ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΚΛΙΜΑΚΩΣΙΜΟΤΗΤΑ BLOCKCHAIN ΜΕ ΧΡΗΣΗ DHT

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δημοσθένης Ε. Θεοφιλάτος

Επιβλέπων: Νεκτάριος Κοζύρης
Καθηγητής Ε.Μ.Π

Αθήνα, Σεπτέμβριος 2017

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΚΛΙΜΑΚΩΣΙΜΟΤΗΤΑ BLOCKCHAIN ΜΕ ΧΡΗΣΗ DHT

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δημοσθένης Ε. Θεοφιλάτος

Επιβλέπων: Νεκτάριος Κοζύρης
Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 31η Οκτωβρίου 2017.

…….	……	……
Ν. Κοζύρης	Ν. Παπασπύρου	Γ. Γκούμας
Καθηγητής Ε.Μ.Π	Αν. Καθηγητής Ε.Μ.Π	Επ. Καθηγητής Ε.Μ.Π

Αθήνα, Σεπτέμβριος 2017

.....

Δημοσθένης Ε. Θεοφιλάτος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Σκοπός της παρούσας διπλωματικής εργασίας είναι η ανάλυση της επαναστατικής τεχνολογίας του blockchain και η πρόταση μιας νέας προσέγγισής του. Το blockchain είναι ένας δυναμικός δημόσιος κατάλογος που βασίζεται σε peer-to-peer δίκτυα. Η πρωτοπορία του έγκειται στη λύση που δίνει στο ζήτημα της ομοφωνίας, δηλαδή της συμφωνίας των κόμβων του δικτύου σε μια κοινή κατάσταση, ενώ η ασφάλεια των δεδομένων του επιτυγχάνεται μέσω κρυπτογραφικών μεθόδων. Εκτός από τα πλεονεκτήματα, όμως, το blockchain έχει ορισμένα σημαντικά μειονεκτήματα που σχετίζονται με την καταχώρηση νέων δεδομένων (ρυθμό και καθυστέρηση) και με τον όγκο των καταλόγων· αντιμετωπίζει, δηλαδή, πρόβλημα κλιμάκωσης. Έχουν ήδη προταθεί ορισμένες σοβαρές λύσεις για την κλιμάκωση του blockchain, όπως το proof-of-stake, τα lightning networks και το sharding. Επιπλέον, στην εργασία αυτή εξετάζεται η δυνατότητα της αποθήκευσης ενός καταλόγου blockchain σε Chord DHT, με στόχο το διαμοιρασμό του όγκου δεδομένων του. Η αποτίμηση της βιωσιμότητας αυτής της πρότασης γίνεται μέσω simulations, τα οποία βασίζονται στο δίκτυο της πρώτης και δημοφιλέστερης εφαρμογής blockchain, του Bitcoin.

Λέξεις Κλειδιά

Blockchain, Bitcoin, Κατανεμημένος Πίνακας Κατακερματισμού, DHT, Κλιμακωσιμότητα

Abstract

The purpose of this diploma thesis is the analysis of a novel technology called blockchain as well as the proposal of a new approach on its implementation. Blockchain is a dynamic public ledger based on peer-to-peer networks. Its breakthrough lies on the resolution of the consensus problem, which is the agreement of the peers on a common state, while its data is being secured with cryptographic methods. Apart from its benefits, the blockchain technology also has some significant drawbacks related to the entry of new data (rate and latency) and the ledger's data volume, basically meaning that it is faced with scalability issues. Notable solutions for the scalability problem, such as the proof-of-stake, the lightning networks and the Sharding method, have already been proposed. Moreover, this thesis considers the possibility of storing a blockchain ledger on a Distributed Hash Table, aiming to the distribution of the storage demands to many peers. The evaluation of this proposal is achieved through simulations of the first and most popular blockchain network, the Bitcoin.

Key Words

Blockchain, Bitcoin, Distributed Hash Table, DHT, Scalability

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο Εργαστήριο Υπολογιστικών Συστημάτων του τομέα Τεχνολογίας Πληροφορικής και Υπολογιστών της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών ΕΜΠ.

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέποντα της διπλωματικής μου εργασίας, Καθηγητή κ. Νεκτάριο Κοζύρη για την εμπιστοσύνη του και την ευκαιρία που μου έδωσε να συμμετάσχω στο Εργαστήριο Υπολογιστικών Συστημάτων, αλλά πρωτίστως για την επιρροή που μου άσκησε κατά τις παραδόσεις των μαθημάτων του. Επίσης, θα ήθελα να ευχαριστήσω τη δόκτωρ Κατερίνα Δόκα για την πολύτιμη καθοδήγησή της και το αμείωτο ενδιαφέρον καθ' όλη τη διάρκεια της εργασίας μου και γενικότερα όλους τους ερευνητές του Εργαστηρίου Υπολογιστικών Συστημάτων για τη συνεργατικότητά τους. Ευχαριστώ ιδιαίτερα τα μέλη της εξεταστικής επιτροπής κ. Νεκτάριο Κοζύρη, κ. Νικόλαο Παπασπύρου και κ. Γεώργιο Γκούμα για το χρόνο που θα αφιερώσουν στη μελέτη της διπλωματικής μου εργασίας. Ακόμη, οφείλω πολλά στο συμφοιτητή Κωνσταντίνο Κανελλόπουλο, που υπήρξε συνεργάτης και συνοδοιπόρος καθ' όλη τη φοιτητική μου πορεία. Φυσικά, η επιτυχία μου στο Πολυτεχνείο δε θα ήταν εφικτή χωρίς την οικογένειά μου, που πάντα με στηρίζουν.

Δημοσθένης Θεοφιλάτος
Αθήνα, Σεπτέμβριος 2017

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

1 Εισαγωγή

Στην εποχή της πληροφορίας ζούμε μια ραγδαία ψηφιοποίηση δεδομένων και υπηρεσιών. Η νέα τάση είναι η ψηφιοποίηση του χρήματος. Πρόκειται για μια ιδέα που ξεκίνησε τα τέλη του 2008, όταν κάποιος με το ψευδώνυμο Satoshi Nakamoto δημοσίευσε ένα άρθρο με τίτλο “Bitcoin: Ένα peer-to-peer ηλεκτρονικό σύστημα μετρητών”. Το σύστημα αυτό βασίζεται στον πρωτοποριακό συνδυασμό βασικών στοιχείων κρυπτογραφίας, του proof-of-work [1] και της τεχνολογίας peer-to-peer [2]. Η καινοτομία του Bitcoin είναι η πρόταση ενός πλήρως κατανεμημένου server που μπορεί να εκτελεί εντολές σε ένα κατανεμημένο σύστημα, που αργότερα έγινε γνωστό ως blockchain. Από την υλοποίησή του το 2009 και τη χρήση του από μερικούς ενθουσιώδεις χρήστες, έχει αναπτυχθεί σε ένα παγκόσμιο σύστημα πληρωμών και σε ένα από τα πιο πολυσυζητημένα τεχνολογικά επιτεύγματα με επενδύσεις δισεκατομμυρίων ευρώ να το υποστηρίζουν και μια ολόκληρη βιομηχανία να κτίζεται πάνω στις βάσεις του.

Τα χαρακτηριστικά που καθιστούν το Bitcoin ελκυστικό ως νόμισμα είναι ο αποκεντρωμένος σχεδιασμός του και το γεγονός ότι δεν απαιτείται εμπιστοσύνη μεταξύ των συναλλασσόμενων. Είναι ένα ανοιχτό σύστημα όπου μπορεί ο καθένας να συμμετέχει τόσο σε συναλλαγές όσο και στην επιβεβαίωση των συναλλαγών, αμοιβόμενος για τη συνεισφορά του. Τα αρχεία του Bitcoin δεν τηρούνται από κάποιον έμπιστο κεντρικό server, αλλά από ένα κατανεμημένο δίκτυο από συνεργαζόμενους εθελοντές. Οι συναλλαγές είναι μη αναστρέψιμες, ενώ μπορούν να πραγματοποιηθούν εύκολα και άμεσα μεταξύ οποιωνδήποτε χρηστών, χωρίς ενδιάμεσους και χωρίς γεωγραφικούς και -προς το παρόν- νομικούς περιορισμούς.

Με αφορμή το Bitcoin έχει ξεκινήσει μια μικρή τεχνολογική επανάσταση, με την τεχνολογία του blockchain να βρίσκει πολλές εφαρμογές, από ψηφιακά νομίσματα μέχρι έξυπνα συμβόλαια (*smart contracts*) [3] και αποκεντρωμένες εφαρμογές ψηφοφορίας.

Ωστόσο, όπως κάθε νέα τεχνολογία, το blockchain καλείται να αντιμετωπίσει μια σειρά προκλήσεων που αφορούν στην πρακτική εφαρμογή του και πρόκειται να καθορίσουν το μέλλον του. Πιο συγκεκριμένα, τα καίρια σημεία στα οποία υστερούν τα σημερινά συστήματα blockchain είναι ο ρυθμός εξυπηρέτησης των χρηστών (throughput), το κόστος και η καθυστέρηση για την προσθήκη νέων δεδομένων στο blockchain και οι απαιτήσεις σε εξοπλισμό (υπολογιστική ισχύ, αποθηκευτικό χώρο δεδομένων). Οι παράμετροι αυτές είναι περιοριστικές για το blockchain διότι μέχρι σήμερα δεν έχει επιτευχθεί η κλιμάκωσή τους.

Σκοπός της παρούσας εργασίας είναι να αναλυθεί η τεχνολογία του blockchain, να εντοπιστούν και να εξηγηθούν τα αδύνατα σημεία του και να παρουσιαστούν οι πιο ενδιαφέρουσες προτάσεις που μελετούνται για την κλιμάκωση του blockchain. Επιπροσθέτως, υπάρχει ο στόχος της συνεισφοράς στην κοινότητα των blockchains με μια πρόταση που βασίζεται στη χρήση DHT και προσβλέπει σε ακόμη πιο αποκεντρωμένα και προσιτά blockchains. Η αποτίμηση της βιωσιμότητας και η αξιολόγηση της πρότασης θα γίνει μέσω simulations.

Πρόκειται να γίνει εκτενής αναφορά στο Bitcoin, ως της πρώτης, μεγαλύτερης εφαρμογής blockchain με τους περισσότερους συμμετέχοντες χρήστες. Στο Κεφάλαιο 2 αναλύεται ο σχεδιασμός και το πρωτόκολλο του Bitcoin, τα χαρακτηριστικά και τα στατιστικά στοιχεία του δικτύου του και εξηγείται η τεχνολογία του blockchain.

Στο Κεφάλαιο 3 εξετάζονται οι επιδόσεις του Bitcoin και η δυνατότητα που έχει το πρώτο ψηφιακό νόμισμα να εξυπηρετεί τις παγκόσμιες συναλλαγές. Ορίζονται οι αδυναμίες της τεχνολογίας του και γίνεται αναφορά στις σημαντικότερες προτάσεις που συζητούνται και στοχεύουν στην κλιμάκωσή της. Επιπλέον, παρουσιάζεται η πρόταση της παρούσας εργασίας, η οποία μελετά την οργάνωση των peer-to-peer κόμβων σε DHT για την αποθήκευση του blockchain στοχεύοντας στη μείωση του απαιτούμενου χώρου αποθήκευσης ανά κόμβο.

Το περιεχόμενο του Κεφαλαίου 4 αφορά στα peer-to-peer δίκτυα. Μετά από ένα σύντομο ορισμό των δικτύων αυτών ακολουθεί αναφορά στα DHTs, στα είδη και τη χρήση τους, στα πλεονεκτήματα αλλά και στους κινδύνους ασφαλείας που αντιμετωπίζουν.

Τέλος, στο Κεφάλαιο 5 ορίζεται το μέσο που χρησιμοποιήθηκε για την προσομοίωση του συστήματος που προτείνεται. Γίνεται παρουσίαση των αποτελεσμάτων, σχολιασμός αυτών και συναγωγή συμπερασμάτων.

2 Το Bitcoin

Το Bitcoin είναι ένα κρυπτονόμισμα (*cryptocurrency*) κι ένα ψηφιακό σύστημα πληρωμών που προτάθηκε από έναν προγραμματιστή, ή μια ομάδα προγραμματιστών, υπό το όνομα Satoshi Nakamoto και κυκλοφόρησε ως λογισμικό ανοιχτού κώδικα το 2009. Το Bitcoin υλοποιείται μέσω ενός peer-to-peer δικτύου και οι συναλλαγές πραγματοποιούνται κατευθείαν μεταξύ χρηστών, χωρίς την ύπαρξη κάποιου ενδιάμεσου. Σε αυτό το κεφάλαιο θα δοθεί μια γενική περιγραφή του Bitcoin, καθώς επίσης και ορισμένες βασικές τεχνικές λεπτομέρειες. Θα εστιάσουμε στο σύστημα και στο πρωτόκολλό του, περιγράφοντας τον τρόπο με τον οποίο γίνεται η δόμηση του blockchain, της τεχνολογίας στην οποία βασίζεται.

Στο Bitcoin οι πληροφορίες διαδίδονται μέσω δύο τύπων πληροφορίας: τις *συναλλαγές* (*transactions*) και τα *μπλοκ* (*blocks*). Τα transactions είναι οι βασικές μονάδες πληροφορίας και εμπεριέχουν όλες τις απαραίτητες πληροφορίες για την ολοκλήρωση μιας μεταφοράς αξίας (bitcoins), ενώ τα blocks είναι ομάδες από transactions και η σύστασή τους εξυπηρετεί στην επίτευξη συγχρονισμού κατάστασης μεταξύ των κόμβων του peer-to-peer δικτύου.

