ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΣΥΓΚΡΙΤΙΚΗ ΜΕΛΕΤΗ ΕΠΙΘΕΣΕΩΝ ΣΕ BLOCKCHAIN

Διπλωματική Εργασία

του

Ταξιάρχου Αναστασίου

Θεσσαλονίκη, Δεκέμβριος 2021

ΣΥΓΚΡΙΤΙΚΗ ΜΕΛΕΤΗ ΕΠΙΘΕΣΕΩΝ ΣΕ BLOCKCHAIN

Ταξιάρχου Αναστασίου

Πτυχίο Μαθηματικών, Πανεπιστήμιο Ιωαννίνων, 2018

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Φουληράς Παναγιώτης

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

ΦΟΥΛΗΡΑΣ ΠΑΝΑΓΙΩΤΗΣ	ΜΑΥΡΙΔΗΣ ΙΩΑΝΝΗΣ	MARIE G. KHAIR
.....	.....	.....

Ταξιάρχου Αναστάσιος

Περίληψη

Κατά την διάρκεια της περασμένης δεκαετίας, η τεχνολογία Blockchain και ο κατανεμημένος της “peer-to-peer” σχεδιασμός είχαν προσελκύσει διάφορους τομείς πέρα από την χρηματοπιστωτική αγορά, όπως την υγειονομική περίθαλψη, την ασφάλεια στον κυβερνοχώρο, την εφοδιαστική αλυσίδα και το διαδίκτυο των πραγμάτων. Λόγω των πλεονεκτημάτων που προσφέρει η κρυπτογραφία που εφαρμόζεται σε blockchain στο επίπεδο ασφάλειας, όπως είναι η χρήση ψηφιακή υπογραφής, η ακεραιότητα, η αμεταβλητότητα και ο κατακερματισμός δεδομένων θεωρείται από πολλούς αναλυτές ότι θα αποτελέσει την πιο ευρέως χρησιμοποιούμενη τεχνολογία. Ο λόγος αυτής της πρόβλεψης είναι ότι η παραβίαση της δομής του blockchain είναι εξαιρετικά δύσκολη. Παρά όμως τα μεγάλα οφέλη που αποφέρει η τεχνολογία blockchain, παρουσιάζει επίσης μερικά μειονεκτήματα, όπως περιορισμοί στην επεκτασιμότητα και ανοχή σφαλμάτων. Ως εκ τούτου, υπάρχουν αρκετές επιθέσεις οι οποίες μπορούν να εξαπολυθούν εκμεταλλευόμενοι προβλήματα της τεχνολογίας. Αυτή η μελέτη συνοψίζει μια ολοκληρωμένη έρευνα των επιθέσεων blockchain. Επιπλέον κατηγοριοποιεί τις επιθέσεις αυτές έχοντας ως συγκριτικούς άξονες, κριτήρια με βάση τον τύπο επίθεσης που επηρεάζει τον ίδιο παράγοντα σε ένα περιβάλλον blockchain, τις επιθέσεις σε σχέση με τα διάφορα επίπεδα αφαίρεσης της τεχνολογίας και τέλος τις επιθέσεις με βάση τα μοντέλα συναίνεσης, όσον αφορά τις πλατφόρμες blockchain 1.0 και blockchain 2.0. Αυτή η έρευνα, θα μπορούσε να βοηθήσει την τεχνολογική κοινότητα που ενδιαφέρεται να υιοθετήσει την τεχνολογία blockchain με οποιαδήποτε προοπτική, όχι μόνο ενημερώνοντας για τις υπάρχουσες απειλές αλλά δίνοντας και κάποιες προτεινόμενες λύσεις για την αποφυγή ορισμένων από τις πιο σημαντικές ευπάθειες της τεχνολογίας

Λέξεις Κλειδιά: Blockchain System, Attack, Scalability, Threat Categorization, Bitcoin, Smart contract, Ledger

Abstract

In the past decade, Blockchain technology and its distributed peer-to-peer design have attracted various areas beyond the financial market, namely the healthcare, government, cybersecurity, supply chain, and internet of things. Due to the advantages lying within cryptography, blockchain offers a diverse variety of elements such as digital signature, integrity, immutability and hashing. Thus, for many technological analysts, it is considered that it will be the most widely used technology, as violating the blockchain structure is extremely difficult. Despite of the great benefits blockchain technology yields, it also poses a few disadvantages such as limitations in scalability, and fault tolerance. Therefore, there are several attacks that can be launched exploiting blockchain problems. This thesis encapsulates a comprehensive survey of the Blockchain attacks. More precisely, the study developed a taxonomy that categorizes the security threats and attacks based on the type of attack that affect the same factor in the blockchain environment, the abstract layers and the consensus mechanisms utilizing the blockchain 1.0 and blockchain 2.0 platforms. This research could assist the technology community that is interested to adopt blockchain technology in any aspect, not only by informing about the existing threats but also by giving some proposed solutions to avoid some of the most essential blockchain vulnerabilities.

Keywords: Blockchain System, Attack, Scalability, Threat Categorization, Bitcoin, Smart contract, Ledger

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο των σπουδών μου για την απόκτηση μεταπτυχιακού τίτλου σπουδών στο Τμήμα Εφαρμοσμένης Πληροφορικής, της σχολής Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας. Το θέμα της παρούσας εργασίας είναι «Συγκριτική μελέτη επιθέσεων σε Blockchain»

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της εργασίας, κύριο Παναγιώτη Φουληρά που με βοήθησε τόσο στην επιλογή του θέματος της εργασίας όσο και στην διεκπεραίωση της. Τον ευχαριστώ θερμά για την υποστήριξη του, την άμεση ανταπόκριση και τις συμβουλές που μου έδωσε.

Τέλος θα αναφερθώ και θα ευχαριστήσω την οικογένεια μου για την στήριξη που μου παρείχε, αλλά και τους φίλους για την υπομονή και την κατανόηση που έδειξαν.

Περιεχόμενα

Κατάλογος Εικόνων

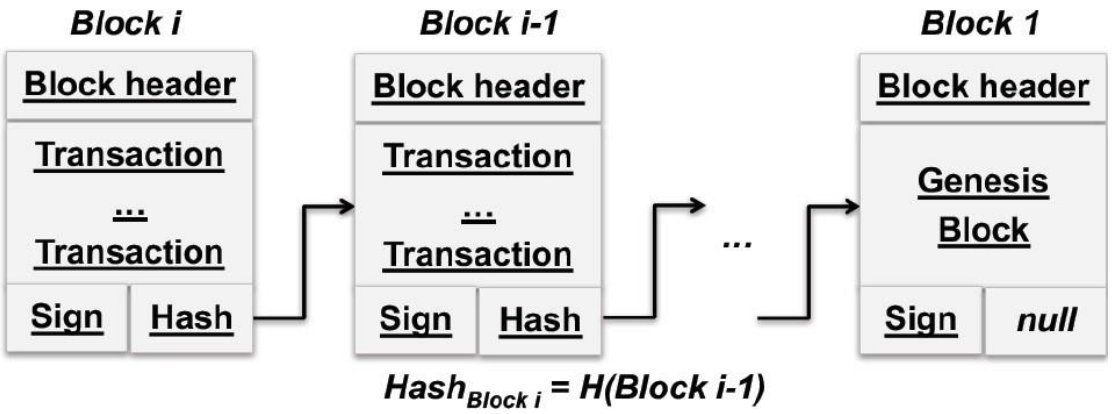
Κατάλογος Πινάκων

1 Εισαγωγή

Με την εφεύρεση του bitcoin το 2009, όπου αποτελεί και την αρχική εφαρμογή του blockchain ο κόσμος έχει εισαχθεί σε μια νέα ιδέα που είναι έχει φέρει την επανάσταση σε ολόκληρη την κοινωνία. Πρόκειται για ένα γεγονός που προβλέπεται να επηρεάσει κάθε κλάδο, συμπεριλαμβανομένων ενδεικτικά τον τομέα της οικονομίας, τον κυβερνητικό παράγοντα, των μέσων ενημέρωσης, της υγείας, κυβερνοασφάλειας κ.α. Επιπλέον με την εισαγωγή των έξυπνων συμβολαίων, το blockchain περνάει στο επόμενο στάδιο των δημόσιων blockchain (blockchain 1.0, blockchain 2.0). Ένα έξυπνο συμβόλαιο αποτελεί ένα υπολογιστικό πρόγραμμα που ελέγχει άμεσα τη μεταφορά περιουσιακών στοιχείων μεταξύ διαφορετικών μερών υπό ειδικές συνθήκες. Το Ethereum αποτελεί ένα έξυπνο συμβόλαιο και είναι μια αποκεντρωμένη εφαρμογή η οποία αξιοποιεί το blockchain προκειμένου να εκτελέσει αυτόματες διαδικασίες (Dannen, 2017). Η τάση αυτή σχετίζεται με το γεγονός ότι εφαρμογές οι οποίες για να εκτελεστούν χρειάζονταν μια έμπιστη κεντρική αρχή, μπορούν πλέον να λειτουργούν σε ένα αποκεντρωμένο περιβάλλον με αποτέλεσμα η αποθήκευση δεδομένων και η διαχείριση ψηφιακής πληροφορίας να μην χρειάζεται τον μηχανισμό ενός κεντρικού ελεγκτικού μηχανισμού. Ουσιαστικά, το blockchain αποτελεί μια μοιραζόμενη, κατανεμημένη βάση δεδομένων η οποία χρησιμοποιεί και διαχειρίζεται ένα καθορισμένο όγκο πληροφοριών ψηφιακής μορφής με ασφαλή και αμετάβλητο τρόπο. Μερικοί το περιγράφουν ως επανάσταση, ενώ μια άλλη σχολή σκέψης διατυπώνει ότι πρόκειται για μια εξέλιξη, όπου θα χρειαστούν πολλά χρόνια όμως για να υπάρχει μια ευρεία εφαρμογή της τεχνολογίας και την εκμετάλλευση των οφελών της. Η βασική καινοτομία όμως στο blockchain, ως αποκεντρωμένη και κατανεμημένη λύση διαχείρισης δεδομένων είναι ότι έχει αναθεωρήσει την έννοια της εμπιστοσύνης, ενσωματώνοντας την κρυπτογραφία με την εφαρμογή μοντέλων συναίνεσης παρέχοντας έτσι ασφάλεια, ανωνυμία και ακεραιότητα δεδομένων χωρίς την ανάγκη ενός τρίτου μέρους όπως έχει σημειωθεί.

Άρα λοιπόν, το blockchain αποτελεί μια κατανεμημένη δομή δεδομένων η οποία είναι μοιραζόμενη από όλα τα μέλη του δικτύου, στο οποίο έχουμε την ύπαρξη ενός “tamper-proof” ψηφιακού λογιστικού βιβλίου συναλλαγών (transactions). Οι συναλλαγές αυτές αποθηκεύονται στο κατανεμημένο λογιστικό αυτό βιβλίο (ledger) το οποίο αποτελείται από συνδεδεμένα μεταξύ τους μπλοκ. Η σύνδεση αυτή επιτυγχάνεται με την

εφαρμογή κρυπτογραφικών τεχνικών και συγκεκριμένα με την χρήση ψηφιακών υπογραφών μέσω της εφαρμογής κρυπτογραφίας δημοσίου κλειδιού. Με την έννοια αυτή, είναι εξαιρετικά δύσκολη η οποιαδήποτε επέμβαση σε κάποιο επικυρωμένο μπλοκ της αλυσίδας που είναι καταγεγραμμένο εντός του "ledger" και το οποίο διακρίνεται από τα χαρακτηριστικά του αμετάβλητου και διαφανούς. Πιο συγκεκριμένα οποιοδήποτε μέλος που συμμετέχει σε ένα blockchain δίκτυο κατέχει ένα αντίγραφο όλων των συναλλαγών των υπολοίπων, διασφαλίζοντας πλήρως έτσι την εμπιστοσύνη όλων των συναλλασσόμενων μερών αφού κάθε "transaction" ενός block της αλυσίδας βασίζεται πλήρως σε μια αλγοριθμική επιβεβαίωση που σχετίζεται με το αμέσως προηγούμενο του με αποτέλεσμα να ελέγχεται πλήρως οποιαδήποτε μεταβολή από κάθε συμμετέχων κόμβο στο δίκτυο (Reyna, Martín, Chen, Soler, & Díaz, 2018). Τα μπλοκ αυτά εμπεριέχουν ένα πλήθος έγκυρων συναλλαγών καθώς επίσης και το αποτέλεσμα της συνάρτησης κατακερματισμού (wining hash) του αμέσως προηγούμενου μπλοκ, δομώντας με αυτόν τον τρόπο την αλυσίδα (εικόνα 1). Να σημειωθεί ότι ως "wining hash" θεωρείται το αποτέλεσμα της συνάρτησης κατακερματισμού που είναι μικρότερο από μια συγκεκριμένη τιμή "difficulty" που έχει διαμορφωθεί εκείνη την στιγμή στο δίκτυο και αφορά τον πρώτο κόμβο που επιτυγχάνει σε αυτή την διαδικασία (Proof of Work), ο οποίος μάλιστα αποτελεί τον κόμβο που χαρακτηρίζεται ως "miner". Στην συνέχεια ακολουθεί έκδοση του νέου μπλοκ από τον "miner" και αφού επικυρωθεί η ισχύς του, μέσω ενός αντιγράφου που αποστέλλεται στους κόμβους του δικτύου, προστίθεται στην αλυσίδα (Christidis & Devetsikiotis, 2016). Εξαίρεση στην διάδοση της αναφοράς αυτής αποτελεί το λεγόμενο "genesis block". Κάθε κόμβος που έχει πρόσβαση στην συγκεκριμένη δομή σύνδεσης των block μπορεί να διαβάσει το "world state" των στοιχείων που ανταλλάσσονται εντός του δικτύου. Όσον αφορά την κρυπτογραφία που εφαρμόζεται, για την δημιουργίας της ψηφιακής υπογραφής χρειαζόμαστε αρχικά τον κατακερματισμό τον δεδομένων του μπλοκ μέσω της συνάρτησης κατακερματισμού . Έπειτα κρυπτογραφείται το "hash value" που έχει παραχθεί με χρήση του ιδιωτικού κλειδιού και έπειτα η επικύρωση της ψηφιακής υπογραφής γίνεται μέσω της αποκρυπτογράφησης με το αρχικό "hash value" όπου χρειάζεται τα δύο αυτά αποτελέσματα να συμπίπτουν.



Εικόνα 1:Τυπική απεικόνιση αλυσίδας μπλοκ

Οι πλατφόρμες που βασίζονται σε τεχνολογία blockchain είναι σχεδιασμένες είτε να εκτελούν απευθείας ηλεκτρονικές συναλλαγές όπως στην περίπτωση του bitcoin είτε να χρησιμοποιούνται ψηφιακά νομίσματα για οικονομικούς σκοπούς όπως συμβαίνει στην περίπτωση του Ethereum. Στο σημείο αυτό αξίζει να σημειωθεί ότι, η χρήση των ψηφιακών νομισμάτων στις δημόσιες πλατφόρμες blockchain αυξάνεται με ταχύτατο ρυθμό, ενώ μόνο η κεφαλαιοποίηση της αγοράς για την περίπτωση του bitcoin αυτή την στιγμή αξίζει περίπου τα 1100 δισεκατομμύρια δολάρια, ενώ μόλις 2 χρόνια πριν δεν ξεπερνούσε τα 200 δισεκατομμύρια δολάρια. Το γεγονός αυτό της εκθετικής αύξησης της αγοραστικής αξίας των κρυπτονομισμάτων αποτελεί αναπόφευκτα ένα σημαντικό λόγο για τους hackers να εκμεταλλευτούν τυχόν αδυναμίες στις υπάρχουσες πλατφόρμες, δημιουργώντας έτσι την ανάγκη στην ερευνητική κοινότητα να διαχειριστεί τους κινδύνους που προκύπτουν με σκοπό να ανακαλύψει πιθανά νέα κενά ασφαλείας, προβλέψεις σε επερχόμενες τάσεις ή προτάσεις για την αντιμετώπιση τους.

1.1 Πρόβλημα-Σημαντικότητα θέματος

Μερικά από τα υπάρχουσα περιστατικά-παραβιάσεις σχετικά με τις υπάρχουσες δημόσιες πλατφόρμες blockchain που έχουν καταγραφεί επηρεάζοντας αρνητικά την συγκεκριμένη τεχνολογία περιγράφονται παρακάτω.

Μια από τις μεγαλύτερες επιθέσεις στην ιστορία του bitcoin συνέβη στο Mt.Gox το μεγαλύτερο ανταλλακτήριο bitcoin (χρησιμοποιούνταν περισσότερο από το 70% του συνόλου των διαθέσιμων ανταλλακτηρίων bitcoin, όπου το αποτέλεσμα προσπαθειών εισβολής για ένα έτος κατέληξε στην απώλεια περίπου 850.000 bitcoin, ποσό αξίας άνω των 450 εκατομμυρίων δολαρίων τότε. Το 2011 hackers χρησιμοποίησαν κλεμμένα διαπιστευτήρια για την μεταφορά bitcoin, όπου πέρα από την απώλεια bitcoins καταφέρανε να τροποποιήσουν την τιμή του bitcoin σε μόλις ένα cent. Τα αποτελέσματα

αυτής της επίθεσης ήταν να υπάρχει ένας ρυθμιστικός έλεγχος στην βιομηχανία συμπεριλαμβανομένου του υπουργείου Εσωτερικής ασφάλειας των ΗΠΑ (Cheung, Roca, & Su, 2015). Έτσι το φιάσκο στο ανταλλακτήριο Mt.Gox είχε ως αποτέλεσμα μια σημαντική πτώση στην τιμή του bitcoin, ενώ χρειάστηκαν χρόνια για την βιομηχανία κρυπτογράφησης στο σύνολο της, ώστε να ανακάμψουν από την φήμη της ζημιάς που προέκυψε από την ζημιά. Στις αρχές του 2014 εντοπίστηκε κλοπή μεγαλύτερη των 850000 bitcoin. Ακόμη ένα ανταλλακτήριο με έδρα την Ιαπωνία, το Coincheck δέχθηκε επίθεση με μια απώλεια της τάξεως των 534 τον Ιανουάριο του 2018.

Σε ένα άλλο ανταλλακτήριο με το όνομα Bitfinex και με έδρα το Hong Kong είχαν σχεδόν κλαπεί btc αξίας 72 εκατομμυρίων δολαρίων, παρόλο που η Bitfinex εφάρμοσε τεχνολογία πολλαπλών υπογραφών μέσω της εταιρίας BitGo. Σχετικά με το "Nicehash", το οποίο αποτελεί μια αγορά ανταλλαγής με την έννοια της ενοικίασης εξορυκτικής ισχύς μεταξύ των ανθρακωρύχων, παραβιάστηκε το 2017, όπου οι χρήστες αντιμετώπισαν κλοπή κρυπτονομισμάτων από τα πορτοφόλια τους, η οποία ανήλθε περίπου στο συνολικό ποσό των 65 εκατομμυρίων δολαρίων. Επιπλέον τον Δεκέμβριο του 2017 πραγματοποιήθηκε DNS επίθεση στο ανταλλακτήριο Ether Delta με κλοπή που ανερχόταν στα 308 ETH, ενώ σε μια επίθεση τύπου Ransomware η οποία διήρκησε 8 μήνες την χρονιά 2013-2014 κατά την οποία μέσω ενός trojan στόχευε σε υπολογιστές με λειτουργικό Windows (Wikipedia, 2021). Ενεργοποιώντας το Trojan ακολουθούσε κρυπτογράφηση αρχείων τα οποία αποθηκεύονταν σε τοπικές μονάδες δικτύου μέσω εφαρμογής κρυπτογραφίας δημοσίου κλειδιού RSA, με το ιδιωτικό κλειδί όμως να αποθηκεύεται μόνο στους διακομιστές ελέγχου του μολυσμένου λογισμικού.

Μια άλλη σημαντική περίπτωση επίθεσης που έβλαψε το δημόσιο blockchain και συγκεκριμένα το Ethereum μέσω της έξυπνης σύμβασης DAO, συνέβη το 2016 ("The DAO Attacked: Code Issue Leads to $60 Million Ether Theft - CoinDesk," n.d.). Στην περίπτωση αυτή, ο εισβολέας εκμεταλλεύτηκε μια αναδρομική προσπάθεια κλήσεων, με αποτέλεσμα στην σύμβαση DAO να χαθούν περίπου 60 εκατομμύρια δολάρια. Αν και υπάρχουν μερικές μελέτες σχετικά με τα θέματα ασφαλείας blockchain, δεν έχουν μια συστηματική έρευνα των προβλημάτων συνολικά των δημόσιων blockchain.

1.2 Σκοπός – Στόχοι

Ο βασικός στόχος αυτής της μελέτης είναι να κάνει μια ανασκόπηση των υπαρχουσών ευπαθειών στο blockchain καθώς και πως οι υπάρχουσες ευπάθειες μπορούν να δημιουργήσουν κενά ασφαλείας σε ένα περιβάλλον, όπου εξ ’ορισμού ο βαθμός δυσκολίας ως προς την παραβίαση του είναι αρκετά μεγάλος, λόγω των ιδιαίτερων χαρακτηριστικών ασφαλείας που διαθέτει.

Για να κατανοήσουμε σημαντικά το πρόβλημα, θα πρέπει να αναλυθούν τα διάφορα στοιχεία που χαρακτηρίζουν το blockchain, κάποια βασικά χαρακτηριστικά που του προσδίδουν την ιδιαίτερη αξία ως τεχνολογία, τους διάφορους τύπους στους οποίους χωρίζεται, τα μοντέλα συναίνεσης που εφαρμόζονται, την αρχιτεκτονική του blockchain καθώς και τα επίπεδα στα οποία διαχωρίζεται. Επιπλέον θα αναλυθούν υπάρχουσες τεχνικές προκλήσεις ή περιορισμοί σε συστήματα blockchain, όπως περιορισμοί στην επεκτασιμότητα, η οποία μάλιστα έχει άμεση σχέση με την ασφάλεια και συγκεκριμένα με την δυνατότητα επίτευξης μιας επιτυχούς επίθεσης σε ένα blockchain σύστημα. Ο κύριος όμως σκοπός θα είναι η μελέτη διαφόρων επιθέσεων ασφαλείας οι οποίες θα ταξινομηθούν με βάση διαφορετικούς παράγοντες οι οποίοι μπορούν να βλάψουν την ομαλή λειτουργία ενός blockchain. Επιπλέον θα προταθούν ενδεικτικές λύσεις καθώς και προτάσεις ως προς την ασφάλεια ή τους περιορισμούς που αντιμετωπίζει η τεχνολογία. Τέλος θα πρέπει να σημειωθεί ότι η μελέτη αυτή θα εστιάσει στα δημόσια blockchain δηλαδή στα blockchain 1.0 (bitcoin) και blockchain 2.0 (Ethereum).

1.3 Βασική Ορολογία

- **Blockchain (αλυσίδα των μπλοκ):** Το αποκεντρωμένο δημόσιο καθολικό σύμφωνα με το οποίο λειτουργεί το bitcoin. Συγκεκριμένα, οποιαδήποτε συναλλαγή και λογαριασμός καταγράφεται σε αυτό. Επιπλέον χρησιμοποιείται για να παραπέμψει σε οποιαδήποτε επερχόμενη τεχνολογία χρησιμοποιεί ένα δημόσιο καθολικό για να παρακολουθεί τις ψηφιακές αξίες, δηλαδή «την ανάπτυξη της δικής τους τεχνολογίας αλυσίδας των μπλοκ.

- **Bitcoin:** Είναι η πρώτη εφαρμογή του blockchain και αποτελεί ένα αποκεντρωμένο σύστημα-δίκτυο “peer-to-peer”, στο οποίο χρησιμοποιούνται τα ψηφιακά νομίσματα bitcoin.

- **Block:** Οι συναλλαγές στην αλυσίδα των μπλοκ καθώς και άλλα δεδομένα εμπεριέχονται σε μπλοκ, τα οποία υπόκεινται την διαδικασία της επιβεβαίωσης ανά δέκα περίπου λεπτά. Το μέγεθος του γενικά ορίζεται 1 MB, αλλά χαρακτηρίζεται από μεταβλητότητα.
- **Εξόρυξη (Mining):** Η εξόρυξη είναι η διαδικασία προσθήκης συναλλαγών στο κατανεμημένο δημόσιο βιβλίο (ledger) ή αλλιώς blockchain.
- **Ανθρακωρύχος(Miner):**Αποτελεί ένα "actor" που συμμετέχει στην διαδικασία της επικύρωσης και επαλήθευσης συναλλαγών και την προσθήκη νέων μπλοκ και στην αλυσίδα(blockchain).
- **Έμπορος (Merchant):**Οποιοσδήποτε άνθρωπος ή επιχείρηση λαμβάνει ψηφιακό νόμισμα ως σύστημα πληρωμών.
- **Συναλλαγή (Exchange):** Ανταλλακτήρια κρυπτονομισμάτων είναι η επιχείρηση που παρέχει υπηρεσίες σε πελάτες για την ανταλλαγή ψηφιακών νομισμάτων με διαφορετικά περιουσιακά στοιχεία(άλλο κρυπτονόμισμα ή νόμισμα Fiat).
- **Αποκέντρωση:** Το γεγονός ότι ένα δίκτυο, υπηρεσία ή ιδιοκτησία εταιρείας μπορεί να διανεμηθεί χωρίς να υπάρχει κάποιο κεντρικό σημείο αποτυχίας.
- **Fork (διακλάδωση):** Η αντιγραφή κώδικα ανοιχτής πηγής και η διαφοροποίηση του. Στην περίπτωση των κρυπτονομισμάτων αφορά την χρονική στιγμή κατά την οποία οι εξ ορυκτές κακόβουλα ξεκινούν την εξόρυξη μιας πλαστής διαφορετικής από την αρχική αλυσίδα.
- **Hard Fork:** Αποτελεί μια αλλαγή των κανόνων που υπακούει το δίκτυο blockchain, με συνέπεια το λογισμικό που επικυρώνεται σύμφωνα με τους προγενέστερους κανόνες αναγνωρίζει ως μη έγκυρα τα μπλοκ που παράγονται σύμφωνα με τους νέους κανόνες. Ως εκ τούτου, απαιτείται αναβάθμιση για όλους τους κόμβους που εφαρμόζουν του νέους κανόνες.
- **Soft Fork**: Αποτελεί την προσθήκη ενός νέου κανόνα που δεν έρχεται σε σύγκρουση με τους παλαιότερους κανόνες. Το πιο χαρακτηριστικό παράδειγμα είναι το Segregated witness το οποίο προέκυψε από την διάσπαση bitcoin με bitcoin cash. Σε αυτή την περίπτωση οι παλιοί κόμβοι μπορούσαν ακόμη να επικυρώσουν συναλλαγές και νέα μπλοκ.
- **Hash (κατακερματισμός):** Αποτελεί ένα αλγόριθμο που λαμβάνει μια αυθαίρετη ποσότητα εισόδου δεδομένων και παράγει μια έξοδος κρυπτογραφημένου κειμένου, όπου θα είναι ένα τυχαίο αλφαριθμητικό 64 χαρακτήρων. Επιπλέον

αποτελεί μονάδα μέτρησης της ποσότητας της υπολογιστικής ισχύος που τίθεται στο δίκτυο.

- **Hashrate (ρυθμός κατακερματισμού):** Το σύνολο των κατακερματισμών που λαμβάνει χώρα στο δίκτυο. Ο συνολικός αριθμός των κατακερματισμών αντιπροσωπεύει τον αριθμό των υπολογιστικών εξισώσεων του δικτύου μπορεί να αναφερόμαστε στο bitcoin ή σε κάποιο άλλο κρυπτονόμισμα. Για παράδειγμα ρυθμός 1 /THs σημαίνει ότι το δίκτυο έχει την δυνατότητα ένα τρισεκατομμύριο υπολογισμούς ανά δευτερόλεπτο.
- **Δημόσιο κλειδί:** Στο bitcoin χρησιμοποιούμε κρυπτογραφία δημοσίου κλειδιού για να δημιουργήσουμε ένα ζεύγος κλειδιών που ελέγχει την πρόσβαση στα bitcoin. Το ζεύγος κλειδιών χρησιμοποιείται για την λήψη bitcoin, ενώ το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή συναλλαγών ώστε να ξοδευτούν αυτά τα bitcoin.
- **Difficulty:** Δείκτης δυσκολίας ως προς την επιτυχή εξόρυξη ενός νέου μπλοκ επί της αλυσίδας.
- **Κόμβος:** Ένα αντίγραφο του καθολικού που χειρίζεται ένας συμμετέχων στο δίκτυο blockchain.
- **Πλήρης κόμβος**: Ορίζουμε ένα πλήρη κόμβο, ως ένα κόμβο που διατηρεί το πλήρες αντίγραφο του blockchain, επικυρώνει όλες τις εισερχόμενες συναλλαγές και μπλοκ. Επιπλέον, ένας πλήρης κόμβος μπορεί να παρέχει μια ανοιχτή θύρα TCP με την οποία συνδέονται οι υπόλοιποι συμμετέχοντες στο δίκτυο.
- **SHA-256:** Αλγόριθμος ασύμμετρης κρυπτογράφησης που εφαρμόζει κατακερματισμό και εξάγει τιμή μήκους 256 bit. Μια “brute force” επίθεση χρειάζεται 2^{256} προσπάθειες για να παράγει τα ίδια δεδομένα. Έτσι το να προκύψουν 2 μηνύματα με την ίδια τιμή κατακερματισμού είναι εξαιρετικά απίθανο, αφού μια μικρή αλλαγή στα αρχικά δεδομένα μεταβάλει πλήρως το παραγόμενο αποτέλεσμα.
- **UTXO:** Αποτελεί την έξοδο συναλλαγής που δεν έχει δαπανηθεί και μπορεί να δαπανηθεί ως είσοδος σε μια νέα συναλλαγή.
- **Τέλος Αναμετάδοσης:** Η χρέωση αναμετάδοσης είναι η ελάχιστη αμοιβή που προσδίδεται κατά την εκτέλεση μιας συναλλαγής η οποία μεταδίδεται μεταξύ των ομότιμων κόμβων.

- **Τέλος εξόρυξης:** Αποτελεί την αμοιβή η οποία αποδίδεται σε ανθρακωρύχο ως κίνητρο για να συμπεριλάβει την συναλλαγή σε ένα μπλοκ, την ώρα που οι ανθρακωρύχοι δίνουν προτεραιότητα σε συναλλαγές που πληρώνουν υψηλότερα τέλη.
- **Επιβεβαίωση συναλλαγής:** Αποτελεί την απόδειξη ότι μια συναλλαγή εξ ορύχθηκε σε ένα μπλοκ, ενώ τα UTXO είναι έγκυρα και μπορούν να χρησιμοποιηθούν από το πορτοφόλι του παραλήπτη. Σημειώνεται ότι όταν η τιμή επιβεβαίωσης είναι μηδέν, η τιμή της συναλλαγής εντός του "mempool" και συνεπώς δεν εντάσσεται ήδη στις συναλλαγές εξόρυξης. Το παραπάνω αποτελεί παράδειγμα μη επιβεβαιωμένης συναλλαγής (UTXO).
- **BIP:** Μια πρόταση βελτίωσης Bitcoin είναι μια πρόταση για αλλαγή του Bitcoin. Τα BIP μπορούν να προτείνουν αλλαγές στο επίπεδο συναίνεσης, στα πρότυπα της κοινότητας ή στη διαδικασία ανάπτυξης. Σε μια από τις πιο γνωστές περιπτώσεις αυτή του SegWit, όπου πρόκειται για μια συναινετική αναβάθμιση με αλλαγές στο σύνολο κανόνων του Bitcoin, οι οποίες προτάθηκαν στο BIP 141.

1.4 Διάρθρωση διπλωματικής

Ο κύριος στόχος αυτής της εργασίας είναι να εντοπίσει τις πιθανές ευπάθειες που αντιμετωπίζει ένα Blockchain και πως οι ευπάθειες αυτές επιδρούν στην εφαρμογή διάφορων απειλών οι οποίες είναι ικανές να διακόψουν την ομαλή λειτουργία ενός τέτοιου συστήματος.

Για την καλύτερη κατανόηση εννοιών που χρησιμοποιούνται στην περιγραφή των προβλημάτων, κρίθηκε απαραίτητο να αναλυθούν διάφορα στοιχεία που συνθέτουν την τεχνολογία και επιτρέπουν την ομαλή εφαρμογή αυτής, όπως είναι τα ιδιαίτερα χαρακτηριστικά που διαθέτει, οι κρυπτογραφικές μέθοδοι στις οποίες στηρίζεται, η αρχιτεκτονική του, κ.α.

Επιπλέον, αναφέρονται διάφορα ποιοτικά θέματα τεχνικής φύσεως που αντιμετωπίζει η τεχνολογία και κατ' επέκταση επηρεάζεται η ασφάλεια αυτής, σχετικά με την επεκτασιμότητα, την κατανάλωση ενέργειας, την δημιουργία διακλαδώσεων κ.α.

Έπειτα πραγματοποιείται μια ενδελεχής περιγραφή και ανάλυση επιθέσεων με βάση διαφορετικές προοπτικές διαχωρισμού αυτών, που στοχεύουν στην καλύτερη κατανόηση των προβλημάτων.

Τέλος, αναλύονται ενδεικτικά ορισμένες λύσεις σε σημαντικά προβλήματα και αναφέρονται μελλοντικές προκλήσεις που χρήζουν επιπλέον έρευνα.

2 Βιβλιογραφική Επισκόπηση – Θεωρητικό Υπόβαθρο

Σε αυτό το κεφάλαιο θα μελετηθεί η έννοια του blockchain, συμπεριλαμβανομένων δομικών στοιχείων της τεχνολογίας, τις εφαρμογές, τις κατηγορίες, τον τρόπο λειτουργίας του blockchain, τα μοντέλα συναίνεσης καθώς και μια μαθηματική προσέγγιση, δεδομένου ότι η τεχνολογία αυτή βασίζεται στην ασύμμετρη κρυπτογραφία.

2.1 Εισαγωγή στην έννοια του blockchain

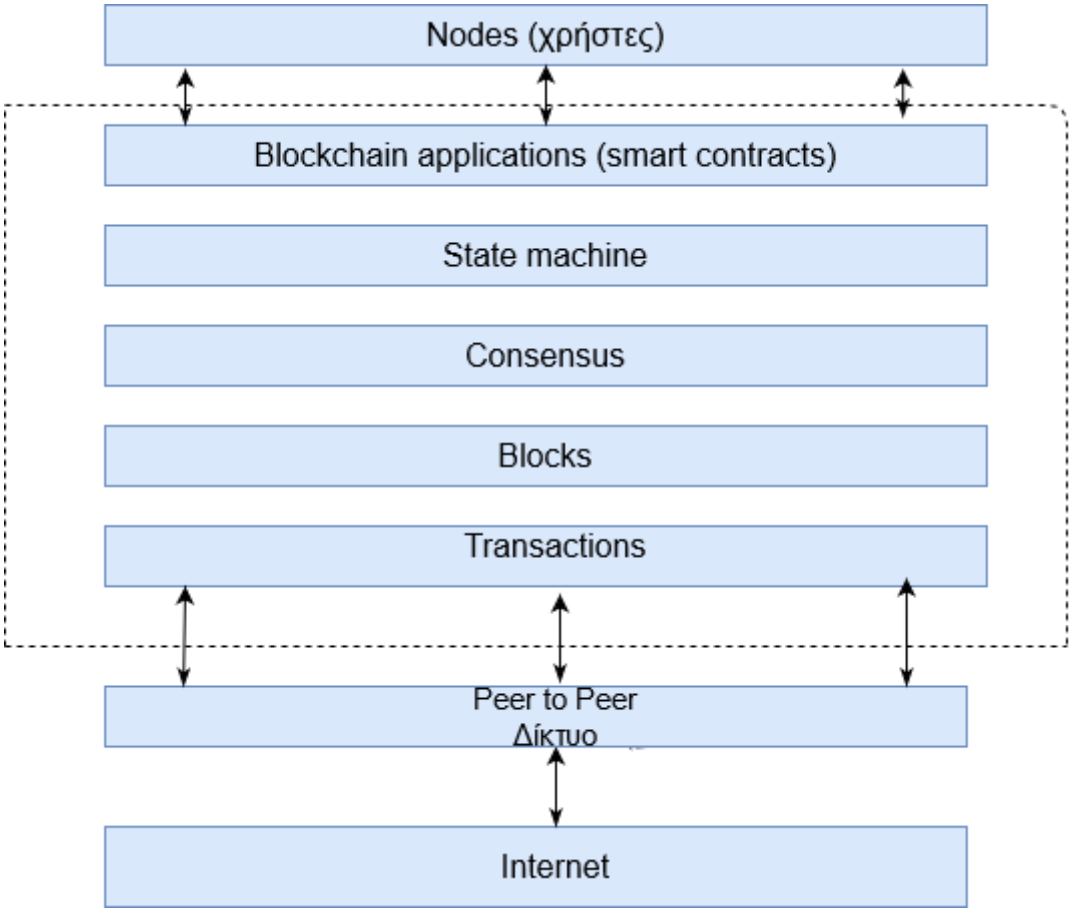
Υπάρχουν διάφοροι ορισμοί του blockchain. Η διαφοροποίηση τους έγκειται στην προοπτική στην οποία στοχεύουμε. Αν για παράδειγμα μας ενδιαφέρει η τεχνολογία στο πλαίσιο μιας επιχειρηματικής προοπτικής ή αν θέλουμε να εστιάσουμε στο τεχνικό πλαίσιο.

Αρχικά σε μια γενική επεξήγηση, η τεχνολογία blockchain στοχεύει στην δημιουργία αποκεντρωμένου περιβάλλοντος όπου κανένα τρίτο μέρος δεν ελέγχει τις συναλλαγές και τα δεδομένα. Σε γενικές γραμμές, το blockchain αποτελεί μια χρονικά σφραγισμένη αλυσίδα μπλοκ που συντηρούνται από όλους τους συμμετέχοντες κόμβους. Τα μπλοκ εμπεριέχουν ένα σύνολο συναλλαγών και συνδέονται μεταξύ τους κρυπτογραφικά. Πιο συγκεκριμένα, κάθε μπλοκ είναι ψηφιακά υπογεγραμμένο και συνδεδεμένο με το προηγούμενο ακριβώς μπλοκ συμπεριλαμβάνοντας την τιμή κατακερματισμού αυτού του μπλοκ (Chowdhury, Colman, Kabir, Han, & Sarda, 2018). Τα νέα μπλοκ μπορούν να προσαρτηθούν μόνο στο τέλος της αλυσίδας, επομένως το blockchain παρέχει μια αμετάβλητη αποθήκευση δεδομένων, αφού οι υπάρχουσες συναλλαγές δεν μπορούν να ενημερωθούν ή να διαγραφούν. Με αυτόν τον τρόπο, πολλά συστήματα που βασίζονται στην τεχνολογία blockchain επιτυγχάνουν την ασφαλή διανομή περιουσιακών στοιχείων μεταξύ μη αξιόπιστων μελών.

Προσεγγίζοντας μία τεχνική του προσέγγιση, το blockchain αποτελεί ένα ψηφιακό λογιστικό στο οποίο κρυπτογραφικά υπογεγραμμένες συναλλαγές εμπεριέχονται ομαδοποιημένα στα μπλοκ. Με άλλα λόγια, κάθε μπλοκ συνδέεται κρυπτογραφικά με το

προηγούμενο αφού έχει προηγηθεί η διαδικασία της επικύρωσης του και με την εφαρμογή ενός μοντέλου συναίνεσης μεταξύ όλων των κόμβων που συμμετέχουν στο δίκτυο (Yaga, Mell, Roby, & Scarfone, 2018). Έτσι λοιπόν, το blockchain ξεκίνησε αρχικά ως μια προσέγγιση πληρωμής συναλλαγών με βάση την κρυπτογραφία για να παρέχει έναν εναλλακτικό μηχανισμό για την εμπιστοσύνη μεταξύ των συναλλασσόμενων μερών. Ειδικότερα, η τεχνολογία αυτή συνθέτει σε ένα συλλογικό σύστημα τήρησης βιβλίων (καθολικό) το οποίο μέσω μιας μαθηματικής συνάρτησης (sha-256) επιτρέπει στους συμμετέχοντες να καταλήξουν σε συμφωνία σχετικά με την έγκριση μια συναλλαγής. Στην συνέχεια οι πληροφορίες σχετικά με τις μεμονωμένες συναλλαγές συγκεντρώνονται σε μπλοκ. Αυτά τα μπλοκ ελέγχονται και επαληθεύονται από το δίκτυο και προστίθενται με χρονολογική σειρά στους υπολογιστές όλων των συμμετεχόντων κόμβων του δικτύου. Ως εκ τούτου, ο παραδοσιακός ρόλος που διαδραματίζουν τα χρηματοπιστωτικά ιδρύματα ως αξιόπιστο τρίτο μέρος για την εξάλειψη του κινδύνου κατά την διαδικασία των συναλλαγών μπορεί να ικανοποιηθεί και μεσώ της συγκεκριμένης τεχνολογίας .

Ο ορισμός του blockchain σε μια προσέγγιση του ως δίκτυο θα μπορούσε να είναι μια “peer-to-peer” αρχιτεκτονική ενός κατανεμημένου λογιστικού το οποίο είναι κρυπτογραφικά ασφαλές με εφαρμογή ασύμμετρης κρυπτογραφίας, το οποίο αυτό λογιστικό είναι αμετάβλητο και ενημερώσιμο μόνο μέσω της διαδικασίας ενός μοντέλου συναίνεσης μεταξύ των ομότιμων κόμβων στο δίκτυο. Με άλλα λόγια το blockchain μπορεί να θεωρηθεί ως ένα στρώμα ενός κατανεμημένου δικτύου που «τρέχει» πάνω από το διαδίκτυο, όπως απεικονίζεται στο παρακάτω σχήμα. Θα μπορούσε να θεωρηθεί κάτι ανάλογο με τα πρωτόκολλα SMTP ή TFTP του μοντέλου tcp/ip.

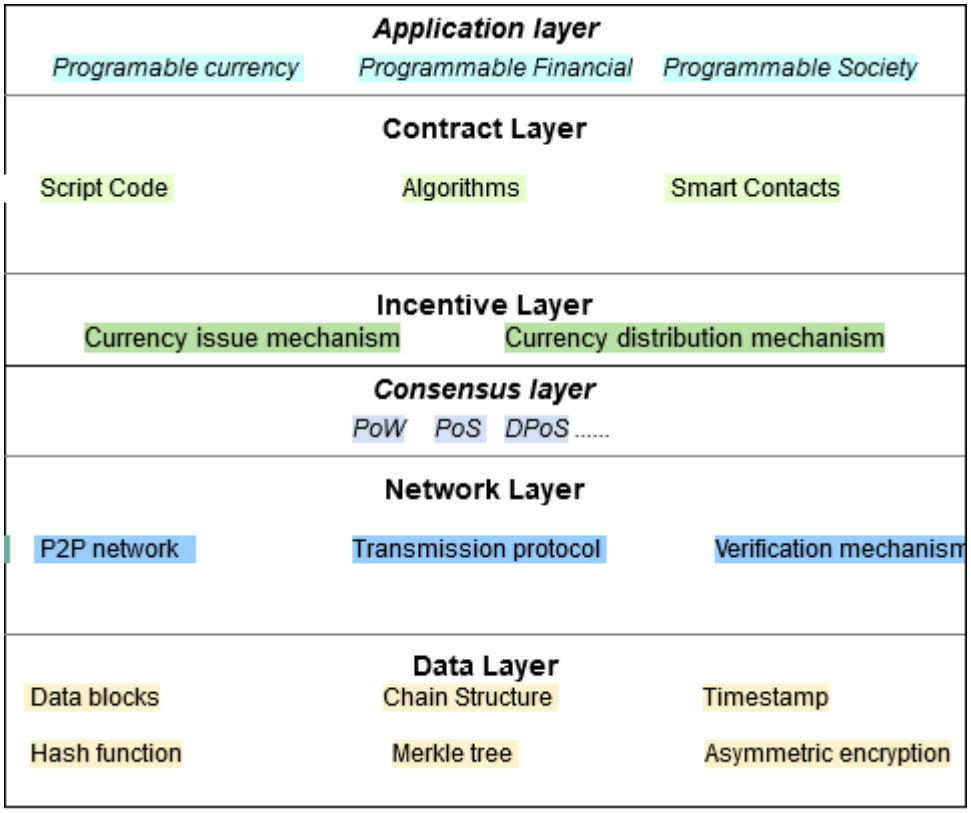


Εικόνα 2:Το blockchain ως δίκτυο

Σε μια πιο στοχευμένη ανάλυση της αρχιτεκτονικής του blockchain διαιρούμενη σε επίπεδα θα μπορούσαμε να πούμε ότι αποτελείται από ένα επίπεδο δεδομένων, ένα επίπεδο δικτύου , ένα επίπεδο συναίνεσης, ένα επίπεδο κινήτρων, ένα επίπεδο συμβολαίου και ένα επίπεδο εφαρμογών. Το επίπεδο δεδομένων είναι αυτό που ενσωματώνει τα μπλοκ μαζί με όλες τις καταχωρημένες πληροφορίες εντός αυτών καθώς και τις σχετικές εφαρμογές ασύμμετρης κρυπτογράφησης και χρονοσήμανσης . Επιπλέον, στο επίπεδο δεδομένων, κάθε κόμβος μπορεί να χρησιμοποιήσει τη συνάρτηση κατακερματισμού SHA, RSA, την δομή δεδομένων merkle trees κ.α.

Το επίπεδο δικτύου αποτελείται από ένα μηχανισμό κατανεμημένου δικτύου, ένα μηχανισμό με τον οποίο μεταδίδονται τα δεδομένα και ένα μηχανισμό επαλήθευσης δεδομένων (M. Li et al., 2019). Ο βασικός σκοπός του επιπέδου δικτύου είναι η συμμετοχή κάθε κόμβου στη διαδικασία καταχώρησης συναλλαγών και επαλήθευσης δεδομένων. Το επίπεδο συναίνεσης εμπεριέχει αλγορίθμους συναίνεσης για όλους τους κόμβους που συμμετέχουν στο blockchain δίκτυο (Romano & Schmid, 2017). Το επίπεδο κινήτρων

μπορεί να περιλαμβάνει οικονομικούς παράγοντες εντός του blockchain, όπως για παράδειγμα το να δίνεται μια ανταμοιβή στους miners που κάνουν εξόρυξη ενός νέου μπλοκ, ώστε να υπάρχει μια δικαιοσύνη μεταξύ των κατανεμημένων κόμβων και κατ' επέκταση ασφάλεια κατά την επέκταση της αλυσίδας. Το επίπεδο συμβάσεων σχετίζεται με τον προγραμματισμό που εφαρμόζεται στα πλαίσια του blockchain περιέχοντας scripts, αλγορίθμους ή «έξυπνες συμβάσεις» στο Ethereum. Τέλος το επίπεδο εφαρμογής περιλαμβάνει εφαρμογών δεδομένου ότι η τεχνολογία blockchain μπορεί να ενσωματωθεί σε διάφορους τομείς όπως health care, IoT, real estate κ.α. (Alladi, Chamola, Parizi, & Choo, 2019).



Εικόνα 3:Αρχιτεκτονική blockchain

Η επικοινωνία των κόμβων σε ένα δίκτυο όπως είναι αυτό του blockchain για να υποστηριχθεί και να λειτουργήσει χρειάζεται την παροχή των παρακάτω λειτουργικοτήτων, σύμφωνα με τις οποίες διαφορετικοί τύποι κόμβων μπορούν να συμμετέχουν στο δίκτυο.

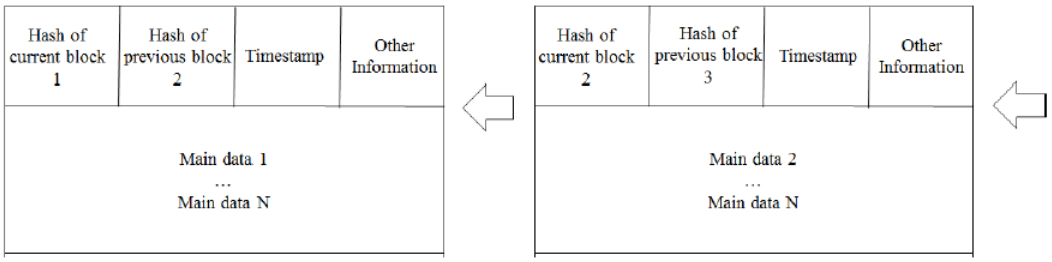
2.1.2 Ιδιαίτερα χαρακτηριστικά του blockchain

Κάποια από τα βασικά χαρακτηριστικά που να προσδώσουν οι blockchain τεχνολογίες είναι:

- Ακεραιότητα: Το blockchain είναι ένα “peer-to-peer” δίκτυο που όλοι οι κόμβοι κατέχουν το ίδιο αντίγραφο αρχείου σε αντίθεση με ένα απλό συγκεντρωτικό “client-server” μοντέλο όπου ένας επιτιθέμενος μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση. Το blockchain διατηρεί κρυπτογραφικό κατακερματισμό για την διασφάλιση της μη παραβίασης του λογιστικού (“ledger”). Ένα βασικό χαρακτηριστικό λειτουργίας της συνάρτησης κατακερματισμού είναι ότι πάντα παράγει διαφορετικό αποτέλεσμα, το οποίο σημαίνει ότι είναι σχεδόν απίθανο να ανακτηθούν δεδομένα από το αποτέλεσμα που παράγει η συνάρτηση κατακερματισμού. Με άλλα λόγια, είναι πρακτικά αδύνατο να προβλεφθούν τα αρχικά δεδομένα καθώς ακόμη και μια μικρή αλλαγή στο πραγματικό μήνυμα μπορεί να οδηγήσει σε μεγάλη διαφορά. Πιο συγκεκριμένα ένα αναγνωριστικό λογαριασμού Ethereum δημιουργείται με κατακερματισμό ενός δημοσίου κλειδιού με τον αλγόριθμο κατακερματισμού Keccak-256, ενώ μια διεύθυνση bitcoin υπολογίζεται με κατακερματισμό ενός δημοσίου κλειδιού με τον αλγόριθμο SHA-256.
- Ανωνυμία: Κάθε χρήστης μπορεί να αλληλοεπιδράσει με το blockchain μέσω μιας διεύθυνσης όπου δεν αποκαλύπτει την πραγματική ταυτότητα του χρήστη (Möser, n.d.).
- Αποκέντρωση: Όλοι οι συμμετέχοντες κόμβοι στο δίκτυο έχουν ένα αντίγραφο του λογιστικού βιβλίου (“ledger”) χωρίς να υπάρχει η ανάγκη μιας κεντρικής αρχής για τον έλεγχο των δεδομένων.
- Απόδειξη παραβίασης: Το πλεονέκτημα της απόδειξης παραβίασης στο blockchain επιτυγχάνεται μέσω της μοναδικότητας της χρονολογικής δομής στην αλυσίδα καθώς και της καταγραφής δεδομένων. Μόλις γίνει μια εγγραφή σε ένα block η οποία καταγράφεται ως συναλλαγή δημιουργείται στην δομή δεδομένων του blockchain μια νέα χρονική σήμανση. Με αυτόν τον τρόπο οποιαδήποτε τροποποίηση δεδομένων που δημιουργήθηκε πριν από αυτή την σήμανση δεν θα επιτρέπεται πλέον. Επιπλέον η διαδικασία καταγραφής μιας νέας συναλλαγής θα ελέγχεται μέσω του μηχανισμού συναίνεσης. Ειδικότερα , απαιτείται έγκριση

συγκεκριμένου ποσοστού χρηστών για να γράψουν δεδομένα σε μπλοκ και συγκεκριμένα το ποσοστό αυτό έχει οριστεί να είναι περισσότερο από το 50%.

- Προστασία προσωπικών δεδομένων: Το blockchain υιοθετεί ασύμμετρο μηχανισμό κρυπτογράφησης, επιτρέποντας έτσι στους χρήστες να κρυπτογραφούν δεδομένα με το δικό τους ιδιωτικό κλειδί. Επιπλέον υπολογίζεται η τιμή κατακερματισμού του δημοσίου κλειδιού ενός χρήστη, κάνοντας έτσι την αντιστοίχιση στην ταυτότητα ενός χρήστη. Ωστόσο η τιμή της συνάρτησης κατακερματισμού δεν σχετίζεται με την πραγματική ταυτότητα ενός χρήστη, διατηρώντας έτσι τις πληροφορίες των προσωπικών δεδομένων ιδιωτικά. Λαμβάνοντας υπόψιν ότι η διαδικασία υπολογισμού μιας τιμής της συνάρτησης κατακερματισμού είναι αντιστρέψιμη, μπορούμε να κατανοήσουμε ότι ο αντίπαλος δεν μπορεί να υποκλέψει το δημόσιο κλειδί ενός χρήστη από την δημόσια διεύθυνση του, καθιστώντας αδύνατο τον υπολογισμό ιδιωτικού κλειδιού από το δημόσιο κλειδί.
- Έξυπνες συμβάσεις: Το blockchain παρέχει την λειτουργικότητα έξυπνων συμβάσεων ή σεναρίων που εκτελούνται αυτόματα όταν πληρούνται ορισμένες προϋποθέσεις.
- Ανιχνευσιμότητα: Κάθε συναλλαγή που προστίθεται σε δημόσιο ή ιδιωτικό blockchain υπογράφεται ψηφιακά φέροντας ψηφιακή σήμανση. Το γεγονός αυτό δίνει την δυνατότητα ανίχνευσης στοιχείων συγκεκριμένης συναλλαγής η οποία πραγματοποιήθηκε σε συγκεκριμένη χρονική στιγμή, η οποία μπορεί να προσδιοριστεί μέσω της δημόσιας διεύθυνσης στο blockchain. Με αυτό τον τρόπο κάθε μπλοκ συνδέεται αμετάβλητα και επαληθεύσιμα με το προηγούμενο μπλοκ στην αλυσίδα (Swan, 2015). Έτσι με αυτό τον τρόπο μπορεί να ανακληθεί ένα πλήρες ιστορικό από το “genesis block” που αποτελεί το αρχικό μπλοκ της αλυσίδας. Για παράδειγμα, στην περίπτωση του bitcoin τα λογιστικά στοιχεία υπολοίπου ενός χρήστη βασίζονται στο μοντέλο UTXO (unspent transaction output). Συνεπώς κάθε τρέχουσα μη εκχωρημένη συναλλαγή καταγράφεται στο blockchain, ενώ όταν η συναλλαγή αυτή χρησιμοποιηθεί θα καταγραφεί ως δαπάνη καθιστώντας έτσι εύκολο τον εντοπισμό και την επαλήθευση μιας συναλλαγής.
- Ανοιχτή πηγή: Τα περισσότερα blockchain συστήματα είναι ανοιχτά σε όλους. Ειδικότερα, τα στοιχεία της αλυσίδας μπορούν να ελεγχθούν δημόσια



Εικόνα 4:Δομή των μπλοκ

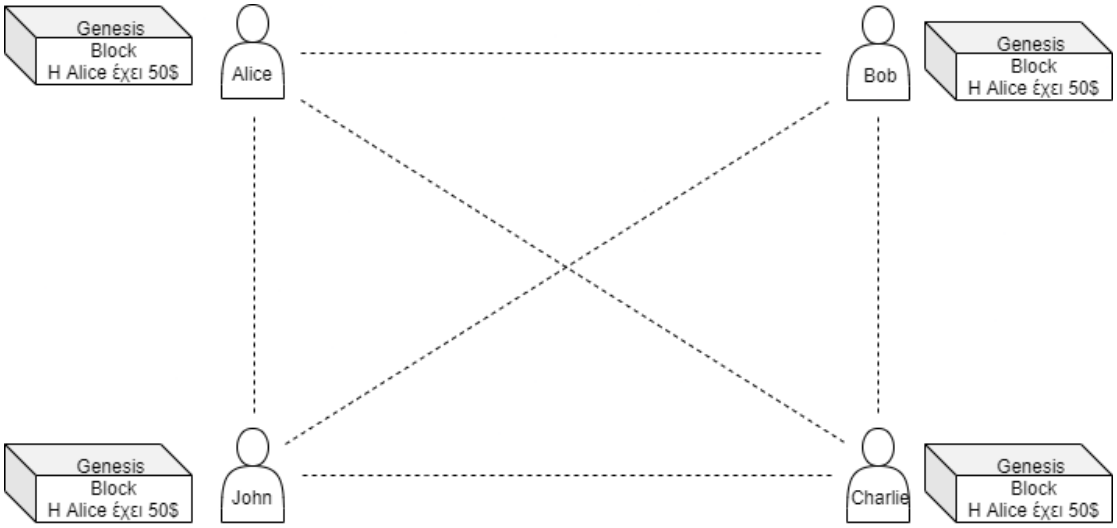
Κάθε κόμβος στο δίκτυο του blockchain έχει το ίδιο αντίγραφο του blockchain. Σε κάθε μπλοκ υπάρχουν δύο κύρια μέρη. Το τμήμα «κεφαλίδα» είναι αυτό που συνδέεται με το προηγούμενο μπλοκ της αλυσίδας. Αυτό σημαίνει ότι κάθε κεφαλίδα μπλοκ περιέχει τον κατακερματισμό του προηγούμενου μπλοκ, έτσι ώστε κανείς να μην μπορεί να αλλάξει οποιαδήποτε συναλλαγή στο προηγούμενο μπλοκ. Το άλλο μέρος ενός μπλοκ είναι το περιεχόμενο «σώματος» το οποίο εμπεριέχει μια επικυρωμένη λίστα συναλλαγών, τα ποσά τους, τις διευθύνσεις των εμπλεκόμενων μερών και μερικές περισσότερες λεπτομέρειες. Έτσι μέσω της πρόσβασης στο τελευταίο μπλοκ είναι δυνατό να υπάρχει πρόσβαση και σε όλα τα προηγούμενα μπλοκ σε ένα blockchain.

Στο σημείο αυτό θα εξετάσουμε ένα πρακτικό παράδειγμα, ώστε να γίνει κατανοητό πως πραγματοποιούνται οι συναλλαγές καθώς και πως επιτυγχάνεται η ενημέρωση του καθολικού λογιστικού (“ledger”), για την καλύτερη κατανόηση λειτουργίας ενός blockchain.

Έστω λοιπόν, ότι υπάρχουν τρείς υποψήφιοι η Αλίκη, ο Μπόμπ και ο Τσάρλυ οι οποίοι πραγματοποιούν κάποιες νομισματικές συναλλαγές μεταξύ τους σε ένα δίκτυο, ενώ το καθολικό ενημερώνεται σε όλο το δίκτυο. θα προσεγγίσουμε μέσω βημάτων τον τρόπο πραγματοποίησης συναλλαγών με στόχο την κατανόηση των δυνατοτήτων μιας αποκεντρωμένης δομής, όπως είναι το blockchain.

Βήμα 1:

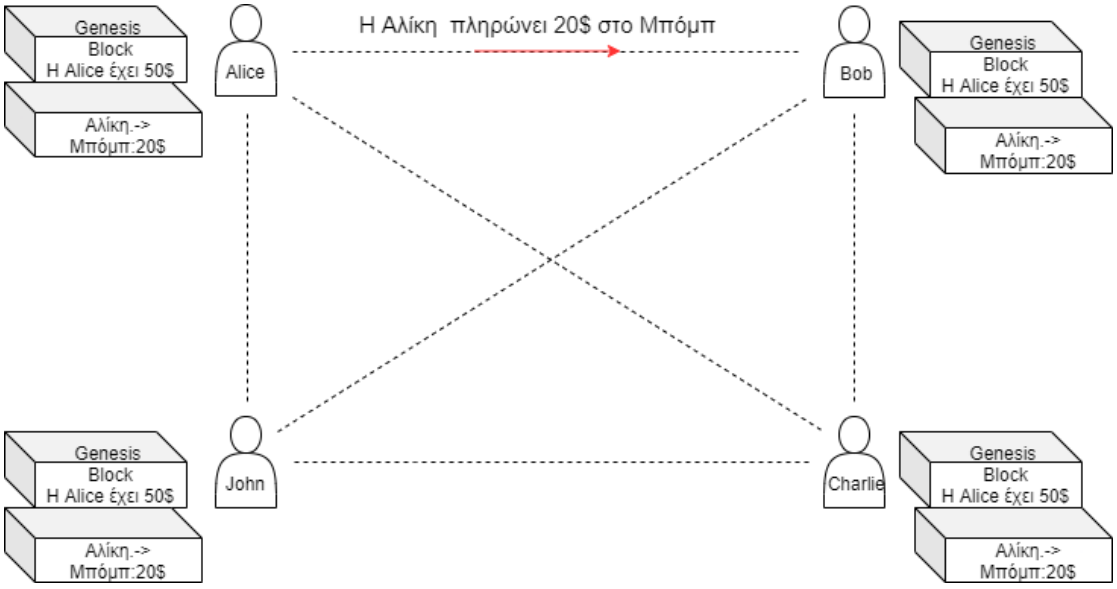
Έστω ότι η Αλίκη έχει 50$, που είναι η προέλευση όλων των συναλλαγών της και κάθε κόμβος το γνωρίζει όπως φαίνεται στο σχήμα.



Εικόνα 5:Το "genesis" block

Βήμα 2:

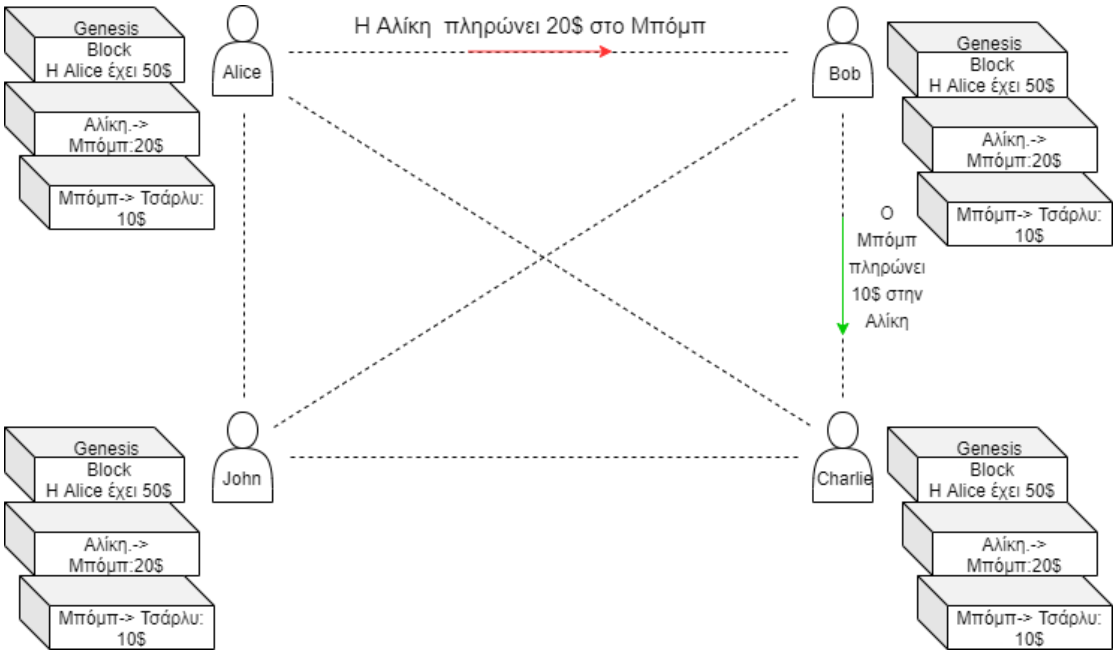
Η Αλίκη κάνει μια συναλλαγή πληρώνοντας 20$ στο Μπόμπ. Στη φάση αυτή ενημερώνεται κάθε κόμβος στο blockchain



Εικόνα 6:Η πρώτη συναλλαγή

Βήμα 3:

Ο Μπόμπ πραγματοποιεί μια άλλη συναλλαγή πληρώνοντας 10$ στον Τσάρλυ και το blockchain ενημερώνεται ξανά.

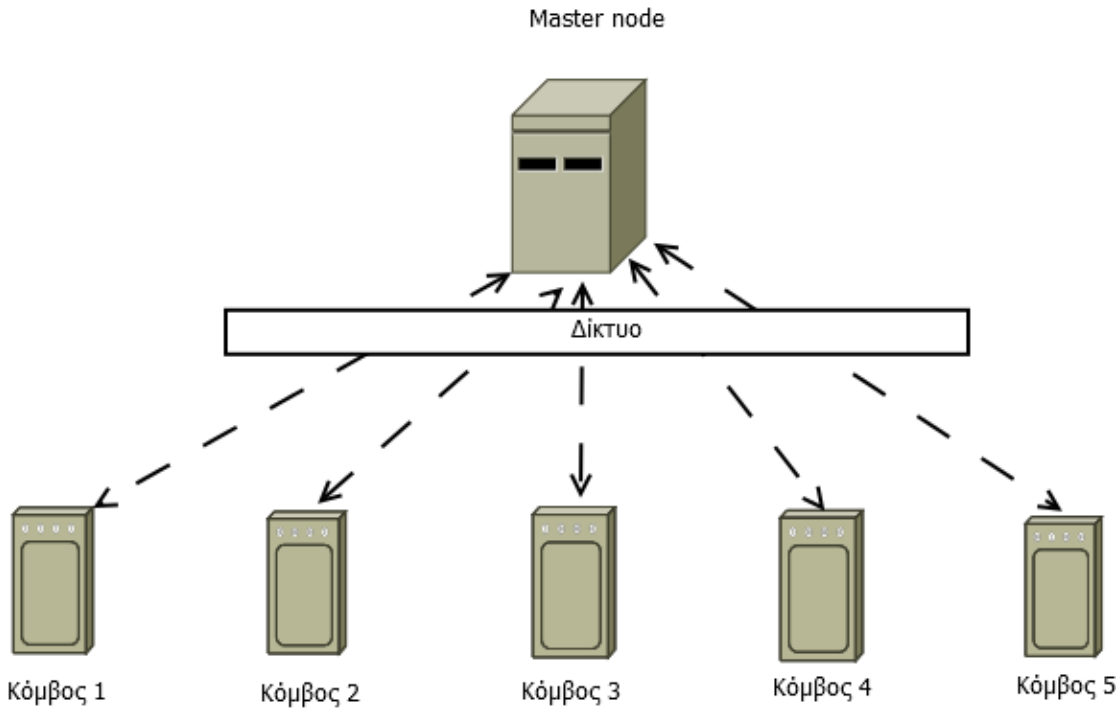


Εικόνα 7:Η δεύτερη συναλλαγή

Θα πρέπει να τονιστεί ότι τα δεδομένα συναλλαγών στα μπλοκ είναι αμετάβλητα, ενώ οι συναλλαγές είναι μη αναστρέψιμες. Αυτό σημαίνει ότι οποιαδήποτε αλλαγή θα έχει ως αποτέλεσμα μια νέα συναλλαγή η οποία θα πρέπει να επικυρωθεί από όλους τους συμβαλλόμενους κόμβους. Όπως έχει σημειωθεί κάθε κόμβος έχει το δικό του αντίγραφο blockchain.

2.1.3 Σύγκριση κεντροποιημένων- αποκεντρωμένων συστημάτων

Ο λόγος που εξετάζουμε τη σύγκριση μεταξύ κεντροποιημένων και αποκεντρωμένων συστημάτων είναι επειδή το blockchain έχει σχεδιαστεί από μια κατανεμημένη και αποκεντρωμένη αρχιτεκτονική. Ωστόσο, ένα σύστημα μπορεί να είναι κατανεμημένο ανεξάρτητα από το αν έχει ή όχι αποκεντρωμένη δομή (Chowdhury et al., 2018). Αναλυτικότερα ένα κεντροποιημένο σύστημα είναι ένα σύστημα στο οποίο υπάρχει για παράδειγμα, ένας κύριος κόμβος υπεύθυνος για την κατανομή των εργασιών ή των δεδομένων καθώς και την διανομή του φορτίου σε κόμβους. Από την άλλη πλευρά, ένα αποκεντρωμένο κατανεμημένο σύστημα είναι αυτό, όπου δεν υπάρχει κάποιος «κύριος» κόμβος και κατ' επέκταση ένας υπολογισμός ή μια διεργασία διανέμεται σε όλους τους κόμβους του δικτύου. Το blockchain αποτελεί ένα τέτοιο παράδειγμα.

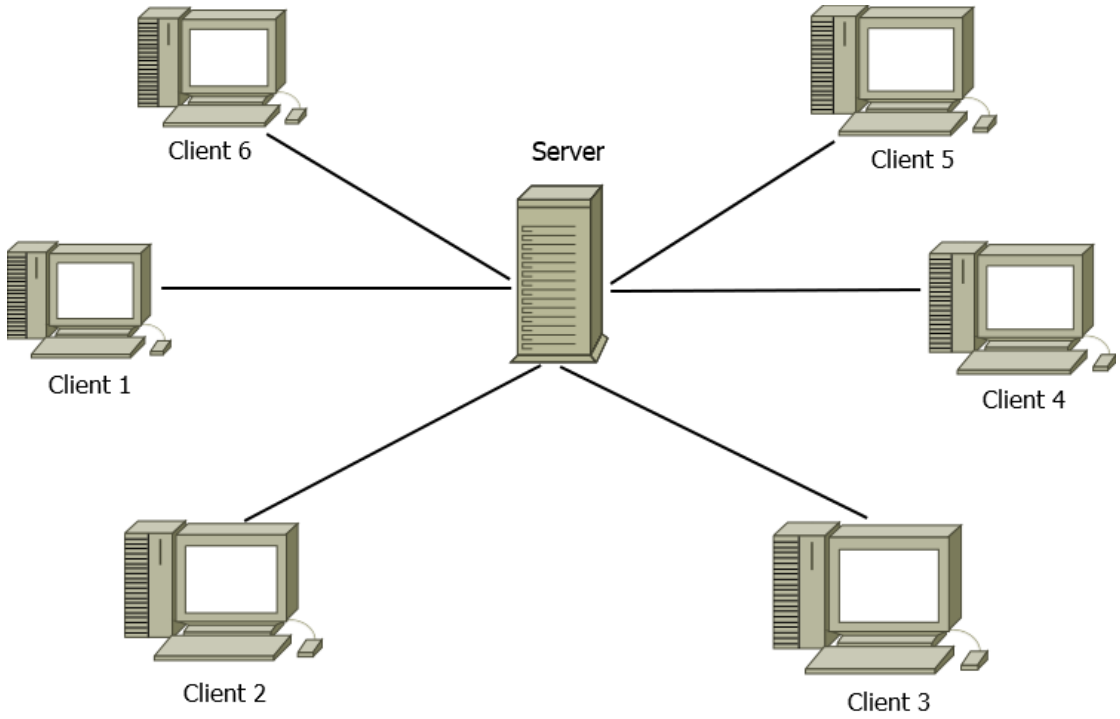


Εικόνα 8:Κατανεμημένο σύστημα με κεντροποιημένο έλεγχο

2.1.4 Κεντροποιημένα Συστήματα

Όπως υποδηλώνει το όνομα, ένα κεντρικό σύστημα έχει κεντρικό έλεγχο με όλες τις διοικητικές αρχές. Όπως είναι λογικό τέτοια συστήματα είμαι εύκολο να σχεδιαστούν, να διατηρηθούν, καθώς επίσης και να επιβληθεί εμπιστοσύνη μεταξύ των συμμετεχόντων μελών του. Ωστόσο μειονεκτούν, αφού παρουσιάζουν πολλούς εγγενείς περιορισμούς. Μερικοί από αυτούς είναι οι παρακάτω:

- Διαθέτουν ένα κεντρικό σημείο αποτυχίας με αποτέλεσμα να είναι λιγότερο σταθερές.
- Τα συστήματα αυτά είναι πιο ευάλωτα σε επιθέσεις και ως εκ τούτου λιγότερο ασφαλή.
- Η δεδομένη συγκέντρωση ισχύος μπορεί να οδηγήσει σε ανήθικες λειτουργίες, αφού είναι αδύνατη η επιβολή κάποιας μορφής ελέγχου από άλλα μέλη του συστήματος.
- Η επεκτασιμότητας είναι δύσκολη τις περισσότερες φορές.



