

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ



ΤΜΗΜΑ: ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ: **Executive MBA**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Darkweb και κρυπτονομίσματα»

**ΔΗΜΗΤΡΙΟΣ ΧΟΥΛΙΑΡΑΣ**

**Πειραιάς, 2021**

## Παράρτημα Β: Βεβαίωση Εκπόνησης Διπλωματικής Εργασίας



**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**  
**ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ**  
**ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ**  
**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ**  
**ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ**

---

### ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

«Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων για Στελέχη : Ε-MBA» με τίτλο:

«Darkweb και κρυπτονομίσματα»

έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Υπογραφή Μεταπτυχιακού Φοιτητή

A handwritten signature in black ink, appearing to read 'Dimitrios Choularas'.

Όνοματεπώνυμο: Δημήτριος Χουλιαράς

Ημερομηνία: 03/12/2021

## Ευχαριστίες

Η ολοκλήρωση αυτής της μεταπτυχιακής εργασίας θα ήταν αδύνατη χωρίς την πολύτιμη καθοδήγηση και υποστήριξη του καθηγητή μου, Καθηγητή Χρηματοοικονομικής του Πανεπιστημίου Πειραιά κ. Φίλιππα Νικόλαου. Του εκφράζω τις ευχαριστίες μου για τον χρόνο που μου διέθεσε και τις γνώσεις που μου μεταλαμπάδευσε καθ' όλη τη διάρκεια της εκπόνησης της διπλωματικής μου εργασίας.

Επιπλέον, θα ήθελα να ευχαριστήσω τον Διευθυντή του Προγράμματος των Μεταπτυχιακών σπουδών, Καθηγητή του Πανεπιστημίου Πειραιά κ. Γεωργακέλλο Δημήτριο, για την υποστήριξη και την κατανόηση του κατά τη διάρκεια των σπουδών και μέχρι την ολοκλήρωση της διατριβής μου.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου, η οποία υπήρξε πάντα ουσιαστικό και ανεκτίμητο στήριγμα σε όλη τη διαδρομή των σπουδών μου έως σήμερα.

# Περιεχόμενα

Βεβαίωση Εκπόνησης Διπλωματικής Εργασίας .....	<b>Error! Bookmark not defined.</b>
Αφιέρωσεις.....	<b>Error! Bookmark not defined.</b>
Ευχαριστίες.....	3
Εισαγωγή .....	6
Κεφάλαιο 1: Εισαγωγή στο Blockchain, στα Κρυπτονομίσματα, και στην εμφάνιση του σκοτεινού διαδικτύου (Dark Web) .....	9
<b>1.1 Εισαγωγή πρώτου κεφαλαίου.....</b>	<b>9</b>
<b>1.2 Το Blockchain και η σύνδεση του με τα κρυπτονομίσματα .....</b>	<b>10</b>
<b>1.3 Εισαγωγή στα κρυπτονομίσματα .....</b>	<b>12</b>
<b>1.4 Ιστορική αναδρομή και η εμφάνιση του Dark Web στην καθημερινότητα</b>	<b>15</b>
<b>1.5 Συμπεράσματα πρώτου κεφαλαίου .....</b>	<b>19</b>
Κεφάλαιο 2: Κρυπτονομίσματα και σκοτεινό διαδίκτυο .....	20
<b>2.1 Εισαγωγή δεύτερου κεφαλαίου .....</b>	<b>20</b>
<b>2.2 Το Bitcoin και η χρήση του στο σκοτεινό διαδίκτυο.....</b>	<b>21</b>
<b>2.3 Τα επικρατέστερα κρυπτονομίσματα εντός του σκοτεινού διαδικτύου ....</b>	<b>23</b>
<b>2.4 Οι λόγοι προτίμησης αλλά και αποθάρρυνσης της χρήσης των κρυπτονομισμάτων στο σκοτεινό διαδίκτυο .....</b>	<b>32</b>
<b>2.5 Λόγοι χρήσης των κρυπτονομισμάτων στο σκοτεινό διαδίκτυο .....</b>	<b>36</b>
<b>2.6 Συμπεράσματα δεύτερου κεφαλαίου .....</b>	<b>43</b>
Κεφάλαιο 3: Το Δίκτυο TOR, TON και η ανάπτυξη του Silk Road .....	45
<b>3.1 Εισαγωγή τρίτου κεφαλαίου .....</b>	<b>45</b>
<b>3.2 Δίκτυο TOR και το δίκτυο TON .....</b>	<b>46</b>
<b>3.3 Silk Road - Ο Δρόμος του μεταξίου .....</b>	<b>50</b>
<b>3.3.1 Το SilkRoad 1 (2011).....</b>	<b>51</b>
<b>3.3.2 Το Silk Road 2.0 (2013) .....</b>	<b>58</b>
<b>3.3.3. Το Silk Road 3.0.....</b>	<b>59</b>
<b>3.3.4 Το Silk Road 3.1. (2016) .....</b>	<b>60</b>
<b>3.4 Συμπεράσματα τρίτου κεφαλαίου .....</b>	<b>64</b>
Κεφάλαιο 4: Μέτρα αντιμετώπισης και περιορισμού του σκοτεινού διαδικτύου από τις παγκόσμιες ρυθμιστικές αρχές.....	66
<b>4.1 Εισαγωγή τέταρτου κεφαλαίου .....</b>	<b>66</b>
<b>4.2 Τα πρώτα βήματα καταπολέμησης του σκοτεινού διαδικτύου από τις ρυθμιστικές αρχές.....</b>	<b>67</b>

<b>4.3 Δράσεις της INTERPOL και της Europol για την αντιμετώπιση του σκοτεινού διαδικτύου παγκοσμίως</b> .....	69
<b>4.4 Συμπεράσματα τέταρτου κεφαλαίου</b> .....	73
Κεφάλαιο 5: Τα κυριότερα κρυπτονομίσματα που χρησιμοποιούνται στο σκοτεινό διαδίκτυο .....	75
<b>5.1 Εισαγωγή πέμπτου κεφαλαίου</b> .....	75
<b>5.2 Αναφορά στα κυριότερα κρυπτονομίσματα που χρησιμοποιούνται στο σκοτεινό διαδίκτυο</b> .....	76
<b>5.2.1 Αναφορά στο κρυπτόνισμα Bitcoin</b> .....	76
<b>5.2.2 Αναφορά στο κρυπτόνισμα Ethereum</b> .....	79
<b>5.2.3 Αναφορά στο κρυπτόνισμα Litecoin</b> .....	81
<b>5.2.4 Αναφορά στο κρυπτόνισμα Monero</b> .....	83
<b>5.2.5 Αναφορά στο κρυπτόνισμα Z cash</b> .....	85
<b>5.2.6 Αναφορά στο κρυπτόνισμα DASH</b> .....	87
<b>5.2.7 Αναφορά στο κρυπτόνισμα Namecoin</b> .....	89
<b>5.2.8 Αναφορά στο κρυπτόνισμα EmerCoin</b> .....	91
<b>5.3 Συμπεράσματα πέμπτου κεφαλαίου</b> .....	93
Κεφάλαιο 6: Εμπειρική και στατιστική ανάλυση των κυριότερων κρυπτονομισμάτων του σκοτεινού διαδικτύου .....	94
<b>6.1 Εισαγωγή έκτου κεφαλαίου</b> .....	94
<b>6.2 Εμπειρική ανάλυση κρυπτονομισμάτων</b> .....	96
<b>6.2.1 Εμπειρικά ευρήματα έτους 2017</b> .....	96
<b>6.2.2 Εμπειρικά ευρήματα έτους 2018</b> .....	98
<b>6.2.3 Εμπειρικά ευρήματα έτους 2019</b> .....	100
<b>6.2.4 Εμπειρικά ευρήματα έτους 2020-03/2021</b> .....	103
<b>6.2.5 Εμπειρικά ευρήματα έτους 2017-03/2021</b> .....	105
<b>6.3 Συμπεράσματα έκτου κεφαλαίου</b> .....	108
Κεφάλαιο 7: Συμπεράσματα Διπλωματικής εργασίας .....	11010
Βιβλιογραφία .....	1144
<b>Επιστημονική</b> .....	1144
<b>Ηλεκτρονική</b> .....	1166

## Εισαγωγή

Τα κρυπτονομίσματα ως έννοια πρωτοεμφανίστηκαν 46 ημέρες μετά την πτώχευση των Lehman Brothers, γεγονός που σηματοδότησε την αρχή μιας από τις μεγαλύτερες οικονομικές κρίσεις στην ανθρώπινη ιστορία. Από το 2008 που εμφανίστηκαν στην παγκόσμια κοινότητα, έχουν προσελκύσει διάφορες κατηγορίες ατόμων σε όλο τον κόσμο που έχουν διαφορετικούς σκοπούς. Μερικοί τα αντιμετωπίζουν ως ένα ανεξάρτητο σύστημα πληρωμών χωρίς την ανάγκη ύπαρξης ενός τρίτου αντισυμβαλλόμενου ατόμου που θα ελέγχει τις συναλλαγές αυτές, ενώ άλλοι αποφάσιζαν να επενδύσουν τα χρήματά τους σε αυτά αποσκοπώντας σε κερδοσκοπικές επενδύσεις. Ενώ επιπρόσθετα, υπήρχαν χρήστες που βρήκαν τα κρυπτονομίσματα ως το μέσο εκείνο που θα υποστήριζε τις παράνομες δραστηριότητες τους κυρίως μέσω συναλλαγών στο σκοτεινό διαδίκτυο (Dark web), αποτελώντας σημείο προβληματισμού για τις εθνικές και τις παγκόσμιες ρυθμιστικές αρχές λόγω των αυξανόμενων περιπτώσεων σε ζητήματα διαφθοράς με κρυπτονομίσματα.

Αρχικά να αναφέρουμε πως τα κρυπτονομίσματα βασίζονται στην τεχνολογία του blockchain η οποία ακόμα και σήμερα είναι μια εξαιρετικά εκκολλημένη και ανεξερεύνητη τεχνολογία καθώς έχει χιλιάδες εφαρμογές. Μπορεί από το 2008 και μετά να γίνεται όλο και πιο πολύπλοκη με το πέρασμα των χρόνων, όμως αυτό δεν εμποδίζει να εισέλθουν νέοι παίχτες στην αγορά και να αυξηθεί η δημοτικότητα των κρυπτονομισμάτων. Αυτό μπορούμε να το παρατηρήσουμε ιδιαίτερα την περίοδο του 2015-2017 που οι τιμές τους παγκοσμίως αυξήθηκαν σε ιδιαίτερα υψηλά επίπεδα, με το Bitcoin, το οποίο αποτελεί το πιο δημοφιλές κρυπτονομίσμα να φτάνει τότε το ιστορικό υψηλό του που ήταν στις 20.000 δολάρια στο τέλος του έτους 2017 όταν το 2008 είχε λιγότερο από 0,10 δολάρια.

Μερικά τυπικά χαρακτηριστικά των κρυπτονομισμάτων όπως η αποκέντρωση, η παγκόσμια φήμη τους, η ανωνυμία ή η ψευδωνυμία που προσφέρουν, σε συνδυασμό με την αρχική έλλειψη κανονισμών για το πεδίο λειτουργίας τους, δημιούργησαν τις βάσεις ώστε να θεωρούνται ένας ενδιαφέρων μηχανισμός για όσους το επιθυμούσαν να παρακάμπτουν το νόμο και να διαπράττουν παράνομες δραστηριότητες, όπως ξέπλυμα χρήματος, εμπόριο ναρκωτικών, σκοτεινές πληρωμές στην αγορά ή ακόμη και χρηματοδότηση τρομοκρατικών δραστηριοτήτων. Για τον λόγο αυτό διάφορες κυβερνητικές αρχές ανά τον κόσμο άρχισαν να εξετάζουν πιο εντατικά την αγορά των κρυπτονομισμάτων

και να αρχίζουν να δημιουργούν μέτρα, κανόνες και νόμους που θα σταματούσαν ή θα περιόριζαν την παράνομη χρήση και θα παρείχαν ορισμένες κατευθυντήριες γραμμές, επιτρέποντας τη βιώσιμη και νομική ανάπτυξή τους.

Ο στόχος λοιπόν της συγκεκριμένης εργασίας είναι αρχικά να παρουσιαστεί το σκοτεινό διαδίκτυο, αναλύοντας το αλλά και πως αυτό αναπτύχθηκε τα τελευταία χρόνια, πως μπορεί κάποιος να αποκτήσει πρόσβαση σε αυτό. Επίσης ποιος είναι ο ρόλος των κρυπτονομισμάτων για τις συναλλαγές και τις δραστηριότητες μέσα σε αυτό, ποια είναι τα κρυπτονομίσματα που είναι ευρέως αποδεκτά και εξυπηρετούν καλύτερα τις παράνομες πρακτικές αλλά και ποια είναι τα μέτρα αντιμετώπισης που εφαρμόζουν οι ρυθμιστικές αρχές όπως η INTERPOL και η Europol για τον περιορισμό του σκοτεινού διαδικτύου. Ενώ τέλος μέσω της συμβολής της εργασίας αυτής παρουσιάζεται μια στατιστική και εμπειρική ανάλυση ανάμεσα στα κρυπτονομίσματα που χρησιμοποιούνται περισσότερο για συναλλαγές εντός του σκοτεινού διαδικτύου αναλύοντας την πορεία τους, τον βαθμό επικινδυνότητάς τους αλλά και την συσχέτισή που έχουν μεταξύ τους από το 2017 μέχρι τον Μάρτιο του 2021, με τελικό στόχο να διερευνηθεί ποιο ή ποια θα μπορούσαν να αποτελέσουν καταλληλότερο μέσω πραγματοποίησης συναλλαγών.

Η δομή της εργασίας έχει ως εξής:

Στο πρώτο κεφάλαιο αναλύεται η τεχνολογία του Blockchain, οι βασικές έννοιες των κρυπτονομισμάτων αλλά και η εμφάνιση του Dark Web στην καθημερινότητα μας για την εξυπηρέτηση παράνομων δραστηριοτήτων

Στο δεύτερο κεφάλαιο παρουσιάζονται στατιστικά στοιχεία γύρω από την χρήση και οι λόγοι επιλογής των κρυπτονομισμάτων, και ιδιαίτερα του Bitcoin στο σκοτεινό διαδίκτυο, εξετάζοντας παράλληλα ποια κρυπτονομίσματα προτιμώνται σε μεγαλύτερο βαθμό τόσο από τους αγοραστές όσο και από τους πωλητές παράνομων προϊόντων ενώ επίσης αναλύεται και ο ρόλος των altcoins, τα οποία αποτελούν μια νέα τεχνολογική κατηγορία κρυπτονομισμάτων.

Στο τρίτο κεφάλαιο αναλύεται η τεχνολογία των δικτύων TOR (The Onion Router) και TON (Telegram Open Network) τα οποία βρίσκονται πίσω από την πρόσβαση στην χρήση του σκοτεινού διαδικτύου αλλά και αναλύεται η εξέλιξη της πρώτης σκοτεινής αγοράς στο διαδίκτυο που ήταν το λεγόμενο SilkRoad (ο δρόμος του μεταξιού) μέσω του οποίου πραγματοποιούνταν αγορές και πωλήσεις παράνομων προϊόντων όπως ναρκωτικών και όπλων.

Στο τέταρτο κεφάλαιο παρουσιάζονται μέτρα και ενέργειες που έχουν ακολουθηθεί από ρυθμιστικούς οργανισμούς παγκοσμίως για τον περιορισμό της δραστηριότητας του σκοτεινού διαδικτύου. Στο κεφάλαιο επικεντρωνόμαστε στις δράσεις της Ιντερπολ και της Ευγοροί που ακολουθούνται και εφαρμόζονται τα τελευταία χρόνια για τον σκοπό αυτό.

Στο πέμπτο κεφάλαιο ακολουθεί μια σύντομη ανάλυση γύρω από τα κυριότερα κρυπτονομίσματα που χρησιμοποιούνται στο Dark web. Παρουσιάζονται στοιχεία όπως το έτος δημιουργίας τους, γενικά χαρακτηριστικά της τεχνολογίας τους, το επίπεδο ανωνυμίας που προσφέρουν, η διαγραμματική απεικόνιση της πορείας της τιμής τους, κλπ. Τα κρυπτονομίσματα αυτά είναι το Bitcoin, το Ethereum, το Monero, το Zcash, το Dash και το Litecoin, αλλά και κάποια λιγότερο γνωστά και δημοφιλή που είναι το Namecoin και το Emercoin, τα οποία σύμφωνα με πρόσφατες έρευνες αρχίζουν και κερδίζουν μερίδιο στις συναλλαγές εντός του σκοτεινού διαδικτύου.

Στο έκτο κεφάλαιο το οποίο αποτελεί και την συμβολή στην διπλωματική εργασία παρουσιάζεται μια στατική και εμπειρική ανάλυση από το 2017 έως τον Μάρτιο του 2021 αλλά και για κάθε έτος ξεχωριστά ανάμεσα στα κρυπτονομίσματα που χρησιμοποιούνται περισσότερο για συναλλαγές εντός του σκοτεινού διαδικτύου. Τα κρυπτονομίσματα αυτά είναι εκείνα που αναλύονται στο πέμπτο κεφάλαιο και σκοπός της ανάλυσης ακολουθεί είναι μέσα από στατιστικές και εμπειρικές τεχνικές να διεξαχθούν συγκριτικά συμπεράσματα σχετικά με την πορεία που παρουσίασαν τα κρυπτονομίσματα αυτά, την επικινδυνότητά τους αλλά και τον βαθμό συσχέτισης που έχουν μεταξύ τους, με τελικό στόχο να διερευνηθεί ποιο ή ποια θα μπορούσαν να αποτελέσουν καταλληλότερο μέσω πραγματοποίησης συναλλαγών στο σκοτεινό διαδίκτυο.

Τέλος, ακολουθούν τα τελικά συμπεράσματα στο έβδομο κεφάλαιο της εργασίας καθώς και η βιβλιογραφικές αναφορές που χρησιμοποιήθηκαν για να συγγραφτεί η εργασία αυτή.



# **Κεφάλαιο 1: Εισαγωγή στο Blockchain, στα Κρυπτονομίσματα και στην εμφάνιση του σκοτεινού διαδικτύου (DarkWeb)**

## **1.1 Εισαγωγή πρώτου κεφαλαίου**

Το πρώτο κεφάλαιο της διπλωματικής εργασίας επικεντρώνεται στην τεχνολογία του Blockchain, στις βασικές έννοιες των κρυπτονομισμάτων αλλά και στην εμφάνιση του Dark Web στην καθημερινότητα μας με την μορφή ενός μέρους του διαδικτύου που χρησιμοποιείται για παράνομες δραστηριότητες και συναλλαγές.

Μπορεί η ιδέα πίσω από την δημιουργία του να προέρχεται από τα τέλη της δεκαετίας του 1990 για ανάπτυξη ενός ανώνυμου και κρυπτογραφημένου δικτύου που θα προστάτευε τις επικοινωνίες που πραγματοποιούσαν οι Αμερικάνικοι κατάσκοποι, όμως η εμφάνιση της τεχνολογίας του Blockchain και γενικότερα των κρυπτονομισμάτων αποτέλεσαν βασικό σημείο για την ανάπτυξη παράνομων διαδικτυακών δραστηριοτήτων εντός αυτού. Έτσι στο κεφάλαιο αυτό αναλύονται τα βασικά χαρακτηριστικά που εμφανίζει το σκοτεινό διαδίκτυο και το οδήγησαν να αποτελεί σημείο παράνομων δραστηριοτήτων αλλά και οι λόγοι που τα κρυπτονομίσματα ταιριάζουν σε εφαρμογή με αυτό.

## 1.2 Το Blockchain και η σύνδεση του με τα κρυπτονομίσματα

Όπως αναφέρεται από την PWC των Ηνωμένων Πολιτειών (2021), το blockchain είναι ένα peer-to-peer αποκεντρωμένο καθολικό δίκτυο συναλλαγών στο οποίο οι συμμετέχοντες χρησιμοποιώντας το μπορούν να επιβεβαιώσουν συναλλαγές χωρίς να απαιτείται η έγκριση τους από κάποια κεντρική αρχή που τις ελέγχει. Ως τεχνολογία είναι εκείνη που επιτρέπει την ύπαρξη και την δημιουργία των κρυπτονομισμάτων χωρίς όμως να έχει εφαρμογή μόνο στο συγκεκριμένο τομέα.

Να αναφέρουμε εν συντομία πως τα κρυπτονομίσματα είναι ένα μέσο συναλλαγών όπως το Αμερικάνικο δολάριο ή όπως το Ευρώ, αλλά έχουν ψηφιακή μορφή και υπόσταση. Χρησιμοποιούν τεχνικές κρυπτογράφησης για τον έλεγχο της δημιουργίας αυτών των νομισματικών μονάδων αλλά και για την επαλήθευση της μεταφοράς των χρημάτων μεταξύ των αντισυμβαλλόμενων ατόμων.

Μπορεί η δημιουργία του Blockchain να οφείλεται στο Bitcoin, το οποίο είναι το πιο γνωστό κρυπτονόμισμα στην σημερινή εποχή, καθώς αποτέλεσε την τεχνολογία για την εφεύρεση του, όμως εμπειρικλείει επίσης πολλές εφαρμογές εκτός από το Bitcoin και τα κρυπτονομίσματα γενικότερα. Οι πιο γνωστές εφαρμογές του Blockchain είναι η μεταφορά χρημάτων, η διευθέτηση συναλλαγών, η διενέργεια ψηφοφοριών, αλλά και διάφορες άλλες περιπτώσεις στις οποίες έχει σημείο εφαρμογής. Αναλυτικότερα θα μπορούσαμε για παράδειγμα να δούμε την τεχνολογία του Blockchain από την πλευρά των επιχειρήσεων καθώς η χρήση της θα οδηγήσει στην βελτίωση της επιχειρηματικής διαδικασίας βελτιώνοντας τα λογισμικά που ήδη χρησιμοποιούνται. Επειδή αποτελεί μια συνεργατική τεχνολογία, υπόσχεται την ικανότητα βελτίωσης των επιχειρηματικών διαδικασιών που γίνονται μεταξύ διαφορετικών εταιρειών μειώνοντας ριζικά το κόστος τους. Ενώ επίσης στην περίπτωση των χρηματοπιστωτικών ιδρυμάτων χρησιμεύει για να βελτιώσει όλες τις διαδικασίες τους. Συνεπώς η τεχνολογία του blockchain έχει τη δυνατότητα να οδηγήσει σε ένα ριζικά διαφορετικό ανταγωνιστικό μέλλον για τη βιομηχανία παροχής χρηματοπιστωτικών υπηρεσιών και όχι μόνο.

Τέλος αυτό που αξίζει να αναφέρουμε είναι μια σύντομη περιγραφή γύρω από την πραγματοποίηση συναλλαγών μέσω του Blockchain. Αρχικά, κάποιο άτομο μέσω του υπολογιστή του αιτείται την διενέργεια μιας συναλλαγής. Τότε η αίτηση της συναλλαγής αυτής μεταδίδεται σε ένα peer-to-peer (P2P) δίκτυο, το οποίο αποτελείται από υπολογιστές που ονομάζονται κόμβοι. Το δίκτυο αυτό των κόμβων επικυρώνει τη συναλλαγή η οποία μπορεί να περιλαμβάνει κρυπτονομίσματα, έξυπνα

συμβόλαια, αρχεία, αλλά και άλλου είδους πληροφορίες. Όταν η συναλλαγή αυτή επικυρωθεί συνδυάζεται με άλλες συναλλαγές και δημιουργούν ένα νέο blockδεδομένων στο καθολικό του δικτύου Blockchain. Τέλος το νέο αυτό blockπροστίθεται στα ήδη υπάρχοντα blockστου blockchainκαι έχει μόνιμο και μη αναστρέψιμο χαρακτήρα. Συνεπώς αφού ακολουθήσει αυτό το στάδιο τότε η συναλλαγή έχει ολοκληρωθεί.

Τέλος μερικά από τα πλεονεκτήματα του Blockchainείναι πως αυξάνει την διαφάνεια στις συναλλαγές, συμβάλει στην παρακολούθηση με ακρίβεια των διαδικασιών που μπορεί να ακολουθούν οι επιχειρήσεις μειώνοντας το κόστος αυτών, αλλά και ενδεικτικά να αναφέρουμε πως έχει σταθερό καθολικό στο οποίο καταγράφονται όλες οι συναλλαγές που δεν αλλάζει και δεν μπορεί να τροποποιηθεί. Αντιθέτως θα μπορούσαμε να πούμε πως η έλλειψη ρυθμιστικού πλαισίου από τις κεντρικές κυβερνητικές αρχές, η περίπλοκη και αρκετά νεοφυής τεχνολογία που χρησιμοποιεί και ο μεγάλος ανταγωνισμός μεταξύ διαφορετικών Blockchain που υπάρχουν αποτελούν μερικά από τα μειονεκτήματα του.

### 1.3 Εισαγωγή στα κρυπτονομίσματα

Προκειμένου να είμαστε σε θέση να αναλύσουμε βασικά χαρακτηριστικά του σκοτεινού διαδικτύου, είναι ιδιαίτερα σημαντικό να κατανοηθούν βασικές έννοιες και στοιχεία των κρυπτονομισμάτων καθώς όπως θα δούμε στην συνέχεια αποτελούν το κύριο μέσο πληρωμών εντός του Dark web.

Αρχικά ένα κρυπτονομίσμα, όπως για παράδειγμα είναι το Bitcoin, θα μπορούσαμε να πούμε πως αποτελεί ένα μέσο πραγματοποίησης συναλλαγών που δημιουργείται και αποθηκεύεται ηλεκτρονικά στο Blockchain, χρησιμοποιώντας κρυπτογραφικές τεχνικές για τον έλεγχο της δημιουργίας χρηματικών μονάδων και της επαλήθευσης των συναλλαγών (PWC, 2021). Βέβαια γεγονός είναι πως παρόλο που η φιλοσοφία των κρυπτονομισμάτων είναι ήδη δέκα ετών, οι ρυθμιστικές αρχές σε διάφορες χώρες στον κόσμο προτείνουν διαφορετικές προσεγγίσεις που ταξινομούν και ορίζουν τα κρυπτονομίσματα. Για παράδειγμα αναγνωρίζονται τόσο ως υποκατηγορία του ευρύτερου ψηφιακού χρήματος όσο και ως υποκατηγορία εικονικών νομισμάτων. Οι δύο αυτοί χαρακτηρισμοί έχουν προέλθει τόσο από την Bank for International Settlements (2015) όσο και από την World Bank (2017). Ενώ η δεύτερη προσέγγιση προτιμάται από την European Banking Association (2014), την European Central Bank (2015), την European Securities and Markets Authority (2018) και το International Monetary Fund (2016), ενώ όλοι συμφωνούν πως αυτό που διακρίνει τα κρυπτονομίσματα από άλλα χρηματοοικονομικά μέσα είναι η ανεξάρτητη έκδοσή τους, και η μη αποδοχή τους από τις επίσημες κυβερνητικές αρχές.

Στο σημείο αυτό ακολουθούν χαρακτηριστικά που διέπουν και αποδόθηκαν για τα κρυπτονομίσματα τα οποία θα μας βοηθήσουν να τα κατανοήσουμε καλύτερα. Αυτά τα χαρακτηριστικά θα μπορούσαν να θεωρηθούν ως πως καλύπτουν όλες τις προσεγγίσεις, λαμβάνοντας υπόψιν τις διαφορές που υπάρχουν γύρω από τους διαφορετικούς ορισμούς τους.

Αρχικά τα κρυπτονομίσματα αποτελούν μια ψηφιακή αναπαράσταση αξίας τα οποία είναι προορισμένα να υποστηρίζουν τις peer to peer συναλλαγές, να χρησιμοποιούνται ως μέσο συναλλαγών γενικής χρήσης και να μην είναι συνδεδεμένα με οποιαδήποτε κεντρική τράπεζα. Επίσης να έχουν επίπεδα ασφάλειας μέσω του μηχανισμού της κρυπτογραφίας που διαθέτουν και να μπορούν να μετατραπούν σε χρήματα τύπου fiat και αντίστροφα (Houben & Snyers, 2018).

Επίσης, ένα βασικό χαρακτηριστικό τους είναι πως τα περισσότερα από αυτά είναι κατασκευασμένα σε δημόσια δίκτυα που δεν χρειάζεται κάποιος να έχει άδεια εισόδου σε αυτά (Hileman & Rauchs, 2017), ελαχιστοποιώντας την ασυμμετρία πληροφόρησης στους χρήστες γύρω από την διαδικασία των συναλλαγών (Tabarrok & Cowen, 2015).

Ακόμη τα κρυπτονομίσματα που βασίζονται στην τεχνολογία blockchain μέσω διαφορετικών αλγορίθμων επαλήθευσης λύνουν το πρόβλημα των «διπλών δαπανών», το οποίο σημαίνει με απλά λόγια πως δεν μπορεί να χρησιμοποιηθεί μια μονάδα του κρυπτονομίσματος περισσότερες από μία φορές (Budish, 2018; Efanov & Roschin, 2018).

Επιπρόσθετα, η νέα αυτή τεχνολογία που εφαρμόζεται από τα κρυπτονομίσματα δηλαδή του blockchain επέτρεψε επίσης την διεξαγωγή συναλλαγών μεταξύ δύο αντισυμβαλλόμενων μερών χωρίς την ανάγκη ύπαρξης ενός μεσάζοντα ο οποίος θα ήταν υπεύθυνος για τη σωστή επικύρωση και τον διακανονισμό των συναλλαγών (Gupta, 2017; Moore & Christin, 2013; Tapscott & Tapscott, 2016). Η κάθε συναλλαγή καταγράφεται σε ένα καθολικό δίκτυο στο οποίο η κάθε καταχώριση πρέπει κατά κύριο λόγο να είναι σωστή, επαληθεύσιμη και αμετάβλητη. Αυτό διασφαλίζεται από τους ανθρακωρύχους (miners) οι οποίοι είναι υπεύθυνοι για την ασφάλεια του συστήματος, την επικύρωση των συναλλαγών, την δημιουργία των νέων Block του δικτύου και γενικά ο ρόλος τους είναι τέτοιος ώστε να διατηρούν την σταθερότητα του συστήματος.

Ακόμη, σύμφωνα με τον Satoshi Nakamoto, ο οποίος με το άρθρο του με τίτλο “a peer to peer electronic cash system” (2008) , αναφέρει πως τα κρυπτονομίσματα αποτελούν ένα σύστημα με παγκόσμιο χαρακτήρα και έχουν την δυνατότητα να κυκλοφορούν ελεύθερα πέρα από τα σύνορα των χωρών, έχοντας πολύ εύκολη χρήση καθώς απαιτείται μόνο η εγκατάσταση λογισμικού σε ηλεκτρονικό υπολογιστή.

Ενώ επίσης ένα ακόμα χαρακτηριστικό τους είναι πως αποτελούν το σημείο έναρξης πολλών περιουσιακών στοιχείων που ονομάζονται cryptoassets, τα οποία έχουν δημιουργηθεί μέσω της χρήσης της τεχνολογίας του blockchain. Τα περισσότερα από αυτά ήδη από την στιγμή που δημιουργούνται έχουν προκαθορισμένη την προσφορά χρήματος. Σε πολλές περιπτώσεις η αρχική διαδικασία έκδοσης τους διαφέρει σημαντικά καθώς κάποια μπορούν να εξορυχθούν ενώ άλλα δίνονται στο ευρύ κοινό μέσω διαδικασίας ICO.

Επιπρόσθετα, παρά το γεγονός ότι το σύστημα τους έχει αποκεντροποιημένο χαρακτήρα που σημαίνει ότι δεν υπάρχει κεντρική οντότητα που να ελέγχει την προσφορά των κρυπτονομισμάτων έχουν μια αρκετά κεντροποιημένη λογική η οποία συνδέεται με το γεγονός πως όλοι οι κανόνες λειτουργίας τους είναι προκαθορισμένοι και ορισμένοι από τον αλγόριθμο ανοιχτού κώδικα που ακολουθούν. Πολλά χαρακτηρίζονται ως ανώνυμα αλλά και κάποια από αυτά ως ψευδό-ανώνυμα. Αυτή η πτυχή είναι εξαιρετικά ελκυστική για έναν παράνομο χρήστη, που επιθυμεί να εκμεταλλευτεί την καινοτόμο αυτή τεχνολογία κάνοντας παράνομες συναλλαγές..

Ένα ακόμα χαρακτηριστικό που συνδέεται με τα κρυπτονομίσματα είναι πως οι χρήστες τους για λόγους κερδοσκοπίας πολλές φορές αυξάνουν την ζήτηση και το ενδιαφέρον για αυτά για να ανεβάσουν σε βραχυπρόθεσμο επίπεδο τις τιμές τους.

Ενώ τέλος υπάρχουν εταιρείες που παρέχουν ψηφιακά πορτοφόλια τα οποία προσφέρονται από πλατφόρμες στις οποίες διατηρούνται και διακρατούνται τα κρυπτονομίσματα αλλά και ανταλλάσσονται μεταξύ των διάφορων χρηστών. Αυτές οι πλατφόρμες παράλληλα επιτρέπουν την ομαλή ανταλλαγή μεταξύ fiat νομισμάτων όπως είναι το ευρώ, το δολάριο, κλπ .

## 1.4 Ιστορική αναδρομή και η εμφάνιση του Dark Web στην καθημερινότητα

Μπορεί η εμφάνιση του σκοτεινού διαδικτύου έγινε πρώτα απ' όλα γνωστή στην δεκαετία του 1970 και αυτός να ήταν ένας όρος που χρησιμοποιήθηκε για τα ιδιωτικά δίκτυα που είχαν υψηλό επίπεδο ιδιωτικότητας, όμως ιστορικά σύμφωνα με τους Kumar A., Rosenbach E.- IMF (2021) στα τέλη της δεκαετίας του 1990, δύο ερευνητικοί οργανισμοί στο Υπουργείο Άμυνας των ΗΠΑ έκαναν προσπάθειες για την ανάπτυξη ενός ανώνυμου και κρυπτογραφημένου δικτύου που θα προστάτευε τις επικοινωνίες που πραγματοποιούσαν οι Αμερικάνικοι κατάσκοποι. Αυτό το μυστικό δίκτυο δεν θα ήταν γνωστό ή προσβάσιμο σε συνηθισμένους χρήστες του διαδικτύου. Όμως η αρχική αυτή υπόθεση δεν πραγματοποιήθηκε ποτέ πλήρως καθώς ορισμένοι από τους ερευνητές διέκριναν πως προσθέτει αξία καθώς είναι ένα δίκτυο μη κερδοσκοπικό που επικεντρώνεται στην ανωνυμία για τα ανθρώπινα δικαιώματα και στην διατήρηση της ιδιωτικής ζωής.

Το σκοτεινό διαδίκτυο χρησιμοποιήθηκε πρώτη φορά από τέσσερις ανώτερους μηχανικούς ασφαλείας της Microsoft (BiddleP.,EnglandP.,PeinadoM. και WillmanB.) τον Νοέμβριο του 2002 στο άρθρο The Darknet and the Future of Content Distribution και με τον όρο του Darknet θέλησαν να περιγράψουν «ένα σύνολο δικτύων και τεχνολογιών που χρησιμοποιούνται στην ανταλλαγή ψηφιακού υλικού».

Το σκοτεινό διαδίκτυο το οποίο στην αγγλική γλώσσα ονομάζεται Darknet ή Darkweb αποτελεί ένα σύνολο ιστοσελίδων που χρησιμοποιούν εργαλεία ανωνυμίας όπως είναι το δίκτυο "TOR " ή το "I2P". Ενώ σύμφωνα με τον ηλεκτρονικό ιστότοπο wired.com (2014), στόχος του είναι να μην αποκαλύπτεται η διεύθυνση IP των χρηστών εντός του διαδικτύου. Ο λόγος που οι χρήστες του διαδικτύου χρησιμοποιούν το σκοτεινό διαδίκτυο είναι για να διαδίδουν την ψηφιακή τους κουλτούρα ελεύθερα, να ανταλλάσσουν αρχεία με ασφάλεια, ιδιωτικότητα, ανωνυμία και ελευθερία, σε ένα «υπόγειο» τμήμα του διαδικτύου.

Αυτό το φαινομενικά κρυφό μέρος του Διαδικτύου, στην αρχή της δημιουργίας του δεν είχε ως απώτερο σκοπό να χρησιμοποιηθεί για απατηλές πράξεις και δραστηριότητες. Παρόλα αυτά σταδιακά όμως μετατράπηκε σε καταφύγιο για την επικοινωνία και τον προγραμματισμό εγκληματικών δραστηριοτήτων και αυτό γιατί διευκόλυνε το εμπόριο παράνομων προϊόντων όπως ναρκωτικά και όπλα και τα

κρυπτονομίσματα, ειδικά το Bitcoin, να γίνονται το νόμισμα επιλογής για τις συναλλαγές αυτές. (hackernoon.com, 2018)

Αυτό που αξίζει να επισημάνουμε είναι πως εκτός από τα εργαλεία που παρέχουν ανωνυμία όπως είναι το δίκτυο “TOR ” ή το “I2P”, ιδιαίτερα μετά την εμφάνιση του Blockchain και της τεχνολογίας των κρυπτονομισμάτων άρχισαν να χρησιμοποιούνται τα δίκτυα P2P (peer-to-peer) τα οποία επιτρέπουν την απευθείας ανταλλαγή πληροφοριών μεταξύ υπολογιστικών κόμβων χωρίς την διαμεσολάβηση κεντρικού διακομιστή. Το χαρακτηριστικό αυτό της P2P τεχνολογίας είναι το βασικό στοιχείο που την διαφοροποιεί από την κλασική και καθιερωμένη λειτουργία του διαδικτύου.

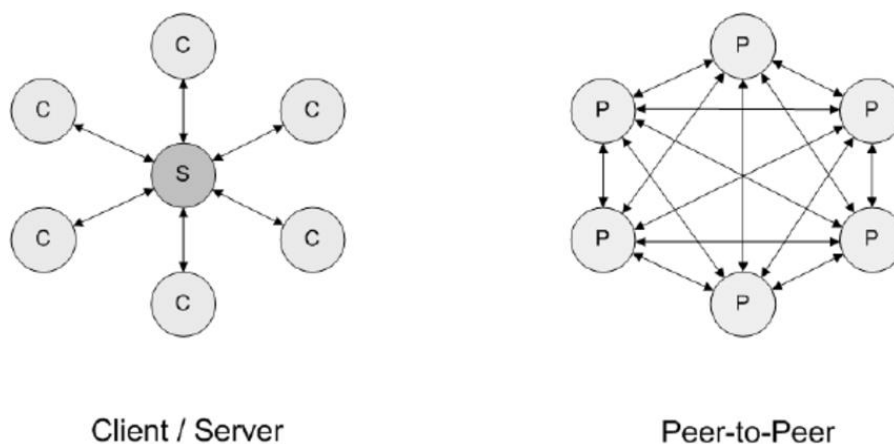
Με λίγα λόγια, με το πέρασμα των χρόνων ο ρόλος του σκοτεινού διαδικτύου άρχισε να αλλάζει και να πραγματοποιούνται μέσω αυτού λαθραίες διαδικτυακές δραστηριότητες, από τη ανταλλαγή αρχείων μικρού μεγέθους μέχρι πολύ επιλεκτικές κλειστές διαδικτυακές λέσχες, απροσπέλαστες βάσεις δεδομένων, καθώς και εγκλήματα και οργανωμένη τρομοκρατία στον κυβερνοχώρο. Επειδή ο βασικός σκοπός ενός σκοτεινού διαδικτύου είναι να δημιουργεί κλειστά δίκτυα που επιτρέπουν την ασφαλή επικοινωνία με τέτοιο τρόπο που αποτρέπεται ο εντοπισμός και η διείσδυση μιας αρχής όπως ένα κράτος ή μια μεγάλη εταιρεία, τα άτομα που το χρησιμοποιούν είναι σε θέση να κατεβάζουν και να ανεβάζουν υλικό από το ίντερνετ με ανώνυμο τρόπο, καθιστώντας πρακτικά αδύνατο στους ξένους ως προς δίκτυο αυτό, να αναγνωρίσουν τους χρήστες ή το περιεχόμενο του υλικού που διακινούν.

Αναλύοντας περισσότερο τα χαρακτηριστικά του διαδικτύου από το σκοτεινό διαδίκτυο που χρησιμοποιεί δίκτυα P2P (peer-to-peer) να αναφέρουμε πως οι συνδεδεμένοι υπολογιστές στο διαδίκτυο επικοινωνούν μεταξύ τους μέσω διακομιστών χρησιμοποιώντας βασικά πρωτόκολλα διαδικτυακής επικοινωνίας. Τα πρωτόκολλα αυτά δηλαδή οι διευθύνσεις Πρωτόκολλου Διαδικτύου (IP: Internet Protocol), αντιστοιχούν σε έναν υπολογιστή και μπορούν να αντιστοιχιστούν σε αναγνωρίσιμες διευθύνσεις όπως είναι το «www.google.com». Με βάση τον τρόπο λειτουργίας τους, τα δεδομένων των πολυμέσων και τα άλλα είδη περιεχομένου είναι αποθηκευμένα σε κεντρικούς διακομιστές (hosts), τα οποία ικανοποιούν μια σχέση μεταξύ πελάτη/διακομιστή (client/server relationship). Ουσιαστικά με το σύστημα αυτό ο χρήστης, δηλαδή ο πελάτης, μπορεί μόνο να έχει πρόσβαση σε πληροφοριακό υλικό μέσω ιστοσελίδων που χρησιμοποιούν το διαδίκτυο και όχι απευθείας με άλλους χρήστες/ πελάτες. Αυτό που συμβαίνει σε αντίθετη μεριά με το δίκτυο P2P είναι πως επιτρέπει σε έναν υπολογιστή συνδεδεμένο στο διαδίκτυο να



είναι ταυτόχρονα και πελάτης και διακομιστής, επιτρέποντάς του με αυτόν τον τρόπο να ανταλλάσσει απευθείας αρχεία με οποιονδήποτε υπολογιστή συνδεδεμένο στο διαδίκτυο. Όλοι οι τύποι δικτύων P2P μοντέλων εντάσσονται στην κατηγορία των αποκεντροποιημένων δικτύων, αφού κανένας κεντρικός διακομιστής δεν αποθηκεύει τα αρχεία. Στην εικόνα 1.3.1 που έπεται στην συνέχεια μπορούμε να κατανοήσουμε μέσω διαγραμμάτων την διαφορά μεταξύ των κλασικού διαδικτύου και του P2P δικτύου.

**Εικόνα 1.3.1:** Σχέση δικτύου πελάτη διακομιστή σε σχέση με την P2Pσυνδεση



Πηγή: BiegM.,Wikimedia. org

Στο αριστερό μέρος της εικόνας παρουσιάζεται ένα δίκτυο που βασίζεται στο μοντέλο πελάτη-διακομιστή, στο οποίο ο κάθε πελάτης ζητάει υπηρεσίες και πόρους από κεντρικούς διακομιστές. Ενώ στο δεξί μέρος μπορούμε να παρατηρήσουμε ένα peer-to-peer (P2P) δίκτυο, στο οποίο οι συνδεδεμένοι κόμβοι (peers) μοιράζονται πόρους μεταξύ τους χωρίς τη χρήση κεντρικού διοικητικού συστήματος- διακομιστή.

