Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή

Στην Ασφάλεια Υπολογιστών και Δικτύων

Ζητήματα Ιδιωτικότητας σε Τεχνολογίες Blockchain

Δημήτριος Πουλής

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ζητήματα Ιδιωτικότητας σε Τεχνολογίες Blockchain

Δημήτριος Πουλής (Α.Μ. 11500117)

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2019

Περίληψη

Το Blockchain γίνεται όλο και πιο δημοφιλές στην ψηφιακή εποχή. Παρόλο που οι κριτικοί αμφισβητούν την επεκτασιμότητα, την ασφάλεια και τη βιωσιμότητά του, έχει ήδη αρχίσει να μεταβάλει τον τρόπο ζωής λόγω της επιρροής του σε κλάδους της οικονομίας και επιχειρήσεις. Τα χαρακτηριστικά της τεχνολογίας Blockchain εγγυώνται πιο αξιόπιστες και γρήγορες υπηρεσίες. Είναι σημαντικό όμως, να εξεταστούν τα θέματα ασφάλειας και προστασίας της ιδιωτικής ζωής πίσω από την καινοτόμο αυτή τεχνολογία. Το φάσμα των εφαρμογών του Blockchain είναι ευρύτατο και με ποικίλες χρήσεις. Μελετώντας τα ζητήματα ιδιωτικότητας που προκύπτουν, οδηγούμαστε στη συνεχή βελτίωση του επιπέδου ασφαλείας των εφαρμογών του Blockchain.

Όροι κλειδιά– Blockchain, Ιδιωτικότητα, Ασφάλεια.

Summary

Blockchain is gaining popularity at the digital age. Although critics question its scalability, security and sustainability, it is already transforming the everyday way of life due to its inordinate influence on the financial sector and businesses. The features of Blockchain technology guarantee more reliable and expedient services. Nonetheless, it is important to consider the security and privacy issues behind this innovative technology. The spectrum of Blockchain applications is wide and with multiple uses. Understanding how Blockchain-based applications can provide strong privacy guarantees, leads us to the constant improvement of their security level.

Index Terms– Blockchain, Privacy, Security.

Ευχαριστίες

Ευχαριστώ τον επιβλέπων καθηγητή Κωνσταντίνο Λιμνιώτη για την καθοδήγηση του σε όλα τα στάδια αυτής της διατριβής και τον απόφοιτο Ε.Μ.Π. Οδυσσέα Λαμτζίδη για τη βοήθεια που μου παρείχε.

Περιεχόμενα

Ευρετήριο εικόνων

Ευρετήριο πινάκων

Κεφάλαιο 1

Εισαγωγή

Το Blockchain είναι μια κατανεμημένη βάση στο Διαδίκτυο στην οποία καταγράφονται και αποθηκεύονται κρυπτογραφημένες συναλλαγές μεταξύ των μελών του. Αποτελεί τον ακρογωνιαίο λίθο του Bitcoin και βασίζεται σε μαθηματικούς υπολογισμούς ανώτερου επιπέδου κάτι το οποίο το καθιστά συγκριτικά ισχυρότερο σε σχέση με τις παραδοσιακές μεθόδους συναλλαγών. Πλέον, η χρήση του συναντάται σε ολοένα και περισσότερους τομείς, όπως τον τραπεζικό, το εμπόριο, τον συμβολαιογραφικό, ακόμη και τον καλλιτεχνικό. Βέβαια, δεν λείπουν τα νομικά ζητήματα που προκύπτουν από την ελλιπή σχετική νομοθεσία, με αποτέλεσμα τον διαφορετικό βαθμό αποδοχής και αφομοίωσής του σε διαφορετικά κράτη. Κοινός ωστόσο είναι ο προβληματισμός σχετικά με τη διαχείριση των δεδομένων και των σχετικών προεκτάσεων αναφορικά με την ιδιωτικότητα των χρηστών. Η απουσία κεντρικού ελέγχου των συναλλαγών και η μόνιμη διατήρηση των δεδομένων, που αποτελεί βασικό χαρακτηριστικό της μορφολογίας του, ενδέχεται να αποτελέσουν τροχοπέδη για τη διασφάλιση της ιδιωτικότητας. Ένας επιπλέον προβληματισμός, είναι η χρήση της τεχνολογίας από επιτήδειους με σκοπό την εκμετάλλευση πιθανών κενών ασφαλείας. Το ερώτημα που τίθεται λοιπόν είναι, *ποιο είναι το σημείο ισορροπίας μεταξύ του μέγιστου επιπέδου διασφάλισης της ιδιωτικότητας και της ελαχιστοποίησης της πιθανότητας παραβίασης της μέσω του Blockchain*. Στην παρούσα διατριβή, θα αναλυθούν τα παραπάνω, ενώ θα δοθεί βαρύτητα στις χρήσεις και τα ζητήματα ιδιωτικότητας που ανακύπτουν, στο τρίπτυχο αντιμετώπιση, οφέλη, περιορισμοί. Επιπλέον, θα γίνει διερεύνηση του τρόπου με τον οποίο το πρωτόκολλο Enigma αντιμετωπίζει τα ζητήματα ιδιωτικότητας που χαρακτηρίζουν τις πλατφόρμες Blockchain με ανάλυση και περιγραφή των συστατικών στοιχείων του και της αρχιτεκτονικής του. Τέλος θα περιγραφεί συνοπτικά η υλοποίηση Enigma Catalyst η οποία και αποτελεί την πρώτη ουσιαστική εφαρμογή του πρωτοκόλλου Enigma για την διασφάλιση τη ιδιωτικότητας των δεδομένων.

Κεφάλαιο 2

Τεχνολογία Blockchain και το Bitcoin

2.1 Τι είναι το Blockchain

Το Blockchain είναι ουσιαστικά μια κατανεμημένη βάση δεδομένων των αρχείων ή του δημόσιου ημερολογίου όλων των συναλλαγών ή των ψηφιακών γεγονότων που έχουν εκτελεστεί και μοιραστεί μεταξύ των συμμετεχόντων μερών. Πρόκειται για ένα αποκεντρωμένο «βιβλίο συναλλαγών» το οποίο είναι προσβάσιμο από όλα τα μέρη που το αποδέχονται ως μέσο συναλλαγών και δεν ελέγχεται από κάποιο άτομο, ίδρυμα ή επιχείρηση. Ακριβώς επειδή είναι προσβάσιμο από όλα τα μέρη (με κρυπτογραφημένο τρόπο, ώστε να διασφαλίζεται η ανωνυμία των συναλλασσόμενων, άρα και να αποφεύγεται η μεροληψία) έχει την ιδιότητα να αυτορυθμίζεται αξιοποιώντας μαθηματικά μοντέλα, χωρίς ανθρώπινη παρέμβαση. Κάθε συναλλαγή στο δημόσιο βιβλίο επαληθεύεται με τη συναίνεση της πλειοψηφίας των συμμετεχόντων στο σύστημα και οι πληροφορίες δεν μπορούν να διαγραφούν. [01-03]

Το Blockchain περιέχει ένα συγκεκριμένο και επαληθεύσιμο αρχείο κάθε συναλλαγής που έγινε οποτεδήποτε. Επί της ουσίας, ο συγκεκριμένος κώδικας έχει την ιδιότητα να κάνει από μόνος του την πιο «δίκαιη» μοιρασιά, χωρίς να λαμβάνει υπόψη εξωγενείς παράγοντες. Διπλές εκδόσεις και συναλλαγές μπορούν να αποτραπούν και όλοι μπορούν να χρησιμοποιήσουν αυτήν τη δημόσια αλυσίδα μπλοκ και να δημιουργήσουν μία βάση για το κρυπτοδίκτυο. Πρόκειται για μια πρακτική που, ειδικά στο πεδίο του νομίσματος, βρίσκει σοβαρό αντίλογο σε σχέση με εξωτερικές συνθήκες που καθιστούν επιτακτικές εξωτερικές πολιτικές παρεμβάσεις. Η βασική υπόθεση είναι ότι το Blockchain καθιερώνει ένα σύστημα δημιουργίας κατανεμημένης συναίνεσης στον ψηφιακό κόσμο. Αυτό επιτρέπει στους συμμετέχοντες φορείς να γνωρίζουν με βεβαιότητα ότι συνέβη ένα ψηφιακό γεγονός δημιουργώντας ένα αδιάψευστο αρχείο σε ένα δημόσιο βιβλίο. Ανοίγει την πόρτα για την ανάπτυξη μιας ανοικτής

και κλιμακούμενης ψηφιακής οικονομίας. Υπάρχουν τεράστιες ευκαιρίες σε αυτή τη νέα τεχνολογία. [01-03]

Το Bitcoin, το αποκεντρωμένο ψηφιακό νόμισμα, είναι το πιο δημοφιλές παράδειγμα που είναι εγγενώς συνδεδεμένο με τεχνολογία Blockchain. Το Bitcoin (BTC) είναι μία ψηφιακή μονάδα χρήματος, το οποίο χάρη στην αποκεντρωμένη διαδικασία γένεσης δεν ελέγχεται κρατικά και αποθηκεύεται offline και online σε ένα ψηφιακό πορτοφόλι. Είναι επίσης αμφιλεγόμενο δεδομένου ότι συμβάλλει στην καθιέρωση μιας παγκόσμιας αγοράς πολλών δισεκατομμυρίων δολαρίων για θεωρητικώς ανώνυμες συναλλαγές χωρίς κυβερνητικό έλεγχο. Ως εκ τούτου, ανακύπτουν ορισμένα ρυθμιστικά ζητήματα που αφορούν εθνικές κυβερνήσεις και χρηματοπιστωτικά ιδρύματα. [03]

Παρακάτω αναλύονται επιγραμματικά ορισμένες ακόμα έννοιες σχετικές με το Blockchain. [01]

Κρυπτονόμισμα: Τα κρυπτονομίσματα είναι ψηφιακά νομίσματα, τα οποία βασίζονται σε ένα αποκεντρωμένο λογιστικό σύστημα. Αυτό το λογιστικό σύστημα είναι η λεγόμενη αλυσίδα μπλοκ. Αυτή αποθηκεύει συναλλαγές με αποκεντρωτικό τρόπο, κρυπτογραφημένες μέσω της κρυπτογράφησης. Εξού και η ονομασία κρυπτονόμισμα.

Tokens (μάρκες): Το token είναι μία μονάδα αξίας. Κάθε κρυπτονόμισμα έχει ένα εμπορεύσιμο αγαθό, όπως τα αντίστοιχα νομίσματα, πιστοποιητικά, εικονικά στοιχεία ή σημεία. Τα tokens χρησιμεύουν ως ισοδύναμα σε αυτά τα εμπορεύσιμα προϊόντα.

Mining (εξόρυξη): Η εξόρυξη είναι η διαδικασία επιβεβαίωσης των συναλλαγών ενός κρυπτονομίσματος. Επιπλέον, αποκεντρωμένα νέα coins εξορύσσονται σε αυτήν τη διαδικασία. Στην περίπτωση αυτή, οι κρυπτογραφικές διαδικασίες πραγματοποιούνται με μεθόδους εντατικής επεξεργασίας υπολογιστών, πράγμα που πρέπει να επιτευχθεί ώστε η δημιουργία νέων μπλοκ να συνδέεται με μια ορισμένη προσπάθεια για να αποφευχθεί μεταγενέστερη τροποποίηση της αλυσίδας μπλοκ.

Proof of Work (απόδειξη εργασίας): Η βάση για την εξόρυξη των ψηφιακών νομισμάτων είναι ένας αλγόριθμος, που ονομάζεται Proof of Work (PoW). Το ακρωνύμιο PoW εκφράζει ένα «υπολογιστικό ή κρυπτογραφικό πρόβλημα» και μεταφράζεται στην ελληνική γλώσσα ως «απόδειξη εργασίας». Όταν κάποιος δηλαδή επιλύει σωστά το τιθέμενο πρόβλημα, αποδεικνύει ότι η αρχή λειτουργεί (απόδειξη εργασίας). Μετά την επίλυση του κρυπτογραφικού προβλήματος ο αλγόριθμος παρέχει στους χρήστες που το έλυσαν μια ανταμοιβή, διότι επαλήθευσαν επιτυχώς συναλλαγές και με αυτόν τον τρόπο δημιούργησαν νέα μπλοκ στην αλυσίδα των μπλοκ.

Smart contracts (έξυπνα συμβόλαια/συμβάσεις): Μια έξυπνη σύμβαση είναι ένας αλγόριθμος ηλεκτρονικού υπολογιστή που έχει σχεδιαστεί για να ολοκληρώσει και να διατηρήσει εμπορικές συμβάσεις σε τεχνολογία Blockchain. Οι συμβαλλόμενοι υπογράφουν μία έξυπνη σύμβαση χρησιμοποιώντας τις ίδιες μεθόδους με την υπογραφή όταν στέλνουν κεφάλαια στα υφιστάμενα δίκτυα κρυπτογράφησης. Με την υπογραφή, η σύμβαση τίθεται σε ισχύ.

Ethereum: Το ethereum είναι μία αλυσίδα μπλοκ που επιτρέπει την εκτέλεση αποκεντρωμένων προγραμμάτων (dApps) και έξυπνων συμβολαίων. Το ethereum είναι η εναλλακτική λύση για την καθιερωμένη αρχιτεκτονική πελάτη-εξυπηρετητή.

Hash Function (Κρυπτογραφημένη συνάρτηση κατακερματισμού): Ο όρος κρυπτονόμισμα ήδη υποδεικνύει ότι υπάρχει μία σύνδεση μεταξύ του Bitcoin κ.α. από την μία μεριά και της κρυπτογράφησης από την άλλη. Αυτή η σχέση εκδηλώνεται στην κρυπτογραφική συνάρτηση κατακερματισμού (Hash Function).

Ledger (Μητρώο/Καθολικό): Η λέξη ledger είναι ο αγγλικός οικονομικός όρος για ένα λογιστικό βιβλίο. Σε αυτό το «λογιστικό» βιβλίο εισάγονται όλες οι πληροφορίες σχετικά με τις κινήσεις χρημάτων. Σε αυτές τις περίπλοκες πληροφορίες συμπεριλαμβάνονται τα ποσά, τα χρηματικά ποσά και η προβλεπόμενη χρήση κεφαλαίων. Στο πλαίσιο των κρυπτονομισμάτων ένα καθολικό έχει δύο έννοιες. Στην πρώτη, το καθολικό είναι ένα σταθερό μέρος του ψηφιακού λογιστηρίου. Στη δεύτερη έννοια, το αποκεντρωμένο καθολικό,

μαζί με μία αλυσίδα μπλοκ, αντικαθιστά όλες τις λειτουργίες μιας συμβατικής τράπεζας.

2.2 Τι είναι το Bitcoin

Το Bitcoin είναι πιθανώς η μεγαλύτερη καινοτομία στο χρηματοοικονομικό σύστημα εδώ και έναν αιώνα. Μεγαλύτερη, ενδεχομένως, και από την εμφάνιση των πιστωτικών καρτών. Με λίγα λόγια, το Bitcoin είναι ένα εντελώς ψηφιακό νόμισμα και δεν υφίσταται επισήμως σε καμία φυσική μορφή κερμάτων ή χαρτονομισμάτων. Δεν παράγεται από καμία συγκεκριμένη χώρα και δεν ελέγχεται από καμία συγκεκριμένη κεντρική τράπεζα ή κυβέρνηση. Η παραγωγή, αποθήκευσή, διακίνησή και όλες οι συναλλαγές με αυτό γίνονται αποκλειστικά σε ηλεκτρονική μορφή. Ακριβέστερα, το Bitcoin είναι ένα peer-to-peer σύστημα πληρωμών και ένα ψηφιακό συνάλλαγμα ανοιχτού κώδικα. Ουσιαστικά ανήκει στην κατηγορία των cryptocurrencies καθώς χρησιμοποιεί μεθόδους κρυπτογραφίας για τη δημιουργία και διαχείριση των χρημάτων και για την επιβεβαίωση της εγκυρότητας των συναλλαγών. Ακολουθεί μια σύντομη ιστορική αναδρομή σχετικά με τη δημιουργία του Bitcoin.

Η ιδέα ενός distributed cryptocurrency προτάθηκε εν μέρει το 1998 από τον WeiDai, στη mailing list της ομάδας ακτιβιστών Cypherpunks που προωθούν ενεργά τη χρήση ισχυρής κρυπτογραφίας. Το 2008, πιθανότατα με έμπνευση την οικονομική κρίση, έγινε η πρώτη επιστημονική δημοσίευση που περιέγραφε το Bitcoin. Η πρώτη λειτουργική εμφάνιση με την κυκλοφορία του πρώτου client ανοιχτού κώδικα και την δημιουργία των αντίστοιχων Bitcoins έγινε το 2009. Ο συγγραφέας της δημοσίευσης και δημιουργός του αντίστοιχου λογισμικού παρέμεινε ανώνυμος, χρησιμοποιώντας το ψευδώνυμο Satoshi Nakamoto. Η πραγματική ταυτότητά του, ή ακόμα και το αν πρόκειται για ένα άτομο ή μία ομάδα, παραμένει ένα μυστήριο μέχρι και σήμερα. Φυσικά το internet λατρεύει ένα καλό μυστήριο και έτσι πολλές θεωρίες έχουν προταθεί για το ποιος μπορεί να κρύβεται πίσω από το ψευδώνυμο αυτό. Ανάμεσα στην πληθώρα θεωριών, αρκετές είναι σχετικά λογικές, υποδεικνύοντας υποψηφίους

με τα κατάλληλα προσόντα: μαθηματικές ιδιοφυΐες, επιστήμονες των υπολογιστών, οικονομικούς κοινωνιολόγους με γνώσεις προγραμματισμού και ομάδες κρυπτογράφων. [02]

2.3 Πώς λειτουργεί η τεχνολογία Blockchain σε σχέση με το Bitcoin

Εξηγούμε την έννοια του Blockchain εξηγώντας πώς λειτουργεί το Bitcoin, καθώς είναι εγγενώς συνδεδεμένα μεταξύ τους. Ωστόσο, η τεχνολογία Blockchain ισχύει για οποιαδήποτε συναλλαγή ψηφιακού περιουσιακού στοιχείου που ανταλλάσσεται στο διαδίκτυο. [05]

Το ηλεκτρονικό εμπόριο συνδέεται αποκλειστικά με τα χρηματοπιστωτικά ιδρύματα που λειτουργούν ως αξιόπιστοι τρίτοι που επεξεργάζονται και διαμεσολαβούν σε οποιαδήποτε ηλεκτρονική συναλλαγή. Ο ρόλος του έμπιστου τρίτου μέρους είναι να επικυρώνει, να διασφαλίζει και να διατηρεί τις συναλλαγές. Ένα ορισμένο ποσοστό απάτης είναι αναπόφευκτο στις ηλεκτρονικές συναλλαγές και χρειάζεται μεσολάβηση από χρηματοπιστωτικές οντότητες. Αυτό έχει ως αποτέλεσμα υψηλό κόστος συναλλαγής. [05]

Το Bitcoin χρησιμοποιεί κρυπτογραφική απόδειξη αντί της εμπιστοσύνης της τρίτης μεριάς για δύο μέρη που επιθυμούν να εκτελέσουν μια ηλεκτρονική συναλλαγή μέσω του Διαδικτύου. Κάθε συναλλαγή προστατεύεται μέσω ψηφιακής υπογραφής και αποστέλλεται στο «δημόσιο κλειδί» του παραλήπτη ψηφιακά υπογεγραμμένο χρησιμοποιώντας το «ιδιωτικό κλειδί» του αποστολέα. Προκειμένου να ξοδέψει χρήματα, ο ιδιοκτήτης του κρυπτονομίσματος πρέπει να αποδείξει την ιδιοκτησία του «ιδιωτικού κλειδιού». Η οντότητα που λαμβάνει το ψηφιακό νόμισμα επαληθεύει την ψηφιακή υπογραφή -ή την ιδιοκτησία του αντίστοιχου «ιδιωτικού κλειδιού» - στη συναλλαγή χρησιμοποιώντας το «δημόσιο κλειδί» του αποστολέα. Κάθε συναλλαγή μεταδίδεται σε κάθε κόμβο στο δίκτυο Bitcoin και στη συνέχεια καταγράφεται σε δημόσιο βιβλίο μετά την επαλήθευση. Κάθε συναλλαγή πρέπει

να επαληθεύεται για την εγκυρότητα πριν καταγραφεί στο δημόσιο βιβλίο. Ο κόμβος επαλήθευσης πρέπει να διασφαλίσει δύο πράγματα πριν από την καταγραφή οποιασδήποτε συναλλαγής:

1. Ο καταναλωτής είναι κάτοχος των κρυπτονομισμάτων και της ψηφιακής υπογραφής της συναλλαγής.

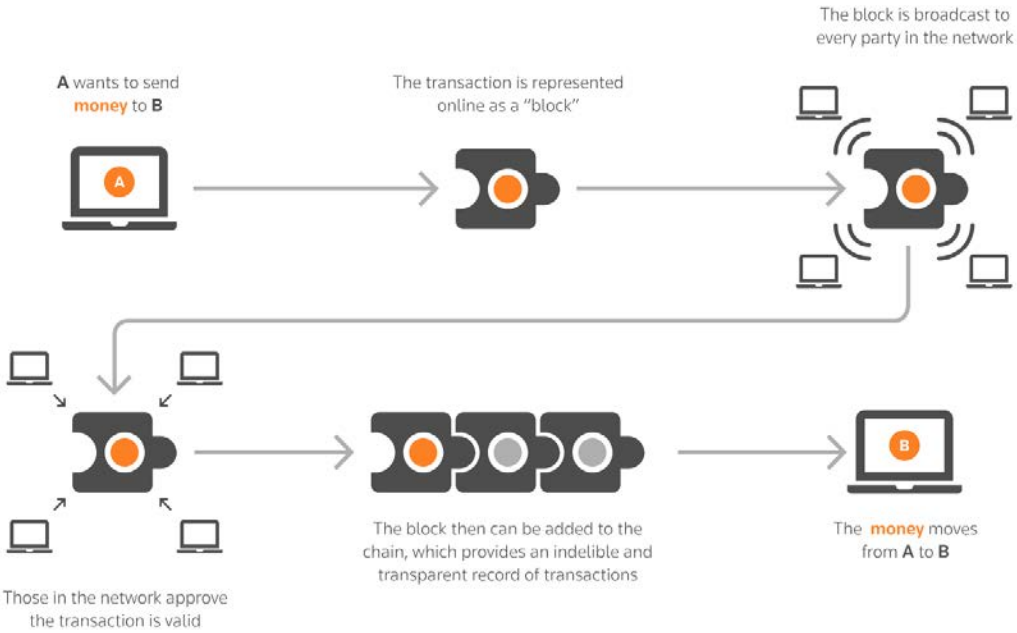
2. Ο καταναλωτής έχει επαρκή κρυπτογράφηση στο λογαριασμό του: ελέγχεται κάθε συναλλαγή με τον λογαριασμό του καταναλωτή (δημόσιο κλειδί) στο βιβλίο για να βεβαιωθεί ότι έχει επαρκή ισορροπία στον λογαριασμό του.

Ωστόσο, υπάρχει ζήτημα διατήρησης της σειράς αυτών των συναλλαγών που μεταδίδονται σε κάθε άλλο κόμβο στο peer-to-peer δίκτυο του Bitcoin. Οι συναλλαγές δεν έρχονται με τη σειρά με την οποία δημιουργούνται και ως εκ τούτου, υπάρχει ανάγκη για ένα σύστημα το οποίο διασφαλίζει ότι δεν μπορεί να συμβεί διπλή συναλλαγή κρυπτονομισμάτων. Με άλλα λόγια, δεν υπάρχει εγγύηση ότι οι εντολές οι οποίες εισάγονται σε έναν κόμβο είναι της ίδιας σειράς με την οποία δημιουργήθηκαν οι αντίστοιχες συναλλαγές. Αυτό σημαίνει ότι υπάρχει ανάγκη να αναπτυχθεί ένας μηχανισμός έτσι ώστε ολόκληρο το δίκτυο Bitcoin να μπορεί να συμφωνήσει σχετικά με τη σειρά των συναλλαγών, πράγμα που αποτελεί τεράστιο έργο σε ένα κατανεμημένο σύστημα. Το Bitcoin λύνει αυτό το πρόβλημα με ένα μηχανισμό που είναι πλέον γνωστός ως τεχνολογία Blockchain. Το σύστημα Bitcoin τοποθετεί τις συναλλαγές του σε ομάδες που ονομάζονται μπλοκ και στη συνέχεια συνδέει αυτά τα μπλοκ μέσω του Blockchain. Οι συναλλαγές σε ένα μπλοκ θεωρούνται ότι έχουν συμβεί ταυτόχρονα. Αυτά τα μπλοκ συνδέονται μεταξύ τους (όπως μια αλυσίδα) σε μια κατάλληλη γραμμική, χρονολογική σειρά με κάθε μπλοκ να περιέχει το hash του προηγούμενου. Το πρόβλημα που παραμένει είναι ότι οποιοσδήποτε κόμβος στο δίκτυο μπορεί να συλλέξει ανεπιβεβαίωτες συναλλαγές και να δημιουργήσει ένα μπλοκ και μετά να το μεταφέρει στο υπόλοιπο δίκτυο σαν πρόταση ως προς το ποιο μπλοκ θα πρέπει να είναι το επόμενο στο Blockchain. Πώς αποφασίζει το δίκτυο ποιο μπλοκ θα πρέπει να είναι το επόμενο στο Blockchain; Μπορούν να δημιουργηθούν πολλαπλά μπλοκ από διαφορετικούς κόμβους ταυτόχρονα; Το Bitcoin λύνει αυτό το πρόβλημα εισάγοντας ένα μαθηματικό πάζλ. Κάθε μπλοκ

θα γίνει αποδεκτό στο Blockchain υπό την προϋπόθεση ότι περιέχει μια απάντηση σε ένα πολύ ιδιαίτερο μαθηματικό πρόβλημα.

Αυτό είναι επίσης γνωστό ως «απόδειξη εργασίας» - ο κόμβος που δημιουργεί ένα μπλοκ πρέπει να αποδείξει ότι έχει βάλει αρκετούς υπολογιστικούς πόρους για να λύσει ένα μαθηματικό πρόβλημα. Η μέση απαιτούμενη προσπάθεια είναι εκθετική αναφορικά με τον αριθμό των μηδενικών bits που απαιτούνται, αλλά η διαδικασία επαλήθευσης είναι πολύ απλή και μπορεί να γίνει με την εκτέλεση ενός μόνο hash. Αυτό το μαθηματικό πάζλ δεν είναι εύκολο να λυθεί και η πολυπλοκότητα του προβλήματος μπορεί να ρυθμιστεί έτσι ώστε κατά μέσο όρο να διαρκέσει δέκα λεπτά για έναν κόμβο στο δίκτυο Bitcoin για να κάνει μια σωστή πρόβλεψη και να δημιουργήσει ένα μπλοκ. Υπάρχει πολύ μικρή πιθανότητα να δημιουργηθούν περισσότερα από ένα μπλοκ στο σύστημα σε δεδομένη χρονική στιγμή. Ο πρώτος κόμβος, για να λύσει το πρόβλημα, μεταδίδει το μπλοκ στο υπόλοιπο του δικτύου. Περιστασιακά, ωστόσο, θα λυθούν ταυτόχρονα περισσότερα από ένα μπλοκ, οδηγώντας σε διάφορους πιθανούς κλάδους. Ωστόσο, τα μαθηματικά της επίλυσης είναι πολύ περίπλοκα και για αυτό το Blockchain σταθεροποιείται γρήγορα, πράγμα που σημαίνει ότι κάθε κόμβος είναι σύμφωνος με την σειρά των τελευταίων μπλοκ. Οι κόμβοι που δωρίζουν τους υπολογιστικούς τους πόρους για να λύσουν το πάζλ και να δημιουργήσουν μπλοκ ονομάζονται «miners» και επιβραβεύονται οικονομικά για τις προσπάθειές τους. Το δίκτυο δέχεται μόνο το μεγαλύτερο Blockchain ως έγκυρο. Ως εκ τούτου, είναι σχεδόν αδύνατο για έναν εισβολέα να εισαγάγει μια δόλια συναλλαγή δεδομένου ότι δεν έχει μόνο να δημιουργήσει ένα μπλοκ μέσω της επίλυσης του μαθηματικού προβλήματος, αλλά πρέπει ταυτόχρονα να ανταγωνιστεί ενάντια στους καλούς κόμβους και να παράγει όλα τα επόμενα μπλοκ προκειμένου να κάνει τους άλλους κόμβους να δεχτούν τη συναλλαγή και το μπλοκ του ως έγκυρο. Αυτή η εργασία καθίσταται ακόμα πιο δύσκολη, καθώς τα μπλοκ στο Blockchain συνδέονται κρυπτογραφικά. Πρακτικά ο οποιοσδήποτε μπορούσε να τρέχει τον Bitcoin client στον υπολογιστή του και μέσα σε σχετικά σύντομο διάστημα να αποκτήσει εκατοντάδες Bitcoins (τα οποία βέβαια τότε δεν άξιζαν σχεδόν τίποτα). [04-07]

Στο γράφημα παρουσιάζεται απλοποιημένα η λειτουργία του Blockchain [07]



Εικόνα 1: Λειτουργία Blockchain

2.4 Εξόρυξη Bitcoin (Mining)

Το Bitcoin Mining, ή αλλιώς εξόρυξη Bitcoin, είναι η διαδικασία με την οποία οι συναλλαγές επαληθεύονται και προστίθενται στο δημόσιο βιβλίο, γνωστό ως Blockchain, καθώς και τα μέσα μέσω των οποίων απελευθερώνεται ένα νέο Bitcoin. Ο καθένας με πρόσβαση στο διαδίκτυο και το κατάλληλο υλικό μπορεί να συμμετέχει στην εξόρυξη. Η διαδικασία εξόρυξης περιλαμβάνει την κατάρτιση των πρόσφατων συναλλαγών σε μπλοκ και την προσπάθεια επίλυσης ενός δύσκολου υπολογιστικού γρίφου. Ο συμμετέχων που λύνει πρώτος το πάζλ τοποθετεί το επόμενο μπλοκ στο Blockchain και διεκδικεί τις ανταμοιβές που αξίζει. Οι ανταμοιβές, οι οποίες ενθαρρύνουν την εξόρυξη, είναι τόσο οι αμοιβές συναλλαγών που σχετίζονται με τις συναλλαγές που συντάσσονται στο μπλοκ, όσο και τα πρόσφατα δημοσιευμένα coins. [08]

Κεφάλαιο 3

Εφαρμογές της τεχνολογίας Blockchain

3.1 Χρήσεις του Blockchain

Όπως γίνεται κατανοητό, η ιδία η δομή και ο σχεδιασμός του Blockchain δημιουργεί κάποια προβλήματα, ιδιαίτερα όσον αφορά συναλλαγές καθώς δεν μπορεί να συναγωνιστεί σε ταχύτητα τις παραδοσιακές πρακτικές. Όμως, θυσιάζοντας την ταχύτητα τα οφέλη που δημιουργούνται είναι εξαιρετικά. Η τεχνολογία Blockchain δεν είναι αμφιλεγόμενη και έχει λειτουργήσει άψογα με την πάροδο των ετών και λειτουργεί με επιτυχία τόσο στις οικονομικές όσο και στις μη οικονομικές εφαρμογές παγκοσμίως.