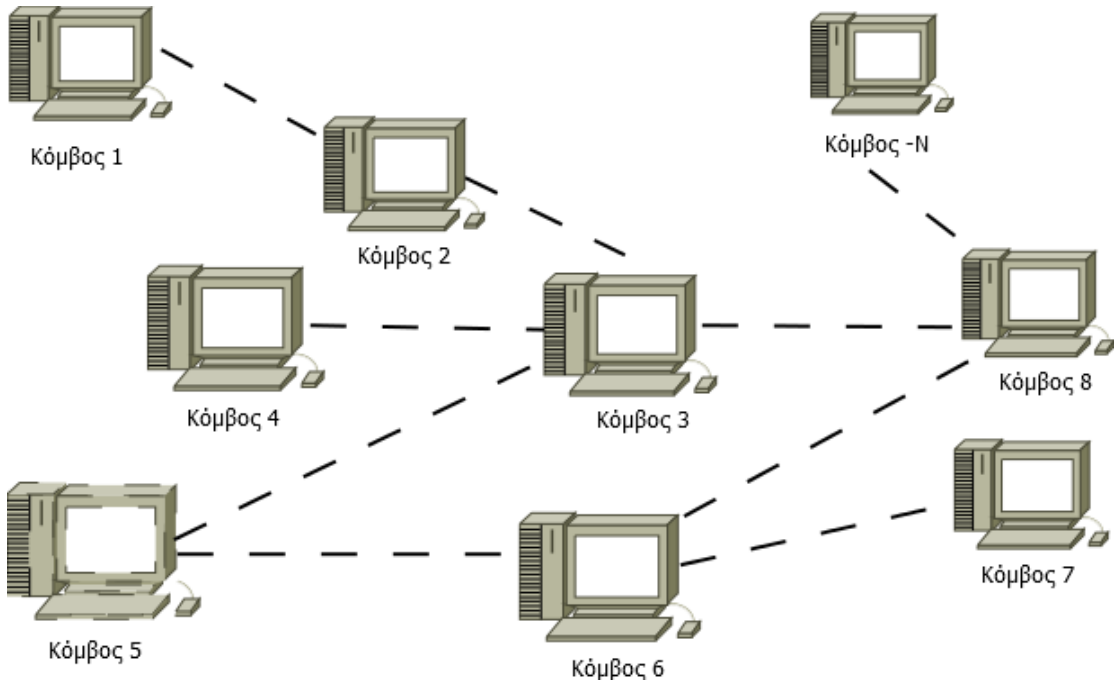
Εικόνα 9:κεντροποιημένο σύστημα

2.1.5 Αποκεντρωμένα Συστήματα

Όπως δηλώνει το όνομα, ένα αποκεντρωμένο σύστημα δεν έχει κεντρικό έλεγχο και συνεπώς κάθε κόμβος έχει τον ίδιο βαθμό επιρροής στο σύστημα. Η αποκέντρωση διαφέρει εντελώς από την συγκέντρωση (Iuon-Chang Lin & Tzu-Chun Liao, 2017). Μπορεί τα αποκεντρωμένα συστήματα να έχουν μεγαλύτερο βαθμό δυσκολίας στον σχεδιασμό τους, στην σωστή λειτουργία τους ή την επιβολή της εμπιστοσύνης μεταξύ των στοιχείων που συνθέτουν το σύστημα, ωστόσο απαλλάσσονται από περιορισμούς των συμβατικών κεντρικών συστημάτων. Μερικά από τα πλεονεκτήματα των αποκεντρωμένων συστημάτων είναι τα παρακάτω:

- Δεν αποτελούνται από κάποιο κεντρικό σημείο αποτυχίας. Συνεπώς διαθέτουν πολύ μεγαλύτερη ανοχή σε σφάλματα.
- Ανθεκτικότητα σε επιθέσεις, αφού για να θεωρηθεί μια επίθεση επιτυχημένη αρκεί να βάλει όχι μόνο ένα κεντρικό «σημείο» όπως θα συνέβαινε σε μια κεντροποιημένη δομή, αλλά θα πρέπει προσβάλλει ένα ποσοστό επί του συνολικού συστήματος αλλά με το εκάστοτε βαθμό ανοχής σε σφάλματα.

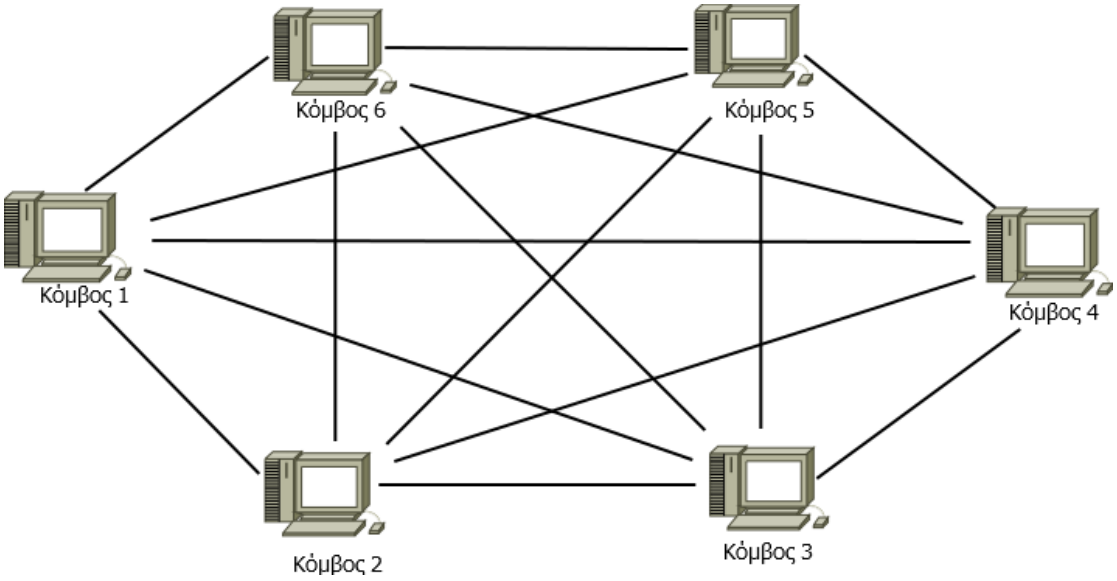
- Αποτελεί ένα συμμετρικό σύστημα με κατανομή ισόποσης εξουσίας σε όλα τα μέλη, γεγονός που προσδίδει διαφάνεια σε πιθανές παράνομες λειτουργίες εντός του συστήματος.



Εικόνα 10:Αποκεντρωμένο σύστημα

Ωστόσο ένα αποκεντρωμένο σύστημα μπορεί να είναι και κατανεμημένο. Ένα τέτοιο παράδειγμα είναι το blockchain. Σε αντίθεση όμως με τα κοινά κατανεμημένα συστήματα, η εργασία δεν υποδιαιρείται και μεταβιβάζεται σε κόμβους, καθώς στο blockchain δεν υπάρχει ο "master" κόμβος που θα έκανε μια τέτοια διεργασία(Collomb & Sok, 2016). Σε ένα αποκεντρωμένο και κατανεμημένο σύστημα, το οποίο καλείται "peer-to-peer", όλοι οι συμβαλλόμενοι κόμβοι δεν λειτουργούν σε ένα μέρος της εργασίας. Αντίθετα στο ομότιμο αυτό δίκτυο οι κόμβοι αποθηκεύουν και μοιράζονται συλλογικά αρχεία όπου κάθε κόμβος λειτουργεί ως μεμονωμένος ομότιμος. Με άλλα λόγια η επικοινωνία σε ένα "p2p" δίκτυο γίνεται χωρίς κεντρική διαχείριση ή διακομιστή, το οποίο σημαίνει ότι όλοι οι κόμβοι έχουν ίση ισχύ και εκτελούν τις ίδιες εργασίες. Η αρχιτεκτονική "peer-to-peer" στο blockchain επιτρέπει την μεταφορά όλων των κρυπτονομισμάτων σε όλο τον κόσμο χωρίς την ανάγκη κάποιου μεσάζοντος ή κεντρικού διακομιστή. Σε ένα κατανεμημένο δίκτυο "peer-to-peer" οποιοσδήποτε επιθυμεί να

συμμετάσχει στην διαδικασία επαλήθευσης και επικύρωσης μπλοκ μπορεί να δημιουργήσει έναν κόμβο Bitcoin. Έτσι στην περίπτωση του blockchain όπου έχουμε ένα αποκεντρωμένο δίκτυο “peer-to-peer” μεταξύ των κόμβων, όλοι οι υπολογιστές είναι συνδεδεμένοι με τέτοιο τρόπο, όπου ο καθένας διατηρεί πλήρες αντίγραφο του καθολικού και το συγκρίνει με άλλες συσκευές για να εξασφαλιστεί αν τα δεδομένα είναι έγκυρα.



Εικόνα 11:Αποκεντρωμένο “peer-to-peer” δίκτυο

2.2 Blockchain in Cyber Security (μοντέλο CIA)

Το μοντέλο CIA αναφέρεται στα χαρακτηριστικά της εμπιστευτικότητας (confidentiality), ακεραιότητας (integrity) και διαθεσιμότητας (availability) τα οποία θα πρέπει να διέπουν το blockchain. Ο σκοπός αυτού του μοντέλου είναι η εξασφάλιση ενός πλαισίου για την ανάπτυξη πολιτικών ασφαλείας πληροφοριών. Η εμπιστευτικότητά αναφέρεται στην διατήρηση κρυφών πληροφοριών από μη εξουσιοδοτημένα άτομα, η ακεραιότητα αποτελεί ένα τρόπο προστασίας της μη εξουσιοδοτημένης παραβίασης πληροφοριών, ενώ η διαθεσιμότητα αναφέρεται στην έγκαιρη και αξιόπιστη πρόσβαση στα δεδομένα.

- **Εμπιστευτικότητα στο blockchain:** Κάθε ψηφιακά συνδεδεμένη τεχνολογία συνοδεύεται από το κόστος των προκλήσεων ασφαλείας και αυτές οι προκλήσεις μπορούν να αφορούν την έκθεση στην προστασία της ιδιωτικής ζωής, τις παραβιάσεις της εμπιστευτικότητας ή την κλοπή ταυτότητας. Η εμπιστευτικότητα στο blockchain αφορά απλώς τη

απόκρυψη πληροφοριών συναλλαγής από ανεπιθύμητους συμμετέχοντες στο δίκτυο, η οποία στα δημόσια blockchain μπορεί να είναι πολύ δύσκολη στην επίτευξη της.

- **Ακεραιότητα στο blockchain:** Η ακεραιότητα είναι ένας τρόπος αποφυγής τυχόν παραβίασης των δεδομένων. Για τον λόγο αυτό το blockchain χρησιμοποιεί κρυπτογραφικό κατακερματισμό για να διασφαλίσει ότι το καθολικό παραμένει αμετάβλητο. Το βασικό χαρακτηριστικό στην συνάρτηση κατακερματισμού είναι το αδύνατο της ανάκτησης δεδομένων από το αποτέλεσμα κατακερματισμού ή από το μοτίβο σύνοψης μηνυμάτων (Salman, Zolanvari, Erbad, Jain, & Samaka, 2019). Ένα αναγνωριστικό λογαριασμού Ethereum δημιουργείται με κατακερματισμό ενός δημόσιου κλειδιού με τον αλγόριθμό κατακερματισμού Keccak-256, ενώ μια διεύθυνση bitcoin υπολογίζεται με κατακερματισμό ενός δημοσίου κλειδιού με τον αλγόριθμο SHA-256.
- **Διαθεσιμότητα στο blockchain:** Η έγκαιρη και αξιόπιστη πρόσβαση σε πληροφορίες μοιάζει με την διαθεσιμότητα. Οι κυβερνοεπιθέσεις όπως DDoS αποτελούν συχνό κίνδυνο στις υπηρεσίες διαδικτύου και έχουν ως αποτέλεσμα να μην είναι προσβάσιμες οι ιστοσελίδες σε επιχειρήσεις ή άλλους οργανισμούς (Swan, M. (2015)). Η αποκεντρωμένη φύση του blockchain καθιστά δυσκολότερη την επίτευξη μιας τέτοιας επίθεσης.

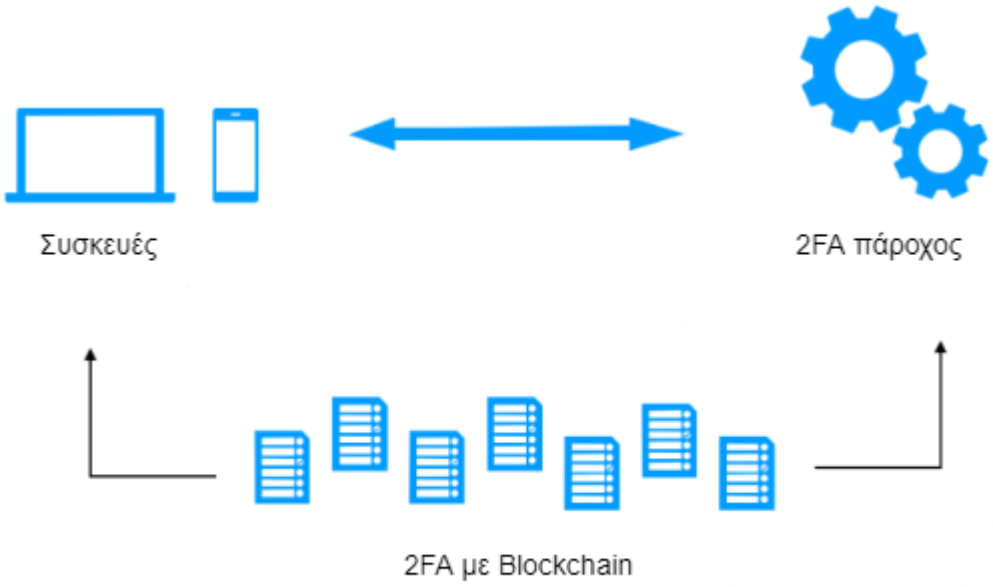
2.3 Αναγνώριση ταυτότητας με εφαρμογή PKI (Public key Infrastructure) σε blockchain

Η υποδομή PKI είναι η πιο συνηθισμένη τεχνική προστασίας ως προς την ταυτότητα για την ασφάλεια ηλεκτρονικών μηνυμάτων, ισότοπων και άλλων μορφών επικοινωνίας. Ωστόσο η PKI υποδομή έχει μια μεγάλη ευπάθεια λόγω του κεντρικού συστήματος διαχείρισης που έχει. Η συνεισφορά του blockchain σε μια τέτοια υποδομή είναι η επίτευξη ενός αποκεντρωμένου δικτύου πολλαπλών συμμετεχόντων χωρίς συμμετοχή τρίτων. Έτσι μια αποκεντρωμένη υποδομή δημοσίου κλειδιού δημιουργεί συστήματα ελέγχου χωρίς κάποια εξάρτηση που μπορεί να θέσει σε κίνδυνο στην ακεραιότητά και την ασφάλεια του συστήματος (Axon & Goldsmith, 2017). Το blockchain

δηλαδή είναι μια φυσική λύση σε ορισμένα από αυτά τα προβλήματα με το pki, ειδικότερα με την διαφάνεια των πιστοποιητικών και την εξάλειψη μεμονωμένων σημείων αποτυχίας, ένα από τα σημαντικότερα προβλήματα των μη αποκεντρωμένων αρχιτεκτονικών. Μια υποδομή pki που ενσωματώνει την τεχνολογία blockchain έχει κατασκευαστεί ως κατανεμημένο δημόσιο βιβλίο (ledger) που συνδέει την αναγνώριση ταυτότητας με ένα δημόσιο κλειδί.

2.4 Two-Factor αυθεντικοποίηση με blockchain

Δεδομένου ότι κάθε οργανισμός έχει εκατοντάδες εφαρμογές και βάσεις δεδομένων, οι υπάλληλοι του έχουν πρόσβαση σε αυτές μέσω κωδικών. Συνεπώς ένας εισβολέας με έγκυρους κωδικούς μπορεί να παρακάμψει τις υπάρχουσες λύσεις ασφαλείας προσποιούμενος ένα νόμιμο χρήστη. Ο έλεγχος ταυτότητας 2 παραγόντων 2FA παρέχει ένα πρόσθετο επίπεδο στο υπάρχον σύστημα προστασίας. Αν και το 2FA αυξάνει το επίπεδο ασφαλείας με το δεύτερο επίπεδο ελέγχου ταυτότητας εξακολουθεί να αντιμετωπίζει το μειονέκτημα ότι η κεντρική βάση αποθηκεύει μια λίστα μυστικών πληροφοριών στον χρήστη (Putri, Sukarno, & Wardana, 2020). Ενσωματώνοντάς λοιπόν το blockchain σε ένα 2FA σύστημα αυθεντικοποίησης , μπορούμε να διασφαλίσουμε ότι αυτές οι ευαίσθητες πληροφορίες δεν θα παραμείνουν ποτέ σε μια βάση δεδομένων. Ειδικότερα οι πληροφορίες αυτές θα εμπεριέχονται στους κόμβους οι οποίοι διαθέτουν ένα αντίγραφο του blockchain, το οποίο είναι εξορισμού αμετάβλητο, με αποτέλεσμα να μην μπορεί να αλλοιωθεί οποιαδήποτε πληροφορία.



Εικόνα 12:2-factor αυθεντικοποίηση

2.5 Πως λειτουργεί το blockchain

Για να κατανοήσουμε καλύτερα την λειτουργία του blockchain θα ήταν σκόπιμο να περιγραφεί η διαδικασία δημιουργίας και επικύρωσης ενός νέου μπλοκ που προστίθεται στην αλυσίδα μέσω βημάτων.

Βήμα 1-Δημιουργία νέας συναλλαγής: Οι συναλλαγές δημιουργούνται από τους συμμετέχοντες στο δίκτυο blockchain. Κάθε συναλλαγή αποτελείται από τουλάχιστον μια είσοδο και έξοδο. Αν μια συναλλαγή κόβει νέα νομίσματα τότε δεν υπάρχει είσοδος και επομένως δεν απαιτείται υπογραφή. Αν όμως μια συναλλαγή πρόκειται να στείλει ψηφιακά νομίσματα σε κάποιον άλλο χρήστη (διεύθυνση bitcoin), τότε πρέπει να υπογραφεί από τον αποστολέα με το ιδιωτικό κλειδί. Απαιτείται επίσης αναφορά στην προηγούμενη συναλλαγή για να δείξει την προέλευση των νομισμάτων. Σε αυτό το στάδιο, έστω ο κόμβος Α δημιουργεί μια συναλλαγή η οποία περιλαμβάνει πληροφορίες που περιέχουν την δημόσια διεύθυνση του παραλήπτη, μια ψηφιακή υπογραφή και ένα μήνυμα συναλλαγής. Πλέον αυτή συναλλαγή διατίθεται σε όλους τους κόμβους του blockchain.

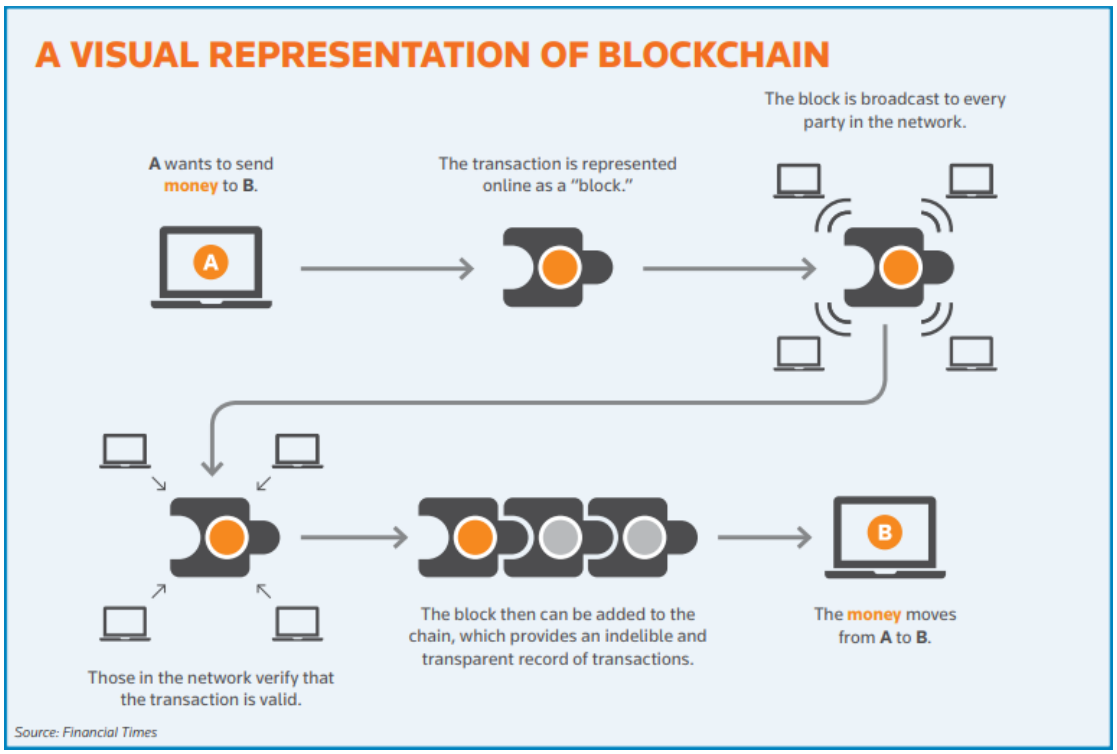
Βήμα 2-Επαλήθευση συναλλαγής: Οι κόμβοι blockchain λειτουργούν ως ένα αξιόπιστο μοντέλο όπου κάθε κόμβος που εκτελεί το λογισμικό πελάτη blockchain λαμβάνει αυτήν την συναλλαγή και επαληθεύει αυτή την συναλλαγή με το δημόσιο κλειδί

του κόμβου Α. Αφού πραγματοποιηθεί με επιτυχία η επαλήθευση η συναλλαγή εμπεριέχεται στην ουρά του καθολικού και περιμένει έως ότου όλοι οι κόμβοι επαληθεύσουν με επιτυχία την ίδια συναλλαγή.

Βήμα 3-Δημιουργία μπλοκ: Οι συναλλαγές στην ουρά τακτοποιούνται μαζί και δημιουργείται ένα block από ένα από τους κόμβους του δικτύου. Ειδικότερα, στο bitcoin blockchain ο κόμβος που θα εξορύξει το νέο μπλοκ λύνοντας το πολύπλοκο κρυπτογραφικό πρόβλημα ανταμείβεται με bitcoin.

Βήμα 4-Επικύρωση μπλοκ: Αφού επιτευχθεί η δημιουργία μπλοκ, οι κόμβοι στο δίκτυο υποβάλλονται σε επεξεργασία για μια διαδικασία επαναληπτικής επικύρωσης όπου η πλειονότητα των κόμβων πρέπει να αποκτήσουν συναίνεση. Οι πιο δημοφιλείς τρόποι επίτευξης συναίνεσης είναι οι Proof of Work, Proof of Stack, Delegated Proof of Stack και Practical Byzantine Fault Tolerance.

Βήμα 5-Σύνδεση του επικυρωμένου μπλοκ στην αλυσίδα: Με την επιτυχημένη ολοκλήρωση του μηχανισμού συναίνεσης, τα επικυρωμένα μπλοκ μπορούν πλέον προσαρτηθούν στην αλυσίδα των μπλοκ.



Εικόνα 13:Αναπαράσταση ενός "transaction" σε "blockchain" δίκτυο[1]

2.6 Η Δομή του Blockchain

Όπως έχει προ ειπωθεί το Blockchain είναι ένα δημόσιο καθολικό το οποίο είναι αποθηκευμένο σε μια κατανεμημένη βάση δεδομένων, το οποίο δεν επιτρέπει απλά την προσθήκη νέων δεδομένων στη βάση δεδομένων, αλλά διασφαλίζει επίσης ότι όλοι οι χρήστες του δίκτυού έχουν ακριβώς τα ίδια δεδομένα. Έτσι, ένα blockchain είναι μια κατανεμημένη και αποκεντρωμένη δομή δεδομένων, η οποία διασφαλίζει ότι τα δεδομένα θα είναι μη τροποποιήσιμα.

Ένα πλήθος συναλλαγών δημιουργούν συνδυασμούς για να σχηματίσουν ένα μπλοκ και με αυτή την έννοια το μπλοκ αποτελεί και αυτό μια δομή δεδομένων. Κάθε κρυπτονόμισμα έχει το δικό του blockchain με τα δικά του συγκεκριμένα χαρακτηριστικά και ιδιότητες. Έτσι ένα μπλοκ σε ένα blockchain bitcoin δημιουργείται κάθε περίπου 10 λεπτά και το μέγεθος ενός τέτοιου μπλοκ είναι 1 mb, ενώ ένα μπλοκ σε ένα blockchain Ethereum δημιουργείται κάθε 12-14 δευτερόλεπτα ενώ το μέγεθος κάθε μπλοκ είναι 2 kb.

Πίνακας 1:Η Δομή του μπλοκ

Bytes	Τμήμα στο block	Περιγραφή
80	Κεφαλίδα μπλοκ	Μια κεφαλίδα μπλοκ μας βοηθάει να αναγνωρίσουμε ένα συγκεκριμένο μπλοκ στο blockchain. Περιέχει ένα σύνολο από μεταδεδόμενα

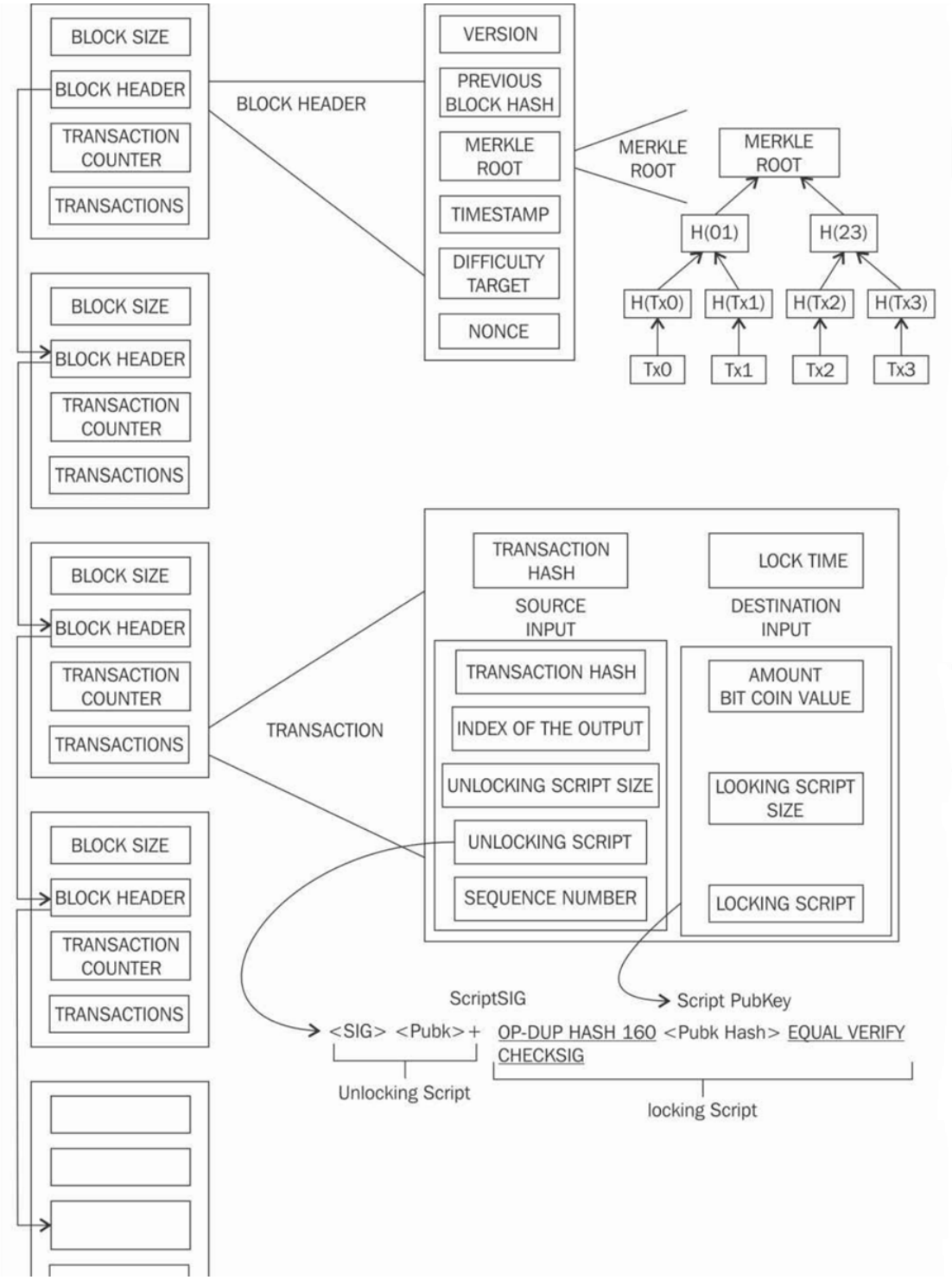
[1] Ανακτήθηκε από: https://www.thomsonreuters.com/en-us/posts/tax-and-accounting/blockchain-impact-tax-and-accounting-industry/

Μεταβλητός αριθμός	Μετρητής συναλλαγών	Το πεδίο αυτό εμπεριέχει τον αριθμό των συναλλαγών που καταχωρούνται στο μπλοκ
Μεταβλητός αριθμός	Συναλλαγές	Ο συνολικός αριθμός συναλλαγών που έχουν καταχωρηθεί στο μπλοκ

Πίνακας 2:Η δομή της κεφαλίδας μπλοκ

Bytes	Όνομα	Περιγραφή
4	Έκδοση	Κατακερματισμός κεφαλίδας προηγούμενου μπλοκ
32	Κατακερματισμός κεφαλίδας προηγούμενου μπλοκ	Το αποτέλεσμα της συνάρτησης κατακερματισμού sha-256 του προηγούμενου μπλοκ
32	Κατακερματισμός Merkle root	Το αποτέλεσμα μετά από διπλό κατακερματισμό με εφαρμογή της συνάρτησης της συνάρτησης sha-256 όλων των συναλλαγών που εμπεριέχονται στο μπλοκ
4	Χρονική σήμανση (timestamp)	Ο αριθμός έκδοσης μπλοκ που υπαγορεύει τους κανόνες για την επικύρωση ενός μπλοκ

4	Difficulty target	Για την δημιουργία ενός νέου μπλοκ ορίζεται ένα “difficulty target” , σύμφωνα με το οποίο για να εξ ορυχθεί ένα νέο μπλοκ θα πρέπει το αποτέλεσμα της συνάρτησης κατακερματισμού μικρότερο από τον ορισμένο «στόχο δυσκολίας»
4	Nonce	Η τιμή nonce σε ένα μπλοκ προσαρμόζεται από τους miners έτσι ώστε η τιμή κατακερματισμού να είναι μικρότερή η ίση με τον τρέχον “difficulty target” του δικτύου



Εικόνα 14:Πλήρης απεικόνιση δομής ενός μπλοκ

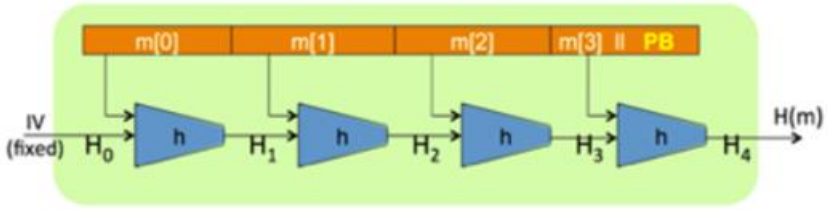
2.7 Βασική εφαρμογή κρυπτογραφίας στο blockchain

Το Bitcoin πρωτόκολλο εφαρμόζει κρυπτογραφικά εργαλεία που αφορούν λειτουργίες κατακερματισμού, όπως είναι συναρτήσεις κατακερματισμού sha-256 και RIPEMD160, δομές δεδομένων όπως είναι τα "merkle trees" καθώς επίσης και τον αλγόριθμο ψηφιακής υπογραφής σε ελλειπτικές καμπύλες (ECDSA).

Οι συναρτήσεις κατακερματισμού έχουν ως είσοδο μια τυχαία ακολουθία bytes και μετατρέπει δηλαδή δεδομένα αυθαίρετου μήκους σε μια σταθερού μήκους έξοδο, η οποία αναφέρεται ως τιμή κατακερματισμού ή σύνοψη. Η τιμή αυτή είναι 256-bit ή 512-bit. Αν για παράδειγμα είναι 256-bit τότε το αποτέλεσμα της συνάρτησης μπορεί να είναι μέχρι 2^{256} διαφορετικές τιμές. Οι κρυπτογραφικές συναρτήσεις κατακερματισμού έχουν 2 βασικές ιδιότητες (Karame, 2016). Είναι μονόδρομες συναρτήσεις με την έννοια ότι είναι εύκολο να υπολογιστεί η έξοδος τους για μια συγκεκριμένη είσοδο αλλά πολύ δύσκολο από την έξοδο να προκύψει η αντίστοιχή είσοδος. Αυτό μεταφράζεται στο ότι γνωρίζοντας το x εύκολα μπορεί να βρεθεί το f(x), αλλά είναι δύσκολο με δεδομένο το f(x) να βρούμε το x (Coron, Dodis, Malinaud, & Puniya, 2005). Επιπλέον μια μονόδρομη συνάρτηση hash, είναι ελεύθερη από συγκρούσεις (collision free), που σημαίνει ότι είναι υπολογιστικά ανέφικτο να βρεθεί x=y : H(x)=H(y). Τέλος, οι συναρτήσεις κατακερματισμού αποτελούν βασική συνιστώσα διαφορετικών τύπων δομών δεδομένων που χρησιμοποιούνται στο bitcoin, όπως για παράδειγμα είναι τα merkle trees.

Το RIPEMD-160 είναι μια κρυπτογραφική συνάρτηση κατακερματισμού, η οποία βασίζεται στην δομή Merkle-Damgard για την οποίας η συνάρτηση συμπίεσης h θα πρέπει να ικανοποιεί τον παρακάτω τύπο:

∀ 1≤ i ≤ n : H_i=h(H_{i-1},m_{i-1}) Θα ισχύει H(m)=H_n , (όπου H συνάρτηση κατακερματισμού)



+

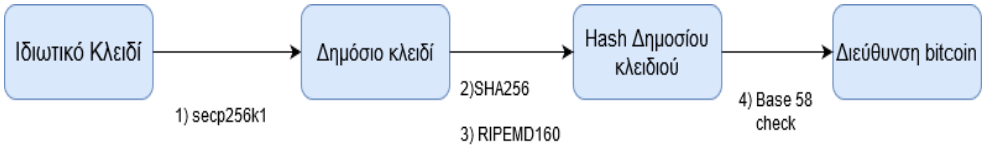
Εικόνα 15:Διαδικασία εφαρμογής συνάρτησης κατακερματισμού RIPEMD-160

Η δομή αυτή αφορά οποιαδήποτε συνάρτηση κατακερματισμού (MD5, SHA256, SHA 512, WHIRLPOOL κ.α.) αλλά στην περίπτωση της συνάρτησης RIPEMD-160 έχουμε μια είσοδο 512 bits σπασμένη σε μπλοκ, ενώ η τιμή κατακερματισμού ως αποτέλεσμα είναι 160 bits.

2.7.1 Δημόσια και ιδιωτικά κλειδιά

Η ασύμμετρη κρυπτογραφία έχει καταστεί ζωτικής σημασίας για μεγάλα συστήματα που υποστηρίζουν το διαδίκτυο. Η κρυπτογραφία δημοσίου κλειδιού όπως αλλιώς ονομάζεται επιτρέπει σε οποιονδήποτε να κρυπτογραφεί εύκολα ένα μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη, το οποίο είναι γνωστό σε οποιονδήποτε. Το μήνυμα μπορεί στην συνέχεια να αποκρυπτογραφηθεί χρησιμοποιώντας το ιδιωτικό κλειδί του παραλήπτη, το οποίο θα πρέπει όμως να είναι διαθέσιμο μόνο στον παραλήπτη (Reisman, 2019). Η ασύμμετρη κρυπτογραφία έχει καταστεί ζωτικής σημασίας και στην εφαρμογή τεχνολογιών blockchain και ειδικότερα στα κρυπτονομίσματα. Για παράδειγμα, με την εγγραφή σε ένα πορτοφόλι bitcoin

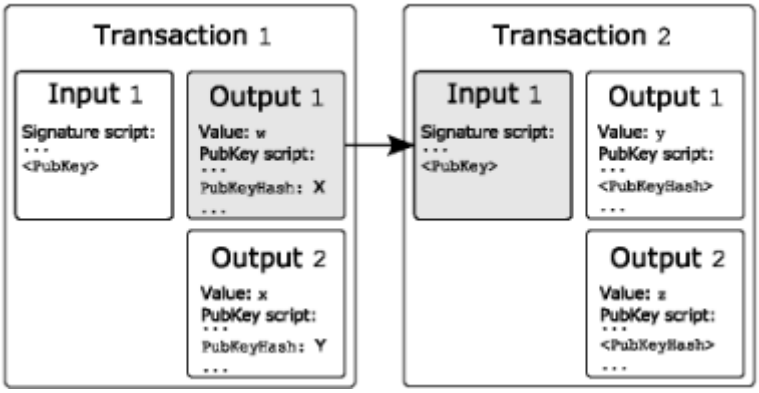
δημιουργείται ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί καθώς και μια διεύθυνση bitcoin. Η διεύθυνση bitcoin αντιστοιχεί στο δημόσιο κλειδί αποτελώντας μια συμπιεσμένη έκδοση του και ουσιαστικά είναι η ταυτότητα του πορτοφολιού από το οποίο θα ληφθούν χρήματα τα οποία μπορούν στην συνέχεια να σταλούν σε άλλες διευθύνσεις. Για την ακρίβεια μια διεύθυνση bitcoin αποτελεί τον κατακερματισμό του δημόσιου κλειδιού με την συνάρτηση sha-256. Με άλλα λόγια, το δημόσιο κλειδί έχει ένα ρόλο σαν ένα όνομα χρήστη, ενώ το ιδιωτικό σαν ένα κωδικό πρόσβασης. Ένα ιδιωτικό κλειδί στο bitcoin είναι ένας τυχαίος αριθμός 256-bit που δημιουργείται από μια τυχαία γεννήτρια. Από αυτό ένας χρήστης μπορεί να δημιουργήσει ένα δημόσιο κλειδί και μια διεύθυνση bitcoin.



Εικόνα 16:Διαδικασία εύρεσης δημοσίου κλειδιού από ιδιωτικό κλειδί

Κάθε είσοδος προσδιορίζει μια διεύθυνση bitcoin που παρέχει τα χρήματα και μια μη χρησιμοποιημένη συναλλαγή που έχει λάβει η διεύθυνση στο παρελθόν. Ομοίως κάθε έξοδος αντιπροσωπεύει τη διεύθυνση bitcoin που λαμβάνει τα χρήματα και το ποσό που λαμβάνει η διεύθυνση. Ειδικότερα η είσοδος μιας συναλλαγής προέρχεται από μια αχρησιμοποίητη έξοδο. Η διαφορά του ποσού μεταξύ της εισόδου και της εξόδου είναι το τέλος συναλλαγής, το οποίο θα κερδίσει ο εξ ορυκτής ενός νέου bitcoin (Wang, Chen, & Zhang, 2021). Κάθε είσοδος περιέχει επίσης μια ψηφιακή υπογραφή, που αποδεικνύει ότι ο κάτοχός αυτής της διεύθυνσης επιτρέπει την ολοκλήρωση της συναλλαγής. Με άλλα λόγια, η πρόσβαση και η κατανάλωση του UTXO επιτυγχάνεται μέσω ψηφιακής υπογραφής. Έτσι μόνο οι «σωστές» (επικυρωμένες) ψηφιακές υπογραφές δικαιούνται να ξεκλειδώσουν το περιεχόμενο των χαρακτηριστικών, στην περίπτωση του bitcoin μιας διεύθυνσης. Όταν ένας χρήστης παρέχει την διεύθυνση εξόδου πραγματοποιεί και ένα σενάριο. Τότε μόνο με το ξεκλείδωμα αυτού του σεναρίου με το ιδιωτικό κλειδί του χρήστη μπορεί να ξεκλειδωθεί και να χρησιμοποιηθεί η αξόδευτη αυτή συναλλαγή UTXO (Chepurnoy, Papamanthou, Zhang, & Srinivasan, n.d.). Τέλος μια συναλλαγή μπορεί να δημιουργηθεί από οποιοδήποτε χρήστη στο blockchain δίκτυο που κατέχει UTXO.

Ωστόσο για να πραγματοποιηθεί μια συναλλαγή αποτελεσματικά πρέπει να επαληθευτεί από το δίκτυο blockchain μέσω της υπογραφής και επικύρωσης συναλλαγών.



Εικόνα 17:UTXO της συναλλαγής 1, ως είσοδος για την συναλλαγή 2

2.7.2 Υπογραφή και επικύρωση συναλλαγών

Κάθε είσοδος συναλλαγής περιέχει μια υπογραφή που περιέχει απόδειξη ότι ο κάτοχος της διεύθυνσης αποστολής έχει εξουσιοδοτήσει την συναλλαγή. Η υπογραφή αυτή δημιουργείται και κρυπτογραφείται εφαρμόζοντας τον αλγόριθμο ψηφιακής υπογραφής ελλειπτικής καμπύλης (ESDSA), ένα κρυπτογραφικό αλγόριθμο που λαμβάνει τα δεδομένα το ιδιωτικό κλειδί και τα δεδομένα συναλλαγών ως εισόδους (Cui, Pan, & Sun, 2019).

Εικόνα 18:Διαδικασία κρυπτογράφησης για την δημιουργία ψηφιακής υπογραφής

Όταν όλοι οι κόμβοι επαληθεύουν την συναλλαγή μπορούν εύκολα να επαληθεύσουν την εγκυρότητα της υπογραφής, εφαρμόζοντας μια διαδικασία επαλήθευσης ECDSA, όπως φαίνεται στο παρακάτω σχήμα.

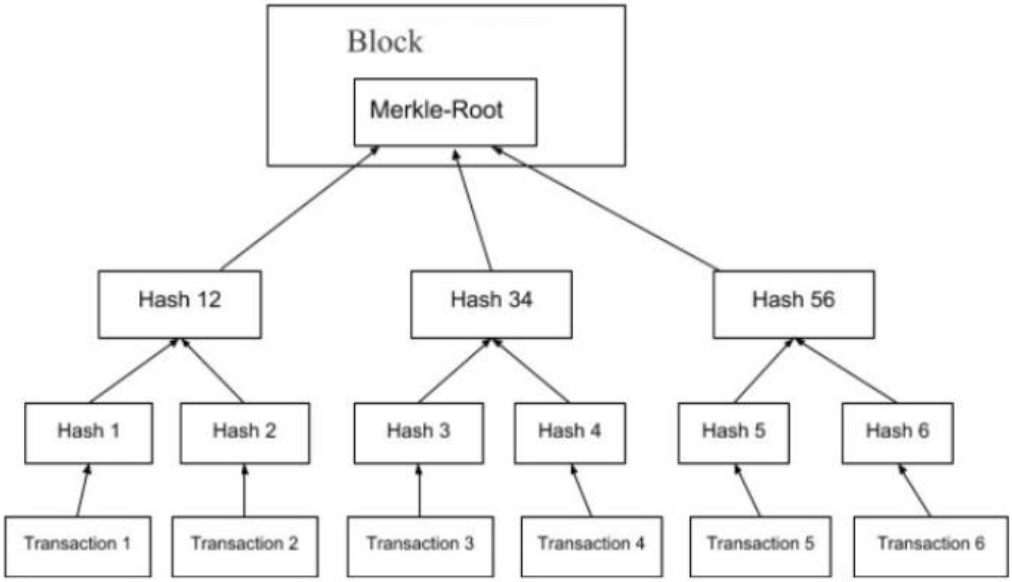
Εικόνα 19:Επικύρωση υπογραφής στην συναλλαγή

Καταλήγοντας, οι ψηφιακές υπογραφές είναι ουσιαστικά σαν μια υπογραφή στο έγγραφο. Αυτό εγγυάται ότι ο δημιουργός μιας συναλλαγής είναι πράγματι το άτομο που κατέχει το ιδιωτικό κλειδί. Συνεπώς, η ψηφιακή υπογραφή είναι βασικός παράγοντας για τις συναλλαγές στο blockchain (Vokerla et al., 2019) Κάθε συναλλαγή έχει διαφορετική ψηφιακή υπογραφή που βασίζεται στο ιδιωτικό κλειδί του χρήστη. Επιπλέον μόλις ο ιδιοκτήτης υπογράψει την συναλλαγή αυτή αποστέλλεται σε μια «δεξαμενή μνήμης» (mempool), την οποία επεξεργάζονται ανθρακωρύχοι προκειμένου να αποφασίσουν ποιες συναλλαγές θα εντάξουν στο νέο μπλοκ. Επιπλέον, ο ανθρακωρύχος χρησιμοποιεί το κοινό κλειδί του αποστολέα προκειμένου να εγγυηθεί ότι η ψηφιακή υπογραφή είναι αυθεντική. Έτσι, μόλις η ιδιοκτησία και η ψηφιακή υπογραφή επαληθεύεται, η συναλλαγή προστίθεται στο επόμενο μπλοκ και τα χρήματα ανταλλάσσονται από το ένα πορτοφόλι στο άλλο.

2.7.3 Δομή δεδομένων Merkle Trees

Η συγκεκριμένη δομή έχει σκοπό όταν ένας κόμβος στο δίκτυο θέλει να διασφαλίσει ότι έχει ακριβώς ίδιο σύνολο συναλλαγών με κάθε άλλο συμμετέχοντα κόμβο στο blockchain δίκτυο. Με αυτό τον τρόπο αποφεύγεται η ανάγκη για έλεγχο κάθε συναλλαγής ξεχωριστά. Το μόνο που απαιτείται είναι η σύγκριση της ρίζας Merkle με την ρίζα κάθε άλλου κόμβου. Το γεγονός αυτό μπορεί να επιτρέψει την ύπαρξη “lightweight” πελατών λογισμικού που δεν απαιτούν την αποθήκευση ολόκληρου του blockchain για την επικύρωση των δικών τους συναλλαγών. Για τον υπολογισμό της ρίζας merkle, δημιουργούμε αρχικά την δομή ενός δέντρου merkle, στο οποίο τα φύλλα είναι οι συναλλαγές στο τρέχων μπλοκ. Το παρακάτω σχήμα δείχνει την δομή ενός δέντρου Merkle. Ο κατακερματισμός $Hash_1$ είναι για την transaction 1, ενώ ο κατακερματισμός $Hash_2$ για την transaction 2. Ο Κατακερματισμός $Hash_{12}$= $Hash_{1+2}$= $Hash_1$ + $Hash_2$

$\Rightarrow Hash_{1+2}$ = SHA256 SHA256(($Hash_1$+ $Hash_2$)), δεδομένου ότι στην συνάρτηση κατακερματισμού για το bitcoin εφαρμόζεται 2 φορές η συνάρτηση SHA-256.



Εικόνα 20:Διάγραμμα Ροής δέντρου Merkle

2.8 Είδη Blockchain

2.8.1 Δημόσια Blockchain

Όπως υποδηλώνει το όνομα, το συγκεκριμένο είδος blockchain δίνει την δυνατότητα σε οποιονδήποτε κόμβο να συμμετάσχει στην διαδικασία λήψης αποφάσεων σχετικά με το δίκτυο, ενώ ανάλογα το σύστημα και την προσφορά τους στο σύστημα ως προς την δημιουργία νέων μπλοκ υφίσταται η διαδικασία ανταμοιβής στους χρήστες. Με άλλα λόγια, η κατανεμημένη βάση δεδομένων που συνθέτει την αλυσίδα των μπλοκ είναι προσβάσιμη σε οποιονδήποτε το επιθυμεί με ίσους όρους, ενώ όλοι οι συμμετέχοντες κόμβοι διατηρούν ένα αντίγραφο του λογιστικού καθολικού που έχει διαμορφωθεί μέχρι εκείνη την στιγμή, ενώ με την εφαρμογή ενός κατάλληλου μηχανισμού συναίνεσης διατηρείται η ασφάλεια και η επέκταση της αλυσίδας των μπλοκ (Yaga et al., 2018). Συνεπώς υπάρχει δικαιοσύνη και πλήρης διαφάνεια μεταξύ των κόμβων, ενώ παράλληλα λόγω της αποκεντρωμένης και κατανεμημένης αρχιτεκτονικής είναι πολύ ασύμφορο να ελεγχθεί πλήρως το δίκτυο από κάποιον μόνο κόμβο.

2.8.2 Ιδιωτικά blockchain

Αντίστοιχα τα ιδιωτικά blockchain είναι προσβάσιμα μόνο σε κόμβους που έχουν ειδική άδεια από τον διαχειριστή του δικτύου για την συμμετοχή τους σε αυτό, χάνοντας έτσι σε ένα βαθμό αυτού του είδους το blockchain την αποκεντρωμένη αρχιτεκτονική του. Συνεπώς το συγκεκριμένο είδος εφαρμόζεται σε οργανισμούς που θέλουν να εκφυλίσουν την πιθανότητα κινδύνου ως προς την έκθεση δεδομένων τους όπως θα συνέβαινε στην περίπτωση των τραπεζών ή κάποιας μεγάλου μεγέθους επιχείρησης. Ένα από τα πιο σημαντικά παραδείγματα ιδιωτικών blockchain είναι το Ripple.

2.9 Μοντέλα συναίνεσης

Τα μοντέλα συναίνεσης αποτελούν ουσιαστικά αλγορίθμους που βοηθούν ένα κατανεμημένο ή αποκεντρωμένο δίκτυο μέσω ενός ομόφωνου τρόπου να λαμβάνονται έγκυρες αποφάσεις σχετικά με τι ποιοι χρήστες του δικτύου θα μπορούν να δημοσιεύουν ένα νέο μπλοκ. Σε κάθε blockchain υπάρχει δημοσιοποιημένο ένα πρώτο μπλοκ με την ονομασία “genesis block” και κάθε νέο μπλοκ συνδέεται με ένα προηγούμενο δημιουργώντας μια αλυσίδα η οποία υπακούει συνολικά σε ένα προσυμφωνημένο μοντέλο. Οι αποφάσεις λοιπόν αυτές λαμβάνονται με την υλοποίηση κάποιων εκ των μοντέλων ομοφωνίας (Crosby, 2016). Με άλλα λόγια, πολλές φορές για την προσθήκη ενός μπλοκ σε ένα blockchain απαιτείται μια κοινή συμφωνία μεταξύ των κόμβων η οποία διαφέρει ανάλογα με το είδος του blockchain.

Η διαδικασία της εξόρυξης έχει σκοπό την δημιουργία μπλοκ που θα προσαρτηθούν στη αποκεντρωμένη βάση δεδομένων του blockchain. Σε κάποιες από τις εφαρμογές blockchain όπως είναι και το bitcoin ο ανθρακωρύχος που δημιουργεί το πρώτο έγκυρο μπλοκ ανταμείβεται οικονομικά από το σύστημα. Η εξόρυξη αποτελεί μια κρίσιμη έννοια για τις blockchain τεχνολογίες, επιτρέποντας σε ένα κόμβο την δημιουργία μπλοκ, τα οποία επικυρώνονται στην συνέχεια ή όχι από τους υπόλοιπους κόμβους του δικτύου. Έτσι λοιπόν αν το νέο μπλοκ κριθεί ως έγκυρο πραγματοποιείται επισύναψη στην βάση δεδομένων. Ως κόμβους εξόρυξης καλούμε τους κόμβους που διεκδικούν την δημιουργία ενός νέου μπλοκ, οι οποίοι αγωνίζονται για την επικύρωση των συναλλαγών με στόχο την ταχύτερη δημιουργία αυτού σε σχέση με τους ανταγωνιστές προκειμένου να επωφεληθούν

της ανταμοιβής που προβλέπει η διαδικασία. Για τον σκοπό αυτό υπάρχουν διαφορετικές λύσεις οι οποίες έχουν τον χαρακτηρισμό ως μοντέλα συναίνεσης. Παρακάτω αναλύονται τα μοντέλα με την μεγαλύτερη εφαρμογή:

2.9.1 Proof of Work

Ο συγκεκριμένος τύπος μηχανισμού συναίνεσης στηρίζεται στην απόδειξη ότι έχουν δαπανηθεί αρκετοί πόροι υπολογισμού, πριν προταθεί μια τιμή "Nonce" η οποία θα είναι αποδεκτή από το δίκτυο. Ο συγκεκριμένος μηχανισμός εφαρμόζεται σε bitcoin καθώς και άλλα κρυπτονομίσματα. Πρέπει να τονιστεί ότι αποτελεί τον μηχανισμό με την μεγαλύτερη αποτροπή ως προς επιθέσεις Sybil (Kaur, Chaturvedi, Sharma, & Kar, 2021). Στην εξόρυξη κρυπτονομισμάτων, στο μοντέλο proof of work χρησιμοποιείται μια συνάρτηση κατακερματισμού (στην περίπτωση του bitcoin ο SHA-256 αλγόριθμος) με στόχο την επαλήθευση δεδομένων. Έτσι η διαδικασία του αλγορίθμου εξόρυξης έχει ως εξής:

- Ο προηγούμενος κατακερματισμός μπλοκ μπορεί να ανακτηθεί από το δίκτυο του bitcoin.
- Ένα σύνολο πιθανών συναλλαγών που μεταδίδεται εντός του δικτύου συσσωρεύεται σε κάθε μπλοκ.
- Υπολογίζεται ο διπλός κατακερματισμός με εφαρμογή αλγορίθμου sha-256 της κεφαλίδας μπλοκ μέχρις ότου βρεθεί κατάλληλη τιμή "nonce". Για την εύρεση της τιμής nonce θεωρούμε την ανίσωση $H(n \| H(b)) < t$ όπου H είναι η συνάρτηση κατακερματισμού, t μικρότερη τιμή της συνάρτησης κατακερματισμού και b το τρέχων μπλοκ (Dinh et al., 2018).
- Αν το αποτέλεσμα του κατακερματισμού είναι μικρότερο της τιμής "difficulty" η διαδικασία σταματά. Αντίθετα επαναλαμβάνεται η διαδικασία αυξάνοντας την τιμή "nonce".

Αναλυτικότερα, κάθε περίπου 10 λεπτά, ένα νέο μπλοκ συναλλαγών bitcoin επιβεβαιώνεται από ένα ανθρακωρύχο. Όπως είναι λογικό επειδή στο δίκτυο υπάρχει ένας μεγάλος αριθμός ανθρακωρύχων προκύπτει η ανάγκη ενός τρόπου συναίνεσης μεταξύ αυτών για το ποιος τελικά θα εκδώσει ένα νέο μπλοκ. Η προϋπόθεση για την δημιουργία ενός νέου μπλοκ από ένα ανθρακωρύχο είναι να δημιουργήσει ένα κατακερματισμό δεδομένων του οποίου το αποτέλεσμα θα θεωρηθεί έγκυρο από το υπόλοιπο δίκτυο. Για να επιτευχθεί κάτι τέτοιο θα πρέπει το αποτέλεσμα αυτό να είναι μικρότερο από το

λεγόμενο τρέχων στόχο δικτύου. Ο στόχος αυτός διαρκώς μεταβάλλεται, ενώ γίνεται και όλο και πιο δύσκολος να επιτευχθεί με την έννοια ότι θα απαιτείται περισσότερη υπολογιστική ισχύς (hash power) από τους εξ ορυκτές. Ο τύπος που ορίζει τον νέο στόχο δικτύου είναι ο παρακάτω:

$$\text{Νέος στόχος} = \text{Τρέχων στόχος} \times \frac{\textit{Χρόνος που απαιτείται για την παραγωγή 2016 μπλοκ}}{\textit{20160 λεπτα}}$$

Με τον όρο "difficulty" εννοούμε την προσπάθεια ενός ανθρακωρύχου να δημιουργήσει κάποιο block βρίσκοντας κάποιο αποτέλεσμα κατακερματισμού το οποίο θα είναι μικρότερο από τον τρέχων στόχο μέχρι εκείνη στιγμή, ενώ η μεταβλητή αυτή διαμορφώνεται κάθε 2016 μπλοκ ή χρονικά κάθε 2 περίπου εβδομάδες. Θα ήταν χρήσιμο ένα σχετικό παράδειγμα ως προς την πιθανότητα εύρεσης του, ενώ ο μαθηματικός τύπος του είναι:

$$\text{Difficulty} = \frac{\textit{Τρέχων στόχος}}{\textit{Μέγιστος στόχος}}$$, όπου τρέχων στόχος = προηγούμενος στόχος * $\frac{\textit{Χρόνος σε δευτερόπλεπτα που χρειάστηκε για την παραγωγή 2016 μπλοκ}}{\textit{1.209.600 δευτερόλεπτα}}$

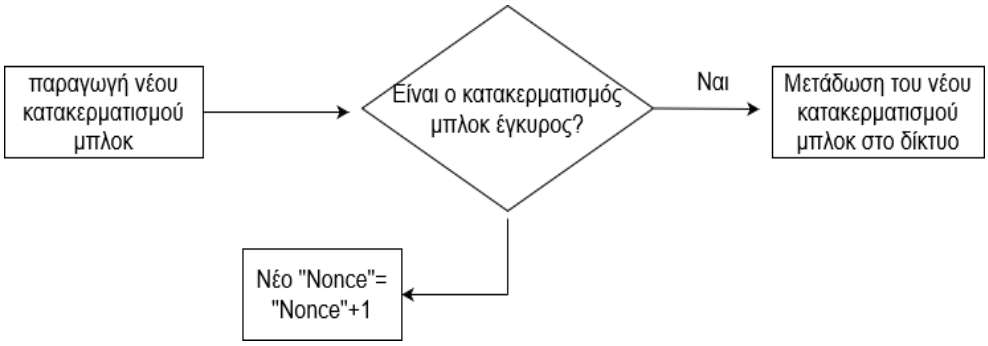
και όπου μέγιστος είναι ό στόχος που ορίστηκε για την δημιουργία του αρχικού μπλοκ (μπλοκ 0), οποίος είναι: `00000000ffff0000000000000000000000000000000000000000000000000000`

Έστω λοιπόν ότι ο τρέχων στόχος είναι:

`0000000000000000000ffaa0000000000000000000000000000000000`

Ο παραπάνω στόχος αποτελείται από 64 δεκαεξαδικούς αριθμούς, ενώ παρατηρούμε ότι οι πρώτοι 19 είναι το δεκαεξαδικό 0. Έτσι όλοι οι πιθανοί συνδυασμοί για τα 64 ψηφία είναι: $16 \times \ldots \times 16 = 16^{64} \approx 1.1579 \times 10^{77} \approx 10^{77}$, ενώ οι πιθανοί συνδυασμοί κατακερματισμών με τα έγκυρα αποτελέσματα θα είναι: $16 \times 16 \times \ldots \times 16 = 16^{64-19} \approx 2 \times 10^{55}$. Συνεπώς η πιθανότητα εύρεσης ενός έγκυρου μπλοκ εκφράζεται από το παρακάτω κλάσμα: $\frac{2 \times 10^{55}}{10^{77}} = 2 \times 10^{-22}$, όπου διαπιστώνουμε ότι είναι μια υπερβολικά μικρή πιθανότητα. Τέλος, να σημειωθεί ότι όταν δημιουργείται ένα νέο μπλοκ

δημιουργείται επίσης ένα νέο bitcoin, ενώ με την δημιουργία 210.000 μπλοκ η επιβράβευση μπλοκ μειώνεται στο μισό. Το φαινόμενο αυτό που είναι γνωστό ως “halving” σύμφωνα με το οποίο η ανταμοιβή ενός ανθρακωρύχου θα μειώνεται στο μισό επαναλαμβανόμενα κάθε 4 χρόνια έως ότου εξ ορυχθούν 21 εκατομμύρια συνολικά bitcoin, το οποίο υπολογίζεται να συμβεί το έτος 2140. Το λεπτό σημείο είναι ότι το αποτέλεσμα του κατακερματισμού μπλοκ με εφαρμογή το αλγορίθμου SHA-256 που θα εμπεριέχει ένα συγκεκριμένο αριθμό δεκαεξαδικών μηδέν θα πρέπει να συμπίπτει με τον αριθμό των δεκαεξαδικών μηδέν του επόμενου μπλοκ για να θεωρηθεί σε πρώτη φάση ένα μπλοκ ως έγκυρο. Έτσι όταν κατοχυρωθεί ένα νέο μπλοκ ως έγκυρο ο ανθρακωρύχος του μπλοκ αυτού μεταδίδει τον κατακερματισμό μπλοκ και στους υπόλοιπους ανθρακωρύχους του δικτύου, ενώ ο πρώτος που θα το καταφέρει καρπώνεται την ανταμοιβή.



Εικόνα 21:Διαδικασία παραγωγής νέου κατακερματισμού μπλοκ

Τέλος ένας ανθρακωρύχος για να συμπεριλάβει τελικά κάποιο καινούριο μπλοκ στην αλυσίδα θα πρέπει να ελέγξει αρχικά ότι το μπλοκ είναι έγκυρο και ότι όλες οι συναλλαγές στο μπλοκ είναι έγκυρες. Αυτό επιτυγχάνεται με την επιβεβαίωση των υπογραφών δεδομένων για το ξεκλείδωμα των εξόδων συναλλαγών.

Για να καταλάβουμε καλύτερα την παραπάνω διαδικασία αναφέρουμε ένα παράδειγμα δημιουργίας και επιβεβαίωσης μιας ψηφιακής συναλλαγής. Έστω ότι η Αλίκη στέλνει μια συναλλαγή και θέλει να αποδείξει ότι είναι η συναλλαγή προέρχεται από την ίδια. Για τον σκοπό αυτό δημιουργεί μια ψηφιακή υπογραφή. Αρχικά κατακερματίζει τα δεδομένα και στην συνέχεια χρησιμοποιεί το ιδιωτικό της κλειδί για να κρυπτογραφήσει τον κατακερματισμό. Ο κρυπτογραφημένος κατακερματισμός με χρήση του ιδιωτικού κλειδιού καλείται ψηφιακή υπογραφή. Έστω τώρα ότι ο Μπομπ είναι ο παραλήπτης της συναλλαγής. Η Αλίκη στέλνει την συναλλαγή και ειδικότερα τον κατακερματισμό όλων των δεδομένων της συναλλαγής συμπεριλαμβανομένου της εξόδου συναλλαγής την οποία θέλουμε να ξεκλειδώσουμε, μαζί με την ψηφιακή υπογραφή. Να τονίσουμε ότι η Ψηφιακή

Υπογραφή είναι ο πολλαπλασιασμός ενός τυχαίου αριθμού r όπου θα αποτελεί τον συντελεστή x ενός τυχαίου σημείου μιας ελλειπτικής καμπύλής πολλαπλασιασμένο με το ιδιωτικό κλειδί της Αλίκης. Στο σημείο αυτό ακολουθεί η διαδικασία επικύρωσης της ψηφιακής υπογραφής από τον Μπομπ.

Ο Μπομπ αποκρυπτογραφεί την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί της Αλίκης. Το αποτέλεσμα είναι η τιμή κατακερματισμού της συναλλαγής (Κατακερματισμός Α)

- Ο Μπομπ εφαρμόζει ξανά τον αλγόριθμο ασύμμετρης κρυπτογράφησης για την συναλλαγή που έχει λάβει (Κατακερματισμό Β).
- Ο Μπομπ συγκρίνει τις 2 τιμές κατακερματισμού
- Αν οι τιμές αυτές ταιριάζουν θεωρούμε την συναλλαγή ως έγκυρη.

Τα παραπάνω συνοψίζονται με τους μαθηματικούς τύπους:

- Η Αλίκη δημιουργεί αρχικά την ψηφιακή υπογραφή: ENC(H(p), priv Key_{Alice}) = digital sign
- Ο Μπομπ επικυρώνει την ψηφιακή υπογραφή: DEC (sign, pub key_{Alice}) = hash
- Θα πρέπει να ισχύει H(p)=hash

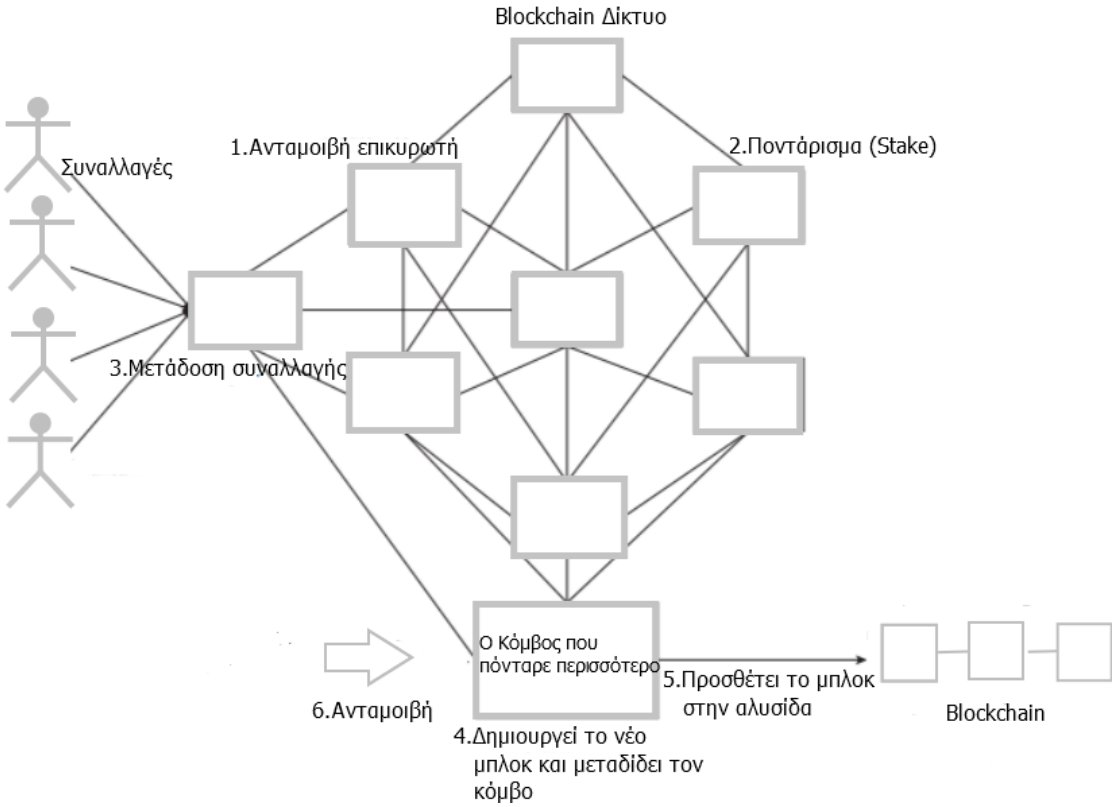
Με τον τρόπο αυτό επιτυγχάνεται το ξεκλείδωμα των εξόδων συναλλαγών για να θεωρηθούν έγκυρες και σε συνδυασμό με την επικύρωση ενός μπλοκ ως έγκυρο με τρόπο που έχει αναλυθεί παραπάνω είναι δυνατό ένα νέο μπλοκ να προστίθεται στην αλυσίδα.

Τέλος, το βασικό χαρακτηριστικό είναι ότι μπορεί να είναι δύσκολο να βρεθεί λύση στο κρυπτογραφικό αυτό πρόβλημα, αλλά είναι εξαιρετικά εύκολο να επαληθευτεί (Kaur et al., 2021). Ως εκ τούτου, το θετικό είναι ότι μόλις δημιουργηθεί ένας κατακερματισμός μπορεί να επαληθευτεί εύκολα και η συναίνεση επιτυγχάνεται εύκολα.

2.9.2 Proof of Stake

Το συγκεκριμένο μοντέλο συναίνεσης αποτελεί βελτιωμένη έκδοση του μοντέλου "proof of work" με την έννοια ότι περιορίζεται η ανάγκη της εξόρυξης. Το "Proof of Stake" αποτελεί μια διαφορετική φιλοσοφία σχεδιασμού blockchain. Στο "Proof of Stake" μοντέλο υπάρχει ένα σύνολο επικυρωτών που συμμετέχουν στην διαδικασία παραγωγής μπλοκ μέσω της κατάθεσης κάποιου ποσού και συνεπώς ο όρος ανθρακωρύχος αντικαθίσταται από τον όρο επικυρωτή. Έτσι σε αυτόν τον σχεδιασμό παρατηρούμε ότι δεν υπάρχουν υψηλές απαιτήσεις υπολογιστικής ισχύς όπως στην περίπτωση του μοντέλου

“proof of work”. Ένας επικυρωτής λοιπόν, επενδύει στα νομίσματα του δικτύου blockchain και για την δημιουργία ενός νέου μπλοκ αυτό που πρέπει να αποδείξει για την απόδοση εξορυκτικής ισχύ αφορά την ιδιοκτησία του ποσού του νομίσματος. Ειδικότερα, ο μεμονωμένος κόμβος που δημιουργεί το επόμενο μπλοκ επιλέγεται με βάση το ποσοστό που έχουν στοιχηματίσει σε αυτόν σε σχέση με τους ανταγωνιστές κόμβους. Με άλλα λόγια ένας “proof of stake” ανθρακωρύχος κάνει εξόρυξη ενός ποσοστού των συναλλαγών οι οποίες αντιστοιχούν στο ποσοστό της ιδιοκτησίας του, με την έννοια ότι θα έχει πρόσβαση σε μια ορισμένη ποσότητα νομισμάτων ώστε να δημιουργηθεί ένα νέο μπλοκ το οποίο θα είναι αποδεκτό από το δίκτυο. Η παραπάνω λογική στηρίζεται στο γεγονός ότι τα άτομα που κατέχουν τα περισσότερα νομίσματα είναι λιγότερο πιθανό να πραγματοποιήσουν επίθεση στο δίκτυο. Γίνεται αντιληπτό όμως αυτός που θα επωφελείται σε μόνιμη βάση μέσω των ανταμοιβών θα είναι αυτός που θα έχει στην κατοχή του το μεγαλύτερο ποσοστό νομισμάτων. Σε αυτό το πρόβλημα δικαιοσύνης που προκύπτει, υπάρχουν κάποιες προτάσεις λύσεων (Zheng, Xie, Dai, Chen, & Wang, n.d.).



Εικόνα 22:Διαδικασία μοντέλου συναίνεσης “Proof of Stake”

Ιδιαίτερα, η πρόταση στο “Blackcoin” εστιάζει στην αναζήτηση της μικρότερης τιμής κατακερματισμού, ενώ το “Peercoin” ευνοεί την επιλογή νομισμάτων βάσει ηλικίας και έτσι προγενέστερα χρονικά νομίσματα έχουν περισσότερες πιθανότητες ως προς την εξόρυξη κάποιου μπλοκ. Ειδικότερα, το μοντέλο συναίνεσης “Proof of Stake” αντιμετωπίζει το πρόβλημα μιας διακλάδωσης στην αλυσίδα με κίνδυνο την δημιουργία μιας “double spending” επίθεσης όπως ισχύει για το “Proof of Work”, ενώ κύριο χαρακτηριστικό της είναι ότι η τιμή “difficulty” γίνεται μικρότερη όσο μεγαλώνει το συνολικό ποσοστό νομισμάτων στο δίκτυο από ένα επικυρωτή. Ως “difficulty” στην προκειμένη περίπτωση χαρακτηρίζεται το απαιτούμενο ποσό νομισμάτων το οποίο ορίζεται από το δίκτυο του blockchain (Dinh et al., 2018). Θεωρούμε την συνάρτηση S ως αυτή που αντιστοιχεί στην τιμή του πονταρίσματος, n είναι η τιμή nonce και M ως τον επικυρωτή-ανθρακωρύχο, ο οποίος για να παράγει ένα νέο μπλοκ υπακούει στην παρακάτω ανίσωση:

$H(n \| H(b)) < S(M) * t,$

όπου t μικρότερη δυνατή τιμή της συνάρτησης κατακερματισμού

Γίνεται λοιπόν αντιληπτό ότι όσο μεγαλύτερη είναι η τιμή της συνάρτησης S, τόσο μεγαλύτερο θα είναι το σύνολο στο οποίο μπορεί να βρεθεί η τιμή nonce και συνεπώς θα είναι πιο εύκολη η εύρεση της.

Λαμβάνοντας υπόψη ότι τα κρυπτονομίσματα που εφαρμόζουν “Proof of Stake” ως μοντέλο συναίνεσης βασίζονται στο “coinage”, όπου αποτελεί ένα παράγοντα που αυξάνει το «βάρος» των αχρησιμοποίητων νομισμάτων γραμμικά με την πάροδο του χρόνου (Vasin, n.d.). Για να προκύψει έτσι ένα νέο μπλοκ θα πρέπει να ικανοποιείται η παρακάτω συνθήκη:

Hash(blockcheader) < coinage * target,

όπου Coinage = number of coins * remaining usage of coin

Καταλήγοντας, θα αναφέρουμε στα θετικά στην μειωμένη κατανάλωση ενέργειας καθώς σε ένα “Proof of Stake” σύστημα δεν χρειάζεται να λυθεί κάποιο δύσκολο υπολογιστικό πρόβλημα. Για την ακρίβεια μειώνει την κατανάλωση ενέργειας κατά 99%, σε σχέση με το “Proof of Work” (Kaur et al., 2021). Με αυτή την έννοια, οι επικυρωτές μπλοκ δεν χρειάζεται να αγχώνονται για φθηνή ηλεκτρική ενέργεια αυξάνοντας έτσι το πρόσφορο έδαφος ως προς την επικύρωση του δικτύου.

2.9.3 Delegated Proof of Stake

Το συγκεκριμένο μοντέλο συναίνεσης εφαρμόζει μια δομή όπου η παραγωγή μπλοκ χαρακτηρίζεται από μια σταθερά με την έννοια ότι είναι περιορισμένη όπως κατά επέκταση και ο αριθμός των κόμβων που επικυρώνουν και στην συνέχεια παράγουν τα μπλοκ είναι συγκεκριμένος. Οι επικυρωτές μπλοκ σε αυτή την περίπτωση καλούνται “Witnesses”. Πιο συγκεκριμένα, στο DPoS μοντέλο ένας κόμβος επιλέγεται ως “witness” με βάση το «στοίχημα» του. Οι κόμβοι δηλαδή που συμμετέχουν στην διαδικασία της δημιουργίας νέου μπλοκ και πήραν το μεγαλύτερο ποσοστό ψήφων έχουν το λογιστικό δικαίωμα. Έτσι λοιπόν οι κόμβοι που χαρακτηρίζονται ως εκλεγμένοι μάρτυρες δημιουργώντας ένα νέο μπλοκ, όπως και στα υπόλοιπα μοντέλα επιδέχονται ανταμοιβής (Mingxiao, Xiaofeng, Zhe, Xiangwei, & Qijun, 2017), ενώ μερικές από τις βασικότερες εφαρμογές τους είναι πρωτόκολλα όπως το Lisk, Steem και Eos. Αναλυτικότερα, ένας υποψήφιος δημιουργός μπλοκ κόμβος, για να μπορέσει να είναι “witness” θα πρέπει να ψηφιστεί από τους υπόλοιπους κόμβους του δικτύου τους λεγόμενους “token holders”. Στο σημείο αυτό, θα πρέπει να τονιστεί ότι ψηφίζεται από τους συμμετέχοντες κόμβους στο δίκτυο ποιος κόμβος θέλουν να δημιουργήσει το νέο μπλοκ ενώ η ισχύς των ψήφων τους στηρίζεται στον αριθμό των νομισμάτων (πονταρίσματα) που κάθε κόμβος κατέχει. Ωστόσο, υπάρχει η δυνατότητα οι κόμβοι να μπορούν να στέλνουν σε άλλους τα νομίσματα τους, τεχνική που περιορίζει τους υποψήφιους δημιουργούς μπλοκ σε ένα σύστημα, αριθμός ο οποίος προκαθορίζεται από το σύστημα.

