Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Ανάλυση των ευπαθειών και επιθέσεων στο Hyperledger Fabric

Ιωάννης Χρηστίδης

Επιβλέπων Καθηγητής
Νικόλαος Κολοκοτρώνης

Δεκέμβριος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ανάλυση των ευπαθειών και επιθέσεων στο Hyperledger Fabric

Ιωάννης Χρηστίδης

Επιβλέπων Καθηγητής
Νικόλαος Κολοκοτρώνης

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

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Δεκέμβριος 2020

Περίληψη

Ένα δίκτυο blockchain αποτελεί ένα κατανεμημένο σύστημα για την καταγραφή του ιστορικού των συναλλαγών που πραγματοποιούνται μέσα σε αυτό, εντός ενός κοινού μητρώου, παρέχοντας με αυτόν τον τρόπο συνέπεια και σταθερότητα, καθώς όλοι οι συμμετέχοντες έχουν την ίδια εικόνα του αρχείου στο οποίο από τη στιγμή που κάποια αλλαγή γίνεται δεκτή δεν μπορεί πλέον να αλλάξει. Η blockchain τεχνολογία συνάντησε ευρεία αποδοχή από την εφαρμογή της στα δημοφιλή κρυπτονομίσματα Bitcoin, όμως σήμερα κερδίζει ολοένα και μεγαλύτερη δυναμική και σε άλλους τομείς και από πολλούς ερευνητές θεωρείται ως μια αλλαγή που προκαλεί ανάλογες προσδοκίες με αυτές που δημιούργησε το λογισμικό ανοιχτού κώδικα ή ακόμη και το Διαδίκτυο. Το Hyperledger Fabric αποτελεί ένα blockchain σύστημα με χρήση αδειών, καθώς η οποιαδήποτε εγγραφή στο αρχείο απαιτεί ορισμένα διαπιστευτήρια από το χρήστη. Το Hyperledger Fabric βασίζεται σε μερικά αξιόπιστα μέρη και συγκεντρωτικές υπηρεσίες για την παροχή μιας γενικευμένης πλατφόρμας για μπλοκ συστοιχίες. Ωστόσο, αυτά μπορούν να αξιοποιηθούν κακόβουλα και μπορεί να οδηγήσουν σε επιθέσεις που δεν θα ήταν εφαρμόσιμες σε ένα παραδοσιακό δίκτυο αποκλεισμού. Η αρθρωτή αρχιτεκτονική του Hyperledger Fabric προωθεί τη χρήση πρωτοκόλλων αυτοεξυπηρέτησης, ωστόσο, τα συστήματα που είναι ενσωματωμένα στα πρωτόκολλα αυτά είναι ασφαλή όσο είναι τα ίδια τα πρωτόκολλα. Το Hyperledger Fabric είναι η πιο δημοφιλής πλατφόρμα αλυσιδωτού κώδικα σήμερα. Με μεγάλες επενδύσεις από τις μεγάλες εταιρείες τεχνολογίας (Intel, Cisco, IBM) καθώς και σημαντικούς χρηματοπιστωτικούς οργανισμούς (JP Morgan, Deutsche Bank) είναι σαφές ότι η τεχνολογία αυτή συγκεντρώνει την προσοχή. Ωστόσο, στη διεθνή βιβλιογραφία δεν απουσιάζουν οι επιθέσεις στο Fabric, όπως η παραβίαση της ασφάλειας από κάποιον κακόβουλο ομότιμο χρήστη, τις επιθέσεις βάσει πρωτοκόλλου, τις ευπάθειες του αλυσιδωτού κώδικα (codechain) και τις επιθέσεις στην αρχιτεκτονική του συστήματος. Σκοπός της συγκεκριμένης εργασίας είναι η περιγραφή των ευπαθειών και των επιθέσεων στο Hyperledger Fabric, καθώς και τα αντιμέτρα που λαμβάνονται για την αντιμετώπισή τους, μέσω της ανασκόπησης της σύγχρονης βιβλιογραφίας.

Summary

A blockchain network is a distributed system for recording the history of transactions carried out within it, within a common register, thus providing consistency and stability, as all participants have the same picture of the book in which from the moment they some change is accepted can no longer be changed. Blockchain technology has gained widespread acceptance from its application in popular Bitcoin cryptocurrencies, but today it is gaining more and more momentum in other areas and is considered by many researchers as a change that meets expectations similar to those created by open source software or even Internet. Hyperledger Fabric is a blockchain system using licenses, as any registration in the book requires certain user credentials. Hyperledger Fabric is based on some reliable parts and centralized services for providing a generalized building permit platform. However, these can be exploited maliciously and can lead to attacks that would not be applicable to a traditional blockade network. Hyperledger Fabric's modular architecture promotes the use of self-service protocols, however, systems built into these protocols are as secure as the protocols themselves. Hyperledger Fabric is the most popular chain code platform today. With large investments from major technology companies (Intel, Cisco, IBM) as well as major financial institutions (JP Morgan, Deutsche Bank) it is clear that this technology is attracting attention. However, in the international literature, attacks on Fabric are not absent, such as the breach of security by an malicious user, protocol-based attacks, vulnerabilities in the codechain code, and attacks on the system's architecture. The purpose of this paper is to describe the vulnerabilities and attacks on Hyperledger Fabric, as well as the countermeasures taken to address them, through a review of modern literature.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή Δρ. Νικόλαο Κολοκοτρώνη για την εμπιστοσύνη που μου έδειξε αναθέτοντας μου το συγκεκριμένο θέμα, τη συνεχή καθοδήγηση και την πολύτιμη βοήθεια του. Επίσης θα ήθελα να ευχαριστήσω τους γονείς μου για την πολύτιμη ηθική στηριξή τους καθ'όλη την δειάρκεια των μεταπτυχιακών μου σπουδών.

Περιεχόμενα

Κεφάλαιο 1
Η Τεχνολογία Blockchain

Η "Τεχνολογία Blockchain (Blockchain Technology - BT)" είναι η βασική τεχνολογία της Bitcoin και έχει προκύψει με μια σειρά υποσχόμενων πιθανών εφαρμογών. Σε λιγότερο από μια δεκαετία, η BT έχει δει επενδύσεις από πολλές εταιρείες, έχει τονώσει τη δημιουργία μιας σειράς κοινοπραξιών και έχει αυξήσει περισσότερα από 3,1 δισεκατομμύρια δολάρια των ΗΠΑ στο συνολικό κεφάλαιο επιχειρηματικού κινδύνου. Οι αγορές κρυπτονομίσματος που δημιουργούνται από την BT εκτιμάται ότι θα φτάσουν σε μια συνολική χρηματιστηριακή αξία μεγαλύτερη των 143 δισεκατομμυρίων δολαρίων των ΗΠΑ. Επιπλέον, η BT έχει εφαρμοστεί στον δημόσιο τομέα, στα ακαδημαϊκά ιδρύματα [19] και οι κυβερνήσεις σχεδιάζουν και αναπτύσσουν τη χρήση του blockchain στο δημόσιο τομέα. Η KPMG ανέφερε το πρώτο εξάμηνο του 2018, οι επενδύσεις στις εταιρείες του UT fintech ήταν 14,2 δισεκατομμύρια δολάρια. Επιπλέον, η BT έχει εφαρμοστεί στο κοινό και οι ιδιωτικοί τομείς με πάνω από το 53% των ερωτηθέντων στην έρευνα της Deloitte δήλωσαν ότι η BT αποτελούσε προτεραιότητα για τους οργανισμούς τους [45].

Η BT υπόσχεται μια νέα διάσταση διεξαγωγής επιχειρηματικών συναλλαγών μεταξύ μη αξιόπιστων οντοτήτων, τα χαρακτηριστικά της οποίας υποστηρίζουν την επαλήθευση, τον εντοπισμό, την επιβεβαίωση της γνησιότητας, την ακεραιότητα και την αμερόληπτη εγγύηση τα οποία εξασφαλίζονται μέσω της κρυπτογράφησης, της διαφάνειας και των αποκεντρωμένων

έξυπνων συμβάσεων όπως και τα έξυπνων λογιστικών βιβλίων. Η ΒΤ προσφέρει όχι μόνο χρονολογικά συνδεδεμένα και αναπαραγόμενα ψηφιακά λογιστικά βιβλία σε αποκεντρωμένη βάση δεδομένων και ανταλλαγή συναλλαγών σε ένα εκτεταμένο δίκτυο μη αξιόπιστων οντοτήτων αλλά και ανεξάρτητες εγγυήσεις επαλήθευσης, οι οποίες εξαλείφουν την ανάγκη να βασίζονται σε μια κεντρική αρχή. Επιπλέον, δεδομένης της απουσίας κεντρικών αρχών, οι υπηρεσίες blockchain είναι σε θέση να παρέχουν καλύτερες ιδιότητες ασφάλειας για συστήματα που διανέμονται μεταξύ διαφορετικών οντοτήτων και μπορούν να εφαρμόζουν σταθερότητα κατά της κατάχρησης και της εποπτείας ακόμη και αν υπάρχει κακόβουλος πληροφοριοδότης.

Δεδομένου ότι η ΒΤ είναι μια πολλά υποσχόμενη τεχνολογία αιχμής, υπάρχουν ανησυχίες για την ευρωστία της [43]. Εάν υπάρχει μια τέτοια αρχή σε ένα σύστημα, η παρεμπόδιση του blockchain ή η παρεμπόδιση της μετάδοσης του περιεχομένου του είναι δυνατή με μια συμπαιγνία μεταξύ των πιο ισχυρών οντοτήτων. Έχουν αναφερθεί πολλές επιθέσεις στον κυβερνοχώρο και έχουν εντοπιστεί πολλές αδυναμίες σε εφαρμογές του blockchain [38]. Ένα πρόσφατο παράδειγμα είναι η επίθεση dusting attack στο δίκτυο Litecoin blockchain, το οποίο δείχνει ότι οι επιτιθέμενοι είναι σε θέση να σπάσουν την ιδιωτικότητα και την ανωνυμία των χρηστών του Bitcoin στέλνοντας μικροσκοπικά ποσά dust coins στα προσωπικά πορτοφόλια των θυμάτων στόχων. Οι επιτιθέμενοι είναι σε θέση να ανιχνεύσουν τη διακρατική δραστηριότητα αυτών των πορτοφολιών πραγματοποιώντας μια συνδυασμένη ανάλυση των διευθύνσεων η οποία είναι σε θέση να εντοπίσει τον ιδιοκτήτη του κάθε πορτοφολιού.

Αυτά τα ελαττώματα εγείρουν ερωτήματα σχετικά με το εάν η ΒΤ μπορεί να παραδώσει στην πράξη τις εγγυήσεις ασφαλείας που υπόσχεται. Η αυξανόμενη χρήση της ΒΤ ως υπηρεσία που παρέχεται από κυβερνήσεις ή μεγάλες επιχειρήσεις, όπως για παράδειγμα ο κλάδος των χρηματοπιστωτικών, έθιξε τις ανησυχίες των χρηστών σχετικά με την ασφάλεια τους. Έχουν δημοσιευθεί αρκετές αναφορές στη ΒΤ σχετικά με τις επιθέσεις και την ευπάθεια της ασφάλειας στον κυβερνοχώρο. Για παράδειγμα, 8.833 υφιστάμενα έξυπνα συμβόλαια του Ethereum είναι ευάλωτα και το συνολικό τους υπόλοιπο είναι 3.068.654 εκατομμύρια Ethers, ποσό ίσο με περίπου 30 εκατομμύρια δολάρια των ΗΠΑ [07].

Οι οικονομικές απώλειες είναι δυνατές λόγω των τρωτών σημείων στις έξυπνες συμβάσεις. Για παράδειγμα, ένας επιτιθέμενος επιτέθηκε στο Mt Gox το 2014, τη μεγαλύτερη πλατφόρμα συναλλαγών Bitcoin, και έκλεψε Bitcoins ίσα με 450 εκατομμύρια δολάρια των ΗΠΑ, γεγονός που οδήγησε στην κατάρρευση του Mt Gox. Άλλο παράδειγμα είναι όταν ένας χάκερ κατόρθωσε να εκμεταλλευτεί μια ευπάθεια και να κλέψει τους Ethers που ήταν ίσοι με περισσότερα από 60

εκατομμύρια δολάρια των ΗΠΑ το 2016 από το DAO, ένα έξυπνο συμβόλαιο στο blockchain του Ethereum. Πρόσφατες έρευνες σχετικά με την ΒΤ όσον αφορά την έννοια της ασφάλειας στον κυβερνοχώρο ασχολούνται κυρίως με τον τρόπο με τον οποίο το blockchain μπορεί να προσφέρει ασφάλεια στα τρέχοντα και τα μελλοντικά συστήματα. Υπάρχει, όμως, μια αδυναμία στις μελέτες σχετικά με τις ευπάθειες στον κυβερνοχώρο της ΒΤ [54].

1.1 Η Έννοια της Τεχνολογίας Blockchain

Το ΒΤ περιλαμβάνει απαραβίαστα και ασφαλισμένα ψηφιακά λογιστικά βιβλία, τα οποία εκτελούνται χωρίς κεντρικό αποθηκευτικό χώρο, ως κατανεμημένο σύστημα και συχνά χωρίς κεντρική αρχή, όπως η κυβέρνηση, η τράπεζα ή μια επιχείρηση. Το ΒΤ επιτρέπει στους χρήστες μιας κοινότητας να αποθηκεύουν συναλλαγές σε έναν κοινό λογαριασμό σε αυτήν την κοινότητα. Οι συναλλαγές δεν μπορούν να αλλάξουν όταν δημοσιεύονται στην κανονική λειτουργία του δικτύου blockchain. Μια νέα κρυπτογράφηση βασισμένη σε blockchain δημιουργήθηκε το 2008 συνδυάζοντας την ιδέα της ΒΤ με άλλες έννοιες και τεχνολογίες πληροφορικής [39].

Το 2009, η ΒΤ έγινε πολύ διάσημη μετά την έναρξη της κρυπτογράφησης Bitcoin, η οποία επέτρεψε τη μεταφορά ψηφιακών μετρητών μέσα σε ένα κατανεμημένο λογιστικό αρχείο. Στο Bitcoin, τα ψηφιακά δικαιώματα των χρηστών μπορούν να υπογραφούν ψηφιακά και να μεταφερθούν σε άλλο χρήστη του Bitcoin. Το blockchain Bitcoin ανακοινώνει δημόσια αυτή τη μεταφορά σε όλους τους χρήστες του δικτύου για να ελέγξει ανεξάρτητα την εγκυρότητα της συναλλαγής. Επιπλέον, μια κατανεμημένη ομάδα χρηστών διαχειρίζεται και διατηρεί ανεξάρτητα το Bitcoin blockchain και μαζί με τους κρυπτογραφικούς μηχανισμούς δημιουργεί την ανθεκτικότητα της ΒΤ σε μεταγενέστερες προσπάθειες τροποποίησης του λογιστικού αρχείου με την πλαστογράφηση της συναλλαγής ή την αλλαγή των μπλοκ. Η ΒΤ επέτρεψε την ανάπτυξη πολυάριθμων συστημάτων κρυπτονομισμάτων, όπως το Ethereum και το Bitcoin, και γι 'αυτό ορισμένοι άνθρωποι τείνουν να περιορίζουν τη ΒΤ μόνο σε λύσεις κρυπτονομίσματος, ωστόσο, μια σειρά διαφορετικών βιομηχανικών κλάδων σκέφτονται να χρησιμοποιήσουν τη ΒΤ στις εφαρμογές τους.

Η λευκή βίβλος [42] εισήγαγε την έννοια των ηλεκτρονικών μετρητών, ενώ η κυκλοφορία του κρυπτονομίσματος Bitcoin το 2009 έκανε τη ΒΤ μία από τις ευρέως διαδεδομένες τεχνολογίες. Το blockchain είναι μια βάση δεδομένων των μπλοκ που συνδέονται μαζί με μια κρυπτογραφική λειτουργία κατακερματισμού με πληροφορίες που έχουν αναπαραχθεί σε όλους τους διακομιστές

των συμμετεχόντων. Τα δεδομένα στη βάση δεδομένων ΒΤ είναι αμετάβλητα. Μπορεί να αναπτυχθεί μόνο προσθέτοντας νέο μπλοκ (δεδομένα) στο τέλος της αλυσίδας από πιστοποιημένους χρήστες με ισχυρή ικανότητα κρυπτογραφίας οι οποίοι μπορούν να προσθέσουν το νέο μπλοκ μέσω ενός ανταγωνιστικού συστήματος εξόρυξης.

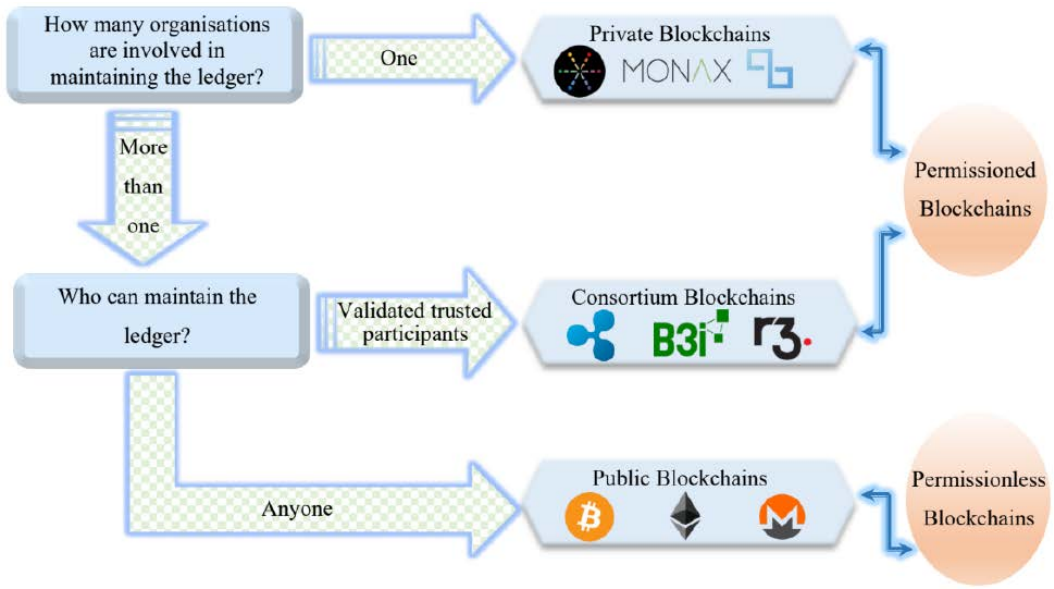
Το Bitcoin (BTC) δεν είναι blockchain αλλά μία από τις πολλές εφαρμογές που χρησιμοποιούν το ΒΤ για να υποστηρίξουν το δίκτυο κρυπτονομίσματος Bitcoin, το οποίο επιτρέπει την μεταφορά ψηφιακών μετρητών μέσα σε ένα κατανεμημένο αρχείο. Υπάρχουν πολλά άλλα κυκλώματα κίνησης όπως το Ripple (XRP), το Ethereum (ETH), το Bitcoin Cash (BCH), το Litecoin (LTC) και το Binance Coin (BNB). Στη BTC, η ιδιοκτησία των χρηστών ενός BTC μπορεί να υπογραφεί ψηφιακά και να μεταφερθεί σε άλλο χρήστη της BTC. Το BTC blockchain ανακοινώνει δημόσια αυτή τη μεταφορά σε όλους τους χρήστες του δικτύου για να ελέγξει ανεξάρτητα την εγκυρότητα της συναλλαγής. Επιπλέον, μια κατανεμημένη ομάδα χρηστών διαχειρίζεται και διατηρεί ανεξάρτητα την blockchain του BTC και μαζί με τους κρυπτογραφικούς μηχανισμούς δημιουργεί την ικανότητα μη αποδοχής της ΒΤ σε προσπάθειες τροποποίησης του αρχείου με την πλαστογράφηση της συναλλαγής ή την αλλαγή των μπλοκ.

Υπάρχουν τρεις κύριοι τύποι ΒΤ: ο ιδιωτικός, ο δημόσιος ή ο χωρίς άδεια, και ομοσπονδιακός ή κοινοπρακτικός blockchain, από τα οποία τα ιδιωτικά μπλοκ και οι κοινοπραξίες θεωρούνται αμφότερες ως αυτά που απαιτούν άδεια. Μια οντότητα διαχείρισης δικαιωμάτων απαιτείται να παραχωρήσει δικαιώματα πρόσβασης σε αξιόπιστους και γνωστούς συμμετέχοντες. Παραδείγματα ιδιωτικών blockchain περιλαμβάνουν Multichain, Monax και Quorum. Ένα blockchain κοινοπραξίας ελέγχεται από περισσότερους από έναν οργανισμούς, των οποίων η ομάδα που ελέγχει τον μηχανισμό συναίνεσης έχει προκαθορισμένους κόμβους στο δίκτυο. Παραδείγματα είναι τα Ripple, R3 (Banks) και B3i (Ασφάλειες).

Σε αντίθεση με τους προηγούμενους δύο τύπους, το δημόσιο blockchain επιτρέπει σε οποιονδήποτε να γράψει ή να διαβάσει τα δεδομένα που είναι αποθηκευμένα στο δίκτυο blockchain χωρίς την άδεια οποιασδήποτε αρχής και η λειτουργία είναι αποκεντρωμένη και ανώμαλη, από τα οποία μερικά παραδείγματα είναι το Monero, το Etherum και το Bitcoin. Το δημόσιο blockchain χρησιμοποιεί συχνά ένα σύστημα βασισμένο στη συναίνεση, της οποίας οι μηχανισμοί καθορίζουν ποιον χρήστη υποβάλλει το επόμενο μπλοκ και σχεδιάζονται έτσι ώστε να επιτρέπουν στους καχύποπτους χρήστες να συνεργαστούν σε ένα δίκτυο blockchain. Στην ΒΤ έχουν χρησιμοποιηθεί πολλοί μηχανισμοί συναίνεσης, μεταξύ των οποίων η "Απόδειξη Εργασίας (Proof of Work - PoW)", η "Απόδειξη Συμμετοχής (Proof of Stake - PoS)", η "Απόδειξη της Εξουσίας

(Proof of Authority - PoA)" ή η "Απόδειξη της Ταυτότητας (Proof of Identity - PoI)" και η "Απόδειξη Περασμένου Χρόνου (Proof of Elapsed Time - PoET)".

Το Σχήμα 1.1 δείχνει την κατηγοριοποίηση ΒΤ του ιδιωτικού, του κοινοπρακτικού, του δημοσίου και όσων δεν χρειάζονται άδεια έναντι αυτών που χρειάζονται. Η κατηγοριοποίηση βασίζεται στο πόσες οργανώσεις συμμετέχουν στη διατήρηση του αρχείου και στο πόσοι επικυρωμένοι αξιόπιστοι ή όχι συμμετέχοντες απαιτούνται.



Σχήμα 1.1: Κατηγοριοποίηση Blockchain. [02]

1.2 Μηχανισμός Συναίνεσης Blockchain

Ο μηχανισμός PoW βασίζεται στην επίλυση ενός πάζλ που απαιτεί υπολογισμό και απαιτεί τη διεξαγωγή υπολογισμών έντασης πόρων. Ένας χρήστης που μπορεί να λύσει αυτό το πάζλ μπορεί να δημοσιεύσει το επόμενο νέο μπλοκ στο δίκτυο blockchain. Ο έλεγχος της ορθότητας της λύσης γίνεται από όλους τους άλλους εξορύκτες για την επαλήθευση τυχόν νέων μπλοκ πριν την προσθήκη τους στο blockchain και την απόρριψη οποιουδήποτε μπλοκ που δεν ικανοποιεί τη λύση. Στον μηχανισμό PoW, είναι δύσκολο να πραγματοποιηθεί μια επίθεση άρνησης εξυπηρέτησης με την πλημμύρα του δικτύου blockchain από κακόβουλα μπλοκ. Θεωρητικά, το PoW επιτρέπει ένα ανοιχτό μη μονοπωλιακό περιβάλλον για όλους τους συμμετέχοντες να συνεισφέρουν. Ωστόσο, λόγω της διαφοράς στην υπολογιστική ισχύ και του κόστους της ηλεκτρικής ενέργειας, αυτό δημιουργεί μια άδικη κατάσταση μεταξύ των χρηστών. Ο τομέας εφαρμογής PoW είναι δημόσιο κρυπτονόμισμα, όπως το Bitcoin και το Ethereum. Ο μηχανισμός

συναίνεσης του PoS βασίζεται στους επενδυτές σε ένα δίκτυο. Η πιθανότητα ότι ένας χρήστης PoS θα δημοσιεύσει ένα νέο μπλοκ στο δίκτυο βασίζεται στο ποσοστό του μεριδίου του στο συνολικό μερίδιο κρυπτονομίσματος στο δίκτυο blockchain. Όταν επενδύουν σε ένα τεράστιο ποντάρισμα, το οποίο είναι συνήθως ένα ποσό κρυπτονομίσματος, η πιθανότητα να καταστρέψουν το δίκτυο μειώνεται και είναι πιθανότερο να βοηθήσουν το σύστημα να επιτύχει. Όταν το κρυπτονόμισμα διακυβεύεται, ο χρήστης δεν θα μπορεί να το ξοδέψει. Το ποντάρισμα ενός χρήστη χρησιμοποιείται από τα δίκτυα αποκλεισμού PoS για να προσδιορίσει ποιος μπορεί να δημοσιεύσει νέα μπλοκ. Ο μηχανισμός PoS έχει πολλά πλεονεκτήματα, εκ των οποίων το ένα είναι ότι, σε σύγκριση με το PoW, είναι λιγότερο υπολογιστικά εντατικό.

Ο μηχανισμός PoS επιτρέπει σε κάθε ενδιαφερόμενο χρήστη να στοιχηματίσει σε κρυπτονόμισμα, ενώ, ταυτόχρονα, το σύστημα που χρησιμοποιεί το PoS ελέγχεται από τα ενδιαφερόμενα μέρη, παρόλο που μερικές φορές θεωρείται μειονέκτημα σε περίπτωση που σχηματίσουν μια ομάδα για να δημιουργηθεί μια κεντρική βάση ενέργειας. Αντίθετα, ο μηχανισμός PoS είναι γνωστός για τα μοναδικά του ζητήματα, όπως το πρόβλημα που προκύπτει όταν κάποια στιγμή, λόγω μιας προσωρινής σύγκρουσης των λογιστικών βιβλίων, εμφανίζονται πολλαπλά blockchains που ανταγωνίζονται μεταξύ τους. Η εμφάνιση αυτών των blockchains θα προκαλέσει διαφορετικά αποτελέσματα από διαφορετικές εκδοχές blockchains που θα δημοσιευθούν σχεδόν ταυτόχρονα. Σε αυτή την περίπτωση, οι παίκτες που στοιχηματίζουν μπορούν να παίξουν σε κάθε αλυσίδα για να αυξήσουν την πιθανότητα κέρδους ανταμοιβής τους, η οποία μπορεί να αναπτυχθεί σε διαφορετικούς κλάδους στο δίκτυο blockchain για μια περίοδο χωρίς να επανενταχθεί σε ένα μόνο κλάδο. Επιπλέον, ο μηχανισμός PoS είναι ευάλωτος σε επίθεση κατά 51%, έχοντας επαρκή οικονομική ισχύ. Ο τομέας εφαρμογής PoS είναι δημόσιο κρυπτονόμισμα, όπως οι Casper και Krypton.

Ο μηχανισμός round-robin επιτρέπει σε κάθε χρήστη να πάρει τη δική του σειρά για να δημιουργήσει το επόμενο μπλοκ, το οποίο μπορεί να περιλαμβάνει ένα χρονικό όριο για κάθε χρήστη για να αποφευχθεί η αναστολή της δημοσίευσης των μπλοκ. Αυτός ο μηχανισμός χρησιμοποιείται από ορισμένα ιδιωτικά και ομοσπονδιακά δίκτυα blockchain και επίσης εμποδίζει τους χρήστες να κάνουν πληθώρα από μπλοκ, κάτι το οποίο είναι εύκολο να κατανοηθεί και δεν απαιτεί υψηλή υπολογιστική ισχύ λόγω έλλειψης κρυπτογραφικών πάζλ.

Από την άλλη πλευρά, αυτός ο μηχανισμός απαιτεί σημαντική εμπιστοσύνη μεταξύ των χρηστών με αποτέλεσμα να είναι άχρηστος στον δημόσιο τομέα blockchain, ο οποίος δεσπόζει στην πλειοψηφία των τρεχουσών υλοποιήσεων blockchain. Η μεγάλη ανάγκη για εμπιστοσύνη σε

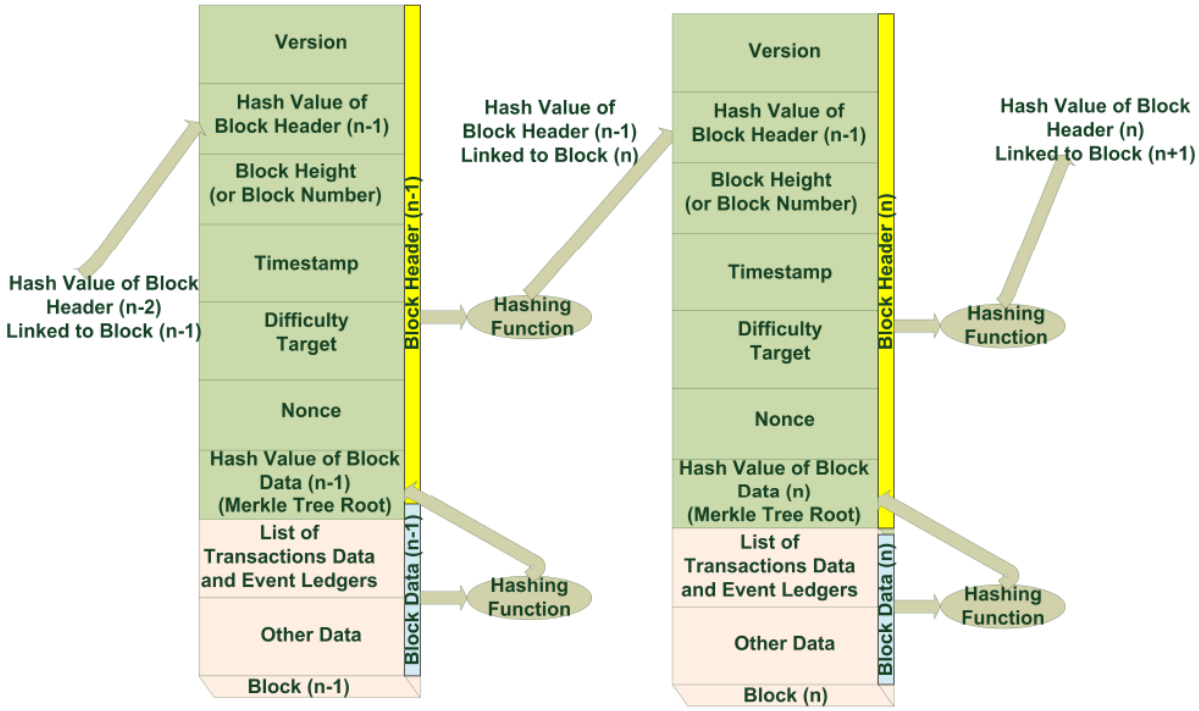
αυτόν τον μηχανισμό οφείλεται στο γεγονός ότι ένας κακόβουλος χρήστης μπορεί να αυξήσει τον αριθμό των χρηστών που συνεισφέρουν στο δίκτυο ώστε να αυξήσει την πιθανότητα δημοσίευσης κακόβουλων νέων μπλοκ με σκοπό να καταστρέψει το δίκτυο. Ο τομέας υλοποίησης round-robin είναι ένα ιδιωτικό και ομοσπονδιακό blockchain, όπως το MultiChain.

Ο μηχανισμός PoA βασίζεται στη μερική εμπιστοσύνη των χρηστών που δημοσιεύουν, η οποία βασίζεται στην πραγματική τους ταυτότητα, η οποία πρέπει να επαληθευτεί, να αποδειχθεί και να συμπεριληφθεί στο δίκτυο blockchain. Η κεντρική ιδέα πίσω από αυτό το μηχανισμό είναι ότι η φήμη ή η ταυτότητα του χρήστη που δημοσιεύει διακυβεύεται στο να δημοσιεύσει νέα μπλοκ. Η φήμη του χρήστη που δημοσιεύει επηρεάζεται από άλλους χρήστες του δικτύου βάσει της συμπεριφοράς του / της. Εάν οι χρήστες του δικτύου blockchain διαφωνούν με τις ενέργειες ενός χρήστη που δημοσιεύει, ο οποίος πρέπει να συμμορφωθεί με τον συμφωνημένο τρόπο στο δίκτυο, ο χρήστης θα χάσει τη φήμη του, ελαχιστοποιώντας την πιθανότητα του χρήστη να δημοσιεύσει ένα μπλοκ.

Ο χρόνος επιβεβαίωσης σε αυτόν τον μηχανισμό είναι γρήγορος και οι ρυθμοί παραγωγής μπλοκ είναι δυναμικοί. Επιπλέον, αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί σε υβριδικά συστήματα, ο οποίος βασίζεται σε άλλο μηχανισμό συναίνεσης. Αντίθετα, αυτός ο μηχανισμός υποθέτει ότι ο χρήστης επικύρωσης δεν διακυβεύεται. Επιπλέον, η φήμη του χρήστη υπόκειται σε πιθανή έκθεση υψηλού κινδύνου που μπορεί να θέσει σε κίνδυνο τον χρήστη ανά πάσα στιγμή. Αυτός ο μηχανισμός οδηγεί επίσης σε ένα μόνο σημείο αποτυχίας. Ο τομέας εφαρμογής της απόδειξης εξουσίας ή η απόδειξη του μηχανισμού ταυτότητας είναι ένα ιδιωτικό και ομοσπονδιακό blockchain και περιλαμβάνει υβριδικά συστήματα όπως το Ethereum, το Kovan Testnet και η αλυσίδα POA.

Ο μηχανισμός PoET ορίζει ότι κάθε χρήστης που δημοσιεύει ζητά έναν χρόνο αναμονής εντός του δικτύου από μια πηγή χρόνου υλικού, η οποία είναι ασφαλής και εγκατεστημένη στο σύστημα υπολογιστή του χρήστη. Στον μηχανισμό αυτό, κάθε χρήστης έκδοσης ζητά χρόνο αναμονής εντός του δικτύου από μια πηγή χρόνου υλικού, η οποία είναι ασφαλής και εγκατεστημένη στο σύστημα του υπολογιστή του χρήστη. Το υλικό παράγει έναν τυχαίο χρόνο αναμονής για τον χρήστη που δημοσιεύει και ο χρήστης καθίσταται ανενεργός κατά τη διάρκεια της περιόδου αναμονής. Όταν ο χρήστης που δημοσιεύει επανενεργοποιηθεί, ο χρήστης δημιουργεί και δημοσιεύει ένα μπλοκ στο δίκτυο και όλοι οι χρήστες που βρίσκονται σε ανενεργή κατάσταση θα σταματήσουν να περιμένουν και η όλη διαδικασία θα ξεκινήσει ξανά.

Στον μηχανισμό αυτό, ο δεδομένος χρόνος αναμονής πρέπει να είναι τυχαίος διαφορετικά ο κακόβουλος χρήστης μπορεί να κυριαρχήσει στο σύστημα διατηρώντας τον χρόνο αναμονής σε ελάχιστο ποσό. Εκτός αυτού, ο εκδότης σε αυτόν τον μηχανισμό δεν πρέπει να ξεκινά νωρίς περιμένοντας την πραγματική δεδομένη ώρα. Αυτές οι προκλήσεις επιλύονται με την εκτέλεση μιας εφαρμογής σε ένα περιβάλλον αξιόπιστης επεξεργασίας, όπως οι επεκτάσεις λογισμικού της Intel, οι οποίες δεν μπορούν να τροποποιηθούν από εξωτερικές εφαρμογές. Αυτός ο μηχανισμός είναι λιγότερο υπολογιστικά ακριβός από τον PoW. Ωστόσο, τα μειονεκτήματα αυτού του μηχανισμού είναι ότι βασίζεται στο υλικό για να παράγει τυχαίο χρόνο και υποθέτει ότι το υλικό δεν είναι συμβιβασμένο. Ο τομέας εφαρμογής του μηχανισμού PoET είναι ένα ιδιωτικό και ομοσπονδιακό blockchain, όπως το Hyperledger Sawtooth.



Σχήμα 1.2: Η δομή ενός μπλοκ και η διαδικασία πρόσδεσής του σε μια blockchain αλυσίδα. [02]

Ένα μπλοκ αποτελείται από μια κεφαλίδα και μια λίστα με τα βιβλία συναλλαγών και γεγονότων. Το Σχήμα 1.2 δείχνει τη δομή ενός μπλοκ και τη διαδικασία της πρόσδεσής του σε μια blockchain αλυσίδα.

1.2.1 Μπλοκ Κεφαλίδας

Το μπλοκ κεφαλίδας αποτελείται από τρία διαφορετικά σύνολα μεταδεδομένων. Το πρώτο είναι η έκδοση και ο προηγούμενος κατακερματισμός του μπλοκ. Το πεδίο Έκδοσης (4 bytes) είναι για την παρακολούθηση των ενημερώσεων λογισμικού και πρωτοκόλλου, ενώ το πεδίο Previous Block Hash (32 bytes) είναι μια αναφορά στον κατακερματισμό του προηγούμενου μπλοκ. Ο αλγόριθμος κρυπτογραφικού κατακερματισμού γίνεται εφαρμόζοντας SHA256 δύο φορές κάθε φορά. Σε ένα blockchain, κάθε μπλοκ συνδέεται από το προηγούμενο μπλοκ, ο κατακερματισμός του οποίου χρησιμοποιείται για τη δημιουργία του κατακερματισμού του νέου μπλοκ. Το πρώτο μπλοκ στο blockchain είναι γνωστό ως μπλοκ γένεσης.

Το δεύτερο είναι το πρόγραμμα ανταγωνισμού μεταλλευμάτων. Αυτό το σύνολο μεταδεδομένων περιέχει το Timestamp (4 bytes), το Nonce (4 bytes) και το στόχο δυσκολίας (4 bytes). Η χρονική σήμανση είναι ο χρόνος δημιουργίας του μπλοκ. Το "nonce", δηλαδή "ο αριθμός που χρησιμοποιείται μόνο μία φορά (number only used once)" είναι ένας αριθμός που προστίθεται σε ένα κατακερματισμένο μπλοκ, το οποίο, όταν ανασυντάσσεται, πληροί τους περιορισμούς του επιπέδου στόχου δυσκολίας.

Το nonce είναι ο πρώτος αριθμός που χρειάζεται να ανακαλύψει ένας εξορύκτης πριν αποφασίσει για ένα μπλοκ στο blockchain. Τέλος, ο κατακερματισμός της ρίζας Merkle Tree (32 bytes) περιέχει μια δομή δεδομένων των συναλλαγών στο μπλοκ. Η ρίζα του Merkle Tree δημιουργείται από επανειλημμένα ζευγάρια εξαναγκασμού κόμβων συναλλαγών μέχρι να απομείνει μόνο ένας κατακερματισμός. Η διαδικασία εκτελείται από κάτω προς τα πάνω, από τον κατακερματισμό των μεμονωμένων συναλλαγών.

1.2.3 Δεδομένα των Μπλοκ

Το Merkle Tree είναι ένα ψηφιακό αποτύπωμα του συνόλου των συναλλαγών σε ένα μπλοκ που επιτρέπει σε ένα χρήστη να επαληθεύει εάν μια συναλλαγή περιλαμβάνεται ή όχι σε ένα μπλοκ. Βοηθά στο να επαληθευτεί ότι οι μεταγενέστερες εκδόσεις του αρχείου καταγραφής συμβάντων περιλαμβάνουν όλη την προηγούμενη έκδοση και στο ότι όλα τα δεδομένα καταγράφονται και παρουσιάζονται με χρονολογική σειρά. Τα δεδομένα αποκλεισμού περιέχουν ένα ημερολόγιο των συμβάντων και των καταλόγων συναλλαγών που περιλαμβάνονται στο μπλοκ καθώς και οποιεσδήποτε άλλες πληροφορίες για όλες τις αυθεντικές και επικυρωμένες συναλλαγές που έχουν δημοσιευτεί στο δίκτυο blockchain.

