ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ

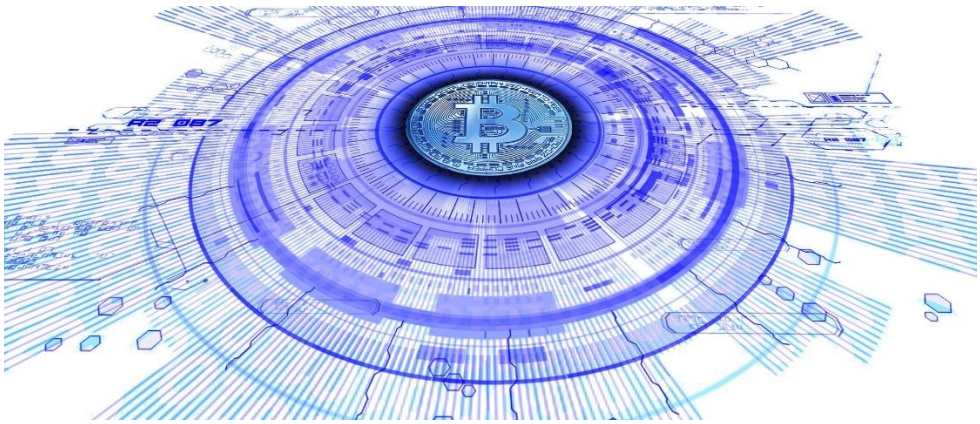
ΠΜΣ: ΨΗΦΙΑΚΗ ΚΑΙΝΟΤΟΜΙΑ ΚΑΙ ΔΙΟΙΚΗΣΗ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

BLOCKCHAIN: ΚΑΙΝΟΤΟΜΕΣ ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΙΘΑΝΟΙ ΚΙΝΔΥΝΟΙ

ΕΠΙΜΕΛΕΙΑ: ΣΤΡΕΚΛΑ ΦΛΩΡΕΝΤΙΑ

ΕΠΙΒΛΕΠΩΝ: ΣΤΑΜΑΤΙΟΥ ΙΩΑΝΝΗΣ, ΚΑΘΗΓΗΤΗΣ



ΠΑΤΡΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS
Σχολή Οικονομικών Επιστημών και Διοίκησης Επιχειρήσεων
Τμήμα Διοικητικής Επιστήμης & Τεχνολογίας

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΨΗΦΙΑΚΗ ΚΑΙΝΟΤΟΜΙΑ ΚΑΙ ΔΙΟΙΚΗΣΗ
DIGITAL INNOVATION AND MANAGEMENT

Στρέκλα Φλωρεντία

2022, Με την επιφύλαξη παντός δικαιώματος

Δηλώνω ότι έχω λάβει γνώση και γνωρίζω τις συνέπειες του νόμου και των οριζομένων στους Κανονισμούς Σπουδών του ΠΜΣ και του Τμήματος και στον Εσωτερικό Κανονισμό Λειτουργίας του Πανεπιστημίου Πατρών, καθώς και ότι η εργασία που καταθέτει με θέμα «Blockchain: Καινοτόμες εφαρμογές και πιθανοί κίνδυνοι» έχει εκπονηθεί με δική μου ευθύνη τηρουμένων των προϋποθέσεων που ορίζονται στις ισχύουσες διατάξεις και στον παρόντα Κανονισμό.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ v

ΠΕΡΙΛΗΨΗ vi

SUMMARY vii

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ vii

ΕΙΣΑΓΩΓΗ viii

1. Η ΤΕΧΝΟΛΟΓΙΑ *BLOCKCHAIN* 1

1.1 ΔΟΜΗ ΤΟΥ *BLOCKCHAIN* 1

1.2 ΣΥΓΚΕΝΤΡΩΤΙΚΑ ΕΝΑΝΤΙ ΑΠΟΚΕΝΤΡΩΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ 2

1.3 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ 3

1.4 ΈΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ (*SMART CONTRACTS*) 6

1.4.1 ΙΔΙΟΤΗΤΕΣ ΕΞΥΠΝΩΝ ΣΥΜΒΟΛΑΙΩΝ 7

1.4.2 Χρήση έξυπνων συμβολαίων 8

1.4.3. ΠΛΑΤΦΟΡΜΕΣ *BLOCKCHAIN* ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝ ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ 9

1.5 ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ *BLOCKCHAIN* 10

1.5.1 ΚΡΥΠΤΟΓΡΑΦΙΑ 10

1.5.2 ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ - *HASH* ΣΥΝΑΡΤΗΣΕΙΣ: ΙΔΙΟΤΗΤΕΣ ΚΑΙ ΧΡΗΣΗ 11

1.5.3 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ 14

1.6 ΤΥΠΟΙ *BLOCKCHAIN* 14

1.6.1 ΔΗΜΟΣΙΟ *BLOCKCHAIN* 15

1.6.2 ΙΔΙΩΤΙΚΟ *BLOCKCHAIN* 16

1.6.3 ΚΟΙΝΟΠΡΑΚΤΙΚΟ *BLOCKCHAIN* 16

1.7 ΑΛΓΟΡΙΘΜΟΙ ΣΥΝΑΙΝΕΣΗΣ ΓΙΑ ΤΟ *BLOCKCHAIN* 16

1.7.1 ΑΠΟΔΕΙΞΗ ΕΡΓΑΣΙΑΣ (*POW – PROOF OF WORK*) 17

1.7.2. ΑΠΟΔΕΙΞΗ ΣΥΜΜΕΤΟΧΗΣ (*POS – PROOF OF STAKE*) 17

1.7.3 ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΗ ΑΠΟΔΕΙΞΗ ΣΥΜΜΕΤΟΧΗΣ 17

1.7.4. ΑΠΟΔΕΙΞΗ ΤΟΥ ΠΑΡΕΛΘΟΝΤΟΣ ΧΡΟΝΟΥ 18

1.7.5 ΠΡΑΚΤΙΚΗ ΑΝΟΧΗ ΒΥΖΑΝΤΙΝΟΥ ΣΦΑΛΜΑΤΟΣ 18

1.7.6. ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΗ ΑΝΟΧΗ ΒΥΖΑΝΤΙΝΟΥ ΣΦΑΛΜΑΤΟΣ 18

1.7.8 ΑΠΟΔΕΙΞΗ ΒΑΡΟΥΣ (*POWEIGHT*) 19

1.7.9 *PROOF OF BURN (POB)* 19

1.7.10 ΑΠΟΔΕΙΞΗ ΙΚΑΝΟΤΗΤΑΣ (*PROOF OF CAPACITY*) 20

1.7.11 ΑΠΟΔΕΙΞΗ ΣΗΜΑΣΙΑΣ (*PROOF OF IMPORTANCE*) 21

1.7.12 ΑΠΟΔΕΙΞΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ (*PROOF OF ACTIVITY*) 22

1.7.13 ΚΑΤΕΥΘΥΝΟΜΕΝΑ ΑΚΥΚΛΙΚΑ ΓΡΑΦΗΜΑΤΑ (*DIRECTED ACYCLIC GRAPHS*) 22
1.8 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ *BLOCKCHAIN* 24
1.9 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ *BLOCKCHAIN* 26
2. ΤΟΜΕΙΣ ΕΦΑΡΜΟΓΗΣ BLOCKCHAIN 28
2.1 ΥΓΕΙΑ 28
2.1.1 ΣΥΣΤΗΜΑ *TMIS (TELECARE MEDICAL INFORMATION SYSTEMS)* 28
2.1.2 ΗΛΕΚΤΡΟΝΙΚΟ ΣΥΣΤΗΜΑ ΥΓΕΙΑΣ 29
2.1.3 ΔΕΔΟΜΕΝΑ ΥΓΕΙΑΣ ΚΑΙ ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΜΟΙΡΑΣΗΣ 30
2.1.4 ΚΛΙΝΙΚΕΣ ΔΟΚΙΜΕΣ 30
2.1.5 ΒΙΟΜΗΧΑΝΙΑ ΦΑΡΜΑΚΩΝ 31
2.2 ΤΟΥΡΙΣΜΟΣ 31
2.3 ΚΥΒΕΡΝΗΣΗ 31
2.4 ΤΡΑΠΕΖΙΚΟΣ ΤΟΜΕΑΣ 32
2.5 MARKETING – ΨΥΧΑΓΩΓΙΑ 33
2.6 ΑΣΦΑΛΕΙΑ 34
3. ΕΜΠΟΡΙΚΕΣ ΕΦΑΡΜΟΓΕΣ BLOCKCHAIN 34
3.1 ΥΓΕΙΑ 34
3.1.1 ΕΦΑΡΜΟΓΗ *PATIENTORY* 34
3.1.2 ΕΦΑΡΜΟΓΗ *MEDICALCHAIN* 35
3.1.3 ΕΦΑΡΜΟΓΗ *CORAL HEALTH* 36
3.1.4 ΕΦΑΡΜΟΓΗ *CLINICO* 36
3.1.5 ΕΦΑΡΜΟΓΗ *ISOLVE* 37
3.1.6 ΕΦΑΡΜΟΓΗ *CURISIUM* 37
3.1.7 ΕΦΑΡΜΟΓΗ *CHRONICLED* 38
3.1.8 ΕΦΑΡΜΟΓΗ *COVID-19* 39
3.2 ΤΟΥΡΙΣΜΟΣ 40
3.2.1 ΕΦΑΡΜΟΓΗ *LOCKTRIP* 40
3.2.2 ΕΦΑΡΜΟΓΗ *SMARTTRIP* 40
3.3.3 ΕΦΑΡΜΟΓΗ *GOUREKA* 41
3.3 ΚΥΒΕΡΝΗΣΗ 41
3.3.1 ΕΦΑΡΜΟΓΗ *FOLLOW MY VOTE* 41
3.4 ΤΡΑΠΕΖΙΚΟΣ ΤΟΜΕΑΣ 42
3.4.1 ΕΦΑΡΜΟΓΗ *RIPPLE* 42
3.5 MARKETING – ΨΥΧΑΓΩΓΙΑ 42
3.5.1 ΕΦΑΡΜΟΓΗ *MEDIACHAIN* 42

3.5.2 ΕΦΑΡΜΟΓΗ *UJO* 42
3.5.3 ΕΦΑΡΜΟΓΗ *CHOON* 42
3.6 ΑΣΦΑΛΕΙΑ 42
3.6.1 ΕΦΑΡΜΟΓΗ *ETHERISC* 42
3.6.2 ΕΦΑΡΜΟΓΗ *BEENEST* 43
3.6.3 ΕΦΑΡΜΟΓΗ *GUARDTIME* 43
3.6.4 ΕΦΑΡΜΟΓΗ *FIDENTIAX* 43
3.6.5 ΕΦΑΡΜΟΓΗ *B3I* 43
3.6.6 ΕΦΑΡΜΟΓΗ *DYNAMIS* 44
3.6.7 ΕΦΑΡΜΟΓΗ *LEMONADE* 44
3.6.8 ΕΦΑΡΜΟΓΗ *FIZZY* 44
3.6.9 ΕΦΑΡΜΟΓΗ *TEAMBRELLA* 44
4. ΚΙΝΔΥΝΟΙ – ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ BLOCKCHAIN 45
4.1 ΟΡΙΣΜΟΙ ΚΙΝΔΥΝΟΙ – ΑΠΕΙΛΕΣ 45
4.1.1 *BLOCKCHAIN* ΚΙΝΔΥΝΟΙ 45
4.1.2 ΑΠΕΙΛΕΣ BLOCKCHAIN 46
4.1.2.1 ΑΠΕΙΛΕΣ BLOCKCHAIN ΣΤΗΝ ΥΓΕΙΑ 46
4.2 ΕΙΔΗ - ΠΕΡΙΠΤΩΣΕΙΣ ΕΠΙΘΕΣΕΩΝ 47
4.2.1 ΕΠΙΘΕΣΕΙΣ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΗΝ ΣΥΝΑΙΝΕΣΗ ΚΑΙ ΤΟ ΚΑΘΟΛΙΚΟ 47
4.2.1.1 ΕΠΙΘΕΣΗ FINNEY 48
4.2.1.2 ΕΠΙΘΕΣΗ RACE (ΑΓΩΝΑ) 49
4.2.1.3 ΕΠΙΘΕΣΗ 51% 49
4.2.2 ΕΠΙΘΕΣΗ ΔΙΚΤΥΟΥ ΑΠΟ ΟΜΟΤΙΜΟΥΣ ΧΡΗΣΤΕΣ 50
4.2.4.1 ΕΠΙΘΕΣΗ SYBIL 50
4.2.4.2 ΕΠΙΘΕΣΗ ΈΚΛΕΙΨΗΣ (ECLIPSE) 51
4.2.4.3 ΚΑΤΑΝΕΜΗΜΕΝΗ ΑΡΝΗΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ (DDOS) 52
4.2.4.4 ΕΠΙΘΕΣΗ ΔΡΟΜΟΛΟΓΗΣΗΣ 53
4.2.3. ΕΠΙΘΕΣΕΙΣ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΕ ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ (*SMART BASED CONTRACT ATTACKS*) 54
4.2.3.1 ΕΠΙΘΕΣΗ DAO 54
4.2.4 ΕΠΙΘΕΣΕΙΣ ΜΕ ΒΑΣΗ ΤΟ ΠΟΡΤΟΦΟΛΙ (*WALLET BASED ATTACKS*) 54
4.3 ΠΕΡΙΠΤΩΣΕΙΣ ΠΡΑΓΜΑΤΙΚΩΝ ΕΠΙΘΕΣΕΩΝ 54
5. ΣΥΜΠΕΡΑΣΜΑΤΑ 58
6. ΒΙΒΛΙΟΓΡΑΦΙΑ 59

ΠΡΟΛΟΓΟΣ

Η σύγχρονη εποχή έχει κάνει αρκετά ψηφιακά άλματα σε όλους τους τομείς της τεχνολογίας. Τα τελευταία χρόνια έχει παρατηρηθεί η εισαγωγή ενός νέου περιουσιακού στοιχείου, του λεγόμενου κρυπτονομίσματος. Η βασική τεχνολογία του κρυπτονομίσματος είναι η τεχνολογία blockchain. Η εν λόγω τεχνολογία είναι ακόμα αναπτυσσόμενη σε αρκετούς κλάδους όπως υγεία, φαρμακοβομηχανία, κυβέρνηση, ασφαλιστικός τομέας, ψυχαγωγία και άλλα και προσφέρει αρκετά οφέλη. Όμως, από την άλλη πλευρά, υπάρχουν και μειονεκτήματα.

ΠΕΡΙΛΗΨΗ

Σκοπός αυτής της διπλωματικής εργασίας είναι να περιγράψει τα κύρια χαρακτηριστικά της τεχνολογίας blockchain και κατόπιν να αναλύσει τις καινοτόμες εφαρμογές αυτής της τεχνολογίας, καθώς και τους πιθανούς κινδύνους.

Η εργασία αναλύει αρχικά όλα τα κύρια σημεία του blockchain, ούτως ώστε ο αναγνώστης να καταλάβει την έννοια και κατόπιν αναλύει τους τομείς εφαρμογής του, τις εφαρμογές που χρησιμοποιείται και τους πιθανούς κινδύνους.

Συγκεκριμένα, το κεφάλαιο 1 είναι αφιερωμένο στην επεξήγηση των σημείων του blockchain. Το κεφάλαιο 2 εξηγεί τους τομείς εφαρμογής του blockhain. Το κεφάλαιο 3 αναλύει τις εμπορικές εφαρμογές που βασίζονται στην τεχνολογία blockchain και το κεφάλαιο 4 αποτυπώνει τους πιθανούς κινδύνους και περιπτώσεις επιθέσεων. Τέλος, στο κεφάλαιο 5 παρατίθενται τα συμπεράσματα από την ανάλυση των προηγούμενων 4 κεφαλαίων.

SUMMARY

The purpose of this thesis is to describe the main features of blockchain technology and then to analyze the innovative applications of this technology, as well as the potential risks.

The work first analyzes all the main points of the blockchain, so that the reader understands the meaning and then analyzes its application areas, the applications used and the potential risks.

Specifically, Chapter 1 is devoted to explaining the points of the blockchain. Chapter 2 explains the application areas of blockhain. Chapter 3 analyzes commercial applications based on blockchain technology and Chapter 4 captures the potential risks and cases of attacks. Finally, chapter 5 presents the conclusions from the analysis of the previous 4 chapters.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Blockchain, Κρυπτονόμισμα, Έξυπνο συμβόλαιο (Smart Contract), Bitcoin, Peer to Peer, Υγεία, Εμπορικές Εφαρμογές, Καθολικό, Δίκτυο, Συνάρτηση Κατακερματισμού (Hash), Επίθεση.

ΕΙΣΑΓΩΓΗ

Το blockchain και οι εφαρμογές του αποκτούν όλο και περισσότερο δημοσιότητα τα τελευταία χρόνια. Αυτό συμβαίνει διότι αρκετές εταιρείες δημιούργησαν τις εμπορικές εφαρμογές, οι οποίες έχουν επιφέρει σημαντικά οφέλη σε πολλούς τομείς. Η παρούσα πτυχιακή εργασία εκπονήθηκε στα πλαίσια του ΜΠΣ Ψηφιακή Καινοτομία & Διοίκηση και έχει ως σκοπό να παρουσιάσει τα κύρια σημεία του blockchain, τους τομείς εφαρμογής του, τα εμπορικές εφαρμογές που αναπτύχθηκαν καθώς και πιθανούς κινδύνους και οφέλη.

1. Η ΤΕΧΝΟΛΟΓΙΑ *BLOCKCHAIN*

Τα τελευταία χρόνια παρατηρήθηκε η εμφάνιση ενός νέου τύπου εμπορεύσιμου περιουσιακού στοιχείου που ονομάζεται κρυπτονόμισμα. Ως βασική τεχνολογία που κρύβεται στα κρυπτονομίσματα αποτελεί η τεχνολογία *blockchain*, η οποία παρέχει ένα κατανεμημένο και αποκεντρωμένο περιβάλλον για συναλλαγές των αναδυόμενων κρυπτονομισμάτων συμπεριλαμβανομένου του κρυπτονομίσματος *Bitcoin*. Μαζί με την ταχεία ανάπτυξη της τεχνολογίας του *blockchain*, αυτά τα κρυπτονομίσματα που βασίζονται στην τεχνολογία *blockchain* έχουν επίσης κερδίσει αυξανόμενη δημοτικότητα και προσοχή την τελευταία δεκαετία.

1.1 ΔΟΜΗ ΤΟΥ *BLOCKCHAIN*

Για να γίνει κατανοητή η έννοια του *blockchain*, πρέπει να γίνει από επιχειρηματική και τεχνική προοπτική. Το *Blockchain* είναι ένα σύστημα εγγραφών για συναλλαγή αξίας σε ένα ομότιμο δίκτυο (*peer to peer network*). Αυτό σημαίνει ότι δεν υπάρχει ανάγκη για κάποιο αξιόπιστο μεσάζοντα όπως τράπεζες, μεσίτες ή άλλες υπηρεσίες για να χρησιμεύσουν ως έμπιστο τρίτο μέρος. Για παράδειγμα, για ποιο λόγο να πληρώσει μέσω τραπέζης ένα ποσό 10€ ο Α στον Β;

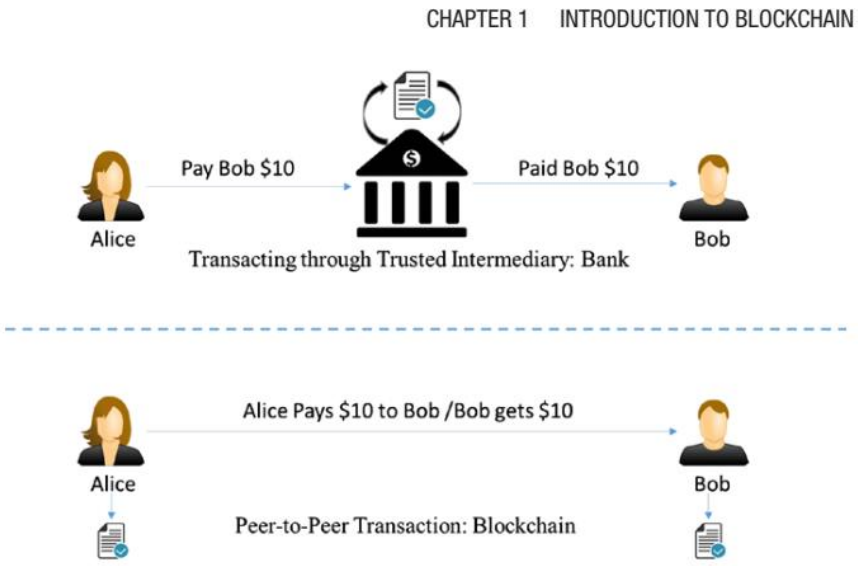


Figure 1-1. *Transaction through an intermediary vs. peer-to-peer transaction*

Πηγή: https://link.springer.com/book/10.1007/978-1-4842-3444-0

Εάν κάποιος θέλει να αγοράσει μετοχές από μια εταιρεία ή ένα άτομο, μπορούν απλώς να τις αγοράσουν απευθείας με άμεσο διακανονισμό, δεν χρειάζονται μεσίτες, γραφεία εκκαθάρισης ή άλλα χρηματοπιστωτικά ιδρύματα ενδιάμεσα.

Το *Blockchain* είναι ένα ομότιμο (*peer-to-peer*) σύστημα συναλλαγής χωρίς έμπιστα μέρη ενδιάμεσα.

• Αποτελεί κοινόχρηστο, αποκεντρωμένο και ανοιχτό καθολικό συναλλαγών. Αυτή η βάση δεδομένων αναπαράγεται σε ένα μεγάλο αριθμό κόμβων (*blocks*).

• Σε αυτή τη βάση δεδομένων δεν μπορεί να αλλάξει ή να τροποποιηθεί κάτι. Αυτό σημαίνει ότι κάθε είσοδος είναι μία μόνιμη εγγραφή. Κάθε νέα καταχώρηση αντικατοπτρίζεται σε όλα τα αντίγραφα των βάσεων δεδομένων που φιλοξενούνται σε διαφορετικούς κόμβους.

• Δεν χρειάζεται να εξυπηρετούνται αξιόπιστα τρίτα μέρη ως μεσάζοντες για την επαλήθευση, την ασφάλεια και τον διακανονισμό συναλλαγών.

• Είναι ένα άλλο επίπεδο πάνω από το Διαδίκτυο και μπορεί να συνυπάρξει με άλλες τεχνολογίες Διαδικτύου.

• Η τεχνολογία *blockchain* σχεδιάστηκε για να ενεργοποιήσει πραγματική αποκέντρωση. Σε μια προσπάθεια να το κάνουν, οι δημιουργοί του *Bitcoin*, άφησαν ανοιχτό τον κώδικα, ώστε να μπορεί να εμπνεύσει πολλές αποκεντρωμένες εφαρμογές.

Κάθε κόμβος στο δίκτυο *blockchain* έχει το ίδιο αντίγραφο του *blockchain*, όπου κάθε μπλοκ είναι μια συλλογή από συναλλαγές. Υπάρχουν δύο κύρια μέρη σε κάθε μπλοκ. Το τμήμα "κεφαλίδα" συνδέεται πίσω με το προηγούμενο μπλοκ στην αλυσίδα. Αυτό σημαίνει ότι κάθε κεφαλίδα μπλοκ περιέχει τον κατακερματισμό του προηγούμενου μπλοκ, έτσι ώστε κανείς να μην μπορεί να αλλάξει οποιαδήποτε συναλλαγή στο προηγούμενο μπλοκ. Το άλλο μέρος ενός μπλοκ είναι το "περιεχόμενο σώματος" που έχει έναν επικυρωμένο κατάλογο συναλλαγών, τα ποσά τους, τις διευθύνσεις των μερών που εμπλέκονται και μερικές ακόμη λεπτομέρειες. Έτσι, δεδομένου του τελευταίου μπλοκ, είναι εφικτή η πρόσβαση σε όλα τα προηγούμενα μπλοκ σε ένα *blockchain*. [1]

1.2 ΣΥΓΚΕΝΤΡΩΤΙΚΑ ΕΝΑΝΤΙ ΑΠΟΚΕΝΤΡΩΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ένα συγκεντρωτικό κατανεμημένο σύστημα είναι αυτό στο οποίο υπάρχει ένας κύριος κόμβος υπεύθυνος για τη διάσπαση των εργασιών ή των δεδομένων και κατανέμει το φορτίο στους κόμβους. Ενώ, το αποκεντρωμένο σύστημα είναι αυτό στο οποίο δεν υπάρχει «κύριος» κόμβος ως τέτοιος και ακόμα ο υπολογισμός μπορεί να διανέμεται.

Συγκεντρωτικό σύστημα

[1] (Γιαννακού, 2019)

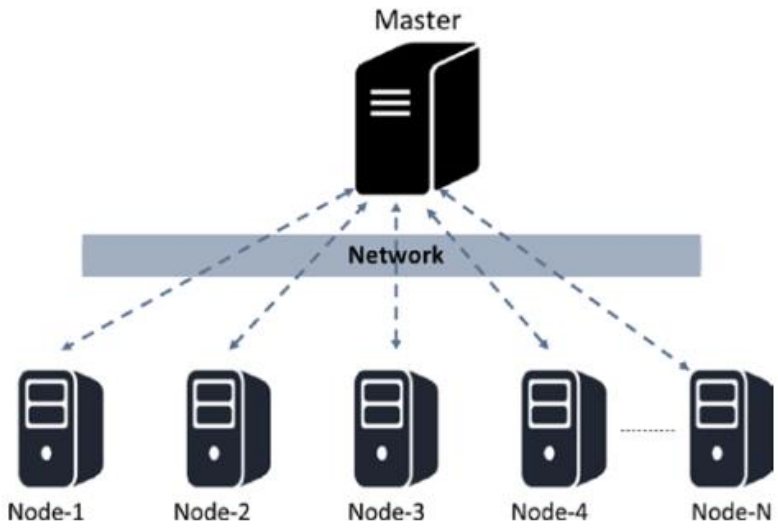


Figure 1-8. *A distributed system with centralized control*

Πηγή: https://link.springer.com/book/10.1007/978-1-4842-3444-0

Για να είναι ένα σύστημα συγκεντρωτικό/αποκεντρωμένο δεν περιορίζεται μόνο στην τεχνική αρχιτεκτονική.

Τεχνική Αρχιτεκτονική: Ένα σύστημα μπορεί να είναι συγκεντρωτικό ή αποκεντρωμένο από άποψη τεχνικής αρχιτεκτονικής. Πρέπει να δούμε πόσοι φυσικοί υπολογιστές (ή κόμβοι) χρησιμοποιούνται για το σχεδιασμό ενός συστήματος, πόσες αστοχίες κόμβων μπορεί να διατηρήσει πριν χαλάσει ολόκληρο το σύστημα κ.α.

Πολιτική προοπτική: Αυτή η προοπτική δείχνει τον έλεγχο που έχει σε ένα σύστημα ένα άτομο, ή μια ομάδα ανθρώπων, ή ένας οργανισμός στο σύνολό του. Εάν οι υπολογιστές του συστήματος ελέγχονται από αυτούς, τότε το σύστημα είναι φυσικά συγκεντρωτικό. Ωστόσο, εάν δεν υπάρχει συγκεκριμένο άτομο ή ομάδες που ελέγχουν το σύστημα και όλοι έχουν ίσα δικαιώματα στο σύστημα, τότε είναι ένα αποκεντρωμένο σύστημα με πολιτική έννοια.

Λογική προοπτική: Ένα σύστημα μπορεί να συγκεντρωθεί λογικά ή αποκεντρωμένα με βάση το πώς φαίνεται, ανεξάρτητα από το αν είναι συγκεντρωτικά ή αποκεντρωμένα τεχνικά ή πολιτικά.

Όλες οι προαναφερθείσες προοπτικές είναι ζωτικής σημασίας για το σχεδιασμό ενός πραγματικού συστήματος και αποκαλώντας το συγκεντρωτικό ή αποκεντρωμένο. [2]

1.3 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

Τα κρυπτονομίσματα είναι μη αναστρέψιμα και καταγράφονται στα μπλοκ, τα οποία συνδέονται με χρονολογική σειρά. Λόγω της ανοιχτής και διαφανούς φύσης του *blockchain*, τα αρχεία συναλλαγών κρυπτονομισμάτων, περιέχουν πλούσιες πληροφορίες. Τα ίχνη χρηματοοικονομικών δραστηριοτήτων είναι δημόσια προσβάσιμα, παρέχοντας έτσι στους ερευνητές πρωτοφανείς ευκαιρίες για εξόρυξη δεδομένων σε αυτή την περιοχή. Η κύρια αξία

[2] (Bashir, I. 2017)

της ανάλυσης και εξόρυξης των δεδομένων συναλλαγών των κρυπτονομισμάτων είναι διπλή: 1) Αφορά σε αρχεία συναλλαγών που είναι σχετικά ανεξερεύνητα γιατί αυτά τα αρχεία συναλλαγών συνήθως δεν είναι δημόσια προσβάσιμα για λόγους ασφάλειας και ενδιαφέροντος. Μέσα από την ανάλυση και την εξόρυξη αρχείων συναλλαγών κρυπτονομισμάτων, μπορούν να διερευνηθούν εκτενώς οι εμπορικές συμπεριφορές, η κατανομή πλούτου και ο παραγωγικός μηχανισμός ενός συστήματος συναλλαγών, καθώς και συμπεράσματα για διακυμάνσεις των οικονομικών στην αγορά κρυπτονομισμάτων.

2) Εξαιτίας της ανωνυμίας των συστημάτων *blockchain* και την έλλειψη εξουσίας, διάφοροι τύποι εγκλημάτων στον κυβερνοχώρο έχουν προκύψει στο οικοσύστημα *blockchain* τα τελευταία χρόνια. Εξαγωγή πληροφοριών από τα αρχεία συναλλαγών μπορεί να βοηθήσει στην παρακολούθηση συναλλαγών με κρυπτονομίσματα και στον εντοπισμό παράνομων συμπεριφορών, καθιερώνοντας έτσι αποτελεσματική ρύθμιση και οικοδομώντας ένα πιο υγιές *blockchain* οικοσύστημα.

Τα δίκτυα είναι μια γενική γλώσσα για την περιγραφή συστημάτων αλληλεπίδρασης στον πραγματικό κόσμο και η περίπλοκη επιστήμη των δικτύων θεωρείται ως ένα αποτελεσματικό εργαλείο για την ανάλυση της μοντελοποίησης, της δυναμικής, και της ευρωστίας πολλών δικτυωμένων συστημάτων. Ένα σημαντικό μέρος της υπάρχουσας εργασίας για συναλλαγές κρυπτονομισμάτων μελετάται από ένα δίκτυο προοπτικής αφαιρώντας αντικείμενα σε συστήματα κρυπτονομισμάτων όπως π.χ. λογαριασμούς, έξυπνα συμβόλαια και οντότητες ως κόμβοι και τις σχέσεις μεταξύ τους ως σύνδεσμοι. Σε ένα συγκεκριμένο σύστημα κρυπτονομισμάτων, εκεί μπορεί να υπάρχουν διάφορες διαφορετικές αλληλεπιδραστικές δραστηριότητες μεταξύ των χρηστών, όπως π.χ. μεταφορά χρημάτων, έξυπνη δημιουργία συμβολαίου και έξυπνη επίκληση συμβολαίου. Τα δίκτυα μπορούν να κατασκευαστούν για να μοντελοποιήσουν αυτές τις δραστηριότητες αλληλεπίδρασης στο σύστημα από διαφορετικές πτυχές και στη συνέχεια σε μία πληθώρα δικτύων μπορούν να χρησιμοποιηθούν προσεγγίσεις ανάλυσης για την ανάλυση χαρακτηριστικών του δικτύου, εξαγωγή πληροφοριών συναλλαγών, καθώς και για τον εντοπισμό μη φυσιολογικών ή παράνομων συμπεριφορών.

Ιστορικό

Τις τελευταίες δεκαετίες, η τεχνολογία του Διαδικτύου γνώρισε ραγδαία ανάπτυξη και σταδιακά γέννησε το ψηφιακό νόμισμα. Η πρώιμη μορφή του ψηφιακού νομίσματος μπορεί να ανιχνευθεί στην πρόταση της τυφλής υπογραφής της τεχνολογίας στη δεκαετία του 1980 και ένα μη ανιχνεύσιμο σύστημα πληρωμών βασισμένο σε αυτή την τεχνολογία. Αυτή η τεχνολογία εμπόδισε τα συγκεντρωτικά ιδρύματα που παρέχουν υπογραφές από τη σύνδεση των χρηστών στις συναλλαγές τους. Μια σειρά άλλων τεχνολογιών πληρωμής ψηφιακού νομίσματος, όπως καθολικά ηλεκτρονικά μετρητά, μη ανιχνεύσιμα μετρητά εκτός σύνδεσης, δίκαιες τυφλές υπογραφές, δίκαια εκτός σύνδεσης ηλεκτρονικά μετρητά, εμφανίστηκαν αργότερα στη δεκαετία του 1990. Ωστόσο, ένα κοινό πρόβλημα που υπήρχε σε αυτές τις τεχνολογίες είναι ότι τα αξιόπιστα τρίτα μέρη χρειάζονται για τον εντοπισμό επιθέσεων διπλών δαπανών.

Στα τέλη της δεκαετίας του 1990, προσεγγίσεις όπως το *B-Money*, το *Bit Gold* προέκυψε με μια προσπάθεια εξάλειψης του μεσάζοντα στη διαδικασία διαπραγμάτευσης. Μεταξύ αυτών, η *B-Money* πρότεινε για πρώτη φορά τη δημιουργία νομισμάτων από επίλυση υπολογιστικών γρίφων και αποκεντρωμένη συναίνεση. Κατά μία έννοια, η εμβρυϊκή μορφή κρυπτονομισμάτων - εικονικών νομισμάτων που εξασφαλίζονται από κρυπτογραφία χωρίς σύνδεση με οποιαδήποτε κεντρική αρχή εμφανίστηκαν στη *B-Money*. Ωστόσο, αυτές οι

προσεγγίσεις τελικά δεν κατάφεραν να κερδίσουν αρκετή προσοχή και η εφαρμογή της αποκεντρωμένης συναίνεσης ήταν ένα άλυτο πρόβλημα για μεγάλο χρονικό διάστημα.

Το 2004 ο *Hal Finney* παρουσίασε την ιδέα των «Επαναχρησιμοποιήσιμων αποδείξεων εργασίας» (*RPoW*) που βασίζεται σε αξιόπιστους υπολογιστές. Το 2008, το σύστημα *Bitcoin,* ένα ηλεκτρονικό σύστημα μετρητών *P2P*, ανακοινώθηκε από τον *Satoshi Nakamoto*.

Ακολούθησε η ανάπτυξη του πελάτη *Bitcoin* το 2009, με νόμισμα *Bitcoin* (*bitcoin,* συντομογραφία *BTC*), το πρώτο αποκεντρωμένο κρυπτονόμισμα, που δημιουργήθηκε ως ανταμοιβές και τέλη συναλλαγής για ανθρακωρύχους *Bitcoin* που δημιουργούν ένα νέο μπλοκ με την επίλυση ενός υπολογιστικά δύσκολου παζλ. Καθώς η βασική τεχνολογία που βασίζεται στο Bitcoin, το blockchain έχει λάβει εκτεταμένη προσοχή, που χρησιμοποιείται ευρέως στην ευφυή χρηματοδότηση, στο Διαδίκτυο των Πραγμάτων (*IoT*).

