτα για να τον βοηθήσει. Γι' αυτό το λόγο οι εταιρίες των κρυπτονομισμάτων συνιστούν στους χρήστες να διαφυλάσσουν τα κλειδιά τους εκτός σύνδεσης και να δημιουργούν πολλά αντίγραφα ασφαλείας αυτών (Frankenfield Jake, 2013 & blogbucket.org, 2017).

Ανωνυμία

Το κυριότερο ίσως χαρακτηριστικό των κρυπτονομισμάτων είναι η ανωνυμία που προσφέρει στους χρήστες. Παρόλα αυτά, η ανώνυμη φύση των συναλλαγών καθιστά πολλές φορές εύκολη τη φοροδιαφυγή, το ξέπλυμα χρημάτων καθώς και συναλλαγές οι οποίες συνδέονται με εγκληματικές δραστηριότητες (Frankenfield Jake, 2013).

Ασφάλεια και συνεχής εξέλιξη

Τα κρυπτονομίσματα δεν έχουν ανοσία σε απειλές και επιθέσεις από κακόβουλους χρήστες. Στης ιστορία τους πολλά κρυπτονομίσματα έχουν υποστεί πολλές επιθέσεις, ακόμα και κλοπές των νομισμάτων τους, όπως το Bitcoin το οποίο αριθμεί πάνω από 40 τέτοιες επιθέσεις οι οποίες αντιστοιχούν σε νομίσματα η αξία των οποίων ξεπερνάει τα 1 εκατομμύριο δολάρια. Μιας και η τεχνολογία των κρυπτονομισμάτων βρίσκεται σε πολύ αρχικό στάδιο ωρίμανσης και διαθέτει πολλά ημιτελή χαρακτηριστικά, παρουσιάζονται κατά καιρούς αρκετά τεχνικά λάθη τα οποία πρέπει να αντιμετωπιστούν ώστε να γίνουν πιο ασφαλή, προσβάσιμα και εν τέλει να μην καταστούν άχρηστα ως μέσα πληρωμών (Frankenfield Jake, 2013).

Μη αναστρεψιμότητα συναλλαγών

Σε αντίθεση με τις παραδοσιακές ηλεκτρονικές συναλλαγές, οι συναλλαγές κρυπτονομισμάτων, παρόμοια με αυτές των μετρητών, δεν μπορούν να αντιστραφούν. Αυτό συμβαίνει διότι δεν υπάρχει μια κεντρική αρχή η οποία να μπορεί να επιβεβαιώσει μια επιστροφή χρημάτων είτε σε περίπτωση λάθους, είτε σε περίπτωση νόμιμου σφάλματος ή μη εξουσιοδοτημένης χρήσης. Στην περίπτωση των ηλεκτρονικών συναλλαγών, οι πληρωμές μπορούν να αντιστραφούν, για παράδειγμα σε περιπτώσεις απάτης ή διαφωνιών, έπειτα από

έναν συγκεκριμένο χρόνο που ονομάζεται «χρόνος εκκαθάρισης» και μπορεί να διαρκέσει 72 ώρες ή περισσότερο (Wikoff Shawn, 2016).

Ταχύτητα

Σύμφωνα με τα πλεονεκτήματα που παρουσιάστηκαν παραπάνω, τα κρυπτονομίσματα έχουν αυξημένες ταχύτητες για την πραγματοποίηση των συναλλαγών. Ωστόσο, η ταχύτητα των κρυπτονομισμάτων φαντάζει πιο γρήγορη σε σύγκριση με την ταχύτητα των παραδοσιακών τρόπων πληρωμής όπως τα μετρητά. Αντιθέτως, αν συγκριθεί η ταχύτητα των κρυπτονομισμάτων με την ταχύτητα των πιστωτικών ή χρεωστικών καρτών, τότε θα γίνει φανερό πως τα κρυπτονομίσματα έχουν πολύ δρόμο ακόμα μέχρι να γίνουν ένα παγκόσμιο σύστημα πληρωμών. Πιο συγκεκριμένα, η VISA και η Mastercard μπορούν να διαχειριστούν χιλιάδες συναλλαγές ανά δευτερόλεπτο, ωστόσο τα πιο εξελιγμένα κρυπτονομίσματα σήμερα, όπως για παράδειγμα το Bitcoin, ακόμα και μετά από διορθώσεις και βελτιώσεις του λογισμικού τους, μπορούν να διαχειρίζονται μόνο 5 έως 7 συναλλαγές ανά δευτερόλεπτο (cryptobeginners.info, The top 10 cryptos explained).

Βαθμός αποδοχής

Τα κρυπτονομίσματα δεν είναι ευρέως αποδεκτά. Ακόμα και σήμερα υπάρχουν πολλοί άνθρωποι οι οποίοι δεν γνωρίζουν την έννοια των κρυπτονομισμάτων και της blockchain. Επομένως, ενώ μπορεί καθημερινά η λίστα των επιχειρήσεων που δέχονται κρυπτονομίσματα να μεγαλώνει, ωστόσο παραμένει αρκετά μικρή σε σύγκριση με αυτό που θα μπορούσε να είναι. Αυτός είναι και ο λόγος που δεν έχουν εμφανιστεί ακόμα αξιόλογα αποτελέσματα σε κάποιο δίκτυο κρυπτονομίσματος (blogbucket.org, 2017). Συμπερασματικά, ο μόνος τρόπος για να διορθωθεί το συγκεκριμένο πρόβλημα είναι η πληροφόρηση και η εκπαίδευση του κόσμου σχετικά με τη χρήση των κρυπτονομισμάτων και με την υιοθέτηση αυτών στην καθημερινή τους ζωή.

Αστάθεια τιμών

Τα κρυπτονομίσματα θεωρούνται από πολλούς ως μια φούσκα η οποία δεν έχει μεγάλη διάρκεια ζωής και στο τέλος θα σκάσει οδηγώντας όλους όσους έχουν επενδύσει σε αυτά στη χρεοκοπία. Πράγματι, με την πάροδο των χρόνων έχουν εντοπιστεί μερικές ραγδαίες αυξήσεις και μερικές απότομες και ξαφνικές μειώσεις στην τιμή των κρυπτονομισμάτων. Επομένως, είναι λογικό να θεωρούνται από πολλούς αναξιόπιστα ανά περιόδους. Ωστόσο, αποτελεί αναμενόμενο γεγονός δεδομένου ότι οι τιμές βασίζονται στη προσφορά και στη

ζήτηση καθώς και σε μικρά γεγονότα, όπως συναλλαγές και επιχειρηματικές δραστηριότητες, και σε μεγάλα γεγονότα, όπως οικονομικές και πολιτικές εξελίξεις, που μπορούν να επηρεάσουν σημαντικά τις τιμές.

Επιπρόσθετα, η μεταβλητότητα των τιμών πολλών κρυπτονομισμάτων προέρχεται πολλές φορές και από τον περιορισμένο αριθμό νομισμάτων που θα παραχθούν συνολικά καθώς και από τον έντονο ανταγωνισμό μεταξύ αυτών. Με αυτόν τον τρόπο ενισχύονται οι φόβοι για τη σταθερότητα των τιμών, ωστόσο προβλέπεται πως τα επόμενα χρόνια καθώς οι αγορές και οι τεχνολογίες θα ωριμάζουν και όλο και περισσότεροι άνθρωποι θα ξεκινήσουν να τα αποδέχονται και να τα χρησιμοποιούν, η τιμή θα μπορέσει να σταθεροποιηθεί (bitcoin.org & coinreport.net, 2014).

Κεφάλαιο 11: Κανόνες κρυπτονομισμάτων

11.1. Οικονομικοί και νομικοί κανόνες

Τα κρυπτονομίσματα αποτελούν μια νέα τεχνολογία η οποία από την στιγμή της ίδρυσής της έχει εισχωρήσει σε σημαντικό βαθμό στις ηλεκτρονικές συναλλαγές και όπως είναι αναμενόμενο, έχει επηρεάσει το παγκόσμιο ηλεκτρονικό εμπόριο και κατά συνέπεια ολόκληρη την οικονομία. Τα χαρακτηριστικά που διέπουν τα κρυπτονομίσματα, όπως η ανωνυμία και η μη αναστρεψιμότητα των συναλλαγών, λειτουργούν ενάντια στους περιορισμούς που έχουν θέσει διάφορα κράτη στις χρηματοπιστωτικές τους συναλλαγές. Συγχρόνως, ο αποκεντρωτικός χαρακτήρας των νομισμάτων ο οποίος συνεπάγεται την απουσία μιας κεντρικής αρχής καθώς και ο περιορισμένος αριθμός νομισμάτων ενός κρυπτονομίσματος τοποθετούνται ενάντια στην ίδια της έννοια της νομισματικής πολιτικής.

Παρόλα αυτά η χρήση των κρυπτονομισμάτων δεν συνάγεται σε οικονομικό περιορισμό αφού οι συναλλαγές μπορούν να πραγματοποιηθούν και με υπομονάδες ενός νομίσματος. Παραδείγματος χάριν, το Bitcoin εν τελεί θα παράξει 21 εκατομμύρια bitcoins, ωστόσο υπάρχουν τα bits όπου 1.000.000 bits αντιστοιχούν σε 1 bitcoin. Φαίνεται ότι μέχρι στιγμής ένα bitcoin μπορεί να διαιρεθεί μέχρι 8 δεκαδικά ψηφία και θα μπορούσε να διαιρεθεί και σε μικρότερες μονάδες αν αυτό ήταν επιθυμητό στο μέλλον. Η συγκεκριμένη πρακτική βοηθάει τα κρυπτονομίσματα να εξαλείφουν το πρόβλημα του πληθωρισμού. Όμως, υπάρχει πάντοτε ο κίνδυνος για τεχνικές αποτυχίες, έντονο ανταγωνισμό ή πολιτικά ζητήματα και φυσικά κανέναν νόμισμα δεν είναι απολύτως ασφαλές σε χρεοκοπίες και δύσκολους καιρούς.

Πρέπει να σημειωθεί πως ενώ τα κρυπτονομίσματα είναι ευρέως διαδεδομένα και ως ένα βαθμό αποδεκτά από τους πολίτες, ωστόσο οι τράπεζες, τα διάφορα χρηματοπιστωτικά ιδρύματα καθώς και πολλές κυβερνήσεις δεν τα αντιμετωπίζουν με τον ίδιο τρόπο σε θέματα νομικών και φορολογικών πλαισίων. Μάλιστα, από τους κρατικούς φορείς τα κρυπτονομίσματα δεν είναι αποδεκτά και δεν θεωρούνται νόμιμο χρήμα. Ωστόσο, εξαιτίας της δυνατότητας απόκτησης εισοδήματος και μισθοδοσίας καθώς και λόγω των πωλήσεων που πραγματοποιούνται με βάση τα κρυπτονομίσματα, προκύπτουν φορολογικές υποχρεώσεις για τους χρήστες ανάλογα με την χώρα που διαμένουν. Τέτοιες φορολογικές συνέπειες μπορεί να είναι ο φόρος προστιθέμενης αξίας ή ο φόρος υπεραξίας.