Πίνακας 3: Συγκριτικός πίνακας μοντέλων συναίνεσης

PoW	PoS	DPoS
Η διαδικασία δημιουργίας μπλοκ ονομάζεται ανθρακωρύχοι	Η διαδικασία δημιουργίας μπλοκ ονομάζεται επικυρωτές	Η διαδικασία δημιουργίας μπλοκ επιτυγχάνεται μόνο από εκλεγμένους παραγωγούς μπλοκ
Ανθρακωρύχοι με περισσότερη ισχύ κατακερματισμού είναι πιθανότερο να εξορύξουν το επόμενο μπλοκ	Επικυρωτές με μεγαλύτερο “Coinage” είναι πιο πιθανό να επικυρώσουν το επόμενο μπλοκ	Οι παραγωγοί μπλοκ επιλέγονται από τους ομότιμους κόμβους μέσω συνεχούς ψηφοφορίας
Η διαδικασία της εξόρυξης απαιτεί υψηλή κατανάλωση ενέργειας	Δεν απαιτείται υπολογιστική ισχύς για την δημιουργία μπλοκ	Η ισχύς ψήφου των ομότιμων εξαρτάται από πόσα νομίσματα κατέχουν

2.10 Βασικές ποιοτικές αδυναμίες της τεχνολογίας Blockchain

- **Scalability** (επεκτασιμότητα): Ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζουν οι υλοποιήσεις blockchain είναι η επεκτασιμότητα. Ειδικότερα, για να υπάρχει θεωρητικά μια πιο εγγυημένη ασφάλεια σε ένα blockchain, θα πρέπει το κατανεμημένο δίκτυο να αποτελείται από ένα μεγάλο αριθμό κόμβων, προκειμένου να περιορίζεται η πιθανότητα δημιουργίας ενός λιγότερο αποκεντρωμένου συστήματος(Koteska, Karafiloski, & Mishev, n.d.). Τα όρια επεκτασιμότητας του blockchain συνδέονται με το μέγεθος δεδομένων που εντάσσονται σε ένα μπλοκ, την ταχύτητα συναλλαγών ή την καθυστέρηση (latency) στην μετάδοση δεδομένων. Το πρόβλημα αυτό της καθυστέρησης των υποβολής συναλλαγών αλλά και της αργής επιβεβαίωσης αυτών στην περίπτωση του bitcoin ανέρχεται στο χρονικό διάστημα της μίας ώρας, διότι το διάστημα δημιουργίας μπλοκ είναι 10 λεπτά ενώ η διαδικασία της επικύρωσης απαιτεί την έξι επιβεβαιώσεις, δηλαδή την δημιουργία έξι μπλοκ. Συνολικά λοιπόν, ο χρόνος που απαιτείται είναι 6x10=60 λεπτά. Ο αντίστοιχος χρόνος στο Ethereum είναι 3 λεπτά, διότι ο χρόνος δημιουργίας μπλοκ είναι 14 δευτερόλεπτα, ενώ η διαδικασία της επιβεβαίωσης απαιτεί την

δημιουργία 12 μπλοκ. Συνεπώς ο συνολικός χρόνος θα είναι 14x12=168 δευ. ≅ 3 λεπτά. Ως προς θέμα της ασφάλειας θεωρητικά είναι καλό να απαιτείται περισσότερος χρόνος για την δημιουργία και επικύρωση ενός νέου μπλοκ, προκειμένου να διασφαλίζεται ότι συναλλαγές δεν έχουν χρησιμοποιηθεί στο παρελθόν, έτσι ώστε να αποφεύγονται επιθέσεις διπλής δαπάνης(Rathod & Motwani, 2018). Παρόλα αυτά για λόγους ανταγωνισμού, ο στόχος θα πρέπει να είναι παράλληλος με την έννοια ότι τα συστήματα blockchain θα πρέπει να βελτιώσουν τον χρόνο δημιουργίας και επικύρωσης μπλοκ, διατηρώντας παράλληλα την ασφάλεια.

- **Throughput** (χρόνος διεκπεραίωσης συναλλαγών): Το πρόβλημα στο τρέχων δίκτυο bitcoin είναι ότι επεξεργάζεται περίπου 7 συναλλαγές ανά δευτερόλεπτο ενώ στο Ethereum το αντίστοιχο νούμερο είναι μόλις 20 συναλλαγές ανά δευτερόλεπτο(Koteska et al., n.d.). Το πρόβλημα αυτό μπορεί να γίνει καλύτερα αντιληπτό, αν σκεφτούμε ότι στο δίκτυο συναλλαγών της Visa έχουμε περίπου 2000 συναλλαγές ανά δευτερόλεπτο ή ακόμη και στην περίπτωση του PayPal με το αντίστοιχο νούμερο να είναι περίπου 200 συναλλαγές ανά δευτερόλεπτο. Στο σημείο αυτό να αναφέρουμε ότι, αν θεωρητικά με κάποιο τρόπο το μέγεθος ενός μπλοκ αυξηθεί, ο αριθμός των συναλλαγών που επεξεργάζονται να δευτερόλεπτο θα αυξανόταν.
- **Costs**: Η εφαρμογή του blockchain δεν είναι δωρεάν, χαρακτηριστικό το οποίο αφορά γενικότερα τις αποκεντρωμένες δομές. Η προμήθεια συναλλαγής παίζει τεράστιο ρόλο στην επιλογή των συναλλαγών που θα ενταχθούν σε μπλοκ, αλλά έχει και άμεσο αντίκτυπο στον χρόνο επιβεβαίωσης συναλλαγών (Rathod & Motwani, 2018). Αναλυτικότερα, οι χρήστες πληρώνουν για τις προμήθειες συναλλαγών (transaction fees) και έμμεσα μέσω της υψηλής υπολογιστικής που απαιτείται για την συμμετοχή τους στο δίκτυο. Και σε αυτή την περίπτωση, σε μια αύξηση του μεγέθους μπλοκ και η παράλληλη αύξηση των συναλλαγών που θα μπορούν να συμπεριληφθούν σε αυτό, θα εξανάγκαζε τους ανταγωνιστές του bitcoin σε χαμηλότερα "transactions fees".

3 Μεθοδολογία

Αυτή η ενότητα εξετάζει μερικές σχετικές μελέτες περί της ασφάλειας στο blockchain και προβλημάτων που αντιμετωπίζει η τεχνολογία. Η μελέτη (Dasgupta, Shrein, & Gupta, 2019) παρέχει μια επισκόπηση του συστήματος ασφαλείας blockchain και συγκεκριμένες απειλές που αντιμετωπίζει η τεχνολογία. Τα ζητήματα ασφάλειας περιγράφονται στο πλαίσιο της αποκεντρωμένης φύσης της τεχνολογίας με έμφαση σε προβλήματα που σχετίζονται με την κρυπτογραφία που εφαρμόζεται. Οι (Atzei, Bartoletti, & Cimoli, 2017) παρέχουν μια έρευνα σχετικά με το Ethereum και τα τρωτά σημεία επιτρέπουν τον αντίπαλο να κλέψει χρήματα ή κάποιο άλλο κίνδυνο. Η δουλειά (Prashanth Joshi, Han, Wang, & ,Kennesaw State University, Marietta, GA 30060, USA, 2018, p.) παρουσιάζει μια έρευνα για την ασφάλεια του blockchain, για προβλήματα στην λειτουργία του καθώς και προκλήσεις για το μέλλον. Το άρθρο αυτό αναφέρεται στο φάσμα των εφαρμογών που κυμαίνεται η τεχνολογία καθώς και στην χρήση του blockchain ως δομή δεδομένων σε διάφορες εφαρμογές (X. Li, Jiang, Chen, Luo, & Wen, 2017) , ενώ εξετάζονται πολλά από τα πιο δημοφιλή συστήματα blockchain (π.χ Ethereum, bitcoin, κ.λ.π.) κάνοντας μια συστηματική διερεύνηση των απειλών ασφαλείας για το blockchain.

Η μελέτη εστιάζει στη συγκέντρωση και ανάλυση στοιχείων με στόχο την απόκτηση περισσότερης γνώσης, προσεγγίζοντας πολύπλευρα και από διαφορετικές οπτικές τα προβλήματα που αντιμετωπίζει το δημόσιο blockchain (blockchain 1.0, blockchain 2.0), εξετάζοντας λόγους δημιουργίας ευπαθειών, επιπτώσεις που προκαλούν καθώς και πιθανές προτάσεις αντιμετώπισης των απειλών οι οποίες θα μπορούσαν να μειώσουν τον κίνδυνο επιτυχούς επίτευξης των επιθέσεων. Ειδικότερα, η ανάλυση των παραπάνω ζητημάτων θα γίνει μέσω του διαχωρισμού της μελέτης σύμφωνα με τρία βασικά κριτήρια, τα οποία είναι τα εξής:

- Κατηγοριοποίηση επιθέσεων με βάση τον ευρύτερο **είδος** στο οποίο ανήκει τον κοινό τους δηλαδή στόχο και την επίδραση την οποία επιφέρει στο blockchain σύστημα.
- Κατηγοριοποίηση επιθέσεων με βάση το **μηχανισμό συναίνεσης** (δημόσιου Blockchain), όπου αποτελεί και τον βασικότερο μηχανισμό σε ένα blockchain σύστημα αφού είναι ο μηχανισμός ουσιαστικά που εγγυάται την ομαλή λειτουργία του. Ειδικότερα, αναλύονται μειονεκτήματα και προβλήματα ασφαλείας σε

καθένα από αυτά, μέσω της οποίας εκπονούνται διάφορα χρήσιμα συγκριτικά συμπεράσματα, όπως για παράδειγμα πόσο γρήγορη ή αργή είναι μια επίθεση, τι κόστος θα έχει για τον επιτιθέμενο (κατανάλωση ενέργειας) ή τη ανοχή σε σφάλμα (fault tolerance) έχει ένας μηχανισμός συναίνεσης προκειμένου να αντιμετωπίσει μια πιθανή επίθεση.

- Κατηγοριοποίηση επιθέσεων με βάση το **επίπεδο αφαίρεσης** στο οποίο ανήκει, που αφορά τον αρχιτεκτονικό σχεδιασμό της τεχνολογίας Blockchain.

Καταλήγοντας, η εργασία αυτή παρουσιάζει ολοκληρωμένα την έννοια του blockchain σε σχέση με διάφορες πτυχές της τεχνολογίας, συσχετίζοντας παράλληλα με την παρουσίαση αυτή μια έμφαση στο ρόλο που διαδραματίζει η τεχνολογία στο πεδίο της ασφάλειας καθώς και πως επηρεάζονται συστατικά του blockchain ως προς αυτήν, ενώ αναφέρονται κάποιες ενδεικτικές λύσεις ορισμένων σημαντικών επιθέσεων καθώς και μελλοντικές επεκτάσεις της τεχνολογίας ως προς την βελτίωση προβλημάτων ασφάλειας.

3.1 Κατηγοριοποίηση επιθέσεων με βάση το ευρύτερο είδος που ανήκουν

Με βάση την ανασκόπηση από την βιβλιογραφία και την εμπειρική γνώση οι επιθέσεις και οι κίνδυνοι στο Blockchain ομαδοποιούνται σε κατηγορίες και υποκατηγορίες ανάλογα με το είδος της επίθεσης και την επίδραση που προκαλεί. Επιπλέον, ο μηχανισμός συναίνεσης όντας η «σπονδυλική στήλη» της τεχνολογίας επηρεάζει κάθε φορά διαφορετικά την λειτουργία του blockchain και την ανοχή του σε τυχόν επιθέσεις και τέλος τα επίπεδα αφαίρεσης που συνθέτουν την αρχιτεκτονική της τεχνολογίας αυτής, αποτελούν ένα πολύ σημαντικό παράγοντα διαχωρισμού.

3.1.1 Επιθέσεις στο πρωτόκολλο επικοινωνίας

Η κατηγορία αυτή διαχωρίζει τις επιθέσεις, σε αυτές που αφορούν το επίπεδο δικτύου, καθώς και σε αυτές που απειλούν το πρωτοκόλλο.

3.1.1.1 Επιθέσεις στο Δίκτυο

3.1.1.1.1 DNS Attack

Με την δημιουργία μιας νέας ταυτότητας ενός νέου συμμετέχοντα πραγματοποιείται καταχώρηση αυτής στο MSP (Membership Service Provider), το οποίο αποτελεί ένα συστατικό διαχείρισης ταυτοτήτων σε ένα blockchain δίκτυο, ως προς την αυθεντικοποίηση των πελατών που επιχειρούν να συμμετέχουν στο δίκτυο. Κατά την εφαρμογή της παραπάνω διαδικασίας προκύπτουν συνθήκες για την δημιουργία επίθεσης. Αναλυτικότερα, σε μια τέτοια περίπτωση κίνδυνοι όπως “man in the middle attack”, “Cache Poisoning” καθώς και άλλες επιθέσεις οι οποίες εντάσσονται στο σύνολο των DNS, ενδέχεται να εκδηλωθούν. Το πρόβλημα λοιπόν έγκειται στο ενδεχόμενο μείωσης της κρυφής μνήμης του DNS resolver γεγονός με το οποίο ο διακομιστής επιστέφει ψεύτικη τιμή, ενώ παράλληλα η αντίστοιχη έγκυρη παύει να είναι διαθέσιμη (Davenport, Shetty, & Liang, 2018). Θα πρέπει να τονιστεί ότι η επίθεση DNS βασίζεται στην επίθεση κατανεμημένης άρνησης DDoS, κατά την οποία ο επιτιθέμενος δημιουργεί πολλαπλά πλαστά αιτήματα σε διακομιστές DNS με στόχο την απόκρυψη της πηγής της εκμετάλλευσης κατευθύνοντας την απάντηση στο διακομιστή στόχο. Συνήθως οι περισσότερες από αυτές τις επιθέσεις έχουν ως στόχο μεγάλες δεξαμενές εξόρυξης (mining pools), ενώ είναι υπεύθυνες για το κλείσιμο των υπηρεσιών από εταιρίες όπως BitQuick και Coinwallet. Σε επίπεδο blockchain συστημάτων διακόπτεται η μεταφορά εμπορευμάτων-υπηρεσιών σε ένα συγκεκριμένο διακομιστή.

Στο Blockchain υπάρχουν 2 κύριες κατηγορίες επιθέσεων σε σχέση με τα κρυπτονομίσματα. Στην αρχική περίπτωση, οι επιτιθέμενοι εκμεταλλευόμενοι τον περιορισμό ως προς το μέγεθος ενός μπλοκ, όπου είναι το 1 mb δημιουργώντας τις λεγόμενες συναλλαγές «σκόνης» με στόχο την κατάληψη του διαθέσιμου χώρου και τον εμποδισμό της εξόρυξης άλλων συναλλαγών, γεγονός το οποίο έχει αντιμετωπιστεί όπως για παράδειγμα με εφαρμογή της μαλακής διακλάδωσης “SegWit” κατά την οποία το μέγεθος ενός μπλοκ μπορεί θεωρητικά να αυξηθεί από το 1 mb στα 4 mb. Η άλλη βασική μεθοδολογία επιθέσεων στοχεύει στα “mempool” το οποίο αποτελεί ένα σύνολο από miners που συλλειτουργεί στην διαδικασία της εξόρυξης, η οποία στοχεύει στον «βομβαρδισμό» τους από μη επιβεβαιωμένες συναλλαγές. Παρόλο που οι πιθανότητες είναι να απορριφθούν τέτοιου είδους συναλλαγές η παρουσία τους στο “mempool” μπορεί να επηρεάσει αρνητικά, αυξάνοντας το τέλος συναλλαγών που καταβάλλεται στους ανθρακωρύχους. Στην περίπτωση ενός μεγάλου “mempool” οι ανθρακωρύχοι είναι δύσκολο να έχουν έλεγχο ως προς την επιλογή των συναλλαγών εξόρυξης και για τον λόγο αυτό οι χρήστες επιλέγουν τις συναλλαγές με το υψηλότερο τέλος εξόρυξης (Saad, Njilla,

Kamhoua, Kim, et al., 2019). Εξαιτίας του παραπάνω γεγονότος, ο επιτιθέμενος με την μέθοδο “mempool flooding” μπορεί να βλάψει κάποιον χρήστη, ώστε να πληρώσει υψηλό τέλος εξόρυξης για την συναλλαγή του.

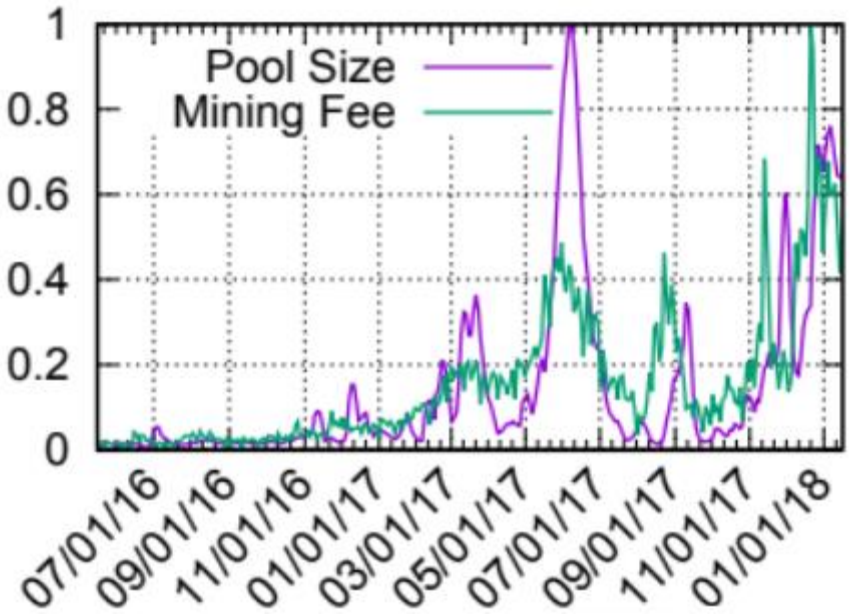
Διαδικασία επίθεσης DDOS attack

Η κατανεμημένη άρνηση υπηρεσίας (DDOS) είναι ένας τύπος επίθεσης που στοχεύει γενικά σε επιθέσεις εναντίον ενός υπολογιστή ή μιας υπηρεσίας με σκοπό να καταστήσουν τον διακομιστή-στόχο ανίκανο να δεχθεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει πιθανούς πελάτες (“Denial-of-Service Attack - Wikipedia,” n.d.). Υποθέτουμε ότι ο επιτιθέμενος αποτελεί ένα πλήρη κόμβο στο δίκτυο ενώ απαιτούμε ότι το υπόλοιπο στο πορτοφόλι του επιτιθέμενου είναι αρκετά μεγάλο ώστε να αρκεί για την πραγματοποίηση πολλαπλών μικρών συναλλαγών, ενώ διατηρεί παράλληλα πολλαπλές ταυτότητες (sybil accounts) με πολλαπλές δημόσιες διευθύνσεις. Θα πρέπει να τονιστεί ότι η αποκεντρωμένη και κατανεμημένη φύση του blockchain μετατρέπει σε πολύ πιο δύσκολη διαδικασία την επιτυχία μιας DDoS επίθεσης σε σχέση με ένα συμβατικό client-server μοντέλο. Παρόλο αυτά η τεχνολογία blockchain εξακολουθεί να είναι επιρρεπής σε επιθέσεις DDoS.

Όταν πραγματοποιείται μια επίθεση «πλημμύρας» σε ένα σύνολο ανθρακωρύχων ο στόχος είναι να μεγεθυνθεί το συνολικό μέγεθος του “mempool” μειώνοντας το τέλος εξόρυξης που πληρώνεται στους ανθρακωρύχους, Η φιλοσοφία της επίθεσης είναι να δημιουργεί συναλλαγές που προσφέρουν μικρό τέλος εξόρυξης με παράλληλο σκοπό οι συναλλαγές αυτές να παραμένουν εντός του “mempool” για όσο το δυνατόν περισσότερο χρόνο. Για να επιτευχθεί κάτι τέτοιο, ο επιτιθέμενος ελέγχει το υπόλοιπο του σε UTXO, ώστε να παραχθεί ένα σύνολο συναλλαγών με εφαρμογή του ελάχιστου δυνατού τέλους εξόρυξης . Στην συνέχεια οι συναλλαγές αυτές στέλνονται σε “sybil accounts”, οι οποίοι προφανώς διαθέτουν είσοδο UTXO το οποίο ποσό έχει εξ ’ορυχθεί προηγουμένως. Το παραπάνω γεγονός αποτελεί την αφετηρία για μια συναλλαγή, ώστε να μπορεί να πληρώσει το ελάχιστο ποσό για την πληρωμή της εισφοράς εξόρυξης. Πιο συγκεκριμένα , ο επιτιθέμενος μπορεί να δημιουργεί συναλλαγές από προηγούμενα UTXO, οι οποίες στέλνονται σε ένα “sybil” πορτοφόλι, λαμβάνοντας την διαφορά πίσω ως μια καινούρια συναλλαγή. Ουσιαστικά, ο κακόβουλος κόμβος χρησιμοποιεί την διαφορά υπολοίπου που δημιουργείται κατά τις συναλλαγές ως μια νέα είσοδο για μια επόμενη συναλλαγή επαναλαμβάνοντας την παραπάνω διαδικασία για τους sybil κόμβους ή χρησιμοποιώντας

το ποσό μιας συναλλαγής ώστε να το διαιρέσει σε εξόδους οι οποίες προορίζονται για αποστολή σε διευθύνσεις “sybil” κόμβων (Saad et al., 2020). Στο σημείο αυτό όλοι οι “sybil” κόμβοι δημιουργούν συναλλαγές με την μικρότερη δυνατή αξία και στην συνέχεια πραγματοποιούν πληρωμές ο ένας κόμβος στον άλλο σε σύντομο χρονικό διάστημα μέσω εφαρμογής λογισμικού “wallet”. Η δραστηριότητα αυτή δημιουργεί “backlog” με αποτέλεσμα ο βαθμός επιβεβαίωσης των συναλλαγών αυτών να αυξάνεται, ενώ παράλληλα ο ανταγωνισμός για την δημιουργία νέων συναλλαγών εξόρυξης αυξάνεται. Το γεγονός αυτό μεταφράζεται σε αύξηση των τελών που πρέπει να πληρώσουν οι κόμβοι στους ανθρακωρύχους. Ωστόσο, οι συναλλαγές οι οποίες έχουν πραγματοποιηθεί μεταξύ των κόμβων αυτών αναμένεται να αποκτήσουν μηδενικό UTXO ποσό λόγω των συνεχόμενων πληρωμών που πραγματοποιούνται στο υποσύνολο των “sybil” κόμβων μεταξύ τους.

Όπως λοιπόν έχει παρατηρηθεί οι χρήστες είναι υποχρεωμένοι να ελέγχουν τα μεγέθη των “mining pools” όπου αναφερόμαστε στον αριθμό των συναλλαγών που πραγματοποιούνται, προκειμένου να υπολογίζουν την σειρά με την οποία πραγματοποιούν τις συναλλαγές τους. Με άλλα λόγια, όσο μεγαλύτερος αριθμός συναλλαγών υπάρχουν σε ένα “mining pool” τόσο πιο δύσκολη θα γίνεται η διαδικασία της εξόρυξης με την έννοια ότι θα απαιτούνται μεγαλύτερα ποσά από τους κόμβους του δικτύου προς τους ανθρακωρύχους ως κίνητρο για να εμπεριέχονται οι συναλλαγές τους σε αυτές του συνόλου που τελικά θα εξ’ορυχθούν. Οι τεχνητές αυξημένες ροές συναλλαγών που πραγματοποιούνται μεταξύ των Sybil κόμβων αυξάνουν το συνολικό μέγεθος σε ένα mining pool. Το λεπτό σημείο σε μια τέτοια περίπτωση είναι ότι παρόλο που οι συναλλαγές αυτές απορρίπτονται από τους ανθρακωρύχους στο blockchain δίκτυο, ο επιτιθέμενος λόγω αυτής της πολιτικής του Blockchain δεν ξοδεύει bitcoin. Αντίθετα, ο μολυσμένος κόμβος λόγω των παραπάνω συνθηκών της τεχνητής αύξησης στο “mining pool” είναι αναγκασμένος να πληρώνει μεγαλύτερες εισφορές εξόρυξης. Ένα τέτοιο φαινόμενο παρατηρήθηκε σε έντονες μορφές για παράδειγμα όπως φαίνεται και στο παρακάτω διάγραμμα τον Μάιο του 2017 ή τον Ιανουάριο του 2018 (Saad, Kim, Nyang, & Mohaisen, 2021). Σε τέτοιες λοιπόν περιπτώσεις αυξάνεται κατά πολύ η πιθανότητα επιτυχούς επίτευξης DDoS επιθέσεων.



Εικόνα 23:Απεικόνιση Συσχέτισης μεγεθών "mining pool" και "mining fee", κατά την διετία 2016-2018[2]

Το γεγονός αυτό αποδεικνύεται υπολογίζοντας τον συντελεστή συσχέτισης Pearson ο οποίος δίνεται από τον τύπο: $\rho(X, Y) = \frac{n\sum(XY)-(\sum X)(\sum Y)}{\sqrt{[n\sum X^2-(\sum X)^2][n\sum Y^2-(\sum Y)^2]}}$, του οποίου το αποτέλεσμα στην προκείμενη περίπτωση είναι $\rho = 0.69$ και επειδή $\rho \in [0.6, 0.79]$, αποτέλεσμα το οποίο αποδεικνύει το οποίο σύμφωνα με τον τύπο Pearson την υψηλή συσχέτιση των δύο μεταβλητών.

3.1.1.1.2 Eclipse attack

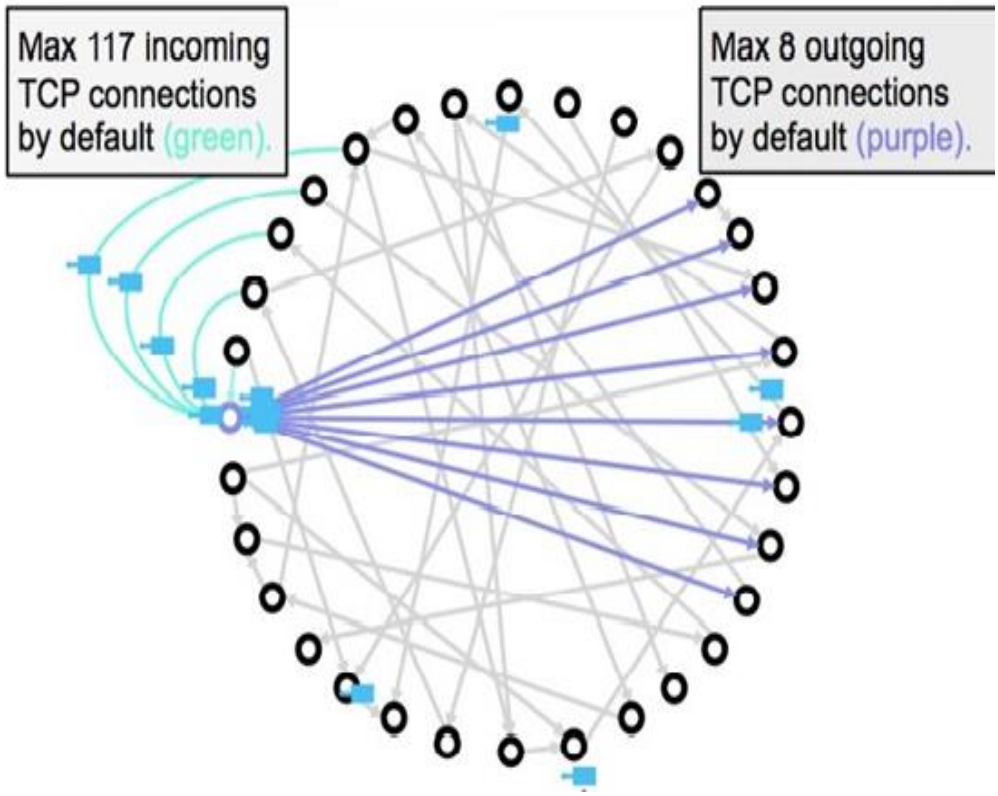
Παρόλο που τα τελευταία χρόνια δόθηκε ιδιαίτερη έμφαση στην ασφάλεια των μοντέλων συναίνεσης του Blockchain, υπήρξε παράλληλα ένα κενό μελέτης ως προς το δίκτυο ομότιμων κόμβων για την μεταξύ τους μετάδοση πληροφοριών. Σε ένα bitcoin peer-to-peer δίκτυο οι κόμβοι αναγνωρίζονται απλά από τις διευθύνσεις IP. Στην περίπτωση μιας επίθεσης "Eclipse" ένας επιτιθέμενος στοχεύει στον έλεγχο ενός πλήθους από IP διευθύνσεις, ώστε όλες οι συνδέσεις προς και από τον κόμβο στόχο να πραγματοποιούνται και να διαχειρίζονται από τον επιτιθέμενο. Με άλλα λόγια, μια "eclipse attack" μπορεί να επιτευχθεί διότι οι κόμβοι σε ένα αποκεντρωμένο περιβάλλον

[2] ανακτήθηκε από: https://arxiv.org/pdf/1904.03487.pdf

αδυνατούν να συνδεθούν ταυτόχρονα με όλους τους κόμβους στο δίκτυο, εξαιτίας ορίων στο εύρος ζώνης του δικτύου και ως συνέπεια αυτού συνδέονται μόνο με περιορισμένο αριθμό διπλανών κόμβων. Το παραπάνω γεγονός αποτελεί αδυναμία με την έννοια ότι ένας κακόβουλος κόμβος αρκεί για την επίθεση ώστε να επιτευχθεί μια σύνδεση του κόμβου (σε κάποιο διπλανό κόμβο), χωρίς δηλαδή την ανάγκη της επίθεσης σε ολόκληρο το δίκτυο ("Eclipse Attacks Explained: What Are They? | Gemini," n.d.). Κάτι τέτοιο επιτυγχάνεται από τον εισβολέα μέσω ενός botnet με την εφαρμογή του οποίου ο κόμβος στόχος «βομβαρδίζεται» από IP διευθύνσεις και με τις οποίες συγχρονίζεται έως ότου συνδεθεί στο blockchain δίκτυο. Έτσι μέσω της παραπάνω διαδικασίας ο επιτιθέμενος αναμένει την σύνδεση του κόμβου στόχου στο δίκτυο και κατ' επέκταση με τους «μολυσμένους», με την εκτέλεση ουσιαστικά μιας DDoS επίθεσης. Σε περίπτωση επιτυχούς έκβασης της επίθεσης, ο επιτιθέμενος μπορεί να είναι σε θέση να επηρεάσει την διαδικασία της εξόρυξης και κατ' επέκταση την σωστή εφαρμογή του μοντέλου ομοφωνίας που εφαρμόζεται καθώς και να δημιουργήσει συνθήκες επίτευξης επιθέσεων όπως "double spending" ή ακόμη την δημιουργία κάποιας διακλάδωσης στην αλυσίδα. Ιδιαίτερα στην κατηγορία επίθεσης "double spend", παρουσιάζονται οι περιπτώσεις των 0-confirmation και N-confirmation συναλλαγών. Αναλυτικότερα σε μια 0-confirmation συναλλαγή η πληρωμή μιας υπηρεσίας επιτυγχάνεται πριν από την προβολή της επιβεβαίωσης ενός μπλοκ. Δηλαδή γίνεται η προβολή της συναλλαγής στους κόμβους, χωρίς ωστόσο να συμπεριληφθεί στην αλυσίδα, παρά μόνο στα δυναμικά "mining pool", σε μια διαδικασία που προηγείται της επιβεβαίωσης των συναλλαγών. Το παραπάνω γεγονός, είναι ικανό για την δημιουργία ευπαθειών τύπου διπλής δαπάνης (Pérez-Solà, Delgado-Segura, Navarro-Arribas, & Herrera-Joancomartí, 2019). Το συγκεκριμένο είδος εφαρμόζεται όταν δεν απαιτείται πολύ μικρός χρονικός περιορισμός ως προς την διαδικασία της επιβεβαίωσης κάποιου μπλοκ. Όσον αφορά την συναλλαγή N-επιβεβαίωσης μπορεί να πραγματοποιηθεί μόνο όταν η συναλλαγή έχει επιβεβαιωθεί σε μπλοκ ύψους N-1. Αναλυτικότερα, ο επιτιθέμενος αποστέλλει την συναλλαγή του σε ανθρακωρύχους οι οποίοι είναι υπό συνθήκη επίθεσης eclipse, γεγονός το οποίο μεταφράζεται στο ότι ο επιτιθέμενος προβάλλει μια νέα διακλάδωση του blockchain, ενώ οι «μολυσμένοι» κόμβοι ενσωματώνουν τις συναλλαγές αυτές στην προηγούμενη έκδοση της αλυσίδας blockchain (μη-διακλαδωμένη μορφή). Κατά συνέπεια, σε μια τέτοια περίπτωση συναλλαγής ο επιτιθέμενος προβάλλει την νέα διακλαδωμένη έκδοση της αλυσίδας στέλνοντας έτσι τόσο στον έμπορο όσο και στους υπόλοιπους ανθρακωρύχους

το αντίγραφο της νέας έκδοσης (Heilman, Kendler, Zohar, & Goldberg, n.d.). Ως εκ τούτου, το blockchain των ανθρακωρύχων μένει ορφανό το οποίο συνεπάγεται την αγορά αγαθών από τον εισβολέα χωρίς όμως την πληρωμή τους.

Στο σημείο αυτό όμως, θα ήταν απαραίτητο να αναφερθούν κάποιες σχετικές πληροφορίες για το bitcoin δίκτυο. Ιδιαίτερα, κάθε κόμβος με δημόσια IP διεύθυνση εφαρμόζει ένα πρωτόκολλο επιλογής 8 κόμβων με τους οποίους έχει επικοινωνία με σκοπό την διάδοση ή την αποθήκευση διευθύνσεων των εν δυνάμει ομότιμων κόμβων που θα συμμετέχουν στο δίκτυο. Με άλλα λόγια, ένας κόμβος μπορεί να συνδεθεί το πολύ με 8 εξερχόμενους κόμβους. Αξίζει επίσης να αναφερθεί ότι οι κόμβοι με δημόσιες IP λαμβάνουν μέχρι και 117 εισερχόμενες συνδέσεις από οποιαδήποτε διεύθυνση IP, με σκοπό την διάδοση συναλλαγών μεταξύ των κόμβων. Η παραπάνω διαδικασία ανταλλαγής πληροφοριών όμως επικεντρώνεται απαραίτητα σε κόμβους οι οποίοι μπορούν να λάβουν εισερχόμενες συνδέσεις και συνεπώς μια “eclipse attack” αφορά μόνο αυτούς.



Εικόνα 24:Απεικόνιση ενός P2P δικτύου bitcoin[3]

Εφόσον λοιπόν πραγματοποιηθεί μια επίθεση “eclipse” σε κάποιο κόμβο στην συνέχεια ο κόμβος αυτό θα επικοινωνεί μόνο με κακόβουλους κόμβους. Θα πρέπει να τονίσουμε ότι κόμβοι στο bitcoin δίκτυο διαδίδουν και αποθηκεύουν μόνο δημόσιες ip διευθύνσεις.

Όσον αφορά την διάδοση πληροφορίας στο δίκτυο του bitcoin, η διαδικασία αυτή πραγματοποιείται μέσω των “dns seeders”, όπου πρόκειται για servers που απαντάνε στα μηνύματα DNS των bitcoin κόμβων σύμφωνα με υπάρχουσα λίστα διευθύνσεων που αντιστοιχούν σε κόμβους, καθώς και των μηνυμάτων ADDR. Τα παραπάνω μηνύματα περιέχουν ως και 1000 διευθύνσεις καθώς και τις χρονικές τους σημάνσεις και ο ρόλος τους είναι η συγκομιδή πληροφοριών σχετικά με τους ομότιμους κόμβους. Έτσι στην περίπτωση που σταλούν περισσότερες από 1000 διευθύνσεις μέσω ενός μηνύματος ADDR, ο ομότιμος κόμβος που στέλνει ένα τέτοιο μήνυμα στιγματίζεται μέσω της καταχώρησης του σε «μαύρη» λίστα, ενώ ένα τέτοιο μήνυμα αποστέλλεται κατά την δημιουργία μιας εξερχόμενης σύνδεσης με ένα ομότιμο κόμβο. Αναλυτικότερα, κάθε κόμβος στέλνει μέσω ενός μηνύματος ADDR την διεύθυνση IP, ενώ όταν δέχεται μήνυμα με περισσότερες από 10 IP διευθύνσεις στην συνέχεια γίνεται προώθηση αυτού με τυχαίο τρόπο σε 2 ομότιμους κόμβους στο δίκτυο.

Σχετικά με το ζήτημα της αποθήκευσης των δημόσιων IP κάθε κόμβος επιλέγει την σύνδεση του με τους ομότιμους από διευθύνσεις οι οποίες αποθηκεύονται είτε στους λεγόμενους δοκιμασμένους είτε σε νέους πίνακες οι οποίοι αποθηκεύονται σε δίσκο και κατά συνέπεια διατηρούνται όλες οι πληροφορίες κατά την επανεκκίνηση ενός μπλοκ. Ειδικότερα ένας νέος πίνακας περιέχει διευθύνσεις οι οποίες είναι «γνωστές» στο δίκτυο, ενώ ένας δοκιμασμένος περιέχει διευθύνσεις με τις οποίες ο κόμβος έχει ήδη συνδεθεί κάποια στιγμή. Με άλλα λόγια ένας δοκιμασμένος πίνακας αποθηκεύει την IP διεύθυνση με την οποία ένας κόμβος έχει πραγματοποιήσει με επιτυχία εισερχόμενες και εξερχόμενες συνδέσεις στο πρωτόκολλο tcp, ενώ σε ένα νέο πίνακα αποθηκεύονται διευθύνσεις οι οποίες προέρχονται μέσω των μηνυμάτων ADDR (Heilman et al., n.d.).

[3] Ανακτήθηκε από: https://medium.com/speaking-frankly/eclipse-attacks-on-bitcoin-s-peer-to-peer-network-e0da797302c2

Όσον αφορά την επιλογή εξερχόμενων συνδέσεων αυτή σχετίζεται με το αν ένας κόμβος κάνει επανεκκίνηση ή υπάρχει διακοπή από το δίκτυο αφού έχει προηγηθεί η καταχώρηση του σε μαύρη λίστα, γεγονός το οποίο μεταφράζεται σε αποστολή από τον κόμβο, μεγάλων μηνυμάτων ADDR. Αναλυτικότερα, θεωρώντας ως **ω** εξερχόμενες συνδέσεις, επιλέγεται η $\boldsymbol{\omega+1^{th}}$ σύνδεση με τον παρακάτω τρόπο:

- Βήμα 1: Ορίζεται αρχικά η επιλογή του πίνακα (δοκιμασμένου ή νέου) για την αποθήκευση των διευθύνσεων IP. Πιο συγκεκριμένα, η πιθανότητα επιλογής από δοκιμασμένο πίνακα περιγράφεται από τον παρακάτω τύπο.

$$P\ [\text{δοκιμασμένου πίνακα}] = \frac{\sqrt{\rho}\,(9-\omega)}{(\omega+1)+\sqrt{\rho}\,(9-\omega)}\ (1),$$

  όπου ρ είναι η αναλογία μεταξύ του πλήθους των διευθύνσεων που αποθηκεύονται στους δοκιμασμένους πίνακες και των διευθύνσεων που αποθηκεύονται στους νέους πίνακες. Η επίθεση eclipse επωφελείται της παραπάνω διαδικασίας επιλογής με σκοπό να μονοπωλήσει όλες τις συνδέσεις του κόμβου θύματος.

- Βήμα 2: Επιλέγεται μια τυχαία διεύθυνση από τον δοκιμασμένο πίνακα. (i)Αν ο πίνακας είναι γεμάτος, τότε επιλέγεται μια τυχαία θέση σε αυτόν. (ii)Αν η θέση αυτή αντιστοιχεί σε κάποια διεύθυνση, επιστρέφεται η διεύθυνση με πιθανότητα

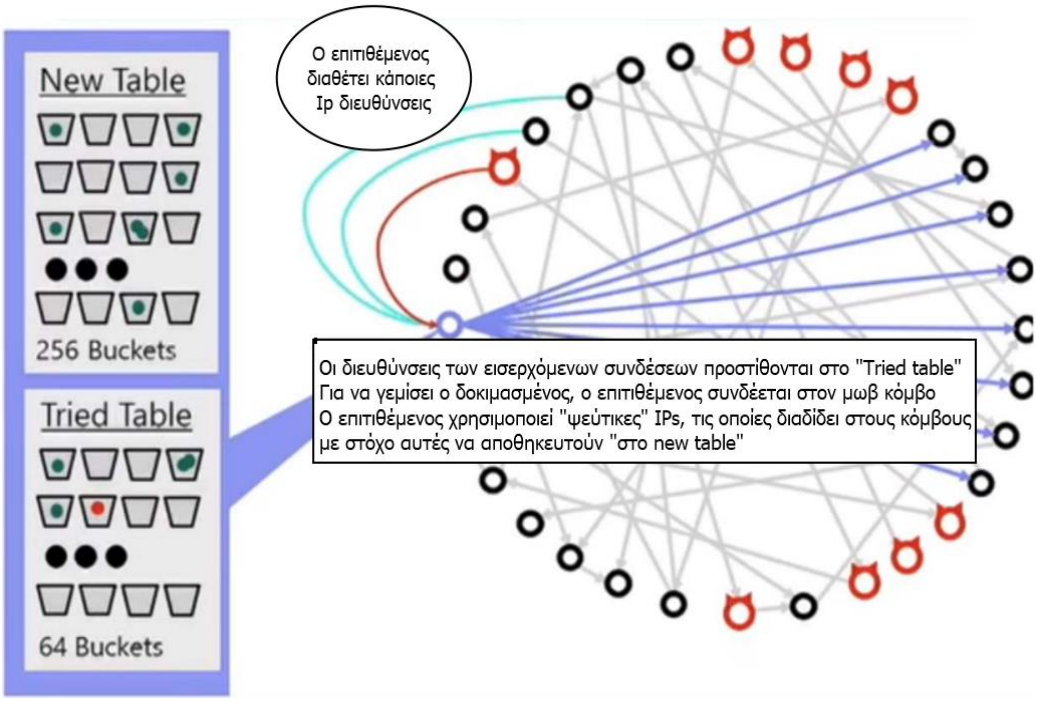
$$P\ (r, t) = \min\left(1, \frac{1.2^{r}}{1+\tau}\right)\ (2),$$

  όπου r είναι ο αριθμός των διευθύνσεων οι οποίες έχουν απορριφθεί και τ η διαφορά μεταξύ της χρονικής σφραγίδας της διεύθυνσης και του τρέχοντος χρόνου, μετρημένος σε μονάδα χρόνου δεκαλέπτου. Διαφορετικά αν η διεύθυνση δεν αντιστοιχεί σε κάποια θέση του πίνακα έχουμε απόρριψη αυτής και επιστροφή στην ενέργεια (i).
- Βήμα 3: Αν η σύνδεση στην διεύθυνση αποτύχει, μεταβαίνουμε στο βήμα 1

Διαδικασία επίτευξης επίθεσης eclipse

Ο επιτιθέμενος κόμβος σε μια τέτοια επίθεση αφού αρχικά έχει στην κατοχή του έναν αριθμό από διευθύνσεις IP των κόμβων του δικτύου όπως για παράδειγμα έχοντας τον έλεγχο ενός κατανεμημένου botnet, η επόμενη του κίνηση είναι να χρησιμοποιήσει αυτές τις διευθύνσεις που βρίσκονται υπό τον έλεγχο του ώστε να τις χρησιμοποιήσει για

να τις τοποθετήσει στις θέσεις του δοκιμασμένου πίνακα του κόμβου που έχει στοχεύσει (Εικόνα 25).

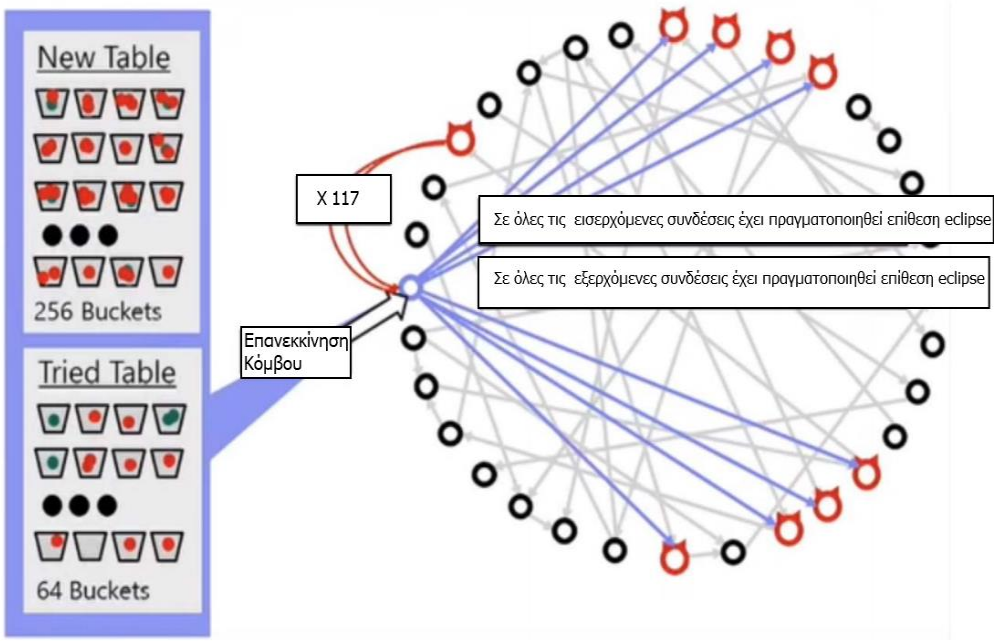


Εικόνα 25:Προσθήκη διευθύνσεων εισερχόμενων συνδέσεων στον δοκιμασμένο πίνακα

Στην συνέχεια, πραγματοποιείται αντικατάσταση των διευθύνσεων αυτών στο νέο πίνακα με ψεύτικες διευθύνσεις, οι οποίες δεν σχετίζονται με το bitcoin δίκτυο και συνεπώς δεν αντιστοιχούν σε κόμβους που ανήκουν σε αυτό (Kendler et al., 2015). Πιο συγκεκριμένα:

- Οι διευθύνσεις εισερχόμενων συνδέσεων εντάσσονται στον δοκιμασμένο πίνακα, ενώ ο επιτιθέμενος μπορεί να εισάγει στο δοκιμασμένο πίνακα του θύματος μια διεύθυνση και κατά συνέπεια να είναι σε θέση να συνδεθεί με το θύμα μέσω αυτής της διεύθυνσης. Επιπλέον θα πρέπει σημειωθεί ότι, οι ψεύτικες αυτές διευθύνσεις (οι οποίες είναι επιλέξιμες από το μητρώο διαθέσιμων διευθύνσεων IPv4 της διαδικτυακής αρχής “IANA”) ή δεν έχουν εκχωρηθεί στον πίνακα ή θα γίνεται κράτηση αυτών για μελλοντική διαθεσιμότητα.
- Ο κόμβος δεχόμενος μηνύματα ADDR εισάγει διευθύνσεις κατευθείαν στον νέο πίνακα χωρίς κάποιο έλεγχο συνδεσιμότητας. Αυτό έχει ως αποτέλεσμα όταν ο επιτιθέμενος συνδέεται με το θύμα μέσω μιας διεύθυνσης που έχει εισάγει στο

δοκιμασμένο πίνακα του θύματος, τότε θα έχει την δυνατότητα να στείλει 1000 ψεύτικες διευθύνσεις. Ως εκ τούτου, γίνεται αντικατάσταση των διευθύνσεων του πίνακα από τις «ψεύτικες» (Zohar et al., 2015). Τέλος θα πρέπει να τονιστεί ότι είναι εφικτή η αντικατάσταση διευθύνσεων στους δοκιμασμένους και νέους πίνακες του θύματος επειδή στο αποκεντρωμένο και κατανεμημένο αυτό δίκτυο οι κόμβοι δεν ζητούν από του ομότιμους τους πληροφορίες.



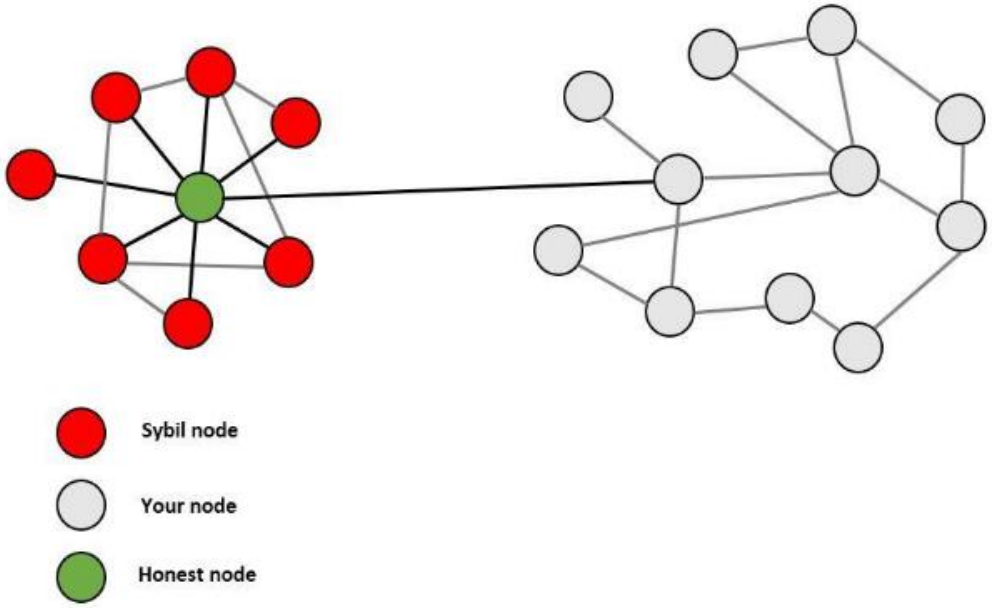
Εικόνα 26:Επίθεση eclipse σε εισερχόμενες και εξερχόμενες συνδέσεις σε κατά την επανεκκίνηση κόμβου

Καταλήγοντας, η επίθεση eclipse επιτυγχάνεται, αφού αρχικά ο κόμβος που αποτελεί στόχο για τον εισβολέα έχει εξερχόμενες συνδέσεις σε IP εισβολέα, ενώ οι πίνακες του ομότιμου κόμβου γεμίζουν με IPs του επιτιθέμενου. Στην συνέχεια ο κόμβος επανεκκινείται και χάνει όλες τις τρέχουσες εξερχόμενες συνδέσεις, ενώ η εξέλιξη αυτού του γεγονότος είναι οι νέες συνδέσεις του κόμβου να είναι μόνο με διευθύνσεις του επιτιθέμενου.

3.1.1.1.3 Sybil attack

Η επίθεση Sybil είναι ένας τύπος επίθεσης που παρατηρείται σε δίκτυα "peer-to-peer" στα οποία ένας κόμβος στο δίκτυο λειτουργεί ενεργά με πολλαπλές ταυτότητες, όπου πρόκειται για ψεύτικους λογαριασμούς χρηστών. Ωστόσο αυτοί οι εικονικοί κόμβοι, λειτουργούν ως πραγματικοί, αποδιοργανώνοντας το δίκτυο. Με άλλα λόγια, μια μεμονωμένη οντότητα ελέγχει πολλές ταυτότητες παράλληλα και μπορεί να επηρεάσει το δίκτυο μέσω πρόσθετης δύναμης ψήφου. Είναι σημαντικό να τονιστεί ότι εφόσον επιτευχθεί μια τέτοια επίθεση μπορεί να γίνει ιδιαίτερα δύσκολος ο εντοπισμός της μεμονωμένης οντότητας που θα ελέγχει του πολλούς λογαριασμούς, ενώ ένα διάσημο παράδειγμα αυτής ήταν το πρόσφατο πρόβλημα των Ηνωμένων Πολιτειών με την ρωσική εκλογική επιρροή μέσω ψεύτικών λογαριασμών στα μέσα κοινωνικής δικτύωσης, όπου το Facebook δεν είχε εντοπίσει.

Στο δίκτυο bitcoin, ένας επιτιθέμενος μπορεί να δημιουργήσει πολλές εικονικές ταυτότητες για να αναλάβει τον έλεγχο ολόκληρου του δικτύου. Οι κόμβοι που αντιστοιχούν στις ψεύτικες ταυτότητες ονομάζονται συβιλιανοί κόμβοι (Swathi, Modi, & Patel, 2019). Ο σκοπός του επιτιθέμενου ο οποίος αντιστοιχεί σε μια ομάδα ανθρακωρύχων ("mining pool") είναι να αποσυνδέσει από το δίκτυο blockchain τους πραγματικούς κόμβους. Ένας επιτιθέμενος προσθέτει στο δίκτυο ένα σημαντικό αριθμό από ανθρακωρύχους με μηδενική όμως ισχύ κατακερματισμού στην κατοχή τους. Η αποστολή αυτών των εικονικών κόμβων είναι να διακόψουν την διάδοση των «νόμιμων» κόμβων στο δίκτυο. Ως εκ τούτου , θα έχουμε την διάδοση στο δίκτυο και τη προσθήκη στην αλυσίδα, μόνο μπλοκ τα οποία θα προέρχονται από τον επιτιθέμενο. Αυτό θα έχει ως προφανές αποτέλεσμα ο επιτιθέμενος να λαμβάνει μεγαλύτερα ποσά ανταμοιβής για την δημιουργία μπλοκ, αφού μόνο αυτός θα μπορεί να προσθέτει μπλοκ στην αλυσίδα και κατ' επέκταση θα είναι αυτός που θα καρπώνεται την ανταμοιβή.



Εικόνα 27:Sybil attack[4]

Σε ένα παράδειγμα αυτής της επίθεσης, θεωρούμε ένα μπλοκ το οποίο παράγεται από «νόμιμο» ανθρακωρύχο (έστω N) και ένα μπλοκ το οποίο παράγεται από τον επιτιθέμενο (έστω Ε). Το κοινό τους χαρακτηριστικό είναι ότι και τα δύο μεταδίδονται στο δίκτυο και είναι μέρος αυτού. Σύμφωνα με την διαδικασία μετάδοσης των μπλοκ, κάθε ανθρακωρύχος εκπέμπει το μπλοκ που παράγει αρχικά στους γειτονικούς κόμβους και στην συνέχεια στο σύνολο του δικτύου (Modi et al., 2019). Γίνεται αντιληπτό λοιπόν ότι και για τις δύο περιπτώσεις κόμβων θα υπάρχει διάδοση αυτών σε όλους τους κόμβους του δικτύου. Ωστόσο αυτό το οποίο συμβαίνει είναι ότι ο επιτιθέμενος μέσω των κακόβουλων κόμβων μεταδίδει στο δίκτυο μόνο το μπλοκ Ε και ταυτόχρονα παρεμποδίζει την διάδοση του μπλοκ Ν. Πιο συγκεκριμένα, επιτυγχάνεται τελικά να διαδίδονται στο δίκτυο και τα δύο είδη μπλοκ, με την διαφορά ότι η διάδοση του μπλοκ Ν θα είναι πολύ πιο αργή από την διάδοση του μπλοκ Ε. Αυτό επιφέρει το αποτέλεσμα, ο εισβολέας να ανταμείβεται σε συχνότερο βαθμό για τα μπλοκ που παράγει σε σχέση με τους «νόμιμους» κόμβους, ενώ παράλληλα οι νόμιμοι ανθρακωρύχοι σπαταλούν την ισχύ κατακερματισμού που έχουν, χωρίς να καταφέρνουν να προσθέσουν κάποιο μπλοκ στην αλυσίδα. Καταλήγοντας, θα λέγαμε ότι ο επιτιθέμενος στοχεύει στο να συνδεθεί σε κάποιο “network

[4] Ανακτήθηκε από:https://www.litefinance.com/blog/for-investors/cryptocurrency-attacks-types-of-vulnerabilities-risks-and-results/

pool” με την προϋπόθεση όμως ότι διαθέτει μεγάλη υπολογιστική δύναμη για την επιτυχή πραγματοποίηση της επίθεσης, αφού όταν υπάρχουν δύο ανταγωνιστικές αλυσίδες σε κόμβους του δικτύου επικρατεί πάντα αυτή που προλαβαίνει την άλλη ως προς την προσθήκη μπλοκ και για να καταφέρει μια από αυτές αυτό το αποτέλεσμα θα πρέπει υποχρεωτικά να υπερτερεί σε ισχύ κατακερματισμού.

Έτσι λοιπόν, για να πραγματοποιηθεί η επίθεση σε ένα κόμβο bitcoin, ο επιτιθέμενος αφού αρχικά εντοπίσει τον κόμβο θύμα στην συνέχεια αντικαθιστά όλους τους ομότιμους του, με κόμβους του εισβολέα.

3.1.1.1.4 Hijacking

Παρά το γεγονός ότι πάρα πολλές επιθέσεις έχουν εξακριβωθεί και μελετηθεί εις βάθος μια κατηγορία επιθέσεων είναι οι επιθέσεις που αφορούν την εκμετάλλευση του νομίσματος μέσω της διαδρομής του internet. Καθίσταται σαφές ότι επηρεάζοντας την δρομολόγηση κυκλοφορίας μηνυμάτων των αυτόματων συστημάτων μπορεί να επηρεάσει και εν τέλει να παραποιήσει την επικοινωνίας ενός blockchain συστήματος.

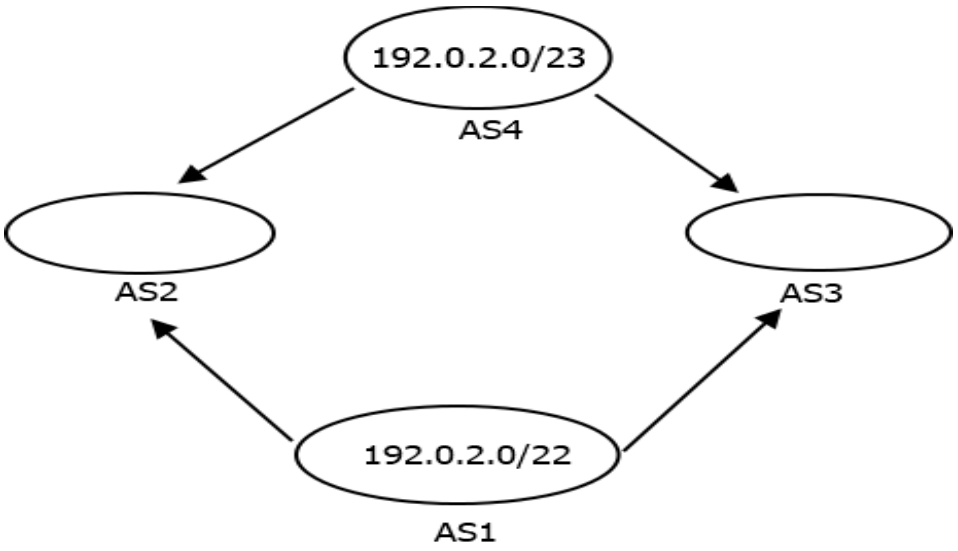
Είναι πάρα πολύ σημαντικό, να διαχωρισθούν οι επιθέσεις που αφορούν τις επιθέσεις δρομολόγησης με βάση την επιρροή που ασκούν στο bitcoin. Τόσο μικρής κλίμακας επιθέσεις όσο και μεγαλύτερης μπορούν να στοχεύσουν στην εκμετάλλευση ολόκληρου του δικτύου. Η αποτελεσματικότητα της εκμετάλλευσης της δρομολόγησης και ο βαθμός κεντροποίησης του συστήματος παίζει καθοριστικό ρόλο στο να ανατραπεί η επίθεση. Μια αρκετά αξιόλογη δουλειά (Apostolaki, Zohar, & Vanbever, 2017), μας καταδεικνύει την ικανότητα κάθε επίθεσης ενάντια στο υλοποιημένο bitcoin σύστημα και μας υπογραμμίζει την πιθανή φθορά στο σύστημα η οποία απαιτεί προσοχή. Φθορές οι οποίες δεν αποτελούν μόνο κομμάτια του συστήματος, αλλά και οικονομικές απώλειες όπως προκαλεί το “double spending”.

Σχετικά με το **πρωτόκολλο BGP (Border Gateway Protocol)**, αποτελεί ένα πρωτόκολλο δρομολόγησης το οποίο σχετίζεται με την προώθηση των πακέτων IP στο διαδίκτυο. Αναλυτικότερα, διαδρομές με διαφορετικά προθέματα IP ανταλλάσσονται με αυτόνομα συστήματα AS. Για κάθε πρόθεμα IP, θα υπάρχει ένα AS το οποίο θα υποδηλώνει την αρχική διαδρομή όπου στη συνέχεια θα διαδοθεί σε όλα τα υπάρχοντα AS. Θα πρέπει να τονιστεί, ότι στο πρωτόκολλο BGP, η εγκυρότητα των ανακοινώσεων διαδρομής δεν ελέγχεται, γεγονός στο οποίο μεταφράζεται ότι κάθε αυτόνομο σύστημα

AS μπορεί να εισάγει πλαστές πληροφορίες σχετικά με τον τρόπο πρόσβασης για κάποιο IP πρόθεμα. Δημιουργούνται έτσι ψεύτικες διαδρομές στο δίκτυο γνωστές ως BGP "hijacks", όπου πρόκειται για ένα αποτελεσματικό τρόπο ώστε ένας εισβολέας να αναχαιτίσει την κυκλοφορία προς ένα νόμιμο προορισμό.

Το πρωτόκολλο BGP όπως αναφέρθηκε, αποτελεί ένα πρωτόκολλο δρομολόγησης του διαδικτύου. Πιο συγκεκριμένα, διαφορετικά αυτόνομα πρωτόκολλα AS μοιράζονται πληροφορίες δρομολόγησης μεταξύ τους κάνοντας χρήση των πρωτοκόλλων BGP. Έτσι για παράδειγμα, αν στο AS1 έχει εκχωρηθεί το πρόθεμα 192.0.2.0/22, θα κάνει γνωστό αυτό το πρόθεμα στους γείτονες του AS2 και AS3. Συνεπώς, αν οι κεντρικοί υπολογιστές που είναι συνδεδεμένοι μέσω AS2 θέλουν να φτάσουν ένα προορισμό στο δίκτυο 192.0.2.0/22, οι δρομολογητές σε AS γνωρίζουν να το στείλουν στο AS1.

Έστω τώρα το AS4 είναι κάτω από τον έλεγχο ενός επιτιθέμενου. Στην επίθεση Hijack, ο AS4 μπορεί να δηλώσει ένα διαφορετικό πρόθεμα (π.χ 192.0.2.0/23) στα AS2 και AS3. Από εδώ και στο εξής, οι δρομολογητές θα επιλέξουν για οποιαδήποτε κίνηση προορίζεται στο 192.0.2.0/23 να σταλεί στο AS4 αντί για το AS1.



Εικόνα 28:Επίθεση Hijack στο πρωτόκολλο BGP

Ο συσχετισμός αυτής της επίθεσης με τα κρυπτονομίσματα γίνεται αν θεωρήσουμε ότι ένας επιτιθέμενος είναι σε θέση να αποκόψει αποτελεσματικά την σύνδεση για ένα σύνολο κόμβων από τους υπόλοιπους κόμβους (π.χ κόμβους εξόρυξης) στο blockchain δίκτυο. Όταν η υπηρεσία αποκατασταθεί μετά την επίθεση, θα υπάρχει ως συνέπεια όλη η προσπάθεια που έχουν κάνει οι κόμβοι εξόρυξης να χαθεί, οδηγώντας σε χάσιμο των

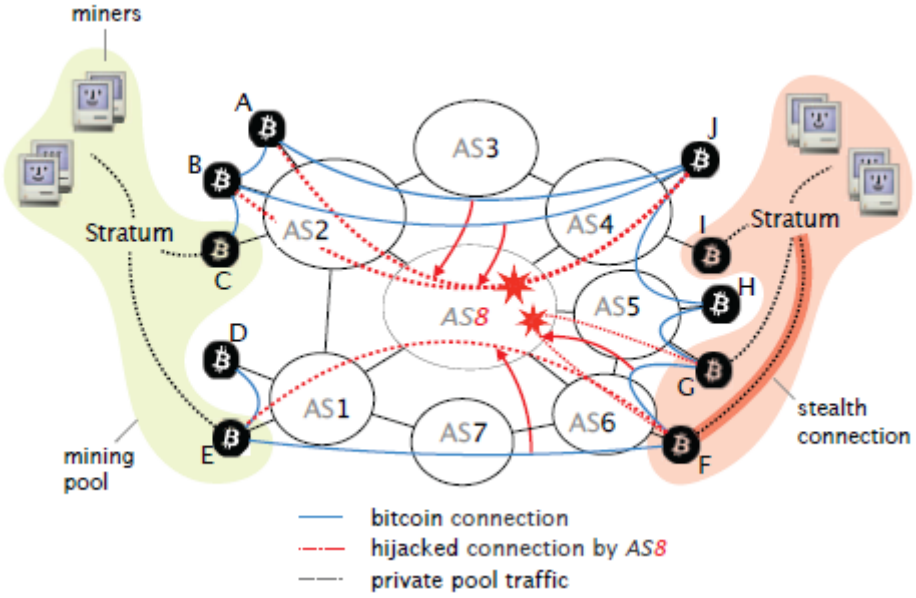
ανταμοιβών εξόρυξης τους. Σε ένα άλλο σενάριο, ο εισβολέας μπορεί να κάνει ανακατεύθυνση της σύνδεσης σε κάποιο "miming pool", όπου η εξόρυξη θα ελέγχεται από τον επιτιθέμενο. Επιπλέον, ένας εισβολέας μπορεί να εμποδίζει την δημιουργία ενός νέου μπλοκ δημιουργώντας έτσι καθυστερήσεις με αποτέλεσμα κάποιος άλλος ανθρακωρύχος στην θέση του να προλάβει να δώσει πρώτος λύση στο μοντέλο συναίνεσης, χωρίς να λαμβάνει τελικά με αυτό τον τρόπο την τυχών ανταμοιβή εξόρυξής.

Στην επίθεση Hijack στο πρωτόκολλο BGP**,** ένας εισβολέας που θέλει να προσελκύσει την περισσότερη κίνησή στο δίκτυο για κάποιο πρόθεμα έστω p, θα μπορούσε είτε να ανακοινώσει ένα συγκεκριμένο πρόθεμα είτε να ανακοινώσει ένα μεγαλύτερο πρόθεμα. Στην πρώτη περίπτωση, η διαδρομή του επιτιθέμενου θα είναι σε άμεσο ανταγωνισμό με την νόμιμη διαδρομή. Δεδομένου λοιπόν ότι οι δρομολογητές BGP προτιμούν μικρότερες διαδρομές ο επιτιθέμενος θα προσπαθήσει να δεσμεύσει κατά μέσο όρο το 50% της κυκλοφορίας. Στην δεύτερη περίπτωση, ο επιτιθέμενος θα προσπαθήσει να προσελκύσει όλη την κυκλοφορία προς την διεύθυνση προορισμού. Όσον αφορά την εσωτερική κίνηση σε ένα AS δεν μπορεί να εκτραπεί καθώς η δρομολόγηση του δεν έχει σχέση με το πρωτόκολλο BGP, αλλά με εσωτερικά πρωτόκολλά. Για παράδειγμα, σκοπεύοντας ο εισβολέας να προσελκύσει όλη την κίνηση που προορίζεται για το πρόθεμα p, θα μπορούσε να παραπλανήσει κάνοντας "advertisement" δύο διαφορετικά προθέματα p' και p''. Σε μια τέτοια περίπτωση οι δρομολογητές σε ολόκληρο το δίκτυο θα άρχιζαν τότε να προωθούν οποιαδήποτε κυκλοφορία που προορίζεται στο αρχικό πρόθεμα p, σε αυτά των p' και p''. Στο σημείο αυτό, θα πρέπει να αναφέρουμε ότι υπάρχουν δύο ειδών επιθέσεις δρομολόγησής. Το ένα είδος αναφέρεται στις επιθέσεις "**Partitioning**", ενώ η δεύτερη είναι γνωστή ως "**Delay**" επιθέσεις και αφορά την καθυστέρηση της μετάδοσης των μπλοκ.

Partitioning attacks

Σε αυτή την επίθεση, ένας αντίπαλος σε επίπεδο AS, προσπαθεί να απομονώσει ένα σύνολο από κόμβους έστω N από το υπόλοιπο δίκτυο, διαμερίζοντας κατά κάποιο τρόπο το bitcoin σε δύο χωριστά σημεία. Αναλυτικότερα, το περιεχόμενο του συνόλου N, εξαρτάται από τους στόχους του εισβολέα και συνήθως κατέχει ένα σημαντικό ποσοστό της συνολικής εξορυκτικής ισχύς (Zohar et al., 2017). Σχετικά με την διαδικασία της επίθεσης, ο επιτιθέμενος εκτρέπει αρχικά την κυκλοφορία που προορίζεται για κόμβους του συνόλου N, στοχεύοντας να χωρίσει το δίκτυο σε τουλάχιστον δύο ξεχωριστά μέρη,

έτσι ώστε να μη μπορεί να ανταλλάσσεται καμιά πληροφορία μεταξύ τους. Για να υποκλέψει όμως την κυκλοφορία, ο επιτιθέμενος δικτύου βασίζεται σε ευπάθειες στο πρωτόκολλο BGP, το οποίο δεν επικυρώνει τις ανακοινώσεις προέλευσης δρομολόγησης. Αυτές οι επιθέσεις περιλαμβάνουν την ψευδή αναφορά ενός δρομολογητή ότι υπάρχει καλύτερη δρομολόγηση σε κάποιο IP πρόθεμα. Με την παραβίαση όλων των προθεμάτων IP που σχετίζονται με τους κόμβους σε ένα μέρος του δικτύου, ο επιτιθέμενος μπορεί να παρεμποδίσει αποτελεσματικά όλη την κίνηση που ανταλλάσσεται μεταξύ των δύο μερών του δικτύου. Έτσι ο επιτιθέμενος θα μπορέσει να αποκόψει όλες αυτές τις συνδέσεις αποσυνδέοντας τα 2 μέρη και αναχαιτίζοντας την πορεία των bitcoin όπως φαίνεται στο παρακάτω σχήμα.



Εικόνα 29:Απεικόνιση "partitioning attack" όπου ένας επιτιθέμενος (AS8) αποσυνδέει την κίνηση μεταξύ των 2 μερών κλέβοντας προθέματα για να απομονώσει το σύνολο των κόμβων P = (A, B,C,D,E,F) [5]

Στο παραπάνω σχήμα, έχουμε μια δομή δικτύου που αποτελείται από 8 αυτόνομα συστήματα (AS) κάποια εκ των οποίων είναι bitcoin κόμβοι. Δεξιά και αριστερά των κόμβων απεικονίζονται δύο διαφορετικά "mining pools" (ομάδα ανθρακωρύχων). Στο σχήμα οι μπλε γραμμές ορίζουν τις αρχικές συνδέσεις κόμβων και με κόκκινες γραμμές τι

[5] Ανακτήθηκε από:
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7958588

συνδέσεις κόμβων που έχουν υποστεί την επίθεση. Όπως παρατηρείται και οι 2 πισίνες έχουν πύλες που συνδέονται σε διαφορετικά AS. Για παράδειγμα, η δεξιά πισίνα έχει πύλες που φιλοξενούνται στα συστήματα AS4, AS5, AS6 (Zohar et al., 2017). Επιπλέον για την επεξήγηση του σχήματος, οι μπλε γραμμές αντιπροσωπεύουν τις αρχικές συνδέσεις Bitcoin, οι κόκκινες τις συνδέσεις που έχουν εκτραπεί εξαιτίας της επίθεσης Hijacking και με διακεκομμένο μαύρο είναι οι ιδιωτικές συνδέσεις μεταξύ των "mining pools". Οποιοδήποτε σύστημα από αυτά μπορεί να παρεμποδίσει το μονοπάτι μιας σύνδεσης.

Έστω τώρα μια επίθεση που ξεκινάει από το σύστημα AS8 του σχήματος σκοπεύει να απομονώσει το σύνολο κόμβων P=(A,B,C,D,E,F). Αρχικά πειράζει τα προθέματα τα οποία σχετίζονται με τα συστήματα AS1, AS2, AS6 καθώς αποτελούν "host" για όλους τους κόμβους του ορισμένου συνόλου P, ελέγχοντας ουσιαστικά την κυκλοφορία που προέρχεται από αυτούς τους κόμβους. Έπειτα, το AS8 απορρίπτει όλες τις συνδέσεις των αρχικών συνδέσεων (μπλε γραμμές σχήματος), όπως για παράδειγμα (A,J), (B,J) και (E,F). Επιπλέον παρατηρώντας ότι ο κόμβος F ∈ P και παράλληλα είναι κόμβος της κόκκινης (δεξιάς) mining pool. Έχοντας αυτά τα χαρακτηριστικά, ο κόμβος F ενδέχεται να μην ανήκει στο πρωτόκολλο bitcoin. Ως εκ τούτου, ακόμα και αν ο επιτιθέμενος ρίξει όλο το bitcoin δίκτυο ο κόμβος F ανήκοντας σε "mining pool" θα έχει πληροφορίες σχετικά με τις εξελίξεις (δημιουργία νέων μπλοκ), οι οποίες πληροφορίες ενδέχεται να διαρρεύσουν στο σύνολο P. Συνεπώς επειδή θεωρείται αδύνατη η απομόνωση του P από τον επιτιθέμενο, το μόνο που μπορεί να πράξει, είναι να περιορίσει τον στόχο του σε ένα νέο σύνολο κόμβων K= (A,B,C.D,E) αποκλείοντας ουσιαστικά τον κόμβο F, όπου K⊂P και μάλιστα K=max{subP}.