Σε αντίθεση με τα παραδοσιακά συναλλάγματα, όπως το ευρώ, το Bitcoin δε βασίζεται σε μια κεντρική αρχή η οποία ελέγχει τη διανομή και την κατανομή των χρημάτων και επιβεβαιώνει την εγκυρότητα των συναλλαγών. Το Bitcoin βασίζεται σε ένα δίκτυο από “εθελοντές” οι οποίοι διατηρούν πιστά αντίγραφα του καταλόγου πληρωμών του (*ledgers*). Το ledger περιέχει όλες τις απαραίτητες πληροφορίες για το συμπερασμό του υπολοίπου κάθε κατόχου bitcoins. Είναι κρίσιμο να υπάρχει συνέπεια των καταστάσεων των ledgers μεταξύ των κόμβων σε όλο το δίκτυο, αφού η εγκυρότητα μιας συναλλαγής επιβεβαιώνεται μέσω αυτών.

2.1 Transactions

Ως πιο αφηρημένη έννοια, το transaction είναι η διαδικασία μεταφοράς bitcoins από έναν ή περισσότερους λογαριασμούς προέλευσης σε έναν ή περισσότερους λογαριασμούς προορισμού. Στην πραγματικότητα, ένας λογαριασμός είναι ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού (*public-/private-key*). Το δημόσιο κλειδί αποτελεί τη διεύθυνση του λογαριασμού κι εξυπηρετεί ως αναγνωριστικό του. Προκειμένου να πραγματοποιηθεί η μεταφορά ενός ποσού bitcoins προς έναν λογαριασμό, δημιουργείται ένα transaction με διεύθυνση προορισμού το αναγνωριστικό αυτού (το δημόσιο κλειδί

του). Για να γίνει αποστολή bitcoins από λογαριασμό, το transaction θα πρέπει να υπογραφεί με το ιδιωτικό κλειδί του λογαρισμού αποστολέα. Η μέθοδος αυτή δεν είναι η μόνη για τη μεταφορά bitcoins σε λογαριασμό, ωστόσο είναι η πιο συνήθης και καθώς η περιγραφή της αρκεί για την ανάπτυξη του θέματος, θα αρκεστούμε σε αυτή.

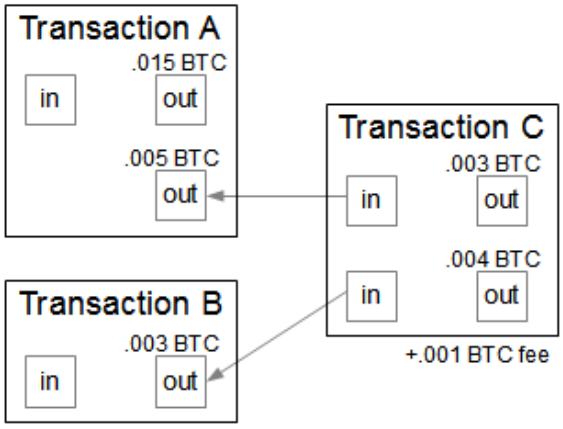
Αντί για τον κλασικό τρόπο προσθαφαίρεσης για τον υπολογισμό του υπολοίπου ενός λογαριασμού γίνεται εντοπισμός και άθροιση συναλλαγών που μεταφέρουν bitcoins (outputs) στο λογαριασμό. Τα outputs στην πραγματικότητα είναι πλειάδες από μια αριθμητική τιμή σε bitcoins και μία συνθήκη. Όποιος μπορεί να ικανοποιήσει την κρυπτογραφικού χαρακτήρα συνθήκη μπορεί να διεκδικήσει και να ξοδέψει τα bitcoins του output. Το υπόλοιπο ενός λογαρισμού προκύπτει απ’ το άθροισμα των αριθμητικών τιμών όλων των αξόδευτων outputs του λογαριασμού.

Τα transactions προσδιορίζονται βάσει της hash τιμής της σειριοποιημένης αναπαράστασής τους. Ένα transaction ξοδεύει outputs παρέχοντας μια απόδειξη κυριότητας αυτών. Οι αναφορές στα διεκδικούμενα outputs μαζί με τις αποδείξεις κυριότητας συνθέτουν αυτό που αποκαλείται *είσοδος* (*input*) σε ένα transaction. Έχοντας έγκυρα inputs, ορίζονται τη συνέχεια τα outputs του transaction.

Τα outputs είναι οι θεμελιώδεις μονάδες πληροφορίας του ledger και η κατάστασή τους θα πρέπει να είναι συνεπής σε όλα τα αντίγραφά του. Για να είναι έγκυρο ένα transaction θα πρέπει να πληρούνται οι παρακάτω περιορισμοί αναφορικά με τα outputs που ξοδεύουν και δημιουργούν:

- Ένα output μπορεί να ξοδευτεί το πολύ μία φορά
- Νέα outputs δημιουργούνται μόνο ως αποτελέσματα transactions
- Το άθροισμα των αριθμητικών τιμών των inputs θα πρέπει να είναι ίσο ή μεγαλύτερο του αθροίσματος των τιμών των outputs που δημιουργούνται.

Καθώς νέα transactions μεταδίδονται στο δίκτυο, η κατάσταση των αντιγράφων ledgers μεταβάλλεται. Όταν ένας κόμβος λαμβάνει ένα νέο transaction, επιβεβαιώνει την εγκυρότητά του και το περιλαμβάνει στο τοπικό του αντίγραφο. Βέβαια, είναι πιθανό κάποιες χρονικές στιγμές να προκύψουν ασυνέπειες μεταξύ των αντιγράφων των ledgers σε διαφορετικούς κόμβους:



Σχήμα 1: *Παράδειγμα: το transaction C χρησιμοποιεί ως inputs τα outputs των transactions A και B, ενώ προσφέρει και 0.001 bitcoin ως αμοιβή προς τον miner που θα συμπεριλάβει το transaction C στο block του.*

- Είναι πιθανό ένας κόμβος να λάβει ένα transaction που μεταφέρει ένα ποσό από έναν λογαριασμό, χωρίς να έχει λάβει ακόμα το transaction που κάνει αυτό το ποσό διαθέσιμο στο λογαριασμό.
- Δύο ή περισσότερα transactions μπορεί να διεκδικούν τα ίδια outputs, επιχειρώντας να ξοδέψουν τα αντίστοιχα ποσά περισσότερες από μία φορές. Αυτή η περίπτωση καλείται επίθεση διπλού ξοδέματος (double spending attack).

Οι επιθέσεις διπλού ξοδέματος έχουν άμεση επίδραση στη συνοχή των αντιγράφων του ledger. Όταν συμβαίνει ένα διπλό ξόδεμα, είτε σκόπιμα είτε καταλάθος, δύο ή περισσότερα transactions επιχειρούν να ξοδέψουν ταυτόχρονα το ίδιο output. Ένας κόμβος που θα λάβει το πρώτο transaction θα το επιβεβαιώσει και θα το συμπεριλάβει στο ledger του. Όταν στη συνέχεια λάβει τα υπόλοιπα, η επιβεβαίωσή τους θα αποτύχει, καθώς το output έχει ήδη ξοδευτεί. Καθώς δεν υπάρχει εγγύηση ότι όλοι οι κόμβοι θα λάβουν τα transactions με την ίδια σειρά, οι κόμβοι θα διαφωνήσουν σχετικά με την εγκυρότητα αυτών των αντικρουόμενων transactions και κάθε άλλου transaction που θα βασίζεται σε αυτά ξοδεύοντας τα outputs τους. Αυτή η ασυμφωνία επιλύεται μέσω των blocks, όπως θα αναλυθεί στην ενότητα που ακολουθεί.

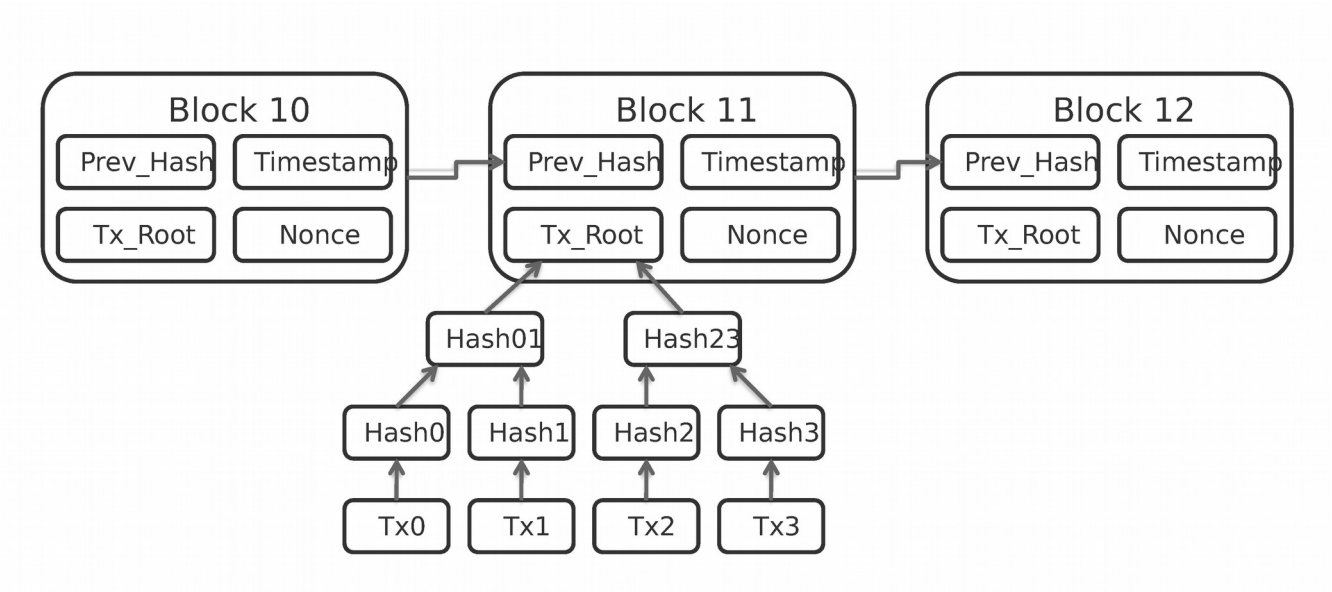
2.2 Blocks

Προκειμένου να διατηρείται η συνέπεια μεταξύ των αντιγράφων ledgers, θα πρέπει να υπάρχει συμφωνία μεταξύ των κόμβων σχετικά με τη σειρά των transactions. Η επίτευξη μιας τέτοιας συμφωνίας δεν αποτελεί τετριμμένη υπόθεση. Το Bitcoin λύνει αυτό το πρόβλημα κάνοντας σε πρώτο στάδιο δοκιμαστική αποδοχή των transactions κι έπειτα κάνοντας συγχρονισμό σε τακτά χρονικά διαστήματα μεταδίδοντας τα blocks που δημιουργούνται απ' τους κόμβους. Ένα block *b* περιέχει ένα σύνολο απο transactions T_b, που είναι τα transactions που έχει αποδεχτεί ο κόμβος-δημιουργός μετά το αμέσως προηγούμενο block. Το block αυτό διανέμεται σε όλους τους κόμβους του δικτύου και ο καθένας αντιστρέφει τα δοκιμαστικά transactions που είχε αποδεχτεί και εφαρμόζει αυτά που περιέχει το νέο block *b*.

Σε αυτό το σημείο όλοι οι κόμβοι έχουν συμφωνήσει για την εγκυρότητα όλων των transactions εντός του *b*. Τα transactions του *b* που είχαν ήδη συμπεριληφθεί δοκιμαστικά στο ledger δε χρειάζεται να επανεφαρμοστούν, ενώ τα δοκιμαστικά transactions που αντιστράφηκαν θα επανεπικυρωθούν και θα συμπεριληφθούν, δοκιμαστικά πάλι, στη νέα βάση κατάστασης του ledger. Τα transactions που δεν είναι πλέον έγκυρα λόγω σύγκρουσης με transactions που κατατέθηκαν ως μέρος του *b* θα απορριφθούν.

Ο κόμβος που δημιούργησε το block *b* κατά κάποιον τρόπο υπαγορεύει την αλλαγή στην κατάσταση του ledger από το προηγούμενο block βάσει της δικής του οπτικής. Ωστόσο, οι αποφάσεις που μπορεί να πάρει ο κόμβος-δημιουργός είναι περιορισμένες. Δεν μπορεί να παραχαράξει ένα transaction καθόσον το κρυπτοσύστημα public/private-key είναι ασφαλές. Ο κόμβος-δημιουργός μπορεί μόνο να αποφασίσει για τη σειρά με την οποία έγιναν τα transactions και για το αν και ποια transactions θα συμπεριλάβει στο block του.