Σήμερα, ένα παγκόσμιο ρυθμιστικό πλαίσιο όσον αφορά τη χρήση των κρυπτονομισμάτων δεν υπάρχει αν και πολλοί οργανισμοί πιστεύεται να ξεκινήσουν να εκδίδουν κανόνες και κατευθυντήριες γραμμές σχετικά με τη νέα τεχνολογία. Ωστόσο, σε παγκόσμια κλίμακα υπαγορεύεται η πλήρης απαγόρευση των κρυπτονομισμάτων με ανεκτική συμπεριφορά. Εντούτοις, οι περισσότερες χώρες δεν έχουν κηρύξει παράνομα τα κρυπτονομίσματα χωρίς όμως αυτό να σημαίνει ότι τα αποδέχονται ως νόμιμο χρήμα. Μέχρι στιγμής μόνο η Ιαπωνία έχει προχωρήσει τόσο πολύ ώστε να αποδεχτεί το Bitcoin ως νόμιμο χρήμα και μέσο πληρωμής.

Από την μια πλευρά, πολλές χώρες έχουν ξεκινήσει να δημιουργούν και να υιοθετούν νομικούς και φορολογικούς κανόνες εξαιτίας της μεγάλης εξάπλωσης των κρυπτονομισμάτων. Από την άλλη πλευρά, κάποιες άλλες προσπαθούν να περιορίσουν με αυστηρούς κανονισμούς και να απαγορεύσουν έως ένα βαθμό τη χρήση των κρυπτονομισμάτων στις συναλλαγές. Κίνητρο των περισσότερων χωρών που αποσκοπούν στην απαγόρευση των ψηφιακών αυτών νομισμάτων είναι η χρήση τους σε συναλλαγές της μαύρης αγοράς, η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, το ξέπλυμα χρημάτων και η φοροδιαφυγή.

Πρέπει να τονισθεί πως η τροποποίηση ή η δημιουργία νέων κανόνων νομικού και φορολογικού πλαισίου όσον αφορά τα κρυπτονομίσματα είναι ιδιαίτερα δύσκολη διαδικασία. Σημαντικό εμπόδιο αποτελεί, το γεγονός ότι οι νομοθέτες δεν διαθέτουν τις απαραίτητες εξειδικευμένες γνώσεις για την τεχνολογία των κρυπτονομισμάτων και για τις λειτουργίες της. Αυτό έχει ως αποτέλεσμα να μην μπορούν να ξεχωρίσουν τη τεχνολογία από τις υπηρεσίες που μπορούν εν τελεί να προσφερθούν. Επιπρόσθετα, η ένταξη των αποκεντρωμένων ψηφιακών νομισμάτων στη νομοθεσία είναι ένα περίπλοκο ζήτημα μιας και οι νομοθέτες θα πρέπει να είναι ιδιαίτερα προσεκτικοί ώστε να μην νομιμοποιήσουν την ύπαρξη των κρυπτονομισμάτων ως νομίσματα.

11.2. Φορολογικά και νομοθετικά πλαίσια χωρών

Στο παρόν κεφάλαιο παρουσιάζονται σε γενικό πλαίσιο οι φορολογικοί και νομοθετικοί κανόνες και περιορισμοί που ισχύουν μέχρι σήμερα σε κάποιες χώρες:

Αίγυπτος

Τον Ιανουάριο του 2018, η Κεντρική Τράπεζα της Αιγύπτου δήλωσε την εναντίωσή της ως προς τα κρυπτονομίσματα, όπως το Bitcoin, εξαιτίας του κινδύνου που συνδέεται με τη συγκεκριμένη δραστηριότητα. Ο κύριος ισλαμικός νομοθέτης της Αιγύπτου, δήλωσε ότι το

εμπόριο κρυπτονομισμάτων απαγορεύεται βάσει ενός θρησκευτικού διατάγματος που παρουσιάζει τις εμπορικές συναλλαγές με ψηφιακά νομίσματα ως haram, δηλαδή απαγορευμένες από τον ισλαμικό νόμο. Ο ίδιος δήλωσε ότι τα κρυπτονομίσματα μπορούν να βλάψουν την εθνική ασφάλεια και τα χρηματοπιστωτικά συστήματα (Acheson Noelle, Is Bitcoin legal?, 2013 & loc.gov, 2018).

Αργεντινή

- Σύμφωνα με το Σύνταγμα της Αργεντινής, η μόνη αρχή η οποία μπορεί να εκδώσει νόμιμο νόμισμα είναι η Κεντρική Τράπεζα. Επομένως, τα κρυπτονομίσματα μπορούν να θεωρηθούν χρήμα, όχι όμως νόμιμο από τη στιγμή που δεν έχουν εκδοθεί από την κρατική νομισματική αρχή. Ωστόσο, κρυπτονομίσματα, όπως το Bitcoin, χρησιμοποιούνται όλο και περισσότερο στην Αργεντινή, μια χώρα που διακατέχεται από αυστηρό έλεγχο ξένων νομισμάτων.
- Σύμφωνα με τον αστικό κώδικα της χώρας, το κρυπτονόμισμα μπορεί να θεωρηθεί αγαθό και οι συναλλαγές με κρυπτονομίσματα μπορούν να υπακούσουν στους ίδιους κανόνες όπως οποιαδήποτε άλλη πώληση αγαθών (loc.gov, 2014). Η τελευταία τροποποίηση του νόμου προβλέπει ότι το κέρδος που προκύπτει από αυτές τις πωλήσεις του ψηφιακού νομίσματος θα θεωρείται εισόδημα και θα φορολογείται (loc.gov, 2018).

Αυστραλία

- Τον Ιούνιο του 2013, η Αυστραλία δήλωσε ότι παρακολουθεί την πορεία των κρυπτονομισμάτων και ειδικότερα του Bitcoin, καθώς και τη μεταβλητότητά του, κατά ποσό είναι ευρέως αποδεκτό και την αλληλεπίδρασή του με τα παραδοσιακά χρήματα μέσα από τις ανταλλαγές.
- Τον Δεκέμβριο του 2013, σε σχετική δήλωση του διοικητή της Κεντρικής Τράπεζας της χώρας τονίστηκε πως αν και τα κρυπτονομίσματα δεν έχουν προκαλέσει κάποιο πρόβλημα, υπάρχουν πολλοί κίνδυνοι για τους κερδοσκόπους. Επίσης, σημειώθηκε πως έπειτα από απόφαση, δεν υπάρχει τίποτα που να εμποδίζει τους ανθρώπους να κατέχουν και να συναλλάσσονται σε άλλα νομίσματα συμπεριλαμβανομένων των κρυπτονομισμάτων (loc.gov, 2014).
- Τον Αύγουστο του 2014, το Australian Taxation Office δημοσίευσε κατευθυντήριες οδηγίες για την φορολόγηση των κρυπτονομισμάτων ως αγαθά.
- Τον Ιούλιο του 2017, η Αυστραλία επιβεβαίωσε επισημά ότι θα αντιμετωπίζει τα κρυπτονομίσματα, όπως το Bitcoin, ακριβώς όπως όλα τα υπόλοιπα χρήματα και δεν θα υπόκειται πλέον σε διπλή φορολογία (Suberg William, 2017), ωστόσο όλες οι συναλλαγές

θα πρέπει να καταγράφονται και να διατηρούνται στο γραφείο οικονομικών της χώρας μαζί με τα στοιχεία των πελατών (Acheson Noelle, Is Bitcoin legal?, 2013 & loc.gov, 2018).

Βολιβία

Το 2014, η Κεντρική Τράπεζα της Βολιβίας δήλωσε πως απαγορεύει το Bitcoin και οποιοδήποτε άλλο νόμισμα δεν εκδίδεται από κάποια νομισματική αρχή (loc.gov, 2018).

Βραζιλία

- Στη Βραζιλία τα κρυπτονομίσματα δεν έχουν νομιμοποιηθεί ούτε απαγορευθεί. Συγκεκριμένα, το 2014 η Κεντρική Τράπεζα της χώρας δήλωσε πως διατηρεί μια αρνητική στάση απέναντι στα κρυπτονομίσματα λόγω των λειτουργικών κινδύνων (bcb.gov.br, 2014).
- Το Νοέμβριο του 2017, η ίδια δήλωση επαναλήφθηκε από την τράπεζα της Βραζιλίας (loc.gov, 2018 & bcb.gov.br, 2017).

Γερμανία

- Το 2013, το Γερμανικό Υπουργείο Οικονομικών ανακοίνωσε πως τα κρυπτονομίσματα και συγκεκριμένα το Bitcoin, συμπίπτουν στην κατηγορία των λογιστικών μονάδων και ως εκ τούτου μπορούν να χρησιμοποιηθούν για φορολογικούς σκοπούς και συναλλαγές (loc.gov, 2014). Πιο συγκεκριμένα, οποιοσδήποτε θέλει να αποκτήσει, να πουλήσει ή να αγοράσει κρυπτονομίσματα απαιτείται να έχει άδεια από το Υπουργείο Οικονομικών και αν εν τελεί έχει στη κατοχή του κρυπτονομίσματα για λιγότερο από ένα έτος τότε θα πρέπει να φορολογηθεί, ενώ αν απλά αποκτήσει κέρδη και δεν τα μετακινήσει τότε δεν δημιουργείται φορολογική υποχρέωση.
- Το Φεβρουάριο του 2018, το Υπουργείο Οικονομικών δημοσίευσε επιπλέον οδηγίες σχετικά με το ΦΠΑ στο Bitcoin και σε άλλα κρυπτονομίσματα, και υπογράμμισε ότι η χρήση των κρυπτονομισμάτων για οποιονδήποτε άλλο σκοπό εκτός από μέσο πληρωμής δεν φορολογείται (loc.gov, 2018).

Δανία

- Στη δήλωση της η Finanstilsynet, εποπτική αρχή χρηματοπιστωτικών υπηρεσιών, απέρριψε το κρυπτονόμισμα και συγκεκριμένα το Bitcoin ως νόμισμα. Επιπρόσθετα, υπογράμμισε πως αξιολόγησε τη χρήση του συστήματος και διαπίστωσε πως δεν ανήκει σε καμία από τις κατηγορίες χρηματοπιστωτικών υπηρεσιών και επομένως δεν ισχύουν οι δημοσιονομικοί κανονισμοί. Μέσα από τη συγκεκριμένη δήλωση, τονίζεται ότι το κρυπτονόμισμα

αντιμετωπίζεται ως ηλεκτρονική υπηρεσία και τα έσοδα από τη χρήση του φορολογούνται. Ωστόσο, η εφορία της Δανίας, δεν προέβη σε κάποια σχετική δήλωση από πλευράς της (loc.gov, 2014).

- Το 2017, η Finanstilsynet δήλωσε ότι η συνεργασία με το Bitcoin δεν εμπίπτει σε δικιά της αρμοδιότητα και επομένως δεν εμποδίζει κανέναν να ανοίξει τέτοιες επιχειρήσεις. Επιπλέον, ο επικεφαλής νομικός σύμβουλος ανέφερε πως μπορεί να εξετάσει το ενδεχόμενο να τροποποιηθεί η υπάρχουσα νομοθεσία για την κάλυψη των ψηφιακών νομισμάτων.
- Από φορολογικής άποψης, το 2016 η Δανία απάλλαξε τα κρυπτονομίσματα από το ΦΠΑ, ενώ το 2018 δήλωσε ότι τα κέρδη μέσα από τα κρυπτονόμισμα υπόκεινται σε φόρο εισοδήματος (loc.gov, 2018).