Η τρέχουσα ψηφιακή οικονομία βασίζεται στην εμπιστοσύνη σε μια συγκεκριμένη αξιόπιστη αρχή. Όλες οι συναλλαγές μας στο διαδίκτυο βασίζονται στην εμπιστοσύνη σε κάποιον που μας λέει την αλήθεια - μπορεί να είναι πάροχος υπηρεσιών ηλεκτρονικού ταχυδρομείου που μας λέει ότι το email μας έχει παραδοθεί, μπορεί να είναι μια αρχή πιστοποίησης που μας λέει ότι ένα συγκεκριμένο ψηφιακό πιστοποιητικό είναι αξιόπιστο, ή μπορεί να είναι ένα κοινωνικό δίκτυο όπως το Facebook που μας λέει ότι οι θέσεις μας σχετικά με τα γεγονότα της ζωής μας έχουν μοιραστεί μόνο με τους φίλους μας ή μπορεί να είναι μια τράπεζα που μας λέει ότι τα χρήματά μας έχουν παραδοθεί αξιόπιστα στους αγαπημένους μας σε μια απομακρυσμένη χώρα. Το γεγονός είναι ότι ζούμε την ζωή μας επισφαλώς στον ψηφιακό κόσμο βασιζόμενοι σε μια τρίτη οντότητα για την ασφάλεια και την ιδιωτικότητα των ψηφιακών στοιχείων μας. Παραμένει βέβαιο ότι αυτές οι πηγές τρίτων μπορούν να παραβιασθούν, να διαχειριστούν ή να διακυβευθούν. Εδώ όμως είναι που η τεχνολογία Blockchain παίρνει θέση. Έχει τη δυνατότητα να φέρει επανάσταση στον ψηφιακό κόσμο επιτρέποντας μια κατανεμημένη συναίνεση, όπου κάθε συναλλαγή στο παρελθόν και στο παρόν με ψηφιακά στοιχεία μπορεί να επαληθευτεί ανά πάσα

στιγμή στο μέλλον. Αυτό γίνεται χωρίς να διακυβεύεται η ιδιωτικότητα των ψηφιακών στοιχείων και των εμπλεκομένων μερών. Η κατανεμημένη συναίνεση και η ανωνυμία είναι δύο σημαντικά χαρακτηριστικά της τεχνολογίας Blockchain. [09-12]

Τα πλεονεκτήματα της τεχνολογίας Blockchain αντισταθμίζουν τα ρυθμιστικά ζητήματα και τις τεχνικές προκλήσεις. Μια βασική αναδυόμενη περίπτωση χρήσης τεχνολογίας Blockchain περιλαμβάνει τις «έξυπνες συμβάσεις» (Smart Contracts). Οι έξυπνες συμβάσεις είναι βασικά προγράμματα ηλεκτρονικών υπολογιστών (API) που μπορούν να εκτελέσουν αυτόματα τους όρους μιας σύμβασης. Όταν μία προκαθορισμένη προϋπόθεση σε μια έξυπνη σύμβαση μεταξύ των συμμετεχόντων οντοτήτων πληρείται, τότε τα μέρη που συμμετέχουν στη συμβατική αυτή συμφωνία μπορούν να πραγματοποιήσουν αυτόματα πληρωμές σύμφωνα με τη σύμβαση με διαφανή τρόπο.

Η έξυπνη ιδιοκτησία (Smart Property) είναι μια άλλη σχετική ιδέα που αφορά τον έλεγχο της ιδιοκτησίας ενός ακινήτου ή ενός στοιχείου μέσω Blockchain χρησιμοποιώντας έξυπνες συμβάσεις. Το αγαθό μπορεί να είναι φυσικό όπως αυτοκίνητο, σπίτι, smartphone κλπ, ή μπορεί να είναι μη φυσικό όπως οι μετοχές μιας εταιρείας. Θα πρέπει να σημειωθεί εδώ ότι ακόμη και το Bitcoin δεν είναι πραγματικά ένα νόμισμα - το Bitcoin έχει να κάνει με τον έλεγχο της ιδιοκτησίας των χρημάτων. Η τεχνολογία Blockchain βρίσκει εφαρμογή σε ευρύ φάσμα τομέων, οικονομικών και μη. Τα χρηματοπιστωτικά ιδρύματα και οι τράπεζες δεν βλέπουν πλέον την τεχνολογία Blockchain ως απειλή για τα παραδοσιακά επιχειρηματικά μοντέλα. Οι μεγαλύτερες τράπεζες του κόσμου αναζητούν ευκαιρίες σε αυτόν τον τομέα, κάνοντας έρευνα για καινοτόμες εφαρμογές Blockchain.

Οι ευκαιρίες για μη οικονομικές εφαρμογές είναι επίσης ατελείωτες. Μπορούμε να ενσωματώσουμε την απόδειξη της ύπαρξης νομικών εγγράφων, των ιατρικών αρχείων και των πληρωμών, δικαιωμάτων στη μουσική βιομηχανία, στον συμβολαιογράφο, στις ιδιωτικές κινητές αξίες και στις άδειες γάμου στο Blockchain. Με την αποθήκευση του δακτυλικού αποτυπώματος του ψηφιακού

στοιχείου αντί για την αποθήκευση του ίδιου του ψηφιακού στοιχείου, μπορεί να επιτευχθεί ο στόχος ανωνυμίας ή ιδιωτικότητας.

Η τεχνολογία Blockchain έχει τη δυνατότητα να γίνει ο νέος κινητήρας της ανάπτυξης στην ψηφιακή οικονομία, όπου όλο και περισσότερο χρησιμοποιούμε το Διαδίκτυο για να διεξάγουμε ψηφιακό εμπόριο και να μοιραζόμαστε τα προσωπικά μας δεδομένα και τα γεγονότα της ζωής. Υπάρχουν τεράστιες ευκαιρίες και η επανάσταση στον χώρο αυτό μόλις ξεκίνησε. Παρακάτω, εστιάζουμε σε ορισμένες βασικές εφαρμογές της τεχνολογίας Blockchain στον χρηματοοικονομικό κλάδο, όσο και στον τομέα των μη οικονομικών εφαρμογών. [09-12]

3.2 Χρηματοοικονομικές εφαρμογές

Χρηματιστήριο.

Η ένταξη μίας εταιρείας στο χρηματιστήριο έχει μεγάλα κόστη. Ένα σύνολο τραπεζών πρέπει να εργαστεί για να αναλάβει τη συμφωνία και να προσελκύσει επενδυτές. Τα χρηματιστήρια κατατάσσουν τις μετοχές της εταιρείας στη δευτερογενή αγορά για να λειτουργήσουν με ασφάλεια. Είναι πλέον θεωρητικά δυνατό οι εταιρείες να εκδίδουν απευθείας τις μετοχές τους μέσω του Blockchain. Αυτές οι μετοχές μπορούν στη συνέχεια να αγοραστούν και να πωληθούν σε μια δευτερογενή αγορά που βρίσκεται στο Blockchain. Η NASDAQ εγκαινίασε το Private Equity Exchange το 2014. Σκοπός του είναι να παράσχει τις βασικές λειτουργίες όπως ο πίνακας Cap και η διαχείριση των σχέσεων με τους επενδυτές για τις ιδιωτικές εταιρείες. Η τρέχουσα διαδικασία διαπραγμάτευσης μετοχών σε αυτή την ανταλλαγή είναι αναποτελεσματική και αργή λόγω της συμμετοχής πολλών τρίτων μερών. Η NASDAQ έχει δώσει τα χέρια με μία Start-up που ονομάζεται chain.com από το Σαν Φρανσίσκο για την υλοποίηση της ανταλλαγής ιδιωτικών μετοχών στο Blockchain. Το Chain.com εφαρμόζει έξυπνες συμβάσεις βασισμένες στο Blockchain για την εφαρμογή λειτουργιών ανταλλαγής. Αυτό το προϊόν αναμένεται να είναι γρήγορο, ανιχνεύσιμο και αποτελεσματικό. [13]

Ασφάλιση.

Περιουσιακά στοιχεία τα οποία μπορούν να αναγνωριστούν με μοναδικό τρόπο από έναν ή περισσότερους αναγνωριστές που είναι δύσκολο να καταστραφούν ή να αναπαραχθούν, μπορούν να καταχωρηθούν σε Blockchain. Αυτό μπορεί να χρησιμοποιηθεί για την επαλήθευση της ιδιοκτησίας ενός στοιχείου και για τον εντοπισμό του ιστορικού συναλλαγών. Οποιοδήποτε αγαθό (φυσικό ή ψηφιακό όπως ακίνητα, αυτοκίνητα, φυσικά περιουσιακά στοιχεία, φορητοί υπολογιστές, άλλα τιμαλφή) μπορεί ενδεχομένως να καταχωρηθεί σε Blockchain καθώς η κυριότητα και το ιστορικό συναλλαγών μπορούν να επικυρωθούν από οποιονδήποτε, ειδικά τους ασφαλιστές. [13]

Τραπεζική.

Είναι κοινός τόπος ότι πρέπει να συζητηθούν τα ζητήματα σχετικά με τις παγκόσμιες απαιτήσεις AML (Anti-Money Laundering) και KYC (Know Your Customer) στον τραπεζικό τομέα. Παρόλο που ενθαρρύνεται η καινοτομία του Blockchain, απαιτείται μεγαλύτερη νομική σαφήνεια για να αποφευχθεί το ενδεχόμενο να εξαιρεθούν οι αναπτυσσόμενες χώρες από το χρηματοπιστωτικό σύστημα. Οι νομοθέτες που υποστηρίζουν τον νόμο για την τραπεζική μυστικότητα (BSA) υπογράμμισαν ότι ένας νέος νόμος δεν θα επιβάρυνε τα χρηματοπιστωτικά ιδρύματα, διότι έχουν ήδη τα περισσότερα από τα απαιτούμενα αρχεία, ενώ παράλληλα θα υπάρχει το περιθώριο για παροχή εξαιρέσεων στις περιπτώσεις όπου το κανονιστικό κόστος θα υπερβαίνει τα οφέλη. Πλέον κάθε νόμος προσθέτει περισσότερες απαιτήσεις για τις τράπεζες και τους αποστολείς χρημάτων. Σήμερα, αυτή η περίληψη των κανονισμών αναφέρεται γενικά ως οι κανόνες για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML) και του γνώρισε τον πελάτη σου (KYC). Εκτός από την αναφορά συναλλαγών που υπερβαίνουν ορισμένα επίπεδα, οι τράπεζες πρέπει τώρα να γνωρίζουν ποιοι είναι οι πελάτες τους και να αναφέρουν τυχόν «ύποπτες ενέργειες». [13-15]

Αβεβαιότητα και αποφυγή κινδύνων.

Οι κανονιστικές επιβαρύνσεις των χρηματοπιστωτικών ιδρυμάτων είναι δαπανηρές και τα αυξανόμενα τραπεζικά τέλη και τέλη υπηρεσιών αντανακλούν

αυτό το γεγονός. Ωστόσο, μετά τη χρηματοπιστωτική κρίση του 2008, οι ρυθμιστικές αρχές πρόσθεσαν και την αβεβαιότητα. Ειδικά στις ΗΠΑ, οι αρχές άρχισαν να χρησιμοποιούν την ευρεία εξουσιοδότηση που τους χορήγησε το Κογκρέσο για να επιβάλουν μεγάλα πρόστιμα, συνολικού ύψους 321 δισ. Δολαρίων, στις τράπεζες μεταξύ 2009 και 2016. Παράλληλα και στην ΕΕ ελήφθησαν πρωτοβουλίες για την θωράκιση του τραπεζικού συστήματος απέναντι σε κινδύνους και δόλιες πρακτικές. Η τυχαιότητα του ποιος θα μπορούσε να τιμωρηθεί προσεχώς και πόσο, πρόσθεσε τεράστια αβεβαιότητα στον τραπεζικό κόσμο. Εκτός από τον οικονομικό αντίκτυπο μεγάλων προστίμων, το να χαρακτηρίζεται μια εταιρία υποστηρικτής της τρομοκρατίας και του οργανωμένου εγκλήματος φέρει τεράστιο κίνδυνο για τη φήμη της. Οι τράπεζες έλαβαν το μήνυμα και η αντίδρασή τους ήταν να διασπάσουν τους δεσμούς με σχεδόν οποιαδήποτε τράπεζα εκτός Ευρωσυστήματος και με πελάτες ή βιομηχανίες που οι ρυθμιστικές αρχές θα μπορούσαν να θεωρήσουν «ύποπτους». [13]

Αποφυγή κινδύνου και ανθρώπινο κόστος.

Το ποσό της δραστηριότητας αποτροπής των κινδύνων ήταν σημαντικό. Μια ερευνητική ομάδα του τραπεζικού κλάδου, διαπίστωσε τον Μάιο του 2017 ότι το 25% των παγκόσμιων τραπεζικών σχέσεων έχουν επιδεινωθεί από το 2009. Οι επιχειρήσεις που ασχολούνται με τα κρυπτονομίσματα έχουν υποστεί κλείσιμο λογαριασμών και δεν έχουν δικαίωμα σε τραπεζικές υπηρεσίες σύμφωνα με την πρακτική πρόληψης κινδύνου. Ορισμένες περιφέρειες όπως η Αφρική και η Καραϊβική έχουν πληγεί περισσότερο, με σχεδόν το 70% των τραπεζών της Καραϊβικής να αναφέρουν την διακοπή των παγκόσμιων τραπεζικών σχέσεων μέχρι το 2018. Μια ξεχωριστή μελέτη που δημοσιεύθηκε από το Φιλανθρωπικό και Ασφαλιστικό Δίκτυο τον Φεβρουάριο του 2017, διαπίστωσε ότι το 66% των φιλανθρωπικών οργανώσεων και των μη κερδοσκοπικών ιδρυμάτων αντιμετωπίζουν εμπόδια όπως οι καθυστερήσεις πληρωμών και οι αυξήσεις των τελών. Συνολικά το 16% των φιλανθρωπικών οργανώσεων που συμμετείχαν στην έρευνα δήλωσαν ότι αντιμετώπισαν κλείσιμο λογαριασμών ή άρνηση ανοίγματος λογαριασμών. Οι περιφερειακές οικονομίες έχουν πληγεί σοβαρά, οι εξαγωγείς δεν είναι σε θέση να

συμμετάσχουν σε χρηματοδότηση του εμπορίου και άτομα που βασίζονται σε πληρωμές εμβασμάτων από συγγενείς, δεν μπορούν να τις λάβουν. Ακόμη και με την παγκόσμια οικονομική ανάπτυξη κατά τη διάρκεια των τελευταίων ετών, οι πληρωμές εμβασμάτων στις αναπτυσσόμενες χώρες μειώθηκαν για δυο συνεχή χρόνια σύμφωνα με την Παγκόσμια Τράπεζα. Οι οικονομικές επιπτώσεις από την αποφυγή του κινδύνου ήταν τόσο σοβαρές ώστε αρκετές κεντρικές τράπεζες της Καραϊβικής άρχισαν να εργάζονται με την εταιρεία Bitt που χρησιμοποιεί Bitcoins, προκειμένου να δημιουργήσουν ένα εναλλακτικό δίκτυο πληρωμών στην Καραϊβική. Ο ιδρυτής και Διευθύνων Σύμβουλος της Bitt, Gabriel Abed, υπήρξε ένας παθιασμένος επικριτής της πολιτικής του περιορισμού των κινδύνων και τονίζοντας ότι για τους ήδη φτωχούς πολίτες της Καραϊβικής, η πολιτική αυτή είναι εξαιρετικά οδυνηρή. Αφού σημείωσε τα πολύ υψηλά έξοδα για να κάνει μια απλή συναλλαγή, ο Abed το συνόψισε λέγοντας απλά: «Είναι ακριβό να είσαι φτωχός.» [13, 14]

Re-Risking.

Με την απομάκρυνση εκατομμυρίων από το χρηματοπιστωτικό σύστημα, η μείωση του κινδύνου δημιουργεί ένα μεγάλο πληθυσμό που δεν έχει άλλη εναλλακτική λύση παρά να χρησιμοποιεί την μαύρη αγορά ή παράνομα μέσα για να κάνει πληρωμές, να μεταφέρει χρήματα ή να συμμετάσχει με άλλο τρόπο στην οικονομία. Ο Henry Balani της Accuity σημειώνει ότι «η ρύθμιση που αποσκοπεί στην προστασία του παγκόσμιου χρηματοπιστωτικού συστήματος έχει, κατά μία έννοια, το αντίθετο αποτέλεσμα και απομακρύνει ολόκληρες περιοχές εκτός του ρυθμιζόμενου χρηματοπιστωτικού συστήματος». Αυτή η περιθωριοποίηση εκατομμυρίων βοήθησε πολλούς να δουν τα οφέλη των Blockchain, των κρυπτονομισμάτων και άλλων μεθόδων που δεν απαιτούν σημαντική αλληλεπίδραση με το παγκόσμιο χρηματοπιστωτικό σύστημα. Χωρίς πρόσβαση στις παραδοσιακές τράπεζες, πολλές κυβερνήσεις δεν βρίσκουν άλλο τρόπο για να εξασφαλίσουν ότι οι πολίτες τους θα έχουν πρόσβαση σε υποδομές πληρωμών και τραπεζών. Με τόσους πολλούς που απομακρύνθηκαν από το σύστημα, η χρηματοοικονομική ενσωμάτωση έχει γίνει κάτι περισσότερο από αναγκαία. Τονίζεται πλέον, ότι η χρηματοοικονομική ένταξη είναι μια εξαιρετικά

σημαντική ανάγκη, όχι μόνο επειδή είναι απαραίτητη για την κοινωνία, αλλά και επειδή λειτουργεί ως μέσο ελαχιστοποίησης των παράνομων ροών. [15]

Χρηματοοικονομική ένταξη και ασφάλεια.

Η προφανής λύση σε αυτό το ανθρωπιστικό πρόβλημα και το πρόβλημα της επιβολής του νόμου είναι να βρεθεί ένας τρόπος για να γίνουν οι περιοχές, οι βιομηχανίες και τα άτομα που χαρακτηρίζονται επικίνδυνα, πάλι μέρος του χρηματοπιστωτικού συστήματος. Οι επιχειρήσεις μεταφοράς κρυπτονομισμάτων είναι πρόθυμες να παράσχουν λύσεις για την αποφυγή του κινδύνου με πολύ χαμηλότερο κόστος από τις παραδοσιακές τράπεζες, αλλά δεν μπορούν εύκολα να αποκτήσουν τραπεζικές σχέσεις. Οι τράπεζες παραμένουν αβέβαιες ως προς το εάν θα επιβραβευθούν ή θα τιμωρηθούν για προσπάθειες οικονομικής ένταξης. Όλα τα μέρη θέλουν να γνωρίζουν ότι λειτουργούν στο πλαίσιο του νόμου. Με αυτό το υπόβαθρο, κανένα χρηματοπιστωτικό ίδρυμα ή επιχείρηση μεταβίβασης χρημάτων δεν κινδυνεύει να αναπτύξει επιχειρηματικές δραστηριότητες με βιομηχανίες, άτομα ή περιοχές που μπορεί να είναι επικίνδυνες έως ότου υπάρξει σχετική ρύθμιση. Το δίκτυο επιβολής οικονομικών εγκλημάτων του αμερικανικού Υπουργείου Οικονομικών (FinCEN) προσπάθησε αρκετές φορές τα τελευταία χρόνια να δηλώσει ότι οι κανονισμοί του είναι σαφείς και δεν απαιτούν από τις τράπεζες να διακόπτουν τις παγκόσμιες σχέσεις μεταξύ τους. Τα εμπειρικά αποτελέσματα δείχνουν ότι αυτό απλά δεν είναι αλήθεια. Ο κίνδυνος απόρριψης συνεχίζεται ασταμάτητα. [15-16]

3.3 Μη Χρηματοοικονομικές Εφαρμογές

Μέχρι σήμερα, το επίκεντρο ήταν οι εφαρμογές Blockchain για τον χρηματοπιστωτικό κλάδο. Ωστόσο, αυτό είναι μόνο η κορυφή του παγόβουνου. Υπάρχουν αρκετοί άλλοι κλάδοι που ήδη εφαρμόζουν τεχνολογία Blockchain. Το Blockchain μπορεί να χρησιμοποιηθεί για να μειωθεί η εγκληματικότητα, η παραχάραξη και ενδεχομένως να σωθούν εν τέλει ανθρώπινες ζωές. [17]

Συμβολαιογραφία.

Η επαλήθευση της αυθεντικότητας του εγγράφου μπορεί να γίνει χρησιμοποιώντας Blockchain και εξαλείφει την ανάγκη κεντρικής εξουσίας. Η υπηρεσία πιστοποίησης εγγράφων βοηθά στην απόδειξη ιδιοκτησίας, ύπαρξης και ακεραιότητας των εγγράφων. Δεδομένου ότι είναι αποδεδειγμένα γνήσιο το έγγραφο και μπορεί να εξακριβωθεί από ανεξάρτητους τρίτους, αυτές οι υπηρεσίες είναι νομικά δεσμευτικές. Η χρήση του Blockchain για τη συμβολαιογραφική πράξη διασφαλίζει την ιδιωτικότητα του εγγράφου και εκείνων που ζητούν πιστοποίηση. Εξαλείφει επίσης την ανάγκη για ακριβές συμβολαιογραφικές αμοιβές και αναποτελεσματικούς τρόπους μεταφοράς εγγράφων. [18-19]

Εφαρμογές του Blockchain στη μουσική βιομηχανία.

Η μουσική βιομηχανία έχει κάνει μια μεγάλη αλλαγή την τελευταία δεκαετία λόγω της ανάπτυξης του Διαδικτύου και της διαθεσιμότητας ορισμένων υπηρεσιών ροής μέσω του Internet. Έχει αντίκτυπο σε όλους τους καλλιτέχνες της μουσικής βιομηχανίας, εκδότες, τραγουδοποιούς και παρόχους υπηρεσιών ροής. Η διαδικασία με την οποία καθορίζονται τα δικαιώματα μουσικής ήταν πάντοτε συγκεχυμένη, αλλά η άνοδος του Διαδικτύου την κατέστησε ακόμα πιο πολύπλοκη λόγω της αύξησης της ζήτησης διαφάνειας στις πληρωμές δικαιωμάτων σε καλλιτέχνες. Εδώ είναι που το Blockchain μπορεί να διαδραματίσει ένα ρόλο διατηρώντας μια ολοκληρωμένη, ακριβή και κατανεμημένη βάση δεδομένων πληροφοριών ιδιοκτησίας δικαιωμάτων μουσικής σε ένα δημόσιο βιβλίο. Εκτός από τις πληροφορίες ιδιοκτησίας δικαιωμάτων, η κατανομή των δικαιωμάτων για κάθε εργασία, όπως καθορίζεται από έξυπνες συμβάσεις, θα μπορούσε να προστεθεί στη βάση δεδομένων. Οι έξυπνες συμβάσεις θα ορίζουν σχέσεις μεταξύ διαφορετικών ενδιαφερομένων (διευθύνσεων) και θα αυτοματοποιούν τις αλληλεπιδράσεις τους. [19]

Αποκεντρωμένη απόδειξη ύπαρξης εγγράφων.

Η επικύρωση της ύπαρξης ή της κατοχής υπογεγραμμένων εγγράφων είναι πολύ σημαντική σε οποιαδήποτε νομική πράξη. Τα παραδοσιακά μοντέλα επικύρωσης

εγγράφων βασίζονται στις κεντρικές αρχές για την αποθήκευση και την επικύρωση των εγγράφων, τα οποία παρουσιάζουν ορισμένες προφανείς προκλήσεις ασφάλειας. Αυτά τα μοντέλα καθίστανται ακόμη πιο δύσκολα καθώς τα έγγραφα παλιώνουν. Η τεχνολογία Blockchain παρέχει ένα εναλλακτικό μοντέλο για την απόδειξη ύπαρξης και κατοχής νομικών εγγράφων. Χρησιμοποιώντας το Blockchain, ο χρήστης μπορεί απλά να αποθηκεύσει την υπογραφή και τη χρονική σήμανση που σχετίζεται με ένα νομικό έγγραφο και να την επικυρώσει ανά πάσα στιγμή χρησιμοποιώντας καθαρά μηχανισμούς Blockchain. Η απόδειξη της ύπαρξης είναι μια απλή υπηρεσία που επιτρέπει σε κάποιον να αποθηκεύει ανώνυμα και με ασφάλεια online την ύπαρξη οποιουδήποτε εγγράφου. Αυτή η υπηρεσία απλά αποθηκεύει την κρυπτογράφηση του αρχείου, που συνδέεται με την ώρα που ο χρήστης υποβάλλει το έγγραφό του. Πρέπει να σημειωθεί εδώ ότι η κρυπτογράφηση ή το δακτυλικό αποτύπωμα - όχι το πραγματικό έγγραφο - αποθηκεύεται σε Blockchain, οπότε ο χρήστης δεν χρειάζεται να ανησυχεί για την πτυχή της ιδιωτικής του ζωής. Αυτό επιτρέπει στη συνέχεια σε έναν χρήστη να πιστοποιήσει την ύπαρξη ενός εγγράφου που υπήρχε σε μια συγκεκριμένη χρονική στιγμή. Τα σημαντικότερα πλεονεκτήματα αυτής της υπηρεσίας είναι η ασφάλεια και η ιδιωτικότητα που επιτρέπουν σε έναν χρήστη να παρέχει αποκεντρωμένη απόδειξη του εγγράφου που δεν μπορεί να τροποποιηθεί από κάποιον τρίτο. Η ύπαρξη του εγγράφου επικυρώνεται χρησιμοποιώντας Blockchain που δεν εξαρτάται από μια ενιαία συγκεντρωτική οντότητα. [19]

Αποκεντρωμένη αποθήκευση (Cloud).

Οι λύσεις αποθήκευσης αρχείων σε cloud, όπως το Dropbox, το Google Drive ή το One Drive, μεγαλώνουν σε δημοτικότητα για την αποθήκευση εγγράφων, φωτογραφιών, βίντεο και αρχείων μουσικής. Παρά την δημοτικότητα τους, οι λύσεις αποθήκευσης αρχείων σε cloud αντιμετωπίζουν συνήθως προκλήσεις σε τομείς όπως η ασφάλεια, η ιδιωτικότητα και ο έλεγχος των δεδομένων. Το βασικό ζήτημα είναι ότι κάποιος πρέπει να εμπιστευτεί σε έναν τρίτο τα εμπιστευτικά αρχεία του. Η Storj παρέχει μια πλατφόρμα αποθήκευσης cloud που βασίζεται σε Blockchain, η οποία επιτρέπει στους χρήστες να μεταφέρουν και να μοιράζονται δεδομένα χωρίς να βασίζονται σε παρόχους δεδομένων. Αυτό

επιτρέπει στους χρήστες να μοιράζονται το αχρησιμοποίητο εύρος ζώνης Internet και τον ελεύθερο χώρο στο δίσκο στις προσωπικές τους υπολογιστικές συσκευές σε όσους θέλουν να αποθηκεύσουν μεγάλα αρχεία σε αντάλλαγμα για μικρές πληρωμές βασισμένες σε Bitcoin. Η απουσία κεντρικού ελέγχου εξαλείφει τις περισσότερες παραδοσιακές αποτυχίες και διακοπές λειτουργίας δεδομένων, καθώς και σημαντική αύξηση της ασφάλειας, της ιδιωτικότητας και του ελέγχου των δεδομένων. Η πλατφόρμα Storj εξαρτάται από έναν αλγόριθμο πρόκλησης για να προσφέρει κίνητρα στους χρήστες να συμμετέχουν σωστά σε αυτό το δίκτυο. Με αυτόν τον τρόπο, η πλατφόρμα Storj μπορεί περιοδικά να ελέγχει κρυπτογραφικά την ακεραιότητα και τη διαθεσιμότητα ενός αρχείου και να προσφέρει άμεσες ανταμοιβές σε εκείνους που διαφυλάττουν το αρχείο. [19-20]

Αποκεντρωμένο Internet of Things (IoT).

Το IoT γίνεται όλο και δημοφιλέστερη τεχνολογία τόσο στον καταναλωτικό όσο και στον επιχειρηματικό χώρο. Η μεγάλη πλειοψηφία των πλατφορμών IoT βασίζεται σε ένα συγκεντρωτικό μοντέλο στο οποίο ελέγχεται η αλληλεπίδραση μεταξύ των συσκευών. Ωστόσο, αυτή η προσέγγιση έχει καταστεί ανέφικτη για πολλά σενάρια στα οποία οι συσκευές πρέπει να ανταλλάσσουν δεδομένα μεταξύ τους αυτόνομα. Αυτή η ειδική απαίτηση οδήγησε σε προσπάθειες για αποκεντρωμένες πλατφόρμες IoT. Η τεχνολογία Blockchain διευκολύνει την υλοποίηση αποκεντρωμένων πλατφορμών IoT όπως η ασφαλής και αξιόπιστη ανταλλαγή δεδομένων καθώς και η τήρηση αρχείων. Σε μια τέτοια αρχιτεκτονική, το Blockchain χρησιμεύει ως γενικό βιβλίο διατηρώντας ένα αξιόπιστο αρχείο όλων των μηνυμάτων που ανταλλάσσονται μεταξύ έξυπνων συσκευών σε μια αποκεντρωμένη τοπολογία IoT. Η IBM σε συνεργασία με τη Samsung έχει αναπτύξει την πλατφόρμα ADEPT (Autonomous Decentralized Peer To Peer Telemetry) που χρησιμοποιεί στοιχεία του υποκείμενου σχεδιασμού του Bitcoin για να δημιουργήσει ένα κατανεμημένο δίκτυο συσκευών - ένα αποκεντρωμένο Ίντερνετ των Πραγμάτων (IoT). Το ADEPT χρησιμοποιεί τρία πρωτόκολλα - BitTorrent (κοινή χρήση αρχείων), Ethereum (Έξυπνα συμβόλαια) και TeleHash (Peer-To-Peer Messaging) στην πλατφόρμα. [19, 21]

Λύσεις κατά της πλαστογράφησης βασισμένες σε Blockchain.

Η πλαστογράφηση είναι μία από τις μεγαλύτερες προκλήσεις στο σύγχρονο ψηφιακό εμπόριο. Οι υπάρχουσες λύσεις βασίζονται στην εμπιστοσύνη σε μια αξιόπιστη οντότητα που εισάγει μια λογική σχέση μεταξύ εμπόρων και καταναλωτών. Η τεχνολογία Blockchain με την αποκεντρωμένη εφαρμογή και τις δυνατότητές της για την ασφάλεια παρέχει μια εναλλακτική λύση στους υφιστάμενους μηχανισμούς καταπολέμησης της πλαστογράφησης. Μπορούμε να φανταστούμε ένα σενάριο, στο οποίο οι έμποροι και οι αγορές αποτελούν μέρος ενός δικτύου Blockchain με κόμβους που αποθηκεύουν πληροφορίες για την επικύρωση της αυθεντικότητας των προϊόντων. Με τη χρήση αυτής της τεχνολογίας, τα ενδιαφερόμενα μέρη στην αλυσίδα εφοδιασμού δεν χρειάζεται να βασίζονται σε μια κεντρική οντότητα για την αυθεντικότητα των επώνυμων προϊόντων. Η BlockVerify παρέχει λύσεις κατά της απομίμησης που βασίζονται σε Blockchain και εισάγουν διαφάνεια στις αλυσίδες εφοδιασμού. Βρίσκει εφαρμογή σε φαρμακευτικά, πολυτελή αντικείμενα, διαμάντια και βιομηχανίες ηλεκτρονικών ειδών. [22]

Έλεγχος ταυτότητας τέχνης.