Ένα από τα πρώτα παράδειγμα που αποδεικνύουν πως χρησιμοποιήθηκε το Darknet από πολλούς ανθρώπους ελεύθερα ανά τον κόσμο είναι η περίπτωση του Limewire (hypebot.com, 2009).

Ο ιστότοπος Limewire χρησιμοποιήθηκε στο Darknet από πολλούς ανθρώπους ελεύθερα ανά τον κόσμο. Το συγκεκριμένο έργο εμφανίστηκε το 2000, αλλά βασικό του μειονέκτημα ήταν το γεγονός πως ήταν πολύ αργό, δύσκολο στη χρήση του και προσέφερε αρκετά περιορισμένο περιεχόμενο. Ο δημιουργός του Ian Clarke που ήταν Ιρλανδός προγραμματιστής υποστήριζε ότι βασικός του στόχος για

την δημιουργία αυτού του σκοτεινού δικτύου ήταν η προστασία των ατόμων που αντιστέκονταν και εξέφραζαν την γνώμη τους και την άποψη τους ενάντια στα καταπιεστικά καθεστώτα. Αυτό που αναφέρεται χαρακτηρίστηκε ήταν πως χωρίς ανωνυμία, δεν θα υπήρχε ποτέ ελευθερία του λόγου, και χωρίς την χρήση αποκεντροποιημένων δικτύων οι επιθέσεις στον κυβερνοχώρο θα ήταν ιδιαίτερα συχνές και εμφανείς. Μία βασική εξέλιξη ήταν η επεκτασιμότητα του, καθώς μέσω του λογισμικού του λογισμικού του επέτρεπε στους χρήστες να ορίζουν το όριο των άλλων χρηστών με τους οποίους επικοινωνούσαν σε αντίθεση με τα κλασικά δίκτυα P2P. Στα θετικά του στοιχεία είναι πως το λογισμικό του επέτρεπε σε τρίτους να γνωρίσουν τι κάνουν οι χρήστες του, ενώ ήταν σχεδόν αδύνατο οι «αντίπαλοι» να γνωρίζουν ότι ένας χρήστης χρησιμοποιεί το λογισμικό του, έχοντας την δυνατότητα να μπορεί να εντοπίσει την ταυτότητα ενός χρήστη που ανεβάζει ή κατεβάζει περιεχόμενο. (Rocic, 2013)

Επειδή αρχικά η σχεδίαση του σκοτεινού διαδικτύου προορίζονταν για έμπειρους χρήστες, με την πάροδο των χρόνων με την βελτίωση του σχεδιασμού της γραφικής διεπαφής του χρήστη (User Interface Design), το σκοτεινό διαδίκτυο έγινε προσβάσιμο για το ευρύ κοινό. Ένα ιδιαίτερα γνωστό χαρακτηριστικό του παράδειγμα είναι το πρόγραμμα LimeWire 5.1, το οποίο επέτρεπε στους χρήστες να δημιουργού ιδιωτικά δίκτυα διακίνησης αρχείων. Ήταν ιδιαίτερα φιλικό προς τον χρήστη και έδινε την δυνατότητα ελέγχου στους χρήστες του βαθμού κοινοποίησης των αρχείων. Μια ρύθμιση που διέθετε το LimeWire 5.1 ήταν η επιλογή να μην μοιράζεται έγγραφα με δημόσιο peer-to-peer δίκτυο και να μην μοιράζεται πληροφορίες με τρίτους εκτός του δικτύου του χρήστη, καθιστώντας δύσκολη ή αδύνατη την ανίχνευση της δραστηριότητας στα δίκτυα των χρηστών. (Rocic, 2013)

Παρά το γεγονός πως το Dropbox ή το RapidShare αποτελούσαν ιδιαίτερα γνωστές εφαρμογές διαμοιρασμού δεδομένων, το LimeWire 5.1 έκανε την πρόσβαση στο σκοτεινό διαδίκτυο διαθέσιμη σε εκείνους που είχαν περιορισμένες τεχνικές γνώσεις και καμία οικειότητα με τα ήδη υπάρχοντα συστήματα του.

Ένα πάρα πολύ σημαντικό χαρακτηριστικό που έκανε το Limewire να ξεχωρίζει ήταν η ιδιωτική ανταλλαγή αρχείων κάθε μεγέθους χωρίς καμία χρέωση μεταφέροντας υλικό απευθείας από υπολογιστή σε υπολογιστή. Αυτό ήταν ιδιαίτερα επαναστατικό για την εποχή καθώς κατήργησε τους παλαιότερους περιορισμούς στο μέγεθος των αρχείων που έθετε και θέτει για παράδειγμα το ηλεκτρονικό ταχυδρομείο αλλά και άλλες υπηρεσίες ανταλλαγής αρχείων.

## 1.5 Συμπεράσματα πρώτου κεφαλαίου

Μπορεί η δημιουργία του Blockchain να οφείλεται στο Bitcoin, το οποίο είναι το πιο γνωστό κρυπτονομίσμα στην σημερινή εποχή, όμως το Blockchainεμπερικλείει επίσης πολλές εφαρμογές εκτός από αυτό και τα κρυπτονομίσματαγενικότερα.Οι πιο γνωστές εφαρμογές του Blockchain είναι η μεταφορά χρημάτων, η διευθέτηση συναλλαγών, η διενέργεια ψηφοφοριών, αλλά και διάφορες άλλες περιπτώσεις στις οποίες έχει σημείο εφαρμογής.

Μερικά από τα πλεονεκτήματα του Blockchainείναι πως αυξάνει την διαφάνεια στις συναλλαγές, συμβάλλει στην παρακολούθηση με ακρίβεια των διαδικασιών που μπορεί να ακολουθούν οι επιχειρήσεις μειώνοντας το κόστος αυτών, ενώ μερικά από τα μειονεκτήματα του θα μπορούσαμε να πούμε πως είναι η έλλειψη ρυθμιστικού πλαισίου από τις κεντρικές κυβερνητικές αρχές, η περίπλοκη και αρκετά νεοφυής τεχνολογία που χρησιμοποιεί.

Τακρυπτονομίσματα είναι ένα μέσο συναλλαγών όπως το Αμερικάνικο δολάριο ή όπως το Ευρώ, αλλά έχουν ψηφιακή μορφή και υπόσταση, χρησιμοποιούν τεχνικές κρυπτογράφησης για τον έλεγχο της δημιουργίας αυτών των νομισματικών μονάδων αλλά και για την επαλήθευση της μεταφοράς των χρημάτων μεταξύ των αντισυμβαλλόμενων ατόμων. Οι συναλλαγές μεταδίδονται μέσα από ένα peer-to-peer (P2P) δίκτυο, το οποίο αποτελείται από υπολογιστές που ονομάζονται κόμβοι. Το δίκτυο αυτό των κόμβων επικυρώνει τη συναλλαγή η οποία μπορεί να περιλαμβάνει κρυπτονομίσματα, έξυπνα συμβόλαια, αρχεία, αλλά και άλλου είδους πληροφορίες.

Όσον αφορά το σκοτεινό διαδίκτυο το οποίο στην αγγλική γλώσσα ονομάζεται Darknet ή Darkweb,η εμφάνιση τουέγινε πρώτα απ' όλα γνωστή στην δεκαετία του 1970 και αυτός να ήταν ένας όρος που χρησιμοποιήθηκε για τα ιδιωτικά δίκτυα που είχαν υψηλό επίπεδο ιδιωτικότητας, ενώ στα τέλη της δεκαετίας του 1990, δύο ερευνητικοί οργανισμοί στο Υπουργείο Άμυνας των ΗΠΑ έκαναν προσπάθειες για την ανάπτυξη ενός ανώνυμου και κρυπτογραφημένου δικτύου που θα προστάτευε τις επικοινωνίες που πραγματοποιούσαν οι Αμερικάνικοι κατάσκοποι. Αυτό το μυστικό δίκτυο δεν θα ήταν γνωστό ή προσβάσιμο σε συνηθισμένους χρήστες του διαδικτύου και με το πέρασμα των χρόνων μετατράπηκε σε καταφύγιο για την επικοινωνία και τον προγραμματισμό εγκληματικών δραστηριοτήτων και αυτό γιατί διευκόλυνε το εμπόριο παράνομων προϊόντων όπως ναρκωτικά και όπλα και τα κρυπτονομίσματα, ειδικά το Bitcoin, να γίνονται το νόμισμα επιλογής για τις συναλλαγές αυτές.

## **Κεφάλαιο 2:Κρυπτονομίσματα και σκοτεινό διαδίκτυο**

### **2.1 Εισαγωγή δευτέρου κεφαλαίου**

Το δεύτερο κεφάλαιο της διπλωματικής εργασίας επικεντρώνεται στην ανάλυση της χρήσης των κρυπτονομισμάτων και ιδιαίτερα του Bitcoin στο σκοτεινό διαδίκτυο. Εξετάζονται ποια κρυπτονομίσματα προτιμώνται σε μεγαλύτερο βαθμό τόσο από τους αγοραστές όσο και από τους πωλητές παράνομων προϊόντων στο Dark Web, καθώς και ποιος είναι πλέον ο ρόλος των τα altcoins, τα οποία αποτελούν μια νέα τεχνολογική κατηγορία κρυπτονομισμάτων.

Επίσης στο κεφάλαιο αυτό αναλύονται μέσω στατιστικών στοιχείων η συνολική αξία των συναλλαγών που πραγματοποιήθηκαν εντός του σκοτεινού διαδικτύου από το 2017 μέχρι τα πλέον πρόσφατα διαθέσιμα στοιχεία, ενώ επίσης αναλύονται και οι λόγοι προτίμησης αλλά και αποθάρρυνσης της χρήσης των κρυπτονομισμάτων για συναλλαγές στο σκοτεινό διαδίκτυο μέσω μιας σειράς παραδειγμάτων για κάθε μια κατηγορία.

## 2.2 Το Bitcoin και η χρήση του στο σκοτεινό διαδίκτυο

Γεγονός είναι πως για τους περισσότερους ανθρώπους μόλις γίνεται αναφορά στο Bitcoin, δύο λέξεις χαράσσονται στο μυαλό τους, το Silk Road. Το Silk Road ήταν η πρώτη σκοτεινή αγορά και έγινε διαβόητη για τη δυνατότητα που έδινε στους ανθρώπους να πωλούν ναρκωτικά και άλλα παράνομα είδη στο διαδίκτυο.

Οι σκοτεινές αγορές δεν είναι απαραίτητα παράνομες και δεν συνδέονται πάντα με εγκληματικές δραστηριότητες. Είναι απλά ψηφιακές αγορές που δημιουργούνται χρησιμοποιώντας την τεχνολογία που υποστηρίζει την λειτουργία του Bitcoin και συνήθως αποδέχονται το Bitcoin ως μέθοδο πληρωμής λόγω των σχεδόν ανώνυμων χαρακτηριστικών του. Όμως οι σκοτεινές αγορές απέκτησαν παράνομο χαρακτήρα λόγω των προϊόντων που επιτρέπονταν να πωλούνται σε αυτές. Συνεπώς όταν μια ψηφιακή αγορά επιτρέπει τη διακίνηση ναρκωτικών, όπλων ή άλλων παράνομων αντικειμένων, τότε παραβιάζει το νόμο και οι αρχές επιβολής του νόμου χρειάζεται να επέλθουν, οπότε αποκτούν παράνομο χαρακτήρα. (Bradbury D., 2020).

Επίσης επικρατεί ακόμη η άποψη ότι το Bitcoin και άλλα κρυπτονομίσματα χρησιμοποιούνται μόνο για εγκληματικούς σκοπούς. Αναμφίβολα, το Bitcoin βοήθησε στη αύξηση της οικονομικής δραστηριότητας εντός του darknet ιδιαίτερα στο Silk Road, όμως σύμφωνα με ειδικούς του Chainalysis.com ιδιαίτερα μετά το 2019 μπορεί οι συναλλαγές στο σκοτεινό διαδίκτυο να γνώρισαν μεγάλη ακμή, όμως πλέον έχουν αρκετά περιοριστεί καθώς τα κρυπτονομίσματα υπόκεινται σε απότομες διακυμάνσεις στην τιμή, η οποία επηρεάζει τη χρήση τους στο darknet. Γεγονός είναι πως οι πωλητές παράνομων προϊόντων μείωσαν τη δραστηριότητά τους κατά τη διάρκεια περιόδων μείωσης της τιμής Bitcoin, φοβούμενοι ότι τα χρήματα που δέχονται ενδέχεται να απωλέσουν την αξία τους. Παρ' όλα αυτά, οι ειδικοί συμφωνούν ότι ανεξάρτητα από την τιμή που έχουν σε γενικές γραμμές τα κρυπτονομίσματα, θα εξακολουθούν να είναι δημοφιλή στο σκοτεινό διαδίκτυο.

Επίσης επειδή σύμφωνα με τον Harper C. (2020), το Bitcoin είναι διαθέσιμο σε οποιονδήποτε στον κόσμο να το χρησιμοποιήσει, αυτό συνεπάγεται πως ένα μέρος των χρηστών του μπορεί να το χρησιμοποιήσει για νόμιμες συναλλαγές, ενώ ένα άλλο μπορεί να το χρησιμοποιήσει για κακόβουλες και εγκληματικές δραστηριότητες. Δυστυχώς, παρά το γεγονός πως το ποσό των Bitcoin που αποστέλλονται και λαμβάνονται από χρήστες του σκοτεινού διαδικτύου έχει μειωθεί από το 2017, η συνολική αξία που ανταλλάχθηκε (σε USD) συνεχίζει να αυξάνεται.

Ανησυχητικό είναι επίσης πως οι χρήστες αυτοί συνεχίζουν να αυξάνουν την ποσότητα του Bitcoin που αντιστοιχεί σε πραγματική χρηματική αξία που αποστέλλονται μεταξύ τους. Αυτά τα στατιστικά στοιχεία δείχνουν ότι το Bitcoin εξακολουθεί να αποτελεί οικονομικό εργαλείο για οντότητες του darknet. Αυτό όμως που είναι καθησυχαστικό, είναι πως πλέον οι δραστηριότητες στο σκοτεινό διαδίκτυο είναι πιο εύκολο να εντοπίζονται και να καταστέλλονται σύμφωνα με κανόνες που θεσπίστηκαν από το Financial Action Task Force (FATF) και την Ευρωπαϊκή Ένωση με απώτερο σκοπό την καταπολέμηση αυτών των παράνομων δραστηριοτήτων

Σύμφωνα με τον Fridi O. (2020), το Bitcoin (BTC) παραμένει ένα ευρέως χρησιμοποιούμενο κρυπτονόμισμα για συναλλαγές στο σκοτεινό διαδίκτυο, με βάση μια νέα έρευνα της Rand Corporation (Research And Development), μιας αμερικανικής μη κερδοσκοπικής παγκόσμιας ομάδας. Η συγκεκριμένη ομάδα ατόμων χρηματοδοτείται από την Αμερικανική κυβέρνηση (και ιδιωτικές εταιρείες, πανεπιστήμια και ιδιώτες) και ισχυρίζεται ότι το Bitcoin (BTC), που είναι το κυρίαρχο κρυπτονόμισμα, χρησιμοποιείται για τη διεξαγωγή ενός σχετικά μεγάλου αριθμού συναλλαγών στο σκοτεινό διαδίκτυο.

Στην μελέτη αυτή εξετάστηκαν από την Rand η χρήση των ψηφιακών νομισμάτων προσανατολισμένων στην προστασία της ιδιωτικής ζωής, όπως το Monero (XMR) και το Zcash (ZEC), τα οποία διευκολύνουν τις συναλλαγές στο σκοτεινό διαδίκτυο. Αυτό που αξίζει να αναφερθεί είναι πως η εταιρεία Electric Coin Company, η οποία είναι πίσω από την ανάπτυξη του Zcash, είχε αναθέσει την ερευνητική αυτή μελέτη, η οποία δημοσιεύθηκε στις 6 Μαΐου 2020.

Η έκθεση αναφέρει ότι το Zcash έχει «μόνο μια μικρή παρουσία στο σκοτεινό διαδίκτυο», το οποίο υποδηλώνει ότι μπορεί να θεωρηθεί «λιγότερο ελκυστική επιλογή για χρήστες σκοτεινού διαδικτύου και χρησιμοποιείται λιγότερο συχνά σε σύγκριση με άλλα κρυπτονομίσματα, ιδίως του Bitcoin και του Monero. Αυτό που επισημαίνεται στην έρευνα είναι πως η τεχνολογία των κρυπτονομισμάτων θα πρέπει να εξετάζεται για το πως θα μπορούσε να χρησιμοποιηθεί σε μια μεγάλη ποικιλία εφαρμογών, και στη συνέχεια να εστιάζονται συγκεκριμένες περιπτώσεις όπως στην περίπτωση των παράνομων συναλλαγών. (rand.org,2020)

Επίσης τον Ιανουάριο του 2020, μια κορυφαία εταιρεία blockchain, η Chainalysis ανέφερε ότι εντόπισε 2,8 δισεκατομμύρια δολάρια σε Bitcoin (BTC) που μεταφέρθηκαν μέσα από εγκληματικές δραστηριότητες μέσω ανταλλακτηρίων κρυπτονομισμάτων το έτος 2019. Η εταιρεία ισχυρίστηκε πως οι περισσότερες από αυτές τις συναλλαγές προήλθαν από τα ανταλλακτήρια Binance και Huobi, τα οποία

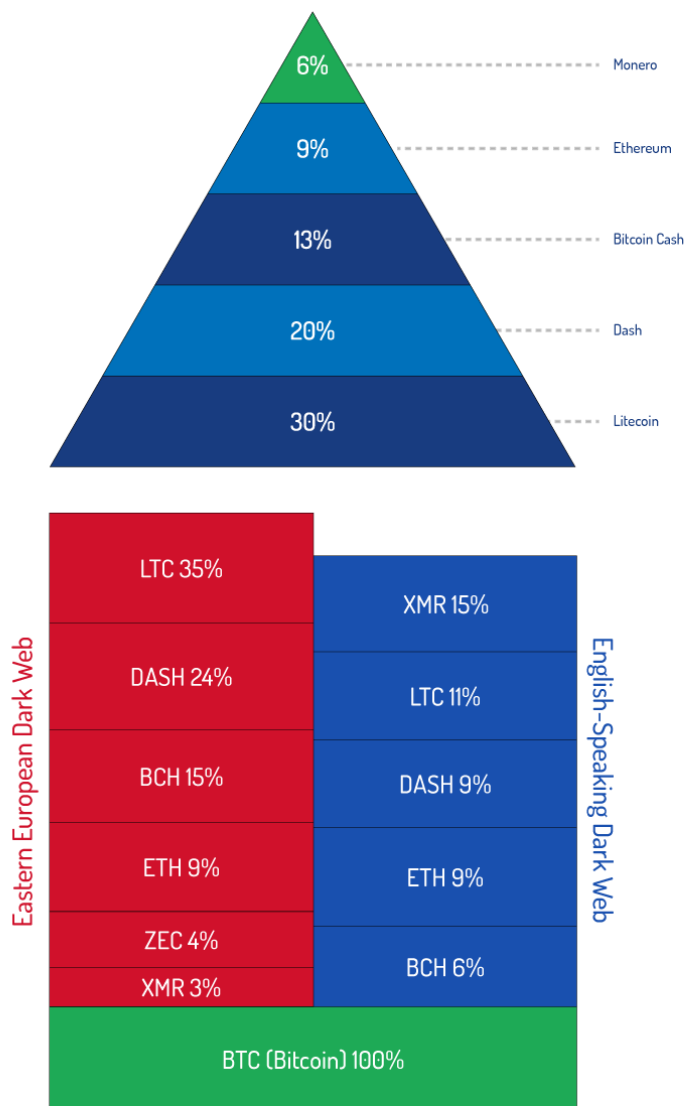
είναι από τις μεγαλύτερες πλατφόρμες συναλλαγών κρυπτονομισμάτων στον κόσμο.  
(Faridi O.,2020)

### **2.3 Τα επικρατέστερα κρυπτονομίσματα εντός του σκοτεινού διαδικτύου**

Όπως αναφέρεται από τον Sharma R. (2019), η ξεπερασμένη τεχνολογία του blockchain του Bitcoin και τα υψηλά κόστη συναλλαγών έχουν φέρει στην επιφάνεια την χρήση άλλων κρυπτονομισμάτων ως μέσο συναλλαγής στο σκοτεινό διαδίκτυο. Με μεγάλη έκπληξη το Litecoin έχει αναδειχθεί ως το δεύτερο πιο δημοφιλές κρυπτονομίσμα για συναλλαγές ηλεκτρονικού εμπορίου. Ενώ σύμφωνα με μια έκθεση του Recorded Future (2018), το Litecoin χρησιμοποιείται από το 30% όλων των πωλητών που χρησιμοποιούν εναλλακτικές μεθόδους πληρωμής. Το Dash, ένα άλλο κρυπτονομίσμα του οποίου το πρωτόκολλο είναι κατάλληλο για καθημερινές συναλλαγές, γίνεται αποδεκτό στο 20% όλων των καταστημάτων στο σκοτεινό διαδίκτυο, με φυσικά το Bitcoin να είναι αποδεκτό σε όλους του ιστότοπους ηλεκτρονικού εμπορίου στο σκοτεινό διαδίκτυο. Στα διάγραμμα 2.1 που ακολουθεί μπορούμε να παρατηρήσουμε την σχετική κατανομή που παρουσιάζουν τα κρυπτονομίσματα

**Διάγραμμα 2.1:** Κρυπτονομίσματα και σκοτεινό διαδίκτυο

## Dark Web Currency



Recorded Future

Στο πάνω μέρος του διαγράμματος 2.1 αυτό που αξίζει να επισημάνουμε είναι πως το Bitcoin παραμένει το νούμερο ένα σε προτίμηση κρυπτονομίσμα από όλους τους πωλητές οι οποίοι το δέχονται ως μέσο πληρωμής, ενώ το Litecoin αναδείχθηκε ως το δεύτερο πιο δημοφιλές κρυπτονομίσμα με αποδοχή της τάξης του 30% , με το Dash να ακολουθεί στενά με ποσοστό 20%. Παραδόξως το Bitcoin Cash ήταν το



τρίτο στην σχετική προτίμηση με ποσοστό 13% από τους πωλητές οι οποίοι το εμπιστεύονται ως μέθοδο πληρωμής.

Αυτό που είναι ιδιαίτερα σημαντικό να εστιάσουμε την προσοχή μας είναι στο κάτω μέρος του διαγράμματος, στο οποίο παρουσιάζεται ότι τα άτομα που προβαίνουν σε αγοροπωλησίες παράνομων προϊόντων της Ανατολικής Ευρώπης είναι πιο προληπτικοί στην εφαρμογή εναλλακτικών επιλογών πληρωμής σε σύγκριση με τις αγγλόφωνες χώρες σε σχέση με το κρυπτονόμισμα που προτιμούν να χρησιμοποιούν. Οι αγγλόφωνες χώρες φαίνεται να είναι περισσότερο προσανατολισμένες στην ασφάλεια, επιλέγοντας το Monero και τα ενσωματωμένα χαρακτηριστικά ασφαλείας του, ενώ οι χώρες της Ανατολικής Ευρώπης προτιμούν περισσότερο το Litecoin μετά το Bitcoin που είναι το κυρίαρχο κρυπτονόμισμα σε αποδοχή.

Ωστόσο, το μερίδιό του Bitcoin στη συνολική αγορά ενδέχεται να μειωθεί στο μέλλον, δεδομένης της θετικής στάσης απέναντι σε άλλα κρυπτονομίσματα από την πλευρά των πωλητών των προϊόντων. Ιδιαίτερα τα κρυπτονομίσματα Dash και Monero, τα οποία έχουν ισχυρά διαπιστευτήρια απορρήτου, δείχνουν να προτιμώνται περισσότερο, ενώ το Bitcoin και το Bitcoin cash έλαβαν την χαμηλότερη προτίμηση. Επίσης να αναφέρουμε πως ο λόγος που άρχισαν να προτιμώνται άλλα κρυπτονομίσματα από τους χρήστες του σκοτεινού διαδικτύου είναι γιατί το Bitcoin έχει αυξημένο κόσμος στις συναλλαγές του, ενώ οι περισσότερες καθημερινές συναλλαγές στο σκοτεινό διαδίκτυο είναι συνήθως μικρές σε χρηματικά ποσά. (Barysevich A, Solad A.,2018)

Ακόμη σύμφωνα με το fortune και τον Roberts J.(2018), το Litecoin είναι δημοφιλές επειδή έχει ταχύτερους χρόνους επεξεργασίας σε σύγκριση με το Bitcoin και μπορεί να αποθηκευτεί σε ψηφιακά πορτοφόλια που είναι εκτός σύνδεσης. Λόγω λοιπόν της φύσης τους τα κρυπτονομίσματα είναι δημοφιλή στο σκοτεινό διαδίκτυο καθώς επιτρέπουν την απόκρυψη της ταυτότητας και διάφορων λεπτομερειών γύρω από τις συναλλαγές. Τον Αύγουστο του 2017, το Bitcoin, το Monero και το Ethereum ήταν τα κρυπτονομίσματα που προτιμώνται περισσότερο από τους χρήστες για την διεξαγωγή συναλλαγών εντός του σκοτεινού διαδικτύου .

Αυτό που έχει ιδιαίτερο ενδιαφέρον να αναφέρουμε είναι πως σύμφωνα με τον Harper C. (2020), σε άρθρο που δημοσίευσε στο forbes.com αναφέρει πως η συνολική δραστηριότητα του Bitcoin στο σκοτεινό διαδίκτυο αυξήθηκε από το έτος 2017 κατά 340%. Αναλυτικότερα, η συνολική αξία του Bitcoin που χρησιμοποιούνταν ως μέσο συναλλαγής στο σκοτεινό διαδίκτυο το 2020 αυξήθηκε κατά 65% και τα

τελευταία τρία χρόνια κατά 340% σύμφωνα με έκθεση της εταιρείας τεχνολογίας Bitcoin Bitfury. (crystalblockchain.com,2020)

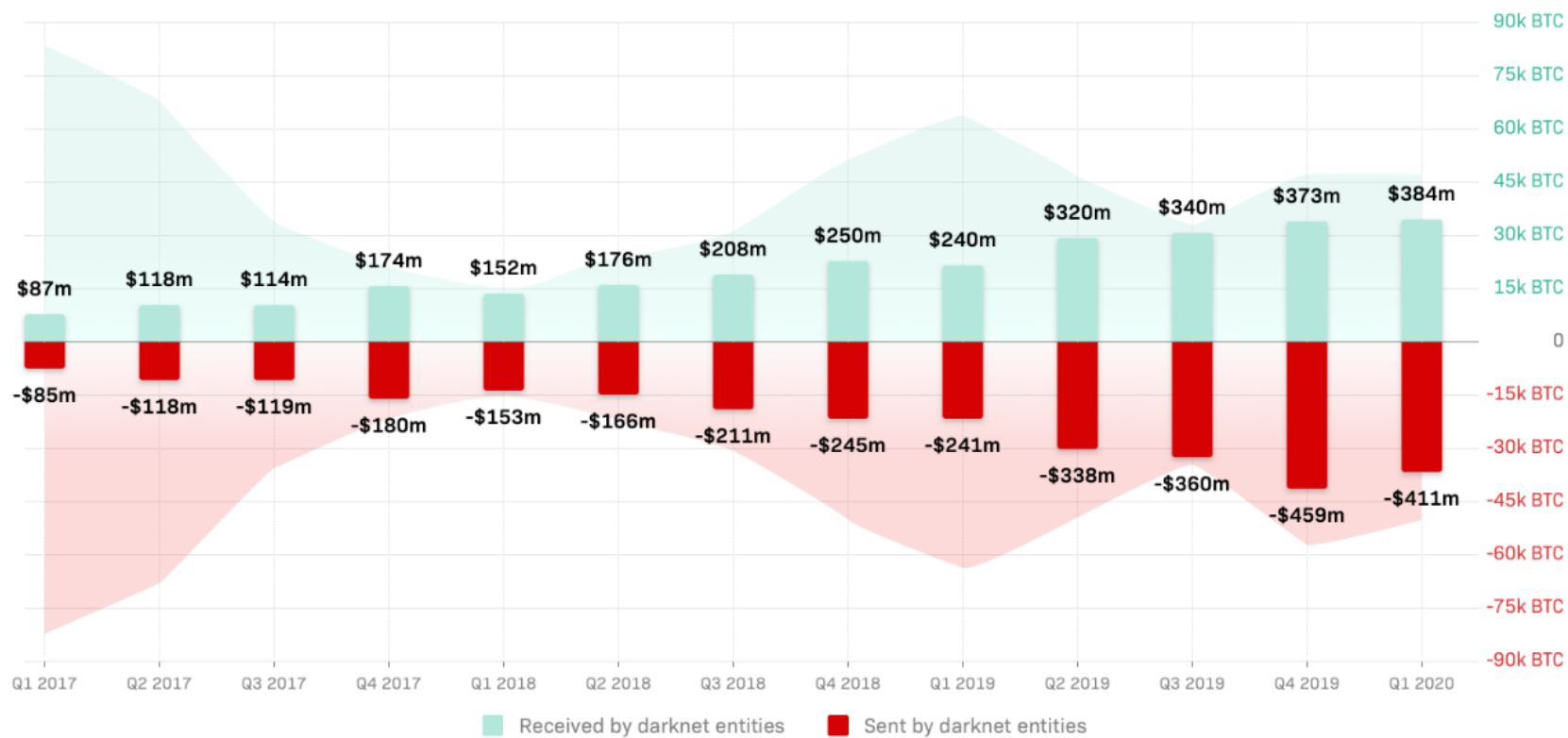
Σύμφωνα με τα δεδομένα που αναλύθηκαν από την πλατφόρμα blockchain της εταιρείας Bitfury's Crystal το πρώτο τρίμηνο του 2019 οι χρήστες του σκοτεινού διαδικτύου συγκέντρωσαν σωρευτικά 240 εκατομμύρια δολάρια σε Bitcoin από τα 87 εκατομμύρια δολάρια που είχαν συγκεντρώσει το πρώτο τρίμηνο του 2017. Ο αριθμός αυτός έχει αυξηθεί ακόμη περισσότερο το 2020 φτάνοντας τα 384 εκατομμύρια δολάρια, φανερώνοντάς μας πως οι σκοτεινές αυτές αγορές συνεχίζουν να χρησιμοποιούν τα ψηφιακά νομίσματα παρά το γεγονός πως πλέον οι παρεμβάσεις από τις κυβερνητικές αρχές είναι αρκετές για την καταστολή των παράνομων αυτών δραστηριοτήτων αλλά και πως το Bitcoin δείχνει πως ελαφρώς υποχωρεί στην χρήση του.

Αναλυτικότερα οι προμηθευτές του σκοτεινού διαδικτύου έλαβαν 47.000 Bitcoin το πρώτο τρίμηνο του 2020, το οποίο βέβαια είναι κατά 25% πιο κάτω σε αριθμό Bitcoin σε σχέση με το αντίστοιχο διάστημα του προηγούμενου έτους. Το γεγονός αυτό μας οδηγεί στο συμπέρασμα πως οι χρήστες του σκοτεινού διαδικτύου προτιμούν άλλα κρυπτονομίσματα, τα λεγόμενα altcoins όπως το Monero και το Litecoin όπως αναφέρθηκε και προηγουμένως. Αυτό βέβαια που αξίζει να τονίσουμε είναι πως η συνολική αξία των συναλλαγών στο σκοτεινό διαδίκτυο παρόλα αυτά αυξάνεται επειδή η τιμή του Bitcoin αυξάνεται.

**Διάγραμμα 2.2:** Η αξία των συναλλαγών που πραγματοποιήθηκαν σε σκοτεινές αγορές



General Analysis of Darknet Entity Interactions Q1 2017 – Q1 2020



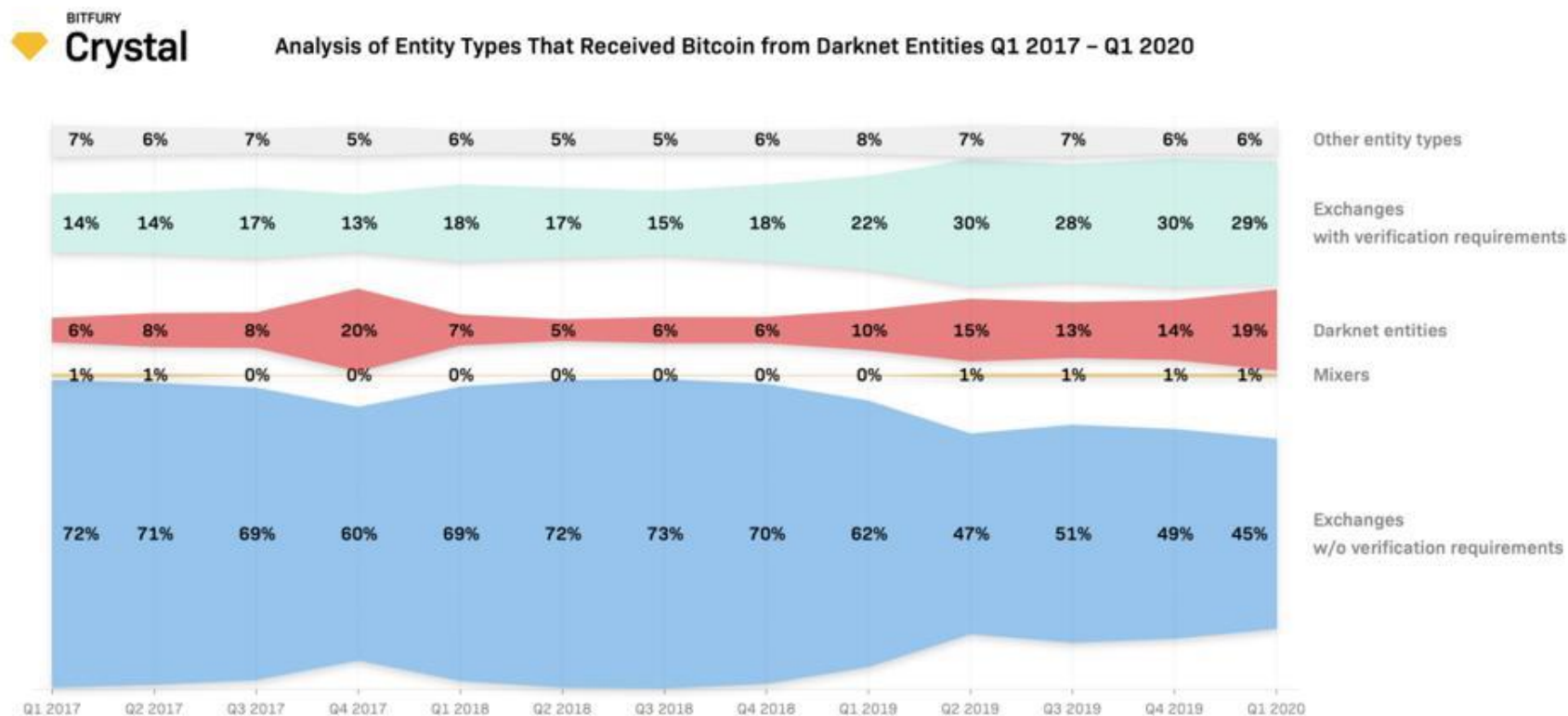
Πηγή:medium.com

(2020)

Παρατηρώντας το Διάγραμμα 2.2 μπορούμε να δούμε την σχέση μεταξύ του ποσού των Bitcoin που έχουν σταλεί και έχουν ληφθεί από άτομα μέσα στο σκοτεινό διαδίκτυο, από το πρώτο τρίμηνο του 2017 μέχρι το πρώτο τρίμηνο του 2020. Αυτό που παρατηρείται είναι πως για παράδειγμα, το 4ο τρίμηνο του 2017, τα συνολικά Bitcoin που στάλθηκαν από χρήστες του σκοτεινού διαδικτύου ήταν 180 εκατομμύρια Αμερικάνικα δολάρια, ενώ εκείνα που ελήφθησαν ήταν 174 εκατομμύρια Αμερικάνικα δολάρια. Παρατηρώντας και πάλι το διάγραμμα 2.2 μπορούμε να δούμε πως τα αντίστοιχα νούμερα για το πρώτο τρίμηνο του 2020 είναι παραπάνω από διπλάσια, καθώς στάλθηκαν 411 εκατ. Αμερικάνικα δολάρια σε Bitcoin ενώ οι χρήστες έλαβαν 384 εκατ. δολάρια.

Παρά το γεγονός πως το Bitcoin χάνει κάποια μερίδια από άλλα altcoins, εξακολουθεί να είναι το κυρίαρχο νόμισμα στο σκοτεινό διαδίκτυο. Μια πολύ ενδιαφέρουσα παρατήρηση είναι πως τα χρήματα που αποστέλλονται μεταξύ των αγορών του ιδίου του σκοτεινού διαδικτύου έχουν αυξητική τάση, γεγονός που φανερώνει ότι οι χρήστες του darknet προσπαθούν να κρύψουν τη ροή και τις συναλλαγές που πραγματοποιούν με Bitcoin μέσα από το ίδιο το σκοτεινό διαδίκτυο.

**Διάγραμμα 2.3:** Η κατανομή της προέλευσης του Bitcoin πριν αποσταλεί μέσα σκοτεινό διαδίκτυο.



Πηγή:medium.com.

(2020)

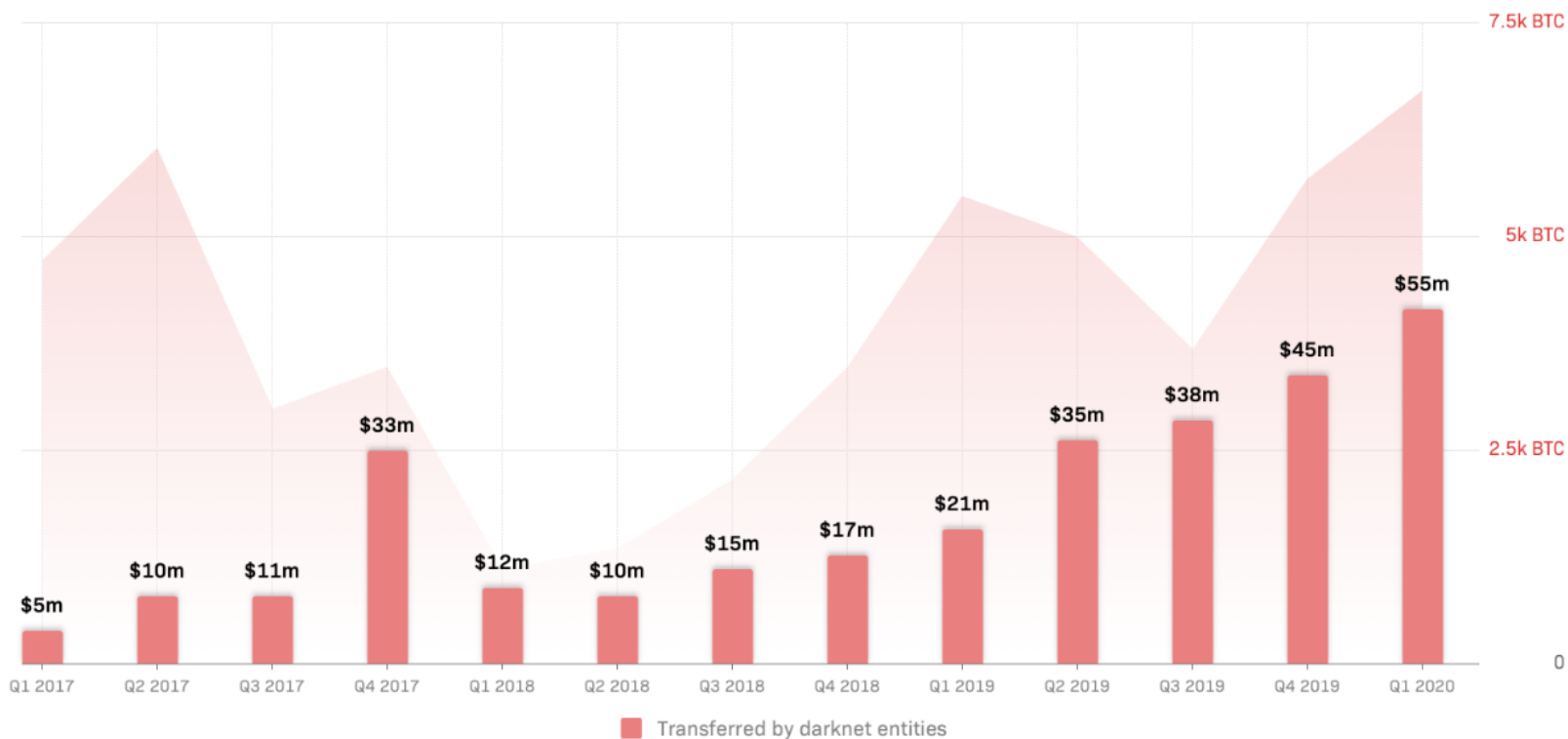
Σύμφωνα με το διάγραμμα 2.3 γίνεται κατανοητό πως οι χρήστες του σκοτεινού διαδικτύου ζητούν συχνά και χρησιμοποιούν ανταλλαγές χωρίς αυστηρές απαιτήσεις επαλήθευσης. Ενώ αυτό που είναι άξιο παρατήρησης είναι πως το μερίδιο των Bitcoin που λάμβαναν όλα τα άτομα μέσα στο σκοτεινό διαδίκτυο μειώθηκε από 62% το πρώτο τρίμηνο του 2019 σε 45% το πρώτο τρίμηνο του 2020.

Ακόμη στο διάγραμμα 2.4 που ακολουθεί μπορούμε να παρατηρήσουμε την αύξηση του bitcoin (κατά αξία σε USD) που μεταφέρεται μεταξύ των διάφορων χρηστών του σκοτεινού διαδικτύου. Είναι φανερό πως το 4ο τρίμηνο του 2017, ποσό αξίας 33 εκατομμυρίων δολαρίων σε Bitcoin μεταφέρθηκαν μεταξύ οντοτήτων στο darknet, με το συγκεκριμένο αριθμό να ακολουθεί πτωτική πορεία αλλά από το δεύτερο τρίμηνο του 2019 να ξεπερνάει το ιστορικό του υψηλό και τα φτάνει τα 35 εκατομμύρια, ενώ στο πρώτο τρίμηνο του 2020 έφτασε τα 55 εκατομμύρια πραγματοποιώντας μια άνοδο της τάξης του 161% από έτος σε έτος.

**Διάγραμμα 2.4:** Η αξία του Bitcoin που μεταφέρεται μεταξύ των διάφορων χρηστών του σκοτεινού διαδικτύου (εκατ. δολάρια ΗΠΑ)



Darknet Interactions with Other Darknet Q1 2017 - Q1 2020



Πηγή:medium.com.

(2020)

## 2.4 Οι λόγοι προτίμησης αλλά και αποθάρρυνσης της χρήσης των κρυπτονομισμάτων στο σκοτεινό διαδίκτυο

Στο σημείο αυτό της διπλωματικής εργασίας παρουσιάζονται στην συνέχεια μερικοί από τους λόγους για τους οποίους τα κρυπτονομίσματα προτιμώνται αλλά και αποθαρρύνουν τους χρήστες τους να τα χρησιμοποιήσουν εντός του σκοτεινού διαδικτύου.