Εκουαδόρ

- Η Κεντρική Τράπεζα του Εκουαδόρ δήλωσε ότι το κρυπτονόμισμα και συγκεκριμένα το Bitcoin δεν είναι εξουσιοδοτημένη μέθοδος πληρωμής στη χώρα, διευκρινίζοντας πως δεν υποστηρίζεται από καμία κεντρική αρχή και πως βασίζεται απλά στη κερδοσκοπία. Ωστόσο, υποστήριξε ότι η αγορά και η πώληση κρυπτονομισμάτων μέσω του διαδικτύου δεν απαγορεύεται, αλλά προειδοποίησε τους πολίτες σχετικά με τους κινδύνους της χρήσης της νέας αυτής τεχνολογίας τονίζοντας πως δεν είναι ένας εγκεκριμένος τρόπος πληρωμής.
- Το 2014, η Εθνική Συνέλευση του Ισημερινού απαγόρευσε τα κρυπτονομίσματα εξαιτίας της δημιουργίας ενός νέου κρατικού ψηφιακού νομίσματος, το οποίο ελέγχεται από τη κυβέρνηση και συνδέεται άμεσα με το τοπικό νόμισμα (Acheson Noelle, Is Bitcoin legal?, 2013 & loc.gov, 2018).
- Το Δεκέμβριο του 2015, κυκλοφόρησε το σύστημα Sistema de Dinero Electronico, δηλαδή σύστημα ηλεκτρονικού χρήματος, καθιστώντας το Εκουαδόρ την πρώτη χώρα με κρατικό σύστημα ηλεκτρονικών πληρωμών (Rosenfeld Everett, 2015).

Ελβετία

- Τον Δεκέμβριο του 2013, υποβλήθηκε πρόταση από 45 μέλη του κοινοβουλίου της Ελβετίας η οποία καλούσε την κυβέρνηση να αξιολογήσει τις δυνατότητες χρησιμοποίησης του κρυπτονομίσματος Bitcoin από τον χρηματοπιστωτικό τομέα της χώρας. Η ίδια πρόταση επιπλέον ζητούσε διευκρινήσεις σχετικά με τη νομική κατάσταση των κρυπτονομισμάτων σε θέματα ΦΠΑ και κινητών αξιών.
- Τον Ιούλιο του 2014, απαντώντας στη συγκεκριμένη πρόταση η Ελβετία δήλωσε ότι δε χρειάζεται να ληφθούν νομοθετικά μέτρα για τα κρυπτονομίσματα.

- Σήμερα, στην Ελβετία, οι επιχειρήσεις κρυπτονομισμάτων, όπως το Bitcoin, υπόκεινται σε κανονισμούς για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και ορισμένες φορές μπορεί να χρειαστεί να λάβουν τραπεζική άδεια.

Ελλάδα

Στην Ελλάδα δεν υπάρχει καμία ειδική νομοθεσία σχετικά με τα κρυπτονομίσματα (loc.gov, 2014). Συγκεκριμένα, η Τράπεζα της Ελλάδος δεν έχει κάνει καμία υπεύθυνη δήλωση σχετικά με τα ψηφιακά νομίσματα πάρα μόνο έχει εκδώσει δυο φορές ανακοινώσεις υιοθετώντας τις απόψεις άλλων ευρωπαϊκών εποπτικών αρχών, προειδοποιώντας τους καταναλωτές για τους κινδύνους (loc.gov, 2018).

Ηνωμένο Βασίλειο

- Το Ηνωμένο Βασίλειο δεν διαθέτει νομούς οι οποίοι να ρυθμίζουν τα κρυπτονομίσματα και η Τράπεζα της Αγγλίας δεν έχει κάνει κάποια σχετική δήλωση σχετικά με τη θέση της προς το συγκεκριμένο θέμα.
- Μια ερευνά υψηλού επιπέδου σχετικά με τη χρήση του Bitcoin πραγματοποιήθηκε το καλοκαίρι του 2013 μέσω της οποίας εκφράστηκαν ανησυχίες σχετικά με τη διαφάνεια του νομίσματος, τη φορολογία και τη χρήση του στη νομιμοποίηση εσόδων από παράνομες δραστηριότητες (loc.gov, 2014).
- Το 2014, η Βρετανική κυβέρνηση αναίρεσε τον προστιθέμενο φόρο απέναντι στο Bitcoin.
- Από το 2017, η κυβέρνηση του Ηνωμένου Βασιλείου δηλώνει ότι το κρυπτονόμισμα θεωρείται ως «ξένο νόμισμα» και ως «περιουσιακό στοιχείο» για διάφορους σκοπούς συμπεριλαμβανομένων των φορολογικών υποχρεώσεων. Η φορολογία των εισοδημάτων που προκύπτουν από τη χρήση των κρυπτονομισμάτων εξαρτάται από τις δραστηριότητές που πραγματοποιούνται (loc.gov, 2018).

Ηνωμένες Πολιτείες

- Τον Μάρτιο του 2013, το Υπουργείο Οικονομικών των Ηνωμένων Πολιτειών εξέδωσε οδηγίες για να διευκρινιστεί ο τρόπος με τον οποίο εφαρμόζεται ο νομός περί τραπεζικής μυστικότητας σε πρόσωπα που δημιουργούν, ανταλλάσσουν και μεταδίδουν ψηφιακά νομίσματα (Financial Crimes Enforcement Network, 2013).
- Τον Μάρτιο του 2014, η IRS, η Εσωτερική Υπηρεσία Εσόδων των Ηνωμένων Πολιτειών της Αμερικής ανακοίνωσε πως το κρυπτονόμισμα καθώς και όλα τα ψηφιακά νομίσματα αντιμετωπίζονται ως «περιουσιακό στοιχείο» για φορολογικούς λογούς.

- Το Μάιο του 2014 η επιτροπή κεφαλαιαγοράς των ΗΠΑ προειδοποίησε για τους κινδύνους από τη χρήση του Bitcoin και άλλων παρόμοιων κρυπτονομισμάτων (Financial Crimes Enforcement Network, 2013).
- Το Υπουργείο Οικονομικών Υπηρεσιών της Νέας Υόρκης, το 2015, ολοκλήρωσε κανονισμούς που απαιτούν από τις εταιρείες που ασχολούνται με bitcoins να καταγράφουν την ταυτότητα των πελατών σε κατάλληλα αρχεία, να διαθέτουν υπεύθυνο συμμόρφωσης και να διατηρούν αποθεματικά κεφαλαίου για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Οι συναλλαγές αξίας 10.000 ή και περισσότερων πρέπει να καταγράφονται και να δηλώνονται.
- Από το 2018, το Υπουργείο Οικονομικών, λαμβάνει περισσότερες από 1.500 δηλώσεις μηνιαίως που αφορούν τα κρυπτονομίσματα (Financial Crimes Enforcement Network, 2018).
- Τον Ιούνιο του 2018, το Ανώτατο Δικαστήριο των Ηνωμένων Πολιτειών συζήτησε για πρώτη φορά το μέλλον των κρυπτονομισμάτων (Farquhar Peter, 2018).

Ιαπωνία

- Τον Μάρτιο του 2014, η Ιαπωνική κυβέρνηση, αποφάσισε πως τα κρυπτονομίσματα, όπως το Bitcoin, δεν αποτελούν νόμιμο νόμισμα βάσει του ισχύοντος νομού και απαγόρευσε στις τράπεζες και στις εταιρείες να διαπραγματεύονται σε bitcoins. Ωστόσο, η απόφαση της κυβέρνησης αναγνωρίζει ότι δεν υπάρχουν νομοί που να απαγορεύουν σε φυσικά ή νομικά πρόσωπα την παραλαβή bitcoins έναντι αγαθών ή υπηρεσιών. Επομένως, αντίστοιχη φορολογία μπορεί να ισχύει και για τα κρυπτονομίσματα.
- Από τον Απρίλιο του 2017, οι επιχειρήσεις που ασχολούνται με τις ανταλλαγές των κρυπτονομισμάτων ρυθμίστηκαν και συμμορφώνονται στους νομούς ως υπηρεσίες πληρωμών. Μέσα από το σχετικό νομό που θεσπίστηκε εκείνη την ημέρα, το κρυπτονόμισμα ορίζεται ως «περιουσιακό στοιχείο» το οποίο μπορεί να χρησιμοποιηθεί ως μέσο πληρωμής. Επιπλέον, οι προαναφερθέντες επιχειρήσεις πρέπει να καταχωρούν αρχεία σχετικά με τις συναλλαγές και να λαμβάνουν μέτρα ασφαλείας για την προστασία των πελατών. Αξίζει να σημειωθεί ότι μέσα από αυτόν τον νέο νόμο η Ιαπωνία έγινε η πρώτη χώρα που δήλωσε ρητώς ότι το κρυπτονόμισμα είναι μια μορφή «νόμιμου νομίσματος» (Acheson Noelle, Is Bitcoin legal?, 2013 & loc.gov, 2018).

Ινδία

- Τον Δεκέμβριο του 2013, η Τράπεζα της Ινδίας ανακοίνωσε δημόσια τους πιθανούς κινδύνους που διέπουν τα κρυπτονομίσματα (loc.gov, 2014).
- Τον Δεκέμβριο του 2017, το Υπουργείο Οικονομικών της Ινδίας δημοσίευσε δήλωση Τύπου στην οποία προειδοποίησε τους επενδυτές σχετικά με τους πραγματικούς και αυξημένους κινδύνους με τη χρήση των κρυπτονομισμάτων στις συναλλαγές (loc.gov, 2018).
- Στην ομιλία του τον Φεβρουάριο του 2018, ο Υπουργός Οικονομικών Arun Jaitley, δήλωσε ότι η κυβέρνηση θα κάνει τα πάντα για να σταματήσει τη χρήση των κρυπτονομισμάτων στην Ινδία για παράνομες ενέργειες. Ο ίδιος επιβεβαίωσε ότι η Ινδία δεν αναγνωρίζει το κρυπτονόμισμα ως νόμιμο χρήμα, ενθαρρύνει ωστόσο την τεχνολογία της blockchain στα συστήματα πληρωμών.
- Τον Απρίλιο του 2018, η Κεντρική Τράπεζα της Ινδίας, ανακοίνωσε την απαγόρευση αγοράς και πώλησης κρυπτονομισμάτων. Επίσης η Κεντρική Τράπεζα, έχει εμποδίσει τα ινδικά χρηματοπιστωτικά ιδρύματα να ασχολούνται με ανταλλαγές κρυπτονομισμάτων και άλλες συναφείς υπηρεσίες (Acheson Noelle, Is Bitcoin legal?, 2013).