Για να γίνει η επιλογή του κόμβου που θα δημιουργήσει το επόμενο block και θα υπαγορεύσει τη νέα κατάσταση του ledger, οι κόμβοι επιχειρούν να βρουν τη λύση σε ένα proof-of-work (PoW) [1] κρυπτογραφικό πρόβλημα, το οποίο έχει ένα δεδομένο βαθμό δυσκολίας. Το proof-of-work στην πραγματικότητα είναι η πρόκληση για εύρεση μιας δυαδικής συμβολοσειράς, που καλείται *nonce*, η οποία σε συνδυασμό με το block header δίνει τιμή hash H_b τέτοια, ώστε να έχει ένα απαιτούμενο πλήθος μηδενικών bits στην αρχή της (*target*). Επειδή οι συναρτήσεις κατακερματισμού είναι μονόδρομες συναρτήσεις, η εύρεση ενός target γίνεται μόνο με εξαντλητική αναζήτηση και δοκιμή πιθανών nonces, έως ότου βρεθεί ένα με την επιθυμητή ιδιότητα. Έτσι, η εύρεση ενός nonce που δίνει



Σχήμα 2: *Bitcoin blocks. Πηγή: commons.wikimedia.org.*

μια λύση στο proof-of-work πρόβλημα είναι δύσκολη, ωστόσο η επικύρωσή του γίνεται εύκολα με τον υπολογισμό ενός αποτελέσματος της συνάρτησης κατακερματισμού. Το nonce είναι μέρος του block, ούτως ώστε οι παραλήπτες κόμβοι να επιβεβαιώνουν ότι ο δημιουργός του έλυσε πραγματικά το proof-of-work πρόβλημα. Η τιμή H_b χρησιμοποιείται επίσης και ως αναγνωριστικό του block. Το target καθορίζεται έπειτα από ομοφωνία μεταξύ όλων των κόμβων έτσι, ώστε ο μέσος χρόνος δημιουργίας ενός νέου block από το δίκτυο συνολικά να είναι 10 λεπτά και επαναπροσαρμόζεται έπειτα από 2016 blocks.

Οι κόμβοι που επιχειρούν την εύρεση μιας λύσης στο proof-of-work καλούνται *εξορύκτες* (*miners*). Προκειμένου οι miners να έχουν κάποιο κίνητρο, ο κόμβος που δημιουργεί ένα block παίρνει μια επιβράβευση σε μορφή νέων σχηματισμένων κρυπτονομισμάτων, π.χ., μπορεί να συμπεριλάβει στο block ένα transaction το οποίο δε θα έχει inputs, αλλά θα ορίσει outputs με αριθμητικό άθροισμα τιμών ένα προκαθορισμένο πλήθος κρυπτονομισμάτων. Αυτή η επιβράβευση είναι έγκυρη μόνο αν παρουσιάζεται εντός του block και αποτελεί τη μοναδική εξαίρεση στον κανόνα ότι το άθροισμα των inputs θα πρέπει να είναι ίσο ή μεγαλύτερο του αθροίσματος των outputs.

2.3 Blockchain

Ένας τρόπος να οριστεί το blockchain είναι ως μια κατανεμημένη βάση δεδομένων που λύνει το Strong Byzantine Generals πρόβλημα (SBG problem) [4], ένα όνομα που προκύπτει από το πρόβλημα των Byzantine Generals και το πρόβλημα του Sybil Attack. Στο πρόβλημα Byzantine Generals [5], οι κόμβοι καλούνται να συμφωνήσουν στην τιμή μιας καταχώρησης μιας κατανεμημένης βάσης δεδομένων, υπό τον περιορισμό ότι οι κόμβοι είναι πιθανό να αποτύχουν με τυχαίους τρόπους (συμπεριλαμβανομένης και της κακοπροαίρετης συμπεριφοράς). Το πρόβλημα του Sybil Attack ανακύπτει όταν ένας ή περισσότεροι κόμβοι βρίσκουν τρόπο να ασκήσουν με αθέμιτο τρόπο δυσανάλογα μεγάλη επιρροή στη διαδικασία συμφωνίας στην τιμή μιας καταχώρησης. Είναι η “επίθεση των κλόνων” - ένα πλήθος φαινομενικά ανεξάρτητων ψηφοφόρων οι οποίοι στην πραγματικότητα συνεργάζονται για να ξεγελάσουν το σύστημα.

Έχοντας αναφερθεί στις προηγούμενες ενότητες περί Bitcoin, δεν υπάρχει κάποιο στοιχείο των blocks που να προσφέρει επιπλέον συγχρονισμό και σειριοποίηση στα transactions. Κάτι τέτοιο, ωστόσο, επιτυγχάνεται όταν τα blocks συνδέονται σε σχηματισμό αλυσίδας, ορίζοντας μια χρονολογική σειρά μεταξύ τους και ως εκ τούτου μεταξύ των transactions.

Τα blocks οργανώνονται σε κατευθυνόμενα δέντρα. Κάθε block περιέχει μια αναφορά στο προηγούμενο block. Όταν το block *b* αναφέρεται από το block *b´* ως προηγούμενό του, τότε καλείται γονέας (*parent*) του *b´*. Η ρίζα του δέντρου αυτού ονομάζεται *genesis block*, υπάρχει εξ’ ορισμού και είναι “επακριβώς γραμμένο” (*hardcoded*) σε όλους τους clients του Bitcoin. Το *genesis block* είναι ο πρόγονος όλων των blocks.

Το *blockchain* ορίζεται ως το μονοπάτι μεγαλύτερου μήκους από οποιοδήποτε block προς το genesis block. Η απόσταση μεταξύ του block *b* και του genesis block αναφέρεται ως το ύψος του block h_b. Το genesis block, λοιπόν, έχει ύψος μηδέν. Το block με το μεγαλύτερο ύψος αναφέρεται ως η κεφαλή του blockchain (*blockchain head*) και έχει ύψος h_{head}.

Καθώς για να γίνει η αναφορά σε ένα block ως γονέα θα πρέπει πρώτα το αναγνωριστικό του block αυτού (η hash τιμή του) να είναι γνωστό, το block παιδί θα πρέπει να δημιουργηθεί αφού πρώτα δημιουργηθεί το block γονέας. Αυτός ο σχηματισμός αλυσίδας χρησιμοποιείται για οριστεί μια χρονολογική σειρά μεταξύ των transactions: τα transactions σε blocks μικρότερου ύψους έχουν επιβεβαιωθεί πριν από αυτά των blocks μεταλύτερου ύψους.

Μόνο τα blocks του blockchain επιβραβεύονται με νέα σχηματισμένα νομίσματα που είναι αποδεκτά από τους χρήστες, οπότε οι miners θα επιχειρούν τη δημιουργία blocks επάνω στο blockchain head. Η δημιουργία σε προγενέστερο block θα απαιτούσε το μονοπάτι αυτό να αποκτήσει μεγαλύτερο μήκος από το h_{head}, δηλαδή να γίνει το blockchain, προκειμένου να επιβραβευτεί.

Έχοντας εξηγήσει τη λειτουργία του blockchain, απαντάται και το ερώτημα που προκύπτει σχετικά με τη χρησιμότητα του proof-of-work. Το proof-of-work εξυπηρετεί στην ασφάλεια του blockchain. Για να θεωρηθεί ένα block έγκυρο θα πρέπει να ικανοποιεί τις απαιτήσεις του target, γεγονός που δείχνει ότι έχει καταβληθεί χρόνος, υπολογιστική ισχύς και ενέργεια για τη δημιουργία του. Καθώς τα blocks οργανώνονται σε σχηματισμό αλυσίδας, η παραποίηση ενός block προϋποθέτει και την επαναδημιουργία όλων των επόμενών του και την καταβολή της έργου που απαιτείται. Με αυτόν τον τρόπο επιτυγχάνεται η επιβεβαίωση των blocks: όσο περισσότερα blocks διαδέχονται ένα block του blockchain, τόσο πιο απίθανο είναι αυτό κάποια στιγμή να αποκλειστεί από το blockchain [6].

2.4 Blockchain forks

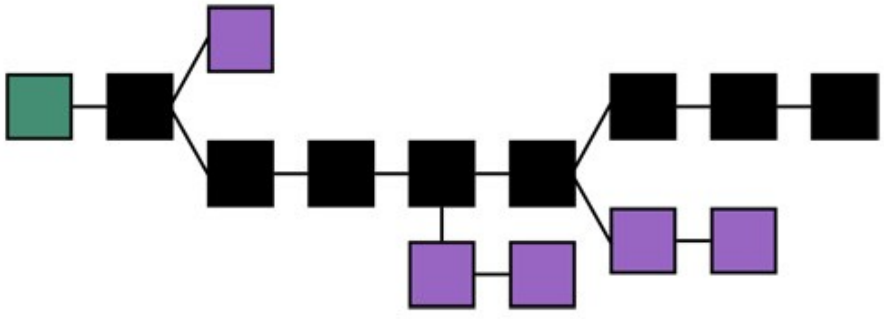
Απ’ τον ορισμό του blockchain προκύπτει πως είναι δυνατό ανά πάσα στιγμή να υπάρχουν πολλαπλά blockchain heads. Αυτή η κατάσταση καλείται *blockchain fork*. Στην περίπτωση ενός blockchain fork υπάρχει διαφωνία μεταξύ των κόμβων του δικτύου αναφορικά με το ποιο block είναι το blockchain head.

Όταν ένας κόμβος, του οποίου το blockchain head b_h βρίσκεται σε ύψος h, λάβει ένα block $b_h{}'$ με ύψος $h' > h$ το ορίζει ως blockchain head. Το νέο block $b_h{}'$ μπορεί να ανήκει είτε στο ίδιο κλαδί του δέντρου, δηλαδή το $b_h{}'$ να είναι απόγονος του b_h, είτε να ανήκει σε διαφορετικό κλαδί.

Εαν το block $b_h{}'$ ανήκει στο ίδιο κλαδί με το b_h, τότε ο κόμβος θα βρει όλα τα ενδιάμεσα blocks του κλαδιού και θα εφαρμόσει σταδιακά όλες τις αλλαγές που αυτά ορίζουν. Στην αντίθετη περίπτωση, όπου το $b_h{}'$ ανήκει σε διαφορετικό κλαδί και το b_h δεν είναι πρόγονός του, γίνεται αναζήτηση ενός κοινού προγόνου. Αφού εντοπιστεί, ο κόμβος θα αναστρέψει όλες τις απαραίτητες αλλαγές από το block b_h μέχρι τον κοινό πρόγονο και θα εφαρμόσει αυτές που ορίζονται στο κλαδί του $b_h{}'$.

Ένα blockchain fork μπορεί να προεκταθεί σε μήκη μεγαλύτερα του ενός block, ως συνέχεια αντικρουόμενων blocks. Τελικά, όμως, μόνο ένα κλαδί θα επικρατήσει αποκτώντας μεγαλύτερο μήκος

από τα υπόλοιπα και οι κόμβοι που υποστήριζαν διαφορετικά κλαδιά θα το υιοθετήσουν. Σε αυτό το σημείο το blockchain fork επιλύεται και όλα τα αντίγραφα του ledger αποκτούν συνοχή αποδεχόμενα το ίδιο blockchain head. Τα blocks που τελικά απορρίπτονται από το blockchain ονομάζονται ορφανά blocks (*orphan blocks*) – *τα μωβ blocks στο Σχήμα 3.*



Σχήμα 3: *Blockchain forks, όπου τα μωβ blocks ανταγωνίζονταν τα ισοϋψή τους ως blockchain heads. Τα μαύρα blocks ορίζουν το blockchain και είναι αυτά που έχουν επικρατήσει επί των μωβ στις περιπτώσεις forks. Παρατηρούμε ότι διαδοχικά μωβ blocks αποτελούν forks με μήκη μεγαλύτερα του ενός block.*

Βάσει των παραπάνω είναι φανερό πως στο Bitcoin δεν καταχωρείται ποτέ οριστικά ένα transaction. Κάθε transaction του blockchain μπορεί να ακυρωθεί αν δημιουργηθεί μονοπάτι μεγαλύτερου μήκους που δεν το περιλαμβάνει, δηλαδή που ξεκινά από σημείο του δέντρου που είναι προγενέστερο αυτού που περιέχει το συγκεκριμένο transaction. Αν ένας επιτιθέμενος επιχειρούσε να αναστρέψει ένα transaction που συμπεριλήφθηκε στο block b_h, θα δημιουργούσε ένα νέο transaction το οποίο αντικρούεται το αρχικό και θα το συμπεριλάμβανε σε ένα block $b_{h'}$, όπου $h' < h$. Στη συνέχεια ο επιτιθέμενος θα δημιουργούσε blocks συνεχίζοντας το κλαδί του $b_{h'}$ έως ότου αυτό ξεπεράσει σε μήκος το αρχικό blockchain. Κάτι τέτοιο θα ήταν εφικτό για κάποιον ο οποίος θα ήλεγχε την πλειοψηφία της υπολογιστικής ισχύος των miners, αφού θα δημιουργούσε blocks με μεγαλύτερο ρυθμό απ’ ότι το υπόλοιπο δίκτυο και θα μπορούσε επομένως να αναστρέψει οποιοδήποτε transaction.

Η στενή σχέση μεταξύ των blocks και της εγκυρότητας ενός transaction όχι μόνο επιβραδύνει το χρόνο επιβεβαίωσης ενός transaction αλλά επίσης περιορίζει τον τρόπο επιβεβαίωσης, ώστε αυτός να ακολουθεί μια μέθοδο που βασίζεται στις πιθανότητες.

2.5 Ηλεκτρονικά πορτοφόλια

Ένα πορτοφόλι (*wallet*) αποθηκεύει τις απαραίτητες πληροφορίες για να μπορεί ένας χρήστης να συναλλάσσεται με bitcoins. Παρότι συχνά γίνεται αναφορά στα Bitcoin wallets ως μέσα “αποθήκευσης bitcoins”, τα bitcoins στην πραγματικότητα είναι άρρηκτα συνδεδεμένα με το ledger του blockchain. Μια πιο ακριβής περιγραφή ενός wallet θα ήταν ότι αποτελεί ένα μέσο “αποθήκευσης των ψηφιακών διαπιστευτηρίων για τα bitcoins που ανήκουν σε κάποιον” [7] και καθιστά δυνατή την πρόσβαση σε αυτά. Καθώς το Bitcoin χρησιμοποιεί κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού, το περιεχόμενο ενός wallet είναι κατά βάση ένα τέτοιο ζεύγος κλειδιών.