Αρχικά να αναφέρουμε πως το Blockchain αποτελεί την βασική τεχνολογία πίσω από τα κρυπτονομίσματα και προσφέρει αποκεντροποιημένες συναλλαγές και θεωρείται το θεμέλιο των κρυπτονομισμάτων με αποτέλεσμα όπως αναφέρεται και στο [hackernoon.com](http://hackernoon.com) (2018) η ανωνυμία είναι ένας από τους βασικότερους λόγους προτίμησης. Το να είναι σε θέση κάποιο άτομο να εκτελεί συναλλαγές χωρίς να φαίνεται είναι ιδιαίτερα σημαντικό στον χώρο του σκοτεινού διαδικτύου. Εκτός από το Bitcoin, κρυπτονομίσματα όπως το Monero δεν μπορούν να εντοπιστούν εύκολα, αποκρύπτοντας τις διευθύνσεις που προέρχονται οι συναλλαγές. Αυτές οι διευθύνσεις μπορεί να είναι ανιχνεύσιμες αλλά δεν μπορούν να εντοπίσουν τον αρχικό κάτοχο τους.

Επίσης το κομμάτι της ασφάλειας που προσφέρουν. Επειδή οι παράνομες συναλλαγές όπως η πώληση παιδικής πορνογραφίας αλλά και η αγορά παράνομων ουσιών όπως ναρκωτικών είναι αρκετά δαπανηρές για χρηματοδότηση και δεν επιτρέπονται καθυστερήσεις, οι έμποροι θέλουν ένα ασφαλές και αξιόπιστο μέσο για να πάρουν τα χρήματά. Το μέσο αυτό είναι τα κρυπτονομίσματα καθώς μπορούν να το επιτρέψουν χωρίς να ελέγχονται από κάποια κυβέρνηση ή κεντρική αρχή.

Ακόμη σύμφωνα με μια Αυστραλιανή μελέτη του έτους 2018 αναφέρθηκε πως το 47% των συναλλαγών που αφορούν το Bitcoin πραγματοποιούνται στον σκοτεινό διαδίκτυο. Αυτό μας δείχνει πως σχεδόν η μισή χρήση του αφιερώνεται στην ικανοποίηση των επιθυμιών των ατόμων που πραγματοποιούσαν παράνομες δραστηριότητες και το άλλο μισό στα άτομα που ήθελαν να το αξιοποιήσουν με άλλο τρόπο όπως για κερδοσκοπικές δραστηριότητες.

Επιπρόσθετα, όταν εμφανίστηκε το Bitcoin, υποσχέθηκε πλήρη ανωνυμία και αυτό έκανε την παγκόσμια κοινότητα να το αγκαλιάσει. Το ίδιο συνέβη και με άλλα κρυπτονομίσματα τα λεγόμενα altcoins. Αυτά τα altcoins επεξεργάζονται συναλλαγές γρηγορότερα, είναι πιο αξιόπιστα και υποστηρίζουν σε μεγαλύτερο βαθμό την ανωνυμία.

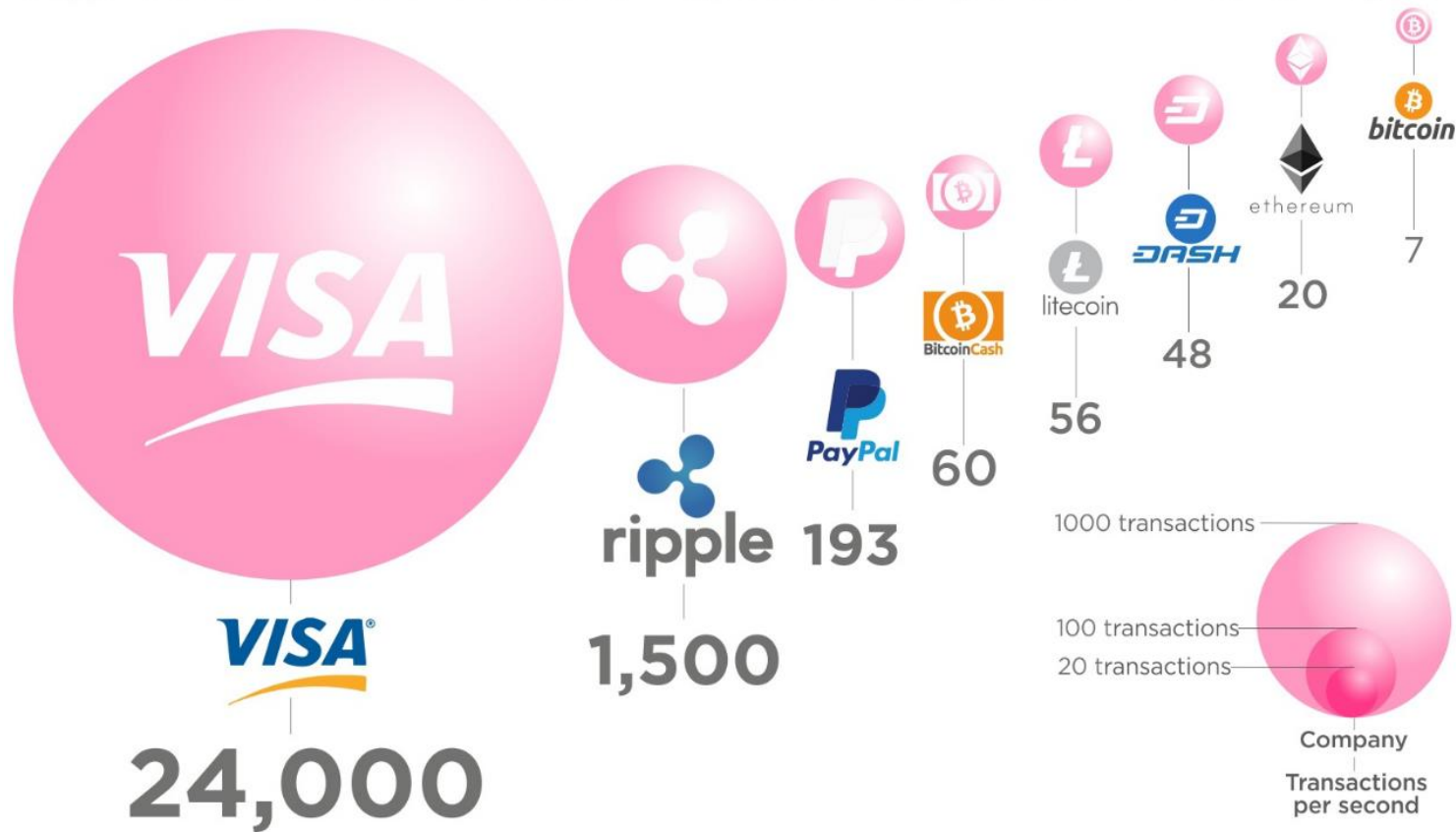


Αντίθετα ένας λόγος που αποθαρρύνει την χρήση τους στο Dark Web είναι η υψηλή αξία τους. Κανείς δεν θέλει να ξοδέψει 40.000 \$ για 1 BTC, ή να αγοράσει κάποιο άλλο κρυπτονόμισμα με υψηλή αξία. Το υψηλό κόστος κτήσης των κρυπτονομισμάτων όπως του Bitcoin και του Ethereum οδηγεί τους ανθρώπους στο να μην μπορούν να κάνουν συναλλαγές σε τόσο υψηλές τιμές. Παρομοίως, τα άτομα δεν είναι πρόθυμα να ανταλλάξουν τα altcoins τους σε χαμηλό ποσό προς το παρόν, επειδή πιστεύουν ότι πρόκειται να ανέβουν υψηλότερα στο μέλλον.

Ένα άλλο μειονέκτημα είναι η ταχύτητα των συναλλαγών. Τους τελευταίους μήνες, το Bitcoin σημείωσε δραστική μείωση της δραστηριότητας στο σκοτεινό διαδίκτυο. Παρόλο που πολλοί αποδίδουν αυτό στην αύξηση της τιμής του, αυτό οφείλεται επίσης στο γεγονός ότι οι συναλλαγές στο δίκτυο blockchain έγιναν εξαιρετικά αργές. Αυτό δικαιολογείται εν μέρη και στην αύξηση της δημοτικότητας του Bitcoin ως κρυπτονόμισμα αλλά ως αναλογιστούμε και έναν χρήστη ναρκωτικών που θέλει να αγοράσει ναρκωτικά γρήγορα. Ένα τέτοιο άτομο δεν μπορεί να περιμένει την εκκαθάριση των συναλλαγών στο δίκτυο και συνήθως θα αναζητήσει κάποια πιο γρήγορη διαθέσιμη επιλογή. Να αναφέρουμε πως κάποια στιγμή στο έτος 2018, ο αριθμός των μη επιβεβαιωμένων συναλλαγών στο Bitcoin ανήλθε σχεδόν σε 60.000, ενώ σε μια πολύ επιβαρυσμένη μέρα μπορεί να φτάσει και τις 150.000. Σύμφωνα και με την εικόνα 3.1 που ακολουθεί στην συνέχεια μπορούμε να παρατηρήσουμε την ταχύτητα των συναλλαγών ανά δευτερόλεπτο που μπορούν να πραγματοποιηθούν τόσο με παραδοσιακούς τρόπους πληρωμής όπως είναι η Visa, το Paypal, όσο και με κρυπτονομίσματα όπως είναι το Bitcoin, το XRP, το Litecoin.

**Εικόνα 2.1:** Ο αριθμός των συναλλαγών ανά δευτερόλεπτο μεταξύ γνωστών μέσων πληρωμών και κρυπτονομισμάτων

### Cryptocurrencies Transaction Speeds Compared to Visa & Paypal



Πηγή: howmuch.net(2018)

Παρατηρώντας την εικόνα 3.1 μπορούμε να παρατηρήσουμε πως ενώ η Visa μπορεί να πραγματοποιήσει 24.000 συναλλαγές ανά δευτερόλεπτο το Bitcoin Μπορεί μόνο 7! Ενώ το κρυπτονόμισμα Ripple είναι το κυρίαρχο μεταξύ των κρυπτονομισμάτων και όχι μόνο καθώς με τις 1.500 ανά δευτερόλεπτο ξεπερνάει και την Paypal.

Επίσης ένας ακόμα λόγος που αποφεύγεται η χρήση των κρυπτονομισμάτων εντός του σκοτεινού διαδικτύου είναι οι κυβερνητικοί κανονισμοί που υπάρχουν. Μερικά από τα μεγαλύτερα ονόματα στις σκοτεινές αγορές αντιμετώπισαν προβλήματα τα τελευταία χρόνια με ιστοσελίδες όπως οι Alphabay και Hansa να σταματούν την λειτουργία τους. Οι κυβερνητικές αρχές προσπαθούν να περιορίσουν τα κρυπτονομίσματα με αποτέλεσμα αυτό να επηρεάζει και τους παράνομους ιστότοπους αγοροπωλησιών, με πλέον να εξετάζονται άλλα μέσα πληρωμών.

Τέλος τα τέλη συναλλαγής, δηλαδή το κόστος χρήσης των κρυπτονομισμάτων για τις συναλλαγές είναι ιδιαίτερα υψηλό. Για παράδειγμα το Bitcoin δεν χρησιμοποιείται πλέον ιδιαίτερα στο σκοτεινό διαδίκτυο και αυτό γιατί υπάρχει μια σχετικά απότομη αύξηση του κόστους συναλλαγών. Ο λόγος για αυτό μπορεί να οφείλεται στο πρόβλημα επιβεβαίωσης των συναλλαγών από την πλευρά των ανθρακωρύχων (miners). Συνεπώς μια συναλλαγή κόστους 30 \$ θα έχει ως επιπλέον κόστος σαν τέλος συναλλαγής άλλα 35 \$ γεγονός ιδιαίτερα αποτρεπτικό για χρήστες του σκοτεινού διαδικτύου

## 2.5 Λόγοι χρήσης των κρυπτονομισμάτων στο σκοτεινό διαδίκτυο

Παρά το γεγονός πως τα κρυπτονομίσματα διακατέχονται από ιδιαίτερο ενδιαφέρον στον τρόπο λειτουργίας τους, δυστυχώς αποδείχθηκε πως συχνά εμπλέκονται σε παράνομες πρακτικές. Όπως αναφέρεται από τον Katarzyna C. (2019), παρόλο που η νέα αυτή ιδέα δημιούργησε μια καταπληκτική ευκαιρία για την ύπαρξη ενός μέσου ικανό να εξυπηρετήσει την ψηφιακή οικονομία, με τους χρήστες να αλληλεπιδρούν σε επίπεδο peer-to-peer, συχνά χρησιμοποιείται από άτομα που θέλουν να δραστηριοποιηθούν με παράνομο τρόπο, καθώς μέσω αυτής της τεχνολογίας η διάπραξη εγκληματικών δραστηριοτήτων έχει γίνει πολύ εύκολη.

Αρχικά μέσω των κρυπτονομισμάτων επιτυγχάνεται η ανάπτυξη απατηλών πράξεων και η ενθάρρυνση πρακτικών κατάχρησης της αγοράς. Ένα βασικό παράδειγμα είναι μέσω της χρήσης των ICO, δηλαδή των Initial Coin Offering. Οι ICOs είναι ένας ιδιαίτερα δημοφιλής μηχανισμός χρηματοδότησης για κρυπτονομίσματα ή για κρυπτο assets, προσελκύοντας ουσιαστικά δυνητικούς επενδυτές και επιχειρηματίες που ανταλλάσσουν δισεκατομμύρια δολάρια για να χρηματοδοτήσουν μια νεοφυή επιχειρηματική δραστηριότητα που είναι βασισμένη στο blockchain (Abraham, 2018; FabricVentures & TokenData, 2018; Fisch, 2019; Howell, Niessner & Yermack, 2018).

Τα ICOs ξεκίνησαν με απώτερο σκοπό την χρηματοδότηση των νεοσύστατων επιχειρήσεων, όμως δυστυχώς ο νέος αυτός μηχανισμός αποδείχθηκε ότι δεν ήταν τόσο ιδανικός όσο είχε αρχικά προγραμματιστεί να είναι. Οι νεοφυείς αυτές επιχειρήσεις συνειδητοποίησαν γρήγορα ότι μπορούν να συγκεντρώσουν χρήματα αρκετά γρήγορα χωρίς να προσφέρουν ουσιαστικά κάποιο σημαντικό τεχνολογικό αλλά και επενδυτικό αντάλλαγμα στους επενδυτές, με αποτέλεσμα να εμφανίζονται νέες ιδέες που επιθυμούσαν να λάβουν χρηματοδότηση, συμπεριλαμβανομένων διαφόρων πρακτικών που σκόπευαν μόνο και μόνο στο να εξαπατήσουν τους επενδυτές. Για παράδειγμα το Pincoin το οποίο συνέλεξε 660 εκατομμύρια USD (Suberg, 2018), η AriseBank η οποία συνέλεξε 600 εκατομμύρια USD (Khatri, 2018), η Savedroid η οποία συνέλεξε 50 εκατομμύρια USD (Esteves, 2018). Βέβαια να αναφέρουμε πως άλλοι επιχειρηματίες που ήθελαν να εξαπατήσουν τους επενδυτές αποφάσισαν να χρησιμοποιήσουν περαιτέρω πρακτικές γνωστές ως «Πρόγραμμα Ponzi / Pyramid» συλλέγοντας συνολικά 115 εκατομμύρια δολάρια (Groendahl, 2018). Σε γενικές γραμμές σύμφωνα με έρευνα του 2017, περίπου το 78% των

νεοφυών έργων τα οποία συγκέντρωναν συνολικά 1,34 δισ. δολάρια, κατέληξαν να εξαπατούν τους επενδυτές (Alexandre, 2018).

Φυσικά ο λόγος που οδήγησε τους επενδυτές να βάλουν χρήματα σε αυτές τις επενδύσεις είναι γιατί είχαν την ελπίδα πως θα αποκόμιζαν γρήγορες και σημαντικές αποδόσεις, αποφασίζοντας να «επενδύσουν» τις αποταμιεύσεις τους σε επενδυτικά έργα ακολουθώντας την επιρροή από τα μέσα ενημέρωσης ή από κινήσεις άλλων επενδυτών χωρίς να εξετάζουν ή να γνωρίζουν σε τι ακριβώς πάνε να επενδύσουν (Smith, 2018). Αυτό το είδος της βιασύνης στην επένδυση έχοντας στο μυαλό τους στο να μην χάσουν την επενδυτική ευκαιρία οδήγησε σε περεταίρω αύξηση εμφάνιση απατηλών επενδυτικών περιπτώσεων (GanTOR i et al., 2017; Johnson, 2018). Αυτό το γεγονός οδήγησε στο "crypto rush" ή "crypto bubble" στο τέλος του 2017 το οποίο ήταν αποτέλεσμα κυρίως κερδοσκοπικών ενεργειών με πολλούς παράνομους χρήστες που επιθυμούσαν να κάνουν χρήση πρακτικών γνωστών και απαγορευμένων σε κανονικές κεφαλαιαγορές. (Adriano, 2018; Benedetti & Kostovetsky, 2018)

Κατά συνέπεια, έχουν ανακαλυφθεί διάφοροι καταχρηστικοί μηχανισμοί με ομάδες που προσπαθούν να χειραγωγήσουν την αγορά (Hamrick et al., 2018; Xu & Livshits, 2018). Αυτοί είναι ιδιαίτερα επιτυχημένοι σε περιπτώσεις που αφορούν επενδύσεις κρυπτονομισμάτων με χαμηλή κεφαλαιοποίηση και χαμηλή εμπορευσιμότητα (Martineau, 2018). Μερικά δημοφιλή παραδείγματα τέτοιων κρυπτονομισμάτων είναι το Bancor14, Cloackcoin και το Agrello (Shifflett & Vigna, 2018).

Επίσης μια ακόμα περίπτωση που τα κρυπτονομίσματα χρησιμοποιούνται στο σκοτεινό διαδίκτυο είναι για χρηματικά λύτρα. Τα κρυπτονομίσματα έχουν γίνει δημοφιλή μεταξύ των hackers που άρχισαν να τα ζητούν ως νέα μορφή χρηματικού ανταλλάγματος με την μορφή λύτρων σε περίπτωση επιθέσεων. Σύμφωνα με στατιστικά στοιχεία του FBI το 2017, περισσότερα από 58,3 εκατομμύρια δολάρια έχουν κλαπεί και εξαφανιστεί σε καταστάσεις λύτρων στον κυβερνοχώρο, καθώς από τους απαγωγείς ζητούνταν να γίνουν οι πληρωμές σε κρυπτονομίσματα, κυρίως σε Bitcoin, Ethereum ή Bitcoin Cash (CipherTrace, 2018).

Τα κίνητρα πίσω από την ζήτηση πληρωμών σε κρυπτονομίσματα αντί για κανονικά χρήματα είναι λόγω του ελκυστικού παγκόσμιου χαρακτήρα τους καθώς και της ανώνυμης ή ψευδοανώνυμης φύσης τους χάρη στην οποία μπορούν να κρύψουν αποτελεσματικότερα την πραγματική τους ταυτότητα οι απαγωγείς. Για τον λόγο αυτό τα προαναφερθέντα κρυπτονομίσματα ήταν σε προτίμηση καθώς ήταν λιγότερο

ευμετάβλητα στην χρηματιστηριακή αγορά των κρυπτονομισμάτων και επέτρεπαν την πιο σταθερή πρόβλεψη και διατήρηση κέρδους.

Επιπρόσθετα στο σκοτεινό διαδίκτυο οι πλατφόρμες ανταλλαγής και διαπραγμάτευσης κρυπτονομισμάτων παίζουν καθοριστικό ρόλο σε ολόκληρο το οικοσύστημα. Επιτρέπουν την ανταλλαγή μεταξύ fiat νομισμάτων και κρυπτονομισμάτων διευκολύνοντας την ανάπτυξη του δικτύου. Ωστόσο, το λειτουργικό τους μοντέλο είναι ιδιαίτερα επιρρεπές σε διάφορους κινδύνους, με τις κλοπές να είναι ένα από τα πιο εμφανή παραδείγματα. Επειδή οι πλατφόρμες ανταλλαγής κρυπτονομισμάτων λόγω του γεγονότος ότι κατέχουν μεγάλες ποσότητες κρυπτονομισμάτων για λογαριασμό των πελατών τους αποτελούν σημείο προσέλκυσης ατόμων με απατηλούς σκοπούς στο να διαπράξουν κάποια κλοπή. Οι εισβολείς αυτοί, σπάνε ή παρακάμπτουν τον μηχανισμό ασφαλείας μιας τέτοιας πλατφόρμας και αποκτούν πρόσβαση σε χιλιάδες, αν όχι εκατομμύρια, λογαριασμούς ψηφιακών πορτοφολιών κρυπτονομισμάτων που είναι αποθηκευμένα εκεί. Πολλές φορές έχει επικρατήσει λανθασμένα πως τέτοιες περιπτώσεις επιθέσεων έχουν γίνει λόγω ευπάθειας στην ασφάλεια που διέπει το blockchain. Αυτό είναι λανθασμένο, καθώς τα ψηφιακά πορτοφόλια διατηρούνται εκτός της αλυσίδας του blockchain και σε περίπτωση κλοπής δεν πραγματοποιείται αλληλεπίδραση με αυτό. Ο λόγος για τον οποίο μπορούν να συμβούν τέτοιες επιθέσεις είναι συχνά η απουσία ισχυρού μηχανισμού ασφαλείας της πλατφόρμας ή η παρουσία ενός συστήματος που μπορεί εύκολα να χειραγωγηθεί κατά την διάρκεια πραγματοποίησης της ανταλλαγής των κρυπτονομισμάτων (Katarzyna C., 2019).

Σύμφωνα με τα στατιστικά στοιχεία που δημοσίευσε το CipherTrace, μεταξύ των ετών 2016-2018 κρυπτονομίσματα αξίας 1,3 δισεκατομμύρια δολαρίων εκλάπησαν από τις πλατφόρμες διακράτησης τους. Παρ' όλα αυτά, μια τέτοια πρακτική είναι ιδιαίτερα συχνή στην αγορά των κρυπτονομισμάτων από την αρχή της δημιουργίας των πλατφορμών ανταλλαγής κρυπτονομισμάτων. Ένα από τα πιο εντυπωσιακά γεγονότα ήταν η χρεοκοπία του ανταλλακτηρίου Mt. Gox με έδρα το Τόκιο όπου χάθηκαν περίπου 750.000 από τα Bitcoin των πελατών του. Ακόμη ένα παράδειγμα που αξίζει να αναφέρουμε είναι η περίπτωση του ανταλλακτηρίου Youbit με έδρα τη Νότια Κορέα, το οποίο χρεοκόπησε μετά την απώλεια περίπου 17% των κρυπτονομισμάτων που είχε στην κατοχή της. Βέβαια υπήρξαν και περιπτώσεις ανταλλακτηρίων που προσπάθησαν να επιβιώσουν μετά τις επιθέσεις που υπέστησαν συμπεριλαμβανομένου του Coincheck.Inc με έδρα την Ιαπωνία, το οποίο τον Ιανουάριο του 2018 έχασε περίπου 530 εκατομμύρια δολάρια σε κρυπτονομίσματα

XEM (NEM) (Cheng, 2018). Φυσικά όπως γίνεται κατανοητό όλες αυτές οι απατηλές πράξεις απέναντι στα ανταλλακτήρια αυτά πλήττουν σημαντικά την φήμη τους.

Ακόμη μέσω του σκοτεινού διαδικτύου επιτυγχάνεται η νομιμοποίηση εσόδων από παράνομες δραστηριότητες κοινώς αναφερόμενη ως ξεπλύμα χρήματος. Η συγκεκριμένη μέθοδος είναι μια παλιά και γνωστή πρακτική που ασκείται ανά τον κόσμο χρησιμοποιώντας διάφορα οικονομικά εργαλεία για την επίτευξη του σκοπού αυτού. Οι εκτιμήσεις για το ποσό των χρημάτων που ξεπλύθηκαν παγκοσμίως κυμαίνονται από 500 δισεκατομμύρια έως 1 τρισεκατομμύριο Αμερικάνικα δολάρια αποτελώντας ένα πολύ βασικό πρόβλημα για διάφορες χώρες ανά τον κόσμο. Σύμφωνα με τον Basel AML Index το 64% των χωρών παγκοσμίως έχουν χαρακτηριστεί ως χώρες με υψηλό κίνδυνο νομιμοποίησης εσόδων από παράνομες δραστηριότητες, με μόνο το 4% των χωρών να μπορούν να βελτιώσουν την κατάταξή τους σε σύγκριση με τα αποτελέσματα του περασμένου έτους (2018). Από το 2008 τα άτομα που παρανομούν με αυτόν τον τρόπο άρχισαν να χρησιμοποιούν ένα ακόμα εργαλείο για την εξυπηρέτηση του σκοπού τους, τα κρυπτονομίσματα.

Αυτά τα κρυπτονομίσματα που χρησιμοποιούνται για την εξυπηρέτηση αυτού του σκοπού προέρχονται από διάφορες πηγές. Αρχικά θα μπορούσαν να προέρχονται από πληρωμές λύτρων που είχαν γίνει, αλλά και από ανταλλαγή fiat νομισμάτων. Σε γενικές γραμμές η διαδικασία του ξεπλύματος ακολουθεί μια διαδικασία ανάμειξης των εσόδων για να μην φαίνεται η αρχική προέλευση τους. Στην περίπτωση που χρησιμοποιούνται κρυπτονομίσματα θα μπορούσε αυτή η διαδικασία να έχει διαφορετικές μορφές. Αρχικά να γίνεται η χρήση μιας αποκλειστικής υποδομής ανάμειξης των χρημάτων όπως είναι η BestMixer<sup>16</sup>, η BitBlender<sup>17</sup>, το CoinMixer<sup>18</sup>. Επίσης μέσω ιστότοπων τζόγου και καζίνο που χρησιμοποιούν κρυπτονομίσματα για πονταρίσματα τα οποία δεν απαιτείται να ακολουθούν κανόνες και κανονισμούς επιτρέποντας μια πολύ αποτελεσματική διαδικασία ξεπλύματος. Ακόμη μέσω συνεχών ανταλλαγών κρυπτονομισμάτων σε ανταλλακτήρια έως ότου δεν υπάρχουν ενδείξεις παράνομων συνδέσεων με τα χρήματα που προέρχεται η αγορά τους, με τα πιο συνηθισμένα να είναι το Zcash και το Monero τα οποία προσφέρουν υψηλά επίπεδα απορρήτου γύρω από τους κατόχους τους.

Αφού ολοκληρωθεί η διαδικασία του ξεπλύματος, το δύσκολο κομμάτι είναι να κατατεθούν τα χρήματα αυτά σε τραπεζικούς λογαριασμούς χωρίς να έχουν τεκμηριωμένο ιστορικό προέλευσης. Για τον λόγο αυτό τα παράνομα αυτά άτομα χρησιμοποιούν μια τακτική κατά την οποία μετατρέπουν μικρά κομμάτια

κρυπτονομισμάτων σε fiat νομίσματα και σε δεύτερο χρόνο τα καταθέτουν σε τραπεζικούς λογαριασμούς έτσι ώστε λόγω της μικρότερης χρηματικής αξίας να φαίνονται λιγότερο ύποπτα. Αυτή η πρακτική χρησιμοποιήθηκε για παράδειγμα από εμπόρους ναρκωτικών στην Ευρώπη για να πληρώνουν το καρτέλ κοκαΐνης της Κολομβίας (The Economist, 2018).

Επίσης μια ακόμα πρακτική χρήσης των κρυπτονομισμάτων στο σκοτεινό διαδίκτυο είναι για την χρηματοδότηση παράνομων σκοπών. Από την αρχή της δημιουργίας τους τα κρυπτονομίσματα έχουν προσελκύσει πολλούς χρήστες που δραστηριοποιούνται στην σκοτεινή αγορά/ σκοτεινό διαδίκτυο. Η ανώνυμη ή ψευδο ανώνυμη φύση τους σε συνδυασμό με τις μη αναστρέψιμες συναλλαγές καθώς και με την έλλειψη κανονισμών ελέγχου από τις αρχές και τις κυβερνήσεις οδήγησαν τα κρυπτονομίσματα να γίνουν ένα πολύ δημοφιλές μέσο πληρωμής ενσωματωμένο σε πλατφόρμες σκοτεινών αγορών (Foley, Karlsen, & Putniņš, 2018).

Οι χρήστες λοιπόν του σκοτεινού διαδικτύου πριν το 2008 που πρωτοεμφανίστηκαν τα κρυπτονομίσματα πραγματοποιούσαν τις συναλλαγές τους με τον κλασικό παραδοσιακό τρόπο μεταφοράς χρημάτων. Διάφορες μελέτες έχουν αποδείξει ότι η χρηματοδότηση παράνομων δραστηριοτήτων κυρίως στις αγορές παράνομων προϊόντων ήταν μια από τις πιο δημοφιλείς περιπτώσεις χρήσης των κρυπτονομισμάτων από τότε που εμφανίστηκαν. Για παράδειγμα το Bitcoin το αντιμετώπιζαν ως μέσο πληρωμών και όχι ως μακροπρόθεσμη ή κερδοσκοπική επένδυση, ιδιαίτερα την περίοδο που δεν είχε ιδιαίτερη ζήτηση αλλά και μεγάλο επενδυτικό ενδιαφέρον. Ιδιαίτερο ενδιαφέρον δείχνουν τα αποτελέσματα μιας έρευνας από τον Nasdaq.com (2018), τα οποία αναφέρουν πως ότι περίπου το 25% όλων των ατόμων που χρησιμοποιούν το Bitcoin και περίπου το 44% όλων των συναλλαγών που πραγματοποιούνται με Bitcoin σχετίζονται με παράνομες πρακτικές, ενώ περίπου το 38% των διευθύνσεων Bitcoin διατηρούνται από παράνομους χρήστες, ενώ επίσης πάνω από το 50% όλων των κυκλοφορούντων Bitcoin έχουν συνδεθεί με παράνομες πρακτικές, καθώς και Bitcoin αξίας περίπου 72 δις. δολαρίων εμπλέκονται κάθε χρόνο σε παράνομες δραστηριότητες.

Παράλληλα αυτό που αξίζει να αναφερθεί είναι πως ενδιαφέρουσα είναι η φθίνουσα αναλογία των Bitcoin που χρησιμοποιούνται για σκοτεινές συναλλαγές, με ταυτόχρονα να αυξάνεται το μέγεθος αυτής της αγοράς, υποδηλώνοντας την αυξανόμενη δημοτικότητα άλλων κρυπτονομισμάτων τα οποία εξυπηρετούν τον σκοπό αυτό (Foley et al., 2018).



Φυσικά γεγονός είναι πως οι ρυθμιστικές αρχές προσπαθούν ενεργά να τερματίσουν τις παράνομες πρακτικές και να περιορίσουν τα κρυπτονομίσματα που χρησιμοποιούνται για αυτό τον σκοπό. Το FBI τερμάτισε το Silk Road, μια από τις πιο διάσημες σκοτεινές αγορές που δέχθηκαν κρυπτονομίσματα και κατασχέθηκαν περίπου 144.000 Bitcoin (Wikipedia, 2019). Επιπλέον, η κοινή πρωτοβουλία της Eurpol, του FBI, της DEA και του Dutch National Policy regulaTOR s ήταν αποτελεσματική στο να σταματήσουν την λειτουργία δύο από τις μεγαλύτερες σκοτεινές αγορές, την AlphaBay και την HANSA το 2017 (FBI 2017; Memoria, 2017).

Επιπρόσθετα, τα κρυπτονομίσματα χρησιμοποιούνται στο σκοτεινό διαδίκτυο για να χρηματοδοτούν την τρομοκρατία. Η χρήση των κρυπτονομισμάτων για την χρηματοδότηση τρομοκρατικών ενεργειών είναι σε νηπιακά επίπεδα σε σχέση με τις προηγούμενες περιπτώσεις που αναλύθηκαν. Οι πιθανοί χρήστες για αυτό τον σκοπό εκμεταλλεύονται τα χαρακτηριστικά των κρυπτονομισμάτων, όπως την ανωνυμία ή την ψευδωνυμία, την έλλειψη κανονισμών, την υψηλή ταχύτητα πραγματοποίησης συναλλαγών και το ότι είναι μη αναστρέψιμες αυτές. Ωστόσο, η υψηλή μεταβλητότητα στην τιμή τους ενεργεί ως περιοριστικός παράγοντας για τη χρηματοδότηση της τρομοκρατίας καθώς για τέτοιους σκοπούς διακινούνται πολύ μεγάλα χρηματικά ποσά τα οποία μπορούν εύκολα να μεταβάλλουν τις τιμές των κρυπτονομισμάτων.

Επίσης επειδή η αποδοχή των κρυπτονομισμάτων είναι αρκετά περιορισμένη, εμποδίζει την ελκυστικότητά τους από την πλευρά των τρομοκρατών για να τα χρησιμοποιούν ως μέσω χρηματοδότησης. Ωστόσο δεν είναι εντελώς αδιάφορα μεταξύ τρομοκρατικών ομάδων, καθώς τα κρυπτονομίσματα προσφέρουν γρήγορες διεθνείς μεταφορές ή επιτρέπουν τη συλλογή δωρεών από όλο τον κόσμο. Τέτοιες πρακτικές έχουν ήδη χρησιμοποιηθεί από το ισλαμικό κράτος του Ιράκ και της Συρίας που συνέστησαν το Bitcoin ως ανώνυμο και ασφαλή μηχανισμό πληρωμής (Higgins, 2014).

Τέλος ένας ακόμα λόγος που έχει οδηγήσει στην άνθηση της χρήσης των κρυπτονομισμάτων στο σκοτεινό διαδίκτυο είναι η έλλειψη φορολογικής και γενικότερα κοινής ρυθμιστικής κατεύθυνσης, καθώς από την στιγμή που δημιουργήθηκαν δεν διέθεταν κάποια κοινή πρακτική όσον αφορούσε την φορολογική τους υπόσταση. Μέχρι το 2017 η παγκόσμια χρηματιστηριακή τους κεφαλαιοποίηση ήταν σε αρκετά χαμηλά επίπεδα με μικρούς ρυθμούς υιοθέτησης και δεν είχαν θεωρηθεί ως δυνητικός κίνδυνος από τις ρυθμιστικές αρχές. Μετά όμως το 2017 αυτή η κατάσταση άλλαξε σημαντικά, με πολλούς νέους επενδυτές να

αποκομίζουν αρκετά υψηλές αποδόσεις αναγκάζοντας τις κυβερνητικές αρχές των χωρών να επανεξετάσουν τους κανόνες και τις προσεγγίσεις γύρω από την φορολόγηση τους.

Διάφορα φορολογικά ερωτήματα που βγήκαν στην επιφάνεια αφορούσαν πως θα μπορούσε να διακριθεί μια συναλλαγή μέσω κρυπτονομισμάτων όταν πραγματοποιείται για διενέργεια χρηματιστηριακών συναλλαγών ή όταν πραγματοποιείται για κάποια δαπάνη καθώς υπάρχει έλλειψη σαφούς ορισμού λόγω της συνεχούς εξελισσόμενης φύσης τους. Κατά συνέπεια, ο καθορισμός και η συμφωνία σχετικά με τη σωστή φορολογική πολιτική που πρέπει να ακολουθηθεί έχει γίνει τεράστια πρόκληση σε διάφορες χώρες ανά τον κόσμο, που προσπαθούν να καθορίσουν εθνικούς κανόνες, το οποίο δεν είναι εφικτό λόγω της τεράστιας πολυπλοκότητας του συστήματος.

Φυσικά παρόμοιες προκλήσεις, που απορρέουν από την παγκόσμια και συνεχώς εξελισσόμενη φύση των κρυπτονομισμάτων, υπάρχουν στο κομμάτι που αφορά και τους λογιστικούς κανόνες. Διάφορες ρυθμιστικές αρχές, όπως το International Accounting Standards Board, το Financial Accounting Standards Board, το Accounting Standards Board of Japan και το Australian Accounting Standards Board ξεκίνησαν να αξιολογούν τα κρυπτονομίσματα προκειμένου να καθορίσουν την σωστή κατηγοριοποίηση τους. Ωστόσο, σύμφωνα με την τελευταία ανακοίνωσή τους, το θέμα απαιτεί περαιτέρω διερεύνηση προκειμένου να καταρτιστεί ένα προτεινόμενο σύνολο ενεργειών γύρω από αυτά (ΕΥ, 2018; PwC, 2018). Ένα ερώτημα που βγαίνει στη επιφάνεια είναι αν πρέπει να δημιουργηθεί μια νέα κατηγορία περιουσιακών στοιχείων που θα αφορά αποκλειστικά τα κρυπτονομίσματα και θα εντάσσονται σε αυτήν, όμως μέχρι στιγμής δεν έχει δοθεί ακόμα μια σαφής απάντηση.

## 2.6 Συμπεράσματα δεύτερου κεφαλαίου

Η αναφορά στις σκοτεινές αγορές δεν είναι απαραίτητα συνδεδεμένη με τις παράνομες και εγκληματικές δραστηριότητες. Οι αγορές αυτές είναι απλά ψηφιακές αγορές που δημιουργούνται χρησιμοποιώντας την τεχνολογία που υποστηρίζει την λειτουργία του Bitcoin και συνήθως αποδέχονται το Bitcoin ως μέθοδο πληρωμής λόγω των σχεδόν ανώνυμων χαρακτηριστικών του. Όμως οι σκοτεινές αγορές απέκτησαν παράνομο χαρακτήρα λόγω των προϊόντων που επιτρέπονταν να πωλούνται σε αυτές. Συνεπώς όταν μια ψηφιακή αγορά επιτρέπει τη διακίνηση ναρκωτικών, όπλων ή άλλων παράνομων αντικειμένων, τότε παραβιάζει το νόμο και οι αρχές επιβολής του νόμου χρειάζεται να επέμβουν, οπότε αποκτούν παράνομο χαρακτήρα.

Μπορεί από την ανάλυση που πραγματοποιήθηκε να καταλήξουμε πως το Bitcoin βοήθησε στη αύξηση της οικονομικής δραστηριότητας εντός του darknet ιδιαίτερα στο Silk Road, όμως η χρήση των ψηφιακών νομισμάτων προσανατολισμένων στην προστασία της ιδιωτικής ζωής, όπως για παράδειγμα το Monero (XMR), το Zcash (ZEC), κλπ, διευκολύνουν και αυτά τις συναλλαγές στο σκοτεινό διαδίκτυο.

Μπορεί η συνολική δραστηριότητα του Bitcoin στο σκοτεινό διαδίκτυο αυξήθηκε από το έτος 2017 κατά 340%, με τους προμηθευτές του σκοτεινού διαδικτύου να έλαβαν 47.000 Bitcoin το πρώτο τρίμηνο του 2020, και μάλιστα 2,8 δισεκατομμύρια δολάρια σε Bitcoin (BTC) που μεταφέρθηκαν μέσα από εγκληματικές δραστηριότητες μέσω ανταλλακτηρίων κρυπτονομισμάτων το έτος 2019, όμως το μερίδιό του Bitcoin στη συνολική αγορά ενδέχεται να μειωθεί στο μέλλον, δεδομένης της θετικής στάσης απέναντι σε άλλα κρυπτονομίσματα από την πλευρά των πωλητών των προϊόντων. Ιδιαίτερα τα κρυπτονομίσματα Dash και Monero, τα οποία έχουν ισχυρά διαπιστευτήρια απορρήτου, δείχνουν να προτιμώνται περισσότερο, ενώ το Litecoin επειδή έχει ταχύτερους χρόνους επεξεργασίας σε σύγκριση με το Bitcoin και μπορεί να αποθηκευτεί σε ψηφιακά πορτοφόλια που είναι εκτός σύνδεσης. Τα κρυπτονομίσματα αυτά αποτελούν νέα τεχνολογική γενιά και ονομάζονται altcoins.

Ακόμη να αναφέρουμε πως μερικοί από τους λόγους για τους οποίους τα κρυπτονομίσματα προτιμώνται από τους χρήστες του σκοτεινού διαδικτύου είναι η ανωνυμία, η οποία είναι ο βασικότερος λόγος προτίμησης καθώς δεν μπορούν να

εντοπιστούν εύκολα, αποκρύπτοντας τις διευθύνσεις που προέρχονται οι συναλλαγές, επίσης, η νομιμοποίηση εσόδων από παράνομες δραστηριότητες κοινώς αναφερόμενη ως ξέπλυμα χρήματος καθώς και η έλλειψη φορολογικής και γενικότερα κοινής ρυθμιστικής κατεύθυνσης, καθώς από την στιγμή που δημιουργήθηκαν δεν διέθεταν κάποια κοινή πρακτική όσον αφορούσε την φορολογική τους υπόσταση.

Ενώ αντίθετα ένας λόγος που αποθαρρύνει την χρήση τους στο Dark Web είναι η υψηλή αξία τους, καθώς για παράδειγμα κανείς δεν θέλει να ξοδέψει 40.000 \$ για 1 BTC, ή να αγοράσει κάποιο άλλο κρυπτονόμισμα με υψηλή αξία, ούτε να ανταλλάξει κρυπτονομίσματα με μικρή αξία καθώς πιστεύουν ότι πρόκειται να ανέβουν υψηλότερα στο μέλλον. Τέλος ένα βασικότατο μειονέκτημα τους είναι η ταχύτητα των συναλλαγών. Η Visa μπορεί να πραγματοποιήσει 24.000 συναλλαγές ανά δευτερόλεπτο, το Bitcoin μπορεί μόνο 7! Ενώ το κρυπτονόμισμα Ripple είναι το κυρίαρχο μεταξύ των κρυπτονομισμάτων και όχι μόνο καθώς με τις 1.500 ανά δευτερόλεπτο ξεπερνάει και την Paypal.

## Κεφάλαιο 3: Το Δίκτυο TOR, TON και η ανάπτυξη του Silk Road

### 3.1 Εισαγωγή τρίτου κεφαλαίου

Το τρίτο κεφάλαιο της διπλωματικής εργασίας εστιάζει στην ανάλυση της τεχνολογίας που βρίσκεται πίσω από την πρόσβαση στην χρήση του σκοτεινού διαδικτύου, αλλά και στην πρώτη σκοτεινή αγορά στο διαδίκτυο που ήταν το λεγόμενο Silk Road (ο δρόμος του μεταξιού).

Αναλυτικότερα, επειδή οι διαδικτυακές τοποθεσίες του Darkweb χρειάζονται ένα ειδικό πρόγραμμα περιήγησης για να έχει κάποιος πρόσβαση σε αυτές αναλύονται τα δίκτυα TOR (The Onion Router) και TON (Telegram Open Network). Το πρώτο δίκτυο αποτελεί ένα πρωτόκολλο επικοινωνίας που έχει σχεδιαστεί για να προσφέρει ανωνυμία σε όσους το χρησιμοποιούν καθώς αποκρύπτει τις ταυτότητες των χρηστών και αντικαθιστά τις διευθύνσεις IP τους, ενώ το δεύτερο είναι μια VPN η οποία έχει σχεδιαστεί για την εξάλειψη ζητημάτων απορρήτου όπως η χαμηλή ασφάλεια και η έλλειψη ανωνυμίας.

Τέλος, όσον αφορά στο Silk Road, στο κεφάλαιο αναλύεται η εξέλιξη του από το 2011 που εμφανίστηκε μέχρι και το 2016 που ήταν η τελευταία που εκδόθηκε, ενώ να αναφέρουμε πως είχε χαρακτηριστεί ως το Amazon των ναρκωτικών, καθώς μέσω αυτού πραγματοποιούνταν παράνομο εμπόριο διάφορων προϊόντων όπως ναρκωτικών και όπλων προσφέροντας ανωνυμία στις συναλλαγές μεταξύ εμπόρων και αγοραστών.