Καναδάς

- Τον Απρίλιο του 2013, το Πρακτορείο Εσόδων του Καναδά δήλωσε ότι οι χρήστες κρυπτονομισμάτων θα πρέπει να πληρώνουν φόρο για τις συναλλαγές στο ψηφιακό νόμισμα βάσει δυο φορολογικών κανόνων που ισχύουν για συναλλαγές ανταλλαγής και πράγματα που αγοράζονται και πωλούνται για κερδοσκοπικούς σκοπούς.
- Σε μια ηλεκτρονική δήλωση τον Ιανουάριο του 2014, ένας αξιωματούχος από το Υπουργείο Οικονομικών του Καναδά δήλωσε ότι ο Καναδάς δεν θεωρεί τα κρυπτονομίσματα ως νόμιμο χρήμα. Ωστόσο, ο ίδιος δήλωσε πως θα συνεχιστεί η παρακολούθηση των εξελίξεων που περιλαμβάνουν τα ψηφιακά νομίσματα.
- Σήμερα, οι εταιρίες που ασχολούνται με κρυπτονομίσματα πρέπει να εγγραφούν στο Financial Transactions and Reports Analysis Centre of Canada (Fintrac), εφαρμόζοντας προγράμματα συμμόρφωσης και αναφέροντας ύποπτες ή τρομοκρατικές συναλλαγές. Ο νομός αυτός, εφαρμόζεται και σε μη καναδικά ανταλλακτήρια τα οποία έχουν όμως καναδούς πελάτες. Αντίστοιχα, οι τράπεζες δεν επιτρέπεται να ανοίγουν, να διατηρούν λογαριασμούς ή να έχουν τραπεζική σχέση με εταιρίες που ασχολούνται με ψηφιακά νομίσματα, εάν η εταιρεία αυτή δεν είναι εγγεγραμμένη στη Fintrac.
- Επιπρόσθετα, η τράπεζα του Καναδά έχει διερευνήσει τη πιθανότητά να δημιουργήσει μια έκδοση του νομίσματος της σε blockchain (Teague Solomon, 2016). Συγκεκριμένα,

συνεργάστηκε με τις πέντε μεγαλύτερες τράπεζες του έθνους - και τη συμβουλευτική ως προς τη blockchain εταιρεία R3 - για το έργο που ονομαζόταν Project Jasper. Σε ένα αρχικό σχέδιο το 2016, η κεντρική τράπεζα εξέδωσε CAD-Coins σε ένα blockchain παρόμοιο με το Ethereum (Popper Nathaniel, 2016).

Κίνα

- Τον Δεκέμβριο του 2013, η Κεντρική Τράπεζα της Κίνας και τέσσερα άλλα υπουργεία και επιτροπές της κεντρικής κυβέρνησης εξέδωσαν από κοινού την ανακοίνωση σχετικά με τις προφυλάξεις κατά των κινδύνων των κρυπτονομισμάτων. Ορίζοντας τους ως ένα «ψηφιακό εμπόρευμα» η ανακοίνωση ανέφερε ότι από τη φύση τους τα κρυπτονομίσματα δεν είναι νομίσματα και δεν πρέπει να χρησιμοποιούνται με αυτόν τον τρόπο στην αγορά. Αντίστοιχα, στην ανακοίνωση έγινε φανερό ότι ενώ επιτρέπεται στους πολίτες να εμπορεύονται και να ανταλλάσσουν ελεύθερα το κρυπτονόμισμα ως εμπόρευμα, απαγορεύεται τις κινέζικες χρηματοπιστωτικές τράπεζες να λειτουργούν χρησιμοποιώντας κρυπτονομίσματα ή να χρησιμοποιούν το κρυπτονόμισμα ως νόμιμο χρήμα (loc.gov, 2014).
- Παρόλο που η Κίνα δεν έχει απαγορεύσει ρητά τα κρυπτονομίσματα, τον Σεπτέμβριο του 2017, όλες οι εταιρίες ανταλλαγής κρυπτονομισμάτων απαγορεύτηκαν λόγω χρηματοδότησης χωρίς έγκριση και μέχρι τον Ιούλιο του 2018, 173 πλατφόρμες έκλεισαν (loc.gov, 2018).

Κύπρος

Τον Δεκέμβριο του 2013, η Κεντρική Τράπεζα της Κύπρου σε σχετική δήλωση με θέμα τα ψηφιακά νομίσματα, τόνισε ότι θεωρεί τη χρήση οποιουδήποτε είδους ψηφιακού νομίσματος ως ιδιαίτερα επικίνδυνο, δεδομένου ότι δεν υπόκειται σε κανένα σύστημα και η λειτουργία του είναι ανεξέλεγκτη (loc.gov, 2014). Παρόλα αυτά, δεν υπάρχει σχετική ρητή νομοθετική ρύθμιση και η Κεντρική Τράπεζα έχει διατυπώσει την άποψη ότι το Bitcoin δεν είναι παράνομο.

Μεξικό

- Το 2014, η κεντρική τράπεζα του Μεξικού εξέδωσε δήλωση που εμποδίζει τις τράπεζες να διαπραγματεύονται σε εικονικά νομίσματα (Acheson Noelle, Is Bitcoin legal?, 2013).
- Το επόμενο έτος, το υπουργείο Οικονομικών διευκρίνισε ότι, παρόλο που το bitcoin δεν είναι "νόμιμο νόμισμα", μπορεί να χρησιμοποιηθεί ως μέσο πληρωμής και ως εκ τούτου

υπόκειται στους ίδιους περιορισμούς κατά του ξεπλύματος χρημάτων όπως τα μετρητά (Acheson Noelle, Is Bitcoin legal?, 2013).

Νήσοι Μάρσαλ

Το Μάρτιο του 2018, οι νήσοι Μάρσαλ έγιναν η πρώτη χώρα η οποία εξέδωσε το δικό της κρυπτονόμισμα, ονόματι «sovereign», πιστοποιώντας το ως νόμιμο νόμισμα (Chavez-Dreyfuss Gertrude, 2018 & sov.global).

Συγκεντρωτικά οι χώρες στις οποίες τα κρυπτονομίσματα δεν διώκονται ποινικά είναι, η Νιγηρία, η Νότια Αφρική, η Ναμίμπια, η Ζιμπάμπουε, ο Καναδάς, οι Η.Π.Α, το Μεξικό, η Νικαράγουα, η Κόστα Ρίκα, η Τζαμάικα, η Αργεντινή, η Βραζιλία, η Χιλή, η Βενεζουέλα, το Κιργιζιστάν, το Ουζμπεκιστάν, η Κύπρος, η Ρωσία, το Ισραήλ, η Ιορδανία, το Λίβανο, η Τουρκία, η Ινδία, το Χονγκ Κονγκ, η Ιαπωνία, η Νότια Κορέα, η Μαλαισία, οι Φιλιππίνες, η Σιγκαπούρη, η Ταϊλάνδη, το Βιετνάμ, το Μπρουνέι, η Αυστρία, η Κροατία, η Τσεχία, η Γερμανία, η Ουγγαρία, η Πολωνία, η Ρουμανία, η Σλοβακία, η Σλοβενία, η Ελβετία, η Λευκορωσία, η Ουκρανία, η Δανία, η Εσθονία, η Φιλανδία, η Ισλανδία, η Λιθουανία, η Νορβηγία, η Σουηδία, η Βοσνία – Ερζεγοβίνη, η Βουλγαρία, η Ελλάδα, η Ιταλία, η Μάλτα, η Πορτογαλία, η Ισπανία, το Βέλγιο, η Γαλλία, η Ιρλανδία, το Λουξεμβούργο, η Ολλανδία, το Ηνωμένο Βασίλειο, η Αυστραλία και η Νέα Ζηλανδία.

Αντίθετα, οι χώρες οι οποίες έχουν καταστήσει παράνομα τα κρυπτονομίσματα είναι, η Αλγερία, η Αίγυπτος, το Μαρόκο, η Βολιβία, η Κολομβία, το Εκουαδόρ (Ισημερινός), η Σαουδική Αραβία, το Ιράν, το Μπαγκλαντές, το Νεπάλ, το Πακιστάν, η Κίνα, η Ταϊβάν, η Καμπότζη και η Ινδονήσια.

Κεφάλαιο 12: Επίλογος

12.1. Το μέλλον της Blockchain

Τα κρυπτονομίσματα, όπως είναι εμφανές, έχουν ξεκινήσει να κατέχουν ένα σημαντικό ρόλο στη σημερινή οικονομία. Ωστόσο, η πραγματική καινοτομία των κρυπτονομισμάτων δεν βρίσκεται στα ψηφιακά νομίσματα που χρησιμοποιούνται στις συναλλαγές αλλά στην τεχνολογία της blockchain που κρύβεται πίσω από αυτές. Οι χρήσεις αυτής της τεχνολογίας την σήμερον ημέρα μπορεί περιορίζονται στην επαλήθευση συναλλαγών, ωστόσο ο τρόπος υλοποίησης και λειτουργίας της υπόσχεται να φέρει επανάσταση σε πολλές διαφορετικές επιστήμες και βιομηχανίες (Dossman Jack, Blockchain explained in 1000 words, 2018).

Συγκεκριμένα, η blockchain είναι μια τεχνολογία που καθιστά δυνατή την ψηφιοποίηση και αποθήκευση οποιαδήποτε πληροφορίας. Πιστεύεται επομένως, ότι μπορεί να αποτελέσει έναν ευνοϊκό παράγοντα και να συνεισφέρει θετικά σε άλλες τεχνολογίες εκτός από τα κρυπτονομίσματα, όπως η τεχνητή νοημοσύνη και τα ηλεκτρονικά παιχνίδια καθώς και σε επιστήμες υγείας, στην δημοσιογραφία, σε κυβερνήσεις, σε τράπεζες και σε επιχειρήσεις.

Αναλυτικότερα, οι κυβερνήσεις μπορούν να χρησιμοποιήσουν τη τεχνολογία της blockchain για να διεξάγουν μια ασφαλή και ακριβή ψηφοφορία, για να βελτιστοποιήσουν την αναγνώριση των πολιτών καθώς και εφαρμόσουν καλύτερους ελέγχους των συνόρων τους (Woolf Nicky, 2018). Οι τράπεζες από τη πλευρά τους, μπορούν να επωφεληθούν από μεγαλύτερη ακρίβεια και ταχύτητα στις πληρωμές που επεξεργάζονται, μειώνοντας παράλληλα το κόστος της επεξεργασίας, ή απλά κρατώντας ένα ιστορικό των συναλλαγών τους (accenture.com, How blockchain technology can revolutionize banking).

Επιπλέον, στη βιομηχανία των μέσων ενημέρωσης και της ψυχαγωγίας η δυνατότητα να μοιράζεται ένα ενιαίο, αμετάβλητο σύνολο αρχείων μπορεί να μεταμορφωθεί σε ένα ευρύ φάσμα πληροφοριών διαθέσιμο για χρήση. Η μεγαλύτερη διαφάνεια, η λεπτομερέστερη κατανόηση του κοινού για ένα συγκεκριμένο θέμα και η αποτελεσματικότερη στόχευση της διαφήμισης είναι μερικά μόνο από τα οφέλη (accenture.com, Reengineering the media value chain). Επιπρόσθετα, τα ιατρικά αρχεία των πολιτών είναι συνήθως ανακριβή και δύσκολο να μεταφερθούν. Για αυτόν τον λόγο, αν τα νοσοκομεία, τα κέντρα υγείας και οι ιδιωτικοί γιατροί καταχωρούσαν το ιατρικό ιστορικό κάθε ασθενούς τους στη blockchain τότε τα δεδομένα θα

ήταν περισσότερο ασφαλή, ακριβή και εύκολα προσβάσιμα από οποιοδήποτε εγκεκριμένο μέρος (Khurana Sukant, 2018).

Αντίστοιχα, αν οι επιχειρήσεις τοποθετήσουν με τη σειρά τους τα αγαθά τους στη blockchain τότε και οι καταναλωτές αλλά και οι ιδίες οι επιχειρήσεις θα αποκτήσουν μεγαλύτερη διαφάνεια για την ποιότητα και τον κύκλο ζωής των προϊόντων τους. Επιπλέον, η τεχνολογία των ηλεκτρονικών παιχνιδιών μπορεί να προοδεύσει σε μεγάλο βαθμό μέσα από τη χρήση της συγκεκριμένης τεχνολογίας. Ήδη υπάρχουν εταιρείες παιχνιδιών που είναι βασισμένες στη blockchain και προσφέρουν δυνατότητες που άλλες πλατφόρμες δεν μπορούν, όπως η πώληση και η εμπορία των παιχνιδιών απευθείας μεταξύ των χρηστών. Συγκεκριμένα, υπάρχει το κρυπτονόμισμα IRON το οποίο μπορεί να χρησιμοποιηθεί για την αγορά τέτοιων παιχνιδιών και μπορεί να αποκτηθεί μέσω της διαδικασίας εξόρυξης (Fitzgerald Nickolas, 2018).