1.2.4 Αλυσίδα των Μπλοκ

Η προσθήκη ενός νέου μπλοκ εκτελείται από τους εξορύκτες Ένα μπλοκ στην αλυσίδα μπορεί να προέλθει από κάθε ορυχείο που έχει το δικαίωμα να προσθέσει το νέο μπλοκ. Ο εξορύκτης συλλέγει τον κατακερματισμό του τελευταίου τμήματος της αλυσίδας, το συνδυάζει με το δικό του σύνολο μηνυμάτων και δημιουργεί ένα νέο κατακερματισμό για το νεοσυσταθέν μπλοκ. Αυτό το νεοσυσταθέν μπλοκ γίνεται πλέον το νέο άκρο της αλυσίδας. Με αυτό, η ακεραιότητα της συναλλαγής και η μη απόρριψη είναι εγγυημένη, καθώς μπορεί να απορριφθεί και να ανιχνευθεί από τυχόν τροποποιημένα μπλοκ. Το Σχήμα 1.2 δείχνει τη γενική διαδικασία της αλυσίδας στη BT.

1.3 Έξυπνα Συμβόλαια

Το Ethereum ξεκίνησε το 2015 και το εικονικό νόμισμα "Ether" προτάθηκε ως κρυπτονόμισμα του Ethereum [55]. Παρόμοια με τα νομίσματα fiat, οι τιμές και οι ισορροπίες του Ether έχουν τυποποιημένες ονομασίες για μικρότερες μονάδες όπως Wei, Kwei (1K Wei), Mwei (Mega Wei) και ένας Ether (10 ** 18 Wei). Οι εξορύκτες του Ethereum διατηρούν την κατάσταση του δικτύου και επιλύουν πιθανές συγκρούσεις λόγω, για παράδειγμα, επιθέσεων ή αποτυχιών χρησιμοποιώντας έναν μηχανισμό συναίνεσης.

Ο τρέχων μηχανισμός συναίνεσης που χρησιμοποιείται στο Ethereum είναι η συναίνεση του PoW που βασίζεται στην υπόθεση ότι οι εξορύκτες είναι διατεθειμένοι να ακολουθήσουν τον μηχανισμό αντί να επιτεθούν, επειδή ο μηχανισμός θα τους πληρώσει για την εκτέλεση των υπολογισμών που απαιτούνται για τη διατήρηση του δικτύου και οι χρήστες θα πληρώνουν τέλη εκτέλεσης για κάθε συναλλαγή [38]. Το Ethereum υποστηρίζει όλους τους τύπους υπολογιστικών δομών που περιλαμβάνουν βρόχους οι οποίοι μπορούν να εκτελέσουν οποιονδήποτε κωδικό προγραμματισμού “αποκεντρωμένης εφαρμογής (decentralized application - dApp)” χρησιμοποιώντας τα "έξυπνα συμβόλαια" του Ethereum.

Οι έξυπνες συμβάσεις είναι ψηφιακές συμβάσεις που εκτελούνται από τον εαυτό τους όταν πληρούνται ακριβείς συνθήκες και μπορούν να αναπτυχθούν και να υλοποιηθούν πάνω από το blockchain Ethereum. Η έξυπνη σύμβαση μπορεί να συμβολίζει την ιδιοκτησία της ψηφιακής ιδιοκτησίας και να επιτρέπει την αντικατάσταση όλων των αξιών όπως οι μετοχές, η περιουσία και τα χρήματα [23]. Όλες οι συναλλαγές αποθηκεύονται στο blockchain Ethereum, ενώ η

ακολουθία συναλλαγών εντοπίζει την ισορροπία κάθε χρήστη και την κατάσταση κάθε έξυπνου συμβολαίου στην blockchain.

Ο τύπος έξυπνων συμβολαίων περιλαμβάνει την ισορροπία που περιέχει την ποσότητα Ether που κατέχουν και την ιδιωτική αποθήκευση που είναι τιμές 256-bit καθώς και μια αποθήκευση βασικής αξίας με κλειδιά 256-bit. Η αποθήκευση είναι ιδιωτική το οποίο σημαίνει ότι δεν μπορεί να τροποποιηθεί ή να διαβαστεί από άλλες συμβάσεις. Μια συναλλαγή μετατοπίζει τον δευτερεύοντα χαρακτήρα του "Ethereum Virtual Machine (EVM)" στο blockchain Ethereum για να δημιουργήσει την πρωτεύουσα κατάσταση με τον κατασκευαστή και να μεταφέρει τον κώδικα της σύμβασης. Οι χρήστες έξυπνων συμβολαίων χρησιμοποιούν μια συναλλαγή που επικαλείται σύμβαση με τη διεύθυνση της έξυπνης σύμβασης στόχου ως παραλήπτης για να επικαλεστεί το έξυπνο συμβόλαιο μετά την έξοδο της έξυπνης σύμβασης.

Κάθε έξυπνη σύμβαση αποκτά μια ανεξάρτητη διεύθυνση για να αλληλεπιδράσει μέσα στο δίκτυο Ethereum. Το συμβόλαιο αποθηκεύεται στο λογιστικό αρχείο, εάν πετύχει και η εκκίνηση έξυπνης σύμβασης και η συναλλαγή ανάπτυξης. Υπάρχουν δύο προσεγγίσεις για τη σύναψη μιας σύμβασης με μια άλλη σύμβαση. Η πρώτη προσέγγιση είναι ένας από τους χρήστες να δημιουργούν απευθείας συναλλαγές στο δεύτερο συμβόλαιο που έχει μια γνωστή διεύθυνση που φέρει το απαιτούμενο σχήμα σύμβασης. Η δεύτερη προσέγγιση είναι ένας από τους χρήστες που κάνει ένα νέο παράδειγμα της δεύτερης σύμβασης, δημιουργώντας ένα νέο συμβόλαιο με την ίδια λειτουργικότητα της συμβατικής τάξης [26].

Στην Solidity, παρέχονται πολλά αρχέτυπα για την πρόσβαση στις πληροφορίες του μπλοκ και της συναλλαγής. Για παράδειγμα, η msg.value χρησιμοποιείται για την πρόσβαση στο ποσό Wei που μεταδίδεται από μια συναλλαγή επικαλούμενη τη μέθοδο. Ένα άλλο παράδειγμα είναι το msg.sender που χρησιμοποιείται για την πρόσβαση στη διεύθυνση λογαριασμού που επικαλέστηκε τη μέθοδο. Η ακριβής υπογραφή της λειτουργίας της έξυπνης επαφής πρέπει να υποδεικνύει εάν κάποιος θέλει να καλέσει μια συγκεκριμένη λειτουργία στο έξυπνο συμβόλαιο. Οποιοδήποτε έξυπνο συμβόλαιο έχει μια εφεδρική λειτουργία η οποία χειρίζεται το αίτημα από συναλλαγές που υποδεικνύουν ασυμβίβαστη ή μη λειτουργία.

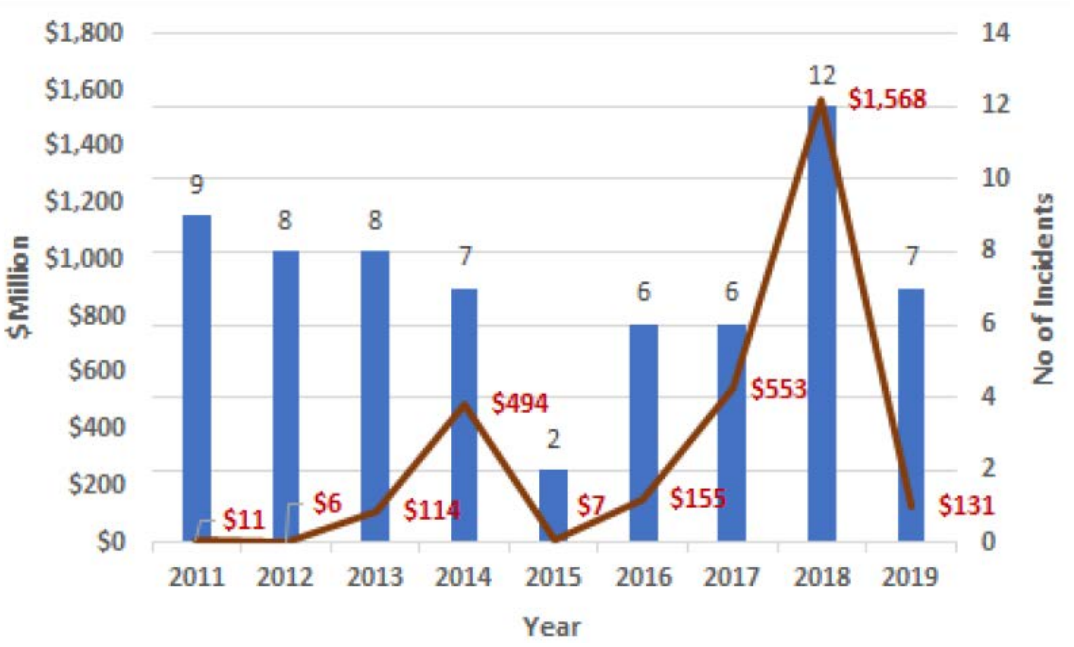
Η συναλλαγή θα εκτελεστεί εκτελώντας τον κώδικα της έξυπνης σύμβασης στο πλαίσιο της υπόθεσης συμβολαίου και κάθε εντολή θα καταναλώσει μια προκαθορισμένη ποσότητα πόρων. Ο αποστολέας της συναλλαγής ορίζει ένα όριο πόρων, το οποίο αν ξεπεραστεί ή εμφανιστεί ένα σφάλμα χρόνου εκτέλεσης, ακυρώνεται ολόκληρη η συναλλαγή και δεν θα επηρεαστεί το αρχείο,

εκτός από το γεγονός ότι ο αποστολέας θα χάσει το χρησιμοποιούμενο πόρο. Η συναλλαγή αντιμετωπίζεται ως εξαίρεση εάν ο υπολογιστικός πόρος τελειώσει πριν η συναλλαγή φτάσει σε ένα κανονικό σημείο στάσης. Σε περίπτωση που ένα έξυπνο συμβόλαιο στείλει ένα μήνυμα σε άλλη σύμβαση, ένα μέρος του υπολογιστικού πόρου αποστολέα μπορεί να προσφερθεί μόνο στον παραλήπτη. Εάν ο υπολογιστικός πόρος τελειώσει από τον δέκτη, ο έλεγχος θα επιστραφεί στον αποστολέα ο οποίος μπορεί να χρησιμοποιήσει το υπόλοιπο του αερίου για να ισιώσει και να αντιμετωπίσει την εξαίρεση [32].

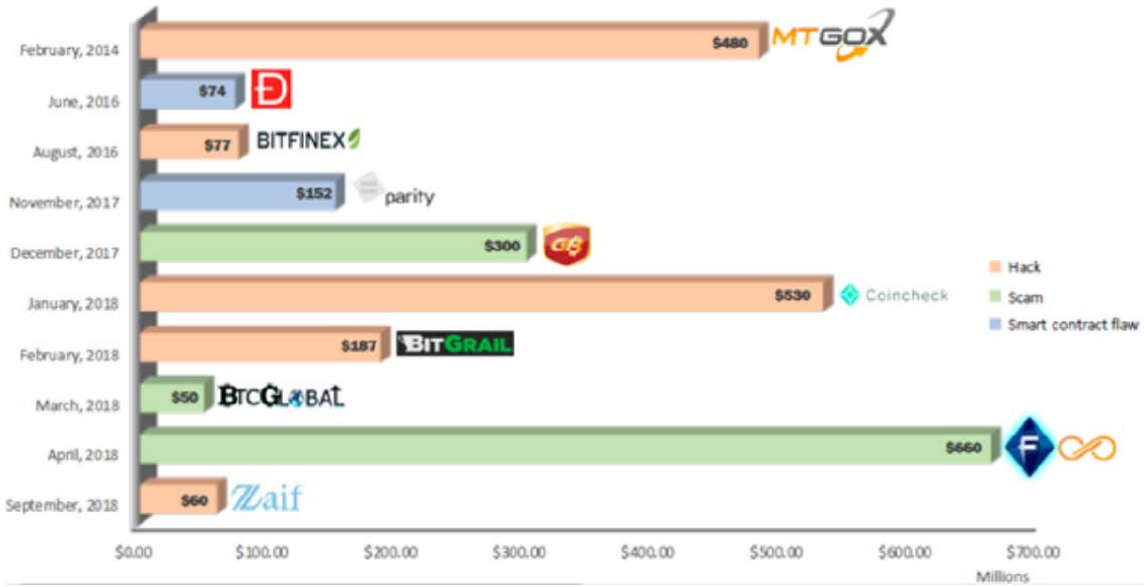
1.4 Απειλές Ασφάλειας στο Δίκτυο Blockchain

Εντοπίστηκαν 65 περιστατικά ασφάλειας δικτύων στον κυβερνοχώρο μεταξύ του 2011 και του πρώτου εξαμήνου του 2019 που επηρέασαν δυσμενώς τα συστήματα blockchain. Υπολογίζονται τα στοιχεία των επιπτώσεων που αναφέρθηκαν, τα οποία βασίζονται στην τιμή των κερδισμένων κερμάτων τη στιγμή που εντοπίστηκαν οι επιθέσεις. Οι αναφερθείσες περιπτώσεις μπορεί να μην είναι πλήρεις, δεδομένου ότι η έρευνα βασίζεται σε διαθέσιμες στο κοινό πληροφορίες για φόρουμ, ενημερωτικά δελτία και άλλα άρθρα περιοδικών. Τα περισσότερα περιστατικά υπολείπονται σε λεπτομέρειες σχετικά με τις πραγματικές συνθήκες που περιβάλλουν τα περιστατικά. Έτσι, παρέχεται μια υψηλού επιπέδου ταξινόμηση τριών τύπων, δηλαδή παράνομη πρόσβαση (hack), απάτη (scam) και ελαττώματα έξυπνων συμβάσεων. Ο συνολικός αντίκτυπος των περιστατικών στον κυβερνοχώρο μεταξύ 2011 και 2019 ήταν πάνω από 3 δισ. δολάρια ΗΠΑ. Η μεγαλύτερη απώλεια αφορά το hacking, η οποία ισούται με παραπάνω από 1,6 δισεκατομμύρια δολάρια ΗΠΑ, ακολουθούμενη από την απάτη, η οποία ισούται με πάνω από 1,1 δισεκατομμύρια δολάρια ΗΠΑ και ελαττώματα έξυπνων συμβάσεων, τα οποία ισούνται με περισσότερα από 289 εκατομμύρια δολάρια ΗΠΑ.

Το Σχήμα 1.3 δείχνει κατά μέσο όρο ότι υπάρχουν επτά περιστατικά ετησίως σταδιακά μειωμένα έως το 2015 που έφθασαν στο κατώτατο σημείο με δύο μόνο περιστατικά. Η πτώση αυτή συμπίπτει με τη μείωση της τιμής του Bitcoin κατά το έτος αυτό. Η τιμή του Bitcoin αυξήθηκε σταδιακά μετά το 2015 και όπως και ο αριθμός των συμβάντων επίθεσης, που αυξήθηκαν σταδιακά σε δώδεκα περιστατικά το 2018. Το ποσό της απώλειας για τα περιστατικά ακολούθησε την ίδια τάση από τα 7 εκατομμύρια δολάρια το 2015 αυξάνεται σε ένα ρεκόρ των $1,6 δισεκατομμυρίων δολαρίων το 2018. Οι πρώτοι έξι μήνες του 2019 έχουν ήδη φτάσει σε επτά περιστατικά, με απώλεια ποσού μόνο $131 εκατομμύρια δολάρια ΗΠΑ. Ωστόσο, πιστεύεται ότι ο αριθμός αυτός θα αυξηθεί κατά το δεύτερο εξάμηνο του 2019.



Σχήμα 1.3: Περιστατικά επιθέσεων Blockchain από το 2011 ως το 2019 ανά 6 μήνες. [02]



Σχήμα 1.4: Τα 10 πιο σημαντικά περιστατικά στα δίκτυα Blockchain. [02]

Το Σχήμα 1.4 δείχνει τα δέκα κορυφαία συμβάντα στον κυβερνοχώρο που είχαν συμβεί στα δίκτυα blockchain μεταξύ 2011 και 2019, όσον αφορά τις οικονομικές απώλειες. Δείχνει ότι η μεγαλύτερη απώλεια οφείλεται σε μια απάτη Ponzi που υπέστησαν θύματα στο Βιετνάμ, καθώς 32.000 επενδυτές επένδυσαν σε Ifan και Pincoin τον Απρίλιο του 2018 με απώλειες συνολικού ύψους $ 660 εκατ. δολαρίων ΗΠΑ [60]. Τα θύματα δεν ήταν σε θέση να αποσύρουν τα κέρδη τους σε μετρητά. Πρόκειται για μια τυπική απάτη πυραμίδας η οποία χαρακτηρίζει την επένδυση ως

«δραστηριότητα χωρίς κίνδυνο» με κέρδη «έως και 40% μηνιαίως» μέσω μιας σειράς δομών μπόνους που επιτρέπουν στους πρώιμους επενδυτές να κερδίσουν κέρδη σε σχέση με τις μεταγενέστερες. Η δεύτερη μεγαλύτερη απώλεια οφείλεται στο γεγονός ότι η Coincheck υπέστη εξωτερικό hacking στο σύστημά της τον Ιανουάριο του 2018 για μια απώλεια ρεκόρ ύψους 530 εκατομμυρίων δολαρίων στην κρυπτογράφηση. Η Coincheck παρέχει υπηρεσία πορτοφολιού και υπηρεσία ανταλλαγής με 68%, έχοντας δεσπόζουσα θέση στην αγορά κρυπτονομίσματος Bitcoin. Το προσωπικό του Coincheck απέτυχε να εφαρμόσει το χαρακτηριστικό της σύμβασης ανταλλαγής NEM που συνιστούσαν οι προγραμματιστές NEM και να αποθηκεύσει όλα τα μπλοκ NEM σε ένα και μόνο πορτοφόλι. Συνιστάται στις ανταλλαγές σήμερα να χρησιμοποιείται ένα υβριδικό σύστημα «ζεστού» / «κρύου» πορτοφολιού, το οποίο αποθηκεύει το μεγαλύτερο μέρος της αξίας στα «κρύα» πορτοφόλια και εξασφαλίζεται μέσω συμβολαίου πολλαπλής ασφάλειας.

Η τρίτη μεγαλύτερη απώλεια είναι το hacking της Mt. Gox, που συνέβη τον Φεβρουάριο του 2014 με απώλειες 480 εκατομμυρίων δολαρίων ΗΠΑ, και άλλα 27,4 εκατομμύρια δολάρια ΗΠΑ τα οποία λείπουν από τους τραπεζικούς λογαριασμούς. Οι χάκερ είχαν παραβιάσει την Mt. Gox και είχαν πάρει ένα τεράστιο μέρος των κρυπτονομισμάτων που ελέγχονταν από την εταιρεία. Το περιστατικό είχε προκαλέσει αφερεγγυότητα της Mt. Gox [23] Η Mt. Gox ήταν η μεγαλύτερη εταιρεία ανταλλαγής bitcoin στον κόσμο την εποχή εκείνη, η οποία είχε υποστεί τρεις ξεχωριστές επιθέσεις τον Ιούνιο του 2011 (8,75 εκατομμύρια δολάρια ΗΠΑ), τον Οκτώβριο του 2011 (8,35 εκατομμύρια δολάρια ΗΠΑ) και τον Φεβρουάριο του 2014 (480 εκατομμύρια δολάρια ΗΠΑ). Η αποτυχία της Mt. Gox αποδόθηκε στην κακή διαχείριση, την έλλειψη ανάπτυξης λογισμικού και τον ανεπαρκή έλεγχο ασφαλείας. Η ελαχιστοποίηση της συναλλαγής αποτελεί μια ευπάθεια στο δίκτυο Blockchain του Bitcoin, το οποίο επιτρέπει στον αντίπαλο να αλλάξει το αναγνωριστικό συναλλαγής (TXID) χωρίς να ανακαλέσει τη συναλλαγή. Η τροποποίηση του TXID θα εξαπατήσει το θύμα να πιστέψει ότι η συναλλαγή απέτυχε, αν και επιβεβαιώνεται αργότερα. Οι ανταλλαγές συναλλάγματος αποτελούν τους κοινούς στόχους για αυτήν την επίθεση. Ο αντίπαλος αποσύρεται από μια ανταλλαγή και στη συνέχεια αναδημοσιεύει την ίδια συναλλαγή με ένα διαφορετικό TXID και ένα από αυτά θα εμφανίζεται στο δίκτυο. Λόγω καθυστερήσεων, είναι πολύ πιθανό ότι η μεταβληθείσα συναλλαγή θα κερδίσει παρά την αρχική απόσυρση. Η ανταλλαγή νομισμάτων δεν θα εντοπίσει την αρχική συναλλαγή στο δίκτυο και θα σκεφτεί ότι η συναλλαγή απέτυχε εάν η ανταλλαγή βασίζεται μόνο σε TXID. Έτσι, ο αντίπαλος μπορεί να κάνει συνεχώς ανάληψη χρημάτων στην επίθεση στη Mt. Gox· οι επιτιθέμενοι διενήργησαν επίθεση κατά της συναλλαγής για την κλοπή νομισμάτων κατά την ανταλλαγή, γεγονός που ανάγκασε το χρηματιστήριο να παγώσει το λογαριασμό των χρηστών και να σταματήσει τις αναλήψεις [20].

Τύπος	Αριθμός Συμβάντων	Συνολικός Αριθμός Ζημιών (εκ. $)
Παράνομη Πρόσβαση (hack)	48	1.621
Απάτη (scam)	10	1.126
Ελαττώματα Έξυπνων Συμβάσεων	7	289

Πίνακας 1.1: Ταξινόμηση συμβάντων Blockchain. [02]

Ο Πίνακας 1.1 δείχνει τις κορυφαίες περιπτώσεις απάτης με 48 περιστατικά με συνολική απώλεια 1,6 δισ. Δολαρίων. Με βάση τις πληροφορίες από την πηγή, τα διανύσματα του hacking περιλαμβάνουν την διακινδύνευση στο σύστημα υπολογιστών, την διακινδύνευση στην υπηρεσία cloud, την διακινδύνευση του λογαριασμού ηλεκτρονικού ταχυδρομείου, την διακινδύνευση του ιδιωτικού κλειδιού, την διακινδύνευση τρίτου μέρους, την διακινδύνευση διακομιστή, την διακινδύνευση ιστότοπου, την διακινδύνευση «ζεστού» και «κρύου» πορτοφολιού, την διακινδύνευση πλατφόρμας, την επίθεση «ηλεκτρονικού ψαρέματος» (phising), την κακόβουλη εμπλοκή και την απάτη αντικατάστασης της SIM. Το Coinbase ανίχνευσε με επιτυχία και εμπόδισε κάτι που θα συνιστούσε hack στις 20 Ιουνίου. Οι χάκερ πιστεύεται ότι έχουν εκμεταλλευτεί ένα σφάλμα zero-day για το Firefox, στοχεύοντας τους υπαλλήλους με δόλωμα ηλεκτρονικού ψαρέματος. Υπάρχουν διάφοροι τύποι ελαττωμάτων στο λογισμικό των χρηστών της αλυσίδας Blockchain, όπως η διάρκεια εκτέλεσης, η ταυτότητα, η μνήμη, η ασφάλεια, οι επιδόσεις, η διαμόρφωση, το "Γραφικό Περιβάλλον Χρήστη (Graphical User Interface - GUI)", η συμβατότητα, και η κατασκευή [09].

Τα ελαττώματα στο λογισμικό των χρηστών της αλυσίδας Blockchain, το οποίο χρησιμοποιείται στο δίκτυο της αλυσίδας Blockchain, μπορεί να οδηγήσουν στην έκθεση των ιδιωτικών κλειδιών των χρηστών. Το 2014, το Blockchain.info, το οποίο είναι ένας υβριδικός παροχέας πορτοφολιού, έκανε λάθος κατά την ενημέρωση του λογισμικού του, καθώς όταν οι χρήστες του δημιούργησαν ένα νέο ζεύγος κλειδιών στον τοπικό τους υπολογιστή χρησιμοποιώντας το λογισμικό που επηρεάστηκε, οι εισροές αλγορίθμου ECDSA δεν είχαν επαρκή τυχαιότητα, οδήγησε έναν αντίπαλο να χειριστεί το λογισμικό για να θέσει σε κίνδυνο τα ιδιωτικά κλειδιά των χρηστών προβάλλοντας μόνο τη δημόσια διεύθυνση. Υπάρχει ένα 0.0002% των χρηστών που επηρεάστηκαν και το πρόβλημα εντοπίστηκε και επιλύθηκε εντός δυόμισι ωρών, παρόλο που κάποια Bitcoins είχαν κλαπεί. Οι αδυναμίες του λογισμικού ενδέχεται να οδηγήσουν σε διαρροή ιδιωτικών κλειδιών χρηστών. Ο αριθμός των συμβάντων αλυσίδας Blockchain που οφείλονται σε

απάτη είναι 10. Το μυστικό της ταυτότητας ιδιοκτησίας που παρέχεται από αλυσίδες Blockchain έχει επιτρέψει να γίνει η πλατφόρμα επιλογής για απάτες. Ο πίνακας δείχνει ότι η δεύτερη υψηλότερη απώλεια οφείλεται σε απάτες όπως το σχέδιο Ponzi και το σύστημα πυραμίδας, προκαλώντας απώλειες ενός δισεκατομμυρίου δολαρίων. Η απάτη περιλαμβάνει όλα τα περιστατικά από τα οποία εξαφανίστηκε ο κάτοχος-στόχος με όλα τα κεφάλαια.

Είδος Θύματος	**Αριθμός Συμβάντων**	**Συνολικός Αριθμός Ζημιών (εκ. $)**
Τράπεζα Bitcoin	1	502.029
Πάροχος Υπηρεσιών Πληρωμών Bitcoin	1	1.800.000
Χρηματιστήριο Bitcoin	2	6.741.039
Δίκτυο Blockchain	1	7.700.000
Σχέδιο κρυπτοσυναλλάγματος	1	40.000
Πρόγραμμα Blockchain	1	500.000
Παροχέας υπηρεσιών Cloud	1	228.845
Darknet αγορά	1	100.000.000
Ψηφιακή πλατφόρμα συναλλαγών νομισμάτων	1	4.100.000
Κατανεμημένη αυτόνομη οργάνωση	1	74.124.000
Ανταλλαγή	36	1.568.184.876
Ατομική	4	6.646.944
Υπηρεσία εμπορίας συναλλαγών	2	2.441.760
Αγορά εξόρυξης	1	64.931.534
Σε απευθείας σύνδεση αίθουσα πόκερ	1	15.543
Σχέδιο Ponzi	4	1.014.500.000
Σχέδιο πυραμίδας	1	2.300.000
Εταιρεία κωδικοποίησης έξυπνων συμβάσεων	2	182.210.733

Χρηματιστήριο	1	10.000
Χρηματιστήριο Bitcoin	2	2.200.000

Πίνακας 1.2: Ταξινόμηση θυμάτων συμβάντων σε αλυσίδες Blockchain. [02]

Ο Πίνακας 1.2 δείχνει ότι τα θύματα των συμβάντων σε αλυσίδες Blockchain κυμαίνονται από άτομα, τράπεζες bitcoin, παρόχους υπηρεσιών Bitcoin, όπως και υπηρεσίες πορτοφολιού, πλατφόρμες συναλλαγών νομισμάτων και ανταλλαγές. Οι ανταλλαγές κρυπτοσυναλλάγματος είναι οι κύριοι στόχοι της επίθεσης. Υπάρχουν 36 περιστατικά με απώλειες ύψους 1,56 δισ. Δολαρίων συνολικά. Η ευπάθεια στην ευμεταβλητότητα της συναλλαγής ήταν η αιτία του Mt. Gox το 2014. Υπάρχουν περιστατικά όπου οι χάκερ χρησιμοποιούν κρυπτογράφηση για να εγκαταστήσουν το κακόβουλο λογισμικό στο μηχάνημα-στόχο ή την κινητή συσκευή για να χρησιμοποιήσουν την υπολογιστική τους ισχύ για να εξορύξουν ένα μπλοκ, το οποίο καταναλώνει μεγάλο όγκο ηλεκτρικής ενέργειας και μπορεί να θέσει σε κίνδυνο τη λειτουργικότητα του συστήματος.

Μόνο τον Φεβρουάριο του 2018, οι ερευνητές ξεκίνησαν μια εκστρατεία κρυπτογράφησης, η οποία επηρέασε περισσότερους από 4000 ιστότοπους, συμπεριλαμβανομένων των ιστοσελίδων της κυβέρνησης του Ηνωμένου Βασιλείου και των ΗΠΑ, ενώ η άλλη καμπάνια στοχεύει εκατομμύρια συσκευές Android. Επιπλέον, η Radiflow, εταιρεία ασφάλειας υποδομής κριτικής σημασίας (critical infrastracture), διαπίστωσε ύπαρξη κακόβουλου λογισμικού στο πρόγραμμα εξόρυξης κρυπτοσυναλλάγματος στο επιχειρησιακό δίκτυο ευρωπαϊκού δικτύου ύδρευσης, το οποίο είχε τεράστιο αντίκτυπο στα συστήματα [44]. Αυτή η ταξινόμηση βασίζεται στα ευρήματα 65 περιστατικών στον κυβερνοχώρο του πραγματικού κόσμου που σημειώθηκαν μεταξύ του 2011 και του πρώτου εξαμήνου του 2019 και παράγουν ένα σύστημα ταξινόμησης σύμφωνα με τους φορείς απειλών και τα τρωτά σημεία των αλυσίδων Blockchain. Κατατάσσουμε τις απειλές και τις ευπάθειες των αλυσίδων Blockchain στις ακόλουθες πέντε κατηγορίες:

- Ευπάθειες των τερματικών (clients)
- Χαρακτηριστικά ευάλωτων μηχανισμών συναίνεσης
- Θέματα ευπαθειών σε «δεξαμενές εξόρυξης» (mining pools)
- Θέματα ευπάθειας δικτύου

- Ευπάθειες ευφυούς συμβολαίου

1.4.1 Ευπάθειες των Τερματικών

- **Ευπάθεια Ψηφιακής Υπογραφής:** Όλη η ασύμμετρη κρυπτογραφία Bitcoin βασίζεται στην κρυπτογράφηση ελλειπτικής καμπύλης (Elliptic Curve Cryptography - ECC). Οι διευθύνσεις στο Bitcoin προέρχονται από δημόσια κλειδιά του ECC και ο έλεγχος ταυτότητας της συναλλαγής χρησιμοποιεί ψηφιακές υπογραφές, οι οποίες δημιουργούνται από τον αλγόριθμο ψηφιακής υπογραφής ελλειπτικής καμπύλης (Elliptic Curve Digital Signing Algorithm - ECDSA). Η χρήση του ECC είναι ανεπαρκής, διότι δεν έχει την απαιτούμενη τυχαιότητα, η οποία μπορεί να θέσει σε κίνδυνο το ιδιωτικό κλειδί του χρήστη. Μια τυχαία τιμή πρέπει να χρησιμοποιείται με το ιδιωτικό κλειδί για τη δημιουργία ψηφιακής υπογραφής όπου η τυχαία τιμή πρέπει να είναι διαφορετική για κάθε συναλλαγή. Για παράδειγμα, σε αλυσίδα Bitcoin, εντοπίστηκαν 158 μοναδικά δημόσια κλειδιά τα οποία χρησιμοποίησαν την ίδια τυχαία τιμή (nonce) σε περισσότερες από μία υπογραφές, γεγονός που κατέστησε δυνατή την υπονόμευση των ιδιωτικών κλειδιών των χρηστών [14].

- **Χαρακτηριστικό Ευπάθειας Λειτουργίας Κατακερματισμού (Hash):** Η λειτουργία σε μερικά από τα δίκτυα αλυσίδων Blockchain, όπως το blockchain του Bitcoin, βασίζεται σε κρυπτογραφικά πρωτότυπα για να εξασφαλίσει την ορθότητα και την ακρίβεια της λειτουργίας. Με την ταχεία εξέλιξη της υπολογιστικής δύναμης και της προηγμένης κρυπτανάλυσης, αυτά τα πρωτότυπα κρυπτογράφησης έχουν καταστεί εύθραυστα [29]. Ένα από αυτά είναι η λειτουργία κατακερματισμού. Για παράδειγμα, το SHA256 είναι η συνάρτηση κατακερματισμού που χρησιμοποιείται στην αλυσίδα Blockchain του Bitcoin, το οποίο είναι ευάλωτο σε διάφορες απειλές στον κυβερνοχώρο, όπως οι επιθέσεις preimage και σύγκρουσης. Μια επίθεση preimage είναι όταν ο εισβολέας λαμβάνει μια έξοδο Y μέσω κατακερματισμού (hashing) μιας εισόδου m· ο εισβολέας προσπαθεί να βρει μια είσοδο m * έτσι ώστε ο κατακερματισμός του m * να ισούται με Y. Ωστόσο, η προσπάθεια του εισβολέα να εντοπίσει δύο εισόδους που παρέχουν τον ίδιο κατακερματισμό θεωρείται επίθεση σύγκρουσης [28]. Ο πιθανός αντίκτυπος της εκτέλεσης της επίθεσης preimage επί του μπλοκ αλυσίδας Bitcoin μπορεί να οδηγήσει στην αποκάλυψη μιας διεύθυνσης ή στην πλήρη αποτυχία του blockchain ενώ η επίπτωση της επίθεσης σύγκρουσης μπορεί να κλαπεί για να καταστρέψει τα νομίσματα ή να

αρνηθεί την πληρωμή. Παρόλο που απαιτείται τεράστια υπολογιστική ισχύς για την πραγματοποίηση τέτοιων επιθέσεων, οι επιθέσεις μπορεί να είναι δυνατές αν ο αντίπαλος έχει κβαντική υπολογιστική ή κυριαρχεί σε μια τεράστια δεξαμενή εξόρυξης.

- **Εξόρυξη Κακόβουλου Λογισμικού:** Το Cryptojacking είναι όταν ο αντίπαλος εγκαθιστά κακόβουλο λογισμικό στο μηχάνημα-στόχο ή σε μια κινητή συσκευή για να χρησιμοποιήσει την υπολογιστική του ισχύ για να εξορύξει μια αλυσίδα, η οποία καταναλώνει μεγάλο όγκο ηλεκτρικής ενέργειας και μπορεί να θέσει σε κίνδυνο τη λειτουργικότητα του συστήματος του στόχου. Μόνο τον Φεβρουάριο του 2018, οι ερευνητές ξεκίνησαν μια εκστρατεία κρυπτογράφησης, η οποία επηρέασε πάνω από 4000 ιστότοπους, συμπεριλαμβανομένων των σελίδων της βρετανικής και αμερικανικής κυβέρνησης. η άλλη καμπάνια στοχεύει εκατομμύρια συσκευές Android. Επιπλέον, η Radiflow - μια εταιρεία ασφάλειας κρίσιμης υποδομής - βρήκε κακόβουλο λογισμικό εξόρυξης κρυπτοσυναλλαγμάτων στο ευρωπαϊκό επιχειρησιακό δίκτυο ύδρευσης, το οποίο είχε τεράστιο αντίκτυπο στα συστήματα [44].

- **Ελαττώματα Λογισμικού:** Υπάρχουν διαφορετικοί τύποι ελαττωμάτων στο λογισμικό των χρηστών των αλυσίδων Blockchain, όπως το περιβάλλον εκτέλεσης (runtime), η συνάφεια και τα ελαττώματα hard fork [57]. Τα ελαττώματα στο λογισμικό των χρηστών της αλυσίδας Blockchain, το οποίο χρησιμοποιείται στο δίκτυο της αλυσίδας, μπορεί να οδηγήσουν στην έκθεση των ιδιωτικών κλειδιών των χρηστών. Το 2014, το Blockchain.info, το οποίο είναι ένας υβριδικός παροχέας πορτοφολιού, έκανε λάθος κατά την αναβάθμιση του λογισμικού τους, καθώς όταν οι χρήστες τους δημιούργησαν ένα νέο ζεύγος κλειδιών στον τοπικό τους υπολογιστή χρησιμοποιώντας το λογισμικό που επηρεάστηκε, οι εισροές αλγορίθμου ECDSA δεν ήταν επαρκώς τυχαίες, σήμαινε ότι ένας αντίπαλος θα μπορούσε να χειριστεί το λογισμικό για να θέσει σε κίνδυνο τα ιδιωτικά κλειδιά των χρηστών προβάλλοντας μόνο τη δημόσια διεύθυνση.

- **Ευπάθειες Διευθύνσεων Χρηστών:** Οι διευθύνσεις στην αλυσίδα Blockchain του Bitcoin είναι ευάλωτες στην απειλή κλοπής ταυτότητας επειδή αυτές οι διευθύνσεις δεν είναι πιστοποιημένες. Για παράδειγμα, μια επίθεση μπορεί να εκτελείται από έναν αντίπαλο για να αλλάξει τη διεύθυνση Bitcoin στόχου στη διεύθυνση του αντιπάλου. Ο αντίπαλος μπορεί να βλάψει τον ιστότοπο προορισμού για να λάβει πληρωμές που προορίζονται για τον στόχο. Ο αντίκτυπος της επίθεσης είναι καταστροφικός, διότι, στην αλυσίδα του

Bitcoin, είναι αδύνατο να επιστραφεί η πληρωμή αν οι κόμβοι του δικτύου την αποδεχθούν και την καταχωρήσουν στο ημερολόγιο [06].

1.4.2 Ευπάθειες Μηχανισμών Συναίνεσης

- **Ευπάθεια του 51%:** Η εδραίωση της αμοιβαίας εμπιστοσύνης στις αλυσίδες Blockchain βασίζεται στον κοινό μηχανισμό συναίνεσης. Ωστόσο, οι επιτιθέμενοι ενδέχεται να ελέγχουν ολόκληρο το δίκτυο αλυσίδων εκμεταλλευόμενοι την ευπάθεια 51%, η οποία είναι ενσωματωμένη στον μηχανισμό. Για παράδειγμα, εάν ένας μόνο χρήστης ή μια ομάδα χρηστών έχει πάνω από το 50% της συνολικής ισχύος κατακερματισμού στα δίκτυα αλυσίδων Blockchain, τα οποία βασίζονται στον PoW mechanism, ο χρήστης ή η ομάδα χρηστών μπορεί να εκμεταλλευτεί την ευπάθεια του 51%. Συνεπώς, η συγκέντρωση της εξορυκτικής δύναμης κάτω από λίγες δεξαμενές εξορύξεως μπορεί να οδηγήσει σε αυτό το ζήτημα. Πρόσφατα, μόνο το GHash.io κυριάρχησε στο 54% της συνολικής ισχύος επεξεργασίας δικτύου Bitcoin για μια ημέρα [20]. Επιπλέον, τα δίκτυα αλυσίδων Blockchain, τα οποία βασίζονται στον μηχανισμό PoS, έχουν επίσης ευπάθεια 51%. Η ευπάθεια μπορεί να αξιοποιηθεί όταν ένας μόνο εξορύκτης (miner) έχει πάνω από το 50% των συνολικών κερμάτων του δικτύου· μια ευπάθεια 51% οδηγεί σε μια επίθεση 51%, που επιτρέπει στον εισβολέα να κάνει τα εξής [59]:

    - Εισχώρηση παραπλανητικών συναλλαγών,
    - Χειρισμός του δικτύου blockchain,
    - Προσπέραση όλων των άλλων χρηστών στο δίκτυο blockchain,
    - Εκτέλεση ενός ταμείου διπλής δαπάνης και
    - Κλοπή των περιουσιακών στοιχείων άλλων χρηστών.

- **Επίθεση Εναλλακτικού Ιστορικού:** Σε αυτήν την επίθεση, ο εισβολέας στέλνει μια συναλλαγή πληρωμής στο στόχο ενώ αυτός ή αυτή εξορύσσουν από κάποια άλλη αλυσίδα που περιλαμβάνει μια παραπλανητική διπλή δαπάνη στη συναλλαγή. Μετά την επιβεβαίωση, ο παραβάτης θα λάβει ένα προϊόν ή μια υπηρεσία από τον στόχο. Εάν ο

επιτιθέμενος κατορθώσει να βρει περισσότερα μπλοκ από την πραγματική αλυσίδα, αυτός ή αυτή διαδίδει το κακόβουλο fork και ανακτά τα κέρματα. Εάν ο επιτιθέμενος δεν μπορεί να προλάβει τους άλλους κόμβους, η επίθεση θα αποτύχει [40].