Υπάρχουν διάφοροι τύποι wallets. Τα Software wallets, εκτός της αποθήκευσης των απαραίτητων διαπιστευτηρίων για την επιβεβαίωση της κυριότητας των bitcoins τους, συνδέονται στο δίκτυο κι επιτρέπουν την πραγματοποίηση συναλλαγών. Τα Software wallets χωρίζονται σε δύο κατηγορίες:

- Πλήρεις κόμβοι (*full nodes*), οι οποίοι επιβεβαιώνουν συναλλαγές διατηρώντας ένα τοπικό αντίγραφο του blockchain ή ένα υποσύνολο αυτού. Λόγω του μεγέθους του blockchain (130GB, Σεπτέμβριος ‘17) και των επεξεργαστικών απαιτήσεών του, τα περισσότερα υπολογιστικά μηχανήματα δεν μπορούν να υποστηρίξουν μια τέτοια λειτουργία.
- Γρήγοροι κόμβοι (*fast nodes*), που είναι μηχανήματα συγχρονισμένα στο Bitcoin blockchain τα οποία όμως δε διατηρούν αντίγραφο αυτού. Μια τέτοια λειτουργία είναι εφικτή, καθώς ένας κόμβος αρκεί να έχει κατεβάσει κατά την εκκίνησή του όλο blockchain – σειριακά όλα τα blocks – για επιβεβαίωση προκειμένου να είναι βέβαιος για την ορθότητα του blockchain. Εφόσον γίνει η επιβεβαίωση της εγκυρότητας ενός block, η διατήρηση του περιεχομένου του περιττεύει.
- Απλοί πελάτες (*lightweight clients ή Simple Payment Verification – SPV clients*), οι οποίοι συμβουλεύονται full nodes για την επιβεβαίωση συναλλαγών, καθώς δε διατηρούν αντίγραφο του blockchain. Έτσι, οι lightweight clients εγκαθίστανται πολύ πιο γρήγορα σε μια συσκευή κι έχουν χαμηλές απαιτήσεις σε ισχύ και εύρος ζώνης, με αποτέλεσμα να είναι κατάλληλοι ακόμη και για smartphones. Κάνοντας χρήση ενός lightweight client, βέβαια, ο χρήστης θα πρέπει να εμπιστεύεται τον πάροχό του, ο οποίος δεν μπορεί να κλέψει bitcoins, αλλά μπορεί να παρέχει λανθασμένες ενδείξεις/επιβεβαιώσεις. Ο χρήστης αυτός μπορεί να έχει ισχυρές αποδείξεις για τις συναλλαγές του, ωστόσο δεν μπορεί να είναι ποτέ βέβαιος γι’ αυτές, μιας και ο μόνος

τρόπος για απόλυτη βεβαιότητα είναι η διατήρηση ενός τοπικού αντιγράφου του blockchain (full node).

Εκτός από τα Software wallets, υπάρχουν και οι υπηρεσίες των Online wallets, με παρόμοια λειτουργία και απλότητα στη χρήση. Σε αυτήν την περίπτωση τα διαπιστευτήρια που εξασφαλίζουν πρόσβαση στο κεφάλαιο ενός χρήστη αποθηκεύονται στον ίδιο τον πάροχο του Online wallet και όχι στο hardware του χρήστη. Αυτό προϋποθέτει την απόλυτη εμπιστοσύνη προς τον πάροχο. Ένας κακόβουλος πάροχος ή ένα κενό ασφαλείας στις online υπηρεσίες θα μπορούσε να οδηγήσει στην απώλεια των κεφαλαίων [8].

Ένας τρίτος τύπος wallet είναι τα Physical wallets, τα οποία αποθηκεύουν τα απαραίτητα διαπιστευτήρια offline [7].

2.6 Αποκέντρωση

Οι πιο σημαντικές παράμετροι του Bitcoin αυτή τη στιγμή είναι η ***εμπιστοσύνη***, η ***ασφάλεια*** και η ***ιδιωτικότητα***. Οι full nodes είναι σε θέση να ελέγξουν ότι όλοι οι κανόνες του Bitcoin ακολουθούνται πιστά. Κανόνες όπως το πρόγραμμα πληθωρισμού, το διπλό ξόδεμα (*double spending*), το ξόδεμα νομισμάτων που δεν ανήκουν στον “αποστολέα” και άλλοι είναι απαραίτητοι για τη λειτουργία του Bitcoin. Οι full nodes είναι αυτοί που δίνουν την ικανότητα στους χρήστες του Bitcoin να είναι βέβαιοι για τη σωστή λειτουργία του χωρίς να έχουν εμπιστοσύνη σε κανέναν (*trustless*). Δε χρειάζεται να υπάρχει εμπιστοσύνη σε κανένα χρηματοπιστωτικό ίδρυμα (τράπεζα, paypal), ο καθένας γνωρίζει την ορθή λειτουργία και ακεραιότητα του blockchain που ο ίδιος διατηρεί στον προσωπικό του υπολογιστή και αυτό είναι αρκετό. Το αν ο κάθε χρήστης του Bitcoin θα διατηρεί το δικό του full node για να τον χρησιμοποιεί ως wallet είναι στην κρίση του.

Εμπιστοσύνη: Η διατήρηση ενός full node και η χρήση του ως wallet είναι ο μόνος τρόπος να γνωρίζει κανείς με βεβαιότητα ότι κανένας κανόνας του Bitcoin δεν έχει παραβιαστεί. Κάθε άλλο είδος wallet προϋποθέτει την εμπιστοσύνη σε κάποιον ενδιάμεσο εξυπηρετητή. Έτσι, μέσω του προσωπικού full node είναι ο μόνος τρόπος επιβεβαίωσης των bitcoins που ο καθένας κατέχει, ενώ κάθε πληροφορία από τρίτο περιέχει μια δόση αβεβαιότητας.

Ασφάλεια: Όλοι οι έλεγχοι εγκυρότητας που πραγματοποιούν οι full nodes αυξάνουν την ασφάλεια. Υπάρχουν διάφορες επιθέσεις προς lightweight client wallets οι οποίες δεν επηρεάζουν τα full node wallets.

Ιδιωτικότητα*:* Τα full node wallets είναι μέχρι στιγμής ο καλύτερος τρόπος διατήρησης της ιδιωτικότητας στο Bitcoin, καθώς κανείς δε διαθέτει την πληροφορία για τη σύνδεση της δημόσιας διεύθυνσης (*public key*) Bitcoin με το φυσικό πρόσωπο που διαθέτει το ιδιωτικό κλειδί (*private key*) αυτής. Κάθε χρήση lightweight wallet διαρρέει πληροφορίες σχετικά με το ποιες διευθύνσεις αντιστοιχούν στον εκάστοτε χρήστη, καθώς αποστέλλουν αιτήματα σε ενδιάμεσους εξυπηρετητές. Ίσως σε πολλές περιπτώσεις τέτοιου είδους η ιδιωτικότητα να μην είναι σημαντική· σε κάθε άλλη περίπτωση η διατήρηση ενός full node είναι ο μόνος τρόπος επίτευξής της.

> "*Η διαδικασία του χρήματος είναι το να ξέρεις ότι έχεις πληρωθεί. Μια διαδικασία έχει μεγαλύτερο βαθμό αποκέντρωσης όσο πιο τοπικά συμβαίνει. Έτσι, αποκεντρωμένο χρήμα είναι το τοπικό κόστος της γνώσης ότι έχεις πληρωθεί: το κόστος του να διατηρείς έναν full node*".

> "*Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own*".
>
> — Satoshi Nakamoto

Για να αντλήσει ένας χρήστης του Bitcoin πληροφορίες σχετικά με το blockchain π.χ. για μια συναλλαγή που τον αφορά, θα πρέπει είτε να κάνει ο ίδιος έλεγχο στο blockchain, είτε να εμπιστευτεί κάποιον τρίτο. Το γεγονός της εμπιστοσύνης σε τρίτο άτομο μειώνει την τοπικότητα, δηλαδή ακυρώνει την ουσία της ύπαρξης ενός peer-to-peer. Για να διατηρηθεί ένα peer-to-peer θα πρέπει οι χρήστες της υπηρεσίας να συμμετέχουν ως μέλη αυτού (ως peers), που για το Bitcoin σημαίνει να διατηρούν έναν full node.

Το κόστος της διατήρησης ενός full node είναι υψηλό. Ωστόσο, σε ένα σύστημα όπου ο κίνδυνος παραχάραξης είναι πάντα υπολογίσιμος, ο full node αποτελεί το μοναδικό μέσο επιβεβαίωσης

ότι τα bitcoins είναι κατανεμημένα σωστά, ακολουθώντας αυστηρά όλους τους κανόνες που ορίζει το πρωτόκολλο του bitcoin.

> “*The only full node that matters is yours*”.
>
> — Peter Todd

Η σημασία της παραπάνω φράσης, ότι δηλαδή μπορεί κανείς να αρκεστεί στις δικές του πληροφορίες (αντίγραφο blockchain) για να αποδείξει την εγκυρότητα ή μη μιας συναλλαγής, οδηγεί σε ένα κρίσιμο συμπέρασμα: Ο βαθμός αποκέντρωσης του Bitcoin δεν καθορίζεται άμεσα από το πλήθος των full nodes, αλλά περισσότερο από το κόστος που απαιτείται για τη διατήρηση ενός full node.

Αν φανταστούμε το ακραίο ενδεχόμενο το κόστος αυτό να ήταν μηδενικό, ο καθένας θα ήταν σε θέση να επιβεβαιώσει την διεκπεραίωση ή μη μιας συναλλαγής και κατ’ επέκταση την ορθότητα του Bitcoin blockchain στο σύνολό του, χωρίς να βασίζεται στην αξιοπιστία ενός τρίτου. Θα ήταν δυνατότητα του κάθε ανθρώπου, ανεξαρτήτως συνόρων ή οικονομικής κατάστασης: *πλήρης αποκέντρωση*. Στο άλλο άκρο, αν το κόστος ενός full node ήταν τόσο υψηλό, ώστε να υπάρχει μόνο ένας, τότε ο διαχειριστής του θα ήλεγχε όλο το δίκτυο: *πλήρης συγκεντρωτισμός*.

2.7 Κόμβοι

Το πλήθος των full nodes του Bitcoin δεν είναι γνωστό. Όλες οι μετρήσεις που γίνονται αφορούν μόνο στους διαθέσιμους full nodes, δηλαδή σε εκείνους οι οποίοι έχουν ανοιχτά ports και είναι προσβάσιμοι. Ωστόσο, πολλοί κόμβοι βρίσκονται πίσω από τείχη προστασίας ή έχουν ρυθμιστεί έτσι, ώστε να μη δέχονται αιτήματα για συνδέσεις. Κύριος λόγος μια τέτοιας απόφασης από πλευράς χρήστη είναι κατά πάσα πιθανότητα η χρησιμοποίηση του δικτύου, αφού το εύρος ζώνης (*bandwidth*) κοστίζει. Έτσι, κανείς δε γνωρίζει τον ακριβή αριθμό των full nodes και είναι πολύ πιθανό οι κόμβοι με κλειστά ports να είναι αρκετές χιλιάδες. Επειδή, λοιπόν, μόνο οι διαθέσιμοι κόμβοι μπορούν να μετρηθούν, είναι συχνό το λάθος της θεώρησης ότι η μέτρηση του πλήθους των διαθέσιμων κόμβων αναπαριστά το σύνολο των κόμβων.

Σύμφωνα με τις μετρήσεις του [9], υπάρχουν 7,500 διαθέσιμοι full nodes. Υποθέτοντας πως όλοι κάνουν χρήση των προκαθορισμένων ρυθμίσεων του Bitcoin Core, ο καθένας είναι σε θέση να προσφέρει 117 TCP/IP συνδέσεις στο δίκτυο (125 διαθέσιμες μείων 8 για ιδία χρήση). Οι lightweight clients (Simple Payment Verification nodes) κατά κανόνα χρησιμοποιούν 4 συνδέσεις και οι Bitcoin nodes 8. Με τον όρο Bitcoin nodes γίνεται αναφορά στους full nodes και στους fast nodes. Επομένως, το δίκτυο μπορεί να υποστηρίξει έως 877,500 συνδέσεις, που μεταφράζονται στο μέγιστο των 109,687 Bitcoin nodes, ή των 219,375 SPV nodes ανά πάσα στιγμή. Βάσει των δεδομένων ενός full node [10] οι TCP/IP συνδέσεις είναι κατά μέσο όρο 100 με άλλους κόμβους και 23 με SPV nodes. Έχοντας ως δεδομένο, λοιπόν, τις 92 TCP/IP συνδέσεις για uploading προς κόμβους και τις 23 TCP/IP συνδέσεις με SPV κόμβους, μπορούμε να κάνουμε τους προσεγγιστικούς υπολογισμούς ότι 7,500*92/8 ≈ 86,000 Bitcoin nodes και 7,500*23/4 ≈ 43,000 SPV nodes.

Οι κόμβοι με ανοιχτά ports είναι χρήσιμοι για το δίκτυο του Bitcoin καθώς βοηθούν στο ξεκίνημα (*bootstrapping*) νέων κόμβων κάνοντας uploading τα blocks του blockchain – το πλήθος τους αποτελεί μετρική του αριθμού των διαθέσιμων αντιγράφων του blockchain. Προς το παρόν, το διαθέσιμο bandwidth αυτών είναι αρκετό [11] για την εξυπηρέτηση όλων των lightweight clients (wallets) και των bootstrapping κόμβων.