Δεν υπάρχουν ακριβή στοιχεία για τα ποσά που ξοδεύονται στην πλαστογραφημένη τέχνη κάθε χρόνο, ενώ μεγάλα περιστατικά κατά την τελευταία δεκαετία έχουν αποκαλύψει ότι οι πλαστογράφοι μπορούν να κερδίσουν εκατομμύρια. Ορισμένες πλαστογραφίες είναι τόσο πειστικές που εμφανίστηκαν στις πιο διάσημες γκαλερί τέχνης του κόσμου. Η εμφάνιση νέων πλατφορμών online πωλήσεων τέχνης, όπως το Artspace, το Paddle8 και η Amazon Art, καθιστούν όλο και πιο δύσκολη την παρακολούθηση των αυθεντικών έργων τέχνης, ενώ αγορά online γίνεται ολοένα δημοφιλέστερη. Όταν αγοράζονται στο διαδίκτυο, τα έργα τέχνης δεν ακολουθούν τα συνηθισμένα κανάλια και τείνουν να προσπεράσουν τους μεσάζοντες, όπως οι δημοπρασίες ή οι γκαλερί, που παίζουν ρόλο στην εξασφάλιση της αυθεντικότητας και στην καταγραφή της ιδιοκτησίας και της θέσης του σπάνιου κομματιού. Στο παρελθόν, η επικύρωση ενός έργου τέχνης περιλάμβανε ορισμένα σημαντικά στάδια, από τον ορισμό της προέλευσης του έργου, την εκπόνηση του κατά πόσο έχει παρουσιαστεί στο παρελθόν και τέλος την

κατοχύρωση της αυθεντικότητας από κάποιον επαγγελματία. Λόγω του επιπέδου των δεξιοτήτων των επαγγελματιών πλαστογράφων, ο μόνος ουσιαστικός τρόπος να αποδειχθεί εάν ένα κομμάτι είναι το γνήσιο είναι μέσω ενός πιστοποιητικού γνησιότητας - το οποίο επίσης θα μπορούσε να πλαστογραφηθεί. Η start-up Verisart, με βάση στο Los Angeles, πιστεύει ότι έχει βρει την απάντηση, χρησιμοποιώντας το Blockchain για να «ξεγελάσει» το σύστημα. Χρησιμοποιώντας την τεχνολογία Blockchain, δημιούργησε μια αποκεντρωμένη βάση δεδομένων της τέχνης που επαληθεύει κάθε έργο, αναθέτοντάς της μοναδικούς κωδικούς αυθεντικότητας. Οι ιδιοκτήτες και οι αγοραστές θα μπορούσαν στη συνέχεια να χρησιμοποιήσουν αυτούς τους μεμονωμένους κωδικούς Blockchain για να επικυρώσουν την αυθεντικότητα των κομματιών και να παρακολουθήσουν την κυκλοφορία τους σε όλο τον κόσμο. Μέσα από το BlockCahin, είναι δυνατό να προσφερθεί ένα δίχτυ ασφαλείας για καλλιτέχνες, έμπορους και συλλέκτες με ένα ψηφιακό σύστημα που θα μπορούσε να επαληθεύσει τα έργα σε πραγματικό χρόνο. Το νέο σύστημα όχι μόνο θα εξασφαλίζει την αυθεντικότητα, αλλά θα παρέχει επίσης ένα επίπεδο ανωνυμίας για τον αγοραστή και τον πωλητή, γεγονός που αποτελεί σημαντικό παράγοντα στον κόσμο της τέχνης, όπου οι ανώνυμοι αγοραστές δεν είναι ασυνήθιστο φαινόμενο. [23]

Προϊόντα υψηλής αξίας.

Σύμφωνα με την Υπηρεσία Τελωνείων και Προστασίας των Συνόρων των ΗΠΑ, εκατομμύρια αποστολές παραποιημένων αγαθών υψηλής αξίας, όπως ηλεκτρονικά αντικείμενα και ψεύτικα ρούχα και αξεσουάρ σχεδιαστών, εισέρχονται στη χώρα κάθε χρόνο. Πάνω από 1.2 δισεκατομμύρια δολάρια αγαθών κατάσχονται ετησίως, αλλά οι αρχές αναγνωρίζουν ότι αυτό είναι ένα κομμάτι του συνόλου των αγαθών που εισέρχονται στη χώρα. Η πλαστογράφηση έχει ονομαστεί το «έγκλημα του αιώνα». Το Διεθνές Εμπορικό Επιμελητήριο (ICC) αναμένει ότι η αξία των παραποιημένων αγαθών θα ξεπεράσει τα 1,7 τρισεκατομμύρια δολάρια παγκοσμίως, αντιπροσωπεύοντας περισσότερο από το 2% της συνολικής οικονομικής δραστηριότητας. [24]

Πλαστά φάρμακα.

Η τεχνολογία Blockchain μπορεί να φανεί χρήσιμη και στην καταπολέμηση του διεθνούς εμπορίου παραποιημένων φαρμάκων. Σύμφωνα με το HavocScope, τα φάρμακα είναι τα πιο συχνά παραποιημένα προϊόντα και αντιπροσωπεύουν ζημιές άνω των 200 δισ. δολαρίων ετησίως. Η Interpol εκτιμά ότι περισσότεροι από 1 εκατομμύριο άνθρωποι σκοτώνονται κάθε χρόνο από παραποιημένα φάρμακα, δηλώνοντας ότι η παραγωγή και η πώληση παραποιημένων φαρμάκων γίνεται μια από τις πιο επικερδείς επιχειρήσεις για οργανωμένες εγκληματικές δραστηριότητες σε όλο τον κόσμο. Τα πιο συχνά παραποιημένα φάρμακα είναι τα αντιβιοτικά, φάρμακα για τον HIV, τα φάρμακα για τον καρκίνο, τα αντικαταθλιπτικά, τα χάπια στυτικής δυσλειτουργίας, τα συμπληρώματα απώλειας βάρους και τα φάρμακα κατά της ελονοσίας. Η Interpol ανέφερε ότι περισσότεροι από 200.000 άνθρωποι πεθαίνουν παγκοσμίως σε ετήσια βάση μόνο από πλαστά αντιαλλεργικά φάρμακα. Όπως διαπιστώνεται, η αύξηση των online πωλήσεων φαρμάκων καθιστά δυσκολότερο για τους υπαλλήλους να παρακολουθούν τη ροή πραγματικών και παραποιημένων προϊόντων. Ορισμένες από τις κορυφαίες εταιρίες στις ΗΠΑ, όπως η Snapdeal Medidart, η Buydrug και η Meramedicare έχουν εγκαταστήσει χαρακτηριστικά ασφαλείας, απαιτώντας από τους χρήστες να ανεβάζουν συνταγές για συνταγογραφούμενα φάρμακα κατά την τοποθέτηση παραγγελιών, ενώ γίνονται και επιπλέον έλεγχοι στους πωλητές. Ωστόσο, ο Παγκόσμιος Οργανισμός Υγείας εκτιμά ότι περισσότερο από το 50% των φαρμάκων που αγοράζονται από διαδικτυακούς πωλητές, όπου το όνομα του γιατρού είναι κρυμμένο, είναι πλαστά. [25]

Εφαρμογές Διαδικτύου.

Το Namecoin είναι μια εναλλακτική τεχνολογία Blockchain (με μικρές παραλλαγές) που χρησιμοποιείται για την υλοποίηση αποκεντρωμένης έκδοσης του Domain Name Server (DNS) που είναι ανθεκτική στη λογοκρισία. Οι τρέχοντες διακομιστές DNS ελέγχονται από κυβερνήσεις και μεγάλες εταιρείες και θα μπορούσαν να καταχραστούν τη δύναμή τους να λογοκρίνουν, να καταπατούν ή να κατασκοπεύουν τη χρήση του Διαδικτύου. Η χρήση της τεχνολογίας Blockchain σημαίνει ότι από τη στιγμή που το DNS ή ο τηλεφωνικός

κατάλογος του Διαδικτύου διατηρείται με αποκεντρωμένο τρόπο και κάθε χρήστης μπορεί να έχει τα ίδια δεδομένα του τηλεφωνικού καταλόγου στον υπολογιστή του. Η τεχνολογία δημόσιου κλειδιού υποδομής (PKI) χρησιμοποιείται ευρέως για την κεντρική διανομή και διαχείριση ψηφιακών πιστοποιητικών. Κάθε συσκευή πρέπει να επαληθεύει την ψηφιακή υπογραφή. Τα χαρακτηριστικά του Blockchain μπορούν να βοηθήσουν στην αντιμετώπιση ορισμένων από τους περιορισμούς του PKI χρησιμοποιώντας το Keyless Security Infrastructure (KSI). Το KSI χρησιμοποιεί κρυπτογραφική λειτουργία κατακερματισμού, επιτρέποντας την επαλήθευση να βασίζεται μόνο στην ασφάλεια των λειτουργιών κατακερματισμού και στη διαθεσιμότητα ενός Blockchain. [18]

Social Media.

Όπως και στον χώρο της ψυχαγωγίας, όπου το YouTube, το SoundCloud, το Netflix κ.ά. ελέγχουν την κατανάλωση των χρηστών, καταναλώνουμε περιεχόμενο μέσα σε πλατφόρμες που έχουν επιτύχει μαζική απήχηση όπως Facebook, Instagram, Twitter, LinkedIn και Pinterest, μεταξύ άλλων. Τα κοινωνικά δίκτυα βασίζονται σε επιχειρηματικά μοντέλα τα οποία με τη σειρά τους βασίζονται σε διαφημίσεις, που παρουσιάζουν ένα σημαντικό μειονέκτημα: οι χρήστες, οι δημιουργοί και οι πλατφόρμες αντισταθμίζονται άνισα για τη συμμετοχή τους στην πλατφόρμα. Για παράδειγμα, ο Μπαράκ Ομπάμα παρήγαγε το πιο δημοφιλές tweet στην ιστορία του Twitter, αλλά δεν έλαβε καμία ανταμοιβή για αυτό. Με τη χρήση του ιδιωτικού μητρώου του Blockchain που παρέχει το Ethereum, οι εταιρείες μπορούν να παρακολουθήσουν καλύτερα την αλληλεπίδραση των χρηστών με το περιεχόμενο. Αυτό επιτρέπει την ποσοτικοποίηση της αξίας του χρήστη στο δίκτυο και επομένως μια πληρέστερη ιδέα για τον τρόπο με τον οποίο πρέπει οι χρήστες να αποζημιωθούν για τη δραστηριότητά τους. Παρόλο που αυτή η έννοια της εξάπλωσης του πλούτου σε όλο το δίκτυο είναι κάπως ριζική, υπάρχουν αρκετές προσπάθειες για να γίνει αυτό πραγματικότητα σε μια σειρά εφαρμογών. Ακολουθούν τρεις από τις πιο σημαντικές. [26-27]

Κατανάλωση περιεχομένου. Τα νομίσματα εντός εφαρμογών που υποστηρίζονται από την τεχνολογία Blockchain μπορούν βασικά να

αναδιαρθρώσουν τον τρόπο με τον οποίο οι χρήστες καταναλώνουν περιεχόμενο στα κοινωνικά δίκτυα.

Πρόσβαση στο Περιεχόμενο. Σε διάφορες χώρες, η κυβέρνηση μπορεί να αποκλείσει τους πολίτες από την πρόσβαση σε κοινωνικά μέσα και συγκεκριμένο περιεχόμενο, συμπεριλαμβανομένων ειδήσεων, μουσικής και πολλών άλλων. Παρόλο που τα δίκτυα VPN προσφέρουν μια λύση σε αυτούς τους περιορισμούς, οι κυβερνήσεις καταστέλλουν και αυτές τις υπηρεσίες. Η έννοια του αποκεντρωμένου περιεχομένου προσφέρει μια εναλλακτική λύση για την καταπολέμηση της λογοκρισίας στο Διαδίκτυο μέσω πρωτοκόλλων ανοιχτού κώδικα.

Αυθεντικότητα περιεχομένου. Μια εφαρμογή κοινωνικών μέσων ενημέρωσης για το Blockchain που έχει κερδίσει περισσότερη φήμη είναι η καταπολέμηση ψεύτικων ειδήσεων (fake news). Στις τελευταίες προεδρικές εκλογές των ΗΠΑ παρατηρήθηκε μια αύξηση στο επιτηδευμένο ψευδές περιεχόμενο σε ιστότοπους όπως το Facebook και το Twitter, το οποίο χρησιμοποιήθηκε για να επηρεάσει τα συναισθήματα και τις απόψεις των ψηφοφόρων. Οι προσπάθειες της πλατφόρμας για την επίλυση αυτού του προβλήματος έχουν επικεντρωθεί γύρω από τις συνεργασίες με ανεξάρτητους ελεγκτές γεγονότων. Μάλιστα, τέτοια συνεργασία για την επαλήθευση γεγονότων εγκαινίασε πρόσφατα το Facebook και στην Ελλάδα ερχόμενο σε συμφωνία με τον ιστότοπο «Ellinika Hoaxes» [28]. Αυτό που προσφέρει το Blockchain είναι μια πιθανή λύση που δεν απαιτεί τρίτους.

3.4 Σύνοψη πλεονεκτημάτων - μειονεκτημάτων Blockchain

Πλεονεκτήματα:

Αποδιαμεσολάβηση: τα δύο μέρη είναι σε θέση να κάνουν μια συναλλαγή χωρίς την επίβλεψη ή την διαμεσολάβηση ενός τρίτου μέρους.

Εξουσιοδοτημένοι χρήστες: οι χρήστες έχουν τον έλεγχο όλων των πληροφοριών και των συναλλαγών τους.

Αντοχή, αξιοπιστία και μακροζωία: λόγω των αποκεντρωμένων δικτύων, το Blockchain δεν έχει ένα κεντρικό σημείο αποτυχίας και είναι σε καλύτερη θέση να αντέξει σε κακόβουλες επιθέσεις. Επίσης, τα δεδομένα στο Blockchain είναι πλήρη, συνεπή, έγκυρα, ακριβή και ευρέως διαθέσιμα.

Ακεραιότητα της διαδικασίας: οι χρήστες μπορούν να εμπιστευθούν ότι οι συναλλαγές θα εκτελούνται όπως ακριβώς ορίζουν οι εντολές του πρωτοκόλλου, καταργώντας την ανάγκη για ένα έμπιστο τρίτο μέρος.

Διαφάνεια και αμεταβλητότητα: οι αλλαγές στο δημόσιο Blockchain είναι ορατές στο κοινό από όλα τα μέρη δημιουργώντας διαφάνεια, καθώς και όλες οι συναλλαγές είναι αμετάβλητες, που σημαίνει ότι δεν μπορούν να τροποποιηθούν ή να διαγραφούν.

Απλούστευση του οικοσυστήματος: όλες οι συναλλαγές προστίθενται σε ένα ενιαίο δημόσιο καθολικό (ledger), μειώνοντας έτσι τις επιπλοκές των πολλαπλών ledgers.

Ταχύτερες συναλλαγές: οι συναλλαγές σε μία τράπεζα μπορεί ενδεχομένως να χρειαστούν μέρες για την εκκαθάριση και τελική διευθέτηση, ιδίως εκτός του ωραρίου εργασίας. Οι συναλλαγές μέσω Blockchain μπορούν να μειώσουν το χρόνο συναλλαγής σε λεπτά αφού η επεξεργασία τους γίνεται άμεσα.

Χαμηλότερο κόστος συναλλαγών: με την εξάλειψη των μεσαζόντων τρίτων και των γενικών εξόδων για την ανταλλαγή περιουσιακών στοιχείων, τα Blockchains έχουν τη δυνατότητα να μειώσουν σημαντικά τα έξοδα συναλλαγής.

Μειονεκτήματα:

Εκκολαπτόμενη τεχνολογία: η επίλυση των προκλήσεων όπως η ταχύτητα των συναλλαγών, η διαδικασία επαλήθευσης, και τα όρια των δεδομένων θα είναι καθοριστικής σημασίας στο να γίνει το Blockchain ευρέως εφαρμόσιμο.

Αβέβαιο ρυθμιστικό καθεστώς: τα νομίσματα δημιουργούνται και ελέγχονται από τις εθνικές κυβερνήσεις και τις κεντρικές τράπεζες. Οι νέες τεχνολογίες

αντιμετωπίζουν εμπόδια στην ευρεία υιοθέτηση τους από τα προϋπάρχοντα χρηματοπιστωτικά ιδρύματα, εφόσον το ρυθμιστικό καθεστώς τους παραμένει ακαθόριστο.

Μεγάλη κατανάλωση ενέργειας: οι miners του Blockchain για το δίκτυο Bitcoin επιχειρούν 450.000 τρισεκατομμύρια λύσεις ανά δευτερόλεπτο για την επικύρωση των συναλλαγών, χρησιμοποιώντας σημαντικές ποσότητες ηλεκτρικής ενέργειας.

Έλεγχος, ασφάλεια και προστασία της ιδιωτικότητας: ενώ υπάρχουν λύσεις, συμπεριλαμβανομένων των ιδιωτικών Blockchains και ισχυρή κρυπτογράφηση, εξακολουθούν να υπάρχουν ανησυχίες στον κυβερνοχώρο για την ασφάλεια οι οποίες πρέπει να αντιμετωπιστούν πριν το ευρύ κοινό αναθέσει τα προσωπικά του δεδομένα σε ένα Blockchain.

Ανησυχίες ενσωμάτωσης: οι εφαρμογές Blockchain προσφέρουν λύσεις που απαιτούν σημαντικές αλλαγές, ή την πλήρη αντικατάσταση των υπαρχόντων συστημάτων. Για να πραγματοποιηθούν αυτές οι αλλαγές, οι εταιρείες πρέπει να καταστρώσουν σχέδια στρατηγικής για την μετάβαση. Το Blockchain αντιπροσωπεύει μια πλήρη στροφή προς ένα αποκεντρωμένο δίκτυο που απαιτεί την συμφωνία των χρηστών και των φορέων του.

Κόστος: Το Blockchain προσφέρει τεράστια εξοικονόμηση του κόστους, των συναλλαγών και του χρόνου, αλλά το υψηλό αρχικό κόστος κεφαλαίου θα μπορούσε να αποτελέσει αποτρεπτικό παράγοντα.

Συμπεραίνουμε λοιπόν πως, είτε έμμεσα, μέσω της προστασίας των πνευματικών δικαιωμάτων, είτε και άμεσα, με την αποτροπή ή έστω τον περιορισμό της διακίνησης πλαστών φαρμάκων, το Blockchain έχει πράγματι πολλά να προσφέρει προς όφελος της ανθρώπινης ζωής. Από τη στιγμή βέβαια που στον κόσμο δεν υπάρχουν μόνο αγνές προθέσεις και όπως οποιαδήποτε μορφή τεχνολογίας δεν είναι από μόνη της καλή ή κακή αλλά εξαρτάται από τη χρήση που κάνουν οι άνθρωποι, έτσι και η τεχνολογία Blockchain αν και από μόνη της δεν είναι επιβλαβής, μπορεί να γίνει, εφόσον οι χρήστες της είναι κακόβουλοι.

Κεφάλαιο 4

Η Νομική πλευρά

Το Blockchain, σαν κάθε τι καινούργιο, ενδεχομένως αρχικά να τρομάζει. Ο νόμος της αδράνειας μας ωθεί στο να αντιδράμε σε μεγάλες αλλαγές. Είναι το Blockchain απολύτως νόμιμο; Εμπίπτει σε κάποιον νόμο; Υπάρχουν νόμοι πάνω σε αυτό; Οι νόμοι που δημιουργήθηκαν αποκλειστικά για το Blockchain, αν και δεν είναι και πολλοί, τείνουν να είναι πρόχειροι, περιττοί και εξαιρετικά επαχθείς.

4.1 Η νομοθεσία στις Η.Π.Α.

Τουλάχιστον επτά πολιτείες έχουν θεσπίσει ή έχουν υιοθετήσει νόμους που αναφέρουν το Blockchain. Μεταξύ άλλων, η Αριζόνα, το Ντέλαγουερ, το Ιλινόις, η Νεβάδα, το Τεννεσί, το Βερμόντ και το Γουαϊόμινγκ. Επίσης, οκτώ πολιτείες τροποποίησαν τους νόμους περί αποστολής χρημάτων, οι οποίοι συνήθως καθορίζουν αυστηρές απαιτήσεις για εταιρείες όπως η Western Union που ασχολούνται με τις μεταφορές χρημάτων για την αντιμετώπιση κρυπτονομισμάτων από την 1η Μαρτίου 2018. Οι νόμοι των ΗΠΑ για το Blockchain κυμαίνονται από τη δημιουργία ομάδων εργασίας για να μελετήσουν την τεχνολογία όπως στο Τεννεσί, έως πιο ουσιαστικές πρωτοβουλίες όπως το διάταγμα του Γουαϊόμινγκ όπου ορισμένα κρυπτονομίσματα που εκδίδονται σε Blockchain δεν θα ρυθμίζονται από το νόμο περί κρατικών τίτλων. Όλοι όμως έχουν κοινό στόχο: να ενθαρρύνουν τις εταιρείες Blockchain να φέρουν τις υψηλά αμειβόμενες δουλειές τους στο κράτος. Σύμφωνα με την ιστοσελίδα CoinDesk, πάνω από 2,4 δισεκατομμύρια δολάρια σε κεφάλαια επιχειρηματικών συμμετοχών έχουν διοχετευθεί σε εταιρείες Blockchain από το 2012. Η τάση της νομοθέτησης του Blockchain γίνεται όλο και πιο έντονη στις ΗΠΑ. Μια αναζήτηση για το Blockchain στη βάση δεδομένων νομοθεσίας LegiScan

εμφανίζει πέντε νομοσχέδια που ήταν τελευταία φορά σε ισχύ το 2017 και άλλα 19 το 2018. Χαβάη, Νέα Υόρκη, Κολοράντο, Νεμπράσκα, Βερμόντ, Βιρτζίνια, Φλόριντα, Μέρυλαντ και η Βόρεια Ντακότα είναι μεταξύ των πολιτειών που εξετάζουν νομοσχέδια γύρω από Blockchain ή τα κρυπτονομίσματα. Ενώ και σε εθνικό επίπεδο βρίσκουμε 5 νομοσχέδια. [29]

Οι τεχνολογίες Blockchain εξακολουθούν να αντιμετωπίζουν σοβαρές προκλήσεις όσον αφορά την ευελιξία και την ασφάλεια, προκειμένου να είναι ανταγωνιστικές με τις συγκεντρωτικές βάσεις δεδομένων. Επιπλέον, υπάρχει μία παρεξήγηση σχετικά με το τι μπορεί να επιτελέσει η τεχνολογία. Ισχυρισμοί όπως ότι είναι «αμετάβλητο», «ασφαλές» και «αξιόπιστο» είναι αμφισβητήσιμοι καθώς αυτά τα χαρακτηριστικά ποικίλλουν σε μεγάλο βαθμό ανάλογα με τον τύπο του Blockchain και τον τρόπο εφαρμογής του. Ορισμένα πρώιμα έργα Blockchain έχουν αντιμετωπίσει εμπόδια καθώς οι προσδοκίες αντιμετωπίζουν την πραγματικότητα. Ορισμένα μεγάλα έργα στον χρηματοπιστωτικό τομέα έχουν σταματήσει. Το Βερμόντ εξέταζε ένα δημόσιο αρχείο καταγραφών με βάση το Blockchain, αλλά μια έκθεση διαπίστωσε ότι η αλλαγή θα είχε υψηλό κόστος και πολύ περιορισμένα πιθανά οφέλη. Ωστόσο, οι κυβερνήσεις έχουν φλερτάρει με εταιρίες Blockchain και σχετικές τεχνολογίες για δημόσιες υπηρεσίες. Στο Ιλινόις, το κράτος ανέλαβε ένα πιλοτικό έργο που έθεσε τα αρχεία της γης στο Blockchain του Bitcoin. Επίσης, το Ιλινόις, το Ντέλαγουερ και ο πάροχος Blockchain Hashed Health έκαναν μαζί μια παρουσίαση σχετικά με το «δυναμικό μετασχηματισμό της Medicaid». Ένα νομοσχέδιο στο Κολοράντο λέει ότι ο επικεφαλής της υπηρεσίας πληροφοριών ασφαλείας στο γραφείο του κυβερνήτη της τεχνολογίας των πληροφοριών είναι υποχρεωμένος να «αξιολογεί κάθε χρόνο τα συστήματα δεδομένων κάθε δημόσιου οργανισμού για τα οφέλη και το κόστος της υιοθέτησης και της εφαρμογής κατανεμημένων λογιστικών βιβλίων, όπως το Blockchain», ενώ η Αριζόνα και το Οχάιο πλέον επιτρέπουν στους κατοίκους να πληρώνουν φόρο εισοδήματος με Bitcoin. [30-33]

Το Γουαϊόμινγκ είναι το πιο επιθετικό στη ψήφιση νομοσχεδίων φιλικά προσκείμενων στο Blockchain, περνώντας πέντε νόμους και δηλώνοντας ότι οι μάρκες χρησιμότητας (utility tokens) δεν υπάγονται στους νόμους περί

κρατικών κινητών αξιών, εξαιρώντας κρυπτονομίσματα από τους φόρους εισοδήματος. [31]

Αυτά όσον αφορά τις Ηνωμένες Πολιτείες. Στη συνέχεια, μετά από μια σύντομη παρουσίαση της νομοθεσίες GDPR, θα δούμε τα νομικά θέματα που έχουν προκύψει στην Ευρώπη σχετικά με το Blockchain.

4.2 Η τεχνολογία Blockchain και ο νέος κανονισμός GDPR της Ε.Ε.

Ο νέος κανονισμός για την προστασία των δεδομένων (Regulation (EU) 2016/679), αποτελεί την τελευταία εξέλιξη σε μια σειρά νομοθετικών ρυθμίσεων της ΕΕ, «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών». [35]

Στο πλαίσιο της προστασίας των δικαιωμάτων των πολιτών της, η ΕΕ προχώρησε στην υιοθέτηση ενός αυστηρότερου πλαισίου για τη διαχείριση και τη διακίνηση των προσωπικών δεδομένων τους. Ο νέος γενικός κανονισμός για την προστασία των δεδομένων, αντικαθιστά την προηγούμενη σχετική οδηγία (Data Protection Directive 95/46/EC), ψηφίστηκε στις 14 Απριλίου του 2016 από το Ευρωπαϊκό Κοινοβούλιο και τέθηκε σε ισχύ στις 25 Μαΐου 2018. Η ισχύς του είναι άμεση σε όλες τις χώρες, χωρίς να υπάρχει ανάγκη για ψήφιση εφαρμοστικού νόμου εκ μέρους των κρατών μελών. [38]

Οι βασικές αλλαγές που προκύπτουν από την εφαρμογή του νέου κανονισμού είναι:

- Συνολική υποχρέωση εναρμόνισης.
- Αυξημένη διαφάνεια εσωτερικών διαδικασιών.
- Ορισμός Data Protection Officer (DPO).
- Υποχρέωση αναφοράς περιστατικών παραβίασης προστασίας δεδομένων.

- Ανάγκη ύπαρξης εσωτερικού μητρώου δεδομένων.
- Σαφής συγκατάθεση εκ μέρους των ατόμων.
- Αυξημένα δικαιώματα σε κάθε άτομο για διαγραφή και μεταβολή των προσωπικών του δεδομένων.
- Επιβολή υψηλών προστίμων (4% παγκόσμιου τζίρου ή €20 εκ. – όποιο είναι μεγαλύτερο).

Όλοι οι οργανισμοί οι οποίοι διατηρούν ή επεξεργάζονται προσωπικά δεδομένα ευρωπαίων πολιτών, ακόμα και αν βρίσκονται ή έχουν έδρα εκτός Ευρωπαϊκής Ένωσης, επηρεάζονται από την εφαρμογή του νέου κανονισμού. Ωστόσο, κάποιες δραστηριότητες θα επηρεαστούν σε μεγαλύτερο βαθμό λόγω της φύσης τους.

- Υπηρεσίες υγείας.
- Χρηματοοικονομικές υπηρεσίες.
- Υπηρεσίες ανθρώπινου δυναμικού.
- Υπηρεσίες φιλοξενίας και μετακινήσεων.
- Υπηρεσίες διαδικτυακών/προσωποποιημένων πωλήσεων.
- Παροχή τηλεπικοινωνιακών υπηρεσιών.
- Παροχή υπηρεσιών ενέργειας.
- Κρατικός τομέας.

Είναι σημαντικό να γίνει απολύτως κατανοητό πως δεν επηρεάζεται μόνο η Διεύθυνση Πληροφοριακών Συστημάτων από την εφαρμογή του νέου κανονισμού. Σε κάθε οργανισμό, οποιαδήποτε λειτουργία στην οποία χρησιμοποιούνται προσωπικά δεδομένα, σε οποιαδήποτε μορφή, επηρεάζονται εξίσου ή και σε μεγαλύτερο βαθμό. [34-35]

Ο νόμος περί ιδιωτικότητας (GDPR), ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου του 2018, μπορεί να αποτελέσει εμπόδιο στην υιοθέτηση του Blockchain στην ΕΕ. Ο νόμος αναφέρει ότι οι άνθρωποι πρέπει να μπορούν να απαιτούν την λήψη ή τη διαγραφή των προσωπικών τους δεδομένων υπό πολλές περιστάσεις. Ένα Blockchain είναι ουσιαστικά ένα αυξανόμενο, κοινό ιστορικό προηγούμενης δραστηριότητας που διανέμεται σε πολλούς υπολογιστές και το όλο θέμα είναι ότι αυτή η αλυσίδα συναλλαγών (ή άλλα τμήματα πληροφοριών) είναι στην

πράξη αμετάβλητη – αυτό εξασφαλίζει την αξιοπιστία των αποθηκευμένων πληροφοριών στο Blockchain. «Η εφαρμογή του Blockchain δεν συμβαδίζει απόλυτα με τις περισσότερες νομικές και κανονιστικές απαιτήσεις συμμόρφωσης που υπάρχουν και όσοι προσπαθούν να τηρήσουν τη συμμόρφωση σε αυτές είναι πιθανόν να μην συνειδητοποιούν όλα τα συναφή ζητήματα συμμόρφωσης», λέει ο Herold προσθέτοντας ότι «η επικύρωση της ασφάλειας και της ιδιωτικότητας του Blockchain δεν είναι μια απλή διαδικασία» [43]. «Ένα Blockchain είναι ουσιαστικά ένα κοινό ιστορικό δραστηριότητας που παραμένει αμετάβλητο», λέει ο John McLeod, επικεφαλής της Υπηρεσίας Ασφάλειας Πληροφοριών για το AlienVault.[43] «Τα ζητήματα ιδιωτικού απορρήτου που μπορεί να προκύψουν έγκεινται στον τρόπο με τον οποίο μια εταιρεία θα επεξεργάζεται τα δεδομένα αυτής της κοινόχρηστης εγγραφής και στα δικαιώματα των υποκειμένων των δεδομένων που εμπίπτουν στο GDPR, καθώς το κοινόχρηστο αρχείο δεν μπορεί να αλλάξει, τα δικαιώματα των υποκειμένων των δεδομένων είναι περιορισμένα» [36-37].

Για τα projects του Blockchain που αφορούν την αποθήκευση προσωπικών δεδομένων, αυτά τα δύο γεγονότα δεν συνδέονται καλά. Και με τις κυρώσεις για την παραβίαση του GDPR, συμπεριλαμβανομένων των προστίμων μέχρι 20 εκατ. ευρώ ή 4% των παγκόσμιων εσόδων, πολλές επιχειρήσεις μπορεί να βρουν την τάση προς το Blockchain πολύ λιγότερο ελκυστική από ότι πίστευαν αρχικά. «Το GDPR είναι αγνωστικιστής για το ποια συγκεκριμένη τεχνολογία χρησιμοποιείται για την επεξεργασία, αλλά εισάγει μια υποχρέωση για τους υπεύθυνους επεξεργασίας δεδομένων να εφαρμόζουν την αρχή της προστασίας δεδομένων από το σχεδιασμό» δήλωσε ο Jan Filip Albrecht, μέλος του Ευρωπαϊκού Κοινοβουλίου [36]. «Αυτό σημαίνει για παράδειγμα ότι τα δικαιώματα του υποκειμένου των δεδομένων μπορούν εύκολα να ασκηθούν, συμπεριλαμβανομένου του δικαιώματος διαγραφής δεδομένων όταν δεν είναι πλέον αναγκαία. Πάνω σε αυτό είναι που οι εφαρμογές Blockchain θα αντιμετωπίσουν προβλήματα και πιθανόν να μην είναι συμβατές με το GDPR» [36]. Η αλλαγή δεδομένων απλά δεν λειτουργεί σε ένα Blockchain, δήλωσε ο John Mathews, ο επικεφαλής χρηματοοικονομικός υπάλληλος για το Bitnation, ένα έργο που αποσκοπεί στην παροχή υπηρεσιών ταυτότητας και

διακυβέρνησης βασισμένων σε Blockchain, καθώς και αποθήκευσης εγγράφων. «Το Blockchain είναι από τη φύση του αμετάβλητο. Το GDPR λέει ότι πρέπει να είστε σε θέση να αφαιρέσετε κάποια δεδομένα, οπότε αυτά τα δύο πράγματα δεν συνδέονται» [36-37].