- **Επίθεση Finney:** Σε αυτήν την επίθεση, μια συναλλαγή προ-εξορύσσεται σε ένα μπλοκ και μια διπλή έκδοση αυτής της συναλλαγής αποστέλλεται σε έναν χρήστη από τον εισβολέα. Μετά την αποδοχή της συναλλαγής και την παράδοση του προϊόντος από τον παραλήπτη, ο εισβολέας προωθεί το μπλοκ, το οποίο περιέχει την αρχική συναλλαγή. Έτσι, η συναλλαγή που αποστέλλεται στον χρήστη δεν θα είναι έγκυρη και ο εισβολέας θα επιτύχει να παράγει μια συναλλαγή διπλής δαπάνης [50].

- **Επίθεση Race:** Αυτή η επίθεση είναι εύκολη στην εκτόξευση σε δίκτυα αλυσίδων, τα οποία βασίζονται στον μηχανισμό PoW· αυτό συμβαίνει κυρίως επειδή ο εισβολέας μπορεί να εκμεταλλευτεί το χρόνο μεταξύ της συναλλαγής δημιουργίας και της συναλλαγής επιβεβαίωσης για να πραγματοποιήσει την επίθεση. Πριν από την εξόρυξη της συναλλαγής επιβεβαίωσης, ο εισβολέας έχει λάβει τα αποτελέσματα της συναλλαγής δημιουργίας, γεγονός που οδηγεί σε διπλή δαπάνη.

- **Επίθεση Vector76:** Αυτή η επίθεση προήλθε αρχικά από τα φόρουμ BitcoinTalk, όπου ένας χρήστης με όνομα Vector76 περιέγραψε μια επίθεση κατά του ηλεκτρονικού πορτοφολιού MyBitcoin, η οποία είχε ως αποτέλεσμα ζητήματα διπλής δαπάνης. Σε αυτή την επίθεση, ο επιτιθέμενος δεν χρειάζεται να δουν δυο διαδοχικά μπλοκ – η εξόρυξη ενός μπλοκ είναι αρκετή για να εκτελέσει αυτή την επίθεση. Ο επιτιθέμενος πρέπει να παρατηρήσει το δίκτυο των αλυσίδων Blockchain για να καθορίσει το χρονοδιάγραμμα των πολλαπλασιαστικών συναλλαγών των κόμβων δικτύου και τον τρόπο με τον οποίο εκπέμπουν μέσω του δικτύου. Ο επιτιθέμενος τότε αναγνωρίζει τους κόμβους που είναι παλαιότεροι στις πολλαπλασιαστικές συναλλαγές από τον στόχο και δημιουργεί μια άμεση σύνδεση με τον στόχο. Μετά από αυτό, ο εισβολέας ξεκινά μια συναλλαγή που κάνει μια νόμιμη κατάθεση στο στόχο και τα μεταφέρει σε ένα μπλοκ χωρίς να το μεταδώσει στο δίκτυο. Ο επιτιθέμενος εξορύσσει το μπλοκ όπως και τους άλλους κόμβους εκτός από το ότι προσθέτει μια επιπλέον συναλλαγή που δεν μεταδίδεται. Όταν ο εισβολέας καταφέρει να ξεκινήσει ένα έγκυρο μπλοκ, δεν το μεταδίδει μέχρι να περάσουν κάποιοι άλλοι κόμβοι. Μόλις ένας κόμβος περάσει ένα μπλοκ, ο επιτιθέμενος μεταδίδει αμέσως το μπλοκ του στο στόχο και εάν ο στόχος δέχεται το μπλοκ εισβολέα πριν από το άλλο μπλοκ, ο στόχος θα δεχτεί το μπλοκ εισβολέα και η συναλλαγή θα κερδίσει μία επιβεβαίωση. Σε

αυτήν την περίπτωση, η αλυσίδα Blockchain συνδέει τον στόχο και οι άλλοι κόμβοι που συνδέονται με το στόχο θα διαιρεθούν κυρίως επειδή ο στόχος που πέρασε στη συναλλαγή γρήγορα θα θεωρήσει τον εισβολέα νόμιμο, ενώ οι άλλοι κόμβοι στο δίκτυο θα θεωρήσουν την άλλη εισαγωγή έγκυρη. Ο εισβολέας μεταφέρει απευθείας τα κέρματα σε μια διαφορετική διεύθυνση που ελέγχεται από τον εισβολέα και ο στόχος θα δημιουργήσει τη συναλλαγή, επειδή ο στόχος πιστεύει ότι πρόκειται για νόμιμη συναλλαγή. Επίσης, ο εισβολέας ξοδεύει τις εισροές μεταφέροντας το κέρμα στον εαυτό του. Οι κόμβοι δικτύου που δεν έλαβαν το πρώτο μπλοκ του εισβολέα θα δεχθούν τη συναλλαγή ως γνήσια συναλλαγή και θα την συμπεριλάβουν στο επόμενο μπλοκ. Εάν ο πρώτος αποκλεισμός του επιτιθέμενου κερδίσει όταν το blockchain έχει διαιρεθεί, ο επιτιθέμενος δεν θα χάσει τίποτα. Ωστόσο, αν το πρώτο μπλοκ αποτύχει, τότε η κατάθεση στο στόχο θα καταστεί άκυρη, αν και η αποσυρόμενη συναλλαγή θα παραμείνει έγκυρη.

1.4.3 Θέματα ευπάθειας δεξαμενής εξόρυξης

- **Επίθεση Block With Holding (BWH):** Σε αυτήν την επίθεση, ο επιτιθέμενος εντάσσεται σε μια ομάδα εξόρυξης για να βοηθήσει τα μέλη της ομάδας στην εξόρυξη. Ωστόσο, ο επιτιθέμενος δεν θα μεταδώσει ποτέ κανένα μπλοκ για να μειώσει το προσδοκώμενο εισόδημα. Αυτή η επίθεση ονομάζεται επίσης «επίθεση σαμποτάζ» επειδή ο εξορύκτης δεν αποκτά τίποτα, αλλά προκαλεί την απώλεια όλων των άλλων [49]

- **Επίθεση Δωροδοκίας:** Αυτή η επίθεση βασίζεται στη δωροδοκία των ορυκτών στη δεξαμενή σε ακριβή forks ή μπλοκ. Ο επιτιθέμενος μπορεί να επικυρώσει τυχαίες συναλλαγές και να τις δημοσιεύσει επειδή έχει πληρώσει σε ανέντιμους κόμβους για να τις επαληθεύσει. Ο επιτιθέμενος μπορεί να κερδίσει την πλειοψηφία των υπολογιστικών πόρων χρησιμοποιώντας τρεις τρόπους δωροδοκίας, δηλαδή την εξωχρηματιστηριακή πληρωμή, την εξόρυξη αρνητικών αμοιβών και την πληρωμή εντός ζώνης. Στην εξωχρηματιστηριακή πληρωμή, ο ιδιοκτήτης υπολογιστικών πόρων πληρώνεται απευθείας από τον εισβολέα για να εξοντώσει τα μπλοκ του εισβολέα. Στην ομάδα εξόρυξης αρνητικών αμοιβών, ο εισβολέας δημιουργεί μια δεξαμενή επιβραβεύοντας την υψηλότερη απόδοση. Τέλος, στην πληρωμή εντός ζώνης, ο επιτιθέμενος επιδιώκει να δωροδοκήσει το ίδιο το blockchain συμπεριλαμβάνοντας δωρεάν χρήματα δωροδοκίας σε κάθε εξορύκτη προσυπογράφει το fork του εισβολέα [13].

- **Επίθεση Pool Hopping:** Σε αυτή την επίθεση, ο εισβολέας κάνει εξόρυξη με βάση το ποσοστό προσφυγής. Αν το ποσοστό είναι υψηλό, ο εισβολέας κάνει εξόρυξη, διαφορετικά εγκαταλείπει την δεξαμενή. Ο εισβολέας χρησιμοποιεί τις πληροφορίες σχετικά με τον αριθμό των μετοχών που έχουν υποβληθεί στην ομάδα εξόρυξης στόχου για να κατανοήσει πόσες μετοχές έχουν υποβληθεί και πόσα μπλοκ έχουν βρεθεί. Χρησιμοποιώντας αυτές τις πληροφορίες, ο επιτιθέμενος σταματά να εξορύσσει στην δεξαμενή-στόχο και συνεισφέρει αλλού. Η κεντρική ιδέα πίσω από αυτή την επίθεση είναι ότι ο επιτιθέμενος επιλέγει διάφορες δεξαμενές για να αποκτήσει το μέγιστο εισόδημα (Rosenfeld, 2011).

- **Επίθεση Απόρριψης Μπλοκ:** Σε αυτήν την επίθεση, σε σύγκριση με τους «ειλικρινείς» κόμβους, ο επιτιθέμενος πρέπει να διαθέτει επαρκή αριθμό συνδέσεων δικτύου και να κυριαρχεί σε πολλαπλούς κόμβους για να αυξήσει την υπεροχή του δικτύου του. Μόλις ο επιτιθέμενος ενημερωθεί για τα νεοαποκτηθέντα μπλοκ, αυτός δημοσιεύει αμέσως το δικό του μπλοκ, το οποίο πρέπει να είναι ταχύτερο από τα υπόλοιπα στο δίκτυο. Επομένως, όταν ένας κόμβος δημοσιεύει ένα μπλοκ, ο επιτιθέμενος μπορεί να διαδώσει αμέσως τα δικά του μπλοκ για να απορρίψει τα μπλοκ των έντιμων κόμβων [10].

- **Εγωιστική Επίθεση Εξόρυξης:** Σε αυτήν την επίθεση, μια ομάδα επιτιθέμενων συνωμοτούν για να δημιουργήσουν μια ομάδα εξόρυξης για να αναιρέσουν την ειλικρινή εργασία των εξορυκτών και να αποκτήσουν καλύτερα εισοδήματα για τον εαυτό τους. Οι επιτιθέμενοι εξορύσσουν στο ιδιωτικό blockchain τους και το μεταδίδουν με βάση τη διαφορά μήκους μεταξύ δημόσιων και ιδιωτικών blockchains για να επηρεάσουν τις ανταμοιβές [51].

- **Επίθεση Fork After Withholding (FAW):** Το αποτέλεσμα της επίθεσης FAW είναι ίσο ή μεγαλύτερο από το αποτέλεσμα επίθεσης BWH και η επίθεση είναι τέσσερις φορές πιο καρποφόρα, συνήθως ανά δημοσκόπηση, από την επίθεση BWH. Αυτή η επίθεση έχει δύο τύπους: επίθεση FAW μίας δεξαμενής και επίθεση FAW με πολλαπλές δεξαμενές. Αυτή η επίθεση συνδυάζει την εγωιστική επίθεση εξόρυξης και την επίθεση BWH. Στην επίθεση FAW μιας μονάδας, ο επιτιθέμενος συνδέεται με την ομάδα εξόρυξης στόχου και εκτελεί την επίθεση εναντίον του, ενώ στην επίθεση FAW με πολλαπλές δεξαμενές ο επιτιθέμενος επιδιώκει να αυξήσει το εισόδημά του διευρύνοντας την επίθεση εναντίον πολλών ομάδων. Η υπολογιστική δύναμη του επιτιθέμενου χωρίζεται σε αυτή την επίθεση σε εξόρυξη διείσδυσης και αθώα εξόρυξη. Όταν το τμήμα διείσδυσης εισβολέα εντοπίζει μια

πλήρη απόδειξη εργασίας (FPoW), ο επιτιθέμενος κρατά το μπλοκ και δεν το μεταδίδει. Με βάση τα επόμενα βήματα, ο επιτιθέμενος μπορεί να δημοσιεύσει το ιδιωτικό του μπλοκ στον διαχειριστή της ομάδας στόχου, ελπίζοντας ότι ένα fork δημιουργείται ταυτόσημο με την εγωιστική επίθεση εξόρυξης ή ο επιτιθέμενος απορρίπτει το μπλοκ που είναι πανομοιότυπο με την επίθεση BWH [36].

1.4.4 Θέματα Ευπάθειας Δικτύου

- **Επιθέσεις Διαχωρισμού:** Σε αυτήν την επίθεση, ο εισβολέας απομονώνει μια ομάδα κόμβων από το υπόλοιπο δίκτυο blockchain του Bitcoin και το δίκτυο είναι χωρισμένο σε διαφορετικά στοιχεία. Ο εισβολέας αποσπά τα πιο συγκεκριμένα προθέματα, τα οποία φιλοξενούν κάθε διεύθυνση IP απομονωμένων κόμβων για να ανακατευθύνουν την κίνηση που προορίζεται για αυτούς. Η κίνηση υποκλέπτεται από τον εισβολέα κατά τη στιγμή που συμβαίνει και καθορίζει ποιες συνδέσεις διασχίζουν το διαχωρισμένο τμήμα που προσπαθεί να δημιουργήσει ο εισβολέας. Εάν η σύνδεση δεν διασχίσει το διαχωρισμένο τμήμα, ο εισβολέας εγκαταλείπει τα πακέτα δεδομένων, διαφορετικά, η σύνδεση περιέχεται στους απομονωμένους κόμβους. Ο εισβολέας παρακολουθεί τα ανταλλασσόμενα μηνύματα για να καθορίσει τα σημεία διαρροής, αυτοί είναι οι κόμβοι στην απομονωμένη ομάδα, οι οποίοι διατηρούν συνδέσεις με τους εξωτερικούς κόμβους και ο αντίπαλος δεν μπορεί να παρεμποδίσει. Ο αντίπαλος απομονώνει τελικά τα σημεία διαρροής από άλλους κόμβους της απομονωμένης ομάδας [04].

- **Επίθεση Καθυστέρησης:** Στην προηγούμενη επίθεση, ο αντίπαλος έπρεπε να αποκτήσει τον πλήρη έλεγχο της κυκλοφορίας του στόχου για να εκτελέσει αποτελεσματικά την επίθεση. Αντίθετα, η επίθεση καθυστέρησης μπορεί να προκαλέσει σημαντικές καθυστερήσεις στη δημοσίευση μπλοκ, ακόμη και όταν ο αντίπαλος παρακολουθήσει μόνο μία από τις συνδέσεις του στόχου. Πρώτον, ο εισβολέας μεταβάλλει το περιεχόμενο συγκεκριμένων μηνυμάτων για να καθυστερήσει την παράδοση του μπλοκ· αυτό είναι εφικτό λόγω έλλειψης ελέγχων ακεραιότητας και κρυπτογράφησης των μηνυμάτων Bitcoin. Επιπρόσθετα, ο αντίπαλος κάνει χρήση του γεγονότος ότι οι κόμβοι στέλνουν πρώτα αιτήματα μπλοκ στον ομότιμο που οδήγησε κάθε μπλοκ και περιμένουν 20 λεπτά για να το παραδώσουν προτού το ζητήσουν από έναν άλλο ομότιμο. Έτσι, ο αντίπαλος παραδίδει ένα μπλοκ σε έναν κόμβο-στόχο σε διάστημα 20 λεπτών, γεγονός που καθιστά

τον στόχο μη ενημερωμένο για τα πιο πρόσφατα εξορυγμένα μπλοκ και καθιστά τον στόχο αδύνατο να συνεισφέρει στο δίκτυο [04].

- **Επίθεση διανεμημένης άρνησης εξυπηρέτησης (Distributed Denial-of-Service - DDoS):** Σήμερα, η "Επίθεση Διανεμημένης Άρνησης Εξυπηρέτησης (Distributed Denial-of-Service - DDoS)" είναι μία από τις πιο κοινές και φθηνές επιθέσεις στο Διαδίκτυο. Παρά το γεγονός ότι είναι μια τεχνολογία peer-to-peer, εξακολουθεί να υπάρχει ευαλωτότητα στην επίθεση DDoS. Δίκτυα όπως το Ethereum και το Bitcoin, συχνά υποβλήθηκαν σε αυτές τις επιθέσεις. Για παράδειγμα, 40 υπηρεσίες Bitcoin υπέστησαν 142 επιθέσεις DDoS σε διάστημα δύο ετών και οι στόχοι περιελάμβαναν το 7% όλων των δημοφιλών φορέων. Οι περισσότερες από αυτές τις επιθέσεις απευθύνονταν σε μεγάλες δεξαμενές εξόρυξης και σε υπηρεσίες συναλλάγματος λόγω της μεγαλύτερης δυνατότητας πώλησης. Αυτές οι επιθέσεις ανάγκασαν επιχειρήσεις όπως το BitQuick και το CoinWallet να διακόψουν την υπηρεσία τους μετά από μερικούς μήνες από την έναρξή τους [20].

- **Επίθεση Sybil:** Σε αυτή την επίθεση, ο αντίπαλος δημιουργεί ψεύτικους κόμβους και επιχειρεί να εκθέσει μέρος του δικτύου blockchain. Ο αντίπαλος μπορεί να χρησιμοποιήσει μια ομάδα εκτεθειμένων κόμβων για να εκτελέσει την επίθεση, για να απομονώσει τον στόχο και να αποσυνδέσει τις συναλλαγές που δημιουργούνται από τον στόχο, ή ο εισβολέας θα κάνει το χρήστη να επιλέξει μόνο τα μπλοκ που διατηρεί ο ίδιος. Ο αντίπαλος με κακόβουλους κόμβους θα περιβάλλει τον στόχο. Ο στόχος θα σκεφτεί ότι αυτός ή αυτή εξακολουθεί να συνδέεται με το δίκτυο μέσω διαφορετικών ειλικρινών κόμβων. Ωστόσο, η πραγματικότητα είναι ότι ο στόχος έχει περιορισμένη πρόσβαση στο δίκτυο επειδή ο αντίπαλος ελέγχει όλους τους κόμβους στους οποίους συνδέεται. Μόλις ο αντίπαλος περιβάλλει τον στόχο, αυτός ή αυτή μπορεί να αρνηθεί να αναμεταδώσει τις συναλλαγές του στόχου. Εκτός αυτού, ο αντίπαλος μπορεί να τροφοδοτεί παραπλανητικές πληροφορίες στο στόχο της κατάστασης του δικτύου. Μια επιτυχημένη επίθεση Sybil μπορεί να καταστήσει ανενεργή τη λειτουργικότητα του αλγόριθμου συναίνεσης και να προκαλέσει πιθανή επίθεση διπλής δαπάνης.

- **Επίθεση Time Jacking:** Αυτή η επίθεση είναι μια συγκεκριμένη επίθεση στο δίκτυο blockchain του Bitcoin. Ο χρόνος δικτύου σε αυτό το δίκτυο διατηρείται από πλήρεις κόμβους. Ο χρόνος του δικτύου αποκτάται με τη λήψη ενός μηνύματος έκδοσης από τους γειτονικούς κόμβους. Ο διάμεσος υπολογίζεται και αν ο διάμεσος χρόνος όλων των γειτονικών κόμβων υπερβαίνει τα 70 λεπτά, ο μετρητής χρόνου δικτύου επιστρέφει από

προεπιλογή στον χρόνο του συστήματος κόμβων. Όταν ο αντίπαλος συνδέεται με τον κόμβο-στόχο, προσπαθεί να αποκαλύψει αόριστες χρονικές σημάνσεις. Μόλις ο αντίπαλος τροποποιήσει τον μετρητή χρόνου δικτύου του κόμβου, ο παραπλανημένος κόμβος μπορεί να υιοθετήσει υποκατάστατο blockchain. Αυτή η επίθεση θα απομονώσει τον κόμβο προορισμού από το δίκτυο ή θα μειώσει την τιμή επιβεβαίωσης συναλλαγής σε ολόκληρο το δίκτυο [50].

- **Επίθεση Μεταβλητότητας Συναλλαγής:** Η μεταβλητότητα της συναλλαγής είναι μια ευπάθεια στο δίκτυο blockchain Bitcoin, το οποίο επιτρέπει στον αντίπαλο να αλλάξει το αναγνωριστικό συναλλαγής (TXID) χωρίς να ανακαλέσει τη συναλλαγή. Η τροποποίηση του TXID θα εξαπατήσει το θύμα να πιστέψει ότι η συναλλαγή απέτυχε, αν και επιβεβαιώνεται αργότερα. Οι ανταλλαγές συναλλάγματος αποτελούν τους κοινούς στόχους για αυτήν την επίθεση. Ο αντίπαλος αποσύρεται από μια ανταλλαγή και στη συνέχεια αναδημοσιεύει την ίδια συναλλαγή με ένα διαφορετικό TXID και ένα από αυτά θα εμφανίζεται στο δίκτυο. Λόγω καθυστερήσεων, είναι πολύ πιθανό ότι η μεταβληθείσα συναλλαγή θα κερδίσει παρά την αρχική απόσυρση. Η ανταλλαγή νομισμάτων δεν θα εντοπίσει την αρχική συναλλαγή στο δίκτυο και θα σκεφτεί ότι η συναλλαγή απέτυχε εάν η ανταλλαγή βασίζεται μόνο σε TXIDs. Έτσι, ο αντίπαλος μπορεί να αποσύρει συνεχώς.

1.4.5 Ευπάθειες Έξυπνου Συμβολαίου

Δύο από τις μεγαλύτερα ευπάθειες του Ethereum συζητούνται στα εξής: Ευάλωτα χαρακτηριστικά στην εικονική μηχανή του Ethereum (Ethereum Virtual Machine - EVM) και ευπάθειες της Solidity του Ethereum.

- **Ευάλωτα Χαρακτηριστικά Εικονικής Μηχανής Ethereum:** Το EVM είναι μια εικονική μηχανή που τρέχει τον bytecode, το οποίο είναι το αποτέλεσμα της σύνταξης του πηγαίου κώδικα ενός έξυπνου συμβολαίου. Κάθε λειτουργία στο EVM καταναλώνει μια συγκεκριμένη ποσότητα υπολογιστικού πόρου. Ο υπολογιστικός πόρος αντιπροσωπεύει το κόστος εκτέλεσης κώδικα.

- **Αδυναμίες Solidity:** Η Solidity είναι η έξυπνη γλώσσα προγραμματισμού υψηλού επιπέδου στο Ethereum, την οποία ο προγραμματιστής χρησιμοποιεί για να γράψει τον πηγαίο κώδικα του έξυπνου συμβολαίου. Υπάρχουν έξι γνωστοί τύποι ευπάθειας στους πηγαίους κώδικες έξυπνων συμβάσεων, οι οποίοι έχουν ήδη χρησιμοποιηθεί και

αντιπροσωπεύουν το υψηλότερο μέρος του αριθμού ευπάθειας των έξυπνων συμβολαίων. Τα περισσότερα από αυτά τα τρωτά σημεία προέρχονται από μια κακή ευθυγράμμιση μεταξύ των προθέσεων των προγραμματιστών και της σημασιολογίας της Solidity (Antzei et al., 2017)

Κεφάλαιο 2
Η Πλατφόρμα Hyperledger Fabric

Το αυξανόμενο ενδιαφέρον από τη βιομηχανία πυροδότησε την ανάπτυξη νέων πλατφορμών όπως είναι οι αλυσίδες συστοιχιών ή αλλιώς μπλοκ αλυσίδας, τα λεγόμενα blockchain, που έχουν σχεδιαστεί με βάση την αντίστοιχη τεχνολογία η οποία κερδίζει διαρκώς έδαφος σε πολλούς τομείς εκτός της βιομηχανίας, όπως είναι η παιδεία, η υγεία κλπ. Επίσης, εκτός από τις ερευνητικές περιοχές χρησιμοποιείται ευρύτατα και στον χώρο της πολιτικής όπως για παράδειγμα στις εκλογές [03].

Η δημοτικότητα των τεχνολογιών blockchain προέρχεται από τις επιχειρηματικές εφαρμογές της που τρέχουν ανάμεσα σε ένα σύνολο τεράστιων δυνατοτήτων ανάπτυξης ενός ευρέος φάσματος κατανεμημένων αναγνωρίσιμων συμμετεχόντων που δεν εμπιστεύονται πλήρως ο ένας τον άλλον, επιτρέποντας την ασφαλή συνεργασία μεταξύ τους [11]. Αυτή είναι μια φυσική εξέλιξη για την αντιμετώπιση των απαιτήσεων που θέτουν οι επιχειρηματικές εφαρμογές που τρέχουν blockchain ανάμεσα σε ένα σύνολο αναγνωρίσιμων συμμετεχόντων που δεν έχουν μεταξύ τους εμπιστοσύνη.

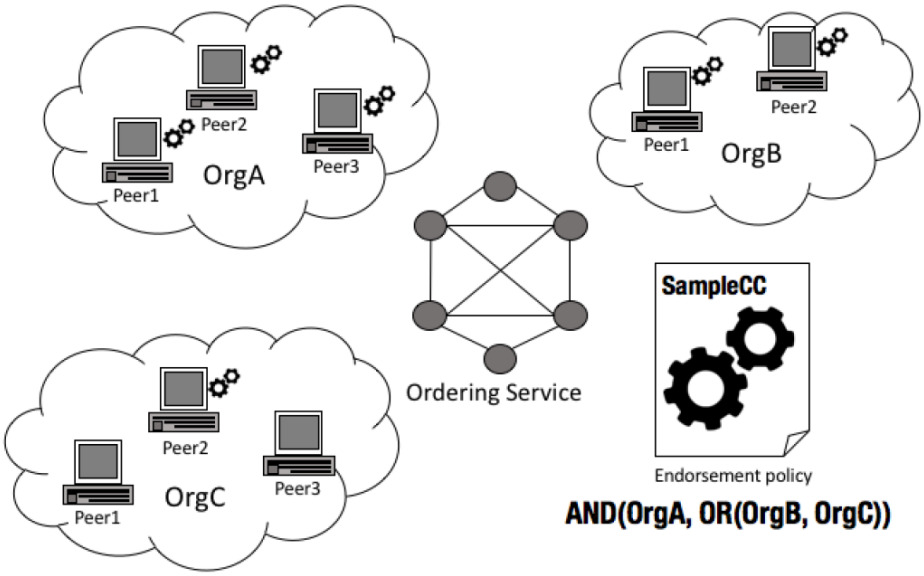
Η εφαρμογή bitcoin ήταν ο προκάτοχος της μεταβλητής δομής δεδομένων. Πρόκειται για ένα κατανεμημένο παγκόσμιο πρότυπο που επιτρέπει τη μεταφορά των εγγενών αρχείων συναλλαγών μεταξύ των συμβαλλόμενων μερών που δεν έχουν εμπιστοσύνη ο ένας στον άλλο, δηλαδή από τον ένα ιδιοκτήτη στον άλλο . Συνήθως, οι έξυπνες συναλλαγές συμβολαίων ομαδοποιούνται σε μπλοκ αλυσίδας. Πολλοί αδειούχοι των blockchains χρησιμοποιούν ένα αναπαραγόμενο πάνω από αυτά τα μπλοκ. Αυτή η διαδικασία αποτελεί ένα παγκόσμιο πρότυπο διαχειριστικής λειτουργίας του μηχανισμού. Ως εκ τούτου, τα πρωτόκολλα blockchain παρουσιάζουν χαρακτηριστικά που επιτυγχάνουν συναλλαγές οι οποίες περιορίζουν σημαντικά την απόδοση. Η Hyperledger Fabric (HLF) είναι ένα έργο που περιλαμβάνει πολλά μπλοκ αλυσίδων (blockchains) ανοιχτού κώδικα καθώς και άλλα σχετικά εργαλεία. Η Hyperledger Fabric (HLF) ξεκίνησε το Δεκέμβριο του 2015 από το Ίδρυμα Linux με παράλληλη βοήθεια από την IBM, την Intel και το SAP Ariba, έτσι ώστε να υποστηρίξει τη συνεργατική ανάπτυξη του blockchain [34, 47, 56].

Όσον αφορά το Bitcoin, επισημαίνεται ότι αυτό λειτουργεί με πλατφόρμες blockchain μετά το νέο παράδειγμα δημοσίως, όπου ο καθένας μπορεί να ενταχθεί ή να εγκαταλείψει το blockchain της εκτέλεσης – παραγγελίας – επικύρωσης για κατανεμημένη εκτέλεση του έξυπνου δικτύου, ενώ παράλληλα κανείς δεν υποχρεούται να καθορίσει την πραγματική του ταυτότητα [03]. Όσον αφορά το πρωτόκολλο συναίνεσης που περιλαμβάνεται στα μπλοκ αλυσίδων, φαίνεται ότι αυτό έχει πολλά σημαντικά μειονεκτήματα. Ειδικότερα, οι επικυρωμένες συναλλαγές δεσμεύονται για το blockchain και έτσι εμφανίζεται ένα τεράστιο υπολογιστικό κόστος. Επίσης, ένα μειονέκτημα είναι η πιθανοτική φύση της συναλλαγής που εκτελείται παράλληλα από αδιάσειστα υποσύνολα ομότιμων, όπως και η αύξηση της επιβεβαίωσης, που οδηγεί σε μεγάλη καθυστέρηση, και η μείωση της ταχύτητας. Αυτοί οι παράγοντες καθιστούν τις δημόσιες αλυσίδες κλειδώματος ακατάλληλες για την εφαρμογή εταιρικού βαθμού.

Οι επικυρωμένες συναλλαγές στη συνέχεια δεσμεύονται στην κατάσταση blockchain. Αυτή η αρχιτεκτονική επιτρέπει την παράλληλη εκτέλεση πολλαπλών συναλλαγών από ασύγκριτα υποσύνολα ομότιμων υπολογιστών, αυξάνοντας την ταχύτητα. Όμως, οι μη έγκυρες συναλλαγές απορρίπτονται στη φάση επικύρωσης [11]. Η πολιτική έγκρισης αφορά το σύνολο των κανόνων που καθορίζει ποιο υποσύνολο υπολογιστών θα πρέπει να εκτελέσει μια συναλλαγή και τι συνιστά έγκυρη εκτέλεση. Κατά μία έννοια, η Hyperledger Fabric (HLF) επωφελείται από το συνδυασμό δύο γνωστών προσεγγίσεων για την αναπαραγωγή, δηλαδή την παθητική και την ενεργητική. Οι εφαρμογές blockchain συνήθως αποτελούνται από δύο βαθμίδες: η πρώτη -που ονομάζεται "βαθμίδα πλατφόρμας" - επικεντρώνεται στην ενσωμάτωση του σχήματος

δεδομένων και την ενσωμάτωση επιχειρηματικών κανόνων στο blockchain μέσω πολιτικών chaincode και έγκρισης. Η δεύτερη -που ονομάζεται "επίπεδο πελάτη" - χρησιμοποιεί το κιτ ανάπτυξης λογισμικού (SDK) που παρέχεται από την Hyperledger Fabric (HLF) για την υλοποίηση εφαρμογών από την πλευρά του πελάτη [03].

Πριν από την Hyperledger Fabric, όλες οι πλατφόρμες blockchain, χωρίς άδεια ή με άδεια, ακολουθούσαν το μοτίβο εκτέλεσης παραγγελιών. Δηλαδή, οι συμμετέχοντες στο δίκτυο χρησιμοποιούν ένα πρωτόκολλο συναίνεσης για να ξεκινήσουν συναλλαγές, και μόνο όταν αποφασιστεί η εντολή, τότε όλες οι συναλλαγές εκτελούνται διαδοχικά, εφαρμόζοντας έτσι ουσιαστικά την ενεργή αναπαραγωγή κατάστασης. Η προσέγγιση εκτέλεσης εντολής όμως θέτει ένα σύνολο περιορισμών [21].



Σχήμα 2.1: Δομή υψηλού επιπέδου του δικτύου blockchain Hyperledger Fabric. Παρουσιάζεται μια ανάπτυξη που περιλαμβάνει τρεις οργανισμούς OrgA, OrgB και OrgC, συμπεριλαμβανομένων ενός, δύο και τριών ομότιμων χριστών αντίστοιχα. Το chaincode SampleCC αναπτύσσεται σε ορισμένους από τους ομότιμους και η σχετική πολιτική έγκρισης απαιτεί τις υπογραφές τουλάχιστον ενός ομότιμου από το OrgA και τουλάχιστον μία φόρμα από ομότιμους είτε OrgB είτε OrgC. Η υπηρεσία παραγγελιών είναι υπεύθυνη για τη συνολική σειρά συναλλαγών. [03]

Το γεγονός ότι οι συναλλαγές πρέπει να εκτελούνται διαδοχικά και αποτελεσματικά οδηγεί σε υποβάθμιση της διοίκησης, δημιουργώντας συμφόρηση. Η Hyperledger Fabric παρέχει μια αρθρωτή αρχιτεκτονική και εισάγει μια νέα διαδικασία για εκτέλεση- παραγγελία- επικύρωση για την αντιμετώπιση των περιορισμών της εντολής - εκτέλεσης που αναφέρεται παραπάνω. Μια κατανεμημένη εφαρμογή Hyperledger αποτελείται βασικά από δύο κύρια μέρη (Σχήμα 2.1):

- **Chaincode:** είναι επιχειρηματική λογική που εφαρμόζεται σε μια γλώσσα προγραμματισμού γενικού σκοπού (Java, Go, Javascript) και χρησιμοποιείται κατά τη διάρκεια της φάσης εκτέλεσης. Το chaincode είναι συνώνυμο της γνωστής έννοιας των έξυπνων συμβάσεων και αποτελεί βασικό στοιχείο της Hyperledger Fabric, η οποία εκτελείται με κατανεμημένο τρόπο.

- **Πολιτικές έγκρισης:** είναι κανόνες που καθορίζουν ποιο είναι το σωστό σύνολο των ομότιμων που είναι υπεύθυνοι για την εκτέλεση και την έγκριση μιας δεδομένης χρήσης του chaincode. Οι εν λόγω ομότιμοι διέπουν την εγκυρότητα των αποτελεσμάτων εκτέλεσης του κώδικα αλυσίδας, παρέχοντας μια υπογραφή σε αυτά τα αποτελέσματα. Οι πολιτικές έγκρισης ορίζονται με λογικές εκφράσεις όπως: AND (OrgA;OR(OrgB;OrgC)) [03].

2.1 Αρχιτεκτονική Δικτύου Hyperledger Fabric

Το δίκτυο blockchain της Hyperledger Fabric σχηματίζεται από κόμβους που θα μπορούσαν να ταξινομηθούν σε τρεις κατηγορίες με βάση τους ρόλους τους:

- **Πελάτες (clients):** είναι κόμβοι δικτύου που εκτελούν τον κωδικό εφαρμογής, ο οποίος συντονίζει την εκτέλεση συναλλαγών. Ο κωδικός εφαρμογής προγράμματος - πελάτη χρησιμοποιεί συνήθως το HLF SDK για να επικοινωνήσει με την πλατφόρμα.

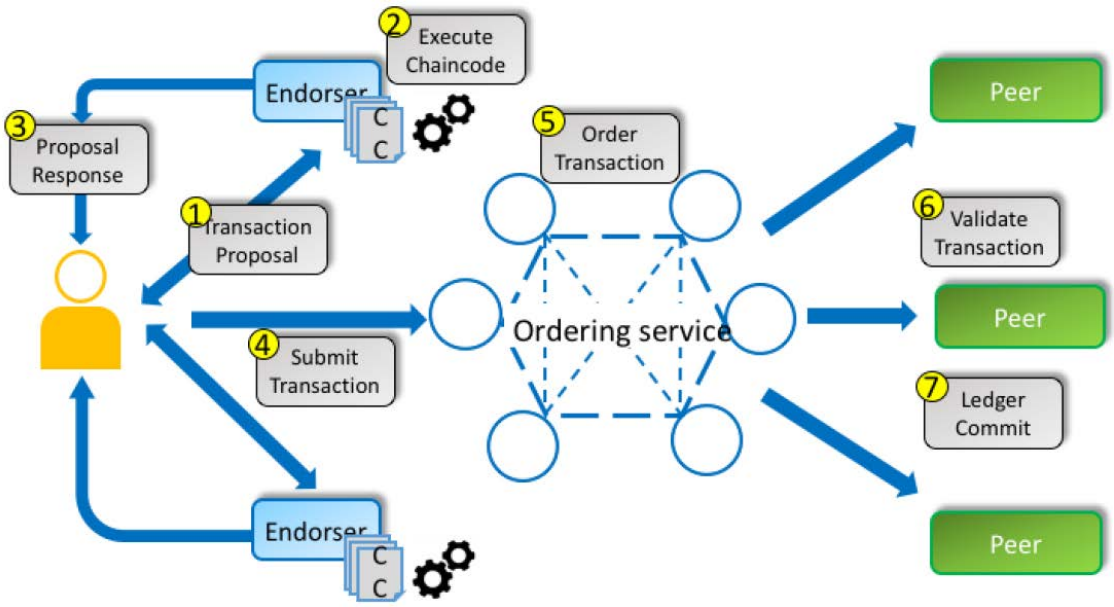
- **Ομότιμοι (Peers):** είναι κόμβοι πλατφόρμας που διατηρούν το αρχείο συναλλαγών χρησιμοποιώντας ένα παγκόσμιο πρότυπο μόνο για προσάρτηση και είναι υπεύθυνοι για την εκτέλεση του chaincode και του κύκλου ζωής του. Αυτοί οι κόμβοι διατηρούν επίσης μια "κατάσταση" με τη μορφή ενός χώρου αποθήκευσης κλειδιών - τιμών έκδοσης. Προκειμένου να επιτραπεί η εξισορρόπηση φορτίου, δεν είναι όλοι οι ομότιμοι υπεύθυνοι για την εκτέλεση του chaincode, αλλά μόνο ένα υποσύνολο των ομότιμων χρηστών υποστηρίζει αυτούς [27].

- **Ταξινομημένων κόμβων (Ordering nodes):** είναι κόμβοι πλατφόρμας που σχηματίζουν ένα σύμπλεγμα που εκθέτει μια αφαίρεση ατομικής μετάδοσης προκειμένου να καθοριστεί η συνολική σειρά μεταξύ όλων των συναλλαγών. Οι κόμβοι παραγγελίας αγνοούν εντελώς την κατάσταση της εφαρμογής και δεν συμμετέχουν στην επικύρωση ή

την εκτέλεση συναλλαγών. Προκειμένου να παρέχει καλύτερη προστασία της ιδιωτικής ζωής και της εμπιστευτικότητας η Hyperledger Fabric εισάγει την έννοια των καναλιών, ένα υψηλό επίπεδο αφαίρεσης που αντιπροσωπεύει ουσιαστικά ένα απομονωμένο δίκτυο blockchain [16]. Κάθε κανάλι μπορεί να περιέχει διαφορετικά ή ακόμα και ασύνδετα σύνολα ομότιμων υπολογιστών, επιτρέποντας έτσι τον διαχωρισμό της κατάστασης εφαρμογής επιτυγχάνοντας μεγαλύτερη προστασία της ιδιωτικής ζωής με το διαχωρισμό των δεδομένων σε διαφορετικούς κόμβους.

2.2 Ροή Εκτέλεσης Συναλλαγής

Παρακάτω συνοψίζεται η ροή εκτέλεσης μιας συναλλαγής που υποβάλλεται από έναν πελάτη στη Hyperledger Fabric (HLF) (Σχήμα 2.2):



Σχήμα 2.2: Hyperledger Fabric (HLF) - υψηλή ροή συναλλαγής επιπέδων. Ο πελάτης (κίτρινο σκαρίφημα) προτείνει μια συναλλαγή στους ομότιμους χρήστες που υποστηρίζουν (μπλε) και συλλέγει απαντήσεις. Στη συνέχεια, ο πελάτης υποβάλλει μια συναλλαγή στην υπηρεσία παραγγελίας, η οποία διατάσσει εισερχόμενες συναλλαγές και τις μοιράζει σε μπλοκ. Οι ομότιμοι (πράσινοι) αποσύρουν τα μπλοκ από την υπηρεσία παραγγελίας, επικυρώνουν τις συναλλαγές, τις προσαρτούν στο παγκόσμιο πρότυπο και εφαρμόζουν έγκυρες συναλλαγές στην κατάσταση. [16]

- Ο πελάτης (client) χρησιμοποιεί ένα SDK για να σχηματίσει μια πρόταση συναλλαγής, η οποία περιλαμβάνει: το όνομα του καναλιού, το όνομα του κωδικού αλυσίδας που πρέπει να καλέσει και τις παραμέτρους εισόδου στον κωδικό αλυσίδας. Στη συνέχεια, ο πελάτης

αποστέλλει την πρόταση συναλλαγής σε όλους τους ομότιμους που υποστηρίζουν για να ικανοποιήσει την πολιτική έγκρισης του συγκεκριμένου κωδικού αλυσίδας [21].

