

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ:

**ΔΙΑΣΦΑΛΙΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΜΕ ΤΗ ΧΡΗΣΗ ΤΗΣ
ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN**



ΚΕΤΣΕΑΣ ΣΤΑΥΡΟΣ Ε15061

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΑΜΠΡΙΝΟΥΛΑΚΗΣ

ΠΕΙΡΑΙΑΣ 2019-2020

Αφιερώσεις και ευχαριστίες

Αφιερώνω την πτυχιακή μου εργασία στους γονείς μου, Θεόδωρο Κετσέα και Κατερίνα Σαμπατακάκη και στον αδερφό μου Δημήτριο Κετσέα...

Θα ήθελα να ευχαριστήσω ιδιαίτερα τους καθηγητές μου, τον Κο. Κωνσταντίνο Λαμπρινουδάκη και την Κα. Δήμητρα Γεωργίου για την συνεχή και άμεση υποστήριξη και καθοδήγησή τους στην εργασία αυτή...

0. Περίληψη

Το Blockchain έχει γίνει μια από τις πιο δημοφιλείς τεχνολογίες για τη δημιουργία και διαχείριση ψηφιακών συναλλαγών πρόσφατα. Χρησιμοποιεί ως αμετάβλητο λογιστικό μητρώο (immutable ledger) που επιτρέπει τις συναλλαγές να πραγματοποιούνται με αποκεντρωμένο τρόπο. Αυτή η ταχέως εξελισσόμενη τεχνολογία έχει τη δυνατότητα να οδηγήσει σε αλλαγή του τρόπου σκέψης σχετικά με τις ψηφιακές συναλλαγές σε πολλούς τομείς, όπως το Διαδίκτυο των πραγμάτων (IoT), η υγειονομική περίθαλψη, η ενέργεια, η αλυσίδα εφοδιασμού, η μεταποίηση, η ασφάλεια στον κυβερνοχώρο και κυρίως οι χρηματοπιστωτικές υπηρεσίες. Ωστόσο, αυτή η αναδυόμενη τεχνολογία είναι ακόμη σε πρώιμο στάδιο και κάθε μέρα προσπαθούμε να την κατανοήσουμε όλο και περισσότερο και να την αξιοποιήσουμε με τον βέλτιστο δυνατό τρόπο. Παρά τις τεράστιες ευκαιρίες που προσφέρει το blockchain, υποφέρει από προκλήσεις και περιορισμούς, όπως η επεκτασιμότητα (scalability), η ασφάλεια, η προστασία της ιδιωτικής ζωής, η συμμόρφωση (compliance) και τα ζητήματα διακυβέρνησης που δεν έχουν ακόμη διερευνηθεί και αντιμετωπιστεί διεξοδικά. Παρόλο που υπάρχουν μερικές μελέτες σχετικά με τα θέματα ασφάλειας και προστασίας της ιδιωτικής ζωής του blockchain, δεν υπάρχει ολοκληρωμένη εξέταση της ασφάλειας των συστημάτων blockchain. Αυτή η πτυχιακή εργασία περιέχει μια εκτενή έρευνα των απειλών για την ασφάλεια των συστημάτων blockchain και επανεξετάζει τα υπάρχοντα τρωτά σημεία του Blockchain. Αυτά τα τρωτά σημεία οδηγούν στην εκτέλεση των διαφόρων απειλών ασφάλειας στην κανονική λειτουργία των πλατφορμών Blockchain. Επιπλέον, η εργασία αυτή παρέχει περιπτωσιολογικές μελέτες, για κάθε είδους επίθεση, εξετάζοντας τα δημοφιλή συστήματα blockchain και προτείνοντας, επίσης, πιθανά αντίμετρα που θα μπορούσαν να χρησιμοποιηθούν στην ανάπτυξη διαφόρων συστημάτων blockchain. Αυτά όλα δύναται να συμβάλουν ευεργετικά στο έργο των προγραμματιστών και των επιχειρήσεων, ώστε να είναι προσεκτικοί στις υφιστάμενες απειλές σε διαφορετικούς τομείς των πλατφορμών που βασίζονται σε blockchain και να σχεδιάζουν ανάλογα για να μετριάσουν τους κινδύνους, αλλά και σε οποιονδήποτε θέλει να εμπλουτίσει τις γνώσεις του αναφορικά με την τεχνολογία blockchain και να αποκτήσει εμπεριστατωμένες γνώσεις. Τέλος, συνοψίζονται οι κρίσιμες και ανοικτές προκλήσεις και προτείνονται οι μελλοντικές κατευθύνσεις της έρευνας του blockchain.

Πίνακας Περιεχομένων

0. Περίληψη	2
1. Εισαγωγή	6
2. Λεξιικό	9
3. Blockchain η ιδέα	14
3.1. Στοιχεία/Elements του Blockchain	16
3.2. Αρχιτεκτονική του Blockchain	19
3.3. Αλγόριθμοι Συναίνεσης (Consensus)	21
3.4. Τύποι Blockchain	26
4. Προβλήματα ασφάλειας και διασφάλισης ιδιωτικότητας	29
4.1. Απαιτήσεις ασφάλειας	30
4.2. Θέματα ασφάλειας χαμηλού επιπέδου	32
4.3. Θέματα ασφάλειας μεσαίου επιπέδου	33
4.4. Θέματα ασφάλειας υψηλού επιπέδου	36
4.5. Ρίσκα στο blockchain	37
4.6 Σενάρια Επιθέσεων/Attack cases	47
4.7. Προβλήματα ασφάλειας στο blockchain	52
4.7.1. Τεχνικοί περιορισμοί	53
4.7.2. Πιθανός κίνδυνος εφαρμογής κρυπτογραφίας	53
4.7.3. Οι πλατφόρμες Blockchain Opensource προσελκύουν έντονες επιθέσεις	54
4.7.4. Διαχείριση της ασφάλειας της αυτο-οργάνωσης και της ανωνυμίας	54
5. Λύσεις για εξειδικευμένες απειλές	55
5.1. Λύσεις ασφάλειας και διασφάλισης ιδιωτικότητας χαμηλού επιπέδου	55
5.2. Λύσεις ασφάλειας και διασφάλισης ιδιωτικότητας μεσαίου επιπέδου	59
5.3. Λύσεις ασφάλειας και διασφάλισης ιδιωτικότητας υψηλού επιπέδου	65
5.4. Περισσότερες λύσεις ασφάλειας και διασφάλισης ιδιωτικότητας με τη χρήση Blockchain	67
5.4.1. Ιστορικό	67
5.4.2. Πιθανές λύσεις σε Blockchain	69
5.5. Βελτιώσεις της ασφάλειας και διασφάλισης ιδιωτικότητας	71
5.5.1. SmartPool	72
5.5.2. Ποσοτικό πλαίσιο	73
5.5.3. Oyente	73
5.5.4. Hawk	74
5.5.5. Town Crier	75
5.6. Ασφαλείς Λύσεις Blockchain στο Cloud Computing	76
6. Case studies στο Blockchain	80

6.1. Blockchain στην υγεία	80
6.2. Blockchain στην οικονομία.	82
6.3. Blockchain στην αυτοκινητοβιομηχανία.	83
6.4. Blockchain στο Internet of Things.....	85
6.5. Blockchain σε κινητές εφαρμογές.	86
6.6. Blockchain στην άμυνα.	87
7. Προκλήσεις και δυνατότητες.....	88
7.1. Προκλήσεις.....	89
7.1.1. Ευελιξία.	89
7.1.2. Διαρροή απορρήτου.....	89
7.1.3. Εγωιστική εξόρυξη.	89
7.1.4. Προσωπικά αναγνωρίσιμα στοιχεία.....	90
7.1.5. Ασφάλεια.	90
7.2. Ευκαιρίες.	90
7.2.1. Στρατηγική ευθυγράμμιση και διακυβέρνηση.....	90
7.2.2. Τεχνολογία της πληροφορίας.....	91
7.2.3. Άλλες προοπτικές του κλάδου.....	93
7.3. Επιπλέον προκλήσεις.....	95
7.3.1. Περιορισμοί πόρων.....	95
7.3.2. Ετερογενείς συσκευές.....	96
7.3.3. Διαλειτουργικότητα των πρωτοκόλλων ασφαλείας.....	96
7.3.4. Ενιαία σημεία αποτυχίας.	96
7.3.5. Σφάλματα υλικού / υλικολογισμικού.....	96
7.3.6. Εμπιστευτικές ενημερώσεις και διαχείριση.....	97
7.3.7. Αδυναμίες μπλοκαρίσματος.....	97
7.3.8. Διακανονισμός Blockchain.....	97
7.3.9. Ασφάλεια Συναλλαγών.....	98
7.3.10. Ασφάλεια του Πορτοφολιού.....	98
7.3.11. Ασφάλεια Λογισμικού.....	99
8. Συμπεράσματα	101
9. Αναφορές/βιβλιογραφία.....	102

Λίστα Πινάκων

Πίνακας 1. Δομή κατασκευής ενός blockchain	14
Πίνακας 2. Elements του blockchain	16
Πίνακας 3. Δομή του blockchain	20
Πίνακας 4. Αλγόριθμοι συναίνεσης	22
Πίνακας 5 Τύποι Blockchain	26
Πίνακας 6. Αναπαράσταση των τύπων blockchain	28
Πίνακας 7. Θέματα ασφάλειας χαμηλού επιπέδου	33
Πίνακας 8. Θέματα ασφάλειας μεσαίου επιπέδου	36
Πίνακας 9. Θέματα ασφάλειας υψηλού επιπέδου	37
Πίνακας 10. Ταξινόμηση των ρίσκων στο blockchain	38
Πίνακας 11. Οι 10 κατηγορίες των πιο διαθέσιμων αντικειμένων στο Silk Road	40
Πίνακας 12. Μοντέλο διπλής δαπάνης(double spending) έναντι γρήγορης πληρωμής στο Bitcoin	41
Πίνακας 13. Παράδειγμα κλοπής κωδικού πρόσβασης	42
Πίνακας 14. Προαναφερθείσες ευπάθειες και αίτια αυτών	45
Πίνακας 15. Τα under-optimized patterns και η κατηγορία στην οποία ανήκουν	47
Πίνακας 16. Τροποποίηση Gas στο EIP150	47
Πίνακας 17. Επιθέσεις που εκμεταλλεύονται τις ευπάθειες των έξυπνων συμβολαίων	49
Πίνακας 18. Μερικές ακόμη επιθέσεις που δύναται να προκληθούν από την επίθεση eclipse	50
Πίνακας 19. Σύνοψη της διαδικασίας επίθεσης Liveness	50
Πίνακας 20. Λύσεις σε θέματα ασφάλειας χαμηλού επιπέδου	57
Πίνακας 21. Λύσεις σε θέματα ασφάλειας μεσαίου επιπέδου	58
Πίνακας 22. Λύσεις σε θέματα ασφάλειας Υψηλού επιπέδου	59
Πίνακας 23. Βελτίωση ασφάλειας και διασφάλισης ιδιωτικότητας με Smart Pool	72
Πίνακας 24. Βελτίωση ασφάλειας και διασφάλισης ιδιωτικότητας με Oyente	74
Πίνακας 25. Βελτίωση ασφάλειας και διασφάλισης ιδιωτικότητας με Town Crier	76
Πίνακας 26. Λύσεις Blockchain στο Cloud Computing	78
Πίνακας 27. Παροχές του blockchain	79
Πίνακας 28. Blockchain Case Studies	80
Πίνακας 29. Blockchain στην Υγεία	81
Πίνακας 30. Blockchain στην Οικονομία	83
Πίνακας 31. Blockchain στην Αυτοκινητοβιομηχανία	84
Πίνακας 32. Blockchain στην αυτοκινητοβιομηχανία	86
Πίνακας 33. Blockchain σε Κινητές Εφαρμογές	87

1. Εισαγωγή

Ένα blockchain είναι ένας κατακεντρωμένος, αποκεντρωμένος ημερολόγιο ή βάση δεδομένων που διευκολύνει τη διαδικασία καταγραφής συναλλαγών (ψηφιακών συμβάντων) στο επιχειρηματικό δίκτυο. Με άλλα λόγια, ένα Blockchain είναι μια κατακεντρωμένη, συναλλακτική (transactional) βάση δεδομένων που μοιράζεται σε όλους τους κόμβους που συμμετέχουν στο δίκτυο. Κάθε συναλλαγή στο δημόσιο βιβλίο επαληθεύεται με συναίνεση της πλειοψηφίας των συμμετεχόντων στο δίκτυο. Μόλις επαληθευτεί η συναλλαγή στο μπλοκ και προστεθεί στο blockchain, είναι σχεδόν αδύνατο να διαγραφούν ή να μεταβληθούν οι εγγραφές. Το Bitcoin είναι η πρώτη εφαρμογή του Blockchain, που εισήχθη το 2009 (Satoshi Nakamoto). Το Bitcoin είναι ένα κρυπτογραφικά ασφαλές ηλεκτρονικό σύστημα πληρωμών ή ένα κρυπτονόμισμα, το οποίο χρησιμοποιεί την τεχνολογία P2P (Peer-to-Peer) και λειτουργεί χωρίς καμία αρχή trusted third-party, όπως μια τράπεζα ή άλλα κεντρικά ιδρύματα. Ο ιδιοκτήτης του Bitcoin μπορεί να το χρησιμοποιήσει οπουδήποτε, ανά πάσα στιγμή χωρίς να εμπλέκεται με καμία κεντρική αρχή. Από την εισαγωγή του Bitcoin, το Blockchain έχει δείξει πολλά υποσχόμενες προοπτικές εφαρμογής και έχει προσελκύσει την προσοχή τόσο από τον ακαδημαϊκό χώρο όσο και από το βιομηχανικό χώρο. Ο λόγος ενδιαφέροντος για το Blockchain είναι τα χαρακτηριστικά του που παρέχουν ασφάλεια, ανωνυμία και ακεραιότητα δεδομένων, χωρίς να εμπλέκεται τρίτος στον έλεγχο των συναλλαγών.

Η τεχνική Blockchain έχει εφαρμοστεί σε πολλούς άλλους κλάδους, όπως το Διαδίκτυο των πραγμάτων (IoT), η υγειονομική περίθαλψη, η αλυσίδα εφοδιασμού, η μηχανική λογισμικού, η ασφάλεια στον κυβερνοχώρο και ούτω καθεξής. Με την εισαγωγή έξυπνων συμβάσεων, το blockchain σηματοδοτεί την έναρξη της εποχής του blockchain 2.0. Μια έξυπνη σύμβαση είναι ένα πρόγραμμα ηλεκτρονικού υπολογιστή που ελέγχει άμεσα τη μεταφορά περιουσιακών στοιχείων μεταξύ των μερών μιας συναλλαγής, κάτω από συγκεκριμένες συνθήκες. Μια έξυπνη σύμβαση όχι μόνο ορίζει κανόνες και κυρώσεις γύρω από μια συμφωνία όπως συμβαίνει σε μια συμβατική σύμβαση, αλλά μπορεί επίσης αυτομάτως να επιβάλλει αυτές τις υποχρεώσεις. Το Ethereum είναι μια νέα γενιά έξυπνης σύμβασης και αποκεντρωμένης πλατφόρμας εφαρμογής, αξιοποιώντας το blockchain, που εισήγαγε το έξυπνο συμβόλαιο. Το Ethereum είναι πλέον η πιο ευρέως χρησιμοποιούμενη έξυπνη πλατφόρμα συμβολαίων.

Δεδομένου ότι η τεχνολογία blockchain έχει ήδη προσελκύσει πολλούς κλάδους, υπάρχουν ορισμένες βασικές προκλήσεις που εξακολουθούν να δημιουργούν τεράστιες ανησυχίες όπως η ασφάλεια, η ιδιωτικότητα, η κλιμάκωση, η συμμόρφωση και η διακυβέρνηση.

Σήμερα υπάρχουν χιλιάδες έργα που βασίζονται σε Blockchain και λειτουργούν παρέχοντας διάφορες υπηρεσίες. Αυτές οι πλατφόρμες προσφέρουν υπηρεσίες, όπως χρηματοοικονομικές υπηρεσίες, έξυπνη οικονομία, IoT, πράσινη ενέργεια, ηλεκτρονική εκπαίδευση, κοινωνικά μέσα, έλεγχο, cloud, μηχανική, υγειονομική περίθαλψη, ασφάλεια στον κυβερνοχώρο και πολλά άλλα. Με την κεφαλαιοποίηση της αγοράς 117 δισεκατομμυρίων δολαρίων (7 Απριλίου 2018), το Bitcoin είναι η κορυφαία κρυπτογράφηση, η οποία είναι ένας ξεχωριστός στόχος των αντιπάλων. Η Ethereum είναι η δεύτερη μεγαλύτερη πλατφόρμα αποκλειστικής χρήσης που παρέχει έξυπνες συμβάσεις. Οι περισσότερες από τις υπάρχουσες πλατφόρμες μπλοκ αλυσίδων βασίζονται είτε στα πρωτόκολλα blockchain Bitcoin ή Ethereum.

Γιατί οι χάκερ επικεντρώνονται ολοένα και περισσότερο σε πλατφόρμες βασισμένες σε blockchain;

Από την επιχειρηματική σκοπιά, υπάρχουν τέσσερις επιθέσεις επιθέσεων στις πλατφόρμες blockchain.

- Οι περισσότερες υπάρχουσες πλατφόρμες τύπου blockchain παρέχουν ψηφιακά νομίσματα (κρυπτονόμισμα) για νομισματικούς σκοπούς, για να χρεώνουν τις υπηρεσίες τους. Για παράδειγμα, η Sia-blockchain που βασίζεται στην αποκεντρωμένη πλατφόρμα αποθήκευσης, απαιτεί από τα άτομα να πληρώσουν στο νόμισμα Sia για να νοικιάσουν την αποθήκευση. Επιπλέον, για να αγοράσουν ψηφιακό νόμισμα (ας υποθέσουμε τα νομίσματα Sia) χρησιμοποιούνται ψηφιακά χρηματιστήρια.

- Οι ανταλλαγές κρυπτονομισμάτων είναι επιχειρήσεις που επιτρέπουν στους πελάτες να εμπορεύονται κρυπτονομίσματα για άλλα περιουσιακά στοιχεία, όπως τα συμβατικά χρηματικά έσοδα ή άλλα ψηφιακά νομίσματα.
- Επιπλέον, μερικές από τις πλατφόρμες Blockchain, όπως η Bitcoin, η Ethereum και άλλοι, χρειάζονται εξόρυξη για να επαληθεύσουν τις συναλλαγές και να κυκλοφορήσουν νέα νομίσματα, καθώς δεν υπάρχει κεντρική αρχή όπως η τράπεζα για να ασχοληθεί με αυτές τις λειτουργίες.
- Για την πρόσβαση σε κέρματα, οι χρήστες χρειάζονται τα ιδιωτικά κλειδιά τους. Τα ιδιωτικά κλειδιά αποθηκεύονται σε πορτοφόλια και το πορτοφόλι παρέχει τις υπηρεσίες των ιδιωτικών κλειδιών των χρηστών και δημιουργεί επίσης συναλλαγές (στο όνομα του χρήστη) στα συστήματα blockchain. Όπως μπορούμε να δούμε, οι παραπάνω τέσσερις τομείς των πλατφορμών (κρυπτονόμισμα, ανταλλαγές, εξόρυξη και πορτοφόλι) συνεπάγονται αλληλεπίδραση με τα χρήματα και ενθαρρύνουν τους αντιπάλους να εκτελούν διάφορα hacks υψηλού κέρδους και κλοπές. Παρόλο που το blockchain θεωρείται ότι είναι απροσπέραστο, εξακολουθούν να υπάρχουν διαφορετικές απειλές για την ασφάλεια και την προστασία της ιδιωτικής ζωής στις πλατφόρμες blockchain, γεγονός που κάνει τη βιομηχανία χρηματοπιστωτικών υπηρεσιών να αναρωτιέται εάν η τεχνολογία blockchain μπορεί να γίνει αρκετά ασφαλής από τους εγκληματίες.

Η προβληματική κατάσταση

Από την κυκλοφορία του Bitcoin το 2009, στην αγορά υπάρχουν σχεδόν 1560 πλατφόρμες βασισμένες σε blockchain. Αυτές οι πλατφόρμες που βασίζονται σε blockchain εξυπηρετούν είτε απευθείας ως ηλεκτρονικό σύστημα πληρωμών (Bitcoin), είτε χρησιμοποιούν ψηφιακό νόμισμα για οικονομικούς σκοπούς για να χρεώνουν τις υπηρεσίες τους (Ethereum). Η χρήση του ψηφιακού νομίσματος από σχεδόν όλες τις δημόσιες πλατφόρμες έχει αυξήσει την οικονομία των κρυπτονομισμάτων σε ένα τεράστιο ποσοστό και τώρα αξίζει πάνω από 259 δισεκατομμύρια δολάρια. Η κεφαλαιοποίηση της αγοράς για την ίδια την Bitcoin τώρα αξίζει περισσότερο από 117 δισεκατομμύρια δολάρια. Αυτή η εκθετική αύξηση της αγοραίας αξίας των κρυπτονομισμάτων παρακινεί τους αντιπάλους να εκμεταλλευτούν την αδυναμία σε αυτές τις πλατφόρμες για κέρδος και οι ερευνητές να ανακαλύψουν νέα τρωτά σημεία στα συστήματα, να προτείνουν αντίμετρα και να προβλέψουν τις επικείμενες τάσεις. Διάφορες επιθέσεις, όπως η διπλή δαπάνη, η ελαχιστοποίηση της συναλλαγής, η επίθεση Sybil, οι επιθέσεις στο δίκτυο Blockchain, οι επιθέσεις σε ορυχεία (mining pools), τα σφάλματα στις έξυπνες συμβάσεις και το λογισμικό πορτοφολιών, δημιουργούν τεράστια προβλήματα ασφάλειας και προστασίας της ιδιωτικής ζωής στην αγορά.

Η εργασία στην επίλυση του προβλήματος

Παρόλο που υπάρχουν μερικές μελέτες σχετικά με τα θέματα ασφάλειας και προστασίας της ιδιωτικής ζωής του blockchain, δεν υπάρχει συστηματική εξέταση της ασφάλειας των συστημάτων blockchain. Η εργασία αυτή διεξήγαγε μια συστηματική έρευνα των απειλών για την ασφάλεια στα συστήματα blockchain και διερεύνησε τις σχετικές επιθέσεις. Αναλυτικότερα, στο Κεφάλαιο 2 γίνεται ομαλή εξοικείωση του αναγνώστη με τις βασικές έννοιες που θα κληθεί να κατανοήσει για να μπορέσει να εμβαθύνει στις πιο σύνθετες που ακολουθούν. Στο Κεφάλαιο 3 περιγράφεται η τεχνολογία blockchain, τα στοιχεία του, η αρχιτεκτονική και οι τύποι του, καθώς και οι αλγόριθμοι συναίνεσης, δίνοντας ξεκάθαρους ορισμούς και ολοκληρωμένες περιγραφές των αντίστοιχων εννοιών. Στο Κεφάλαιο 4 αναλύονται τα προβλήματα που προκύπτουν σε σχέση με την ασφάλεια και την διασφάλιση της ιδιωτικότητας. Ορίζονται οι δύο αυτές έννοιες και παρατίθενται τα ρίσκα, τα σενάρια επιθέσεων και οι κίνδυνοι που ελλοχεύουν. Στο Κεφάλαιο 5 συγκεντρώνονται οι λύσεις στις προαναφερθείσες απειλές και οι μέθοδοι αποφυγής τους. Στο Κεφάλαιο 6 αναπτύσσονται μερικά από τα πολυπληθή case studies του blockchain, όπως αυτά της υγείας, της οικονομίας, της αυτοκινητοβιομηχανίας, του Internet of Things (IoT), των κινητών εφαρμογών και της άμυνας. Στο Κεφάλαιο 7 η εργασία επικεντρώνεται στις προκλήσεις που καλείται να αντιμετωπίσει η νέα αυτή τεχνολογία του blockchain, καθώς και τις δυνατότητες που δημιουργεί για το μελλοντικές έρευνες και ακόμα μεγαλύτερη ανάπτυξη. Τέλος η εργασία ολοκληρώνεται με την παράθεση

προσωπικών συμπερασμάτων στο Κεφάλαιο 8. Το 9^ο Κεφάλαιο περιέχει όλες τις βιβλιογραφικές αναφορές. Αυτή η εργασία θα βοηθήσει τους προγραμματιστές και τους ερευνητές, καθώς και τις επιχειρήσεις να κατανοήσουν τη φύση των διαφόρων απειλών για την ασφάλεια και την διασφάλιση ιδιωτικότητας. Για παράδειγμα, οι απειλές για την ασφάλεια και την ιδιωτικότητα, θα μπορούσαν να επηρεάσουν τα διαφορετικά επίπεδα των συστημάτων blockchain ή τις διεργασίες του blockchain ή και στοχευμένους επιχειρησιακούς χρήστες. Συνεπώς είναι ένα θέμα μείζονος σημασίας, το οποίο καλείται αυτή η εργασία να διαλευκάνει.

2. Λεξικό

Σε αυτή την ενότητα αναλύονται μερικές από τις βασικότερες έννοιες/ορολογίες αναφορικά με το blockchain, οι οποίες επαναλαμβάνονται καθ' όλη την έκταση της εργασίας και βοηθούν στην ευκολότερη κατανόησή της. Μερικές από αυτές αναλύονται ακόμη περισσότερο στις αντίστοιχες ενότητες που ανήκουν. Προτείνεται κάθε φορά που βρίσκετε άγνωστη λέξη να ανατρέξετε σε αυτό το λεξικό.

- **Blockchain:** Ένα blockchain είναι ένα κοινό μητρώο όπου οι συναλλαγές καταγράφονται μόνιμα με την προσθήκη μπλοκ.
- **Block/Μπλοκ-κελί:** Τα μπλοκ είναι πακέτα δεδομένων που μεταφέρουν μόνιμα καταγεγραμμένα δεδομένα στο blockchain. Μια συλλογή συναλλαγών συγκεντρώνεται σε ένα μπλοκ που μπορεί στη συνέχεια να κρυπτογραφηθεί και να προστεθεί στο blockchain.
- **Bitcoin:** Το Bitcoin είναι η πρώτη αποκεντρωμένη κρυπτοεμφάνιση ανοιχτού κώδικα που τρέχει σε ένα παγκόσμιο δίκτυο ομότιμων. Είναι η πρώτη εφαρμογή του blockchain.
- **Κρυπτονόμισμα/Cryptocurrency:** Ονομάζεται ψηφιακό νόμισμα ή κρυπτονόμισμα και είναι αναπαραστάσεις ψηφιακών στοιχείων.
- **Central Ledger:** Ένα ημερολόγιο/λογιστικό μητρώο/βιβλίο που διατηρείται από μια κεντρική υπηρεσία.
- **Κατανεμημένο/Distributed Ledger:** Ημερολόγιο/λογιστικό μητρώο/βιβλίο στο οποίο τα δεδομένα αποθηκεύονται σε ένα δίκτυο αποκεντρωμένων κόμβων. Ένα διανεμημένο ημερολόγιο δεν χρειάζεται να έχει δικό του νόμισμα και μπορεί να πάρει άδεια και ιδιωτικό.
- **Διεύθυνση/Address:** Οι διευθύνσεις κρυπτογράφησης χρησιμοποιούνται για την αποστολή ή λήψη συναλλαγών στο δίκτυο.
- **Εξόρυξη/Mining:** Η εξόρυξη είναι η πράξη επικύρωσης συναλλαγών blockchain. Η ανάγκη επικύρωσης δικαιολογεί ένα κίνητρο για τους ανθρακωρύχους, συνήθως με τη μορφή νομισμάτων. Ονομάζεται επίσης ανταμοιβή του blockchain.
- **Δυσκολία/Difficulty:** Αυτό αναφέρεται στο πόσο εύκολα μπορεί να εξαχθεί με επιτυχία ένα μπλοκ δεδομένων των πληροφοριών συναλλαγής.

- **Πιρούνι/Fork:** Τα πιρούνια δημιουργούν μια εναλλακτική έκδοση του blockchain, αφήνοντας δύο μπλοκ αλυσίδες να τρέχουν ταυτόχρονα σε διαφορετικά μέρη του δικτύου.
- **Κόμβος/Node:** Ένα αντίγραφο του ημερολογίου που λειτουργεί ως ένας συμμετέχων του δικτύου blockchain.
- **Συναίνεση/Consensus:** Η συναίνεση επιτυγχάνεται όταν όλοι οι συμμετέχοντες στο δίκτυο συμφωνούν για την εγκυρότητα των συναλλαγών, εξασφαλίζοντας ότι το βιβλίο/ημερολόγιο έχει ακριβή αντίγραφα μεταξύ τους.
- **Ευπάθεια/Vulnerability:** Αδυναμία ή βλάβη που μπορεί να οδηγήσει σε έκθεση.
- **Απειλή/Threat:** Γενικός όρος για αντικείμενα, ανθρώπους, άλλες οντότητες που αποτελούν συνεχή κίνδυνο για ένα περιουσιακό στοιχείο (μέσω επιθέσεων).
- **Απειλητικός πράκτορας/Threat agent:** Συγκεκριμένο αντικείμενο, άτομο που θέτει δυνητικό κίνδυνο (πραγματοποιώντας επίθεση). Η επίθεση DDoS αποτελεί απειλή. αν ένας χάκερ κάνει μια επίθεση DDoS, είναι ένας παράγοντας απειλής.
- **Vector:** Πώς πραγματοποιήθηκε η επίθεση, π.χ., κακόβουλο συνημμένο ηλεκτρονικού ταχυδρομείου.
- **Έκθεση/Exposure:** Μια επιτυχής επίθεση.
- **Περιστατικό/Incident:** Οποιαδήποτε επίθεση, ή όλες οι επιθέσεις που χρησιμοποιούν ευπάθεια X, κλπ.
- **Ρίσκο/Risk:** Η πιθανότητα ότι "κάτι κακό" συμβαίνει φορές αναμενόμενη ζημία στον οργανισμό.
- **Δίκτυο P2P:** Ένα δίκτυο υπολογιστών peer-to-peer (ή P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα.

- **Trusted Third Party/Αξιόπιστο τρίτο μέρος:** Στην κρυπτογραφία, ένα αξιόπιστο τρίτο μέρος (TTP) είναι μια οντότητα που διευκολύνει τις αλληλεπιδράσεις μεταξύ δύο μερών που εμπιστεύονται το τρίτο μέρος. το τρίτο μέρος εξετάζει όλες τις επικοινωνίες κρίσιμης συναλλαγής μεταξύ των μερών, με βάση την ευκολία δημιουργίας παράνομου ψηφιακού περιεχομένου. Στα μοντέλα TTP, τα εμπλεκόμενα μέρη χρησιμοποιούν αυτή την εμπιστοσύνη για να εξασφαλίσουν τις δικές τους αλληλεπιδράσεις. Τα TTP είναι κοινά σε οποιοδήποτε αριθμό εμπορικών συναλλαγών και σε κρυπτογραφικές ψηφιακές συναλλαγές καθώς και κρυπτογραφικά πρωτόκολλα, για παράδειγμα, μια αρχή πιστοποίησης (CA) θα εκδώσει ένα ψηφιακό πιστοποιητικό ταυτότητας σε ένα από τα δύο μέρη στο επόμενο παράδειγμα. Στη συνέχεια, η CA γίνεται το Αξιόπιστο τρίτο μέρος σε αυτή την έκδοση πιστοποιητικών. Ομοίως, οι συναλλαγές που χρειάζονται εγγραφή τρίτου μέρους θα χρειαστούν επίσης μια υπηρεσία αποθετηρίου τρίτου μέρους κάποιου είδους ή άλλου. «Εμπιστος» σημαίνει ότι ένα σύστημα πρέπει να έχει εμπιστοσύνη να ενεργεί προς το συμφέρον μας, αλλά έχει την επιλογή (είτε κατά βούληση είτε ακούσια) να αντιδράσει στα συμφέροντά μας. Το "αξιόπιστο" σημαίνει επίσης ότι δεν υπάρχει τρόπος να επαληθεύσει εάν το σύστημα αυτό λειτουργεί προς το συμφέρον μας, εξ ου και η ανάγκη εμπιστοσύνης. Συνέπεια: εάν ένα σύστημα μπορεί να επαληθευτεί ότι λειτουργεί για τα συμφέροντά μας, δεν θα χρειαζόταν την εμπιστοσύνη μας. Και αν μπορεί να αποδειχθεί ότι λειτουργεί ενάντια στα συμφέροντά μας, δεν θα το χρησιμοποιήσουμε.
- **Ηγούμενα μηδενικά/Leading Zeros:** Ένα ηγούμενο μηδενικό είναι κάθε 0 ψηφίο που έρχεται πριν από το πρώτο μη μηδενικό ψηφίο σε μια συμβολοσειρά αριθμών στη σημείωση θέσης|(positional notation). Για παράδειγμα, το διάσημο αναγνωριστικό του James Bond, 007, έχει δύο ηγετικά μηδενικά. Όταν τα ηγετικά μηδενικά καταλαμβάνουν τα σημαντικότερα ψηφία ενός ακέραιου αριθμού, θα μπορούσαν να παραμείνουν κενά ή να παραλειφθούν για την ίδια αριθμητική τιμή. Επομένως, η συνηθισμένη δεκαδική σημείωση των ακέραιων αριθμών δεν χρησιμοποιεί ηγετικά μηδενικά, εκτός από το ίδιο το μηδέν, το οποίο θα υποδείχθηκε αλλιώς ως κενή συμβολοσειρά. Ωστόσο, σε δεκαδικά κλάσματα αυστηρά μεταξύ -1 και 1, τα πρώτα ψηφία μηδενός μεταξύ του δεκαδικού και του πρώτου μη ψηφιακού ψηφίου είναι απαραίτητα για τη μεταφορά του μεγέθους ενός αριθμού και δεν μπορούν να παραληφθούν, ενώ τα ηγετικά μηδενικά που εμφανίζονται μετά το δεκαδικό σημείο και μετά το τελευταίο μη μηδενικό ψηφίο, μπορούν να παραλειφθούν χωρίς να αλλάξει η έννοια.
- **Έξυπνη Σύμβαση/Smart Contract:** Μια έξυπνη σύμβαση είναι ένα πρωτόκολλο ηλεκτρονικού υπολογιστή προοριζόμενο να διευκολύνει ψηφιακά και να επαληθεύσει ή να επιβάλει τη διαπραγμάτευση ή την εκτέλεση μιας σύμβασης. Οι έξυπνες συμβάσεις επιτρέπουν την εκτέλεση αξιόπιστων συναλλαγών χωρίς τρίτους. Οι συναλλαγές αυτές είναι εντοπίσιμες και μη αναστρέψιμες. Οι υποστηρικτές των έξυπνων συμβολαίων υποστηρίζουν ότι πολλά είδη συμβατικών ρητρών μπορούν να γίνουν μερικώς ή πλήρως αυτοεκτελέσιμα, αυτοεπιβαλλόμενα ή και τα δύο. Ο στόχος των έξυπνων συμβάσεων είναι να παράσχουν ασφάλεια ανώτερη από το παραδοσιακό δίκαιο των συμβάσεων και να μειώσουν τα άλλα κόστη συναλλαγών που συνδέονται με τη σύναψη συμβάσεων. Διάφορα κρυπτονομίσματα έχουν εφαρμόσει τύπους έξυπνων συμβάσεων.

- **Block Γέννησης/Genesis Block:** Ένα μπλοκ γενεάς/γέννησης είναι το πρώτο μπλοκ μιας αλυσίδας μπλοκ. Οι σύγχρονες εκδόσεις του Bitcoin τον χαρακτηρίζουν ως το μπλοκ 0, αν και οι πολύ πρώτες εκδόσεις το υπολογίζουν ως το μπλοκ 1. Το μπλοκ γέννησης είναι σχεδόν πάντα hardcoded στο λογισμικό των εφαρμογών που χρησιμοποιούν blockchain. Είναι μια ειδική περίπτωση που δεν αναφέρεται σε προηγούμενο block, και για το Bitcoin και σχεδόν όλα τα παράγωγά του, παράγει μια μη αξόδευτη επιδότηση (unspendable subsidy).
- **IoT(Internet of Things):** Το Διαδίκτυο των πραγμάτων (IoT) είναι ένα σύστημα αλληλένδετων υπολογιστικών συσκευών, μηχανικών και ψηφιακών μηχανών, αντικειμένων, ζώων ή προσώπων που διαθέτουν μοναδικά αναγνωριστικά στοιχεία (UID) και τη δυνατότητα μεταφοράς δεδομένων μέσω δικτύου χωρίς να απαιτείται από άνθρωπο-σε-άνθρωπο ή από άνθρωπο-σε-υπολογιστή αλληλεπίδραση. Ο ορισμός του Διαδικτύου των πραγμάτων έχει εξελιχθεί λόγω της σύγκλισης πολλαπλών τεχνολογιών, αναλύσεων σε πραγματικό χρόνο, μηχανικής μάθησης, αισθητήρων εμπορευμάτων και ενσωματωμένων συστημάτων. Τα παραδοσιακά πεδία των ενσωματωμένων συστημάτων, τα ασύρματα δίκτυα αισθητήρων, τα συστήματα ελέγχου, η αυτοματοποίηση (συμπεριλαμβανομένου του αυτοματισμού κατοικιών και των κτιρίων) και άλλα συμβάλλουν στην ενεργοποίηση του IoT. Στην αγορά των καταναλωτών, η τεχνολογία IoT είναι περισσότερο συνώνυμη με τα προϊόντα που εμπίπτουν στην έννοια του "έξυπνου σπιτιού", καλύπτοντας συσκευές και συσκευές (όπως φωτιστικά, θερμοστάτες, συστήματα οικιακής ασφάλειας και κάμερες και άλλες οικιακές συσκευές) πιο κοινά οικοσυστήματα και μπορούν να ελέγχονται μέσω συσκευών που σχετίζονται με αυτό το οικοσύστημα, όπως τα smartphones και τα έξυπνα ηχεία.
- **6LoWPAN:** Το 6LoWPAN είναι ένα αρκτικόλεξο του IPv6 σε δίκτυα χαμηλής κατανάλωσης ασύρματων δικτύων. Το 6LoWPAN είναι το όνομα μιας ομάδας εργασίας που συνάπτεται στην περιοχή του IoT (Internet of Things) του IETF. Η ιδέα του 6LoWPAN προέκυψε από την ιδέα ότι «το πρωτόκολλο του Διαδικτύου θα μπορούσε και πρέπει να εφαρμοστεί ακόμη και στις μικρότερες συσκευές» και ότι οι συσκευές χαμηλής ισχύος με περιορισμένες δυνατότητες επεξεργασίας θα πρέπει να μπορούν να συμμετέχουν στο IoT. Η ομάδα 6LoWPAN έχει ορίσει μηχανισμούς συμπίεσης (encapsulation) και συμπίεσης κεφαλίδων (header compression) που επιτρέπουν την αποστολή και λήψη πακέτων IPv6 μέσω δικτύων βασισμένων στο IEEE 802.15.4. Το IPv4 και το IPv6 είναι τα άλογα εργασίας για την παροχή δεδομένων για τοπικά δίκτυα, δίκτυα μητροπολιτικών περιοχών και δίκτυα ευρείας περιοχής όπως το Διαδίκτυο. Παρομοίως, οι συσκευές IEEE 802.15.4 παρέχουν δυνατότητα επικοινωνίας στον τομέα ασύρματης επικοινωνίας. Οι εγγενείς φύσεις των δύο δικτύων όμως είναι διαφορετικές.
- **Proof of Work (απόδειξη εργασίας) :** Η βάση για την εξόρυξη των ψηφιακών νομισμάτων είναι ένας αλγόριθμος, που ονομάζεται Proof of Work (PoW). Το ακρωνύμιο PoW εκφράζει ένα «υπολογιστικό ή κρυπτογραφικό πρόβλημα» και μεταφράζεται στην ελληνική γλώσσα ως «απόδειξη εργασίας». Όταν κάποιος δηλαδή επιλύει σωστά το τιθέμενο πρόβλημα, αποδεικνύει, ότι η αρχή λειτουργεί (απόδειξη εργασίας). Μετά την επίλυση του κρυπτογραφικού προβλήματος ο αλγόριθμος παρέχει στους χρήστες που το έλυσαν μια ανταμοιβή. Γιατί επαλήθευσαν επιτυχώς συναλλαγές και με αυτόν τον τρόπο δημιούργησαν νέα μπλοκ στην αλυσίδα των μπλοκ.
- **Ethereum:** Το ethereum είναι μία αλυσίδα μπλοκ που επιτρέπει την εκτέλεση αποκεντρωμένων προγραμμάτων (dApps) και έξυπνων συμβολαίων. Το ethereum είναι η εναλλακτική λύση για την καθιερωμένη αρχιτεκτονική πελάτη-εξυπηρετητή.

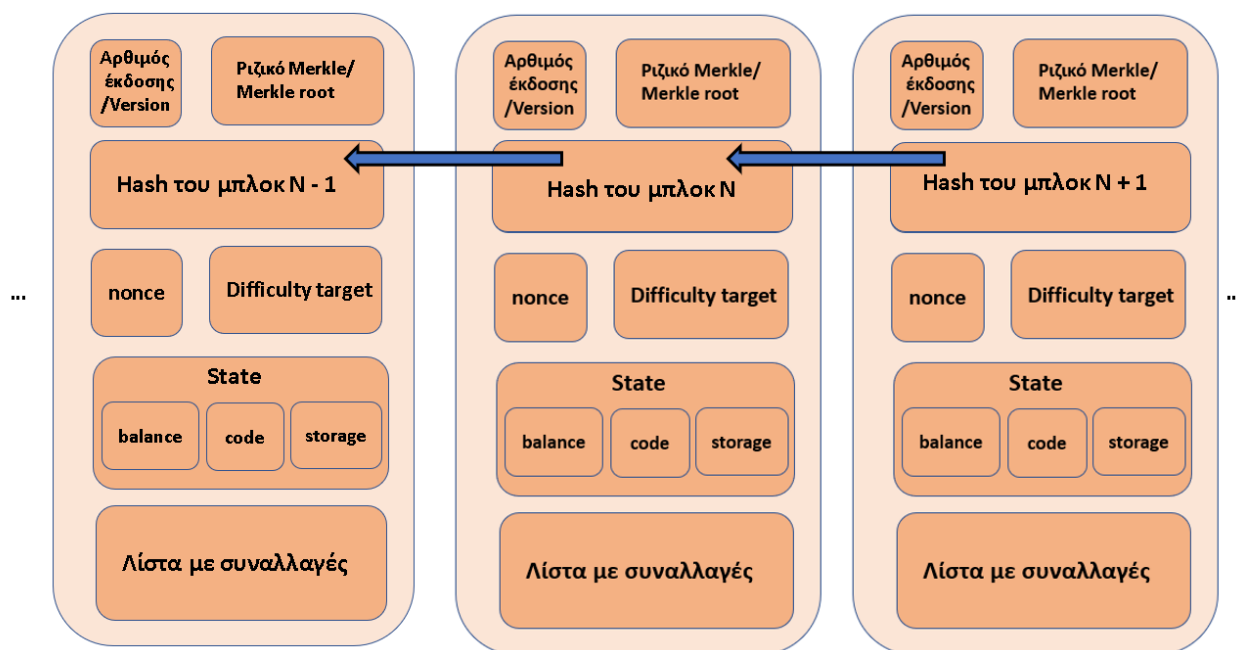
- **Hash Function (Κρυπτογραφημένη συνάρτηση κατακερματισμού):** Ο όρος κρυπτονόμισμα ήδη υποδεικνύει ότι υπάρχει μία σύνδεση μεταξύ του bitcoin κ.τ.λ. από την μία μεριά και της κρυπτογράφησης από την άλλη. Αυτή η σχέση εκδηλώνεται στην κρυπτογραφική συνάρτηση κατακερματισμού (hash function).

3. Blockchain η ιδέα

Ένα blockchain είναι ένα αποκεντρωμένο, κατανεμημένο, κοινόχρηστο και αμετάβλητο ημερολόγιο βάσεων δεδομένων (database ledger) που αποθηκεύει μητρώο δεδομένων (stores registry of assets) και συναλλαγών σε ένα δίκτυο peer-to-peer (P2P). Έχει αλυσιδωτά μπλοκ δεδομένων που έχουν επισημανθεί και επικυρωθεί από τους ανθρακωρύχους (miners). Το blockchain χρησιμοποιεί κρυπτογράφηση ελλειπτικής καμπύλης (ECC) και SHA-256 hashing για να παρέχει ισχυρή κρυπτογραφική απόδειξη για έλεγχο ταυτότητας και ακεραιότητα δεδομένων. Βασικά, τα δεδομένα μπλοκ περιέχουν μια λίστα με όλες τις συναλλαγές και ένα hash με το προηγούμενο μπλοκ. Το blockchain έχει ένα πλήρες ιστορικό όλων των συναλλαγών και παρέχει διασυννοριακή, παγκόσμια, κατανεμημένη εμπιστοσύνη. Τα εμπιστευμένα τρίτα μέρη (TTP-trusted third parties) ή οι κεντρικές αρχές και υπηρεσίες μπορούν να διαταραχθούν, να διακυβευθούν ή να υποπέσουν σε hacking. Μπορούν επίσης να παραβιαστούν και να καταστραφούν στο μέλλον, ακόμα κι αν είναι αξιόπιστα τώρα. Στο blockchain, κάθε συναλλαγή στο κοινό δημόσιο ημερολόγιο (shared public ledger) επαληθεύεται από την πλειοψηφική συναίνεση (majority consensus) των miner κόμβων που συμμετέχουν ενεργά στην επαλήθευση και επικύρωση των συναλλαγών. Σε ένα δίκτυο bitcoin [10] οι ανθρακωρύχοι (miners) επικυρώνουν το μπλοκ υπολογίζοντας ένα hash με αρχικά μηδενικά (leading zeros) ώστε να φτάσουν την επιθυμητή δυσκολία. Μόλις οι συναλλαγές επικυρωθούν και επαληθευτούν με συναίνεση (by consensus), τα μπλοκ που περιέχουν τα δεδομένα είναι αμετάβλητα, δηλ. τα δεδομένα δεν μπορούν ποτέ να διαγραφούν ή να μεταβληθούν. Το blockchain μπορεί να κατασκευαστεί ως:

- (1) δίκτυο με άδεια (ή ιδιωτικό) (permissioned or private) που μπορεί να περιοριστεί σε μια συγκεκριμένη ομάδα συμμετεχόντων ή
- (2) δίκτυο χωρίς άδεια ή δημόσιο δίκτυο (permission-less or public) που είναι ανοικτό για οποιονδήποτε να συμμετέχει, προσδίδοντας καλύτερο έλεγχο πρόσβασης.

Ο πρώτος πίνακας απεικονίζει μια τυπική δομή κατασκευής ενός Blockchain.

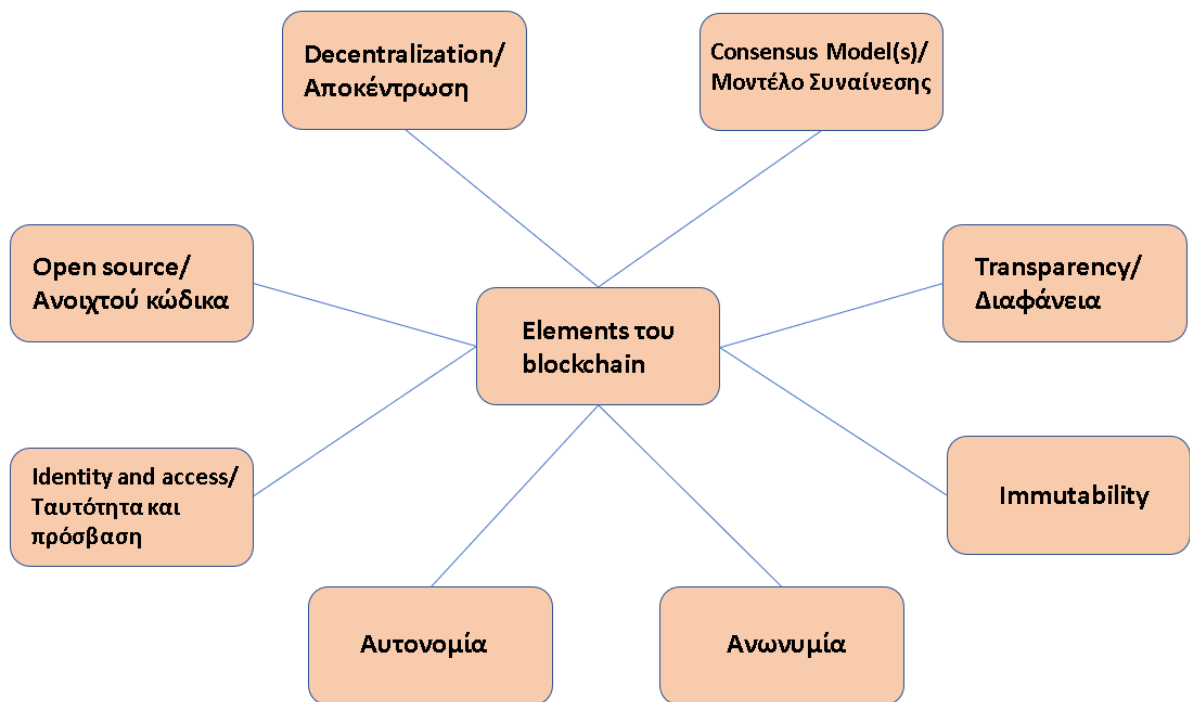


Πίνακας 1. Δομή κατασκευής ενός blockchain

Η δομή του σχεδίου αποτελείται κυρίως από την κεφαλίδα του μπλοκ και το σώμα του μπλοκ που περιέχει έναν κατάλογο συναλλαγών. Η κεφαλίδα του μπλοκ περιέχει διάφορα πεδία, ένα από τα οποία είναι ένας αριθμός έκδοσης για την παρακολούθηση του λογισμικού αναβάθμισης πρωτοκόλλων. Επίσης, η κεφαλίδα περιέχει μια χρονική σήμανση, το μέγεθος του μπλοκ και τον αριθμό των συναλλαγών. Το ριζικό πεδίο Merkle (merkle root field) αντιπροσωπεύει την τιμή κατακερματισμού του τρέχοντος μπλοκ. Το Merkle tree hashing χρησιμοποιείται συνήθως σε καταναμημένα συστήματα και δίκτυα P2P για αποτελεσματική επαλήθευση δεδομένων. Το πεδίο nonce χρησιμοποιείται για τον αλγόριθμο απόδειξης εργασίας (PoW) και είναι η τιμή του μετρητή δοκιμής (trial counter value) που παρήγαγε το hash με αρχικά μηδενικά (leading zeros). Η δυσκολία καθορίζει τον αριθμό των αρχικών μηδενικών και χρησιμοποιείται για να διατηρήσει το blocktime περίπου 10 λεπτά για το Bitcoin [1] και 17,5 s για το Ethereum [2]. Η δυσκολία ρυθμίζεται περιοδικά και αυξάνεται (με περισσότερα αρχικά μηδενικά) καθώς η υπολογιστική ισχύς του υλικού αυξάνεται με την πάροδο του χρόνου. Το blocktime καθορίζεται εξ' αρχής για να υπολογίσει το χρόνο διάδοσης των μπλοκ για να φτάσουν σε όλους τους ανθρακωρύχους (miners) και ώστε όλοι οι miners να συνεναίσουν (reach consensus).

Το Bitcoin είναι μία από τις πρώτες και τις πιο δημοφιλείς εφαρμογές που τρέχουν στην κορυφή της υποδομής blockchain. Σε γενικές γραμμές, το bitcoin blockchain υπήρξε η βασική πλατφόρμα και η τεχνολογία πολλών από τα πιο δημοφιλή κρυπτονομίσματα σήμερα. Ωστόσο, με την έλευση του blockchain Ethereum, το οποίο υλοποιεί έξυπνες συμβάσεις, ο πιθανός χώρος χρήσης για blockchain έχει γίνει ατελείωτος. Το blockchain Ethereum εγκαινιάστηκε και ανοίχθηκε για χρήση στο κοινό τον Ιούλιο του 2015. Στη συνέχεια, αναδείχθηκαν πρόσφατα παρόμοιες πλατφόρμες έξυπνων συμβολαίων. Αυτά περιλαμβάνουν το Hyperledger [3], το Eris [4], το Stellar [5], το Ripple [6] και το Tendermint [7]. Σε αντίθεση με το bitcoin blockchain που χρησιμοποιείται κυρίως για συναλλαγές με ψηφιακό νόμισμα, το Ethereum blockchain έχει τη δυνατότητα να αποθηκεύει αρχεία και, κυρίως, να τρέχει έξυπνες συμβάσεις. Ο όρος "έξυπνες συμβάσεις" επινοήθηκε για πρώτη φορά από τον Nick Szabo το 1994. Μια έξυπνη σύμβαση είναι βασικά ένα μηχανογραφημένο πρωτόκολλο συναλλαγών που εκτελεί τους όρους της σύμβασης. Στον απλουστευμένο ορισμό, τα έξυπνα συμβόλαια είναι προγράμματα γραμμένα από τους χρήστες που πρόκειται να μεταφορτωθούν και να εκτελεστούν στο blockchain. Η γλώσσα προγραμματισμού για έξυπνες συμβάσεις ονομάζεται Στερεότητα (Solidity), που είναι μια γλώσσα που μοιάζει με JavaScript. Το Ethereum Blockchain παρέχει EVM (Εικονικές Μηχανές Ethereum -Ethereum Virtual Machines) οι οποίες είναι βασικά οι miner κόμβοι. Αυτοί οι κόμβοι είναι σε θέση να παρέχουν αξιόπιστη εκτέλεση και επιβολή αυτών των προγραμμάτων ή συμβολαίων κρυπτογραφημένα.

Το Ethereum υποστηρίζει το δικό του ψηφιακό νόμισμα που ονομάζεται Ether. Όπως και στο bitcoin, έτσι και στο Ethereum, οι χρήστες μπορούν να μεταφέρουν κέρματα ο ένας στον άλλο χρησιμοποιώντας κανονικές συναλλαγές που καταγράφονται στο ημερολόγιο (on the ledger), και για τέτοιες συναλλαγές, δεν υπάρχει ανάγκη για blockchain στο bitcoin. Εντούτοις, για την υποστήριξη της έξυπνης εκτέλεσης συμβολαίων της Ethereum, χρησιμοποιείται ένα blockchain, όπως φαίνεται στον δεύτερο πίνακα.



Πίνακας 2. Elements του blockchain

Ένα έξυπνο συμβόλαιο έχει δικό του λογαριασμό και διεύθυνση και έχει τον δικό του εκτελέσιμο κώδικα και υπόλοιπο νομισμάτων Ether. Η αποθήκευση είναι συνεχής και διατηρεί τον κώδικα που πρέπει να εκτελεστεί στους κόμβους EVM. Η αποθήκευση EVM είναι σχετικά ακριβή και για την αποθήκευση μεγάλου όγκου δεδομένων στο blockchain, μπορεί να χρησιμοποιηθεί ένα άλλο απομακρυσμένο αποκεντρωμένο store δεδομένων όπως το BitTorrent, το IPFS ή το Swarm. Εντούτοις, τα έξυπνα συμβόλαια μπορούν να περιέχουν ένα hash επικύρωσης τέτοιων απομακρυσμένων αποθηκευμένων πληροφοριών. Οι πιθανές περιπτώσεις χρήσης και οι εφαρμογές των εφαρμογών blockchain έξυπνης σύμβασης είναι τεράστιες και ατελείωτες, από την κρυπτογράφηση και τις συναλλαγές έως τις αυτόνομες συναλλαγές μηχανής με μηχανή (machine-to-machine), από την αλυσίδα εφοδιασμού και την παρακολούθηση στοιχείων έως τον αυτοματοποιημένο έλεγχο πρόσβασης και την κοινή χρήση και από την ψηφιακή ταυτότητα και την ψηφοφορία έως την πιστοποίηση, τη διαχείριση και τη διακυβέρνηση αρχείων, δεδομένων ή αντικειμένων. Οι εμπορικές τεχνολογίες που βασίζονται σε blockchain αυξάνονται γρήγορα. Για παράδειγμα, το SafeShare [8] έχει προσφέρει ασφαλιστική λύση χρησιμοποιώντας blockchain με βάση bitcoin. Ομοίως, η IBM ξεκίνησε το πλαίσιο blockchain χρησιμοποιώντας την πλατφόρμα Hyperledger Fabric [9]. Το πλαίσιο υποστηρίζει την ανάπτυξη εφαρμογών blockchain, και σε αντίθεση με άλλα πλαίσια, δεν απαιτεί κρυπτονόμισμα. Το blockchain της IBM χρησιμοποιείται εμπορικά σε τράπεζες, συστήματα εφοδιαστικής αλυσίδας και εταιρείες ναυτιλίας.

3.1. Στοιχεία/Elements του Blockchain.

Υπάρχουν πολλά στοιχεία blockchain και τα οκτώ πιο σημαντικά στοιχεία αναφέρονται σε αυτό το τμήμα.

•Decentralization/Αποκέντρωση.

Η αποκέντρωση είναι η διασπορά λειτουργιών και ελέγχων από μια κεντρική αρχή σε όλες τις εμπλεκόμενες μονάδες. Στο blockchain δεν υπάρχει κεντρική αρχή. Αντίθετα, κάθε χρήστης blockchain (miner) διαθέτει ένα αντίγραφο του βιβλίου συναλλαγών (transaction ledger) και προστίθεται ένα νέο μπλοκ επικυρώνοντας τη συναλλαγή από τους εμπλεκόμενους miners. Σε ένα αποκεντρωμένο περιβάλλον, το δίκτυο λειτουργεί με βάση το χρήστη (peer-to-peer) (χρήστης προς χρήστη). Οι ερευνητές χρησιμοποιούν αυτό το στοιχείο του blockchain ως μία από τις σημαντικότερες πτυχές στην ανάπτυξη του ψηφιακού νομίσματος Ethereum.

•Consensus model(s)/Μοντέλο(-α) συναίνεσης (consensus model).

Τα μοντέλα συναίνεσης συμβάλλουν στη διατήρηση της ιεράρχησης των δεδομένων που καταγράφονται σε ένα blockchain. Στο [10], αναφέρεται ότι διάφοροι μηχανισμοί και ζητήματα συναίνεσης θα μπορούσαν να προκύψουν όταν ο μηχανισμός συναίνεσης αποτύχει, συμπεριλαμβανομένων των blockchain forks, των αποτυχιών συναίνεσης, των ζητημάτων κυριαρχίας (dominance issues), των επικυρωμένων κόμβων και των ικανοποιητικών επιδόσεων του δικτύου blockchain [11]. Ένα πρωτόκολλο συναίνεσης έχει τρεις ιδιότητες βασισμένες στην εφαρμοσιμότητα και την αποτελεσματικότητα:

- **Ασφάλεια (safety):** Ένα πρωτόκολλο συναίνεσης πρέπει να είναι ασφαλές και συνεπές, που σημαίνει ότι όλοι οι κόμβοι πρέπει να παράγουν την ίδια έξοδο η οποία είναι έγκυρη σύμφωνα με τους κανόνες του πρωτοκόλλου.
- **Ζωτικότητα (Liveness):** Ένα πρωτόκολλο συναίνεσης υπόσχεται τη ζωτικότητα όλων των μη ελαττωματικών κόμβων για να παράξει μια τιμή.
- **Αντοχή σφάλματος (Fault Tolerance):** Ένα πρωτόκολλο συναίνεσης παρέχει ανοχή, ενώ παρέχει ανάκτηση (recovery), σε έναν ελαττωματικό κόμβο που συμμετέχει στη συναίνεση.