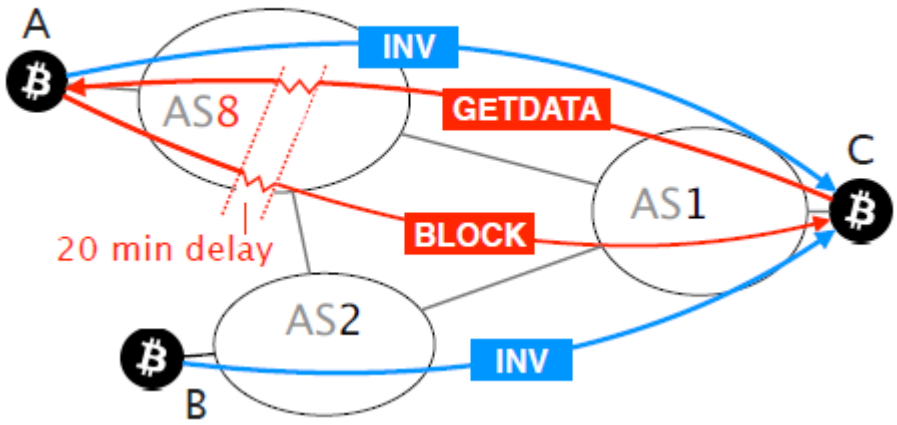
Όσον αφορά το μέγεθος της **επίδρασης** μιας τέτοιας επίθεσης στο blockchain σύστημα, είναι κάτι που εξαρτάται από τον αριθμό των απομονωμένων κόμβων που υπάρχουν στο δίκτυο καθώς και την εξορυκτική ισχύ που κατέχουν συνολικά σε αυτό. Πιο συγκεκριμένα, η απομόνωση κόμβων ουσιαστικά ευνοεί την περίπτωση της επίθεσης "0-confirmation" διπλής δαπάνης. Κάτι τέτοιο θα έχει ως επίδραση στην μείωση της ισχύς εξόρυξης στο δίκτυο, το οποίο με την σειρά του εκδηλώνει την πιθανότητα δημιουργία διακλάδωσης στην αλυσίδα.

Delay attack

Σε μια επίθεση καθυστέρησης, ο στόχος του επιτιθέμενου είναι να επιβραδύνει την δημιουργία νέων μπλοκ που αποστέλλονται σε ένα σύνολο κόμβων bitcoin. Όπως και στην περίπτωση της "partitioning" επίθεσης έτσι και στην "Delay", η επίθεση μπορεί να είναι στοχευμένη με την έννοια ότι θα επικεντρώνεται σε συγκεκριμένους κόμβους, έχοντας ως σκοπό την διατάραξη της επίτευξής της διαδικασίας της συναίνεσης για το δίκτυο (Zohar et al., 2017). Ειδικότερα, στην "Delay" επίθεση ο επιτιθέμενος μπορεί να καθυστερήσει την συνολική διάδοση των μπλοκ προς ένα κόμβο, πράγμα το οποίο ισχύει ακόμη και αν παρεμποδίσει τελικά ένα υποσύνολο των συνδέσεων του.

Οι επιθέσεις "Delay" αξιοποιούν τρείς βασικές πτυχές του bitcoin πρωτόκολλου. Αναλυτικότερα, ένας bitcoin κόμβος περιμένει 20 λεπτά από την στιγμή αίτησης μπλοκ από κάποιο ομότιμο κόμβο, προτού προβεί σε κάποια νέα αίτηση από κάποιο άλλο κόμβο, ώστε να αποφευχθεί η υπερφόρτωση του δικτύου με υπερβολικές μεταδόσεις μπλοκ. Αυτός ο σχεδιαστικός τρόπος, σε συνδυασμό με το γεγονός ότι η κίνηση του bitcoin δεν είναι κρυπτογραφημένη δημιουργεί ευνοϊκότητα ως προς την δημιουργία επίθεσης, όπου ο εισβολέας εμποδίζει την «κίνηση» του bitcoin, δημιουργώντας καθυστερήσεις στην διάδοση μπλοκ ως προς τις αντίστοιχες συνδέσεις. Επιπλέον, καθώς τα μηνύματα δεν προστατεύονται από παραβιάσεις, ούτε ο παραλήπτης ούτε ο αποστολέας έχουν καμία ένδειξη ότι το μήνυμα έχει τροποποιηθεί (μη κρυπτογραφημένα), δίνοντας «χώρο» στον εισβολέα.

Όπως φαίνεται στο παρακάτω σχήμα τα μηνύματα που ανταλλάσσουν οι παρακάτω κόμβοι είναι τα INV, GETDATA και BLOCK. Στο παράδειγμα της παρακάτω εικόνας, θεωρούμε ως επιτιθέμενο το σύστημα AS8 και ως C το θύμα. Ακόμη θεωρείται ότι οι κόμβοι A και B αιτούνται την μετάδοση ενός μπλοκ (έστω μπλοκ X) στο C μέσω του μηνύματος INV. Όπως φαίνεται στο σχήμα, το μήνυμα στέλνεται αρχικά από το κόμβο A σε αυτό του C. Στην συνέχεια, ο κόμβος C στέλνει ένα μήνυμα GETDATA πίσω στον κόμβο A, ζητώντας την μετάδοση του μπλοκ X, το οποίο ξεκινά μια μέτρηση χρονικού ορίου 20 λεπτών. Ο επιτιθέμενος αρχικά τροποποιεί το μήνυμα GETDATA που λαμβάνει ο κόμβος A, ελέγχοντας έτσι το περιεχόμενο του μηνύματος. Με αυτό τον τρόπο, ο εισβολέας μπορεί να καθυστερήσει την μετάδοση του μπλοκ ξεπερνώντας έτσι το όριο των 20 λεπτών, αποφεύγοντας έτσι τον εντοπισμό και την αποσύνδεση του. Εναλλακτικά, θα μπορούσε απλά να τροποποιήσει το μπλοκ X.



Εικόνα 30:Απεικόνιση επίθεσης "Delay"[6]

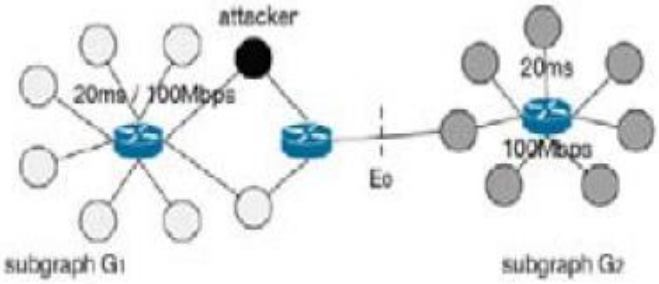
Καταλήγοντας, ο πραγματικός αντίκτυπος μιας τέτοιας επίθεσης κυμαίνεται από την επίτευξη μιας καταστάσεως "double spending" (για τους κόμβους του «εμπόρου») έως την σπατάλη υπολογιστικής ισχύος (για τους ανθρακωρύχους).

3.1.1.1.5 Balance Attack

Η επίθεση Balance αποτελεί μια επίθεση που επηρεάζει τον αλγόριθμο "Proof of Work" και ιδιαίτερα το blockchain 2.0 και την περίπτωση του Ethereum. Κατά την επίθεση ισορροπίας (balance attack), ένας εισβολέας διακόπτει παροδικά την επικοινωνία μεταξύ υποομάδων παρόμοιας εξορυκτικής ισχύος. Ειδικότερα, θεωρείται ότι ο εισβολέας εκδίδει συναλλαγές σε μια υποομάδα (συναλλαγών) και πραγματοποιεί εξόρυξη μπλοκ σε μια διαφορετική υποομάδα (μπλοκ). Με άλλα λόγια, οι εισβολείς προσπαθούν να ομαδοποιήσουν τους κόμβους εξόρυξης σε δύο ίσες ομάδες έστω G_1 (υποομάδα συναλλαγών) και G_2 (υποομάδα εξόρυξης). Η λογική αυτής της ευπάθειας σχετίζεται με τον γνωστό κανόνα της «μεγαλύτερης διακλάδωσης» (Natoli & Gramoli, 2016). Στο πλαίσιο αυτό, μέσω μιας καθυστέρησης στην διάδοση των μπλοκ στο σύστημα, θα μπορεί κάποιος ανθρακωρύχος να αυξήσει τον αριθμό των μπλοκ που σπαταλούν ποσό εξορυκτικής ισχύς και με αυτό τον τρόπο να επιτυγχάνεται αναλογικά μια επιβράδυνση στην διαδικασία δημιουργίας μεγαλύτερης αλυσίδας (διακλάδωσης) στο σύστημα.

[6] Ανακτήθηκε από:
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7958588

Ωστόσο, η καθυστέρηση αυτή ενδέχεται να δημιουργήσει μια κατάσταση διπλής δαπάνης. Για την καλύτερη κατανόηση της παραπάνω συνθήκης θεωρούμε ότι ο εισβολέας στέλνει συναλλαγές στην υποομάδα G_1, ξεκινώντας όμως και την εξόρυξη στην υποομάδα G_2. Πιο συγκεκριμένα, Θεωρούμε για k=2 τα υπογραφήματα G_1= <V_1, E_1> και G_2=<V_2, E_2> ενός γραφήματος G=<V, E> έτσι ώστε κάθε υπογράφημα/υποομάδα να διαθέτει την μισή εξορυκτική ισχύ της συνολικής (ίση ισχύς μεταξύ τους) που υπάρχει στο σύστημα (Natoli & Gramoli, 2016). Επιπλέον θεωρείται ένα σύνολο ακμών (edge set) ενός γραφήματος έστω E_0, στο οποίο συνδέονται οι κόμβοι V_1 με τους κόμβους V_2. Ακόμη, θα χρειαστεί να οριστεί η καθυστέρηση των συνδέσεων η οποία προκαλείται από τον επιτιθέμενο στις ακμές του γραφήματος. Αναλυτικότερα, ο επιτιθέμενος προσπαθεί να δημιουργήσει μια μεγάλη καθυστέρηση κατά την οποία οι ανθρακωρύχοι της υποομάδας G_1 πραγματοποιούν εξόρυξη ανεξάρτητα (σε απομόνωση) από αυτούς της υποομάδας G_2.



Εικόνα 31:Συναλλαγή στην υποομάδα G_1 και εξόρυξη στην υποομάδα G_2[7]

Το γεγονός αυτό επιφέρει ως συνέπεια διαφορετικές συναλλαγές να πραγματοποιούνται σε διαφορετική σειρά μπλοκ μεταξύ των δύο αλυσίδων που προκύπτουν από τις G_1, G_2. Στο σημείο αυτό θεωρούμε ένα μπλοκ B το οποίο βρίσκεται μόνο στο blockchain που προβάλλεται από την G_2. Ο επιτιθέμενος εκδίδει συναλλαγές δαπανώντας νομίσματα στην G_1 και πραγματοποιεί εξόρυξη ξεκινώντας με το μπλοκ B στην G_2, πριν την λήξη της καθυστέρησης.

Μετά την λήξη της καθυστέρησης και μέσω της εφαρμογής του αλγορίθμου συναίνεσης η αλυσίδα G_2 θα είναι μεγαλύτερη και συνεπώς τα μπλοκ της θα διατηρούνται ως έγκυρα και θα καταγράφονται στο καθολικό blockchain (Natoli & Gramoli, 2016). Στην ουσία, μέσω αυτής της μεθόδου ένας εισβολέας στέλνει μια συναλλαγή στην G_1 και

[7] https://arxiv.org/pdf/1612.09426.pdf

στοχεύει στην αγορά ενός αγαθού με ένα μικρό αριθμό επιβεβαιώσεων (συνήθως τρείς), προκειμένου ο έμπορος να προσφέρει την υπηρεσία στον επιτιθέμενο. Το κρίσιμο σημείο σε αυτή την περίπτωση, είναι ότι ο επιτιθέμενος στέλνει το ίδιο ποσό νομίσματος εκτός από την G_1 και σε διαφορετική διεύθυνση πορτοφολιού στην G_2. Συμπερασματικά, οι συναλλαγές που εστάλησαν στην G_2, θα θεωρούνται έγκυρες και ως εκ τούτου ο επιτιθέμενος χρησιμοποιεί τα ίδια νομίσματα δύο φορές προκαλώντας το πρόβλημα της διπλής δαπάνης.

3.1.1.2 Επιθέσεις στο πρωτόκολλο του blockchain

Οι επιθέσεις πρωτοκόλλου blockchain αποτελούν μια υποκατηγορία της γενικότερης κατηγορίας των επιθέσεων στο πρωτόκολλο επικοινωνίας. Έτσι η συγκεκριμένη υποκατηγορία αποτελείται από τις επιθέσεις “Refund attack”, “Transaction Privacy Leakage”, “Transaction Malleability”, “Timejacking”.

3.1.1.2.1 Transaction Privacy Leakage

Στα δημόσια blockchain οι συναλλαγές είναι ανοιχτές και διαφανείς. Αυτό συμβαίνει επειδή η αρχιτεκτονική τους καθιστά κάθε συναλλαγή ανιχνεύσιμη. Με αυτή την έννοια, η δημοσιότητα των δεδομένων στο δίκτυο διατηρεί τις πληροφορίες συγχρονισμένες, γεγονός που επιτρέπει την επίτευξη συναίνεσης μεταξύ των κατανεμημένων κόμβων. Δεδομένου λοιπόν ότι οι συμπεριφορές των χρηστών είναι ανιχνεύσιμες, τα συστήματα blockchain λαμβάνουν μέτρα για την προστασία της ιδιωτικότητας των συναλλαγών των χρηστών (X. Li, Jiang, Chen, Luo, & Wen, 2020). Για παράδειγμα, στο bitcoin αλλά και στην διακλάδωση του Zcash, οι συναλλαγές υπογράφονται ψηφιακά με το ιδιωτικό κλειδί του χρήστη και με αυτό τον τρόπο η ιδιωτικότητα της συναλλαγής παραμένει ασφαλής. Έτσι η αποθήκευση του ιδιωτικού κλειδιού σε κάθε συναλλαγή από τον χρήστη αποτρέπει από τον επιτιθέμενο να μπορέσει να συμπεράνει αν το κρυπτονόμισμα σε διαφορετικές συναλλαγές λαμβάνεται από τον ίδιο χρήστη.

Ωστόσο στο κρυπτονόμισμα Monero, υπάρχει μια προαιρετική διάταξη για την χρήση των λεγόμενων «μιξίνων» για την προστασία των πληροφοριών σχετικά με το πόσο κέρμα δαπανάται σε μια συναλλαγή και συγκεκριμένα κρύβοντας από τον εισβολέα την σύνδεση των πραγματικών νομισμάτων που δαπανήθηκαν από την συναλλαγή (X. Li et

al., 2020). Ωστόσο, διαπιστώθηκε ότι περίπου το στο 66% των συναλλαγών δεν βρέθηκαν «μιξίνες» κρίνοντας το μέτρο αυτό ως όχι τόσο αποτελεσματικό. Έτσι, μια συναλλαγή με 0-μιξίνες θα οδηγήσει σε διαρροή απορρήτου του αποστολέα της. Ειδικότερα, μια συναλλαγή χωρίς «μιξίνες» μπορεί να χρησιμοποιηθεί για την ανακάλυψη μεγαλύτερης ποσότητας συναλλαγών, γεγονός το οποίο μπορεί να χρησιμοποιηθεί για την έναρξη ορισμένων εξελιγμένων επιθέσεων όπως η επίθεση “man-in-the-middle” ή η επίθεση “Transaction malleability”.

3.1.1.2.2 Refund attack

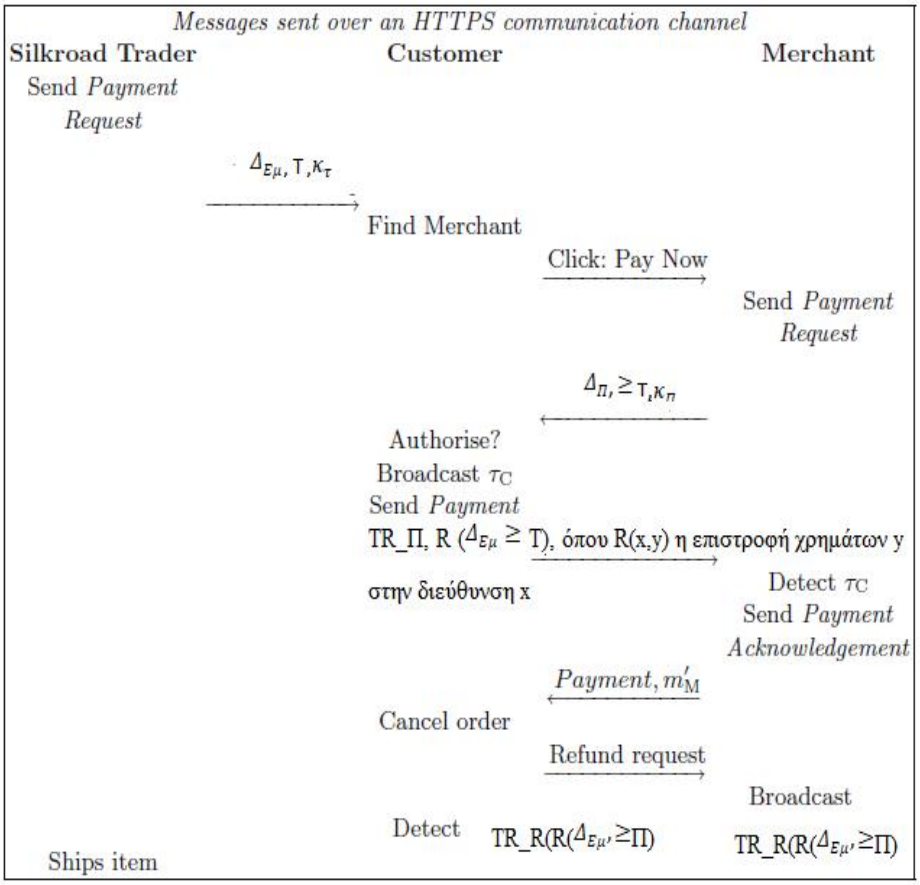
Η Refund attack στοχεύει στην απόκτηση παράνομων εσόδων, ενώ ο επιτιθέμενος χρησιμοποιεί προς όφελος του τις ευνοϊκές για αυτόν πολιτικές επιστροφής χρημάτων. Επιπλέον η επίθεση θεωρείται ότι κατηγοριοποιείται περαιτέρω σε δύο μορφές: Η επίθεση “SilkRoad”, η οποία αφορά μια ευπάθεια ελέγχου ταυτότητας στο BIP 70 (Bitcoin Improvement Proposal) και η “Marketplace Trader” επίθεση, στην οποία γίνεται κατάχρηση των πολιτικών επιστροφής χρημάτων των υπάρχοντών διεκπεραιωτών πληρωμών. Όσον αφορά το BIP 70 πρόκειται για μια προτεινόμενη αλλαγή στο πρωτόκολλο του Bitcoin (“Bips/Bip-0070.Mediawiki at Master · Bitcoin/Bips · GitHub,” n.d.). Το πρωτόκολλο BIP 70 υποστηρίζεται από πολλά πορτοφόλια, ενώ ο στόχος του θα μπορούσε να περιγράφει ως εξής: Το BIP 70 περιγράφει ένα πρωτόκολλο επικοινωνίας μεταξύ ενός εμπόρου και του πελάτη του, επιστρέφοντας τόσο καλύτερη «εμπειρία» για τον πελάτη όσο και καλύτερη ασφάλεια έναντι επιθέσεων “man in the middle” στην διαδικασία πληρωμής.

Πιο συγκεκριμένα, η επικοινωνία μεταξύ του πελάτη και του εμπόρου στέλνεται μέσω πρωτοκόλλου HTTPS, ενώ ο πελάτης είναι παράλληλα υπεύθυνος για την μετάδοση της πληρωμής συναλλαγής στο δίκτυο Bitcoin. Να σημειωθεί ότι οι επιθέσεις βασίζονται στην αδυναμία του εμπόρου να αποτρέψει το γεγονός, αν η διεύθυνση επιστροφής χρημάτων προέρχεται από τον ίδιο πελάτη που εξουσιοδότησε την πληρωμή. Επίσης, αυτές οι επιθέσεις είναι επιτυχείς ακόμα και όταν όλα τα μηνύματα αποστέλλονται μέσω καναλιού επικοινωνίας HTTPS.

1)Silkroad Attack

Στην επίθεση Silkroad ένας πελάτης βρίσκεται υπό τον έλεγχο ενός κακόβουλου εμπόρου. Έτσι όταν ένας πελάτης ξεκινά τις συναλλαγές με τον έμπορο η διεύθυνση του αποκαλύπτεται στον κακόβουλο έμπορο. Όταν η συναλλαγή ολοκληρώνεται, ο αντίπαλος ξεκινά την επίθεση εισάγοντας την διεύθυνση των πελατών ως διεύθυνση επιστροφής χρημάτων στον έμπορο-προμηθευτή. Τότε, αυτός στέλνει το ποσό στον Silkroad και με αυτό τον τρόπο εξαπατάται χωρίς να λάβει επιστροφή χρημάτων από τον κακόβουλο έμπορο. Μια τέτοια περίπτωση επίθεσης είναι, όταν ένας πελάτης επιθυμεί να πουλήσει ένα παράνομο προϊόν από ένα έμπορο (Εμ), πραγματοποιεί τότε αυτή την επίθεση για να αρνηθεί την συμμέτοχή του στην συναλλαγή, εκμεταλλευόμενος ένα το τρίτο μέρος που υπάρχει στο σύστημα, ένα προμηθευτή (Π) (McCorry, Shahandashti, & Hao, 2017). Στο συγκεκριμένο σύστημα ο πελάτης αποτελεί και τον επιτιθέμενο (Επ), έχοντας ως στόχο της επίθεσης του, τον προμηθευτή (Π). Τα ακριβή βήματα της Silkroad επίθεσης περιγράφονται παρακάτω:

- Ο πελάτης (Επ) κατεβάζει από τον ιστότοπο του εμπόρου “Silkroad trader” (Εμ) ένα μήνυμα αίτησης πληρωμής στο οποίο περιέχεται η διεύθυνση του εμπόρου $\Delta_{E\mu}$, η τιμή πληρωμής (Τ) και το δημόσιο κλειδί του εμπόρου (κ_{τ}).
- Η αναζήτηση για προμηθευτή “Merchant” (Π) που πουλάει ένα προϊόν σε τιμή ίση ή μεγαλύτερη από αυτή του παρανόμου (Silkroad trader). Όταν βρεθεί κάποιος προμηθευτής, ο (Επ) ξεκινάει την διαδικασία πληρωμής για το προϊόν του προμηθευτή, «κατεβάζοντας» ένα μήνυμα αίτησης πληρωμής που περιέχει την διεύθυνση του προμηθευτή (Δ_{Π}), την τιμή πληρωμής (Τ) και το δημόσιο κλειδί του προμηθευτή (κ_{Π}).
- Το πορτοφόλι του πελάτη-επιτιθέμενου αναγνωρίζει τη συναλλαγή πληρωμής και εισάγει την διεύθυνση του εμπόρου ($\Delta_{E\mu}$), στο μήνυμα αίτησης πληρωμής ως την διεύθυνση επιστροφής χρημάτων.
- Με την λήψη του μηνύματος επιβεβαίωσης πληρωμής από τον προμηθευτή (Merchant), ο πελάτης ακυρώνει την παραγγελία και ζητά επιστροφή χρημάτων από τον προμηθευτή.
- Εάν ο προμηθευτής συμβαδίζει με την παραλλαγή στο πρωτόκολλο του bitcoin BIP 70, τα κέρματα που επιστρέφονται αποστέλλονται στον έμπορο (Silkroad trader).



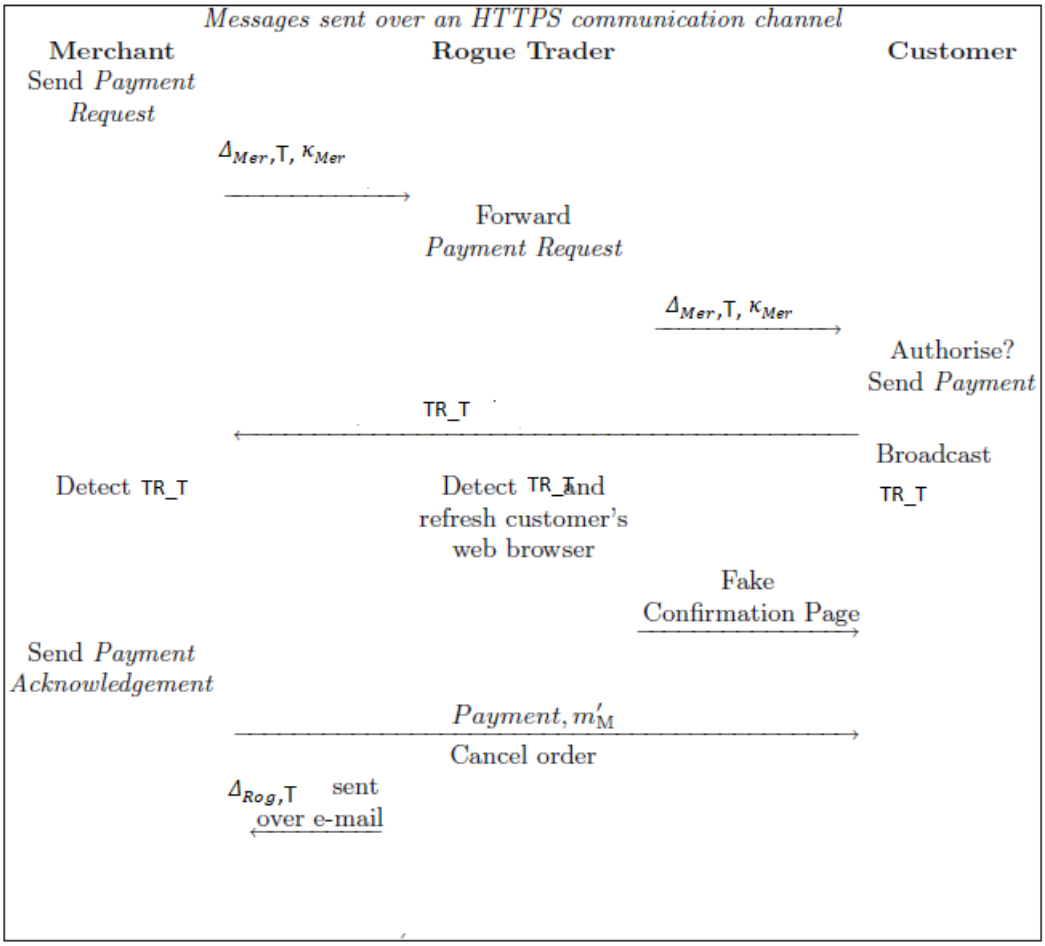
Εικόνα 32:Σχηματική απεικόνιση της επίθεσης "Silkroad

2) Marketplace Trader Attack

Η συγκεκριμένη επίθεση, αποτελεί μια τυπική περίπτωση επίθεσης "man in the middle attack". Σε αυτή την επίθεση η ρύθμιση του αντιπάλου είναι ένας «ελκυστικός» ιστότοπος, όπου θα προσελκύσει τον πελάτη όπου θα γίνει στην συνέχεια θύμα. Ειδικότερα, ο εισβολέας απεικονίζει τον εαυτό του ως έμπιστο μέρος πραγματοποιώντας πληρωμές μέσω ενός αξιόπιστου εμπόρου. Έτσι όταν ο πελάτης συνδεθεί στον ιστότοπο, αποκαλύπτει κατά λάθος την διεύθυνση του και άλλες πληροφορίες που αρκούν για τον κακόβουλο έμπορο με τον ψεύτικο ιστότοπο (Conti, Sandeep Kumar, Lal, & Ruj, 2018). Στην επίθεση "Market place Trader" ένας απατεώνας έμπορος, ο οποίος αποτελεί τον επιτιθέμενο δημιουργεί ένα ιστότοπο στον οποίο προϊόντα και άλλα εμπορεύματα πωλούνται σε τιμές χαμηλότερες της αγοράς, πραγματοποιώντας πληρωμές μέσω ενός μεγάλου αξιόπιστου λιανοπωλητή, ώστε οι πελάτες να νιώθουν ασφάλεια (McCorry et al., 2017). Έτσι, μόλις εξαπατηθεί ένας πελάτης αγοράζοντας ένα προϊόν στον ιστότοπο, ο επιτιθέμενος (έμπορος) ακυρώνει την παραγγελία και κερδίζει τα έσοδα ζητώντας από

τον πωλητή να επιστρέψει τα χρήματα στον έμπορο και συγκεκριμένα τα bitcoin που πληρωθήκαν από τον πελάτη. Όπως αναφέρθηκε, αυτή την φορά ο έμπορος (Εμ) είναι ο επιτιθέμενος ενώ ο πελάτης (Π) είναι ο στόχος. Τα ακριβή βήματα της "Marketplace Trader" επίθεσης περιγράφονται παρακάτω:

- Ο επιτιθέμενος έμπορος (Rogue Trader) δημιουργεί ένα ιστότοπο, όπου πωλούνται προϊόντα σε χαμηλότερες τιμές από αυτές της αγοράς, ενώ καταφέρνει να παρουσιάζεται ως ένας αξιόπιστος έμπορος μέσω ενός αξιόπιστου λιανοπωλητή (Merchant).
- Μόλις ο πελάτης αγοράσει το προϊόν του από τον απατεώνα έμπορο (rogue trader), τότε ο έμπορος λαμβάνει από τον ιστότοπο του αξιόπιστου λιανοπωλητή (Merchant), ένα μήνυμα αίτησης πληρωμής που περιέχει την διεύθυνση του Merchant (Δ_{Mer}) , την τιμή (Τ) και το δημόσιο κλειδί του Merchant (κ_{Mer}), προωθώντας στο στον πελάτη.
- Το πορτοφόλι του πελάτη ανοίγει το πραγματικό μήνυμα αίτησης πληρωμής που εμφανίζει το όνομα του αξιόπιστου εμπόρου (Merchant). Αυτό θα έχει ως αποτέλεσμα την εμπιστοσύνη του πελάτη στον επιτιθέμενο έμπορο (Rogue Trader) και ως συνέπεια αυτού να στείλει τη συναλλαγή πληρωμής στον έμπορο Merchant (TR_T).
- Όταν ο ιστότοπος του επιτιθέμενου εμπόρου ανιχνεύει την συναλλαγή TR_T στο δίκτυο, τότε ανανεώνει το πρόγραμμα περιήγησης ιστού του πελάτη για να εμφανίσει μια ψεύτικη σελίδα επιβεβαίωσης.
- Ο επιτιθέμενος έμπορος ενημερώνει τον αξιόπιστο έμπορο (Merchant) για την ακύρωση της παραγγελίας του πελάτη και στην συνέχεια στέλνει σε αυτόν ένα email που περιέχει τη διεύθυνση επιστροφής χρημάτων (Δ_{Rog}) και την τιμή Τ.
- Τέλος, με βάση την πολιτική που επιτρέπει τον έλεγχο ταυτότητας μέσω email τα νομίσματα αξίας Τ που έχουν σταλεί στην διεύθυνση Δ_{Rog}.



Εικόνα 33:Σχηματική απεικόνιση της επίθεσης "Marketplace Trader"

3.1.1.2.3 Time jacking attack

Σε ένα πλήρη κόμβο, με βάση την δομή ενός μπλοκ στο πεδίο της κεφαλίδας μπλοκ εμπεριέχεται μια χρονική σήμανση όπου ουσιαστικά αποτελεί ένα πεδίο αποθήκευσης δεδομένων που αφορούν την ακριβή στιγμή κατά την οποία το μπλοκ εξορύχθηκε και επικυρώθηκε από το δίκτυο της αλυσίδας μπλοκ.

Το πρόβλημα της συγκεκριμένης επίθεσης προκύπτει όταν αναγγέλλονται ανακριβείς χρονικές σημάνσεις κατά την σύνδεση σε ένα κόμβο, γεγονός όπου θα αποτελέσει ευνοϊκή συνθήκη για ένα εισβολέα ώστε να μπορέσει να αλλάξει τον μετρητή χρόνου δικτύου ενός κόμβου και να τον εξαπατήσει ώστε να δεχθεί μια εναλλακτική αλυσίδα μπλοκ (Tareq, n.d.). Κάτι τέτοιο θα μπορούσε να αυξήσει σημαντικά τις πιθανότητες επιτυχούς επίτευξης της επίθεσης "double spending", να εξαντλήσει τους

υπολογιστικούς πόρους ενός κόμβου ή απλά να επιβραδύνει τον ρυθμό επιβεβαίωσης της συναλλαγής.

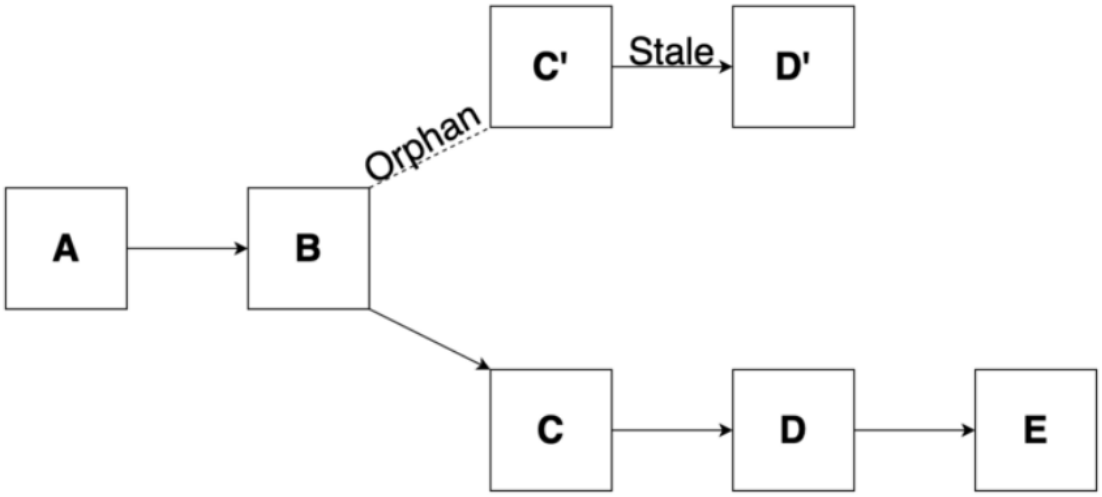
Όσον αφορά την πραγματοποίηση της επίθεσης, θεωρούμε ότι κάθε κόμβος διατηρεί εσωτερικά ένα μετρητή που αντιπροσωπεύει τον χρόνο δικτύου. Αυτό σχετίζεται με τον μέσο χρόνο των ομότιμων ενός κόμβου, δηλαδή με τον χρόνο που αποστέλλεται το μήνυμα έκδοσης όταν συνδέονται ομότιμοι κόμβοι. Ουσιαστικά, ο μετρητής χρόνου δικτύου επιστρέφει τον χρόνο του συστήματος με την προϋπόθεση όμως ότι ο μέσος χρόνος διαφέρει περισσότερο από 70 λεπτά από την ώρα του συστήματος. Ένας εισβολέας θα μπορούσε ενδεχομένως να επιβραδύνει ή να επιταχύνει τον μετρητή χρόνου δικτύου ενός κόμβου συνδεόμενος με πολλαπλούς κόμβους δικτύου και καταγράφοντας σε αυτούς λανθασμένες χρονικές σημάνσεις ("Culubas: Timejacking & Bitcoin," n.d.). Έτσι, σε ένα ενδεχόμενο επίθεσης που θα υπήρχε επιτάχυνση των τιμών χρόνου στους περισσότερους ανθρακωρύχους του δικτύου, παράλληλα θα υπήρχε και επιβράδυνση στον μετρητή χρόνου του κόμβου στόχου. Λαμβάνοντας ως δεδομένο, ότι η χρονική τιμή ενός μετρητή μπορεί να μεταβληθεί έως 70 λεπτά, η διαφορά μεταξύ των κόμβων θα μπορεί να φτάσει τα 140 λεπτά. Θα πρέπει να σημειωθεί ότι ο χρόνος δικτύου αξιοποιείται στην διαδικασία επικύρωσης νέων μπλοκ διαδικασία η οποία θέτει άνω και κάτω όρια σε σχέση με το αποδεκτό εύρος των χρονικών σφραγίδων μπλοκ, ενώ οι κόμβοι δεν δέχονται τις χρονικές σημάνσεις μπλοκ στις παρακάτω περιπτώσεις:

- Αν η χρονική σήμανση στο μπλοκ είναι περισσότερη από 2 ώρες σε σχέση με την τρέχουσα χρονική σήμανση στο δίκτυο.
- Οι χρονικές σημάνσεις μπλοκ που είναι προγενέστερες σε σχέση με τον μέσο χρόνο των τελευταίων 11 μπλοκ.

Σε ένα ενδεχόμενο για παράδειγμα, όπου ο επιτιθέμενος με το 10% της υπολογιστικής ισχύς του δικτύου θα μπορούσε να στείλει έξι επιβεβαιώσεις (οποιοδήποτε μπλοκ με περισσότερες από έξι επιβεβαιώσεις θεωρείται αμετάκλητο) σε διάστημα 5,5 ωρών άνω του 10%. Μετά από 6 επιβεβαιώσεις, η τυπική διεπαφή bitcoin
μεταβάλει την κατάσταση της σε επιβεβαιωμένη. Αντίστοιχα ο εισβολέας με το 10% της υπολογιστικής ισχύς αν έστελνε τις 6 επιβεβαιώσεις σε μικρότερο διάστημα των 3,5 ωρών το ποσοστό επιτυχίας θα έπεφτε περίπου στο 1%. Συνεπώς γίνεται αντιληπτό ότι, μια επίθεση χαμηλών πιθανοτήτων για να έχει πιθανότητες επιτυχίας θα πρέπει να επαναληφθεί αρκετές φορές.

Σενάριο επίθεσης σε κόμβο ανθρακωρύχο:

Αν ο στόχος της επίθεσης είναι ανθρακωρύχος, θα υπάρχει ως συνέπεια μείωση της εξορυκτικής του ισχύς, αφού θα έκανε προσπάθειες εξόρυξης σε μια ορφανή διακλάδωση της αλυσίδας (εικόνα), ενώ το δίκτυο θα εξελισσόταν σε διαφορετική αλυσίδα (“Culubas: Timejacking & Bitcoin,” n.d.). Στην περίπτωση έτσι ενός κακόβουλου ανθρακωρύχου, θα μπορούσε να επαναλάβει την παραπάνω διαδικασία πολλές φορές στους ανταγωνιστές ανθρακωρύχους του προκειμένου να αναλώνουν την προσπάθεια τους στην απορριπτόμενη διακλάδωση (παρόλο που τα μπλοκ αυτής είναι έγκυρα και



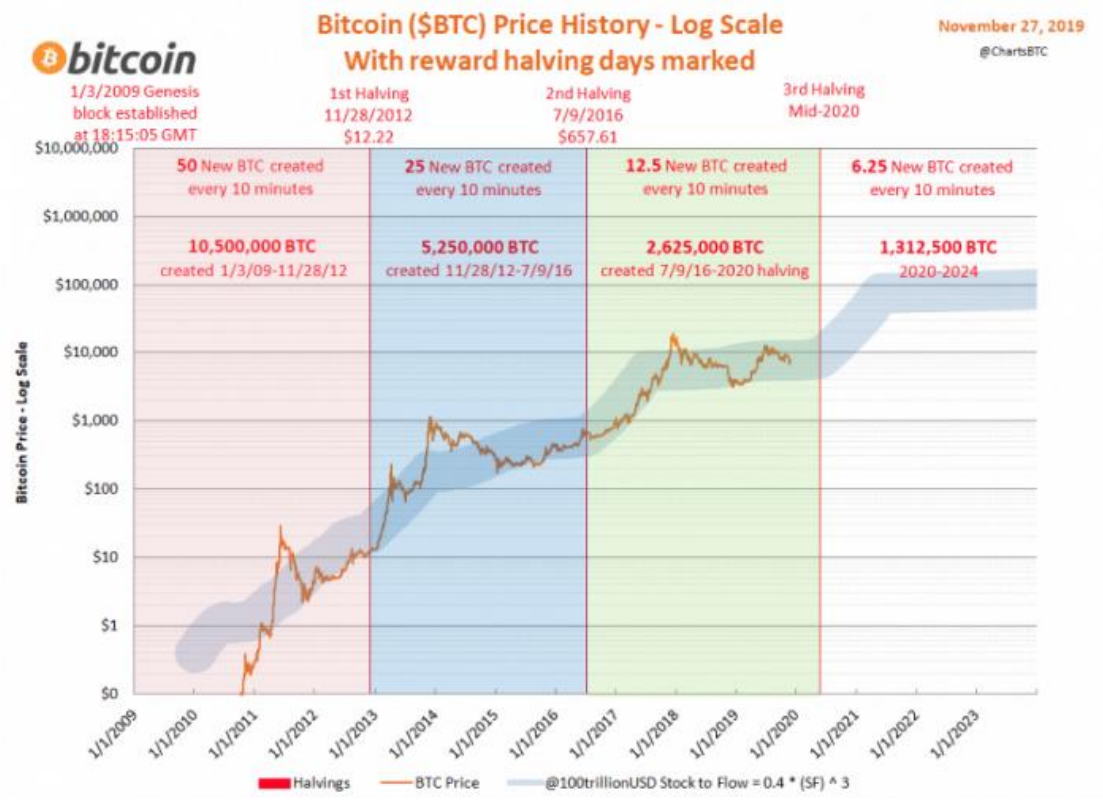
Εικόνα 34:Οι ανθρακωρύχοι των μπλοκ C΄, D΄ δεν λαμβάνουν ανταμοιβή για την προσπάθεια εξόρυξης.[8]

επικυρωμένα), προκειμένου να αυξήσει εις βάρος τους το μερίδιο του ως προς την συνολική υπολογιστική ισχύ του δικτύου. Θα πρέπει επίσης να τονιστεί ότι η συγκεκριμένη περίπτωση επίθεσης θα λειτουργεί ακόμη και αν ο χρόνος δικτύου του στόχου διέφερε μόνο κατά 1 δευτερόλεπτο από την πλειοψηφία των χρόνων που είχαν οι περισσότεροι κόμβοι στο δίκτυο (“Culubas: Timejacking & Bitcoin,” n.d.). Έτσι ο στόχος βλέποντας ότι το νέο μπλοκ ήταν ένα δευτερόλεπτο επιπλέον από το όριο των 2 ωρών θα προέβαινε στην απόρριψη του, με αποτέλεσμα να συνεχίζει την εξορυκτική του δράση επί της ορφανής διακλάδωσης.

[8] Ανακτήθηκε από: https://medium.com/coinmonks/an-in-depth-look-at-orphan-blocks-45baeaca9d28

Κίνητρα επίθεσης για τους ανθρακωρύχους

Η μέθοδος που χρησιμοποιεί τον υπολογισμό του μέσου χρόνου μπορεί να φαίνεται ότι είναι δίκαιη τουλάχιστον σε τεχνικό επίπεδο (“Culubas: Timejacking & Bitcoin,” n.d.), ωστόσο είναι ικανή να δημιουργήσει δυναμικά ελαττώματα μέσω της δημοσίευσης υψηλότερων χρονικών σημάνσεων κάνοντας το επίπεδο δυσκολίας χαμηλό.



Εικόνα 35:Υποδιπλασιασμός αξίας στην ανταμοιβή μπλοκ[9]

Δεδομένου ότι κάθε μπλοκ δίνει 6.25 bitcoin στον λογαριασμό του ανθρακωρύχου, διαπιστώνεται ότι με μια ρύθμιση χαμηλής δυσκολίας (αυτό σημαίνει ότι θα απαιτείται λιγότερη υπολογιστική ισχύς ως προς την επιτυχία δημιουργίας νέου μπλοκ) θα προέκυπτε μια δυναμική δημιουργίας περισσότερων μπλοκ σε λιγότερο χρόνο . Αυτό θα έχει ως

[999] Ανακτήθηκε από: https://www.coinmama.com/blog/the-bitcoin-halving-a-history

συνέπεια γρηγορότερη διεκπεραίωση συναλλαγών με τίμημα όμως την αξιοπιστία των επιβεβαιώσεων.

3.1.1.2.4 Transaction Malleability

Το κενό ασφαλείας με την ονομασία transaction malleability είναι γνωστό περίπου από το 2011 και σχετίζεται με την κλοπή bitcoin. Ωστόσο έχει καταγραφεί επίσης ότι έχει εφαρμοστεί ο παραπάνω όρος και σε επιθέσεις DDoS όπου επιτιθέμενοι χρησιμοποιούσαν το παραπάνω κενό ασφαλείας για την δημιουργία της DDoS, ώστε να σταματήσουν τις υπηρεσίες ελέγχου στο ανταλλακτήριο BitStamp το οποίο διαχειριζόταν τον μεγαλύτερο όγκο συναλλαγών σε κρυπτονομίσματα παγκοσμίως εκείνη την περίοδο.

Με την έννοια “transaction malleability” αναφερόμαστε σε ένα σχεδιαστικό ελάττωμα στο bitcoin εξαιτίας της δυνατότητας να υπάρξει τροποποίηση σε μια συναλλαγή μετά την δημιουργία της, αλλά πριν την προσθήκη του σε κάποιο μπλοκ. Αυτό θα έχει ως επακόλουθο την τροποποίηση της αλυσίδας. Προφανώς δεν μπορεί να τροποποιηθεί κάποια διεύθυνση είτε προέλευσης είτε προορισμού μιας συναλλαγής, αλλά μπορεί να διαφοροποιηθούν στοιχεία της συναλλαγής, γεγονός που θα έχει αντίκτυπο στο αναγνωριστικό συναλλαγής, αφού θα διαφέρει από το πραγματικό (Decker & Wattenhofer, 2014).

Ο παραπάνω κίνδυνος επιβεβαιώθηκε το 2014 στο ανταλλακτήριο bitcoin Mt. Gox, εταιρία με έδρα στο Τόκιο, όπου η τροποποίηση των αναγνωριστικών συναλλαγής καθώς και η ανικανότητα της εταιρίας για την επαλήθευση του έδινε την δυνατότητα υποκλοπής κεφαλαίων σε επιτιθέμενους. Μια διεύθυνση κλειδιών προέρχεται από ένα ζεύγος κλειδιών ασύμμετρης κρυπτογράφησης. Θεωρώντας λοιπόν ένα χρήστη με ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού (prK,pk) και έστω x η διεύθυνση του παραλήπτη που δημιουργείται από τον κατακερματισμό του δημοσίου κλειδιού. Έστω τώρα y ο κατακερματισμός της συναλλαγής tr, η οποία στέλνει χρήματα στην διεύθυνση x. Η συναλλαγή tr που μεταφέρει επιπλέον χρήματα σε κάποια άλλη διεύθυνση έστω tr΄ είναι η ψηφιακή υπογραφή Sig είναι η κρυπτογράφηση του κατακερματισμού της συναλλαγής tr με χρήση prK (Nguyen & Zhou, 2017). Πιο συγκεκριμένα, με εφαρμογή του αλγορίθμου ψηφιακής υπογραφής ελλειπτικής καμπύλης το λεγόμενο ECDSA αλγόριθμο(Elliptic Curve Digital Signature Algorithm) δημιουργείται ένα ζευγάρι κλειδιών που αποτελείται από:

- Ιδιωτικό κλειδί (ακέραιος)
- Δημόσιο κλειδί (σημείο ελλειπτικής καμπύλης): **Δημόσιο κλειδί = ιδιωτικό κλειδί * G**, όπου G = γεννήτορας σημείο το οποίο χρησιμοποιείται ως πολλαπλασιαστής για την εύρεση του δημόσιου κλειδιού το οποίο θα είναι ένα σημείο της ελλειπτικής καμπύλης. Επιπλέον, η τάξη n της υποομάδας των σημείων της ελλειπτικής καμπύλης η οποία είναι και κυκλική (αφού n πρώτος αριθμός) ορίζει το μήκος των ιδιωτικών κλειδιών (π.χ 256 bit). Πιο συγκεκριμένα, το ιδιωτικό κλειδί μπορεί να είναι οποιοδήποτε αριθμός μεταξύ 1 έως n-1, όπου n είναι μια σταθερά (n=1,158 * $10^{77} \sim 2^{256}$) που ορίζει την τάξη της ελλειπτικής καμπύλης. Συνεπώς για την δημιουργία ενός τέτοιου κλειδιού επιλέγεται ένας αριθμός 256 bit ο οποίος πρέπει να είναι οπωσδήποτε μικρότερος από n-1.

Αναλυτικότερα, ένα αναγνωριστικό συναλλαγής είναι ένα μοναδικό αλφαριθμητικό δεδομένων 32 byte, το οποίο προκύπτει μέσω του κατακερματισμού των δεδομένων συναλλαγής εφαρμόζοντας την συνάρτηση κατακερματισμού 2 φορές, για τα δεδομένα της συναλλαγής(κατακερματισμός συναλλαγής, δείκτης εξόδου, σενάριο ξεκλειδώματος, μέγεθος σεναρίου ξεκλειδώματος) τα οποία περιγράφονται παρακάτω:

Tx id = SHA-256(SHA-256(Δεδομένα συναλλαγής))

- Κατακερματισμός συναλλαγής : Αναφορά στην συναλλαγή που περιέχει το UTXO που δαπανάται
- Δείκτης εξόδου: Ο ακριβής αριθμός του ποσού UTXO που δαπανάται.
- Σενάριο ξεκλειδώματος: Σενάριο που ικανοποιεί τις συνθήκες του σεναρίου ξεκλειδώματος. Ως προς την έννοια σενάριο, αναφερόμαστε στην διαδικασία έγκρισης συναλλαγών, η οποία στηρίζεται σε 2 τύπους σεναρίων, αυτών του κλειδώματος και ξεκλειδώματος. Ένα σενάριο κλειδώματος είναι ένα «εμπόδιο» που τοποθετείται σε μια έξοδο και ορίζει τις συνθήκες που πρέπει να ικανοποιηθούν για το ξόδεμα αυτής της εξόδου. Ένα σενάριο κλειδώματος ή αλλιώς scriptPubKey (script το οποίο απαιτεί ένα δημόσιο κλειδί και μια ψηφιακή υπογραφή) εμπεριέχει ένα δημόσιο κλειδί. Με άλλα λόγια, περιέχει την διεύθυνση προορισμού που πρόκειται να σταλούν bitcoin, ενώ στο πλαίσιο του script

καθορίζονται οι προϋποθέσεις που οφείλει να πληροί ο παραλήπτης προκειμένου να γίνει εξαργύρωση της συναλλαγής. Έτσι, μόλις λάβουν την συναλλαγή οι ανθρακωρύχοι θα εκτελέσουν αυτό το σενάριο για να επαληθεύσουν την συναλλαγή. Παράλληλα, ένα σενάριο ξεκλειδώματος (scriptSig) είναι αυτό που ικανοποιεί τις συνθήκες που έχουν τοποθετηθεί σε μια έξοδο από ένα σενάριο κλειδώματος επιτρέποντας έτσι στην έξοδο να ξοδευτεί. Ειδικότερα, το scriptSig περιέχει υπογεγραμμένες πληροφορίες μαζί με το δημόσιο κλειδί, έτσι ώστε οι ανθρακωρύχοι να μπορούν να επαληθεύσουν την υπογραφή στο σενάριο. Τα σενάρια ξεκλειδώματος είναι μέρος κάθε εισόδου συναλλαγής (Rajput, Abbas, & Oh, 2018). Ο παρακάτω πίνακας περιγράφει την ακριβής δομή μιας συναλλαγής. Να σημειωθεί ότι, η είσοδος αφορά τα bitcoin που πρόκειται να μεταφερθούν, ενώ η έξοδος αφορά την διεύθυνση που πιστώνεται την μεταφορά τους.

Πίνακας 4:Ακριβής δομή συναλλαγής μπλοκ

	V: έκδοση	**4 bytes**
Είσοδοι	ic: Μετρητής εισόδου	1 byte
	Txid: το προηγούμενο tr id (κατακερματισμός)	Μεταβλητό μήκος
	pc: προηγούμενη έξοδος	4 bytes
	sigLen: μήκος σεναρίου υπογραφής	1 byte
	s: ακολουθία	4 bytes
Έξοδοι	oc: μετρητής εξόδου	1 byte
	ποσό συναλλαγής: αξία	8 bytes
	len: μήκος σεναρίου	1 byte
	addr: σενάριο δημοσίου κλειδιού	Μεταβλητό μήκος
	bt: χρόνος κλειδώματος μπλοκ	4 bytes

Η έννοια λοιπόν του scriptSig εκφράζεται αναλυτικά από την παρακάτω ισότητα: **scriptSig = Len (Sig_data) + Sig_data + Len (pub key) + pub key**, όπου Len ορίζει το μήκος σε bytes των υπογεγραμμένων πληροφοριών, ενώ ως Sig_data εκφράζεται η υπογραφή για το ECDSA ζευγάρι κλειδιών (δημόσιο κλειδί, ιδιωτικό κλειδί). Με αυτό τον αλγόριθμο (ESDSA) εξασφαλίζεται με απλά λόγια ότι τα ποσά σε bitcoin είναι δυνατό να ξοδευτούν μόνο από τους «ιδιοκτήτες» τους.

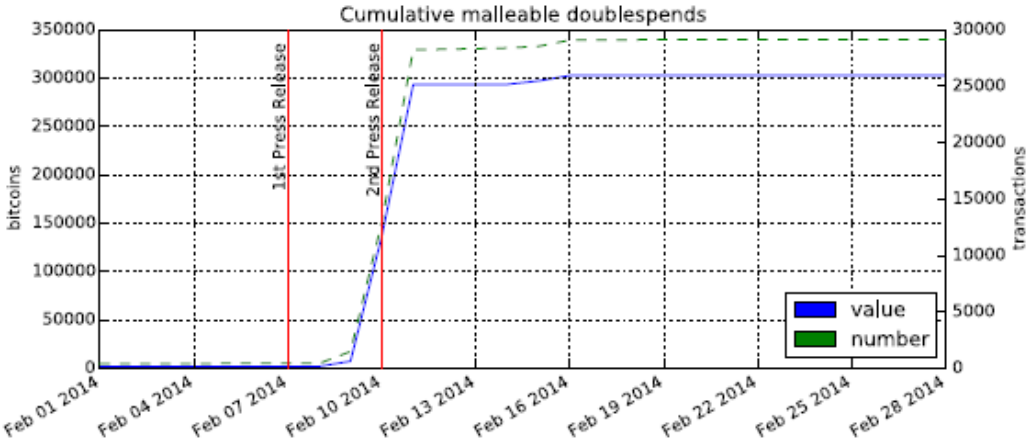
- Μέγεθος (σε bytes) σεναρίου ξεκλειδώματος
- Αριθμός ακολουθίας

Η επίτευξη μιας τέτοιας κατάστασης είναι δυνατή επειδή το σενάριο ξεκλειδώματος ή scriptSig που περιέχει την ψηφιακή υπογραφή μπορεί να τροποποιηθεί από τον επιτιθέμενο. Σε μια τέτοια περίπτωση, τα σειριακά δεδομένα συναλλαγής θα τροποποιηθούν και κατ' επέκταση η ίδια η αλυσίδα. Η ψηφιακή υπογραφή του σεναρίου ξεκλειδώματος όμως μπορεί να αλλάξει και έχει νόημα για τον επιτιθέμενο πριν από την επιβεβαίωση ενός μπλοκ, αφού μετά η ψηφιακή υπογραφή και το αναγνωριστικό συναλλαγής είναι αμετάβλητα.

Για την καλύτερη κατανόηση, θέτουμε το παρακάτω παράδειγμα. Έστω ότι η Αλίκη στέλνει 1 bitcoin στον Μπομπ, έχοντας ως Tx id = a. Όμως πριν επιβεβαιωθεί η συναλλαγή ο Μπομπ μεταβάλλει τα δεδομένα υπογραφής της συναλλαγής με σκοπό την αλλαγή του Tx id, έστω Tx id=b. Με αυτό τον τρόπο, ο Μπομπ έχοντας πάρει το 1 bitcoin που του έστειλε η Αλίκη με το διαφορετικό όμως Tx id, ειδοποιεί την Αλίκη ότι δεν του έχει σταλθεί το ποσό. Έτσι όταν η Αλίκη αναζητά σε μια εφαρμογή εξερευνητή μπλοκ την συναλλαγή κάνοντας χρήση όμως το Tx id= a, ώστε να επαληθεύσει τον ισχυρισμό του Bob, δεν εντοπίζει την συναλλαγή. Για τον λόγο αυτό θεωρεί την συναλλαγή αποτυχημένη και ότι το ποσό σε bitcoin δεν στάλθηκε ποτέ. Συνεπώς, η Αλίκη ξαναστέλνει το ίδιο ποσό στον Μπομπ, καταφέρνοντας να λάβει τελικά από την Αλίκη το διπλάσιο ποσό.

Όσον αφορά το ιστορικό αυτού προβλήματος σχετίζεται όπως αναφέρθηκε με το ανταλλακτήριο MtGox τον Φεβρουάριο του 2014, όπου τελικά ακολούθησε η κατάθεση πτώχευσης του τον ίδιο μήνα. Παρατηρώντας το χρονοδιάγραμμα επιθέσεων από τις ανακοινώσεις που έκανε η MtGox, προσδιορίζονται 3 χρονικές περίοδοι, όπως καταγράφεται και στο σχήμα:

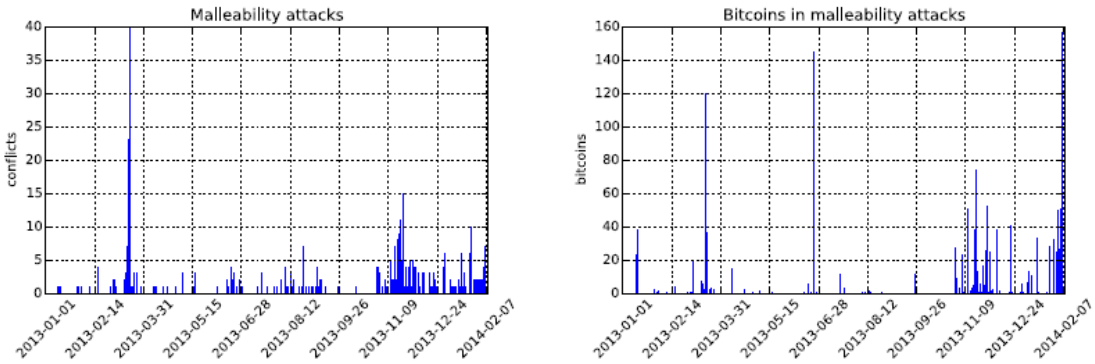
- Φάση 1 (Ιανουάριος 2013 – 7 Φεβρουαρίου 2014): Περίοδος μέχρι το κλείσιμο των αναλήψεων του Mt.Gox.
- Φάση 2 (8 Φεβρουάριου – 9 Φεβρουάριου 2014): Είναι η περίοδος που το ανταλλακτήριο σταματά να λειτουργεί με την διακοπή αναλήψεων, χωρίς όμως να γίνεται ευρέως γνωστό το ακριβές πρόβλημα.
- Φάση 3 (10 Φεβρουαρίου – 28 Φεβρουαρίου 2014): Αναγνώριση του προβλήματος με την ονομασία "transaction malleability", ακολουθώντας στην συνέχεια η πτώχευση του ανταλλακτηρίου.



Εικόνα 36:Γράφημα απεικόνισης αριθμού και αξίας επιθέσεων malleability σε 3 φάσεις (περιόδους)[10]

Θα πρέπει ωστόσο να τονιστεί ότι οι επιθέσεις "malleability" στις περιόδους 2 και 3 δεν σχετίζονται με τις απώλειες ποσών από την Mt.Gox αφού συνέβησαν μετά την διακοπή των αναλήψεων (Kutyłowski & Vaidya, 2014). Στο παρακάτω σχήμα απεικονίζονται τα ποσά των bitcoin που σχετίζονται με την συγκεκριμένη επίθεση, αλλά και η συχνότητα των επιθέσεων κατά την φάση 1. Με βάση λοιπόν τα 2 αυτά σχήματα συμπεραίνεται ότι το σύνολο των επιθέσεων malleability δεν επηρεάζει σε απόλυτο βαθμό την απώλεια σε bitcoin που συνέβησαν λόγω του Mt.Gox ανταλλακτηρίου.

[10] Ανακτήθηκε από: http://link.springer.com/10.1007/978-3-319-11212-1



Εικόνα 37:Συσχέτιση επιθέσεων malleability και απωλειών σε bitcoin κατά την πρώτη φάση[11]

Καταλήγοντας, η επίθεση malleability μπορεί να θεωρηθεί και ως μια παραλλαγή της επίθεσης διπλής δαπάνης (double spending), σημειώνοντάς όμως ότι στην πρώτη περίπτωση ο επιτιθέμενος δεν πραγματοποιεί εκείνος την συναλλαγή, αλλά αντί αυτού ο επιτιθέμενος κάνει το θύμα να δημιουργήσει μια συναλλαγή η οποία θα μεταφέρει κάποιο ποσό σε διεύθυνση η οποία θα ελέγχεται από τον ίδιο (Decker & Wattenhofer, 2014). Έτσι όταν η συναλλαγή σταλεί στην διεύθυνση του εισβολέα στην συνέχεια υπόκειται σε αλλαγές, ενώ παράλληλα προκύπτει και αλλαγή στην υπογραφή της. Συνεπώς αφού αλλάζουν τα δεδομένα αλλάζει και ο κατακερματισμός αυτών. Αυτό έχει ως ακόλουθο την μετάδοση της συναλλαγής στο δίκτυο μαζί με την μη τροποποιημένη (αρχική), γεγονός που γεννά το ενδεχόμενο επιβεβαίωσης της από τους κόμβους του δικτύου.

3.1.2 Double spending attacks

Η επίθεση double spending αποτελεί μια επίθεση η οποία συμβαίνει κατά την δημιουργία μιας συναλλαγής στο bitcoin, όπου ο επιτιθέμενος με την χρήση συγκεκριμένων bitcoin δημιουργεί επιτυχώς περισσότερες από μια συναλλαγές. Με άλλα λόγια, η επίθεση αυτή επιτυγχάνεται με την χρησιμοποίηση των ίδιων bitcoin και

[11] Ανακτήθηκε από: http://link.springer.com/10.1007/978-3-319-11212-1

γενικότερα κρυπτονομισμάτων για μια συναλλαγή. Πιο συγκεκριμένα, αν μια συναλλαγή έχει να κάνει με την μεταφορά νομισμάτων από ένα χρήστη σε κάποιον άλλο και από κάποια δηλαδή διεύθυνση σε κάποια άλλη γίνεται μια μεταφορά της ιδιοκτησίας των "assets" του χρήστη από μία διεύθυνση του αποστολέα στην δημόσια διεύθυνση του παραλήπτη η οποία αντιστοιχίζεται με το δημόσιο κλειδί του, ενώ η αξία της συναλλαγής θα πρέπει να υπογραφεί από τον αποστολέα με την χρήση του ιδιωτικού του κλειδιού (Stetsenko, Khalimov, & Kotukh, 2020). Αφού επιτευχθεί αυτή η διαδικασία για την συναλλαγή προβάλλεται σε ολόκληρο το δίκτυο, ενώ ο παραλήπτης επικυρώνει την συναλλαγή. Ειδικότερα, η επικύρωση από τον δέκτη πραγματοποιείται όταν ο αποστολέας «ψάχνει» την λεγόμενη αξόδευτη συναλλαγή "UTXO" (unspent transaction output) του αποστολέα, επικυρώνοντας έτσι την ψηφιακή υπογραφή του αποστολέα, μέσω του ιδιωτικού του κλειδιού, περιμένοντας στην συνέχεια μέσω της διαδικασίας της εξόρυξης να ενταχθεί σε μπλοκ, το οποίο θα αποτελεί μέρος της αλυσίδας. Η διαδικασία αυτή της ένταξης ενός νέου μπλοκ στην αλυσίδα διαρκεί κάποια λεπτά και στην περίπτωση του bitcoin είναι 10 λεπτά.

Σε ένα περιβάλλον που λαμβάνουν χώρα ταχείες συναλλαγές υπάρχει πιθανότητα το οποιοδήποτε προϊόν να απελευθερωθεί από τον αποστολέα, πριν η συναλλαγή εξ ορυχθεί στο blockchain. Το γεγονός αυτό δίνει στον αποστολέα την δυνατότητα να υπογράψει την ίδια συναλλαγή και να την αποστείλει σε διαφορετικό παραλήπτη. Έχουμε δηλαδή την υπογραφή της ιδίας συναλλαγής με ένα ιδιωτικό κλειδί και την αποστολή της σε διαφορετικούς παραλήπτες. Ωστόσο, για δύο συναλλαγές προερχόμενες από τα ίδια "UTXO" μόνο μία από αυτές ενσωματώνεται στο blockchain. Στο σημείο αυτό να τονιστεί ότι μια καθυστέρηση στην εφαρμογή του μοντέλου συναίνεσης στο δίκτυο ή μια επίθεση 51% μπορεί να προκαλέσει επιπλέον καθυστερήσεις στην διαδικασία επικύρωσης ενός μπλοκ το οποίο με την σειρά του αυξάνει τις πιθανότητες πραγματοποίησης μιας "double spending" επίθεσης. Για να επιτευχθεί μια τέτοια επίθεση οι επιτιθέμενοι πρέπει να έχουν υψηλή ισχύς κατακερματισμού, ώστε να μπορούν να δημιουργήσουν μια μεγαλύτερη αλυσίδα ενώ σημειώνεται ότι συσχετιζόμενες επιθέσεις είναι οι race, Finney, 51% και Vector 76. Επιπλέον μια προσέγγιση μέσω βημάτων μπορεί να αποτυπωθεί ως εξής:

> **Βήμα 1**: Έστω ότι ο επιτιθέμενος ξεκινάει από το block N, προσπαθώντας να κάνει εξόρυξη ενός νέου μπλοκ, χωρίς ωστόσο να δημοσιευθεί. Η δημοσίευση ενός μπλοκ σημαίνει ότι έχει προηγουμένως έχει επικυρωθεί, δηλαδή η συναλλαγή έχει ενταχθεί στο "mempool" (transaction queue), όπου βρίσκεται υπό διαδικασία

ένταξης της σε μπλοκ. Στην προκειμένη περίπτωση η συναλλαγή δεν δημοσιεύεται και συνεπώς δεν εντάσσεται σε κάποιο μπλοκ. Ο επιτιθέμενος χρήστης λοιπόν κάνει αίτηση για συναλλαγή μέσω του πορτοφολιού του. Η μη επιβεβαιωμένη αυτή συναλλαγή συμμετέχει σε κάποιο "mining pool" προκειμένου να είναι μια από τις συναλλαγές που θα επιλέξει ο ανθρακωρύχος κατά την επίλυση του μοντέλου συναίνεσης, ώστε να ανήκει τελικά στο νέο μπλοκ.

Βήμα 2: Γίνεται προβολή (αναμετάδοση) της συναλλαγής στους υπόλοιπους κόμβους που συμμετέχουν στο δίκτυο.

Βήμα 3: Όσο οι ηθικοί ανθρακωρύχοι επαληθεύουν ένα νέο μπλοκ, το μπλοκ προστίθεται στο πραγματικό blockchain. Ο επιτιθέμενος περιμένει ώστε να υπάρχουν αρκετές επιβεβαιώσεις της συναλλαγής (συνήθως 6 επιβεβαιώσεις αρκούν για να θεωρηθεί μια συναλλαγή έγκυρη), ώστε να επαληθευθεί η συναλλαγή και να καταγραφεί στην αλυσίδα των μπλοκ (Begum et al., 2020). Εκείνη την στιγμή ο «μολυσμένος» ανθρακωρύχος ξεκινά την δική του αλυσίδα με το επαληθευμένο μπλοκ, ενώ ο επιτιθέμενος ανθρακωρύχος στέλνει δεδομένα συναλλαγών (ξοδεύει το νόμισμα του) στην αρχική αλυσίδα (πραγματικό blockchain) και όχι στην δική του ιδιωτική αλυσίδα.

Βήμα 4: Ακολουθεί μυστική εξόρυξη για επέκταση της ιδιωτικής διακλάδωσης στην αλυσίδα. Σε αυτό το στάδιο, ο κακόβουλος ανθρακωρύχος επιλέγει συναλλαγές και προσθέτει μπλοκ στην ιδιωτική του αλυσίδα, οι οποίες επικυρώνονται από τον ίδιο με γρηγορότερο ρυθμό από τι προσθέτουν μπλοκ οι ειλικρινείς ανθρακωρύχοι στο πραγματικό blockchain, ώστε τελικά το ιδιωτικό blockchain να αποτελείται από περισσότερα μπλοκ. Εφόσον επιτευχθεί αυτό, γίνεται δημοσίευση της διακλάδωσης που έχει δημιουργηθεί η οποία τελικά θεωρείται ως έγκυρη, αναιρώντας την αρχική και πραγματική αλυσίδα.

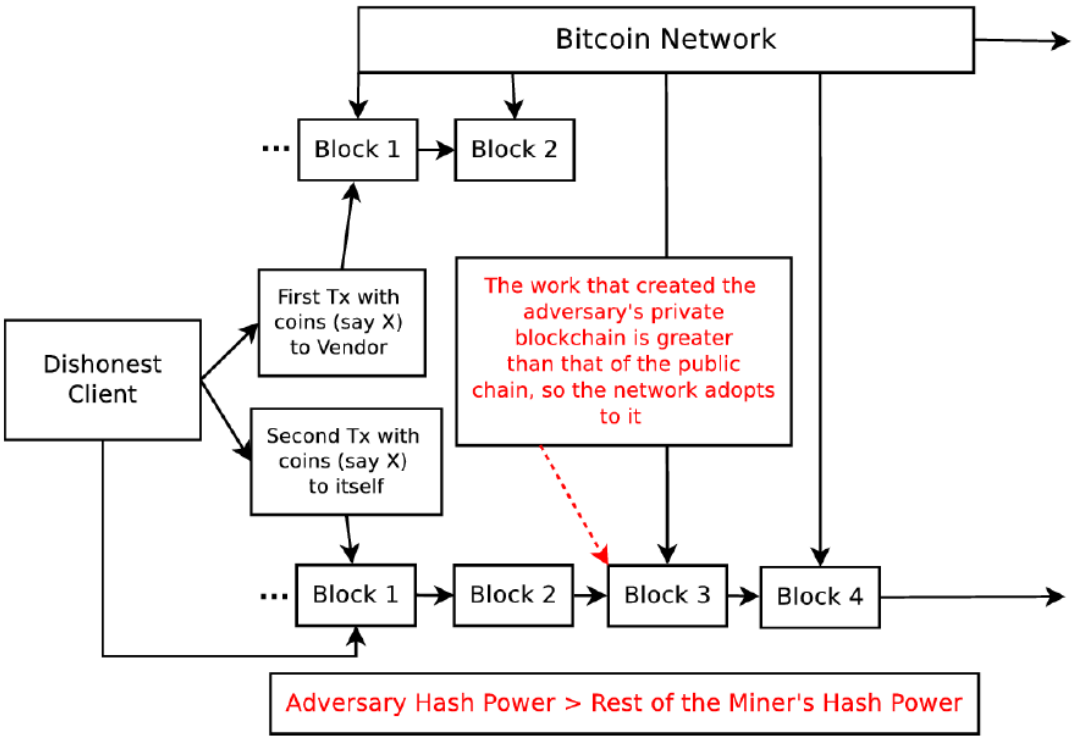
Όσον αφορά τις πιθανότητες επίτευξης της επίθεσης , θεωρούμε ότι η πιθανότητα (a_z) επιτυχίας μια "double spend" εκφράζεται παρακάτω ως εξής:

$$a_z = \min\left(\frac{q}{p}, 1\right)^{max(z+1,0)} = \begin{cases} 1, \ \alpha\nu \ z < 0, q > p \\ (q/p)^{z+1}, \alpha\nu \ z \geq 0, q \ \leq p \end{cases}$$

όπου a_z = double spending επίθεση

p = hash rate των ηθικών κόμβων

z = Αριθμός των μπλοκ



Εικόνα 38:Επίθεση double spending [12]

Βήμα 5: Σύμφωνα με τον κανόνα της υπερίσχυσης της μεγαλύτερης αλυσίδας τα μπλοκ τελικά θα προστεθούν σε αυτή διαγράφοντας ουσιαστικά τα αρχεία στο πραγματικό blockchain. Έτσι το block του πραγματικού blockchain είχε τα δεδομένα συναλλαγής που ξόδεψε ο κακόβουλος ανθρακωρύχος, χωρίς να να τα έχει (γνωρίζει) η ιδιωτική αλυσίδα. Όταν όμως τα μπλοκ προστεθούν στην ιδιωτική αλυσίδα του επιτιθέμενου, αφαιρούνται όλες οι προηγούμενες πληροφορίες συναλλαγών.