### 3.2 Δίκτυο TOR και το δίκτυο TON

Σύμφωνα με τον Love D. (2013) γεγονός είναι πως ο μέσος άνθρωπος γνωρίζει μόνο ένα μέρος του διαδικτύου καθώς υπάρχει ένα μυστικό διαδίκτυο που χρησιμοποιείται από εμπόρους ναρκωτικών, δολοφόνους και παιδόφιλους που ονομάζεται σκοτεινό διαδίκτυο. Σε αυτό το μέρος του διαδικτύου η πρόσβαση είναι αρκετά εύκολη καθώς μπορεί να προσεγγιστεί από οποιονδήποτε ο οποίος έχει ένα συμβατικό πρόγραμμα περιήγησης.

Οι τοποθεσίες αυτές ονομάζονται “Deep Web” ή “Undernet” και υφίστανται εκτός του πεδίου εφαρμογής του Google, του Facebook και του προγράμματος ανάγνωσης RSS (Really Simply Syndication) και αποτελούν μεθόδους ανταλλαγής ψηφιακού πληροφοριακού περιεχομένου διαμέσου του διαδικτύου. Επειδή οι διαδικτυακές τοποθεσίες αυτές είναι πολύ καλά κλειδωμένες, χρειάζεται ένα ειδικό πρόγραμμα περιήγησης για να έχει κάποιος πρόσβαση σε αυτές. Αυτό το πρόγραμμα ονομάζεται πρόγραμμα περιήγησης «TOR » και προσφέρει έναν εντελώς νέο τρόπο σύνδεσης στο Διαδίκτυο.

Το δίκτυο TOR , το οποίο είναι τα πρώτα γράμματα από όλα το αρκτικόλεξο «The Onion Router», είναι ένα δίκτυο ανωνυμίας που έχει σχεδιαστεί για να διατηρεί την ταυτότητα και την τοποθεσία των χρηστών απόλυτα ασφαλή κατά την περιήγηση στον ιστό. Τα δεδομένα που φτάνουν στους χρήστες, πολλές φορές κρυπτογραφούνται. Οι άνθρωποι λοιπόν που χρησιμοποιούν το TOR είναι για να προστατεύσουν τις επικοινωνίες τους, να αναζητήσουν ευαίσθητα θέματα και να αποκτήσουν πρόσβαση σε πληροφορίες που διαφορετικά δεν θα είχαν, ιδιαίτερα εάν για παράδειγμα βρίσκονται πίσω από ένα «τείχος προστασίας».

Συνεπώς, το TOR είναι ένα πρωτόκολλο επικοινωνίας που έχει σχεδιαστεί για να προσφέρει ανωνυμία σε όσους το χρησιμοποιούν, το οποίο είναι αντίθετο με τα συμβατικά προγράμματα περιήγησης ιστού, όπως το Chrome και το Firefox, τα οποία δεν καταβάλλουν καμία προσπάθεια να αποκρύψουν τη θέση ή την ταυτότητα του κάθε χρήστη. Ιστορικά να αναφέρουμε πως αναπτύχθηκε από το Πολεμικό Ναυτικό των Η.Π.Α., ενώ έγινε δημοφιλές μεταξύ εκείνων που ήθελαν να προστατεύσουν τις ταυτότητές τους στο διαδίκτυο και να έχουν ανωνυμία. (Bradbury D., 2020)

Όπως αναφέρει ο Kire V. (2017), το TOR είναι ένα δίκτυο ανωνυμίας που αποτελείται από περισσότερους από 7000 διακομιστές που επιτρέπουν την ασφαλή χρήση του Διαδικτύου, είναι δωρεάν και το λογισμικό του είναι ανοιχτού κώδικα. Σε

καθημερινή βάση περισσότεροι από δύο εκατομμύρια χρήστες συνδέονται στο δίκτυο αυτό και συνεχώς αναπτύσσεται και κυκλοφορούν νέες ανανεωμένες εκδόσεις του. (βλ. εικόνα 3.0)

Βέβαια, αξίζει να σημειωθεί ότι μια τέτοια ανώνυμη δύναμη που διατίθεται δωρεάν, μπορεί να αποτελέσει σημείο εκμετάλλευσης από κάποιες λιγότερο νόμιμες ή και ακόμα εντελώς κακόβουλες δραστηριότητες, οι οποίες μπορούν να λειτουργήσουν ανενόχλητες και χωρίς να μπορούν να ελέγχονται από αρχές επιβολής του νόμου.

Μεταξύ άλλων κάποιοι ιστότοποι που προσφέρουν αγαθά και υπηρεσίες μέσω του TOR δικτύου είναι το Silk Road, το οποίο είχε χαρακτηριστεί ως το Amazon των ναρκωτικών, το Euroarms το οποίο ασχολείται με το εμπόριο όπλων, το White Wolves μέσω του οποίου ενοικιάζονται υπηρεσίες δολοφόνων, αλλά και ιστότοποι παιδικής πορνογραφίας και ιατρικών πειραμάτων που εκτελούνται σε ανθρώπους παρά τη θέλησή τους. Να αναφέρουμε πως παρά το γεγονός ότι το FBI κατόρθωσε να συλλάβει τον δημιουργό του Silk Road, συνδέοντας στοιχεία και αναφορές που γίνονταν εκτός του δικτύου TOR , ακόμα και σήμερα μετά το Silk Road έχουν εμφανιστεί και άλλες σκοτεινές αγορές που ασχολούνται με ναρκωτικά και συναφή προϊόντα.

Όσον αφορά το δίκτυο TON, σύμφωνα με την Perez E. (2020) παρά την πτώση της χρήσης των κρυπτονομισμάτων τα τελευταία χρόνια στο darknet, η εγκληματική δραστηριότητα φαίνεται να μετακινείται σε κατανεμημένες πλατφόρμες και κρυπτογραφημένες εφαρμογές όπως είναι το Telegram Open Network, το οποίο εν συντομία ονομάζεται TON. Επειδή στο darknet όλες οι διευθύνσεις IP είναι κρυφές, επομένως δεν είναι δυνατή η είσοδος σε αυτό μέσω γνωστών προγραμμάτων περιήγησης όπως το Chrome, το Firefox ή το Safari, ολόκληρο το δίκτυο λειτουργεί βάσει της αρχής της αποκέντρωσης και δεν ελέγχεται από καμία αρχή. Λόγω αυτού, πολλοί ιστότοποι στο darknet χρησιμοποιούν πρωτόκολλα κρυπτογράφησης TOR , τα οποία αποκρύπτουν τις ταυτότητες των χρηστών και αντικαθιστούν τις διευθύνσεις IP τους.

Σύμφωνα με τον Cuthbertson A (2019) το TON είναι μια VPN η οποία έχει σχεδιαστεί για την εξάλειψη ζητημάτων απορρήτου όπως η χαμηλή ασφάλεια και η έλλειψη ανωνυμίας, με αποτέλεσμα να μπορεί να λειτουργήσει ως τρόπος εκπλήρωσης παράνομων δραστηριοτήτων. Από την τεχνική πλευρά μιλώντας, οι ιστότοποι που δημιουργούνται στο δίκτυο TON θα μοιάζουν με κανονικές ιστοσελίδες, αλλά η διαφορά τους θα είναι ότι το περιεχόμενο δεν θα αποθηκεύεται

σε κανέναν διακομιστή, αλλά θα διανέμεται σε κόμβους δικτύου και σε χρήστες. Ουσιαστικά αντί για διευθύνσεις IP σε αυτό το δίκτυο, θα υπάρχει ένα πρωτόκολλο τύπου Abstract Datagram Network Layer που θα παρέχει κρυπτογράφηση, ενώ η πρόσβαση σε κανονικούς ιστότοπους τύπου “http” και αντίστροφα θα είναι δυνατή μέσω κάποιας πύλης.

Επίσης αυτό που αξίζει να αναφέρουμε είναι πως σύμφωνα με την Perez E. (2020), υπάρχουν πολλοί ιστότοποι στο σκοτεινό διαδίκτυο που πωλούν παράνομα αγαθά, μεταξύ των οποίων ξεχωρίζουν το AlphaBay και το Oasis. Οι συγκεκριμένοι εκτός από την χρήση του Bitcoin προκάλεσαν την μεγάλη χρήση του κρυπτονομίσματος Monero (XMR) το οποίο προσανατολίζεται περισσότερο στην προστασία της ιδιωτικότητας και ακόμα και σήμερα στο μυαλό πολλών ανθρώπων είναι συνυφασμένο με τις παράνομες δραστηριότητες.

Ενώ επιπλέον δεν αποτελεί έκπληξη πως ορισμένοι αναλυτές βλέπουν τους ιστότοπους που χρησιμοποιούν την τεχνολογία TON ως στοιχείο μιας τεχνολογικά προηγμένης πλατφόρμας darknet, με τον πυρήνα της να αποτελεί το κρυπτονομίσμα Gram. Ήδη οι ρωσικές αρχές επιβολής του νόμου εξέφρασαν ανησυχίες για την τεχνολογία αυτή και ανακοίνωσαν τον Μάρτιο του 2020 πως απαγορεύονται και μπλοκάρονται τα ανώνυμα δίκτυα, συμπεριλαμβανομένων τόσο του TOR όσο και του TON δικτύου.

Τέλος, να αναφέρουμε πως οι πλατφόρμες του Darknet όπως το TOR ή πιθανώς το TON δεν χρησιμοποιούν αποκλειστικά κρυπτονομίσματα, αλλά την τεχνολογία του blockchain συνολικά. Πολλά παράνομα καταστήματα πώλησης ναρκωτικών λειτουργούν μέσω του Blockchain DNS, το οποίο χρησιμοποιεί το Namecoin και το Emercoin για την προστασία των αγορών αυτών για να διασφαλίσει την ακεραιότητα των συναλλαγών των πελατών τους.

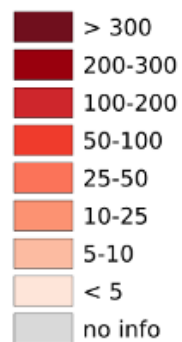
Στην εικόνα 1 που ακολουθεί στην συνέχεια μπορούμε να δούμε την διάδοση του δικτύου TOR στον κόσμο το έτος 2015 και πιο συγκεκριμένα τους καθημερινούς χρήστες του.



**Εικόνα 3.0:** Η διάδοση του δικτύου TOR στον κόσμο (2015)

# The Anonymous Internet, 2015

Daily Tor users per 100'000 Internet users

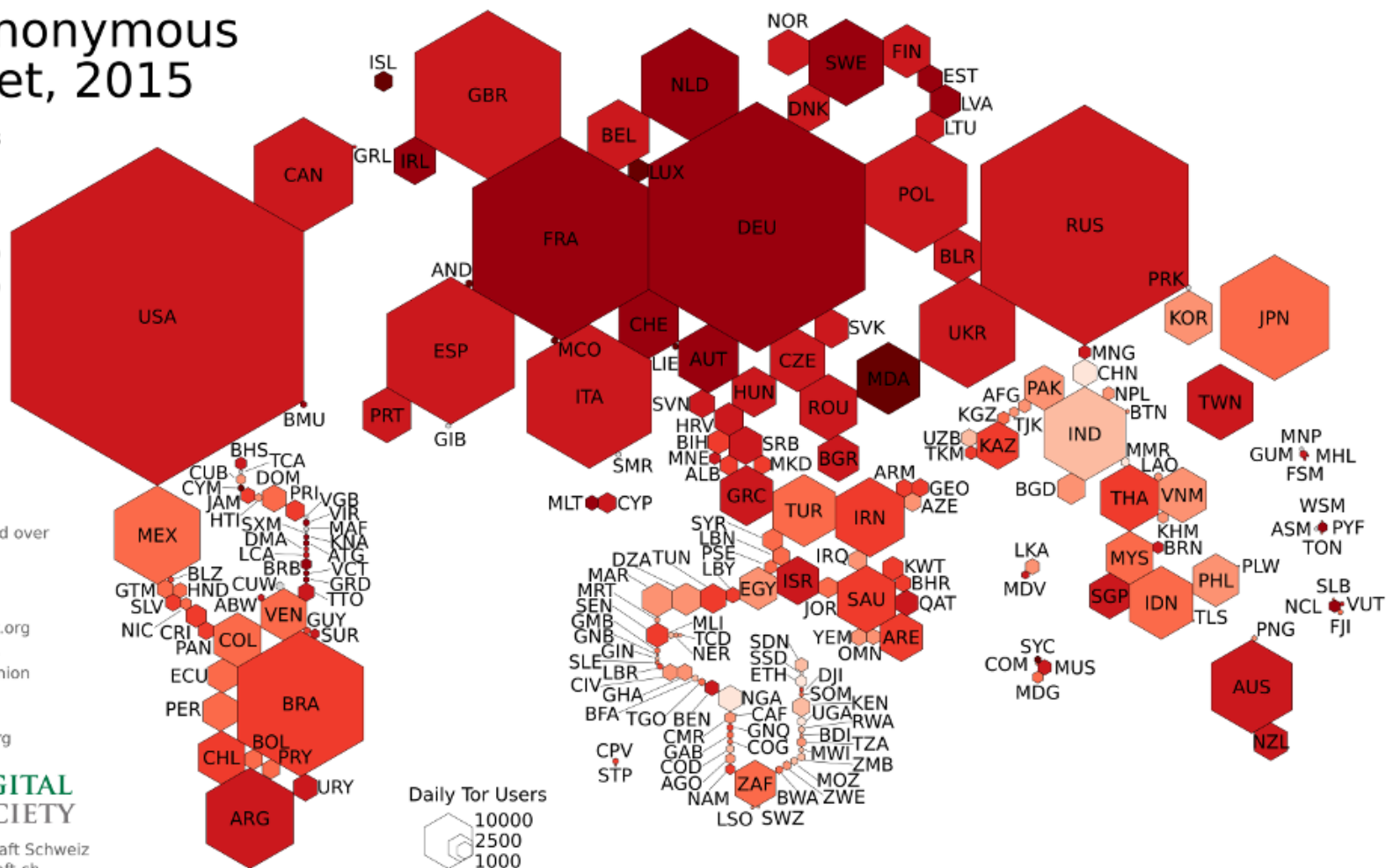


Tor users averaged over the year 2015.

Data sources:  
 Tor Metrics Portal  
[metrics.torproject.org](http://metrics.torproject.org)  
 International Tele-communication Union  
[itu.org](http://itu.org)  
 World Bank  
[data.worldbank.org](http://data.worldbank.org)



Digitale Gesellschaft Schweiz  
[digitale-gesellschaft.ch](http://digitale-gesellschaft.ch)  
 CC-BY-SA, 2017-03-28



### 3.3 Silk Road - Ο Δρόμος του μεταξιδιού

Το Silk Road που στα Ελληνικά θα μπορούσε να μεταφραστεί ως «Ο Δρόμος του μεταξιδιού», ήταν μια από τις πρώτες - αν όχι η πρώτη - σκοτεινή αγορά στο διαδίκτυο. Δημιουργήθηκε από τον Ross Ulbricht και ήταν μια ψηφιακή αγορά που συνέδεε τους πωλητές παράνομων προϊόντων όπως ναρκωτικών με πιθανούς αγοραστές. Οι πωλητές αυτοί είχαν την δυνατότητα να διαφημίζουν τα προϊόντα τους στο Silk Road, με τον ίδιο τρόπο που γινόταν σε μια νόμιμη αγορά ηλεκτρονικού εμπορίου. (Bradbury D., 2020)

Επειδή οι επιχειρήσεις που δραστηριοποιούνται γύρω από τα ναρκωτικά δεν είναι νόμιμες, το Silk Road προσέφερε την επιλογή να μπορούν να γίνονται αγορές, πωλήσεις αλλά και διαφημίσεις με ανώνυμο τρόπο καθώς, παρ' όλο που η αγορά αυτή δεν ήταν αποκεντρωμένη, έτρεχε μέσω υπολογιστών στο δίκτυο «TOR » όπου και προστατεύονταν.

Ο τρόπος λειτουργίας του ήταν ιδιαίτερα απλός. Να αναφέρουμε πως όταν κάποιος αποφάσιζε να αγοράζει ναρκωτικά μέσω του ιστότοπου αυτού, δεν ήθελε να στέλνει τα χρήματα απευθείας στον πωλητή γιατί δεν γνώριζε εάν υπάρχει εμπιστοσύνη μεταξύ των αντισυμβαλλόμενων ατόμων. Για τον λόγο αυτό την λύση την έδωσε το Silk Road που παρείχε μια ενδιάμεση υπηρεσία. Ουσιαστικά οι πελάτες που αγοράζουν ναρκωτικά από πωλητές μέσω του Silk Road θα έστελναν τα χρήματά τους στο Silk Road, αντί για τον πωλητή και στη συνέχεια αυτό θα κρατούσε αυτά τα χρήματα έως ότου ο πελάτης επιβεβαιώσει ότι έχει λάβει το προϊόν αυτό που είχε παραγγείλει. Στην συνέχεια, το Silk Road θα αποδέσμευε και θα απέδιδε τα χρήματα στον πωλητή. Επίσης να αναφέρουμε πως η αποστολή και παράδοση των προϊόντων γινόταν συνήθως με εταιρείες courier στην διεύθυνση του σπιτιού του αγοραστή.

Αξίζει να αναφέρουμε πως σύμφωνα με την επισήμανση του Bradbury D. (2020), οι αγοροπωλησίες γίνονταν κυρίως σε κρυπτονομίσματα και μάλιστα σε Bitcoin και όχι σε fiat νομίσματα, επειδή προσέφεραν μεγάλο βαθμό ανωνυμίας στο δίκτυο. Ενώ επίσης να αναφέρουμε πως ένα από τα πρώτα πράγματα που προειδοποίησαν τις αρχές επιβολής του νόμου για την δραστηριότητα που πραγματοποιούσε η πλατφόρμα του Silk Road, ήταν η άνοδος της αναφοράς στα ναρκωτικά μέσα στο ηλεκτρονικό ταχυδρομείο.

### 3.3.1 To SilkRoad 1 (2011)

Το Silk Road 1 αποτελούσε ένα δικτυακό ιστότοπο που δραστηριοποιούνταν στο σκοτεινό διαδίκτυο και δημιουργήθηκε το έτος 2011. Συνδέθηκε με το παράνομο εμπόριο διάφορων προϊόντων όπως ναρκωτικών και όπλων. Στην ελληνική γλώσσα θα μεταφραζόταν ως «ο δρόμος του μεταξίου» και λειτούργησε στο δίκτυο TOR, ένα δίκτυο ανωνυμίας έξω από το πεδίο εφαρμογής των γνωστών σε όλους μας ιστότοπων όπως το Google, το Facebook, αλλά ακόμα και των συμβατικών προγραμμάτων περιήγησης όπως το Google Chrome, το Internet Explorer κλπ.

Ο τρόπος σχεδιασμού του δικτύου αυτού ήταν τέτοιος ώστε έδινε την δυνατότητα στους χρήστες να διατηρούν την πλήρη ανωνυμία τους και να μην είναι ανιχνεύσιμες οι κινήσεις τους. Όταν οι αγοροπωλησίες προϊόντων και υπηρεσιών εντός του Silk Road συνδυάστηκαν με κάποιο ανώνυμο ψηφιακό νόμισμα το οποίο μπορεί να μετατρέπεται σε πραγματικά χρήματα, όπως είναι το Bitcoin, έγινε σαφές πως το Silk Road όχι μόνο θα λειτουργούσε, αλλά και θα ευδοκίμοιζε για παράνομες δραστηριότητες.

Σύμφωνα με τον Love D. (2013) όπως αναφέρεται σε σχετικό άρθρο του στο [businessinsider.com](http://businessinsider.com), χρησιμοποιώντας το δίκτυο TOR, ο καθένας μπορούσε να έχει πρόσβαση στο Silk Road μέσω της ηλεκτρονικής διεύθυνσης: <http://silkroadvb5piz3r.onion> δημιουργώντας ιδιαίτερα εύκολα έναν ηλεκτρονικό λογαριασμό και ξεκινώντας τις αγοροπωλησίες των παράνομων προϊόντων. Παρατηρώντας την εικόνα 3.1 βλέπουμε τα στοιχεία που χρειαζόνταν για να ανοίξει ένας λογαριασμός.

**Εικόνα 3.1:** Τα στοιχεία που χρειαζόνταν για να ανοίξει ένας λογαριασμός στο Silk Road 1.



The image shows a registration form for Silk Road 1. It features four input fields: 'user name', 'passphrase', a field containing a redacted alphanumeric string 's a d d e 4 0 7', and an empty field. A 'Go' button is located to the right of the bottom input field. Below the form, there is a link that says '- click here to join'.

Ακόμη όπως αναλύονταν στο ίδιο άρθρο, μετά την πρόσβαση στο Silk Road, εμφανιζόταν η αρχική σελίδα του ιστότοπου και παρουσιαζόταν ο κατάλογος των προϊόντων ανάλογα με την κατηγορία που ανήκαν. Οι χρήστες είχαν την επιλογή να επιλέξουν εκείνες που τους ενδιέφεραν για να βρουν πιο εύκολα τα προϊόντα της επιλογής τους. Όπως μπορούμε να παρατηρήσουμε στην εικόνα 3.2 ο κατάλογος δεν περιλαμβάνει μόνο ναρκωτικά, αλλά και ρουχισμό, ηλεκτρονικά, κοσμήματα, βιβλία κλπ, όπως φαίνεται παρακάτω.

**Εικόνα 3.2:** Ο κατάλογος και οι κατηγορίες των προϊόντων που διέθετε το SilkRoad 1

The screenshot shows the Silk Road anonymous market interface. At the top left is the logo featuring a camel and the text "Silk Road anonymous market". To the right of the logo are navigation links: "messages 0", "orders 0", and "account \$0.00". Below this is a search bar with a "Go" button. On the left side, there is a "Shop by Category" menu listing various product categories and their counts. The main area on the right displays a grid of product listings, each with a small image, a title, and a price.

**Shop by Category**

- Drugs 8,670
  - Cannabis 2,066
  - Dissociatives 165
  - Ecstasy 660
  - Opioids 591
  - Other 455
  - Precursors 50
  - Prescription 2,146
  - Psychedelics 981
  - Stimulants 1,102
- Apparel 264
- Art 127
- Biotic materials 1
- Books 861
- Collectibles 5
- Computer equipment 32
- Custom Orders 68
- Digital goods 509
- Drug paraphernalia 305
- Electronics 77
- Erotica 540
- Fireworks 2
- Food 9
- Forgeries 81
- Hardware 23
- Herbs & Supplements 8
- Home & Garden 8
- Jewelry 54
- Lab Supplies 71
- Lotteries & games 77
- Medical 57






**Product Listings:**

1g MDMA 82%+ High Quality -Made in Germany- \$1.30	50 gr. Crystal MDMA Rocks \$23.33	Valium 10mg/ Diazepam (100 Pills) \$2.32	3g XxX AAA QUALITY WEED,AMAZING \$0.98
Kamagra jelly (India), 1 week pack \$0.98	Honeycomb Wax (85+% THC) Fully Purged \$1.45	1 gram * Moroccan Hash * DUTCH QUALITY \$0.27	Citalopram 10x 20mg table \$0.10
10 grams ketamine crystals \$7.15	[3g] Greenstone NZ Hash (B Grade) \$2.49	+++ 100 x 25i-NBOMe Strawberry Snuff Caps +++ \$3.80	300x 25i/25c-NBOMe Liqui Dropper 1200µg \$4.14

Αυτό που μπορεί να γίνει εύκολα κατανοητό είναι πως η διαδικασία αγοράς θυμίζει σε μεγάλο βαθμό τις αντίστοιχες που ακολουθούνται για την πραγματοποίηση αγορών από ηλεκτρονικά καταστήματα εταιρειών όπως το Amazon.

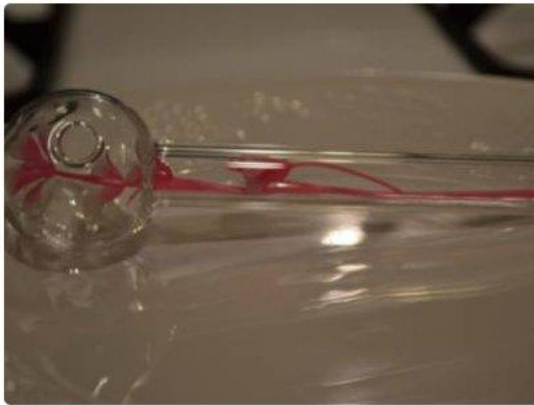
Ας δούμε στην εικόνα 3.3 που έπεται στην συνέχεια πως εάν για παράδειγμα ένας χρήστης του ιστότοπου επιλέξει την κατηγορία “Drug paraphernalia ” , εμφανίζεται ο παρακάτω πίνακας προϊόντων.

**Εικόνα 3.3:** Τα προϊόντα της κατηγορίας Drug paraphernalia

<ul style="list-style-type: none"> <li>Drug paraphernalia 305</li> <li>  Accessories 50</li> <li>  Bongs 15</li> <li>  Grinders 45</li> <li>  Pipes 50</li> <li>  Rolling Supplies 20</li> <li>  Scales 53</li> <li>  Storage 7</li> <li>  Vaporizers 14</li> <li>Apparel 264</li> <li>Art 127</li> <li>Biotic materials 1</li> <li>Books 861</li> <li>Collectibles 5</li> <li>Computer equipment 32</li> <li>Custom Orders 68</li> <li>Digital goods 510</li> <li>Drugs 8,671</li> <li>Electronics 77</li> <li>Erotica 540</li> <li>Fireworks 2</li> <li>Food 9</li> <li>Forgeries 81</li> <li>Hardware 23</li> <li>Herbs &amp; Supplements 8</li> <li>Home &amp; Garden 8</li> <li>Jewelry 54</li> <li>Lab Supplies 71</li> <li>Lotteries &amp; games 76</li> <li>Medical 57</li> <li>Money 123</li> <li>Musical instruments 2</li> <li>Packaging 72</li> <li>Services 70</li> <li>Spa/fitness goods 1</li> </ul>	sort by: <input type="text" value="bestselling"/> <input type="checkbox"/> Domestic only <input type="button" value="update"/>		
		<b>1 GLASS BALL METH PIPE !!!!</b> <small>seller: vicious86(100) ships from: United States of America</small>	<b>฿0.29</b> <small>add to cart</small>
		<b>200g 0.01 Digital Accuracy Scales</b> <small>seller: optiman(100) ships from: United States of America</small>	<b>฿0.52</b> <small>add to cart</small>
		<b>The Bomb Bubble Vaporizer</b> <small>seller: plutopete(98) ships from: United Kingdom</small>	<b>฿0.49</b> <small>add to cart</small>
		<b>Deluxe Powder Snuffer</b> <small>seller: plutopete(98) ships from: United Kingdom</small>	<b>฿0.23</b> <small>add to cart</small>
		<b>10 Pack Syringes ,Needles,Works,Ect 1cc 1/2 inch</b>	<b>฿0.07</b>

Αν υποθετικά επιλέγαμε το πρώτο προϊόν της παραπάνω λίστας, το οποίο είναι μια γυάλινη πίπα ναρκωτικού μεθ, παρατηρούμε πως κόστιζε 0,29 Bitcoin το οποίο ισοδυναμούσε με μόλις \$13,67 το έτος εκείνο. Πατώντας την επιλογή «προσθήκη στο καλάθι» εμφανίζονται λεπτομερώς οι πληροφορίες του προϊόντος αλλά και ο τρόπος αποστολής του, που στην περίπτωση που θα αποστέλλονταν εντός ΗΠΑ ήταν δωρεάν. (Εικόνα 3.4)

**Εικόνα 3.4:** Πληροφορίες για το προϊόν αλλά και ο τρόπος αποστολής του



## 1 GLASS BALL METH PIPE !!!!

฿0.29 [add to cart](#)

seller: vicious86(100)  
ships from: United States of America  
ships to: United States of America  
category: Pipes

[bookmark this item](#)

postage options:

[Free Shipping USA \(฿0\)](#) [?](#)

[report this item](#)

### Description

Why embarrass yourself and get evil looks at the local Quickimart when your buying your Paraphernalia. Now you don't have to worry about where you will buy such an item. We have a ton of them and we ship very discreetly and quickly to anywhere in the US. Made with the highest grade boriscilcate glass materials! This glass is both thick and very strong, not the thin brittle glass that you normally receive when ordering these items. Because we buy quality glass not Chinese crap our pipes are a bit more money than others. With us you are buying quality and we stand behind our product 100 percent. So keep your business private and out of the eyes of your neighbors and buy QUALITY PIPES right here right now!!!!

Aprox 5 inches long. Great for DMT as well.

All PIPES ARE CLEAR. The pic shows a plastic flower INSIDE the pipe so you can distinguish the pipe better in the picture. They are also sold with a plastic flower inside so they can be sold in some States. Flower NOT included.

Every pipe is individually hand blown so every one is very slightly different from the next one.

They are true works of art!

!!ALWAYS FREE SHIPPING TO THE USA!!!!

Μετά την διαδικασία πληρωμής όπως βλέπουμε στην εικόνα 3,5, ακολουθεί ένας πίνακας στον οποίο διακρίνεται τόσο η τιμή όσο και η ποσότητα του προϊόντος που επιλέχθηκε.

**Εικόνα 3.5:** Η τελική επιλογή των προϊόντων και η τιμολόγηση τους

### Shopping cart

seller	item	price	quantity	sub-total	postage	total	hedged <a href="#">?</a>
Lucydrop(94)	10 hits 100+ug CLEAN and REAL LSD *limited bonus*	฿1.58	1 <small>max: 116</small>	฿1.58	<input type="text" value="select one"/> <input type="button" value="go"/>	฿1.58	hedged
vicious86(100)	1 GLASS BALL METH PIPE !!!!	฿0.29	1 <small>max: 30</small>	฿0.29	<input type="text" value="select one"/> <input type="button" value="go"/>	฿0.29	hedged

Add gift codes in the order you want them used.

**Total: ฿1.87**

Στην συνέχεια ακολουθούν στοιχεία που αφορούν την διεύθυνση πληρωμής μέσω Bitcoin(Εικόνα 3.6) που θα γίνει η συναλλαγή αλλά και στοιχείων σχετικά με την αποστολή των προϊόντων (Εικόνα 3.7).

**Εικόνα 3.6:**Πληροφορίες για την πληρωμή της συναλλαγής

escrow (usd)	escrow (btc)	available
\$0.00	฿0.00	฿0.00

[Click here to make a deposit](#)

Withdraw bitcoins:

฿  PIN:

Send bitcoins to another member:

฿  PIN:

**Εικόνα**

**Total: ฿1.87**

Please enter your name and address as it would be written on a letter: ?

PIN:

**You have insufficient funds in your account**

**3.7:**Πληροφορίες για την διεύθυνση αποστολής των προϊόντων

Λόγω του άμεσου τρόπου αγοροπωλησιών παράνομων προϊόντων, οι αρχές προσπάθησαν να περιορίσουν τον ιστότοπο αυτόν και δύο χρόνια αργότερα το 2013 τον έκλεισαν. Στις 2 Οκτωβρίου του 2013 αμέσως μετά την είδηση ότι το Silk Road έκλεισε από το FBI συνελήφθη και ο φερόμενος ιδιοκτήτης του Ross William Ulbricht., γνωστός και ως «Dread Pirate Roberts», παρόλο που προστάτευε την ταυτότητα του μέσω εργαλείων κρυπτογράφησης και ανωνυμίας. Σύμφωνα με τον Greenberg A. (2013), σε άρθρο που δημοσίευσε στο Forbes (2013) μεταξύ άλλων στην σύλληψη του φαίνεται να συνετέλεσε το γεγονός πως χρησιμοποιούσε πλαστά έγγραφα ταυτότητας, στα οποία χρησιμοποίησε διαφορετικό όνομα, αλλά παρουσίαζε τη φωτογραφία όταν πέρανε τα σύνορα προς τον Καναδά, η πραγματοποίηση λαθών ασφαλείας στις IP διευθύνσεις που χρησιμοποιούσε αλλά και οι αναρτήσεις που πραγματοποιούσε στο φόρουμ Bitcoin Talk χρησιμοποιώντας την πραγματική διεύθυνση του ηλεκτρονικού του ταχυδρομείου. Ενώ ακόμη να αναφέρουμε πως υπήρξαν αναφορές ότι, κατά τη σύλληψη του Ulbricht, κατασχέθηκαν από εκείνον 26.000 Bitcoin, τα οποία ισοδυναμούσαν με περίπου 3,26 εκατομμύρια δολάρια την 1η Οκτωβρίου του 2013.Ενώ σύμφωνα με τον Warner B. (2014) φημολογείται ότι ο Ulbricht είχε στην κατοχή του 144.000 Bitcoin που σήμερα η αξία τους είναι πάνω από 8 δις δολάρια (2.4.2021)

Επειδή οι περισσότερες συναλλαγές σε αυτό γινόντουσαν μέσω κρυπτονομισμάτων και κυρίως μέσω του Bitcoin, το γεγονός της σύλληψης του Ulbricht και το κλείσιμο της υπηρεσίας οδήγησαν σε μεγάλη πτώση της τιμής του(Spaven E., 2013). Η ιστοιμία του Bitcoin κατρακύλησε κατά 20% τον Οκτώβριο του 2013, όμως ανέκαμψε σχεδόν πλήρως σε σύντομο χρονικό διάστημα, όπως φαίνεται χαρακτηριστικά κι από το παρακάτω διάγραμμα (Διάγραμμα 3.1)

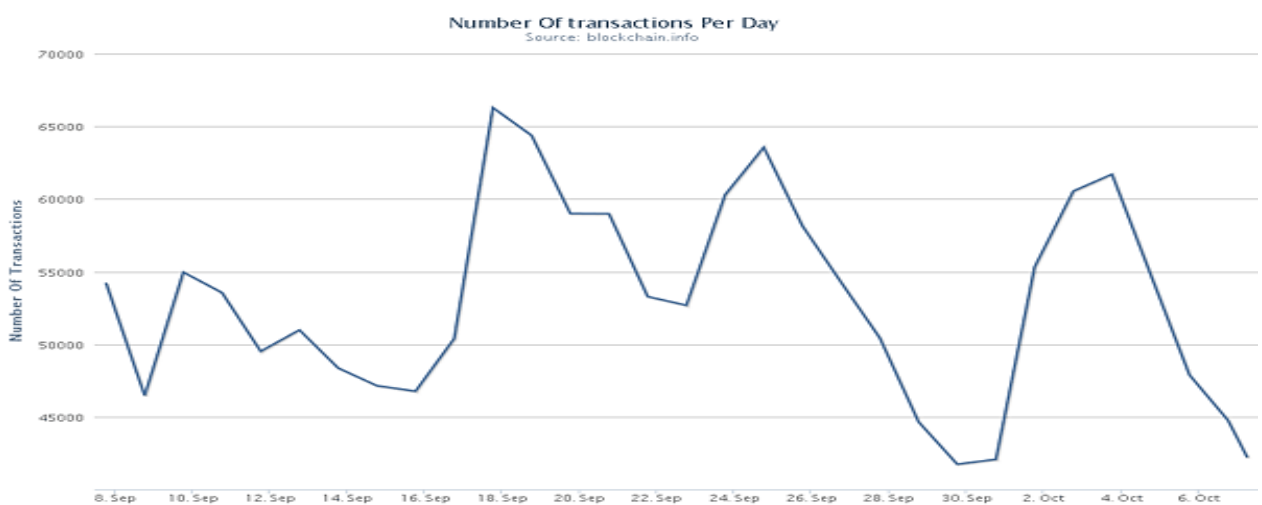


**Διάγραμμα 3.1:** Η πορεία της τιμής του Bitcoin μετά το κλείσιμο του Silk Road και την σύλληψη του Ulbricht



Βέβαια το κλείσιμο του Silk Road, όπως αναφέρεται από τον Τσακούμη Α. (2013) ήταν αναμενόμενο να φέρει και μείωση του συνολικού αριθμού των ημερήσιων συναλλαγών του κρυπτονομίσματος. Όλες οι συναλλαγές που γίνονταν καθημερινά στο Silk Road πλέον δεν υφίστανται και όπως φαίνεται και στο παρακάτω Διάγραμμα 3.2, την περίοδο από τις 8 Σεπτεμβρίου 2013 μέχρι τις 6 Οκτώβρη του 2013 μειώθηκαν πάρα πολύ.

**Διάγραμμα 3.2:** Η πτώση του αριθμού των συναλλαγών του Bitcoin με το κλείσιμο



του Silk Road

Πηγή: Blockchain.info

### 3.3.2 To Silk Road 2.0 (2013)

Στις 6 Νοεμβρίου του 2013, περίπου ένα μήνα μετά το κλείσιμο του πρώτου ιστότοπου με το ομώνυμο όνομα, οι διαχειριστές του πλέον κλειστού Silk Road 1, ξεκίνησαν εκ νέου την ιστοσελίδα, καθοδηγούμενοι από ένα νέο πρόσωπο με το ψευδώνυμο «Dread Pirate Roberts» και το ονόμασαν Silk Road 2.0.

Σύμφωνα με το trendmicro.com (2016), ο νέος αυτός ιστότοπος είχε βελτιωμένη ασφάλεια και χρησιμοποιούσε τεχνολογία προφύλαξης από τη διανομή κρυπτογραφημένων αντιγράφων του πηγαίου κώδικα του ιστότοπου, ώστε να επιτρέπεται η γρήγορη αναδημιουργία του σε περίπτωση άλλου τερματισμού του όπως του προηγούμενου.

Στις 20 Δεκέμβρη του 2013, όπως αναφέρεται από τον Greenberg A. (2013) σε δημοσίευση του στο Forbes, ανακοινώθηκε ότι τρεις υποτιθέμενοι διαχειριστές του Silk Road 2.0 είχαν συλληφθεί, ενώ δύο από αυτούς τους υπόπτους, ο Andrew Michael Jones και ο Gary Davis ως διαχειριστές είχαν τα κωδικά ονόματα "Indigo" και "Libertas". Ενώ όπως αναφέρεται από τον Berkman F. (2013), μπορεί γύρω από αυτό το χρονικό διάστημα ο ιστότοπος να ανέστειλε την δραστηριότητά του και την λειτουργία του, όμως ένας νέος προσωρινός διαχειριστής με το κωδικό όνομα "Defcon" ανέλαβε την διαχείριση και υποσχέθηκε να επαναφέρει τον ιστότοπο πίσω σε κατάσταση λειτουργίας.

Επίσης ένα σημαντικό γεγονός που συνέβη κατά την διάρκεια λειτουργίας του SilkRoad 2.0 ήταν πως σύμφωνα με τον Russel B. (2013), στις 13 Φεβρουαρίου 2014, ο Defcon ανακοίνωσε ότι οι λογαριασμοί των ατόμων που πραγματοποιούνταν οι συναλλαγές στον ιστότοπο βρισκόνταν σε κίνδυνο να παραβιαστούν λόγω μιας παθογένειας του πρωτοκόλλου του Bitcoin που ονομαζόταν "transaction malleability". Αυτό το γεγονός οδήγησε στην απώλεια Bitcoin αξίας 2,7 εκατομμυρίων δολαρίων καθώς υπήρχε ένα πρόβλημα στη λειτουργία "refresh deposits" του ιστότοπου και οι διαχειριστές αποφάσισαν να αποζημιώσουν και να επιστρέψουν στους χρήστες τα χρήματα που έχασαν από τις προσωπικές τους προμήθειες. Να αναφερθεί πως το 50% των περιπτώσεων εξοφλήθηκε όμως πλήρως στις 8 Απριλίου του ίδιου έτους.

Στις 6 Νοεμβρίου 2014, οι κυβερνητικές αρχές σε συνεργασία με το FBI, την Europol και το Eurojust ανακοίνωσαν τη σύλληψη του Blake Benthall, του ιδιοκτήτη και διαχειριστή του Silk Road 2.0. με το ψευδώνυμο «Defcon». Η σύλληψη του πραγματοποιήθηκε την προηγούμενη ημέρα στις 5 Νοεμβρίου στο Σαν Φρανσίσκο,

στο πλαίσιο της διεθνούς επιχείρησης επιβολής νόμου που είχε ως στόχο τις αγορές σκοτεινού δικτύου και άλλες κρυφές υπηρεσίες που λειτουργούσαν στο δίκτυο TOR με την κωδική ονομασία Operation Onymous. (Pepitone J.(2014), Cook J. (2014))

Ενώ τέλος στην έκθεση του το FBI όπως αναφέρεται από τον Rizzo P. (2014), αναλύει πως το Silk Road 2.0 χρησιμοποιήθηκε από χιλιάδες εμπόρους ναρκωτικών οι οποίοι πραγματοποίησαν ξέπλυμα εκατομμυρίων δολαρίων τα οποία δημιουργήθηκαν από παράνομες συναλλαγές και δραστηριότητες. Οι αρχές επιβολής του νόμου εκτιμούν ότι το Silk Road 2.0 παρήγαγε 8 εκατομμύρια δολάρια το μήνα σε πωλήσεις σε περισσότερους από 150.000 ενεργούς χρήστες

### **3.3.3. Το Silk Road 3.0**

Μετά το κλείσιμο του Silk Road 2.0. στις 5 Νοέμβρη του 2014, η Diabolus Market μετονομάστηκε σε «Silk Road 3.0 Reloaded» για να αξιοποιήσει το εμπορικό όνομα που είχε δημιουργηθεί τα προηγούμενα χρόνια στον χώρο αυτό.

Σύμφωνα με το darknetmarkets.com (2013), το Silk Road 3.0 Reloaded ήταν μια αγορά στο σκοτεινό διαδίκτυο που πωλούσε κυρίως παράνομα αγαθά καθώς και υπηρεσίες, συμπεριλαμβανομένων και των ναρκωτικών. Οι χρήστες που διατηρούσαν λογαριασμούς στις προηγούμενες εκδόσεις του Silk Road, με μία αναβάθμιση του ήδη υπάρχοντος λογαριασμού τους μπορούσαν να έχουν πρόσβαση στο Silk Road 3.0, ενώ οι πληρωμές συνεχίζονται να γίνονται μέσω Bitcoin.

Αυτό που αξίζει να σημειωθεί είναι πως η τρίτη έκδοση του Silk Road έχει ως σκοπό να βελτιώσει την αποδοχή και τη δημοτικότητά του μέσα από μια φιλανθρωπική κίνηση. Ως μέρος του φιλανθρωπικού κινήματος που πραγματοποιήθηκε λίγο μετά τις 8 Ιουνίου του 2016, το Silk Road 3.0 δώριζε 5 δολάρια από κάθε πώληση στο site, ακόμα και αν το ποσό της πώλησης ήταν μικρότερο από 5 δολάρια, στην Last Door Recovery Society. Ο οργανισμός αυτός είχε έδρα στο Βανκούβερ του Καναδά και ήταν ένα κέντρο απεξάρτησης από ναρκωτικά και αλκοόλ. Επίσης για όσους μπορεί να έχουν πρόβλημα υγείας λόγω τοξικών ουσιών, το site τους ενθάρρυνε να σταματήσουν τη χρήση τους και να κατευθυνθούν στην κατάλληλη ιατρική βοήθεια. (bitcoinist.com, 2013).