•Transparent/Διαφάνεια.

Το δίκτυο blockchain ελέγχει συνήθως με τον εαυτό του κάθε δέκα λεπτά προκειμένου να ελέγξει αυτόματα το οικοσύστημα μιας ψηφιακής τιμής, που συνδιαλλάσσει τις συναλλαγές που συμβαίνουν σε διαστήματα δέκα λεπτών. Μια συλλογή από αυτές τις συναλλαγές αναφέρεται ως «block». Δημιουργούνται δύο ιδιότητες που προκύπτουν. Αυτές είναι η διαφάνεια (transparency) και η αδυναμία της διαφθοράς (inability of corruption).

•Open source/Ανοιχτή πηγή-ανοιχτού κώδικα.

Μια αποκεντρωμένη εφαρμογή και μια εφαρμογή κλειστού κώδικα (closed source) χρειάζεται να προσδίδουν εμπιστοσύνη στον χρήστη, πρέπει δηλαδή η εφαρμογή είναι να αποκεντρωμένη και τα δεδομένα να μην είναι προσβάσιμα από μια κεντρική πηγή. Οι εφαρμογές κλειστού κώδικα λειτουργούν ως εμπόδιο στην υιοθέτησή τους από τους χρήστες. Η απήχηση σε ένα δίκτυο κλειστής πηγής (closed source network) παρατηρείται όταν η εφαρμογή προορίζεται για τη λήψη, τη διατήρηση ή τη μεταφορά χρημάτων των χρηστών. Παρόλο που είναι δυνατή η εκκίνηση μιας αποκεντρωμένης εφαρμογής κλειστής πηγής, το επίπεδο της δυσκολίας για την επίτευξη του επιθυμητού αποτελέσματος θα ήταν καταστροφικό, καθιστώντας προφανές για τους χρήστες να ευνοούν τους συμμετέχοντες ανοιχτού κώδικα (open source participants). Το open

sourcing μιας αποκεντρωμένης εφαρμογής τροποποιεί τη δομή των επιχειρηματικών πρακτικών, οι οποίες παλιότερα χρησιμοποιούσαν το Internet ως κοινό παρονομαστή.

•Identity and access/Ταυτότητα και προσβασιμότητα.

Η ταυτότητα και η προσβασιμότητα ενός blockchain σχετίζονται με τρία βασικά κριτήρια, όπως δημόσιο ή άδειο (public or permissionless), ιδιωτικό ή άδειο (private or permissioned), και κοινοπραξία (consortium) . Ένα ιδιωτικό blockchain περιορίζει τους χρήστες από το να έχουν την εξουσιοδότηση να επικυρώνουν συναλλαγές μπλοκ και να δημιουργούν έξυπνες συμβάσεις. Αυτό είναι κατάλληλο για τις παραδοσιακές επιχειρήσεις και τα μοντέλα διακυβέρνησης (governance models). Τα δημόσια blockchains έχουν σχεδιαστεί για να κόψουν τον μεσάζοντα έξω από τις συναλλαγές, διατηρώντας παράλληλα την ασφάλεια άθικτη. Σε δημόσια blockchains οποιοσδήποτε χρήστης με πρόσβαση στο διαδίκτυο μπορεί να συμμετάσχει στο δίκτυο συμμετέχοντας σε πιστοποιήσεις μπλοκ και δημιουργώντας έξυπνες συμβάσεις (smart contracts). Τα blockchains της κοινοπραξίας (consortium blockchains) είναι εν μέρει ιδιωτικά και επιτρέπουν σε ορισμένους προκαθορισμένους επιλεκτικούς κόμβους να έχουν πλήρη έλεγχο. Είναι ένα υποκατάστατο που επιτρέπει σε οποιονδήποτε τυχαίο χρήστη με σύνδεση στο διαδίκτυο να επαληθεύει τις συναλλαγές. Η πλατφόρμα όπως το ιδιωτικό blockchain παρέχει την αποτελεσματικότητα και την ιδιωτικότητα των συναλλαγών.

•Autonomy/Αυτονομία.

Ο κύριος στόχος της τεχνολογίας blockchain είναι η αλλαγή της εμπιστοσύνης από μια κεντρική αρχή σε ολόκληρο το δίκτυο χωρίς παρεμβολές. Κάθε κόμβος στο σύστημα blockchain μπορεί να μεταφέρει και να ενημερώνει με ασφάλεια τις πληροφορίες. Ένας αποκεντρωμένος αυτόνομος οργανισμός (DAO), ο οποίος συχνά κατηγοριοποιείται ως αποκεντρωμένος αυτόνομος φορέας (DAC-corporation), είναι ένας οργανισμός που ακολουθεί ένα σύνολο κανόνων που έχουν προκαθοριστεί ως προγράμματα ηλεκτρονικών υπολογιστών και ονομάζονται έξυπνες συμβάσεις. Το αρχείο των συναλλαγών και λεπτομέρειες των έξυπνων συμβάσεων διατηρούνται ως μπλοκ στο blockchain.

•Immutability/Μετατόπιση.

Η μετατόπιση είναι κάτι που δεν αλλάζει σε μια περίοδο. Στο πλαίσιο του blockchain, η μετατόπιση είναι συναφής με τα δεδομένα ή τις πληροφορίες που αποθηκεύονται στα μπλοκ. Μόλις τα δεδομένα ή οι πληροφορίες είναι γραμμένα σε ένα μπλοκ του blockchain, κανείς δεν μπορεί να το αλλάξει. Αυτό είναι ιδιαίτερα σημαντικό για τον έλεγχο των δεδομένων. Από τη μία πλευρά, ο πάροχος δεδομένων μπορεί να επαληθεύσει ότι τα δεδομένα είναι ασφαλή, αποτελεσματικά και δεν έχουν αλλοιωθεί ή τροποποιηθεί. Από την άλλη πλευρά, ο παραλήπτης των δεδομένων βεβαιώνεται ότι τα δεδομένα είναι αυθεντικά και αμετάβλητα. Το αμετάβλητο στοιχείο του blockchain είναι εξαιρετικά ευεργετικό για τις βάσεις δεδομένων που χρησιμοποιούνται στις χρηματικές συναλλαγές δεδομένου ότι τα αρχεία διατηρούνται για πάντα και δεν μπορούν να «κρεμαστούν» εκτός αν κάποιος παίρνει τον έλεγχο πάνω από το 51% των κόμβων του δικτύου ταυτόχρονα, αλλά θα μιλήσουμε για τους κινδύνους που ελλοχεύουν σε επόμενο κεφάλαιο.

•Anonymity/Ανωνυμία.

Η διεύθυνση blockchain ενός miner είναι απαραίτητη για αυτό το στοιχείο και καμία άλλη λεπτομέρεια δεν απαιτείται, με αποτέλεσμα η ανωνυμία να επιλύει τα θέματα

εμπιστοσύνης. Η ανωνυμία μιας οντότητας μέσα σε ένα σύνολο οντοτήτων δεν είναι διακριτή. Σε ένα σύστημα επικοινωνίας, το σύνολο ανωνυμίας μπορεί να χωριστεί σε δύο σύνολα: το σύνολο του αποστολέα και αυτό του παραλήπτη.

3.2. Αρχιτεκτονική του Blockchain.

Το Blockchain είναι ένας δημόσιος κατάλογος (ledger) που περιλαμβάνει διάφορες διεργασίες και η λειτουργία του blockchain περιλαμβάνει διάφορες διαδικασίες που αναλύονται ως εξής:

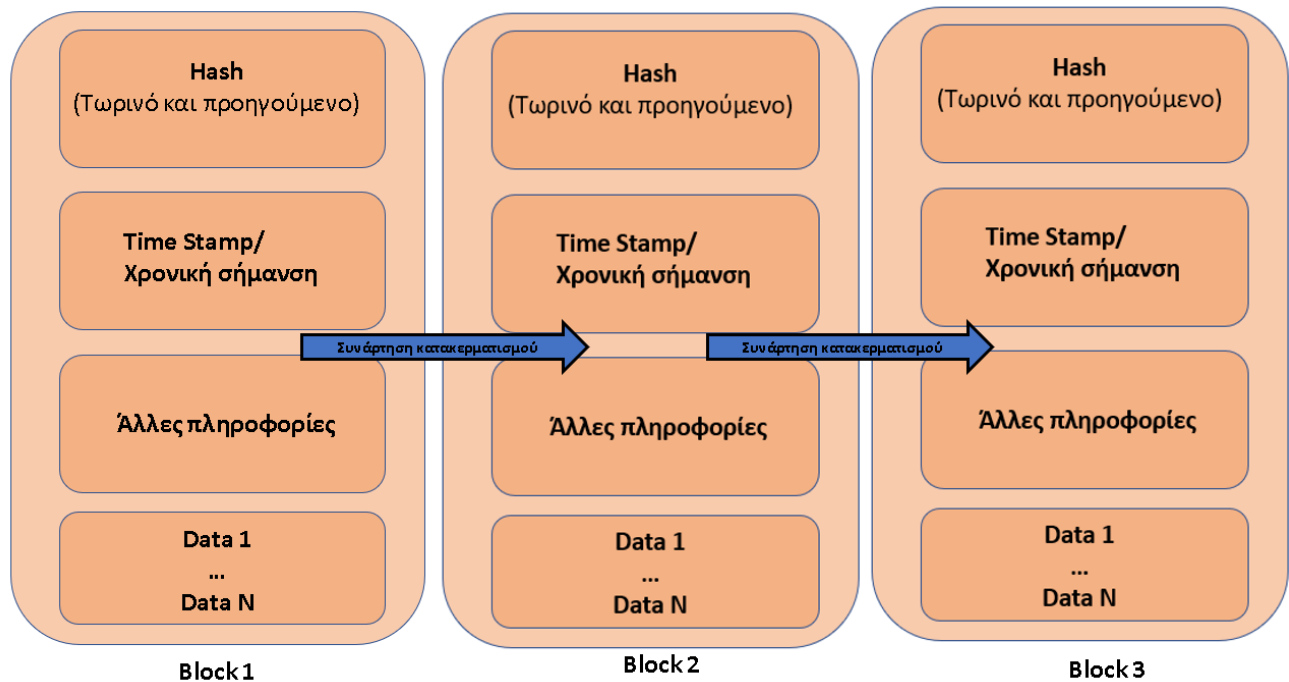
1. Ο κόμβος ή ο χρήστης που θέλει να ξεκινήσει μια συναλλαγή θα καταγράφει και θα μεταδίδει τα δεδομένα στο δίκτυο.
2. Ο κόμβος ή ο χρήστης που λαμβάνει τα δεδομένα επαληθεύει την αυθεντικότητα των δεδομένων που λαμβάνονται στο δίκτυο. Στη συνέχεια τα αποθηκευμένα δεδομένα αποθηκεύονται σε ένα μπλοκ.
3. Όλοι οι κόμβοι ή οι χρήστες του δικτύου επικυρώνουν τη συναλλαγή εκτελώντας είτε τον αλγόριθμο απόδειξης εργασίας (proof of work) είτε την απόδειξη του αλγορίθμου πονταρίσματος (proof of stake) στο μπλοκ που χρειάζεται επικύρωση.
4. Ο αλγόριθμος συναίνεσης που χρησιμοποιείται από το δίκτυο θα αποθηκεύσει τα δεδομένα στο μπλοκ που προστίθεται στο blockchain. Και όλοι οι κόμβοι στο δίκτυο δέχονται το αντίστοιχο μπλοκ και επεκτείνουν τη βάση της αλυσίδας στο μπλοκ.

Δομή blockchain.

Η τεχνολογία Blockchain αναμένεται να επηρεάσει σε μεγάλο βαθμό περίπου όλες τις βιομηχανίες στο εγγύς μέλλον. Τα χρηματοπιστωτικά ιδρύματα αναπτύσσονται με έξυπνο τρόπο για να ξεκινήσουν τη δοκιμή και την επένδυση σε αυτή την τεχνολογία, καθιστώντας εξαιρετικά σημαντικό για όλους να καταλάβουν τη δομή καθώς και τον αλγόριθμο λειτουργίας της τεχνολογίας blockchain. Ένα blockchain είναι ένας συνεχώς αυξανόμενος κατάλογος αρχείων που ονομάζεται μπλοκ, τα οποία συνδέονται και ασφαρίζονται με κρυπτογραφία. Κάθε μπλοκ περιέχει συνήθως ένα κρυπτογραφικό hash του προηγούμενου μπλοκ, ένα χρονικό σήμα (timestamp) και δεδομένα συναλλαγής. Η δομή των δεδομένων blockchain είναι αποτελεσματική και ο κατάλογος παρακέντησης (adjoin list) των μπλοκ συναλλαγών μπορεί να διατηρηθεί σε μια βάση δεδομένων ή με τη μορφή επίπεδων αρχείων. Αυτά τα μπλοκ είναι συνδεδεμένα μεταξύ τους, με κάθε μπλοκ να αναφέρεται στο προηγούμενό του στην αλυσίδα. Το πρώτο μπλοκ της αλυσίδας ονομάζεται μπλοκ γένεσης. Το blockchain μπορούμε να το φανταστούμε ως μια κάθετη στοίβα και τα μπλοκ στοιβάζονται το ένα πάνω στο άλλο με το μπλοκ γένεσης να είναι η βάση της στοίβας. Το [\[12\]](#) περιγράφει λεπτομερώς τη δομή του blockchain. Επισημαίνεται ότι όλα τα μπλοκ αναγνωρίζονται από τις κρυπτογραφικές τιμές hash που δημιουργούνται από τον αλγόριθμο SHA256 και αυτές οι τιμές hash αποτελούν μέρος της κεφαλίδας του μπλοκ. Με το σκεπτικό ότι ένα μπλοκ σε οποιοδήποτε δεδομένο σημείο έχει έναν γονέα, τότε μπορεί να έχει πολλαπλά παιδιά. Κάθε μπλοκ-παιδί στην αλυσίδα αναφέρεται στο ίδιο μπλοκ με το γονέα του και έχει την ίδια γονική τιμή hash. Παρόλο που η κατάσταση των πολλαπλών παιδιών εμφανίζεται κυρίως όταν συναντάμε ένα blockchain fork, μόλις ολοκληρωθεί η απλοποίηση/λύση του fork και προσδιοριστεί το έγκυρο μπλοκ, τα μπλοκ του fork θα είναι ορφανά και δεν θα ακολουθηθούν στο μέλλον. Η ταυτότητα των μπλοκ-

παιδιών εξαρτάται από την ταυτότητα του γονικού μπλοκ και ποικίλλει αναλόγως. Στη συνέχεια αλλάζει η τιμή κατακερματισμού του γονικού μπλοκ. Ως αποτέλεσμα, ο προηγούμενος δείκτης κατακερματισμού μπλοκ του παιδικού μπλοκ έχει αλλάξει. Αυτή η διαδικασία συνεχίζεται μέχρι να φτάσει σε κάθε ένα από τα μπλοκ των εγγονών. Οι καταρρακτώδεις επιδράσεις διασφαλίζουν ότι όταν ένα μπλοκ έχει πολλούς απογόνους και προγόνους, δεν μπορεί να αναμειχθεί (meddled) χωρίς επιτακτικούς επανυπολογισμούς όλων των διαδοχικών μπλοκ.

Η δομή του blockchain απεικονίζεται στον τρίτο πίνακα και περιγράφεται ως εξής:



Πίνακας 3. Δομή του blockchain

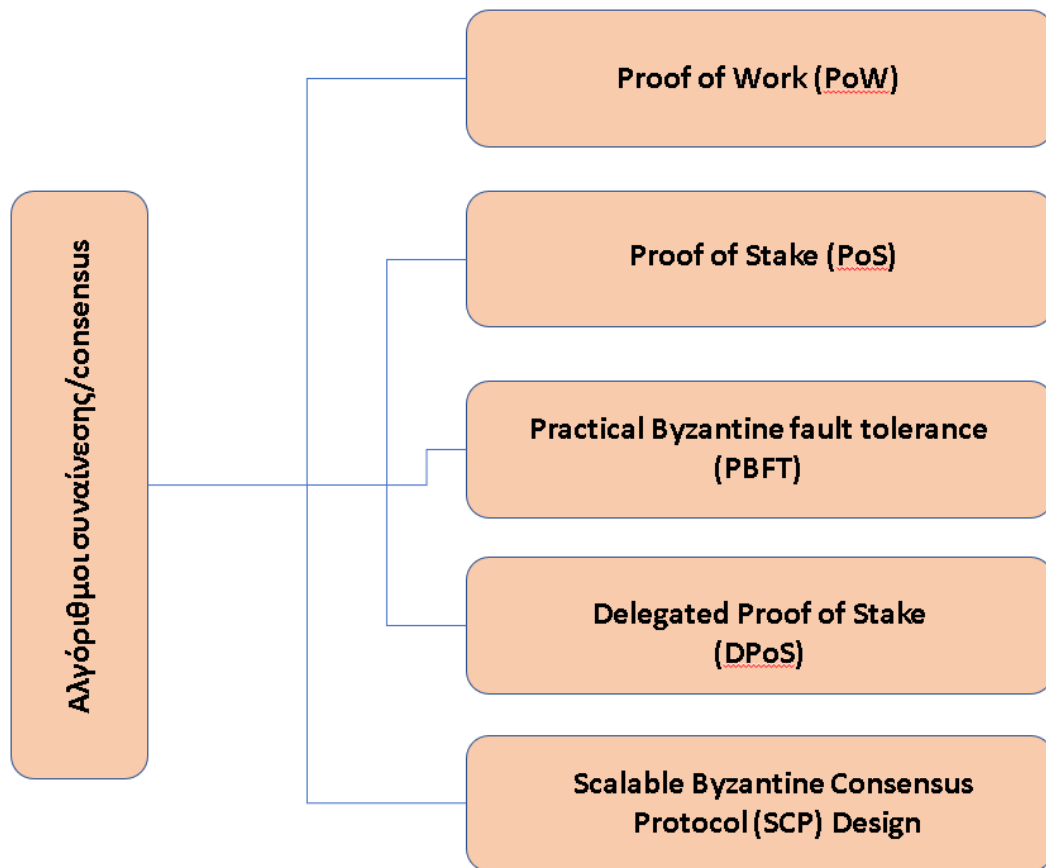
- **Δεδομένα.** Τα δεδομένα που είναι αποθηκευμένα στο blockchain εξαρτώνται από την υπηρεσία και την εφαρμογή. Θα μπορούσαν να χρησιμοποιηθούν σε ένα σύστημα peer-to-peer, όπως το IPFS, σε κατανεμημένες βάσεις δεδομένων όπως apache Cassandra, σε cloud αποθήκευση όπως storj και Ethereum swarm, sia κλπ. Τα αποθηκευμένα δεδομένα μπορούν να χρησιμοποιηθούν σε διάφορες εφαρμογές όπως η καταγραφή λεπτομερειών συναλλαγών, οι τραπεζικές εργασίες, οι συμβάσεις και το IoT.
- **Hash.** Μια συνάρτηση κατακερματισμού είναι αυτή που λαμβάνει μια είσοδο οποιουδήποτε μήκους και παράγει την έξοδο με μοναδικό fixed μήκος. Εάν τροποποιηθεί μία μόνο τιμή στην είσοδο, η έξοδος είναι εξαιρετικά διαφορετική. Οι λειτουργίες Hash χρησιμοποιούνται συνεχώς στην τεχνολογία blockchain. Κάθε μπλοκ που περιέχει δεδομένα είναι κατακερματισμένο και οι αλλαγές μπορεί να είναι μεγάλες ή μικρές. Για παράδειγμα, ένας χρήστης που ονομάζεται Alex προσπαθεί να αλλάξει τα δεδομένα που είναι αποθηκευμένα σε ένα μπλοκ. Στη συνέχεια, το

τροποποιημένο μπλοκ θα έχει μια τελείως διαφορετική τιμή κατακερματισμού, εξασφαλίζοντας ότι κάθε κόμβος ή miner στο δίκτυο θα έχει γνώση της τροποποίησης που έγινε με την ενημέρωση του αντιγράφου του βιβλίου (ledger) όλων των χρηστών. Αυτό μπορεί να αυξήσει την αξιοπιστία των δεδομένων που είναι αποθηκευμένα σε μπλοκ αλυσίδες. Σε ένα δέντρο κατακερματισμού ή στο δέντρο Merkle κάθε κόμβος αναπαρίσταται ως φύλλο και φέρει ετικέτα με μπλοκ. Αυτό το δέντρο Merkle επιτρέπει στον χρήστη να αποθηκεύει μεγάλες δομές δεδομένων με ασφαλή και αποτελεσματικό τρόπο.

- **Χρονική σήμανση (Time Stamp).** Είναι απαραίτητο να καταγραφεί η ώρα που δημιουργήθηκε το μπλοκ. Η χρονική σήμανση είναι μια μέθοδος που χρησιμοποιείται για την παρακολούθηση της δημιουργίας ή της τροποποίησης ενός εγγράφου με ασφαλή τρόπο. Αυτή η μέθοδος γίνεται ένα βασικό εργαλείο στον επιχειρηματικό κόσμο σήμερα, καθώς επιτρέπει στα εμπλεκόμενα parties να προσδιορίσουν την προέλευση και τη διαθεσιμότητα ενός εγγράφου σε μια συγκεκριμένη ημερομηνία και ώρα.
- **Άλλες πληροφορίες.** Στις άλλες πληροφορίες περιέχονται οι ψηφιακές υπογραφές, οι τιμές nonce, τα nBits και μερικές άλλες τιμές χρήστη. Κάθε χρήστης διαθέτει δύο κλειδιά, ιδιωτικό και δημόσιο κλειδί. Μια ψηφιακή υπογραφή που περιέχει αυτά τα δύο κλειδιά αφορά τόσο τη φάση υπογραφής όσο και τη φάση ελέγχου. Το ιδιωτικό κλειδί παραμένει συμβατό και χρησιμοποιείται για να υπογράψει μια συναλλαγή για την κρυπτογράφηση των δεδομένων. Το δημόσιο κλειδί είναι γνωστό από όλους και χρησιμοποιείται για την επικύρωση και αποκρυπτογράφηση των δεδομένων στη φάση της επαλήθευσης της συναλλαγής, οδηγώντας στην επαλήθευση της γνησιότητας των δεδομένων. Μια τιμή nonce είναι βασικά μια τιμή 4 byte που αρχίζει με 0 και αυξάνει κάθε φορά που εκτελείται υπολογισμός κατακερματισμού. Η τιμή nbits καθορίζει την τιμή κατωφλίου-στόχου ενός έγκυρου hash μπλοκ όπως εξηγείται στο [\[13\]](#).

3.3. Αλγόριθμοι Συναίνεσης (Consensus).

Αλγόριθμοι συναίνεσης (Consensus Algorithms). Το πρόβλημα των βυζαντινών στρατηγών (BG-Byzantine Generals) συζητήθηκε λεπτομερώς στο [\[14\]](#). Το πρόβλημα των BG προέκυψε εξαιτίας ενός συνόλου στρατηγών που διέταξαν ένα ποσοστό του βυζαντινού στρατού να περιβάλλει την πόλη. Μερικοί από τους στρατηγούς που διεύθυναν την μάχη ήθελαν να επιτεθούν στην πόλη ενώ οι άλλοι στρατηγοί προτιμούσαν την επιλογή της υποχώρησης. Παρ' όλα αυτά, η επίθεση θα ήταν ανεπιτυχής εάν μόνο ένα μέρος των στρατηγών επιτιθόταν στην πόλη. Ως εκ τούτου, μια μεγάλη πρόκληση είναι ότι πρέπει να επιτευχθεί συναίνεση σχετικά με την επίθεση ή την υποχώρηση σε ένα διαδεδομένο (disseminated) περιβάλλον. Αυτή είναι και η πρόκληση που αντιμετωπίζει το blockchain, καθώς το δίκτυο blockchain διανέμεται χωρίς κεντρική αρχή ή κεντρικό κόμβο. Μερικοί αλγόριθμοι συναίνεσης παρουσιάζονται στον τέταρτο πίνακα.



Πίνακας 4. Αλγόριθμοι συναίνεσης

- Απόδειξη εργασίας (PoW-Proof of Work).** Το πρωτόκολλο Proof of Work (PoW) είναι ένα αποθεματικό μέτρο (fiscal measure) για την αποθάρρυνση των επιθέσεων απόρριψης της υπηρεσίας (Denial of Service) και άλλων εκμεταλλεύσεων υπηρεσιών δικτύου όπως είναι οι spam που καταναλώνουν τον χρόνο επεξεργασίας του υπολογιστή [15]. Στο blockchain, κάποιος έχει οριστεί για να καταγράψει τις συναλλαγές επιλέγοντας έναν τυχαίο χρήστη ή κόμβο. Ωστόσο, αυτό οδηγεί σε επιθέσεις ευπάθειας. Εάν ένας κόμβος επιθυμεί να δημοσιεύσει ένα μπλοκ με συναλλαγές, πρέπει να γίνουν πολλοί υπολογισμοί για την επαλήθευση του τυχαίου χρήστη ή του κόμβου που επιλέχθηκε. Στο PoW, οι κόμβοι που υπολογίζουν τις τιμές κατακερματισμού ονομάζονται ανθρακωρύχοι (miners). Κάθε κόμβος στο δίκτυο υπολογίζει την τιμή κατακερματισμού της κεφαλίδας του μπλοκ που περιέχει ένα nonce. Στη συνέχεια, οι ανθρακωρύχοι αλλάζουν συχνά αυτήν την τιμή για να παράγουν διαφορετικές τιμές κατακερματισμού. Αυτό το πρωτόκολλο συνεπάγεται ότι οι υπολογιζόμενες τιμές είναι ίσες ή μικρότερες από μια καθορισμένη τιμή. Μόλις ένας κόμβος φθάσει την τιμή στόχου, μεταδίδει το μπλοκ σε άλλους κόμβους και με τη σειρά του συνειδητοποιεί την ακρίβεια της τιμής κατακερματισμού. Εάν ένα μπλοκ έχει πιστοποιηθεί, άλλοι κόμβοι προσθέτουν αυτό το νέο επικυρωμένο μπλοκ στο δικό τους blockchain. Η διαδικασία υπολογισμού των τιμών κατακερματισμού ονομάζεται εξόρυξη. Σε ένα αποκεντρωμένο σύστημα, τα έγκυρα μπλοκ παράγονται ταυτόχρονα από κόμβους πολλαπλής δειγματοληψίας που βρίσκουν το nonce περίπου την ίδια στιγμή. Αυτό θα έχει ως αποτέλεσμα τη δημιουργία forks. Τα πιρούνια

επιλύονται όταν δημιουργηθεί το επόμενο μπλοκ. Στο PoW, η μεγαλύτερη αλυσίδα είναι η πιο αξιόπιστη και σωστή. Για να βρεθεί η μεγαλύτερη έγκυρη αλυσίδα, χάνεται πολλή υπολογιστική ισχύς. Ορισμένα πρωτόκολλα χρησιμοποιούν πλευρικές εφαρμογές μαζί με PoW για να μετριάσουν την απώλεια.

- **Απόδειξη του Stake (PoS-Proof of Stake).** Η απόδειξη του Stake (PoS) είναι ένα πρωτόκολλο που δηλώνει ότι ένας χρήστης ή miner μπορεί να απομακρύνει ή να επικυρώσει συναλλαγές σε ένα μπλοκ ανάλογα με το ποσό που κατέχει ο χρήστης. Αυτό το πρωτόκολλο εμπιστεύεται ότι οι άνθρωποι έχουν περισσότερα νομίσματα, είναι λιγότερο πιθανό να επιτεθούν στο δίκτυο. Οι miners σε PoS πρέπει να αποδείξουν την ιδιοκτησία του ποσού των χρημάτων. Ωστόσο, αυτή η μέθοδος επιλογής είναι άδικη βάσει της έρευνας από το πλουσιότερο άτομο στο δίκτυο, στην οποία εξηγεί λεπτομερώς το πρωτόκολλο και παρέχει παραδείγματα για καλύτερη κατανόηση [16]. Σε αυτό το πρωτόκολλο το blockchain παρακολουθεί ένα σύνολο miners και κάθε miner πρέπει να κρατάει κρυπτονόμισμα βάσης (base) για να γίνει έγκυρος. Ο miner στέλνει μια συγκεκριμένη μορφή συναλλαγής, η οποία κλειδώνει την κρυπτογράφηση ως κατάθεση. Στη συνέχεια, η διαδικασία δημιουργίας και επικύρωσης ενός νέου μπλοκ εκτελείται από όλους τους επικυρωμένους συμμετέχοντες. Ο αλγόριθμος PoS έχει παραλλαγές, ανάλογα με τους τρόπους με τους οποίους έχουν αποδοθεί οι ανταμοιβές. Σύμφωνα με τις δυνατότητες των αλγορίθμων, οι τρόποι μπορούν να ταξινομηθούν ως βασισμένοι στην αλυσίδα (chain-based) PoS και Βυζαντινής βλάβης ανοχής PoS (BFT-Byzantine fault tolerance). Σε chain based PoS, ο επικυρωτής επιλέγεται ψευδοτυχαία για μια χρονική θέση (slot) και του δίνεται η εξουσιοδότηση για να δημιουργήσει ένα μπλοκ. Το δημιουργημένο μπλοκ πρέπει να έχει το προηγούμενο μπλοκ ως πρόδρομο για να επιτευχθεί μια ενιαία και συνεχώς αυξανόμενη αλυσίδα επιμήκυνσης μπλοκ. Σε BFT-style PoS, οι ανθρακωρύχοι επιτρέπεται τυχαία να προτείνουν τη δημιουργία ενός νέου μπλοκ. Ωστόσο, η έγκριση του μπλοκ είναι κανονική και διεξάγεται με μια διαδικασία πολλαπλών multiround ψηφοφοριών, όπου κάθε επικυρωτής ψηφίζει για ένα συγκεκριμένο μπλοκ και τέλος, όλοι οι επικυρωτές συμφωνούν σχετικά με την εγκυρότητα του μπλοκ στο blockchain.

- **Πρακτική ανοχή βλαβών (PBFT – Practical Byzantine Fault Tolerance).** Η PBFT είναι ένας αλγόριθμος απομίμησης που δημιουργήθηκε για να αντέχει στα βυζαντινά σφάλματα. Το [17] αναφέρει λεπτομερώς το πρωτόκολλο, δείχνοντας ότι για να ανεχθεί το βυζαντινό λάθος πρέπει να καταλάβουμε το βυζαντινό πρόβλημα που μπορεί να χαρακτηριστεί ως πρόβλημα συμφωνίας, όπου ένα σύμπλεγμα στρατηγών, που διοικούν μεμονωμένα ένα ποσοστό του βυζαντινού στρατού, πολιορκούν την πόλη. Οι στρατηγοί θέλουν να διατυπώσουν ένα σχέδιο για να επιτεθούν στην πόλη. Βασικά, οι στρατηγοί πρέπει να αποφασίσουν για την πορεία δράσης που θα ήταν είτε να επιτεθεί στην πόλη είτε να υποχωρήσει. Το πιο σημαντικό είναι ότι όλοι οι στρατηγοί καταλήγουν σε αμοιβαία απόφαση. Εάν μόνο μερικοί στρατηγοί επιτεθούν στην πόλη, η επίθεση θα αποτύχει. Το βυζαντινό πρόβλημα γίνεται ακόμη πιο περίπλοκο από την ύπαρξη ανυπάκουων στρατηγών που μπορούν να ψηφίσουν για μια ασήμαντη στρατηγική. Ο αλγόριθμος PBFT διαχειρίζεται

έως και $1/3$ κακόβουλα βυζαντινά αντίγραφα. Μόλις ένα νέο μπλοκ είναι resolute σε ένα γύρο (round), ένα πρωτεύον (primary) επιλέγεται με βάση τους προκαθορισμένους κανόνες και είναι υπεύθυνο να καλέσει τη συναλλαγή για κάθε γύρο. Η όλη διαδικασία χωρίζεται σε τρεις φάσεις: pre-prepared, prepared και commit. Σε όλες τις φάσεις, ο κόμβος εισέρχεται στην επόμενη φάση μόνο αφού λάβει $2/3$ από τις ψήφους από όλους τους κόμβους του δικτύου. Στο PBFT, κάθε κόμβος είναι γνωστός από άλλους κόμβους του δικτύου και μπορεί να ελέγξει ο ένας τον άλλον. Η Δεσμευμένη Ανοχή Βυζαντινής Βλάβης (dBFT-delegated) είναι ένας αλγόριθμος όπως ο PBFT. Ωστόσο, στο dBFT μια ομάδα επαγγελματικών κόμβων ψηφίζεται να καταγράψει συναλλαγές σε αντίθεση με τυχαίους κόμβους.

Στον αλγόριθμο βυζαντινής συναίνεσης προσδιορίζονται νέα μπλοκ σε γύρους. Ένας χορηγός (sponsor) έχει επιλεγεί για να εκπέμψει ένα ασυνόδευτο μπλοκ σε ένα γύρο. Η επικύρωση μιας συναλλαγής μπορεί να γίνει σε τρία στάδια. Το πρώτο είναι το βήμα προώλησης. Σε αυτό το βήμα, οι επικυρωτές υποδεικνύουν την ανάγκη μετάδοσης ενός μπλοκ για την πρόληψη. Είναι δυνατό να παραλειφθεί αυτό το βήμα, εάν οι επικυρωτές θεωρούν ότι είναι περιττό για μια συγκεκριμένη συναλλαγή και να εγκρίνουν άμεσα την πρόβλεψη ενός μπλοκ ή συναλλαγής κερδίζοντας $2/3$ ψήφους από το δίκτυο. Το δεύτερο βήμα είναι το προκαταρκτικό βήμα. Σε αυτό το βήμα, οι επικυρωτές αποφασίζουν να δεσμεύσουν ένα μπλοκ ή μια συναλλαγή. Για να εισαγάγουν αυτό το βήμα, ο κόμβος χρειάζεται $2/3$ ψήφους από το πρώτο βήμα. Εάν το prevote βήμα είναι μηδενικό, η φάση προαγοράς (precommit) περνάει από την κουραστική φάση της ψηφοφορίας (tedious voting phase) για μετάδοση και επικύρωση. Μόλις το μπλοκ λάβει $2/3$ ψήφους για το βήμα προαγοράς, εισέρχεται στη φάση δέσμευσης (commit phase), που είναι το τελευταίο βήμα. Σε αυτό το βήμα, ένας κόμβος επικυρώνει ένα μπλοκ ή μια συναλλαγή και μεταδίδει μια δέσμευση γι' αυτό. Η φάση δέσμευσης με $2/3$ ψήφους από το μπλοκ ή τη συναλλαγή, γίνεται αποδεκτή ως έγκυρη.

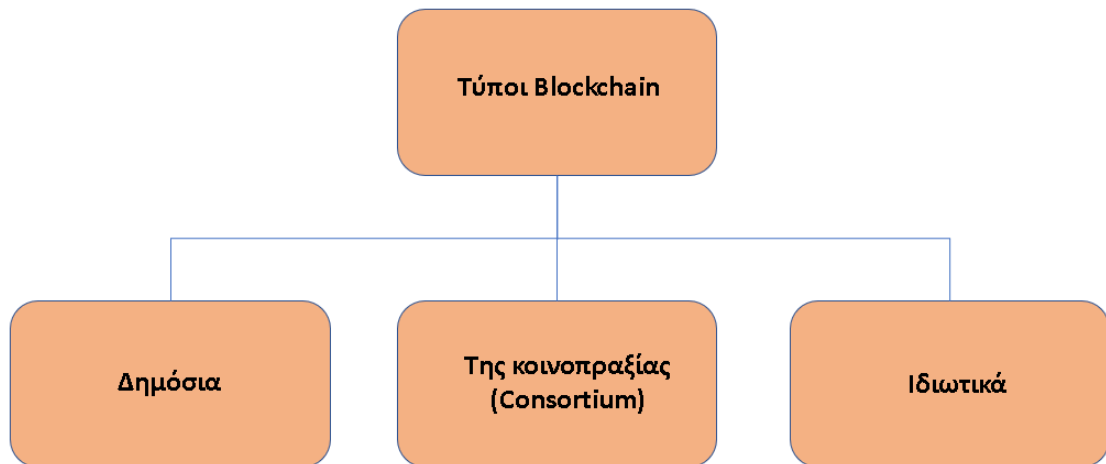
- **Αποδεδειγμένη απόδειξη πληρωμής (DPoS-delegated).** Η εξουσιοδοτημένη απόδειξη της συμμετοχής (DPoS) είναι ένας αλγόριθμος όπως το πρωτόκολλο PoS. Η DPoS στοχεύει στην επίτευξη μιας κατανεμημένης συναίνεσης σε ένα σύστημα κρυπτονομίσματος. Διαφέρει από τον αλγόριθμο PoS στην άποψη ότι στην DPoS, οι κάτοχοι κερμάτων του συστήματος κρυπτονομίσματος ψηφίζουν ώστε οι αντιπρόσωποι να επικυρώνουν και να επεξεργάζονται μια συναλλαγή σε αντάλλαγμα των τελών συναλλαγής (transaction fees), που είναι διαφορετικό στο PoS στο οποίο ένας ενδιαφερόμενος επικυρώνει και επεξεργάζεται μια συναλλαγή για να κερδίσει ανταμοιβές και τέλη συναλλαγών. Τα εμπλεκόμενα μέρη σε ένα σύστημα κρυπτονομίσματος εκλέγουν τον αντιπρόσωπό τους (delegated), ο οποίος με τη σειρά του παράγει και επικυρώνει μπλοκ. Το DPoS είναι το πιο γρήγορο, παραγωγικό, αποδοτικό, αποκεντρωμένο και ευέλικτο μοντέλο συναίνεσης που διατίθεται. Η DPoS ανεβάζει τη δύναμη της ψηφοφορίας με την έγκριση των ενδιαφερομένων μερών (stakeholders) για την επίλυση των προβλημάτων συναίνεσης με δίκαιο και δημοκρατικό τρόπο. Η ντετερμινιστική επιλογή των παραγωγών μπλοκ επιτρέπει τη διαπίστωση των συναλλαγών κατά μέσο όρο μόνο ενός δευτερολέπτου. Ίσως το πιο σημαντικό, το πρωτόκολλο συναίνεσης έχει σχεδιαστεί για την προστασία όλων των συμμετεχόντων από ανεπιθύμητες

ρυθμιστικές παρεμβολές [18]. Μια συναλλαγή επιβεβαιώνεται άμεσα, εάν χρειάζεται να επικυρωθούν λιγότεροι κόμβοι, αλλά αυτή η μορφή επικύρωσης μπλοκ θα μπορούσε να οδηγήσει σε παραβίαση των παραμέτρων του μπλοκ όπως το μέγεθος και το διάστημα από τους επιλεγμένους αντιπροσώπους. Η διαδικασία DPoS περιλαμβάνει τη χρήση αξιόπιστων υποδικτύων σε ένα μεγαλύτερο δίκτυο στο οποίο οι κόμβοι μπορούν να χωριστούν είτε σε ένα server είτε στον πελάτη. Ένας server συμβάλλει στη διαδικασία συναίνεσης και κάθε server περιέχει μια μοναδική λίστα κόμβων (UNL) ενώ ο πελάτης θα μεταφέρει κεφάλαια (funds). Προκειμένου να επικυρωθεί μια συναλλαγή, ο server ερωτά τους κόμβους που παρατίθενται στην UNL. Εάν οι συμφωνίες φτάσουν τουλάχιστον το 80%, η συναλλαγή επικυρώνεται και προστίθεται στο ημερολόγιο (ledger). Σύμφωνα με την οπτική γωνία των κόμβων, ο λογαριασμός ή η συναλλαγή παραμένει ακριβής και σωστή έως ότου το ποσοστό των ελαττωματικών κόμβων του UNL παραμείνει κάτω από το 20%.

- **Σχεδίαση SCP (design).** Το σχέδιο SCP είναι ένα υπολογιστικά προσαρμόσιμο πρωτόκολλο βυζαντινής συναίνεσης για blockchain και αυτός ο αλγόριθμος ασχολείται με μια συναλλαγή ή μπλοκ βασισμένη σε εποχές ή χρονικές περιόδους. Κάθε εποχή στοχεύει και αποφασίζει για ένα σύνολο τιμών. Το [19] αναλύει λεπτομερώς τα βήματα αυτού του πρωτοκόλλου. Επισημαίνεται ότι η βασική ιδέα του σχεδιασμού SCP είναι η αποτελεσματική χρήση της διαθέσιμης υπολογιστικής ισχύος. Το πρωτόκολλο αυτό διαιρεί την διαθέσιμη υπολογιστική ισχύ στις υποεπιτροπές (sub-committees) και κάθε επιτροπή εφαρμόζει εσωτερικό πρωτόκολλο συναίνεσης για να συμφωνήσει σε ένα ενιαίο αποτέλεσμα. Μια επιτροπή συναίνεσης είναι αρμόδια να συλλέγει και να συνδυάζει τις αξίες/τιμές που αποφασίζουν όλες οι επιτροπές. Είναι επίσης υπεύθυνη για τον υπολογισμό μιας κρυπτογραφικής σύνοψης και τη μετάδοσή της σε ολόκληρο το δίκτυο. Καθώς ο αριθμός των επιτροπών αυξάνεται, η συνολική υπολογιστική ισχύς του δικτύου αυξάνεται αντίστοιχα. Στο τελευταίο βήμα μιας εποχής, η τελική επιτροπή δημιουργεί ένα σύνολο τυχαίων δημόσιων bit strings που χρησιμοποιούνται από τις επόμενες εποχές ως πηγή τυχαιότητας. Ο επεξεργαστής εκτελεί 5 βήματα σε κάθε εποχή. Το πρώτο βήμα είναι η σύσταση επιτροπής, η οποία είναι ένας τοπικός υπολογισμός σε κάθε επεξεργαστή. Ο τοπικός υπολογισμός αποκαλύπτει την εικονική ταυτότητα της επιτροπής στον επεξεργαστή που συμμετέχει σε μια εποχή. Το δεύτερο βήμα είναι η ένωση επικάλυψης επιτροπών (committee overlay join), όπου οι επεξεργαστές επικοινωνούν για να μάθουν τις ταυτότητες άλλων επεξεργαστών που εμπλέκονται στην επιτροπή τους. Το τρίτο βήμα είναι η ενδοεπιτροπική συναίνεση, στην οποία οι επεξεργαστές τρέχουν ένα πρωτόκολλο ελέγχου ταυτότητας για να συμφωνήσουν σε μια αξία/τιμή. Κάθε εμπλεκόμενη επιτροπή στέλνει την αξία/τιμή στην ορισθείσα τελική επιτροπή. Το επόμενο τέταρτο βήμα είναι η οριστική μετάδοση συναίνεσης, όπου η τελική επιτροπή υπολογίζει μια τελική τιμή από όλες τις ληφθείσες τιμές και μεταδίδει το τελικό αποτέλεσμα στο δίκτυο. Το πέμπτο και το τελευταίο βήμα είναι η κοινή κατανομή τυχαίων αποτελεσμάτων, όπου η τελική επιτροπή εφαρμόζει ένα σύστημα διάδοσης (disseminated scheme) για να παράγει μια επαρκώς αμερόληπτη τυχαία τιμή.

3.4. Τύποι Blockchain.

Τύποι blockchains. Ο πέμπτος πίνακας απεικονίζει τις τρεις μορφές του blockchain, συμπεριλαμβανομένου του δημόσιου blockchain, του ιδιωτικού blockchain και του blockchain της κοινοπραξίας (consortium) [20], ενώ ο έκτος εμφανίζει τις αντίστοιχες παραστάσεις σχεδίου.

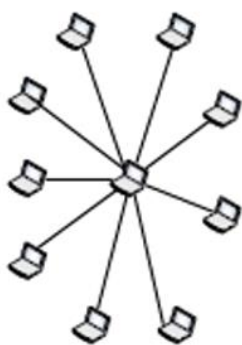


Πίνακας 5 Τύποι Blockchain

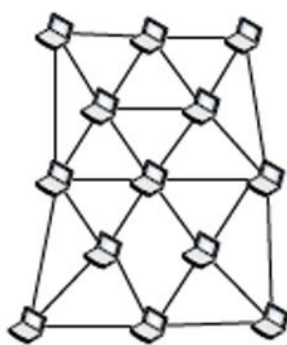
- **Δημόσιο blockchain.** Σε αυτόν τον τύπο blockchain, όλοι στο δίκτυο μπορούν να επικυρώσουν τη συναλλαγή και να συμμετάσχουν στη διαδικασία επίτευξης συναίνεσης. Το Blockchain σχεδιάστηκε αρχικά για να αποκόψει την κεντρική αρχή με ασφαλή τρόπο. Εξασφαλίζει την αποκέντρωση δημιουργώντας ένα μπλοκ P2P συναλλαγών. Κάθε συναλλαγή συνδέεται με το blockchain πριν από την εγγραφή της στο σύστημα. Έτσι, μπορεί να επιβεβαιωθεί και να συγχρονιστεί με κάθε κόμβο στο δίκτυο. Οποιοσδήποτε με υπολογιστή και σύνδεση στο διαδίκτυο μπορεί να εγγραφεί ως κόμβος και μπορεί να του παρασχεθεί το πλήρες ιστορικό του blockchain. Ο πλεονασμός αυτός του δημόσιου blockchain το καθιστά εξαιρετικά ασφαλές. Ωστόσο, είναι πολύ αργό και αναποτελεσματικό. Η ηλεκτρική ισχύς που απαιτείται για την επικύρωση κάθε συναλλαγής είναι σημαντική και αυξάνεται δραματικά με κάθε κόμβο που προστίθεται στο δίκτυο. Από την άλλη πλευρά, το κέρδος του δημόσιου δικτύου είναι η ανωνυμία του χρήστη και η πλήρης διαφάνεια του βιβλίου (ledger). Σε σύγκριση με ένα ιδιωτικό blockchain, το κόστος είναι υπερβολικό και οι ταχύτητες είναι απρόσμενες. Ωστόσο, το δημόσιο blockchain είναι ταχύτερο και λιγότερο ακριβό από τα υπολογιστικά συστήματα και τις μεθόδους που χρησιμοποιήθηκαν πριν από τη χρήση του blockchain. Ένα αποκεντρωμένο δίκτυο είναι η καρδιά του blockchain και ένα δημόσιο blockchain είναι ο πιο αποτελεσματικός τρόπος για την αποκέντρωση ενός δικτύου.
- **Ιδιωτικό blockchain.** Το ιδιωτικό blockchain είναι ο τύπος blockchain που επιτρέπει τον μεσάζοντα σε κάποιο βαθμό. Τα ιδιωτικά blockchains έχουν

αυστηρή διαχείριση με σεβασμό στην αρχή της πρόσβασης δεδομένων στο δίκτυο. Κανένας από τους κόμβους του δικτύου δεν μπορεί να συμμετάσχει στην εξακρίβωση και επικύρωση των συναλλαγών. Αντ' αυτού, μια εταιρεία ή ένας οργανισμός ξεκινά, επαληθεύει και επικυρώνει κάθε συναλλαγή. Αυτό παρέχει υψηλότερο επίπεδο αποτελεσματικότητας κατά την επαλήθευση και επικύρωση των συναλλαγών. Η μόνη υποδεέστερη έλλειψη των ιδιωτικών blockchains είναι ότι δεν παρέχουν αποκεντρωμένη ασφάλεια όπως προβλέπεται από τα δημόσια blockchain. Από την άλλη πλευρά, το πλεονέκτημα του ιδιωτικού blockchain είναι ότι μια εταιρεία μπορεί να επιλέξει τα δικαιώματα πρόσβασης σε άτομα και να επιτρέψει υψηλότερο επίπεδο ιδιωτικότητας σε σύγκριση με τα δημόσια blockchains. Ένα ιδιωτικό blockchain σχετίζεται με μια παραδοσιακή και model based επιχειρηματική λειτουργία. Τα ιδιωτικά blockchains είναι πιο πιθανά στην αποδοχή τους από τις κυβερνητικές εταιρείες ή εταιρείες του ιδιωτικού τομέα, καθώς επιτρέπουν σε μια κεντρική αρχή να είναι παρούσα με πιο ασφαλή, αποδοτικότερη και ταχύτερη τεχνολογία.

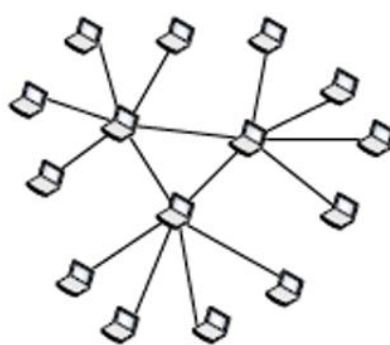
- **Consortium blockchain.** Το blockchain της κοινοπραξίας είναι ένας συνδυασμός δημόσιων και ιδιωτικών blockchains και μπορεί να θεωρηθεί ως εν μέρει αποκεντρωμένο. Σε αυτό το δίκτυο μπλοκ αλυσίδων, τα δεδομένα ή οι λεπτομέρειες των συναλλαγών μπορούν είτε να είναι ανοιχτού κώδικα είτε να είναι ιδιωτικά και ο κόμβος έχει την εξουσία να επιλέξει εκ των προτέρων. Είναι ζωτικής σημασίας να πραγματοποιηθεί η διάκριση ανάμεσα σε ένα blockchain της κοινοπραξίας και ένα εντελώς ιδιωτικό blockchain. Ωστόσο, η διαφορά δεν διερευνάται σε βάθος μέχρι και σήμερα. Γενικά, το blockchain της κοινοπραξίας είναι ένας συνδυασμός μεταξύ της χαμηλής εμπιστοσύνης των δημοσίων blockchains και του ενιαίου υψηλά αξιόπιστου υποδείγματος οντότητας (single highly trustable entity model) των ιδιωτικών blockchains, ενώ τα ιδιωτικά blockchains μπορούν να ορίζονται με ακρίβεια ως παραδοσιακά κεντρικά συστήματα με κρυπτογραφική επαλήθευση και επικυρώσεις. Αυτός ο τύπος blockchain επιτρέπει σε ένα σύνολο προκαθορισμένων κόμβων να επαληθεύουν και να επικυρώνουν τις συναλλαγές ή τα μπλοκ, αντί να επιτρέπουν σε οποιοδήποτε πρόσωπο με σύνδεση στο Internet ή σε μία μόνο εταιρεία να έχει τον πλήρη έλεγχο για την επαλήθευση και επικύρωση των συναλλαγών ή των μπλοκ. Ένα blockchain κοινοπραξίας παρέχει πολλά από τα ίδια πλεονεκτήματα που συνδέονται με τα ιδιωτικά blockchains. Επικεντρώνονται κυρίως στην αποτελεσματικότητα και τη διακριτική ευχέρεια των συναλλαγών χωρίς να εξουσιοδοτούν μια ενιαία εταιρεία ή οργανισμό. Τα blockchains της κοινοπραξίας λειτουργούν υπό τη διοίκηση μιας ομάδας φορέων όπως τα μέλη ενός διοικητικού συμβουλίου. Αυτή η πλατφόρμα προσφέρει ένα εξαιρετικό πλεονέκτημα στις οργανωτικές συνεργασίες (organizational partnerships) παρέχοντας ατελείωτες δυνατότητες.



Δημόσιο



Της κοινοπραξίας
(Consortium)



Ιδιωτικό

Πίνακας 6. Αναπαράσταση των τύπων blockchain

4. Προβλήματα ασφάλειας και διασφάλισης ιδιωτικότητας

Ιδιωτικότητα σε blockchain.

Η ιδιωτικότητα είναι η δυνατότητα ενός μόνο ατόμου ή μιας ομάδας να αποκλείσει τους εαυτούς τους ή τα δεδομένα, εκφράζοντας τον εαυτό τους διακριτικά. Η ιδιωτικότητα σε blockchain σημαίνει να είναι κανείς σε θέση να πραγματοποιεί συναλλαγές χωρίς να διαρρέουν πληροφορίες ταυτοποίησης. Ταυτόχρονα, η ιδιωτικότητα επιτρέπει σε έναν χρήστη να παραμείνει συμμορφούμενος με τη διακριτική αποκάλυψή του, χωρίς να παρουσιάσει τη δραστηριότητά του σε ολόκληρο το δίκτυο. Ο στόχος της ενίσχυσης της ιδιωτικής ζωής στα blockchains είναι να καταστεί εξαιρετικά δύσκολο για τους άλλους χρήστες να αντιγράψουν ή να χρησιμοποιήσουν κρυπτογράφηση άλλων χρηστών. Ένας ανυπολόγιστος όγκος παραλλαγών μπορεί να γίνει αντιληπτός κατά την εφαρμογή τεχνολογίας blockchain. Ορισμένα κοινά χαρακτηριστικά είναι ιδιαίτερα σημαντικά και συνοψίζονται ως εξής [59]:

- **Διαλογή αποθηκευμένων δεδομένων (Stored data sorting).** Το Blockchain παρέχει την ευκολία αποθήκευσης όλων των μορφών δεδομένων. Η προοπτική προστασίας προσωπικών δεδομένων σε blockchain ποικίλλει για προσωπικά και οργανωτικά δεδομένα. Αν και οι κανόνες απορρήτου ισχύουν για προσωπικά δεδομένα, ισχύουν αυστηρότεροι κανόνες απορρήτου για ευαίσθητα και οργανωτικά δεδομένα.
- **Διανομή αποθήκευσης (Storage distribution).** Οι κόμβοι του δικτύου που αποθηκεύουν πλήρη αντίγραφα του blockchain καλούνται πλήρεις κόμβοι. Οι πλήρεις κόμβοι σε συνδυασμό με το χαρακτηριστικό «μόνο της προσάρτησης» του blockchain οδηγούν σε πλεονασμό δεδομένων. Αυτός ο πλεονασμός δεδομένων υποστηρίζει δύο βασικά χαρακτηριστικά της τεχνολογίας blockchain, συμπεριλαμβανομένης της διαφάνειας και της ικανότητας επαλήθευσης. Η συμβατότητα της εφαρμογής με την ελαχιστοποίηση των δεδομένων καθορίζει το επίπεδο διαφάνειας και εγγύτητας του δικτύου αυτού για μια εφαρμογή.
- **Προσάρτηση μόνο (Append-only).** Είναι αδύνατο να αλλάξουν τα δεδομένα των προηγούμενων μπλοκ στο blockchain χωρίς να εντοπιστεί αυτή η αλλαγή. Η προσθήκη του χαρακτηριστικού “Append-only” του blockchain σε ορισμένες περιπτώσεις δεν περιορίζει το δικαίωμα διόρθωσης των χρηστών, ειδικά αν τα δεδομένα έχουν καταγραφεί εσφαλμένα. Πρέπει να δοθεί ιδιαίτερη προσοχή κατά την ανάθεση δικαιωμάτων στα πρόσωπα στα οποία αναφέρονται τα δεδομένα σε τεχνολογία blockchain.
- **Ιδιωτικό εναντίον δημόσιο blockchain.** Η προσβασιμότητα του blockchain είναι αξιοσημείωτη από την άποψη της ιδιωτικής ζωής. Σε προχωρημένο επίπεδο, τα περιορισμένα δεδομένα σε ένα μπλοκ μπορούν να κρυπτογραφηθούν για πρόσβαση υπό όρους από εξουσιοδοτημένους χρήστες, καθώς κάθε κόμβος του blockchain διατηρεί ένα αντίγραφο ολόκληρου του blockchain.
- **Μη εξουσιοδοτημένοι εναντίον εξουσιοδοτημένων τύπων blockchain.** Με δημόσιες ή μη εξουσιοδοτημένες εφαρμογές blockchain, όλοι οι χρήστες επιτρέπεται καταρχήν να προσθέσουν δεδομένα. Η αποδοχή της αποκατάστασης αξιόπιστων διαμεσολαβητών επηρεάζει την κατανομή του ελέγχου στο δίκτυο.

Ασφάλεια σε blockchain. Η ασφάλεια σε blockchain μπορεί να οριστεί ως η προστασία των πληροφοριών, συναλλαγών και δεδομένων σε ένα μπλοκ (ανεξάρτητα από τη μορφή των δεδομένων) κατά των εσωτερικών και περιφερειακών, κακόβουλων και ακούσιων απειλών. Συνήθως, αυτή η προστασία περιλαμβάνει την ανίχνευση απειλής, την πρόληψη της απειλής και την καταλληλότερη αντιμετώπισή της, χρησιμοποιώντας πολιτικές ασφαλείας, εργαλεία

και υπηρεσίες πληροφορικής. Ορισμένες σημαντικές ιδέες και αρχές στην ασφάλεια παρατίθενται παρακάτω:

- **Άμυνα κατά τη διείσδυση (defence in penetration).** Αυτή είναι μια στρατηγική που χρησιμοποιεί πολλά διορθωτικά μέτρα για την προστασία των δεδομένων. Ακολουθεί την αρχή ότι η προστασία των δεδομένων σε πολλαπλά στρώματα είναι πιο αποτελεσματική σε αντίθεση με το ενιαίο στρώμα ασφαλείας.
- **Ελάχιστο προνόμιο(minimum privilege).** Στη στρατηγική αυτή η πρόσβαση στα δεδομένα μειώνεται στο χαμηλότερο δυνατό επίπεδο για να ενισχυθεί το αυξημένο επίπεδο ασφαλείας.
- **Διαχείριση τρωτών σημείων (manage vulnerabilities).** Σε αυτή τη στρατηγική ελέγχουμε για ευπάθειες και τις διαχειριζόμαστε με τις μεθόδους του εντοπισμού, της επικύρωσης, τροποποίησης και επιδιόρθωσης.
- **Διαχείριση κινδύνων (manage risks).** Σε αυτή τη στρατηγική επεξεργαζόμαστε τους κινδύνους σε ένα περιβάλλον εντοπίζοντας, αξιολογώντας και ελέγχοντας τους κινδύνους.
- **Διαχείριση ενημερώσεων κώδικα (Manage patches).** Σε αυτή τη στρατηγική επεξεργαζόμαστε τα ελαττωματικά κομμάτια όπως ο κώδικας, μια εφαρμογή, ένα λειτουργικό σύστημα, λογισμικό κτλ., δοκιμάζοντας και εγκαθιστώντας patches. Η τεχνολογία Blockchain χρησιμοποιεί πολλές τεχνικές για να επιτύχει την ασφάλεια των δεδομένων των συναλλαγών ή να αποκλείσει τα δεδομένα, ανεξάρτητα από τη χρήση ή τα δεδομένα του μπλοκ. Πολλές εφαρμογές, όπως το bitcoin, χρησιμοποιούν την τεχνική κρυπτογράφησης για την ασφάλεια των δεδομένων. Τα [21] εξηγούν λεπτομερώς τη χρήση ενός συνδυασμού δημόσιου και ιδιωτικού κλειδιού για ασφαλή κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Η άλλη πιο ασφαλής έννοια του blockchain είναι ότι η μεγαλύτερη αλυσίδα είναι και η αυθεντική. Αυτό εξαλείφει τους κινδύνους ασφαλείας που οφείλονται σε 51% προβλήματα πλειοψηφίας επίθεσης και πιρουνία. Καθώς η μακρύτερη αλυσίδα είναι η τελικά αυθεντική, οι άλλες επιθέσεις καθίστανται άκυρες, καθώς καταλήγουν να είναι ορφανά πιρουνία. Το [22] εξετάζει τα επιτεύγματα βελτίωσης ασφαλείας blockchain για συστήματα blockchain όπως Smart pool, Quantitative framework, Oyente, Hawk και Town Crier.