Συμπερασματικά, για να επιτευχθεί με κάποιο τυχαίο ποσοστό κατακερματισμού παρατηρείται ότι η πιθανότητα επιτυχίας μειώνεται εκθετικά, όσο ο αριθμός των επιβεβαιώσεων μιας συναλλαγής αυξάνεται (Tareq, n.d.). Τέλος, πρέπει να σημειωθεί ότι η ισχύς κατακερματισμού του επιτιθέμενου καθώς και ο αριθμός των μπλοκ καθορίζουν την επιτυχία μιας τέτοιας επίθεσης. Αυτό που συμβαίνει στην πραγματικότητα, είναι ότι ο επιτιθέμενος ανθρακωρύχος συμμετέχει στην πραγματική αλυσίδα πραγματοποιώντας

[12] Ανακτήθηκε από: https://ieeexplore.ieee.org/document/8369416

συναλλαγές, ενώ οι κόμβοι θύματα που στοχεύουν στην διαδικασία της εξόρυξης στην νέα όμως διακλάδωση δεν είναι ενήμεροι για τις συναλλαγές του. Συνεπώς δίνεται έτσι η δυνατότητα στον επιτιθέμενο να πραγματοποιήσει τις ίδιες συναλλαγές (άρα δύο φορές) που έκανε στην αρχική αλυσίδα και στην νέα διακλάδωση της.

3.1.2.1 51% attack (Majority attack)

Η 51% επίθεση χρησιμοποιήθηκε αρχικά για επιθέσεις σε bitcoin, αλλά εφαρμόζεται και σε άλλα blockchain συστήματα. Το πρόβλημα έγκειται όταν κακόβουλοι κόμβοι και συγκεκριμένα "mining pools" κατέχουν περισσότερο από το 51% της εξορυκτικής ισχύς στο δίκτυο. Σε αυτό το είδος επίθεσης θα πρέπει οι επιτιθέμενοι κόμβοι να είναι σε θέση αρχικά να εμποδίσουν την διαδικασία εγκυρότητας των συναλλαγών και κατ' επέκταση των block. Επιπλέον να επιτευχθεί η αντιστροφή συναλλαγών κατά την διάρκεια ελέγχου ώστε να είναι εφικτό το φαινόμενο της διπλής δαπάνης, καθώς και να εμποδίσουν από άλλους εξ ορυκτές στο δίκτυο, «παγώνοντας» την διαδικασία δημιουργίας νέων μπλοκ για κάποιο συγκεκριμένο χρονικό διάστημα. Έτσι με την εφαρμογή των παραπάνω ενεργειών επιτυγχάνεται η κατοχή της πλειοψηφίας της ισχύς κατακερματισμού από τους κακόβουλους κόμβους και εν συνεχεία θα είναι σε θέση να είναι αυτοί που θα προσαρτήσουν το νέο μπλοκ στην αλυσίδα (Saad, Spaulding, Njilla, Kamhoua, et al., 2019). Καταλήγοντας, ευπάθειες που μπορεί να προκαλέσει μια 51% επίθεση είναι αποκλεισμός ή τροποποίηση συναλλαγών, τερματισμός της διαδικασίας επαλήθευσης, παράνομες λειτουργείες των εξ ορυκτών, αντιστροφή μια συναλλαγής κ.α.

Για την ανάπτυξη μιας αμοιβαίας εμπιστοσύνης, ένα blockchain σύστημα εφαρμόζει κατανεμημένα μοντέλα συναίνεσης. Με αυτό τον τρόπο, η υπολογιστική ισχύς κατανέμεται σε όλους τους διαθέσιμους εξ ορυκτές και συνήθως από mining pools ή staking pools έτσι ώστε να συγκεντρώνουν μεγαλύτερη υπολογιστική ισχύ και κατά συνέπεια μεγαλύτερες πιθανότητες στην δημιουργία ενός νέου μπλοκ. Ειδικότερα, στα δημόσια blockchain η επίτευξη μιας τέτοιας επίθεσης αφορά την συγκέντρωση περισσότερο του 50% της ισχύς που κατανέμεται στο δίκτυο. Ειδικότερα, στο proof of work η κατοχή του 51% της συνολικής ισχύς του δικτύου αφορά την δύναμη κατακερματισμού η οποία προέρχεται κατά βάση από ASICS, GPUs και CPUs , ενώ στον αλγόριθμο proof of stake κάποιος stakeholder ή καλύτερα επικυρωτής θα πρέπει να

κατέχει την πλειοψηφία των «νομισμάτων» που υπάρχει συνολικά στο δίκτυο, τα οποία για να αποκτηθούν χρειάζεται να αγοραστούν ή να αποκτηθούν μέσω ανταμοιβών που λαμβάνουν οι επικυρωτές ενός νέου μπλοκ.

3.1.2.2 Finney attack

Μία παραλλαγή της “double spending” αποτελεί η επίθεση “Finney”. Σε αυτήν έχουμε έναν απατηλό κόμβο ο οποίος προσπαθεί να εξορύξει ένα νέο μπλοκ υπό μυστικότητα στο οποίο θα εμπεριέχεται μια συναλλαγή έστω σ2, ενώ στην ίδια περίπου χρονική στιγμή προσπαθεί να δημιουργήσει μια συναλλαγή σ1 χρησιμοποιώντας όμως για αυτό ακριβώς τα ίδια ψηφιακά περιουσιακά στοιχεία (bitcoin ή οτιδήποτε άλλο) (Dasgupta et al., 2019). Το μπλοκ που έχει εξ ορυχτεί από το κακόβουλο κόμβο δεν έχει ενταχθεί στην αλυσίδα και ο κακόβουλος κόμβος κρατάει την συναλλαγή σ1 μέχρι την στιγμή που ο κόμβος τον οποίο έχει ως στόχο ενημερωθεί σχετικά με τις συναλλαγές . Μόλις ενημερωθεί ο στόχος ως προς την συναλλαγή σ1 και αφού γίνει η επιβεβαίωση από τους miners ως προς την εγκυρότητα της συναλλαγής, η σ1 ενσωματώνεται τελικώς στην αλυσίδα. Ωστόσο η ενσωμάτωση γίνεται με την δημιουργία μιας διακλάδωσης επί της αρχικής αλυσίδας, η οποία στοχεύει σε μια ακολουθία από μπλοκ τουλάχιστον ίση με την υπάρχουσα. Τα κρίσιμο σημείο σε μια τέτοια περίπτωση εφόσον δηλαδή το μήκος της διακλαδωμένης αλυσίδας ισοφαρίσει το μήκος της κύριας αλυσίδας είναι η εξόρυξη του ακριβώς επόμενου μπλοκ (Vokerla et al., 2019). Έτσι λοιπόν, αν η επόμενη εξόρυξη γίνει επί της διακλαδωμένης αλυσίδας θα έχει ως συνέπεια να αποτελείται από περισσότερα μπλοκ σε σχέση με την αρχική. Το γεγονός αυτό συνεπάγεται την αγνόηση της βασικής αλυσίδας από τους miners και την διαδικασία της εξόρυξης, αφού όλη η δραστηριότητα πλέον περιορίζεται στη διακλαδωμένη (updated αλυσίδα). Το αποτέλεσμα αυτής της κατάστασης είναι ότι η συναλλαγή σ1 που εμπεριέχεται σε κόμβο του βασικού blockchain μετατρέπεται σε μη έγκυρη, ενώ σε επίπεδο συναλλαγής με bitcoin αυτό που συμβαίνει είναι στον αγοραστή του προϊόντος επιστέφεται το ποσό ενώ ο πωλητής δεν λαμβάνει πίσω το προϊόν του.

Συμπερασματικά λοιπόν στην “Finney” επίθεση, μια συναλλαγή προ-εισέρχεται σε κάποιο μπλοκ και μια διπλότυπη έκδοση αυτής της συναλλαγής αποστέλλεται σε κάποιο άλλο κόμβο του δικτύου. Αφού γίνει επικύρωση και αποδοχή της συναλλαγής

γίνεται η μεταφορά του προϊόντος στον παραλήπτη. Με αυτό τον τρόπο εισέρχεται το «μολυσμένο» μπλοκ από τον επιτιθέμενο στην αλυσίδα, όπου εμπεριέχει την παραπάνω συναλλαγή.

3.1.2.3 Vector 76 attack

Εκ σχεδιασμού το bitcoin στοχεύει στην ελαχιστοποίηση του προβλήματος των διπλών δαπανών. Ωστόσο όμως λόγω της αποκεντρωμένης φύσης του bitcoin θα υπάρχει πάντα κάποιο στοιχείο αποτυχίας που μπορεί να χρησιμοποιηθεί για να διπλασιαστεί η δαπάνη. Την αδυναμία αυτή της αρχιτεκτονικής του bitcoin προσπαθεί να εκμεταλλευτεί η επίθεση "Vector 76" ή αλλιώς επιβεβαίωσης. Η επίθεση αυτή αποτελεί υποσύνολο της "double spend" και επιτρέπει στον επιτιθέμενο να συμπεριλάβει μια διπλής δαπάνης συναλλαγή σε ένα μπλοκ. Η επίθεση αυτή μπορεί να πραγματοποιηθεί όταν έχει τον έλεγχο ένας κακόβουλος ανθρακωρύχος, ο οποίος έχει τον έλεγχο σε ένα δίκτυο δύο πλήρων κόμβων και συνδέει ένα από αυτά έστω τον κόμβο Α στην διαδικασία μιας συναλλαγής. Στην συνέχεια, ο δεύτερος πλήρης κόμβος διασυνδέεται με άλλους κόμβους του δικτύου blockchain. Για να επιλέξει σε ποιους κόμβους θα συνδεθεί ο ανθρακωρύχος θα πρέπει να παρακολουθεί την στιγμή κατά την οποία οι κόμβοι μεταδίδουν τις συναλλαγές και πως τις διαδίδουν στην συνέχεια στους άλλους κόμβους του δικτύου. Έτσι, θα μπορεί να γνωρίζει ποιοι κόμβοι είναι πρώτοι που μεταδίδουν τις λειτουργίες και θα είναι σε θέση να συνδεθεί με την αντικειμενική υπηρεσία και με τους σωστά τοποθετημένους κόμβους.

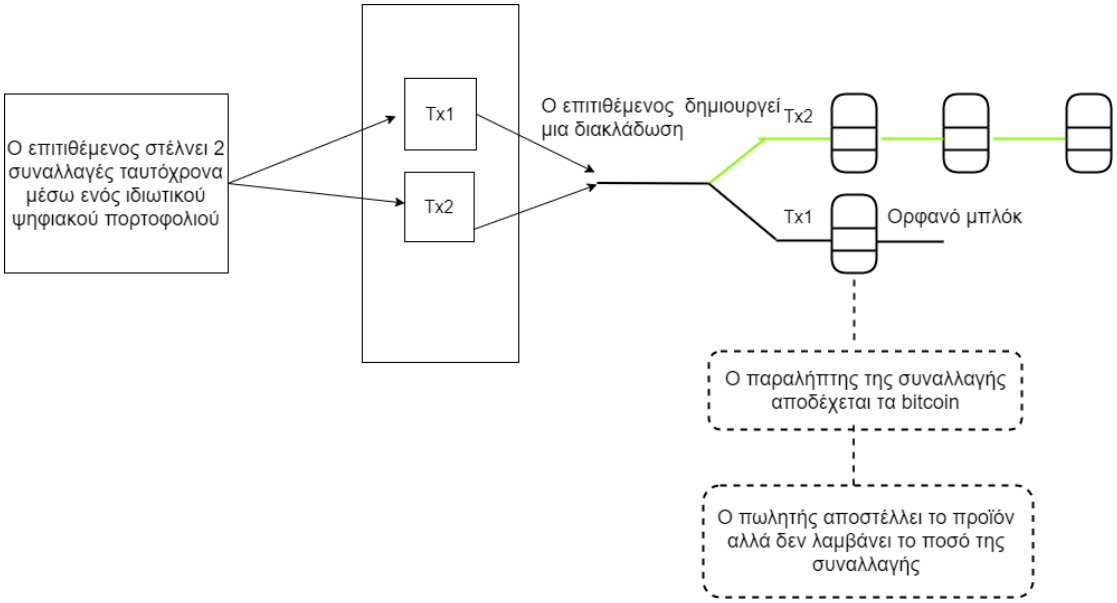
Η επίθεση αυτή παρατηρήθηκε για πρώτη φορά στο "bitcoin talk" forum, όπου ένας χρήστης που έφερε το όνομα Vector76 περιέγραψε μια επίθεση ενάντια στο ηλεκτρονικό πορτοφόλι του, η οποία είχε ως αποτέλεσμα προβλήματα διπλής δαπάνης. Σε αυτήν την περίπτωση ο επιτιθέμενος δεν χρειάζεται να εξορύξει 2 συνεχόμενα μπλοκ, αφού ένα μπλοκ είναι αρκετό (one-confirmation attack) για την εκτέλεση αυτής της επίθεσης (Alkhalifah et al., 2019). Ο εισβολέας χρειάζεται να παρατηρεί την κινητικότητα στο blockchain δίκτυο ώστε να επιλέξει τον σωστό χρόνο διάδοσης των συναλλαγών στους κόμβους του δικτύου. Στη συνέχεια, ο επιτιθέμενος προσδιορίζει αυτούς τους κόμβους που απαιτούν λιγότερο χρόνο μετάδοσης των συναλλαγών σε σχέση με τον κόμβο-στόχο προσπαθώντας να δημιουργήσει μια άμεση σύνδεση με τον στόχο. Στην συνέχεια, ο εισβολέας αποστέλλει μια νόμιμη συναλλαγή στον κόμβο-στόχο και

πραγματοποιεί εξόρυξη ενός νέου μπλοκ χωρίς όμως να διαδίδεται και στους άλλους κόμβους του blockchain δικτύου. Έτσι με αυτό τον τρόπο, ο επιτιθέμενος πραγματοποιεί την διαδικασία εξόρυξης ενός νέου μπλοκ, προσθέτοντας όμως σε αυτό μία επιπλέον συναλλαγή η οποία δεν προβάλλεται στους άλλους κόμβους. Ειδικότερα όταν ο επιτιθέμενος κόμβος δημιουργήσει ένα έγκυρο μπλοκ δεν το προβάλλει στους υπόλοιπους κόμβους έως ότου υπάρξει εξόρυξη ενός νέου μπλοκ από κάποιο άλλο κόμβο. Μόλις συμβεί αυτό ο επιτιθέμενος αμέσως προβάλλει το δικό του μπλοκ (με την έξτρα συναλλαγή) στον κόμβο στόχο. Σε αυτό το σημείο, αν ο στόχος λάβει το μπλοκ του επιτιθέμενου πριν από κάποιο άλλο μπλοκ τότε θα προσθέσει στην αλυσίδα το «κακόβουλο» μπλοκ, με αποτέλεσμα η επιπλέον συναλλαγή του επιτιθέμενου να έχει αποκτήσει μια επιβεβαίωση. Σε μια τέτοια περίπτωση, ο κόμβος-στόχος καθώς και οι άλλοι κόμβοι που θα συνδεθούν με αυτόν, θα δημιουργήσουν μια διακλάδωση επί της αρχικής αλυσίδας. Αυτό συμβαίνει διότι στον κόμβο στόχο έχει περαστεί γρήγορα η συναλλαγή θεωρώντας ότι το μπλοκ του επιτιθέμενου που εμπεριέχει την κακόβουλη συναλλαγή ως νόμιμο (Dasputa et al., 2019). Με αυτό τον τρόπο και οι υπόλοιποί κόμβοι που έχουν συνδεθεί στην νέα αυτή διακλάδωση θεωρούν με την σειρά τους το μπλοκ ως έγκυρο. Στο σημείο αυτό ο επιτιθέμενος στέλνει την συναλλαγή σε μια διαφορετική διεύθυνση που ελέγχεται από τον ίδιο και στην συνέχεια ο κόμβος στόχος συμπεριλαμβάνει την συναλλαγή αυτή στο αντίγραφο της αλυσίδας, διότι έχει θεωρήσει ότι πρόκειται για μια νόμιμη συναλλαγή. Ο επιτιθέμενος επίσης ξοδεύει 2 φορές τις εισόδους των συναλλαγών μεταφέροντας έτσι τα «νομίσματα» στον εαυτό του. Οι κόμβοι του δικτύου οι οποίοι δεν λαμβάνουν το αρχικό μπλοκ του επιτιθέμενου θα αποδεχθούν την συναλλαγή ως νόμιμη και θα την συμπεριλάβουν στο επόμενο μπλοκ. Θα πρέπει να τονιστεί ότι αν το πρώτο μπλοκ του επιτιθέμενου επικρατήσει και δημιουργηθεί η διακλάδωση η επίθεση θα έχει επιτευχθεί.

3.1.2.4 Race Attack

Η επίθεση αυτή αφορά μόνο τα δημόσια blockchain και ιδιαίτερα αυτά που εφαρμόζουν τον αλγόριθμο proof of work στην διαδικασία του mining. Συγκεκριμένα ο εισβολέας προσπαθεί να εκμεταλλευτεί τον χρόνο που μεσολαβεί μεταξύ της δημιουργίας της συναλλαγής και της επιβεβαίωσης της συναλλαγής. Σκοπός και σε αυτή την περίπτωση είναι η δημιουργία διπλοσυναλλαγής. Γενικά, μια “race attack” επιτυγχάνεται

όταν έχουμε 2 αντικρουόμενες συναλλαγές μια αυθεντική και μία ψεύτικη. Η πρώτη συναλλαγή αποστέλλεται στο θύμα, το οποίο δέχεται την πληρωμή (για παράδειγμα για την αποστολή ενός προϊόντος), χωρίς να περιμένει επιβεβαίωση συναλλαγής (Dasgupta et al., 2019). Ταυτόχρονα, η «παράνομη» συναλλαγή, η οποία επιστρέφει το ίδιο ποσό κρυπτονομισμάτων στον εισβολέα μεταδίδεται στο δίκτυο, καθιστώντας τελικά την πρώτη συναλλαγή άκυρη. Ο στόχος δηλαδή, είναι κάποιος κόμβος που αποδέχεται συναλλαγές οι οποίες θα είναι ορατές στο δίκτυο, αλλά δεν έχουν συμπεριληφθεί σε κάποιο μπλοκ. Ο επιτιθέμενος δηλαδή αφού αποτελεί αρχικά κόμβο του "peer to peer" δικτύου στέλνει την ψεύτικη συναλλαγή στο στόχο, ενώ παράλληλα την αυθεντική συναλλαγή στο "miming pool". Σε αυτό το σημείο, η επίθεση επιτυγχάνεται αν ο στόχος δεχθεί την κακόβουλη συναλλαγή και βιαστεί ώστε να παρέχει ως αντάλλαγμα υπηρεσίες πριν δει την νόμιμη συναλλαγή. Αυτό είναι και ο λόγος που συνίσταται να υπάρχει κάποιος ελάχιστος αριθμός επιβεβαιώσεων μιας συναλλαγής, πριν κριθεί ως έγκυρη. Σε επίπεδο κρυπτογραφίας, σε ένα παράδειγμα περιγραφής μιας τέτοιας επίθεσης μεταξύ Αλίκης, Μπομπ και Εύας θα ήταν ως εξής. Η Εύα προσφέρει στην Αλίκη ένα bitcoin σε αντάλλαγμα αγαθών, δημιουργώντας έτσι μια συναλλαγή. Όμως δημιουργεί μια ακόμη συναλλαγή ταυτόχρονα στέλνοντας το ίδιο bitcoin στον Μπομπ. Η Αλίκη μπορεί να μειώσει τον κίνδυνο μιας "race attack", ορίζοντας ότι δεν θα παραδώσει τα αγαθά πριν η πληρωμή της Eve's στην Αλίκη εμφανιστεί στο blockchain.



Εικόνα 39:Απεικόνιση Race attack

3.1.2.5 Alternative History attack

Η συγκεκριμένη επίθεση σημαίνει ότι το ιστορικό καταγραφής στο blockchain μπορεί να παραβιαστεί από κακόβουλους ανθρακωρύχους. Ειδικότερα σε μια "alternative history" επίθεση, ο εισβολέας πραγματοποιεί εξόρυξη σε μια διαφορετική αλυσίδα (διακλάδωση) η οποία περιλαμβάνει ένας γεγονός διπλής δαπάνης από τον επιτιθέμενο. Στην συνέχεια κατά την γνωστή μέθοδο "longest chain", αν ο εισβολέας καταφέρει να επικρατήσει η διακλάδωση του θα μπορεί να τροποποιήσει ένα επιβεβαιωμένο ιστορικό και έπειτα να χρησιμοποιήσει το ίδιο νόμισμα δύο φορές (διπλή δαπάνη). Η πιο διάσημη περίπτωση αυτής της επίθεσης συνέβη τον Μάιο του 2014 στο blockchain σύστημα Reddcoin, όπου αύξησε τον απαραίτητο αριθμό των επιβεβαιώσεων από 6 σε 60.

Αναλυτικότερα, ο κακόβουλος ανθρακωρύχος υποβάλλει στον έμπορο ή το δίκτυο μια συναλλαγή την οποία πληρώνει ο έμπορος. Παράλληλα, ο ανέντιμος ανθρακωρύχος εξορύσσει ιδιωτικά την εναλλακτική blockchain αλυσίδα στην οποία περιλαμβάνεται μια μολυσμένη συναλλαγή διπλή δαπάνης. Μετά την αναμονή για n επιβεβαιώσεις, ο έμπορος στέλνει το προϊόν στον εισβολέα (Liu, Xu, Cao, Zhang, & Peng, 2021). Έτσι, αν ο εισβολέας βρει περισσότερα από n μπλοκ, «ελευθερώνει» την διακλάδωση του και αρχίζει να ανακτά τα νομίσματα του. Από την άλλη, αν ο εισβολέας δεν καταφέρει να επεκτείνει την διακλάδωση του σε σύγκριση με την αρχική αλυσίδα, τότε η επίθεση θα αποτύχει και οι πόροι του θα σπαταληθούν χάνοντας παράλληλα την ανταμοιβή του για τα εξορυσσόμενα μπλοκ. Στο σημείο αυτό, αξίζει να σημειωθεί ότι η πιθανότητα επιτυχίας μιας τέτοιας επίθεσης ισούται με το κλάσμα $\frac{attacker\ hash\ rate}{network\ hashrate}$, ενώ ο έμπορος περιμένει για τις επιβεβαιώσεις (μπλοκ) που χρειάζεται.

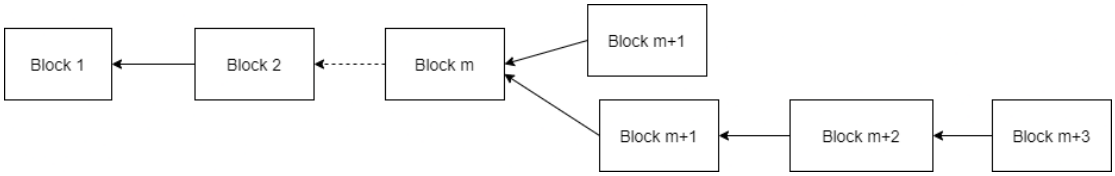
Για την αντιμετώπιση των επιθέσεων αυτών, οι ανθρακωρύχοι οδηγούνται στην μεγαλύτερη τοπικά γνωστή διακλάδωση, αυτή δηλαδή η οποία διαθέτει την περισσότερη υπολογιστική ισχύ . Θα πρέπει να σημειωθεί ότι οι "alternative history" επιθέσεις είναι πιθανό να έχουν θετική έκβαση, απλά και μόνο με την επιτυχή εφαρμογή της μεθόδου "longest chain" από τον επιτιθέμενο (Liu et al., 2021). Καταλήγοντας με μια λογική παρατήρηση, όσο υψηλότερος αριθμός επιβεβαιώσεων μπλοκ υπάρχει τόσο χαμηλότερη θα είναι και η πιθανότητα για την πραγματοποίηση μιας "alternative history" επίθεσης.

3.1.3 Mining attacks

Για μεγάλα κρυπτονομίσματα όπως είναι το Bitcoin, έχει καταστεί αδύνατο για μεμονωμένους ανθρακωρύχους να αποκομίσουν κέρδος. Έτσι οι ανθρακωρύχοι αναγκάζονται να ενώσουν την υπολογιστική του ισχύ δημιουργώντας δεξαμενές εξόρυξης. Αυτό τους επιτρέπει να εξορύξουν περισσότερα μπλοκ και ο καθένας να λάβει ένα μερίδιο της ανταμοιβής.

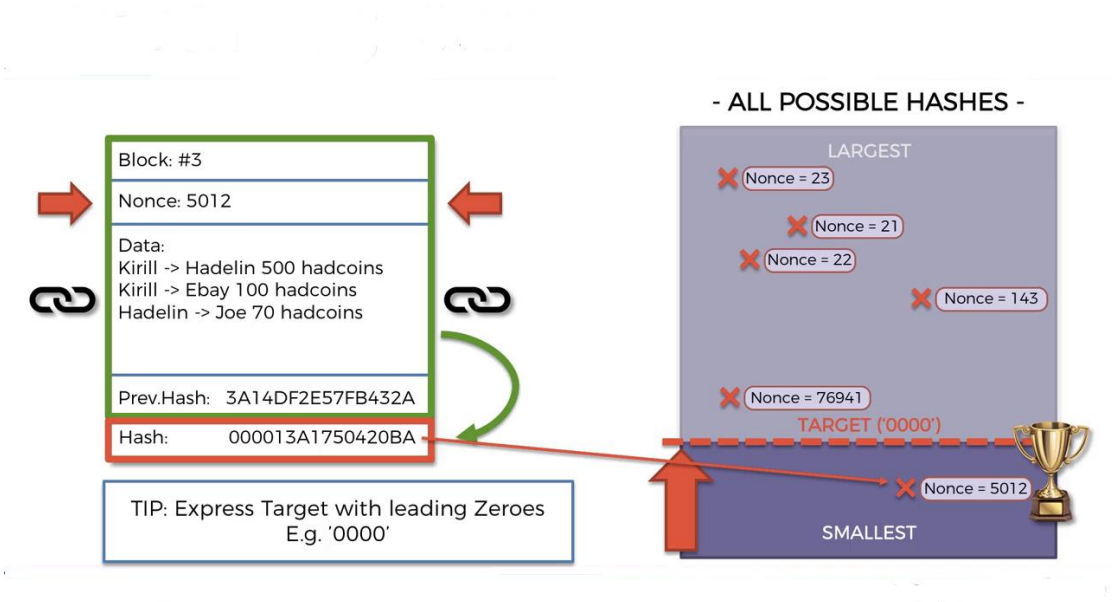
3.1.3.1 Selfish Mining attack

Η Επίθεση selfish mining πραγματοποιείται από ανθρακωρύχους bitcoin οι οποίοι στοχεύουν στην απόκτηση υψηλών ανταμοιβών μέσω της διαδικασίας της εξόρυξης ή μπορεί να στοχεύουν στην σπατάλη της υπολογιστικής ισχύς των έντιμων ανθρακωρύχων. Πιο συγκεκριμένα, ο εισβολέας διατηρεί μπλοκ ιδιωτικά και σε δεύτερη φάση προσπαθεί να δημιουργήσει μια διακλάδωση επί της αλυσίδας που θα εμπεριέχονται αυτά τα μπλοκ. Αναλυτικότερα, προσπαθεί να εξορύξει κάποιο μπλοκ στην διακλάδωση που έχει δημιουργηθεί στοχεύοντας η διακλάδωση να αποτελείται από περισσότερα μπλοκ σε σύγκριση με τον αριθμό των μπλοκ της αρχικής αλυσίδας. Παράλληλα, οι υπόλοιποι νόμιμοι εξ ορυκτές, συνεχίζουν την εξόρυξη στην δημόσια αλυσίδα. Τα νέα μπλοκ που εξ ορύσσονται από τον επιτιθέμενο θα αποκαλυφθούν όταν το ιδιωτικό κακόβουλο blockchain του εισβολέα ισοφαρίζει το δημόσιο νόμιμο blockchain. Στο σημείο αυτό οι «έντιμοι» ανθρακωρύχοι στην προσπάθεια της δημιουργίας νέων μπλοκ θα ξοδεύουν υπολογιστική ισχύ, χωρίς όμως να λαμβάνουν την αντίστοιχη ανταμοιβή όπως ορίζει η διαδικασία. Το γεγονός αυτό έχει ως συνέπεια, ο εισβολέας να αποκτά ουσιαστικό πλεονέκτημα στην διαδικασία εξόρυξης ενός νέου μπλοκ. Με άλλα λόγια, η επίθεση “selfish mining” αποτελεί μια προσπάθεια ορισμένων ανθρακωρύχων να αποκτούν μεγαλύτερες ανταμοιβές στην διαδικασία εξόρυξης νέων μπλοκ επί της ιδιωτικής αλυσίδας (διακλάδωσης) που αναπτύσσουν με απώτερο στόχο την δημιουργία μιας αλυσίδας μεγαλύτερου μήκους σε σχέση με το αντίστοιχο δημόσιο blockchain που αποτελεί την νόμιμη αλυσίδα. Το παρακάτω σχήμα αναπαριστά μια selfish mining attack με την δημιουργία διακλάδωσης η οποία στην συνέχεια αναπτύσσεται αποκτώντας περισσότερο μήκος σε σύγκριση με το δημόσιο blockchain.



Εικόνα 40:Αναπαράσταση "selfish miming"

Έστω ότι έχουμε ένα blockchain που αποτελείται από τα μπλοκ B_1, B_2,…, B_m. Θεωρώντας ένα νόμιμο κόμβο-ανθρακωρύχο ο οποίος πραγματοποιεί την εξόρυξη ενός νέου μπλοκ έστω του B_{m+1} του παραπάνω σχήματος, ενώ παράλληλα επιτυγχάνεται η εξόρυξη του B_{m+1} από ένα «εγωιστή» κόμβο (selfish miner). Στο κρίσιμο αυτό σημείο δεν γίνεται απελευθέρωση του μπλοκ και η σύνδεση του στην αλυσίδα όπως θα έπρεπε αλλά πραγματοποιεί την επιπλέον εξόρυξη των μπλοκ B_{m+2} και B_{m+3}, επεκτείνοντας έτσι την ιδιωτική του αλυσίδα, πριν προλάβει κάποιος άλλος ανθρακωρύχος να προσθέσει ένα μπλοκ στο δημόσιο blockchain (S. S. Shetty, Kamhoua, & Njilla, 2019). Ακόμη, θεωρούμε ότι το μπλοκ B_{m+1} του «ειλικρινή» κόμβου-ανθρακωρύχου έχει διαφορετική τιμή κατακερματισμού (hash value) από την αντίστοιχη τιμή του εγωιστή ανθρακωρύχου, σημειώνοντας όμως ότι και οι 2 τιμές είναι μικρότερες από τον ορισμένο στόχο (difficulty target) όπως ορίζει η διαδικασία της εξόρυξης μπλοκ, με αποτέλεσμα να παραχθεί το μπλοκ B_{m+1} και από τον «ειλικρινή» και από τον «εγωιστή» ανθρακωρύχο.



Εικόνα 41:Λειτουργία difficulty target στην διαδικασία εξόρυξης νέου μπλοκ [13]

[13] Ανακτήθηκε από: Udemy.com

Στην περίπτωση όμως που ο εγωιστής κόμβος πραγματοποιήσει την εξόρυξη των μπλοκ B_{m+2} και B_{m+3}, το δίκτυο του blockchain διατηρεί μόνο την μεγαλύτερη σε μήκος αλυσίδα και συνεπώς θα απορρίψει το μπλοκ B_{m+1} που εξ ορύχθηκε από τον ειλικρινή κόμβο, παρόλο που μπορεί να προηγούνταν χρονικά ως προς την εξόρυξη λόγω ισχυρότερης υπολογιστικής ισχύς. Όπως γίνεται αντιληπτό, ό λόγος για να επιδιώξει ένας κόμβος ανθρακωρύχος να είναι «εγωιστής» αποτελεί το γεγονός ότι μπορεί να αυξήσει τις ανταμοιβές του μέσω της δημιουργίας μια μεγαλύτερης αλυσίδας σε σχέση με ένα ανταγωνιστή «ειλικρινή» ανθρακωρύχο .

Θα πρέπει να τονίσουμε, ότι η πιθανότητα επίτευξης μιας τέτοιας επίθεσης είναι μικρή και ένα από τους λόγους είναι το υψηλό κόστος (Saad, Njilla, Kamhoua, Kwiat, & Mohaisen, 2019). Πιο συγκεκριμένα θεωρώντας την πιθανότητα ενός εγωιστή ανθρακωρύχου P(ε) και μ τον αριθμό των μπλοκ που επιθυμεί να προσθέσει στην ιδιωτική του αλυσίδα, α είναι το κλάσμα (κατακερματισμοί/δευτερόλεπτο) της ισχύς κατακερματισμού του εγωιστή ανθρακωρύχου, ενώ ως γ ορίζεται το υπόλοιπο του κλάσματος της ισχύς κατακερματισμού: α+γ=1. Έτσι λοιπόν η πιθανότητα επιτυχίας του εγωιστή ανθρακωρύχου ορίζεται ως εξής:

$$P(\varepsilon)=\begin{cases} 1, \alpha > \gamma \\ (\frac{\alpha}{\gamma})^{\mu}, \alpha < \gamma \end{cases}$$

Αναλυτικότερα, όσο λιγότερους κατακερματισμούς ανά δευτερόλεπτο έχουμε τόσο μικρότερη θα είναι και η πιθανότητα επιτυχούς επίτευξης της επίθεσης και συνεπώς να μην λάβει ο «νόμιμος» ανθρακωρύχος την ανταμοιβή εξόρυξης που του αναλογεί. Για να επιτευχθεί όμως η επίθεση ενός «εγωιστή» ανθρακωρύχου απαιτείται και σε αυτήν την περίπτωση για έναν ανθρακωρύχο να κατέχει τουλάχιστον το 51% της ισχύς κατακερματισμού του δικτύου και μάλιστα το ποσοστό αυτό θα πρέπει να επιτευχθεί σε προγενέστερο χρόνο από την δημιουργία ενός νέου μπλοκ από κάποιο άλλο κόμβο. Αξίζει όμως να σημειωθεί ότι η απόκτηση του 51% της ισχύς κατακερματισμού είναι μια διαδικασία με πολύ υψηλό κόστος. Συγκεκριμένα στην προσπάθεια αυτή απαιτείται η εφαρμογή μηχανημάτων Asic, αλλά το σημαντικότερο είναι ότι το γεγονός της απόκτησης του παραπάνω ποσοστού ως προς την ισχύ κατακερματισμού του δικτύου μπορεί να

εντοπιστεί από τους υπόλοιπους κόμβους του δικτύου και ως εκ τούτου να απορρίψουν τα προηγούμενα δημοσιευμένα μπλοκ του εγωιστή ανθρακωρύχου. Έτσι λοιπόν γίνεται αντιληπτό ότι, η συγκεκριμένη επίθεση χαρακτηρίζεται από ένα μεγάλο βαθμό δυσκολίας επιτυχούς έκβασης σε ένα blockchain περιβάλλον. Ωστόσο διατίθενται κάποιες υπηρεσίες κατακερματισμού, όπου ένας εγωιστής ανθρακωρύχος για παράδειγμα μπορεί να νοικιάσει έως και 50% της ισχύς κατακερματισμού ενός bitcoin στόχου για κάποιο ορισμένο χρόνο με σκοπό να το χρησιμοποιήσει στην εφαρμογή μιας "selfish mining" επίθεσης. Με αυτόν τον τρόπο το κόστος της επίθεσης για τον εγωιστή ανθρακωρύχο θα είναι η πληρωμή του στην υπηρεσία. Παράλληλα όμως θα προκύπτουν οι ανταμοιβές μόλις προστίθεται ένα νέο μπλοκ στην ιδιωτική τους αλυσίδα (Saad, Njilla, Kamhoua, Kwiat, et al., 2019). Ειδικότερα, ο ακριβής υπολογισμός του κόστους έστω p μιας επιτυχούς επίθεσης σε k μπλοκ σε ένα bitcoin σύστημα υπολογίζεται από τον παρακάτω τύπο, όπου t ο χρόνος για την δημιουργία ενός μπλοκ και r η ανταμοιβή που αντιστοιχεί στον κόμβο που δημοσίευσε το καινούριο μπλοκ και c το κόστος δανεισμού του 50% ισχύς κατακερματισμού στο blockchain σύστημα ανά ώρα :

$$p = (k \times r) - \left(\frac{k \times t \times c}{60} \right)$$

Όπως και στις επιθέσεις διπλοσυναλλαγών, σε μια "selfish mining" επίθεση ένα "mining pool" πραγματοποιεί εξόρυξη στην ιδιωτική αλυσίδα του εγωιστή ανθρακωρύχου ενώ η δημοσίευση νέου μπλοκ πραγματοποιείται σε βάση την «οδηγό» παράμετρο, η οποία αναφέρεται στην διαφορά των μηκών μεταξύ ιδιωτικής και δημόσιας αλυσίδας, καθώς και τις διακλαδώσεις που πραγματοποιούνται δεδομένου ότι τα "mining pools" των ειλικρινών και εγωιστών κόμβων έχουν προφανώς διαφορετικά «γονικά» μπλοκ. Αναλυτικότερα, ως προς την «οδηγό» παράμετρο την οποία θα ορίσουμε ως L, προκύπτουν οι παρακάτω περιπτώσεις:

- Αν L = 2, και ο ειλικρινής κόμβος πραγματοποιεί την εξόρυξη του επόμενου μπλοκ, τότε γίνεται δημοσίευση ολόκληρης της ιδιωτικής αλυσίδας.
- Αν L=0, τότε ο ειλικρινής κόμβος δραστηριοποιείται με σκοπό την δημιουργία νέου μπλοκ επί της αλυσίδας των ιδιωτικών μπλοκ και όταν ο εγωιστής ανθρακωρύχος κατορθώσει να εξορύξει το νέο μπλοκ την στιγμή εκείνη δημοσιεύεται ολόκληρη η ιδιωτική αλυσίδα.

- Αν L≥ 0 και ο εγωιστής ανθρακωρύχος δημοσιεύσει το νέο μπλοκ, τότε διατηρεί το κακόβουλο μπλοκ υπό μυστικότητα

Δεδομένου των διαφορετικών περιπτώσεων της τιμής L, το αναμενόμενο κέρδος έστω E του εγωιστή ανθρακωρύχου εκφράζεται από τον παρακάτω τύπο:

$$E_{εξόρυξης} = \frac{\alpha(1-\alpha)^2(4\alpha+\gamma(1-2\alpha))-\alpha^3}{1-\alpha(1+2(2-\alpha)\alpha},$$

όπου α είναι η δύναμη κατακερματισμού του εγωιστή ανθρακωρύχου, γ είναι η αναλογία των ειλικρινών κόμβων που προσπαθούν να κάνουν εξόρυξη μπλοκ σε "mining pool" του του εγωιστή κόμβου. Επιπλέον θεωρούμε ότι η τιμή του α θα πρέπει να ικανοποιεί την ανισωτική σχέση $0 \geq \alpha \geq 0.5$, έτσι ώστε να μην μπορεί να επιτευχθεί η 51% επίθεση. Θα πρέπει όμως να σημειωθεί ότι να μπορεί να επιτευχθεί μεγαλύτερο ποσό ανταμοιβής εξόρυξης για ένα εγωιστή ανθρακωρύχο, αν ικανοποιούνται ταυτόχρονα οι παρακάτω ανισότητες για την τιμή του α.

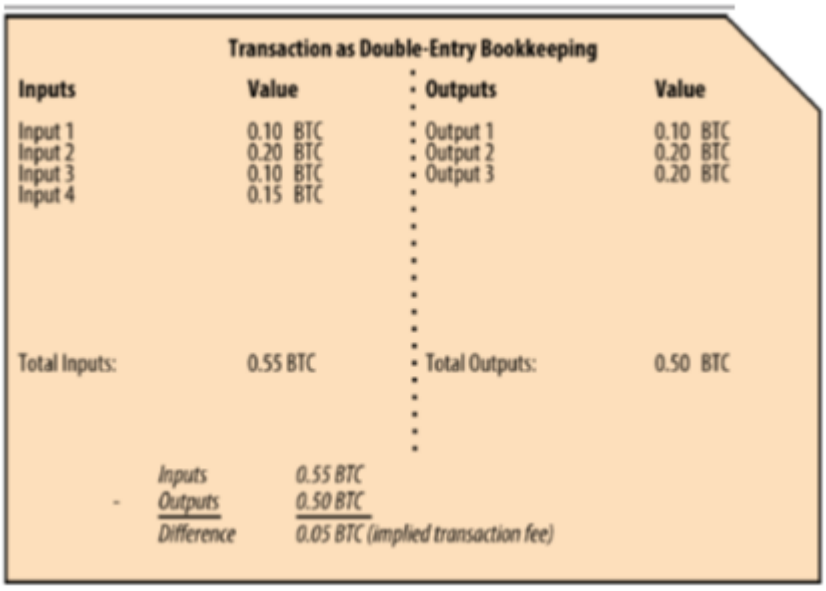
$$\frac{1-\gamma}{3-2\gamma} < \alpha < 0.5$$

Όπως ακριβώς τονίστηκε εξαιτίας της εξάρτησης του μεγέθους ενός "mining pool" με τα τέλη εξόρυξης που θα πρέπει να καταβάλουν οι τυχόν κόμβοι για ένα ανθρακωρύχο σε μια DDoS επίθεση, γίνεται αντιληπτό ότι όσο αυξάνεται το "mining pool" ενός εγωιστή ανθρακωρύχου τόσο μεγαλύτερα ποσά θα πρέπει να καταβάλουν οι νόμιμοι κόμβοι σε αυτούς ώστε να συμπεριληφθούνε οι συναλλαγές τους εντός του "mining pool" και να ανήκουν τελικά στο σύνολο των συναλλαγών εξόρυξης που θα επικρατήσουν κατά την διαδικασία αυτή. Το παραπάνω γεγονός δημιουργεί ως αναπόφευκτη συνέπεια λόγω των υψηλότερων τελών που θα πληρώνονται στους εγωιστές ανθρακωρύχους να αποκτούν σταδιακά τον έλεγχο του δικτύου συσσωρεύοντας περισσότερη ισχύ κατακερματισμού, υπονομεύοντας έτσι την αποκεντρωμένη δομή του δικτύου.

3.1.3.2 Pool-Hopping

Η επίθεση "Pool Hopping" έχει το χαρακτηριστικό ότι χρησιμοποιεί τις πληροφορίες σχετικά με τα υποβληθέν "shares" (αναλογική ανταμοιβή στα μέλη ενός mining pool, ανάλογα με την εξορυκτική ισχύ που αντιστοιχεί σε καθένα από αυτά) σε ένα "miming pool" προκειμένου να εκτελέσει μια επίθεση "selfish mining". Αναλυτικότερα, σε αυτή την επίθεση ο αντίπαλος πραγματοποιεί συνεχή ανάλυση του αριθμού των

"shares" που υποβάλλονται στους ανθρακωρύχους από άλλους κόμβους του δικτύου (Conti et al., 2018). Στο αυτό το σημείο θα ήταν καλό να αναφέρουμε από πού πηγάζει η ανταμοιβή μπλοκ (fees). Έτσι λοιπόν κάθε συναλλαγή που εμπεριέχεται τελικά σε ένα μπλοκ, πληρώνει την διαφορά του αθροίσματος των εξόδων και των εισόδων στον ανθρακωρύχο του μπλοκ, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 42:Παράδειγμα για το πώς δημιουργείται η ανταμοιβή μπλοκ[14]

Ως προς την βασική ιδέα της επίθεσης "Pool-Hopping", αν είναι ήδη αρκετά μεγάλος ο αριθμός των "shares" και συνεπώς έχουν ξοδευτεί ποσά από κόμβους χωρίς αποτέλεσμα, τότε ο αντίπαλος θα επωμισθεί ένα μερίδιο από την ανταμοιβή μπλοκ που θα προκύψει επειδή η ανταμοιβή αυτή θα διανεμηθεί με βάση το μερίδιο που καταλαμβάνει στην «πισίνα εξόρυξης» (mining pool). Για αυτόν ακριβώς τον λόγο, ο εισβολέας επιλέγει συνήθως κάποιο "mining pool" μέσα στο οποίο θα του αντιστοιχίζεται ένα μεγαλύτερο μερίδιο με σκοπό να αποκομίσει όσο το δυνατόν μεγαλύτερο κέρδος.

[14] Κάθε συναλλαγή περιέχει μια ή περισσότερες εισόδους οι οποίες είναι χρεώσεις έναντι ενός λογαριασμού bitcoin

3.1.3.3 Block Withholding Attack

Για τους ανθρακωρύχους που επιλέγουν να πραγματοποιήσουν την διαδικασία της εξόρυξης μέσω της συμμετοχής τους σε ένα "mining pool" της επιλογής τους, συμβάλουν σε αυτό με τον δανεισμό των υπολογιστικών τους πόρων με σκοπό την επίλυση του αλγορίθμου συναίνεσης προκειμένου να δημιουργηθεί ένα μπλοκ, ενώ η ανταμοιβή τους (block reward) γίνεται αναλογικά, ανάλογα δηλαδή με το ποσοστό κατακερματικής ισχύς που διαθέτουν. Οι ανθρακωρύχοι όμως ανάλογα με την εγκυρότητα (verifications number) του μπλοκ μπορούν να καθυστερήσουν την υποβολή του μπλοκ, γεγονός το οποίο μπορεί να χρησιμοποιηθεί ως μια κατάσταση εν δυνάμει επίθεσης (Shrivas, M. K., Dean & T. Y., 2020). Ειδικότερα, η δολιοφθορά που πραγματοποιείται σε "mining pool" μπορεί να είναι ιδιαίτερα σοβαρή, καθώς ο επιτιθέμενος δεν στέλνει κάποιο μπλοκ στο "mining pool", ενώ παράλληλα λαμβάνει (λόγω αδυναμίας του συστήματος) το αναλογικό "block reward" που θα δικαιούταν.

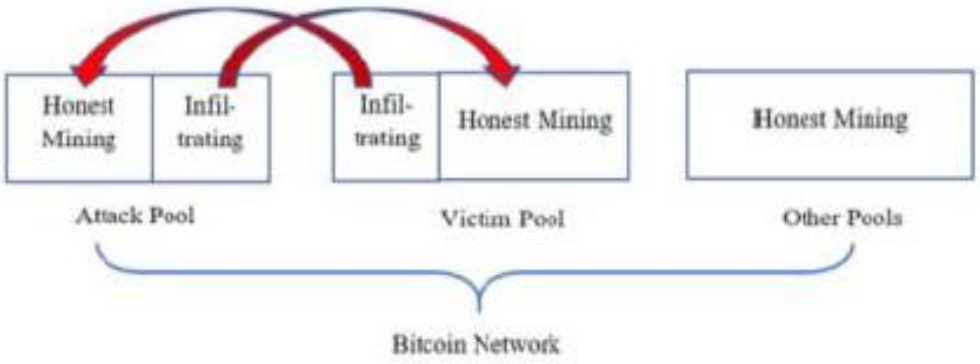
Ο επιτιθέμενος ανθρακωρύχος, ο οποίος θα ανήκει σε μια συγκεκριμένη ομάδα ανθρακωρύχων (mining pool) δημιουργεί επιτυχώς ένα νέο μπλοκ αλλά αποστέλλει (ως πληροφορία) ένα μέρος μόνο της ανταμοιβής που έλαβε, ενώ σύμφωνα με τον προκαθορισμό των προσεχών μπλοκ στέλνει το μπλοκ όπου είναι πιο κερδοφόρο για αυτόν. Με άλλα λόγια, στην επίθεση "Block Withholding attack" ο επιτιθέμενος ανθρακωρύχος δεσμεύει ένα μέρος των εσόδων από το "mining pool". Με αυτό τον τρόπο, ο ειλικρινής ανθρακωρύχος θα λαμβάνει τελικά μικρότερο μερίδιο κέρδους, αφού η ανταμοιβή θα διανέμεται σε περισσότερους ανθρακωρύχους.

Με αυτή την έννοια, γίνεται σαφώς πιο δύσκολος ο εντοπισμός μιας επίθεσης που σχετίζεται με μια "mining pool", όταν κατά κάποιο τρόπο έχουμε μια ταχτοποίηση ενός μεγαλύτερου αριθμού ανθρακωρύχων που είναι υποψήφιοι για την πραγματοποίηση της επίθεσης "withholding". Στο σημείο αυτό, θα πρέπει να τονιστεί ότι η συγκεκριμένη επίθεση δεν περιορίζεται μόνο σε επίπεδο ανθρακωρύχων που εντάσσονται και αφορούν ένα "mining pool", αλλά μπορεί να είναι και σε επίπεδο διαφορετικών "mining pools". Για παράδειγμα, έστω ότι υπάρχουν δύο διαφορετικές ομάδες ανθρακωρύχων P_a, P_b και θεωρείται επιπλέον ότι κάποιοι από τους ανθρακωρύχους της P_b διεισδύουν στην P_a, για να ξεκινήσουν την επίθεση "Block Withholding" σε αυτήν (Shrivas, Dean, & Brunda, 2020). Για να το πετύχουν αυτό στέλνουν αρχικά ένα έγκυρο μπλοκ στην P_b. Έτσι, οι επιτιθέμενοι ανθρακωρύχοι οι οποίοι εντάσσονται στην P_a, αλλά εργάζονται για την επίλυση του μοντέλου συναίνεσής ως προς την P_b, θα καρπωθούν τελικά ανταμοιβή

εξόρυξης και τα δύο “mining pools”. Γίνεται έτσι εύκολα αντιληπτό ότι η P_a θα έχει απώλειες, ενώ αντίθετα η P_b θα παράγει περισσότερα μπλοκ και κατ’ επέκταση θα καρπώνεται περισσότερες ανταμοιβές μπλοκ, αφού θα «εργάζονται» τελικά για αυτήν και ανθρακωρύχοι από εξωτερικά “mining pools”.

Συμπερασματικά, αυτή η επίθεση στοχεύει στην καταστροφή μιας δεξαμενής εξόρυξης και στην άδικη απόκτηση εσόδων (ανταμοιβών), μέσω της παρακράτησης μπλοκ που ο επιτιθέμενος έχει εξορύξει. Η επίθεση μάλιστα κατηγοριοποιείται σε δύο τύπους με βάση την τακτική που χρησιμοποιείται. Την δολιοφθορά και την παραμονή. Στην δολιοφθορά, η τακτική του επιτιθέμενου είναι απλώς να μην υποβάλλει κανένα μπλοκ που έχει εξορύξει στον χειριστή της ομάδας εξόρυξης που ανήκει. Σε αυτήν την περίπτωση ο χειριστής δεν υφίσταται κάποια απώλεια, αλλά οι ανταμοιβές για τους ανθρακωρύχους που συνθέτουν την ομάδα εξόρυξης (συμπεριλαμβάνοντας στο σύνολο αυτό και τον επιτιθέμενο) δεν θα λαμβάνουν ως “block reward” αυτό που πραγματικά τους αναλογεί, σύμφωνα με την εξορυκτική ισχύ που «προσφέρουν» και συνεπώς είναι ζημιωμένοι. Από την άλλη, η τακτική της επίθεσης σε αναμονή επιτρέπει στον επιτιθέμενο να κερδίσει έσοδα, κάτι το οποίο το πετυχαίνει μέσω της ταυτόχρονης εξόρυξης σε διαφορετικά “mining pools”. Έτσι μόλις δημιουργεί ένα μπλοκ σε ένα από αυτά, ο επιτιθέμενος το κρατά ιδιωτικό, συγκεντρώνοντας εκεί όλη την ισχύ κατακερματισμού του. Στην συνέχεια ο επιτιθέμενος υποβάλλει τελικά το μπλοκ του σε χρόνο t μετά την δημιουργία του, αυξάνοντας την ανταμοιβή με το επιπλέον ποσό να αφορά την ορισμένη ανταμοιβή που θα λάμβανε από το άλλο “mining pool” που ανήκει με βάση την συμμετοχή του ως προς την εξορυκτική ισχύς σε αυτό :

t = (n-1)/(2n-1) t_0, όπου n= ο συνολικός αριθμός “mining pools” και t_0 ο μέσος χρόνος δημιουργίας ενός μπλοκ



Εικόνα 43:Block withholding attack[15]

3.1.3.4 Fork after withholding attack

Η συγκεκριμένη επίθεση αποτελεί ένα συνδυασμό των επιθέσεων “Selfish mining” και “block withholding” ουσιαστικά αποτελεί μια παραλλαγή της επίθεσης “block withholding”. Αναλυτικότερα, το κοινό της με την “block withholding” είναι το γεγονός ότι συμμετέχει σε δύο διαφορετικές «δεξαμενές εξόρυξης» μοιράζοντας την ισχύ εξόρυξης τους μεταξύ μιας τίμιας και μιας κακόβουλης (Shrivas et al., 2020). Στην περίπτωση της “Fork after withholding” επίθεσης, η ανταμοιβή του επιτιθέμενου είναι πάντα μεγαλύτερη ή ίση από τον αντίστοιχο επιτιθέμενο της επίθεσης “block withholding”, ενώ έχει υπολογιστεί ότι πρόκειται για περίπου τέσσερις φορές πιο αποτελεσματική για τον επιτιθέμενο σε σχέση με σε σύγκριση , με την “block withholding” επίθεση.

3.1.3.5 Bribery attack

Στην επίθεση Bribery, ένας εισβολέας δωροδοκεί έναν ανθρακωρύχο ώστε να νοικιάσει υπολογιστικούς πόρους με στόχο προφανώς να αυξήσει ο ίδιος την συνολική ισχύ κατακερματισμού που διαθέτει, ώστε να χρησιμοποιηθεί σε τυχόν επιθέσεις στο δίκτυο. Για τον λόγο αυτό προτείνεται ως άμεση λύση η μείωση του κινήτρου που το προκαλεί με την αντίστροφη ενέργεια της «αντιπληρωμής» σε ανθρακωρύχους και ειδικότερα σε ομάδες ανθρακωρύχων (mining pools), οι οποίες διαθέτουν αθροιστικά μεγαλύτερη αξία σε σχέση με το ποσό που θα τους προσφέρει ο τυχών εισβολέας ώστε να μετατραπούν σε κακόβουλους κόμβους. Με άλλα λόγια, βασίζεται στην δωροδοκία επικυρωτών ή ανθρακωρύχων (ανάλογα το περιβάλλον του blockchain), με στόχο τελικά ο εισβολέας να είναι σε θέση να πραγματοποιεί αυθαίρετες συναλλαγές ως έγκυρες μέσω ανέντιμων κόμβων οι οποίοι όπως αναφέρθηκε έχουν πληρωθεί για την επαλήθευση των συναλλαγών. Ωστόσο για να μετατραπούν οι κόμβοι σε «ανέντιμους» θα πρέπει να έχουν κέρδος τουλάχιστον ίσο με το ποσό ανταμοιβής που προκύπτει από την εξόρυξη του μπλοκ. Με αυτό τον τρόπο, ειδικά αν το ποσό είναι μεγαλύτερο δίνεται ένα ισχυρό κίνητρο

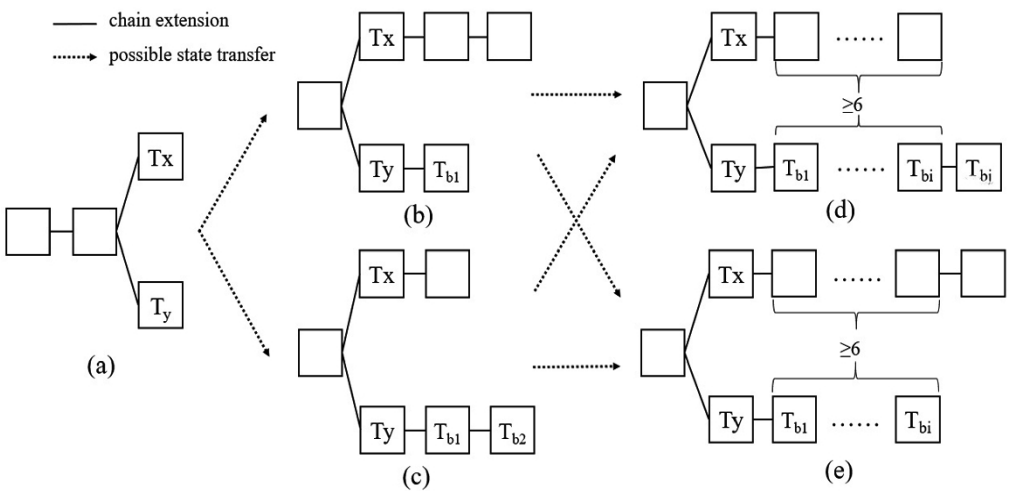
[15] Ανακτήθηκε από: https://www.researchgate.net/profile/Asif-Karim-4/publication/337284911_An_Overview_of_Blockchain_Applications_and_Attacks/links/5de1255f4585159aa453d600/An-Overview-of-Blockchain-Applications-and-Attacks.pdf

σε ανθρακωρύχο να επιλέξει τελικά την αλυσίδα του εισβολέα για να συνεχίσει την διαδικασία της εξόρυξης. Με άλλα λόγια, είναι δυνατό να δωροδοκηθούν κόμβοι χωρίς να χρειάζεται να πληρωθούν, με την έννοια ότι το σύστημα δωροδοκεί τους κακόβουλους κόμβους της ιδιωτικής διακλάδωσης που δημιουργείται. Αναλυτικότερα, ο επιτιθέμενος μπορεί να αντιμετωπίζει ένα πιο σημαντικό πρόβλημα όπως για παράδειγμα όταν μια κακόβουλη διακλάδωση αναστρέφεται (με την έννοια ότι ανέντιμοι κόμβοι σταματούν την δραστηριότητα τους επί της διακλάδωσης και συνεπώς ο επιτιθέμενος δεν μπορεί να τους δωροδοκήσει για να πετύχει τον σκοπό του. Σε μια τέτοια περίπτωση ο επιτιθέμενος θα έπρεπε να πληρώσει ένα μεγάλο ποσό δωροδοκιών, για να καλύψει τις δωροδοκίες για κάθε μπλοκ που κόπηκε.

Στην bribery attack, οι ανθρακωρύχοι που έχουν ήδη εξορύξει και συνεπώς λάβει προσωρινές ανταμοιβές εξόρυξης για την τρέχων μακρύτερη διακλάδωση έτσι ώστε να τεθούν κίνητρα να υπάρχει αντίσταση στον εισβολέα μέσω αντιδωροδοκίας, προκειμένου να πεισθούν οι ανθρακωρύχοι να συνεχίσουν την εξόρυξη στην τρέχουσα μεγαλύτερη αλυσίδα και να πιστέψουν ότι οι ανταμοιβές εξόρυξης τους δεν θα χαθούν. Με άλλα λόγια αν ο επιτιθέμενος, επιχειρήσει την δημιουργία ιδιωτικής διακλάδωσης μήκους k μπλοκ, σε περίπτωση που πετύχει η επίθεσή θα υπάρχει ως ακόλουθη συνέπεια κάποιοι ανθρακωρύχοι να χάσουν όλο αυτό τον αριθμό μπλοκ που έχουν δημιουργηθεί ως εκείνη την στιγμή στην ιδιωτική αλυσίδα του επιτιθέμενου (Bonneau, n.d.). Τότε αυτοί θα προσπαθήσουν να ξοδέψουν σχεδόν όλα τους τα ποσά για να αμυνθούν στον επιτιθέμενο, οποίος θα έχει εξαφανιστεί σε περίπτωση επιτυχίας της επίθεσης. Σε μια τέτοια περίπτωση ο εισβολέας θα πρέπει να πληρώσει $k \times b$ σε δωροδοκίες.

Το **αναμενόμενο κόστος** θα είναι $k \times \varepsilon \times b + c$, όπου:

- b είναι η ανταμοιβή για το νέο μπλοκ
- k είναι ο αριθμός των μπλοκ πίσω από τα οποία είναι ο επιτιθέμενος
- ε είναι ο συντελεστής ο οποίος αποφασίζει την αξία της εισφοράς δωροδοκίας η οποία δεν είναι ίδια πάντα.
- c είναι μια προσφορά την αν ο επιτιθέμενος χρειάζεται να υλοποιήσει κάποιο έξυπνο συμβόλαιο.



Εικόνα 44:Απεικόνιση επίθεσης bribe attack, όπου Tx:συναλλαγή στόχος και Ty:διπλής-σπατάλης συναλλαγή[16]

Όσον αφορά το φαινόμενο της διπλής δαπάνης στην ουσία ο εισβολέας δεν αποκτά διπλό κεφάλαιο, αλλά μόνο ξεγελά προσωρινά κάποιο άλλο μέρος ότι έχει λάβει πληρωμή. Το λεπτό ρόλο σε αυτή την περίπτωση παίζει ο αντισυμβαλλόμενος εισβολέας (ο οποίος είναι μέρος της αρχιτεκτονικής της επίθεσης) και μπορεί να ξεγελάσει το θύμα του μεταφέροντας άμεσα (μετά από k μπλοκ επιβεβαίωσης) μια ίσης αξίας ανταλλαγή, όπως για παράδειγμα ίσης αξίας ποσό σε bitcoin. Με άλλα λόγια, ο επιτιθέμενος δεν μπορεί να διπλασιάσει τις δαπάνες χωρίς να πληρώσει τέλη συναλλαγής στο αντισυμβαλλόμενο μέρος. Πάντως η έννοια του ορίου έχει νόημα εξαιτίας του πεπερασμένου αριθμού νομισμάτων bitcoin. Έτσι το δυναμικό κέρδους έχει όρια ενώ τα κέρδη από την επίτευξη μιας διπλής δαπάνης θα είναι υψηλότερα από τις ανταμοιβές εξόρυξης των μπλοκ. Αυτός ακριβώς είναι και ο λόγος του μεγάλου όγκου των δωροδοκιών που απαιτείται.

Για την καλύτερη κατανόηση της διαδικασίας, θέτουμε ένα παράδειγμα. Έστω ότι η Αλίκη πραγματοποιεί μια συναλλαγή με τον Μπομπ έχοντας μάλιστα την μειοψηφία της ισχύς κατακερματισμού στο δίκτυο, προσπαθώντας να ξεκινήσει μια επίθεση διπλής δαπάνης στον Μπομπ (Ebrahimpour & Haghighi, 2021) . Έτσι αφού πραγματοποιήσει την συναλλαγή αυτή και στην συνέχεια συμπεριληφθεί στην αλυσίδα θα συμμετέχει στην διαδικασία εξόρυξης της διακλάδωσης, όπου θα κάνει εξόρυξη ενός μπλοκ στο οποίο δεν θα εμπεριέχει αυτή την συναλλαγή, κρατώντας αυτή την πληροφορία μυστική, χωρίς

[16] Ανακτήθηκε από: https://doi.org/10.1007/978-3-030-59013-0_28

δηλαδή να το κάνει γνωστό στου υπόλοιπους κόμβους. Η Αλίκη όμως θα πρέπει να δημιουργήσει τουλάχιστον ένα νέο μπλοκ στην αλυσίδα της (διακλάδωση), πριν όμως προλάβει να γίνει επιβεβαίωση της συναλλαγής, που σημαίνει να προστεθεί η συναλλαγή σε μπλοκ της βασικής αλυσίδας. Αυτό το μπλοκ της διακλάδωσης που δημιούργησε θα περιέχει κάποιες ειδικές συναλλαγές, όπου μεταφέρει η Αλίκη bitcoin σε νέες διευθύνσεις, τις οποίες όμως έχει δημιουργήσει η ίδια σε προηγούμενο χρόνο. Στο σημείο αυτό, μόλις η συναλλαγή της Αλίκης επιβεβαιωθεί (και γίνει και μη αναστρέψιμη που σημαίνει ότι επιβεβαιωθεί για έξι τουλάχιστον μπλοκ), ο Μπομπ στέλνει το εμπόρευμα στην Αλίκη η οποία απελευθερώνει το μπλοκ της και στην συνέχεια προσπαθεί να δωροδοκήσει επόμενους ανθρακωρύχους για να ακολουθήσουν την διαδικασία της εξόρυξης στην διακλάδωση της Αλίκης.

Για να επιτευχθεί αυτό, η Αλίκη αποκαλύπτει το ιδιωτικό κλειδί των διευθύνσεων που έχει μεταφέρει τα bitcoin, στα μπλοκ που δημιούργησε. Αυτό έχει ως συνέπεια οι ανθρακωρύχοι που βλέπουν το ιδιωτικό κλειδί, θα επιλέξουν να συμμετέχουν στην διαδικασία της εξόρυξης στην αλυσίδα-διακλάδωση της Αλίκης (Ebrahimpour & Haghighi, 2021). Έτσι μόλις ένα ανθρακωρύχος βρει μια λύση και δημιουργήσει ένα νέο μπλοκ, η Αλίκη το επιβεβαιώνει με την δημιουργία ενός μπλοκ από την πλευρά της αποκαλύπτοντας το επόμενο ιδιωτικό κλειδί. Σε αυτή την φάση, αν τα καταφέρει δίνοντας κίνητρα για συγκέντρωση ισχύς εξόρυξης στην διακλάδωση της θα δημιουργηθούν με αυτό τον τρόπο επιπλέον μπλοκ με αποτέλεσμα το μήκος της διακλάδωσης να περάσει το μήκος της αρχικής αλυσίδας, έτσι ώστε να μην επιτευχθεί η αρχική συναλλαγή ανάμεσα στην Αλίκη και στον Μπομπ και να αναιρεθεί.

Μελλοντικά, η επίθεση δωροδοκίας (Bribery attack) σε κρυπτονομίσματα και ειδικά στο Bitcoin, που όπως ξέρουμε ο αριθμός των νομισμάτων είναι περιορισμένος και θα μειώνεται με την πάροδο του χρόνου, θα έχει ως συνέπεια να αποκτά όλο και μεγαλύτερο προβάδισμα η επίτευξη της επίθεσης. Αυτό γίνεται εύκολα κατανοητό, αν σκεφθούμε ότι συγκριτικό κριτήριο μεταξύ των 2 αλυσίδων που δημιουργούνται είναι η σύγκριση των τελών συναλλαγής είτε στην κύρια αλυσίδα είτε σε αυτή που έχει δημιουργήσει ο επιτιθέμενος. Δεδομένου λοιπόν του φαινομένου “halving”, όπου κάθε 4 χρόνια θα μειώνεται η ανταμοιβή μπλοκ ενός ανθρακωρύχου, μπορούμε λοιπόν να διαπιστώσουμε ότι το απαιτούμενο ποσό δωροδοκίας ώστε κάποιος ανθρακωρύχος να επιλέξει να κάνει εξόρυξη αντί για την κύρια αλυσίδα στην αλυσίδα του επιτιθέμενου θα υποστεί και αυτό μείωση.

3.1.4 Cryptographic attacks

Δεδομένου ότι στα περισσότερα από τα κρυπτονομίσματα εφαρμόζεται ασύμμετρη κρυπτογραφία για την ασφάλεια συναλλαγών, γίνεται εύκολα αντιληπτό ότι η κρυπτογραφία αποτελεί τον πυρήνα της τεχνολογίας blockchain. Στα χαρακτηριστικά της κρυπτογραφίας δημοσίου κλειδιού ή αλλιώς ασύμμετρης κρυπτογραφίας είναι ότι ο πελάτης διατηρεί ένα ιδιωτικό κλειδί το οποίο είναι μοναδικό και αποθηκεύεται στο blockchain πορτοφόλι. Το blockchain χρησιμοποιεί τον αλγόριθμο ecdsa για να δημιουργήσει μια διάταξη ιδιωτικών κλειδιών που αντιστοιχούν σε σχετικά δημόσια κλειδιά.

3.1.4.1 Private key attack

Όπως αναφερθήκαμε οι ψηφιακές υπογραφές εκτελούνται μέσω του αλγορίθμου ECDSA. Στοχεύοντας να αναλύσουμε τον συγκεκριμένο αλγόριθμό στον οποίο βασίζεται και το σύστημα bitcoin αναφέρουμε αρχικά το σύνολο παραμέτρων του συστήματος: η εξίσωση C εκφράζει την ελλειπτική καμπύλη, G είναι ο γεννήτορας της ελλειπτικής καμπύλης και έστω n πρώτος αριθμός που αντιστοιχεί στην τάξη του G, όπου είναι ορισμένα στην καμπύλη secp256k1. Θεωρούμε τον βαθμωτό πολλαπλασιασμό *, ως την πράξη (σημείου) της ελλειπτικής καμπύλης . Επιπλέον θεωρούμε d το ιδιωτικό κλειδί (Pérez-Solà et al., 2019). Ο αλγόριθμος υπογραφής για μήνυμα m χρησιμοποιώντας μια συνάρτηση κατακερματισμού: h=hash(m) ορίζεται παρακάτω ως εξής.

1. Αρχικά επιλέγεται ένας ακέραιος k στο διάστημα [1,n-1]. Στην περίπτωση ντετερμινιστικής ECDSA, η τιμή k είναι HMAC προερχόμενη από την τιμή h+privkey. Αυτή η τιμή (k), χρησιμοποιείται για τον υπολογισμό ενός τυχαίου σημείου στην ελλειπτική καμπύλη του οποίου η συντεταγμένη x χρησιμοποιείται στον υπολογισμό της υπογραφής
2. Υπολογίζεται το τυχαίο σημείο της καμπύλης R = (x,y)=k*G, όπου r = Rx
3. r = x mod n
4. Υπολογίζεται η απόδειξη υπογραφής: s = k^{-1} *(m+r*d) mod n, όπου k^{-1} mod n είναι ένας ακέραιος: k * k^{-1} = 1 mod n
5. Αν s = 0 ή r = 0, επιστρέφουμε στο βήμα 1
6. Έξοδος: signature(m)={r,s}

Θα πρέπει να τονίσουμε ότι υπάρχει μια ευπάθεια στον αλγόριθμο ECDSA, σύμφωνα με την οποία ένας εισβολέας που εντοπίζει 2 υπογραφές διαφορετικών μηνυμάτων οι οποίες γίνονται με το ίδιο ιδιωτικό κλειδί είναι σε θέση να εξαγάγει το ιδιωτικό κλειδί αν ο υπογράφων χρησιμοποιήσει ξανά το ίδιο k που επιλέχτηκε στο βήμα 1 (Pérez-Solà et al., 2019). Αυτό σημαίνει, ότι αν 2 υπογραφές ECDSA που δημιουργήθηκαν χρησιμοποιώντας το ίδιο k και το ίδιο ιδιωτικό κλειδί: sig_a=sig (m_a)=(r, s_a) και sig_b=sig(m_b)=(r , s_b) με m_a=m_b τότε ο εισβολέας που αποκτά τις 4 πληροφορίες sig_a, sig_b, m_a, m_b θα μπορεί να βρει το ιδιωτικό κλειδί d.

Αναλυτικότερα, με βάση τον ορισμό της ψηφιακής υπογραφής:

$s_a = k^{-1}(m_a$ + rd) mod q ⇒ k$s_a = m_a$+ rd mod q (*)

s_b=k^{-1} (m_b + rd) mod q ⇒ ks_b = m_b + rd mod q (**)

Δεδομένου ότι το r παράγεται από το k ντετερμινιστικά , όπως φαίνεται στο βήμα 2 με τις υπόλοιπες παραμέτρους σταθερές συνεπάγεται ότι ή τιμή r για τις ψηφιακές υπογραφές s_a, s_b θα είναι ίδια. Έτσι από τις εξισώσεις (*),(**) ένας επιτιθέμενος μπορεί να υπολογίσει την τιμή k = $\frac{m_b - m_a}{s_b - s_a}$. Με αυτό τον τρόπο αφού γνωρίζει ήδη την τιμή k, **ο επιτιθέμενος βρίσκει το ιδιωτικό κλειδί** λύνοντας από τις εξισώσεις (*),(**) ως προς d: d = $\frac{s_a k - m_a}{r}$ ή d = $\frac{s_b k - m_b}{r}$. Λόγω αυτής της ευπάθειας κάποια πορτοφόλια bitcoin εφαρμόζουν μέθοδο ντετερμινιστικής ECDSA, όπως αναφέρεται στο βήμα 1, όπου k = h+privkey, με h=hash(m).

Καταλήγοντας, ο επιτιθέμενος μπορεί να υπολογίσει το ιδιωτικό κλειδί γεγονός το οποίο μπορεί να προκαλέσει την απώλεια όλων των χρημάτων ενός πορτοφολιού ή να τροποποιήσει πλήρως τα δεδομένα συναλλαγής, αφού αποκτάται ο πλήρης έλεγχος στον λογαριασμό blockchain.

3.1.4.2 Vulnerable Signature

Τα δίκτυα blockchain χρησιμοποιούν διάφορους κρυπτογραφικούς αλγορίθμους για να δημιουργήσουν υπογραφές χρηστών, αλλά μπορεί επίσης να έχουν τρωτά σημεία. Για παράδειγμα, το bitcoin χρησιμοποιεί τον κρυπτογραφικό αλγόριθμο ecdsa για να δημιουργεί αυτόματα μοναδικά ιδιωτικά κλειδιά που αντιστοιχούν σε σχετικά δημόσια κλειδιά. Η IOTA αντιμετώπιζε προβλήματα κρυπτογράφησης με την παλιά συνάρτηση κατακερματισμού.

Διαπιστώνεται λοιπόν, ότι και ο αλγόριθμος ecdsa έχει ανεπαρκή εντροπία, η οποία μπορεί να οδηγήσει στην ίδια τυχαία τιμή σε περισσότερες από μία υπογραφές. Αυτό συνέβη για παράδειγμα με το περιστατικό ονόματι “Anyswap hack” τον Ιούλιο του 2021. Έτσι σε αυτή την περίπτωση, η ίδια τιμή k χρησιμοποιήθηκε για την δημιουργία πολλαπλών διαφορετικών ψηφιακών υπογραφών (“How Hackers Can Exploit Weak ECDSA Signatures,” n.d.). Προτείνεται λοιπόν να ελέγχεται κάθε φορά μεμονωμένα κατά την παραγωγή τυχαίων τιμών για κάποιο k , ώστε η τιμή r να είναι διαφορετική για όλες τις συναλλαγές.

