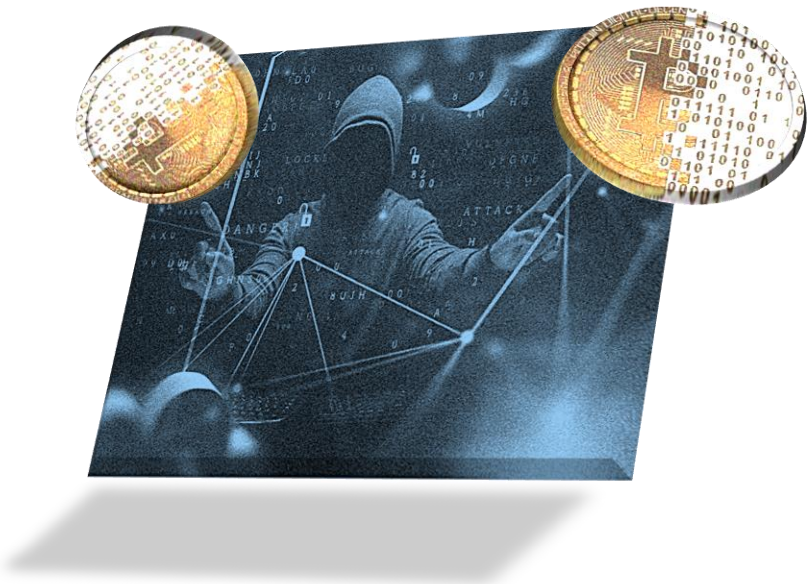
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ BITCOIN ΚΑΙ ΟΙ ΕΓΚΛΗΜΑΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ ΠΟΥ ΑΠΟΡΡΕΟΥΝ ΑΠΟ ΤΗΝ ΧΡΗΣΗ ΤΟΥ



Διπλωματική Εργασία
της

Ευγενίας – Υβόννης Τσελώνη
(Α.Μ. 17040)

ΘΕΣΣΑΛΟΝΙΚΗ, ΙΟΥΝΙΟΣ 2021

ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ BITCOIN
ΚΑΙ ΟΙ ΕΓΚΛΗΜΑΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ
ΠΟΥ ΑΠΟΡΡΕΟΥΝ ΑΠΟ ΤΗΝ ΧΡΗΣΗ ΤΟΥ

Ευγενία – Υβόννη Τσελώνη

Πτυχίο Νομικής Σχολής
Εθνικού Καποδιστριακού Πανεπιστημίου Αθηνών

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες Καθηγητές

Θεοχάρης Δαλακούρας – Εμμανουήλ Στειακάκης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ηη/μμ/εεεε

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
.....	.....	.....

Ευγενία – Υβόννη Τσελώνη

ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ BITCOIN
ΚΑΙ ΟΙ ΕΓΚΛΗΜΑΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ
ΠΟΥ ΑΠΟΡΡΕΟΥΝ ΑΠΟ ΤΗΝ ΧΡΗΣΗ ΤΟΥ

Αφιερώνεται στη μαμά μου

ΕΥΓΕΝΙΑ ΥΒΟΝΝΗ ΤΣΕΛΩΝΗ

Ευχαριστίες

Με την ολοκλήρωση της παρούσας Διπλωματικής εργασίας, κλείνει ο κύκλος σπουδών μου στο Διατμηματικό Μεταπτυχιακό Πρόγραμμα «Δίκαιο και Πληροφορική». Το συγκεκριμένο θέμα εργασίας συνδυάζει προκλήσεις και γνώσεις που αναδύονται από την συνάντηση των δύο επιστημών.

Θα ήθελα να ευχαριστήσω θερμά τους καθηγητές μου Θεοχάρη Δαλακούρα και Εμμανουήλ Στειακάκη που με εμπιστεύθηκαν για την εργασία αυτή. Η υποστήριξη και η πολύτιμη καθοδήγησή τους καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής εργασίας υπήρξε καταλυτική.

Ακόμη, ευχαριστώ θερμά την κυρία Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου για την εξαιρετική πρωτοβουλία δημιουργίας του πρωτοπόρου μεταπτυχιακού προγράμματος, του οποίου είχα την τύχη και τιμή να είμαι φοιτήτρια, στον πρώτο κύκλο που λειτούργησε.

Τέλος, ευχαριστώ θερμά τη μητέρα μου Ιωάννα Αρχοντή, που με παραστέκει σε κάθε μου βήμα, ακλόνητος αρωγός.

Περίληψη

Τα κρυπτονομίσματα είναι μια μορφή ψηφιακού χρήματος, το οποίο εισήγαγε ένα εντελώς ριζοσπαστικό σύστημα οικονομικών σχέσεων. Στο εξής, η ανταλλαγή των χρημάτων πραγματοποιείται χωρίς να εμπλέκεται κάποιος ενδιάμεσος· την ίδια στιγμή, η ασφάλεια και η αξιοπιστία των συναλλαγών διασφαλίζονται από ένα κατανεμημένο καθολικό, απαρτιζόμενο από ένα δίκτυο υπολογιστών, οι οποίοι δια της κρυπτογραφίας ελέγχουν και καταγράφουν αξιόπιστα τις πραγματοποιούμενες συναλλαγές. Ως εκ τούτου, το Bitcoin αποτελεί εργαλείο ή στόχο των κυβερνοεγκληματιών και η εμπλοκή του στο χώρο του κυβερνοεγκλήματος είναι ανησυχητική. Μέσα στο νέο αυτό κλίμα, μία πράξη ρηξικέλευθος για τη νομοθετική προσέγγιση των κρυπτονομισμάτων είναι η υπαγωγή τους στην Οδηγία για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας.

Λέξεις Κλειδιά: χρήμα, κρυπτονομίσματα, πορτοφόλι, ασύμμετρη κρυπτογραφία, ιδιωτικό κλειδί, δημόσιο κλειδί, έξοδος αξόδευτης συναλλαγής, ομότιμο δίκτυο, κατακερματισμός, μπλοκ, κόμβοι, εξόρυξη, αλγόριθμος απόδειξης εργασίας, ανταλλακτήρια, Οδηγία AML5, ξέπλυμα χρήματος, σκοτεινό δίκτυο, λυτρισμικό, ψάρεμα, εισβολή, cryptojacking, Blockchain, bitcoin, Vinnik, Mt.Gox, Silk Road.

Abstract

Cryptocurrencies are a form of digital money, which have introduced a completely radical system of economic relations. Henceforth, the exchange of money takes place without involving any intermediary; concurrently, the security and reliability of the transactions are ensured by a distributed ledger system, consisting of a network of computers, which through cryptography reliably control and record the transactions made. Consequently, the Bitcoin has become the tool or target of cybercriminals and its involvement in the field of cybercrime is alarming. In this new era, a groundbreaking legislative approach to cryptocurrencies is their inclusion in the Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

Keywords: money, cryptocurrency, wallet, asymmetric encryption, private key, public key, UTXO, peer-to-peer, hash, block, nodes, mining, proof of work algorithm, exchange, Directive AML5, anti-money laundering, dark web, ransomware, phishing, hacking, cryptojacking, Blockchain, bitcoin, Vinnik, Mt.Gox, Silk Road.

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

Ελληνικές	
ΑΚ	Αστικός Κώδικας
ΑΠ	Άρειος Πάγος
Αρ.	Άρθρο
Βλ.	Βλέπε
Ε.Ε.	Ευρωπαϊκή Ένωση
Ε.Κ.	Ευρωπαϊκές Κοινότητες
ΕΚΤ	Ευρωπαϊκή Κεντρική Τράπεζα
Επ.	Επόμενα
μτφρ	μετάφραση
Ν.	Νόμος
παρ.	παράγραφος
ΠΚ	Ποινικός Κώδικας
ΣΤΕ	Συμβούλιο Της Επικρατείας
Φ.Π.Α.	Φόρος Προστιθέμενης Αξίας
σελ.	σελίδα
στ.	στοιχείο
Ξένες	
AML	Anti-money Laundering
BATM	Bitcoin Automated Teller Machine
BTC	Bitcoin
CTF	Combating The Financing of Terrorism
CWPs	Custodian Wallet Providers
DDoS attack	Distributed Denial of Service attack
EBA	EBA
ECB	European Central Bank
FAFT	Financial Action Task Force

FBI	Federal Bureau of Investigation
ICO	Inicial Coin Offering
ISIS	Islamic State of Iraq and Syria
KYC	Know Your Customer
LR	Liberty Reserve
Multisig	Multiple signatures
PoW	Proof of Work
P2P	Peer-to-Peer
P2Pool	Peer-to-Pool
SHA	Secure Hash Algorithm
SPV	Simplified Payment Verification
UTXO	Unspent Transaction Output
VCEPs	Virtual Currency Exchange Platforms

Π Ε Ρ Ι Ε Χ Ο Μ Ε Ν Α

ΣΕΛ

Ε Ι Κ Ο Ν Ε Σ

Εισαγωγή

Τα τελευταία χρόνια υπάρχουν στην αγορά αρκετά πρωτοποριακά συστήματα πληρωμών, που τυγχάνει να λειτουργούν αποκλειστικά μέσω κινητών τηλεφώνων και διαδικτύου. Τα εναλλακτικά αυτά συστήματα έχουν ως βάση το παραστατικό χρήμα και είναι το Apple Pay, το PayPal, το Transferwise. Την τελευταία δεκαετία παρατηρείται αύξηση της χρήσης μιας νέας μορφής συστήματος πληρωμών, που χρησιμοποιεί ψηφιακά νομίσματα. Τα νομίσματα αυτά μεταφέρουν αξία από τον αποστολέα στον παραλήπτη, δεν υπάρχουν σε φυσική μορφή και διευκολύνουν ώστε οι συναλλαγές να γίνουν πιο γρήγορες, πιο ευέλικτες, πιο ασφαλείς προσφέροντας πληρωμές καινοτόμες και αποκτώντας χαρακτήρα διασυνοριακό.

Το πρώτο ψηφιακό νόμισμα που δημιουργήθηκε είναι το Bitcoin. Από την αρχή της εμφάνισής του, οι άνθρωποι προσπάθησαν να κατανοήσουν τη λειτουργία του και να το εντάξουν σε κάποια νομοθεσία από τις ήδη υπάρχουσες. Υποστηρίχθηκε λοιπόν ότι το Bitcoin είναι χρήμα, όμοιο με το παραστατικό ή ακόμη ότι είναι υποκατάστατο χρήματος, ή ηλεκτρονικό χρήμα ή οικονομικό εργαλείο ή εμπόρευμα ή περιουσιακό αγαθό. Η κρατούσα γνώμη υποστηρίζει ότι το Bitcoin είναι χρήμα, υπό ευρεία έννοια, το οποίο υπάρχει μόνο στο διαδίκτυο. Η πρώτη συναλλαγή με Bitcoin έγινε από τον Laszlo Hanyecz, ο οποίος αγόρασε δύο πίτσες για 10000 bitcoins, ποσό που εκείνη την εποχή ισοδυναμούσε με 0,008$.

Το όνομα «Bitcoin» προέρχεται από την σύνθεση των λέξεων «bit» και «coin». Η λέξη «bit» με την σειρά της προέρχεται από τη σύμμειξη των λέξεων binary (= δυαδικό) και «digit» (=ψηφίο), γνωστοί όροι της πληροφορικής και τηλεπικοινωνιών. «Coin» σημαίνει νόμισμα. Κατά κυριολεξία λοιπόν η λέξη Bitcoin μεταφράζεται ως «δυφιονόμισμα[1]». Η ονομασία «Bitcoin» έχει διττό περιεχόμενο, καθώς αφενός αναφέρεται στο όνομα του πρωτοκόλλου και του δικτύου, έννοια που περιλαμβάνει μία συλλογή εννοιών και τεχνολογιών, οι οποίες σχηματίζουν τα θεμέλια του οικοσυστήματος των ψηφιακών νομισμάτων και αφετέρου αναφέρεται στη μονάδα του νομίσματος που υποστηρίζεται από το δίκτυο αυτό. Το Bitcoin αποτελεί ένωση τεσσάρων καινοτομιών, δηλαδή ενός αποκεντρωμένου δικτύου Peer-to-Peer, το οποίο αξιοποιεί τη μέθοδο της κρυπτογραφίας,

[1] Το δυφίο λαμβάνει μόνο δύο τιμές, οι οποίες αναπαριστώνται με τα ψηφία 0 και 1.

ενός αμετάβλητου δημόσιου αρχείου συναλλαγών, του Blockchain, μιας ιδιόμορφης διαδικασίας δημιουργίας νέων ψηφιακών νομισμάτων και, τέλος, ενός αποκεντρωμένου συστήματος επαλήθευσης συναλλαγών μέσω ενός μηχανισμού συναίνεσης, βασισμένου στην απόδειξη εργασίας. Τα ψηφιακά νομίσματα μπορούν να αποκτηθούν με πρωτογενή ή με παράγωγο τρόπο ανάλογα με το αν οι χρήστες δημιουργούν οι ίδιοι τα Bitcoin ή αν χρησιμοποιούν συμβατικά είδη χρημάτων για να αγοράζουν Bitcoin σε τιμή ισοτιμίας[2].

Το Bitcoin προσείλκυσε πάραυτα την προσοχή των κυβερνοεγκληματιών, λόγω της ανωνυμίας και δυσκολίας εντοπισμού που παρέχει στις συναλλαγές. Παρατηρήθηκε λοιπόν μεταστροφή στη συμπεριφορά τους, αφού οι πληρωμές έπαψαν να γίνονται μέσω PayPal ή Western Union και εκτελούνται αποκλειστικά με κρυπτονομίσματα. Συνάμα, οι κυβερνοεγκληματίες εμπιστεύτηκαν το Bitcoin ως το νέο μέσον που θα αποτελέσει σύμμαχο στην εγκληματική τους δράση και ως το νέο στόχο που θα τους αποφέρει τεράστια κέρδη.

Επακόλουθο της συμπεριφοράς των εγκληματιών του κυβερνοχώρου είναι η αύξηση των εγκληματικών ενεργειών τους. Το γεγονός αυτό θορύβησε την Ευρωπαϊκή Ένωση και την οδήγησε στο να αρχίσει να λαμβάνει μέτρα για τη νέα τεχνολογία, η οποία με τις ιδιομορφίες της δημιουργεί μεγάλους προβληματισμούς και δυσκολίες στην αντιμετώπισή της. Πριν τη καθολική νομοθετική οριοθέτηση των κρυπτονομισμάτων, κρίθηκε αναγκαίο να ληφθούν κάποιες ρυθμίσεις σε ειδικά νομοθετήματα, προκειμένου να ανακοπεί εν μέρει η ανεξέλεγκτη δράση τους. Και η πρώτη προσπάθεια της ΕΕ πραγματώθηκε με την υπαγωγή των κρυπτονομισμάτων Οδηγία για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και για τη χρηματοδότηση της τρομοκρατίας.

Το εξεταζόμενο θέμα έχει πολλαπλές εκφάνσεις και θα πρέπει να τεθούν ορισμένα όρια ως προς τη μελέτη αυτών. Στην παρούσα εργασία λοιπόν, εξετάζεται η υπαγωγή του Bitcoin στην έννοια του χρήματος και μόνον, καθώς ο πρωταρχικός σκοπός της εμφάνισής του είναι να αποτελεί εναλλακτικό μέσον πληρωμών. Επίσης, αναλύονται και αξιολογούνται

[2] Βλ. Αρχοντάκη, Α., Simsive, Ρ., 2014. Οι νέες μορφές του ψηφιακού χρήματος στην Ελλάδα: Η περίπτωση του Bitcoin. *Εφαρμογές Αστικού Δικαίου & Αστικού Δικονομικού Δικαίου,* 7(10-11), σελ. 835, Μεταξάκης, Ε., 2017. *Μπίτκοϊν (bitcoin), κρυπτοχρήμα και κυβερνοέγκλημα.* Αθήνα: Α. Σάκκουλας, σελ. 47, Παπαδοπούλου, Α., 2018. Blockchain: Η τεχνολογία που υπόσχεται «ψηφιακή ασφάλεια»: πιθανές εφαρμογές και συνέπειες για το δίκαιο πνευματικής ιδιοκτησίας και ιδίως στο ζήτημα της ψηφιακής ανάλωσης. *Επισκόπηση Εμπορικού Δικαίου*, 24(2), σελ. 211, Χρυσοχού, Χ., 2018. *Πιστωτικά Ιδρύματα: Νομικές & Θεσμικές Όψεις.* Πρακτικά Συνεδρίου από το 7ο Πανελλήνιο Συνέδριο e-ΘΕΜΙΣ που διεξήχθη στη Θεσσαλονίκη 25-26 Μαρτίου 2016. Φορέας διεξαγωγής: Ένωση Ελλήνων Νομικών. Αθήνα: Νομική Βιβλιοθήκη, σελ. 266, *Antonopoulos, A.*, 2015. Mastering Bitcoin: Unlocking Digital Crypto-Currencies. Sebastopol, California: O'Reilly, σελ. 1.

μόνον οι νεοπαγείς διατάξεις που αναφέρονται συγκεκριμένα στα κρυπτονομίσματα και όχι οι διατάξεις που εφαρμόζονται μεν για την αντιμετώπιση κυβερνοεγκλημάτων σχετικών με κρυπτονομίσματα, προϋπήρχαν δε στον Ποινικό Κώδικα ρυθμίζοντας εργαλεία και τεχνικές που χρησιμοποιούνται γενικά στον κυβερνοχώρο.

Στο **πρώτο κεφάλαιο** γίνεται προσέγγιση της έννοιας των κρυπτονομισμάτων από τη σκοπιά της οικονομικής θεωρίας περί χρήματος. Αναλύεται η ιστορία του χρήματος και μελετώνται οι ιδιότητες και τα χαρακτηριστικά του, προκειμένου να διαπιστωθεί εν συνεχεία εάν τα κρυπτονομίσματα πληρούν τις λειτουργίες του χρήματος και επομένως εάν υπάγονται σε αυτό.

Στα δύο επόμενα κεφάλαια αποπειράται, πολύπλοκες έννοιες που συναντώνται κατά τη διάρκεια της, εις βάθος, μελέτης του Bitcoin να αποσαφηνιστούν και να παρουσιαστούν με θεωρητικό και εύληπτο τρόπο. Έτσι λοιπόν:

Στο **δεύτερο κεφάλαιο** αναλύεται ο κύκλος της ζωής μιας συναλλαγής με bitcoin, από τη στιγμή της δημιουργίας του στο πορτοφόλι ενός χρήστη μέχρι τη στιγμή που θα περιέλθει στο πορτοφόλι ενός άλλου. Ιδίως μελετάται ο ρόλος της ασύμμετρης κρυπτογραφίας, της ψηφιακής υπογραφής και του δικτύου Peer-to-Peer.

Στο **τρίτο κεφάλαιο** αναλύεται το Blockchain. Προσεγγίζεται η έννοια του μπλοκ και του περιεχομένου του, αναλύονται τα στάδια που απαρτίζουν τη διαδικασία της εξόρυξης Bitcoin, εξηγείται η συμβολή του αλγόριθμου απόδειξης εργασίας και επισημαίνονται τυχόν επιθέσεις που μπορεί να δημιουργήσουν πρόβλημα στην ομαλή λειτουργία της διαδικασίας των συναλλαγών.

Στο **τέταρτο κεφάλαιο** εξετάζεται η διττή σχέση του Bitcoin με το κυβερνοέγκλημα. Αναλύονται οι περιπτώσεις του Bitcoin ως εργαλείο, δίνοντας ιδιαίτερη έμφαση στο ρόλο που διαδραματίζει στο Dark Web, καθώς και οι περιπτώσεις του Bitcoin ως δέλεαρ για την διάπραξη των κυβερνοεγκλημάτων.

Στο **πέμπτο κεφάλαιο** αναφέρονται οι πρώτες νομοθετικές προβλέψεις που λήφθηκαν και στις οποίες υπάγονται ρητώς τα κρυπτονομίσματα. Γίνεται η ανάλυση και αξιολόγηση της Οδηγίας 843/2018, η οποία τροποποιεί την Οδηγία 849/2015 σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας.

Στο **έκτο κεφάλαιο** αναφέρονται έξι νομολογιακές αποφάσεις, στις οποίες το Bitcoin συνδέθηκε με εγκληματικές ενέργειες και οι οποίες αποτέλεσαν σταθμό, η καθεμία για διαφορετικό λόγο.

Στο **έβδομο κεφάλαιο** γίνεται μια συνολική αξιολόγηση του Bitcoin και αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματα που έχει η νέα τεχνολογία και η χρήση της.

Α΄ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 1ο
ΤΟ BITCOIN ΚΑΙ Η ΣΧΕΣΗ ΤΟΥ ΜΕ ΤΟ ΧΡΗΜΑ

Το χρήμα είναι έννοια αφηρημένη και αποτελεί μια επινόηση του ανθρώπου προκειμένου να μπορεί να ανταλλάσσει οικονομικά αγαθά πιο εύκολα. Η θεσμική παρεμβολή που έχει το κράτος δεν πρέπει να συγχέεται με την ίδια την ουσία του χρήματος και με το χρηματικό φαινόμενο, το οποίο αναπτύχθηκε ιστορικά πριν και ανεξάρτητα από οποιαδήποτε κρατική παρέμβαση. Δεν δημιουργήθηκε από τους κανόνες δικαίου αλλά προϋπάρχει αυτών. Γι' αυτό δεν πρέπει να συγχέεται με τους κανόνες δικαίου που το ρυθμίζουν, καθώς δεν αποτελεί δημιούργημα της έννομης τάξης αλλά εισέρχεται σε αυτήν, όταν μια οργανωμένη σε κράτος κοινωνία αποφασίζει να το συμπεριλάβει στο ρυθμιστικό της πεδίο. Αναπτύχθηκε, ώστε να εξυπηρετεί τις συναλλακτικές ανάγκες, μέσα δε στους αιώνες εξελίχθηκε και μετασχηματίσθηκε, προκειμένου αφενός να προσαρμοστεί στις εκάστοτε οικονομικές και τεχνολογικές εξελίξεις και αφετέρου να διευκολύνει τις οικονομικές συναλλαγές, καθιστώντας αυτές ακόμα πιο αποτελεσματικές. Το χρήμα λοιπόν έχει αλλάξει πολλές μορφές και σταδιακά έγινε πιο αφηρημένο, εικονικό και ψηφιακό. Στη σημερινή εποχή νόμισμα μπορεί να αποτελέσει οποιοδήποτε αντικείμενο το οποίο θα είναι πολύ σημαντικό για την κοινωνία, τη συγκεκριμένη περίοδο. Αυτό συνέβη για παράδειγμα στην Ουκρανία, όταν μετά την πτώση της Σοβιετικής Ένωσης, ως επίσημο χρήμα κηρύχθηκε το δελτίο διανομής τροφίμων λόγω της πολύ μεγάλης αξίας που απέκτησε[3].

[3] Βλ. Καλαμίτσης, Σ., 1995. *Ξένο νόμισμα [συνάλλαγμα] και [ελληνικό] δίκαιο*. Αθήνα: Αφοί Π. Σάκκουλα, σελ. 45-46, Παπαρσενίου, Π., 2020. *Χρηματική ενοχή: ιδίως σε ξένο νόμισμα*. Αθήνα: Π. Σάκκουλας, σελ. 15,38,51, Μαλλέρου, Α., 2007. *Το δίκαιο του ηλεκτρονικού χρήματος*. Αθήνα: Νομική Βιβλιοθήκη, σελ. 89-90, 98, 112-113, Gajdek, S., Kozak, S., 2019. Bitcoin as an Electronic Payment Tool. *Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Seria: Administracja i Zarządzanie* [online]. Vol 47(120). August, σελ. 5: Available at: https://www.researchgate.net/publication/338627957_Bitcoin_as_an_Electronic_Payment_Tool (Accessed 27/02/2021), Surowiecki J., 2012. *A brief history of money*, ό.π., σελ. 46: Available at: https://www.researchgate.net/publication/254059731_A_brief_history_of_money (Accessed 10/02/2021).

1.1. Μορφές χρήματος

1.1.1. Το χρήμα στην αρχαιότητα

Στις φυλετικές και πρωτόγονες οικονομίες τα χρήματα χρησιμοποιούνταν για τον προσδιορισμό της δομής των κοινωνικών σχέσεων, επιτελώντας έναν πολύ διαφορετικό ρόλο. Ο κάτοχος χρημάτων είχε την απόλυτη εξουσία μέσα στην κοινωνία, ώστε να κανονίζει γάμους, να ξεκινά βεντέτες, να παρέχει συγχώρεση σε περιπτώσεις εγκλημάτων, να διαπραγματεύεται συνθήκες, να έχει ακολούθους κ.ο.κ.[4].

Στη συνέχεια, ως χρήμα λογίζονταν τα προϊόντα δηλαδή οι ανταλλαγές σε είδος. Οι άνθρωποι, προκειμένου να αποκτήσουν αγαθά και υπηρεσίες που χρειάζονταν, αντάλλασσαν προϊόντα με ιδιαίτερη συναλλακτική αξία, όπως κοσμήματα, γεωργικά προϊόντα, όστρακα ή ακόμη δέρματα ζώων, οικόσιτα ζώα, ευγενή μέταλλα και πολύτιμους λίθους, με αυτά τα αγαθά που ήθελαν να αποκτήσουν. Ο αντιπραγματισμός, όπως ονομαζόταν, σιγά σιγά καθιστούσε τις συναλλαγές δυσκίνητες καθώς προϋπέθετε την απόλυτη σύμπτωση επιθυμιών σε είδος και σε ποσότητα προϊόντων και υπηρεσιών. Επιπλέον, με την αύξηση του όγκου των συναλλαγών και των συναλλασσόμενων, η εύρεση ενός αντισυμβαλλόμενου άρχισε να γίνεται όλο και πιο δύσκολη, καθώς οι ανάγκες της συναλλακτικής πραγματικότητας δεν μπορούσαν πλέον να καλυφθούν με τα μέσα που ήδη υπήρχαν. Έτσι, η εμφάνιση ενός κοινού ανταλλακτικού μέσου κατέστη επιτακτική και αναγκαία[5].

Το τέλος της εποχής του εμπορευματικού χρήματος και η παράλληλη εμφάνιση της κρατικής επιρροής στο χρήμα σηματοδοτούνται με την εμφάνιση των μεταλλικών νομισμάτων στις συναλλαγές. Το χρήμα δεν είναι πλέον ένα εμπόρευμα, αλλά ένα μέσον για την ανταλλαγή εμπορευμάτων. Επικρατεί το δίπτυχο είδος-χρήμα, με το χρήμα να αποτελεί την αντιπαροχή για απόκτηση ή για διάθεση ενός αγαθού ή μιας υπηρεσίας. Η αξία των χρημάτων αυτών βασιζόταν στο υλικό από το οποίο ήταν φτιαγμένα και για το λόγο αυτό καθιερώνονται ως μέσο ανταλλαγής, μέτρο και φορέας αξίας[6].

Τα προβλήματα που παρουσιάστηκαν με αυτή τη μορφή χρήματος ήταν κυρίως δύο. Αφενός η δυσκολία μεταφοράς των νομισμάτων όταν τα χρηματικά ποσά ήταν μεγάλα,

[4] Βλ. Surowiecki J., ό.π., σελ. 46, Βλ. Βλ. *Καλαμίτσης, Σ.,* ό.π., σελ. 45-46.
[5] Βλ., *Μαλλέρου, Α.*, ό.π., σελ. 112-113, *Μεταξάκης, Ε.*, ό.π., σελ. 23-24, *Παπαρσενίου, Π.*, ό.π., σελ. 23, 40-41.
[6] Βλ. *Παπαρσενίου, Π.*, ό.π., σελ. 24, Σταθόπουλος, Μ., 2004. Επιτομή Γενικού Ενοχικού Δικαίου, 4η έκδ. Αθήνα: Εκδόσεις Σάκκουλα, σελ. 222.

με αποτέλεσμα οι συναλλαγές να καθίστανται δυσχερείς και αφετέρου η εξάρτηση του μεταλλικού χρήματος από το μέταλλο κατασκευής τους[7]. Έτσι οδηγηθήκαμε στη μορφή χρήματος που γνωρίζουμε μέχρι σήμερα, τα τραπεζογραμμάτια και τα κέρματα.

1.1.2. Το χρήμα στη σύγχρονη εποχή

Τα πρώτα χαρτονομίσματα εκδόθηκαν από την Stockholm Banco το 1661. Στην αρχή τα χαρτονομίσματα είχαν αντίκρισμα σε συγκεκριμένη ποσότητα χρυσού. Ο κανόνας του χρυσού, όπως ονομάστηκε, ήταν ένα σύνολο κανόνων ή αρχών που έπρεπε να τηρούνται από όλες τις οι χώρες που είχαν δεσμευτεί να το ακολουθούν και αποσκοπούσε στην καθιέρωση ενός συστήματος σταθερών συναλλαγματικών ισοτιμιών. Τα νομίσματα των κρατών που συμμετείχαν στον κανόνα του χρυσού ήταν συνδεδεμένα μεταξύ τους με αναγωγή στα εκάστοτε αποθέματα χρυσού που διέθεταν. Για το λόγο αυτό, οι ισοτιμίες μεταξύ τους έπρεπε να ήταν σταθερές. Οι κανόνες του συστήματος έγκειτο στη μετατρεψιμότητα των τραπεζογραμματίων της κάθε χώρας σε χρυσό, στη δυνατότητα ελεύθερης εισαγωγής και εξαγωγής χρυσού ώστε διευκολύνεται η πραγματοποίηση διασυνοριακών συναλλαγών, στην υποχρεωτική διατήρηση από την Κεντρική Τράπεζα κάθε χώρας ενός σταθερού λόγου «διαθέσιμου χρυσού/νομισματική κυκλοφορία» και στην αυτόματη αποκατάσταση της ισορροπίας του ισοζυγίου πληρωμών μέσω των αυξομειώσεων στην εγχώρια προσφορά χρήματος, που θα έπρεπε να καλύπτεται από τις διαθέσιμες ποσότητες χρυσού της κάθε χώρας. Προβλήματα όμως οικονομικής ύφεσης και πολέμων οδήγησαν στην εγκατάλειψη του κανόνα του χρυσού[8].

Ακολούθησε η διάσκεψη Bretton Woods, το 1944, η οποία αποτέλεσε μια προσπάθεια της Παγκόσμιας Οικονομικής κοινότητας να επιστρέψει στον κανόνα του χρυσού. Το σύστημα που υιοθετήθηκε διέφερε από το κλασικό σύστημα του κανόνα του χρυσού των αρχών του 20ου αιώνα στο ότι μετατρεψιμότητα σε χρυσό διατηρούσε μόνο το αμερικάνικο δολάριο, το οποίο λειτουργούσε ως παρεμβατικό νόμισμα για τη διατήρηση των συναλλαγματικών ισοτιμιών. Οι υπόλοιπες χώρες καθόριζαν τις ισοτιμίες τους σε σχέση με τον χρυσό μόνο έμμεσα, καθώς υπολόγιζαν την σχέση εθνικού νομίσματος ανά ουγγιά χρυσού και όριζαν αντίστοιχα την ισοτιμία τους με το δολάριο. Οι ισοτιμίες λοιπόν των νομισμάτων των χωρών που συμμετείχαν ήταν σταθερές μεν σε σχέση με τον χρυσό, όμως

[7] Βλ. *Παπαρσενίου, Π.*, ό.π., σελ. 29, 32.
[8] *Ibid* σελ. 32.

τα νομίσματά τους δεν ήταν απ' ευθείας μετατρέψιμα σε χρυσό. Μόνο το δολάριο ήταν προσαρμοσμένο και μετατρέψιμο με σταθερή ισοτιμία με το χρυσό και έτσι αποτέλεσε τον κεντρικό άξονα του συστήματος. Το σύστημα αυτό εγκαταλείφθηκε το 1971, επειδή οι ΗΠΑ σταμάτησαν την μετατρεψιμότητα του δολαρίου σε χρυσό, ώστε τα φυσικά αποθέματα χρυσού που έχει ένα κράτος να μη συνδέονται με την αξία του χρήματος.

Έκτοτε υιοθετήθηκε το Παραστατικό χρήμα (fiat), το οποίο δεν έχει αντίκρισμα σε χρυσό, αλλά η αξία του είναι μόνο ανταλλακτική. Υπάρχει λοιπόν διαχωρισμός της αξίας που μεταβιβάζεται και του υλικού φορέα αυτής. Η αποσβεστική ισχύς επέρχεται λόγω της χρηματικής αξίας όπως αυτή παριστάνεται από τις νομισματικές μονάδες και όχι λόγω του μετάλλου των κερμάτων ή του χαρτιού των τραπεζογραμματίων, καθώς η αξία των υλικών αντικειμένων που ενσωματώνουν τα χρήματα είναι πολύ μικρότερη από την αξία των χρηματικών μονάδων που παριστάνουν[9].

Είναι αξιοσημείωτο ότι η πρώτη φορά που διατυπώθηκε η θεωρία για την ύπαρξη χρήματος χωρίς αντίκρισμα ήταν τον 13ο αιώνα στην Κίνα από τον Kublai Khan, πρωτοπόρο για την εποχή του, ο οποίος δεν επικεντρώθηκε στο πώς μοιάζουν τα χρήματα ή στο αν έχουν αντίκρισμα, αλλά στο εάν οι άνθρωποι επιδεικνύουν τέτοιου βαθμού πίστη ως προς αυτά, ώστε να τα χρησιμοποιήσουν. Η πεποίθηση αυτή αποτελεί σήμερα τον θεμέλιο λίθο όλων των νομισματικών συστημάτων, τα οποία επί της ουσίας βασίζονται αφενός στην στήριξη που τους παρέχουν οι κυβερνήσεις και αφετέρου στην πίστη των ανθρώπων[10].

Μια άλλη μορφή χρήματος, που εμφανίστηκε παράλληλα με το παραστατικό χρήμα, είναι το λεγόμενο Λογιστικό χρήμα. Το χρήμα, από μέσο ανταλλαγής στην φυσική εκδοχή του, μετασχηματίστηκε σε μέσο πίστωσης και εν συνεχεία σε μέσο πληρωμής, μέσω της απόσβεσης των χρεών δια λογιστικών εγγραφών. Στην πράξη, η σημερινή μορφή του χρήματος είναι ως επί το πλείστον η λογιστική, καθώς το χρήμα αποτελεί λογιστικές εγγραφές σε τραπεζικούς λογαριασμούς και δεν χρειάζεται να μετατραπεί σε τραπεζογραμμάτια, προκειμένου να αποτελέσει μέσο εκπλήρωσης υποχρεώσεων. Κυριότερα μορφώματα λογιστικού χρήματος είναι η επιταγή, η συναλλαγματική όψεως, η εντολή μεταφοράς χρηματικού ποσού από τον τραπεζικό λογαριασμό του οφειλέτη σε

[9] Βλ. *Λοΐζου*, ό.π., σελ. 2-3, *Μαλλέρου, Α.*, ό.π., σελ. 96-97, *Σταθόπουλος, Μ*, ό.π., σελ. 223, Surowiecki J., ό.π., σελ. 46, βλ. Σύστημα σταθερών ισοτιμιών του Μπρέττον Γουντς. *Ο κανόνας του χρυσού.* Ανακτήθηκε από: https://bit.ly/3bOz7uJ (Πρόσβαση 01/03/2021).

[10] Βλ.Surowiecki J., ό.π., σελ. 45

εκείνον του δανειστή, καθώς και τα πιστωτικά δελτία (κάρτες ή πλαστικό χρήμα), τα οποία αποτελούν και την πιο διαδεδομένη μορφή λογιστικού χρήματος. Υπό την ευρεία έννοια του όρου, το λογιστικό θεωρείται χρήμα διότι προσδιορίζεται ως τέτοιο από τις κρατούσες συναλλακτικές συνήθειες[11].

Μια ακόμη μορφή χρήματος αποτελεί το λεγόμενο Ηλεκτρονικό χρήμα, το οποίο είναι ένα μέσο αποϋλοποίησης και ηλεκτρονικής αποθήκευσης, του νόμιμου χρήματος. Δεν αποτελεί αυτό καθ' εαυτό μέσον συναλλαγών, καθώς τα συναλλασσόμενα με ηλεκτρονικό χρήμα μέρη εξακολουθούν να χρησιμοποιούν ως μέσο ανταλλαγής την ενσωματωμένη στο ηλεκτρονικό απόθεμα νομισματική αξία, δηλαδή το νόμιμο χρήμα[12]. Σύμφωνα με το άρθρο 2 περίπτωση 2 της Οδηγίας 2009/110/ΕΚ για το ηλεκτρονικό χρήμα[13], όπως ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν.4021/2011[14], ως «ηλεκτρονικό χρήμα νοείται οιαδήποτε αποθηκευμένη σε ηλεκτρονικό, μεταξύ άλλων και μαγνητικό υπόθεμα, νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για τον σκοπό της πραγματοποίησης πράξεων πληρωμών, όπως ορίζονται στο άρθρο 4 σημείο 5 της οδηγίας 2007/64/ΕΚ και η οποία γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη». Το ηλεκτρονικό χρήμα λοιπόν είτε περιέχεται σε κάποια συσκευή πληρωμής που ανήκει στον κάτοχο του ηλεκτρονικού χρήματος, είτε είναι αποθηκευμένο σε κάποιον απομακρυσμένο διακομιστή και το διαχειρίζεται ο κάτοχος του ηλεκτρονικού χρήματος μέσω ειδικού λογαριασμού για ηλεκτρονικό χρήμα[15].

---

[11] Βλ. Καλλιμόπουλος, Γ., 1993. *Το δίκαιο του χρήματος*. Αθήνα-Κομοτηνή: Α. Σάκκουλας, σελ. 44, 47, *Παπαρσενίου, Π.*, ό.π., σελ. 33, 36.

[12] Βλ. Καζαζάκης, Θ., 2015. "Bitcoin": Νομική θεώρηση ενός αρρύθμιστου ψηφιακού νομίσματος. *Ελληνική Δικαιοσύνη.* 4/2015, σελ. 4, Παρασκευόπουλος-Κόλιας, Χ., 2015. *Κρυπτονομίσματα (digital-currencies) υπό το φως του εποπτικού δικαίου της χρηματαγοράς.* Πρακτικά Συνεδρίου από το 24ο Πανελλήνιο Συνέδριο Εμπορικού Δικαίου που διεξήχθη στα Ιωάννινα 17-19 Οκτωβρίου 2014. Φορέας διεξαγωγής: Σύνδεσμος Ελλήνων Εμπορικολόγων. Αθήνα: Νομική Βιβλιοθήκη, σελ. 503.

[13] Οδηγία 2009/110/ΕΚ, άρθρο 2, (16/09/2009): «*Για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος, την τροποποίηση των οδηγιών 2005/60/ΕΚ και 2006/48/ΕΚ και την κατάργηση της οδηγίας 2000/46/ΕΚ.*»: Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0110&from=EL (Πρόσβαση 26/01/2021).

[14] Ν. 4021/2011, «*Ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος (ενσωμάτωση Οδηγίας 2009/110/ΕΚ)»,* άρθρο 10 παρ. 1: «Ηλεκτρονικό χρήμα»: οποιαδήποτε νομισματική αξία αποθηκευμένη σε ηλεκτρονικό, συμπεριλαμβανομένου μαγνητικού, υπόθεμα, που εμφανίζεται ως απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, η οποία έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για το Σκοπό της πραγματοποίησης πράξεων πληρωμών όπως ορίζονται στο άρθρο 4 παρ. 5 του ν. 3862/2010 (Α` 113) και γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη», ΝΟΜΟΣ.

[15] Οδηγία 2009/110/ΕΚ, Αιτ. Σκέψη 8.

1.1.3. Τα κρυπτονομίσματα

Κατά την έναρξη της παγκόσμιας χρηματοπιστωτικής κρίσης το 2008, η απογοήτευση και αμφισβήτηση απέναντι στο παγκόσμιο χρηματοπιστωτικό δίκτυο έλαβε τεράστιες διαστάσεις. Εμφανίστηκε λοιπόν στο προσκήνιο το Ψηφιακό χρήμα, για την υλοποίηση του οποίου είχαν γίνει προσπάθειες και στο παρελθόν. Η επανεμφάνιση βιώσιμου ψηφιακού χρήματος σηματοδοτεί και την αναβίωση του ενδιαφέροντος για την κρυπτογράφηση[16].

1.1.3.1. Τα πρώιμα ψηφιακά νομίσματα

Στα τέλη τη δεκαετίας του 1980 πολλοί ερευνητές άρχισαν να χρησιμοποιούν την κρυπτογραφία για την κατασκευή ψηφιακών νομισμάτων. Αυτά τα πρώιμα ψηφιακά νομίσματα υποστηρίζονταν συνήθως από ένα εθνικό νόμισμα ή από πολύτιμα μέταλλα, όπως ο χρυσός[17].

Η πρώτη γνωστή απόπειρα κρυπτογράφησης έγινε στην Ολλανδία, στα τέλη της δεκαετίας του 1980, όταν κάποιος είχε την ιδέα να βάλει χρήματα σε έξυπνες κάρτες, προκειμένου να προστατεύσει τα πρατήρια βενζίνης που βρισκόντουσαν σε απομακρυσμένες περιοχές και δεχόντουσαν επιθέσεις κατά τη διάρκεια της νύχτας, καθώς έπρεπε να μένουν ανοιχτά για να ανεφοδιάζονται τα φορτηγά, ενώ οι ιδιοκτήτες αυτών δεν επιθυμούσαν να προσλάβουν φύλακες. Οι έξυπνες κάρτες λοιπόν αποτέλεσαν την ιδανική λύση, επιλύοντας ένα πρόβλημα ετών[18].

Το 1981, ο Αμερικανός κρυπτογράφος David Chaum δημοσίευσε ένα άρθρο με τίτλο «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms[19]», στο οποίο περιέγραψε ένα ανώνυμο σύστημα ψηφιακών πληρωμών. Παρουσιάστηκαν για πρώτη φορά οι «τυφλές υπογραφές», οι οποίες είχαν τη δυνατότητα να αποκρύπτουν το περιεχόμενο ενός κειμένου και εφάρμοζαν ένα συνδυασμό δημόσιων και ιδιωτικών

[16] Βλ. *Antonopoulos, A.*, ό.π., σελ. 3.
[17] *Ibid* σελ. 3.
[18] Griffith, K., 2014. *A Quick History Of Cryptocurrencies BBTC - Before Bitcoin*. Available at: https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630 (Accessed 27/01/2021), Reiff, N., 2019. *Were There Cryptocurrencies Before Bitcoin?* Available at: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/ (Accessed 27/01/2021).
[19] Chaum, D., 1981. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*. Available at: https://www.cs.utexas.edu/~shmat/courses/cs395t_fall04/chaum81.pdf (Accessed 27/01/2021).

κλειδιών για να επαληθεύσουν την εγκυρότητα των συμμετεχόντων. Έτσι, το 1989, ο Chaum δημιούργησε το «eCash» ιδρύοντας την εταιρεία DigiCash Inc., προκειμένου να πραγματώσει όλα όσα ανέλυε στο άρθρο του. Το σύστημα που δημιούργησε πραγματοποιούσε διαδικτυακές πληρωμές εντός και εκτός σύνδεσης, εξασφαλίζοντας την αποφυγή διπλών δαπανών και την προστασία του απορρήτου των χρηστών. Ως το πρώτο κρυπτονόμισμα, το σύστημα eCash ήταν διαθέσιμο σε διάφορες χώρες, όπως οι ΗΠΑ και η Φινλανδία, μέσω διαφόρων τραπεζών και έξυπνων καρτών. Αν και η DigiCash Inc. χρεοκόπησε το 1998, οι έννοιες, οι τύποι και τα εργαλεία κρυπτογράφησης που εισήγαγε έπαιξαν σημαντικό ρόλο στην ανάπτυξη μεταγενέστερων ψηφιακών νομισμάτων[20].

Το 1998, ο προγραμματιστής Wei Dai, πρότεινε ένα ηλεκτρονικό σύστημα μετρητών[21], το οποίο ήταν ανώνυμο, ιδιωτικό, ασφαλές, κατανεμημένο και αποκεντρωμένο, έκανε χρήση της κρυπτογραφίας και προέβλεπε αφενός ένα σύστημα απόδειξης εργασίας για τη δημιουργία νέων μονάδων χρήματος και αφετέρου τη δημόσια ανακοίνωση όλων των συναλλαγών για την αποτροπή της διπλής δαπάνης των ίδιων μονάδων. Στο σύστημα «B-money», όπως ονομάστηκε, χρησιμοποιούνταν ψηφιακά ψευδώνυμα, προκειμένου να μεταφερθούν νομίσματα σε ένα αποκεντρωμένο δίκτυο. Το B-money δεν υλοποιήθηκε ποτέ, είχε όμως πολύ σημαντικό αντίκτυπο στον κόσμο των ψηφιακών νομισμάτων, καθώς στοιχεία του αναφέρθηκαν ρητώς μια δεκαετία αργότερα από το δημιουργό του Bitcoin στη λευκή βίβλο που δημοσίευσε[22].

Την ίδια περίοδο με το B-money, ο κρυπτογράφος Nick Szabo εμφάνισε το Bit Gold, ο κύριος στόχος του οποίου ήταν η εξάλειψη του μεσάζοντα, που υπήρχε σε κάθε συναλλαγή. Το αποκεντρωμένο ψηφιακό νόμισμα που προτάθηκε βασιζόταν σε έναν αλγόριθμο απόδειξης εργασίας για τη δημιουργία μπλοκ, που θα περιλάμβανε αποθηκευμένες εγγραφές των συναλλαγών που είχαν γίνει. Το B-money αν και ήταν τελικά ανεπιτυχές, υπήρξε πρόδρομος για τα ψηφιακά νομίσματα που θα εισέρχονταν αργότερα στην αγορά[23].

---

[20] Costello, A., 2020. *The history of first cryptocurrencies before Bitcoin*. Available at:https://bit.ly/3cx9YVN (Accessed 27/01/2021), Kuo Chuen, D. L., Pak Nian, L., 2015.Introduction to Bitcoin. [online]. *In*: Kuo Chuen, D. L. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data.* 1st Ed. 2015, pp. 5-30. UK: Esevier Inc, σελ. 8-9.: Available at: https://bit.ly/3zmpU6Q (Accessed 26/01/2021), *Reiff, N.*, ό.π., *Griffith, K.*, ό.π., *Gajdek, S.*, *Kozak, S.*, ό.π., σελ. 2.

[21] Wei Dai, http://www.weidai.com/bmoney.txt.

[22] Βλ. *Μεταξάκης, Ε.*, ό.π., σελ. 37, *Costello, A.*, ό.π., *σελ.37*, *Reiff, N.*, ό.π.

[23] Βλ. Belotti, M., AA et al.2019. A Vademecum on Blockchain Technologies: When, Which and How. *IEEE Communications Surveys & Tutorials* [online]. 21(4). 12 July, σελ. 35: Available at: https://bit.ly/35bXgYw (Accessed 27/01/2021), *Costello, A.*, ό.π., *Reiff, N.*, ό.π..

Το 1999 και αρχές δεκαετίας του 2000, τέθηκε στο προσκήνιο το ψηφιακό νόμισμα «e-gold», το οποίο αποτέλεσε το πρώτο επιτυχημένο σύστημα μικροπληρωμών στο διαδίκτυο. Ο τρόπος λειτουργίας ήταν εξαιρετικά καινοτόμος. Οι ιδιώτες έστελναν χρυσό ή άργυρο στην εταιρεία e-gold Ltd. και το αντίστοιχο ποσό πιστωνόταν στον e-gold λογαριασμό τους. Με την χρήση του e-gold νομίσματος που διέθεταν οι χρήστες, μπορούσαν αφενός να αγοράζουν χρυσό και άλλα πολύτιμα μέταλλα και αφετέρου να συναλλάσσονται με τους υπόλοιπους χρήστες. Η πραγματοποίηση πληρωμών γινόταν μέσω μιας κρυπτογραφημένης σύνδεσης. Οι πολλαπλές επιθέσεις που δεχόταν το e-gold από hackers, καθώς οι υποψίες απάτης και ξεπλύματος μαύρου χρήματος οδήγησαν τις αρχές των ΗΠΑ[24] στην κατάσχεση των αποθεμάτων χρυσού που διέθετε η εταιρεία. Υπολογίζεται ότι η e-gold επεξεργαζόταν συναλλαγές πολύτιμων μετάλλων αξίας άνω των 2 δισεκατομμυρίων δολαρίων ΗΠΑ ετησίως[25].

Το 1997, ο κρυπτογράφος Adam Back παρουσίασε το HashCash το οποίο αρχικά εμφανίστηκε ως ένα σύστημα απόδειξης εργασίας, με κύριο σκοπό να περιορίσει τα spam του ηλεκτρονικού ταχυδρομείου και τις επιθέσεις άρνησης υπηρεσιών (DoS attacks). Στη συνέχεια, προτάθηκε η χρήση του αλγόριθμου απόδειξης εργασίας για την επιβεβαίωση των συναλλαγών που γίνονται μέσω διαδικτύου. Παρά το γεγονός ότι το HashCash τελικά καταργήθηκε, πολλά από τα στοιχεία του συστήματός του χρησιμοποιούνται στην εξορυκτική διαδικασία του Bitcoin. Πολλοί λάτρεις της κρυπτογράφησης πιστεύουν ότι ο άμεσος προκάτοχος του Bitcoin είναι το HashCash[26].

Στην πράξη τα πρώιμα ψηφιακά νομίσματα χρησιμοποιούσαν ανά τακτά χρονικά διαστήματα μια κεντρική διαχείριση για την εκκαθάριση των συναλλαγών, ακριβώς όπως συμβαίνει σε ένα παραδοσιακό τραπεζικό σύστημα. Η αδυναμία τους αυτή έγινε στόχος των κυβερνοεγκληματιών αλλά και των ίδιων των κυβερνήσεων, έτσι ώστε κατέστη αναγκαία η ανάγκη για την δημιουργία ενός πλήρως αποκεντρωμένου ψηφιακού νομίσματος. Το Bitcoin είναι ένα τέτοιο σύστημα, χωρίς καμία κεντρική αρχή ή κανένα κεντρικό σημείο ελέγχου, που να μπορούν να δεχθούν επίθεση ή να διαβληθούν. Αποτελεί μία από τις πιο

[24] United States Court of Appeals, District of Columbia Circuit, 2008. *UNITED STATES of America, Appellee v. E-GOLD, LTD., et al., Appellants*. No. 07-3074, Decided: April 11, 2008. Available at: https://caselaw.findlaw.com/us-dc-circuit/1465631.html (Accessed 25/01/2021).
[25] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π, σελ. 832, *Griffith, K.*, ό.π.., *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 9, *Reiff, N.*, ό.π..
[26] Βλ. *Costello, A.*, ό.π.., *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 11, *Reiff, N.*

ασφαλείς και εύκολες μεθόδους πληρωμής και από πολύ νωρίς συγκέντρωσε το ενδιαφέρον προγραμματιστών και οργανισμών[27].

1.1.3.2. Η εμφάνιση του Bitcoin

Η πρώτη εμφάνιση του Bitcoin αναφέρεται στις 31 Οκτωβρίου 2008, όταν σε μια κρυπτογραφημένη λίστα ηλεκτρονικού ταχυδρομείου δημοσιεύτηκε ένα έγγραφο με τίτλο «Bitcoin: Ένα peer-to-peer ηλεκτρονικό σύστημα μετρητών»[28]. Ως συντάκτης του εγγράφου εμφανίζεται ο Satoshi Nakamoto, ένα όνομα που δεν αντιστοιχεί σε κανένα υπαρκτό πρόσωπο. Το Bitcoin έμελλε να κλονίσει συθέμελα τον χρηματοπιστωτικό και οικονομικό κόσμο όπως ήταν γνωστός μέχρι τότε, καθώς η διαδικασία με την οποία παράγεται είναι πολύ διαφορετική από την παραδοσιακή διαδικασία των συμβατικών νομισμάτων.

Στις 3 Ιανουαρίου 2009 δημιουργήθηκε το δίκτυο Bitcoin και έγινε η εξόρυξη του πρώτου μπλοκ. Ο Nakamoto συνδύασε αρκετά στοιχεία που συναντήθηκαν για πρώτη φορά στο B-money και Hash Cash, δίνοντας λύση σε όλα τα προβλήματα, που συνάντησαν τα ψηφιακά νομίσματα στο παρελθόν. Η ταυτότητα του ατόμου ή της ομάδας που βρίσκεται πίσω από τη δημιουργία του Bitcoin παραμένει άγνωστη[29].

Ο Nakamoto δημιούργησε ένα εντελώς αποκεντρωμένο ηλεκτρονικό σύστημα μετρητών, που βασίζεται σε ένα ομότιμο δίκτυο το οποίο, μέσω της χρήσης μια αλγοριθμικής διαδικασίας απόδειξης εργασίας, καταλήγει σε συναίνεση, προκειμένου να γίνει η αποθήκευση μια δημόσιας αλληλουχίας συναλλαγών. Η φύση του Bitcoin, ως λογισμικού ανοιχτού κώδικα, σημαίνει ότι ο πηγαίος κώδικας είναι πλήρως αποκαλυμμένος και διαθέσιμος σε όλους τους χρήστες. Η νέα αυτή τεχνολογία ονομάζεται Blockchain και παρέχει την δυνατότητα για «ηλεκτρονικές συναλλαγές, που δεν στηρίζονται στην εμπιστοσύνη, αλλά στην κρυπτογραφική απόδειξη[30]», καθώς τα ηλεκτρονικά δεδομένα

[27] *Antonopoulos, A.*, ό.π., σελ. 3., Ghimire, H., Selvaraj, H., 2018. *A Survey on Bitcoin Cryptocurrency and its Mining.* [online]. 26th International Conference on Systems Engineering. 18-20 December 2018, Sydney, Australia. 02 February 2019, σελ. 1: Available at: https://bit.ly/3pIQ6Ei (Accessed 26/01/2001).

[28] Nakamoto, S. 2009. *A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf (Accessed 26/01/2021).

[29] Βλ. *Antonopoulos, A.*, ό.π., σελ. 4., *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 9.

[30] *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 497, *Γιαννόπουλος, Α.*, 2019. Νομικά θέματα σχετικά με την εφαρμογή της τεχνολογίας Blockchain στον τομέα της ηλεκτρικής ενέργειας. Περιβάλλον και Δίκαιο, 23(2), σελ. 220, *Antonopoulos, A.*, ό.π., σελ. 4, *Gajdek, S., Kozak, S.*, ό.π., σελ. 2, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 15, *Swan, M.*, 2015. Blockchain: Blueprint for a New Economy. Sebastopol, California: O'Reilly, σελ. 2.

είναι μοιρασμένα σε ένα δίκτυο υπολογιστών και δεν βρίσκονται συγκεντρωμένα σε κάποιον διακομιστή.

Η εφεύρεση του Satoshi Nakamoto έδωσε λύση σε αρκετά προβλήματα που συναντούσαν τα πρώιμα ψηφιακά νομίσματα και που τα εμπόδιζαν να καθιερωθούν στο παγκόσμιο οικονομικό γίγνεσθαι. Αρχικά, επέλυσε το πρόβλημα που συναντάται στα διανεμημένα συστήματα και είναι γνωστό ως «πρόβλημα των βυζαντινών στρατηγών[31]». Υποστήριξε δηλαδή, ότι η επίτευξη συναίνεσης μεταξύ μη εμπιστευτικών κόμβων και χωρίς τη μεσολάβηση τρίτου μέρους, μπορεί να γίνει μόνο αν όλες οι συναλλαγές είναι γνωστές σε όλους. Στην πράξη, αυτό σημαίνει πρώτον ότι όλες οι συναλλαγές θα πρέπει να ανακοινώνονται δημόσια και δεύτερον ότι όλοι οι συμμετέχοντες θα πρέπει να συναινούν σε ένα κοινό ιστορικό συναλλαγών[32].

Επίσης, επιλύθηκε το πρόβλημα του διπλοξοδέματος. Πριν από την λύση του Nakamoto, προκειμένου η συναλλαγή να μην ξοδευτεί δύο φορές, έπρεπε ανά διαστήματα να γίνεται εκκαθάριση όλων των συναλλαγών μέσω ενός κεντρικού γραφείου εκκαθαρίσεως. Αυτή όμως η διαδικασία έβλαπτε τον αποκεντρωμένο χαρακτήρα που ήθελαν να προβάλουν τα ψηφιακά νομίσματα. Ο Nakamoto παρουσίασε τον αλγόριθμο απόδειξης εργασίας, μέσω του οποίου, το αποκεντρωμένο δίκτυο καταλήγει σε συναίνεση, όσον αφορά τη χρονολογική σειρά των συναλλαγών, ακολουθώντας μια συγκεκριμένη διαδικασία, η οποία επαναλαμβάνεται κάθε λίγα λεπτά[33].

Ο Satoshi Nakamoto αποσύρθηκε από τα κοινά τον Απρίλιο του 2011. Ωστόσο, η φύση του Bitcoin ως λογισμικού ανοιχτού κώδικα επέτρεψε σε άλλους εθελοντές-προγραμματιστές να συνεχίσουν να εργάζονται σε αυτό, με αποτέλεσμα η κοινότητα του Bitcoin σήμερα να ευδοκιμεί. Το σύστημα του Bitcoin λειτουργεί με βάση απόλυτα διαφανείς μαθηματικές αρχές και οποιοσδήποτε προγραμματιστής μπορεί να εξετάσει το πρωτόκολλο, ώστε να δημιουργήσει δικές του εκδόσεις του λογισμικού για δοκιμή ή περαιτέρω ανάπτυξη. Σε κάθε περίπτωση, για οποιαδήποτε τροποποίηση του πηγαίου

[31] Εν συντομία, το πρόβλημα συνίσταται στη δυσκολία που αντιμετώπιζαν οι στρατηγοί όταν βρίσκονταν στη μάχη και έπρεπε να βρουν τρόπο ώστε να έχουν ένα συντονισμένο μηχανισμό επικοινωνίας, χωρίς παρεμβολές από επιτήδειους που θα ήθελαν να δημιουργήσουν πρόβλημα στην επικοινωνία.

[32] Βλ. *Antonopoulos, A.*, ό.π., σελ. 217., *Belotti, M., AA et al.*, ό.π., σελ. 33, *Nakamoto, S.*, ό.π., σελ. 2., *Swan, M.*, ό.π., σελ. 2.

[33] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 220, *Antonopoulos, A.*, ό.π., σελ. 4, *Nakamoto, S.*, ό.π., σελ. 1, Bongcayao, R.J., *29-DOLES SILVA-Cryptocurrencies and International Regulation,*: Available at: https://bit.ly/3gipNSC (Accessed 23/02/2021).

κώδικα, το Bitcoin απαιτεί πλήρη συμφωνία μεταξύ χρηστών και προγραμματιστών. Η ασφάλεια και η ανθεκτικότητα που παρέχει η κατανεμημένη υπολογιστική ισχύς είναι τόσο μεγάλη, ώστε υπολογίζεται ότι υπερβαίνει όλη τη συνδυασμένη ικανότητα επεξεργασίας των κορυφαίων υπέρ-υπολογιστών του κόσμου[34].

Σήμερα η παγκόσμια αγορά κατακλύζεται από χιλιάδες κρυπτονομίσματα. Η εμφάνισή τους σηματοδότησε την εισαγωγή του αποκεντρωμένου συστήματος στον παγκόσμιο οικονομικό χάρτη και την απαγκίστρωση των οικονομικών συναλλαγών από την εποπτεία και έλεγχο των χρηματοπιστωτικών ιδρυμάτων. Τα κρυπτονομίσματα αποτελούν μορφή ιδιωτικού χρήματος, αξιοποιώντας στο έπακρο την κρυπτογραφία και χρησιμοποιούνται για πληρωμές αντί παραστατικού χρήματος, ενώ η τιμή τους καθορίζεται με βάσει τους κανόνες της προσφοράς και της ζήτησης[35].

Τα κρυπτονομίσματα δεν πρέπει να συγχέονται με το ηλεκτρονικό χρήμα. Το ηλεκτρονικό χρήμα ξεκινά έχοντας ως αφετηρία τα κρατικά νομίσματα και δεν είναι κρυπτογραφημένο ενώ το Bitcoin συμπεριφέρεται αυτοτελώς ως νόμισμα και δεν ενσωματώνει συγκεκριμένη νομισματική αξία για να την αποθηκεύσει ή να τη μεταφέρει. Η αρχική νομισματική αξία μετατρέπεται σε άλλη νομισματική αξία, η οποία υπόκειται στις δυνάμεις της αγοράς όπως ισχύει και για κάθε άλλο νόμισμα[36]. Η άποψη αυτή ενισχύεται και από το στοιχ.10 της νέας τροποποίησης της Οδηγίας 843/2018 για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες σύμφωνα με το οποίο: «*Τα εικονικά νομίσματα δεν θα πρέπει να συγχέονται με το ηλεκτρονικό χρήμα*[37] *όπως ορίζεται στην οδηγία 2009/110, με την ευρύτερη έννοια των*

[34] Βλ. *Antonopoulos, A.*, ό.π., σελ. 4-5, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 15, Bongcayao, R.J., ό.π., σελ.5.

[35] Βλ. Κεχαγιά, Χ., 2018. Η αγορά και πώληση "bitcoin" συνιστά φορολογητέα πράξη;: μια δύσκολη απάντηση σε μια πρόκληση της εποχής μας. *Δελτίο Φορολογικής Νομοθεσίας*, 72(1618), σελ. 3.

[36] Βλ. *Αρχοντάκη, Α., Simsive, P., ό.π., σελ.* 835-836, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 503, *Μεταξάκης, Ε.*, ό.π., σελ. 32, Cvetkova I. 2018. Cryptocurrencies legal regulation. *BRICS Law Journal* [online]. Vol 5 (2), p.p. 128-153, σελ. 134-137: Available at: https://doi.org/10.21684/2412-2343-2018-5-2-128-153 (Accessed 29/01/2021), *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 6.

[37] Αρ. 2 σημείο 2) της οδηγίας 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος: «ως «ηλεκτρονικό χρήμα» νοείται οιαδήποτε αποθηκευμένη σε ηλεκτρονικό, μεταξύ άλλων και μαγνητικό υπόθεμα νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για τον σκοπό της πραγματοποίησης πράξεων πληρωμών όπως ορίζονται στο άρθρο 4 σημείο 5) της οδηγίας 2007/64/ΕΚ και η οποία γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη» Διαθέσιμη στην:
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0110&from=EL
(Πρόσβαση 26/05/2021).

«χρηματικών ποσών[38]*» της οδηγίας (ΕΕ) 2015/2366, ούτε με νομισματική αξία αποθηκευμένη σε μέσα που εξαιρούνται όπως προσδιορίζονται στην οδηγία (ΕΕ) 2015/2366*[39]*, ούτε με νομίσματα ηλεκτρονικών παιχνιδιών, που μπορούν να χρησιμοποιηθούν αποκλειστικά μέσα στο περιβάλλον των συγκεκριμένων παιχνιδιών*. Στόχος της παρούσας οδηγίας είναι να καλύψει όλες τις δυνητικές χρήσεις των εικονικών νομισμάτων».

1.2. Το χρήμα στην έννομη τάξη

Η κάθε πολιτεία προσδιορίζει τι αναγνωρίζεται ως χρήμα στα πλαίσια της επικράτειάς της και είναι αυτή που δίνει την ιδιότητα του φορέα της ονομαστικής αξίας και τη σκυτάλη στην αγορά για τη διαμόρφωση της τρέχουσας αξίας. Η αξία λοιπόν του χρήματος προσδιορίζεται βάσει της νομισματικής πολιτικής που ακολουθεί ένα κράτος ή υπερεθνικός οργανισμός. Η πολιτεία επιβάλλει τον φορέα αυτό της αξίας ως το εργαλείο για την εκπλήρωση των υποχρεώσεων και παράλληλα το ορίζει ως κοινό μέτρο οικονομικών

[38] Αρ. 4 σημείο 25) της οδηγίας (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά: ««χρηματικά ποσά»: χαρτονομίσματα και κέρματα, λογιστικό ή ηλεκτρονικό χρήμα κατά την έννοια του άρθρου 2 σημείο 2) της οδηγίας 2009/110/ΕΚ». Διαθέσιμη στη:https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015L2366&from=EL , (Πρόσβαση 26/05/2021).

[39] Αρ. 3 στοιχεία ια) και ιβ) της οδηγίας (ΕΕ) 2015/2366 σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά: «Η παρούσα οδηγία δεν εφαρμόζεται: ια) στις υπηρεσίες οι οποίες βασίζονται σε συγκεκριμένα μέσα πληρωμών που μπορούν να χρησιμοποιηθούν μόνο με περιορισμένο τρόπο και που πληρούν μία από τις ακόλουθες προϋποθέσεις: i) μέσα που επιτρέπουν στον κάτοχο να αποκτήσει αγαθά ή υπηρεσίες μόνο στην επαγγελματική στέγη που χρησιμοποιεί ο εκδότης ή εντός περιορισμένου δικτύου παρόχων υπηρεσιών στο πλαίσιο απευθείας εμπορικής συμφωνίας με επαγγελματία εκδότη ii) μέσα που μπορούν να χρησιμοποιηθούν μόνο για την απόκτηση ενός πολύ περιορισμένου φάσματος αγαθών ή υπηρεσιών·iii) Η παρούσα οδηγία δεν μέσα που ισχύουν μόνο σε ένα κράτος μέλος, παρέχονται κατ' αίτηση επιχείρησης ή οντότητας του δημόσιου τομέα και ρυθμίζονται από εθνική ή περιφερειακή δημόσια αρχή για ειδικούς κοινωνικούς ή φορολογικούς σκοπούς για την απόκτηση συγκεκριμένων αγαθών ή υπηρεσιών από προμηθευτές που έχουν συνάψει εμπορική συμφωνία με τον εκδότη·ιβ) σε πράξεις πληρωμής από πάροχο δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών οι οποίες παρέχονται επιπλέον των υπηρεσιών ηλεκτρονικών επικοινωνιών για συνδρομητή του δικτύου ή της υπηρεσίας: i) για την αγορά ψηφιακού περιεχομένου και φωνητικών υπηρεσιών, ανεξάρτητα από τη συσκευή που χρησιμοποιείται για την αγορά ή την κατανάλωση του ψηφιακού περιεχομένου και χρεώνονται στον σχετικό λογαριασμό· ή ii) οι οποίες πραγματοποιούνται από ή μέσω ηλεκτρονικής συσκευής και χρεώνονται στον σχετικό λογαριασμό στο πλαίσιο φιλανθρωπικής δραστηριότητας ή για την αγορά εισιτηρίων· υπό την προϋπόθεση ότι η αξία κάθε μεμονωμένης πράξης πληρωμής η οποία αναφέρεται στα σημεία i) και ii) δεν υπερβαίνει τα 50 EUR και: — η συνολική αξία των πράξεων πληρωμής για έναν μεμονωμένο συνδρομητή δεν υπερβαίνει τα 300 EUR ανά μήνα, ή — όταν ο συνδρομητής προχρηματοδοτεί τον λογαριασμό του στον πάροχο ηλεκτρονικού επικοινωνιακού δικτύου ή υπηρεσίας, η συνολική αξία των πράξεων πληρωμής δεν υπερβαίνει τα 300 EUR ανά μήνα». Διαθέσιμη στη:https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015L2366&from=EL.

αξιών. Η αναγνώριση του χρήματος ως κοινού μέσου ανταλλαγής σημαίνει αυτόματα ότι όλα τα οικονομικά αγαθά πρέπει να εκφραστούν σε μονάδες ενός κοινού μεγέθους[40].

Το χρήμα λοιπόν αποτελεί την χρηματική μονάδα, που είναι άυλη, προσδιορίζεται από το όνομά της δηλαδή ευρώ, ρούβλι, ευρώ, κούνα, και χρησιμεύει ως αναφορά στα πλαίσια συγκεκριμένου νομισματικού συστήματος. Κάθε αγαθό ή υπηρεσία εκφράζεται σε συγκεκριμένες μονάδες και υποδιαιρέσεις, βάσει των οποίων αποτιμώνται τα επιμέρους αγαθά και οι υπηρεσίες και μπορεί να αποκτηθούν έπειτα από ανταλλαγή με αυτό. Οι τρόποι μετακίνησης των χρηματικών μονάδων ποικίλουν. Άλλες φορές μπορεί να γίνουν με τη βοήθεια υλικών συναλλακτικών μέσων όπως χαρτονομίσματα και κέρματα, άλλες δε με άυλα μέσα όπως χρέωση τραπεζικού λογαριασμού και μεταφορά μέσω χρήσης πλατφορμών Blockchain[41].

1.2.1. Οι λειτουργίες του χρήματος

Ορισμός του χρήματος δεν υπάρχει, αλλά η έννοιά του προκύπτει από τις λειτουργίες που επιτελεί και που ορίζουν τι κάνει το χρήμα και όχι τι είναι χρήμα. Σύμφωνα με τον Αριστοτέλη, το χρήμα έχει τρεις βασικές λειτουργίες, οι οποίες συνδέονται άρρηκτα μεταξύ τους. Είναι δηλαδή μέσον ανταλλαγής, μονάδα επιμέτρησης των αξιών και μέσον διατήρησης σταθερής ανταλλακτικής αξίας, συνυφασμένης στενά με την αγοραστική του δύναμη. Η αξία είναι μια αφηρημένη δύναμη, εκφραζόμενη ως πολλαπλάσια ή ως υποδιαίρεση της νομισματικής μονάδας και η οποία γίνεται φανερή μέσω των συναλλαγών. Υπάρχουν αρκετές διαφωνίες σχετικά με το πλήθος και το είδος των λειτουργιών. Η κρατούσα άποψη ωστόσο αναγνωρίζει τρεις κύριες λειτουργίες, οι οποίες πρέπει να συντρέχουν αθροιστικά, σύμφωνα με τις οποίες το χρήμα είναι μέσον πληρωμών (medium of exchange), μέτρον αξίας (unit of account) και μέσον αποταμίευσης (store of value)[42].

Το χρήμα γίνεται δεκτό ως μέσον πληρωμής αγαθών και υπηρεσιών ή ως μέσον συναλλαγών και ανταλλαγής. Είναι αυτό, στο οποίο το κράτος παρέχει εξοφλητική ικανότητα ως μέσο εκπλήρωσης οικονομικών υποχρεώσεων. Για το λόγο αυτό, η προσφορά

[40] Βλ. *Καλλιμόπουλος, Γ.*, ό.π., σελ. 13, *Παπαρσενίου, Π.*, ό.π., σελ. 15, 41.
[41] Βλ. *Καλλιμόπουλος, Γ.*, ό.π., σελ. 26, *Μαλλέρου, Α.*, ό.π., σελ. 93-94, *Μεταξάκης, Ε.*, ό.π., σελ. 31.
[42] Βλ. *Καλλιμόπουλος, Γ.*, ό.π., σελ. 12, 15, *Μαλλέρου, Α.*, ό.π., σελ. 97, *Μεταξάκης, Ε.*, ό.π., σελ. 27, *Παπαρσενίου, Π.*, ό.π., σελ. 36, 38-40, 45.

του επιφέρει απόσβεση, δια καταβολής ενώ η απόκρουση της καταβολής επιφέρει την υπερημερία του δανειστή[43].

Επιπροσθέτως, το χρήμα είναι κοινό μέτρο οικονομικής αξίας, λειτουργώντας ως κοινή λογιστική μονάδα ή μονάδα υπολογισμού και παρέχοντας σε αυτόν που το κατέχει την δυνατότητα συμμετοχής στην οικονομική ζωή. Βάσει της μονάδας αυτής δημιουργείται ένα σύστημα τιμών, μέσω του οποίου μπορούν να αποτιμηθούν τα αγαθά και οι υπηρεσίες, τα έσοδα, έξοδα και δαπάνες, αλλά και τα υπόλοιπα οικονομικά μεγέθη όπως η μέτρηση του εθνικού προϊόντος. Τα αγαθά και οι υπηρεσίες θα πρέπει να είναι αποτιμητέα σε χρήμα, ακόμη και αν δεν ανταλλάσσονται. Το ίδιο το χρήμα δηλαδή έχει οικονομική αξία, η οποία προσδιορίζεται σε σχέση με τις τιμές, που εκφέρονται σε μονάδες χρήματος. Έτσι, η αξία κάθε αγαθού υπολογίζεται ως πολλαπλάσιο ή υποπολλαπλάσιο της νομισματικής μονάδας. Η αξία είναι υποκειμενικά τόση, όση και το αγαθό με το οποίο ανταλλάσσεται, δηλαδή αποτελεί την αγοραία αξία του[44].