Υπάρχουν δύο κύριοι τύποι Blockchain: ιδιωτικά ή «εξουσιοδοτημένα» Blockchain που βρίσκονται υπό τον έλεγχο μιας περιορισμένης ομάδας (όπως το Blockchain Ripple που έχει σχεδιαστεί για να διευκολύνει τις πληρωμές μεταξύ παρόχων χρηματοπιστωτικών υπηρεσιών), και δημόσια ή «αόριστα» Blockchain που δεν βρίσκονται υπό τον έλεγχο κανενός (όπως τα δίκτυα Bitcoin ή Ethereum). Είναι τεχνικά δυνατό να ξαναγράψουμε τα δεδομένα που διατηρούνται σε ένα Blockchain, αλλά μόνο αν οι περισσότεροι κόμβοι στο δίκτυο συμφωνούν να δημιουργήσουν μια νέα έκδοση του Blockchain που περιλαμβάνει τις αλλαγές – και στη συνέχεια να συνεχίσουν να χρησιμοποιούν αυτή την έκδοση και όχι την πρωτότυπη. Αυτό είναι σχετικά εύκολο σε ένα ιδιωτικό Blockchain, αν όχι ιδανικό, αλλά σε ένα δημόσιο Blockchain είναι ένα εξαιρετικά σπάνιο γεγονός. Τουλάχιστον δεδομένου ότι η τεχνολογία έχει σχεδιαστεί, επί του παρόντος υπάρχουν λίγα ή καθόλου περιθώρια για τον καθορισμό ή την αφαίρεση δυαδικών ψηφίων πληροφοριών εδώ και εκεί σε συνεχή βάση. «Από τη σκοπιά του Blockchain, το GDPR είναι ήδη ξεπερασμένο», δήλωσε ο Mathews. «Ο κανονισμός παίζει κυνηγητό με την τεχνολογία. Το GDPR γράφτηκε υποθέτοντας ότι έχετε συγκεντρωτικές υπηρεσίες που ελέγχουν τα δικαιώματα πρόσβασης στα δεδομένα του χρήστη, το οποίο είναι το αντίθετο από αυτό που κάνει το Blockchain» [36-37].

Η Jutta Steiner, που είναι η ιδρυτής της Parity.io, μιας start-up που αναπτύσσει αποκεντρωμένες τεχνολογίες, και πρώην επικεφαλής ασφαλείας του Ethereum, συμφωνεί με τον Mathews ότι «το GDPR χρειάζεται μια σωστή αναθεώρηση». «Μου φαίνεται ότι συντάχθηκε προσπαθώντας να εφαρμόσει μια συγκεκριμένη προοπτική για τον τρόπο με τον οποίο ο κόσμος πρέπει να είναι, χωρίς να λαμβάνει υπόψη τον τρόπο με τον οποίο λειτουργεί η τεχνολογία», δήλωσε η Steiner [36]. «Ο τρόπος με τον οποίο λειτουργεί η αρχιτεκτονική του δημόσιου αποκεντρωμένου δικτύου σημαίνει ότι δεν μπορεί να υπάρχει η διαγραφή των προσωπικών δεδομένων. Το ζήτημα των πληροφοριών είναι όταν βγουν έξω,

είναι έξω. Λαμβάνοντας υπόψη το στάδιο όπου βρίσκεται η τεχνολογία, νομίζω ότι υπάρχει χρόνος να προσαρμοστούν ορισμένα πράγματα στο GDPR» και πρόσθεσε, «Δεν μπορώ να καταλάβω γιατί οι ρυθμιστικές αρχές είναι τόσο επίμονες ώστε να μην προσαρμόσουν τον κανονισμό. Απλά θα δουν μόνο ότι οι άλλες χώρες θα χρησιμοποιήσουν την τεχνολογία και η Ευρώπη βρίσκεται σε μειονεκτική θέση» [36]. Αυτό φαίνεται απίθανο να συμβεί σύντομα. Το GDPR είναι ένας νέος κανονισμός και οι νόμοι της ΕΕ τείνουν να διαρκούν πολύ καιρό πριν από την αναθεώρηση τους. Η οδηγία για την προστασία των δεδομένων που προηγήθηκε της GDPR συντάχθηκε το 1995. «Ορισμένες τεχνολογίες δεν θα είναι συμβατές με το GDPR αν δεν προβλέπουν βάσει του αρχιτεκτονικού τους σχεδιασμού», τόνισε ο Albrecht. «Αυτό δεν σημαίνει ότι η τεχνολογία Blockchain γενικά πρέπει να προσαρμοστεί στο GDPR, σημαίνει απλά ότι δεν μπορεί να χρησιμοποιηθεί για την επεξεργασία προσωπικών δεδομένων. Αυτή η απόφαση είναι ευθύνη κάθε οργανισμού που επεξεργάζεται τα προσωπικά δεδομένα» [36-37].

Η σύγκρουση μεταξύ της τεχνολογίας GDPR και Blockchain έχει λάβει λίγη προσοχή μέχρι στιγμής. Η Ευρωπαϊκή βάση δεδομένων αποτελούσε, μέχρι πρόσφατα, ένα έργο που αποσκοπούσε στην οικοδόμηση ενός συστήματος βασισμένου σε Blockchain, όπου οι κόμβοι του δικτύου είχαν προεπιλεγεί. Θα μπορούσε να στείλει συναλλαγές στο δίκτυο ή να διαβάσει τα δεδομένα που είναι αποθηκευμένα σε αυτό. Σύμφωνα με τον συνιδρυτή του Ιδρύματος IPDB, δικηγόρο Greg McMullen, η έδρα του Βερολίνου είχε πλήρη επίγνωση των προβλημάτων που θέτει το GDPR. Ένα πρόβλημα ήταν η αδυναμία να τροποποιήσει ή να διαγράψει δεδομένα αποθηκευμένα σε ένα Blockchain. Αλλά υπήρχε και άλλο ζήτημα. «Το GDPR γράφεται για ένα μοντέλο υπηρεσιών Cloud. Έστω ότι έχω μια start-up επιχείρηση και συλλέγω τα δεδομένα παραγγελίας εστιατορίων και τα αποθηκεύω όλα στην Amazon Web Services που φιλοξενεί τα δεδομένα για μένα, οπότε πρέπει να έχω μια σύμβαση με την Amazon που μεταβιβάζει τις υποχρεώσεις μου σε αυτούς», δήλωσε ο McMullen [36]. «Λειτουργεί πολύ καλά όταν υπάρχουν ένας ή δύο πάροχοι, αλλά όταν αρχίζει να υπάρχει ένα αποκεντρωμένο δίκτυο, καταρρέει εξ ολοκλήρου. Δεν είναι εφικτό να υπογράφονται συμβόλαια με όλους τους κόμβους του δικτύου Ethereum.

Επομένως, ποιος είναι υπεύθυνος για την προστασία των δεδομένων σε ένα αποκεντρωμένο δίκτυο; Εξάλλου, ένα από τα μεγάλα κατορθώματα τέτοιων δικτύων είναι ότι είναι ανθεκτικά στη λογοκρισία, επειδή δεν υπάρχει κεντρικό σώμα - ούτε το Amazon ή το Facebook - για τους υπεύθυνους επιβολής του νόμου, καθώς και επειδή οι κόμβοι ή οι χρήστες που απαρτίζουν το δίκτυο είναι διάσπαρτοι στον κόσμο» [36]. Σύμφωνα με τον Albrecht, εάν πρόκειται για ιδιωτικό Blockchain, η συμμόρφωση με το GDPR είναι ευθύνη του οργανισμού που την αναπτύσσει. «Για αποκεντρωμένες και δημόσιες εφαρμογές Blockchain, θα ήταν ευθύνη του κάθε χρήστη που βάζει δεδομένα προσωπικού χαρακτήρα στο κατανεμημένο βιβλίο για να διασφαλίσει ότι αυτό είναι συμβατό με GDPR. Που στις περισσότερες περιπτώσεις δεν θα είναι», δήλωσε ο βουλευτής [36]. Το ζήτημα της ευθύνης θα φοβίσει πολλές επιχειρήσεις εκτός χρήσης Blockchain, προειδοποιεί ο McMullen. «Είναι αλήθεια ότι οι κανονισμοί θα πρέπει να καλύψουν την τεχνολογία, αλλά πρέπει να είμαστε ρεαλιστές για το γεγονός ότι το GDPR είναι ένα πραγματικό πράγμα και συμβαίνει και θα υπάρξει επιβολή του. Όταν ζητείται από τις εταιρείες να χρησιμοποιούν Blockchains, δεν πρόκειται να αναλάβουν αυτόν τον κίνδυνο με τα δεδομένα των πελατών τους» [36]. Σύμφωνα με τον McMullen, το Ίδρυμα IPDB εργάστηκε σε διάφορες ιδέες για την αντιμετώπιση του προβλήματος της προστασίας δεδομένων. Το ένα ήταν ένα σύστημα «μαύρης λίστας» ορισμένων δεδομένων, έτσι ώστε ακόμη και αν δεν διαγράφηκαν από το δίκτυο όταν αυτό ήταν απαραίτητο, δεν θα λαμβάνονται όταν ζητηθεί.

Μια άλλη ιδέα ήταν να βάλουμε μόνο τα hashes των προσωπικών δεδομένων στο Blockchain, παρά τα ίδια τα δεδομένα. Τα hashes είναι μαθηματικές παραδοχές δεδομένων που, εάν εφαρμοστούν σωστά, δεν μπορούν να αντιστραφούν για να εκθέσουν τα δεδομένα που αντιπροσωπεύουν, αλλά μπορούν να χρησιμοποιηθούν για την επαλήθευση των δεδομένων, επαναλαμβάνοντας τον αλγόριθμο κατακερματισμού σε αυτά τα δεδομένα και συγκρίνοντας το αποτέλεσμα με το αποθηκευμένο hash. Με ένα Blockchain από hashes, αντί για τα ίδια τα δεδομένα, μπορεί να είναι δυνατή η διαγραφή των δεδομένων χωρίς να χρειαστεί αλλαγή του Blockchain. Με αυτόν τον τρόπο, το

Blockchain μπορεί να καταφέρει να είναι χρήσιμο για την επαλήθευση των δεδομένων ενώ παραμένει συμβατό με GDPR, πρότεινε ο McMullen [36].

Είναι πιθανό οι ρυθμιστικές αρχές να σταθούν εμπόδιο στην ανάδυση της νέας αυτής τάσης; Ο McMullen, δήλωσε ότι οι πρώτοι στόχοι επιβολής του νόμου πιθανότατα θα είναι «οι συνήθεις ύποπτοι - οι Google, Facebook, Amazon», αλλά θα μπορούσε να είναι πολύ εύκολο για μια ρυθμιστική αρχή να αποφασίσει να κάνει το ίδιο σε μια εταιρεία που ασχολείται με το Blockchain. «Καθώς οι εταιρείες αρχίζουν να κατανοούν τις συνέπειες του GDPR, θα μπορούσαμε να δούμε μια πραγματική κίνηση για να προσαρμοστούν στους νόμους, συλλέγοντας λιγότερα δεδομένα και χρησιμοποιώντας τα δεδομένα με τρόπο που να μην τα εκθέτει στο δημόσιο διαδίκτυο, όπως για παράδειγμα με hashes» δήλωσε ο McMullen. «Με τον τρόπο αυτό, η τεχνολογία μπορεί να προσαρμόζεται στον νόμο όπως και ο νόμος να προσαρμόζεται στην τεχνολογία. Θα μπορούσε τελικά να είναι πολύ καλό για την ιδιωτικότητα των χρηστών» [36-38].

Βλέπουμε λοιπόν, πως αναλόγως το καθεστώς, τις υπάρχουσες αρχές και διατάξεις και τους αντίστοιχους νόμους, η ίδια τεχνολογία μπορεί να αντιμετωπιστεί διαφορετικά από κάθε σκοπιά. Ο νόμος φαίνεται άλλοτε να είναι στο πλευρό του Blockchain και άλλοτε αντιμέτωπός του.

Κεφάλαιο 5

Ζητήματα ιδιωτικότητας

Όπως έχει προαναφερθεί, οι συζητήσεις σχετικά με την τεχνολογία Blockchain φαίνεται να είναι παντού, με πιθανές εφαρμογές που καλύπτουν ποικίλες βιομηχανίες όπως τραπεζική, υγειονομική περίθαλψη, ακίνητη περιουσία, επιβολή του νόμου, ψυχαγωγία μέχρι ακόμη και πωλήσεις κρασιού και κοσμημάτων. Οι διαφορετικές εφαρμογές του Blockchain παρουσιάζουν διαφορετικές και μοναδικές προκλήσεις και ευκαιρίες για την ασφάλεια των δεδομένων και την ιδιωτική ζωή, αλλά υπάρχουν και θέματα που απασχολούν τους εμπειρογνώμονες νομικού απορρήτου. Εδώ παρουσιάζονται τα τρία μεγαλύτερα εξ' αυτών, χωριζόμενα σε κατηγορίες. Το πρώτο περιλαμβάνει την αναγκαία γέφυρα μεταξύ του φυσικού κόσμου και του κυβερνοχώρου. Το δεύτερο περιλαμβάνει ευαίσθητες πληροφορίες που αποθηκεύονται στο Blockchain, και το τρίτο αφορά την ίδια την ύπαρξη του Blockchain. [39]

5.1 Πρόβλημα ιδιωτικότητας: Γέφυρα μεταξύ φυσικού κόσμου και κυβερνοχώρου

Η γέφυρα μεταξύ φυσικού κόσμου και κυβερνοχώρου αναφέρεται στην έννοια ότι όταν ένα πρόσωπο αλληλεπιδρά στον κυβερνοχώρο, το κάνει μέσω ενός ηλεκτρονικού αναγνωριστικού. Για παράδειγμα, εάν θέλετε να αλληλεπιδράσετε με τους χρήστες στο Facebook, πρέπει να δημιουργήστε ένα όνομα χρήστη και να συνδεθείτε ώστε το δίκτυο του Facebook να γνωρίζει ποιοι είστε. Το ίδιο ισχύει και για οποιαδήποτε ηλεκτρονική αλληλεπίδραση, είτε πρόκειται για τραπεζικές συναλλαγές, αγορά εισιτηρίων συναυλιών ή για λήψη μουσικής, δηλαδή προκειμένου να λάβετε μέρος σε μια συναλλαγή, πρέπει να υπάρξει κάποια σύνδεση μεταξύ εσάς και του ηλεκτρονικού σας αναγνωριστικού. Το αναγνωριστικό μπορεί να είναι ψευδώνυμο (π.χ. ένας τραπεζικός λογαριασμός ή

μια διεύθυνση ηλεκτρονικού ταχυδρομείου που δεν έχει ένα πραγματικό όνομα συνδεδεμένο με αυτό), αλλά σε κάποιο σημείο πρέπει να υπάρχει κάποια γέφυρα μεταξύ του φυσικού κόσμου και του κυβερνοχώρου. Επί του παρόντος, αυτή η γέφυρα επιτυγχάνεται κυρίως μέσω συνδυασμών ονόματος χρήστη και κωδικού πρόσβασης, μερικές φορές με την προσθήκη διαδικασιών επαλήθευσης πολλαπλών σταδίων. Εντούτοις, στο εγγύς μέλλον, είναι πιθανό τα βιομετρικά αναγνωριστικά να αντικαταστήσουν τα ονόματα χρήστη και τους κωδικούς πρόσβασης ως μέσο διέλευσης της γέφυρας αυτής. Ένα πρόβλημα με αυτό το σύστημα είναι ότι, προκειμένου ένα φυσικό πρόσωπο να μπορέσει να συνδεθεί σε ένα δίκτυο, το δίκτυο πρέπει να έχει ένα αντίγραφο των διαπιστευτηρίων σύνδεσης αυτού του ατόμου σε συνδυασμό με το ηλεκτρονικό αναγνωριστικό αυτού του ατόμου. Σε ένα συγκεντρωτικό σύστημα, αυτά τα διαπιστευτήρια πρέπει να αποθηκεύονται μόνο σε ένα μέρος (π.χ. στους κεντρικούς διακομιστές του Facebook ή στην τράπεζά σας). Σε ένα δίκτυο Blockchain, αυτά τα διαπιστευτήρια θα αποθηκεύονται σε όλους τους κόμβους που περιέχουν τα Blockchains με τα οποία θέλετε να αλληλεπιδράσετε, μερικά από τα οποία ενδέχεται να παραβιάζονται ευκολότερα από ότι σε έναν ασφαλή κεντρικό διακομιστή. Αυτό αφορά ιδιαίτερα τα βιομετρικά στοιχεία ταυτοποίησης, τα οποία, όταν παραβιάζονται από κλέφτες ταυτότητας, δεν μεταβάλλονται εύκολα. Ενσωματώνοντας αυτή την ανησυχία, είναι γεγονός ότι, όπως θα συζητηθεί παρακάτω, η φύση ενός Blockchain σημαίνει ότι όλες οι πληροφορίες που αποθηκεύονται σε ένα Blockchain παραμένουν αποθηκευμένες καθώς πρόσθετα μπλοκ προστίθενται στην αλυσίδα, πράγμα που σημαίνει ότι ευαίσθητες προσωπικές πληροφορίες μπορούν να αποθηκευτούν στον κυβερνοχώρο για πάντα.

Ένα άλλο ζήτημα είναι ότι, ελλείψει μιας ισχυρής κεντρικής εξουσίας, μπορεί να είναι δύσκολο να αποτραπεί η πρόσβαση των hackers σε ευαίσθητες πληροφορίες μόλις τεθούν σε κίνδυνο τα διαπιστευτήρια σύνδεσης ενός ατόμου. Για παράδειγμα, αν κάποιος χτυπήσει τον τραπεζικό λογαριασμό σας ή κλέψει τα στοιχεία της πιστωτικής σας κάρτας, μπορείτε να καλέσετε την τράπεζά σας και να ενημερώσετε τα στοιχεία σύνδεσής σας ή να ακυρώσετε την παλιά πιστωτική σας κάρτα. Σε ένα δίκτυο Blockchain χωρίς ισχυρή κεντρική εξουσία,

μπορεί να είναι δύσκολο να ενημερώσετε τα διαπιστευτήριά σας σύνδεσης και ακόμη και για έναν hacker να σας αποκλείσει ενημερώνοντας τα διαπιστευτήρια μόλις αποκτήσει πρόσβαση. Όχι μόνο η πιθανότητα hacking αυτών των ευαίσθητων πληροφοριών είναι προβληματική από την άποψη της ασφάλειας, αλλά δημιουργεί επίσης αβεβαιότητα σχετικά με το ποιος, αν κάποιος, είναι υπεύθυνος για την ειδοποίηση ατόμων εάν τα διαπιστευτήριά τους σύνδεσης έχουν διαρρεύσει. Τα περισσότερα κράτη έχουν περάσει νόμους σχετικούς με την κοινοποίηση παραβιάσεων των δεδομένων, οι οποίοι απαιτούν από τους θεματοφύλακες των ευαίσθητων προσωπικών δεδομένων να ειδοποιούν τους ίδιους, εάν διακυβεύονται τα δεδομένα τους. Σε αυτό το σημείο δεν είναι σαφές πώς αυτοί οι νόμοι θα εφαρμοστούν σε ένα κατανεμημένο δίκτυο όπως το Blockchain. [40]

5.2 Πρόβλημα απορρήτου: Πληροφορίες που εισέρχονται είτε εξέρχονται από το Blockchain

Ορισμένα από τα δεδομένα που θα αποθηκευτούν στα Blockchain θα είναι ιδιαίτερα ευαίσθητα. Τα δίκτυα Blockchain εξετάζονται επί του παρόντος ως μέσα καταγραφής και ενημέρωσης των αρχείων ιατροφαρμακευτικής περίθαλψης, γονιδιωματικών ακολουθιών και βιομετρικών διαπιστευτηρίων. Ενώ οι ευαίσθητες πληροφορίες που αποθηκεύονται στο Blockchain θα είναι κρυπτογραφημένες, λόγω της κατανεμημένης φύσης του Blockchain, οι hackers ενδέχεται να στοχεύσουν εκείνους τους συγκεκριμένους κόμβους που για τεχνικό ή άλλο λόγο μπορούν να παραβιάζονται ευκολότερα και να έχουν πρόσβαση στις κρυπτογραφημένες πληροφορίες. Η ανησυχία αυτή επιδεινώνεται όταν πρόκειται για κυβερνητικά απασχολούμενους hackers, οι οποίοι μπορούν να επωφεληθούν από τη φυσική θέση των κόμβων σε χώρες όπου οι πληροφορίες είναι πιο ευάλωτες, ή όπου οι νόμοι είναι ανεπαρκείς για να αποτρέψουν τέτοια φαινόμενα. Ενώ οι κίνδυνοι της προστασίας της ιδιωτικής ζωής μπορούν να μετριαστούν με τη λειτουργία σε κλειστά δίκτυα, υπάρχουν οφέλη για το άνοιγμα δικτύων που θα απαιτήσουν τουλάχιστον

ορισμένα Blockchain που περιέχουν ευαίσθητες πληροφορίες να λειτουργούν σε δίκτυα που δεν είναι τελείως κλειστά. Μια άλλη ανησυχία για τα ανοιχτά δίκτυα είναι ότι, ακόμη και αν οι πληροφορίες είναι κρυπτογραφημένες, ευαίσθητες πληροφορίες μπορούν να συλλεχθούν. Για παράδειγμα, εάν δύο μεγάλες τράπεζες συμμετέχουν σε μεγάλο όγκο συναλλαγών μεταξύ τους σε σύντομο χρονικό διάστημα, οι πληροφορίες αυτές μπορούν να παραβιαστούν από άλλες τράπεζες ή ιδιώτες οι οποίοι μπορούν να δουν τις συναλλαγές, ακόμη και αν δεν μπορούν να δουν τις λεπτομέρειες των ίδιων των συναλλαγών. Σε πιο προσωπικό επίπεδο, εάν ένας γιατρός έχει πρόσβαση στα αρχεία υγείας ενός ασθενούς για να κάνει αλλαγές, ένας κακόβουλος χρήστης μπορεί να δει τη συγκεκριμένη συναλλαγή εάν γνωρίζει τα ηλεκτρονικά αναγνωριστικά στοιχεία του γιατρού και του ασθενούς. Ο hacker δεν θα μπορέσει να δει τα αρχεία υγείας ή τι άλλαξε χωρίς να αποκτήσει πρόσβαση και να αποκρυπτογραφήσει τα αρχεία, μπορεί όμως να συμπεράνει ότι ο ασθενής είδε έναν συγκεκριμένο γιατρό σε συγκεκριμένη ημερομηνία, πληροφορίες που ο ασθενής μπορεί να επιθυμεί να κρατήσει κρυφές. Εξίσου προβληματικό είναι το γεγονός ότι, σε αυτό το σημείο, δεν είναι σαφές ποιος, αν μπορεί κάποιος, να είναι νομικά υπεύθυνος στην περίπτωση που έχουμε παραβίαση αυτών των πληροφοριών. [40]

5.3 Πρόβλημα απορρήτου: Φύση του Blockchain – Μόνιμα αρχεία

Μία από τις μεγάλες προκλήσεις που αντιμετωπίζει η ιδιωτικότητα στον 21ο αιώνα είναι η κατάσταση που δημιουργείται από τον συνδυασμό της προόδου στη διατήρηση δεδομένων και στις δυνατότητες αναζήτησης δεδομένων. Καθώς δημιουργούμε όλο και περισσότερα δεδομένα για τη ζωή μας και καθώς αυτά τα δεδομένα καταγράφονται και καθίστανται εύκολα ανακτήσιμα, τα δεδομένα γίνονται αιώνια και ορατά στο ευρύ κοινό με τρόπο που δεν υπήρξε ποτέ πριν. Η τεχνολογία Blockchain είναι πιθανό να επιταχύνει αυτή την τάση. Ένα από τα πλεονεκτήματα που προσφέρει το Blockchain είναι ότι καταγράφει όλες τις

συναλλαγές, επιτρέποντας σχεδόν τέλεια διατήρηση αρχείων. Καθώς οι τύποι των συναλλαγών που αποθηκεύονται σε Blockchains αυξάνονται, έτσι θα αυξάνονται και τα αρχεία για κάθε μία από αυτές τις συναλλαγές. Στο μέλλον, είναι πιθανό κάθε συναλλαγή η οποία πραγματοποιείται να αποθηκεύεται σε ένα Blockchain και να μην υφίσταται κανένας έλεγχος σχετικά με το πού αποθηκεύονται αυτές οι πληροφορίες ή πώς χρησιμοποιούνται. Οι ανησυχίες περί ιδιωτικότητας και οι νόμοι που εμπλέκονται σε αυτά τα μόνιμα αρχεία είναι πολυάριθμα. Το απλό γεγονός ότι υπάρχουν τέτοια αρχεία θα μπορούσε να δημιουργήσει προβλήματα για όποιον δεν θέλει να υπάρχει πλήρης καταγραφή όλων των συναλλαγών του για πάντα. Επιπλέον, αυτή τη στιγμή δεν υπάρχει σαφής συμφωνία ως προς το ποιος κατέχει τις πληροφορίες που περιέχονται σε αυτά τα αρχεία ως νομικό θέμα. Είναι πιθανό τα δίκτυα Blockchain να είναι σε θέση να πωλούν τις πληροφορίες που περιέχονται σε αυτά τα αρχεία χωρίς οποιαδήποτε συναίνεση από τα άτομα που περιέχονταν στις συναλλαγές και τα άτομα αυτά δεν θα έχουν καμία διέξοδο. Ελλείψει σαφών κανόνων ιδιοκτησίας, ενδέχεται επίσης να είναι δυνατή η πρόσβαση των κυβερνητικών φορέων και ιδιωτών σε αυτά τα δεδομένα χωρίς τη συγκατάθεση των ατόμων που συμμετέχουν στη συναλλαγή. Στα Blockchains με αδύναμη ή κεντρική αρχή, τα αλλοιωμένα δεδομένα που μπαίνουν στην αλυσίδα μπορεί να είναι αδύνατο να διορθωθούν. [40]

5.4 Ιδιωτικότητα και ανωνυμία στο Blockchain

Το παραδοσιακό τραπεζικό σύστημα επιτυγχάνει ένα επίπεδο ιδιωτικότητας μέσω της περιορισμένης πρόσβασης στα δεδομένα συναλλαγών στις οντότητες που εμπλέκονται άμεσα σε αυτές και τον εκάστοτε διαμεσολαβητή (τράπεζα). Από την άλλη, με τα Bitcoins το δημόσιο Blockchain αποκαλύπτει όλη την πληροφορία που σχετίζεται με τις συναλλαγές σε καθένα συνδεδεμένο χρήστη στο δίκτυο. Ωστόσο, η ιδιωτικότητα μπορεί να διατηρηθεί ως ένα επίπεδο διακόπτοντας την ροή της πληροφορίας σε κάποιο ενδιάμεσο σημείο της αλυσίδας. Το Bitcoin το επιτυγχάνει αυτό διατηρώντας ανώνυμα τα δημόσια

κλειδιά. Όλοι μπορούν να δουν ότι κάποιος αποστέλλει ένα ποσό σε κάποιον άλλον, χωρίς όμως να υπάρχει κάποια πληροφορία που να συνδέει τη συναλλαγή με κάποιον συγκεκριμένα. Για την περαιτέρω βελτίωση της ιδιωτικότητας των χρηστών, συνιστάται η χρήση ενός νέου ζεύγους κλειδιών για κάθε συναλλαγή προς αποφυγή σύνδεσής της με έναν συγκεκριμένο χρήστη.

Ωστόσο, η σύνδεση είναι ακόμα δυνατή σε συναλλαγές πολλαπλών εισροών, οι οποίες αναγκαστικά αποκαλύπτουν ότι οι εισροές ανήκαν στον ίδιο ιδιοκτήτη. Επίσης, αν ο ιδιοκτήτης ενός κλειδιού αποκαλυφθεί, υπάρχει ο κίνδυνος η σύνδεση να αποκαλύψει άλλες συναλλαγές που ανήκουν στον ίδιο χρήστη. Συγκεκριμένα, τα Bitcoin προσφέρουν μερική μη-συνδεσιμότητα (δηλαδή ψευδωνυμία), και έτσι είναι δυνατή η σύνδεση ορισμένων συναλλαγών με ένα άτομο-χρήστη με τον εντοπισμό της ροής χρημάτων μέσω μιας ισχυρής διαδικασίας ανάλυσης Blockchain.