Φυσικά ιδιαίτερα φανερή είναι η αντίφαση μεταξύ της πώλησης παράνομων ουσιών και της παροχής χρημάτων για την απεξάρτηση από αυτές. Ωστόσο παρά το γεγονός πως η εταιρεία είχε μειωμένα κέρδη, φαίνεται ότι οι διαχειριστές επικεντρώνονταν στην κοινωνική αυτή στάση αντί για την δημιουργία περισσότερων κερδών.

Επιπλέον, να αναφέρουμε πως η κοινωνική αυτή φιλανθρωπική κίνηση που πραγματοποιήθηκε στις 8 Ιουνίου 2016, δεν ήταν η πρώτη φιλανθρωπία που διοργανώθηκε από το Silk Road 3.0, καθώς σύμφωνα με τον επίσημο ηλεκτρονικό ιστότοπο του, οι διαχειριστές της πλατφόρμας παροτρύναν τους χρήστες του site να στέλνουν τακτικά δωρεές σε Bitcoin σε διάφορες φιλανθρωπικές ενέργειες που προωθούσαν. Η προσπάθεια αυτή από τη μεριά του Silk Road 3.0. να οργανώνει φιλανθρωπικές κινήσεις είχε χαρακτηριστεί από κάποιους ιδιαίτερα αξιόλογη. (Silkroaddrugs.org, 2013).

### **3.3.4 To Silk Road 3.1. (2016)**

Το έτος 2016 έκανε την εμφάνιση του το Silk Road 3.1., το οποίο αποτελούσε την επανεκκίνηση του Silk Road 3.0. Αυτή την φορά οι χρήστες του χρειάζονταν να κάνουν απλώς μια αναβάθμιση του λογαριασμού τους από το προηγούμενο για να μπορέσουν να αποκτήσουν πρόσβαση. Παρά το γεγονός ότι όλα τα Silk Road έκλειναν μετά από κάποιο διάστημα, ο διαχειριστής του Silk Road 3.1 επισήμανε πως με την επαναλειτουργία του το 2016 κέρδιζε τρεις νέους χρήστες κάθε λεπτό. (deepdotweb.com, 2017)

Αυτό που αξίζει να σημειωθεί είναι πως λίγο μετά το άνοιγμα του, το Silk Road 3.1 στις 19 Ιουλίου του 2016, έπεσε θύμα επίθεσης χάκερς και οι διαχειριστές του το έκλεισαν προσωρινά. Με την επαναλειτουργία του, επειδή οι συναλλαγές γίνονταν κυρίως σε Bitcoin, αναγκάστηκαν να αποζημιώσουν και να επιστρέψουν τα κρυπτονομίσματα αυτά σε όποιον τα έχασε για να μπορέσουν να διατηρήσουν την εμπιστοσύνη στην αγορά. Ενώ με ανακοίνωσή του ο ιδιοκτήτης του Silk Road 3.1 επισήμανε πως τα προσωπικά δεδομένων των χρηστών είναι κρυπτογραφημένα και ασφαλή και δεν έχουν διαρρεύσει. (reddit.com, 2016)

Να αναφέρουμε πως τόσο στον ιστότοπο του Silk Road 3.0 όσο και στον ιστότοπο του Silk Road 3.1 ήταν απαραίτητη τη χρήση του προγράμματος περιήγησης TOR από τους υποψήφιους αγοραστές και πωλητές προϊόντων.

Όπως παρουσιάζεται στην εικόνα 3.8, η λειτουργία της διαδικτυακής αγοράς αυτής ήταν ιδιαίτερα εύκολη. Οι χρήστες μπορούσαν να χρησιμοποιούν διάφορα φίλτρα αναζήτησης για να γίνει πιο εύκολη και γρήγορη η εύρεση των προϊόντων που επιθυμούσαν, όπως μεταξύ άλλων ήταν η κάνναβη, τα οπιοειδή, η έκσταση, η ηρωίνη, η κοκαΐνη, κλπ. Μερικά από αυτά μπορούμε να τα παρατηρήσουμε στην εικόνα 3.8 που ακολουθεί

**Εικόνα 3.8:** Μερικά από τα προϊόντα που εμπορεύονταν στο Silk Road 3.1

The screenshot shows the Silk Road 3.1 marketplace interface. At the top, there's a navigation bar with links like 'home', 'messages', 'notifications', 'profile', 'orders', 'support', 'settings', 'uchat', 'faq', 'forums', and 'logout'. Below this is a search bar and filters for 'Escrow' (Both), 'Ships From' (None Selected), and 'Order by' (Most active vendor). A 'Market News' section displays the current Bitcoin price: 1 BTC = 2361.31 USD. The 'Vendors News' section lists recent vendor announcements. The main content area shows a search for 'ALL' with a list of 15 items, each with a thumbnail, title, price, vendor, and category. A sidebar on the right lists various drug categories and their item counts, such as Cannabis (5502), Stimulants (2030), and Prescription (148).

Όπως μπορούμε να παρατηρήσουμε στην εικόνα 3.8, για κάθε αναφερόμενο προϊόν υπήρχαν πολλές πληροφορίες γύρω από αυτό. Για παράδειγμα υπήρχε μια αξιολόγηση για τους πωλητές με μια διαβάθμιση, το όνομα του προϊόντος, μια εικόνα για αυτό, η τιμή του σε δολάρια ΗΠΑ και σε Bitcoin, αλλά και η χώρα προέλευσης του.

Τέλος αυτό που αξίζει να σημειωθεί είναι πως με την άνοδο άλλων αγορών σκοτεινού δικτύου όπως η Agora και η AlphaBay, το Silk Road 3.1 δεν κατάφερε να φτάσει στο ίδιο επίπεδο δημοτικότητας με τις προηγούμενες εκδόσεις του και να συνεχίσει να φέρει τον χαρακτηρισμό ως το Amazon ή το eBay των ναρκωτικών (NPR Staff, 2012).

### 3.4 Συμπεράσματα τρίτου κεφαλαίου

Επειδή η γνώση του διαδικτύου από τον μέσο άνθρωπο είναι ιδιαίτερα περιορισμένη, υπάρχει ένα μυστικό μέρος του διαδικτύου που χρησιμοποιείται από εμπόρους ναρκωτικών, δολοφόνους και παιδόφιλους που ονομάζεται σκοτεινό διαδίκτυο. Σε αυτό το μέρος του διαδικτύου η πρόσβαση είναι αρκετά εύκολη καθώς μπορεί να προσεγγιστεί από οποιονδήποτε ο οποίος έχει ένα συμβατικό πρόγραμμα περιήγησης. Επειδή οι διαδικτυακές τοποθεσίες αυτές είναι πολύ καλά κλειδωμένες, χρειάζεται ένα ειδικό πρόγραμμα περιήγησης για να έχει κάποιος πρόσβαση σε αυτές. Τέτοια προγράμματα είναι τα δίκτυα TOR (The Onion Router) και TON (Telegram Open Network).

Το TOR είναι ένα πρωτόκολλο επικοινωνίας που έχει σχεδιαστεί για να προσφέρει ανωνυμία σε όσους το χρησιμοποιούν, το οποίο είναι αντίθετο με τα συμβατικά προγράμματα περιήγησης ιστού, όπως το Chrome και το Firefox, τα οποία δεν καταβάλλουν καμία προσπάθεια να αποκρύψουν τη θέση ή την ταυτότητα του κάθε χρήστη. Ενώ το TON είναι μια VPN η οποία έχει σχεδιαστεί για την εξάλειψη ζητημάτων απορρήτου όπως η χαμηλή ασφάλεια και η έλλειψη ανωνυμίας, με αποτέλεσμα να μπορεί να λειτουργήσει ως τρόπος εκπλήρωσης παράνομων δραστηριοτήτων.

Οι πλατφόρμες αυτές χρησιμοποιούν κυρίως τα κρυπτονομίσματα για την διενέργεια των πληρωμών μεταξύ των αντισυμβαλλόμενων ατόμων όπως είναι το Bitcoin, όμως δεν χρησιμοποιούν αποκλειστικά τα κρυπτονομίσματα αυτά κάθε αυτά, καθώς εκμεταλλεύονται την τεχνολογία του blockchain συνολικά. Για παράδειγμα πολλά παράνομα καταστήματα πώλησης ναρκωτικών λειτουργούν μέσω του Blockchain DNS, το οποίο χρησιμοποιεί το Namecoin και το Emercoin για την προστασία των αγορών αυτών για να διασφαλίσει την ακεραιότητα των συναλλαγών των πελατών τους.

Μια πολύ χαρακτηριστική διαδικτυακή αγορά πώλησης παράνομων προϊόντων, η οποία ήταν και η πρώτη που εμφανίστηκε, ήταν το Silk Road που στα Ελληνικά θα μπορούσε να μεταφραστεί ως «Ο Δρόμος του μεταξιού» το Silk Road προσέφερε την επιλογή να μπορούν να γίνονται αγορές, πωλήσεις αλλά και διαφημίσεις με ανώνυμο τρόπο και οι αγοροπωλησίες να πραγματοποιούνται κυρίως σε κρυπτονομίσματα και μάλιστα σε Bitcoin και όχι σε fiat νομίσματα επειδή προσέφεραν μεγάλο βαθμό ανωνυμίας στο δίκτυο.



Το Silk Road εμφανίστηκε πρώτη φορά το 2011 και αποτελούσε ένα δικτυακό ιστότοπο που δραστηριοποιούνταν στο σκοτεινό διαδίκτυο και εμπορεύονταν προϊόντα όπως ναρκωτικά και όπλα. Μετά από προσπάθειες των κυβερνητικών αρχών το 2013 σταμάτησε η λειτουργία του. Όμως, στις 6 Νοεμβρίου του 2013, περίπου ένα μήνα μετά το κλείσιμο του πρώτου ιστότοπου, ξεκίνησαν εκ νέου την ιστοσελίδα με την ονομασία Silk Road 2.0. Η συγκεκριμένη είχε βελτιωμένη ασφάλεια και τεχνολογία, ώστε να επιτρέπεται η γρήγορη αναδημιουργία του σε περίπτωση άλλου τερματισμού του όπως του προηγούμενου ιστότοπου. Παρόλα αυτά τον Νοέμβριο του 2014, οι κυβερνητικές αρχές σε συνεργασία με το FBI, την Ευροpol και το Eurojust ανακοίνωσαν το κλείσιμο του ιστότοπου. Μετά το κλείσιμο του Silk Road 2.0. και πάλι τον Νοέμβρη του 2014, η Diabolus Market μετονομάστηκε σε «Silk Road 3.0 Reloaded» για να αξιοποιήσει το εμπορικό όνομα που είχε δημιουργηθεί τα προηγούμενα χρόνια στον χώρο αυτό. Και ο συγκεκριμένος ιστότοπος ήταν μια αγορά στο σκοτεινό διαδίκτυο που πωλούσε κυρίως παράνομα αγαθά καθώς και υπηρεσίες, συμπεριλαμβανομένων και των ναρκωτικών, με τις πληρωμές να συνεχίζονται να γίνονται μέσω Bitcoin. Τέλος το έτος 2016 έκανε την εμφάνιση του το Silk Road 3.1., το οποίο αποτελούσε την επανεκκίνηση του Silk Road 3.0. Παρά το γεγονός ότι όλα τα Silk Road έκλειναν μετά από κάποιο διάστημα, ο διαχειριστής του Silk Road 3.1 επισήμανε πως με την επαναλειτουργία του το 2016 κέρδιζε τρεις νέους χρήστες κάθε λεπτό. Βέβαια με την άνοδο άλλων αγορών σκοτεινού δικτύου όπως η Agora και η AlphaBay, το Silk Road 3.1 δεν κατάφερε να φτάσει στο ίδιο επίπεδο δημοτικότητας με τις προηγούμενες εκδόσεις του και να συνεχίσει να φέρει τον χαρακτηρισμό ως το Amazon ή το eBay των ναρκωτικών.

## **Κεφάλαιο 4: Μέτρα αντιμετώπισης και περιορισμού του σκοτεινού διαδικτύου από τις παγκόσμιες ρυθμιστικές αρχές**

### **4.1 Εισαγωγή τέταρτου κεφαλαίου**

Στο τέταρτο κεφάλαιο της διπλωματικής εργασίας αναλύονται μέτρα και ενέργειες που έχουν ακολουθηθεί από ρυθμιστικούς οργανισμούς παγκοσμίως για τον περιορισμό της δραστηριότητας του σκοτεινού διαδικτύου. Αναλυτικότερα παρουσιάζονται μηχανισμοί και τεχνικές που ακολουθούνται από τις ρυθμιστικές αρχές σε όλο τον κόσμο οι οποίες ανησυχούν όλο και περισσότερο για το ρόλο των κρυπτονομισμάτων στη νομιμοποίηση εσόδων από παράνομες δραστηριότητες αλλά και τη γενικότερη χρηματοδότηση τους εντός του σκοτεινού διαδικτύου.

Πιο συγκεκριμένα το κεφάλαιο επικεντρώνεται στις δράσεις της INTERPOL και της Europol που ακολουθούν για να αντιμετωπίσουν την επέκταση του σκοτεινού διαδικτύου όπως είναι μεταξύ άλλων το εργαλείο GraphSense, το Darkweb MoniTOR, το πρόγραμμα IOCTA, κλπ.

## 4.2 Τα πρώτα βήματα καταπολέμησης του σκοτεινού διαδικτύου από τις ρυθμιστικές αρχές

Οι ρυθμιστικές αρχές σε όλο τον κόσμο ανησυχούν όλο και περισσότερο για το ρόλο των κρυπτονομισμάτων στη νομιμοποίηση εσόδων από παράνομες δραστηριότητες αλλά και τη γενικότερη χρηματοδότηση τους. Σύμφωνα με το World Economic Forum (2020), από τις αρχές του 2020, πολλές κυβερνήσεις έχουν αρχίσει να καταπολεμούν ενεργά αυτήν την κατάσταση και έχουν εισαγάγει διάφορα νομικά μέτρα που αποσκοπούν στην ενίσχυση της προστασίας της κάθε χώρας έναντι του οικονομικού εγκλήματος στον κυβερνοχώρο.

Αναλυτικότερα, όπως αναφέρεται από τους ειδικούς του Chainalysis.com (2020), ο αριθμός των χρηστών που δραστηριοποιείται στο Darknet συνδέεται άμεσα με το πόσο αυστηρές είναι οι κυβερνητικές πολιτικές της εκάστοτε χώρας προς το διαδίκτυο και γενικότερα προς τον κυβερνοχώρο. Συνεπώς, οι χώρες στις οποίες το σκοτεινό διαδίκτυο χρησιμοποιείται περισσότερο, είναι κυρίως οι Ηνωμένες Πολιτείες, η Ρωσία και ορισμένες Ευρωπαϊκές χώρες όπως η Γερμανία, η Ολλανδία και η Γαλλία. Για τον λόγο αυτό οι χώρες αυτές έκαναν κάποιες ενέργειες για τον περιορισμό της δραστηριότητας αυτής, όπου με βάση την OzelliS. (2020) είναι οι ακόλουθες. Για παράδειγμα, η Ρωσία εισήγαγε με περιοδικό τρόπο μέσω της Κεντρικής της τράπεζας αυστηρές συστάσεις σχετικά με τον τρόπο με τον οποίο τα χρηματοπιστωτικά ιδρύματα πρέπει να εντοπίζουν ύποπτες συναλλαγές συμπεριλαμβανομένων εκείνων με κρυπτονομίσματα. Ενώ όσον αφορά στις ρυθμιστικές αρχές των ΗΠΑ, δημιούργησαν ένα πρόγραμμα πληροφοριών κρυπτογράφησης τον Μάρτιο του 2020 που πρότεινε νέους κανόνες και απαιτήσεις φορολογικής αναφοράς για να ανοίξουν τον δρόμο για την ευρεία υιοθέτηση της τεχνολογίας του blockchain.

Ένα πολύ γνωστό παράδειγμα επιτυχημένης επιχείρησης περιορισμού του σκοτεινού διαδικτύου είναι η επιχείρηση Onymous. Σύμφωνα με τον Higgins S. (2014), τουλάχιστον 400 διαδικτυακοί ιστότοποι σκοτεινού δικτύου και 17 άτομα συνελήφθησαν στην επιχείρηση αυτή η οποία πραγματοποιήθηκε με σκοπό την παγκόσμια καταστολή εγκλήματος στον κυβερνοχώρο στις 7 Νοεμβρίου του 2014. Ένας μεγάλος αριθμός σκοτεινών αγορών στο διαδίκτυο που ήταν κυρίως προσβάσιμοι μέσω του δικτύου TOR , όπως και το Silk Road 2.0 σταμάτησαν την λειτουργία τους. Με βάση τις δηλώσεις του επικεφαλής της Europol του τμήματος European Cybercrime Centre (EC3) Troels Oerting, ανέφερε πως οι εγκληματικές αυτές οργανώσεις μπορεί να υφίστανται και να υπάρχει η δραστηριοποίησή τους,

όμως δεν μπορούν να μην βγουν στην ανακαλυφθούν και θα καταβληθούν προσπάθειες για τον περαιτέρω περιορισμό τους.

Αυτό που αξίζει να αναφερθεί είναι πως στην συγκεκριμένη επιχείρηση μεταξύ των συλληφθέντων είναι και ο προγραμματιστής Blake Benthall, ο οποίος ομολόγησε πως ήταν ο διαχειριστής του ιστότοπου Silk Road 2.0. Ενώ το σημαντικό είναι να αναδειχτεί πως διάφορες κυβερνητικές αρχές όπως η Εθνική Υπηρεσία Εγκλήματος του Ηνωμένου Βασιλείου (UK National Crime Agency - NCA) δημοσίευσε σε δήλωση της στις 7 Νοεμβρίου του 2014, ότι είχε συντονιστεί με άλλους κυβερνητικούς οργανισμούς για τη σύλληψη έξι ατόμων στην Ουαλία, στο Λίνκολνσαϊρ και στο Λίβερπουλ στην έρευνα που πραγματοποιήθηκε. Ενώ αναφέρθηκε πως οι συλλήψεις ήταν μέρος μιας ευρύτερης προσπάθειας που ξεκίνησε μετά το κλείσιμο της αρχικής αγοράς Silk Road το προηγούμενο έτος.

Παρά το γεγονός πως η επιχείρηση αυτή οδήγησε στο να τερματιστεί η λειτουργία για πολλούς παράνομους ιστότοπους, είναι γεγονός πως πολλοί συνεχίζουν να λειτουργούν και το οικοσύστημα της αγοράς σκοτεινού διαδικτύου δεν θα περιοριστεί εύκολα. Ένα μεγάλο ερώτημα που βγαίνει στην επιφάνεια είναι πως θα μπορέσουν οι υπηρεσίες και οι αρχές επιβολής του νόμου να περιορίσουν και να παρακολουθήσουν τις δραστηριότητες που γίνονται στο TOR δίκτυο.

### 4.3 Δράσεις της INTERPOL και της Europol για την αντιμετώπιση του σκοτεινού διαδικτύου παγκοσμίως

Γεγονός είναι πως το σκοτεινό διαδίκτυο αποτελεί ένα μεγάλο τμήμα του διαδικτύου που γνωρίζουμε, στο οποίο υπάρχει πρόσβαση μέσω χρήσης εξειδικευμένου λογισμικού. Σε αυτό γίνεται χρήση των κρυπτονομισμάτων καθώς έχουν πολλά θετικά οφέλη γιατί εστιάζουν στην ανωνυμία και γίνεται κατάχρησή τους από τους εγκληματίες. Η παράνομη πώληση ναρκωτικών, πυροβόλων όπλων και εκρηκτικών, το λαθρεμπόριο ανθρώπων, η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, οι τρομοκρατικές δραστηριότητες και το έγκλημα στον κυβερνοχώρο αποτελούν μερικά παραδείγματα δραστηριοτήτων που διευκολύνονται μέσω του σκοτεινού διαδικτύου. Για όλους τους παραπάνω λόγους σύμφωνα με τον επίσημο ηλεκτρονικό ιστότοπο του Διεθνούς Οργανισμού Εγκληματικής Αστυνομίας (International Criminal Police Organization) γνωστού και ως INTERPOL αναπτύσσονται διάφορες δράσεις για να περιοριστεί η εγκληματική δραστηριότητα στο σκοτεινό διαδίκτυο και να βοηθηθούν οι αστυνομικές αρχές σε παγκόσμιο επίπεδο για να είναι σε θέση να διερευνήσουν τα ψηφιακά εγκλήματα με περισσότερο αποτελεσματικό τρόπο.

Αρχικά, η INTERPOL ανέπτυξε ένα πρόγραμμα με το όνομα TITANIUM, που χρηματοδοτείται από την Ευρωπαϊκή Ένωση, στο οποίο αναπτύχθηκε ένα εργαλείο το οποίο ονομάζεται GraphSense το οποίο εντοπίζει τις συναλλαγές που γίνονται μέσω κρυπτονομισμάτων. Αυτό το εργαλείο επιτρέπει στους ερευνητές να αναζητούν διευθύνσεις κρυπτονομισμάτων και να ακολουθούν την πορεία που ακολουθούν τα χρήματα που έχουν μετατραπεί σε κρυπτονομίσματα.

Επίσης με βάση μια ανάγκη που εντοπίστηκε από τις χώρες μέλη της Ε.Ε., η INTERPOL αναπτύσσει ένα ακόμα εργαλείο που ονομάζεται Darkweb MoniTOR , το οποίο συλλέγει δεδομένα σχετικά με εγκληματικές δραστηριότητες και θα το χρησιμοποιεί για να υποστηρίζει τις αστυνομικές έρευνες παγκοσμίως. Τα δεδομένα και η επακόλουθη ανάλυση τους θα βοηθήσουν επίσης στον εντοπισμό νέων τάσεων στο σκοτεινό διαδίκτυο, αλλά και στην παροχή συμβουλών για δραστηριότητες πρόληψης . Τα δεδομένα που αναλύει το εργαλείο είναι οι ηλεκτρονικές διευθύνσεις των κρυπτονομισμάτων, τα PGP (Pretty Good Privacy encryption program), τα διαδικτυακά ονόματα των χρηστών και τα ψευδώνυμα τους, οι διευθύνσεις ηλεκτρονικού ταχυδρομείου, οι ηλεκτρονικές διευθύνσεις των αγορών σκοτεινού διαδικτύου, τα φόρουμ επικοινωνίας στο σκοτεινό διαδίκτυο και τέλος μια ιστορική ανάλυση δεδομένων απ' όλο το σκοτεινό διαδίκτυο από το 2015 μέχρι σήμερα.

Μία ακόμα παρέμβαση που κάνει η INTERPOL είναι να πραγματοποιεί μια ταξινόμηση του σκοτεινού διαδικτύου και των κρυπτονομισμάτων. Ομάδες έρευνας και επέμβασης που ειδικεύονται σε έρευνες για το σκοτεινό διαδίκτυο και τα κρυπτονομίσματα έχουν σχεδιάσει μια παγκόσμια ταξινόμηση κρυπτονομισμάτων που καθορίζουν ποιες κατηγορίες δεδομένων από ύποπτες συναλλαγές κρυπτονομισμάτων πρέπει να ελεγχθούν. Αυτά τα δεδομένα περιλαμβάνουν για παράδειγμα την αναφορά στα κρυπτονομίσματα που ανταλλάσσονται περισσότερο, αλλά και τον τύπο της εγκληματικής δραστηριότητας που συνδέονται οι συναλλαγές με αυτά.

Το σχέδιο της ταξινόμησης αυτής επικεντρώνεται σε τρεις κατηγορίες πληροφοριών. Πρώτον, στις Οντότητες, δηλαδή στα άτομα και στις οργανώσεις. Δεύτερον, στις υπηρεσίες, δηλαδή στις σκοτεινές αγορές, στις ανταλλαγές μεταξύ κρυπτονομισμάτων, στα μηνύματα επικοινωνίας αλλά και σε άλλες υπηρεσίες που συνδέονται με τις συναλλαγές. Τρίτον, με τον τύπο της εγκληματικής δραστηριότητας, δηλαδή με ποια εγκλήματα σχετίζεται η συναλλαγή, όπως για παράδειγμα πωλήσεις ναρκωτικών ή όπλων, σεξουαλική κακοποίηση παιδιών, τρομοκρατία, εγκλήματα στον κυβερνοχώρο κλπ.

Επίσης η INTERPOL δραστηριοποιείται στο κομμάτι της υποστήριξης διαδικτυακών αντιτρομοκρατικών ερευνών. Με το πρόγραμμα CaraCT, το οποίο διαχειρίζεται το Κέντρο Καινοτομίας της INTERPOL και υποστηρίζεται από το Υπουργείο Εξωτερικών της Ολλανδίας καταρτίζει ένα «Εγχειρίδιο» για να βοηθήσει την επιβολή του νόμου στη Νοτιοανατολική Ασία να αντιμετωπίσει την κατάχρηση του σκοτεινού διαδικτύου και των κρυπτονομισμάτων από τρομοκράτες.

Το «Εγχειρίδιο» αυτό αποσκοπεί να παρέχει στους χρήστες οδηγίες για την επιβολή του νόμου, για την διερεύνηση τρομοκρατικών δραστηριοτήτων στο σκοτεινό διαδίκτυο αλλά και πληροφορίες χρήσης των κρυπτονομισμάτων για αυτές τις ενέργειες. Επίσης, θα περιγράψει διάφορα εργαλεία, μεθοδολογίες και διαδικασίες για την ανάλυση πληροφοριών που συνδέονται με την διαδικτυακή τρομοκρατία, καθώς και προκλήσεις που ενδέχεται να αντιμετωπίσουν οι ερευνητές.

Ουσιαστικά με τις πληροφορίες που περιέχονται στο εγχειρίδιο, η INTERPOL θα βοηθήσουν να αναπτυχθούν μαθήματα κατάρτισης των ειδικών σε θέματα διαδικτυακού εγκλήματος σε παγκόσμιο επίπεδο, αλλά και άλλες πρωτοβουλίες. Μερικές από αυτές είναι οι διαδικτυακές πλατφόρμες εκπαίδευσης που βασίζονται σε προσομοίωση των αγορών του σκοτεινού διαδικτύου, αναπαράσταση των φόρουμ

του σκοτεινού διαδικτύου, αλλά και εκπαίδευση για τον εντοπισμό συστημάτων συναλλαγών κρυπτογράφησης που ενισχύουν την ανωνυμία.

Επιπρόσθετα, η INTERPOL και το Υπουργείο Δικαιοσύνης της Βαυαρίας οργανώνουν ομάδες εργασιών και ομάδες δράσης οι οποίες αποτελούνται από εμπειρογνώμονες για το σκοτεινό διαδίκτυο και τα κρυπτονομίσματα για να μοιραστούν μεθοδολογίες και εργαλεία για τον εντοπισμό εγκληματιών που επωφελούνται από την ανωνυμία των κρυπτονομισμάτων και του σκοτεινού διαδικτύου. Μεταξύ των μεθοδολογιών περιλαμβάνονται βέλτιστες πρακτικές σε διαδικτυακές έρευνες, πρότυπα αντιμετώπισης και επιβολής του νόμου. Οι ομάδες αυτές επικεντρώνονται αρχικά στην δημιουργία μιας διεθνούς βάσης δεδομένων με ψηφιακά πορτοφόλια κρυπτονομισμάτων που χρησιμοποιούνται σε εγκληματικές δραστηριότητες. Επίσης στην δόμηση μιας ενοποιημένης βάσης δεδομένων σε αναφορές στα κρυπτονομίσματα που μέσω αναλύσεων μπορούν να βοηθήσουν και να εξελίξουν τις έρευνες γύρω από το σκοτεινό διαδίκτυο. Ακόμη στον καθορισμό τυποποιημένων λέξεων και εκφράσεων που χρησιμοποιούνται στις κοινότητες του σκοτεινού διαδικτύου. Και τέλος στην προώθηση ατόμων με ειδικές γνώσεις γύρω από τον προγραμματισμό και τα νομικά θέματα για να υποστηρίξουν και να καθοδηγήσουν τις προσπάθειες αυτές.

Τέλος, όπως αναφέρεται από τον HaigS. (2020), στα τέλη του Μαρτίου του 2020 μια ακόμα συνεργασία της INTERPOL είναι η συνεργασία με το S2W Lab της Νότιας Κορέας με στόχο την ανάλυση της δραστηριότητας στο σκοτεινό διαδίκτυο συμπεριλαμβανομένων των συναλλαγών με κρυπτονομίσματα. Φυσικά αυτό που αξίζει να αναφέρουμε είναι πως οι χρήστες του σκοτεινού διαδικτύου τείνουν να βρίσκουν νέους τρόπους συνέχισης των παράνομων δραστηριοτήτων τους ξεπερνώντας τους περιορισμούς από τις ρυθμιστικές αρχές.

Όσον αφορά την Europol, η οποία αποτελεί τον οργανισμό της Ευρωπαϊκής Ένωσης που βοηθά τις εθνικές αρχές επιβολής του νόμου στην καταπολέμηση του σοβαρού διεθνούς εγκλήματος και της τρομοκρατίας, με πρόσφατα στοιχεία του 2020 δραστηριοποιείται και αυτή ως οργανισμός ενεργά στην καταπολέμηση και στον εντοπισμό των παράνομων δραστηριοτήτων στον κυβερνοχώρο. (europa.eu, 2021, europol.europa.eu, 2020)

Αναλυτικότερα, μέσω του προγράμματος IOCTA, το οποίο είναι ένα εμβληματικό στρατηγικό προϊόν της Europol που επισημαίνει τις δυναμικές και εξελισσόμενες απειλές από το έγκλημα στον κυβερνοχώρο, παρέχει μια μοναδική επιβολή του νόμου στις αναδυόμενες προκλήσεις και τις βασικές εξελίξεις στον χώρο

του εγκλήματος στον κυβερνοχώρο. Ουσιαστικά εκτιμάει απειλές και τάσεις, καθώς και προκλήσεις όπως είναι η εγκληματική κατάχρηση κρυπτονομισμάτων.

Αυτό που είναι ιδιαίτερα αξιοσημείωτο είναι πως η συλλογή δεδομένων για το IOCTA 2020, πραγματοποιήθηκε κατά την διάρκεια του lockdown που εφαρμόστηκε ως μέτρο για τον περιορισμό της πανδημίας COVID-19. Και αυτό επειδή η πανδημία προκάλεσε σημαντική αλλαγή στην αύξηση της εγκληματικής δραστηριότητας στον κυβερνοχώρο, οι εγκληματίες επινόησαν νέους τρόπους επίθεσης αλλά και απάτης σε διάφορες ομάδες ανθρώπων.

Με βάση την μελέτη της Europol με τίτλο Internet Organised Crime Threat Assessment (2020), το IOCTA 2020 συνέβαλε στον καθορισμό των προτεραιοτήτων για το επιχειρησιακό σχέδιο δράσης του 2021 ακολουθώντας τρεις προτεραιότητες. Αρχικά, την διακοπή εγκληματικών δραστηριοτήτων που σχετίζονται με επιθέσεις εναντίον συστημάτων πληροφοριών και συστημάτων που προωθούν το διαδικτυακό έγκλημα. Επίσης, την καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών, συμπεριλαμβανομένης της παραγωγής και διάδοσης πορνογραφικού υλικού. Ενώ τέλος, στοχεύει τους εγκληματίες που εμπλέκονται σε απάτες και παραχαράξεις μέσω πληρωμής χωρίς την χρήση μετρητών συμπεριλαμβανομένης της απάτης σε πιστωτικές κάρτες, αναδυόμενες απειλές για άλλα μέσα πληρωμής χωρίς μετρητά που επιτρέπουν εγκληματικές δραστηριότητες. Επιπλέον, το πρόγραμμα IOCTA στοχεύει στην ενοποίηση των ευρημάτων σχετικά με τις τρέχουσες απειλές στον κυβερνοχώρο, οι οποίες θα μπορούσαν να συμβάλουν στη συζήτηση των προτεραιοτήτων έρευνας και ανάπτυξης καθώς και στον προγραμματισμό σε επίπεδο Ευρωπαϊκής Ένωσης.



## 4.4 Συμπεράσματα τέταρτου κεφαλαίου

Οι ρυθμιστικές αρχές σε όλο τον κόσμο ανησυχούν όλο και περισσότερο για την εξάπλωση του σκοτεινού διαδικτύου σε παγκόσμιο επίπεδο. Ο αριθμός των χρηστών που δραστηριοποιείται στο Darknet συνδέεται άμεσα με το πόσο αυστηρές είναι οι κυβερνητικές πολιτικές της εκάστοτε χώρας προς το διαδίκτυο και γενικότερα προς τον κυβερνοχώρο. Συνεπώς οι χώρες στις οποίες το σκοτεινό διαδίκτυο χρησιμοποιείται περισσότερο είναι κυρίως οι Ηνωμένες Πολιτείες, η Ρωσία και ορισμένες Ευρωπαϊκές χώρες όπως η Γερμανία, η Ολλανδία και η Γαλλία άρα και η εξάπλωση του είναι μεγαλύτερη.

Ένα μεγάλο ερώτημα που βγαίνει στην επιφάνεια είναι πως θα μπορέσουν οι υπηρεσίες και οι αρχές επιβολής του νόμου να περιορίσουν και να παρακολουθήσουν τις δραστηριότητες που γίνονται στο Darkweb καθώς χρησιμοποιούν τα κρυπτονομίσματα για τις συναλλαγές τους. Μέσω των κρυπτονομισμάτων οι χρήστες του έχουν θετικά οφέλη γιατί εστιάζουν στην ανωνυμία που προσφέρουν και γίνεται καταχρηστική χρήση τους από τους εγκληματίες. Η παράνομη πώληση ναρκωτικών, πυροβόλων όπλων και εκρηκτικών, το λαθρεμπόριο ανθρώπων, η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, οι τρομοκρατικές δραστηριότητες και το έγκλημα στον κυβερνοχώρο αποτελούν μερικά παραδείγματα δραστηριοτήτων που διευκολύνονται μέσω του σκοτεινού διαδικτύου και αρχές καλούνται να αντιμετωπίσουν.

Τόσο η INTERPOL όσο και η Europol, που αποτελούν οργανισμούς που βοηθούν τις εθνικές αρχές επιβολής του νόμου στην καταπολέμηση του σοβαρού διεθνούς εγκλήματος και της τρομοκρατίας έχουν δημιουργήσει μια σειρά από μηχανισμούς και επιχειρήσεις περιορισμού των δραστηριοτήτων αυτών. Αναπτύσσονται διάφορες δράσεις για να περιοριστεί η εγκληματική δραστηριότητα στο σκοτεινό διαδίκτυο και να βοηθηθούν τις αστυνομικές αρχές σε παγκόσμιο επίπεδο για να είναι σε θέση να διερευνήσουν τα ψηφιακά εγκλήματα με περισσότερο αποτελεσματικό τρόπο.

Ένα από τα πρώτα πολύ γνωστά παραδείγματα επιτυχημένης επιχείρησης περιορισμού του σκοτεινού διαδικτύου είναι η επιχείρηση Onymous που έγινε το 2014 και μεταξύ των συλληφθέντων ήταν και ο διαχειριστής του ιστότοπου Silk Road 2.0.

Φυσικά από τότε μέχρι σήμερα έχουν πραγματοποιηθεί πολλές επιχειρήσεις αλλά και αναπτυχθεί πολλά προγράμματα που έχουν ως στόχο τον σκοπό αυτό. Για

παράδειγμα από την πλευρά της INTERPOL είναι το πρόγραμμα με το όνομα TITANIUM, που χρηματοδοτείται από την Ευρωπαϊκή Ένωση, στο οποίο αναπτύχθηκε ένα εργαλείο το οποίο εντοπίζει τις συναλλαγές που γίνονται μέσω κρυπτονομισμάτων και επιτρέπει στους ερευνητές να αναζητούν διευθύνσεις κρυπτονομισμάτων και να ακολουθούν την πορεία που ακολουθούν τα χρήματα που έχουν μετατραπεί σε κρυπτονομίσματα. Επίσης το πρόγραμμα Darkweb MoniTOR, το οποίο συλλέγει δεδομένα σχετικά με εγκληματικές δραστηριότητες και θα τα χρησιμοποιεί για να υποστηρίξει τις αστυνομικές έρευνες παγκοσμίως εντοπίζοντας ηλεκτρονικές διευθύνσεις κρυπτονομισμάτων, τα διαδικτυακά ονόματα των χρηστών, τα ψευδώνυμα τους, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, κλπ με ιστορική ανάλυση δεδομένων απ' όλο το σκοτεινό διαδίκτυο από το 2015 μέχρι σήμερα. Επίσης να αναφερθούμε στο CaraCT, το οποίο διαχειρίζεται το Κέντρο Καινοτομίας της INTERPOL και υποστηρίζεται από το Υπουργείο Εξωτερικών της Ολλανδίας καταρτίζει ένα «Εγχειρίδιο» για να βοηθήσει την επιβολή του νόμου στη Νοτιοανατολική Ασία να αντιμετωπίσει την κατάχρηση του σκοτεινού διαδικτύου και των κρυπτονομισμάτων από τρομοκράτες.

Ενώ τέλος όσον αφορά τις δράσεις της Europol, μέσω του προγράμματος IOCTA, εκτιμώνται οι απειλές και οι τάσεις, καθώς και οι προκλήσεις όπως είναι η εγκληματική κατάχρηση κρυπτονομισμάτων. Η συλλογή δεδομένων για το IOCTA 2020, πραγματοποιήθηκε κατά την διάρκεια του lockdown που εφαρμόστηκε ως μέτρο για τον περιορισμό της πανδημίας COVID-19 και αυτό επειδή η πανδημία προκάλεσε σημαντική αλλαγή στην αύξηση της εγκληματικής δραστηριότητας στον κυβερνοχώρο, με τους εγκληματίες να επινοούν νέους τρόπους επιθέσεων αλλά και απατηλών πράξεων σε διάφορες ομάδες ανθρώπων.

## **Κεφάλαιο 5: Τα κυριότερα κρυπτονομίσματα που χρησιμοποιούνται στο σκοτεινό διαδίκτυο**

### **5.1 Εισαγωγή πέμπτου κεφαλαίου**

Στο σημείο αυτό της διπλωματικής εργασίας με βάση τα στοιχεία που αναλύθηκαν και ερευνήθηκαν στα προηγούμενα κεφάλαια μέσω της βιβλιογραφικής ανασκόπησης γύρω από το σκοτεινό διαδίκτυο και την χρήση των κρυπτονομισμάτων σε αυτό, ακολουθεί μια σύντομη ανάλυση γύρω από τα κυριότερα εξ αυτών που χρησιμοποιούνται στο Dark web. Στόχος της ανάλυσης αυτής είναι να γίνει μια σύντομη καταγραφή και ανάλυση των κρυπτονομισμάτων αυτών, αναδεικνύοντας στοιχεία για αυτά όπως το έτος δημιουργίας τους, γενικά χαρακτηριστικά της τεχνολογίας τους, το επίπεδο ανωνυμίας που προσφέρουν, η διαγραμματική απεικόνιση της πορείας της τιμής τους κλπ.

Στα κρυπτονομίσματα που αναλύονται στην συνέχεια περιλαμβάνεται τα πιο γνωστά και δημοφιλέστερα απ' όλα, το οποίο είναι το Bitcoin, το δεύτερο πιο γνωστό και μεγαλύτερο σε χρηματιστηριακή κεφαλαιοποίηση παγκοσμίως το Ethereum, κάποια κρυπτονομίσματα που ήταν ιδιαίτερα δημοφιλή τα προηγούμενα χρόνια και γνωστά στο ευρύ επενδυτικό και όχι μόνο κοινό, τα οποία είναι το Monero, το Zcash, το Dash και το Litecoin, αλλά και κάποια λιγότερο γνωστά και δημοφιλή που είναι το Namecoin και το Emercoin, τα οποία σύμφωνα με πρόσφατες έρευνες αρχίζουν και κερδίζουν μερίδιο στις συναλλαγές εντός του σκοτεινού διαδικτύου. Να αναφέρουμε πως το κοινό χαρακτηριστικό όλων των παραπάνω κρυπτονομισμάτων είναι η διατήρηση του επιπέδου ανωνυμίας που προσφέρει στους χρήστες του, γεγονός ιδανικό για την χρήση τους για συναλλαγές σε παράνομες δραστηριότητες όπως αγορές ή πωλήσεις ναρκωτικών, όπλων, υλικού πορνογραφίας εντός του σκοτεινού διαδικτύου.

## 5.2 Αναφορά στα κυριότερα κρυπτονομίσματα που χρησιμοποιούνται στο σκοτεινό διαδίκτυο

### 5.2.1 Αναφορά στο κρυπτονόμισμα Bitcoin

Το κρυπτονόμισμα Bitcoin σύμφωνα με το Coingecko.com (20.04.2021) είχε χρηματιστηριακή κεφαλαιοποίηση \$1.038.017.444.488 δολάρια κατέχοντας την πρώτη θέση στην παγκόσμια αγορά κρυπτονομισμάτων με συνολικά το 50,06% αυτής. Η ιστορικά υψηλότερη τιμή του ήταν τα \$64.804,72 στις 14 Απριλίου 2021. Στο διάγραμμα 5.1 μπορούμε να παρατηρήσουμε την εξέλιξη της πορείας της τιμής του από την 1/1/2017 έως τις 30/3/2021.