Η χρηματική αξία, ως ένα σύνολο νομισματικών μονάδων, είναι άυλη και μεταβιβάζεται από τον οφειλέτη στον δανειστή είτε ενσωματωμένη σε έναν υλικό φορέα, είτε με τη χρήση μέσων πληρωμής που δεν έχουν υλική υπόσταση. Ο υλικός φορέας τίθεται σε δεύτερη μοίρα Αυτό που έχει σημασία είναι η αξία και μέσω αυτής επιτελούνται στην έννομη τάξη οι λειτουργίες του χρήματος. Η μορφή του υλικού φορέα, ακόμη και η ανυπαρξία αυτού, επηρεάζεται από τις τρέχουσες συναλλακτικές συνήθειες και από τις τεχνολογικές εξελίξεις. Ενσωμάτωση της νομισματικής αξίας υπάρχει και στο ηλεκτρονικό χρήμα. Η μόνη διαφορά είναι ότι οι νομισματικές μονάδες μεταβιβάζονται χωρίς να μεταβιβάζεται και το μέσον που τις ενσωματώνει, σε αντίθεση με ό,τι συμβαίνει στα μετρητά, όπου η ενσωμάτωση των νομισματικών μονάδων στον υλικό φορέα προσδίδει σε αυτές υλική υπόσταση. Τα χαρτονομίσματα και τα κέρματα στην περίπτωση των μετρητών, καθώς και η κάρτα ή ο μικροεπεξεργαστής στην περίπτωση του ηλεκτρονικού χρήματος δεν προκαλούν την απόσβεση, αλλά απλώς ενσωματώνουν την χρηματική αξία[45].

Λόγω της ιδιότητάς του να είναι φορέας αξίας, το χρήμα, κατ' επέκταση, έχει και την ιδιότητα να είναι μέσον αποταμίευσης. Η αποταμίευση του χρήματος είναι ευχερέστερη

[43] Βλ. *Μαλλέρου, Α.*, ό.π., σελ. 93-94, *Μεταξάκης, Ε.*, ό.π., σελ. 27, *Παπαρσενίου, Π.*, ό.π., σελ. 49.
[44] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 3, *Καλλιμόπουλος, Γ.*, ό.π., σελ. 27, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 502, *Μαλλέρου, Α.*, ό.π., σελ. 94, *Σταθόπουλος, Μ,* ό.π., σελ. 222-223.
[45] Βλ. . *Καλλιμόπουλος, Γ.*, ό.π., σελ. 38, *Μαλλέρου, Α.*, ό.π., σελ. 97, 99, European Central Bank. *VIRTUAL CURRENCY SCHEMES.* σελ.16, Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (Accessed 28/05/2021).

και λιγότερο δαπανηρή εν σχέσει με την αποταμίευση λοιπών υλικών αγαθών, τα οποία μπορεί να φθείρονται με την πάροδο του χρόνου ή έχουν ημερομηνίας λήξης. Επιπροσθέτως, η λειτουργία αυτή επιτρέπει στο χρήμα να αποτελεί μέσον αναβολής πληρωμών ή μέσον δανεισμού, όταν χρησιμοποιείται για μετάθεση των πληρωμών σε μεταγενέστερο χρόνο, γεγονός το οποίο επιτρέπει να κρατά σταθερή την αγοραστική του δύναμη[46].

1.2.2. Το χρήμα υπό ευρεία και στενή έννοια

Το χρήμα αποτελεί μελέτη κυρίως της οικονομικής επιστήμης. Από την πλευρά της νομικής επιστήμης, αποκτά σημασία ιδίως στο ιδιωτικό δίκαιο, καθώς το χρήμα αποτελεί μέσον απόσβεσης των χρηματικών υποχρεώσεων, ενώ και οι μη χρηματικές παροχές μπορούν εν τέλει να μετατραπούν σε παροχές χρηματικές αποζημιώσεως και να αποσβεστούν με την καταβολή χρήματος. Η πιο ουσιαστική διαφορά μεταξύ ευρείας και στενής έννοιας του χρήματος είναι η υποχρεωτικότητα της λήψης του από το δανειστή, καθώς μόνο το νόμιμο χρήμα θεωρείται ως προσήκουσα καταβολή χρηματικής οφειλής, η οποία οδηγεί σε απόσβεση του χρέους[47].

Κάποιες φορές γίνεται ταύτιση της έννοιας του χρήματος, όπως αποδίδεται στην οικονομική επιστήμη, με την έννοια που λαμβάνει υπό τη νομική επιστήμη. Επί της ουσίας, η διαφορά μεταξύ των δύο εννοιών του χρήματος έγκειται στο κατά πόσο η πολιτεία επιβάλλει προαιρετικό ή υποχρεωτικό χαρακτήρα στην αποδοχή του χρήματος. Έτσι, αυτό που αναγνωρίζεται από την οικονομική επιστήμη ως χρήμα είναι για τη νομική το υπό ευρεία έννοια χρήμα, ενώ χρήμα υπό στενή έννοια είναι αυτό που νομοθετικά εκπληρώνει τις υπό ευρεία έννοια λειτουργίες του χρήματος και καθιερώνεται ως τέτοιο, δηλαδή το νόμισμα δηλαδή της κάθε επιμέρους πολιτείας[48].

Υπό ευρεία έννοια, χρήμα είναι τα αντικαταστατά πράγματα, όπως χρησιμοποιούνται και γίνονται δεκτά στις συναλλαγές, προσδιοριζόμενο από τις λειτουργίες που επιτελεί στην συναλλακτική πραγματικότητα και όπως αναλυτικά της αναφέραμε ανωτέρω. Θα πρέπει επομένως το χρήμα να έχει σχετικά ευρεία διάδοση, να είναι ευχερώς και για αρκετό χρόνο αποταμιεύσιμο και η αξία χρήσης του να είναι μικρότερη από την αξία

[46] Βλ. *Μαλλέρου, Α.*, ό.π., σελ. 93, *Μεταξάκης, Ε.*, ό.π., σελ. 27, 32, *Σταθόπουλος, Μ*, ό.π., σελ. 223, Surowiecki J., ό.π., σελ. 46.
[47] Βλ. *Καζαζάκης, Θ.*, ό.π, σελ. 4, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π.,, ό.π., σελ. 503, *Μαλλέρου, Α.*, ό.π., σελ. 90.
[48] Βλ. *Καλλιμόπουλος, Γ.*, ό.π., σελ. 14, *Μαλλέρου, Α.*, ό.π., σελ. 110.

του ανταλλασσόμενου αγαθού[49]. Η νομική επιστήμη προσεγγίζει την έννοια του χρήματος βάσει των οικονομικών λειτουργιών του. Κατά τον Σταθόπουλο[50]: «χρήμα είναι ο,τιδήποτε χρησιμοποιείται ως γενικό μέσο πληρωμών σε μια κοινωνία, που παράλληλα, όχι όμως αναγκαστικά, αποτελεί και γενικό μέτρο της αξίας των αγαθών». Στον ΑΚ Άρθρο 950: «χρήμα θεωρείται οποιοδήποτε υλικό αντικείμενο φέρει τα χαρακτηριστικά αντικαταστατού πράγματος, χρησιμοποιείται δε σε συγκεκριμένη κοινωνία και χρονική περίοδο ως κοινό ανταλλακτικό μέσο, ως μέσο εξόφλησης των υποχρεώσεων και ως μέσο σύγκρισης της αξίας των αγαθών και υπηρεσιών». Στην ευρεία έννοια του χρήματος εμπίπτει και το λογιστικό χρήμα, τα νομίσματα ξένων χωρών, οι ταξιδιωτικές επιταγές ή άλλα κοινά μέσα πληρωμής, των οποίων η λήψη από το δανειστή δεν είναι υποχρεωτική καθώς δεν αποτελούν νόμιμα μέσα πληρωμής. Απαραίτητη προϋπόθεση, για να αποτελέσει ένα αγαθό «χρήμα» υπό ευρεία έννοια, είναι η αξία χρήσης που έχει το ίδιο το αγαθό να είναι μικρότερη από την αξία των αγαθών, στην ανταλλαγή των οποίων μεσολαβεί[51].

Υπό στενή έννοια λογίζεται το χρήμα όταν συντρέχουν δύο προϋποθέσεις, αφ' ενός να εκπληρώνει τις λειτουργίες του ως υπό ευρεία έννοια χρήμα και αφ' ετέρου να έχει καθιερωθεί από την πολιτεία ως υποχρεωτικό μέσον πληρωμής. Υπό στενή έννοια χρήμα είναι τα κινητά πράγματα και διακρίνονται σε κέρματα και τραπεζογραμμάτια, έχοντας ονομαστική και τρέχουσα κυκλοφοριακή αξία. Ονομαστική είναι η αξία του νομίσματος που αποδίδει ο νόμος και αναγράφεται πάνω σε κάθε νομισματική μονάδα, ενώ τρέχουσα είναι η αξία που έχει το νόμισμα συγκριτικά με τα άλλα νομίσματα[52].

Σύμφωνα με το άρθρο 10 του Κανονισμού 974/98 ΕΚ[53] «Για την εισαγωγή του ευρώ»: «η ΕΚΤ και οι κεντρικές τράπεζες των συμμετεχόντων κρατών μελών θέτουν σε κυκλοφορία τραπεζογραμμάτια ευρώ στα συμμετέχοντα κράτη μέλη. [..] τα τραπεζογραμμάτια ευρώ είναι τα μόνα που έχουν την ιδιότητα νόμιμου χρήματος στα συμμετέχοντα κράτη μέλη». Αυτό σημαίνει ότι δια της καταβολής τους επέρχεται εξόφληση

[49] Βλ. *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 502, *Μαλλέρου, Α.*, ό.π., σελ. 110-111.
[50] Βλ. *Σταθόπουλος, Μ,* ό.π., σελ. 223.
[51] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 3-4, *Μαλλέρου, Α.*, ό.π., σελ. 111-110, *Καλλιμόπουλος, Γ.*, ό.π., σελ. 15.
[52] Βλ. *Αρχοντάκη, Α., Simsive, P., ό.π., σελ.* 835-836, *Καζαζάκης, Θ.*, ό.π., σελ. 4., *Καλλιμόπουλος, Γ.*, ό.π., σελ. 19, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 503, *Μαλλέρου, Α.*, ό.π., σελ. 111-112.
[53] Κανονισμός (ΕΚ) αριθ. 974/98. (03/05/1998). «*Για την εισαγωγή του ευρώ*»: Ανακτήθηκε από: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1998R0974:20110101:EL:PDF (Πρόσβαση 01/02/2021).

των υποχρεώσεων ενώ οποιαδήποτε απόκρουσή τους από τον δανειστή έχει ως αποτέλεσμα την υπερημερία αυτού[54].

Πέραν ωστόσο των τραπεζογραμματίων και κερμάτων, μπορούν και άλλα εργαλεία να λάβουν τον ρόλο του χρήματος, ως φορέα αξίας εκφρασμένου σε νομισματικές μονάδες και ως μέσον εξοφλήσεως των υποχρεώσεων. Το γεγονός ότι ο νομοθέτης καθιστά υποχρεωτική την απόσβεση με τραπεζογραμμάτια και κέρματα δεν σημαίνει ότι την καθιστά περιοριστική και δεν συνεπάγεται τον αποκλεισμό οποιασδήποτε αναγνώρισης ή την ρύθμιση άλλων εργαλείων ως χρήμα. Η έμμεση αυτή πολιτειακή αναγνώριση σε καμία περίπτωση δεν μπορεί να ερμηνευτεί ότι τα μέσα αυτά πληρωμής καθίστανται υποχρεωτικά. Αντιθέτως υποχρεωτικό χαρακτήρα θα μπορούσαν να αποκτήσουν εφόσον υπάρχει κοινωνική συναίνεση που καθιερώνει την χρήση τους στις συναλλαγές και στηρίζεται στην καλή πίστη και τα συναλλακτικά ήθη[55].

1.2.3. Η υπαγωγή του Bitcoin στην έννοια του χρήματος

Το θέμα που ερίζει στη δημόσια συζήτηση είναι αν το κρυπτονόμισμα αποτελεί χρήμα ή όχι. Η υπαγωγή του Bitcoin καθώς και των κρυπτονομισμάτων εν γένει στο υπό στενή έννοια χρήμα αποκλείεται εκ προοιμίου, καθώς δεν έχει επιβληθεί από κανένα κράτος ως υποχρεωτικό μέσο πληρωμής. Ωστόσο, οι απόψεις διίστανται, εάν το Bitcoin μπορεί να ενταχθεί στην ευρεία έννοια του χρήματος και επομένως να λειτουργήσει ως χρήμα και δη ως αξιόπιστος και σταθερός φορέας ανταλλακτικής αξίας[56].

Όσο περνάει ο καιρός, το Bitcoin γίνεται αποδεκτό ως γενικό μέσον πληρωμών από όλο και μεγαλύτερο μέρος της εγχώριας και διεθνούς αγοράς. Στην πράξη, η αποδοχή του ως μέσου συναλλαγής είναι καθαρά θέμα ιδιωτικής βούλησης και δεν έχει υποχρεωτικό χαρακτήρα. Έτσι, εφόσον δεν υπάρχει αντίθετη συμφωνία, ο δανειστής δεν είναι υποχρεωμένος να το δεχτεί ως καταβολή, ούτε καν βάσει των γενικών αρχών για την καλή πίστη και τα συναλλακτικά ήθη[57].

[54] Βλ. *Καλλιμόπουλος, Γ.*, ό.π., σελ. 19.
[55] Βλ. *Καλλιμόπουλος, Γ.*, ό.π., σελ. 19, 58, *Μαλλέρου, Α.*, ό.π., σελ. 113-114, *Gajdek, S., Kozak, S.*, ό.π., σελ. 6.
[56] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 4, *Παπαρσενίου, Π.*, ό.π., σελ. 16
[57] ΑΚ 281, 288, Βλ. *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 503-504.

Καταλυτική στην αναγνώριση του Bitcoin ως μέσου πληρωμής υπήρξε η απόφαση C-264/14[58] «Skatteverket v. David Hedqvist C-264/14». Σε αυτήν, το Δ.Ε.Ε. χαρακτήρισε το Bitcoin ως μέσον πληρωμής, αναφέροντας συγκεκριμένα ότι η αγοραπωλησία του από επιτηδευματίες δεν υπόκειται στην επιβολή ΦΠΑ. Πιο συγκεκριμένα, στο σημείο 11 της απόφασης το Δ.Ε.Ε. αναφέρει ότι: «το Bitcoin χρησιμοποιείται ως επί το πλείστον για πληρωμές μεταξύ ιδιωτών στο Διαδίκτυο, καθώς και σε ορισμένα διαδικτυακά εμπορικά καταστήματα που δέχονται το συγκεκριμένο νόμισμα. […] Το σύστημα του Bitcoin επιτρέπει την κατοχή και μεταφορά, ανωνύμως, ποσών εκπεφρασμένων σε Bitcoin εντός του δικτύου από χρήστες που διαθέτουν διευθύνσεις Bitcoin». Έκρινε λοιπόν ότι η εταιρία, που παρείχε υπηρεσίες από αγοραπωλησίες συμβατικών νομισμάτων έναντι του εικονικού νομίσματος Bitcoin και αντιστρόφως, παρείχε υπηρεσίες από επαχθή αιτία, οι οποίες κανονικά υπόκεινται σε ΦΠΑ σύμφωνα με την Οδηγία 2006/112/ΕΚ[59] «σχετικά με το κοινό σύστημα φόρου προστιθέμενης αξίας». Στην προκειμένη όμως περίπτωση λόγω της φύσης και του σκοπού του Bitcoin ως μέσου πληρωμών, εφαρμόστηκε η εξαίρεση που προβλέπεται στην Οδηγία, άρθρο 135 παρ.1 περίπτωση δ΄: «Τα κράτη μέλη απαλλάσσουν τις ακόλουθες πράξεις, περιλαμβανομένης της διαπραγμάτευσης, οι οποίες αφορούν καταθέσεις, τρεχούμενους λογαριασμούς, πληρωμές, μεταφορές χρημάτων, απαιτήσεις, επιταγές».

Η δεύτερη λειτουργία του χρήματος που θα πρέπει να μελετηθεί είναι αν το Bitcoin αποτελεί μέτρο αξίας ή μονάδα μέτρησης. Όπως αναφέρθηκε ήδη η χρηματική αξία είναι άυλη και δεν πρέπει να συγχέεται με τον υλικό φορέα που την πραγματώνει. Ενώ λοιπόν το ηλεκτρονικό χρήμα ενσωματώνει χρηματική αξία, το Bitcoin αποτελεί το ίδιο χρηματική αξία χωρίς να αποτυπώνεται σε κάποιον υλικό φορέα. Το Bitcoin επίσης χωρίζεται σε μονάδες και υποδιαιρέσεις. Οι υποδιαιρέσεις μάλιστα μπορεί να φτάσουν τις οκτώ, τέσσερεις περισσότερες από το κλασσικό νόμισμα. Αυτή η ιδιότητα αυξάνει την ακρίβεια της αποτίμησης των περιουσιακών στοιχείων και την χρησιμότητά της κατά τη διάρκεια των

[58] Βλ. Απόφαση ΔΕΕ C-264/14, 2015. Skatteverket v David Hedqvist. *Προδικαστική παραπομπή — Κοινό σύστημα φόρου προστιθέμενης αξίας (ΦΠΑ) — Οδηγία 2006/112/ΕΚ — Άρθρα 2, παράγραφος 1, στοιχείο γ΄, και 135, παράγραφος 1, στοιχεία δ΄ έως στ΄ — Υπηρεσίες παρεχόμενες εξ επαχθούς αιτίας — Συναλλαγές ανταλλαγής εικονικού νομίσματος "bitcoin" με συμβατικά νομίσματα — Απαλλαγή.* Αποφασίσθηκε την 22α Οκτωβρίου 2015. Ανακτήθηκε από: https://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=EL (Πρόσβαση 06/06/2021).

[59] Βλ. Οδηγία 2006/112/ΕΚ, (28/11/2006). *Σχετικά με το κοινό σύστημα φόρου προστιθέμενης αξίας.* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32006L0112 (Πρόσβαση 06/06/2021).

συναλλαγών. Εφόσον λοιπόν μπορεί να εκφράσει την αξία κάθε αγαθού και υπηρεσίας, φαίνεται να αποτελεί και μέτρο αξιών[60].

Το πιο δύσκολο ερώτημα είναι αν όντως το Bitcoin μπορεί να χαρακτηρισθεί ως μέσο αποθησαυρισμού. Η δυσκολία έγκειται στην απουσία κεντρικής διαχείρισης που μπορεί να προκαλέσει ακραίες διακυμάνσεις της αξίας του. Πρέπει λοιπόν να πληρούνται δύο προϋποθέσεις, τα κρυπτονομίσματα να μπορούν αφενός να διατηρήσουν την αγοραστική τους δύναμη και αφετέρου να χρησιμοποιηθούν σε βάθος χρόνου. Αμφιβολίες υπάρχουν για το κατά πόσο η τιμή του Bitcoin είναι αρκετά σταθερή, ώστε αυτό να λειτουργεί ως νόμισμα. Οι τεράστιες αυξομειώσεις που έχει λάβει η τιμή του ανά περιόδους, προκαλεί προβληματισμούς στο κατά πόσο μπορεί πράγματι να διατηρήσει την αγοραστική του δύναμη. Για παράδειγμα, τον Οκτώβριο του 2013 η τιμή του Bitcoin ήταν 200 δολάρια, ενώ στις αρχές Νοεμβρίου του 2013 η τιμή του έφθασε στα 1200 δολάρια. Τα χρήματα θα πρέπει επίσης να είναι ανθεκτικά. Η έλλειψη υλικού φορέα επιτελεί αυτή την προϋπόθεση. Τα αρχεία του ιστορικού συναλλαγών κατανέμονται μεταξύ όλων των συσκευών που εμπλέκονται σε κάθε συναλλαγή. Όσο περισσότερες συσκευές εμπλέκονται στο σύστημα του Bitcoin, τόσο περισσότερα αντίγραφα του μητρώου δημιουργούνται. Επιπροσθέτως, στις μέρες μας πολλοί επενδυτές χρησιμοποιούν το Bitcoin ως εναλλακτικό μέσον επένδυσης, προσδίδοντάς του τον χαρακτήρα του αποθησαυρισμού[61].

Συμπεραίνουμε λοιπόν ότι το Bitcoin πληροί και τις τρεις λειτουργίες του χρήματος.

Τα κρυπτονομίσματα, όπως θα αναφερθεί αναλυτικά στο πέμπτο κεφάλαιο, αποτελούν υποκατηγορία των εικονικών νομισμάτων. Οι ορισμοί που έχουν δώσει για τα εικονικά νομίσματα η Ευρωπαϊκή Κεντρική Τράπεζα (European Central Bank, στο εξής ECB), η Ευρωπαϊκή Αρχή Τραπεζών (European Bank Authority, στο εξής EBA) και η Ομάδα Χρηματοοικονομικής Δράσης (Financial Task Force, στο εξής FAFT) είναι:

- ECB[62]: «εικονικά νομίσματα μπορούν να ορισθούν ως η ψηφιακή αναπαράσταση αξίας, που δεν εκδίδονται από κεντρική τράπεζα, πιστωτικό ίδρυμα ή ίδρυμα ηλεκτρονικού

[60] Βλ. *Μαλλέρου, Α.*, ό.π., σελ. 97, *Μεταξάκης, Ε.*, ό.π., σελ. 43, *Gajdek, S., Kozak, S.*, ό.π., σελ. 6, Kozak, ό.π., σελ. 6.
[61] Βλ. *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 499, *Μεταξάκης, Ε.*, ό.π., σελ. 44, Kozak, ό.π., σελ. 6, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 11-12.
[62] Πρωτότυπο κείμενο: «virtual currency can therefore be defined as a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money». European Central Bank. *Virtual currency schemes - a further analysis [2015]*, σελ25, Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (Accessed 08/06/2021).

χρήματος, το οποίο σε ορισμένες περιπτώσεις μπορεί να χρησιμοποιηθεί αντί του χρήματος».

- ΕΒΑ[63]: « τα εικονικά νομίσματα ορίζονται ως ψηφιακές αναπαραστάσεις αξίας που ούτε εκδίδονται από κεντρική τράπεζα ή δημόσια αρχή ούτε δεσμεύονται απαραίτητα σε νόμισμα fiat, αλλά χρησιμοποιούνται από φυσικά ή νομικά πρόσωπα ως μέσο ανταλλαγής και μπορούν να μεταφερθούν, να αποθηκευτούν ή να ανταλλαχθούν ηλεκτρονικά».
- FAFT[64]: «εικονικό νόμισμα είναι μια ψηφιακή αναπαράσταση αξίας, που μπορεί να ανταλλαχθεί ψηφιακά και να λειτουργεί ως (1) μέσο ανταλλαγής ή/και ως (2) μέτρο αξίας ή/και ως (3) μέσον αποταμίευσης, αλλά δεν έχει καθεστώς υποχρεωτικού νομίσματος πληρωμών ή συναλλαγών σε οποιαδήποτε δικαιοδοσία».

Παρατηρείται ότι και οι τρεις ορισμοί συνηγορούν στην άποψη ότι τα κρυπτονομίσματα έχουν τις λειτουργίες του χρήματος και αναγνωρίζονται ως χρήμα υπό την ευρεία έννοια. Στον ορισμό αναφέρονται και οι τρεις λειτουργίες του χρήματος.

<table>
<tr><td rowspan="3">Legal status</td><td rowspan="2">Unregulated</td><td>– Certain types of local currencies</td><td>– Virtual currency</td></tr>
<tr><td rowspan="2">Regulated</td><td rowspan="2">– Banknotes and coins</td><td>– E-money</td></tr>
<tr><td>– Commercial bank money (deposits)</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Physical</td><td>Digital</td></tr>
<tr><td colspan="2">Money format</td></tr>
</table>

Εικόνα 1: Κατηγορίες χρήματος [65]

Όπως προκύπτει και από την εικόνα, το εικονικό νόμισμα είναι μια υποκατηγορία του ψηφιακού και δεν πρέπει οι δύο όροι να συγχέονται.

Στην Αμερική για πρώτη φορά το Bitcoin αναγνωρίστηκε ως μορφή χρήματος από το Περιφερειακό Δικαστήριο των ΗΠΑ, που εδρεύει στην Ανατολική Περιφέρεια της

[63] Πρωτότυπο κείμενο: «virtual currency is defined as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically», EBA. *Opinion on 'virtual currencies'*. σελ.11 *Available at:https://service.betterregulation.com/document/159234 (Accessed 03/06/2021).*

[64] Πρωτότυπο κείμενο: «Virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction.», σελ. 4, FATF. *Virtual Currencies Key Definitions and Potential AML/CFT Risks.* Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Accessed 08/06/2021).

[65] Βλ. European Central Bank, [2012], ό.π, σελ.22.

Πολιτείας του Τέξας**.** Στην υπόθεση «Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust[66]», το δικαστήριο αναγνώρισε το Bitcoin ως «μορφή νομίσματος ή κάποιας μορφής χρήμα», επισημαίνοντας ότι μπορεί να χρησιμοποιηθεί ως νόμισμα στα μέρη όπου γίνεται δεκτό ως τέτοιο και χωρίς πάντως να προσδιορίζεται κάτι περαιτέρω[67]. Η απόφαση αυτή του Δικαστηρίου θεωρείται ιστορική, καθώς είναι η πρώτη που αποφαίνεται ρητώς ότι τα Bitcoins θα υπόκεινται στην ίδια ρύθμιση με όλα τα υπόλοιπα νομίσματα αναγκαστικής κυκλοφορίας και ως εκ τούτου θα επιβλέπονται από τις ίδιες ρυθμιστικές αρχές[68].

Σε κάθε περίπτωση η απουσία ενός κεντρικού συστήματος ελέγχου δεν πρέπει να δημιουργεί την λανθασμένη εντύπωση ότι τα κρυπτονομίσματα άγονται και φέρονται από την τύχη. Το Bitcoin αποτέλεσε το εφαλτήριο για την δημιουργία και εμφάνιση πληθώρας νομισμάτων, ο μηχανισμός της λειτουργίας των οποίων είναι εντυπωσιακός, ενώ η τεχνολογία στην οποία βασίζεται εξελίσσεται συνεχώς, καθώς αποτελεί μια διαρκή πρόκληση για όλους όσους ασχολούνται με τον κλάδο αυτό[69].

[66] CASE NO. 4:13-CV-416, United States District Court EASTERN DISTRICT OF TEXAS SHERMAN DIVISION SECURITIES AND EXCHANGE COMMISSION V. TRENDON T. SHAVERS and BITCOIN SAVINGS AND TRUST, Securities and Exchange Commission v. Shavers et al. No. 4:2013cv00416 - Document 23 (E.D. Tex. 2013). Available at: https://bit.ly/2Tmu8Ld (Accessed 05/06/2021).

[67] Πρωτότυπο κείμενο απόφασης: «It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money, and investors wishing to invest in BTCST provided an investment of money».

[68] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 5-6, *Κεχαγιά, Χ.*, ό.π., σελ. 3.

[69] Βλ. *Μεταξάκης, Ε.*, ό.π., σελ. 43-44.

ΚΕΦΑΛΑΙΟ 2ο
ΟΙ ΣΥΝΑΛΛΑΓΕΣ ΜΕ BITCOIN

Οι συναλλαγές είναι ο λόγος ύπαρξης του συστήματος Bitcoin. Όλα όσα υπάρχουν σε αυτό είναι σχεδιασμένα ούτως ώστε αυτές να μπορούν να δημιουργηθούν, να διαδοθούν στο δίκτυο, να επικυρωθούν και τελικά να προστεθούν στο παγκόσμιο κατάστιχο των συναλλαγών που ονομάζεται Blockchain. Η διεξαγωγή συναλλαγών με τη χρήση BTC δεν είναι μια διαδικασία γνώριμη όπως είναι μια γνωστή δοσοληψία σε τραπεζικό κατάστημα. Συστατικό στοιχείο για την είσοδο ενός χρήστη στο οικοσύστημα του Bitcoin είναι η δημιουργία ενός πορτοφολιού. Η πρώτη ενέργεια για να γίνει κάποιος μέλος της κοινότητας του Bitcoin είναι είτε να εγκαταστήσει στον υπολογιστή το λογισμικό Bitcoin Client, το οποίο παρέχεται δωρεάν από την κοινότητα του Bitcoin και άλλες ιστοσελίδες, είτε να χρησιμοποιήσει μια εφαρμογή ιστού, η οποία «τρέχει» το πρωτόκολλο Bitcoin. Τότε μόνο μπορεί να αποκτήσει ένα πορτοφόλι Bitcoin. Δεν χρειάζεται να παρασχεθούν περαιτέρω προσωπικά στοιχεία της ταυτότητας των μερών.

Το ταξίδι μιας συναλλαγής ξεκινά τη στιγμή που δημιουργείται και τελειώνει όταν η συναλλαγή καταγράφεται στην αλυσίδα των μπλοκ και γίνεται η αλλαγή στο ψηφιακό πορτοφόλι του χρήστη. Κάθε συναλλαγή είναι μια δημόσια εγγραφή στην αλυσίδα των μπλοκ του Bitcoin και έχει ένα επαληθεύσιμο ιστορικό το οποίο είναι προσβάσιμο από τον οποιοδήποτε. Έτσι οποιοσδήποτε το επιθυμεί μπορεί να ανατρέξει στις συναλλαγές που έχουν γίνει από και προς μια συγκεκριμένη διεύθυνση, φτάνοντας ακόμη και στην αρχική συναλλαγή. Οι συμμετέχοντες σε μία συναλλαγή στο σύστημα του Bitcoin μπορεί να είναι είτε μεμονωμένα άτομα είτε πολλοί χρήστες[70].

[70] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 833, 835, *Κεχαγιά, Χ.*, 2018. Η αγορά και πώληση "bitcoin" συνιστά φορολογητέα πράξη;: μια δύσκολη απάντηση σε μια πρόκληση της εποχής μας. Δελτίο Φορολογικής Νομοθεσίας, 72(1618), σελ. 3, Μούζουλας, Σ., 2017. Επενδυτικά κεφάλαια εικονικού νομίσματος. *Δίκαιο Επιχειρήσεων και Εταιριών*, 24(10), σελ. 1184, *Antonopoulos, A.*, ό.π., σελ. 6, 10, 274, 117, *Belotti, M., AA et al.*, ό.π., σελ. 3, 6, *Gajdek, S., Kozak, S.*, ό.π., σελ. 2, Jokić, S., AA et al., 2019. *Comparative analysis of cryptocurrency wallets vs traditional wallets* [online]. 5th International Conference Sinteza 2018. Belgrade, Serbia. 20 April 2018. *Ekonomika* 65(3), σελ. 67. Available at: https://bit.ly/2TupMBN (Accessed 28/01/2001), *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 18, *Swan, M.*, ό.π., σελ. 97, *Βλ. Bongcayao, R.J., ό.π.*, ό.π., σελ. 3.

2.1. Το Πορτοφόλι Bitcoin

Τα πορτοφόλια Bitcoin ποικίλουν σε ποιότητα, αποδοτικότητα, ιδιωτικότητα και αξιοπιστία. Υπάρχουν πορτοφόλια που στοχεύουν σε συγκεκριμένες πλατφόρμες και άλλα που στοχεύουν σε συγκεκριμένους χρήστες, ανάλογα με την εμπειρία τους στο συγκεκριμένο χώρο. Εν τέλει, η επιλογή εξαρτάται από τη χρήση που αυτός επιδιώκει και είναι καθαρά υποκειμενική[71].

2.1.1. Κατηγορίες πορτοφολιών

Τα πορτοφόλια Bitcoin κατηγοριοποιούνται ανάλογα με το αν χρειάζονται σύνδεση στο Διαδίκτυο και ανάλογα με το ποσοστό αυτονομίας και την αλληλεπίδραση που έχουν με το λοιπό δίκτυο του Bitcoin. Όσα χρειάζονται σύνδεση στο διαδίκτυο χωρίζονται με τη σειρά τους σε περαιτέρω κατηγορίες, ανάλογα με την πλατφόρμα που χρησιμοποιούν. Στην πράξη βέβαια, οι χρήστες μοιράζουν τον κίνδυνο ανάμεσα σε πολλά και διαφορετικά πορτοφόλια.[72].

❖ **Ανάλογα με τη σύνδεση στο διαδίκτυο**

Τα πορτοφόλια χωρίζονται σε δυο κατηγορίες, σε hot wallets ή θερμά πορτοφόλια και σε cold wallets ή ψυχρά πορτοφόλια, ανάλογα με το αν η πρόσβαση στο Διαδίκτυο είναι απαραίτητη για τη χρήση τους.

1) Οι χρήστες των **hot wallets** έχουν συχνές συναλλαγές στο χώρο του διαδικτύου και για λόγους ασφαλείας επιλέγουν να κρατούν μέσα στο πορτοφόλι μόνο ένα μικρό ποσό του συνόλου των BTC που κατέχουν. Σε αυτήν την κατηγορία πορτοφολιού συναντώνται τέσσερεις υποκατηγορίες[73]: mobile wallet, web wallet, desktop wallet και multisig / multi-signature wallet.

α) Το mobile wallet ή κινητό πορτοφόλι είναι το πιο διαδεδομένο. Υποστηρίζεται από κινητές συσκευές με λειτουργικό σύστημα iOS ή Android. Χαρακτηρίζεται από ευκολία στην χρήση τους, γεγονός που τα κάνει ιδανικά για νέους χρήστες, ενώ παράλληλα έχει όλα τα χαρακτηριστικά, ώστε να το επιλέξουν και έμπειροι χρήστες. Ωστόσο, αν το τηλέφωνο παραβιαστεί, ένας χρήστης μπορεί να χάσει τα διακριτικά κρυπτογράφησής του, ενώ παράλληλα είναι ευάλωτο σε κακόβουλα προγράμματα, καταγραφικό κλειδιών και ιούς[74].

[71] Βλ. *Antonopoulos, A.*, ό.π., σελ. 274.
[72] *Ibid* σελ. 274.
[73] Βλ. *Antonopoulos, A.*, ό.π., σελ. 6, *Jokić, S., AA et al.*, ό.π., σελ. 67.
[74] Βλ. *Jokić, S., AA et al.*, ό.π., σελ. 68, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 18.

β) Στο web wallet ή πορτοφόλι ιστού/ διαδικτυακό, η πρόσβαση γίνεται με σύνδεση στο διαδίκτυο μέσω ενός προγράμματος περιήγησης, ανεξάρτητα από τη συσκευή που χρησιμοποιείται μόνο. Στην πράξη, ο πλήρης έλεγχος του ψηφιακού πορτοφολιού βρίσκεται στο χέρι τρίτων ή κεντρικών αρχών. Οι περισσότεροι πάροχοι υπηρεσιών διατηρούν τον έλεγχο των BTC των χρηστών τους, παρέχοντας ως αντάλλαγμα ευκολία χρήσης. Μπορεί λοιπόν οι συναλλαγές να ολοκληρώνονται σε σύντομο χρονικό διάστημα, ωστόσο θεωρείται αναξιόπιστο να αποθηκεύονται μεγάλα ποσά BTC σε συστήματα που κατέχουν τρίτα πρόσωπα, καθώς υπάρχει ο κίνδυνος να χαθούν τα BTC, εάν δεν ληφθεί η κατάλληλη ασφάλεια. Επιπλέον, η έλλειψη γνώσεων στις τεχνολογίες πληροφοριών επιφυλάσσει για τους χρήστες τον κίνδυνο διαφόρων διαδικτυακών απατών[75].

γ) Το desktop wallet ή πορτοφόλι επιτραπέζιου υπολογιστή, θεωρείται το πιο ασφαλές εν σχέσει με τις προηγούμενες δυο κατηγορίες. Οι χρήστες δημιουργούν και διατηρούν τα πορτοφόλια στον υπολογιστή τους εξασφαλίζοντας απόλυτη αυτονομία και έλεγχο. Τα desktop wallets, ωστόσο, παρουσιάζουν κάποια μειονεκτήματα. Αυτά είναι κυρίως η ελλιπής διαμόρφωση και αστάθεια όταν χρησιμοποιούνται σε περιβάλλον MacOS ή Windows, και το ευάλωτο απέναντι σε κακόβουλους χρήστες ή λογισμικά. Για το λόγο αυτό, απαιτείται περιοδική δημιουργία αντιγράφων ασφαλείας ή η χρήση ενός παλαιότερου φορητού υπολογιστή με καθαρό λειτουργικό σύστημα, με μοναδικό σκοπό την αποθήκευση ψηφιακών στοιχείων[76].

δ) Το multisig / multi-signature wallet ή το πορτοφόλι πολλαπλών υπογραφών είναι μια πολύ ιδιαίτερη κατηγορία, καθώς η πρόσβαση σε αυτό απαιτεί την ταυτόχρονη παρουσία δύο ή τριών χρηστών που ο καθένας διαθέτει το δικό του ψηφιακό κλειδί πρόσβασης στον κοινό λογαριασμό. Τα πορτοφόλια αυτά επιλέγονται κυρίως από εταιρείες ώστε η πρόσβαση στο πορτοφόλι να γίνεται μόνο με την ταυτόχρονη εισαγωγή ψηφιακών κλειδιών από δύο ή τρεις χρήστες. Παράδειγμα είναι το BitGo, όπου ένα πρώτο κλειδί αποθηκεύεται από τον χρήστη, ένα δεύτερο κλειδί αποθηκεύεται από άτομο εμπιστοσύνης της εταιρείας και το τρίτο κλειδί διατηρείται από την ίδια την εταιρεία[77].

[75] Βλ. *Antonopoulos, A.*, ό.π., σελ. 6-7, *Jokić, S., AA et al.*, ό.π., σελ. 7, 68, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 18-19.
[76] Βλ. *Antonopoulos, A.*, ό.π., σελ. 6., *Jokić, S., AA et al.*, ό.π., σελ. 68, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 18.
[77] *Jokić, S., AA et al.*, ό.π., σελ. 67.

2) Οι χρήστες των **cold wallets** τα επιλέγουν προκειμένου να αποθηκεύσουν τα BTC τους για μεγάλο χρονικό διάστημα[78]. Στην κατηγορία αυτή περιλαμβάνονται: τα hardware wallet και τα paper wallet.

α) Το hardware wallet ή πορτοφόλι υλισμικού είναι μια εξιδεικευμένη συσκευή, που χρησιμοποιείται ως ένα ασφαλές και αυτόνομο πορτοφόλι Bitcoin. Μπορεί να συνδέεται μέσω θύρας USB με κάποιο browser, ή εναλλακτικά να διαθέτει οθόνη οπότε ο χρήστης δεν χρειάζεται υπολογιστή για να ολοκληρώσει μια συναλλαγή. Στη συσκευή δεν αποθηκεύονται τα BTC, αλλά το ψηφιακό ιδιωτικό κλειδί του χρήστη. Για τη λειτουργία του απαιτούνται δύο υπολογιστές, οι οποίοι μοιράζονται μέρη του ίδιου ψηφιακού πορτοφολιού. Ο πρώτος πρέπει να είναι εκτός σύνδεσης από οποιοδήποτε δίκτυο και περιέχει την εξουσιοδότηση για την υπογραφή της συναλλαγής. Ο δεύτερος υπολογιστής έχει σύνδεση με το διαδίκτυο και χρησιμοποιεί το ψηφιακό πορτοφόλι αποκλειστικά και μόνο για να παρακολουθεί και να μπορεί να δημιουργεί συναλλαγές, αλλά χωρίς υπογραφή. Με τον τρόπο αυτό εξασφαλίζεται μεγαλύτερη ασφάλεια[79]. Τα μειονεκτήματα που παρουσιάζουν είναι κυρίως η δυσκολία στη χρήση τους και το κόστος τους.

β) Το paper wallet ή χάρτινο πορτοφόλι είναι το ασφαλέστερο πορτοφόλι που υπάρχει. Δεν αντιμετωπίζει τα προβλήματα που δημιουργούνται στους άλλους τύπους πορτοφολιών, την απώλεια των κλειδιών λόγω δυσλειτουργίας του υπολογιστή ή καταστροφής του σκληρού δίσκου, ή κλοπής ή διαγραφής ή ακόμη λόγω κακόβουλων επιθέσεων και απειλών. Στην πράξη πρόκειται για την αποτύπωση του της διεύθυνσης και του ιδιωτικού κλειδιού σε έντυπη μορφή. Τα χάρτινα πορτοφόλια βγαίνουν σε πολλά σχήματα, μεγέθη και σχέδια, ο δε όρος «χάρτινο» έχει ευρύτερη έννοια και περιλαμβάνει εκτυπώσεις και σε άλλα υλικά, όπως ξύλο, μέταλλο, πλαστικό κλπ. Το μειονέκτημα του χάρτινου πορτοφολιού είναι ότι αυξάνει το χρόνο εκπλήρωσης μιας συναλλαγής και ότι τα τυπωμένα κλειδιά μπορούν πολύ εύκολα να κλαπούν[80].

[78] *Ibid* σελ. 67-68.
[79] Βλ. *Antonopoulos, A.*, ό.π., σελ. 6, *Jokić, S., AA et al.*, ό.π., σελ. 69, 72, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 19.
[80] Βλ. *Μούζουλας, Σ.* σελ.1183, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 497, *Antonopoulos, A.*, ό.π., σελ. 88, *Jokić, S., AA et al.*, ό.π., σελ. 69.

❖ **Ανάλογα με το ποσοστό αυτονομίας**

Τα πορτοφόλια διακρίνονται σε τρεις κατηγορίες λογισμικού[81]: Full Client, Lightweight Client και Web Client, ανάλογα με το ποσοστό αυτονομίας του πορτοφολιού, με την αλληλεπίδραση με το δίκτυο Bitcoin και με τον έλεγχο που ο χρήστης θέλει να έχει στα χρήματά του.

α) Ο Full Client αποθηκεύει την ιστορία όλων των συναλλαγών που έχουν πραγματοποιηθεί στο δίκτυο Bitcoin, έχει λειτουργίες για δημιουργία και διαχείριση του πορτοφολιού για τους χρήστες και μπορεί να κάνει συναλλαγές απευθείας στο δίκτυο του Bitcoin. Παρουσιάζει ομοιότητες με έναν αυτόνομο διακομιστή ηλεκτρονικού ταχυδρομείου στο ότι χειρίζεται τις πτυχές του πρωτοκόλλου, χωρίς να στηρίζεται σε οποιοδήποτε άλλο διακομιστή ή υπηρεσίες τρίτων. Ένας Full Client προσφέρει το υψηλότερο επίπεδο ελέγχου και ανεξαρτησίας, αλλ' όμως μεταφέρει στο χρήστη την ευθύνη των αντιγράφων ασφαλείας.

β) Ο Lightweight Client αποθηκεύει μόνο το πορτοφόλι του χρήστη και όχι το πλήρες αντίγραφο όλων των συναλλαγών, με αποτέλεσμα για την επικύρωση μιας συναλλαγής BTC να βασίζεται σε διακομιστές ιδιοκτησίας τρίτων.

γ) Ο Web Client είναι προσβάσιμος μέσω ενός browser. Το πορτοφόλι του χρήστη αποθηκεύεται σε ένα διακομιστή τρίτου. Ένας Web Client είναι μεν ο ευκολότερος στη χρήση, ενέχει όμως ο κίνδυνος της εξαπάτησης του χρήστη καθώς η ασφάλεια και ο έλεγχος γίνονται από κοινού από τον χρήστη και τον ιδιοκτήτη της διαδικτυακής υπηρεσίας.

2.1.2. Το περιεχόμενο του πορτοφολιού

Μια κοινή παρανόηση σχετικά με το Bitcoin είναι ότι τα πορτοφόλια περιέχουν μονάδες του νομίσματος BTC. Στην πραγματικότητα το κάθε πορτοφόλι είναι ένα αρχείο ή μια βάση δεδομένων ή αλυσίδες ή μια συλλογή διευθύνσεων και κλειδιών τα οποία παρέχουν την πρόσβαση στο λογαριασμό του χρήστη. Με την εκκίνηση του πορτοφολιού δημιουργούνται αυτόματα η διεύθυνση, το δημόσιο και το ιδιωτικό κλειδί. Κάθε BTC λοιπόν είναι ένα κρυπτογραφημένο κλειδί που αποτελείται από ένα δημόσιο και ένα ιδιωτικό μέρος[82].

[81] Βλ. *Antonopoulos, A.*, ό.π., σελ. 7-8.
[82] Βλ. *Μούζουλας, Σ.*, ό.π., σελ. 1183, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 497, *Antonopoulos, A.*, ό.π., σελ.10, 55, 93, *Swan, M.*, ό.π., σελ. 97, Chandel, S., AA et al. 2020. *A Multi-dimensional Adversary Analysis of RSA and*

Οι τεχνολογίες που χρησιμοποιούνται στα πορτοφόλια Bitcoin είναι ως επί το πλείστον φιλικές προς το χρήστη, ασφαλείς και ευέλικτες. Αφενός, το πορτοφόλι ελέγχει την πρόσβαση στα χρήματα ενός χρήστη, τη διαχείριση των κλειδιών και διευθύνσεων, την παρακολούθηση του υπολοίπου και τη δημιουργία και υπογραφή συναλλαγών. Αφετέρου, οι χρήστες ελέγχουν τα BTC, υπογράφοντας συναλλαγές με τα κλειδιά που έχουν στα πορτοφόλια τους. Συμπερασματικά, από τη σκοπιά ενός μεμονωμένου χρήστη, τα πιο σημαντικά στοιχεία, όσον αφορά στις συναλλαγές με BTC, είναι το πορτοφόλι, το ιδιωτικό κλειδί και η διεύθυνση του πορτοφολιού καθώς μέσω αυτών καθιερώνεται ο έλεγχος της κυριότητας των χρημάτων και η ιδιοκτησία πάνω σε κάποιο BTC[83].

2.2. Η δημιουργία της συναλλαγής

Μια συναλλαγή BTC είναι μία δομή δεδομένων που κωδικοποιεί τη μεταφορά αξίας από μία πηγή χρημάτων, που ονομάζεται είσοδος, προς έναν προορισμό που ονομάζεται έξοδος. Οι έξοδοι των συναλλαγών αυτών είναι αδιαίρετα ποσά BTC, τα οποία είναι κλειδωμένα σε συγκεκριμένο ιδιοκτήτη, μπορούν να ξεκλειδώσουν μόνο από αυτόν που έχει το κατάλληλο κλειδί, είναι καταγεγραμμένα στο Blockchain και αναγνωρίζονται ως νομισματικές μονάδες από ολόκληρο το δίκτυο[84].

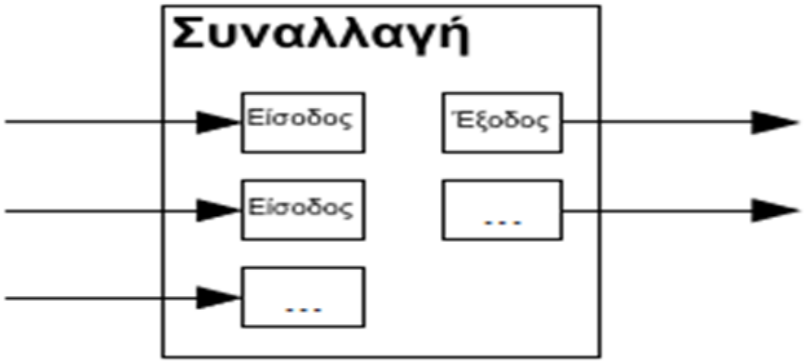
Οι συναλλαγές που γίνονται με BTC είναι κρυπτογραφημένες, ώστε αφενός να εξασφαλίζεται η ανωνυμία των συναλλασσόμενων και αφετέρου να επιλύεται το πρόβλημα των διπλών δαπανών. Η κρυπτογραφία στην οποία βασίζεται το BTC χρησιμοποιεί προηγμένες μαθηματικές συναρτήσεις για την αποθήκευση, τη μετατροπή και μετάδοση προσιτών δεδομένων σε μια κωδικοποιημένη μορφή. Τα δεδομένα μετασχηματίζονται με τέτοιο τρόπο, ώστε η ανάγνωσή τους να είναι εφικτή μόνο μέσω ενός κλειδιού

ECC in Blockchain Encryption. [online]. Future of Information and Communication Conference (FICC) 14-15 March 2019, San Francisco, USA. *In*: Arai, K., Bhatia, R. *Advances in Information and Communication*. pp. 988-1003, σελ. 989: Available at: http://dx.doi.org/10.1007/978-3-030-12385-7_67 (Accessed 26/01/2021), Ferrer-Gomila, J., AA et al., 2019. *A fair contract signing protocol with blockchain support. Electronic Commerce Research and Applications* [online]. Vol 36, July–August 2019, σελ. 2. Available at: https://www.sciencedirect.com/science/article/pii/S1567422319300468 (Accessed 27/01/2021).

[83] Βλ. *Antonopoulos, A.*, ό.π., σελ.7, 55, 93, *Swan, M.*, ό.π., σελ.3.

[84] *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 833, *Δελούκα-Ιγγλέση, Κ.*, 2005. Νομικά θέματα ηλεκτρονικού εμπορίου. Αθήνα: Α. Σάκκουλας, σελ. 157, Καράκωστας, Ι., 2009. *Δίκαιο & Internet: Νομικά ζητήματα του Διαδικτύου.* Αθήνα: Π. Σάκκουλας, σελ. 175, *Χρυσοχού, Χ.*, ό.π., σελ. 266, *Antonopoulos, A.*, ό.π., σελ. 18, 117, 119, *Belotti, M., AA et al.*, ό.π., σελ. 30, *Chandel, S., AA et al.*, ό.π., σελ. 989, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 16.

αποκρυπτογράφησης. Πάντως είναι παράδοξο ότι τα δεδομένα επικοινωνίας και συναλλαγών στο σύστημα Bitcoin δεν είναι κρυπτογραφημένα, ούτε και χρειάζεται να κρυπτογραφούνται για την προστασία των χρημάτων[85].



Εικόνα 2: Η συναλλαγή[86].

2.2.1. Η ασύμμετρη κρυπτογραφία

Ο Κανονισμός 428/2009[87] «περί κοινοτικού συστήματος ελέγχου των εξαγωγών της μεταφοράς, της μεσιτείας και της διαμετακόμισης ειδών διπλής χρήσης», περιέχει τον ορισμό της κρυπτογραφίας την οποία ορίζει ως: «τον κλάδο που συνδυάζει τις αρχές, τα μέσα και τις μεθόδους για την μετατροπή δεδομένων με σκοπό την απόκρυψη των πληροφοριών που περιέχουν, την πρόληψη της μη αντιληπτής τροποποίησής του ή της μη επιτρεπτής χρήσης του. Η «κρυπτογραφία» περιορίζεται στην μετατροπή πληροφοριών χρησιμοποιώντας μία ή περισσότερες 'μυστικές παραμέτρους' (π.χ. κρυπτομεταβλητές) ή σχετική διαχείριση κλειδιών».

Δύο είναι τα είδη της κρυπτογραφίας που συναντώνται, η συμμετρική και η ασύμμετρη. Η συμμετρική χρησιμοποιεί για την κωδικοποίηση και αποκωδικοποίηση ένα μυστικό-ιδιωτικό κλειδί, κοινό και για τους δύο χρήστες. Δηλαδή, για την ανταλλαγή ενός μηνύματος πρέπει και οι δύο να διαθέτουν εκ των προτέρων το ίδιο κλειδί κρυπτογράφησης και αποκρυπτογράφησης. Η ασύμμετρη κρυπτογραφία χρησιμοποιεί διαφορετικούς αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης μέσω ενός ζεύγους ψηφιακών

[85] Βλ. *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 16.
[86] Βλ. *Nakamoto, S.*, ό.π., σελ. 2.
[87] Κανονισμός (ΕΚ) αριθ. 428/2009. (05/052009). «*Περί κοινοτικού συστήματος ελέγχου των εξαγωγών της μεταφοράς, της μεσιτείας και της διαμετακόμισης ειδών διπλής χρήσης*». Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32009R0428 (Πρόσβαση 26/01/2021).

κλειδιών, ενός δημόσιου και ενός ιδιωτικού. Στη μέθοδο της ασύμμετρης κρυπτογράφησης στηρίζεται και η ψηφιακή υπογραφή[88].

2.2.1.1. Τα ψηφιακά κλειδιά και οι διευθύνσεις πορτοφολιών

Στο Bitcoin υιοθετείται η μέθοδος της ασύμμετρης κρυπτογραφίας. Η δημιουργία και διαχείριση των δυο ψηφιακών κλειδιών, ιδιωτικού και δημοσίου, γίνεται μέσα από το πορτοφόλι του χρήστη, χωρίς αυτά να αναφέρονται στο Blockchain ή να χρειάζονται πρόσβαση στο διαδίκτυο ή να βρίσκονται στη θέα των χρηστών.

α) Το ιδιωτικό κλειδί είναι ένας αριθμός τυχαία δημιουργημένος, χρησιμοποιείται ώστε να σφραγιστεί το ηλεκτρονικό μήνυμα και επιτρέπει στον κάτοχο την πρόσβαση στο ψηφιακό πορτοφόλι. Πρέπει να μένει πάντα μυστικό, διότι η τυχόν αποκάλυψή του σε τρίτους ισοδυναμεί με την παραχώρηση του απόλυτου ελέγχου των BTC που είναι ασφαλισμένα με αυτό το κλειδί. Μπορούν να υπάρχουν περισσότερα ιδιωτικά κλειδιά, τα οποία αποθηκεύονται στο πορτοφόλι και τα οποία σχετίζονται με όλες τις διευθύνσεις Bitcoin που δημιουργούνται για το πορτοφόλι αυτό.

β) Το δημόσιο κλειδί αποτελεί την διεύθυνση του προσώπου στο δίκτυο, αποστέλλεται μαζί με τα σχετικά προς αποκρυπτογράφηση δεδομένα και χρησιμοποιείται για την αποκρυπτογράφηση του μηνύματος. Στην ασύμμετρη κρυπτογραφία το δημόσιο κλειδί δημιουργείται από το ιδιωτικό κλειδί μέσω της χρήσης μιας μονόδρομης κρυπτογραφικής συνάρτησης.

Σε περίπτωση που το δημόσιο κλειδί χαθεί, η ανάκτησή του μπορεί να γίνει εύκολα, ενώ εάν χαθεί το ιδιωτικό κλειδί, χάνεται δια παντός η πρόσβαση στο πορτοφόλι. Είναι λοιπόν σημαντικό το ιδιωτικό κλειδί να διασφαλίζεται, να έχει αντίγραφο ασφαλείας και να προστατεύεται από τυχαία απώλεια. Το ιδιωτικό κλειδί προσομοιάζει με τον μυστικό κωδικό PIN ή με την υπογραφή σε βιβλιάριο τραπέζης που επιτρέπουν τον έλεγχο του λογαριασμού, το δε δημόσιο κλειδί προσομοιάζει με τον αριθμό του τραπεζικού λογαριασμού[89].

---

[88] Βλ. *Καραδημητρίου, Κ,.* 2006. Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο. Αθήνα–Θεσσαλονίκη: Εκδ. Σάκκουλα, σελ.36-37, *Καράκωστας, Ι.*, ό.π, σελ. 176, Μυλωνόπουλος, Χ., 2005. *Ποινικό Δίκαιο-Ειδικό μέρος: Τα εγκλήματα σχετικά με τα υπομνήματα (Άρθρ. 216-223 ΠΚ)*. Αθήνα: Π. Σάκκουλας, σελ. 33, *Jokić, S., AA et al.*, ό.π., σελ. 67.

[89] Βλ., *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 834, *Κεχαγιά, Χ.*, ό.π., σελ. 3,7, *Γεωργιάδης, Γ.*, 2003. Η σύναψη της σύμβασης μέσω του διαδικτύου. Αθήνα: Α. Σάκκουλας, σελ. 177, *Θεοδωράκης, Ν., Καλογεράκης Γ*, 2019. Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα : ιδίως, οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου. Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 16(1), σελ. 8-9, *Ιγγλεζάκης, Ι.*, 2008. Δίκαιο της Πληροφορικής, Β΄ έκδ. Αθήνα–Θεσσαλονίκη: Α. Σάκκουλας, σελ. 177, *Μυλωνόπουλος, Χ.,*

Μία διεύθυνση Bitcoin αποτελεί το ψηφιακό αποτύπωμα του δημοσίου κλειδιού και δημιουργείται μέσω αυτού, με τη χρήση μιας μονόδρομης συνάρτησης κατακερματισμού. Αποτελείται από μια αλφαριθμητική ακολουθία 24 έως 36 χαρακτήρων, που ξεκινούν με το ψηφίο «1»[90], αντιπροσωπεύει έναν πιθανό προορισμό για μια πληρωμή BTC και είναι η μοναδική αναπαράσταση από κλειδιά που βλέπουν οι χρήστες σε τακτική βάση, διότι αποτελεί το στοιχείο εκείνο, που προσδιορίζει τον αποστολέα ή τον παραλήπτη της συναλλαγής. Παράδειγμα διεύθυνσης Bitcoin[91]:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Η διεύθυνση χρησιμοποιείται για τη μεταφορά BTC από ένα άτομο προς ένα άλλο. Όλες οι συναλλαγές που καταχωρούνται στο σύστημα Bitcoin είναι συνδεδεμένες αποκλειστικά και μόνο με τις διευθύνσεις των χρηστών, έτσι ώστε να μην μπορεί να εξακριβωθεί η αληθινή ταυτότητα του κατόχου.

Δεν τίθεται όριο στον αριθμό των διευθύνσεων που μπορεί να δημιουργήσει ένας χρήστης, με αποτέλεσμα ένα πορτοφόλι να μπορεί να περιέχει πολλές διευθύνσεις. Όλες οι διευθύνσεις που ανήκουν στον ίδιο χρήστη θα κατευθύνουν τα χρήματα στο πορτοφόλι του. Με τον τρόπο αυτό επιτυγχάνεται μεγαλύτερη ιδιωτικότητα, καθώς για κάθε συναλλαγή μπορεί να χρησιμοποιηθεί μια διαφορετική διεύθυνση. Άπαξ και δημιουργηθεί μια διεύθυνση, δεν γίνεται γνωστή στο δίκτυο, δεν υπάρχει κάποιος λογαριασμός και κάποια συσχέτιση μεταξύ αυτής και κάποιου λογαριασμού, ούτε εγγράφεται σε κάποιο μέρος στο σύστημα αλλά για να γίνει γνωστή θα πρέπει να αναφερθεί ως αποδέκτης της αξίας σε μια συναλλαγή, η οποία δημοσιεύτηκε στο σύστημα. Μέχρι τότε, παραμένει μέρος του αριθμού των πιθανών διευθύνσεων που είναι έγκυρες στο Bitcoin[92].

ό.π., σελ. 33, *Antonopoulos, A.*, ό.π., σελ 55-58, 63, Gao, Y., AA et al. 2018. A Secure Cryptocurrency Scheme based on Post-Quantum Blockchain. *IEEE Access* [online]. 18 April, σελ. 1: Available at: https://ieeexplore.ieee.org/document/8340794 (Accessed 26/01/2021), *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 21.

[90] Βλ. *Antonopoulos, A.*, ό.π., σελ. 64, Μπορούν επίσης να ξεκινούν και με το ψηφίο «3» σε συγκεκριμένες περιπτώσεις που δεν άπτονται της συγκεκριμένης ανάλυσης.

[91] Διαθέσιμό στο:https://www.blockchain.com/btc/address/1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa?page=31

[92] Βλ. *Κεχαγιά, Χ.*, ό.π., σελ. 3-4, *Antonopoulos, A.*, ό.π., σελ. 10, 56-58, 65, *Chandel, S., AA et al*, ό.π., σελ. 990, *Ghimire, H., Selvaraj, H.*, ό.π., σελ. 2-3, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 15, 21, *Swan, M.*, ό.π., σελ. 97-98

2.2.1.2. Η ψηφιακή υπογραφή

Η ψηφιακή υπογραφή αξιοποιεί τις μαθηματικές αρχές της ασύμμετρης κρυπτογραφίας, δημιουργώντας μια κλειδωμένη, ηλεκτρονική σύντμηση του ηλεκτρονικού εγγράφου που υποκαθιστά την παραδοσιακή υπογραφή και αποτελεί την απόδειξη ότι τα μέρη συμφωνούν στην πραγματοποίηση της συναλλαγής. Οι πληροφορίες μαζί με την ψηφιακή υπογραφή αποτελούν τη συναλλαγή, που θα ενσωματωθεί μαζί με άλλες συναλλαγές στο οικείο μπλοκ της αλυσίδας[93].

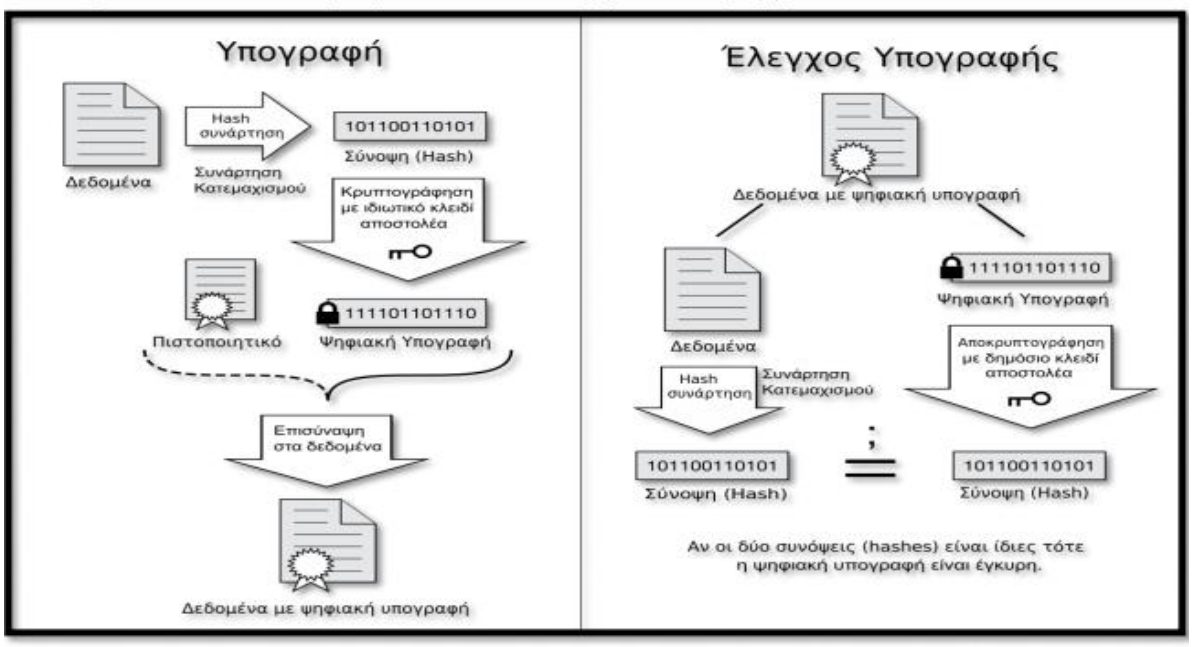
Για τη δημιουργία και επαλήθευση μιας ψηφιακής υπογραφής ακολουθείται μια συγκεκριμένη διαδικασία διαδοχικών σταδίων που το καθένα αποτελεί προϋπόθεση για το επόμενο. Έτσι λοιπόν, για την αποστολή εκτενούς κειμένου δεν κρυπτογραφείται ολόκληρη η συναλλαγή, αλλά δημιουργείται το λεγόμενο δακτυλικό αποτύπωμα, το οποίο είναι μια σύνοψη του συνόλου της συναλλαγής. Το δακτυλικό αποτύπωμα προκύπτει από την εφαρμογή μιας συνάρτησης-αλγόριθμου κατακερματισμού. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί είναι μια συγκεκριμένου μήκους σειρά αριθμητικών ψηφίων. Ο αλγόριθμος που χρησιμοποιείται είναι εξαιρετικά ευαίσθητος σε μεταβολές, που γίνονται στο αρχικό κείμενο και έτσι είναι πρακτικά αδύνατο να βρεθούν δυο κείμενα από τα οποία να παράγεται η ίδια σύντμηση. Το νέο συντετμημένο κείμενο (δακτυλικό αποτύπωμα) κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα και το νέο αυτό μήνυμα που προκύπτει αποτελεί την ψηφιακή υπογραφή[94].

Στον αντίποδα, ο παραλήπτης, λαμβάνει την ψηφιακή υπογραφή, το δημόσιο κλειδί του αποστολέα και την εκτενή συναλλαγή που αποτελεί το μήνυμα. Για την επαλήθευση της υπογραφής, ο παραλήπτης αφενός προχωρεί σε σύνοψη της μεταβιβαζόμενης συναλλαγής και αφετέρου με το δημόσιο κλειδί αποκρυπτογραφεί το δακτυλικό αποτύπωμα. Αν τα δύο δακτυλικά αποτυπώματα που προκύπτουν ταυτίζονται, τότε δεν έχει εμφιλοχωρήσει καμία αλλοίωση. Έτσι, η επιτυχής λειτουργία του μηχανισμού αποκρυπτογράφησης της ηλεκτρονικής υπογραφής, σε συνδυασμό με το γεγονός ότι το απόρρητο υλικό παραγωγής της προηγμένης ηλεκτρονικής υπογραφής χρησιμοποιείται μόνο από τον χρήστη, οδηγεί στο συμπέρασμα ότι η συναλλαγή είναι γνήσια και δημιουργεί μαχητό τεκμήριο σχετικά με την

[93] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 221, *Δελούκα-Ιγγλέση, Κ.*, ό.π., σελ. 159, *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 9, , *Μυλωνόπουλος, Χ.*, ό.π., σελ. 33, *Χρυσοχού, Χ.*, ό.π., σελ. 267, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 21

[94] Βλ. *Γεωργιάδης, Γ.*, ό.π., σελ. 177, *Δελούκα-Ιγγλέση, Κ.*, ό.π., σελ. 159, *Ιγγλεζάκης, Ι.*, ό.π., σελ. 177, *Καραδημητρίου, Κ.*, ό.π., σελ. 50, *Μυλωνόπουλος, Χ.*, ό.π., σελ. 33.

γνησιότητα της ηλεκτρονικής υπογραφής. Η διαδικασία αυτή πρακτικά σημαίνει ότι η ψηφιακή υπογραφή σε αντίθεση με την ιδιόχειρη είναι διαφορετική για κάθε μήνυμα παρόλο που δημιουργείται πάντα από το ίδιο ιδιωτικό κλειδί[95]. Η παραπάνω διαδικασία μπορεί να αποτυπωθεί σχηματικά ως εξής:



Εικόνα 3: Διαδικασία ασύμμετρης κρυπτογραφίας[96].

Μια ψηφιακή υπογραφή[97] εξυπηρετεί ορισμένους σκοπούς, δηλαδή αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα και μη αποποίηση ευθύνης εκάστου μεταδιδόμενου μηνύματος. Αρχικά, πιστοποιείται η αυθεντικότητα της ταυτότητας του συγκεκριμένου συναλλασσόμενου, καθόσον τα άτομα που συναλλάσσονται και επικοινωνούν μπορεί να είναι άγνωστα μεταξύ τους. Αποδεικνύεται λοιπόν ότι ο

[95] Βλ. *Ιγγλεζάκης, Ι.*, ό.π., σελ. 441, *Μανιώτης, Δ*, 2004. Ζητήματα από την ηλεκτρονική κατάρτιση των δικαιοπραξιών. Πρακτικά Συνεδρίου με θέμα: Ψηφιακή τεχνολογία και Δίκαιο. Φορέας διεξαγωγής και συγγραφέας: Εταιρεία Νομικών Βορείου Ελλάδος 52. Αθήνα: ΕΚΔΟΣΕΙΣ ΣΑΚΚΟΥΛΑΣ, σελ. 21, *Antonopoulos, A.*, ό.π., σελ. 18-19, 139, *Nakamoto, S.*, ό.π., σελ. 2,.

[96] Βλ. *Πηγή Wikipedia.*

[97] Ν. 4727/2020 «*Ψηφιακή Διακυβέρνηση (ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις»*, Αρ.2.στοιχ.49:
«Προηγμένη ηλεκτρονική υπογραφή: ηλεκτρονική υπογραφή που πληροί τις ακόλουθες απαιτήσεις: α) συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα, β) είναι ικανή να ταυτοποιεί τον υπογράφοντα, γ) δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής υπογραφής τα οποία ο υπογράφων μπορεί, με υψηλό βαθμό εμπιστοσύνης, να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο, και δ) συνδέεται με τα δεδομένα που έχουν υπογραφεί σε σχέση με αυτή, κατά τρόπο ώστε να μπορεί να ανιχνευθεί οποιαδήποτε επακόλουθη τροποποίηση των εν λόγω δεδομένων».

συναλλασσόμενος είναι ο ιδιοκτήτης του ιδιωτικού κλειδιού και εμμέσως είναι ο ιδιοκτήτης των BTC και έχει εγκρίνει την δαπάνη αυτών των κεφαλαίων. Στη συνέχεια, διαφυλάσσει το αναλλοίωτο του περιεχομένου του μηνύματος, αποδεικνύοντας ότι η συναλλαγή, ή συγκεκριμένα μέρη της συναλλαγής, δεν έχει και δεν μπορεί να τροποποιηθεί από κανέναν μετά την υπογραφή της, καθώς ο παραλήπτης πρέπει να είναι σίγουρος ότι λαμβάνει το μήνυμα ακριβώς όπως το απέστειλε ο αποστολέας. Έπειτα, εξασφαλίζει την εμπιστευτικότητα, που σημαίνει αφενός προστασία του αποστελλόμενου μηνύματος από πρόσβαση μη εξουσιοδοτημένων προσώπων και αφετέρου αδυναμία του εισβολέα να αναγνώσει το κείμενο. Τέλος, εξασφαλίζει την μη αποποίηση της ευθύνης, καθώς ο αποστολέας των δεδομένων δεν έχει την ευχέρεια να αρνηθεί ότι δημιούργησε και απέστειλε το ηλεκτρονικό μήνυμα και επομένως αποδεικνύεται ότι η έγκριση είναι αναμφισβήτητη[98].

2.2.1.3. Οι έξοδοι αξόδευτης συναλλαγής (UTXO)

Κάθε συναλλαγή περιέχει μία ή περισσότερες εισόδους, οι οποίες επί της ουσίας είναι χρεώσεις στο λογαριασμό και μία ή περισσότερες εξόδους, οι οποίες απεικονίζουν δαπανήσιμα κομμάτια BTC, που ονομάζονται έξοδοι αξόδευτων συναλλαγών ή Unspent Transaction Outputs (στο εξής UTXO). Οι UTXO παρακολουθούνται από κάθε πλήρη κόμβο, κρατούνται σε μία βάση δεδομένων και μπορούν να δαπανηθούν μόνο μια φορά. Κάθε φορά που ένας χρήστης λαμβάνει BTC, το ποσό αυτό καταγράφεται μόνιμα στο Blockchain ως UTXO και ως εκ τούτου είναι αμετάβλητη και ανεπηρέαστη από αποτυχημένες προσπάθειες ξοδέματός της[99]. Οι συναλλαγές λοιπόν αποτελούν μια αλυσίδα, όπου οι είσοδοι από την τελευταία συναλλαγή αντιστοιχούν σε εξόδους από προηγούμενες συναλλαγές, από τις οποίες θα δαπανηθούν μελλοντικά τα BTC. Άρα οι είσοδοι συναλλαγής είναι UTXO, που δεν έχουν ακόμη δαπανηθεί. Εξαίρεση στην αλυσίδα εξόδου και εισόδου είναι ένας ειδικός τύπος συναλλαγής, που ονομάζεται coinbase, και είναι η πρώτη συναλλαγή σε κάθε μπλοκ. Πρόκειται για μια ειδική συναλλαγή που δημιουργεί νέο νόμισμα. Η συναλλαγή αυτή λειτουργεί ως ανταμοιβή του κόμβου εξόρυξης για την

[98] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 9, *Καραδημητρίου, Κ.*, ό.π., σελ. 24-26, Σιδηρόπουλος, *Θ.*, 2008. *Το Δίκαιο του Διαδικτύου*, Β΄ έκδ.. Αθήνα–Θεσσαλονίκη: Α. Σάκκουλας, σελ. 106, *Belotti, M., AA et al.*, ό.π., σελ. 29-30, *Gao, Y., AA et al.*, ό.π., σελ. 1.
[99] Βλ. *Antonopoulos, A.*, ό.π., σελ. 119, 121.

ενσωμάτωση της συναλλαγής σε ένα μπλοκ και την τοποθέτησή της στο αρχείο συναλλαγών Blockchain[100].

Η UTXO είναι το θεμελιώδες δομικό στοιχείο μίας συναλλαγής Bitcoin καθώς εκχωρεί αξία σε ένα νέο ιδιοκτήτη, συνδέοντάς τη με ένα νέο κλειδί που αντιστοιχεί σε μια συγκεκριμένη δημόσια διεύθυνση Bitcoin και το οποίο δίνεται στον λήπτη, ενώ παράλληλα το κλειδί του μεταβιβάζοντος εξαφανίζεται. Με αυτόν τον τρόπο, κομμάτια αξίας BTC πηγαίνουν από χρήστη σε χρήστη σε μία αλυσίδα συναλλαγών.