4.1. Απαιτήσεις ασφαλείας.

- **Το απόρρητο-ιδιωτικότητα (privacy) των δεδομένων, η εμπιστευτικότητα (confidentiality) και η ακεραιότητα (integrity).**
Δεδομένου ότι τα δεδομένα ταξιδεύουν μέσω πολλαπλών hops (αλμάτων) σε ένα δίκτυο, απαιτείται ένας κατάλληλος μηχανισμός κρυπτογράφησης για να διασφαλιστεί η εμπιστευτικότητα των δεδομένων. Λόγω της ποικίλης ενοποίησης των υπηρεσιών, των συσκευών και του δικτύου, τα δεδομένα που είναι αποθηκευμένα σε μια συσκευή είναι ευάλωτα στην παραβίαση της ιδιωτικότητας, θέτοντας σε κίνδυνο τους κόμβους που υπάρχουν σε ένα δίκτυο. Οι συσκευές που είναι επιρρεπείς σε επιθέσεις μπορεί να οδηγήσουν τον εισβολέα στο να επηρεάσει την ακεραιότητα των δεδομένων τροποποιώντας τα αποθηκευμένα δεδομένα για κακόβουλους σκοπούς.
- **Έλεγχος ταυτότητας (authentication), εξουσιοδότηση (authorization) και λογιστική (accounting).**
Για να εξασφαλιστεί η επικοινωνία μεταξύ συσκευών που επικοινωνούν σε ένα δίκτυο, απαιτείται η εξακρίβωση της ταυτότητας μεταξύ δύο μερών που επικοινωνούν μεταξύ τους. Για προνομιακή πρόσβαση σε υπηρεσίες, οι

συσκευές πρέπει να επικυρωθούν. Η ποικιλομορφία των μηχανισμών ελέγχου ταυτότητας σε ένα δίκτυο υπάρχει κυρίως λόγω των ποικίλων ετερογενών υποκείμενων αρχιτεκτονικών και περιβαλλόντων που υποστηρίζουν τις συσκευές στο δίκτυο αυτό. Αυτά τα περιβάλλοντα αποτελούν πρόκληση για τον ορισμό του καθιερωμένου παγκόσμιου πρωτοκόλλου για τον έλεγχο ταυτότητας σε ένα δίκτυο. Ομοίως, οι μηχανισμοί έγκρισης εξασφαλίζουν ότι η πρόσβαση σε συστήματα ή πληροφορίες παρέχεται σε όσους έχουν εξουσιοδότηση. Η σωστή εφαρμογή της εξουσιοδότησης και της αυθεντικότητας οδηγεί σε ένα αξιόπιστο περιβάλλον το οποίο εξασφαλίζει ένα ασφαλές περιβάλλον επικοινωνίας. Επιπλέον, ο υπολογισμός για τη χρήση των πόρων, μαζί με τον έλεγχο και την υποβολή εκθέσεων, παρέχουν έναν αξιόπιστο μηχανισμό για την εξασφάλιση της διαχείρισης του δικτύου.

- **Διαθεσιμότητα υπηρεσιών.**

Οι επιθέσεις σε συσκευές που συνδέονται σε ένα δίκτυο ενδέχεται να παρεμποδίσουν την παροχή υπηρεσιών μέσω των συμβατικών επιθέσεων άρνησης εξυπηρέτησης (denial of service). Διάφορες στρατηγικές, όπως οι sinkhole attacks, οι jamming adversaries ή οι επαναληπτικές επιθέσεις, εκμεταλλεύονται τα στοιχεία του δικτύου σε διαφορετικά επίπεδα για να επιδεινώσουν την ποιότητα της υπηρεσίας (QoS) που παρέχεται στους χρήστες του.

- **Ενεργειακή απόδοση.**

Οι συσκευές σε ένα δίκτυο είναι συνήθως περιορισμένες από τους πόρους και χαρακτηρίζονται από χαμηλή κατανάλωση ενέργειας και λιγότερη αποθήκευση. Οι επιθέσεις κατά της αρχιτεκτονικής του δικτύου μπορεί να οδηγήσουν σε αύξηση της κατανάλωσης ενέργειας με πλημμύρες του δικτύου και εξάντληση πόρων μέσω περιττών ή πλαστογραφημένων αιτημάτων παροχής υπηρεσιών.

- **Ενιαία σημεία αποτυχίας.**

Μια συνεχής ανάπτυξη ετερογενών δικτύων για την υποδομή ενός δικτύου στο οποίο επικοινωνούν συσκευές, μπορεί να εκθέσει ένα μεγάλο αριθμό σημείων αποτυχίας που μπορεί με τη σειρά τους να επιδεινώσουν κάποιες υπηρεσίες. Απαιτείται η ανάπτυξη ενός περιβάλλοντος που να προστατεύει από παραβιάσεις για μεγάλο αριθμό συσκευών καθώς και να παρέχει εναλλακτικούς μηχανισμούς για την υλοποίηση ενός ανεκτικού σε σφάλματα δικτύου.

Κατηγοριοποίηση των προβλημάτων ασφάλειας

Μια ταξινόμηση των ζητημάτων ασφαλείας για ένα δίκτυο συσκευών που επικοινωνούν μεταξύ τους και συνεπώς και για το blockchain δίνεται στους πίνακες 7, 8 και 9, μαζί με τις αναφορές δημοσίευσης που σχετίζονται με κάθε θέμα. Τα θέματα αυτά αφορούν κυρίως το διαδίκτυο, το οποίο είναι και το μέσο επικοινωνίας επάνω στο οποίο εφαρμόζεται η τεχνολογία blockchain. Έτσι αντιλαμβανόμαστε ότι τα

θέματα που θα ακολουθήσουν, αφορούν σε πρώτο βαθμό το διαδίκτυο, αλλά τελικά έχουν μείζουσα σημασία και για την διατήρηση της ασφάλειας στην τεχνολογία blockchain. Οι δύο αυτές έννοιες εξάλλου είναι άρρηκτα συνδεδεμένες και η δεύτερη δεν θα υλοποιούταν χωρίς την πρώτη. Πρέπει να συνειδητοποιήσουμε ότι οι ευπάθειες του διαδικτύου ανάγονται σε ευπάθειες του blockchain. Σε επόμενη ενότητα θα αναλυθούν περιστατικά και απειλές που αφορούν άμεσα την τεχνολογία blockchain.

Έτσι λοιπόν κατηγοριοποιούμε τις απειλές ασφάλειας σε σχέση με την αρχιτεκτονική ανάπτυξης ενός δικτύου όπως περιγράφεται παρακάτω.

- Θέματα ασφάλειας χαμηλού επιπέδου
- Θέματα ασφάλειας σε ενδιάμεσο επίπεδο
- Θέματα ασφάλειας υψηλού επιπέδου

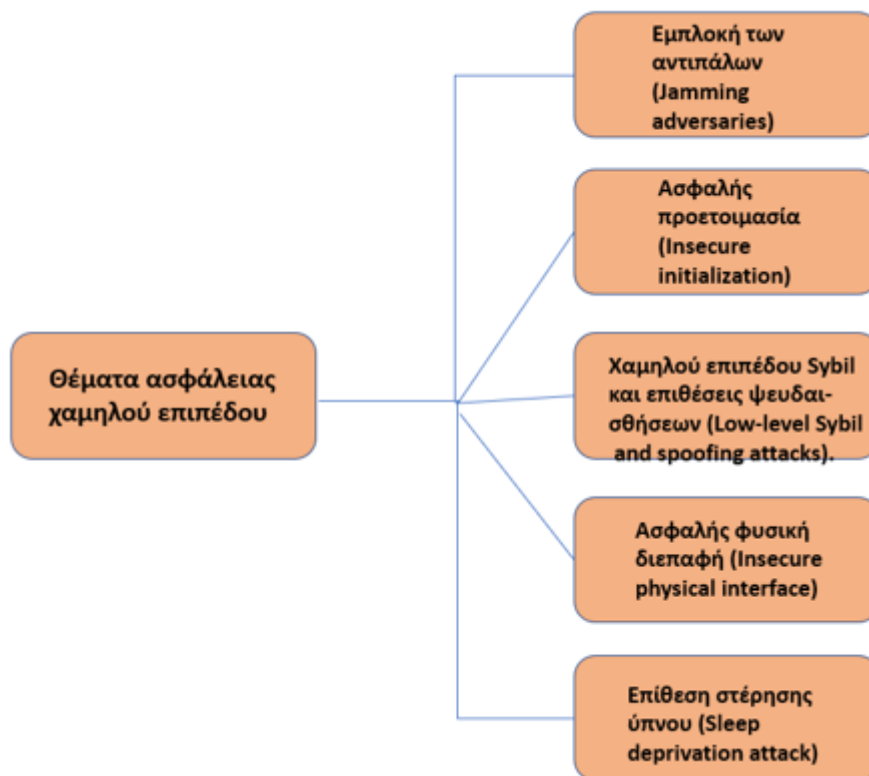
4.2. Θέματα ασφάλειας χαμηλού επιπέδου.

Το πρώτο επίπεδο ασφάλειας αφορά τα ζητήματα ασφαλείας στα επίπεδα επικοινωνίας καθώς και το επίπεδο υλικού, όπως φαίνεται λεπτομερώς παρακάτω.

- **Εμπλοκή των αντιπάλων (Jamming adversaries).** Οι επιθέσεις εμπλοκής σε ασύρματες συσκευές στοχεύουν στην αλλοίωση ενός δικτύου, εκπέμποντας σήματα ραδιοσυχνοτήτων χωρίς να ακολουθήσουν ένα συγκεκριμένο πρωτόκολλο [23]. Οι ραδιοφωνικές παρεμβολές επηρεάζουν σοβαρά τις λειτουργίες του δικτύου και μπορούν να επηρεάσουν την αποστολή και τη λήψη δεδομένων από νόμιμους κόμβους, με αποτέλεσμα τη δυσλειτουργία ή την απρόβλεπτη συμπεριφορά του συστήματος.
- **Ασφαλής προετοιμασία (Insecure initialization).** Ένας ασφαλής μηχανισμός αρχικοποίησης και διαμόρφωσης ενός δικτύου και πιο συγκεκριμένα στο physical layer, εξασφαλίζει την κατάλληλη λειτουργικότητα ολόκληρου του συστήματος χωρίς να παραβιάζεται η ιδιωτικότητα και η διακοπή των υπηρεσιών δικτύου [24]. Πρέπει επίσης να εξασφαλιστεί η επικοινωνία physical layer, ώστε να καταστεί απρόσιτη στους μη εξουσιοδοτημένους δέκτες.
- **Χαμηλού επιπέδου Sybil και επιθέσεις ψευδαισθήσεων (Low-level Sybil and spoofing attacks).** Οι επιθέσεις Sybil σε ένα ασύρματο δίκτυο προκαλούνται από κακόβουλους κόμβους Sybil που χρησιμοποιούν ψεύτικες ταυτότητες για να υποβαθμίσουν τη λειτουργικότητά του. Στο physical layer, ένας κόμβος Sybil μπορεί να χρησιμοποιήσει τυχαίες πλαστές τιμές MAC για μεταμφίεση ως μια διαφορετική συσκευή ενώ στοχεύει στην εξάντληση πόρων δικτύου [25]. Κατά συνέπεια, στους νόμιμους κόμβους μπορεί να στερηθεί η πρόσβαση στους πόρους.
- **Ασφαλής φυσική διεπαφή (Insecure physical interface).** Αρκετοί φυσικοί παράγοντες μπορούν να δημιουργήσουν σοβαρές απειλές που επηρεάζουν την καλή λειτουργία των συσκευών στο Διαδίκτυο. Η κακή φυσική ασφάλεια, η πρόσβαση σε λογισμικό μέσω φυσικών διεπαφών και τα εργαλεία για έλεγχο

/ εντοπισμό σφαλμάτων μπορούν να αξιοποιηθούν για να συμβιβάσουν τους κόμβους του δικτύου [26].

- **Επίθεση στέρησης ύπνου (Sleep deprivation attack).** Οι συσκευές με περιορισμένη ενεργειακή κατανάλωση σε ένα δίκτυο είναι ευάλωτες στις επιθέσεις "στέρησης ύπνου" προκαλώντας τους κόμβους των αισθητήρων (sensor nodes) να παραμείνουν άγρυπνοι . Αυτό έχει ως αποτέλεσμα την εξάντληση της μπαταρίας όταν ένας μεγάλος αριθμός εργασιών έχει ρυθμιστεί να εκτελείται στο περιβάλλον 6LoWPAN.



Πίνακας 7. Θέματα ασφάλειας χαμηλού επιπέδου

4.3. Θέματα ασφάλειας μεσαίου επιπέδου.

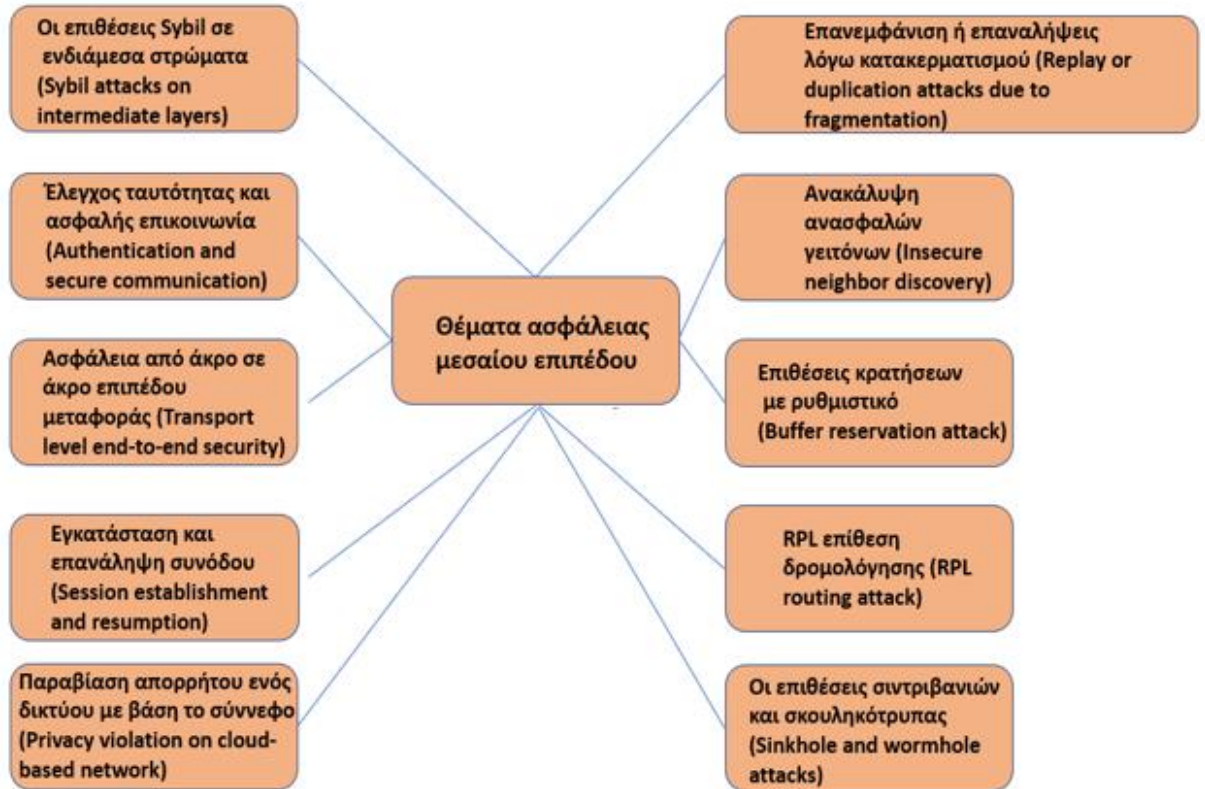
Τα ζητήματα ασφάλειας ενδιάμεσου επιπέδου αφορούν κυρίως την επικοινωνία, τη δρομολόγηση και τη διαχείριση των συνεδριάσεων (session) που πραγματοποιούνται σε επίπεδο δικτύου και των transport layers του δικτύου, όπως περιγράφεται στη συνέχεια.

- **Επανεμφάνιση ή επαναλήψεις λόγω κατακερματισμού (Replay or duplication attacks due to fragmentation).** Ο κατακερματισμός των πακέτων IPv6 απαιτείται για συσκευές που συμμορφώνονται με το πρότυπο IEEE 802.15.4 το οποίο χαρακτηρίζεται από μικρά μεγέθη πλαισίων. Μια ανακατασκευή των πεδίων θραυσμάτων πακέτων (packet fragment fields) στο

στρώμα 6LoWPAN μπορεί να οδηγήσει σε εξάντληση πόρων, υπερχείλιση buffer και επανεκκίνηση των συσκευών [27]. Τα διπλά κομμάτια (duplicate fragments) που αποστέλλονται από κακόβουλους κόμβους επηρεάζουν την επανασυναρμολόγηση των πακέτων, εμποδίζοντας έτσι την επεξεργασία άλλων νόμιμων πακέτων .

- **Ανακάλυψη ανασφαλών γειτόνων (Insecure neighbor discovery).** Η αρχιτεκτονική ανάπτυξης ενός δικτύου απαιτεί κάθε συσκευή να αναγνωρίζεται μοναδικά στο δίκτυο. Η επικοινωνία μηνυμάτων που λαμβάνει χώρα για αναγνώριση, πρέπει να είναι ασφαλής ώστε να εξασφαλίζεται ότι τα δεδομένα που μεταδίδονται σε μια συσκευή στην επικοινωνία από άκρο σε άκρο φθάνουν στον καθορισμένο προορισμό. Η φάση ανακάλυψης του γείτονα πριν από τη μετάδοση δεδομένων εκτελεί διαφορετικά βήματα, συμπεριλαμβανομένης της ανεύρεσης δρομολογητή και της ανάλυσης διευθύνσεων [28]. Η χρήση των πακέτων ανακάλυψης γείτονα χωρίς κατάλληλη επαλήθευση μπορεί να έχει σοβαρές επιπτώσεις μαζί με την άρνηση εξυπηρέτησης.
- **Επιθέσεις κρατήσεων με ρυθμιστικό(Buffer reservation attack).** Δεδομένου ότι ο κόμβος λήψης (receiving node) απαιτεί να διατηρήσει χώρο buffer για επανασυναρμολόγηση των εισερχόμενων πακέτων, ένας εισβολέας μπορεί να το εκμεταλλευτεί στέλνοντας ατελή πακέτα . Αυτή η επίθεση οδηγεί σε άρνηση εξυπηρέτησης καθώς τα άλλα πακέτα θραυσμάτων απορρίπτονται λόγω του χώρου που καταλαμβάνουν τα ελλιπή πακέτα που αποστέλλονται από τον εισβολέα.
- **RPL επίθεση δρομολόγησης (RPL routing attack).** Το πρωτόκολλο δρομολόγησης IPv6 για δίκτυα χαμηλής κατανάλωσης και απώλειες (RPL) είναι ευάλωτο σε διάφορες επιθέσεις που ενεργοποιούνται μέσω συμβιβασμένων κόμβων που υπάρχουν στο δίκτυο [29]. Η επίθεση μπορεί να έχει ως αποτέλεσμα την εξάντληση πόρων και την υποκλοπή.
- **Οι επιθέσεις σιντριβανιών και σκουληκότρυπας (Sinkhole and wormhole attacks).** Με τις επιθέσεις sinkholes, ο κόμβος εισβολέα ανταποκρίνεται στις αιτήσεις δρομολόγησης (routing requests), καθιστώντας έτσι τα πακέτα δρομολογημένα μέσω του κόμβου εισβολέα, ο οποίος στη συνέχεια μπορεί να χρησιμοποιηθεί για να εκτελέσει κακόβουλη δραστηριότητα στο δίκτυο. Οι επιθέσεις στο δίκτυο ενδέχεται να επιδεινώσουν περαιτέρω τις λειτουργίες του 6LoWPAN λόγω επιθέσεων σκουληκότρυπας, στις οποίες δημιουργείται μια σήραγγα μεταξύ δύο κόμβων, έτσι ώστε τα πακέτα που φθάνουν σε έναν κόμβο να φτάσουν σε άλλο κόμβο αμέσως [30]. Αυτές οι επιθέσεις έχουν σοβαρές επιπτώσεις, όπως η υποκλοπή, η παραβίαση της ιδιωτικής ζωής και η άρνηση παροχής υπηρεσιών.

- **Οι επιθέσεις Sybil σε ενδιάμεσα στρώματα (Sybil attacks on intermediate layers).** Παρόμοια με τις επιθέσεις Sybil σε στρώματα χαμηλού επιπέδου, οι κόμβοι Sybil μπορούν να αναπτυχθούν για να υποβαθμίσουν την απόδοση του δικτύου και ακόμη και να παραβιάζουν το ιδιωτικό απόρρητο δεδομένων. Η επικοινωνία από τους κόμβους Sybil με τη χρήση πλαστών ταυτοτήτων σε ένα δίκτυο μπορεί να οδηγήσει σε ανεπιθύμητη αλληλογραφία, διάδοση κακόβουλου λογισμικού ή εκκίνηση επιθέσεων ηλεκτρονικού "ψαρέματος" .
- **Έλεγχος ταυτότητας και ασφαλής επικοινωνία (Authentication and secure communication).** Οι συσκευές και οι χρήστες ενός δικτύου πρέπει να πιστοποιούνται μέσω συστημάτων διαχείρισης κλειδιών. Οποιοδήποτε κενό σε κάποιο layer ενός δικτύου, μπορεί να εκθέσει το δίκτυο σε μεγάλο αριθμό ευπαθειών [\[31\]](#). Για παράδειγμα, λόγω περιορισμένων πόρων, απαιτείται η ελαχιστοποίηση των γενικών επιβαρύνσεων του DTLS και οι κρυπτογραφικοί μηχανισμοί που εξασφαλίζουν την ασφαλή επικοινωνία των δεδομένων στην διαδικτυακή πύλη πρέπει να λαμβάνουν υπόψη την αποτελεσματικότητα και τη σπανιότητα άλλων πόρων.
- **Ασφάλεια από άκρο σε άκρο επιπέδου μεταφοράς (Transport level end-to-end security).** Η ασφάλεια από άκρο σε άκρο επιπέδου μεταφοράς στοχεύει στην παροχή ενός ασφαλούς μηχανισμού έτσι ώστε τα δεδομένα από τον κόμβο αποστολέα να λαμβάνονται με τον πιο αξιόπιστο τρόπο από τον επιθυμητό κόμβο προορισμού . Απαιτεί ολοκληρωμένους μηχανισμούς ελέγχου ταυτότητας που εξασφαλίζουν την ασφαλή επικοινωνία μηνυμάτων σε κρυπτογραφημένη μορφή χωρίς να παραβιάζουν την ιδιωτική ζωή [\[32\]](#).
- **Εγκατάσταση και επανάλληψη συνόδου (Session establishment and resumption).** Η απόπειρα συνόδου (hijacking session) σε στρώμα μεταφοράς με «σφυρηλατημένα» (forged) μηνύματα μπορεί να οδηγήσει σε άρνηση εξυπηρέτησης [\[33\]](#). Ένας κόμβος επίθεσης μπορεί να μιμηθεί τον κόμβο του θύματος για να συνεχιστεί η συνεδρία μεταξύ δύο κόμβων. Οι κόμβοι που επικοινωνούν μεταξύ τους μπορεί ακόμη να απαιτούν την εκ νέου μετάδοση των μηνυμάτων μεταβάλλοντας τους αριθμούς ακολουθίας.
- **Παραβίαση απορρήτου ενός δικτύου με βάση το σύννεφο (Privacy violation on cloud-based network).** Μπορεί να πραγματοποιηθούν μέσω cloud διαφορετικές επιθέσεις που ενδέχεται να παραβιάζουν την ιδιωτικότητα της ταυτότητας και της τοποθεσίας ή να προκαλέσουν την καθυστέρηση ανεκτικών δικτύων [\[34\]](#). Ομοίως, ένας κακόβουλος φορέας παροχής υπηρεσιών cloud μπορεί να έχει πρόσβαση σε εμπιστευτικές πληροφορίες που μεταδίδονται σε έναν επιθυμητό προορισμό.



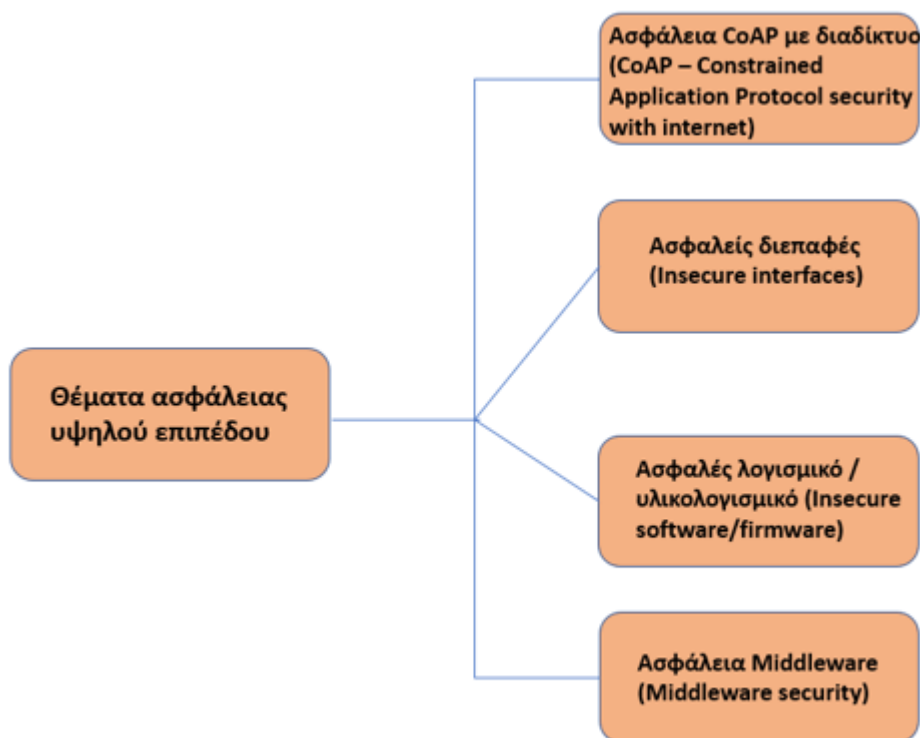
Πίνακας 8. Θέματα ασφάλειας μεσαίου επιπέδου

4.4. Θέματα ασφάλειας υψηλού επιπέδου.

Τα ζητήματα ασφάλειας υψηλού επιπέδου του blockchain περιγράφονται παρακάτω.

- **Ασφάλεια CoAP με διαδίκτυο (CoAP – Constrained Application Protocol security with internet).** Το High-level layer που περιέχει το Application Layer είναι επίσης ευάλωτο στις επιθέσεις [35]. Το πρωτόκολλο περιορισμένης εφαρμογής (CoAP- constrained application protocol) είναι ένα πρωτόκολλο μεταφοράς ιστού για περιορισμένη συσκευή που χρησιμοποιεί συνδέσεις DTLS με διάφορες λειτουργίες ασφαλείας για την παροχή ασφάλειας από άκρο σε άκρο. Τα μηνύματα του CoAP ακολουθούν μια συγκεκριμένη μορφή που ορίζεται στο RFC-7252 Z [36], τα οποία πρέπει να κρυπτογραφηθούν για ασφαλή επικοινωνία. Ομοίως, η υποστήριξη πολυεκπομπής (multicast support) στο CoAP απαιτεί επαρκείς μηχανισμούς διαχείρισης κλειδιών και ελέγχου ταυτότητας.
- **Ασφαλείς διεπαφές (Insecure interfaces).** Για την πρόσβαση στις υπηρεσίες ενός δικτύου, οι διασυνδέσεις που χρησιμοποιούνται μέσω του δικτύου, ενός κινητού και του cloud είναι ευάλωτες σε διάφορες επιθέσεις που ενδέχεται να επηρεάσουν σοβαρά την ιδιωτικότητα των δεδομένων [37].

- **Ασφαλές λογισμικό / υλικολογισμικό (Insecure software/firmware).** Διάφορες ευπάθειες στο διαδίκτυο περιλαμβάνουν αυτές που προκαλούνται από ανασφαλές λογισμικό / υλικολογισμικό. Ο κώδικας με γλώσσες όπως JSON, XML, SQLi και XSS πρέπει να δοκιμαστεί προσεκτικά. Ομοίως, οι ενημερώσεις λογισμικού / υλικολογισμικού πρέπει να πραγματοποιούνται με ασφαλή τρόπο.
- **Ασφάλεια Middleware (Middleware security).** Το middleware που έχει σχεδιαστεί για να καταστήσει την επικοινωνία μεταξύ ετερογενών οντοτήτων του διαδικτύου πρέπει να είναι αρκετά ασφαλές για την παροχή υπηρεσιών. Διαφορετικές διεπαφές και περιβάλλοντα που χρησιμοποιούν μεσαία λογισμικά πρέπει να ενσωματωθούν για την ασφαλή επικοινωνία [38].



Πίνακας 9. Θέματα ασφάλειας υψηλού επιπέδου

4.5. Ρίσκα στο blockchain.

Διαχωρίζουμε τους κοινούς κινδύνους blockchain σε εννέα κατηγορίες, όπως φαίνεται στον πίνακα 10, και αναλύουμε λεπτομερώς τα πιθανά αίτια κάθε κινδύνου. Οι κίνδυνοι που περιγράφονται υφίστανται στο blockchain 1.0 και 2.0 και οι αιτίες τους σχετίζονται κυρίως με τον μηχανισμό λειτουργίας blockchain. Αντίθετα, οι κίνδυνοι είναι μοναδικοί για το blockchain 2.0 και συνήθως προκύπτουν από την ανάπτυξη, την εγκατάσταση και την εκτέλεση έξυπνων συμβάσεων. Αναπόφευκτη είναι και η

ανάλυση στο κρυπτονόμισμα Bitcoin, του οποίου η ασφάλεια υλοποιείται σε blockchain.

Ρίσκο	Αίτια	Επιρροή
51% Ευπάθεια	Μηχανισμός Συναίνεσης	Blockchain 1.0 , 2.0
Ασφάλεια ιδιωτικού κλειδιού	Κρυπτογράφηση δημοσίου κλειδιού	
Εγγληματική Δραστηριότητα	Εφαρμογή κρυπτονομίσματος	
Διπλό ξόδεμα/δαπάνη (double spending)	Μηχανισμός πιστοποίησης συναλλαγής	
Διαρροή απορρήτου συναλλαγής	Σχεδιασμός ελλειψμάτων συναλλαγής	
Εγγληματικά έξυπνα συμβόλαια/δαπάνες	Εφαρμογή έξυπνων συμβολαίων	Blockchain 2.0
Ευπάθειες στα έξυπνα συμβόλαια	Ελλειψμματα σχεδιασμού προγράμματος	
Under-optimized έξυπνα συμβόλαια	Ελλειψμματα γραφής προγράμματος	
Under-priced λειτουργίες	Ελλειψμματα σχεδιασμού EVM	

Πίνακας 10. Ταξινόμηση των ρίσκων στο blockchain

- **51% ευπάθεια/51% vulnerability.**

Το blockchain βασίζεται στον κατανεμημένο μηχανισμό συναίνεσης για την εδραίωση της αμοιβαίας εμπιστοσύνης. Ωστόσο, ο ίδιος ο μηχανισμός συναίνεσης έχει 51% ευπάθεια, η οποία μπορεί να χρησιμοποιηθεί από τους εισβολείς για να ελέγξει ολόκληρο το blockchain. Πιο συγκεκριμένα, σε blockchains που βασίζονται σε PoW, εάν η υπολογιστική δύναμη hashing ενός miner αντιπροσωπεύει περισσότερο από το 50% της συνολικής υπολογιστικής δύναμης hashing ολόκληρου του blockchain, τότε μπορεί να ξεκινήσει η επίθεση κατά 51%. Ως εκ τούτου, η εξορυκτική δύναμη που επικεντρώνεται σε λίγες δεξαμενές εξορύξεως μπορεί να οδηγήσει σε φόβους μιας ακούσιας κατάστασης, όπως μια ενιαία ομάδα που ελέγχει περισσότερο από το ήμισυ της συνολικής υπολογιστικής ισχύος. Τον Ιανουάριο του 2014, αφοτό η δεξαμενή εξόρυξης (mining pool) ghash.io έφτασε το 42% της συνολικής υπολογιστικής ισχύος Bitcoin, αρκετοί miners αποσύρθηκαν οικειοθελώς από την δεξαμενή και η ghash.io εξέδωσε δήλωση Τύπου για να καθησυχάσει την κοινότητα Bitcoin, φθάνοντας το όριο του 51% [39]. Σε blockchains που βασίζονται σε PoS, η 51% επίθεση μπορεί επίσης να συμβεί αν ο αριθμός των κερμάτων που ανήκουν σε έναν μόνο miner είναι

περισσότερος από το 50% του συνολικού blockchain. Αρχίζοντας με την επίθεση κατά 51%, ένας εισβολέας μπορεί να χειριστεί αυθαίρετα και να τροποποιήσει τις πληροφορίες blockchain. Συγκεκριμένα, ένας εισβολέας μπορεί να εκμεταλλευτεί αυτή την ευπάθεια για να διεξάγει τις ακόλουθες επιθέσεις :

- Αντιστρεπτές συναλλαγές και έναρξη διπλής επίθεσης.
- Τα ίδια νομίσματα ξοδεύονται πολλές φορές (reverse transactions and double spending).
- Εξαίρεση και τροποποίηση της παραγγελίας των συναλλαγών.
- Παροχή κανονικών εργασιών εξόρυξης άλλων ανθρακωρύχων.
- Παρεμπόδιση της λειτουργίας επιβεβαίωσης κανονικών συναλλαγών.

- **Ασφάλεια Ιδιωτικού Κλειδιού.**

Όταν χρησιμοποιείται το blockchain, το ιδιωτικό κλειδί του χρήστη θεωρείται ως η ταυτότητα και η πιστοποίηση ασφαλείας, η οποία παράγεται και συντηρείται από το χρήστη αντί των third-parties agencies. Για παράδειγμα, όταν δημιουργείται ένα πορτοφόλι ψυχρής αποθήκευσης (cold storage) σε blockchain Bitcoin, ο χρήστης πρέπει να εισάγει το ιδιωτικό του κλειδί. Στο [40] ανακαλύπτουν μια ευπάθεια στο σύστημα ECDSA (Allipitmn Elliptic Curve Digital Signature Algorithm), μέσω του οποίου ένας εισβολέας μπορεί να ανακτήσει το ιδιωτικό κλειδί του χρήστη επειδή δεν παράγει αρκετή τυχειότητα κατά τη διάρκεια της διαδικασίας υπογραφής. Μόλις χαθεί το ιδιωτικό κλειδί του χρήστη, δεν θα μπορέσει να ανακτηθεί. Εάν το ιδιωτικό κλειδί κλαπεί από εγκληματίες, ο λογαριασμός blockchain του χρήστη θα αντιμετωπίσει τον κίνδυνο να παραβιαστεί από άλλους. Δεδομένου ότι το blockchain δεν εξαρτάται από κανένα κεντρικό όργανο εμπιστοσύνης τρίτου μέρους, εάν το ιδιωτικό κλειδί του χρήστη κλαπεί, είναι δύσκολο να εντοπιστεί η συμπεριφορά του εγκληματία και να ανακτήσει τις τροποποιημένες πληροφορίες blockchain.

- **Εγγληματική δραστηριότητα/Criminal activity.**

Οι χρήστες Bitcoin μπορούν να έχουν πολλές διευθύνσεις Bitcoin και η διεύθυνση δεν έχει καμία σχέση με την ταυτότητα της πραγματικής ζωής τους. Ως εκ τούτου, το Bitcoin έχει χρησιμοποιηθεί σε παράνομες δραστηριότητες. Μέσω κάποιων platforms ανταλλαγής third-parties agencies που υποστηρίζουν το Bitcoin, οι χρήστες μπορούν να αγοράσουν ή να πουλήσουν οποιοδήποτε προϊόν. Δεδομένου ότι η διαδικασία αυτή είναι ανώνυμη, είναι δύσκολο να εντοπιστούν οι συμπεριφορές των χρηστών, πόσο μάλλον να υπόκεινται σε νομικές κυρώσεις. Ορισμένες συχνές εγκληματικές δραστηριότητες με το Bitcoin περιλαμβάνουν:

- **Ransomware.** Οι εγκληματίες χρησιμοποιούν συχνά ransomware για εκβίαση χρημάτων και χρησιμοποιούν το Bitcoin ως νόμισμα διαπραγμάτευσης. Τον Ιούλιο του 2014, ένα ransomware με την επωνυμία CTB-Locker [41] εξαπλώθηκε σε όλο τον κόσμο αποκρύπτοντας τον εαυτό του ως συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου. Εάν ο χρήστης κάνει κλικ στο συνημμένο, το ransomware θα εκτελεστεί στο παρασκήνιο του συστήματος και θα κρυπτογραφήσει περίπου 114 τύπους κάθε αρχείου. Το θύμα πρέπει να πληρώσει στον εισβολέα ένα ορισμένο ποσό Bitcoin μέσα σε 96 ώρες. Διαφορετικά, τα κρυπτογραφημένα αρχεία δεν θα αποκατασταθούν. Τον Μάιο του 2017, ένα άλλο ransomware WannaCry (που ονομάστηκε επίσης WannaCrypt) [42] μόλυνε περίπου

230.000 θύματα σε 150 χώρες σε δύο ημέρες. Χρησιμοποίησε μια ευπάθεια στο σύστημα των Windows για να εξαπλωθεί, και κρυπτογραφημένα αρχεία χρηστών για να ζητήσει Bitcoin λύτρα.

- **Υπόγεια αγορά.** Το Bitcoin χρησιμοποιείται συχνά ως νόμισμα στην υπόγεια αγορά. Για παράδειγμα, το Silk Road είναι μια ανώνυμη, διεθνής διαδικτυακή αγορά που λειτουργεί ως υπηρεσία Tor hidden και χρησιμοποιεί το Bitcoin ως νόμισμα ανταλλαγής. Οι πρώτες 10 κατηγορίες αντικειμένων που είναι διαθέσιμες στο Silk Road παρατίθενται στον πίνακα 11[43]. Τα περισσότερα από τα είδη που πωλούνται στο Silk Road είναι τα ναρκωτικά ή κάποια άλλα ελεγχόμενα αντικείμενα στον πραγματικό κόσμο. Δεδομένου ότι οι διεθνείς συναλλαγές αντιπροσωπεύουν ένα σημαντικό ποσοστό στη Silk Road, το Bitcoin κάνει τη συναλλαγή στην υπόγεια αγορά πιο βολική, γεγονός που θα προκαλέσει βλάβη στην κοινωνική ασφάλιση.
- **Νομιμοποίηση εσόδων από παράνομες δραστηριότητες.** Δεδομένου ότι το Bitcoin έχει τα χαρακτηριστικά γνωρίσματα όπως η ανωνυμία και η εικονική πληρωμή του δικτύου και έχει υιοθετηθεί από πολλές χώρες, σε σύγκριση με άλλα νομίσματα, το Bitcoin φέρει τον χαμηλότερο κίνδυνο να χρησιμοποιηθεί για ξέπλυμα χρημάτων. Το [44] προτείνει το Dark Wallet, μια εφαρμογή Bitcoin που μπορεί να κάνει τη συναλλαγή Bitcoin εντελώς κρυφή και ιδιωτική. Το Dark Wallet μπορεί να κρυπτογραφεί τις πληροφορίες συναλλαγών και να αναμειγνύει τα έγκυρα νομίσματα του χρήστη με κέρματα νομισμάτων (chaff coins) και επομένως μπορεί να κάνει πολύ πιο εύκολη τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες.

Αριθμός	Κατηγορία	Αντικείμενα	Ποσοστό
1	Μαριχουάνα	3338	13.7%
2	Ναρκωτικά	2194	9.0%
3	Ιατρική Συνταγή	1874	7.3%
4	Βενζο-πυρένιο	1193	4.9%
5	Βιβλία	955	3.9%
6	Κάναβη	877	3.6%
7	Χασίσι	820	3.4%
8	Κοκαΐνη	630	2.6%
9	Χάπια	473	1.9%
10	LSD	440	1.8%

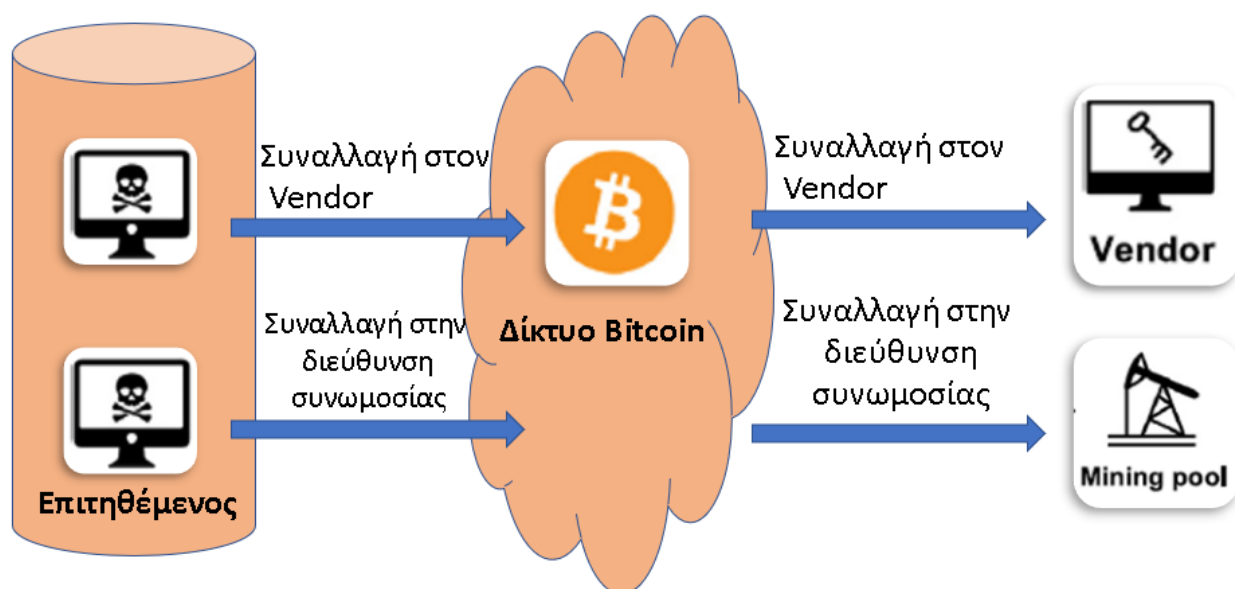
Πίνακας 11. Οι 10 κατηγορίες των πιο διαθέσιμων αντικειμένων στο Silk Road

- **Διπλή δαπάνη-ξόδεμα/Double spending.**

Παρόλο που ο μηχανισμός συναίνεσης του blockchain μπορεί να επικυρώνει συναλλαγές, είναι αδύνατον να αποφευχθούν οι διπλές δαπάνες. Η διπλή δαπάνη αναφέρεται στο ότι ένας καταναλωτής χρησιμοποιεί την ίδια κρυπτογράφηση

πολλές φορές για συναλλαγές. Για παράδειγμα, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει την race attack για διπλές δαπάνες. Αυτό το είδος επίθεσης είναι σχετικά εύκολο να εφαρμοστεί σε blockchains με βάση το PoW, επειδή ο εισβολέας μπορεί να εκμεταλλευτεί τον ενδιάμεσο χρόνο μεταξύ της έναρξης και επιβεβαίωσης δύο συναλλαγών για να ξεκινήσει γρήγορα μια επίθεση. Προτού η δεύτερη συναλλαγή θεωρηθεί άκυρη, ο επιτιθέμενος έχει ήδη βγάλει την έξοδο της πρώτης συναλλαγής, με αποτέλεσμα τη διπλή δαπάνη.

Υποθέτοντας ότι ένας εισβολέας γνωρίζει τη διεύθυνση του πωλητή πριν από την επίθεση, για να πραγματοποιήσει διπλές δαπάνες, ο εισβολέας θα στείλει δύο συναλλαγές TXn και TXa και θα επιλέξει τα ίδια BTC (κρυπτογράφηση σε Bitcoin) ως εισόδους για TXn και TXa. Η διεύθυνση παραλήπτη του TXn έχει οριστεί στη διεύθυνση του πωλητή και η διεύθυνση του παραλήπτη TXa έχει οριστεί στη διεύθυνση σύγκρουσης που ελέγχεται από τον εισβολέα. Εάν πληρούνται οι ακόλουθες τρεις προϋποθέσεις, οι διπλές δαπάνες θα είναι επιτυχείς, όπως φαίνεται στον πίνακα 12.



Πίνακας 12. Μοντέλο διπλής δαπάνης(double spending) έναντι γρήγορης πληρωμής στο Bitcoin

- (1) Το TXn προστίθεται στο πορτοφόλι του στοχευμένου πωλητή.
- (2) Το TXa εξορύσσεται ως έγκυρο στο blockchain.
- (3) Ο εισβολέας παίρνει την έξοδο του TXn πριν ο πωλητής εντοπίσει κακή συμπεριφορά. Εάν η επίθεση είναι επιτυχής, το TXn τελικά θα επαληθευτεί ως μη έγκυρη συναλλαγή και τα BTCs θα δαπανηθούν πραγματικά από την TXa. Ο επιτιθέμενος έχει λάβει την έξοδο του TXn, η οποία είναι η κανονική υπηρεσία του πωλητή. Δεδομένου ότι η διεύθυνση παραλήπτη της TXa ελέγχεται από τον εισβολέα, αυτά τα BTC εξακολουθούν να ανήκουν στον εαυτό της. Σε αυτό το μοντέλο διπλής δαπάνης, ο επιτιθέμενος απολαμβάνει την υπηρεσία χωρίς να πληρώσει κανένα BTC.

- **Διαρροή Ιδιωτικότητας συναλλαγής/Transaction privacy leakage.**

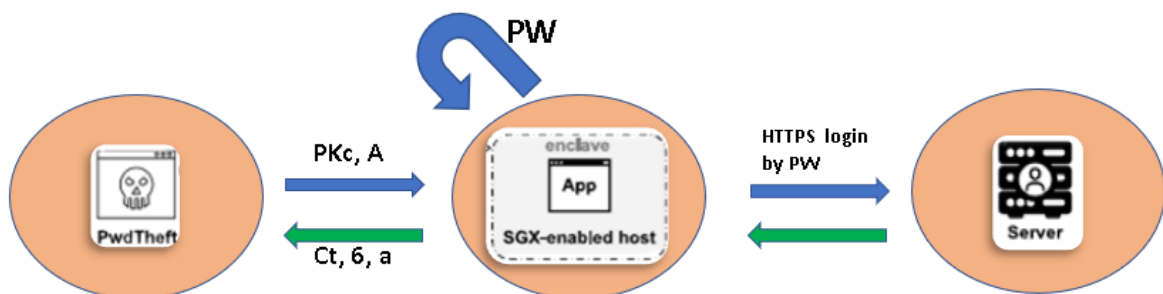
Δεδομένου ότι οι συμπεριφορές των χρηστών στο blockchain είναι ανιχνεύσιμες, τα συστήματα blockchain λαμβάνουν μέτρα για την προστασία του ιδιωτικού απορρήτου συναλλαγών των χρηστών. Στο Bitcoin και στο Zcash, χρησιμοποιούν τους λογαριασμούς μοναδικής χρήσης για να αποθηκεύσουν την ληφθείσα κρυπτογράφηση. Επιπλέον, ο χρήστης πρέπει να εκχωρήσει ένα ιδιωτικό κλειδί σε κάθε συναλλαγή. Με αυτόν τον τρόπο, ο εισβολέας δεν μπορεί να συνειδητοποιήσει εάν το κρυπτονόμισμα σε διαφορετικές συναλλαγές λαμβάνεται από τον ίδιο χρήστη. Στο Monero, οι χρήστες μπορούν να συμπεριλάβουν μερικά νομίσματα ("mixins") όταν ξεκινούν μια συναλλαγή, έτσι ώστε ο εισβολέας να μην μπορεί να συνάγει τη σύνδεση των πραγματικών κερμάτων που ξοδεύει η συναλλαγή.

Δυστυχώς, τα μέτρα προστασίας της ιδιωτικής ζωής στο blockchain δεν είναι πολύ ισχυρά. Το [45] αξιολογεί εμπειρικά δύο αδυναμίες συνδεσιμότητας στη στρατηγική δειγματοληψίας mixin του Monero και ανακαλύπτει ότι το 66,09% όλων των συναλλαγών δεν περιέχουν αναλογίες. Η συναλλαγή 0-mixin θα οδηγήσει στη διαρροή απορρήτου του αποστολέα της.

Δεδομένου ότι οι χρήστες μπορούν να χρησιμοποιήσουν τις εξόδους της συναλλαγής 0-mixin ως mixins, αυτές οι mixins θα μπορούσαν να συναχθούν (deducible). Επιπλέον, μελετούν τη μέθοδο δειγματοληψίας των mixins και διαπιστώνουν ότι η επιλογή των mixins δεν είναι πραγματικά τυχαία. Τα νεότερα TXOs (εξερχόμενες συναλλαγές) τείνουν να χρησιμοποιούνται συχνότερα. Ανακαλύπτουν επίσης ότι το 62,32% των εισροών συναλλαγών με τις mixins απορροφώνται. Χρησιμοποιώντας αυτές τις αδυναμίες στο Monero, μπορούν να συμπεράνουν τις πραγματικές εισροές συναλλαγών με ακρίβεια 80%.

- **Εγκληματικά έξυπνα συμβόλαια-συμβάσεις/Criminal smart contracts.**

Οι εγκληματίες μπορούν να εκμεταλλευτούν έξυπνες συμβάσεις για διάφορες κακόβουλες δραστηριότητες, οι οποίες μπορεί να αποτελέσουν απειλή για την καθημερινότητά μας. Τα CSCs (Ποινικά Έξυπνα Συμβόλαια) μπορούν να διευκολύνουν τη διαρροή εμπιστευτικών πληροφοριών, την κλοπή κρυπτογραφικών κλειδιών και διάφορα εγκλήματα πραγματικού κόσμου (π.χ. δολοφονία, εμπρησμός, τρομοκρατία κλπ.). Στο [46] προτείνεται ένα παράδειγμα κλοπής κωδικού πρόσβασης CSC Pwd Theft, η διαδικασία του οποίου φαίνεται στον παρακάτω πίνακα.



Πίνακας 13. Παράδειγμα κλοπής κωδικού πρόσβασης

Το Pwd Theft μπορεί να αξιοποιηθεί για δίκαιη ανταλλαγή μεταξύ του εργολάβου (contractor) C και του δράστη (perpetrator) P. Ο C θα πληρώσει μια ανταμοιβή για τον P εάν και μόνο αν ο P δώσει έναν έγκυρο κωδικό πρόσβασης στον C. Η όλη διαδικασία συναλλαγής μπορεί να γίνει χωρίς third-parties agencies. Από τη στιγμή που το έξυπνο συμβόλαιο που αναπτύσσεται στο blockchain δεν μπορεί να έχει άμεση πρόσβαση στο δίκτυο, στην πραγματική διαδικασία εργασίας του PwdTheft, συνδυάζεται με αξιόπιστη τεχνολογία υλικού, όπως η Intel SGX (Software Guard extension), για να αποδείξει την εγκυρότητα του κωδικού πρόσβασης μέσω HTTPS (Ασφαλές πρωτόκολλο μεταφοράς υπερκειμένου). Το SGX θα δημιουργήσει ένα περιβάλλον αξιόπιστης εκτέλεσης με την ονομασία enclave, το οποίο μπορεί να προστατεύσει την εφαρμογή από το να επιτεθεί από άλλους. Οποιοδήποτε προνομιούχο ή μη προνομιούχο λογισμικό δεν μπορεί να έχει πρόσβαση στο περιβάλλον χρόνου εκτέλεσης του θύλακα. Επιπλέον, η SGX μπορεί να παράγει ένα γνωμικό (quote), μια ψηφιακά υπογεγραμμένη βεβαίωση. Το γνωμικό μπορεί να πάρει την τιμή κατακερματισμού της εφαρμογής σε περιβάλλον enclave. Εν τω μεταξύ, το γνωμικό μπορεί να έχει πρόσβαση στα σχετικά δεδομένα κατά τη διάρκεια εκτέλεσης της εφαρμογής. Η όλη διαδικασία ανταλλαγής κωδικών χωρίζεται σε τρία βήματα:

- (1) Το PwdTheft παρέχει (pkC, A), το pkC είναι το δημόσιο κλειδί του C, και το A είναι ο λογαριασμός στόχος για κλοπή.
- (2) Η εφαρμογή που εκτελείται στο SGX, χρησιμοποιώντας το PW που παρέχεται από το P, συνδέεται στο λογαριασμό διακομιστή A, δημιουργώντας μια σύνδεση HTTPS.
- (3) Εάν τα προηγούμενα βήματα είναι επιτυχή, τα δεδομένα ct, σ και α θα μεταδοθούν στην PwdTheft. $ct = \text{enc}_{pkC} [PW]$ και $\sigma = \text{Sig}_{skapp} [ct]$. Το skapp είναι το ιδιωτικό κλειδί της υπογραφής της εφαρμογής. το α είναι ένα απόσπασμα που τρέχει στον οικοδεσπότη με δυνατότητα SGX της P.

Αφού ο PwdTheft λάβει ct, σ και α, ο C μπορεί να τους αποκρυπτογραφήσει για να επαληθεύσει τα δεδομένα και στη συνέχεια να αποφασίσει αν πρέπει να καταβληθεί μια ανταμοιβή στον P. Σε αυτή τη διαδικασία, για να αποτρέψει την P να αλλάξει κακόβουλα τον κωδικό μετά τη μετάδοση δεδομένων στο PwdTheft, μπορεί να προστεθεί μια χρονική σήμανση στα δεδομένα. Επιπλέον, το PwdTheft μπορεί εύκολα να επεκταθεί για τη διεξαγωγή άλλων κακόβουλων δραστηριοτήτων. Για παράδειγμα, οι εγκληματίες μπορούν να ωθήσουν τις CSCs να κάνουν συναλλαγές ευπάθειας 0 ημερών (0-day vulnerability transactions), οι οποίες είναι σημαντικός κυβερνο-οπλισμός.

- **Ευπάθειες στις έξυπνες συμβάσεις-συμβόλαια/Vulnerabilities in smart contract.**

Ως προγράμματα που λειτουργούν στο blockchain, τα έξυπνα συμβόλαια μπορεί να έχουν ευπάθειες ασφαλείας που προκαλούνται από ελαττώματα του προγράμματος. Στο [47] διεξάγεται συστηματική έρευνα για 12 τύπους ευπάθειας σε έξυπνα συμβόλαια, όπως φαίνεται στον παρακάτω πίνακα και προτείνεται ένα συμβολικό εργαλείο εκτέλεσης που ονομάζεται Oyente για να βρούν 4 είδη δυνητικών σφαλμάτων ασφαλείας. Ανακάλυψαν ότι 8833 από τις 19.366 έξυπνες συμβάσεις του Ethereum είναι ευάλωτες. Οι λεπτομέρειες αυτών των 4 σφαλμάτων έχουν ως εξής:

- **Εξάρτηση από την εντολή συναλλαγής (transaction-ordering dependence).** Οι έγκυρες συναλλαγές μπορούν να αλλάξουν την κατάσταση του μπλοκ αλφαριθμητικού Ethereum από σ σε σ' : $\sigma \vdash T \rightarrow \sigma'$. Σε κάθε εποχή, κάθε ανθρακωρύχος προτείνει το δικό του μπλοκ για να ενημερώσει το blockchain. Επειδή ένα μπλοκ μπορεί να περιέχει πολλαπλές συναλλαγές, η κατάσταση blockchain σ μπορεί να αλλάξει πολλές φορές μέσα σε μια εποχή. Όταν ένα νέο μπλοκ περιέχει δύο συναλλαγές T_i και T_j , οι οποίες επικαλούνται το ίδιο έξυπνο συμβόλαιο, αυτό μπορεί να προκαλέσει αυτήν την ευπάθεια. Επειδή η εκτέλεση της έξυπνης σύμβασης σχετίζεται με την κατάσταση σ , η εντολή εκτέλεσης των T_i και T_j επηρεάζουν την τελική κατάσταση. Η σειρά εκτέλεσης των συναλλαγών εξαρτάται αποκλειστικά από τους ανθρακωρύχους. Στην περίπτωση αυτή, οι συμβάσεις TOD (εξαρτώμενες από την εντολή συναλλαγής) είναι ευάλωτες.
- **Εξάρτηση χρονικής σήμανσης/Timestamp dependence.** Στο blockchain, κάθε μπλοκ έχει μια χρονική σήμανση. Ορισμένες προϋποθέσεις ενεργοποίησης έξυπνων συμβολαίων εξαρτώνται από τη χρονική σήμανση, η οποία καθορίζεται από τον ανθρακωρύχο σύμφωνα με τον τοπικό χρόνο του συστήματος. Εάν ένας εισβολέας μπορεί να το τροποποιήσει, οι συμβάσεις που εξαρτώνται από τη χρονική σήμανση είναι ευάλωτες.
- **Ελαττωματικές εξαιρέσεις (Mishandled exceptions).** Αυτή η κατηγορία ευπάθειας μπορεί να συμβεί όταν καλούνται διαφορετικές έξυπνες συμβάσεις η μία από την άλλη. Όταν η σύμβαση A καλεί τη σύμβαση B, αν η B τρέξει ασυνήθιστα, η B θα σταματήσει να τρέχει και να επιστρέψει «ψευδές». Σε ορισμένες επικλήσεις, η σύμβαση A πρέπει να ελέγξει ρητά την τιμή επιστροφής για να επαληθεύσει εάν η κλήση έχει εκτελεστεί σωστά. Αν το A δεν ελέγξει σωστά τις πληροφορίες εξαίρεσης, μπορεί να είναι ευάλωτο.
- **Ευπάθεια επανεμφάνισης.** Κατά την επίκληση της έξυπνης σύμβασης, η πραγματική κατάσταση του λογαριασμού της σύμβασης αλλάζει μετά την ολοκλήρωση της κλήσης. Ένας εισβολέας μπορεί να χρησιμοποιήσει την ενδιάμεση κατάσταση για να κάνει επανειλημμένες κλήσεις προς το έξυπνο συμβόλαιο. Αν το σύμβολο που επικαλείται περιλαμβάνει συναλλαγή Ether, μπορεί να οδηγήσει σε παράνομη κλοπή του Ether.