5.5 Προτάσεις και τεχνικές για την ενίσχυση της ιδιωτικότητας και της ανωνυμίας

Η ιδιωτικότητα δεν ορίζεται ως εγγενής ιδιότητα στον αρχικό σχεδιασμό του Bitcoin, αλλά συνδέεται στενά με το σύστημα. Ως εκ τούτου, τα τελευταία χρόνια ήρθαν στην επιφάνεια διάφορες αδυναμίες που σχετίζονται με την προστασία της ιδιωτικότητας στο τρέχον πρωτόκολλο του Bitcoin. Σαν συνέπεια, αναπτύχθηκαν τεχνολογίες διασφάλισης της ιδιωτικότητας με στόχο την ενίσχυση αυτής και τη βελτίωση της ανωνυμίας, χωρίς ταυτόχρονα να θίγονται οι βασικές αρχές σχεδιασμού του Bitcoin. Σε αυτή την ενότητα, συζητάμε αυτά τα πρωτόκολλα τελευταίας τεχνολογίας τα οποία κατευθύνονται προς την ενίσχυση της ιδιωτικότητας και της ανωνυμίας στο Bitcoin. Είναι προφανές ότι η δημόσια φύση του Blockchain θέτει μια σημαντική απειλή για το απόρρητο των χρηστών του Bitcoin. Ακόμη χειρότερα, καθώς τα χρήματα μπορούν να εντοπιστούν και να «μολυνθούν», δεν υπάρχουν δύο ίσα νομίσματα και η εμπορευσιμότητα, μια βασική ιδιότητα που απαιτείται σε κάθε νόμισμα, κινδυνεύει. Με αυτές τις απειλές κατά νου, έχουν προταθεί πολλές τεχνολογίες

βελτίωσης της προστασίας της ιδιωτικότητας στα πλαίσια συναλλαγών στο Bitcoin. Οι τελευταίες τάσεις-προτάσεις της τεχνολογίας (παρουσιάζονται επιγραμματικά στους πίνακες 1 & 2 παρακάτω) για την διασφάλιση της ιδιωτικότητας στις συναλλαγές με κρυπτονομίσματα μπορούν να ταξινομηθούν ευρέως σε τρεις σημαντικές κατηγορίες: Πρωτόκολλα Ανάμιξης Peer-to-Peer (P2P), Κατανεμημένα Πρωτόκολλα και Altcoins. [41-42]

5.5.1 Πρωτόκολλα ανάμειξης Peer-to-Peer

Οι «αναμεικτήρες» (mixers) είναι ανώνυμοι πάροχοι υπηρεσιών, που χρησιμοποιούν ανάμεικτα πρωτόκολλα για να συγχέουν τις διαδρομές συναλλαγών. Στη διαδικασία ανάμειξης, τα κεφάλαια του πελάτη είναι χωρισμένα σε μικρότερα τμήματα. Αυτά τα μέρη αναμιγνύονται τυχαία με παρόμοια τυχαία τμήματα άλλων πελατών, και καταλήγουν να δημιουργούνται εντελώς νέα νομίσματα. Αυτό βοηθά να εξαλειφθεί η οποιαδήποτε σύνδεση μεταξύ του χρήστη και των κερμάτων που αγόρασε. Ωστόσο, οι mixers δεν είναι ένα αναπόσπαστο μέρος του Bitcoin, αλλά διάφορες υπηρεσίες ανάμειξης χρησιμοποιούνται σε μεγάλο βαθμό για την ενίσχυση της ανωνυμίας και της μη-συνδεσιμότητας στο σύστημα. Στα πρωτόκολλα ανάμειξης Peer-to-Peer ένα σύνολο μη αξιόπιστων χρηστών του Bitcoin ταυτόχρονα μεταδίδουν τα δικά τους μηνύματα για να δημιουργηθεί μια σειρά συναλλαγών χωρίς να απαιτείται κάποιο αξιόπιστο τρίτο μέρος. Το κύριο χαρακτηριστικό ενός P2P πρωτοκόλλου ανάμειξης είναι η διασφάλιση της ανωνυμίας του αποστολέα στο σύνολο των συμμετεχόντων μέσω μεταβίβασης της κυριότητας των κερμάτων τους. Στόχος είναι η αποτροπή ενός εισβολέα ο οποίος ελέγχει ένα μέρος του δικτύου ή ορισμένους συμμετέχοντες χρήστες να συσχετίσει μια συναλλαγή με τον αντίστοιχο αξιόπιστο αποστολέα. Ο βαθμός ανωνυμίας στα P2P πρωτόκολλα εξαρτάται από τον αριθμό των χρηστών στο σετ ανωνυμίας. Ο πίνακας 1 παρακάτω δείχνει μια σειρά πρωτοκόλλων ανάμιξης P2P μαζί με τη σύντομη περιγραφή τους, τα πλεονεκτήματα και τα μειονεκτήματά τους ως προς την ανωνυμία του χρήστη και την ασφάλεια των συναλλαγών.

Το CoinJoin, ένα απλό πρωτόκολλο για την εφαρμογή ανάμειξης P2P, στοχεύει στην ενίσχυση της ιδιωτικότητας και στην αποτροπή των κλοπών. Η βασική

ιδέα του CoinJoin έγκειται στο ότι δύο συναλλαγές ενώνονται σε μία ενώ οι εισροές και οι εκροές παραμένουν αμετάβλητες. Στο CoinJoin, ένα σύνολο χρηστών με συμφωνημένες (μέσω πρωτογενών υπογραφών) εισροές και εκροές δημιουργούν μια τυποποιημένη συναλλαγή Bitcoin, ώστε κανένας εξωτερικός παράγοντας να μην γνωρίζει ποιοι σύνδεσμοι εξόδου αντιστοιχούν σε ποια εισροή. Κατ' αυτόν τον τρόπο διασφαλίζει την εξωτερική του μη-συνδεσιμότητα. Προς αποφυγήν κλοπής, ένας χρήστης υπογράφει μια συναλλαγή μόνο εάν η επιθυμητή έξοδος της εμφανίζεται στις διευθύνσεις εξόδου της συναλλαγής. Με αυτό τον τρόπο, το CoinJoin καθιστά τις πολλαπλές εισόδους μιας συναλλαγής ανεξάρτητες τη μία από την άλλη και έτσι, οι εισροές μιας συναλλαγής ανήκουν πλέον στον ίδιο χρήστη. Ωστόσο, το CoinJoin έχει μερικά σημαντικά μειονεκτήματα, τα οποία περιλαμβάνουν την περιορισμένη επεκτασιμότητα καθώς και κενά ασφάλειας και ιδιωτικότητας λόγω της ανάγκης διαχείρισης υπογραφών των εμπλεκόμενων συμμετεχόντων στο σύνολο ανάμιξης. Επιπλέον, η υποχρέωση υπογραφής μιας συναλλαγής από όλους τους συμμετέχοντες μπορεί να καταστήσει το CoinJoin ευάλωτο σε επιθέσεις DoS (άρνησης υπηρεσίας) αναγκάζοντας κάθε συμμετέχοντα να μοιράζεται την υπογραφή και τις διευθύνσεις εξόδου με το υπόλοιπο σύνολο, ενέργεια που προκαλεί εσωτερική μη-συνδεσιμότητα. [42-43]

Για να αντιμετωπιστεί το ζήτημα της εσωτερικής μη-συνδεσιμότητας και για να αυξηθεί η ανθεκτικότητα στις επιθέσεις DoS, προτείνεται το CoinShuffle, ένα αποκεντρωμένο πρωτόκολλο που συντονίζει CoinJoin συναλλαγές χρησιμοποιώντας μια τεχνική κρυπτογραφικής ανάμειξης. Αργότερα, μια σειρά από πρωτόκολλα χτίστηκαν πάνω στη βάση του CoinJoin ή του CoinShuffle, γεγονός που ενισχύει την ανάμειξη P2P παρέχοντας πολλές βελτιώσεις, περιλαμβάνοντας την αντοχή έναντι επιθέσεων DoS, επιθέσεων κλοπής ταυτότητας και επιθέσεων διασταύρωσης, χαμηλό χρόνο ανάμειξης και επεκτασιμότητα των ομάδων ανάμειξης. [42-43]

5.5.2 Κατανεμημένα δίκτυα ανάμειξης

Από αυτήν την κατηγορία προτείνεται το MixCoin, ένα πρωτόκολλο ανάμειξης τρίτων για τη διασφάλιση της ανωνυμίας σε πληρωμές με Bitcoin και παρόμοια

κρυπτονομίσματα. Το MixCoin χρησιμοποιεί το αναδυόμενο φαινόμενο των συνδυασμών νομισμάτων, στην οποία ένας χρήστης μοιράζεται έναν αριθμό κερμάτων με έναν τρίτο, χρησιμοποιώντας μια συναλλαγή κανονικού μεγέθους και παίρνει πίσω τον ίδιο αριθμό κερμάτων από το μείγμα που υποβάλλεται από κάποιον άλλο χρήστη, ως εκ τούτου παρέχει ισχυρή ανωνυμία από εξωτερικές καταχωρήσεις. Ωστόσο, τα κέρματα χρηστών ενδέχεται να υποκλαπούν ανά πάσα στιγμή ή να αποτελέσουν απειλή για την ανωνυμία του χρήστη, επειδή το σύνολο θα γνωρίζει την εσωτερική χαρτογράφηση μεταξύ των χρηστών και των εξόδων. Για την επίτευξη εσωτερικής μη-συνδεσιμότητας στο MixCoin, προτείνεται το BlindCoin που επεκτείνει το πρωτόκολλο MixCoin χρησιμοποιώντας τυφλές υπογραφές για τη δημιουργία εισόδων χρήστη και κρυπτογραφικά τυφλές εξόδους που ονομάζονται τυφλές μάρκες (blinded tokens). Ωστόσο, για να επιτευχθεί αυτή η εσωτερική μη-συνδεσιμότητα, το BlindCoin απαιτεί δύο επιπλέον συναλλαγές για τη δημοσίευση και την εξαργύρωση των blinded tokens. Παρόλα αυτά ο κίνδυνος υποκλοπής παραμένει. [44]

Πρόσφατα προτάθηκε το TumbleBit, ένα μη κατευθυνόμενο κέντρο πληρωμών με δυνατότητα μη συνδεσιμότητας και συμβατό με Bitcoin, που επιτρέπει στους χρήστες να πραγματοποιούν ανώνυμα πληρωμές χωρίς χρέωση μέσω ενός μη αξιόπιστου διαμεσολαβητή που ονομάζεται Tumbler. Παρόμοιο με το αρχικό πρωτόκολλο eCash του Chaumian, το TumbleBit ενισχύει την ανωνυμία εξασφαλίζοντας ότι κανείς, ούτε καν το Tumbler, δεν μπορεί να συνδέσει μια συναλλαγή του αποστολέα με τον παραλήπτη του. Η ανάμειξη των πληρωμών από 800 χρήστες δείχνει ότι το TumbleBit παρέχει ισχυρή ανωνυμία και αντίσταση στην κλοπή και φαίνεται να έχει καλές προοπτικές. [44]

Ο Πίνακας 1 παρακάτω δείχνει μια σειρά πρωτοκόλλων ανάμιξης P2P μαζί με τη σύντομη περιγραφή τους, τα πλεονεκτήματα και τα μειονεκτήματά τους ως προς την ανωνυμία του χρήστη και την ασφάλεια των συναλλαγών.

Ονομασία	Τύπος-Κατηγορία	Χαρακτηριστικά	Πλεονεκτήματα	Μειονεκτήματα
CoinJoin	P2P	uses multisignature transactions to enhance privacy	prevent thefts, lower per transaction fee	anonymity level depends on the number of participants, vulnerable to DoS (by stalling joint transactions), Sybil and intersection attacks, prevents plausible deniability
CoinShuffle	P2P	decentralized protocol for coordinating CoinJoin transactions through a cryptographic mixing protocol	internal unlinkability, robust to DoS attacks, theft resistance	lower anonymity level and deniability, prone to intersection and Sybil attacks
Xim	P2P	anonymously partnering and multiround mixing	distributed pairing, internal unlinkability, prevents sybil and DoS attacks	higher mixing time
CoinShuffle++ DiceMix	P2P	based on CoinJoin concept, optimal P2P mixing solution to improve anonymity in cryptocurrencies	low mixing time (8" for 50 peers), resistant to deanonymization attack, ensures sender anonymity and termination	vulnerable to DoS and Sybil attacks, limited scalability, no support for Confidential Transactions (CT)
ValueShuffle	P2P	based on CoinShuffle++ concept, uses Confidential Transactions mixing approach to achieve comprehensive transaction privacy	unlinkability, CT compatibility and theft resistance, normal payment using ValueShuffle needs only one transaction	vulnerable to DoS and Sybil attacks, limited scalability

Dandelion	P2P	networking policy to prevent network facilitated deanonymization of Bitcoin users	provides strong anonymity even in the presence of multiple adversaries	vulnerable to DoS and Sybil attacks
SecureCoin	P2P	based on CoinParty concept, an efficient and secure protocol for anonymous and unlinkable Bitcoin transactions	protect against sabotage attacks, attempted by any number of participating saboteurs, low mixing fee, deniability	vulnerable to DoS attacks, limited scalability
CoinParty	Partially P2P	based on CoinJoin concept, uses threshold ECDSA and decryption mix-nets to combine pros of centralized and decentralized mixes in a single system	improves on robustness, anonymity, scalability and deniability, no mixing fee	partially prone to coin theft and DoS attack, high mixing time, requires separate honest mixing peers
MixCoin	Distributed	third-party mixing with accountability	DoS and Sybil resistance	partial internal unlinkability and theft resistance
BlindCoin	Distributed	based on MixCoin concept, uses blind signature scheme to ensure anonymity	internal unlinkability, DoS and Sybil resistance	partial theft resistance, additional costs and delays in mixing process
TumbleBit	Distributed	undirectional unlinkable payment hub that uses an untrusted intermediary	prevents theft, anonymous, resists intersection, Sybil and DoS, scalable (implemented with 800 users)	normal payment using TumbleBit, needs at least two sequential transactions

Source: A Survey on Security and Privacy Issues of Bitcoin[44]

Πίνακας 1: Πρωτόκολλα ανάμιξης P2P

5.5.3 Bitcoin επεκτάσεις ή Altcoins

Το Bitcoin δεν είναι μόνο το δημοφιλέστερο κρυπτονόμισμα στη σημερινή αγορά, αλλά έχει ανοίξει το δρόμο για ένα κύμα άλλων κρυπτονομισμάτων που χτίζονται σε αποκεντρωμένα δίκτυα ομότιμων χρηστών. Στην πραγματικότητα, το Bitcoin έχει γίνει το de facto πρότυπο, το σημείο αναφοράς θα μπορούσαμε να πούμε, για τα άλλα κρυπτονομίσματα. Τα άλλα νομίσματα που εμπνέονται από το Bitcoin είναι γνωστά ως Altcoins. Υπάρχουν δύο τύποι Altcoins [46]:

- Altcoins που δημιουργούνται με βάση το πρωτότυπο πρωτόκολλο ανοιχτού κώδικα Bitcoin, με πολλές αλλαγές στον υποκείμενο κώδικα. Ουσιαστικά πρόκειται για νέα coins με διαφορετικό σύνολο χαρακτηριστικών. Ένα παράδειγμα τέτοιου Altcoin είναι το Litecoin.
- Altcoins που δεν βασίζονται στο πρωτόκολλο ανοιχτού κώδικα Bitcoin, αλλά έχουν δικό τους πρωτόκολλο και κατανεμημένο ledger. Γνωστά παραδείγματα τέτοιων Altcoins είναι τα Ethereum και Ripple.

Αντί να προτείνουν τεχνικές (όπως ανάμειξη και ανακατεύθυνση) για την ενίσχυση της ιδιωτικότητας και της ανωνυμίας στις συναλλαγές των χρηστών, τα Altcoins λειτουργούν ως επέκταση του Bitcoin είτε ως ένα πλήρες νόμισμα. Τα δημοφιλή Altcoins μαζί με τη συνοπτική τους περιγραφή παρουσιάζονται στον Πίνακα 2 που παρατίθεται παρακάτω. Ορισμένα από αυτά τα νομίσματα είναι ευκολότερο να εξορυχτούν από το Bitcoin, ωστόσο υπάρχει αντιστάθμισμα, συμπεριλαμβανομένου του μεγαλύτερου κινδύνου που προκαλείται από τη μικρότερη ρευστότητα, αποδοχή και διατήρηση αξίας. Επίσης προτείνεται το ZeroCoin, μια κρυπτογραφική επέκταση του Bitcoin που παρέχει ανωνυμία από το σχεδιασμό του εφαρμόζοντας αποδείξεις μηδενικής γνώσης που επιτρέπουν την επικύρωση των πλήρως κρυπτογραφημένων συναλλαγών. Πιστεύεται ότι αυτή η νέα ιδιοκτησία θα μπορούσε να επιφέρει τη δημιουργία εξ ολοκλήρου νέων κατηγοριών Blockchain. Στο ZeroCoin, ένας χρήστης μπορεί απλώς να κρύψει τα ίχνη σύνδεσης από τα νομίσματά του ανταλλάσσοντάς τα με μια ίση τιμή των ZeroCoins. [44]

Παρακάτω παρουσιάζονται επιγραμματικά δημοφιλή AltCoins.

Ονομασία	**Χαρακτηριστικά & Ιδιότητες**	**Πλεονεκτήματα**	**Μειονεκτήματα**
ZeroCoin / ZeroCash / Zcash	a cryptographic extension to Bitcoin, unlinkable and untraceable transactions by using zero knowledge proofs	provides internal unlinkability, theft and DoS resistance	relies on a trusted setup and non-falsifiable cryptographic assumptions, Blockchain pruning is not possible
CryptoNote	relies on ring signatures to provide anonymity	provides strong privacy and anonymity guarantees	higher computational complexity, not compatible with pruning
MimbleWimble	a design for a cryptocurrency with confidential transactions	CT compatibility, improve privacy, fungibility and scalability	vulnerable to DoS attacks, not compatible with smart contracts
ByzCoin	Bitcoin-like cryptocurrency with strong consistency via collective signing	lower consensus latency and high transaction throughput, resistance to selfish and stubborn mining [8], eclipse and delivery-tampering and double-spending attacks	vulnerable to slow down or temporary DoS attack and 51% attack,
Ethereum (ETH)	uses proof-of-stake, open-ended decentralized software platform that enables Smart Contracts and Distributed Applications	run without any downtime, fraud, control or interference from a third party, support developers to build and publish distributed applications	scalability issues (uses complex network), running untrusted code, limited (i.e., non-turing-complete) scripting language
Mastercoin (or Omni)	uses enhanced Bitcoin Core ad Proof of Authenticity, Colored coins, Exodus address	Easy to use, secure web wallets available, Escrow fund (insurance against panic), Duress protection using a trusted entity	wallets handling the transactions should aware of the concept of colored coins, possibility to acciden-tally uncolor colored coin assets exists
Litecoin (LTC, lite-coin.org)	uses Segwit, which allows technologies like Lightning Network	scalable, low transaction mining time, anonymous and cheaper	very few stores accept payment in Litecoins, high power consumption
Dash (DASH, dash-pay.io)	uses Proof of Service, implements native CoinJoin like transactions	higher privacy (mixes transactions using master nodes), InstantX provides faster transaction processing	less liquid, technology is too young, does not yet have a critical mass of merchants or users
Ripple (XRP, ripple.com)	implements a novel low-latency consensus algorithm based on byzantine agreement protocol	fast transaction validation, less energy-intensive, no 51% attack	not fully decentralized, vulnerable to attacks such as consensus split, transaction flood and software backdoor

Monero (XMR, get-monero.org)	based on the CryptoNote protocol,	improves user privacy by using ring signatures, lower transaction pro-cessing time (average every 2 minutes)	transaction linkability could be achieved by leveraging the ring signature size of zero, output merging, temporal analysis
Counterparty (XCP, counterparty.io)	created and distributed by destroying Bitcoins in a process known as *proof of burn*	same as Bitcoins	same as Bitcoins
			Source: A Survey on Security and Privacy Issues of Bitcoin[44]

Πίνακας 2: Δημοφιλή AltCoins

Σε αντίθεση με τις προαναφερθείσες προσεγγίσεις, ο χρήστης δεν θα πρέπει να ζητήσει την ανταλλαγή σε ένα σύνολο ανάμιξης, αντί αυτού ο χρήστης μπορεί να παράγει ο ίδιος ZeroCoins αποδεικνύοντας ότι κατέχει την ίδια αξία σε Bitcoins μέσω του πρωτοκόλλου ZeroCoin. Για παράδειγμα, κάποιος μπορεί να αποδείξει σε άλλους ότι κατέχει ένα Bitcoin και ως εκ τούτου είναι επιλέξιμος για να ξοδέψει οποιοδήποτε άλλο Bitcoin. Για το σκοπό αυτό, πρώτα παράγεται μια ασφαλής δέσμευση, δηλαδή το ZeroCoin, η οποία καταγράφεται στο Blockchain έτσι ώστε οι άλλοι να το επικυρώσουν. Για να ξοδέψει κάποιος ένα Bitcoin, μεταδίδει μια απόδειξη μηδενικής γνώσης για το αντίστοιχο ZeroCoin μαζί με μια συναλλαγή. Η κρυπτογραφία μηδενικής γνώσης προστατεύει από τη σύνδεση του ZeroCoin με τον κάτοχο του. Επιπλέον, οι άλλοι συμμετέχοντες μπορούν να επαληθεύσουν τη συναλλαγή και την απόδειξη. Αντί μιας συνδεδεμένης λίστας συναλλαγών Bitcoin, το ZeroCoin εισάγει ενδιάμεσα στάδια. Με αυτόν τον τρόπο, η χρήση των αποδείξεων μηδενικής γνώσης αποτρέπουν τις αναλύσεις γραφημάτων συναλλαγών. Δυστυχώς, παρόλο που οι ιδιότητες του ZeroCoin μπορεί να φαίνονται ελκυστικές, είναι υπολογιστικά πολύπλοκες, υπερφορτώνουν το Blockchain και απαιτούν τροποποιήσεις πρωτοκόλλου. Ωστόσο, αποδεικνύει την ύπαρξη μιας εναλλακτικής προσέγγισης για την προστασία της ιδιωτικότητας. Επί του παρόντος, το ZeroCoin έρχεται πρώτο τόσο ως προς την ανωνυμία όσο και ως προς την ασφάλεια κατά της παραποίησης / απομίμησης, χαρακτηριστικά τα οποία βέβαια αποκτά έναντι υψηλού κόστους υπολογιστικής πολυπλοκότητας και μεγέθους. [42-45]

Μια επέκταση του ZeroCoin που ονομάζεται ZeroCash (επίσης γνωστή ως Zcash) χρησιμοποιεί μια βελτιωμένη έκδοση απόδειξη μηδενικής γνώσης (όσον

αφορά τη λειτουργικότητα και αποτελεσματικότητα) που αποκαλείται zk-SNARK, η οποία επιπλέον αποκρύπτει πληροφορίες σχετικές με συναλλαγές όπως το ποσό και οι διευθύνσεις του παραλήπτη, για την επίτευξη ισχυρών εγγυήσεων απορρήτου. Το ZeroCash βασίζεται σε μια αξιόπιστη εγκατάσταση για τη δημιουργία μυστικών παραμέτρων που απαιτούνται για την υλοποίηση του SNARK, απαιτεί τροποποιήσεις πρωτοκόλλου και παρεμποδίζει το κλάδεμα του Blockchain. Πρόσφατα, προτάθηκε επίσης το MimbleWimble, ένα AltCoin που υποστηρίζει εμπιστευτικές συναλλαγές (confidential transactions - CT). Τα CTs μπορούν να συγκεντρωθούν μη-αλληλεπιδραστικά και ακόμη και διαμέσου blocks, κι έτσι αυξάνουν σημαντικά την επεκτασιμότητα του υποκείμενου Blockchain. Ωστόσο, αυτή η συγκέντρωση από μόνη της δεν εξασφαλίζει μη-συνδεσιμότητα εισόδου-εξόδου έναντι των μερών που εκτελούν τη συσσωμάτωση, π.χ. οι miners. Επιπλέον, το MimbleWimble δεν είναι συμβατό με τα Smart Contracts εξαιτίας της έλλειψης γραφής υποστήριξης (Script). [42-45]

Πέρα από το Bitcoin, η λεγόμενη δεύτερη γενιά κρυπτονομισμάτων, όπως τα Ethereum (Ether), Mastercoin (MSC), Counterparty (XCP), Ripple (XRP), Stellar (XLM) κ.α., έχει εισαχθεί στην αγορά. Αυτά τα κρυπτονομίσματα υλοποιούν μια νέα σύνταξη συναλλαγών βασισμένη στη γλώσσα Turing και καλύπτοντας τους τομείς των Smart Contracts και Colored Coins. Σε αντίθεση με το Bitcoin, το Ethereum σχεδιάστηκε για να είναι κάτι πολύ περισσότερο από ένα σύστημα πληρωμών. Συγκεκριμένα, πρόκειται για μια αποκεντρωμένη πλατφόρμα που τρέχει έξυπνες συμβάσεις (Smart Contracts), οι οποίες είναι οι εφαρμογές που τρέχουν ακριβώς όπως έχουν προγραμματιστεί χωρίς καμία πιθανότητα διακοπής, λογοκρισίας, απάτης ή παρεμβολής τρίτων. Αυτό υπονοεί ότι αυτά τα ψηφιακά περιουσιακά στοιχεία μπορούν να χρησιμοποιηθούν για την πραγματοποίηση εξελιγμένων χρηματοπιστωτικών συναλλαγών όπως τα αποθέματα με αυτόματες αποπληρωμές μερισμάτων ή για τη διαχείριση και το εμπόριο φυσικών ιδιοκτησιών όπως ένα σπίτι. Όπως και το Ripple, το Stellar είναι ένα κατανεμημένο πρωτόκολλο ανοιχτού κώδικα. Δημιουργήθηκε το 2014 από έναν από τους ιδρυτές του Ripple. Στόχος του είναι να συνδέσει τους ανθρώπους με χρηματοπιστωτικές υπηρεσίες χαμηλού κόστους για την καταπολέμηση της φτώχειας και την ανάπτυξη. Το Stellar υποστηρίζει τις

έξυπνες συμβάσεις και έχει δικό του ειδικό πρωτόκολλο συναίνεσης. Το κρυπτονόμισμα που βασίζεται στο Stellar είναι το Lumen (XLM). Τα Lumens χρησιμοποιούνται για συναλλαγές στο δίκτυο Stellar και συμβάλλουν στην μεταφορά χρημάτων σε όλο τον κόσμο και στη γρήγορη και ασφαλή διεξαγωγή συναλλαγών μεταξύ διαφορετικών νομισμάτων. [46] Όπως και το Ethereum, το Cardano έχει σχεδιαστεί ως πλατφόρμα στην οποία μπορούν να εκτελεστούν έξυπνες συμβάσεις και αποκεντρωμένες εφαρμογές (dApps). Το Cardano ξεκίνησε το 2015 και κυκλοφόρησε 2017. Βασίζεται στον αλγόριθμο Ouroboros και φιλοξενεί το αποκεντρωμένο ανοιχτού κώδικα κρυπτονόμισμα Ada (ADA) το οποίο λειτουργεί όπως το Ether για την αποστολή και λήψη κεφαλαίων. Το Cardano στοχεύει στη βελτίωση της επεκτασιμότητας, της ασφάλειας και της διαλειτουργικότητας στη σχέση με τους παραδοσιακούς χρηματοπιστωτικούς θεσμούς, μέσω της εμπειρίας που αντλείται από τις κοινότητες Bitcoin και Ethereum. Το Cardano σχεδιάστηκε από μια ομάδα κορυφαίων ακαδημαϊκών και μηχανικών, ενώ το Ada (ADA) μπορεί να αποθηκευτεί μόνο στο δικό του ψηφιακό πορτοφόλι Daedalus. [46] Παρόμοια λειτουργία έχει και το NEO αφού είναι ανοιχτού κώδικα και υποστηρίζει smart contract και dApps. Ξεκίνησε το 2014 και πολλές φορές αναφέρεται ως το «Κινέζικο Ethereum». [46]

Στον πίνακα 3 παρουσιάζονται κρυπτονομίσματα με βάση επτά κύρια χαρακτηριστικά τα οποία είναι τα εξής:

- Ανοιχτό ή όχι πρωτόκολλο.
- Αποκεντρωμένο ή όχι.
- Αρχική έκδοση από συγκεκριμένο άτομο ή οντότητα.
- Ηλεκτρονική διαπραγμάτευση.
- Απευθείας μετατρέψιμο σε φυσικό νόμισμα.
- Δυνατότητα χρήσης για αγορές.
- Επίπεδο ανωνυμίας.

Ονομασία	**Permissionless (1) / Permissioned (2)**	**Decentralized**	**IO by an identifiable person or entity**	**Electronically traded**	**Directly convertible into fiat currency**	**Medium of exchange**	**Pseudoanonymous (1) /Anonymous (2)**
Bitcoin	1	Ναι	Όχι	Ναι	Ναι	Ναι	1
Ethereum	1	Ναι	Ναι	Ναι	Ναι	Ναι	1
Ripple	2	Ναι	Ναι	Ναι	Ναι	Ναι	1
BTC Cash	1	Ναι	Όχι	Ναι	Ναι	Ναι	1
Litecoin	1	Ναι	Όχι	Ναι	Ναι	Ναι	1
Stellar	1	Ναι	Ναι	Ναι	Ναι	Μερικώς	1
Cardano	1 & 2	Ναι	Ναι	Ναι	Ναι	Μερικώς	1
IOTA	1	Ναι	Ναι	Ναι	Μερικώς	Όχι	1
NEO	2	Ναι	Ναι	Ναι	Μερικώς	Όχι	1
Monero	1	Ναι	Όχι	Ναι	Ναι	Ναι	2
Dash	1	Ναι	Όχι	Ναι	Ναι	Ναι	2

Source: Cryptocurrencies and blockchain TAX3 committee study[46]

Πίνακας 3: Ταξινόμηση κρυπτονομισμάτων

Τα περισσότερα από αυτά τα νομίσματα επόμενης γενιάς λειτουργούν βασιζόμενα σε Bitcoins Blockchain και ως εκ τούτου είναι επίσης γνωστά ως on-chain νομίσματα. Δεδομένου ότι κωδικοποιούν τις συναλλαγές τους σε Bitcoins συναλλαγές, αυτές δεν επικυρώνονται από miners , επειδή οι miners του Bitcoin δεν κατανοούν τους νέους τύπους συναλλαγών. Για το σκοπό αυτό, ένα νέο στρώμα πρωτοκόλλου έχει χτιστεί επάνω στην ισχυρή βάση και την ασφάλειά του Bitcoin. Επιπλέον, θεωρείται ως μια αύξηση στην τιμή Bitcoins από την οποία και οι δύο αποκομίζουν κέρδος. Τα Bitcoins χρησιμοποιούν ουσιαστικά την ψευδωνυμία καθώς οι λογαριασμοί συνδέονται με τυχαίες και πολλαπλές διευθύνσεις Bitcoin και όχι με τους ίδιους τους χρήστες ως πρόσωπα. Με την ταχύτατη δημοτικότητα που έχουν αποκτήσει τα Bitcoins η ανάγκη για προστασία της ιδιωτικότητας και της ανωνυμίας κρίνεται όλο και πιο επιτακτική. Είναι απαραίτητο να επιτευχθεί σε ικανοποιητικά επίπεδα για τους χρήστες η διασφάλιση της ιδιωτικότητας, της ασφάλειας και της ανωνυμίας τους. [42-45]

Κεφάλαιο 6

Ζητήματα ιδιωτικότητας - Πρωτόκολλο Enigma

Στην ενότητα αυτή μελετάται το πρωτόκολλο Enigma με σκοπό την διερεύνηση του τρόπου με τον οποίο αντιμετωπίζει τα ζητήματα ιδιωτικότητας που χαρακτηρίζουν τις πλατφόρμες Blockchain. Στη μελέτη αναλύονται και περιγράφονται τα συστατικά στοιχεία του πρωτόκολλου καθώς και η αρχιτεκτονική υλοποίησης του. Ιδιαίτερη αναφορά γίνεται στη στον τρόπο εκτέλεσης των υπολογισμών μιας και στην ουσία είναι η καινοτομία που αξιοποιείται για την διασφάλιση τη ιδιωτικότητας των δεδομένων. Τέλος περιγράφεται συνοπτικά η υλοποίηση Enigma catalyst η οποία και αποτελεί την πρώτη ουσιαστική εφαρμογή του πρωτοκόλλου.

6.1 Το πρωτόκολλο Enigma

Το Blockchain αποτελεί μια από τις τελευταίες σημαντικότερες εξελίξεις στον χώρο της τεχνολογίας και αναμένεται να επιφέρει σημαντικές αλλαγές σε τομείς όπως η οικονομία οι μεταφορές και η επικοινωνία. Η σημαντικότερη αλλαγή που επιφέρει είναι ότι πλέον καταργείται πλήρως η ανάγκη για έμπιστο τρίτο ο οποίος θα επικυρώνει την κάθε είδους ηλεκτρονική συναλλαγή. Με βάση το γεγονός αυτό, αλλά και μιας σειράς άλλων πλεονεκτημάτων αναμένεται ευρύτατη ανάπτυξη και υιοθέτηση του Blockchain τα επόμενα χρόνια. Ωστόσο, το Blockchain υποφέρει από δύο θεμελιώδη προβλήματα - αυτά της ιδιωτικής ζωής και της επεκτασιμότητας και στο σημείο αυτό είναι που εμφανίζεται το πρωτόκολλο Enigma.