3.1.4.3 Flawed Key generation

Η επίθεση αυτή εμφανίστηκε τον Δεκέμβριο του 2014, όταν ένας χάκερ γνωστός ως Johoe απέκτησε πρόσβαση στα ιδιωτικά κλειδιά που υπήρχαν στο πορτοφόλι Blockchain.info. Ως προς το αποτέλεσμα της επίθεσης στο πορτοφόλι Blockchain.info χάθηκαν 250 bitcoin. Αναλυτικότερα, η επίθεση συνέβη, ως αποτέλεσμα ενός λάθους που εμφανίστηκε κατά την διάρκεια μιας ενημέρωσης κώδικα που είχε ως αποτέλεσμα την κακή τυχαιότητα των εισόδων για την δημιουργία των δημοσίων κλειδιών των χρηστών. Με άλλα λόγια, οι είσοδοι στο αλγόριθμο ecdsa λόγω του προβλήματος τυχαιότητας δεν παρήγαγαν αποτελεσματικά μια αποτελεσματική μονόδρομη συνάρτηση για την δημιουργία δημόσιων κλειδιών. Το θέμα αυτό αντιμετωπίστηκε μέσα σε μόλις 2.5 ώρες, αλλά ποτέ δεν αποκλείεται να υπάρξει ξανά κάποιο ελάττωμα στις υλοποιήσεις το οποίο θα δημιουργούσε επαναφορά του προβλήματος και διαρροή των ιδιωτικών κλειδιών

3.1.4.4 Tampering

Σε ένα δίκτυο bitcoin, μετά την εξόρυξη ενός μπλοκ οι ανθρακωρύχοι μεταδίδουν πληροφορίες σχετικά με τις νέες εξορύξεις μπλοκ που υπάρχουν. Αυτή η επίθεση στοχεύει στην καθυστέρηση της διάδοσης συναλλαγών ή μπλοκ ενός συγκεκριμένου κόμβου, ενώ με την καθυστέρηση αυτή προκαλείται συμφόρηση στο δίκτυο ή μπορεί με την αποστολή αλλεπάλληλων αιτήσεων σε όλες τις θύρες ενός κόμβου να στοχεύεται η απασχόληση αυτού (Conti et al., 2018). Έτσι ένας τέτοιος τύπος επίθεσης είναι δυνατό να προκαλέσει άλλους τύπους επιθέσεων στο δίκτυο, όπως επιθέσεις DDoS ή Double Spending σε ηθικούς ανθρακωρύχους, οι οποίες επιθέσεις έχουν ως αποτέλεσμα την αύξηση της εξορυκτικής ισχύς για τον επιτιθέμενο. Σε επίπεδο κρυπτογραφίας η ιδιότητα κατακερματισμού αποθηκεύει τις συναλλαγές από τυχόν παραβιάσεις, εφαρμόζοντας

επαναυπολογισμό κατακερματισμού για κάθε μπλοκ σε περίπτωση τροποποίησης. Με αυτό τον τρόπο ένας εισβολέας δεν μπορεί να κάνει παραποίηση λόγω των ιδιοτήτων κατακερματισμού στο blockchain (Anita. & Vijayalakshmi., 2019). Αυτό συνεπάγεται ότι η τιμή κατακερματισμού υπολογίζεται εκ νέου για κάθε μπλοκ, δημιουργώντας με αυτό τον τρόπο τις καθυστερήσεις στις συναλλαγές.

3.1.4.4 Quantum attacks

Οι κβαντικοί υπολογιστές αποτελούν απειλή για πολλά κρυπτογραφικά πρωτόκολλα. Έτσι εκτιμάται ότι μέχρι το 2035 θα υπάρχει υπολογιστής που θα μπορεί να σπάσει το κρυπτογραφικό σχήμα RSA2048. Όσον αφορά την τεχνολογία blockchain εκτιμάται ότι τα πρωτόκολλα που χρησιμοποιεί θα είναι επιρρεπή σε κβαντικές επιθέσεις. Με βάση την υπολογιστική ισχύ των κβαντικών υπολογιστών είναι βέβαιο ότι θα μπορούν να παραβιάσουν σε ελάχιστο χρόνο ένα πορτοφόλι (Kearney, n.d.). Για τον λόγο αυτό αποτελεί την πιο σοβαρή απειλή για το blockchain, θέτοντας σε αμφισβήτηση την επόμενη μέρα της τεχνολογίας, δημιουργώντας την ανάγκη να ενσωματώσει η τεχνολογία την κβαντική φιλοσοφία, προκειμένου να επιβιώσει, αφού οι περισσότεροι αλγόριθμοι ασύμμετρης κρυπτογράφησης όπως SHA256, RSA, Keccak256 κ.α. δεν είναι ασφαλείς σε μια τέτοια περίπτωση. Δεδομένου όμως ότι η τεχνολογία είναι σχετικά νέα όπως και οι κβαντικοί υπολογιστές, δίνονται χρονικά περιθώριά προκειμένου η τεχνολογία blockchain να έχει προοπτικές προσαρμογής σε αυτές τις επιθέσεις.

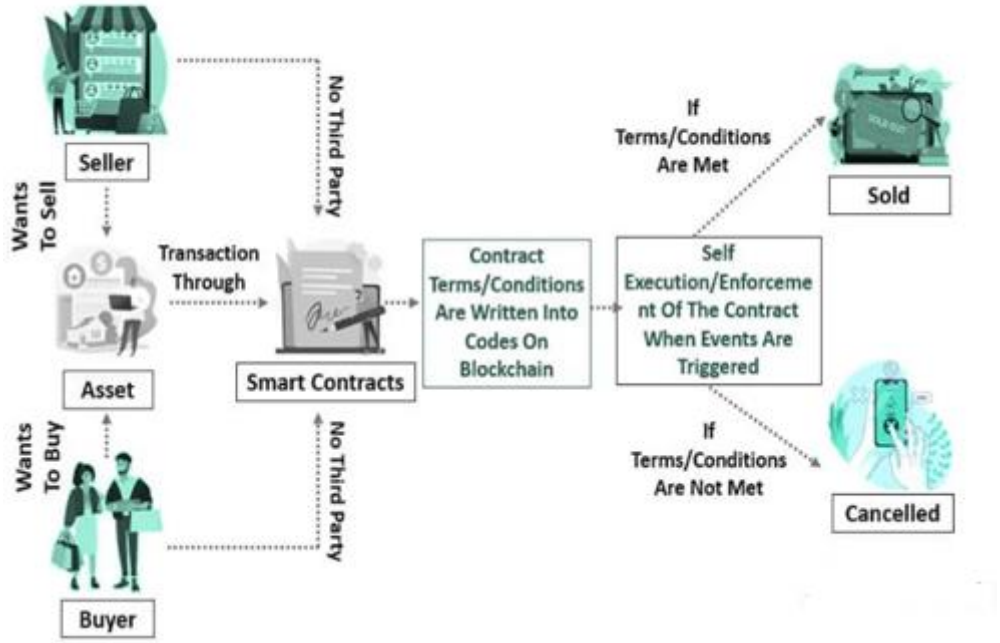
3.1.5 Smart contract attacks

Τα έξυπνα συμβόλαια είναι προγράμματα ή σενάρια που εκτελούνται αυτόματα υπό την προϋπόθεση όμως ότι πληρούνται κάποιες προϋποθέσεις. Ένα έξυπνο συμβόλαιο είναι ένα κομμάτι εκτελέσιμου κώδικα στο blockchain για να εκτελέσει αυτόνομα και να εφαρμόσει τους προκαθορισμένους όρους μιας συμφωνίας χωρίς την εμπλοκή ενός αξιόπιστου τρίτου μέρους. Μερικά από τα βασικά πλεονεκτήματα του είναι το χαμηλό κόστος συναλλαγής αλλά και πλεονεκτήματα σε ζητήματα ασφαλείας, όπως είναι η εγγενής αμετάβλητη λειτουργία ενός έξυπνου συμβολαίου στα πλαίσια του blockchain (Mense & Flatscher, 2018). Το Ethereum αποτελεί μια blockchain πλατφόρμα η οποία υποστηρίζει τα έξυπνα συμβόλαια, ενώ το περιβάλλον στο οποίο εκτελούνται τα έξυπνα συμβόλαια ονομάζεται Ethereum virtual machine (EVM). Κάθε λειτουργία που «τρέχει»

στην εικονική μηχανή, εκτελείται ταυτόχρονα σε κάθε κόμβο στο δίκτυο (Dika & Nowostawski, 2018). Επιπλέον, κάθε συναλλαγή στα συμβόλαια έχει ένα κόστος το οποίο αποτιμάται σε "gas", ενώ κάθε μονάδα gas που καταναλώνεται από μια συναλλαγή πληρώνεται σε νομίσματα "ether" με βάση την δυναμική τιμή "gas".

Ένα δίκτυο Ethereum είναι ένα κατανεμημένο και αποκεντρωμένο δίκτυο. Το δίκτυο Ethereum έχει δύο τύπους λογαριασμών. Ο ένας είναι ο λογαριασμός χρήστη που ελέγχεται από το ιδιωτικό κλειδί και ο άλλος είναι ο λογαριασμός έξυπνου συμβολαίου από τον μεταγλωττισμένο κώδικα. Οι λογαριασμοί χρηστών δεν έχουν κάποιο κωδικό και μπορούν να στείλουν μηνύματα σε άλλους λογαριασμούς δημιουργώντας και υπογράφοντας μια συναλλαγή χρησιμοποιώντας τα ιδιωτικά τους κλειδιά. Ειδικότερα, ο λογαριασμός του παραλήπτη αναγνωρίζει τον λογαριασμό του αποστολέα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Επιπλέον κάθε Ethereum λογαριασμός έχει μήκος 20 byte και αποτελείται από μια μοναδική διεύθυνση, το τρέχων υπόλοιπο σε νομίσματα ether, τα δεδομένα αποθήκευσης και ένα "nonce" (Buterin, n.d.).

Γενικά, ένα "smart contract" αποτελεί ένα σύνολο συναρτήσεων καθεμία από τις οποίες ορίζεται από μια ακολουθία εντολών bytecode. Ένα από τα βασικά χαρακτηριστικά των "smart contracts" είναι ότι οι χρήστες μεταφέρουν μέσω των συμβολαίων το νόμισμα ether. Με άλλα λόγια, οι χρήστες αποστέλλουν συναλλαγές στο δίκτυο του Ethereum για να δημιουργήσουν νέα συμβόλαια, για να ορίσουν λειτουργίες σε αυτά ή απλά να κάνουν μεταφορά του νομίσματος ether σε κάποιο χρήστη του δικτύου. Οι συναλλαγές αυτές μπορεί να είναι μια έκδοση εισιτηρίων ή μια αποστολή ενημερώσεων και εκτελούνται μόνο όταν ικανοποιούνται και έχουν επαληθευτεί οι ορισμένες συνθήκες του συμβολαίου, ενώ εκτελούνται με εντολές "if…then…else" γραμμένες σε κώδικα με την γλώσσα Solidity. Όπως ακριβώς συμβαίνει και με το bitcoin (blockchain 1.0) έτσι και στα smart contracts οι συναλλαγές καταγράφονται σε μια δημόσια δομή δεδομένων. Όσον αφορά τα κενά ασφαλείας στα smart contracts θα αναφέρουμε ότι εκατομμύρια δολάρια που κατείχαν ως "assets", κλάπηκαν ή δεσμεύτηκαν από τις διάσημες επιθέσεις μεταξύ των ετών 2016 και 2018 όπως η επίθεση "DAO", η επίθεση πορτοφολιού πολλαπλών σημείων ισοτιμίας κ.α.



Εικόνα 45:Λειτουργία ενός smart contract [17]

Σε ένα αποκεντρωμένο δίκτυο έξυπνων συμβολαίων δεν είναι εύκολο να τροποποιηθούν ή να αναβαθμιστούν, εκτός αν ληφθούν ακραία μέτρα. Η αμετάβλητη φύση των έξυπνων συμβολαίων στο πλαίσιο της τεχνολογίας blockchain έχει πλεονεκτήματα και μειονεκτήματα σχετικά με την ασφάλεια αυτών. Λόγω του ότι η δομή δεδομένων του blockchain είναι αμετάβλητη, οι επιτιθέμενοι δεν μπορούν εύκολα να τροποποιήσουν τα έξυπνα συμβόλαια και μάλιστα αυτό συμβαίνει ακόμα και από του ίδιους τους προγραμματιστές των έξυπνων συμβολαίων. Για την ακρίβεια το μόνο που μπορούν να κάνουν είναι να τερματίσουν την υπάρχουσα σύμβαση και να δημιουργήσουν ένα καινούριο συμβόλαιο από την αρχή. Για τον λόγο αυτό, κατά την δημιουργία τους ελέγχονται διεξοδικά με ένα ευρύ φάσμα δοκιμών για λόγους ασφαλείας.

Μια αξιόλογη δουλειά σχετικά με τις ευπάθειες στα έξυπνα συμβόλαια είναι από τους (Mense & Flatscher, 2018), η οποία αναλύει μερικά από τα τρωτά σημεία, τα περισσότερα από τα οποία έχουν υποστεί την επίθεση. Στο σημείο αυτό, θα πρέπει να αναφέρουμε ότι οι επιθέσεις στα Ethereum smart contracts διαχωρίζονται σε τρία διαφορετικά είδη: i)Solidity, ii)EVM, iii)Blockchain

[17] Ανακτήθηκε από: https://www.wallstreetmojo.com/smart-contracts/

Ο πρώτος λοιπόν διαχωρισμός αφορά την γλώσσα Solidity, η οποία μεταγλωττίζει το πρόγραμμα και χρησιμοποιείται για την υλοποίηση των έξυπνων συμβολαίων Ethereum, τα οποία εκτελούνται στην Ethereum εικονική μηχανή (EVM). Οι πιο σημαντικές ευπάθειες που προκύπτουν είναι οι παρακάτω:

3.1.5.1 Call to the unknown

Αναφέρεται στην χρήση ορισμένων λειτουργιών της γλώσσας (Solidity), όπως στην κλήση συναρτήσεων ή την μεταφορά ether από κάποιο χρήστη σε κάποιον άλλο, η οποία μπορεί να οδηγήσει σε κάποια κακόβουλη συνάρτηση επιστροφής (fallback function). Πιο συγκεκριμένα, η συνάρτηση που προορίζεται να κληθεί (έστω f) δεν υπάρχει και αντί αυτής εκτελείται μια εναλλακτική συνάρτηση. Εξαιτίας αυτής της ευπάθειας, κακόβουλοι χρήστες μπορούν να την εκμεταλλευτούν καλώντας την δική τους ενναλακτική συνάρτηση (Atzei et al., 2017). Αναλυτικότερα, κάποια «primitives» στην Solidity για την συγκεκριμένη επίθεση είναι:

- call: χρησιμοποιείται για να καλέσω μια συνάρτηση ή για την μεταφορά ether μεταξύ των χρηστών από το τρέχων συμβόλαιο σε κάποιο άλλο
- send: χρησιμοποιείται για την μεταφορά αιθέρα από την τρέχουσα σύμβαση σε κάποιο άλλο συμβόλαιο
- delegatecall: χρησιμοποιείται για την κλήση μιας συνάρτησης ή την μεταφορά αιθέρα στο περιβάλλον του καλούντος (Samreen & Alalfi, 2021).
- direct call: (βλέπε εικόνα 46)

```
1 contract Alice{ function ping(uint) { returns (uint); }}
2 contract Bob{ function pong (Alice c) { c.ping (42); }}
```

Εικόνα 46:Call to the unknown[18]

Στο σημείο αυτό, θα αναφέρουμε μια περίπτωση εκμετάλλευσης ευπάθειας “call-to-the-unknown” με την ονομασία επίθεση “Parity multisig wallet”. Ειδικότερα, τον Ιούλιο του 2017 σημειώθηκε μια από τις μεγαλύτερες επιθέσεις όταν κλάπηκαν ethers στο δίκτυο του Ethereum. Ο εισβολέας βρήκε μια ευπάθεια σε έκδοση του πορτοφολιού “Parity Multisig” με αποτέλεσμα την κλοπή περισσότερων από 150000 ethers. Το ευάλωτο

[18] Ανακτήθηκε από: https://arxiv.org/pdf/2105.06974.pdf

πορτοφόλι “Multisig” χωρίστηκε σε 2 συμβόλαια προκειμένου να μειωθεί το μέγεθος κάθε πορτοφολιού και κατ’επέκταση να προκύψει εξοικονόμηση gas. Σε αυτή την περίπτωση, ο εισβολέας στέλνει δύο συναλλαγές για καθένα από τα επηρεαζόμενα συμβόλαια, όπου η πρώτη συναλλαγή αποκτά εξ ολοκλήρου την ιδιοκτησία του πορτοφολιού multisig, ενώ η δεύτερη αφαιρεί μετακινώντας όλα τα κεφάλαια που εμπεριέχονται σε αυτό.

3.1.5.2 Reentracy-DAO attack

Η ουσία της επίθεσης επανεισόδου είναι να προκαλέσει μια κατάσταση “Hijack” στο συμβόλαιο ελέγχοντας την ροή και καταστρέφοντας την ατομικότητα της συναλλαγής. Η συγκεκριμένη επίθεση αξιοποιήθηκε για την δημιουργία της επίθεσης “DAO”, η οποία αποτελεί την μεγαλύτερη επίθεση που πραγματοποιήθηκε ποτέ σε ένα Ethereum Smart Contract. Η επίθεση DAO είχε ως συνέπεια τον σχεδόν υποδιπλασιασμό της τιμή του Ethereum, καθώς επίσης αποτελεί και τον λόγο για τον οποίο το blockchain Ethereum χωρίστηκε μέσω ενός hard fork σε Ethereum και Ethereum Classic, προκειμένου να ανακτηθεί αυτό (το χαμένο) μέρος των κεφαλαίων. Μέσω λοιπόν της δημιουργίας αυτού του “hard fork”, έγινε μια προσπάθεια να επαναφέρει όλα τα αρχεία συναλλαγών και την επιδιόρθωση των τρωτών σημείων του συμβολαίου στη νέα διακλάδωση. Η επίθεση επανεισόδου στο συμβόλαιο DAO είχε ως αποτέλεσμα την δημιουργία κέρδους για τον επιτιθέμενο της τάξεως των 60 εκατομμυρίων δολαρίων. Μια επίθεση επανεισόδου (reentrancy) μπορεί να εξαντλήσει τα νομίσματα ether σε ένα έξυπνο συμβόλαιο, παραβιάζοντας τον κώδικα της σύμβασης. Ένας ορισμός που θα μπορούσαμε να αναφέρουμε για την συγκεκριμένη ευπάθεια είναι ο παρακάτω: οποιαδήποτε αλληλεπίδραση ενός έξυπνου συμβολαίου (έστω Α) με κάποιο άλλο (έστω Β) και οποιαδήποτε συναλλαγή ether δίνει τον έλεγχο σε αυτό το συμβόλαιο, συνεπάγεται ότι το Β μπορεί να καλέσει πίσω στο Α προτού ολοκληρωθεί η αλληλεπίδραση αυτή. Με άλλα λόγια, το συμβόλαιο Β μπορεί να ανακτήσει επιστροφές χρημάτων πολλές φορές μέχρι να εξαντλήσει το υπόλοιπο του συμβολαίου Α (Mense & Flatscher, 2018). Με αυτό τον τρόπο, το έξυπνο συμβόλαιο Β μπορεί να ανακτήσει πολλαπλές επιστροφές χρημάτων και να αδειάσει το υπόλοιπο του έξυπνου συμβολαίου Α.

Πιο συγκεκριμένα, το πρόβλημα επανεισόδου επιτρέπει στον επιτιθέμενο να πραγματοποιεί συνεχόμενες κλήσεις αιτήματος και λήψης κεφαλαίων από το έξυπνο

συμβόλαιο DAO.sol. Σε αυτό ο επιτιθέμενος διατηρεί νομίσματα ethers που έχει αποσύρει (συνάρτηση withdraw), πραγματοποιώντας αίτηση στο συμβόλαιο DAO , πριν κάνει ανανέωση του υπολοίπου του συμβολαίου. Επιπλέον η συνάρτηση "withdraw" του συμβολαίου στόχου DAO.sol, καλείται επαναλαμβανόμενα μέχρι το υπόλοιπο του συμβολαίου να μηδενιστεί.

```
1  // DAO.sol
2  contract DAO {
3      // assign Ethers to an address
4      mapping(address => uint256) public deposit;
5
6      // credit an amount to sender's account
7      function credit(address to) payable {
8          deposit[msg.sender] += msg.value;
9      }
10
11     // get credited amount
12     function getCreditedAmount(address)
           returns (uint) {
13         return deposit[msg.sender];
14     }
15
16     // withdraw fund from contract
17     function withdraw(uint amount) {
18         if (deposit[msg.sender] >= amount) {
19         msg.sender.call.value(amount)();
20         deposit[msg.sender] -= amount; }
21     }
22 }
```

Εικόνα 47:Έξυπνο συμβόλαιο DAO

Στις γραμμές 7-13, οι συμμετέχοντες στέλνουν Ether στην διεύθυνση του συμβολαίου (DAO) και οι πληροφορίες αυτές της αποστολής των Ether αποθηκεύονται ως ποσό πίστωσης ether. Στην συνέχεια το συμβόλαιο του παραλήπτη καλεί την λειτουργία απόσυρσης του DAO για την λήψη κεφαλαίων. Το συμβόλαιο DAO ελέγχει όμως πριν στείλει την συναλλαγή αν έχει συγκεντρωθεί αρκετό ποσό πίστωσης (γραμμή 18) και αφού ισχύει η προϋπόθεση στην συνέχεια ολοκληρώνεται η συναλλαγή ακολουθεί η μείωση του ποσού συναλλαγής λόγω πίστωσης. Αναλυτικότερα, ο επιτιθέμενος ενσωματώνει την συνάρτηση "withdraw" σε μια παρόμοια συνάρτηση του συμβολαίου DAOAttacker.sol, η οποία είναι είδος προεπιλεγμένης συνάρτησης στα έξυπνα συμβόλαια και έχει το χαρακτηριστικό ότι καλείται αυτόματα (Praitheeshan, Pan, Yu, Liu, & Doss, 2020). Όταν ο εισβολέας λαμβάνει ένα ether ποσό, τότε απαιτεί την ενσωμάτωση

συνάρτησης “withdraw”. Έτσι η παραπάνω ρύθμιση επιτρέπει σε ένα εισβολέα να καλέσει την συνάρτηση “withdraw” αναδρομικά και πριν ενημερωθεί το υπόλοιπο του χρήστη. Στην παρακάτω εικόνα έχουμε την σύνδεση του έξυπνου συμβολαίου DAO.sol με το συμβόλαιο του επιτιθέμενου DAOAttacker.sol. Ουσιαστικά τα δύο αυτά διαφορετικά συμβόλαια συνεργάζονται και επικοινωνούν για την υλοποίηση της επίθεσης στέλνοντας το πρώτο συμβόλαιο στο δεύτερο (μετά την υλοποίηση του) ένα ποσό ether. Η μέθοδος που ακολουθεί ο επιτιθέμενος είναι η παρακάτω:

- Ο επιτιθέμενος στέλνει ένα ποσό ethers στο συμβόλαιο DAO, πιστώνοντας το ποσό αυτό στο λογαριασμό του
- Το υπόλοιπο στο λογαριασμό του επιτιθέμενου ενημερώνεται από το έξυπνο συμβόλαιο DAO, ανάλογα με το ποσό που έχει πιστωθεί (βλέπε DAO.sol γραμμή 8)
- Ο επιτιθέμενος στέλνει ένα αίτημα, να αποσύρει το ποσό αυτό και το ποσό ether επιστρέφεται στο συμβόλαιο του επιτιθέμενου (βλέπε 17-21 του συμβολαίου DAO.sol)
- Αφού τα ethers έχουν επιστραφεί στον επιτιθέμενο, στην συνέχεια καλεί την αντίστοιχη ενσωματωμένη συνάρτηση της “withdraw” (απόσυρσης ποσού) στο συμβόλαιο του επιτιθέμενου η οποία όπως αναφέρθηκε καλείται αυτόματα για την συνεχή ανάληψη, ως ενσωματωμένη συνάρτηση της “withdraw” του συμβολαίου DAO.sol (βλέπε DAOAttacker.sol γραμμή 15). Δεδομένου όμως ότι το συμβόλαιο στόχος (DAO.sol) δεν έχει ήδη ενημερώσει το υπόλοιπο του επιτιθέμενου, εκτελείται με επιτυχία η αίτηση απόσυρσης.

Μέσω αυτής της επαναλαμβανόμενης διαδικασίας, ο επιτιθέμενος καταφέρνει να κλέψει όλα τα διαθέσιμα υπόλοιπα από το συμβόλαιο στόχο. Επιπλέον ο επιτιθέμενος κάνει μεταφορά των ethers που έχει συλλέξει στο συμβόλαιο DAOAttacker.sol σε μια προσωπική διεύθυνση λογαριασμού (βλέπε DAOAttacker.sol, γραμμή 20).

```
// DAOAttacker.sol
import 'DAO.sol';
contract DAOAttacker {

    // initialize DAO contract instance
    DAO public dao = DAO(0xDa32C9e....);
    address owner;

    //set contract creator as owner
    constructor(DaoAttacker) public {
        owner = msg.sender;
    }
    //fallback function calls widthraw function
    function() public {
        dao.withdraw(dao.getCreditedAmount(this));
    }

    /*send stolen funds to attacker's address*/
    function stealFunds() payable public{
        owner.transfer(address(this).balance);
    }
}
```

Εικόνα 48:DAOAttacker.sol

Η μέθοδος call (βλέπε DAO.sol, γραμμή 19), αναγκάζει τον επιτιθέμενο να επικαλεστεί την μέθοδο "withdraw" της εφεδρικής αυτοματοποιημένης συνάρτησης του συμβολαίου DAO.sol στο συμβόλαιο του επιτιθέμενου, την συνάρτηση "fallback". Μέσω λοιπόν της επίκλησης της μεθόδου call, ενημερώνεται το διαθέσιμο υπόλοιπο. Ωστόσο υπάρχει το πρόβλημα ότι τα δεδομένα δεν αποθηκεύονται σε πραγματικό χρόνο. Αυτό ακριβώς το πρόβλημα εκμεταλλεύεται ο επιτιθέμενος, την ενδιάμεση δηλαδή κατάσταση του υπολοίπου και των δεδομένων προκειμένου να αντλήσει ιδίον όφελος. Συνεπώς, πρόκειται για ένα προγραμματιστικό σφάλμα στο έξυπνο συμβόλαιο.

3.1.5.3 Gasless Send

Η ευπάθεια "Gasless send" κάνει μια συναλλαγή να αποτύχει αν δεν παρέχεται αρκετό αέριο για μια συγκεκριμένη κλήση. Θα πρέπει να σημειωθεί ότι το μέγιστο όριο αερίου μπορεί να διαφέρει με την πάροδο του χρόνου ανάλογα με τις αμοιβές συναλλαγής. Η ευπάθεια προκύπτει όταν η κατανάλωση ενέργειας, η οποία στην περίπτωση των smart contract αντιστοιχεί σε ποσότητα "gas" το οποίο χρησιμοποιείται για την διεξαγωγή μιας Ethereum συναλλαγής, υπερβαίνει το αναμενόμενο ποσό. Αναλυτικότερα, δεν επιτρέπεται ο καθορισμός της μέγιστης ποσότητας "gas" το οποίο μπορεί να χρησιμοποιηθεί για την εκτέλεση εναλλακτικής "fallback" συνάρτησης στο έξυπνο συμβόλαιο του επιτιθέμενου (Staderini, Palli, & Bondavalli, 2020). Κανονικά όμως το ποσό αυτό "gas" είναι σταθερό

και θα τείνει να εξαντληθεί με ρυθμό ανάλογο του περιεχομένου των οδηγιών της συνάρτησης “fallback” η οποία ουσιαστικά ενεργοποιεί την επίθεση.

3.1.5.4 Keeping Secrets

Τα πεδία στα έξυπνα συμβόλαια μπορεί να είναι δημόσια (αναγνωρίσιμα από χρήστες/συμβόλαια) ή ιδιωτικά. Η δήλωση ενός πεδίου ως ιδιωτικού δεν εγγυάται το απόρρητο του. Αυτό οφείλεται στο γεγονός ότι, για να ορίσετε την αξία ενός πεδίου, οι χρήστες πρέπει να στείλουν μια κατάλληλη συναλλαγή στους επικυρωτές, οι οποίοι δημοσιεύουν στην συνέχεια τις συναλλαγές αυτές στο δίκτυο blockchain και λόγω του ότι αναφερόμαστε σε δημόσια blockchain ο κάθε κόμβος θα μπορεί να επιθεωρήσει τα περιεχόμενα της συναλλαγής για τον σωστό ορισμό της νέας της τιμής. Σε ορισμένες απαιτείται κάποιο πεδίο να είναι μυστικό, προκειμένου να μην αποκαλυφθεί κάποια πληροφορία, χρήσιμη για την επόμενη κίνηση (Atzei et al., 2017). Σε κάποιες περιπτώσεις, για να διασφαλιστεί ότι κάποιο πεδίο θα παραμείνει μυστικό μέχρις ότου συμβεί ένα συγκεκριμένο γεγονός, το έξυπνο συμβόλαιο θα πρέπει να εφαρμόσει συγκεκριμένες κρυπτογραφικές μεθόδους, όπως για παράδειγμα χρονομετρικές δεσμεύσεις.

3.1.5.5 Timestamp Dependency

Ένα έξυπνο συμβόλαιο χρησιμοποιεί την χρονική σήμανση μπλοκ ως αρχική προϋπόθεση για την εκτέλεση ορισμένων κρίσιμων λειτουργιών. Έτσι όταν εξ ορύσσεται ένα μπλοκ, ο ανθρακωρύχος αυτού δημιουργεί την χρονική σήμανση για το μπλοκ. Αν ένας ανθρακωρύχος αφού επιβεβαιωθούν οι συνθήκες εγκυρότητας μέσω του μοντέλου συναίνεσης λάβει ένα νέο μπλοκ, στην συνέχεια πραγματοποιεί έλεγχο, συγκρίνοντας αν η χρονική σήμανση του μπλοκ που έχει λάβει είναι μεταγενέστερη από την χρονική σήμανση του προηγούμενου μπλοκ. Ωστόσο υπάρχει ένα χρονικό εύρος περίπου 900 δευτερολέπτων που δεν μπορεί να ξεπεραστεί μεταξύ της χρονικής σήμανσης της τοπικής μηχανής και την χρονικής σήμανσης κατά την οποία έχει ληφθεί το νέο μπλοκ. Λόγω της ύπαρξης αυτού του χρονικού εύρους στον ορισμό της χρονικής σήμανσης ενός μπλοκ από του ανθρακωρύχους, η εξάρτηση από χρονική σήμανση παρουσιάζει μια κοινή ευπάθεια και ευνοεί ένα κακόβουλο ανθρακωρύχο/επικυρωτή. Εάν ένα συμβόλαιο έχει εφαρμογή στο να ελέγχει κάποια συνθήκη, ένας κακόβουλος ανθρακωρύχος μπορεί να χειριστεί ο ίδιος μια χρονική σήμανση και να την μεταβάλλει με βάση τον στόχο του (Praitheeshan et al., 2020). Για παράδειγμα , εάν ένα έξυπνοι συμβόλαιο χρησιμοποιεί τον τρέχων χρόνο, με βάση τον χρόνο έναρξης και τον χρόνο λήξης στη χρονική σήμανση του μπλοκ,

συνεπάγεται ότι ο ανθρακωρύχος μπορεί να χειριστεί την χρονική σήμανση για μερικά δευτερόλεπτα αλλάζοντας το αποτέλεσμα υπέρ του. Ωστόσο, η συγκεκριμένη ευπάθεια έχει νόημα για τον επιτιθέμενο ανθρακωρύχο, μόνο εφόσον διαθέτει υψηλούς υπολογιστικούς πόρους.

3.1.5.6 External Calls

Οι εξωτερικές κλήσεις μπορούν να εισάγουν αρκετούς κινδύνους καθώς εξωτερικά συμβόλαια μπορούν να εκτελέσουν κακόβουλο κώδικα. Γενικά εξωτερικές κλήσεις ή όπως αλλιώς λέγονται «κλήσεις προς το άγνωστο» πρέπει να αποφεύγονται. Για τον λόγο αυτό, εφόσον υπάρχει «επικοινωνία» μεταξύ εξωτερικών έξυπνων συμβολαίων θα πρέπει να υπάρχουν τα αντίστοιχα προληπτικά μέτρα. Όπως η σήμανση σε μη αξιόπιστα συμβόλαια, αποφεύγοντας αλλαγές κατάστασης μετά από εξωτερικές κλήσεις.

3.1.5.7 Mishandled Exceptions

Υπάρχουν πολλές περιπτώσεις όπου μπορούν να προκύψουν εξαιρέσεις στον προγραμματισμό της Solidity, αλλά όπως είναι αναμενόμενο παίζει ιδιαίτερο ρόλο ο τρόπος με τον οποίο αντιμετωπίζονται. Ο χειρισμός εξαιρέσεων έχει να κάνει με την «επικοινωνία» που έχουν οι συμβάσεις μεταξύ τους (Samreen & Alalfi, 2021). Η επικοινωνία αυτή καθιστά τα συμβόλαια ευάλωτα σε επιθέσεις, επειδή οι προγραμματιστές δεν θα είναι σε θέση να αντιλαμβάνονται αν υπάρχει απώλεια σε νομίσματα “ether” και εφόσον αυτές οι εξαιρέσεις δεν αντιμετωπίζονται σωστά, μπορεί να υπάρξει αντιστροφή συναλλαγών.

```
1 contract Alice {
2 function ping(uint) {
3 // this function throws an exception
4 returns (uint);}}
5 contract Bob {
6    uint x=0;
7    function pong(Alice c){ x=1; c.ping(42); x=2;} }
```

Εικόνα 49:Mishandled Exceptions[19]

[19] Ανακτήθηκε από: https://[19]arxiv.org/pdf/2105.06974.pdf

Στον παραπάνω κώδικα, η τιμή της μεταβλητής x, μετά την εκτέλεση του συμβολαίου του Bob εξαρτάται από την μέθοδο της συνάρτησης call (Η συνάρτηση call είναι μια συνάρτηση χαμηλού επιπέδου για αλληλεπίδραση με άλλα συμβόλαια, ενώ αποτελεί την συνιστάμενη μέθοδο για αποστολή νομισμάτων ether μέσω της κλήσης της "fallback" συνάρτησης). Αν η συνάρτηση ping του έξυπνου συμβολαίου της Αλίκης καλείται χρησιμοποιώντας μια άμεση κλήση, στην συνέχεια η τιμή του ισούται με μηδέν. Επιπλέον, στην περίπτωση των εξαιρέσεων, εάν δεν υπάρχει ορισμένο κάποιο όριο, τότε χάνεται όλο το διαθέσιμο "gas" που απαιτείται για την εκτέλεση του συμβολαίου .

Το «σφάλμα μη επιλεγμένης αποστολής» είναι μέρος του προβλήματος "mishandled exceptions". Αυτή η κατηγορία ευπαθειών στα smart contract αναφέρεται ως «αποστολή αντί για μεταφορά». Αναλυτικότερα, ο όρος «μεταφορά», αναφέρεται στον αυτόματο έλεγχο της επιστρεφόμενης τιμής, ενώ ο όρος «αποστολή» στο γεγονός ότι πρέπει να ελεγχθεί χειροκίνητα η επιστρεφόμενη τιμή, κάνοντας όμως μια εξαίρεση εάν η αποστολή αποτύχει (Dika & Nowostawski, 2018). Εάν δεν μπορεί να γίνει κάτι τέτοιο, είναι πιθανόν κάποιος επιτιθέμενος να εκτελέσει κακόβουλο κώδικα στην σύμβαση. Καταλήγοντας θα μπορούσαμε να πούμε ότι οι συνέπειες της επίθεσης αυτής είναι παρόμοιες με αυτές της "reentrancy" και "call to the unknown".

3.1.5.8 DoS

Το DoS εξηγείται από εργαλείο ανάλυσης κώδικα SmartCheck ως μια κατάσταση στην οποία οι εκφράσεις (if, for, while) εξαρτώνται από μια εξωτερική κλήση. Πιο συγκεκριμένα, ο καλούμενος μπορεί να αποτύχει οριστικά, εμποδίζοντας τον καλούντα (caller) να ολοκληρώσει την εκτέλεση ενός έξυπνου συμβολαίου. Επιπλέον ο εισβολέας μπορεί να προκαλέσει ταλαιπωρία με την παροχή της σύμβασης προσθέτοντας σε αυτή δεδομένα των οποίων είναι δαπανηρή η επεξεργασία, εμποδίζοντας έτσι άλλους να αλληλοεπιδρούν με αυτά (Dika & Nowostawski, 2018). Αυτή η ευπάθεια είναι στενά συνδεδεμένη με την ευπάθεια των εξωτερικών κλήσεων (external calls), ενώ για να αντιμετωπιστεί ένας τέτοιος κίνδυνος, απαιτείται χειρισμός ώστε να βγουν εκτός εξωτερικές κλήσεις καθώς επίσης και να αποφευχθούν καταστάσεις "looping" (for, while,..).

Όταν η ροή του ελέγχου μεταφέρεται σε μια εξωτερική σύμβαση, η εκτέλεση του συμβολαίου του καλούντος (caller) μπορεί να αποτύχει τυχαία ή και μεθοδευμένα, οδηγώντας με αυτό τον τρόπο στο να προκαλέσει μια κατάσταση DoS στο συμβόλαιο

αυτό. Ειδικότερα, το συμβόλαιο του καλούντος μπορεί να βρίσκεται σε κατάσταση DoS όταν μια συναλλαγή επαναφέρεται λόγω αποτυχίας σε μια εξωτερική κλήση ή όταν στο συμβόλαιο του καλούμενου γίνει επαναφορά της συναλλαγής ώστε να διακοπεί η εκτέλεση του συμβολαίου του καλούντος.

Για την καλύτερη κατανόηση, θα δείξουμε μια περίπτωση επίθεσης DoS από εξωτερική κλήση ενός συμβολαίου το οποίο αποτελεί σχήμα Πόντσι. Να σημειωθεί ότι το συγκεκριμένο σχήμα αναφέρεται σε οποιαδήποτε χρηματική απάτη στηρίζεται στην έννοια της πυραμίδας επενδυτών όπου αποτελεί ένα επενδυτικό σχήμα, σύμφωνα με το οποίο επενδυτές πληρώνονται από τα χρήματα που δίνονται από μεταγενέστερους επενδυτές αντί από τα καθαρά κέρδη που συγκεντρώνονται από πραγματικές πωλήσεις (“Denial-of-Service Attack - Wikipedia,” n.d.). Με άλλα λόγια, το συγκεκριμένο συμβόλαιο στέλνει πληρωμές στου δανειστές από κεφάλαια που συλλέγονται μέσω νέων δανειστών. Στην παρακάτω εικόνα κώδικα η συνάρτηση sendPayment() περιέχει την περίπτωση DoS από ευπάθεια εξωτερικής κλήσης. Αναλυτικότερα, το συμβόλαιο του επιτιθέμενου δανείζει κεφάλαια σε αυτό που θέλει να μολύνει (contract HYIP), εξαιρώντας την εναλλακτική συνάρτηση (fallback function). Επιπλέον, όταν η συνάρτηση sendPayment() καλείται να πληρώσει τους δανειστές και η εφεδρική συνάρτηση (fallback) δημιουργεί μια εξαίρεση, προκαλώντας με αυτό τον τρόπο μια σκόπιμη επαναφορά της συναλλαγής και στην συνέχεια επιτυγχάνοντας την επίθεση DoS (Samreen & Alalfi, 2021).

```
1  contract HYIP {
2     Lenders[] private lender;
3     function sendPayment() {
4          for(uint i = lender.length; iâĹŠâĹŠ > 0; ) {
5               uint payment=(lenders[i].amount*/1000;
6               if(!lenders[i].addr.send(payment)) throw;
7               } }}
8  contract AttackerContract {
9     bool private attack = true;
10    function() payable {
11         if (attack) throw;
12         // callee fails the caller execution deliberately
                }
13         }}
```

Εικόνα 50:Επίθεση DoS σε συμβόλαιο μέσω της ευπάθειας εξωτερικής κλήσης[20]

[20] Ανακτήθηκε από: https://arxiv.org/pdf/2105.06974.pdf

3.1.5.9 TX. Origin

Η έννοια “Tx.origin” είναι μια καθολική μεταβλητή που επιστρέφει την διεύθυνση του μηνύματος ανασύροντας την πλήρη αλυσίδα κλήσης, δηλαδή την διεύθυνση της προέλευσης της κλήσης αντί για την διεύθυνση που χρησιμοποιείται για την τρέχουσα κλήση. Πρόκειται για ένα έξυπνο συμβόλαιο θύμα και είναι τύπου “wallet”, ενώ το συμβόλαιο αυτό δεν πρέπει να χρησιμοποιείται για σκοπούς εξουσιοδότησης. Η επίθεση Tx.origin είναι ένα συμβόλαιο που χρησιμοποιείται από ένα επιτιθέμενο. Στο συμβόλαιο αυτό θα οριστεί η διεύθυνση του εισβολέα ως κάτοχο του συμβολαίου, δίνοντας στον εισβολέα πλήρη πρόσβαση στα κεφάλαια που κατέχει το υπό την επιρροή του συμβόλαιο. Ειδικότερα, η απαγόρευση του συγκεκριμένου αυτού συμβολαίου για θέματα εξουσιοδότησης, συμβαίνει επειδή στο συμβόλαιο αυτό ορίζεται ως κύρια διεύθυνση η διεύθυνση του εισβολέα (Dika, n.d.). Με αυτό τον τρόπο γίνεται εφικτή ή άμεση χρήση όλων των κεφαλαίων, αφού ο εισβολέας αποκτά πρόσβαση στα συμβατικά (αλληλοεπιδρώντα) έξυπνα συμβόλαια. Τέλος να τονίσουμε ότι η διαλειτουργικότητα του συγκεκριμένου συμβολαίου (Tx.origin) είναι περιορισμένη, με την έννοια ότι κάποιο άλλο συμβόλαιο με το οποίο θα αλληλοεπιδρά δεν μπορεί να είναι Tx.origin.

3.1.5.10 Ether lost in transfer

Η συγκεκριμένη περίπτωση επίθεσης συμβαίνει όταν αποστέλλονται κάποια ethers σε μια διεύθυνση παραλήπτη που είναι ορφανή, δηλαδή δεν αλληλοεπιδρά με κανένα συμβόλαιο ή χρήστη (Mense & Flatscher, 2018). Έτσι εάν σταλούν ethers σε μια ορφανή διεύθυνση, θα πρέπει προγραμματιστικά να αποφευχθεί ένας τέτοιος κίνδυνος να μην να εξασφαλιστεί με μη αυτόματο τρόπο η ορθότητα των διευθύνσεων των παραληπτών.

Αναλυτικότερα, κατά την αποστολή ether ο χρήστης πρέπει να καθορίσει την διεύθυνση παραλήπτη, η οποία έχει την μορφή μιας ακολουθίας 160 bit. Ωστόσο, πολλές από αυτές τις διευθύνσεις θα είναι όπως έχει ειπωθεί ορφανές, δηλαδή δεν θα σχετίζονται με κανένα χρήστη ή σύμβαση. Έτσι, εάν κατά τύχη ο χρήστης στείλει κάποιο ether σε μια ορφανή διεύθυνση χάνεται για πάντα. Κάτι τέτοιο όμως μπορεί να έχει ιδιαίτερα αρνητικές συνέπειες στο σύστημα γενικώς. Μέχρις στιγμής δεν υπάρχει κανένας τρόπος να ελέγξουμε εάν μια διεύθυνση είναι ορφανή ή όχι. Και επειδή τα χαμένα ether δεν μπορούν να ανακτηθούν είναι απαραίτητο για τους προγραμματιστές ένας μη αυτόματος τρόπος εξακρίβωσης της ορθότητας των διευθύνσεων των παραληπτών.

Όσον αφορά τα ορφανά μπλοκ, πρόκειται για ένα φαινόμενο το οποίο συμβαίνει όταν δύο ανθρακωρύχοι βρίσκουν ένα έγκυρο μπλοκ (έστω μπλοκ Α και μπλοκ Β) και έχουν το χαρακτηριστικό ότι διαδίδουν την ίδια σχεδόν στιγμή το μπλοκ τους στο δίκτυο. Στο σημείο αυτό, με βάση τον κανόνα "longest chain", ο ανθρακωρύχος (μεταξύ αυτών) που θα καταφέρει στην συνέχεια να εξορύξει το επόμενο μπλοκ θα είναι αυτός που θα ενσωματώσει στην αλυσίδα το καινούριο μπλοκ, ενώ ο ανταγωνιστής ανθρακωρύχος θα απορριφθεί τελικά θα από το δίκτυο. Για την ακρίβεια, τα ορφανά μπλοκ είναι έγκυρα και επαληθευμένα, αλλά δεν προστίθενται στην αλυσίδα. Το κρίσιμο σημείο όμως σχετικά με τον κίνδυνο που δημιουργεί η κατάσταση αυτή, είναι το γεγονός ότι στο χρόνο που μεσολαβεί κατά την διαδικασία τελικής επιλογής των συναλλαγών που θα προστεθεί τελικά στην αλυσίδα μπορεί ο επιτιθέμενος να στείλει ether στο ορφανό μπλοκ την στιγμή που έχει προστεθεί αρχικά στην αλυσίδα, αλλά δεδομένου ότι στην συνέχεια θα απορριφθεί να χάσει αναπόφευκτα όλα τα ether.

3.1.5.11 Immutable Bugs

Τα αμετάβλητα σφάλματα (immutable bugs) αναφέρονται σε μια από τις βασικές αρχές του blockchain την αμεταβλητότητα το οποίο αυτό χαρακτηριστικό ισχύει προφανώς και για τα έξυπνα συμβόλαια. Ειδικότερα, μόλις αναπτυχθεί στο blockchain ένα συμβόλαιο δεν μπορεί να τροποποιηθεί, ενώ η εμπιστοσύνη εξασφαλίζεται μέσω της προβλεπόμενης προγραμματιστικής λειτουργίας του συμβολαίου (Atzei et al., 2017). Αυτό όμως το οποίο πρέπει να τονιστεί είναι ότι αν αναπτυχθεί ένα συμβόλαιο το οποίο περιέχει σφάλμα πιθανόν να είναι αδύνατη η διόρθωση του. Η αντιμετώπιση σε αυτή την κατάσταση είναι να υπάρχει πρόβλεψη τροποποίησης κατά την διάρκεια της ανάπτυξης του ή ο οριστικός τερματισμός του συμβολαίου.

Το αμετάβλητο των σφαλμάτων έχει αξιοποιηθεί σε διάφορες επιθέσεις οι οποίες σχετίζονται για παράδειγμα με την κλοπή ether ή για να καταστήσει ether μη εξαργυρώσιμα για κάποιο χρήστη. Να σημειωθεί όμως ότι σε όλες αυτές τις επιθέσεις δεν υπήρχε δυνατότητα άμυνας (Mense & Flatscher, 2018). Ωστόσο στην περίπτωση της πιο γνωστής και σημαντικής επίθεσης που έχει υποστεί ποτέ στο Ethereum, την λεγόμενη "DAO" επίθεση, η αντιμετώπιση που ακολούθησε ήταν η δημιουργία μιας σκληρής διακλάδωσης (hard fork), που ουσιαστικά ακύρωνε τα αποτελέσματα των συναλλαγών που εμπλέκονταν στην επίθεση. Ωστόσο αυτή η λύση δεν ήταν ομόφωνα αποδεκτή από την κοινότητα του Ethereum με αποτέλεσμα την άρνηση της δημιουργίας τελικά (από την

κοινότητα) μιας σκληρής διακλάδωσης. Έτσι αντί αυτού οι ανθρακωρύχοι προέβησαν στην δημιουργία ενός εναλλακτικού blockchain.

3.1.5.12 Unpredictable State

Τα πεδία και οι ισορροπίες καθορίζουν την κατάσταση ενός έξυπνου συμβολαίου. Πιο συγκεκριμένα, όταν ένας χρήστης στέλνει μια συναλλαγή προκειμένου να επικαλεστεί κάποιο έξυπνο συμβόλαιο, δεν μπορεί να είναι σίγουρος ότι η συναλλαγή θα τρέχει στην ίδια κατάσταση που βρισκόταν το συμβόλαιο την στιγμή της αποστολής αυτής της συναλλαγής (Atzei et al., 2017). Κάτι τέτοιο ενδέχεται να συμβεί, διότι ταυτόχρονα άλλη συναλλαγή μπορεί να αλλάξει την κατάσταση των ίδιων συμβολαίων, ενώ επίσης αν κάποιος χρήστης στείλει σε προγενέστερο χρόνο μια συναλλαγή δεν συνεπάγεται ότι η συναλλαγή αυτή θα είναι η πρώτη που θα εκτελέσει ένα έξυπνο συμβόλαιο.

Μια άλλη περίπτωση που καταγράφεται αυτός ο κίνδυνος είναι όταν στη αλυσίδα (blockchain) δημιουργείται μια διακλάδωση, γεγονός το οποίο συμβαίνει για παράδειγμα όταν δύο ανθρακωρύχοι δημιουργούν σχεδόν ταυτόχρονα ένα νέο έγκυρο μπλοκ. Έτσι λοιπόν ορισμένοι ανθρακωρύχοι θα προσπαθήσουν να προσθέσουν ένα μπλοκ στην μια διακλάδωση της αλυσίδας ενώ κάποιοι ανθρακωρύχοι θα κάνουν την ίδια δουλειά στην άλλη διακλάδωση, επικρατώντας στο τέλος μόνο μια από τις διακλαδώσεις. Κατά συνέπεια οι συναλλαγές που ήταν ενταγμένες στα μπλοκ της διακλάδωσης που τελικά απορρίφθηκε θα αγνοηθούν. Το συμπέρασμα είναι ότι η κατάσταση (state) ενός συμβολαίου μπορεί να είναι μεταβλητή. Η παραπάνω συνθήκη όπως είναι λογικό δημιουργεί τρωτά σημεία και δεδομένου ότι κάποιος χρήστης θέλει να δημοσιεύει νέες συναλλαγές στέλνοντας για παράδειγμα κάποια ether σε ένα έξυπνο συμβόλαιο, δεν υπάρχει καμία εγγύηση σε αυτόν αν θα χάσει τα ether αυτά.

3.1.5.13 Creating Randomness

Όταν η εκτέλεση του bytecode EVM είναι ντετερμινιστική (για μια συγκεκριμένη είσοδο, παράγεται πάντα η ίδια έξοδος), συνεπάγεται ότι υπό φυσιολογικές συνθήκες όλοι οι ανθρακωρύχοι που εκτελούν μια συναλλαγή θα έχουν πάντα τα ίδια αποτελέσματα. Στην αντίθετη περίπτωση, όταν η εκτέλεση bytecode EVM είναι μη ντετερμινιστική δημιουργούνται ψευδοτυχαίοι αριθμοί, όπου επιλέγεται η αρχή εκκίνησης μοναδικά από όλους τους ανθρακωρύχους (Atzei et al., 2017). Έτσι ένας κακόβουλος ανθρακωρύχος θα μπορούσε να εκμεταλλευτεί αυτή την ευπάθεια, προσπαθώντας να δημιουργήσει το μπλοκ του με στόχο να επηρεάσει το αποτέλεσμα της ψευδοτυχαίας γεννήτριας για την

δημιουργία τυχαίων αριθμών. Για να μπορέσει όμως κάποιος ανθρακωρύχος ή μια ομάδα (mining pool) να προκαλέσει μια τέτοια κατάσταση θα πρέπει αρχικά να καταφέρει να ελέγξει ένα σημαντικό ποσοστό της συνολικής ισχύς κατακερματισμού του δικτύου και στην συνέχεια να επενδύσει ένα ικανό ποσό Bitcoin (το οποίο αυτό ποσό τείνει να μειώνεται σε σχέση με το αρχικό απαιτούμενο).

3.1.5.14 Low-Level attacks

Εκτός από τις επιθέσεις που σχετίζονται με τον κώδικα συμβολαίων, στόχος κακόβουλων χρηστών έχει γίνει επίσης και το Ethereum δίκτυο. Ειδικότερα, επιθέσεις που εκμεταλλεύονται τα τρωτά σημεία σε επίπεδο προδιαγραφών EVM, καθώς και ελαττώματα ασφαλείας στον πελάτη Ethereum (Atzei et al., 2017). Για παράδειγμα, σε μια περίπτωση επίθεσης “Denial-of-service” επιτυγχάνεται εκμετάλλευση μιας εντολής EVM, του οποίου το κόστος σε μονάδες “gas” ήταν πολύ χαμηλό σε σύγκριση με τους υπολογιστικού πόρους που απαιτήθηκαν για την εκτέλεση του. Αυτό το οποίο θα προσπαθήσει ο επιτιθέμενος από την πλευρά του είναι να δημιουργήσει συνθήκες “flooding” στο δίκτυο, προκαλώντας σημαντική μείωση της υπολογιστική ισχύς καθώς και επιβράδυνση στην διαδικασία συγχρονισμού στο blockchain. Να σημειωθεί ότι το πρόβλημα το οποίο χρήζει αντιμετώπισης στην συγκεκριμένη επίθεση σχετίζεται με την διακλάδωση που δημιουργείται στην αλυσίδα (forking).

Τέλος θα πρέπει να τονίσουμε ότι, τα τρωτά σημεία σε υλοποιήσεις πελατών μπορεί επίσης να είναι η αιτία επιθέσεων. Ιδιαίτερα, με την εκμετάλλευση του αλγορίθμου διάδοσης μπλοκ μπορεί να διαιρεθεί το δίκτυο Ethereum σε μικρές ομάδες κόμβων οι οποίοι έχουν ως σκοπό την δημιουργία “ad-hoc” από τον επιτιθέμενο, μέσω των οποίων εξαναγκάζουν το θύμα να αποδεχθεί (μολυσμένα) μπλοκ.

Πίνακας 5:Κύριες επιθέσεις έξυπνων συμβολαίων

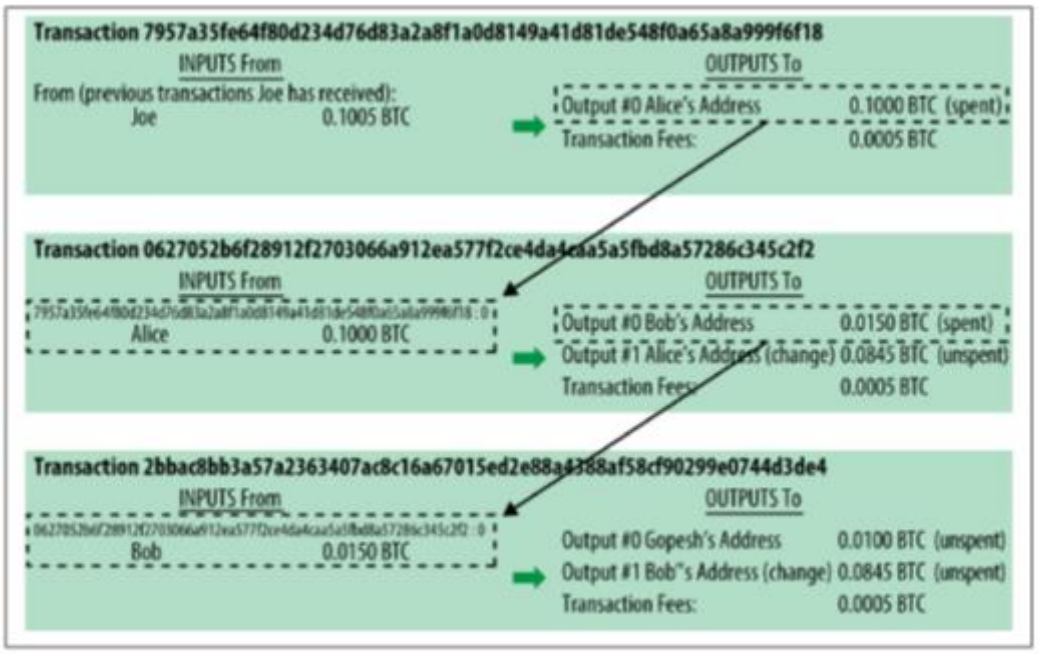
Επίπεδο Μόλυνσης	Αιτία Ευπάθειας	Ευπάθεια
Solidity	Καλείται συνάρτηση η οποία δεν υπάρχει	Call to the Unknown
	Μια μη αναδρομική συνάρτηση εισάγεται ξανά πριν τον τερματισμό	Reentrancy attack-DAO attack
	Καλείται η εναλλακτική συνάρτηση του καλούντος	Gasless send
	Μη εγγύηση απορρήτου	Keeping secrets
	Ευάλωτη επικοινωνία μεταξύ των συμβάσεων-απώλεια ether	Mishandled exceptions
	Εμπόδιο σε “caller” ενός έξυπνου συμβολαίου για την εκτέλεση του	DoS
	Εξουσιοδότηση συμβολαίου	TX. Origin
EVM	Αμεταβλητότητα έξυπνων συμβολαίων	Immutable bugs
	Ορφανή διεύθυνση παραλήπτη	Ether lost in transfer
Blockchain	Αλλοίωση συναλλαγής κατά την αποστολή	Unpredictable Stale
	Μη ντετερμινιστική εκτέλεση κώδικα	Creating randomness
	Ύπαρξη περιορισμένου χρονικού ορίου μεταξύ χρονικής σήμανσης τοπικής μηχανής και χρονικής σήμανσης δημιουργίας νέου μπλοκ	Timestamp dependency

3.2 Κατηγοριοποίηση επιθέσεων με βάση τα blockchain επίπεδα αφαίρεσης

Η Δομή ενός Blockchain όπως έχει αναφερθεί διαχωρίζεται σε επίπεδο εφαρμογής, επίπεδο έξυπνου συμβολαίου, επίπεδο κινήτρων, επίπεδο δικτύου και επίπεδο δεδομένων, ενώ οι στρώσεις των επιπέδων είναι με τη σειρά αυτή από πάνω προς τα κάτω. Παρακάτω θα ακολουθήσει μια ανάλυση των επιπέδων αυτών σε συνάρτηση με την ασφάλεια στο Blockchain, καθώς και μια συσχέτιση τους με υπάρχουσες επιθέσεις.

3.2.1 Επίπεδο δεδομένων

Το επίπεδο δεδομένων αφορά την δομή δεδομένων του blockchain. Το blockchain αποτελεί μια αλυσίδα μπλοκ και κάθε μπλοκ περιέχει μια λίστα έγκυρων συναλλαγών που έχουν καταγραφεί στο καθολικό. Ως βασική μονάδα του blockchain θεωρείται το μπλοκ, όπου κάθε μπλοκ αποτελείται από δύο μέρη, δηλαδή την κεφαλίδα μπλοκ και το σώμα μπλοκ. Η κεφαλίδα μπλοκ αποτελείται από την έκδοση μπλοκ, τον τυχαίο αριθμό, την χρονική σήμανση, τον προηγούμενο κατακερματισμό μπλοκ και την δομή του δέντρου Merkle με τον κατακερματισμό της ρίζας (Sifra & Wu, n.d.). Το υπόλοιπο μέρος (σώμα μπλοκ) περιλαμβάνει τον μετρητή συναλλαγών και το ιστορικό συναλλαγών του μπλοκ. Ένα έγκυρο μπλοκ θα πρέπει να περιέχει προηγούμενο κατακερματισμό μπλοκ ώστε να γίνει η σύνδεση με το προηγούμενο μπλοκ. Με αυτό τον τρόπο, εξασφαλίζεται το χαρακτηριστικό του blockchain της μη αναίρεσης και διαγραφής δεδομένων στο λογιστικό βιβλίο (ledger). Αναλυτικότερα, εντός της κεφαλίδας μπλοκ στο πεδίο “merkle root” διατηρείται η τιμή κατακερματισμού μιας συναλλαγής για την διασφάλιση της ακεραιότητας των συναλλαγών, του αμετάβλητου και της μη αντιστρεψιμότητας.



Εικόνα 51:Μια αλυσίδα συναλλαγών, όπου η έξοδος μιας συναλλαγής ισοδυναμεί με την είσοδο της επόμενης συναλλαγής[21]

Συνεπώς γίνεται αντιληπτό, ότι το πλεονέκτημα στο blockchain της αμεταβλητότητας των δεδομένων μπορεί να μετατραπεί με μειονέκτημα σε περίπτωση όπου κακόβουλες πληροφορίες ενταχθούν στην αλυσίδα των μπλοκ, ενώ τα προβλήματα αυτά οφείλονται κυρίως σε λόγους κρυπτογράφησης των δεδομένων. Αναλυτικότερα, η κρυπτογραφία είναι το κλειδί για την διασφάλιση της ασφάλειας και του απαραβίαστου στο blockchain, ενώ η βάση της συγκεκριμένης τεχνολογίας είναι η κρυπτογραφία.

Οι συναρτήσεις κατακερματισμού αποτελούν κρυπτογραφικά “primitives” στην δομή δεδομένων του blockchain (Singhal, Dhameja, & Panda, 2018). Χρησιμοποιούνται σε πολλά κρυπτογραφικά πρωτόκολλα, όπως είναι και οι ψηφιακές υπογραφές. Η μια οικογένεια συναρτήσεων κατακερματισμού ονομάζεται MD (message digest), ενώ η άλλη ονομάζεται SHA (secure hash algorithm) όπου αποτελείται από 4 αλγορίθμους. Αυτός που μας ενδιαφέρει στην περίπτωση του Blockchain είναι του αλγορίθμου SHA-2 και

[21]https://books.google.gr/books?hl=el&lr=&id=MpwnDwAAQBAJ&oi=fnd&pg=PP1&dq=mastering+bitcoin&ots=wR7mrfw3B2&sig=yeGMrLuQaP-ExgUfl0y7LbJvT_Q&redir_esc=y#v=onepage&q=mastering%20bitcoin&f=false

συγκεκριμένα ο SHA256. Με άλλα λόγια, μια επίθεση που σχετίζεται με το επίπεδο δεδομένων αφορά στην ουσία επιθέσεις στον κρυπτογραφικό αλγόριθμο του blockchain. Συνεπώς επιθέσεις που συσχετίζονται με αυτή την αιτία είναι Vulnerable Signature, Brute force attack, collision attack, length expansion attack, back door attack quantum attack, flawed key generation (Yun et al., 2019). Τέλος, επιθέσεις που σχετίζονται έμμεσα είναι η transaction malleability attack καθώς και της οικογένειας επιθέσεων Hijacking στο πρωτόκολλο BGP (Partition Routing, Delay attack).

3.2.2 Επίπεδο Δικτύου

Οι κόμβοι στο blockchain δίκτυο προσδιορίζονται ως υπολογιστικές συσκευές. Διασυνδέονται με γειτονικούς κόμβους για την δημιουργία ενός δικτύου "peer-to-peer" P2P). Το δίκτυο αυτό είναι ένα αποκεντρωμένο μοντέλο επικοινωνίας και είναι ένας τρόπος διανομής δεδομένων σε ένα δίκτυο. Επιπλέον σε αυτό το μοντέλο δικτύου κάθε μέρος έχει τις ίδιες δυνατότητες και κατ'επέκταση κάθε κόμβος λειτουργεί τόσο ως πελάτης όσο και ως διακομιστής, το οποίο έρχεται σε αντίθεση με το μοντέλο πελάτη/διακομιστή (Sifra & Wu, n.d.). Υπάρχουν διάφορα πρωτόκολλα P2P που μπορούν να διευκολύνουν την διάδοση δεδομένων μεταξύ του αποστολέα και του παραλήπτη. Στην περίπτωση του P2P δικτύου ενός blockchain συστήματος, η ευθύνη αυτού του επιπέδου είναι να διαδώσει τις συναλλαγές και να εκτελέσει νέες συναλλαγές μεταξύ των κόμβων P2P, βρίσκοντας την καλύτερη διαδρομή χωρίς καμία κεντρική διαχείριση. Με άλλα λόγια, δεν υπάρχει το πρόβλημα "single point of failure", αλλά λόγω ακριβώς του ότι δεν υπάρχει κάποιος κεντρικός διακομιστής για να διαχειριστεί κάποια θέματα ασφαλείας όπως πιθανές ενημερώσεις με τον ίδιο τρόπο για όλους τους συμμετέχοντες κόμβους στο δίκτυο. Αυτό το πρόβλημα στα P2P δίκτυα έρχονται να λύσουν τα μοντέλα συναίνεσης ώστε να διασφαλίσουν την ασφάλεια και την σωστή λειτουργία μεταξύ των κόμβων.

Όσον αφορά τις επιθέσεις που σχετίζονται με αυτό το επίπεδο αφαίρεσης, θα πρέπει να σημειωθεί ότι καταλαμβάνουν το μεγαλύτερο ποσοστό των κινδύνων για ένα blockchain σύστημα. Ειδικότερα, επιθέσεις όπως Sybil, και eclipse οι οποίες αφορούν μόνο το συγκεκριμένο επίπεδο, αλλά και άλλες επιθέσεις, BGP hijacking, DDoS, Balance, 51%, Selfish mining, bribery, pool hoping, Time jacking, tampering, block withholding, fork after with holding οι οποίες αφορούν και επηρεάζουν το επίπεδο δικτύου και οι οποίες έχουν αναλυθεί. Ενδεικτικά, θα αναφέρουμε την eclipse (που αφορά αποκλειστικά το

επίπεδο δικτύου) κατά την οποία ένας αντίπαλος διαχειρίζεται όλες τις εισερχόμενες και εξερχόμενες συνδέσεις ενός κόμβου θύματος, δημιουργώντας έτσι πρόβλημα στο blockchain δίκτυο το οποίο με την σειρά του μπορεί να δημιουργήσει νέους κίνδυνους όπως double spending. Από την άλλη μια επίθεση που επηρεάζει το επίπεδο δικτύου είναι η επίθεση routing στην οποία πραγματοποιείται απομόνωση ενός συνόλου κόμβων του δικτύου bitcoin, καθυστερώντας την διάδοση των μπλοκ στο δίκτυο, ενώ μπορεί να δημιουργήσει μια επίθεση DoS ή σπατάλη υπολογιστικών πόρων.

3.2.3 Επίπεδο Συναίνεσης

Τα μοντέλα συναίνεσης αποτελούν αυτό το χαρακτηριστικό του blockchain, το οποίο διαφοροποιεί την συγκεκριμένη τεχνολογία από τις υπόλοιπες P2P τεχνολογίες. Τα μοντέλα που χρησιμοποιούνται στα δημόσια blockchain όπως έχουν αναλυθεί σε προηγούμενο κεφάλαιο είναι τα PoW, PoS και DPoS, στα οποία αντιστοιχούν ορισμένες κοινές επιθέσεις για όλα τα μοντέλα όπως είναι η “Sybil Attack” κατά την οποία έχουμε την δημιουργία ψεύτικων ταυτοτήτων οι οποίες απειλούν την ιδιωτικότητα ενός κόμβου ή επιθέσεις που αφορούν μόνο ένα μηχανισμό συναίνεσης όπως είναι η επίθεση “Bribe” που σχετίζεται με τον PoS μηχανισμό, κατά την οποία ο αντίπαλος δωροδοκεί ανθρακωρύχους για να κάνει ο ίδιος εξόρυξη αντί για αυτούς αυξάνοντας έτσι την πιθανότητα δημιουργίας νέων κινδύνων όπως δημιουργίας επίθεσης “double spending” κατά την οποία ξοδεύονται τα ίδια bitcoin σε διαφορετικές συναλλαγές έχοντας ως συνέπεια να χάνουν τα προϊόντα τους ή την δημιουργία διακλαδώσεων, ενώ μια άλλη συνέπεια που μπορεί να επιφέρει η “Bribe attack” είναι η κατάσταση “Block Withholding” στην οποία βάλλονται ειλικρινείς ανθρακωρύχοι των οποίων σπαταλούνται οι υπολογιστικοί πόροι. Στο σημείο αυτό, θα πρέπει να τονίσουμε ότι επιθέσεις που σχετίζονται μόνο με το συγκεκριμένο επίπεδο αφαίρεσης είναι οι Race , Alternative history και Finney.

Αυτήν την στιγμή ,οι μηχανισμοί συναίνεσης έχουν περιθώρια βελτίωσης, αν και υπάρχουν σημαντικές προτάσεις μηχανισμών όμως που αφορούν τα ιδιωτικά Blockchain όπως είναι το μοντέλο συναίνεσης “Proof of Authority” και κρίνεται σημαντικό να μελετηθεί ένα πιο ασφαλές και γρήγορο μοντέλο που θα περιορίσει την δυνατότητα δημιουργίας ευνοϊκών συνθηκών για επιθέσεις.

3.2.4 Επίπεδο Κινήτρων

Ο σκοπός του συγκεκριμένου επίπεδου αφαίρεσης είναι να παρέχει ορισμένα κίνητρα για την ενθάρρυνση των κόμβων να συμμετέχουν στην επαλήθευση ασφάλειας

του blockchain. Για παράδειγμα, η ασφάλεια του blockchain bitcoin εξαρτάται από την συμμετοχή πολλών κόμβων και ειδικότερα η ασφάλεια του blockchain bitcoin βασίζεται στο μέγεθος της ισχύς κατακερματισμού βάσει της οποίας οι κόμβοι διεκδικούν την επίλυση του προβλήματος "proof of work", το οποίο αυτό μέγεθος (ποσοστό) είναι πολύ δύσκολο να ανταγωνιστεί ένας επιτιθέμενος προκειμένου να παράγει μια μεγαλύτερη ισχύ υπολογισμού (Yun et al., 2019). Η διαδικασία επικύρωσης ενός κόμβου καταναλώνει υπολογιστικούς πόρους. Για τον λόγο αυτό, προκειμένου το blockchain να κινητοποιήσει ένα κόμβο να συμμετάσχει στην διαδικασία, προσφέρει ανταμοιβή (block reward). Ωστόσο, στον μηχανισμό αυτό ανταμοιβής όταν το κόστος λειτουργίας του κόμβου είναι κοντά ή μεγαλύτερο από το εισόδημα, συχνά επιλέγεται από τους κόμβους να μην εργάζονται για αυτό το blockchain, γεγονός το οποίο μπορεί να οδηγήσει σε **προβλήματα κεντροποίησης**.

3.2.5 Επίπεδο Εκτέλεσης

Κάθε σύστημα blockchain χρησιμοποιεί τις δικές του γλώσσες προγραμματισμού με το αντίστοιχο χρόνο εκτέλεσης, μεταγλωττιστή, εικονική μηχανή κ.α. Οι περισσότερες από αυτές τις λειτουργείες διατηρούνται στο επίπεδο εκτέλεσης των συστημάτων blockchain (Dinh et al., 2017). Έτσι, όταν ένα συμβόλαιο εκτελείται σε "runtime" περιβάλλον υπάρχουν δύο απαιτήσεις. Η αρχική είναι ότι πρέπει να είναι γρήγορο γιατί υπάρχουν πολλά συμβόλαια και συναλλαγές σε ένα μπλοκ και φυσικά να είναι επαληθεύσιμα (τα μπλοκ) από του κόμβους, ενώ η δεύτερη απαίτηση είναι ότι η εκτέλεση πρέπει να είναι ντετερμινιστική προκειμένου να αποτρέπονται ατυχείς καταστάσεις εισόδου και εξόδου της συναλλαγής, οι οποίες ενδέχεται να προκαλέσουν ακυρώσεις μπλοκ και κατ'επέκταση μη εκμεταλλεύσιμη κατανάλωση ισχύς κατακερματισμού.

Όπως έχει ειπωθεί προηγούμενα, ένα έξυπνο συμβόλαιο είναι κάτι περισσότερο από ένα απλό πρόγραμμα το οποίο μπορεί να εκτελεστεί αυτόματα. Ειδικότερα, πρόκειται για ένα πρόγραμμα που μπορεί να λάβει και να αποθηκεύσει αξία καθώς επίσης να ανταποκριθεί σε ένα ληφθέν μήνυμα ή να στείλει πληροφορίες (Yun et al., 2019). Συνεπώς οι επιθέσεις που σχετίζονται με το επίπεδο εκτέλεσης αφορούν τις επιθέσεις σε smart contract (κάθε τύπου), οι οποίες έχουν αναλυθεί σε προηγούμενο κεφάλαιο. Ενδεικτικά, θα αναφερθούμε σε κάποιες από αυτές:

- Timestamp Dependency: Ένας επιτιθέμενος μπορεί να κατασκευάσει την δική του συναλλαγή βασισμένη σε εκκρεμείς συναλλαγές με στόχο να εισάγει την συναλλαγή σε προγενέστερο χρόνο σε σχέση με τους ανταγωνιστές κόμβους.
- DoS από εξωτερικά συμβόλαια: Αυτή η ευπάθεια προκύπτει από την εξάρτηση των δηλώσεων υπό όρους από εξωτερικές κλήσεις, δεδομένου ότι η συνθήκη να συνεχιστεί η εκτέλεση μπορεί να μην ικανοποιηθεί ποτέ.
- Call to the unknown: Κάποια "primitives" (π.χ call, delegate call, send) στην γλώσσα Solidity για την επίκληση κάποιας συνάρτησης και την μεταφορά ether, έχουν την «παρενέργεια» της επίκλησης της εφεδρικής λειτουργίας του καλούντος (Calle)/παραλήπτη (Staderini et al., 2020). Το γεγονός αυτό μπορεί να οδηγήσει σε απροσδόκητες συμπεριφορές, λόγω της εκτέλεσης εξωτερικού τμήματος κώδικα. Για τον λόγο αυτό, στόχος είναι ο μετριασμός στο δυνατό βαθμό των εξωτερικών κλήσεων. Αξίζει να σημειωθεί μια ακόμη ευπάθεια που αποτελεί υποσύνολο της με την ονομασία "Delegatecall to the untrusted Calle". Ειδικότερα, η "delegate call" (primitive), δημιουργεί μια κλήση μηνύματος που εκτελεί τον κώδικα στην διεύθυνση στόχο στο πλαίσιο της κλήσης ενός συμβολαίου.