Ο παρακάτω πίνακας συγκεντρώνει μερικές ευπάθειες με τα αίτιά τους, ενώ ο πίνακας 15 παρουσιάζει τα under-optimized patterns και την κατηγορία στην οποία ανήκουν.

Αριθμός	Ευπάθεια	Αίτια	Επίπεδο
1	Call to the unknown	Απουσία της συνάρτησης που καλείται	Σύμβαση πηγαίου κώδικα
2	Out-of-gas send		
3	Exception disorder	Παρατυπία όσον αφορά την αντιμετώπιση των εξαιρέσεων	
4	Type casts	Type-check λάθος στην εκτέλεση συμβολαίου	
5	Reentrancy	Η συνάρτηση ξανακαλείται πριν τον τερματισμό	
6	Field disclosure	Η ιδιωτική τιμή γνωστοποιείται από τον miner	
7	Immutable bug	Αλλαγή μιας σύμβασης μετά την ανάπτυξη	EVM Bytecode
8	Ether lost	Αποστολή ether σε ορφανή διεύθυνση	
9	Stack Overflow	Το πλήθος των τιμών στο stack ξεπερνά το 1024	
10	Unpredictable State	Η κατάσταση της σύμβασης αλλάζει πριν επικαλεστεί	Μηχανισμός Blockchain
11	Randomness bug	Το seed είναι προκατελημμένο από κακόβουλο miner	
12	Timestamp dependence	Η χρονική σήμανση του block έχει αλλάξει από κακόβουλο miner	

Πίνακας 14. Προαναφερθείσες ευπάθειες και αίτια αυτών

- **Under-optimized smart contract**

Όταν ένας χρήστης αλληλεπιδρά με ένα έξυπνο συμβόλαιο που αναπτύσσεται στο Ethereum, χρεώνεται κάποια ποσότητα αερίου (gas). Το αέριο μπορεί να ανταλλαγεί με Ether, το οποίο είναι το κρυπτονόμισμα στο Ethereum. Δυστυχώς, η ανάπτυξη συμβολαίων δεν είναι επαρκώς βελτιστοποιημένη. Στο [48] προσδιορίζονται 7 μοντέλα που κοστίζουν αέριο και τα ομαδοποιούν σε 2 κατηγορίες (όπως φαίνεται στον παρακάτω πίνακα): σχέδια που σχετίζονται με άχρηστο κώδικα και μοτίβα που σχετίζονται με το βρόχο. Προτείνεται ένα εργαλείο που ονομάζεται Gasper, το οποίο μπορεί να ανακαλύψει αυτόματα 3 μοντέλα κόστους αερίου σε έξυπνα συμβόλαια: νεκρό κώδικα, αδιαφανές κατηγορημα (opaque predicate) και δαπανηρές λειτουργίες σε βρόχο. Χρησιμοποιώντας το Gasper, διαπιστώνεται ότι πάνω από 80% έξυπνων συμβολαίων που αναπτύσσονται στο Ethereum (4240 πραγματικά έξυπνα συμβόλαια) έχουν τουλάχιστον ένα από αυτά τα 3 πρότυπα. Οι λεπτομέρειες είναι οι εξής:

- **Νεκρός κώδικας/Dead code.** Σημαίνει ότι ορισμένες λειτουργίες σε ένα έξυπνο συμβόλαιο δεν θα εκτελεστούν ποτέ, αλλά θα εξακολουθήσουν να χρησιμοποιούνται στο blockchain. Δεδομένου ότι στην έξυπνη διαδικασία ανάπτυξης συμβολαίων η κατανάλωση αερίου σχετίζεται με το μέγεθος bytecode, ο νεκρός κώδικας θα προκαλέσει πρόσθετη κατανάλωση αερίου.

- **Αδιαφανές κατηγορημα/Opaque predicate.** Για ορισμένες δηλώσεις (statements) σε μια έξυπνη σύμβαση, τα αποτελέσματα εκτέλεσής τους είναι πάντα τα ίδια και δεν θα επηρεάσουν άλλες δηλώσεις ούτε το έξυπνο συμβόλαιο. Η παρουσία του αδιαφανούς κατηγορήματος προκαλεί το EVM να εκτελέσει άχρηστες λειτουργίες, καταναλώνοντας έτσι επιπλέον αέριο.
- **Ακριβείς εργασίες σε βρόχο/Expensive operations in a loop.** Αναφέρεται σε μερικές δαπανηρές λειτουργίες εντός ενός βρόχου, οι οποίες μπορούν να μετακινηθούν εκτός του βρόχου για να εξοικονομήσουν κατανάλωση αερίου.

- **Under-priced operations**

Όπως αναφέρθηκε προηγουμένως, κάθε πράξη έχει οριστεί σε μια συγκεκριμένη τιμή αερίου στο Ethereum. Το Ethereum ρυθμίζει την τιμή αερίου με βάση τον χρόνο εκτέλεσης, το εύρος ζώνης, την κατοχή μνήμης και άλλες παραμέτρους. Γενικά, η τιμή του αερίου είναι ανάλογη προς τους υπολογιστικούς πόρους που καταναλώνονται από τη λειτουργία. Ωστόσο, είναι δύσκολο να μετρηθεί με ακρίβεια η κατανάλωση υπολογιστικών πόρων μιας μεμονωμένης λειτουργίας και επομένως ορισμένες τιμές αερίου δεν έχουν ρυθμιστεί σωστά. Παραδείγματος χάριν, ορισμένες τιμές αερίου των λειτουργιών βαρέος τύπου IO ρυθμίζονται πολύ χαμηλά και επομένως αυτές οι λειτουργίες μπορούν να εκτελεστούν σε ποσότητα σε μία συναλλαγή. Με αυτόν τον τρόπο, ένας εισβολέας μπορεί να ξεκινήσει μια επίθεση DoS (Denial of Service) στο Ethereum.

Στην πραγματικότητα, οι επιτιθέμενοι έχουν εκμεταλλευτεί την χαμηλού κόστους λειτουργία EXTCODESIZE για να επιτεθούν στην Ethereum. Όταν εκτελείται το EXTCODIZE, πρέπει να διαβάσει πληροφορίες κατάστασης και στη συνέχεια ο κόμβος θα διαβάσει τον σκληρό δίσκο. Δεδομένου ότι η τιμή αερίου του EXTCODESIZE είναι μόνο 20, ο επιτιθέμενος μπορεί να το καλέσει περισσότερο από 50.000 φορές σε μία συναλλαγή. Αυτό θα προκαλέσει στον χρήστη να καταναλώσει πολλούς υπολογιστικούς πόρους και ο συγχρονισμός των μπλοκ θα είναι σημαντικά πιο αργός σε σύγκριση με την κανονική κατάσταση. Ως άλλο παράδειγμα, ορισμένοι επιτιθέμενοι εκμεταλλεύτηκαν την υποτιμημένη λειτουργία SUICIDE για να ξεκινήσουν επιθέσεις DoS. Χρησιμοποιήθηκε το SUICIDE για να δημιουργηθούν περίπου 19 εκατομμύρια άδεια λογαριασμοί, οι οποίοι πρέπει να αποθηκευτούν στο κρατικό δέντρο (state tree). Αυτή η επίθεση προκάλεσε σπατάλη πόρων σκληρού δίσκου. Ταυτοχρόνως, ο συγχρονισμός πληροφοριών κόμβου και η ταχύτητα επεξεργασίας συναλλαγών μειώνονται σημαντικά. Προκειμένου να επιλυθεί το πρόβλημα ασφάλειας που προκαλείται από τις πράξεις υποτιμολόγησης, οι τιμές αερίου 7 επιχειρησιακών εργασιών μεγάλης κλίμακας τροποποιούνται σε EIP (Ethereum Improvement Proposal) 150 [\[49\]](#), όπως φαίνεται στον παρακάτω πίνακα. Σημειώστε ότι το EIP150 έχει ήδη εφαρμοστεί στην δημόσια αλυσίδα Ethereum με σκληρό πιρούνι και οι νέες παράμετροι του πίνακα αερίου χρησιμοποιούνται μετά το μπλοκ No.2463000.

Αριθμός	Under-optimized pattern	Κατηγορία
1	Νεκρός κώδικας	Πρότυπα σχετικά με άχρηστο κώδικα
2	Αδιαφανές κατηγορήμα	
3	Ακριβείς εργασίες	Πρότυπα σχετικά με βρόγχους
4	Συνεχής έκβαση	
5	Σύντηξη βρόγχου	
6	Αλληπάλληλοι υπολογισμοί	
7	Σύγκριση με μονομερή έκβαση	

Πίνακας 15. Τα under-optimized patterns και η κατηγορία στην οποία ανήκουν

Αριθμός	Λειτουργία	Παλιά Τιμή	Τιμή EIP150
1	EXTCODESIZE	20	700
2	EXTCODECOPY	20	700
3	BALANCE	20	400
4	SLOAD	50	200
5	CALL	40	700
6	SUICIDE (δε δημιουργεί λογαριασμό)	0	5000
7	SUICIDE (δημιουργεί λογαριασμό)	0	25000

Πίνακας 16. Τροποποίηση Gas στο EIP150

4.6 Σενάρια Επιθέσεων/Attack cases.

- **Εγωιστική επίθεση εξόρυξης /Selfish mining attack.**

Η εγωιστική επίθεση εξόρυξης διεξάγεται από επιτιθέμενους (δηλαδή εγωιστές ανθρακωρύχους) με σκοπό την απόκτηση αδικαιολόγητων ανταμοιβών ή τη σπατάλη της υπολογιστικής ισχύος των ειλικρινών ανθρακωρύχων . Ο επιτιθέμενος αποκαλύπτει ιδιωτικά τα μπλοκ και στη συνέχεια επιχειρεί να περάσει μια ιδιωτική αλυσίδα. Στη συνέχεια, οι εγωιστές ανθρακωρύχοι θα βρεθούν σε αυτή την ιδιωτική αλυσίδα και θα προσπαθήσουν να διατηρήσουν έναν ιδιωτικό κλάδο μεγαλύτερο από τον δημόσιο κλάδο, επειδή κατέχουν περισσότερα ιδιωτικά μπλοκ που ανακάλυψαν πρόσφατα. Εν τω μεταξύ, οι ειλικρινείς ανθρακωρύχοι συνεχίζουν να εξορύζουν τη δημόσια αλυσίδα. Τα νέα μπλοκ που εξορύσσονται από τον επιτιθέμενο θα αποκαλυφθούν όταν το δημόσιο κλάδο

προσεγγίσει το μήκος του ιδιωτικού κλάδου, έτσι ώστε οι ειλικρινείς ανθρακωρύχοι καταλήγουν να σπαταλούν υπολογιστική ισχύ και να μην κερδίζουν καμία ανταμοιβή, επειδή οι εγωιστές ανθρακωρύχοι δημοσιεύουν τα νέα μπλοκ λίγο πριν από τους έντιμους ανθρακωρύχους. Ως αποτέλεσμα, οι εγωιστές ανθρακωρύχοι κερδίζουν ένα ανταγωνιστικό πλεονέκτημα και οι έντιμοι ανθρακωρύχοι θα ενθαρρυνθούν να ενταχθούν στο κλαδί που διατηρούν οι εγωιστές ανθρακωρύχοι. Μέσω μιας περαιτέρω ενοποίησης της εξουσίας εξόρυξης προς όφελος του εισβολέα, αυτή η επίθεση υπονομεύει τον χαρακτήρα αποκέντρωσης του blockchain.

Στο [50] προτείνεται μια στρατηγική επίθεσης με την ονομασία Selfish-Mine, η οποία μπορεί να αναγκάσει τους έντιμους ανθρακωρύχους να εκτελέσουν σπαταλημένους (wasted) υπολογισμούς στον κλασσικό δημόσιο κλάδο. Στην αρχική περίπτωση του Selfish-Mine, το μήκος της δημόσιας αλυσίδας και της ιδιωτικής αλυσίδας είναι το ίδιο. Το Selfish-Mine περιλαμβάνει τα ακόλουθα τρία σενάρια:

(1) **Η δημόσια αλυσίδα είναι μεγαλύτερη από την ιδιωτική αλυσίδα.** Δεδομένου ότι η υπολογιστική ισχύς των εγωιστών ανθρακωρύχων μπορεί να είναι μικρότερη από εκείνη των ειλικρινών ανθρακωρύχων, οι εγωιστές ανθρακωρύχοι θα επικαιροποιήσουν την ιδιωτική αλυσίδα σύμφωνα με την δημόσια αλυσίδα και σε αυτό το σενάριο, οι εγωιστές ανθρακωρύχοι δεν μπορούν να κερδίσουν ανταμοιβή.

(2) **Οι εγωιστές ανθρακωρύχοι και οι έντιμοι ανθρακωρύχοι βρίσκουν σχεδόν ταυτόχρονα το πρώτο νέο μπλοκ.** Σε αυτό το σενάριο, εγωιστές ανθρακωρύχοι θα δημοσιεύσουν το νεοανακαλυφθέν μπλοκ, και θα υπάρχουν δύο ταυτόχρονα πιρούνια του ίδιου μήκους. Οι ειλικρινείς ανθρακωρύχοι θα δουν στο καθένα από τα δύο κλαδιά, ενώ οι εγωιστές ανθρακωρύχοι θα συνεχίσουν να εξορύσσονται στην ιδιωτική αλυσίδα. Εάν οι εγωιστές ανθρακωρύχοι βρουν πρώτα το δεύτερο νέο μπλοκ, θα δημοσιεύσουν αυτό το μπλοκ αμέσως. Σε αυτό το σημείο, οι εγωιστές ανθρακωρύχοι θα κερδίσουν ταυτόχρονα δύο ανταμοιβές. Επειδή η ιδιωτική αλυσίδα είναι μεγαλύτερη από τη δημόσια αλυσίδα, η ιδιωτική αλυσίδα θα είναι ο τελικός έγκυρος κλάδος. Εάν οι ειλικρινείς ανθρακωρύχοι βρουν πρώτα το δεύτερο νέο μπλοκ και αυτό το μπλοκ γράφεται στην ιδιωτική αλυσίδα, οι εγωιστές ανθρακωρύχοι θα κερδίσουν τις πρώτες νέες ανταμοιβές του μπλοκ και οι ειλικρινείς ανθρακωρύχοι θα κερδίσουν τις ανταμοιβές του δεύτερου νέου μπλοκ. Διαφορετικά, αν αυτό το μπλοκ είναι γραμμένο στο δημόσιο μπλοκ, οι αληθινοί ανθρακωρύχοι θα κερδίσουν τις ανταμοιβές των δύο νέων μπλοκ και οι εγωιστές ανθρακωρύχοι δεν θα κερδίσουν ανταμοιβή.

(3) **Αφού οι εγωιστές ανθρακωρύχοι βρίσκουν το πρώτο νέο μπλοκ, βρίσκουν επίσης το δεύτερο νέο μπλοκ.** Σε αυτό το σενάριο, οι εγωιστές ανθρακωρύχοι θα κρατήσουν αυτά τα δύο νέα μπλοκ ιδιωτικά και συνεχίζουν να εξορύσσουν νέα μπλοκ στην ιδιωτική αλυσίδα. Όταν το πρώτο νέο μπλοκ θα βρεθεί από ειλικρινείς ανθρακωρύχους, οι εγωιστές ανθρακωρύχοι θα δημοσιεύσουν το πρώτο τους νέο μπλοκ.

Όταν οι έντιμοι ανθρακωρύχοι βρουν το δεύτερο νέο μπλοκ, οι εγωιστές ανθρακωρύχοι θα δημοσιεύσουν αμέσως το δικό τους δεύτερο νέο μπλοκ. Στη συνέχεια, οι εγωιστές ανθρακωρύχοι θα ακολουθήσουν αυτή την αντίδραση με τη σειρά τους, μέχρι το μήκος της δημόσιας αλυσίδας να είναι μόνο 1 μεγαλύτερο από την ιδιωτική αλυσίδα, μετά την οποία οι εγωιστές ανθρακωρύχοι θα

δημοσιεύσουν το τελευταίο νέο μπλοκ πριν οι ειλικρινείς ανθρακωρύχοι βρουν αυτό το μπλοκ. Σε αυτό το σημείο, η ιδιωτική αλυσίδα θα θεωρηθεί έγκυρη και συνεπώς οι εγωιστές ανθρακωρύχοι θα κερδίσουν τις ανταμοιβές όλων των νέων μπλοκ.

Αριθμός	Περίπτωση Επίθεσης	Σχετικές Ευπάθειες
1	King of the ether throne	Out-of-gas send Exception disorder
2	Multi-player games	Field disclosure
3	Επίθεση Rubixi	Immutable bug
4	Επίθεση GovernMental	Immutable bug Stack Overflow Unpredictable state Timestamp dependence
5	Επίθεση δυναμικών βιβλιοθηκών	Unpredictable state

Πίνακας 17. Επιθέσεις που εκμεταλλεύονται τις ευπάθειες των έξυπνων συμβολαίων

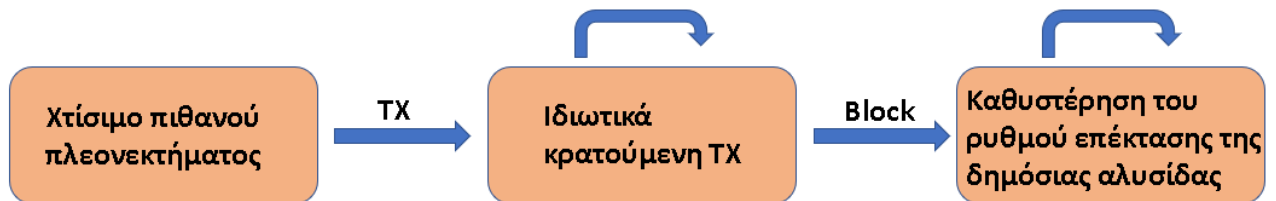
- **DAO επίθεση/attack.**

Το DAO είναι ένα έξυπνο συμβόλαιο που αναπτύχθηκε στο Ethereum στις 28 Μαΐου του 2016, το οποίο υλοποιεί μια πλατφόρμα χρηματοδότησης από το πλήθος. Η σύμβαση DAO δέχθηκε επίθεση 20 μέρες μετά την κυκλοφορία της. Πριν από την επίθεση που συνέβη, η DAO είχε ήδη συγκεντρώσει 150 εκατομμύρια δολάρια ΗΠΑ, το οποίο είναι η μεγαλύτερη χρηματοδότηση από το πλήθος στην ιστορία. Ο επιτιθέμενος έκλεψε περίπου 60 εκατομμύρια δολάρια ΗΠΑ.

Ο επιτιθέμενος εκμεταλλεύτηκε την ευπάθεια της επανάκτησης (reentrancy) σε αυτή την περίπτωση. Πρώτον, ο επιτιθέμενος δημοσιεύει μια κακόβουλη έξυπνη σύμβαση, η οποία περιλαμβάνει μια withdraw() function call προς τη DAO στη λειτουργία επανάκλησης. Η withdraw () θα στείλει το Ether στον καλούντα, ο οποίος έχει επίσης τη μορφή κλήσης. Επομένως, θα επικαλεστεί πάλι τη λειτουργία επανάκλησης του κακόβουλου έξυπνου συμβολαίου. Με αυτόν τον τρόπο, ο εισβολέας είναι σε θέση να κλέψει όλους τους Ether από το DAO. Υπάρχουν κάποιες άλλες περιπτώσεις που εκμεταλλεύονται τις ευπάθειες των έξυπνων συμβάσεων, οι οποίες παρατίθενται στον παρακάτω πίνακα.

Αριθμός	Επίθεση	Επίπτωση
1	Engineering block races	Ξόδεμα ισχύος εξόρυξης σε ορφανά μπλοκ Πρόκληση 51% ευπάθειας Ο επιτιθέμενος ενδέχεται να κερδίσει περισσότερα από τις φυσιολογικές επιβραβεύσεις εξόρυξης
2	Splitting mining power	
3	Selfish mining	
4	0-confirmation double spend	Ο vendor δεν θα επιβραβευθεί για τις υπηρεσίες του
5	N-confirmation double spend	

Πίνακας 18. Μερικές ακόμη επιθέσεις που δύναται να προκληθούν από την επίθεση eclipse



Πίνακας 19. Σύνοψη της διαδικασίας επίθεσης Liveness

- **BGP hijacking επίθεση/attack.**

Το BGP (Border Gateway Protocol) είναι ένα πρωτόκολλο δρομολόγησης και ρυθμίζει τον τρόπο προώθησης των πακέτων IP στον προορισμό τους. Για να παρεμποδίσουν την κυκλοφορία του blockchain στο δίκτυο, οι επιτιθέμενοι αξιοποιούν ή χειραγωγούν τη δρομολόγηση BGP. Το BGP hijacking συνήθως απαιτεί τον έλεγχο των χειριστών δικτύου, οι οποίοι θα μπορούσαν ενδεχομένως να αξιοποιηθούν για να καθυστερήσουν μηνύματα δικτύου. Το [51] αναλύει διεξοδικά την επίδραση των επιθέσεων δρομολόγησης, συμπεριλαμβανομένων των επιθέσεων σε επίπεδο κόμβου και επιπέδου δικτύου στο Bitcoin και να δείξει ότι ο αριθμός των επιτυχώς πιθανών για να υποπέσουν σε πειρατεία διαδικτυακών προθημάτων (prefixes) εξαρτάται από την κατανομή της δύναμης εξόρυξης. Λόγω της μεγάλης συγκέντρωσης κάποιων Bitcoin mining pools, αν επιτεθεί από BGP hijacking, θα έχει σημαντική επίδραση. Οι εισβολείς μπορούν να χωρίσουν αποτελεσματικά το δίκτυο Bitcoin ή να καθυστερήσουν την ταχύτητα της διάδοσης των μπλοκ. Οι επιτιθέμενοι διεξάγουν BGP hijacking για να παρακολουθήσουν τις συνδέσεις των ανθρακωρύχων Bitcoin με έναν εξυπηρετητή mining pool, όπως αναλύθηκε από την Dell Secure Works το 2014.

Με τη μετατόπιση της επισκεψιμότητας σε μια ομάδα εξόρυξης που ελέγχεται από τον εισβολέα, ήταν δυνατό να κλαπεί η κρυπτοσυχνότητα από το θύμα. Αυτή η επίθεση συνέλεξε περίπου 83.000 δολάρια ΗΠΑ κρυπτογράφησης για περίοδο δύο μηνών. Δεδομένου ότι οι επεκτάσεις ασφαλείας του BGP δεν αναπτύσσονται

ευρέως, οι φορείς εκμετάλλευσης δικτύων πρέπει να βασίζονται σε συστήματα παρακολούθησης, τα οποία θα αναφέρουν ανακριβείς ανακοινώσεις, όπως το BGPMon [52]. Ωστόσο, ακόμα και αν εντοπιστεί κάποια επίθεση, η επίλυση ενός χρόνου hijacking εξακολουθεί να κοστίζει, καθώς πρόκειται για διαδικασία που βασίζεται στον άνθρωπο και συνίσταται στην αλλαγή της διαμόρφωσης ή στην αποσύνδεση του εισβολέα. Για παράδειγμα, το YouTube χρειάστηκε περίπου τρεις ώρες για να επιλύσει μια hijacking των prefixes του από Πακιστανούς παρόχους υπηρεσιών διαδικτύου (Internet Service Provider) [53].

- **Eclipse επίθεση/attack.**

Η Eclipse attack επιτρέπει σε έναν εισβολέα να μονοπωλεί όλες τις εισερχόμενες και εξερχόμενες συνδέσεις του θύματος, οι οποίες απομονώνουν το θύμα από τους άλλους peers του δικτύου. Στη συνέχεια, ο επιτιθέμενος μπορεί να φιλτράρει την άποψη του θύματος σχετικά με το blockchain ή να αφήσει το θύμα να καταναλώσει άσκοπη υπολογιστική ισχύ σε παρωχημένες προβολές του blockchain. Επιπλέον, ο επιτιθέμενος είναι σε θέση να αξιοποιήσει την υπολογιστική δύναμη του θύματος ώστε να διεξάγει τις δικές του κακόβουλες πράξεις. Στο [54] θεωρούν δύο τύπους επίθεσης έκλειψης στο δίκτυο ομότιμων χρηστών του Bitcoin, δηλαδή επίθεση κατά του botnet και επίθεση υποδομής. Η επίθεση του botnet ξεκινάει από bots με ποικίλες διευθύνσεις διευθύνσεων IP. Η επίθεση υποδομής διαμορφώνει την απειλή από έναν ISP, μια εταιρεία ή ένα έθνος-κράτος που έχει συνεχόμενες διευθύνσεις IP. Το δίκτυο Bitcoin ενδέχεται να υποστεί βλάβη και η οπτική του θύματος στο blockchain θα φιλτραριστεί λόγω της επίθεσης έκλειψης. Επιπλέον, η Eclipse attack αποτελεί χρήσιμη βάση για άλλες επιθέσεις, όπως φαίνεται στον παρακάτω πίνακα.

- **Liveness attack**

Στο [55] προτείνουν την Liveness attack, η οποία είναι σε θέση να καθυστερήσει όσο το δυνατόν περισσότερο τον χρόνο επιβεβαίωσης μιας συναλλαγής στόχου. Παρουσιάζουν επίσης δύο περιπτώσεις μιας τέτοιας επίθεσης σε Bitcoin και Ethereum. Η Liveness attack έχει τρεις φάσεις, δηλαδή φάση προετοιμασίας επίθεσης, φάση άρνησης συναλλαγής και φάση επιβράδυνσης φραγμού (που φαίνεται στον παρακάτω πίνακα):

(1) Φάση προετοιμασίας επίθεσης (attack preparation phase). Ακριβώς όπως η εγωιστική επίθεση εξόρυξης, ένας επιτιθέμενος χτίζει πλεονέκτημα έναντι των ειλικρινών ανθρακωρύχων με κάποιο τρόπο πριν η συναλλαγή-στόχος TX μεταδοθεί προς την δημόσια αλυσίδα. Ο επιτιθέμενος χτίζει την ιδιωτική αλυσίδα, η οποία είναι μεγαλύτερη από την δημόσια αλυσίδα.

(2) Φάση άρνησης συναλλαγής (transaction denial phase). Ο εισβολέας κρατά ιδιωτικά το μπλοκ που περιέχει το TX, προκειμένου να αποφευχθεί η εγγραφή του TX στην δημόσια αλυσίδα.

(3) Φάση επιβράδυνσης Blockchain (Blockchain retarder phase). Στην αναπτυξιακή διαδικασία της δημόσιας αλυσίδας, η TX δεν θα είναι πλέον σε θέση να διεξαχθεί σε συγκεκριμένο χρόνο. Σε αυτή την περίπτωση, ο εισβολέας θα δημοσιεύσει το μπλοκ που περιέχει TX. Σε ορισμένα συστήματα blockchain, όταν το βάθος του μπλοκ που περιέχει το TX είναι μεγαλύτερο από μια σταθερά, το TX θεωρείται έγκυρο. Ως εκ τούτου, ο επιτιθέμενος θα συνεχίσει να κατασκευάζει ιδιωτική αλυσίδα προκειμένου να δημιουργήσει πλεονέκτημα έναντι της δημόσιας

αλυσίδας. Μετά από αυτό, ο επιτιθέμενος θα δημοσιεύσει τα ιδιόκτητα μπλοκ του σε δημόσια αλυσίδα σε εύθετο χρόνο για να επιβραδύνει τον ρυθμό ανάπτυξης της δημόσιας αλυσίδας. Η επίθεση ζωής θα λήξει όταν το TX επαληθεύεται ως έγκυρο στην δημόσια αλυσίδα.

- **Επίθεση ισορροπίας/Balance attack.**

Το [56] προτείνει την επίθεση ισορροπίας εναντίον του PoWbased blockchain, η οποία επιτρέπει σε έναν εισβολέα χαμηλής εξορυκτικής δύναμης να διαταράξει στιγμιαία τις επικοινωνίες μεταξύ υποομάδων με παρόμοια εξόρυξη. Ανακάλυψαν blockchain σε ένα δέντρο DAG (κατευθυνόμενο ακυκλικό γράφημα), στο οποίο $DAG = \langle B, P \rangle$. Οι B είναι οι κόμβοι που υποδεικνύουν τις πληροφορίες των μπλοκ και συνδέονται μέσω των κατευθυνόμενων άκρων P. Μετά την καθυστέρηση μεταξύ των σωστών υποομάδων ισοδύναμης εξόρυξης, ο εισβολέας εκδίδει συναλλαγές σε μία υποομάδα (αποκαλούμενη «υποομάδα συναλλαγών») μια άλλη υποομάδα (αποκαλούμενη υποομάδα μπλοκ) για να εγγυηθεί ότι το δέντρο της υποομάδας μπλοκ ξεπερνά το δέντρο της υποομάδας συναλλαγών. Παρόλο που οι συναλλαγές διαπράττονται, ο επιτιθέμενος είναι σε θέση να αντισταθμίσει το δέντρο που περιέχει αυτή τη συναλλαγή και να ξαναγράψει τα μπλοκ με μεγάλη πιθανότητα.

Η επίθεση ισορροπίας παραβιάζει εγγενώς την εμμονή του κύριου κλαδιού και επιτρέπει τις διπλές δαπάνες. Ο επιτιθέμενος πρέπει να εντοπίσει την υποομάδα που εμπλέκεται στο εμπόριο και να δημιουργήσει συναλλαγές για την αγορά αγαθών από αυτούς τους εμπόρους. Στη συνέχεια, ο εισβολέας εκδίδει συναλλαγές σε αυτήν την υποομάδα και προωθεί τα εξορυσσόμενα μπλοκ στους υπόλοιπους κόμβους της ομάδας. Με μεγάλη πιθανότητα το δέντρο DAG που βλέπει ο έμπορος να αντισταθμίζεται από ένα άλλο δέντρο, ο επιτιθέμενος θα μπορούσε να επαναδημιουργήσει εκ νέου μια άλλη συναλλαγή χρησιμοποιώντας ακριβώς τα ίδια νομίσματα. Η επίθεση εξισορρόπησης αποδεικνύει ότι PoW based blockchain είναι αποκλεισμένο. Δηλαδή, όταν γράφεται μια συναλλαγή στην κύρια αλυσίδα, υπάρχει μια πιθανότητα ότι ο εισβολέας μπορεί να παρακάμψει ή να διαγράψει το μπλοκ που περιέχει αυτή τη συναλλαγή. Στο σχετικό πείραμα, οι συγγραφείς διαμορφώνουν μια ιδιωτική αλυσίδα Ethereum με ισοδύναμες παραμέτρους της κοινοπραξίας R3 και έδειξαν ότι μπορούν να εκτελέσουν με επιτυχία την επίθεση ισορροπίας, η οποία χρειάζεται μόνο να ελέγξει περίπου το 5% της συνολικής υπολογιστικής ισχύος.

4.7. Προβλήματα ασφάλειας στο blockchain.

Με τη συνεχή αύξηση της παγκόσμιας προσοχής στο blockchain, η έρευνα που σχετίζεται με το blockchain γίνεται σε πλήρη εξέλιξη. Αλλά αντικειμενικά, όπως φαίνεται από το στρώμα εφαρμογής, το blockchain βρίσκεται ακόμα στο ερευνητικό του στάδιο. Υπάρχει ακόμα μια μακρά διαδικασία ενσωμάτωσης και ανάπτυξης για να προχωρήσουμε μέχρι την τελειότητα της τεχνολογίας και την εμβάθυνση της εφαρμογής. Παρά τις καινοτόμες αλλαγές του blockchain, η ίδια η τεχνολογία εξακολουθεί να παρουσιάζει ορισμένους εγγενείς κινδύνους για την ασφάλεια.

Επιπλέον, η επαναστατική φύση της αποκέντρωσης και της αυτο-οργάνωσης στο blockchain έχει ήδη προκαλέσει άγνωστα προβλήματα ασφάλειας [57],[58] .

4.7.1. Τεχνικοί περιορισμοί.

- **Ο περιορισμός της χωρητικότητας μπλοκ περιορίζει σε μεγάλο βαθμό την ευρεία εφαρμογή μπλοκ αλυσίδων.**

Η χωρητικότητα ενός μπλοκ είχε οριστεί αρχικά σε 1MB για να αντισταθεί σε πιθανές επιθέσεις DoS. Και υπήρξε πάντα μια διαμάχη μεταξύ μεγαλύτερης ή μικρότερης χωρητικότητας μπλοκ. Επειδή ένα μεγαλύτερο μπλοκ μπορεί να αποθηκεύσει περισσότερα αρχεία το οποίο θα απαιτήσει την ανάπτυξη. Όμως, μεγαλύτερα μπλοκ μπορεί να προκαλέσουν δυσκολία στην εκτέλεση και διαχείριση κόμβων blockchain. Από την άλλη πλευρά, παρόλο που τα μικρότερα μπλοκ είναι εύκολο να διαχειριστούν και είναι πιο αξιόπιστα σε μια λύση πληρωμής τρίτου μέρους (third party payment solution), ο διαθέσιμος χώρος είναι εξαιρετικά περιορισμένος, ειδικά σε πολύπλοκα περιβάλλοντα μεγάλων δεδομένων.

- **Ο μηχανισμός καταναμημένου αποθηκευτικού χώρου δημιουργεί ένα boarder attack surface στο blockchain.** Ένα σύστημα blockchain επιλέγει να αποθηκεύσει ένα πλήρες αντίγραφο όλων των δεδομένων από την πλευρά του κάθε χρήστη. Αυτό σημαίνει ότι ένας εισβολέας θα έχει περισσότερες εναλλακτικές λύσεις για να έχει πρόσβαση σε αυτά τα δεδομένα. Αν και το περιεχόμενο στο blockchain δεν επιτρέπεται να αλλοιωθεί, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν άλλες τεχνικές, όπως η εξόρυξη δεδομένων και η ανάλυση συσχετισμού, για να ανακτήσουν πολύτιμες πληροφορίες σχετικά με εφαρμογές blockchain, χρήστες, δίκτυο , δομή κλπ.

- **Ο μηχανισμός συναίνεσης μπορεί να προκαλέσει συνεταιριστική επίθεση.** Ο μηχανισμός συναίνεσης του blockchain βασίζεται στην υπόθεση ότι η πλειοψηφία των κόμβων είναι ειλικρινής για να τρέξει και να διατηρήσει το σύστημα. Μόλις ένας ή περισσότεροι κόμβοι ελέγξουν περισσότερο από 51% την υπολογιστική ισχύ ολόκληρου του συστήματος, μπορούν να ενώσουν μαζί για να ξεκινήσουν μια επίθεση για να παραβιάσουν το περιεχόμενο σε μπλοκ και να διεξάγουν καταστροφικές επιθέσεις όπως το DoS.

4.7.2. Πιθανός κίνδυνος εφαρμογής κρυπτογραφίας.

- **Το πρόβλημα της διαχείρισης ιδιωτικού κλειδιού δεν λύνεται με blockchain.** Οι υπάρχουσες εφαρμογές blockchain χρησιμοποιούν συνήθως ιδιωτικό κλειδί για να επιβεβαιώσουν την ταυτότητα ενός χρήστη και να ολοκληρώσουν μια συναλλαγή πληρωμής. Έτσι, η προϋπόθεση ότι η πληροφορία δεν μπορεί να παραποιηθεί είναι η ασφάλεια του ιδιωτικού κλειδιού. Σε αντίθεση με την παραδοσιακή κρυπτογραφία δημόσιου κλειδιού, οι χρήστες blockchain είναι υπεύθυνοι για τα δικά τους ιδιωτικά κλειδιά, πράγμα που σημαίνει ότι παράγεται ένα ιδιωτικό κλειδί και φροντίζεται από τον χρήστη αντί τρίτου. Εάν ένας χρήστης χάσει το ιδιωτικό του κλειδί, θα είναι αδύνατο να αποκτήσει πρόσβαση στα ψηφιακά του στοιχεία σε blockchain.

- **Η ευρεία εφαρμογή του κρυπτογραφικού αλγορίθμου μπορεί να εισάγει άγνωστα backdoors ή ευπάθειες.** Υπάρχει εκτεταμένη υιοθέτηση

κρυπτογραφικών αλγορίθμων σε blockchain, όπως ECC και RSA. Τα backdoors και τα τρωτά σημεία ασφαλείας ενδέχεται να προκύψουν στους ίδιους τους αλγόριθμους ή στις διαδικασίες υλοποίησης. Και στη συνέχεια να βλάψουν τις εφαρμογές blockchain και ολόκληρο το σύστημα. Επιπλέον, οι νέες τεχνολογίες πληροφορικής, όπως ο κβαντικός υπολογιστής, θα αυξήσουν επίσης την πιθανότητα πυρόλυσης (cracking) των ασύμμετρων αλγορίθμων κρυπτογράφησης.

4.7.3. Οι πλατφόρμες Blockchain Opensource προσελκύουν έντονες επιθέσεις.

Ως βασική τεχνολογία των εφαρμογών ανώτερου στρώματος, η πλατφόρμα blockchain υποστηρίζει τη διαλειτουργικότητα διαφορετικών εφαρμογών και χρηστών. Για παράδειγμα, μπορούν να παραχθούν, να αποθηκευτούν, να ενημερωθούν και να μεταδοθούν μέσω βιομηχανικής πλατφόρμας τα δεδομένα του κλάδου της ιατρικής, της οικονομικής και της επικοινωνίας. Το τεράστιο οικονομικό όφελος ενθαρρύνει τους χάκερς να αναζητούν τις αδυναμίες ασφάλειας της ανοικτής πλατφόρμας blockchain.

4.7.4. Διαχείριση της ασφάλειας της αυτο-οργάνωσης και της ανωνυμίας.

- **Η κατανεμημένη αποθήκευση δεδομένων μπορεί να προκαλέσει τη δημιουργία αυτόνομων και συχνών δεδομένων διασυννοριακά σε περιπτώσεις χρήσης blockchain.** Επειδή το blockchain υιοθετεί έναν κατανεμημένο τρόπο αποθήκευσης δεδομένων και διατηρεί ένα πλήρες αντίγραφο των δεδομένων από κάθε πλευρά του χρήστη. Μόλις προστεθεί μια νέα συναλλαγή σε ένα μπλοκ, όλα τα αντίγραφα δεδομένων πρέπει να ενημερώνονται συγχρονισμένα. Όταν οι χρήστες μπλοκ αλυσίδων προέρχονται από διαφορετικές χώρες, τα αρχικά και συχνά διασυννοριακά δεδομένα θα βελτιώσουν τη δυσκολία εποπτείας.

- **Ο μηχανισμός ανωνυμίας μπορεί να προκαλέσει πρόβλημα επίθεσης στο backtrack.** Το Blockchain υπολογίζει την τιμή κατακερματισμού του δημόσιου κλειδιού ενός χρήστη για τον εντοπισμό ενός μοναδικού χρήστη. Ωστόσο, αυτή η λειτουργία διατήρησης της ιδιωτικής ζωής καθιστά αδύνατη την επαλήθευση και την ανίχνευση της πραγματικής ταυτότητας του χρήστη κατά την επίθεση δικτύου και τον κανονισμό για την κυβερνοασφάλεια.

5. Λύσεις για εξειδικευμένες απειλές

Οι απειλές για την ασφάλεια στο blockchain εκμεταλλεύονται τα τρωτά σημεία των διαφόρων εξαρτημάτων όπως οι εφαρμογές / διεπαφές, τα συστατικά στοιχεία του δικτύου, το λογισμικό, το υλικολογισμικό και τις φυσικές συσκευές που υπάρχουν σε διαφορετικά επίπεδα. Οι χρήστες σε ένα πρότυπο δίκτυο αλληλεπιδρούν με αυτά τα στοιχεία μέσω πρωτοκόλλων που μπορούν επίσης να αποσυναρμολογηθούν από τα μέτρα ασφαλείας τους. Τα αντίμετρα για απειλές ασφάλειας αντιμετωπίζουν τις ευπάθειες αυτής της αλληλεπίδρασης σε διαφορετικά επίπεδα για να επιτευχθεί ένα συγκεκριμένο επίπεδο ασφάλειας. Τα διαφορετικά πρωτόκολλα που υποστηρίζουν την ανάπτυξη των εξαρτημάτων προσθέτουν στην πολυπλοκότητα αυτών των αντιμέτρων. Μια συγκριτική ανάλυση των απειλών για την ασφάλεια και οι πιθανές λύσεις τους δίδονται για το χαμηλό επίπεδο, το ενδιάμεσο επίπεδο κάτω από τη στρώση μεταφοράς, το ενδιάμεσο επίπεδο που περιλαμβάνει το στρώμα μεταφοράς και το υψηλό επίπεδο σε παρακάτω πίνακες. Η συγκριτική ανάλυση εξετάζει τις παραμέτρους των απειλών, τις επιπτώσεις τους, τα επηρεαζόμενα επίπεδα, τα αντίστοιχα επίπεδα και τις πιθανές λύσεις που προτείνονται.

5.1. Λύσεις ασφάλειας και διασφάλισης ιδιωτικότητας χαμηλού επιπέδου.

Για ασύρματα δίκτυα αισθητήρων, οι επιθέσεις παρεμβολής σχετίζονται με παρεμβολές που προκαλούν συγκρούσεις μηνυμάτων ή πλημμύρες των καναλιών. Μια προσέγγιση για την ανίχνευση jamming attack προτείνεται στο [60]. Η ανίχνευση των επιθέσεων γίνεται δυνατή με τη μέτρηση της έντασης του σήματος που στη συνέχεια χρησιμοποιείται για την εξαγωγή σημάτων που μοιάζουν με θόρυβο. Αυτά τα στατιστικά στοιχεία συγκρίνονται στη συνέχεια με προσαρμοσμένες τιμές κατωφλίου για ανίχνευση επίθεσης. Στο [61] προτείνεται μια προσέγγιση ανίχνευσης επιθέσεων εμπλοκής μέσω υπολογισμού επιτυχούς αναλογίας πακέτων. Οι προτεινόμενοι αλγόριθμοι λειτουργούν διενεργώντας ελέγχους συνέπειας στην ισχύ σήματος και στις θέσεις των κόμβων. Ένας άλλος μηχανισμός κατά του μπλοκαρίσματος που χρησιμοποιεί κρυπτογραφικές λειτουργίες και κώδικες διόρθωσης σφαλμάτων προτείνεται στο [62]. Η προσέγγιση λειτουργεί με την κωδικοποίηση των πακέτων διαμέσου διαίρεσης σε μπλοκ και την παρεμβολή των κωδικοποιημένων δυαδικών πακέτων. Ομοίως, προτείνονται επίσης οι στρατηγικές που ενσωματώνουν κανάλια surfing και spatial retreats για να αντιμετωπίσουν τις επιθέσεις εμπλοκής (jamming attack) [63]. Η πλοήγηση καναλιών επιτρέπει στις νόμιμες συσκευές επικοινωνίας να αλλάζουν συχνότητες καναλιών, ενώ οι spatial retreats προκαλούν τις συσκευές αυτές να αλλάζουν τη θέση τους ενώ μετακινούνται σε μια επιθυμητή θέση σε κάποια συγκεκριμένη απόσταση. Μια ασφαλής επικοινωνία φυσικού στρώματος, προτείνεται στο [64]. Ο ελάχιστος ρυθμός δεδομένων ρυθμίζεται μεταξύ των κόμβων αποστολής και λήψης για να εξασφαλιστεί η απουσία υποκλοπών. Άλλες προσεγγίσεις εισαγωγής τεχνητού θορύβου [65], [66] σε σήματα χρησιμοποιούνται επίσης για την εξασφάλιση της επικοινωνίας.

Ένας κακόβουλος κόμβος Sybil μπορεί να χρησιμοποιήσει fakeMACvalues για μεταμφιέσεις ως διαφορετική συσκευή. Μπορεί να οδηγήσει σε εξάντληση πόρων καθώς και άρνηση πρόσβασης σε νόμιμες συσκευές στο δίκτυο. Μια προσέγγιση ανίχνευσης επιθέσεων Sybil με τη χρήση μετρήσεων ισχύος σήματος δίνεται στο [67]. Η προσέγγισή τους λειτουργεί με την ανάπτυξη κόμβων ανιχνευτών για τον υπολογισμό της θέσης του αποστολέα κατά την επικοινωνία μηνυμάτων. Μια άλλη επικοινωνία μηνύματος με την ίδια τοποθεσία αποστολέα αλλά διαφορετική ταυτότητα αποστολέα υπονοείται ως επίθεση Sybil. Οι υποθέσεις της προτεινόμενης προσέγγισης την καθιστούν εφαρμόσιμη στα στατικά δίκτυα. Άλλες προσεγγίσεις όπως τα [68], [69]

χρησιμοποιούν μετρήσεις ισχύος σήματος για διευθύνσεις MAC για ανίχνευση επιθέσεων παραποίησης / απομίμησης. Μια άλλη προσέγγιση από τους στο [70] ενσωματώνει εκτίμηση καναλιών για την ανίχνευση επιθέσεων της Sybil. Η προσέγγιση χρησιμοποιεί αριθμό ταυτοτήτων και άλλες παραμέτρους που σχετίζονται με την εκτίμηση του καναλιού για την ανίχνευση των κόμβων Sybil. Ομοίως, η προσέγγιση στο [71] χρησιμοποιεί την απάντηση του καναλιού για να διαφοροποιήσει τους νόμιμους χρήστες και τους επιτιθέμενους. Οι συσκευές που έχουν ακατάλληλη φυσική ασφάλεια χαρακτηρίζονται από την ύπαρξη εξωτερικών διεπαφών που παρέχουν πρόσβαση σε υλικολογισμικό ή λογισμικό και παρέχουν ευάλωτα εργαλεία χρησιμότητας όπως αυτά για δοκιμή και σφαλμάτωση. Το Open Project Security Project (OWASP) παρέχει συστάσεις για τη βελτίωση της φυσικής ασφάλειας των συσκευών στο Διαδίκτυο [72]. Πρέπει να αποφεύγονται οι περιττές διεπαφές υλικού, όπως τα USB που παρέχουν πρόσβαση στο υλικολογισμικό / το λογισμικό της συσκευής. Τα εργαλεία δοκιμής και εντοπισμού σφαλμάτων πρέπει να απενεργοποιηθούν και να ενσωματωθούν μηχανισμοί που βασίζονται σε υλικό, όπως είναι οι μονάδες Trusted Platform Modules (TPM), προκειμένου να βελτιωθεί η φυσική ασφάλεια. Ένα πλαίσιο για την άμβλυνση επιθέσεων στέρησης ύπνου σε ασύρματα δίκτυα αισθητήρων περιγράφεται στο [73]. Το προτεινόμενο πλαίσιο ενσωματώνει προσέγγιση με βάση το σύμπλεγμα, όπου κάθε σύμπλεγμα χωρίζεται σε διάφορους τομείς. Η κατανάλωση ενέργειας μειώνεται αποφεύγοντας την επικοινωνία μεγάλων αποστάσεων. Το πλαίσιο εκτελεί ανίχνευση εισβολής με μοντέλο 5 επιπέδων του ασύρματου δικτύου αισθητήρων. Ένας συντονιστής συμπλέγματος περιλαμβάνει ένα εκτεταμένο σύστημα ανίχνευσης εισβολής μαζί με τους κόμβους ηγέτη και τους κόμβους νεροχύτη στα ανώτερα στρώματα του μοντέλου WSN. Ομοίως, οι κόμβοι των ακόλουθων που υπάρχουν στα χαμηλότερα στρώματα του μοντέλου WSN είναι εξοπλισμένα με απλά συστήματα ανίχνευσης εισβολής. Οι πίνακες 20, 21 και 22 παρουσιάζουν συγκεντρωτικά τις λύσεις σε θέματα ασφάλειας και των τριών επιπέδων.

Αριθμός	Θέμα Ασφάλειας Χαμηλού επιπέδου	Επιπτώσεις	Προτεινόμενες Λύσεις
1	Εμπλοκή των αντιπάλων/Jamming adversaries	Διάσπαση/Disruption και Denial-of-service	Μέτρηση ισχύος σήματος, computing packet delivery ratio, διόρθωση πακέτων με λάθος κώδικα και αλλαγή συχνοτήτων και τοποθεσίας
2	Χαμηλού επιπέδου Sybil και επιθέσεις ψευδαισθήσεων/Low-level Sybil and spoofing attacks	Διάσπαση/Disruption και Denial-of-service	Μετρήσεις ισχύος σήματος και εκτίμηση καναλιού
3	Ανασφαλής προετοιμασία/Insecure initialization	Παραβίαση ιδιωτικότητας και Denial-of-service	Επανάθεση τιμών αποστολής δεδομένων και εισαγωγή τεχνητού θορύβου
4	Ανασφαλής φυσική διεπαφή/Insecure physical interface	Παραβίαση ιδιωτικότητας και Denial-of-service	Αποφυγή πρόσβασης λογισμικού σε USB και αποφυγή εργαλείων testing και debugging
5	Επίθεση στέρησης ύπνου/Sleep deprivation attack	Κατανάλωση ενέργειας	Πολυεπίπεδο σύστημα εντοπισμού εισβολέων

Πίνακας 20. Λύσεις σε θέματα ασφάλειας χαμηλού επιπέδου

Αριθμός	Θέμα Ασφάλειας Μεσαίου επιπέδου	Επιπτώσεις	Προτεινόμενες Λύσεις
1	Επανεμφάνιση ή επαναλήψεις λόγω κατακερματισμού/Replay or duplication attacks due to fragmentation	Διάσπαση/Disruption και Denial-of-service	Introduction of timestamp and nonce options for protecting against replay attacks, and fragment verification through hash chains
2	Ανακάλυψη ανασφαλών γειτόνων/Insecure neighbor discovery	IP Spoofing	Authentication using Elliptic Curve Cryptography (ECC) based signatures
3	Επιθέσεις κρατήσεων με ρυθμιστικό/Buffer reservation attack	Μπλοκάρισμα μνήμης επαναφοράς (resembly buffer)	Split buffer approach requiring complete transmission of fragments
4	RPL επίθεση δρομολόγησης/RPL routing attack	Υποκλοπή, επιθέσεις με στόχο συγκεκριμένο άτομο	Hashing and Signature based authentication, and monitoring node behavior
5	Οι επιθέσεις σιντριβανιών και σκουληκότρυπας/Sinkhole and wormhole attacks	Denial of Service	Rank verification through hash chain function, trust level management, nodes/communication behavior analysis, anomaly detection through IDS, cryptographic key management, graph traversals, and measuring signal strength
6	Οι επιθέσεις Sybil σε ενδιάμεσα στρώματα /Sybil attacks on intermediate layers	Παραβίαση ιδιωτικότητας, spamming, Byzantine fault, αναξιόπιστο broadcast	Random walk on social graphs, analyzing user behavior, and maintaining lists of trusted/un-trusted users
7	Έλεγχος ταυτότητας και ασφαλής επικοινωνία/Authentication and secure communication	Παραβίαση ιδιωτικότητας	Compressed AH and ESP, Header compression and software based AES, TPM using RSA, SHA1/AES, hybrid authentication, authentication with fuzzy extractor, encryption of payload dispatch type values with compressed AH, IACAC using the Elliptic Curve Cryptography, distributed logs, and symmetric homomorphic mapping

Πίνακας 21. Λύσεις σε θέματα ασφάλειας μεσαίου επιπέδου

Αριθμός	Θέμα Ασφάλειας Υψηλού επιπέδου	Επιπτώσεις	Προτεινόμενες Λύσεις
1	Ασφάλεια CoAP με διαδίκτυο /CoAP – Constrained Application Protocol security with internet	Συμφόρηση δικτύου	TLS/DTLS and HTTP/CoAP mapping, Mirror Proxy (MP) and Resource Directory, TLS-DTLS tunnel and message filtration using 6LBR
2	Ασφαλείς διεπαφές/Insecure interfaces	Διάσπαση/Disruption δικτύου, Denial-of-service και παράβαση ιδιωτικότητας	Disallowing weak passwords, testing the interface against the vulnerabilities of software tools (SQLi and XSS), and using https along with firewalls
3	Ασφαλές λογισμικό-υλικολογισμικό/Insecure software/firmware	Διάσπαση/Disruption δικτύου, Denial-of-service και παράβαση ιδιωτικότητας	Regular secure updates of software/firmware, use of file signatures, and encryption with validation
4	Ασφάλεια Middleware/Middleware security	Διάσπαση/Disruption δικτύου, Denial-of-service και παράβαση ιδιωτικότητας	Secure communication using authentication, security policies, key management between devices, gateways & M2M components, service layer M2M security, transparent middleware using authentication/encryption mechanisms

Πίνακας 22. Λύσεις σε θέματα ασφάλειας Υψηλού επιπέδου

5.2. Λύσεις ασφάλειας και διασφάλισης ιδιωτικότητας μεσαίου επιπέδου.

Οι απειλές που προκύπτουν από επιθέσεις επανάληψης λόγω κατακερματισμού των πακέτων στο 6LoWPAN αντιμετωπίζονται με την προσθήκη επιλογών χρονικής σήμανσης (timestamp) και nonce στα αποσπασματικά πακέτα [74]. Αυτά τα πακέτα προστίθενται στο στρώμα προσαρμογής 6LoWPAN που αντιστοιχεί στα κατακερματισμένα πακέτα. Η επιλογή timestamp και η επιλογή nonce λειτουργούν για τα μονοκατευθυντικά και αμφίδρομα πακέτα, αντίστοιχα. Η τιμή της χρονικής σήμανσης 64-bit στο fragment εξασφαλίζει την εξάλειψη των περιττών διαφημίσεων και ανακατευθύνσεων στο δίκτυο. Η επιλογή nonce εξασφαλίζει ότι η διαφήμιση γίνεται μόνο για να ανταποκριθεί σε μια νέα προσέλευση. Ομοίως, μια στρατηγική αλυσίδας περιεχομένου που εξασφαλίζει τη μετάδοση των θραυσμάτων πακέτων IPv6 εντός σειράς στο 6LoWPAN προτείνεται στο [75]. Τα περιεχόμενα του θραύσματος (fragment) προστίθενται στην δημιουργία αλυσίδας κατακερματισμού προκειμένου να επαληθευτούν τα θραύσματα. Ένα πλαίσιο ασφαλείας με ενότητες για ασφαλή ανακάλυψη γείτονα, έλεγχο ταυτότητας, δημιουργία κλειδιών και κρυπτογράφηση δεδομένων προτείνεται στο [76]. Για την ασφαλή ανακάλυψη του γείτονα χρησιμοποιείται η κρυπτογραφία ελλειπτικής καμπύλης (ECC) [77]. Οι υπογραφές δημόσιου κλειδιού ECC χρησιμοποιούνται για τον εντοπισμό κόμβων στη φάση ανακάλυψης του γείτονα. Τόσο τα συμμετρικά όσο και τα ασύμμετρα συστήματα διαχείρισης κλειδιών προτείνεται να αναπτυχθούν ανάλογα με τις απαιτήσεις εφαρμογής. Στη συνέχεια, τα κρυπτογραφημένα δεδομένα ανακοινώνονται για να διασφαλιστεί η ασφάλεια κόμβου-κόμβου. Μέσω μιας επίθεσης κρατήματος buffer, η μνήμη επανασύνδεσης ενός κόμβου μπορεί να αποκλειστεί. Αυτή η επίθεση μετριάζεται μέσω προσέγγισης διαχωρισμένου buffer [78], η οποία αυξάνει το κόστος εκτόξευσης, απαιτώντας την πλήρη μετάδοση αποσπασματικών πακέτων σε σύντομες εκρήξεις. Κάθε κόμβος είναι υποχρεωμένος να υπολογίζει το ποσοστό ολοκλήρωσης

ενός πακέτου και να καταγράφει τη συμπεριφορά της αποστολής θραυσμάτων. Με την υπερφόρτωση, ο κόμβος μπορεί να απορρίψει τα πακέτα με χαμηλό ποσοστό ή να έχει μεγάλη διακύμανση στο μοτίβο αποστολής θραυσμάτων. Για τον μετριασμό των επιθέσεων εναντίον των αντιπάλων κατά τη δρομολόγηση μέσω του πρωτοκόλλου δρομολόγησης IPv6 για δίκτυα χαμηλής κατανάλωσης και απώλειας (RPL), μια υπηρεσία ασφαλείας για τον έλεγχο ταυτότητας των αριθμών βαθμών και εκδόσεων προτείνεται στο [79]. Το πρωτόκολλο RPL λειτουργεί με την κατασκευή του Κατευθυνόμενου Ακυκλικού Γράφου (DAG) με ρίζα σε οποιαδήποτε από τις πύλες. Ο αριθμός έκδοσης ενημερώνεται όταν κατασκευάζεται μια νέα έκδοση του DAG προορισμού. Το RPL χρησιμοποιεί σειρές για την αναπαράσταση της ποιότητας της διαδρομής στον τελικό κόμβο νεροχύτη (sink node). Η τιμή κατάταξης ενός κόμβου μπορεί να μειωθεί για να συνδεθεί με τη ρίζα για υποκλοπές. Ο προτεινόμενος μηχανισμός ασφαλείας που ονομάζεται Αριθμός έκδοσης και έλεγχος ταυτότητας κατάταξης (VeRA) χρησιμοποιεί τη λειτουργία κατακερματισμού (SHA [80]), τη λειτουργία MAC (HMAC [81] και την ψηφιακή υπογραφή (RSA [82] κλπ. , με την RPL, η αξία κατάταξης που υπολογίζεται με βάση την τάξη του προτιμώμενου γονέα μεταδίδεται σε άλλους κόμβους. Το πρότυπο RPL απαιτεί τον γονικό κόμβο να έχει χαμηλότερη βαθμίδα από τα παιδιά. Η επίθεση που προτείνεται από τους Le et al. ο κακόβουλος κόμβος για να επιλέξει τον χειρότερο γονέα αντί για τον καλύτερο γονέα. Ο συμβιβασμένος κόμβος δεν προωθεί τα μηνύματα DAO, προσθέτοντας έτσι την καθυστέρηση της κυκλοφορίας κατά τη μετάδοση μέσω κακόβουλων κόμβων. Η επίθεση γίνεται πιο σοβαρή ανάλογα με το φορτίο προώθησης της περιοχής δικτύου. για να μετριαστεί η επίθεση, προτείνεται να παρακολουθείται η συμπεριφορά των κόμβων για διάφορες παραμέτρους, συμπεριλαμβανομένων των μηνυμάτων που παραδόθηκαν και της καθυστέρησης από άκρο σε άκρο κ.λπ.