- Η έγκριση των ομότιμων (peers) προσομοιώνει τη συναλλαγή με βάση τις παραμέτρους που λαμβάνονται από τον πελάτη. Οι ομότιμοι που υποστηρίζουν επικαλούνται τον κωδικό αλυσίδας, καταγράφουν ενημερώσεις κατάστασης και εκτελούν την παραγωγή με τη μορφή ενός συνόλου ανάγνωσης - εγγραφής με έκδοση. Στη συνέχεια, κάθε ομότιμος υπολογιστής υπογράφει το σύνολο read-write και επιστρέφει το αποτέλεσμα πίσω στον υπολογιστή - πελάτη.

- Ο πελάτης συλλέγει απαντήσεις από όλους τους ομότιμους χρήστες του δικτύου που υποστηρίζουν, επικυρώνει ότι τα αποτελέσματα είναι συνεπή, δηλαδή όλοι οι ομότιμοί τους έχουν υπογράψει το ίδιο ωφέλιμο φορτίο. Στη συνέχεια, συνενώνει όλες τις υπογραφές των ομότιμων που υποστηρίζουν μαζί με τα σύνολα ανάγνωσης- εγγραφής, δημιουργώντας μια συναλλαγή που υποβάλλεται στην υπηρεσία παραγγελίας [18].

- Η υπηρεσία ταξινόμησης συλλέγει όλες τις εισερχόμενες συναλλαγές, τις διατάζει να επιβάλλουν συνολική σειρά συναλλαγών σε ένα πλαίσιο καναλιού και περικόπτει περιοδικά μπλοκ που περιλαμβάνουν όλες αυτές τις συναλλαγές που ταξινομήθηκαν.

- Για κάθε οργανισμό, ένα μόνο peer τραβά νέα μπλοκ από την υπηρεσία παραγγελίας και τη διάδοσή τους με τη χρήση middleware για την αναπαραγωγή παγκόσμιων προτύπων.

- Μετά τη λήψη ενός νέου μπλοκ, κάθε peer επαναλαμβάνει τις συναλλαγές σε αυτό και επικυρώνει: α) την πολιτική έγκρισης, δηλαδή κατά πόσον το σύνολο των υπογραφών που υποστηρίζουν τους ομότιμους χρήστες ικανοποιεί την πολιτική έγκρισης που σχετίζεται με τον κωδικό αλυσίδας β) εκτελεί ελέγχους ταυτοχρονισμού πολλαπλών εκδόσεων σε βάρος της κατάστασης [03].

- Μόλις ολοκληρωθεί η επικύρωση συναλλαγής, ο ομότιμος προσαρτά το μπλοκ στο παγκόσμιο πρότυπο και ενημερώνει την κατάστασή του με βάση έγκυρες συναλλαγές. Μετά τη δέσμευση του μπλοκ, ο ομότιμος υπολογιστής εκπέμπει συμβάντα για να ειδοποιήσει τους υπολογιστές - πελάτες που είναι συνδεδεμένοι σε αυτό.

Ένα από τα άμεσα οφέλη της αρχιτεκτονικής Hyperledger Fabric (HLF) είναι η δυνατότητα ανεξάρτητης κλίμακας σε κάθε μία από τις φάσεις επικύρωσης της εντολής εκτέλεσης. Ωστόσο, το πέμπτο στάδιο της ροής εκτέλεσης συναλλαγών - η διάδοση των μπλοκ σε ομότιμους χρήστες - θέτει πρόσθετες προκλήσεις. Οι περισσότεροι αλγόριθμοι συναίνεσης (τόσο BFT και CFT) είναι πολύ ευαίσθητοι στο διαθέσιμο εύρος ζώνης, και ως εκ τούτου, η δυνατότητα να κλιμακωθεί η υπηρεσία παραγγελίας περιορίζεται από τη χωρητικότητα του δικτύου των κόμβων της [33].

Προσπάθειες οριζόντιας κλιμάκωσης της συναίνεσης με την προσθήκη περισσότερων κόμβων υπηρεσιών παραγγελίας, οδηγούν τελικά σε υποβάθμιση της διχοτόμησης. Ευτυχώς, η αποσύνδεση μεταξύ της παραγγελίας και της επικύρωσης επιτρέπει τον μετριασμό αυτού του περιορισμού, επινοώντας ένα κλιμακούμενο στρώμα επικοινωνίας που είναι υπεύθυνο για την αποτελεσματική διάδοση μπλοκ [25].

2.3 Διάδοση Φραγμών

Τα πρωτόκολλα φραγμών ανταλλάσσουν τις παραδοσιακές ισχυρές εγγυήσεις αξιοπιστίας υπέρ μιας πιθανοτικής προσέγγισης, που οδηγεί στη μεγαλύτερη επεκτασιμότητα και την ανοχή των ελαττωμάτων. Το στρώμα φραγμών του Hyperledger Fabric (HLF) χρησιμοποιεί έναν συνδυασμό ώθησης - τραβήγματος για την αξιοπιστία και την αποδοτικότητα των φραγμών συναλλαγής. Το Σχήμα 2.3 απεικονίζει μια αρχιτεκτονική υψηλού επιπέδου του στρώματος στο Hyperledger Fabric (HLF) και τα βασικά συστατικά του [11]:

- **Επικοινωνία:** το επίπεδο επικοινωνίας βασίζεται στο gRPC και τα βοηθητικά προγράμματα TLS με αμοιβαίο έλεγχο ταυτότητας, το οποίο επιτρέπει σε κάθε πλευρά της σύνδεσης να συνδέσει τα διαπιστευτήρια TLS με την ταυτότητα του απομακρυσμένου ομότιμου.

- **Έλεγχος ταυτότητας / ACL:** είναι υπεύθυνος για τον έλεγχο ταυτότητας απομακρυσμένων ομότιμων, την επικύρωση και την αποθήκευση των πιστοποιητικών ομότιμων, καθώς και την επιβολή του διαχωρισμού των πληροφοριών που εισάγονται από τα κανάλια.

- **Διάδοση:** προς τα εμπρός (ωθήσεις) και τραβά τα μηνύματα προς/από τους συμμετέχοντες σύμφωνα με τις πολιτικές δρομολόγησης.

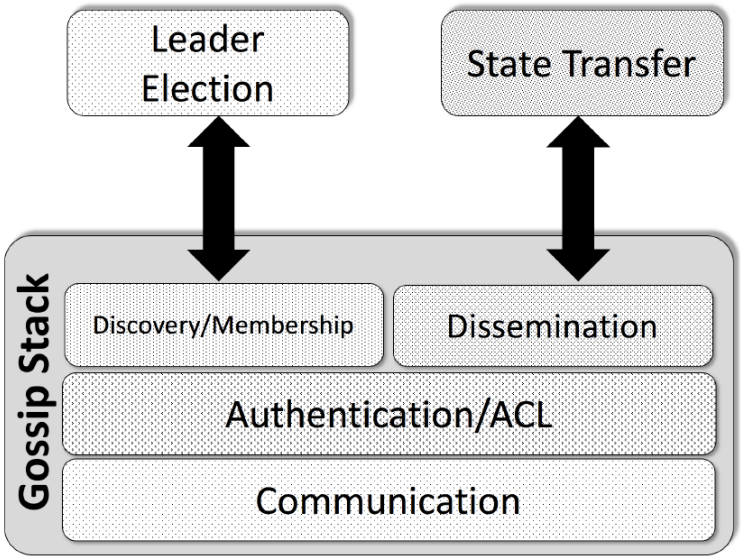
- **Ανακάλυψη / Σύνθεση:** διατηρείται μια ενημερωμένη άποψη της ιδιότητας μέλους σε απευθείας σύνδεση με τους ομότιμους χρήστες στο σύστημα.

- **Εκλογή Ηγέτη:** προκειμένου να μειωθεί το φορτίο της αποστολής των μπλοκ από την παραγγελία κόμβων στο δίκτυο, το πρωτόκολλο εκλέγει επίσης έναν ομότιμο ηγέτη που τραβά μπλοκ από την υπηρεσία ταξινόμησης για λογαριασμό τους και ξεκινά τη διανομή. Αυτός ο μηχανισμός είναι ανθεκτικός στις αποτυχίες των ήχων.

- **Μεταφορά Κατάστασης:** ένα σημείο σε μηχανισμό αναπαραγωγής φέρνει νέους κόμβους γρήγορα

2.4 Μέλη και Διασπορά Μεταδεδομένων

Στο Hyperledger Fabric οι ομότιμοι ανταλλάσσουν πληροφορίες σχετικά με τους διαθέσιμους ομότιμους χρήστες, αναπαράγοντας τα δικά τους "ζωντανά" μηνύματα, τη χρονική σήμανση, τα αναγνωριστικά ομότιμων υπολογιστών και το χρόνο ενσάρκωσης ομότιμων. Επιπλέον, το επίπεδο της συζήτησης είναι υπεύθυνο για τη διάδοση μεταδεδομένων που σχετίζονται με την κατάσταση του παγκόσμιου προτύπου και τη διαμόρφωση των πολιτικών chaincode και έγκρισης. Αυτό περιλαμβάνει πληροφορίες όπως το ύψος του παγκόσμιου προτύπου, τους κωδικούς αλυσίδων που είναι ενεργοί στο κανάλι και σε ποιους ομότιμους υπολογιστές είναι εγκατεστημένοι αυτοί οι κωδικοί αλυσίδων [53]. Στη συνέχεια, αυτά τα μεταδεδομένα χρησιμοποιούνται από την υπηρεσία εντοπισμού στον ομότιμο υπολογιστή, προκειμένου να γνωρίζουν ποιοι ομότιμοι υπολογιστές μπορούν να εκτελέσουν συγκεκριμένους κωδικούς αλυσίδων.



Σχήμα 2.3: Στοίβα επιπέδων συζήτησης. [53]

2.5 Πολιτική Επικυρώσεων

Η φάση εκτέλεσης του αλυσιδωτού κώδικα αποσυνδέεται από τις φάσεις παραγγελίας και επικύρωσης με τη χρήση κλιμακούμενης τεχνικής αναπαραγωγής "εκτέλεσης επαλήθευσης". Η συμφωνία για τα αποτελέσματα εκτέλεσης διέπεται από πολιτικές έγκρισης, δηλαδή κάθε συναλλαγή εκτελείται από ένα υποσύνολο ομότιμων που επιτρέπει την παράλληλη εκτέλεση [18].

Λόγω της φύσης της Fabric, κάθε κόμβος στο δίκτυο Hyperledger Fabric έχει μια ταυτότητα που πιστοποιεί την υπαγωγή του σε έναν από τους οργανισμούς που σχηματίζουν το δίκτυο blockchain. Κάθε ταυτότητα σχετίζεται με μια υπηρεσία παροχής μελών (MSP) - μια αρθρωτή αφαίρεση που ελέγχει τις ταυτότητες στο σύστημα.

Μια πολιτική έγκρισης στη Hyperledger Fabric (HLF) καθορίζει τους ομότιμους ή το πλήθος των ομότιμων που απαιτούνται για να παρέχουν βεβαίωση της ορθής εκτέλεσης ενός συγκεκριμένου chaincode. Οι πολιτικές έγκρισης αξιολογούνται πριν από την ολοκλήρωση αποκλεισμού, κατά τη φάση επικύρωσης της συναλλαγής. Ως μέρος της επικύρωσης της πολιτικής έγκρισης, η υπογραφή πάνω από τα αποτελέσματα εκτέλεσης του κωδικού αλυσίδας επαληθεύεται κάτω από το δημόσιο κλειδί της ταυτότητας του ομότιμου υποστηρικτή [03].

Η πολιτική έγκρισης είναι στην πραγματικότητα πιο εκφραστική από τις ταυτότητες - απαιτεί μια ταυτότητα από έναν οργανισμό και έναν συγκεκριμένο ρόλο, όπου οι ρόλοι μπορούν να είναι, για παράδειγμα: "Μέλος", "Ελεγκτής", κλπ.

Η πολιτική έγκρισης για το chaincode SampleCC ορίζεται ως εξής: AND (OrgA:Member; OR (orgb:μέλος;orgc:μέλος)) ενώ οι διαθέσιμοι ομότιμοι της υποστήριξης μπορούν να είναι:

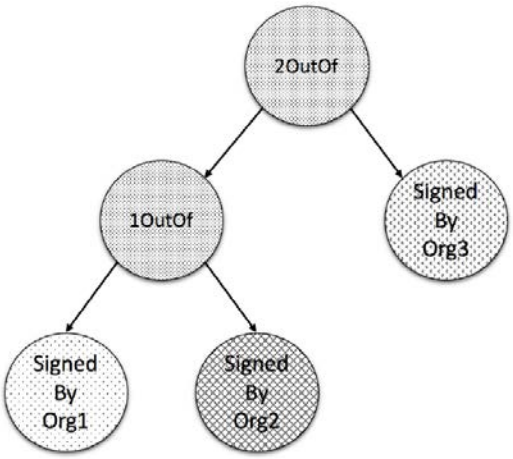
peer1.orga, peer2.orga, peer3.orga, peer1.orgb, peer2.orgb, peer1.orgC, peer2.orgC, peer3.orgCg (υποθέτοντας ότι όλοι αυτοί οι ομότιμοι πληρούν το ρόλο του "Μέλους"). Ως εκ τούτου, για να ικανοποιήσει τη δεδομένη πολιτική επικύρωσης κάποιος θα έπρεπε να ζητήσει την επικύρωση ενός OrgA και ενός είτε OrgB είτε OrgC [11].

Είναι σαφές ότι η πολιτική έγκρισης θα μπορούσε να ικανοποιηθεί με περισσότερους από έναν τρόπους. Μια πολιτική έγκρισης αποτελείται από μια σειρά από εντολείς: ένας εντολέας αποτελεί μια δήλωση πάνω από μια ταυτότητα.

Πιο επίσημα, για να αξιολογήσει την πολιτική έγκρισης για ένα δεδομένο σύνολο των ομότιμων ταυτοτήτων, το δέντρο έγκρισης διασχίζεται αναδρομικά για να βρεθεί ο πρώτος συνδυασμός των εντολέων που είναι ικανοποιημένοι με το δεδομένο σύνολο των ταυτοτήτων. Η υπηρεσία εντοπισμού υπολογίζει μια περιγραφή που επιτρέπει να υπολογιστούν όλοι οι πιθανοί συνδυασμοί ομότιμων, έτσι ώστε οι εγκρίσεις που συλλέγονται από κάθε συνδυασμό να ικανοποιούν την πολιτική έγκρισης [21].

2.6 Υπολογισμός των Συνόλων Εντολέων

Στην υπηρεσία ανακάλυψης, μια πολιτική έγκρισης αξιολογείται για να παραγάγει τους συνδυασμούς εντολέων έτσι ώστε κάθε συνδυασμός να ικανοποιεί την πολιτική επικύρωσης από μόνος του.



Σχήμα 2.4: Παρουσιάζεται το δέντρο έγκρισης που αντιστοιχεί στο παράδειγμα που παρουσιάζεται στο ότι το επίπεδο φύλλων σε κάθε τέτοιο υποδέντρο είναι ένας συνδυασμός εντολέων που ικανοποιεί την πολιτική. Αυτό γίνεται με τον υπολογισμό για κάθε εσωτερική κορυφή με ένα NoutOf ποσοτικοποιητή του n, όλες οι παραλλαγές των απογόνων του μεγέθους ν. Στη συνέχεια, το δέντρο έγκρισης διασχίζεται σε BFS και για κάθε εσωτερική κορυφή, το υποδέντρο διπλώνεται για να φιλοξενήσει όλες τις παραλλαγές, μέχρι να επισκεφτούν όλες τις κορυφές. [03]

Για κάθε τέτοιο κύριο σύνολο που ικανοποιεί την πολιτική έγκρισης μπορεί να υπάρχουν διαφορετικά είδη των εντολέων που απαιτούνται. Για παράδειγμα – μια πολιτική έγκρισης ενδέχεται να απαιτεί πολλές υπογραφές διαφορετικών ομότιμων υπολογιστών από τον ίδιο οργανισμό. Κάθε μια τέτοια χαρτογράφηση είναι ένας συνδυασμός εντολών και ονομάζεται διάταξη. Για παράδειγμα, μια ενιαία διάταξη θα ήθελε αυτό: f'OrgA. Μέλος»: 2, «OrgB: Ελεγκτής» να αναφέρει ότι δύο ομότιμοι «μελών» από την «OrgA» και ένας ομότιμος «ελεγκτής» από την «OrgB» θα ικανοποιούσαν την πολιτική έγκρισης [03].

2.7 Ανάγνωση Υπηρεσίας

Για την εκτέλεση του κωδικού αλυσίδας σε ομότιμους υπολογιστές, την υποβολή των συναλλαγών και για ενημέρωση σχετικά με την κατάσταση των συναλλαγών, οι εφαρμογές συνδέονται με ένα API που εκτίθεται από ένα SDK. Ωστόσο, το SDK χρειάζεται πολλές πληροφορίες για να επιτρέψει στις εφαρμογές να συνδεθούν με τους σχετικούς κόμβους δικτύου. Θα πρέπει να γνωρίζουν τα πιστοποιητικά εγγραφής και TLS CA των παραγγελιοδόχων και των ομότιμων στο κανάλι - καθώς και τις διευθύνσεις IP και τους αριθμούς θύρας. Επιπλέον, πρέπει να γνωρίζει τις σχετικές πολιτικές έγκρισης που συνδέονται με τον κωδικό αλυσίδας που έχουν εγκαταστήσει σε αυτές οι ομότιμοι. Αυτό είναι απαραίτητο, έτσι ώστε η εφαρμογή να γνωρίζει σε

ποιους ομότιμους να στείλουν προτάσεις chaincode. Σε προηγούμενες εκδόσεις του Hyperledger Fabric (πριν από το v1.2), οι πληροφορίες αυτές κωδικοποιήθηκαν στατικά. Ωστόσο, αυτή η υλοποίηση δεν ανταποκρίθηκε ικανοποιητικά στις αλλαγές δικτύου (όπως η προσθήκη ομότιμων υπολογιστών που έχουν εγκαταστήσει τον σχετικό κωδικό αλυσίδας ή ομότιμους υπολογιστές που είναι προσωρινά εκτός σύνδεσης).

Οι στατικές ρυθμίσεις παραμέτρων επίσης δεν επιτρέπουν στις εφαρμογές να αντιδρούν στις αλλαγές της ίδιας της πολιτικής έγκρισης (όπως μπορεί να συμβεί όταν ένας νέος οργανισμός συμμετέχει σε ένα κανάλι) [56]. Επιπλέον, η εφαρμογή-πελάτης δεν είχε τρόπο να γνωρίζει ποιοι ομότιμοι χρήστες έχουν ενημερωμένα στοιχεία και ποιοι όχι, επομένως μπορεί να υποβάλει προτάσεις σε ομότιμους υπολογιστές των οποίων τα δεδομένα παγκόσμιου προτύπου δεν είναι συγχρονισμένα με το υπόλοιπο δίκτυο, με αποτέλεσμα η συναλλαγή να ακυρωθεί κατά την ολοκλήρωση. Η υπηρεσία εντοπισμού βελτιώνει αυτήν τη διαδικασία, έχοντας τους ομότιμους να υπολογίζουν τις απαραίτητες πληροφορίες δυναμικά και να τις παρουσιάζουν στο SDK με αναλώσιμο τρόπο [16].

2.8 Λειτουργίες Ανακάλυψης Υπηρεσιών

Η εφαρμογή εκδίδει ένα ερώτημα ρύθμισης παραμέτρων στην υπηρεσία εντοπισμού και λαμβάνει όλες τις στατικές πληροφορίες που διαφορετικά θα χρειαζόταν για να επικοινωνήσει με τους υπόλοιπους κόμβους του δικτύου. Αυτές οι πληροφορίες μπορούν να ανανεωθούν σε οποιοδήποτε σημείο στέλνοντας ένα επόμενο ερώτημα στην υπηρεσία εντοπισμού ενός ομότιμου υπολογιστή.

Η υπηρεσία εκτελείται σε ομότιμους υπολογιστές – όχι στην εφαρμογή – και χρησιμοποιεί τις πληροφορίες μεταδεδομένων δικτύου που διατηρεί η gossip Sec. 3 για να διαμορφώσει τη λίστα των ομότιμων χρηστών που είναι συνδεδεμένοι. Λαμβάνει επίσης πληροφορίες, όπως σχετικές πολιτικές έγκρισης, από τη βάση δεδομένων κατάστασης του ομότιμου. Με τον εντοπισμό της υπηρεσίας, οι εφαρμογές δεν χρειάζεται πλέον να καθορίζουν από ποιους ομότιμους υπολογιστές χρειάζονται εγκρίσεις. Το SDK μπορεί απλά να στείλει ένα ερώτημα στην υπηρεσία εντοπισμού ζητώντας από τους ομότιμους υπολογιστές που απαιτούνται, δεδομένου ενός καναλιού και ενός αναγνωριστικού κωδικού αλυσίδας [21]. Η υπηρεσία εντοπισμού μπορεί να ανταποκριθεί στα ακόλουθα ερωτήματα:

- **Ερώτημα ρύθμισης παραμέτρων:** επιστρέφει τη ρύθμιση παραμέτρων που απαιτείται για την προετοιμασία των πιστοποιητικών CA όλων των οργανισμών στο κανάλι μαζί με τα τελικά σημεία παραγγελίας του καναλιού.

- **Ομότιμο ερώτημα ιδιότητας μέλους:** επιστρέφει τους ομότιμους υπολογιστές που έχουν ενταχθεί στο κανάλι. Πρόσθετα μετα-δεδομένα, όπως οι κωδικοί αλυσίδων που εγκαθίστανται, τα πιστοποιητικά των ομότιμων υπολογιστών και το μέγεθος του κάθε πακέτου πληροφοριών περιλαμβάνονται στις πληροφορίες.

- **Το ερώτημα έγκρισης:** επιστρέφει μια περιγραφή έγκρισης για δεδομένο chaincode. Ο περιγραφέας επιτρέπει την εύκολη επιλογή ορισμένων ομότιμων, έτσι ώστε εάν οι θεωρήσεις λαμβάνονται από το σύνολο, η πολιτική έγκρισης θα ικανοποιηθεί. Τα ίδια μετα-δεδομένα σε ομότιμους υπολογιστές που επιστρέφονται στο ερώτημα ιδιότητας μέλους, περιλαμβάνονται επίσης στα αποτελέσματα.

- **Τοπική peer ερώτημα ιδιότητας μέλους:** επιστρέφει το κανάλι, αγνοεί πληροφορίες που είναι γνωστές στον ομότιμο, δηλαδή - όλα τα peer γνωρίζει, ανεξάρτητα από τα κανάλια.

2.9 Chaincode στην Επίκληση και την Επικύρωση

Ένας κωδικός αλυσίδας μπορεί επίσης να επικαλεστεί έναν άλλο κωδικό αλυσίδας κατά την εκτέλεσή του. Σε ένα τέτοιο σενάριο, η συναλλαγή που προκύπτει μπορεί να επηρεάσει πολλούς χώρους ονομάτων της παγκόσμιας κατάστασης και όχι μόνο το χώρο ονομάτων του κωδικού αλυσίδας προορισμού στον οποίο έστειλε ο υπολογιστής-πελάτης την πρόταση συναλλαγής. Κατά την επικύρωση, μια τέτοια συναλλαγή ισχύει μόνο εάν οι καταχωρίσεις πληρούν τις πολιτικές έγκρισης όλων των κωδικών αλυσίδων που σημειώνονται στη συναλλαγή και όχι μόνο της πολιτικής έγκρισης του κωδικού-στόχου. Η υπηρεσία εντοπισμού υποστηρίζει αυτούς τους τύπους σεναρίων, υπολογίζοντας κύρια σύνολα όλων των κωδικών αλυσίδων στην αλυσίδα κλήσης ενός ερωτήματος έγκρισης και ενοποιώντας κύρια σύνολα που είναι ασυνάρτητα μεταξύ των διαφόρων κωδικών αλυσίδων στην αλυσίδα κλήσης του ερωτήματος, έτσι ώστε κάθε κύριο σύνολο να ικανοποιεί όλες τις πολιτικές έγκρισης [03].

2.10 Ιδιωτικές Συλλογές Δεδομένων και Ερωτήματα Έγκρισης

Η Hyperledger Fabric (HLF) διαθέτει επίσης ένα μηχανισμό για την ανταλλαγή δεδομένων μεταξύ ενός υποσυνόλου των μελών του καναλιού - που ονομάζεται "ιδιωτική συλλογή δεδομένων" (ή συλλογή, εν ολίγοις). Αυτό γίνεται με την αποθήκευση στα αποτελέσματα προσομοίωσης συναλλαγών, με τα hashes (χρησιμοποιώντας μια λειτουργία κρυπτογραφικού κατακερματισμού, όπως SHA256) και με τη διάδοση του κατακερματισμού προ-εικόνων μόνο μεταξύ των ομότιμων που είναι μέλη της συλλογής.

Αυτό προσθέτει ένα άλλο εμπόδιο στην επιλογή έγκρισης του υπολογιστή-πελάτη - ένας ομότιμος υπολογιστής που δεν αποτελεί μέρος μιας συλλογής, δεν μπορεί να προσομοιώσει συναλλαγές που χρησιμοποιούν κλειδιά που είναι γνωστά μόνο σε ομότιμους υπολογιστές που είναι μέλη της συλλογής. Επιπλέον, η εισαγωγή του υπολογιστή-πελάτη στον κωδικό αλυσίδας ενδέχεται να περιέχει ευαίσθητες πληροφορίες που θα πρέπει να αποκρύπτονται από ομότιμους υπολογιστές που δεν είναι μέλη της συλλογής [03]. Ως εκ τούτου, ο πελάτης πρέπει να στείλει προτάσεις σε ομότιμους που είναι μέλη της συλλογής και να αποφύγει την αποστολή σε εκείνους που δεν είναι. Η υπηρεσία εντοπισμού αντιμετωπίζει αυτήν την απαίτηση, έχοντας τα ερωτήματα έγκρισης του υπολογιστή-πελάτη να καθορίζουν συλλογές ανά κωδικό αλυσίδας και επιστρέφοντας στον υπολογιστή-πελάτη μια περιγραφή που περιέχει μόνο ομότιμους υπολογιστές που αποτελούν μέρος της συλλογής [11].

Η Hyperledger Fabric (HLF) ήταν η πρώτη πλατφόρμα blockchain που χρησιμοποίησε το μοτίβο για την εκτέλεση- παραγγελία- επικύρωση. Αυτή η καινοτομία αποσυνδέει την εκτέλεση και την έγκριση μιας συναλλαγής από την πλήρη παραγγελία και τη δέσμευσή της στο παγκόσμιο πρότυπο και ανοίγει την πόρτα για την παράλληλη εκτέλεση ανεξάρτητων συναλλαγών. Αυτές οι συναλλαγές φιλτράρονται είτε από τον υπολογιστή-πελάτη που συλλέγει εγκρίσεις είτε από τη φάση επικύρωσης που επιβάλλει τις έγκυρες θεωρήσεις [33].

Ωστόσο, τα πλεονεκτήματα αυτά προέρχονται από το κόστος της πρόσθετης πολυπλοκότητας. Η ροή συναλλαγών στο Hyperledger Fabric είναι πιο περίπλοκη σε σύγκριση με το Bitcoin ή το Ethereum, για παράδειγμα, και το βάρος του συντονισμού αυτής της ροής πέφτει στον πελάτη. Ο υπολογιστής-πελάτης πρέπει να επικοινωνεί με πολλές οντότητες και να γνωρίζει: τη θέση του κωδικού αλυσίδας, την πολιτική έγκρισης, τους ομότιμους υπολογιστές που υποστηρίζουν και την

υπηρεσία παραγγελίας. Όλες αυτές οι οντότητες υπόκεινται σε αλλαγές κατά τη διάρκεια του κύκλου ζωής της πλατφόρμας: οι ομότιμοι και οι οργανισμοί μπορούν να έρχονται και να φεύγουν, ο κωδικός αλυσίδας μπορεί να αναβαθμιστεί και οι πολιτικές έγκρισης μπορούν να ενημερωθούν [21]

Το στοιχείο Service Discovery βοηθά τον κώδικα εφαρμογής του υπολογιστή-πελάτη να αντιμετωπίσει την πολυπλοκότητα και τη δυναμική φύση της πλατφόρμας. Επιτρέποντας στον πελάτη να προσαρμόζεται εύκολα και αυτόματα στις αλλαγές στην πλατφόρμα, η αξιοπιστία και η διαθεσιμότητα της εφαρμογής blockchain αυξάνεται σημαντικά. Το στοιχείο Service Discovery απλοποιεί επίσης την εργασία του προγραμματιστή εφαρμογών, καθιστώντας το έργο της εγγραφής ισχυρού κώδικα εφαρμογής πολύ πιο εύκολη.

Κεφάλαιο 3
Βιβλιογραφική Ανασκόπηση Ευπαθειών και Επιθέσεων στο Hyperledger Fabric

Σύμφωνα με το Forbes, περισσότερα από 24 από δισεκατομμύρια δολάρια επενδύονται στο Hyperledger Fabric. Η Κεντρική Τράπεζα του Ιράν έχει αναλάβει ένα φιλόδοξο έργο για την ανανέωση του τραπεζικού της συστήματος και τη μετατροπή της σε ψηφιακή οικονομία χρησιμοποιώντας το Fabric. Υπάρχουν πολλά άλλα παραδείγματα, τα οποία απεικονίζουν το βάθος στο οποίο το Fabric έχει διεισδύσει σήμερα στην τεχνολογία. Και έτσι είναι ολοφάνερο ότι η υποδομή ασφαλείας του Fabric έχει τεράστιες συνέπειες που δεν πρέπει να υποτιμηθούν [08].

Σε αυτό το κεφάλαιο αναλύονται τα σενάρια επίθεσης για το Fabric, αποτελώντας μια συστηματική μελέτη των υποθετικών επιθέσεων στα δίκτυα Fabric. Αυτά τα μοντέλα επίθεσης λαμβάνουν υπόψη την πιθανότητα συμβιβασμού των μελών του δικτύου και περιγράφουν τον βαθμό στον οποίο μια κακόβουλη υπηρεσία μπορεί να διεισδύσει και να βλάψει το δίκτυο.

Το Fabric βασίζεται σε μερικά αξιόπιστα μέρη και συγκεντρωτικές υπηρεσίες για την παροχή μιας γενικευμένης πλατφόρμας για δεδομένα σε μορφή μπλοκ συστοιχιών. Ωστόσο, αυτά μπορούν να αξιοποιηθούν κακόβουλα και μπορεί να οδηγήσουν σε επιθέσεις που δεν θα ήταν εφαρμόσιμες σε ένα δίκτυο που δεν είναι ενημερωμένο να αποκλείει τέτοιου είδους επιθέσεις. Η αρθρωτή αρχιτεκτονική του Hyperledger προωθεί τη χρήση πρωτοκόλλων αυτοεξυπηρέτησης, ωστόσο, τα συστήματα που είναι ενσωματωμένα στα πρωτόκολλα αυτά είναι ασφαλή όσο είναι τα ίδια τα πρωτόκολλα. Ωστόσο, αυτή η αρθρωτή αρχιτεκτονική παρουσιάζει επίσης ένα πρόβλημα για τον εισβολέα, καθώς διαφορετικοί συνδυασμοί πρωτοκόλλων πρέπει να αξιοποιηθούν με διαφορετικούς τρόπους. Το Fabric είναι η πιο δημοφιλής πλατφόρμα αλυσιδωτού κώδικα σήμερα. Με μεγάλες επενδύσεις ύψους άνω των 100 εκατομμυρίων δολαρίων, από τις μεγάλες εταιρείες τεχνολογίας όπως η Intel, η Cisco, η IBM κ.λπ., καθώς και σημαντικοί χρηματοπιστωτικοί οργανισμοί όπως η JP Morgan, η Deutsche Bank κ.λπ., είναι σαφές ότι η τεχνολογία αυτή συγκεντρώνει την προσοχή [17, 47]. Στη συνέχεια του κεφαλαίου, κατηγοριοποιούνται και περιγράφονται διάφορες επιθέσεις στο Fabric, όπως παρουσιάζονται στη διεθνή βιβλιογραφία, ενώ στο Παράρτημα της εργασίας παρατίθεται συγκριτικός πίνακας αυτών, ο οποίος σχολιάζεται στα συμπεράσματα της εργασίας.

3.1 Συμβιβαζόμενος MSP

Αυτή η περίπτωση ασχολείται με το σενάριο όταν ο "Πάροχος Υπηρεσιών Μέλους (Membership Service Provider – MSP)" είναι κακόβουλος / συμβιβάζεται λόγω παραβίασης της ασφάλειας. Δεδομένου ότι το MSP είναι η μόνη αρχή που είναι υπεύθυνη για τη διαχείριση της ταυτότητας, ένα κακόβουλο MSP μπορεί να προκαλέσει καταστροφικές βλάβες στο δίκτυο [52].

3.1.1 Επίθεση Sybil

Σε μια επίθεση Sybil, ο εισβολέας ανατρέπει το σύστημα φήμης ενός δικτύου, δημιουργώντας ένα μεγάλο αριθμό ψευδώνυμων ταυτοτήτων και τις χρησιμοποιεί για να αποκτήσει δυσανάλογα μεγάλη επιρροή. Καθώς το MSP κινδυνεύει, ένας εισβολέας μπορεί να πλημμυρίσει το δίκτυο με ψεύτικες ταυτότητες και να χρησιμοποιήσει την πλειοψηφία προς όφελός του [17]. Το Org1 είναι μια επιχείρηση με μια μικρή υποδομή δικτύου που έχει αναπτύξει το Fabric για να παρακολουθεί τους λογαριασμούς του. Εφαρμόζει πολιτική MAJORITY για την έγκριση συναλλαγών. Ας υποτεθεί ότι ένας επιτιθέμενος A είναι σε θέση να παραβιάσει την ασφάλεια και να αποκτήσει τον έλεγχο του MSP-admin M. Στη συνέχεια διατηρεί την αναπαραγωγή πολλαπλών κόμβων και τους συνδέει

στο δίκτυο. Χρησιμοποιεί το Μ για τη δημιουργία αξιόπιστων πιστοποιητικών για αυτούς τους κόμβους. Συνεχίζει να προσθέτει κόμβους στο δίκτυο έως ότου έχει την πλειοψηφία και είναι έπειτα σε θέση να δώσει την έγκριση για παράνομες συναλλαγές [35].

3.1.2 Μη Έγκυρη Επίθεση Ταυτότητας

Το MSP ενός οργανισμού αναγνωρίζει την Αρχή Πιστοποίησης που εκδίδει αξιόπιστα πιστοποιητικά X.509 στους κόμβους μελών. Τα πιστοποιητικά περιέχουν ένα πεδίο "Οργανικής Μονάδας (Organizational Unit - OU)" που έχει εκχωρηθεί από το MSP. Σε περίπτωση που διαφορετικοί οργανισμοί χρησιμοποιούν την ίδια αλυσίδα εμπιστοσύνης, το πεδίο OU χρησιμοποιείται για τον προσδιορισμό των μελών ενός οργανισμού. Μια άλλη χρήση του πεδίου OU είναι η παροχή πρόσβασης καναλιού [08]. Ας υποτεθεί ότι το δίκτυο Org1 έχει 2 κανάλια C1 και C2. Και το Α θέλει πρόσβαση στο κανάλι στο C2. Το Α έως το Μ δημιουργεί εύκολα ένα πιστοποιητικό με το OU που έχει οριστεί σε C2 και τον εκχωρεί σε έναν κακόβουλο κόμβο. Το Α μέσω αυτού του κόμβου είναι σε θέση να βλέπει το ledger και να δηλώνει στο C2, παραβιάζοντας έτσι την εγγύηση απορρήτου ενός καναλιού. Κάποιες άλλες πιθανές επιθέσεις είναι:

- Δημιουργία δόλιων πιστοποιητικών για γνήσιους ομότιμους / ανταγωνιστικούς οργανισμούς

- Ακύρωση των υφιστάμενων αναγνωριστικών των γνήσιων ομότιμων/ ανταγωνιστικών οργανισμών

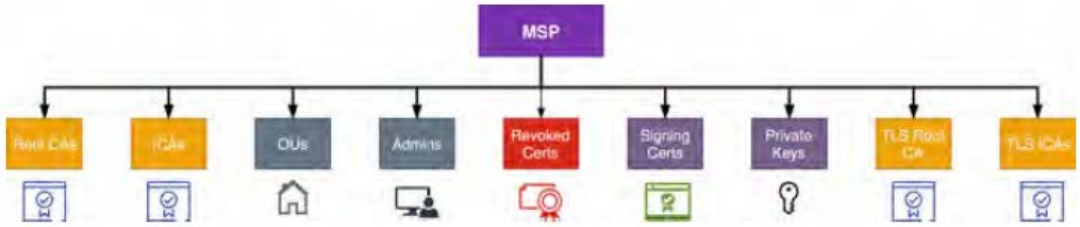
3.1.3 Επιθέσεις Boycott

Ας υποτεθεί ότι δύο οργανώσεις Org1 και Org2 ήταν κάτω από το ίδιο MSP. Εάν ο επιτιθέμενος Α αποκτήσει τον έλεγχο του MSP-admin Μ, τότε θα μπορούσε να τροποποιήσει τις υπάρχουσες πολιτικές και να αρνηθεί να παράσχει πιστοποιητικά στα μέλη του Org2, οπότε δεν θα τους επιτρέψει να συνδεθούν στο δίκτυο [37].

3.1.4 Επιθέσεις Μαύρης Λίστας

Σε περίπτωση προεπιλεγμένης υλοποίησης του MSP, καθορίζονται ορισμένες παράμετροι που επιτρέπουν την επικύρωση ταυτότητας. Μία από αυτές τις παραμέτρους είναι μια σειρά "Λιστών

Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists – CRLs)", η καθεμία από τις οποίες αντιστοιχεί σε μία από τις καταχωρημένες Αρχές Πιστοποίησης MSP. Αυτά τα CRLs αναγνωρίζουν τους κόμβους των οποίων τα δικαιώματα στο δίκτυο έχουν ανακληθεί (συμπεριλαμβανομένων και άλλων μελών του MSP). Αν υποτεθεί ότι το MSP του Org1 περιλαμβάνει δύο ενδιάμεσες CAs C1 και C2. Ο επιτιθέμενος A αποκτά πρόσβαση στο MSP και προσθέτει το πιστοποιητικό C2 στο CRL. Αυτό αναγκάζει την αρχή του C2 να ανακληθεί [48].



Σχήμα 3.1:. Τοπική MSP δομή. [22]

3.2 Υπηρεσία Κακόβουλης Παραγγελίας

Η υπηρεσία παραγγελίας ενός δικτύου Fabric είναι αποκλειστικά υπεύθυνη για τη συναίνεση σχετικά με τα παραγόμενα μπλοκ στον αλυσιδωτό κώδικα. Σε αντίθεση με τα Bitcoin και Ethereum τα οποία βασίζονται σε πιθανολογικά πρωτόκολλα συναίνεσης, το πρωτόκολλο συναίνεσης του Fabric είναι καθοριστικό. Η άμεση συνέπεια της χρήσης τέτοιων πρωτοκόλλων είναι ότι τα μπλοκ που δημιουργούνται από το λειτουργικό σύστημα είναι τα τελικά και τα σωστά [46].

3.2.1 Επιθέσεις Σαμποτάζ

Οι "Κόμβοι Υπηρεσιών Παραγγελίας (Ordering Service Nodes – OSN)" είναι υπεύθυνοι για τη συγκέντρωση συναλλαγών και την ενοποίησή τους σε μπλοκ. Ας υποτεθεί ότι το κακόβουλο λογισμικό "O", θέλει να προκαλέσει ζημιά στον οργανισμό Orga. Υποθετικά οι Pa1 είναι οι κόμβοι που ανήκουν στην Orga. Κατά την ενοποίηση του μπλοκ, το "O" δεν περιλαμβάνει συναλλαγές από Pa1. Αυτό θα μπορούσε να καταστήσει ανενεργή την Orga [56].