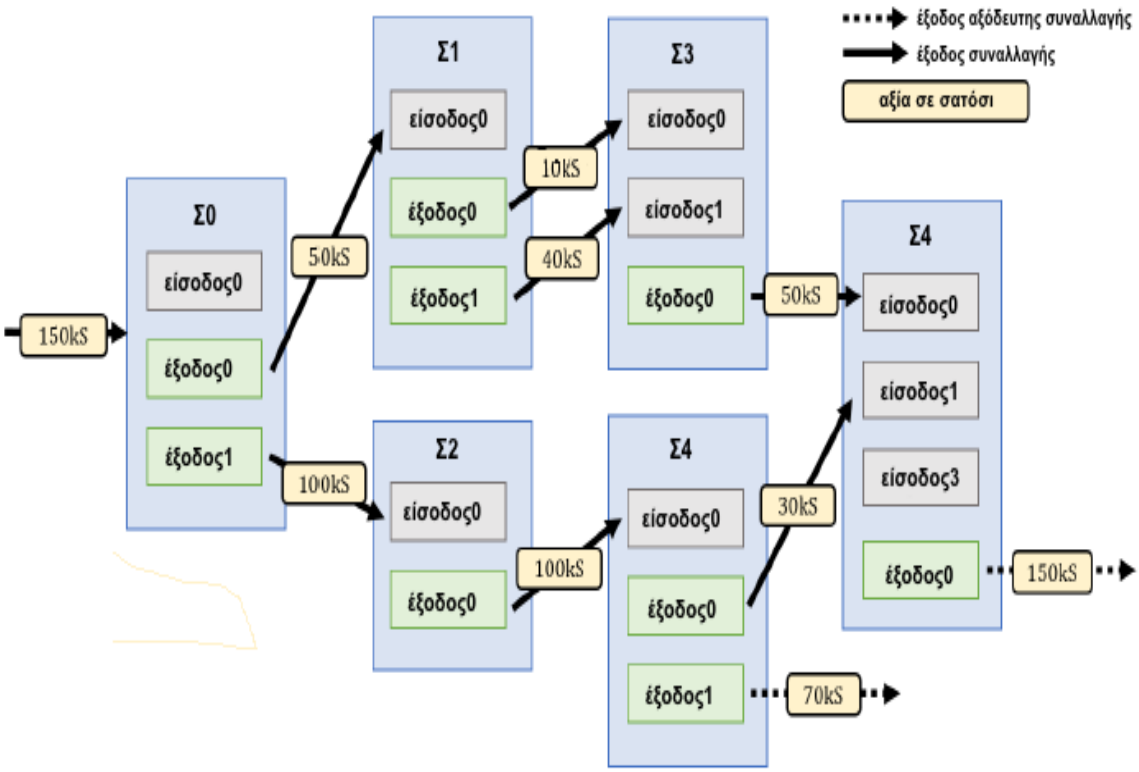
Οι UTXO μόλις δημιουργηθούν είναι αδιαίρετες και έχουν μία οποιαδήποτε τιμή στο εύρος των satoshi. Η εφαρμογή Bitcoin θα χρησιμοποιήσει πολλαπλές στρατηγικές για να καλύψει το ποσό της αγοράς. Είτε συνδυάζοντας αρκετές μικρότερες μονάδες, είτε βρίσκοντας τα ακριβή ποσά, είτε χρησιμοποιώντας μία μονάδα μεγαλύτερη από την αξία της συναλλαγής και δημιουργώντας επιστροφή ή αλλιώς ρέστα. Όλη αυτή η περίπλοκη συναρμολόγηση των UTXO γίνεται αυτόματα από το πορτοφόλι του χρήστη και είναι αόρατη στους χρήστες[101].

Μία εφαρμογή πορτοφολιού που λειτουργεί ως Full Client περιέχει ένα αντίγραφο της κάθε UTXO από κάθε συναλλαγή που έχει γίνει και βρίσκεται στο Blockchain. Επιτρέπει έτσι στο πορτοφόλι αφενός να κατασκευάζει εισόδους συναλλαγών και αφετέρου να επαληθεύει γρήγορα τις εισερχόμενες συναλλαγές ως σωστές εισόδους. Τα πορτοφόλια που λειτουργούν ως Lightweight Client είτε παρέχουν άμεση πρόσβαση μόνο στις αξόδευτες εξόδους του χρήστη είτε ανακτούν τις UTXO, έπειτα από αίτημα του χρήστη. Η έννοια «του υπολοίπου πορτοφολιού ενός χρήστη» αποτελεί λοιπόν κατασκεύασμα των εφαρμογών πορτοφολιού, καθώς επί της ουσίας δεν υπάρχει αποθηκευμένο υπόλοιπο BTC, αλλά διάσπαρτες UTXO, οι οποίες είναι κλειδωμένες σε συγκεκριμένους ιδιοκτήτες. Το πορτοφόλι ενός χρήστη όταν λαμβάνει BTC πρακτικά αναγνωρίζεται ως μια UTXO, η οποία μπορεί να ξοδευτεί με ένα από τα κλειδιά που ελέγχονται από το συγκεκριμένο πορτοφόλι. Τα BTC λοιπόν κάποιου χρήστη μπορεί να βρίσκονται διάσπαρτα ως UTXO, ανάμεσα σε

[100] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 835, *Antonopoulos, A.*, ό.π., σελ. 18, 93, 119, 121, *Belotti, M., AA et al.*, ό.π., σελ. 30, *Ferrer-Gomila, J., AA et al.*, ό.π., σελ. 2, *Gao, Y., AA et al.*, ό.π., σελ. 2, Pérez-Solà, S., AA et al., 2019. *Another coin bites the dust: an analysis of dust in UTXO-based cryptocurrencies*, σελ. 3. Available at: https://royalsocietypublishing.org/doi/10.1098/rsos.180817 (Accessed 26/01/2021), *Nakamoto, S.*, ό.π., σελ. 4.

[101] Βλ. *Antonopoulos, A.*, ό.π., σελ. 24, 120, *Belotti, M., AA et al.* ό.π., σελ. 3, 30, *Pérez-Solà, S., AA et al.*, ό.π., σελ. 2, Vallois, V., Guenane, F., 2017. *Bitcoin transaction: From the creation to validation, a protocol overview [online]. 1st Cyber Security in Networking Conference* 2017. Brazil. Oct. 18-20 October 2017, σελ. 67. Available at:https://www.researchgate.net/publication/322201810_Bitcoin_transaction_From_the_creation_to_validationa_protocol_overview (Accessed 28/01/2001).

εκατοντάδες συναλλαγών και εκατοντάδες μπλοκ. Το άθροισμα όλων των UTXO που ξεκλειδώνει μια συγκεκριμένη διεύθυνση υποδεικνύει το υπόλοιπο του πορτοφολιού, ενώ το άθροισμα όλων των UTXO που υπάρχουν στο σύστημα αντιπροσωπεύουν τον αριθμό όλων των BTC που κυκλοφορούν[102].



Εικόνα 4: Παράδειγμα UTXO[103].

2.3. Η μετάδοση της συναλλαγής μέσω του δικτύου Peer-to-Peer

Μια συναλλαγή, αν και δεν χρειάζεται να κατασκευαστεί και να υπογραφεί ενώ είναι εντός σύνδεσης, εντούτοις προκειμένου να γίνει τμήμα του κατανεμημένου αρχείου συναλλαγών, πρέπει να διαβιβαστεί στο δίκτυο του Bitcoin. Η διαβίβαση αυτή μπορεί να

[102] Βλ. *Antonopoulos, A.*, ό.π., σελ. 22, 119, *Belotti, M., AA et al.*, ό.π., σελ. 30, *Ferrer-Gomila, J., AA et al.*, ό.π., σελ. 2, *Vallois, V., Guenane, F.* ό.π., σελ. 67.
[103] Βλ. Βλ. *Belotti, M., AA et al.* ό.π., σελ. 31.

γίνει μέσω οποιουδήποτε δικτύου ακόμα και μη ασφαλούς[104], όπως Wi-Fi, Bluetooth, barcode, δορυφορική μετάδοση, να σταλεί ως μήνυμα κειμένου, μήνυμα συνομιλίας Skype, ακόμη και να κωδικοποιηθεί ως emoticons[105].

Το Bitcoin είναι ένα Peer-to-Peer[106] (στο εξής P2P) ανθεκτικό, αποκεντρωμένο και ανοιχτό σύστημα μετρητών, αποτελείται από κόμβους και επιτρέπει σε δύο ή περισσότερους από αυτούς να μοιράζονται τους πόρους τους ισοδύναμα. Ο όρος P2P, σημαίνει ότι οι κόμβοι που συμμετέχουν στο δίκτυο συνδέονται απευθείας μεταξύ τους και είναι ομότιμοι, χωρίς να υπάρχει κάποιος κεντρικός διακομιστής ή ιεραρχία μέσα στο δίκτυο. Κόμβος καλείται κάθε σύστημα που συμμετέχει στο δίκτυο του Bitcoin εφαρμόζοντας το πρωτόκολλο Bitcoin, εκτελείται κυρίως από εθελοντές και επιχειρήσεις που δημιουργούν Bitcoin εφαρμογές και λειτουργεί ως διαχειριστής. Για παράδειγμα, κόμβος είναι ένας διακομιστής, μια εφαρμογή επιτραπέζιου υπολογιστή ή ένα πορτοφόλι. Η συμβολή τους είναι πάρα πολύ μεγάλη, καθώς είναι οι υπεύθυνοι για την τήρηση, την ενημέρωση με νέες εγγραφές, την φύλαξη μέρους ή και ολόκληρου του Blockchain. Οι κόμβοι δεν χρειάζεται να εμπιστεύονται τον αποστολέα, ούτε χρειάζεται να προσκομίσουν ή να λάβουν κάποια ταυτότητα ως διαπιστευτήριο. Το πιο σημαντικό λοιπόν στάδιο στη μετάδοση της συναλλαγής είναι αυτή να μεταφερθεί με οποιονδήποτε τρόπο στον πρώτο κόμβο, ενώ δεν είναι απαραίτητο οι συναλλαγές να φτάσουν σε όλους τους κόμβους[107].

Η συναλλαγή διαδίδεται ταχέως ανάμεσα σε όλο το P2P δίκτυο, επιτυγχάνοντας τη σύνδεση με ένα μεγάλο ποσοστό των κόμβων, μέσα σε λίγα δευτερόλεπτα. Στην πράξη, όταν μια συναλλαγή Bitcoin αποστέλλεται σε οποιοδήποτε κόμβο, πρέπει πρώτα να εγκριθεί από αυτόν τον κόμβο. Εάν είναι έγκυρη, ο κόμβος θα τη διαδώσει σε άλλους κόμβους με τους οποίους είναι συνδεδεμένος και συγχρόνως θα επιστρέψει ένα μήνυμα επιτυχίας στον δημιουργό της συναλλαγής. Αν είναι άκυρη, ο κόμβος θα την απορρίψει και θα επιστρέψει ένα μήνυμα απόρριψης. Με τον τρόπο αυτό διασφαλίζεται ότι μόνο οι νόμιμες συναλλαγές επαληθεύονται και καταγράφονται σε ένα υποψήφιο μπλοκ και επομένως και στο

[104] Το αντίθετο συμβαίνει με τις συναλλαγές πιστωτικών καρτών, οι οποίες περιέχουν ευαίσθητες πληροφορίες και μπορούν να μεταδοθούν μόνο σε κρυπτογραφημένα δίκτυα.
[105] Βλ. *Antonopoulos, A.*, ό.π., σελ. 22, 25.
[106] Το πιο γνωστό παράδειγμα μιας αρχιτεκτονικής P2P δικτύου ήταν το Διαδίκτυο στην πρώιμη του κατάσταση, όπου οι κόμβοι στο IP δίκτυο ήταν ισάξιοι. Επιπλέον, μια ακόμη μεγάλη και επιτυχημένη εφαρμογή της P2P τεχνολογίας είναι ο διαμοιρασμός αρχείων με BitTorrent, *Antonopoulos, A.*, ό.π., σελ. 171.
[107] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 221, *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 7, *Κεχαγιά, Χ.*, ό.π., σελ. 3, *Παπαδοπούλου, Α., ό.π.,* σελ. 213, *Antonopoulos, A.*, ό.π., σελ. 25, *Nakamoto, S.*, ό.π., σελ. 4.

Blockchain. Οι κόμβοι τηρούν ολόκληρο το ιστορικό συναλλαγών για κάθε μεμονωμένο BTC, δίνοντας τη δυνατότητα να ευρεθεί το ιστορικό των κατόχων, οι μεταβιβάσεις που έγιναν και ο,τιδήποτε αφορά το συγκεκριμένο νόμισμα[108].

2.3.1. Η διαδικασία εύρεσης των ομότιμων κόμβων

Όταν ένας νέος κόμβος εκκινεί, προκειμένου να συμμετάσχει στο δίκτυο, πρέπει πρώτα να ανακαλύψει τουλάχιστον έναν υπάρχοντα κόμβο και να συνδεθεί μαζί του[109]. Η γεωγραφική τοποθεσία των κόμβων δεν έχει σημασία, καθώς η τοπολογία του δικτύου Bitcoin δεν προσδιορίζεται γεωγραφικά. Οι κόμβοι Bitcoin επιλέγονται τυχαία με την εκκίνηση του P2P. Μόλις μία ή περισσότερες συνδέσεις εγκαθιδρυθούν, ο νέος κόμβος αποστέλει ένα μήνυμα με τη δική του διεύθυνση IP στους κόμβους με τους οποίους συνδέεται και αυτοί με τη σειρά τους προωθούν αυτό το μήνυμα στους κόμβους με τους οποίους συνδέονται, διασφαλίζοντας ότι ο νέος συνδεδεμένος κόμβος γίνεται ευρύτερα γνωστός. Επιπρόσθετα, ο νέος συνδεδεμένος κόμβος μπορεί να αποστείλει μήνυμα σε όλους τους συνδεδεμένους με αυτόν κόμβους, ζητώντας να του αποστείλουν μία λίστα των IP διευθύνσεων άλλων ομότιμων κόμβων. Με αυτόν τον τρόπο, ένας κόμβος βρίσκει ομότιμους κόμβους για να συνδεθεί και να κάνει εμφανή την παρουσία του στο δίκτυο. Είναι σημαντικό ο κόμβος να συνδεθεί με αρκετούς διαφορετικούς ομότιμους κόμβους, ώστε να εγκαθιδρύσει πολλές διαφορετικές διαδρομές στο δίκτυο Bitcoin. Οι κόμβοι μπορούν να αποχωρήσουν και να επανέλθουν στο δίκτυο κατά βούληση. Για το λόγο αυτό ο κάθε κόμβος πρέπει συνεχώς να ανακαλύπτει νέους κόμβους και να βοηθάει άλλους κόμβους όταν κάνουν εκκίνηση. Μετά την εκκίνηση, ένας κόμβος θα θυμάται τις πιο πρόσφατες επιτυχημένες συνδέσεις του με ομότιμους κόμβους, έτσι ώστε εάν κάνει επανεκκίνηση να μπορεί γρήγορα να επανιδρύει συνδέσεις με το προηγούμενό του δίκτυο. Κατά περιόδους, οι κόμβοι στέλνουν μήνυμα για να διατηρήσουν τη σύνδεση με τους κόμβους στους οποίους δεν υπάρχει κίνηση. Εάν ένας κόμβος δεν έχει επικοινωνήσει σε μία σύνδεση για πάνω από

[108] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 10, *Antonopoulos, A.*, ό.π., σελ. 25, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 1

[109] Υπάρχουν διάφοροι τρόποι για να βρει ένας κόμβος άλλους ομότιμους κόμβους. Ένας τρόπος είναι να στείλει αιτήματα σε Domain Name Server, χρησιμοποιώντας έναν αριθμό από διακομιστές DNS που παρέχουν μία στατική λίστα IP διευθύνσεων από Bitcoin κόμβους. Ο Bitcoin Client περιέχει ονόματα από πέντε διαφορετικούς DNS προέλευσης. Μετά την χρήση του αρχικού κόμβου προέλευσης για δημιουργία συστάσεων, θα γίνει αποσύνδεση από αυτόν και θα χρησιμοποιηθούν οι νέοι ομότιμοι κόμβοι που έχουν ανακαλυφθεί, Βλ.*Antonopoulos, A.*, ό.π, σελ. 177-178.

90 λεπτά, θεωρείται ότι είναι αποσυνδεδεμένος και θα αναζητηθεί ένας νέος ομότιμος κόμβος. Έτσι, το δίκτυο μπορεί να προσαρμόζεται δυναμικά σε προβλήματα δικτύου και παροδικών κόμβων[110].

Η πρώτη ενέργεια ενός «πλήρους» κόμβου, που θα συνδεθεί με τους ομότιμους κόμβους, είναι η κατασκευή ολόκληρου του Blockchain. Ο καινούργιος κόμβος γνωρίζει μόνο το πρώτο μπλοκ που δημιουργήθηκε ποτέ και το οποίο είναι στατικά ενσωματωμένο στο Bitcoin Client. Ξεκινώντας με το μπλοκ No 0, ο νέος κόμβος θα πρέπει να κάνει λήψη εκατοντάδων χιλιάδων μπλοκ για να συγχρονιστεί με το δίκτυο και να δημιουργήσει την πλήρη Blockchain. Η διαδικασία ξεκινά με την αποστολή ενός μηνύματος, που αποσκοπεί στην αναζήτηση του τωρινού ύψους (αριθμού) των μπλοκ ενός κόμβου. Ένας κόμβος θα λάβει τα μηνύματα από τους ομότιμους κόμβους του, τα οποία θα περιέχουν τον κατακερματισμό του μπλοκ που βρίσκεται στην κορυφή της τοπικής Blockchain. Έτσι, θα είναι σε θέση να συγκρίνει τον αριθμό αυτό με αυτόν των μπλοκ που έχει στη δική του αλυσίδα. Ο ομότιμος κόμβος, που έχει τη μακρύτερη αλυσίδα των μπλοκ, σημαίνει ότι έχει περισσότερα μπλοκ από τον άλλο κόμβο. Στην πράξη λοιπόν, ένας από τους ομότιμους κόμβους μπορεί να αναγνωρίσει ότι ο κατακερματισμός που έχει ληφθεί ανήκει σε ένα μπλοκ που δεν είναι στην κορυφή, αλλά σε ένα παλαιότερο μπλοκ, συμπεραίνοντας ότι η δική του αλυσίδα των μπλοκ είναι μακρύτερη από τους ομότιμους κόμβους του. Έτσι μπορεί να αναγνωρίσει ποια μπλοκ χρειάζεται ο άλλος κόμβος μέχρι να φτάσει στο ίδιο ύψος με το άλλο μπλοκ.

Η διαδικασία σύγκρισης της τοπικής αλυσίδας των μπλοκ με τους ομότιμους κόμβους και η ανάκτηση των μπλοκ που υπολείπονται, δεν συμβαίνει μόνο την πρώτη φορά που ένας κόμβος θα συνδεθεί στο δίκτυο, αλλά κάθε φορά που ένας κόμβος βρίσκεται εκτός σύνδεσης για κάποια χρονική περίοδο. Είτε ένας κόμβος έχει βρεθεί εκτός σύνδεσης για κάποια λεπτά και υπολείπεται μερικά μπλοκ, είτε ένα μήνα και υπολείπεται μερικές χιλιάδες μπλοκ, με την επανεκκίνησή του, η πρώτη ενέργεια που θα κάνει είναι να στείλει μήνυμα για να κάνει λήψη των υπολειπόμενων μπλοκ[111].

2.3.2. Πλήρεις κόμβοι και Κόμβοι απλοποιημένης επαλήθευσης πληρωμών (SPV)

[110] Βλ. *Antonopoulos, A.*, ό.π., σελ. 171, 176, 178, 180, *Nakamoto, S.*, ό.π., σελ. 1
[111] Βλ. *Antonopoulos, A.*, ό.π., σελ. 181-182.

Οι κόμβοι μπορεί να αναλάβουν διαφορετικούς ρόλους με βάση τη λειτουργικότητα που υποστηρίζουν, χωρίς όμως αυτό να σημαίνει ότι παύουν να είναι ισάξιοι. Έτσι ένας κόμβος μπορεί να πραγματοποιεί τις εξής λειτουργίες: δρομολόγηση, βάση δεδομένων Blockchain, εξόρυξη και υπηρεσίες πορτοφολιού. Όλοι οι κόμβοι περιλαμβάνουν λειτουργία δρομολόγησης για να συμμετέχουν στο δίκτυο, καθώς όλοι οι κόμβοι εγκρίνουν και διαδίδουν συναλλαγές και μπλοκ, ανακαλύπτοντας και διατηρώντας συνδέσεις με ομότιμους κόμβους. Μπορούν παράλληλα να περιλαμβάνουν και κάποια από τις άλλες λειτουργίες. Στο σημείο αυτό θα εξετάσουμε τους κόμβους ανάλογα με το αν διατηρούν ολόκληρο και ενημερωμένο αντίγραφο του Blockchain. Οι κατηγορίες που υπάρχουν είναι δύο, οι Full Nodes ή Πλήρεις κόμβοι και οι Simplified Payment Verification Nodes ή Κόμβοι Απλοποιημένης Επαλήθευσης Πληρωμών (στο εξής SPV).

α) Οι πλήρεις κόμβοι διατηρούν ένα ολοκληρωμένο και ενημερωμένο με όλες τις συναλλαγές αντίγραφο Blockchain. Ένας πλήρης κόμβος μπορεί να εγκρίνει οποιαδήποτε συναλλαγή ανεξάρτητα και εξουσιοδοτημένα, χωρίς να καταφεύγει ή να εξαρτάται από οποιοδήποτε άλλο κόμβο και πηγή πληροφοριών. Για παράδειγμα, έστω ότι ένας πλήρης κόμβος εξετάζει τη συναλλαγή στο μπλοκ No 500000. Τότε συνδέει και τα 500000 μπλοκ μέχρι να φτάσει στο μπλοκ No 0, χτίζοντας μία πλήρη βάση δεδομένων από UTXO και κατοχυρώνοντας την εγκυρότητα της συναλλαγής, αφού πρώτα επιβεβαιώσει ότι η UTXO παραμένει αξόδευτη.

β) Οι SPV κατά τη σύνδεσή τους στο δίκτυο, δεν κάνουν λήψη ολόκληρου του Blockchain, αλλά διατηρούν το αντίγραφο μόνο των κεφαλίδων των μπλοκ της μακρύτερης αλυσίδας του Blockchain και επαληθεύουν τις συναλλαγές χρησιμοποιώντας μία μέθοδο που ονομάζεται απλοποιημένη επαλήθευση πληρωμών. Εξυπηρετούνται από τους πλήρεις κόμβους, ώστε να μπορέσουν να επαληθεύσουν τις πληροφορίες της συναλλαγής που τους ενδιαφέρει. Η μέθοδος αυτή χρησιμοποιείται σε συσκευές με περιορισμένο χώρο και ενέργεια, όπως επί παραδείγματι smartphone και tablet. Το Blockchain, που προκύπτει χωρίς συναλλαγές, είναι 1000 φορές μικρότερο από το πλήρες[112].

[112] Βλ. Annison, T., 2018. *Bloom Filters and SPV nodes within the bitcoin blockchain.* Available at: https://tara-annison.medium.com/bloom-filters-and-spv-nodes-within-the-bitcoin-blockchain-66c36ea673f2 (Accessed 29/02/2021), *Antonopoulos, A.*, ό.π., σελ. 183, *Belotti, M., AA et al.*, ό.π., σελ. 3, Matetic, S., AA et al., 2019. *BITE: Bitcoin Lightweight Client Privacy using Trusted Execution*, σελ. 3. Available at: https://www.usenix.org/system/files/sec19fall_matetic_prepub.pdf (Accessed 27/01/2021), *Nakamoto, S.*, ό.π., σελ. 5.

Οι κόμβοι SPV παρουσιάζουν διάφορες αδυναμίες. Μια αδυναμία είναι ότι δεν μπορούν να αποδείξουν ότι η UTXO είναι αξόδευτη και γι' αυτό είναι ευάλωτοι σε επιθέσεις διπλοξοδέματος. Σύμφωνα με το προηγούμενο παράδειγμα, έστω ότι ο SPV δημιουργεί μία σύνδεση[113] μεταξύ της συναλλαγής και του μπλοκ που την περιέχει και περιμένει μέχρι να δει τα έξι μπλοκ, από το No 500001 μέχρι το No 500006 που ακολουθούν το μπλοκ, στο οποίο περιλαμβάνεται η συναλλαγή. Δηλαδή απόδειξη ότι η συναλλαγή δεν ήταν διπλοξόδεμα αποτελεί το γεγονός ότι άλλοι κόμβοι στο P2P αποδέχτηκαν το μπλοκ No 500000 και έπειτα έκαναν τις απαραίτητες ενέργειες για να παράξουν έξι ακόμα μπλοκ μετά από αυτό.

Άλλες αδυναμίες των SPV είναι ότι δεν είναι σίγουροι ότι λαμβάνουν το σύνολο των συναλλαγών, με αποτέλεσμα η ύπαρξη μίας συναλλαγής να μπορεί να αποκρυφτεί από αυτούς, καθώς και ότι δεν μπορούν να επαληθεύσουν ότι μία συναλλαγή δεν υπάρχει. Θεωρητικά λοιπόν, μια συναλλαγή θα μπορούσε να αποκρυφτεί εάν ο SPV συνδεόταν με μια σειρά από ψεύτικους κόμβους και λάμβανε λανθασμένες πληροφορίες. Θα πρέπει λοιπόν οι πληροφορίες για τις συναλλαγές να ζητώνται από πολλούς και διαφορετικούς κόμβους καθώς έτσι αυξάνεται η πιθανότητα ο SPV να βρίσκεται συνδεδεμένος τουλάχιστον με έναν «έντιμο» κόμβο.

Η πιο σοβαρή αδυναμία που παρουσιάζουν οι SPV είναι ότι θέτουν σε κίνδυνο τα προσωπικά δεδομένα του χρήστη. Η επαλήθευση των συναλλαγών στηρίζεται στη συλλογή συγκεκριμένων δεδομένων και έτσι αποκαλύπτονται ακούσια οι διευθύνσεις που υπάρχουν στο πορτοφόλι. Ένας τρίτος λοιπόν που παρακολουθεί το δίκτυο μπορεί να συσχετίσει διευθύνσεις Bitcoin με τον χρήστη του συγκεκριμένου πορτοφολιού[114].

Για την αντιμετώπιση κάποιων από τις αδυναμίες που συναντώνται στους κόμβους SPV, δημιουργήθηκαν τα φίλτρα bloom. Μέσα από έναν μηχανισμό φιλτραρίσματος, που χρησιμοποιεί πιθανότητες αντί για σταθερά και καθορισμένα μοτίβα, τα φίλτρα bloom επιτρέπουν στους κόμβους να λαμβάνουν από τους ομότιμους κόμβους ένα υποσύνολο των συναλλαγών. Το φίλτρο bloom, που έχει δημιουργήσει ο SPV, θα φιλτράρει τις συναλλαγές αυτές, προκειμένου να βρει τις πληροφορίες που ταιριάζουν στις διευθύνσεις που κρατούνται στο πορτοφόλι του. Έτσι, ένα πιο εξειδικευμένο φίλτρο bloom θα παράξει

[113] Η σύνδεση αυτή γίνεται δημιουργώντας μια διαδρομή Merkle.

[114] Βλ. *Antonopoulos, A.*, ό.π., σελ. 183-184, Fyookball, J., 2017. *Why Every Bitcoin User Should Understand "SPV Security*". Available at https://medium.com/@jonaldfyookball/why-every-bitcoin-user-should-understand-spv-security-520d1d45e0b9 (Accessed 27/01/2021), *Matetic, S., AA et al.*, ό.π., σελ. 4.

ακριβή αποτελέσματα, αλλά με το κόστος της αποκάλυψης των διευθύνσεων που χρησιμοποιούνται στο πορτοφόλι του χρήστη, ενώ ένα λιγότερο ειδικό φίλτρο bloom θα παράξει περισσότερα δεδομένα σχετικά με περισσότερες συναλλαγές, πολλές εκ των οποίων είναι άνευ σημασίας για τον κόμβο. Με αυτόν τον τρόπο, διασφαλίζεται η διατήρηση του απορρήτου, χωρίς να γίνεται λήψη όλων των συναλλαγών από κάθε μπλοκ[115].

2.4. Η επιβεβαίωση της συναλλαγής

Με το που διεξάγεται μια συναλλαγή, είναι μεν άμεσα φανερή σε όλους, αλλ' όμως θεωρείται ότι είναι επιβεβαιωμένη, περιλαμβάνεται στο αρχείο συναλλαγών του Bitcoin και μπορεί να δαπανηθεί, μόνον εφόσον ενταχθεί σε ένα μπλοκ από έναν κόμβο εξόρυξης. Η επιβεβαίωση αυτή είναι εξέχουσας σημασίας καθώς διασφαλίζει ότι τα BTC είναι έγκυρα και δεν έχουν ήδη δαπανηθεί. Ο κάθε κόμβος εξόρυξης επιλέγει μια δέσμη συναλλαγών από την ομάδα μη επιβεβαιωμένων συναλλαγών και προσπαθεί να αποδείξει την εγκυρότητα του μπλοκ μέσα από μια διαδικασία που ονομάζεται εξόρυξη. Ενώ λοιπόν οι μεταφορές BTC μεταδίδονται στιγμιαία μέσω του δικτύου, στην πράξη η επιβεβαίωση μιας συναλλαγής γίνεται μετά από 10 λεπτά, καθώς τόσος είναι ο χρόνος που χρειάζεται για τη δημιουργία και την προσθήκη ενός μπλοκ στο Blockchain. Συνήθως, οι περισσότεροι χρήστες περιμένουν μια ώρα, δηλαδή περίπου έξι επιπλέον επιβεβαιώσεις προτού θεωρήσουν μια συναλλαγή ως επιβεβαιωμένη, καθώς κάθε μπλοκ που προστίθεται πάνω στο μπλοκ που περιέχει τη συναλλαγή κάποιου χρήστη αποτελεί μια πρόσθετη επιβεβαίωση, ενισχύοντας την εμπιστοσύνη στη συναλλαγή. Οποιοδήποτε μπλοκ με περισσότερες από έξι επιβεβαιώσεις θεωρείται ως αμετάκλητο, επειδή θα απαιτούνταν τεράστιο ποσό υπολογισμού για να ακυρωθούν και να υπολογιστούν εκ νέου έξι μπλοκ[116].

2.5. Ειδικές περιπτώσεις ομάδων συναλλαγών

Σε αυτές ανήκουν η ομάδα των ορφανών συναλλαγών και η ομάδα των μη επιβεβαιωμένων συναλλαγών. Η σειρά που καταφθάνουν οι συναλλαγές όταν μεταδίδεται

[115] Βλ. *Antonopoulos, A.*, ό.π., σελ. 185, 189, *Matetic, S., AA et al.*, ό.π., σελ. 3.
[116] Βλ. *Antonopoulos, A.*, ό.π., σελ. 26-27, 29, *Ghimire, H., Selvaraj, H.*, ό.π., σελ. 3-4, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 20, *Vallois, V., Guenane, F.*, ό.π., σελ. 64, *Γιαννόπουλος, Α.*, ό.π., σελ. 222, *Παρασκευόπουλος-Κόλιας, Χ.* σελ. 497.

μια αλυσίδα συναλλαγών στο δίκτυο δεν είναι ίδια. Όπως έχουμε ήδη αναφέρει παραπάνω, οι συναλλαγές σχηματίζουν μία αλυσίδα, στην οποία η μία συναλλαγή ξοδεύει τις UTXO της προηγούμενης. Η συναλλαγή αυτή καλείται μητρική και δημιουργεί εξόδους για μια επακόλουθη συναλλαγή, η οποία ονομάζεται παιδική.

α) Μερικές φορές, μία ολόκληρη αλυσίδα συναλλαγών, οι οποίες εξαρτώνται η μία από την άλλη, δημιουργείται την ίδια στιγμή με αποτέλεσμα έγκυρες παιδικές συναλλαγές να υπογράφονται πριν υπογραφεί η μητρική συναλλαγή. Ένας κόμβος που βλέπει πρώτα μία παιδική συναλλαγή μπορεί να δει και την μητρική στην οποία αναφέρεται. Αντί λοιπόν η παιδική συναλλαγή να απορριφθεί, τοποθετείται σε μία προσωρινή ομάδα, ώστε να αναμείνει την άφιξη της μητρικής της και έπειτα να διαδοθεί σε όλους τους κόμβους. Η ομάδα αυτή ονομάζεται ομάδα ορφανών συναλλαγών[117].

Η άφιξη της μητρικής συναλλαγής σηματοδοτεί μια αλληλουχία ανακατασκευής μίας ολόκληρης αλυσίδας από αλληλεξαρτώμενες συναλλαγές με την ένωση των ορφανών με τις μητρικές τους[118]. Ο μηχανισμός των ορφανών συναλλαγών διασφαλίζει αφενός, ότι δεν θα απορριφθούν έγκυρες συναλλαγές εξαιτίας καθυστέρησης της μητρικής τους και αφετέρου, ότι ανεξάρτητα από τη σειρά που καταφθάνουν, η αλυσίδα που τις περικλείει στο τέλος θα ανακατασκευαστεί με τη σωστή σειρά.

β) Επειδή το μέγεθος ενός μεμονωμένου μπλοκ είναι περιορισμένο, οι συναλλαγές πριν προστεθούν σε ένα μπλοκ αποθηκεύονται σε μια ομάδα, που ονομάζεται ομάδα μη επιβεβαιωμένων συναλλαγών ή ομάδα μνήμης,. Όταν μία συναλλαγή προστεθεί στην ομάδα αυτή, γίνεται πρώτα ο έλεγχος της ομάδας ορφανών συναλλαγών, ώστε να διαπιστωθεί εάν υπάρχουν ορφανές-παιδικές συναλλαγές που αναφέρονται στις UTXO αυτής της συναλλαγής και στη συνέχεια επαληθεύεται ποιες ορφανές ταιριάζουν. Εάν είναι έγκυρες, αφαιρούνται από την ομάδα των ορφανών και προστίθενται στην ομάδα των συναλλαγών, ολοκληρώνοντας την αλυσίδα που ξεκίνησε από την μητρική συναλλαγή.

Οι κόμβοι χρησιμοποιούν αυτήν την ομάδα για να παρακολουθούν τις συναλλαγές που είναι γνωστές στο δίκτυο, αλλά δεν έχουν περιληφθεί ακόμα στο Blockchain. Αφού ληφθούν και επαληθευτούν, οι συναλλαγές προστίθενται στην ομάδα συναλλαγών και μεταδίδονται

[117] Βλ. *Antonopoulos, A.*, ό.π., σελ. 192-193, Imtiaz, M. A., Starobinski, D. et Trachtenberg, A., 2020. *Characterizing Orphan Transactions in the Bitcoin Network* [online]. IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2020. Toronto, ON, Canada. 2-6 May 2020, σελ. 1. Available at: https://arxiv.org/pdf/1912.11541.pdf (Accessed 28/01/2021).

[118] Βλ. *Antonopoulos, A.*, ό.π., σελ. 192-193.

στους γειτονικούς κόμβους ώστε να διαδοθούν στο δίκτυο. Για παράδειγμα, ένας κόμβος που διατηρεί το πορτοφόλι ενός χρήστη θα χρησιμοποιήσει την ομάδα συναλλαγών για να παρακολουθήσει τις εισερχόμενες πληρωμές στο πορτοφόλι, γνωρίζοντας ότι οι πληρωμές έχουν ληφθεί στο δίκτυο χωρίς όμως να έχουν ακόμα επιβεβαιωθεί[119].

Συγκρίνοντας τις ομάδες ορφανών συναλλαγών και μη επιβεβαιωμένων συναλλαγών με την ομάδα UTXO, βρίσκουμε τρεις σημαντικές διαφορές[120]. Αμφότερες οι ομάδες των ορφανών συναλλαγών και των μη επιβεβαιωμένων συναλλαγών:

1) Αποθηκεύονται στην τοπική μνήμη και όχι σε κάποιο μόνιμο αποθηκευτικό χώρο. Άρα όταν ένας κόμβος κάνει εκκίνηση, οι δύο ομάδες είναι κενές και σταδιακά συμπληρώνονται από νέες συναλλαγές που λαμβάνονται από το δίκτυο. Αντίθετα, η ομάδα UTXO μπορεί να αποθηκευτεί ως βάση δεδομένων σε μόνιμο χώρο και έτσι κατά την εκκίνηση δεν διαμορφώνεται ως κενή, αλλά αντίθετα περιέχει εκατομμύρια καταχωρήσεις UTXO, φθάνοντας χρονικά ακόμα και σε συναλλαγές που έγιναν στο 2009.

2) Αντιπροσωπεύουν μόνο την οπτική ενός κόμβου και μπορούν να διαφέρουν σημαντικά από κόμβο σε κόμβο, καθώς εξαρτώνται από το πότε ο κόμβος έκανε εκκίνηση ή επανεκκίνηση. Από την άλλη μεριά, η ομάδα UTXO δεν διαφέρει ανάμεσα στους κόμβους, επειδή αντιπροσωπεύει την αναδυόμενη συναίνεση του δικτύου.

3) Περιέχουν μόνο μη επιβεβαιωμένες συναλλαγές, ενώ η ομάδα UTXO περιέχει μόνο επιβεβαιωμένες εξόδους συναλλαγών.

[119] Βλ. *Antonopoulos, A.*, ό.π., σελ. 192, *Ferrer-Gomila, J., AA et al.*, ό.π., σελ. 6, *Imtiaz, M. A., Starobinski, D. et Trachtenberg, A.*, ό.π., σελ. 1, *Vallois, V., Guenane, F.*, ό.π., σελ. 64.
[120] Βλ. *Antonopoulos, A.*, ό.π., σελ. 193, *Vallois, V., Guenane, F.*, ό.π., σελ. 64

ΚΕΦΑΛΑΙΟ 3ο
ΤΟ BITCOIN ΩΣ ΕΦΑΡΜΟΓΗ ΤΟΥ BLOCKCHAIN

Το Blockchain είναι η αναμφισβήτητα εφεύρεση του 21ου αιώνα. Περιγράφηκε το 1991, ως ανεξάρτητη εφαρμογή, από μια ομάδα ερευνητών και είχε αρχικά ως στόχο την χρονική σήμανση των ψηφιακών εγγράφων, έτσι ώστε να μην είναι δυνατή η προχρονολόγησή τους ή η αλλοίωση αυτών. Είναι το αποτέλεσμα του συνδυασμού κρυπτογραφίας, μαθηματικών, αλγόριθμων συναίνεσης και οικονομικών μοντέλων και αποτελεί την τεχνολογία που χρησιμοποιείται για τα προϊόντα που είναι διαθέσιμα στην αγορά. Αυτό πρακτικά σημαίνει ότι μπορεί οι άνθρωποι ακόμη και να αγνοούν ότι η τεχνολογία του Blockchain είναι πίσω από ένα προϊόν που αγοράζουν ή χρησιμοποιούν[121].

Το Blockchain αναγνωρίζεται ως ένα δημόσιο, κοινόχρηστο, αποκεντρωμένο, κατανεμημένο και συνεχώς αυξανόμενο καθολικό[122], που καταγράφει όλα τα δεδομένα συναλλαγών μέσα σε μπλοκ, με επαληθεύσιμο και μόνιμο τρόπο, διασφαλίζοντας την διαφάνεια, ακεραιότητα και ασφάλεια των δεδομένων. Με την αξιοποίηση των δικτύων P2P και των μηχανισμών συναίνεσης, επιλύεται το πρόβλημα του κατανεμημένου συγχρονισμού δεδομένων, καθιστώντας περιττή την ύπαρξη μιας κεντρικής αξιόπιστης αρχής. Τα μπλοκ συνδέονται προς τα «πίσω», με το κάθε ένα να αναφέρεται στο προηγούμενο μπλοκ δημιουργώντας με τον τρόπο αυτό μια αλυσίδα από μπλοκ. Η δομή δεδομένων της αλυσίδας των μπλοκ είναι μία ταξινομημένη, συνδεδεμένη προς τα πίσω λίστα των συναλλαγών. Η αλυσίδα των μπλοκ μπορεί να αποθηκευτεί ως ένα απλό αρχείο ή ως μία απλή βάση δεδομένων. Η αλυσίδα των μπλοκ απεικονίζεται συχνά ως κατακόρυφη στοίβα, με τα μπλοκ να τοποθετούνται το ένα πάνω από το άλλο σε επίπεδα, με το πρώτο μπλοκ από αυτά να είναι το γενεσιουργό της στοίβας. Η απεικόνιση των στοιβαγμένων μπλοκ έχει ως

[121] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 220, *Ghimire, H., Selvaraj, H.*, ό.π., σελ. 3.
[122] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 6: «Ως γενικό καθολικό ορίζεται στην λογιστική η συλλογή όλων των λογαριασμών της εταιρείας, η οποία περιέχει περιληπτικά όλες τις οικονομικές συναλλαγές κατά τη διάρκεια κάποιας συγκεκριμένης λογιστικής περιόδου και χρησιμοποιεί το διπλογραφικό λογιστικό σύστημα. Οι λογαριασμοί σε κάθε γενικό καθολικό χωρίζονται σε δύο μέρη και έχουν συνήθως την μορφή δίστηλων Τ λογαριασμών. Το αριστερό μέρος περιέχει χρεωστικές συναλλαγές και το δεξί μέρος πιστωτικές».

αποτέλεσμα να χρησιμοποιούνται όροι όπως «ύψος» για την αναφορά στην απόσταση από το πρώτο μπλοκ και «κορυφή» ή «άκρο» για την αναφορά στο μπλοκ που έχει προστεθεί τελευταίο[123].

Το Blockchain αποτελεί την τεχνολογική υποδομή του Bitcoin, καθώς και όλων των ψηφιακών νομισμάτων. Αποτελεί το παγκόσμιο αρχείο όλων των συναλλαγών, το οποίο στο δίκτυο Bitcoin όλοι δέχονται ως την αυθεντική καταγραφή της ιδιοκτησίας. Στην πραγματικότητα, το Bitcoin δεν μπορεί να υπάρξει χωρίς το Blockchain, ενώ το Blockchain μπορεί να υπάρξει χωρίς το Bitcoin και να αξιοποιηθεί για πλήθος διαφορετικών δραστηριοτήτων[124]. Υπάρχουν περισσότερα από ένα δίκτυα Bitcoin με αλυσίδες μπλοκ. Το κύριο ονομάζεται mainnet, δημιουργήθηκε από τον Satoshi Nakamoto στις 3 Ιανουαρίου 2009 και ξεκινά με το μπλοκ γέννησης. Τα άλλα που υπάρχουν χρησιμοποιούνται για σκοπούς δοκιμής. Παραδείγματα τέτοιων είναι παράδειγμα το testnet ή το regtest[125].

[123] Βλ. Μάλαμας, Φ., 2019. *Σύγχρονες φορολογικές πρακτικές της ψηφιακής οικονομίας*. Αθήνα: Νομική Βιβλιοθήκη, σελ. 600, *Antonopoulos, A.*, ό.π., σελ. 195, Chytis, E., Kitsantas, T. and Vazakidis, A., 2019. *A Review of Blockchain Technology and Its Applications in the Business Environment*. [online]. International Conference on Enterprise, Systems, Accounting, Logistics & Management. July 2019. Chania, Crete, Greece, σελ. 1. Available at:https://www.researchgate.net/publication/334615432_A_Review_of_Blockchain_Technology_and_Its_Applications_in_the_Business_Environment (Accessed 28/01/2021), *Ghimire, H., Selvaraj, H.*, ό.π., σελ. 3, Yi-Cheng, C., Yueh-Peng, C. and Yung-Chen, C., 2019. An Image Authentication Scheme Using Merkle Tree Mechanisms. *Future Internet* [online]. 6 July, σελ. 2. Available at: https://www.researchgate.net/publication/334291891_An_Image_Authentication_Scheme_Using_Merkle_Tree_Mechanisms (Accessed 26/01/2021),

[124] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 6, *Μάλαμας, Φ.*, ό.π., σελ. 599, *Antonopoulos, A.*, ό.π., σελ. 217.

[125] Το **testnet** χρησιμοποιείται για δοκιμαστικούς σκοπούς και είναι ένα πλήρως εξοπλισμένο P2P δίκτυο, με πορτοφόλια, δοκιμαστικά Bitcoin, εξόρυξη και όλα τα άλλα χαρακτηριστικά του mainnet. Υπάρχουν μόνο δύο διαφορές: τα νομίσματα testnet προορίζονται να είναι άχρηστα και η δυσκολία εξόρυξης πρέπει να είναι αρκετά χαμηλή, ώστε ο καθένας να μπορεί να εξορύσσει νομίσματα testnet σχετικά εύκολα. Οποιαδήποτε ανάπτυξη λογισμικού που προορίζεται για χρήση στην παραγωγή στο mainnet του Bitcoin θα πρέπει πρώτα να δοκιμαστεί στο testnet με δοκιμαστικά νομίσματα. Αυτό προστατεύει τόσο τους προγραμματιστές από νομισματικές απώλειες λόγω σφαλμάτων, όσο και το δίκτυο από ακούσια συμπεριφορά λόγω σφαλμάτων.
Το **regtest** επιτρέπει να δημιουργήσει κάποιος μια τοπική αλυσίδα με μπλοκ για σκοπούς δοκιμών. Προορίζονται να λειτουργούν ως κλειστά συστήματα για τοπικές δοκιμές. Ξεκινάει λοιπόν κάποιος ένα Blockchain regtest από το μηδέν, δημιουργώντας ένα τοπικό μπλοκ γένεσης, *Antonopoulos, A.*, ό.π., σελ. 211.

3.1. Το μπλοκ

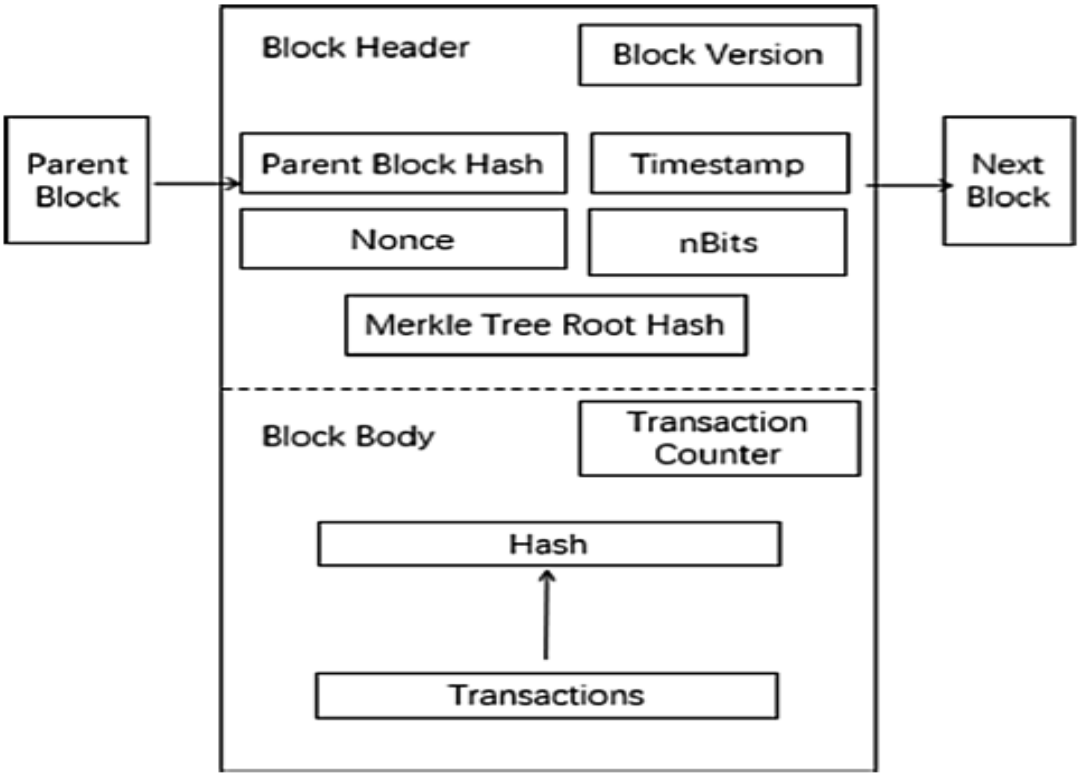
Το πρώτο γέννησης που δημιουργήθηκε το 2009 είναι στατικά κωδικοποιημένο στο λογισμικό του Bitcoin, ώστε να μην μπορεί να αλλαχθεί. Αποτελεί με αυτόν τον τρόπο μια ασφαλή ρίζα, από την οποία μπορεί να κατασκευαστεί μια αξιόπιστη αλυσίδα. Είναι ο κοινός πρόγονος όλων των μπλοκ, που σημαίνει ότι από οποιοδήποτε μπλοκ αν ξεκινήσει κάποιος και ακολουθήσει χρονικά την αλυσίδα προς τα πίσω θα καταλήξει στο μπλοκ γέννησης. Το ύψος του είναι Νο 0 και μετά από αυτό κάθε μπλοκ που προστίθεται αυξάνει το ύψος της αλυσίδας κατά 1. Κάθε κόμβος γνωρίζει τον κατακερματισμό και τη δομή του μπλοκ γέννησης, την απόλυτη χρονική στιγμή που δημιουργήθηκε και τη μοναδική συναλλαγή που περιλαμβάνεται μέσα σε αυτό. Το μπλοκ γέννησης περιέχει ένα κρυμμένο μήνυμα, το οποίο ενσωματώθηκε σε αυτό από τον ίδιο τον δημιουργό του Bitcoin. Η είσοδος της coinbase συναλλαγής περιέχει το κείμενο: «The Times 03/Jan/2009 Chancellor on brink of second bailout for banks». Μέσω της αναφοράς του σε επικεφαλίδα τίτλου εφημερίδας αυτό το μήνυμα υποστηρίζεται ότι είχε διττό στόχο. Αφενός να αποτελέσει μια απόδειξη του χρόνου που δημιουργήθηκε το μπλοκ γέννησης και αφετέρου να υπενθυμίσει τη σημασία ενός ανεξάρτητου νομισματικού συστήματος καθώς η έναρξη του Bitcoin συνέβη την ίδια χρονική στιγμή με την παγκόσμια χρηματοπιστωτική κρίση[126].

Οι τρόποι με τους οποίους μπορεί να προσδιοριστεί ένα μπλοκ, είναι δύο. Ο πρώτος γίνεται μέσω του κατακερματισμού του μπλοκ, ο οποίος προσδιορίζει το μπλοκ μοναδικά και αδιαμφισβήτητα. Ο κατακερματισμός του μπλοκ δεν περιλαμβάνεται στη δομή δεδομένων του μπλοκ, όταν το μπλοκ μεταδίδεται στο δίκτυο ή όταν αποθηκεύεται στον μόνιμο αποθηκευτικό χώρο του κόμβου ως κομμάτι του Blockchain. Αντιθέτως υπολογίζεται από τον κάθε κόμβο ξεχωριστά, όταν το μπλοκ λαμβάνεται από το δίκτυο[127]. Ο δεύτερος τρόπος προσδιορισμού γίνεται μέσω του ύψους που έχει το μπλοκ στο Blockchain. Σε αντίθεση με τον κατακερματισμό του μπλοκ, το ύψος μπλοκ δεν αποτελεί ένα μοναδικό αναγνωριστικό. Παρά το γεγονός, ότι το μπλοκ θα έχει πάντα ένα συγκεκριμένο και αμετάβλητο ύψος, όμως ο αντίστροφο δεν ισχύει. Δηλαδή το ύψος δεν προσδιορίζει πάντοτε ένα μοναδικό μπλοκ, διότι δύο ή περισσότερα μπλοκ μπορούν να

[126] Βλ. *Antonopoulos, A.*, ό.π., σελ. 198-199, *Ghimire, H., Selvaraj, H.* 3.
[127] Ο κατακερματισμός του μπλοκ μπορεί να αποθηκευτεί σε έναν ξεχωριστό πίνακα βάσεως δεδομένων, ως κομμάτι των μετά-δεδομένων του μπλοκ, ώστε να διευκολύνει την εύρεση και τη γρηγορότερη ανάκτηση του από τα μπλοκ στο δίσκο.

έχουν το ίδιο ύψος όταν ανταγωνίζονται για την ίδια θέση στο Blockchain, όπως συμβαίνει στην περίπτωση της διακλάδωσης. Επίσης, το ύψος δεν αποτελεί μέρος της δομής δεδομένων του μπλοκ και γι' αυτό δεν αποθηκεύεται εντός αυτού[128]. Κάθε κόμβος προσδιορίζει δυναμικά τη θέση ενός μπλοκ στο Blockchain, όταν λαμβάνεται από το δίκτυο Bitcoin[129].

Οι πληροφορίες που περιέχονται σε ένα μπλοκ είναι τριών ειδών: περιέχεται η εξωτερική κεφαλίδα, μέσα στο σώμα του μπλοκ αποθηκεύεται η λίστα και ένας μετρητής συναλλαγών και τέλος περιέχεται η κεφαλίδα του μπλοκ[130].



Εικόνα 5: Δομή μπλοκ[131].

[128] Το ύψος του μπλοκ ωστόσο μπορεί να αποθηκεύεται ως μετά-δεδομένα σε έναν ευρετηριασμένο πίνακα βάσης δεδομένων για την ταχύτερη ανάκτηση.
[129] Βλ. *Antonopoulos, A.*, ό.π., σελ. 197-198, Cosset, D., 2017. *Blockchain: what is in a block?* Available at: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo (Accessed 28/01/2021).
[130] Βλ. *Belotti, M., AA et al.*, ό.π., σελ. 28, *Chandel, S., AA et al.*,, ό.π., σελ. 989, *Yi-Cheng, C., Yueh-Peng, C. and Yung-Chen, C.*, ό.π., σελ. 2.
[131] *Chandel, S., AA et al*, ό.π., σελ. 990.

3.2. Η κεφαλίδα του μπλοκ

Η κεφαλίδα του μπλοκ (Εικόνα 6) εμπεριέχει μια σειρά από μεταδεδομένα[132]: α) δύο αναφορές, η μία στον αριθμό έκδοσης του μπλοκ, ο οποίος σχετίζεται με το ποσοστό συναίνεσης που έλαβε το μπλοκ όταν επικυρώθηκε και η δεύτερη στον κατακερματισμό του προηγούμενου μπλοκ, ο οποίος συνδέει το παρόν μπλοκ με το προηγούμενο, β) τη χρονοσφραγίδα και την κρυπτογραφική τυχαία τιμή (nonce), η οποία σχετίζεται με τον ανταγωνισμό στην εξόρυξη και γ) τη ρίζα του δέντρου Merkle.

3.2.1. Ο κατακερματισμός της κεφαλίδας

Η συνάρτηση κατακερματισμού είναι το θεμελιώδες συστατικό για το Blockchain. Κάθε μπλοκ συνδέεται με το αμέσως προηγούμενο μέσω μιας τιμής κατακερματισμού, η οποία χαρακτηρίζει μοναδικά το μπλοκ και ενσωματώνεται στο επόμενο μπλοκ, αποτελώντας αναπόσπαστο τμήμα του. Η τιμή κατακερματισμού προκύπτει έπειτα από τον διπλό κατακερματισμό της κεφαλίδας με τη χρήση ενός αλγόριθμου κρυπτογραφικού κατακερματισμού που ονομάζεται SHA256 (Secure Hash Algorithm). Η τιμή κατακερματισμού αποτελεί το ψηφιακό αποτύπωμα του κάθε μπλοκ και ονομάζεται κατακερματισμός κεφαλίδας μπλοκ[133].

Μέσα στην κεφαλίδα του τρέχοντος μπλοκ βρίσκεται και η τιμή κατακερματισμού του προηγούμενου μπλοκ (μητρικό μπλοκ). Όταν το μητρικό με οποιοδήποτε τρόπο τροποποιείται, αλλάζει και ο κατακερματισμός του. Αν λοιπόν κάποιος προσπαθήσει να αλλοιώσει ένα δεδομένο ενός μπλοκ, τότε αυτόματα η τιμή κατακερματισμού του εν λόγω μπλοκ μεταβάλλεται και επομένως θα προκληθεί αναντιστοιχία με τα υπόλοιπα νεότερα μπλοκ (παιδικά), καθώς θα επηρεάσει αυτόματα και τα δεδομένα του επόμενου μπλοκ προκαλώντας σφάλμα. Η αλυσιδωτή αυτή αντίδραση ονομάζεται φαινόμενο κυματισμού και δρα προστατευτικά στην περίπτωση που ένας ανέντιμος κόμβος προσπαθεί να αλλάξει ένα μπλοκ που ακολουθείται από αρκετές γενεές του, καθώς τον υποχρεώνει να επαναλάβει την απόδειξη εργασίας όλων των μπλοκ που εξορύχθησαν μετά από αυτό και την ίδια στιγμή

[132] Βλ. *Antonopoulos, A.*, ό.π., σελ. 197.
[133] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 10, *Antonopoulos, A.*, ό.π., σελ. 196-197, *Belotti, M., AA et al.*, ό.π., σελ. 28, *Chandel, S., AA et al*, ό.π., σελ. 990, *Ghimire, H., Selvaraj, H.*, ό.π., σελ.3, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 20, *Yi-Cheng, C., Yueh-Peng, C. and Yung-Chen, C.*, ό.π., σελ. 2,

να ανταγωνιστεί όλους του έντιμους κόμβους που υπάρχουν στο δίκτυο για να τους ξεπεράσει. Ένας τέτοιος υπολογισμός όμως θα απαιτούσε τεράστια υπολογιστική ισχύ.
Ένα μπλοκ έχει μόνο ένα μητρικό, αλλά μπορεί να έχει πολλά παιδικά. Τα πολλαπλά παιδικά ανακύπτουν κατά τη διάρκεια διακλάδωσης της αλυσίδας των μπλοκ, μία κατάσταση προσωρινή που προκύπτει όταν ανακαλύπτονται την ίδια στιγμή διαφορετικά μπλοκ από διαφορετικούς κόμβους εξόρυξης. Εν τέλει όμως, μόνο ένα παιδικό μπλοκ γίνεται μέρος της αλυσίδας των μπλοκ και η διακλάδωση επιλύεται[134].

Μια συνάρτηση κατακερματισμού λοιπόν μπορεί να χρησιμοποιηθεί για την απόκρυψη των πληροφοριών που μεταδίδονται και να τις καταστήσει πιο ασφαλείς. Οποιαδήποτε αλλαγή συμβεί στο μπλοκ, συνεπάγεται και αλλαγή της τιμής που θα προκύψει από την διαδικασία του κατακερματισμού. Η τιμή αυτή διευκολύνει τους κόμβους στο να ελέγξουν αν έχουν τον ίδιο κατάλογο συναλλαγών μέσα στο μπλοκ τους, χωρίς να χρειάζεται να γνωρίζουν την κάθε συναλλαγή ξεχωριστά[135].

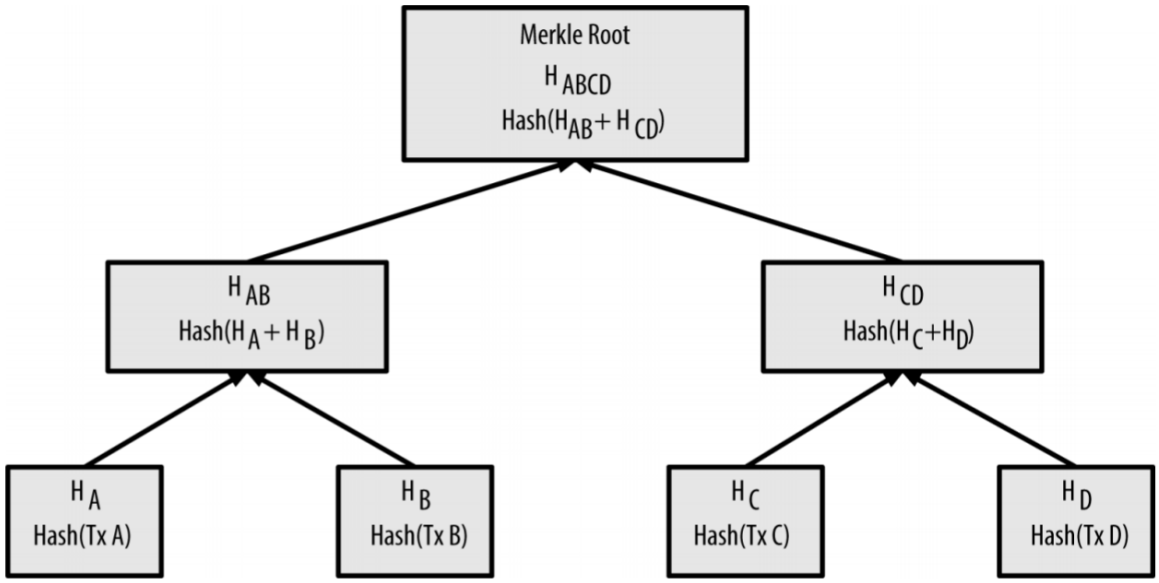
3.2.2. Η χρονοσφραγίδα

Η χρονοσφραγίδα επιβεβαιώνει τα δεδομένα, τα οποία είναι ενσωματωμένα στο εν λόγω μπλοκ τη συγκεκριμένη χρονική στιγμή, καταγράφοντας τον χρόνο δημιουργίας του μπλοκ. Έχει τη βάση της στον αριθμό των δευτερολέπτων που έχουν περάσει από την 1η Ιανουαρίου 1970 UTC/GMT (UNIX time). Η αποτύπωση του χρόνου γίνεται με ακρίβεια κλάσματος δευτερολέπτου και αποτελεί την απόδειξη πιστοποίησης της κατοχής του περιεχομένου που είναι κωδικοποιημένο με το ψηφιακό αποτύπωμα. Η χρονοσφραγίδα αποδεικνύει ότι τα δεδομένα υπήρχαν εκείνη τη στιγμή και περιλήφθηκαν στο κατακερματισμό. Κάθε χρονική σήμανση περιλαμβάνει την προηγούμενη χρονική σήμανση στον κατακερματισμό της, σχηματίζοντας μια αλυσίδα, με κάθε πρόσθετη χρονική σήμανση να ενισχύει αυτές που προηγούνται[136].

3.2.3. Τα δέντρα Merkle

[134] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 222, *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 10-11, *Antonopoulos, A.*, ό.π., σελ. 195-196, *Chandel, S., AA et al*, ό.π., σελ. 990, *Ghimire, H., Selvaraj, H.*, ό.π., σελ.3, *Nakamoto, S.*, ό.π., σελ. 2-3.
[135] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 221, *Chandel, S., AA et al*, ό.π., σελ. 990.
[136] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 11, *Παπαδοπούλου, Α.*, ό.π., σελ. 212, 217, *Nakamoto, S.*, ό.π., σελ.3.

Ο όρος «δέντρα Merkle» παρουσιάστηκαν πρώτη φορά το 1979 από τον Ralph Merkle. Η δομή τους βοηθά στην επαλήθευση της συνέχειας του περιεχομένου των δεδομένων. Η ορολογία «δέντρο» χρησιμοποιείται για να περιγράψει μία κλαδωτή δομή δεδομένων, η οποία απεικονίζεται αντίστροφα, με τη «ρίζα» στην κορυφή και τα «κλαδιά» στον πάτο του διαγράμματος. Το δέντρο εκτείνεται από τη ρίζα έως την άκρη του μακρύτερου κλάδου[137].



Εικόνα 6: Δέντρο Merkle[138]

Τα δέντρα Merkle χρησιμοποιούνται στο Bitcoin για να συναθροίζουν όλες τις συναλλαγές ενός μπλοκ, παράγοντας ένα ψηφιακό αποτύπωμα για το σύνολο της ομάδας των συναλλαγών. Στην πράξη, κατακερματίζουν τις συναλλαγές, έπειτα συνδυάζουν τους κατακερματισμούς σε ζεύγη και τους συνοψίζουν σε ένα μητρικό κόμβο και τέλος κατακερματίζουν τους μητρικούς κόμβους δημιουργώντας το κάθε επίπεδο του δέντρου. Η διαδικασία συνεχίζεται μέχρι στην κορυφή να υπάρξει μόνο ένας κόμβος που κατακερματίζεται και ονομάζεται ρίζα Merkle. Η ρίζα είναι η μόνη που περιλαμβάνεται στο μπλοκ. Χάρη στη ρίζα οι εσωτερικοί κατακερματισμοί δεν χρειάζεται να αποθηκευτούν με

[137] Βλ. Βλ. *Antonopoulos, A.*, ό.π., σελ. 201, *Vallois, V., Guenane, F.*, ό.π., σελ. 64, *Yi-Cheng, C., Yueh-Peng, C. and Yung-Chen, C.*, ό.π., σελ. 4.
[138] Πηγή *Yi-Cheng, C., Yueh-Peng, C. and Yung-Chen, C.*, ό.π., σελ. 4

αποτέλεσμα τα παλιά μπλοκ να μπορούν να συμπιεστούν απομακρύνοντας τα «κλαδιά» και εξοικονομώντας χώρο στο δίσκο[139].

Τα δέντρα Merkle επιτρέπουν σε κάθε κόμβο να επαληθεύει μεμονωμένες συναλλαγές, χωρίς να χρειάζεται να κατεβάσει και να επαληθεύσει ολόκληρο το μπλοκ και εγγυώνται ότι τα δεδομένα στο μπλοκ δεν μπορούν να παραποιηθούν. Έτσι αν ένα αντίγραφο του μπλοκ στο δίκτυο έχει την ίδια ρίζα Merkle με ένα άλλο, τότε οι συναλλαγές σε αυτό το μπλοκ είναι οι ίδιες. Λόγω των ιδιοτήτων του κατακερματισμού, όταν μια συναλλαγή εισέρχεται στο μπλοκ, το πεδίο υπολογίζεται εκ νέου. Ακόμα λοιπόν και λίγα λανθασμένα δεδομένα θα οδηγούσαν σε πολύ διαφορετική ρίζα Merkle, γεγονός που διασφαλίζει το αμετάβλητο των συναλλαγών του μπλοκ. Επομένως για την επαλήθευση των συναλλαγών αρκεί η σύγκριση μεταξύ των ριζών Merkle[140].

Οι κόμβοι SPV κάνουν εκτενή χρήση των δέντρων Merkle χρησιμοποιώντας μία διαδρομή πιστοποίησης ή αλλιώς διαδρομή Merkle. Οι κόμβοι αυτοί, έπειτα από αίτημα που απευθύνουν στους υπόλοιπους κόμβους, κάνουν λήψη μόνο των κεφαλίδων της μακρύτερης αλυσίδας. Στη συνέχεια, διατηρούν το κλαδί Merkle συνδέοντας τη συναλλαγή με το μπλοκ στο οποίο βρίσκεται. Ο SPV δεν μπορεί να επαληθεύσει τη συναλλαγή μόνος του, αλλά το γεγονός ότι μπορεί να τη συνδέσει με ένα μπλοκ στο δίκτυο, σημαίνει ότι το δίκτυο των κόμβων την έχει επικυρώσει και αυτό μόνο του αποτελεί επιβεβαίωση. Επίσης, ο κόμβος SPV χρησιμοποιεί την κεφαλίδα του μπλοκ για να το συνδέσει με το Blockchain. Ο συνδυασμός αυτών των δύο συνδέσεων, συναλλαγής-μπλοκ και μπλοκ-Blockchain, αποδεικνύει ότι η συναλλαγή είναι καταγεγραμμένη στο Blockchain[141].

3.3. Η διαδικασία της εξόρυξης

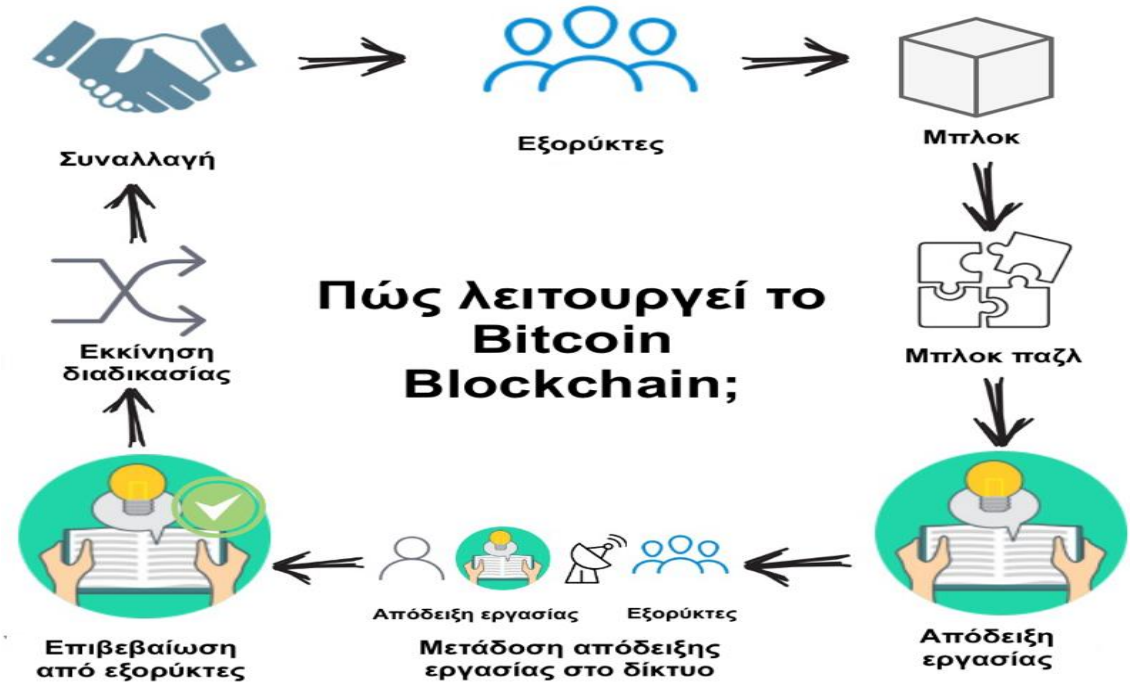
Ο κεντρικός άξονας του Bitcoin δεν είναι κάποια κεντρική τράπεζα, αλλά οι εξορύκτες ή miners, οι οποίοι κατέχουν υπολογιστικά συστήματα μεγάλης ισχύος με τα οποία επιλύουν έναν περίπλοκο μαθηματικό γρίφο, που οδηγεί στην επαλήθευση και στην ενσωμάτωση των συναλλαγών στο μπλοκ. Η εξόρυξη, όπως ονομάζεται, είναι η κύρια διαδικασία της αποκεντρωμένης εκκαθάρισης των συναλλαγών. Πρόκειται για μια

[139] Βλ. *Antonopoulos, A.*, ό.π., σελ. 201-202, 207, *Chandel, S., AA et al.,*, ό.π., σελ. 990, *Cosset, D.* ό.π., *Nakamoto, S.*, ό.π., σελ. 4, *Yi-Cheng, C., Yueh-Peng, C. and Yung-Chen, C.*, ό.π., σελ. 4

[140] Β λ. *Antonopoulos, A.*, ό.π., σελ. 227, *Chandel, S., AA et al*, ό.π., σελ. 990, *Vallois, V., Guenane, F.*, ό.π., σελ. 66, *Yi-Cheng, C., Yueh-Peng, C. and Yung-Chen, C.*, ό.π., σελ. 4..

[141] Βλ. *Antonopoulos, A.*, ό.π., σελ. 207, *Nakamoto, S.*, ό.π., σελ. 5.

διαδικασία, η οποία για να αποδειχθεί απαιτεί ένα τεράστιο ποσό υπολογιστικής ισχύος, αλλ' όμως για να επαληθευθεί ως αποδεδειγμένη αρκεί μόνο μια μικρή ποσότητα.
Η διαδικασία της εξόρυξης εξυπηρετεί δύο σκοπούς. Παρέχει ασφάλεια για τις συναλλαγές Bitcoin, καθώς μέσω της εξόρυξης και της αναδυόμενης συναίνεσης που προκύπτει, επιβεβαιώνονται οι συναλλαγές και απορρίπτονται οι ανεπιβεβαίωτες. Επίσης, δημιουργεί νέα BTC, καθώς αποτελεί τον μόνο τρόπο που υπάρχει για τη δημιουργία επιπρόσθετου ψηφιακού νομίσματος. Στους εξορύκτες παρέχονται ως ανταμοιβή νέα ψηφιακά νομίσματα και χρεώσεις συναλλαγών[142].



Εικόνα 7: Πώς λειτουργεί το Bitcoin[143].

Αρχικά κατασκευάζεται και προετοιμάζεται ένα υποψήφιο προς εξόρυξη μπλοκ μέσα στο οποίο προστίθενται μη επιβεβαιωμένες συναλλαγές. Στη συνέχεια, ο κόμβος εξόρυξης μεταδίδει την κεφαλίδα του μπλοκ στο υλισμικό εξόρυξης, το οποίο ξεκινά να δοκιμάζει τρισεκατομμύρια κρυπτογραφικές περιστασιακές τιμές ανά δευτερόλεπτο. Σχεδόν 10 λεπτά μετά το ξεκίνημα της εξόρυξης του μπλοκ, κάποια από τις μηχανές

[142] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 835, *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 9, *Antonopoulos, A.*, ό.π., σελ. 26, 213, *Ghimire, H., Selvaraj, H.*, ό.π., σελ. 2-3, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 19.
[143] Πηγή: *Ghimire, H., Selvaraj, H*, ό.π.