3 Κλιμακωσιμότητα του Bitcoin

3.1 Πρόβλημα κλιμάκωσης

Η ολοένα και αυξανόμενη υιοθέτηση ορισμένων κρυπτονομισμάτων ως μέσων πληρωμών έχει αρχίσει να προκαλεί ανησυχίες ως προς τη δυνατότητα κλιμάκωσης της τεχνολογίας τους. Καθώς το Bitcoin είναι ένα αυτοδιαχειριζόμενο σύστημα που λειτουργεί με τη δημιουγία blocks ανά χρονικά διαστήματα κατά προσέγγιση σταθερά (*block intervals*), ο μέγιστος ρυθμός εξυπηρέτησης συναλλαγών είναι ως εκ τούτου περιορισμένος και ίσος με το λόγο του μέγιστου αριθμού συναλλαγών που μπορεί να περιέχει ένα block προς το block interval.

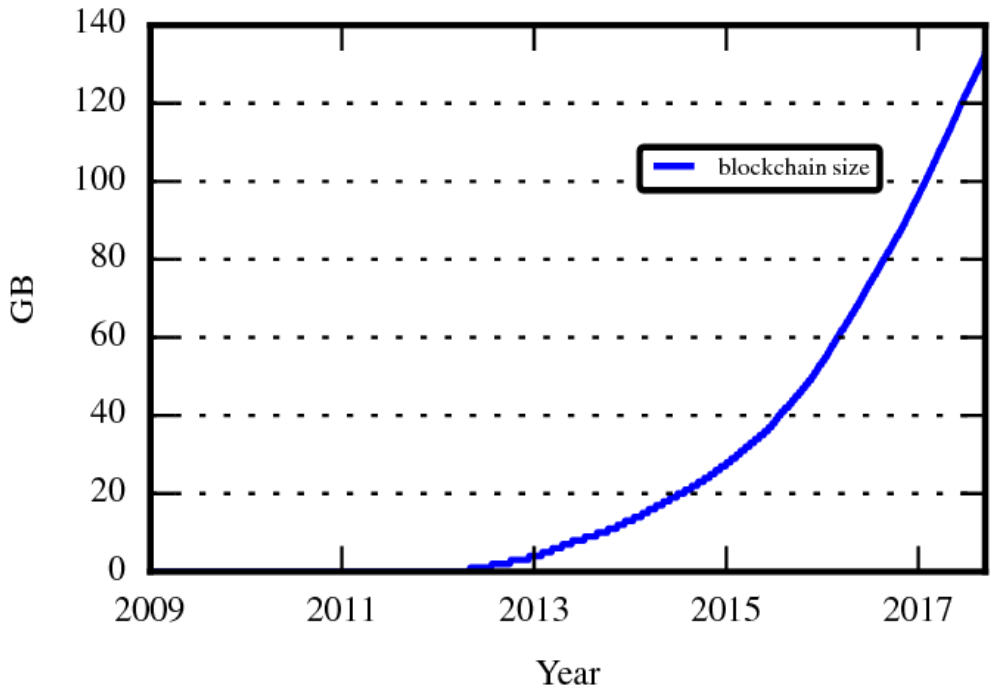
Στην κοινότητα των κρυπτονομισμάτων γίνονται διαρκώς συζητήσεις για το πώς μπορεί να βελτιωθεί η κλιμακωσιμότητα των blockchains, με πολλές ενδιαφέρουσες προτάσεις, χωρίς όμως κάποια να μοιάζει ικανή να λύση το πρόβλημα στην ολότητά του. Συγκεκριμένα για το Bitcoin, το SegWit [12] είναι η πιο επίκαιρη και αξιόλογη ενημέρωση και εφαρμόστηκε τον Αύγουστο του 2017. Επιτυγχάνει αύξηση της κλιμάκωσης του Bitcoin blockchain αλλάζοντας τη δομή του block και επιτρέποντας μεγέθη που ξεπερνούν το αρχικό όριο του 1MB, με ανώτερο όριο τα 4MB. Βέβαια, το SegWit εκτός από υποστηρικτές, όπως ήταν αναμενόμενο, συνάντησε και ορισμένους επικριτές οι οποίοι απέρριψαν το update που αποφασίστηκε από το 95% της κοινότητας του Bitcoin και όρισαν μια δική τους ενημέρωση δημιουργώντας ένα νέο κρυπτονόμισμα, το Bitcoin Cash. Το γεγονός αυτό του διχασμού μεταξύ της κοινότητας είναι ενδεικτικό της αδυναμίας καθορισμού μιας σαφούς πορείας για την αντιμετώπιση του προβλήματος της κλιμάκωσης του blockchain. Αξίζει να σημειωθεί πως το SegWit μπορεί να επιτρέπει αύξηση στο ρυθμό των συναλλαγών του Bitcoin, ωστόσο δεν αποτελεί μια μακροπρόθεσμη, αλλά ούτε καν μεσοπρόθεσμη λύση για το πρόβλημα της κλιμάκωσης του Bitcoin.

Για να έχουμε μια εικόνα των σημερινών δυνατοτήτων του Bitcoin αρκεί να σημειωθεί ότι μπορεί να εξυπηρετήσει κατά μέγιστο 7 συναλλαγές ανά δευτερόλεπτο (στην πράξη είναι 3txs/s, Αύγ. ‘17), ενώ μια συναλλαγή κατά κανόνα χρειάζεται αρκετά λεπτά ή και ώρες για να επιβεβαιωθεί. Από την άλλη, ένας συμβατικός εξυπηρετητής πληρωμών όπως η Visa είναι σε θέση να επιβεβαιώνει πληρωμές σε δευτερόλεπτα, ενώ κατά μέσο όρο επεξεργάζεται 2,000 συναλλαγές ανά δευτερόλεπτο, με μέγιστο δυνατό ρυθμό εξυπηρέτησης τις 56,000 συναλλαγές ανά δευτερόλεπτο [13]. Είναι προφανές, ότι το Bitcoin χρειάζεται μια ρηξικέλευθη αλλαγή, μια πραγματική κλιμάκωση προκειμένου να φτάσει στα επίπεδα ενός συμβατικού μέσου πληρωμών.

Το **throughput** (ρυθμός txs/s**)** μπορεί θεωρητικά να είναι παραμετροποιήσιμο, είτε αυξάνοντας το όριο στο μέγεθος ενός block είτε μειώνοντας το block interval, ωστόσο και οι δύο αυτές λύσεις συνεπάγονται κινδύνους στην ομοφωνία του blockchain και στην ασφάλεια των συναλλαγών. Πιο συγκεκριμένα, η μείωση του block interval σημαίνει ευκολότερη δημιουργία νέων blocks και εξασθένιση της ασφάλειας του proof-of-work, όπως αυτή έχει εξηγηθεί στην Ενότητα 2.3. Ακόμη, η αύξηση του μεγέθους του block θα οδηγήσει σε καθυστέρηση της διάδοσης των νέων blocks, δηλαδή σε χαμηλότερα επίπεδα ομοφωνίας, αφού μειώνεται το *effective throughput*, το οποίο αναφέρεται στο ποσοστό των κόμβων οι οποίοι είναι σε θέση να συμβαδίζουν με την εξέλιξη του blockchain δεδομένων των καθυστερήσεων του δικτύου και των ταχυτήτων που υποστηρίζουν οι συνδέσεις τους [14]. Επομένως, ο ρυθμός των συναλλαγών είναι μια παράμετρος που δύσκολα παραμετροποιείται με βάση τα σημερινά δεδομένα του Bitcoin.

Ένα δεύτερο σημείο στο οποίο υστερεί το Bitcoin έναντι άλλων μεθόδων πληρωμών είναι το **latency** (χρόνος επιβεβαίωσης μιας συναλλαγής). Μια συναλλαγή που έχει συμπεριληφθεί στο blockchain θεωρητικά δεν είναι ποτέ 100% εξασφαλισμένη. Αυτό έχει εξηγηθεί αναλυτικά στην Ενότητα 2.4 περί blockchain forks. Ωστόσο, καθώς όσο “βαθύτερα” είναι ένα block ως προς το ύψος του blockchain τόσο πιο απίθανο θεωρείται το ενδεχόμενο απόρριψής του· είθισται το block να θεωρείται οριστικοποιημένο στο blockchain αφού το έχουν διαδεχτεί ορισμένα blocks, κατ’ ελάχιστον 6 [15]. Έτσι, η επιβεβαίωση μια συναλλαγής απαιτεί τουλάχιστον μια ώρα, χωρίς να υπολογίζεται ο χρόνος που απαιτείται για να κατατεθεί αυτή σε κάποιο block του blockchain.

Μια επιπλέον περιοριστική παράμετρος είναι αυτή του **capacity και bandwidth** (αποθηκευτικού χώρου και εύρους ζώνης). Το μέγεθος του Bitcoin blockchain είναι 130GB (Αύγ. ‘17) και παρουσιάζει εκθετική αύξηση στο χρόνο (*Σχήμα 4*). Βέβαια, αυτό οφείλεται και στην αύξηση της χρήσης του Bitcoin ως μέσου πληρωμής· η σταθεροποίηση του ρυθμού των συναλλαγών στη μονάδα του χρόνου θα συνεπάγεται και σταθεροποίηση του ρυθμού αύξησης του blockchain. Δεν είναι απαραίτητο για έναν κόμβο που συμμετέχει στο mining του Bitcoin να διατηρεί στο δίσκο του όλο το αρχείο του blockchain. Στη δημοσίευση του Satoshi [16] περιγράφεται η διαδικασία του “pruning”, κατά την οποία γίνεται διαγραφή μη απαραίτητων δεδομένων σχετικών με πλήρως ξοδεμένων συναλλαγών. Με αυτόν τον τρόπο μειώνεται ο όγκος των απαιτούμενων δεδομένων για έναν κόμβο ο οποίος πραγματοποιεί επιβεβαίωση συναλλαγών (miner). Το σύνολο των μη ξοδεμένων συναλλαγών καλείται *Unspent Transaction Output set* (*UTXO-set*) και για το Bitcoin είναι περίπου 2.7GB (Αύγ. ‘17) και μαζί με κάποια δεδομένα για το χειρισμό των επαναδιατάξεων (*reorganazations*) είναι όλη η



Σχήμα 4: *Μέγεθος Bitcoin blockchain. Πηγή δεδομένων: www.blockchain.info.*

πληροφορία που χρειάζεται ένας miner. Μπορεί το σύνολο του blockchain να μην απαιτείται για τη λειτουργία του mining, ωστόσο η διατήρησή του κρίνεται απαραίτητη για τη λειτουργία ενός blockchain. Ένας λόγος είναι ότι σε ένα blockchain εξ' ορισμού θα πρέπει να μπορεί να αποδειχθεί η εγκυρότητα κάθε πληροφορίας, εν προκειμένω συναλλαγής, παρέχοντας όλη την ιστορία δημιουργίας της ξεκινώντας απ' το genesis block. Επιπλέον, το αρχείο του blockchain στο σύνολό του χρειάζεται και για την εκκίνηση (bootstrapping) νέων κόμβων, μια διαδικασία κατά την οποία γίνεται επανάληψη όλης της ιστορίας του blockchain προκειμένου ο νέος κόμβος να επιβεβαιώσει ο ίδιος την τήρηση των κανόνων του blockchain και την ορθότητα της τρέχουσας κατάστασης του blockchain, δηλαδή του UTXO-set.

Επομένως, παρ' ότι ο όγκος του Bitcoin blockchain δεν είναι απαραίτητος για έναν miner, η διατήρησή του από ορισμένους κόμβους (full nodes) είναι υποχρεωτική. Από την άλλη, ο όγκος του Bitcoin UTXO-set μοιάζει μικρός, καθώς τα 2.7GB του τωρινού μεγέθους του χωρούν στη μνήμη RAM κάθε συμβατικού υπολογιστή, όμως το μέγεθος αυτό αντιστοιχεί σε ένα ρυθμό συναλλαγών 3txs/s. Η περαιτέρω διάδοση του Bitcoin ως μέσου πληρωμών μπορεί να οδηγήσει σε μεγέθη UTXO-set που δε χωρούν στη μνήμη ενός συμβατικού υπολογιστή, κάτι που συνεπάγεται προσβάσεις στο

δίσκο. Σε αυτήν την περίπτωση η χρήση δίσκων SSD μπορεί να είναι αρκετή, ώστε το μέγεθος του UTXO-set είναι πιθανό να μην αποτελέσει περιοριστικό παράγοντα για τις επιδόσεις του Bitcoin [17] και μπορεί -προς το παρόν- να θεωρηθεί δευτερεύουσας σημασίας για την κλιμάκωσή του.

3.2 Προτάσεις κλιμάκωσης

3.2.1 Sharding

Η βασική ιδέα του sharding είναι ο διαχωρισμός του state ενός blockchain σε K = O(n/c) διαμερίσεις που καλούνται “shards” (n διευθύνσεις, c διευθύνσεις ανά shard). Για παράδειγμα, ένα σενάριο sharding του Ethereum είναι ο διαχωρισμός βάσει διεύθυνσης: οι διευθύνσεις που ξεκινούν από 0x00 αποτελούν το πρώτο shard, αυτές που ξεκινούν από 0x01 το δεύτερο κ.ο.κ. Στο απλούστερο μοντέλο, κάθε shard έχει τη δική του ιστορία από transactions, δηλαδή τα transactions ενός shard k επηρεάζουν μόνο την κατάσταση (state) του shard k. Σε πιο εξελιγμένες μορφές sharding περιλαμβάνεται και η δυνατότητα cross-shard επικοινωνίας (επικοινωνία μεταξύ shards), όπου τα transactions ενός shard μπορούν να προκαλέσουν γεγονότα σε άλλα shards.