3.2.2 Διεθνείς Fork Attacks

Η υπηρεσία παραγγελίας δημιουργεί ένα μπλοκ ενοποιώντας τις συναλλαγές που θεωρούνται τελικές και σωστές. Αλλά μια κακόβουλη υπηρεσία παραγγελίας "Ο" θα μπορούσε να στείλει διαφορετικές εκδόσεις των μπλοκ ως απάντηση στις αιτήσεις εκπομπής και παράδοσης ενεργοποιώντας έτσι το δίκτυο. Ας υποτεθεί ότι το "Ο" είναι συνδεδεμένο με δύο οδηγούς P1 και P2. Τα P1 και P2 ζητούν αμφότερα τα μπλοκ από το "Ο". Το "Ο" δημιουργεί δύο μπλοκ B1 και B2 και τα παραδίδει στα P1 και P2 αντίστοιχα. Κατά τη διάρκεια του Gossip, τα μέλη που έχουν B1 θα απορρίψουν τα άλλα μπλοκ και αντίστροφα [17].

3.2.3 Επιθέσεις Μεγέθους Block

Η Υπηρεσία Παραγγελίας είναι επίσης υπεύθυνη για τη ρύθμιση των Καναλιών Επιβεβαίωσης. Οι επιβεβαιώσεις αποθηκεύονται στο ημερολόγιο σε ένα config-block. Κάθε φορά που αλλάζει η επιβεβαίωση, πρέπει να δημοσιευθεί νέο config-block στο ledger. Το τελευταίο μπλοκ διαμόρφωσης είναι τραβηγμένο και διατηρείται στη μνήμη για γρήγορες και αποδοτικές λειτουργίες. Αρχικά υποθέσαμε ότι το "Ο" αποτελεί ένα κακόβουλο λογισμικό. Το "Ο" αλλάζει την τιμή του μεγέθους παρτίδας σε μια εξαιρετικά μικρή / εξαιρετικά μεγάλη τιμή. Το μέγεθος της παρτίδας ορίζει τον αριθμό των συναλλαγών που πρέπει να συμπεριληφθούν πριν από την κοπή του μπλοκ. Εάν η τιμή είναι πολύ μεγάλη, τότε το μπλοκ δεν θα δημοσιευθεί ποτέ καθώς ο αριθμός των απαιτούμενων συναλλαγών είναι πολύ υψηλός. Εάν είναι πολύ χαμηλό, τότε θα υπάρξει ένας μη πρακτικός αριθμός μπλοκ στον αλυσιδωτό κώδικα. Και οι δύο επιθέσεις θα μειώσουν την αποδοτικότητα του δικτύου. Επίσης, δεδομένου ότι το "Ο" είναι λειτουργικό σύστημα – admin η υπογραφή του αρκεί για να γίνει αποδεκτή η συναλλαγή [22].

3.2.4 Επίθεση Batch Time

Μια παρόμοια επίθεση μπορεί να τοποθετηθεί στο Batch Timeout, το οποίο είναι ο χρόνος μετά την άφιξη της πρώτης συναλλαγής για πρόσθετες συναλλαγές πριν κοπεί ένα μπλοκ. Η μείωση αυτής της τιμής θα βελτιώσει την καθυστέρηση, αλλά η μείωση της υπερβολικά μεγάλης ποσότητας μπορεί να μειώσει την απόδοση, μη επιτρέποντας στο μπλοκ να γεμίσει με τη μέγιστη χωρητικότητά του. Το κακόβουλο λογισμικό "Ο" μπορεί να μειώσει το χρονικό όριο για να βλάψει τη διακίνηση του δικτύου [03].

3.2.5 Επίθεση Withholding Block

Αυτοί που δίνουν τις εντολές θα μπορούσαν να συγκρατήσουν τα μπλοκ και να κατευθύνουν την απελευθέρωση ορισμένων μπλοκ που θα τους ευνοούσαν. Αυτό θα φαινόταν σαν απόλυτα φυσιολογική συμπεριφορά και το υπόλοιπο δίκτυο θα αγνοούσε την πρόθεση του κόμβου [08].

3.2.6 Επίθεση Αναδιάταξης Συναλλαγών (Transaction Reordering Attack)

Το λειτουργικό σύστημα είναι υπεύθυνο για την παραγγελία των συναλλαγών σε μπλοκ. Η σειρά με την οποία συμπεριλαμβάνονται οι συναλλαγές θεωρείται οριστική και επομένως δεν επαληθεύεται και πάλι. Ας υποτεθεί ότι το δίκτυο έπαιζε ένα παιχνίδι, όπου ένας κακός γραμμικός αλυσιδωτός κώδικας υποσχέθηκε να πληρώσει τον κόμβο που θα λύσει πρώτο ένα παζλ. Άμεσα το P1 λύνει το παζλ και μετά από κάποιο χρονικό διάστημα το κάνει και το P2. Και οι δύο υποβάλλουν τις συναλλαγές τους σε αυτόν που κάνει την παραγγελία μέσω του "O", ο διαχειριστής όμως προτιμά το P2 και ως εκ τούτου τοποθετεί τις συναλλαγές του πριν από την συναλλαγή της P1. Το "O" τότε μεταδίδει το μπλοκ για επικύρωση. Οι υπεύθυνοι δέχονται το P2 ως νικητή και επικυρώνουν τη συναλλαγή του. Η συναλλαγή της P1 χαρακτηρίζεται ως διπλή δαπάνη και μη έγκυρη [48].

3.3 Κακόβουλοι Επικυρωμένοι Κόμβοι

Είναι έργο των επικυρωμένων κόμβων να επικυρώνουν τελικά τις συναλλαγές σύμφωνα με τον αλυσιδωτό κώδικα του συστήματος επικύρωσης και στη συνέχεια, μετά από μερικές επιπλέον δοκιμές, να ενημερώσουν το ledger και την κατάσταση [52].

3.3.1 Επίθεση Διπλών Εξόδων (Double Spend Attack)

Οι Κόμβοι Επαλήθευσης ελέγχουν τους αριθμούς έκδοσης των πεδίων readset και τα τρέχοντα πεδία για ισότητα. Εάν είναι διαφορετικά τότε, ισοδυναμεί με διπλό κόστος. Οι κακόβουλοι επικυρωμένοι κόμβοι θα μπορούσαν να επιτρέψουν τη διπλή δαπάνη και να την προσαρτήσουν στο ledger, καταστρέφοντας έτσι την ακεραιότητά τους [52].

3.3.2 Επίθεση DDos

Η "Κατανεμημένη Άρνηση Παροχής Υπηρεσίας (Distributed Denial of Service - DDos)" είναι μια επίθεση στην οποία ο εισβολέας προσπαθεί να καταστήσει μια κοινή υπηρεσία μη διαθέσιμη

στους χρήστες κάνοντας κακόβουλα ερωτήματα από πολλές μηχανές, έτσι ώστε ο διακομιστής (ο οποίος φιλοξενεί την υπηρεσία) να είναι υπερφορτωμένος από τον αριθμό των αιτημάτων και να μην μπορεί να τα επεξεργαστεί. Τα δίκτυα Blockchain είναι εγγενώς DDos ανεκτικά. Με τη συγκέντρωση της Υπηρεσίας Παραγγελίας, το Fabric γίνεται κάπως επιρρεπές σε επιθέσεις DDos. Για να μετριάσει αυτό το ζήτημα σε κάποιο βαθμό, το λειτουργικό σύστημα χρησιμοποιεί πρωτόκολλα CFT όπως Kafka, Raft κλπ [03].

3.4 Εξωτερικές Επιθέσεις

Ένα από τα μεγαλύτερα πλεονεκτήματα του αλυσιδωτού κώδικα ήταν ότι ήταν καθαρά αποκεντρωμένο. Εντούτοις, στο Fabric, η εισαγωγή ενός ορισμένου ποσού συγκέντρωσης ήταν απαραίτητη για την παροχή μιας γενικευμένης πλατφόρμας. Αυτή η επανέγχυση σημείων ελέγχου, και επομένως σημείων ευπάθειας, στον αλυσιδωτό κώδικα για παράδειγμα, μέσω της "χορήγησης άδειας" ακυρώνει τα κύρια οφέλη του, τα οποία προέρχονται από την αφαίρεση σημείων ευπάθειας [56]. Εστιάζοντας στις επιθέσεις, οι διαχειριστές των MSP, οι OSNs είναι όλες οι κεντρικές υπηρεσίες σε μια αποκεντρωμένη πλατφόρμα και ως εκ τούτου είναι ευάλωτες σε:

- Επιθέσεις DoS
- Crash Faults
- Επιθέσεις Man in the Middle

3.4.1 Συμπαιγνία (Collusion)

Εάν κάποιοι από τους συμμετέχοντες φορείς στο δίκτυο συνεργάζονται, θα μπορούσαν αποτελεσματικά να ξεκινήσουν μια εναλλακτική επίθεση ιστορικού που θα τους επέτρεπε να ξαναγράψουν το ledger προς όφελός τους. Δεδομένου ότι σε ένα αλυσιδωτό κώδικα με άδεια, δεν επιτρέπεται σε όλους να συμμετάσχουν και ο αριθμός των συμμετεχόντων κόμβων είναι πολύ μικρός σε σύγκριση με τους αδέσμευτους αλυσιδωτούς κώδικες, η συμφωνία είναι ευκολότερη και ένα πολύ πιο ρεαλιστικό σενάριο από ό, τι στο Bitcoin [46].

3.4.2 Επιθέσεις Διεπαφής

Κάθε DApp θα έχει μια πλευρική διεπαφή πελάτη για να λαμβάνει δεδομένα εισόδου και για να επιτρέπει στους πελάτες να εκκινούν συναλλαγές στο Fabric. Οι εφαρμογές Web που είναι συμβατές με πλατφόρμες χρησιμοποιούνται γενικά για το σκοπό αυτό. Λαμβάνοντας υπόψη ότι οι αλυσιδωτοί κώδικες είναι πλατφόρμες για να δημιουργηθεί εμπιστοσύνη μεταξύ των αμοιβαία ομότιμων, οι συναλλαγές περιλαμβάνουν γενικά εμπιστευτικά δεδομένα που μεταβιβάζονται ως εισροές. Οι μη επιμελώς κατασκευασμένες διεπαφές μπορούν να διαρρεύσουν δεδομένα [35]. Στην περίπτωση εφαρμογών δικτύου, ας εξεταστεί ένα παράδειγμα:

Η SSL επίθεση είναι μια επίθεση MITM στην οποία ο εισβολέας εξαπατά τον πελάτη στην επικοινωνία μέσω ενός μη ασφαλούς πρωτοκόλλου HTTP, παρεμποδίζοντας έτσι όλα τα δεδομένα ως απλό κείμενο. Η επίθεση λειτουργεί ως εξής:

- Ένας εισβολέας A παρακολουθεί την κίνηση μεταξύ του πελάτη C και του σέρβερ S.

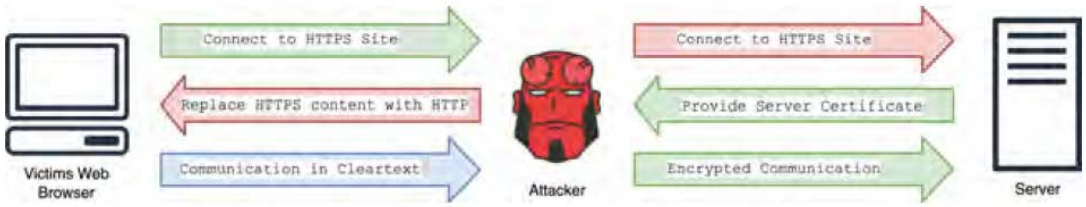
- Ο C θέλει να συνδεθεί στον τραπεζικό του λογαριασμό, ο οποίος φιλοξενείται στον S. Γι 'αυτό στέλνει ένα αίτημα HTTPS (κρυπτογραφημένο) στο S ζητώντας το πιστοποιητικό και προμηθεύει το δικό του πιστοποιητικό.

- Ο A παρακολουθεί αυτό το αίτημα και αντικαθιστά το πιστοποιητικό του C με το δικό του.

- Ο A ανιχνεύει την απόκριση από το S και μεταδίδει το πιστοποιητικό στο C αλλά κάνει μια μικρή αλλαγή. Αντικαθιστά το περιεχόμενο HTTPS με σηματοδότηση περιεχομένου HTTP στο C, ώστε να επικοινωνεί μόνο μέσω HTTP.

- Έτσι το C ανακοινώνει τώρα τις πληροφορίες σύνδεσης με το A στο cleartext. Κατά τη λήψη των πακέτων, το A τους ανοίγει και επιθεωρεί το περιεχόμενό τους, μετά από το οποίο κρυπτογραφεί και τα διαβιβάζει στο S.

- Η απόκριση αποκρυπτογραφείται και παρέχεται στον C



Σχήμα 3.2: Επίθεση SSL. [22]

3.4.3 Κακόβουλοι Clients

Οι κόμβοι Client υποβάλλουν εγκριθείσες συναλλαγές στο λειτουργικό σύστημα για τη δημιουργία μπλοκ. Το κακόβουλο λογισμικό "Ο" από προεπιλογή δεν ελέγχει διαδοχικά τις συναλλαγές σε σχέση με την πολιτική επικύρωσης αυτού του αλυσιδωτού κώδικα. Ένας κακόβουλος πελάτης C θα μπορούσε να χρησιμοποιήσει αυτό το γεγονός προς όφελός του. Ο C εκκινεί την επίθεση συνεχίζοντας να στέλνει μια σταθερή ροή από μη εκκρεμείς συναλλαγές στο "Ο". Το κακόβουλο λογισμικό "Ο" λαμβάνει τις συναλλαγές και εκτελεί ελέγχους επιπέδου πρόσβασης καναλιού. Δεδομένου ότι ο C έχει πρόσβαση εγγραφής στο ημερολόγιο, το "Ο" πακετάρει τις άκυρες συναλλαγές σε μπλοκ και τις στέλνει στους κόμβους επικύρωσης. Παρόλο που οι επικυρωμένοι κόμβοι επισημαίνουν τις συναλλαγές ως άκυρες, εξακολουθούν να περιλαμβάνονται στον αλυσιδωτό κώδικα. Αυτές μολύνουν τον αλυσιδωτό κώδικα και μπορεί να αυξήσουν το μέγεθος του κατά ένα μεγάλο ποσό [17].

3.5 Επιθέσεις Βάσει Πρωτοκόλλου

Ένα από τα μοναδικά χαρακτηριστικά του Hyperledger Fabric είναι η δυνατότητα σύνδεσης και αναπαραγωγής πρωτοκόλλων συναίνεσης, ανάλογα με την εφαρμογή. Κάθε πρωτόκολλο έχει τα δικά του πλεονεκτήματα και ελαττώματα.

3.5.1 Πρωτόκολλα CFT , BFT και PoW

Τα πρωτόκολλα CFT (Crash Fault Tolerant) είναι εξαιρετικά αποτελεσματικά πρωτόκολλα για τη δημιουργία συναίνεσης μεταξύ των κόμβων παραγγελίας. Είναι ανεκτικά σε σύγκρουση, δηλαδή εάν ο κόμβος του ηγέτη καταρρεύσει, το σύστημα μπορεί να ανακάμψει και να λειτουργήσει εξίσου αποτελεσματικά χωρίς απώλεια δεδομένων. Το Fabric προσφέρει πρωτόκολλα CFT όπως Kafka (με βάση το Zookeeper), Raft, κλπ. ως πρωτόκολλα συναίνεσης για το λειτουργικό σύστημα.

Ωστόσο, τα πρωτόκολλα CFT (που αναφέρονται παραπάνω) είναι ευάλωτα στους Βυζαντινούς κόμβους. Ακόμη και ένας και μόνο κακόβουλος κόμβος μπορεί να αποτρέψει αποτελεσματικά το δίκτυο από την επίτευξη συναίνεσης [52].

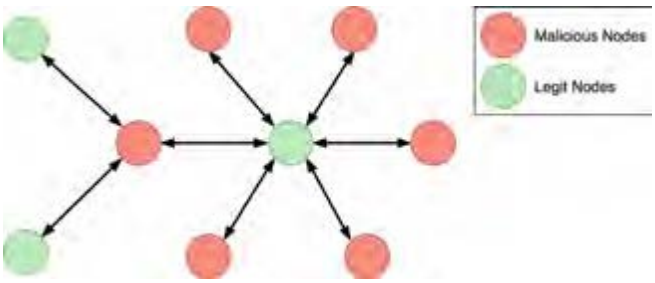
Από την άλλη πλευρά, τα πρωτόκολλα BFT (Tolerant of Byzantine Fault) μπορούν να χειριστούν τους Βυζαντινούς κόμβους σε κάποιο βαθμό (γενικά 33%). Αυτά τα πρωτόκολλα απαιτούνται όταν τα μέλη του δικτύου είναι αναξιόπιστα. Ωστόσο, αυτά τα πρωτόκολλα δεν βαθμονομούνται πολύ καλά και καθώς ο αριθμός των κόμβων αυξάνεται, η απόδοση μειώνεται δραματικά. Είναι ενεργειακά αποδοτικές, αποδίδουν καλά όταν ο αριθμός των πελατών είναι μεγάλος και ικανοποιούν το αμετάκλητο της συναίνεσης. Το PoW (Proof of Work) είναι το πρωτόκολλο συναίνεσης που χρησιμοποιείται από τα δίκτυα Bitcoin και Ethereum. Αυτό το πρωτόκολλο είναι εξαιρετικά επεκτάσιμο με χιλιάδες ανταγωνιστές και είναι αποκεντρωμένο. Τα μειονεκτήματα της PoW είναι ότι δεν εγγυάται το αμετάκλητο της τελικής συναίνεσης, έχει πολύ μεγάλη κατανάλωση ενέργειας και έχει πολύ χαμηλή απόδοση [22].

3.5.2 Πρωτόκολλο Gossip

Το πρωτόκολλο Gossip μπαίνει στο πλάνο όταν ο διαχειριστής παραδώσει τα μπλοκ στους ομότιμους. Αντί να μεταδίδει το μπλοκ σε αρκετούς ομότιμους, το λειτουργικό σύστημα στέλνει τα νέα μπλοκ μόνο στους "ομότιμους" του οργανισμού. Ο ομότιμος ηγέτης στη συνέχεια επεκτείνει το μπλοκ σε άλλους χρησιμοποιώντας Gossip. Αυτό το σύστημα είναι ευάλωτο σε επίθεση Eclipse
.

3.5.3 Επίθεση Eclipse

Οι επιθέσεις Eclipse επικεντρώνονται στην επίθεση ενός μεμονωμένου κόμβου στο δίκτυο. Ο σκοπός αυτής της επίθεσης είναι να ελέγξει όλες τις εξερχόμενες συνδέσεις του στόχου για να τον απομονώσει. Οι νέοι κόμβοι ή οι αποσυνδεδεμένοι κόμβοι αποκτούν ένα ενημερωμένο αντίγραφο του ledger χρησιμοποιώντας μια λειτουργία του πρωτοκόλλου Gossip που ονομάζεται pull. Εάν όλοι οι συνδεδεμένοι κόμβοι του στόχου είναι κακόβουλοι, τότε μπορούν θεωρητικά να παρασύρουν τον στόχο δίνοντάς του μια κατασκευασμένη έκδοση του αλυσιδωτός κώδικας [03].



Σχήμα 3.3: Επίθεση Eclipse. [22]

3.6 Ευπάθειες Κώδικα Αλυσίδας

Το Fabric χτίστηκε με το όραμα του να μην περιορίζεται σε μια συγκεκριμένη γλώσσα πλατφόρμας, όπως το Script του Bitcoin ή η Solidity του Ethereum, αλλά να μπορεί να αναπτύξει έξυπνες συμβάσεις γραμμένες σε γλώσσες γενικής χρήσης. Ως αποτέλεσμα, οι συμβάσεις Fabric που ονομάζονται αλυσωτοί κώδικες μπορούν να γραφτούν σε γλώσσες όπως Go, NodeJS κλπ. Με τέτοιες γλώσσες που μπορούν να προκαλέσουν παρενέργειες στο σύστημα, η ακατάλληλη κατανομή του δικτύου και η χαλαρή πρόσβαση-έλεγχος μπορούν να οδηγήσουν σε επιθέσεις [22]. Πιθανές ευπάθειες είναι:

- Απεριόριστα κοντέινερ αλυσίδας
- Οι μη ντετερμινιστικοί αλυσιδωτοί κώδικες μπορούν να προκαλέσουν την αποτυχία της συναίνεσης
- Ακύρωση του προβλήματος
- Η χαμηλού επιπέδου πρόσβαση θα μπορούσε να χρησιμοποιηθεί για να καταστρέψει τη στοίβα
- Έλλειψη επικύρωσης εισόδου

Οι επικλήσεις αλυσιδωτού κώδικα απαιτούνται γενικά από τους πελάτες μέσω διαδικτυακών διεπαφών ή του front-end. Ωστόσο, με την εκτέλεση εντολών απευθείας στο Fabric, ο εισβολέας μπορεί να παρακάμψει τα στοιχεία ελέγχου εξουσιοδότησης που εφαρμόζονται στη διεπαφή της εφαρμογής. Αυτές οι επιθέσεις είναι πιθανές επειδή οι αλυσιδωτοί κώδικες δεν έχουν ενσωματωμένους ελέγχους πρόσβασης. Η εξουσιοδότηση πρέπει να κωδικοποιείται ρητά,

πράγμα που συχνά παραβλέπεται καθώς υπάρχει υπερβολική εξάρτηση από τους ελέγχους εξουσιοδότησης διεπαφών. Δεδομένου ότι οι αλυσιδωτοί κώδικες χρειάζονται συχνά προσωπικά δεδομένα ως εισροή, η μη εξουσιοδοτημένη εκτέλεση μπορεί να οδηγήσει σε διαρροές προσωπικών δεδομένων, γεγονός που είναι καταστροφικό [22].

3.7 Εκτέλεση / Αρχιτεκτονικές Επιθέσεις

Δεδομένου ότι το Fabric χρησιμοποιεί άλλα λογισμικά ανοιχτής προέλευσης για να παρέχει τις υπηρεσίες του (Docker, gRPC, Apache Kafka), κληρονομεί και τα ελαττώματα και τις ευπάθειες τους. Έτσι, οι προγραμματιστές πρέπει να το λάβουν υπόψη κατά την ανάπτυξη των εφαρμογών τους. Επιπλέον, το Fabric δίνει στον οργανισμό την ευελιξία να καθορίσει τις δικές του Πολιτικές Ελέγχου Πρόσβασης, Συμμετοχής, Επικύρωσης, Συναίνεσης. Οι σωστά καθορισμένες πολιτικές αποτελούν τεράστιο αποτρεπτικό παράγοντα για τις εξωτερικές επιθέσεις. Εντούτοις, οι υποκείμενες εφαρμογές συχνά καθίστανται θύματα βασικών επιθέσεων, κλπ. Οι περισσότεροι προγραμματιστές αντιγράφουν-επικολλούν προηγουμένως γραπτό παράδειγμα κώδικα από το GitHub, StackOverflow, Companybases κ.λπ. για να εξοικονομήσουν χρόνο και προσπάθεια. Παρόλο που η πρακτική αυτή αυξάνει την αποδοτικότητά τους, μεταδίδει σφάλματα στον υπάρχοντα κώδικα που κάνει το σύστημα ευρέως ανοιχτό σε μια ποικιλία επιθέσεων. Παρακάτω περιγράφονται δύο επιθέσεις για την απεικόνιση κάθε σημείου αποτυχίας.

3.7.1 Docker TOCTOU Bug

Οι αλυσιδωτοί κώδικες εκτελούνται σε docker containers στα συστήματα στα οποία είναι εγκατεστημένα. Οι αλυσιδωτοί κώδικες δημιουργούνται σε ένα συγκεκριμένο κανάλι. Δεδομένου ότι κάθε κανάλι είναι λογικά ένα ιδιωτικό υποδίκτυο, ο εισαγόμενος αλυσιδωτός κώδικας εντοπίζεται μόνο σε αυτό το κανάλι. Το Docker TOCTOU bug στο docker θα μπορούσε να δώσει πρόσβαση εισερχόμενης ανάγνωσης / εγγραφής ως root στο σύστημα κεντρικού υπολογιστή με έξυπνα γραμμένο αλυσιδωτό κώδικα (chaincode) και πρόσβαση στην εντολή docker cp. Το TOCTOU attack (χρόνος ελέγχου σε ώρα χρήσης) στα Docker containers εκμεταλλεύεται το γεγονός ότι η ανάλυση διαδρομής κατά τη χρήση του docker cp δεν είναι ατομική. Δηλαδή, υπάρχει ένα μικρό παράθυρο μεταξύ του χρόνου που επιλύεται η διαδρομή στόχου και του χρόνου που χρησιμοποιείται. Εάν ένας εισβολέας μπορεί να προσθέσει μια συνιστώσα symlink στη διαδρομή μετά την ανάλυση, αλλά πριν λειτουργήσει, τότε το σύστημα θα μπορούσε να καταλήξει στην πλοήγηση στον κεντρικό υπολογιστή ως root [17].

Έτσι, εάν ένα σύστημα κεντρικού υπολογιστή εκτελεί εντολή docker cp με ένα συμβιβασμένο docker container, τότε ένας εισβολέας Α μπορεί να αντιγράψει προστατευμένα αρχεία ιδιωτικού κλειδιού στον κεντρικό υπολογιστή και ακόμη και να τοποθετήσει μια επίθεση εγγραφής στον συνομιλητή για να αντικαταστήσει τα αρχεία ρυθμίσεων και τα αρχεία ιδιωτικού κλειδιού [35]. Ουσιαστικά, ο Α θα μπορούσε να καταστρέψει ολόκληρο το σύστημα.

3.7.2 Ευπάθεια CouchDB

Όπως συμβαίνει με τις περισσότερες εφαρμογές λογισμικού, πολλές εφαρμογές βασίζονται σε προεπιλεγμένες βάσεις κωδίκων και σε αντικανονικά διαμορφωμένους ελέγχους πρόσβασης. Τα δίκτυα Fabric δεν είναι διαφορετικά και ως εκ τούτου πολλά σενάρια επίθεσης, συμπεριλαμβανομένων των παρακάτω, τα οποία επιδείχθηκαν σε ένα παράδειγμα κώδικα από τα μοτίβα κώδικα της IBM στο Defcon, είναι εξαιρετικά δυνατά [47].

Κάθε ομότιμος χρήστης στο δίκτυο Fabric περιέχει μια σύνοψη της τρέχουσας κατάστασης του αλυσιδωτού κώδικα (που ονομάζεται "παγκόσμια κατάσταση") που είναι αποθηκευμένο σε ένα σύστημα διαχείρισης βάσεων δεδομένων (LevelDB ή CouchDB) ως Key-Value Store. Οι ομότιμοι χρησιμοποιούν αυτό το κατάστημα για επικύρωση και για να παρακολουθήσουν την πραγματική κατάσταση του αλυσιδωτού κώδικα. Επομένως, αν ένας εισβολέας μπορεί να τροποποιήσει τη βάση δεδομένων χωρίς να επικαλεστεί αλυσιδωτό κώδικα, μπορεί να αλλάξει ανώνυμα την εικόνα του αλυσιδωτού κώδικα για τον ομότιμο [35].

Το Apache CouchDB είναι ένα σύστημα διαχείρισης βάσεων δεδομένων που ακολουθεί ένα μοντέλο αποθήκευσης εγγράφων χωρίς σχήμα, το οποίο είναι βελτιστοποιημένο για modularisation και κλιμάκωση. Χρησιμοποιείται εκτενώς σε έργα που βασίζονται στο Fabric επειδή μιλάει JSON εγγενώς και υποστηρίζει την αποθήκευση δυαδικών δεδομένων με ασφάλεια. Το CouchDB παρέχει μια βολική διεπαφή ιστού για πρόσβαση στη βάση δεδομένων, η οποία από προεπιλογή δεν προστατεύεται με κωδικό πρόσβασης. Επομένως, αν ένας εισβολέας Α συνδεθεί με ένα Ρ, μπορεί να έχει πρόσβαση και να αλλάξει την κατάσταση του Ρ από την ίδια την διεπαφή ιστού [46].

Κεφάλαιο 4

Αντιμέτρα Προστασίας στις Ευπάθειες και τις Επιθέσεις στο Hyperledger Fabric

4.1 Υποστήριξη Ιδιωτικών Δεδομένων στο Hyperledger Fabric με Ασφαλείς Πολύπλευρους Υπολογισμούς

Στη βιβλιογραφία υπάρχουν έρευνες [12], όπου χρησιμοποιώντας πρωτόκολλα ασφαλών "Πολύπλευρων Υπολογισμών (Multiparty Computation - MPC)" για την υποστήριξη των ιδιωτικών δεδομένων στο Hyperledger Fabric, ενσωμάτωσαν την εκτέλεση του πρωτοκόλλου ασφάλειας MPC ως μέρος της έξυπνης σύμβασης. Οι κρυπτογραφικές ασφαλείς τεχνικές MPC, που αναπτύχθηκαν από τη δεκαετία του '80 [30, 61], επιτρέπουν σε αμοιβαία μέρη να υπολογίζουν μια κοινή λειτουργία στις μυστικές εισόδους τους, φθάνοντας στο σωστό αποτέλεσμα χωρίς να χρειάζεται να αποκαλύψουν τις εισροές μεταξύ τους. Ένας καλός τρόπος σκέψης για τέτοια πρωτόκολλα είναι ότι αυτά μιμούνται τις εγγυήσεις ασφάλειας που θα ήταν δυνατό να πετύχει κάποιος έχοντας ένα μέλος εμπιστοσύνης να κάνει τον υπολογισμό εξ ονόματος των συμμετεχόντων.

Ωστόσο, αυτό το αξιόπιστο μέλος είναι απλώς εικονικό και αντικαθίσταται από κρυπτογραφικά μηνύματα που αποστέλλονται μεταξύ των πραγματικών μελών. Την τελευταία δεκαετία σημειώθηκε μεγάλη πρόοδος σε πρακτικά πρωτόκολλα κρυπτογραφικού ασφαλούς υπολογισμού, και αυτή η τεχνολογία είναι πλέον αρκετά αποτελεσματική.

Τα μέρη αποθηκεύουν κρυπτογραφημένα με το δικό τους μυστικό κλειδί τα προσωπικά τους δεδομένα σε ένα αρχείο, κάνοντας χρήση μιας κρυπτογράφησης συμμετρικού κλειδιού. Όταν απαιτούνται ιδιωτικά δεδομένα σε ένα έξυπνο συμβόλαιο, το μέλος που έχει το κλειδί το αποκρυπτογραφεί και χρησιμοποιεί την αποκρυπτογραφημένη τιμή ως τοπική εισήγησή του στο πρωτόκολλο των ασφαλών MPC. Αυτό επιτρέπει στην έξυπνη σύμβαση να εξαρτάται από οποιονδήποτε συνδυασμό δημόσιων και ιδιωτικών δεδομένων του αρχείου [12].

Αρχικά, διαφορετικά από άλλα συστήματα όπως το Enigma [63], η προσέγγισή τους ενσωμάτωνε ασφαλή πρωτόκολλα MPC στην αρχιτεκτονική μπλοκ αλυσίδων, χωρίς να διαθέτει ξεχωριστούς κόμβους που να εκτελούνται εκτός της αλυσίδας. Η προσέγγισή τους φάνηκε να αντιστοιχούσε καλύτερα για ένα εξουσιοδοτημένο blockchain όπως το Hyperledger Fabric, όπου οι ομότιμοι συσχετίζονται τυπικά με σημασιολογικά σημαντικές οντότητες που έχουν συμμετοχή στα δεδομένα του αρχείου. Πράγματι, το υποκείμενο μοντέλο εμπιστοσύνης σε ένα εξουσιοδοτημένο blockchain είναι ουσιαστικά το ίδιο με αυτό που χρησιμοποιείται στα πρωτόκολλα ασφαλών-MPC, δηλαδή αμοιβαία και ομότιμα μέλη που επικοινωνούν για να επιτύχουν έναν κοινό στόχο. Για παράδειγμα, στην περίπτωση χρήσης ιατρικών δεδομένων, είναι πιθανό ότι κάθε ομότιμος χρήστης του συστήματος θα ανήκει σε κάποιο νοσοκομείο και επομένως θα έχει κάποια δεδομένα που μπορεί να δει, αλλά οι υπόλοιποι δεν θα μπορούν. Έχοντας τους ίδιους ομότιμους που γράφουν στο αρχείο και εκτελώντας το πρωτόκολλο ασφαλούς-MPC, επιτρέπει να ευθυγραμμιστούν τα μοντέλα εμπιστοσύνης, οδηγώντας σε ένα πιο εύχρηστο και ασφαλέστερο σύστημα.

Επιπλέον, η εκτέλεση του ασφαλούς πρωτοκόλλου MPC επί της αλυσίδας επιτρέπει να χρησιμοποιηθούν οι εγκαταστάσεις blockchain στο ίδιο το πρωτόκολλο. Για παράδειγμα, είναι δυνατόν να χρησιμοποιηθούν οι λειτουργίες του blockchain για τη διαχείριση ταυτότητας και την επικοινωνία ή ακόμα και να χρησιμοποιηθεί μια υπάρχουσα εφαρμογή ενός πρωτοκόλλου συναίνεσης για την εφαρμογή ενός καναλιού εκπομπής

που μπορεί να χρειαστεί στο πρωτόκολλο. Η ανάθεση του πρωτοκόλλου ασφαλούς-MPC σε ένα στοιχείο εκτός αλυσίδας θα σήμαινε την εκ νέου υλοποίηση αυτών των λειτουργιών για το νέο αυτό στοιχείο.

Το βασικό επιχείρημα κατά της χρήσης πρωτοκόλλων ασφαλών MPC επί της αλυσίδας είναι ότι οι ανεπάρκειες του πρωτοκόλλου αλλά και του ίδιου του blockchain μπορούν να συνενωθούν μεταξύ τους, αλλά αυτό το επιχείρημα ισχύει περισσότερο για τα blockchains χωρίς άδεια, τα οποία είναι συνήθως πιο αργά από τα εξουσιοδοτημένα. Στα πειράματά τους με απλά ασφαλή πρωτόκολλα MPC, το κόστος του πρωτοκόλλου ασφαλούς-MPC ήταν πολύ μικρό και μια βελτιστοποιημένη έκδοση θα μπορούσε να γίνει πολύ πιο γρήγορα.

Στη συνέχεια, για να βοηθήσουν την έρευνα τους, εφάρμοσαν μια επίδειξη ενός απλού σεναρίου υποβολής προσφορών, όπου οι τιμές των αποθεματικών και οι προσφορές είναι μυστικές, ενώ όλες οι άλλες λεπτομέρειες δημοπρασίας είναι δημόσιες. Η έξυπνη σύμβαση υλοποιεί ένα μηχανισμό δημοπρασίας προσφοράς σφραγίδας 1ης τιμής (1st-price seal-bid auction mechanism), όπου οι συμμετέχοντες δεν μαθαίνουν παρά το αποτέλεσμα και ιδίως δεν μαθαίνουν τις προσφορές που χάνουν ή την τιμή αποθεματικού του πωλητή.

4.1.1 Εφαρμογή Πρωτοκόλλου Ασφαλείας MPC στο Hyperledger Fabric

Για να υποστηρίξουν συναλλαγές που εξαρτώνται από ιδιωτικά δεδομένα, έπρεπε να προσθέσουν δύο στοιχεία στο Fabric. Το πρώτο ήταν η τοπική διαμόρφωση. Για τη διαχείριση δεδομένων που είναι ορατά μόνο σε μερικούς χρήστες αλλά όχι σε άλλους, ο chaincode που εφαρμόζει τη λογική υποστήριξης στους διαφορετικούς ομότιμους χρήστες θα πρέπει να έχει πρόσβαση σε τοπικές παραμέτρους που δεν είναι διαθέσιμες σε άλλους χρήστες. Για παράδειγμα, οι ομότιμοι χρήστες συχνά χρειάζονται πρόσβαση στο μυστικό κλειδί της οργάνωσής τους. Ένα άλλο στοιχείο που προστέθηκε ήταν η επικοινωνία μεταξύ των ομότιμων χρηστών κατά τη διάρκεια της έγκρισης. Συγκεκριμένα, ο chaincode που τρέχει σε έναν ομότιμο χρήστη πρέπει να επικοινωνεί με τον ίδιο chaincode που τρέχει σε άλλους ομότιμους χρήστες, έτσι ώστε οι πληροφορίες σχετικά με τα ιδιωτικά δεδομένα να επηρεάζουν την απόφαση επικύρωσης των ομότιμων που δεν βλέπουν αυτά τα δεδομένα.

Στη διεθνή βιβλιογραφία [12], έχουν εφαρμοστεί αυτά τα στοιχεία χρησιμοποιώντας έναν "βοηθητικό εξυπηρετητή" που ανέπτυξαν. Ο βοηθητικός εξυπηρετητής αποθηκεύει τις τοπικές παραμέτρους κάθε ομότιμου χρήστη και διευκολύνει τη ρύθμιση καναλιών επικοινωνίας μεταξύ των περιπτώσεων του chaincode σε διαφορετικούς ομότιμους. Ο chaincode που τρέχει σε έναν ομότιμο χρήστη επικοινωνεί με τον βοηθητικό εξυπηρετητή, η διεύθυνση του οποίου κωδικοποιείται στο ίδιο chaincode. Η επικοινωνία μεταξύ των παραδειγμάτων του chaincode και του βοηθητικού εξυπηρετητή πραγματοποιείται μέσω ενός πλαισίου “Κλήσης Απομακρυσμένης Διαδικασίας (Remote Procedure Call - gRPC)” που χρησιμοποιείται εκτεταμένα στο Fabric. Δεδομένου ότι ο chaincode στο Fabric δεν γνωρίζει καν το αναγνωριστικό της ομότιμης ομάδας στο οποίο εκτελείται, αποστέλλει απλώς στον βοηθητικό εξυπηρετητή το περιεχόμενο της ταυτότητας Docker (from /proc/1/cpuset) και ο βοηθητικός εξυπηρετητής χρησιμοποιεί το εκτελέσιμο αρχείο Docker για να το μετατρέψει σε ένα όνομα περιεχομένου και εξάγει το ομότιμο όνομα από αυτό. Σημειώνεται ότι ο βοηθητικός εξυπηρετητής αποτελεί μια ασφαλή τεχνική για την εφαρμογή των δύο παραπάνω στοιχείων, καθώς αποτελεί ένα αξιόπιστο μέλος με καθολική πρόσβαση, το οποίο επιτρέπει την μελέτη της σκοπιμότητας της προσέγγισής χωρίς να χρειάζεται αλλαγή της ίδιας της αρχιτεκτονικής Fabric και αποδεικνύει ότι τα ασφαλή πρωτόκολλα MPC μπορούν να χρησιμοποιηθούν στην αλυσίδα του Fabric με αποτελεσματικό τρόπο.

Τα προσωπικά δεδομένα διατηρούνται στο αρχείο σε κρυπτογραφημένη μορφή, κάτω από κλειδιά που είναι διαθέσιμα μόνο στους ομότιμους χρήστες που υποτίθεται ότι θα το δουν. Επομένως, πρέπει να απαντηθεί το ερώτημα πώς θα μπορούσαν να τοποθετηθούν αυτά τα κρυπτογραφημένα δεδομένα στο αρχείο. Ο μόνος τρόπος για να βάλει κανείς δεδομένα στο αρχείο είναι ένας χρήστης να στείλει μια πρόταση συναλλαγής σε μερικούς ομότιμους χρήστες, ενώ όλοι αυτοί οι ομότιμοι χρήστες θα πρέπει να δουν μια ίδια πρόταση. Εάν η πολιτική επικύρωσης απαιτεί ομότιμους χρήστες από διαφορετικούς οργανισμούς, τότε ο μόνος τρόπος για να διατηρούνται τα δεδομένα κρυφά από ορισμένους ομότιμους είναι ο χρήστης να κρυπτογραφήσει τα δεδομένα προτού συμπεριληφθούν στην πρόταση. Ως εκ τούτου, αυτή η λύση απαιτεί ότι μερικοί χρήστες έχουν πρόσβαση στα κλειδιά κρυπτογράφησης.