εξόρυξης βρίσκει μία λύση και τη στέλνει πίσω στον κόμβο εξόρυξης. Όσο μεγαλύτερη υπολογιστική ισχύ έχει ένας εξορύκτης, τόσο αυξάνονται και ο πιθανότητές του να λύσει πρώτος τον γρίφο. Αμέσως, ο κόμβος εξόρυξης μεταδίδει το μπλοκ σε όλους τους ομότιμους κόμβους, οι οποίοι λαμβάνουν, επαληθεύουν και στη συνέχεια διαδίδουν το νέο μπλοκ σαν κυματισμό μέσα στο δίκτυο, οπότε ο κάθε κόμβος το προσθέτει στο δικό του αντίγραφο Blockchain, επεκτείνοντας την αλυσίδα του κατά ένα μπλοκ. Καθώς οι κόμβοι εξόρυξης λαμβάνουν και επαληθεύουν το νέο μπλοκ, εγκαταλείπουν τις προσπάθειες για την εύρεση μπλοκ στο ίδιο ύψος και ξεκινούν αμέσως τον υπολογισμό του επόμενου μπλοκ που θα προστεθεί στην αλυσίδα[144].

3.3.1. Η συναίνεση

Η κύρια εφεύρεση του Satoshi Nakamoto είναι ο αποκεντρωμένος μηχανισμός αναδυόμενης[145] συναίνεσης, η οποία καθιστά την παρουσία του τρίτου έμπιστου[146] μέρους περιττή. Το ίδιο το δίκτυο αναλαμβάνει να επικυρώσει τις συναλλαγές και να εξασφαλίσει την απαραίτητη συναίνεση. Η συναίνεση είναι ένα πρωτόκολλο, που έχει προσυμφωνηθεί από τους κόμβους του δικτύου και με το οποίο εξασφαλίζεται ότι το μπλοκ, που θα ενταχθεί από τον εξορύκτη στην αλυσίδα, αποτελεί και τον μοναδικό νεότερο κρίκο της πάνω στον οποίο θα ενωθεί και το αμέσως επόμενο μπλοκ. Το Blockchain λοιπόν συναρμολογείται από τον κάθε κόμβο ανεξάρτητα και αναγνωρίζεται από κάθε πλήρη κόμβο ως το αυθεντικά καταγεγραμμένο αρχείο[147].

Η αποκεντρωμένη συναίνεση του Bitcoin αναδύεται μέσα από τέσσερεις διαδικασίες που συμβαίνουν σε κάθε κόμβο του δικτύου: επαλήθευση κάθε συναλλαγής από κάθε πλήρη κόμβο, περισυλλογή των συναλλαγών σε νέα μπλοκ από κόμβους εξόρυξης, επαλήθευση από κάθε κόμβο των νέων μπλοκ και συναρμολόγηση σε αλυσίδα και τέλος επιλογή από κάθε κόμβο της αλυσίδας με τον περισσότερο σωρευτικό υπολογισμό.

---

144 Βλ. *Antonopoulos, A.*, ό.π., σελ. 200, 237-238, *Γιαννόπουλος, Α.*, ό.π., σελ. 222.

145 Η συναίνεση χαρακτηρίζεται ως «αναδυόμενη», αφενός επειδή δεν είναι ρητή διεξαχθείσα για παράδειγμα μέσω κάποιας εκλογικής διαδικασίας και αφετέρου δεν προκύπτει κάποια σταθερή δεδομένη στιγμή, *Antonopoulos, A.*, ό.π., σελ. 217.

146 Όλα τα παραδοσιακά συστήματα πληρωμών εξαρτώνται από ένα πρότυπο εμπιστοσύνης, το οποίο περιλαμβάνει μία κεντρική αρχή, οποία είναι επιφορτισμένη με το να παρέχει την υπηρεσία της εκκαθάρισης των συναλλαγών δηλαδή να επαληθεύει και να εκκαθαρίζει αυτές, Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 320.

147 Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 320, *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 9, *Antonopoulos, A.*, ό.π., σελ. 217, *Belotti, M., AA et al.*, ό.π., σελ. 3.

3.3.1.1. Η ανεξάρτητη επαλήθευση των συναλλαγών

Η πρώτη διαδικασία της αποκεντρωμένης συναίνεσης σχετίζεται με την ανεξάρτητη επαλήθευση των συναλλαγών. Όπως έχει αναφερθεί, το πορτοφόλι Bitcoin δημιουργεί συναλλαγές συλλέγοντας UTXO και κατασκευάζοντας νέες εξόδους εκχωρημένες σε νέο ιδιοκτήτη. Η συναλλαγή αποστέλλεται στους ομότιμους κόμβους, ώστε να μπορέσει να διαδοθεί διαμέσου του δικτύου Bitcoin. Ωστόσο, προτού μεταδοθεί περαιτέρω η ληφθείσα συναλλαγή, πρέπει πρώτα ο κάθε κόμβος να την επαληθεύσει. Με τον τρόπο αυτό διασφαλίζεται ότι μόνο έγκυρες συναλλαγές διαδίδονται διαμέσου του δικτύου, ενώ οι άκυρες συναλλαγές θα απορριφθούν στον πρώτο κόμβο που θα τις συναντήσει. Τα κριτήρια που πρέπει να πληρούνται αναπροσαρμόζονται κατά χρονικά διαστήματα και γίνονται είτε πιο αυστηρά για να αντιμετωπίζονται επιθέσεις άρνησης υπηρεσιών, είτε πιο ήπια ώστε να περιλαμβάνονται περισσότεροι τύποι συναλλαγών[148]. Μέσω της ανεξάρτητης επαλήθευσης της κάθε συναλλαγής ο κάθε κόμβος μπορεί να κατασκευάζει την ομάδα μη επιβεβαιωμένων συναλλαγών.

3.3.1.2. Οι κόμβοι εξόρυξης και ο αλγόριθμος απόδειξης εργασίας (PoW)

Το δεύτερο βήμα στο μηχανισμό συναίνεσης αφορά τους κόμβους εξόρυξης. Οι κόμβοι εξόρυξης συλλέγουν, επαληθεύουν και μεταδίδουν νέες συναλλαγές όπως κάνει και κάθε άλλος κόμβος και, επιπρόσθετα από τους άλλους κόμβους, συγκεντρώνουν τις νόμιμες συναλλαγές μέσα σε ένα υποψήφιο μπλοκ, αναλαμβάνοντας επί της ουσίας να διεξάγουν το δύσκολο έργο της εξόρυξης. Εξορύκτης μπορεί να γίνει οποιοσδήποτε έχει πρόσβαση σε μια σταθερή σύνδεση στο διαδίκτυο, διαθέτει ειδικό εξοπλισμό εξόρυξης και είναι συνδεδεμένος σε διακομιστή που τρέχει πλήρη κόμβο[149].

Η άφιξη ενός νέου μπλοκ σηματοδοτεί αφενός το τέλος ενός γύρου ανταγωνισμού που επικρατεί ανάμεσα στους εξορύκτες και αφετέρου το ξεκίνημα ενός νέου γύρου. Έτσι, κάθε φορά που εξορύσσεται ένα μπλοκ, οι κόμβοι εξόρυξης ελέγχουν τις συναλλαγές στην ομάδα μη επιβεβαιωμένων συναλλαγών, αφαιρούν όσες έχουν περιληφθεί στο μπλοκ που μόλις έχει εξορυχθεί, προσθέτουν αυτές που δημιουργήθηκαν πρόσφατα και κατασκευάζουν ένα νέο άδειο μπλοκ για να ξεκινήσουν εκ νέου την διαδικασία εξόρυξης. Ο έλεγχος αυτός είναι απαραίτητος, καθώς δεν μπορούν να υπάρξουν δύο διαφορετικά μπλοκ με την ίδια

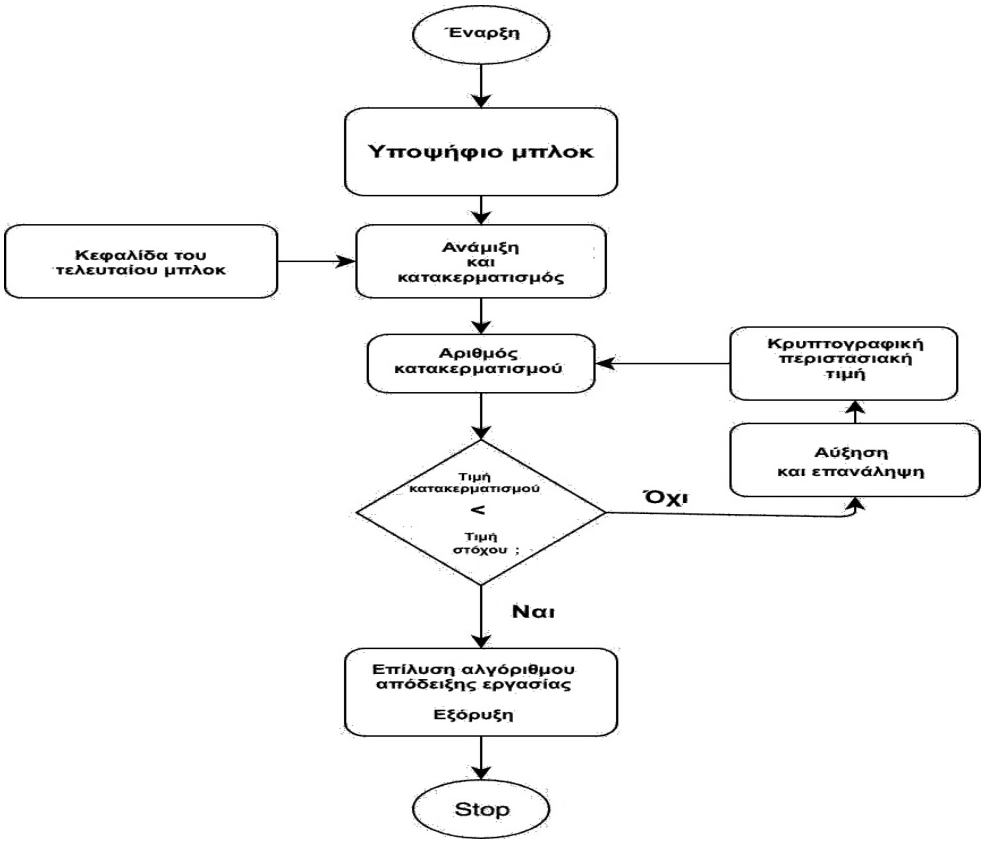
[148] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 6, *Antonopoulos, A.*, ό.π., σελ. 218-219.
[149] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 835, *Antonopoulos, A.*, ό.π., σελ. 219-220.

συναλλαγή, διότι η διπλή παρουσία αυτής συνεπάγεται ότι ο οφειλέτης οφείλει να καταβάλει δυο φορές. Οι ίδιες συναλλαγές μπορεί να περιλαμβάνονται σε περισσότερα του ενός υποψήφια μπλοκ, που δημιουργούνται την ίδια χρονική στιγμή από διαφορετικούς εξορύκτες.

Η πρώτη συναλλαγή που προστίθεται στο μπλοκ είναι μια ειδική συναλλαγή, που ονομάζεται συναλλαγή coinbase. Αυτή η συναλλαγή κατασκευάζεται από τον κόμβο εξόρυξης του εξορύκτη και είναι η ανταμοιβή του για την προσπάθεια εξόρυξης που καταβάλει. Το κάθε μπλοκ μπορεί να ενσωματώσει συγκεκριμένο αριθμό συναλλαγών, τηρώντας ένα δεδομένο όριο μεγέθους μπλοκ. Μόλις συμπληρωθεί ο αριθμός αυτός, οι εξορύκτες επιδίδονται στον αγώνα εξεύρεσης της λύσης.

Οι συναλλαγές δεν έχουν ημερομηνία λήξης. Ωστόσο, εάν κάποια συναλλαγή διαδοθεί διαμέσου του δικτύου μόνο μία φορά, θα παραμείνει μόνο όσο κρατείται σε μία ομάδα μη επιβεβαιωμένων συναλλαγών ενός κόμβου εξόρυξης. Κάθε φορά που ο κόμβος εξόρυξης κάνει επανεκκίνηση, η ομάδα συναλλαγών του διαγράφεται πλήρως, καθώς αποτελεί προσωρινή μορφή αποθήκευσης. Το γεγονός αυτό έχει σαν αποτέλεσμα για μία επαληθευμένη συναλλαγή να μπορεί μεν να διαδοθεί στο δίκτυο, εάν όμως δεν εκτελεστεί, τελικά να μην παραμείνει στην ομάδα συναλλαγών κανενός εξορύκτη[150].

[150] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 222, *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 9, *Antonopoulos, A.*, ό.π., σελ. 220, *Belotti, M., AA et al.*, ό.π., σελ. 15, Bissias, G., AA et al., 2016. *An Analysis of Attacks on Blockchain Consensus (DRAFT)*, σελ. 19. Available at: https://www.researchgate.net/publication/309424665_An_Analysis_of_Attacks_on_Blockchain_Consensus (Accessed 29/02/2021), *Pérez-Solà, S., AA et al.*, ό.π., σελ. 3.



Εικόνα 8: Διάγραμμα λειτουργίας αλγόριθμου απόδειξης εργασίας[151].

Ο κόμβος εξόρυξης αφού ελέγξει τις συναλλαγές προσθέτει στην κεφαλίδα του μπλοκ τον κατακερματισμό της κεφαλίδας του μητρικού μπλοκ, τη ρίζα Merkle, την χρονοσφραγίδα και συμπληρώνει τη δυσκολία του στόχου, η οποία προσδιορίζει την απαιτούμενη δυσκολία απόδειξης εργασίας, ώστε αυτό το μπλοκ να γίνει έγκυρο. Η μέθοδος συναίνεσης που ακολουθείται στο Bitcoin είναι ο αλγόριθμος απόδειξης εργασίας. Συγχρόνως, οι εξορύκτες προσπαθούν να λύσουν ένα κρυπτογραφικό-υπολογιστικό πρόβλημα, χρησιμοποιώντας την υπολογιστική τους ισχύ. Η εξεύρεση λύσης σε αυτό το πρόβλημα ονομάζεται αλγόριθμος απόδειξης εργασίας και έγκειται στην ανεύρεση μιας σειράς 64 ψηφίων του δεξαεξαδικού συστήματος, που αποτελούνται από αριθμούς και γράμματα. Πιο αναλυτικά, ο αλγόριθμος απόδειξης εργασίας χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης SHA256 για τον επανειλημμένο κατακερματισμό της κεφαλίδας του μπλοκ μαζί με την τυχαία τιμή που συμπεριλαμβάνεται στην κεφαλίδα. Ο κατακερματισμός θα επαναλαμβάνεται συνεχώς μέχρι αυτός που θα προκύψει να είναι ίσος ή χαμηλότερος

[151] Βλ. *Ghimire, H., Selvaraj, H.*, ό.π.

από μια συγκεκριμένη δυσκολία στόχου. Ο στόχος είναι ένας αριθμός 256-bit, ο οποίος είναι γνωστός σε όλους τους εξορύκτες.

Ο αριθμός, που χρησιμοποιείται ως μεταβλητή σε ένα τέτοιο σενάριο, ονομάζεται κρυπτογραφική περιστασιακή τιμή (nonce). Η τιμή βρίσκεται στην κεφαλίδα του μπλοκ, ξεκινά από το 0 και αυξάνεται συνεχώς, μέχρι να βρεθεί το νούμερο που θα δώσει στον κατακερματισμό του μπλοκ τα μηδενικά που απαιτούνται, σύμφωνα με τον στόχο δυσκολίας. Αν ο κατακερματισμός που θα προκύψει είναι μεγαλύτερος από τον στόχο, η λύση είναι άκυρη και ο εξορύκτης θα τροποποιήσει την κρυπτογραφική περιστασιακή τιμή και θα προσπαθήσει ξανά. Ο κόμβος εξόρυξης θα χρειαστεί να ελέγξει δισεκατομμύρια ή τρισεκατομμύρια κρυπτογραφικές περιστασιακές τιμές, πριν βρεθεί μία που να ικανοποιεί τον στόχο. Ο πρώτος εξορύκτης που θα βρει τη σωστή λύση, κερδίζει τον γύρο του ανταγωνισμού και δημοσιεύει αυτό το μπλοκ στο Blockchain. Όσο περισσότεροι εξορύκτες συμμετέχουν στο δίκτυο Bitcoin, τόσο πιο δύσκολη γίνεται η επίλυση του αλγόριθμου απόδειξης εργασίας[152].

Εικόνα 9: Τιμή κατακερματισμού[153].

[152] *Antonopoulos, A.*, ό.π., σελ. 27, 228, 231, *Belotti, M., AA et al.*, ό.π., σελ. 8, *Ghimire, H., Selvaraj, H.* σελ.3. Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ.9, *Μάλαμας, Φ.*, ό.π., σελ.196-197, *Antonopoulos, A.*, ό.π., σελ. 214, *Ghimire, H., Selvaraj, H.*, ό.π., σελ. 3-4, *Nakamoto, S.* ό.π., σελ.3.

[153] Βλ. *Euny Hong*, "How Does Bitcoin Mining Work", Available at: https://www.investopedia.com/tech/how-does-Bitcoin-mining-work/, (Accessed 28/01/2021).

Το αποτέλεσμα της συνάρτησης κατακερματισμού δεν μπορεί να προσδιοριστεί εκ των προτέρων, ούτε μπορεί να δημιουργηθεί κάποιο μοτίβο που θα παράξει μία συγκεκριμένη τιμή κατακερματισμού, καθόσον αυτή αποτελεί προϊόν τύχης. Ακόμη, το πρόβλημα δεν παραμένει σταθερό, αλλά αλλάζει σε κάθε διαδικασία εξόρυξης. Ο κατακερματισμός που προκύπτει ως αποτέλεσμα θα είναι πάντα ο ίδιος και μπορεί εύκολα να υπολογιστεί και να επαληθευτεί από οποιονδήποτε κόμβο υλοποιεί τον ίδιο αλγόριθμο κατακερματισμού. Το πιο σημαντικό χαρακτηριστικό ενός κρυπτογραφικού αλγόριθμου κατακερματισμού είναι ότι είναι πρακτικά αδύνατη η εύρεση δύο διαφορετικών εισόδων, που παράγουν το ίδιο αποτύπωμα. Ενώ λοιπόν για την εύρεση μιας κρυπτογραφικής περιστασιακής τιμής χρειάζονται πάρα πολλοί υπολογισμοί κατακερματισμών, για την επαλήθευσή της απαιτείται ένας μόνο υπολογισμός κατακερματισμού[154].

Κάθε 2016 μπλοκ γίνεται αναστόχευση δυσκολίας, προκειμένου να διασφαλιστεί ότι ανά 10 λεπτά θα εξορύσσεται ένα νέο μπλοκ. Η αναστόχευση δυσκολίας είναι μία δυναμική παράμετρος που ρυθμίζεται περιοδικά και συμβαίνει αυτόματα και ξεχωριστά σε κάθε πλήρη κόμβο. Η εξίσωση για την αναστόχευση δυσκολίας μετράει πόσος χρόνος χρειάστηκε για έκαστο μπλοκ από το σύνολο των τελευταίων 2016 μπλοκ και τον συγκρίνει με τον αναμενόμενο χρόνο των 10 λεπτών. Έτσι, εάν ένα μπλοκ εξορύσσεται σε λιγότερο από 10 λεπτά, το δίκτυο αυξάνει τη δυσκολία εξόρυξης, ενώ στην αντίθετη περίπτωση το δίκτυο μειώνει τη δυσκολία[155].

3.3.1.3. Η επαλήθευση του νέου μπλοκ

Το τρίτο βήμα στον μηχανισμό συναίνεσης του Bitcoin είναι η επαλήθευση κάθε νέου μπλοκ από κάθε κόμβο στο δίκτυο. Μόλις ο κόμβος εξόρυξης υπολογίσει τη σωστή τιμή κατακερματισμού, το μπλοκ μεταδίδεται αμέσως στο δίκτυο. Κάθε κόμβος λαμβάνει το μπλοκ που μεταδόθηκε και πριν το διαδώσει στους ομότιμους κόμβους επαληθεύει την αυθεντικότητά του συγκρίνοντας την τιμή κατακερματισμού που δίνεται στο μπλοκ λήψης με την τιμή στόχου.

Αν τα κριτήρια που έχουν τεθεί για την επαλήθευση του μπλοκ δεν τηρούνται, τότε αυτό απορρίπτεται. Αυτό διασφαλίζει αφενός ότι θα διαδίδονται στο δίκτυο μόνο έγκυρα μπλοκ

[154] Βλ. *Κεχαγιά, Χ.*, ό.π., σελ. 3, *Antonopoulos, A.*, ό.π., σελ. 228, 231.
[155] Βλ. *Antonopoulos, A.*, ό.π., σελ. 236, *Ghimire, H., Selvaraj, H.* σελ.3-4, *Kuo Chuen, D. L., Pak Nian, L.* σελ.20, *Nakamoto, S.*, ό.π., σελ. 3.

και αφετέρου ότι μόνο τα μπλοκ των εξορυκτών που λειτουργούν με τιμιότητα ενσωματώνονται στην αλυσίδα των μπλοκ και επομένως κερδίζουν τις αμοιβές. Επίσης, οποιεσδήποτε αλλαγές που γίνονται μέσα στο μπλοκ ακυρώνονται, ενισχύοντας έτσι την ανθεκτικότητα και ασφάλεια του συστήματος.

Αν όμως η πλειονότητα των εξορυκτών θεωρεί το μπλοκ έγκυρο, αυτό προστίθεται στο Blockchain. Το νέο μπλοκ εντάσσεται στην αλυσίδα με γραμμική, χρονολογική σειρά και αποτελεί μοναδικό και αναπόσπαστο μέρος της, ενώ με την επιβεβαίωση αυτού, όλες οι εγγραφές που εμπεριέχονται σε αυτό αποκτούν μια μοναδικότητα, η οποία αποτρέπει τυχόν διπλοεγγραφές[156].

Στην πράξη, οι ποσότητες υπολογιστικής ισχύος που απαιτούνται για την δημιουργία ενός μπλοκ και για την ενημέρωση της αλυσίδας είναι πάρα πολύ μεγάλες και αυτό οφείλεται αφενός στο πλήθος των υπολογιστών που καταναλώνουν τεράστιες ποσότητες ηλεκτρικής ενέργειας και αφετέρου στη χρονική διάρκεια που χρειάζεται για την δημιουργία του μπλοκ. Αν λοιπόν λειτουργήσουν με δόλιους σκοπούς, τότε το μπλοκ θα απορριφθεί και θα έχουν καταναλώσει άχρηστη ενέργεια για την εύρεση λύσης απόδειξης εργασίας, αναλαμβάνοντας επί της ουσίας ένα κόστος του ηλεκτρισμού χωρίς αποζημίωση. Αυτός είναι ο λόγος που η επαλήθευση είναι από τα πλέον σημαντικά χαρακτηριστικά της αποκεντρωμένης συναίνεσης[157].

3.3.1.4. Η συναρμολόγηση και η επιλογή αλυσίδας

Τέλος, το τέταρτο βήμα στον μηχανισμό αποκεντρωμένης συναίνεσης του Bitcoin περιλαμβάνει τη συναρμολόγηση του μπλοκ στις αλυσίδες και την επιλογή της αλυσίδας με την περισσότερη απόδειξη εργασίας. Μόλις επιβεβαιωθεί ένα μπλοκ, συνδέεται με το προηγούμενο σχηματίζοντας το Blockchain. Η αλυσίδα αυτή είναι κατανεμημένη στους επιμέρους κόμβους. Το κάθε μπλοκ που δημιουργείται είναι άφθαρτο, πράγμα που σημαίνει ότι δεν μπορεί να διαγραφεί, αλλά ότι η ταυτότητα και οι πληροφορίες του παραμένουν εγγεγραμμένες για πάντα[158].

---

[156] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ 221-222, *Θεοδωράκης, Ν., Καλογεράκης Γ* σελ.10, *Antonopoulos, A.*, ό.π., σελ. 238-239, *Chytis, E., Kitsantas, T. and Vazakidis, A.*, ό.π., σελ 2, *Ghimire, H., Selvaraj, H.* σελ.4, *Vallois, V., Guenane, F.*, ό.π., σελ. 66.

[157] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 10, *Antonopoulos, A.*, ό.π., σελ. 238-239.

[158] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 835, . *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 3.

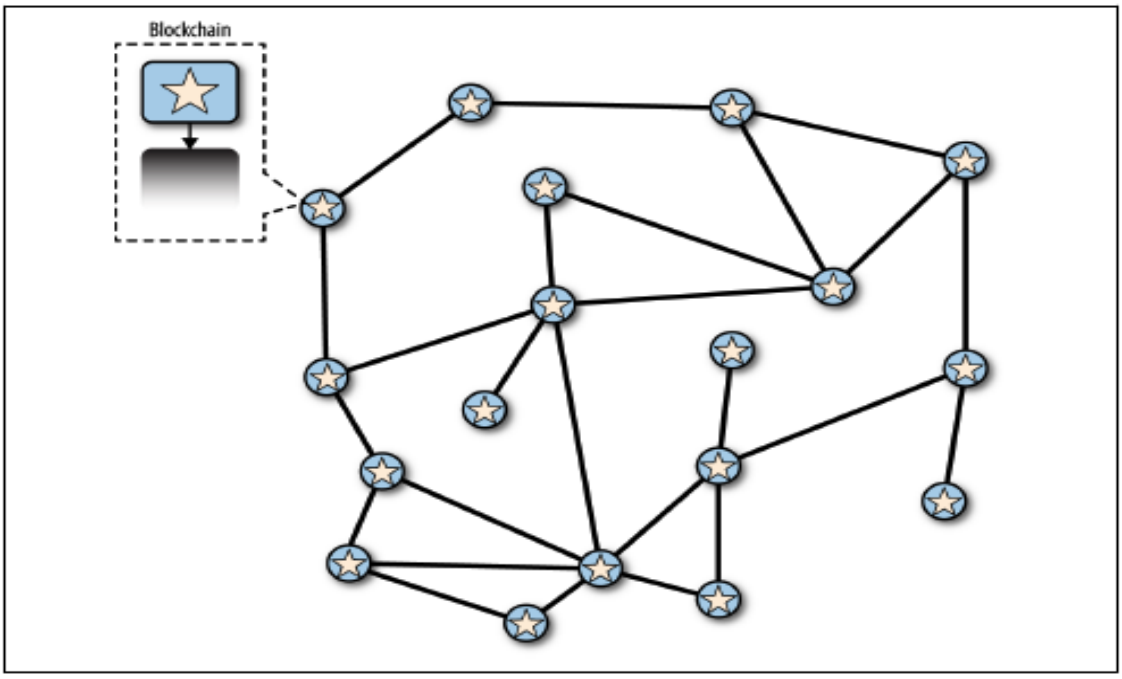
Οι κόμβοι διατηρούν τρεις κατηγορίες με μπλοκ. Η πρώτη περιέχει αυτά που είναι συνδεδεμένα στην κύρια αλυσίδα. Η δεύτερη περιέχει όσα δεν έχουν μητρικό στις γνωστές αλυσίδες και τα οποία καλούνται ορφανά μπλοκ. Και η τρίτη κατηγορία περιέχει τα μπλοκ που σχηματίζουν κλάδους από την κύρια αλυσίδα[159].

α) Κύρια αλυσίδα είναι αυτή που σε οποιαδήποτε χρονική στιγμή έχει αθροιστικά την περισσότερη δυσκολία. Συνήθως είναι η αλυσίδα με τα περισσότερα μπλοκ. Όταν λαμβάνεται ένα νέο μπλοκ, ο κόμβος θα προσπαθήσει να το βάλει μέσα στην υπάρχουσα αλυσίδα, ελέγχοντας τον κατακερματισμό του μητρικού μπλοκ. Έπειτα, ο κόμβος θα επιχειρήσει να βρει το μητρικό στην υπάρχουσα Blockchain. Τις περισσότερες φορές, το μητρικό θα είναι η κορυφή της κύριας αλυσίδας, που σημαίνει ότι το νέο μπλοκ θα επεκτείνει την κύρια αλυσίδα. Μερικές φορές το νέο μπλοκ επεκτείνει μία αλυσίδα που δεν είναι η κύρια. Στην περίπτωση αυτή, ο κόμβος θα προσαρτήσει το νέο μπλοκ στη δευτερεύουσα αλυσίδα και έπειτα θα συγκρίνει την απόδειξη εργασίας της δευτερεύουσας με την κύρια αλυσίδα. Εάν η δευτερεύουσα αλυσίδα έχει περισσότερη δυσκολία αθροιστικά από ότι η κύρια, ο κόμβος θα ανασυγκλίνει στην δευτερεύουσα αλυσίδα, επιλέγοντάς την ως νέα κύρια αλυσίδα και ορίζοντας την παλιά αλυσίδα από κύρια σε δευτερεύουσα. Εάν ο κόμβος είναι κόμβος εξόρυξης, το επόμενο μπλοκ που θα κατασκευάσει θα επεκτείνει τη νέα και μακρύτερη αλυσίδα. Η επιλογή της μακρύτερης αλυσίδας γίνεται για λόγους προστασίας του δικτύου Bitcoin σε περίπτωση επιθέσεων, καθώς η αλλαγή ενός μπλοκ στο Blockchain θα απαιτούσε επανυπολογισμό των αποδείξεων εργασίας όλων των επόμενων μπλοκ[160].

β) Κάποιες φορές όταν δυο μπλοκ εξορύσσονται με μικρή διαφορά χρόνου μεταξύ τους, μπορεί να φτάσουν με αντίστροφη σειρά σε έναν κόμβο, δηλαδή πρώτα το παιδικό και μετά το μητρικό. Το μητρικό μπλοκ επειδή δεν είχε αρκετό χρόνο για να διαδοθεί μέσω του δικτύου, δεν βρίσκεται ακόμα στην κορυφή της αλυσίδας. Στην περίπτωση αυτή ο κόμβος αντιλαμβάνεται ότι δεν έχει λάβει ακόμα το μητρικό μπλοκ και το ζητάει από το δίκτυο. Αυτά τα μπλοκ χαρακτηρίζονται ως ορφανά, είναι όμως έγκυρα και αφού επικυρωθούν αποθηκεύονται στην ομάδα ορφανών μπλοκ μέχρι ότου ληφθεί το μητρικό τους. Μόλις

[159] Βλ. *Vallois, V., Guenane, F.*, ό.π., σελ. 64.
[160] Βλ. *Antonopoulos, A.*, ό.π., σελ. 239-240, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 20.

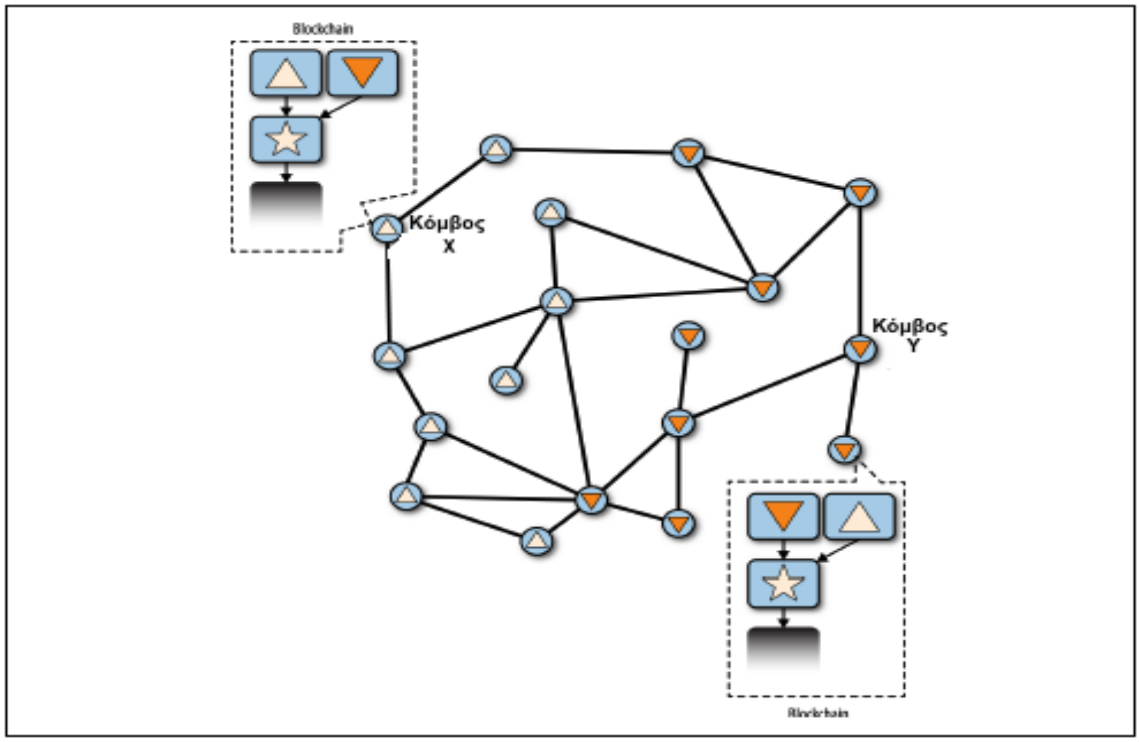
λαμβάνεται το μητρικό και συνδέεται με τις υπάρχουσες αλυσίδες, το ορφανό εξάγεται από την ομάδα και συνδέεται με το μητρικό, κάνοντάς το κομμάτι της αλυσίδας[161].
γ) Κάποιες φορές τα αντίγραφα της αλυσίδας των μπλοκ δεν είναι απόλυτα συνεπή μεταξύ τους, εξαιτίας του ότι οι κόμβοι έχουν διαφορετικές οπτικές του Blockchain.



Εικόνα 10: Το δίκτυο πριν από τη διακλάδωση[162].

Αυτό συμβαίνει όταν δύο ή περισσότεροι εξορύκτες λύνουν τον αλγόριθμο απόδειξης εργασίας σε παραπλήσιους χρόνους, οπότε δημιουργούν ταυτόχρονα από ένα μπλοκ ο καθένας. Επομένως και οι δύο κόμβοι μεταδίδουν ταυτόχρονα διαφορετικές «εκδόσεις» του επόμενου μπλοκ, οι οποίες όμως έχουν το ίδιο μητρικό μπλοκ.

[161] Βλ. *Antonopoulos, A.*, ό.π., σελ. 240, *Vallois, V., Guenane, F.*, ό.π., σελ. 64, *Nakamoto, S.*, ό.π., σελ. 4.
[162] Βλ. *Antonopoulos, A.*, ό.π., σελ. 240.



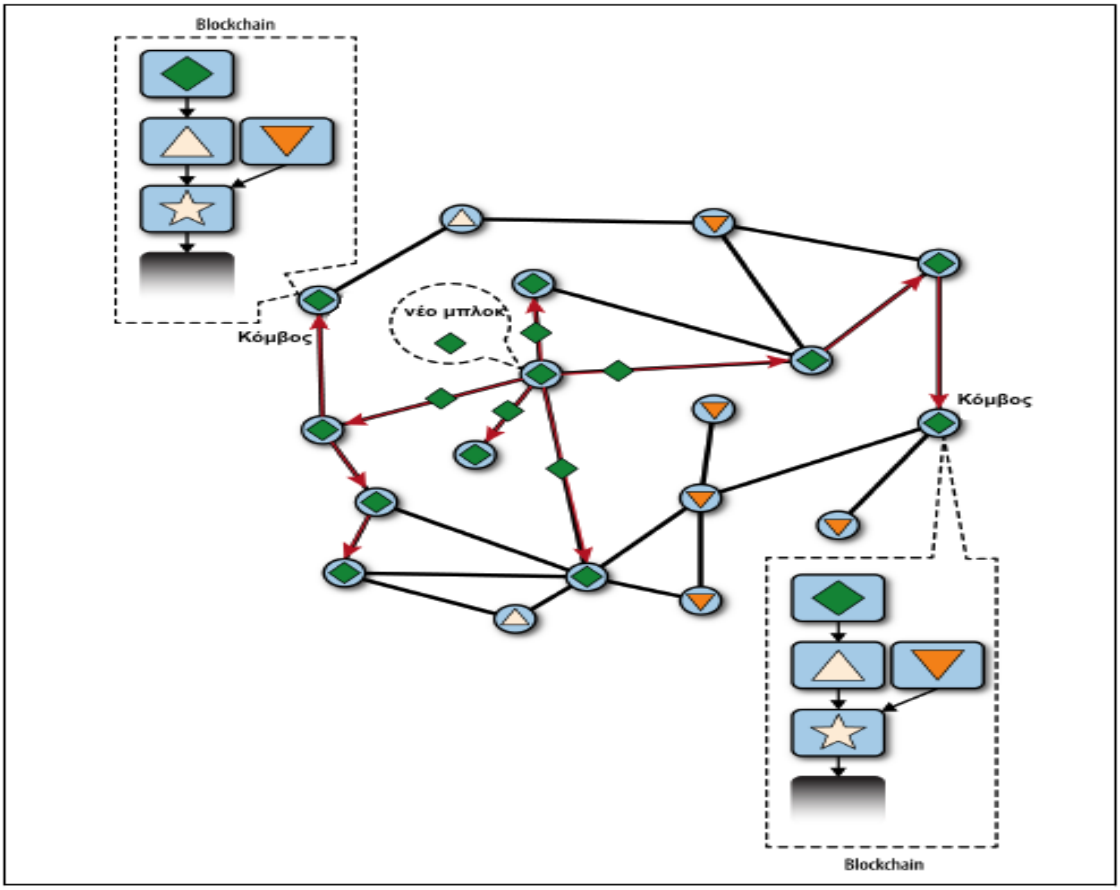
Εικόνα 11: Διακλάδωση όταν δυο μπλοκ εξορύσσονται ταυτόχρονα[163].

Οι διακλαδώσεις επιλύονται λόγω των νέων μπλοκ που προστίθενται σε μία από αυτές. Κάθε κόμβος που λαμβάνει ένα έγκυρο μπλοκ το ενσωματώνει στο Blockchain του, επεκτείνοντας το κατά ένα μπλοκ. Εάν αργότερα ο κόμβος αυτός «δει» κάποιο άλλο υποψήφιο μπλοκ το οποίο συνδέεται με το ίδιο μητρικό που είχε το τελευταίο μπλοκ που έχει ενσωματώσει, τότε το συνδέει σε μία δευτερεύουσα αλυσίδα. Έτσι, κάποιοι κόμβοι πρώτα θα δουν το ένα υποψήφιο μπλοκ, ενώ άλλοι κόμβοι θα δουν το άλλο υποψήφιο μπλοκ με αποτέλεσμα να αναδυθούν δύο ανταγωνιστικές «εκδόσεις» Blockchain, οι οποίες είναι αμφότερες έγκυρες[164].

Η προσωρινή σύγκρουση που δημιουργείται, επιλύεται μέσω του κανόνα της υπερίσχυσης της μακρύτερης αλυσίδας μπλοκ. Σύμφωνα με την αρχή της πλειοψηφίας, τεκμαίρεται ότι η μακρύτερη αλυσίδα έχει ενσωματώσει μεγαλύτερο συνολικό αριθμό συναινέσεων των κόμβων και αντιπροσωπεύει την περισσότερη απόδειξη εργασίας. Η αλυσίδα αυτή καλείται αλυσίδα μεγαλύτερης αθροιστικής δυσκολίας. Άρα, η λύση για το

[163] Βλ. *Antonopoulos, A.*, ό.π., σελ. 243.
[164] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 10, *Antonopoulos, A.*, ό.π., σελ. 240, 242-243, *Nakamoto, S.*, ό.π., σελ. 3, *Vallois, V., Guenane, F.*, ό.π., σελ. 64.

ποια θα είναι η κύρια αλυσίδα δίνεται όταν βρεθεί η επόμενη απόδειξη της εργασίας και η μία αλυσίδα επεκταθεί κατά ένα μπλοκ[165].



Εικόνα 12: Το δίκτυο μετά την επικράτηση της μακρύτερης αλυσίδας[166].

Ακόμα και αν η ισχύς κατακερματισμού είναι μοιρασμένη ισόποσα, είναι πολύ πιθανό μια ομάδα εξορυκτών να βρει πρώτη μία λύση και να τη διαδώσει. Με την άθροιση της καταγεγραμμένης δυσκολίας από κάθε μπλοκ που υπάρχει στην αλυσίδα, ένας κόμβος μπορεί να υπολογίσει τη συνολική ποσότητα απόδειξης εργασίας, που έχει καταναλωθεί για τη δημιουργία αυτής της αλυσίδας. Όσο όλοι οι κόμβοι επιλέγουν την αλυσίδα μεγαλύτερης

[165] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 10, *Antonopoulos, A.*, ό.π., σελ. 240, *Belotti, M., AA et al.,*, ό.π., σελ. 35-36, Bissia, ό.π., σελ. 19, Eyal, I., Sirer, *E. G.*, 2013. *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*. [online]. International Conference on Financial Cryptography and Data Security. 15 November 2013, σελ. 4. Available at: https://www.researchgate.net/publication/258224002_Majority_Is_Not_Enough_Bitcoin_Mining_Is_Vulnerable (Accessed 28/01/2021), *Vallois, V., Guenane, F.*, ό.π., σελ. 64, *Nakamoto, S.*, ό.π., σελ. 1,3.

[166] Βλ. *Antonopoulos, A.*, ό.π., σελ. 246.

αθροιστικά δυσκολίας, το παγκόσμιο δίκτυο Bitcoin συγκλίνει τελικά σε μία συνεπή κατάσταση[167].

3.3.2. Οι επιθέσεις συναίνεσης

Ο μηχανισμός συναίνεσης του Bitcoin είναι ευάλωτος στις επιθέσεις από μεμονωμένους εξορύκτες ή από ομάδες αυτών[168], που επιχειρούν να χρησιμοποιήσουν την ισχύ κατακερματισμών με ανέντιμους ή καταστροφικούς σκοπούς. Οι επιθέσεις συναίνεσης δεν επηρεάζουν την ασφάλεια των ιδιωτικών κλειδιών και τον αλγόριθμο υπογραφής. Μία επίθεση συναίνεσης δεν μπορεί να κλέψει BTC, δεν μπορεί να ξοδέψει BTC χωρίς υπογραφές, δεν μπορεί να ανακατευθύνει BTC ή αλλιώς να αλλάξει τις παλιές συναλλαγές ή την κυριότητα των UTXO. Μπορεί μόνο να επηρεάσει τα πιο πρόσφατα μπλοκ και να προκαλέσει επιπλοκές άρνησης υπηρεσιών στη δημιουργία μελλοντικών μπλοκ. Η ασφάλεια και διαθεσιμότητα του δικτύου του Bitcoin μπορεί να διαταραχθεί μόνο αν κάποιος εξορύκτης αποκτήσει περισσότερη υπολογιστική ισχύ από αυτήν, που έχει η πλειοψηφία των κόμβων συνολικά. Έτσι, οι διάφοροι τύποι επιθέσεων κατά της συναίνεσης καθίστανται εφικτοί τουλάχιστον με 30%[169] της ισχύος των κατακερματισμών του δικτύου[170].

Αν υποτεθεί ότι μια ομάδα εξορυκτών ελέγχουν την πλειοψηφία της συνολικής ισχύος κατακερματισμών του δικτύου και συνωμοτούν μεταξύ τους, μπορούν να προκαλέσουν επιτηδευμένες διακλαδώσεις στο Blockchain και με τον τρόπο αυτό να διπλοξοδέψουν συναλλαγές ή να εκτελέσουν επιθέσεις άρνησης υπηρεσιών εναντίον συγκεκριμένων συναλλαγών ή διευθύνσεων ή απλώς να επιδιώκουν τη δολιοφθορά του δικτύου Bitcoin.

α) Μία επίθεση διπλοξοδέματος μπορεί να συμβεί με δύο τρόπους. Είτε πριν να επιβεβαιωθεί μία συναλλαγή, είτε όταν ο επιτιθέμενος εκμεταλλεύεται μία διακλάδωση της

[167] Το διάστημα 10 λεπτών των μπλοκ του Bitcoin είναι ένας σχεδιαστικός συμβιβασμός μεταξύ γρήγορων χρονικά επιβεβαιώσεων (δηλαδή διευθέτηση των συναλλαγών) και της πιθανότητας μιας διακλάδωσης. Ένας γρηγορότερος χρόνος εύρεσης μπλοκ θα έκανε την εκκαθάριση των συναλλαγών γρηγορότερη, αλλά θα οδηγούσε σε συχνότερες διακλαδώσεις της αλυσίδας των μπλοκ, ενώ ένας πιο αργός χρόνος θα μείωνε τον αριθμό των διακλαδώσεων, αλλά θα έκανε τη διευθέτηση των συναλλαγών πιο αργή, βλ. *Antonopoulos, A.*, ό.π., σελ. 241, 244, 247.

[168] Οι ομάδες δημιουργούν ολόκληρες φάρμες εξόρυξης. Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 9.

[169] Το όριο του 51% είναι το επίπεδο εκείνο στο οποίο είναι σχεδόν βέβαιη η επιτυχία του εγχειρήματος. Απλά με λιγότερη επεξεργαστική ισχύ κατακερματισμών, η πιθανότητα για επιτυχία μειώνεται, επειδή άλλοι έντιμοι εξορύκτες ελέγχουν τη δημιουργία κάποιων μπλοκ, βλ. *Antonopoulos, A.*, ό.π., σελ. 255.

[170] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ*, ό.π., σελ. 9, *Antonopoulos, A.*, ό.π., σελ. 255, Βλ. *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 25.

αλυσίδας των μπλοκ για να αναιρέσει αρκετά μπλοκ. Ο επιτιθέμενος προκαλεί μπλοκ που έχουν επαληθευτεί μπλοκ προηγουμένως να ακυρωθούν, δημιουργώντας διακλαδώσεις κάτω από αυτά και συγκλίνοντας σε μια εναλλακτική αλυσίδα. Το διπλοξόδεμα μπορεί να συμβεί μόνο στις συναλλαγές του ίδιου του επιτιθέμενου, καθώς μόνο σε αυτές τις συναλλαγές μπορεί αυτός να παράγει μία έγκυρη υπογραφή. Επιτρέπει λοιπόν στους επιτιθέμενους να διπλοξοδέψουν τις δικές τους συναλλαγές στη νέα αλυσίδα, αναιρώντας την αντίστοιχη συναλλαγή στην παλιά αλυσίδα. Για να προστατευθεί κάποιος από τέτοιου είδους επιθέσεις, πρέπει να περιμένει να γίνουν τουλάχιστον έξι επιβεβαιώσεις, καθώς όσο πιο πολλές είναι οι επιβεβαιώσεις, τόσο πιο δύσκολο είναι να παραβιαστεί μια συναλλαγή.

β) Η πρόκληση άρνησης υπηρεσιών συνοδεύεται από μία παρατεταμένη άρνηση της υπηρεσίας για μία ή πολλές συγκεκριμένες διευθύνσεις. Ένας επιτιθέμενος, που κατέχει την πλειοψηφία της επεξεργαστικής ισχύος της εξόρυξης, μπορεί να αγνοήσει συγκεκριμένες συναλλαγές, οι οποίες περιλαμβάνονται σε ένα μπλοκ που έχει ήδη εξορυχθεί από άλλον εξορύκτη. Για να το καταφέρει αυτό, θα δημιουργήσει μία διακλάδωση, ώστε να προκαλέσει την εκ νέου εξόρυξη αυτού του μπλοκ και έτσι να εξαιρέσει τις συγκεκριμένες συναλλαγές[171].

γ) Δεν έχουν όμως όλοι οι επιτιθέμενοι ως κίνητρο το κέρδος. Μία ακόμα υπόθεση επίθεσης είναι όταν ένας επιτιθέμενος σκοπεύει να διαταράξει το δίκτυο του Bitcoin, χωρίς καμμία επιθυμία να επωφεληθεί από κάτι τέτοιο. Οι προθέσεις του αποσκοπούν μόνο στο να ακρωτηριάσει το δίκτυο του Bitcoin. Προκειμένου όμως να το πετύχει θα πρέπει να κάνει μια κολοσσιαία επένδυση και με συγκεκαλυμμένο σχεδιασμό. Αν και θεωρητικά, αυτό θα μπορούσε να υποστηριχτεί από κάποιον που διαθέτει πολλούς πόρους, ο οποίος παράλληλα θα έκανε συμπαιγνία με χειριστές ομάδων ή και επίθεση άρνησης υπηρεσιών σε άλλες ομάδες.

Στην πράξη, όσο περνάει ο χρόνος το Blockchain γίνεται περισσότερο αμετάβλητο. Όσο αυξάνεται το ύψος των μπλοκ, τόσο μεγαλώνει η υπολογιστική ισχύς που χρειάζεται ώστε μια διακλάδωση να γίνει πολύ βαθιά, γεγονός που καθιστά τα παλαιά μπλοκ πρακτικά αμετάβλητα. Καθίσταται επομένως υπερβολικά ασύμφορο για κάποιον να κάνει επίθεση με

[171] Βλ. *Antonopoulos, A.*, ό.π., σελ. 254-255, *Bissias, G., AA et al.*, ό.π., σελ. 2, *Eyal, I., Sirer, E. G.*, ό.π., σελ. 1, Frankenfield, J., 2019. 51% Attack. Available at: https://www.investopedia.com/terms/1/51-attack.asp (Accessed 27/01/2021), Haslhofer, B., Judmayer, A., Romiti, M. & Zamyatin, A., 2019. *A Deep Dive into Bitcoin Mining Pools.* σελ. 1 Available at: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_30.pdf (Accessed 03/06/2021), , *Nakamoto, S.*, ό.π., σελ. 6.

σκοπό να προβεί σε αλλοίωση των συναλλαγών. Όσο πιο μεγάλο μέρος της ισχύος κατακερματισμού είναι υπό τον έλεγχο έντιμων εξορυκτών, τόσο πιο μεγάλη ασφάλεια παρέχεται προς αποτροπή βίαιων επιθέσεων κατάκτησης του δικτύου[172].

3.4. Η ανταμοιβή των εξορυκτών

Οι εξορύκτες λαμβάνουν δύο τύπους ανταμοιβών, οι οποίες τους παρακινούν να ανταγωνίζονται συνεχώς στον αγώνα για την εύρεση ενός έγκυρου μπλοκ και οι οποίες είναι τα νέα ψηφιακά νομίσματα και οι χρεώσεις συναλλαγών.

α) Οι εξορύκτες λαμβάνουν νέα ψηφιακά νομίσματα λόγω της συμβολής τους στην επίλυση για την εύρεση λύσης στην απόδειξη εργασίας. Η διαδικασία δημιουργίας νέων ψηφιακών νομισμάτων είναι σχεδιασμένη να προσομοιώνει σε φθίνουσα αποδοτικότητα της τάξεως 50%. Ο ρυθμός δημιουργίας των BTC και ο συνολικός αριθμός που θα υπάρξει ποτέ είναι εξαρχής προσχεδιασμένος. Δεδομένου λοιπόν ότι υπάρχει περιορισμένος αριθμός BTC, το ποσό των νέων δημιουργημένων BTC, που ένας εξορύκτης μπορεί να προσθέσει σε ένα μπλοκ, μειώνεται κάθε 210000 μπλοκ ή περίπου κάθε τέσσερα χρόνια. Τον Ιανουάριο του 2009 ξεκίνησε από 50 BTC ανά μπλοκ και υποδιπλασιάστηκε τον Νοέμβριο του 2012 σε 25 BTC ανά μπλοκ, τον Ιούλιο του 2016 σε 12,5 BTC ανά μπλοκ, το Μάϊο του 2020 σε 6,25 BTC ανά μπλοκ και κάποια στιγμή το 2024 θα φτάσει τα 3,125 BTC ανά μπλοκ. Δεδομένου ότι αυτή η επιβράβευση μειώνεται γεωμετρικά με την πάροδο του χρόνου, αυτό σημαίνει ότι δεν θα υπάρξουν ποτέ περισσότερα από 21000000 BTC. Συγκεκριμένα μετά το 2140, δεν θα εκδοθεί κανένα νέο BTC.

β) Οι εξορύκτες κερδίζουν επίσης μέσω των χρεώσεων των συναλλαγών. Κάθε συναλλαγή ενδέχεται να περιλαμβάνει μία χρέωση συναλλαγής, στη μορφή ενός περισσεύματος από BTC ανάμεσα στις εισόδους και τις εξόδους της συναλλαγής. Ο νικητής εξορύκτης που θα βρει τη λύση αμείβεται με αυτές τις χρεώσεις συναλλαγών που περιλαμβάνονται στο νικητήριο μπλοκ. Οι χρεώσεις συναλλαγών δεν υπολογίζονται με βάση την αξία της συναλλαγής, αλλά με βάση το μέγεθος της συναλλαγής σε Kbyte. Οι χρεώσεις αυτές λειτουργούν ως κίνητρο για την ενσωμάτωση μίας συναλλαγής στο επόμενο μπλοκ, αλλά

[172] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 220, *Antonopoulos, A.*, ό.π., σελ. 237, 253- 256, *Chytis, E., Kitsantas, T. and Vazakidis, A.*, ό.π., σελ. 2, *Frankenfield, J.*, ό.π.

και ως αντικίνητρο για οποιουδήποτε τύπου κατάχρηση του συστήματος. Αν και η χρέωση συναλλαγής είναι εθελοντική, στην πράξη όσο υψηλότερο είναι το τέλος συναλλαγής, τόσο πιο γρήγορα μπορεί να εκτελεστεί και να επιβεβαιωθεί η συναλλαγή[173].

Στην πράξη, καθώς η ανταμοιβή μειώνεται με τον χρόνο και ο αριθμός των συναλλαγών ανά μπλοκ αυξάνεται, το μεγαλύτερο ποσοστό των κερδών της εξόρυξης BTC θα προέρχεται από τις χρεώσεις. Όταν το τελευταίο satoshi, που αντιστοιχεί σε 0,00000001 ενός BTC, παραχθεί μέσω εξόρυξης, οι εξορύκτες που θα συνεχίσουν να συνεισφέρουν την υπολογιστική τους δύναμη επαληθεύοντας τις συναλλαγές, θα αμείβονται αποκλειστικά με τα τέλη συναλλαγής. Έτσι μετά το 2140, όλα τα κέρδη των εξορυκτών του Bitcoin θα είναι στη μορφή των χρεώσεων συναλλαγών. Με τον τρόπο αυτό διασφαλίζεται ότι το κίνητρο των εξορυκτών θα παραμείνει ακέραιο, ώστε αυτοί να διατηρούν σε λειτουργία το δίκτυο ακόμη και μετά την εξόρυξη του τελευταίου BTC[174].

3.5. Οι ομάδες εξόρυξης

Στα πρώτα χρόνια λειτουργίας του Bitcoin, την δημιουργία ενός μπλοκ μπορούσε να επιτελέσει ένας κοινός υπολογιστής. Σήμερα δεν υπάρχει αυτή η δυνατότητα, αν ο υπολογιστής δεν είναι εφοδιασμένος με την κατάλληλη επεξεργαστική ισχύ. Με την πάροδο του χρόνου μεμονωμένοι εξορύκτες που εργάζονται ατομικά δεν έχουν καμία τύχη, καθώς η πιθανότητα να βρουν μπλοκ ώστε να αντισταθμίζουν το κόστος του ηλεκτρισμού και του εξοπλισμού είναι πολύ χαμηλή. Ακόμα και το γρηγορότερο σύστημα εξόρυξης δεν μπορεί να ανταπεξέλθει σε σύγκριση με τις βιομηχανικές εγκαταστάσεις που στοιβάζουν χιλιάδες τέτοια τσιπ σε γιγαντιαίες αποθήκες πλησίον υδροηλεκτρικών σταθμών ενέργειας. Για το λόγο αυτό, οι εξορύκτες άρχισαν να ενώνουν τις δυνάμεις τους και να δημιουργούν ομάδες εξόρυξης ή αλλιώς mining pools που είτε έχουν κεντρική διαχείριση είτε όχι[175].

---

[173] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 835, *Κεχαγιά, Χ.*, ό.π., σελ 3, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 497-498, *Antonopoulos, A.*, ό.π., σελ. 18, 24, 121, 127, 132, *Gao, Y., AA et al.*, ό.π., σελ. 2, *Ferrer-Gomila, J., AA et al.*, ό.π., σελ. 2,6, *Gajdek, S., Kozak, S.* , ό.π., σελ. 7, *Ghimire, H., Selvaraj, H.*, ό.π., σελ. 3,5, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 19-20, *Nakamoto, S.*, ό.π., σελ. 4, *Pérez-Solà, S., AA et al.*, ό.π., σελ. 2.

[174] Βλ. *Antonopoulos, A.*, ό.π., σελ. 214-215, *Bissias, G., AA et al.*, ό.π., σελ. 19, *Gajdek, S., Kozak, S.* ό.π., σελ. 3, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ.13-14, 20, *Gajdek, S., Kozak, S.* ό.π., σελ. 3, *Nakamoto, S.*, ό.π., σελ. 4, Bongcayao, R.J., ό.π., σελ. 5.

[175] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 835, *Bissias, G., AA et al.*, ό.π., σελ. 19, *Haslhofer, B., Judmayer, A., Romiti, M. & Zamyatin, A.*, ό.π., σελ. 3.

1) Με κεντρική διαχείριση

Οι ομάδες εξόρυξης συντονίζουν πολλές εκατοντάδες ή χιλιάδες εξορύκτες μέσω εξειδικευμένων πρωτοκόλλων ομαδικής εξόρυξης και είναι ανοιχτές σε οποιονδήποτε εξορύκτη, μικρό ή μεγάλο, επαγγελματία ή ερασιτέχνη. Μία ομάδα μπορεί να έχει μερικούς συμμετέχοντες, είτε με ένα μόνο μικρό μηχάνημα εξόρυξης, είτε με ένα γκαράζ γεμάτο από τελευταίας τεχνολογίας εξοπλισμό. Οι μεμονωμένοι εξορύκτες, αφού δημιουργήσουν έναν λογαριασμό για την ομάδα, ρυθμίζουν τον εξοπλισμό τους ώστε να συνδέεται και να παραμένει συνδεδεμένος στον διακομιστή της όσο αυτή κάνει εξόρυξη, ενώ παράλληλα συγχρονίζουν και ομαδοποιούν την ισχύ των κατακερματισμών που διαθέτουν με τους υπόλοιπους εξορύκτες[176].

Οι ομάδες εξόρυξης φέρονται ως μονάδα έχοντας μια κεντρική διαχείριση, που είναι είτε κάποια εταιρία είτε κάποιος ιδιώτης, ο οποίος διαχειρίζεται τον διακομιστή της ομάδας και είναι ο χειριστής της. Ο διακομιστής της ομάδας τρέχει εξειδικευμένο λογισμικό με ένα πρωτόκολλο ομαδικής εξόρυξης, το οποίο συντονίζει τις δραστηριότητες των εξορυκτών της ομάδας, είναι συνδεδεμένος σε έναν ή περισσότερους πλήρεις κόμβους Bitcoin, έχει απευθείας πρόσβαση σε πλήρες αντίγραφο της Blockchain βάσης δεδομένων και επαληθεύει μπλοκ και συναλλαγές για χάρη των εξορυκτών.

Στην πράξη, ο διακομιστής της ομάδας κατασκευάζει ένα υποψήφιο μπλοκ συγκεντρώνοντας συναλλαγές, προσθέτοντας μία συναλλαγή coinbase, υπολογίζοντας τη ρίζα Merkle και συνδέοντας το υποψήφιο μπλοκ με τον κατακερματισμό του προηγούμενου μπλοκ. Στη συνέχεια, η κεφαλίδα του υποψήφιου μπλοκ αποστέλλεται σε κάθε έναν από τους εξορύκτες της ομάδας, ως έτοιμο πρότυπο. Η ομάδα εξόρυξης θέτει έναν κατώτερο στόχο δυσκολίας για το κέρδος ενός μεριδίου, συνήθως 1000 φορές πιο εύκολο από τη συνολική δυσκολία του δικτύου του Bitcoin. Με τον τρόπο αυτό παρέχεται κίνητρο στους μικρότερους εξορύκτες, ώστε να αξίζει τον κόπο η συνεισφορά τους. Κάθε φορά που ένας εξορύκτης της ομάδας βρίσκει έναν κατακερματισμό κεφαλίδας μικρότερο της δυσκολίας που τέθηκε για την ομάδα, αποδεικνύει ότι αυτός έχει κάνει την εργασία των κατακερματισμών για να βρει το αποτέλεσμα. Χιλιάδες εξορύκτες που προσπαθούν να

[176] Βλ. *Antonopoulos, A.*, ό.π., σελ. 250-251.

βρουν μικρές τιμές κατακερματισμών τελικά θα βρουν μία ικανοποιητικά χαμηλή τιμή που θα ικανοποιεί τον στόχο του δικτύου Bitcoin[177].

Με τη συμμετοχή τους σε μία ομάδα, οι εξορύκτες ανταμείβονται συνήθως κάθε μέρα με μικρότερο μεν μερίδιο της συνολικής αμοιβής, αλλά χωρίς να χρειάζεται τεράστιο ρίσκο και εξασφαλίζουν τακτικά έσοδα. Τα επιτυχημένα μπλοκ πληρώνουν την ανταμοιβή σε μία διεύθυνση Bitcoin της ομάδας, αντί σε διεύθυνση των μεμονωμένων εξορυκτών. Περιοδικά, ο διακομιστής της ομάδας στέλνει τις ανταμοιβές στις διευθύνσεις των εξορυκτών, ανάλογα με το μερίδιο συνεισφοράς που είχαν στη διαδικασία της εξόρυξης, ενώ παράλληλα χρεώνει και μία ποσοστιαία χρέωση ως παροχή για τις υπηρεσίες που τους έχει προσφέρει συνολικά[178].

Αν και γενικά το σύστημα θεωρείται ότι είναι ασφαλές, διότι οι έντιμοι κόμβοι έχουν συλλογικά περισσότερη υπολογιστική ισχύ από οποιαδήποτε ομάδα συνεργαζόμενων κόμβων-εισβολέων, ωστόσο το γεγονός ότι ο χειριστής της ομάδας είναι αυτός που ελέγχει την κατασκευή των υποψήφιων μπλοκ και το ποιες συναλλαγές περιλαμβάνονται, του δίνει τη δύναμη να εξαιρεί συναλλαγές ή να εισάγει συναλλαγές διπλοξοδέματος. Μια τέτοια κατάχρηση εξουσίας μπορεί να λαμβάνει χώρα με περιορισμένο και ανεπαίσθητο τρόπο, ώστε ο χειριστής να επωφεληθεί από μία επίθεση συναίνεσης χωρίς να γίνεται αντιληπτό. Επιπλέον, εάν ο διακομιστής της ομάδας βρεθεί εκτός σύνδεσης ή καθυστερήσει από κάποια επίθεση άρνησης υπηρεσιών, οι εξορύκτες της ομάδας δεν μπορούν να κάνουν εξόρυξη[179].

2) Χωρίς κεντρική διαχείριση

Η Peer-to-Pool (στο εξής P2Pool) εξόρυξη είναι μια αποκεντρωμένη ομαδική εξόρυξη, η οποία δημιουργήθηκε για την επίλυση των προβλημάτων που προκύπτουν από την ύπαρξη κεντρικής διαχείρισης. Η P2Pool εξόρυξη είναι μία υβριδική προσέγγιση, η οποία παρέχει το πλεονέκτημα των πολύ πιο συχνών πληρωμών σε σχέση με την μεμονωμένη εξόρυξη, χωρίς να δίνει μεγάλο έλεγχο στον χειριστή ομάδας, όπως συμβαίνει στις ομάδες κεντρικής διαχείρισης. Στην P2Pool εξόρυξη οι εξορύκτες της ομάδας λειτουργούν περισσότερο μεμονωμένα, κατασκευάζοντας τα δικά τους υποψήφια μπλοκ και συγκεντρώνοντας συναλλαγές, κάνουν όμως συνεργατική εξόρυξη στην κοινή αλυσίδα.

[177] Βλ. Ibid σελ. 251-252, *Eyal, I., Sirer, E. G.*, ό.π., σελ. 5.
[178] Βλ. *Αρχοντάκη, Α., Simsive, P.*, ό.π., σελ. 835, *Antonopoulos, A.*, ό.π., σελ. 250-251, *Eyal, I., Sirer, E. G.*, ό.π., σελ. 4.-5
[179] Βλ. *Antonopoulos, A.*, ό.π., σελ. 252, 256, *Nakamoto, S.*, ό.π., σελ. 1.

Η εξόρυξη αυτή είναι αρκετά πιο περίπλοκη από την εξόρυξη κεντρικής διαχείρισης, επειδή οι εξορύκτες χρειάζεται να χρησιμοποιούν αποκλειστικά γι' αυτήν την εργασία έναν υπολογιστή που να διαθέτει αρκετό χώρο στο δίσκο, μνήμη και εύρος ζώνης στο διαδίκτυο[180], για την υποστήριξη αφενός ενός πλήρους κόμβου Bitcoin και αφετέρου του λογισμικού ενός P2Pool κόμβου. Οι P2Pool εξορύκτες συνδέουν τον εξοπλισμό εξόρυξής τους στον τοπικό P2Pool κόμβο, ο οποίος προσομοιώνει τις λειτουργίες ενός διακομιστή ομάδας, στέλνοντας πρότυπα μπλοκ στο υλισμικό.

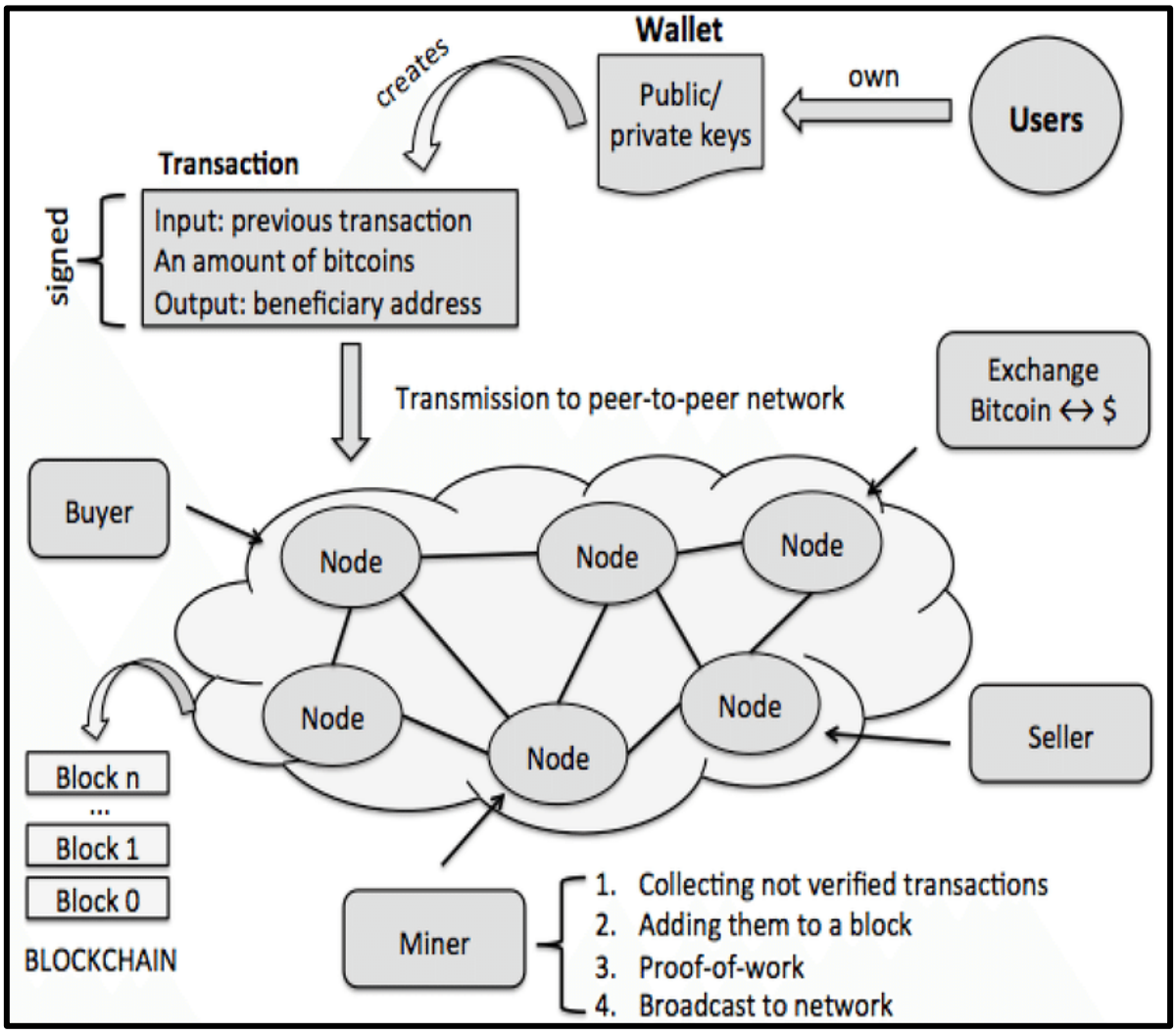
Η ομάδα αυτή αποκεντρώνει τις λειτουργίες του διακομιστή της ομάδας, λειτουργώντας σε ένα σύστημα παρόμοιο με το Blockchain του Bitcoin, το οποίο ονομάζεται κοινή αλυσίδα. Η κοινή αλυσίδα επιτρέπει στους εξορύκτες της ομάδας να συνεργάζονται σε μία αποκεντρωμένη ομάδα και να εξορύσσουν μερίδια στην κοινή αλυσίδα, ακολουθώντας το ρυθμό ενός κοινού μπλοκ ανά 30 δευτερόλεπτα. Ακόμη, τους επιτρέπει να παρακολουθούν όλα τα μερίδια χρησιμοποιώντας έναν μηχανισμό αποκεντρωμένης συναίνεσης, όπως είναι ο μηχανισμός συναίνεσης του Bitcoin. Καθένα από τα μπλοκ της κοινής αλυσίδας καταγράφει το ανάλογο μερίδιο ανταμοιβής, που αντιστοιχεί στους εξορύκτες της ομάδας που συνεισφέρουν εργασία, προωθώντας τα μερίδια από το προηγούμενο κοινό μπλοκ. Αν ένα από αυτά τα κοινά μπλοκ επιτύχει και το στόχο δυσκολίας του δικτύου του Bitcoin, διαδίδεται και περιλαμβάνεται στην αλυσίδα των μπλοκ του Bitcoin. Όλοι δε οι εξορύκτες της ομάδας που συνεισέφερε, ανταμείβονται και με όλα τα μερίδια που προηγήθηκαν από το νικητήριο κοινό μπλοκ.

Η ομάδα αυτή αποκεντρώνει τις λειτουργίες του διακομιστή της ομάδας, λειτουργώντας σε ένα σύστημα παρόμοιο με το Blockchain στο Bitcoin[181].

[180] Εύρος ζώνης (bandwidth) είναι η απόλυτη μέγιστη ποσότητα δεδομένων, που μπορούν να μεταφερθούν μέσω μιας σύνδεσης στο διαδίκτυο κατά τη διάρκεια μιας χρονικής περιόδου. Δεν αναφέρεται στην ταχύτητα μεταφοράς δεδομένων αλλά μόνο στη μέγιστη χωρητικότητα. Μετράται σε bits ανά sec.

[181] Βλ. *Antonopoulos, A.*, ό.π., σελ. 253, P2Pool. l.e. 23.07.2020. Available at: https://en.bitcoin.it/wiki/P2Pool (Accessed 27/01/2021).

Εικόνα 13[182]: **Συνοπτική αποτύπωση της λειτουργίας του δικτύου Bitcoin**



[182] Βλ. Bistarelli, S., Mantilacci, M., Santancini, P. & Santini, F., 2017 . *An End-to-end Voting-system Based on Bitcoin* [online]. Proceedings of the Symposium on Applied Computing. April 2017. p.p 1836–1841. Available at: http://dx.doi.org/10.1145/3019612.3019841 (Accessed 26/05/2021).