Ένας βασικός σχεδιασμός ενός sharded blockchain θα μπορούσε να είναι ο ακόλουθος. Υπάρχουν κόμβοι που καλούνται συλλέκτες (collators) οι οποίοι δέχονται transactions ενός συγκεκριμένου shard k (η επιλογή τους εξαρτάται απ’ το πρωτόκολλο) και δημιουργούν συλλογές (collations). Κάθε συλλογή έχει τη δική της επικεφαλίδα, που περιέχει στοιχεία όπως:

- ταυτότητα – όνομα shard
- root προηγούμενης κατάστασής του (pre-state)
- root κατάστασης αφού εφαρμοστούν τα transactions του (post-state)
- ταυτότητες των συλλεκτών που το υπογράφουν

Ένα (top-level) block θα πρέπει να περιέχει μια επικεφαλίδα συλλογής για κάθε shard και θεωρείται έγκυρο όταν:

- το pre-state root κάθε συλλογής ταυτίζεται με το root της τρέχουσας κατάστασης.
- όλα τα transactions των συλλογών είναι έγκυρα.

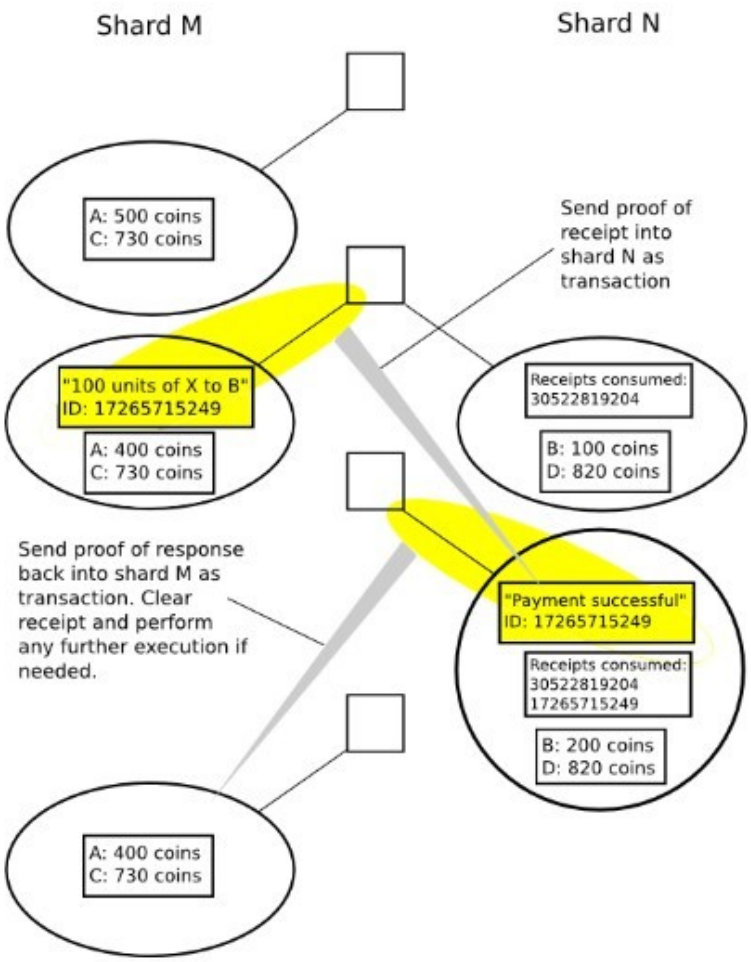
- το post-state root που δίνεται σε κάθε συλλογή ταυτίζεται με το αποτέλεσμα της εφαρμογής των transactions του στο pre-state.
- κάθε συλλογή διαθέτει τις υπογραφές τουλάχιστων των 2/3 των συλλεκτών που είναι εγγεγραμμένοι στο αντίστοιχο shard.

Σε ένα τέτοιο σύστημα μπορεί να υπάρχουν κόμβοι διαφόρων επιπέδων:

- Super-full node: επεξεργάζεται όλες τις συναλλαγές σε όλες τις συλλογές και διατηρεί την κατάσταση όλων των shards.
- Top-level node: επεξεργάζεται όλα τα top-level blocks, αλλά δεν κάνει επεξεργασία ούτε λήψη των transactions κάθε συλλογής. Αντ' αυτού, τα αποδέχεται εμπιστευόμενοι τουλάχιστον τα 2/3 των συλλεκτών κάθε shard ως μη καλόβουλους χρήστες.
- Single-shard node: ενεργεί όπως ένας top-level node, αλλά επεξεργάζεται τα transactions και διατηρεί το full state ενός συγκεκριμένου shard.
- Light node: κάνει λήψη και επιβεβαίωση μόνο των επικεφαλίδων των top-level blocks. Δεν επεξεργάζεται καμία επικεφαλίδα συλλογής ή transaction, εκτός κι αν επιθυμεί να διαβάσει κάποια καταχώρηση στο state ενός shard, οπότε και κάνει λήψη του Merkle branch της πιο πρόσφατης επικεφαλίδας συλλογής του και απομονώνει την απόδειξη (Merkle proof) της επιθυμητής τιμής του state.

Οι πιο σημαντικές προκλήσεις που πρέπει να αντιμετωπιστούν είναι:

- η ανίχνευση απάτης από τα διάφορα είδη κόμβων, για παράδειγμα συλλογή με μη έγκυρο transaction.
- η ανοχή σε επιθέσεις κατάληψης, όταν ένας επιτιθέμενος καταλαμβάνει την πλειοψηφία των συλλεκτών ενός shard.
- η cross-shard επικοινωνία.
- το superquadratic sharding, όταν $n > c^2$ και υπάρχουν περισσότερες από O(c) επικεφαλίδες συλλογής. Σε αυτήν την περίπτωση ένας κοινός κόμβος δε θα δύναται να επεξεργαστεί ούτε καν τα top-level blocks και απαιτούνται περισσότερα του ενός στρώματος ανακατεύθυνσης των transactions (shards εντός shards).



Σχήμα 5: *Cross-shard transaction αποστολής 100 νομισμάτων από τον A του shard M στον B του shard N. Πηγή:* https://github.com/ethereum.

Ορισμένες εφαρμογές σε blockchain δεν απαιτούν καμία αλληλεπίδραση με άλλη εφαρμογή. Τα blockchains με πλήρως ετερογενείς εφαρμογές, λοιπόν, δε χρειάζονται διαλειτουργικότητα και είναι οι απλούστερες περιπτώσεις. Σχετικά με εφαρμογές που χρειάζονται αλληλεπίδραση, η λύση είναι εύκολη αν αυτή μπορεί να γίνει με ασύγχρονο τρόπο. Μια μεταφορά χρημάτων, επί παραδείγματι, είναι δυνατό να γίνει σε δύο στάδια. Για τη μεταφορά κεφαλαίου από το shard M στο shard N αρχικά γίνεται ένα transaction χρέωσης που καταστρέφει κεφάλαιο στο shard M. Σε δεύτερο χρόνο μπορεί να γίνει ένα transaction πίστωσης του ποσού στο shard N, το οποίο θα αναφέρει την απόδειξη του shard M ως απόδειξη νομιμότητας της πίστωσης. Τα προβλήματα αρχίζουν όταν απαιτούνται ατομικές ενέργειες μεταξύ shards, δηλαδή ενέργειες σε δύο ή περισσότερα shards που είτε θα πραγματοποιούνται όλες μαζί είτε δε θα γίνεται καμία.

3.2.2 Proof-of-stake

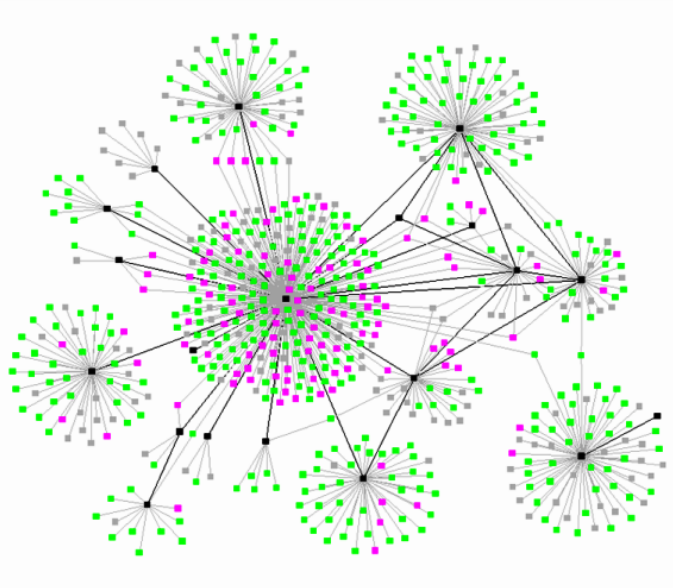
Το proof-of-stake (PoS) είναι η εναλλακτική πρόταση του proof-of-work και σύμφωνα με αυτό οι miners επιλέγονται για εξόρυξη blocks σύμφωνα με το κεφάλαιο κρυπτονομισμάτων που διαθέτουν. Αυτό σημαίνει πως όσο περισσότερα bitcoins έχει ένας miner ενός υποτιθέμενου proof-of-stake Bitcoin, τόσο μεγαλύτερη θα είναι και η ισχύς εξόρυξής του. Πρόκειται για ένα πρωτόκολλο που υιοθετήθηκε πρώτα από το κρυπτονόμισμα Peercoin, ενώ τα Nxt, Blackcoin και ShadowCoin σύντομα ακολούθησαν.

Το proof-of-stake δημιουργήθηκε ως εναλλακτική του proof-of-work, προκειμένου να ξεπεραστούν τα εγγενή προβλήματα του δεύτερου (χρόνος, ισχύς, εξοπλισμός). Ενδεικτικά, υπολογίζεται πως το 2015 η ηλεκτρική ενέργεια που ξοδευόταν για μία συναλλαγή του Bitcoin ήταν 57% μεγαλύτερη από αυτή που κατανάλωνε ένα μέσο αμερικάνικο νοικοκυριό σε μία ημέρα [18]. Το proof-of-stake αντιμετωπίζει το ζήτημα αποδίδοντας την ισχύ εξόρυξης στο σύνολο των κατόχων του εκάστοτε κρυπτονομίσματος, αναλογικά με το κεφάλαιό τους. Με αυτόν τον τρόπο, αντί να ξοδεύει ενέργεια για να βρίσκει λύσεις σε proof-of-work γρίφους, ένας miner περιορίζεται στην εξόρυξη του ποσοστού των συναλλαγών που ορίζεται βάσει του κεφαλαίου που διαθέτει. Αν, για παράδειγμα, ένας miner διαθέτει το 2% των συνολικών Bitcoins, θα μπορεί θεωρητικά να κάνει mining του 2% των blocks.

Ο τρόπος με τον οποίο εξασφαλίζεται η άμυνα έναντι κακόβουλων miners είναι η ποινή της απώλειας του κεφαλαίου για όποιον χρήστη δημοσιοποιήσει block με παραποιημένα στοιχεία. Ένα επιπλέον προτέρημα του proof-of-stake είναι η μεγαλύτερη ασφάλεια έναντι της επίθεσης του 51%. Καθώς για να είναι δυνατή μια τέτοια επίθεση θα πρέπει ο επιτιθέμενος να διαθέτει το 51% του συνολικού κεφαλαίου, μια επίθεση σε ένα δίκτυο που διαθέτει την πλειοψηφία των “μετοχών” σίγουρα δε θα ήταν προς το συμφέρον του, καθώς θα μπορούσε να ρίξει σημαντικά την αξία του κεφαλαίου του. Στην πραγματικότητα, ένας τέτοιος κεφαλαιούχος θα επιθυμούσε τη διατήρηση της σταθερότητας και της ασφάλειας του δικτύου.

3.2.3 Lightning networks

Το Bitcoin πρακτικά δεν έχει τη δυνατότητα να λειτουργήσει ως πλατφόρμα για την πραγματοποίηση μικροσυναλλαγών (*micropayments*), συναλλαγών μικροποσών που αφορούν στην καθημερινότητα, όπως η αγορά ενός καφέ ή η πληρωμή μιας θέσης parking. Παρ' ότι είναι δυνατή η αποστολή μιας πολύ μικρής αξίας σε bitcoin, υπάρχουν ορισμένοι παράγοντες που ουσιαστικά καθιστούν τη χρήση του Bitcoin για μικροσυναλλαγές απαγορευτική. Αρχικά, η αποστολή πολλών συναλλαγών σε μικρό χρονικό διάστημα ενεργοποιεί διάφορους αλγορίθμους που αποτρέπουν την πλημμύρα στο δίκτυο του Bitcoin, οδηγώντας είτε σε χαμηλή προτεραιότητα είτε σε άρνηση αναμετάδοσης των συναλλαγών. Εκτός αυτού, ο παραλήπτης πολλών μικροπληρωμών θα καταλήξει με ένα wallet γεμάτο *"dust"*, δηλαδή πολύ μικρά unspent transaction outputs των οποίως το κόστος ξοδέματος είναι μεγαλύτερο της αξίας τους. Αλλά εκτός όλων αυτών των τεχνικών εμποδίων, το πρόβλημα είναι επίσης καθαρά πρακτικό: δεν είναι δυνατό να εξυπηρετούνται μικροπληρωμές από ένα σύστημα που έχει δυνατότητα εξυπηρέτησης 7 txs/s και απαιτεί τουλάχιστον μία ώρα για να επιβεβαιώσει μια συναλλαγή που μάλιστα αυξάνει το ledger του κατά 0.4KB.