Μετά την επιτυχία του *Bitcoin*, μια σειρά από εναλλακτικά κρυπτονομίσματα γνωστά ως «*altcoins*» εμφανίστηκαν γρήγορα. Από το δεύτερο τρίμηνο του 2020, υπάρχουν περισσότερα από 7000 είδη κρυπτονομισμάτων με συνολικό ανώτατο όριο αγοράς 300 δισεκατομμυρίων δολαρίων. Μεταξύ αυτών, το *Ethereum* είναι το μεγαλύτερο σύστημα *blockchain* που επιτρέπει τα *turing*-complete έξυπνα συμβόλαια και το κύριο νόμισμα στο *Ethereum*, το οποίο αναφέρεται ως *Ether* (συντομογραφία *ETH*), είναι σήμερα το δεύτερο μεγαλύτερο κρυπτονόμισμα στον κόσμο μετά το *Bitcoin*. Ένα από τα πρώτα *altcoins* που ονομάζεται *Namecoin* επιτρέπει στους χρήστες να εγγραφούν με τους δικούς τους τομείς. Το *Litecoin,* που δημιουργήθηκε το 2011, είναι ένα είδος κρυπτονομίσματος παρόμοιο με το *Bitcoin* αλλά τέσσερις φορές γρηγορότερο από το *Bitcoin* κατά την επιβεβαίωση συναλλαγής. Το *Peercoin,* που προτάθηκε το 2012, υιοθετεί το *Proof of Stake* (*PoS*) ως συναινετικό αλγόριθμο και το *PoS* είναι μία εναλλακτική λύση εξοικονόμησης ενέργειας στο *Proof of Work* (*PoW*) στο *Bitcoin*. Το *Ripple* είναι ένα πιστωτικό δίκτυο βασισμένο σε κατανεμημένο πρωτόκολλο ανοιχτού κώδικα, παρέχει ένα διασυνοριακό περιβάλλον πληρωμών σε πραγματικό χρόνο που επιτρέπει συναλλαγές μεταξύ νόμιμων προσφορών και κρυπτονομισμάτων με χαμηλές χρεώσεις συναλλαγών. Λόγω του επιτυχημένου επιχειρηματικού μοντέλου του *Ripple*, το *token XRP* της *Ripple* έχει βρεθεί στην τρίτη θέση στην αγορά κρυπτονομισμάτων. Άλλα διάσημα κρυπτονομίσματα είναι το *Monero, Zerocash, EOS* και το *Libra*, των οποίων οι αναλυτικές πληροφορίες μπορούν να βρεθούν στα λευκά χαρτιά τους.[3]

Συναλλαγή

Στα συστήματα *blockchain*, μια συναλλαγή μπορεί να θεωρηθεί ως η λειτουργία χρήστη στο σύστημα. Όταν ξεκινά μια νέα συναλλαγή από έναν χρήστη, θα μεταδοθεί σε όλους τους κόμβους στο δίκτυο *P2P* και θα προστεθεί σε νέο μπλοκ.

Τα μοντέλα συναλλαγών των συστημάτων *blockchain* μπορούν γενικά να κατηγοριοποιηθούν στο μοντέλο με επίκεντρο τη συναλλαγή και στο λογαριασμό-κεντρικό μοντέλο, με το *Bitcoin* και το *Ethereum* να είναι τυπικά παραδείγματα, αντίστοιχα.

Στο *Bitcoin*, οι χρήστες προσδιορίζονται από τις διευθύνσεις *Bitcoin*, οι οποίες είναι *hashes* (συναρτήσεις κατακερματισμού) που δημιουργούνται από τα αντίστοιχα δημόσια κλειδιά τους. Ένας χρήστης μπορεί να έχει πολλές διευθύνσεις για να αυξήσει την ανωνυμία του. Το μοντέλο συναλλαγής του *Bitcoin* είναι ένα μοντέλο με επίκεντρο τη συναλλαγή, όπου μια συναλλαγή μπορεί να έχει πολλαπλές εισόδους και πολλαπλές εξόδους, που σχετίζεται με πολυδιευθύνσεις. Οι εισροές αποτελούνται από ένα σύνολο αδιάθετων συναλλαγών εκροές (*UTXO*) των οποίων το άθροισμα του ποσού δεν είναι μικρότερο από το ποσό αυτό πρέπει να

[3] (DeMartino, 2017)

πληρωθεί και ο πληρωτής μπορεί να ορίσει μια νέα διεύθυνση για να λάβει την αλλαγή. Επιπλέον, δεν υπάρχει έννοια για το υπόλοιπο του λογαριασμού στο *Bitcoin*. Το υπόλοιπο ενός χρήστη *Bitcoin* μπορεί να υπολογιστεί με το άθροισμα της αξίας των διαθέσιμων *UTXO* στο πορτοφόλι του. Το μοντέλο συναλλαγών στο *Ethereum* είναι ένα μοντέλο με επίκεντρο τον λογαριασμό, που περιέχει δύο είδη λογαριασμών, συγκεκριμένα λογαριασμούς εξωτερικής ιδιοκτησίας (EOA) και λογαριασμούς συμβολαίου. Ένας EOA είναι παρόμοιος με μια τράπεζα λογαριασμού, ο οποίος μπορεί να καταθέσει/αντλήσει χρήματα και να καταγράψει κάποιες δυναμικές πληροφορίες σχετικά με το υπόλοιπο λογαριασμού. Συγκεκριμένα, ένας EOA μπορεί να δημιουργήσει σύμβαση λογαριασμών και επίκληση έξυπνων συμβάσεων. Κάθε λογαριασμός συμβολαίου σχετίζεται με ένα κομμάτι εκτελέσιμου *bytecode* και διατηρεί κατάσταση πληροφοριών όπως η τιμή κατακερματισμού του *bytecode* καθώς και την ισορροπία του λογαριασμού. Μια συναλλαγή στο *Ethereum* είναι ένα υπογεγραμμένο πακέτο δεδομένων από λογαριασμό σε άλλο και περιέχει μόνο μία είσοδο και μία έξοδο, η οποία είναι διαφορετική από το σενάριο στο *Bitcoin*.

Υπάρχουν τρεις κύριοι τύποι λειτουργιών που μπορούν να ολοκληρώσουν οι συναλλαγές στο *Ethereum*, κυρίως μεταβίβαση χρημάτων, δημιουργία συμβολαίου και επίκληση συμβολαίου. Σύμφωνα με το είδος αποστολέα συναλλαγών, οι συναλλαγές μπορούν να χωριστούν σε εξωτερικές συναλλαγές και εσωτερικές συναλλαγές. Μια συναλλαγή είναι εξωτερική μόνο εάν ξεκινά από EOA, ενώ μια εσωτερική συναλλαγή ενεργοποιείται από επίκληση συμβολαίου και η σύμβαση είναι ο αποστολέας της συναλλαγής της.

Αξίζει να σημειωθεί ότι μια εξωτερική συναλλαγή (δηλαδή μια λειτουργία συμβολαίου κλήση) μπορεί να οδηγήσει σε πολλές εσωτερικές συναλλαγές. [4] [5]

1.4 ΈΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ (*SMART CONTRACTS*)

Η τεχνολογία *Blockchain* είναι μια ισχυρή και αποκεντρωμένη πλατφόρμα ικανή να προχωρήσει πολύ περισσότερο από τις συναλλαγές με *bitcoin*. Μπορεί να ορίζεται ως αυτοματοποιημένο μηχανογραφικό πρωτόκολλο που χρησιμοποιείται για ψηφιακή χρήση, διευκολύνει, επαληθεύει ή εφαρμόζει τη συμφωνία για την εκτέλεση νομικής σύμβασης. Αποφεύγει την κεντρική αρχή ή τον ενδιάμεσο και επικυρώνει άμεσα τη σύμβαση μέσω ενός ταχύτερου, φθηνότερου και ασφαλέστερου τρόπου μέσω μιας κατανεμημένης πλατφόρμας. Π.χ. δύο άτομα που έρχονται σε επαφή μεταξύ τους για ορισμένες νομικές συμβάσεις. Μπορούν να επικοινωνήσουν μεταξύ τους με τεχνολογία *blockchain* όπου τα έξυπνα συμβόλαια χρησιμοποιούνται για τον έλεγχο και τη διαχείριση τέτοιου είδους συμβάσεων νομικής συμβουλευτικής χωρίς κανέναν δικηγόρο. Έτσι, με τη βοήθεια της τεχνολογίας *blockchain* που χρησιμοποιεί έξυπνα συμβόλαια, δεν υπάρχει ανάγκη για μεσάζοντες να συνάψουν νομική σύμβαση με οποιονδήποτε ανά πάσα στιγμή.

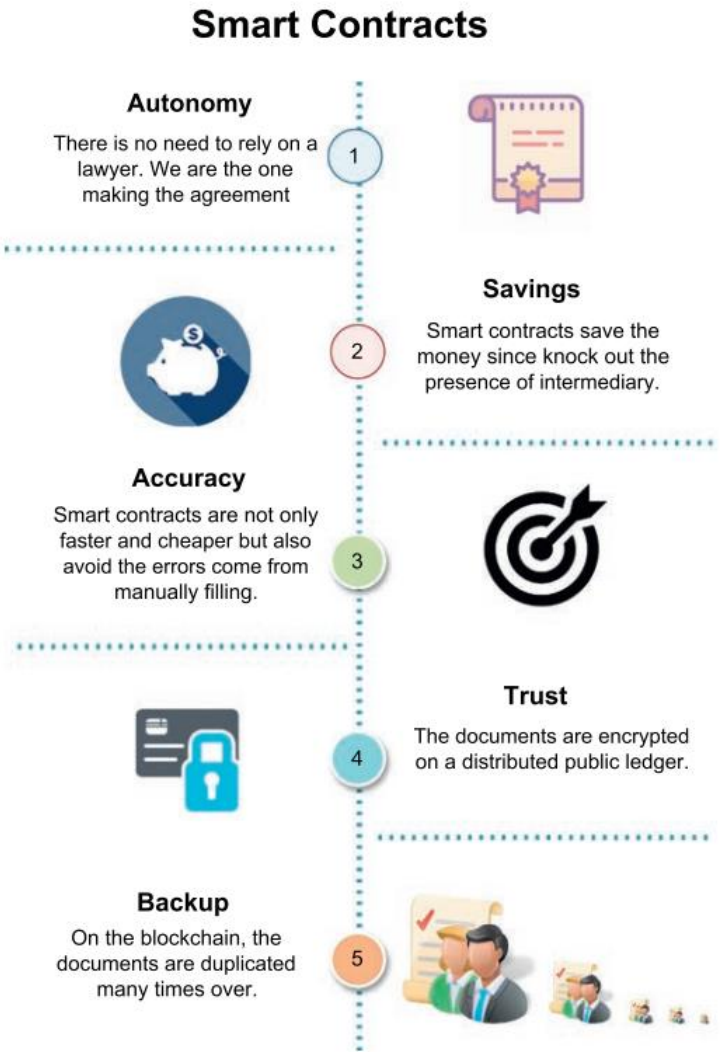
Ο όρος έξυπνο συμβόλαιο αναπτύχθηκε από τον *Nick Szabo* το 1994, έναν επιστήμονα υπολογιστών και κρυπτογράφο. Ως εκ τούτου, το *blockchain* είναι ανάπτυξη τεχνολογίας που χρησιμοποιείται για την πραγματοποίηση έξυπνων συμβόλαιων. Σε αυτό το πλαίσιο, τα έξυπνα συμβόλαια μπορούν να μετατραπούν σε κωδικούς υπολογιστών που μπορούν να αποθηκεύονται και να αναπαράγονται στο δίκτυο και εποπτεύονται από τους κόμβους δικτύου που υπάρχουν στο *blockchain*. Είναι ένα πρωτόκολλο υπολογιστή και αυτο-εκτελούμενο τμήμα, το οποίο ελέγχεται και διαχειρίζεται από ένα δίκτυο *P2P*. Βοηθάει στην ανταλλαγή μετοχών, νομίσματος, περιουσίας ή χρημάτων με διαφανή και ασφαλή τρόπο με τον οποίο αποφεύγονται οι υπηρεσίες μιας κεντρικής αρχής. Ο καλύτερος τρόπος για πλήρη

[4] (Jianjing, Jieli, Yijing, κ.α. 2021)
[5] (Καρσλίδης Δ., 2021)

κατανόηση των έξυπνων συμβολαίων είναι η σύγκριση με ένα μηχάνημα αυτόματης πώλησης. Παραδοσιακά, ένα άτομο πήγαινε σε συμβολαιογράφο ή δικηγόρο για τα έγγραφά του, τα πλήρωνε και περίμενε μέχρι κάποιος να πάρει τα έγγραφα πίσω. Αλλά, με τη βοήθεια των έξυπνων συμβάσεων, ένα άτομο απλώς «ρίχνει» ένα νόμισμα σε έναν αυτόματο πωλητή (όπως ένας δικηγόρος) και ρίχνει τα έγγραφα (π.χ. άδεια οδήγησης) στο λογαριασμό. [6]

1.4.1 ΙΔΙΟΤΗΤΕΣ ΕΞΥΠΝΩΝ ΣΥΜΒΟΛΑΙΩΝ

Η μη αυτόματη εγγραφή κωδικών μπορεί να έχει κάποια σφάλματα κατά την εκτέλεση και δαπάνη χρόνου για την ολοκλήρωση. Όμως τα έξυπνα συμβόλαια χρησιμοποιούν κώδικες λογισμικού που εκτελούν αυτόματα εργασίες και για την ολοκλήρωσή τους σε ένα χρονικό διάστημα. Οι ιδιότητες που μας δίνει το έξυπνο συμβόλαιο σε πραγματικό χρόνο είναι οι ακόλουθες:



Πηγή:
https://reader.elsevier.com/reader/sd/pii/S006524582030070X?token=D829FF236E7D0EA2CEDC8E0F3A577F6C0AB253291B8DF5EF128497C3EDCD8EA8FA060698B705A9E170A20BD3277A4B6C&originRegion=eu-west-1&originCreation=20211213172326

[6] (Καρσλίδης Δ., 2021)

• Αυτονομία: Χρησιμοποιώντας έξυπνα συμβόλαια, δεν υπάρχει ανάγκη για μεσάζοντα ή για δικηγόρο. Υπάρχει μόνο ένα άτομο που κάνει τη συμφωνία. Προστατεύει και διαχειρίζεται το σύστημα από κάποιον τρίτο και η εκτέλεση του κώδικα διαχειρίζεται και ελέγχεται από το δίκτυο *blockchain* παρά από ένα ή περισσότερα άτομα.

• Εξοικονόμηση: Τα έξυπνα συμβόλαια εξοικονομούν χρήματα επειδή δεν χρειάζεται η παρουσία ενδιάμεσου φορέα. Το ίδιο το άτομο είναι το μόνο που πρέπει να πληρώσει π.χ. έναν συμβολαιογράφο για να παρακολουθήσει τις συναλλαγές του.

• Ακρίβεια: Τα έξυπνα συμβόλαια δεν είναι μόνο φθηνότερα ή γρηγορότερα, αλλά και παρακάμπτουν τα λάθη που προέρχονται από τη μη αυτόματη εγγραφή των κωδικών.

• Εμπιστοσύνη: Στην τεχνολογία *blockchain*, έγγραφα ή αρχεία μοιράζονται σε μία κρυπτογραφημένη μορφή. Έτσι, δεν υπάρχει τρόπος να χαθεί ή να «χακαριστεί» ένα αρχείο.

• Δημιουργία αντιγράφων ασφαλείας: Στην τεχνολογία *blockchain*, κάθε κόμβος έχει ένα αντίγραφο δεδομένων στα δημόσια βιβλία τους. Έτσι, υπάρχει ένας αριθμός διπλότυπων αντιγράφων που υπάρχουν στο δίκτυο *blockchain* με τη μορφή αντιγράφων ασφαλείας.

1.4.2 Χρήση έξυπνων συμβολαίων

Τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν στις παρακάτω περιπτώσεις:

• Κυβέρνηση: Τα έξυπνα συμβόλαια θα παίζουν σημαντικό ρόλο στο σύστημα ψηφοφορίας παρέχοντας άπειρη ασφάλεια χρησιμοποιώντας τεχνολογία *blockchain*.

Οι ψήφοι θα πρέπει να αποκωδικοποιηθούν και να απαιτηθούν υψηλά επίπεδα υπολογιστικής ισχύος για πρόσβαση. Όμως, κανείς δεν έχει τόση ποσότητα υπολογιστικής ισχύος. Συνεπώς, δεν υπάρχει τρόπος να αλλοιωθεί το αποτέλεσμα.

Με αυτήν την τεχνολογία, οι άνθρωποι μπορούν επίσης να ψηφίσουν στο διαδίκτυο, κάτι που μειώνει το χρόνο και το κόστος υποδομής.

• Διαχείριση: Η τεχνολογία *blockchain* μπορεί να μειώσει την πιθανή σύγχυση στη ροή εργασίας και στην επικοινωνία για ακρίβεια, ασφάλεια, διαφάνεια. Διαχειρίζεται και περικόπτει όλες τις ανομοιότητες που συμβαίνουν λόγω ανεξάρτητης επεξεργασίας και μπορεί να οδηγήσει σε δαπανηρά επιχειρήματα και υψηλές καθυστερήσεις.

• Αλυσίδα εφοδιασμού: Οι αλυσίδες εφοδιασμού βρίσκουν εμπόδια σε συστήματα που βασίζονται σε χαρτί, όπου τα έγγραφα πρέπει να μεταφερθούν με κανάλια δικτύου για επιβεβαίωση που αυξάνει την απώλεια και την απάτη. Όμως, η τεχνολογία *blockchain* καταργεί όλα αυτά τα ζητήματα παρέχοντας ασφάλεια, την προσβάσιμη ψηφιακή έκδοση σε όλους τους κόμβους του δικτύου και εκτελεί αυτόματα τις εργασίες και τις πληρωμές.

• Αυτοκίνητο: Τα έξυπνα συμβόλαια παίζουν σημαντικό ρόλο στα αυτόνομα οχήματα ή οχήματα αυτόματης στάθμευσης όπου μπορούσαν να εντοπίσουν τις βλάβες σε συγκρούσεις οχημάτων.

Χρησιμοποιώντας έξυπνα συμβόλαια, μια ασφαλιστική αυτοκινητοβιομηχανία μπορεί να χρεώσει διαφορετικές τιμές με βάση το σύστημα στάθμευσης. Μπορούν επίσης να χρεώνουν σύμφωνα με τις προϋποθέσεις, υπό τις οποίες ο πελάτης μπορεί να σταθμεύσει τα οχήματά του.

• Ακίνητα: Χρησιμοποιώντας έξυπνα συμβόλαια, οι άνθρωποι μπορούν να κερδίσουν περισσότερα χρήματα. Στην τεχνολογία *blockchain*, όλες οι πληρωμές γίνονται μέσω *bitcoin* και κωδικοποιούν τη σύμβαση στα δημόσια καθολικά (*ledgers*). Έτσι, όλοι μπορούν να δουν και να ολοκληρώσουν αυτόματα του τι χρειάζεται. Ως εκ τούτου, μεσίτες, δανειστές

χρημάτων και οποιοσδήποτε σχετίζεται με τα ακίνητα μπορούν να επωφεληθούν από έξυπνα συμβόλαια.

• Υγειονομική περίθαλψη: Στο σύστημα υγειονομικής περίθαλψης, το *blockchain* παρέχει ασφάλεια και εμπιστευτικότητα στα ιατρικά αρχεία. Οι αναφορές αυτές και η παραλαβή των χειρουργικών επεμβάσεων μπορούν να κωδικοποιηθούν και να αποθηκευτούν στα δημόσια καθολικά (*ledgers*) του *blockchain* με ιδιωτικό κλειδί. Στα δημόσια αυτά καθολικά (*ledgers*) θα έχουν πρόσβαση μόνο κάποια συγκεκριμένα άτομα. Αυτά τα καθολικά μπορούν επίσης να χρησιμοποιηθούν για διαχείριση στα συστήματα υγειονομικής περίθαλψης, όπως αποτελέσματα δοκιμών, εκθέσεις χειρουργικής επέμβασης, έλεγχος κανονισμών, επίβλεψη φαρμάκων και διαχείριση ιατρικών προμηθειών.

1.4.3. ΠΛΑΤΦΟΡΜΕΣ *BLOCKCHAIN* ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝ ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ

Ακολουθούν οι πλατφόρμες *blockchain* που χρησιμοποιούνται για έξυπνα συμβόλαια.

1. *Bitcoins*: Το *Bitcoin* χρησιμοποιεί γλώσσα σεναρίου για την επεξεργασία συναλλαγών *bitcoin*. Αυτή η γλώσσα έχει περιορισμένες δυνατότητες για την επεξεργασία των εγγράφων.

2. *Ethereum*: Είναι μία από τις δημοφιλείς πλατφόρμες *blockchain* για έξυπνη γραφή

συμβολαίων. Εκτελεί τον κώδικα σε οποιαδήποτε γλώσσα προγραμματισμού και είναι προσβάσιμος από οπουδήποτε στον κόσμο.

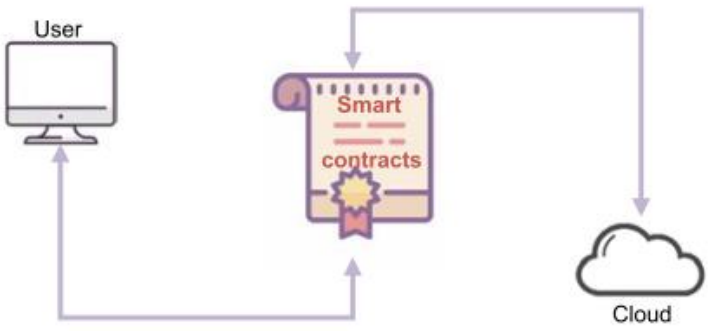
3. *Hyperledger fabric*: Η πλατφόρμα *hyperledger fabric*, χρησιμοποιείται για ιδιωτικά

blockchain όπου ο κωδικός αλυσίδας κωδικοποιείται με πρόγραμμα στο δίκτυο.

Εκτελείται και επικυρώνεται από αλυσιδωτούς επικυρωτές κατά τη διάρκεια της επεξεργασίας συναίνεσης.

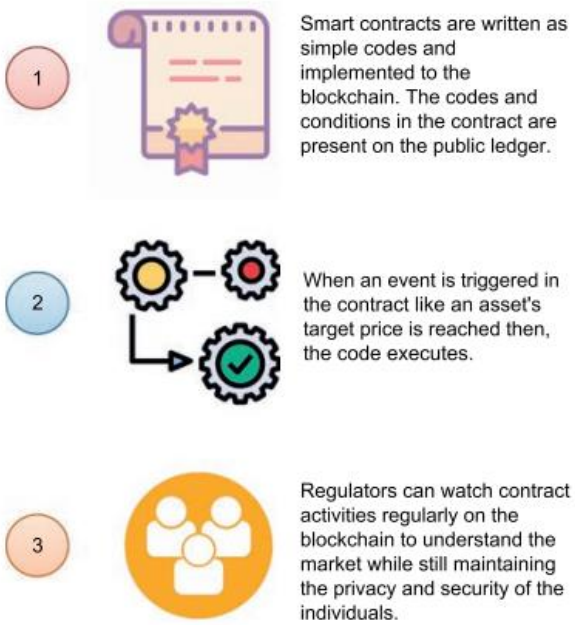
4. *NXT*: Η πλατφόρμα *NXT* που χρησιμοποιείται για δημόσιο *blockchain* και περιλαμβάνει περιορισμένο αριθμό προτύπων για τη σύνταξη των έξυπνων συμβολαίων. Χρησιμοποιείται όταν ο χρήστης δεν μπορεί να γράψει τον κώδικα μόνος του.

5. Πλευρικές αλυσίδες (*Side chains*): Αυτή η πλατφόρμα *blockchain* ενισχύει την προστασία της ιδιωτικής ζωής των έξυπνων συμβολαίων. Αυξάνει επίσης την απόδοση του *blockchain* προσθέτοντας δυνατότητες όπως ασφαλείς χειρολαβές και αρχείο πραγματικής ιδιοκτησίας.



Πηγή:
https://reader.elsevier.com/reader/sd/pii/S006524582030070X?token=D829FF236E7D0EA2CEDC8E

0F3A577F6C0AB253291B8DF5EF128497C3EDCD8EA8FA060698B705A9E170A20BD3277A4B6C&originRegion=eu-west-1&originCreation=20211213172326



Πηγή:
https://reader.elsevier.com/reader/sd/pii/S006524582030070X?token=D829FF236E7D0EA2CEDC8E0F3A577F6C0AB253291B8DF5EF128497C3EDCD8EA8FA060698B705A9E170A20BD3277A4B6C&originRegion=eu-west-1&originCreation=20211213172326

1.5 ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ *BLOCKCHAIN*

1.5.1 ΚΡΥΠΤΟΓΡΑΦΙΑ

Η κρυπτογραφία είναι το πιο σημαντικό συστατικό του *blockchain*. Αποτελεί σίγουρα ένα ερευνητικό πεδίο από μόνο του και βασίζεται σε προηγμένα μαθηματικά και τεχνικές που είναι αρκετά περίπλοκες στην κατανόηση. Γενικά έχουν αναφερθεί πολλές παραβιάσεις σε πορτοφόλια και ανταλλαγές λόγω κακών εφαρμογών κρυπτογραφίας.

Η κρυπτογραφία υπάρχει εδώ και περισσότερα από δύο χιλιάδες χρόνια. Είναι η επιστήμη της διατήρησης εμπιστευτικών πληροφοριών χρησιμοποιώντας τεχνικές κρυπτογράφησης. Ωστόσο, η εμπιστευτικότητα δεν είναι ο μόνος στόχος. Υπάρχουν διάφορες άλλες χρήσεις κρυπτογραφίας όπως αναφέρονται στην παρακάτω λίστα:

• Εμπιστευτικότητα: Το μήνυμα μπορεί να το καταλάβει μόνο ο προοριζόμενος ή εξουσιοδοτημένος παραλήπτης.

• Ακεραιότητα δεδομένων: Τα δεδομένα δεν μπορούν να πλαστογραφηθούν ή να τροποποιηθούν από κάποιον άλλο σκόπιμα ή ακούσια από τυχαία σφάλματα. Αν και η ακεραιότητα των δεδομένων δεν μπορεί να αποτρέψει τη μεταβολή των δεδομένων, μπορεί να παρέχει ένα μέσο ανίχνευσης αν τα δεδομένα έχουν τροποποιηθεί.

• Αυθεντικοποίηση: Η αυθεντικότητα του αποστολέα είναι εξασφαλισμένη και επαληθεύσιμη από τον παραλήπτη.

• Μη άρνηση: Ο αποστολέας, αφού στείλει ένα μήνυμα, δεν μπορεί να αρνηθεί αργότερα ότι το έστειλε. Αυτό σημαίνει ότι μια οντότητα (ένα άτομο ή ένα σύστημα) δεν μπορεί να αρνηθεί την κυριότητα προηγούμενης δέσμευσης ή μιας ενέργειας.

Οποιαδήποτε πληροφορία με τη μορφή μηνύματος, κειμένου, αριθμητικών δεδομένων ή πρόγραμμα υπολογιστή μπορεί να ονομαστεί σε απλό κείμενο. Η ιδέα είναι να κρυπτογραφηθεί το απλό κείμενο χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης και ένα κλειδί που παράγει το κρυπτογραφημένο κείμενο. Το κρυπτογραφημένο κείμενο μπορεί στη συνέχεια να μεταδοθεί στον προοριζόμενο παραλήπτη, ο οποίος αποκρυπτογραφεί χρησιμοποιώντας τον αλγόριθμο αποκρυπτογράφησης και το κλειδί. [7]

1.5.2 ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ - *HASH* ΣΥΝΑΡΤΗΣΕΙΣ: ΙΔΙΟΤΗΤΕΣ ΚΑΙ ΧΡΗΣΗ

Μία από τις πιο σημαντικές κατηγορίες κρυπτογραφικών αλγορίθμων σε τρέχουσα χρήση είναι η κατηγορία των κρυπτογραφικών συναρτήσεων κατακερματισμού. Οι λειτουργίες κατακερματισμού είναι πανταχού παρούσες στα σημερινά συστήματα πληροφορικής και έχουν ένα ευρύ φάσμα εφαρμογών σε πρωτόκολλα και σχήματα ασφαλείας, όπως η ακεραιότητα παροχής λογισμικού, ψηφιακές υπογραφές, έλεγχος ταυτότητας μηνυμάτων και προστασία με κωδικό πρόσβασης. Οι αλγόριθμοι κρυπτογραφικής λειτουργίας κατακερματισμού πρέπει να εμφανίζονται με μια ιδιότητα γνωστή ως αντίσταση σύγκρουσης, δηλαδή, πρέπει να είναι ανέφικτη η κατασκευή δύο ξεχωριστών εισόδων με την ίδια έξοδο κατακερματισμού.

Οι λειτουργίες κατακερματισμού (*hash*) είναι ουσιαστικά εύκολες στον υπολογισμό συναρτήσεων που παράγουν ένα ψηφιακό δακτυλικό αποτύπωμα μηνυμάτων ή δεδομένων.

Σε αντίθεση με τους περισσότερους αλγόριθμους που χρησιμοποιούνται στη συμμετρική και ασύμμετρη κρυπτογραφία, στη βασική τους μορφή οι συναρτήσεις κατακερματισμού είναι αλγόριθμοι χωρίς κλειδί, δηλαδή δεν χρησιμοποιούν μυστικό κλειδί. Αυτό σημαίνει ότι οι λειτουργίες κατακερματισμού από μόνες τους δεν μπορούν να παρέχουν εμπιστευτικότητα, έλεγχο ταυτότητας ή μη απόρριψη, αν και χρησιμοποιούνται συχνά ως στοιχεία μεγαλύτερων σχημάτων που παρέχουν αυτές τις υπηρεσίες. Μια τυπική χρήση συναρτήσεων κατακερματισμού είναι η ανίχνευση αλλαγών στα δεδομένα. Εξαιτίας αυτού, οι συναρτήσεις κατακερματισμού συχνά ονομάζονται κωδικοί ανίχνευσης τροποποιήσεων (*MDC*).

Αν και αυτά τα απλά σχήματα μπορούν συχνά να παρέχουν κάποιας μορφής προστασίας από τυχαία λάθη, η σύγχρονη κρυπτογραφία αντιμετωπίζει την ασφάλεια έναντι πολύ μεγαλύτερου συνόλου απειλών. Οι αντίπαλοι μπορεί να θέλουν να τροποποιήσουν σκόπιμα τα δεδομένα, ή συμπεραίνουν πληροφορίες που βασίζονται αποκλειστικά στις τιμές κατακερματισμού. Οι λειτουργίες κατακερματισμού χρησιμοποιούνται επίσης σε διάφορες κατασκευές στη σύγχρονη κρυπτογραφία, όπως πρωτόκολλα αυθεντικοποίησης μηνύματος και οντότητας και ψηφιακές υπογραφές. Επομένως οι συναρτήσεις *hash* απαιτούν περαιτέρω ιδιότητες.

[7] (Γιαννακού, 2019)

Ιδιότητα 1 - αντίσταση προεικόνισης. Μια συνάρτηση κατακερματισμού h λέγεται ότι είναι ανθεκτική στην προεικόνιση αν, δεδομένης μιας έγκυρης εξόδου κατακερματισμού y, είναι αδύνατο να βρεθεί οποιοδήποτε προεικόνιση x τέτοια ώστε h (x) =y. Αυτό σημαίνει ότι οι αντιστάσεις που είναι ανθεκτικές στην απεικόνιση είναι δύσκολο να αναστραφούν.

Ιδιότητα 2 - δεύτερη αντίσταση προεικόνισης. Μια συνάρτηση κατακερματισμού h λέγεται ότι είναι δεύτερη ανθεκτική στην προεικόνιση αν, εάν σε ένα ζευγάρι (x, y) με h (x) = y, είναι αδύνατο να βρεθεί άλλη είσοδος x' τέτοια όπου h (x) = y. Καθώς οι συναρτήσεις hash είναι πολλές προς μία συναρτήσεις, γνωρίζουμε ότι γενικά πρέπει να υπάρχουν περισσότερες από μία τιμές

x με h (x) = y. Ωστόσο, για τις δεύτερες ανθεκτικές στην προεικόνιση συναρτήσεις hash, ακόμη και όταν δίνεται μία προεικόνιση x, είναι δύσκολο να βρεθεί άλλες είσοδοι x' με την ίδια τιμή κατακερματισμού.

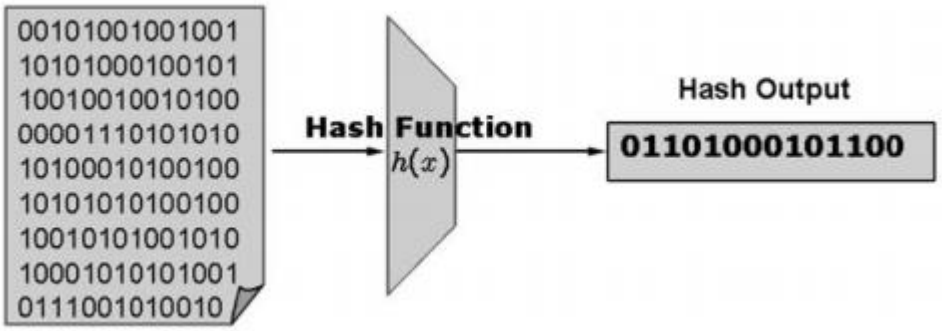
Hash συναρτήσεις που ικανοποιούν τις ιδιότητες της προεικόνισης και της δεύτερης αντίστασης στην προεικόνιση είναι γνωστές ως λειτουργίες μονόδρομου κατακερματισμού (*OWHF*). Οι ακόλουθες εφαρμογές είναι χαρακτηριστικές χρήσεις μονόδρομων συναρτήσεων κατακερματισμού.

Προστασία με κωδικό πρόσβασης: Οι συναρτήσεις *Hash* χρησιμοποιούνται συχνά για προστασία των κωδικών πρόσβασης στα συστήματα υπολογιστών. Για λόγους ασφάλειας, τα περισσότερα συστήματα αποθηκεύουν κωδικούς πρόσβασης κατακερματισμού (αντί για κωδικούς πρόσβασης απλού κειμένου) στον πίνακα κωδικών πρόσβασής τους. Κατά τη διάρκεια της σύνδεσης, το *hash* του κωδικού πρόσβασης που παρέχεται από τον χρήστη υπολογίζεται χρησιμοποιώντας τον ίδιο αλγόριθμο και συγκρίνεται με το αποθηκευμένο *hash* για εξουσιοδότηση ή άρνηση πρόσβασης χρήστη. Ο αλγόριθμος συνάρτησης κατακερματισμού πρέπει να είναι ανθεκτικός στην προεικόνιση για να χρησιμοποιηθεί για προστασία κωδικού πρόσβασης. Αυτό είναι απαραίτητο για να διασφαλιστεί ότι κάποιος με πρόσβαση στον πίνακα κωδικών πρόσβασης δεν μπορεί εύκολα να ανακτήσει τον πραγματικό κωδικό πρόσβασης αντιστρέφοντας τη λειτουργία κατακερματισμού.

Έλεγχος ταυτότητας πληροφοριών: Μια άλλη κοινή εφαρμογή των μονόδρομων λειτουργιών κατακερματισμού είναι η πιστοποίηση της γνησιότητας των δεδομένων.

Συστήματα ανίχνευσης εισβολής με βάση τον κεντρικό υπολογιστή, όπως το *Tripwire* το πραγματοποιούν αυτό υπολογίζοντας τιμές κατακερματισμού πολλών σημαντικών αρχείων συστήματος και αποθηκεύοντας αυτές τις τιμές σε ασφαλείς και αξιόπιστες συσκευές. Αυτά τα ψηφιακά δακτυλικά αποτυπώματα συγκρίνονται συχνά για την επαλήθευση της ακεραιότητας των προστατευμένων αρχείων. Ένας αντίπαλος ή κακόβουλο λογισμικό που επιθυμεί να αντικαταστήσει ένα τέτοιο αρχείο θα χρειαστεί να δημιουργήσει ένα άλλο αρχείο με την ίδια τιμή κατακερματισμού. Συνεπώς, απαιτείται η δεύτερη αντίσταση στην προεικόνιση για αντιμετώπιση αυτών των απειλών.

Δεδομένου ότι οι λειτουργίες *hash* έχουν πολλές εφαρμογές στο σύγχρονο κρυπτογραφία, ο μονόδρομος συχνά δεν είναι επαρκής για ασφαλή χρήση. Μία από τις πιο ενδιαφέρουσες χρήσεις συναρτήσεων κατακερματισμού είναι σε ψηφιακές υπογραφές.