Β΄ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 4ο
Η ΣΧΕΣΗ ΤΟΥ BITCOIN ΜΕ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Η χρήση του διαδικτύου είναι τόσο διαδεδομένη πλέον, ώστε να γίνεται λόγος για διαδικτυακό αναλφαβητισμό, όσων δεν γνωρίζουν να το χρησιμοποιούν. Τα ηλεκτρονικά δεδομένα και οι πληροφορίες, τα οποία δημιουργούνται, διακινούνται, γίνονται αντικείμενο επεξεργασίας και αποθηκεύονται σε κάθε είδους ηλεκτρονική συσκευή, όλα συνέβαλλαν στη δημιουργία του «ψηφιακού ανθρώπου». Η εμφάνιση του «ψηφιακού ανθρώπου», σε συνδυασμό με τη ραγδαία ανάπτυξη και εφαρμογή νέων τεχνολογιών πληροφόρησης, πυροδότησε την εμφάνιση νέων μορφών εγκληματικής δραστηριότητας, αποκαλούμενης «ηλεκτρονικό έγκλημα». Αν και δεν υπάρχει κάποιος γενικά αποδεκτός ορισμός, ωστόσο θα μπορούσαμε να εκλάβουμε ως ηλεκτρονικό έγκλημα, αυτό που στρέφεται κατά περιουσιακών και άλλων δικαιωμάτων φυσικών ή νομικών προσώπων και το οποίο συναρτάται αναγκαίως με ηλεκτρονικό υπολογιστή ή δίκτυο υπολογιστών, διασυνδεδεμένων -ή και μη- σε διαδίκτυο. Υπό το πρίσμα λοιπόν του κριτηρίου τέλεσής τους, τα ηλεκτρονικά εγκλήματα διακρίνονται σε τρεις κατηγορίες. Σε αυτά που τελούνται σε κοινό περιβάλλον ή στο διαδίκτυο, σε αυτά που διαπράττονται αποκλειστικά σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς τη χρήση διαδικτύου και στα κυβερνοεγκλήματα, τα οποία ενσωματώνουν το στοιχείο της δικτύωσης. Τα κυβερνοεγκλήματα διακρίνονται στα γνήσια πληροφορικά, τελούμενα μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών όπως είναι η απάτη, στα εγκλήματα με ψηφιακό περιεχόμενο και στα εγκλήματα κατά πληροφοριακών συστημάτων. Στα κύρια χαρακτηριστικά του κυβερνοεγκλήματος περιλαμβάνονται η ευκολία του τρόπου τέλεσης, με χρήση ηλεκτρονικής συσκευής, η ταχύτητα τέλεσης, με αποτέλεσμα να μη γίνονται αντιληπτά από το θύμα και η εκτός κρατικών γεωγραφικών ορίων τέλεση, καθώς οι παραβάσεις μπορούν να διαπράττονται από οποιοδήποτε σημείο, σε βάρος οποιουδήποτε

χρήστη ηλεκτρονικού υπολογιστή ανά την υφήλιο, αποκτώντας με τον τρόπο αυτό παγκόσμιο χαρακτήρα[183].

Ανέκαθεν τα χρήματα χρησιμοποιήθηκαν για την επίτευξη νόμιμων ή και παράνομων σκοπών. Το BTC και η τεχνολογία Blockchain δεν είναι παράνομα εκ φύσεως, αλλά, όπως συμβαίνει με τις περισσότερες τεχνολογικές καινοτομίες, μπορούν να χρησιμοποιηθούν και για καλούς και για κακούς σκοπούς, ανάλογα με τον χρήστη. Ο σκοπός δημιουργίας του Bitcoin ήταν να αποτελέσει ένα εναλλακτικό μέσον πληρωμών που θα λειτουργεί ως χρήμα και θα υφίσταται μόνο στον κυβερνοχώρο, καθώς αντίθετα με τις παραδοσιακές τραπεζικές συναλλαγές, για τη χρήση του δεν απαιτείται η φυσική παρουσία των συναλλασσομένων, ούτε η εποπτεία από κάποια κεντρική αρχή.

Η εμφάνιση νέων οντοτήτων που ανήκουν στο οικοσύστημα του BTC καθιστά μεγαλύτερη την απειλή, που ήδη υπήρχε στον κυβερνοχώρο, καθώς συμβάλλει στην άμεση ενεργοποίηση του κυβερνοεγκλήματος. Εξάλλου στην πράξη, το BTC απεδείχθη πρώτον ότι συμβάλλει στην ανάπτυξη του εγκλήματος ως υπηρεσία (crime as a service) στον κυβερνοχώρο, επειδή οι συναλλαγές με BTC χρησιμοποιήθηκαν νωρίτατα σαν αντικείμενο κατάχρησης και σαν μέσον ανάπτυξης εγκληματικής δραστηριότητας και δεύτερον ότι γίνεται δέλεαρ για την εφαρμογή του ηλεκτρονικού εγκλήματος, με τον ηλεκτρονικό υπολογιστή να γίνεται είτε ο στόχος είτε το υποκείμενο των κυβερνοεγκληματιών[184].

[183] *Ζημιανίτης*, Η τεχνολογία ως το περιβάλλον εκδήλωσης και ανάδειξης συμπεριφορών ως εγκληματικών: Ηλεκτρονικό έγκλημα, διαδικτυακό έγκλημα, παθόντες, έννομα αγαθά και δυνατότητα αντίδρασης, Εισηγητές: Δ. Αναστασόπουλος/Δ. Ζημιανίτης/Μ. Καϊάφα-Γκμπάντι/Ε. Καράντζαλη/Ζ. Καρδασιάδου/Ε. Παπακωνσταντίνου, «Το Δίκαιο στην ψηφιακή εποχή», 3ο Πανελλήνιο Συνέδριο e-ΘΕΜΙΣ, Βόλος, 9-10 Μαρτίου 2012, σελ 162, *Κ. Χ.* Βλαχόπουλος, Κ., 2007. *ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ: ΜΟΡΦΕΣ - ΠΡΟΛΗΨΗ – ΑΝΤΙΜΕΤΩΠΙΣΗ.* Αθήνα: Νομική Βιβλιοθήκη, σελ. 119, 123, HM Treasury. *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence.* σελ. 40, Available at: https://bit.ly/3gmegjG (Accessed 08/06/2021), Δαλακούρας, Θ., 2019. *Ηλεκτρονικό Έγκλημα.* σελ.3-5.

[184] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 10, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 24, *HM Treasury*. ό.π., σελ. 40, *Ζημιανίτης, Δ.*, ό.π., σελ.162: «Ο ηλεκτρονικός υπολογιστής γίνεται: στόχος όταν υποκλαπούν δεδομένα του, υποκείμενο, υποκείμενο όταν συμβάλλει στη διάδοση κακόβουλου λογισμικού και μέσο του εγκλήματος, στην περίπτωση της κλοπής ταυτότητας».

4.1. Οι οντότητες που συναντώνται στο οικοσύστημα του Bitcoin

Στο σύστημα του Bitcoin, όπως εξάλλου και σε κάθε σύστημα κρυπτονομισμάτων, συναντώνται αρκετές κατηγορίες οντοτήτων, καθεμιά από τις οποίες έχει ένα πολύ διαφορετικό πλην όμως καταλυτικό ρόλο και μπορεί να συμβάλει στην περεταίρω διευκόλυνση του κυβερνοεγκλήματος ως εργαλείο ή ως στόχος. Απαντώνται επτά κατηγορίες[185], που κατηγοριοποιούνται ανάλογα με το ρόλο που διαδραματίζουν και η συνύπαρξη και συμβολή των οποίων επιτρέπουν την αρμονική λειτουργία του συστήματος.

➢ Οι **χρήστες** κρυπτονομισμάτων είναι φυσικά πρόσωπα ή νομικές οντότητες που κατέχουν κρυπτονομίσματα για αγορά αγαθών και υπηρεσιών, για πληρωμές ή απλώς για επενδυτικούς σκοπούς. Υπάρχουν πολλοί τρόποι για να αποκτήσει κάποιος κρυπτονομίσματα. Μπορεί να τα αγοράσει απευθείας από έναν χρήστη μέσω μιας πλατφόρμας ανταλλαγών (P2P Exchange) ή από ένα ανταλλακτήριο κρυπτονομισμάτων χρησιμοποιώντας παραστατικό χρήμα ή κάποιο άλλο κρυπτονόμισμα. Μπορεί ακόμα να πουλάει αγαθά και υπηρεσίες με αντάλλαγμα κρυπτονομίσματα, ή να δέχεται κρυπτονομίσματα ως πληρωμή για τέτοιες υπηρεσίες, ή να λάβει κρυπτονομίσματα ως δώρο ή δωρεά από κάποιον άλλο χρήστη. Τέλος μπορεί να δημιουργήσει νέα κρυπτονομίσματα, συμμετέχοντας στην διαδικασία της εξόρυξης.

➢ Οι **εξορύκτες** είναι μεμονωμένα φυσικά πρόσωπα ή ομάδες προσώπων που επιλύουν τον περίπλοκο μαθηματικό γρίφο που τίθεται από το σύστημα, με σκοπό να επαληθεύουν τις συναλλαγές ώστε να λάβουν την ανταμοιβή τους. Αποτελούν τη σπονδυλική στήλη του συστήματος Blockchain.

➢ Τα **ανταλλακτήρια κρυπτονομισμάτων** είναι φυσικά πρόσωπα ή νομικές οντότητες που προσφέρουν υπηρεσίες ανταλλαγής στους χρήστες κρυπτονομισμάτων, λαμβάνοντας

[185] Βλ. Houben, R., Snyers, A., 2018. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. *Policy Department for Economic, Scientific and Quality of Life Policies* [online]. June 2018, σελ. 25-27: Available at: https://bit.ly/3iybevC (Accessed 26/01/2021), Brown, C., Gitlitz, M. A. & Greene, C., 2021. An introduction to virtual currency money transmission regulation [online]. In: *Blockchain & Cryptocurrency Regulation.* 3st Ed. 2021, p.p. 93-110. Global Legal Group Ltd, London.) σελ.98 Available at: https://www.acc.com/sites/default/files/resources/upload/GLI-BLCH21_E-Edition.pdf Accessed 06/06/2021), Fromberger, M., Haffke, L. & Zimmermann, P., 2019. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them. Journal of Banking Regulation [online]. Vol. 21, p.p. 125–138, σελ.3-5: Available at: https://doi.org/10.1057/s41261-019-00101-4 (Accessed 07/06/2021).

συνήθως κάποια προμήθεια για την παροχή των υπηρεσιών αυτών. Λειτουργούν ταυτοχρόνως ως χρηματιστήριο και ανταλλακτήριο την ίδια στιγμή. Τα ανταλλακτήρια είναι δύο ειδών. Αυτά που επιτρέπουν στους χρήστες να ανταλλάξουν τα κρυπτονομίσματά τους με παραστατικό χρήμα και το αντίστροφο, όπως είναι τα ανταλλακτήρια Kraken, Bitfinex και το Coinbase. Και αυτά που ανταλλάσσουν κρυπτονομίσματα μόνο με άλλα κρυπτονομίσματα, όπως είναι το ανταλλακτήριο Binance.

- Οι **πλατφόρμες συναλλαγών** (P2P exchanges ή decentralized exchanges) είναι οντότητες που ο ρόλος τους είναι πολύ σημαντικός στην ανταλλαγή των κρυπτονομισμάτων. Πρόκειται για αγορές που λειτουργούν αποκλειστικά από λογισμικό, το οποίο δεν έχει κεντρικό σημείο ελέγχου και οι οποίες παρέχουν ένα περιβάλλον για απευθείας ανταλλαγή κρυπτονομισμάτων μεταξύ χρηστών που ψάχνουν να αγοράσουν ή να πωλήσουν κρυπτονομίσματα. Οι χρήστες είναι αυτοί που θα διαπραγματευτούν τη συμφωνία διαδικτυακά, ή ακόμη και τοπικά με προσωπική συνάντηση. Οι πλατφόρμες αυτές αναφέρονται και ως το «eBay των κρυπτονομισμάτων». Παράδειγμα αυτής της κατηγορίας είναι το LocalBitcoins. Οι πλατφόρμες ανταλλαγών δεν πρέπει να συγχέονται με τα ανταλλακτήρια, καθώς δεν αγοράζουν ούτε πωλούν νομίσματα αυτές οι ίδιες, ούτε λειτουργούν ως οντότητα που επιβλέπει και επεξεργάζεται τις ανταλλαγές.

- Οι **πάροχοι πορτοφολιών** είναι οντότητες που παρέχουν στους χρήστες κρυπτονομισμάτων ψηφιακά πορτοφόλια (web wallet), ώστε αυτοί να διατηρήσουν, να αποθηκεύσουν και να μεταφέρουν τα BTC τους. Οι πάροχοι αυτοί συνήθως έχουν γνώση του ιδιωτικού κλειδιού του χρήστη και παρουσιάζουν το ιστορικό συναλλαγών του χρήστη σε μια εύκολη και αναγνώσιμη φόρμα, η οποία μοιάζει αρκετά με ένα περιβάλλον τραπεζικού λογαριασμού.

- Οι **δημιουργοί των κρυπτονομισμάτων** είναι φυσικά πρόσωπα, που ανέπτυξαν τις τεχνικές προδιαγραφές για την δημιουργία ενός κρυπτονομίσματος και έθεσαν τους κανόνες για την χρήση τους. Στην περίπτωση του Bitcoin, η ταυτότητα αυτού του προσώπου παραμένει άγνωστη.

- Οι **πάροχοι κρυπτονομισμάτων** είναι φυσικά πρόσωπα ή νομικές οντότητες που προσφέρουν τη δυνατότητα σε χρήστες είτε έναντι πληρωμής είτε χωρίς χρέωση, να αποκτήσουν κρυπτονομίσματα πριν από την επίσημη κυκλοφορία του κρυπτονομίσματος. Η κίνηση αυτή αποσκοπεί κυρίως στην αύξηση της δημοτικότητας του κρυπτονομίσματος και στην μακροπρόθεσμη ανάπτυξή του. Η διαδικασία αυτή ονομάζεται Initial Coin Offerings (ICOs).

- Τα **ΒΑΤΜ** είναι μηχανήματα που λειτουργούν ως μεσάζοντες μεταξύ αγοραστών και πωλητών BTC και είναι δύο ειδών, μονόδρομης ή αμφίδρομης ροής. Τα πρώτα επιτρέπουν μόνο τη μετατροπή παραστατικού χρήματος σε BTC, ενώ τα δεύτερα επιτρέπουν και τη μετατροπή BTC σε παραστατικό χρήμα.

4.2. Το Bitcoin ως μέσον επίτευξης του κυβερνοεγκλήματος

Ο παγκόσμιος ιστός αποτελείται από δύο στρώματα, τον επιφανειακό ιστό και τον αόρατο ιστό. Η έννοια του παγκόσμιου ιστού συχνά χρησιμοποιείται αντί του όρου διαδίκτυο. Η σύγχυση όμως αυτή μπορεί να προκαλέσει παρερμηνείες καθώς ο όρος Διαδίκτυο αποτελεί το «όλον» και είναι ευρύτερος του όρου Παγκόσμιος Ιστός που αποτελεί το «μέρος». Το Διαδίκτυο ή Internet δημιουργήθηκε πρώτο και αποτελεί ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι ανταλλάσσουν δεδομένα χρησιμοποιώντας την καθιερωμένη ομάδα πρωτοκόλλων, που αποκαλείται TCP/IP (Transmission Control Protocol/Internet Protocol). Αντίθετα, ο όρος Παγκόσμιος Ιστός ή World Wide Web (γνωστός ως WWW), γεννήθηκε το 1989 και είναι ένα ανοιχτό σύστημα διασυνδεδεμένων πληροφοριών και πολυμεσικού περιεχομένου, που επιτρέπει στους χρήστες του Διαδικτύου να αναζητήσουν πληροφορίες χρησιμοποιώντας αναγνωριστικά που ονομάζονται URL (Uniform Resource Identifiers). Έχει χτιστεί με βάση το πρωτόκολλο μεταφοράς υπερκειμένου (HyperText Transfer Protocol – HTTP), μια γλώσσα προγραμματισμού που επιτρέπει τη μετάβαση μέσω υπερσυνδέσμων (hyperlinks) σε οποιαδήποτε δημόσια σελίδα του διαδικτύου. Η ιστοσελίδα προβάλλεται με τη χρήση

λογισμικού που ονομάζεται φυλλομετρητής ιστοσελίδων ή περιηγητής ιστού (Web Browser)[186].

α) Ο **επιφανειακός ιστός ή surface web ή clearnet** είναι μια συλλογή από ιστοσελίδες, οι οποίες ταξινομούνται από μηχανές αναζήτησης όπως η Google, προκειμένου να γίνει ευκολότερη η πρόσβαση στους χρήστες. Η ταξινόμηση αυτή γίνεται με τη βοήθεια κάποιων διαδικτυακών ρομπότ (web bot), όπως οι ανιχνευτές ιστού (web crawlers)[187]. Στον επιφανειακό ιστό όλες οι πληροφορίες είναι ελεύθερα διαθέσιμες στο κοινό χωρίς να χρειάζεται κάποια επιπλέον εφαρμογή που θα παράσχει πρόσβαση στα δεδομένα. Υπολογίζεται ότι ο επιφανειακός ιστός καλύπτει μόνο το 4% των πληροφοριών που κυκλοφορούν στο διαδίκτυο.

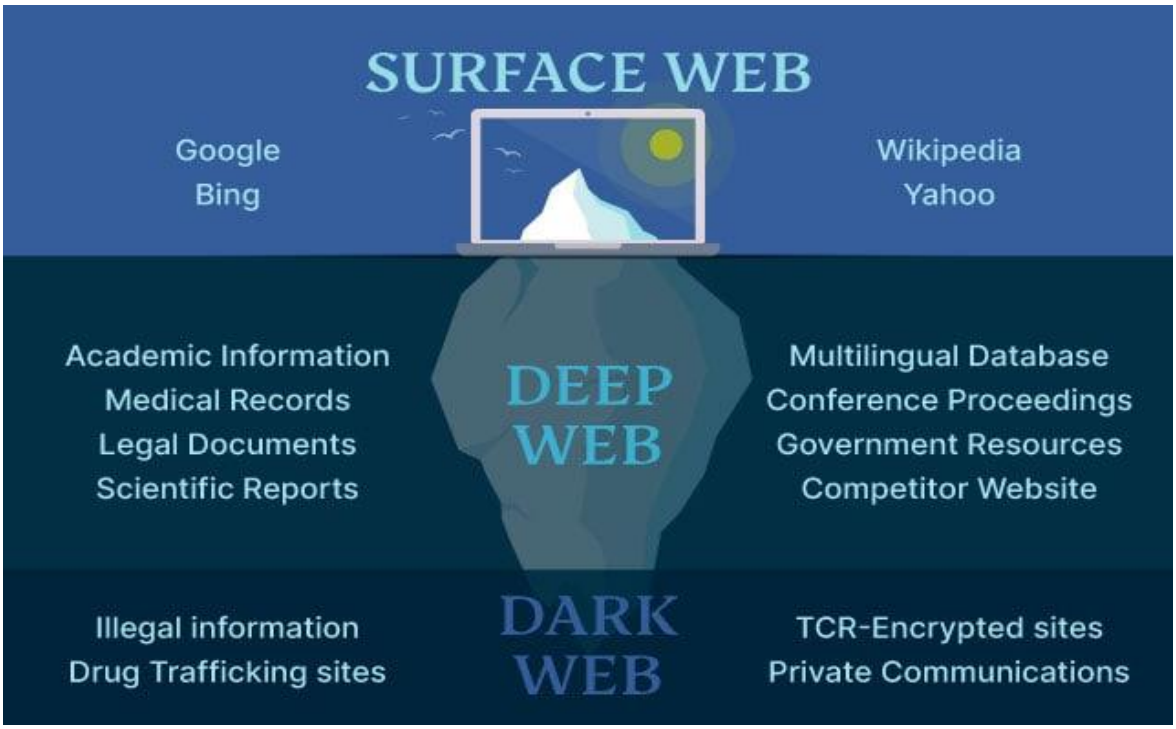
β) Ο **αόρατος ιστός ή deep web ή deepnet** είναι το δεύτερο στρώμα του παγκόσμιου ιστού και αυτό που καταλαμβάνει τη μεγαλύτερη έκταση, όντας τέσσερις με πέντε φορές μεγαλύτερος από τον επιφανειακό ιστό. Το περιεχόμενο του deep web δεν είναι ευρετηριασμένο από τις παραδοσιακές μηχανές αναζήτησης. Τουναντίον, η πρόσβαση στις πληροφορίες και δεδομένα απαιτεί μία επιπλέον εξουσιοδότηση, η οποία γίνεται μέσω της χρήσης login είτε μέσω συγκεκριμένης διεύθυνσης IP ή URL. Στο deep web βρίσκονται εφαρμογές, χρησιμοποιούμενες σε καθημερινή βάση όπως είναι το Facebook, Gmail, κυβερνητικά site όπως το Taxis, τραπεζικοί λογαριασμοί κλπ[188]

---

[186] W3C. *Leading the web to its full potential*. Available at: https://www.w3.org/Help/#webinternet (Accessed 20/05/2021), W3C. *HELP AND FAQ*. Available at: https://www.w3.org/Help/#webinternet (Accessed 20/05/2021), Jacobs, I., 2004. *Architecture of the World Wide Web, Volume One*. Available at: https://www.w3.org/TR/webarch/ (Accessed 27/05/2021).

[187] Τα web bot είναι προγράμματα ή εφαρμογές λογισμικού που επισκέπτονται ιστοσελίδες και πραγματοποιούν διάφορες αυτοματοποιημένες εργασίες. Το bot διατρέχει το διαδίκτυο ανιχνεύοντας συνδέσμους και ιστοσελίδες. Χρησιμοποιείται συνήθως από τις μηχανές αναζήτησης, ώστε να συγκεντρώσει στοιχεία για τη βάση δεδομένων τους, προκειμένου οι ιστοσελίδες που χρησιμοποιούνται από τους χρήστες να εμφανίζουν πιο γρήγορα τα αποτελέσματα αναζήτησης, βλ.: IGURU. *Τι είναι το ο web crawler.* Ανακτήθηκε από: https://iguru.gr/2021/03/02/einai-web-crawler/ (Πρόσβαση 23/05/2021) και Γεωργούλας, Λ., *Τα είδη των ρομπότ του διαδικτύου που επισκέπτονται τον ιστότοπο μας και πως να τα μπλοκάρεις.* Ανακτήθηκε από: https://nextnet.gr/040-ta-eidh-tvn-rompot-toy-diadiktyoy-poy-episkeptontai-ton-istotopo-mas-kai-pvs-na-ta-mplokareis.php (Πρόσβαση 22/04/2021).

[188] Βλ. Broadhurst, R., AA et al., 2018. *Malware Trends on 'Darknet' Crypto-markets: Research Review*. [online]. Report number: Australian National University Cybercrime Observatory and the Korean Institute of Criminology. Affiliation: Australian National University. Cybercrime O{bservatory. Project: *Monitoring web-browser activity and risks of cybercrime.*, σελ. 6-7: Available at: https://bit.ly/2SlxKxf (Accessed 26/01/2021), CIS. Center for Internet Security. *Cybersecurity Spotlight - The Surface Web, Dark Web, and Deep Web*. Available at: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web/ (Accessed 23/02/2021).



Εικόνα 14: Δομή Παγκόσμιου Ιστού[189].

γ) Ο **σκοτεινός ιστός ή dark web ή darknet** είναι το τμήμα εκείνο του deep web, το οποίο εκ προθέσεως περιέχει κρυμμένο περιεχόμενο. Αποτελεί ένα ξεχωριστό δίκτυο που λειτουργεί στο χώρο του deep web, υποστηρίζει κρυπτογραφημένες ιστοσελίδες και προϋποθέτει ειδικά λογισμικά, εργαλεία και εξοπλισμό για να αποκτήσει κάποιος πρόσβαση σε αυτό. Στο dark web οι ιστοσελίδες είναι ορατές στο κοινό, ωστόσο τρέχουν πίσω από πολλαπλά επίπεδα κρυπτογράφησης εξασφαλίζοντας την ανωνυμία των διευθύνσεων και εμποδίζοντας τις παραδοσιακές μηχανές αναζήτησης να τις εντοπίσουν και να τις καταγράψουν.

Η πρόσβαση στο dark web γίνεται από οποιονδήποτε διαθέτει έναν Onion browser. Ο πιο διαδεδομένος τέτοιος browser είναι ο TOR[190]. Από τη στιγμή που το λογισμικό θα

[189] Ciso platform. *Surface Web vs Deep Web vs Dark Web.* Available at: https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different (Accessed 23/05/2021).

[190] TOR είναι αρχικά των λέξεων The Onion Router. Το TOR είναι μια έκδοση του δημοφιλούς προγράμματος περιήγησης ιστού του Firefox, που έχει τροποποιηθεί για να επιτρέπει στους χρήστες να περιηγούνται στο διαδίκτυο ανώνυμα. Η λέξη "onion" που σημαίνει κρεμμύδι, χρησιμοποιείται μεταφορικά για να δηλώσει τα πολλαπλά στρώματα κρυπτογράφησης που παρέχει η χρήση του TOR. Τα δεδομένα περνούν από τυχαία επιλεγμένους κόμβους, οι οποίοι κρυπτογραφούν τα δεδομένα σε κάθε πέρασμα. Οι κόμβοι γνωρίζουν από πού προέρχεται το σήμα και πού πηγαίνει, αλλά δεν μπορούν να δουν όλη τη διαδρομή που κάνουν τα δεδομένα.

εγκατασταθεί στον υπολογιστή, χρησιμοποιεί μια αλυσίδα από εικονικά κανάλια-κόμβους, προκειμένου να συνδέσει τους χρήστες με το dark web. Τα κανάλια αυτά μεταμφιέζουν την IP[191] του χρήστη, διασφαλίζοντας την ανωνυμοποίηση της επικοινωνίας του. Οι ιστοσελίδες στο dark web διαφέρουν από τις παραδοσιακές ιστοσελίδες. Έχουν την κατάληξη « .onion» αντί για « .com», ενώ και το όνομα της διεύθυνσής τους είναι διαμορφωμένο με τέτοιο τρόπο, ώστε να αποτελεί μια σειρά από ακανόνιστους αριθμούς και γράμματα π.χ. η ιστοσελίδα της αγοράς του Dream Market ήταν «eajwlvm3z2lcca76.onion». Για το λόγο αυτό, προκειμένου ο χρήστης να συνδεθεί με κάποια ιστοσελίδα στο dark web, θα πρέπει να γνωρίζει τη διεύθυνσή της ιστοσελίδα και να πληκτρολογήσει την κρυπτογράφηση αυτής. Ο πιο εύκολος τρόπος για να βρει ο χρήστης ιστοσελίδες είναι να λάβει έναν σύνδεσμο της συγκεκριμένη σελίδας από άλλο χρήστη που ήδη γνωρίζει γι' αυτήν[192].

4.2.1. Η πληρωμή αγαθών και υπηρεσιών στο Dark web

Στο dark web χρησιμοποιείται για νόμιμες και για παράνομες δραστηριότητες προσφέροντας ανωνυμία. Οι νόμιμες σχετίζονται κυρίως με πρόσβαση σε πληροφορίες, με προστασία ταυτότητας προσώπων, με διαμοιρασμό πληροφοριών και με επικοινωνία με άλλους. Στην πράξη βέβαια το όνομα του dark web έχει συνδεθεί κυρίως με την ανάπτυξη

βλ. Andreas, K., 2021. *Tor έναντι VPN – Ποιο Είναι Πιο Ασφαλές.* Available at: https://bit.ly/3hRg72t (Accessed 20/04/2021), Slim, T., 2021. *Πώς να αποκτήσετε πρόσβαση στο Dark Web: Οδηγός για την περιήγηση στο Dark Web χρησιμοποιώντας το TOR Browser.* Available at: https://bit.ly/3cBsTPi (Accessed 27/04/2021).

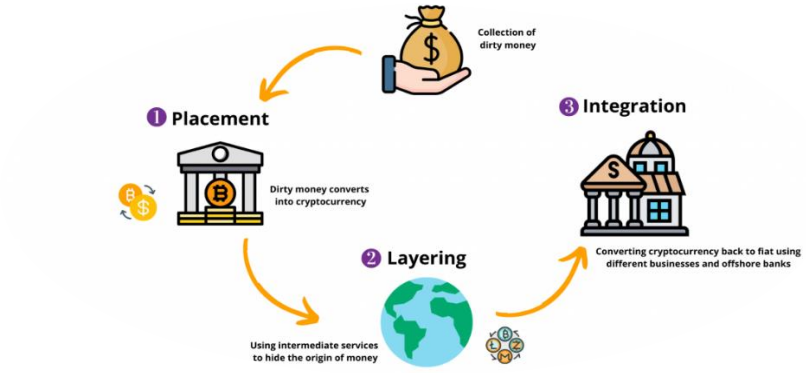
[191] IP σημαίνει Internet Protocol. Είναι ένας αριθμός χωρισμένος με τελείες (πχ 192.168.1.37). Όλες οι συσκευές που έχουν πρόσβαση στο διαδίκτυο λαμβάνουν μια IP, η οποία είναι μοναδική σε όλο τον κόσμο και αποτελεί την ταυτότητα της συγκεκριμένης συσκευής.

[192] Βλ. Reddy, E., Minnaar, A., 2018. Cryptocurrency: a tool and target for cybercrime. *Acta Criminologica: Southern African Journal of Criminology* [online]. Vol 31(3), p.p.71-92 σελ. 74-75: Available at: https://bit.ly/3zm0WVn (Accessed 27/04/2021), Broadhurst, R., AA et al., ό.π., σελ. 6-7, WLEARN-Πρόσβαση στη Γνώση. *Τι είναι το Σκοτεινό Διαδίκτυο (Dark Web) και πως μπορεί κάποιος να αποκτήσει πρόσβαση σε αυτό*. Available at: https://www.wlearn.gr/index.php/articles/1391-what-is-dark-web (Πρόσβαση 03/03/2021), *CIS. Center for Internet Security*, ό.π., βλ. Tor. *Σχετικά Με Ιστορία.*. Ανακτήθηκε από: https://www.torproject.org/about/history/ (Πρόσβαση 01/03/2021), Reed, M., Syverson, P., Onion Routing. *AIPA 99 Theme Relevance: Tools and Technologies for Intelligence Community Analysts* [online]. Available at: https://www.onion-router.net/Publications/AIPA-1999.pdf (Accessed 27/02/2021), *Oerlemans, J., J., van Deventer, O. et van Wegberg, R., ό.π.,* σελ.421, Stearns, B., 2019. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review* [online]. Vol 34(6), p.p. 1180-1196, σελ.1188-1189: Available at: https://www.sciencedirect.com/science/article/abs/pii/S026736491830308X# (Accessed 24/02/2021).
Περισσότερα για το dark net και τον Tor βλ. Moore, D., Rid, T., 2016. Cryptopolitik and the Darknet. *Survival* [online]. Vol 58(1), p.p. 7-38, σελ.7 επ.: Available at: https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true& (Accessed 27/04/2021).

παράνομων δραστηριοτήτων. Τα πλεονεκτήματα που παρέχει το δίκτυο είχε ως αποτέλεσμα την ραγδαία ανάπτυξη των διαδικτυακών μαύρων αγορών. Σε αυτές μπορεί κάποιος να αγοράσει λογαριασμούς πρόσβασης σε ιστοσελίδες που παρέχουν περιεχόμενο επί πληρωμή όπως το Spotify ή το Netflix, αριθμούς πιστωτικών ή προπληρωμένων καρτών, ναρκωτικά, όπλα, να πληρώσει για παράνομες υπηρεσίες όπως αυτές ενός hacker, να συμμετάσχει στη διακίνηση παράνομων βίντεο όπως πορνογραφίας, παιδεραστίας. Στην τεχνολογική εξέλιξη των μαύρων αγορών συνέβαλε η εμφάνιση των κρυπτονομισμάτων, τα οποία λειτουργούν ως ιδανικός σύμμαχος για γρήγορες και ανώνυμες συναλλαγές για παράνομες υπηρεσίες και πωλήσεις. με αποτέλεσμα το Bitcoin να γίνει τάχιστα το επιλεγόμενο σύστημα πληρωμών στο ηλεκτρονικό εμπόριο που διεξάγεται στο dark web[193].

4.2.2. Η νομιμοποίηση εσόδων από παράνομες δραστηριότητες

Το dark web δεν χρησιμεύει μόνο για το εμπόριο παράνομων προϊόντων αλλά και για την εξυπηρέτηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή αλλιώς για το ξέπλυμα «βρώμικου» χρήματος (money laundering). Πρόκειται για οικονομικές συναλλαγές που διαπράττονται με στόχο την συγκάλυψη της πραγματικής προέλευσης των εσόδων. Το οικοσύστημα του Bitcoin χρησιμοποιείται ως μέρος της στρατηγικής για την εκταμίευση βρώμικων χρημάτων που προέρχονται από εγκληματικές δραστηριότητες. Τα στάδια που ακολουθούνται για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες είναι τρία[194].



[193] Βλ. *Reddy, E., Minnaar, A.,*, ό.π., σελ. 74, *CIS. Center for Internet Security*, ό.π..

[194] Βλ. Cavin, C., Chiriaeva, M. & Poskriakov, F., 2019. Cryptocurrency compliance and risks: A European KYC/ AML perspective [online]. In: *Blockchain & Cryptocurrency Regulation.* 1st Ed. 2019, p.p. 163-174. Global Legal Group Ltd, London. Σελ.165: Available at: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf (Accessed 06/06/2021)

Εικόνα 15: Στάδια ξεπλύματος χρήματος[195]

α) Placement

Το στάδιο υφίσταται μόνο στην περίπτωση που η αρχική μορφή των «βρώμικων» χρημάτων είναι παραστατικό χρήμα που μετατρέπεται σε BTC μέσω των ανταλλακτηρίων. Αναφέρεται χρονικά στη στιγμή που οι εγκληματίες παρουσιάζουν νέα χρήματα στο σύστημα και επομένως καθίστανται ευάλωτοι. Το κάθε ανταλλακτήριο έχει διαφορετικό επίπεδο κανονισμών συμμόρφωσης, όσον αφορά τις οικονομικές συναλλαγές. Έτσι, κάποια εφαρμόζουν την τακτική Know Your Customer (στο εξής KYC) ή και την Anti-Money Laundering (στο εξής AML), προκειμένου να ταυτοποιήσουν την πηγή των κεφαλαίων. Το στάδιο αυτό παραλείπεται όταν το βρώμικο χρήμα είναι ήδη στη μορφή BTC[196].

β) Layering

Αφού τα χρήματα έχουν πλέον τη μορφή BTC, στη συνέχεια γίνεται η αποσύνδεσή τους από την αρχική πηγή προέλευσης των κεφαλαίων με διάφορες μεθόδους/ υπηρεσίες[197], όπως:

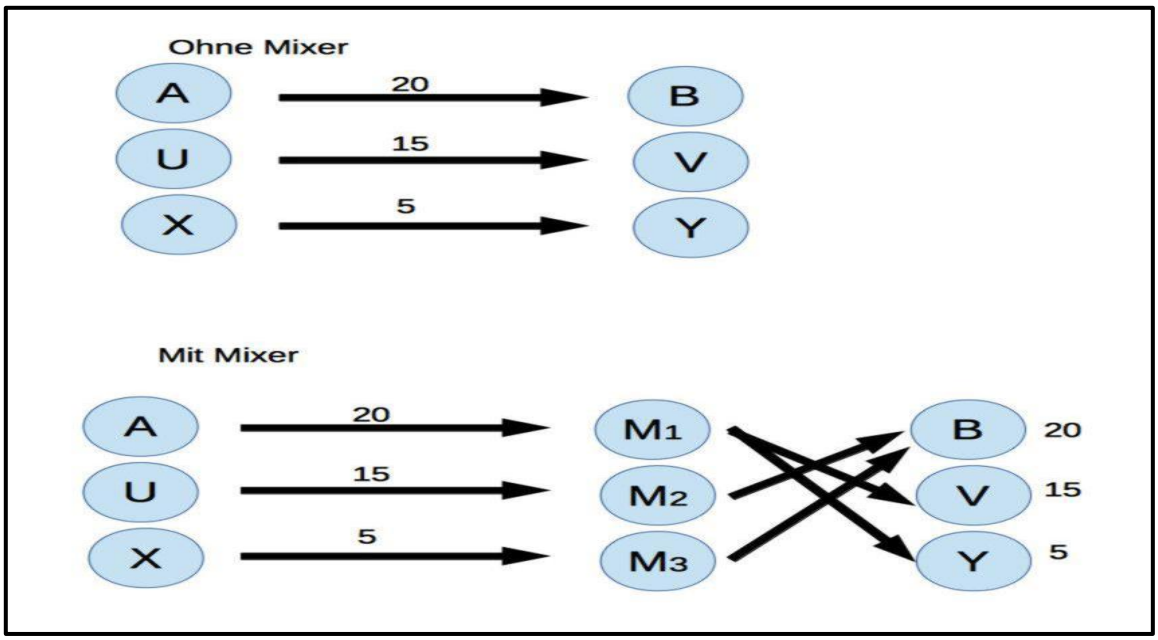
---

[195] Βλ. Agrawal, G., 2020. Cryptocurrency Money Laundering Explained. *Bitquery* [online]. August 6, 2020. Available at: https://bitquery.io/blog/cryptocurrency-money-laundering#Placement (Accessed 27/04/2021).

[196] Βλ. *Ibid.*

[197] Βλ. *Reddy, E., Minnaar, A.,*, ό.π., σελ.77, Dykyi, O., Dyntu, V., 2019. CRYPTOCURRENCY IN THE SYSTEM OF MONEY LAUNDERING. *Baltic Journal of Economic Studies.* [online]. Vol. 4 (5), p.p.75-81, σελ.78: Available at: https://bit.ly/3uVEsag (Accessed 15/04/2021), *Reddy, E., Minnaar, A.,*, ό.π., σελ.77, Moore, D., Rid, T., ό.π., σελ.22, Freel, J., Howard II, B. 2019. Do Bitcoin ATMs Make Money Laundering too Easy? Regulators Try to Keep up with Emerging Cryptocurrency Trend. *LEXOLOGY.* Available at: https://bit.ly/3vazreh (Accessed 27/05/2021), Oerlemans, J., J., van Deventer, O. et van Wegberg, R., 2018. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime* [online]. Vol 25(1), p.p. 419-435, σελ. 423-424: Available at: https://bit.ly/2TPI2Gb (Accessed 24/05/2021), *Agrawal, G.,* ό.π., Kadar, T., 2020. *How are crypto and blockchain being utilised in the gaming sector?*. Available at: https://bit.ly/3pslJ56 (Accessed 22/03/2021), Hoete-Dodd, V., 2019. *How Are Regulators Fighting the use of Cryptocurrencies in Money Laundering at Casinos?*. Available at: https://www.bitprime.co.nz/blog/regulators-fighting-cryptocurrencies-money-laundering-casinos/ (Accessed 23/03/2021), ELLIPTIC. *Bitcoin Money Laundering: How Criminals Use Crypto.* Available at: https://www.elliptic.co/blog/bitcoin-money-laundering (Accessed 23/04/2021). Theodorakis, N., 2018. The Use of Cryptocurrencies for Illicit Activities and Relevant Legislative Initiatives. *The Art of Crime* [online]. Vol 2018(5), p.p.71-92. Available at: https://theartofcrime.gr/the-use-of-cryptocurrencies-for-illicit-activities-and-relevant-legislative-initiatives/ (Accessed 24/03/2021), Holman, D., Stettner, B., 2018. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approache*, σελ.32. Available at: file:///C:/Users/zarch/Downloads/AML18_AllenOvery.pdf (Accessed 27/03/2021), Sándor, B., Fehér, D.J., 2019. *Examining the Relationship between the Bitcoin and Cybercrime* [online]. IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara, Romania. 29-31 May 2019, σελ. 124: Available at: https://doi.org/10.1109/SACI46893.2019.9111568 (Accessed 25/01/2021), *Reddy, E., Minnaar, A.,*, ό.π., σελ.77, https://link.springer.com/article/10.1057/s41261-019-00101-4 σελ.6

➢ Η κυριότερη υπηρεσία που παρέχεται για το ξέπλυμα χρήματος είναι οι **«mixers»**. Επειδή οι συναλλαγές στο Bitcoin συνδέονται η μία με την άλλη μέσω εισόδων και εξόδων, σχηματίζοντας μια αλυσίδα, μπορεί κάποιος που παρακολουθεί το ιστορικό συναλλαγών μιας διεύθυνσης Bitcoin να συνδέσει τη διεύθυνση που χρησιμοποιήθηκε στο παρελθόν για κυβερνοεγκλήματα με τη διεύθυνση που χρησιμοποιείται για την εκταμίευση «βρώμικων χρημάτων». Οι mixers χρησιμεύουν για να κρύψουν τα ίχνη που αφήνουν οι συναλλαγές. Αποσυνδέουν τα BTC από την αρχική εγκληματική πηγή και τα κάνουν να φαίνονται ότι προέρχονται από πολλές διαφορετικές συναλλαγές και διευθύνσεις, με αποτέλεσμα να είναι πολύ δύσκολο σε κάποιον να παρακολουθεί όλες τις κινήσεις ενός πορτοφολιού. Οι υπηρεσίες mixer λειτουργούν δίνοντας στον πελάτη μια νέα διεύθυνση Bitcoin για να καταθέσει το ποσό που επιθυμεί. Η διεύθυνση αυτή λειτουργεί ως μια δεξαμενή κρυπτονομισμάτων. Στη συνέχεια η υπηρεσία mixer, με τη χρήση άλλων διευθύνσεων Bitcoin, πληρώνει το ποσό που έχει ζητήσει ο πελάτης στη διεύθυνση που της έχει υποδείξει. Κάθε φορά που κάποιος πελάτης κάνει μια νέα κατάθεση στη διεύθυνση Bitcoin ενός mixer, λαμβάνει έναν νέο αριθμό πελάτη. Με τον τρόπο αυτό η υπηρεσία γνωρίζει ποια BTC κατατέθηκαν από τον συγκεκριμένο πελάτη, ώστε την επόμενη φορά που ο πελάτης θα θελήσει να χρησιμοποιήσει την υπηρεσία mixer να μην χρησιμοποιηθούν τα ίδια BTC για να γίνει η πληρωμή. Ο τρόπος λειτουργίας των υπηρεσιών αυτών βοηθά εξαιρετικά όσους θέλουν να προβούν σε ξέπλυμα χρήματος.



Εικόνα 16: Mixer[198]

➢ Μία δεύτερη μέθοδος είναι **η χρήση Bitcoin ATM** (στο εξής BATM). Η λογική λειτουργίας των BATM είναι παρόμοια με των γνωστών ATM. Επιτρέπουν την ανταλλαγή BTC σε παραστατικό χρήμα και το αντίστροφο. Εν αντιθέσει όμως με ένα παραδοσιακό ATM, δεν υπάρχει κάποια τράπεζα που να εμπλέκεται στη μεταφορά αυτή και επομένως να μπορεί να ελέγξει σε ποιον ανήκει ένα συγκεκριμένο πορτοφόλι Bitcoin. Τα BATM συνήθως ζητούν ελάχιστες πληροφορίες για τα άτομα που τα χρησιμοποιούν, οι οποίες μάλιστα μπορεί να είναι και πλαστές, καθώς μένουν ανεπιβεβαίωτες. Οι μεταφορές είναι εντελώς ανώνυμες, εκτός αν υπάρχουν ρυθμίσεις KYC, που αναγκάζουν τον ιδιοκτήτη του ATM να τις εφαρμόσει.

[198] Eurospinder: relevancy retrieval. *What is a cryptocurrency mixer?*. Available at: https://www.eurospider.com/en/know-how/compliance/211-what-is-a-cryptocurrency-mixer (Accessed 28/03/2021).

Εικόνα 17: Bitcoin ATM around the world[199]

➢ Μια τρίτη μέθοδος είναι **η χρήση ιστοσελίδων που παρέχουν υπηρεσίες τυχερών παίγνιων (gambling)**. Οι κυβερνοεγκληματίες παρουσιάσουν τα «βρώμικα »χρήματα ως έσοδα από τη χρήση των ιστοσελίδων αυτών. Στην πράξη, καταθέτουν ένα μεγάλο ποσό χρημάτων στον λογαριασμό που έχουν στην ιστοσελίδα. Αφού συμμετάσχουν σε μερικά παιχνίδια, δείχνοντας ότι ο λογαριασμός είναι ενεργός, στη συνέχεια αποσύρουν τα χρήματά τους. Άλλες φορές πάλι, καταθέτουν διάφορα ποσά σε διαφορετικούς λογαριασμούς που έχουν δημιουργήσει στις συγκεκριμένες ιστοσελίδες και χρησιμοποιώντας την μέθοδο «chip dumping[200]» συνεννοούνται ποιος από τους συμμετέχοντες στο τυχερό παιχνίδι θα κερδίσει την παρτίδα, ώστε στη συνέχεια να στείλουν τα «βρώμικα» χρήματα στον λογαριασμό του για να τα εκταμιεύσει πλέον ως νόμιμα-«καθαρά» έσοδα.

➢ Μια τέταρτη μέθοδος είναι **η χρήση ανταλλακτηρίων που δεν υπόκεινται σε κανονιστικές ρυθμίσεις KYC/AML**. Τα Bitcoin μετατρέπονται σε άλλα κρυπτονομίσματα (Altcoins). Η διαδικασία αυτή γίνεται διαρκώς μέχρις ότου να μην υπάρχει πλέον καμία σύνδεση με την αρχική πηγή.

[199] KURANT-ATMs. *Bitcoin ATM Map.* Available at: https://coinatmradar.com/ (Accessed 30/05/2021).

[200] Ο όρος «chip dumping» χρησιμοποιείται στο χαρτοπαίγνιο πόκερ για να την σκόπιμη συνεργασία δύο ή περισσότερων παικτών με απώτερο σκοπό τα παράνομα χρήματα του ενός να κερδηθούν από τους άλλους και να εμφανιστούν ως νόμιμα έσοδα, πλέον «καθαρά» χρήματα.

➢ Μια πέμπτη μέθοδος είναι **η χρήση P2P δικτύων**. Οι εγκληματίες χρησιμοποιούν χρήστες που τυγχάνουν υπεράνω πάσης υποψίας και οι οποίοι στέλνουν τα κεφάλαια σε ανταλλακτήρια που βρίσκονται σε άλλες χώρες, στις οποίες δεν ισχύουν κανονισμοί AML και εκεί τα Bitcoin μετατρέπονται σε τοπικό νόμισμα.

➢ Μια έκτη μέθοδος που χρησιμοποιείται είναι **η χρήση ICO**. Οι εγκληματίες παρουσιάζονται ως επενδυτές, αγοράζοντας ICO και μετατρέποντας τα BTC σε άλλα κρυπτονομίσματα.

γ) Inegration

Στο τρίτο και τελευταίο στάδιο τα χρήματα ξαναπαρουσιάζονται στο οικονομικό σύστημα και κάποιες φορές θα πρέπει να παρασχεθούν εξηγήσεις για το πώς αποκτήθηκαν. Τότε οι εγκληματίες δημιουργούν νέες εικονικές επιχειρήσεις, οι οποίες δέχονται τα BTC ως μέσο πληρωμής και στη συνέχεια τα μετατρέπουν σε παραστατικό χρήμα. Ή ακόμη τα παρουσιάζουν ως κέρδη από τυχερά παίγνια ή από επενδύσεις σε ICO.

4.2.3. Η χρηματοδότηση της τρομοκρατίας

Μολονότι η χρήση των κρυπτονομισμάτων δεν είναι ευρέως διαδεδομένη, εντούτοις οι τρομοκρατικές ομάδες έχουν αρχίσει να πειραματίζονται με το Bitcoin, καθιστώντας το ένα ακόμη μέσον για την χρηματοδότηση της τρομοκρατίας. Για τις δραστηριότητές τους, που αφορούν κυρίως προπαγάνδα, χρηματοδότηση, σχεδιασμό, εκτέλεση των φυσικών επιθέσεων, σαμποτάζ διαδικτυακών υποδομών, χρησιμοποιούν το dark web για να κρύψουν επαρκώς την ταυτότητά τους. Το Bitcoin χρησιμοποιείται κυρίως μέσω εκστρατειών στα μέσα κοινωνικής δικτύωσης για συγκέντρωση χρημάτων με τη μορφή δωρεών. Μεταξύ των εγκληματικών οργανώσεων που επωφελούνται από το Bitcoin είναι το Islamic State of Iraq and Syria (στο εξής ISIS). Για παράδειγμα μια τέτοια εκστρατεία ήταν η Al-Sadaqah (μτφρ αραβικά: φιλανθρωπική προσφορά), η οποία σκοπούσε στη χρηματοδότηση του jihad και λάμβανε χώρα κυρίως μέσω του κοινωνικού δικτύου Telegram. Η ομάδα αυτή συγκέντρωνε κεφάλαια BTC για τη χρηματοδότηση μαχητών (mujahideen) που βρίσκονταν στη Συρία και πάλευαν ενάντια στο καθεστώς του Assad, εκμεταλλευόμενη κυρίως την ανωνυμία των δωρεών που μπορούσαν να γίνουν με τη χρήση του BTC. Παρότι η εκστρατεία αυτή δεν στέφθηκε με επιτυχία καθώς δεν μπόρεσε

να συλλέξει μεγάλο ποσό δωρεών, εντούτοις η σπουδαιότητά της έγκειται στο γεγονός ότι το BTC έκανε την εμφάνισή του και στο χώρο της χρηματοδότησης της τρομοκρατίας.

Μέχρι στιγμής, αν και οι τρομοκρατικές οργανώσεις έχουν προσπαθήσει να εντάξουν το BTC ως μέσον για την επίτευξη των σκοπών τους, εντούτοις η πολυπλοκότητα του τρόπου λειτουργίας των κρυπτονομισμάτων σε συνδυασμό με την προτίμησή τους για μετρητά, λειτουργεί ανασταλτικά για την ευρύτερη χρήση του BTC. Ακόμα ένας ανασταλτικός παράγοντας για την υιοθέτηση του BTC είναι η απουσία της απαραίτητης τεχνολογικής υποδομής, όπως το γρήγορο internet σε χώρες του τρίτου κόσμου, καθώς και η έλλειψη γνώσεων ασφαλείας εκ μέρους των τρομοκρατών. Ένα άλλο αίτιο είναι η φύση της δημοσιότητας που αποκτούν οι συναλλαγές μόλις γίνουν μέρος στο Blockchain. Αφ' ης στιγμής οι συγκεκριμένοι λογαριασμοί συνδεθούν με κάποια τρομοκρατική οργάνωση, όπως όταν γίνεται μια φιλανθρωπική δωρεά τύπου Al-Sadaqah, οι αρχές μπορούν να παρακολουθούν την δραστηριότητα της συγκεκριμένης διεύθυνσης Bitcoin και σε περίπτωση που τα χρήματα μετακινηθούν ή ξοδευτούν, μπορούν να προβλέψουν μια επερχόμενη τρομοκρατική επίθεση.

Η Ghost Security Group, μια ακτιβιστική και αντιτρομοκρατική ομάδα, δήλωσε ότι το ISIS χρησιμοποιεί εκτενώς BTC για την χρηματοδότηση των δραστηριοτήτων του. Όπως ισχυρίστηκε η ομάδα, μια αλυσίδα συναλλαγών εντοπίστηκε σε πορτοφόλια Bitcoin, τα οποία πιστεύεται ότι ανήκουν στο ISIS και τα οποία περιείχαν κεφάλαια μεταξύ 4,7 εκατομμυρίων και 15,7 εκατομμυρίων δολαρίων. Το 2015, η γερμανική εταιρεία μέσων ενημέρωσης Deutsche Welle ανέφερε ότι ένα πορτοφόλι Bitcoin που πιστεύεται ότι ανήκε στο ISIS έλαβε περίπου 23 εκατομμύρια δολάρια μέσα σε ένα μήνα. Στην πραγματικότητα η υιοθέτηση των BTC από τους τρομοκράτες κατά κάποιο τρόπο καθρεφτίζει την κοινή γνώμη. Αυτό σημαίνει ότι, εάν η ζήτηση BTC και γενικά κρυπτονομισμάτων αυξηθεί, τότε είναι πολύ πιθανό να αυξηθεί και η χρήση τους από τρομοκρατικές οργανώσεις[201].

[201] Βλ. *Sándor, B., Fehér, D.J.*, ό.π., σελ. 122, *Holman, D., Stettner, B.*, ό.π., σελ 32, Emerald PUBLISHING. *Is the Bitcoin frenzy making the world less safe?*. Available at: https://bit.ly/3cmTZJW (Accessed 23/04/2021), U.S. House of Representatives, Subcommittee on Terrorism and Illicit Finance, Committee on Financial Services, Washington, D.C., 2018. *SURVEY OF TERRORIST GROUPS AND THEIR MEANS OF FINANCING* [online]. 31-576 PDF, SEPTEMBER 7, 2018. Available at: https://bit.ly/35hBjqY (Accessed 26/05/2021), Barone, D.M., 2019. *Suspicious crowdfunding campaigns in bitcoin and their exploitation of exchange services.* Available at: https://bit.ly/3imrKyz (Accessed 21/05/2021), Casadei-Bernardi, S., 2019. *Terrorist Use of Cryptocurrencies: A Blockchain Compliance White Paper*. Available at: https://bit.ly/3x9AVqt (Accessed 27/05/2021).

4.3. Το Bitcoin ως δέλεαρ για το κυβερνοέγκλημα

Από τη στιγμή που το BTC χρησιμοποιείται αντί του παραστατικού χρήματος, πολύ συχνά αποτελεί και το ίδιο τον στόχο κυβερνοεγκληματιών. Έτσι, τα ανταλλακτήρια κρυπτονομισμάτων, οι πάροχοι πορτοφολιών και οι επεξεργαστές πληρωμών δεν έχουν «ανοσία» στις παραδοσιακές μορφές του κυβερνοεγκλήματος, αλλά τουναντίον αρκετοί από αυτούς έχουν καταγγείλει επιθέσεις που είχαν ως αποτέλεσμα να χαθούν Bitcoin και σε κάποιες περιπτώσεις να οδηγήσουν ακόμα και στο κλείσιμο των ανταλλακτηρίων. Πολλές από τις μεθόδους που χρησιμοποιούν οι κυβερνοεγκληματίες συνδυάζονται μεταξύ τους. Έτσι για παράδειγμα μια επίθεση DDoS μπορεί να συνοδευτεί και από απαίτηση λύτρων (ransomware).

4.3.1. Το malware

Το malware (κακόβουλο λογισμικό) έχει δημιουργηθεί για να προκαλέσει ζημιά σε ένα δίκτυο ή σε έναν υπολογιστή. Μπορεί και διαπερνά την επιβεβαίωση ταυτότητας και τα συστήματα ασφαλείας και συνδέει τις συσκευές έχοντας ως απώτερο σκοπό την υποκλοπή πληροφοριών που θα επιτρέψουν στους δημιουργούς τους να πάρουν υπό τον έλεγχό τους τα BTC των θυμάτων τους. Ο όρος αυτός λειτουργεί ως «ομπρέλα» και περιλαμβάνει πολλές υποκατηγορίες[202].

- Οι **virus (ιοί)** απαιτούν κάποια ενέργεια από τον χρήστη προκειμένου να αποκτήσουν πρόσβαση στον υπολογιστή του, όπως είναι το άνοιγμα ενός μολυσμένου email ή ενός αρχείου από USB stick. Από τη στιγμή που εγκαθίστανται μολύνουν περισσότερα αρχεία, εκμεταλλεύονται διεργασίες και επηρεάζουν την αποδοτικότητα του συστήματος.

- Οι **trojan horses (δούρειοι ίπποι)** υπεισέρχονται στον υπολογιστή και υποκλέπτουν σημαντικές πληροφορίες. Η κατηγορία αυτή είναι περισσότερο αρεστή στους κυβερνοεγκληματίες, καθώς έχει σχεδιαστεί να διαπερνά το τείχος ενός ηλεκτρονικού υπολογιστή ή ενός δικτύου και να δημιουργεί μια κερκόπορτα για τους επιτιθέμενους ή να παραδίδει ένα φορτίο όπως έναν ιό, χωρίς καν να χρειάζεται οι δράστες να παραβιάσουν το

[202] Βλ. *Μεταξάκης, Ε.*, ό.π., σελ.236-241, *Broadhurst, R., AA et al.*, ό.π., σελ. 25, *Reddy, E., Minnaar, A.,*, ό.π., σελ. 81-82, Broadhurst, R., AA et al., ό.π., σελ. 28, Karspersky. *What is Riskware?*. Available at: https://www.kaspersky.com/resource-center/threats/riskware (Accessed 28/05/2021), Coindesk, *Computer security firm Dell SecureWorks has managed to identify 146 types of bitcoin malware in the wild*. Available at: https://www.coindesk.com/nearly-150-strains-malware-bitcoins (Accessed 23/03/2021).

σύστημα. Στην πράξη, ο χρήστης πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία, ενώ εγκαθίστανται κρυφά στον υπολογιστή του άλλα κακόβουλα προγράμματα. Οι δούρειοι ίπποι συνήθως χρησιμοποιούν εργαλεία όπως οι keyloggers, που ανιχνεύουν την δραστηριότητα του πληκτρολογίου, προκειμένου να καταγράψουν τους κωδικούς πρόσβασης-ιδιωτικά κλειδιά των πορτοφολιών του θύματος.

- Τα **worms (σκουλήκια)** δεν μολύνουν αρχεία σε έναν υπολογιστή, αλλά από τη στιγμή που θα εγκατασταθούν σταματούν κάθε λειτουργία του υπολογιστή και αρχίζουν να αναπαράγονται. Ο υπολογιστής που έχει καταστραφεί, λειτουργεί πλέον ως μηχανή παραγωγής σκουληκιών, τα οποία στη συνέχεια μολύνουν τους άλλους υπολογιστές που συνδέονται με αυτόν. Η διάδοσή τους γίνεται συνήθως μέσω email, οπότε απαιτείται ενέργεια του χρήστη ή μέσω του δικτύου οπότε η διάδοσή τους γίνεται αυτόματα.

- Οι **«αντικαταστάτες διεύθυνσης»** ανιχνεύουν την ενέργεια αντιγραφής μιας διεύθυνσης Bitcoin στο clipboard του υπολογιστή, στην οποία ο χρήστης επιθυμεί να αποστείλει BTC και αντικαθιστούν την διεύθυνση αυτή με άλλη που ελέγχεται από τον κυβερνοεγκληματία.

- Ο **«thiefwallet»** αναζητά πορτοφόλια λογισμικού σε συγκεκριμένες τοποθεσίες του υπολογιστή ή σκανάροντας όλο το σύστημα. Μόλις εντοπίσει το πορτοφόλι, το ανεβάζει σε έναν απομακρυσμένο server, δίνοντας στον κυβερνοεγκληματία χρόνο για να ξεκλειδώσει το πορτοφόλι και να κλέψει τα BTC.

Σήμερα, ο όρος malware περιλαμβάνει και προγράμματα που, αν και είναι νόμιμα, υπό ορισμένες συνθήκες χρησιμοποιούνται για παράνομους σκοπούς. Τέτοια προγράμματα είναι τα botnets ή bots και το riskware, τα οποία δεν έχουν σχεδιαστεί ως κακόβουλα, αλλά έχουν λειτουργίες που μπορούν να χρησιμοποιηθούν για κακόβουλους σκοπούς.

- Πρόγραμμα **bot** είναι οι web crawler που χρησιμοποιούνται από τις μηχανές αναζήτησης για την ευρετηρίαση των ιστοσελίδων. Ωστόσο η χρήση τους γίνεται και από κυβερνοεγκληματίες οι οποίοι αποβλέπουν κυρίως στη διεξαγωγή επιθέσεων σε servers. Ο hacker δημιουργεί ένα δίκτυο από bots, το botnet, που αποτελεί μια συλλογή από υπολογιστές «ζόμπι», ελεγχόμενους από αυτόν. Στη συνέχεια, με την ταυτόχρονη βοήθεια

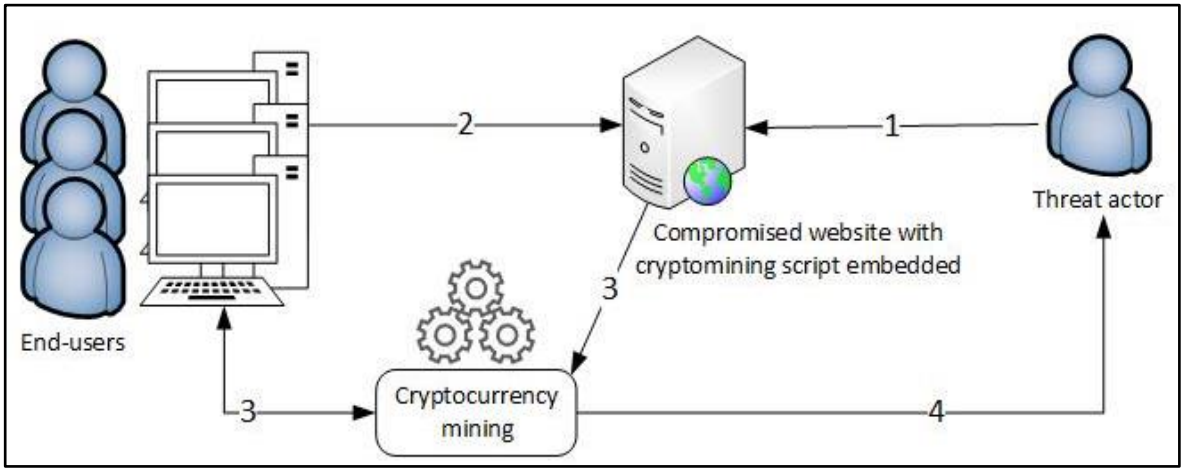
όλων αυτών επιτίθεται σε έναν server του διαδικτύου όπως είναι ένα ανταλλακτήριο Bitcoin και προκαλεί πρόβλημα στη λειτουργία του.

- Πρόγραμμα **riskware** είναι ένα πρόγραμμα το οποίο αποσκοπεί στο να εντοπίσει όλους τους πιθανούς κινδύνους εξαιτίας έλλειψης επαρκούς ασφάλειας, μη συμβατότητας λογισμικού ή εγκληματικής παραβίασης και καταστρατήγησης νόμιμων προγραμμάτων. Παράδειγμα riskware είναι το λογισμικό για απομακρυσμένη πρόσβαση σε υπολογιστή. Η κατάχρηση του λογισμικού κινδύνου γίνεται για κλοπή δεδομένων, παραβίαση συστημάτων υπολογιστών ή για πρόκληση διαταραχών.

4.3.2. Το cryptojacking

Ένας από τους τρόπους για να αποκτήσει κάποιος BTC είναι μέσω της διαδικασίας της εξόρυξης, η οποία όμως απαιτεί τεράστια υπολογιστική ισχύ. Προκειμένου λοιπόν να παραχθεί αυτή, οι hackers παραβιάζουν μια πληθώρα υπολογιστών και δημιουργούν ένα botnet. Η διαδικασία αυτή ονομάζεται cryptojacking. Το θύμα ακούσια εγκαθιστά κακόβουλα προγράμματα, τα οποία επιτρέπουν στους κυβερνοεγκληματίες να αποκτήσουν πρόσβαση στον υπολογιστή του ή σε άλλες συσκευές που συνδέονται με το internet. Αυτό συνήθως επιτυγχάνεται μέσω email ή μέσω διαφόρων «προσθέτων» (plugin) που τοποθετούνται σε ιστοσελίδες στο διαδίκτυο. Συνέπεια του cryptojacking είναι ο επεξεργαστής της προσβαλλόμενης συσκευής συχνά να φτάνει στα όριά του και να επηρεάζεται η αποδοτικότητα της συσκευής, να υπερθερμαίνεται η μπαταρία, να κλείνει αυτόματα η συσκευή και να αυξάνεται το κόστος του ηλεκτρικού ρεύματος του χρήστη.

- Στην περίπτωση του cryptojacking μέσω email, ο χρήστης λαμβάνει με email έναν σύνδεσμο, που περιέχει κακόβουλο λογισμικό με κώδικα εξόρυξης. Με το που θα πατήσει τον σύνδεσμο, «φορτώνει» ο κώδικας εξόρυξης στον υπολογιστή και αρχίζει να «τρέχει» στο παρασκήνιο. Κάθε φορά που γίνεται εξόρυξη, το ποσό ανακατευθύνεται στο ψηφιακό πορτοφόλι του κυβερνοεγκληματία.



Εικόνα 18: Cryptojacking[203]

➢ Η περίπτωση του cryptojacking μέσω plugin ξεκίνησε ως μια απολύτως νόμιμη διαδικασία. Κάθε φορά που ένας χρήστης επισκεπτόταν μια ιστοσελίδα του δινόταν η επιλογή να επιλέξει αν ήθελε ή όχι η συσκευή του να χρησιμοποιηθεί ως κόμβος εξόρυξης προς όφελος του ιδιοκτήτη της ιστοσελίδας. Η εξόρυξη αυτή θα λάμβανε χώρα μόνο για όσο χρονικό διάστημα ο χρήστης θα χρησιμοποιούσε την ιστοσελίδα. Παράδειγμα αποτέλεσε το Coinhive, το οποίο αρχικά χρησιμοποιήθηκε ως εναλλακτικό μέσον εσόδων, αντί των διαφημίσεων. Το Coinhive ήταν γραμμένο σε κώδικα JavaScript, ο οποίος εγκαθίστατο σε ιστοσελίδες και, αντλώντας υπολογιστική ισχύ από τους υπολογιστές των επισκεπτών της ιστοσελίδας, προχωρούσε στην νόμιμη εξόρυξη του κρυπτονομίσματος Monero, το οποίο χρησιμοποιούσε υπολογισμούς που μπορούσαν να τρέξουν σε οποιαδήποτε συσκευή. Πολύ γρήγορα οι κυβερνοεγκληματίες εκμεταλλεύτηκαν το Coinhive προς όφελός τους, τοποθετώντας το σε ποικίλες ιστοσελίδες, προκειμένου να εξορύσσουν και να λαμβάνουν τα οφέλη της εξόρυξης. Έτσι, οι χρήστες της ιστοσελίδας και δεν γνώριζαν ότι η συσκευή τους χρησιμοποιείται ως εξορύκτης και η εξόρυξη συνέχιζε όταν αποχωρούσαν από τη συγκεκριμένη ιστοσελίδα. Επίσης, το cryptojacking υφίσταται όταν η ιστοσελίδα δεν ζητήσει ρητώς την άδεια των επισκεπτών προτού εκτελέσει το λογισμικό εξόρυξης και όταν δεν δίνει στους επισκέπτες την επιλογή «opt-out», ώστε να απενεργοποιήσουν τη λειτουργία του cryptomining. Άλλες φορές δε, το cryptojacking

[203] Enisa. *Cryptojacking - Cryptomining in the browser*. Available at: https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser (Accessed 03/06/2021).

λειτουργεί σαν ιός τύπου worm, κινούμενος μέσα στο δίκτυο και μολύνοντας διαδοχικά συσκευές[204].

4.3.3. Το cryptohacking

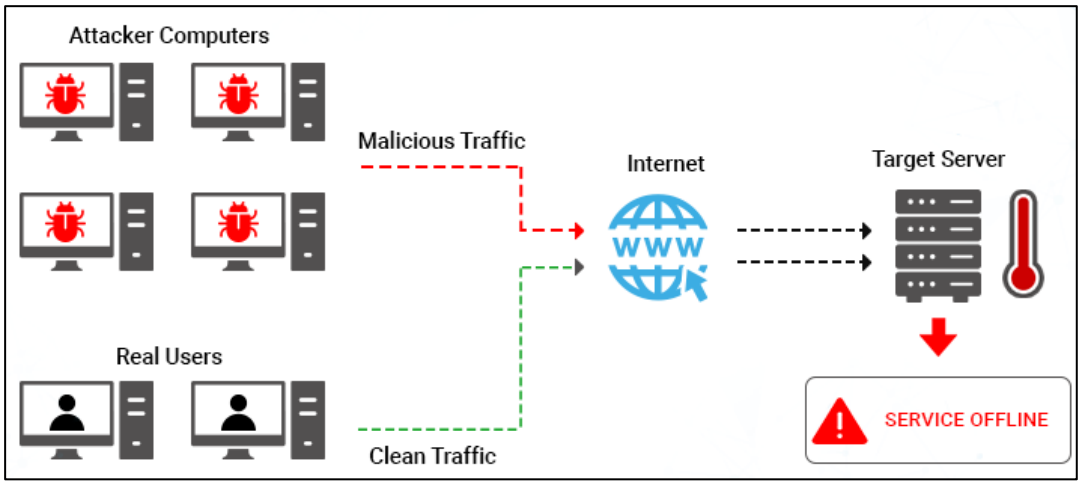
Η περίπτωση hacking (εισβολή) είναι η πιο δημοφιλής κατηγορία εγκλήματος στον κυβερνοχώρο. Ξεκίνησε ως μια μυστική τεχνική ικανότητα που σχεδιάστηκε να αποκτά πρόσβαση σε υπολογιστές ή σε δικτυακά συστήματα με σκοπό την αξιολόγηση κινδύνων και απειλών. Υπάρχουν ο όρος «white hat», που χρησιμοποιείται για να περιγράψει δραστηριότητες hacking, οι οποίες δεν έχουν εγκληματικό χαρακτήρα από τη φύση τους και ο όρος «black hat» που αναφέρεται σε οποιαδήποτε εγκληματική δραστηριότητα ή απόπειρα αυτής σχετίζεται με το hacking. Σήμερα ο όρος hacking αναφέρεται σε οποιαδήποτε δραστηριότητα περιλαμβάνει την απόκτηση ή την απόπειρα απόκτησης μη εξουσιοδοτημένης πρόσβασης σε συστήματα τεχνολογίας πληροφοριών, με σκοπό κλοπή, τροποποίηση πληροφοριών, αλλαγή στο λογισμικό ή στο υλισμικό της συσκευής.
Στο πεδίο των κρυπτονομισμάτων, το hacking έχει πολλές εφαρμογές. Χρησιμοποιείται για πρόσβαση στο ιδιωτικό κλειδί που ξεκλειδώνει το ηλεκτρονικό πορτοφόλι του χρήστη. Επιπλέον, μέσω αυτού ο hacker μπορεί να λάβει τον έλεγχο μιας ομάδας εξόρυξης και να εκμεταλλευτεί την υπολογιστική ισχύ της ομάδας προς όφελός του, προκειμένου να εξορύξει κρυπτονομίσματα για τον εαυτό του, ή προκειμένου να αντικαταστήσει τις διευθύνσεις των εξορυκτών με δικές του, ώστε να λάβει ο ίδιος την ανταμοιβή. Επιπροσθέτως, μέσω αυτού ο hacker μπορεί να χρησιμοποιήσει κάποιο malware προκειμένου να μολύνει έναν συγκεκριμένο εξορύκτη ή το σύστημα μιας εταιρείας που προσφέρει λογισμικό εξόρυξης, αναζητώντας τα ιδιωτικά κλειδιά που είναι αποθηκευμένα στα συστήματά τους[205].

4.3.4. Η επίθεση DDoS

[204] Βλ. *Μεταξάκης, Ε.*, ό.π., 240-241, Higbee, A., 2018. The role of crypto-currency in cybercrime. *Computer Fraud & Security* [online]. Vol 2018 (7), p.p. 13-15. July 2018, σελ. 13-14: Available at: https://doi.org/10.1016/S1361-3723(18)30064-2 (Accessed 27/01/2021), Enisa. *Cryptojacking: ENISA Threat Landscape.* Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cryptojacking (Accessed 03/06/2021), *Enisa,* [Cryptojacking - Cryptomining in the browser] ό.π.
[205] Βλ. *Reddy, E., Minnaar, A.,*, ό.π., σελ. 78.

Η επίθεση Distributed Denial of Service (στο εξής DDoS) έχει στόχο να προκαλέσει δυσλειτουργίες λειτουργικές, μέχρι και την πλήρη κατάρρευση του συστήματος στο οποίο επιτίθεται, ασκείται δε μέσω botnet. Οι επιτιθέμενοι δημιουργούν έναν τεράστιο αριθμό συναλλαγών, μεταφέροντας σε πολύ σύντομο χρονικό διάστημα μικρά ποσά από ένα πορτοφόλι σε άλλο. Τέτοιες ενέργειες μπορεί να αποβλέπουν στη συγκάλυψη οικονομικών συναλλαγών ή ακόμα στην ενίσχυση της απόδοσης του συστήματος και όχι τόσο στην κατάρρευση του συστήματος.

Το ίδιο το σύστημα Bitcoin προσπαθεί να εμποδίσει επιθέσεις DDoS θέτοντας υψηλά ποσά ως έξοδα μεταφοράς, τα οποία πολλές φορές είναι υψηλότερα από το ποσό της συναλλαγής. Οι επιθέσεις DDoS προκαλούν την δημιουργία τεράστιων ποσοτήτων δεδομένων, διότι το σύστημα Bitcoin δεν δίνει την δυνατότητα να διαγράφονται επιλεκτικά κάποιες αλληλουχίες συναλλαγών, με αποτέλεσμα ακόμα και οι ψεύτικες συναλλαγές να αποθηκεύονται στο Blockchain και να συμμετέχουν στις περεταίρω συναλλαγές.