Για να αντιμετωπισθούν οι επιδρομές των βυθισμάτων στα δίκτυα απώλειας χαμηλής κατανάλωσης, προτείνεται από τον Weekly et al. Μηχανισμός που ενσωματώνει τεχνικές αποτυχίας και αυθεντικοποίησης. [83]. Για την επαλήθευση της κατάταξης που αντιστοιχεί σε ένα μήνυμα αντικειμένου πληροφοριών προορισμού (DIO), χρησιμοποιείται μια συνάρτηση κατακερματισμού μονής κατεύθυνσης μαζί με μια λειτουργία αλυσίδας κατακερματισμού. Μια τιμή hash που παράγεται για έναν τυχαίο αριθμό που επιλέγεται από τον κόμβο ρίζας μεταδίδεται μέσω του μηνύματος DIO. Οι έγκυροι κόμβοι στο δίκτυο εκτελούν περαιτέρω κατακερματισμό πριν από την προώθηση των μηνυμάτων, ενώ οι συμβιβασμένοι κόμβοι ανακοινώνουν τις ληφθείσες τιμές κατακερματισμού. Μετά τη σύγκλιση του δένδρου δρομολόγησης, η ρίζα εκτελεί μια μετάδοση της αρχικά επιλεγμένης τυχαίας τιμής για επαλήθευση από μεμονωμένους κόμβους. Μια αναντιστοιχία σε έναν κόμβο συνεπάγεται μια μη αυθεντική αξία μητρικής κατάταξης. Ομοίως, η τεχνική γονικής ανακατεύθυνσης ενισχύει το μήνυμα DIO με ένα ειδικό πεδίο που υπογράφεται από τον κόμβο ρίζας. Το ειδικό πεδίο αντιπροσωπεύει τους μη ριζικούς κόμβους που δεν μπορούν να μεταδώσουν το 30% των δεδομένων αισθητήρα σε συγκεκριμένα χρονικά διαστήματα. Οι γονείς τέτοιων κόμβων είναι συνεπώς μαύροι για μεταγενέστερη επικοινωνία. Μια άλλη προσέγγιση στο [84] εντοπίζει ύποπτους κόμβους αναλύοντας τη συμπεριφορά των γειτονικών κόμβων. Στη συνέχεια απαιτεί τον ύποπτο κόμβο να επαληθεύεται ως μαύρη τρύπα. Μια άλλη στρατηγική για την αντιμετώπιση των επιθέσεων από τις βυθιζόμενες επιφάνειες χρησιμοποιώντας διαφορετικά επίπεδα εμπιστοσύνης δίνεται στο [85] . Η προσέγγισή τους χρησιμοποιεί διαφορετικά χαρακτηριστικά του πρωτοκόλλου Dynamic Source Routing (DSR) για την ανίχνευση και την αποφυγή των επιθέσεων σκουληκότρυπας και σκουληκότρυπας σε ασύρματα δίκτυα. Η προσέγγιση βασίζεται στα επίπεδα ακρίβειας και ειλικρίνειας που υπολογίζονται με επαλήθευση

των διαβιβαζόμενων πακέτων μέσω ορισμένων ελέγχων ακεραιότητας. Ομοίως, ένα πρωτόκολλο δρομολόγησης ad hoc που ενσωματώνει τους συμμετρικούς αλγόριθμους που βασίζονται στην κρυπτογράφηση είναι σχεδιασμένο για τη διασφάλιση των κόμβων από τους συμβιβασμένους ασύρματους κόμβους σε ένα δίκτυο. Μια άλλη προσέγγιση για την ανίχνευση επιθέσεων σκουληκότρυπας σε ασύρματα δίκτυα αισθητήρων λειτουργεί με τη μετάδοση αποστάσεων που υπολογίζονται μεταξύ γειτόνων [86]. Οι παραμορφώσεις του δικτύου αναλύονται στη συνέχεια για να ανιχνεύσουν τις σκουληκότρυπες. Το [87] στοχεύει στην ανίχνευση επιθέσεων χελώνας ή σκουληκότρυπας για ένα ιεραρχικό ασύρματο δίκτυο αισθητήρων. Το σύνολο του δικτύου διανέμεται σε πολλά σύνολα με κάθε σύμπλεγμα που περιέχει έναν κόμβο αισθητήρα υψηλής ισχύος που λειτουργεί για την ανίχνευση κατακλυσμών για το σύμπλεγμα του. Διάφορες προσεγγίσεις που χρησιμοποιούν μηχανισμό ανίχνευσης εισβολών για την ανίχνευση και την αποφυγή προσβολών από τις βυθίσεις [88], [89], [90]. Οι προτεινόμενες στρατηγικές ενσωματώνουν ανάλυση πακέτων δικτύου και ανίχνευση ανωμαλιών χρησιμοποιώντας προκαθορισμένους κανόνες. Άλλες προσεγγίσεις της ανίχνευσης σκουληκότρυπας χρησιμοποιούν τα διαγράμματα δικτύου [91], [92], αναλύοντας μηνύματα ισχύος σήματος [93] ή συστήματα διαχείρισης κλειδιών [94], [95]. Οι επιθέσεις της Sybil στη στρώση δικτύου χρησιμοποιούν ψευδο-ταυτότητες για να μιμηθούν πολλαπλές μοναδικές ταυτότητες που ονομάζονται Sybil κόμβοι [96]. Αυτές οι επιθέσεις αποτελούν σοβαρή απειλή για τα κατανεμημένα καθώς και τα συστήματα peer to peer (p2p), συμπεριλαμβανομένου του Διαδικτύου. Αυτές οι επιθέσεις μπορεί επίσης να επηρεάσουν την άμυνα κατά των βλαβών του Βυζαντίου προκαλώντας έτσι εμπόδιο στην αξιόπιστη μετάδοση στο δίκτυο. Για τα κοινωνικά δίκτυα, ενσωματώνεται μια σχέση εμπιστοσύνης για να περιοριστεί η δημιουργία ταυτότητας Sybil. Τα αντίμετρα που χρησιμοποιούν τα κοινωνικά γραφήματα επιτρέπουν στους νόμιμους κόμβους να ανιχνεύουν κόμβους Sybil περνώντας το γράφημα μέσω τυχαίων περιπάτων ή χρησιμοποιώντας τους κοινοτικούς αλγόριθμους ανίχνευσης [97], [98], [99], [100]. Ομοίως, αναλύεται η συμπεριφορά των χρηστών όσον αφορά τις δραστηριότητες στο δίκτυο και, στη συνέχεια, οι χρήστες με καθορισμένο πρότυπο δραστηριοτήτων θεωρούνται χρήστες του Sybil [101], [102]. Για τα δίκτυα κινητής τηλεφωνίας, οι κατάλογοι αξιόπιστων και μη αξιόπιστων χρηστών μπορούν να διατηρηθούν για την ανίχνευση κόμβων Sybil [103]. Για τη διασφάλιση του στρώματος δικτύου των δικτύων που βασίζονται στο IPv6 χρησιμοποιώντας το επίπεδο προσαρμογής 6LoWPAN, οι συμπιεσμένες μορφές κεφαλίδας ελέγχου ταυτότητας (AH) [104] και Encapsulating Security Payload (ESP) [105] προτείνεται στο [106]. Τα 8 bits της επικεφαλίδας διευθύνσεων IPv6 σύμφωνα με την προδιαγραφή επιπέδου προσαρμογής 6LowPAN χρησιμοποιούνται για τον καθορισμό των τύπων αποστολής κεφαλίδων και διευθύνσεων. Οι συμπιεσμένες κεφαλίδες χρησιμοποιούνται στην επικοινωνία σε δύο τρόπους: τρόπος μεταφοράς και λειτουργία σήραγγας, ανάλογα με την κρυπτογράφηση ωφέλιμου φορτίου. Η αξιολόγηση των διαφορετικών τεχνικών κρυπτογράφησης που εφαρμόζονται για τη νέα προτεινόμενη μορφή ασφαλείας δείχνει τον αλγόριθμο SHA1 [107] να έχει λιγότερες απαιτήσεις χρόνου και ενέργειας. Ομοίως, μια συμπιεσμένη μορφή του IPsec περιγράφεται στα [108], [109], [110] για την παροχή ασφάλειας από άκρο σε άκρο. Οι συγγραφείς χρησιμοποιούν την κεφαλίδα ελέγχου ταυτότητας (AH) και το Encapsulating Security Payload (ESP) για την παροχή ασφάλειας χρησιμοποιώντας το IPsec. Οι κωδικοποιήσεις των κεφαλίδων AH και ESP εκτελούνται χρησιμοποιώντας κωδικοποίηση NHC η οποία ορίζεται στον μηχανισμό συμπίεσης HC13 [111]. Για τον έλεγχο ταυτότητας και την κρυπτογράφηση, εφαρμόζονται διαφορετικές παραλλαγές των SHA1 και AES. Οι κωδικοποιήσεις των δυαδικών ψηφίων οδηγούν σε μειωμένο

μέγεθος πακέτων, ωστόσο, η προτεινόμενη προσέγγιση προκαλεί γενικά έξοδα όσον αφορά την κατανάλωση ενέργειας και το μέσο χρόνο απόκρισης.

Ένας άλλος μηχανισμός για τη διασφάλιση του στρώματος δικτύου του 6LoWPAN υποστηρίζοντας νέες τιμές τύπου αποστολής προτείνεται στο [112]. Οι συγγραφείς προτείνουν τη χρήση αποκλειστικών τιμών του byte ωφέλιμου φορτίου όπως αναφέρεται στο RFC 4944 [113]. Τα πρώτα 3 bits των τιμών τύπου αποστολής περιγράφουν την κεφαλίδα ασφαλείας και τη λειτουργία χρήσης, ενώ τα υπόλοιπα 3 bits περιγράφουν τους τύπους επικεφαλίδων διευθύνσεων 6LoWPAN. Για να εξαχθούν πληροφορίες από ένα πακέτο σχετικά με τους κρυπτογραφικούς αλγορίθμους και τα κλειδιά που πρέπει να εφαρμοστούν για την επεξεργασία του πακέτου, χρησιμοποιείται ένας δείκτης παραμέτρων ασφαλείας 2-byte (SPI). Σε αντίθεση με αυτή την προσέγγιση, στο [114] προτείνεται ένα πρωτόκολλο για την εξασφάλιση του Διαδικτύου ενάντια στις επιθέσεις άρνησης εξυπηρέτησης (DoS), man-in-the-middle και επαναλήψεων. Οι επιθέσεις DoS ενδέχεται να προκύψουν σε περιορισμένες συσκευές, καθώς οι εισβολείς ενδέχεται να στείλουν μηνύματα για τη χρήση των πόρων. Παρομοίως, τα μυστικά κλειδιά που αποκαλύπτονται λόγω υποκλοπής μπορεί να οδηγήσουν σε κλοπή ταυτότητας εξαιτίας των επιθέσεων κυρίως στο μέσο σε ένα δικτυωμένο περιβάλλον. Επιπλέον, οι πληροφορίες ταυτότητας ή τα διαπιστευτήρια μπορούν να επαναληφθούν από τους εισβολείς για να επηρεάσουν την κυκλοφορία του δικτύου. Η προτεινόμενη προσέγγιση που ονομάζεται έλεγχος πρόσβασης βάσει ελέγχου ταυτότητας ταυτότητας και ικανότητας (IACAC) δημιουργεί μυστικά κλειδιά χρησιμοποιώντας τον αλγόριθμο Diffie Hellman βασισμένο στην κρυπτογράφηση ελλειπτικής καμπύλης. Για επικοινωνία και πρόσβαση, οι συσκευές αλληλοεξαρτώνται μέσω κρυπτογράφησης με μυστικά κλειδιά. Ένας έλεγχος πρόσβασης που βασίζεται σε δυνατότητες εφαρμόζεται όταν η δυνατότητα αντιπροσωπεύει μια δομή που περιέχει δικαιώματα πρόσβασης και αναγνωριστικό συσκευής. Με την πρόσβαση βάσει της ικανότητας, επαληθεύεται αρχικά η επικοινωνία που πραγματοποιείται μεταξύ δύο συσκευών. Επιπλέον, ελέγχεται η δυνατότητα της συσκευής να εκτελέσει την επιθυμητή λειτουργικότητα πριν γίνει η πραγματική λειτουργία. Στα [115], [116] περιγράφεται μια προσέγγιση για την ασφάλεια από άκρο σε άκρο χρησιμοποιώντας αμφίδρομη πιστοποίηση μέσω κρυπτογραφίας δημόσιου κλειδιού. Έχει αναπτυχθεί ένας αξιόπιστος διακομιστής ελέγχου πρόσβασης για την αποθήκευση δικαιωμάτων πρόσβασης εκδοτών στο δίκτυο. Το πιστοποιητικό του εκδότη και της Αρχής Πιστοποίησης (CA) πρέπει να υπάρχει στον ιστότοπο του εκδότη. Ο έλεγχος ταυτότητας μπορεί να πραγματοποιηθεί μέσω των τσιπ Trusted Platform Module (TPM) [117] χρησιμοποιώντας RSA ή μέσω των προ-κοινόχρηστων κλειδιών DTLS. Με τα TPM, τα πιστοποιητικά RSA μεταδίδονται σε μορφή X.509. Η επικοινωνία από άκρο σε άκρο πραγματοποιείται μόνο μετά από έλεγχο ταυτότητας των συνδρομητών με το διακομιστή ελέγχου πρόσβασης. Η προτεινόμενη προσέγγιση φαίνεται να λειτουργεί με χαμηλές απαιτήσεις ενέργειας και μνήμης. Ένα άλλο σύστημα επαλήθευσης και έγκρισης βάσει πολλαπλών παραγόντων προτείνεται στο [118]. Το προτεινόμενο σχήμα ενσωματώνει έλεγχο ταυτότητας κωδικού πρόσβασης κατά τη χρήση έξυπνων καρτών. Στη συνέχεια χρησιμοποιείται ένας ασαφής εκχυλιστής για την εξαγωγή μυστικών τυχαίων συμβολοσειρών από βιομετρικά στοιχεία. Το πρωτόκολλο ελέγχου ταυτότητας υποστηρίζει τέσσερις σημαντικές λειτουργίες που σχετίζονται με τη δημιουργία παραμέτρων ασφαλείας, την αποθήκευση πληροφοριών εγγραφής σε μια βάση δεδομένων, τον έλεγχο ταυτότητας και την τροποποίηση των διαπιστευτηρίων πιστοποίησης. Οι συγγραφείς προτείνουν έναν αυτόνομο μηχανισμό επαλήθευσης ταυτότητας, όπου η συνδεσιμότητα με τον διακομιστή ελέγχου ταυτότητας δεν είναι

λειτουργική. Ένα κατανεμημένο πλαίσιο για ασφαλή επικοινωνία μεταξύ δικτύων διαδικτύου προτείνεται στο [\[119\]](#). Για να προστατευτεί ένα δίκτυο από ένα κακόβουλο φορέα υπηρεσιών cloud, το προτεινόμενο πλαίσιο επιτρέπει τη διαμόρφωση του δικτύου από μια κεντρική τοποθεσία. Καταγράφει μηνύματα ελέγχου σε πολλαπλές τοποθεσίες, προκειμένου να επαληθευτεί μέσω διαφορετικών πύλων. Το μέγεθος των μηνυμάτων καταγραφής μειώνεται ελαχιστοποιώντας συνεχώς την παλιά μηνύματα. Η επαλήθευση των μηνυμάτων καταγραφής χρησιμοποιείται στη συνέχεια για να υποδείξει κακόβουλη συμπεριφορά η οποία με τη σειρά της προστατεύει το δίκτυο από την τροποποίηση, την παρακράτηση, την εισαγωγή και την αναδιάταξη των μηνυμάτων. Με στόχο τη διατήρηση της ιδιωτικής ζωής για την ταυτότητα και την τοποθεσία σε στο δίκτυο, ένας μηχανισμός ελέγχου ταυτότητας με ασφαλή προώθηση πακέτων δίνεται στο [\[120\]](#). Ο προτεινόμενος αλγόριθμος χρησιμοποιεί συμμετρική ομοιομορφική χαρτογράφηση για δίκτυα ανοχής με καθυστέρηση τα οποία δεν έχουν συνεπή διασύνδεση από άκρο σε άκρο, απαιτώντας έτσι από τους ενδιαμέσους κόμβους να συνεργάζονται κατά τη διάρκεια της μετάδοσης μηνυμάτων. Παρομοίως, στο πρόγραμμα SMARTIE [\[121\]](#) προτείνεται μια πλατφόρμα για την εξασφάλιση δεδομένων που μοιράζονται συσκευές του δικτύου. Η πλατφόρμα δεδομένων που προτείνεται από το πρόγραμμα SMARTIE ορίζει ένα σχήμα ελέγχου ταυτότητας για την πρόσβαση στην υπηρεσία μαζί με διάφορες βιβλιοθήκες για τη διαχείριση κρυπτογραφικών κλειδιών. Για την παροχή ενός ασφαλούς καναλιού επικοινωνίας

μεταξύ των συσκευών και του νέφους, το έργο καθορίζει το ασφαλές πρωτόκολλο CoAP ελαφρού βάρους χρησιμοποιώντας κρυπτογράφηση ελλειπτικής καμπύλης. Παρομοίως, για τη διατήρηση της ιδιωτικής ζωής κατά την κοινή χρήση δεδομένων και την ασφαλή παρακολούθηση αντικειμένων του δικτύου, περιλαμβάνει υπηρεσίες μεσαίου και τοποθεσίας.

Για την παροχή ασφάλειας από άκρο σε άκρο, η χρήση του TLS-PSK προτείνεται στο [\[122\]](#) ενώ καθίσταται δυνατή η επικοινωνία μεταξύ HTTP και CoAP. Αυτό απαιτεί μετάφραση μηνυμάτων από το στρώμα DTLS και από άλλα πρωτόκολλα υψηλού επιπέδου. Παρομοίως, για την εξασφάλιση μηνυμάτων multicast, προτείνεται μια επέκταση του DTLS που ενσωματώνει PSK και nonces για να υποστηρίξει τη διαπραγμάτευση των κλειδιών συνόδου. Για την ασφάλεια επιπέδου μεταφοράς προτείνεται επίσης ένας εξουσιοδοτημένος μηχανισμός επαλήθευσης ταυτότητας με χρήση του δρομολογητή συνόρων 6LoWPAN (6LBR) ο οποίος αναχαιτίζει τα πακέτα, εκτελεί υπολογισμό για τον έλεγχο ταυτότητας δημόσιου κλειδιού και προωθεί τα πακέτα [\[123\]](#). Ένας διακομιστής ελέγχου πρόσβασης έχει ενσωματωθεί για να υποστηρίξει τον έλεγχο ταυτότητας μεταξύ 6LBR και των συσκευών ανίχνευσης. Η κρυπτογραφία ελλειπτικής καμπύλης (ECC) χρησιμοποιείται για την υλοποίηση της ασφάλειας επιπέδου μεταφοράς. Η επικοινωνία από άκρο σε άκρο είναι ασφαλισμένη με κλειδιά διαπραγματεύσεων 6LBR και επικοινωνεί για άλλα βήματα ελέγχου ταυτότητας μεταξύ των δύο άκρων. Ο υπολογισμός που μεταβιβάστηκε σε 6LBR έχει ως αποτέλεσμα καλύτερη απόδοση για ασφαλή επικοινωνία παρά τους μεγάλους υπολογισμούς που απαιτούνται από το ECC. Ένα άλλο πλαίσιο που ονομάζεται BlinkToSCoAP για την παροχή ασφάλειας από άκρο σε άκρο προτείνεται στο [\[124\]](#). Το προτεινόμενο πλαίσιο ενσωματώνει ελαφρές εφαρμογές του CoAP, του DTLS και του 6LoWPAN για την εξασφάλιση του δικτύου. Ο κρυπτογράφος DTLS βασίζεται στους αλγόριθμους SHE 128-bit AES και 26-bit SHA. Όσον αφορά τις συσκευές περιορισμένης πρόσβασης, το προτεινόμενο πλαίσιο λειτουργεί με ελάχιστες απαιτήσεις όσον αφορά το μέγεθος της μνήμης RAM, το μέγεθος μνήμης flash και την κατανάλωση ενέργειας. Μία στρατηγική που ενσωματώνει τη συμπίεση κεφαλίδας για το πρωτόκολλο 6LoWPAN για τη μείωση των γενικών εξόδων DTLS δίνεται στο

[125]. Η προτεινόμενη στρατηγική εκτελεί τη συμπίεση κεφαλίδας DTLS και χρησιμοποιεί την εφαρμογή AES που βασίζεται σε λογισμικό. Η στρατηγική συμπίεσης βελτιώνει την κατανάλωση ενέργειας καθώς και τον χρόνο απόκρισης του δικτύου. Το σχέδιο RERUM [126] προτείνει ένα πλαίσιο για τις εφαρμογές Smart City για την προστασία της ιδιωτικής ζωής και της ασφάλειας. Για την ανάπτυξη αξιόπιστων εφαρμογών, προσαρμόζονται οι προσεγγίσεις που βασίζονται στην ακεραιότητα δεδομένων και την εξακρίβωση της ταυτότητας. Νέοι μηχανισμοί ελέγχου πρόσβασης για δυναμικά μεταβαλλόμενα συστήματα, μαζί με το hop-to-hop και τον έλεγχο ταυτότητας από άκρο σε άκρο, χρησιμοποιούνται για τη διασφάλιση της επικοινωνίας προς / από αντικείμενα στο Διαδίκτυο. Σκοπός της είναι επίσης να εξασφαλίσει την προστασία της ιδιωτικής ζωής μέσω συστημάτων υπογραφής και τεχνικών ανίχνευσης θορύβου. Ένα άλλο πλαίσιο πειραματισμού με πρωτόκολλα ασφάλειας σε μια υποδομή βασίζεται στο έργο ARMOR [127]. Το πρόγραμμα στοχεύει στην αξιοποίηση της εμπιστοσύνης και της ασφάλειας για σενάρια που βασίζονται σε ένα δίκτυο όπως το Smart City και η Healthcare. Ο πειραματισμός ARMOR ορίζει την αρχιτεκτονική ασφαλείας, δημιουργεί δοκιμαστικές μονάδες, εκτελεί πειράματα και δημιουργεί ετικέτες πιστοποίησης. Τα πειράματα μπορούν να χρησιμοποιηθούν για την εξασφάλιση αξιόπιστης διασύνδεσης από άκρο σε άκρο καθώς και για ειδικές απαιτήσεις ασφαλείας. Παρομοίως, το πρόγραμμα BUTLER [128] παρέχει υποστήριξη σε πληροφοριακά συστήματα, συμπεριλαμβανομένων έξυπνων κατοικιών, έξυπνων αγορών, έξυπνης υγειονομικής περίθαλψης και έξυπνων πόλεων. Οι υπηρεσίες που υλοποιούνται στο έργο επιτρέπουν την αξιόπιστη επικοινωνία αντικειμένων μεταξύ του δικτύου χρησιμοποιώντας πληροφορίες περιβάλλοντος. Το έργο περιελάμβανε ελαφριά κρυπτογραφικά πρωτόκολλα με στόχο τη βελτίωση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων. Διαφορετικές τεχνικές συμπίεσης κεφαλίδων έχουν προταθεί για την παροχή ασφάλειας από άκρο σε άκρο μεταφοράς. Στο [129] περιγράφουν μια προσέγγιση για τη συμπίεση των κεφαλίδων DTLS Record και Handshake μαζί με διαφορετικά μηνύματα Handshake έτσι ώστε να ταιριάζουν σε ένα μόνο MTU του 6LoWPAN. Η προτεινόμενη προσέγγιση κωδικοποιεί τα bits κεφαλίδας για συνδυασμένη κωδικοποίηση του byte εγγραφής και χειραψίας [130], καθώς και για ατομική κωδικοποίηση της κεφαλίδας εγγραφής μετά την ολοκλήρωση του Handshake. Ομοίως, μια ενισχυμένη έκδοση του DTLS που ενσωματώνει τη συμπίεση κεφαλίδας για την εξασφάλιση του δικτύου παρουσιάζεται στο [131]. Για τη συμπίεση επόμενης κεφαλίδας (NHC) με βάση το UDP χρησιμοποιούνται ειδικά 05 μπιτ στην κεφαλίδα DTLS για την αναγνώριση συμπίεσμένων κεφαλίδων, ενώ τα υπόλοιπα 03 bits χρησιμοποιούνται για την απεικόνιση του αθροίσματος ελέγχου και των θυρών. Ομοίως, για τις εγγραφές και τις κεφαλίδες χειραψίας με μέγεθος 13 bytes και 12 bytes, η προτεινόμενη στρατηγική συμπιέζει τις κεφαλίδες στο μέγεθος των 05 bytes και 03 bytes, αντίστοιχα. Για το CoAP, η βελτίωση του DTLS που περιλαμβάνει τη συμπίεση κεφαλών μειώνει το γενικό κόστος DTLS, βελτιώνοντας έτσι την κατανάλωση ενέργειας και τον χρόνο απόκρισης. Μια ελαφριά εφαρμογή του Internet Key Exchange (IKE) με στόχο τη βελτίωση της διαχείρισης κλειδιού για το 6LoWPAN προτείνεται στο [132]. Το πρωτόκολλο IKE χρησιμοποιείται από την IPSec για τη διαχείριση των κλειδιών, ωστόσο θεωρείται ακατάλληλο για συσκευές περιορισμένης πρόσβασης. Οι συγγραφείς προτείνουν μια συμπίεσμένη έκδοση του IKEv2 χρησιμοποιώντας μια συμπίεσμένη μορφή UDP που μπορεί να αναγνωριστεί ως κεφαλίδα IKE. Διαφορετικά πεδία στην κεφαλίδα IKE συμπιέζονται κατά τη χρήση του μηχανισμού κωδικοποίησης NHC. Προτείνεται επίσης η χρήση του πεδίου αναγνωριστικού πρωτοκόλλου στο ωφέλιμο φορτίο του συνδέσμου ασφαλείας του IKEv2 για την ασφάλεια στρώματος σύνδεσης IEEE 802.15.4.

Ένα σχέδιο αμοιβαίας πιστοποίησης για ασφαλή διαχείριση συνεδριών χρησιμοποιώντας μεθόδους κρυπτογράφησης συμμετρικού κλειδιού δίνεται στο [133]. Το προτεινόμενο σχήμα επιλέγει αρχικά έναν τυχαίο αριθμό και εκτελεί κρυπτογράφηση και παράγει ένα κλειδί περιόδου λειτουργίας το οποίο στη συνέχεια χρησιμοποιείται για την κρυπτογράφηση ενός άλλου τυχαίου αριθμού. Στη συνέχεια χρησιμοποιείται η κρυπτογραφημένη τιμή για έλεγχο ταυτότητας. Για κάθε σύνοδο, μπορεί να δημιουργηθεί ένα νέο κλειδί συνόδου χωρίς να απαιτείται επανάληψη παραμέτρων. Παρομοίως, προτείνεται επίσης μια άλλη μέθοδος κρυπτογράφησης με χρήση hashes για συσκευές περιορισμένης πόρων που υποστηρίζουν λειτουργίες κατακερματισμού. Λειτουργεί αποτελεσματικά λόγω μικρών επιβαρύνσεων των υπολογισμών. Ένα άλλο σχέδιο αμοιβαίας αναγνώρισης ταυτότητας για υπολογιστικά περιβάλλοντα ομίχλης που έχουν συσκευές περιορισμένης πηγής προτείνεται στο [134]. Το προτεινόμενο σχήμα που ονομάζεται Octopus απαιτεί να έχει ένα μυστικό κλειδί μακράς διάρκειας που στη συνέχεια χρησιμοποιείται για έλεγχο ταυτότητας με οποιονδήποτε διακομιστή ομίχλης. Μια προσαρμογή της Διατροφής Διατροφής HIP έχει χρησιμοποιηθεί για τη βελτίωση της ασφάλειας του δικτύου στο [135]. Με την ενσωμάτωση μιας αποτελεσματικής τεχνικής επανάληψης περιόδου λειτουργίας, μειώνονται τα γενικά έξοδα των λειτουργιών που βασίζονται σε δημόσιο κλειδί. Η επανάληψη της συνδιάσκεψης έχει ως αποτέλεσμα οι συνομηλίκες να εκτελούν βαριές εργασίες κατά την προετοιμασία της σύστασης της σύσκεψης. Στη συνέχεια αποθηκεύεται η κατάσταση της περιόδου σύνδεσης, η οποία στη συνέχεια βελτιώνει την επανάληψη της περιόδου λειτουργίας με επανεγγραφές. Οι διαπραγματεύσεις που απαιτούνται για την επανάληψη της περιόδου σύνδεσης μπορούν επίσης να ενσωματωθούν σε DTLS και IKEv2.

5.3. Λύσεις ασφάλειας και διασφάλισης ιδιωτικότητας υψηλού επιπέδου.

Για την εξασφάλιση δικτύου με χαμηλή κατανάλωση και απώλειες (LLN) με βάση το CoAP που συνδέεται με το Διαδίκτυο, μια προσέγγιση που ενσωματώνει TLS και DTLS προτείνεται στο [136]. Η προτεινόμενη προσέγγιση λειτουργεί για σενάρια όπου ο 6LoWPAN Border Router (6LBR) συνδέει το LLN με το Διαδίκτυο για να αποκτήσει πρόσβαση σε συσκευές από απόσταση. Οι κόμβοι LLN χρησιμοποιούνται για την παροχή υπηρεσιών σε πελάτες CoAP και HTTP. Σχεδιάζεται η χαρτογράφηση των TLS και DTLS για την παροχή ασφάλειας από άκρο σε άκρο που προστατεύει τα LLN από επιθέσεις με βάση το διαδίκτυο. Ωστόσο, ο υπολογισμός χαρτογράφησης, όταν μεταβιβάζεται στις συσκευές περιορισμένης χρήσης πόρων, ενδέχεται να επιφέρει σημαντική επιβάρυνση. Μια άλλη προσέγγιση για την εξασφάλιση μηνυμάτων για εφαρμογές που επικοινωνούν μέσω διαδικτύου χρησιμοποιώντας διάφορες επιλογές ασφαλείας CoAP προτείνεται στο [137]. Οι νέες επιλογές ασφαλείας που σχετίζονται με το CoAP είναι: SecurityOn, SecurityToken και SecurityEncap. Η επιλογή SecurityOn αφορά την προστασία των μηνυμάτων CoAP σε επίπεδο εφαρμογής. Η επιλογή SecurityToken διευκολύνει τον εντοπισμό και την εξουσιοδότηση για την παροχή πρόσβασης σε πόρους του CoAP σε επίπεδο εφαρμογής. Η επιλογή SecurityEncap χρησιμοποιεί τη διαμόρφωση της επιλογής SecurityOn και κυρίως εκτελεί τη διαβίβαση των δεδομένων που απαιτούνται για την εξακρίβωση της ταυτότητας και την προστασία από τις επαναλήψεις. Μια ασφάλεια βασισμένη στο AES / CCM ενσωματώνεται για την προστασία των μηνυμάτων. Χρησιμοποιώντας τις παραπάνω επιλογές, φαίνεται ότι η προτεινόμενη προσέγγιση έχει καλές επιδόσεις όσον αφορά το χώρο ωφέλιμου φορτίου του πακέτου, την κατανάλωση ενέργειας και το ρυθμό επικοινωνίας. Ομοίως, για ένα δίκτυο που βασίζεται σε δίκτυα IP, προτείνεται ένα μοντέλο ασφαλείας με 6LBR που χρησιμοποιείται για φιλτράρισμα μηνυμάτων

προκειμένου να παρέχεται ασφάλεια από άκρο σε άκρο [\[138\]](#). Η σήραγγα TLS-DTLS μπορεί να δημιουργηθεί ενώ το 6LBR χρησιμοποιείται για χαρτογράφηση κατά τη διάρκεια της χειραψίας. Ομοίως, με δύο κεντρικούς υπολογιστές που μοιράζονται ένα κοινό κλειδί, προτείνεται να πραγματοποιηθεί η επαλήθευση μηνυμάτων ή η ανίχνευση επαναλήψεων στη συσκευή CoAP. Ένα μοντέλο ασφαλείας με ενεργειακή απόδοση που χρησιμοποιεί κρυπτογραφία δημόσιου κλειδιού για CoAP προτείνεται στο [\[139\]](#). Το προτεινόμενο μοντέλο ασφαλείας που εφαρμόζεται μέσω ενός πρωτοτύπου χρησιμοποιεί ένα διακομιστή μεσολάβησης Mirror (MP) και έναν κατάλογο πόρων που αντιπροσωπεύει τον εξυπηρετητή για την εξυπηρέτηση αιτημάτων κατά τη διάρκεια της κατάστασης ύπνου και της λίστας πόρων στον διακομιστή (ή τα τελικά σημεία), αντίστοιχα. Το MP καταγράφει τα τελικά σημεία, προσθέτει τους πόρους σε ένα δέντρο πόρων και αποθηκεύει επίσης τα δημόσια κλειδιά των τελικών σημείων. Οι πόροι προσεγγίζονται από τους πελάτες μέσω αναγνωριστικών πόρων. Τα δημόσια κλειδιά μεταδίδονται στον πελάτη, τα οποία στη συνέχεια χρησιμοποιούνται για τον έλεγχο ταυτότητας των ενημερώσεων δεδομένων. Η εφαρμογή του πρωτοτύπου φαίνεται να απαιτεί μικρή ποσότητα ενέργειας για συσκευές περιορισμένης πρόσβασης. Το έργο OWASP [\[140\]](#) παρέχει συστάσεις αντιμέτρων για την εξασφάλιση της διατήρησης του Ίντερνετ. Για να αντιμετωπίσουν ανασφαλείς διεπαφές υψηλού επιπέδου, οι μηχανισμοί ασφαλείας περιλαμβάνουν τις διαμορφώσεις που αποθαρρύνουν τους αδύναμους κωδικούς πρόσβασης, δοκιμάζοντας τη διεπαφή ενάντια στις γνωστές ευπάθειες των εργαλείων λογισμικού (SQLi και XSS) και τη χρήση του https μαζί με τα firewalls. Επιπλέον, το λογισμικό ή το υλικολογισμικό που είναι εγκατεστημένο στη συσκευή θα πρέπει να ενημερώνεται τακτικά μέσω ενός κρυπτογραφημένου μηχανισμού μετάδοσης. Τα ενημερωμένα αρχεία πρέπει να ληφθούν από ασφαλή διακομιστή και τα αρχεία αυτά πρέπει να υπογραφούν και να επικυρωθούν σωστά πριν από την εγκατάσταση.

Το μεσαίο λογισμικό VIRTUS [\[141\]](#) που προτείνεται στο [\[142\]](#) υλοποιεί έλεγχο ταυτότητας και κρυπτογράφηση για την εξασφάλιση καταναμημένων εφαρμογών που εκτελούνται στο δίκτυο. Το ενδιάμεσο λογισμικό χρησιμοποιεί μια προσέγγιση επικοινωνίας μεταξύ συμβάντων και συμβάντων ενώ ενσωματώνει TLS και SASL για την ακεραιότητα των δεδομένων, την κρυπτογράφηση ροής XML και την επικύρωση. Ο μηχανισμός ελέγχου ταυτότητας διασφαλίζει την ανταλλαγή δεδομένων και την πρόσβαση σε πόρους μόνο για εξουσιοδοτημένους χρήστες. Το ενδιάμεσο λογισμικό VIRTUS που είναι ενσωματωμένο σε υπηρεσίες web έχει ως αποτέλεσμα την εφαρμογή αξιόπιστων και κλιμακούμενων εφαρμογών. Ένα σημασιολογικό πλαίσιο που ονομάζεται Otsopack [\[143\]](#) ενεργεί ως ενδιάμεσο λογισμικό για να αλληλεπιδράσει με ετερογενείς εφαρμογές με έναν ασφαλή τρόπο. Για τη διαλειτουργικότητα, χρησιμοποιεί σημασιολογική μορφή βασισμένη σε Τριπλή Διαστημική Υπολογιστική (TSC) για αλληλεπίδραση μεταξύ εφαρμογών που εκτελούνται εντός ενός εικονικού χώρου. Για την ασφαλή ανταλλαγή δεδομένων, προτείνεται μια λύση ασφαλείας βασισμένη σε Open-ID. Ένας πάροχος ταυτότητας χρησιμοποιείται για την παροχή πρόσβασης περιορισμένων δεδομένων σε εξουσιοδοτημένους χρήστες. Ένας διακομιστής μεσαίας βάσης που υποστηρίζει το φιλτράρισμα δεδομένων κατά τη διάρκεια της επικοινωνίας μεταξύ ετερογενών περιβαλλόντων του δικτύου προτείνεται στο [\[144\]](#). Το προτεινόμενο μεσαίο λογισμικό υποστηρίζει αποτελεσματικό μηχανισμό για την ονομασία, τη διεύθυνσιδότηση και τη δημιουργία προφίλ σε ετερογενή περιβάλλοντα. Οι τυπικές λειτουργίες ελέγχου ταυτότητας, εξουσιοδότησης και λογιστικής (AAA) υλοποιούνται μέσω μιας ιεραρχίας κλειδιών με πλήκτρα για ρίζες, εφαρμογές και υπηρεσίες. Για την εγγραφή υπηρεσίας, υλοποιείται μια δικτυακή πύλη που παρέχει πρόσβαση σε υπηρεσίες μόνο σε

εξουσιοδοτημένους χρήστες. Για τις επικοινωνίες μηχανής προς μηχανή (M2M) στο περιβάλλον του Διαδικτύου, προτείνεται μια τυποποιημένη αρχιτεκτονική με διαφορετικά επίπεδα ασφάλειας [145]. Η προτεινόμενη αρχιτεκτονική περιλαμβάνει στρώματα για υπηρεσίες ασφαλείας που αντιστοιχούν στη λειτουργικότητα της ασφάλειας, το περιβάλλον και την αφαίρεση. Για την ασφάλεια επιπέδου υπηρεσίας M2M, τα περιεχόμενα των πόρων προτείνεται να κρυπτογραφούνται μαζί με την ασφαλή ανταλλαγή μηνυμάτων χρησιμοποιώντας συνεδρίες TLS ή DTLS.

5.4. Περισσότερες λύσεις ασφάλειας και διασφάλισης ιδιωτικότητας με τη χρήση Blockchain.

Η τεχνολογία Blockchain έχει προβλεφθεί από τη βιομηχανία και την ερευνητική κοινότητα ως μια αποδιοργανωτική τεχνολογία που είναι έτοιμη να διαδραματίσει σημαντικό ρόλο στη διαχείριση, τον έλεγχο και κυρίως τη διασφάλιση συσκευών IoT. Αυτή η ενότητα περιγράφει τον τρόπο με τον οποίο το blockchain μπορεί να είναι μια βασική τεχνολογία ενεργοποίησης για την παροχή βιώσιμων λύσεων ασφάλειας στα σημερινά προκλητικά προβλήματα ασφάλειας του IoT. Η ενότητα δίνει πρώτα ένα σύντομο υπόβαθρο σχετικά με το blockchain και, στη συνέχεια, περιγράφει τα ανοικτά ερευνητικά ερευνητικά προβλήματα IoT και τις προκλήσεις που μπορεί να προσφέρει λύσεις για το blockchain. Το τμήμα εξετάζει επίσης τη βιβλιογραφία των λύσεων που βασίζονται σε blockchain για προβλήματα ασφάλειας του Διαδικτύου [146].

5.4.1. Ιστορικό.

Ένα blockchain είναι βασικά ένας αποκεντρωμένος, καταναμημένος, κοινόχρηστος και αμετάβλητος ημερολογέας βάσης δεδομένων που αποθηκεύει μητρώο περιουσιακών στοιχείων και συναλλαγών μέσω ενός δικτύου peer-to-peer (P2P). Έχει αλυσιδωτά μπλοκ δεδομένων που έχουν επισημανθεί και επικυρωθεί από τους ανθρακωρύχους. Το blockchain χρησιμοποιεί κρυπτογράφηση ελλειπτικής καμπύλης (ECC) και SHA-256 hashing για να παρέχει ισχυρή κρυπτογραφική απόδειξη για έλεγχο ταυτότητας και ακεραιότητα δεδομένων [147]. Βασικά, τα δεδομένα μπλοκ περιέχουν μια λίστα με όλες τις συναλλαγές και ένα hash με το προηγούμενο μπλοκ. Το blockchain έχει ένα πλήρες ιστορικό όλων των συναλλαγών και προσφέρει μια διασυνωριακή παγκόσμια καταναμημένη εμπιστοσύνη. Τα εμπιστευμένα τρίτα μέρη (TTP) ή οι κεντρικές αρχές και υπηρεσίες μπορούν να διαταραχθούν, να συμπεράσουν (compromised) ή να τεθούν σε πειρατεία. Μπορούν επίσης να παραβιάζουν και να καταστρέφονται στο μέλλον, ακόμα κι αν είναι αξιόπιστοι τώρα. Σε blockchain, κάθε συναλλαγή στο κοινό κοινό μητρώο επαληθεύεται από την πλειοψηφία συναίνεση των μεταλλικών κόμβων που συμμετέχουν ενεργά στην επαλήθευση και επικύρωση των συναλλαγών. Σε ένα δίκτυο bitcoin [148], οι ανθρακωρύχοι επικυρώνουν το μπλοκ υπολογίζοντας μια κατακερματισμό με μηδενικά που οδηγούν προς επίτευξη του στόχου δυσκολίας. Μόλις οι συναλλαγές επικυρωθούν και επαληθευτούν με συναίνεση, τα δεδομένα μπλοκ είναι αμετάβλητα, δηλ. Τα δεδομένα δεν μπορούν ποτέ να διαγραφούν ή να διαγραφούν. Το blockchain μπορεί να κατασκευαστεί ως: (1) δίκτυο με άδεια (permissioned ή ιδιωτικό) που μπορεί να περιοριστεί σε μια συγκεκριμένη ομάδα συμμετεχόντων ή (2) δίκτυο χωρίς άδεια ή δημόσιο δίκτυο που είναι ανοιχτό για οποιονδήποτε να συμμετάσχει. και καλύτερος έλεγχος πρόσβασης. Η δομή του σχεδίου αποτελείται κυρίως από την κεφαλίδα του μπλοκ και το σώμα του μπλοκ που περιέχει έναν κατάλογο συναλλαγών. Η κεφαλίδα του μπλοκ περιέχει διάφορα πεδία, ένα από τα οποία είναι ένας αριθμός έκδοσης για την παρακολούθηση

του λογισμικού των αναβαθμίσεων πρωτοκόλλων. Επίσης, η κεφαλίδα περιέχει μια χρονική σήμανση, το μέγεθος μπλοκ και τον αριθμό των συναλλαγών. Το ριζικό πεδίο Merkle αντιπροσωπεύει την τιμή κατακερματισμού του τρέχοντος μπλοκ. Ο εντοπισμός δένδρων Merkle χρησιμοποιείται συνήθως σε κατανεμημένα συστήματα και δίκτυα P2P για αποτελεσματική επαλήθευση δεδομένων. Το πεδίο nonce χρησιμοποιείται για τον αλγόριθμο απόδειξης εργασίας και είναι η τιμή του μετρητή δοκιμής που παρήγαγε το hash με αρχικά μηδενικά. Ο στόχος δυσκολίας καθορίζει τον αριθμό των κορυφαίων μηδενικών και χρησιμοποιείται για να διατηρηθεί ο αποκλεισμός περίπου 10 λεπτά για Bitcoin [149] και 17,5 s για το Ethereum [150]. Ο στόχος δυσκολίας ρυθμίζεται περιοδικά και αυξάνεται (με μεγαλύτερα μηδενικά) καθώς η υπολογιστική ισχύς του υλικού αυξάνεται με την πάροδο του χρόνου. Ο χρόνος αποκλεισμού καθορίζεται από το σχεδιασμό για να υπολογίζεται ο χρόνος διάδοσης των μπλοκ για να φτάσει σε όλους τους ανθρακωρύχους και για όλους τους ανθρακωρύχους να επιτευχθεί συναίνεση.

Το Bitcoin είναι μία από τις πρώτες και τις πιο δημοφιλείς εφαρμογές που τρέχουν στην κορυφή της υποδομής blockchain. Σε γενικές γραμμές, το blockchain bitcoin υπήρξε η βασική πλατφόρμα και η τεχνολογία πολλών από τις πιο δημοφιλείς κρυπτοσυχρότητες σήμερα. Ωστόσο, με την έλευση του blockchain Ethereum, το οποίο υλοποιεί έξυπνες συμβάσεις, ο πιθανός χώρος χρήσης για blockchain έχει γίνει ατελείωτος. Το μπλοκάριθρο Ethereum εγκαινιάστηκε και ανοίχθηκε για χρήση στο κοινό τον Ιούλιο του 2015. Στη συνέχεια, αναδείχθηκαν πρόσφατα παρόμοια πλατφόρμες έξυπνων συμβάσεων. Αυτά περιλαμβάνουν το Hyperledger [151], το Eris [152], το Stellar [153], το Ripple [154] και το Tendermint [155]. Σε αντίθεση με το blockchain bitcoin που χρησιμοποιείται κυρίως για συναλλαγές σε ψηφιακό νόμισμα, το block block της Ethereum έχει την ικανότητα να αποθηκεύει αρχεία και, κυρίως, να τρέχει έξυπνες συμβάσεις. Ο όρος "έξυπνες συμβάσεις" επινοήθηκε για πρώτη φορά από τον Nick Szabo το 1994. Μια έξυπνη σύμβαση είναι βασικά ένα μηχανογραφημένο πρωτόκολλο συναλλαγών που εκτελεί τους όρους της σύμβασης. Στον απλουστευμένο ορισμό, τα έξυπνα συμβόλαια είναι προγράμματα γραμμένα από τους χρήστες που πρόκειται να μεταφορτωθούν και να εκτελεστούν στο blockchain. Η γλώσσα προγραμματισμού ή προγραμματισμού για έξυπνες συμβάσεις ονομάζεται Στερεότητα, που είναι μια γλώσσα που μοιάζει με JavaScript. Το Ethereum Blockchain παρέχει EVM (Εικονικές Μηχανές Ethereum) οι οποίες είναι βασικά οι μεταλλικοί κόμβοι. Αυτοί οι κόμβοι είναι σε θέση να παρέχουν αξιόπιστη εκτέλεση και επιβολή αυτών των προγραμμάτων ή συμβολαίων κρυπτογραφικά.

Το Ethereum υποστηρίζει το δικό του ψηφιακό νόμισμα που ονομάζεται Ether. Όπως και στο bitcoin, στο Ethereum, οι χρήστες μπορούν να μεταφέρουν κέρματα ο ένας στον άλλο χρησιμοποιώντας κανονικές συναλλαγές που καταγράφονται στο ημερολόγιο, και για τέτοιες συναλλαγές, δεν υπάρχει ανάγκη για μια κατάσταση blockchain στο bitcoin. Ωστόσο, για να υποστηρίξει την έξυπνη εκτέλεση συμβόλων για την Ethereum, χρησιμοποιείται μια κατάσταση blockchain. Μια έξυπνη σύμβαση έχει δικό της λογαριασμό και διεύθυνση και συνδέεται με αυτήν είναι ο δικός της εκτελεστός κώδικας και ισορροπία των κερμάτων του Αιθέρα. Η αποθήκευση είναι συνεχής και διατηρεί τον κώδικα που πρέπει να εκτελεστεί στους κόμβους EVM. Η αποθήκευση EVM είναι σχετικά δαπανηρή και για την

αποστολή μεγάλου αποθηκευτικού χώρου στο blockchain, μπορεί να χρησιμοποιηθεί ένα άλλο απομακρυσμένο αποκεντρωμένο κατάστημα δεδομένων όπως το BitTorrent, το IPFS ή το Swarm. Εντούτοις, τα έξυπνα συμβόλαια μπορούν να περιέχουν χάρτες επικύρωσης τέτοιων απομακρυσμένων αποθηκευμένων πληροφοριών.

Οι πιθανές περιπτώσεις χρήσης και οι εφαρμογές των εφαρμογών blockchain έξυπνης σύμβασης είναι τεράστιες και ατελείωτες, από την κρυπτογράφηση και τις συναλλαγές έως τις αυτόνομες συναλλαγές μηχανής με μηχανή, από την αλυσίδα εφοδιασμού και την παρακολούθηση στοιχείων έως τον αυτοματοποιημένο έλεγχο πρόσβασης και την κοινή χρήση και από την ψηφιακή ταυτότητα και την ψηφοφορία την πιστοποίηση, τη διαχείριση και τη διακυβέρνηση αρχείων, δεδομένων ή αντικειμένων [156]. Οι εμπορικές αναπτύξεις που βασίζονται σε μπλοκ αλυσίδες αυξάνονται γρήγορα. Για παράδειγμα, το SafeShare [157] έχει προσφέρει ασφαλιστική λύση χρησιμοποιώντας blockchain με βάση bitcoin. Ομοίως, η IBM ξεκίνησε το πλαίσιο blockchain χρησιμοποιώντας την πλατφόρμα Hyperledger Fabric [158]. Το πλαίσιο υποστηρίζει την ανάπτυξη εφαρμογών blockchain, και σε αντίθεση με άλλα πλαίσια, δεν απαιτεί κρυπτοσυχνότητα. Το blockchain της IBM χρησιμοποιείται εμπορικά σε τράπεζες, συστήματα εφοδιαστικής αλυσίδας και εταιρείες ναυτιλίας.

5.4.2. Πιθανές λύσεις σε Blockchain.

Στο πλαίσιο του IoT, το blockchain που βασίζεται σε έξυπνες συμβάσεις αναμένεται να διαδραματίσει σημαντικό ρόλο στη διαχείριση, τον έλεγχο και, κυρίως, στην εξασφάλιση συσκευών IoT. Σε αυτή την ενότητα, συνοψίζω μερικά από τα εγγενή χαρακτηριστικά του blockchain που μπορεί να είναι εξαιρετικά χρήσιμα για το IoT εν γένει και ειδικότερα για την ασφάλεια του IoT. Χώρος διεύθυνσης. Το Blockchain διαθέτει ένα χώρο διεύθυνσης 160-bit, ως προς το χώρο διεύθυνσης IPv6 που έχει χώρο διευθύνσεων 128-bit [159]. Μία διεύθυνση blockchain είναι 20 bytes ή ένα hash 160-bit του δημόσιου κλειδιού που παράγεται από τον ECDSA (Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικής Καμπύλης). Με διεύθυνση 160-bit, το blockchain μπορεί να δημιουργήσει και να διαθέσει διαφημίσεις offline για περίπου 1,46 συσκευές 1048 IoT. Η πιθανότητα σύγκρουσης διεύθυνσης είναι περίπου 1048, η οποία θεωρείται επαρκώς ασφαλής για την παροχή GUID (Global Unique Identifier) που δεν απαιτεί έλεγχο εγγραφής ή μοναδικότητας κατά την εκχώρηση και την κατανομή μιας διεύθυνσης σε μια συσκευή IoT. Με το blockchain, εξαλείφεται μια κεντρική αρχή και διακυβέρνηση, όπως αυτή της Αρχής Τηλεφωνικών Αριθμών (IANA). Επί του παρόντος, ο IANA επιβλέπει την κατανομή των παγκόσμιων διευθύνσεων IPv4 και IPv6. Επιπλέον, το blockchain παρέχει 4.3 δισεκατομμύρια διευθύνσεις περισσότερο από το IPv6, καθιστώντας έτσι το blockchain μια πιο επεκτάσιμη λύση για το IoT από το IPv6. Τέλος, αξίζει να σημειωθεί ότι πολλές συσκευές IoT περιορίζονται στη μνήμη και την ικανότητα υπολογισμών και συνεπώς δεν είναι ικανές να εκτελέσουν μια στοίβα IPv6.

Ταυτότητα των πραγμάτων (IDoT) και διακυβέρνηση. Η διαχείριση ταυτότητας και πρόσβασης (IAM) για το Διαδίκτυο πρέπει να αντιμετωπίσει μια σειρά προβλημάτων με αποτελεσματικό, ασφαλή και αξιόπιστο τρόπο. Μια πρωταρχική πρόκληση αφορά την ιδιοκτησία και τις σχέσεις ταυτότητας των συσκευών του Διαδικτύου. Η ιδιοκτησία μιας συσκευής αλλάζει κατά τη

διάρκεια της ζωής της συσκευής από τον κατασκευαστή, τον προμηθευτή, τον έμπορο λιανικής πώλησης και τον καταναλωτή [160], [161]. Η ιδιοκτησία του καταναλωτή μιας συσκευής IoT μπορεί να αλλάξει ή να ανακληθεί, εάν η συσκευή μεταπωληθεί, παροπλισθεί ή διακυβευτεί. Η διαχείριση των χαρακτηριστικών και των σχέσεων μιας συσκευής IoT είναι μια άλλη πρόκληση. Τα χαρακτηριστικά μιας συσκευής μπορούν να περιλαμβάνουν τον κατασκευαστή, τη μάρκα, τον τύπο, τον αύξοντα αριθμό, τις συντεταγμένες GPS εγκατάστασης, τη θέση κλπ. Εκτός από τις ιδιότητες, τις δυνατότητες και τις λειτουργίες, οι συσκευές IoT έχουν σχέσεις. Οι σχέσεις διαδικτύου μπορεί να περιλαμβάνουν τη συσκευή από άνθρωπο, συσκευή σε συσκευή ή συσκευή σε υπηρεσία. Οι σχέσεις συσκευών IoT μπορούν να αναπτυχθούν από, να χρησιμοποιηθούν, να μεταφερθούν, να πωληθούν, να αναβαθμιστούν, να επισκευαστούν, να πωληθούν, κ.λπ.

Το Blockchain έχει την ικανότητα να επιλύει αυτές τις προκλήσεις εύκολα, με ασφάλεια και αποτελεσματικά. Το Blockchain έχει χρησιμοποιηθεί ευρέως για την παροχή αξιόπιστης και εγκεκριμένης εγγραφής ταυτότητας, παρακολούθησης ιδιοκτησίας και παρακολούθησης προϊόντων, αγαθών και περιουσιακών στοιχείων. Οι προσεγγίσεις όπως το TrustChain [162] προτείνονται για να επιτρέψουν την εμπιστοσύνη των συναλλαγών χρησιμοποιώντας blockchain, διατηρώντας ταυτόχρονα την ακεραιότητα των συναλλαγών σε ένα κατακευματισμένο περιβάλλον. Οι συσκευές IoT δεν αποτελούν εξαίρεση. Το Blockchain μπορεί να χρησιμοποιηθεί για την καταχώρηση και την αναγνώριση ταυτότητας σε συνδεδεμένες συσκευές IoT, με ένα σύνολο χαρακτηριστικών και περίπλοκων σχέσεων που μπορούν να μεταφορτωθούν και να αποθηκευτούν στον κατακευματισμένο κατάλογο blockchain.

Το Blockchain παρέχει επίσης μια αξιόπιστη αποκεντρωμένη διαχείριση, διακυβέρνηση και παρακολούθηση σε κάθε σημείο της αλυσίδας εφοδιασμού και στον κύκλο ζωής μιας συσκευής IoT. Η αλυσίδα εφοδιασμού μπορεί να περιλαμβάνει πολλαπλούς παίκτες όπως εργοστάσιο, πωλητή, προμηθευτή, διανομέα, αποστολέα, εγκαταστάτη, ιδιοκτήτη, επισκευαστή, επανεγκατάσταση, κλπ. Όπως φαίνεται στην εικόνα. Τα keypairs μπορούν να αλλάξουν και να εκδοθούν εκ νέου σε πολλά σημεία κατά τη διάρκεια του κύκλου ζωής μιας συσκευής IoT. Η έκδοση των keypairs μπορεί να γίνει αρχικά από τον κατασκευαστή, στη συνέχεια από τον ιδιοκτήτη, περιοδικά μετά την εγκατάσταση.

Έλεγχος ταυτότητας δεδομένων και ακεραιότητα. Με τη σχεδίαση, τα δεδομένα που μεταδίδονται από συσκευές IoT που είναι συνδεδεμένα στο δίκτυο μπλοκ αλυσίδων θα είναι πάντοτε κρυπτογραφημένα και θα υπογράφονται από τον πραγματικό αποστολέα που κατέχει ένα μοναδικό δημόσιο κλειδί και GUID και έτσι θα εξασφαλίζει τον έλεγχο ταυτότητας και την ακεραιότητα των μεταδιδόμενων δεδομένων. Επιπρόσθετα, όλες οι συναλλαγές που γίνονται σε ή από μια συσκευή IoT καταγράφονται στον λογαριθμικό κατακευματισμένο κατάλογο και μπορούν να παρακολουθηθούν με ασφάλεια.

Έλεγχος ταυτότητας, εξουσιοδότηση και ιδιωτικό απόρρητο. Τα έξυπνα συμβόλαια Blockchain έχουν τη δυνατότητα να παρέχουν κανόνες

αποκεντρωμένης αυθεντικότητας και λογική ώστε να είναι σε θέση να παρέχουν έλεγχο ταυτότητας μεμονωμένων και πολλαπλών μερών σε μια συσκευή IoT. Επίσης, οι έξυπνες συμβάσεις μπορούν να παρέχουν αποτελεσματικότερους κανόνες πρόσβασης σε εξουσιοδοτήσεις σε συνδεδεμένες συσκευές IoT με λιγότερη πολυπλοκότητα σε σύγκριση με τα παραδοσιακά πρωτόκολλα εξουσιοδότησης όπως RBAC, OAuth 2.0, OpenID, OMA DM και LWM2M. Αυτά τα πρωτόκολλα χρησιμοποιούνται ευρέως αυτές τις μέρες για έλεγχο ταυτότητας συσκευών IoT, εξουσιοδότηση και διαχείριση. Επιπλέον, το ιδιωτικό απόρρητο δεδομένων μπορεί να διασφαλιστεί και με τη χρήση έξυπνων συμβάσεων που ορίζουν τους κανόνες πρόσβασης, τους όρους και τον χρόνο που επιτρέπουν σε μεμονωμένα άτομα ή ομάδες χρηστών ή μηχανών να κατέχουν, να ελέγχουν ή να έχουν πρόσβαση σε δεδομένα σε κατάσταση ηρεμίας ή διαμετακόμισης. Οι έξυπνες συμβάσεις μπορούν επίσης να διευκρινίσουν ποιος έχει το δικαίωμα να ενημερώσει, να αναβαθμίσει, να διορθώσει το λογισμικό ή το υλικό του IoT, να επαναφέρει τη συσκευή IoT, να παράσχει νέα πληκτρολόγια, να ξεκινήσει μια υπηρεσία ή επισκευή, να αλλάξει ιδιοκτησία και να παράσχει ή να επαναφέρει η συσκευή.