Μεταφερόμενοι σε άλλες επιστήμες, όπως η τεχνητή νοημοσύνη είναι φανερό πως ο ρόλος της blockchain μπορεί να είναι θαυματουργός για την εξέλιξή της. Η τεχνητή νοημοσύνη επιτρέπει στους υπολογιστές να λύσουν προβλήματα για τον εαυτό τους δίνοντας τους τη δυνατότητα να γράψουν κώδικα ως απάντηση σε νέες δυσκολίες που αντιμετωπίζουν. Σε συνδυασμό με τη blockchain, η τεχνητή νοημοσύνη είναι σε θέση να γίνει περισσότερο κατανοητή από τους ανθρώπους και να λειτουργήσει πιο αποτελεσματικά κάνοντας και την ίδια τη blockchain πιο αποδοτική. Δεδομένου ότι οι μηχανές τεχνητής νοημοσύνης δεν έχουν αισθήσεις για να αντιληφθούν διάφορες καταστάσεις, χρειάζονται δεδομένα και η λήψη δεδομένων από blockchain μπορεί να βοηθήσει στην ανάκτηση των πληροφοριών γρηγορότερα και ακριβέστερα.

Επιπρόσθετα, καθίσταται πολύ πιο εύκολο για τους επιστήμονες να εντοπίσουν μια διαδρομή που ακολουθήσε ένα μηχανήμα τεχνητής νοημοσύνης για να βρει τη λύση σε ένα πρόβλημα αφού η διαδρομή αυτή είναι αποθηκευμένη σε ένα αμετάβλητο δίκτυο (Shilov Kirill, 2018 & Thibodeaux Wanda, 2018). Τελικώς, ο συνδυασμός blockchain και τεχνητής νοημοσύνης θα μπορούσε να βελτιστοποιήσει εκπληκτικά και τον χώρο της ιατρικής, προσαρμόζοντας θεραπείες ασθενειών και συμβουλές υγείας βάσει του ιατρικού ιστορικού του ασθενούς, της γενετικής του προέλευσης, των επίπεδων στρες που έχει, της τρέχουσας διατροφής του και της γεωγραφικής του θέσης (Nesbitt Audrey, 2018).

Επομένως, δεδομένης της αποκέντρωσης, η τεχνολογία blockchain προσφέρει τη δυνατότητα δημιουργίας επιχειρήσεων και λειτουργιών που είναι ευέλικτες και ασφαλείς. Ωστόσο, αν θα καταφέρουν εν τελεί οι εταιρίες να εισαγάγουν την τεχνολογία και να την αναπτύξουν ώστε να δημιουργήσουν προϊόντα και υπηρεσίες τα οποία οι καταναλωτές θα εμπιστεύονται παραμένει ακόμα άγνωστο. Παρόλα αυτά, καθώς ο κόσμος της blockchain αναπτύσσεται συνεχώς είναι ορθό κάποιος να παρακολουθεί τις σχετικές εξελίξεις. Η ζήτηση της τεχνολογίας συνεχώς αυξάνεται καθώς αυτή ωριμάζει και εξελίσσεται με ταχείς ρυθμούς.

12.2. Γενικά συμπεράσματα

Η εξέλιξη των χρήματων και οι συναλλαγές έχουν βελτιστοποιηθεί σε μεγάλο βαθμό με τη πάροδο των χρόνων πληρώντας κάθε φορά τις ανάγκες του πληθυσμού. Οι ανταλλαγές εμπορευμάτων μετατράπηκαν σε αντικείμενα με σφραγίδες αξίας για τη διευκόλυνση των συναλλαγών. Τα αντικείμενα μετατράπηκαν σε λεπτά νομίσματα από πολύτιμα υλικά για τον έλεγχο της προσφοράς και την καλύτερη εξασφάλιση της αξίας. Οι συναλλαγές με νομίσματα μετατράπηκαν σε συναλλαγές με χαρτονομίσματα και πιστωτικές ή χρεωστικές κάρτες για ευκολία χρήσης και ελέγχου του πληθωρισμού. Σήμερα, τα χαρτονομίσματα χρησιμοποιούνται όλο και λιγότερο καθώς το χρήμα μετατρέπεται σε ψηφιακό νόμισμα και έχουν αναπτυχθεί έννοιες όπως τα κρυπτονομίσματα (Li Kenny, 2018).

Πιο συγκεκριμένα, στη σημερινή εποχή, το μεγαλύτερο μέρος της παραδοσιακής προσφορά χρήματος είναι τα τραπεζικά χρήματα τα οποία κρατούνται σε υπολογιστές. Αυτό θεωρείται επίσης ψηφιακό νόμισμα, αλλά δεν παρουσιάζεται ως τέτοιο αφού τα ψηφιακά νομίσματα δεν γίνονται δεκτά από τις τράπεζες και δεν αναγνωρίζονται ως νόμιμο χρήμα. Επομένως, είναι φανερό πως ο πόλεμος μεταξύ των χρηματοπιστωτικών ιδρυμάτων και των ψηφιακών νομισμάτων είναι ακόμα σε εξέλιξη. Ωστόσο, τα κρυπτονομίσματα δεν αποτελούν κίνδυνο για τη σταθερότητα των τιμών των παραδοσιακών νομισμάτων, παρόλο που είναι ασταθή, εξαιτίας της περιορισμένης σύνδεσης τους με την πραγματική οικονομία, το χαμηλό όγκο συναλλαγών τους και της έλλειψης ευρείας αποδοχής από τους χρήστες (Ευρωπαϊκή Κεντρική Τράπεζα (2012)).

Μέσα από όλα τα δεδομένα που παρουσιάστηκαν στη συγκεκριμένη πτυχιακή εργασία κατέστη φανερό πως το ψηφιακό νόμισμα είναι μια καινοτόμα τεχνολογία η οποία συμβάλει στο ηλεκτρονικό επιχειρείν. Η χρήση του ψηφιακού νομίσματος στις επιχειρήσεις και στην παγκόσμια αγορά, ως ένα νέο αποκεντρωμένο μέσο συναλλαγής και ταυτόχρονα καινοτόμο

σύστημα πληρωμών, αυξάνεται ραγδαία με την πάροδο του χρόνου. Συγκεκριμένα, το Bitcoin, το σημαντικότερο εκ των κρυπτονομισμάτων, επεξεργάζεται στο δευτερόλεπτο έναν πάρα πολύ μεγάλο αριθμό συναλλαγών και βρίσκεται σε συνεχή βελτίωση και εξειδίκευση. Εκτός του Bitcoin όμως, έχουν δημιουργηθεί και άλλα κρυπτονομίσματα, τα λεγόμενα Altcoins, τα οποία κυκλοφορούν με νέες καινοτομίες σε ορισμένα χαρακτηριστικά του είδη υπάρχοντος πρωτοκόλλου Bitcoin.

Παρόλη την ευρεία γκάμα κρυπτονομισμάτων που υπάρχει σήμερα κανένα από αυτά δεν είναι σε θέση να αντικαταστήσει εξολοκλήρου το κυρίαρχο κρυπτονόμισμα Bitcoin όσον αφορά την τιμή, τη χρήση ή την ασφάλεια, διότι παρα τις καινοτομίες που προσφέρουν σε θέματα ταχύτητας ή ιδιωτικότητας, το μεγαλύτερο επίτευγμα μέσα από την όλη διαδικασία είναι η αποκέντρωση την οποία εισήγαγε το πρωταρχικό πρωτόκολλο του Bitcoin. Σύμμαχος φυσικά του Bitcoin είναι ο χρόνος ο οποίος έχει αποδείξει την ασφάλεια του κρυπτονομίσματος τα τελευταία δέκα χρόνια. Επίσης, πρέπει να σημειωθεί ότι όλα τα νέα κρυπτονομίσματα που δημιουργούνται έχουν ένα ιδρυτή ή μια εταιρεία που τα δημιούργησε και που εν τέλει έχει τη μεγαλύτερη επιρροή πάνω στο νόμισμα. Αντιθέτως, το Bitcoin διαφέρει διότι ο ιδρυτής του, ο Satoshi Nakamoto, εξαφανίστηκε, αφήνοντας τον έλεγχο του νομίσματος στα χέρια όλων των χρηστών του δικτύου προσφέροντας στους χρήστες μεγαλύτερα επίπεδα ανεξαρτησίας (Song Jimmy, 2018).

Στη σημερινή εποχή, τα κρυπτονομίσματα λειτουργούν περισσότερο ως μετοχές στις οποίες επενδύουν οι κερδοσκόποι και λιγότερο ως μέσα πληρωμών. Για να μπορέσει ένα κρυπτονόμισμα όπως το Bitcoin να εξαπλωθεί σε όλον τον κόσμο θα πρέπει οι υποστηρικτές του να αποφασίσουν εάν επιθυμούν εν τελεί να το χρησιμοποιούν ως νόμισμα ή ως επένδυση, διότι δεν γίνεται να έχει και τις δυο ιδιότητες. Ωστόσο, στη σημερινή τους μορφή, κανένα από τα διαθέσιμα κρυπτονομίσματα δεν φαίνεται να είναι κατάλληλο για να χρησιμοποιηθεί εξολοκλήρου ως μέσο πληρωμής.

Συγκεκριμένα, τα κρυπτονομίσματα τα οποία είναι διαθέσιμα σήμερα έχουν πολύ μέλλον μπροστά τους πριν καταφέρουν να γίνουν μια εναλλακτική λύση έναντι των παραδοσιακών νομισμάτων (Shobhit Seth, Is Bitcoin failing as a currency?, 2018). Όμως, μέσα από την ωρίμανση των δικτύων και μετά από την προσπέλαση αρκετών εμποδίων ίσως κάποια στιγμή καταφέρει ένα από τα κρυπτονομίσματα να γίνει το ιδανικότερο αποκεντρωμένο ψηφιακό μέσο πληρωμής έναντι των άλλων. Επίσης, είναι πιθανό κάποιο κρυπτονόμισμα μέσα από βελτιώσεις

να καταφέρει να ξεπεράσει το Bitcoin ή μπορεί το Bitcoin να υιοθετήσει βελτιώσεις ενός ανταγωνιστικού νομίσματος, εφόσον δεν αλλάζει θεμελιώδη κομμάτια του πρωτοκόλλου, και έτσι να καταφέρει να φτάσει ένα βήμα πιο κοντά στην τελειοποίηση του.