Εικόνα 19: Επίθεση DDoS[206]

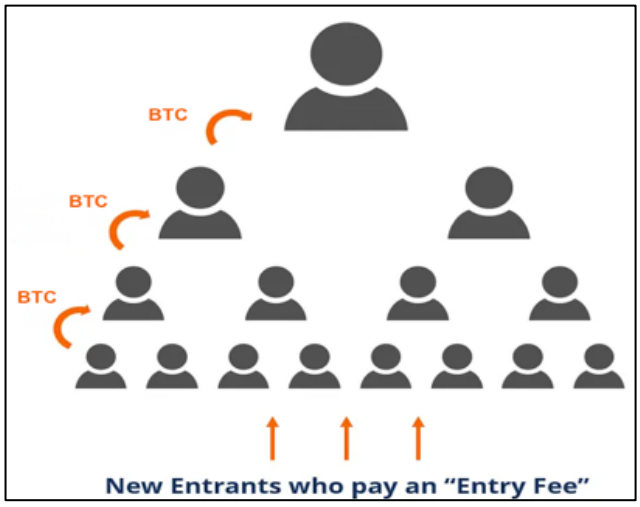
Ακόμη, οι επιθέσεις DDoS μπορεί να στοχεύουν στα ανταλλακτήρια κρυπτονομισμάτων βομβαρδίζοντάς τα με πολλαπλά πλαστά αιτήματα συναλλαγών. Ως εκ τούτου τα καθιστούν μη διαθέσιμα για κάποιο χρονικό διάστημα και αυτό έχει ως αποτέλεσμα τη μείωση του όγκου των κρυπτονομισμάτων που διακινούνται μέσω των συγκεκριμένων ανταλλακτηρίων. Λόγοι για να γίνει επίθεση σε ένα ανταλλακτήριο είναι ο ανταγωνισμός ή και η αποτροπή συγκεκριμένων επενδυτών, οι οποίοι φυλάττουν τα BTC τους στο

[206] Βλ. Coindesk. *Computer security firm Dell SecureWorks has managed to identify 146 types of bitcoin malware in the wild.* Available at: https://www.coindesk.com/nearly-150-strains-malware-bitcoins (Accessed 23/03/2021).

συγκεκριμένο ανταλλακτήριο από το να αγοράσουν ή να πωλήσουν BTC. Τέτοιου είδους επιθέσεις δεν επηρεάζουν την τιμή του BTC, αλλά τουναντίον στοχεύουν στο ίδιο το ανταλλακτήριο το οποίο υφίσταται απώλεια εσόδων, φήμης, πελατών και ζημία στο υλικό και λογισμικό του[207].

4.3.5. Η απάτη – σχήμα Ponzi

Το σχήμα Ponzi[208] είναι ένας τύπος απάτης που αποσκοπεί στο να αποκομίσει ο κυβερνοεγκληματίας υψηλά κέρδη, μέσω χαμηλού κινδύνου επενδύσεων. Προς τούτο χρησιμοποιεί μια επενδυτική επιχείρηση ώστε να παραπλανήσει το κοινό να επενδύσει BTC. Ο δράστης δελεάζει τους μελλοντικούς επενδυτές υποσχόμενος υψηλά και άμεσα κέρδη, χωρίς να διατρέχουν ιδιαίτερο κίνδυνο.



[207] Βλ. Kochkarov, A., Kochkarov, R. et Osipovich, S., 2020. Analysis of DDoS Attacks on Bitcoin Cryptocurrency Payment System. *Revista ESPACIOS* [online]. Vol. 41 (03), p. 29, σελ. 2-3: Available at: http://www.revistaespacios.com/a20v41n03/a20v41n03p29.pdf (Accessed 29/03/2021), Abhishta, A, Dragomiretskiy, S., Joosten, R. & Nieuwenhuis, B., 2019. *Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange* [online]. 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, 13-15 February 2019, at Pavia, Italy, σελ.1: Available at: https://bit.ly/3fYOP8Y (Accessed 26/05/2021), Feder, A., Gandal, N., Hamrick, J. T. & Moore, T., 2017. The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. *Journal of Cybersecurity* [online]. Vol. 3(2), p.p. 137–144. June 2017, σελ.137-138: Available at: https://bit.ly/3pvbkFK (Accessed 28/05/2021).

[208] Το όνομα το πήρε από τον δημιουργό του, Charles Ponzi τη δεκαετία του 1920, *Sándor, B., Fehér, D.J.*, ό.π., σελ. 123.

Εικόνα 20: Απάτη Ponzi[209]

Στην πράξη χρησιμοποιείται μία κυκλική τεχνική που στοχεύει στη συνεχή διεύρυνση του δικτύου των θυμάτων. Οι επενδυτές που έχουν ήδη επενδύσει, πληρώνονται με χρήματα των νέων επενδυτών και έτσι στην πραγματικότητα τα χρήματα δεν επενδύονται κάπου, αλλά ανακυκλώνονται. Τα προβλήματα με το σχήμα Ponzi, αρχίζουν όταν δεν υπάρχει πλέον νέος επενδυτής[210].

4.3.6. Το cryptophising

Το phishing (ψάρεμα) χρησιμοποιεί κυρίως την επικοινωνία μεταξύ email, για να εξαπατήσει μεμονωμένα άτομα ή οργανισμούς κάνοντάς τους να πιστεύουν ότι επικοινωνούν με νόμιμες επιχειρήσεις όπως είναι μια τράπεζα. Μόλις το θύμα πιστεί για την αξιοπιστία του αποστολέα, στόχος είναι να παρέχει προσωπικές πληροφορίες όπως στοιχεία τραπεζικού λογαριασμού, στοιχεία πιστωτικής ή χρεωστικής κάρτας, διευθύνσεις και στοιχεία ταυτότητας. Με το cryptophising στόχος των κυβερνοεγκληματιών είναι οι πληροφορίες που σχετίζονται με τις διευθύνσεις των ηλεκτρονικών πορτοφολιών των θυμάτων.

- Ένας τρόπος για να μάθουν τη διεύθυνση του ηλεκτρονικού πορτοφολιού είναι μέσω email που στέλνουν στο θύμα και που φαίνεται ότι προέρχεται από παρόχους υπηρεσιών που σχετίζονται με κρυπτονομίσματα, όπως πάροχοι πορτοφολιών ή ανταλλακτήρια κρυπτονομισμάτων. Το email είναι εξαιρετικά προσεγμένο και λεπτομερές. Για παράδειγμα μπορεί να είναι μία προειδοποίηση ασφαλείας προς το θύμα, ότι κάποιος τρίτος προσπάθησε να συνδεθεί στο λογαριασμό του από μια διεύθυνση της οποίας το link του παρέχουν, προτρέποντας συγχρόνως να συνδεθεί στο πορτοφόλι του για να διαπιστώσει αν συντρέχει κάποιος κίνδυνος. Μπορεί ακόμα, να είναι μια πρόσκληση με τη μορφή συνδέσμου για συμμετοχή σε έρευνα σχετικά με τα κρυπτονομίσματα, παρέχοντας μάλιστα και ανταμοιβή για τη συμμετοχή. Σε κάθε περίπτωση, όποιο και αν είναι το περιεχόμενο του email, το αποτέλεσμα είναι το ίδιο. Το θύμα κατευθύνεται σε μια ψεύτικη έκδοση της ιστοσελίδας, η οποία παρουσιάζει εξαιρετικές ομοιότητες με την αυθεντική. Εκεί ζητώνται τα διαπιστευτήρια του χρήστη, δηλαδή τα στοιχεία σύνδεσης στο ηλεκτρονικό του πορτοφόλι.

[209] Βλ. CFI. *Ponzi vs. Pyramid Schemes: Two investment schemes with distinctly different structures and modes of operation.* Available at: https://corporatefinanceinstitute.com/resources/knowledge/other/ponzi-vs-pyramid-schemes/ (Accessed 27/05/2021).
[210] Βλ. *Reddy, E., Minnaar, A.,* ό.π., σελ. 85, *Sándor, B., Fehér, D.J.*, ό.π., σελ. 123.

➢ Άλλος τρόπος είναι η πλαστογράφηση (spoofing) μιας νόμιμης ιστοσελίδας. Οι κυβερνοεγκληματίες δημιουργούν την εντύπωση στον χρήστη ότι συναλλάσσεται με ένα έμπιστο, νόμιμο πρόσωπο ή μια εταιρεία, καθώς η ιστοσελίδα στην οποία τον παραπέμπουν παρουσιάζει τεράστια ομοιότητα με την αυθεντική και γίνεται δυσχερές σε αυτόν να διακρίνει ότι πρόκειται για απάτη. Μόλις λοιπόν ο χρήστης συμπληρώσει το username και το password, οι κυβερνοεγκληματίες αποκτούν πρόσβαση στο πορτοφόλι του[211].

4.3.7. Η κυβερνοεκβίαση – Το cryptoransomware

Οι κυβερνοεγκληματίες, χρησιμοποιώντας κάποια από τις μεθόδους που αναλύθηκαν ανωτέρω, αποκτούν πρόσβαση σε πληροφορίες που οι χρήστες θέλουν να κρατήσουν μυστικές και ζητούν λύτρα σε BTC, προκειμένου να μην τις δημοσιοποιήσουν. Για παράδειγμα στέλνουν στον κάτοχο πορτοφολιού email και ισχυρίζονται ότι έχουν καταγράψει την δραστηριότητά του σε «ιστοσελίδες ενηλίκων» και, με την απειλή ότι θα δημοσιοποιήσουν τα στοιχεία αυτά για να τον εκθέσουν, ζητούν ως λύτρα μέχρι και το ιδιωτικό του κλειδί. Άλλο παράδειγμα αποτελεί η περίπτωση της Ashley Madison, ενός κοινωνικού δικτύου που διευκολύνει την επικοινωνία παντρεμένων ή όσων βρίσκονται σε σχέση με τρίτα άτομα. Τον Αύγουστο του 2015, hackers κατάφεραν να υποκλέψουν προσωπικά στοιχεία χρηστών που ήταν εγγεγραμμένοι στην ιστοσελίδα και παράλληλα έστελναν απειλητικά email προς τους χρήστες ζητώντας BTC για να μην δημοσιεύσουν τα στοιχεία τους[212].

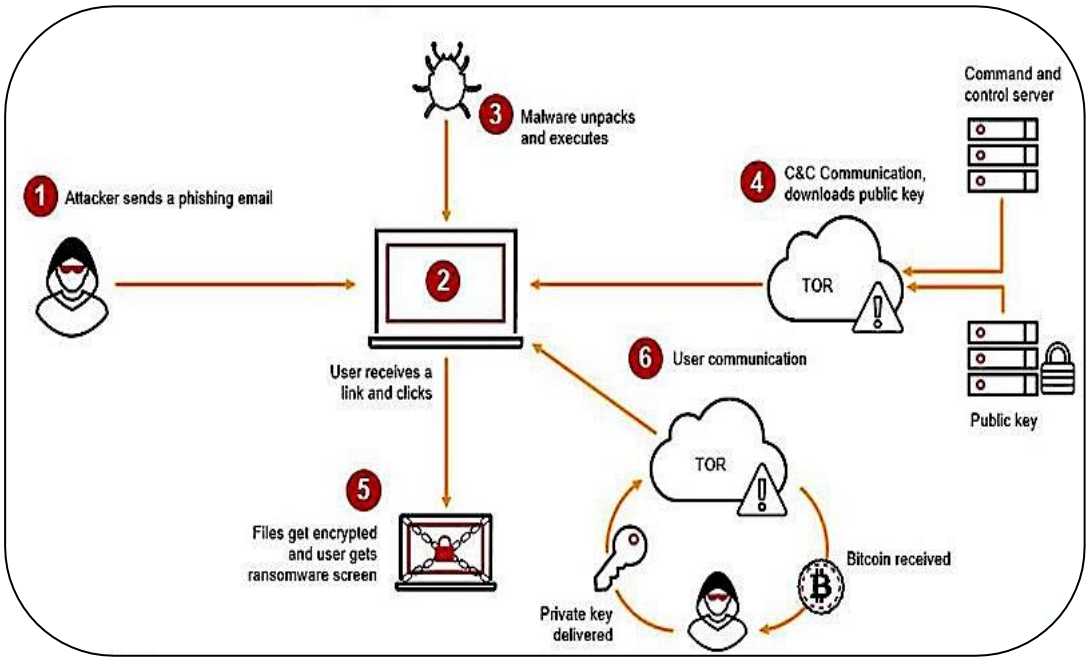
Η κυβερνοεκβίαση συναντάται κυρίως στην περίπτωση του ransomware (λυτρισμικό), το οποίο είναι ένα malware που εμποδίζει το χρήστη να έχει πρόσβαση στη συσκευή του μέχρι να καταβάλει στον επιτιθέμενο λύτρα. Τις περισσότερες φορές το ransomware ξεκινά με επίθεση phishing μέσω email, του οποίου η λήψη δεν προκαλεί μόλυνση παρά μόνο αν γίνει άνοιγμα του συνημμένου ή συνδεδεμένου αρχείου. Τότε το ransomware απελευθερώνεται και πηγαίνει απευθείας στον σκληρό δίσκο του υπολογιστή προκειμένου να τον κρυπτογραφήσει. Η επίθεση μπορεί να γίνει επίσης μέσω λήψης

---

[211] Βλ. *Higbee, A.*, ό.π., σελ. 15, *Reddy, E., Minnaar, A.,*, ό.π., σελ. 80 Liebkind, J., 2020. *Beware of These Five Bitcoin Scams.* Available at: https://www.investopedia.com/articles/forex/042315/beware-these-five-bitcoin-scams.asp (Accessed 27/01/2021), Phishing.org. *Phishing and Spoofing.* Available at: https://www.phishing.org/phishing-and-spoofing (Accessed 27/04/2021), Drozhzhin, A., 2018. *Phishing for cryptocurrencies: How bitcoins are stolen.* Available at: https://www.kaspersky.com/blog/crypto-phishing/20765/ (Accessed 10/01/2021).

[212] *WLEARN-Πρόσβαση στη Γνώση*, ό.π., *Liebkind, J.*, ό.π.

συνδέσμου από μολυσμένες ιστοσελίδες, οι οποίες εμφανίζονται ως update κάποιων δημοφιλών εφαρμογών ή μέσω των «exploit kit», δηλαδή εργαλείων που φυτεύονται από εισβολείς σε ιστοσελίδες και ανιχνεύουν τη συσκευή του χρήστη όταν επισκέπτεται την ιστοσελίδα, ώστε να εντοπίσουν ελαττώματα ή ευπάθειες που μπορούν να εκμεταλλευτούν. Μόλις εντοπιστεί μια ευπάθεια, το exploit kit εκτελεί το cryptoransomware στη συσκευή.
Από τη στιγμή που θα γίνει λήψη συνδέσμου, μπορεί να χρησιμοποιηθούν δύο τρόποι επίθεσης. Πρώτον, μπορεί να αποκλείσουν το χρήστη απενεργοποιώντας το λειτουργικό σύστημα. Έτσι, όταν ο χρήστης ενεργοποιεί τη συσκευή του, εμφανίζεται μια ειδοποίηση για λύτρα που πρέπει να καταβάλει προκειμένου η συσκευή να λειτουργήσει φυσιολογικά.



Εικόνα 21: Επίθεση Ransomware[213]

Ο δεύτερος τρόπος επίθεσης χρησιμοποιεί την ασύμμετρη κρυπτογραφία. Τα αρχεία του χρήστη κρυπτογραφούνται με ένα δημόσιο κλειδί και στη συνέχεια του εμφανίζεται μήνυμα με το οποίο οι κυβερνοεγκληματίες ζητούν λύτρα σε BTC, με αντάλλαγμα να του στείλουν το ιδιωτικό κλειδί που θα του αποκρυπτογραφήσει τα αρχεία.
Σε ορισμένες περιπτώσεις, οι κυβερνοεγκληματίες, θέλοντας να ασκήσουν επιπλέον πίεση στα θύματα τους, δίνουν περιορισμένο χρονικό διάστημα για την πληρωμή των λύτρων και τους απειλούν ότι τα αρχεία θα χαθούν, αν γίνει απόπειρα διαγραφής του ransomware. Αν

[213] Columbus, L., *How To Deal With Ransomware In A Zero Trust World.* Available at: https://bit.ly/3g10vs0 (Accessed 08/06/2021).

παρέλθει ο χρόνος που τους έχουν δώσει, το κλειδί αποκρυπτογράφησης μπορεί να διαγραφεί ή το ποσό των λύτρων να αυξηθεί. Στην πράξη, κάποιες φορές το κλειδί αποκρυπτογράφησης δεν παραδίδεται παρότι έχουν πληρωθεί τα λύτρα, με αποτέλεσμα το θύμα να υφίσταται διπλή ζημία.

Το 2017 έγινε η πιο μεγάλη επίθεση ransomware με το cryptoworm WannaCry, το οποίο επηρέασε συστήματα Windows σε ολόκληρο τον κόσμο, συμπεριλαμβανομένων πολλών που χρησιμοποιούνταν από το Εθνικό Σύστημα Υγείας του Ηνωμένου Βασιλείου (National Health System - NHS). Οι hackers απαιτούσαν λύτρα με την μορφή BTC.

Είναι πραγματικά αβέβαιο εάν στο μέλλον θα συνεχίζονται να ζητώνται ως λύτρα BTC, εξαιτίας της μεταβλητότητας της τιμής του BTC. Διότι εάν το ποσό των λύτρων είναι εξ αρχής καθορισμένο, υπάρχει ο κίνδυνος είτε να εξαιρετικά χαμηλό, οπότε τα λύτρα να μην ανταποκρίνονται στην προσπάθεια που κατέβαλαν οι hackers, είτε να έχει αυξηθεί τόσο πολύ, που στην πράξη να είναι εντελώς ανέφικτο να αποπληρωθεί. Η αβεβαιότητα αυτή οδήγησε πολλούς hackers να επιτρέπουν στα θύματά τους τη διαπραγμάτευση της τιμής των BTC, που τους επιβάλλεται να πληρώσουν[214].

4.4. Τα social media και κυβερνοέγκλημα

Τα τελευταία χρόνια τα social media χρησιμοποιούνται ως τα κατεξοχήν μέσα διαφήμισης, με αποτέλεσμα να αποτελούν το ιδανικό εργαλείο για την εξαπάτηση χρηστών Bitcoin. Ένας τρόπος είναι η παραβίαση δημοφιλών λογαριασμών με πιο διάσημο παράδειγμα την περίπτωση hacking τον Ιούλιο του 2020, όταν παραβιάστηκαν λογαριασμοί στο Twitter, οι οποίοι ανήκαν σε διασήμους όπως ο Elon Musk και ο Bill Gates ή σε εταιρείες όπως η Apple και η Uber. Οι hackers έλαβαν τον διαχειριστικό έλεγχο των λογαριασμών και προέβησαν σε δημοσιεύσεις, με τις οποίες ζητούσαν από τους ακόλουθούς τους να στείλουν χρήματα προς μία συγκεκριμένη διεύθυνση Bitcoin, με την υπόσχεση ότι

[214] Βλ. *Higbee, A.*, ό.π., σελ. 14, Connolly, L., Wall, D., 2019. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security* [online]. Vol 87, σελ. 1: Available at: https://www.sciencedirect.com/science/article/pii/S0167404819301336 (Accessed 28/01/2021), *Reddy, E., Minnaar, A.,*, ό.π., σελ. 84, Dupont, B., Haslhofer, B.,et Paquet/Clouston, M., 2019. Ransomware payments in the Bitcoin ecosystem. *JOURNAL OF CYBERSECURITY* [online]. Vol. 5 (1), p. 11. Available at:https://academic.oup.com/cybersecurity/article/5/1/tyz003/5488907 (Accessed 15/01/2021), *Sándor, B., Fehér, D.J.*, ό.π., σελ. 123, Stone, J., 2021. *Ransomware hackers launder bitcoin through just a handful of locations, researchers find.* Available at:https://www.cyberscoop.com/ransomware-hack-bitcoin-money-laundering-chainalysis/ (Accessed 29/01/2021).

τα αρχικά κεφάλαια αφού διπλασιαστούν, θα σταλούν πίσω σε όσους θα έχουν ανταποκριθεί στην παράκλησή τους. Υπολογίζεται, ότι μέσα σε λίγα λεπτά από την δημοσίευση των συγκεκριμένων tweets πραγματοποιήθηκαν 320 συναλλαγές.

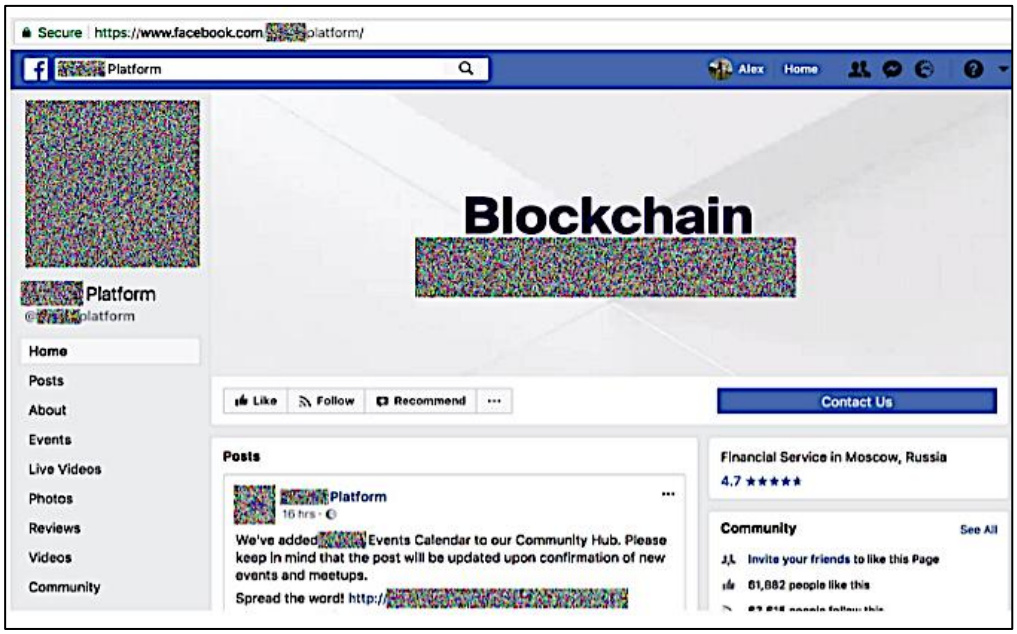
Εικόνα 22: Tweets Elon Musk και Bill Gates [215]

Ένας άλλος τρόπος εξαπάτησης χρηστών BTC είναι η δημιουργία ψεύτικων προφίλ στα social media, προκειμένου αρχικά να κερδίσουν την εμπιστοσύνη και στη συνέχεια να ζητήσουν BTC από τους ακολούθους τους. Για παράδειγμα οι απατεώνες βρίσκουν μια σελίδα στο Facebook που ασχολείται με τα κρυπτονομίσματα και δημιουργούν τον κλώνο της. Κάνουν ακόμα και τη διεύθυνση να είναι παρεμφερής με την πραγματική, αλλάζοντας για παράδειγμα μόνο ένα γράμμα, γεγονός που καθιστά δύσκολο να δει κάποιος τη διαφορά. Στη συνέχεια, στέλνουν από την ψεύτικη σελίδα μηνύματα phishing προς μέλη της πραγματικής σελίδας, κοινοποιώντας φωτογραφίες τους και κάνοντάς τους tag στην δημοσίευση. Στο Facebook, η φωτογραφία προφίλ είναι πάντα δημόσια, γεγονός που διευκολύνει τους απατεώνες να κάνουν tag όποιο άτομο επιλέξουν να εξαπατήσουν[216]. Το

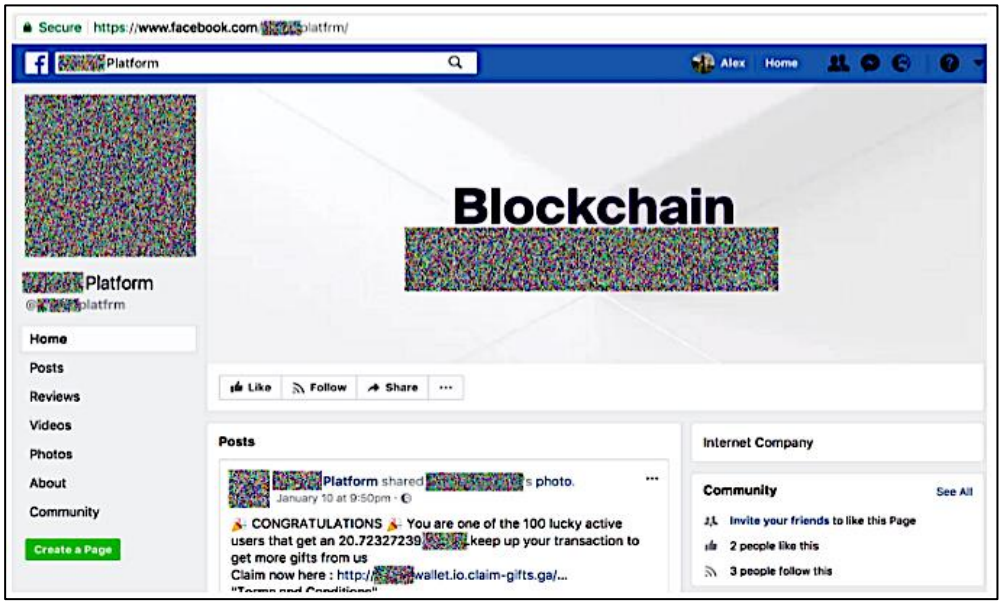
[215] D'Souza, D., 2020. *Twitter Shares Fall After Hackers Pull Off Bitcoin Scam.* Available at: https://www.investopedia.com/twitter-shares-fall-after-hackers-pull-off-bitcoin-scam-5071449 (Accessed 06/06/2021).

[216] Ο μόνος τρόπος για να μπορέσει κάποιος να αποφύγει το tag, είναι να πάει στις ρυθμίσεις και να απενεργοποιήσει τη δυνατότητα που αφορά τη δημιουργία tag από άγνωστους (για τον συγκεκριμένο χρήστη) χρήστες, σελίδες και ομάδες του Facebook.

μήνυμα που δημοσιεύουν περιέχει λεπτομέρειες τόσο αληθοφανείς και ακριβείς, που σε αρκετές περιπτώσεις γίνεται πιστευτό[217].



Εικόνα 23: Αυθεντικό προφίλ Facebook[218]



Εικόνα 24: Ψεύτικο προφίλ Facebook[219].

[217] Βλ. *Drozhzhin, A.*, ό.π., *Liebkind, J.*, ό.π.
[218] Βλ. *Drozhzhin, A.*, ό.π.
[219] Βλ. *Ibid.*

ΚΕΦΑΛΑΙΟ 5ο
ΕΙΔΙΚΕΣ ΝΟΜΟΘΕΤΙΚΕΣ ΠΡΟΒΛΕΨΕΙΣ ΓΙΑ ΤΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

Οι εξελίξεις στον κλάδο των κρυπτονομισμάτων είναι καταιγιστικές και δεν πρέπει να μας αφήνουν αδιάφορους. Τα κρυπτονομίσματα πολύ γρήγορα έγιναν παγκοσμίως γνωστά και δημιούργησαν μια νέα σφαίρα στον τομέα των δημοσίων σχέσεων, η οποία θα πρέπει να οριοθετηθεί με κανονισμούς και να υπάρχει έλεγχος. Μέσα στο κλίμα αυτό, οι αρμόδιες αρχές καλούνται να αντιμετωπίσουν πάρα πολλές προκλήσεις. Και ενώ, όσον αφορά στις υποθέσεις που τα κρυπτονομίσματα χρησιμοποιούνται ως δέλεαρ, υπάρχει νομοθετικό καθεστώς στο οποίο αυτά μπορούν να υπαχθούν, όμως στις περιπτώσεις υποθέσεων που τα κρυπτονομίσματα αποτελούν το μέσον για την τέλεση εγκληματικών ενεργειών, το πεδίο είναι θολό.

Η νέα τεχνολογία των κρυπτονομισμάτων δημιουργεί μία δομή συναλλαγών με τρόπο που δεν έχουμε ξαναδεί. Το θεσμικό πλαίσιο είναι αδύνατον να προβλέψει ρυθμίσεις για ένα τόσο καινοτόμο σύστημα πληρωμών, με αποτέλεσμα η νομική αντιμετώπιση των κρυπτονομισμάτων να μην έχει ακόμη διευκρινιστεί, αλλά να εξαρτάται από την εκάστοτε τελολογική ερμηνεία της διάταξης. Αυτό έχει ως αποτέλεσμα, η εξόρυξη και η ανταλλαγή ή οποιασδήποτε μορφής επαγγελματική συναλλαγή Bitcoin που γίνεται στην Ελλάδα, να διαφεύγει από τον έλεγχο των θεσμικών εποπτών του χρηματοπιστωτικού συστήματος. Σε κάθε ανταλλαγή ή απόθεση κρυπτονομισμάτων ελλοχεύουν κίνδυνοι παρόμοιοι με την διενέργεια μιας συναλλαγής «στο δρόμο». Κανείς δεν ελέγχει τον αντισυμβαλλόμενο, δεν πληροί κάποια προϋπόθεση για να τελεί επαγγελματικά τέτοιες συναλλαγές, αλλά ούτε εγγυάται κανείς τις συναλλαγές αυτές.

Τα τελευταία χρόνια, όλο και περισσότεροι άνθρωποι αγοράζουν κρυπτονομίσματα από ανταλλακτήρια, γεγονός που οδήγησε τις χρηματοοικονομικές αρχές σε μεγάλη ανησυχία, διότι, αν και πολλά μεγάλα ανταλλακτήρια έχουν συμμορφωθεί με τους κανόνες KYC και AML, υπάρχουν ακόμα κάποια άλλα που αντιστέκονται, εξαιτίας του ότι επιθυμούν να κρατήσουν στις πλατφόρμες τους ως χρήστες τους τρομοκράτες και τους κακούς παράγοντες. Αυτό προκάλεσε την μεγαλύτερη χρήση των κρυπτονομισμάτων, οπότε

αυξήθηκαν οι περιπτώσεις νομιμοποίησης εσόδων από παράνομες δραστηριότητες, γεγονός που διευκόλυνε απίστευτα εγκληματικές χρηματοοικονομικές ροές. Προκειμένου να προστατευτεί η παγκόσμια οικονομία και ειδικά η αγορά, θα πρέπει να υιοθετηθούν μέτρα, τα οποία δεν θα εμποδίζουν την καινοτομία ούτε θα στοχεύουν στον έλεγχο της χρήσης των κρυπτονομισμάτων, αλλά θα αποσκοπούν στην αποτροπή τυχόν παρεκκλίσεων της χρήσης, για την οποία τα μέτρα αυτά έχουν τεθεί σε λειτουργία. Μέσα στο κλίμα αυτό που έχει δημιουργηθεί, η ΕΕ δεν έμεινε άπραγη, τουναντίον παρατηρείται ότι το ευρωπαϊκό ρεύμα ανανεώνεται, καθώς υιοθετούνται νέοι κανόνες, που αφορούν το ξέπλυμα χρήματος και την χρηματοδότηση της τρομοκρατίας. Οι κανόνες αυτοί περιλαμβάνουν μέτρα και ρητές προβλέψεις για τα κρυπτονομίσματα και για κάποιες από τις οντότητες που συμμετέχουν στο οικοσύστημα των κρυπτονομισμάτων[220].

[220] Βλ. *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ.502, *Μούζουλας, Σ.*, ό.π., σελ. 1182, Ντότσιας, Σ., 2018. Ο λογιστικός λαβύρινθος των ψηφιακών νομισμάτων. *Επιχείρηση,* 12(141), σελ. 324, Alekseeva, S.S., Bolotaeva, O.S. et Stepanova, A.A., 2019. The Legal Nature of Cryptocurrency. *IOP Conference Series: Earth and Environmental Science* [online]. Vol 272(3), p. 5. June 2019, σελ. 2: Available at: https://bit.ly/2RMY5E0 (Accessed 27/01/2021), *U.S. House of Representatives, Subcommittee on Terrorism and Illicit Finance, Committee on Financial Services, Washington, D.C.*, ό.π., Simon, ό.π., σελ. 1, *HM Treasury*. ό.π., σελ. 40, Houben, R., Snyers, A., ό.π., σελ. 57, Bongcayao, R.J., ό.π., σελ. 14.

5.1. Ευρωπαϊκή Ένωση - Η Οδηγία AML5

Η Ευρωπαϊκή Ένωση σχεδόν εξαρχής ενδιαφέρθηκε για τα κρυπτονομίσματα. Αρχικά έγιναν προσπάθειες για την πλήρη κατανόηση της τεχνολογίας του Blockchain. Το 2017 ήταν η πρώτη φορά που αντιμετώπισε σοβαρά την ύπαρξή του καθώς και τις επιπτώσεις που μπορεί να προκαλέσει, οπότε και δημοσιεύτηκε από το ερευνητικό τμήμα του Ευρωπαϊκού Κοινοβουλίου η πρώτη έκθεση που αφορούσε το Blockchain, με τίτλο «How Blockchain technology could change our lives». Ένα χρόνο αργότερα, τον Φεβρουάριο 2018, ιδρύθηκε το EU Blockchain Observatory and Forum[221] με κύριο σκοπό την ενημέρωση οργάνων, κυβερνήσεων και του κοινού για τις κυριότερες εξελίξεις αυτής της τεχνολογίας, την αξιοποίηση των νέων δυνατοτήτων που παρέχει, την συγκέντρωση εμπειρογνωσίας, την προώθηση ευρωπαϊκών φορέων, καθώς και την ενίσχυση της συνεργασίας μεταξύ των κρατών-μελών και μεταξύ όσων συμμετέχουν σε δραστηριότητες που χρησιμοποιούν την τεχνολογία Blockchain.

Τα κρυπτονομίσματα δεν ελέγχονται από κάποια κεντρική αρχή γεγονός, που αποκλείει τη δυνατότητα οποιασδήποτε νομισματικής παρέμβασης, ως εργαλείο άσκησης οικονομικής πολιτικής. Μια από τις μεγαλύτερες προκλήσεις που καλείται να αντιμετωπίσει η ΕΕ είναι να ρυθμίσει ένα σύστημα που στηρίζεται στο αποκεντρωμένο δίκτυο, ως να απευθυνόταν σε κεντρικό σύστημα, διότι ως γνωστόν τα κρυπτονομίσματα είναι αποκεντρωμένα και εντελώς αντιθετικά στην ήδη υπάρχουσα κανονιστική δομή των νομισματικών και οικονομικών κανονισμών. Αν και τα κρυπτονομίσματα φημίζονται ότι κατάφεραν να αποτινάξουν τον έλεγχο κάποιας κεντρικής αρχής, στην πράξη δημιούργησαν κάποια νέα είδη ενδιαμέσων, τα οποία καλούνται ανταλλακτήρια κρυπτονομισμάτων, πάροχοι πορτοφολιών και πλατφόρμες συναλλαγών.

Από νωρίς κατέστη σαφές ότι κάθε εταιρεία που δρα ως ενδιάμεσος ή που εμπλέκεται σε μια συναλλαγή όπου γίνεται χρήση κρυπτονομισμάτων, θα πρέπει να έχει ένα πρόγραμμα συμμόρφωσης και προστασίας για ξέπλυμα χρήματος μέσω της εφαρμογής της πολιτικής KYC/AML. Η ανάγκη λοιπόν υπαγωγής των ενδιαμέσων στη νομοθεσία για το ξέπλυμα χρήματος κατέστη επιτακτική, καθώς αυτός ήταν ο μόνος τρόπος ώστε, τουλάχιστον σε επίπεδο ΕΕ να μειωθούν οι πιθανότητες να χρησιμοποιηθούν τα κρυπτονομίσματα με

[221] EUBlockchain. *Η Ευρωπαϊκή Επιτροπή εγκαινιάζει το παρατηρητήριο - φόρουμ της ΕΕ για την τεχνολογία blockchain.* Ανακτήθηκε από: https://ec.europa.eu/greece/news/20180201_blockchain_el (Πρόσβαση 27/05/2021).

δόλιους σκοπούς. Στην πραγματικότητα βέβαια, η έννοια του «ενδιαμέσου» βοήθησε την ΕΕ να εξέλθει από το τέλμα αδράνειας στο οποίο την είχε εγκλωβίσει η νέα τεχνολογία των κρυπτονομισμάτων και να επικεντρωθεί στο να ρυθμίσει αυτήν την έννοια ως πιο γνώριμη, ξεκινώντας με την Οδηγία 2018/843, η οποία τροποποιεί την οδηγία 2015/849 σχετικά με «την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και για τη χρηματοδότηση της τρομοκρατίας» (Combating the Financing of Terrorism, στο εξής CFT) /Anti-Money Laundering (στο εξής AML5). Η AML5 επικεντρώνεται κυρίως στις διαδικασίες που γενικά ακολουθούνται για την μετακίνηση χρημάτων που συνδέονται με εγκληματικές δραστηριότητες. Η CFT υπάγεται στην AML5, αποτελεί μια περεταίρω εξειδίκευση, καθώς επικεντρώνεται στην πρόληψη κίνησης κεφαλαίων που σχετίζονται με την τρομοκρατία και επίσης περιλαμβάνει το μπλοκάρισμα συναλλαγών που προορίζονται για επίτευξη ιδεολογικών, θρησκευτικών και πολιτικών εξτρεμιστικών σκοπών[222].

5.1.1. Οι έννοιες AML και KYC

Οι κανονισμοί, που αποσκοπούν στη διακοπή του τεράστιου κύματος της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, έχουν αρχίσει να ανανεώνονται ώστε να συμπεριλάβουν στο ρυθμιστικό τους πεδίο και τις οντότητες που συνδέονται με τη χρήση κρυπτονομισμάτων.

Ο όρος AML (Anti-Money Laundering) αναφέρεται σε ένα σύνολο διαδικασιών και νομικών κανονισμών που στοχεύουν στον εντοπισμό και στην αποτροπή κτήσης κέρδους από παράνομες δραστηριότητες. Ένα πρόγραμμα AML περιλαμβάνει μία πολιτική αποδοχής πελατών (Customer Acceptance Policy – στο εξής CAP), ένα πρόγραμμα ταυτοποίησης πελατών (Customer Identification Program στο εξής CIP), τον έλεγχο των συναλλαγών και τις διαδικασίες διαχείρισης κινδύνου.

Ο όρος KYC (Know Your Customer) συμπεριλαμβάνει τις διαδικασίες που ακολουθούνται στα CAP και CIP, όντας το αρχικό στάδιο της επισταμένης έρευνας που πρέπει να

[222] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ.*, ό.π., σελ. 11, Παρασκευόπουλος-Κόλιας, Χ., 2014. *Οικονομικές τεχνικές και Νομικές όψεις του Bitcoin*, σελ. 2: Ανακτήθηκε από: https://www.yiannatsis.gr/download/bitcoin%20gr.pdf (Πρόσβαση 22/04/2021), *Παπαδοπούλου, Α.*, ό.π., σελ. 211, Nabilou, H., 2019. How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency. *International Journal of Law and Information Technology* [online]. Vol 27(3), p.p. 266-291, σελ. 1-2: Available at: DOI:10.2139/ssrn.3360319 (Accessed 26/02/2021), Bongcayao, R.J., ό.π., σελ. 13-14, Getit. *The 2021 Guide to AML and KYC for Crypto Exchanges & Wallets. Available at: https://getid.ee/aml-kyc-crypto-exchanges-wallets/* (Accessed 23/05/2021).

διεξάγεται. Δηλαδή, επαληθεύει την ταυτότητα του υποψηφίου πελάτη, μέσω της συλλογής προσωπικών στοιχείων του δηλαδή όνομα, ημερομηνία γέννησης, διεύθυνση, ΑΜΚΑ, email, τα οποία επαληθεύονται από επίσημα έγγραφα του κράτους όπως διαβατήριο ή δίπλωμα αυτοκινήτου και από λογαριασμούς κοινής ωφέλειας. Υπάρχουν ακόμη και τα συστήματα Digital ID, τα οποία ζητούν από τους χρήστες να βγάλουν μια selfie για να γίνει βιομετρική αναγνώριση προσώπου ή να βγάλουν ένα βίντεο[223] του προσώπου προκειμένου το σύστημα μέσω της διαδικασίας liveness detection να μπορέσει να εντοπίσει ότι βιομετρικά δεδομένα είναι αληθή. Ο έλεγχος των συναλλαγών από τα ανταλλακτήρια γίνεται με διαδικασίες αναγνώρισης ύποπτων δραστηριοτήτων, ανάλυσης συμπεριφοράς των πελατών και επαλήθευσης ότι τα δεδομένα πελατών κρατούνται ενημερωμένα[224].

5.1.2. Το οικοσύστημα των κρυπτονομισμάτων υπό το πρίσμα της AML5

Υπό το πρίσμα της Οδηγίας AML4[225] (*2015/849)*, τα κρυπτονομίσματα δεν μπορούσαν να υπαχθούν σε καμία οντότητα από αυτές που προβλέπονταν, γεγονός που οδήγησε στις 5 Ιουλίου 2016 στο να κατατεθεί πρόταση από την Ευρωπαϊκή Επιτροπή για την τροποποίηση αυτής. Η πρόταση αυτή υποστηρίχθηκε και από την EBA και την ECB και πλέον η Οδηγία AML5[226] έχει ενσωματωθεί και στην ελληνική έννομη τάξη με τον Ν.4734/2020, ο οποίος τροποποίησε το Ν.4557/2018 περί «πρόληψης και καταστολής της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες». Η αιτιολογία της AML5 αναφέρει συγκεκριμένα στη σκέψη 8 ότι: «*οι πάροχοι υπηρεσιών ανταλλαγής μεταξύ «εικονικών νομισμάτων» και παραστατικών νομισμάτων, καθώς και οι πάροχοι υπηρεσιών θεματοφυλακής ψηφιακών πορτοφολιών δεν έχουν υποχρέωση κατά την ενωσιακή νομοθεσία να εντοπίζουν την ύποπτη δραστηριότητα. Συνεπώς, οι τρομοκρατικές ομάδες είναι πιθανώς*

---

[223] Το σύστημα ζητά από το χρήστη να ολοκληρώσει κάποια βήματα όπως να ανοιγοκλείσει τα μάτια, να σηκώσει τα φρύδια, να χαμογελάσει, γυρίσει το κεφάλι δεξιά και αριστερά.

[224] Βλ. *Getit.* ό.π., *Hoete-Dodd,* V., ό.π.

[225] Οδηγία 2015/849/ΕΕ, ΕΚ και ΣΕΕ (20/05/2015). *Σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 2006/70/ΕΚ της Επιτροπής (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015L0849&from=DA (Πρόσβαση 08/06/2021).

[226] Οδηγία 2018/843/ΕΕ και ΣΕΕ, (30/05/2018). *Για την τροποποίηση της οδηγίας (ΕΕ) 2015/849 σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, και για την τροποποίηση των οδηγιών 2009/138/ΕΚ και 2013/36/ΕΕ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32018L0843&from=EN (Πρόσβαση 26/05/2021).

σε θέση να μεταφέρουν χρήματα στο χρηματοπιστωτικό σύστημα της Ένωσης ή εντός δικτύων εικονικών νομισμάτων, συγκαλύπτοντας μεταφορές ή επωφελούμενες από έναν ορισμένο βαθμό ανωνυμίας στις εν λόγω πλατφόρμες. Ως εκ τούτου, είναι σημαντικό να επεκταθεί το πεδίο εφαρμογής της οδηγίας (ΕΕ) 2015/849 ούτως ώστε να περιλαμβάνει παρόχους υπηρεσιών ανταλλαγής μεταξύ εικονικών και παραστατικών νομισμάτων, καθώς και παρόχους υπηρεσιών θεματοφυλακής ψηφιακών πορτοφολιών. Για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, οι αρμόδιες αρχές θα πρέπει να μπορούν, μέσω υπόχρεων οντοτήτων, να παρακολουθούν τη χρήση των εικονικών νομισμάτων. Μια τέτοια παρακολούθηση θα παρείχε ισορροπημένη και αναλογική προσέγγιση, διασφαλίζοντας την τεχνολογική πρόοδο και τον υψηλό βαθμό διαφάνειας που έχει επιτευχθεί στον τομέα της εναλλακτικής χρηματοδότησης και της κοινωνικής επιχειρηματικότητας».

Πράγματι λοιπόν η AML5 εισήγαγε πλέον ρητώς, στο άρ.1 παρ.1 περίπτωση γ΄, στοιχεία ζ΄ και η΄, δύο νέες υπόχρεες οντότητες, τους «*ζ) **παρόχους που ασχολούνται με υπηρεσίες ανταλλαγής** μεταξύ εικονικών νομισμάτων και παραστατικών νομισμάτων»* (Virtual Currency Exchange Platforms, στο εξής VCEPs) και τους «*η) **παρόχους υπηρεσιών θεματοφυλακής ψηφιακών πορτοφολιών***» (Custodian Wallet Providers, στο εξής CWPs). Τα ανταλλακτήρια και οι πάροχοι πορτοφολιών θα πρέπει να αποδεικνύουν ότι έχουν τα κατάλληλα προγράμματα AML/KYC και να αναφέρουν στις αρμόδιες αρχές κάθε ύποπτη συναλλαγή που θα υποπέσει στην αντίληψή τους[227].

Σύμφωνα λοιπόν με το στοιχ.18 στο άρ.1 παρ.2 περίπτ.δ' της AML5: ως ***«εικονικό νόμισμα»*** *νοείται μια ψηφιακή αναπαράσταση αξίας που δεν εκδίδεται από κεντρική τράπεζα ή δημόσια αρχή ούτε έχει την εγγύησή τους, δεν συνδέεται κατ' ανάγκη με νομίμως κυκλοφορούν νόμισμα και δεν διαθέτει το νομικό καθεστώς νομίσματος ή χρήματος, όμως γίνεται αποδεκτή από φυσικά ή νομικά πρόσωπα ως μέσο συναλλαγής και μπορεί να μεταφέρεται, να αποθηκεύεται ή να διακινείται ηλεκτρονικά».*

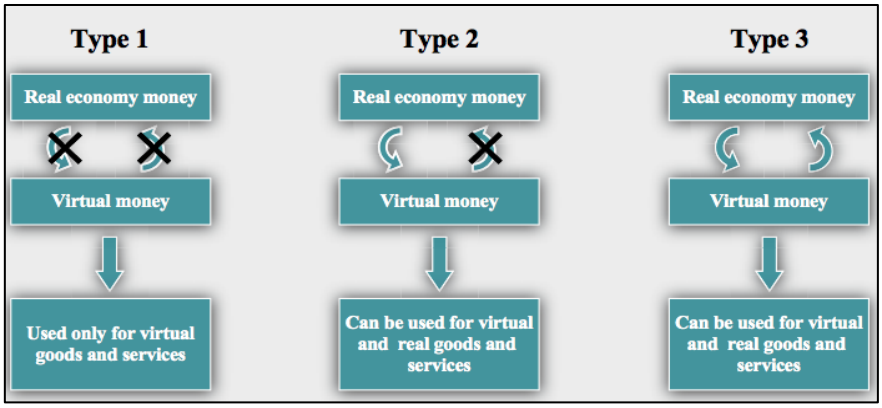
Ακόμη προστίθεται το στοιχ.19 στο άρ.1 παρ.2 περίπτ.δ' σύμφωνα με το οποίο: ως «***πάροχος υπηρεσιών θεματοφυλακής πορτοφολιών*** *νοείται μια οντότητα που παρέχει υπηρεσίες για τη διασφάλιση ιδιωτικών κρυπτογραφικών κλειδιών για λογαριασμό των πελατών της, με στόχο τη διακράτηση, αποθήκευση και μεταβίβαση εικονικών νομισμάτων»*.

[227] Βλ. Houben, R., Snyers, A., ό.π., σελ. 62, 65-66, Βλ. *Getit*. ό.π.

5.2. Η αξιολόγηση της Οδηγίας AML5

Όπως αναφέρεται στην AML5: *«Στόχος της παρούσας οδηγίας είναι να καλύψει όλες τις δυνητικές χρήσεις των εικονικών νομισμάτων»*. Είναι πραγματικά μια αξιόλογη προσπάθεια υπαγωγής του νέου αυτού οικοσυστήματος στη νομοθεσία της ΕΕ. Εντούτοις υπάρχουν ακόμα αρκετά σημεία για τα οποία δεν υπάρχει πρόβλεψη και ενδέχεται να δημιουργήσουν προβλήματα στο μέλλον. Υπάρχουν κάποια σημεία[228] της οδηγίας που τυγχάνουν της προσοχής:

➢ Στην AML5 παρατηρείται ότι δεν αναφέρεται ο όρος «κρυπτονομίσματα», αλλά ο όρος «εικονικά νομίσματα». Η ECB σε έκθεση που δημοσίευσε το 2012, υποστήριξε ότι τα κρυπτονομίσματα είναι ένα υποσύνολο των εικονικών νομισμάτων, που αποτελούνται από τις εξής τρεις κατηγορίες[229]:



Εικόνα 25: Τύποι εικονικών νομισμάτων[230]

[228] Βλ. Houben, R., Snyers, A., ό.π., σελ. 75-79, Βλ. *Getit.* ό.π., *Cavin, C., Chiriaeva, M. & Poskriakov, F*, ό.π., σελ.168-169, Perry, M., 2019. *Bitcoin ATMs a "Hole" in EU Anti-Money Laundering Rules*. Available at: https://www.occrp.org/en/daily/10200-bitcoin-atms-a-hole-in-eu-anti-money-laundering-rules (Accessed 26/05/2021), HFW. *A NEW FRONTIER FOR AML REGULATION: THE FIFTH ANTI-MONEY LAUNDERING DIRECTIVE AND CRYPTOCURRENCIES. Available at:* https://www.hfw.com/A-New-Frontier-for-AML-Regulation-Sep-18 (Accessed 05/06/2021), Covolo, V., 2019. The EU Response to Criminal Misuse of Cryptocurrencies: The young, already outdated 5th Anti-Money Laundering Directive1. *European Journal of Crime, Criminal Law and Criminal Justice*[online]. Vol 28(3). 29 Sept.2020. σελ.14-16: Available at: https://doi.org/10.1163/15718174-bja10003 (Accessed 28/05/2021), Miggiani, K., 2020. *AMLD 5 and the EU May 2020 AML/CFT Action Plan – where do crypto assets fit into the emerging landscape?*. Available at: https://bit.ly/3git0Bs (Accessed 07/06/2021), Fromberger, M., Haffke, L. & Zimmermann, P., ό.π., σελ.7-14, *Getit.* ό.π., SYGNA. *A Guide to the EU's 5th Anti-Money Laundering Directive (AMLD5).* Available at: https://www.sygna.io/blog/what-is-amld5-anti-money-laundering-directive-five-a-guide/ (Accessed 27/04/2021).

[229] *European Central Bank [2012]. ό.π.*,σελ.13-16, *European Central Bank.[2015]* ό.π., σελ. 25.

[230] Βλ. *European Central Bank [2012], ό.π.*,σελ.16.

- Πρώτον, τα εικονικά νομίσματα που υπάρχουν στα ηλεκτρονικά παιχνίδια. Τα νομίσματα που αποκτώνται σχετίζονται μόνο με τον εικονικό κόσμο των παιχνιδιών και ουδεμία σχέση έχουν με την πραγματική οικονομία ή με τα οικονομικά και τραπεζικά συστήματα. Οι χρήστες αποκτούν τα νομίσματα αυτά είτε μέσω των εικονικών δραστηριοτήτων και της εκπλήρωσης αποστολών, που λαμβάνουν χώρα στο περιβάλλον των παιχνιδιών που παίζουν, είτε μέσω της αγοράς αυτών με χρήση του παραστατικού χρήματος. Τέτοιο παράδειγμα αποτελεί το World of Warcraft Gold.
- Δεύτερον, τα εικονικά νομίσματα μονόδρομης κατεύθυνσης που είναι διαθέσιμα είτε στα παιχνίδια για αγορά εικονικών αγαθών και υπηρεσιών είτε στον πραγματικό κόσμο για αγορά πραγματικών αγαθών και υπηρεσιών. Τέτοιο παράδειγμα είναι τα Nintendo Points αλλά και τα Facebook Credits όταν υπήρχαν.
- Τρίτον, τα εικονικά νομίσματα αμφίδρομης ροής, στα οποία οι χρήστες είναι ελεύθεροι να αγοράσουν και να πουλήσουν εικονικά νομίσματα, σύμφωνα με την ισοτιμία παραστατικού χρήματος και να τα χρησιμοποιήσουν στον πραγματικό κόσμο, όπως κάθε άλλο νόμισμα. Με αυτού του είδους τα νομίσματα μπορούν να αγοραστούν και πραγματικά και εικονικά αγαθά και υπηρεσίες. Στην κατηγορία αυτή ανήκει το ψηφιακό νόμισμα BTC[231].

➢ Προβληματισμός προκύπτει από τον ορισμό των εικονικών νομισμάτων, στον οποίο αναφέρεται ότι αυτά θα πρέπει να μεταφέρονται, αποθηκεύονται και εμπορεύονται ηλεκτρονικά, χωρίς να διευκρινίζει αν θα πρέπει να είναι μόνο αμφίδρομης ροής και να είναι ανταλλάξιμα με παραστατικό χρήμα. Η ορθότερη προσέγγιση και το νομικό δόγμα που έχει επικρατήσει, όπως προκύπτει από το άρ.1 παρ.1 περίπτωση γ΄, στοιχείο ζ΄, είναι ότι ο σκοπός της οδηγίας τείνει να συμπεριλάβει μόνο συγκεκριμένα σχήματα αμφίδρομης κατεύθυνσης και όχι σχήματα των άλλων δύο κατηγοριών. Δηλαδή, όχι τα νομίσματα που αποκτήθηκαν με χρήση του παραστατικού χρήματος και στη συνέχεια χρησιμοποιήθηκαν μόνο στον εικονικό κόσμο για αγορά αγαθών και υπηρεσιών ή και για ανταλλαγή με άλλα εικονικά νομίσματα. Τούτο διότι, αυτά ή δεν συνδέονται με την πραγματική οικονομία ή είναι μονόδρομης κατεύθυνσης, δηλαδή μετατρέπονται μόνο από παραστατικό χρήμα σε

[231] Βλ. Σύμφωνα με την έκθεση της Ευρωπαϊκής Κεντρικής Τράπεζας, ο όρος ψηφιακό νόμισμα είναι ευρύτερος του όρου εικονικό. Αυτό προκύπτει και από τον ορισμό που δίνει, *European Central Bank.[2015]* ό.π., σελ.25.

εικονικό. Επομένως, στο κείμενο της AML5 η έννοια εικονικά νομίσματα είναι ταυτόσημη με αυτήν των κρυπτονομισμάτων. Η συστολή αυτή του ορισμού των εικονικών νομισμάτων δημιουργεί κενό δικαίου, επιτρέποντας δραστηριότητες που οδηγούν σε ξέπλυμα χρήματος και χρηματοδότηση της τρομοκρατίας. Προς το παρόν, το κενό δικαίου δεν φαίνεται να επηρεάζει ιδιαίτερα όσες συναλλαγές γίνονται με χρήση εικονικών νομισμάτων, διότι ακόμη και αν υπάρχουν έσοδα από παράνομες δραστηριότητες ή από χρηματοδότηση της τρομοκρατίας, αυτά τα χρήματα είναι κατά κάποιοι τρόπο εγκλωβισμένα στον εικονικό κόσμο και δεν επιδρούν στην πραγματική οικονομία. Φυσικά, τα κρυπτονομίσματα μπορούν να χρησιμοποιηθούν ως μέσον πληρωμής για παράδειγμα όταν ένα άλλο άτομο συμφωνεί να τα λάβει ως πληρωμή, στην πράξη όμως δεν εφαρμόζεται για μεγάλα χρηματικά ποσά που προέρχονται από ξέπλυμα χρήματος. Μελλοντικά, εφόσον η αποδοχή των εικονικών νομισμάτων αυξηθεί, δεν θα χρειάζεται να μετατραπούν σε παραστατικό χρήμα.

- Στο στοιχ.11 της οδηγίας αναφέρεται ότι: «*Τα τοπικά νομίσματα*[232]*, γνωστά επίσης ως συμπληρωματικά νομίσματα, που χρησιμοποιούνται σε πολύ περιορισμένα δίκτυα, όπως πόλεις ή περιφέρειες, και μεταξύ μικρού αριθμού χρηστών δεν θα πρέπει να θεωρούνται εικονικά νομίσματα*». Αυτό σημαίνει ότι τα κρυπτονομίσματα δεν αρκεί μόνο να πληρούν τα κριτήρια που θέτει ο ορισμός της οδηγίας, αλλά και να έχουν λάβει αναγνώριση, τουλάχιστον μεγαλύτερη των γεωγραφικών ορίων μιας πόλης.

- Στην AML5 δεν υπάρχει πρόβλεψη για όλες τις οντότητες που συναντώνται στο οικοσύστημα των κρυπτονομισμάτων. Ο νομοθέτης περιόρισε το σκοπό της Οδηγίας μόνο στους CWPs και στα VCEPs είτε επιτηδευμένα για κάποιες κατηγορίες όπως για τους παρόχους πορτοφολιών λογισμικού και για τα ανταλλακτήρια κρυπτονομισμάτων που επιτρέπουν την ανταλλαγή μόνο με άλλα κρυπτονομίσματα (στο εξής crypto-crypto), είτε επιδεικνύοντας αμέλεια για κάποιες άλλες όπως για τις πλατφόρμες ανταλλαγής, για τους εξορύκτες και για τους παρόχους πορτοφολιών υλισμικού.

Πιο συγκεκριμένα:

[232] Παράδειγμα τοπικού νομίσματος είναι ο «Ήλιος», που κυκλοφορεί στην Πιερία, Ελλάδα και η ισοτιμία του είναι 1 Ήλιος = 1 ευρώ.

- Οι **χρήστες** εκπίπτουν του σκοπού της Οδηγίας, καθώς αυτή επικεντρώνεται πρωτίστως στη ρύθμιση των ενδιαμέσων.
- Οι **εξορύκτες** δεν περιλαμβάνονται στον σκοπό της οδηγίας κυρίως για δύο λόγους. Ο πρώτος είναι ότι αντιμετωπίζονται περισσότερο ως «πάροχοι» τεχνικών υπηρεσιών παρά ως οι ενδιάμεσοι στην εικονική σφαίρα και στον πραγματικό κόσμο. Ο δεύτερος λόγος σχετίζεται με την παρουσία των εξορυκτών γεωγραφικά, διότι εντοπίζονται ως επί το πλείστον στην Κίνα, όπου η AML5 δεν μπορεί να εφαρμοστεί. Οι εξορύκτες μπορεί να είναι μεμονωμένος χρήστης ή ομάδες χρηστών, οι οποίες χρησιμοποιώντας την εξόρυξη κρυπτονομισμάτων για επιχειρηματικούς λόγους τα πωλούν παίρνοντας παραστατικό χρήμα ή άλλα κρυπτονομίσματα. Ο νομοθέτης πήρε ως παράδειγμα το BTC και κατέληξε στο συμπέρασμα ότι οι κυβερνοεγκληματίες δύσκολα θα λειτουργήσουν ως εξορύκτες, καθώς η διαδικασία της εξόρυξης απαιτεί τεράστια υπολογιστική ισχύ και τεχνογνωσία (know-how). Η σκέψη του αυτή όμως δημιουργεί προβληματισμούς, καθώς υπάρχει πληθώρα άλλων κρυπτονομισμάτων, τα οποία εξορύσσονται με απλούστερες διαδικασίες και πιθανόν όχι στην Κίνα. Το κενό πρόβλεψης που υπάρχει στην οδηγία ενδέχεται να δημιουργήσει προβλήματα στο μέλλον και σε καμία περίπτωση δεν πρέπει να υποτιμηθεί το ενδιαφέρον που μπορεί να επιδείξουν οι εγκληματίες για την εξορυκτική διαδικασία έχοντας όμως απώτερο στόχο την παράνομη χρήση των κρυπτονομισμάτων. Ενδεχομένως, η υιοθέτηση μιας πολιτικής Know-Your-Miner να οδηγήσει σε κάποιες ικανοποιητικές λύσεις.
- Οι **πάροχοι πορτοφολιών** περιλαμβάνονται μερικώς στο σκοπό της AML5. Υπάρχουν τρείς κατηγορίες παρόχων, οι πάροχοι υλισμικού, οι πάροχοι λογισμικού και οι διαδικτυακοί πάροχοι. Όπως προκύπτει από τον ορισμό της οδηγίας, στο πεδίο εφαρμογής της εμπίπτουν μόνο οι διαδικτυακοί πάροχοι δηλαδή αυτοί που είναι επιφορτισμένοι με *«τη διασφάλιση ιδιωτικών κρυπτογραφικών κλειδιών για λογαριασμό των πελατών της, με στόχο τη διακράτηση, αποθήκευση και μεταβίβαση εικονικών νομισμάτων»*. Οι πάροχοι υλισμικού και οι λογισμικού δεν εντάσσονται, καθώς δεν αποθηκεύουν τα ιδιωτικά κλειδιά για λογαριασμό των πελατών τους απλώς παρέχουν τα μέσα και τα εργαλεία, αντίστοιχα, προκειμένου οι πελάτες να τα διαφυλάξουν μόνοι τους.

- Τα **ανταλλακτήρια** crypto-crypto δεν συμπεριλαμβάνονται στην AML5 με αποτέλεσμα οι κυβερνοεγκληματίες, όταν θελήσουν να μετατρέψουν τα κρυπτονομίσματα σε παραστατικό χρήμα, να δύνανται να εκμεταλλευθούν ένα επιπλέον επίπεδο για απόκρυψη της προέλευσης κρυπτονομισμάτων που προέρχονται από παράνομες δραστηριότητες. Στην πράξη, πολλάκις τα ανταλλακτήρια crypto-crypto λειτουργούν και ως CWPs και ίσως αυτός είναι ο λόγος που δεν συμπεριλήφθηκαν στις οντότητες της οδηγίας[233]. Ένα κράτος μέλος όμως μπορεί να προβλέψει και να συμπεριλάβει και τα ανταλλακτήρια crypto-crypto κατά την ενσωμάτωση της οδηγίας στο εθνικό του δίκαιο.
- Οι **πλατφόρμες συναλλαγών** λειτουργούν αποκλειστικά με λογισμικό χωρίς να επιβλέπονται και η ανταλλαγή κρυπτονομισμάτων γίνεται απευθείας μεταξύ των χρηστών. Η περίπτωση της ατομικής αυτής συναλλαγής δεν μπορεί να ενταχθεί στον σκοπό της οδηγίας καθώς από αυτήν ελλείπει η έννοια του ενδιάμεσου προσώπου. Μελλοντικά θα ήταν σημαντική η επέκταση του σκοπού της οδηγίας στις πλατφόρμες ανταλλαγών (P2P), καθώς αυτές αποτελούν περιβάλλον όπου οι χρήστες εύκολα θα πέσουν θύματα ή εξαπάτησης, ή κοινωνικών μηχανών (social engineering[234]) ή επιστροφής χρεώσεων.
- Οι **δημιουργοί των κρυπτονομισμάτων** δεν εμπίπτουν στο σκοπό της οδηγίας, γεγονός το οποίο δεν δημιουργεί προβληματισμούς καθώς έχουν μόνο ρόλο δημιουργού για εκάστοτε κρυπτονομίσματα και παρέχουν τα τεχνολογικά εργαλεία σε άλλους για εργαστούν με αυτά. Θα επανεξεταστεί αν εμπίπτουν στο πεδίο εφαρμογής της οδηγίας σε περίπτωση που λάβουν και άλλους ρόλους στο οικοσύστημα των κρυπτονομισμάτων.
- Οι **προσφέροντες κρυπτονομίσματα** δεν περιλαμβάνονται στον σκοπό της οδηγίας, γεγονός που επίσης δημιουργεί κενό δικαίου και αυξάνει τον κίνδυνο τα ICO να πληθαίνουν και κατά το τρίτο στάδιο (integrate) νομιμοποίησης εσόδων

[233] Το αντίθετο ισχύει στις ΗΠΑ όπου ο FinCEN's Final Rule δεν κάνει διάκριση σε ανταλλακτήρια fiat-crypto και crypto-crypto.

[234] Ο όρος Social Engineering χρησιμοποιείται για όλες τις κακόβουλες δραστηριότητες που επιτυγχάνονται μέσω ανθρώπινων αλληλεπιδράσεων. Χρησιμοποιεί την ψυχολογική χειραγώγηση για να εξαπατήσει τους χρήστες ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, el.wikipedia. *Κοινωνική μηχανική.* Ανακτήθηκε από: https://bit.ly/3izbcDJ (Πρόσβαση 07/06/2021).

από παράνομες δραστηριότητες, να χρησιμοποιούνται όλο και από περισσότερους κυβερνοεγκληματίες.

- Τέλος, προβληματισμός προκύπτει εάν τα **BATM** υπάγονται στην οδηγία καθώς δεν υπάρχει ρητή πρόβλεψη για αυτά. Αποτελεί εντούτοις αναμφισβήτητο γεγονός ότι τα τελευταία χρόνια, λόγω των ελαστικών ρυθμίσεων που εφαρμόζουν προς τους πελάτες τους, τα BATM πληθαίνουν και χρησιμοποιούνται όλο και περισσότερο στο πεδίο ξεπλύματος «βρώμικου» χρήματος.

➢ Στον σκοπό της οδηγίας δεν υπάγονται οι πάροχοι ανώνυμων υπηρεσιών «mixer», οι οποίοι είναι οι κατεξοχήν ενδιάμεσοι κατά το δεύτερο στάδιο (layering) νομιμοποίησης εσόδων από παράνομες δραστηριότητες και έχουν τη δυνατότητα να αποσυνδέουν το τελικό κρυπτονόμισμα από την αρχική πηγή προέλευσής του υπηρετώντας το κυβερνοέγκλημα.

➢ Αξιοσημείωτο είναι ότι στην AML5 γίνεται ιδιαίτερη αναφορά στην «ανωνυμία». Σύμφωνα με τη σκέψη 9: «*Η ανωνυμία των εικονικών νομισμάτων καθιστά δυνατή τη δυνητική αθέμιτη χρήση τους για εγκληματικούς σκοπούς*». Γίνεται λοιπόν αντιληπτό, ότι η ανωνυμία των χρηστών προβληματίζει την ΕΕ, καθώς την θεωρεί το έναυσμα για εγκληματικές ενέργειες.
Στην ίδια σκέψη αναφέρεται ότι: «*Η συμπερίληψη παρόχων που ασχολούνται με υπηρεσίες ανταλλαγής μεταξύ εικονικών νομισμάτων και παραστατικών νομισμάτων και παρόχων υπηρεσιών θεματοφυλακής πορτοφολιών* ***δεν θα αντιμετωπίσει εξολοκλήρου το ζήτημα της ανωνυμίας*** *που συνδέεται με συναλλαγές σε εικονικά νομίσματα, από τη στιγμή που μεγάλο μέρος του περιβάλλοντος εικονικών νομισμάτων θα παραμείνει* ***ανώνυμο διότι οι χρήστες μπορούν επίσης να συναλλάσσονται χωρίς τους εν λόγω παρόχους***». Δηλαδή, παρατηρείται ότι όσοι χρησιμοποιούν ανταλλακτήρια VCEPs και CWPs θα πρέπει να παρέχουν στοιχεία της ταυτότητάς τους, οπότε καταρρίπτεται άμεσα ένα από τα κύρια πλεονεκτήματα που προέρχονται απευθείας από τον πυρήνα δημιουργίας των κρυπτονομισμάτων, το Blockchain. Η ΕΕ παρέλειψε ηθελημένα να επεκτείνει το σκοπό της AML5 και σε άλλες οντότητες. Για παράδειγμα, δεν ρύθμισε και τις κατηγορίες παρόχων πορτοφολιού, λογισμικού και υλισμικού, διότι εάν επέβαλλε και σε αυτούς να κρατούν αναγνωριστικά στοιχεία των πελατών τους, το Blockchain θα επωνυμοποιείτο πλήρως.

Αποτέλεσμα, η ρύθμιση θα έφθανε στα όρια της υπερβολής, τη στιγμή που καθημερινά πραγματοποιείται ανώνυμα τεράστιος όγκος πληρωμών με μετρητά.

Προκειμένου τα κρυπτονομίσματα να φτάσουν στο σημείο μαζικής υιοθέτησης από τους πολίτες και να μην διαταράσσουν τον χρηματοπιστωτικό τομέα, πρέπει να αποπνέουν εμπιστοσύνη. Το ιστορικό παραβάσεων και σκανδάλων που τα συνοδεύει μπορεί να καταπολεμηθεί μόνο με την υπαγωγή τους σε ρυθμιστικούς κανόνες, ώστε να μπορέσουν να αποκτήσουν κάποιο ποσοστό αξιοπιστίας και ο κάθε νέος πελάτης που θα εισέρχεται στα ανταλλακτήρια να γνωρίζει ότι συναλλάσσεται με έμπιστους χρήστες. Η πολιτική AML/KYC, η οποία εντάχθηκε νομοθετικά στην οδηγία AML5, αποδείχτηκε εν τέλει χρήσιμη και σε άλλους τομείς του κυβερνοεγκλήματος, όπως σε περιπτώσεις hacking, phishing και απατών, διότι οι κακόβουλοι χρήστες αποτρέπονται και αποφεύγουν να εισέλθουν στο σύστημα του ανταλλακτηρίου και να εφαρμόσουν τις μεθόδους τους. Εντούτοις, υπάρχει πληθώρα αρρύθμιστων περιπτώσεων. Το πόσο επιτακτική καθίσταται η ανάγκη για πρόβλεψη αυτών, θα κριθεί από το κατά πόσο τα κενά δικαίου θα αποτελέσουν αντικείμενο εκμετάλλευσης από όλο και περισσότερους κυβερνοεγκληματίες για να επεκτείνουν και να καλύψουν τη δράση τους. Αν συμβεί κάτι τέτοιο, τότε η σκέψη 9 της AML5: «*Για* ***την καταπολέμηση των κινδύνων που σχετίζονται με την ανωνυμία****, οι εθνικές Μονάδες Χρηματοοικονομικών Πληροφοριών*[235] *(ΜΧΠ) θα πρέπει να* ***μπορούν να αποκτούν πληροφορίες*** *που θα τους δίνουν τη δυνατότητα* ***να συσχετίζουν τις διευθύνσεις του εικονικού νομίσματος με την ταυτότητα του ιδιοκτήτη του****»*, θα πρέπει να διευρυνθεί. Σε κάθε περίπτωση, η οδηγία AML5 αποτελεί μία πολύ σημαντική αφετηρία για τη ρύθμιση των κρυπτονομισμάτων, τα οποία κάθε μέρα λαμβάνουν όλο και μεγαλύτερη αναγνώριση και αποδοχή.

5.3. Το υπάρχον νομικό πλαίσιο

[235] Hellenic.F.I.U. Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες. Ανακτήθηκε από: http://www.hellenic-fiu.gr/index.php?lang=el (Πρόσβαση 27/05/2021).
«Το δίκτυο FIU.net είναι ένα αποκεντρωμένο και εξελιγμένο δίκτυο υπολογιστών που υποστηρίζει τις εθνικές μονάδες χρηματοοικονομικών πληροφοριών στην Ευρωπαϊκή Ένωση για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας»:
EUROPOL. *FINANCIAL INTELLIGENCE UNITS – FIU.NET*. Available at: https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net (Accessed 03/06/2021).

Για την πληρότητα του νομικού πλαισίου που καλύπτει την χρήση των κρυπτονομισμάτων στον κυβερνοχώρο, αν δεν αποτελεί αντικείμενο της παρούσας εργασίας, εντούτοις κρίνεται αναγκαίο η απλή αναφορά των διατάξεων, όπου υπάγονται οι περιπτώσεις στις οποίες το BTC αποτελεί το δέλεαρ για τη διάπραξη εγκλημάτων στον κυβερνοχώρο. Οι κυβερνοεγκληματίες, όταν αντιμετωπίζουν το BTC ως στόχο τον οποίο θέλουν να κατακτήσουν, χρησιμοποιούν κυρίως τεχνικές που προϋπήρχαν της εμφάνισης του Bitcoin και ο Έλληνας νομοθέτη τις είχε ήδη αντιμετωπιστεί νομοθετικά[236].

Στην Ελλάδα, τα κρυπτονομίσματα εντάσσονται στην έννοια της περιουσίας καθώς κατά την επικρατούσα θεωρία: «περιουσία είναι το σύνολο των αγαθών του προσώπου που έχουν οικονομική – χρηματική αξία και μπορεί να διαπιστωθεί λογιστικά, ανεξάρτητα αν αυτά αναγνωρίζονται και επιδοκιμάζονται από την έννομη τάξη[237]». Το cryptophishing και η απάτη Ponzi αντιμετωπίζονται με τη βασική διάταξη της απάτης του άρθρου 386 ΠΚ, καθώς οι δράστες έχουν γνώση και θέληση για την παράνομη δραστηριότητά τους και «η βλάβη» παρότι είναι αποτέλεσμα διαδικασίας επεξεργασίας ψηφιακών δεδομένων, εντούτοις αποτελεί παραπλάνηση φυσικού προσώπου με χρήση ηλεκτρονικού υπολογιστή, ως αναγκαίου μέσου για την τέλεση του εγκλήματος.

Η Σύμβαση της Βουδαπέστης του 2001 και η μεταφορά στο ελληνικό δίκαιο της Οδηγίας[238] 2013/40/ΕΕ, η οποία επικυρώθηκε στην Ελλάδα με το Ν.4411/2016[239] υπήρξε καταλυτικής σημασίας για την επικαιροποίηση του νομικού πλαισίου για την αντιμετώπιση των εγκλημάτων που διεξάγονται στον κυβερνοχώρο. Μεταξύ των άλλων υπάρχει η πρόβλεψη για εγκλήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικού υπολογιστή, η οποία

[236] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 11-12, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 503, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 25, *Δαλακούρας, Θ.*., ό.π., σελ. 7-12, Γανιάρης, Ν., Η αξιόποινη εξόρυξη κρυπτονομισμάτων Bitcoin. *The Art of Crime* [online]. ΝΟΕΜΒΡΙΟΣ 2018. Ανακτήθηκε από: https://bit.ly/3vgjumC (Πρόσβαση 02/06/2021).