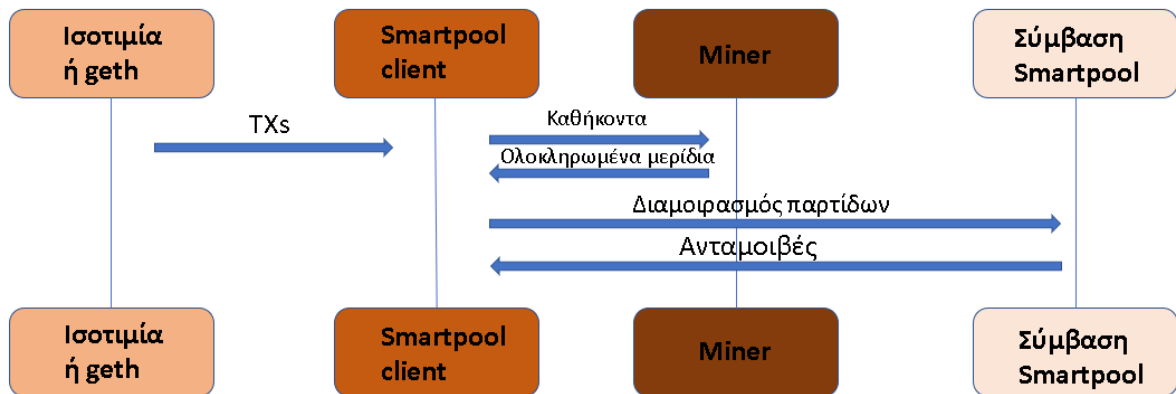
Πρωτόκολλα όπως αυτά του HTTP, MQTT, CoAP ή XMPP, ή ακόμα και πρωτόκολλα που σχετίζονται με τη δρομολόγηση όπως αυτά των RPL και 6LoWPAN, δεν είναι ασφαλή από το σχεδιασμό. Τέτοια πρωτόκολλα πρέπει να περιτυλιγμένα με άλλα πρωτόκολλα ασφάλειας όπως το DTLS ή το TLS για μηνύματα και πρωτόκολλα εφαρμογής για την ασφαλή επικοινωνία. Ομοίως, για τη δρομολόγηση, το IPSec χρησιμοποιείται συνήθως για την παροχή ασφάλειας για τα πρωτόκολλα RPL και 6LoWPAN. Το DTLS, το TLS, το IPSec ή ακόμα και τα ελαφριά πρωτόκολλα TinyTLS είναι βαρύ και σύνθετα από πλευράς υπολογισμών και απαιτήσεων μνήμης και περιπλέκονται με μια κεντρική διαχείριση και διακυβέρνηση βασικών διευθύνσεων και διανομών χρησιμοποιώντας το δημοφιλές πρωτόκολλο PKI. Με blockchain, η διαχείριση και η διανομή των κλειδιών εξαλείφονται πλήρως, καθώς κάθε συσκευή IoT θα έχει το δικό της μοναδικό GUID και ασύμμετρο ζευγάρι κλειδιών μόλις εγκατασταθεί και συνδεθεί στο δίκτυο blockchain. Αυτό θα οδηγήσει επίσης σε σημαντική απλοποίηση άλλων πρωτοκόλλων ασφαλείας, όπως αυτή του DTLS, χωρίς να χρειάζεται να χειρίζονται και να ανταλλάσσουν πιστοποιητικά PKI στη φάση χειραγίας σε περίπτωση DTLS ή TLS (ή IKE σε περίπτωση IPSec) για διαπραγμάτευση παράμετροι κρυπτογράφησης για κρυπτογράφηση και αντιστοίχιση και για τον καθορισμό των πλήκτρων κύριας και συνεδρίας. Επομένως, τα πρωτόκολλα ασφαλείας ελαφρού βάρους που θα ταιριάζουν και διαστρωματίζουν τις απαιτήσεις για τους υπολογιστές και τους πόρους μνήμης των συσκευών IoT γίνονται πιο εφικτοί.

5.5. Βελτιώσεις της ασφάλειας και διασφάλισης ιδιωτικότητας.

Σε αυτή την ενότητα, συνοψίζουμε τις βελτιώσεις ασφαλείας στα συστήματα blockchain, τα οποία μπορούν να χρησιμοποιηθούν στην ανάπτυξη συστημάτων blockchain.

5.5.1. SmartPool.

Υπάρχει ήδη μια δεξαμενή εξόρυξης με περισσότερο από το 40% της συνολικής υπολογιστικής ισχύος του blockchain. Αυτό αποτελεί σοβαρή απειλή για τη φύση της αποκέντρωσης, καθιστώντας το blockchain ευάλωτο σε διάφορες επιθέσεις. Στο [163] προτείνουν ένα νέο σύστημα συλλογής εξορυκτικών στοιχείων που ονομάζεται SmartPool. Το SmartPool παίρνει τις συναλλαγές από τους πελάτες κόμβων Ethereum (δηλαδή, parity [164] ή geth [165]), οι οποίοι περιέχουν πληροφορίες σχετικά με εργασίες εξόρυξης. Στη συνέχεια, ο ορυχείο διεξάγει υπολογισμό κατακερματισμού με βάση τα καθήκοντα και επιστρέφει τις ολοκληρωμένες μετοχές στον πελάτη Smartpool. Όταν ο αριθμός των ολοκληρωμένων μετοχών φθάσει σε ένα ορισμένο ποσό, θα δεσμευτούν για σύμβαση Smartpool, η οποία αναπτύσσεται στο Ethereum. Η σύμβαση Smartpool θα επαληθεύσει τις μετοχές και θα αποδώσει ανταμοιβές στον πελάτη. Σε σύγκριση με την παραδοσιακή πισίνα P2P, το σύστημα SmartPool έχει τα ακόλουθα πλεονεκτήματα:



Πίνακας 23. Βελτίωση ασφάλειας και διασφάλισης ιδιωτικότητας με Smart Pool

- Αποκέντρωση. Ο πυρήνας του SmartPool υλοποιείται με τη μορφή έξυπνης σύμβασης, η οποία αναπτύσσεται σε blockchain. Οι ανθρακωρύχοι πρέπει πρώτα να συνδεθούν με το Ethereum για να πετάξουν μέσω του πελάτη. Η εξορυκτική πισίνα μπορεί να βασιστεί στον μηχανισμό συναίνεσης του Ethereum για να τρέξει. Με αυτόν τον τρόπο, διασφαλίζει τη φύση της αποκέντρωσης των ανθρακωρύχων. Η κατάσταση της οργάνωσης της εξορυκτικής βιομηχανίας διατηρείται από την Ethereum και δεν απαιτεί πλέον την εκμετάλλευση της πισίνας.
- Αποδοτικότητα. Οι ανθρακωρύχοι μπορούν να στείλουν τις ολοκληρωμένες μετοχές στη σύμβαση smartpool σε παρτίδες. Επιπλέον, οι ανθρακωρύχοι πρέπει μόνο να στείλουν μέρος των μετοχών που πρέπει να εξακριβωθούν, όχι όλες οι μετοχές. Ως εκ τούτου, το SmartPool είναι πιο αποτελεσματικό από το pool P2P.
- Ασφάλεια. Το SmartPool εκμεταλλεύεται μια νέα δομή δεδομένων, η οποία μπορεί να αποτρέψει τον εισβολέα από την εκ νέου υποβολή μετοχών σε διαφορετικές παρτίδες. Επιπλέον, η μέθοδος επαλήθευσης του SmartPool μπορεί να εγγυηθεί ότι οι ειλικρινείς ανθρακωρύχοι θα

αποκτήσουν τις αναμενόμενες ανταμοιβές ακόμη και αν υπάρχουν κακοί ανθρακωρύχοι στην πισίνα.

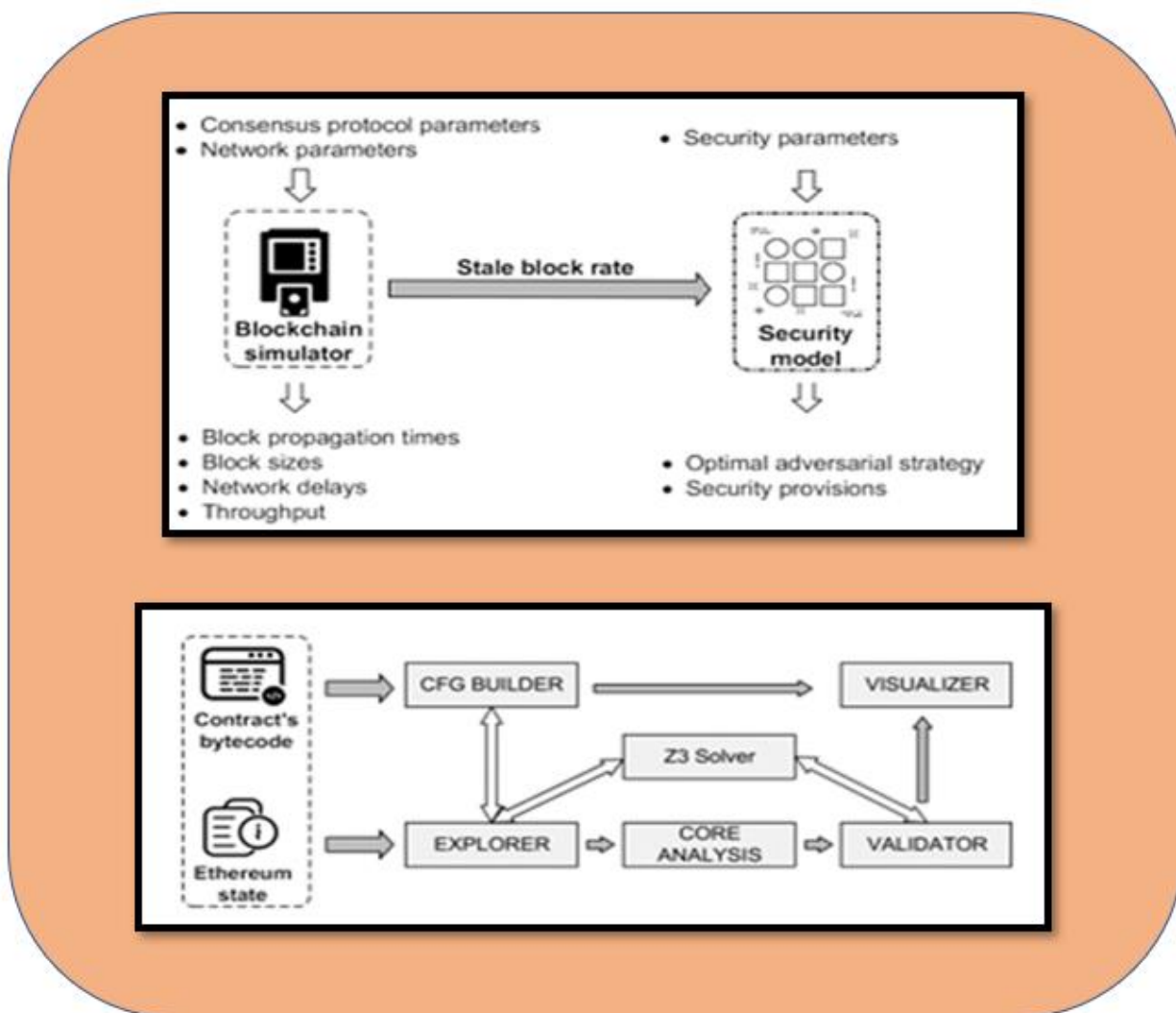
5.5.2. Ποσοτικό πλαίσιο.

Υπάρχουν συμφωνίες μεταξύ της απόδοσης και της ασφάλειας του blockchain. Στο [130] προτείνουν ένα ποσοτικό πλαίσιο, το οποίο αξιοποιεί την ανάλυση των εκτελεστικών εξουσιών εκτέλεσης και των προτύπων ασφαλείας που βασίζονται στο PoW. Το πλαίσιο έχει δύο συνιστώσες: διεγέρτης blockchain και μοντέλο ασφαλείας. Ο διεγέρτης μιμείται την εκτέλεση του blockchain, των οποίων οι εισοδοί είναι παράμετροι πρωτοκόλλου συναίνεσης και δικτύου. Μέσω της ανάλυσης του προσομοιωτή, μπορεί να αποκτήσει στατιστικά στοιχεία απόδοσης του μπλοκ-στόχου στόχου, συμπεριλαμβανομένων των χρόνων πολλαπλασιασμού των μπλοκ, των μεγεθών των μπλοκ, των καθυστερήσεων του δικτύου, του παγώματος, της απόδοσης, κλπ. Το παλιό μπλοκ αναφέρεται σε μπλοκ που εξορύσσεται αλλά όχι γραμμένο στη δημόσια αλυσίδα. Η απόδοση είναι ο αριθμός των συναλλαγών που μπορεί να χειριστεί το blockchain ανά δευτερόλεπτο. Ο παρών ρυθμός μπλοκαρίσματος θα περάσει ως παράμετρος για το στοιχείο μοντέλου ασφαλείας, το οποίο βασίζεται στο MDP (Markov Decision Processes) για την αποτροπή διπλών δαπανών και εγωκεντρικών επιθέσεων εξόρυξης. Το πλαίσιο τελικά καταλήγει σε βέλτιστη αντίπαλη στρατηγική ενάντια στις επιθέσεις και διευκολύνει την κατασκευή διατάξεων ασφαλείας για το blockchain.

5.5.3. Oyente.

Στο [166] προτείνεται η Oyente να ανιχνεύει σφάλματα στις έξυπνες συμβάσεις του Ethereum. Oyente αξιοποιεί την συμβολική εκτέλεση για να αναλύσει τον bytecode των έξυπνων συμβολαίων και ακολουθεί το μοντέλο εκτέλεσης της EVM. Εφόσον η Ethereum αποθηκεύει τον παρελθόν των έξυπνων συμβολαίων στο blockchain της, το Oyente μπορεί να χρησιμοποιηθεί για την ανίχνευση σφαλμάτων στις αναπτυγμένες συμβάσεις.

Ο παρακάτω πίνακας δείχνει την αρχιτεκτονική και τη διαδικασία εκτέλεσης του Oyente. Παίρνει την είσοδο του bytecode της έξυπνης σύμβασης και της παγκόσμιας κατάστασης του Ethereum. Πρώτον, με βάση τον bytecode, ο CFG BUILDER θα κατασκευάσει στατικά το CFG (Flow Flow Graph) της έξυπνης σύμβασης. Στη συνέχεια, σύμφωνα με την πληροφορία του Ethereum και της CFG, η EXPLORER διεξάγει απλή εκτέλεση έξυπνης συμβολικής εκτέλεσης έξυπνης σύμβασης. Σε αυτή τη διαδικασία, το CFG θα εμπλουτιστεί περαιτέρω και θα βελτιωθεί επειδή ορισμένοι στόχοι άλματος δεν είναι σταθερές. Αντίθετα, θα πρέπει να υπολογίζονται κατά τη συμβολική εκτέλεση. Η ενότητα CORE ANALYSIS χρησιμοποιεί τους συναφείς αλγόριθμους ανάλυσης για την ανίχνευση τεσσάρων διαφορετικών τρωτών σημείων (που περιγράφονται στην Ενότητα 3.2.2). Το μοντέλο VALIDATOR επικυρώνει τα εντοπισμένα τρωτά σημεία και τις ευάλωτες διαδρομές. Η επιβεβαιωμένη ευπάθεια και οι πληροφορίες CFG θα αποσταλούν τελικά στη λειτουργική μονάδα VISUALIZER, η οποία μπορεί να χρησιμοποιηθεί από τους χρήστες για την εκτέλεση εντολών εντοπισμού σφαλμάτων και ανάλυσης προγράμματος. Επί του παρόντος, το Oyente είναι ανοικτού κώδικα για δημόσια χρήση [167].



Πίνακας 24. Βελτίωση ασφάλειας και διασφάλισης ιδιωτικότητας με Oyente

5.5.4. Hawk.

Η διαρροή απορρήτου αποτελεί σοβαρή απειλή για την αποκλειστικότητα. Στην εποχή του blockchain 2.0, όχι μόνο οι συναλλαγές αλλά και οι σχετικές με το συμβόλαιο πληροφορίες είναι δημόσιες, όπως ο bytecode της σύμβασης, η επίκληση παραμέτρων κλπ.

Στο [168] προτείνει το Hawk, ένα νέο πλαίσιο για την ανάπτυξη έξυπνων συμβολαίων για τη διατήρηση της ιδιωτικής ζωής. Χρησιμοποιώντας το Hawk, οι κατασκευαστές μπορούν να γράψουν ιδιωτικά έξυπνα συμβόλαια και δεν είναι απαραίτητο να χρησιμοποιήσουν οποιαδήποτε κρυπτογράφηση κώδικα ή τεχνικές θωράκισης. Επιπλέον, οι πληροφορίες της χρηματοοικονομικής συναλλαγής δεν θα αποθηκεύονται ρητά σε blockchain. Όταν οι προγραμματιστές αναπτύσσουν συμβόλαιο Hawk, η σύμβαση μπορεί να χωριστεί σε δύο μέρη: ιδιωτική μερίδα και δημόσιο τμήμα. Οι κωδικοί

ιδιωτικών δεδομένων και των οικονομικών λειτουργιών μπορούν να εγγραφούν στο ιδιωτικό τμήμα και οι κωδικοί που δεν περιλαμβάνουν ιδιωτικές πληροφορίες μπορούν να γραφτούν στο δημόσιο τμήμα. Η σύμβαση Hawk καταρτίζεται σε τρία κομμάτια.

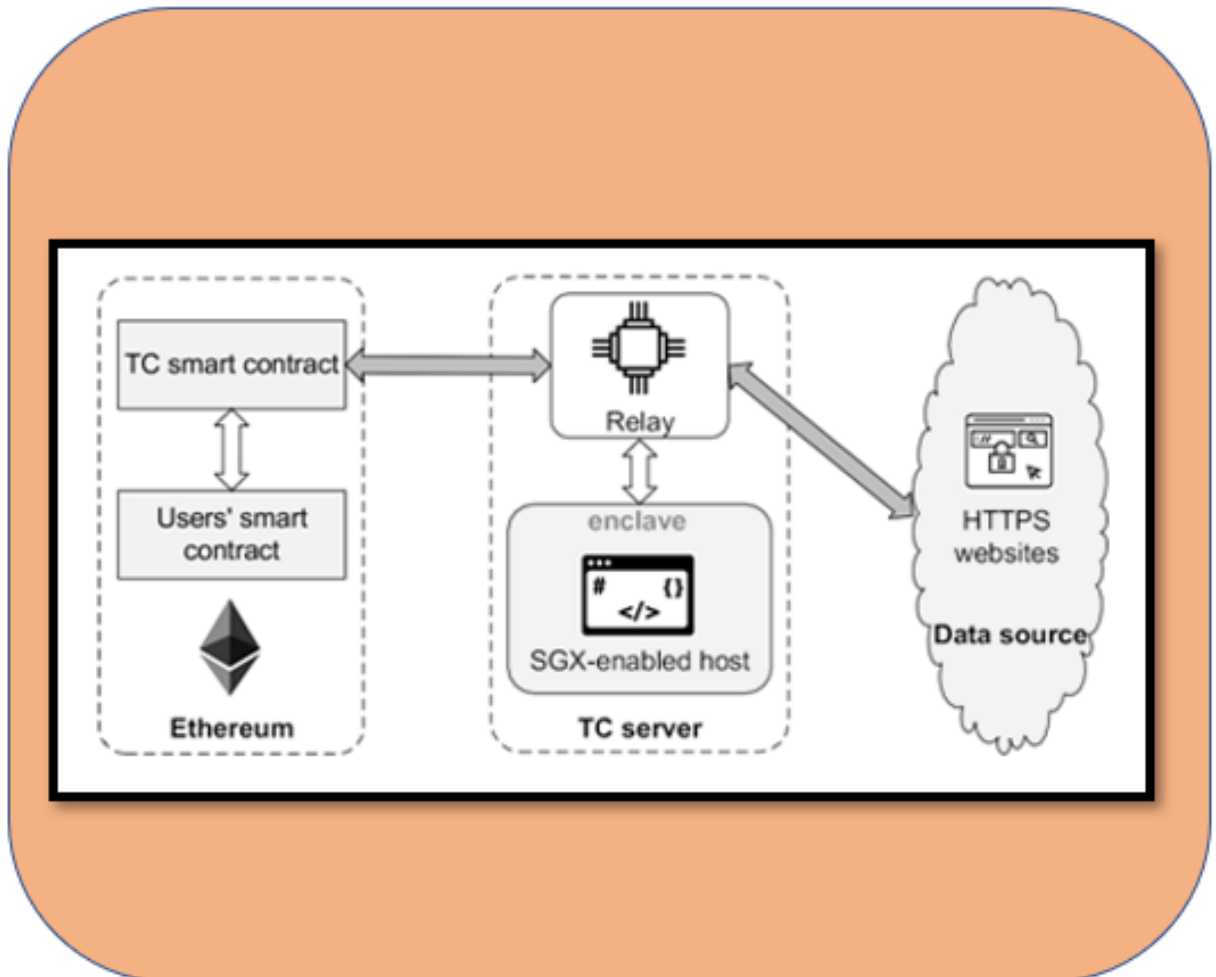
- Το πρόγραμμα που θα εκτελεστεί σε όλες τις εικονικές μηχανές κόμβων, όπως και οι έξυπνες συμβάσεις στο Ethereum.
- Το πρόγραμμα που θα εκτελεστεί μόνο από τους χρήστες έξυπνων συμβάσεων.
- Το πρόγραμμα που θα εκτελεστεί από τον διαχειριστή, το οποίο είναι ένα ειδικό αξιόπιστο κόμμα στο Hawk. Ο διαχειριστής Hawk εκτελείται σε θύρα Intel SGX και μπορεί να δει τις πληροφορίες απορρήτου της σύμβασης αλλά δεν θα το αποκαλύψει. Το γεράκι δεν μπορεί μόνο να προστατεύσει την προστασία της ιδιωτικής ζωής από το κοινό αλλά και να προστατεύσει την ιδιωτική ζωή μεταξύ των διαφόρων συμβάσεων Hawk. Εάν ο διαχειριστής ακυρώσει το πρωτόκολλο του Hawk, αυτό θα τιμωρηθεί αυτόματα οικονομικά και οι χρήστες θα αποζημιωθούν. Συνολικά, το Hawk μπορεί σε μεγάλο βαθμό να προστατεύσει το απόρρητο των χρηστών όταν χρησιμοποιούν blockchains.

5.5.5. Town Crier.

Το έξυπνο συμβόλαιο πρέπει συχνά να αλληλεπιδράσει με την εξωτερική (δηλαδή εξωτερική) πηγή δεδομένων. Στο [169] προτείνει το TC (Town Crier), το οποίο είναι ένα πιστοποιημένο σύστημα ροής δεδομένων για αυτήν τη διαδικασία αλληλεπίδρασης δεδομένων. Από τη στιγμή που το έξυπνο συμβόλαιο που αναπτύσσεται σε blockchain δεν μπορεί να έχει πρόσβαση απευθείας στο δίκτυο, δεν μπορούν να λάβουν δεδομένα μέσω του HTTPS. Το TC λειτουργεί ακριβώς ως γέφυρα μεταξύ πηγής δεδομένων με δυνατότητα HTTPS και έξυπνων συμβολαίων. Η βασική αρχιτεκτονική του TC εμφανίζεται παρακάτω. Το συμβόλαιο TC είναι το εμπρόσθιο τμήμα του συστήματος TC, το οποίο λειτουργεί ως API μεταξύ των συμβάσεων χρηστών και του εξυπηρετητή TC. Το βασικό πρόγραμμα του TC εκτελείται σε θύρα Intel SGX Η κύρια λειτουργία του εξυπηρετητή TC είναι η απόκτηση των αιτημάτων δεδομένων από τα συμβόλαια των χρηστών και η απόκτηση των δεδομένων από τους ιστότοπους με δυνατότητα HTTPS με στόχο. Τέλος, ο διακομιστής TC θα επιστρέψει ένα datagram στις συμβάσεις χρηστών με τη μορφή ψηφιακά υπογεγραμμένων blockchain μηνυμάτων.

Το TC μπορεί σε μεγάλο βαθμό να προστατεύσει την ασφάλεια των διαδικασιών που ζητούν δεδομένα. Οι βασικές ενότητες του TC λειτουργούν αντίστοιχα σε αποκεντρωμένο Ethereum, ενεργοποιημένο από SGX και σε διαδικτυακό τόπο με δυνατότητα HTTPS. Επιπλέον, ο θύλακας απενεργοποιεί τη λειτουργία του δικτύου για να μεγιστοποιηθεί η ασφάλειά του. Η μονάδα αναμετάδοσης έχει σχεδιαστεί ως κόμβος επικοινωνίας δικτύου για έξυπνες συμβάσεις, περιβάλλον enclave SGX και ιστοσελίδες προέλευσης δεδομένων. Επομένως, επιτυγχάνει απομόνωση μεταξύ της επικοινωνίας δικτύου και της εκτέλεσής του.

Το βασικό πρόγραμμα της TC. Ακόμα και αν επιτεθεί η μονάδα Ρελέ ή τα πακέτα επικοινωνίας δικτύου παραβιάζονται, δεν θα αλλάξει η κανονική λειτουργία του TC. Το σύστημα TC παρέχει ένα ισχυρό μοντέλο ασφάλειας για την αλληλεπίδραση δεδομένων έξυπνων συμβάσεων έξυπνων συμβάσεων και έχει ήδη ξεκινήσει ηλεκτρονικά ως δημόσια υπηρεσία [170].



Πίνακας 25. Βελτίωση ασφάλειας και διασφάλισης ιδιωτικότητας με Town Crier

5.6. Ασφαλείς Λύσεις Blockchain στο Cloud Computing.

Εάν τα δεδομένα χρήστη αποκαλυφθούν στο περιβάλλον του cloud computing, μπορεί να προκύψουν νομισματικές και ψυχολογικές ζημιές εξαιτίας της διαρροής ευαίσθητων πληροφοριών των χρηστών. Η ασφάλεια των δεδομένων αποθήκευσης και μετάδοσης, όπως η εμπιστευτικότητα και η ακεραιότητα, στο περιβάλλον του cloud computing, μελετάται κυρίως. Σημειώστε, ωστόσο, ότι οι μελέτες για την προστασία της ιδιωτικής ζωής και την ανωνυμία δεν επαρκούν. Το Blockchain είναι αντιπροσωπευτική τεχνολογία για την εξασφάλιση ανωνυμίας. Σε συνδυασμό με το περιβάλλον υπολογιστικού νέφους, το blockchain μπορεί να αναβαθμιστεί σε μια βολική υπηρεσία που παρέχει ισχυρότερη ασφάλεια. Η ανωνυμία του χρήστη μπορεί να διασφαλιστεί εάν χρησιμοποιείται η μέθοδος blockchain κατά την αποθήκευση των

πληροφοριών του χρήστη στο περιβάλλον του cloud computing. Ένα ηλεκτρονικό πορτοφόλι είναι εγκατεστημένο όταν χρησιμοποιείτε την τεχνολογία blockchain. Εάν το ηλεκτρονικό πορτοφόλι δεν διαγραφεί σωστά, οι πληροφορίες χρήστη μπορούν να μείνουν πίσω. Οι υπόλοιπες πληροφορίες χρήστη μπορούν να χρησιμοποιηθούν για να μαντέψουν τις πληροφορίες χρηστών. Για την επίλυση αυτού του προβλήματος, προτείνουμε μια λύση που εγκαθιστά και διαγράφει με ασφάλεια το ηλεκτρονικό πορτοφόλι.

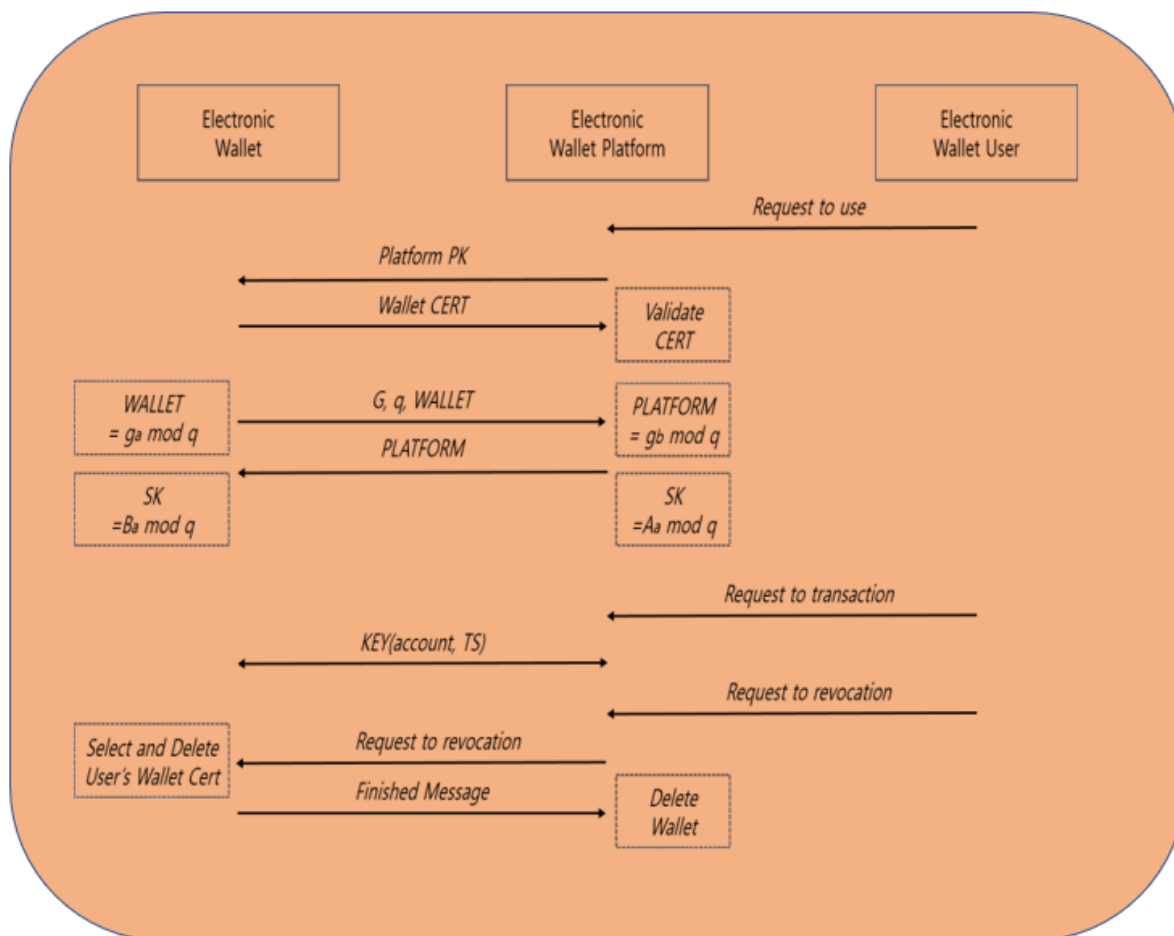
Οι περιπτώσεις πλαστογράφησης του βιβλίου ή του bitcoin και οι διπλές συναλλαγές του blockchain αποτελούν το μεγαλύτερο πρόβλημα. Ένα ασφαλές πορτοφόλι είναι απαραίτητο για την επίλυση τέτοιων προβλημάτων ασφάλειας. Αν και το ηλεκτρονικό πορτοφόλι που είναι εγκατεστημένο στον υπολογιστή χρησιμοποιείται γενικά, η ασφάλεια των ηλεκτρονικών πορτοφολιών σε κινητές συσκευές πρέπει να επαληθεύεται καθώς οι κινητές συσκευές έχουν γίνει πολύ δημοφιλείς. Δεδομένου ότι μια συναλλαγή συμβαίνει με βάση την τιμή χρόνου μιας κινητής συσκευής, η ασφάλεια μιας συναλλαγής μπορεί να επιβεβαιωθεί μόνο όταν είναι εγγυημένη τόσο η ακεραιότητα όσο και η ακρίβεια μιας χρονικής σφραγίδας που παράγεται σε μια κινητή συσκευή [171].

Επιπλέον, πρέπει να επαληθευτεί και η βασική τεχνολογία, καθώς τα τρωτά σημεία διαφέρουν ανάλογα με τη γλώσσα προγραμματισμού και την πλατφόρμα που χρησιμοποιείται για την ανάπτυξη του περιβάλλοντος ηλεκτρονικού πορτοφολιού. Ένα ασφαλές ηλεκτρονικό πορτοφόλι πρέπει να αναπτυχθεί με την ελαχιστοποίηση και την επαλήθευση των προβλημάτων που μπορεί να προκύψουν σε κάθε στάδιο του σχεδιασμού, της ανάλυσης απαιτήσεων, της εφαρμογής, της διασφάλισης της ποιότητας (QA) και της συντήρησης [172].

Το ηλεκτρονικό πορτοφόλι πρέπει να έχει μέτρα για ασφαλή αποκατάσταση εάν παραβιάζεται από εισβολέα, επαλήθευση ενός δυαδικού εγκατεστημένου για αυτοπροστασία και προστασία των υπόλοιπων δεδομένων για αποκατάσταση. Πρέπει να παρέχει ασφάλεια για τα δεδομένα που είναι αποθηκευμένα στο ηλεκτρονικό πορτοφόλι καθώς και τις ρυθμίσεις που απαιτούνται για τη χρήση του ηλεκτρονικού πορτοφολιού. Πρέπει επίσης να είναι σε θέση να διαγράψει τα υπόλοιπα δεδομένα με ασφάλεια όταν το ηλεκτρονικό πορτοφόλι δεν χρησιμοποιείται πλέον και πρέπει συνεπώς να απορριφθεί.

Για να χρησιμοποιήσετε με ασφάλεια ένα ηλεκτρονικό πορτοφόλι, ένας χρήστης το εγκαθιστά στον υπολογιστή του και η πλατφόρμα στέλνει το ηλεκτρονικό πορτοφόλι και δεδομένα για να δημιουργήσει ένα ασφαλές περιβάλλον. Ο χρήστης κατεβάζει και εγκαθιστά το λογισμικό ηλεκτρονικού πορτοφολιού για να χρησιμοποιήσει το bitcoin με blockchain και το δημόσιο κλειδί της πλατφόρμας αποστέλλεται στο ηλεκτρονικό πορτοφόλι όταν ολοκληρωθεί η εγκατάσταση. Το ηλεκτρονικό πορτοφόλι στέλνει το πιστοποιητικό που κατανεμήθηκε κατά την ανάπτυξη στην πλατφόρμα, το οποίο στη συνέχεια επαληθεύει την εγκυρότητα του πιστοποιητικού στο ηλεκτρονικό πορτοφόλι. Η πλατφόρμα και το ηλεκτρονικό πορτοφόλι ανταλλάσσουν το κλειδί χρησιμοποιώντας τη μέθοδο Diffie-Hellman, με το καθένα να διαθέτει το κοινόχρηστο κλειδί. Όταν ένας χρήστης ζητήσει μια συναλλαγή που περιλαμβάνει τη χρήση ενός bitcoin, τα δεδομένα του ημερολογίου που περιέχουν τα δεδομένα της χρονικής σφραγίδας μεταξύ του ηλεκτρονικού πορτοφολιού και της πλατφόρμας είναι κρυπτογραφημένα με το κοινό κλειδί και αποστέλλονται. Όταν εκτελείται μια αίτηση για απόρριψη, το πιστοποιητικό χρήστη βρίσκεται και διαγράφεται από το ηλεκτρονικό πορτοφόλι και αποστέλλεται το τελικό μήνυμα για να επιβεβαιωθεί ότι έχει απορριφθεί

με ασφάλεια. Επιπλέον, όλα τα σχετικά αρχεία διαγράφονται ώστε τα υπόλοιπα δεδομένα να απομακρύνονται με ασφάλεια.



Πίνακας 26. Λύσεις Blockchain στο Cloud Computing

Αυτή η μέθοδος χρησιμοποιεί ένα ηλεκτρονικό πορτοφόλι με βάση το blockchain στο περιβάλλον του cloud computing. Η μέθοδος blockchain χρησιμοποιείται για την κατάρτιση των πληροφοριών του χρήστη που χρησιμοποιεί cloud computing. Αυτή η μέθοδος εγκαθιστά και χρησιμοποιεί ένα ηλεκτρονικό πορτοφόλι και το απομακρύνει κανονικά. Το ηλεκτρονικό πορτοφόλι αφαιρείται με ασφάλεια αποστέλλοντας το τελικό μήνυμα. Η διαρροή πληροφοριών χρηστών μπορεί να αποτραπεί μόνο όταν αφαιρεθεί εντελώς το ηλεκτρονικό πορτοφόλι. Παρόλο που πολλές υπάρχουσες μελέτες έχουν διεξαχθεί στο πρωτόκολλο blockchain, παρουσιάζεται μια μέθοδος για την πλήρη απομάκρυνση του ηλεκτρονικού πορτοφολιού ώστε να διασφαλίζεται η ανωνυμία του χρήστη και η προστασία της ιδιωτικής ζωής.

Συγκρίναμε τη μέθοδο με τις υπάρχουσες μελέτες όσον αφορά την εμπιστευτικότητα, την ακεραιότητα, την ανωνυμία, την προστασία της ιδιωτικής ζωής και την προστασία των υπόλοιπων πληροφοριών. Η εμπιστευτικότητα ελέγχει εάν οι πληροφορίες διαχέονται σε μη εξουσιοδοτημένους συνομηλίκους, ενώ η ακεραιότητα ελέγχει εάν τα δεδομένα που χρησιμοποιούνται στις συναλλαγές μεταβάλλονται ή παραποιούνται

χωρίς κυρώσεις κατά τη μεταφορά ή την αποθήκευση. Η ανωνυμία πρέπει να διασφαλίζει ότι ο ομότιμος που συμμετέχει σε μια συναλλαγή δεν είναι αναγνωρίσιμος. Η προστασία προσωπικών δεδομένων προστατεύει τα προσωπικά στοιχεία των συνομηλίκων που συμμετέχουν στη συναλλαγή, ενώ η προστασία των υπόλοιπων πληροφοριών ελέγχει την ασφαλή απομάκρυνση των δεδομένων χρήστη τη στιγμή της λήξης της συναλλαγής και της κατάργησης του προγράμματος.

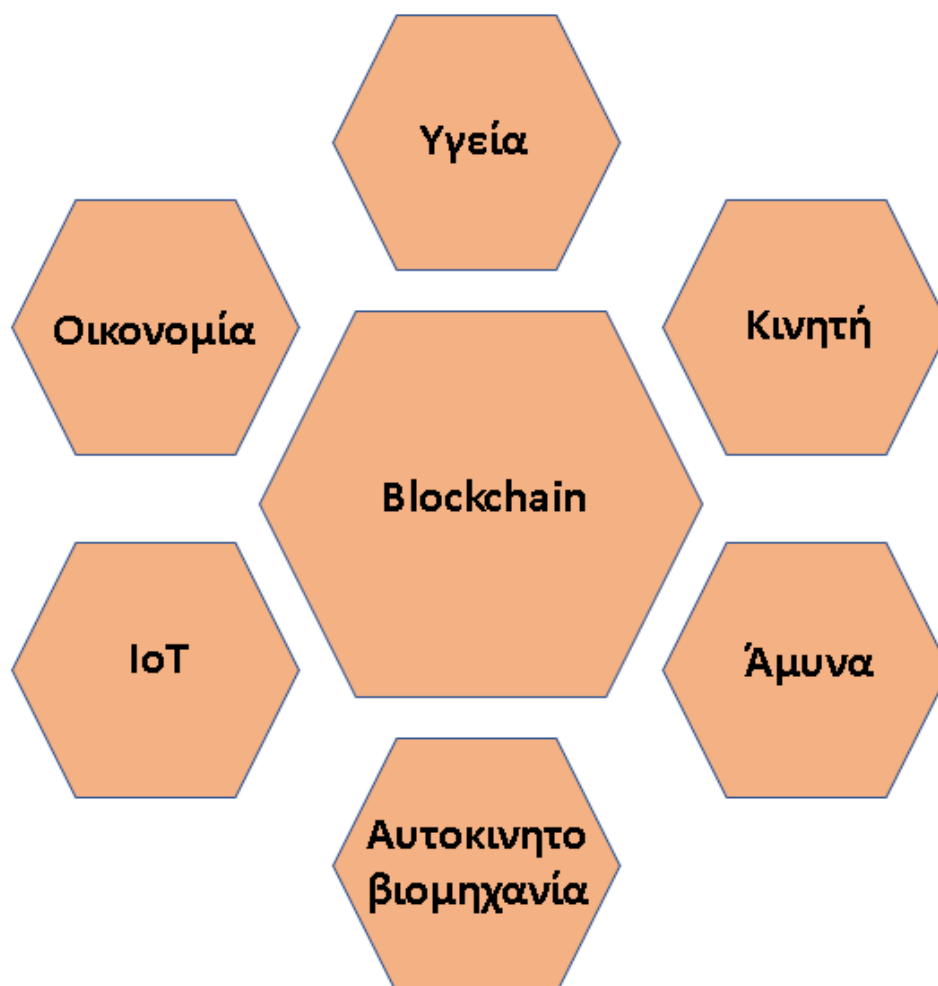
	Περίπτωση αυθεντικοποίησης	Περίπτωση περιστατικών ασφάλειας	Περίπτωση επίθεσης 51%	Περίπτωση Βελτιωμένου Blockchain	Ασφαλής λύση του Blockchain
Confidentiality		✓	✓	✓	✓
Integrity	✓	✓			✓
Anonymity	✓	✓	✓	✓	✓
Privacy Protection					✓
Residual Information	✓	✓	✓	✓	✓
Protection					✓

Πίνακας 27. Παροχές του blockchain

Η περίπτωση ελέγχου ταυτότητας [173] δεν παρέχει ακεραιότητα, καθώς έχει το πρόβλημα της διαρροής του κλειδιού, χάνοντας το προσωπικό κλειδί για να επιτεθεί στο blockchain. Επίσης, δεν παρέχει προστασία υπολειπόμενης πληροφόρησης, καθώς δεν ελέγχει την πλήρη απομάκρυνση του ηλεκτρονικού πορτοφολιού. Η περίπτωση περιστατικών ασφαλείας [174] δεν παρέχει διαθεσιμότητα, δεδομένου ότι η υπηρεσία δεν είναι διαθέσιμη λόγω μόλυνσης από κακόβουλο λογισμικό και δεν παρέχει προστασία υπολειπόμενης πληροφόρησης, καθώς δεν επαληθεύει την πλήρη απομάκρυνση του ηλεκτρονικού πορτοφολιού. Η περίπτωση επίθεσης 51% [175] μπορεί να έχει προβλήματα παραβίασης της ακεραιότητας του βιβλίου συναλλαγών και μη διαθεσιμότητα μετά από επίθεση που μεταβάλλει το 51% του βιβλίου συναλλαγών. Επιπλέον, δεν παρέχει προστασία υπολειπόμενης πληροφόρησης, καθώς δεν ελέγχει την πλήρη απομάκρυνση του ηλεκτρονικού πορτοφολιού. Η βελτιωμένη περίπτωση blockchain [176] ούτε εξασφαλίζει ακεραιότητα ούτε παρέχει διαθεσιμότητα, καθώς η ευπάθεια της διπλής συναλλαγής παραμένει. Επιπλέον, δεν παρέχει προστασία υπολειπόμενης πληροφόρησης, καθώς δεν ελέγχει την πλήρη απομάκρυνση του ηλεκτρονικού πορτοφολιού. Η ασφαλής λύση blockchain βελτιώνει την ασφάλεια παρέχοντας προστασία υπολειπόμενης πληροφορίας, καθώς κρυπτογραφεί τα δεδομένα χρησιμοποιώντας ένα δημόσιο κλειδί και επαληθεύει την πλήρη απομάκρυνση του ηλεκτρονικού πορτοφολιού.

6. Case studies στο Blockchain.

Μερικοί από τους τομείς στους οποίους εφαρμόζεται η τεχνολογία blockchain είναι η Υγεία, η οικονομία, η κινητή τηλεφωνία, η αυτοκινητοβιομηχανία, η άμυνα, το IoT και αλλά και πολλοί περισσότεροι ακόμα.

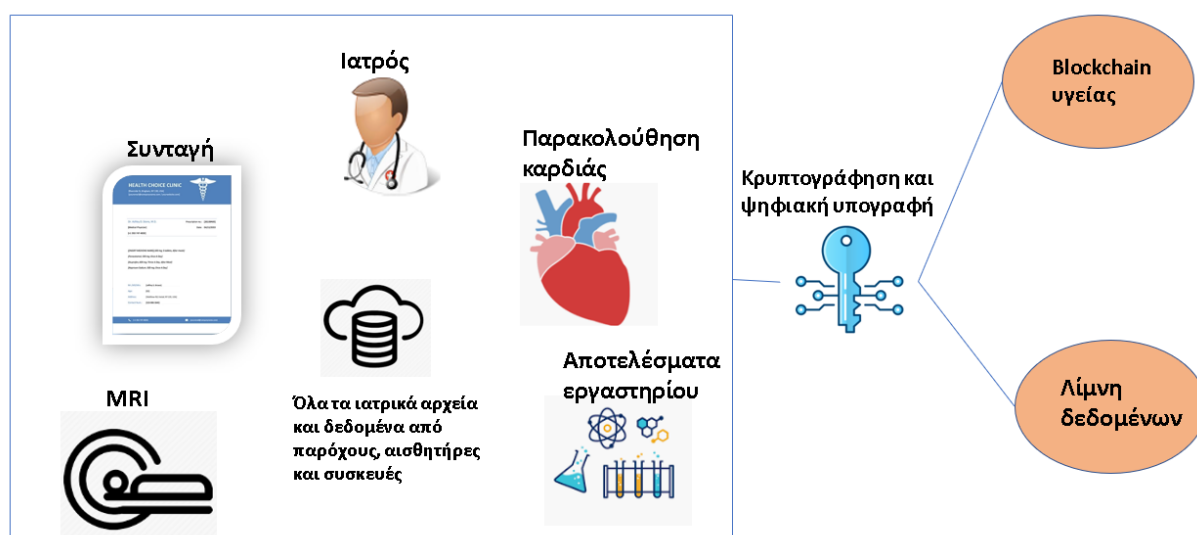


Πίνακας 28. Blockchain Case Studies

6.1. Blockchain στην υγεία .

Το Blockchain στον τομέα της υγειονομικής περίθαλψης πρέπει να είναι δημόσιο και θα πρέπει να είναι κλιμακωτό, ασφαλές και να διατηρεί το απόρρητο των δεδομένων. Τα τμήματα της υγειονομικής περίθαλψης περιλαμβάνουν κυρίως αρχεία υγείας, έγγραφα και εικόνες. [177] αναλύει λεπτομερώς το blockchain για την υγειονομική περίθαλψη και έδειξε ότι τα δεδομένα αντιμετωπίζουν τις συνέπειες αποθήκευσης και τους περιορισμούς απόδοσης. Εάν τα δεδομένα αποθηκεύονται σε μπλοκ αλυσίδες με μοντελοποίηση bithoin, κάθε χρήστης θα περιέχει ένα αντίγραφο της καταγραφής υγείας κάθε ατόμου στο δίκτυο. Αυτό δεν είναι μια ιδανική μέθοδος αποθήκευσης και είναι εντάσεως εύρους ζώνης. Δημιουργεί μια σπατάλη των πόρων του δικτύου και των δεδομένων σχετικά με τη διακίνηση δεδομένων. Για να εφαρμόσουμε τη χρήση μπλοκ αλυσίδων στον τομέα της υγειονομικής περίθαλψης, πρέπει να δημιουργήσουμε

έναν διαχειριστή ελέγχου πρόσβασης για τη διαχείριση και αποθήκευση δεδομένων. Το πραγματικό blockchain περιέχει μόνο ένα ευρετήριο ή μια λίστα με όλα τα δεδομένα των χρηστών. Λειτουργεί σαν κατάλογος μεταδεδωμένων σχετικά με ασθενείς και τοποθεσίες και τα δεδομένα αποθηκεύονται για να έχουν πρόσβαση σε εξουσιοδοτημένο χρήστη. Για να βελτιωθεί η αποτελεσματικότητα της πρόσβασης στα δεδομένα, τα δεδομένα κρυπτογραφούνται, χρονοσήμαντα και ανακτώνται με τη βοήθεια ενός μοναδικού αναγνωριστικού. Όλα τα δεδομένα που σχετίζονται με την υγειονομική περίθαλψη αποθηκεύονται σε αποθήκες δεδομένων blockchain που ονομάζονται λίμνες δεδομένων. Οι λίμνες δεδομένων είναι εξαιρετικά πολύτιμες για την έρευνα και την ανάλυση δεδομένου ότι μπορούν να αποθηκεύσουν οποιαδήποτε μορφή δεδομένων. Οι λίμνες δεδομένων υποστηρίζουν επίσης τεχνολογίες όπως η διαλογική αναζήτηση, η εξόρυξη και η ανάλυση κειμένων και η εκμάθηση μηχανών. Ο παρακάτω πίνακας παρουσιάζει μια συνολική εικόνα των συναλλαγών με blockchain στον τομέα της υγειονομικής περίθαλψης.



Πίνακας 29. Blockchain στην Υγεία

Για να διατηρηθεί η ιδιωτικότητα, τα δεδομένα σε λίμνες δεδομένων κρυπτογραφούνται και υπογράφονται ψηφιακά και μπορούν να αποκτήσουν πρόσβαση μόνο από πιστοποιημένους χρήστες. Είναι επίσης ψηφιακά υπογεγραμμένα και κρυπτογραφημένα πριν από την τοποθέτηση νέου ρεκόρ στη λίμνη δεδομένων. Κάθε χρήστης έχει πλήρη πρόσβαση στα δεδομένα του και μπορεί να ελέγχει τον τρόπο με τον οποίο μοιράζονται τα δεδομένα του. Ένας δείκτης διατηρείται στην πρόσβαση και ενημέρωση κάθε εγγραφής με τη βοήθεια του μοναδικού αναγνωριστικού των χρηστών. Ο χρήστης μπορεί να εκχωρήσει δικαιώματα πρόσβασης σε άλλους χρήστες και να εξουσιοδοτήσει επιλεκτικά τους χρήστες να ενημερώσουν τα δεδομένα του / της στο blockchain.

Η τεχνολογία Blockchain προσφέρει πολλά πλεονεκτήματα για τον τομέα της υγειονομικής περίθαλψης, καθώς περιλαμβάνει στοιχεία όπως ανοιχτού κώδικα, υλικό βασικών προϊόντων και ανοιχτά API. Αυτά τα στοιχεία συμβάλλουν στη γρήγορη και εύκολη διαλειτουργικότητα μεταξύ συστημάτων και μπορούν να κλιμακωθούν σε μεγαλύτερους όγκους δεδομένων και χρηστών. Το Blockchain επιτρέπει στους

χρήστες να έχουν πρόσβαση στην κοινή πηγή δεδομένων για την επίτευξη έγκαιρων, ακριβών και ολοκληρωμένων δεδομένων περίθαλψης. Επιπλέον, το υλικό βασικών προϊόντων του blockchain παρέχει υπολογισμό χαμηλού κόστους και ασχολήθηκε με τις προκλήσεις διαλειτουργικότητας στον τομέα της υγειονομικής περίθαλψης. Ένα άλλο πλεονέκτημα της κατανεμημένης αρχιτεκτονικής blockchains είναι η ενσωματωμένη ανοχή σφάλματος και η δυνατότητα αποκατάστασης καταστροφών. Δεδομένου ότι τα δεδομένα διαδίδονται σε πολλούς διακομιστές, δεν υπάρχει ένα μόνο σημείο αποτυχίας.

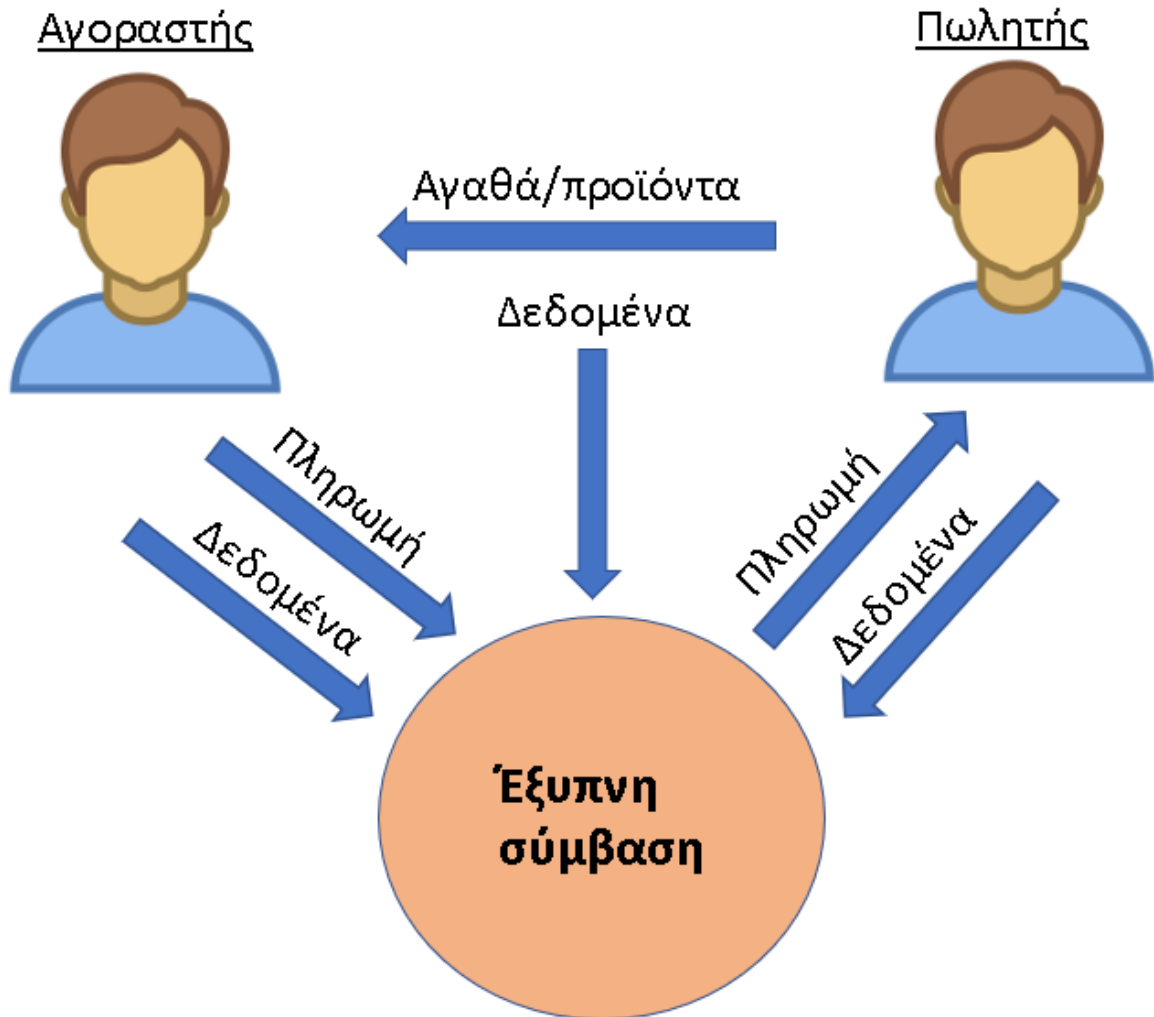
6.2. Blockchain στην οικονομία.

Το Blockchain αναπτύχθηκε αρχικά ως η ραχοκοκαλιά του Bitcoin, ένα δημοφιλές αποκεντρωμένο ψηφιακό νόμισμα. Το blockchain από αργά χρησιμοποιείται σε πολλά ψηφιακά νομίσματα όπως το Altercoin, το Peercoin, το Ethereum [178], το Karma [179], το Hashcash [180] και το BinaryCoin. Τα περισσότερα ψηφιακά νομίσματα χρησιμοποιούν τη δομή blockchain ως βάση, παρόλο που χρησιμοποιούν διαφορετικούς αλγόριθμους συναίνεσης για επαλήθευση και επικύρωση των μπλοκ. [181] αναλύει λεπτομερώς το νόμισμα bitcoin και το blockchain στη χρηματοδότηση και επεσήμανε ότι το μεγαλύτερο μέρος του blockchain στον τομέα της χρηματοδότησης είναι η χρήση έξυπνων συμβάσεων. Ο παρακάτω πίνακας παρουσιάζει μια συνήθη οικονομική συναλλαγή χρησιμοποιώντας έξυπνες συμβάσεις. Σε αυτό το έγγραφο, συζητούμε περαιτέρω τις ανησυχίες που σχετίζονται με την ασφάλεια και την προστασία της ιδιωτικής ζωής, ενώ χρησιμοποιούν μπλοκ αλυσίδες στον οικονομικό τομέα.

Οι κοινές ανησυχίες που σχετίζονται με την ασφάλεια οποιουδήποτε οργανισμού, ενώ χρησιμοποιούν blockchain, διασφαλίζουν την εξουσιοδότηση των μερών να έχουν πρόσβαση σε σωστά και κατάλληλα δεδομένα. Η εγγύηση της ασφάλειας των δεδομένων και της πρόσβασης σε δεδομένα στο blockchain δίκτυο είναι θεμελιώδης. Η απόκτηση πρόσβασης στο δίκτυο blockchain και τα δεδομένα μπορούν να ενισχύσουν την ανάγκη εφαρμογής ελέγχου ταυτότητας και ελέγχου εξουσιοδότησης. Το blockchain επιτρέπει την πλήρη κρυπτογράφηση των μπλοκ δεδομένων και εξασφαλίζει αποτελεσματικά την εμπιστευτικότητα. Η κρυπτογράφηση δεδομένων μπορεί να προσφέρει στην οργάνωση επίπεδα προστασίας από το απόρρητο των δεδομένων και τον έλεγχο πρόσβασης δεδομένων σε ένα δίκτυο blockchain. Η χρήση ιδιωτικών και δημόσιων κλειδιών σε συνδυασμό με την κρυπτογράφηση δεδομένων παρέχει στο δίκτυο και τον οργανισμό υψηλότερο επίπεδο ασφάλειας. Μια πολύ σημαντική πτυχή των συστημάτων πληροφοριών είναι η διατήρηση της συνέπειας και της ακεραιότητας των δεδομένων. Το Blockchain διασφαλίζει την ακεραιότητα των δεδομένων βάσει των βασικών χαρακτηριστικών της αμετάβλητης και ανιχνευσιμότητας. Η συγχώνευση της διαδοχικής τεχνικής κατακερματισμού και της κρυπτογράφησης το καθιστά εξαιρετικά δύσκολο για κάθε χρήστη ή κόμβους του δικτύου να παραβιάζουν τα δεδομένα σε blockchain.

Το δικαίωμα να ξεχαστεί εξασφαλίζει την ιδιωτικότητα του χρήστη σε οποιοδήποτε δίκτυο, το οποίο είναι ιδιαίτερα σημαντικό όσον αφορά την αναλλοίωσή του. Η μεγαλύτερη πρόκληση είναι η διασφάλιση της εφαρμογής αυτού του δικαιώματος σε μια τεχνολογία που βασίζεται στην αρχή της μη διαγραφής οποιωνδήποτε δεδομένων. Προφανώς, το blockchain παρέχει πολλές λύσεις. Ένας από αυτούς είναι η κρυπτογράφηση προσωπικών πληροφοριών στο δίκτυο. Σε περίπτωση που ξεχνάμε τα κλειδιά, τα δεδομένα είναι απρόσιτα και μπορούν να διασφαλίσουν την ασφάλεια. Μια άλλη επιλογή είναι να επικεντρωθεί στην αξία του blockchain για να προσφέρει μη αναστρέψιμα γεγονότα γράφοντας το hash των συναλλαγών σε αυτό, ενώ τα δεδομένα

συναλλαγής αποθηκεύονται εκτός του συστήματος. Η ανιχνευσιμότητα είναι η δυνατότητα παρακολούθησης του χρόνου και των πληροφοριών σχετικά με μια συναλλαγή σε blockchain καθώς κάθε συναλλαγή υπογράφεται ψηφιακά και χρονοσήμανση. Αυτή η λειτουργία βοηθάει στην μη αποθάρρυνση δεδομένων που εγγυάται την αναπαραγωγή των δεδομένων. Ως εκ τούτου, αυξάνει την αξιοπιστία του blockchain.