Αναλύοντας την περίπτωση που τα κρυπτονομίσματα αναλάβουν εξολοκλήρου τον ρόλο των χρήματων σε όλο τον κόσμο, φαίνεται πως θα πρέπει να αναπτυχθεί μια νέα υποδομή ώστε να μπορέσει ο κόσμος να εκπαιδευτεί και να προσαρμοστεί στο νέο σύστημα. Φυσικό επακόλουθο της αυξημένης χρήσης των κρυπτονομισμάτων θα είναι η μείωση της αξίας των παραδοσιακών νομισμάτων και μερικοί άνθρωποι αναγκαστικά θα βρεθούν με χαμένα περιουσιακά στοιχεία. Επίσης, η μετάβαση σε μια οικονομία η οποία θα βασίζεται σε κρυπτονόμισμα θα είναι ιδιαίτερα δύσκολη, αφού τα χρηματοπιστωτικά ιδρύματα θα πρέπει να αλλάξουν τις μεθόδους τους και η κυβέρνηση αναπόφευκτα θα σταματήσει να έχει μεγάλη επιρροή στο νέο αυτό μέσο πληρωμών (Reiff Nathan, Could cryptocurrencies replace cash?, 2017).

Πρέπει ωστόσο να τονισθεί πως η τεχνολογία των κρυπτονομισμάτων, όπως και κάθε τεχνολογία πρώιμου σταδίου, έχει τα ελαττώματά της. Ο μηχανισμός Proof – of –work ο οποίος υπάρχει στο σύστημα Bitcoin, μέσω της διαδικασίας εξόρυξης χρησιμοποιεί πολύ μεγάλες ποσότητες ενέργειας οι οποίες εν τελεί αποτελούν ένα αυξανόμενο περιβαλλοντικό πρόβλημα (Dossman Jack, 10 things blockchain isn't, 2018). Συγκεκριμένα, η αύξηση της ενέργειας που καταναλώνεται είναι εξαρτωμένη από την δυσκολία που υπάρχει στο δίκτυο. Όσο πιο δύσκολη γίνεται η διαδικασία τόσο περισσότερα μηχανήματα και ενέργεια χρειάζονται για να ολοκληρωθεί το mining των κρυπτονομισμάτων.

Στα τέλη του 2018 και στις αρχές του 2019, πολλά από τα μηχανήματα τα οποία κατασκευάστηκαν μέσα στο 2018 για τη διαδικασία της εξόρυξης αχρηστεύτηκαν. Μάλιστα, συμφωνά με μελέτες σχεδόν το μισό του συνολικού εξοπλισμού εξόρυξης που λειτουργούσε τον Οκτώβριο του 2018 βρίσκεται πλέον εκτός λειτουργίας (Chollet Francois, 2018). Εκτιμάται ότι το δίκτυο χρησιμοποιεί σχεδόν την ίδια ποσότητα ηλεκτρικής ενέργειας με όλη την Ιρλανδία και την Αλγερία. Ωστόσο, η Soluna, μια νέα εταιρεία ανανεώσιμων πηγών ενέργειας έχει ένα φιλόδοξο σχέδιο παραγωγής αιολικής ενέργειας αποκλειστικά για διαδικασίες εξόρυξης κρυπτονομισμάτων (Orcutt Mike, 2018).

Επίσης, είναι σημαντικό να αναφερθεί πως σήμερα η ζήτηση στην αγορά εργασίας για προγραμματιστές blockchain εφαρμογών είναι εξαιρετικά υψηλή, γεγονός που αποδεικνύει ότι η

αξία των κρυπτονομισμάτων αυξάνεται επίσης. Μάλιστα, η συγκεκριμένη θέση είναι από τις καλύτερες αμειβόμενες στο χώρο της πληροφορικής μαζί με τους ειδικούς που επικεντρώνονται στην τεχνητή νοημοσύνη. Σύμφωνα με τις έρευνες, ο μέσος μισθός ενός προγραμματιστή ο οποίος ασχολείται με blockchain είναι 150.000 δολάρια έως 175.000 δολάρια ετησίως σε αντίθεση με το ανώτατο όριο των 135.000 δολαρίων που λαμβάνουν οι υπόλοιποι προγραμματιστές σε άλλους κλάδους. Από τα τέλη του 2017, η ζήτηση για μηχανικούς blockchain έχει αυξηθεί κατά 400% και ο λόγος είναι υιοθέτηση της τεχνολογίας σε έργα μεγάλων εταιρειών όπως Facebook, Amazon, IBM και Microsoft (Redenom, 2018 & Huillet Marie, 2018).

Συνοψίζοντας, παρόλη την μεγάλη απήχηση και επιτυχία που κατέχει το Bitcoin στην κεφαλαιαγορά, δεν έχει καταφέρει να πραγματοποιήσει το όνειρο του Satoshi Nakamoto και να οριστεί ως ένα νόμισμα για καθημερινές συναλλαγές. Μπορεί το όνειρο του δημιουργού του να απέχει ακόμα από την πραγματικότητα, ωστόσο το Bitcoin καθώς και όλα τα υπόλοιπα κρυπτονομίσματα αναμφισβήτητα θα συνεχίσουν να απασχολούν τον κόσμο για τα επόμενα χρόνια είτε σε ερευνητικό επίπεδο, είτε μέσα από την ανάδειξη ενός από αυτά ως το νέο παγκόσμιο ηλεκτρονικό νόμισμα. Με άλλα λόγια, όλα δείχνουν ότι τα κρυπτονομίσματα είναι εδώ για να μείνουν, πόσα όμως θα εμφανιστούν και αν τελικά θα μπορέσουν να συνυπάρξουν μέσα σε αυτόν τον ανταγωνιστικό κλάδο μόνο ο χρόνος θα δείξει. Βέβαια, κανείς δεν μπορεί να αποκλείσει το ενδεχόμενο όλες οι χώρες να κηρύξουν παράνομο το ψηφιακό νόμισμα, και από τη μια στιγμή στην άλλη να χάσουν όλα τα κρυπτονομίσματα την αξία τους.

Συμπερασματικά, το αν τελικά τα κρυπτονομίσματα είναι μια «φούσκα» δεν μπορεί κανείς να το απαντήσει με σιγουριά, ωστόσο μέχρι στιγμής πάρα τους κινδύνους και τα εμπόδια φαίνεται να έχουν αντέξει για πάνω από 10 χρονιά στην αγορά, γεγονός που τα καθιστά ως ένα βαθμό ασφαλή ως μέσο συναλλαγής. Παρόλα αυτά, πρέπει να γίνει αντιληπτό ότι ουσιαστικά η blockchain πάνω στη οποία είναι βασισμένα τα κρυπτονομίσματα αποτελεί την πιο σημαντική καινοτομία στον κλάδο της τεχνολογίας. Πρόκειται για μια τεχνολογία η οποία μπορεί να χρησιμοποιηθεί σε πολλές νέες εφαρμογές δίνοντας στον εκάστοτε χρήστη τη δυνατότητα να επωφελείται από όλα της τα πλεονεκτήματα και να διαχειρίζεται ο ίδιος όλες τις πληροφορίες που τον αφορούν. Δεν πρέπει ούτε είναι αναγκαίο να παραγκωνιστούν τα κρυπτονομίσματα για να αναδειχθεί η τεχνολογία η οποία κρύβεται πίσω από αυτά, άλλα μπορούν ταυτόχρονα να εξελίσσονται μαζί προσπερνώντας εμπόδια και προβλήματα μέσα από μια συνεργατική διαδικασία.

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

- Εικ.1.Φωτογραφία εξωφύλλου.....σελ.1
Πηγή: https://wccftech.com/bulgarian_bitcoin_horde/
- Εικ.2. Ανταλλακτικό εμπόριο μεταξύ κτηνοτρόφου και ιχθυοτρόφου.....σελ.11
Πηγή: <https://historyplex.com/barter-services-history-of-barter-system>
- Εικ.3.Μεταλλικά αντικείμενα από χαλκό.....σελ.13
Πηγή:<http://www.haniotika-nea.gr/elliniki-epochi-tou-chalkou-teliose-100-chronia-noritera/>
- Εικ.4.Χάλκινα ιατρικά εργαλεία από το ιερό του Ασκληπιού στην Επίδαυρο.....σελ.13
Πηγή:<http://www.orykta.gr/istoria/istoria-ellinikis-metalleias/41-proistoria-kai-prwtoistoria>
- Εικ.5.Στατήρ της Λυδίας, 6^{ος} αιώνας π.Χ.....σελ.15
Πηγή: <https://www.cngcoins.com/Coin.aspx?CoinID=57383>
- Εικ.6. Αργυρό τετράδραχμο του Μεγάλου Αλεξάνδρου, 323 π.Χ.....σελ.16
Πηγή: <https://www.cngcoins.com/Coin.aspx?CoinID=120975>
- Εικ.7. Πρώιμο Κινέζικο χαρτονόμισμα της περιόδου της δυναστείας Σονγκ.....σελ.17
Πηγή: https://commons.wikimedia.org/wiki/File:Jiao_zi.jpg
- Εικ.8. Ολόγραμμα σε χαρτονόμισμα των 5 ευρώ.....σελ.18
Πηγή: <https://www.flickr.com/photos/spacepleb/391612461/>
- Εικ.9. QR Code για την εφαρμογή PayPal.....σελ.20
Πηγή: <https://www.theverge.com/2013/10/8/4815986/paypal-payment-codes-allow-retail-sales-using-app-qr-codes>
- Εικ.10. Το κρυπτονόμισμα Bitcoin.....σελ.20
Πηγή:<https://medium.com/@martinimontoya/2-9-18-a-primer-on-cryptos-32436b358ebb>
- Εικ.11. Η απογραφή των χρημάτων ενός παίκτη στο World of Warcraft.....σελ.32
Πηγή: https://wow.gamepedia.com/File:Backpack_4.3.png
- Εικ.12. Τα πρώτα κουπόνια της Coca-Cola.....σελ.35
Πηγή[α]: <https://www.suredividend.com/coca-colas-growth-potential/>
Πηγή[β]: <http://jmainewoods.blogspot.com/2008/07/>
- Εικ.13. Η υπογραφή των blocks.....σελ.41
Πηγή: <https://blog.goodaudience.com/blockchain-explained-in-1000-words-6bb83020b03>

- Εικ.14. Δημιουργία νέων υπογραφών με την τροποποίηση των δεδομένων στο Block 2.....σελ.42
Πηγή: <https://blog.goodaudience.com/blockchain-explained-in-1000-words-6bb83020b036>
- Εικ.15. Η μέθοδος κατακερματισμού hash.....σελ.43
Πηγή: <https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348>
- Εικ.16. Τα στοιχεία που απαρτίζουν ένα block.....σελ.44
Πηγή: <https://blog.goodaudience.com/blockchain-explained-in-1000-words-6bb83020b036>
- Εικ.17. Λογαριασμός χρήστη Bitcoin.....σελ.47
Πηγή: <https://bitinfocharts.com/bitcoin/address/1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx>
- Εικ.18. Επίσημο λογότυπο Bitcoin.....σελ.50
Πηγή: https://en.bitcoin.it/wiki/Promotional_graphics
- Εικ.19. Το genesis block της Bitcoin Blockchain.....σελ.52
Πηγή: <https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>
- Εικ.20. Τα στοιχεία του λογαριασμού του Satoshi Nakamoto.....σελ.55
Πηγή: <http://p2pfoundation.ning.com/profile/SatoshiNakamoto>
- Εικ.21. Αντιστοιχία ενός bitcoin νομίσματος σε δολάρια και ευρώ, 26/01/2019.....σελ.69
Πηγή: <https://coinmarketcap.com/currencies/bitcoin/>
- Εικ.22. Η πορεία του Bitcoin από τον Οκτώβριο του 2010 έως τον Οκτώβριο του 2011.....σελ.70
Πηγή: <https://cointelegraph.com/news/a-dazzling-history-of-bitcoins-ups-and-downs>
- Εικ.23. Η πορεία του Bitcoin από τον Μάιο του 2012 έως τον Μάιο του 2013.....σελ.71
Πηγή: <https://cointelegraph.com/news/a-dazzling-history-of-bitcoins-ups-and-downs>
- Εικ.24. Η πορεία του Bitcoin από τα τέλη του 2013 έως τα μέσα του 2015.....σελ.71
Πηγή: <https://cointelegraph.com/news/a-dazzling-history-of-bitcoins-ups-and-downs>
- Εικ.25. Η πορεία του Bitcoin από τις αρχές του 2016 έως τις αρχές του 2018.....σελ.72
Πηγή: <https://cointelegraph.com/news/a-dazzling-history-of-bitcoins-ups-and-downs>