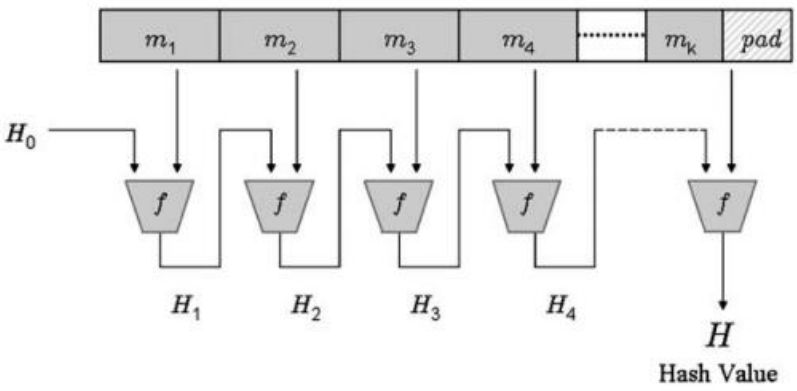


Πηγή: https://www.sciencedirect.com/science/article/pii/S1363412706000203

Δομή συνάρτησης *Hash*

Αν και οι κρυπτογραφικές συναρτήσεις κατακερματισμού μπορούν επίσης να κατασκευαστούν με βάση κρυπτογράφηση μπλοκ ή άλλες αλγεβρικές δομές, οι πιο συχνά χρησιμοποιούμενοι αλγόριθμοι είναι προσαρμοσμένες σχεδιασμένες επαναληπτικές συναρτήσεις. Οι επαναληπτικές συναρτήσεις *hash* βασίζονται σε πολύ αποτελεσματικές συναρτήσεις συμπίεσης, οι οποίες λαμβάνουν ως συμβολοσειρές εισόδου το *n* και *m bits*, και εξάγουν μια συμβολοσειρά *n bits*. Οι συναρτήσεις συμπίεσης εφαρμόζονται συνήθως ως ένα μικρό σύνολο σύνθετων λειτουργιών που επαναλαμβάνονται για ένα αριθμό γύρων. Για να υπολογιστεί το *hash* της τιμή συνάρτησης, τα μηνύματα γεμίζονται και χωρίζονται σε μπλοκ *m bits* (τυπικά *m* ¼ 512 *bits*). Η λειτουργία συμπίεσης λαμβάνει ως είσοδο ένα μπλοκ μηνυμάτων και μια συμβολοσειρά *n-bit* γνωστή ως μεταβλητή αλυσίδας. Η αρχική μεταβλητή αλυσίδας είναι σταθερή και κάθε μπλοκ μηνυμάτων υποβάλλεται σε επεξεργασία κάθε φορά. Η έξοδος της επανάληψης *i* της συνάρτησης συμπίεσης χρησιμεύει ως μεταβλητή αλυσίδας για την επανάληψη *i* + 1. Η τελευταία έξοδος της συμπίεσης η λειτουργία αντιστοιχεί στην έξοδο κατακερματισμού.

Αυτός ο τύπος κατασκευής είναι γνωστός ως *Merkle – Damga˚rd* κατασκευή. Μπορεί να αποδειχθεί ότι με την κατάλληλη επένδυση και αρχική σταθερή αλυσίδα μεταβλητή τιμή, εφόσον η συνάρτηση συμπίεσης f ικανοποιεί ορισμένες ιδιότητες, η προκύπτουσα λειτουργία κατακερματισμού θα είναι ασφαλής.



Πηγή: https://www.sciencedirect.com/science/article/pii/S1363412706000203

1.5.3 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

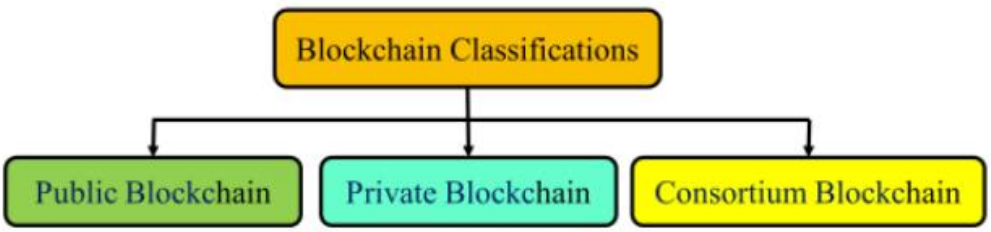
Οι ψηφιακές υπογραφές είναι από τις πιο ενδιαφέρουσες και πρωτότυπες εφαρμογές της σύγχρονης κρυπτογραφίας. Οι ψηφιακές υπογραφές προσπαθούν να μιμηθούν τις συνηθισμένες χειρόγραφες υπογραφές στον ψηφιακό κόσμο. Οι ψηφιακές υπογραφές χρησιμοποιούν κρυπτογραφικούς αλγόριθμους που απαιτούν ως πληροφορίες εισόδου που είναι γνωστές μόνο από τον υπογράφων, ενώ οι δημόσιες πληροφορίες μπορούν να χρησιμοποιηθούν για επαλήθευση υπογραφών. Εάν χρησιμοποιούνται ισχυροί αλγόριθμοι, μια έγκυρη υπογραφή θα πρέπει θεωρητικά να παρέχει έλεγχο ταυτότητας και μη απόρριψη μηνύματος, δηλαδή να διασφαλίζει ότι το μήνυμα είναι αυθεντικό και δεν έχει παραβιαστεί και το άτομο που έχει υπογράψει ψηφιακά το μήνυμα, δεν θα πρέπει να είναι σε θέση να αρνηθεί τις δεσμεύσεις που έχουν συμφωνηθεί από το υπογεγραμμένο μήνυμα.

Οι ψηφιακές υπογραφές βασίζονται σε κρυπτογραφία δημόσιου κλειδιού. Ο υπογράφων έχει ένα ιδιωτικό κλειδί γνωστό μόνο στον εαυτό του, δηλαδή χρησιμοποιείται για την υπογραφή δεδομένων. Το δημόσιο κλειδί του είναι δημόσια διαθέσιμο και μπορεί να χρησιμοποιηθεί για την επαλήθευση της εγκυρότητας των υπογραφών. Στην πράξη, οι αλγόριθμοι δημόσιου κλειδιού δεν είναι ιδιαίτερα αποτελεσματικοί. Οι περισσότεροι αλγόριθμοι βασίζονται σε πολλά θεωρητικά προβλήματα, και συχνά απαιτούν ένα μεγάλο αριθμό εντατικών λειτουργιών υπολογιστή. Κατά την ανάλυση πρέπει να διασφαλιστεί η ασφάλεια των συστημάτων ψηφιακής υπογραφής και να ληφθούν υπόψη οι ιδιότητες τόσο του αλγορίθμου δημόσιου κλειδιού όσο και η συνάρτηση κατακερματισμού που χρησιμοποιείται.

Ο κύριος στόχος ενός επιτιθέμενου σε μια ψηφιακή υπογραφή είναι η παραγωγή πλαστών υπογραφών, δηλαδή ενός ζεύγους που αποτελείται από ένα μήνυμα και μια αντίστοιχη έγκυρη υπογραφή. Η πιο φιλόδοξη μορφή επίθεσης θα ήταν η ανάκτηση του ιδιωτικού κλειδιού, επιτρέποντας επομένως την κατασκευή πολλών τέτοιων ζευγαριών. Ένας πιθανός στόχος για τον επιτιθέμενο μπορεί επομένως να είναι ο αλγόριθμος συνάρτησης κατακερματισμού, ο οποίος χρησιμοποιείται. [8]

1.6 ΤΥΠΟΙ *BLOCKCHAIN*

Τα δίκτυα *Blockchain* μπορούν να ταξινομηθούν σε δημόσια, αδειοδοτημένα (ιδιωτικά) και κοινοπραξίες *blockchain* σύμφωνα με τα χαρακτηριστικά και τις πολιτικές τους.



Πηγή: https://www.researchgate.net/publication/326102908_Everything_You_Wanted_to_Know_About_the_Blockchain_Its_Promise_Components_Processes_and_Problems

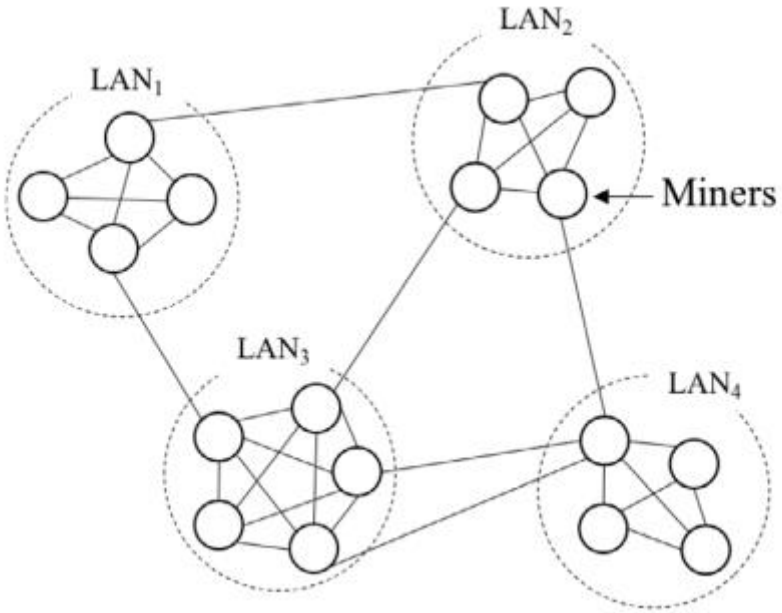
[8] (Cid, 2006)

1.6.1 ΔΗΜΟΣΙΟ *BLOCKCHAIN*

Ένα δημόσιο *blockchain* (*open blockchain*) είναι μια ανοιχτή πλατφόρμα για όλους. Δεν υπάρχουν περιορισμοί και ο καθένας μπορεί να πάρει μέρος. Επομένως, αυτά ονομάζονται επίσης *blockchain* χωρίς άδεια (*permissionless*). Ο κάθε συμμετέχοντας έχει πλήρη εξουσιοδότηση να διαβάζει / γράφει συναλλαγές, να διεξάγει έλεγχο στο *blockchain* ή να ελέγχει οποιοδήποτε μέρος του *blockchain*, ανά πάσα στιγμή. Το *blockchain* είναι ανοιχτό και διαφανές και δεν υπάρχουν συγκεκριμένοι «κόμβοι επικύρωσης». Όλοι οι χρήστες μπορούν να συλλέγουν συναλλαγές και να αρχίζουν με την εξόρυξη (*mining*) ούτως ώστε να κερδίσουν ανταμοιβές εξόρυξης.

Φυσικά, η δημόσια διαθεσιμότητα του καθολικού σε ένα ιδιωτικό σύστημα *blockchain* το εκθέτει σε επιθέσεις. Δεδομένου ότι ο καθένας έχει το δικαίωμα να συμμετέχει, κάποιοι κακόβουλοι χρήστες ενδέχεται να επιχειρήσουν να δημοσιεύσουν *block* με τέτοιο τρόπο ώστε να ανατραπεί το σύστημα. Για να αποφευχθεί αυτό, υπάρχει μηχανισμός της απόδειξης εργασίας (*proof of work*) συνδυασμένος με κρυπτογραφική επικύρωση ολόκληρου του *blockchain* κάθε φορά που προστίθεται ένα νέο *block* αντισταθμίζοντας αυτό το μειονέκτημα. Παραδείγματα αυτού του τύπου είναι τα κρυπτονομίσματα *Bitcoin & Ethereum*.

Θεωρούμε τα δημόσια *blockchain* όταν τα μπλοκ εξορύσσονται παράλληλα και βασίζονται σε προβλήματα συναίνεσης σε διαφορετικούς ανθρακωρύχους. Αυτά τα μπλοκ έρχονται σε σύγκρουση μεταξύ τους, αν και μπορεί να περιέχουν το ίδιο σύνολο συναλλαγών. Μόνο ένα από τα αντικρουόμενα μπλοκ μπορεί να γίνει αποδεκτό σε ένα *blockchain*. Τα άλλα μπλοκ απορρίπτονται.[9] [10] [11]



Πηγή: https://www.sciencedirect.com/science/article/pii/S0140366421002437

[9] (Τσάφου Αποστολοπούλου, 2020)
[10] (Wang, Ni, Zha, κ.α. 2021)
[11] (Mohanty, 2018)

1.6.2 ΙΔΙΩΤΙΚΟ *BLOCKCHAIN*

Το ιδιωτικό *blockchain* (*private blockchain*) είναι ένας τύπος συστήματος *blockchain* που έχει ρυθμιστεί για να διευκολύνει την ιδιωτική κοινή χρήση και ανταλλαγή δεδομένων μεταξύ μιας ομάδας ατόμων (σε έναν οργανισμό) ή μεταξύ πολλών οργανισμών με εξόρυξη που ελέγχεται από έναν οργανισμό ή επιλεκτικά από άτομα.

Τα ιδιωτικά *blockchains* είναι δίκτυα *blockchain* που δημιουργήθηκαν μεταξύ κόμβων που λειτουργούν από επιχειρήσεις. Μόνο οι επιτρεπόμενοι κόμβοι που ανήκουν σε συμμετέχουσες επιχειρήσεις επιτρέπεται να συμμετάσχουν στο δίκτυο *peer-to-peer* του ιδιωτικού *blockchain* και μόνο εγκεκριμένοι λογαριασμοί που ανήκουν στη συμμετοχή επιτρέπεται στις επιχειρήσεις να υποβάλλουν συναλλαγές στους κόμβους.

Ονομάζεται επίσης *blockchain* με άδεια (*permissioned*), καθώς άγνωστοι χρήστες δεν μπορούν να έχουν πρόσβαση σε αυτό, εκτός εάν λάβουν μια ειδική πρόσκληση. Η συμμετοχή των κόμβων αποφασίζεται είτε από ένα σύνολο κανόνων είτε από τον υπεύθυνο του δικτύου, για έλεγχο της πρόσβασης.

Σε ένα ιδιωτικό σύστημα *blockchain*, ένας κόμβος γίνεται μέρος του δικτύου, συμβάλλοντας στη λειτουργία ενός αποκεντρωμένου δικτύου, με κάθε κόμβο να διατηρεί ένα αντίγραφο του καθολικού, και συνεργασία για την επίτευξη συναίνεσης για ενημέρωση, αλλά σε αντίθεση με το δημόσιο *blockchain*, οι εγγραφές είναι περιορισμένες.[12] [13] [14]

1.6.3 ΚΟΙΝΟΠΡΑΚΤΙΚΟ *BLOCKCHAIN*

Μια κοινοπραξία *blockchain* (*consortium blockchain*) μπορεί να θεωρηθεί ως εν μέρει ιδιωτικό και με άδεια *blockchain*, όπου υπεύθυνα είναι ένα σύνολο προκαθορισμένων κόμβων για τη συναίνεση και την επικύρωση του μπλοκ. Αυτοί οι κόμβοι αποφασίζουν ποιος μπορεί να είναι μέρος του δικτύου και ποιος μπορεί να κάνει εξόρυξη. Για επικύρωση μπλοκ, χρησιμοποιείται ένα σχήμα πολλαπλών υπογραφών, όπου το μπλοκ θεωρείται έγκυρο, μόνο αν υπογράφεται από αυτούς τους κόμβους. Έτσι, είναι ένα μερικώς συγκεντρωτικό σύστημα, λόγω του ότι ο έλεγχος γίνεται από ορισμένους επιλεγμένους κόμβους επικύρωσης, σε αντίθεση με το ιδιωτικό *blockchain* που είναι εντελώς κεντρικό και το δημόσιο *blockchain* που είναι εντελώς αποκεντρωμένο. [15] [16]

1.7 ΑΛΓΟΡΙΘΜΟΙ ΣΥΝΑΙΝΕΣΗΣ ΓΙΑ ΤΟ *BLOCKCHAIN*

Ο τρόπος επίτευξης συμφωνίας σε ένα δίκτυο *blockchain* είναι ένα πολύπλοκο και σημαντικό έργο. Θα προστεθούν νέα αρχεία συναλλαγών στο *blockchain* αφού το νέο μπλοκ επαληθεύεται από όλους τους κόμβους στο δίκτυο. Πρέπει να σημειωθεί ότι μόλις επαληθευτούν τα μπλοκ, είναι δεν είναι εφικτή η τροποποίηση ή η διαγραφή τους. Η δομή των *blockchains* έχει σχεδιαστεί για να είναι έγκυρη σε ένα αξιόπιστο και αναξιόπιστο δίκτυο με εχθρικούς χρήστες. Διάφορες μέθοδοι σχεδιάζονται και αναπτύσσονται ως αλγόριθμοι συναίνεσης. Ο αριθμός αυτών των αλγορίθμων αυξάνεται καθημερινά ανάλογα με την ανάπτυξη του *blockchain*. Παρακάτω παρατίθενται οι πιο σημαντικοί αλγόριθμοι συναίνεσης που χρησιμοποιούνται ευρέως στα δίκτυα *blockchain*.

---

[12] (Τσάφου Αποστολοπούλου, 2020)
[13] (Mohanty, 2018)
[14] (Robinson, Hyland-Wood, Saltini, κ.α. 2019)
[15] (Τσάφου Αποστολοπούλου, 2020)
[16] (Mohanty, 2018)

1.7.1 ΑΠΟΔΕΙΞΗ ΕΡΓΑΣΙΑΣ (*POW – PROOF OF WORK*)

Η πιο γνωστή μέθοδος συναίνεσης είναι η απόδειξη της εργασίας (*PoW*) που την εισήγαγε ο *Nakomoto* και χρησιμοποιείται στο *Bitcoin*. Η Απόδειξη της Εργασίας υπήρχε για πολλά χρόνια ως κατάλληλη μέθοδος για την κρυπτογραφία νομίσματος. Σε αυτή την μέθοδο, ο υπολογιστής κάνει πολλούς υπολογισμούς για να λύσει ένα μαθηματικό παζλ. Αυτή η επίλυση παζλ γίνεται μέσω της συνάρτησης κατακερματισμού (*Hash*). Η συνάρτηση κατακερματισμού (*Hash*) είναι ένας τυχαίος και πολύπλοκος μαθηματικός τύπος που χρησιμοποιείται για την επιβεβαίωση των συναλλαγών που είναι αποθηκευμένες σε μπλοκ. Εν συντομία, κάθε μπλοκ αποτελείται από την αξία κατακερματισμού προηγούμενου μπλοκ, ιστορικό συναλλαγών και τρέχον μπλοκ κατακερματισμού. Ένας ανθρακωρύχος, αυτός είναι ο υπολογιστής που προσπαθεί να λύσει τη συνάρτηση κατακερματισμού (*hash*), θα προσπαθήσει να βρει μια συγκεκριμένη τιμή με τέτοιο τρόπο ώστε η τιμή κατακερματισμού να πληροί μια προκαθορισμένη συνθήκη.

1.7.2. ΑΠΟΔΕΙΞΗ ΣΥΜΜΕΤΟΧΗΣ (*POS – PROOF OF STAKE*)

Μετά την απόδειξη της εργασίας, ο επόμενος κοινός αλγόριθμος συναίνεσης στην τεχνολογία *blockchain* είναι η απόδειξη συμμετοχής (*Proof of Stake*). Σημαντικά προβλήματα στην απόδειξη των συστημάτων εργασίας (*PoW*), όπως η ενεργειακή ανεπάρκεια ήταν ο λόγος για τη δημιουργία των αποδείξεων συμμετοχής. Ο αλγόριθμος *PoS* βασίζεται στην ιδέα ότι ο δημιουργός του επόμενου μπλοκ θα πρέπει να επιλέγεται μέσω διαφόρων συνδυασμών τυχαίας επιλογής και ηλικίας που μπορεί να παρέχει καλή επεκτασιμότητα. Αυτή η ιδέα εισήχθη το 2011 για το κρυπτονόμισμα *Peercoin* και μετά χρησιμοποιήθηκε σε άλλα όπως το *Nxt* και το *Blackcoin*. Ο επιλεγμένος κόμβος για την δημιουργία του επόμενου μπλοκ, θα επιλεγεί μέσω μιας οιονεί τυχαίας διαδικασίας στην οποία η επιλογή εξαρτάται από τα περιουσιακά στοιχεία που είναι αποθηκευμένα στο πορτοφόλι (ή το σύνολο των μετοχών) που σχετίζονται με αυτόν τον κόμβο. Αυτή η μέθοδος δεν χρειάζεται υψηλή υπολογιστική ισχύ για την επικύρωση οποιασδήποτε απόδειξης και ως εκ τούτου, οι ανθρακωρύχοι (*miners*) δεν θα λάβουν ανταμοιβή εκτός από τις αμοιβές συναλλαγής. Αν και αυτή η μέθοδος δεν χρειάζεται απόδειξη της υπολογιστικής ισχύος της εργασίας, εξαρτάται σε μεγάλο βαθμό από τους κόμβους που έχουν το μεγαλύτερο μερίδιο και το *blockchain* θα γίνει κάπως συγκεντρωτικό. Εξάλλου, υπάρχει ένα άλλο κοινό πρόβλημα για το σύστημα *Proof-of-Stake* ονομάζεται "τίποτα δεν διακυβεύεται", που σημαίνει ότι εάν ένας κόμβος δεν έχει τίποτα μέσα, δεν φοβάται να χάσει κάτι. Επομένως, δεν θα υπάρχουν εμπόδια για τον κόμβο που θα τον αποτρέψει από την κακή συμπεριφορά. Συμπερασματικά, υπάρχουν ορισμένα πλεονεκτήματα στους αλγόριθμους συναίνεσης που βασίζονται σε *PoS*, όπως ο γρήγορος χρόνος δημιουργίας μπλοκ, η υψηλή απόδοση *t*, η ενεργειακή απόδοση, η επεκτασιμότητα (αλλά μικρότερη από *PoW*) και ανεξαρτησία στο ειδικό υλικό. Ωστόσο, αυτή η ομάδα αλγορίθμων πάσχει από κάποιο είδος συγκεντρωτισμού και χαμηλότερο κόστος κακής συμπεριφοράς σε δίκτυα *blockchain*.

1.7.3 ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΗ ΑΠΟΔΕΙΞΗ ΣΥΜΜΕΤΟΧΗΣ

Αυτή η μέθοδος είναι μια βελτιωμένη εκδοχή της μεθόδου *Proof of Stake* έτσι ώστε οι κόμβοι να επιλέγουν εκπροσώπους μέσω ψηφοφορίας με εντολή επικύρωσης μπλοκ. Ο αριθμός των εκπροσώπων είναι περιορισμένος και αυτό θα καταστήσει δυνατή την αποτελεσματικότερη οργάνωση του δικτύου και κάθε εκπρόσωπος θα μπορεί να καθορίσει τον επαρκή χρόνο για τη δημοσίευση κάθε μπλοκ. Ωστόσο, αυτός ο περιορισμός στον αριθμό των αντιπροσώπων

θα κάνει το δίκτυο πιο συγκεντρωτικό. Τα σημαντικότερα χαρακτηριστικά αυτού του μηχανισμού μπορεί να αναφερθεί ως επεκτασιμότητα, ενεργειακή απόδοση και χαμηλό κόστος συναλλαγών. Παρά όλα αυτά τα οφέλη, είναι ημι-συγκεντρωτικός μηχανισμός και είναι καλύτερα να χρησιμοποιείται σε ιδιωτικά *blockchains*. Ωστόσο, εάν ένας επιλεγμένος αντιπρόσωπος καθυστερήσει ή κάνει λάθος στην παρουσίαση των απαιτούμενων αναφορών, οι κόμβοι του δικτύου μπορεί να ψηφίσουν για τον προσδιορισμό της αντικατάστασής του.

1.7.4. ΑΠΟΔΕΙΞΗ ΤΟΥ ΠΑΡΕΛΘΟΝΤΟΣ ΧΡΟΝΟΥ

Η απόδειξη του παρελθόντος χρόνου εισάγεται ως μία από τις συναινετικές μεθόδους των *blockchains*, παρόμοια με το *PoW*, και ο κάθε ανθρακωρύχος απαιτείται να λύσει ένα πρόβλημα κατακερματισμού. Κάθε εγκριτής μπλοκ επιλέγεται στον συντομότερο αναμενόμενο χρόνο και με σεβασμό σε αξιόπιστη λειτουργία λόγω παραγωγής μπλοκ. Ο ανθρακωρύχος επιλέγεται τυχαία από όλο το δίκτυο και χρησιμοποιούν το Αξιόπιστο Περιβάλλον Εκτέλεσης (TEE) για τη διασφάλιση της ασφάλειας της διαδικασίας εκλογής.

1.7.5 ΠΡΑΚΤΙΚΗ ΑΝΟΧΗ ΒΥΖΑΝΤΙΝΟΥ ΣΦΑΛΜΑΤΟΣ

Αυτή η συναινετική μέθοδος χρησιμοποιείται για την επίλυση του Βυζαντινού προβλήματος. Σήμερα, οι κακόβουλες επιθέσεις στο λογισμικό είναι όλο και πιο συχνές. Η αυξανόμενη εξάρτηση της βιομηχανίας και οι κυβερνήσεις στις διαδικτυακές υπηρεσίες πληροφόρησης θα κάνουν τις κακόβουλες επιθέσεις πιο ελκυστικές και τις συνέπειες πιο σοβαρές.

Αυτός ο αλγόριθμος είναι μια μορφή ανταπόκρισης λειτουργίας μηχανής. Αυτή η υπηρεσία θα διαμορφωθεί ως μηχανή λειτουργίας, που είναι υπεύθυνη για τους κόμβους σε ένα αποκεντρωμένο σύστημα. Σε αυτή τη μέθοδο, όλοι οι κόμβοι πρέπει να συμμετέχουν στη διαδικασία ψηφοφορίας για να προσθέσουν το επόμενο μπλοκ και επιτυγχάνεται η συναίνεση όταν περισσότερα από τα δύο τρίτα των κόμβων έχουν ευνοϊκή γνώμη του μπλοκ. Η πρακτική ανοχή βυζαντινού σφάλματος μπορεί να αντέξει τη συμπεριφορά του ενός τρίτου φυσιολογικά από τις πλατφόρμες. Για παράδειγμα, σε ένα σύστημα με κακόβουλο λογισμικό κόμβου, τουλάχιστον τέσσερις κόμβοι πρέπει να έχουν συμφωνία για να φτάσουν στο σωστό τέλος. Διαφορετικά, δεν θα επιτευχθεί συμφωνία και συναίνεση.

Με αυτόν τον τρόπο, η συναίνεση επιτυγχάνεται ταχύτερα και είναι πιο οικονομική σε σύγκριση με την Απόδειξη Εργασίας.

Συμπερασματικά, η ενεργειακή απόδοση και η υψηλή απόδοση θεωρούνται τα πλεονεκτήματά της και ορισμένα σημεία, όπως λίγες ή καθόλου διαθέσιμες παράμετροι για κλιμάκωση και πιθανές καθυστερήσεις όπως το δίκτυο θα πρέπει να περιμένουν έως ότου οι ψήφοι όλων των κόμβων σημειωθούν ως μειονεκτήματά του

1.7.6. ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΗ ΑΝΟΧΗ ΒΥΖΑΝΤΙΝΟΥ ΣΦΑΛΜΑΤΟΣ

Αυτή η μέθοδος ακολουθεί τους κανόνες της Πρακτικής ανοχής βυζαντινού σφάλματος, αλλά δεν απαιτεί τη συμμετοχή όλων των κόμβων στη διαδικασία ψηφοφορίας για προσθήκη ενός νέου μπλοκ. Ένας αριθμός κόμβων επιλέγονται ως εκπρόσωποι άλλων κόμβων και, με βάση

μια σειρά κανόνων, ακολουθούν μια διαδικασία συναίνεσης όπως η μέθοδος Πρακτικής ανοχή βυζαντινού σφάλματος.

Σε αυτήν τη μέθοδο, ορισμένοι επαγγελματικοί κόμβοι ψηφίζονται για την καταγραφή συναλλαγών για όλους τους κόμβους. Αυτή η μέθοδος χρησιμοποιείται στον αλγόριθμο NEO. Αξίζει να αναφερθεί ότι η εξουσιοδοτημένη βυζαντινή ανοχή σε σφάλματα είναι λιγότερο πιθανό να αντιμετωπίσει καθυστερήσεις από την Πρακτική ανοχή βυζαντινού σφάλματος αλλά ο περιορισμός του αριθμού των ψηφοφόρων μπορεί να απειλήσει την αποκέντρωση του δικτύου.

1.7.8 ΑΠΟΔΕΙΞΗ ΒΑΡΟΥΣ (*POWEIGHT*)

Το *Proof of Weight* συνδυάζει ένα ευρύ φάσμα ελαφρώς διαφορετικών αλγορίθμων συναίνεσης που βασίζονται στο μοντέλο συναίνεσης *Algorand.*

Ο *Algorand* επιτυγχάνει συμφωνία μέσω ενός Βυζαντινού πρωτοκόλλου συμφωνίας που μπορεί να κατηγοριοποιήσει τους χρήστες σύμφωνα με διαφορετικές παραμέτρους που ονομάζονται βάρη. Σε *blockchain* βασισμένο στο *Proof of Weight*, ένα βάρος επισυνάπτεται σε κάθε χρήστη. Το βάρος υπολογίζεται από διαφορετικούς παράγοντες που θα οδηγούσαν σε διαφορετικούς αλγόριθμους συναίνεσης απόδειξης βάρους. Αυτοί οι παράγοντες βασίζονται συνήθως στο πόσα χρήματα έχει ένας χρήστης στο λογαριασμό του. Το δίκτυο θα παραμείνει ασφαλές εφόσον τα δύο τρίτα ή μεγαλύτερα τμήματα χρηστών είναι ειλικρινείς.

Οι επιθέσεις διπλής δαπάνης δεν μπορούν επίσης να απειλήσουν την ασφάλεια μιας απόδειξης δικτύου με βάση το βάρος.

Το *Algorand* έχει ομοιότητες με τον αλγόριθμο *Proof of Stake*. Στον αλγόριθμο του *Proof of Stake*, το ποσοστό των κερμάτων που διαθέτει ένας χρήστης στο δίκτυο καθορίζει το ποσό της ανταμοιβής που θα αυξήσει την κερδοφορία της ανακάλυψης του επόμενου μπλοκ. Στο *PoWeight*, μία διαφορετική σταθμισμένη αξία θα χρησιμοποιηθεί. Το *Filecoin* και το *Chia* είναι παραδείγματα κρυπτονομισμάτων που χρησιμοποιούν επί του παρόντος το *PoWeight*.

Συνοψίζοντας, ο αλγόριθμος *PoWeight* φέρνει σημαντικά μεγάλη προσαρμογή και επεκτασιμότητα, επιβεβαιώνει πολύ γρήγορα & αποτελεσματικά τις συναλλαγές με τη χρήση τροφοδοτικού. Αφ 'ετέρου, καθώς οι συμμετέχοντες δεν λαμβάνουν ανταμοιβές σε αυτό το δίκτυο, είναι δύσκολο να διατηρήσουν τα κίνητρα τους για συμμετοχή. Αν και η δημιουργία παθητικών ροών εσόδων δεν έχει σχεδιαστεί στον πυρήνα *PoWeight*, αυτό το ζήτημα μπορεί να αντιμετωπιστεί με την ανάπτυξη δημιουργικών λύσεων.

1.7.9 *PROOF OF BURN (POB)*

Η απόδειξη της καύσης είναι μια εναλλακτική μέθοδος για την επίτευξη συμφωνίας σε δίκτυο *blockchain*. Η ιδέα πίσω από αυτό είναι ότι οι ανθρακωρύχοι δεν πρέπει να σπαταλούν ενέργεια ή χρόνο για να αποδείξουν ότι έχουν κάνει κάτι δύσκολο. Σε αυτόν τον αλγόριθμο, οι ανθρακωρύχοι πρέπει να «κάψουν» μερικά από τα κρυπτονομίσματα που ήδη τους ανήκουν για να λάβουν ανταμοιβές.

Το “κάψιμο” εδώ σημαίνει ότι ένας χρήστης καλείται να στείλει κάποιο κρυπτονόμισμα σε "διεύθυνση *eater*" για να λάβει νομίσματα, μάρκες ή προνόμια εξόρυξης στο δίκτυο. Τα χρήματα που στάλθηκαν στη "διεύθυνση *eater*" είναι μη ανακτήσιμα και κανείς δεν μπορεί

να τα ξοδέψει ξανά, και έτσι αποκαλούνται «καμμένα» και είναι εκτός κυκλοφορίας. Όπως ακριβώς και οι διαδικασίες που γίνονται στο *PoW*, η καύση νομισμάτων είναι μια δαπανηρή δραστηριότητα για τον χρήστη, αλλά δεν καταναλώνει πόρους και ενέργεια. Ο μόνος πόρος που χρησιμοποιείται στο *Proof of Burn (PoB)* είναι η προθυμία του χρήστη να υποστεί μια βραχυπρόθεσμη απώλεια για να λάβει μία μακροπρόθεσμη ανταμοιβή.

Όπως αναφέρθηκε, στην περίπτωση της "διεύθυνσης *eater*", η διεύθυνση δημιουργείται τυχαία και δεν σχετίζεται με κανένα ιδιωτικό κλειδί. Η σχέση με οποιοδήποτε ιδιωτικό κλειδί σημαίνει ότι τα χρήματα είναι κατά βάση απρόσιτα και κανείς δεν μπορεί να τα ξοδέψει. Θα πρέπει να σημειωθεί ότι όλα τα κρυπτονομίσματα *PoB* απαιτούν απόδειξη της απόδοσης κρυπτονομισμάτων εργασίας όπως το *bitcoin*.

Το *Slimcoin* (*SLM*) είναι ένα κρυπτονόμισμα που καίει το *bitcoin* ως μέθοδος εξόρυξης και ως αλγόριθμος συναίνεσης. Όσο περισσότερα νομίσματα καίει ο χρήστης, τόσο περισσότερες πιθανότητες έχει να βρει το επόμενο μπλοκ. Αυτό είναι επίσης παρόμοιο με το *Proof of Stake* (*PoS*) στο οποίο οι πλούσιοι πιθανότατα γίνονταν πλουσιότεροι. Συνοψίζοντας τα χαρακτηριστικά του, δημιουργεί περισσότερη σταθερότητα αφού διακινδυνεύει μια βραχυπρόθεσμη απώλεια και ξοδεύει τα χρήματά του με αυτόν τον τρόπο, και θα μείνει στο δίκτυο για μεγαλύτερο χρονικό διάστημα για να κερδίσει κέρδη.

Επιπλέον, καθώς δεν υπάρχει κανένας παράγοντας που να κάνει τους επενδυτές συγκεντρωτικούς, το *Proof of Burn* (*PoB*) ενισχύει την αποκέντρωση και δημιουργεί ένα κατανεμημένο δίκτυο. Από την άλλη πλευρά, η καύση εξόρυξης νομισμάτων *PoW* σπαταλά ενέργεια και χρόνο. Εάν μια μέρα η αξία των κερμάτων *PoB* γίνει μεγαλύτερη από τα καμένα νομίσματα *PoW*, θα μπορούσαμε να πούμε ότι το *PoB* είναι πιο ενεργειακά αποδοτικό από το *PoW* και τα χαμένα νομίσματα, ενέργεια και χρόνος θα ανακτηθούν κατά κάποιο τρόπο.