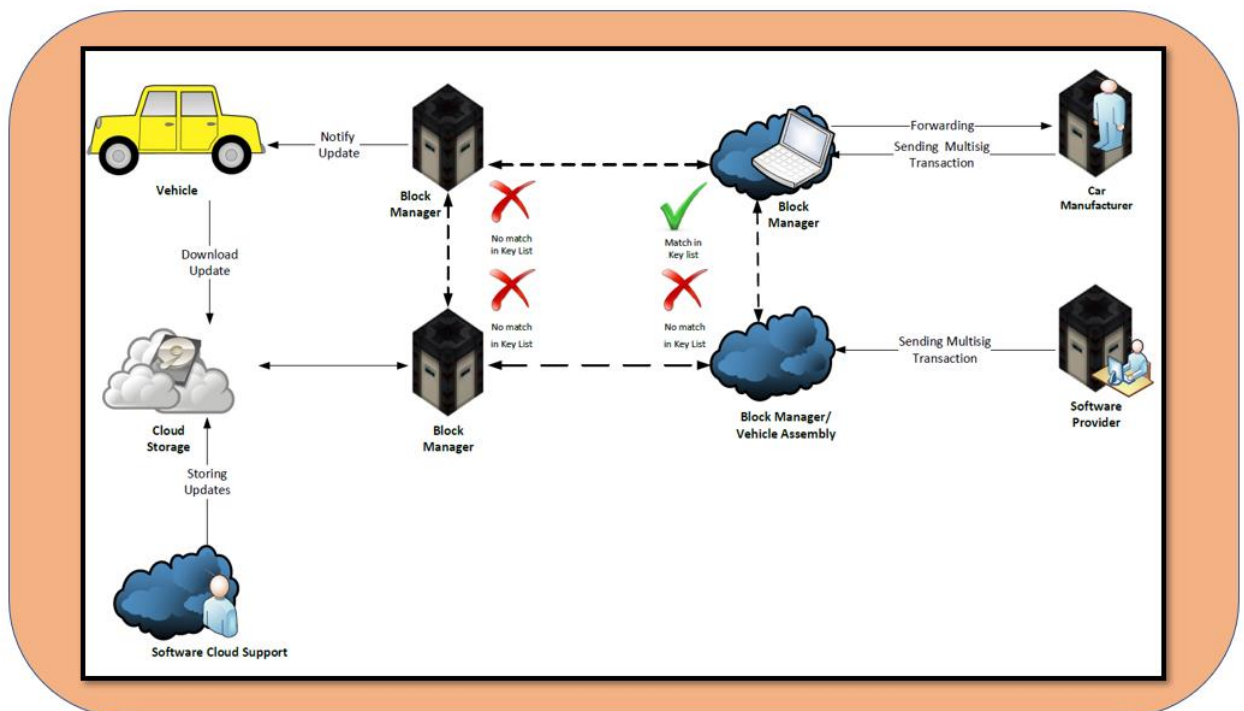


Πίνακας 30. Blockchain στην Οικονομία

6.3. Blockchain στην αυτοκινητοβιομηχανία.

Τα σύγχρονα οχήματα συνδέονται ολόένα και περισσότερο με εφαρμογές στο διαδίκτυο ή μέσω δικτύου και ως εκ τούτου παρέχουν μια εξαιρετική βάση για τη χρήση της τεχνολογίας blockchain. Όπως αναφέρθηκε στην [\[182\]](#), [\[183\]](#), [\[184\]](#), οι αρχιτεκτονικές ασφάλειας της αυτοκινητοβιομηχανίας πρέπει να αντιμετωπίσουν μερικές απαιτήσεις για να καλυφθούν οι μελλοντικές ανάγκες για έξυπνα οχήματα. Οι αρχιτεκτονικές ασφάλειας της αυτοκινητοβιομηχανίας πρέπει να αντιμετωπίσουν τις προκλήσεις για την ικανοποίηση των αναγκών των μελλοντικών υπηρεσιών των έξυπνων οχημάτων από τις προοπτικές που απαριθμούνται ως εξής:

- **Επεκτασιμότητα.** Η αρχιτεκτονική είναι απαραίτητη, καθώς το οικοσύστημα των οχημάτων περιλαμβάνει πολυάριθμα οχήματα και κάθε ράφτες με άφθονες ηλεκτρονικές μονάδες ελέγχου.
- **Ασφάλεια.** Μια ασφαλής αρχιτεκτονική ενός έξυπνου οχήματος θα πρέπει να προστατεύει τον χρήστη από απειλές που συνεπάγονται παραβιάσεις ασφαλείας που οφείλονται σε δυσλειτουργία καθώς και από πολλές αυτόνομες λειτουργίες οδήγησης.
- **Κεντριοποίηση.** Μια κεντρική αρχιτεκτονική οδηγεί σε ένα σημείο αποτυχίας, με αποτέλεσμα να διακυβεύεται η ασφάλεια του συστήματος. Ως εκ τούτου, η αποκεντρωμένη αρχιτεκτονική προτιμάται περισσότερο λόγω της χαμηλής κλίμακας ικανότητας της κεντρικής αρχιτεκτονικής.
- **Συντήρηση.** Η αρχιτεκτονική της αυτοκινητοβιομηχανίας πρέπει να αντιμετωπίσει τη δυνατότητα συντήρησης λογισμικού και υλικού για καθορισμένη χρονική περίοδο και την επιλογή επέκτασης για τη συντήρηση ενός οχήματος.



Πίνακας 31. Blockchain στην Αυτοκινητοβιομηχανία

Οι ενημερώσεις ασύρματου απομακρυσμένου λογισμικού (WRSU) είναι ένα από τα πιο δύσκολα και κρίσιμα ζητήματα ασφάλειας στην αυτοκινητοβιομηχανία. Το WRSU πρέπει να αναβαθμίσει τα σφάλματα στερέωσης στη λειτουργικότητα των ηλεκτρονικών μονάδων ελέγχου κάθε φορά που απαιτείται εγκατάσταση εγκατάστασης αναβάθμισης λογισμικού. Με αυτόν τον τρόπο, η WRSU υποστηρίζει τον πλήρη κύκλο ζωής ενός οχήματος, καθώς μπορεί να εισέλθει στον κύκλο ζωής του οχήματος ήδη από την ανάπτυξη και τη συναρμολόγηση του οχήματος έως τη συντήρηση και πολλά άλλα. Σήμερα, η κύρια προσπάθεια γίνεται στην αποδοτικότητα και την ασφάλεια της αρχιτεκτονικής WRSU για καλύτερη διαχείριση των δεδομένων




των οχημάτων. Ο παραπάνω πίνακας περιγράφει ολόκληρη τη διαδικασία ενημέρωσης λογισμικού που βασίζεται στην αρχιτεκτονική WRSU. Ο πάροχος λογισμικού παράγει μια πιο πρόσφατη έκδοση ή αναβάθμιση λογισμικού και στη συνέχεια το αποθηκεύει στο cloud που είναι διαθέσιμο σε όλους τους κόμβους επικάλυσης. Στη συνέχεια δημιουργεί μια συναλλαγή multisig και την κρυπτογραφεί με το ιδιωτικό κλειδί και την ψηφιακή υπογραφή. Το δημόσιο κλειδί του κατασκευαστή αυτοκινήτων και των διαχειριστών μπλοκ χρησιμοποιείται για την προώθηση των συναλλαγών με μια λίστα με κλειδιά, παρέχοντας έτσι την ακεραιότητα των δεδομένων. Στη συνέχεια, η συναλλαγή αποστέλλεται σε επικάλυση, καθώς η τρέχουσα συναλλαγή που περιέχει ένα μόνο κλειδί δεν μπορεί να θεωρηθεί έγκυρη από όλους τους διαχειριστές ομάδων. Οι διαχειριστές μπλοκ εκπέμπουν μόνο τη συναλλαγή στο δίκτυο. Μόλις ληφθεί η συναλλαγή από τον διαχειριστή ομάδας του συμπλέγματος που περιέχει τον σχετικό κατασκευαστή αυτοκινήτου, επαληθεύει την έκδοση λογισμικού και αποστέλλει μια επιβεβαίωση στον διαχειριστή μπλοκ. Η συναλλαγή μεταδίδεται σε όλους τους διαχειριστές μπλοκ και επαληθεύεται με το δημόσιο κλειδί του παρόχου λογισμικού και του κατασκευαστή αυτοκινήτων. Το έξυπνο όχημα λαμβάνει τη συναλλαγή από τον διαχειριστή ομάδας και τον επαληθεύει. Το όχημα στη συνέχεια κατεβάζει το λογισμικό απευθείας από την αποθήκευση σύννεφο χρησιμοποιώντας τις παραμέτρους ελέγχου ταυτότητας.

Επιπλέον, όπως αναλύθηκε στο [185], η δομή του blockchain μπορεί να χρησιμοποιηθεί με πολλούς τρόπους στην αυτοκινητοβιομηχανία, όπως οι υπηρεσίες ασφάλισης, ηλεκτρικής και έξυπνης χρέωσης, η μίσθωση αυτοκινήτων και οι υπηρεσίες κοινής χρήσης.

6.4. Blockchain στο Internet of Things.

Το IoT ορίζεται ως ένα σύστημα διασυνδεδεμένων υπολογιστικών συσκευών, μηχανικών και ψηφιακών μηχανών, αντικειμένων, ζώων ή προσώπων που παρέχονται με μοναδικά αναγνωριστικά στοιχεία και τη δυνατότητα μεταφοράς δεδομένων μέσω δικτύου χωρίς να απαιτούνται ανθρώπινα προς ανθρώπινα ή ανθρωπογενή άτομα, αλληλεπίδραση υπολογιστή [186], [187]. Οι πιο συνηθισμένες Ηνωμένες Πολιτείες, δηλαδή η blockchain, είναι η αποθήκευση δεδομένων και η πρόσβαση σε IoT. Ο χρήστης πρέπει να έχει τη δυνατότητα πρόσβασης σε δεδομένα από απόσταση από οποιαδήποτε τοποθεσία με ασφαλή τρόπο και να διασφαλίζει την ιδιωτικότητα των δεδομένων που είναι αποθηκευμένα στο δίκτυο. Κατά τη δημιουργία του λογαριασμού του, ο χρήστης καθορίζει δικαιώματα και απαιτούμενα στοιχεία ελέγχου για τον λογαριασμό του. Αφού ελέγξει τα δικαιώματα και εξάγει τον προηγούμενο αριθμό μπλοκ και την τιμή κατακερματισμού, ο χρήστης δημιουργεί ένα τυχαίο μοναδικό αναγνωριστικό και στέλνει δεδομένα στην αποθήκευση χρησιμοποιώντας αυτό το id. Η εγκυρότητα της συναλλαγής επαληθεύεται και επιβεβαιώνεται η διαθεσιμότητα της αποθήκευσης. Ο πάροχος υπηρεσιών για μια εφαρμογή μπορεί να χρειαστεί να έχει πρόσβαση στα δεδομένα που είναι αποθηκευμένα για μια συγκεκριμένη περίοδο ή εποχή χρόνου. Οι χρήστες, όπως οι πάροχοι υπηρεσιών, δημιουργούν μια συναλλαγή πολλαπλών εντολών που υπογράφονται από τον πάροχο υπηρεσιών και τον αιτούντα υπηρεσία. Οι μεταβιβάσεις αποστέλλονται στο κεφάλαιο συμπλέγματος αυτού του δικτύου. Στη συνέχεια, η κεφαλή συμπλέγματος επαληθεύει το αίτημα ως συναλλαγή είτε μεταδίδοντας το στο δικό του σύμπλεγμα είτε σε άλλες επικεφαλίδες συμπλέγματος. Για να διασφαλιστεί η ιδιωτικότητα, ο χρήστης χρησιμοποιεί μεθόδους όπως η ασφαλής απάντηση, η εισαγωγή θορύβου για την προστασία των δεδομένων. Η έξοδος μιας συναλλαγής πολλαπλών εντολών μπορεί να οριστεί σε 1 ή 0 για να υποδείξει αν ο χρήστης έχει πρόσβαση στα δεδομένα ή όχι αντίστοιχα. Αυτές οι

συναλλαγές πολλαπλών συναλλαγών μπορούν να θεωρηθούν ως απόδειξη ότι η ημερομηνία αποστέλλονται από τον χρήστη και μπορούν να χρησιμοποιηθούν για την ενημέρωση άλλων χρηστών για παράπτωμα, αν υπάρχουν. Ο παρακάτω πίνακας παρουσιάζει τα κυριότερα πλεονεκτήματα της χρήσης μπλοκ αλυσίδων σε IoT.

Χτίσιμο εμπιστοσύνης	Μείωση κόστους	Επιτάχυνση συναλλαγών
		
1. Χτίσιμο εμπιστοσύνης μεταξύ μελών και συσκευών	1. Αφαιρεί τον μεσάζοντα	1. Μειώνει το χρόνο διακανονισμών
2. Μείωση κινδύνων αλλοίωσης	2. Αφαιρεί τα γενικά έξοδα	

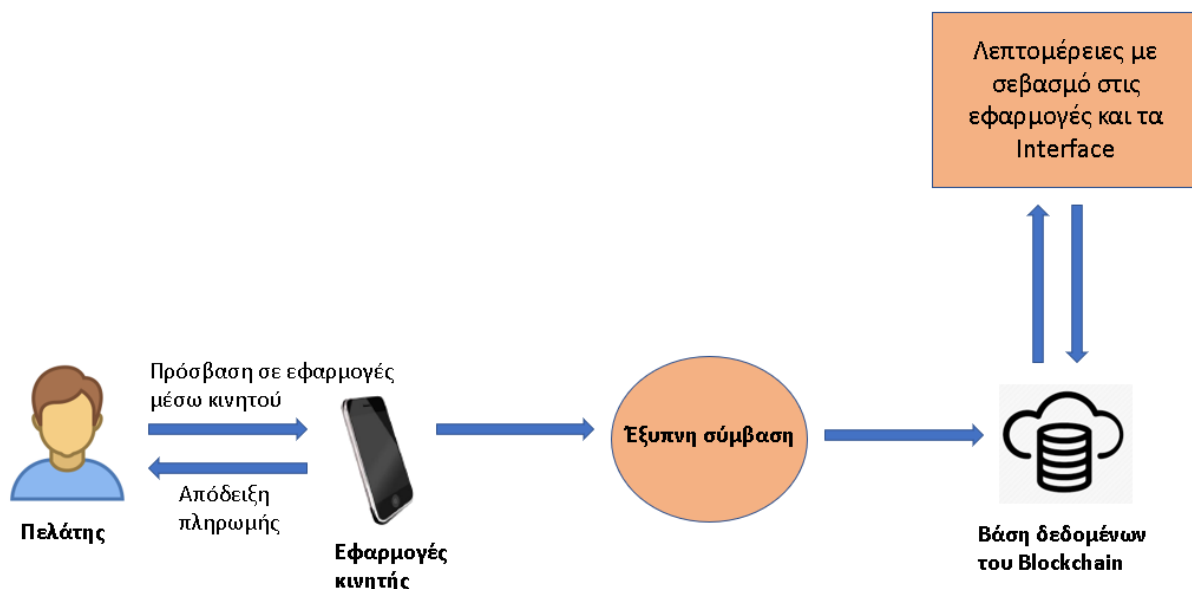
Πίνακας 32. Blockchain στην αυτοκινητοβιομηχανία

Δεδομένου ότι η πλειονότητα των συσκευών προστίθενται σε IoT κάθε μέρα, οι οργανισμοί εντοπίζουν τις δυνατότητες του IoT και του blockchain για τη βελτίωση των επιχειρηματικών διαδικασιών και την επιτάχυνση της ανάπτυξης. Η επείγουσα ανάγκη ασφαλούς μοντέλου IoT για την εκτέλεση ακόμη και κοινών καθηκόντων ανίχνευσης, επεξεργασίας, αποθήκευσης δεδομένων και επικοινωνίας αυξάνεται επίσης. Το δημόσιο blockchain παρέχει ένα μεγάλο πλεονέκτημα σε αυτά τα προβλήματα, καθώς όλοι συμμετέχουν και οι πληροφορίες προστατεύονται από ένα ιδιωτικό κλειδί. Χωρίς ενιαία κεντρική αρχή που τον ελέγχει, το μοντέλο που βασίζεται στο blockchain προϋποθέτει μεγάλη εμπιστοσύνη. Η μεγαλύτερη πρόκληση της εφαρμογής blockchain στο IoT είναι η δυνατότητα κλιμάκωσης, καθώς ο χρόνος απόκρισης σε αιτήματα αυξάνεται καθώς αυξάνεται ο αριθμός των υπολογιστικών συσκευών.

6.5. Blockchain σε κινητές εφαρμογές.

Μια εφαρμογή για κινητά μπορεί να περιγραφεί ως εφαρμογή λογισμικού που έχει σχεδιαστεί ειδικά για κινητές συσκευές όπως smartphones και tablet. Το Blockchain υποστηρίζει την υπηρεσία δεδομένων peer-to-peer σε κινητές εφαρμογές, όπως αναφέρεται στα [188] και [189] σχετικά με τη μεταφορά αρχείων από ομότιμους χρήστες και την άμεση πληρωμή. Το [190] αναφέρει επίσης ότι ο πρώτος ανθρακωρύχος που επιλύει επιτυχώς το παζλ για να επικυρώσει μια συναλλαγή χρησιμοποιώντας οποιαδήποτε από τις συναινετικές τεχνικές καθορίζει μια ανταμοιβή. Αυτό ονομάζεται παιχνίδι ταχύτητας ανάμεσα στους ανθρακωρύχους και το παζλ δεν μπορεί να αντιμετωπιστεί χρησιμοποιώντας κινητές συσκευές. Για να επιτύχουμε την επεξεργασία κινητών μπλοκ αλυσίδων μπορούμε να χρησιμοποιήσουμε την ιδέα της υπολογιστικής ακμής. Θεωρούμε ότι μια ομάδα N χρηστών κινητής εφαρμογής που αντιπροσωπεύονται ως $N = 1, 2, \dots, N$. Κάθε χρήστης ή κόμβος προσπαθεί να λύσει το παζλ χρησιμοποιώντας την εξουσία κατακερματισμού και την υπολογιστική ισχύ για μια ανταμοιβή που συνδέεται με τη λύση. Οι χρήστες κινητών χρησιμοποιούν την εφαρμογή blockchain για κινητά με τη βοήθεια κόμβων υπολογιστών άκρη για τους

ανθρακωρύχους που αναπτύσσονται με τους παρόχους υπηρεσιών υπολογιστικής ακριβείας. Αυτή η υπηρεσία παρέχει υπολογιστικούς πόρους σε χρήστες κινητής τηλεφωνίας, ο οποίος τιμολογείται από τον πάροχο υπηρεσιών. Ο πίνακας 33 απεικονίζει τη χρήση του blockchain σε κινητές εφαρμογές.



Πίνακας 33. Blockchain σε Κινητές Εφαρμογές

Το Blockchain μπορεί να προσθέσει τεράστια αξία στις στρατηγικές ασφαλείας που αφορούν τις εφαρμογές για κινητά. Είναι πιο ασφαλές να χρησιμοποιείται σε διαφορετικές εφαρμογές που ασχολούνται ειδικά με ευαίσθητα δεδομένα, καθώς το blockchain δεν έχει κανένα σημείο αποτυχίας. Το Blockchain είναι ιδανικό για χρήση όταν υπάρχει αυστηρή απαίτηση για έλεγχο ταυτότητας για την προστασία δεδομένων. Η κύρια χρήση εφαρμογών που βασίζονται σε κινητά συστήματα προέκυψε κατά την πρόσβαση στα ψηφιακά πορτοφόλια. Το μεγαλύτερο μέρος της εφαρμογής για κινητά επιτρέπει στον χρήστη να πληρώνει χρησιμοποιώντας ψηφιακά πορτοφόλια ή σε περιπτώσεις όπως bitcoin επιτρέπει στους χρήστες να πραγματοποιούν συναλλαγές μέσω διαδικτύου μέσω κινητών συσκευών χρησιμοποιώντας τις υπηρεσίες ηλεκτρονικών υπολογιστών που παρέχονται στο δίκτυο. Επομένως, η χρήση κινητών εφαρμογών καθιστά την εφαρμογή φορητή και πιο αποδεκτή.

6.6. Blockchain στην άμυνα.

Για να ξεπεραστούν τα περιβάλλοντα με υψηλή συμφόρηση στο μέλλον, η υπεράσπιση πρέπει να εξαρτάται από τα συστήματα με δυνατότητα πρόσβασης στον κυβερνοχώρο και τα δεδομένα που περιέχουν.

Η σημερινή άμυνα στον κυβερνοχώρο φαίνεται να είναι παραπαίουσα και οι αυξανόμενες βελτιώσεις υπολείπονται της αυξανόμενης απειλής του κυβερνοχώρου. Η τεχνολογία Blockchain ανατρέπει το πρότυπο ασφαλείας του κυβερνοχώρου λόγω της αβέβαιης, διαφανούς και ανεκτικής σφάλματός του, μειώνοντας έτσι την πιθανότητα συμβιβασμού των δεδομένων. Το [\[191\]](#) αναλύει λεπτομερώς την εφαρμογή

της τεχνολογίας blockchain στην εθνική άμυνα. Τα βασικά στοιχεία στη λειτουργία του blockchain, όπως ο ασφαλής κατακερματισμός, η επανασυνδεδεμένη δομή δεδομένων και ο μηχανισμός συναίνεσης, διαδραματίζουν σημαντικό ρόλο καθώς αποδίδουν τον παράγοντα ασφαλείας των μπλοκ αλυσίδων. Δεδομένου ότι οποιοσδήποτε εξουσιοδοτημένος χρήστης στο δίκτυο μπορεί να έχει πρόσβαση στα δεδομένα του δικτύου, ένα σημαντικό ζήτημα για την ασφάλεια blockchain είναι η εμπιστευτικότητα των δεδομένων. Αυτό μπορεί να ξεπεραστεί με την κρυπτογράφηση δεδομένων και τη διατήρηση ενός ελέγχου πρόσβασης με την αποθήκευση σε μπλοκ αλυσίδες. Το blockchain μπορεί να χρησιμοποιηθεί στην αμυντική εφαρμογή ενεργώντας με το λειτουργικό ως εξής:

- **Κυβερνο-άμυνα.** Πρόκειται για μια εφαρμογή χαμηλού κόστους, υψηλής απόδοσης του blockchain. Πρώτον, το blockchain διασφαλίζει ότι όλα τα ψηφιακά συμβάντα γίνονται ευρέως αντιληπτά με τη μετάδοσή τους σε όλους τους άλλους κόμβους του δικτύου και στη συνέχεια χρησιμοποιεί διαφορετικούς αλγόριθμους συναίνεσης για επικύρωση και επαλήθευση. Μόλις εξασφαλιστούν τα δεδομένα που φέρουν χρονική σήμανση και αποθηκεύονται, δεν είναι δυνατή η επεξεργασία τους. Σε περίπτωση που τα δεδομένα αλλάξουν ή ενημερωθούν, είναι και πάλι χρονικά επισημασμένα και διατηρείται το ημερολόγιο. Τα μοντέρνα στοιχεία όπλων και εξαρτημάτων μπορούν να απεικονιστούν, να χυθούν και να ασφαλιστούν στη βάση δεδομένων και να παρακολουθούνται συνεχώς χρησιμοποιώντας μπλοκ αλυσίδες. Αυτό συζητείται λεπτομερώς στο [\[192\]](#).
- **Διαχείριση αλυσίδας εφοδιασμού.** Η αυξανόμενη ανησυχία σχετικά με την διαχείριση της αλυσίδας εφοδιασμού στην άμυνα οδηγεί στην ανάγκη μιας τεχνολογίας για τον καθορισμό της προέλευσης και της ανιχνευσιμότητας του ιδιοκτήτη. Το Blockchain παρέχει μια λύση σε αυτά τα θέματα όπως συζητείται στο [\[193\]](#).
- **Ανθεκτικές επικοινωνίες.** Στα ιδιαίτερα αμφισβητούμενα περιβάλλοντα, το blockchain παρέχει ελαστική επικοινωνία εξαιτίας της ικανότητάς του να παράγει, να προστατεύει και να μοιράζεται δεδομένα με αδιαπέραστο τρόπο. Η ανθεκτικότητα που προσφέρει το blockchain συζητείται στο [\[194\]](#). Όλα αυτά τα χαρακτηριστικά εξασφαλίζουν την αξιοπιστία της επαληθευμένης μετάδοσης δεδομένων σε όλο τον κόσμο, παρά τις κακόβουλες επιθέσεις κατά των διαύλων επικοινωνίας, των κόμβων ή του ίδιου του μπλοκ.

7. Προκλήσεις και δυνατότητες

Η τεχνολογία blockchain αντιμετωπίζει μερικές μελλοντικές ευκαιρίες καθώς και προκλήσεις. Αν και σημαντικό, οι προκλήσεις μπορούν να ξεπεραστούν με την ωριμότητα και την ενίσχυση της τεχνολογίας στο μέλλον. Αυτό θα οδηγήσει σε πληθώρα μελλοντικών ευκαιριών για

μπλοκχεντ που θα εφαρμοστούν και θα γίνουν αποδεκτές. Οι προκλήσεις και οι ευκαιρίες θα συζητηθούν λεπτομερώς σε αυτό το τμήμα.

7.1. Προκλήσεις.

Μια πρόκληση μπορεί να οριστεί ως μια σιωπηρή απαίτηση για απόδειξη. Ορισμένες από τις σημαντικότερες προκλήσεις που αντιμετωπίζει σήμερα η τεχνολογία blockchain παρατίθενται παρακάτω.

7.1.1. Ευελιξία.

Με όλο και αυξανόμενο όγκο χρήσης μπλοκ αλυσίδων και την αύξηση του πλήθους των συναλλαγών καθημερινά, το blockchain γίνεται σταδιακά κολοσσιαίο σε μέγεθος. Όλες οι συναλλαγές αποθηκεύονται σε κάθε κόμβο για να επικυρωθούν. Η πηγή της τρέχουσας συναλλαγής πρέπει να επικυρωθεί πρυνά πριν την επικύρωση της συναλλαγής. Το περιορισμένο μέγεθος μπλοκ και η χρονική παρεμβολή που χρησιμοποιείται για την παραγωγή ενός νέου μπλοκ παίζουν επίσης ρόλο στην μη εκπλήρωση της απαίτησης επεξεργασίας εκατομμυρίων συναλλαγών ταυτόχρονα σε σενάρια σε πραγματικό χρόνο. Εν τω μεταξύ, το μέγεθος των μπλοκ σε blockchain ενδέχεται να δημιουργήσει πρόβλημα καθυστέρησης της συναλλαγής σε περίπτωση μικρών συναλλαγών, καθώς οι ανθρακωρύχοι θα προτιμούσαν να επικυρώσουν συναλλαγές με μεγαλύτερες συναλλαγματικές προμήθειες. Όπως αναφέρθηκε στην [\[195\]](#), οι προτεινόμενες λύσεις στο ζήτημα της επεκτασιμότητας των μπλοκ αλυσίδων μπορούν να κατηγοριοποιηθούν σε δύο κατηγορίες: βελτιστοποίηση αποθήκευσης και επανασχεδιασμός μπλοκ αλυσίδων. Αυτή η βάση δεδομένων διατηρεί το υπόλοιπο των μη κενών διευθύνσεων. Ένας πελάτης ελαφρού βάρους θα μπορούσε επίσης να χρησιμοποιηθεί ως εναλλακτικό για να διορθώσει το ζήτημα της επεκτασιμότητας. Κατά τον επανασχεδιασμό, το blockchain μπορεί να κατακερματιστεί σε ένα μπλοκ κλειδιού και ένα μικρό μπλοκ, με το κλειδί μπλοκ να είναι υπεύθυνο για τις εκλογές leader, ενώ το micro block είναι υπεύθυνο για την αποθήκευση των συναλλαγών.

7.1.2. Διαρροή απορρήτου.

Το blockchain είναι ιδιαίτερα ευάλωτο στη διαρροή της ιδιωτικής ζωής των συναλλαγών λόγω του γεγονότος ότι οι λεπτομέρειες και οι ισορροπίες όλων των δημόσιων κλειδιών είναι ορατά σε όλους στο δίκτυο. Οι προτεινόμενες λύσεις για την επίτευξη ανωνυμίας στα blockchains μπορούν να ταξινομηθούν ευρέως σε διάλυμα ανάμιξης και ανώνυμη λύση. Η ανάμειξη είναι μια υπηρεσία που προσφέρει ανωνυμία με μεταφορά χρημάτων από πολλαπλές διευθύνσεις εισόδου σε πολλαπλές διευθύνσεις εξόδου. Anonymous είναι μια υπηρεσία που αποσυνδέει την προέλευση των πληρωμών για μια συναλλαγή για να αποτρέψει την ανάλυση γραφημάτων συναλλαγής όπως συζητείται στο [\[196\]](#).

7.1.3. Εγωιστική εξόρυξη.

Η εγωκεντρική εξόρυξη είναι μια άλλη πρόκληση που αντιμετωπίζουν οι μπλοκ αλυσίδες. Ένα μπλοκ είναι επιρρεπές σε εξαπάτηση εάν χρησιμοποιείται ένα μικρό μέρος της δύναμης καταστροφής. Στην εγωιστική

εξόρυξη, οι ανθρακωρύχοι κρατούν τα εξορυσσόμενα μπλοκ χωρίς να μεταδίδουν στο δίκτυο και δημιουργούν ένα ιδιωτικό κλαδί το οποίο μεταδίδεται μόνο αφού πληρούνται ορισμένες προϋποθέσεις. Σε αυτή την περίπτωση, οι ειλικρινείς ανθρακωρύχοι σπαταλούν πολύ χρόνο και πόρους, ενώ η ιδιωτική αλυσίδα εξορύσσεται από εγωιστές ανθρακωρύχους.

7.1.4. Προσωπικά αναγνωρίσιμα στοιχεία.

Στοιχεία προσωπικής ταυτοποίησης (PII) είναι οποιαδήποτε πληροφορία που μπορεί να χρησιμοποιηθεί για την εξαφάνιση της ταυτότητας ενός ατόμου. [197] συζητά το PII σε σχέση με την επικοινωνία και την ιδιωτικότητα της τοποθεσίας.

7.1.5. Ασφάλεια.

Η ασφάλεια μπορεί να συζητηθεί όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα όπως συζητείται στο [198]. Είναι πάντα μια πρόκληση σε ανοιχτά δίκτυα, όπως τα δημόσια μπλοκ. Η εμπιστευτικότητα είναι χαμηλή σε κατανεμημένα συστήματα που μιμούνται πληροφορίες μέσω του δικτύου τους. Η ακεραιότητα είναι ο στίχος των μπλοκ αλυσίδων, αν και υπάρχουν πολλές προκλήσεις. Η διαθεσιμότητα σε blockchains είναι υψηλή από την άποψη της αναγνωσιμότητας λόγω της ευρείας αναπαραγωγής σε σύγκριση με τη διαθεσιμότητα εγγραφής. Η επίθεση της πλειοψηφίας του 51% είναι περισσότερο θεωρητική σε ένα μεγάλο δίκτυο αποκλεισμού λόγω αυτών των ιδιοτήτων.

7.2. Ευκαιρίες.

Οι ευκαιρίες μπορούν να αναφερθούν ως ευκαιρία ενσωμάτωσης της τεχνολογίας blockchain σε υπάρχουσες εφαρμογές για τη βελτίωση της αποδοτικότητας και της χρήσης καθώς και για την προώθηση αυτής της τεχνολογίας σε μελλοντικές εφαρμογές. Ορισμένες από τις μελλοντικές ευκαιρίες παρατίθενται με περισσότερες λεπτομέρειες ως εξής.

7.2.1. Στρατηγική ευθυγράμμιση και διακυβέρνηση.

Η ενεργή διαχείριση των συνδέσεων μεταξύ των προόδων των επιχειρήσεων και των διοικητικών προτεραιοτήτων που στοχεύει στη διευκόλυνση των επιχειρησιακών ενεργειών για τη βελτίωση των επιδόσεων των επιχειρήσεων μπορεί να αναφέρεται ως στρατηγική ευθυγράμμιση. Η ανάλυση περιλαμβάνει την αξιολόγηση διαφορετικών διαδικασιών σχετικά με τον τρόπο με τον οποίο μπορούν να βελτιωθούν με τη χρήση τεχνολογίας blockchain. Οι κίνδυνοι αυτών των στρατηγικών ανάλογοι με τις επιπτώσεις κλειδώματος ενδέχεται επίσης να αναλυθούν.

Η διακυβέρνηση είναι περισσότερο σε σχέση με την κατάλληλη και διαφανή λογοδοσία όσον αφορά τα καθήκοντα, τα μέρη και τις διαδικασίες λήψης αποφάσεων για διάφορα έργα και επιχειρήσεις. Η τεχνολογία Blockchain διακυβεύει τη διακυβέρνηση προς μια πιο αλληλεπικαλυπτόμενη συνεργασία ως νέο τρόπο διαχείρισης των διαδικασιών. Όπως αναφέρθηκε στο [199], οι επιπτώσεις της διακυβέρνησης έχουν τέσσερις προοπτικές. Πρώτον, πρέπει να καθοριστούν οι αποκλειστικοί ρόλοι που συντονίζουν τόσο τις εσωτερικές όσο και τις εξωτερικές ομάδες για τη δημιουργία υποστήριξης μπλοκ αλυσίδων.

Αυτό απαιτεί τεχνικά και νομικά περιστατικά. Δεύτερον, πρέπει να καθοριστούν πολιτικές για τη χρήση και τη σχετική διαδικασία blockchain. Τρίτον, πρέπει να καθοριστεί μια σειρά κατευθυντήριων γραμμών για τη χρήση δημόσιων, ιδιωτικών και κοινοπραξιών. Αυτό θα μας βοηθήσει να προβλέψουμε τα σενάρια επίθεσης και να είμαστε καλύτερα προετοιμασμένοι γι' αυτούς. Τέλος, μπορούν να χρησιμοποιηθούν έξυπνα συμβόλαια για να ξεκινήσουν νέα μοντέλα διακυβέρνησης που συνθέτουν το DAO.

Η διακυβέρνηση της τεχνολογίας blockchain προτείνει ότι οι περισσότερες εφαρμογές των επιχειρήσεων πρέπει να λειτουργούν σε αποκλειστικές και ιδιωτικές μπλοκ αλυσίδες. Ο παράγοντας διακυβέρνησης διασφαλίζει ότι οι εφαρμογές δεν είναι εφαρμογές ενός ιδιοκτήτη, αλλά μοιράζονται από μια ομάδα ανταγωνιστών. Για παράδειγμα, οι τράπεζες πρέπει να συνεργαστούν για να αναπτύξουν καινοτόμα συστήματα πληρωμών για την ανάπτυξη λύσεων χρηματοδότησης του εμπορίου που θα αποτρέψουν τις δημόσιες μπλοκ για την επίτευξη της απαιτούμενης απόδοσης και εμπιστευτικότητας. Από την άλλη πλευρά, οι ιδιωτικές μπλοκ αλυσίδες πρέπει να καταλήξουν σε συμφωνία σχετικά με τους κανόνες διακυβέρνησης για να λειτουργήσουν κάτω. Στο μέλλον, πρέπει να καθοριστούν διεθνή πρότυπα για να επιτευχθεί η συναίσθηση σχετικά με έναν τεράστιο αριθμό προτύπων όπως είναι η συμμετοχή, οι έλεγχοι πρόσβασης, η ταξινόμηση και αποθήκευση δεδομένων, η μέτρηση για την επαλήθευση και επικύρωση των συναλλαγών, η ιδιοκτησία μπλοκ αλυσίδων, θα εξασφαλίσει επαρκές όφελος για να ξεπεραστούν τόσο τα τεχνολογικά εμπόδια όσο και τα εμπόδια διακυβέρνησης και να επιτευχθεί ευρεία χρήση στο μέλλον.

7.2.2. Τεχνολογία της πληροφορίας.

Η τεχνολογία πληροφοριών ενσωματώνει όλα τα συστήματα που υποστηρίζουν την εκτέλεση της διαδικασίας. Η τεχνολογία Blockchain επιτρέπει και παρέχει άφθονες ευκαιρίες για την εκτέλεση της διαδικασίας, αν και υπάρχουν πολλαπλές προκλήσεις που πρέπει ακόμα να αντιμετωπιστούν. Πρώτον, οι διαδικασίες υλοποίησης με blockchains απαιτούν νέα στοιχεία λογισμικού και την ενσωμάτωση των αναπτυξιακών περιβαλλόντων. Δεύτερον, η εκτέλεση διαδικασιών βάσει μπλοκ αλυσίδων δημιουργεί νέες προκλήσεις όσον αφορά την ασφάλεια και την προστασία της ιδιωτικής ζωής, όπως τον τρόπο αποφυγής διαρροών εμπιστευτικών δεδομένων των επιχειρήσεων. Ενώ η ορατότητα των κρυπτογραφημένων δεδομένων σε ένα blockchain είναι περιορισμένη, εναπόκειται στους συμμετέχοντες στη διαδικασία να διασφαλίσουν ότι αυτοί οι μηχανισμοί χρησιμοποιούνται σύμφωνα με τις απαιτήσεις εμπιστευτικότητας τους. Ορισμένες από τις απαιτήσεις αυτές εξετάζονται επί του παρόντος στον χρηματοπιστωτικό τομέα. Περαιτέρω προβλήματα μπορούν να αναμένονται με τη θέσπιση του κανονισμού για την γενική προστασία δεδομένων. Τέλος, πρέπει να ληφθούν υπόψη εγγενείς περιορισμοί των μπλοκ αλυσίδων, συμπεριλαμβανομένης της υπολογιστικής ισχύος, της αποθήκευσης δεδομένων, της απόδοσης και του κόστους επεξεργασίας. Αντί να χρησιμοποιήσει ένα υπάρχον blockchain, θα μπορούσε να υιοθετηθεί μια εναλλακτική λύση όπως ιδιωτικά μπλοκ αλυσίδες για τη μείωση του κόστους.

Το δυναμικό της τεχνολογίας blockchain είναι τεράστιο. Με την απόκτηση του χρόνου και της ωριμότητας της τεχνολογίας, το blockchain θα είναι σε θέση να υποστηρίξει τις ικανότητες συναλλαγών που είναι απαραίτητες για την υποστήριξη των περισσότερων εφαρμογών καινοτομίας και τεράστιων μεγεθών, καθώς και την υποστήριξη της θέσπισης κανόνων διακυβέρνησης στις επικείμενες δεκαετίες. Οι μπλοκ επιχειρήσεις που χρησιμοποιούνται τη στιγμή αυτή είναι σχετικά μικρής κλίμακας. Οι εφαρμογές ενός χρήστη περιλαμβάνουν εκείνες που χρησιμοποιούν τεχνολογία blockchain για την παρακολούθηση της ιδιοκτησίας ενός ακριβού ή πολύτιμου αντικειμένου. Κάθε ημερολόγιο κατέχει και διαχειρίζεται το blockchain του, το οποίο είναι ιδανικό για μη συχνές συναλλαγές. Παρόλο που η ταχύτητα επεξεργασίας μπλοκ αλφαριθμητισμού δεν έχει σκληρό όριο, η μεγαλύτερη πρόκληση για τις μελλοντικές εφαρμογές είναι η υψηλή συνολική και η εμπιστευτικότητα που συσσωρεύονται μαζί ως απαίτηση. Η επίτευξη αυτών των δύο πτυχών από κοινού θα οδηγήσει στην υψηλότερη αποδοχή και χρήση της τεχνολογίας blockchain στο μέλλον. Οι εφαρμογές στις λύσεις τεχνολογίας καινοτόμου φάσης είναι το μέλλον των εξελισσόμενων αγορών όπως η επιστήμη των δεδομένων, η μηχανική μάθηση, η διαδικτυακή πύλη κτλ. Ένα από τα πιο συναρπαστικά χαρακτηριστικά των blockchains είναι η επιλογή των μικροπληρωμών μαζί με τα έξυπνα συμβόλαια. Αυτός ο συνδυασμός δημιουργεί μια ενδιαφέρουσα λύση για τη ροή χρηματοοικονομικών πληρωμών, η οποία είναι αντιφατική με την παραδοσιακή διμηνιαία ή μηνιαία αμοιβή. Με απλά έξυπνα συμβόλαια, οποιοσδήποτε υπάλληλος ή επαγγελματίας μπορεί να καταβάλλεται σε πραγματικό χρόνο ενώ εργάζεται. Μπορούν να παρακολουθήσουν την πρόοδο των εργασιών τους, θέτοντας μικρογραφικά πλήκτρα για να μετρήσουν την παραγωγικότητα και την αποτελεσματικότητα της ποιότητας εργασίας και να κάνουν πληρωμές σε πραγματικό χρόνο. Αυτός ο τύπος πληρωμής σε πραγματικό χρόνο ήταν σχεδόν εφικτός με τη χρήση μπλοκ αλυσίδων, αλλά με μεγαλύτερα ποσά που παρεμποδίζουν το δίκτυο με επιλογές μικροπληρωμών. Οι μικρές πληρωμές είναι επωφελείς τόσο για την επιχείρηση όσο και για τους εργαζόμενους, καθώς αυτή η μέθοδος εξασφαλίζει ότι οι καλύτεροι εργαζόμενοι πληρώνονται περισσότερο και τα κίνητρα θα ευθυγραμμιστούν με καλύτερο τρόπο. Επιπλέον, οι μικροπληρωμές βοηθούν τους απομακρυσμένους υπαλλήλους σε πραγματικό χρόνο και παρακολουθούν το έργο τους, ο αντίκτυπος αυτής της χρήσης του blockchain είναι βαθύς.

Οι εκφράσεις ψηφιακής διαφήμισης αντιμετωπίζουν διαγωνισμούς που σχετίζονται με τις απάτες στον τομέα, την κυκλοφορία bot, την έλλειψη διαφάνειας και τα μοντέλα πληρωμής. Το κυριότερο θέμα είναι η ευθυγράμμιση των κινήτρων που οδηγούν στην αποθάρρυνση της διαφήμισης και των εκδοτών. Το Blockchain είναι η λύση για την επίτευξη της απαιτούμενης διαφάνειας στην αλυσίδα εφοδιασμού και μπορεί να φέρει εμπιστοσύνη σε περιβάλλοντα εμπιστοσύνης. Επιτρέπει στις εταιρείες να ευημερούν μειώνοντας τον αριθμό των κακών παραγόντων στην αλυσίδα εφοδιασμού. Αν και το blockchain είναι στα σπάργανα, η υποκείμενη τεχνολογία είναι εδώ για να παραμείνει και μπορεί να είναι ένας πολύ σημαντικός παράγοντας στη βελτίωση των επιχειρήσεων. Το πιο επιτακτικό χαρακτηριστικό του blockchain είναι η παροχή ασύγκριτης ασφάλειας σε ένα ανασφαλές διαδίκτυο, όπου το phishing, κακόβουλο λογισμικό, DDOS, spam και hacks στην παγκόσμια επιχείρηση. Ένα σημαντικό πλεονέκτημα του

blockchain έναντι άλλων λογιστικών βιβλίων είναι ότι βασίζεται στην κρυπτογραφία και είναι άκαμπτο προγραμματισμένο, καθιστώντας αδύνατο για οποιονδήποτε να επιστρέψει ένα βήμα και να αλλάξει πληροφορίες σχετικά με blockchains. Η κατανεμημένη πτυχή των μπλοκ αλυσίδων προσφέρει επίσης ένα σημαντικό πλεονέκτημα, γεγονός που καθιστά εξαιρετικά προβληματικό τον περιορισμό σε περίπτωση ελέγχου κυβερνητικών ή παράνομων επιχειρηματικών πρακτικών. Τέλος, το blockchain είναι ένα τεράστιο εργαλείο που πρέπει να χρησιμοποιηθεί όταν τεράστιες ποσότητες σημαντικών τεκμηρίων πρέπει να αποθηκευτούν, όπως η υγειονομική περίθαλψη, τα πνευματικά δικαιώματα, η εφοδιαστική κλπ. Οι έξυπνες συμβάσεις σε blockchain απομακρύνουν την ανάγκη ή τους μεσάζοντες να νομιμοποιήσουν τις συμβάσεις με φιλικούς προς τον χρήστη τρόπους.

Το Blockchain θεωρείται από πολλούς ως ψηφιακό σύστημα βιβλίων. Ωστόσο, η κρυπτογραφημένη δομή βάσεων δεδομένων των μπλοκ αλυσίδων είναι επαναστατική και διατηρεί πραγματικό δυναμικό. Το Διαδίκτυο μας επιτρέπει να επεκτείνουμε την ικανότητά μας να προωθούμε τα όρια και έχει μετακινηθεί με ταχύτητα σε σχέση με την προστασία από το spyware, τους ιούς και τους hackers. Το Blockchain έχει τη δυνατότητα να επισημάνει ουσιαστικά μια εκτενή ποικιλία διαδικασιών και τεχνολογιών. Τα Blockchains αντιμετωπίζουν αυτές τις ανησυχίες με ένα βιβλίο που περιλαμβάνει καταγεγραμμένο και επικυρωμένο ιστορικό συναλλαγών. Μειώνει την ανάγκη οργάνωσης να παρέχει μετριασμό του κινδύνου και αξιόπιστες υπηρεσίες, με αποτέλεσμα το κλείσιμο υποθηκών για ένα κλάσμα του κόστους και του χρόνου με σημαντικά υψηλότερα επίπεδα εμπιστοσύνης.

7.2.3. Άλλες προοπτικές του κλάδου.

Η Blockchain μπορεί να προσφέρει πρόσβαση στον τομέα των τραπεζών και των πληρωμών, παρέχοντας χρηματοπιστωτικές υπηρεσίες σε δισεκατομμύρια χρήστες σε όλο τον κόσμο, συμπεριλαμβανομένων των χωρών του τρίτου κόσμου χωρίς να έχουν πρόσβαση σε παραδοσιακούς τραπεζικούς λογαριασμούς. Οι πολυκαταστήματα χρησιμοποιούνται από πολλά τραπεζικά ιδρύματα για να κάνουν τις επιχειρηματικές τους δραστηριότητες ταχύτερες, πιο αποτελεσματικές και πιο ασφαλείς. Υπάρχει μια αυξανόμενη επένδυση σε μπλοκ μπάρες στις τραπεζικές επιχειρήσεις και στις νέες επιχειρήσεις και τα έργα. Η Cybersecurity είναι ένας άλλος τομέας ενδιαφέροντος και κορυφαίος για τα blockchains. Παρόλο που το βιβλίο blockchain είναι δημόσιο, τα δεδομένα επαληθεύονται και κρυπτογραφούνται χρησιμοποιώντας προηγμένη κρυπτογραφία, καθιστώντας τον λιγότερο επιρρεπή σε hacking και τροποποιήσεις χωρίς άδεια. Η Supply Chain Management είναι ένας άλλος τομέας της υλοποίησης τεχνολογίας blockchain. Οι συναλλαγές μπορούν να τεκμηριώνονται σε μόνιμο αποκεντρωμένο αρχείο και να παρακολουθούνται με ασφάλεια και διαφάνεια. Αυτό μειώνει σημαντικά τις χρονικές καθυστερήσεις και τα ανθρώπινα σφάλματα. Η τεχνολογία blockchain μπορεί επίσης να χρησιμοποιηθεί για την παρακολούθηση του κόστους, της εργασίας, των αποβλήτων και των εκπομπών σε κάθε σημείο, δεδομένου ότι οι αλυσίδες εφοδιασμού έχουν σοβαρές συνέπειες για την κατανόηση και τον έλεγχο των περιβαλλοντικών επιπτώσεων των προϊόντων ελέγχοντας την αυθεντικότητα. Επιπλέον, το blockchain μπορεί να χρησιμοποιηθεί για την πρόβλεψη των

αλλαγών σε ολόκληρη την προσέγγιση της έρευνας, της διαβούλευσης και της ανάλυσης.

Το IoT χρησιμοποιεί το blockchain ως νέα ιδέα για τη δημιουργία ενός αποκεντρωμένου δικτύου συσκευών IoT που λειτουργεί ως δημόσιο βιβλίο για σημαντικό αριθμό συσκευών. Αυτό θα μπορούσε να εξαλείψει την ανάγκη για μια κεντρική τοποθεσία για να χειριστεί την επικοινωνία όπως ενημερώσεις λογισμικού, διαχείριση σφαλμάτων και παρακολούθηση της χρήσης ενέργειας. Η διαχείριση της εμπιστοσύνης είναι η ρίζα της παγκόσμιας ασφαλιστικής αγοράς για την ενσωμάτωση δεδομένων πραγματικού κόσμου με έξυπνες συμβάσεις. Οι ιδιωτικές συγκοινωνίες και η ανταλλαγή βαρών χρησιμοποιούν αποκλεισμούς για τη δημιουργία αποκεντρωμένων εκδόσεων εφαρμογών κοινής χρήσης μεταξύ ομότιμων χρηστών, επιτρέποντας έτσι στους ιδιοκτήτες αυτοκινήτων και τους χρήστες να οργανώνουν τους όρους και τις προϋποθέσεις με ασφαλή τρόπο χωρίς τους τρίτους. Τα ηλεκτρονικά πορτοφόλια επιτρέπουν στους ιδιοκτήτες αυτοκινήτων να πληρώνουν για στάθμευση, διόδια και αναβαθμίσεις αυτόματα για τα οχήματά τους. Οι παραδοσιακά συγκεντρωμένοι εξυπηρετητές μπορεί να είναι εξαιρετικά ευάλωτοι για να τους πειραματιστεί. Αντ' αυτού, τα blockchains αποθηκεύουν τα δεδομένα στην αποθήκευση σύννεφων με αποκεντρωμένο τρόπο, γεγονός που την καθιστά ασφαλέστερη και ισχυρότερη. Η ανεπάρκεια και η διαφθορά είναι οι πιο κοινές επικρίσεις σε φιλικούς χώρους που εμποδίζουν τα χρήματα να φτάσουν στους επιδιωκόμενους ανθρώπους. Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για την παρακολούθηση των δωρεών με ασφαλή, διαφανή και επαληθεύσιμο τρόπο, ώστε να διασφαλιστεί ότι τα δωρεά χρημάτων φθάνουν στο συμβαλλόμενο μέρος. Το blockchain μπορεί επίσης να χρησιμοποιηθεί για την ψηφοφορία με την καταγραφή των ψηφοφόρων και την επαλήθευση της ταυτότητας, αφού η καταμέτρηση των ψηφοφοριών σε έναν παραδοσιακά συγκεντρωμένο εξυπηρετητή μπορεί να είναι εξαιρετικά ευάλωτη σε hacking, απώλεια δεδομένων ή ανθρώπινα σφάλματα. Η ψηφοφορία είναι ένας σημαντικός τομέας που μπορεί να διαταραχθεί από μπλοκ αλυσίδες, καθώς το blockchain θα μπορούσε να δημιουργήσει ένα αμετάβλητο και δημοσίως καταγεγραμμένο βιβλίο καταγεγραμμένων ψήφων και να παράσχει τη μεγάλη ανάγκη διαφάνειας στο σύστημα ψηφοφορίας του κόσμου. Τα κυβερνητικά συστήματα είναι συνηθισμένα σκόπιμα απρόσβλητα και προδιάθετα στη διαφθορά. Εφαρμογή συστήματος βασισμένου σε blockchain

μπορεί να βελτιώσει σημαντικά την ασφάλεια, την αποδοτικότητα και τη διαφάνεια των κυβερνητικών πράξεων.

Το δημόσιο σύστημα welfares είναι μια εναλλακτική υποδιαίρεση που υποφέρει από την απελευθέρωση και τη γραφειοκρατία. Μια άλλη βιομηχανία που εξαρτάται από τα παλαιότερα συστήματα και είναι κατάλληλη για διακοπή είναι η υγειονομική περίθαλψη. Στα νοσοκομεία, συχνά πέφτουν θύματα πειρατείας δεδομένων λόγω των απαρχαιωμένων υποδομών. Τα μεγάλα νοσοκομεία διαγωνισμού αντιμετωπίζουν την απουσία προστατευμένου βάθρου για την αποθήκευση και την ανταλλαγή δεδομένων. Η τεχνολογία Blockchain επιτρέπει στα νοσοκομεία να αποθηκεύουν με ασφάλεια τα δεδομένα όπως τα ιατρικά αρχεία και να τα μοιράζονται με εγκεκριμένες αρχές

ή ασθενείς, γεγονός που μπορεί να βελτιώσει την ασφάλεια των δεδομένων και να βοηθήσει με την ακρίβεια και την ταχύτητα της διάγνωσης.

Η διαχείριση της ενέργειας είναι μια ιδιαίτερα συγκεντρωτική βιομηχανία. Οι κατασκευαστές ενέργειας και οι καταναλωτές δεν μπορούν να το αγοράσουν άμεσα μεταξύ τους και πρέπει να εμπλέκουν έναν αξιόπιστο ιδιωτικό διαμεσολαβητή. Η τεχνολογία Blockchain μπορεί να προσφέρει μια καλύτερη και αποτελεσματικότερη λύση σε αυτό το πρόβλημα. Η ηλεκτρονική μουσική είναι ένας άλλος τομέας στον οποίο μπορεί να υλοποιηθεί το blockchain. Πολλές εταιρείες αναπτύσσουν τρόπους ώστε οι μουσικοί να πληρώνονται ανεπιφύλακτα από τους οπαδούς τους, αντί να μοιράζονται μεγάλα ποσοστά πωλήσεων με πλατφόρμες ή δισκογραφικές εταιρείες. Τα έξυπνα συμβόλαια επιλύουν αυτόματα τα ζητήματα αδειοδότησης και τα τραγούδια καταλόγων με τους αντίστοιχους δημιουργούς τους με καλύτερο και αποδοτικότερο τρόπο. Ένας άλλος τομέας είναι η λιανική πώληση, στην οποία πρέπει να εμπιστευόμαστε το σύστημα λιανικής πώλησης το οποίο με τη σειρά του μας δεσμεύει στο κατάστημα ή στην αγορά. Οι επιχειρήσεις κοινής ωφέλειας που βασίζονται στο Blockchain λειτουργούν αντιθέτως συνδέοντας τους αγοραστές και τους πωλητές και εξαιρώντας τον μεσάζοντα καθώς και τα τέλη που συνδέονται με αυτά. Σε τέτοιες περιπτώσεις, η εμπιστοσύνη προέρχεται από έξυπνα συμβόλαια, ασφάλεια αλληλεπίδρασης και ενσωματωμένα συστήματα διαχείρισης φήμης.

Η ακίνητη περιουσία αντιμετωπίζει προβλήματα με διαφάνεια, απάτη και ανατροπές σε δημόσια αρχεία. Όσον αφορά την αγορά και την πώληση ακινήτων, η τεχνολογία blockchain μπορεί να επιταχύνει τον τομέα των ακινήτων μειώνοντας την ανάγκη για χαρτιά και μπορεί να βοηθήσει στην παρακολούθηση, την επαλήθευση, την ιδιοκτησία, την ακρίβεια των εγγράφων και τη μεταβίβαση περιουσιακών στοιχείων. Η Crowdfunding έχει αναπτύξει μια επικρατούσα μέθοδο συγκέντρωσης κεφαλαίων για καινοτόμες επιχειρήσεις και έργα τα τελευταία χρόνια. Ωστόσο, οι πλατφόρμες crowdfunding χρεώνουν υψηλά τέλη. Σε φράγκο με βάση το crowdfunding, δημιουργείται εμπιστοσύνη σε έξυπνες συμβάσεις και συστήματα φήμης στο διαδίκτυο. Αυτό θα μπορούσε να εξαλείψει την ανάγκη για μεσάζοντα και να μειώσει το κόστος. Τα έργα προχωρούν σε κεφάλαια απελευθερώνοντας τα δικά τους μάρκες που χαρακτηρίζουν αξία και μπορούν να ανταλλάσσονται με προϊόντα, υπηρεσίες ή μετρητά όποτε χρειάζεται. Οποιοσδήποτε κλάδος που ασχολείται με δεδομένα ή συναλλαγές οποιουδήποτε είδους μπορεί να διαταραχθεί με τεχνολογία blockchain. Ο χώρος είναι ανεπτυγμένος και υπάρχουν πολλές ευκαιρίες.

7.3. Επιπλέον προκλήσεις.

Ανοιχτές προκλήσεις και μελλοντικές κατευθύνσεις έρευνας.

Στην ενότητα αυτή εξετάζονται οι προκλήσεις που προβλέπονται για την αποτελεσματική εφαρμογή της ασφάλειας για συσκευές IoT.

7.3.1. Περιορισμοί πόρων.

Η αρχιτεκτονική του IoT με περιορισμένο πόρο αποτέλεσε κύριο εμπόδιο για τον καθορισμό ενός ισχυρού μηχανισμού ασφαλείας. Σε αντίθεση με τα συμβατικά παραδείγματα, οι κρυπτογραφικοί αλγόριθμοι πρέπει να

περιοριστούν στην εργασία εντός αυτών των περιορισμών. Με τυχόν εκπομπές ή πολυκάναλες που απαιτούνται για την ανταλλαγή κλειδιών ή πιστοποιητικών, πρέπει να αντιμετωπιστούν οι απαιτήσεις αποθήκευσης καθώς και οι ενεργειακές απαιτήσεις, προκειμένου να επιτευχθεί η επιτυχής εφαρμογή των πρωτοκόλλων ασφάλειας και επικοινωνίας για το Διαδίκτυο. Αυτό συνεπάγεται τον επανασχεδιασμό αυτών των πρωτοκόλλων ώστε να είναι ελαφρύς και ενεργειακώς αποδοτικός παρά την ανάγκη πολύπλοκων υπολογισμών μαζί με τη βελτίωση των τεχνικών συλλογής ενέργειας [200].

7.3.2. Ετερογενείς συσκευές.

Όπως συμβαίνει με τις ετερογενείς συσκευές που κυμαίνονται από μικρές συσκευές χαμηλής ισχύος με αισθητήρες έως διακομιστές υψηλού επιπέδου, πρέπει να εφαρμοστεί ένα πλαίσιο ασφαλείας πολλαπλών επιπέδων. Το πλαίσιο θα πρέπει αρχικά να προσαρμόζεται στους υφιστάμενους πόρους, να λαμβάνει αποφάσεις σχετικά με την επιλογή μηχανισμών ασφαλείας σε στρώματα διαδικτύου πριν από την παροχή οποιωνδήποτε υπηρεσιών στους τελικούς χρήστες. Ένα τέτοιο δυναμικά προσαρμόσιμο πλαίσιο ασφαλείας απαιτεί νοημοσύνη, η οποία υπόκειται στην τυποποίηση των πόρων που θα χρησιμοποιηθούν σε αρχιτεκτονικές διαδικτύου.