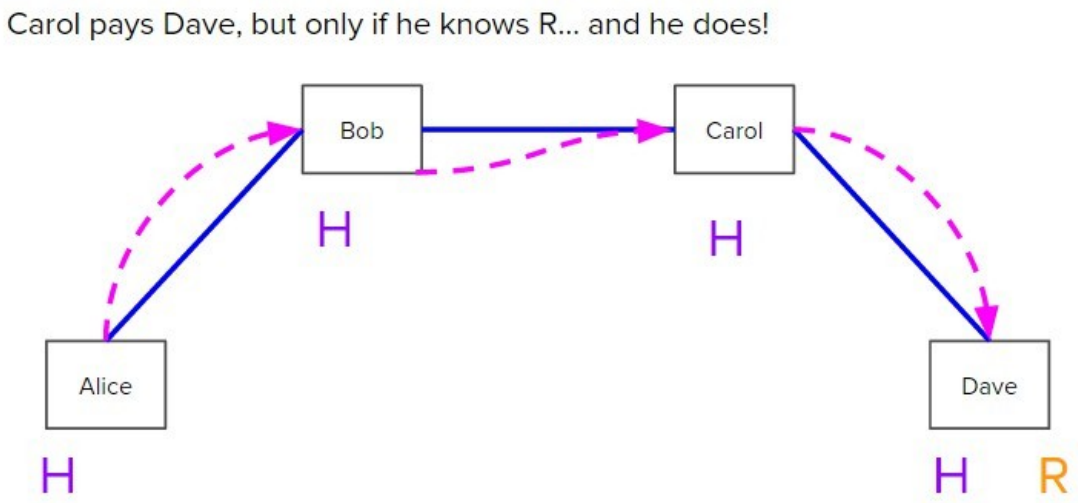
Σχήμα 6: *Η δομή ενός hub spoke lightning network, όπου οι απλοί χρήστες συνδέονται με κεντρικά σημεία (hubs). Η διασύνδεση των τελευταίων οδηγεί σε συνδεδεμένο γράφο. Πηγή: https://chrispacia.wordpress.com.*

Καθώς το Bitcoin αδυνατεί να εξυπηρετήσει μικροπληρωμές, προτείνεται η δημιουργία ενός δικτύου που λειτουργεί ως δίκτυο ανώτερου στρώματος του Bitcoin (overlay network) το οποίο καλείται lightning network. Το lightning network είναι ένα peer-to-peer σύστημα για την εξυπηρέτηση

micropayments μέσω ψηφιακών νομισμάτων όπως το Bitcoin μέσω ενός scale-free δικτύου από αμφίδρομα κανάλια πληρωμών (*payment channels*) χωρίς να γίνεται ανάθεση κεφαλαίων ή να απαιτείται εμπιστοσύνη σε τρίτα πρόσωπα. Μέσω των payment channels οι συμμετέχοντες μπορούν να πραγματοποιούν μεταφορές χρημάτων μεταξύ τους χωρίς να χρειάζεται η δημοσίευση όλων των συναλλαγών τους στο blockchain. Αυτό είναι δυνατό καθώς το πρωτόκολλο του lightning network παρέχει προστασία στους συμμετέχοντες τόσο έναντι μη συνεργάσιμων χρηστών όσο και έναντι απώλειας κεφαλαίου, εκμεταλλευόμενο τις ιδιότητες του ίδιου του Bitcoin. Για τη συμμετοχή σε ένα lightning network απαιτείται μόνο μία συναλλαγή στο blockchain, αυτή της ενεργοποίησης ενός payment channel του χρήστη, ενώ η συμμετοχή μπορεί να διακοπεί οποιαδήποτε στιγμή με μια συναλλαγή τερματισμού του payment channel.

Η τυπική χρήση του lightning network ξεκινά με το άνοιγμα ενός payment channel κάνοντας μια συναλλαγή χρηματοδότησης στο blockchain. Στη συνέχεια είναι δυνατή η πραγματοποίηση οσωνδήποτε συναλλαγών εντός του lightning network. Οι συναλλαγές αυτές ενημερώνουν την κατανομή των κεφαλαίων στο channel αλλά όχι στο blockchain. Ο τρόπος διασφάλισης της εγκυρότητας των συναλλαγών αυτών είναι η υπογραφή μιας προσωρινής συναλλαγής, την οποία μπορεί ανά πάσα στιγμή κάποιος απ’ τους συμμετέχοντες να καταθέσει στο blockchain και να διεκδικήσει το κεφάλαιό του. Με αυτόν τον τρόπο γίνεται και το κλείσιμο ενός payment channel.

> If we *presume a large network of channels on the Bitcoin blockchain, and all Bitcoin users are participating on this graph by having at least one channel open on the Bitcoin blockchain, it is possible to create a near-infinite amount of transactions inside this network. The only transactions that are broadcast on the Bitcoin blockchain prematurely are with uncooperative channel counterparties.*
>
> — Lightning Paper [19]



Σχήμα 7: *Υλοποίηση πληρωμής εντός lightning network. Η Alice επιθυμεί να στείλει ένα x ποσό στον Dave και μοιράζεται μαζί του το ιδιωτικό κλειδί R ενός ζεύγους δημόσιου-ιδιωτικού κλειδιού H-R. Στη συνέχεια, γίνονται διαδοχικές υποσχέσεις πληρωμής στο μπλε μονοπάτι "θα σου δώσω το x ποσό αν γνωρίζεις το R", (ροζ βέλη). Το R ξεκινά απ' τον Dave και καταλήγει στην Alice, με τελικό αποτέλεσμα την αποστολή x ποσού απ' την Alice προς τον Dave.*

Η υλοποίηση lightning networks έχει ήδη αρχίσει για το Bitcoin. Η ενημέρωση SegWit [12], η οποία αυξάνει το μέγεθος των blocks και αναδιατάσσει τα δεδομένα τους, επιλύοντας ταυτόχρονα ένα ζήτημα ασφάλειας που υπήρχε σχετικά με τις συναλλαγές, δίνει ουσιαστικά το πράσινο φως για τη λειτουργία lightning networks στο mainnet [20].

3.2.4 Τι νέο προτείνεται στην εργασία

Στην παρούσα εργασία θα γίνει μελέτη με στόχο τη μείωση του capacity, ενός εκ των προβλημάτων κλιμάκωσης του blockchain. Όπως έχει αναλυθεί και στην Ενότητα 2.6, η διατήρηση όλων των δεδομένων ενός blockchain κρίνεται απαραίτητη για τη λειτουργία του. Ένας full node του Bitcoin σήμερα διαθέτει 130GB αποθηκευτικού χώρου για την αποθήκευση του blockchain. Μπορεί ένας κόμβος να μην είναι υποχρεωτικό να διατηρεί την πληροφορία αυτή τοπικά, ωστόσο η αποθήκευσή του είναι αυτή που κάνει το blockchain αποκεντρωμένο· είναι η ειδοποιός διαφορά μεταξύ του blockchain κι ενός συστήματος που βασίζεται σε κεντρικούς servers.

Ο τρόπος με τον οποίο θα γίνει η κλιμάκωση του capacity είναι με την οργάνωση των κόμβων ενός blockchain σε ένα Distributed Hash Table. Το DHT είναι ένα δομημένο peer-to-peer δίκτυο το οποίο προσφέρει υπηρεσίες αναζήτησης δεδομένων διαμοιράζοντάς τα στο σύνολο των συμμετέχοντων κόμβων. Τα peer-to-peer δίκτυα και συγκεκριμένα τα DHTs θα αναλυθούν στο Κεφάλαιο 4, ενώ θα ακολουθήσει αξιολόγηση του εν λόγω συστήματος στο Κεφάλαιο 5.

4 Peer-to-peer δίκτυα

Το peer-to-peer είναι μια αρχιτεκτονική για κατανεμημένες εφαρμογές η οποία διαμερίζει εργασίες και διαμοιράζει το φόρτο εργασίας σε ένα σύνολο από ομότιμους κόμβους. Οι κόμβοι είναι ομότιμοι (*peers*), δηλαδή έχουν τα ίδια προνόμια, τις ίδιες δυνατότητες και τον ίδιο ρόλο ως συμμετέχοντες στην εκάστοτε εφαρμογή. Οι peers διαθέτουν ένα μέρος των πόρων τους, π.χ. επεξεργαστική ισχύ, αποθηκευτικό χώρο δίσκου, εύρος ζώνης δικτύου, στους συμμετέχοντες του δικτύου χωρίς να απαιτείται κάποιος κεντρικός συντονισμός από servers ή συγκεκριμένα μέλη του δικτύου. Οι peers είναι εξυπηρετητές και καταναλωτές πόρων μάζι, σε αντίθεση με το παραδοσιακό μοντέλο πελάτη-εξυπηρετητή στο οποίο οι ρόλοι είναι διακριτοί. Παρότι τα peer-to-peer συστήματα είχαν εμφανιστεί νωρίτερα σε ποικίλες εφαρμογές, η αρχιτεκτονική αυτή έγινε κυρίως γνωστή από την εφαρμογή της στο σύστημα ανταλλαγής αρχείων Napster, το οποίο κυκλοφόρησε το 1999. Η ιδέα του Napster έχει έκτοτε αποτελέσει πηγή έμπνευσης για πληθώρα νέων εφαρμογών και δομών με βάση την peer-to-peer αρχιτεκτονική. Το κίνημα του peer-to-peer έχει δώσει τη δυνατότητα σε εκατομμύρια χρηστών του ίντερνετ να συνδέονται κατευθείαν, σχηματίζοντας ομάδες και να “συνεργάζονται για τη δημιουργία μηχανών αναζήτησης, εικονικών υπερυπολογιστών και συστημάτων αρχείων” [21].

4.1 Αρχιτεκτονική peer-to-peer

Ένα peer-to-peer δίκτυο είναι σχεδιασμένο πάνω στην έννοια των ομότιμων κόμβων (*peers*) οι οποίοι λειτουργούν ταυτόχρονα ως πελάτες (*clients*) και εξυπηρετητές (*servers*) προς τους άλλους κόμβους του δικτύου.

Τα peer-to-peer δίκτυα εφαρμόζουν ένα είδος εικονικού δικτύου ανώτερου στρώματος πάνω στο φυσικό επίπεδο της τοπολογίας του δικτύου, όπου οι κόμβοι στο στρώμα του peer-to-peer αποτελούνται από ένα υποσύνολο κόμβων του φυσικού δικτύου. Τα δεδομένα αποστέλλονται κατευθείαν μέσω του υποκείμενου TCP/IP δικτύου, ωστόσο στο στρώμα εφαρμογής οι peers έχουν τη δυνατότητα απευθείας επικοινωνίας μεταξύ τους, διαμέσω των λογικών συνδέσεων του δικτύου ανέτερου στρώματος (καθεμία εκ των οποίων αντιστοιχεί σε μια πραγματική σύνδεση στο φυσικό στρώμα του δικτύου). Τα στρώματα ανώτερου επιπέδου χρησιμοποιούνται για τη δεικτοδότηση και την εύρεση των peers, καθιστώντας το peer-to-peer σύστημα ανεξάρτητο της τοπολογίας του δικτύου φυσικού στρώματος. Ανάλογα με τον τρόπο που οι κόμβοι συνδέονται στο δίκτυο ανώτερου

στρώματος και οι πόροι δεικτοδοτούνται και ευρίσκονται, τα peer-to-peer δίκτυα κατατάσσονται σε *αδόμητα* (*unstructured*) και δομημένα (*structured*).

Αδόμητα: Τα αδόμητα peer-to-peer δίκτυα εκ σχεδιασμού δεν επιβάλλουν κάποια συγκεκριμένη δομή στο δίκτυο ανώτερου στρώματος, αλλά σχηματίζονται μέσω κόμβων οι οποίοι πραγματοποιούν τυχαίες συνδέσεις μεταξύ τους (π.χ. Gnutella, Kazaa) [22]. Επειδή δεν επιβάλλεται συγκεκριμένη δομή, τα αδόμητα δίκτυα κτίζονται εύκολα και επιτρέπουν βελτιστοποιήσεις ανάλογα με την τοποθεσία των κόμβων. Επίσης, καθώς όλοι οι κόμβοι έχουν τον ίδιο ρόλο, τα αδόμητα δίκτυα είναι εύρωστα σε συνθήκες υψηλών ρυθμών άφιξης και αναχώρησης κόμβων (*churn*). Ωστόσο, η έλλειψη ορισμένης δομής επιφέρει και ορισμένα αρνητικά. Συγκεκριμένα, στην περίπτωση όπου ένας κόμβος αναζητά συγκεκριμένα δεδομένα, το ερώτημά του θα πρέπει να πλημμυριστεί στο δίκτυο ώστε να βρει όσο το δυνατό περισσότερους κόμβους που το διαθέτουν και μπορούν να το μοιραστούν. Η μέθοδος της πλημμύρας προκαλεί πολύ υψηλά επίπεδα συμφόρησης του δικτύου, απαιτεί συνολικά απ' το δίκτυο περισσότερη υπολογιστική ισχύ και μνήμη (απαιτώντας από κάθε κόμβο να επεξεργάζεται όλα τα ερωτήματα αναζήτησης). Ταυτόχρονα, δεν εξασφαλίζει ότι το ερώτημα θα φτάσει στον κατάλληλο κόμβο για να εξυπηρετηθεί, αφού δεν υπάρχει συσχετισμός μεταξύ των κόμβων και των δεδομένων που αυτοί διαχειρίζονται. Δημοφιλή δεδομένα είναι πιθανό να βρίσκονται σε πολλούς κόμβους και να εντοπίζονται εύκολα. Στην περίπτωση, όμως, που ένας κόμβος αναζητεί πιο σπάνια δεδομένα που μόνο λίγοι κόμβοι διαθέτουν, είναι πολύ πιθανό η αναζήτησή τους να μην είναι επιτυχής.