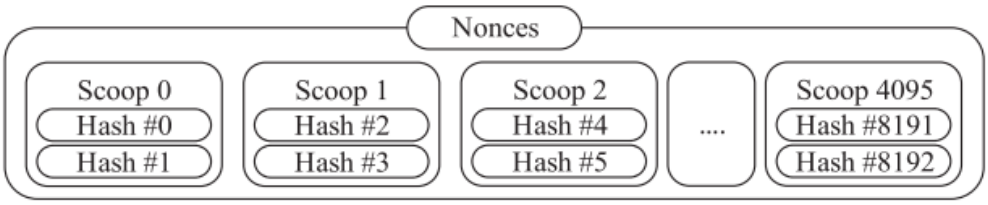
1.7.10 ΑΠΟΔΕΙΞΗ ΙΚΑΝΟΤΗΤΑΣ (*PROOF OF CAPACITY*)

Η έννοια της απόδειξης της ικανότητας (*PoC*), είναι επίσης γνωστή ως απόδειξη χώρου (*PoSpace*). Σε αυτό τον αλγόριθμο, οι ανθρακωρύχοι χρησιμοποιούν τους ελεύθερους χώρους στο σκληρό δίσκο τους για να εξορύξουν δωρεάν νομίσματα. Το πρώτο κρυπτονόμισμα που χρησιμοποίησε αυτόν τον αλγόριθμο ιδρύθηκε από το *Burstcoin* το 2014. Ο αλγόριθμος *PoC* αποτελείται από τη γραφική παράσταση του σκληρού δίσκου που σημαίνει υπολογισμός και αποθήκευση λύσεων στον σκληρό δίσκο πριν ξεκινήσει η εξόρυξη. Ορισμένες λύσεις είναι πιο γρήγορες από άλλες. Αν ένας σκληρός δίσκος τυχαίνει να έχει αποθηκεύσει την ταχύτερη (πλησιέστερη) λύση στο παζλ του πρόσφατου μπλοκ, τότε κερδίζει το μπλοκ. Στο *Burstcoin*, η εφαρμογή του αλγορίθμου *PoC* αποτελείται από δύο στάδια. Το πρώτο στάδιο ονομάζεται *plotting* στο οποίο δημιουργούν οι ανθρακωρύχοι κάτι που ονομάζεται "*Nonce*". Τα *Nonces* δημιουργούνται από επαναλαμβανόμενο κατακερματισμό δεδομένων, συμπεριλαμβανομένου του αναγνωριστικού ανθρακωρύχου χρησιμοποιώντας μια πολύ αργή λειτουργία κατακερματισμού γνωστή ως *Shabal*. Καθώς τα *hashes* της *Shabal* είναι δύσκολο να υπολογιστούν, υπολογίζονται εκ των προτέρων και αποθηκεύονται στο σκληρό δίσκο στη μορφή *Nonces*. Όσο περισσότερο ελεύθερο χώρο διαθέτει ένας ανθρακωρύχος στην πλοκή, τόσο περισσότερα *nonces* θα δημιουργούνται. Τα *Nonces* περιέχουν 8192 κατακερματισμούς.

Κάθε δύο *hashes* κάνουν μια μεζούρα, οπότε ένα *nonce* περιέχει 4096 *scoops* τα οποία επισημαίνονται από 0 έως 4095 όπως παρουσιάζεται στο ακόλουθο σχήμα. Πριν την εκκίνηση του *mining*, ένας ανθρακωρύχος πρέπει να γεμίσει όλο τον επιθυμητό ελεύθερο χώρο στο σκληρό δίσκο του με *nonces*. Αυτά τα *nonces* λειτουργούν σαν ένα λαχείο που

περιέχει μία σειρά αριθμών και γραμμάτων. Εάν ένα από τα *hashes* σε ένα *nonce* είναι το πιο κοντινό στο πρόσφατο παζλ στο δίκτυο, σημαίνει ότι κερδίζει τη μάχη εξόρυξης.

Πρέπει να σημειωθεί ότι σε αντίθεση με το *bitcoin* που χρειάζεται ειδικό υλικό όπως *ASIC* και *CPU/GPU* για εξόρυξη, το μόνο υλικό που χρησιμοποιείται στο *PoC* είναι οποιοσδήποτε συνηθισμένος σκληρός δίσκος και επομένως κανείς δεν μπορεί να επωφεληθεί από ειδικό λογισμικό. Επιπλέον, εφόσον όλοι έχουν έχουν εύκολη πρόσβαση σε σκληρούς δίσκους, το δίκτυο θα παραμείνει αποκεντρωμένο.



Πηγή: https://www.sciencedirect.com/science/article/abs/pii/S0957417420302098

1.7.11 ΑΠΟΔΕΙΞΗ ΣΗΜΑΣΙΑΣ (*PROOF OF IMPORTANCE*)

Το *Proof of Importance* (*PoI*) είναι ένας άλλος αλγόριθμος συναίνεσης που εισήχθη για πρώτη φορά προκειμένου να αντιμετωπιστούν οι επικρίσεις στον αλγόριθμο *Proof of Stake*. Στο *blockchain* κάθε λογαριασμός ή στον κόμβο λαμβάνει μια βαθμολογία σπουδαιότητας που επηρεάζει την πιθανότητα του λογαριασμού να λάβει μια μικρή οικονομική ανταμοιβή σε αντάλλαγμα προσθήκης συναλλαγών χρηστών στο δίκτυο.

Τρεις παράγοντες που καθορίζουν τη συνολική βαθμολογία ενός λογαριασμού είναι:

• **Κατοχύρωση:** όσο μεγαλύτερος είναι ο αριθμός των κατοχυρωμένων νομισμάτων, τόσο υψηλότερο είναι το σκορ. Μετράνε μόνο τα νομίσματα που υπήρχαν σε έναν λογαριασμό για ένα σύνολο ημερών.

• **Συνεργασία συναλλαγών:** Όποιος κάνει περισσότερες συναλλαγές με άλλους λογαριασμούς στο δίκτυο θα έχει καλύτερη βαθμολογία.

• **Αριθμός και μέγεθος συναλλαγών τις τελευταίες 30 ημέρες:** κάθε συναλλαγή πάνω από ένα ελάχιστο μέγεθος θα αυξήσει το σκορ του λογαριασμού. Μεγαλύτερες και συχνότερες συναλλαγές έχουν μεγαλύτερο αντίκτυπο.

Μετά τον υπολογισμό της βαθμολογίας του λογαριασμού, ο λογαριασμός θα λάβει μια πιθανότητα που σχετίζεται με την επιτευχθείσα βαθμολογία για την προσθήκη ενός μπλοκ στο δίκτυο *blockchain*. Αυτή η μέθοδος διασφαλίζει την αποκέντρωση του *blockchain* ενώ δημιουργεί επίσης μια ισορροπία μεταξύ κλειδώματος χρημάτων σε λογαριασμούς και τη διάδοση τους. Αυτά τα αντίμετρα κάνουν την Απόδειξη Σημασίας (*Proof of Importance*) ανθεκτική στις επιθέσεις τύπου *Sybil* που είναι ελαττωματικά ή κακόβουλα και παρουσιάζονται με πολλαπλές ταυτότητες προκειμένου να αποκτήσουν τον έλεγχο ενός συστήματος.

Συνοψίζοντας, ο αλγόριθμος *PoI* μπορεί να είναι γρήγορος και αποτελεσματικός, καθώς δεν απαιτείται εξόρυξη και το σύστημα βαθμολόγησής του είναι αποκεντρωμένο, επεκτάσιμο και ασφαλές. Δεν υπάρχει ειδικό υλικό που απαιτείται για την εξόρυξη και αποτελεί σημαντική βελτίωση στον παραδοσιακό αλγόριθμο *PoS*.

1.7.12 ΑΠΟΔΕΙΞΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ (*PROOF OF ACTIVITY*)

Η απόδειξη δραστηριότητας (*PoA*) είναι ένας άλλος κοινός αλγόριθμος συναίνεσης. Οι συγγραφείς δήλωσαν ότι πρότειναν έναν αλγόριθμο συναίνεσης που βασίζεται στον συνδυασμό *PoW* και *PoS*. Είναι ένας σχεδόν ασφαλής αλγόριθμος έναντι πιθανών πρακτικών επιθέσεων σε *Bitcoin* και έχει χαμηλή ποινή όσον αφορά την επικοινωνία δικτύου και τον αποθηκευτικό χώρο.

Αυτός ο αλγόριθμος εισάγεται ως φύλακας από τα δυναμικά προβλήματα στο *Bitcoin* όπως η «τραγωδία των κοινών», όπου οι ανθρακωρύχοι αρχίζουν να ενεργούν μόνο για τα συμφέροντά τους, και τις επιθέσεις δικτύου, όπως άρνηση λειτουργίας δικτύου και απομόνωση δικτύου. Για το *bitcoin*, μπορεί να συμβεί η τραγωδία των κοινών αφού όλα τα 21 εκατομμύρια κέρματα εξόρυξης-ανταμοιβής έχουν εξορυχθεί και οι ανθρακωρύχοι λαμβάνουν μόνο ανταλλακτικές ανταμοιβές.

Όταν η συνδεσιμότητα μεταξύ των κόμβων είναι χαμηλή, καθίσταται ευκολότερο να αρνηθείτε την υπηρεσία πλημμυρίζοντας κόμβους ανθρακωρύχων ή μεταφέροντας την εκτέλεση επίθεσης *Sybil* με την απομόνωση και συναλλαγή με κάποιο συγκεκριμένο κόμβο. Επιπλέον, στο *Bitcoin* ένας εισβολέας μπορεί να προσπαθήσει να διαχειριστεί την τιμή στα χρηματιστήρια στα οποία διαπραγματεύεται το *Bitcoin*, για να προκαλέσει ζημιά της εμπιστοσύνης. Ωστόσο, με τα πρωτόκολλα που βασίζονται στο *Proof of Stake*, τα ενδιαφερόμενα μέρη είναι λιγότερο πιθανό να μειώσουν τις σπείρες των τιμών, επειδή τα νομίσματα που κατέχουν παράγουν έσοδα ανάλογα με το πραγματικό εμπόριο που λαμβάνει χώρα.

Όσον αφορά την ασφάλεια, η πιθανότητα επίθεσης 51% στο *PoA* πέφτει σχεδόν στο μηδέν, καθώς μια τέτοια επίθεση θα απαιτούσε ο εισβολέας να έχει το 51% όλων των νομισμάτων και επίσης το 51% της εξορυκτικής δύναμης ταυτόχρονα και ως εκ τούτου, το *PoA* είναι πιο ασφαλές σε σύγκριση σε *PoW* και *PoS*. Από την άλλη πλευρά, το *PoA* εκμεταλλεύεται το εξορυκτικό τμήμα του *PoW* και ως εκ τούτου χρειάζεται μια τεράστια ποσότητα ενέργειας και υπολογιστική ισχύ. Αναφέρεται επίσης ότι το *PoA* θα μπορούσε να είναι ευάλωτο στην επίθεση με διπλές δαπάνες.

Συμπερασματικά, ενώ διασφαλίζεται το δίκτυο έναντι πιθανών προβλημάτων όπως η επίθεση 51%, η απόδειξη δραστηριότητας έχει σημαντικά ελαττώματα. Το *PoA* απαιτεί πολλούς πόρους και ενέργεια και επίσης είναι επιρρεπής σε επιθέσεις διπλής δαπάνης με βάση τη δωροδοκία. Δύο δημοφιλή κρυπτονομίσματα, το *Decred* και το *Espers* έχουν υιοθετήσει το *PoA* στο *blockchain* τους, ενώ το *Decred* (*DCR*) έχει υιοθετήσει πολύ καλύτερες επιδόσεις όσον αφορά την τιμολόγηση της αγοράς σε σύγκριση με *Espers*.

1.7.13 ΚΑΤΕΥΘΥΝΟΜΕΝΑ ΑΚΥΚΛΙΚΑ ΓΡΑΦΗΜΑΤΑ (*DIRECTED ACYCLIC GRAPHS*)

Αν και τα κατευθυνόμενα ακυκλικά γραφήματα ή *DAGs* είναι βασικά μια μορφή των δομών δεδομένων και δεν είναι πραγματικά δίκτυα *blockchain*, χρησιμοποιούνται ευρέως σε επιτυχημένα κρυπτονομίσματα.

Οι *NXT*, *IOTA* και *IoT Chain* είναι από τις πιο επιτυχημένες εφαρμογές του *DAG*. Σε πραγματικά δίκτυα *blockchain*, οι συναλλαγές αποθηκεύονται σε μια αλυσίδα δικτύων αλλά στις συναλλαγές *DAG* αποθηκεύονται τοπολογικά σε μία γραφική παράσταση.

Το ακυκλικό γράφημα είναι ένα γράφημα που δεν έχει κύκλο. Σε ακυκλικό γράφημα, οι πληροφορίες δεν μπορούν να περάσουν από έναν κόμβο σε άλλο κόμβο και επιστρέφουν στον αρχικό κόμβο χωρίς να συναντήσουν έναν κόμβο περισσότερο από μία φορές. Ένα κατευθυνόμενο ακυκλικό γράφημα είναι ένα ακυκλικό γράφημα που οι πληροφορίες μπορούν να περάσουν μόνο από μια προκαθορισμένη κατεύθυνση.

Λόγω της δομής τους χωρίς μπλοκ, τα *DAG* θεωρούνται ως *blockchains* χωρίς μπλοκ. Οι συναλλαγές κρυπτονομισμάτων επαληθεύονται και προστίθενται στο δίκτυο με τρόπο που είναι ταχύτερη από τα δίκτυα που βασίζονται σε *PoW* και *PoS*, καθώς δεν υπάρχει ανάγκη να τα αποθηκευθούν μέσα σε ένα πραγματικό μπλοκ και στη συνέχεια να επαληθευθεί ολόκληρο το μπλοκ. Σε ένα *blockchain*, πρέπει να καθοριστεί μία αυθαίρετη χρονική περίοδος για να διασφαλιστεί ότι η κύρια αλυσίδα παραμένει βιώσιμη. Αυτός ο χρόνος αναμονής είναι γνωστός ως χρόνος αποκλεισμού και δίνει στο δίκτυο χρόνο για να εμπεδώσει και να επαληθεύσει ποιος κλάδος της αλυσίδας είναι σωστός. Ωστόσο, στις *DAGs*, εφόσον οι πληροφορίες κατευθύνονται με τον ίδιο τρόπο, οι κόμβοι μπορούν να υπάρχουν παράλληλα.

Αυτός ο τύπος δικτύου δίνει τη δυνατότητα να εξαλειφθεί η ανάγκη για χρόνους αποκλεισμού και την ταχύτερη επαλήθευση των συναλλαγών.

Το αποτέλεσμα είναι ένα γρήγορο, επεκτάσιμο και εντελώς αποκεντρωμένο δίκτυο. Τα *blockchains* είναι επιρρεπή στο διπλασιασμό δαπανών, ωστόσο, στις *DAGs* η επικύρωση μιας συγκεκριμένης συναλλαγής αποφασίζεται από τον αριθμό των συναλλαγών πίσω από αυτήν. Αυτό καθιστά ένα σύστημα *DAG* πιο γρήγορο και προστατευμένο ενάντια σε μια επίθεση διπλών δαπανών.

Όσον αφορά το πλάτος του δικτύου, προσθέτοντας τη συναλλαγή σε μια προηγούμενη συναλλαγή κάθε φορά κάνει το δίκτυο επίσης πλατύ. Σε ένα *DAG*, κάθε επικυρωμένη συναλλαγή πρέπει να συνδέεται με μια υπάρχουσα και νέα συναλλαγή του δικτύου. Όταν μια συναλλαγή συμβαίνει σε ένα πλήρες δίκτυο *DAG*, το δίκτυο θα επιλέξει μια υπάρχουσα μεταγενέστερη συναλλαγή προς σύνδεση. Αυτή η προσέγγιση θα διατηρήσει το πλάτος του δικτύου μέσα σε ένα συγκεκριμένο εύρος που μπορεί να υποστηρίξει γρήγορα επικύρωση για συναλλαγές. Η *IOTA* πρότεινε τον δικό της αλγόριθμο που ονομάζεται *Tangle* για τον έλεγχο του πλάτους του δικτύου. Δεν υπάρχει διαδικασία εξόρυξης σε δίκτυο *DAG* και ως εκ τούτου, δεν υπάρχει εξάρτηση από ειδικό υλικό, επομένως η κατανάλωση ενέργειας είναι πολύ χαμηλή. Η επικύρωση των συναλλαγών συμβαίνει σχεδόν αμέσως. Το τέλος συναλλαγής μπορεί να είναι πολύ χαμηλό και γρήγορο.

Έτσι, αυτό καθιστά ένα δίκτυο *DAG* φιλικό προς μικρές, ακόμη και μικροσυναλλαγές ή πληρωμές. Η αλυσίδα *IoT*, για παράδειγμα, μπορεί να χειριστεί 10.000 συναλλαγές ανά δευτερόλεπτο. Αυτά τα χαρακτηριστικά ενός δικτύου *DAG* μαζί με την ικανότητά του να αμύνεται στην επίθεση 51%, το έχει καταστήσει μια τέλεια προσέγγιση για Διαδίκτυο των Πραγμάτων (*Internet-of-things*) και επικοινωνίες Μηχάνημα προς Μηχάνημα (*Machine-to-Machine*). [17]

[17] (Πατσιλίβας, 2020)

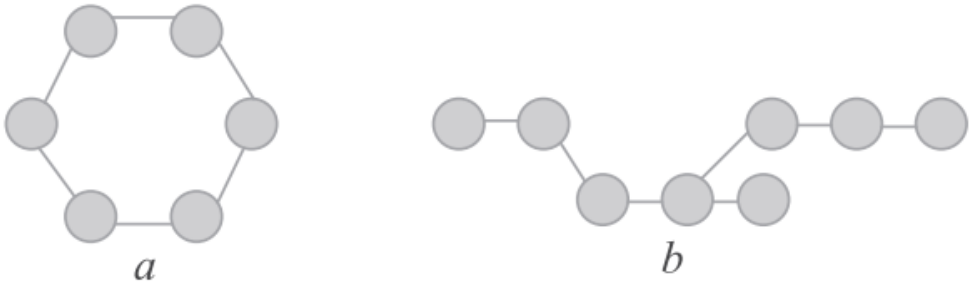


Fig. 3. (a) a cyclic and non-directed graph (b) an acyclic graph.

Πηγή: https://www.sciencedirect.com/science/article/abs/pii/S0957417420302098

1.8 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ *BLOCKCHAIN*

Ενισχυμένη ασφάλεια

Τα δεδομένα είναι ευαίσθητα και κρίσιμα και το *blockchain* μπορεί να αλλάξει σημαντικά τον τρόπο εμφάνισης των κρίσιμων πληροφοριών. Δημιουργώντας μια εγγραφή που δεν μπορεί να τροποποιηθεί και είναι κρυπτογραφημένη από άκρο σε άκρο, το *blockchain* βοηθά στην αποφυγή απάτης και μη εξουσιοδοτημένης δραστηριότητας. Τα ζητήματα απορρήτου μπορούν επίσης να αντιμετωπιστούν στο *blockchain* παρέχοντας ανωνυμοποίηση για τα προσωπικά δεδομένα και χρησιμοποιώντας δικαιώματα για να αποτραπεί πρόσβαση. Οι πληροφορίες αποθηκεύονται σε ένα δίκτυο υπολογιστών και όχι σε έναν μόνο διακομιστή, καθιστώντας δύσκολο για τους χάκερ να δουν τα δεδομένα.

Μεγαλύτερη διαφάνεια

Χωρίς το *blockchain*, ο κάθε οργανισμός πρέπει να διατηρεί ξεχωριστή βάση δεδομένων. Επειδή το *blockchain* χρησιμοποιεί ένα κατανεμημένο βιβλίο, οι συναλλαγές και τα δεδομένα καταγράφονται πανομοιότυπα σε πολλές τοποθεσίες. Όλοι οι συμμετέχοντες στο δίκτυο με άδεια πρόσβασης βλέπουν τις ίδιες πληροφορίες ταυτόχρονα, παρέχοντας πλήρη διαφάνεια. Όλες οι συναλλαγές καταγράφονται αμετάβλητες και φέρουν σφραγίδα ώρας και ημερομηνίας. Αυτό επιτρέπει στα μέλη να βλέπουν ολόκληρο το ιστορικό μιας συναλλαγής και ουσιαστικά εξαλείφει κάθε ευκαιρία για απάτη.

Άμεση ιχνηλασιμότητα

Το *Blockchain* δημιουργεί ένα μονοπάτι ελέγχου που τεκμηριώνει την προέλευση ενός περιουσιακού στοιχείου σε κάθε βήμα στο ταξίδι του. Σε βιομηχανίες όπου οι καταναλωτές ανησυχούν για περιβαλλοντικά ή ανθρώπινα δικαιώματα που σχετίζονται με ένα προϊόν - ή μια βιομηχανία που προβληματίζεται από την παραχάραξη και την απάτη - αυτό βοηθά στην απόδειξη. Με το *blockchain*, είναι δυνατό να μοιρασθούν δεδομένα σχετικά με την προέλευση απευθείας με τους πελάτες. Τα δεδομένα ιχνηλασιμότητας μπορούν επίσης να εκθέσουν αδυναμίες σε οποιαδήποτε αλυσίδα εφοδιασμού - όπου τα εμπορεύματα ενδέχεται να βρίσκονται σε μια αποβάθρα φόρτωσης που περιμένουν τη διέλευση.

Αυξημένη απόδοση και ταχύτητα

Οι παραδοσιακές διαδικασίες με χαρτί είναι χρονοβόρες, επιρρεπείς σε ανθρώπινο λάθος και συχνά απαιτούν διαμεσολάβηση τρίτων. Με τον εξορθολογισμό αυτών των διαδικασιών με *blockchain*, οι συναλλαγές μπορούν να ολοκληρωθούν γρηγορότερα και πιο αποτελεσματικά.

Τα έγγραφα μπορούν να αποθηκευτούν στο *blockchain* μαζί με τα στοιχεία της συναλλαγής, εξαλείφοντας την ανάγκη ανταλλαγής χαρτιού.

Αυτοματοποίηση

Οι συναλλαγές μπορούν ακόμη και να αυτοματοποιηθούν με «έξυπνα συμβόλαια», τα οποία αυξάνουν την αποδοτικότητά σας και επιταχύνουν ακόμη περισσότερο τη διαδικασία. Μόλις πληρούνται οι προκαθορισμένες προϋποθέσεις, ενεργοποιείται αυτόματα το επόμενο βήμα στη συναλλαγή ή τη διαδικασία. Τα έξυπνα συμβόλαια μειώνουν την ανθρώπινη παρέμβαση καθώς και την εξάρτηση από τρίτα μέρη για να επαληθεύσουν ότι πληρούνται οι όροι μιας σύμβασης. Στην ασφάλιση, για παράδειγμα, όταν ένας πελάτης έχει παράσχει όλη την απαραίτητη τεκμηρίωση για την υποβολή απαίτησης, η απαίτηση μπορεί αυτόματα να τακτοποιηθεί και να πληρωθεί.

Πώς επωφελούνται οι βιομηχανίες από το *blockchain*;

Οφέλη *Blockchain* στις αλυσίδες εφοδιασμού και στην τροφική αλυσίδα

Η οικοδόμηση εμπιστοσύνης μεταξύ των εμπορικών εταίρων, η ορατότητα από άκρη σε άκρη, ο εξορθολογισμός των διαδικασιών και η ταχύτερη επίλυση ζητημάτων με το *blockchain* προσθέτουν ισχυρότερες, πιο ανθεκτικές αλυσίδες εφοδιασμού και καλύτερες επιχειρηματικές σχέσεις. Επιπλέον, οι συμμετέχοντες μπορούν να ενεργήσουν νωρίτερα σε περίπτωση διαταραχών. Στη βιομηχανία τροφίμων, το *blockchain* μπορεί να βοηθήσει στη διασφάλιση της ασφάλειας και της φρεσκάδας των τροφίμων και στη μείωση των απορριμμάτων. Σε περίπτωση μόλυνσης, τα τρόφιμα μπορούν να εντοπιστούν στην πηγή τους σε δευτερόλεπτα και όχι σε ημέρες.

Οφέλη από το *blockchain* στην τραπεζική και στην χρηματοπιστωτική βιομηχανία

Όταν τα χρηματοπιστωτικά ιδρύματα αντικαθιστούν παλιές διαδικασίες και γραφειοκρατία με *blockchain*, τα οφέλη περιλαμβάνουν την άρση τριβών και καθυστερήσεων και την αύξηση της λειτουργικής αποτελεσματικότητας σε ολόκληρο τον κλάδο, συμπεριλαμβανομένου του παγκόσμιου εμπορίου, της χρηματοδότησης του εμπορίου, της εκκαθάρισης και του διακανονισμού, της τραπεζικής καταναλωτών, του δανεισμού και άλλων συναλλαγών.

Οφέλη *blockchain* στον χώρο της υγείας

Σε μια βιομηχανία που προβληματίζεται από παραβιάσεις δεδομένων, το *blockchain* μπορεί να βοηθήσει την υγειονομική περίθαλψη να βελτιώσει την ασφάλεια των δεδομένων των ασθενών, καθιστώντας ευκολότερη την κοινή χρήση αρχείων μεταξύ παρόχων, συνδρομητών και ερευνητών. Ο έλεγχος της πρόσβασης παραμένει στα χέρια του ασθενούς, αυξάνοντας την εμπιστοσύνη.

Φαρμακευτικά οφέλη *blockchain*

Καθώς τα φαρμακευτικά προϊόντα κινούνται στην αλυσίδα εφοδιασμού, κάθε δράση καταγράφεται. Το ίχνος ελέγχου που προκύπτει σημαίνει ότι ένα προϊόν μπορεί να εντοπιστεί από την προέλευση στο φαρμακείο ή τον λιανοπωλητή, βοηθώντας στην αποτροπή της παραποίησης και επιτρέποντας στους κατασκευαστές να εντοπίσουν ένα προϊόν που ανακαλείται σε δευτερόλεπτα.

Κυβερνητικά οφέλη *blockchain*

Το *blockchain* μπορεί να βοηθήσει τις κυβερνήσεις να λειτουργήσουν πιο έξυπνα και να καινοτομήσουν γρηγορότερα. Η ασφαλής ανταλλαγή δεδομένων μεταξύ πολιτών και φορέων μπορεί να αυξήσει την εμπιστοσύνη, παρέχοντας παράλληλα ένα αμετάβλητο ίχνος ελέγχου για συμμόρφωση με τις κανονιστικές ρυθμίσεις, διαχείριση συμβάσεων, διαχείριση ταυτότητας και υπηρεσίες πολιτών.

Οφέλη ασφάλισης *blockchain*

Οι ασφαλιστικές εταιρείες χρησιμοποιούν *blockchain* και έξυπνα συμβόλαια για να αυτοματοποιήσουν χειροκίνητες και έντασης διαδικασίες όπως η ανάληψη εγγυήσεων και ο διακανονισμός απαιτήσεων, η αύξηση της ταχύτητας και της αποδοτικότητας και η μείωση του κόστους. Οι ταχύτερες, επαληθεύσιμες ανταλλαγές δεδομένων του *Blockchain* συμβάλλουν στη μείωση της απάτης και της κατάχρησης.[18]

1.9 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ *BLOCKCHAIN*

Οι παρακάτω είναι οι βασικοί λόγοι μειονεκτημάτων που πρέπει να ληφθούν υπόψη σχετικά με το *blockchain*:

1) Τα *blockchains* χρησιμοποιούν υπερβολική ενέργεια

2) Το *blockchain* δεν είναι ένα τεράστιο κατανεμημένο υπολογιστικό σύστημα

3) Η εξόρυξη δεν παρέχει ασφάλεια δικτύου

4) Οι καταχωρήσεις *blockchain* δεν διαρκούν για πάντα ή δεν είναι αμετάβλητες

5) Η επεκτασιμότητα παραμένει η αδυναμία του *blockchain*

6) Το *blockchain* δεν είναι άφθαρτο

7) ο ανώνυμος/ανοιχτός χαρακτήρας των *blockchains* δεν είναι περιουσιακό στοιχείο

8) Η απόδειξη της εργασίας είναι υπερβολική

9) Το *blockchain* μπορεί να δημιουργήσει πολυπλοκότητα

10) Τα *blockchains* μπορεί να είναι αρκετά αναποτελεσματικά.

1) Τα *blockchains* χρησιμοποιούν υπερβολική ενέργεια

Ανταγωνιστές ανθρακωρύχοι και γιγαντιαία αγροκτήματα εξόρυξης καίνε μια δυσανάλογη ποσότητα ηλεκτρικής ενέργειας σε σύγκριση με το αποτέλεσμα, τη δημιουργία του επόμενου μπλοκ. Σε έναν κόσμο όπου η τρέχουσα παραγωγή ενέργειας είναι ένα θέμα για το κλίμα, η επεξεργασία *blockchain* δεν έχει πολύ νόημα. Π.χ. το *Bitcoin* χρησιμοποιεί το ισοδύναμο της ετήσιας κατανάλωσης ενέργειας της Ελβετίας. Η κατανάλωση ενέργειας για επεξεργασία *blockchain* (εξόρυξη, όπως και να έχει σχεδιαστεί και παραδοθεί) είναι ένα ζήτημα που δεν φαίνεται να εξαφανίζεται. Η χρήση ενέργειας θα πρέπει να είναι ένα υπαρξιακό ζήτημα για όλες τις επιχειρήσεις που εξετάζουν την τεχνολογία *blockchain*. Η κατανόηση της

[18] (Μαυρουδής, 2019)

«ενεργειακής αλυσίδας» σε όλες τις πτυχές της δεν είναι απλή. Αλλά είναι απαραίτητη για να σωθεί ο πλανήτης.

2) Το *blockchain* δεν είναι ένα τεράστιο κατανεμημένο υπολογιστικό σύστημα

Όλοι οι κόμβοι που διατηρούν ένα *blockchain* κάνουν ακριβώς το ίδιο πράγμα. Επαληθεύουν τις ίδιες συναλλαγές σύμφωνα με τους ίδιους κανόνες και εκτελούν πανομοιότυπες πράξεις. Καταγράφουν το ίδιο πράγμα σε ένα *blockchain*, αποθηκεύουν όλη την ιστορία, η οποία είναι η ίδια για όλους, για όλες τις εποχές. Δεν υπάρχει παραλληλισμός, συνέργεια και αμοιβαία βοήθεια. Υπάρχει μόνο άμεση, πολλαπλή διπλή αντιγραφή. Αυτό είναι το αντίθετο του αποδοτικού και, ενώ είναι διανεμημένο, δεν είναι ένα κατανεμημένο σύστημα υπολογιστή που θα ωφελήσει όλους.

3) Η εξόρυξη δεν παρέχει ασφάλεια δικτύου

Πολλοί υποστηρικτές του *blockchain* (ειδικά του *Bitcoin*) υποστηρίζουν ότι οι ανθρακωρύχοι διατηρούν τη σταθερότητα και την ασφάλεια ενός *blockchain*. Αν υπάρχουν αρκετοί ανθρακωρύχοι αυτό είναι αλήθεια. Το πρόβλημα είναι ότι οι ανθρακωρύχοι μπορούν να συνδυαστούν. Αν το κάνουν, δημιουργούν μία συγκέντρωση (στην περίπτωση του *Bitcoin,*> 50% της εξορυκτικής δύναμης) και μπορούν να ξαναγράψουν ή να αλλάξουν το ρεκόρ του *blockchain*. Εάν αυτό είναι δυνατό, η ασφάλεια των δεδομένων εξαφανίζεται. Το αντίθετο επιχείρημα είναι ότι δεν υπάρχει οικονομικό κίνητρο για τους ανθρακωρύχους. Αυτό μπορεί να είναι σωστό όταν υπάρχει επαρκές οικονομικό κίνητρο.

4) Οι καταχωρήσεις *blockchain* δεν διαρκούν για πάντα ή δεν είναι αμετάβλητες

Ισχύουν τα προαναφερόμενα.

5) Η επεκτασιμότητα παραμένει η αδυναμία του *blockchain*

Το *Bitcoin* είναι η πιο επιτυχημένη εφαρμογή *blockchain* από πολλούς χρήστες. Ωστόσο, μόνο ένας στους χίλιους ανθρώπους στον πλανήτη το χρησιμοποιεί. Δεδομένης της αργής ταχύτητας επεξεργασίας των συναλλαγών, η σημαντική αύξηση του αριθμού των ενεργών χρηστών δεν είναι πρακτική.

6) Το *blockchain* δεν είναι άφθαρτο

Μπορεί να φαίνεται ότι, αν ένα *blockchain* είναι αποθηκευμένο σε κάθε κόμβο δικτύου, τότε ειδικές υπηρεσίες ή αρχές δεν μπορούν να κλείσουν ένα *blockchain*. Εάν δεν υπάρχει κεντρικός διακομιστής ή σημείο ελέγχου, τότε δεν υπάρχει τρόπος να κλείσει το *blockchain*.

7) ο ανώνυμος/ανοιχτός χαρακτήρας των *blockchains* δεν είναι περιουσιακό στοιχείο

Ένα από τα χαρακτηριστικά του *blockchain* είναι ότι είναι ανοιχτό. Όποιος είναι εξουσιοδοτημένος μπορεί να δει τα πάντα.

8) Η απόδειξη της εργασίας είναι υπερβολική

Η απόδειξη της εργασίας είναι υπερβολική. Αυτό ισχύει ακόμη και αν κάνετε έκπτωση ή αγνοήσετε την κατανάλωση ενέργειας.

9) Το *blockchain* μπορεί να δημιουργήσει πολυπλοκότητα

Πολλοί θεωρούν την αποκέντρωση ως το λόγο ύπαρξης του *blockchain*. Ωστόσο, η τεχνολογία *blockchain* - στην τρέχουσα κατάσταση της - έχει περιορισμούς. Ταυτόχρονα, οι

υπάρχουσες συγκεντρωτικές δομές και υπηρεσίες θα πρέπει να προσαρμοστούν στις τεχνολογίες *blockchain*, προκειμένου να συνεχιστούν οι υπάρχουσες επενδύσεις. Σε αυτό το πλαίσιο ορισμένοι υποστηρίζουν ότι είναι λογικό για τις επιχειρήσεις να εξετάσουν μια υβριδική προσέγγιση που συνδυάζει τις καλύτερες πτυχές των συγκεντρωτικών και αποκεντρωμένων συστημάτων. Οραματίζονται αυτό ως σημείο αναφοράς στο ταξίδι προς το τελικό σημείο της εντελώς αποκεντρωμένης δομής. Το πρόβλημα με αυτό είναι η πολυπλοκότητα. Σκεφτείτε μερικά από τα ζητήματα. Πάρτε, για παράδειγμα, ένα *blockchain* το οποίο περιέχει μόνο δείκτες σε αρχεία που διατηρούνται σε συμβατικές βάσεις δεδομένων και/ή πλευρικές αλυσίδες (*sidechains*). Το *blockchain* μπορεί να λειτουργεί με μεγάλη αποδοτικότητα και αποτελεσματικότητα - επειδή πρέπει να επεξεργαστεί τόσο λίγα. Αλλά προσθέτοντας έναν εξωτερικό σύνδεσμο, σε μία ή περισσότερες συμβατικές βάσεις δεδομένων προσθέτει περισσότερα κινούμενα μέρη για να αποτύχουν.

10) Τα *blockchains* μπορεί να είναι αρκετά αναποτελεσματικά.

Οι περισσότεροι υψηλής ποιότητας πελάτες δικτύου *blockchain* αποθηκεύουν ένα ολόκληρο ιστορικό συναλλαγών. Στην περίπτωση του *Bitcoin*, αυτό το ρεκόρ ξεπερνά τα 100 GB - το σημαντικό ποσοστό της χωρητικότητας αποθήκευσης ενός φορητού υπολογιστή ή *smartphone*. Ακόμη χειρότερα, αυτό επαναλαμβάνεται στους περισσότερους, όχι σε όλους, συμμετέχοντες κόμβους.

Για να αποθηκεύσετε δεδομένα *blockchain*, πρέπει να τα κατεβάσετε. Όπως όλοι όσοι έχουν προσπαθήσει να χρησιμοποιήσουν τοπικά αποθηκευμένο πορτοφόλι για κρυπτονόμισμα γνωρίζουν ότι δεν μπορούν να πραγματοποιήσουν ή να λάβουν πληρωμές μέχρι να ολοκληρωθεί ολόκληρη η διαδικασία λήψης και επαλήθευσης. Σε ορισμένες περιπτώσεις αυτό διαρκεί μερικές ημέρες, τις οποίες οι χρήστες δύσκολα θα θεωρήσουν πρόοδο. Επιπλέον, όσο περισσότερες συναλλαγές διεκπεραιώνονται, τόσο πιο γρήγορα μεγαλώνει το μέγεθος. Αναμφισβήτητα, η διάρκεια ζωής ενός *blockchain* είναι περιορισμένη υπό τις τρέχουσες συνθήκες.

Αν και υπάρχουν αρνητικά για το *blockchain*, ο στόχος δεν είναι να απαξιωθεί το *blockchain*. Μάλλον ο σκοπός είναι να ενθαρρυνθούν οι επιχειρήσεις να σκεφτούν πριν δράσουν.