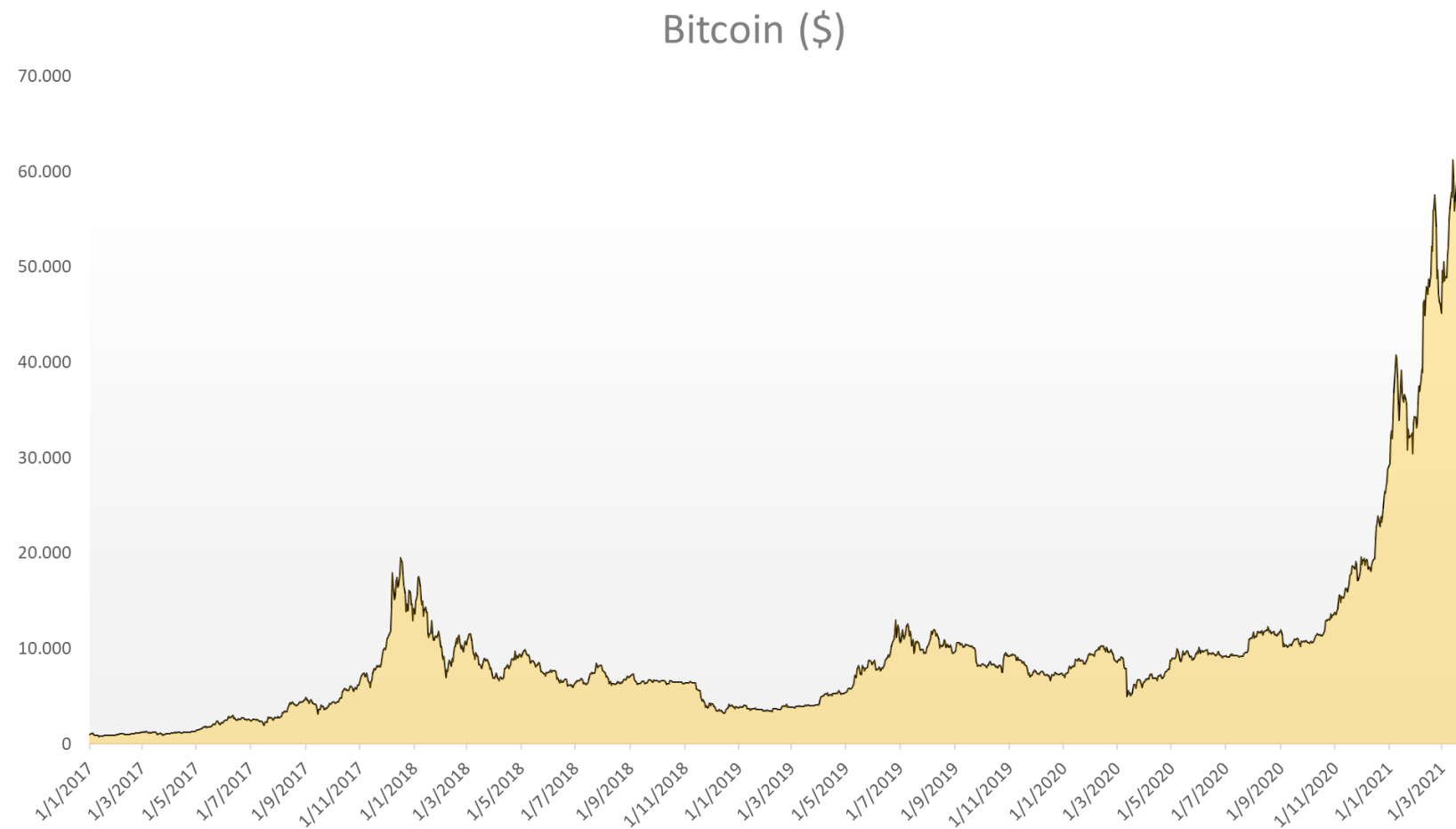
Σύμφωνα με το Coinmarketcap.com/Bitcoin (2021) και το Coingecko.com/Bitcoin (2021), το Bitcoin συμβολίζεται με τα αρχικά BTC και ανήκει στην οικογένεια των κρυπτονομισμάτων. Είναι ένα αποκεντρωμένο ψηφιακό νόμισμα που βασίζεται στην κρυπτογραφία. Ως εκ τούτου, μπορεί να λειτουργεί χωρίς την ανάγκη παρεμβολής κάποιου κεντρικής αρχής όπως μίας κεντρικής τράπεζας ή μιας εταιρείας. Αυτό το γεγονός είναι αντίθετο με τα νομίσματα που εκδίδονται από μια κυβέρνηση τα οποία ονομάζονται fiat νομίσματα, όπως για παράδειγμα είναι το ευρώ ή το δολάριο καθώς ελέγχονται από την κεντρική αυτή αρχή. Η αποκεντρωμένη φύση του επιτρέπει να λειτουργεί σε ένα δίκτυο peer-to-peer όπου οι χρήστες του είναι σε θέση να στέλνουν χρήματα ο ένας στον άλλο χωρίς να παρεμβάλουν κάποιον άλλο ενδιάμεσο.

Ο δημιουργός του Bitcoin μέχρι και σήμερα είναι ένα άγνωστο άτομο ή ομάδα ατόμων που έχουν το όνομα ή το ψευδώνυμο όνομα Satoshi Nakamoto. Ο συγκεκριμένος ήταν ο πρώτος που είχε την ιδέα ενός peer-to-peer συστήματος συναλλαγών όπως το περιέγραψε στο έγγραφο δημιουργίας του Bitcoin (white paper). Μέχρι σήμερα, η πραγματική ταυτότητα του Satoshi Nakamoto δεν έχει επαληθευτεί.

Μπορεί κατά το παρελθόν να υπήρχαν παρόμοιες ιδέες για την δημιουργία ενός αποκεντροποιημένου δικτύου ηλεκτρονικών συναλλαγών, αλλά το Bitcoin αποτελεί το πρώτο ιστορικά κρυπτονόμισμα που έκανε την ιδέα αυτή πράξη. Πρωτοεμφανίστηκε τον Ιανουάριο του 2009 με το πρώτο του block στο blockchain να ονομάζεται genesis block, το οποίο εξορύχθηκε στις 9 Ιανουαρίου του 2009. Με το πέρασμα των χρόνων ένας μεγάλος αριθμός ατόμων συνέβαλε στη βελτίωση του λογισμικού κρυπτογράφησης του, διορθώνοντας παράλληλα ευπάθειες στο λογισμικό του και προσθέτοντας νέες δυνατότητες. Η φύση της τεχνολογίας του το

έκανε από την πρώτη στιγμή να αποτελεί ιδανικό μέσο πληρωμών στο σκοτεινό διαδίκτυο.

**Διάγραμμα 5.1:** Η πορεία της τιμής του Bitcoin από την 1/1/2017 έως τις 30/3/2021



Πηγή

Δεδομένων

coinmarketcap.com

(Ημερήσια

στοιχεία

### 5.2.2 Αναφορά στο κρυπτονόμισμα Ethereum

Το κρυπτονόμισμα Ethereum σύμφωνα με το Coingecko.com (20.04.02021) είχε τιμή \$2,450,84 και χρηματιστηριακή κεφαλαιοποίηση \$281.377.001.276 δολάρια κατέχοντας την δεύτερη θέση στην παγκόσμια αγορά κρυπτονομισμάτων με συνολικά το 13,09% αυτής. Η ιστορικά υψηλότερη τιμή του ήταν τα \$2.544,30 στις 16 Απριλίου 2021. Στο διάγραμμα 5.2 μπορούμε να παρατηρήσουμε την εξέλιξη της πορείας της τιμής του από την 1/1/2017 έως τις 30/3/2021.

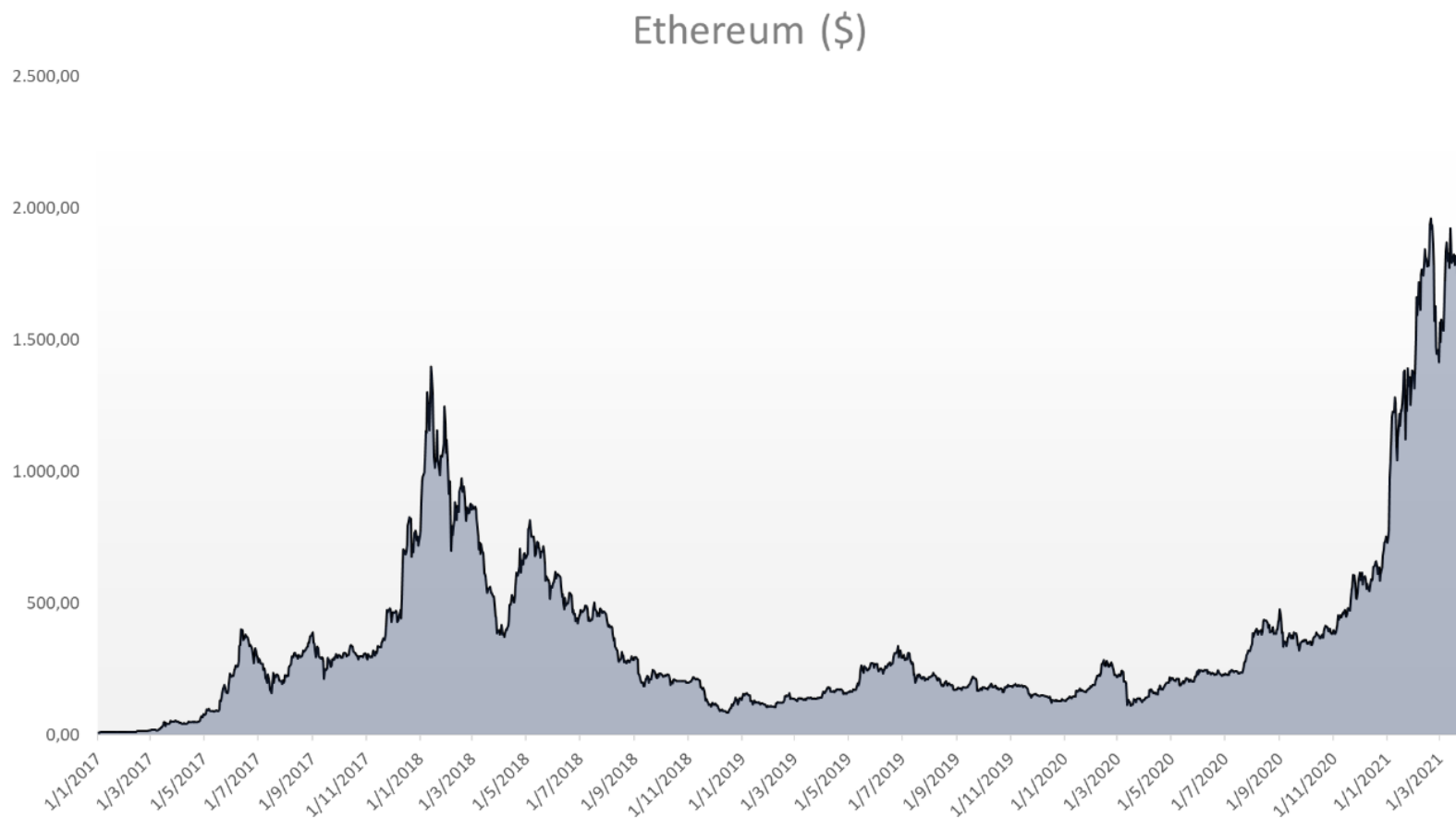
Σύμφωνα με το Coinmarketcap.com/Ethereum (2021) και το Coingecko.com/Ethereum (2021), το Ethereum αποτελεί μια παγκόσμια πλατφόρμα ανοιχτού κώδικα για εφαρμογή αποκεντροποιημένων εφαρμογών. Η φιλοδοξία των δημιουργών του ήταν να δημιουργηθεί μια πλατφόρμα στην οποία ο καθένας θα μπορεί να δημιουργήσει εφαρμογές με αποκεντρωμένο τρόπο με όλα τα δεδομένα να διανέμονται και είναι προσβάσιμα απ' όλους τους συμμετέχοντες.

Η πλατφόρμα Blockchain που χρησιμοποιεί το Ethereum υποστηρίζει τα έξυπνα συμβόλαια (smart contracts). Παραδείγματα τέτοιων αποκεντρωμένων εφαρμογών (decentralized apps- dapps) περιλαμβάνουν εφαρμογές χρηματοδότησης, πρωτόκολλα δανεισμού, κλπ. και πραγματοποιούνται μεταξύ δύο αντισυμβαλλόμενων. Οι όροι των συναλλαγών αυτών καθορίζονται εκ των προτέρων και δεν χρειάζεται να εμπιστεύονται τα άτομα αυτά κάποιο τρίτο αντισυμβαλλόμενο άτομο ή αρχή για την εκτέλεση τους.

Σε αντίθεση με το Bitcoin στο οποίο ο δημιουργός του δεν είναι γνωστός στο ευρύ κοινό, η ιδρυτική ομάδα του Ethereum είναι γνωστή. Πιο συγκεκριμένα το Ethereum περιγράφεται για πρώτη φορά στο έγγραφο δημιουργίας του το έτος 2013 από τον Vitalik Buterin, με τον Mihai Alisie, τον Anthony Di Iorio, τον Charles Hoskinson, τον Amir Chetrit, τον Joseph Lubin, τον Gavin Wood και τον Jeffrey Wilke να αποτελούν ιδρυτικά μέλη του. Βέβαια σήμερα αρκετοί από αυτούς δεν δραστηριοποιούνται στην κοινότητα του Ethereum αλλά έχουν προχωρήσει σε άλλα εγχειρήματα γύρω από τα κρυπτονομίσματα όπως είναι το Cardano και το Polkadot.

Να αναφέρουμε πως η χρηματοδότηση για το έργο του Ethereum ξεκίνησε με μια διαδικτυακή δημόσια πώληση που έγινε το καλοκαίρι του 2014 και ξεκίνησε επίσημα το blockchain του στις 30 Ιουλίου 2015. Επίσης, ενώ το Ethereum αναφέρεται στο δίκτυο blockchain, το κρυπτονόμισμα Ether (ETH) χρησιμοποιείται συνήθως για τις συναλλαγές εντός του δικτύου ως βασικό νόμισμα και προσφέρει υψηλά επίπεδα ανωνυμίας στους χρήστες του, καθιστώντας το πολύ καλό για εφαρμογή εντός του σκοτεινού διαδικτύου.

**Διάγραμμα 5.2:** Η πορεία της τιμής του Ethereum από την 1/1/2017 έως τις 30/3/2021



Πηγή Δεδομένων: Coinmarketcap.com (Ημερήσια στοιχεία)



### 5.2.3 Αναφορά στο κρυπτονόμισμα Litecoin

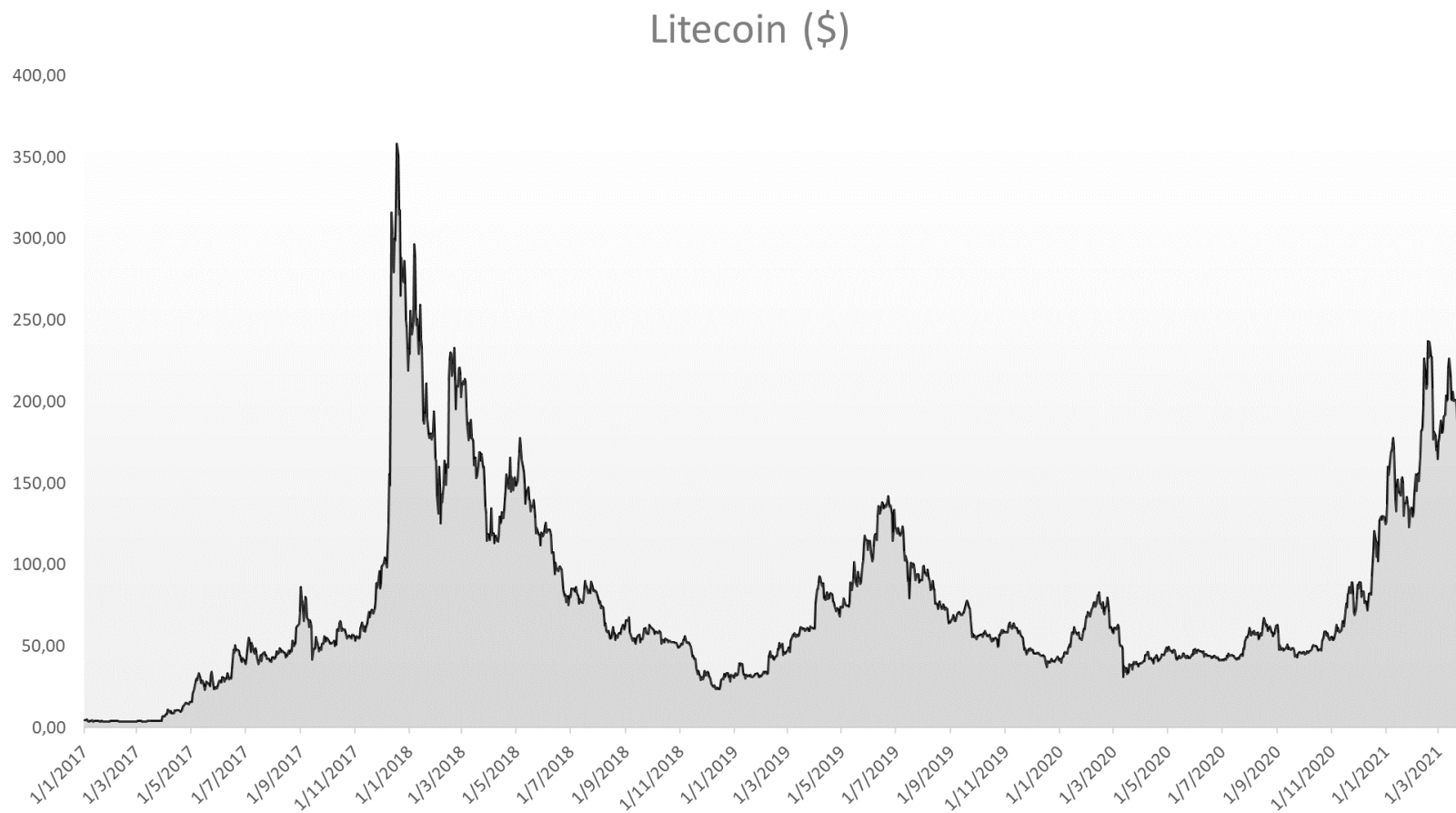
Το κρυπτονόμισμα Litecoin σύμφωνα με το Coingecko.com (20.04.2021) είχε τιμή \$272,49 και χρηματιστηριακή κεφαλαιοποίηση \$18.300.557.261 δολάρια κατέχοντας την ένατη θέση στην παγκόσμια αγορά κρυπτονομισμάτων με συνολικά το 0,85% αυτής. Η ιστορικά υψηλότερη τιμή του ήταν τα \$360,66 στις 18 Δεκεμβρίου 2017, ενώ συνολικά έχει σε κυκλοφορία 67 εκατομμύρια LTC νομίσματα με την μέγιστη προσφορά που μπορούν να φτάσουν να είναι τα 84 εκατομμύρια. Στο διάγραμμα 5.3 μπορούμε να παρατηρήσουμε την εξέλιξη της πορείας της τιμής του από την 1/1/2017 έως τις 30/3/2021.

Σύμφωνα με το Coinmarketcap.com/Litecoin(2021) και το Coingecko.com/Litecoin(2021) το Litecoin είναι ένα κρυπτονόμισμα αρκετά παρόμοιο τεχνολογικά με το Bitcoin. Είναι αποκεντροποιημένο και τα πρωτόκολλα του είναι τροποποιημένα σε σχέση με του Bitcoin, παρέχοντας γρήγορες, ασφαλείς και χαμηλού κόστους πληρωμές αξιοποιώντας τις μοναδικές ιδιότητες της τεχνολογίας του blockchain. Τα χαρακτηριστικά αυτά μας οδηγούν στο συμπέρασμα πως μπορεί να αποτελέσει εξαιρετικό μέσο πληρωμών στο σκοτεινό διαδίκτυο προσφέροντας ανωνυμία στους χρήστες του.

Αναλυτικότερα, όσον αφορά τα τεχνολογικά χαρακτηριστικά του, το Litecoin βασίζεται στην επαλήθευση των συναλλαγών μέσω του συστήματος Proof of Work (PoW) και λειτουργεί σε ένα δίκτυο peer-to-peer στο οποίο οι χρήστες μπορούν να μεταφέρουν χρήματα ο ένας στον άλλο χωρίς να χρειάζεται να βασίζονται σε οποιαδήποτε κεντρική αρχή.

Τέλος να αναφέρουμε πως το Litecoin δημιουργήθηκε από τον Charlie Lee, πρώην υπάλληλο της Google και διευθυντή προγραμματισμού στην Coinbase (2015-2017), τον Οκτώβριο του 2011 και θεωρείται ως ένα από τα πρώτα εναλλακτικά κρυπτονομίσματα (altcoins). Ο στόχος του ήταν να προσφέρει καλύτερες τεχνολογικές καινοτομίες από το Bitcoin. Το πρώτο block του δικτύου του Litecoin, το οποίο ονομάζεται genesis block εξορύχθηκε στις 7 Οκτωβρίου 2011.

**Διάγραμμα 5.3:** Η πορεία της τιμής του Litecoin από την 1/1/2017 έως τις 30/3/2021



Πηγή Δεδομένων: Coinmarketcap.com (Ημερήσια στοιχεία)

#### 5.2.4 Αναφορά στο κρυπτονόμισμα Monero

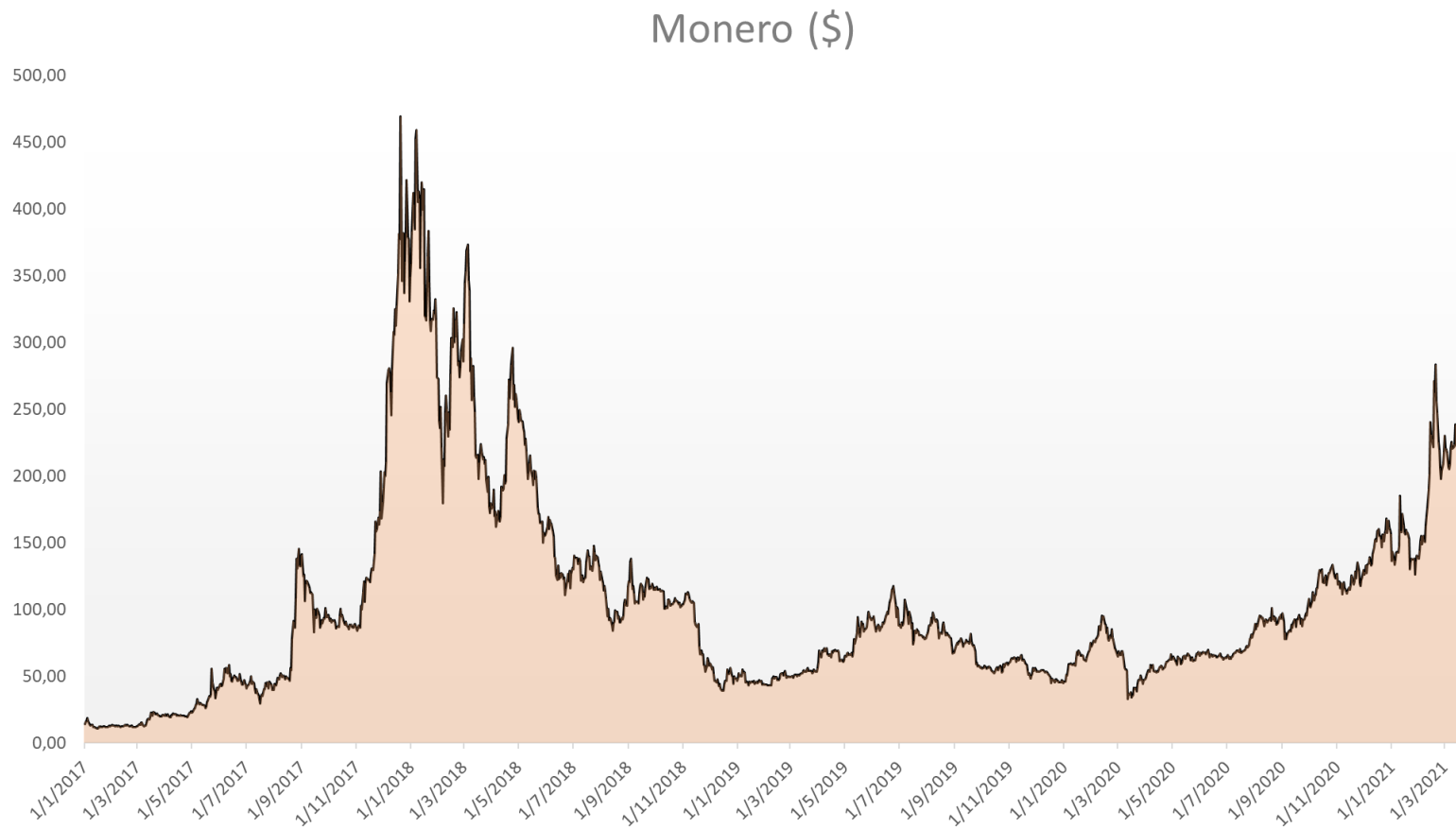
Το κρυπτονόμισμα Monero σύμφωνα με το Coingecko.com (20.04.2021) είχε τιμή \$398,69 και χρηματιστηριακή κεφαλαιοποίηση \$7.127.464.732 δολάρια κατέχοντας την εικοστή δεύτερη θέση στην παγκόσμια αγορά κρυπτονομισμάτων με συνολικά το 0,33% αυτής. Η ιστορικά υψηλότερη τιμή του ήταν τα \$542,33 στις 9 Ιανουαρίου 2018. Στο διάγραμμα 5.4 μπορούμε να παρατηρήσουμε την εξέλιξη της πορείας της τιμής του από την 1/1/2017 έως τις 30/3/2021.

Σύμφωνα με το Coinmarketcap.com/ Monero (2021) και το Coingecko.com/ Monero (2021), το Monero που έχει ως νόμισμα το XMR κυκλοφόρησε το 2014 και ο στόχος του ήταν απλός. Να επιτρέψει τις συναλλαγές να πραγματοποιούνται ιδιωτικά και με ανωνυμία. Το Monero αποτελεί κορυφαίο σε επίπεδο ανωνυμίας κρυπτονόμισμα που βασίζεται στο πρωτόκολλο CryptoNote, ένα ασφαλές, ιδιωτικό και μη ανιχνεύσιμο σύστημα. Χρησιμοποιεί ένα ειδικό είδος κρυπτογραφίας για να διασφαλίσει ότι όλες οι συναλλαγές μέσω αυτού δεν μπορούν να συνδεθούν με το ποιος τις πραγματοποίησε αλλά και να ανιχνευτούν.

Όσον αφορά την δημιουργία του, το Monero προέρχεται από την διακλάδωση της αλυσίδας του Blockchain του Bytecoin, με την αρχική του ονομασία να ήταν Bitmonero, όπου αργότερα μετονομάστηκε. Οι ιδρυτές του Monero είναι επτά προγραμματιστές, με τους πέντε να μην έχουν αποκαλύψει την ταυτότητα τους, ενώ υπήρξαν φήμες ότι εφευρέθηκε από τον Satoshi Nakamoto, τον εφευρέτη του Bitcoin.

Να αναφέρουμε πως η απόρρητη φύση του κρυπτονομίσματος επιτυγχάνεται μέσω μερικών ιδιαίτερων χαρακτηριστικών. Για παράδειγμα ενώ κάθε Bitcoin σε κυκλοφορία έχει τον δικό του σειριακό αριθμό, που σημαίνει ότι μπορεί να παρακολουθείται, αυτό δεν ισχύει στην περίπτωση του XMR. Συνεπώς τα χαρακτηριστικά και η τεχνολογία του Monero, το έχουν οδηγήσει να χρησιμοποιείται όλο και περισσότερο για παράνομες συναλλαγές αντί για το Bitcoin, ειδικά στις αγορές του darknet.

**Διάγραμμα 5.4:** Η πορεία της τιμής του Monero από την 1/1/2017 έως τις 30/3/2021



Πηγή Δεδομένων: Coinmarketcap.com (Ημερήσια στοιχεία)

## 5.2.5 Αναφορά στο κρυπτονόμισμα Z cash

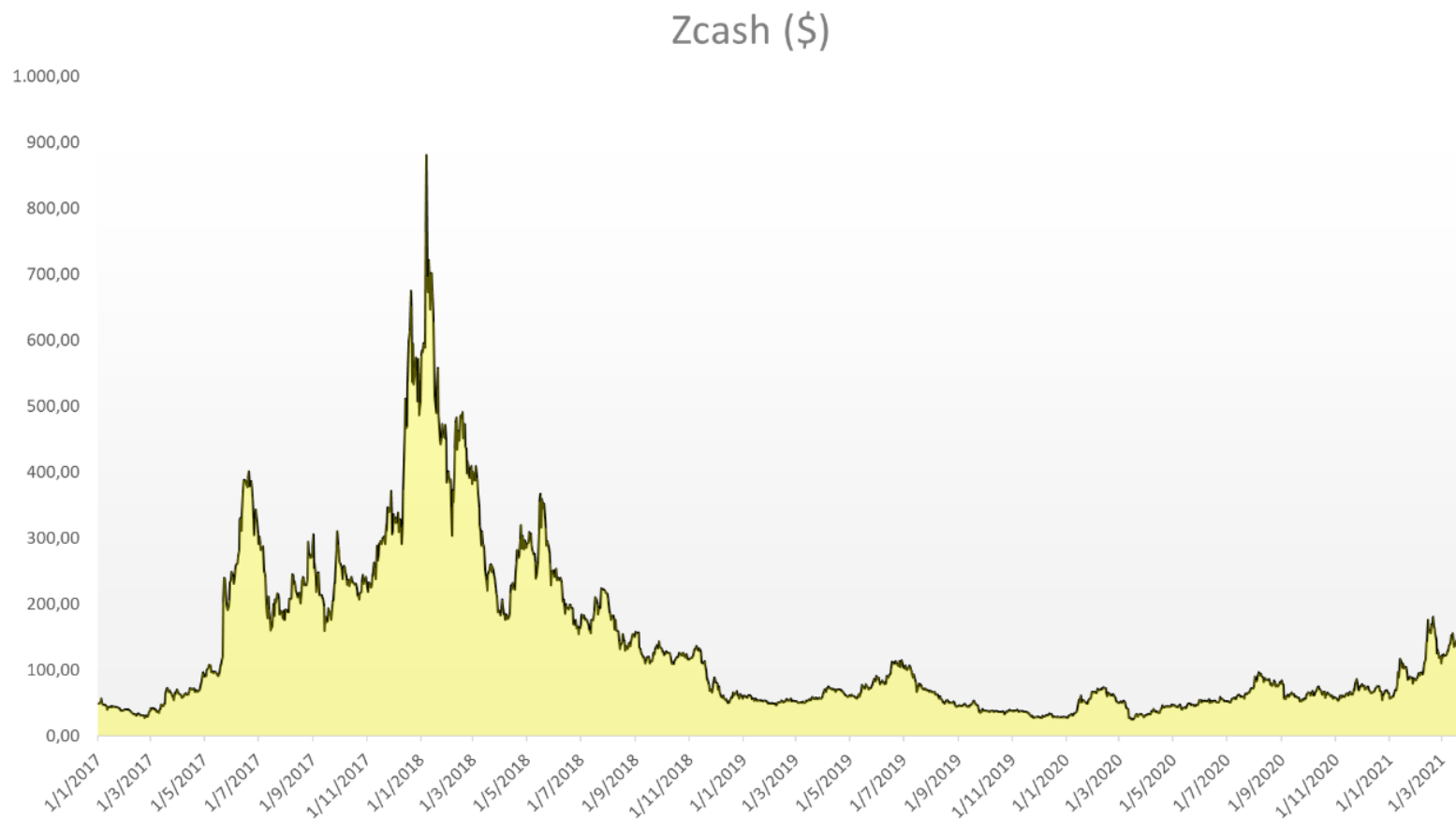
Το κρυπτονόμισμα Z cash σύμφωνα με το Coingecko.com (20.04.02021) είχε τιμή \$247,93 και χρηματιστηριακή κεφαλαιοποίηση \$2.730.933.355 δολάρια κατέχοντας την πεντηκοστή τρίτη θέση στην παγκόσμια αγορά κρυπτονομισμάτων με συνολικά το 0,13% αυτής. Η ιστορικά υψηλότερη τιμή του ήταν τα \$3.191,93 στις 29 Οκτωβρίου 2016. Στο διάγραμμα 5.5 μπορούμε να παρατηρήσουμε την εξέλιξη της πορείας της τιμής του από την 1/1/2017 έως τις 30/3/2021.

Σύμφωνα με το Coinmarketcap.com/ Zcash (2021) και το Coingecko.com/Zcash (2021), το Zcash ή ZEC είναι ένα αποκεντροποιημένο κρυπτονόμισμα ανοιχτού κώδικα που προσφέρει προστασία της ιδιωτικής ζωής και παράλληλα επιλεκτική διαφάνεια στις συναλλαγές. Οι πληρωμές μέσω Zcash δημοσιεύονται σε δημόσιο blockchain, αλλά ο αποστολέας, ο παραλήπτης και το ποσό μιας συναλλαγής παραμένουν ιδιωτικές. Χρησιμοποιεί την τεχνολογία zk-SNARK που επιτρέπει στους κόμβους του δικτύου να επαληθεύουν συναλλαγές χωρίς να αποκαλύπτουν ευαίσθητες πληροφορίες σχετικά με αυτές τις συναλλαγές.

Το Zcash βασίζεται στον κώδικα λειτουργίας του Bitcoin αλλά διαθέτει την βελτίωση της προσθήκης της διασφάλισης του απορρήτου, καθώς χρησιμοποιεί προηγμένες κρυπτογραφικές τεχνικές για να εγγυηθεί την εγκυρότητα των συναλλαγών χωρίς να αποκαλύψει πρόσθετες πληροφορίες σχετικά με αυτές. Οι χρήστες του έχουν την επιλογή να πραγματοποιούν συναλλαγές είτε δημόσιες είτε ιδιωτικού χαρακτήρα. Σε αντίθεση με την πλειονότητα των κρυπτονομισμάτων στην αγορά, συμπεριλαμβανομένου και του Bitcoin και του Ethereum δεν χαρακτηρίζονται ως ανώνυμα, αλλά ως ψευδώνυμα. Οι συναλλαγές με το κρυπτονόμισμα ZEC δεν αποκαλύπτουν τις διευθύνσεις αποστολής και λήψης αλλά και το ποσό που αποστέλλεται με αποτέλεσμα να χρησιμοποιείται πολύ στο σκοτεινό διαδίκτυο.

Τέλος να αναφέρουμε πως δημιουργός του Zcash είναι ο ειδικός για θέματα ασφάλειας υπολογιστών Zooko Wilcox-O'Hearn, ενώ η κυκλοφορία του πραγματοποιήθηκε πρώτη φορά στις 28 Οκτωβρίου του 2016.

**Διάγραμμα 5.5:** Η πορεία της τιμής του Z cash από την 1/1/2017 έως τις 30/3/2021



Πηγή Δεδομένων: Coinmarketcap.com (Ημερήσια στοιχεία)

## 5.2.6 Αναφορά στο κρυπτονόμισμα DASH

Το κρυπτονόμισμα DASH σύμφωνα με το Coingecko.com (20.04.2021) είχε τιμή \$312,54 και χρηματιστηριακή κεφαλαιοποίηση \$3.165.221.303 δολάρια κατέχοντας την τεσσαρακοστή ένατη θέση στην παγκόσμια αγορά κρυπτονομισμάτων με συνολικά το 0,15% αυτής. Η ιστορικά υψηλότερη τιμή του ήταν τα \$1.493,59 στις 20 Δεκεμβρίου 2017. Στο διάγραμμα 5.6 μπορούμε να παρατηρήσουμε την εξέλιξη της πορείας της τιμής του από την 1/1/2017 έως τις 30/3/2021.

Αναλυτικότερα, σύμφωνα με το Coinmarketcap.com/ DASH (2021) και το Coingecko.com/DASH (2021), το Dash είναι ένα blockchain ανοιχτού κώδικα με το κρυπτονόμισμα του να επικεντρώνεται στην προσφορά ενός γρήγορου, φθηνού παγκόσμιου δικτύου πληρωμών που είναι αποκεντρωμένο. Οι πληρωμές είναι άμεσες, εύκολες και ασφαλείς, με σχεδόν μηδενικές χρεώσεις. Σύμφωνα με το έγγραφο δημιουργίας του επιδιώκει να βελτιώσει την τεχνολογία του Bitcoin (BTC) παρέχοντας ισχυρότερο απόρρητο και γρηγορότερες συναλλαγές.

Το Dash, του οποίου το όνομα προέρχεται από το “Digital Cash” κυκλοφόρησε τον Ιανουάριο του 2014 ως διακλάδωση του πρωτοκόλλου του Litecoin. Από τότε που κυκλοφόρησε έχει εξελιχθεί σε χαρακτηριστικά, αλλά από τη στιγμή που δημιουργήθηκε, έχει επιδείξει ηγετικό ρόλο στην καινοτομία και πρωτοπορία καθώς εφαρμόζει χαρακτηριστικά όπως δίκτυο δύο επιπέδων, άμεσες πληρωμές σε συναλλαγές, αλλά και προαιρετικό απόρρητο για συναλλαγές. Συνεπώς τα χαρακτηριστικά του το μετατρέπουν σε εξαιρετικό μέσο για την χρησιμοποίηση του εντός του σκοτεινού διαδικτύου.

Τέλος να αναφέρουμε πως το Dash ιδρύθηκε από τους προγραμματιστές λογισμικού Evan Duffield και Kyle Hagan, με το έργο τους αρχικά να είχε ονομαστεί XCoin, ενώ μετέπειτα σε Darkcoin και τελικώς σε Dash. Αυτό συνέβη τον Μάρτιο του 2015 σε μια προσπάθεια να αλλάξει θετικά την εικόνα του. Ενώ η αρχική ιδέα των δημιουργών του ήταν από το 2012 να φτιάξουν ένα κρυπτονόμισμα που θα προσέθετε περισσότερη ανωνυμία από το Bitcoin.

**Διάγραμμα 5.6:** Η πορεία της τιμής του DASH από την 1/1/2017 έως τις 30/3/2021



Πηγή

Δεδομένων:

Coinmarketcap.com

(Ημερήσια

στοιχεία)



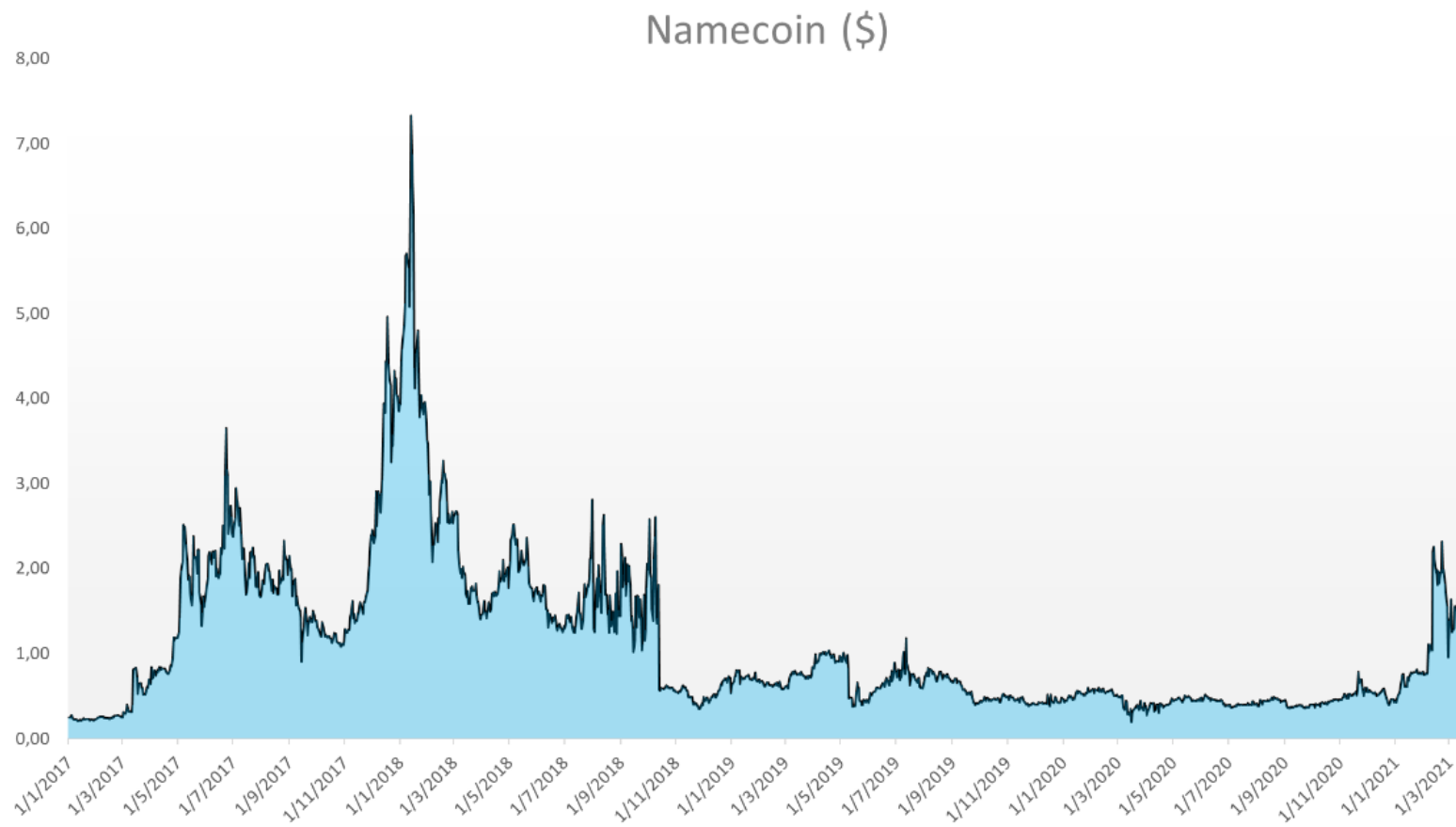
### 5.2.7 Αναφορά στο κρυπτονόμισμα Namecoin

Το κρυπτονόμισμα Namecoin σύμφωνα με το Coingecko.com (20.04.2021) είχε τιμή \$2,36 και χρηματιστηριακή κεφαλαιοποίηση \$37.614.671 δολάρια κατέχοντας την εξηκοστή εικοστή έκτη θέση στην παγκόσμια αγορά κρυπτονομισμάτων με συνολικά το 0,00% αυτής. Η ιστορικά υψηλότερη τιμή του ήταν τα \$13,11 στις 29 Νοεμβρίου 2013. Διαθέτει σε κυκλοφορία 16 εκατομμύρια νομίσματα NMC με την μέγιστη προσφορά να είναι τα 21 εκατομμύρια. Στο διάγραμμα 5.7 μπορούμε να παρατηρήσουμε την εξέλιξη της πορείας της τιμής του από την 1/1/2017 έως τις 30/3/2021.

Σύμφωνα με το Coinmarketcap.com/Litecoin (2021) και το Coingecko.com/Namecoin (2021), το Namecoin ήταν το πρώτο κρυπτονόμισμα που προέκυψε από την διάσπαση του Blockchain του Bitcoin. Ήταν το πρώτο κρυπτονόμισμα που χρησιμοποίησε την τεχνολογία Auxiliary Proof of Work (AuxPoW) για τη συναίνεσή στις συναλλαγές των χρηστών του και λόγω ότι χρησιμοποιεί το Blockchain του Bitcoin, κάθε φορά που δημιουργείται ένα νέο block στο Bitcoin blockchain τότε προστίθεται και στο blockchain του Namecoin.

Ο δημιουργός του Namecoin φέρει το όνομα "Vince" και το έτος δημιουργίας του είναι το 2011. Από τότε μέχρι σήμερα το έργο του Vince το έχει αναλάβει μια εξειδικευμένη ομάδα προγραμματιστών για να το εξελίξει. Μπορεί το 2014 να ήταν στην λίστα με τα δέκα κορυφαία κρυπτονομίσματα σε κεφαλαιοποίηση αλλά αυτό δεν συνεχίστηκε καθώς εισήχθησαν στην αγορά εκατοντάδες νέα κρυπτονομίσματα με καλύτερες τεχνολογικές εξελίξεις. Παρόλα αυτά επειδή ενσωματώνει πολλά κοινά χαρακτηριστικά με το Bitcoin αποτελεί αρκετά καλό μέσο πραγματοποίησης συναλλαγών εντός του σκοτεινού διαδικτύου.