Η πρώτη εμφάνιση του πρωτοκόλλου Enigma έγινε ως αποτέλεσμα σχετικής έρευνα στο MIT όπου στην επιστημονική δημοσίευση [47] περιλαμβανόταν μια θεωρητική προσέγγιση/προτεινόμενη λύση γύρω από την αντιμετώπιση ζητημάτων ιδιωτικότητας τα οποία χαρακτήριζαν τις διάφορες υλοποιήσεις Blockchain [48]. Όπως αναφέρεται, είναι αδύνατη μια ευρεία αποδοχή και

εξέλιξη τεχνολογικών λύσεων με βάση το Blockchain εφόσον δεν επιλυθούν τα βασικά ζητήματα ιδιωτικότητας. Ειδικότερα σε περιβάλλοντα κρυπτονομισμάτων (Bitcoin) ή εκτέλεσης έξυπνων συμβολαίων (Smart Contracts) όπως το Ethereum που διαθέτουν σοβαρά πλεονεκτήματα όπως η ασφάλεια των συναλλαγών και η αποκεντρωμένη αρχιτεκτονική αναμένεται να φέρουν επανάσταση στον τρόπο που σχεδιάζονται οι ηλεκτρονικές εφαρμογές το πρόβλημα της ιδιωτικότητας είναι ακόμα μεγαλύτερο.

Αρχικά θα πρέπει να αναφερθεί ότι το Enigma παρουσιάστηκε ως πρωτόκολλο μιας και στην αρχική δημοσίευση περιλαμβάνεται ένα σύνολο προδιαγραφών και παραμέτρων όπως το αρχιτεκτονικό μοντέλο η επικοινωνία μεταξύ των κόμβων, το υπολογιστικό μοντέλο και η αποθήκευση των δεδομένων. Στη συνέχεια οι ίδιοι επιστήμονες υλοποίησαν εφαρμογές με βάση το πρωτόκολλο καθώς επίσης και κρυπτονόμισμα στο οποίο θα πληρώνεται η αμοιβή τους αφού στην τελική του έκδοση το Enigma αποτελεί πλέον μια υποδομή υπηρεσιών ιδιωτικότητας και επεκτασιμότητας στον Blockchain.

Το πρωτόκολλο Enigma όπως προαναφέρθηκε έκανε την εμφάνισή του σε θεωρητικό/ερευνητικό επίπεδο περιγράφεται ως ένα αποκεντρωμένο και κατανεμημένο δίκτυο κόμβων (nodes), οι οποίοι με χρήση μυστικών συμβάσεων (secret contracts), είναι σε θέση να υπολογίζουν τα δεδομένα με τρόπο που διατηρείται η εμπιστευτικότητα και η ακεραιότητα τους. Ως στόχος δημιουργίας του πρωτοκόλλου Enigma αναφέρεται η παροχή της δυνατότητας σε προγραμματιστές να χτίζουν ολοκληρωμένες, αποκεντρωμένες εφαρμογές με την προστασία της ιδιωτικότητας να είναι ενσωματωμένη ήδη κατά τον σχεδιασμό και χωρίς την παρουσία έμπιστου τρίτου μέρους. Συνοπτικά το πρωτόκολλο Enigma το χαρακτηρίζουν[47]:

Η διασφάλιση της ιδιωτικότητας: με τη χρήση του υπολογιστικού μοντέλου ασφαλούς υπολογισμού πολλαπλών συμβαλλομένων (Secure multi-party computation, sMPC), τα διάφορα ερωτήματα ή υπολογισμοί επί των δεδομένων εκτελούνται κατανεμημένα χωρίς την ανάγκη ύπαρξης αξιόπιστου τρίτου μέρους. Τα δεδομένα κατανέμονται μεταξύ διαφορετικών κόμβων και εκτελούνται υπολογισμοί χωρίς να διαρρέουν πληροφορίες σε άλλους κόμβους. Συγκεκριμένα, κανένας κόμβος δεν έχει ποτέ πρόσβαση στα συνολικά δεδομένα

παρά μόνο στο τμήμα των δεδομένων που του έχει διανεμηθεί. Στο σημείο αυτό θα πρέπει να αναφερθεί ότι αρχική έκδοση testnet του Enigma παρέχει μια τελείως διαφορετική προσέγγιση για το ζήτημα αυτό το οποίο είναι το μοντέλο Εμπιστευτικό Περιβάλλον Εκτέλεσης (Trusted Execution Environment TEE) και πιο συγκεκριμένα η τεχνολογία Intel Software Guard Extensions-SGX. Κατωτέρω και για την πληρότητα της μελέτης αναπτύσσονται και οι δύο τεχνολογίες διασφάλισης της εμπιστευτικότητας.

Επεκτασιμότητα: Το βασικό δομικό στοιχείο της αρχιτεκτονικής Enigma που εξασφαλίζει την επεκτασιμότητα είναι το μοντέλο αποθήκευσης εκτός αλυσίδας (off chain storage). Το Enigma περιλαμβάνει έναν αποκεντρωμένο κατανεμημένο πίνακα κατακερματισμού (ή DHT) που είναι προσπελάσιμος μέσω γειτονικών κόμβων. Σε αυτό το μοντέλο, το Blockchain αποθηκεύει αναφορές στα δεδομένα, αλλά όχι τα ίδια τα δεδομένα. Τα ιδιωτικά δεδομένα θα πρέπει να κρυπτογραφούνται στην πλευρά του πελάτη πριν από την αποθήκευση και τα πρωτόκολλα ελέγχου πρόσβασης προγραμματίζονται στο Blockchain. Από την άποψη της αποθήκευσης, το Enigma μπορεί να θεωρηθεί ως μια συλλογή κατανεμημένων κόμβων. Κάθε κόμβος έχει μια ξεχωριστή προβολή των μετόχων και των κρυπτογραφημένων δεδομένων, έτσι ώστε η διαδικασία υπολογισμού να είναι εγγυημένη για προστασία της ιδιωτικότητας και της ανοχής σε σφάλματα. Σε αντίθεση με την υφιστάμενη αρχιτεκτονική Blockchain, οι υπολογισμοί και η αποθήκευση δεδομένων δεν αναμεταδίδονται σε όλους τους κόμβους στο δίκτυο. Μόνο ένα μικρό υποσύνολο των κόμβων συμμετέχει στους υπολογισμούς σε μέρος του συνόλου των δεδομένων. Το γεγονός αυτό ελαττώνει τις υπολογιστικές καθώς και τις αποθηκευτικές απαιτήσεις συνεπώς υπάρχει περιθώριο για εκτέλεση περισσότερο απαιτητικών υπολογισμών και αποθήκευσης δεδομένων από τους κόμβους. Το Enigma παρέχει την δυνατότητα εκτέλεσης υπολογισμών σε δεδομένα Blockchain χωρίς πρόσβαση στα ίδια δεδομένα. Επίσης ο τρόπος που είναι σχεδιασμένο το Enigma καθιστά πολύ εύκολη την συνεργασία με υπάρχουσες υλοποιήσεις έξυπνων συμβολαίων όπως το Ethereum.

Το Enigma περιλαμβάνει επίσης δικό του νόμισμα (token) για την αποζημίωση των κόμβων (nodes) που συμμετέχουν στους υπολογισμούς. Το Enigma token (ENG) χρησιμοποιείται στις εξής περιπτώσεις:

- Τέλη Υπολογισμού: Τα ENG tokens χρησιμοποιούνται για την πληρωμή οποιουδήποτε αιτήματος (Query) στο δίκτυο Enigma.
- Τέλη αποθήκευσης: Τα ENG tokens χρησιμοποιούνται για τη διατήρηση δεδομένων στο δίκτυο για ορισμένο χρονικό διάστημα.
- Καταθέσεις Ασφαλείας: Οι κόμβοι του δικτύου μπορούν να χρησιμοποιήσουν τα ENG tokens ως εγγύηση για να εξασφαλίσουν τη συμμετοχή τους στις συναλλαγές.

Ως πρωτόκολλο γενικής χρήσης το Enigma μπορεί να παίξει πολλαπλούς ρόλους ανάλογα με την χρήση του: στην περίπτωση αξιοποίησης ως μέσου ανταλλαγής κρυπτογραφημένων δεδομένων στο Blockchain μπορεί να θεωρηθεί ως ένα ακόμα πρωτόκολλο κρυπτογράφησης κοινής χρήσης. Αν αξιοποιηθεί ως κύριο δίκτυο όπου θα εκτελούνται έξυπνα συμβόλαια που περιέχουν ευαίσθητες πληροφορίες τότε μπορεί να θεωρηθεί πως είναι μια υποδομή απόρρητου Blockchain. Αν τέλος το Enigma αξιοποιηθεί ως ένα ανοιχτό παγκόσμιο δίκτυο κόμβων στο οποίο θα πραγματοποιούνται με ασφάλεια οι υπολογισμοί δικτύων με υψηλές απαιτήσεις ιδιωτικότητας και ασφάλειας όπως οι χρηματοπιστωτικές συναλλαγές συστήματα υγειονομικής περίθαλψης τότε το Enigma μπορεί να θεωρηθεί ως η βασική υποδομή του Web της επόμενης γενιάς.

Ο αρχιτεκτονικός σχεδιασμός του Enigma καθορίζει τον ρόλο τον οποίο προορίζεται να παίξει το Enigma σε ένα Blockchain περιβάλλον: θα λειτουργεί ως ένα συνδεδεμένο δίκτυο σε αυτό και θα αναλαμβάνει την εκτέλεση και αποθήκευση μόνο του μέρους εκείνου των συμβολαίων για τα οποία υπάρχει απαίτηση διαφύλαξης της εμπιστευτικότητας. Ο κώδικας των έξυπνων συμβολαίων θα εκτελείται τόσο στο Blockchain (δημόσια τμήματα) όσο και στο Enigma (τμήματα κώδικα για τα οποία απαιτείται εμπιστευτικότητα). Με τον τρόπο αυτό διασφαλίζεται ταυτόχρονα η ιδιωτικότητα και η ορθότητα, ενώ σε περιβάλλοντα Blockchain διασφαλίζεται μόνο η ορθότητα.

Αξιοποιώντας το Enigma οι προγραμματιστές μπορούν πλέον να σχεδιάζουν εφαρμογές για το Blockchain χωρίς να ανησυχούν για την διαφύλαξη της ιδιωτικότητας των δεδομένων τους [41, 48]. Συνοπτικά τα τεχνολογικά χαρακτηριστικά του Enigma είναι τα εξής:

- Ο πυρήνας της λειτουργίας του Enigma είναι η τεχνολογία του Υπολογισμού Πολλαπλών Συμβαλλομένων (MPC), η οποία επιτρέπει την διενέργεια υπολογισμών επί κρυπτογραφημένων δεδομένων. Οι υπολογισμοί εκτελούνται στους κόμβους του Enigma οι οποίοι έχουν πρόσβαση μόνο σε τμήμα των δεδομένων και ποτέ στο σύνολό τους διασφαλίζοντας έτσι την ιδιωτικότητα.
- Η τεχνολογία DHT (distributed hash-table) του πρωτοκόλλου Enigma επιτρέπει την αποθήκευση των δεδομένων εκτός δικτύου Blockchain. Ένας πίνακας κατακερματισμού αποθηκεύει τις αναφορές στα δεδομένα αντί των ίδιων των δεδομένων. Αυτό διασφαλίζει περαιτέρω την προστασία δεδομένων και βοηθά στην επεκτασιμότητα του δικτύου. Μαζί, η MPC και η DHT συνεργάζονται για να εξασφαλίσουν πλήρη προστασία της ιδιωτικότητας των δεδομένων, διατηρώντας τα δεδομένα κατανεμημένα και εκτός Blockchain .
- Το Enigma για την εκτέλεση των συναλλαγών χρησιμοποιεί την τεχνική της κατανομής απορρήτων (Secret Sharing). Ο υπολογισμός των κρυπτογραφημένων πληροφοριών πραγματοποιείται μέσω της διανομής των δυαδικών ψηφίων τους σε μια ομάδα κόμβων χωρίς να δίνεται η δυνατότητα πρόσβασης σε ένα κόμβο ή δίκτυο στα πλήρη δεδομένα. Όλες οι πληροφορίες που διανέμονται με αυτό τον τρόπο δεν έχουν νόημα από μόνες τους, αλλά δημιουργούν την πληροφορία όταν συνδυάζονται.
- Το Enigma υποστηρίζει την εκτέλεση κώδικα ο οποίος εγγυάται την ορθότητα των υπολογισμών και την προστασία της ιδιωτικότητας, παρόμοια με τις πλατφόρμες έξυπνων συμβολαίων, όπως το Ethereum. Η βασική διαφορά στο Enigma είναι ότι τα ίδια τα δεδομένα είναι κρυμμένα από τους κόμβους που εκτελούν υπολογισμούς. Αυτό επιτρέπει στους προγραμματιστές να συμπεριλαμβάνουν ευαίσθητα δεδομένα στις

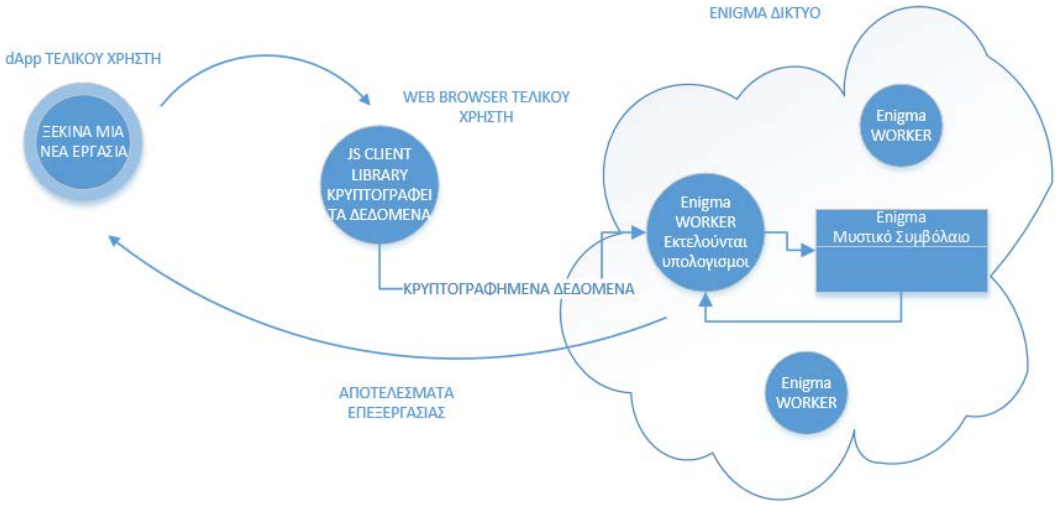
έξυπνες συμβάσεις τους χωρίς να μετακινούνται εκτός Blockchain σε λιγότερο ασφαλή συστήματα, επιτρέποντας έτσι πραγματικά ιδιωτικές και κλιμακούμενες αποκεντρωμένες εφαρμογές. Οι αποδείξεις ορθής εκτέλεσης αποθηκεύονται στο Blockchain και μπορούν να ελεγχθούν. Οι προγραμματιστές θα πρέπει να χρησιμοποιούν την λέξη-κλειδί private για να καθορίσουν δεδομένα ή λειτουργίες που θα πρέπει να διαφυλάσσεται η ιδιωτικότητα τους. Αυτό εξασφαλίζει αυτόματα ότι οποιοσδήποτε υπολογισμός που αφορά αυτά τα αντικείμενα παραμένει ασφαλής και ιδιωτικός.

Για την συγγραφή κώδικα, το Enigma υποστηρίζει μια script γλώσσα προγραμματισμού παρόμοια με την γλώσσα ethereum solidity για τον σχεδιασμό αποκεντρωμένων εφαρμογών από άκρο σε άκρο χρησιμοποιώντας ιδιωτικές συμβάσεις, οι οποίες είναι μια πιο ισχυρή ποικιλία έξυπνων συμβολαίων που μπορούν να χειριστούν ιδιωτικά κάποιες από τις πληροφορίες που επιλέγει ο προγραμματιστής ως ιδιωτικές. Η γλώσσα προγραμματισμού είναι Turing-πλήρης. Οι μυστικές συμβάσεις εκτελούνται σε μια εικονική μηχανή EVM (Virtual Machine) που τρέχει μέσα σε ένα Trusted Execution Environment (TEE), βασισμένο στην τεχνολογία SGX της Intel. Αυτό υποστηρίζει τη διαλειτουργικότητα του δικτύου με το δίκτυο Ethereum.

Το Enigma διαθέτει μια αρκετά απλή φιλοσοφία αναφορικά με τον τρόπο που λειτουργεί έτσι ώστε να διασφαλίζει την ιδιωτικότητα: διαχωρίζει τους υπολογισμούς που απαιτούν ιδιωτικότητα και τους εκτελεί στο δικό του δίκτυο. Επιπρόσθετα πριν να γίνει η διανομή στο δίκτυο Enigma γίνεται κρυπτογράφηση από βιβλιοθήκη Enigma-JS, η οποία κρυπτογραφεί ευαίσθητα δεδομένα στη μνήμη. Τα συμβόλαιο Enigma που αναπτύσσεται επί της αλυσίδας μεταδίδει το έργο στο δίκτυο Enigma και εκτελεί τυχαία λοταρία δειγματοληψίας για να καθορίσει ποιος κόμβος πρέπει να το εκτελέσει. Ο επιλεγμένος εργαζόμενος δίνει οδηγίες στο αξιόπιστο υλικό του να αποσυσκευάζει την εργασία, να αποκρυπτογραφεί τα επιχειρήματά της και να μεταβιβάζει την εκτέλεση στην εσωτερική EVM.

Μια συνοπτική περιγραφή του τρόπου λειτουργίας του Enigma :

1. Μια dApp εφαρμογή στο Blockchain ξεκινά μια εργασία. Τα δεδομένα αποστέλλονται τοπικά στην βιβλιοθήκη Js του Enigma.
2. Τα δεδομένα κρυπτογραφούνται από την βιβλιοθήκη και αποστέλλονται στο δίκτυο Enigma.
3. Τα κρυπτογραφημένα δεδομένα βρίσκονται στο δίκτυο Enigma.
4. Η εργασία κοινοποιείται στο δίκτυο Enigma. Ένας κόμβος του δικτύου (worker) αναλαμβάνει την εκτέλεση της εργασίας.
5. Υλοποιείται ο υπολογισμός, ο κόμβος που εκτέλεσε την εργασία ανταμείβεται και το αποτέλεσμα της εργασίας επιστρέφει στην dApp.



Εικόνα 2: Σε υψηλό επίπεδο συνοπτική περιγραφή της λειτουργίας του Enigma

Το δίκτυο Enigma αποσπά τις εργασίες που εμπεριέχουν ιδιωτικά δεδομένα από δίκτυα όπως το Ethereum. Οι εργασίες αυτές έχουν ως παραγωγό μια εφαρμογή dApp και στην πορεία παρεμβάλλεται η βιβλιοθήκη JS του Enigma η οποία κρυπτογραφεί τα ευαίσθητα δεδομένα στη μνήμη για άμεση χρήση ή αποθήκευση, και λαμβάνει μια απόδειξη ότι ο κόμβος που θα εκτελέσει την επεξεργασία (worker) λειτουργεί το αξιόπιστο υλικό (SGX) πριν από την αποστολή δεδομένων και την καταβολή τελών.

Αμέσως μόλις δεχθεί κάποια υπολογιστική εργασία από την βιβλιοθήκη JS το κρυφό συμβόλαιο αναμεταδίδει την εργασία εντός του δικτύου Enigma. Στη

συνέχεια, κάθε εγγεγραμμένος κόμβος Enigma τρέχει τυχαίο αλγόριθμο για να καθορίσει εάν πρέπει να εκτελέσει την εργασία. Με την τυχαία διαδικασία επιλέγεται ο κόμβος που θα εκτελέσει την εργασία.

Ο επιλεγμένος κόμβος worker από την προηγούμενη διαδικασία αναλύει την προς εκτέλεση εργασία, αποκρυπτογραφεί τα δεδομένα που τη συνοδεύουν και τα διαβιβάζει στην εσωτερική EVM προς εκτέλεση. Μετά την εκτέλεση, ένα hash των χαρακτηριστικών εργασίας δηλαδή της εισόδου, του κώδικα και της εξόδου υπογράφεται με ένα ιδιωτικό κλειδί που υπάρχει μόνο στο αξιόπιστο υλικό [49]. Τα δεδομένα αυτά δεσμεύονται στη συνέχεια στην αλυσίδα όπου η προέλευση και η ακεραιότητά τους είναι κρυπτογραφικά επαληθευμένα. Αυτή η επαλήθευση επί της αλυσίδας εγγυάται:

- Την ακεραιότητα των χαρακτηριστικών εργασίας.
- Ασφαλή εκτέλεση σε αξιόπιστο υλικό.
- Εκτέλεση από τον επιλεγμένο worker.

Τέλος, τα αποτελέσματα μεταφέρονται στη dApp και ο worker εισπράττει την αμοιβή του.

Το σύστημα Enigma αποτελείται από υποσυστήματα το καθένα εκ των οποίων λειτουργεί ως πάροχος υπηρεσιών το οποίο παραμένει αδρανές έως ότου κληθεί να διεκπεραιώσει κάποια υπηρεσία που θα του ζητηθεί.

- Υπηρεσία εγγραφής (Registration): Όταν ένας κόμβος εισαχθεί στο Enigma τότε θα πρέπει να καταχωρηθεί ως εν δυνάμει worker. Το πρωτόκολλο εγγραφής επιβεβαιώνει ότι ο κόμβος τρέχει σε υλικό SGX.
- Κρυπτογράφηση/Αποθήκευση (Encryption / Storage): Η ροή των δεδομένων πραγματοποιείται μεταξύ της dApp εφαρμογής και του δικτύου Enigma με τη χρήση πρωτοκόλλου κρυπτογράφησης ελλειπτικών καμπυλών (Elliptic-curve Diffie–Hellman - ECDH) [50]. Η ελλειπτική καμπύλη Diffie-Hellman (ECDH) είναι ένα πρωτόκολλο συμφωνίας κλειδιού που επιτρέπει σε δύο μέρη, καθένα από τα οποία έχει ένα ζεύγος κλειδιών δημόσιου και ιδιωτικού κλειδιού ελλειπτικής καμπύλης, να δημιουργήσει ένα κοινό μυστικό πάνω σε ένα ανασφαλές κανάλι. Αυτό το κοινόχρηστο μυστικό μπορεί να χρησιμοποιηθεί

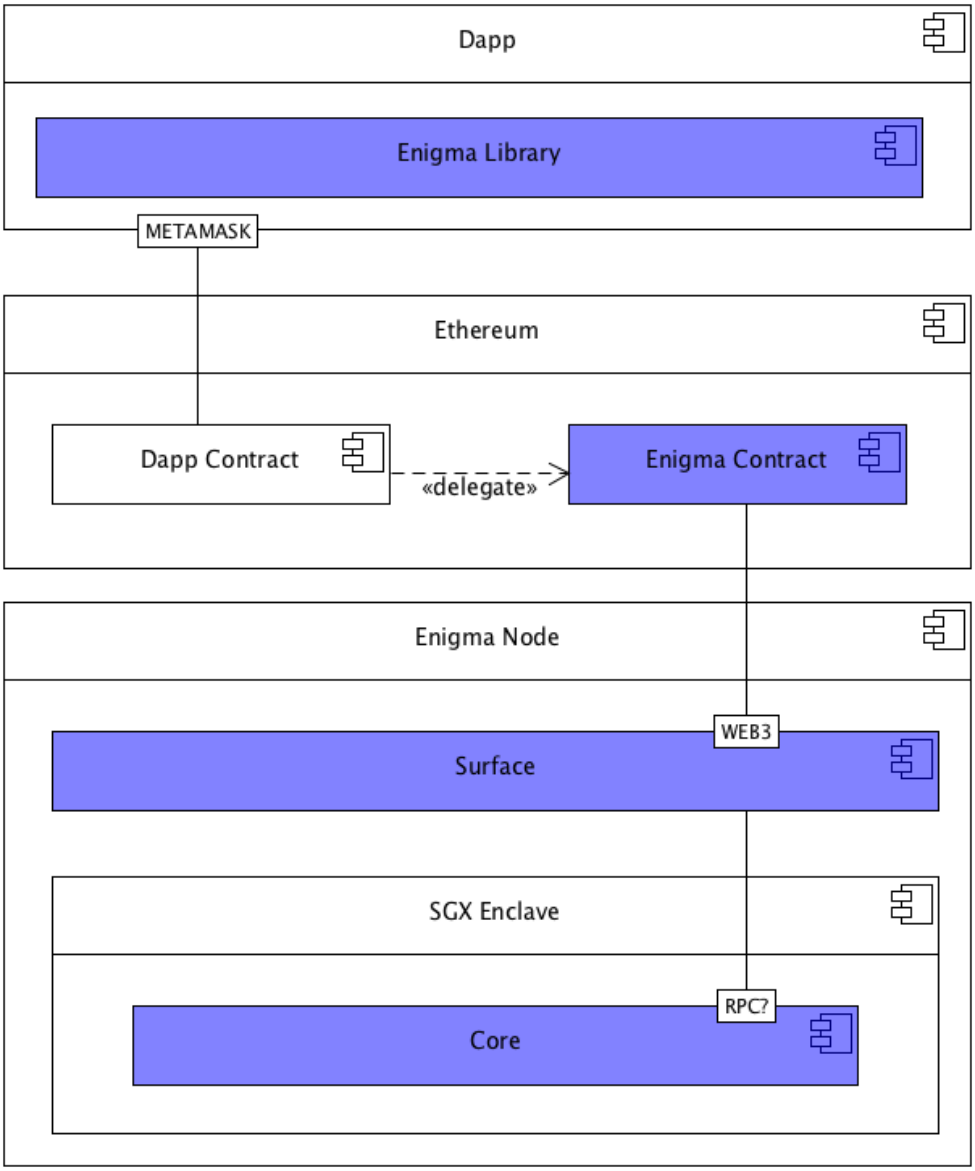
απευθείας ως κλειδί ή για να αντλήσει άλλο κλειδί. Το κλειδί ή το παράγωγο κλειδί μπορεί στη συνέχεια να χρησιμοποιηθεί για την κρυπτογράφηση επικοινωνιών χρησιμοποιώντας έναν κρυπτογράφο συμμετρικού κλειδιού. Είναι μια παραλλαγή του πρωτοκόλλου Diffie-Hellman που χρησιμοποιεί κρυπτογράφηση ελλειπτικής καμπύλης. Τα κρυπτογραφημένα δεδομένα παραμένουν στην dApp εφαρμογή (Cached) για μελλοντική χρήση.

- Υπηρεσία επιλογής κόμβου Worker: Πολλοί κόμβοι συμμετέχουν στο δίκτυο Enigma με σκοπό να κερδίζουν ανταμοιβές εκτελώντας τα καθήκοντα υπολογισμού ως workers. Η επιλογή των worker γίνεται για κάθε εργασία υπολογισμού. Κάθε κόμβος καθορίζει εάν είναι ο επιλεγμένος εργαζόμενος εκτελώντας έναν αλγόριθμο που βασίζεται σε έναν κοινόχρηστο τυχαίο seed.
- Υπηρεσία εκτέλεσης υπολογισμών (Computation): Οι εργασίες υπολογισμού κατευθύνονται από τις εφαρμογές dApp στον ασφαλή κλωβό (SGX enclave) αφού πρώτα περάσουν από διάφορα υποσυστήματα.
- Υπηρεσία επαλήθευσης Enigma (On-chain Verification): Οι μυστικές συμβάσεις Enigma έχουν ως βασικό ρόλο την επαλήθευση υπογεγραμμένων δεδομένων από κόμβους.
- Υπηρεσία επιβεβαίωσης (Attestation): Μια εφαρμογή dApp μπορεί να επιβεβαιώσει την αυθεντικότητα ενός κόμβου worker αν δηλαδή διαθέτει SGX hardware πριν να ζητήσει την εκτέλεση κάποιας εργασίας από τον κόμβο.

Το δίκτυο Enigma δεν είναι αυτόνομο πρόγραμμα. Η αποκεντρωμένη φύση του και η στενή σύνδεση του με το Ethereum αυξάνουν την πολυπλοκότητα, απαιτώντας τη μορφοποίηση της αρχιτεκτονικής σύμφωνα με τα ήδη υπάρχοντα συστατικά (components). Τα βασικά λειτουργικά στοιχεία που συνθέτουν το σύστημα Enigma είναι:

- Enigma Library (EnigmaP.js): Μια βιβλιοθήκη γραμμένη σε JavaScript library η οποία υλοποιεί λειτουργίες για το Enigma (πχ κρυπτογράφηση) και βρίσκεται εγκατεστημένη στην πλευρά του dApp (web browser).

- dApp Contract: Ένα έξυπνο συμβόλαιο (smart contract) το οποίο έχει δημιουργηθεί από τον δημιουργό της εφαρμογής dApp και περιλαμβάνει τα δεδομένα και την επιχειρησιακή λογική των υπολογιστικών εργασιών καθώς και την διαχείριση των απαντήσεων από το Enigma.
- Enigma Contract: Αναφέρεται στο παρόν και ως κρυφό συμβόλαιο. Αποτελεί ένα έξυπνο συμβόλαιο το οποίο είναι εγκατεστημένο στους κόμβους Enigma και συντονίζει τις λειτουργίες του δικτύου.
- Surface: Ένα μη εμπιστευτικό συστατικό στοιχείο του Enigma του οποίου η βασική λειτουργία είναι ο συντονισμός των υπολογισμών ανάμεσα στα κρυφά συμβόλαια και στο συστατικό core.
- Core: Το εμπιστευτικό συστατικό στοιχείο του Enigma όπου εκτελούνται λειτουργίες με υψηλές απαιτήσεις εμπιστευτικότητας και εκτελείται σε ένα κλωβό SGX.
- Principal Node: κόμβος προσωρινού χαρακτήρα ο οποίος μεταδίδει στο δίκτυο τυχαίους αριθμούς.
- Attestation Service: Αυτόνομη υπηρεσία η οποία επαληθεύει τις αναφορές που έχουν δημιουργηθεί με την τιμή μέτρησης MRENCLAVE και στη συνέχεια τις μετατρέπει και υπογράφει χρησιμοποιώντας ένα ασύμμετρο κλειδί ειδικά για την συσκευή, το κλειδί EPID Intel. Η έξοδος αυτής της διαδικασίας ονομάζεται attestation, η οποία μπορεί να εξακριβωθεί εκτός της πλατφόρμας.



Εικόνα 3: Αρχιτεκτονική αναπαράσταση των components του Enigma

6.2 Μυστικά Συμβόλαια (Secret Contracts) Enigma

Η έννοια «έξυπνα συμβόλαια» (Smart Contracts) εισήχθηκε για πρώτη φορά από τον Szabo το 1994 ως «ένα πρωτόκολλο ηλεκτρονικής συναλλαγής που εκτελεί τους όρους μιας σύμβασης» [51]. Στην ουσία ο Szabo πρότεινε να υλοποιούνται σε κώδικα οι όροι των συμβάσεων (εξασφαλίσεις, δεσμεύσεις κ.λπ.) και να

ενσωματώνονται σε υλικό ή λογισμικό με χαρακτηριστικά υποχρεωτικής εκτέλεσης, έτσι ώστε να ελαχιστοποιείται η ανάγκη για έμπιστα τρίτα μέρη μεταξύ των συναλλασσόμενων και η εμφάνιση κακόβουλων ή τυχαίων εξαιρέσεων. Στο Blockchain, τα έξυπνα συμβόλαια υλοποιούνται ως script κώδικας που βρίσκεται αποθηκευμένος σε blocks και μπορεί να θεωρηθούν κατά προσέγγιση ανάλογα με τις αποθηκευμένες διαδικασίες στα συστήματα διαχείρισης σχεσιακών βάσεων δεδομένων. Στο Blockchain τα έξυπνα συμβόλαια διαθέτουν μια μοναδική διεύθυνση η οποία αποτελεί και το σημείο ενεργοποίησης της καλώντας την μέσα από κάποια εφαρμογή ή άλλο συμβόλαιο. Εν συνεχεία εκτελείται ανεξάρτητα και αυτόματα με έναν προκαθορισμένο τρόπο σε κάθε κόμβο του δικτύου, σύμφωνα με τα δεδομένα που συμπεριλήφθηκαν στη συναλλαγή ενεργοποίησης.