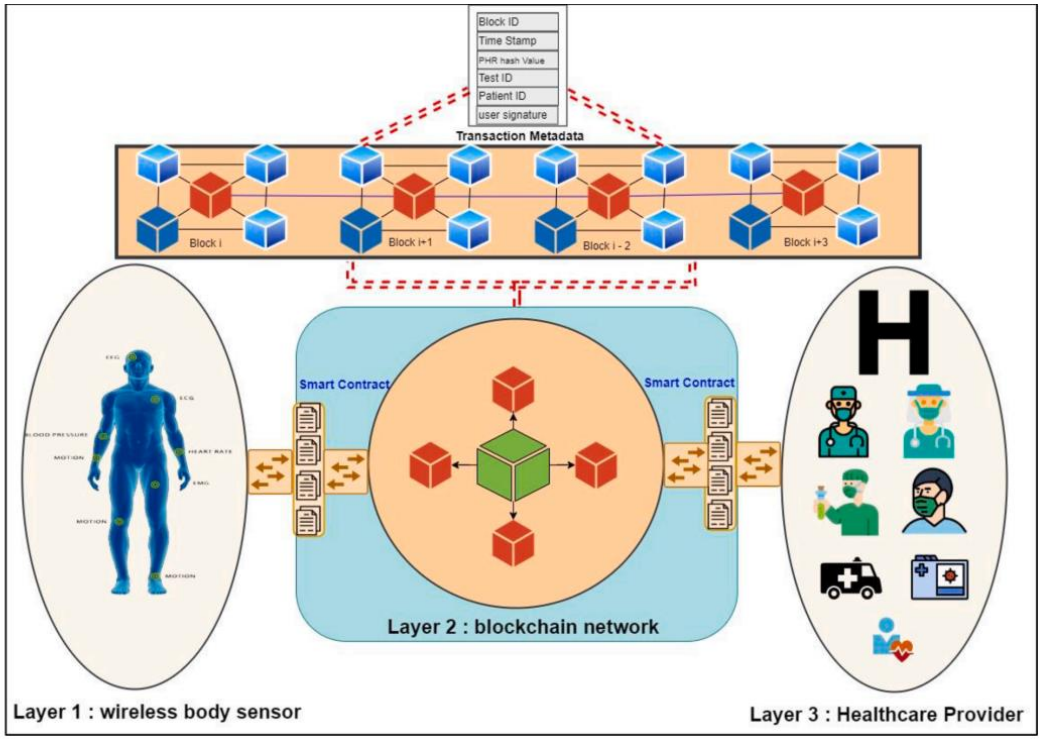
2. ΤΟΜΕΙΣ ΕΦΑΡΜΟΓΗΣ BLOCKCHAIN

2.1 ΥΓΕΙΑ

2.1.1 ΣΥΣΤΗΜΑ *TMIS (TELECARE MEDICAL INFORMATION SYSTEMS)*

Η ενσωμάτωση της τεχνολογίας *blockchain* στην εφαρμογή του τηλεπικοινωνιακού ιατρικού συστήματος πληροφοριών αφορά 3 στρώματα, τα οποία αποτυπώνονται στο ακόλουθο σχήμα. Υπάρχει αισθητήρας ασύρματου σώματος, το οποίο αφορά μία ομάδα ασθενών που συνδέονται με τους αισθητήρες για να παρακολουθήσουν τις συνθήκες υγείας τους για διαγνωστικούς σκοπούς όπως χειρουργική επέμβαση, επισκέψεις σε νοσοκομείο και παρακολούθηση ηλικιωμένων ασθενών στο σπίτι.
Το δίκτυο *blockchain* είναι υπεύθυνο για την αποθήκευση, την κοινή χρήση, την ενημέρωση των οντοτήτων της υγείας. Οι πάροχοι υγειονομικής περίθαλψης είναι μια ομάδα υγείας από επαγγελματίες, όπως γιατροί, νοσοκομεία, ασφάλιση υγείας, ιατρικές οργανώσεις, που αναζητούν καλύτερη και πιο προσιτή θεραπεία για ασθενείς χρησιμοποιώντας το δίκτυο *blockchain*.

Το *TMIS* είναι μια τεχνολογία που επιτρέπει στους γιατρούς και τους ασθενείς να στέλνουν και να λαμβάνουν υπηρεσίες υγείας ή ιατρικές πληροφορίες από απομακρυσμένες τοποθεσίες. Ως εκ τούτου, η προστασία του απορρήτου των δεδομένων των ασθενών είναι σημαντική. Έχουν αναπτυχθεί πολλές μελέτες που παρέχονται από αυτή την τεχνολογία.
Ο κύριος στόχος αυτών των μελετών είναι να ξεπεράσουν την απόσταση και τα εμπόδια και να υπάρξει ενίσχυση της πρόσβασης σε ιατρικές υπηρεσίες σε απομακρυσμένες κοινότητες. [19]

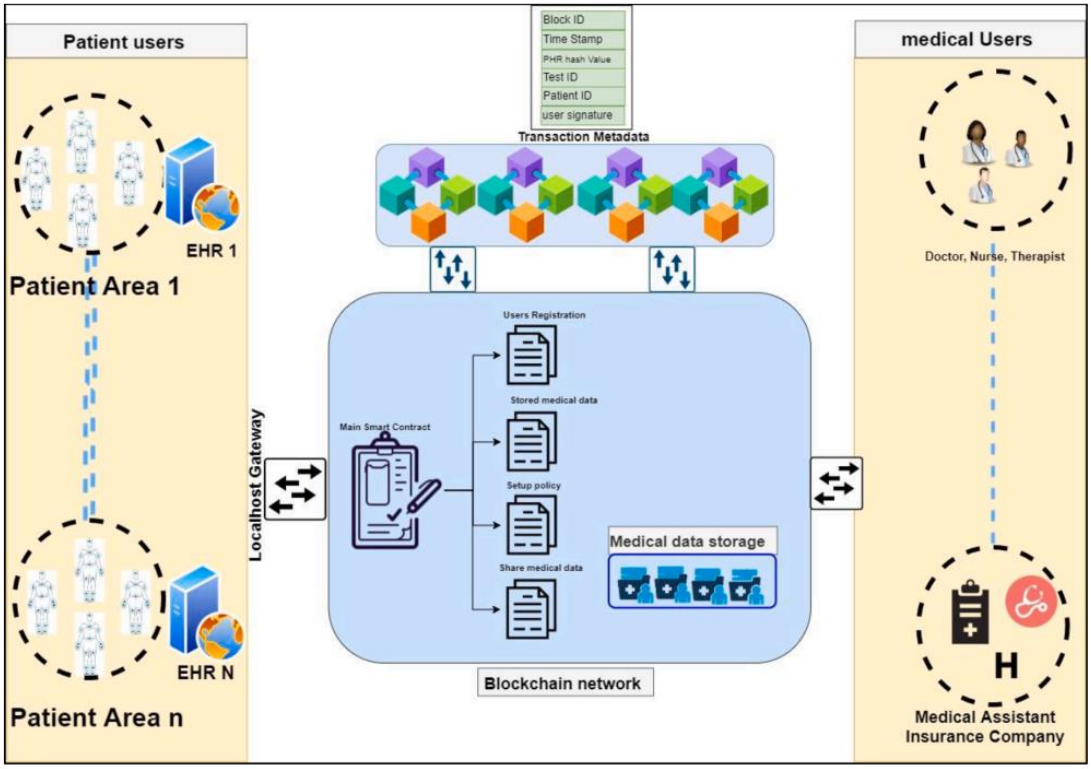


Πηγή: https://www.sciencedirect.com/science/article/abs/pii/S2452414X21000170

2.1.2 ΗΛΕΚΤΡΟΝΙΚΟ ΣΥΣΤΗΜΑ ΥΓΕΙΑΣ

Η ηλεκτρονική υγεία είναι μια τεχνολογία καινοτομίας που έχει γίνει κρίσιμα σημαντική με την πάροδο του χρόνου, που κυμαίνεται από απομακρυσμένη πρόσβαση έως ιατρικά δεδομένα καταγεγραμμένα από τον ασθενή. Η ικανότητα του *blockchain* είναι η αποθήκευση ιατρικών πληροφοριών μέσω αποκεντρωμένης αποθήκευσης στην οποία υπάρχει πρόσβαση μόνο μέσω έξυπνων συμβάσεων. Τα ιατρικά αρχεία μπορούν να είναι φορητά και εύκολα στη μεταφορά από ένα νοσοκομείο σε άλλο για τη μείωση του πρόσθετου κόστους των ασθενών χωρίς επαναλαμβανόμενα διαγνωστικά τεστ. Επίσης, επιτρέπει στους πιθανούς γιατρούς να γνωρίζουν το ιατρικό ιστορικό του ασθενούς με προσιτό τρόπο, ώστε να μπορούν οι ασθενείς να αντιμετωπίζονται ανάλογα. Η διαφάνεια και ο χειρισμός του ασθενούς επιτυγχάνεται σημαντικά με την αποθήκευση κάθε αντιγράφου των δεδομένων σε πολλαπλούς κόμβους του δικτύου *blockchain*.

[19] (Hussien, Yasin, Udzir, κ.α. 2021)



Πηγή: https://www.sciencedirect.com/science/article/abs/pii/S2452414X21000170

2.1.3 ΔΕΔΟΜΕΝΑ ΥΓΕΙΑΣ ΚΑΙ ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΜΟΙΡΑΣΗΣ

Τα δεδομένα ασθενών μπορούν να ανήκουν πραγματικά και να ελέγχονται από τον ασθενή. Επιπλέον, η τεχνολογία *blockchain* επιτρέπει στα αρχεία υγείας να σφραγίζονται χρονικά, πράγμα που σημαίνει ότι κανείς δεν μπορεί να αλλοιώσει τα έγγραφα αφού αποθηκευτούν στο κατανεμημένο καθολικό. Χρησιμοποιώντας την τεχνολογία *blockchain*, οι ασθενείς έχουν το δικαίωμα να εξουσιοδοτούν ποιοι μπορούν να έχουν πρόσβαση στα δεδομένα τους. Ωστόσο, απαιτούνται περαιτέρω μελέτες για πολλές ανοιχτές προκλήσεις, όπως κοινή χρήση διασυνοριακών δεδομένων για την υγεία, η οποία μπορεί να εμποδίσει τα πλεονεκτήματα της κοινής χρήσης δεδομένων *blockchain*. Επιπλέον, οι ατομικές προσδοκίες απορρήτου διαφέρουν μεταξύ των χωρών που οφείλονται στον κανονισμό της κυβέρνησης κάθε χώρας.

2.1.4 ΚΛΙΝΙΚΕΣ ΔΟΚΙΜΕΣ

Πραγματοποιούνται κλινικές δοκιμές για την αξιολόγηση της αποτελεσματικότητας οποιουδήποτε νέο φαρμάκου που έχει αναπτυχθεί και συνιστάται για τη θεραπεία μιας συγκεκριμένης ασθένειας. Τα νέα φάρμακα μπορούν να δοκιμαστούν με βάση την επιτυχία της δοκιμής και μπορούν να χρησιμοποιηθούν σε μεγαλύτερη κλίμακα. Οι ερευνητές διεξάγουν κλινική δοκιμή φαρμάκων με έμφαση σε διάφορες περιστάσεις για τη δημιουργία αποτελεσμάτων, στατιστικών δεδομένων και λόγων αποτελεσματικότητας για περαιτέρω αποφάσεις φαρμάκων. Το μεγαλύτερο μέρος της φαρμακευτικής βιομηχανίας είναι πρόθυμη να αποκαλύψει τα πραγματικά αποτελέσματα μιας ανάλυσης φαρμάκων που μπορεί να προσφέρει ορισμένα οφέλη για τις επιχειρήσεις τους. Ωστόσο, ορισμένοι ερευνητές συχνά κρύβουν ή τροποποιούν τις πληροφορίες τους και δεδομένα που συλλέγονται για να αλλάξει το αποτέλεσμα. Μια ελκυστική ευκαιρία είναι η ανάπτυξη ενός αποκεντρωμένου συστήματος βασισμένου σε *blockchain* για να διασφαλιστούν δίκαιες και διαφανείς κλινικές δοκιμές και για τη βελτίωση της ασφάλειας των δεδομένων.

2.1.5 ΒΙΟΜΗΧΑΝΙΑ ΦΑΡΜΑΚΩΝ

Τα πλαστά φάρμακα μπορούν να πάρουν τη ζωή χιλιάδων ανθρώπων. Το βασικό χαρακτηριστικό του *blockchain* χρησιμοποιείται για να διασφαλιστεί η ιχνηλασιμότητα ιατρικών προϊόντων παρέχοντας ένα αποκεντρωμένο διαφανές σύστημα παρακολούθησης. Η αμετάβλητη και χρονική σήμανση των συναλλαγών *blockchain* μπορεί να διευκολύνει τους κατασκευαστές φαρμάκων να παρακολουθούν τα προϊόντα και να διασφαλίζουν ότι οι πληροφορίες στο μπλοκ δεν μπορούν να τροποποιηθούν. [20]

2.2 ΤΟΥΡΙΣΜΟΣ

Η παραδοσιακή τουριστική βιομηχανία χρειάζεται επειγόντως ψηφιακές τεχνολογίες για μείωση κόστους και βελτίωση της αποτελεσματικότητας. Το *Blockchain*, ως μια αναδυόμενη τεχνολογία, υπόσχεται να μεταρρυθμίσει την τουριστική βιομηχανία γιατί παρέχει μια αξιόπιστη πλατφόρμα για τη σύνδεση της τουριστικής εταιρείας και των τουριστών. Ωστόσο, οι υπάρχουσες λύσεις έξυπνου τουρισμού βασισμένες σε *blockchain* είναι είτε εννοιολογικές είτε περιορισμένες στην επίλυση των θεμελιωδών τουριστικών προκλήσεων. Η τουριστική βιομηχανία διαδραματίζει σημαντικό ρόλο στην καθημερινή ζωή των ανθρώπων και την παγκόσμια οικονομία. Γενικά, οι στατιστικές έχουν δείξει μεγάλη αξία της τουριστικής βιομηχανίας. Παρά τη μεγάλη σημασία, η παραδοσιακή τουριστική βιομηχανία αντιμετωπίζει σοβαρές προκλήσεις στην ανάπτυξη. Οι τουριστικές διαδρομές των επισκεπτών καθορίζονται πάντα παθητικά, το οποίο οδηγεί σε ελλιπή ανακάλυψη των αξιοθέατων. Συγκεκριμένα, μερικά μεγάλα πάρκα ψυχαγωγίας αποτελούνται από μια σειρά από εκδηλώσεις. Είναι δύσκολο να παρακινηθούν οι τουρίστες να συμμετάσχουν σε όλες τις εκδηλώσεις. Επίσης, δεν αποτελεί κίνητρο για τους τουρίστες να επισκέπτονται συνεχώς τα αξιοθέατα και γενικά είναι δύσκολο να προωθηθούν οι εκδηλώσεις. Κατά την πανδημία του *COVID-19*, οι προκλήσεις στον κλάδο του τουρισμού γίνονται περισσότερο αυστηρές. Συνεπώς, η παραδοσιακή τουριστική βιομηχανία πρέπει να αναμορφωθεί επειγόντως.

Το διαδίκτυο των πραγμάτων (*IoT*) και τα μεγάλα αναλυτικά δεδομένα μπορούν να χρησιμοποιηθούν για τη βελτίωση των εμπειριών των τουριστών κατά τη διάρκεια των περιηγήσεων στα αξιοθέατα, ωστόσο, δεν μπορούν να παρακινήσουν ούτως ώστε οι τουρίστες να είναι τακτικοί πελάτες ή να δοκιμάζουν νέες εκδηλώσεις. Από την προοπτική του έξυπνου τουρισμού, το *blockchain* είναι πιθανό να λειτουργήσει ως πλατφόρμα για τη σύνδεση των τουριστών και των αξιοθέατων με αξιόπιστο τρόπο. Το *blockchain* είναι μια πολλά υποσχόμενη συμπληρωματική λύση για παροχή κινήτρων στους τουρίστες. [21]

2.3 ΚΥΒΕΡΝΗΣΗ

Η τεχνολογία *Blockchain* μπορεί να χρησιμοποιηθεί για οποιαδήποτε συναλλαγή ή ανταλλαγή πληροφοριών που πραγματοποιείται και στην οποία εμπλέκεται η κυβέρνηση. Τα θεμελιώδη χαρακτηριστικά αυτής της τεχνολογίας καθιστούν δυνατή την εφαρμογή σε ένα ευρύ φάσμα διαδικασιών για μητρώο περιουσιακών στοιχείων, απογραφή και ανταλλαγή πληροφοριών, φυσική ιδιοκτησία και άυλα περιουσιακά στοιχεία όπως ψήφοι, διπλώματα ευρεσιτεχνίας, ιδέες, φήμη, πρόθεση, δεδομένα υγείας, πληροφορίες κ.λπ.

Κυβερνήσεις από όλο τον κόσμο διεξάγουν πιλοτικά *project* χρησιμοποιώντας το *blockchain*. Οι κυβερνητικές εφαρμογές του *blockchain* έχουν διαφορετικό χαρακτήρα και περιλαμβάνουν ψηφιακή ταυτότητα, αποθήκευση δικαστικών αποφάσεων, χρηματοδότηση σχολικών κτιρίων και ανίχνευση χρημάτων, οικογενειακή κατάσταση, ηλεκτρονική

[20] (Hussien, Yasin, Udzir, κ.α. 2021)

[21] (Luo, Zhou 2021)

ψηφοφορία, επιχειρηματικές άδειες, διαβατήρια, ποινικά αρχεία ακόμη και φορολογικά αρχεία.[22]

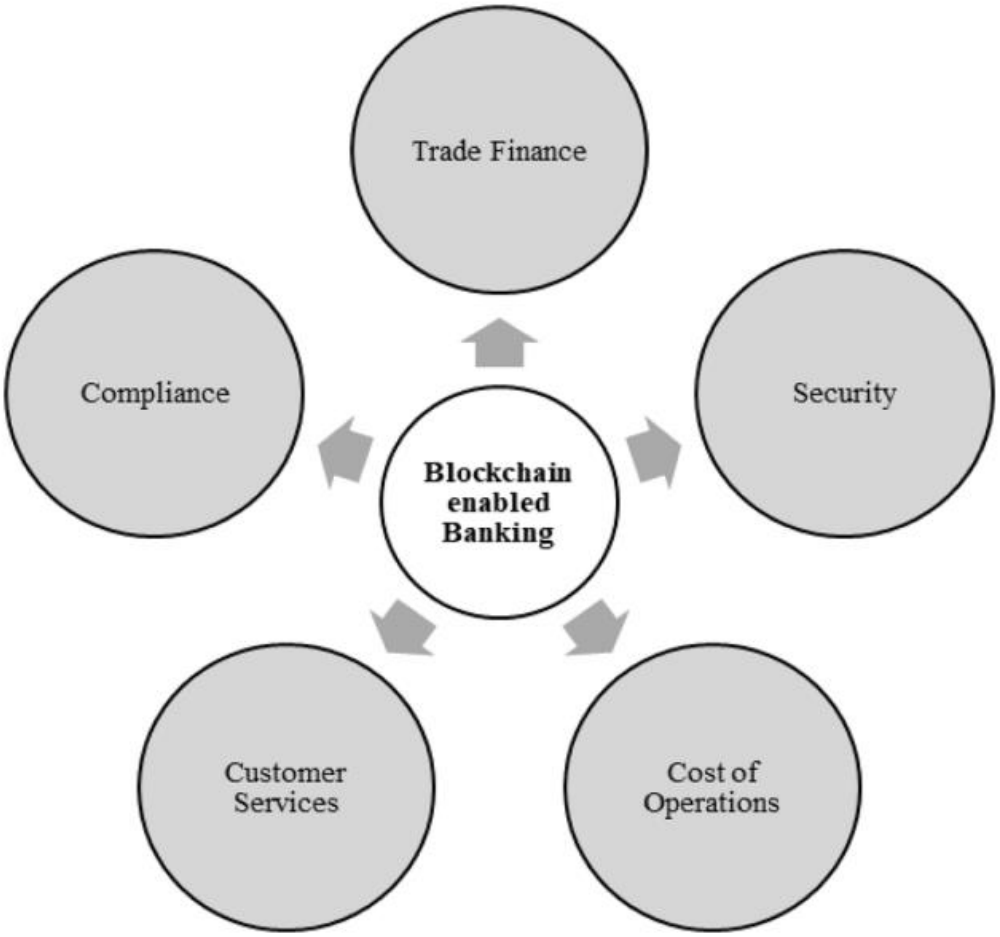
2.4 ΤΡΑΠΕΖΙΚΟΣ ΤΟΜΕΑΣ

Το *Blockchain* είναι μια αναδυόμενη τεχνολογία με τεράστιες δυνατότητες εφαρμογής. Αναφορικά με τον τραπεζικό τομέα και το παγκόσμιο οικονομικό οικοσύστημα, το *blockchain* μπορεί να αντιμετωπιστεί ως υπόσχεση ασφάλειας, εμπιστοσύνης, σταθερότητας, διαφάνειας, μείωσης κόστους και αποτελεσματικότητας.

Η εφαρμογή της τεχνολογίας *blockchain* στον τραπεζικό τομέα είναι απαραίτητη για τη χρηματοδότηση συναλλαγών ή πιστώσεων, την κλασματική συναλλαγή περιουσιακών στοιχείων, τον αυτοματισμό διαδικασίας και τις διατραπεζικές ή διασυνοριακές πληρωμές. Οι τράπεζες βλέπουν στην τεχνολογία *blockchain* μια λύση πολλών οργανωτικών θεμάτων όπως: χειρωνακτική εργασία, πολυπλοκότητα διαδικασιών, ασαφείς διαδικασίες.

Οι τράπεζες εφαρμόζουν κυρίως την τεχνολογία *blockchain* για μεταφορά χρημάτων, εγγραφές και συντήρηση βοηθητικών προγραμμάτων. Αυτή η τεχνολογία λειτουργεί σαν κατανεμημένο καθολικό και είναι εντελώς ανοιχτή σε όλους. Μόλις τα δεδομένα καταχωρηθούν στο *blockchain*, είναι πολύ δύσκολο να τροποποιηθούν καθιστώντας το *blockchain* ασφαλές. Διαφορετικές τράπεζες έχουν διαφορετικές προσεγγίσεις για να πειραματιστούν και να υιοθετήσουν αυτήν την τεχνολογία. Ορισμένες τράπεζες διερευνούν πρώτα τις εσωτερικές επιλογές, ενώ άλλες προσπαθούν να χρησιμοποιήσουν την τεχνολογία για να διερευνήσουν πρώτα τις επιλογές μεταξύ των τραπεζών. [23] [24] [25]

[22] (Ølnes, Ubacht, Janssen, 2017)
[23] (Jajuga, Locarek-Junge, Orlowski, κ.α. 2021)
[24] (Guo, Liang, 2016)
[25] (Garg P., Gupta B., Chauhan A., κ.α. 2021).



Πηγή: https://www.sciencedirect.com/science/article/abs/pii/S0040162520312336.

2.5 MARKETING – ΨΥΧΑΓΩΓΙΑ

Η βιομηχανία μέσων και ψυχαγωγίας βασίζεται κυρίως στη σχέση, που σημαίνει ότι οι δημιουργοί συχνά τίθενται σε μειονεκτική θέση από μεσάζοντες περιθώρια και κρυφά κέρδη. Με τη βοήθεια της τεχνολογίας *blockchain*, η βιομηχανία θα μπορούσε δυνητικά να εξαλείψει την απάτη, να μειώσει σημαντικά το κόστος και να αυξήσει τη διαφάνεια. Ένα από τα μεγαλύτερα ζητήματα στην ψυχαγωγία είναι η ιδιοκτησία και τα δικαιώματα διαχείρισης του περιεχομένου. Το *Blockchain* υπόσχεται έναν τρόπο αποτελεσματικής παρακολούθησης *IP* σε πολλά κανάλια. Χρησιμοποιώντας αυτήν τη νέα τεχνολογία, τα δικαιώματα πνευματικής ιδιοκτησίας μπορούν να παρακολουθούνται σωστά, και οι εταιρείες διαχείρισης ψηφιακών δικαιωμάτων μπορούν να έχουν πρόσβαση στο πλήρες αρχείο των συναλλαγών που πραγματοποιήθηκαν.

Επίσης, σήμερα όλες οι πλατφόρμες όπως *Youtube, Spotify, Netflix* κ.α. λειτουργούν ως διανεμητές της μουσικής και των βίντεο. Αυτό το μοντέλο έχει οδηγήσει σε διαμάχες αναφορικά με τις πληρωμές μεταξύ των καλλιτεχνών. Η τεχνολογία *blockchain* έρχεται στο να δώσει λύση σε αυτά τα προβλήματα αφού θα μπορούν να εκτελούνται πληρωμές απευθείας στους καλλιτέχνες.

2.6 ΑΣΦΑΛΕΙΑ

Ο ασφαλιστικός τομέας περιλαμβάνει εταιρείες που προσφέρουν διαχείριση κινδύνων στους ασφαλισμένους. Η βασική ιδέα είναι ότι ένα μέρος, ο ασφαλιστής, εγγυάται προστασία από τυχόν ατυχή μελλοντικά γεγονότα, ενώ το άλλο μέρος, ο αντισυμβαλλόμενος, πληρώνει ένα μικρό ποσό ως ένα ασφάλιστρο σε αντάλλαγμα για την προστασία από κινδύνους. Ως κλάδος, ο ασφαλιστικός τομέας θεωρήθηκε αργά-αναπτυσσόμενος και ασφαλής για επενδυτές. Οι πιο συνηθισμένοι τύποι ασφαλιστηρίων προσωπικής ασφάλισης είναι η υγεία, το αυτοκίνητο και η ζωή. Ασφαλιστικές εταιρείες ατυχήματος και υγείας παρέχουν προστασία από τυχόν γεγονότα φυσικής σωματικής ασθένειας ή τυχαίων τραυματισμών. Οι ασφαλιστές ζωής ασφαλίζουν τον αντισυμβαλλόμενο έναντι της περίπτωσης θανάτου τους και παρέχουν εφάπαξ ποσό στους δικαιούχους τους.

Παραδοσιακά, ο ασφαλιστικός κλάδος ήταν αργός στην προσαρμογή των νέων τεχνολογιών στον τομέα του. Αλλά ο τομέας έχει αρχίσει να διερευνά τις δυνατότητες χρήσης τεχνολογία στην αλυσίδα αξίας της. Οι ασφαλιστικές εταιρείες έχουν αρχίσει να κάνουν ερωτήσεις σχετικά με την πραγματική χρήση περιπτώσεις χρήσης *blockchain* και έξυπνων συμβάσεων στον ασφαλιστικό τομέα, τι είδους αρχιτεκτονική *blockchain* θα ταιριάζει στις ανάγκες του κλάδου και αν η τεχνολογία είναι αρκετά ώριμη για χρήση στον τομέα.

Η αποτροπή δόλιων αξιώσεων εξακολουθεί να είναι η κορυφαία προτεραιότητα για την υιοθέτηση τεχνολογίας στον ασφαλιστικό κλάδο. Ο κύριος στόχος της χρήσης *blockchain* θα είναι έτσι για τον εξορθολογισμό της διαδικασίας διαχείρισης πληρωμών και απαιτήσεων, ελαχιστοποιώντας έτσι τις αξιώσεις απάτης στον κλάδο. Περαιτέρω, η υιοθέτηση του *blockchain* μπορεί να αφαιρέσει τη δυνατότητα οποιονδήποτε ενδιάμεσων φορέων, όπως οι μεσίτες που είναι γενικά το πρόσωπο των ασφαλιστών στους καταναλωτές. Η τεχνολογία όχι μόνο βελτιώνει και βελτιστοποιεί τις υπάρχουσες λειτουργικές διαδικασίες στον ασφαλιστικό κλάδο, αλλά έχει επίσης τη δυνατότητα να μετατρέψει τα υπάρχοντα προϊόντα σε προϊόντα όπως η ομότιμη ασφάλιση. [26]

3. ΕΜΠΟΡΙΚΕΣ ΕΦΑΡΜΟΓΕΣ BLOCKCHAIN

3.1 ΥΓΕΙΑ

3.1.1 ΕΦΑΡΜΟΓΗ *PATIENTORY*

Το οικοσύστημα υγειονομικής περίθαλψης έχει ορισμένα ζητήματα όπως: να καταστήσει σαφή τα συστήματα πληροφοριών για την υγειονομική περίθαλψη των ασθενών, ηλεκτρονικά αρχεία υγείας και κλινικά δεδομένα, αύξηση της αποδοτικότητας και μείωση των δαπανών, βελτίωση της ασφάλειας και πραγματοποίηση αμετάβλητων ιατρικών ελέγχων, κατάργηση διπλών δεδομένων και εξάλειψη εργασιών σε χαρτί. Το *Patientory* δίνει τη δυνατότητα σε ασθενείς να συνδεθούν περισσότερο με τα έγγραφα υγειονομικής περίθαλψης. Ειδικά για όσους πάσχουν από χρόνιες παθήσεις όπως ο διαβήτης, η πρόσβαση σε έγγραφα υγείας θα επιτρέψει στους ασθενείς να διατηρούν αρχεία των δεδομένων υγείας τους και ως εκ τούτου να έχουν μεγαλύτερη ευθύνη, διαθεσιμότητα και έλεγχο της υγείας τους, ακόμη και για εκείνους που έχουν αντιμετωπίσει μόνο μία φορά ένα ιατρικό πρόβλημα όπως η χειρουργική επέμβαση. Το *Patientory* επιτρέπει στους ασθενείς να επικοινωνούν γρήγορα και αβίαστα με τους παρόχους μέσω των προφίλ τους. Επίσης, ιατροί χρησιμοποιούν το *Patientory* για να διατηρούν, να αποθηκεύουν και να στέλνουν εύκολα ασφαλή ιατρικά δεδομένα. Επίσης, επιτρέπει στους ιατρούς να ενταχθούν σε άλλους παρόχους υγειονομικής περίθαλψης στο

[26] (Kar, Navin, 2021)

δίκτυο των ασθενών, επιτρέποντάς τους να απολαύσουν ένα πιο ενοποιημένο δίκτυο και να προσφέρουν το καλύτερο επίπεδο ιατρικής περίθαλψης στους ασθενείς τους. Πολλοί οργανισμοί υγειονομικής περίθαλψης ανησυχούν για τα κενά πληροφοριών. Εφαρμόζοντας την τεχνολογία *blockchain* της *Patientory* για αποθήκευση και αποστολή αρχείων, οι οργανισμοί μπορούν να βασίζονται σε ειδικούς για την ασφάλεια των δεδομένων. Το *Patientory* παρουσίασε μια διανεμημένη εφαρμογή *DApp* στην οποία το *Patientory's DApp* συνέδεσε την τεχνολογία *blockchain*, η οποία είναι μια ανοιχτή και ασφαλής τεχνολογία που διατηρεί αρχεία συναλλαγών σε μπλοκ που είναι ενωμένα και τα αποθηκεύει σε μια κατανεμημένη και κωδικοποιημένη βάση δεδομένων που λειτουργεί ως καθολικό. Οι εφαρμογές *DApp* είναι εφαρμογές που ενώνονται με *blockchains* που δεν δεσμεύονται ή ελέγχονται από μια οντότητα ή σε ένα μόνο μέρος. Αυτό σημαίνει ότι ένας συγκεκριμένος πάροχος υγειονομικής περίθαλψης δεν ελέγχει μόνο τα δεδομένα υγειονομικής περίθαλψης ενός ατόμου, αλλά επιτρέπει επίσης πιο αποτελεσματική, εύχρηστη και ασφαλή ανταλλαγή πληροφοριών υγειονομικής περίθαλψης σε διαφορετικούς παρόχους και πλατφόρμες.

3.1.2 ΕΦΑΡΜΟΓΗ *MEDICALCHAIN*

Οι γιατροί βρίσκονται αντιμέτωποι με ένα μεγάλο όγκο πληροφοριών που είναι αρκετά δύσκολο να αντιμετωπίσουν. Η εταιρεία τεχνολογίας *Medicalchain* χρησιμοποιεί *blockchain* για να δημιουργήσει ένα κεντρικό ηλεκτρονικό αρχείο υγείας και να διατηρήσει μια πραγματική αναφορά των δεδομένων του χρήστη. Αρχικά, η *Medicalchain* αντιμετώπισε περιλήψεις εξόδου από το νοσοκομείο, η οποία περιέχει μια περίληψη της θεραπείας και της ουσιαστικής φροντίδας παρακολούθησης. Τα νοσοκομεία πρέπει να είναι σίγουρα για αυτά τα έγγραφα χωρίς σφάλματα ευθύνης και να τα επεξεργάζονται γρήγορα για να απελευθερώσουν ασθενείς για τον επόμενο που περιμένει στην ουρά. Η *Medicalchain* έχει προσφέρει μια ψηφιοποιημένη λύση που οδηγεί τους γιατρούς μέσω μιας δομημένης διαδικασίας εξόδου που μειώνει τα λάθη και τη διαγραφή και επιταχύνει την εξέταση από τους αρμόδιους.

Αυτό το σύστημα εφαρμόζει μια διπλή δομή *blockchain*, η οποία θα βοηθήσει στην αποτελεσματική αποκεντρωμένη ανταλλαγή πληροφοριών μεταξύ των εταίρων. Το πρώτο ελέγχει τη διαθεσιμότητα εγγράφων υγείας και δημιουργείται χρησιμοποιώντας ύφασμα *Hyperledger*. Το δεύτερο παρέχεται από ένα διακριτικό *ERC20* στο *Ethereum* και τα πλαίσια όλων των εφαρμογών για την πλατφόρμα μας. Το *blockchain Hyperledger*, είναι ένα δίκτυο που βασίζεται σε άδειες και χρειάζεται να εγγραφούν οι συμμετέχοντες για να το χρησιμοποιήσουν. Αυτό το *blockchain* χρησιμοποιεί μοντέλα *Hyperledger* και γλώσσες ελέγχου πρόσβασης για τον έλεγχο της άδειας σε ένα δίκτυο. Το *Hyperledger Fabric*, ως κατανεμημένη πλατφόρμα λογιστικής, βασίζεται σε μια αρθρωτή αρχιτεκτονική με μεγαλύτερη ασφάλεια, ανθεκτικότητα και επεκτασιμότητα. Οι ιατρικές πληροφορίες είναι τόσο σημαντικές τόσο από κοινωνική όσο και από νομική πλευρά, οπότε ένα *blockchain* με άδεια, όπως το *Hyperledger Fabric*, βοηθά στη διατήρηση της απαραίτητης ιδιωτικότητας που απαιτείται για μια τέτοια υπηρεσία. Το *Hyperledger Fabric* διαχειρίζεται την πρόσβαση σε αποδεικτικά στοιχεία υγείας, καθώς έχει πολλαπλά επίπεδα άδειας, σημαίνει ότι ο κάτοχος των δεδομένων μπορεί να αποφασίσει ποια μέρη των δεδομένων τους είναι διαθέσιμα. Το *Medicalchain* χρησιμοποιεί επίσης έξυπνες συμβάσεις για τη δημιουργία ψηφιακών εφαρμογών και υπηρεσιών υγείας. Αυτές οι εφαρμογές και οι υπηρεσίες θα ενσωματωθούν στις πληροφορίες υγείας του χρήστη. Η ομάδα του *Medicalchain* διευκολύνει το οικοσύστημα υγείας να προσφέρει αξία, να μειώσει το κόστος και τελικά να τροποποιήσει τη ζωή των ανθρώπων.

3.1.3 ΕΦΑΡΜΟΓΗ *CORAL HEALTH*

Στο παραδοσιακό σύστημα υγειονομικής περίθαλψης, όλοι οι φορείς όπως οι πάροχοι, τα εργαστήρια, οι πληρωτές, δηλαδή οι ασφαλιστικές εταιρείες και οι εταιρείες φαρμάκων αποθηκεύουν δεδομένα ασθενών σε διάφορες μορφές και ως εκ τούτου, δεν υπάρχει τυποποίηση στη διατήρηση των αρχείων. Η κακή υποδομή ανταλλαγής δεδομένων προκαλεί σύγχυση δεδομένων στα αρχεία υγείας. Πολλά άλλα προβλήματα που αντιμετωπίζει το σημερινό σύστημα υγειονομικής περίθαλψης, όπως η επεξεργασία δεδομένων, η ασυμφωνία των παλαιών βάσεων δεδομένων, τα μειονεκτήματα της ανάλυσης αδόμητων δεδομένων, το απαγορευτικά υψηλό διοικητικό κόστος, η έλλειψη ασφάλειας δεδομένων και οι απρόσβλητες ανησυχίες για την προστασία της ιδιωτικής ζωής μπορούν να αντιμετωπιστούν από τέτοιες τεχνολογίες ως *blockchain*. Η *Coral Health* χρησιμοποιεί τεχνολογία *blockchain* για να διευκολύνει την ανταλλαγή και την εύκολη πρόσβαση στις πληροφορίες των ασθενών σε όλο το σύστημα.