- Εικ.26. Η πορεία του Bitcoin από τις αρχές του 2018 έως τις αρχές του 2019.....σελ.72
Πηγή: <https://markets.bitcoin.com/crypto/BTC>
- Εικ.27. Το επίσημο λογότυπο του Namecoin.....σελ.87
Πηγή: <https://coinmarketcap.com/currencies/namecoin/>
- Εικ.28. Το επίσημο λογότυπο του Litecoin.....σελ.89
Πηγή: <https://blockogy.com/lab/litecoin/>
- Εικ.29. Το επίσημο λογότυπο του Ripple.....σελ.91
Πηγή: <https://www.cryptocoinminingsolutions.com/currency/ripple-xrp/>
- Εικ.30. Το επίσημο λογότυπο του Ethereum.....σελ.94
Πηγή: <https://www.ethereum.org/assets>
- Εικ.31. Το επίσημο λογότυπο του Bitcoin Cash.....σελ.97
Πηγή: <https://dwglogo.com/bitcoin-cash-logo/>

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Kulick, Alex (2017). *What is Money?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/insights/what-is-money/>
- Smithin, John N. (2000). *what is Money?*. London, New York and Canada: Routledge International Studies in Money and Banking
- Beattie Andrew (2016). *The History of Money: From Barter to Banknotes*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://www.investopedia.com/articles/07/roots_of_money.asp
- Banco Central do Brasil (2004). *Origin and Evolution of Money*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.bcb.gov.br/ingles/origevoli.asp>
- Αρχές Οικονομίας – Α Γενικού Λυκείου (2010). Ανακτήθηκε το 2018 από το διαδίκτυο: <http://ebooks.edu.gr/modules/ebook/show.php/DSGL-A114/547/3581,15262/>
- Kulick, Alex (2003). *Barter*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/b/barter.asp>
- Orykta.gr. *Ορυκτοί πόροι και η διαχρονική σημασία τους στην οικονομία*. Ανακτήθηκε το 2018 από το διαδίκτυο: <http://www.orykta.gr/oryktoi-poroi-kai-h-diahroniki-simasia-tous-stin-oikonomia>
- Jan van der Crabben (2011). *Coinage: Definition*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.ancient.eu/coinage/>
- Εγκυκλοπαίδεια Μπριτάνικα - Τεύχος 21 (2016). *Φείδων -Pheidon*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://en.wikisource.org/wiki/1911_Encyclop%C3%A6dia_Britannica/Pheidon
- Αργολική Αρχαική Βιβλιοθήκη Ιστορίας και Πολιτισμού, argolikivivliothiki.gr. *Φείδων*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://argolikivivliothiki.gr/tag/%CF%86%CE%B5%CE%AF%CE%B4%CF%89%CE%BD>
- Kenton, Will (2003). *Currency*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/c/currency.asp>
- Investopedia.com (2010). *Mobile Payment*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/m/mobile-payment.asp>
- Αρχές Οικονομικής Θεωρίας – Γ' Γενικού Λυκείου (2011). Ανακτήθηκε το 2018 από το διαδίκτυο: <http://ebooks.edu.gr/modules/ebook/show.php/DSGL-C117/130/944,3455/>
- Mankiw Gregory N. (2006). *Macroeconomics*. Worth Publishers
- Greco Thomas H. (2001). *Money: Understanding and Creating Alternatives to Legal Tender*. Canada: Chelsea Green Publishing Company

- Ευρωπαϊκή Κεντρική Τράπεζα (2015). *Τι είναι το χρήμα*; Ανακτήθηκε το 2018 από το διαδίκτυο: https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.el.html
- Investopedia.com (2007). *Paper Money*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://www.investopedia.com/terms/p/paper_money.asp
- Investopedia.com (2003). *Credit Card*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/c/creditcard.asp>
- Frankenfield, Jake (2011). *Digital Money*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/d/digital-money.asp>
- Wagner, Andrew (2014). *Digital vs. Virtual Currencies*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507/>
- Wikoff, Shawn (2016). *The expert Shawn Wikoff talks about Electronic money*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/@wikoff.shawn/the-expert-shawn-wikoff-talks-about-electronic-money-d01964dd669c>
- Weidai.com. Ανακτήθηκε το 2018 από το διαδίκτυο: <http://www.weidai.com/bmoney.txt>
- Peck, Morgen E. (2012). *Bitcoin: The cryptoanarchists' answer to cash*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0>
- Acheson, Noelle (2013). *What is Bitcoin?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/what-is-bitcoin>
- Frankenfield, Jake (2018). *Digital Currency*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/d/digital-currency.asp>
- Bank for International Settlements (2018). *Central bank digital currencies*. Ανακτήθηκε το 2018 από το διαδίκτυο: www.bis.org/cpmi/publ/d174.pdf
- Ευρωπαϊκή Κεντρική Τράπεζα (2012). *Virtual Currency Schemes*. Ανακτήθηκε το 2018 από το διαδίκτυο: www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
- Financial Crimes Enforcement Network (2013). *Application of FinCEN's Regulations to Persons Administering Exchanging or Using Virtual Currencies*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>
- Ευρωπαϊκή Αρχή Τραπεζών (2014). *EBA Opinion on 'virtual currencies'*. Ανακτήθηκε το 2018 από το διαδίκτυο: <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>
- Conference of State Bank Supervisors (2015). *State Regulatory Requirements for Virtual Currency Activities*. Ανακτήθηκε το 2018 από το διαδίκτυο:

<https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf>

- FBI – Federal Bureau of Investigation (2012). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf
- Frankenfield, Jake (2018). *Virtual Currency*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/v/virtual-currency.asp>
- Federal Reserve Board (2008). *Electronic Fund Transfer Act*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf
- Economist.com (2013). *Bitcoin under pressure*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.economist.com/technology-quarterly/2013/11/30/bitcoin-under-pressure>
- Frankenfield, Jake (2013). *Cryptocurrency*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/c/cryptocurrency.asp>
- Σπαθάς, Βαγγέλης (2017). *Τι είναι το ψηφιακό νόμισμα;*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.e-dromos.gr/ti-einai-to-pshfiako-nomisma/>
- Korolov, Maria (2012). *Virtual Currency 101*. Ανακτήθηκε το 2018 από το διαδίκτυο: <http://www.hypergridbusiness.com/2012/07/virtual-currency-101/>
- New York Magazine (1992). *America is coupon crazy*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://books.google.gr/books?id=M-MCAAAAMBAJ&lpg=PA18&ots=OOi0srDEQW&dq>
- Virwox.com. *What is the Open Metaverse Currency (OMC) ?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.virwox.com/omc-open-metaverse-currency.php>
- Accenture.com. *Blockchain*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.accenture.com/gr-en/insights/blockchain-index>
- S. Jimi (2018). *How does blockchain work in 7 steps – A clear and simple explanation*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/coinmonks/blockchain-for-beginners-what-is-blockchain-519db8c6677a>
- Mamoria Mohit (2017). *What is the Blockchain?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348>

- Dossman Jack (2018). *Blockchain explained in 1000 words*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://blog.goodaudience.com/blockchain-explained-in-1000-words-6bb83020b036>
- Murray, Maryanne (2018). *Blockchain explained*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html>
- Newgenapps.com (2018). *8 Famous Blockchain Consensus Mechanisms and their Benefits*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.newgenapps.com/blog/8-blockchain-consensus-mechanisms-and-benefits>
- Chaum, David (1983). *Blind Signatures for Untraceable Payments*. Ανακτήθηκε το 2018 από το διαδίκτυο: <http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF>
- Pitta, Julie (1999). *Requiem for a Bright Idea*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.forbes.com/forbes/1999/1101/6411390a.html#1803e8c4715f>
- Brito, Jerry and Castillo, Andrea (2013). *BITCOIN: A Primer for Policymakers*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf
- Steadman, Ian (2013). *Wary of Bitcoin? A guide to some other cryptocurrencies*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://arstechnica.com/information-technology/2013/05/wary-of-bitcoin-a-guide-to-some-other-cryptocurrencies/>
- Theuknews.com (2014). *UK launches initiative to explore potential of virtual currencies*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.theuknews.com/news/224504231/uk-launches-initiative-to-explore-potential-of-virtual-currencies>
- Capital.gr (2018). *Δέκα χρόνια bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <http://www.capital.gr/agores/3324980/deka-xronia-bitcoin>

- Frankenfield, Jake (2011). *Bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/b/bitcoin.asp>
- Wallace, Benjamin (2011). *The rise and fall of Bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.wired.com/2011/11/mf-bitcoin/>
- Frankenfield, Jake (2018). *Genesis Block*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/g/genesis-block.asp>
- Thetimes.co.uk (2009). *Chancellor Alistair Darling on brink of second bailout for bank*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h>
- Nakamoto, Satoshi (2009). *Bitcoin v0.1 released*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html>
- Sourceforge.net. (2009). *Bitcoin v0.1 released – P2P e-cash*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://sourceforge.net/p/bitcoin/news/>
- Peterson, Andrea (2014). *Hal Finney received the first Bitcoin transaction. Here's how he describes it*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/?noredirect=on&utm_term=.68b4b7de6c32
- Popper, Nathaniel (2014). *Hal Finney, Cryptographer and Bitcoin Pioneer, Dies at 58*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://www.nytimes.com/2014/08/31/business/hal-finney-cryptographer-and-bitcoin-pioneer-dies-at-58.html?_r=1
- National Vulnerability Database - nvd.nist.gov. *CVE-2010-5139 Detail*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://nvd.nist.gov/vuln/detail/CVE-2010-5139>

- Groups.csail.mit.edu (1996). *How to make a mint: The cryptography of anonymous electronic cash*. Ανακτήθηκε το 2018 από το διαδίκτυο:
<http://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm>
- Sourceforge.net. (2010). *bitcoin-list — General discussion*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://sourceforge.net/p/bitcoin/mailman/bitcoin-list/?viewmonth=2010>
- Likeinamirror (2013). *Satoshi Nakamoto is (probably) Nick Szabo*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://likeinamirror.wordpress.com/2013/12/01/satoshi-nakamoto-is-probably-nick-szabo/#%21>
- Greenberg, Andy (2014). *Nakamoto's Neighbor: My Hunt for Bitcoin's Creator led to a Paralyzed Crypto Genius*. Ανακτήθηκε το 2018 από το διαδίκτυο:
<https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/#4d8a45e84a37>
- Goodman, Leah McGrath (2014). *The face behind Bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html>
- McMillan, Robert (2013). *Who owns the world's biggest Bitcoin wallet? The FBI*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.wired.com/2013/12/fbi-wallet/>
- P2pfoundation.ning.com. *Satoshi Nakamoto's Page*. Ανακτήθηκε το 2018 από το διαδίκτυο:
<http://p2pfoundation.ning.com/profile/SatoshiNakamoto>
- Davis, Joshua (2011). *The Crypto-Currency: Bitcoin and its mysterious inventor*. Ανακτήθηκε το 2018 από το διαδίκτυο:
<https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency>
- Bosker, Bianca (2013). *Gavin Andresen, Bitcoin Architect: Meet the man bringing you Bitcoin (and getting paid in it)*. Ανακτήθηκε το 2018 από το διαδίκτυο:
https://www.huffingtonpost.com/2013/04/16/gavin-andresen-bitcoin_n_3093316.html?guccounter=1