Σε δοκιμαστικές εφαρμογής τους [12] έχουν χρησιμοποιηθεί ορισμένοι "προνομιακοί χρήστες" ανά οργανισμό που έχουν πρόσβαση στα κλειδιά που χρησιμοποιούν οι οργανισμοί για την κρυπτογράφηση των ιδιωτικών τους δεδομένων, τα ίδια κλειδιά που

χρησιμοποιούν οι ομότιμοι χρήστες αυτών των οργανώσεων για την αποκρυπτογράφηση των τιμών κατά τη διάρκεια της φάσης επικύρωσης. Μια άλλη επιλογή είναι η χρήση κρυπτογράφησης δημόσιου κλειδιού, όπου οι πελάτες χρησιμοποιούν τα δημόσια κλειδιά κρυπτογράφησης των σχετικών οργανισμών για την κρυπτογράφηση των ιδιωτικών δεδομένων και οι συνοδευόμενοι ομότιμοι χρήστες χρησιμοποιούν τα αντίστοιχα μυστικά κλειδιά αποκρυπτογράφησης για να ανακτήσουν τα ιδιωτικά δεδομένα για χρήση στο ασφαλές MPC πρωτόκολλο. Είτε έτσι είτε αλλιώς, η ανάπτυξη αυτού του τύπου λύσης σε ένα σύστημα παραγωγής θα απαιτούσε σωστή διαχείριση κλειδιών, για να διασφαλιστεί ότι μόνο τα εξουσιοδοτημένα συστατικά έχουν πρόσβαση σε κρυπτογραφικά κλειδιά.

Ενώ ο chaincode στο Fabric είναι συνήθως γραμμένος σε Go, οι περισσότερες κρυπτογραφικές βιβλιοθήκες για ασφαλείς πρωτόκολλα MPC είναι γραμμένες σε C++. Για να καλέσουν το EMP-toolkit από τον αλγόριθμο Go, ορισμένοι ερευνητές [12] χρησιμοποίησαν το SWIG, το οποίο επιτρέπει την κλήση του κώδικα C++ από άλλες γλώσσες. Για να προσθέσουν υποστήριξη για τα εργαλεία SWIG και EMP-toolkit, ενημέρωσαν το Fabric SDK για το Node.js έτσι ώστε τα αρχεία SWIG (* .cpp, * .hpp, * .swigcxx) να συμπεριληφθούν στο πακέτο αλγορίθμων που θα εγκατασταθούν. Χρησιμοποίησαν επίσης ένα προσαρμοσμένο περιβάλλον δημιουργίας που περιελάμβανε SWIG και EMP-toolkit.

Το EMP-Toolkit χρησιμοποιεί κανονικά τα δικά του κανάλια επικοινωνίας χρησιμοποιώντας υποδοχές UNIX, αλλά για να το χρησιμοποιήσουν μέσα στο Fabric, μελετητές [12] εφάρμοσαν νέα συγχρονισμένα κανάλια για το EMP-toolkit πάνω από το gRPC (χρησιμοποιώντας τον εξυπηρετητή βοήθειας). Τα κανάλια τους δημιουργήθηκαν στον chaincode του Go και διαβιβάστηκαν στο EMP-toolkit χρησιμοποιώντας το SWIG [58].

Στην αρχιτεκτονική Fabric, είναι ευθύνη του πελάτη-χρήστη να επιλέξει τους ομότιμους χρήστες για τις συναλλαγές του. Σε ορισμένες περιπτώσεις [12], ήταν σημαντικό ο πελάτης να επιλέγει ομότιμα μέλη του δικτύου που μπορούν να αποκρυπτογραφήσουν συλλογικά όλα τα ιδιωτικά πεδία από τα οποία εξαρτάται η συναλλαγή. Επίσης, ο χρήστης στην περίπτωσή τους έπρεπε να ενημερώνει τους ομότιμους χρήστες, καθώς κάθε ομότιμος χρήστης θα πρέπει να γνωρίζει τις ταυτότητες των άλλων ομότιμων προκειμένου να μπορεί να τρέξει ένα πρωτόκολλο ασφαλούς-MPC μαζί τους.

Εξετάστηκαν αρκετές πτυχές που σχετίζονται με την ασφάλεια, κάτι το οποίο πρέπει να αντιμετωπιστεί σε οποιοδήποτε σύστημα παραγωγής. Το πρώτο είναι οι πολιτικές ενίσχυσης καθώς είναι σημαντικό να ευθυγραμμιστεί το μοντέλο εμπιστοσύνης του πρωτοκόλλου ασφαλούς MPC με εκείνο της πολιτικής επικύρωσης στο αρχείο. Για παράδειγμα, αν το μοντέλο εμπιστοσύνης του πρωτοκόλλου αναλαμβάνει κατ' ανώτατο όριο t ανταγωνιστικά μέρη, μπορεί να οριστεί μια πολιτική που απαιτεί περισσότερους από t θεατές, εξασφαλίζοντας ότι μια μη έγκυρη συναλλαγή δεν θα εγκριθεί ποτέ στο μοντέλο εμπιστοσύνης. Η ευθυγράμμιση των μοντέλων εμπιστοσύνης είναι λιγότερο σημαντική στις ρυθμίσεις, όπου είναι δυνατόν να υποτεθεί ότι τα μέλη είναι ειλικρινή αλλά περίεργα, αφού ένα έντιμο, αλλά περίεργο, μέλος δεν θα υποστηρίξει μια άκυρη συναλλαγή.

Ως ένα άλλο παράδειγμα, μπορεί να οριστεί η πολιτική επικύρωσης για να διασφαλιστεί ότι οι μυστικές αξίες ενός οργανισμού δεν μπορούν να τροποποιηθούν χωρίς την επικύρωση αυτού του οργανισμού. Ωστόσο, η γλώσσα πολιτικής που χρησιμοποιείται στο Fabric δεν μπορεί να καθορίσει έναν τέτοιο περιορισμό. Εντός της υποστηριζόμενης γλώσσας πολιτικής, φαίνεται ότι το μόνο "ασφαλές περιβάλλον" είναι να απαιτείται κάθε συναλλαγή να επικυρώνεται από όλες τις οργανώσεις, γεγονός που μπορεί να κάνει τη διαδικασία έγκρισης πολύ αργή. Ίσως ένας καλός συμβιβασμός είναι να απαιτηθεί η έγκριση από τουλάχιστον τρεις οργανώσεις. Ένα παρόμοιο ζήτημα είναι ότι πρέπει να χρησιμοποιηθεί μια ενιαία πολιτική επικύρωσης για όλες τις συναλλαγές, ενώ σε πολλές περιπτώσεις μπορεί να επιβάλλονται διαφορετικοί περιορισμοί σε διαφορετικές δράσεις. Για παράδειγμα, στην επίδειξη του σεναρίου τους φαίνεται φυσικό να επιτραπεί στις οργανώσεις να εγκρίνουν τις συναλλαγές τους με νέα στοιχεία μόνοι τους, αλλά απαιτούνταν οι δημοπρασίες να εγκρίνονται από όλους τους συμμετέχοντες. Τέτοιες μη τυποποιημένες πολιτικές εγκρίσεων θα μπορούσαν να εφαρμοστούν στο Fabric χρησιμοποιώντας ένα προσαρμοσμένο "σύστημα κώδικα αλυσίδας", αλλά δεν διερεύνησαν αυτήν την επιλογή.

Επιπλέον, ένα σύστημα παραγωγής πρέπει να εφαρμόζει κατάλληλες πολιτικές εξουσιοδότησης για τους πελάτες. Για παράδειγμα, στη δοκιμαστική τους παρουσίαση, ίσως να ήθελαν να ορίσουν μερικούς προνομιούχους πελάτες ανά οργανισμό, οι οποίοι μπορούσαν να απαριθμήσουν νέα στοιχεία και να ενεργοποιήσουν δημοπρασίες για υπάρχοντα αντικείμενα αυτού του οργανισμού. Οι μη προνομιούχοι πελάτες ενδέχεται να εξακολουθούσαν να υποβάλλουν ερωτήματα για την κατάσταση του ημερολογίου, όπως

η περιγραφή όλων των αντικειμένων προς πώληση.

Οι συναλλαγές Fabric προστίθενται μέσω μιας διεργασίας δύο φάσεων και το πρωτόκολλο ασφαλούς-MPC εκτελείται στην πρώτη φάση για να επιτρέπει στους ομότιμων να αποφασίσουν αν θα εγκρίνουν ή όχι τη συναλλαγή. Αυτή η ρύθμιση, ωστόσο, επιτρέπει σε έναν απατεώνα ομότιμο να μάθει πρώτα το αποτέλεσμα του πρωτοκόλλου ασφαλούς-MPC και, στη συνέχεια, να αρνηθεί την επικύρωσή του, αν δεν του αρέσει αυτό το αποτέλεσμα. Ένας τρόπος αντιμετώπισης περιλαμβάνει τη χρήση πολιτικής κατώτερης επικύρωσης, έτσι ώστε κανένας ομότιμος χρήστης να μην μπορεί να μπλοκάρει τη συναλλαγή. Είναι δυνατόν επίσης να εφαρμοστεί μια συναλλαγή δέσμευσης στην οποία το αποτέλεσμα κρατιέται μυστικό, ακολουθούμενη από μια συναλλαγή αποκάλυψης κατά την οποία αυτό αποκαλύπτεται.

Τέλος, η συμπερίληψη μυστικών δεδομένων στη διαδικασία έγκρισης καθιστά δυσχερέστερη την εκ των υστέρων επαλήθευση της κατάλληλης επικύρωσης. Ένας τρόπος αντιμετώπισης αυτής της ανησυχίας είναι η καταγραφή στο μητρώο μη αλληλεπιδραστικών αποδείξεων μηδενικής γνώσης σχετικά με τη σωστή έγκριση. Μια φθηνότερη εναλλακτική λύση είναι να επιτρέπεται η επαλήθευση μόνο από προνομιούχους ελεγκτές, καταγράφοντας μαζί με τη συναλλαγή και το πρωτόκολλο (ή το hash), ενώ οι ομότιμοι να διατηρούν τα προσωπικά τους δεδομένα και τυχαία στοιχεία για να δείξουν στον ελεγκτή.

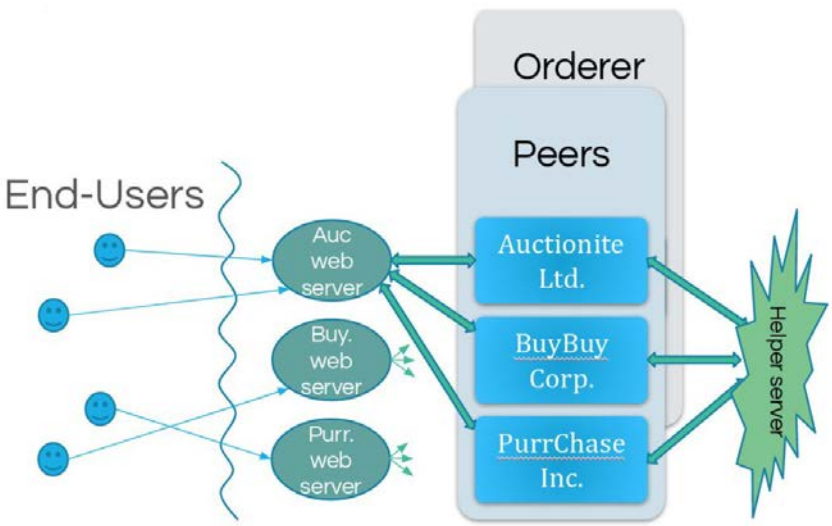
4.1.2 Δοκιμαστική Εφαρμογή Ασφαλείας MPC στο Hyperledger Fabric

Στη διεθνή βιβλιογραφία υπάρχουν δοκιμαστικές εφαρμογές [12] που υλοποίησαν ένα απλό σενάριο δημοπρασίας πρώτης τιμής με μυστικές τιμές αποθεμάτων και προσφορές. Περιελάμβανε τρεις οργανώσεις, που ονομάζονταν AUCIONITE LTD., BUYBUY CORP. και PURRCHASE INC., η καθεμία με έναν μοναδικό ομότιμο στο σύστημα. Κάθε οργανισμός μπορούσε να καταγράψει στοιχεία με μυστικές τιμές αποθεματικού και να τοποθετήσει σφραγισμένες προσφορές για αντικείμενα που παρατίθενται από τους άλλους. Όλες οι πληροφορίες σχετικά με τα στοιχεία καταγράφονταν στο αρχείο, συμπεριλαμβανομένου μιας μοναδικής ταυτότητας για την λίστα, μιας περιγραφής, μιας (προαιρετικής) εικόνας, μιας κατηγορίας, ενός ελάχιστου ποσού προσφοράς για το σαφές κείμενο, μιας κρυπτογραφημένης τιμής αποθεματικού και της ώρας / ημερομηνίας της δημοπρασίας. Ομοίως, κάθε εγγραφή προσφοράς περιελάμβανε την ταυτότητα του στοιχείου, την

ταυτότητα του υποψήφιου και ένα κρυπτογραφημένο ποσό προσφοράς.

Όταν μια συναλλαγή πλειστηριασμού ενεργοποιείται (κάνοντας κλικ σε ένα κουμπί στο περιβάλλον του χρήστη), και οι τρεις ομότιμοι ενεργοποιούνται για να την υποστηρίξουν, ενώ ο κάθε ομότιμος χρησιμοποιεί το οργανωτικό κλειδί για να αποκρυπτογραφήσει τα δικά του μυστικά από το αρχείο, τα οποία για τον πωλητή είναι η τιμή του αποθεματικού και για κάθε δυνητικό αγοραστή το ποσό της προσφοράς. Στη συνέχεια εκτελούν ένα ασφαλές πρωτόκολλο MPC για να καθορίσουν την υψηλότερη προσφορά και αν πληροί ή όχι την τιμή αποπληρωμής, ενώ το αποτέλεσμα της δημοπρασίας δημοσιεύεται στο αρχείο. Μετά τη διεξαγωγή της δημοπρασίας, όλα τα αρχεία προσφορών για τη δημοπρασία χαρακτηρίζονται ως "μη έγκυρα" και εάν η δημοπρασία επιτύχει, τότε το στοιχείο επισημαίνεται ως "πουλημένο", με νέο ιδιοκτήτη και με την τιμή πώλησης.

Όπως απεικονίζεται στο Σχήμα 4.1, η επίδειξη έχει τρία επίπεδα: ένα back-end Fabric (με τον εξυπηρετητή βοήθειας), τους διακομιστές δικτύου του οργανισμού (που παίζουν τους πελάτες Fabric) και το περιβάλλον εργασίας τελικού χρήστη που βασίζεται στον browser. Χρησιμοποίησα, επίσης, τρεις οργανισμούς με έναν ομότιμο ο καθένας (και IDs org<n>.example.com και peer<n>.org<n>.example.com, αντίστοιχα, <n> ∈ {0, 1, 2}). Χρησιμοποίησαν έναν μοναδικό διαχειριστή και τον εξυπηρετητή βοήθειας τον οποίο συνήθιζαν να εφαρμόζουν στους τοπικούς σταθμούς και στα κανάλια επικοινωνίας. Το περιβάλλον εργασίας τελικού χρήστη βασίζεται σε πρόγραμμα περιήγησης, υλοποιείται με το πλαίσιο εκκίνησης χρησιμοποιώντας HTML 5, CSS και Javascript.



Σχήμα 4.1: Οι τελικοί χρήστες έχουν πρόσβαση στους διακομιστές ιστού των διαφόρων οντοτήτων. Αυτοί

οι διακομιστές ιστού παίζουν το ρόλο των πελατών Fabric, μιλώντας με το back-end του Fabric (peers and orderer), το οποίο υποστηρίζεται από τον βοηθητικό εξυπηρετητή. [12]

Στο μεταξύ, είχαν ένα στρώμα διακομιστών δικτύου, έναν ανά οργανισμό. Από τη μία πλευρά αυτοί οι εξυπηρετητές εξυπηρετούν τη διεπαφή που βασίζεται στον browser στους τελικούς χρήστες και από την άλλη παίζουν το ρόλο των πελατών Fabric, αλληλεπιδρώντας με τους ομότιμων. Αυτή η στρώση αναπτύχθηκε με το Hyperledger Fabric SDK για το Node.js και χρησιμοποιεί τα πρότυπα hapijs και τα Handlebars.js. Για να απλοποιήσουν την κωδικοποίηση, εφάρμοσαν στην επίδειξη τους έναν ενιαίο εξυπηρετητή δικτύου ο οποίος εξυπηρετεί τον ιστότοπο και των τριών οργανισμών (αλλά φυσικά ένα σύστημα παραγωγής θα είχε διαφορετικούς εξυπηρετητές δικτύου για διαφορετικούς οργανισμούς).

Στη δοκιμαστική εφαρμογή [12], υπήρξε το ίδιο περιβάλλον εργασίας για τους τρεις οργανισμούς. Η "Διεπαφή Χρήστη (User Interface - UI)" επέτρεπε στους τελικούς χρήστες να δημιουργήσουν νέα στοιχεία, να απαριθμήσουν όλα τα διαθέσιμα στοιχεία, να υποβάλουν προσφορές σε ένα αντικείμενο που ανήκει σε άλλο οργανισμό, να καταγράψουν όλες τις προσφορές και να εκτελέσουν δημοπρασία για ένα στοιχείο. Η κανονική ροή μιας δημοπρασίας έχει ως εξής. Αρχικά, ένας πωλητής συνδέεται με τον ιστότοπο της οργάνωσής του και δημιουργεί ένα νέο ρεκόρ στοιχείου, καθορίζοντας πράγματα όπως η κατηγορία, η περιγραφή, η τιμή εκκίνησης και η εφεδρική τιμή. Η τιμή αποθεματικού είναι εμπιστευτική και αποστέλλεται κρυπτογραφημένη μόνο στον κώδικα αλυσίδας και κανένα άλλο μέρος δεν έχει πρόσβαση σε αυτήν. Στη συνέχεια, οι ενδιαφερόμενοι αγοραστές συνδέονται με τον ιστότοπο της οργάνωσής τους, βλέπουν τη λίστα των στοιχείων και τοποθετούν τις προσφορές τους. Η τιμή προσφοράς είναι επίσης εμπιστευτική και αποστέλλεται κρυπτογραφημένη στον αλυσιδωτό κωδικό. Τέλος, ο ιδιοκτήτης ενός στοιχείου συνδέεται με τον ιστότοπο για να ενεργοποιήσει τη δημοπρασία. Ο διακομιστής του δικτύου έπειτα επικοινωνεί με έναν ομότιμο από κάθε οργανισμό και όλοι υποστηρίζουν τη συναλλαγή αυτή, εκτελώντας το πρωτόκολλο ασφαλούς-MPC για να πάρει το αποτέλεσμα της δημοπρασίας. Ο αγοραστής που προσέφερε την υψηλότερη προσφορά θα είναι ο νικητής, εφόσον αυτή η προσφορά υπερβαίνει την τιμή αποθεματικού. Διαφορετικά, επιστρέφεται ένα κατάλληλο σφάλμα. Το αποτέλεσμα της δημοπρασίας τελικά δεσμεύεται στο αρχείο.

Η δοκιμαστική εφαρμογή [12], διαχειρίζεται μόνο τρία μέρη, δηλαδή έναν πωλητή και

μέχρι δύο χρήστες. Οι ερευνητές αναφέρθηκαν σε αυτά τα μέρη ως Sally ο πωλητής και οι χρήστες ως Boyd και Debra. Καθώς το EMP-toolkit δεν υποστηρίζει ακόμα πολλά πολυκομματικά πρωτόκολλα (δηλαδή περισσότερα από 2 μέρη), σχεδίασαν ένα απλό πρωτόκολλο τριών κομματιών για τα τρία αυτά μέρη, με βάση την εφαρμογή δύο ημι-ειλικρινών πρωτοκόλλων στη EMP - βιβλιοθήκη εργαλείων. Το πρωτόκολλό τους είναι ασφαλές στο ημι-τίμιο μοντέλο, υποθέτοντας την ειλικρινή πλειοψηφία (δηλαδή, το πολύ ένα αντίπαλο μέρος).

Η είσοδος της Sally είναι η τιμή αποθεματικού *s* για το στοιχείο και οι εισροές των δύο υποψηφίων είναι *b* (Boyd) και *d* (Debra). Αυτοί οι αριθμοί είναι όλοι ακέραιοι αριθμοί 32 bit. Στο τέλος του πρωτοκόλλου, όλα τα μέρη θα πρέπει να λάβουν το τριψήφιο ψηφίο εξόδου του οποίου η αξία είναι είτε 0 εάν η τιμή αποθεματικού δεν πληρείται (ή ο υπολογισμός αποβάλλεται), 1 εάν ο Boyd κέρδισε τη δημοπρασία, ή 2 εάν η Debra κέρδισε τη δημοπρασία. Σε περίπτωση που ο Boyd και η Debra υποβάλουν την ίδια προσφορά, άφησαν αυθαίρετα τον Boyd να κερδίσει τη δημοπρασία. Δηλαδή, η λειτουργία που υπολογίζουν είναι:

$$f(s, b, d) = \begin{cases} (0, 0)\ s > \max(b, d)\ //\ \text{Δεν βρέθηκε αποθεματικό} \\ (1, b)\ b \geq \max(s, d)\ //\ \text{Νίκησε ο Boyd} \\ (2, d)\ d \geq s, d > b\ //\ \text{Νίκησε η Debra} \end{cases}$$

Το πρωτόκολλο αποτελείται από τρία κύρια βήματα. Πρώτα οι δύο πλειοδότες συγκρίνουν τις προσφορές τους χρησιμοποιώντας το πρωτόκολλο του Yao για το πρόβλημα των εκατομμυριούχων, όπου η παραγωγή μοιράζεται μυστικά μεταξύ τους [61]. Συγκεκριμένα στο τέλος αυτού του βήματος παίρνουν δυο bits *xb* (Boyd) και *xd* (Debra) που είναι ξεχωριστά ομοιόμορφα και ικανοποιούν $xb \oplus xd = \{0$ εάν b <d ή 1 if b ≥ d$\}$.

Έπειτα, οι πλειοδότες τρέχουν δύο παραδείγματα της 1-από τις-2 συμβολοσειράς "Μεταφοράς σε Άγνοιας (Oblivious Transfer - OT)", για να λάβουν μια κατανομή "(Exclusive OR - XOR)" της μέγιστης τιμής (*b, d*). Στην πρώτη περίπτωση η Debra παίζει τον δέκτη OT, χρησιμοποιώντας το *xd* ως το κομμάτι επιλογής της. Ο Boyd επιλέγει μια τυχαία ακολουθία 32-bit *rb*, και στη συνέχεια παίζει τον αποστολέα OT,

χρησιμοποιώντας *rb* και *rb* ⊕ *b* ως τις δύο σειρές του, ταξινομημένες σύμφωνα με το *xb*. Δηλαδή αν *xb* = 0 τότε ο Boyd χρησιμοποιεί το ζεύγος (*rb, rb* ⊕ *b)*, και αλλιώς χρησιμοποιεί (*rb* ⊕ b*, rb)*. Το μερίδιο εξόδου Boyd είναι *rb*, και το μερίδιο της Debra είναι η ληφθείσα συμβολοσειρά (που δηλώνεται *rb*). Είναι εύκολο να ελεγχθεί ότι *rb* ⊕ *rd* = {0 εάν *xb* ⊕ *xd* = 0, ή *b* εάν *xb* ⊕ *xd*= 1}. Η δεύτερη περίπτωση είναι συμμετρική, με αποτέλεσμα οι δύο υποψήφιοι να έχουν σειρές εξόδου *rb, rd* ικανοποιώντας την συνθήκη *rb* ⊕ *rd* = {d εάν *xb* ⊕ *xd* = 0, ή 0 αν *xb* ⊕ *xd* = 1}. Οι δύο υποψήφιοι XOR τα μερίδιά τους από τις δύο περιπτώσεις, παίρνοντας έτσι *yb* = *rb* ⊕ *rb* και *yd* = *rd* ⊕ *rd*, και μάλιστα *yb* ⊕ *yd* = max (*b*, *d*).

Στη συνέχεια, ο Boyd στέλνει τα μερίδια του *xb* και *yb* σε Sally μέσω ενός ιδιωτικού καναλιού. Στη συνέχεια, οι Sally και Debra συμμετέχουν σε ένα άλλο πρωτόκολλο Yao, υπολογίζοντας κατά πόσο τηρήθηκε η τιμή αποθεματικού, δηλαδή ο δείκτης bit για (*yb* ⊕ *yd*) ≥ s. Εάν το αποθεματικό πληρείται, τότε η Debra στέλνει *xd, yd* στην Sally και στον Boyd, οι οποίοι μπορούν να ανακτήσουν τη νικηφόρα προσφορά *yb* ⊕ *yd* και τον νικητή *xb* ⊕*xd* και στη συνέχεια να τους στείλουν πίσω στη Debra [61].

4.2 Ασφαλής Εκτέλεση Έξυπνων Συμβολαίων

Στη διεθνή βιβλιογραφία υπάρχουν έρευνες που περιγράφουν το πρόβλημα της ασφαλούς εκτέλεσης έξυπνων συμβολαίων χρησιμοποιώντας αξιόπιστο υπολογιστικό υλικό για blockchains με τελική συναίνεση, το οποίο είναι εστιασμένο σε εφαρμογές Hyperledger Fabric [3, 15]. Συγκεκριμένα, εξετάζουν τις επιπλοκές που ενδέχεται να προκληθούν από τις επιθέσεις επαναφοράς σε αυτή τη ρύθμιση, απεικονίζοντας μια προσέγγιση strawman που είναι ανέφικτη και εισάγουν την προσέγγισή τους για την υποστήριξη της ασφαλούς εκτέλεσης αλυσιδωτού κώδικα (chaincode) χρησιμοποιώντας το σετ οδηγιών “Intel Software Guard Extensions (Intel SGX)” το οποίο αυξάνει την ασφάλεια του κώδικα και των δεδομένων της εφαρμογής. Αυτό εκτελεί κάθε αλυσιδωτό κώδικα στο δικό του θύλακα κατά τη διάρκεια της επικύρωσης σε ομότιμη ομάδα και επομένως προστατεύει την εμπιστευτικότητα και την ακεραιότητα της εφαρμογής blockchain και κατ’ επέκταση της εφαρμογής Hyperledger Fabric [15].

4.2.1 Μοντέλο Συστήματος Ασφαλούς Εκτέλεσης Έξυπνων Συμβολαίων

Θεωρώντας ένα δίκτυο blockchain στο Fabric με ορισμένους clients, μια υπηρεσία παραγγελιών και μια ομάδα ομότιμων χρηστών, οι οποίοι εκτελούν σε συνεργασία συναλλαγές και διατηρούν ένα κατανεμημένο αρχείο σε ένα μόνο "κανάλι" του Fabric, ένας client επικαλείται συναλλαγές στέλνοντας μια λειτουργία αλυσιδωτού κώδικα σε κάποιον ομότιμο χρήστη, ο οποίος στη συνέχεια την εκτελεί (προσομοιώνει) και παράγει μια θεώρηση που περιέχει την προκύπτουσα μεταβολή κατάστασης στο αρχείο [15]. Η λειτουργία, η ανταπόκριση, καθώς και η ενημέρωση του αρχείου μπορεί να περιέχουν ευαίσθητες πληροφορίες που πρέπει να παραμείνουν μυστικές. Για να αποφευχθεί η διαρροή πληροφοριών από αυτές τις ενέργειες, κάθε ομότιμος χρήστης είναι εφοδιασμένος με CPU με δυνατότητες SGX και εκτελεί συναλλαγές μέσα σε ένα θύλακα. Ο αλυσιδωτός κώδικας δεν έχει κάποια συγκεκριμένη προέλευση και μια συναλλαγή παίρνει τη λειτουργία εισόδου και την κατάσταση του blockchain ως “Αποθηκευμένη Τιμή-Κλειδί (Key-Value Store – KVS)”, μόνο μέσω της λειτουργίας getState. Ο αλυσιδωτός κώδικας πρέπει να πραγματοποιεί ενημερώσεις στο αρχείο και αυτό πραγματοποιείται μόνο μέσω των λειτουργιών putState. Η εκτέλεση μιας λειτουργίας αλυσιδωτού κώδικα επιστρέφει μια απάντηση που μπορεί να περιλαμβάνει ένα αποτέλεσμα υπολογισμού, την ενημέρωση κατάστασης και τις εξαρτήσεις μεταξύ ανάγνωσης και εγγραφής.

Παρόλο που οι περισσότεροι ομότιμοι χρήστες είναι συνήθως σωστοί, ένας ομότιμος μπορεί να γίνει κακόβουλος και να συμπεριφέρεται εσφαλμένα, για παράδειγμα, όταν προσπαθεί να μεγιστοποιήσει το δικό του κέρδος ή στην πραγματικότητα να αποτελεί έναν εισβολέα. Ένας ομότιμος χρήστης έχει τον πλήρη έλεγχο του λειτουργικού συστήματος, των εφαρμογών και των δεδομένων που βρίσκονται στη μνήμη και της μόνιμης αποθήκευσης, δηλαδή της κατάστασης του blockchain. Ωστόσο, ένας κακόβουλος ομότιμος χρήστης δεν μπορεί να αποκτήσει πρόσβαση ή να παραβιάσει τον κώδικα και τα δεδομένα που διαμένουν σε ένα θύλακα. Ένας κακόβουλος ομότιμος χρήστης δεν μπορεί ούτε να σπάσει παλαιότερες κρυπτογραφημένες πληροφορίες ούτε να εξαγάγει οποιαδήποτε μυστική πληροφορία από ένα θύλακα. Συνεπώς, ένας αλυσιδωτός κώδικας που τρέχει σε ένα θύλακα παράγει πάντα τα σωστά αποτελέσματα, δηλαδή, ο αλυσιδωτός κώδικας δεν αποκλίνει από τις προδιαγραφές του, ενώ η εσωτερική κατάσταση του θύλακα είναι γνωστή μόνο στον ίδιο το θύλακα και τίποτα δεν αποκαλύπτεται εκτός από την προκύπτουσα μεταβολή της κατάστασής του. Ωστόσο, ένας κακόβουλος ομότιμος χρήστης μπορεί να επικαλεσθεί τον αλυσιδωτό κώδικα του θύλακα με οποιαδήποτε είσοδο και σε αυθαίρετη σειρά. Ο ομότιμος χρήστης μπορεί να

παρακολουθήσει, να τροποποιήσει, να αναδιατάξει, να απορρίψει ή να επαναλάβει τις λειτουργίες του αλυσιδωτού κώδικα και όταν ο αλυσιδωτός κώδικας του θύλακα αποκτήσει πρόσβαση στο KVS, ο ομότιμος χρήστης μπορεί να τροφοδοτήσει οποιαδήποτε κατάσταση του blockchain σε αυτό.

Όπως είναι ευρέως γνωστό από τη βιβλιογραφία για ασφαλή υπολογισμό με κρυπτογραφικά πρωτόκολλα [01], η ακεραιότητα και η εμπιστευτικότητα δεν μπορούν να εξεταστούν χωριστά. Ομοίως, για μια ασφαλή εφαρμογή που εκτελείται σε ένα θύλακα, ένας κακόβουλος κεντρικός υπολογιστής μπορεί να παραβιάσει την εμπιστευτικότητα ενεργοποιώντας τον θύλακα να εκτελέσει σε "εσφαλμένες" εισόδους. Στο πλαίσιο του blockchain, αυτό σημαίνει ότι η εκτέλεση του αλυσιδωτού κώδικα αποκλίνει από τη σειρά συναλλαγών που βασίζεται στη συναίνεση. Επαναλαμβάνοντας και επεκτείνοντας το παράδειγμα δημοπρασίας από την εισαγωγή, μια τέτοια επίθεση θα μπορούσε να αποκαλύψει μυστικές πληροφορίες ως εξής. Υποθέτοντας ότι η αξιολόγηση της δημοπρασίας στην τρέχουσα κατάσταση του blockchain s1 θα αφήσει μια προσφορά b1 να κερδίσει τη δημοπρασία. Εάν ο κακόβουλος κόμβος μπορεί να ενεργοποιήσει τη συναλλαγή αξιολόγησης δημοπρασιών, μαθαίνει το b1. Εάν ο κόμβος μπορεί να επαναφέρει τον θύλακα σε s1 και να εκτελέσει άλλη συναλλαγή, μπορεί να υποβάλει προσφορά b2, να την προσθέσει στο αρχείο, να αξιολογήσει στη συνέχεια τη δημοπρασία και να μάθει εάν b2> b1. Μια τέτοια επίθεση κατάργησης σαφώς παραβιάζει την εμπιστευτικότητα των μεμονωμένων προσφορών. Όπως αναφέρθηκε προηγουμένως, οι επιθέσεις επαναφοράς σε περιβάλλοντα εμπιστοσύνης εκτέλεσης και η πρόληψή τους μόλις πρόσφατα κατανοήθηκαν καλύτερα [15].

4.2.2 Προσέγγιση Strawman

Αν αφεθεί ο θύλακας να εκτελεί μόνο συναλλαγές που έχουν παραγγελθεί από το δίκτυο με τελικό αποτέλεσμα εμποδίζεται το πρόβλημα της επαναφοράς. Αυτό ισοδυναμεί με την εκτέλεση ολόκληρου του blockchain ομότιμων χρηστών σε ένα θύλακα, όπως προτείνει και το Microsoft Coco [41], και το σχετικό έργο. Οι ερευνητές [15], αποκαλούν αυτό ως "προσέγγιση strawman" που μπορεί να λειτουργήσει για μια αρχιτεκτονική εκτέλεσης εντολών όπου η διαδικασία συναίνεσης έχει μόνο τελικές αποφάσεις , αλλά υποστηρίζουν αργότερα γιατί υπάρχουν καλύτεροι σχεδιασμοί.

Για το Fabric, ο σχεδιασμός strawman θα σήμαινε την ενσωμάτωση της εκτέλεσης του

αλυσιδωτού κώδικα, του endorser, του committer, της πρόσβασης στα αρχεία και όλων των άλλων στοιχείων ενός ομότιμου χρήστη μέσα σε ένα θύλακα. Αυτό προφανώς προστατεύει την ακεραιότητα της ακολουθίας εισόδου για τον αλυσιδωτό κώδικα, δεδομένου ότι ολόκληρο το Fabric ομότιμων χρηστών τρέχει μέσα στο SGX. Μια παρόμοια προσέγγιση λαμβάνεται στην πλατφόρμα blockchain-as-a-service της IBM, η οποία αναπτύσσει το Fabric ομότιμων χρηστών ως ασφαλές σύνολο υπηρεσιών σε ένα σύστημα IBM Z. Το ασφαλές σύστημα περιλαμβάνει ολόκληρο το λειτουργικό σύστημα, τη στοίβα middleware και την πλατφόρμα του blockchain, [47].

Παρόλο που κανένα λειτουργικό σύστημα δεν εκτελείται εντός του SGX, πρόσφατη έρευνα έχει καταδείξει πως οι εφαρμογές παλαιού τύπου μπορούν να εκτελούνται σε SGX μέσω ενός λειτουργικού συστήματος βιβλιοθήκης που εκτελεί μη τροποποιημένες εφαρμογές σε ένα θύλακα [05]. Σημειώνεται ότι το λειτουργικό σύστημα αρχειοθέτησης προσθέτει δεκάδες χιλιάδες γραμμές κώδικα που τρέχουν επίσης κατά μήκος της εφαρμογής στον θύλακα.

Αυτή η προσέγγιση εισάγει όμως πολλαπλά προβλήματα. Πρώτον, βρίσκεται σε αντίθεση με τη σημαντική αρχή της ασφάλειας των υπολογιστών που συνίσταται στην ελαχιστοποίηση του μεγέθους της "Βάσης Αξιοπιστίας Υπολογιστών (Trusted Computing Base - TCB)". Συγκεκριμένα, επίσης οι κατευθυντήριες γραμμές των προγραμματιστών SGX συνιστούν να χωριστεί μια εφαρμογή σε ένα αξιόπιστο και μη αξιόπιστο στοιχείο. Μόνο ένα μικρό τμήμα του κώδικα εφαρμογής πρέπει να εκτελείται εντός του θύλακα. Ένα μικρότερο TCB έχει λιγότερα σφάλματα, μειώνει την επιφάνεια επίθεσης και είναι περισσότερο επιδεκτικό στην ανάλυση ασφαλείας από ό, τι ολόκληρη η εφαρμογή.

Ένα δεύτερο πρόβλημα πηγάζει από την περιορισμένη μνήμη που είναι διαθέσιμη στους θύλακες. Η μνήμη ενός θύλακα βρίσκεται στην προσωρινή "Μνήμη της Σελίδας του Θύλακα (Enclave Page Cache - EPC)" που είναι απομονωμένη από το υπόλοιπο σύστημα. Το EPC περιορίζεται επί του παρόντος σε 128 MB. Μόλις ένας θύλακας φθάσει αυτό το όριο οι σελίδες ανατίθενται σε DRAM. Αυτό έχει ως αποτέλεσμα μια δραματική απώλεια απόδοσης, όπως αναφέρεται σε πολλά έργα [05]. Συγκεκριμένα, δεδομένου ότι το αρχείο αυξάνεται με κάθε μπλοκ, η κράτηση ολόκληρης της κατάστασης του blockchain στον θύλακα, φτάνει γρήγορα στον περιορισμό της μνήμης.

4.2.3 Προσέγγιση για το Hyperledger Fabric

Για να αποφύγουν τα μειονεκτήματα της προσέγγισης Strawman, ορισμένοι ερευνητές [15], υιοθετούν μια αρθρωτή αρχιτεκτονική που χωρίζει την εκτέλεση του αλυσιδωτού κώδικα εννοιολογικά από τον ομότιμο χρήστη και μετακινεί την εκτέλεση σε ένα θύλακα. Οι παράμετροι που σχετίζονται με το πρωτόκολλο του ομότιμου χρήστη είναι ενσωματωμένες σε μια αφηρημένη υπηρεσία παραγγελίας, εκ της οποίας μια διαδικασία μπορεί να τρέξει στον ίδιο ομότιμο χρήστη. Η υπηρεσία παραγγελιών είναι αξιόπιστη υπό την έννοια ότι δεν μπορεί να επαναληφθεί.

Η υπηρεσία παραγγελίας παράγει μια υπογεγραμμένη ακολουθία συναλλαγών για εκτέλεση εντός του θύλακα. Ο θύλακας μπορεί να επαληθεύσει ότι οι συναλλαγές προέρχονται από την υπηρεσία παραγγελιών, είναι στη σωστή σειρά και δεν έχουν αλλοιωθεί. Ο θύλακας διατηρεί επίσης πληροφορίες σχετικά με το ιστορικό συναλλαγών, το οποίο επιτρέπει την ανίχνευση παραβιάσεων παραγγελιών συναλλαγών ή επαναλαμβανόμενων συναλλαγών. Ο κακόβουλος κεντρικός υπολογιστής ενδέχεται να επαναφέρει τον θύλακα σε ένα προηγούμενο σημείο της ακολουθίας εκτέλεσης, αλλά αυτό δεν θα έβλαπτε την εφαρμογή, αφού οι συναλλαγές είναι ντετερμινιστικές και η εκτέλεση απλώς θα παράγει και πάλι τις ίδιες εξόδους.

Όπως περιγράφηκε μέχρι τώρα, αυτή η προσέγγιση λειτουργεί καλά με μια αρχιτεκτονική εντολής εκτέλεσης για την αναπαραγωγή κατάσσυτασης μηχανής. Το Fabric, ωστόσο, χρησιμοποιεί το παραδειγματισμό εκτέλεσης-παραγγελίας-επικύρωσης, όπου ένας ομότιμος χρήστης εκτελεί μια συναλλαγή προτού επιτευχθεί ομοφωνία σχετικά με την παραγγελία.