Βελτιώνει την αποτελεσματικότητα στις αλληλεπιδράσεις μεταξύ βασικών παραγόντων στον τομέα της υγειονομικής περίθαλψης, οδηγώντας σε παραγωγική ανταλλαγή δεδομένων, μεγαλύτερη κερδοφορία και βελτιωμένα αποτελέσματα δημόσιας υγείας. Το οικοσύστημα *Coral Health* συνδέει γιατρούς, επιστήμονες, τεχνικούς εργαστηρίου και αρχές δημόσιας υγείας βάζοντας πληροφορίες ασθενών σε τεχνολογία κατανεμημένων βιβλίων που επιτρέπει στους ασθενείς να μοιράζονται εύκολα και με ασφάλεια τα ιατρικά τους αρχεία με παρόχους, εργαστήρια, πληρωτές και άλλους ενδιαφερόμενους, διατηρώντας παράλληλα τον έλεγχο των ιδιωτικών πληροφοριών. Χρησιμοποιεί επίσης το *blockchain* για να επιταχύνει τη διαδικασία φροντίδας, να αυτοματοποιήσει τις διοικητικές διαδικασίες και να χρησιμοποιήσει έξυπνα συμβόλαια μεταξύ ασθενών και εμπειρογνωμόνων υγειονομικής περίθαλψης για να διασφαλίσει ότι τα δεδομένα και οι θεραπείες είναι ακριβείς.

Το οικοσύστημα *Coral Health* έχει επίσης πολλά οφέλη για τις φαρμακευτικές εταιρείες βελτιώνοντας τη διαδικασία μελέτης θεραπείας και μειώνοντας τον διοικητικό φόρτο εργασίας. Η πλατφόρμα του μειώνει το κόστος πρόσληψης κλινικών δοκιμών και επιτρέπει στις φαρμακευτικές εταιρείες να αξιολογήσουν καλύτερα την ασφάλεια και την αποτελεσματικότητα των θεραπειών τους.

Οι φαρμακευτικές εταιρείες μπορούν να αναζητήσουν τα μεταδεδομένα που είναι αποθηκευμένα στο σύστημα *Coral Health* για να επιτύχουν πιθανά μεγέθη δείγματος για τη δοκιμή τους. Μπορούν να ζητήσουν πρόσβαση σε πολλά υποσχόμενα δείγματα αρχείων και να προσελκύσουν ενδιαφερόμενα άτομα να παρακολουθήσουν το επιθυμητό τεστ. Επιπλέον, μπορούν να πραγματοποιήσουν αναδρομική ανάλυση αναζητώντας τα δεδομένα ασθενών που έλαβαν τα φάρμακά τους περισσότερο και να στρατολογήσουν αυτά τα άτομα για να συμμετάσχουν σε μια μελέτη. Οι φαρμακευτικές εταιρείες έχουν πρόσβαση στα πλήρη ιατρικά αρχεία αυτών των συμμετεχόντων ασθενών για να αξιολογήσουν την επιτυχία των θεραπειών τους και να εντοπίσουν υποσχόμενους ασθενείς για διευρυμένες ενδείξεις. Η συμμετοχή στο οικοσύστημα *Coral Health* μειώνει επίσης το διοικητικό κόστος για τις φαρμακευτικές εταιρείες αυτοματοποιώντας τις αναφορές συμμόρφωσης. Μπορούν επίσης να χρησιμοποιήσουν την έξυπνη πλατφόρμα συμβολαίου της *Coral Health* για τη διαχείριση των αναφορών ανεπιθύμητων συμβάντων στην κλινική δοκιμή και να εξοικονομήσουν διοικητικό κόστος που δαπανάται για την αναφορά συμμόρφωσης. Αυτό βελτιώνει την ποιότητα των πληροφοριών και αυξάνει την ασφάλεια των μελλοντικών κλινικών δοκιμών.

3.1.4 ΕΦΑΡΜΟΓΗ *CLINICO*

Το *Clinico* είναι μία εφαρμογή *blockchain* με έδρα τις ΗΠΑ που χρησιμοποιεί τεχνολογία *blockchain* για τη βελτίωση της υγειονομικής περίθαλψης και των φαρμακευτικών

βιομηχανιών, η οποία ενισχύεται από τους ασθενείς και ενεργοποιείται από το *blockchain*. Το *Clinico* είναι ένα προϊόν υγειονομικής περίθαλψης με ψηφιακό σύστημα διαχείρισης αρχείων ασθενών που επέτρεψε στους ασθενείς της κλινικής δοκιμής να μοιραστούν, να διαχειριστούν και να επωφεληθούν από τα δεδομένα των κλινικών δοκιμών τους. Επιτρέπει στους ασθενείς σε κλινικές δοκιμές να εισάγουν τα δεδομένα τους σε μια πλατφόρμα και οι ερευνητές μπορούν να επιτύχουν και να χρησιμοποιήσουν τα δεδομένα με ενημερωμένη συγκατάθεση χρησιμοποιώντας κρυπτογραφημένα συμβόλαια. Στη συνέχεια, οι ασθενείς λαμβάνουν αυτόματες πληρωμές όποτε χρησιμοποιούνται τα δεδομένα τους. Φαρμακευτικές εταιρείες επωφελούνται από τα δεδομένα των κλινικών δοκιμών των ασθενών, αλλά το *Clinico* δίνει στους ασθενείς τον έλεγχο των δεδομένων τους. Κάθε εταιρεία ανταγωνίζεται για το πλεονέκτημα της αγοράς και το όφελος από τα δεδομένα των ασθενών. Έχουν πρόσβαση σε περιορισμένα δεδομένα, γεγονός που καθιστά τις έρευνές τους επαναλαμβανόμενες και δαπανηρές.

3.1.5 ΕΦΑΡΜΟΓΗ *ISOLVE*

Το *iSolve* αναπτύχθηκε για να δημιουργήσει ισχυρότερα δίκτυα χρηστών και να βελτιώσει τα αποτελέσματα και την ασφάλεια των ασθενών. Οι ομάδες του *iSolve* προσπαθούν να λύσουν ένα κοινό πρόβλημα, όπως η συσσώρευση δεδομένων και η έλλειψη δεδομένων σε βιομηχανίες.

Έχουν παράσχει μια πλατφόρμα *Advanced Digital Ledger Technology (ADLT)*, η οποία είναι πρακτική. Αυτή η πλατφόρμα είναι συμπληρωματικά υπάρχοντα συστήματα και μπορεί επίσης να περιέχει νέα τεχνολογία όπως το *Internet of Medical Things (IoMT)* και να βελτιώσει τη μηχανική μάθηση και τα μεγάλα δεδομένα. Αυτή η πλατφόρμα μπορεί να λύσει μια τεράστια ποικιλία προκλήσεων όπως η παγκόσμια αλυσίδα εφοδιασμού, η Ε & Α, οι κλινικές δοκιμές και η μετακίνηση ιατρικών εγγράφων ασθενών. Το *ADLT* χρησιμοποιεί επίσης το *blockchain* ως σύστημα παρακολούθησης, επαλήθευσης και διατήρησης όλων των υλικοτεχνικών κινήσεων φαρμάκων για την ανάπτυξη του κύκλου ζωής της αλυσίδας εφοδιασμού φαρμάκων και φαρμάκων στη βιομηχανία βιοφαρμάκων και υγειονομικής περίθαλψης. Η ακριβής παρακολούθηση είναι τόσο σημαντική για τη διατήρηση των πλαστών και δόλιων φαρμάκων. Το *ADLT* μπορεί να ελέγξει τον κύκλο ζωής από την παραγωγή στη διανομή μέσω *blockchain*, επομένως απλά πράγματα όπως οι ημερομηνίες λήξης μπορούν να αναγνωριστούν με ακρίβεια και μειώνεται η πιθανότητα δόλιας επανεμφάνισης αλλαγής ημερομηνιών. Το *iSolve* μπορεί να αυξήσει τα κεφάλαια και να βελτιώσει την ανάπτυξη φαρμάκων μέσω της *Smart Market*, όπου τα δεδομένα διατηρούνται με ασφάλεια και είναι ανιχνεύσιμα, αμετάβλητα και ορατά ως αγορά για τους επενδυτές και τους παρόχους υπηρεσιών.

Επιπλέον, το *iSolve* διαθέτει μια πλατφόρμα γνωστή ως *BlockRX* που ενσωματώνει τεχνολογία *blockchain* και *ADLT* του *iSolve*. Αυτή η πλατφόρμα έχει αναπτυχθεί για τη βελτίωση των αποτελεσμάτων των ασθενών ενοποιώντας τη διερεύνηση ερευνητών επιστημών της ζωής, εταιρειών *BioPharma*, παραγωγών ιατρικών συσκευών, λιανοπωλητών ιατρικού εξοπλισμού και παρόχων υγειονομικής περίθαλψης. Το οικοσύστημα *BlockRX* για το *BioPharma* δημιουργεί νέες ροές εισοδήματος και διαχειρίζεται το κόστος και επιτρέπει την ασφαλή πρόσβαση στα δεδομένα. Ο στόχος του *BlockRX* είναι η ένωση συστημάτων που δεν συνδέονται ήδη και δεν αποτελούν πηγή δεδομένων που πληροί τις κανονιστικές και εμπορικές απαιτήσεις.

3.1.6 ΕΦΑΡΜΟΓΗ *CURISIUM*

Το *Curisium* είναι μια τεχνολογία και υπηρεσίες υγειονομικής περίθαλψης που ενσωματώνει τη μηχανική της *Silicon Valley* με τη μεγάλη ανάλυση δεδομένων της *Wall Street* για να δημιουργήσει μια πρωτοποριακή πλατφόρμα *blockchain* για τους καταναλωτές, τους φαρμακευτικούς κατασκευαστές και τους παρόχους να προσφέρουν ασφαλή, προσανατολισμένη στον ασθενή, κλιμακούμενη και αποτελεσματική καινοτόμο προσαρμογή συμβάσεων. Το *Curisium* μπορεί να ελέγξει μια μεγάλη ποικιλία δεδομένων με χαμηλό κόστος. Τα κρυπτογραφικά τους συστήματα διασφαλίζουν ότι τα δεδομένα χρησιμοποιούνται μόνο για τους προκαθορισμένους και επιτρεπόμενους σκοπούς τους. Η πλατφόρμα *Curisium* συμμορφώνεται πλήρως με τον Γενικό Κανονισμό Προστασίας Δεδομένων (*GDPR*) και το *blockchain* τους διατηρεί μια αυτοματοποιημένη ακολουθία έρευνας όλων των δραστηριοτήτων. Επιπλέον, το μοντέλο δεδομένων που βασίζεται στην κατάσταση υγείας του *Curisium* επιτρέπει να περιπλέκονται οι συμβάσεις επιπέδου ασθενούς που πρέπει να δημιουργηθούν με έναν σύντομο, ευανάγνωστο και ελεγχόμενο τρόπο. Σε συνδυασμό με ασφαλείς και αξιόπιστες τεχνολογίες υπολογισμού, η πλατφόρμα *Curisium* παρέχει τη βάση στους πληρωτές, τους παρόχους και τις εταιρείες επιστήμης της ζωής για να αυτοματοποιήσουν συμβάσεις με επίκεντρο τον ασθενή, με βάση την αξία και να μειώσουν τα πλαστά φάρμακα και να αυξήσουν τη διαφάνεια σχετικά με το κόστος.

Επιπλέον, το *Curisium* έχει ορισμένα οφέλη στον χρηματοπιστωτικό τομέα για τους χρήστες του. Το σύστημα που βασίζεται στο *blockchain* του *Curisium* παρέχει μια μοναδική πηγή αλήθειας για τη μείωση των αμφισβητούμενων ισχυρισμών για ιατρικές εκπτώσεις. Οποιοσδήποτε ισχυρισμός μπορεί να επιλυθεί γρήγορα και αποτελεσματικά. Καθ 'όλη τη διάρκεια της διαφοράς, η πλατφόρμα δημιουργεί πλήρη προβολή και παρακολούθηση θέσης. Η πλατφόρμα αποτελείται από ποσοτική ανάλυση για να βοηθήσει τους χρήστες να βελτιώσουν τα κλινικά αποτελέσματα μειώνοντας παράλληλα το κόστος. Επιπλέον, οι χρήστες μπορούν να αξιολογήσουν τις αποφάσεις τους σχετικά με το όφελος και την παρακολούθηση της αποτελεσματικότητας αμέσως και να προσομοιώσουν τα σχέδιά τους για να αποκομίσουν κέρδη μέσω της διαχείρισης του κινδύνου τους για κάθε ομάδα φαρμάκων.

Η προοπτική πληρωμών αγνοήθηκε στις παραδοσιακές μεθόδους αντίκτυπου στον προϋπολογισμό και η αξία και η χρησιμότητά τους ήταν περιορισμένες. Η γνώση και η προσοχή στη μοναδική προοπτική του πληρωτή είναι πολύ σημαντικά για να καταστήσουν το οικονομικό μοντέλο για τον πληρωτή. Το *Curisium* αντιμετωπίζει αυτόν τον περιορισμό καθορίζοντας τον κλινικό και οικονομικό αντίκτυπο ενός δεδομένου προϊόντος στα συγκεκριμένα μέλη του πληρωτή. Παρόλο που τα εμπορικά προσβάσιμα σύνολα δεδομένων στον τομέα της υγείας και της φαρμακοβιομηχανίας έχουν κάποια προβλήματα, όπως συχνά ατελή, ασαφή, άκαμπτα και μη επικυρωμένα, το *Curisium* λύνει αυτά τα ζητήματα κάνοντας ακριβή, επικυρωμένα σύνολα δεδομένων που είναι πλήρως προσαρμοσμένα στις απαιτήσεις των χρηστών.

3.1.7 ΕΦΑΡΜΟΓΗ *CHRONICLED*

Ένα άτομο μπορεί να επιστρέψει πλαστά φάρμακα που μεταπωλούνται ακούσια από τον κατασκευαστή ή τον χονδρέμπορο. Επομένως, όλα τα προϊόντα πρέπει να έχουν σειριακό αριθμό για να επαληθευτούν ως αυθεντικά κατά την επιστροφή τους.

Η *Chronicled*, μια *start-up* εταιρία *blockchain* με έδρα το Σαν Φρανσίσκο είναι μια εταιρία τεχνολογίας λογισμικού που αξιοποιεί το *blockchain* για να κάνει μια αλυσίδα εφοδιασμού

πιο αξιόπιστη, αποδοτική και αυτόματη. Παρέχει εργαλεία και πρωτόκολλα για πολυκομματικά οικοσυστήματα εφοδιαστικής αλυσίδας που χρησιμοποιούν αποκεντρωμένα δίκτυα *blockchain*. Αυτό το αποκεντρωμένο δίκτυο ανέπτυξε τα όρια εμπιστοσύνης και επιβάλλει τους εμπορικούς κανόνες μεταξύ του οργανισμού διατηρώντας ιδιωτικά δεδομένα. Η εταιρεία δραστηριοποιείται επίσης στην αλυσίδα εφοδιασμού της φαρμακευτικής βιομηχανίας. Τα πρωτόκολλα απορρήτου και ασφάλειας αυτού του δικτύου βοηθούν τις φαρμακευτικές επιχειρήσεις να προστατεύσουν και να αυτοματοποιήσουν τις αλυσίδες εφοδιασμού τους, να απλοποιήσουν τις επιχειρηματικές διαδικασίες και να μειώσουν το λειτουργικό κόστος

Το 2017, η *Chronicled* δημιούργησε το *Mediledger Project*, το οποίο είναι ένα καθολικό σύστημα που αποδίδεται στην ασφάλεια, την ιδιωτικότητα και την αποτελεσματικότητα των αλυσίδων εφοδιασμού φαρμάκων. Το *MediLedger* είναι μια κοινοπραξία ηγετών από 25 φαρμακευτικές εταιρείες που ξεκίνησαν το πρωτόκολλο συμμόρφωσης που βασίζεται σε *blockchain*.

Το *Chronicled* χρησιμοποιεί έναν ελαφρύτερο και ταχύτερο αλγόριθμο συναίνεσης σε σύγκριση με τη δημόσια ρύθμιση *Ethereum*.

Η *MediLedger* σκοπεύει να είναι η κοινοπραξία του κλάδου για την αντιμετώπιση της σειριοποίησης και άλλων εμπορικών προβλημάτων των αλυσίδων εφοδιασμού. Το *Blockchain* είναι ένα καλό εργαλείο για τη φαρμακευτική σειριοποίηση και τον εντοπισμό λόγω της ικανότητάς του να είναι η ίδια πηγή για την ασφαλή ανταλλαγή πληροφοριών μεταξύ πολλών μερών. Η αποκεντρωμένη λειτουργία του *blockchain* του *MediLedger* κάνει τα δεδομένα να αποθηκεύονται σε πολλούς ξεχωριστούς διακομιστές και καθιστά τόσο δύσκολο το χειρισμό δεδομένων. Ακόμα κι αν ένας διακομιστής παραβιαστεί, είναι τόσο δύσκολο να χειριστείτε τα δεδομένα άλλων διακομιστών. Οι πάροχοι φαρμακευτικών υπηρεσιών και ακόμη και μεμονωμένες εταιρείες μπορούν να χρησιμοποιήσουν τη λύση του *MediLedger* για τα προϊόντα τους.

3.1.8 ΕΦΑΡΜΟΓΗ *COVID-19*

Επί του παρόντος, η ανθρωπότητα είναι μάρτυρας αυξανόμενων και ολοένα και πιο σύνθετων αλλαγών στον κόσμο. Η έγκαιρη και αποτελεσματική απάντηση σε αυτές τις αλλαγές αποτελεί ουσιαστική πρόκληση για τις κυβερνήσεις και τα έθνη σε όλο τον κόσμο. Το ξέσπασμα του *COVID-19* είναι μία από αυτές τις προκλήσεις του 21ου αιώνα που έθεσε την κινητικότητα και την ικανότητα των κρατών του συστήματος υγείας σε μια μεγάλη δοκιμασία. Η επίδραση της πανδημίας του *COVID-19* και οι συνέπειές της αντικατοπτρίζονται σε κάθε γωνιά της καθημερινής μας ζωής, στις επιχειρήσεις, στην παγκόσμια οικονομία, στις κινήσεις των ανθρώπων και εντελώς στον τρόπο αλληλεπίδρασης μεταξύ τους και του κόσμου. Διαφορετικά εμβόλια έχουν εγκριθεί κατά του κορονοϊού, ενώ το καθένα έχει συγκεκριμένη κατάσταση της αλυσίδας εφοδιασμού. Στην πραγματικότητα, η διαχείριση της ψυχρής αλυσίδας περιλαμβάνει τη διασφάλιση ότι τα εξαιρετικά ευαίσθητα στη θερμοκρασία εμβόλια κορωνοϊού διατηρούνται στη σωστή θερμοκρασία κατά τη διαδικασία παραγωγής, αποθήκευσης, μεταφοράς και διανομής. Η διαχείριση ψυχρής αλυσίδας εμβολίων θα απαιτήσει διαφορετικούς βαθμούς συνεργασίας μεταξύ διαφόρων ενδιαφερομένων.

Διάφορες τεχνολογίες στις επιστήμες των υπολογιστών, όπως η Τεχνητή Νοημοσύνη, η Εικονική και η Επαυξημένη Πραγματικότητα, το *IoT*, οι ιχνηλάτες υγειονομικής περίθαλψης και οι αισθητήρες έχουν χρησιμοποιηθεί για τη θεραπεία της νόσου όπως το *AIDS*, ο *EBOLA*

κ.λπ. Όπως και στην περίπτωση του κορωνοϊού, η ανάγκη για ένα σύστημα που μπορεί να διασφαλίσει αξιόπιστη και ασφαλή μεταφορά κλινικών πληροφοριών μαζί με τα μέρη που δεν ελέγχονται από μια κεντρική αρχή ή μια κυβέρνηση. Στην πραγματικότητα, είναι αναπόφευκτο για τις χώρες να μοιραστούν τις εμπειρίες τους για τη σωστή διαχείριση της εξάπλωσης του ιού *COVID-19*. Η τεχνολογία *Blockchain* μπορεί να διασφαλίσει την παραβίαση της ανταλλαγής πληροφοριών λόγω των μοναδικών χαρακτηριστικών της όσον αφορά την ανταλλαγή πληροφοριών, όπως αξιοπιστία, ασφάλεια, ανωνυμία και αποκεντρωμένη προσέγγιση. Με την επέκταση του Διαδικτύου των Ιατρικών Πραγμάτων (*IoMT*) που περιλαμβάνει βιοαισθητήρες, ιατρικές συσκευές και τεχνολογίες επικοινωνίας, τα συστήματα υγειονομικής περίθαλψης θα ενδυναμώσουν σημαντικά στην πρόληψη και καταπολέμηση του *COVID-19*. Ωστόσο, αυτά τα συστήματα υποφέρουν από ζητήματα ασφάλειας και ιδιωτικότητας που η τεχνολογία *blockchain* τους δίνει τη δυνατότητα να αντιμετωπίσουν αυτά τα προβλήματα. Επιπλέον, το *IoMT* με δυνατότητα *blockchain* παρέχει αποτελεσματικές λύσεις σε θέματα όπως ο εντοπισμός της πανδημικής προέλευσης, η καραντίνα και η κοινωνική απόσταση, έξυπνα νοσοκομεία, προέλευση ιατρικών δεδομένων, απομακρυσμένη υγειονομική περίθαλψη και τηλεϊατρική.

Επιπλέον, η τεχνολογία κατανεμημένου καθολικού *blockchain* μπορεί να χρησιμοποιηθεί για να αυξήσει την ολοκλήρωση μεταξύ οντοτήτων με ασφαλή τρόπο. Τρεις επισημασμένες δυνατότητες μπορεί να παρέχονται με τη χρήση συναλλαγών *blockchain* σε οντότητες:

1) Η αμετάβλητη ως πληροφορία σχετικά με την υγεία που αποθηκεύεται στο καθολικό του *blockchain* δεν μπορεί να αλλάξει καθώς θα καταχωρηθεί με τις νέες τιμές κατακερματισμού

2) Οι συναλλαγές μπορούν να τροποποιηθούν από τους περισσότερους κόμβους σε ένα αποκεντρωμένο δίκτυο και

3) Η ανάλυση των συναλλαγών καθολικού προκαλεί ιχνηλασιμότητα

Επιπλέον, τα έξυπνα συμβόλαια μπορούν να γίνουν με βάση το *blockchain* και να επιτρέπουν αυτοματοποιημένες συμβατικές συμφωνίες μέσω ορισμένων προκαθορισμένων χαρακτηριστικών. Συνοψίζοντας, τα οφέλη της χρήσης *blockchain* στην ιχνηλασιμότητα, το διαβατήριο ασυλίας και η αναγνώριση του *COVID-19* και άλλα σενάρια υγείας βοηθούν στην καταπολέμηση της πανδημίας. [27]

3.2 ΤΟΥΡΙΣΜΟΣ

3.2.1 ΕΦΑΡΜΟΓΗ *LOCKTRIP*

Το *LockTrip* είναι ένα πολύπλευρο έργο που αποτελείται από τρία στοιχεία. Το πρώτο είναι η αγορά ταξιδίων, που φιλοξενείται στο *LockTrip.com*. Επιτρέπει στους πελάτες να κάνουν κράτηση ξενοδοχείων και ενοικιάσεις διακοπών κατά μέσο όρο 20% φθηνότερα από τους κορυφαίους ανταγωνιστές όπως *Booking.com, Expedia* και *Airbnb*. Διατίθενται επίσης πτήσεις, με τιμή περίπου 5% φθηνότερα από τον ανταγωνισμό.

3.2.2 ΕΦΑΡΜΟΓΗ *SMARTTRIP*

Η έξυπνη πλατφόρμα ταξιδιού (*STP*) είναι ένα αποκεντρωμένο οικοσύστημα που θα συνδέει ταξιδιώτες και παρόχους υπηρεσιών, συνδυάζοντας όλες τις λειτουργίες που απαιτούνται για ασφαλή, άνετα και αυθεντικά ταξίδια - αναψυχής ή επιχείρησης. Είναι ένα ολοκαίνουργιο μοντέλο ταξιδιού - ελαχιστοποιώντας τον χρόνο που αφιερώνεται στην έρευνα και μεγιστοποιώντας την αυθεντικότητα της εμπειρίας.

[27] (Mojtaba, Bamakan, Moghaddam, κ.α. 2021)

Η πλατφόρμα *Smart Trip* θα προσφέρει:

Μεγάλες τιμές για ταξιδιωτικές υπηρεσίες.

Εργαλείο σχεδιασμού ταξιδιού Α έως Ω

Μια δυναμική κοινότητα ταξιδιωτών και επαγγελματιών της τουριστικής βιομηχανίας

Η έξυπνη πλατφόρμα ταξιδιού θα προσφέρει ένα εξαιρετικά ευρύ φάσμα υπηρεσιών: από τις πωλήσεις αεροπορικών εισιτηρίων έως την κράτηση πεζοπορίας στη ζούγκλα, από λεπτομερείς πληροφορίες για τα αξιοθέατα της περιοχής μέχρι την εξεύρεση ταξιδιωτικών συντρόφων. [28]

3.3.3 ΕΦΑΡΜΟΓΗ *GOUREKA*

Η *GOeureka*, μια ταξιδιωτική τεχνολογική εταιρεία που χρησιμοποιεί τεχνολογία *blockchain* για να δημιουργήσει μια πλατφόρμα κρατήσεων ξενοδοχείων, δήλωσε ότι κυκλοφόρησε την άλφα έκδοση της πλατφόρμας της, επιτρέποντας στους καταναλωτές να κάνουν κράτηση σε δωμάτια ξενοδοχείων με μηδενική προμήθεια, να λαμβάνουν ανταμοιβές και οφέλη πίστης, όλα χωρίς κρυφές χρεώσεις. Η *GOeureka* είναι από τις πρώτες σε αυτόν τον χώρο που δοκιμάζει κρατήσεις χρησιμοποιώντας τεχνολογία *blockchain* μέσω έξυπνων συμβάσεων στο *Ethereum*, κάτι που καθίσταται εφικτό, εν μέρει, λόγω της τεράστιας υπάρχουσας υποδομής των διαθέσιμων ξενοδοχείων. Η *GOeureka* συγκέντρωσε ένα εντυπωσιακό Διοικητικό Συμβούλιο αποτελούμενο από στελέχη του *C-Level* από τα *Accor Hotels* και *Agoda*, μεταξύ άλλων στην παγκόσμια ξενοδοχειακή βιομηχανία. Ο αριθμός των ξενοδοχείων με δυνατότητα κράτησης μέσω του *GOeureka* (400.000) επεκτείνεται ραγδαία, δίνοντάς του ένα σημαντικό πλεονέκτημα έναντι των ανταγωνιστών, τόσο εντός όσο και εκτός του κόσμου του *blockchain*.

Επί του παρόντος, μια σειρά ιστότοπων κρατήσεων κυριαρχούν στον χώρο κρατήσεων του ξενοδοχείου, χρεώνοντας οτιδήποτε μεταξύ 10 - 30% προμήθεια πάνω από την τιμή του δωματίου. Αυτή η χρέωση πραγματοποιείται στο πίσω μέρος του ιστότοπου κράτησης, με μικρή διαφάνεια κόστους για τον καταναλωτή. Η λιανική τιμή για ένα μονό δωμάτιο ποικίλλει σημαντικά, ανάλογα με τις συναλλαγές μεταξύ του ξενοδοχείου, του χονδρέμπορου της τράπεζας κρεβατιών και του ιστότοπου *online* κρατήσεων.

Η *GOeureka* απλοποιεί και μειώνει το κόστος των κρατήσεων ξενοδοχείων, δίνοντας μια δίκαιη και συνεπή τιμή στον πελάτη και ευκολία συναλλαγής στο ξενοδοχείο. Διακόπτοντας τους μεσάζοντες και επιτρέποντας στο ξενοδοχείο να αντιμετωπίσει απευθείας τον πελάτη, τα αυθαίρετα τέλη διαγράφονται και ο πελάτης συγκεντρώνει το όφελος και τις ανταμοιβές καθώς και λαμβάνει πολύ καλύτερες τιμές. Ομοίως, τα ξενοδοχεία είναι σε θέση να μειώσουν την αλυσίδα εφοδιασμού στο ελάχιστο, καθιστώντας την πιο αποτελεσματική και φθηνότερη για τη λειτουργία τους.

3.3 ΚΥΒΕΡΝΗΣΗ

3.3.1 ΕΦΑΡΜΟΓΗ *FOLLOW MY VOTE*

Μια άλλη εφαρμογή για τεχνολογία *blockchain* είναι η ψηφοφορία. Με την ψήφο ως συναλλαγή, μπορούμε να δημιουργήσουμε ένα *blockchain* το οποίο παρακολουθεί τις μετρήσεις των ψήφων. Με αυτόν τον τρόπο, όλοι μπορούν να συμφωνήσουν στην τελική καταμέτρηση επειδή μπορούν να μετρήσουν οι ίδιοι τις ψήφους και λόγω της διαδρομής

[28] (Ozdemir, Ar, Erol, 2020)

ελέγχου *blockchain*, μπορούν να επαληθεύσουν ότι καμία ψήφος δεν άλλαξε ή αφαιρέθηκε και δεν προστέθηκαν παράνομες ψήφοι.

3.4 ΤΡΑΠΕΖΙΚΟΣ ΤΟΜΕΑΣ

3.4.1 ΕΦΑΡΜΟΓΗ *RIPPLE*

Το *Ripple*, ή το *XRP*, είναι ένα κρυπτονόμισμα και μια πλατφόρμα. Τεχνικά, το *Ripple* είναι το όνομα της εταιρείας και του δικτύου και το *XRP* είναι το κρυπτονόμισμα. Η πλατφόρμα *Ripple* είναι ένα πρωτόκολλο ανοιχτού κώδικα που έχει σχεδιαστεί για να επιτρέπει γρήγορες και φθηνές ψηφιακές συναλλαγές. Η πλατφόρμα *Ripple* επιτρέπει γρήγορες και φθηνές ψηφιακές συναλλαγές.

3.5 MARKETING – ΨΥΧΑΓΩΓΙΑ

3.5.1 ΕΦΑΡΜΟΓΗ *MEDIACHAIN*

Χρησιμοποιεί έξυπνα συμβόλαια ούτως ώστε οι μουσικοί να πάρουν τα χρήματα που αξίζουν. Συνάπτοντας μια αποκεντρωμένη, διαφανή σύμβαση, οι καλλιτέχνες μπορούν να συμφωνήσουν σε υψηλότερα δικαιώματα και να πληρώνονται πραγματικά πλήρως και εγκαίρως. Η εταιρεία *Spotify* έχει αποκτήσει την *Mediachain*.

3.5.2 ΕΦΑΡΜΟΓΗ *UJO*

Η αποκεντρωμένη πλατφόρμα του *Ujo* δημιουργεί μια βάση δεδομένων με δικαιώματα ιδιοκτησίας μουσικής και αυτοματοποιεί τις πληρωμές δικαιωμάτων. Το *Ujo* διαθέτει μια πλατφόρμα που βασίζεται σε *blockchain*, όπου οι καλλιτέχνες μπορούν να ανεβάζουν πρωτότυπα έργα, να δημοσιοποιούν έργα τους, να ελέγχουν τις επιλογές αδειοδότησης και να διαχειρίζονται τις διανομές των έργων. Η πλατφόρμα *Ethereum* εξαλείφει τη σύγχυση της ιδιοκτησίας μουσικής και πληρώνει καλλιτέχνες χρησιμοποιώντας έξυπνα συμβόλαια και κρυπτονομίσματα.

3.5.3 ΕΦΑΡΜΟΓΗ *CHOON*

Το *Choon* είναι μια πλατφόρμα ροής μουσικής και ψηφιακών πληρωμών που χρησιμοποιεί *blockchain* για να πληρώνει τους καλλιτέχνες εγκαίρως.

Η πλατφόρμα του *Choon Ethereum* επιτρέπει στους καλλιτέχνες να συνάψουν έξυπνες συμβάσεις με κάθε συντελεστή τραγουδιού, εξασφαλίζοντας ένα καθορισμένο μέρος των συνολικών εσόδων (80%). Αντί να περιμένει έναν χρόνο για να πληρώσει καλλιτέχνες, όπως συνηθίζεται, η πλατφόρμα *Choon* μπορεί να τους ανταμείψει σχεδόν αμέσως με βάση τον αριθμό των ροών που ηχογραφήθηκαν για οποιαδήποτε ημέρα.

3.6 ΑΣΦΑΛΕΙΑ

3.6.1 ΕΦΑΡΜΟΓΗ *ETHERISC*

Το *Etherisc* είναι μια πλατφόρμα ανάπτυξης ανοιχτού κώδικα που επικεντρώνεται σε αποκεντρωμένες ασφαλιστικές εφαρμογές.

Το *Etherisc* δημιουργεί αποκεντρωμένες εφαρμογές με επίκεντρο το *blockchain* για διαφορετικούς τομείς του ασφαλιστικού κλάδου. Η εταιρεία επικεντρώνεται στη χρήση της τεχνολογίας καθολικού για να μειώσει τις ανεπάρκειες, συγκεκριμένα τα υψηλά τέλη επεξεργασίας και τους εκτεταμένους χρόνους διεκπεραίωσης των απαιτήσεων.

Η *Etherisc* έχει ήδη αναπτύξει έξι διαφορετικές αποκεντρωμένες εφαρμογές που σχετίζονται με την ασφάλιση. Ένα από αυτά είναι μια εφαρμογή ασφάλισης καλλιεργειών με την οποία οι

αγρότες προσδιορίζουν τη γη και τις καλλιέργειές τους καθώς και τυχόν απώλειες λόγω καιρού. Μια άλλη εφαρμογή ασφαλίζει τα μέλη της *Etherisc* για πιθανές παραβιάσεις κρυπτογραφικών πορτοφολιών.

3.6.2 ΕΦΑΡΜΟΓΗ *BEENEST*

Το *Beenest* είναι μια αποκεντρωμένη πλατφόρμα κοινής χρήσης σπιτιού για λάτρεις της κρυπτογράφησης. Παρόμοια με το *AirBnb*, οι χρήστες του *Beenest* μπορούν να κάνουν κράτηση για σπίτια χρησιμοποιώντας το *Bee Token* της εταιρείας.

Ασφαλιστική εφαρμογή *Blockchain*: Η εταιρεία συνεργάζεται με την *WeTrust* για την ανάπτυξη ασφαλιστικής ασφάλισης με βάση το *blockchain* για τους ιδιοκτήτες σπιτιού *Beesnest*.

Υπόθεση χρήσης σε πραγματικό χρόνο: Ξεκινώντας από τα τέλη του 2017, η *Beenest* βρίσκεται ακόμα στα πρώτα στάδια της ασφάλισης ιδιοκτήτη σπιτιού για ζημιές σε περιουσία.

3.6.3 ΕΦΑΡΜΟΓΗ *GUARDTIME*

Το *Guardtime* αναπτύσσει λύσεις *blockchain* σε όλους τους κλάδους της κυβερνοασφάλειας, της κυβέρνησης, της χρηματοδότησης, της άμυνας και της εφοδιαστικής αλυσίδας.

Η *Guardtime* συνεργάστηκε με τον κολοσσό *logistics Maersk* για να εφαρμόσει μια πλατφόρμα θαλάσσιας ασφάλισης με βάση το *blockchain* που θα διαχειρίζεται τον κίνδυνο, θα χρησιμοποιεί έξυπνα συμβόλαια και θα καθιερώνει μια αμετάβλητη αλυσίδα αποστολής για να βοηθήσει τις ασφαλιστικές εταιρείες να παρέχουν πλήρη κάλυψη.