**Διάγραμμα 5.7:** Η πορεία της τιμής του Namecoin από την 1/1/2017 έως τις 30/3/2021



Πηγή Δεδομένων: Coinmarketcap.com (Ημερήσια στοιχεία)

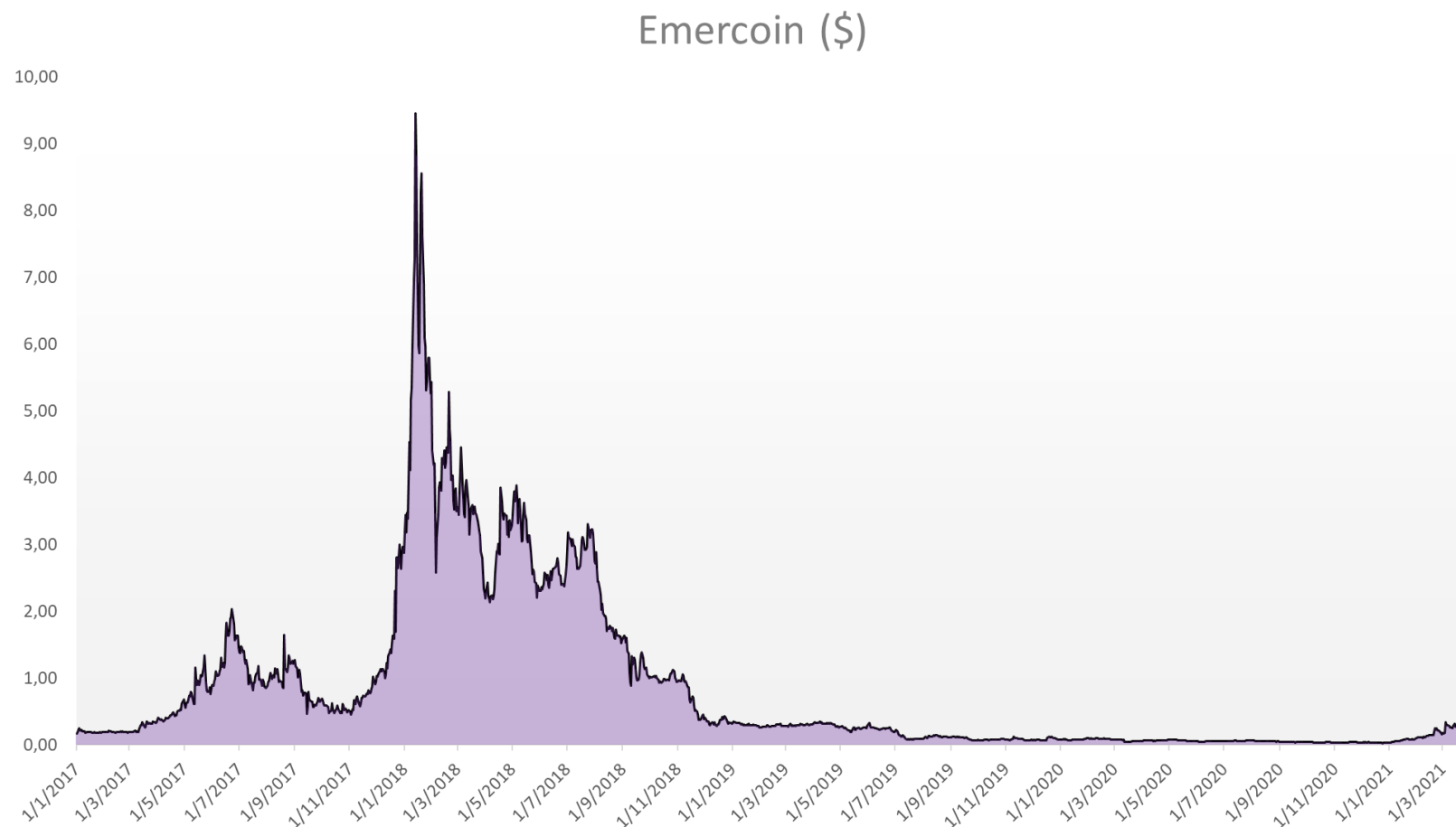
## 5.2.8 Αναφορά στο κρυπτονόμισμα EmerCoin

Το κρυπτονόμισμα EmerCoin σύμφωνα με το Coingecko.com (20.04.2021) είχε τιμή \$0,347 και χρηματιστηριακή κεφαλαιοποίηση \$11.188.194 δολάρια κατέχοντας την εννιακοσίοστη ογδοηκοστή τέταρτη θέση στην παγκόσμια αγορά κρυπτονομισμάτων με συνολικά το 0,00% αυτής. Η ιστορικά υψηλότερη τιμή του ήταν τα \$11,21 στις 18 Απριλίου 2018. Διαθέτει σε κυκλοφορία 47 εκατομμύρια νομίσματα EMC με την μέγιστη προσφορά τους να είναι το 1 δισεκατομμύριο. Στο διάγραμμα 5.8 μπορούμε να παρατηρήσουμε την εξέλιξη της πορείας της τιμής του από την 1/1/2017 έως τις 30/3/2021.

Σύμφωνα με το Coingecko.com/EmerCoin (2021), η πλατφόρμα του Emercoin έχει ως κρυπτονόμισμα το EMC το οποίο είναι ένα κρυπτονόμισμα ανοιχτού κώδικα που προέρχεται από το Bitcoin, το Peercoin και το Namecoin. Εκτός από κρυπτονόμισμα χρησιμοποιείται από τους χρήστες του για πρόσβαση στις υπηρεσίες του blockchain του Emercoin προσφέροντας μεταξύ άλλων ασφαλείς επιχειρηματικές υπηρεσίες και αποκεντροποιημένες εφαρμογές. Ως πλατφόρμα blockchain κληρονομεί την αξιοπιστία και την ασφάλεια του Bitcoin, ενώ ταυτόχρονα προσθέτει περισσότερα χαρακτηριστικά στο δικό του blockchain αξιοποιώντας τεχνολογικές καινοτομίες.

Το Emercoin ιδρύθηκε το 2013 από τον Eugene Shumilov, ενώ βρίσκεται στην αγορά των κρυπτονομισμάτων από το 2014. Από τότε μέχρι σήμερα έχει αναπτύξει αρκετές συνεργασίες με οργανισμούς με τις σημαντικότερες από αυτές να είναι με την Coca Cola και την Microsoft. Ορισμένοι άλλοι συνεργάτες είναι οι RedHat, LLoyd's, Bitfury, Aspanta, Deloitte, Authorizers, Foundico, Anteko, κ.λπ.

**Διάγραμμα 5.8:** Η πορεία της τιμής του EmerCoin από την 1/1/2017 έως τις 30/3/2021



Πηγή

Δεδομένων:

Coinmarketcap.com

(Ημερήσια

στοιχεία)

### 5.3 Συμπεράσματα πέμπτου κεφαλαίου

Όσον αφορά στα κρυπτονομίσματα που χρησιμοποιούνται περισσότερο στο σκοτεινό διαδίκτυο, συμπεραίνουμε πως παρά τις διαφορές που μπορεί να παρουσιάζουν στην τεχνολογία τους, όλα συγκλίνουν προς ένα κοινό χαρακτηριστικό, την προστασία της ιδιωτικής ταυτότητας και της ανωνυμίας των χρηστών τους. Μπορεί αρχικά οι αγορές του Darkweb να βασίζονταν στην χρησιμοποίηση μόνο του Bitcoin, ωστόσο τα τελευταία χρόνια αυτό έχει αλλάξει και ο αυξανόμενος όγκος των κρυπτονομισμάτων στην παγκόσμια αγορά αναγνωρίζει τα οφέλη από την προσφορά και άλλων κρυπτονομισμάτων.

Το Litecoin, το Ethereum είναι μερικά παραδείγματα, ενώ το Monero γίνεται σταδιακά το πιο καθιερωμένο νόμισμα απορρήτου για συναλλαγές στο σκοτεινό διαδίκτυο, ενώ ακολουθεί το Zcash και το Dash. Όλα αυτά τα κρυπτονομίσματα που έχουν υψηλά επίπεδα απορρήτου ενδέχεται να αποτελούν σημαντικό εμπόδιο για τις αρχές επιβολής του νόμου για τον περιορισμό του σκοτεινού διαδικτύου.

## **Κεφάλαιο 6: Εμπειρική και στατιστική ανάλυση των κυριότερων κρυπτονομισμάτων του σκοτεινού διαδικτύου**

### **6.1 Εισαγωγή έκτου κεφαλαίου**

Στο έκτο κεφάλαιο της διπλωματικής εργασίας που ακολουθεί, το οποίο αποτελεί και την συμβολή σε αυτήν, παρουσιάζεται μια στατική και εμπειρική ανάλυση ανάμεσα στα κρυπτονομίσματα που χρησιμοποιούνται περισσότερο για συναλλαγές εντός του σκοτεινού διαδικτύου. Αναλυτικότερα, μετά την βιβλιογραφική ανασκόπηση που πραγματοποιήθηκε στα προηγούμενα κεφάλαια, καταλήξαμε πως τα κρυπτονομίσματα αυτά είναι το Bitcoin, το Ethereum, το Litecoin, το Monero, το Zcash, το DASH, το Namecoin και το EmerCoin.

Σκοπός της ανάλυσης που ακολουθεί είναι μέσα από στατιστικές και εμπειρικές τεχνικές να διεξαχθούν συγκριτικά συμπεράσματα σχετικά με την πορεία που παρουσίασαν τα κρυπτονομίσματα αυτά, την επικινδυνότητα τους αλλά και τον βαθμό συσχέτισης που έχουν μεταξύ τους, με τελικό στόχο να διερευνηθεί ποιο ή ποια θα μπορούσαν να αποτελέσουν καταλληλότερο μέσω πραγματοποίησης συναλλαγών.

Αναλυτικότερα, μέσω ημερήσιων δεδομένων για τις τιμές κλεισίματος τους, τα οποία αντλήθηκαν από τον έγκυρο ηλεκτρονικό ιστότοπο [coinmarketcap.com](https://coinmarketcap.com), υπολογίζεται η απόδοση που πραγματοποίησαν στο σύνολο της περιόδου ανάλυσης, η μέση ημερήσια απόδοση τους, η μέγιστη ημερήσια απόδοση τους και η ελάχιστη ημερήσια απόδοση τους. Ενώ επίσης εκτιμάται και ο βαθμός επικινδυνότητάς τους μέσω του υπολογισμού της ημερήσιας τυπικής απόκλισης αλλά και του συντελεστής συσχέτισης του παρουσιάζουν.

Τα ευρήματα που αναλύονται στην συνέχεια αφορούν το διάστημα από την 1/1/2017 έως τις 30/3/2021, με την επιλογή του συγκεκριμένου διαστήματος να είναι καθαρά και μόνο επειδή ήταν κοινό για όλα τα κρυπτονομίσματα στην δραστηριοποίησή τους. Βέβαια η ανάλυση δεν περιορίζεται μόνο στο συνολικό αυτό διάστημα αλλά γίνεται για κάθε έτος ξεχωριστά από το 2017 έως το Μάρτιο του 2021 για να έχουμε μια πιο πλήρη εικόνα και αντιπροσωπευτική εικόνα.

Τέλος, όσον αφορά στα εμπειρικά ευρήματα που θα εξετάσουμε, πιο συγκριμένα να αναφέρουμε πως στην διεθνή βιβλιογραφία ο πιο συνήθης τρόπος

μέτρησης του κινδύνου των επενδύσεων είναι μέσω της εκτίμησης της τυπικής απόκλισης των αποδόσεων τους, με την γνώση του κινδύνου να είναι μια σημαντική μεταβλητή η οποία είναι απαραίτητη για την επιστημονική αξιολόγηση τους. Ενώ επίσης όσον αφορά τον συντελεστή συσχέτισης να προσθέσουμε πως αποτελεί ένα στατιστικό μέτρο εκτίμησης του βαθμού παράλληλης κίνησης δυο μεταβλητών. Η μεταβλητή αυτή παίρνει τιμές μεταξύ του διαστήματος -1 και 1 με τους συντελεστής κοντά στη μονάδα (+1) υποδηλώνουν ισχυρή, παράλληλη και ομόρροπη κίνηση μεταξύ των εξεταζόμενων μεταβλητών, ενώ τιμές κοντά στο -1, δείχνουν ισχυρή, παράλληλη, αλλά αντίθετης κατεύθυνσης κίνηση (Φίλιππας Ν.,2005).

## 6.2 Εμπειρική ανάλυση κρυπτονομισμάτων

Στο υποκεφάλαιο 6.2 ακολουθεί η παρουσίαση των εμπειρικών ευρημάτων για τα κρυπτονομίσματα Bitcoin, Ethereum, Litecoin, Monero, Zcash, DASH, Namecoin και EmerCoin για το έτος 2017, για το έτος 2018, για το έτος 2019, για το διάστημα από το 2020 έως τον Μάρτιο του 2021 αλλά και για το συνολικό διάστημα από την αρχή του 2017 έως τον Μάρτιο του 2021. Στα ευρήματα αυτά υπολογίζεται η απόδοση της κάθε περιόδου, η μέση ημερήσια απόδοση τους, η μέγιστη ημερήσια απόδοση τους και η ελάχιστη ημερήσια απόδοση τους, η τυπική απόκλιση των αποδόσεων τους αλλά και ο συντελεστής συσχέτισης που παρουσιάζουν μεταξύ τους

### 6.2.1 Εμπειρικά ευρήματα έτους 2017

Στους πίνακες 6.1 και 6.2 παρουσιάζονται τα εμπειρικά ευρήματα για τα οκτώ κρυπτονομίσματα που χρησιμοποιούνται περισσότερο εντός του σκοτεινού διαδικτύου για το διάστημα από 01.01.2017 έως 31.12.2016. Αναλυτικότερα, στον Πίνακα 6.1 παρουσιάζεται η απόδοση που παρουσίασαν την προαναφερθείσα περίοδο, η μέση ημερήσια απόδοση τους, η μέγιστη ημερήσια απόδοση τους και η ελάχιστη ημερήσια απόδοση τους αλλά και ο βαθμός επικινδυνότητάς τους, ενώ στον Πίνακα 6.2 εκτιμάται ο συντελεστής συσχέτισης των ημερησίων αποδόσεων τους.

**Πίνακας 6.1:** Στατιστικά ευρήματα επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το έτος 2017

	Δ% 31.12.17- 01.01.17	Average Daily Return (%)	Maximum Daily Return (%)	Minimum Daily Return (%)	Daily Standard Deviation (%)
Dash	9265%	1,56%	54,92%	-21,59%	8,17%
Ethereum	9162%	1,51%	33,66%	-27,06%	7,31%
Litecoin	5046%	1,43%	66,59%	-32,64%	8,70%
Monero	2398%	1,19%	53,77%	-25,41%	8,02%
Emercoin	1654%	1,37%	92,94%	-40,86%	11,67%
Namecoin	1516%	1,24%	102,50%	-36,88%	10,42%
Bitcoin	1318%	0,85%	25,25%	-18,74%	5,00%
Zcash	943%	0,93%	69,58%	-19,44%	7,93%

Πηγή Δεδομένων: Coinmarketcap.com



Σύμφωνα με τα αποτελέσματα του Πίνακα 6.1 στον οποίο η κατάταξη έχει πραγματοποιηθεί σε φθίνουσα σειρά ανάλογα με την απόδοση περιόδου, παρατηρούμε πως το κρυπτονόμισμα Dash πραγματοποίησε την καλύτερη του διαστήματος 01.01.2017 - 31.12.2017 πετυχαίνοντας 9.265%. Αντιθέτως το κρυπτονόμισμα Zcash την χειρότερη μεταξύ των συγκρινόμενων κρυπτονομισμάτων πετυχαίνοντας 943%. Το πολύ γνωστό σε όλους Bitcoin έλαβε την 7η θέση μεταξύ των οκτώ κρυπτονομισμάτων πετυχαίνοντας 1.318%

Με βάση τον υπολογισμό της μέσης ημερήσιας απόδοσης του διαστήματος 01.01.2017-31.12.2017, το κρυπτονόμισμα Dash είχε την καλύτερη μεταξύ των εξεταζόμενων κρυπτονομισμάτων με 1,56% ενώ την χειρότερη είχε το Bitcoin με 0,85%. Επίσης με βάση τα αποτελέσματα του πίνακα την υψηλότερη μέγιστη απόδοση σε ημερήσια βάση πέτυχε το κρυπτονόμισμα Namecoin με 102,50% με την λιγότερο καλή να κάνει το Bitcoin με 25,25%. Ενώ, όσον αφορά την ελάχιστη ημερήσια απόδοση, μεγαλύτερες απώλειες σε ημερήσια βάση είχε το Emercoin το οποίο έχασε -40,86%, ενώ τις λιγότερες είχε το Bitcoin το οποίο έχασε -18,74%.

Τέλος, όσον αφορά στην επικινδυνότητα των παραπάνω κρυπτονομισμάτων, παρατηρούμε πως την μεγαλύτερη ημερήσια τυπική απόκλιση παρουσίασε το κρυπτονόμισμα Emercoin με 11,67% ενώ την μικρότερη το Bitcoin με 5,00%, φανερώνοντας μας μικρότερη μεταβλητότητα στις ημερήσιες αποδόσεις του μεταξύ των συγκρινόμενων κρυπτονομισμάτων

**Πίνακας 6.2:** Ο συντελεστής συσχέτισης επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το έτος 2017

	BITCOIN	DASH	EMERCOIN	ETHEREUM	LITECOIN	MONERO	NAMECOIN	ZCASH
BITCOIN	1,000	0,298	0,281	0,355	0,369	0,412	0,386	0,301
DASH	0,298	1,000	0,188	0,366	0,262	0,493	0,203	0,527
EMERCOIN	0,281	0,188	1,000	0,272	0,263	0,229	0,302	0,240
ETHEREUM	0,355	0,366	0,272	1,000	0,343	0,460	0,402	0,480
LITECOIN	0,369	0,262	0,263	0,343	1,000	0,348	0,401	0,293
MONERO	0,412	0,493	0,229	0,460	0,348	1,000	0,428	0,467
NAMECOIN	0,386	0,203	0,302	0,402	0,401	0,428	1,000	0,280
ZCASH	0,301	0,527	0,240	0,480	0,293	0,467	0,280	1,000

Πηγή Δεδομένων: Coinmarketcap.com

Όπως μπορούμε να παρατηρήσουμε στον Πίνακα 6.2, που παρουσιάζονται τα αποτελέσματα της ανάλυσης του συντελεστή συσχέτισης, το κρυπτονόμισμα Bitcoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Monero έχοντας 0,412 και την μικρότερη με το Dash έχοντας 0,298. Το Dash παρουσιάζει την μεγαλύτερη συσχέτιση με το Zcash έχοντας 0,527 και την μικρότερη με το Emercoin έχοντας 0,188. Το Emercoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Namecoin έχοντας 0,302 και την μικρότερη με το Dash έχοντας 0,188. Το Ethereum παρουσιάζει την μεγαλύτερη συσχέτιση με το Zcash, έχοντας 0,480 και την μικρότερη με το Emercoin, έχοντας 0,272. Το Litecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Namecoin, έχοντας 0,401 και την μικρότερη με το Dash, έχοντας 0,262. Το Monero παρουσιάζει την μεγαλύτερη συσχέτιση με το Dash έχοντας 0,493 και την μικρότερη με το Emercoin, έχοντας 0,229. Το Namecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Monero, έχοντας 0,428 και την μικρότερη με το Dash, έχοντας 0,203. Τέλος, το Zcash παρουσιάζει την μεγαλύτερη συσχέτιση με το Dash, έχοντας 0,527 και την μικρότερη με το Emercoin, έχοντας 0,240.

### **6.2.2 Εμπειρικά ευρήματα έτους 2018**

Στους πίνακες 6.3 και 6.4 παρουσιάζονται τα εμπειρικά ευρήματα για τα οκτώ κρυπτονομίσματα που χρησιμοποιούνται περισσότερο εντός του σκοτεινού διαδικτύου για το διάστημα από 01.01.2018 έως 31.12.2018. Αναλυτικότερα, στον Πίνακα 6.3 παρουσιάζεται η απόδοση που παρουσίασαν την προαναφερθείσα περίοδο, η μέση ημερήσια απόδοση τους, η μέγιστη ημερήσια απόδοση τους και η ελάχιστη ημερήσια απόδοση τους αλλά και ο βαθμός επικινδυνότητάς τους, ενώ στον Πίνακα 6.4 εκτιμάται ο συντελεστής συσχέτισης των ημερησίων αποδόσεων τους.

**Πίνακας 6.3:** Στατιστικά ευρήματα επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το έτος 2018

	Δ% 31.12.18- 01.01.18	Average Daily Return (%)	Maximum Daily Return (%)	Minimum Daily Return (%)	Daily Standard Deviation (%)
Bitcoin	-73%	-0,27%	13,22%	-16,85%	4,24%
Ethereum	-83%	-0,32%	18,07%	-18,69%	5,60%
Namecoin	-86%	0,32%	60,16%	-68,59%	12,96%
Litecoin	-87%	-0,40%	33,73%	-19,09%	5,61%
Monero	-87%	-0,36%	19,27%	-22,80%	6,22%
Emercoin	-90%	-0,29%	49,81%	-25,65%	8,09%
Zcash	-90%	-0,39%	29,79%	-21,04%	6,43%
Dash	-92%	-0,52%	33,34%	-19,45%	6,17%

Πηγή Δεδομένων: Coinmarketcap.com

Σύμφωνα με τα αποτελέσματα του Πίνακα 6.3 στον οποίο η κατάταξη έχει πραγματοποιηθεί σε φθίνουσα σειρά ανάλογα με την απόδοση περιόδου, παρατηρούμε πως το κρυπτονόμισμα Bitcoin πραγματοποίησε την καλύτερη του διαστήματος 01.01.2018 - 31.12.2018 πετυχαίνοντας τις μικρότερες απώλειες χάνοντας -73% της αξίας του. Αντιθέτως, το κρυπτονόμισμα Dash είχε τις μεγαλύτερες απώλειες μεταξύ των συγκρινόμενων κρυπτονομισμάτων χάνοντας -92%.

Με βάση τον υπολογισμό της μέσης ημερήσιας απόδοσης του διαστήματος 01.01.2018-31.12.2018, το κρυπτονόμισμα Namecoin είχε την καλύτερη μεταξύ των εξεταζόμενων κρυπτονομισμάτων με 0,32% ενώ την χειρότερη είχε το Dash με -0,52%. Επίσης, με βάση τα αποτελέσματα του πίνακα την υψηλότερη μέγιστη απόδοση σε ημερήσια βάση πέτυχε το κρυπτονόμισμα Namecoin με 60,16% με την λιγότερο καλή να κάνει το Bitcoin με 13,22%. Ενώ όσον αφορά στην ελάχιστη ημερήσια απόδοση, μεγαλύτερες απώλειες σε ημερήσια βάση είχε το Namecoin, το οποίο έχασε -68,59%, ενώ τις λιγότερες είχε το Bitcoin το οποίο έχασε -16,85%.

Τέλος, όσον αφορά στην επικινδυνότητα των παραπάνω κρυπτονομισμάτων, παρατηρούμε πως την μεγαλύτερη ημερήσια τυπική απόκλιση παρουσίασε το κρυπτονόμισμα Namecoin με 12,96%, ενώ την μικρότερη το Bitcoin με 4,24%, φανερώνοντας μας μικρότερη μεταβλητότητα στις ημερήσιες αποδόσεις του μεταξύ των συγκρινόμενων κρυπτονομισμάτων.

**Πίνακας 6.4:** Ο συντελεστής συσχέτισης επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το έτος 2018

	BITCOIN	DASH	EMERCOIN	ETHEREUM	LITECOIN	MONERO	NAMECOIN	ZCASH
BITCOIN	1,000	0,802	0,534	0,813	0,835	0,826	0,297	0,733
DASH	0,802	1,000	0,508	0,807	0,802	0,823	0,217	0,787
EMERCOIN	0,534	0,508	1,000	0,499	0,493	0,524	0,169	0,490
ETHEREUM	0,813	0,807	0,499	1,000	0,827	0,790	0,251	0,752
LITECOIN	0,835	0,802	0,493	0,827	1,000	0,805	0,267	0,741
MONERO	0,826	0,823	0,524	0,790	0,805	1,000	0,220	0,784
NAMECOIN	0,297	0,217	0,169	0,251	0,267	0,220	1,000	0,198
ZCASH	0,733	0,787	0,490	0,752	0,741	0,784	0,198	1,000

Πηγή Δεδομένων: Coinmarketcap.com

Όπως μπορούμε να παρατηρήσουμε στον Πίνακα 6.4, που παρουσιάζονται τα αποτελέσματα της ανάλυσης του συντελεστή συσχέτισης, το κρυπτονόμισμα Bitcoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Monero, έχοντας 0,826 και την μικρότερη με το Namecoin, έχοντας 0,296. Το Dash παρουσιάζει την μεγαλύτερη συσχέτιση με το Monero, έχοντας 0,823 και την μικρότερη με το Namecoin, έχοντας 0,216. Το Emercoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin, έχοντας 0,534 και την μικρότερη με το Namecoin έχοντας 0,169. Το Ethereum παρουσιάζει την μεγαλύτερη συσχέτιση με το Litecoin, έχοντας 0,827 και την μικρότερη με το Namecoin, έχοντας 0,251. Το Litecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin, έχοντας 0,835 και την μικρότερη με το Namecoin, έχοντας 0,266. Το Monero παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin, έχοντας 0,826 και την μικρότερη με το Namecoin, έχοντας 0,220. Το Namecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin, έχοντας 0,297 και την μικρότερη με το Emercoin, έχοντας 0,169. Τέλος, το Zcash παρουσιάζει την μεγαλύτερη συσχέτιση με το Dash, έχοντας 0,787 και την μικρότερη με το Namecoin, έχοντας 0,198.

### 6.2.3 Εμπειρικά ευρήματα έτους 2019

Στους πίνακες 6.5 και 6.6 παρουσιάζονται τα εμπειρικά ευρήματα για τα οκτώ κρυπτονομίσματα που χρησιμοποιούνται περισσότερο εντός του σκοτεινού

διαδικτύου για το διάστημα από 01.01.2019 έως 31.12.2019. Αναλυτικότερα, στον Πίνακα 6.5 παρουσιάζεται η απόδοση που παρουσίασαν την προαναφερθείσα περίοδο, η μέση ημερήσια απόδοση τους, η μέγιστη ημερήσια απόδοση τους και η ελάχιστη ημερήσια απόδοση τους αλλά και ο βαθμός επικινδυνότητάς τους, ενώ στον Πίνακα 6.6 εκτιμάται ο συντελεστής συσχέτισης των ημερησίων αποδόσεων τους.

**Πίνακας 6.5:** Στατιστικά ευρήματα επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το έτος 2019

	Δ% 31.12.19- 01.01.19	Average Daily Return (%)	Maximum Daily Return (%)	Minimum Daily Return (%)	Daily Standard Deviation (%)
Bitcoin	87%	0,24%	17,36%	-14,09%	3,56%
Litecoin	29%	0,20%	30,82%	-16,50%	4,87%
Monero	-8%	0,08%	15,16%	-17,30%	4,20%
Ethereum	-8%	0,08%	15,60%	-16,74%	4,11%
Namecoin	-25%	0,30%	56,13%	-43,54%	8,35%
Dash	-49%	-0,10%	20,96%	-17,05%	3,91%
Zcash	-54%	-0,11%	13,96%	-18,40%	4,11%
Emercoin	-77%	-0,19%	42,88%	-17,93%	6,55%

Πηγή Δεδομένων: Coinmarketcap.com

Σύμφωνα με τα αποτελέσματα του Πίνακα 6.5 στον οποίο η κατάταξη έχει πραγματοποιηθεί σε φθίνουσα σειρά ανάλογα με την απόδοση περιόδου, παρατηρούμε πως το κρυπτονόμισμα Bitcoin πραγματοποίησε την καλύτερη του διαστήματος 01.01.2019 - 31.12.2019 πετυχαίνοντας 87%. Αντιθέτως, το κρυπτονόμισμα Emercoin την χειρότερη μεταξύ των συγκρινόμενων κρυπτονομισμάτων, έχοντας απώλειες -77%.

Με βάση τον υπολογισμό της μέσης ημερήσιας απόδοσης του διαστήματος 01.01.2019-31.12.2019, το κρυπτονόμισμα Namecoin είχε την καλύτερη μεταξύ των εξεταζόμενων κρυπτονομισμάτων με 0,30%, ενώ την χειρότερη είχε το Emercoin με -0,19%. Επίσης με βάση τα αποτελέσματα του πίνακα την υψηλότερη μέγιστη απόδοση σε ημερήσια βάση πέτυχε το κρυπτονόμισμα Namecoin με 56,13%, με την λιγότερο καλή να κάνει το Zcash με 13,96%. Ενώ όσον αφορά στην ελάχιστη ημερήσια απόδοση, μεγαλύτερες απώλειες σε ημερήσια βάση είχε το Namecoin, το οποίο έχασε -43,54%, ενώ τις λιγότερες είχε το Bitcoin το οποίο έχασε -14,09%.

Τέλος, όσον αφορά στην επικινδυνότητα των παραπάνω κρυπτονομισμάτων, παρατηρούμε πως την μεγαλύτερη ημερήσια τυπική απόκλιση παρουσίασε το

κρυπτονόμισμα Namecoin, με 8,35% ενώ την μικρότερη το Bitcoin, με 3,56%, φανερώνοντας μας μικρότερη μεταβλητότητα στις ημερήσιες αποδόσεις του μεταξύ των συγκρινόμενων κρυπτονομισμάτων.

**Πίνακας 6.6:** Ο συντελεστής συσχέτισης επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το έτος 2019

	BITCOIN	DASH	EMERCOIN	ETHEREUM	LITECOIN	MONERO	NAMECOIN	ZCASH
BITCOIN	1,000	0,769	0,341	0,821	0,728	0,757	0,471	0,702
DASH	0,769	1,000	0,286	0,814	0,733	0,767	0,414	0,772
EMERCOIN	0,341	0,286	1,000	0,347	0,290	0,309	0,128	0,275
ETHEREUM	0,821	0,814	0,347	1,000	0,816	0,774	0,402	0,784
LITECOIN	0,728	0,733	0,290	0,816	1,000	0,723	0,384	0,696
MONERO	0,757	0,767	0,309	0,774	0,723	1,000	0,386	0,730
NAMECOIN	0,471	0,414	0,128	0,402	0,384	0,386	1,000	0,397
ZCASH	0,702	0,772	0,275	0,784	0,696	0,730	0,397	1,000

Πηγή Δεδομένων: Coinmarketcap.com

Όπως μπορούμε να παρατηρήσουμε στον Πίνακα 6.6, που παρουσιάζονται τα αποτελέσματα της ανάλυσης του συντελεστή συσχέτισης, το κρυπτονόμισμα Bitcoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Dash, έχοντας 0,769 και την μικρότερη με το Emercoin, έχοντας 0,341. Το Dash παρουσιάζει την μεγαλύτερη συσχέτιση με το Zcash, έχοντας 0,772 και την μικρότερη με το Emercoin, έχοντας 0,286. Το Emercoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Ethereum, έχοντας 0,347 και την μικρότερη με το Namecoin, έχοντας 0,128. Το Ethereum παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin, έχοντας 0,821 και την μικρότερη με το Emercoin, έχοντας 0,346. Το Litecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Ethereum, έχοντας 0,816 και την μικρότερη με το Namecoin, έχοντας 0,384. Το Monero παρουσιάζει την μεγαλύτερη συσχέτιση με το Ethereum, έχοντας 0,774 και την μικρότερη με το Emercoin, έχοντας 0,309. Το Namecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin, έχοντας 0,471 και την μικρότερη με το Emercoin, έχοντας 0,128. Τέλος, το Zcash παρουσιάζει την μεγαλύτερη συσχέτιση με το Ethereum, έχοντας 0,784 και την μικρότερη με το Emercoin έχοντας 0,275.

## 6.2.4 Εμπειρικά ευρήματα έτους 2020-03/2021

Στους πίνακες 6.7 και 6.8 παρουσιάζονται τα εμπειρικά ευρήματα για τα οκτώ κρυπτονομίσματα που χρησιμοποιούνται περισσότερο εντός του σκοτεινού διαδικτύου για το διάστημα από 01.01.2020 έως 30.03.2021. Αναλυτικότερα, στον Πίνακα 6.7 παρουσιάζεται η απόδοση που παρουσίασαν την προαναφερθείσα περίοδο, η μέση ημερήσια απόδοση τους, η μέγιστη ημερήσια απόδοση τους και η ελάχιστη ημερήσια απόδοση τους αλλά και ο βαθμός επικινδυνότητάς τους, ενώ στον Πίνακα 6.8 εκτιμάται ο συντελεστής συσχέτισης των ημερησίων αποδόσεών τους.

**Πίνακας 6.7:** Στατιστικά ευρήματα επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το διάστημα 2020-03.2021

	Δ% 30.03.21- 01.01.20	Average Daily Return (%)	Maximum Daily Return (%)	Minimum Daily Return (%)	Daily Standard Deviation (%)
Ethereum	1311%	0,73%	25,95%	-42,35%	5,21%
Bitcoin	718%	0,55%	18,75%	-37,17%	4,01%
Zcash	450%	0,57%	24,65%	-33,82%	6,22%
Monero	437%	0,50%	25,46%	-38,99%	4,96%
Dash	417%	0,59%	57,03%	-36,83%	6,92%
Litecoin	368%	0,49%	21,05%	-36,17%	5,28%
Emercoin	310%	0,58%	88,86%	-37,84%	7,91%
Namecoin	261%	0,73%	111,54%	-43,55%	10,06%

Πηγή Δεδομένων: Coinmarketcap.com

Σύμφωνα με τα αποτελέσματα του Πίνακα 6.7 στον οποίο η κατάταξη έχει πραγματοποιηθεί σε φθίνουσα σειρά ανάλογα με την απόδοση περιόδου, παρατηρούμε πως το κρυπτονόμισμα Ethereum πραγματοποίησε την καλύτερη του διαστήματος 01.01.2020 - 30.03.2021, πετυχαίνοντας 1.311%. Αντιθέτως, το κρυπτονόμισμα με την χειρότερη μεταξύ των συγκρινόμενων κρυπτονομισμάτων, ήταν το Namecoin με 261%.

Με βάση τον υπολογισμό της μέσης ημερήσιας απόδοσης του διαστήματος 01.01.2020-30.03.2021, το κρυπτονόμισμα Ethereum είχε την καλύτερη μεταξύ των εξεταζόμενων κρυπτονομισμάτων με 0,73%, ενώ την χειρότερη είχε το Litecoin, με 0,49%. Επίσης, με βάση τα αποτελέσματα του πίνακα την υψηλότερη μέγιστη απόδοση σε ημερήσια βάση πέτυχε το κρυπτονόμισμα Namecoin, με 111,54% με

την λιγότερο καλή να κάνει το Bitcoin με 18,75%. Ενώ όσον αφορά στην ελάχιστη ημερήσια απόδοση, μεγαλύτερες απώλειες σε ημερήσια βάση είχε το Namecoin, το οποίο έχασε -44,55%, ενώ τις λιγότερες είχε το Zcash, το οποίο έχασε -33,82%.

Τέλος, όσον αφορά στην επικινδυνότητα των παραπάνω κρυπτονομισμάτων, παρατηρούμε πως την μεγαλύτερη ημερήσια τυπική απόκλιση παρουσίασε το κρυπτονόμισμα Namecoin, με 10,06% ενώ την μικρότερη το Bitcoin με 4,01%, φανερώνοντας μας μικρότερη μεταβλητότητα στις ημερήσιες αποδόσεις του μεταξύ των συγκρινόμενων κρυπτονομισμάτων.

**Πίνακας 6.8:** Ο συντελεστής συσχέτισης επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το διάστημα 2020-03.2021

	BITCOIN	DASH	EMERCOIN	ETHEREUM	LITECOIN	MONERO	NAMECOIN	ZCASH
BITCOIN	1,000	0,535	0,327	0,796	0,805	0,686	0,432	0,604
DASH	0,535	1,000	0,162	0,548	0,617	0,686	0,344	0,803
EMERCOIN	0,327	0,162	1,000	0,278	0,242	0,229	0,148	0,181
ETHEREUM	0,796	0,548	0,278	1,000	0,820	0,669	0,367	0,645
LITECOIN	0,805	0,617	0,242	0,820	1,000	0,700	0,342	0,676
MONERO	0,686	0,686	0,229	0,669	0,700	1,000	0,313	0,711
NAMECOIN	0,432	0,344	0,148	0,367	0,342	0,313	1,000	0,383
ZCASH	0,604	0,803	0,181	0,645	0,676	0,711	0,383	1,000

Πηγή Δεδομένων: Coinmarketcap.com

Όπως μπορούμε να παρατηρήσουμε στον Πίνακα 6.8, που παρουσιάζονται τα αποτελέσματα της ανάλυσης του συντελεστή συσχέτισης, το κρυπτονόμισμα Bitcoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Litecoin, έχοντας 0,805 και την μικρότερη με το Emercoin, έχοντας 0,326. Το Dash παρουσιάζει την μεγαλύτερη συσχέτιση με το Zcash, έχοντας 0,803 και την μικρότερη με το Emercoin, έχοντας 0,162. Το Emercoin, παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin, έχοντας 0,327 και την μικρότερη με το Namecoin, έχοντας 0,148. Το Ethereum παρουσιάζει την μεγαλύτερη συσχέτιση με το Litecoin, έχοντας 0,820 και την μικρότερη με το Emercoin, έχοντας 0,278. Το Litecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Ethereum, έχοντας 0,820 και την μικρότερη με το Emercoin, έχοντας 0,278. Το Monero παρουσιάζει την μεγαλύτερη συσχέτιση με το Dash και το Bitcoin, έχοντας 0,686, και την μικρότερη με το Emercoin, έχοντας 0,229. Το Namecoin παρουσιάζει



την μεγαλύτερη συσχέτιση με το Bitcoin, έχοντας 0,432 και την μικρότερη με το Emercoin, έχοντας 0,148. Τέλος, το Zcash παρουσιάζει την μεγαλύτερη συσχέτιση με το Dash, έχοντας 0,803 και την μικρότερη με το Emercoin, έχοντας 0,181.

## 6.2.5 Εμπειρικά ευρήματα έτους 2017-03/2021

Στους πίνακες 6.9 και 6.10 παρουσιάζονται τα εμπειρικά ευρήματα για τα οκτώ κρυπτονομίσματα που χρησιμοποιούνται περισσότερο εντός του σκοτεινού διαδικτύου για το διάστημα από 01.01.2017 έως 30.03.2021. Αναλυτικότερα, στον Πίνακα 6.9 παρουσιάζεται η απόδοση που παρουσίασαν την προαναφερθείσα περίοδο, η μέση ημερήσια απόδοση τους, η μέγιστη ημερήσια απόδοση τους και η ελάχιστη ημερήσια απόδοση τους αλλά και ο βαθμός επικινδυνότητάς τους, ενώ στον Πίνακα 6.10 εκτιμάται ο συντελεστής συσχέτισης των ημερησίων αποδόσεων τους.

**Πίνακας 6.9:** Στατιστικά ευρήματα επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το διάστημα 2017-03.2021

	Δ% 30.03.21- 01.01.17	Average Daily Return (%)	Maximum Daily Return (%)	Minimum Daily Return (%)	Daily Standard Deviation (%)
Ethereum	22495%	0,51%	33,66%	-42,35%	5,69%
Bitcoin	5802%	0,35%	25,25%	-37,17%	4,24%
Litecoin	4261%	0,43%	66,59%	-36,17%	6,27%
Dash	1829%	0,39%	57,03%	-36,83%	6,54%
Monero	1657%	0,36%	53,77%	-38,99%	5,99%
Namecoin	579%	0,65%	111,54%	-68,59%	10,54%
Zcash	218%	0,27%	69,58%	-33,82%	6,33%
Emercoin	90%	0,38%	92,94%	-40,86%	8,73%

Πηγή Δεδομένων: Coinmarketcap.com

Σύμφωνα με τα αποτελέσματα του Πίνακα 6.9 στον οποίο η κατάταξη έχει πραγματοποιηθεί σε φθίνουσα σειρά ανάλογα με την απόδοση περιόδου, παρατηρούμε πως το κρυπτονομίσμα Ethereum πραγματοποίησε την καλύτερη του διαστήματος 01.01.2020 - 30.03.2021 πετυχαίνοντας 22.495%. Αντιθέτως, το κρυπτονομίσμα με τη χειρότερη μεταξύ των συγκρινόμενων κρυπτονομισμάτων, ήταν το Emercoin με 90%.

Με βάση τον υπολογισμό της μέσης ημερήσιας απόδοσης του διαστήματος 01.01.2020-30.03.2021, το κρυπτονόμισμα Namecoin είχε την καλύτερη μεταξύ των εξεταζόμενων κρυπτονομισμάτων με 0,65%, ενώ την χειρότερη είχε το Zcash με 0,27%. Επίσης με βάση τα αποτελέσματα του πίνακα την υψηλότερη μέγιστη απόδοση σε ημερήσια βάση πέτυχε το κρυπτονόμισμα Namecoin, με 111,54% με την λιγότερο καλή να κάνει το Bitcoin με 25,25%. Ενώ όσον αφορά την ελάχιστη ημερήσια απόδοση, μεγαλύτερες απώλειες σε ημερήσια βάση είχε το Namecoin, το οποίο έχασε -68,59%, ενώ τις λιγότερες είχε το Zcash το οποίο έχασε -33,82%.

Τέλος, όσον αφορά στην επικινδυνότητα των παραπάνω κρυπτονομισμάτων, παρατηρούμε πως την μεγαλύτερη ημερήσια τυπική απόκλιση παρουσίασε το κρυπτονόμισμα Namecoin με 10,54%, ενώ την μικρότερη το Bitcoin με 4,24%, φανερώνοντας μας μικρότερη μεταβλητότητα στις ημερήσιες αποδόσεις του μεταξύ των συγκρινόμενων κρυπτονομισμάτων.

**Πίνακας 6.10:** Ο συντελεστής συσχέτισης επιλεγμένων κρυπτονομισμάτων που χρησιμοποιούνται για συναλλαγές στο σκοτεινό διαδίκτυο για το διάστημα 2020-2021

	BITCOIN	DASH	EMERCOIN	ETHEREUM	LITECOIN	MONERO	NAMECOIN	ZCASH
BITCOIN	1,000	0,539	0,360	0,646	0,627	0,626	0,383	0,542
DASH	0,539	1,000	0,262	0,566	0,518	0,645	0,270	0,695
EMERCOIN	0,360	0,262	1,000	0,338	0,312	0,310	0,197	0,287
ETHEREUM	0,646	0,566	0,338	1,000	0,620	0,628	0,344	0,625
LITECOIN	0,627	0,518	0,312	0,620	1,000	0,573	0,337	0,533
MONERO	0,626	0,645	0,310	0,628	0,573	1,000	0,325	0,634
NAMECOIN	0,383	0,270	0,197	0,344	0,337	0,325	1,000	0,296
ZCASH	0,542	0,695	0,287	0,625	0,533	0,634	0,296	1,000

Πηγή Δεδομένων: Coinmarketcap.com

Όπως μπορούμε να παρατηρήσουμε στον Πίνακα 6.10, που παρουσιάζονται τα αποτελέσματα της ανάλυσης του συντελεστή συσχέτισης, το κρυπτονόμισμα Bitcoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Ethereum, έχοντας 0,646 και την μικρότερη με το Emercoin, έχοντας 0,360. Το Dash παρουσιάζει την μεγαλύτερη συσχέτιση με το Zcash, έχοντας 0,695 και την μικρότερη με το Emercoin, έχοντας 0,262. Το Emercoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Ethereum, έχοντας 0,338 και την μικρότερη με το Namecoin έχοντας 0,196. Το Ethereum παρουσιάζει

την μεγαλύτερη συσχέτιση με το Bitcoin έχοντας 0,646 και την μικρότερη με το Emercoin, έχοντας 0,338. Το Litecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin έχοντας 0,627 και την μικρότερη με το Emercoin έχοντας 0,312. Το Monero παρουσιάζει την μεγαλύτερη συσχέτιση με το Dash έχοντας 0,645 και την μικρότερη με το Emercoin, έχοντας 0,310. Το Namecoin παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin έχοντας 0,383 και την μικρότερη με το Emercoin, έχοντας 0,196. Τέλος, το Zcash παρουσιάζει την μεγαλύτερη συσχέτιση με το Dash, έχοντας 0,695 και την μικρότερη με το Emercoin, έχοντας 0,286.