[237] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 11.

[238] Οδηγία 2013/40/ΕΕ, ΕΚ και ΣΕΕ (12/08/2013). *Για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013L0040&from=NL (Πρόσβαση 08/06/2021).

[239] «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης - πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις».

αποβλέπει στην ασφάλεια των δεδομένων που διακινούνται στο διαδίκτυο και στην ποινικοποίηση της σοβαρής παρεμπόδισης της λειτουργίας συστήματος υπολογιστή.

Ρητή πρόβλεψη της ποινικοποίησης του hacking υπάρχει στο άρθρο 370Β. Σκοπός της «πρόσβασης» στην προκειμένη περίπτωση είναι πρωτίστως η επιβεβαίωση ύπαρξης ικανότητας εισβολής σε ένα υπολογιστικό σύστημα και η ικανοποίηση του δράστη από την παράκαμψη των συστημάτων ασφαλείας και όχι η αποκόμιση κέρδους, η δολιοφθορά και η καταστροφή. Η ποινικοποίηση της πρόσβασης, η οποία γίνεται ανεξάρτητα από την επέλευση περιουσιακού οφέλους ή ζημίας, αντανακλά την ανάγκη αντιμετώπισης των κινδύνων από τις εξελίξεις της πληροφορικής. Έχει υποστηριχθεί εντούτοις και η άποψη ότι εκτός του απορρήτου των επικοινωνιών, η διάταξη προστατεύει και το έννομο αγαθό της περιουσίας και της ασφάλειας ηλεκτρονικών συστημάτων.

Οι επιθέσεις DDoS έχουν ως αποτέλεσμα την παρεμπόδιση λειτουργίας του συστήματος με προσωρινό ή μόνιμο τρόπο. Υπάγονται λοιπόν στην έννοια ης «σοβαρής επίθεσης» που απαιτείται για την πλήρωση της αντικειμενικής υπόστασης της διάταξης 292Β ΠΚ. Εν προκειμένω, προστατευόμενο έννομο αγαθό είναι η εξασφάλιση δυνατότητας των χειριστών και χρηστών ηλεκτρονικών υπολογιστών να λειτουργούν προβλέψιμα και ανεμπόδιστα. Η ίδια αξίωση επιβαλλόταν από την Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών, υπό το φως της οποίας και ενσωματώθηκε το άρθρο 292Β στον ΠΚ.

Η περίπτωση του cryptojacking αντιμετωπίζεται με το άρθρο 370Β ΠΚ, καθώς βαθμηδόν η υπερπήδηση του συστήματος ασφαλείας, η επέμβαση στο μητρώο δεδομένων του υπολογιστή, η ενεργοποίηση της θύρας σύνδεσης με το διαδίκτυο, η εκκίνηση του προγράμματος cryptomining, η εξόρυξη κρυπτονομισμάτων και εν συνεχεία η μετάδοση των κρυπτονομισμάτων-στοιχείων του υπολογιστή στη βάση δεδομένων του κατηγορουμένου στοιχειοθετούν την παράνομη πρόσβαση σε σύστημα πληροφοριών. Το cryptojacking αντιμετωπίζεται επιπλέον με τη διάταξη 292Β ΠΚ, καθώς πράγματι λόγω της διαδικασίας εξόρυξης που τρέχει στο παρασκήνιο, παρακωλύεται η φυσιολογική λειτουργία του υπολογιστή.

Τα malware και οι κατηγορίες που το απαρτίζουν υπάγονται στα άρθρα 292Β, 370Β, 370Γ και 386Α ΠΚ, ανάλογα με τη λειτουργία την οποία επιτελούν και τις επιπτώσεις που προκαλούν στον ηλεκτρονικό υπολογιστή. Ο επηρεασμός των στοιχείων υπολογιστή τρίτου με πρόθεση υποκλοπής BTC εμπίπτει στο πεδίο εφαρμογής της διάταξης 386Α ΠΚ, η ειδική υπόσταση της οποίας πληρείται όταν ο δράστης με τις ενέργειές του προκαλεί αποτέλεσμα

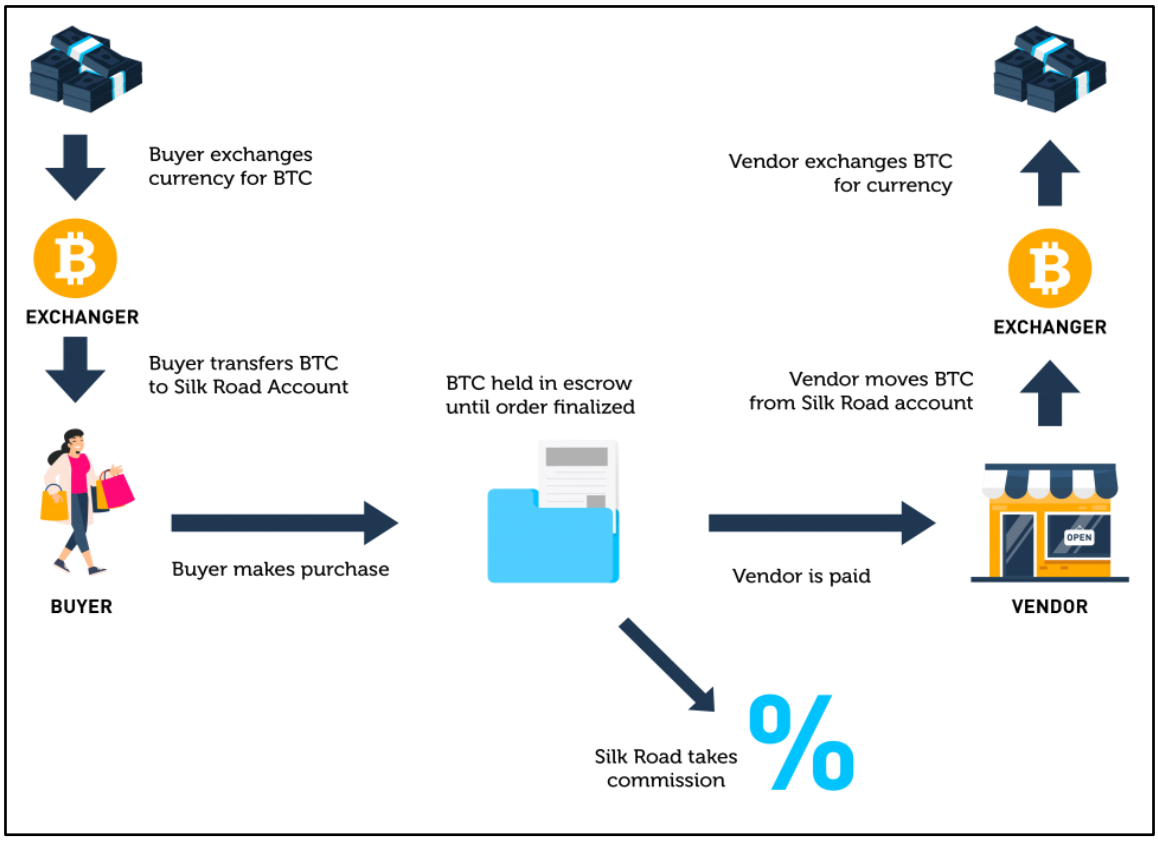
διαφορετικό από εκείνο που θα προέκυπτε από την διαδικασία της επεξεργασίας των στοιχείων, βλάπτοντας ξένη περιουσία προς όφελος αυτού ή τρίτου. Έτσι διώκονται, «οι αντικαταστάτες διεύθυνσης» και σύμφωνα με το 386Α για απάτη με υπολογιστή, τα botnets σύμφωνα με το 292Β παρ.2 περιπτ. α και τα worms σύμφωνα με το 370Β καθώς αποκτούν πρόσβαση σε σύστημα πληροφοριών.

ΚΕΦΑΛΑΙΟ 6ο
ΣΗΜΑΝΤΙΚΕΣ ΝΟΜΟΛΟΓΙΑΚΕΣ ΥΠΟΘΕΣΕΙΣ

6.1. Η Υπόθεση του Silk Road

Η υπόθεση «United States of America v. Ross William Ulbricht[240]» είναι μία από τις πιο χαρακτηριστικές περιπτώσεις χρήσης του BTC ως μέσον για πληρωμή αγαθών και υπηρεσιών στο dark web. Τον Ιανουάριο του 2011, ο Ross William Ulbricht (γνωστός με το ψευδώνυμο Dead Pirate Roberts, στο εξής DPR) δημιούργησε στο dark web την ιστοσελίδα Silk Road, με στόχο να δημιουργήσει μια ψηφιακή online παγκόσμια αγορά, για την διευκόλυνση της παράνομης δραστηριότητας. Η Silk Road αποτέλεσε την πιο διάσημη ανώνυμη αγορά του dark web και ήταν η πρώτη στο είδος της που υποστήριζε συναλλαγές αποκλειστικά με BTC. Στην αρχή, η ιστοσελίδα εξυπηρετούσε την διαδικτυακή πώληση ναρκωτικών, πληροφοριών πιστωτικών καρτών και πλαστών διαβατηρίων. Στη συνέχεια, επέτρεψε την ανωνυμοποίηση των χρηστών, εφόσον αυτοί πλήρωναν σε BTC. Αργότερα δε, σε μια προσπάθεια για να ανωνυμοποιήσει περεταίρω τις συναλλαγές, η ιστοσελίδα παρείχε υπηρεσίες ξεπλύματος χρήματος. Οι πωλητές και αγοραστές επικοινωνούσαν μέσω ενός ηλεκτρονικού συστήματος ηλεκτρονικής αλληλογραφίας που διέθετε η Silk Road. Οι πωλητές καταχωρούσαν τα προϊόντα τους και οι αγοραστές, αφού επέλεγαν αυτά που επιθυμούσαν, κατέβαλλαν το αντίτιμο σε BTC και στη συνέχεια λάμβαναν την παραγγελία τους μέσω ταχυδρομείου.

[240] United States Court of Appeals For the Second Circuit, 2008. *UNITED STATES of America, Appellee v. ROSS WILLIAM ULBRICHT, a/k/a DREAD PIRATE ROBERTS, a/k/a SILK ROAD, a/k/a SEALED DEFENDANT 1, a/k/a DPR.* No. 15-1815, Decided: May 31, 2017. Available at: https://cases.justia.com/federal/appellate-courts/ca2/15-1815/15-1815-2017-05-31.pdf?ts=1496241010 (Accessed 05/06/2021).



Εικόνα 26: Σύστημα πληρωμής μέσω BTC στο Silk Road[241]

Ο κάθε χρήστης είχε ένα προφίλ στην ιστοσελίδα Silk Road προκειμένου να μπορεί να διεξάγει συναλλαγές. Ο λογαριασμός αυτός συνδεόταν με τουλάχιστον μία διεύθυνση Bitcoin, η οποία με τη σειρά της αποθηκευόταν σε έναν server, που βρισκόταν υπό τον έλεγχο του Silk Road.

Υπήρχε πρόβλεψη ακόμα και για την προστασία των πωλητών και των αγοραστών από τις ακραίες διακυμάνσεις της τιμής του BTC. Έτσι λοιπόν, το αντίτιμο που έπρεπε να πληρώσει ο αγοραστής διατηρούνταν ως μεσεγγύηση, μέχρι αυτός να παραλάβει το προϊόν. Ακόμη ο πωλητής είχε την δυνατότητα να επιλέξει την ισοτιμία του BTC να είναι σε δολάρια ΗΠΑ, μέχρις ότου να παραδοθεί το προϊόν. Η χρήση της διαδικασίας της μεσεγγύησης είχε ως αποτέλεσμα η ιστοσελίδα να επιφορτιστεί να καλύψει τη διαφορά και να πληρώσει τον πωλητή, αν η ισοτιμία προς το δολάριο έπεφτε. Αν όμως η ισοτιμία ανέβαινε, η ιστοσελίδα κέρδιζε το προκύπτον πλεόνασμα.

[241] Bitorb. *SILK ROAD DAY- WHAT IS THE SILK ROAD MARKETPLACE?*. Available at: https://www.bitorb.com/campus/silk-road-day-what-is-the-silk-road-marketplace/ (Accessed 27/01/2021).

Επειδή οι συναλλαγές με BTC αποθηκεύονται στο Blockchain που είναι προσβάσιμο και από κυβερνητικές και ελεγκτικές αρχές, η ιστοσελίδα δημιούργησε τα λεγόμενα dark wallets, τα οποία κρυπτογραφούσαν και μεταμφίεζαν όλες τις συναλλαγές που γινόντουσαν με BTC, εξασφαλίζοντας στους χρήστες της ένα επιπλέον επίπεδο ιδιωτικότητας.

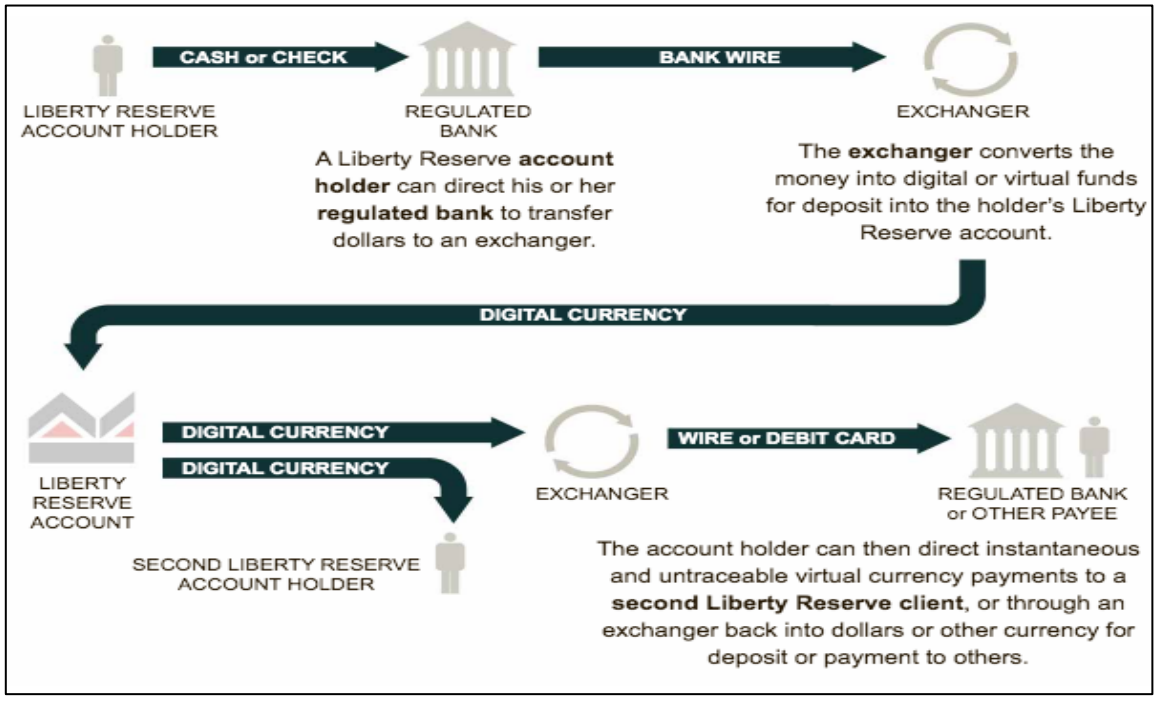
Οι αρχές των ΗΠΑ ενημερώθηκαν από το 2011 για την ύπαρξη αυτής της ιστοσελίδας. Προκειμένου όμως να εξακριβώσουν την ταυτότητα των δραστών, διεξήγαγαν μυστική έρευνα, η οποία επιβεβαίωσε ότι εν τέλει η ιστοσελίδα λειτουργούσε για την διευκόλυνση εγκληματικής δραστηριότητας και οδηγήθηκαν στη δίωξη των υπευθύνων. Η έρευνα ολοκληρώθηκε το 2013, οπότε ο Ulbricht συνελλήφθη. Στην δίκη που ακολούθησε, παραδέχτηκε ότι δημιούργησε την ιστοσελίδα, αλλά αρνήθηκε ότι είχε τον διαχειριστικό έλεγχο του ψευδωνύμου DPR. Ο Ulbricht καταδικάστηκε σε ισόβια φυλάκιση.

Η Silk Road άνοιξε το δρόμο για την εμφάνιση πολλών παρόμοιων αγορών που προσομοιάζουν αρκετά στον τρόπο λειτουργίας και αποδοχής κρυπτονομισμάτων, ως μέσον πληρωμής. Στην πραγματικότητα όμως η σύλληψη του DPR, βοήθησε ώστε να αποσυνδεθεί η συσχέτιση μεταξύ BTC και εγκλήματος. Το ίδιο το Federal Bureau of Investigation (στο εξής FBI) στην δίκη που διεξήχθη για την υπόθεση του Silk Road δήλωσε ότι: «τα BTC δεν είναι παράνομα εκ της φύσεώς τους και είναι γνωστά και για νόμιμες χρήσεις». Η δήλωση αυτή είναι είναι πάρα πολύ σημαντική για την νομιμότητα των BTC. Επιπλέον, μπορεί μεν η δημιουργία της Silk Road και η χρήση του BTC να αφύπνησε τις αρχές για τους κινδύνους που μπορεί να επιφέρει η χρήση ενός αποκεντρωμένου συστήματος πληρωμών, εντούτοις όμως επέδειξε και κάτι άλλο ακόμα πιο σημαντικό. Απέδειξε στην πράξη ότι τα BTC θα μπορούσαν να λειτουργήσουν στον πραγματικό κόσμο, καθώς το αποκεντρωμένο αυτό νόμισμα ήταν ικανό και να έχει διάρκεια και να μεταφέρει αξία μεταξύ των χρηστών μιας παγκόσμια αγοράς[242].

[242] Βλ. *Μεταξάκης, Ε.*, ό.π., σελ.228-233, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 24, *Reddy, E., Minnaar, A.*,, ό.π., σελ.75, Frankenfield, J., 2021. *Silk Road (Website)*.. Available at:https://www.investopedia.com/terms/s/silk-road.asp (Accessed 27/05/2021), GDPO. *Silk Road and Bitcoin.* Available at:https://www.swansea.ac.uk/media/Silk-Road-and-Bitcoin.pdf (Accessed 23/05/2021), Adler, D., 2018. Silk Road: The Dark Side of Cryptocurrency. *FORDHAM JOURNAL OF CORPORATE & FINANCIAL LAW* [online]. February 21, 2018. Available at: https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/ (Accessed 27/01/2021), *Dykyi, O., Dyntu, V.*, ό.π., σελ.79, *Oerlemans, J., J., van Deventer, O. et van Wegberg, R., ό.π.,* σελ. 42, Sykes, J., Vatanko, N., 2019. Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals. *Congressional Research Service* [online]. R45664, April 3, 2019. Available at: https://fas.org/sgp/crs/misc/R45664.pdf (Accessed 26/01/2021).

6.2. Η υπόθεση Liberty Reserve

Η υπόθεση «US v Liberty Reserve et al[243]» είναι η πιο σημαντική περίπτωση για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες με χρήση κρυπτονομισμάτων. Ο ένας εκ των συγκατηγορουμένων, ο Arthur Budovsky, καταδικάστηκε σε 20 χρόνια φυλάκιση για το γεγονός ότι διευκόλυνε το ξέπλυμα «βρώμικου-μαύρου» χρήματος μέσω του Liberty Reverse, ενός διαδικτυακού συστήματος πληρωμών με έδρα την Costa Rica. Η ονομασία Liberty Reserve είχε διττό περιεχόμενο, καθώς παρέπεμπε και στο εναλλακτικό δίκτυο πληρωμών και στο ψηφιακό νόμισμα (στο εξής LR) που παρεχόταν. Το Liberty Reserve χαρακτηρίστηκε ως μια «τράπεζα μαύρης αγοράς» που δεχόταν καταθέσεις μόνο στο δικό του νόμισμα και που αποτελούσε τον διαδικτυακό «παράδεισο» όλων όσων ήθελαν να νομιμοποιήσουν έσοδα από παράνομες δραστηριότητες.



Εικόνα 27: Τρόπος λειτουργίας του Liberty Reserve [244]

[243] United States Court for the Southern District of New York, 2015. *United States v. Budovsky*. Decided; September 23, 2015, Filed 13cr368 (DLC). Available at: https://bit.ly/2RgU7mR (Accessed 05/06/2021).

[244] The New York Times. *How Liberty Reserve's Virtual Currency Works.* Available at: [244] https://nyti.ms/3vK6arS (Accessed 23/05/2021).

Αρχικά, ο ενδιαφερόμενος άνοιγε ένα λογαριασμό στο Liberty Reserve. Στη συνέχεια, μετέφερε τα «βρώμικα» χρήματα από το λογαριασμό που διατηρούσε σε μια παραδοσιακή τράπεζα, προς ανταλλακτήρια τα οποία λειτουργούσαν χωρίς άδεια, δεν υπόκειτο σε κανονιστικές ρυθμίσεις και ασκούσαν μηδαμινό έλεγχο στους χρήστες τους και βρίσκονταν σε χώρες όπως η Μαλαισία, η Νιγηρία ή το Βιετνάμ. Τα ανταλλακτήρια αυτά λάμβαναν LR σε χονδρική τιμή απευθείας από το Liberty Reserve και ήταν επιφορτισμένα με τη μετατροπή των «βρώμικων »χρημάτων σε LR, καθιστώντας έτσι μη ανιχνεύσιμη την αρχική τους πηγή. Στη συνέχεια, τα LR αυτά κατατίθεντο στον λογαριασμό που διατηρούσε ο ενδιαφερόμενος στο Liberty Reserve. Δεν υπήρχε όριο στο ύψος της συναλλαγής παρά μόνο μια χρέωση 1% για κάθε μεταφορά, όλες δε οι συναλλαγές ήταν αμετάκλητες.

Επειδή οι καταθέσεις και οι αναλήψεις χρημάτων γίνονταν αποκλειστικά από τα ανταλλακτήρια, το Liberty Reserve δεν μπορούσε να αντλήσει δεδομένα για τους χρήστες όπως, να καταγράψει πώς ή από πού είχαν στείλει τα χρήματα. Επιπλέον, αν και οι χρήστες παρείχαν ονοματεπώνυμο, email και ημερομηνία γέννησης, δεν γινόταν καμία επαλήθευση ταυτότητας σύμφωνα με τους κανόνες AML/KYC, από πλευράς ανταλλακτηρίου. Με τον τρόπο αυτό δινόταν η δυνατότητα στους χρήστες να παρουσιάσουν ακόμη και ψευδή στοιχεία και ταυτότητες.

Το LR συνδέθηκε με το δολάριο και το ευρώ καθιστώντας έτσι την τιμή του σχετικά σταθερή και σε πολύ σύντομο διάστημα έγινε παγκοσμίως μια από τις κύριες υπηρεσίες μεταφοράς χρημάτων από κυβερνοεγκληματίες, οι οποίοι αποσκοπούσαν σε συγκέντρωση, διανομή, αποθήκευση και νομιμοποίηση εσόδων παράνομης δραστηριότητας, συμπεριλαμβανομένων και των εσόδων από απάτη επενδύσεων, απάτη με πιστωτικές κάρτες, κλοπή ταυτότητας και ηλεκτρονική εισβολή. Εξίσου σημαντικό είναι επίσης ότι το LR λειτούργησε και ως ψηφιακό νόμισμα, δεκτό ως μέσο πληρωμής από κυβερνοεγκληματίες για την παροχή των δραστηριοτήτων τους. Από την αρχή της λειτουργίας του Liberty Reverse το 2006, υπολογίζεται ότι επεξεργάστηκε περίπου 55 εκατομμύρια συναλλαγές αξίας 6 δισεκατομμυρίων δολαρίων, ενώ ο ίδιος ο Budovski παραδέχτηκε ότι είχαν ξεπλυθεί με τη συγκατάθεσή του περισσότερα από 250 εκατομμύρια δολάρια που προέρχονταν από εγκληματικές δραστηριότητες[245].

[245] THE US DEPARTMENT of JUSTICE. *Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business.* Available at: https://www.justice.gov/opa/pr/founder-liberty-

6.3. Υπόθεση BitInstant

Πολύ σημαντική υπόθεση είναι επίσης η «United States of America vs Robert M. Faiella and Charlie Shrem[246]». Ο Charlie Shrem ήταν διευθύνων σύμβουλος, υπεύθυνος ελέγχου συμμόρφωσης και συνιδρυτής της εταιρείας BitInstant, η οποία ήταν ένα από τα πρώτα ανταλλακτήρια που δημιουργήθηκαν και παρείχαν την δυνατότητα μετατροπής παραστατικού χρήματος σε BTC. Το 2014, ο Shrem άρχισε να δέχεται παραγγελίες από τον Robert Faiella, προκειμένου να μετατρέψει παραστατικό χρήμα σε BTC. Ο Faiella έλεγχε ένα παράνομο ανταλλακτήριο Bitcoin, μέσω του οποίου πωλούσε τα BTC σε πελάτες που επιθυμούσαν να κάνουν χρήση των υπηρεσιών της ιστοσελίδας Silk Road. Ο Faiella λοιπόν λάμβανε τις παραγγελίες για BTC και στη συνέχεια τις προωθούσε στον Shrem, για να κάνει τη μετατροπή σε BTC, τα οποία εν συνεχεία τα έστελνε σε λογαριασμό που έλεγχε ο Faiella σε ανταλλακτήριο στην Ιαπωνία. Υπολογίζεται ότι το ποσό που ανταλλάχτηκε με αυτόν τον τρόπο έφτανε το ένα εκατομμύριο δολάρια. Ο Shrem και ο Faiella παραπέμφθηκαν σε δίκη με τις κατηγορίες της λειτουργίας επιχείρησης μεταφοράς χρημάτων χωρίς άδεια, του ξεπλύματος «βρώμικου» χρήματος και της σκόπιμης παράλειψης αναφοράς ύποπτων συναλλαγών στις αρμόδιες αρχές. Η απόφαση αυτή είναι σημαντική, διότι επεσήμανε τη σπουδαιότητα που έχει η ρητή υπαγωγή των οντοτήτων αυτών στην περίπτωση του νόμου «περί νομιμοποίησης εσόδων από παράνομες δραστηριότητες»[247].

6.4. Η υπόθεση Shavers

Τα δικαστήρια των ΗΠΑ απασχόλησε η υπόθεση «The Security and Exchange Commission v. Shavers[248]». Ήταν η πρώτη υπόθεση που αφορούσε την περίπτωση τέλεσης απάτης μέσω διενέργειας συναλλαγών με BTC. Ο Trendon Shaver χρησιμοποίησε το σχήμα Ponzi μέσω της επιχείρησης «Bitcoin Saving and Trust (BCS&T)» και κατάφερε να

---

reserve-pleads-guilty-laundering-more-250-million-through-his-digital (Accessed 07/06/2021), KYC-CHAIN. *Liberty Reserve – The Digital Currency That Laundered Millions.* Available at: https://kyc-chain.com/liberty-reserve-the-digital-currency-that-laundered-millions/ (Accessed 25/04/2021), Surowiecki J., 2013. *Why Did Criminals Trust Liberty Reserve?* Available at: https://www.newyorker.com/news/news-desk/why-did-criminals-trust-liberty-reserve (Accessed 10/02/2021), *Sykes, J., Vatanko, N.*, ό.π..

[246] United States District Court, 2014. *UNITED STATES of America v. Robert M. FAIELLA, a/k/a "BTCKing," and Charlie Shrem, Defendants.* No. 14–cr–243 (JSR). 2014-08-19. Available at: https://bit.ly/3iaPgyD (Accessed 05/06/2021).

[247] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 6, *Μεταξάκης, Ε.*, ό.π., σελ.216-219.

[248] CASE NO. 4:13-CV-416, Βλ. *United States District Court EASTERN DISTRICT OF TEXAS SHERMAN DIVISION*, ό.π.

δελεάσει επενδυτές ώστε να επενδύσουν BTC. Εγγυόταν υψηλά κέρδη της τάξεως 7%, υποστηρίζοντας ψευδώς ότι δημιουργούνταν από την πώληση BTC σε αγοραστές που δεν ήθελαν να αποκαλύψουν την ταυτότητά τους, αλλά που ενδιαφερόντουσαν να αγοράσουν μεγάλα ποσά BTC. Ισχυριζόταν ότι λόγω αυτού ο επενδυτικός κίνδυνος ήταν μειωμένος και ότι τα κεφάλαια σπάνια μπορούν να μείνουν ακάλυπτα πάνω από μερικές ώρες, καθώς ο όγκος εργασιών ήταν μεγάλος. Αποτέλεσμα ήταν ότι κατάφερε να πάρει περισσότερα από 700000 BTC, τα οποία στην πραγματικότητα δεν επενδύθηκαν πουθενά, αλλά χρησιμοποιήθηκαν είτε για ιδία χρήση από τον Shaver, είτε ως κέρδη για να πληρωθούν δήθεν κέρδη στους ίδιους τους επενδυτές ή εκκρεμείς τόκοι σε παρόμοια επένδυση. Κάποιοι από τους επενδυτές όμως απευθύνθηκαν στην Αμερικανική Επιτροπή Ασφάλειας Συναλλάγματος και αυτή κινήθηκε δικαστικά εναντίον του Shavers. Το Δικαστήριο έκρινε ένοχο τόσο τον Shavers όσο και την εταιρεία του[249].

6.5. Η υπόθεση Mt.Gox

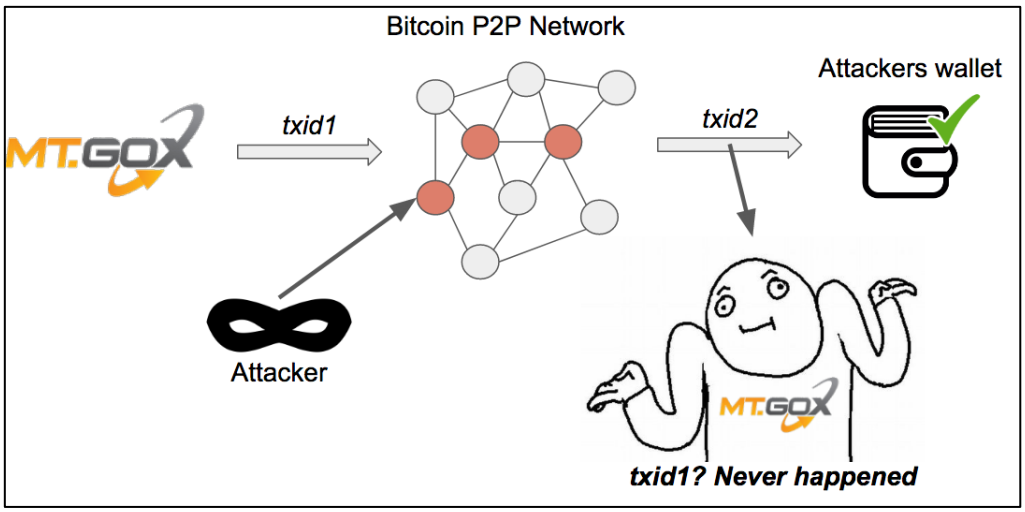
Το Mt.Gox[250] αποτέλεσε το μεγαλύτερο ανταλλακτήριο BTC στον κόσμο και λειτούργησε από το 2010 έως το 2014 στην Ιαπωνία. Δημιουργήθηκε από τον Jed McCaleb ως ανταλλακτήριο για να διευκολύνει τους παίχτες του παιχνιδιού «Magic: The Gathering» να ανταλλάσσουν διαδικτυακά κάρτες. Σχεδόν αμέσως όμως μετέβαλε τη λειτουργία του και έγινε ανταλλακτήριο BTC. Το 2011, η ιστοσελίδα πουλήθηκε στον Mark Karpelès. Το Mt.Gox έγινε γρήγορα στόχος των hackers, οι οποίοι κατά καιρούς προκαλούσαν προβλήματα στο σύστημα ασφαλείας του και χρησιμοποιούσαν κλεμμένα διαπιστευτήρια για να μεταφέρουν BTC. Το Mt.Gox αντιμετώπιζε για αρκετούς μήνες προβλήματα ασφαλείας και τελικά παραδέχτηκε ότι είχε χάσει το μεγαλύτερο μέρος των BTC των πελατών του, καθώς και ένα μεγάλο μέρος των BTC που κατείχε το ίδιο. Το 2014, η εταιρεία υπέβαλε αίτηση για πτώχευση καθώς οι μακρόχρονες επιθέσεις hacking είχαν ως αποτέλεσμα να κλαπούν 850000 BTC ή άλλως 480 εκατομμύρια δολάρια.

---

[249] Βλ. *Καζαζάκης, Θ.*, ό.π., σελ. 5-6, *Μεταξάκης, Ε.*, ό.π., σελ.212-215.
SAKS-MCLEOD, A., 2014. Trenton Shavers' Bitcoin Ponzi scheme lands him with $40 million fine from federal judge in Texas. *LeapRate.com* [online]. September 19, 2014. Available at: https://www.leaprate.com/news/trenton-shavers-bitcoin-ponzi-scheme-lands-him-with-40-million-fine-from-federal-judge-in-texas/ (Accessed 26/05/2021).

[250] Το όνομα Mt.Gox αποτελεί ακρωνύμιο της φράσης Magic: The Gathering Online Exchange.

Ο Karpelès κατηγόρησε μια ατέλεια του συστήματος Bitcoin για την απώλεια των BTC, η οποία ονομάζεται transaction malleability και δίνει τη δυνατότητα στον hacker να επηρεάσει την ταυτότητα μια συναλλαγής, ώστε να φαίνεται το ανταλλακτήριο να την βλέπει ως μη επιβεβαιωμένη, ενώ στην πραγματικότητα είναι. Έτσι το ανταλλακτήριο δημιουργεί εκ νέου μια συναλλαγή με αποτέλεσμα ο επιτιθέμενος να πληρώνεται εις διπλούν με το ίδιο ποσό.



Εικόνα 28: Transaction Malleability στο Mt.Gox[251]

Έχουν αναπτυχθεί πολλές θεωρίες σχετικά με το ποιος είναι ο υπεύθυνος και πού πήγαν τα κλεμμένα BTC. Είναι αδιαμφισβήτητο γεγονός πάντως ότι το Mt.Gox ήταν για πολλά χρόνια αφερέγγυο, καθώς επέτρεψε να λάβει χώρα μια αργή κλοπή, η οποία κατέστη δυνατή εξαιτίας των χαλαρών πρακτικών ασφαλείας που το ανταλλακτήριο ήταν ανίκανο ή απρόθυμο να διορθώσει. Κατά την περίοδο ακμής του, ήταν υπεύθυνο για το 70% των BTC που κυκλοφορούσαν. Το 2019, Ο Karpelès κρίθηκε ένοχος για παραποίηση δεδομένων, αλλά όχι για υπεξαίρεση όπως αρχικά είχε κατηγορηθεί.

Το Mt.Gox αποτελεί καθοριστικό σταθμό στην ιστορία του Bitcoin διότι πριν από την εμφάνισή του η ανταλλαγή παραστατικού χρήματος με BTC γινόταν εκτός αγοράς. Με την εμφάνιση όμως του ανταλλακτηρίου αυτού, οι χρήστες μπορούσαν αφενός να έχουν πρόσβαση στο ποσό, το οποίο άλλοι χρήστες ήταν διατεθειμένοι να πληρώσουν για το BTC και αφετέρου μπορούσαν να δουν τα ποσά που είχαν καταβληθεί στο παρελθόν. Με τον τρόπο αυτό τα BTC μπορούσαν να αποκτήσουν πραγματική τιμή και πραγματική αξία. Το

[251] Βλ. Laptev, D., 2017. Bitcoin: transactions, malleability, SegWit and scaling. *Medium* [online]. Aug. 24, 2017. Available at: https://bit.ly/2Towo4K (Accessed 06/06/2021).

Mt.Gox και τα όσα επακολούθησαν την πτώχευσής του, έβγαλαν το BTC από την «παιδική ηλικία» του. Το BTC είχε μπει πλέον στο σύστημα και είχε αποτελέσει το στόχαστρο των ίδιων ανθρώπων που πρώτα γοήτευε. Η αξία πλέον του εξαρτάται από τη χρησιμότητά του και η χρησιμότητα αυτή στηρίζεται στην ασφάλεια. Αν δεν υπάρχει ασφάλεια, τότε κανείς δεν μπορεί να εμπιστευθεί το σύστημα Bitcoin[252].

6.6. Υπόθεση Alexander Vinnik[253]

Η ελληνική δικαιοσύνη ήρθε αντιμέτωπη με το οικοσύστημα των κρυπτονομισμάτων στην υπόθεση του Alexander Vinnik, την έκδοση του οποίου ζήτησαν οι ΗΠΑ, η Γαλλία και η Ρωσία, έπειτα από τη σύλληψή του τον Ιούλιο του 2017 στη Θεσσαλονίκη.

Πραγματικά περιστατικά

Ο Vinnik, από 2012 μέχρι το 2017, ήταν υπεύθυνος και διαχειριστής ενός από τα μεγαλύτερα και πιο ευρέως χρησιμοποιούμενα ανταλλακτήρια κρυπτονομισμάτων με την ονομασία BTC-e, που λειτουργούσε χωρίς να έχει λάβει την απαιτούμενη άδεια και χωρίς να εφαρμόζει τις προβλεπόμενες μεθόδους του KYC για τον προσδιορισμό των πραγματικών ταυτοτήτων των πελατών του. Για να γίνει κάποιος χρήστης δημιουργούσε ένα λογαριασμό στην ιστοσελίδα του, χρησιμοποιώντας μόνον ένα όνομα χρήστη, έναν κωδικό πρόσβασης και μια διεύθυνση e-mail, χωρίς να χρειάζεται να παρέχει ακόμα και τις πιο βασικές αναγνωριστικές πληροφορίες, όπως όνομα, ημερομηνία γέννησης, διεύθυνση ή άλλα αναγνωριστικά, με αποτέλεσμα να ανοίγονται λογαριασμοί εύκολα και ανώνυμα.

Το BTC-e στηριζόταν στη χρήση εταιρειών «βιτρίνας» και σε συνεργαζόμενες διαδικτυακές επιχειρήσεις, που επίσης δεν είχαν επίσημη άδεια και δεν ακολουθούσαν πολιτικές AML/KYC. Οι εταιρείες «βιτρίνες» εξυπηρετούσαν μια παγκόσμια ηλεκτρονική βάση πελατών και μετέφεραν παραστατικό χρήμα παράνομα. Έτσι, μια εταιρεία-βιτρίνα του BTC-e είχε βάση στις Σεϋχέλες, συνδεόταν με ένα ρωσικό αριθμό τηλεφώνου, οι

[252] Βλ. *Reddy, E., Minnaar, A.,*, ό.π., σελ. 78. Coindesk. *Launched in 2010 Mt. Gox was the world's largest bitcoin exchange until its demise in 2014.* Available at: https://www.coindesk.com/company/mt-gox (Accessed 23/05/2021), Coindesk. *What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability.* Available at: https://www.coindesk.com/bitcoin-bug-guide-transaction-malleability (Accessed 23/05/2021), DeMartino, I., 2017. *Bitcoin: Ο Απόλυτος Οδηγός.* μετάφραση Κ. Μπουλούκου, Αθήνα: Φανταστικός Κόσμος. (το πρωτότυπο έργο εκδόθηκε 2016).

[253] ΝΟΜΟΣ: ΣΤΕ 110/2020, ΣΤΕ 41/2021, ΑΠ 2980/2017.

διευθύνσεις διαδικτύου της ήταν εγγεγραμμένες σε εταιρείες-βιτρίνες σε διάφορες χώρες όπως Σιγκαπούρη, Βρετανικοί Παρθένοι νήσοι, Γαλλία, Νέα Ζηλανδία, ενώ η ιστοσελίδα του BTC-e διατηρούσε στις ΗΠΑ τους διακομιστές του, μέσω των οποίων ο Vinnik και οι συναυτουργοί του πραγματοποιούσαν τις δραστηριότητές τους. Υπεύθυνος διαχειριστής, κύριος δικαιούχος και διαχειριστής των οικονομικών λογαριασμών της BTC-e και των εταιρειών «βιτρίνας» ήταν πάντα ο Vinnik. Ακόμα, το BTC-e χρησιμοποιούσε στις συναλλαγές του και εταιρείες τρίτων ή ακόμα εταιρείες που διευκόλυναν το ξέπλυμα χρημάτων για τη μεταφορά χρημάτων διεθνώς. Σε λογαριασμούς που σχετίζονται με τον Vinnik, έγιναν μεγάλες πληρωμές από συγκεκριμένο λογαριασμό, ο οποίος είχε έσοδα προερχόμενα από πολύ γνωστά hacking και από κλοπές σε ανταλλακτήρια κρυπτονομισμάτων.

Ο κάθε χρήστης μπορούσε να χρηματοδοτήσει ένα λογαριασμό της BTC-e με πολλούς διαφορετικούς τρόπους. Ένας τρόπος ήταν η χρηματοδότηση του λογαριασμού με παραστατικό χρήμα, το οποίο ο χρήστης μετέφερε απευθείας σε ένα τραπεζικό λογαριασμό που τηρείτο από μια από τις εταιρείες-«βιτρίνες» και το οποίο στη συνέχεια μπορούσε να μετατραπεί σε κρυπτονόμισμα. Ένας άλλος τρόπος περιελάμβανε την χρηματοδότηση του BTC-e με τη μορφή καταθέσεων απευθείας σε κρυπτονομίσματα, από ένα χρήστη που είχε ψηφιακό συνάλλαγμα. Επίσης, οι χρήστες του BTC-e μπορούσαν να αγοράσουν ένα «κώδικα», ο οποίος μπορούσε να σταλεί και να ανταλλαχθεί ανάμεσα σε χρήστες του BTC-e και ο οποίος επέτρεπε στο χρήστη του να στείλει ή και να λάβει παραστατικά χρήματα και κρυπτονομίσματα από άλλους χρήστες του BTC-e ανώνυμα, διευκολύνοντας έτσι το ξέπλυμα χρημάτων που προέρχονταν από εγκληματικές ενέργειες.

Μέσω των ανωτέρω μηχανισμών χρηματοδότησης, το BTC-e, εν γνώσει του και εν γνώσει του, Vinnik δέχτηκε μεταφορές χρημάτων από τράπεζες και από πολίτες των ΗΠΑ. Καθ' όλη την διάρκεια της λειτουργίας, του το BTC-e προέβη στη μεταφορά, αποθήκευση, ανταλλαγή, αγοραπωλησία και μετατροπή κρυπτονομισμάτων συμμετέχοντας στο ξέπλυμα και στη ρευστοποίηση εγκληματικών εσόδων από παράνομες δραστηριότητες, όπως το hacking υπολογιστών και ο εκβιασμός μέσω διαδικτύου, η απάτη, η κλοπή ταυτότητας, τα σχέδια απάτης επιστροφής φόρων και η διακίνηση ναρκωτικών.

Ιδιαίτερα μετά την κατάρρευση των διαδικτυακών ανταλλακτηριών ψηφιακού συναλλάγματος, το BTC-e, λειτουργούσε ως το κατεξοχήν ανταλλακτήριο που επέλεγαν οι κυβερνοεγκληματίες για τη μετατροπή κρυπτονομίσματος σε παραστατικό χρήμα.

Συγκεκριμένα, αμέσως μετά την κατάρρευση του Mt.Gox το 2013, το BTC-e είχε μεγάλη εισροή πρόσθετων πελατών-χρηστών και κυρίως όσων είχαν προηγουμένως κάνει χρήση των υπηρεσιών του BTC-e για το ξέπλυμα χρήματος από εγκληματικές δραστηριότητες. Επίσης, μερικοί από τους κυβερνοεγκληματίες που χρησιμοποιούσαν τον διαδικτυακό εκβιασμό, για να αποσπάσουν χρήματα από τους χρήστες ηλεκτρονικών υπολογιστών, χρησιμοποιούσαν το BTC-e ως μέσον για την φύλαξη, την διανομή και το ξέπλυμα των εγκληματικών εσόδων τους αξίας πολλών εκατοντάδων χιλιάδων δολαρίων σε πολλές εκατοντάδες χιλιάδες δολάρια. Ο Vinnik κατηγορήθηκε και για συμμετοχή στο ransomware «Locky», το οποίο μόλυνε υπολογιστές και στη συνέχεια ζητούσε τα λύτρα να καταβληθούν σε BTC.

Ακόμα, σε λογαριασμούς οι οποίοι ελέγχονταν, ανήκαν και λειτουργούσαν από το BTC-e, από τον Vinnik και από τρίτα πρόσωπα, κατατέθηκε ένα μεγάλο τμήμα των κλεμμένων κρυπτονομισμάτων προερχομένων από το ανταλλακτήριο Mt.Gox, που υπέστη κατ' εξακολούθηση επιθέσεις hacking και επακόλουθες κλοπές περίπου από το Σεπτέμβριο 2011 έως το Μάιο 2014. Επίσης, το BTC-e χρησιμοποιήθηκε από διακινητή ναρκωτικών για το για ξέπλυμα εσόδων από την πώληση ναρκωτικών. Όταν ο εν λόγω διακινητής συνελήφθη αποκάλυψε ότι προτίμησε το BTC-e αντί άλλων ανταλλακτηρίων, επειδή το συγκεκριμένο υπέβαλλε λίγες ή καθόλου ερωτήσεις σχετικά με την πραγματική ταυτότητα των χρηστών και επειδή ο αυτός ήθελε να αποφύγει να δείξει την ταυτότητά του online λόγω των παράνομων δραστηριοτήτων του. Τέλος, το BTC-e χρησιμοποιήθηκε και από δύο διεφθαρμένους Ομοσπονδιακούς Πράκτορες των ΗΠΑ, για να ξεπλύνουν αρκετές εκατοντάδες χιλιάδες δολάρια από εγκληματικά έσοδα, προερχόμενα από κλοπές κυβερνητικής περιουσίας και από εκβιασμούς.

Κατηγορητήριο

α) ΗΠΑ

Ο ΑΠ με την απόφαση 2080/2017 επικύρωσε την απόφαση υπ` αριθ. 690/4-10-2017 του Εφετείου Θεσσαλονίκης σύμφωνα με την οποία ανοιγόταν ο δρόμος για την έκδοση του Vinnik στις ΗΠΑ. Ο ΑΠ εξέτασε εκ μέρους της εκζητούσας αρχής των ΗΠΑ κατά πόσον οι υποβληθείσες αποδείξεις παρείχαν πιθανότητα ενοχής του Vinnik για τα εγκλήματα, για τα οποία ζητείτο η έκδοσή του. Σύμφωνα με το ένταλμα σύλληψης των ΗΠΑ, ο Vinnik κατηγορείτο για τα εγκλήματα **α)** λειτουργίας μη αδειοδοτημένης επιχείρησης υπηρεσιών

χρηματικών συναλλαγών[254], **β)** συνωμοσίας για διάπραξη ξεπλύματος χρήματος[255], **γ)** ξεπλύματος χρήματος[256] και **δ)** διεξαγωγής παράνομων χρηματικών συναλλαγών[257].

Από τις καταθέσεις, σε συνδυασμό και με τα λοιπά έγγραφα της δικογραφίας, προέκυψε ότι πράγματι τα μέσα και οι τρόποι που χρησιμοποιήθηκαν από τον Vinnik και τα συνεργαζόμενα με αυτόν πρόσωπα, με τα οποία είχε ενωθεί για τη μετατροπή και μεταβίβαση περιουσίας προερχόμενης από εγκληματικές ενέργειες μέσω του BTC-e και ενός πλέγματος κατονομαζόμενων εταιρειών και διαδικτυακών λογαριασμών.

Άλλωστε, και κατά την Ελληνική Νομοθεσία για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες[258], η γνώση, η πρόθεση ή ο σκοπός που απαιτούνται ως στοιχείο του πραγματικού μπορούν να συνάγονται και από τις συντρέχουσες πραγματικές περιστάσεις. Η πιθανολόγηση των ως άνω σοβαρών ενδείξεων ενοχής του Vinnik, η οποία πιστοποιείται από την μεταφορά χρημάτων μέσω των προαναφερθέντων λογαριασμών που διαχειριζόταν ο ίδιος προσωπικά, δεν ανατρέπεται από τις καταθέσεις των εξετασθέντων μαρτύρων, πρωτοδίκως και κατ` έφεση, αφού από όλα τα αποδεικτικά στοιχεία επιβεβαιώθηκε τόσο ο καθοριστικός έλεγχος και η διαχείριση που ασκούσε ο εκζητούμενος στο BTC-e, το οποίο, όπως προέκυψε, διέκοψε τη λειτουργία του όταν ο εκζητούμενος συνελήφθη και αφαιρέθηκε από την κατοχή του ο υπολογιστής του, όσο και ο δόλος του τελευταίου, αφού προέκυψε ότι αυτός συνειδητά και σκόπιμα δεν πραγματοποιούσε στην ιστοσελίδα του BTC-e, που διαχειριζόταν έλεγχο της ταυτότητας και του διαβατηρίου των χρηστών, διότι γνώριζε ότι γινόταν από τους ανώνυμους χρήστες ξέπλυμα χρήματος, που προερχόταν από εγκληματικές δραστηριότητες, όπως διακίνηση ναρκωτικών, διαδικτυακός εκβιασμός, κλοπές από λογαριασμούς ψηφιακών νομισμάτων και άλλες.

---

[254] Παράβαση του τίτλου 18, εδάφια 1960 και 2 του ΠΚ των ΗΠΑ, που τιμωρείται με πρόστιμο ή και ποινή φυλάκισης έως πέντε (5) ετών.

[255] Παράβαση του τίτλου 18, εδάφιο 1956 (h) του ΠΚ των ΗΠΑ, που τιμωρείται με ποινή φυλάκισης μέχρι είκοσι (20) ετών ή και πρόστιμο μέχρι 500.000 δολαρίων ή διπλάσιο της αξίας των περιουσιακών στοιχείων της συναλλαγής.

[256] Παράβαση του τίτλου 18, εδάφια 1956 (a) (1) (A) (i), (a) (1) (B) (i) και 2 του ΠΚτων ΗΠΑ, που τιμωρείται με ποινή φυλάκισης μέχρι είκοσι (20) ετών ή και πρόστιμο μέχρι 500.000 δολαρίων ή διπλάσιο της αξίας των περιουσιακών στοιχείων της συναλλαγής.

[257] Παράβαση του τίτλου 18, εδάφια 1957 και 2 του ΠΚ των ΗΠΑ, που τιμωρείται με ποινή φυλάκισης μέχρι δέκα (10) ετών ή και πρόστιμο μέ-χρι 500.000 δολαρίων ή διπλάσιο της αξίας των περιουσιακών στοιχείων της συναλλαγής.

[258] Ν. 3691/2008, άρθ. 2 παρ. 2,3,5.

Σημαντική φημολογείται και η εμπλοκή του Vinnik στα κλεμμένα BTC του ανταλλακτηρίου Mt.Gox, καθώς σύμφωνα με μια ομάδα ερευνητών που βρίσκεται στο Τόκιο, τη στιγμή της σύλληψής του ήταν ο κατεξοχήν ύποπτος για την εμπλοκή του στην κλοπή[259].

Ο ΑΠ απεφάνθη ότι, «πέραν της κατηγορίας για τη λειτουργία μη αδειοδοτημένης επιχείρησης υπηρεσιών χρηματικών συναλλαγών», οι λοιπές αποδιδόμενες πράξεις εμπίπτουν στην έννοια του διπλού αξιοποίνου, ανεξάρτητα από την κατηγορία εγκλημάτων στην οποία κατατάσσονται, τον τρόπο περιγραφής τους και την χρησιμοποιούμενη γι` αυτές ορολογία στο Ποινικό Δίκαιο των ΗΠΑ, είναι αξιόποινες και κατά την ελληνική νομοθεσία και στοιχειοθετούν, κατ` αντιστοιχία, τη νομοτυπική μορφή του εγκλήματος της νομιμοποίησης εσόδων από τις εγκληματικές δραστηριότητες της διακίνησης ναρκωτικών ουσιών[260], της διακεκριμένης απάτης με υπολογιστή[261] (ΠΚ 386Α, σε συνδυασμό με ΠΚ 386 παρ. 2, της εκβίασης)[262] (ΠΚ 385 περ. 1 εδ. β`) και διακεκριμένης κλοπής (ΠΚ 374 περ. ε`), που τελέσθηκε εν γνώσει του δράστη με: **α)** τη μετατροπή και τη μεταβίβαση περιουσίας προερχόμενης από τις ανωτέρω εγκληματικές δραστηριότητες, με σκοπό την απόκρυψη και συγκάλυψη της παράνομης προέλευσής της και την παροχή συνδρομής σε οποιονδήποτε εμπλέκεται στις δραστηριότητες αυτές, προκειμένου να αποφύγει τις έννομες συνέπειες των πράξεών του, **β)** την απόκρυψη και συγκάλυψη της φύσης, προέλευσης, διάθεσης, διακίνησης και χρήσης περιουσίας προερχόμενης από τις ανωτέρω εγκληματικές δραστηριότητες, **γ)** την απόκτηση, κατοχή, διαχείριση και χρήση της προερχόμενης από τις ανωτέρω εγκληματικές δραστηριότητες περιουσίας, **και δ)** τη σύσταση οργάνωσης ή ομάδας δύο τουλάχιστον ατόμων για την διάπραξη των εν λόγω πράξεων, από πρόσωπο το οποίο ενεργεί τόσο για λογαριασμό του, όσο και προς όφελος και εντός των πλαισίων εγκληματικής οργάνωσης ή ομάδας, όπως προβλέπεται από τις διατάξεις των άρθρων 1, 2 περ. α`, β`, γ`, ε`, 3 περ. ζ`, θ`, κ`, 4 παρ. 1, 45 παρ. 1 περ. γ` - α`, 46, 48, 49 και 50 του Ν. 3691/2008 και τιμωρείται με κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή από 50.000,00 ευρώ έως 2.000.000,00 ευρώ. Η νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες, όπως προκύπτει από το συνδυασμό των ως άνω διατάξεων του Ν. 3691/2008, είναι κατά το ελληνικό ποινικό δίκαιο έγκλημα υπαλλακτικώς μικτό, αφού οι

---

[259]. Schwartz, M., 2018. *Hacked Mt. Gox Bitcoin Exchange Chief Maintains Innocence.* Available at: https://www.bankinfosecurity.com/hacked-mt-gox-bitcoin-exchange-chief-maintains-innocence-a-11904 (Accessed 10/05/2021.

[260] Αρ. 20 Ν. 3459/2006, όπως αντικαταστάθηκε με το άρθ. 20 του Ν. 4139/2013.

[261] Αρ. 20 Ν. 3459/2006, όπως αντικαταστάθηκε με το άρθ. 20 του Ν. 4139/2013.

[262] Αρθ. 20 Ν. 3459/2006, όπως αντικαταστάθηκε με το άρθ. 20 του Ν. 4139/2013.

περισσότεροι τρόποι τελέσεώς του αποτελούν εκφάνσεις του ίδιου εγκλήματος που μπορούν να εναλλαχθούν και σε περίπτωση που συντρέχουν περισσότεροι τρόποι τελέσεώς του, μόνον ένα έγκλημα τελείται και όχι περισσότερα».

β) Γαλλία

Στις 16/06/2018 ζητήθηκε από τη Γαλλία η παράδοση στις δικαστικές αρχές της Γαλλίας του Vinnik, προκειμένου να δικασθεί για μια σειρά αδικημάτων[263] μεταξύ των οποίων τα αδικήματα της «υπεξαίρεσης από οργανωμένη σπείρα», της «απόπειρας υπεξαίρεσης από οργανωμένη σπείρα», του «ξεπλύματος χρήματος από οργανωμένη σπείρα». Ο Vinnik ειδικότερα διώκετο διότι θεωρήθηκε υπεύθυνος για τη μαζική διάδοση μέσω email ενός malware-ιού, του «Locky», ο οποίος εμφανίστηκε από το Φεβρουάριο του 2016 σε διάφορες περιοχές της Γαλλίας και των Η.Π.Α. Ο «Locky» ήταν ικανός να κρυπτογραφήσει εν αγνοία των θυμάτων προσωπικά και επαγγελματικά τους δεδομένα, ζητώντας από αυτά την πληρωμή λύτρων σε BTC για την αποκρυπτογράφηση των δεδομένων τους. Οι έρευνες που διενεργήθηκαν για τον ανωτέρω ιό αποκάλυψαν μία ιδιαίτερα περίπλοκη και φροντισμένη λειτουργία, τόσο κατά την προετοιμασία των μηνυμάτων και των μολυσμένων με τον εν λόγω ιό επισυνάψεών τους, όσο και κατά τη μαζική του διάδοση, ενώ επιβεβαιώθηκε η ύπαρξη εγκληματικής οργάνωσης στην πηγή αυτών των υπεξαιρέσεων. Η ανάλυση των πληρωμών των λύτρων επέτρεψε να ανιχνευθούν τα καταβληθέντα λύτρα και να ταυτοποιηθεί το BTC-e ως κεντρικός παράγοντας της εν λόγω εγκληματικής οργάνωσης, η οποία φαινόταν να έχει υπεξαιρέσει συνολικά 20643 BTC αξίας άνω των 130 εκατομμυρίων

[263] Αναλυτικά τα αδικήματα: «υπεξαίρεση από οργανωμένη σπείρα», «απόπειρα υπεξαίρεσης από οργανωμένη σπείρα», «ξέπλυμα χρήματος από οργανωμένη σπείρα», «συμμετοχή σε οργάνωση κακοποιών ενόψει παρασκευής εγκλήματος», «δόλια πρόσβαση στο σύνολο ή μέρος συστήματος αυτόματης επεξεργασίας δεδομένων», «δόλια πρόσβασης στο σύνολο ή μέρος συστήματος αυτόματης επεξεργασίας δεδομένων με το επιπλέον στοιχείο ότι οι ενέργειες διαπράχθηκαν εις βάρος κρατικού συστήματος αυτόματης εξεργασίας προσωπικών δεδομένων και από οργανωμένη σπείρα», «δόλια κατακράτησης όλου ή μέρους του συστήματος αυτόματης επεξεργασίας δεδομένων», «δόλια κατακράτησης όλου ή μέρους του συστήματος αυτόματης επεξεργασίας δεδομένων με το επιπλέον στοιχείο ότι οι σχετικές ενέργειες διαπράχθηκαν εις βάρος κρατικού συστήματος αυτόματης επεξεργασίας προσωπικών δεδομένων και από οργανωμένη σπείρα», «δόλια εισαγωγής δεδομένων σε σύστημα αυτόματης επεξεργασίας δεδομένων», «δόλια εισαγωγής δεδομένων σε σύστημα αυτόματης επεξεργασίας δεδομένων με το επιπλέον στοιχείο ότι οι σχετικές ενέργειες διαπράχθηκαν εις βάρος κρατικού συστήματος αυτόματης επεξεργασίας προσωπικών δεδομένων και από οργανωμένη σπείρα», «δόλια τροποποίησης δεδομένων που περιέχονται σε σύστημα αυτόματης επεξεργασίας δεδομένων», «δόλια τροποποίησης δεδομένων που περιέχονται σε σύστημα αυτόματης επεξεργασίας δεδομένων με το επιπλέον στοιχείο ότι οι σχετικές ενέργειες διαπράχθηκαν εις βάρος κρατικού συστήματος αυτόματης επεξεργασίας προσωπικών δεδομένων και από οργανωμένη σπείρα», τα οποία διεπράχθησαν κατά παράβαση των άρθρων 312-1, 312-6, 312-13, 312-14, 132-71, 131-26- 2, 121-5, 312-9, 324-1, 342-2, 324-3, 324-7, 324-8, 450-1, 450-3, 450-5, 323-1, 323-2, 323-3, 323-3-1, 323-5, 323-7, 323-4-1 του Γαλλικού Ποινικού Κώδικα.

ευρώ από τουλάχιστον 5700 θύματα παγκοσμίως, εκ των οποίων περισσότεροι από 100 ήταν Γάλλοι. Οι αμερικανικές αρχές, κατά τη διεξαγωγή αυτόνομης, σε σχέση με τις γαλλικές αρχές, έρευνας, ταυτοποίησαν τον Vinnik ως έναν από τους διαχειριστές του ανταλλακτηρίου.

Το Συμβούλιο Εφετών Θεσσαλονίκης με την υπ' αριθ. 532/2018 απόφασή του διέταξε την εκτέλεση του προαναφερθέντος Ευρωπαϊκού Εντάλματος Σύλληψης. Ειδικότερα, το ανωτέρω Συμβούλιο δέχτηκε ότι τα περιγραφόμενα στο εν λόγω ένταλμα εγκλήματα συνιστούν αξιόποινες πράξεις και κατά την ελληνική νομοθεσία, καθόσον αυτά προσομοιάζουν: με: **α)** εγκληματική οργάνωση - συγκρότηση, ένταξη[264], **β)** εκβίαση κατά συναυτουργία κατά συρροή, κατ' εξακολούθηση, κατ' επάγγελμα και κατά συνήθεια[265], **γ)** απάτη με υπολογιστή κατά συναυτουργία, κατ' εξακολούθηση, κατ' επάγγελμα και κατά συνήθεια με συνολικό περιουσιακό όφελος και προξενηθείσα ζημία που υπερβαίνουν συνολικά το ποσό των 120000 ευρώ[266], **δ)** παραβίαση προσωπικών δεδομένων με σκοπό παρανόμου περιουσιακού οφέλους κατ' εξακολούθηση[267] **και ε)** νομιμοποίηση εσόδων που πηγάζουν από εγκληματική δραστηριότητα κατ' εξακολούθηση, κατ' επάγγελμα και κατά συνήθεια εντός των πλαισίων εγκληματικής οργάνωσης[268]. Κατά της ανωτέρω αποφάσεως του Συμβουλίου Εφετών Θεσσαλονίκης ο Vinnik άσκησε έφεση, η οποία απορρίφθηκε με την υπ' αριθ. 2191/2018 απόφαση του Αρείου Πάγου.

γ) Ρωσία

- Στις 25/08/2017 ζητήθηκε από την Ρωσική Ομοσπονδία η έκδοση του Vinnik, προκειμένου να δικασθεί για το αποδιδόμενο σε αυτόν έγκλημα της απάτης, δηλαδή της κατάχρησης ξένης περιουσίας μέσω δόλου, διαπραχθείσης σε μεγάλη ποσότητα[269]. Ειδικότερα, σε αυτόν αποδόθηκε ότι, διαθέτοντας ειδικές γνώσεις στον τομέα προγραμματισμού ηλεκτρονικών υπολογιστών, τον Μάρτιο του 2015 επέτυχε να υπεξαιρέσει από μια εταιρεία ΕΠΕ χρηματικό ποσό ύψους 667250 ρουβλίων, δημιουργώντας στους υπαλλήλους αυτής την ψευδή εντύπωση ότι μια άλλη εταιρεία ΕΠΕ,

[264] Αρ.187 παρ. 1 του ΠΚ.
[265] Αρ.13στ, 45, 94 παρ. 1, 98, 385 παρ. 1γ του ΠΚ.
[266] Αρ.13στ, 45, 94 παρ. 1, 98, 386 Α σε συνδυασμό με το άρθρ. 386 παρ. 3α και ιβ του ΠΚ.
[267] Αρ.22 παρ. 4 και 6 του ν. 2472/1997, 98 του ΠΚ.
[268] Αρ.98 του Ποινικού Κώδικα, 3 στοιχ. α΄, ζ΄, κ΄, 45 παρ. 1α του ν. 3691/2008.
[269] Παράβαση του άρ. 159 παρ. 3 του Ρωσικού Ποινικού Κώδικα.

η οποία έφερε τα χαρακτηριστικά γνωρίσματα πλασματικής εταιρείας, θα της προμηθεύσει συγκεκριμένο εξοπλισμό, ο οποίος στην πραγματικότητα δεν υφίστατο. Το Συμβούλιο Εφετών Θεσσαλονίκης, στο οποίο εισήχθη η αίτηση εκδόσεως του Vinnik στη Ρωσική Ομοσπονδία, με την υπ' αριθ. 719/2017 απόφασή του γνωμοδότησε υπέρ της εκδόσεως του ανωτέρω στη Ρωσική Ομοσπονδία, προκειμένου να δικασθεί για το ανωτέρω αδίκημα. Ειδικότερα, το ανωτέρω Συμβούλιο δέχτηκε ότι η αποδιδόμενη πράξη είναι αξιόποινη και κατά το ελληνικό ποινικό δίκαιο και στοιχειοθετεί τη νομοτυπική μορφή του εγκλήματος της απάτης (άρθρο 386 παρ. 1. εδ. α΄ του Ποινικού Κώδικα). Τέλος, το ίδιο Συμβούλιο εδέχθη ότι το αποδιδόμενο έγκλημα είναι εξ εκείνων για τα οποία επιτρέπεται η έκδοση σύμφωνα με τις διεθνείς συμβάσεις που εφαρμόζονται εν προκειμένω, σύμφωνα δε με τους νόμους του Ελληνικού Κράτους και της Ρωσικής Ομοσπονδίας δεν συντρέχει νόμιμος λόγος που να εμποδίζει τη δίωξη του Vinnik ή να αποκλείει ή να εξαλείφει το αξιόποινο της αποδιδομένης σε αυτόν πράξης. Κατά της ανωτέρω αποφάσεως του Συμβουλίου Εφετών Θεσσαλονίκης δεν ασκήθηκε κάποιο ένδικο μέσο.

- Ακολούθως, στις 08/06/2018 ζητήθηκε ξανά από τη Ρωσική Ομοσπονδία η έκδοση του Vinnik, αυτή τη φορά για το αδίκημα της απάτης στον τομέα πληροφορίας υπολογιστών, δηλαδή της κλοπής ξένης περιουσίας μέσω εισόδου, διαγραφής, αποκλεισμού και τροποποίησης της πληροφορίας υπολογιστών, διαπραττόμενη σε ιδιαίτερα μεγάλες ποσότητες[270]. Ειδικότερα, από το 2011 έως το 2017, προέβη σε συμφωνίες με μεγάλο αριθμό πωλητών και αγοραστών κρυπτονομισμάτων για τους ειδικούς όρους εισαγωγής, ανταλλαγής και εξαγωγής κρυπτονομισμάτων και χρημάτων αναγκαστικής κυκλοφορίας, τα οποία, προηγουμένως, είχαν κλαπεί από τους πολίτες της Ρωσικής Ομοσπονδίας, τους οργανισμούς που δραστηριοποιούνται στο έδαφός της και τους πιστωτικούς οργανισμούς, κατόπιν δε τα κρυπτονομίσματα και τα χρήματα αναγκαστικής κυκλοφορίας μετετράπησαν σε μετρητά από συνεργούς του Vinnik. Ακόμα, σε μετρητά μετετράπηκαν τα χρήματα που είχαν κλαπεί από τους λογαριασμούς των τραπεζών που ευρίσκονται στο έδαφος της Ρωσικής Ομοσπονδίας, με τη μέθοδο hacking στα δίκτυα υπολογιστών των τραπεζών.

Τα κλαπέντα χρήματα μετεφέρθηκαν από συνεργούς του Vinnik σε διαφορετικές κάρτες τράπεζας και στη συνέχεια μετετράπησαν από συνεργούς του ιδίου σε μετρητά μέσω ATM. Αποτέλεσμα της κατά τα ανωτέρω απάτης στον τομέα του κυβερνοχώρου ήταν να

[270] Παράβαση του άρ. 159. 6 παρ. 4 του Ρωσικού Ποινικού Κώδικα.

προκληθεί ζημία σε πολίτες και οργανισμούς της Ρωσικής Ομοσπονδίας, συνολικού ύψους άνω των 750 εκατομμυρίων ρουβλίων. Το Συμβούλιο Εφετών Θεσσαλονίκης υπ' αριθ. 561/2018 απόφασή του γνωμοδότησε υπέρ της εκδόσεως του Vinnik στη Ρωσική Ομοσπονδία, προκειμένου να δικασθεί για το ανωτέρω αδίκημα. Κατά της ανωτέρω αποφάσεως του Συμβουλίου Εφετών Θεσσαλονίκης ασκήθηκε έφεση, η οποία απορρίφθηκε με την υπ' αριθ. 2191/2018 απόφαση του Αρείου Πάγου.

Ο ίδιος ο Vinnik ζήτησε να εκδοθεί στη χώρα καταγωγής του, τη Ρωσία, επικαλούμενος λόγους παραβίασης ανθρωπίνων δικαιωμάτων, σε περίπτωση που η έκδοσή του γινόταν σε κάποια άλλη χώρα. Εν τέλει εκδόθηκε στην Γαλλία τον Ιανουάριο του 2020, έπειτα από απόφαση του Υπουργού Δικαιοσύνης. Μετά από δίκη που διεξήχθη στο Παρίσι, αθωώθηκε για την πληθώρα των κατηγοριών και κρίθηκε ένοχος μόνο για το ξέπλυμα χρήματος από παράνομες δραστηριότητες. Του επιβλήθηκε ποινή φυλάκισης πέντε χρόνων και χρηματικό πρόστιμό 100000 ευρώ. Στην απόφαση ασκήθηκε έφεση σύμφωνα με τον γαλλικό δίκαιο. Ο Έλληνας νομοθέτης πήρε μια γεύση για το τι μπορεί να προκαλέσουν τα κρυπτονομίσματα, για το πόσο επιθετικά εισβάλλουν στον κόσμο μας και για το τι συνέπειες μπορεί να έχει η χρήση τους, κρούοντας τον κώδωνα του κινδύνου και αναλογιζόμενοι ότι μελλοντικά πρέπει να γίνουν νομοθετικές καινοτομίες.

ΚΕΦΑΛΑΙΟ 7ο
ΑΞΙΟΛΟΓΗΣΗ ΤΗΣ ΧΡΗΣΗΣ ΤΟΥ BITCOIN

Αποτελεί αδιαμφισβήτητο γεγονός ότι το νομικό μας σύστημα, υπό το πρίσμα της τεχνολογικής καινοτομίας συναντά και ανακαλύπτει τα όριά του. Οι Κεντρικές Τράπεζες, τα Κρατικά Όργανα και τα Ιδιωτικά Χρηματοπιστωτικά Ιδρύματα βρίσκονται μπροστά σε ένα νέο είδος νομίσματος το οποίο αδυνατούν να ελέγξουν με οποιονδήποτε τρόπο. Στο νέο «ψηφιακό οικοσύστημα» που έχει δημιουργηθεί εμπλέκονται αρκετές κατηγορίες ανθρώπων, γεγονός που αναγκάζει σιγά σιγά όλο και περισσότερες ρυθμιστικές αρχές να αρχίζουν να παρέχουν κανόνες και οδηγίες για τη διαμόρφωση του ρυθμιστικού τοπίου και τη μεταχείριση των ψηφιακών νομισμάτων. Η ανάγκη λοιπόν κατανόησης των ωφελειών και κινδύνων που δημιουργούν τα νέα ηλεκτρονικά συστήματα πληρωμών και χρηματοοικονομικών συναλλαγών καθίσταται αναγκαία προκειμένου να διασφαλιστεί εν συνεχεία και η απαραίτητη για τη σταθερότητά τους δικαιική ρύθμιση. Μόνο στην περίπτωση αυτή τα συστήματα των κρυπτονομισμάτων θα αποπνέουν ασφάλεια δικαίου και θα μπορέσουν να αποκτήσουν τόση πίστη από τους συναλλασσόμενους, ώστε να ωριμάσουν και να γνωρίσουν μια γενική ανάπτυξη[271].

Το Bitcoin είναι μια εναλλακτική λύση σε σχέση με τις άλλες μεθόδους ηλεκτρονικών πληρωμών που γίνονται αποδεκτές από επιχειρήσεις. Οι θιασώτες της τεχνολογίας του Blockchain, επικαλούνται τις ωφέλειες-πλεονεκτήματα[272] προκειμένου να το υπερασπιστούν. Οι πολέμιοι όμως της τεχνολογίας αυτής ισχυρίζονται ότι τα βασικά πλεονεκτήματα του Bitcoin μπορούν εύκολα να δημιουργήσουν κινδύνους και να καταστούν μειονεκτήματα[273], γεγονός που καθιστά την εφαρμογή του μερικώς επισφαλή.

---

[271] Βλ. *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 503, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 25.

[272] Βλ. *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 499, *Θεοδωράκης, Ν., Καλογεράκης Γ.*, ό.π., σελ. 7, 12, *Ντότσιας, Σ.*, ό.π., σελ. 324, *Μάλαμας, Φ.*, ό.π., σελ.195-196, Antonopoulos, ό.π., σελ. 216-217, 269-270, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 20, 22-23, *Chytis, E., Kitsantas, T. and Vazakidis, A.*, ό.π., σελ. 10-11, *Cavin, C., Chiriaeva, M. & Poskriakov, F*, ό.π., σελ.166.