3.6.4 ΕΦΑΡΜΟΓΗ *FIDENTIAX*

Με το *FidentiaX*, οι χρήστες έχουν τη δυνατότητα να αγοράσουν, να πουλήσουν ή να αποθηκεύσουν τα ασφαλιστήρια τους συμβόλαια στο *blockchain* της εταιρείας. Η αγορά που λειτουργεί με *blockchain* λαμβάνει τις υπάρχουσες πολιτικές και τις τοποθετεί στην κρυπτογραφημένη βάση δεδομένων. Σε πραγματικό χρόνο, οι χρήστες μπορούν να εξαργυρώσουν τα συμβόλαιά τους, να αγοράσουν συμβόλαια από άλλους ή να βρουν όλες τις ασφαλιστικές τους πληροφορίες σε ένα μέρος.

Το *FideniaX* δημιούργησε το *ISLEY*, ένα ψηφιακό καθολικό για ασφαλιστήρια συμβόλαια που λειτουργεί με *blockchain*. Η *ISLEY* παρέχει στους πελάτες μια πλήρη επισκόπηση των ασφαλιστηρίων συμβολαίων τους, τους ειδοποιεί όταν λήγουν τα ασφάλιστρα τους και εμφανίζει μια αμετάβλητη καταγραφή ολόκληρου του ιστορικού τους.

3.6.5 ΕΦΑΡΜΟΓΗ *B3I*

Η *Blockchain Insurance Industry Initiative (B3i)* είναι μια ομάδα ασφαλιστών που δημιουργήθηκε για να διερευνήσει τη χρησιμότητα του *blockchain* και της *Distributed Ledger Technology (DLT)* στον ασφαλιστικό κλάδο.

Η αποστολή της εταιρείας είναι να χρησιμοποιήσει το *blockchain* για να βελτιώσει τον τρόπο διαχείρισης των δεδομένων και των πληρωμών, να μειώσει τον κίνδυνο και να κάνει την ασφάλιση πιο προσιτή.

Το πρώτο ολοκληρωμένο προϊόν της *B3i* είναι ένα πρωτότυπο *blockchain* για συμβόλαια αντασφάλισης ακινήτων.

3.6.6 ΕΦΑΡΜΟΓΗ *DYNAMIS*

Η *Dynamis* είναι μια ασφαλιστική εταιρεία peer-to-peer που έχει χτιστεί πλήρως στο *blockchain Ethereum*.

Η *Dynamis* επικεντρώνεται στην ασφάλιση της ανεργίας (ή σε αυτό που αποκαλούν «κοινωνικό κεφάλαιο»). Οι αιτούντες θα πρέπει μόνο να παρέχουν το προφίλ τους στο *LinkedIn* για να επαληθεύσουν την τρέχουσα κατάσταση απασχόλησης. Για όσους είναι άνεργοι, το *blockchain* της εταιρείας θα επαληθεύσει μέσω συνδέσεων προφίλ και θα εκδώσει τις ασφαλιστικές πληρωμές.

Η κοινωνική ασφάλιση κεφαλαίου της εταιρείας συνδυάζει έξυπνα συμβόλαια και κοινωνικό δίκτυο ομότιμων για να επαληθεύσει διπλά την κατάσταση απασχόλησης ενός αιτούντος ασφαλιστηρίου συμβολαίου. Ακόμα στη νεοσύστατη κατάσταση, η *Dynamis* προσπαθεί να κάνει την ασφάλειά της ευρύτερα διαθέσιμη τους επόμενους μήνες.

3.6.7 ΕΦΑΡΜΟΓΗ *LEMONADE*

Η εφαρμογή *Lemonade* συνδυάζει τεχνολογία τεχνητής νοημοσύνης και κατανεμημένο καθολικό για να προσφέρει ασφάλιση σε ενοικιαστές και ιδιοκτήτες σπιτιού, ξεκινώντας από 5 $ και 25 $ μηνιαίως, αντίστοιχα.

Στην *Lemonade*, το *blockchain* μπαίνει στο παιχνίδι μέσω έξυπνων συμβολαίων. Το επιχειρηματικό μοντέλο της εταιρείας παίρνει ένα πάγιο τέλος από κάθε μηνιαία πληρωμή και κατανέμει το υπόλοιπο σε μελλοντικές αξιώσεις. Εάν γίνει αξίωση, τα έξυπνα συμβόλαια του *blockchain* θα προσπαθήσουν αμέσως να επαληθεύσουν την απώλεια, ώστε ένας πελάτης να μπορεί να πληρωθεί γρήγορα.

Εάν εγκριθεί μια αξίωση, ο συνδυασμός τεχνητής νοημοσύνης και *blockchain* της *Lemonade* θα πληρώσει σε τρία δευτερόλεπτα.

3.6.8 ΕΦΑΡΜΟΓΗ *FIZZY*

Η εφαρμογή *Fizzy*, ένα εργαλείο ασφάλισης καθυστέρησης πτήσης, είναι θυγατρική του παγκόσμιου ασφαλιστικού κολοσσού AXA.

Η *Fizzy* χρησιμοποιεί *blockchain* για να διασφαλίσει ότι τα μέλη των οποίων οι πτήσεις καθυστερούν περισσότερο από δύο ώρες αποζημιώνονται αμέσως. Το *blockchain* της εταιρείας συμπληρώνει ταξιδιωτική ασφάλιση που συνήθως δεν καλύπτει οικονομικές ζημίες λόγω καθυστερήσεων πτήσεων.

Το εργαλείο χρησιμοποιεί έξυπνες συμβάσεις για να κλειδώσει όσον αφορά τις πληρωμές και τις πληροφορίες πολιτικής. Οι χρήστες δεν έχουν παρά να καταχωρίσουν τα στοιχεία της πτήσης τους, να εξατομικεύσουν την κάλυψή τους και να πραγματοποιήσουν μια πληρωμή. Στη συνέχεια, η *Fizzy* θα χρησιμοποιήσει το blockchain για να επαληθεύσει αμετάκλητα δεδομένα καθυστέρησης πτήσης και να αποζημιώσει τους πελάτες.

3.6.9 ΕΦΑΡΜΟΓΗ *TEAMBRELLA*

Η *Teambrella* είναι μια ασφαλιστική πλατφόρμα, σύμφωνα με την οποία η ομάδα σας, και όχι μια κεντρική ασφαλιστική εταιρεία, εξασφαλίζει τις απαιτήσεις σας.

Για παράδειγμα, ένα μέλος της *Teambrella* στις ΗΠΑ μπορεί να πει στην ομάδα ότι ο σκύλος του χρειάζεται επείγουσα χειρουργική επέμβαση. Η υπόλοιπη ομάδα θα ψηφίσει εάν θα πληρώσει για την επέμβαση του ζώου και πόσο από το κόστος θα πρέπει να καλύψει.

Η *Teambrella* χρησιμοποιεί *blockchain* και έξυπνα συμβόλαια για την εκτέλεση ασφαλιστικών πληρωμών. Τα μέλη μιας συγκεκριμένης ομάδας *Teambrella* είναι κλειδωμένα σε ένα έξυπνο συμβόλαιο και χρησιμοποιούν αυτές τις συμβάσεις για να ψηφίσουν με διαφάνεια και να εκτελέσουν πληρωμή για κάθε αξίωση.

4. ΚΙΝΔΥΝΟΙ – ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ BLOCKCHAIN

4.1 ΟΡΙΣΜΟΙ ΚΙΝΔΥΝΟΙ – ΑΠΕΙΛΕΣ

4.1.1 *BLOCKCHAIN* ΚΙΝΔΥΝΟΙ

Η αποκέντρωση είναι ακριβή

Οι ενημερώσεις στο *blockchain* που παρακολουθούν την ιδιοκτησία *bitcoin* βασίζονται σε έναν αλγόριθμο που απαιτεί από τους χρήστες να επιλύουν χρονοβόρα και υπολογιστικά ακριβά μαθηματικά προβλήματα-τη λεγόμενη απόδειξη εργασίας-για να κρατήσουν τη διαδικασία ειλικρινή.

Η ποσότητα ηλεκτρικής ενέργειας για να οδηγήσει αυτούς τους υπολογισμούς είναι εξωφρενική, οδηγώντας ορισμένους ανθρακωρύχους να κλέψουν την ενέργεια. Ορισμένα *blockchains* χρησιμοποιούν απλούστερους μηχανισμούς, αλλά εξακολουθούν να προσθέτουν επίπεδα πολυπλοκότητας λογισμικού που είναι δαπανηρά για να αναπτυχθούν και να γίνουν σωστά.

Η αποκέντρωση είναι δύσκολο να διασφαλιστεί

Καθώς το *bitcoin* έγινε πιο πολύτιμο, αρκετοί συνασπισμοί ανέπτυξαν ακριβό προσαρμοσμένο υλικό για να κυριαρχήσουν στην εξόρυξη. Οι λίγες ομάδες με το κεφάλαιο και την τεχνογνωσία είναι οι μόνες που μπορούν να φτιάξουν αυτές τις προσαρμοσμένες μάρκες και όλοι οι άλλοι δεν μπορούν να ανταγωνιστούν στην επίλυση των μαθηματικών παζλ.

Θεωρητικά, ο αλγόριθμος εξακολουθεί να είναι αποκεντρωμένος και ο καθένας μπορεί να προσπαθήσει να ανταγωνιστεί, αλλά στην πράξη μόνο εκείνοι με το σωστό υλικό μπορούν να δικαιολογήσουν το κόστος για να κερδίσουν μια θέση στο εικονικό τραπέζι. Αυτό αφήνει τον έλεγχο στα χέρια λίγων.

Τα ιδιωτικά *blockchains* είναι απλώς βάσεις δεδομένων με κρυπτογραφικές υπογραφές.

Μερικά από τα πιο αποτελεσματικά *blockchains* λέγεται ότι είναι "ιδιωτικά" και αφήνουν τον έλεγχο στα χέρια μερικών κεντρικών ομάδων.

Η ταυτότητα είναι δύσκολα να διαχειρίσιμη

Οι χρήστες ορίζουν την ταυτότητά τους με ένα κρυπτογραφικό κλειδί και πρέπει να κρατήσουν το μέρος τους μυστικό. Εάν κάποιος λάβει ένα αντίγραφο του κλειδιού, μπορεί να πλαστοπροσωπήσει τον αποκαλούμενο κάτοχο, έναν κίνδυνο που έχει οδηγήσει πολλούς χρήστες *bitcoin* να αποθηκεύσουν το *bitcoin* τους σε μονάδες δίσκου αντίχειρα σε παλιομοδίτικα θησαυροφυλάκια.

Η πλαστοπροσωπία, φυσικά, είναι πολύ χειρότερη εάν το *blockchain* παρακολουθεί κάτι αξιόλογο, επειδή οι υποδυόμενοι συνήθως πρόκειται να κλέψουν τα ψηφιακά προϊόντα.

Οι χαμένες ταυτότητες είναι το μεγαλύτερο πρόβλημα

Εάν το κλειδί χαθεί ή καταστραφεί, κάτι που είναι πολύ εύκολο, ο έλεγχος των περιουσιακών στοιχείων στο *blockchain* χάνεται σε όλους για πάντα.

Πολλοί αναρωτιούνται πόσα νομίσματα στο *blockchain* έχουν παγώσει για πάντα, και ελέγχονται από κάποιο κλειδί που δεν δημιουργήθηκε σωστά. Είναι αρκετά κακό όταν μια περιουσία εξαφανίζεται επειδή κάποιος έχασε τον έλεγχο της, αλλά μπορεί να είναι χειρότερο για όλους εάν ορισμένα γενικά περιουσιακά στοιχεία που χρησιμοποιούνται από την κοινωνία παγώσουν εγκαίρως.

Οι τακτικοί μηχανισμοί διαφορών δεν λειτουργούν

Εάν κάποιος χάσει μια δίκη, το δικαστήριο μπορεί να διατάξει τις τράπεζες να μεταφέρουν χρήματα σε αυτόν που κέρδισε την υπόθεση. Αλλά εάν ένας κάτοχος ενός περιουσιακού στοιχείου στο *blockchain* δεν θέλει να χρησιμοποιήσει το κλειδί για να αποσυνδεθεί από τη συναλλαγή, δεν μπορεί κανείς να κάνει τίποτα.[29]

4.1.2 ΑΠΕΙΛΕΣ BLOCKCHAIN

4.1.2.1 ΑΠΕΙΛΕΣ BLOCKCHAIN ΣΤΗΝ ΥΓΕΙΑ

Τεχνικές – Τεχνολογικές Απειλές

Το θέμα της επεκτασιμότητας της τεχνολογίας *blockchain* σχετίζεται με το περιορισμένο ποσοστό επεξεργασίας συναλλαγών που εκτελούνται ανά δευτερόλεπτο στο δίκτυο. Η επεκτασιμότητα και ο περιορισμός αποδόθηκε στην αντιστάθμιση μεταξύ του όγκου της συναλλαγής και της ισχύος του υπολογιστή που απαιτείται για τον χειρισμό των συναλλαγών. Η εξουσιοδότηση και η ασφάλεια είναι αλληλένδετα θέματα στην τεχνολογία *blockchain*. Η τεχνολογία *blockchain* είναι ευαίσθητη σε κυβερνοεπιθέσεις όπως επίθεση συστήματος ονομάτων τομέα (*DNS*) και επιθέσεις όπου τα μπλοκ πλημμύρισαν με συναλλαγές και ο εισβολέας ανέλαβε τον έλεγχο της πλειοψηφίας των δικτύων *blockchain*.

Άλλες βασικές προκλήσεις που σχετίζονται με τον αγοραστή των δημόσιων *blockchains* ιδιαίτερα, περιλαμβάνουν υψηλή κατανάλωση ενέργειας και αργή ταχύτητα επεξεργασίας λόγω μεγάλου αριθμού χρηστών που συμμετέχουν στο δίκτυο.

Κοινωνικές απειλές.

Η μεγάλη πρόκληση που αντιμετωπίζεται στην υιοθέτηση της τεχνολογίας *blockchain* είναι η κοινωνική αποδοχή. Η αποκέντρωση των ιατρικών δεδομένων και η απεμπλοκή ενός αξιόπιστου τρίτου δυσκολεύουν τις νομικές αρχές να εκδώσουν πρόσβαση τονίζοντας την ιδιωτικότητα ως νόμιμο μέλημα. Επίσης τόνισε την έλλειψη κανονισμών και κατευθυντήριων γραμμών διακυβέρνησης που μπορεί να αποτρέψει την εφαρμογή *blockchain* στην υγειονομική περίθαλψη.

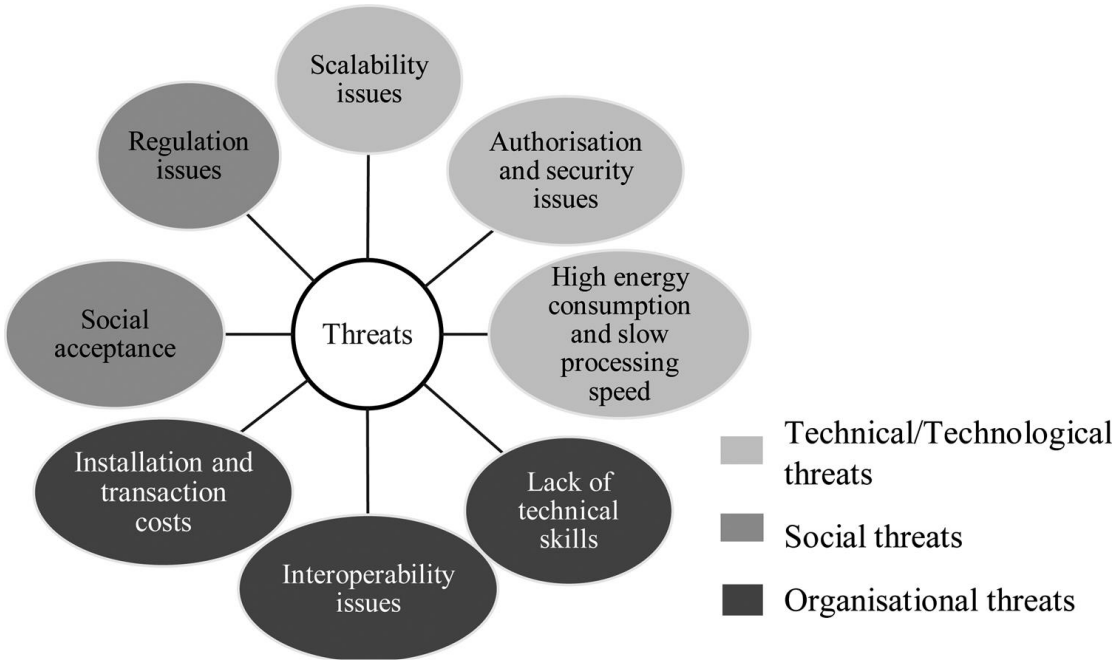
Οργανωτικές Απειλές

Η διαλειτουργικότητα είναι ένα από τα σημαντικότερα ζητήματα της εφαρμογής *blockchain* στον τομέα της υγειονομικής περίθαλψης. Το ζήτημα διαλειτουργικότητας αποδόθηκε από τρεις μελέτες για την έλλειψη εμπιστοσύνης μεταξύ των μερών και περιορισμένων ανοιχτών προτύπων που προκαλούν δυσκολίες για μια ολοκληρωμένη ανταλλαγή πληροφοριών για την υγεία μεταξύ των οργανισμών υγειονομικής περίθαλψης.

Ένα άλλο πρόβλημα που έχει εντοπιστεί είναι η συντήρηση μίας ολοκληρωμένης φαρμακευτικής αλυσίδας εφοδιασμού μεταξύ των ενδιαφερομένων για το *blockchain* με

[29] (Wayner, 2015)

έλλειψη βασικών τεχνικών δεξιοτήτων και επαγγελματιών πληροφορικής που είναι ειδικοί στη λειτουργία της τεχνολογίας. Επιπλέον, αν και το *blockchain* μπορεί να εξοικονομήσει κόστος μακροπρόθεσμα, το αρχικό κόστος εγκατάστασης είναι αρκετά υψηλό. [30]



Πηγή:
https://reader.elsevier.com/reader/sd/pii/S1386505620301544?token=F05170697DDA252377C76BA139A46D7D405B0F2399514A47D608DD643F5ACC64267A7E9E27FA4343F2B027D5490B1286&originRegion=eu-west-1&originCreation=20210729164925

4.2 ΕΙΔΗ - ΠΕΡΙΠΤΩΣΕΙΣ ΕΠΙΘΕΣΕΩΝ

4.2.1 ΕΠΙΘΕΣΕΙΣ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΗΝ ΣΥΝΑΙΝΕΣΗ ΚΑΙ ΤΟ ΚΑΘΟΛΙΚΟ

Η διπλή δαπάνη είναι ένα πρόβλημα, που σημαίνει ότι ξοδεύουμε το ίδιο κρυπτονόμισμα δύο φορές όπως φαίνεται ακολούθως.

[30] (Abu-elezz, Hassan, Nazeemudeen, κ.α. 2020)

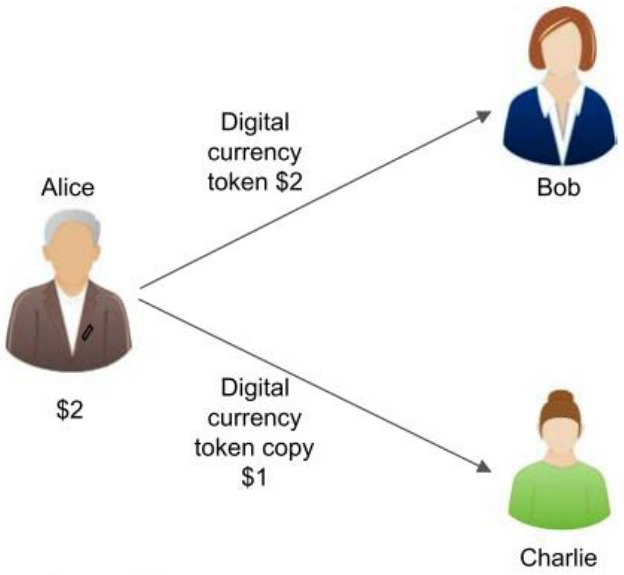


Fig. 2 Double-spending problem.

Πηγή:https://www.sciencedirect.com/science/article/pii/S0065245820300759?via%3Dihub

Για να αποτρέψετε το σύστημα από αυτό πρόβλημα, το δίκτυο πρέπει να παραμείνει αποκεντρωμένο, έτσι ώστε ένα μέρος να μην μπορεί αναλάβει τον έλεγχο όλων των συναλλαγών στο δίκτυο. Το *Bitcoin* χρησιμοποιεί μηχανισμό αποφυγής συναίνεσης της κεντρικής αρχής που επαληθεύει ότι η συναλλαγή δεν είναι διπλής δαπάνης. Σε αυτήν, μία αποκεντρωμένη ομάδα ατόμων γνωστή ως ανθρακωρύχοι *bitcoin* πραγματοποίησαν τη διαδικασία επαλήθευσης. Οι συναλλαγές καταγράφονται ως έγκυρες μόλις προστεθούν στα μπλοκ του *blockchain*. Όσα περισσότερα μπλοκ προστίθενται στο *blockchain*, καθίσταται δύσκολο να επιστρέψουν και να υπάρξει διπλή δαπάνη για τη συναλλαγή. Σημαίνει ότι απαιτείται πολύ υψηλή υπολογιστική ισχύ με την ίδια ποσότητα υπολογιστικής ισχύος που έχει χρησιμοποιηθεί κατά τη διάρκεια της εξόρυξης. Όλες οι συναλλαγές μοιράζονται στα δημόσια καθολικά. Αυτό διασφαλίζεται με το οποιοσδήποτε κόμβος που επιθυμεί να δαπανήσει *bitcoin* είναι πραγματικά υπό κράτηση αυτού του *bitcoin*.

Η σιγουριά ότι η συναλλαγή δεν μπορεί να είναι διπλή δαπάνη είναι άμεσα ανάλογη με τον αριθμό των επιβεβαιώσεων μπλοκ που έχει λάβει η συναλλαγή. Ο αυξημένος αριθμός επιβεβαιώσεων θα αυξήσει την πιθανότητα της συναλλαγής χωρίς διπλή δαπάνη. Το δίκτυο *bitcoin* ξοδεύει περίπου 1 ώρα για να προστατεύσει μια συναλλαγή από διπλές δαπάνες.

4.2.1.1 ΕΠΙΘΕΣΗ FINNEY

Αυτή η επίθεση συμβαίνει όταν οι πληρωμές γίνονται αποδεκτές με μηδενικές επιβεβαιώσεις. Για την εκτέλεση αυτής της επίθεσης απαιτείται ένας ανθρακωρύχος που έχει ήδη εξορύξει ένα μπλοκ αλλά δεν μεταδίδεται ακόμη στο υπόλοιπο δίκτυο. Σε αυτό, ο ανθρακωρύχος θα μπορούσε να περιλαμβάνει μια συναλλαγή πληρωμής από τη διεύθυνση Α στη διεύθυνση Β στο υπό εξόρυξη μπλοκ. Στη συνέχεια, πάλι ο ανθρακωρύχος θα μπορούσε να αγοράσει μια υπηρεσία πραγματοποιώντας τις πληρωμές από τη διεύθυνση Α στη διεύθυνση Γ. Η εταιρεία θα μπορούσε να πουλήσει την υπηρεσία σε έναν ανθρακωρύχο εν αναμονή πληρωμών *bitcoin*. Ο ανθρακωρύχος θα μπορούσε να εξαπατήσει την υπηρεσία μεταδίδοντας προηγουμένως εξόρυξη μπλοκ στο δίκτυο που περιλαμβάνει τη συναλλαγή από Α σε Β σε περίπτωση συναλλαγής από το Α στο Γ. Με αυτόν τον τρόπο, αυτή η επίθεση που συμβαίνει περιλαμβάνει διπλή δαπάνη στο δίκτυο.

4.2.1.2 ΕΠΙΘΕΣΗ RACE (ΑΓΩΝΑ)

Αυτή η επίθεση συμβαίνει επίσης στους χονδρεμπόρους και στους άλλους ειδικούς που αποδέχονται τη συναλλαγή πληρωμής με μηδενικές επιβεβαιώσεις. Θα μπορούσε να συμβεί στέλνοντας δύο αντικρουόμενες συναλλαγές με γρήγορη ακολουθία στο δίκτυο.

Για παράδειγμα, ο κακόβουλος ηθοποιός θα μπορούσε να στείλει μια συναλλαγή *bitcoin* για μία υπηρεσία στον χονδρέμπορο. Ταυτόχρονα, στέλνει μια αντικρουόμενη συναλλαγή στο δίκτυο που ξοδεύει το ίδιο *bitcoin* για τον εαυτό του. Στην περίπτωση αυτή, η δεύτερη συναλλαγή που συγκρούεται εξορύσσεται στο μπλοκ και εμφανίζεται ως γνήσια συναλλαγή μέσω των κόμβων δικτύου. Αυτή θα ήταν η ζημιά του χονδρέμπορου που εξυπηρετεί τον ηθοποιό εν αναμονή των πληρωμών *bitcoin*.

Η εικονογραφική αναπαράσταση της επίθεσης του αγώνα (*Race*) είναι όπως φαίνεται ακολούθως:

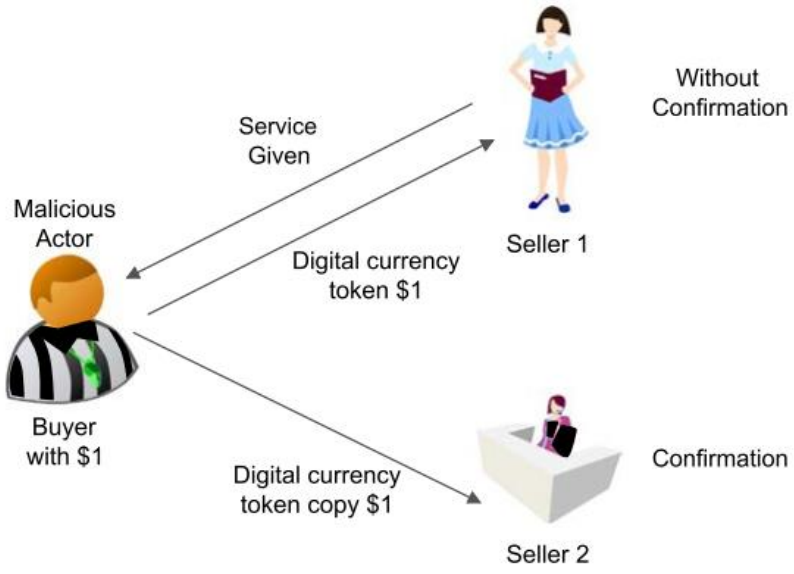


Fig. 4 Race attack.

Πηγή:https://www.sciencedirect.com/science/article/pii/S0065245820300759?via%3Dihub

4.2.1.3 ΕΠΙΘΕΣΗ 51%

Είναι επίσης γνωστή ως επίθεση πλειοψηφίας. Ένας επιτιθέμενος μπορεί να κάνει διπλές δαπάνες αν έχει τον έλεγχο πάνω από το μισό του δικτύου. Με αυτήν την επίθεση, μπορεί να δημιουργήσει και να παράξει μπλοκς γρηγορότερα από τους άλλους κόμβους του δικτύου. Θα μπορούσε να ξοδέψει χρήματα για το δίκτυο που χτίζεται από τους έντιμους ανθρακωρύχους αλλά στη συνέχεια, δεν περιλαμβάνεται στο ιδιωτικό *blockchain*. Ο εισβολέας στη συνέχεια μεταδίδει το ιδιωτικό *blockchain* και έχει τη δυνατότητα να μπορεί να κάνει ξανά τη συναλλαγή με τα κεφάλαιά τους. Η εικονογραφική αναπαράσταση εάν η επίθεση 51% είναι όπως φαίνεται στο Σχ. 5.

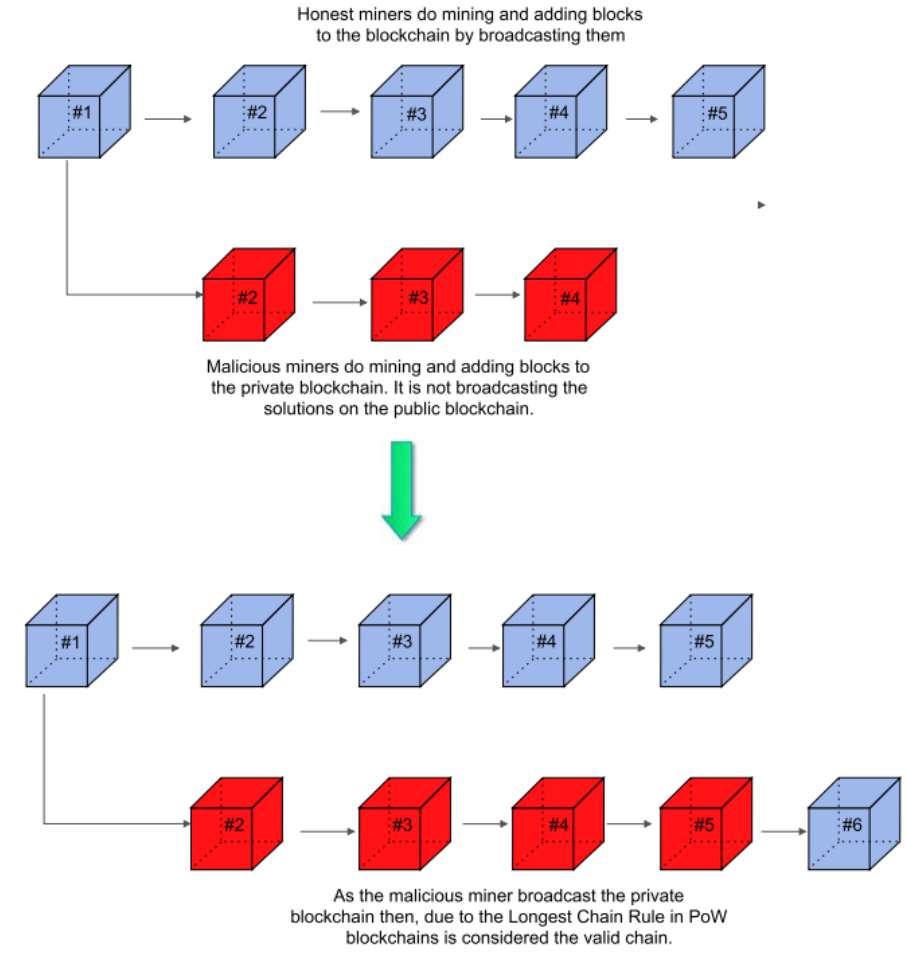


Fig. 5 51% attack.

Πηγή:https://www.sciencedirect.com/science/article/pii/S0065245820300759?via%3Dihub

4.2.2 ΕΠΙΘΕΣΗ ΔΙΚΤΥΟΥ ΑΠΟ ΟΜΟΤΙΜΟΥΣ ΧΡΗΣΤΕΣ

Το σημαντικό χαρακτηριστικό της τεχνολογίας *blockchain* είναι η βελτίωση της ασφάλειας και της ιδιωτικής ζωής χωρίς τη συμμετοχή ελέγχου ταυτότητας τρίτου μέρους.

Ένα δίκτυο υπολογιστών *P2P* που τρέχουν όλοι το πρωτόκολλο και διαθέτουν ένα πανομοιότυπο αντίγραφο του βιβλίου συναλλαγών, επιτρέποντας συναλλαγές αξίας *P2P* μέσω ενός μηχανισμού συναίνεσης. Ακολούθως περιγράφονται 4 μεγάλες επιθέσεις:

4.2.4.1 ΕΠΙΘΕΣΗ SYBIL

Μια επίθεση *Sybil* είναι εκείνη όπου ένας επιτιθέμενος προσποιείται ότι είναι ταυτόχρονα πολλοί άνθρωποι στο ίδιο σημείο. Είναι ένα από τα σημαντικότερα ζητήματα κατά τη σύνδεση σε δίκτυο *P2P*. Αυτού του είδους η επίθεση χειρίζεται το δίκτυο και ελέγχει ολόκληρο το δίκτυο δημιουργώντας πολλαπλές πλαστές ταυτότητες. Αυτές οι διαφορετικές ταυτότητες μοιάζουν σαν τακτικοί χρήστες, αλλά σε μια μεμονωμένη οντότητα, ο επιτιθέμενος, ελέγχει όλες αυτές τις ψεύτικες οντότητες ταυτόχρονα.

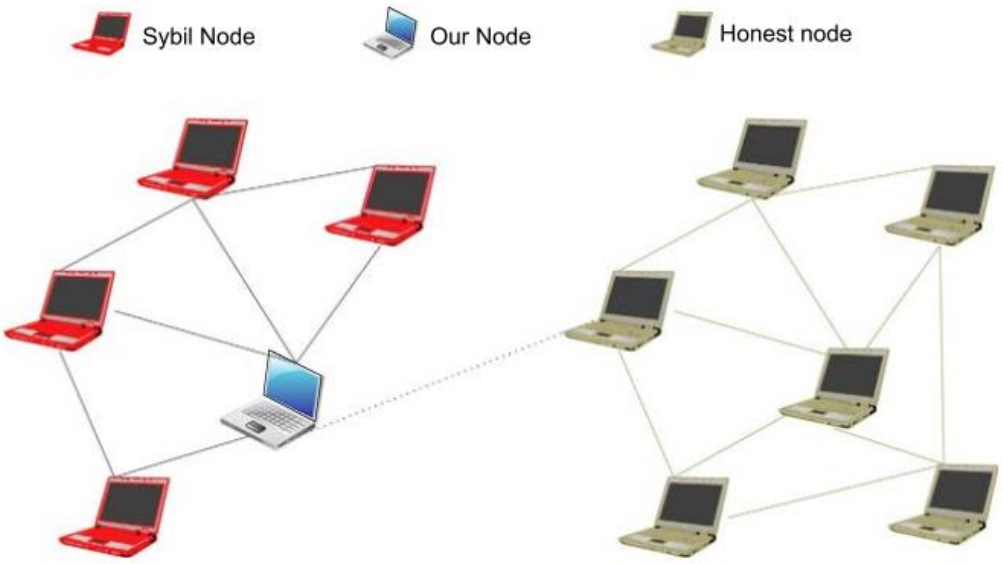


Fig. 6 Sybil attack.

Πηγή:https://www.sciencedirect.com/science/article/pii/S0065245820300759?via%3Dihub

Ο μόνος τρόπος να μειωθούν οι επιθέσεις *Sybil* είναι να αυξηθεί το κόστος δημιουργίας νέας ταυτότητας. Αυτό το κόστος θα πρέπει να εξισορροπηθεί έτσι ώστε οι νέοι συμμετέχοντες να μην περιορίζονται από τη συμμετοχή στο δίκτυο και να δημιουργούν νόμιμες ταυτότητες. Θα πρέπει επίσης να είναι τόσο υψηλό ώστε να η δημιουργία μεγάλου αριθμού ταυτοτήτων σε σύντομο χρονικό διάστημα να επιβάλλει υψηλό κόστος.

4.2.4.2 ΕΠΙΘΕΣΗ ΈΚΛΕΙΨΗΣ (ECLIPSE)

Οι επιθέσεις έκλειψης είναι ένας τύπος επίθεσης δικτύου που στοχεύει στην έκλειψη ορισμένων κόμβων από ολόκληρο το δίκτυο *P2P*. Είναι ένας τύπος επίθεσης, που διαχειρίζεται τη σύνδεση του κόμβου με τέτοιο τρόπο ώστε να λαμβάνουν πληροφορίες μόνο οι επιτιθέμενοι κόμβοι από ότι οι άλλοι κόμβοι. Επικεντρώνεται κυρίως στην επίθεση μονού κόμβου και όχι ολόκληρου του δικτύου ταυτόχρονα. Η επίθεση μπορεί να γίνει στέλνοντας στον κόμβο του θύματος μια συναλλαγή που δείχνει απόδειξη πληρωμής κρύβοντας τη από το δίκτυο. Οι επιθετικοί κόμβοι είναι με κόκκινο χρώμα και απομονώνουν έναν από τους τους κανονικούς κόμβους με μπλε χρώμα από ολόκληρο το δίκτυο μονοπωλώντας και τον έλεγχο των συνδέσεών του.