Μόλις αναπτυχθεί ένα έξυπνο συμβόλαιο σε ένα κατανεμημένο και αποκεντρωμένο δίκτυο, γίνεται αντιληπτό με βάση τα χαρακτηριστικά που έχει μια τέτοια δομή ότι είναι πολύ δύσκολο να τροποποιηθεί. Ωστόσο, όταν το blockchain αντιμετωπίζει μια επίθεση το πλεονέκτημα της δομής του μπορεί κάποιες φορές να γίνει μειονέκτημα, με την έννοια ότι λόγω των χαρακτηριστικών της τεχνολογίας αυτής όπως είναι η αμεταβλητότητα είναι πολύ δύσκολο να αντιστραφεί οποιαδήποτε κακόβουλη ενέργεια επί του κατανεμημένου ψηφιακού καταλόγου (ledger). Επομένως, προτείνεται η πρόληψη στον κώδικα των έξυπνων συμβολαίων, διεξάγοντας ένα σύνολο δοκιμών ασφαλείας πριν εκδοθεί για τον περιορισμό τυχών τρωτών σημείων.

3.2.6 Επίπεδο Εφαρμογής

Το επίπεδο εφαρμογής είναι ένα επίπεδο που επιτρέπει τον "end user" να χρησιμοποιήσει το σύστημα. Ειδικότερα, επιτρέπει την αλληλεπίδραση μεταξύ του χρήστη και του συστήματος blockchain. Τα Blockchain πορτοφόλια επιτρέπουν στους χρήστες να αποθηκεύουν, να μεταφέρουν και να διαχειρίζονται των νομίσματα τους. Και για να λειτουργήσει ένα τέτοιο πορτοφόλι απαιτείται από τον χρήστη να είναι

εγγεγραμμένος σε κάποιο ανταλλακτήριο, αφού οι πελάτες δεν μπορούν να επικοινωνούν κατευθείαν με την εφαρμογή του πορτοφολιού. Για τον λόγο αυτό υπάρχει η ανάγκη του επιπέδου εφαρμογής για να καλύψει το κενό αυτό, όπως ακριβώς ένα πρόγραμμα περιήγησης στο διαδίκτυο που παρέχει την διεπαφή για την επικοινωνία με τον χρήστη. Έτσι για παράδειγμα, όσον αφορά το επίπεδο εφαρμογής περιλαμβάνει περιπτώσεις χρήσης στην εφαρμογή της τεχνολογίας με τα γνωστά ιδιαίτερα χαρακτηριστικά που διαθέτει (διαφάνεια, αμετάβλητη βάση δεδομένων κ.α). Η ασφάλεια του επιπέδου εφαρμογής καλύπτει κυρίως τα θέματα ασφαλείας κεντρικών κόμβων όπως είναι οι ανταλλαγές που περιλαμβάνουν μετασχηματισμό ψηφιακών νομισμάτων και διαχείριση μεγάλων ποσών. Αυτοί οι κόμβοι μπορεί να βρίσκονται σε οποιοδήποτε σημείο αποτυχίας (point of failure) εντός του δικτύου blockchain. Επιπλέον αυτό που αξίζει να σημειωθεί είναι ότι η απόδοση επίθεσης είναι υψηλή, ενώ παράλληλα το κόστος χαμηλό, δεδομένα που φαίνονται ευνοϊκά για έναν επιτιθέμενο. Μερικά παραδείγματα προβλημάτων σε αυτό το επίπεδο αφαίρεσης του blockchain είναι τα παρακάτω:

Μη εξουσιοδοτημένη πρόσβαση σε διακομιστή ανταλλαγής. Στα ανταλλακτήρια συχνά καταθέτονται μεγάλες ποσότητες χρηματικών ποσών που αναμενόμενα αποτελούν στόχο. Μόλις ο διακομιστής ανταλλακτηρίου αποκτήσει εξουσιοδότηση και με αυτό τον τρόπο μπορέσει να τροποποιηθεί το κλειδί (ιδιωτικό) ενός χρήστη, τότε ο επιτιθέμενος θα είναι σε θέση να κλέψει χρηματικά ποσά από το πορτοφόλι του χρήστη στο ανταλλακτήριο στο οποίο είναι εγγεγραμμένος, προκαλώντας έτσι ανεπανόρθωτο πλήγμα στη αξιοπιστία ενός ανταλλακτηρίου (Yun et al., 2019). Το πλήγμα αυτό όπως αναφέραμε, μεταφέρεται στο πορτοφόλι του χρήστη στο οποίο είναι αποθηκευμένο το ιδιωτικό κλειδί. Ένα τέτοιο παράδειγμα κλοπιμαίων από ανταλλακτήριο ήταν σε αυτό του "Yapizon" τον Απρίλιο του 2017, όπου υπήρχαν κλοπές σε 4 πορτοφόλια του ανταλλακτηρίου και εξαφανίστηκαν 3,816 bitcoin, ποσό που κάλυπτε το 36% των κεφαλαίων του ανταλλακτηρίου. Συνεπώς θα μπορούσαμε να πούμε ότι επιθέσεις που ανήκουν στην ευρύτερη κατηγορία των "wallet attacks" όπως για παράδειγμα η επίθεση "**Vulnerable Signature**", "**key leakage attack**" που σχετίζονται με την αυθεντικοποίηση του συστήματος στο blockchain, αφορούν το συγκεκριμένο επίπεδο αφαίρεσης. Όσον αφορά την τελευταία επίθεση (leakage attack), θα πρέπει να αναφέρουμε ότι όλες οι αξίες συναλλαγής καθώς και οι υπολειπόμενες σε ένα λογαριασμό ενός χρήστη που αντιστοιχεί στο δημόσιο κλειδί του το οποίο θα είναι ορατό σε όλους τους υπόλοιπους χρήστες. Με άλλα λόγια οι πληροφορίες ενός χρήστη θα είναι «κατασκευαστικά» ορατές στους υπόλοιπους με την μορφή ωστόσο ενός

ψευδωνύμου. Ως προέκταση αυτού του χαρακτηριστικού, προκύπτει ο «χώρος» για ένα επιτιθέμενο να προσπαθήσει να συσχετίσει το ψευδώνυμο του χρήστη (Bitcoin Wallet) με την διεύθυνση IP του κεντρικού υπολογιστή που δημιουργεί την συναλλαγή (Conti et al., 2018). Η επίθεση αυτή γνωστή ως "**Deanonymization**" δεν αφορά άμεσα το "application layer", αλλά προκύπτει εξαιτίας των χαρακτηριστικών αυτού. Ακόμη, οι (Goldfeder, Gennaro, & Kalodner, n.d.) αναλύουν την κακή τυχαιότητα της δημιουργίας κλειδιών στον αλγόριθμο ελλειπτικής καμπύλης (ecdsa) που εφαρμόζεται για την υπογραφή και επικύρωση των συναλλαγών. Αναδεικνύεται λοιπόν το ενδεχόμενο , της ελλιπούς υπογραφής που προκαλεί τον κίνδυνο παραβίασης του ιδιωτικού κλειδιού (Vulnerable Signature).

Επιπλέον μια επίθεση που βασίζεται στην αδυναμία ενός εμπόρου να ελέγξει αν η διεύθυνση επιστροφής χρημάτων προέρχεται από τον ίδιο τον πελάτη που εξουσιοδότησε την πληρωμή και θα μπορούσαμε να εντάξουμε στο επίπεδο αφαίρεσης "application" στο blockchain είναι η επίθεση επιστροφής χρημάτων (**refund attack**).

Exchange DDoS. Λόγω της μεγάλης απαίτησης εύρους ζώνης στις πλατφόρμες trading, μια επίθεση DDoS θα αποτελούσε ένα πολύ σοβαρό πλήγμα για την πλατφόρμα. Έτσι, εάν η πλατφόρμα συναλλαγών δεχθεί μια τέτοια επίθεση, οι αρνητικές επιπτώσεις δεν θα περιοριστούν μόνο σε αυτή, αλλά κυρίως θα περιοριστεί ο όγκος συναλλαγών του εκάστοτε νομίσματος blockchain, γεγονός που θα επηρεάσει έμμεσα την τιμή του νομίσματος. Όπως έχει αναφερθεί και προηγούμενα στην εργασία το Bitcoin αποτελεί μια βιομηχανία η οποία έχει δείξει ιδιαίτερη ευαλωτότητα σε DDoS επιθέσεις με πιο γνωστό παράδειγμα την επίθεση στο ανταλλακτήριο Bitfinex στο οποίο οι υπηρεσίες του διακόπηκαν για χρονικό διάστημα ενός μήνα το 2017. Μια από τις επιθέσεις που σχετίζονται με προβλήματα DDoS στο bitcoin και γενικότερα την εφαρμογή του bitcoin είναι αυτή της "**transaction malleability**", κατά την οποία μπορεί να μην τροποποιούνται διευθύνσεις προέλευσης ή προορισμού μιας συναλλαγής , αλλά μπορεί να υπάρχουν αλλαγές στα στοιχεία της συναλλαγής και κατ' επέκταση στο αναγνωριστικό της. Αναλυτικότερα, η επίθεση αυτή συσχετίζεται πλήρως με την επίθεση του ανταλλακτηρίου Mt.Gox του 2011. Σε αυτή την περίπτωση ο διακομιστής του δεν παραβιάστηκε αλλά ο επιτιθέμενος απέκτησε πρόσβαση σε ένα υπολογιστή που χρησιμοποιήθηκε από κάποιο "auditor" του ανταλλακτηρίου από το οποίο έλαβε ένα αρχείο βάσης δεδομένων με ευαίσθητες πληροφορίες καθώς και κρυπτογραφημένες. Έπειτα ο επιτιθέμενος έχοντας στην κατοχή του τις πληροφορίες αυτές, έσπασε το κωδικό πρόσβασης ενός από τους

μεγαλύτερους λογαριασμούς και πούλησε ένα μεγάλο ποσό, που ευτυχώς λόγω ορισμένων ορίων χρηματικής μεταφοράς από την εφαρμογή η ζημιά ήταν περιορισμένη.

Μόλυνση από κακόβουλο πρόγραμμα. Αν υπάρχει εμφύτευση ενός κακόβουλου προγράμματος σε ένα ανταλλακτήριο, γίνεται εφικτή η διαρροή ευαίσθητων πληροφοριών με αποκορύφωμα το ιδιωτικό κλειδί ενός πορτοφολιού, γεγονός το οποίο οδηγεί αναπόφευκτα στην απώλεια του ελέγχου όλων των περιουσιακών στοιχείων ενός χρήστη. Στην περίπτωση του ανταλλακτηρίου Mt.Gox για παράδειγμα, το αρχείο κλειδιού του Mt.Gox αποθηκεύτηκε καθαρά (μη κρυπτογραφημένο) και ο φάκελος του κλειδιού διέρρευσε λόγω μόλυνσης Trojan. Ένα αξιοσημείωτο γεγονός ως προς την μεθοδολογία που ακολούθησε ο επιτιθέμενος ήταν το γεγονός ότι μετέφερε σταδιακά περιουσιακά στοιχεία με στόχο να αποτραπεί η ανάκτηση της ζημιάς μέσω “hard forks”. Η παραπάνω αδυναμία σήμανε για πρώτη φορά την ανάγκη της παρακολούθησης συναλλαγών για τυχόν ανωμαλίες όχι μόνο για βραχυπρόθεσμη δραστηριότητα, αλλά και για πιο μακροπρόθεσμη.

Αντίστοιχα για το Blockchain 2.0, μια επίθεση που σχετίζεται με μόλυνση από κακόβουλο κώδικα είναι η επίθεση DAO (Yun et al., 2019). Πιο συγκεκριμένα, έχουμε την επίθεση **Reentrancy** κατά την οποία η εκτέλεση ενός έξυπνου συμβολαίου μπορεί να διακοπεί στην μέση με την εισαγωγή ενός άλλου συμβολαίου για εκτέλεση, με την ολοκλήρωση και των δύο εξ ’αυτών χωρίς σφάλματα. Ο επιτιθέμενος όμως, χρησιμοποιεί την ενδιάμεσή κατάσταση για την πραγματοποίηση των επαναλαμβανόμενων κλήσεων στο έξυπνο συμβόλαιο. Αυτή η επίθεση, εκμεταλλεύεται την ευπάθεια επανεισόδου από δημοσίευση ενός κακόβουλου συμβολαίου η οποία έχει μια συνάρτηση “withdraw” σε ένα συμβόλαιο DAO η οποία καλείται επαναλαμβανόμενα μέσω της συνάρτησης “callback”, έχοντας ως στόχο μέσω αυτών των επανακλήσεων τον μηδενισμό του υπολοίπου στο smart contract.

Όσον αφορά το θέμα της αρχικής προσφοράς νομισμάτων (ICO), πρόκειται για τα χρήματα που πρέπει να συγκεντρώσει μια εταιρία για να δημιουργήσει ένα νέο νόμισμα ή μια εφαρμογή έχοντας ως χρηματικό σημείο εκκίνησης ένα “ICO” ως τρόπο συγκέντρωσης κεφαλαίων. Μόλις το “ICO” συγκεντρώσει κεφάλαια, αναρτά την διεύθυνση παραλαβής στην επίσημη ιστοσελίδα της εφαρμογής και τότε ο εκάστοτε επενδυτής θα μπορεί να μεταφέρει τα αντίστοιχα χρήματα σε αυτή την διεύθυνση για να αποκτήσει τα αντίστοιχα Tokens. Συνεπώς, επιτιθέμενοι στοχεύουν στην παραβίαση της διεύθυνσης αυτής, όπως είναι επίθεση **“Hijacking”** ή πιο απλά μέσω κοινωνικής

μηχανικής (Yun et al., 2019). Στο σημείο αυτό, θα αναφέρουμε την επίθεση **"Phishing attack"** όπου ο επιτιθέμενος κάνει χρήση της κοινωνικής μηχανικής με σκοπό να μιμηθεί την επίσημη ιστοσελίδα, κάνοντας τον χρήστη εν αγνοία του να μεταφέρει χρήματα στην διεύθυνση πορτοφολιού του εισβολέα.

Στον τομέα της εξόρυξης και συγκεκριμένα τις «πισίνες εξόρυξης», θα συσχετίσουμε με το Application Layer την επίθεση **"Selfish Mining",** κατά την οποία μια κακόβουλη ομάδα εξόρυξης αποφασίζει να μην ελευθερώσει ένα μπλοκ στην υπάρχουσα αλυσίδα, δημιουργώντας την διακλάδωση**.** Στην συνέχεια όταν η διακλάδωση ξεπεράσει σε μήκος την αρχική αλυσίδα σε μπλοκ θα έχει ως αποτέλεσμα την απόρριψη/διαγραφή της αρχικής.

Καταλήγοντας, είναι αδύνατο να αποτραπούν διάφορες επιθέσεις στο επίπεδο εφαρμογής. Για τον λόγο αυτό το βάρος πέφτει στους προγραμματιστές εφαρμογών, όπου θα πρέπει να διασφαλίσουν ότι τα προϊόντα τους δεν έχουν ευπάθειες. Από την πλευρά του χρήστη, οφείλει να προστατέψει το λογαριασμό του στο ανταλλακτήριο της επιλογής του με το να μην χάσει το ιδιωτικό κλειδί του πορτοφολιού του.

Πίνακας 6:Κατηγοριοποίηση επιθέσεων ανά επίπεδο αφαίρεσης σε Blockchain

	Blockchain Abstract Layers					
Threat	*Application Layer*	*Execution Layer*	*Incentive Layer*	*Consensus Layer*	*Network Layer*	*Data Layer*
Vulnerable Signature	✓	✗	✗	✗	✗	✓

	Blockchain Abstract Layers					
Threat	*Application Layer*	*Execution Layer*	*Incentive Layer*	*Consensus Layer*	*Network Layer*	*Data Layer*
Vulnerabilities in Solidity [22]	✗	✓	✗	✗	✗	✗
Key leakage attack	✓	✗	✗	✗	✗	✗
Selfish mining	✓	✗	✓	✓	✓	✗
Sybil attack	✗	✗	✗	✗	✓	✗
Block withholding attack	✗	✗	✓	✓	✓	✗
Vector 76	✗	✗	✗	✓	✗	✗
Eclipse attack	✗	✗	✗	✗	✓	✗
Brute force attack	✗	✗	✗	✗	✗	✓
Deanonymization	✓	✗	✗	✗	✗	✗
Alternative History	✗	✗	✗	✓	✗	✗

[22] Call to the unknown, DAO attack, Gasless send, keeping secrets, Mishandled exceptions, DoS, and Tx Origin

	Blockchain Abstract Layers					
Threat	*Application Layer*	*Execution Layer*	*Incentive Layer*	*Consensus Layer*	*Network Layer*	*Data Layer*
Hijacking	✓	✗	✗	✗	✓	✗
Collision attack	✗	✗	✗	✗	✗	✓
Refund attack	✓	✗	✓	✓	✗	✗
Bribery	✗	✗	✓	✓	✓	✗
51% attack	✗	✗	✗	✓	✓	✗
DDoS	✓	✗	✓	✗	✓	✗
Length expansion attack	✗	✗	✗	✗	✗	✓
Pool Hoping attack	✗	✗	✗	✓	✓	✗
Delay attack	✗	✗	✗	✗	✗	✓
Balance attack	✗	✗	✗	✗	✓	✗
Back Door attack	✗	✗	✗	✗	✗	✓
Transaction Malleability	✓	✗	✗	✗	✗	✓
Quantum attack	✗	✗	✗	✗	✗	✓
Reentrancy attack	✓	✗	✗	✗	✗	✗

	Blockchain Abstract Layers					
Threat	*Application Layer*	*Execution Layer*	*Incentive Layer*	*Consensus Layer*	*Network Layer*	*Data Layer*
Flawed key generation	✗	✗	✗	✗	✗	✓
Finney attack	✗	✗	✗	✓	✗	✗
Portioning Routing	✗	✗	✗	✗	✗	✓
Timejacking	✗	✗	✗	✓	✓	✓
Delay attack	✗	✗	✗	✗	✗	✓
Fork after withholding attack	✗	✗	✗	✓	✗	✗
BGP routing	✗	✗	✗	✗	✓	✗
reentrancy	✗	✓	✗	✗	✗	✗
Block withholding	✗	✗	✓	✓	✗	✗
Private key	✓	✗	✗	✗	✗	✓

3.3 Κατηγοριοποίηση επιθέσεων με βάση το μοντέλο ομοφωνίας

Σε αυτό το κεφάλαιο συζητάμε τα τρία μοντέλα συναίνεσης που χρησιμοποιούνται στο δημόσιο blockchain και τις αδυναμίες τους, καθώς επίσης γίνεται και μια κατηγοριοποίηση επιθέσεων.

3.3.1 Βασικά χαρακτηριστικά και αδυναμίες μοντέλου συναίνεσης “Proof of work” (PoW)

Το PoW μοντέλο συναίνεσης θεωρεί ότι οι μισοί κόμβοι δικτύου είναι πάντα ειλικρινείς ανθρακωρύχοι. Με αυτήν την έννοια , η απόκτηση εξορυκτικής ισχύς για κάποιο κόμβο ή “mining pool” είναι περισσότερο από το ήμισυ της ισχύς κατακερματισμού που υπάρχει στο blockchain δίκτυο, η συναίνεση αυτή γίνεται ευάλωτη.

3.3.1.1 Μειονεκτήματα

Ένα από τα σημαντικότερα μειονεκτήματα του μοντέλου αυτού είναι η κατανάλωση ηλεκτρικής ενέργειας και η σπατάλη υπολογιστικών πόρων, καθώς κατά την εφαρμογή του όλοι οι κόμβοι εξόρυξης προσπαθούν να δώσουν μια λύση στο δύσκολο κρυπτογραφικό πρόβλημα κατά την διαδικασία της εξόρυξης (Kaur et al., 2021). Έρευνες έχουν δείξει ότι η κατανάλωση ρεύματος στην διαδικασία εξόρυξης bitcoin είναι περισσότερη από την κατανάλωση που έχουν πάνω από 160 χώρες. Λαμβάνοντας ακόμη υπόψη ότι η τιμή της ηλεκτρική ενέργειας διαφέρει ανά την υφήλιο, γίνεται αντιληπτό ότι μόνο συγκεκριμένες περιοχές πλεονεκτούν και η έντονη δραστηριοποίηση ισχυρών “miming pools” επιτυγχάνεται μόνο σε αυτές. Έτσι λοιπόν ο ρυθμός κατακερματισμού συγκεντρώνεται σε περιοχές που έχουν φτηνό ηλεκτρικό ρεύμα. Με αυτή την έννοια υπάρχει απειλή στο δίκτυο αφού συγκεκριμένα μόνο “mining pools” τείνουν να ελέγχουν την διαδικασία. Η διαδικασία εξόρυξης του PoW είναι συγκριτικά αργή σε σύγκριση με αυτή άλλων πρωτοκόλλων συναίνεσης. Λαμβάνοντας ακόμη υπόψη ότι μερικά “mining pools” διαθέτουν μεγάλη ισχύ κατακερματισμού και υπερπλεονεκτούν έναντι άλλων, έχουν την δυνατότητα να δημιουργούν σοβαρές διακοπές στο δίκτυο bitcoin.

3.3.1.2 Προβλήματα ασφαλείας επιθέσεις που αντιμετωπίζει το Μοντέλο συναίνεσης “Proof of Work”

Ως προς τις αδυναμίες του συγκεκριμένου μοντέλου μπορεί να υπάρχει η πιθανότητα να παραχθούν την ίδια στιγμή διαφορετικά έγκυρα μπλοκ. Σε μια τέτοια περίπτωση έχουμε την δημιουργία μιας διακλάδωσης στην αλυσίδα, αλλά είναι ανέφικτη η δημιουργία ενός νέου επόμενου μπλοκ ταυτόχρονα από τις διαφορετικές αλυσίδες της διακλάδωσης (Kaur et al., 2021). Η αλυσίδα που γίνεται τελικά δεκτή είναι αυτή που θα

μπορέσει να διατηρήσει πρώτη τουλάχιστον 6 νέα μπλοκ, έτσι ώστε να είναι αυτή που θα εγκριθεί από το δίκτυο.

Η πιο γνωστή επίθεση που επισκιάζει λοιπόν το συγκεκριμένο μοντέλο συναίνεσης είναι η επίθεση 51%. Αλλά και επιθέσεις που σχετίζονται με το επίπεδο δικτύου όπως η DDoS, BGB Hijacking ή η Eclipse επιδεικνύουν ιδιαίτερη ευαλωτότητα στο συγκεκριμένο μοντέλο συναίνεσης. Οι δεξαμενές εξόρυξης AntPool, Nicehash, GHash.io είναι μερικές από τις δεξαμενές εξόρυξης που έχουν υποστεί ζημίες από επιθέσεις DDoS ("Bitcoin Mining Pools Targeted in Wave of DDOS Attacks," n.d.). Επιπλέον, βασικές επιθέσεις που αφορούν το μοντέλο PoW είναι η επίθεσης διπλής δαπάνης, όπου αποτελεί θεμελιώδης πρόβλημα του πρωτοκόλλου blockchain, η επίθεση "Finney" όπου αποτελεί και αυτή μια παραλλαγή της "double spending", στην οποία (Finney) πραγματοποιεί μια κρυφή εξόρυξη μπλοκ και το διαδίδει με απώτερο σκοπό την επίτευξη διπλής δαπάνης. Τέλος, θα αναφέρουμε και την brute force attack, η οποία αποτελεί μια αναβαθμισμένη μορφή της Finney.

3.3.2 Βασικά χαρακτηριστικά και αδυναμίες του μοντέλου συναίνεσης "Proof of Stake" (PoS)

Το μοντέλο συναίνεσης είναι ευάλωτο εξαιτίας ορισμένων ιδιοτήτων κεντροποίησης με τις οποίες λειτουργεί. Επιπλέον , όπως έχει ειπωθεί το PoS είναι ένας συναινετικός μηχανισμός που εξουσιοδοτεί μπλοκ με βάση τα πονταρίσματα (Staking) με τα οποία ένας συμμετέχων εισέρχεται στο δίκτυο. Συνεπώς οι ανθρακωρύχοι που έχουν στην κατοχή τους μεγάλο αριθμό νομισμάτων κατέχουν περισσότερα δύναμη «επικύρωσης» προκειμένου να γίνουν επικυρωτές μπλοκ και να ενισχύσουν το δίκτυο. Ο πιο γρήγορος και ευκολότερος τρόπος για να ξεκινήσετε το ποντάρισμα Ethereum είναι οι κεντροποιημένες συναλλαγές ("How Does Ethereum Staking Work?," n.d.). Ειδικότερα, τα ανταλλακτήρια Binance και Coinbase προσφέρουν στον χρήστη "Ethereum Staking", χωρίς περιορισμό κατώτατου ορίου.

3.3.2.1 Μειονεκτήματα

Στο μοντέλο "Proof of Stake" το δίκτυο επηρεάζεται αναπόφευκτα από κόμβους που κατέχουν μεγαλύτερο ποσοστό νομισμάτων. Ακόμη η βιωσιμότητα του είναι αμφισβητήσιμη, καθώς σε καμία από τις πιο γνωστές εφαρμογές του blockchain (Bitcoin,

Ethereum) δεν εφαρμόζεται αυτό το μοντέλο. Τέλος, δεν είναι εφικτή η ύπαρξή «κρύου» πορτοφολιού (το πορτοφόλι στο οποίο μπορεί να γίνει αποθήκευση των ιδιωτικών κλειδιών σε "offline" περιβάλλον), αφού είναι απαραίτητος ο συγχρονισμός των πορτοφολιών τους ως προς την απόδειξη της ιδιοκτησίας τους.

3.3.2.2 Προβλήματα ασφάλειας και επιθέσεις που αντιμετωπίζει το Μοντέλο συναίνεσης "Proof of Stake"

Όσο αναφορά στις αδυναμίες των κρυπτονομισμάτων που βασίζονται στον υπολογισμό του "coinage", ένας εισβολέας θα μπορούσε να επηρεάσει την τιμή της ηλικίας με στόχο να αυξήσει την ισχύ του ως κόμβος στο δίκτυο. Σε μια κακόβουλη τέτοια περίπτωση ο επιτιθέμενος κόμβος δύναται να δημιουργήσει μια διακλάδωση στην αλυσίδα, στοχεύοντάς σε μια "double spending" επίθεση. Αφού επιτευχθεί κάτι τέτοιο στην συνέχεια μια δεύτερη "double spending" επίθεση θα υποχρέωνε τον εισβολέα σε μια δεύτερη αλλαγή της τιμής coinage με στόχο να αυξήσει την ισχύ του ως κόμβος έναντι των ανταγωνιστών του. Κάτι τέτοιο για να επιτευχθεί ή θα χρειαστεί πολύ χρόνος ή πολλά νομίσματα. Ωστόσο μια τέτοια επίθεση θα έχει ως αντίκτυπο την υποτίμηση του ίδιου του συστήματος, γεγονός το οποίο συνεπάγεται περιορισμένο κίνητρο για την εφαρμογή της. Η επίθεση αυτή αναφέρεται ως "**attack by accumulating the coin age**". Αναλυτικότερα η ηλικία των κερμάτων χρησιμοποιείται ως μέτρο κατοχής ποσοστού νομισμάτων από τους κόμβους του συστήματος. Για παράδειγμα, ένας επιτιθέμενος που έχει στην κατοχή του ένα ποσοστό της τάξεως 5% θα μπορούσε να μοιράσει τα χρήματα του σε πολλές εξόδους περιμένοντας μέχρι η ηλικία του UTXO να μεγαλώσει κατά 10 φορές από τον μέσο όρο (Averin & Averina, 2019). Να σημειωθεί ότι ως UTXO ορίζεται ως η έξοδος μιας συναλλαγής blockchain η οποία δεν έχει δαπανηθεί με σκοπό να χρησιμοποιηθεί ως είσοδος σε μια νέα συναλλαγή.

Οι επιθέσεις που συναντάμε σε αυτό το μοντέλο χρήζουν μεγαλύτερης ανάλυσης αρχικά λόγω της σπουδαιότητας του ως (το πιο χρησιμοποιούμενο μαζί με το PoW), αλλά και εξαιτίας του ότι θα αναλύσουμε νέες επιθέσεις που δεν σχετίζονται με το PoW είτε δεν έχουν αναλυθεί σε προηγούμενο κεφάλαιο.

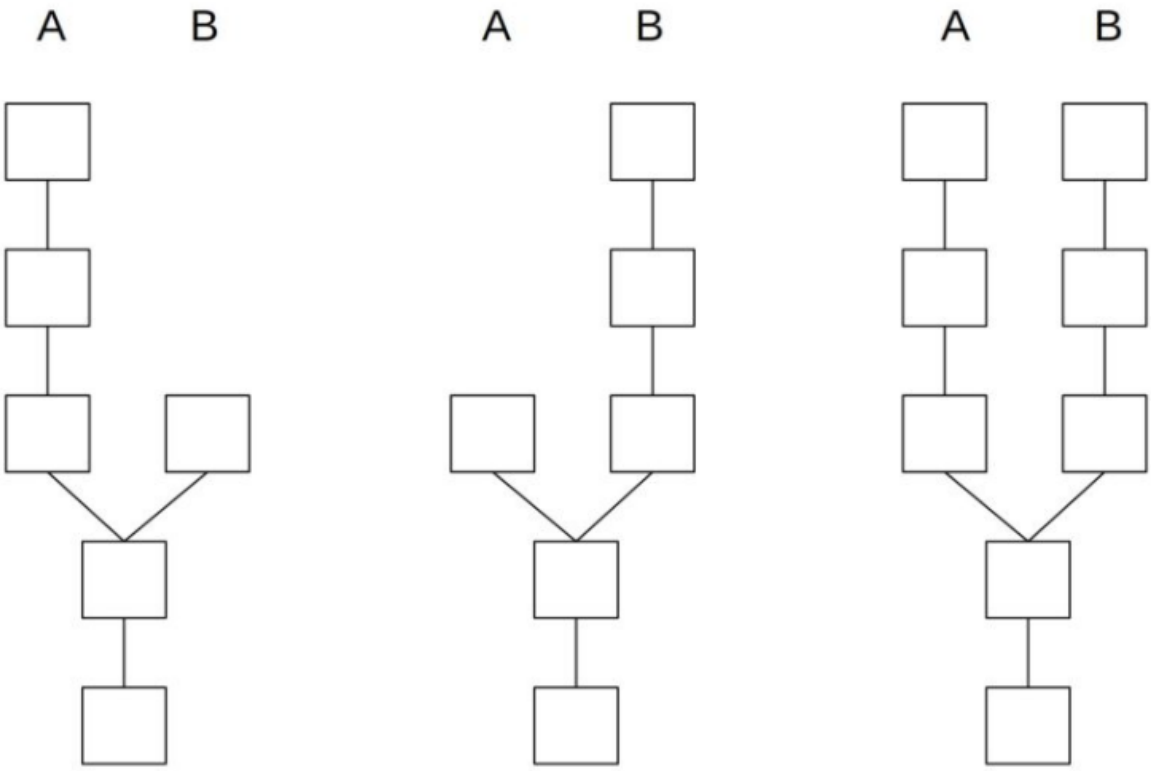
Αρχικά θα αναφέρουμε μια από τις πιο γνωστές επιθέσεις στο blockchain, αυτή με την ονομασία 51% επίθεση. Όπως αναλύσαμε, αν κάποιος ανθρακωρύχος (ή mining pool) αποκτήσει υπολογιστική δύναμή της τάξεως 51% επί της συνολικής ισχύς που έχει το

δίκτυο θα έχει τον έλεγχο του δικτύου και θα αποκτά τις ανταμοιβές μπλοκ (όσον αφορά το PoW). Στο PoW μοντέλο η αντίστοιχη επίθεση για να επιτευχθεί από ένα επικυρωτή το αντίστοιχο ποσοστό είναι 34% (Fault Tolerance) του συνολικού πονταρίσματος (Stake) στο δίκτυο (Deirmentzoglou, Papakyriakopoulos, & Patsakis, 2019). Σε μια τέτοια περίπτωση, μιας **επίθεση πλειοψηφίας (34%)** υπάρχει το ενδεχόμενο ως επακόλουθο ένα ήδη οριστικοποιημένο μπλοκ να αμφισβητηθεί από κάποιο άλλο ανταγωνιστικό μπλοκ προκαλώντας νέες επιθέσεις όπως την επίθεση **"Censorship"**. Σε αυτή την περίπτωση, οι επικυρωτές αποκτούν ορισμένων συναλλαγών τις οποίες μπορούν να προσθέσουν σε ένα μπλοκ, ενώ παράλληλα υπάρχει η δυνατότητα να εντάξουν σε μια λίστα ορισμένες διευθύνσεις (κόμβων). Ειδικότερα, οι επικυρωτές ενδέχεται να αφαιρέσουν ορισμένες συναλλαγές από τα μπλοκ τους. Για παράδειγμα στο σενάριο ενός μεμονωμένου επικυρωτή που εκτελεί τη επίθεση "Censorship", ενδέχεται ορισμένες συναλλαγές να καθυστερήσουν ή να ακυρωθούν λόγω χρονικών περιορισμών. Με αυτή την έννοια, αν υποθέσουμε ότι η πράξη αυτή γίνεται από ένα πλήθος επικυρωτών, η πιθανότητα επίτευξης της επίθεσης "Censorship" στο δίκτυο αυξάνεται. Σε αυτό το σημείο θα αναφέρουμε άλλη μια επίθεση, που σχετίζεται και με τα 2 βασικά μοντέλα συναίνεσης, η οποία είναι η επίθεση **"Bribery"**, η οποία με την ίδια λογική που την είδαμε στο PoW, βασίζεται στην δωροδοκία των επικυρωτών (αντί των ανθρακωρύχων) για να εργαστούν προς όφελος του επιτιθέμενου στην παραγωγή μπλοκ ή διακλαδώσεων. Υπενθυμίζουμε ότι η λογική αυτή στηρίζεται στην καταβολή ποσού ίσου ή μεγαλύτερου στους κόμβους θύματα σε σχέση με την ανταμοιβή που θα έπαιρναν σε περίπτωση που παρήγαγαν κάποιο μπλοκ, με την προϋπόθεση όμως ότι η προσπάθεια αυτή από του κόμβους θύματα θα γίνεται στην ιδιωτική διακλάδωση του επιτιθέμενου. Με τον τρόπο αυτό, το σύστημα θα δωροδοκήσει του κόμβους που παράγουν μπλοκ μόνο στην δική του ιδιωτική διακλάδωση. Ωστόσο στα μοντέλα PoS, το πρόβλημα αυτό αντιμετωπίζεται μέσω της λεγόμενης «συνθήκης περικοπής».

Ένα χαρακτηριστικό πρόβλημα στο PoS ονομάζεται **"Nothing at Stake"** και προκύπτει όταν μπορεί το blockchain δίκτυο να μην επιτύχει συναίνεση με βάση τον κανόνα "longest chain|" (DLT-Repo, 2021). Αναλυτικότερα, όπως έχει τονιστεί στο μοντέλο PoS, οι επικυρωτές επιλέγονται με βάση το ποσό των κεφαλαίων τους. Συνεπώς η πιθανότητα επιλογής είναι μεγαλύτερη όσο περισσότερα είναι τα κεφάλαια. Έτσι, όπως και στο PoW υπάρχει η έννοια της ανταμοιβής μπλοκ μέσω της λήψης ορισμένων

νομισμάτων για την προσπάθεια αυτή. Για την καλύτερη κατανόηση του προβλήματος, δίνουμε το παρακάτω παράδειγμα.

Έστω ότι υπάρχει μια διακλάδωση στα μπλοκ Α και Β. Οι παραγωγοί (επικυρωτές) μπλοκ έχουν τρείς επιλογές. Αυτές είναι να εργαστούν μόνο στο στην αλυσίδα Α, μόνο στην Β ή και στις δύο. Θεωρείται επιπλέον ότι ο επικυρωτής θεωρεί ότι η αλυσίδα Α θα



Εικόνα 52:Τρείς διαφορετικές περιπτώσεις επικύρωσης μπλοκ (nothing at Stake attack)[23]

έχει το μεγαλύτερο μήκος, με πιθανότατα 0.1, ενώ η Β θα έχει την εναπομείναντα πιθανότητα 1-0.1=0.9. Έτσι αν τυχαία η ανταμοιβή για το μπλοκ είναι 7, τότε ο επικυρωτής για την κάθε περίπτωση αντιστοίχως δέχεται μια διαφορετική ανταμοιβή: 1)5*0.1=7, 2)7*0.9=6.3, 3)7*0.1+7*0.9=13,3. Με αυτή την έννοια, ένας ορθολογικός επικυρωτής θα αποφάσιζε πάντα να εργαστεί στην τρίτη περίπτωση (και στις 2 αλυσίδες), προκειμένου να κερδίσει μεγαλύτερη ανταμοιβή. Στην περίπτωση όμως όπου και οι 2 αλυσίδες επικυρώνονται την ίδια στιγμή, τότε όλοι οι επικυρωτές θα έχουν τα νομίσματα τους και

[23] Ανακτήθηκε από: https://dlt-repo.net/nothing-at-stake-in-proof-of-stake-pos/

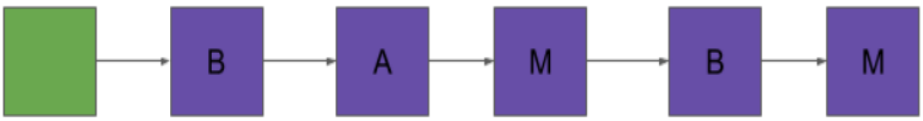
στις δύο αλυσίδες (σε αντίθεση με το PoW, όπου θα έπρεπε να χωρίσουν τα νομίσματα τους μεταξύ των blockchain, ενώ παράλληλα το κόστος είναι ελάχιστο). Με αυτό τον τρόπο χωρίς να υπάρχει κάποιο ρίσκο ή κίνδυνος για τον επιτιθέμενο επικυρωτή ως προς τις συναινετικές του αποφάσεις και έτσι αναπόφευκτα μπορεί να προκαλέσει αποτυχία στο δίκτυο, δεδομένου ότι με βάση το συμφέρον του θα επιλέξει να συμμετέχει σε όσο το δυνατό περισσότερες διακλαδώσεις μπορεί, χωρίς να γνωρίζει ποια είναι η κύρια ("Nothing at Stake in Proof of Stake (PoS) - DLT-Repo," n.d.). Αυτό ακριβώς συμβαίνει εξαιτίας του φαινομένου "Costless Simulation". Έτσι λοιπόν το κύριο πλεονέκτημα των πρωτοκόλλων αυτών, αποτελεί παράλληλα και την πρωταρχική πηγή επιθέσεων ως προς αυτά. Καταλήγοντας λοιπόν , εξαιτίας του γεγονότος ότι στα PoS πρωτόκολλα δεν υπάρχουν ανθρακωρύχοι και υπολογιστικά προβλήματα, αλλά απαιτείται μόνο το χαρακτηριστικό της εμπιστοσύνης, ουσιαστικά δεν απαιτείται εξίσου δύσκολη προσπάθεια για τους επικυρωτές, όπως θα συνέβαινε στην περίπτωση των ανθρακωρύχων.

Η **"Coin-age accumulation"** επίθεση τοποθετείται επίσης σε αυτές του αλγορίθμου PoS. Ειδικότερα, ο αλγόριθμος PoS που βασίζεται στην χωρίς περιορισμό παράμετρο («ηλικία» των νομισμάτων) είναι επιρρεπείς σε αυτή την επίθεση. Η μέθοδος του εισβολέα είναι να περιμένει ώστε τα νομίσματα του να συγκεντρώσουν αρκετό "Coinage", (η περίοδος κράτησης σε μέρες ενός νομίσματος από τον ιδιοκτήτη) προκειμένου να εκμεταλλευτεί τον αλγόριθμο για την εκκίνηση της επίθεσης "double spending" ξεκινώντας την δημιουργία μιας διακλάδωσης (Ferdous, Chowdhury, Hoque, & Colman, n.d.). Γίνεται λοιπόν αντιληπτό, ότι ο κίνδυνος αυτός είναι εύκολα αντιμετωπίσιμος, με την εφαρμογή ενός ανώτατου ορίου της τιμής "coinage" με στόχο την ελαχιστοποίηση του υπεύθυνου παράγοντα που προκαλεί την επίθεση.

Μια ακόμη πολύ σημαντική επίθεση που αφορά όμως αποκλειστικά το μοντέλο συναίνεσης "Proof of Stake" είναι η **"Liveness Denial"** επίθεση (Deirmentzoglou et al., 2019). Σε αυτήν την επίθεση ορισμένοι ή όλοι οι επικυρωτές αποφασίζουν να αποκλείουν σκόπιμα συναλλαγές σταματώντας να εκδίδουν μπλοκ. Με αυτόν τον τρόπο αποφεύγουν την διαδικασία της επικύρωσης μπλοκ, γεγονός το οποίο σταματά την εξέλιξη της αλυσίδας μπλοκ, αφού δεν μπορούν να επικυρωθούν νέα μπλοκ ώστε να δημοσιευθούν στην συνέχεια. Για τον λόγο αυτό προκύπτει μια «απαίτηση ζωντάνιας» (Liveness attack**)**, όπου πρόκειται για μια επίθεση η οποία αποστραγγίζει το διαθέσιμο ποσό (Stake) που είχαν στην κατοχή τους οι ανενεργοί αυτοί επικυρωτές. Εάν ωστόσο υπάρχει άρνηση από την πλευρά τους ως προς την απαίτηση αυτή, δεν θα τεθεί σε κίνδυνο το δίκτυο.

Η **“Long range attack”** αποτελεί και αυτή μια χαρακτηριστική επίθεση για το συγκεκριμένο μοντέλο συναίνεσης. Το σενάριο σε αυτή την περίπτωση είναι όταν ένας αντίπαλος επιστρέφει στο “genesis block” της αλυσίδας , προκειμένου να δημιουργήσει σε αυτό το σημείο διακλάδωση (Deirmentzoglou et al., 2019). Η νέα αυτή διακλάδωση συμπληρώνεται μερικώς ή και με εντελώς διαφορετική ιστορία από την κύρια. Η επίθεση επιτυγχάνεται με βάση τον κανόνα “longest chain” όταν η διακλάδωση η οποία δημιουργήθηκε από τον εισβολέα, γίνεται μεγαλύτερη από την κύρια αλυσίδα. Κατά κάποιο τρόπο οι επιθέσεις “Long range” στα πρωτόκολλα PoS σχετίζονται με τις επιθέσεις “Selfish mining” στα μοντέλα PoW. Ωστόσο στα PoW μοντέλα εξαιτίας της «απαγορευτικής» υπολογιστικής προσπάθειας που πρέπει να καταβάλει ο επιτιθέμενος δεν είναι εφικτό για αυτόν να επιστρέψει στο αρχικό “genesis block”. Ειδικότερα, η επίθεση διαχωρίζεται σε τρείς διαφορετικούς τύπους με τις αντίστοιχες ονομασίες **Simple**, **Posterior Corruption**, **Stake bleeding** (Deirmentzoglou et al., 2019). Δεδομένου ότι οι επιθέσεις αυτές είναι σε παρόμοια λογική θα να αναλύσουμε μόνο παραθέτοντας ένα παράδειγμα για την πρώτη (Precomputing attack**)**. Στο παράδειγμα αυτό, θεωρούμε μια πισίνα επικύρωσης (validator pool), στην οποία συμμετέχουν τρείς επικυρωτές η Αλίκη, ο Μπομπ και ο Μάλορυ:

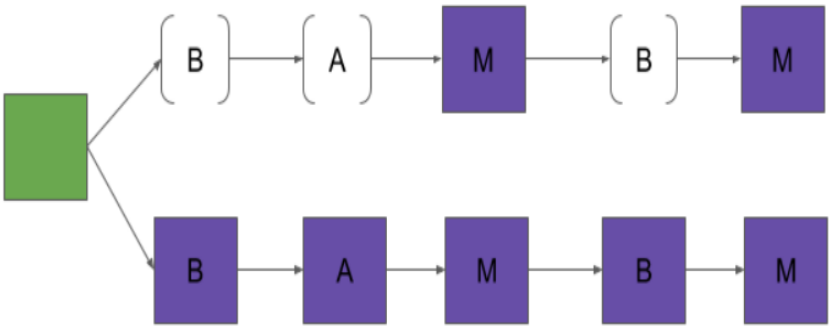
Simple: Αυτού του είδους τις επιθέσεις (Long range attack), θεωρούνται μια «αφελής» υλοποίηση του πρωτοκόλλου PoS στο οποίο οι κόμβοι δεν ελέγχουν τις χρονικές σημάνσεις των μπλοκ. Σε ένα κανονικό κύκλο του πρωτοκόλλου PoS, κάθε επικυρωτής θα έχει την ευκαιρία να επικυρώσει μπλοκ.



Εικόνα: Ίδια πιθανότητα για όλους τους εν δυνάμει επικυρωτές B,A,M.[24]

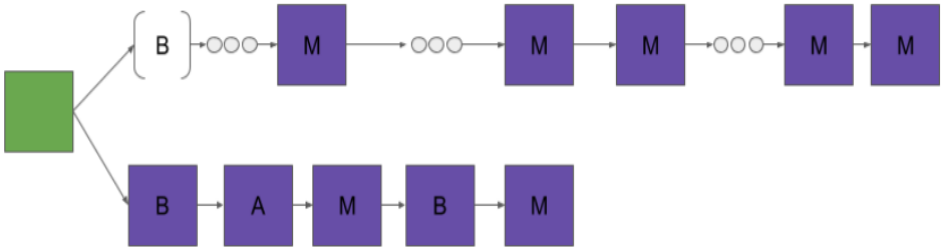
[24] Ανακτήθηκε από: https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9

Ο Μάλορυ ξεκινά την επίθεση, μέσω της δημιουργίας μιας εναλλακτικής διακλάδωσης του blockchain. Ειδικότερα, πηγαίνει στο “genesis block” και σε εκείνο το σημείο (πρώτο μπλοκ) διακλαδώνει την αλυσίδα.



Εικόνα 53:Η Malory έχει τις ίδιες πιθανότητες να εκλεγεί και στις δύο διακλαδώσεις. Σε παρένθεση είναι τα χαμένα μπλοκ.[25]

Λαμβάνοντας υπόψη ότι εντός του “genesis block” εμπεριέχονται οι πληροφορίες της επικύρωσης, συνεπάγεται ότι η Μάλορυ δεν θα μπορεί να παράγει μπλοκ πιο γρήγορα από τι στην κύρια αλυσίδα, αλλά περιορίζεται στον ίδιο ρυθμό. Αναγκαστικά λοιπόν για να επιτύχει την επίθεση, θα πρέπει να παράγει μπλοκ σε πιο γρήγορο χρόνο, προκειμένου η ιδιωτική διακλάδωση της να ξεπεράσει την αρχική αλυσίδα, όπως φαίνεται στην επόμενη εικόνα.



[25] Ανακτήθηκε από: https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9

Εικόνα 54:Με την χρήση τριπλών κουκίδων δηλώνονται τα πολλαπλά χαμένα μπλοκ. Ίδιο μήκος των 2 αλυσίδων.[26]

Δεδομένου ότι η Μάλορυ είναι η μόνη ενεργή "Stakeholder" στην διακλάδωση που δημιούργησε, συνεπώς μπορεί να την διαχειριστεί όπως θέλει. Για παράδειγμα, σε ένα ενδεχόμενο όπου οι κόμβοι δεν συμμετέχουν με την ύπαρξη χρονικών σημάνσεων οι κόμβοι δεν θα μπορούσαν να εντοπίσουν την πλαστογραφία της Malory.

Καταλήγοντας, θα περιγράψουμε τους άλλους δύο τύπων "Long-range" επιθέσεων οι οποίες είναι σε παρόμοια λογική με τύπο "Simple". Έτσι λοιπόν, έχουμε την περίπτωση "**Posterior corruption**" όπου πρόκειται για μια προσπάθεια να κοπούν περισσότερα μπλοκ από την κύρια αλυσίδα σε ένα δεδομένο χρονικό πλαίσιο, ενώ η περίπτωση "**Stake bleeding**" σχετίζεται με την αντιγραφή μιας συναλλαγής από το ειλικρινά διατηρημένο blockchain σε ένα ιδιωτικό blockchain που διατηρεί ο εισβολέας.

Κατά την διεξαγωγή μιας "Long-Range" επίθεσης λοιπόν, ένας επιτιθέμενος χρησιμοποιεί ένα αγορασμένο ή ιδιωτικό κλειδί ενός σημαντικού υπολοίπου token, που έχει χρησιμοποιηθεί για επικύρωση στο παρελθόν. Στην συνέχεια, ο εισβολέας μπορεί να δημιουργήσει ένα εναλλακτικό ιστορικό του blockchain και να αυξήσει τις ανταμοιβές με βάση την επικύρωση PoS.

3.3.3 Βασικά χαρακτηριστικά και αδυναμίες του μοντέλου συναίνεσης "Delegated Proof of Stake" (DPOS)

Η κύρια ιδέα του DPoS είναι να μειώσει την σπατάλη ενέργειας και να ενισχύσει την ταχύτητα στις συναλλαγές. Η συνολική διαδικασία δημιουργίας μπλοκ καθιστά αυτό τον μηχανισμό συναίνεσης γρηγορότερο από τον PoW (Kaur et al., 2021). Το DPoS μοντέλο χαρακτηρίζεται από την «πολιτική της μια ψήφου», σύμφωνα με την οποία δίνεται η ευκαιρία στα ενδιαφερόμενα μέρη να ρίξουν περισσότερες ψήφους, ενώ έχουν περισσότερα νομίσματα. Έτσι, οι μάρτυρες (Witnesses) ανταμείβονται για την δημιουργία μπλοκ, ενώ σε περίπτωση αποτυχίας τιμωρούνται, χωρίς την προσθήκη ψήφου. Συνεπώς,

[26] Ανακτήθηκε από: https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9

οι μάρτυρες στοχεύουν να αποκτήσουν μεγαλύτερο αριθμό ψήφων προκειμένου να εκτελέσουν τον μηχανισμό συναίνεσης.

3.3.3.1 Μειονεκτήματα

Στο μηχανισμό DPoS λόγω της περιορισμένης δυνατότητα ως προς την λήψη αποφάσεων των κόμβων, αφού το κριτήριο είναι η κατοχή νομισμάτων του κάθε κόμβου με αποτέλεσμα δημιουργείται η τάση μιας κεντροποιημένης διαχείρισης του δικτύου. Επιπλέον κάποιες φορές είναι δυνατόν να δημιουργηθούν συμπράξεις μεταξύ των κόμβων που είναι υποψήφιοι για την δημιουργία μπλοκ (witnesses), ώστε τελικά να είναι αυτοί που θα ελέγξουν το δίκτυο.

3.3.3.2 Προβλήματα ασφαλείας και επιθέσεις που αντιμετωπίζει το Μοντέλο συναίνεσης " Delegated Proof of Stake"

Όσο αναφορά τα ζητήματα ασφάλειας που αντιμετωπίζει το μοντέλο συναίνεσης "Delegated Proof of Stake", μια από τις σημαντικότερες είναι η **"bribe attack"**, κατά την οποία ο επιτιθέμενος επιδιώκει να ξοδέψει τα χρήματα του δύο φορές για την αγορά υπηρεσιών αφού γίνει η επιβεβαίωση της συναλλαγής από τον πωλητή, σε ένα διακλαδωμένο blockchain, στο οποίο ο κακόβουλος αυτός κόμβος θα έχει την δυνατότητα να δίνει μεγάλη ανταμοιβή στους κόμβους που συμμετέχουν στο συγκεκριμένο δίκτυο (Averin & Averina, 2019). Με αυτό τον τρόπο η διακλάδωση αυτή ανταγωνίζεται το πρωτότυπο δίκτυο, ενώ η διαδικασία αυτή εξελίσσεται έως ότου το διακλαδωμένο blockchain αποκτήσει μεγαλύτερο μήκος από το αρχικό.

Θα πρέπει να τονιστεί ότι, λόγω της μεγάλης συμμετοχής κόμβων στην διαδικασία της ψηφοφορίας σε ένα τέτοιο μοντέλο δημιουργούνται ευνοϊκότερες συνθήκες για την επίτευξη μιας επίθεσης. Έτσι για ένα κόμβο ο οποίος διαθέτει ένα μικρό ποσοστό πονταρίσματος είναι σχεδόν αδύνατο να επηρεάσει με την ψήφο του τις υπάρχουσες συνθήκες στο σύστημα. Το γεγονός αυτό συνεπάγεται ότι το να ξοδεύεται χρόνος για ψήφιση από τους κόμβους μπορεί να γίνει ασύμφορο με την έννοια ότι η διαδικασία αυτή είναι πιο κοστοβόρα, σε σύγκριση με την αξία της ψήφου. Το πρόβλημα αυτό αντιμετωπίζεται μέσω μιας proxy ψηφοφορίας, κατά την οποία ένας κόμβος που μπορεί να ποντάρει ένα μικρό ποσό έχει την δυνατότητα να μεταφέρει το ποσό αυτό σε κάποιον άλλον ο οποίος μπορεί να ποντάρει μεγαλύτερο ποσό ούτως ώστε να προστεθούν και να

χρησιμοποιηθούν από τον δεύτερο αυξάνοντας έτσι τις πιθανότητες για την εύρεση συναίνεσης.

Ένας ακόμη κίνδυνος που παρουσιάζεται στα DPoS μοντέλα όσον αναφορά την συνεργατική παραγωγή μπλοκ μεταξύ των κόμβων, εκτός της δημιουργίας διπλοσυναλλαγής είναι και η αλλαγή παραμέτρων συστήματος (Kaur et al., 2021). Τέλος, η κατανεμημένη επίθεση άρνησης υπηρεσίας (**distributed denial of service attack**) αποτελεί ακόμη ένα πρόβλημα στα μοντέλα DPoS, όπου επιτιθέμενοι κόμβοι μπορούν να προβλέψουν τον επόμενο παραγωγό μπλοκ. Ωστόσο είναι κατανοητό ότι θα αποτελεί πολύ δύσκολο εγχείρημα για ένα επιτιθέμενο να βλάψει ταυτόχρονα ένα μεγάλο αριθμό από παραγωγούς μπλοκ ενός κατανεμημένου blockchain συστήματος σε αντίθεση με μια περίπτωση ενός κεντροποιημένου συστήματος όπου θα αρκούσε η επίθεση σε ένα συγκεκριμένο κόμβο. Στο σημείο αυτό αξίζει να σημειωθεί, ότι αν ένα σύνολο κόμβων αποτυγχάνει επανειλημμένα να παράγει νέα μπλοκ λόγω των παραπάνω επιθέσεων δύναται να αντικαθίστανται από τους παραγωγούς τους.

Καταλήγοντας, το μοντέλο DPoS αναπτύχθηκε για να αυξήσει την αποτελεσματικότητα στις συναλλαγές και να ξεπεράσει τους περιορισμούς, άλλων μηχανισμών συναίνεσης. Ωστόσο, περιλαμβάνει σημαντικά ελαττώματα. Έτσι, ένα από αυτά είναι η αποτυχία επαρκής αποκέντρωσης, γεγονός το οποίο επιβραδύνει το δίκτυο σε μια τέτοια περίπτωση λόγω του μεγάλου αριθμού επικυρωτών. Τέλος αυτός ο μηχανισμός ως επέκταση του PoS αντιμετωπίζει κοινές επιθέσεις όπως DDoS και Sybil.

Πίνακας 7:Σύγκριση επιθέσεων στα μοντέλα συναίνεσης του blockchain

Μοντέλο Συναίνεσης	**Έτος**	**Τύπος Blockchain**	**Τρόπος εξόρυξης**	**Βασικές επιθέσεις που μπορεί να αντιμετωπίσει**	**Κατανάλωση ενέργειας**
Proof of work	2008	Δημόσιο Blockchain	Βασίζεται στην κατανάλωση ενέργειας	Bribe, Sybil, 51%, Brute Force, Race, double spending, Balance, BGB Hijacking Attacks	33TWh κατανάλωση ενέργειας

Μοντέλο Συναίνεσης	Έτος	Τύπος Blockchain	Τρόπος εξόρυξης	Βασικές επιθέσεις που μπορεί να αντιμετωπίσει	Κατανάλωση ενέργειας
Proof of Stake	2012	Δημόσιο Blockchain	Επικύρωση	Double Spending, Majority, DoS, Sybil, Bribe (short range attack), Long-Range, Prosterior corruption, Nothing at stake, Liveness denial, censorship, coin age accumulation	0.073 TWh Κατανάλωση ενέργειας
Delegated Proof of Stake	2014	Δημόσιο Blockchain	Επικύρωση	Majority attack, Bribe attack, DDoS attack, double spending attack, Sybil attack, Long-Range attack, Sybil attack, Balance attack, distributed denial of service attack, Coin-age accumulation	0.0016TWh Κατανάλωση ενέργειας

Πίνακας 8:Σύγκριση σημαντικών χαρακτηριστικών των μοντέλων συναίνεσης δημοσίου Blockchain

	PoW	PoS	DPoS

Κατανάλωση Ενέργειας	Υψηλή	Χαμηλή	Εξαρτάται από τον αριθμό των παραγωγών μπλοκ
Δυνατότητα Αποκέντρωσης	Χαμηλή	Μέτρια (μερική κεντροποίηση)	Μέτρια/χαμηλή
Δυνατότητα δημιουργίας Διακλάδωσης	Υψηλή	Χαμηλή	-
Επεκτασιμότητα	Χαμηλή	Μέτρια	Υψηλή
Ανοχή σε σφάλατα	<51%	<34%	<51%
Χρόνος επιβεβαίωσης	Υψηλός	Χαμηλός	Πολύ Χαμηλός
Ταχύτητα Δημιουργίας Μπλοκ	Αργή	Γρήγορη	Μέτρια
Διεκπεραίωση συναλλαγών	Χαμηλή	Μέτρια	Μέτρια
Εξοικονόμηση ενέργειας	Καθόλου	Μερική	Μερική
Απαιτητικό Hardware	Πολύ σημαντικό	Όχι	Όχι

Καταλήγοντας, θα πρέπει να σημειώσουμε ότι το μοντέλο συναίνεσης PoW διακρίνεται για την αναλογικότητα στην υψηλή κατανάλωση ενέργειας και την υψηλή ασφάλεια, σε αντίθεση με τα υπόλοιπα μοντέλα των δημόσιων blockchain PoS και DPoS τα οποία μπορεί να έχουν το πλεονέκτημα της χαμηλότερης κατανάλωσης αλλά υστερούν στο επίπεδο της ασφάλειας.

4 Ενδεικτικές λύσεις επιθέσεων σε blockchain συστήματα

4.1 Double Spending

Αρχικά, θεωρούμε ότι το πρόβλημα της διπλής δαπάνης ξεκινά στην φάση κατά την οποία ο κακόβουλος ανθρακωρύχος επιλέγει συναλλαγές και εντάσσει μπλοκ στην ιδιωτική αλυσίδα που δημιούργησε η οποία επαληθεύεται από τον ίδιο σε γρηγορότερο χρόνο σε σύγκριση με την πραγματική αλυσίδα, εξαιτίας της υψηλότερης υπολογιστικής ισχύς που έχει συγκεντρωμένη στην κατοχή του.

Υποθέτοντας ότι ένας κακόβουλος ανθρακωρύχος A_1 καταναλώνει όλο το διαθέσιμο ποσό bitcoin που έχει στην κατοχή του προκειμένου να πραγματοποιήσει την αγορά ενός προϊόντος από πωλητή έστω Π_1. Ο κακόβουλος ανθρακωρύχος δηλαδή εμπεριέχει την συναλλαγή στο μπλοκ του ενώ παράλληλα διαδίδει την πληροφορία της συναλλαγής στο πραγματικό blockchain και κατ'επέκταση στους ειλικρινείς ανθρακωρύχους με στόχο να επαληθευτεί η συναλλαγή στο πραγματικό (αρχικό) blockchain (Begum et al., 2020). Το κρίσιμο σημείο σε μια τέτοια περίπτωση είναι ότι ο κακόβουλος ανθρακωρύχος δεν προσθέτει την συναλλαγή έστω T_1 στην δική του κακόβουλη αλυσίδα. Αυτό επιφέρει ως συνέπεια κάποιος ανθρακωρύχος που δημιουργεί το μπλοκ του στην ιδιωτική αλυσίδα να μην γνωρίζει σχετικά με την συναλλαγή T_1. Αναλυτικότερα, την στιγμή που ο κακόβουλος ανθρακωρύχος καταφέρει η δική του ιδιωτική αλυσίδα να ξεπεράσει σε μήκος την πραγματική τότε αποφασίζει να διαδώσει την πληροφορία μιας συναλλαγής που είναι ενταγμένη μέχρι πρότινος στην ιδιωτική αλυσίδα η οποία με βάση το κανόνα «μεγαλύτερης αλυσίδας» μετατρέπεται στην πραγματική αλυσίδα. Το αποτέλεσμα μιας τέτοιας κατάστασης θα είναι η επικράτηση των κανόνων σύμφωνα με την νέα (επικρατούσα) αλυσίδα. Ωστόσο όπως αναφέρθηκε σχετικά με την συναλλαγή T_1 δεν προστίθεται σε μπλοκ της ιδιωτικής αλυσίδας. Αντίθετα προστίθεται σε μπλοκ της νέας αλυσίδας. Το γεγονός αυτό συνεπάγεται ότι όταν ένα παλιό μπλοκ από την πραγματική προστεθεί στη νέα αλυσίδα θα διαγράφονται οι πληροφορίες σχετικά με την συναλλαγή T_1. Με αυτό τον τρόπο ο κακόβουλος ανθρακωρύχος θα δημιουργούσε το πρόβλημα της διπλής δαπάνης ξοδεύοντας δηλαδή ποσό bitcoin το οποίο θα έχει ήδη δαπανηθεί. Σε μια τέτοια κατάσταση κατά την οποία δηλαδή ένα μπλοκ προσπαθεί να προστεθεί στην νέα (ιδιωτική) αλυσίδα, **θα ενημερώνει τα δεδομένα κατακερματισμού, κρατώντας παράλληλα τα δεδομένα του πραγματικού blockchain**. Έτσι λοιπόν, όταν ένα μπλοκ από την αρχική μικρότερη αλυσίδα του πραγματικού blockchain προστεθεί

στην ιδιωτική αλυσίδα η οποία θα έχει στα δεδομένα του τον κατακερματισμό της συναλλαγής T_1 θα γίνεται μεν ενημέρωση των πληροφοριών συναλλαγής (νέα συναλλαγή) με την παράλληλη όμως διατήρηση των πληροφοριών της προηγούμενης συναλλαγής (Begum et al., 2020). Με άλλα λόγια, αν στην ιδιωτική αλυσίδα του κακόβουλου ανθρακωρύχου υπάρχουν σε κάποια φάση οι πληροφορίες των συναλλαγών T_2, T_3 και προστεθεί ένα μπλοκ Β σε αυτή που περιέχει την συναλλαγή T_1, τότε αφού προστεθεί αυτό το μπλοκ θα διαδώσει στο ιδιωτικό blockchain και τις πληροφορίες για την συναλλαγή T_1. Συνεπώς, στο ιδιωτικό blockchain θα υπάρχουν οι πληροφορίες για όλες τις συναλλαγές T_1, T_2, T_3. Το σημαντικό λοιπόν αυτής της πρότασης, είναι ότι αν έχει πραγματοποιηθεί οποιαδήποτε συναλλαγή θα καταγράφεται μόνιμα για όλα τα μπλοκ της αλυσίδας και συνεπώς όλα τα μπλοκ θα έχουν τις πληροφορίες όλων των συναλλαγών ανεξάρτητα της αλυσίδας της οποίας προέρχονται.

4.2 Selfish Mining

Για την αντιμετώπιση του παραπάνω προβλήματος, προκύπτει η πρόταση να αυξηθεί το όριο για την επίτευξη εύρεσης ενός κατάλληλου κατακερματισμού (nonce) σε τέτοιο βαθμό έτσι ώστε να είναι αδύνατο για κάποιο κόμβο να επωφεληθεί μέσω της εξόρυξης από ένα "mining pool" που θα ανήκει σε ένα εγωιστή ανθρακωρύχο (Saad, Njilla, Kamhoua, & Mohaisen, 2019). Επιπλέον οι κόμβοι θα πρέπει να διαδίδουν ολόκληρη την αλυσίδα (ως αντίγραφο) όταν είναι γνωστό ότι υπάρχει διακλάδωση της αλυσίδας χωρίς ωστόσο το μήκος κάποιας διακλάδωσης να υπερτερεί έναντι κάποιας άλλης και η επιλογή της διακλάδωσης που θα επιλέξουν για την εξόρυξη ενός νέου μπλοκ να πραγματοποιείται με τυχαίο τρόπο. Σε αυτή την περίπτωση λοιπόν που προκύπτει κάποια διακλάδωση στην αλυσίδα η τιμή γ είναι 0.5 και για αυτό τον λόγο η τιμή μεταβάλλεται σε 0.25. Η μεταβολή αυτή της τιμής γ μεταφράζεται στο ενδεχόμενο κάποιος κόμβος και συγκεκριμένα το "mining pool" κάποιου κόμβου να συγκεντρώνει τουλάχιστον το 25% της υπολογιστικής ισχύς του δικτύου και το νόημα του είναι να ενημερωθεί το δίκτυο σε προγενέστερο χρόνο ώστε να «φρενάρει» την επέκταση της νέας ανταγωνιστικής διακλάδωσης.

.

4.3 Eclipse

Σύμφωνα με το άρθρο (Heilman et al., n.d.) προτείνονται 8 μέτρα ως προς την αντιμετώπιση της επίθεσης eclipse με σκοπό να δημιουργηθεί επιπλέον δυσκολία για την επιτυχή επίτευξη της. Ένας τρόπος η τυχαία επιλογή διευθύνσεων από τον δοκιμασμένο και τον νέο πίνακα. Αναλυτικότερα λόγω του ότι δίνεται βάση στην προγενέστερη χρονική σήμανση μιας διεύθυνσης προκειμένου να υπάρξει μια νέα εξερχόμενη σύνδεση. Το γεγονός αυτό συνεπάγεται ότι, αν ένας επιτιθέμενος κατέχει ένα μικρό ποσοστό του δοκιμασμένου πίνακα του στόχου του, υπάρχει δυνατότητα να αυξήσει το ποσοστό αυτό απλά αφιερώνοντας περισσότερο χρόνο στην επίθεση. Έτσι, η παραπάνω αδυναμία για το θύμα θα μπορούσε να περιοριστεί αν η επιλογή των διευθύνσεων από τον πίνακα δοκιμασμένο ή νέο γινόταν με τυχαιότητα. Με αυτό τον τρόπο, αν ο επιτιθέμενος προσπαθεί για παράδειγμα να ελέγξει το 50% των διευθύνσεων του δοκιμασμένου πίνακα θα πρέπει ο εισβολέας να γεμίσει με διευθύνσεις τον πίνακα σε ποσοστό 91.7% = $\sqrt[8]{0.5}$.

Ένα από τα πιο προφανή μέτρα, θα ήταν η αύξηση του μεγέθους του δοκιμασμένου και νέου πίνακα. Κάτι τέτοιο θα σήμαινε ότι η πλευρά του επιτιθέμενου θα χρειαζόταν περισσότερο χρόνο και κόστος για να για να γεμίσει με μολυσμένες διευθύνσεις με το απαιτούμενο αναγκαίο ποσοστό επί του δοκιμασμένου πίνακα. Για παράδειγμα στην περίπτωση ενός botnet θα χρειαζόταν να διπλασιαστεί ο αριθμός των bots. Σε παρόμοια λογική, θα ήταν πολύ πιο εύκολος ο εντοπισμός του επιτιθέμενου αν ένας bitcoin αν όλες οι εισερχόμενες συνδέσεις ενός προέρχονταν από την ίδια διεύθυνση IP. Για τον λόγο αυτό προτείνεται ή αποδοχή μόνο ενός συγκεκριμένου αριθμού συνδέσεων από την ίδια IP.

Τέλος θα αναφερθεί η πρόταση της απαγόρευσης ανεπιθύμητων μηνυμάτων ADDR. Αναλυτικότερα, ένας κόμβος θα μπορούσε να θέσει ένα ανώτατο όριο για παράδειγμα 10 διευθύνσεων στα μηνύματα ADDR που δέχεται από άλλους κόμβους και ως επέκταση αυτού του μέτρου όταν ο νέος πίνακας είναι αρκετά άδειος να δέχεται μόνο νόμιμα ADDR μηνύματα από εξερχόμενες συνδέσεις. Με αυτό τον τρόπο θα περιορίζεται ο κίνδυνος να γεμίσει με «ψεύτικες» επικίνδυνες διευθύνσεις, που δεν ανήκουν στο δίκτυο.

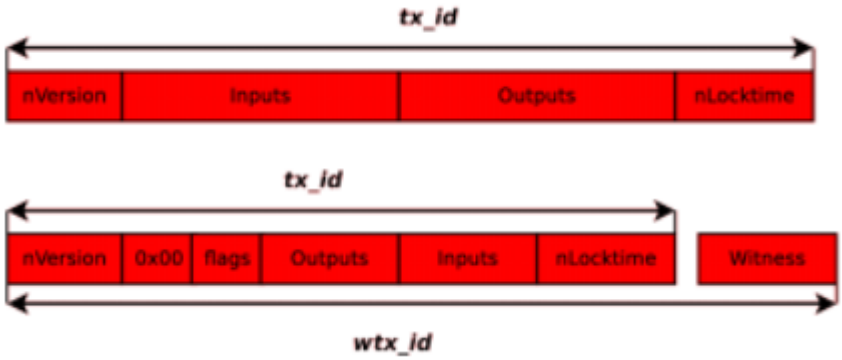
4.4 Transaction Malleability

Οι επιθέσεις transaction malleability στο δίκτυο bitcoin έχουν περιοριστεί μέσω της εφαρμογής μιας αναβάθμισης πρωτοκόλλου μαλακής διακλάδωσης (soft fork) η οποία είναι γνωστή ως Segregated Witness ή SegWit. Αναλυτικότερα μέσω του πρωτοκόλλου

μαλακής διακλάδωσης έχουμε τον επαναπροσδιορισμό της δομής τη συναλλαγής για τον υπολογισμό των αναγνωριστικών των συναλλαγών (Tx id), χωρίς την καταμέτρηση των υπογραφών (Pérez-Solà et al., 2019)(. Η πρόταση SegWit ουσιαστικά αύξησε το μέγεθος του μπλοκ έως και τέσσερις φορές από 1mb σε 4 mb.

Αναλυτικότερα, η βασική ιδέα σχετικά με την πρόταση SegWit ήταν να υπάρχει δυνατότητα εκμαίευσης πληροφοριών σχετικά με την συναλλαγή, οι οποίες απαιτούνται για την επικύρωση της ορθότητας, έχοντας παράλληλα πληροφορίες σχετικά με τα αποτελέσματα της. Πιο συγκεκριμένα, αυτές οι πληροφορίες περιλαμβάνουν σενάρια και υπογραφές τα οποία θα εντάσσονται σε μια νέα δομή καλούμενη Witness, όπου μέσω των υπογραφών εξασφαλίζεται το στοιχείο της μοναδικότητας στις συναλλαγές. Ο μάρτυρας πρέπει να περιλαμβάνεται στο μπλοκ που εντάσσεται η συναλλαγή.

Ως αποτέλεσα της χρήσης του SegWit, το μέγεθος μιας συναλλαγής μειώνεται αυξάνοντας τον αριθό των συναλλαγών που χωρούν σε ένα μπλοκ μεγέθους 1 mb. Τα τέλη της συναλλαγής μειώνονται επίσης. Το βασικό στοιχείο όμως του SegWit είναι ότι εισάγει ένα σύστημα έκδοσης σεναρίων μέσω προτοκόλλων μαλακής διακλάδωσης.



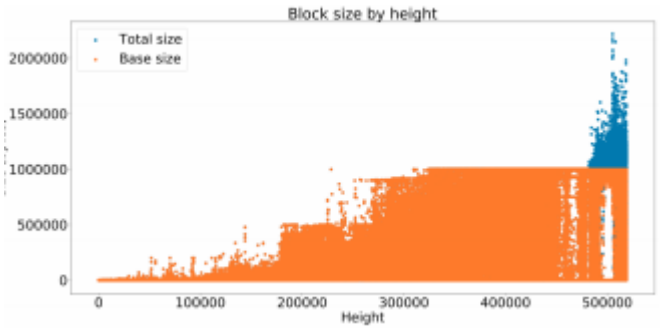
Εικόνα 55:transaction id με και χωρίς SegWit εφαρμογή[27]

Η έννοια “Segregated Witness” έκανε την εμφάνιση της στο κύριο δίκτυο bitcoin όταν το ύψος των μπλοκ (block height) ήταν 481.824. Έπειτα ακολούθησε μια μεταβατική περίοδο 2 εβδομάδων από εκείνη την στιγμή για την αναβάθμιση στα πορτοφόλια των χρηστών. Έτσι μόλις έγινε ενεργοποίηση των καινούριων κανόνων συναίνεσης, ακολούθησε επιβολή αυτών με την έννοια ότι η δημιουργία νέων συναλλαγών ήταν επιτρεπτή μόνο εφόσον τα δεδομένα της υπογραφής ανήκαν πλέον στην νέα μορφή

[27] Ανακτήθηκε από: https://deic.uab.cat/~gnavarro/files/papers/2018.recsi.segwit.pdf

συναλλαγής. Να αναφερθεί ότι υπάρχουν διάφοροι τύποι σεναρίων SegWit, οι οποίες χρησιμοποιούνται είτε εγγενώς είτε ενθυλακώνονται σε εξόδους P2SH (Delgado-Segura et al,2019). Το σημαντικό όμως πλεονέκτημα που προκύπτει με την εφαρμογή του SegWit σεναρίου είναι ότι πραγματοποιείται μείωση του μεγέθους μιας συναλλαγής, αυξάνοντας με αυτό τον τρόπο τον αριθμό των συναλλαγών που μπορούν να ενταχθούν σε ένα μπλοκ μεγέθους 1 mb.