Κατά συνέπεια, η εκτέλεση είναι θεωρητική και μπορεί να επαναληφθεί χωρίς να επηρεαστεί η κατάσταση του blockchain, καθώς οι συναλλαγές προσομοιώνονται κατά τη διάρκεια της έγκρισης και παράγουν αποτελέσματα μόνο μετά την παραγγελία. Αυτό σημαίνει ότι ένας κακόβουλος κεντρικός υπολογιστής θα μπορούσε να συνάγει πληροφορίες σχετικά με τα δεδομένα μυστικής εφαρμογής από την θεωρητική εκτέλεση. Ακόμα και μια αξιόπιστη υπηρεσία παραγγελιών δεν μπορεί να αποτρέψει αυτόν τον τύπο διαρροής.

Για να επιλύσουν αυτό το ζήτημα, οι ερευνητές θα έπρεπε να προσαρμόσουν τις

εφαρμογές ώστε να λαμβάνουν υπόψη τον θεωρητικό χαρακτήρα της εκτέλεσης στο Fabric [15]. Για το παράδειγμα δημοπρασίας, ειδικότερα, ένα εμπόδιο θα αποθηκευτεί στο blockchain έτσι ώστε ο θύλακας του αλυσιδωτού κώδικα να αξιολογεί τη δημοπρασία μόνο εάν υπάρχει το εμπόδιο. Το εμπόδιο ορίζεται από την κλήση του αλυσιδωτού κώδικα με μια συναλλαγή που «κλείνει» τη δημοπρασία αλλά δεν την αξιολογεί ακόμα. Αν το εμπόδιο υπάρχει στο αρχείο, ένας κακόβουλος ομότιμος χρήστης δεν μπορεί πλέον να υποβάλει νέες προσφορές στη δημοπρασία. Από την άλλη πλευρά, η αξιολόγηση της δημοπρασίας θα εξετάσει μόνο προσφορές που προστίθενται στο αρχείο πριν από το εμπόδιο. Σημειώνεται ότι αυτό το εμπόδιο παίζει ρόλο παρόμοιο με ένα φράγμα μνήμης σε ένα πολυπύρηνο σύστημα υπολογιστή με ταυτόχρονα πλέγματα.

Μετά την αρχιτεκτονική εκτέλεσης-παραγγελίας-επικύρωσης, ο αλυσιδωτός κώδικας πρέπει να εκτελεί συναλλαγές μόνο στην δεσμευμένη κατάσταση blockchain, δηλαδή με καταχωρήσεις στο αρχείο που προκύπτουν από παραγγελθείσες συναλλαγές και έχουν διαπραχθεί από όλους τους ομότιμους χρήστες. Διαφορετικά, ένας κακόβουλος ομότιμος χρήστης μπορεί να παράγει το ίδιο το εμπόδιο και να τροφοδοτήσει την κατάσταση που θα προκύψει στο θύλακα κατά την αξιολόγηση της δημοπρασίας. Το σύστημα που περιγράφεται στην επόμενη ενότητα το εξασφαλίζει.

Για να σχηματίσουν τυπικά τη διαρροή πληροφοριών που επιτρέπεται στην αρχιτεκτονική εκτέλεσης-παραγγελίας-επικύρωσης του Fabric, οι ερευνητές [15], μοντελοποιούν ένα blockchain ως stateful λειτουργικότητα $F: S \times T \rightarrow S$. Ανά πάσα στιγμή η κατάσταση του αλυσιδωτού κώδικα είναι ένα στοιχείο του S. Οι πελάτες επικαλούνται συναλλαγές στο T, οι οποίες μπορεί να περιέχουν πράξεις με ορίσματα σύμφωνα με το F, αλλά αυτές εμπίπτουν στο διαφορετικό $t \in T$. Λαμβάνοντας το $s \in S$, εφαρμόζοντας μια συναλλαγή $t \in T$ του F σημαίνει να υπολογιστεί το $s' \leftarrow F(s, t)$, με αποτέλεσμα μια μεταγενέστερη κατάσταση $s' \in S$. Χρησιμοποιώντας μια υπηρεσία αξιόπιστης παραγγελίας όπως παρουσιάστηκε νωρίτερα, η εξέλιξη της κατάστασης του blockchain ορίζεται μέσω της ακολουθίας των συναλλαγών που υπογράφονται από την παραγγελία.

Με τη λειτουργικότητα αλυσιδωτού κώδικα F που τρέχει σε ένα θύλακα SGX, ακόμη και ένας κακόβουλος ομότιμος χρήστης μπορεί να μάθει μόνο την επόμενη κατάσταση που προκύπτει από μια συναλλαγή, αλλά τίποτα για τον ίδιο τον υπολογισμό.

Δεδομένου ότι τα κρυπτογραφικά κλειδιά θα μπορούσαν να διαμένουν στο θύλακα, η

κατάσταση του αρχείου δεν αποκαλύπτει απαραιτήτως όλες τις σχετικές πληροφορίες. Λόγω των επιθέσεων κατά της επαναφοράς που έχουν εισαχθεί νωρίτερα, ωστόσο, ένας τέτοιος ομότιμος χρήστης μπορεί να εκτελέσει οποιαδήποτε συναλλαγή σε οποιαδήποτε κατάσταση εισόδου που βρίσκεται στο ιστορικό συναλλαγών που εκδίδονται από την υπηρεσία παραγγελιών. Οι ερευνητές [15] ορίζουν για την ασφάλεια έως επαναφορά ότι εξετάζεται ένα σύστημα blockchain με μια αρχιτεκτονική ελέγχου εκτέλεσης-παραγγελίας-αξιολόγησης και υποτίθεται ότι η σωστή υπηρεσία παραγγελιών παράγει μια ακολουθία καταστάσεων $<s_0, s_1, \ldots, s_m>$ όπου $s_j = F(s_{j-1}, t_j)$ για το $t_j \in T$ και $j \in [1, m]$. Σύμφωνα με τους ερευνητές ο αλυσιδωτός κώδικας είναι ασφαλής μέχρι να ξαναρυθμιστεί εάν οποιοσδήποτε κακόβουλος ομότιμος, χρήστης μέσω της αλληλεπίδρασης με τον αλυσιδωτό κώδικα που τρέχει μέσα στο θύλακα, μπορεί να λάβει καταστάσεις $s^*_{k+1} = F(s_k, t)$, για κάθε $k \in \{0, 1, \ldots, m\}$ και μια αυθαίρετη συναλλαγή $t \in T$, αλλά όχι περισσότερες πληροφορίες.

Η έννοια ασφαλείας έως επαναφορά επισημοποιεί τις επιθέσεις κατά της εκτέλεσης που βασίζεται στο Fabric, όπου ένας κακόβουλος ομότιμος χρήστης μπορεί να συνεννοηθεί με έναν πελάτη. Ο πελάτης επικαλείται μια αυθαίρετη συναλλαγή t που αποκαλύπτει πληροφορίες σχετικά με την κατάσταση του αλυσιδωτού κώδικα. Ο ομότιμος χρήστης επιτρέπει στο Fabric να εκτελέσει t και να παράγει μια έξοδο, αλλά η έγκριση δεν αποστέλλεται ποτέ για παραγγελία και η συναλλαγή δεν συνδέεται ποτέ με το blockchain. Ο αλυσιδωτός κώδικας μπορεί να διαρρεύσει όλες τις καταστάσεις που προκύπτουν από αυτές τις εκτελέσεις.

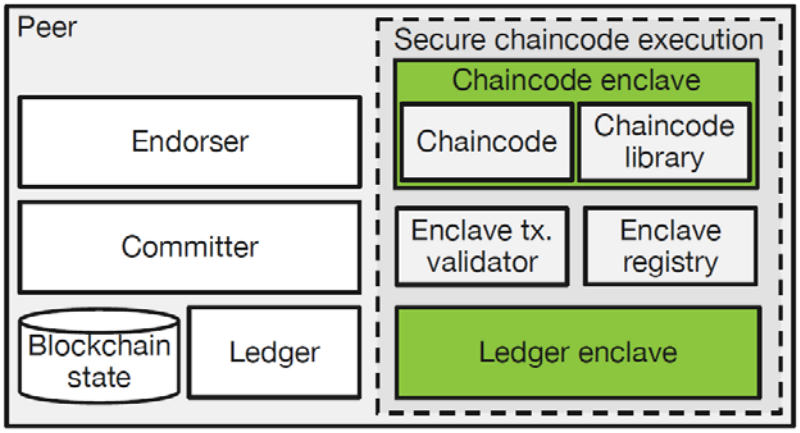
Σημειώνεται ότι το Fabric επιτρέπει παραλληλισμό κατά την εκτέλεση για τον διαχωρισμό υποθέσεων εμπιστοσύνης και την αύξηση της επεκτασιμότητας. Με την προσθήκη ενός εμποδίου στο blockchain, μια εφαρμογή επωφελείται ουσιαστικά από τις εγγυήσεις του σχεδίου παραγγελίας-εκτέλεσης σε σχέση με τις επαναφορές σε όλο το εμπόδιο. Η απαίτηση ενός εμποδίου μετά από κάθε συναλλαγή θα επιβάλλει στην πραγματικότητα το παραδειγματισμό παραγγελίας - εκτέλεσης στο Fabric.

4.2.4 Αρχιτεκτονική Συστήματος

Η παραπάνω προσέγγιση επεκτείνει ένα Fabric ομότιμων χρηστών με τα ακόλουθα συστατικά: Ένα θύλακα αλυσιδωτού κώδικα που εκτελεί έναν συγκεκριμένο αλυσιδωτό κώδικα και ένα θύλακα αρχείου που επιτρέπει σε όλους τους θύλακες αλυσιδωτού

κώδικα να επαληθεύσουν την ακεραιότητα κατάστασης του blockchain. Όλα τρέχουν μέσα στο SGX. Στο μη αξιόπιστο τμήμα του ομότιμου χρήστη, ένα μητρώο θύλακα διατηρεί την ταυτότητα όλων των θυλάκων αλυσιδωτού κώδικα και έναν θύλακα επικύρωσης συναλλαγής που είναι υπεύθυνος για την επικύρωση συναλλαγών που εκτελούνται από ένα θύλακα αλυσιδωτού κώδικα πριν από τη δέσμευσή τους στο αρχείο [15]. Το Σχήμα 4.2 δείχνει τα στοιχεία.

- **Θύλακας Αλυσιδωτού Κώδικα (Chaincode Enclave):** Ο θύλακας αλυσιδωτού κώδικα εκτελεί έναν συγκεκριμένο αλυσιδωτό κώδικα και έτσι τον απομονώνει από τον ομότιμο χρήστη και από άλλους αλυσιδωτούς κώδικες. Μια βιβλιοθήκη αλυσιδωτού κώδικα ενεργεί ως ενδιάμεσος μεταξύ του αλυσιδωτού κώδικα στον θύλακα και του ομότιμου χρήστη. Η βιβλιοθήκη αλυσιδωτού κώδικα εκθέτει τη διασύνδεση αλυσιδωτού κώδικα και Fabric και την επεκτείνει με πρόσθετη υποστήριξη για κρυπτογράφηση κατάστασης, βεβαίωση και ασφαλή πρόσβαση στο blockchain.



Σχήμα 4.2: Αρχιτεκτονική συστήματος. Το διακεκομμένο πλαίσιο υποδηλώνει τα στοιχεία που προστέθηκαν στον ομότιμο χρήστη για να επιτρέψει την ασφαλή εκτέλεση αλυσιδωτού κώδικα με το SGX. Τα στοιχεία που λειτουργούν εντός των θυλάκων SGX υποδηλώνονται σε πράσινο χρώμα. [15]

- **Θύλακας Αρχείου (Ledger Enclave):** Ο θύλακας αρχείου διατηρεί το αρχείο σε ένα θύλακα με τη μορφή μεταδεδομένων ειδικών για την ακεραιότητα που αντιπροσωπεύουν την πλέον πρόσφατη κατάσταση του blockchain. Εκτελεί τα ίδια βήματα επικύρωσης με τον ομότιμο χρήστη όταν φτάνει ένα νέο μπλοκ, αλλά παράγει επιπλέον ένα κρυπτογραφικό hash κάθε ζεύγους κλειδιού-τιμής της κατάστασης του blockchain και το αποθηκεύει εντός του θύλακα. Ο θύλακας

αρχείου αποκαλύπτει μια διεπαφή με το θύλακα αλυσιδωτού κώδικα για την πρόσβαση στα συγκεκριμένης ακεραιότητας μεταδεδομένα. Αυτό χρησιμοποιείται για την επαλήθευση της ορθότητας των δεδομένων που ανακτώνται από την κατάσταση του blockchain.

- **Μητρώο Θύλακα (Enclave Registry):** Το μητρώο θύλακα είναι ένας αλυσιδωτός κώδικας που εκτελείται εκτός του SGX και διατηρεί μια λίστα με όλους τους υπάρχοντες θύλακες αλυσιδωτού κώδικα στο δίκτυο. Εκτελεί βεβαίωση με τον αλυσιδωτό κώδικα και αποθηκεύει το αποτέλεσμα βεβαίωσης στο blockchain. Η βεβαίωση αποδεικνύει ότι ένας συγκεκριμένος αλυσιδωτός κώδικας εκτελείται σε έναν πραγματικό θύλακα. Αυτό επιτρέπει στους ομότιμους χρήστες και στους πελάτες να επιθεωρήσουν τη βεβαίωση ενός θύλακα αλυσιδωτού κώδικα προτού προβούν σε διαδικασίες αλυσιδωτού κώδικα ή πραγματοποιήσουν αλλαγές κατάστασης.
- **Θύλακας Επικύρωσης Συναλλαγής (Enclave Transaction Validator):** Ο θύλακας επικύρωσης συναλλαγής συμπληρώνει το σύστημα επικύρωσης του ομότιμου χρήστη και είναι υπεύθυνος για την επικύρωση συναλλαγών που παράγονται από ένα θύλακα αλυσιδωτού κώδικα. Συγκεκριμένα, ο θύλακας επικύρωσης συναλλαγής ελέγχει ότι μια συναλλαγή περιέχει έγκυρη υπογραφή που εκδίδεται από καταχωρημένο θύλακα αλυσιδωτού κώδικα. Εάν η επικύρωση είναι επιτυχής, επισημαίνει τις συναλλαγές ως έγκυρες και τις παραδίδει στο θύλακα αρχείου, ο οποίος διασταυρώνει την απόφαση πριν τελικά δεσμεύσει τη συναλλαγή στο αρχείο.

4.2.5 Αρχικοποίηση Συστήματος

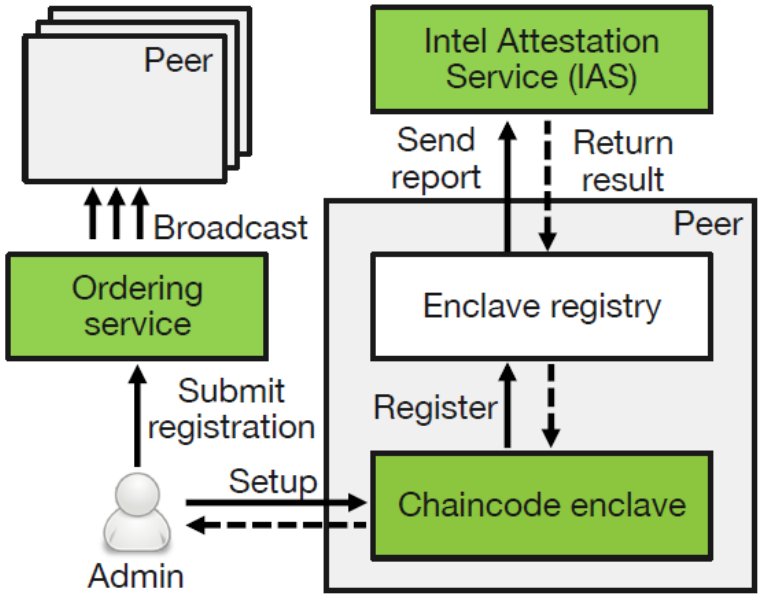
Όταν ένας ομότιμος συνδέεται με το δίκτυο blockchain, ο θύλακας αρχείου είναι αρχικοποιημένος από το διαχειριστή με το μπλοκ genesis, το οποίο περιέχει τη διαμόρφωση του blockchain και το αναμενόμενο hash (mrenclave) του θύλακα αρχείου. Αν το πραγματικό mrenclave που αποκτάται από τον ομότιμο χρήστη δεν ταιριάζει με την τιμή στο μπλοκ genesis, ο θύλακας αρχείου δεν προχωρά στην αρχικοποίηση. Στη συνέχεια, ο θύλακας αρχείου δημιουργεί ένα ζεύγος ιδιωτικών / δημόσιων κλειδιών (SKLE, PKLE), το οποίο επιτρέπει την μοναδική αναγνώριση του θύλακα αρχείου. Το δημόσιο κλειδί αποκαλύπτεται στους θύλακες αλυσιδωτού κώδικα ενώ το ιδιωτικό κλειδί κρατείται μυστικό μέσα στο θύλακα αρχείου.

Ο θύλακας αρχείου διατηρεί διάφορες τιμές διαμόρφωσης που λαμβάνονται αρχικά από το μπλοκ genesis, όπως οι ταυτότητες (δηλαδή τα δημόσια κλειδιά) των ομότιμων χρηστών, των πελατών και της υπηρεσίας παραγγελιών, τα οποία χρησιμοποιούνται για τον έλεγχο ταυτότητας όλων των ληφθέντων μπλοκ και συναλλαγών. Ο θύλακας αρχείου δέχεται μόνο μπλοκ που προέρχονται από την υπηρεσία παραγγελιών όπως ορίζεται στο μπλοκ genesis. Για να διασφαλιστεί αυτό, επαληθεύει ότι κάθε μπλοκ έχει έγκυρη υπογραφή που εκδίδεται από την υπηρεσία παραγγελιών. Σημειώνεται ότι η διαμόρφωση της κοινοπραξίας του blockchain μπορεί να ενημερωθεί χρησιμοποιώντας συναλλαγές διαμόρφωσης. Για απλότητα, ωστόσο, πολλές φορές οι ερευνητές θεωρούν μια στατική κοινοπραξία [15].

Κάθε μπλοκ έχει έναν αριθμό ακολουθίας και περιέχει μια λίστα συναλλαγών. Ο θύλακας αρχείου διατηρεί πληροφορίες σχετικά με την πιο πρόσφατα επεξεργασμένη συναλλαγή, για να διασφαλίσει ότι όλα τα μπλοκ θα υποστούν επεξεργασία με τη σωστή σειρά και δεν θα λείπουν μπλοκ. Μόλις ο ομότιμος χρήστης έχει ενταχθεί στο δίκτυο και έχει ξεκινήσει τον θύλακα αρχείου του, ο διαχειριστής ομότιμων χρηστών εγκαθιστά επίσης το μητρώο θύλακα σε κάθε ομότιμη ομάδα χρηστών και το εκδηλώνει. Αυτό ολοκληρώνει την προετοιμασία του ομότιμου χρήστη.

4.2.6 Θύλακας Αλυσιδωτού Κώδικα Εκκίνησης

Η αρχικοποίηση ενός θύλακα αλυσιδωτού κώδικα, ξεκινάει από τον διαχειριστή ομότιμο χρήστη και αποτελείται από τις ακόλουθες φάσεις: (1) δημιουργία του θύλακα αλυσιδωτού κώδικα, (2) εγγραφή στο μητρώο θύλακα, (3) πρόβλεψη μυστικών και (4) δέσμευση του θύλακα αλυσιδωτού κώδικα στο θύλακα του αρχείου [15]. Οι παραπάνω φάσεις φαίνονται στο Σχήμα 4.3.



Σχήμα 4.3: Διαδικασία εγγραφής θύλακα. [15]

Στην πρώτη φάση, ο διαχειριστής εγκαθιστά το θύλακα αλυσιδωτού κώδικα στον ομότιμο χρήστη και στη συνέχεια στέλνει μια πρόταση συναλλαγής εγκατάστασης. Στη συνέχεια, ο ομότιμος χρήστης ξεκινά το θύλακα αλυσιδωτού κώδικα, ο οποίος δημιουργεί ζεύγος ιδιωτικού / δημόσιου κλειδιού (SK_{CC}, PK_{CC}). Όσο για τον θύλακα του αρχείου, το δημόσιο κλειδί χρησιμοποιείται για την μονοσήμαντη αναγνώριση του θύλακα αλυσιδωτού κώδικα.

Δεύτερον, ο θύλακας αλυσιδωτού κώδικα κωδικοποιείται με το μητρώο του θύλακα όπως φαίνεται στο Σχήμα 4.3. Για το σκοπό αυτό, ο θύλακας αλυσιδωτού κώδικα καλεί τον καταχωρητή και με τη σειρά του, το μητρώο θύλακα εκτελεί απομακρυσμένη πιστοποίηση του αλυσιδωτού κώδικα. Λεπτομερέστερα, ο θύλακας αλυσιδωτού κώδικα παράγει πρώτα μια αναφορά βεβαίωσης που καταδεικνύει ότι είναι κατάλληλα δημιουργημένη με έναν συγκεκριμένο αλυσιδωτό κώδικα και αναγνωρίζεται από το PK_{CC}. Η αναφορά περιέχει $mrenclave_{CC}$ και (hash του) PK_{CC}. Ο θύλακας του αλυσιδωτού κώδικα καλεί στη συνέχεια τον καταχωρητή στο μητρώο του θύλακα με την αναφορά και το δημόσιο κλειδί του ως ορίσματα. Το μητρώο του θύλακα ελέγχει πρώτα ότι η αναφορά περιέχει την αναμενόμενη $mrenclave_{CC}$ και το σωστό hash του PK_{CC}. Στη συνέχεια, αποστέλλει την αναφορά στην "Υπηρεσία Επικύρωσης της Intel (Intel Attestation Service – IAS)" για επαλήθευση και σε αντάλλαγμα λαμβάνει ένα αποτέλεσμα βεβαίωσης, το οποίο δείχνει αν η αναφορά ήταν έγκυρη ή όχι.

Σημειώνεται ότι το αποτέλεσμα της βεβαίωσης υπογράφεται από το IAS και το κλειδί επαλήθευσης του είναι κοινά διαθέσιμο. Εάν η επαλήθευση επιτύχει, το μητρώο θύλακα ολοκληρώνει την εγγραφή καλώντας την putState για να αποθηκεύσει το αποτέλεσμα βεβαίωσης μαζί με το PK_{CC} στο αρχείο. Αυτό καθιστά το αποτέλεσμα βεβαίωσης προσβάσιμο σε όλους τους ομότιμους χρήστες στο δίκτυο μέσω του αρχείου, πιστοποιώντας ότι αυτός ο θύλακας τρέχει τον συγκεκριμένο αλυσιδωτό κώδικα του συγκεκριμένου ομότιμου χρήστη. Οι πελάτες και άλλοι ομότιμοι χρήστες χρησιμοποιούν αυτό με δύο τρόπους. Κατ 'αρχάς, ένας πελάτης επαληθεύει ότι επικαλείται συναλλαγές που περιλαμβάνουν μυστικά δεδομένα σε έναν εξουσιοδοτημένο για αυτό θύλακα. Δεύτερον, η κλάση που επικυρώνει τη συναλλαγή θύλακα ενός ομότιμου χρήστη, ο οποίος ενημερώνει την κατάσταση του blockchain, επαληθεύει ότι τα αποτελέσματα εκτέλεσης είναι γνήσια και προκύπτουν από την ασφαλή εκτέλεση στον θύλακα.

Μετά την επιτυχή εγγραφή του θύλακα αλυσιδωτού κώδικα, ο διαχειριστής προαιρετικά παρέχει το θύλακα αλυσιδωτού κώδικα με μυστικά. Για παράδειγμα, ο διαχειριστής μπορεί να εισάγει ένα κλειδί κρυπτογράφησης για τα δεδομένα που είναι αποθηκευμένα στο blockchain στον θύλακα αλυσιδωτού κώδικα.

Στην τελευταία φάση, ο θύλακας του αλυσιδωτού κώδικα συνδέεται με το θύλακα του αρχείου μέσω της τοπικής βεβαίωσης. Αυτό σημαίνει ότι ο θύλακας του αλυσιδωτού κώδικα ζητά από το θύλακα του αρχείου να αποδείξει ότι τρέχει τον αναμενόμενο κώδικα θύλακα αρχείου και λειτουργεί στην ίδια πλατφόρμα υποδοχής. Ο θύλακας αρχείου παράγει μια αναφορά βεβαίωσης και την επιστρέφει στον θύλακα αλυσιδωτού κώδικα, ο οποίος στη συνέχεια εκτελεί τα ίδια βήματα επαλήθευσης όπως περιγράφεται παραπάνω. Σε αντίθεση με την απομακρυσμένη βεβαίωση, η κρυπτογραφική προστασία της τοπικής βεβαίωσης χρησιμοποιεί HMAC και κοινόχρηστο κλειδί για επαλήθευση, που παρέχεται από την πλατφόρμα SGX. Εάν η επαλήθευση επιτύχει, ο θύλακας αλυσιδωτού κώδικα αποθηκεύει το δημόσιο κλειδί PKLE του θύλακα αρχείου και δεσμεύεται έτσι με το θύλακα αρχείου, με την έννοια ότι ο θύλακας αλυσιδωτού κώδικα χρησιμοποιεί αυτό για την επαλήθευση των προσπελάσεων στην κατάσταση του blockchain. Ο θύλακας αλυσιδωτού κώδικα απορρίπτει τυχόν τιμές κατάστασης του blockchain που δεν προέρχονται από αυτό το θύλακα αρχείου.

4.2.7 Εκτέλεση Αλυσιδωτού Κώδικα

Ένας πελάτης (client) ενεργοποιεί την εκτέλεση αλυσιδωτού κώδικα στέλνοντας μια πρόταση συναλλαγής επίκλησης με μια λειτουργία αλυσιδωτού κώδικα στον ομότιμο χρήστη. Ο ομότιμος χρήστης προωθεί τη λειτουργία του αλυσιδωτού κώδικα στον θύλακα αλυσιδωτού κώδικα, ο οποίος στη συνέχεια το επεξεργάζεται σύμφωνα με το έξυπνο συμβόλαιο. Ο θύλακας αλυσιδωτού κώδικα προετοιμάζει μια απάντηση και την επιστρέφει στον ομότιμο χρήστη, ο οποίος στη συνέχεια τη στέλνει ως απάντηση πρότασης συναλλαγής στον πελάτη.

Λεπτομερέστερα, πριν από την κλήση του θύλακα αλυσιδωτού κώδικα, ο πελάτης ερωτά τον ομότιμο χρήστη να ανακτήσει το δημόσιο κλειδί PK_{CC} του θύλακα και το αντίστοιχο αποτέλεσμα βεβαίωσης από το μητρώο θύλακα. Στη συνέχεια, ο πελάτης επαληθεύει την αυθεντικότητα του αποτελέσματος της βεβαίωσης, χρησιμοποιώντας το κλειδί επαλήθευσης IAS και ελέγχει ότι η βεβαίωση περιέχει την αναμενόμενη mrenclave του θύλακα αλυσιδωτού κώδικα, που ταιριάζει με το PK_{CC}. Εάν η επαλήθευση επιτύχει, ο πελάτης επικαλείται το θύλακα αλυσιδωτού κώδικα προετοιμάζοντας μια πρόταση συναλλαγής για τον αλυσιδωτό κώδικα που είναι στόχος. Συγκεκριμένα, ο πελάτης κρυπτογραφεί τη λειτουργία του αλυσιδωτού κώδικα χρησιμοποιώντας PK_{CC} και στη συνέχεια στέλνει την πρόταση στον ομότιμο χρήστη, ο οποίος εξάγει τη λειτουργία του αλυσιδωτού κώδικα και την μεταδίδει στον θύλακα αλυσιδωτού κώδικα. Στο εσωτερικό του θύλακα, η βιβλιοθήκη αλυσιδωτού κώδικα αποκρυπτογραφεί τη λειτουργία χρησιμοποιώντας SK_{CC} και επικαλείται τον αλυσιδωτό κώδικα με την επιχειρησιακή λειτουργία ως όρισμα.

Ο αλυσιδωτός κώδικας επεξεργάζεται τη λειτουργία, παράγει ένα αποτέλεσμα και το επιστρέφει στη βιβλιοθήκη αλυσιδωτού κώδικα. Ο αλυσιδωτός κώδικας μπορεί να αποκτήσει πρόσβαση στην κατάσταση του blockchain χρησιμοποιώντας τη βιβλιοθήκη αλυσιδωτού κώδικα, η οποία εκτελεί και επαληθεύει τις προσβάσεις.

Για να ολοκληρωθεί η κλήση του αλυσιδωτού κώδικα, η βιβλιοθήκη θύλακα δημιουργεί μια απάντηση, την υπογράφει χρησιμοποιώντας το SK_{CC} και την επιστρέφει στον ομότιμο χρήστη. Η απάντηση περιλαμβάνει τη λειτουργία, το set ανάγνωσης και το set γραφής και το αποτέλεσμα εκτέλεσης. Προαιρετικά, η βιβλιοθήκη αλυσιδωτού κώδικα κωδικοποιεί το αποτέλεσμα εκτέλεσης πριν φύγει από το θύλακα χρησιμοποιώντας ένα κλειδί κρυπτογράφησης που παρέχεται από τον πελάτη. Ο ομότιμος χρήστης στέλνει στη συνέχεια την απάντηση της πρότασης συναλλαγής στον πελάτη, ο οποίος εξάγει το

αποτέλεσμα εκτέλεσης και υποβάλλει τη συναλλαγή στην υπηρεσία παραγγελίας.

Επικύρωση και ενημέρωση κατάστασης. Η υπηρεσία παραγγελιών δέχεται συναλλαγές που υποβάλλονται από τους πελάτες, τις εκχωρεί σε ένα μπλοκ και μεταδίδει το μπλοκ σε όλους τους ομότιμους χρήστες στο δίκτυο. Προκειμένου να ολοκληρωθεί μια συναλλαγή, κάθε ομότιμος χρήστης επικυρώνει τη συναλλαγή και ενημερώνει το αντίγραφο αρχείου της.

Για την επικύρωση των συναλλαγών που παράγονται από ένα θύλακα αλυσιδωτού κώδικα, η κλάση επικύρωσης συναλλαγής θύλακα ουσιαστικά εκτελεί τα ίδια βήματα με τον "Αλυσιδωτό Κώδικα Συστήματος Επικύρωσης (Validation System Chaincode - VSCC)", ελέγχοντας για συγκρούσεις και αξιολογώντας την πολιτική επικύρωσης.

Επιπροσθέτως, επαληθεύει ότι η συναλλαγή παράχθηκε από το σωστό θύλακα αλυσιδωτού κώδικα ως εξής. Η κλάση επικύρωσης προσεγγίζει το μητρώο θύλακα για να ανακτήσει το αποτέλεσμα της βεβαίωσης και το δημόσιο κλειδί για το θύλακα που υποδεικνύεται από τη συναλλαγή. Στη συνέχεια, τα επαληθεύει ακολουθώντας τα ίδια βήματα που περιγράφηκαν προηγουμένως. Στη συνέχεια, επαληθεύει επίσης την υπογραφή του θύλακα στη συναλλαγή. Εάν αυτό επιτύχει, η κλάση επικύρωσης συναλλαγής θύλακα χαρακτηρίζει τη συναλλαγή ως έγκυρη, και ο ομότιμος χρήστης δεσμεύει τη συναλλαγή στο τοπικό της αρχείο και ενημερώνει αναλόγως την κατάσταση blockchain.

4.2.8 Πρόσβαση στην Κατάσταση του Blockchain

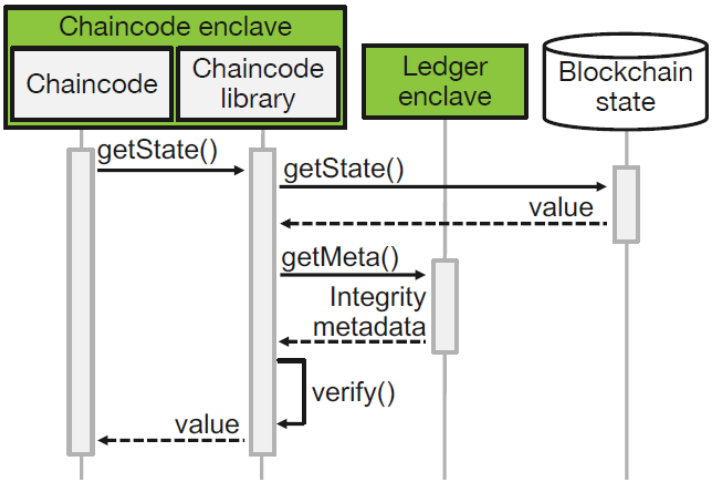
Ένας αλυσιδωτός κωδικός στο Fabric πρέπει μόνο να χρησιμοποιεί και να έχει πρόσβαση στην κατάσταση του blockchain. Η βιβλιοθήκη του αλυσιδωτού κώδικα μαζί με το θύλακα του αρχείου προστατεύει αυτά τα δεδομένα από το χειρισμό από τον τοπικό ομότιμο χρήστη.

Ακεραιότητα κατάστασης και συνέπεια. Όπως φαίνεται στο Σχήμα 4.4, όταν ο αλυσιδωτός κώδικας καλεί την getState (k) για να έχει πρόσβαση στα δεδομένα για το κλειδί k, η βιβλιοθήκη αλυσιδωτού κώδικα φορτώνει την αντίστοιχη τιμή val από την κατάσταση του blockchain στο θύλακα μέσω API αλυσιδωτού κώδικα που παρέχεται από τον ομότιμο χρήστη.

Επιπλέον, η βιβλιοθήκη αλυσιδωτού κώδικα ζητά τα αντίστοιχα μεταδεδομένα ακεραιότητας από το θύλακα αρχείου, καλώντας την getMeta (k, z) με ένα nonce z. Ο θύλακας αρχείου επιστρέφει την αναμενόμενη hash h_{val} της val στην κατάσταση blockchain και μία υπογραφή φ, που παράγεται από το θύλακα αρχείου ως $\varphi = sign_{SK_{LE}}(k\|z\|h_{val})$. Η βιβλιοθήκη αλγορίθμων έχει αποκτήσει το PK_{LE} κατά την εκκίνηση και το χρησιμοποιεί για να επαληθεύσει το φ.

Αν η επαλήθευση της υπογραφής πάνω από το k‖z‖Hash(val) επιτύχει, τότε το val είναι σωστό σύμφωνα με την κατάσταση του θύλακα αρχείου. Το nonce εξασφαλίζει ότι η απόκριση είναι σύγχρονη.

Εμπιστευτικότητα κατάστασης. Η βιβλιοθήκη αλυσιδωτού κώδικα μπορεί επίσης να προστατεύσει την εμπιστευτικότητα της κατάστασης του blockchain που διατηρείται από το θύλακα του αλυσιδωτού κώδικα. Η εγγενής μέθοδος σφράγισης δεδομένων του SGX για την προστασία των επίμονων δεδομένων δεν είναι κατάλληλη για δεδομένα που μοιράζονται από πολλαπλούς θύλακες σε διαφορετικούς ομότιμους χρήστες. Ο λόγος είναι ότι τα σφραγισμένα δεδομένα μπορούν να αποσφραγιστούν και πάλι από τον ίδιο θύλακα.



Σχήμα 4.4: Επαλήθευση κατάστασης blockchain με τη βοήθεια του θύλακα του αρχείου. [15]

Αντίθετα, η βιβλιοθήκη αλυσιδωτού κώδικα παρέχει έναν μηχανισμό κρυπτογράφησης κατάστασης που υποστηρίζει δύο τρόπους: την κρυπτογράφηση με βάση τον πελάτη και την κρυπτογράφηση ανά αλυσιδωτό κώδικα. Με την κρυπτογράφηση που βασίζεται στον πελάτη, ο πελάτης είναι υπεύθυνος για τη διαχείριση κλειδιών και πρέπει να

παράσχει ένα κλειδί κρυπτογράφησης μαζί με κάθε λειτουργία αλυσιδωτού κώδικα. Για την κρυπτογράφηση που βασίζεται σε αλυσιδωτό κώδικα, ένα κλειδί που αφορά συγκεκριμένο αλυσιδωτό κώδικα πρέπει να παρέχεται από έναν διαχειριστή σε όλους τους θύλακες αλυσιδωτού κώδικα κατά τη διάρκεια της εκκίνησης. Και στις δύο λειτουργίες, η κρυπτογράφηση και η αποκρυπτογράφηση εμφανίζονται με διαφάνεια στον αλυσιδωτό κώδικα κατά τη διάρκεια των κλήσεων putState και getState, αντίστοιχα.

Ως πρόσθετο πλεονέκτημα της διαχείρισης κλειδιού που βασίζεται σε πελάτη ή αλυσιδωτό κώδικα σε σύγκριση με τις εγγενείς μεθόδους SGX, τα δεδομένα στο blockchain μπορούν επίσης να ανακτηθούν από το blockchain αργότερα, χωρίς την υποστήριξη ενός θύλακα.

4.2.9 Υποστήριξη Επανεκκίνησης και Ανάκτησης

Μια συντριβή συστήματος ή επανεκκίνηση τερματίζει όλους τους θύλακες που έχουν δημιουργηθεί στον ομότιμο χρήστη. Για να αντιμετωπιστούν χωρίς χειροκίνητη παρέμβαση, οι εσωτερικές καταστάσεις κάθε θύλακα αλυσιδωτού κώδικα και ο θύλακας του αρχείου αποθηκεύονται διαρκώς περιοδικά [15].

Ο θύλακας του αρχείου διευκολύνει τη σφράγιση για την προστασία της κατάστασής του (συμπεριλαμβανομένων των μεταδεδομένων ακεραιότητας και του ιδιωτικού κλειδιού). Για να εξασφαλιστεί η συνέχεια της κατάστασης σε συντριβές, ο ομότιμος χρήστης θα πρέπει καταρχήν να γράψει την κατάσταση του θύλακα αρχείου στον δίσκο συγχρονισμένα μετά την επεξεργασία κάθε μπλοκ. Αυτό επηρεάζει σαφώς την απόδοση και μπορεί να μετριαστεί στην πράξη καθορίζοντας ένα διάστημα μπλοκ για την κράτηση της κατάστασης του θύλακα.

Ο θύλακας αλυσιδωτού κώδικα, αντίθετα, έχει απλώς αμετάβλητη κατάσταση (συμπεριλαμβανομένου του ιδιωτικού κλειδιού) που δημιουργήθηκε κατά την εκκίνηση του θύλακα. Αρκεί να σφραγιστεί και να αποθηκευτεί αυτή μία φορά μετά την αρχικοποίηση. Όταν ο θύλακας αλυσιδωτού κώδικα επανεκκινηθεί και αποκατασταθεί από τη σφραγισμένη κατάσταση, θα διατηρήσει την ίδια ταυτότητα του θύλακα και δεν χρειάζεται πάλι να κάνει εγγραφή ή απομακρυσμένη βεβαίωση.

4.2.10 Επέκταση Αλυσιδωτού Κώδικα

Υποστήριξη για τον εμπιστευτικό αλυσιδωτό κώδικα. Ο θύλακας αλυσιδωτού κώδικα μπορεί επίσης να επεκταθεί για να υποστηρίξει την εκτέλεση του εμπιστευτικού αλυσιδωτού κώδικα, το οποίο απαιτεί υποστήριξη για δυναμική φόρτωση κρυπτογραφημένου κώδικα σε θύλακες [15, 31]. Αυτό επιτρέπει την ανάπτυξη ιδιόκτητου κώδικα έξυπνης σύμβασης χωρίς να αποκαλύπτεται στους εκτελεστές ομότιμους χρήστες. Για να ενεργοποιηθεί αυτή η λειτουργία, ο θύλακας αλυσιδωτού κώδικα επεκτείνεται με ένα bootloader που εισάγει ένα δυαδικό κρυπτογραφημένο αλυσιδωτό κώδικα στον θύλακα. Ο bootloader τον αποκρυπτογραφεί και εκτελεί τον αλυσιδωτό κώδικα.