Με τη χρήση των έξυπνων συμβολαίων στο Blockchain ενισχύεται περαιτέρω η διαλειτουργικότητα και η αποτελεσματικότητα των εφαρμογών που αναπτύσσονται σε αυτό όμως το βασικό πρόβλημα της ιδιωτικότητας παραμένει. Κάθε κόμβος έχει πρόσβαση τόσο στον κώδικα όσο και στα δεδομένα των έξυπνων συμβολαίων καταργώντας την έννοια της ιδιωτικότητας. Το πρόβλημα έρχεται να επιλύσει η χρήση των μυστικών συμβολαίων (Secret Contracts) τα οποία αποτελούν στην ουσία επέκταση των έξυπνων συμβολαίων.

Η επέκταση συνίσταται στο ότι εν αντιθέσει με τα έξυπνα συμβόλαια τα οποία αντιμετωπίζουν επιτυχώς το ζήτημα της επαλήθευσης της ορθότητας των υπολογισμών τα μυστικά συμβόλαια καλύπτουν τα ζητήματα ιδιωτικότητας.

Ως παράδειγμα της ανάγκης υιοθέτηση μυστικών συμβολαίων μπορεί να αναφερθεί η ανάγκη πρόσβασης εφαρμογής έγκρισης δανείων που υλοποιείται και λειτουργεί στο Blockchain σε ιστορικά στοιχεία του χρήστη προκειμένου να μετρήσει τον κίνδυνο αποπληρωμής του δανείου (πχ στο παρελθόν ο χρήστης δεν αποπλήρωσε κάποιο δάνειο). Αν η εφαρμογή κάνει χρήση κάποιου έξυπνου συμβολαίου τότε έχει πλήρη πρόσβαση στο ιστορικό κινήσεων του πελάτη/χρήστη. Αντίθετα με την βοήθεια των μυστικών συμβάσεων αποκρύπτεται το ιστορικό και η εφαρμογή (μέσω του συμβολαίου) έχει στην διάθεση της μόνο την απάντηση αν ο πελάτης είναι αξιόπιστος ή όχι. Βέβαια δημιουργείται το ερώτημα γιατί να μην υπάρχει τρίτος πάροχος ο οποίος να

δίνει απευθείας την απάντηση κατά πόσο είναι αξιόπιστος ο πελάτης για να λάβει το δάνειο, τότε όμως έρχεται σε πλήρη αντίθεση με την φιλοσοφία Blockchain περί μη ανάγκης ύπαρξης αξιόπιστου τρίτου μέρους.

Αντίθετα, σε ένα περιβάλλον όπου υπάρχουν μυστικές συμβάσεις, ένας χρήστης μπορεί να μοιράζεται με ασφάλεια το ιστορικό συναλλαγών. Οι κόμβοι μπορούν να εκτελέσουν τη σύμβαση και να λάβουν το αποτέλεσμα χωρίς να είναι σε θέση να παρακολουθήσουν τις συναλλαγές του χρήστη. Αυτή η εφαρμογή θα μπορούσε να είναι αυτόνομη από άκρο σε άκρο, ενώ θα εγγυάται και την ορθότητα -εάν ένας χρήστης είναι επιλέξιμος για ένα δάνειο, θα πάρει ένα δάνειο-, καθώς και την προστασία της ιδιωτικότητας - κανείς δεν μπορεί να δει το ιστορικό συναλλαγών τους.

Με δεδομένη τη χρησιμότητα των μυστικών συμβολαίων το αμέσως επόμενο ερώτημα που γεννάται είναι με ποιον τρόπο θα διασφαλίζεται η ιδιωτικότητα. Με άλλα λόγια με ποια τεχνολογία θα διασφαλίζεται η απαίτηση κάποια δεδομένα να είναι κρυπτογραφημένα, αλλά την ίδια στιγμή να είναι δυνατή και η επεξεργασία τους χωρίς όμως την ύπαρξη τρίτου μέρους που θα διασφαλίζει την πρόσβαση.

Όπως γίνεται αντιληπτό από τα ανωτέρω το βασικό τεχνολογικό ζήτημα για το Blockchain που καλείται να επιλύσει το Enigma είναι η ισορροπία ανάμεσα στη διαφάνεια και την προστασία της ιδιωτικότητας.

Τα τμήματα που ακολουθούν περιγράφουν τα βασικά χαρακτηριστικά μιας μυστικής σύμβασης Enigma:

- Καταγραφή υπολογιστικών εργασιών (Task Registry): Οι υπολογιστικές εργασίες τηρούνται σε ξεχωριστή αποθηκευτική δομή μαζί με το κόστος που αντιστοιχεί στην κάθε μια σε κρυπτονόμισμα Enigma (ENG).
- Events: Οι ακόλουθες λίστες περιλαμβάνουν τα βασικά συμβάντα (events) που είναι διαθέσιμα.
- ComputeTask: Παρέχει στους workers τις παραμέτρους των εργασιών.
- Callable: Παραλλαγή υπογραφής μεθόδου (method signature) μιας δημόσιας λειτουργίας της έξυπνης σύμβασης στην οποία περιέχεται η επιχειρησιακή λογική.

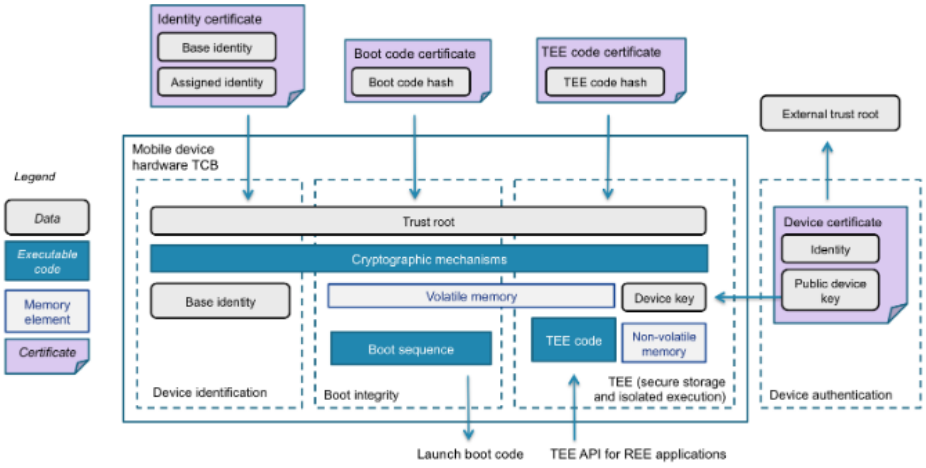
- CallableArgs: Οι κρυπτογραφημένοι παράμετροι της callable συνάρτησης.
- Callback: Η υπογραφή της μεθόδου την οποία καλεί ο worker όταν επιστρέφει κάποιο αποτέλεσμα υπολογισμού στην έξυπνη σύμβαση.
- Preprocessors: Λίστα λειτουργιών προεπεξεργασίας.
- Fee: Ο υπολογισμός του κόστους χρήστης που αναλογεί στον worker όταν η εργασία ολοκληρωθεί.
- WorkersParameterized: Αποστέλλει στους workers τις απαιτούμενες παραμέτρους για την επιλογή.
- Seed: Το sampling seed.
- ActiveWorkers: Λίστα των ενεργών workers.

6.3 Έμπιστα περιβάλλοντα εκτέλεσης κώδικα (Trusted Execution Environments) και Intel SGX

Ένα έμπιστο περιβάλλον εκτέλεσης (Trusted Execution Environment - TEE) είναι ένα ασφαλές περιβάλλον επεξεργασίας που προστατεύει την ακεραιότητα των δεδομένων και συνδυάζει δυνατότητες επεξεργασίας, μνήμης και αποθήκευσης [52]. Είναι απομονωμένο από το «κανονικό» περιβάλλον επεξεργασίας, που μερικές φορές ονομάζεται περιβάλλον πλούσιας εκτέλεσης (Rich Execution Environment), όπου εκτελείται το λειτουργικό σύστημα και οι εφαρμογές. Όσο τα λειτουργικά συστήματα μεγαλώνουν σε μέγεθος και πολυπλοκότητα, είναι όλο και πιο ευάλωτα σε ευπάθειες λογισμικού. Για να παρέχουν προστασία από επιθέσεις που εκμεταλλεύονται τέτοιες ευπάθειες, τα TEE καθιστούν δυνατή τη σχεδίαση εφαρμογών και υπηρεσιών REE που παραμένουν ασφαλείς ακόμη και εν όψει της συμβιβαστικής λύσης των λειτουργικών συστημάτων διαχωρίζοντάς τα, έτσι ώστε οι ευαίσθητες λειτουργίες να περιορίζονται στο TEE και ευαίσθητα δεδομένα όπως κρυπτογραφικά κλειδιά, μην αφήνουν ποτέ το TEE.

Αυτά τα TEE επιτρέπουν στα προγράμματα να τρέχουν σε ασφαλείς θύλακες (Enclaves), οι οποίοι αποτελούν μαύρα κουτιά όπου η κατάσταση του προγράμματος είναι κρυμμένη και απρόσιτη από οποιονδήποτε. Αυτό είναι ενδιαφέρον επειδή μπορεί κανείς να δημιουργήσει ένα ζεύγος ιδιωτικού /

δημόσιου κλειδιού μέσα σε ένα θύλακα, να κρυπτογραφήσει ένα αρχείο με αυτό το δημόσιο κλειδί, καθιστώντας το αρχείο διαθέσιμο μόνο μέσα από τον θύλακα. Φυσικά, αυτό θέτει το στάδιο για τον ιδιωτικό υπολογισμό επειδή οι χρήστες είναι σε θέση να κρυπτογραφήσουν τα αρχεία τους, να τα στείλουν στο TEE και να αφήσουν το TEE να εκτελέσει τον υπολογισμό χωρίς τις εισόδους να εκτίθενται ποτέ.



Εικόνα 4: Περιγραφή του περιβάλλοντος SGX από την ιστοσελίδα της Intel

Το Enigma χρησιμοποιεί μια από τις υλοποιήσεις TEE, τις επεκτάσεις λογισμικού Intel SGX [53] οι οποίες στην ουσία αποτελούν ένα σύνολο εσωτερικών εντολών σχετικών με την ασφάλεια που ενσωματώνονται σε ορισμένες σύγχρονες κεντρικές μονάδες επεξεργασίας της Intel (CPU). Επιτρέπουν στον κώδικα του χρήστη και του λειτουργικού συστήματος να ορίζουν ιδιωτικές περιοχές μνήμης, που ονομάζονται θύλακες, τα περιεχόμενα των οποίων προστατεύονται και δεν μπορούν να διαβαστούν ή να αποθηκευτούν από οποιαδήποτε διαδικασία εκτός του ίδιου του θύλακα, συμπεριλαμβανομένων των διαδικασιών που εκτελούνται σε υψηλότερα επίπεδα προνομίων. Το SGX είναι απενεργοποιημένο από προεπιλογή και πρέπει να είναι ενεργοποιημένο από τον χρήστη μέσω των ρυθμίσεων BIOS του σε ένα υποστηριζόμενο σύστημα.

Το SGX περιλαμβάνει κρυπτογράφηση από τη CPU ενός τμήματος μνήμης. Ο θύλακας αποκρυπτογραφείται κατά την εκτέλεση μόνο εντός της ίδιας της CPU και μόνο για τον κώδικα και τα δεδομένα που τρέχουν μέσα από τον ίδιο το

θύλακα. Ο επεξεργαστής επομένως προστατεύει τον κώδικα από το να «κατασκοπεύεται» ή να εξετάζεται από άλλο κώδικα.

Το δίκτυο Enigma χρησιμοποιεί την τεχνολογία θύλακα Intel SGX επειδή παρέχει ισχυρές κρυπτογραφικές εγγυήσεις. Οι παρακάτω εγγυήσεις λειτουργίας εξηγούν γιατί μπορεί κανείς να εμπιστευθεί το πρωτόκολλο Enigma για ιδιωτικότητα και ορθότητα.

- Η διαδικασία βεβαίωσης παρέχει επαλήθευση για τρία πράγματα. Την ταυτότητα της εφαρμογής, την ακεραιότητα της (πχ δεν έχει αλλοιωθεί) και το ότι εκτελείται με ασφάλεια σε ένα θύλακα σε μια πλατφόρμα με δυνατότητα Intel SGX.
- Το κλειδί υπογραφής ενός θύλακα υφίσταται μόνο εντός του θύλακα. Επομένως, τα δεδομένα μπορούν να υπογραφούν μόνο με αυτό το κλειδί ως μέρος του καθορισμένου συνόλου εντολών που εκτελείται σε ένα θύλακα.
- Οι εργασίες υπολογισμού υπογράφονται εντός του θύλακα και επαληθεύονται στο Blockchain. Αυτό εγγυάται την ακεραιότητα όλων των παραμέτρων τους: εντολές, εισόδους και εξόδους. Δεδομένου ότι γνωρίζουμε πως όλες οι οδηγίες και οι είσοδοι είναι άθικτες, οι έξοδοι είναι αναγκαστικά και αυτές σωστές.
- Οι ίδιες εγγυήσεις ισχύουν για τον κύριο κόμβο που έχει ως αποστολή τη δημιουργία τυχαίου seed. Επιπλέον, το SGX υποστηρίζει μόνο γεννήτριες τυχαίων αριθμών ικανές για αληθινή τυχαία λειτουργία.

Αυτές οι εγγυήσεις είναι κρίσιμες. Επιτρέπουν στο πρωτόκολλο Enigma να αποδείξει την ιδιωτικότητα και την ορθότητα των δεδομένων με ελάχιστη επιβάρυνση (σε σύγκριση με το Ethereum για παράδειγμα). Αυτές οι εγγυήσεις προσφέρουν τεράστια οφέλη τόσο όσον αφορά την επεκτασιμότητα όσο και την προστασία της ιδιωτικής ζωής.

Πολλοί υπολογιστές έχουν ενεργοποιημένη την Intel SGX και δεν υπάρχει σημαντική επιβράδυνση της απόδοσης χρησιμοποιώντας έναν ασφαλή θύλακα για την εκτέλεση ενός προγράμματος. Ωστόσο, υπάρχουν και αρνητικά στοιχεία από αυτή την προσέγγιση. Πρώτον, η πλειοψηφία των TEE στην αγορά σήμερα είναι Intel SGX. Αυτό κρύβει κίνδυνο συγκέντρωσης επειδή δεν είναι σαφές ποια

είναι η ακριβής αρχιτεκτονική των τσιπ και αν η Intel μπορεί να έχει μειώσει την ασφάλεια του SGX για να βελτιώσει την απόδοση του τσιπ συνολικά λόγω της εξειδικευμένης αγοράς για SGXs σήμερα. Δεύτερον, για να αποδείξει ότι ένας υπολογιστής διαθέτει έναν επεξεργαστή Intel SGX, ο υπολογιστής πρέπει να επικοινωνήσει με την απομακρυσμένη υπηρεσία πιστοποίησης της Intel. Και πάλι, αυτή είναι μια κεντρική υπηρεσία cloud που παρακολουθεί όλες τις μάρκες που έχουν κατασκευαστεί και περιέχουν τεχνολογία Intel SGX. Ένας hacker που είναι σε θέση να παραβιάσει αυτή την υπηρεσία μπορεί να εισάγει πλαστά IDs που «πιστοποιούν» τους υπολογιστές που περιέχουν Intel SGX, έστω και αν δεν το κάνουν. Εάν μια έξυπνη σύμβαση τρέχει σε ένα από αυτά τα ψεύτικα TEE, ο επιτιθέμενος θα μπορέσει να δει όλες τις πληροφορίες.

6.4 Secure Multi-party Computation (sMPC)

Ο πυρήνας γύρω από τον οποίο είναι χτισμένη η διασφάλιση της ιδιωτικότητας σε δίκτυα Blockchain είναι η κρυπτογραφική τεχνική ασφαλούς υπολογισμού πολλαπλών συμμετοχών (Secure multiparty computation sMPC). Με απλά λόγια με την χρήση sMPC, εάν θέλουμε να εκτελέσουμε έναν υπολογισμό, χωρίζουμε τα δεδομένα σε πολλαπλά κομμάτια με ένα πολύ συγκεκριμένο τρόπο και στη συνέχεια έχουμε μεμονωμένα υπολογιστικά περιβάλλοντα να εκτελούν αριθμητικές πράξεις σε αυτά τα κομμάτια χωρίς να αποκαλύπτουν τίποτα για τα αρχικά δεδομένα. Αυτά τα κομμάτια μπορούν στη συνέχεια να ανασυνδυαστούν για να παραγάγουν το τελικό αποτέλεσμα.

Για παράδειγμα, ας υποθέσουμε ότι θέλουμε να υπολογίσουμε το A + B χωρίς να αποκαλύψουμε τι είναι A και B. Μπορούμε να χωρίσουμε το A σε 3 μέρη ([A] 1, [A] 2, [A] 3) και B σε 3 μέρη ([B] ℓ, [B] + [B] $_x$ = [C] $_x$). Διανέμουμε τα μέρη των δεδομένων τα οποία από μόνα τους δεν περιέχουν καμιά χρήσιμη πληροφορία σε 3 διαφορετικούς κόμβους. Μετά από τον υπολογισμό των αντίστοιχων τιμών του [C], οι 3 κόμβοι μπορούν να έρθουν μαζί και να συνδυάσουν τις τιμές τους [C], παράγοντας-καταλήγοντας σε C. Μέσω αυτής της διαδικασίας, οι 3 κόμβοι θα έχουν καταφέρει να υπολογίσουν το [C] $_x$ μαζί χωρίς κανένας από αυτούς να γνωρίζει ποτέ τι ήταν τα A και B. Οι πολλαπλασιασμοί είναι πιο δύσκολοι αλλά μπορούν να επιτευχθούν με μερικά τεχνάσματα.

Θεωρητικά, όταν μπορούμε να κάνουμε προσθέσεις και πολλαπλασιασμό μέσω ενός πρωτοκόλλου sMPC, μπορούμε να επιτύχουμε οποιουσδήποτε υπολογισμούς. Αυτός είναι ένας τρόπος υπολογισμού με διατήρηση της ιδιωτικότητας, επειδή ο μόνος τρόπος για να αποκαλυφθούν τα δεδομένα είναι η συνεργασία όλων των κόμβων. Ακόμα και μόνο ένας έμπιστος κόμβος αρκεί για να μην γίνει διαρροή εμπιστευτικών πληροφοριών, γεγονός που το καθιστά εξαιρετικά ανθεκτικό σε επιθετική συμπεριφορά. Ωστόσο, το ζήτημα είναι ότι γενικά το πρωτόκολλο sMPC είναι αργό λόγω του κόστους επικοινωνίας μεταξύ των κόμβων. Όλοι οι κόμβοι πρέπει επίσης να εκτελέσουν το πρόγραμμα σωστά χρησιμοποιώντας τα μυστικά κοινά δεδομένα που τους δόθηκαν. Εάν ένας μοναδικός κόμβος αντικαθιστά την έξοδο $[C]_x$ με τυχαία τιμή, η συνδυασμένη τιμή C των κόμβων δεν θα είναι αποτελεσματική. Κάνοντας αυτό, ένας εισβολέας θα καταστρέψει την υπολογιστική προσπάθεια όλων των άλλων συμμετεχόντων.

Τα δύο έργα που προσεγγίζουν τις έξυπνες συμβάσεις για την προστασία της ιδιωτικότητας με το sMPC είναι το Keep Network και το Enigma. Στην αρχική επιστημονική δημοσίευση το Enigma παρουσιάστηκε με ένα σχέδιο αξιοποίησης της τεχνολογίας sMPC, αλλά από τότε άλλαξε κατεύθυνση υιοθετώντας στην τρέχουσα έκδοση την τεχνολογία Intel SGX. Ωστόσο, καθώς αναμένονται στο μέλλον βελτιστοποιήσεις στο sMPC το Enigma θα επαναφέρει το sMPC στις μελλοντικές του υλοποιήσεις.

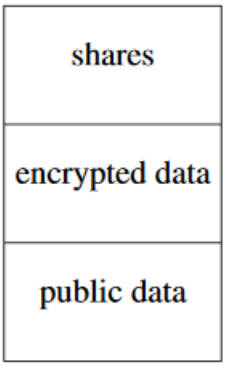
6.5 Κατανεμημένη αποθήκευση δεδομένων

Το βασικό δομικό στοιχείο της αρχιτεκτονικής Enigma που εξασφαλίζει την επεκτασιμότητα είναι το μοντέλο αποθήκευσης εκτός αλυσίδας (off chain). Το enigma περιλαμβάνει έναν αποκεντρωμένο κατανεμημένο πίνακα κατακερματισμού (ή DHT) που είναι προσβάσιμος μέσω γειτονικών κόμβων. Σε αυτό το μοντέλο, το Enigma αποθηκεύει συνδέσεις στα δεδομένα, αλλά όχι τα ίδια τα δεδομένα. Τα ιδιωτικά δεδομένα πρέπει να είναι κρυπτογραφημένα στην πλευρά του πελάτη πριν από την αποθήκευση και τα πρωτόκολλα ελέγχου πρόσβασης προγραμματισμένα στο Blockchain.

Από την άποψη της αποθήκευσης, το Enigma μπορεί να θεωρηθεί ως μια συλλογή κατανεμημένων κόμβων. Κάθε κόμβος έχει μια ξεχωριστή αποθήκη όπου αποθηκεύει τα shares και τα κρυπτογραφημένα δεδομένα, έτσι ώστε η διαδικασία υπολογισμού να είναι εγγυημένη για την προστασία της ιδιωτικότητας και να έχει ανοχή σε σφάλματα.

Αρχιτεκτονικά, υπάρχουν τρεις διαφορετικές αποκεντρωμένες βάσεις δεδομένων που ζουν στο σύστημα Enigma.

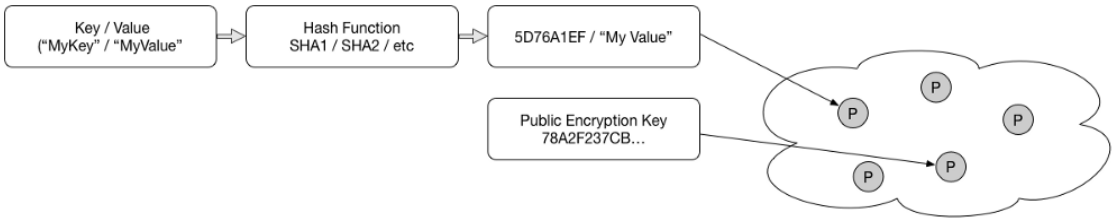
- Public Ledger όπου φυλάσσονται δημόσια δεδομένα και συνδέσεις (References) στα ιδιωτικά δεδομένα.
- DHT, στην βάση δεδομένων DHT αποθηκεύονται δεδομένα εκτός δικτύου (Off chain) τα οποία είναι προσπελάσιμα με τον ίδιο τρόπο που προσπελαύνουν τα δημόσια δεδομένα.
- Και η MPC βάση από όπου παρέχεται πρόσβαση στα δεδομένα τα οποία είναι κατανεμημένα σε διαφορετικούς κόμβους του δικτύου.



Σε επίπεδο δικτύου, η κατανεμημένη αποθήκευση βασίζεται σε ένα τροποποιημένο πρωτόκολλο DHT του Kademlia με ανοχή και ασφαλή κανάλια από σημείο σε σημείο, που προσομοιώνεται χρησιμοποιώντας ένα κανάλι εκπομπής και κρυπτογράφηση δημόσιου κλειδιού. Το πρωτόκολλο αυτό συμβάλλει στη διανομή των shares με αποτελεσματικό τρόπο. Κατά την αποθήκευση των shares, η αρχική μέτρηση απόστασης Kademlia τροποποιείται για να ληφθεί υπόψη η πιθανότητα να προτιμηθεί ένας κόμβος.

Τα DHT απαιτούν την ομοιόμορφη κατανομή των πληροφοριών στο δίκτυο. Για να επιτευχθεί αυτός ο στόχος, χρησιμοποιείται η έννοια του συνεπούς

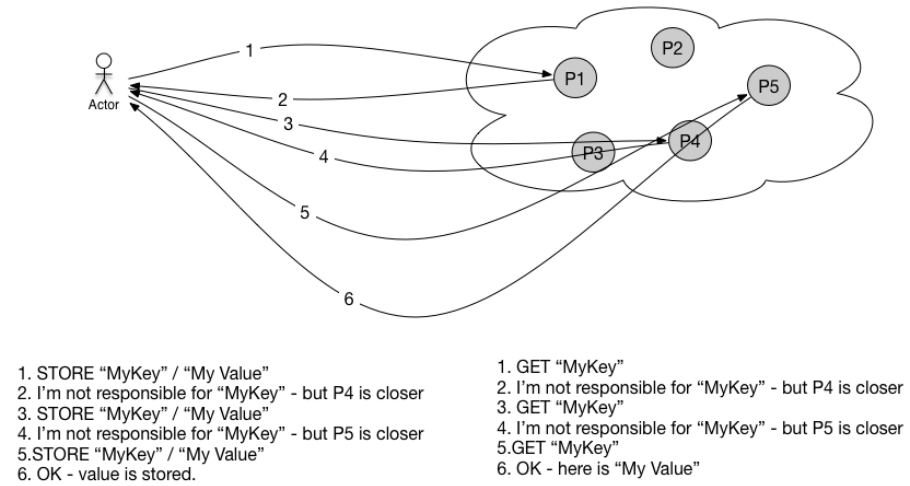
κατακερματισμού (consistent hashing) [54]. Ένα κλειδί περνάει μέσα από έναν αλγόριθμο κατακερματισμού που χρησιμεύει ως λειτουργία τυχαίας επιλογής. Αυτό εξασφαλίζει ότι κάθε κόμβος στο δίκτυο έχει ίσες πιθανότητες να επιλεγεί για να αποθηκεύσει το ζεύγος κλειδιού / τιμής.



Εικόνα 5: Αποθήκευση δεδομένων με το πρωτόκολλο Distributed Hash Table

Επειδή κάθε κόμβος περιέχει μόνο ένα τμήμα του πίνακα δρομολόγησης, η διαδικασία εύρεσης ή αποθήκευσης ενός ζεύγους κλειδιού / τιμής απαιτεί την επαφή με πολλαπλούς κόμβους. Ο αριθμός των κόμβων που πρέπει να επικοινωνήσουν μεταξύ τους σχετίζεται με το όγκο των πληροφοριών δρομολόγησης που αποθηκεύει κάθε κόμβος. Η συνήθης πολυπλοκότητα αναζήτησης είναι η O (log n) όπου n είναι ο αριθμός κόμβων στο δίκτυο. Μερικοί αλγόριθμοι DHT επιτρέπουν την ανταλλαγή απόψεων για την αύξηση του ποσού της κατάστασης του δρομολογητή για περαιτέρω μείωση του κόστους χειρότερης περίπτωσης αναζήτησης. Οι πίνακες δρομολογίων είναι σχετικά μικροί και ένα DHT παραγωγής που λειτουργεί σε περιβάλλον WAN πιθανόν να επιλέξει να αυξήσει το μέγεθος του πίνακα δρομολόγησης και θα μπορούσε να μειώσει περαιτέρω τη χειρότερη αναζήτηση κατά μισό ή περισσότερο.

Υπάρχουν δύο είδη λειτουργιών αναζήτησης. Σε μια επαναληπτική αναζήτηση, ένας αιτούμενος κόμβος θα ερωτά έναν άλλο κόμβο που ζητά ένα ζευγάρι κλειδιών / τιμών. Αν αυτός ο κόμβος δεν έχει αυτόν τον κόμβο, θα επιστρέψει έναν ή περισσότερους κόμβους που είναι «πιο κοντά». Ο αιτών κόμβος θα ερωτήσει τον επόμενο κοντινότερο κόμβο. Αυτή η διαδικασία επαναλαμβάνεται μέχρι να βρεθεί και να επιστραφεί το κλειδί/τιμή ή ο τελευταίος ερωτημένος κόμβος επιστρέφει ένα σφάλμα λέγοντας ότι το κλειδί απλά δεν μπορεί να βρεθεί.



Εικόνα 6: Αναζήτηση σε DHT

Με αναδρομικές αναζητήσεις, ο πρώτος αιτών κόμβος θα ερωτά τον επόμενο κόμβο που κλείνει, ο οποίος στη συνέχεια θα ερωτά τον επόμενο πλησιέστερο κόμβο μέχρι να βρεθούν τα δεδομένα. Στη συνέχεια, τα δεδομένα διαβιβάζονται πίσω στην αλυσίδα αιτήσεων πίσω στον αιτούντα.

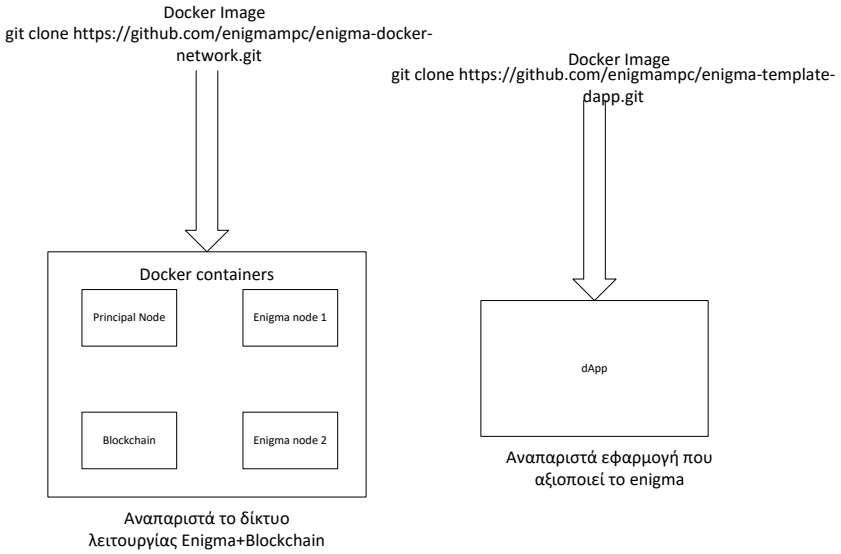
6.6 Περιβάλλον δοκιμών (testnet) Enigma

Στην ενότητα αυτή γίνεται μια συνοπτική περιγραφή της έκδοσης Enigma/testnet η οποία υλοποιείται σε περιβάλλον Docker και παρέχει τη δυνατότητα σε προγραμματιστές να υλοποιήσουν και να εκτελέσουν μυστικά συμβόλαια. Σημειώνεται, ότι η εγγραφή κώδικα για Secret Contracts απαιτεί πολύ υψηλή εξειδίκευση. Η έκδοση αυτή υπολείπεται της τελικής έκδοσης σε λειτουργικότητα όμως σε γενικές γραμμές δίνεται η δυνατότητα μελέτης του τρόπου με το οποίο αντιμετωπίζονται ζητήματα ιδιωτικότητας από το Enigma.

Η πρώτη υλοποίηση του Enigma για τις ανάγκες δοκιμών έχει γίνει από τους δημιουργούς ως έργο ανοιχτού λογισμικού και ο κώδικας έχει τοποθετηθεί στο αποθετήριο git όπου είναι προσβάσιμο από όλους στην διεύθυνση *https://github.com/enigmampc*.