Συμπερασματικά, μπορεί το SegWit να εισάγει ένα είδος πολυπλοκότητας στο bitcoin, αλλά προκύπτει το πλεονέκτημα καλύτερης επεκτασιμότητας του. Αυτό συμβαίνει διότι, τα δεδομένα των μαρτύρων (Witnesses) μειώνονται κατά τον υπολογισμό του συνολικού μεγέθους μπλοκ. Δίνεται έτσι η δυνατότητα να δημιουργηθούν μεγαλύτερου μεγέθους μπλοκ, όπως υποδεικνύεται και στο παρακάτω σχήμα. Πιο συγκεκριμένα, οι πορτοκαλί κουκίδες δηλώνουν το μέγεθος του μπλοκ χωρίς δεδομένα μάρτυρα, παρατηρώντας ταυτόχρονα ότι το μέγεθος του έχει ανώτατο όριο το 1mb.



Εικόνα 56:Σύγκριση μεγεθών μπλοκ με και χωρίς δεδομένα Witness[28]

Η ανάλυση του μεγέθους του ύψους του βασικού μπλοκ δείχνει να σταθεροποιείται στο μέγιστο δυνατό μέγεθος όταν το ύψος κυμαίνεται περίπου στην μέση μεταξύ των 300.000 και 400.000. Παράλληλα, οι μπλε κουκίδες αντιπροσωπεύουν τα συνολικά μεγέθη μπλοκ, αυτών δηλαδή που συμπεριλαμβάνουν τα δεδομένα μαρτύρων. Όπως παρατηρείται όταν το ύψος των μπλοκ είναι 500.000, αντίστοιχα το μέγεθος φαίνεται να ξεπερνά τα 2 mb. Ωστόσο τα πραγματικά αυτά μεγέθη των μπλοκ κάτω από του κανόνες συναίνεσης της μαλακής διακλάδωσης αντιστοιχούν σε εικονικά ποσά μεγεθών κάτω του

[28] Ανακτήθηκε από: https://deic.uab.cat/~gnavarro/files/papers/2018.recsi.segwit.pdf

1 mb, προκειμένου να κρίνονται ως έγκυρα σύμφωνα με τους υπάρχοντες κανόνες συναίνεσης. Έτσι για παράδειγμα το μπλοκ 500.000 ή κάποιο μεγαλύτερο αυτού έχει εικονικό μέγεθος μικρότερου του 1 mb, ενώ στο σχήμα απεικονίζεται μεγαλύτερο του 2 mb που είναι και το πραγματικό.

4.5 Timejacking

Η μελέτη (“Culubas: Timejacking & Bitcoin,” n.d.) αναφέρει ένα σύνολο προτάσεων επί των προβλημάτων που παρουσιάζονται. Πιο συγκεκριμένα αναφέρεται στην χρησιμοποίηση του χρόνου συστήματος του κόμβου αντί για τον χρόνο δικτύου σχετικά με τον προσδιορισμό του ανώτατου ορίου των χρονικών σφραγίδων μπλοκ καθώς και πότε δημιουργούνται τα μπλοκ.

Επιπλέον μια από τις λύσεις που προτείνει είναι η απαίτηση ασφαλών κόμβων να χρησιμοποιούν έμπιστους ομότιμους. Ωστόσο, η παραπάνω φιλοσοφία μετατρέπει τους ασφαλείς αυτούς κόμβους σε περισσότερο ευάλωτους, αφού τότε ο αριθμός αυτός των αξιόπιστων ομότιμων θα είναι περιορισμένος και συνεπώς το μικρό αυτό σύνολο των κόμβων πιο εύκολο να ανατραπεί. Το λεπτό σημείο αυτής της πρότασης είναι ότι με την παραπάνω μέθοδο, είναι ότι το σύστημα μας παύει να έχει πλήρως αποκεντρωμένη δομή, με την έννοια ότι απαιτείται πλέον εμπιστοσύνη και κατ’ επέκταση έλεγχος σε ένα υποσύνολο ομότιμων κόμβων, δημιουργώντας κατά κάποιο τρόπο ένα ελεγχόμενο υποδίκτυο.

Ακόμη, θα αναφέρουμε την τροποποίηση στο εύρος των χρονικών σφραγίδων μπλοκ. Έτσι για παράδειγμα ο χρόνος δικτύου του κόμβου σε σχέση με τον τρέχων κόμβο δικτύου θα μπορούσε να περιοριστεί από τις 2 ώρες στα 30 λεπτά. Κάτι τέτοιο θα άλλαζε το μέγιστο «παράθυρο» επίθεσης από 70 σε 140 λεπτά που είναι, να μειωνόταν σε 30 και 60 λεπτά.

4.6 Bribery attack

Ο έλεγχος της επίθεσης απαιτεί την προσφορά μεγαλύτερων ανταμοιβών εξόρυξης, έτσι ώστε να υπάρχει ένα υψηλό κίνητρο αντιδωροδοκίας, κάτι το οποίο στην πραγματικότητά είναι ιδιαίτερα δύσκολο. Έτσι μια προσπάθεια θα ήταν η απαίτηση της ανταμοιβής μπλοκ έστω b, να έχει ένα κατώτατο όριο έστω V, όπου V είναι το σύνολο των συναλλαγών σε κάθε μπλοκ τα οποία θα μπορούσαν να είναι χρήματα τα οποία ο

επιτιθέμενος επιδιώκει να διπλασιάσει (Bonneau, n.d.). Αυτό θα μεταφραζόταν στο γεγονός ότι το ποσοστό προμήθειας μιας συναλλαγής θα έπρεπε να ήταν 50%.

Με άλλα λόγια, η επίθεση αυτή μπορεί να αντιμετωπιστεί για παράδειγμα με τον περιορισμό του ποσού του bitcoin που στέλνει κάποιος κόμβος. Ο περιορισμός αυτός όπως έχει αναφερθεί διαμορφώνεται επηρεαζόμενος από το ποσό της ανταμοιβής μπλοκ. Έτσι αν το ποσό που διαθέτει ο επιτιθέμενος παραμένει σταθερό, μια πιθανή μείωση της ανταμοιβής θα αυξήσει την πιθανότητα επιτυχούς επίθεσης. Για τον λόγο αυτό σε κάποια κρυπτονομίσματα που έχουν το χαρακτηριστικό του "halving" και θα υπάρχει μείωση ανταμοιβής εξόρυξης, προτείνεται η ύπαρξη μηχανισμού (στο μοντέλο εξόρυξης) που θα προσαρμόζει το όριο (Ebrahimpour & Haghighi, 2021). Παρόλο αυτά, η παραπάνω πρόταση μειονεκτεί δεδομένου ότι ο επιτιθέμενος μεταφέρει bitcoin πολλές διευθύνσεις στο ίδιο μπλοκ. Μια λύση σε αυτό πρόβλημα, είναι ο περιορισμός των συνολικών ποσών συναλλαγής που στέλνονται σε κάθε μπλοκ. Με αυτή την έννοια, όπως και πριν θα πρέπει να υπάρχει ένας μηχανισμός για την προσαρμογή ορίου και ως λύση. Ωστόσο, μια τέτοια λύση θα πρέπει να λάβει υπόψη την συνθήκη στην οποία δεν υπάρχει ανταμοιβή μπλοκ και η μόνη ανταμοιβή να είναι η χρέωση συναλλαγής. Τέλος, θα πρέπει να σημειωθεί ότι για τις παραπάνω περιπτώσεις θα είναι απαραίτητη η ύπαρξη ενός "soft fork" επί της αλυσίδας.

Οι ανθρακωρύχοι θα έπρεπε να κινητοποιούνται ενάντια στα βραχυπρόθεσμα κέρδη τους, αφού μια τέτοια τακτική θα κατέστρεφε την μακροχρόνια δυνατότητα κερδών. Με άλλα λόγια, όλοι οι ανθρακωρύχοι μπορεί να αναγνωρίσουν ότι το μακροπρόθεσμο κοινό τους κίνητρο είναι ότι πρέπει να αρνηθούν να δεχθούν τις δωροδοκίες του εισβολέα και η κατεύθυνση των λύσεων σε ένα τέτοιο πρόβλημα θα πρέπει να είναι η ενίσχυση των κινήτρων σε σχέση με αυτά του εισβολέα, ώστε να μειώνουν το βραχυπρόθεσμο κέρδος του ανθρακωρύχου.

4.7 Hijack

Όσον αφορά στις επιθέσεις δικτύου αυτού του τύπου υπάρχουν τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα αντίμετρα. Αρχικά, ένα από τα σημαντικά μέτρα τα οποία θα μπορούσαμε να αναφέρουμε είναι η δημιουργία ποικιλομορφίας σχετικά με τις συνδέσεις των κόμβων. Με άλλα λόγια, όσες περισσότερες συνδέσεις έχει ένα αυτόματο σύστημα είναι όλο και πιο δύσκολο στο να «χτυπηθεί» από μια επίθεση. Για τον

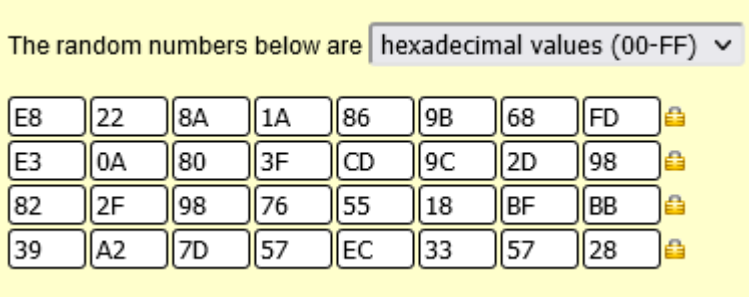
λόγο αυτό προτείνεται η πολλαπλή σύνδεση με διαφορετικά αυτόματα συστήματα για ένα κόμβο. Η παραπάνω προσέγγιση ελαχιστοποιεί τον κίνδυνο ο εισβολέας να μπορεί να υποκλέψει όλες τις συνδέσεις Το ίδιο αποτέλεσμα θα μπορούσε να επιτευχθεί ακόμη και σε κόμβο ο οποίος έχει σύνδεση με ένα AS με την χρήση VPN υπηρεσιών, μέσω κρυπτογραφημένων καναλιών. Με αυτό τον τρόπο, οι επιτιθέμενοι οι οποίοι θα αρνιόντουσαν συνδεσιμότητα μέσω των καναλιών θα πρέπει να γνώριζαν τις συσχετιζόμενες διευθύνσεις IP είτε διαφορετικά να διέκοπταν όλη την κρυπτογραφημένη κίνηση από και προς του κόμβους, γεγονός το οποίο κάνει αισθητό στο δίκτυο ότι δέχεται επίθεση.

Δεδομένου ότι σε κάποιες ομάδες ανθρακωρύχων (mining pools) χρησιμοποιούν “gateways” σε ένα συγκεκριμένο μόνο αυτόματο σύστημα (AS), για τον λόγο αυτό η χρήση των “gateways” θα γίνεται σε διαφορετικά αυτόματα συστήματα, γεγονός το οποίο θα δημιουργούσε μεγαλύτερη ανθεκτικότητα σχετικά με τις επιθέσεις δρομολόγησης.

Σχετικά τώρα με τα μακροπρόθεσμα μέτρα, προτείνεται η κρυπτογράφηση σχετικά με την επικοινωνία των bitcoin κόμβων για την μη τροποποίηση μηνυμάτων μεταξύ των κόμβων ή με την εφαρμογή ενός κωδικού ελέγχου ταυτότητας μηνυμάτων (MAC) για την επικύρωση του περιεχομένου κάθε μηνύματος ως προς την ακεραιότητα του, δυσκολεύοντας έτσι την πραγματοποίηση της επίθεσης “Delay”.

4.8 Sybil attack

Δεδομένου ότι στην επίθεση “Sybil” πραγματοποιείται πλαστογράφηση γνήσιων χρηστών, η φιλοσοφία αντιμετώπισης ενός τέτοιου κινδύνου θα έπρεπε να εστιάζει στην παρακολούθηση της συμπεριφοράς κάθε κόμβου και για την προκειμένη περίπτωση ενός κατανεμημένου δικτύου, όπως είναι αυτό του blockchain. Η δουλειά (Swathi et al., 2019) προτείνει να περιλαμβάνεται μια γεννήτρια διευθύνσεων για κάθε χρήστη στο δίκτυο του blockchain. Όπως είναι γνωστό, κάθε κόμβος στο blockchain δίκτυο έχει μια μοναδική διεύθυνση η οποία παράγεται στην εφαρμογή του πορτοφολιού και με αυτό τον τρόπο το αναγνωριστικό του χρήστη γίνεται μέσω αυτής διεύθυνσης. Θεωρούμε για παράδειγμα ότι η γεννήτρια παράγει ένα ιδιωτικό κλειδί με αποτέλεσμα της μορφής αυτής της παρακάτω εικόνα.



Εικόνα 57:παραγωγή ιδιωτικού κλειδιού από γεννήτρια

Στην προκειμένη περίπτωση δηλαδή ισχύει:
ΙδιωτικόΚλειδίHex=E8228A1A869B68FDE30A803FCD9C2D98822F98765518BFBB39A27D57EC335728

- Στην συνέχεια εφαρμόζεται η συνάρτηση κατακερματισμού για το ιδιωτικό κλειδί: $Hash_1$=sha256(Privatekey)=D1CAD9973CF7224DA6CFA456239E7B9B21AF2C51D87272311FB9EC00C590956F
- $Hash_2$=sha256($Hash_1$)=41C52FA863D4B50FC37A19D38CD33588725B0D3E14C63BFADEFECA5C4A7904A9
- Στο επόμενο βήμα παίρνουμε τα πρώτα 4 bytes ή τους 8 πρώτους χαρακτήρες της τιμής κατακερματισμού $Hash_2$. Έτσι λοιπόν ορίζουμε ως **checksum** την τιμή 41C52FA8 την οποία προσθέτουμε στο τέλος της τιμής του ιδιωτικού κλειδιού
- Στη συνέχεια, μετατρέπεται η τιμή checksum σε ένα αλφαριθμητικό base58, όπου αποτελεί την επιθυμητή μορφή του ιδιωτικού κλειδιού ως προς το πορτοφόλι bitcoin
- Θεωρούμε k το δημόσιο κλειδί και G ένα γεννήτορα σημείο στην ελλειπτική καμπύλη. Ορίζουμε ως K=k*G το δημόσιο κλειδί του χρήστη. Το δημόσιο κλειδί κατακερματίζεται με εφαρμογή του αλγορίθμου sha256, ενώ το αποτέλεσμα αυτού ξανακερματίζεται αυτή την φορά με τον αλγόριθμο RIPEMD-160. Τέλος, μετατρέπεται το τελευταίο αποτέλεσμα σε δυαδική τιμή, η οποία τελικά αντιστοιχεί στην **μοναδική διεύθυνση** του χρήστη.

Σχετικά με την προτεινόμενη λύση (Swathi et al., 2019), προτείνει την επέκταση της υπάρχουσας δομής μπλοκ στο blockchain με την μοναδική διεύθυνση του χρήστη να εμπεριέχεται στα συστατικά του μπλοκ. Το επόμενο χαρακτηριστικό της πρότασης αυτής είναι ότι κάθε κόμβος θα διαθέτει ένα πίνακα που θα καταγράφει ένα σύνολο στοιχείων

(φυσική διεύθυνση του κόμβου που προωθείται το μπλοκ, διεύθυνση ανθρακωρύχου, αριθμός μπλοκ, μετρητής). Αναλυτικότερα, τα στοιχεία του αριθμού μπλοκ και της διεύθυνσης του ανθρακωρύχου θα εντάσσονται στο τμήμα της κεφαλίδας μπλοκ, ενώ ο μετρητής αναφέρεται στον αριθμό των φορών που ο κόμβος προώθησης του μπλοκ έχει στείλει διαφορετικά μπλοκ για μια συγκεκριμένη διεύθυνση (ανθρακωρύχου).

Σε μια επίθεση Sybil υπάρχει το χαρακτηριστικό ότι ο κόμβος που δέχεται το μπλοκ (με διεύθυνση εισβολέα) λαμβάνει πολύ υψηλότερο αριθμό μπλοκ από τους κακόβουλους (Sybil) κόμβους, σε σχέση με τον κόμβο που λαμβάνει μπλοκ από ηθικούς κόμβους του δικτύου. Το παραπάνω γεγονός αποτελεί και την βάση της επίθεσης Sybil, διότι οι κακόβουλοι αυτοί κόμβοι ως μέρος της επίθεσης προωθούν στο δίκτυο μόνο μπλοκ επιτιθέμενου και παράλληλα απομονώνουν τα θεμιτά μπλοκ που παράγονται από τους νόμιμους χρήστες. Συνεπάγεται λοιπόν ότι και η διάδοση των κακόβουλών μπλοκ στους κόμβους του κατανεμημένου δικτύου θα είναι πολύ ταχύτερη. Ωστόσο με την εφαρμογή της πρότασης χρήσεως ενός πίνακα (που θα διαθέτει κάθε κόμβος) θα καταγραφεί η διαφορά στο ρυθμό λήψης μπλοκ από Sybil κόμβους και διεύθυνση αποστολής αυτού από εισβολέα. Συνεπώς κάθε κόμβος από την στιγμή που θα διαθέτει ένα τέτοιο πίνακα παρακολούθησης θα είναι σε θέση να εντοπίσει την επαναληπτικότητα μιας τέτοιας κατάστασης μέσω του μετρητή από τον πίνακα του.

Για την αντιμετώπιση και την πρόληψη των κινδύνων τέτοιων επιθέσεων προτείνεται στον προηγούμενο πίνακα καταγραφής η ύπαρξη κάποιου κατώτατου ορίου στο πεδίο του μετρητή ο οποίος μετρά τον αριθμό των φορών όπου κάποιος κόμβος προωθεί διαφορετικά μπλοκ με μια συγκεκριμένη διεύθυνση. Έτσι όταν παρατηρείται ότι από μια διεύθυνση ενός κόμβου-ανθρακωρύχου στέλνεται ένα πλήθος διαφορετικών μπλοκ και το πλήθος αυτό ξεπερνά το κατώτατο όριο που έχει τεθεί, η διεύθυνση αυτή θα εισέρχεται σε μια λίστα ύποπτων διευθύνσεων καθώς και τον αριθμό των κόμβων στους οποίους έχει προωθηθεί μπλοκ από αυτή την διεύθυνση (τον αριθμό των υπόπτων κόμβων). Αναλυτικότερα, η λίστα αυτή καταχωρεί την φυσική διεύθυνση που θεωρείται ύποπτη καθώς και το πλήθος των κόμβων που εντοπίζονται έχοντας την ύποπτη αυτή διεύθυνση. Θα πρέπει να τονιστεί ότι πρόκειται για μια κατανεμημένη λίστα που αφορά όλο το blockchain δίκτυο. Η φιλοσοφία της είναι η καταγραφή των διευθύνσεων των κόμβων που προωθούν το μπλοκ στο δίκτυο, ώστε να υπάρχει πλήρης παρακολούθηση των διευθύνσεων προκειμένου να διατηρείται η μοναδικότητα αυτών ως προς την αντιστοιχία τους με κόμβους.

Συνοψίζοντας, εάν λάβει κάποιος κόμβος ένα μπλοκ ελέγχει την διεύθυνση του ανθρακωρύχου που παρήγαγε το μπλοκ στην κεφαλίδα μπλοκ (η πρόσθετη πληροφορία της πρότασης που θα περιέχει το πεδίο κεφαλίδα μπλοκ) καθώς και μια φυσική διεύθυνση στη δημόσια διαθέσιμη λίστα προκειμένου να αποφασίσει σχετικά με την προώθηση αυτού του μπλοκ σε άλλους κόμβους. Έτσι όσο πιο μεγάλος είναι ο αριθμός των φορών που εμφανίζεται μια φυσική διεύθυνση κόμβου προώθησης μπλοκ στη δημόσια αυτή λίστα καταγραφής, τότε ο κόμβος για τον οποίο προορίζεται το μπλοκ θα το αναγνωρίζει ως μπλοκ που προέρχεται από Sybil κόμβο και ως εκ τούτου θα τον απορρίπτει. Ωστόσο σε αυτή την περίπτωση ο ύποπτος ανθρακωρύχος μπορεί να ξεφύγει από την δημόσια λίστα κάνοντας προώθηση του μπλοκ σε γνήσιους κόμβους (αντί για Sybil κόμβους). Έτσι όμως θα εντάσσεται η διεύθυνση των γνήσιων κόμβων στην δημοσία λίστα, δημιουργώντας τους πρόβλημα. Παρόλα αυτά η κατάσταση αυτή είναι μεταβλητή, με την έννοια ότι αν ένας νόμιμος ανθρακωρύχος έχει προστεθεί στην λίστα θα μπορεί να αποχωρήσει από αυτή αν κάνει την προώθηση του μπλοκ που παρήγαγε σε νόμιμους κόμβους.

4.9 Reentrancy attack (Smart contract attack)

Όπως έχει αναφερθεί, η επίθεση επανεισόδου σημαίνει ότι οι συναρτήσεις μπορούν να κληθούν επανειλημμένα πριν ακόμη ολοκληρωθεί η πρώτη κλήση της συνάρτησης. Έτσι το γεγονός αυτό ενδέχεται να οδηγήσει σε κακόβουλη δραστηριότητα. Η προσπάθεια έγκειται στο να μηδενιστεί το υπόλοιπο του έξυπνου συμβολαίου στόχου, ύστερα από αλλεπάλληλες λήψεις κεφαλαίων από το θύμα, μέσω της συνάρτησης “withdraw”. Στην παρακάτω εικόνα, έχουμε μια περίπτωση επανεισόδου, όπου για να γίνει πλήρως μηδενισμός του υπόλοιπου του “caller” θα πρέπει να εκτελεσθεί και η γραμμή 7. Μέχρι τότε, θα έχουμε τις συνεχόμενες αφαιρέσεις υπολοίπου (Mense & Flatscher, 2018). Ένα ακόμη πρόβλημα που πρέπει να αναφέρουμε στην συγκεκριμένη περίπτωση είναι η χρήση της κλήσης (call), διότι μέσω αυτής της συνάρτησης (από προεπιλογή) καταναλώνονται οι εισφορές οι οποίες απαιτούνται για την εκτέλεση μιας συναλλαγής Ethereum (κατανάλωση εισφορών gas), δημιουργώντας με αυτό τον τρόπο κατάλληλες συνθήκες για έναν εισβολέα, κατά την κλήση ενός εξωτερικού συμβολαίου.

Τέλος, μια ακόμη πρόταση για την αποφυγή μιας επίθεσης reentrancy είναι να πραγματοποιηθεί “call” με μια εξωτερική έξυπνη σύμβαση, αφού ολοκληρωθεί η εσωτερική εργασία.

```
1  contract Fund {
2      mapping(address => uint) shares;
3
4      function withdraw() public {
5          var share = shares[msg.sender];
6          shares[msg.sender] = 0;
7          msg.sender.transfer(share);
8      }
9  }
```

Εικόνα 58:Αντιμετώπιση ευπάθειας “Reentrancy”[29]

Στην προκειμένη περίπτωση, έχουμε αποφυγή του κώδικα της συνάρτησης call, προκειμένου να αποφευχθούν ανεπιθύμητα αποτελέσματα, διότι η συνάρτηση αυτή αναγκάζει τον εισβολέα να επικαλεστεί την “fallback” συνάρτηση η οποία καλεί την εναλλακτική “withdraw”, όπως είδαμε στο συμβόλαιο του επιτιθέμενου DAOAttacker.sol. Όπως φαίνεται στην παραπάνω εικόνα αρχικά θα πρέπει να υπάρχει ικανοποίηση συγκεκριμένης προϋπόθεσης (βλέπε γραμμή 6), ενώ στην συνέχεια γίνονται νέες επεμβάσεις στην κατάσταση της σύμβασης (βλέπε γραμμή 7) και μόνο μετά την ολοκλήρωση των παραπάνω θα είναι εφικτή η αλληλεπίδραση με εξωτερικά έξυπνα συμβόλαια.

4.10 Gasless send

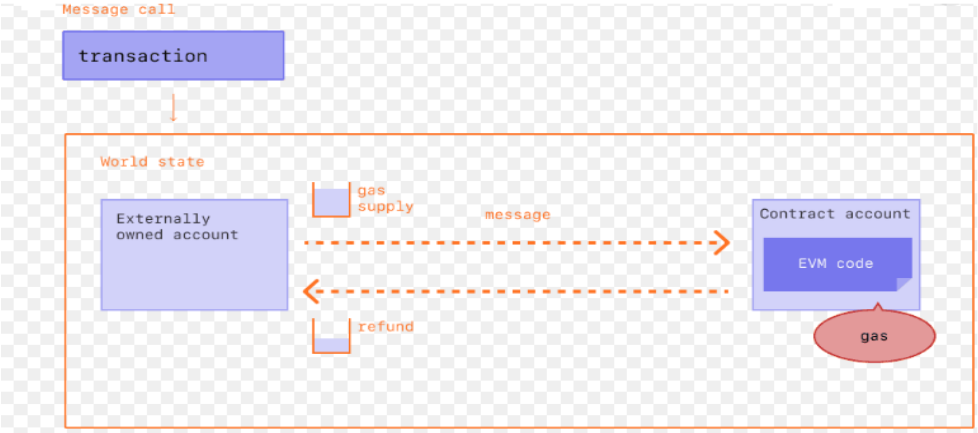
Σε μια άλλη ερμηνεία, η επίθεση αυτή κάνει μια συναλλαγή να αποτύχει, εάν δεν παρέχεται αρκετό ποσό “gas” έτσι ώστε να αρκεί για την πραγματοποίηση μιας συγκεκριμένης κλήσης. Έτσι λοιπόν, το μέγιστο όριο φυσικού αερίου (gas) που απαιτείται στο δίκτυο μπορεί να ποικίλλει με βάση τα τέλη συναλλαγής. Για τον λόγο αυτό θα πρέπει να τονίσουμε ότι θα μπορούσε να τεθεί κάποια εξαίρεση εάν μια αποτυχία βασίζεται στα

[29] https://dl.acm.org/doi/abs/10.1145/3282373.3282419

δεδομένα που σχετίζονται με την κατανάλωση του φυσικού αερίου. Για παράδειγμα, θα ήταν σημαντικό να οριστεί μια εξαίρεση εάν μια αποτυχία συσχετίζεται με το τι συμβαίνει στην κατανάλωση φυσικού αερίου. Με άλλα λόγια, προτείνεται να αναπτυχθούν λειτουργίες που δεν απαιτούν από ένα smart contract κάποια υψηλό ποσό "gas" ως εισφορά, μέτρο το οποίο θα αποσκοπεί και στην μείωση των τελών που θα πρέπει να πληρώνουν οι χρήστες.

4.11 Ether Lost

Υποθέτοντας ότι έχουμε ένα πραγματικό σενάριο, όπου ένας χρήστης έχει υπογράψει τρείς συναλλαγές με αντίστοιχα nonces 20, 21, 22. Θα πρέπει να σημειωθεί ότι στο Ethereum κάθε συναλλαγή έχει ένα nonce, το οποίο αναφέρεται στον αριθμό των συναλλαγών που αποστέλλονται από μια δεδομένη διεύθυνση. Όπως και στο bitcoin, κάθε φορά που στέλνεται μια συναλλαγή, η τιμή του nonce αυξάνεται κατά 1, και με βάση τους κανόνες τους οποίους θεσπίζει το nonce κρίνεται μια συναλλαγή ως έγκυρη ή μη. Επιπλέον, θεωρούμε ότι εξορύσσονται τα μπλοκ B_1, B_2, B_3 σχεδόν ταυτόχρονα, οπότε με βάση τον κανόνα του "longest chain", θα ακολουθήσει η διαδικασία της «αναδιοργάνωσης της αλυσίδας», κατά την οποία συμβαίνουν προσωρινές προσθήκες μπλοκ στην αλυσίδα προκειμένου να καταλήξουμε στο τελικό αποτέλεσμα της αλυσίδας. Για παράδειγμα, ας υποθέσουμε ότι έχουμε την διαδικασία της αναδιοργάνωσης της αλυσίδας για το μπλοκ B_3 με τα νέα μπλοκ που θα προκύψουν τελικά με την ολοκλήρωση της διαδικασίας να είναι B_2', B_3',B_4'. Αυτό το οποίο συνεπάγεται τελικά είναι ότι οι συναλλαγές που πραγματοποιούνται στα μπλοκ B_2, B_3 και δεν εμφανίζονται στα νεότερα μπλοκ B_2', B_3',B_4' δεν θα θεωρούνται ως εξορυσσόμενες, με τη έννοια ότι θα βρίσκονται σε μια μεταβατική φάση αναμονής για την ένταξη τους στη αλυσίδα των μπλοκ. Στην πραγματικότητα, οι συναλλαγές 21, 22 θεωρούνται εν δυνάμει εξορυσσόμενες και θεωρητικά μπορούν να προστεθούν σε επόμενα μπλοκ. Καταλήγοντας, οι συναλλαγές της "pending pool" (οι εν δυνάμει εξορυσσόμενες συναλλαγές) απορρίπτονται. Ο χρήστης θα πρέπει να επιθεωρήσει την "pending pool" και να τις να τις ξαναεντάξει, σε περίπτωση που έχουν εξαφανιστεί.



Εικόνα 59:Διαδικασία συναλλαγής στο Ethereum[30]

Το ερώτημα όμως που γεννάται είναι ο χρόνος που χρειάζεται να περιμένουμε, προκειμένου να ξαναπραγματοποιήσουμε μια συναλλαγή ether. Η απάντηση σε αυτό είναι ότι εξαρτάται από την διεργασία που απαιτείται εντός της "pending pool". Για παράδειγμα, η αύξηση της τιμής gas θα μπορούσε να βοηθήσει για να ενταχθεί η συναλλαγή και να μην απορριφθεί από το δίκτυο. Εναλλακτικά, προτείνεται μια περιοδική προσπάθεια μέχρις ότου η συναλλαγή ενσωματωθεί από το δίκτυο.

4.12 Refund Attack

Ως πρόταση κατά της επίθεσης επιστροφής χρημάτων είναι να παρέχεται στον πωλητή ένα δημόσια επαληθεύσιμο αποδεικτικό στοιχείο το οποίο θα μπορεί να αποδείξει κρυπτογραφικά την λήψη της διεύθυνσης επιστροφής χρημάτων, η οποία θα έχει εγκριθεί από τον ίδιο τον αγοραστή (πελάτη) που εξουσιοδότησε την πληρωμή. Με άλλα λόγια, σκοπός αυτής της πρότασης είναι το να εμποδιστεί η επίθεση, ζητώντας από τον αγοραστή να εγκρίνει την διεύθυνση επιστροφής χρημάτων του, κάνοντας χρήση του κλειδιού που επαλήθευσε την συναλλαγή.

[30] Ανακτήθηκε από: https://ethereum.org/en/developers/docs/transactions/

5 Επίλογος

5.1 Συνεισφορά

Η τεχνολογία blockchain είναι μια ενδιαφέρουσα αλλά και περίπλοκη τεχνολογία λόγω των μηχανισμών λειτουργίας της. Συνοπτικά, η βασική ιδέα πίσω από το blockchain είναι να αποκεντρωθεί η αποθήκευση δεδομένων σε ένα P2P δίκτυο με τρόπο που να μην υπάρχει μια ενιαία κεντρική αρχή που να ελέγχει ολόκληρο το δίκτυο. Η φιλοσοφία αυτή παρέχει επαρκές επίπεδο ασφάλειας και ιδιωτικότητας, γεγονός που έχει προκαλέσει μεγάλη απήχηση στον τεχνολογικό κόσμο. Παρόλο που το blockchain προσφέρει αδιαμφισβήτητα πολύ σημαντικά χαρακτηριστικά σε επίπεδο ιδιωτικότητας, διαφάνειας αποκέντρωσης και ευρύτερα ασφάλειας, διάφορες ευπάθειες προκαλούν σημαντικά προβλήματα στο οικοσύστημα blockchain.

Η μελέτη αυτή επικεντρώθηκε στην τεχνολογία blockchain υπό το πρίσμα της ασφάλειας δίνοντας έμφαση στην κατανόηση όλων αυτών των ιδιαίτερων χαρακτηριστικών που διακρίνει την αποκεντρωμένη αρχιτεκτονική της τεχνολογίας blockchain, όπως είναι η ακεραιότητα, ανωνυμία η ανιχνευσιμότητα κ.α.. Αρχικά, κάναμε μια εισαγωγή στα χαρακτηριστικά, την δομή, τα μοντέλα συναίνεσης. Επιπλέον έγινε η απαραίτητη σύνδεση της τεχνολογίας με το τομέα του “Cyber security” και την ικανοποίηση των αρχών της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, αλλά και μια ανάλυση της κρυπτογραφίας που εφαρμόζεται, όπως την κρυπτογραφία του δημοσίου κλειδιού (ασύμμετρη κρυπτογραφία) και της ελλειπτικής καμπύλης.

Όσον αφορά την μελέτη των επιθέσεων, πραγματοποιήθηκε στο πλαίσιο τριών βασικών αξόνων οι οποίοι αποτελούνται από διάφορες υποκατηγορίες επιθέσεων προκειμένου να κατανοηθούν οι ευπάθειες με βάση ομοιότητες των επιθέσεων ή συγκριτικά κριτήρια τα οποία ενδέχεται να κινητοποιήσουν ένα εισβολέα να πραγματοποιήσει μια επίθεση σε δημόσια blockchain. Συγκεκριμένα, η αρχική κατηγοριοποίηση με βάση το είδος ταξινομεί 39 επιθέσεις διαιρούμενες συνολικά σε 6 διαφορετικές κατηγορίες, επεξηγώντας την ευρύτερη κατηγορία στην οποία είναι ενταγμένες. Ακολουθεί μια επιπλέον κατηγοριοποίηση των επιθέσεων που έχουν αναλυθεί με βάση το επίπεδο αφαίρεσης Blockchain που αφορούν. Τέλος πραγματοποιείται κατηγοριοποίηση με βάση τον πιο σημαντικό μηχανισμό στο blockchain αυτόν του αλγορίθμου συναίνεσης, ο οποίος είναι υπεύθυνος για την ομαλή λειτουργία

της τεχνολογίας, ενώ επηρεάζονται κάθε φορά (ανάλογα με την εφαρμογή του αλγορίθμου) διάφοροι παράγοντες που αφορούν άμεσα τον επιτιθέμενο αφού θα πρέπει να «ζυγίσει» για παράδειγμα το κόστος που θα υπάρχει για αυτόν προκειμένου να πραγματοποιήσει επιτυχώς μια επίθεση, την ανοχή σε σφάλμα που μπορεί να υπάρξει ή την δυνατότητα δημιουργίας διακλάδωσης ανάλογα με τον αλγόριθμο συναίνεσης που εφαρμόζεται κάθε φορά. Στην συγκεκριμένη κατηγοριοποίησή πραγματοποιείται ανάλυση επιπλέον επιθέσεων που σχετίζονται μόνο με συγκεκριμένα μοντέλα συναίνεσης. Συνεπώς γίνεται μια σύγκριση διάφορων κριτηρίων τα οποία είναι σημαντικά για ένα επιτιθέμενο προκειμένου να υπάρχει θετική ή όχι έκβαση μιας επίθεσης. Καταλήγοντας, προτείνονται ενδεικτικές λύσεις σε ορισμένες σημαντικές επιθέσεις, ενώ μέσω ενός συγκεντρωτικού πίνακα γίνεται αναφορά για κάθε επίθεση ξεχωριστά ο τομέας λειτουργίας που επηρεάζει καθώς και την αρνητική επίδραση που επιφέρει, έτσι ώστε να αποτυπωθούν και μέσω αυτού κοινά σημεία και διαφορές μεταξύ των επιθέσεων. Συνεπώς μελετώνται πολύπλευρα και από διάφορες προοπτικές οι υπάρχουσες επιθέσεις, βοηθώντας στην καλύτερη κατανόηση τους, αλλά και σε τυχόν κίνητρα που έχει ένας επιτιθέμενος ή στόχους που πρέπει να υπερβεί προκειμένου να επιτύχει μια επίθεση.

5.2 Μελλοντικές επεκτάσεις

Πρωτόκολλο επικοινωνίας: Οι τυχόν παρεμβολές στην επικοινωνία των κόμβων, επηρεάζει την διαδικασία συναίνεσης αποσκοπώντας στην αποκόμιση οφέλους. Σε συνθήκες πραγματικής επίθεσης οι επιτιθέμενοι λαμβάνουν πληροφορίες όπως η καθυστέρηση επικοινωνίας στους κόμβους, την διαμονή των ανταμοιβών στους κόμβους που δημιουργούν κάποιο νέο μπλοκ ή να υπολογίσουν το κόστος επίθεσης. Συνεπώς ένας εισβολέας προσπαθεί να συνυπολογίσει ένα πλήθος παραγόντων προκειμένου να κρίνει ότι θα προβεί στην πραγματοποίηση μιας επίθεσης. Αντίστοιχα η μεθοδολογία άμυνας μιας επίθεσης στο πρωτόκολλο επικοινωνίας δικτύου θα βασίζεται στην εξαγωγή ενός πλήθους χαρακτηριστικών και δεδομένων επικοινωνίας. Επειδή μια τέτοια μεθοδολογία, αναλύει ολόκληρο το πρωτόκολλο επικοινωνίας, αδυνατώντας με αυτό τον τρόπο να εστιάσει στην «συμπεριφορά» ενός μεμονωμένου κόμβου, ο εντοπισμός κακόβουλων κόμβων που εκτοξεύουν την επίθεση επικοινωνίας δικτύου δεν είναι εύκολος. Για τον λόγο αυτό, η εφαρμογή **μηχανικής μάθησης** θα ήταν μια λύση για την περαιτέρω

ανάπτυξη των μεθόδων μελέτης υπολογισμού δεδομένων καθώς και μεθόδων άμυνας στις επιθέσεις πρωτοκόλλου επικοινωνίας, ως προς εντοπισμό κακόβουλων κόμβων.

Smart contracts: Η μέθοδος άμυνας σε μια επίθεση έξυπνου συμβολαίου, εντοπίζει την ύπαρξη τρωτών σημείων με βάση τα χαρακτηριστικά της ευπάθειας. Ωστόσο η μέθοδος αυτή θα μπορούσε να προσθέσει μοντέλα τα οποία θα επεξεργάζονται χαρακτηριστικά προσομοιώνοντας σενάρια προβλημάτων τα οποία μειώνουν σε ορισμένο βαθμό την αποτελεσματικότητα ανίχνευσης τρωτών σημείων. Κάτι τέτοιο θα μπορούσε να συνεισφέρει στην δημιουργία νέων σημαντικών μεθόδων σε επιθέσεις έξυπνων συμβολαίων αναβαθμίζοντας την αποτελεσματικότητα στην ανίχνευση τρωτών σημείων.

Παράλληλη εξόρυξη: Η παράλληλη εκτέλεση συναλλαγών κατά το χρόνο εκτέλεσης θα μπορούσε να αποτελέσει μια βελτιωμένη μέθοδο ως προς την διαδικασία της δημιουργίας μπλοκ και την επαλήθευση των συναλλαγών. Ειδικότερα, μέσω της παράλληλης εκτέλεσης της εξόρυξης θα μπορούσε να μειωθεί η πιθανότητα οι κακόβουλοι ανθρακωρύχοι να καταστρέψουν τα περιουσιακά στοιχεία (κάποιο κρυπτονόμισμα) που βρίσκονται στην ουρά μιας «δεξαμενής εξόρυξης» (mining pool), επειδή οι συναλλαγές θα μπορούν να εκτελούνται ταυτόχρονα σε αυτή.

Κβαντική αλυσίδα μπλοκ: Η ενίσχυση της ασφάλειας του blockchain θα μπορούσε να επιτευχθεί με την εφαρμογή κβαντικής κρυπτογραφίας. Ειδικότερα, το κατανεμημένο δίκτυο θα βασίζεται σε ένα κβαντικό κλειδί. Ως εκ τούτου οι συμμετέχοντες στο δίκτυο θα μπορούν με ασφάλεια τα κλειδιά επικυρώνοντας ο ένας κόμβος τον άλλο, προστατεύοντας με αυτό τον τρόπο την επικοινωνία στο δίκτυο. Έτσι σε μια περίπτωση όπου το blockchain δίκτυο αποτελείται από κβαντικούς υπολογιστές, οι συναλλαγές blockchain θα μεταδίδονται χρησιμοποιώντας κβαντική τηλεμεταφορά κάνοντας πού δύσκολη την επίτευξη οποιαδήποτε επίθεσης δεδομένου ότι θεωρείται η κλωνοποίηση κβαντικής πληροφορίας.

Βιβλιογραφία

Alkhalifah, A., Ng, A., Kayes, A. S. M., Chowdhury, J., Alazab, M., & Watters, P. (2019). *A Taxonomy of Blockchain Threats and Vulnerabilities* [Preprint]. MATHEMATICS & COMPUTER SCIENCE. https://doi.org/10.20944/preprints201909.0117.v1

Alladi, T., Chamola, V., Parizi, R. M., & Choo, K.-K. R. (2019). Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. *IEEE Access*, *7*, 176935–176951. https://doi.org/10.1109/ACCESS.2019.2956748

Anita., N., & Vijayalakshmi., M. (2019). Blockchain Security Attack: A Brief Survey. *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–6. Kanpur, India: IEEE. https://doi.org/10.1109/ICCCNT45670.2019.8944615

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. *2017 IEEE Symposium on Security and Privacy (SP)*, 375–392. San Jose, CA, USA: IEEE. https://doi.org/10.1109/SP.2017.29

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In M. Maffei & M. Ryan (Eds.), *Principles of Security and Trust* (Vol. 10204, pp. 164–186). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-54455-6_8

Averin, A., & Averina, O. (2019). Review of Blockchain Technology Vulnerabilities and Blockchain-System Attacks. *2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 1–6. Vladivostok, Russia: IEEE. https://doi.org/10.1109/FarEastCon.2019.8934243

Axon, L., & Goldsmith, M. (2017). PB-PKI: A Privacy-aware Blockchain-based PKI: *Proceedings of the 14th International Joint Conference on E-Business and Telecommunications*, 311–318. Madrid, Spain: SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0006419203110318

Begum, A., Tareq, A. H., Sultana, M., Sohel, M. K., Rahman, T., & Sarwar, A. H. (2020). Blockchain Attacks, Analysis and a Model to Solve Double Spending Attack. *International Journal of Machine Learning and Computing*, *10*(2), 6.

Bips/bip-0070.mediawiki at master · bitcoin/bips · GitHub. (n.d.). Retrieved January 26, 2021, from https://github.com/bitcoin/bips/blob/master/bip-0070.mediawiki

Bitcoin Mining Pools Targeted in Wave of DDOS Attacks. (n.d.). Retrieved January 27, 2021, from https://www.coindesk.com/markets/2015/03/12/bitcoin-mining-pools-targeted-in-wave-of-ddos-attacks/

Bonneau, J. (n.d.). *Why buy when you can rent?* 8.

Buterin, V. (n.d.). *A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM*. 36.

Chepurnoy, A., Papamanthou, C., Zhang, Y., & Srinivasan, S. (n.d.). *EDRAX: A Cryptocurrency with Stateless Transaction Validation*. 18.

Cheung, A. (Wai-K., Roca, E., & Su, J.-J. (2015). Crypto-currency bubbles: An application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. *Applied Economics*, *47*(23), 2348–2358. https://doi.org/10.1080/00036846.2015.1005827

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018). Blockchain Versus Database: A Critical Analysis. *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), 1348–1353. New York, NY, USA: IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00186

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Collomb, A., & Sok, K. (2016). *Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector?* (103), 20.

Conti, M., Sandeep Kumar, E., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460

Coron, J.-S., Dodis, Y., Malinaud, C., & Puniya, P. (2005). Merkle-Damgård Revisited: How to Construct a Hash Function. In V. Shoup (Ed.), *Advances in Cryptology – CRYPTO 2005* (pp. 430–448). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/11535218_26

Crosby, M. (2016). *BlockChain Technology: Beyond Bitcoin*. (2), 16.

Cui, Y., Pan, B., & Sun, Y. (2019). A Survey of Privacy-Preserving Techniques for Blockchain. In X. Sun, Z. Pan, & E. Bertino (Eds.), *Artificial Intelligence and Security* (pp. 225–234). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-24268-8_21

culubas: Timejacking & Bitcoin. (n.d.). Retrieved January 26, 2021, from https://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html

Dannen, C. (2017). *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-2535-6

Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from security perspective. *Journal of Banking and Financial Technology*, *3*(1), 1–17. https://doi.org/10.1007/s42786-018-00002-6

Davenport, A., Shetty, S., & Liang, X. (2018). Attack Surface Analysis of Permissioned Blockchain Platforms for Smart Cities. *2018 IEEE International Smart Cities Conference (ISC2)*, 1–6. Kansas City, MO, USA: IEEE. https://doi.org/10.1109/ISC2.2018.8656983

Decker, C., & Wattenhofer, R. (2014). Bitcoin Transaction Malleability and MtGox. In M. Kutyłowski & J. Vaidya (Eds.), *Computer Security—ESORICS 2014* (pp. 313–326). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-11212-1_18

Deirmentzoglou, E., Papakyriakopoulos, G., & Patsakis, C. (2019). A Survey on Long-Range Attacks for Proof of Stake Protocols. *IEEE Access*, *7*, 28712–28725. https://doi.org/10.1109/ACCESS.2019.2901858

Denial-of-service attack—Wikipedia. (n.d.). Retrieved January 26, 2021, from https://en.wikipedia.org/wiki/Denial-of-service_attack

Dika, A. (n.d.). *Ethereum Smart Contracts: Security Vulnerabilities and Security Tools*. 97.

Dika, A., & Nowostawski, M. (2018). Security Vulnerabilities in Ethereum Smart Contracts. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 955–962. Halifax, NS, Canada: IEEE. https://doi.org/10.1109/Cybermatics_2018.2018.00182

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, *30*(7), 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K.-L. (2017). BLOCKBENCH: A Framework for Analyzing Private Blockchains. *Proceedings of the 2017 ACM International Conference on Management of Data*, 1085–1100. Chicago Illinois USA: ACM. https://doi.org/10.1145/3035918.3064033

Ebrahimpour, G., & Haghighi, M. S. (2021). Analysis of Bitcoin Vulnerability to Bribery Attacks Launched Through Large Transactions. *ArXiv:2105.07501 [Cs]*. Retrieved from http://arxiv.org/abs/2105.07501

Eclipse Attacks Explained: What Are They? | Gemini. (n.d.). Retrieved January 26, 2021, from https://www.gemini.com/cryptopedia/eclipse-attacks-defense-bitcoin

Ferdous, S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. (n.d.). *Blockchain Consensus Algorithms: A Survey*. 39.

Goldfeder, S., Gennaro, R., & Kalodner, H. (n.d.). *Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme*. 26.

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (n.d.). *Eclipse Attacks on Bitcoin's Peer-to-Peer Network*. 18.

How Does Ethereum Staking Work? (n.d.). Retrieved January 27, 2021, from https://finance.yahoo.com/news/does-ethereum-staking-173615797.html

How Hackers Can Exploit Weak ECDSA Signatures. (n.d.). Retrieved January 27, 2021, from https://halborn.com/how-hackers-can-exploit-weak-ecdsa-signatures/

Iuon-Chang Lin & Tzu-Chun Liao. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, *19*(5). https://doi.org/10.6633/IJNS.201709.19(5).01

Karame, G. (2016). On the Security and Scalability of Bitcoin's Blockchain. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1861–1862. Vienna Austria: ACM. https://doi.org/10.1145/2976749.2976756

Kaur, S., Chaturvedi, S., Sharma, A., & Kar, J. (2021). A Research Survey on Applications of Consensus Protocols in Blockchain. *Security and Communication Networks*, *2021*, 1–22. https://doi.org/10.1155/2021/6693731

Kearney, J. J. (n.d.). *Blockchain Technologies Vulnerability to Quantum Attacks*. 24.

Koteska, B., Karafiloski, E., & Mishev, A. (n.d.). *Blockchain Implementation Quality Challenges: A Literature Review*. 8.

Kutyłowski, M., & Vaidya, J. (Eds.). (2014). *Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-11212-1

Li, M., Weng, J., Yang, A., Lu, W., Zhang, Y., Hou, L., … Deng, R. H. (2019). CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing. *IEEE Transactions on Parallel and Distributed Systems*, *30*(6), 1251–1266. https://doi.org/10.1109/TPDS.2018.2881735

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*, S0167739X17318332. https://doi.org/10.1016/j.future.2017.08.020

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020

Liu, Q., Xu, Y., Cao, B., Zhang, L., & Peng, M. (2021). Unintentional forking analysis in wireless blockchain networks. *Digital Communications and Networks*, *7*(3), 335–341. https://doi.org/10.1016/j.dcan.2020.12.005

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). Refund Attacks on Bitcoin's Payment Protocol. In J. Grossklags & B. Preneel (Eds.), *Financial Cryptography and Data Security* (pp. 581–599). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-54970-4_34

Mense, A., & Flatscher, M. (2018). Security Vulnerabilities in Ethereum Smart Contracts. *Proceedings of the 20th International Conference on Information Integration and Web-Based Applications & Services*, 375–380. Yogyakarta Indonesia: ACM. https://doi.org/10.1145/3282373.3282419

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2567–2572. Banff, AB: IEEE. https://doi.org/10.1109/SMC.2017.8123011

Möser, M. (n.d.). *Anonymity of Bitcoin Transactions*. 10.

Natoli, C., & Gramoli, V. (2016). The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example. *ArXiv:1612.09426 [Cs]*. Retrieved from http://arxiv.org/abs/1612.09426

Nguyen, P. Q., & Zhou, J. (Eds.). (2017). *Information Security*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-69659-1

Nothing at stake in Proof of Stake (PoS)—DLT-Repo. (n.d.). Retrieved January 27, 2021, from https://dlt-repo.net/nothing-at-stake-in-proof-of-stake-pos/

Pérez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2019). Double-Spending Prevention for Bitcoin Zero-Confirmation Transactions. *International Journal of Information Security*, *18*(4), 451–463. https://doi.org/10.1007/s10207-018-0422-4

Praitheeshan, P., Pan, L., Yu, J., Liu, J., & Doss, R. (2020). Security Analysis Methods on Ethereum Smart Contract Vulnerabilities: A Survey. *ArXiv:1908.08605 [Cs]*. Retrieved from http://arxiv.org/abs/1908.08605

Prashanth Joshi, A., Han, M., Wang, Y., & ,Kennesaw State University, Marietta, GA 30060, USA. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, *1*(2), 121–147. https://doi.org/10.3934/mfc.2018007

Putri, M. C. I., Sukarno, P., & Wardana, A. A. (2020). Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on web application. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, *6*(2), 74. https://doi.org/10.26594/register.v6i2.1932

Rajput, U., Abbas, F., & Oh, H. (2018). A Solution towards Eliminating Transaction Malleability in Bitcoin. *Journal of Information Processing Systems*, *14*(4), 837–850. https://doi.org/10.3745/JIPS.03.0101

Rathod, N., & Motwani, D. (2018). *Security threats on Blockchain and its countermeasures*. *05*(11), 7.

Reisman, R. (2019). Blockchain Serverless Public/Private Key Infrastructure for ADS-B Security, Authentication, and Privacy. *AIAA Scitech 2019 Forum*. Presented at the

AIAA Scitech 2019 Forum, San Diego, California. https://doi.org/10.2514/6.2019-2203

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046

Romano, D., & Schmid, G. (2017). Beyond Bitcoin: A Critical Look at Blockchain-Based Systems. *Cryptography, 1*(2), 15. https://doi.org/10.3390/cryptography1020015

Saad, M., Kim, J., Nyang, D., & Mohaisen, D. (2021). Contra-∗: Mechanisms for countering spam attacks on blockchain's memory pools. *Journal of Network and Computer Applications, 179*, 102971. https://doi.org/10.1016/j.jnca.2020.102971

Saad, M., Njilla, L., Kamhoua, C. A., Kwiat, K., & Mohaisen, A. (2019). Blockchain for Distributed Systems Security. In S. Shetty, C. Kamhoua, & L. Njilla (Eds.), *Blockchain for Distributed Systems Security* (1st ed., pp. 205–232). Wiley. https://doi.org/10.1002/9781119519621.ch10

Saad, M., Njilla, L., Kamhoua, C., Kim, J., Nyang, D., & Mohaisen, A. (2019). Mempool optimization for Defending Against DDoS Attacks in PoW-based Blockchain Systems. *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 285–292. Seoul, Korea (South): IEEE. https://doi.org/10.1109/BLOC.2019.8751476

Saad, M., Njilla, L., Kamhoua, C., & Mohaisen, A. (2019). Countering Selfish Mining in Blockchains. *2019 International Conference on Computing, Networking and Communications (ICNC)*, 360–364. Honolulu, HI, USA: IEEE. https://doi.org/10.1109/ICCNC.2019.8685577

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C. A., Nyang, D., & Mohaisen, A. (2019). Overview of Attack Surfaces in Blockchain. In S. Shetty, C. Kamhoua, & L. Njilla

(Eds.), *Blockchain for Distributed Systems Security* (1st ed., pp. 51–66). Wiley. https://doi.org/10.1002/9781119519621.ch3

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020). Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *22*(3), 1977–2008. https://doi.org/10.1109/COMST.2020.2975999

Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys & Tutorials*, *21*(1), 858–880. https://doi.org/10.1109/COMST.2018.2863956

Samreen, N. F., & Alalfi, M. H. (2021). A Survey of Security Vulnerabilities in Ethereum Smart Contracts. *ArXiv:2105.06974 [Cs]*. Retrieved from http://arxiv.org/abs/2105.06974

Shetty, S. S., Kamhoua, C. A., & Njilla, L. L. (2019). *Blockchain for Distributed Systems Security*. Retrieved from http://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9781119519591

Shrivas, M. K., Dean, T. Y., & Brunda, S. S. (2020). The Disruptive Blockchain Security Threats and Threat Categorization. *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*, 327–338. Raipur, India: IEEE. https://doi.org/10.1109/ICPC2T48082.2020.9071475

Sifra, E. M., & Wu, G. (n.d.). *Security Vulnerabilities of Blockchain-Based Smart Contracts and Countermeasures: A Survey*. 16.

Singhal, B., Dhameja, G., & Panda, P. S. (2018). *Beginning Blockchain*. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-3444-0

Staderini, M., Palli, C., & Bondavalli, A. (2020). Classification of Ethereum Vulnerabilities and their Propagations. *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, 44–51. Antalya, Turkey: IEEE. https://doi.org/10.1109/BCCA50787.2020.9274458

Stetsenko, P. I., Khalimov, G. Z., & Kotukh, E. V. (2020). Analysis of planes of attacks on the Blockchain system. *Radiotekhnika*, *1*(200), 114–121. https://doi.org/10.30837/rt.2020.1.200.10

Swan, M. (2015). *Blockchain: Blueprint for a new economy* (First edition). Beijing : Sebastopol, CA: O'Reilly.

Swathi, P., Modi, C., & Patel, D. (2019). Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners. *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–6. Kanpur, India: IEEE. https://doi.org/10.1109/ICCCNT45670.2019.8944507

Tareq, A. H. (n.d.). *Blockchain Attacks and A Model for Double Spending Attack*. 36.

The DAO Attacked: Code Issue Leads to $60 Million Ether Theft—CoinDesk. (n.d.). Retrieved January 25, 2021, from https://www.coindesk.com/markets/2016/06/17/the-dao-attacked-code-issue-leads-to-60-million-ether-theft/

Vasin, P. (n.d.). *BlackCoin's Proof-of-Stake Protocol v2*. 2.

Vokerla, R. R., Shanmugam, B., Azam, S., Karim, A., Boer, F. D., Jonkman, M., & Faisal, F. (2019). An Overview of Blockchain Applications and Attacks. *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, 1–6. Vellore, India: IEEE. https://doi.org/10.1109/ViTECoN.2019.8899450

Wang, X., Chen, Y., & Zhang, Q. (2021). Incentivizing cooperative relay in UTXO-based blockchain network. *Computer Networks*, *185*, 107631. https://doi.org/10.1016/j.comnet.2020.107631

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview* (No. NIST IR 8202; p. NIST IR 8202). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Yun, X., Wen, W., Lang, B., Yan, H., Ding, L., Li, J., & Zhou, Y. (Eds.). (2019). *Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, August 14–16, 2018, Revised Selected Papers*. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-13-6621-5

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (n.d.). *Blockchain challenges and opportunities: A survey*. 24.

Συγκεντρωτικός πίνακας επιθέσεων

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
51% attack	Έλεγχος περισσότερο από το 50% της συνολικής ισχύς κατακερματισμού του δικτύου blockchain	Δίκτυο blockchain, ανθρακωρύχους (εξόρυξη), Ανταλλακτήρια νομισμάτων, Χρήστες(πωλητές, έμποροι)	Η επίθεση 51% αποτελεί τη χειρότερη περίπτωση για το Blockchain δίκτυο
Double Spending	Ο χρήστης πραγματοποιεί παραπάνω από μια συναλλαγή, χρησιμοποιώντας/ξοδεύοντας το ίδιο ακριβώς κεφάλαιο	Πωλητές, εμπόρους	Ο πωλητής μπορεί να χάσει το προϊόν πώλησης από κακόβουλο χρήστη, δημιουργία διακλάδωσης στην αλυσίδα
Finney attack	Μορφή διπλής δαπάνης, όπου ο επιτιθέμενος ανθρακωρύχος πραγματοποιεί κρυφά εξόρυξη μπλοκ για να το μεταδώσει στο δίκτυο με σκοπό την δημιουργία διπλής δαπάνης	Πωλητές, εμπόρους	Ο έμπορος να μην λάβει υπηρεσίες για τις έχει πληρώσει

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Vector 76	Είναι τύπου “one confirmation” επίθεση, ο επιτιθέμενος δεν χρειάζεται να εξορύξει 2 συνεχόμενα μπλοκ. Ο εισβολέας δημιουργεί νέο μπλοκ χωρίς να το δημοσιεύσεις στέλνοντας συναλλαγή στον κόμβο στόχο, διπλής δαπάνης. Αποτελεί συνδυασμό double spending και Finney attack.	Ανταλλακτήρια νομισμάτων	Ευνοείται η δημιουργία συναλλαγής διπλής δαπάνης
DDOS	Ένα σύνολο ανθρακωρύχων προσπαθεί να διαταράξει το μέγεθος ενός mempool, μειώνοντας το τέλος εξόρυξης (σπατάλη υπολογιστικών πόρων). **Πιο ευάλωτο το μοντέλο συναίνεσης PoW**	Δίκτυο blockchain, ανθρακωρύχους	Άρνηση υπηρεσιών σε ειλικρινούς κόμβους (απομόνωση τους από το δίκτυο)

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Race attack	Εκμετάλλευση χρονικού διαστήματος μεταξύ δημιουργίας συναλλαγής και επιβεβαίωσης της με την αποστολή 2 συναλλαγών από τον επιτιθέμενο (αυθεντική, ψεύτικη), όπου η αυθεντική δεν επιβεβαιώνεται ποτέ.	Πωλητές, εμπόρους	Τελικός στόχος επίθεσης η δημιουργία διπλής δαπάνης
Selfish Mining	Κακόβουλος ανθρακωρύχος διατηρεί ιδιωτικά μπλοκ και δημιουργεί διακλάδωση στην οποία τα εντάσσει.	Ειλικρινείς ανθρακωρύχοι (εξόρυξη)	Σπατάλη υπολογιστικής ισχύς έντιμων ανθρακωρύχων, Σπατάλη της εξορυκτικής ισχύς ειλικρινών ανθρακωρύχων (>50%) προκαλεί Goldfinger attack

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Eclipse attack	Ο κόμβος θύμα απομονώνεται από το υπόλοιπο δίκτυο και χειραγωγείται από τον εισβολέα. Οι κόμβοι στόχοι γίνονται αποδέκτες των εισερχόμενων συνδέσεων που στέλνουν οι επιτιθέμενοι. **Πιο ευάλωτο το μοντέλο συναίνεσης PoW**	Ανθρακωρύχοι, απλοί συμμετέχοντες κόμβοι στο δίκτυο	Ο ανθρακωρύχος είναι σε θέση να εξαπολύσει επίθεση 51%, ακόμη και με μικρότερη ισχύς εξόρυξης στην κατοχή του από αυτό το ποσοστό.
Refund attack	Ο επιτιθέμενος χρησιμοποιεί ευνοϊκές πολιτικές(ευπάθεια ελέγχου ταυτότητας, πολιτικές επιστροφής χρημάτων διεκπεραιωτών πληρωμών)	Πωλητές, εμπόρους Ανταλλακτήρια νομισμάτων	Απώλεια χρημάτων, αξιοπιστία ανταλλακτηρίου
Time jacking	Ο επιτιθέμενος μεταβάλλει την χρονική σήμανση ενός κόμβου στο δίκτυο, ώστε να δεχθεί ένα εναλλακτικό (κακόβουλο) blockchain	Ανθρακωρύχους (εξόρυξη)	Απομονώνει τον ανθρακωρύχο θύμα καταναλώνοντας τους εξορυκτικούς τους πόρους, επηρεάζει τον ορισμό της τιμής “difficulty” ως προς την εξόρυξη νέων κόμβων

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Bribery attack	Ο επιτιθέμενος δωροδοκεί ανθρακωρύχο με σκοπό να πραγματοποιεί την διαδικασία της εξόρυξης αντί για αυτόν	Ανθρακωρύχους (εξόρυξη), πωλητές έμποροι	Αυξάνει την πιθανότητα πρόκλησης επίθεσης “double spending” ή “block withholding”
Transaction Malleability	Ο επιτιθέμενος μεταβάλλει την τιμή Tx_id πριν την επικύρωση της συναλλαγής. Παραλλαγή διπλής δαπάνης με την ιδιαιτερότητα ότι το θύμα στέλνει συναλλαγή σε διεύθυνση ελεγχόμενη από τον ίδιο	Ανταλλακτήρια νομισμάτων	Ανταλλακτήρια χάνουν χρήματα , εξαιτίας φαινόμενου διπλής δαπάνης
BGP Hijacking	Δημιουργία ψεύτικων διαδρομών (BGP hijacks) με σκοπό την αναχαίτηση της κυκλοφορίας προς ένα νόμιμο προορισμό	Πρωτόκολλο (BGP), blockchain βάση δεδομένων, Δίκτυο	Δημιουργία ψεύτικων συναλλαγών, Ψεύτικοι κόμβοι

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Routing attack	Απομόνωση ενός συνόλου κόμβων από το bitcoin δίκτυο	Ανθρακωρύχοι, κόμβοι	Ευαλωτότητα δημιουργίας επίθεσης “0-confirmation” διπλής δαπάνης, μείωση της συνολικής ισχύς εξόρυξης στο δίκτυο
Delay attack	Ο επιτιθέμενος στοχεύει στην καθυστέρηση της διάδοσης των μπλοκ στο δίκτυο	Ανθρακωρύχοι, έμποροι	Δημιουργία συνθήκης διπλής δαπάνης για τους κόμβους του εμπόρου, σπατάλη υπολογιστικής ισχύς για τους ανθρακωρύχους
Sybil	Ο επιτιθέμενος δημιουργεί πολλαπλές ταυτότητες, όπου αποτελούν ψεύτικους λογαριασμού χρηστών	Δίκτυο Blockchain, ανθρακωρύχοι, κόμβοι (χρήστες)	Δημιουργεί ευνοϊκές συνθήκες για επίτευξη επιθέσεων όπως “double spending”, DDoS, Time jacking
Deanonymization	Ο επιτιθέμενος προσπαθεί να συνδέσει διεύθυνσης IP με bitcoin πορτοφόλι	Κόμβοι (χρήστες)	Παραβίαση ιδιωτικότητας χρήστη
Tampering	Ο επιτιθέμενος στοχεύει στην καθυστέρηση της διάδοσης συναλλαγών	Ανθρακωρύχοι, κόμβοι (χρήστες)	Πιθανόν να προκληθούν επιθέσεις όπως DDoS ή double spending-Αύξηση εξορυκτικής ισχύς
Wallet threats	Ο επιτιθέμενος κλέβει ιδιωτικά κλειδί του χρήστη	Χρήστες, επιχειρήσεις	Προκαλείται εξαφάνιση του ποσού νομισμάτων (bitcoin) από το χρήστη

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Block withholding	Αυτή η επίθεση εκμεταλλεύεται την ευπάθεια του δικτύου bitcoin να επιτρέπει σε ένα ανθρακωρύχο που έχει δημιουργήσει ένα νόμιμο μπλοκ να το κρατήσει ιδιωτικό, χωρίς να γίνει αμέσως δημοσίευση αυτού	Ειλικρινείς ανθρακωρύχοι	Απώλεια πόρων εξόρυξης για κάποια δεξαμενή εξόρυξης και μείωση των εσόδων αυτής
Fork after withholding attack	Αυξάνει ακόμη περισσότερο τα αποτελέσματα (κέρδη) για τον επιτιθέμενο σε σχέση με τις επιθέσεις “Selfish mining” και “block withholding”	Ειλικρινείς ανθρακωρύχους (mining pools)	Απώλεια πόρων εξόρυξης για κάποια δεξαμενή εξόρυξης και μείωση των εσόδων αυτής
Transaction privacy leakage	Σε ορισμένα κρυπτονομίσματα, οι συναλλαγές των χρηστών είναι ανιχνεύσιμες. Η χρήση «μιξίνων» περιορίζει μερικώς το πρόβλημα	Κόμβοι (χρήστες), πρωτόκολλο bitcoin	Συναλλαγή με 0-μιξίνες μπορεί να οδηγήσει σε επίθεση “man in the middle” και “Transaction malleability”

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Private key attack/ Vulnerable Signature	2 ψηφιακές υπογραφές με την ίδια τιμή k. Δυνατότητα εύρεσης τιμής k και υπολογισμός ιδιωτικού κλειδιού από τον επιτιθέμενο (κλοπή ιδιωτικού κλειδιού χρηστών)	Κόμβοι (χρήστες), επιχειρήσεις	Απώλεια του ποσού (bitcoin) των πορτοφολιών
Tampering	Καθυστέρηση των συναλλαγών και των μπλοκ σε συγκεκριμένους κόμβους	Ανθρακωρύχοι, χρήστες	Ευνοείται η δημιουργία επιθέσεων όπως DDoS ή double spending μέσω κακόβουλης αύξησης της εξορυκτικής ισχύς
Long Range attack	Δημιουργία διακλάδωσης στο “genesis block”	Κατανεμημένη βάση δεδομένων (ledger)	Παραβίαση του ιστορικού συναλλαγών
Pool hoping attack	Ο επιτιθέμενος εκμεταλλεύεται προς όφελος του τα δεδομένα “shares” των συναλλαγών	Ανθρακωρύχοι (mining pools)	Χρήση των δεδομένων “shares” με απώτερο στόχο την επίθεση “selfish mining”

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Balance attack	Ορίζονται οι ομάδες που διαθέτουν την ίδια ισχύ εξόρυξης G_1, G_2. Ο εισβολέας στέλνει συναλλαγές στην υποομάδα συναλλαγών G_1, ξεκινώντας όμως και την εξόρυξη στην υποομάδα G_2. Ο επιτιθέμενος προκαλεί καθυστέρηση των συνδέσεων επιφέροντας ανισορροπία μεταξύ των συναλλαγών G_1, G_2	Δίκτυο blockchain, εμπόρους/επιχειρήσεις	Η επίθεση “Balance” δημιουργεί πρόβλημα στη συνοχή του δικτύου και επιτρέπει στον επιτιθέμενο να πραγματοποιήσει την επίθεση “double spend”
Nothing at Stake	Ο επιτιθέμενος με βάση το συμφέρον του επιλέγει να συμμετέχει σε όσο το δυνατό περισσότερες διακλαδώσεις χωρίς να γνωρίζει ποια είναι η κύρια αλυσίδα	Μπλοκ	Καθυστέρηση στον χρόνο συναίνεσης

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Coinage accumulating attack	Ο εισβολέας επηρεάζει την τιμή coinage με στόχο να αυξήσει την ισχύ του ως κόμβος στο δίκτυο	Πωλητές/εμπόρους	Ο επιτιθέμενος δημιουργεί νέα διακλάδωση πραγματοποιώντας 2 φορές επίθεση διπλής δαπάνης/υποτίμηση νομίσματος
Call to the unknown	Η κλήση συνάρτησης για μεταφορά ether μπορεί να οδηγήσει σε εκτέλεση κακόβουλης εναλλακτικής συνάρτησης	Όσοι αναμιγνύονται στην εφαρμογή και εκτέλεση ενός έξυπνου συμβολαίου (ιδιοκτήτης, επιχειρήσεις κλπ.)	Η συνάρτηση “fallback” ενδέχεται να δημιουργήσει επιπλέον μολύνσεις όπως την “unpredictable state”
Gasless send	Η ευπάθεια προκύπτει αν η κατανάλωση ενέργειας (gas) υπερβαίνει ένα όριο, το οποίο είναι δυναμικό	Ιδιοκτήτες έξυπνων συμβολαίων (ιδιώτες, επιχειρήσεις)	Κάνει μια συναλλαγή να έχει αποτυχημένη κατάληξη, δημιουργώντας υψηλές καταναλώσεις “gas”

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Timestamp dependence	Για κάθε μπλοκ εφαρμόζεται χρονική σήμανση. Οι συνθήκες ενεργοποίησης ενός έξυπνου συμβολαίου εξαρτώνται από την χρονική σήμανση η οποία ορίζεται από τον ανθρακωρύχο με βάση την χρονική σήμανση του συστήματος	Ανθρακωρύχοι, ιδιοκτήτες συμβολαίων (ιδιώτες, επιχειρήσεις)	Η χρονική σήμανση του μπλοκ μπορεί να χειραγωγείται από τον ανθρακωρύχο
Reentrancy	Η συνάρτηση fallback ενός συμβολαίου επιτρέπει να εισέλθει ξανά σε μια λειτουργία καλούντος πριν τερματιστεί. Εξαντλεί τα νομίσματα ether σε ένα smart contract	Ιδιοκτήτη συμβολαίου	Ο εισβολέας καλεί την συνάρτηση “withdraw” αναδρομικά και πριν ενημερωθεί το υπόλοιπο του χρήστη προκειμένου να το μηδενίσει σε συνδυασμό με το συμβόλαιο DAO
Generating randomness	Προκειμένου το περιεχόμενο των μελλοντικών μπλοκ να είναι απρόβλεπτο με ασφαλή τρόπο χρησιμοποιούνται ψευδοτυχαίοι αριθμοί	Ανθρακωρύχοι, Ιδιοκτήτη συμβολαίου	Ο κακόβουλος ανθρακωρύχος στοχεύει στην δημιουργία ενός μπλοκ με το οποίο θα επηρεάσει το αποτέλεσμα της ψευδοτυχαίας γεννήτριας για την δημιουργία τυχαίων αριθμών

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Immutable bugs	Η ανάπτυξη ενός συμβολαίου που περιέχει σφάλμα στο κώδικα ή οποιοδήποτε άλλο σφάλμα δεν μπορεί να αλλάξει με	Ανθρακωρύχοι, Ιδιοκτήτη συμβολαίου	Το αμετάβλητο σφαλμάτων αξιοποιείται σε διάφορες επιθέσεις όπως την “Ether lost” ή για την μετατροπή των ether ενός χρήστη σε μη εξαργυρώσιμα
Mishandled exception	Ο χειρισμός εξαιρέσεων αφορά την επικοινωνία που έχουν οι συμβάσεις μεταξύ τους και	Ιδιοκτήτη συμβολαίου	Αυτές οι εξαιρέσεις χωρίς σωστό χειρισμό προκαλούν απώλεια ether ή αντιστροφή συναλλαγών
DoS από εξωτερικό συμβόλαιο	Όταν οι εκφράσεις (if, for, while) εξαρτώνται από μια εξωτερική κλήση. Η εκτέλεση συμβολαίου του καλούμενου μπορεί να αποτύχει, πραγματοποιώντας την επίθεση DoS στο συμβόλαιο	Ιδιοκτήτη συμβολαίου	Διακόπτεται η εκτέλεση ενός έξυπνου συμβολαίου
TX. Origin	Στο tx.origin συμβόλαιο, ορίζεται ως κύρια διεύθυνση η διεύθυνση του εισβολέα,	Ιδιοκτήτη συμβολαίου	Η χρησιμοποίηση του συμβολαίου Tx.origin δημιουργεί ευπάθεια σε επιθέσεις όπως Phishing attack. Περιορισμένη διαλειτουργικότητα

Επίθεση	Περιγραφή	Τομέας λειτουργίας που επηρεάζει	Πρόβλημα που δημιουργεί
Ether lost in transfer	Το ποσό των ethers που στέλνεται σε μια ορφανή διεύθυνση, ουσιαστικά δεν ανήκει σε κανένα ιδιωτικό κλειδί ή συμβόλαιο και επομένως τα “ethers θα χαθούν χωρίς να μπορούν να ανακτηθούν	Ιδιοκτήτη συμβολαίου	Τα “ethers” θα χαθούν οριστικά εάν σταλούν σε ορφανή διεύθυνση, χωρίς να υπάρχει τρόπος να ελεγχθεί αν μια διεύθυνση είναι ορφανή ή όχι
Unpredictable Stale	Κατά την αποστολή μιας συναλλαγής ενδέχεται μια άλλη συναλλαγή να αλλάξει την κατάσταση ενός συμβολαίου καθώς και να δημιουργηθεί πρόβλημα στον χρόνο πραγματοποίησης συναλλαγών	Ιδιοκτήτη συμβολαίου	Η κατάσταση State ενός συμβολαίου είναι μεταβλητή
Low level attacks	Ο επιτιθέμενος εκμεταλλεύεται τρωτά σημεία στην EVM καθώς και στο πελάτη Ethereum	Δίκτυο Ethereum , ανθρακωρύχοι, κόμβοι, ανταλλακτήρια	Διαιρείται το Ethereum Δίκτυο σε μικρές ομάδες κόμβων εξαναγκάζοντας μέσω “ad-hoc” το θύμα να δεχθεί μολυσμένα μπλοκ