Για το σκοπό αυτό, ο διαχειριστής που εγκαθιστά τον αλυσιδωτό κώδικα σε έναν ομότιμο χρήστη ή ο προγραμματιστής αλυσιδωτού κώδικα κωδικοποιεί τον δυαδικό αλυσωτό κώδικα για το θύλακα αλυσιδωτού κώδικα χρησιμοποιώντας το δημόσιο κλειδί του. Επιπλέον, η λειτουργικότητα βεβαίωσης του θύλακα αλυσιδωτού κώδικα πρέπει να προσαρμοστεί έτσι ώστε οι ομότιμοι χρήστες και οι πελάτες να μπορούν να επαληθεύσουν ότι ένας συγκεκριμένος, κρυπτογραφημένος αλυσιδωτός κώδικας εκτελείται από τον θύλακα. Δεδομένου ότι το mrenclave υποδηλώνει τον κώδικα bootloader που εκτελείται στον θύλακα, η βεβαίωση πρέπει επίσης να περιέχει ένα hash του δυαδικού αλυσιδωτού κώδικα, το οποίο είναι δημόσια γνωστό από τους ομότιμους χρήστες και τους πελάτες.

Μεταφορά αξιόπιστης κατάστασης. Όταν ένας ομότιμος χρήστης συνδέεται με ένα υπάρχον blockchain, αυτό πρέπει να επικυρώσει όλα τα μπλοκ που έχουν υποστεί επεξεργασία πριν και να ανακατασκευάσει την τρέχουσα κατάσταση blockchain. Ανάλογα με την ηλικία του blockchain, αυτή η προσπάθεια μπορεί να είναι απαγορευτική. Επίσης, ένας ομότιμος χρήστης μπορεί να ήταν εκτός σύνδεσης για μεγαλύτερο χρονικό διάστημα και πρέπει να καλύψει το κενό όταν επανέλθει στο διαδίκτυο. Εάν ο ομότιμος χρήστης δεν θέλει να εμπιστευτεί κάποιον άλλον ομότιμο χρήστη για την παροχή της πιο πρόσφατης κατάστασης του blockchain, τότε μπορεί να εκμεταλλευτεί ένα θύλακα αρχείου για να αποκτήσει την τρέχουσα κατάσταση με ασφάλεια.

Όταν ο ομότιμος χρήστης P_A συνδέεται ή επανέρχεται μετά από μεγάλο χρονικό διάστημα διακοπής, επικοινωνεί με άλλον ομότιμο χρήστη P_B για υποστήριξη. Ο P_A

στέλνει ένα μήνυμα που περιέχει το hash του μπλοκ genesis και τα μεταδεδομένα ακεραιότητας, ανάλογα με τη θέση του θύλακα αρχείου του LE_A στο blockchain. Ο ομότιμος χρήστης P_B περνάει αυτό στο θύλακα αρχείου του LE_B , ο οποίος εκτελεί τέσσερα βήματα: (1) Ελέγχει ότι ο LE_A είναι μέρος του ίδιου blockchain με τη σύγκριση των hashes των μπλοκ genesis. (2) υπολογίζει τη διαφορά Δ (σε όρους κλειδιών KVS) μεταξύ της κατάστασης του P_A και της δικής του κατάστασης από τα μεταδεδομένα ακεραιότητας του P_A. (3) δημιουργεί μια έκθεση βεβαίωσης που περιέχει το Δ και τον τελευταίο γνωστό αριθμό ακολουθίας του μπλοκ. και (4) επιστρέφει την αναφορά και Δ στον P_B. Σε αυτό το σημείο το Δ περιέχει μόνο τα κλειδιά KVS και τα αντίστοιχα μεταδεδομένα ακεραιότητας, οπότε ο P_B συμπληρώνει το Δ με τις πραγματικές τιμές από την κατάσταση του blockchain. Ο P_B διαβιβάζει επίσης την έκθεση βεβαίωσης στο IAS για επαλήθευση. Στη συνέχεια, ο P_B στέλνει το αποτέλεσμα βεβαίωσης και το Δ στον P_A, και ο P_A επαληθεύει το περιεχόμενό του. Εάν είναι επιτυχής, τότε ο P_A ενημερώνει τον τελευταίο δικό του γνωστό αριθμό ακολουθίας μπλοκ και την κατάσταση blockchain του αντίστοιχα και διαβιβάζει τα δεδομένα στον LE_A, ο οποίος εκτελεί τα ίδια βήματα επαλήθευσης με τον ομότιμο χρήστη και ενημερώνει επίσης τα μεταδεδομένα ακεραιότητας.

Κεφάλαιο 5
Συμπεράσματα

Ένα δίκτυο blockchain αποτελεί ένα κατανεμημένο σύστημα για την καταγραφή του ιστορικού των συναλλαγών που πραγματοποιούνται μέσα σε αυτό, εντός ενός κοινού μητρώου, παρέχοντας με αυτόν τον τρόπο συνέπεια και σταθερότητα, καθώς όλοι οι συμμετέχοντες έχουν την ίδια εικόνα του αρχείου στο οποίο από τη στιγμή που κάποια αλλαγή γίνεται δεκτή δεν μπορεί πλέον να αλλάξει. Αρχικά, η blockchain τεχνολογία συνάντησε ευρεία αποδοχή από την εφαρμογή της στα δημοφιλή κρυπτονομίσματα Bitcoin, όμως σήμερα κερδίζει ολοένα και μεγαλύτερη δυναμική και σε άλλους τομείς και από πολλούς ερευνητές θεωρείται ως μια αλλαγή που προκαλεί ανάλογες προσδοκίες με αυτές που δημιούργησε το λογισμικό ανοιχτού κώδικα [39] ή ακόμη και το Διαδίκτυο [47]. Το Hyperledger Fabric αποτελεί ένα blockchain σύστημα με χρήση αδειών, καθώς η οποιαδήποτε εγγραφή στο αρχείο απαιτεί ορισμένα διαπιστευτήρια από το χρήστη. Οι συμμετέχοντες που επιτρέπεται να γράψουν στο αρχείο στο Hyperledger Fabric ονομάζονται ομότιμοι και συνήθως το πλήθος τους είναι μικρό. Αυτή η ρύθμιση διευκολύνει στον έλεγχο των συναλλαγών που πραγματοποιούνται στο αρχείο και συνήθως οι απαιτούμενες διεργασίες είναι ταχύτερες από τις αντίστοιχες του δημόσιου blockchains, το οποίο χρησιμοποιείται στα περισσότερα κρυπτονομίσματα. Σχεδόν όλες οι αρχιτεκτονικές blockchain υποστηρίζουν την έννοια των έξυπνων συμβολαίων, δηλαδή μια προγραμματιζόμενη λογική εφαρμογή που χρησιμοποιείται για οποιουδήποτε είδους συναλλαγή. Στο Hyperledger Fabric, τα έξυπνα

συμβόλαια υλοποιούνται μέσω ενός "αλυσιδωτού κώδικα" (chaincode), ο οποίος μπορεί να αποτελεί ένα αυθαίρετο πρόγραμμα, το οποίο εκτελείται από ορισμένους ομότιμους χρήστες. Ο chaincode έχει πρόσβαση στο τρέχον αρχείο καθώς και στα στοιχεία της νέας συναλλαγής και αποφασίζει αν θα πραγματοποιηθεί ή όχι η συναλλαγή αλλά και για τα δεδομένα που τελικά θα προστεθούν στο αρχείο.

Το Fabric βασίζεται σε μερικά αξιόπιστα μέρη και συγκεντρωτικές υπηρεσίες για την παροχή μιας γενικευμένης πλατφόρμας για δεδομένα τύπου μπλοκ. Ωστόσο, αυτά μπορούν να αξιοποιηθούν κακόβουλα και μπορεί να οδηγήσουν σε επιθέσεις που δεν θα ήταν εφαρμόσιμες σε ένα παραδοσιακό δίκτυο αποκλεισμού. Η αρθρωτή αρχιτεκτονική του Hyperledger προωθεί τη χρήση πρωτοκόλλων αυτοεξυπηρέτησης, ωστόσο, τα συστήματα που είναι ενσωματωμένα στα πρωτόκολλα αυτά είναι ασφαλή όσο είναι τα ίδια τα πρωτόκολλα. Ωστόσο, αυτή η αρθρωτή αρχιτεκτονική παρουσιάζει επίσης ένα πρόβλημα για τον εισβολέα, καθώς διαφορετικοί συνδυασμοί πρωτοκόλλων πρέπει να αξιοποιηθούν με διαφορετικούς τρόπους. Το Fabric είναι η πιο δημοφιλής πλατφόρμα αλυσιδωτού κώδικα σήμερα. Με μεγάλες επενδύσεις ύψους άνω των 100 εκατομμυρίων δολαρίων, από τις μεγάλες εταιρείες τεχνολογίας όπως η Intel, η Cisco, η IBM κ.λπ., καθώς και σημαντικοί χρηματοπιστωτικοί οργανισμοί όπως η JP Morgan, η Deutsche Bank κ.λπ., είναι σαφές ότι η τεχνολογία αυτή συγκεντρώνει την προσοχή. Ωστόσο, όπως περιγράφηκε εκτενώς στη συγκεκριμένη εργασία και όπως αυτές παρουσιάζονται στη διεθνή βιβλιογραφία δεν απουσιάζουν οι επιθέσεις στο Fabric. Αυτές σχετίζονται κυρίως με την παραβίαση της ασφάλειας από κάποιον κακόβουλο MSP, με τις υπηρεσίες κακόβουλης παραγγελίας, με τους κακόβουλους επικυρωμένους κόμβους, τις εξωτερικές επιθέσεις, τις επιθέσεις βάσει πρωτοκόλλου, τις ευπάθειες του αλυσιδωτού κώδικα (codechain) και τις επιθέσεις στην αρχιτεκτονική του συστήματος.

Παρ' όλη την επικινδυνότητα των παραπάνω επιθέσεων και ευπαθειών του Hyperledger Fabric, οι ερευνητές έχουν αναπτύξει διάφορες μεθόδους αντιμετώπισής τους, λαμβάνοντας ορισμένα αντιμέτρα για τους παραπάνω κινδύνους. Στη συγκεκριμένη εργασία αναλύθηκαν τα αντιμέτρα που σχετίζονται με τη διατήρηση της ιδιωτικότητας των δεδομένων στο Hyperledger Fabric χρησιμοποιώντας πρωτόκολλα ασφαλών MPC επί της αλυσίδας και της ασφαλούς εκτέλεσης του αλυσιδωτού κώδικα (chaincode). Στο Hyperledger Fabric, οι κόμβοι που έχουν πρόσβαση στο αρχείο καλούνται ομότιμοι και κάθε ομότιμος ανήκει σε κάποια οργάνωση. Η προσθήκη συναλλαγών στο Fabric είναι μια διαδικασία δύο φάσεων. Ο πελάτης που ζητά μια συναλλαγή προσεγγίζει πρώτα έναν ή περισσότερους ομότιμους με μια πρόταση συναλλαγής και τους ζητά να εκτελέσουν και

να εγκρίνουν την πρόταση. Οι υποψήφιοι ομότιμοι χρήστες στη συνέχεια εκτελούν ένα έξυπνο συμβόλαιο, το οποίο ονομάζεται chaincode στο Fabric, για να καθορίσουν αν θα υποστηρίξουν τη συναλλαγή ή όχι και αν ναι, τότε πώς θα αλλάξει αυτή η συναλλαγή την κατάσταση στο αρχείο. Μια σχετική λεπτομέρεια είναι ότι όλοι οι υποστηρικτές πρέπει να βλέπουν μια ίδια πρόταση συναλλαγής (αλλιώς απορρίπτεται στην επόμενη φάση). Δεδομένου ότι η "λογική εγκυρότητα" των συναλλαγών προσδιορίζεται στη φάση επικύρωσης, ορισμένοι ερευνητές επέλεξαν να τρέξουν τα πρωτόκολλα ασφαλών-MPC κατά τη διάρκεια αυτής της φάσης [12].

Από τη στιγμή που λαμβάνονται επαρκείς δεσμεύσεις, ο πελάτης αποστέλλει την εγκεκριμένη συναλλαγή σε μια υπηρεσία παραγγελιών, η οποία επιβάλλει μια γραμμική σειρά στις συναλλαγές και στη συνέχεια τις προσθέτει πραγματικά στο αρχείο. Ο αριθμός των απαιτούμενων θεωρήσεων για μια συναλλαγή καθορίζεται από μια πολιτική επικύρωσης, η οποία τίθεται όταν προετοιμάζεται το αρχείο. Ορισμένες πολιτικές αυτής της τεχνικής προϋποθέτουν την ύπαρξη τουλάχιστον ενός υποστηρικτή ή τουλάχιστον δύο κλπ. Σε γενικές γραμμές, το αρχείο έχει μόνο μία πολιτική επικύρωσης που ισχύει για όλες τις συναλλαγές σε αυτήν.

Όπως είδαμε στην παρούσα εργασία, στη διεθνή βιβλιογραφία υπάρχουν έρευνες [12] για την υποστήριξη ιδιωτικών δεδομένων για Hyperledger Fabric χρησιμοποιώντας πρωτόκολλα ασφαλών MPC επί της αλυσίδας. Συγκεκριμένα, περιγράφηκε ο τρόπος σχεδίασης μιας αρχιτεκτονικής που υποστήριζε τέτοια ιδιωτικά δεδομένα και υλοποίησαν μια δημοπρασία που την χρησιμοποιεί. Η συγκεκριμένη προσέγγιση εντόπισε δύο στοιχεία που έπρεπε να προστεθούν στο Fabric για να καταστεί δυνατή η εκτέλεση έξυπνων συμβάσεων που εξαρτώνται από τέτοια ιδιωτικά δεδομένα.

Όσον αφορά το ασφαλές σύστημα εκτέλεσης αλυσιδωτού κώδικα που παρουσιάστηκε στην παρούσα εργασία, αυτό διατηρεί την ασφάλεια μέχρι την επαναφορά. Υπενθυμίζεται ότι αυτή η έννοια ασφαλείας ορίζεται με αναφορά σε μια ακολουθία καταστάσεων blockchain που παράγονται από συναλλαγές όπως αποφασίστηκε από την αξιόπιστη υπηρεσία παραγγελιών. Για ασφάλεια έως τις επανεκκινήσεις, οποιοδήποτε σύνολο κακόβουλων ομότιμων χρηστών που αλληλεπιδρούν με SGX TEEs που φιλοξενούν έναν αλυσιδωτό κώδικα CC που αναπτύσσεται στο Fabric δεν πρέπει να μπορεί να συνάγει περισσότερο από αυτό που δίνεται από οποιαδήποτε συναλλαγή του CC που έχει επικαλεστεί σε μία από αυτές τις καταστάσεις. Το επιχείρημα προχωρά σε

τρία βήματα. Αρχικά, κάθε ενημέρωση κατάστασης (με τη μορφή ενός σετ γραφής) που παράγεται από ένα θύλακα αλυσιδωτού κώδικα με δημόσιο κλειδί PK_{CC} και είναι αποδεκτή από ένα θύλακα αρχείου στην κατάσταση του ομότιμου του χρήστη προέρχεται από ένα θύλακα του οποίου η έκθεση βεβαίωσης αποθηκεύεται στο αρχείο με δημόσιο κλειδί PK_{CC}. Επιπλέον, κάθε έξοδος συναλλαγής παράγεται από ένα θύλακα αλυσιδωτού κώδικα, για τον οποίο ένας σωστός πελάτης έχει πιστοποιήσει με επιτυχία την έξοδο σε ένα θύλακα με κλειδί PK_{CC}. Αυτό προκύπτει από τις λειτουργίες του μητρώου θύλακα και της κλάσης επικύρωσης συναλλαγής θύλακα. Συγκεκριμένα, το μητρώο θύλακα εκτελεί απομακρυσμένη βεβαίωση με το θύλακα αλυσιδωτού κώδικα και δημιουργεί έτσι την έκθεση βεβαίωσης που αποθηκεύει στο αρχείο. Αυτό πείθει τους πελάτες και τους ομότιμους χρήστες ότι ο θύλακας αλυσιδωτού κώδικα κωδικοποιήθηκε με τον αλυσιδωτό κωδικό που αντιπροσωπεύεται από τη τιμή mrenclaveCC στο αρχείο. Οι σωστοί πελάτες και οι ομότιμοι χρήστες αποκτούν την κατάστασή τους με τη μορφή της ακολουθίας μπλοκ με ενημερώσεις από το Ο και μπορούν να επαληθεύσουν την ακεραιότητα των ενημερώσεων κατάστασης που υπογράφει το PK_{CC}.

Σε οποιουσδήποτε ομότιμους, οι καταχωρήσεις κατάστασης αρχείου που λαμβάνονται από τον αλυσιδωτό κώδικα CC μέσα σε ένα θύλακα αντιπροσωπεύουν την κατάσταση blockchain μετά την εκτέλεση ενός προθέματος της ακολουθίας έγκυρων ενημερώσεων κατάστασης που εξάγονται από το Ο. Σημειώνεται ότι ένας κακόβουλος ομότιμος χρήστης μπορεί να επαναφέρει το θύλακα αρχείου κατά βούληση σε μια από τις σφραγισμένες και επίμονα αποθηκευμένες καταστάσεις που παράγει ο θύλακας. Λόγω των ελέγχων VSCC και της μονότονα αυξανόμενης αλληλουχίας αριθμών μπλοκ που περιμένει ο θύλακα αρχείου από το Ο, η κατάσταση blockchain που αντιπροσωπεύεται στο θύλακα αρχείου προκύπτει πάντα από την εκτέλεση της ακολουθίας συναλλαγών που καθορίζεται από το Ο και θεωρείται έγκυρη από το VSCC και τις πολιτικές επικύρωσης. Όταν ο αλυσιδωτός κώδικας στο εσωτερικό του θύλακα αλυσιδωτού κώδικα αποκτά πρόσβαση στη κατάσταση στο KVS, ο αμοιβαίος έλεγχος ταυτότητας μεταξύ του αρχείου και του θύλακα αλυσιδωτού κωδικού και ο μηχανισμός επαλήθευσης κατάστασης εξασφαλίζουν ότι οι καταχωρήσεις κατάστασης που λαμβάνονται από το CC είναι σωστές ανάλογα με την κατάσταση του θύλακα αρχείου. Δεδομένου ότι ο θύλακας αρχείου διατηρεί την κατάσταση μετά την εκτέλεση ενός προθέματος της ακολουθίας συναλλαγών από το Ο, ακολουθεί η παραπάνω δήλωση.

Κάθε κατάσταση που διατηρείται από έναν αλυσιδωτό κώδικα εντός ενός θύλακα

παραμένει εμπιστευτική μέχρι αυτού που αποκαλύπτεται με την εκτέλεση συναλλαγών του αλυσιδωτού κώδικα, που επικαλείται σε ένα πρόθεμα της πλήρους ακολουθίας των έγκυρων ενημερώσεων κατάστασης που εξάγονται από τον Ο. Αυτό συμβαίνει επειδή η λογική εκτέλεσης των θυλάκων και τα δεδομένα προστατεύονται εντός του TEE. Τα περιεχόμενα του θύλακα αρχείου είναι σφραγισμένα πριν καταγραφούν σε συνεχή αποθήκευση, επομένως δεν μπορούν να μεταβληθούν από κακόβουλο ομότιμο χρήστη χωρίς να εντοπιστούν. Η κατάσταση του ίδιου του θύλακα αλυσιδωτού κώδικα παραμένει αμετάβλητη μετά την αρχικοποίηση και αποθηκεύεται από τον ομότιμο χρήστη. Ωστόσο, όλοι οι σωστοί ομότιμοι χρήστες επαληθεύουν ότι αλληλεπιδρούν μόνο με θύλακες αλυσιδωτού κώδικα καταχωρημένους στον ίδιο το αρχείο. Ο θύλακας αρχείου μπορεί επίσης να περιέχει ένα κλειδί κρυπτογράφησης για την προστασία των δεδομένων στο αρχείο μέσω της βιβλιοθήκης αλυσιδωτού κώδικα, η οποία χειρίζεται την κρυπτογράφηση και την αποκρυπτογράφηση κατάστασης με διαφάνεια.

Από τον συγκριτικό πίνακα του Παραρτήματος φαίνεται ότι οι επικινδυνότερες επιθέσεις στο Hyperledger Fabric, είναι αυτές που μπορούν να θέσουν σε κίνδυνο ολόκληρο το σύστημα, με την επίθεση Docker TOCTOU Bug να συγκαταλέγεται στις επικινδυνότερες. Ακολουθούν οι επιθέσεις που θέτουν σε κίνδυνο τη λειτουργία του δικτύου, όπως οι επιθέσεις Κακόβουλων Clients και οι επιθέσεις στο πρωτόκολλο CFT και στο Gossip. Στη συνέχεια ακολουθούν οι επιθέσεις σε κόμβους του δικτύου, όπως η επίθεση Eclipse, η επίθεση διπλών εξόδων και η επίθεση σαμποταζ. Στη συνέχεια, στις επιθέσεις που μπορούν να βλάψουν τους ίδιους τους χρήστες ανήκουν οι επιθέσεις Μαύρης Λίστας, η Μη Έγκυρη Επίθεση Ταυτότητας, η Διεθνείς Fork Attacks, η Επίθεση Αναδιάταξης Συναλλαγών, η επίθεση συμπεγνίας και οι Επιθέσεις Διεπαφής. Στις επιθέσεις που μπορούν να μειώσουν την απόδοση του συστήματος ανήκουν οι Επιθέσεις Μεγέθους Block, η Επίθεση Batch Time και οι επιθέσεις στο πρωτόκολλο BFT και PoW. Τέλος, οι επιθέσεις που γίνονται με σκοπό να αποφέρουν κέρδος σε ένα συγκεκριμένο ή σε συγκεκριμένους χρήστες ανήκει η Επίθεση Sybil.

Η συγκεκριμένη εργασία μελέτησε τις επιθέσεις και τις ευπάθειες του Hyperledger Fabric, μέσω μελετών της διεθνούς βιβλιογραφίας. Μελλοντικά, θα μπορούσαν οι επιθέσεις που περιγράφηκαν στην εργασία να μελετηθούν και σε πρακτικό επίπεδο, για την εξαγωγή πρωτογενών αποτελεσμάτων.

Βιβλιογραφία

[01] Algesheimer, J., Cachin, C., Camenisch, J., & Karjoth, G. (2000, May). Cryptographic security for mobile code. In *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001* (pp. 2-11). IEEE.

[02] Alkhalifah, A., Ng, A., Kayes, A. S. M., Chowdhury, J., Alazab, M., & Watters, P. (2019). A taxonomy of blockchain threats and vulnerabilities.

[03] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., Cocco, S. & Yellick, J. (2018). "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference,* EuroSys 2018, Porto, Portugal, April 23-26, 2018, pp. 30:1–30: 15.

[04] Apostolaki, M., Zohar, A., & Vanbever, L. (2017, May). Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 375-392). IEEE.

[05] Arnautov, S., Trach, B., Gregor, F., Knauth, T., Martin, A., Priebe, C., ... & Goltzsche, D. (2016). {SCONE}: Secure Linux Containers with Intel {SGX}. In *12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16)* (pp. 689-703).

[06] Ateniese, G., Faonio, A., Magri, B., & De Medeiros, B. (2014, June). Certified bitcoins. In *International Conference on Applied Cryptography and Network Security* (pp. 80-96). Springer, Cham.

[07] Atzei, N., Bartoletti, M., & Cimoli, T. (2017, April). A survey of attacks on ethereum smart contracts (sok). In *International conference on principles of security and trust* (pp. 164-186). Springer, Berlin, Heidelberg.

[08] Avan-Nomayo, O. 2019. *Iran developing national blockchain platform on hyperledger fabric.* https://cointelegraph.com/news/iran-developing-nationalblockchain-platform-on-ibm-hyperledger-fabric

[09] Awuson-David, K., Al-Hadhrami, T., Funminiyi, O., & Lotfi, A. (2019). Using Hyperledger Fabric Blockchain to Maintain the Integrity of Digital Evidence in a Containerised Cloud Ecosystem. In International Conference of Reliable Information and Communication Technology (pp. 839-848). Springer, Cham.

[10] Bahack, L. (2013). Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft). *arXiv preprint arXiv:1312.7013*.

[11] Barger, Y., Manevich, B., Mandler, V., Bortnikov, G., Laventman & Chockler, G. 2017. "Scalable communication middleware for permissioned distributed ledgers," in *Proceedings of the 10th ACM International Systems and Storage Conference. ACM,* p. 23.

[12] Benhamouda, F., Halevi, S., & Halevi, T. (2019). Supporting private data on hyperledger fabric with secure multiparty computation. *IBM Journal of Research and Development*, *63*(2/3), 3-1

[13] Bonneau, J., Felten, E. W., Goldfeder, S., Kroll, J. A., & Narayanan, A. (2016). Why buy when you can rent? bribery attacks on bitcoin consensus.

[14] Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014, March). Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security* (pp. 157-175). Springer, Berlin, Heidelberg.

[15] Brandenburger, M., Cachin, C., Lorenz, M., & Kapitza, R. (2017, June). Rollback and forking detection for trusted execution environments using lightweight collective memory. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 157-168). IEEE.

[16] Buterin V. et al. 2014. *A next-generation smart contract and decentralized application platform.*

[17] Castillo, M.D. The dao attacked: Code issue leads to $60 million ether theft, http://www. coindesk. com/dao-attacked-code-issue-leads-60-million-ether-theft, 2019-08-11.

[18] Charron-Bost, B., Pedone, F. & Schiper, A. "Replication," *LNCS, vol. 5959*, pp. 19–40, 2010.

[19] Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018, August). Blockchain as a notarization service for data sharing with personal data store. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1330-1335). IEEE.

[20] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416-3452.

[21] Croman, K., Decker, I., Eyal, A., Gencer, A., Juels, A., Kosba, A., Miller, P. Saxena, E., Shi, E. G. 2016, "On scaling decentralized blockchains," in *International Conference on Financial Cryptography and Data Security.* Springer, pp. 106–125.

[22] Dabholkar, A., & Saraswat, V. (2019, November). Ripping the Fabric: Attacks and Mitigations on Hyperledger Fabric. In *International Conference on Applications and Techniques in Information Security* (pp. 300-311). Springer, Singapore.

[23] Dannen, C. (2017). *Introducing Ethereum and Solidity* (Vol. 1). Berkeley: Apress.

[24] del Castillo, M. 2019. *Blockchain 50: billion dollar babies.* https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/#39a73cc657cc

[25] Demers, A., Greene, C., Hauser, W., Irish, J., Larson, S., Shenker, H. Sturgis, Swinehart, D. & Terry, D. 1987. "Epidemic algorithms for replicated database maintenance," in *Proceedings of the sixth annual ACM Symposium on Principles of distributed computing.* ACM, pp. 1–12.

[26] Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., & Hierons, R. (2018, March). Smart contracts vulnerabilities: a call for blockchain software engineering?. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (pp. 19-25). IEEE.

[27] Eugster, P., Guerraoui, S., Handurukande, P. Kouznetsov & Kermarrec, A. 2003. "Lightweight probabilistic broadcast," *ACM Transactions on Computer Systems (TOCS), vol. 21*, no. 4, pp. 341–374.

[28] Gauravaram, P., Kelsey, J., Knudsen, L. R., & Thomsen, S. S. (2010). On hash functions using checksums. *International Journal of Information Security*, *9*(2), 137-151.

[29] Giechaskiel, I., Cremers, C., & Rasmussen, K. B. (2016, September). On bitcoin security in the presence of broken cryptographic primitives. In *European Symposium on Research in Computer Security* (pp. 201-222). Springer, Cham.

[30] Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM (JACM)*, *38*(3), 690-728.

[31] Goltzsche, D., Wulf, C., Muthukumaran, D., Rieck, K., Pietzuch, P., & Kapitza, R. (2017, April). Trustjs: Trusted client-side execution of javascript. In *Proceedings of the 10th European Workshop on Systems Security* (pp. 1-6).IBM. 2017. Secure Service Container User's Guide SC28-6971-01. (2017). https://www-

01.ibm.com/support/docview.wss?uid=isg2bb79df265313634d85258088005188e3&aid=1.

[32] Hajdu, Á., & Jovanović, D. (2019). solc-verify: A modular verifier for Solidity smart contracts. *arXiv preprint arXiv:1907.04262*.

[33] Hopcroft J. & Karp, R. 1973. "An nˆ5/2 algorithm for maximum matchings in bipartite graphs," *SIAM Journal on computing*, *vol. 2*, no. 4, pp. 225–231.

[34] Intel. 2018. Intel Software Guard Extensions (Intel SGX) Developer Guide. (2018). https://01.org/intel-software-guard-extensions/documentation/intel-sgx-developer-guide.

[35] Kfir, S., Rooz, Y., Saraniecki, E. 2014. *Digital asset*. https://digitalasset.com/

[36] Kwon, Y., Kim, D., Son, Y., Vasserman, E., & Kim, Y. (2017, October). Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 195-209).

[37] Li, Z., Lu, S., Myagmar, S., Zhou, Y. 2006. CP-Miner: finding copy-paste and related bugs in large-scale software code. IEEE Trans. *Softw. Eng. 32*(3), 176–192

[38] Luu, L.; Chu, D.H.; Olickel, H.; Saxena, P.; Hobor, A. Making Smart Contracts Smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; ACM: New York, NY, USA, 2016; CCS '16, pp. 254–269. doi:10.1145/2976749.29783

[39] Mearian, L. (2017). What is blockchain? The most disruptive tech in decades. *Computerworld*, 1-8.

[40] Mechkaroska, D., Dimitrova, V., & Popovska-Mitrovikj, A. (2018, November). Analysis of the possibilities for improvement of BlockChain technology. In *2018 26th Telecommunications Forum (TELFOR)* (pp. 1-4). IEEE.

[41] Microsoft. 2017. The Coco Framework. (2017). Whitepaper, https://github.com/Azure/coco-framework.

[42] Nakamoto, S. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*.

[43] Natarajan, H., Krause, S. K., & Gradstein, H. L. (2019). Distributed Ledger Technology (DLT) and blockchain. FinTech note; no. 1. Washington, DC: World Bank Group.

[44] O'Rourke, M. (2018). Hackers hijack computers to mine cryptocurrency. *Risk Management*, *65*(27), 692.

[45] Pollari, I.; Ruddenklau, A. The pulse of FinTech 2018, Biannual global analysis of investment in FinTech, https://assets.kpmg/content/dam/kpmg/au/pdf/2018/pulse-of-fintech-h1-2018.pdf, 2019-08-11.

[46] Potter, J. 2018. *The unfortunate rise of permissioned blockchains* https://blog.xtrabytes.global/technology/the-unfortunate-rise-of-permission-blockchains/

[47] Rapier, G. (2017). From Yelp reviews to mango shipments: IBM's CEO on how blockchain will change the world. *Business Insider*, *21*, 2017.

[48] Riedesel, S., Hakimian, P., Buyens, K., Biehn, T. 2018. *Tineola: taking a bite out of enterprise blockchain* https://github.com/tineola/tineola/raw/master/docs/TineolaWhitepaper.pdfSanders , C.: SSL stripping. http://techgenix.com/understanding-man-in-themiddle-attacks-arp-part4/

[49] Rosenfeld, M. (2011). Analysis of bitcoin pooled mining reward systems. *arXiv preprint arXiv:1112.4980*.

[50] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the attack surface of blockchain: A systematic overview. *arXiv preprint arXiv:1904.03487*.

[51] Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016, February). Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 515-532). Springer, Berlin, Heidelberg.

[52] Sarai, A. 2019. *Bugzilla bug report: CVE-2018-15664.* https://bugzilla.redhat.com/showbug.cgi?id=1714722

[53] Schneider, F. “Implementing fault-tolerant services using the state machine approach: A tutorial,” *ACM Computing Surveys (CSUR), vol. 22, no. 4*, pp. 299–319, 1990.

[54] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2019). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*.

[55] Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E., & Alexandrov, Y. (2018, May). Smartcheck: Static analysis of ethereum smart contracts. In *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain* (pp. 9-16).

[56] Vukoli´c, M. 2015. “The quest for scalable blockchain fabric: Proof - of work vs. bft replication,” in *International Workshop on Open Problems in Network Security.* Springer, pp. 112–125.

[57] Wan, Z., Lo, D., Xia, X., & Cai, L. (2017, May). Bug characteristics in blockchain systems: a large-scale empirical study. In *2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR)* (pp. 413-424). IEEE.

[58] Wei, J., Pu, C. 2005. *TOCTTOU vulnerabilities in UNIX-style file systems: an anatomical study.*

[59] Xu, J. J. (2016). Are blockchains immune to all malicious attacks?. *Financial Innovation*, *2*(1), 1-9.

[60] Yaga, D.; Mell, P.; Roby, N.; Scarfone (2018). K. NISTIR 8202 Blockchain Technology Overview. Retrieved from National Institute of Standards and Technology, US Department of Commerce 2018.

[61] Yao, A. C. (1982, November). Protocols for secure computations. In *23rd annual symposium on foundations of computer science (sfcs 1982)* (pp. 160-164). IEEE.

[62] Zyskind, G., Nathan, O., & Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*.

Παράρτημα – Συγκριτικός Πίνακας Επιθέσεων στο Hyperledger Fabric

Είδος Επίθεσης	Τίτλος Επίθεσης	Περιγραφή	Επικινδυνότητα
Συμβιβαζόμενος MSP	Επίθεση Sybil	Ο εισβολέας ανατρέπει το σύστημα φήμης ενός δικτύου, δημιουργώντας ένα μεγάλο αριθμό ψευδώνυμων ταυτοτήτων και τις χρησιμοποιεί για να αποκτήσει δυσανάλογα μεγάλη επιρροή.	Αποκόμιση κέρδους για συγκεκριμένο χρήστη
Συμβιβαζόμενος MSP	Μη Έγκυρη Επίθεση Ταυτότητας	Δημιουργία δόλιων πιστοποιητικών για γνήσιους ομότιμους / ανταγωνιστικούς οργανισμούς, ακύρωση των υφιστάμενων αναγνωριστικών των γνήσιων ομότιμων/ ανταγωνιστικών οργανισμών	Προσβολή χρηστών του δικτύου
Συμβιβαζόμενος MSP	Επιθέσεις Boycott	Ο επιτιθέμενος αποκτά τον έλεγχο του MSP-admin M, τροποποιεί υπάρχουσες πολιτικές και δεν παρέχει πιστοποιητικά σε υπάρχοντα μέλη του δικτύου	Προσβολή χρηστών του δικτύου
Συμβιβαζόμενος MSP	Επιθέσεις Μαύρης Λίστας	Ο επιτιθέμενος αποκτά πρόσβαση στο MSP και προσθέτει πιστοποιητικά υπάρχοντων χρηστών στη Λίστα Ανάκλησης Πιστοποιητικών (CRL)	Προσβολή χρηστών του δικτύου
Υπηρεσία Κακόβουλης Παραγγελίας	Επιθέσεις Σαμποτάζ	Κακόβουλο λογισμικό δεν επιτρέπει την ενοποίηση των μπλοκ από συγκεκριμένους κόμβους του δικτύου	Προσβολή κόμβων του δικτύου
Υπηρεσία Κακόβουλης Παραγγελίας	Διεθνείς Fork Attacks	Κακόβουλο λογισμικό στέλνει πλαστά block, με τα μέλη που τα παραλαμβάνουν να απορρίπτουν block από άλλους χρήστες	Προσβολή χρηστών του δικτύου
Υπηρεσία Κακόβουλης Παραγγελίας	Επιθέσεις Μεγέθους Block	Κακόβουλο λογισμικό αλλάζει την τιμή του μεγέθους του config-block σε μια εξαιρετικά μικρή ή εξαιρετικά μεγάλη τιμή, μειώνοντας την αποδοτικότητα του δικτύου	Προσβολή αποδοτικότητας του δικτύου

Υπηρεσία Κακόβουλης Παραγγελίας	Επίθεση Batch Time	Κακόβουλο λογισμικό μειώνει το χρονικό όριο στο Batch Timeout για να βλάψει τη διακίνηση του δικτύου	Προσβολή διακίνησης του δικτύου
Υπηρεσία Κακόβουλης Παραγγελίας	Επίθεση Αναδιάταξης Συναλλαγών	Κακόβουλο λογισμικό αναδιατάσσει την προτεραιότητα των block που έρχονται από διαφορετικούς χρήστες με αποτέλεσμα την λανθασμένη καταχώρηση και απόρυψη block στην αλυσίδα.	Προσβολή χρηστών του δικτύου
Κακόβουλοι Επικυρωμένοι Κόμβοι	Επίθεση Διπλών Εξόδων	Κακόβουλοι επικυρωμένοι κόμβοι θα μπορούσαν να επιτρέψουν τη διπλή δαπάνη και να την προσαρτήσουν στο ledger, καταστρέφοντας έτσι την ακεραιότητά τους	Προσβολή κόμβων του δικτύου
Κακόβουλοι Επικυρωμένοι Κόμβοι	Επίθεση DDos	Ο εισβολέας καθιστά μια κοινή υπηρεσία μη διαθέσιμη στους χρήστες κάνοντας κακόβουλα ερωτήματα από πολλές μηχανές, υπερφορτώνοντας τον διακομιστή χωρίς να μπορεί να τα επεξεργαστεί	Προσβολή συγκεκριμένης υπηρεσίας του δικτύου
Εξωτερικές Επιθέσεις	Συμπαιγνία	Συμμετέχοντες φορείς στο δίκτυο συνεργάζονται για να ξεκινήσουν μια επίθεση ιστορικού που τους επιτρέπει να ξαναγράψουν το ledger προς όφελός τους.	Προσβολή χρηστών του δικτύου
Εξωτερικές Επιθέσεις	Επιθέσεις Διεπαφής	Μη επιμελώς κατασκευασμένες διεπαφές μπορούν να διαρρεύσουν δεδομένα κατά τις συναλλαγές του δικτύου	Προσβολή χρηστών του δικτύου
Εξωτερικές Επιθέσεις	Κακόβουλοι Clients	Κακόβουλος χρήστης στέλνει μια σταθερή ροή από μη εκκρεμείς συναλλαγές στο κακόβουλο λογισμικό που τις ενσωματώνει στην αλυσίδα μολύνοντας τον αλυσιδωτό κώδικα και αυξάνοντας το μέγεθος του	Προσβολή λειτουργίας του δικτύου
Επιθέσεις Βάσει Πρωτοκόλλου	Πρωτόκολλο CFT	Ευάλωτα στους Βυζαντινούς κόμβους, μπορούν να αποτρέψουν αποτελεσματικά το δίκτυο από την επίτευξη συναίνεσης	Προσβολή λειτουργίας του δικτύου
Επιθέσεις Βάσει Πρωτοκόλλου	Πρωτόκολλο BFT	Καθώς ο αριθμός των κόμβων αυξάνεται, η απόδοση μειώνεται δραματικά	Προσβολή απόδοσης του δικτύου

Επιθέσεις Βάσει Πρωτοκόλλου	Πρωτόκολλο PoW	Δεν εγγυάται το αμετάκλητο της τελικής συναίνεσης, έχει πολύ μεγάλη κατανάλωση ενέργειας και έχει πολύ χαμηλή απόδοση	Προσβολή απόδοσης του δικτύου
Επιθέσεις Βάσει Πρωτοκόλλου	Πρωτόκολλο Gossip	Κίνδυνος μη μετάδοσης των μπλοκ σε αρκετούς ομότιμους, αλλά μόνο στους ομότιμους του οργανισμού	Προσβολή λειτουργίας του δικτύου
Επιθέσεις Βάσει Πρωτοκόλλου	Επίθεση Eclipse	Έλεγχος όλων των εξερχόμενων συνδέσεων του κόμβου στόχου με αποτέλεσμα την απομόνωσή του.	Προσβολή κόμβου του δικτύου
Εκτέλεση / Αρχιτεκτονικές Επιθέσεις	Docker TOCTOU Bug	Θα μπορούσε να δώσει πρόσβαση εισερχόμενης ανάγνωσης / εγγραφής ως root στο σύστημα κεντρικού υπολογιστή. Ένας εισβολέας μπορεί να αντιγράψει προστατευμένα αρχεία ιδιωτικού κλειδιού καταστρέφοντας ολόκληρο το σύστημα	Προσβολή ολόκληρου του συστήματος
Εκτέλεση / Αρχιτεκτονικές Επιθέσεις	Ευπάθεια CouchDB	Ένας εισβολέας μπορεί να τροποποιήσει τη βάση δεδομένων χωρίς να επικαλεστεί αλυσιδωτό κώδικα, μπορεί να αλλάξει ανώνυμα την εικόνα του αλυσιδωτού κώδικα για τον ομότιμο	Προσβολή χρηστών του δικτύου