7.3.3. Διαλειτουργικότητα των πρωτοκόλλων ασφαλείας.

Για την τυποποίηση ενός παγκόσμιου μηχανισμού ασφαλείας για το Διαδίκτυο, οι προληπτικοί κανόνες που εφαρμόζονται σε διαφορετικά επίπεδα πρέπει να αλληλεπιδρούν παρέχοντας μηχανισμούς μετατροπής. Στο πλαίσιο του παγκόσμιου μηχανισμού, ένας αποτελεσματικός συνδυασμός προτύπων ασφαλείας σε κάθε στρώμα μπορεί στη συνέχεια να καθοριστεί με την εξέταση αρχιτεκτονικών περιορισμών.

7.3.4. Ενιαία σημεία αποτυχίας.

Με τα ετερογενή δίκτυα, τις αρχιτεκτονικές και τα πρωτόκολλα, το πρότυπο IoT γίνεται πιο ευάλωτο σε απλά σημεία αποτυχίας από οποιοδήποτε άλλο παράδειγμα. Ωστόσο, πρέπει να πραγματοποιηθεί σημαντικός αριθμός ερευνητικών εργασιών για να διασφαλιστεί η επαρκής διαθεσιμότητα στοιχείων IoT, ιδίως για εφαρμογές κρίσιμης σημασίας. Θα απαιτούσε μηχανισμούς και πρότυπα για την εισαγωγή πλεονασμάτων, διατηρώντας παράλληλα υπόψη το αντιστάθμισμα μεταξύ του κόστους και της αξιοπιστίας ολόκληρης της υποδομής.

7.3.5. Σφάλματα υλικού / υλικολογισμικού.

Με τη χρήση συσκευών χαμηλού κόστους και χαμηλής κατανάλωσης, η αρχιτεκτονική IoT μπορεί να είναι πιο εκτεθειμένη σε ευπάθειες υλικού. Δεν είναι απλώς η φυσική δυσλειτουργία, αλλά η εφαρμογή αλγορίθμων ασφαλείας στο υλικό, οι μηχανισμοί δρομολόγησης και επεξεργασίας πακέτων πρέπει επίσης να επαληθευτούν πριν από την ανάπτυξη σε IoT. Τυχόν ευπάθειες που εκμεταλλεύονται μετά την ανάπτυξη είναι δύσκολο να

εντοπιστούν και να ανακουφιστούν. Επομένως, ένα τυπικό πρωτόκολλο επαλήθευσης αποτελεί βασική προϋπόθεση για την αξιοποίηση της ασφάλειας του IoT.

7.3.6. Εμπιστευτικές ενημερώσεις και διαχείριση.

Ένα από τα βασικά ανοικτά ζητήματα για τη μελλοντική έρευνα είναι η παροχή επεκτάσιμης και αξιόπιστης διαχείρισης και ενημέρωσης λογισμικού σε εκατομμύρια συσκευές IoT. Επιπλέον, τα θέματα που σχετίζονται με την ασφαλή και αξιόπιστη διακυβέρνηση της ιδιοκτησίας συσκευών IoT, της αλυσίδας εφοδιασμού και της ιδιωτικής ζωής των δεδομένων είναι ανοικτά ερευνητικά προβλήματα που πρέπει να αντιμετωπιστούν από την ερευνητική κοινότητα για να προωθηθεί μια ευρεία και μαζική υιοθέτηση της κλίμακας για το Διαδίκτυο. Η τεχνολογία blockchain μπορεί να αποτελέσει παράγοντα για τέτοιες λύσεις ασφάλειας IoT. Ωστόσο, η τεχνολογία μπλοκ αλουμινίου δημιουργεί από μόνη της τις ερευνητικές προκλήσεις που πρέπει να αντιμετωπιστούν όσον αφορά την επεκτασιμότητα, την αποδοτικότητά της, τη διαιτησία / τους κανονισμούς και τη σύγκρουση-κλειδί.

7.3.7. Αδυναμίες μπλοκαρίσματος.

Παρά την ύπαρξη ισχυρών προσεγγίσεων για την εξασφάλιση του IoT, τα συστήματα blockchain είναι επίσης ευάλωτα [201]. Ο μηχανισμός συναίνεσης που εξαρτάται από την εξουδετερωτική δύναμη του ανθρακωρύχου μπορεί να καταστραφεί, επιτρέποντας έτσι στον επιτιθέμενο να φιλοξενήσει το blockchain. Ομοίως, τα ιδιωτικά κλειδιά με περιορισμένη τυχαιότητα μπορούν να αξιοποιηθούν για να διακυβεύσουν τους λογαριασμούς blockchain. Ωστόσο, πρέπει να οριστούν αποτελεσματικοί μηχανισμοί για να εξασφαλιστεί η ιδιωτικότητα των συναλλαγών και να αποφευχθούν οι φυλετικές επιθέσεις που ενδέχεται να οδηγήσουν σε διπλή δαπάνη κατά τη διάρκεια των συναλλαγών.

Η τεχνολογία Blockchain έχει υλοποιηθεί ή υλοποιηθεί ως χρήματα στον κυβερνοχώρο και χρησιμοποιείται πραγματικά. Σημειώστε, ωστόσο, ότι έχουν αναφερθεί διάφορα ζητήματα ασφάλειας που συμβαίνουν σε συμφωνία blockchain, συναλλαγή, πορτοφόλι και λογισμικό. Αυτό το έγγραφο ελέγχει τις τάσεις των ζητημάτων ασφαλείας που έχουν τεθεί μέχρι σήμερα και το επίπεδο ασφάλειας του τρέχοντος blockchain. Θεωρούμε ότι αυτή η απόπειρα είναι πολύ σημαντική καθώς τα αποτελέσματα μπορούν να χρησιμεύσουν ως δεδομένα βάσης για την ανάπτυξη της μελλοντικής τεχνολογίας blockchain και για την συμπλήρωση της ασφάλειας.

7.3.8. Διακανονισμός Blockchain.

Αν και θα πρέπει να υπάρχει μόνο ένα blockchain αφού είναι η διαδοχική σύνδεση των παραγόμενων μπλοκ, ένα blockchain μπορεί να χωριστεί σε δύο διότι τα δύο τελευταία μπλοκ μπορούν να δημιουργηθούν προσωρινά αν δύο διαφορετικοί ομότιμοι επιτύχουν στην εξόρυξη της απάντησης για τη δημιουργία του μπλοκ ταυτόχρονα. Σε αυτή την περίπτωση, το μπλοκ που δεν έχει επιλεγεί ως το τελευταίο μπλοκ από την πλειονότητα των συνομηλίκων στο δίκτυο Bitcoin για να συνεχίσει την εξόρυξη θα καταστεί άνευ σημασίας.

Με άλλα λόγια, το bitcoin θα ακολουθήσει την πλειοψηφία των συνομηλίκων που έχουν 50% ή περισσότερες δυνατότητες εξόρυξης (λειτουργική ικανότητα). Επομένως, εάν ένας εισβολέας έχει δυνατότητα εξόρυξης 51%, ένα "51% Attack", όπου ο επιτιθέμενος έχει τον έλεγχο του blockchain και μπορεί να περιλαμβάνει πλαστές συναλλαγές, μπορεί να είναι ένα πρόβλημα. Σύμφωνα με μια μελέτη, ένας εισβολέας μπορεί να πραγματοποιήσει παράνομο κέρδος με μόνο 25% ικανότητα λειτουργίας μέσω μιας κακόβουλης διαδικασίας εξόρυξης αντί του 51%. Δεδομένου ότι η τρέχουσα ικανότητα λειτουργίας ολόκληρου του δικτύου bitcoin είναι ήδη υψηλή, επιτυγχάνοντας σημαντική λειτουργική ικανότητα θεωρείται δύσκολη. Παρ' όλα αυτά, τα εξορυκτικά ορυχεία - οι συνεταιρισμοί ορυχείων - εξόρυζαν ενεργά για να αυξήσουν την πιθανότητα εξόρυξης. Έτσι, ο κίνδυνος αυτός έχει καταστεί πρόβλημα. Πρόσφατα, η GHash, ηγετική δεξαμενή εξόρυξης, ξεπέρασε προσωρινά το κατώτατο όριο του 50%, αναγκάζοντας την κοινότητα bitcoin να προχωρήσει σε εσωτερικές και εξωτερικές προσαρμογές για να αντιμετωπίσει τον κίνδυνο. Συγκεκριμένα, η δυνατότητα κυριαρχίας στο blockchain σχετίζεται με τη βασική ασφάλεια του bitcoin και οι εν λόγω απειλές ασφαλείας έχουν επηρεάσει προσωρινά τους οικονομικούς παράγοντες λόγω των χαρακτηριστικών του bitcoin, το οποίο είναι πάντα στενά συνδεδεμένο με την αγοραία τιμή [\[202\]](#), [\[203\]](#).

7.3.9. Ασφάλεια Συναλλαγών.

Δεδομένου ότι το σενάριο που χρησιμοποιείται στις εισόδους και εξόδους είναι μια γλώσσα προγραμματισμού με ευελιξία, μπορούν να δημιουργηθούν διαφορετικές μορφές συναλλαγών χρησιμοποιώντας τέτοια. Μια σύμβαση bitcoin [\[204\]](#) είναι μια μέθοδος εφαρμογής bitcoin για την υπάρχουσα πιστοποίηση ταυτότητας και χρηματοοικονομική υπηρεσία. Μια ευρέως χρησιμοποιούμενη μέθοδος περιλαμβάνει τη δημιουργία της σύμβασης χρησιμοποιώντας το σενάριο που περιλαμβάνει μια τεχνική πολλαπλών υπογραφών που ονομάζεται multisig. Παρόλο που τα σενάρια χρησιμοποιούνται για την επίλυση ενός ευρέος φάσματος προβλημάτων bitcoin, η πιθανότητα μιας ακατάλληλα διαμορφωμένης συναλλαγής έχει επίσης αυξηθεί καθώς η πολυπλοκότητα του σεναρίου αυξάνεται. Ένα bitcoin χρησιμοποιώντας ένα σωστά διαμορφωμένο σενάριο κλειδώματος απορρίπτεται, αφού κανείς δεν μπορεί να το χρησιμοποιήσει καθώς το σενάριο ξεκλειδώματος δεν μπορεί να δημιουργηθεί. Για το σκοπό αυτό, υπάρχουν μελέτες που υποδεικνύουν μοντέλα συναλλαγών τύπου bitcoin συμβολοσειράς για την επαλήθευση της ακρίβειας ενός σεναρίου που χρησιμοποιείται σε μια συναλλαγή [\[205\]](#).

7.3.10. Ασφάλεια του Πορτοφολιού.

Η διεύθυνση bitcoin είναι η τιμή κατακερματισμού ενός δημόσιου κλειδιού που κωδικοποιείται με ένα ζεύγος δημόσιων και προσωπικών κλειδιών. Επομένως, το σενάριο κλειδώματος μιας συναλλαγής bitcoin με μια διεύθυνση ως έξοδο μπορεί να ξεκλειδωθεί με ένα σενάριο ξεκλειδώματος που έχει την τιμή που έχει υπογραφεί με το δημόσιο κλειδί της διεύθυνσης και το προσωπικό κλειδί. Το πορτοφόλι bitcoin αποθηκεύει πληροφορίες όπως το προσωπικό κλειδί της διεύθυνσης που θα χρησιμοποιηθεί για τη δημιουργία του σεναρίου ξεκλειδώματος. Αυτό σημαίνει ότι η απώλεια πληροφοριών στο πορτοφόλι οδηγεί σε απώλεια bitcoin δεδομένου ότι η πληροφορία είναι

απαραίτητη για τη χρήση του bitcoin. Ως εκ τούτου, το πορτοφόλι bitcoin έχει γίνει το κύριο θέμα της επίθεσης bitcoin μέσω hacking [206].

Για να διασφαλιστεί η ασφάλεια του πορτοφολιού bitcoin, οι υπηρεσίες έχουν εισαγάγει multisig για πολλαπλές υπογραφές. Εφόσον το multisig επιτρέπει μόνο μια συναλλαγή όταν υπάρχουν περισσότερες από μία υπογραφές, ανάλογα με τη ρύθμιση, μπορεί να χρησιμοποιηθεί ως πλεονάζον χαρακτηριστικό ασφαλείας του πορτοφολιού. Για παράδειγμα, αν το multisig έχει οριστεί σε ένα online πορτοφόλι bitcoin και είναι ρυθμισμένο να απαιτεί την υπογραφή του ιδιοκτήτη εκτός από την υπογραφή του ιστότοπου του διαδικτυακού πορτοφολιού κάθε φορά που εκτελείται μια συναλλαγή από το πορτοφόλι, μπορεί να αποτραπεί η κακόβουλη απόσυρση από το bitcoin, δεν αποθηκεύεται, ακόμη και όταν ο ιστότοπος του διαδικτυακού πορτοφολιού παραλαμβάνεται από μια επίθεση κατά του hacking. Επιπλέον, το multisig εξελίσσεται σε υπηρεσίες που επιτρέπουν την απόσυρση από το πορτοφόλι bitcoin μόνο με βιομετρικά δεδομένα ή χωριστό εξοπλισμό χρησιμοποιώντας έλεγχο ταυτότητας δύο παραγόντων και άλλα μέτρα [207].

Δεδομένου ότι η βασική λύση για την επίθεση hacking ενός πορτοφολιού bitcoin, offline, πορτοφόλια τύπου ψυχρού αποθηκευτικού τύπου, όπως ένα φυσικό κέρμα bitcoin ή ένα πορτοφόλι bitcoin χαρτί που δεν είναι συνδεδεμένο με το Διαδίκτυο, είναι διαθέσιμα. Παρόμοιες προσεγγίσεις περιλαμβάνουν τα πορτοφόλια bitcoin τύπου hardware για τη μείωση του κινδύνου που συνδέεται με τις ηλεκτρονικές συναλλαγές. Το πορτοφόλι υλικού, όπως το Trezor, αποθηκεύει το κλειδί σε μια μονάδα αποθήκευσης με προστασία από παραβίαση που είναι συνδεδεμένη στον υπολογιστή μέσω USB, δηλαδή μόνο όταν χρησιμοποιείται και η υπογεγραμμένη συναλλαγή μεταφέρεται χρησιμοποιώντας το κλειδί που έχει αποθηκευτεί εσωτερικά και μόνο όταν ο χρήστης έχει πιστοποιηθεί. Με άλλα λόγια, η μονάδα αποθήκευσης συνδέεται μόνο όταν υπάρχει ανάγκη να δημιουργηθεί μια συναλλαγή bitcoin, που παραμένει σε κατάσταση ψυχρής αποθήκευσης όπως ο υπόλοιπος χρόνος. Παρόλο που είναι πιο ασφαλής από την αποθήκευση εν ψυχρώ, επειδή υπάρχει μία ακόμη διαδικασία ελέγχου ταυτότητας, προβλήματα όπως η απώλεια ψυκτικής αποθήκευσης και η έλλειψη φιλικότητας προς το χρήστη επηρεάζουν επίσης το πορτοφόλι υλικού [208].

7.3.11. Ασφάλεια Λογισμικού.

Το σφάλμα του λογισμικού που χρησιμοποιείται στο bitcoin μπορεί να είναι κρίσιμο. Αν και η επίσημη τοποθεσία του Bitcoin Developer Documentation [209] εξηγεί σαφώς όλες τις διαδικασίες bitcoin, το λογισμικό core bitcoin εξακολουθεί να είναι αποτελεσματικό ως αναφορά, αφού οι λεπτομερείς διαδικασίες του πρώτου συστήματος bitcoin έχουν προσδιοριστεί μέσω του λογισμικού που εφαρμόζει ο Satoshi Nakamoto.

Παρ' όλα αυτά, ακόμα και το λογισμικό πυρήνα bitcoin, το οποίο πρέπει να είναι πιο αξιόπιστο από οτιδήποτε άλλο, δεν είναι απαλλαγμένο από το πρόβλημα της δυσλειτουργίας του λογισμικού, όπως το σφάλμα. Το πιο γνωστό σφάλμα λογισμικού είναι το θέμα ευπάθειας CVE-2010-5139 που παρουσιάστηκε τον Αύγουστο του 2010. Λόγω του σφάλματος που προκλήθηκε από την υπερχειλίση ακέραιων αριθμών, μια μη έγκυρη συναλλαγή στην οποία δόθηκε 0,5 bitcoin ως 184 τρισεκατομμύρια bitcoin συμπεριλήφθηκε σε ένα κανονικό μπλοκ και το πρόβλημα δεν επιλύθηκε μέχρι

8 ώρες αργότερα. Επιπλέον, υπήρξε ένα σφάλμα όπου ένα μπλοκ που επεξεργάστηκε στην έκδοση 0.8 δεν επεξεργάστηκε στην έκδοση 0.7 καθώς η βάση δεδομένων άλλαξε από BerkeleyDB σε LevelDB από την έκδοση bitcoin του πυρήνα bitcoin αναβαθμίστηκε από 0,7 σε 0,8. Προκάλεσε τους συνομηλίκους της έκδοσης 0.7 και τους συνομηλίκους της έκδοσης 0.8 να έχουν διαφορετικές μπλοκ αλυσίδες για 6 ώρες. Και τα δύο αυτά προβλήματα είναι περιπτώσεις που δείχνουν ότι η γενική εμπιστοσύνη στην ασφάλεια των συναλλαγών bitcoin ενός μπλοκ ως έχει σημαντικό βάθος μετά από μια χρονική περίοδο και μπορεί να απειληθεί από ένα λογισμικό bug [\[210\]](#).

8. Συμπεράσματα

Αυτό το κεφάλαιο ολοκληρώνει αυτή την εργασία και προτείνει τα διδάγματα που αποκομίζονται, συμπεράσματα και μελλοντικές κατευθύνσεις έρευνας .

Αποτελέσματα

Μία από τις σημαντικότερες συμβολές του blockchain είναι ο βαθμός διαφάνειας και αποκέντρωσης που παρέχει, παράλληλα με το επαρκές επίπεδο ασφάλειας και ιδιωτικότητας, το οποίο προηγουμένως θεωρήθηκε σχεδόν απροσπέραστο. Ωστόσο, το blockchain εξακολουθεί να είναι μια εξελισσόμενη τεχνολογία και εκτός από πολλά ενδιαφέροντα χαρακτηριστικά ασφάλειας και προστασίας της ιδιωτικής ζωής, εξακολουθούν να υπάρχουν τεράστιες ανησυχίες για την ασφάλεια και την προστασία της ιδιωτικής ζωής σε ένα σύστημα Blockchain. Με βάση τη διεξοδική έρευνα σχετικά με την πτυχή ασφάλειας του blockchain, υπάρχουν απειλές για την ασφάλεια που οφείλονται σε διαθέσιμα τρωτά σημεία στο blockchain. Εκτός αυτού, υπάρχουν απειλές για την ασφάλεια που οδηγούν σε επιθέσεις διπλής δαπάνης, υπάρχουν απειλές για την ασφάλεια του δικτύου Blockchain γενικότερα, και απειλές των ανθρακωρύχων ή των ορυχείων και των έξυπνων συμβολαίων. Η μελέτη απειλές ασφάλειας και ιδιωτικότητας σε διαφορετικά πεδία του blockchain.

Συμπέρασμα

Αυτή η μελέτη επικεντρώνεται στα ζητήματα ασφάλειας και διασφάλισης της ιδιωτικότητας της τεχνολογίας blockchain. Μελετώντας τα διάφορα πεδία του blockchain, όπως οι μηχανισμοί συναίνεσης, το blockchain δίκτυο, την εξορυκτική διαδικασία, την αποθήκευση δεδομένων , την διαχείριση κλειδιών, τη λειτουργικότητα έξυπνων συμβάσεων, εξετάσαμε όλες τις υφιστάμενες αδυναμίες στους αντίστοιχους τομείς. Με αυτή την εργασία, ελπίζω να βοηθήσω τους προγραμματιστές και τους ερευνητές, καθώς και τις επιχειρήσεις να κατανοήσουν τη φύση των διαφόρων απειλών για την ασφάλεια και την διασφάλιση ιδιωτικότητας. Για παράδειγμα, οι απειλές για την ασφάλεια και την ιδιωτικότητα, θα μπορούσαν να επηρεάσουν τα διαφορετικά επίπεδα των συστημάτων blockchain ή τις διεργασίες του blockchain ή και στοχευμένους επιχειρησιακούς χρήστες. Συνεπώς είναι ένα θέμα μεγάλου ενδιαφέροντος, που απλοποιείται με αυτή την εργασία .

9. Αναφορές/βιβλιογραφία

- [0] URL <https://bitcoin.org/en/how-it-works>.
- [1] BitInfoCharts, Block - Bitcoin Wiki, 2016. URL <https://en.bitcoin.it/wiki/Block>.
- [2] EtherScan, Ethereum Average BlockTime Chart, 2016. URL <https://etherscan.io/chart/blocktime>.
- [3] Linux-Foundation, Blockchain technologies for business, 2017. URL <https://www.hyperledger.org/>.
- [4] C. Kuhlman, What is eris? 2016 Edition, 2016. URL <https://monax.io/2016/04/03/wtf-is-eris/>.
- [5] Stellar, Stellar network overview, 2014. URL <https://www.stellar.org/developers/guides/get-started/>.
- [6] Ripple, Ripple network, 2013. URL <https://ripple.com/network>.
- [7] All-In-Bits, Introduction to tendermint, 2017. URL <https://tendermint.com/intro>.
- [8] EconoTimes, Safeshare releases first blockchain insurance solution for sharing economy, 2016. URL <https://www.econotimes.com/SafeShare-Releases-First-Blockchain-Insurance-Solution-For-Sharing-Economy-181326>.
- [9] IBM, IBM blockchain based on hyperledger fabric from the linux foundation, 2017. URL <https://www.ibm.com/blockchain/hyperledger.html>.
- [10] T. Swanson, Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems, Report, available online, Apr.
- [11] Data aggregation scheduling in probabilistic wireless networks with cognitive radio capability, in 2016 IEEE Global Communications Conference (GLOBECOM), 2016, 1- 6.
- [12] I.-C. Lin and T.-C. Liao, A survey of blockchain security issues and challenges., *IJ Network Security*, 19 (2017), 653- 659.
- [13] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in *Big Data (BigData Congress)*, 2017 IEEE International Congress on, IEEE, 2017, 557- 564.
- [14] V. King and J. Saia, Scalable byzantine computation, *ACM SIGACT News*, 41 (2010), 89- 104.
- [15] M. Vukolic, The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in *International Workshop on Open Problems in Network Security*, Springer, 2015, 112- 125.
- [16] D. Larimer, Transactions as proof-of-stake, 2013.

- [17] R. Kotla, L. Alvisi, M. Dahlin, A. Clement and E. Wong, Zyzyva: Speculative byzantine fault tolerance, in ACM SIGOPS Operating Systems Review, ACM, 41 (2007), 45-58.
- [18] D. Larimer, Delegated proof-of-stake white paper, 2014.
- [19] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert and P. Saxena, Scp: A computationally-scalable byzantine consensus protocol for blockchains., IACR Cryptology ePrint Archive, 2015 (2015), 1168.
- [20] I.-C. Lin and T.-C. Liao, A survey of blockchain security issues and challenges., IJ Network Security, 19 (2017), 653 - 659.
- [21] F. Gierschner, Bitcoin and beyond.
- [22] X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems, (2017), URL <http://www.sciencedirect.com/science/article/pii/S0167739X17318332>.
- [23] G. Noubir, G. Lin, Low-power DoS attacks in data wireless LANs and countermeasures, SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 29–30.
- [24] S.H. Chae, W. Choi, J.H. Lee, T.Q.S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans. Info. for. Sec. 9 (10) (2014) 1617–1628. <http://dx.doi.org/10.1109/TIFS.2014.2341453>.
- [25] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-Based detection of sybil attacks in wireless networks, IEEE Transa. Inf. Forensics Secur. 4 (3) (2009) 492–503.
- [26] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.
- [27] H. Kim, Protection against packet fragmentation attacks at 6LoWPAN adaptation layer, in: 2008 International Conference on Convergence and Hybrid Information Technology, 2008, pp. 796–801. <http://dx.doi.org/10.1109/ICHIT.2008.261>.
- [28] R. Riaz, K.-H. Kim, H.F. Ahmed, Security analysis survey and framework design for IP connected LoWPANs, in: 2009 International Symposium on Autonomous Decentralized Systems, 2009, pp. 1–6. <http://dx.doi.org/10.1109/ISADS.2009.5207373>.
- [29] A. Dvir, T. Holczer, L. Buttyan, VeRA - version number and rank authentication in RPL, in: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 709–714. <http://dx.doi.org/10.1109/MASS.2011.76>.
- [30] M. Wazid, A.K. Das, S. Kumari, M.K. Khan, Design of sinkhole node detection mechanism for hierarchical wireless sensor networks, Sec. Commun. Netw.9 (17) (2016) 4596–4614. <http://dx.doi.org/10.1002/sec.1652>.
- [31] J. Granjal, E. Monteiro, J.S. Silva, Enabling network-layer security on IPv6 wireless sensor networks, in: 2010 IEEE Global Telecommunications Conference

- GLOBECOM 2010, 2010, pp. 1–6. <http://dx.doi.org/10.1109/GLOCOM.2010.5684293>.
- [32] S. Raza, T. Voigt, V. Jutvik, Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security, in: Proceedings of the IETF Workshop on Smart Object Security, vol. 23, 2012.
 - [33] M.H. Ibrahim, Octopus: An edge-fog mutual authentication scheme, *Internat. J. Netw. Secur.* 18 (6) (2016) 1089–1101.
 - [34] M. Henze, B. Wolters, R. Matzutt, T. Zimmermann, K. Wehrle, Distributed configuration, authorization and management in the cloud-based internet of things, in: 2017 IEEE Trustcom/BigDataSE/ICSS, 2017, pp. 185–192. <http://dx.doi.org/10.1109/Trustcom/BigDataSE/ICSS.2017.236>.
 - [35] M. Sethi, J. Arkko, A. Kernen, End-to-end security for sleepy smart object networks, in: 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 964–972. <http://dx.doi.org/10.1109/LCNW.2012.6424089>.
 - [36] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (CoAP), 2014. URL <https://tools.ietf.org/html/rfc7252>.
 - [37] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.
 - [38] C.H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in Internet-of-Things sensory environments, *Ad Hoc Netw.* 18 (Suppl. C) (2014) 85–101. <http://dx.doi.org/10.1016/j.adhoc.2013.02.008>.
 - [39] Dean, 51% attack, 2015. URL <http://cryptorials.io/glossary/51-attack/>.
 - [40] H. Mayer, Ecdsa security in bitcoin and ethereum: a research survey, 2016. URL <http://blog.coinfabrik.com/wp-content/uploads/2016/06/ECDSA-Security-in-Bitcoin-and-Ethereum-a-Research-Survey.pdf>.
 - [41] S. Alliance, Know your ransomware: Ctb-locker, 2017. URL <https://www.secalliance.com/blog/ransomware-ctb-locker/>.
 - [42] Wikipedia, Wannacry ransomware attack, 2017. URL https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.
 - [43] N. Christin, Traveling the silk road: A measurement analysis of a large anonymous online marketplace, in: The 22nd International Conference on World Wide Web, 2013, pp. 213–224.
 - [44] H. Treasury, UK national risk assessment of money laundering and terrorist financing, 2015. URL https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf.
 - [45] A. Miller, M. Möser, K. Lee, A. Narayanan, An empirical analysis of linkability in the monero blockchain, 2017. ArXiv preprint: arXiv:1704.04299.
 - [46] A. Juels, A. Kosba, E. Shi, The ring of gyges: Investigating the future of criminal smart contracts, in: The ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 283–295.

- [47] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, 2017, pp. 164–186.
- [48] T. Chen, X. Li, X. Luo, X. Zhang, Under-optimized smart contracts devour your money, in: IEEE 24th International Conference on Software Analysis, Evolution and Reengineering, SANER, 2017, pp. 442–446.
- [49] E. Community, Long-term gas cost changes for io-heavy operations to mitigate transaction spam attacks, 2016. URL <https://github.com/ethereum/EIPs/issues/150>.
- [50] I. Eyal, E.G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, in: Financial Cryptography and Data Security - 18th International Conference, in: Lecture Notes in Computer Science, vol. 8437, 2014, pp. 436–454.
- [51] M. Apostolaki, A. Zohar, L. Vanbever, Hijacking bitcoin: Routing attacks on cryptocurrencies, in: IEEE Symposium on Security and Privacy, 2017, pp. 375–392.
- [52] Gautham, Ethereum network comes across yet another dos attack, 2016. URL <http://www.newsbtc.com/2016/09/23/ethereum-dao-attack-attack-platforms-credibility/>.
- [53] D. Research, Pakistan hijacks youtube, 2008. URL <http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/>.
- [54] E. Heilman, A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoin’s peer to-peer network, in: 24th USENIX Security Symposium, 2015, pp. 129–144.
- [55] A. Kiayias, G. Panagiotakos, On trees, chains and fast transactions in the blockchain, 2016. URL <https://eprint.iacr.org/2016/545.pdf>.
- [56] C. Natoli, V. Gramoli, The balance attack against proof-of-work blockchains: The r3 testbed as an example, 2016. ArXiv preprint: [arXiv:org/1612.09426](https://arxiv.org/abs/1612.09426).
- [57] Ali Dorri, Salil S. Kanhere, and Raja Jurdak, Blockchain in Internet of Things: Challenges and Solutions.
- [58] Fangfang Dai, Yue Shi, Nan Meng, Liang Wei, Zhiguo Ye Security Research Department China Academy of Information and Communications Technology Beijing, China, From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues.
- [59] G. Zyskind, O. Nathan et al., Decentralizing privacy: Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, IEEE, 2015, 180–184.
- [60] M. Young, R. Boutaba, Overcoming adversaries in sensor networks: A survey of theoretical models and algorithmic approaches for tolerating malicious interference, IEEE Commun. Surv. Tutor. 13 (4) (2011) 617–641. <http://dx.doi.org/10.1109/SURV.2011.041311.00156>.
- [61] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc ’05, ACM, New York, NY, USA, 2005, pp. 46–57. <http://dx.doi.org/10.1145/1062689.1062697>.

- [62] G. Noubir, G. Lin, Low-power DoS attacks in data wireless LANs and countermeasures, *SIGMOBILE Mob. Comput. Commun. Rev.* 7 (3) (2003) 29–30.
- [63] W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel surfing and spatial retreats: Defenses against wireless denial of service, in: *Proceedings of the 3rd ACM Workshop on Wireless Security, WiSe '04*, ACM, New York, NY, USA, 2004, pp. 80–89. <http://dx.doi.org/10.1145/1023646.1023661>.
- [64] T. Pecorella, L. Brilli, L. Muchhi, The role of physical layer security in IoT: A novel perspective, *Information* 7 (3) (2016).
- [65] S.H. Chae, W. Choi, J.H. Lee, T.Q.S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, *Trans. Info. for. Sec.* 9 (10) (2014) 1617–1628. <http://dx.doi.org/10.1109/TIFS.2014.2341453>.
- [66] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, *IEEE Signal Process. Mag.* 30 (5) (2013) 29–40.
- [67] M. Demirbas, Y. Song, An RSSI-based scheme for sybil attack detection in wireless sensor networks, in: *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM '06*, IEEE Computer Society, Washington, DC, USA, 2006, pp. 564–570. <http://dx.doi.org/10.1109/WOWMOM.2006.27>.
- [68] Y. Chen, W. Trappe, R.P. Martin, Detecting and localizing wireless spoofing attacks, in: *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2017, pp. 193–202.
- [69] Q. Li, W. Trappe, Light-weight detection of spoofing attacks in wireless networks, in: *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 2006, pp. 845–851.
- [70] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-Based detection of sybil attacks in wireless networks, *IEEE Transa. Inf. Forensics Secur.* 4 (3) (2009) 492–503.
- [71] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, Fingerprints in the ether: Using the physical layer for wireless authentication, in: *2007 IEEE International Conference on Communications*, 2007, pp. 4646–4651. <http://dx.doi.org/10.1109/ICC.2007.767>.
- [72] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.
- [73] T. Bhattasali, R. Chaki, A survey of recent intrusion detection systems for wireless sensor network, in: D.C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, D. Nagamalai (Eds.), *Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15–17, 2011*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 268–280.
- [74] H. Kim, Protection against packet fragmentation attacks at 6LoWPAN adaptation layer, in: *2008 International Conference on Convergence and Hybrid Information Technology*, 2008, pp. 796–801. <http://dx.doi.org/10.1109/ICHIT.2008.261>.

- [75] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN Fragmentation attacks and mitigation mechanisms, in: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, ACM, New York, NY, USA, 2013, pp. 55–66. <http://dx.doi.org/10.1145/2462096.2462107>.
- [76] R. Riaz, K.-H. Kim, H.F. Ahmed, Security analysis survey and framework design for IP connected LoWPANs, in: 2009 International Symposium on Autonomous Decentralized Systems, 2009, pp. 1–6. <http://dx.doi.org/10.1109/ISADS.2009.5207373>.
- [77] R. Harkanson, Y. Kim, Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications, in: Proceedings of the 12th Annual Conference on Cyber and Information Security Research, CISRC '17, ACM, New York, NY, USA, 2017, pp. 6:1–6:7. <http://dx.doi.org/10.1145/3064814.3064818>.
- [78] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN Fragmentation attacks and mitigation mechanisms, in: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, ACM, New York, NY, USA, 2013, pp. 55–66. <http://dx.doi.org/10.1145/2462096.2462107>.
- [79] A. Dvir, T. Holczer, L. Buttyan, VeRA - version number and rank authentication in RPL, in: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 709–714. <http://dx.doi.org/10.1109/MASS.2011.76>.
- [80] D. Eastlake, P.E. Jones, RFC 3174 - US Secure Hash Algorithm 1 (SHA1), 2001. URL <https://tools.ietf.org/html/rfc3174>.
- [81] H. Krawczyk, M. Bellare, R. Canetti, HMAC: keyed-hashing for message authentication, 1997. URL <https://tools.ietf.org/rfc/rfc2104.txt>.
- [82] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126. <http://dx.doi.org/10.1145/359340.359342>.
- [83] K. Weekly, K. Pister, Evaluating sinkhole defense techniques in RPL networks, in: Proceedings of the 2012 20th IEEE International Conference on Network Protocols (ICNP), ICNP '12, IEEE Computer Society, Washington, DC, USA, 2012, pp. 1–6. <http://dx.doi.org/10.1109/ICNP.2012.6459948>.
- [84] F. Ahmed, Y.-B. Ko, Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks, Secur. Commun. Netw. 9 (18) (2016) 5143–5154 SCN-16-0443.R1.
- [85] A.A. Pirzada, C. McDonald, Circumventing sinkholes and wormholes in wireless sensor networks, in: International Workshop on Wireless Ad-Hoc Networks, 2005.
- [86] W. Wang, J. Kong, B. Bhargava, M. Gerla, Visualisation of wormholes in underwater sensor networks: A distributed approach, Int. J. Secur. Netw. 3 (1) (2008) 10–23.
- [87] M. Wazid, A.K. Das, S. Kumari, M.K. Khan, Design of sinkhole node detection mechanism for hierarchical wireless sensor networks, Sec. Commun. Netw. 9 (17) (2016) 4596–4614. <http://dx.doi.org/10.1002/sec.1652>.

- [88] I. Krontiris, T. Dimitriou, T. Giannetsos, M. Mpasoukos, Intrusion detection of sinkhole attacks in wireless sensor networks, in: M. Kutylowski, J. Cichoń, P. Kubiak (Eds.), *Algorithmic Aspects of Wireless Sensor Networks: Third International Workshop, ALGOSENSORS 2007*, Wroclaw, Poland, July 14, 2007, Revised Selected Papers, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 150–161.
- [89] I. Raju, P. Parwekar, Detection of sinkhole attack in wireless sensor network, in: S.C. Satapathy, K.S. Raju, J.K. Mandal, V. Bhateja (Eds.), *Proceedings of the Second International Conference on Computer and Communication Technologies: IC3T 2015*, Volume 3, Springer India, New Delhi, 2016, pp. 629–636.
- [90] E.C.H. Ngai, J. Liu, M.R. Lyu, On the intruder detection for sinkhole attack in wireless sensor networks, in: *2006 IEEE International Conference on Communications*, vol. 8, 2006, pp. 3383–3389. <http://dx.doi.org/10.1109/ICC.2006.255595>.
- [91] R. Poovendran, L. Lazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks, *Wirel. Netw.* 13 (1) (2007) 27–59. <http://dx.doi.org/10.1007/s11276-006-3723-x>.
- [92] S.A. Salehi, M.A. Razzaque, P. Naraei, A. Farrokhtala, Detection of sinkhole attack in wireless sensor networks, in: *2013 IEEE International Conference on Space Science and Communication (IconSpace)*, 2013, pp. 361–365. <http://dx.doi.org/10.1109/IconSpace.2013.6599496>.
- [93] C. Tumrongwittayapak, R. Varakulsiripunth, Detecting Sinkhole attacks in wireless sensor networks, in: *2009 ICCAS-SICE*, 2009, pp. 1966–1971.
- [94] Jang, T. Kwon, J. Song, A time-based key management protocol for wireless sensor networks, in: *Proceedings of the 3rd International Conference on Information Security Practice and Experience, ISPEC'07*, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 314–328.
- [95] S. Sharmila, G. Umamaheswari, Detection of sinkhole attack in wireless sensor networks using message digest algorithms, in: *2011 International Conference on Process Automation, Control and Computing*, 2011, pp. 1–6. <http://dx.doi.org/10.1109/PACC.2011.5978973>.
- [96] H. Yu, M. Kaminsky, P.B. Gibbons, A. Flaxman, SybilGuard: defending against sybil attacks via social networks, *SIGCOMM Comput. Commun. Rev.* 36 (4) (2006) 267–278. <http://dx.doi.org/10.1145/1151659.1159945>.
- [97] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things, *IEEE Internet Things J.* 1 (5) (2014) 372–383. <http://dx.doi.org/10.1109/JIOT.2014.2344013>.
- [98] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, A. Panconesi, SoK: the evolution of sybil defense via social networks, in: *Proceedings of the 2013 IEEE Symposium on Security and Privacy, SP '13*, IEEE Computer Society, Washington, DC, USA, 2013, pp. 382–396. <http://dx.doi.org/10.1109/SP.2013.33>.
- [99] Q. Cao, X. Yang, SeybilFence: Improving Social-Graph-Based Sybil Defenses with User Negative Feedback. Tech. Rep., Duke, Duke University, USA, 2012 URL <https://users.cs.duke.edu/~qiangcao/>.

- [100] A. Mohaisen, N. Hopper, Y. Kim, Keep your friends close: incorporating trust into social network-based sybil defenses, in: 2011 Proceedings IEEE INFOCOM, 2011, pp. 1943–1951. <http://dx.doi.org/10.1109/INFCOM.2011.5934998>.
- [101] G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, B.Y. Zhao, Social turing tests: Crowdsourcing sybil detection, in: Symposium on Network and Distributed System Security, NDSS, 2013.
- [102] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things, *IEEE Internet Things J.* 1 (5) (2014) 372–383. <http://dx.doi.org/10.1109/JIOT.2014.2344013>.
- [103] D. Quercia, S. Hailes, Sybil attacks against mobile users: Friends and foes to the rescue, in: Proceedings of the 29th Conference on Information Communications, INFOCOM'10, IEEE Press, Piscataway, NJ, USA, 2010, pp. 336–340. URL <http://dl.acm.org/citation.cfm?id=1833515.1833583>.
- [104] S. Kent, RFC 4302 - ip authentication header, 2005. URL <https://tools.ietf.org/html/rfc4302>.
- [105] S. Kent, RFC 4303 - IP Encapsulating Security Payload (ESP), 2005. URL <https://tools.ietf.org/html/rfc4303>.
- [106] J. Granjal, E. Monteiro, J.S. Silva, Enabling network-layer security on IPv6 wireless sensor networks, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–6. <http://dx.doi.org/10.1109/GLOCOM.2010.5684293>.
- [107] D. Eastlake, P.E. Jones, RFC 3174 - US Secure Hash Algorithm 1 (SHA1), 2001. URL <https://tools.ietf.org/html/rfc3174>.
- [108] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing communication in 6LoWPAN with compressed IPsec, in: 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011, pp. 1–8. <http://dx.doi.org/10.1109/DCOSS.2011.5982177>.
- [109] S. Raza, T. Chung, S. Duquennoy, D. Yazar, T. Voigt, U. Roedig, Securing Internet of Things with Lightweight IPsec, SICS, Lancaster University, UK, 2011. URL <http://soda.swedishict.se/4052/2/reportRevised.pdf>.
- [110] S. Raza, S. Duquennoy, J. Hglund, U. Roedig, T. Voigt, Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN, *Secur. Commun. Netw.* 7 (12) (2014) 2654–2668. <http://dx.doi.org/10.1002/sec.406>.
- [111] J.W. Hui, P. Thubert, Compression Format for IPv6 Datagrams in 6LoWPAN Networks draft-ietf-6lowpan-hc-13, 2010. URL <https://tools.ietf.org/html/draft-ietf-6lowpan-hc-13>.
- [112] J. Granjal, E. Monteiro, J.S. Silva, Network-layer security for the Internet of Things using TinyOS and BLIP, *Int. J. Commun. Syst.* 27 (10) (2014) 1938– 1963. <http://dx.doi.org/10.1002/dac.2444>.
- [113] G. Montenegro, N. Kushalnagar, J.W. Hui, D.E. Culler, Transmission of IPv6 Packets over IEEE 802.15.4 Networks, 2007. URL <https://tools.ietf.org/html/rfc4944>.

- [114] P.N. Mahalle, B. Anggorojati, N.R. Prasad, R. Prasad, Identity authentication and capability based access control (iacac) for the internet of things, *J. Cyber Secur. Mobility* 1 (4) (2013) 309–348.
- [115] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle, 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 956–963. <http://dx.doi.org/10.1109/LCNW.2012.6424088>.
- [116] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle, {DTLS} based security and two-way authentication for the Internet of Things, *Ad Hoc Netw.* 11 (8) (2013) 2710–2723. <http://dx.doi.org/10.1016/j.adhoc.2013.05.003>.
- [117] S.L. Kinney, *Trusted Platform Module Basics: Using TPM in Embedded Systems*, Newnes, Newton, MA, USA, 2006.
- [118] X. Huang, Y. Xiang, E. Bertino, J. Zhou, L. Xu, Robust multi-factor authentication for fragile communications, *IEEE Trans. Dependable Secure Comput.* 11 (6) (2014) 568–581. <http://dx.doi.org/10.1109/TDSC.2013.2297110>.
- [119] M. Henze, B. Wolters, R. Matzutt, T. Zimmermann, K. Wehrle, Distributed configuration, authorization and management in the cloud-based internet of things, in: 2017 IEEE Trustcom/BigDataSE/ICSS, 2017, pp. 185–192. <http://dx.doi.org/10.1109/Trustcom/BigDataSE/ICSS.2017.236>.
- [120] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, Security and privacy for cloud-based IoT: Challenges, *IEEE Commun. Mag.* 55 (1) (2017) 26–33. <http://dx.doi.org/10.1109/MCOM.2017.1600363CM>.
- [121] J.M. Bohli, A. Skarmeta, M.V. Moreno, D. Garca, P. Langendörfer, SMARTIE project: Secure IoT data management for smart cities, in: 2015 International Conference on Recent Advances in Internet of Things (RIoT), 2015, pp. 1–6. <http://dx.doi.org/10.1109/RIOT.2015.7104906>.
- [122] M. Brachmann, O. Garcia-Morchon, M. Kirsche, Security for practical CoAP applications: Issues and solution approaches, in: 10th GI/ITG KuVS Fachgespräch Sensornetze (FGSN 2011), 2011.
- [123] J. Granjal, E. Monteiro, J.S. Silva, End-to-end transport-layer security for internet-integrated sensing applications with mutual and delegated ecc public-key authentication, in: 2013 IFIP Networking Conference, 2013, pp.1–9.
- [124] G. Peretti, V. Lakkundi, M. Zorzi, BlinkToSCoAP: An end-to-end security framework for the Internet of Things, in: 2015 7th International Conference on Communication Systems and Networks (COMSNETS), 2015, pp. 1–6. <http://dx.doi.org/10.1109/COMSNETS.2015.7098708>.
- [125] D.U. Sinthan, M.-S. Balamurugan, Identity authentication and capability based access control (IACAC) for the Internet of Things, *J. Cyber Secur. Mob.* 1 (4) (2013) 309–348.
- [126] H.C. Phls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E.Z. Tragos, R.D. Rodriguez, T. Mouroutis, RERUM: Building a reliable IoT upon privacyand security-enabled smart objects, in: 2014 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2014, pp. 122–127. <http://dx.doi.org/10.1109/WCNCW.2014.6934872>.

- [127] S. Prez, J.A. Martnez, A.F. Skarmeta, M. Mateus, B. Almeida, P. Mal, ARMOUR: Large-scale experiments for IoT security trust, in: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016, pp. 553–558. <http://dx.doi.org/10.1109/WF-IoT.2016.7845504>.
- [128] BUTLER-Consortium, BUTLER smartlife –uBiquitous, secUre inTernet-ofthings with Location and contExt-awaReness, 2014. URL <http://cordis.europa.eu/docs/projects/cnect/1/287901/080/deliverables/001-287901BUTLERD25.pdf>.
- [129] S. Raza, D. Tralalza, T. Voigt, 6LoWPAN compressed DTLS for CoAP, in: 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, 2012, pp. 287–289. <http://dx.doi.org/10.1109/DCOSS.2012.55>.
- [130] M. Demirbas, Y. Song, An RSSI-based scheme for sybil attack detection in wireless sensor networks, in: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM '06, IEEE Computer Society, Washington, DC, USA, 2006, pp. 564–570. <http://dx.doi.org/10.1109/WOWMOM.2006.27>.
- [131] D. Giusto, A. Iera, G. Morabito, L. Atzori, The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, Springer Publishing Company, Incorporated, 2014.
- [132] S. Raza, T. Voigt, V. Jutvik, Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security, in: Proceedings of the IETF Workshop on Smart Object Security, vol. 23, 2012.
- [133] N. Park, N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors 6 (1) (2016) 20–20.
- [134] M.H. Ibrahim, Octopus: An edge-fog mutual authentication scheme, Internat. J. Netw. Secur. 18 (6) (2016) 1089–1101.
- [135] R. Hummen, H. Wirtz, J.H. Ziegeldorf, J. Hiller, K. Wehrle, Tailoring end-to-end IP security protocols to the Internet of Things, in: 2013 21st IEEE International Conference on Network Protocols (ICNP), 2013, pp. 1–10. <http://dx.doi.org/10.1109/ICNP.2013.6733571>.
- [136] M. Brachmann, S.L. Keoh, O.G. Morchon, S.S. Kumar, End-to-end transport security in the IP-based Internet of Things, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–5. <http://dx.doi.org/10.1109/ICCCN.2012.6289292>.
- [137] J. Granjal, E. Monteiro, J.S. Silva, Application-layer security for the WoT: extending CoAP to support end-to-end message security for internet-integrated sensing applications, in: International Conference on Wired/Wireless Internet Communication, Springer Berlin Heidelberg, 2013, pp. 140–153.
- [138] M. Brachmann, O. Garcia-Morchon, S.-L. Keoh, S.S. Kumar, Security considerations around end-to-end security in the IP-based Internet of Things, in: 2012 Workshop on Smart Object Security, in Conjunction with IETF83, 2012, pp. 1–3.
- [139] M. Sethi, J. Arkko, A. Kernen, End-to-end security for sleepy smart object networks, in: 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 964–972. <http://dx.doi.org/10.1109/LCNW.2012.6424089>.

- [140] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.
- [141] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M.A. Spirito, The VIRTUS middleware: An XMPP based architecture for secure IoT communications, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–6. <http://dx.doi.org/10.1109/ICCCN.2012.6289309>.
- [142] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M.A. Spirito, The VIRTUS middleware: An XMPP based architecture for secure IoT communications, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–6. <http://dx.doi.org/10.1109/ICCCN.2012.6289309>.
- [143] A. Gmez-Goiri, P. Ordua, J. Diego, D.L. de Ipiña, Otsopack: Lightweight semantic framework for interoperable ambient intelligence applications, *Comput. Hum. Behav.* 30 (Suppl. C) (2014) 460–467. <http://dx.doi.org/10.1016/j.chb.2013.06.022>.
- [144] C.H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in Internet-of-Things sensory environments, *Ad Hoc Netw.* 18 (Suppl. C) (2014) 85–101. <http://dx.doi.org/10.1016/j.adhoc.2013.02.008>.
- [145] OneM2M, Security solutions –OneM2M Technical Specification, 2017. URL <http://onem2m.org/technical/latest-drafts>.
- [146] H.G.C. Ferreira, R.T. de Sousa, F.E.G. de Deus, E.D. Canedo, Proposal of a secure, deployable and transparent middleware for Internet of Things, in: 2014 9th Iberian Conference on Information Systems and Technologies, CISTI, 2014, pp. 1–4. <http://dx.doi.org/10.1109/CISTI.2014.6877069>.
- [147] A.M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Crypto-Currencies*, first ed., O'Reilly Media, Inc., 2014.
- [148] The-Bitcoin-Foundation, How does Bitcoin work?, 2014. URL <https://bitcoin.org/en/how-it-works>.
- [149] BitInfoCharts, Block - Bitcoin Wiki, 2016. URL <https://en.bitcoin.it/wiki/Block>.
- [150] EtherScan, Ethereum Average BlockTime Chart, 2016. URL <https://etherscan.io/chart/blocktime>.
- [151] Linux-Foundation, Blockchain technologies for business, 2017. URL <https://www.hyperledger.org/>.
- [152] C. Kuhlman, What is eris? 2016 Edition, 2016. URL <https://monax.io/2016/04/03/wtf-is-eris/>.
- [153] Stellar, Stellar network overview, 2014. URL <https://www.stellar.org/developers/guides/get-started/>.
- [154] Ripple, Ripple network, 2013. URL <https://ripple.com/network>.
- [155] All-In-Bits, Introduction to tendermint, 2017. URL <https://tendermint.com/intro>.
- [156] J. Mattila, The blockchain phenomenon: The disruptive potential of distributed consensus architectures, ETLA working papers: Elinkeinoelämän Tutkimuslaitos,

- Research Institute of the Finnish Economy, 2016 URL <https://books.google.com.pk/books?id=StNQnQAACAAJ>.
- [157] EconoTimes, Safeshare releases first blockchain insurance solution for sharing economy, 2016. URL <https://www.econotimes.com/SafeShare-Releases-First-Blockchain-Insurance-Solution-For-Sharing-Economy-181326>.
 - [158] IBM, IBM blockchain based on hyperledger fabric from the linux foundation, 2017. URL <https://www.ibm.com/blockchain/hyperledger.html>.
 - [159] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Crypto-Currencies, first ed., O'Reilly Media, Inc., 2014.
 - [160] I. Friese, J. Heuer, N. Kong, Challenges from the Identities of Things: Introduction of the Identities of Things discussion group within Kantara initiative, in: 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 1–4. <http://dx.doi.org/10.1109/WF-IoT.2014.6803106>.
 - [161] P.N. Mahalle, B. Anggorojati, N.R. Prasad, R. Prasad, Identity authentication and capability based access control (iacac) for the internet of things, J. Cyber Secur. Mobility 1 (4) (2013) 309–348.
 - [162] P. Otte, M. de Vos, J. Pouwelse, TrustChain: A Sybil-resistant scalable blockchain, Future Gener. Comput. Syst. (2017). <http://dx.doi.org/10.1016/j.future.2017.08.048>.
 - [163] L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smart pool: Practical decentralized pooled mining, in: USENIX Security Symposium, 2017.
 - [164] R. consortium, R3, 2017. URL <https://www.r3.com/>.
 - [165] P. technologies, Parity, 2017. URL <https://parity.io/>.
 - [166] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: The 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269.
 - [167] L. Luu, D. Chu, H. Olickel, P. Saxena, A. Hobor, Oyente: An analysis tool for smart contracts, 2016. URL <https://www.comp.nus.edu.sg/~loiluu/oyente.html>.
 - [168] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: IEEE Symposium on Security and Privacy, 2016, pp. 839–858.
 - [169] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier: An authenticated data feed for smart contracts, in: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 270–282.
 - [170] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier, 2017. URL <http://www.town-crier.org/>.
 - [171] Haber, S.; Stornetta, W.S. How to time-stamp a digital document. In Proceedings of the Conference on the Theory and Application of Cryptography, Sydney, NSW, Australia, 8–11 January 1990; Springer: Berlin/Heidelberg, Germany, 1990.
 - [172] Jin Ho Park and Jong Hyuk Park, Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions

- [173] Mann, C.; Loebenberg, D. Two-factor authentication for the Bitcoin protocol. In International Workshop on Security and Trust Management; Springer International Publishing: Cham, Switzerland, 2015.
- [174] Vasek, M.; Thornton, M.; Moore, T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014.
- [175] Bastiaan, M. Preventing the 51%-Attack: A Stochastic Analysis of Two Phase Proof of Work in Bitcoin. Available online: <http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf> (accessed on 29 June 2017).
- [176] Karame, G.O.; Elli, A.; Srdjan, C. Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, CA, USA, 16–18 October 2012.
- [177] L. A. Linn and M. B. Koo, Blockchain for health data and its potential use in health it and health care related research, in ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, 2016.
- [178] G. Wood, Ethereum: A secure decentralised generalised transaction ledger, Ethereum Project Yellow Paper, 151 (2014), 1- 32.
- [179] V. Vishumurthy, S. Chandrakumar and E. G. Sirer, Karma: A secure economic framework for peer-to-peer resource sharing, in Proceedings of the 2003 Workshop on Economics of Peer-to-Peer Systems, Berkeley CA, 2003.
- [180] A. Back et al., Hashcash-a denial of service counter-measure.
- [181] F. Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials, 18 (2016), 2084- 2123.
- [182] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, Blockchain: A distributed solution to automotive security and privacy, IEEE Communications Magazine, 55 (2017), 119-125.
- [183] M. Steger, C. Boano, M. Karner, J. Hillebrand, W. Rom and K. R• omer, Secup: Secure and efficient wireless software updates for vehicles, in Digital System Design (DSD), 2016 Euromicro Conference on, IEEE, 2016, 628- 636.
- [184] H. Heinecke, K.-P. Schnelle, H. Fennel, J. Bortolazzi, L. Lundh, J. Le our, J.-L. Mate, K. Nishikawa and T. Scharnhorst, Automotive Open System Architecture-An Industry-Wide Initiative to Manage the Complexity of Emerging Automotive E/E-Architectures, Technical report, SAE Technical Paper, 2004.
- [185] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, Blockchain: A distributed solution to automotive security and privacy, IEEE Communications Magazine, 55 (2017), 119-125.

- [186] F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos and X. Rong, Data mining for the internet of things: Literature review and challenges, *International Journal of Distributed Sensor Networks*, 11 (2015), 431047.
- [187] A. Dorri, S. S. Kanhere and R. Jurdak, Blockchain in internet of things: challenges and solutions, *arXiv preprint*, arXiv:1608.05187.
- [188] F. Gierschner, Bitcoin and beyond.
- [189] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang and Z. Han, Performance analysis and application of mobile blockchain, *arXiv preprint*, arXiv:1712.03659.
- [190] Z. Xiong, S. Feng, D. Niyato, P. Wang and Z. Han, Edge computing resource management and pricing for mobile blockchain, *arXiv preprint*, arXiv:1710.01567.
- [191] N. Barnas, Blockchains in national defense: Trustworthy systems in a trustless world, Blue Horizons Fellowship, Air University, Maxwell Air Force Base, Alabama.
- [192] W. Tirenin and D. Faatz, A concept for strategic cyber defense, in *Military Communications Conference Proceedings*, 1999. MILCOM 1999. IEEE, vol. 1, IEEE, 1999, 458- 463.
- [193] K. Korpela, J. Hallikas and T. Dahlberg, Digital supply chain transformation toward blockchain integration, in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017, 10pp.
- [194] X. Liang, J. Zhao, S. Shetty and D. Li, Towards data assurance and resilience in iot using blockchain, in *Military Communications Conference (MILCOM)*, MILCOM 2017-2017 IEEE, IEEE, 2017, 261- 266.
- [195] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in *Big Data (BigData Congress)*, 2017 IEEE International Congress on, IEEE, 2017, 557- 564.
- [196] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in *Big Data (BigData Congress)*, 2017 IEEE International Congress on, IEEE, 2017, 557-564.
- [197] A. S. Elmaghraby and M. M. Losavio, Cyber security challenges in smart cities: Safety, security and privacy, *Journal of Advanced Research*, 5 (2014), 491-497.
- [198] J. Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar et al., Blockchains for business process management-challenges and opportunities, *ACM Transactions on Management Information Systems (TMIS)*, 9 (2018), Article No. 4.
- [199] J. Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar et al., Blockchains for business process management-challenges and opportunities, *ACM Transactions on Management Information Systems (TMIS)*, 9 (2018), Article No. 4.
- [200] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V.C.M. Leung, Y.L. Guan, Wireless energy harvesting for the Internet of Things, *IEEE Commun. Mag.* 53 (6) (2015) 102–108. <http://dx.doi.org/10.1109/MCOM.2015.7120024>.

- [201] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, *Future Gener. Comput. Syst.* (2017). <http://dx.doi.org/10.1016/j.future.2017.08.020>.
- [202] S. Ji, Z. Cai, M. Han and R. Beyah, Whitespace measurement and virtual backbone construction for cognitive radio networks: From the social perspective, in *Sensing, Communication, and Networking (SECON)*, 2015 12th Annual IEEE International Conference on, IEEE, 2015, 435- 443.
- [203] P. Jin Ho and P. Jong Hyuk, Blockchain security in cloud computing: Use cases, challenges, and solutions., *Symmetry* (20738994), 9 (2017), 1- 13.
- [204] Z. Duan, M. Yan, Z. Cai, X. Wang, M. Han and Y. Li, Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems, *Sensors*, 16 (2016), p481.
- [205] A. Kiayias and G. Panagiotakos, Speed-security tradeoffs in blockchain protocols, *IACR Cryptology ePrint Archive*, 2015 (2015), 1019.
- [206] V. King and J. Saia, Scalable byzantine computation, *ACM SIGACT News*, 41 (2010), 89- 104.
- [207] K. Korpela, J. Hallikas and T. Dahlberg, Digital supply chain transformation toward blockchain integration, in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017, 10pp.
- [208] R. Kotla, L. Alvisi, M. Dahlin, A. Clement and E. Wong, Zyzzyva: Speculative byzantine fault tolerance, in *ACM SIGOPS Operating Systems Review*, ACM, 41 (2007), 45-58.
- [209] D. Larimer, Delegated proof-of-stake white paper, 2014
- [210] D. Larimer, Transactions as proof-of-stake, 2013.