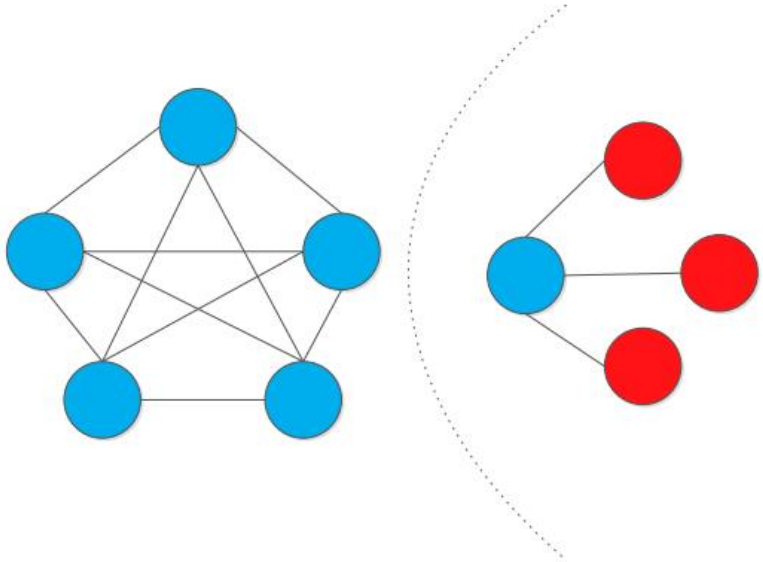


Fig. 7 Eclipse attack.

Πηγή:https://www.sciencedirect.com/science/article/pii/S0065245820300759?via%3Dihub

4.2.4.3 ΚΑΤΑΝΕΜΗΜΕΝΗ ΑΡΝΗΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ (DDOS)

Η επίθεση *DDoS* είναι μια επίθεση, όπου ένας εισβολέας υπερφορτώνει το δίκτυο και το πλημμυρίζει με μεγάλο αριθμό αιτημάτων σε μία προσπάθεια. Με αυτό τον τρόπο οι πόροι δικτύου είναι μη διαθέσιμοι στους χρήστες του. Στην περίπτωση μιας επίθεσης *DDoS*, όλα αυτά τα αιτήματα προέρχονται από μεγάλο αριθμό διαφορετικών πηγών.

Ο μετριασμός αυτής της επίθεσης είναι η εισαγωγή ενός τέλους συναλλαγής που αυτόματα μειώνει τα παράνομα αιτήματα συναλλαγών.

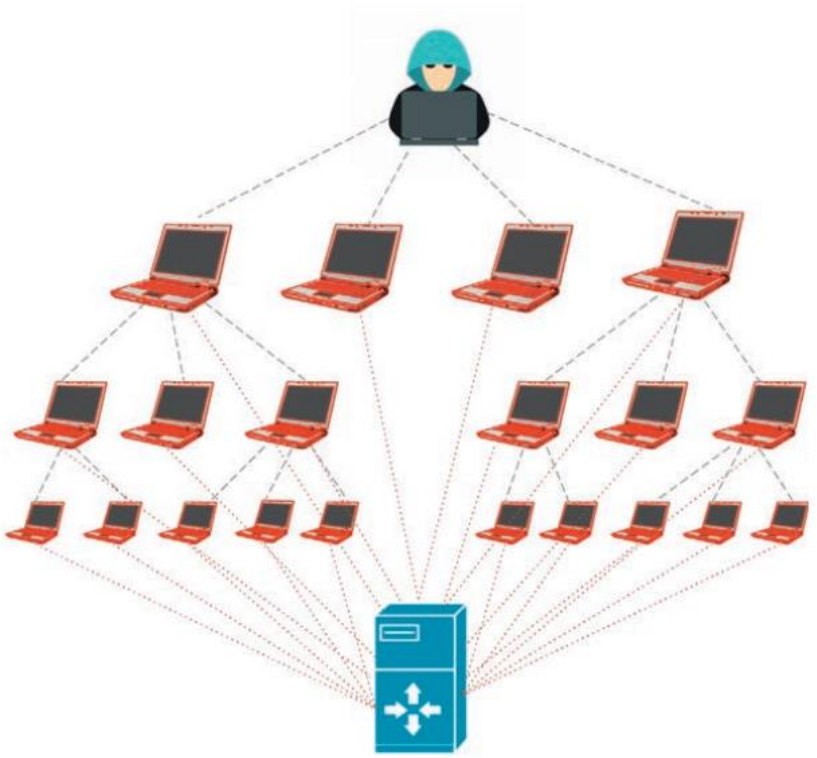


Fig. 8 Distributed denial-of-service attack.

Πηγή:https://www.sciencedirect.com/science/article/pii/S0065245820300759?via%3Dihub

4.2.4.4 ΕΠΙΘΕΣΗ ΔΡΟΜΟΛΟΓΗΣΗΣ

Οι επιθέσεις δρομολόγησης βασίζονται στον αποκλεισμό των μηνυμάτων που διαδίδονται μέσω του δικτύου και την δημιουργία αλλαγών πριν την μεταφορά τους. Ο μόνος τρόπος για τον εντοπισμό τέτοιων τύπων επιθέσεων είναι όταν ένας δέκτης λαμβάνει ένα διαφορετικό αντίγραφο από έναν άλλο κόμβο. Με άλλα λόγια, ένας επιτιθέμενος διαιρεί το δίκτυο σε δύο ή περισσότερα μέρη που δεν μπορούν να επικοινωνήσουν ο ένας με τον άλλο. Οι επιθέσεις δρομολόγησης ταξινομούνται σε δύο μικρότερες επιθέσεις.

• Επίθεση κατάτμησης: Ένας εισβολέας προσπαθεί να χωρίσει το δίκτυο σε δύο ή

περισσότερες ασύνδετες ομάδες. Αυτό μπορεί να γίνει με επίθεση σε ορισμένα σημεία μέσα στο δίκτυο, το οποίο λειτουργεί ως το σημείο σύνδεσης μεταξύ των δύο ομάδων.

• Καθυστέρηση επίθεσης: Ένας εισβολέας παίρνει τα μηνύματα, κάνει αλλαγές και τελικά τα μεταφέρει στην πλευρά του δικτύου που δεν τα έχει ξαναδεί.

Η μέθοδος αποφυγής αυτής της επίθεσης είναι η συνεχής διαφοροποίηση στις συνδέσεις δικτύου. Αυτή η διαδικασία θα δυσκολέψει τον επιτιθέμενο να βρει σημεία συνδέσεων και να χωρίσει το δίκτυο σε δύο ή περισσότερες ασύνδετες ομάδες.

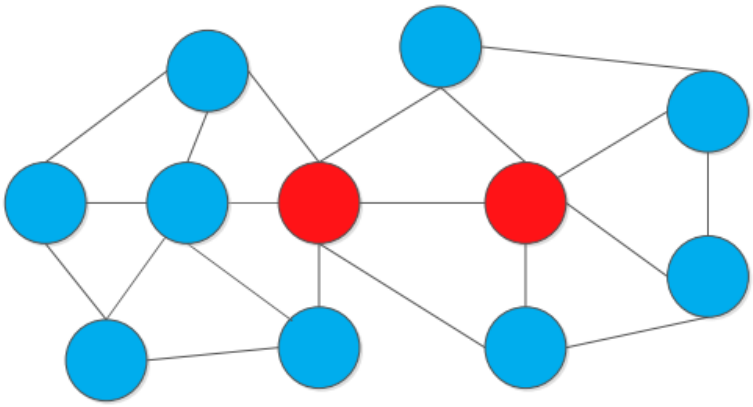


Fig. 9 Routing attack.

Πηγή:https://www.sciencedirect.com/science/article/pii/S0065245820300759?via%3Dihub

4.2.3. ΕΠΙΘΕΣΕΙΣ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΕ ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ (*SMART BASED CONTRACT ATTACKS*)

Τα έξυπνα συμβόλαια είναι αυτοματοποιημένες γραμμές προγραμματισμού που χρησιμοποιούνται στο *blockchain* για την εκτέλεση αποκεντρωμένων εφαρμογών. Εκτελούν τη συναλλαγή μεταξύ των συμμετεχόντων με συμφωνημένη συμφωνία, με εισροές από τον πραγματικό κόσμο και χωρίς τη συμμετοχή μεσάζοντα. Έτσι, μόλις ξεκινήσει το έξυπνο συμβόλαιο, δεν μπορεί να διακοπεί. Όταν ολοκληρωθεί η στο δίκτυο *blockchain*, γίνεται αμετάβλητη. Συνεπώς, εάν τα έξυπνα συμβόλαια έχουν σφάλματα, εκατομμύρια νομίσματα διακυβεύονται και δεν μπορούν να γίνουν αλλαγές.

4.2.3.1 ΕΠΙΘΕΣΗ DAO

Το *DAO* είναι μια αποκεντρωμένη αυτόνομη οργάνωση. Έχει στόχο να γράψει τον κώδικα των γραμμών μιας εταιρείας για την εξάλειψη της ανάγκης για έγγραφα και την καθοδήγηση των ατόμων για τον έλεγχο των αποκεντρωμένων δομών.

4.2.4 ΕΠΙΘΕΣΕΙΣ ΜΕ ΒΑΣΗ ΤΟ ΠΟΡΤΟΦΟΛΙ (*WALLET BASED ATTACKS*)

Τα συμβόλαια πορτοφολιού είναι λογικά από ό, τι μπορούν να δημιουργηθούν σε πορτοφόλια χρηστών για τακτικές αυτοματοποιημένες πληρωμές. Κάθε κόμβος στο δίκτυο έχει το πορτοφόλι του για να πραγματοποιήσει πληρωμές. Ένας εισβολέας μπορεί να επιτεθεί στο πορτοφόλι του κόμβου στο *blockchain* για κακόβουλη δραστηριότητα στο δίκτυο. [31]

4.3 ΠΕΡΙΠΤΩΣΕΙΣ ΠΡΑΓΜΑΤΙΚΩΝ ΕΠΙΘΕΣΕΩΝ

Πολλές τεχνολογίες που σχετίζονται με το *blockchain* και τα κρυπτονομίσματα εξακολουθούν να είναι πειραματικές και κερδοσκοπικές. Τα τρωτά σημεία μπορούν να οδηγήσουν σε παραβίαση των πορτοφολιών - και των κρυπτονομισμάτων που είναι αποθηκευμένα μέσα. Παρακάτω παρατίθενται πραγματικές επιθέσεις σε συστήματα *blockchain*.

***Poloniex*:** Η *Poloniex* ανακάλυψε παραβίαση δεδομένων και επέβαλε μαζική επαναφορά κωδικών πρόσβασης για τους χρήστες μετά τη διαρροή των δεδομένων στα κοινωνικά μέσα.

[31] (Aggarwal, Kumar, 2021)

***Helix*:** Ένας άνδρας από το Οχάιο συνελήφθη για την εκτέλεση της υπηρεσίας μίξης *Helix Bitcoin*. Υπολογίζεται ότι ξεπλύθηκαν 300 εκατομμύρια δολάρια.

Κλοπή από μηχανικό της *Microsoft*: Ένας μηχανικός λογισμικού καταδικάστηκε για κλοπή άνω των 10 εκατομμυρίων δολαρίων από τη *Microsoft*.

***IOTA*:** Το ίδρυμα *IOTA* έκλεισε ολόκληρο το δίκτυό του λόγω ενός χάκερ που εκμεταλλεύθηκε μια αδυναμία στην εφαρμογή πορτοφολιού *IOTA*.

***Altsbit*:** Το ιταλικό χρηματιστήριο κρυπτονομισμάτων έκλεισε μετά από υποτιθέμενη κυβερνοεπίθεση στην οποία κλέφθηκαν τα περισσότερα κεφάλαια χρηστών.

***Prometei*:** Οι ερευνητές βρήκαν ένα δίκτυο μολυσμένων υπολογιστών που εκμεταλλεύεται το πρωτόκολλο *Microsoft Windows SMB* για εξόρυξη κρυπτονομίσματος.

***YouTube*:** Οι λογαριασμοί *YouTub*e παραβιάστηκαν για να προωθήσουν μια απάτη κρυπτονομίσματος *Ponzi* με θέμα τον Μπιλ Γκέιτς.

***Lendf.me*:** Κρυπτονομίσματα 25 εκατομμυρίων δολλαρίων εκλάπησαν από την πλατφόρμα *Lendf.me*.

***Bisq*:** Πάνω από $ 250.000 έκλεψαν χρήστες χρηματιστηρίων του *Bisq Bitcoin*.

Υπερυπολογιστές: Οι υπερυπολογιστές σε όλη την Ευρώπη παραβιάστηκαν προκειμένου να εξορύξουν κρυπτονομίσματα.

***BTC-e*:** Η επιβολή του νόμου της Νέας Ζηλανδίας πάγωσε 90 εκατομμύρια δολάρια σε περιουσιακά στοιχεία της *BTC-e* στο πλαίσιο έρευνας για ξέπλυμα χρήματος.

***CryptoCore*:** Οι ερευνητές είπαν ότι η ομάδα hacking *CryptoCore* έχει κλέψει τουλάχιστον 200 εκατομμύρια δολάρια σε κρυπτονομίσματα από διαδικτυακές ανταλλαγές.

***Coincheck*:** Ένας χάκερ διείσδυσε στην υπηρεσία ανταλλαγής κρυπτονομισμάτων,

***Twitter*:** Τα προφίλ *Twitter* υψηλού προφίλ που ανήκουν σε πρόσωπα συμπεριλαμβανομένων των *Joe Biden, Bill Gates* και *Elon Musk* παραβιάστηκαν για να διαφημίσουν μια απάτη κρυπτονομισμάτων.

***Coinbase*:** Η *Coinbase* απέκλεισε μια προσπάθεια επιτιθέμενων να κλέψουν $ 280,000 σε *Bitcoin*.

***VaultAge Solutions*:** Ο Διευθύνων Σύμβουλος κρύφτηκε αφού φέρεται να εξαπάτησε επενδυτές κατά 13 εκατομμύρια δολάρια.

***AT&T*:** Η *AT&T* οδηγήθηκε στο δικαστήριο για υπόθεση κλοπής κρυπτονομισμάτων και κλοπής νομισματικής κάρτας 1,9 εκατομμυρίων δολαρίων *SIM*.

***GPay Ltd*:** Οι βρετανικές ρυθμιστικές αρχές έκλεισαν το *GPay* για εξαπάτηση επενδυτών κρυπτονομισμάτων χρησιμοποιώντας ψεύτικες εγκρίσεις διασημοτήτων.

***FritzFrog*:** Ανακαλύφθηκε ένα *botnet* εξόρυξης κρυπτονομισμάτων που έθεσε σε κίνδυνο τουλάχιστον 500 εταιρικούς και κυβερνητικούς διακομιστές.

Ουκρανικές συλλήψεις: Οι αρχές της Ουκρανίας συνέλαβαν ύποπτα μέλη μιας συμμορίας που ξέπλυνε 42 εκατομμύρια δολάρια σε κρυπτογράφηση για ομάδες ransomware.

2together: 1,2 εκατομμύρια ευρώ κρυπτονομίσματος κλέφθηκαν από το χρηματιστήριο.

***PlusToken*:** Η κινεζική αστυνομία συνέλαβε πάνω από 100 άτομα ύποπτα για συμμετοχή στην απάτη επενδύσεων κρυπτονομισμάτων *PlusToken*.

***Lazarus*:** Οι ερευνητές ανακάλυψαν μια νέα καμπάνια Lazarus που στοχεύει σε μια εταιρεία κρυπτονομισμάτων μέσω αγγελιών εργασίας *LinkedIn*.

***KuCoin*:** Περίπου 150 εκατομμύρια δολάρια σε κρυπτονόμισμα έκλεψαν μετά την αποθήκευσή του σε πορτοφόλια.

Ψάρεμα (*phishing*) κρυπτονομισμάτων: Δύο Ρώσοι κατηγορήθηκαν για κλοπή σχεδόν 17 εκατομμυρίων δολλαρίων σε εκστρατείες ψαρέματος με θέμα κρυπτονομίσματα.

***Eterbase*:** Το χρηματιστήριο κρυπτονομισμάτων έχασε 5,4 εκατομμύρια δολάρια, που έκλεψαν άγνωστοι επιτιθέμενοι από ζεστά πορτοφόλια.

***Kik*:** Η αμερικανική *SEC* επέβαλε στην *Kik* ποινή 5 εκατομμυρίων δολαρίων για δήθεν παράνομη προσφορά κινητών αξιών.

***Harvest Finance*:** Οι χάκερ έκλεψαν 24 εκατομμύρια δολάρια, αλλά αργότερα επέστρεψαν 2,5 εκατομμύρια δολάρια.

***GoDaddy*:** Το *GoDaddy* παραδέχτηκε ότι το προσωπικό του είχε πέσει θύμα μιας εκστρατείας κοινωνικής μηχανικής που οδήγησε σε επιθέσεις με *email* και *DN*S εναντίον *Liquid.com* και *NiceHash*.

Acropolis: Η εταιρεία *Acropolis* υπέστη μια άμεση επίθεση δανείου και έκλεψαν κρυπτονομίσματα 2 εκατομμυρίων δολαρίων. Η εταιρεία προσέφερε αργότερα στον χάκερ μια «πληρωμή ανταμοιβής σφάλματος» σε αντάλλαγμα για τα κλεμμένα κεφάλαια.

Επιχείρηση *Egypto*: Οι αρχές επιβολής του νόμου των ΗΠΑ και της Βραζιλίας κατέσχεσαν κρυπτονομίσματα 24 εκατομμυρίων δολαρίων από άτομα που φέρονται να συνδέονται με απάτη επενδυτών μέσω διαδικτύου.

***Silk Road*:** Το αμερικανικό υπουργείο Δικαιοσύνης κατέσχεσε 1 δισεκατομμύριο δολάρια σε Bitcoin, το οποίο λέγεται ότι προέρχεται από την αγορά του *Silk Road*.

Ληστεία *Bitcoin* 24 εκατομμυρίων ευρώ: Οι ύποπτοι φέρονται να έχουν εκτελέσει μια απάτη και απέσπασαν 24 εκατομμύρια ευρώ σε *Bitcoin* (*BTC*).

***Upbit*:**. Το χρηματιστήριο έχει υποσχεθεί ότι οι πελάτες δεν θα επηρεαστούν και τα κεφάλαια θα καλυφθούν από περιουσιακά στοιχεία της *Upbit*.

***PureBit*:** Παρά το γεγονός ότι λειτουργούσε μόνο λίγους μήνες, το νόμισμα της Κορέας ανταλλακτήριο κρυπτονομισμάτων *PureBit* φέρεται να τράβηξε μια απάτη εξόδου, παίρνοντας μαζί του 3 εκατομμύρια δολάρια σε *Ethereum*.

***PlusToken*:** Η *PlusToken* φέρεται να έκανε απάτη εξόδου, αποχωρώντας με καταθέσεις 2,9 δισεκατομμυρίων δολαρίων. Ορισμένα άτομα που θεωρούνταν ύποπτα για συμμετοχή έχουν συλληφθεί.

***Monero*:** Ο επίσημος ιστότοπος *Monero* παραβιάστηκε για να παραδώσει ένα κακόβουλο δυαδικό *Official Linux CLI* το οποίο παραποιήθηκε για να κλέψει χρήματα από χρήστες ακούσια.

***Cryptopia*:**Η ανταλλαγή κρυπτονομισμάτων *Cryptopia* της Νέας Ζηλανδίας αποσύρθηκε εκτός σύνδεσης λόγω κάποιας μορφής *hack*, αλλά οι λεπτομέρειες είναι ελάχιστες. Οι εκτιμήσεις δείχνουν ότι μπορεί να έχουν χαθεί έως και 16 εκατομμύρια δολάρια.

***Bitgrail*:** Ο προηγούμενος ιδιοκτήτης του παραβιασμένου χρηματιστηρίου *Bitgrail* - το οποίο έχασε 195 εκατομμύρια δολάρια σε νομίσματα *Nano* - έλαβε εντολή από ένα ιταλικό δικαστήριο να επιστρέψει όσο το δυνατόν περισσότερα χρήματα πελατών, οδηγώντας στην κατάσχεση περιουσιακών στοιχείων.

***Bithumb*:** Η *Bithumb* ανέφερε ένα άλλο περιστατικό ασφαλείας το 2019, το τρίτο σε δύο χρόνια. Πιστεύεται ότι οι κυβερνοεπιθέτες μπορεί να έχουν κλέψει έως και 20 εκατομμύρια δολάρια σε μάρκες *EOS* και *Ripple*.

***Binance*:** Οι κυβερνοεπιθέτες παραβίασαν την πλατφόρμα ανταλλαγής κρυπτονομισμάτων *Binance* και κέρδισαν 41 εκατομμύρια δολάρια σε *Bitcoin*.

***Bitpoint*:** Η ανταλλαγή κρυπτονομισμάτων *Bitpoint* με έδρα την Ιαπωνία υπέστη κλοπή κρυπτονομισμάτων ύψους 32 εκατομμυρίων δολαρίων, εκ των οποίων τα 23 εκατομμύρια δολάρια ανήκαν σε πελάτες του οργανισμού.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Το *Blockchain* εξακολουθεί να είναι μια αναδυόμενη τεχνολογία και τα πρότυπα και οι παραλλαγές του *blockchain* εξακολουθούν να εξελίσσονται. Ως εκ τούτου, μπορεί να υποστηριχθεί ότι η πρόσφατη τεχνολογία *blockchain* είναι εφικτή μόνο για ορισμένες εφαρμογές τουλάχιστον μέχρι την εμφάνιση νέων προόδων.

Οι έρευνες δείχνουν γενικότερα ότι η έρευνα τεχνολογίας *blockchain* και η εφαρμογή της στην υγειονομική περίθαλψη και όχι μόνο είναι αυξανόμενη. Οι τρέχουσες τάσεις της έρευνας *blockchain* στην υγειονομική περίθαλψη δείχνουν ότι χρησιμοποιείται κυρίως για κοινή χρήση δεδομένων, αρχεία υγείας και έλεγχο πρόσβασης, αλλά σπάνια για άλλα σενάρια, όπως η αλυσίδα εφοδιασμού, διαχείριση συνταγογράφησης φαρμάκων. Επομένως, υπάρχουν ακόμη πολλές δυνατότητες για το *blockchain* ανεκμετάλλευτες.

Ειδικότερα, τα έξυπνα συμβόλαια θα μπορούσαν να χρησιμοποιηθούν περισσότερο, καθώς επιτρέπουν την αυτοματοποίηση των διαδικασιών μέσα σε μια πλατφόρμα *blockchain*. Οι περισσότερες έρευνες θα μπορούσαν επίσης να παρέχουν μια πρωτότυπη υλοποίηση ή τουλάχιστον συζητούν ορισμένες λεπτομέρειες εφαρμογής των προτάσεών τους.

Όσον αφορά την περαιτέρω έρευνα, τα *blockchains* εξακολουθούν να είναι αρκετά νέα τεχνολογία στον τομέα της υγειονομικής περίθαλψης και μπορούν ακόμα να βρεθούν και να ερευνηθούν νέοι τρόποι χρησιμοποίησής του. Συνοψίζοντας, το *blockchain* θα πρέπει να συνεχιστεί να χρησιμοποιείται σε σενάρια όπου είναι λογικό και απαραίτητο.

Συμπερασματικά, υποστηρίζουμε ότι υπάρχει σίγουρα μια δυνατότητα για πιο επιτυχημένο *blockchain* σε όλες τις εφαρμογές και τους τομείς. Ωστόσο, απαιτείται πιο συστηματική έρευνα για να έχουμε ένα μεγάλο αντίκτυπο στη διαδικασία ανάπτυξης. Υπάρχει άφθονο περιθώριο για περαιτέρω πρόοδο στον καθορισμό του βέλτιστου πλαισίου, τεχνολογιών και εργαλείων για εφαρμογές *blockchain* σε όλους τους τομείς.

6. ΒΙΒΛΙΟΓΡΑΦΙΑ

Α) Ελληνική

Γιαννακού Μ. (2019). *Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΓΙΑ ΤΗΝ ΕΞΥΠΗΡΕΤΗΣΗ ΠΟΛΙΤΩΝ Πρωτόκολλο Blockchain: Κρυπτονομίσματα και Ηλεκτρονική Ταυτοποίηση.* Εθνικό και Καποδιστριακό Πανεπιστήμιο, Αθήνα. Ανακτήθηκε 15 Σεπτεμβρίου, 2021, από https://eclass.uoa.gr/modules/document/file.php/MEDIA313/%CF%80%CF%84%CF%85%CF%87%CE%B9%CE%B1%CE%BA%CE%AE%20%CE%B5%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1%20%CE%9C.%CE%93%CE%B9%CE%B1%CE%BD%CE%BD%CE%AC%CE%BA%CE%BF%CF%85.pdf

Γκρίτζαλης Σ., Κάτσικας Σ. & Λαμπρινουδάκης Κ. (2021). *Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο.* Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

Καρσλίδης Δ., (2021). *Σχεδιασμός και Ανάπτυξη Έξυπνων Συμβολαίων και Κατανεμημένων Εφαρμογών σε Ethereum Blockchain.* Πανεπιστήμιο Δυτικής Αττικής, Αθήνα. Ανακτήθηκε 16 Σεπτεμβρίου, 2021, από https://polynoe.lib.uniwa.gr/xmlui/bitstream/handle/11400/678/eee_50106729.pdf?sequence=2&isAllowed=y

Πατσιλίβας Α. (2020). *Τεχνολογία Blockchain και Εφαρμογές.* Πανεπιστήμιο Πατρών, Πάτρα. Ανακτήθηκε 20 Ιουλίου, 2021, από http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/9187/%20%20%20%20%20%20%20%20%20%20%20%20%20%20Blockchain%20%20%20%20%20%20%20%20%20%20%20%20%20%20.pdf?sequence=1

Μαυρουλής, Ι. (2019). *Τεχνολογίες Blockchain και Θέματα Συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων.* Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα. Ανακτήθηκε 10 Δεκεμβρίου, 2021 από https://apothesis.eap.gr/bitstream/repo/41030/1/Blockchain%20and%20GDPR%20compliance%20issues.pdf

Τσάφου Αποστολοπούλου, Σ. (2020). *Η συμβολή της τεχνολογίας Blockchain στο χώρο της υγείας.* Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα. Ανακτήθηκε 15 Σεπτεμβρίου, 2021, από

Χαντζιάρας Β. (2019). *Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.* Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα.

Β) Αγγλική

Abu-elezz I., Hassan A., Nazeemudeen A., Household M., Abd-alrazaq A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics.* Ανακτήθηκε 29 Ιουλίου, 2021 από https://reader.elsevier.com/reader/sd/pii/S1386505620301544?token=64735C0E379EA6886038C9E720B8A6945BAF7050B433DC538E82B9333E0E02989C44132AC92A6E53C6EE0A691D78EDA8&originRegion=eu-west-1&originCreation=20211115164255

Aggarwal, S., Kumar N. (2021). Blockchain 2.0: Smart contracts. *Advances in Computers.* Ανακτήθηκε 19 Σεπτεμβρίου, 2021 από https://www.sciencedirect.com/science/article/pii/S006524582030070X?via%3Dihub

Bashir, I. (2017). *Mastering Blockchain. Distributed ledgers, decentralization and smart contracts explained*. BIRMINGHAM – MUMBAI: Packt Publishing

Bikramaditya S., Gautam D., Priyansu S. (2018.) *Beginning Blockchain. A Beginner's Guide to Building Blockchain Solutions*. (Βερολίνο). A press. Ανακτήθηκε 3 Αυγούστου, 2021, από https://reader.elsevier.com/reader/sd/pii/S006524582030070X?token=D829FF236E7D0EA2CEDC8E0F3A577F6C0AB253291B8DF5EF128497C3EDCD8EA8FA060698B705A9E170A20BD3277A4B6C&originRegion=eu-west-1&originCreation=20211213172326

Cid C. (2006). Recent developments in cryptographic hash functions: Security implications and future directions. *Information Security Technical Report*. Ανακτήθηκε 18 Σεπτεμβρίου, 2021, από https://www.sciencedirect.com/science/article/pii/S1363412706000203

DeMartino I. (2017). *Bitcoin. Ο απόλυτος οδηγός.* Αθήνα. Φανταστικός Κόσμος.

Garg P., Gupta B., Chauhan A., Sivarajah U., Gupta S., Modgil S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological Forecasting & Social Change.* Ανακτήθηκε 25 Ιουλίου, 2021 από https://www.sciencedirect.com/science/article/abs/pii/S0040162520312336.

Guo Y., Liang C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation.* Ανακτήθηκε 25 Ιουλίου, 2021 από https://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0034-9

Hussien H., Yasin S., Udzir N., Ninggal M., Salman S. (2021). Blockchain technology in the healthcare industry: Trends and opportunities. *Journal of Industrial Information Integration.* Ανακτήθηκε 21 Ιουλίου, 2021 από https://www.sciencedirect.com/science/article/abs/pii/S2452414X21000170

Jajuga K., Locarek-Junge H., Orlowski L., Staehr K. (2021). *Contemporary Trends and Challenges in Finance.* Switzerland: Springer Proceedings in Business and Economics. Ανακτήθηκε 25 Ιουλίου, 2021 από https://link.springer.com/book/10.1007/978-3-030-73667-5

Jianjing W., Jieli L., Yijing Z., Zibin Z. (2021). Analysis of cryptocurrency transactions from a network perspective: An overview. *Journal of Network and Computer Applications*. Ανακτήθηκε 15 Σεπτεμβρίου, 2021, από https://www.sciencedirect.com/science/article/pii/S1084804521001557

Kar A., Navin L., (2021). Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. *Telematics and Informatics.* Ανακτήθηκε 30 Ιουλίου, 2021 από https://www.sciencedirect.com/science/article/abs/pii/S073658532030191X

Karame, G. & Androulaki, E. (2016). *Bitcoin and Blockchain Security*. Norwood, MA: ARTECH HOUSE

Luo L., Zhou J. (2021). BlockTour: A blockchain-based smart tourism platform. *Computer Communications.* Ανακτήθηκε 21 Ιουλίου, 2021 από https://www.sciencedirect.com/science/article/abs/pii/S014036642100195X

Mojtaba S., Bamakan H., Moghaddam S., Manshadi S., (2021). Blockchain-enabled pharmaceutical cold chain: Applications, keychallenges, and future trends. *Journal of Cleaner Production.* Ανακτήθηκε 3 Σεπτεμβρίου, 2021 από https://reader.elsevier.com/reader/sd/pii/S0959652621012403?token=50678C049D88626C4C13243E417729FF024869F56F7CC47C7E45966E53D7800386447C167485FAE7D45700FBCB929158&originRegion=eu-west-1&originCreation=20211114161248

Mojtaba S., Bamakan H., Motavali A., Bondarti A. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems With Applications.* Ανακτήθηκε 7 Οκτωβρίου, 2021, από https://www.sciencedirect.com/science/article/abs/pii/S0957417420302098

Ølnes S., Ubacht J., Janssen M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly.* Ανακτήθηκε 24 Ιουλίου, 2021 από https://www.sciencedirect.com/science/article/abs/pii/S0740624X17303155

Ozdemir, A.I., Ar, I.M. & Erol, I. (2020). Assessment of blockchain applications in travel and tourism industry. *Qual Quant* **54,** 1549–1563 (2020). Ανακτήθηκε 29 Ιουλίου, 2021 από https://doi.org/10.1007/s11135-019-00901-w

Puthal D, Malik N., Mohanty S., Kougianos E. (2018). Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. . *IEEE Consumer Electronics Magazine,* 7(4):*1-10.* Ανακτήθηκε 26 Ιουλίου, 2021, από https://www.researchgate.net/publication/326102908_Everything_You_Wanted_to_Know_About_the_Blockchain_Its_Promise_Components_Processes_and_Problems

Robinson P., Hyland-Wood D., Saltini R., Johnson S., Brainard J. (2019). *Atomic Crosschain Transactions for Ethereum Private Sidechains.* University of Queensland, Australia. Ανακτήθηκε 26 Ιουλίου, 2021 από https://www.researchgate.net/publication/332751175_Atomic_Crosschain_Transactions_for_Ethereum_Private_Sidechains

Stallone V., Wetzels M., Klaas M., (2021). Applications of Blockchain Technology in marketing systematic review of marketing technology companies, *Blockchain: Research and Applications.* Ανακτήθηκε 26 Ιουλίου 2021 από : https://www.sciencedirect.com/science/article/pii/S209672092100018X?via%3Dihub

Wang X., Ni W., Zha X., Yu G., Peng Liu R., Georgalas N., Reeves A. (2021). Capacity analysis of public blockchain. *Computer Communications.* Ανακτήθηκε στις 26 Ιουλίου, 2021, από https://www.sciencedirect.com/science/article/pii/S0140366421002437

Γ) Ιστοσελίδες

Brett C., (2018). *Blockchain disadvantages: 10 possible reasons not to enthuse.* Ανακτήθηκε 25 Σεπτεμβρίου, 2021 από https://www.enterprisetimes.co.uk/2018/10/15/blockchain-disadvantages-10-possible-reasons-not-to-enthuse/

Escobar M.C., (2018). *GOeureka Debuts Its Blockchain Powered Booking Platform.* Ανακτήθηκε 29 Ιουλίου, 2021 από https://hospitalitytech.com/goeureka-debuts-its-blockchain-powered-booking-platform

Followmyvote: *A Quantum Shift In App Development Is Coming... Secure dApp Development.* Ανακτήθηκε 29 Ιουλίου, 2021 από https://followmyvote.com/

Daley S., (2021). *34 Blockchain Applications and Real-World Use Cases Disrupting the Status Quo.* Ανακτήθηκε 28 Ιουλίου, 2021 από https://builtin.com/blockchain/blockchain-applications

Daley S., (2021). *15 Companies Utilizing Blockchain in Music to Reshape a Changing Industry.* Ανακτήθηκε 28 Ιουλίου, 2021 από https://builtin.com/blockchain/blockchain-music-innovation-examples

Daley S., (2019). *9 Companies Using Blockchain in Insurance to Revolutionize Possibilities.* Ανακτήθηκε 30 Ιουλίου, 2021 από https://builtin.com/blockchain/blockchain-insurance-companies

Dhillon S., (2018). *How Blockchain Can Transform The Future Of Entertainment.* Ανακτήθηκε 26 Ιουλίου, 2021 από https://www.forbes.com/sites/valleyvoices/2018/02/01/how-blockchain-can-transform-the-future-of-entertainment/?sh=276e8ad86b6b

IBM: *Benefits of Blockchain.* Ανακτήθηκε 25 Σεπτεμβρίου, 2021 από https://www.ibm.com/topics/benefits-of-blockchain

Koffman T., (2020). *How Blockchain Will Transform Media & Entertainment.* Ανακτήθηκε 26 Ιουλίου, 2021 από https://www.forbes.com/sites/tatianakoffman/2020/02/26/how-blockchain-will-transform-media--entertainment/?sh=5cbc06e71d1b

Locktrip: *LT BlockChain, Ecosystem & Marketplace DAPP.* Ανακτήθηκε 28 Ιουλίου, 2021 από https://locktrip.com/whitepaper_v1.2_t.pdf

Patientory: *Changing healthcare from the ground up.* Ανακτήθηκε 3 Σεπτεμβρίου, 2021 από https://patientory.com/about

Osborne C,. (2020). *2020's worst cryptocurrency breaches, thefts, and exit scams.* Ανακτήθηκε 26 Σεπτεμβρίου 2021, από https://www.zdnet.com/article/2020s-worst-cryptocurrency-breaches-thefts-and-exit-scams/

Osborne C,. (2019). *Cryptocurrency cyberattacks and breaches of 2019 (in pictures).* Ανακτήθηκε 26 Σεπτεμβρίου, 2021, από https://www.zdnet.com/pictures/the-worst-cryptocurrency-catastrophes-cyberattacks-and-breaches-of-2019-in-pictures/

Reiff N. (2021). *How to Buy Ripple (XRP) Cryptocurrency*. [Review by Rasure E.]. Ανακτήθηκε 28 Ιουλίου, 2021 από https://www.investopedia.com/tech/ripple-xrp-cryptocurrency-how-to-buy/

TradingPlatforms: *Best Trading Platform Canada 2021 – Cheapest Platform Revealed*. Ανακτήθηκε 29 Ιουλίου, 2021 https://smarttripplatform.io/

Wayner P., (2015). *The hidden dangers of blockchain: An essential guide for enterprise use.* Ανακτήθηκε 29 Ιουλίου, 2021 από https://techbeacon.com/security/hidden-dangers-blockchain-essential-guide-enterprise-use