Η παρουσίαση της έκδοσης testnet έγινε σε τοπικό υπολογιστή με Linux Ubuntu 18 και με εγκατεστημένη την έκδοση Docker CE [55] και τα πακέτα npm, scrypt, nodejs and node-gyp. Οι εικόνες docker κατέβηκαν από το git

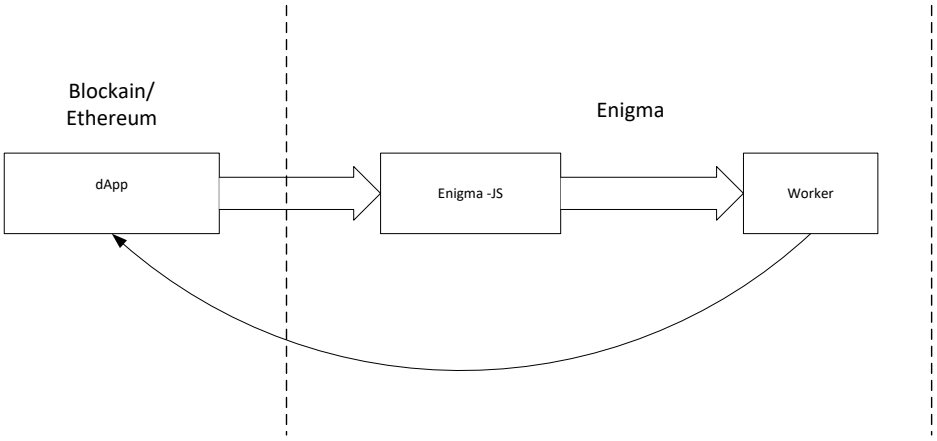
https://github.com/enigmampc/enigma-template-dapp.git και *https://github.com/enigmampc/enigma-docker-network.git*. Μια συνοπτική εικόνα παρουσιάζεται ακολούθως:



Εικόνα 7: Περιβάλλον Enigma/testnet σε docker

Μέσα στο Docker υπάρχουν τέσσερις ανεξάρτητοι υποδοχείς (containers) οι οποίοι προσομοιάζουν το περιβάλλον Enigma σε ένα δίκτυο Ethereum και οι οποίοι επικοινωνούν εντός του Docker περιβάλλοντος και αντιστοιχούν σε τέσσερις κόμβους: ένας κύριος κόμβος (Principal node), δύο πρότυποι κόμβοι (Enigma node) και ένας με τη λογική του Blockchain.

Αφού ένας χρήστης ενός dApp ξεκινήσει μια εργασία (είτε πρόκειται για αγορά, προσφορά σε δημοπρασία είτε για οποιαδήποτε άλλη περίπτωση χρήσης), η τοπική βιβλιοθήκη πελάτη Enigma-JS κρυπτογραφεί τα δεδομένα και αποστέλλει το αίτημα σε έναν επιλεγμένο worker στο Enigma δίκτυο για την εκτέλεση της υπολογιστικής εργασίας. Δεδομένου ότι τα δεδομένα είναι κρυπτογραφημένα πριν από την αποστολή τους, επομένως διατηρούνται ιδιωτικά από τους κόμβους δικτύου (και οποιοσδήποτε άλλος μπορεί να παρακολουθεί, για αυτό το θέμα). Μετά την ολοκλήρωση, η απάντηση μεταφέρεται με ασφάλεια στον τελικό χρήστη.



Εικόνα 8: Λειτουργία σε περιβάλλον Enigma/docker

Τα βασικά συστατικά στοιχεία της υλοποίησης Enigma Testnet είναι:

Η βιβλιοθήκη Enigma-JS. Η βιβλιοθήκη Enigma JS, είναι μια βιβλιοθήκη javascript που διασυνδέεται με το πρωτόκολλο Enigma. Το API για αυτήν τη βιβλιοθήκη περιγράφει εργασίες τις οποίες θα χρειαστεί ένα dApp για να αλληλεπιδράσει με το Enigma, όπως κρυπτογράφηση και επαλήθευση. Το Enigma-JS περιέχει εργαλεία για: 1) ασφαλή κρυπτογράφηση ευαίσθητων δεδομένων σε μνήμη για άμεση χρήση ή αποθήκευση, 2) απόκτηση μιας έγκυρης απόδειξης ότι ο εργαζόμενος-στόχος χρησιμοποιεί με ασφάλεια το αξιόπιστο υλικό πριν από την αποστολή δεδομένων και την καταβολή τελών.

Το συμβόλαιο Enigma. Το συμβόλαιο Enigma περιέχει κυρίως τις λειτουργίες για την ασφαλή λειτουργία του δικτύου. Στο πλαίσιο αυτό διατηρεί κατάλογο με τους καταχωρημένους κόμβους enigma (enigma workers). Λαμβάνει αιτήματα πραγματοποίησης εργασιών (tasks) από τα dApps και τα μεταδίδει στο δίκτυο Enigma. Μπορεί επίσης να επαληθεύσει την ακεραιότητα των αποτελεσμάτων που υποβάλλει κάθε worker.

Κύριος κόμβος. Ο κύριος κόμβος είναι ένας προσωρινός κόμβος ο οποίος εκτελεί δύο βασικές λειτουργίες: 1) Δημιουργία τυχαίων seeds για επιλογή workers. 2) Διαμοιράζει το κλειδί κρυπτογράφησης σε άλλους κόμβους που εισέρχονται στο δίκτυο. Ο κύριος κόμβος υπάρχει μόνο στην έκδοση testnet for programmers και δεν διαδίδει αυτή τη στιγμή κλειδιά στους κόμβους. Χρησιμοποιώντας αυτό το στοιχείο επιτυγχάνεται πραγματική τυχαιότητα ενώ απλοποιείται η

αρχιτεκτονική. Στις μελλοντικές εκδόσεις, το στοιχείο αυτό θα αντικατασταθεί από ένα πλήρως αποκεντρωμένο σύστημα το οποίο θα επιτύχει επίσης πραγματική τυχαιότητα στον τρόπο επιλογής των workers.

Κόμβος Enigma. Ένας κόμβος Enigma αποτελείται από τα κάτωθι δύο στοιχεία.

Surface: Αποτελεί το μη έμπιστο στοιχείο ενός κόμβου Enigma και έχει ως καθήκον τον συντονισμό μεταξύ της κρυφής σύμβασης Enigma και του στοιχείου core. Επίσης εμπλέκεται στην επιλογή workers καθώς και σε υπολογιστικές εργασίες.

Core: Το στοιχείο Core αποτελεί το στοιχείο εκτέλεσης λειτουργιών εμπιστευτικότητας στο δίκτυο Enigma. Το στοιχείο core λειτουργεί εντός του θύλακα SGX και εμπλέκεται σε λειτουργίες κρυπτογράφησης, καταγραφής νέων κόμβων, υπολογισμών, επαλήθευσης και επιστροφής αποτελεσμάτων. Η κρυφή σύμβαση Enigma αναθέτει στο core την επιβεβαίωση ορθής εκτέλεσης των εργασιών.

6.7 Χρονοπρογραμματισμός εκδόσεων και εξέλιξη του Enigma

Το πρωτόκολλο Enigma βρίσκεται υπό ανάπτυξη. Με δεδομένο ότι οι δημιουργοί του θεωρούν ότι ο ρόλος του Enigma θα είναι ιδιαίτερα κρίσιμος για τα συστήματα Blockchain προχωρούν με αργά βήματα υλοποίησης και διάθεσης εκδόσεων έτσι ώστε να είναι σίγουροι για το αποτέλεσμα. Οι εκδόσεις που προετοιμάζονται και τα χαρακτηριστικά τους έχουν δημοσιοποιηθεί στην ιστοσελίδα του project και παρουσιάζονται ακολούθως με χρονολογική σειρά [56].

Έκδοση Discovery—2018 (τρέχουσα)

Η έκδοση Discovery είναι η πρώτη έκδοση που εισάγει την έννοια των «μυστικών συμβολαίων» και την δυνατότητα του Enigma να κρυπτογραφεί τους υπολογισμούς. Αυτό επιτρέπει τελικά στους προγραμματιστές των dApp εφαρμογών να συμπεριλάβουν ευαίσθητα δεδομένα στις έξυπνες συμβάσεις τους, χωρίς να μετακινούνται εκτός αλυσίδας σε κεντρικά (και λιγότερο

ασφαλή) συστήματα. Η έκδοση Discovery είναι η πρώτη που δίνει τη δυνατότητα δημιουργίας dApps με χαρακτηριστικά ιδιωτικότητας από άκρο σε άκρο.

Από τεχνική άποψη, ο μηχανισμός εκτέλεσης των μυστικών συμβολαίων βασίζεται στην εκτέλεση όλου του κώδικα των συμβολαίων εντός των TEE (Trusted Execution Environments), τα οποία μπορούν να κρύψουν δεδομένα ακόμη και στην περίπτωση που ο υπολογιστής που φιλοξενεί την dApp εφαρμογή έχει μολυνθεί από κακόβουλο λογισμικό. Στην έκδοση αυτή παραμένει σε συμβατότητα με την εκτέλεση έξυπνων συμβολαίων Ethereum με την απαίτηση τα έξυπνα συμβόλαια Ethereum να χαρακτηρίζουν private ή public τα δεδομένα για τα οποία υπάρχει απαίτηση διαφύλαξης της ιδιωτικότητας.

Voyager—2019

Η έκδοση Voyager είναι η δεύτερη έκδοση και στοχεύει σε μεγαλύτερη διασφάλιση ιδιωτικότητας για τις εφαρμογές dApp. Οι εφαρμογές αυτές θα μπορούν να αξιοποιήσουν την νέα έκδοση εικονικής μηχανής με κατανεμημένη αρχιτεκτονική (Distributed VM) εντός της οποίας θα μπορούν να εκτελεστούν κρυφά συμβόλαια με την μεθοδολογία sMPC. Οι προγραμματιστές θα μπορούν να επιλέξουν μεταξύ των δύο επιλογών για την εκτέλεση των κρυφών συμβολαίων είτε σε TEE (για την έκδοση κρυφών συμβολαίων 1.0 ή σε sMPC για την έκδοση κρυφών συμβολαίων 2.0. Επιπλέον, αυτή η έκδοση θα σηματοδοτήσει το πρώτο σημαντικό βήμα προς την ανεξαρτησία. Το Enigma θα ξεκινήσει τη δική της έκδοση Blockchain με απλοποιημένο μοντέλο συναίνεσης και περιορισμένα χαρακτηριστικά, μετακινώντας όλα τα dApps στο δικό της δίκτυο αντί να στηρίζεται στην Ethereum. Αυτό θα αυξήσει την επεκτασιμότητα κατά τάξεις μεγέθους. Η αλυσίδα θα συνεχίσει να χρησιμοποιεί το Ethereum ως γονική αλυσίδα για πρόσθετη ασφάλεια, μέχρι να κυκλοφορήσει αργότερα η έκδοση Defiant.

Valiant—2019

Στην έκδοση Valiant υλοποιούνται οι βασικές προσπάθειες κλιμάκωσης και αποκέντρωσης. Σε αυτήν την σημαντική ενημερωτική έκδοση του Enigma, ο

στόχος είναι να υπάρξει μια πλήρως ανοικτή και ασφαλής συναίνεση στην αλυσίδα Enigma, χωρίς να μειώνεται η απόδοση.

Defiant—2020

Η έκδοση Defiant αναμένεται να φέρνει πλήρη ανεξαρτησία του Enigma. Το δίκτυο θα λειτουργήσει στο δικό του εσωτερικό Blockchain πλήρως ανεξάρτητα από άλλα δίκτυα, πράγμα που επίσης σημαίνει μετακίνηση στο φυσικό νόμισμα Enigma. Αυτό θα ολοκληρώσει τη διαδικασία μετακίνησης του Enigma που θα γίνει εντελώς ανεξάρτητο από οποιαδήποτε άλλη λύση.

Σε αυτήν την έκδοση, θα υλοποιηθούν επίσης σημαντικές ενημερώσεις κρυπτογραφικών πρωτοκόλλων (κυρίως γύρω από την MPC), οι οποίες αυξάνουν την ασφάλεια και την αποκέντρωση. Αυτή θα είναι και η τελευταία έκδοση Enigma.

6.8 Εφαρμογές που χρησιμοποιούν το πρωτόκολλο Enigma

Αυτή την στιγμή παρόλο που η βασική τεχνολογία Enigma δεν είναι ακόμα διαθέσιμη, βρίσκονται σε κυκλοφορία δύο εφαρμογές που επιβεβαιώνουν τις δυνατότητες του Enigma.

Η εφαρμογή Enigma/Catalyst είναι μια αλγοριθμική βιβλιοθήκη συναλλαγών για κρυπτογραφικά περιουσιακά στοιχεία γραμμένη σε Python. Επιτρέπει την εύκολη έκφραση των στρατηγικών διαπραγμάτευσης και τους εκ των υστέρων ελέγχους σε σχέση με ιστορικά δεδομένα, παρέχοντας αναλύσεις και πληροφορίες σχετικά με την απόδοση μιας συγκεκριμένης στρατηγικής. Η Catalyst υποστηρίζει επίσης τη ζωντανή διαπραγμάτευση των κρυπτογραφικών περιουσιακών στοιχείων (Crypto-assets) αρχικά με τέσσερα χρηματιστήρια (Binance, Bitfinex, Bittrex και Poloniex) ενώ αναμένεται η προσθήκη περισσότερων με την πάροδο του χρόνου. Η λύση Enigma/Catalyst δίνει τη δυνατότητα στους χρήστες να μοιράζονται και να επεξεργάζονται δεδομένα και να δημιουργούν επικερδείς επενδυτικές στρατηγικές που βασίζονται σε δεδομένα.

Η λύση Catalyst υποστηρίζεται από το Enigma Data Marketplace, μια άλλη λύση που αξιοποιεί τις δυνατότητες της πλατφόρμας Enigma και λειτουργεί ως πύλη σε διαφορετικές βάσεις δεδομένων και μοιράζεται τις αναφορές στα δεδομένα με αποκεντρωμένο τρόπο, ενώ ταυτόχρονα διαφυλάσσει την ιδιωτικότητα των πληροφοριών. Τα βασικά χαρακτηριστικά του Enigma/Catalyst:

- Ευκολία χρήσης, καθώς η προσπάθεια του προγραμματιστή επικεντρώνεται μόνο στην υλοποίηση των κατάλληλων αλγορίθμων.
- Υποστήριξη των κορυφαίων αγορών νομισμάτων με βάση τον όγκο συναλλαγών: Bitfinex, Bittrex, Poloniex and Binance.
- Ασφάλεια, αφού μόνο ο χρήστης έχει πρόσβαση στα κλειδιά exchange API του λογαριασμού του.
- Είσοδος ιστορικότητας τιμών για όλα τα κρυπτονομίσματα με ημερήσια και ανά λεπτό ανάλυση.
- Δυνατότητα ελέγχου επενδυτικής στρατηγικής (Backtesting) και συναλλαγές σε πραγματικό χρόνο και δυνατότητα αλλαγής μεταξύ των δύο modes.
- Έξοδος στατιστικών απόδοσης.

Η εφαρμογή Enigma Data Marketplace ανήκει στο επίπεδο πλατφόρμας που βρίσκεται μεταξύ του πρωτοκόλλου και των επιπέδων εφαρμογής του δικτύου Enigma. Παρέχει την αποκεντρωμένη και ασφαλή υποδομή δεδομένων πάνω στην οποία μπορούν να κατασκευαστούν εφαρμογές, όπως η Catalyst. Σκοπός η συλλογή και πώληση δεδομένων σε τρίτους.

Η εφαρμογή βρίσκεται αυτή τη στιγμή στη φάση 1 της ανάπτυξής της. Η τρέχουσα υλοποίηση περιλαμβάνει το τμήμα on chain, το οποίο ασχολείται με data sets, τους χώρους ονομάτων και τις συνδρομές. Η λογική λειτουργίας της εφαρμογής βρίσκεται σε έξυπνες συμβάσεις που αναπτύσσονται στο δίκτυο Ethereum και λειτουργεί απευθείας με token Enigma (ENG). Σε αυτή την πρώτη εφαρμογή, όλα τα σύνολα δεδομένων (data sets) παρέχονται εκτός δικτύου από διάφορους παρόχους και η αποθήκευση τους διαχειρίζεται ανεξάρτητα από τη λογική που ενσωματώνεται στο έξυπνο συμβόλαιο. Τα σύνολα δεδομένων

χρησιμοποιούνται ως δεδομένα για την δημιουργία έξυπνων αλγορίθμων συναλλαγών που μπορούν βελτιώσουν την απόδοση των επενδύσεων.

Η φάση 2 ανάπτυξης της εφαρμογής Enigma data Marketplace περιλαμβάνει την πρώτη υλοποίηση off chain, το οποίο θα λειτουργεί σε ένα δίκτυο γνωστών κόμβων (περίπου σαν ιδιωτικό Blockchain). Αυτό θα μπορούσε επίσης να θεωρηθεί ως ένα μοντέλο περιορισμένης απειλής.

Στη φάση 3 υλοποιείται σαν ανοιχτό off chain δίκτυο όπου ο καθένας μπορεί να γίνει κόμβος και να προσφέρει αποθηκευτικούς και υπολογιστικούς πόρους σε αντάλλαγμα ENG tokens. Τέλος, στη φάση ανάπτυξης 4 εισάγονται σημαντικά χαρακτηριστικά προστασίας προσωπικών δεδομένων και προστασίας της ιδιωτικότητας. Αυτό θα επέτρεπε την επέκταση της χρηστικότητας του πρωτοκόλλου σε όλα τα είδη δεδομένων, συμπεριλαμβανομένων εκείνων που περιλαμβάνουν προσωπικά αναγνωρίσιμα στοιχεία.

Κεφάλαιο 7

Επίλογος - Συμπεράσματα

Στις μέρες μας, μια νέα γενιά συστημάτων στηρίζεται σε τεχνολογίες που εμπνέονται από το Blockchain και συγκεντρώνουν υψηλό ενδιαφέρον λόγω των προοπτικών που εμφανίζουν. Τα πλεονεκτήματα είναι πολλά. Αρχικά, αποκλείουν κάθε κεντρική αρχή, με αποτέλεσμα να αποφεύγουν ένα μόνο σημείο επίθεσης. Επίσης, αποτελούν μια προσπάθεια να προσφέρουν στο ιδιωτικό απόρρητο αλλά και στο απόρρητο του παραλήπτη αξιόπιστες συναλλαγές. Αυτά μπορούν να συμβούν χάρη σε κρυπτογραφικά πρωτόκολλα, αλλά και σχήματα με καινοτόμα σχέδια που ανοίγουν τον δρόμο σε ενδιαφέρουσες νέες εφαρμογές ασκώντας επίδραση στην κοινωνία. Όταν αναφερόμαστε σε κρυπτονομίσματα προκύπτουν πολλά πλεονεκτήματα όπως τα χαμηλότερα κόστη και οι ταχύτερες συναλλαγές. Ταυτόχρονα, είναι εμφανείς και κάποιες αδυναμίες αναφορικά με την ασφάλεια και την ιδιωτικότητα, όπως για παράδειγμα hacking, κλοπή πορτοφολιού, επιθέσεις DoS**.** Τα δύο θεμελιώδη προβλήματα που αντιμετωπίζει το Blockchain – αυτά της ιδιωτικής ζωής και της επεκτασιμότητας – ευνοούν την εμφάνιση πρωτοκόλλων όπως το Enigma. Συστήματα όπως αυτό είναι ενθαρρυντικά και δείχνουν μια επιτυχημένη προσπάθεια αντιμετώπισης επιθέσεων και ευπαθειών**.** Παρόλα, αυτά, μια από τις μεγαλύτερες επικρίσεις ενάντια στον σημερινό σχεδιασμό των συστημάτων που βασίζονται στο Blockchain είναι η ζήτηση για ανωνυμία. Αυτό με τη σειρά του επιβάλλει ειδικά έξοδα για τη διαχείριση του Blockchain μέσα από τις κατάλληλες λειτουργίες τιμολόγησης. Από την άλλη πλευρά, η ανωνυμία ενδεχομένως να ενθαρρύνει το έγκλημα. Επιπρόσθετα, το κόστος που απαιτεί η διαχείριση των συστημάτων αυτών επηρεάζει την πορεία υιοθέτησής τους. Ωστόσο, το πρόβλημα της εξόρυξης είναι στην πραγματικότητα ένα είδος γρίφου που δεν συνιστά καμία πρακτική ανησυχία εκτός από την ύπαρξη του ίδιου του δικτύου που απαιτεί αύξηση της ποσότητας των πόρων.

Πρωτόκολλα όπως το Enigma καινοτομούν ως προς τον τρόπο εκτέλεσης των υπολογισμών και ενισχύουν την διασφάλιση τη ιδιωτικότητας των δεδομένων και την ασφάλεια των συναλλαγών. Στην παρούσα διατριβή, αναλύθηκαν οι χρήσεις του Blockchain και τα ζητήματα ιδιωτικότητας που ανακύπτουν με βάση τρίπτυχο αντιμετώπιση, οφέλη, περιορισμοί. Επιπλέον, έγινε διερεύνηση του τρόπου με τον οποίο αντιμετωπίζονται τα ζητήματα ιδιωτικότητας που χαρακτηρίζουν τις πλατφόρμες Blockchain, τόσο γενικά, όσο και ειδικότερα μέσω του πρωτοκόλλου Enigma. Αναλύθηκαν τα συστατικά στοιχεία του πρωτόκολλου καθώς και η αρχιτεκτονική υλοποίησης του, με ιδιαίτερη αναφορά στον τρόπο εκτέλεσης των υπολογισμών. Τέλος, έγινε περιγραφή της υλοποίησης Enigma Catalyst η οποία και αποτελεί την πρώτη ουσιαστική εφαρμογή του πρωτοκόλλου Enigma για την διασφάλιση τη ιδιωτικότητας των δεδομένων. Με βάση την ανάλυση που έγινε, με ευκολία συμπεραίνει κανείς πως ναι μεν οι προκλήσεις είναι μεγάλες, αλλά από τη άλλη υπάρχει συνεχής εξέλιξη και πρόοδος σε ότι έχει να κάνει με τη διασφάλιση της ιδιωτικότητας και την θωράκιση του Blockchain απέναντι σε ευπάθειες. Είναι υλοποιήσιμο ένα πλαίσιο ισορροπίας μεταξύ του μέγιστου επιπέδου διασφάλισης της ιδιωτικότητας και της ελαχιστοποίησης της πιθανότητας παραβίασης της μέσω του Blockchain, κρατώντας παράλληλα το πρωτόκολλο χρηστικό και εύκολα προσβάσιμο στον μέσο χρήστη.

Κλείνοντας την παρούσα διατριβή, αξίζει να σημειωθεί πως στατιστικές σχετικές με το Bitcoin [57] –βασικό χρήστη των τεχνολογιών Blockchain– αναφέρουν ότι σε πραγματικό χρόνο η ενέργεια που χρειάζεται να καταναλώσει το δίκτυο είναι ίση με το 100% της κατανάλωσης σε ηλεκτρισμό της Κολομβίας, ενώ αγγίζει το 45% και 89% της ζήτησης σε Ιταλία και Τσεχία αντίστοιχα. Γίνεται λοιπόν αντιληπτό πως με τις προκλήσεις που αντιμετωπίζει η ανθρωπότητα σχετικά με το κλίμα και το περιβάλλον, η αύξηση της κατανάλωσης ενέργειας δεν αποτελεί μια εφικτή επιλογή. Είναι προφανές ότι η κλιματική αλλαγή θα αποτελέσει κύριο προβληματισμό στο μέλλον αναφορικά και με τις τεχνολογίες Blockchain καθώς οι προκλήσεις και τα οφέλη είναι πολλά.

Βιβλιογραφία

[01] https://www.blockchaintechnologies.com/glossary/

[02] https://www.coindesk.com/information

[03] https://bitcoin.org/en/developer-documentation

[04] Nolan Bauerle, What is Blockchain Technology?
Από https://www.coindesk.com/information/what-is-blockchain-technology

[05] https://bitcoin.org/en/blockchain-guide

[06] Margaret Leigh Sinrod, Still don't understand the blockchain? This explainer will help, 2018. Από https://www.weforum.org/agenda/2018/03/blockchain-bitcoin-explainer-shiller-roubini/

[07] Thomson Reuters Reports, Are you ready for blockchain?, 2018. Από https://www.thomsonreuters.com/en/reports/blockchain.html

[08] Noelle Acheson, How Bitcoin Mining Works, 2018. Από https://www.coindesk.com/information/how-bitcoin-mining-works

[09] Nolan Bauerle, What Are the Applications and Use Cases of Blockchains?, 2018. Από https://www.coindesk.com/information/applications-use-cases-blockchains

[10] Blockgeeks report, 17 Blockchain Applications That Are Transforming Society, 2018. Από https://blockgeeks.com/guides/blockchain-applications/

[11] Jacob Boersma, 5 blockchain technology use cases in financial services, 2019. Από https://www2.deloitte.com/nl/nl/pages/financial-services/articles/blockchain-technology-use-cases-in-financial-services.html

[12] Blockchain Applications and Services, SAP, 2019. Από https://www.sap.com/greece/products/leonardo/blockchain.html

[13] Mayank Pratap, How is Blockchain Revolutionizing Banking and Financial Markets, 2018. Από https://hackernoon.com/how-is-blockchain-revolutionizing-banking-and-financial-markets-9241df07c18b

[14] Bitsy article, Banking and Blockchain: Why We Need an AML/KYC Safe Harbor, 2018. Από https://bitsy.com/news/banking-and-blockchain-why-we-need-an-amlkyc-safe-harbor/

[15] Steven Hopkins, Banking and Blockchain: Why We Need an AML/KYC Safe Harbor, 2017. Από https://www.coindesk.com/banking-and-blockchain-why-we-need-an-amlkyc-safe-harbor

[16] EY Reporting Insights, Impact of blockchain services on the Financial sector, 2018. Από https://www.ey.com/Publication/vwLUAssets/ey-impact-of-blockchain-on-the-financial-services-sector/$File/ey-impact-of-blockchain-on-the-financial-services-sector.pdf

[17] https://github.com/machinomy/awesome-non-financial-blockchain

[18] Forbes, Five Non-Financial Blockchain Use Cases Marketers Need To Understand, 2018. Από https://www.forbes.com/sites/forbescommunicationscouncil/2018/03/27/five-non-financial-blockchain-use-cases-marketers-need-to-understand/

[19] Bogdan Tanygin, Blockchain in Non-Financial Industries: Overview, 2018. Από https://www.infopulse.com/blog/blockchain-in-non-financial-industries-overview/

[20] https://storj.io/whitepaper/

[21] Stan Higgins, IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things, 2015. Από https://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things

[22] EY startup challenge, 2016. Από https://www.ey.com/uk/en/services/specialty-services/ey-startup-challenge

[23] Mike Butcher, Verisart brings blockchain certification to the global art auction market, 2018. Από https://techcrunch.com/2018/05/03/verisart-brings-blockchain-certification-to-the-global-art-auction-market/

[24] https://www.havocscope.com/tag/united-states/

[25] https://www.havocscope.com/tag/counterfeit-drugs/

[26] Arnon Benshahar, 6 Ways the Blockchain is Revitalizing Social Networking, 2019. Από https://cryptopotato.com/6-ways-blockchain-revitalizing-social-networking/

[27] Sam Mire, Blockchain For Social Media: 11 Possible Use Cases, 2018. Από https://www.disruptordaily.com/blockchain-use-cases-social-media/

[28] Συντακτική ομάδα «ellinika hoaxes», Το Facebook ανέθεσε στα Ellinika Hoaxes την επαλήθευση γεγονότων, 2019. Από https://www.ellinikahoaxes.gr/2019/05/02/facebook-third-party-fact-checking-program/

[29] https://legiscan.com/gaits/search?state=US&keyword=blockchain

[30] Yogita Khatri, Christine Kim, Wyoming Lawmakers Pass Three Bills in Boost for State's Crypto Industry, 2019. Από https://www.coindesk.com/wyoming-lawmakers-pass-three-bills-in-boost-for-states-crypto-industry

[31] Yogita Khatri, US Income Tax Payers Can Now Get Refunds in Bitcoin, 2019. Από https://www.coindesk.com/us-income-tax-payers-can-now-get-refunds-in-bitcoin

[32] Kevin C. Desouza, Chen Ye, and Kiran Kabtta Somvanshi, Blockchain and U.S. state governments: An initial assessment, Brookings TechTank, 2018. Από https://www.brookings.edu/blog/techtank/2018/04/17/blockchain-and-u-s-state-governments-an-initial-assessment/

[33] Axel P. Lehmann, The future of crypto-assets, from opportunities to policy implications, World Economic Forum, 2018. Από

https://www.weforum.org/agenda/2018/12/crypto-assets-opportunities-policy-implications-ubs/

[34] General Data Protection Regulation (GDPR), Grant Thornton, 2017. Από https://www.grant-thornton.gr/globalassets/1.-member-firms/greece/insights/pdfs/publications/gt_gdpr_2017-brochure.pdf

[35] Μιχάλης Ροδάκης, Ο νέος κανονισμός & η επίδρασή του στο σύγχρονο επιχειρηματικό περιβάλλον, Grant Thornton Articles and Publications, 2017. Από https://www.grant-thornton.gr/insights/article/GDPR/

[36] David Meyer, Blockchain technology is on a collision course with EU privacy law, The Privacy Advisor, 2018. Από https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/

[37] Karen Epper Hoffman, Will privacy be a stumbling block for blockchain?, SC Media, 2018. Από https://www.scmagazine.com/home/security-news/features/will-privacy-be-a-stumbling-block-for-blockchain/

[38] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679

[39] Lotte Schou-Zibell, Nigel Phair, How secure is blockchain?, World Economic Forum, 2018. Από https://www.weforum.org/agenda/2018/04/how-secure-is-blockchain/

[40] Adam Waks, Blockchain and Privacy, 2017.
Από https://www.blockchainandthelaw.com/2017/11/blockchain-and-privacy/

[41] Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops, 2015. Από https://enigma.co/ZNP15.pdf & https://ieeexplore.ieee.org/abstract/document/7163223

[42] https://en.bitcoin.it/wiki/CoinJoin

[43] Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate, CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin?, MMCI, Saarland University, 2014. Από https://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf

[44] Mauro Conti, E. Sandeep Kumar, Chhagan Lal, Sushmita Ruj, A Survey on Security and Privacy Issues of Bitcoin, IEEE Communications Surveys & Tutorials 2018, 2018. Από https://www.semanticscholar.org/paper/A-Survey-on-Security-and-Privacy-Issues-of-Bitcoin-Conti-Kumar/1973f0f8815ec63abd21b0e191846efa2041125a & https://ieeexplore.ieee.org/document/8369416

[45] http://wcibtc.com

[46] Robby Houben, Alexander Snyers, Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion. Directorate-General for Internal Policies. 2018. Από http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

[47] Marco Iansiti, Karim Lakhani. The truth about blockchain. *Harvard Business Review*, 2017, 95.1: 118-127.

[48] Primavera De Filippi, The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production, Issue*, 2016, 7.

[49] Eric Rescorla, N. Resonance, Introduction to distributed hash tables. *IETF-65 Technical Plenary*, 2006, 130-138.

[50] Rakel Haakegaard, Joanna Lang, The elliptic curve diffie-hellman (ecdh). Από https://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Haakegaard+Lang.pdf, 2015.

[51] Nick Szabo, Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought, (16)*, 1996, 18.

[52] Jan-Erik Ekberg, Kari Kostiainen, N. Asokan, The untapped potential of trusted execution environments on mobile devices. *IEEE Security & Privacy*, 2014, 12.4: 29-37.

[53] Intel, Intel Software Guard Extensions-SGX. Από https://software.intel.com/en-us/sgx

[54] David Karger, et al. Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the world wide web. In: *STOC*. 1997. p. 654-663.

[55] https://docs.docker.com/install/linux/docker-ce/ubuntu/

[56] https://blog.enigma.co/

[57] https://digiconomist.net/bitcoin-energy-consumption

Σημείωση: Όλοι οι σύνδεσμοι είναι έγκυροι την 12η Μαΐου 2019.