- Acheson, Noelle (2013). *How Bitcoin mining works*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/how-bitcoin-mining-works>
- Coindesk.com (2014). *What are Bitcoin mining pools?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/get-started-mining-pools>
- Acheson, Noelle (2013). *How can I buy bitcoin?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/how-can-i-buy-bitcoins>
- Acheson, Noelle (2013). *How to store your bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/how-to-store-your-bitcoins>
- Buybitcoinworldwide.com. *Which is the best Bitcoin wallet?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.buybitcoinworldwide.com/wallets/>
- Finley, Klint (2018). *After 10 years, Bitcoin has changed everything and nothing*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.wired.com/story/after-10-years-bitcoin-changed-everything-nothing/>
- Bitcointalk.org (2010). *Pizza for bitcoins?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://bitcointalk.org/index.php?topic=137.0>
- Greenberg, Andy (2011). *Crypto Currency*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#5818ceee353e>
- Chen, Adrian (2011). *The underground website where you can buy any drug imaginable*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160>
- Cronimund, Christoph (2014). *Understanding Bitcoin price charts*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/understanding-bitcoin-price-charts>

- Μπαλάς, Φώτης (2017). *Ποιος είναι ο κίνδυνος να είναι φούσκα το Bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.pcsteps.gr/231467-o-κίνδυνος-να-είναι-φούσκα-το-bitcoin/>
- Tar, Andrew (2017). *Bitcoin price, explained*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://cointelegraph.com/explained/bitcoin-price-explained>
- Barker, Jonathan Todd (2014). *Why is Bitcoin's value so volatile?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp>
- Acheson, Noelle (2013). *How do Bitcoin transactions work?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/how-do-bitcoin-transactions-work>
- Bitcoinfees.info. *Bitcoin Transaction Fees*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://bitcoinfees.info>
- Trssllc.com (2013). *Bitcoin 101: How to get started with the new trend in virtual currencies*. Ανακτήθηκε το 2018 από το διαδίκτυο: https://web.archive.org/web/20160813163512/http://www.trssllc.com/wp-content/uploads/2013/05/White_Paper_Bitcoin_101.pdf
- Cryptobeginners.info. *Common crypto scams and how to avoid them*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.cryptobeginners.info/blog/common-crypto-scams/>
- Κυρίτσης, Άγγελος (2014). *Bitcoin: Είναι ασφαλές; Τι κινδύνους εμπεριέχει;*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.pcsteps.gr/13813-bitcoin/>
- Frankenfield, Jake (2014). *Altcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/a/altcoin.asp>
- Namecoin.org. *Namecoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://namecoin.org>

- Bajpai, Prableen (2017). *The 10 most important cryptocurrencies other than Bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/>
- Coindesk.com (2014). *What is the difference between Litecoin and Bitcoin?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/comparing-litecoin-bitcoin>
- Cryptobeginners.info. *The top 10 cryptos explained*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.cryptobeginners.info/blog/top-10-cryptos-explained/>
- Μπαλάς, Φώτης (2016). *Τα πιο σημαντικά, εναλλακτικά του Bitcoin, ψηφιακά νομίσματα*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.pcsteps.gr/107937-ψηφιακά-νομίσματα-εναλλακτικά-του-bitcoin/>
- Lightning Network. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://lightning.network/>
- Reiff, Nathan (2017). *What is the biggest security threat to ripple cryptocurrency?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/news/what-biggest-security-threat-ripple-cryptocurrency/>
- Frankenfield, Jake (2016). *Ethereum*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/terms/e/ethereum.asp>
- Shobhit, Seth (2018). *All about Ethereum*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/tech/all-about-ethereum/>
- Hertig, Alyssa and Palmer, Daniel (2017). *What is ether?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency>
- Acheson, Noelle (2018). *What is Bitcoin Cash?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/what-is-bitcoin-cash>

- Sharma, Rakesh (2017). *Bitcoin.com co-founder dumps Bitcoin for Bitcoin Cash*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/news/bitcoincom-cofounder-dumps-bitcoin-bitcoin-cash/>
- Φυτίλης, Γιάννης (2017). *Τι είναι το Bitcoin Cash και τι σημαίνει το hard fork του Bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.pcsteps.gr/216861-τι-είναι-το-bitcoin-cash-bitcoin-hard-fork/>
- Coinreport.net (2014). *What are the advantages and disadvantages of Bitcoin?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://coinreport.net/coin-101/advantages-and-disadvantages-of-bitcoin/>
- Blogbucket.org (2017). *What is crypto currency and what are the advantages and disadvantages of it*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.blogbucket.org/what-is-crypto-currency/>
- Weacceptbitcoin.gr. *Σε τι διαφέρει το Bitcoin από μετρητά, από καταθέσεις στην τράπεζα, από το χρυσό και τις πιστωτικές κάρτες;*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://weacceptbitcoin.gr/#compare>
- Bitcoin.org. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://bitcoin.org/en/>
- Pal, Kaushik (2016). *How Bitcoin can change the world*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.techopedia.com/2/31536/trends/how-bitcoin-can-change-the-world>
- Medema, Todd (2018). *Why I sold all of my bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/@toddmmedema/why-i-sold-all-of-my-bitcoin-68b4113a0207>
- Techopedia.com. *Digital Currency*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.techopedia.com/definition/6702/digital-currency>
- Acheson, Noelle (2013). *Is Bitcoin legal?*, Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.coindesk.com/information/is-bitcoin-legal>
- The Law Library of Congress (2018). *Regulation of Cryptocurrency around the world*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>
- The Law Library of Congress (2014). *Regulation of Bitcoin in selected jurisdictions*. Ανακτήθηκε το 2018 από το διαδίκτυο: <http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf>
- Suber, William (2017). *Bitcoin to become 'just like money' in Australia July 1*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://cointelegraph.com/news/bitcoin-to-become-just-like-money-in-australia-july-1>

- Branco Central do Brasil (2014). *Comunicado N° 25.306, de 19 de fevereiro de 2014*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>
- Branco Central do Brasil (2017). *Comunicado N° 31.379, de 16 de novembro de 2017*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.bcb.gov.br/acessoinformacao/legado?url=https:%2F%2Fwww.bcb.gov.br%2Fpre%2Fnormativos%2Fbusca%2Fnormativo.asp%3Fnumero%3D31379%26tipo%3DComunicado%26data%3D16%2F11%2F2017>
- Rosenfeld, Everett (2015). *Ecuador becomes the first country to roll out its own digital cash*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.cnn.com/2015/02/06/ecuador-becomes-the-first-country-to-roll-out-its-own-digital-durrency.html>
- Financial Crimes Enforcement Network (2018). *Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block>
- Farquhar, Peter (2018). *The US Supreme Court just spoke about a Bitcoin future for the first time*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.businessinsider.com.au/the-us-supreme-court-just-spoke-about-a-bitcoin-future-for-the-first-time-2018-6>
- Teague, Solomon (2016). *Celent calls on central banks to issue their own digital currencies*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.euromoney.com/article/b12kpwlr3gtmbb/celent-calls-on-central-banks-to-issue-their-own-digital-currencies>
- Popper, Nathaniel (2016). *Central Banks consider Bitcoin's technology, if not Bitcoin*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.nytimes.com/2016/10/12/business/dealbook/central-banks-consider-bitcoins-technology-if-not-bitcoin.html>
- Chavez-Dreyfuss (2018). *Marshall Islands to issue own sovereign cryptocurrency*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.reuters.com/article/us-cryptocurrencies-marshall-islands/marshall-islands-to-issue-own-sovereign-cryptocurrency-idUSKCN1GC2UD>
- Sov.global. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.sov.global>

- Woolf, Nicky (2018). *What could blockchain do for politics?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/s/welcome-to-blockchain/what-could-blockchain-do-for-politics-de3942d8edda>
- Accenture.com. *How blockchain technology can revolutionize banking*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.accenture.com/gr-en/insight-blockchain-technology-how-banks-building-real-time>
- Accenture.com. *Reengineering the media value chain*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.accenture.com/gr-en/insight-reengineering-media-value-chain>
- Khurana, Sukant (2018). *How blockchain technology can transform the healthcare sector?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/swlh/how-blockchain-technology-can-transform-the-healthcare-sector-604d1bcd16b>
- Fitzgerald, Nickolas (2018). *How blockchain is about to impact the gaming industry*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/@nfitzgerald745/how-blockchain-is-about-to-impact-the-gaming-industry-6721f49792fd>
- Shilov, Kirill (2018). *Artificial Intelligence + Blockchain = Passive income (forever?)*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://hackernoon.com/artificial-intelligence-blockchain-passive-income-forever-edad8c27844e>
- Thibodeaux, Wanda (2018). *A.I. is awesome, blockchain is a powerhouse. But here's what combining them could do*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/inc./a-i-is-awesome-blockchain-is-a-powerhouse-but-heres-what-combining-them-could-do-39c071bd477a>
- Nesbitt, Audrey (2018). *Dr. Robot will see you now: AI, blockchain technology & the future of healthcare*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/datadriveninvestor/dr-robot-will-see-you-now-ai-blockchain-technology-the-future-of-healthcare-edf6d11b7309>
- Li, Kenny (2018). *The history of money & the future of Bitcoin and cryptocurrency economy*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://hackernoon.com/the-history-of-money-the-future-of-bitcoin-and-the-cryptocurrency-economy-5cc25e808275>
- Song, Jimmy (2018). *Why Bitcoin is different*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/@jimmysong/why-bitcoin-is-different-e17b813fd947>
- Shobhit, Seth (2018). *Is Bitcoin failing as a currency?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/news/bitcoin-failing-currency/>

- Reiff, Nathan (2017). *Could cryptocurrencies replace cash?*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://www.investopedia.com/news/could-cryptocurrencies-replace-cash-bitcoin-flipping/>
- Dossman Jack (2018). *10 things blockchain isn't*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://hackernoon.com/10-things-blockchain-isnt-dcb7966d22e5>
- Chollet, Francois (2018). *The Bitcoin network at risk*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/@francois.chollet/the-bitcoin-network-at-risk-bd54a1473a1d>
- Orcutt, Mike (2018). *This company thinks it can help solve Bitcoin's energy problem*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/mit-technology-review/this-company-thinks-it-can-help-solve-bitcoins-energy-problem-d313892b9e45>
- Redenom (2018). *Blockchain engineers are on demand*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://medium.com/redenom/blockchain-engineers-are-on-demand-cc9f5023509>
- Hauillet, Marie (2018). *Demand for blockchain engineers has grown 400% since end of 2017, report say*. Ανακτήθηκε το 2018 από το διαδίκτυο: <https://cointelegraph.com/news/demand-for-blockchain-engineers-has-grown-400-since-end-of-2017-report-says>
- buybitcoinworldwide.com. *How many bitcoins are there?*. Ανακτήθηκε το 2019 από το διαδίκτυο: <https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/>