[273] Βλ. *Θεοδωράκης, Ν., Καλογεράκης Γ.*, ό.π., σελ. 8, 12, *Παρασκευόπουλος-Κόλιας, Χ.*, [2014], ό.π., σελ. 4, 498-499, *Ντότσιας, Σ.*, ό.π., σελ. 324-325, *Μάλαμας, Φ.*, ό.π., σελ. 197, 206, *Μούζουλας, Σ.*, ό.π., σελ. 1184,

1) Ασφάλεια

Οι συναλλαγές που γίνονται με BTC είναι απόλυτα ασφαλείς με τη χρήση της κρυπτογραφίας και αλγόριθμων ασφαλούς κατακερματισμού όπως ο SHA-256, ο οποίος αρχικά σχεδιάστηκε από την NSA στις Ηνωμένες Πολιτείες. Όλες οι συναλλαγές σφραγίζονται ψηφιακά με έναν κρυπτογραφικό κωδικό, ώστε η παραβίασή του καθίσταται αν όχι αδύνατη, τουλάχιστον εξαιρετικά δυσχερής.

ΟΜΩΣ

Η παρουσία και χρήση κλειδιών για την πραγματοποίηση των συναλλαγών, εκτός από ασφάλεια, εγκυμονεί και κινδύνους. Οι χρήστες του Bitcoin χρησιμοποιούν περίπλοκους κωδικούς και κρατούν τα κλειδιά τους ασφαλή, χωρίς να τα μοιράζονται με κανέναν, με αποτέλεσμα αυτά να καθίστανται απρόσιτα σε περίπτωση που αυτοί δεν δύνανται να τα ξεκλειδώσουν, λόγω μη-ικανότητας ή θανάτου τους. Υπάρχουν ακόμη περιπτώσεις, που οι οικογένειες των χρηστών αγνοούν παντελώς την ύπαρξη των BTC. Λύση στην περίπτωση αυτή δίνεται με το σύστημα των πολλαπλών υπογραφών και της διαθήκης διαμέσου δικηγόρου, που λειτουργεί ως «εκτελεστής της διαθήκης». Σημαντικό κίνδυνο για τους χρήστες είναι επίσης η περίπτωση που το ιδιωτικό κλειδί χαθεί, καθώς η πρόσβαση στα BTC δεν είναι ανακτήσιμη. Ακόμη, η κακή προστασία του πορτοφολιού μπορεί να αφήσει τους χρήστες ευάλωτους σε κλοπές από ειδικά κατασκευασμένο κακόβουλο λογισμικό, σχεδιασμένο για να κλέβει BTC. Επιπλέον, τα κλειδιά που βρίσκονται σε ένα πορτοφόλι Bitcoin μπορούν να αντιγραφούν τόσο εύκολα όπως αντιγράφεται ένας οποιοσδήποτε φάκελος σε έναν υπολογιστή, να αποθηκευτούν σε πολλαπλά αντίγραφα και να εκτυπωθούν σε έντυπη μορφή.

2) Αποκέντρωση

Ο αποκεντρωμένος χαρακτήρας του Bitcoin είναι εξαιρετικά σημαντικός, διότι, αποσκοπώντας να πετύχει την απεξάρτησή του από κάθε είδους κεντρική εξουσία, τοποθετεί μεγάλη δύναμη στα χέρια των χρηστών του. Μέσω του δικτύου P2P τα δεδομένα μπορούν να καταγραφούν, να αποθηκευτούν και να ενημερωθούν από μια ομάδα κόμβων, με απουσία της μεσολάβησης και της επιβολής περιορισμών από τρίτα μέρη ή μεσάζοντες. Σε αντίθεση,

Antonopoulos, ό.π., σελ. 216-217, 255-256, 269-270, 274, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 13-14, 21-23, Bongcayao, R.J., ό.π., σελ. 13, Stevo, ό.π., σελ. σελ. 73, *Swan, M.*, ό.π., σελ. 3, *Chytis, E., Kitsantas, T. and Vazakidis, A.*, ό.π., σελ. 11, *European Central Bank.[2015]* ό.π., *Stearns, B.*, ό.π., σελ.1191-1192.

ένα κεντρικά σχεδιασμένο μοντέλο, όπως μία παραδοσιακή τράπεζα ή ένα δίκτυο πληρωμών, είναι επιφορτισμένο να ελέγχει όποιον έχει πρόσβαση και να παρέχει προστασία για να διατηρεί εκτός συστήματος αυτούς που επιθυμούν να το παραβιάσουν και να υποκλέψουν πληροφορίες.

ΟΜΩΣ

Πολλά πρώιμα ανταλλακτήρια BTC αποτέλεσαν εύκολα θύματα για κυβερνοεγκληματίες και οδήγησαν στην απώλεια των BTC, διότι συγκέντρωσαν όλα τα κεφάλαια των χρηστών τους σε ένα μόνο συνδεδεμένο πορτοφόλι και αποθήκευσαν τα κλειδιά σε ένα μοναδικό διακομιστή. Επίσης, η αποκεντρωμένη αυτονομία με τη μορφή ιδιωτικών κλειδιών, που αποθηκεύονται με ασφάλεια στο πορτοφόλι συνεπάγεται ότι το BTC χάνεται δια παντός διότι δεν είναι δυνατή η ανάκτηση κωδικού πρόσβασης εάν δεν υπάρχουν αντίγραφα ασφαλείας του κλειδιού. Οι χρήστες θα πρέπει είναι οι ίδιοι υπεύθυνοι για την διατήρηση της μυστικότητας των κλειδιών τους.

3) Ανωνυμία

Η ένταξη χρηστών στο δίκτυο Bitcoin γίνεται χωρίς την έγκριση από τρίτους ή την πλήρωση κάποιας τυπικής πράξης, εν αντιθέσει με ένα παραδοσιακό σύστημα πληρωμών, για παράδειγμα με πιστωτικές κάρτες, όπου η πληρωμή είναι ανοιχτού τύπου και περιέχει τα προσωπικά αναγνωριστικά στοιχεία του χρήστη, όπως τον αριθμό της πιστωτικής κάρτας του. Στο δίκτυο Bitcoin οι εγγραφές γίνονται μέσω κωδικών ονομάτων με αποτέλεσμα να εξασφαλίζεται η ανωνυμία των χρηστών και να μην χρειάζεται να είναι κρυπτογραφημένο ή προστατευμένο από υποκλοπές. Έτσι, μία συναλλαγή με BTC δεν αποκαλύπτει καμία προσωπική πληροφορία, όπως τις ταυτότητες των συμβεβλημένων, δεν μπορεί να χρησιμοποιηθεί για να εξουσιοδοτήσει περεταίρω πληρωμές και μπορεί να μεταδοθεί μέσω οποιουδήποτε μη ασφαλούς δικτύου, χωρίς τον κίνδυνο απώλειας ασφαλείας.

ΟΜΩΣ

Οι πολέμιοι του δικτύου Bitcoin ισχυρίζονται ότι δεν είναι ανώνυμο αλλά ότι είναι ψευδώνυμο. Παρά το γεγονός ότι οι επιμέρους κόμβοι ελέγχουν τις συναλλαγές και ότι γίνεται χρήση κωδικών ονομάτων, ελλοχεύει ο κίνδυνος αποκάλυψης της ταυτότητας του χρήστη σε κάποιον που παρακολουθεί τις συναλλαγές από και προς μια διεύθυνση Bitcoin για μεγάλο χρονικό διάστημα. Ακόμα και στην περίπτωση που κάποιος κατέχει πολλαπλούς λογαριασμούς και χρησιμοποιεί πολλαπλά ψευδώνυμα δεν μπορεί να είναι σίγουρους ότι

έχει καταφέρει να έχει την τέλεια ανωνυμία. Κάποιος λοιπόν με κατάλληλες γνώσεις μπορεί να επεξεργαστεί τις πληροφορίες που παρέχει η ψευδώνυμη διεύθυνση και να καταλήξει στην πραγματική ταυτότητα του χρήστη. Για παράδειγμα, όταν ένας χρήστης θα αγοράσει ένα προϊόν με BTC και συμπληρώσει ή το email του ή τη διεύθυνση της κατοικίας του για την παράδοση των αγαθών\υπηρεσιών που αγόρασε ή ακόμα τον τραπεζικό λογαριασμό που χρησιμοποίησε για την αγορά BTC, τότε η ταυτότητά του θα αποκαλυφθεί σε όλους, με αποτέλεσμα να μπορούν να ελεγχθούν όλες οι συναλλαγές που έχει διεξάγει. Μια λύση στο πρόβλημα που προκύπτει είναι η διαρκής χρήση νέων διευθύνσεων ή η χρήση συνδυαστικών υπηρεσιών που διακόπτουν τον σύνδεσμο μεταξύ του χρήστη και των BTC του. Ένα ακόμη πρόβλημα που δημιουργεί η ανωνυμία της χρήσης του Bitcoin είναι ότι διευκολύνει τη διενέργεια των παράνομων συναλλαγών.

4) Συναίνεση και Διαφάνεια

Χάρη στον αλγόριθμο απόδειξης εργασίας εξασφαλίζεται η συναίνεση. Υπάρχει πλήρης και άμεσος έλεγχος των αξιών που κατέχονται από τους χρήστες, καθώς το Blockchain είναι διανεμημένο μεταξύ των ηλεκτρονικών υπολογιστών που συνδέονται στο δίκτυο P2P και η επαλήθευση των συναλλαγών ή ο οποιοσδήποτε έλεγχος να μπορεί να γίνει ανά πάσα στιγμή από κάθε κόμβο.

Επίσης, όλες οι συναλλαγές που πραγματοποιούνται με BTC είναι διαφανείς, καθώς στο Blockchain περιλαμβάνονται όλες οι λεπτομέρειες που αφορούν την αρχική πηγή, τον προορισμό, την ώρα και την ημερομηνία των συναλλαγών.

ΟΜΩΣ

Στην περίπτωση που το δίκτυο Bitcoin δεχθεί επίθεση συναίνεσης από συνεργαζόμενους κόμβους, δημιουργούνται αμφιβολίες σχετικά με την εγκυρότητα του Blockchain. Μία πιθανή επίθεση συναίνεσης θα έπληττε άμεσα την εμπιστοσύνη στο δίκτυο Bitcoin και θα προκαλούσε σημαντική μείωση της τιμής του BTC. Από τη μία λοιπόν, η τεράστια αύξηση της συνολικής ισχύος των κατακερματισμών κάνει το δίκτυο του Bitcoin αδιαπέραστο από επιθέσεις μεμονωμένων εξορυκτών, διότι δεν υπάρχει κανένας εφικτός τρόπος για έναν μεμονωμένο εξορύκτη να ελέγξει παραπάνω από ένα μικρό ποσοστό της συνολικής ισχύος εξόρυξης. Από την άλλη όμως, ο συγκεντρωτισμός του ελέγχου που προκαλείται από τις ομάδες εξόρυξης, εισάγει τον κίνδυνο επιθέσεων προς όφελος του χειριστή της ομάδας. Εξάλλου, γνωρίζοντας ότι η βιωσιμότητα του δικτύου Bitcoin εξαρτάται από την εξόρυξη,

προβληματίζει το γεγονός ότι αν εξαφανιστούν τα κίνητρα για εξόρυξη και αυτή σταματήσει, κανείς δεν ξέρει αν θα συνεχίσει η ύπαρξη συναίνεσης στο δίκτυο Bitcoin ή αν θα μπορούσε να υπάρξει κάποια «εναλλακτική θύρα» που να επιτρέπει σε κάποιον να ελέγχει το σύστημα.

5) Ταχύτητα

Η χρήση του Blockchain μειώνει τον χρόνο που απαιτείται για την επεξεργασία συναλλαγών από περίπου τρεις ημέρες σε μερικά λεπτά ή δευτερόλεπτα και τεράστιες ποσότητες δεδομένων μεταφέρονται με μεγάλη ταχύτητα, ακρίβεια και αμεσότητα.

ΟΜΩΣ

Λόγω της σύνθετης διαδικασίας επαλήθευσης, ο παράγοντας χρόνος αποτελεί μειονέκτημα σε περιπτώσεις μαζικών συναλλαγών.

6) Αυτονομία

Οι κόμβοι στο Blockchain μπορούν να μεταδίδουν και να λαμβάνουν δεδομένα μεταξύ τους δρώντας ως αυτόνομες οντότητες. Η σημασία της λειτουργίας αυτής είναι εξέχουσα και καθώς κανείς δεν μπορεί να παρεμβαίνει σε αυτόν τον μηχανισμό.

ΟΜΩΣ

Καθώς οι κόμβοι δρουν αυτόνομα και επιφορτίζονται με την επαλήθευση των συναλλαγών, υπάρχει φόβος ότι το δίκτυο Bitcoin θα καταστεί ανεξέλεγκτο σε τέτοιο βαθμό ώστε να εκτοπίζει με εξαιρετική ευκολία οποιαδήποτε δυνατότητα νομισματικής παρέμβασης.

7) Αδιάβλητο συναλλαγών

Κάθε νέα συναλλαγή που περιλαμβάνεται στο Blockchain σχετίζεται με τις προηγούμενες, δημιουργώντας μια ενδοσυνδεδεμένη αλυσίδα. Οι αλγόριθμοι, τα κρυπτογραφικά κλειδιά και οι χρονοσφραγίδες διασφαλίζουν το αδιάβλητο των συναλλαγών. Από τη στιγμή λοιπόν που η συναλλαγή θα ενταχθεί σε ένα μπλοκ που έχει εξορυχθεί, αποτελεί μία μη τροποποιήσιμη, μόνιμη και αξιόπιστη καταχώρηση.

ΟΜΩΣ

Στο Blockchain καταγράφονται ακόμα και τα λάθη με αποτέλεσμα να δημιουργείται πρόβλημα σε επόμενες συναλλαγές. Το πρόβλημα επιλύεται μόνο με τη συναίνεση των συμμετεχόντων.

8) Κόστος συναλλαγών

Χάρη στην τεχνολογία του Blockchain αποφεύγονται όλα τα πρόσθετα γενικά έξοδα και τα τέλη συναλλαγής και καθιερώνεται χαμηλό κόστος συναλλαγών. Για παράδειγμα, η χρήση πιστωτικών καρτών είναι δαπανηρή και οι πελάτες καταλήγουν να πληρώνουν για λογαριασμό του εμπόρου και διάφορες χρεώσεις όπως τα τέλη κίνησης. Αντίθετα, οι πληρωμές με BTC μπορούν να διεκπεραιωθούν με ελάχιστες ή καθόλου χρεώσεις, καθώς εναπόκειται στη διακριτική ευχέρεια του αποστολέα αν θα συμπεριλάβει μια χρέωση συναλλαγής, που θα του διασφαλίσει ταχύτερη επιβεβαίωση. Οι χρήστες μπορούν επίσης να επιλέξουν να χρησιμοποιήσουν BTC για γρήγορες διασυνοριακές μεταφορές, χωρίς να πληρώνουν ακριβά έξοδα για εμβάσματα.

ΟΜΩΣ

Οι ποσότητες υπολογιστικής ισχύος που απαιτούνται για την δημιουργία ενός μπλοκ και της ενημέρωσης του Blockchain είναι πάρα πολύ μεγάλες. Η υπολογιστική ισχύς μεταφράζεται σε πλήθος υπολογιστών που καταναλώνουν τεράστιες ποσότητες ηλεκτρικής ενέργειας και σε χρόνο που χρειάζεται για την δημιουργία ενός μπλοκ. Αν συγκρίνουμε τις συναλλαγές που γίνονται μέσω κάποιου κεντρικού συστήματος όπως είναι η τράπεζα και οι οποίες διαρκούν μόλις μερικά δευτερόλεπτα, αντιλαμβανόμαστε ότι τα 10 λεπτά που απαιτούνται για τη δημιουργία ενός μπλοκ είναι πολύς χρόνος. Βέβαια το μειονέκτημα αυτό αντισταθμίζεται από την τεράστια ασφάλεια που προσφέρει η αποκεντρωμένη δομή του Blockchain.

9) Πληθωρισμός - Αποπληθωρισμός

Χαρακτηριστικό του δικτύου Bitcoin είναι η απουσία πληθωριστικού κινδύνου για δύο λόγους. Πρώτον, ο Satoshi Nakamoto εξ υπαρχής προβλέπει την πεπερασμένη και φθίνουσα έκδοση των BTC και δεύτερον, το BTC δεν κινδυνεύει να υποστεί πληθωρισμό μέσω εκτύπωσης.

ΟΜΩΣ

Το γεγονός ότι ο αριθμός των BTC που θα εκδοθούν είναι εξ υπαρχής προκαθορισμένος, δημιουργεί προοπτικές αποπληθωρισμού. Ο αποπληθωρισμός είναι η υπερτίμηση της αξίας ενός νομίσματος λόγω αναντιστοιχίας μεταξύ προσφοράς και ζήτησης και συν τω χρόνω το νόμισμα αποκτά μεγαλύτερη αγοραστική δύναμη. Πολλές φορές το BTC χρησιμοποιείται ως μέσον αποταμίευσης, αφού κάποιοι χρήστες το αντιμετωπίζουν ως μέσον επένδυσης, που

μπορεί να τους εξασφαλίσει μελλοντικά κέρδη. Με δεδομένο λοιπόν ότι το BTC χρησιμοποιείται συστηματικά στις συναλλαγές, θα αυξανόταν μεν η ζήτησή του, θα μειωνόταν όμως η προσφορά του, με αποτέλεσμα η τιμή του να φτάνει στα ύψη. Όσοι κατέχουν Bitcoin θα το κρατούν λόγω της αύξησης της τιμής του και δεν θα θέλουν να το χρησιμοποιήσουν για πληρωμές. Αν συμβεί κάτι τέτοιο θα έχει ως αποτέλεσμα τον αποπληθωρισμό του νομίσματος, μετατρέποντας ουσιαστικά ένα από τα πλεονεκτήματά του σε φρικτό μειονέκτημα καθότι μια αποπληθωριστική οικονομία είναι καταστροφική και πρέπει πάση θυσία να αποφευχθεί.

Επίλογος.

Εξαρχής το Bitcoin παρουσίασε οικονομικό ενδιαφέρον. Από τους αμφισβητίες του θεωρήθηκε ως ένας νέος απαιτητικός εχθρός, βρήκε όμως και πολλούς υπέρμαχους, οι οποίοι αντιλήφθηκαν ότι λόγω της ιδιομορφίας του δεν θα υφίστατο τον ζυγό του κρατικού ελέγχου, εάν το χρησιμοποιούσαν. Το Bitcoin διακόπτει το σύστημα πληρωμών, επιτρέπει να προσεγγιστεί η έννοια των μη τραπεζικών λογαριασμών, σχεδόν εξαφανίζει τον ρόλο του έμπιστου τρίτου και μεταμορφώνει τον τρόπο λειτουργίας του χρηματοοικονομικού κόσμου. Ωστόσο, δέκα χρόνια μετά την πρώτη εμφάνισή τους, τα κρυπτονομίσματα εξακολουθούν να αντιμετωπίζονται με καχυποψία, λόγω του σκοτεινού παρελθόντος που απέκτησαν εν τη γενέσει τους στο Dark web και της εγκληματικής χρήσης τους. Είναι αναμφισβήτητο ότι όσο υπάρχει η δυνατότητα να εξορύσσονται νομίσματα, τόσο οι κυβερνοεγκληματίες θα κάνουν αισθητή την παρουσία τους και θα βρίσκουν τρόπους να αποκτήσουν πρόσβαση και να αξιοποιούν τα συστήματα των χρηστών προς όφελός τους. Το BTC δημιουργεί ψηφιακά περιουσιακά στοιχεία που έχουν εγγενή αξία, είναι εξαιρετικά ευάλωτα παρά τις αρκετές δεκαετίες έρευνας και εξελίξεων στην ασφάλεια των πληροφοριών και μπορεί να κλαπούν και να σταλούν προς νέους ιδιοκτήτες άμεσα και αμετάκλητα. Αυτό είναι κάτι που αποτελεί τεράστιο κίνητρο για κυβερνοεγκληματίες καθώς καθιστά το έργο τους πιο εύκολα υλοποιήσιμο. Στις μέρες μας κυκλοφορούν πάρα πολλά είδη κρυπτονομισμάτων και στο άμεσο μέλλον τα παραδοσιακά νομισματικά συστήματα θα αναγκαστούν αν όχι να υιοθετήσουν, τουλάχιστον να συμβιώσουν με τα ψηφιακά νομίσματα.

Μέσα σε αυτό το περιβάλλον της απόλυτης τεχνολογικής καινοτομίας, πρέπει να ληφθούν νομοθετικά μέτρα, που θα αναγνωρίζουν τις ιδιαιτερότητες και τις λειτουργίες των κρυπτονομισμάτων και που θα στοχεύουν στην αποτελεσματική προστασία όσων τα χρησιμοποιούν. Οι εθνικοί νομοθέτες, τα δικαστήρια και οι επιμέρους διοικητικές εθνικές και υπερεθνικές αρχές θα πρέπει να βρίσκονται σε εγρήγορση, για να αντιμετωπίσουν τις νέες προκλήσεις και να εξετάσουν την εφαρμογή ενός αυτόνομου νομοθετικού πλαισίου. Η δημιουργία τέτοιων συνθηκών, που θα εξασφαλίσουν την εφαρμογή νόμιμων και ασφαλών σχέσεων με κρυπτονομίσματα, μπορεί να επιτευχθεί μόνο μέσω προοδευτικών δικαιοδοσιών και κρατικών κανονισμών. Με τον τρόπο αυτό οι μελλοντικοί χρήστες της

τεχνολογίας θα αισθανθούν ασφάλεια, θα μειωθούν οι νομικοί κίνδυνοι που συνεπάγεται η χρήση των κρυπτονομισμάτων και αυτά θα μπορέσουν να γίνουν ευρύτερα αποδεκτά[274].

Δυο πιθανές προσεγγίσεις μπορεί να λάβει η νομική φύση των κρυπτονομισμάτων. Η μία είναι να υπαχθούν σε κάποια κατηγορία, για την οποία υφίσταται νομοθεσία, με την εισαγωγή συγκεκριμένων ρυθμίσεων που θα συμπεριλάβουν τα κρυπτονομίσματα ως μια ακόμα παραλλαγή του συγκεκριμένου αντικειμένου. Η άλλη προσέγγιση είναι τα κρυπτονομίσματα να αναγνωριστούν ως ένα νέο αντικείμενο που εισάγεται στην έννομη τάξη και για το οποίο εξαρχής θα πρέπει να δημιουργηθούν κανόνες και νόμοι.

Στην πράξη, τη νομοθετική αντιμετώπιση χαρακτηρίζει η σποραδικότητα, καθώς οι περισσότερες χώρες ρυθμίζουν τις σχέσεις που δημιουργούνται μέσω της χρήσης κρυπτονομισμάτων και τις οριοθετούν, επικεντρώνοντας την προσοχή τους κυρίως σε θέματα αδειοδότησης λειτουργίας, φορολόγησης, νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας. Θα πρέπει ωστόσο να υπάρξει μια πιο συστηματική προσέγγιση που να χαρακτηρίζεται από μια ενιαία νομική άποψη ως προς τον τρόπο με τον οποίο αντιμετωπίζονται τα κρυπτονομίσματα σε κάθε ισχύουσα δικαιοδοσία, καθώς η έλλειψη συναίνεσης όσον αφορά στον τρόπο αντιμετώπισης των κρυπτονομισμάτων, μπορεί να δυσχεράνει την εκτέλεση ορισμένων πράξεων σε διαφορετικές δικαιοδοσίες. Μια ενιαία νομοθετική πρόβλεψη υπό το ευρωπαϊκό πρίσμα θα ήταν πολύ σημαντική αλλά μια παγκόσμια κοινή πολιτική για τα κρυπτονομίσματα θα ήταν ιδανική.

Το Bitcoin αποτελεί τον προπομπό για πιθανή εμφάνιση και σταδιακή καθιέρωση και άλλων νομισμάτων ή νομισματικών συστημάτων, τα οποία θα λειτουργούν αυτοδύναμα και θα αντιμετωπίζουν τα οποιαδήποτε προβλήματά τους με μεθόδους και πρακτικές ήδη γνωστές από την εφαρμογή τους με την χρήση του bitcoin. Χρήζει λοιπόν, επιτακτικής ανάγκης να ενταχθούν στην ευρωπαϊκή νομοθεσία ρυθμίσεις με τη μορφή Κανονισμού, καθώς αυτός δύναται να βρει άμεση εφαρμογή στα κράτη της Ευρωπαϊκής Ένωσης[275].

Στην σύγχρονη ψηφιακή εποχή το μέλλον είναι αβέβαιο και οι εκπλήξεις που μας περιμένουν θα είναι πολλές. Η τεχνολογία που προτάθηκε από τον Satoshi Nakamoto αντιπροσωπεύει μια τόσο σημαντική ανακάλυψη στην επιστήμη των κατανεμημένων

[274] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 223, *Θεοδωράκης, Ν., Καλογεράκης Γ.,* ό.π., σελ. 22, *Παπαδοπούλου, Α.*, ό.π., σελ. 237, *Παρασκευόπουλος-Κόλιας, Χ.*, ό.π., σελ. 503.

[275] Βλ. *Μούζουλας, Σ.*, ό.π., σελ. 1182, *Alekseeva, S.S., Bolotaeva, O.S. et Stepanova, A.A.*, ό.π., σελ. 3, *Gajdek, S., Kozak, S.*, ό.π., σελ. 206, *Nabilou, H.*, ό.π., σελ. 4, Bongcayao, R.J., ό.π., σελ. 14.

υπολογιστικών συστημάτων ώστε δεν μπορούμε να παραβλέψουμε το γεγονός ότι το Blockchain, έχει δυνητικές δυνατότητες πολύ παραπέρα από της απλές πληρωμές. Η ανάπτυξη πλατφορμών Blockchain, όπως είναι το Bitcoin, είναι ακόμα η αρχή, το μικρό κύμα που προηγείται του τεχνολογικού τσουνάμι. Ακόμα βρίσκεται σε πειραματικό στάδιο καθώς οι δυνατότητες που η τεχνολογία αυτή κρύβει δεν έχουν αξιοποιηθεί στο έπακρο. Η απόδειξη εργασίας μπορεί να χρησιμοποιηθεί για την επίτευξη συναίνεσης σε αποκεντρωμένα δίκτυα προκειμένου να αποδείξει την εντιμότητα σε συμβολαιογραφικές υπηρεσίες, έξυπνα συμβόλαια, παγκόσμια συστήματα πληρωμών και εμβασμάτων, αποκεντρωμένες ανταλλαγές, διαδικτυακά τυχερά παιχνίδια, σε εκλογές, μητρώα περιουσιακών στοιχείων, ψηφιακές συμβολαιογραφικές πράξεις, ηλεκτρονική διακυβέρνηση, λογιστική, χρηματοοικονομική, υγειονομική περίθαλψη.

Το Blockchain λοιπόν από μόνο του θεωρείται μια επαναστατική τεχνολογία που έχει τη δυνατότητα να αλλάξει τον κόσμο και να σημειώσει σημαντικές ανακατατάξεις στην κοινωνία. Από πολλούς συγκρίνεται με την επανάσταση που έφερε το Διαδίκτυο και δεν διστάζουν να χαρακτηρίσουν το Blockchain ως την εξέλιξη του διαδικτύου αποτελώντας μια αναδυόμενη και πολλά υποσχόμενη τεχνολογία της νέας οικονομίας που θα παρέχει νέους τρόπους διάθεσης και ελέγχου του περιεχομένου του διαδικτύου, καθώς και εισαγωγή καινοτόμων λύσεων, ανάλογα με την περιοχή ή τον τομέα της εφαρμογής του. Με τη συμβολή του στην επίλυση προβλημάτων ακεραιότητας δεδομένων, στη βελτίωση της διαφάνειας, στην ενίσχυση της ασφάλειας, στην πρόληψη της απάτης και στη δημιουργία εμπιστοσύνης και απορρήτου, οδηγεί σε ένα νέο γύρο τεχνολογικού ανταγωνισμού, με νέες αγορές να ανταγωνίζονται ισάξια τις ήδη υπάρχουσες[276].

[276] Βλ. *Γιαννόπουλος, Α.*, ό.π., σελ. 222, *Θεοδωράκης, Ν., Καλογεράκης Γ.,* ό.π., σελ. 5, 22, *Μάλαμας, Φ.*, ό.π., σελ. 195-196, *Παπαδοπούλου, Α.*, ό.π., σελ. 211, *Antonopoulos, A.*, ό.π., σελ..4, 155, *Kuo Chuen, D. L., Pak Nian, L.*, ό.π., σελ. 13, *Suman*, ό.π., σελ. 3, *Chytis, E., Kitsantas, T. and Vazakidis, A.*, ό.π., σελ. 10,12.

Βιβλιογραφία

Β.1 Βιβλία

Β.1.1 Ελληνικά

Βλαχόπουλος, Κ., 2007. *ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ: ΜΟΡΦΕΣ - ΠΡΟΛΗΨΗ – ΑΝΤΙΜΕΤΩΠΙΣΗ.* Αθήνα: Νομική Βιβλιοθήκη.

Γεωργιάδης, Γ., 2003. *Η σύναψη της σύμβασης μέσω του διαδικτύου*. Αθήνα: Α. Σάκκουλας.

Δαλακούρας, Θ., 2019. *Ηλεκτρονικό Έγκλημα.* Αθήνα: Νομική Βιβλιοθήκη.

Δελούκα-Ιγγλέση, Κ., 2005. *Νομικά θέματα ηλεκτρονικού εμπορίου.* Αθήνα: Α. Σάκκουλας.

Ιγγλεζάκης, Ι., 2008. *Δίκαιο της Πληροφορικής*, Β΄ έκδ.. Αθήνα–Θεσσαλονίκη: Α. Σάκκουλας.

Καλαμίτσης, Σ., 1995. *Ξένο νόμισμα [συνάλλαγμα] και [ελληνικό] δίκαιο*. Αθήνα: Αφοί Π. Σάκκουλα.

Καλλιμόπουλος, Γ., 1993. *Το δίκαιο του χρήματος*. Αθήνα-Κομοτηνή: Α. Σάκκουλας.

Καραδημητρίου, Κ., 2006. *Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο*. Αθήνα–Θεσσαλονίκη: Εκδ. Σάκκουλα.

Καράκωστας, Ι., 2009. *Δίκαιο & Internet: Νομικά ζητήματα του Διαδικτύου.* Αθήνα: Π. Σάκκουλας.

Μάλαμας, Φ., 2019. *Σύγχρονες φορολογικές πρακτικές της ψηφιακής οικονομίας.* Αθήνα: Νομική Βιβλιοθήκη.

Μαλλέρου, Α., 2007. *Το δίκαιο του ηλεκτρονικού χρήματος*. Αθήνα: Νομική Βιβλιοθήκη.

Μεταξάκης, Ε., 2017. *Μπίτκοϊν (bitcoin), κρυπτοχρήμα και κυβερνοέγκλημα.* Αθήνα: Α. Σάκκουλας.

Μυλωνόπουλος, Χ., 2005. *Ποινικό Δίκαιο-Ειδικό μέρος: Τα εγκλήματα σχετικά με τα υπομνήματα (Άρθρ. 216-223 ΠΚ)*. Αθήνα: Π. Σάκκουλας.

Παπαρσενίου, Π., 2020. *Χρηματική ενοχή: ιδίως σε ξένο νόμισμα*. Αθήνα: Π. Σάκκουλας.

Σιδηρόπουλος, Θ., 2008. *Το Δίκαιο του Διαδικτύου*, Β΄ έκδ.. Αθήνα–Θεσσαλονίκη: Α. Σάκκουλας.

Σταθόπουλος, Μ., 2004. *Επιτομή Γενικού Ενοχικού Δικαίου*, 4η έκδ.. Αθήνα: ΕΚΔΟΣΕΙΣ ΣΑΚΚΟΥΛΑ.

DeMartino, I., 2017. *Bitcoin: Ο Απόλυτος Οδηγός.* μετάφραση Κ. Μπουλούκου, Αθήνα: Φανταστικός Κόσμος. (το πρωτότυπο έργο εκδόθηκε 2016).

Β.1.2 Ξενόγλωσσα

Antonopoulos, A., 2015. *Mastering Bitcoin: Unlocking Digital Crypto-Currencies.* Sebastopol, California: O'Reilly.

Swan, M., 2015. *Blockchain: Blueprint for a New Economy.* Sebastopol, California: O'Reilly.

Β.1.3 Κεφάλαια σε βιβλία

Kuo Chuen, D. L., Pak Nian, L., 2015.Introduction to Bitcoin [online]. *In*: Kuo Chuen, D. L. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data.* 1st Ed. 2015, p.p. 5-30. UK: Esevier Inc. Available at: https://www.researchgate.net/publication/285601622_Introduction_to_Bitcoin (Accessed 26/01/2021).

Cavin, C., Chiriaeva, M. & Poskriakov, F., 2019. Cryptocurrency compliance and risks: A European KYC/ AML perspective [online]. In: *Blockchain & Cryptocurrency Regulation.* 1st Ed. 2019, p.p. 163-174. Global Legal Group Ltd, London. Available at: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf (Accessed 06/06/2021).

Brown, C., Gitlitz, M. A. & Greene, C., 2021. An introduction to virtual currency money transmission regulation [online]. In: *Blockchain & Cryptocurrency Regulation.* 3st Ed. 2021, p.p. 93-110. Global Legal Group Ltd, London. Available at: https://www.acc.com/sites/default/files/resources/upload/GLI-BLCH21_E-Edition.pdf (Accessed 06/06/2021).

Β.2 Έντυπα περιοδικά

Αρχοντάκη, Α., Simsive, P., 2014. Οι νέες μορφές του ψηφιακού χρήματος στην Ελλάδα: Η περίπτωση του Bitcoin. *Εφαρμογές Αστικού Δικαίου & Αστικού Δικονομικού Δικαίου,* 7(10-11), σελ.. 832-840.

Γιαννόπουλος, Α., 2019. Νομικά θέματα σχετικά με την εφαρμογή της τεχνολογίας Blockchain στον τομέα της ηλεκτρικής ενέργειας. *Περιβάλλον και Δίκαιο*, 23(2), σελ. 219-231.

Θεοδωράκης, Ν., Καλογεράκης Γ., 2019. Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα : ιδίως, οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου. *Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας*, 16(1), σελ. 5-22.

Καζαζάκης, Θ., 2015. "Bitcoin": Νομική θεώρηση ενός αρρύθμιστου ψηφιακού νομίσματος. *Ελληνική Δικαιοσύνη.* 4/2015, σελ 1-13.

Κεχαγιά, Χ., 2018. Η αγορά και πώληση "bitcoin" συνιστά φορολογητέα πράξη;: μια δύσκολη απάντηση σε μια πρόκληση της εποχής μας. *Δελτίο Φορολογικής Νομοθεσίας*, 72(1618), σελ. 3-5.

Μούζουλας, Σ., 2017. Επενδυτικά κεφάλαια εικονικού νομίσματος. *Δίκαιο Επιχειρήσεων και Εταιριών*, 24(10), σελ. 1181-1187.

Παπαδοπούλου, Α., 2018. Blockchain: Η τεχνολογία που υπόσχεται «ψηφιακή ασφάλεια»: πιθανές εφαρμογές και συνέπειες για το δίκαιο πνευματικής ιδιοκτησίας και ιδίως στο ζήτημα της ψηφιακής ανάλωσης. *Επισκόπηση Εμπορικού Δικαίου*, 24(2), σελ. 211-237.

Ντότσιας, Σ., 2018. Ο λογιστικός λαβύρινθος των ψηφιακών νομισμάτων. *Επιχείρηση,* 12(141), σελ. 323-326.

Β.3 Συνέδρια

Β.3.1 Εισηγήσεις σε Πρακτικά Συνεδρίων

Ζημιανίτης, Δ., 2012. *Η τεχνολογία ως το περιβάλλον εκδήλωσης και ανάδειξης συμπεριφορών ως εγκληματικών: ηλεκτρονικό έγκλημα, διαδικτυακό έγκλημα, παθόντες, έννομα αγαθά και δυνατότητα αντίδρασης.* Πρακτικά Συνεδρίου με θέμα: Το Δίκαιο στην ψηφιακή εποχή: Προστασία προσωπικότητας- Σύγχρονες μορφές εγκλήματος - Ηλεκτρονικό επιχειρείν, από το 3ο Πανελλήνιο Συνέδριο e-Θέμις που διεξήχθη στο Βόλο 9-12 Μαρτίου 2012 . Φορέας διεξαγωγής: Ένωση Ελλήνων Νομικών e-Θέμις. Αθήνα: Νομική Βιβλιοθήκη. σελ. 162.

Μανιώτης, Δ, 2004. *Ζητήματα από την ηλεκτρονική κατάρτιση των δικαιοπραξιών.* Πρακτικά Συνεδρίου με θέμα: Ψηφιακή τεχνολογία και Δίκαιο. Φορέας διεξαγωγής και συγγραφέας: Εταιρεία Νομικών Βορείου Ελλάδος 52. Αθήνα: ΕΚΔΟΣΕΙΣ ΣΑΚΚΟΥΛΑΣ.

Παρασκευόπουλος-Κόλιας, Χ., 2015. *Κρυπτονομίσματα (digital-currencies) υπό το φως του εποπτικού δικαίου της χρηματαγοράς.* Πρακτικά Συνεδρίου από το 24ο Πανελλήνιο Συνέδριο Εμπορικού Δικαίου που διεξήχθη στα Ιωάννινα 17-19 Οκτωβρίου 2014. Φορέας διεξαγωγής: Σύνδεσμος Ελλήνων Εμπορικολόγων. Αθήνα: Νομική Βιβλιοθήκη. σελ.497-505.

Χρυσοχού, Χ., 2018. *Πιστωτικά Ιδρύματα: Νομικές & Θεσμικές Όψεις.* Πρακτικά Συνεδρίου από το 7ο Πανελλήνιο Συνέδριο e-ΘΕΜΙΣ που διεξήχθη στη Θεσσαλονίκη 25-26 Μαρτίου 2016. Φορέας διεξαγωγής: Ένωση Ελλήνων Νομικών. Αθήνα: Νομική Βιβλιοθήκη.

Abhishta, A, Dragomiretskiy, S., Joosten, R. & Nieuwenhuis, B., 2019. *Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange* [online]. 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, 13-15 February 2019, at Pavia, Italy. Available at: https://www.researchgate.net/publication/331955109_Impact_of_Successful_DDoS_Attacks_on_a_Major_Crypto-Currency_Exchange (Accessed 26/05/2021).

Bistarelli, S., Mantilacci, M., Santancini, P. & Santini, F., 2017 . *An End-to-end Voting-system Based on Bitcoin* [online]. Proceedings of the Symposium on Applied Computing. April 2017. p.p 1836–1841. Available at: http://dx.doi.org/10.1145/3019612.3019841 (Accessed 26/05/2021).

Chandel, S., AA et al. 2020. *A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption* [online]. Future of Information and Communication Conference (FICC) 14-15 March 2019, San Francisco, USA. *In*: Arai, K., Bhatia, R. *Advances in Information and Communication.* p.p. 988-1003. Available at: http://dx.doi.org/10.1007/978-3-030-12385-7_67 (Accessed 26/01/2021).

Chytis, E., Kitsantas, T. and Vazakidis, A., 2019. *A Review of Blockchain Technology and Its Applications in the Business Environment* [online]. International Conference on Enterprise, Systems, Accounting, Logistics & Management. July 2019. Chania, Crete, Greece. Available at: https://www.researchgate.net/publication/334615432_A_Review_of_Blockchain_Technology_and_Its_Applications_in_the_Business_Environment (Accessed 28/01/2021).

Eyal, I., Sirer, E. G., 2013. *Majority Is Not Enough: Bitcoin Mining Is Vulnerable* [online]. International Conference on Financial Cryptography and Data Security. 15 November 2013. Available at: https://www.researchgate.net/publication/258224002_Majority_Is_Not_Enough_Bitcoin_Mining_Is_Vulnerable (Accessed 28/01/2021).

Ghimire, H., Selvaraj, H., 2018. *A Survey on Bitcoin Cryptocurrency and its Mining* [online]. 26th International Conference on Systems Engineering. 18-20 December 2018, Sydney, Australia. 02 February 2019. Available at: https://www.researchgate.net/publication/331040157_A_Survey_on_Bitcoin_Cryptocurrency_and_its_Mining (Accessed 26/01/2021).

Jokić, S., AA et al. 2019. *Comparative analysis of cryptocurrency wallets vs traditional wallets* [online]. 5th International Conference Sinteza 2018. Belgrade, Serbia. 20 April 2018. *Ekonomika.* Vol 65(3), p.p. 65-75. Available at: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo (Accessed 28/01/2021).

Imtiaz, M. A., Starobinski, D. et Trachtenberg, A., 2020. *Characterizing Orphan Transactions in the Bitcoin Network* [online]. IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2020. Toronto, ON, Canada. 2-6 May 2020. Available at: https://www.researchgate.net/publication/343704211_Characterizing_Orphan_Transactions_in_the_Bitcoin_Network (Accessed 28/01/2021).

Sándor, B., Fehér, D.J., 2019. *Examining the Relationship between the Bitcoin and Cybercrime* [online]. IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara, Romania. 29-31 May 2019. Available at: https://doi.org/10.1109/SACI46893.2019.9111568 (Accessed 25/01/2021).

Vallois, V., Guenane, F., 2017. *Bitcoin transaction: From the creation to validation, a protocol overview* [online]. 1st Cyber Security in Networking Conference 2017. Brazil. Oct. 18-20 October 2017. Available at: https://www.researchgate.net/publication/322201810_Bitcoin_transaction_From_the_creation_to_validation_a_protocol_overview (Accessed 28/01/2021).

Β.4 Άρθρα

Β.4.1 Σε Εφημερίδες Ηλεκτρονικές

Γανιάρης, Ν., Η αξιόποινη εξόρυξη κρυπτονομισμάτων Bitcoin. *The Art of Crime* [online]. ΝΟΕΜΒΡΙΟΣ 2018. Ανακτήθηκε από: https://bit.ly/3vgjumC (Πρόσβαση 02/06/2021).

Adler, D., 2018. Silk Road: The Dark Side of Cryptocurrency. *FORDHAM JOURNAL OF CORPORATE & FINANCIAL LAW* [online]. February 21, 2018. Available at: https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/

Agrawal, G., 2020. Cryptocurrency Money Laundering Explained. *Bitquery* [online]. August 6, 2020. Available at: https://bitquery.io/blog/cryptocurrency-money-laundering#Placement (Accessed 27/04/2021).

Gao, Y., AA et al. 2018. A Secure Cryptocurrency Scheme based on Post-Quantum Blockchain. *IEEE Access* [online]. 18 April. Available at: https://bit.ly/3iAu9pp (Accessed 26/01/2021).

Laptev, D., 2017. Bitcoin: transactions, malleability, SegWit and scaling. *Medium* [online]. Aug. 24, 2017. Available at: https://medium.com/lightningto-me/bitcoin-transactions-malleability-segwit-and-scaling-258af8ed9cbf (Accessed 06/06/2021).

SAKS-MCLEOD, A., 2014. Trenton Shavers' Bitcoin Ponzi scheme lands him with $40 million fine from federal judge in Texas. *LeapRate.com* [online]. September 19, 2014. Available at: https://www.leaprate.com/news/trenton-shavers-bitcoin-ponzi-scheme-lands-him-with-40-million-fine-from-federal-judge-in-texas/ (Accessed 26/05/2021).

Yi-Cheng, C., Yueh-Peng, C. and Yung-Chen, C. 2019. An Image Authentication Scheme Using Merkle Tree Mechanisms. *Future Internet* [online]. 6 July. Available at: https://www.researchgate.net/publication/334291891_An_Image_Authentication_Scheme_Using_Merkle_Tree_Mechanisms (Accessed 26/01/2021).

Β.4.2 Σε Περιοδικά Ηλεκτρονικά

Alekseeva, S.S., Bolotaeva, O.S. et Stepanova, A.A., 2019. The Legal Nature of Cryptocurrency. *IOP Conference Series: Earth and Environmental Science* [online]. Vol 272(3), p. 5. June 2019. Available at: https://iopscience.iop.org/article/10.1088/1755-1315/272/3/032166/meta (Accessed 27/01/2021).

Belotti, M., AA et al., 2019. A Vademecum on Blockchain Technologies: When, Which and How. *IEEE Communications Surveys & Tutorials* [online]. Vol 21(4). 12 July. Available at: https://www.researchgate.net/publication/334434726_A_Vademecum_on_Blockchain_Technologies_When_Which_and_How (Accessed 27/01/2021).

Connolly, L., Wall, D., 2019. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security* [online]. Vol 87. Available at: https://www.sciencedirect.com/science/article/pii/S0167404819301336 (Accessed 28/01/2021).

Covolo, V., 2019. The EU Response to Criminal Misuse of Cryptocurrencies: The young, already outdated 5th Anti-Money Laundering Directive1. *European Journal of Crime, Criminal Law and Criminal Justice*[online]. Vol 28(3). 29 Sept.2020. Available at: https://doi.org/10.1163/15718174-bja10003 (Accessed 28/05/2021).

Cvetkova I. 2018. Cryptocurrencies legal regulation. *BRICS Law Journal* [online]. Vol 5 (2), p.p. 128-153. Available at: https://doi.org/10.21684/2412-2343-2018-5-2-128-153 (Accessed 29/01/2021).

Dupont, B., Haslhofer, B.,et Paquet/Clouston, M., 2019. Ransomware payments in the Bitcoin ecosystem. *JOURNAL OF CYBERSECURITY* [online]. Vol. 5 (1), p. 11. Available at: https://academic.oup.com/cybersecurity/article/5/1/tyz003/5488907 (Accessed 15/01/2021).

Dykyi, O., Dyntu, V., 2019. CRYPTOCURRENCY IN THE SYSTEM OF MONEY LAUNDERING. *Baltic Journal of Economic Studies.* [online]. Vol. 4 (5), p.p. 75-81. Available at: https://www.researchgate.net/publication/331092947_CRYPTOCURRENCY_IN_THE_SYSTEM_OF_MONEY_LAUNDERING (Accessed 15/04/2021).

Feder, A., Gandal, N., Hamrick, J. T. & Moore, T., 2017. The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. *Journal of Cybersecurity* [online]. Vol. 3(2), p.p. 137–144. June 2017. Available at: https://www.researchgate.net/publication/322840689_The_impact_of_DDoS_and_other_security_shocks_on_Bitcoin_currency_exchanges_Evidence_from_Mt_Gox (Accessed 28/05/2021).

Ferrer-Gomila, J., AA et al. 2019. A fair contract signing protocol with blockchain support. *Electronic Commerce Research and Applications* [online]. Vol 36, July–August 2019. Available at: https://www.sciencedirect.com/science/article/pii/S1567422319300468 (Accessed 27/01/2021).

Gajdek, S., Kozak, S., 2019. Bitcoin as an Electronic Payment Tool. *Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Seria: Administracja i Zarządzanie* [online]. Vol 47(120). August. Available at: https://www.researchgate.net/publication/338627957_Bitcoin_as_an_Electronic_Payment_Tool (Accessed 27/02/2021).

Fromberger, M., Haffke, L. & Zimmermann, P., 2019. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them. *Journal of Banking Regulation* [online]. Vol. 21, p.p. 125–138 https://doi.org/10.1057/s41261-019-00101-4 (Accessed 07/06/2021).

Higbee, A., 2018. The role of crypto-currency in cybercrime. *Computer Fraud & Security* [online]. Vol 2018 (7), p.p. 13-15. July 2018. Available at: https://doi.org/10.1016/S1361-3723(18)30064-2 (Accessed 27/01/2021).

Kochkarov, A., Kochkarov, R. et Osipovich, S., 2020. Analysis of DDoS Attacks on Bitcoin Cryptocurrency Payment System. *Revista ESPACIOS* [online]. Vol. 41 (03), p. 29. Available at: http://www.revistaespacios.com/a20v41n03/a20v41n03p29.pdf (Accessed 29/03/2021).

Moore, D., Rid, T., 2016. Cryptopolitik and the Darknet. *Survival* [online]. Vol 58(1), p.p. 7-38. Available at: https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true& (Accessed 27/04/2021).

Nabilou, H., 2019. How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency. *International Journal of Law and Information Technology* [online]. Vol 27(3), p.p. 266-291. Available at: DOI:10.2139/ssrn.3360319 (Accessed 26/02/2021).

Oerlemans, J., J., van Deventer, O. et van Wegberg, R., 2018. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime* [online]. Vol 25(1), p.p. 419-435. Available at: https://www.researchgate.net/publication/323630331_Bitcoin_money_laundering_mixed_results_An_explorative_study_on_money_laundering_of_cybercrime_proceeds_using_bitcoin (Accessed 24/05/2021).

Reddy, E., Minnaar, A., 2018. Cryptocurrency: a tool and target for cybercrime. *Acta Criminologica: Southern African Journal of Criminology* [online]. Vol 31(3), p.p.71-92. Available at: https://www.researchgate.net/publication/338572871_CRYPTOCURRENCY_A_TOOL_AND_TARGET_FOR_CYBERCRIME (Accessed 27/04/2021).

Reed, M., Syverson, P., Onion Routing. *AIPA 99 Theme Relevance: Tools and Technologies for Intelligence Community Analysts* [online]. Available at: https://www.onion-router.net/Publications/AIPA-1999.pdf (Accessed 27/02/2021).

Stearns, B., 2019. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review* [online]. Vol 34(6), p.p. 1180-1196. Available at: https://www.sciencedirect.com/science/article/abs/pii/S026736491830308X# (Accessed 24/02/2021).

Theodorakis, N., 2018. The Use of Cryptocurrencies for Illicit Activities and Relevant Legislative Initiatives. *The Art of Crime* [online]. Vol 2018(5), p.p.71-92. Available at: https://theartofcrime.gr/the-use-of-cryptocurrencies-for-illicit-activities-and-relevant-legislative-initiatives/ (Accessed 24/03/2021).

B.4.3 Σε Ιστοσελίδες

Γεωργούλας, Λ., *Τα είδη των ρομπότ του διαδικτύου που επισκέπτονται τον ιστότοπο μας και πως να τα μπλοκάρεις.* Ανακτήθηκε από: https://nextnet.gr/040-ta-eidh-tvn-rompot-toy-diadiktyoy-poy-episkeptontai-ton-istotopo-mas-kai-pvs-na-ta-mplokareis.php (Πρόσβαση 22/04/2021).

Παρασκευόπουλος-Κόλιας, Χ., 2014. *Οικονομικές τεχνικές και Νομικές όψεις του Bitcoin.* Ανακτήθηκε από: https://www.yiannatsis.gr/download/bitcoin%20gr.pdf (Πρόσβαση 22/04/2021).

Andreas, K., 2021. *Tor έναντι VPN – Ποιο Είναι Πιο Ασφαλές.* Available at: https://bit.ly/3hRg72t (Accessed 20/04/2021).

Annison, T., 2018. *Bloom Filters and SPV nodes within the bitcoin blockchain.* Available at: https://tara-annison.medium.com/bloom-filters-and-spv-nodes-within-the-bitcoin-blockchain-66c36ea673f2 (Accessed 21/02/2021).

Barone, D.M., 2019. *Suspicious crowdfunding campaigns in bitcoin and their exploitation of exchange services.* Available at: https://www.itstime.it/w/suspicious-crowdfunding-campaigns-in-bitcoin-and-their-exploitation-of-exchange-services-by-daniele-maria-barone/ (Accessed 21/05/2021).

Bissias, G., AA et al. 2016. *An Analysis of Attacks on Blockchain Consensus (DRAFT).* Available at: https://www.researchgate.net/publication/309424665_An_Analysis_of_Attacks_on_Blockchain_Consensus (Accessed 22/02/2021).

Bongcayao, R.J., *29-DOLES SILVA-Cryptocurrencies and International Regulation.* Available at: https://www.scribd.com/document/464467969/29-DOLES-SILVA-Cryptocurrencies-and-International-Regulation (Accessed 23/02/2021).

Casadei-Bernardi, S., 2019. *Terrorist Use of Cryptocurrencies: A Blockchain Compliance White Paper.* Available at: https://www.blockchainconsultus.io/wp-content/uploads/2019/08/3191-BCU-Crypto-Terrorist.pdf (Accessed 27/05/2021).

Chaum, D., 1981. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* Available at: https://www.cs.utexas.edu/~shmat/courses/cs395t_fall04/chaum81.pdf (Accessed 27/01/2021).

Columbus, L., *How To Deal With Ransomware In A Zero Trust World.* Available at: https://www.forbes.com/sites/louiscolumbus/2019/07/30/how-to-deal-with-ransomware-in-a-zero-trust-world/?sh=6e10fee720e5 (Accessed 08/06/2021).

Cosset, D., 2017. *Blockchain: what is in a block?* Available at: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo (Accessed 28/01/2021).

Costello, A., 2020. *The history of first cryptocurrencies before Bitcoin.* Available at: https://medium.com/hashmart-blog/the-history-of-first-cryptocurrencies-before-bitcoin-6eccebca152a (Accessed 27/01/2021).

Davis, P., 2020. *To Avoid Ponzi Schemes, Exercise Due Diligence When Investing.* Available at: https://www.businessknowhow.com/security/ponzi.htm (Accessed 27/05/2021).

Drozhzhin, A., 2018. *Phishing for cryptocurrencies: How bitcoins are stolen.* Available at: https://www.kaspersky.com/blog/crypto-phishing/20765/ (Accessed 10/01/2021).

D'Souza, D., 2020. *Twitter Shares Fall After Hackers Pull Off Bitcoin Scam.* Available at: https://www.investopedia.com/twitter-shares-fall-after-hackers-pull-off-bitcoin-scam-5071449 (Accessed 06/06/2021).

Frankenfield, J., 2019. *51% Attack.* Available at: https://www.investopedia.com/terms/1/51-attack.asp (Accessed 27/01/2021).

Frankenfield, J., 2021. *Silk Road (Website).*. Available at: https://www.investopedia.com/terms/s/silk-road.asp (Accessed 27/05/2021).

Freel, J., Howard II, B. 2019. Do Bitcoin ATMs Make Money Laundering too Easy? Regulators Try to Keep up with Emerging Cryptocurrency Trend. *LEXOLOGY*. Available at: https://www.velaw.com/insights/do-bitcoin-atms-make-money-laundering-too-easy-regulators-try-to-keep-up-with-emerging-cryptocurrency-trend/ (Accessed 27/05/2021).

Fyookball, J., 2017. *Why Every Bitcoin User Should Understand "SPV Security"*. Available at https://medium.com/@jonaldfyookball/why-every-bitcoin-user-should-understand-spv-security-520d1d45e0b9 (Accessed 27/02/2021).

Griffith, K., 2014. *A Quick History Of Cryptocurrencies BBTC - Before Bitcoin*. Available at: https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630 (Accessed 27/01/2021).

Haslhofer, B., Judmayer, A., Romiti, M. & Zamyatin, A., 2019. *A Deep Dive into Bitcoin Mining Pools.* Available at: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_30.pdf (Accessed 03/06/2021).

Hoete-Dodd, V., 2019. *How Are Regulators Fighting the use of Cryptocurrencies in Money Laundering at Casinos?*. Available at: https://www.bitprime.co.nz/blog/regulators-fighting-cryptocurrencies-money-laundering-casinos/ (Accessed 23/03/2021).

Holman, D., Stettner, B., 2018. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches.* Available at: file:///C:/Users/zarch/Downloads/AML18_AllenOvery.pdf (Accessed 27/03/2021).

Jacobs, I., 2004. *Architecture of the World Wide Web, Volume One.* Available at: https://www.w3.org/TR/2004/REC-webarch-20041215/ (Accessed 27/05/2021).

Kadar, T., 2020. *How are crypto and blockchain being utilised in the gaming sector?.* Available at: https://www.finextra.com/blogposting/19885/how-are-crypto-and-blockchain-being-utilised-in-the-gaming-sector (Accessed 22/03/2021).

Liebkind, J., 2020. *Beware of These Five Bitcoin Scams.* Available at: https://www.investopedia.com/articles/forex/042315/beware-these-five-bitcoin-scams.asp (Accessed 27/01/2021).

Matetic, S., AA et al. 2019. *BITE: Bitcoin Lightweight Client Privacy using Trusted Execution.* Available at: https://www.usenix.org/system/files/sec19fall_matetic_prepub.pdf (Accessed 27/01/2021).

Miggiani, K., 2020. *AMLD 5 and the EU May 2020 AML/CFT Action Plan – where do crypto assets fit into the emerging landscape?.* Available at: https://regulation-y.com/2020/06/14/amld-5-and-the-eu-may-2020-aml-cft-action-plan-where-do-crypto-assets-fit-into-the-emerging-landscape/ (Accessed 07/06/2021).

Nakamoto, S., 2009. *A Peer-to-Peer Electronic Cash System.* Available at: https://bitcoin.org/bitcoin.pdf (Accessed 26/01/2021).

Pérez-Solà, S., AA et al. 2019. *Another coin bites the dust: an analysis of dust in UTXO-based cryptocurrencies*. Available at: https://royalsocietypublishing.org/doi/10.1098/rsos.180817 (Accessed 26/01/2021).

Perry, M., 2019. *Bitcoin ATMs a "Hole" in EU Anti-Money Laundering Rules*. Available at: https://www.occrp.org/en/daily/10200-bitcoin-atms-a-hole-in-eu-anti-money-laundering-rules (Accessed 26/05/2021).

Reiff, N., 2019. *Were There Cryptocurrencies Before Bitcoin?* Available at: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/ (Accessed 27/01/2021).

Schwartz, M., 2018. *Hacked Mt. Gox Bitcoin Exchange Chief Maintains Innocence.* Available at: https://www.bankinfosecurity.com/hacked-mt-gox-bitcoin-exchange-chief-maintains-innocence-a-11904 (Accessed 10/05/2021).

Slim, T., 2021. *Πώς να αποκτήσετε πρόσβαση στο Dark Web: Οδηγός για την περιήγηση στο Dark Web χρησιμοποιώντας το TOR Browser.* Available at: https://www.webhostingsecretrevealed.net/el/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/ (Accessed 27/04/2021).

Stone, J., 2021. *Ransomware hackers launder bitcoin through just a handful of locations, researchers find.* Available at: https://www.cyberscoop.com/ransomware-hack-bitcoin-money-laundering-chainalysis/ (Accessed 29/01/2021).

Surowiecki J., 2012. *A brief history of money*. Available at: https://www.researchgate.net/publication/254059731_A_brief_history_of_money (Accessed 10/02/2021).

Surowiecki J., 2013. *Why Did Criminals Trust Liberty Reserve?* Available at: https://www.newyorker.com/news/news-desk/why-did-criminals-trust-liberty-reserve (Accessed 10/02/2021).

B.5 Ιστοσελίδες

Bitcoin.org. *Το Bitcoin είναι ένα καινοτόμο δίκτυο πληρωμών και ένα νέο είδος χρημάτων*. Ανακτήθηκε από: https://bitcoin.org/el/ (Πρόσβαση 27/04/2021).

el.wikipedia. *Κοινωνική μηχανική.* Ανακτήθηκε από: https://bit.ly/3izbcDJ (Πρόσβαση 07/06/2021).

EUBlockchain. *Η Ευρωπαϊκή Επιτροπή εγκαινιάζει το παρατηρητήριο - φόρουμ της ΕΕ για την τεχνολογία blockchain.* Ανακτήθηκε από: https://ec.europa.eu/greece/news/20180201_blockchain_el (Πρόσβαση 27/05/2021).

Hellenic.F.I.U. *Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες.* Ανακτήθηκε από: http://www.hellenic-fiu.gr/index.php?lang=el (Πρόσβαση 27/05/2021).

IGURU. *Τι είναι το ο web crawler.* Ανακτήθηκε από: https://iguru.gr/2021/03/02/einai-web-crawler/ (Πρόσβαση 23/05/2021).

Σύστημα σταθερών ισοτιμιών του Μπρέττον Γουντς. *Ο κανόνας του χρυσού.* Ανακτήθηκε από: https://bit.ly/3bOz7uJ (Πρόσβαση 01/03/2021).

Tor. *Σχετικά Με Ιστορία.*. Ανακτήθηκε από: https://www.torproject.org/about/history/ (Πρόσβαση 01/03/2021).

Τράπεζα Νομικών Πληροφοριών ΝΟΜΟΣ-NOMOS. Ανακτήθηκε από: https://lawdb.intrasoftnet.com/

WLEARN-Πρόσβαση στη Γνώση. *Τι είναι το Σκοτεινό Διαδίκτυο (Dark Web) και πως μπορεί κάποιος να αποκτήσει πρόσβαση σε αυτό*. Available at: https://www.wlearn.gr/index.php/articles/1391-what-is-dark-web (Πρόσβαση 03/03/2021).

Bitcoin Wiki. *P2Pool.* Available at: https://en.bitcoin.it/wiki/P2Pool (Accessed 27/01/2021).

Bitorb. *SILK ROAD DAY- WHAT IS THE SILK ROAD MARKETPLACE?.* Available at: https://www.bitorb.com/campus/silk-road-day-what-is-the-silk-road-marketplace/ (Accessed 27/01/2021).

CFI. *Ponzi vs. Pyramid Schemes: Two investment schemes with distinctly different structures and modes of operation.* Available at: https://corporatefinanceinstitute.com/resources/knowledge/other/ponzi-vs-pyramid-schemes/ (Accessed 27/05/2021).

CIS. Center for Internet Security. *Cybersecurity Spotlight - The Surface Web, Dark Web, and Deep Web.* Available at: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web/ (Accessed 23/02/2021).

Ciso platform. *Surface Web vs Deep Web vs Dark Web.* Available at: https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different (Accessed 23/05/2021).

Coding Villa. *What is a DDoS Attack?.* Available at: https://www.codingvilla.in/what-is-a-ddos-attack (Accessed 02/04/2021).

Coindesk. *Computer security firm Dell SecureWorks has managed to identify 146 types of bitcoin malware in the wild.* Available at: https://www.coindesk.com/nearly-150-strains-malware-bitcoins (Accessed 23/03/2021).

Coindesk. *Launched in 2010 Mt. Gox was the world's largest bitcoin exchange until its demise in 2014.* Available at: https://www.coindesk.com/company/mt-gox (Accessed 23/05/2021).

Coindesk. *What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability.* Available at: https://www.coindesk.com/bitcoin-bug-guide-transaction-malleability (Accessed 23/05/2021).

ELLIPTIC. *Bitcoin Money Laundering: How Criminals Use Crypto.* Available at: https://www.elliptic.co/blog/bitcoin-money-laundering (Accessed 23/04/2021).

Emerald PUBLISHING. *Is the Bitcoin frenzy making the world less safe?.* Available at: https://www.emeraldgrouppublishing.com/archived/realworldresearch/world_events/bitcoin-frenzy-making-the-world-less-safe.htm (Accessed 23/04/2021).

Enisa. *Cryptojacking - Cryptomining in the browser.* Available at: https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser (Accessed 03/06/2021).

Enisa. *Cryptojacking: ENISA Threat Landscape.* Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cryptojacking (Accessed 03/06/2021).

EUROPOL. *FINANCIAL INTELLIGENCE UNITS – FIU.NET.* Available at: *https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net* (Accessed 03/06/2021).

Eurospinder: relevancy retrieval. *What is a cryptocurrency mixer?.* Available at: https://www.eurospider.com/en/know-how/compliance/211-what-is-a-cryptocurrency-mixer (Accessed 28/03/2021).

GDPO. *Silk Road and Bitcoin.* Available at: https://www.swansea.ac.uk/media/Silk-Road-and-Bitcoin.pdf (Accessed 23/05/2021).

Getit. *The 2021 Guide to AML and KYC for Crypto Exchanges & Wallets. Available at: https://getid.ee/aml-kyc-crypto-exchanges-wallets/* (Accessed 23/05/2021).

HFW. *A NEW FRONTIER FOR AML REGULATION: THE FIFTH ANTI-MONEY LAUNDERING DIRECTIVE AND CRYPTOCURRENCIES. Available at:* https://www.hfw.com/A-New-Frontier-for-AML-Regulation-Sep-18 (Accessed 05/06/2021).

The New York Times. *How Liberty Reserve's Virtual Currency Works.* Available at: [1] https://nyti.ms/3vK6arS (Accessed 23/05/2021).

Karspersky. *What is Riskware?.* Available at: https://www.kaspersky.com/resource-center/threats/riskware (Accessed 28/05/2021).

KURANT-ATMs. *Bitcoin ATM Map.* Available at: https://coinatmradar.com/ (Accessed 30/05/2021).

KYC-CHAIN. *Liberty Reserve – The Digital Currency That Laundered Millions.* Available at: https://kyc-chain.com/liberty-reserve-the-digital-currency-that-laundered-millions/ (Accessed 25/04/2021).

Phishing.org. *Phishing and Spoofing.* Available at: https://www.phishing.org/phishing-and-spoofing (Accessed 27/04/2021).

SYGNA. *A Guide to the EU's 5th Anti-Money Laundering Directive (AMLD5).* Available at: https://www.sygna.io/blog/what-is-amld5-anti-money-laundering-directive-five-a-guide/ (Accessed 27/04/2021).

THE US DEPARTMENT of JUSTICE. *Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business.* Available at: https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital (Accessed 07/06/2021).

W3C. *Leading the web to its full potential*. Available at: https://www.w3.org/Help/#webinternet (Accessed 20/05/2021).

W3C. *HELP AND FAQ*. Available at: https://www.w3.org/Help/#webinternet (Accessed 20/05/2021).

Β.6 Μελέτες

Broadhurst, R., AA et al., 2018. *Malware Trends on 'Darknet' Crypto-markets: Research Review*. [online]. Report number: Australian National University Cybercrime Observatory and the Korean Institute of Criminology. Affiliation: Australian National University. Cybercrime O{bservatory. Project: *Monitoring web-browser activity and risks of cybercrime*. Available at: https://www.researchgate.net/publication/326436666_Malware_Trends_on_'Darknet'_Crypto-markets_Research_Review (Accessed 26/01/2021).

EBA. *Opinion on 'virtual currencies'. Available at* *https://service.betterregulation.com/document/159234 (Accessed 03/06/2021).*

European Central Bank. *VIRTUAL CURRENCY SCHEMES.* Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (Accessed 28/05/2021).

European Central Bank. *Virtual currency schemes - a further analysis.* Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (Accessed 08/06/2021).

FATF. *Virtual Currencies Key Definitions and Potential AML/CFT Risks.* Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Accessed 08/06/2021).

HM Treasury. *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf (Accessed 08/06/2021).

Houben, R., Snyers, A., 2018. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. *Policy Department for Economic, Scientific and Quality of Life Policies* [online]. June 2018. Available at: https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (Accessed 26/01/2021).

Sykes, J., Vatanko, N., 2019. Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals. *Congressional Research Service* [online]. R45664, April 3, 2019. Available at: https://fas.org/sgp/crs/misc/R45664.pdf (Accessed 26/01/2021).

U.S. House of Representatives, Subcommittee on Terrorism and Illicit Finance, Committee on Financial Services, Washington, D.C., 2018. *SURVEY OF TERRORIST GROUPS AND THEIR MEANS OF FINANCING* [online]. 31-576 PDF, SEPTEMBER 7, 2018. Available at: https://www.govinfo.gov/content/pkg/CHRG-115hhrg31576/html/CHRG-115hhrg31576.htm (Accessed 26/05/2021).

Β.7 Νομοθεσία

Β.7.1. Νόμοι

Ν. 4021/2011. (ΦΕΚ Α' 218/03-10-2011). *Ενισχυμένα μέτρα εποπτείας και εξυγίανσης των πιστωτικών ιδρυμάτων - Ρύθμιση θεμάτων χρηματοπιστωτικού χαρακτήρα - Κύρωση της Σύμβασης - Πλαίσιο του Ευρωπαϊκού Ταμείου Χρηματοπιστωτικής Σταθερότητας και των τροποποιήσεων της και άλλες διατάξεις.*

Ν.4557/2018. (ΦΕΚ Α' 139/30-07-2018). *Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ενσωμάτωση της Οδηγίας 2015/849/ΕΕ) και άλλες διατάξεις , κωδικοποιημένος με τον 4798/2021.*

Ν. 4727/2020. (ΦΕΚ 184/Α/23-9-2020). *Ψηφιακή Διακυβέρνηση (ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.*

Ν.4734/2020. (ΦΕΚ Α' 196/08-10-2020). *Τροποποίηση του ν. 4557/2018 (Α΄ 139) για την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας (ΕΕ) 2018/843 (L 156) και του άρθρου 3 της Οδηγίας (ΕΕ) 2019/2177 (L 334) και λοιπές διατάξεις.*

Β.7.2. Κανονισμοί Ευρωπαϊκής Ένωσης

Κανονισμός (ΕΚ) αριθ. 428/2009. (05/052009). *Περί κοινοτικού συστήματος ελέγχου των εξαγωγών της μεταφοράς, της μεσιτείας και της διαμετακόμισης ειδών διπλής χρήσης.* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32009R0428 (Πρόσβαση 26/01/2021).

Κανονισμός (ΕΚ) αριθ. 974/98. (03/05/1998). *Για την εισαγωγή του ευρώ*. Ανακτήθηκε από: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1998R0974:20110101:EL:PDF (Πρόσβαση 01/02/2021).

Β.7.3. Οδηγίες Ευρωπαϊκής Ένωσης

Οδηγία 2006/112/ΕΚ, (28/11/2006). *Σχετικά με το κοινό σύστημα φόρου προστιθέμενης αξίας.* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32006L0112 (Πρόσβαση 06/06/2021).

Οδηγία 2009/110/ΕΚ και ΣΕΕ, (16/09/2009). *Για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος, την τροποποίηση των οδηγιών 2005/60/ΕΚ και 2006/48/ΕΚ και την κατάργηση της οδηγίας 2000/46/ΕΚ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* Ανακτήθηκε από: *https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0110&from=EL* (Πρόσβαση 08/06/2021).

Οδηγία 2013/40/ΕΕ, ΕΚ και ΣΕΕ (12/08/2013). *Για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013L0040&from=NL (Πρόσβαση 08/06/2021).

Οδηγία 2015/849/ΕΕ, ΕΚ και ΣΕΕ (20/05/2015). *Σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 2006/70/ΕΚ της Επιτροπής (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015L0849&from=DA (Πρόσβαση 08/06/2021).

Οδηγία 2015/2366/ΕΕ, (25/11/2015). *Σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015L2366&from=EL (Πρόσβαση 26/05/2021).

Οδηγία 2018/843/ΕΕ και ΣΕΕ, (30/05/2018). *Για την τροποποίηση της οδηγίας (ΕΕ) 2015/849 σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, και για την τροποποίηση των οδηγιών 2009/138/ΕΚ και 2013/36/ΕΕ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32018L0843&from=EN (Πρόσβαση 26/05/2021).

Β.8 Νομολογία

Απόφαση ΔΕΕ C-264/14, 2015. Skatteverket v David Hedqvist. *Προδικαστική παραπομπή — Κοινό σύστημα φόρου προστιθέμενης αξίας (ΦΠΑ) — Οδηγία 2006/112/ΕΚ — Άρθρα 2, παράγραφος 1, στοιχείο γ΄, και 135, παράγραφος 1, στοιχεία δ΄ έως στ΄ — Υπηρεσίες παρεχόμενες εξ επαχθούς αιτίας — Συναλλαγές ανταλλαγής εικονικού νομίσματος "bitcoin" με συμβατικά νομίσματα — Απαλλαγή.* Αποφασίσθηκε την 22α Οκτωβρίου 2015. Ανακτήθηκε από: https://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=EL (Πρόσβαση 06/06/2021).

United States Court of Appeals, District of Columbia Circuit, 2008. *UNITED STATES of America, Appellee v. E-GOLD, LTD., et al., Appellants*. No. 07-3074, Decided: April 11, 2008. Available at: https://caselaw.findlaw.com/us-dc-circuit/1465631.html (Accessed 25/01/2021).

United States Court of Appeals For the Second Circuit, 2008. *UNITED STATES of America, Appellee v. ROSS WILLIAM ULBRICHT, a/k/a DREAD PIRATE ROBERTS, a/k/a SILK ROAD, a/k/a SEALED DEFENDANT 1, a/k/a DPR.* No. 15-1815, Decided: May 31, 2017. Available at: https://cases.justia.com/federal/appellate-courts/ca2/15-1815/15-1815-2017-05-31.pdf?ts=1496241010 (Accessed 05/06/2021).

United States District Court EASTERN DISTRICT OF TEXAS SHERMAN DIVISION, 2013. *MEMORANDUM OPINION REGARDING THE COURT'S SUBJECT MATTER JURISDICTION.* Securities and Exchange Commission v. Shavers et al. No. 4:2013cv00416 - Document 23 (E.D. Tex. 2013). Available at: https://law.justia.com/cases/federal/district-courts/texas/txedce/4:2013cv00416/146063/23/ (Accessed 05/06/2021).

United States District Court, 2014. *UNITED STATES of America v. Robert M. FAIELLA, a/k/a "BTCKing," and Charlie Shrem, Defendants.* No. 14–cr–243 (JSR). 2014-08-19. Available at: https://bit.ly/3iaPgyD (Accessed 05/06/2021).

United States Court for the Southern District of New York, 2015. *United States v. Budovsky.* Decided; September 23, 2015, Filed 13cr368 (DLC). Available at: https://bit.ly/2RgU7mR (Accessed 05/06/2021).