### 6.3 Συμπεράσματα έκτου κεφαλαίου

Σύμφωνα με την ανάλυση των εμπειρικών ευρημάτων καταλήγουμε στα παρακάτω συμπεράσματα. Αρχικά πως με βάση τα αποτελέσματα που παρουσιάστηκαν, την καλύτερη απόδοση περιόδου για το διάστημα της ανάλυσης μας πέτυχε το κρυπτονόμισμα Ethereum καθώς από την 1.1.2017 μέχρι την 31.03.2021 πέτυχε 22.495% με την τιμή του να εκτοξεύεται από τα 8,17\$ στα \$1,846.03. Ενώ αντιθέτως, εκείνο με την λιγότερο καλή μεταξύ των συγκρινόμενων κρυπτονομισμάτων να την πετυχαίνει το Namecoin με 261%. Στα επιμέρους διαστήματα της ανάλυσης για το έτος 2017 καλύτερη είχε το Dash με 9.265% ενώ χειρότερη είχε το ZCash με 943%. Το 2018 το οποίο ήταν ένα πτωτικό διάστημα για την αγορά των κρυπτονομισμάτων, τις μικρότερες απώλειες είχε το Bitcoin το οποίο έπεσε 72,6%, ενώ εκείνο με τις μεγαλύτερες απώλειες ήταν το Dash το οποίο έχασε το 92,5% της αξίας του. Το 2019 το Bitcoin είχε την μεγαλύτερη άνοδο κερδίζοντας 87%, με το Emercoin να έχει τις μεγαλύτερες απώλειες με -77%. Ενώ τέλος, το διάστημα από το 2020 έως το Μάρτιο 2021 είχε το Ethereum το οποίο κέρδισε 1.311% πετυχαίνοντας την καλύτερη απόδοση, με το Namecoin να πετυχαίνει την μικρότερη ή οποία ήταν 261%.

Επίσης σύμφωνα με τις εκτιμήσεις που πραγματοποιήσαμε το κρυπτονόμισμα με την καλύτερη μέση ημερήσια απόδοση για το συνολικό διάστημα της ανάλυσης δηλαδή από το 2017 έως τον Μάρτιο του 2021 ήταν το Namecoin με 0,65%, ενώ εκείνο με την μικρότερη ήταν το Zcash με 0,27%. Για το έτος 2017, εκείνο με την μεγαλύτερη ήταν το Dash με 1,56% ενώ εκείνο με την μικρότερη ήταν το Bitcoin με 0,85%. Για το έτος 2018, εκείνο με την μεγαλύτερη ήταν το Namecoin με 0,32% ενώ εκείνο με την μικρότερη ήταν το Dash το οποίο έχανε 0,52% κατά μέσο όρο σε ημερήσια βάση. Για το έτος 2019, εκείνο με την μεγαλύτερη ήταν και πάλι το Namecoin με 0,30%, ενώ εκείνο με την μικρότερη ήταν το Emercoin με -0,19%. Τέλος, για το διάστημα από το 2020 έως τον Μάρτιο του 2021 εκείνο με την μεγαλύτερη μέση ημερήσια απόδοση ήταν το Ethereum το οποίο κέρδιζε 0,73% ενώ το Litecoin ήταν εκείνο με την μικρότερη με 0,49%.

Ακόμη, να αναφέρουμε πως το Namecoin για το σύνολο του εξεταζόμενου διαστήματος, δηλαδή από το 2017 έως τον Μάρτιο του 2021 πέτυχε την μεγαλύτερη ημερήσια απόδοση κερδίζοντας 111%, αλλά και την χειρότερη χάνοντας 68,59%.

Επιπρόσθετα, όσον αφορά τον βαθμό επικινδυνότητας των οκτώ κρυπτονομισμάτων που συμμετείχαν στην ανάλυση, το Bitcoin ήταν το λιγότερο

επικίνδυνο κρυπτονόμισμα σύμφωνα με την τυπική απόκλιση των αποδόσεων του σε όλα τα εξεταζόμενα έτη, αλλά και στο σύνολο της περιόδου. Πιο συγκεκριμένα, το έτος 2017 παρουσιάζει ημερήσια τυπική απόκλιση 5,00%, το 2018 4,24%, το 2019 2,56%, το 2020 έως το Μάρτιο του 2021 4,01% ενώ το συνολικό διάστημα 2017 έως το Μάρτιο του 2021 και πάλι παραμένει το λιγότερο επικίνδυνο με 4,24% ημερήσια τυπική απόκλιση. Αντιθέτως, το κρυπτονόμισμα Namecoin με εξαίρεση το 2017 που κατατάχθηκε δεύτερο, όλες τις υπόλοιπες περιόδους ήταν το πιο επικίνδυνο με ημερήσια τυπική απόκλιση 10,42% (έτος 2017), 12,96% (έτος 2018), 8,35% (έτος 2019) 10,06% (διάστημα 2020-03.2021) και 10,54% (διάστημα 2017-03.2021).

Επίσης, σύμφωνα με την εκτίμηση του συντελεστή συσχέτισης μεταξύ των κρυπτονομισμάτων της ανάλυσης, για το συνολικό διάστημα δηλαδή από το 2017 έως το Μάρτιο του 2021, η υψηλότερη συσχέτιση παρατηρήθηκε μεταξύ του κρυπτονομίσματος Dash και του Zcash, η οποία ήταν ίση με 0,695, ενώ η μικρότερη μεταξύ του κρυπτονομίσματος Namecoin και Emercoin, που ήταν ίση με 0,196. Όσον αφορά στα επιμέρους έτη, το 2017 το Dash με το Zcash είχαν την υψηλότερη η οποία ισούταν με 0,527, ενώ η μικρότερη παρατηρήθηκε μεταξύ του Dash και του Emercoin, η οποία ήταν ίση με 0,188. Για το έτος 2018, το Bitcoin με το Litecoin είχαν την υψηλότερη η οποία ισούταν με 0,835, ενώ η μικρότερη παρατηρήθηκε μεταξύ του Namecoin και του Emercoin, η οποία ήταν ίση με 0,169. Το έτος 2019 το Bitcoin παρουσίασε τον υψηλότερο συντελεστή συσχέτισης με το Ethereum, ο οποίος ήταν ίσος με 0,821, ενώ η μικρότερη παρατηρήθηκε μεταξύ του Namecoin και του Emercoin, η οποία ήταν ίση με 0,128. Τέλος, για το διάστημα από το 2020 έως το Μάρτιο του 2021, ο μεγαλύτερος συντελεστής συσχέτισης ήταν ανάμεσα στο Ethereum και το Litecoin ο οποίος ήταν 0,820, ενώ ο μικρότερος ανάμεσα στο Namecoin και το Emercoin ο οποίος ήταν 0,148.

Συμπερασματικά λοιπόν, σύμφωνα με την ανάλυση όλων των εμπειρικών ευρημάτων, οδηγούμαστε στο συμπέρασμα πως οι χρήστες του σκοτεινού διαδικτύου εάν εξαιρέσουμε τις τεχνολογικές διαφοροποιήσεις που έχουν τα παραπάνω κρυπτονομίσματα, καθώς το καθένα από αυτά προσφέρει διαφορετικά πλεονεκτήματα και διαφορετικά μειονεκτήματα στην χρήση του, καταλήγουμε πως το Bitcoin είναι λογικό να προτιμάται καθώς διαχρονικά έχει πολύ καλές αποδόσεις, χαμηλή μεταβλητότητα σε σχέση με τα υπόλοιπα.

## Κεφάλαιο 7: Συμπεράσματα Διπλωματικής εργασίας

Όταν εμφανίζεται μια νέα τεχνολογία έρχεται με δύο υποσχέσεις. Πρώτον, ότι προσφέρει μεγάλες ευκαιρίες στις υπάρχουσες πρακτικές, καθιστώντας τις πιο αποτελεσματικές και ασφαλείς, και δεύτερον, στους πιθανούς κινδύνους και προκλήσεις που μπορεί να εμφανιστούν. Το ίδιο ισχύει και για την περίπτωση των κρυπτονομισμάτων και κατ' επέκταση του blockchain, της τεχνολογίας πίσω από αυτά.

Μπορεί η ιδέα πίσω από την δημιουργία του blockchain να προέρχεται από τα τέλη της δεκαετίας του 1990 ως ένα peer-to-peer αποκεντρωμένο καθολικό δίκτυο συναλλαγών στο οποίο οι συμμετέχοντες χρησιμοποιώντας το μπορούν να επιβεβαιώσουν συναλλαγές χωρίς να απαιτείται η έγκριση τους από κάποια κεντρική αρχή που τις ελέγχει, όμως η τεχνολογία αυτή επικοινωνήθηκε κυρίως μέσω του Bitcoin το 2008.

Η τεχνολογία αυτή προσέλκυσε το ενδιαφέρον τόσο των καλοπροαίρετων όσο και των κακοπροαίρετων χρηστών, με τους τελευταίους να το χρησιμοποιούν ως εργαλείο για παράνομες ενέργειες και πρακτικές, με αυτό να συμβαίνει κυρίως μέσω των σκοτεινών αγορών του διαδικτύου. Να αναφέρουμε πως οι σκοτεινές αγορές δεν είναι απαραίτητα συνδεδεμένες με τις παράνομες και εγκληματικές δραστηριότητες, αλλά αποκτούν παράνομο χαρακτήρα λόγω των προϊόντων που επιτρέπονταν να πωλούνται σε αυτές όπως ναρκωτικά, όπλα ή άλλα παράνομα προϊόντα και παραβιάζουν το νόμο αποκτώντας παράνομο χαρακτήρα.

Η φύση των κρυπτονομισμάτων, που είναι ψηφιακή τους δίνει την δυνατότητα να μπορούν να έχουν μεγάλο πεδίο εφαρμογής σε διάφορες δραστηριότητες. Μια εξ αυτών είναι η χρήση τους ως τρόπου πληρωμής στο σκοτεινό διαδίκτυο - Dark Web/ DarkNet. Τα κρυπτονομίσματα προτιμώνται από τους τους χρήστες του σκοτεινού διαδικτύου, διότι προσφέρουν ανωνυμία, η οποία είναι ο βασικότερος λόγος προτίμησης, καθώς δεν μπορούν να εντοπιστούν εύκολα, αποκρύπτοντας τις διευθύνσεις που προέρχονται οι συναλλαγές, επίσης μπορούν να συμβάλλουν στην νομιμοποίηση εσόδων από παράνομες δραστηριότητες, κοινώς αναφερόμενη ως ξέπλυμα χρήματος, καθώς στον μικρό έως μηδενικό έλεγχο φορολογικής και γενικότερα κοινής ρυθμιστικής κατεύθυνσης, καθώς από την στιγμή που δημιουργήθηκαν δεν διέθεταν κάποια κοινή πρακτική όσον αφορούσε την φορολογική τους υπόσταση.

Τα κρυπτονομίσματα που χρησιμοποιούνται περισσότερο στο σκοτεινό διαδίκτυο, παρά τις διαφορές που μπορεί να παρουσιάζουν στην τεχνολογία τους, όλα συγκλίνουν προς ένα κοινό χαρακτηριστικό, την προστασία της ιδιωτικής ταυτότητας και της ανωνυμίας των χρηστών τους. Αυτό μπορούμε να το παρατηρήσουμε αρκεί να δούμε πως η συνολική δραστηριότητα του Bitcoin στο σκοτεινό διαδίκτυο αυξήθηκε από το έτος 2017 κατά 340%, με τους προμηθευτές προϊόντων εντός αυτού να έλαβαν 47.000 Bitcoin το πρώτο τρίμηνο του 2020, και μάλιστα 2,8 δισεκατομμύρια δολάρια σε Bitcoin (BTC) που μεταφέρθηκαν μέσα από εγκληματικές δραστηριότητες μέσω ανταλλακτηρίων κρυπτονομισμάτων το έτος 2019, όμως το μερίδιό του Bitcoin στη συνολική αγορά ενδέχεται να μειωθεί στο μέλλον, δεδομένης της θετικής στάσης απέναντι σε άλλα κρυπτονομίσματα από την πλευρά των πωλητών των προϊόντων.

Μπορεί αρχικά οι αγορές του Darkweb να βασίζονταν στην χρησιμοποίηση μόνο του Bitcoin, ωστόσο τα τελευταία χρόνια αυτό έχει αλλάξει και ο αυξανόμενος των κρυπτονομισμάτων στην παγκόσμια αγορά αναγνωρίζει τα οφέλη από την προσφορά και άλλων κρυπτονομισμάτων. Το Litecoin, το Ethereum είναι μερικά παραδείγματα, ενώ το Monero γίνεται σταδιακά το πιο καθιερωμένο νόμισμα απορρήτου για συναλλαγές στο σκοτεινό διαδίκτυο, ενώ ακολουθεί το Zcash και το Dash. Όλα αυτά τα κρυπτονομίσματα που έχουν υψηλά επίπεδα απορρήτου ενδέχεται να αποτελούν σημαντικό εμπόδιο για τις αρχές επιβολής του νόμου για τον περιορισμό του σκοτεινού διαδικτύου.

Ένα από τα πιο γνωστά παραδείγματα σκοτεινών αγορών στο Dark web ήταν η περίπτωση του Silk Road, το οποίο εμφανίστηκε το 2011 μέχρι το 2016 και είχε χαρακτηριστεί ως το Amazon των ναρκωτικών, καθώς μέσω αυτού πραγματοποιούνταν παράνομο εμπόριο διάφορων προϊόντων όπως ναρκωτικών, όπλων, πορνογραφικού υλικού προσφέροντας ανωνυμία στις συναλλαγές μεταξύ εμπόρων και αγοραστών χρησιμοποιώντας τα κρυπτονομίσματα και κυρίως το Bitcoin για πληρωμές. Να αναφέρουμε πως για την πρόσβαση στις διαδικτυακές τοποθεσίες του Darkweb χρειάζεται ένα ειδικό πρόγραμμα περιήγησης όπως είναι τα δίκτυα TOR (The Onion Router) και TON (Telegram Open Network), καθώς αποκρύπτουν τις πραγματικές ταυτότητες των χρηστών και τις διευθύνσεις IP τους.

Έχοντας εμφανιστεί σχεδόν δέκα χρόνια πριν τα κρυπτονομίσματα, μπορούμε να πούμε πως ακόμα και σήμερα υπάρχει έλλειψη προτύπων συμπεριφοράς, κανονισμών, φορολογικής αντιμετώπισης κλπ από τις ρυθμιστικές

αρχές. Επειδή τα κρυπτονομίσματα απέκτησαν ιδιαίτερο ενδιαφέρον όχι μόνο σε εθνικό αλλά και σε παγκόσμιο επίπεδο, οι ρυθμιστικές αρχές από όλο τον κόσμο συμφωνούν ότι υπάρχει ανάγκη εναρμονισμένης προσέγγισης απέναντι σε αυτά. Η ανησυχία περισσότερο για την εξάπλωση του σκοτεινού διαδικτύου σε παγκόσμιο επίπεδο είναι συνεχής, και ο αριθμός των χρηστών που δραστηριοποιείται στο Darknet συνδέεται άμεσα με το πόσο αυστηρές είναι οι κυβερνητικές πολιτικές της εκάστοτε χώρας προς το διαδίκτυο και γενικότερα προς τον κυβερνοχώρο. Συνεπώς, οι χώρες στις οποίες το σκοτεινό διαδίκτυο χρησιμοποιείται περισσότερο είναι κυρίως οι Ηνωμένες Πολιτείες, η Ρωσία και ορισμένες Ευρωπαϊκές χώρες όπως η Γερμανία, η Ολλανδία και η Γαλλία, άρα και η εξάπλωση του είναι μεγαλύτερη. Για τον λόγο αυτό, τόσο η INTERPOL όσο και η Europol, που αποτελούν οργανισμούς που βοηθούν τις εθνικές αρχές επιβολής του νόμου στην καταπολέμηση του σοβαρού διεθνούς εγκλήματος και της τρομοκρατίας έχουν δημιουργήσει μια σειρά από μηχανισμούς και επιχειρήσεις περιορισμού των δραστηριοτήτων αυτών. Αναπτύσσονται διάφορες δράσεις για να περιοριστεί η εγκληματική δραστηριότητα στο σκοτεινό διαδίκτυο και να βοηθηθούν τις αστυνομικές αρχές σε παγκόσμιο επίπεδο για να είναι σε θέση να διερευνήσουν τα ψηφιακά εγκλήματα με περισσότερο αποτελεσματικό τρόπο. Έχουν αναπτύξει μια σειρά από μηχανισμούς ελέγχου όπως είναι μεταξύ άλλων το εργαλείο GraphSense, το Darkweb MoniTOR, το πρόγραμμα IOCTA κλπ, με απώτερο σκοπό την εξάλειψη των εγκληματικών δραστηριοτήτων στο σκοτεινό διαδίκτυο.

Τέλος, όσον αφορά στην συμβολή της διπλωματικής εργασίας, στην οποία εξετάστηκε μέσω μιας εμπειρικής και στατιστικής ανάλυσης ανάμεσα στα κρυπτονομίσματα Bitcoin, Ethereum, Litecoin, Monero, Zcash, DASH, Namecoin και EmerCoin, τα οποία χρησιμοποιούνται περισσότερο για συναλλαγές εντός του σκοτεινού διαδικτύου, διερευνήθηκε η πορεία τους, ο βαθμός επικινδυνότητας τους αλλά και η συσχέτισή που είχαν μεταξύ τους από το 2017 μέχρι τον Μάρτιο του 2021, με τελικό στόχο να διερευνηθεί ποιο ή ποιά θα μπορούσαν να αποτελέσουν καταλληλότερο μέσω πραγματοποίησης συναλλαγών, καταλήγοντας κυρίως στα ακόλουθα συμπεράσματα.

Αρχικά, πως την καλύτερη απόδοση περιόδου για το διάστημα της ανάλυσης μας πέτυχε το κρυπτονόμισμα Ethereum, καθώς από την 1.1.2017 μέχρι την 31.03.2021 πέτυχε 22.495%, με την τιμή του να εκτοξεύεται από τα 8,17\$ στα \$1,846.03. Ενώ αντιθέτως, εκείνο με την λιγότερο καλή μεταξύ των συγκρινόμενων κρυπτονομισμάτων, να την πετυχαίνει το Namecoin με 261%. Επίσης, για το 2018, το οποίο ήταν ένα πτωτικό διάστημα για την αγορά των κρυπτονομισμάτων, τις



μικρότερες απώλειες είχε το Bitcoin το οποίο έπεσε 72,6%, ενώ εκείνο με τις μεγαλύτερες απώλειες ήταν το Dash, το οποίο έχασε το 92,5% της αξίας του. Ενώ το 2019, το Bitcoin είχε την μεγαλύτερη άνοδο κερδίζοντας 87% σε σχέση με τα εξεταζόμενα κρυπτονομίσματα.

Επιπρόσθετα, όσον αφορά στον βαθμό επικινδυνότητας των οκτώ κρυπτονομισμάτων που συμμετείχαν στην ανάλυση, το Bitcoin ήταν το λιγότερο επικίνδυνο κρυπτονόμισμα σύμφωνα με την τυπική απόκλιση των αποδόσεων του σε όλα τα εξεταζόμενα έτη, αλλά και στο σύνολο της περιόδου. Πιο συγκεκριμένα, το έτος 2017 παρουσιάζει ημερήσια τυπική απόκλιση 5,00%, το 2018 4,24%, το 2019 2,56%, το 2020 έως το Μάρτιο του 2021 4,01%, ενώ το συνολικό διάστημα 2017 έως το Μάρτιο του 2021 και πάλι παραμένει το λιγότερο επικίνδυνο με 4,24% ημερήσια τυπική απόκλιση. Αντιθέτως το κρυπτονόμισμα Namecoin, με εξαίρεση το 2017 που κατατάχθηκε δεύτερο, ήταν το πιο επικίνδυνο με ημερήσια τυπική απόκλιση 10,42% (έτος 2017), 12,96% (έτος 2018), 8,35% (έτος 2019) 10,06% (διάστημα 2020-03.2021) και 10,54% (διάστημα 2017-03.2021).

Ακόμη, σύμφωνα με την εκτίμηση του συντελεστή συσχέτισης μεταξύ των κρυπτονομισμάτων της ανάλυσης, για το συνολικό διάστημα δηλαδή από το 2017 έως το Μάρτιο του 2021, η υψηλότερη συσχέτιση παρατηρήθηκε μεταξύ του κρυπτονομίσματος Dash και του Zcash, η οποία ήταν ίση με 0,695, ενώ η μικρότερη μεταξύ του κρυπτονομίσματος Namecoin και Emercoin, που ήταν ίση με 0,196. Ενώ αξίζει να αναφέρουμε πως το έτος 2018, το Bitcoin με το Litecoin είχαν την υψηλότερη, η οποία ισούταν με 0,835 καθώς και το έτος 2019 το Bitcoin παρουσίασε τον υψηλότερο συντελεστή συσχέτισης με το Ethereum, ο οποίος ήταν ίσος με 0,821.

Συμπερασματικά λοιπόν, σύμφωνα με την ανάλυση όλων των εμπειρικών ευρημάτων, οδηγούμαστε στο συμπέρασμα πως οι χρήστες του σκοτεινού διαδικτύου, εάν εξαιρέσουμε τις τεχνολογικές διαφοροποιήσεις που έχουν τα παραπάνω κρυπτονομίσματα, καθώς το καθένα από αυτά προσφέρει διαφορετικά πλεονεκτήματα και διαφορετικά μειονεκτήματα στην χρήση του, καταλήγουμε πως το Bitcoin είναι λογικό να προτιμάται, καθώς διαχρονικά έχει πολύ καλές αποδόσεις και χαμηλή μεταβλητότητα σε σχέση με τα υπόλοιπα.

# Βιβλιογραφία

## Επιστημονική

Abraham, C. (2018, October 13). The Origin Story of the Initial Coin Offering (ICO) Token Sale History

Afilipoaie A., Shortis P. (2015), Silk Road: After being closed twice, Swansea University

Bartoletti, M., & Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns.

Benedetti, H., & Kostovetsky, L. (2018). Digital Tulips? Returns to Investors in Initial Coin Offerings (SSRN)

Biddle P., England P., Peinado M., etc (2002), The Darknet and the Future of Content Distribution, Microsoft Corporation

Bonneau, J., Felten, E., Miller, A., & Narayanan, A. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press.

Bower, J. L., & Christensen, C. M. (1995). Disruptive Technologies: Catching the Wave.

Budish, E. (2018). The Economic Limits of Bitcoin and the Blockchain, 23.

Chanson, M., Gjoen, J., Risius, M., & Wortmann, F. (2018). Initial Coin Offerings (ICOs): The role of Social

Christensen, C. M., Raynor, M. E., & McDonald, R. (2015). What Is Disruptive Innovation? Harvard Business

Clark, J., & Narayanan, A. (2017), Bitcoin's Academic Pedigree. Communication of the ACM, 60(12), 36–45.

Crypto-Assets Shifflett, S., & Vigna, P. (2018). Some Traders Are Talking Up Cryptocurrencies, Then Dumping Them,

Cryptocurrencies Beneath the Bubble (2017). UBS

Efanov, D., & Roschin, P. (2018). The All-Pervasiveness of the Blockchain Technology. In The AllPervasiveness of the Blockchain Technology (Vol. 123, pp. 116–121). Procedia Computer Science

Financed Through Cryptocurrencies? (SSRN Scholarly Paper No. ID 3102645)

Fisch, C. (2019). Initial coin offerings (ICOs) to finance new ventures. Journal of Business Venturing, 34(1), 1–22.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2018). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is

- Friedman, H. H., & Friedman, L. W. (2009). The Global Financial Crisis of 2008: What Went Wrong? (SSRN Scholarly Paper No. ID 1356193)
- Fry, J., & Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, 47, 343–352.
- Gantori, S., Donovan, P., Ganesh, K., DeMichiel, M., Dennean, K., Trussari, F., & Klien, M. (2017).
- Groendahl, B. (2018). Austrian Bitcoin ‘Scam’ Triggers Police Search Across Europe - Bloomberg.
- Gupta, V. (2017, March 6). The Promise of Blockchain Is a World Without Middlemen.
- Hacker, P., & Thomale, C. (2017). Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law (SSRN Scholarly Paper No. ID 3075820)
- Hamrick, J. T., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T., & Vasek, M. (2018). The Economics of Cryptocurrency Pump and Dump Schemes (SSRN Scholarly Paper No. ID 3303365)
- Heidelberg: Springer Berlin Heidelberg
- Hileman, G., & Rauchs, M. (2017). 2017 Global Blockchain Benchmarking Study (SSRN Scholarly Paper No. ID 3040224)
- Houben, D. R., & Snyers, A. (2018). Cryptocurrencies and blockchain, 103.
- Katarzyna C. (2019), Cryptocurrencies: Opportunities, Risks and Challenges for anti-corruption compliance systems, OECD Global anti-corruption & intelligence forum
- Keatinge, T., Carlisle, D., & Keen, F. (2018). Virtual Currencies and terrorist financing: assessing the risks and evaluating responses
- Keidar, R., & Blemus, S. (2018). Cryptocurrencies and Market Abuse Risks: It’s Time for Self-Regulation (SSRN Scholarly Paper No. ID 3123881). Rochester, NY: Social Science Research Network
- Khatri, Y. (2018). FBI Arrests AriseBank CEO Over \$4 Million Crypto Fraud
- Knight, K. B. and J. (2009, September 16). Lehman’s Three Big Mistakes
- Memoria, F. (2017). Tracing Ethereum and Bitcoin? Darknet’s Two Biggest Marketplaces are Busted
- Memoria, F. (2018). First Bitcoin Cash Ransomware Makes It Impossible to Decrypt Files
- Moore, T., & Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In A.-
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System
- R. Sadeghi (Ed.), *Financial Cryptography and Data Security* (Vol. 7859, pp. 25–33). Berlin,

Scholarly Paper No. ID 3182169). Rochester, NY: Social Science Research Network.

Securities and Markets Stakeholder Group. (2018). Own Initiative Report on Initial Coin Offerings and

Xu, J., & Livshits, B. (2018). The Anatomy of a Cryptocurrency Pump-and-Dump Scheme

Φίλιππας Ν. (2005), Επενδύσεις, Εκδόσεις: Λογισοφία

## Ηλεκτρονική

Abraham, C. (2018, October 13). The Origin Story of the Initial Coin Offering (ICO) Token Sale History

Adriano, A. (2018, June). Crypto Bubble? An Historical Analysis of Financial Crises. IMF F&D Magazine,55(2)

Alexandre, A. (2018). New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams.

Bank für Internationalen Zahlungsausgleich, & Committee on Payments and Market Infrastructures. (2015).

Barysevich A., Solad A. (2018), Litecoin Emerges as the Next Dominant Dark Web Currency, ηλεκτρονικός ιστότοπος: <https://www.recordedfuture.com/dark-web-currency/>

Basel Institute on Governance. (2018). Basel AML Index 2018 Report.

Berkman F. (2013), New Dread Pirate Roberts Abandons Ship on Silk Road 2.0, ηλεκτρονικός ιστότοπος: <https://mashable.com/archive/silk-road-2-0-reopens>

Bieg M. (2021), File:Server-based-network.svg, ηλεκτρονικός ιστότοπος: <https://commons.wikimedia.org/wiki/File:Server-based-network.svg>

Brandom R. (2014), the Silk Road 2 has been hacked for \$2.7 million, ηλεκτρονικός ιστότοπος: <https://www.theverge.com/2014/2/13/5409340/the-silk-road-2-has-been-hacked-for-2-7-million>

Browne, R. (2017). Hackers withdraw \$143,000 from bitcoin wallets tied to WannaCry ransomware.

"Buntinx Jp. (2016), ηλεκτρονικός ιστότοπος: <https://bitcoinist.com/silk-road-3-0-announces-bitcoin-charity-drive/>

Silk Road 3.0 Announces Bitcoin Charity Drive, "

Businessinsider.com, 2013, TOR- Silk-road deep web, ηλεκτρονικός ιστότοπος: <https://www.businessinsider.com/TOR%20-silk-road-deep-web-2013-3>

Castillo M. (2020), Cypherpunk Zooko Wilcox Aims To Bring Anonymous Zcash To Law-Abiding Masses, ηλεκτρονικός ιστότοπος: <https://www.forbes.com/sites/michaeldelcastillo/2020/05/06/cypherpunk-zooko-wilcox-wants-zcash-mainstream/?sh=544736f9416b>

Cheng, E. (2018). Japanese cryptocurrency exchange loses more than \$500 million to hackers.

CipherTrace. (2018). Cryptocurrency Anti-Money Laundering report Q2.

Coin Gecko.com, (2021), Bitcoin (BTC), ηλεκτρονικός ιστότοπος:  
<https://www.coin Gecko.com/en/coins/bitcoin>

Coin Gecko.com, (2021), Dash (DASH), ηλεκτρονικός ιστότοπος:  
<https://www.coin Gecko.com/en/coins/dash>

Coin Gecko.com, (2021), EmerCoin (EMC), ηλεκτρονικός ιστότοπος:  
<https://www.coin Gecko.com/en/coins/emercoin>

Coin Gecko.com, (2021), Ethereum (ETH), ηλεκτρονικός ιστότοπος:  
<https://www.coin Gecko.com/en/coins/ethereum>

Coin Gecko.com, (2021), Litecoin (LTC), ηλεκτρονικός ιστότοπος:  
<https://www.coin Gecko.com/en/coins/litecoin>

Coin Gecko.com, (2021), Monero (XMR), ηλεκτρονικός ιστότοπος:  
<https://www.coin Gecko.com/en/coins/monero>

Coin Gecko.com, (2021), Zcash (ZEC), ηλεκτρονικός ιστότοπος:  
<https://www.coin Gecko.com/en/coins/zcash>

Coinmarketcap.com, (2021), Bitcoin, ηλεκτρονικός ιστότοπος:  
<https://coinmarketcap.com/currencies/bitcoin/>

Coinmarketcap.com, (2021), Dash,  
ηλεκτρονικός ιστότοπος:<https://coinmarketcap.com/currencies/dash/>

Coinmarketcap.com, (2021), Emercoin, ηλεκτρονικός ιστότοπος:  
<https://coinmarketcap.com/currencies/emercoin/>

Coinmarketcap.com, (2021), Ethereum, ηλεκτρονικός ιστότοπος:  
<https://coinmarketcap.com/currencies/ethereum/>

Coinmarketcap.com, (2021), Litecoin, ηλεκτρονικός ιστότοπος:  
<https://coinmarketcap.com/currencies/litecoin/>

Coinmarketcap.com, (2021), Monero, ηλεκτρονικός ιστότοπος:  
<https://coinmarketcap.com/currencies/monero/>

Coinmarketcap.com, (2021), Zcash, ηλεκτρονικός ιστότοπος:  
<https://coinmarketcap.com/currencies/zcash/>

Cointelegraph.com (2021), Darknet News, ηλεκτρονικός ιστότοπος:  
<https://cointelegraph.com/tags/darknet>

Cook J. (2014), FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0, ηλεκτρονικός ιστότοπος:  
<https://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11>

Crypto-Assets Shifflett, S., & Vigna, P. (2018). Some Traders Are Talking Up Cryptocurrencies, Then Dumping Them,

Crystal analytics team (2020), Darknet Use and Bitcoin — A Crypto Activity Report by Crystal Blockchain, ηλεκτρονικός ιστότοπος:

<https://crystalblockchain.com/articles/darknet-use-and-bitcoin-a-crypto-activity-report-by-crystal-blockchain>

Crystal Blockchain (2020), Darknet Use and Bitcoin — A Crypto Activity Report by Crystal Blockchain, ηλεκτρονικός ιστότοπος: <https://medium.com/meetbitfury/darknet-use-and-bitcoin-a-crypto-activity-report-by-crystal-blockchain-353a8678730>

Cuthbertson A. (2019), Dark web criminals switch to popular apps to sell drugs, using bots and secret graffiti messages to do business, ηλεκτρονικός ιστότοπος: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-app-drugs-sell-channels-bots-crime-graffiti-dropgangs-dark-web-a8814671.html>

Deepdotweb.com (2017), silk road3.1 got hacked owner claims bankruptcy, ηλεκτρονικός ιστότοπος: <https://www.deepdotweb.com/2017/08/02/silk-road-3-1-got-hacked-owner-claims-bankruptcy/>

EBA. (2014). EBA Opinion on Virtual Currencies.

Esteves, R. (2018). Savedroid Fakes \$50 Million ICO Exit Scam, Community Outraged.

Europa.eu (2021), Οργανισμός της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Europol), ηλεκτρονικός ιστότοπος: [https://europa.eu/european-union/about-eu/agencies/europol\\_el](https://europa.eu/european-union/about-eu/agencies/europol_el)

European Central Bank. (2015). Virtual currency schemes: a further analysis. Frankfurt am Main: EuropeanCentral Bank

Europol (2020), internet organised crime threat assessment, ηλεκτρονικός ιστότοπος: <https://www.europol.europa.eu/iocta-report>

EY. (2018). IFRS: Accounting for crypto-assets

FabricVentures, & TokenData. (2018). The State of the Token Market Final2.pdf.

Faridi O. (2020), Bitcoin (BTC) Remains a Widely-Used Cryptocurrency for Dark Web Transactions, a New Report Claims, ηλεκτρονικός ιστότοπος: <https://www.crowdfundinsider.com/2020/05/161146-bitcoin-btc-remains-a-widely-used-cryptocurrency-for-dark-web-transactions-a-new-report-claims/>

Faridi O. (2020), Chainalysis: Binance, Huobi, other Major Exchanges Used to Transfer \$2.8 Billion in Bitcoin to Criminals in 2019, Ηλεκτρονικός ιστότοπος: <https://www.crowdfundinsider.com/2020/01/156404-chainalysis-binance-huobi-other-major-exchanges-used-to-transfer-2-8-billion-in-bitcoin-to-criminals-in-2019/>

Federal Bureau of Investigation. (2017). AlphaBay Takedown

Greenberg A. (2013), At Least Two Moderators Of 'Silk Road 2.0' Drug Site Forums Arrested, ηλεκτρονικός ιστότοπος: <https://www.forbes.com/sites/andygreenberg/2013/12/20/at-least-two-moderators-of-the-silk-road-2-0-drug-site-forums-arrested/?sh=35c943937c9a>

Groendahl, B. (2018). Austrian Bitcoin 'Scam' Triggers Police Search Across Europe - Bloomberg.

Haig S. (2020), Interpol Enlists Korean Startup to Track Crypto on the Dark Web, ηλεκτρονικός ιστότοπος: <https://cointelegraph.com/news/interpol-enlists-korean-startup-to-track-crypto-on-the-dark-web>

Harper C. (2020), Bitcoin Dark Web Activity Up 340% Since 2017: Report, ηλεκτρονικός ιστότοπος: <https://www.forbes.com/sites/colinharper/2020/05/19/bitcoin-dark-web-activity-up-340-since-2017-report/?sh=637e80cd1418>

Higgins S. (2014), Day of Reckoning for Dark Markets as Hundreds of Domains Seized, ηλεκτρονικός ιστότοπος: <https://www.coindesk.com/day-reckoning-dark-markets-hundreds-illicit-domains>

Higgins, S. (2014, July 7). ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide

Higgins, S. (2017). From \$900 to \$20,000: Bitcoin's Historic 2017 Price Run Revisited.

Houghton B. (2009), New Limewire Darknet Client Broadens Front In Pointless P2P Battle, ηλεκτρονικός ιστότοπος: <https://www.hypebot.com/hypebot/2009/03/new-darknet-client-broadens-front-in-pointless-p2p-battle.html>

Howell, S. T., Niessner, M., & Yermack, D. (2018). Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales (No. w24774). National Bureau of Economic Research

Howmuch.net (2018), Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?, ηλεκτρονικός ιστότοπος: <https://howmuch.net/articles/crypto-transaction-speeds-compared>

IMF Staff Team. (2016). Virtual Currencies and Beyond: Initial Considerations. Staff Discussion Notes, 16(03), 1

Interpol.int (2021), Darknet and Cryptocurrencies, ηλεκτρονικός ιστότοπος: <https://www.interpol.int/en/How-we-work/Innovation/Darknet-and-Cryptocurrencies>

Johnson, S. (2018, January 16). Beyond the Bitcoin Bubble. The New York Times Magazine

Jong, M. de, & Dijk, M. van. (2015). Disrupting beliefs: A new approach to business-model innovation | McKinsey

Khatri, Y. (2018). FBI Arrests AriseBank CEO Over \$4 Million Crypto Fraud

Knight, K. B. and J. (2009, September 16). Lehman's Three Big Mistakes

Kumar A., Rosenbach E. (2021), imf.org, ηλεκτρονικός ιστότοπος: <https://www.imf.org/external/pubs/ft/fandd/2019/09/pdf/the-truth-about-the-dark-web-kumar.pdf>

Martineau, P. (2018). Inside the group chats where people pump and dump cryptocurrency

Nasdaq.com (2018), Study Suggests 25 Percent of Bitcoin Users Are Associated With Illegal Activity, ηλεκτρονικός ιστότοπος: <https://www.nasdaq.com/articles/study-suggests-25-percent-of-bitcoin-users-are-associated-with-illegal-activity-2018-01-22>

NPR Staff (2011), Silk Road: Not Your Father's Amazon.com, ηλεκτρονικός ιστότοπος: <https://text.npr.org/137138008>

Partnoy, F. (2013, September 16). Five Years After Lehman's Collapse, Bankers Still Haven't Confronted

Pepitone, Julianne (2014), FBI Arrests Alleged 'Silk Road 2.0' Operator Blake Benthall, ηλεκτρονικός ιστότοπος: <https://www.nbcnews.com/tech/security/fbi-arrests-alleged-silk-road-2-0-operator-blake-benthall-n242751>

Perez E. (2020), On the Darknet Side: The Role of Crypto as a Means of Exchange, ηλεκτρονικός ιστότοπος: <https://cointelegraph.com/news/on-the-darknet-side-the-role-of-crypto-as-a-means-of-exchange>

PwC. (2018). Cryptocurrency-bitcoin-accounting

Reddit.com (XXXX), DarkNetMarkets, ηλεκτρονικός ιστότοπος: [https://www.reddit.com/r/DarkNetMarkets/comments/6rsjkg/silk\\_road\\_31\\_got\\_hacked\\_owner\\_claims\\_bankruptcy/](https://www.reddit.com/r/DarkNetMarkets/comments/6rsjkg/silk_road_31_got_hacked_owner_claims_bankruptcy/)

Rizzo P. (2014), Silk Road 2.0 Seized, Alleged Operator Unmasked in FBI Crackdown, ηλεκτρονικός ιστότοπος: <https://www.coindesk.com/silk-road-2-0-seized-alleged-admins-unmasked-fbi-crackdown>

Roberts J. (2018), Litecoin Is Now a Surprise Favorite of Criminals Tired of Bitcoin, ηλεκτρονικός ιστότοπος: <https://fortune.com/2018/02/08/litecoin-monero-cryptocurrency-bitcoin/>

Rocic (2013), Penetrating the Darknet: Silk Road, Bitcoins, and the Onion Router, ηλεκτρονικός ιστότοπος: [https://www.vanderbilt.edu/olli/class-materials/Penetrating\\_the\\_Darknet.pdf](https://www.vanderbilt.edu/olli/class-materials/Penetrating_the_Darknet.pdf)

Sharma R. (2019), Litecoin Gains Ground On Bitcoin In The Dark Web, ηλεκτρονικός ιστότοπος: <https://www.investopedia.com/news/litecoin-gains-ground-bitcoin-dark-web/>

Shevchenko A. (2020), Russian Central Bank Links Crypto Transactions With Money Laundering, ηλεκτρονικός ιστότοπος: <https://cointelegraph.com/news/russian-central-bank-links-crypto-transactions-with-money-laundering>

Silfversten E., Favaro M., Slapakova L., etc (2020), Exploring the use of Zcash cryptocurrency for illicit or criminal purposes, ηλεκτρονικός ιστότοπος: [https://www.rand.org/pubs/research\\_reports/RR4418.html](https://www.rand.org/pubs/research_reports/RR4418.html)

Silkroadrugs.org, (2014), Silk Road 3.0, ηλεκτρονικός ιστότοπος: <https://silkroadrugs.org/tag/silk-road-3-0/>

Silkroadrugs.org, (2014), Silk Road, ηλεκτρονικός ιστότοπος: <https://silkroadrugs.org/silk-road-url/>

Spaven E. (2013), Silk Road shut down and 'owner' Ross William Ulbricht arrested, ηλεκτρονικός ιστότοπος: <https://www.coindesk.com/silk-road-allegedly-shut-owner-ross-william-ulbricht-arrested>

Stock J. (2020), Partnerships are our best weapon in the fight against cybercrime. Here's why, ηλεκτρονικός ιστότοπος:



<https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/>

Suberg, W. (2018). Vietnam: Pincoin, Ifan ICOs Exposed As Scams That Allegedly Stole \$660 Million

Tabarrok, A., & Cowen, T. (2015, April 6). The End of Asymmetric Information.

Tapscott, D., & Tapscott, A. (2016, May 10). The Impact of the Blockchain Goes Beyond Financial Services

The Economist. (2018, April 26). Crypto money-laundering

The Law Library of Congress. (2018, June). Regulation of Cryptocurrency Around the World

Thebalance.com (XXXX), What is the dark net, ηλεκτρονικός ιστότοπος:  
<https://www.thebalance.com/what-is-a-dark-market-391289>

Trendmicro.com (2016), Dark Web Marketplace Silk Road 3.0 Launched... Again, ηλεκτρονικός ιστότοπος:  
<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/dark-web-marketplace-silk-road-3-0-launched-again>

US Confiscates Millions in Cryptocurrencies in Alphabay Forfeiture Case. (2018)

Warner B. (2021), Please Don't Tell Ross Ulbricht What His 144,000 Bitcoin Are Worth Today..., ηλεκτρονικός ιστότοπος:  
<https://www.celebritynetworth.com/articles/entertainment-articles/ross-ulbricht-silk-road-bitcoin/>

Wikipedia. (2019). Silk Road (marketplace)

Wikipedia.org (2021), Silk Road (marketplace), ηλεκτρονικός ιστότοπος:  
[https://en.wikipedia.org/wiki/Silk\\_Road\\_\(marketplace\)#Silk\\_Road\\_2.0%20https://darknetmarkets.co/silk-road-3/](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)#Silk_Road_2.0%20https://darknetmarkets.co/silk-road-3/)

Williams-Grut, O. (2018, January 31). Startups raised \$5.6 billion through ICOs in 2017 - Business Insider

World Bank Group. (2017). Distributed Ledger Technology (DLT) and Blockchain (FinTech Note, No. 1).

Τσακούμης Α. (2013), Silk Road τέλος: Επίδραση στο Bitcoin, ηλεκτρονικός ιστότοπος: <https://bitcoinx.gr/silk-road-%CF%84%CE%AD%CE%BB%CE%BF%CF%82-%CE%B5%CF%80%CE%AF%CE%B4%CF%81%CE%B1%CF%83%CE%B7-%CF%83%CF%84%CE%BF-bitcoin/>