Δομημένα: Στα δομημένα peer-to-peer δίκτυα το στρώμα ανώτερου επιπέδου οργανώνεται σχηματίζοντας συγκεκριμένη τοπολογία και το πρωτόκολλό τους εξασφαλίζει ότι οποιοσδήποτε κόμβος μπορεί να αναζητήσει αποτελεσματικά ένα αρχείο ή κάποιον πόρο του δικτύου, ανεξάρτητα από τη σπανιότητα αυτού. Ο πιο κοινός τύπος εφαρμογής δομημένου peer-to-peer δικτύου είναι το *distributed hash table* (DHT), όπου γίνεται χρήση μιας συνάρτησης κατακερματισμού (hash function) για την ανάθεση της κυριότητας αρχείων στους κόμβους του δικτύου. Αυτό επιτρέπει τους peers να κάνουν αναζήτηση πόρων στο δίκτυο με τη χρήση ενός hash table: τα αρχεία αποθηκεύονται στο DHT σε ζεύγη [κλειδί,τιμή] και κάθε κόμβος μπορεί να ανακτήσει με αποτελεσματικότητα την τιμή που σχετίζεται με κάποιο δοσμένο κλειδί.

4.2 DHT

Ένα distributed hash table (DHT) είναι μια κλάση από αποκεντρωμένα κατανεμημένα συστήματα η οποία προσφέρει μια υπηρεσία αναζήτησης δεδομένων παρόμοια με αυτή του hash table: [κλειδί, τιμή] ζεύγη αποθηκεύονται σε ένα DHT και κάθε συμμετέχων κόμβος μπορεί με αποτελεσματικό τρόπο να ανακτήσει την τιμή με την οποία σχετίζεται ένα δοθέν κλειδί. Η ευθύνη για τη διατήρηση των συσχετίσεων κλειδιών-τιμών κατανέμεται σε όλους τους κόμβους, με τέτοιον τρόπο ώστε η αλλαγή στο σύνολο των συμμετέχοντων κόμβων να προκαλεί τον ελάχιστο δυνατό αποσυντονισμό. Αυτή η ιδιότητα επιτρέπει σε ένα DHT να κλιμακώνει σε εκπληκτικά μεγάλα νούμερα πλήθους κόμβων και να αντεπεξέρχεται σε συνεχείς αφίξεις, αναχωρήσεις και αποτυχίες κόμβων.

Ιστορία

Το ενδιαφέρον και η έρευνα γύρω απ’ το DHT ξεκίνησε με την εμφάνιση peer-to-peer συστημάτων όπως τα Freenet, Gnutella, BitTorrent και Napster, τα οποία εκμεταλλεύονταν πόρους κατανεμημένους στο ίντερνετ για να προσφέρουν μια εφαρμογή. Πιο συγκεκριμένα, εκμεταλλεύτηκαν το μεγάλο εύρος ζώνης και αποθηκευτικό χώρο σκληρού δίσκου των κατανεμημένων πόρων για να προσφέρουν μια υπηρεσία ανταλλαγής αρχείων.

Αυτά τα συστήματα διέφεραν στον τρόπο με τον οποίο εντόπιζαν τα δεδομένα που προσέφεραν οι χρήστες (peers). Το Napster, το πρώτο peer-to-peer σύστημα μεταφοράς δεδομένων μεγάλης κλίμακας, απαιτούσε έναν κεντρικό εξυπηρετητή δεικτών (central index server): κάθε κόμβος, κατά την είσοδό του στο σύστημα, θα έστελνε μια λίστα των τοπικά αποθηκευμένων αρχείων του στον εξυπηρετητή, ο οποίος επιτελούσε την εργασία της παραπομπής των αιτημάτων για συγκεκριμένα αρχεία στους peers που τα διέθεταν. Αυτό το κεντρικό κομμάτι του συστήματος το έκανε ευπαθές σε ψηφιακές και νομικές επιθέσεις.

Το Gnutella και παρόμοια δίκτυα υιοθέτησαν τη λογική ενός μοντέλου πλυμμήρας των ερωτημάτων (query flooding) – με αποτέλεσμα κάθε μήνυμα αναζήτησης να αναμεταδίδεται σε σε κάθε μηχάνημα που συμμετέχει στο δίκτυο. Παρ’ ότι λύνει το πρόβλημα του ενός σημείου αποτυχίας (single point of failure), αυτή η μέθοδος ήταν σημαντικά λιγότερο αποδοτική από αυτή του Napster.

Το Freenet είναι πλήρων κατανεμημένο, αλλά εφαρμόζει μια μέθοδο δρομολόγησης σύμφωνα με την οποία κάθε αρχείο συσχετίσεται με ένα κλειδί, και αρχεία με παρόμοια κλειδιά τείνουν να

συγκεντρώνονται σε συστάδες κόμβων. Παρ’ ότι τα ερωτήματα είναι πολύ πιθανό να οδηγηθούν διαμέσω του δικτύου σε μια τέτοια συστάδα, ωστόσο το Freenet δεν εγγυάται πως τα δεδομένα που αναζητούνται θα μπορέσουν να εντοπιστούν.

Τα distributed hash tables κάνουν χρήση μιας πιο δομημένης μεθόδου δρομολόγησης βασιζόμενης σε κλειδιά, με στόχο να πετύχει τόσο την αποκέντρωση των Freenet και Gnutella, όσο και την αποδοτικότητα και τα εγγυημένα αποτελέσματα του Napster.

Το 2001, τέσσερα συστήματα – CAN [23], Chord [24], Pastry, Tapestry – έδωσαν το έναυσμα για την ανάδειξη των DHTs σε δημοφιλές πεδίο έρευνας. Ένα project με όνομα Infrastructure for Resilient Internet Systems (Iris) χρηματοδοτήθηκε από το Αμερικάνικο Ίδρυμα Επιστημών (US NSF) με $12 εκατομμύρια [25]. Στους ερευνητές συμπεριλαμβάνονταν οι Sylvia Ratnasamy, Ion Stoica, Hari Balakrishnan και Scott Shenker [26]. Εκτός της ακαδημαϊκής κοινότητας, η τεχνολογία του DHT έχει υιοθετηθεί ως στοιχείο του BitTorrent [27] και στο Coral Content Distribution Network [28].

Ιδιότητες

Τα DHTs δίνουν ιδιαίτερη έμφαση στις παρακάτω ιδιότητες:

- Αυτονομία και αποκέντρωση: οι κόμβοι σχηματίζουν συλλογικά το σύστημα χωρίς την ύπαρξη κάποιου κεντρικού συντονιστή.
- Ανοχή σε σφάλματα: το σύστημα θα πρέπει να είναι αξιόπιστο ακόμη και υπό συνθήκες συνεχών αφίξεων, αναχωρήσεων και αποτυχιών κόμβων.
- Κλιμακωσιμότητα: το σύστημα θα πρέπει αν λειτουργεί αποδοτικά ακόμη και με χιλιάδες ή εκατομμύρια κόμβους.

Η βασική τεχνική που χρησιμοποιείται για να επίτευξη αυτών των στόχων είναι ότι ο κάθε κόμβος χρειάζεται να συντονίζεται μόνο με ένα μικρό μέρος των συνολικών κόμβων του συστήματος – συνήθως με O(log n) όπου n το πλήθος των κόμβων του συστήματος – έτσι ώστε να χρειάζεται μικρό ποσό εργασίας για κάθε αλλαγή στους συμμετέχοντες κόμβους (π.χ. αναχώρηση).

Υπάρχουν κάποια κλασικά ζητήματα τα οποία τα DHTs καλούνται να αντιμετωπίζουν, όπως η κατανομή του φορτίου, η ακεραιότητα των δεδομένων και η απόδοση (συγκεκριμένα, η εξασφάλιση

ότι λειτουργίες όπως η δρομολόγηση και η αποθήκευση ή ανάκτηση δεδομένων ολοκληρώνονται με ταχύτητα).

Δομή

Η δομή ενός DHT μπορεί να αναλυθεί σε διάφορα κύρια στοιχεία [29], [30]. Το θεμελιώδες είναι ένα αφηρημένο πεδίο κλειδιών (keyspace), όπως το σύνολο όλων των 160-bit συμβολοσειρών. Ένα σχήμα διαμέρισης του πεδίου κλειδιών κατανέμει την κυριότητα αυτού στο σύνολο των συμμετέχοντων κόμβων. Στη συνέχεια, ένα δίκτυο ανώτερου στρώματος (overlay network) συνδέει τους κόμβους, δίνοντάς τους την ικανότητα να βρίσκουν τον κάτοχο οποιουδήποτε δοθέντος κλειδιού εντός του πεδίου κλειδιών.

Μια τυπική χρήση ενός DHT για αποθήκευση και ανάκτηση δεδομένων μπορεί να γίνεται ως ακολούθως. Υποθέτουμε ότι το πεδίο κλειδιών είναι το σύνολο των 160-bit συμβολοσειρών. Για να δεικτοδοτήσουμε ένα αρχείο με κάποιο συγκεκριμένο όνομα (*filename*) και δεδομένα (*data*) σε ένα DHT, παράγεται η SHA-1 hash τιμή του ονόματος αρχείου (hash(*filename*)), η οποία δημιουργεί ένα 160-bit κλειδί *k*, κι ένα μήνυμα *put(k, data)* αποστέλλεται σε οποιονδήποτε κόμβο που συμμετέχει στο DHT. Το μήνυμα προωθείται από κόμβο σε κόμβο διαμέσω του overlay δικτύου έως ότου φτάσει στο μοναδικό κόμβο ο οποίος είναι υπεύθυνος για το κλειδί *k*, όπως ορίζεται βάσει της διαμέρισης του πεδίου κλειδιών. Στη συνέχεια, ο κόμβος αυτός αποθηκεύει το ζεύγος (*k, data*). Μετά απ’ αυτό οποιοσδήποτε χρήστης/πελάτης μπορεί να ανακτήσει τα περιεχόμενα του αρχείου παράγοντας πάλι το κλειδί *k* μέσω της συνάρτησης SHA-1 με είσοδο το filename και κάνοντας αίτηση σε οποιονδήποτε κόμβο του DHT για εύρεση των δεδομένων που σχετίζονται με το k με ένα μήνυμα *get(k)*. Το μήνυμα αυτό θα δρομολογηθεί ξανά διαμέσω του overlay δικτύου στον κόμβο που είναι υπεύθυνος για το *k*, ο οποίος θα απαντήσει με τα *data* που έχει αποθηκευμένα.

Δίκτυο ανώτερου στρώματος (overlay)

Κάθε κόμβος διατηρεί ένα σύνολο από συνδέσμους (*links*) προς άλλους κόμβους (τους γείτονές του, ή τον πίνακα δρομολόγησης). Όλα αυτά τα *links* αποτελούν το *overlay* δίκτυο. Ένας κόμβος επιλέγει τους γείτονές του με βάση μια συγκεκριμένη δομή, η οποία καλείται τοπολογία του δικτύου.

Όλες οι διαφορετικές τοπολογίες DHT έχουν μια παραλλαγή της πιο σημαντικής ιδιότητας: για κάθε κλειδί *k*, κάθε κόμβος είτε έχει τέτοια ταυτότητα *node ID* ώστε να είναι κάτοχος του *k*, είτε διαθέτει ένα *link* προς έναν κόμβο του οποίου το *ID* είναι πιο κοντά στο *k*, σε όρους απόστασης στο πεδίο κλειδιών, όπως αυτό έχει οριστεί. Διαθέτοντας αυτή την ιδιότητα, είναι εύκολο να γίνει η δρομολόγηση ενός μηνύματος στον κάτοχο οποιουδήποτε *k*, κάνοντας χρήση του ακόλουθου άπληστου αλγορίθμου (ο οποίος δεν είναι κατ' ανάγκη ο βέλτιστος σε κάθε τοπολογία): σε κάθε βήμα, προώθησε το μήνυμα στον γείτονα του οποίου το *ID* είναι πιο κοντά στο *k*. Όταν δεν υπάρχει τέτοιος γείτονας, τότε το μήνυμα έχει φτάσει στον πιο κοντινό κόμβο, ο οποίος είναι ο κάτοχος του *k*. Αυτή η μορφή δρομολόγησης καλείται δρομολόγηση βάσει κλειδιού (key-based routing).

Εφαρμογές DHT

Στις πιο αξιοσημείωτες διαφορές που απαντώνται σε πρακτικές εφαρμογές DHT συμπεριλαμβάνονται οι ακόλουθες:

- Το πεδίο κλειδιών διαφέρει μεταξύ DHTs. Πολλά πραγματικά DHTs κάνουν χρήση 128-bit ή 160-bit πεδίων κλειδιών.
- Ορισμένα DHTs χρησιποιούν διαφορετικές hash συναρτήσεις, αντί της SHA-1.
- Πολλές φορές του κλειδί *k* είναι το hash αποτέλεσμα του περιεχομένου του αρχείου, αντί του ονόματός του. Κατ' αυτόν τον τρόπο τα αρχεία δεικτοδοτούνται βάσει περιεχομένου, μια ιδιότητα που επιτρέπει τη μετονομασία των αρχείων χωρίς αυτό να επηρεάζει τη δυνατότητα για ανάκτησή τους από τους χρήστες.
- Κατά κανόνα εφαρμόζεται η τακτική της διατήρησης αντιγράφων των δεδομένων με στόχο την αξιοπιστία. Τα ζεύγη [κλειδί,τιμή] αποθηκεύονται σε περισσότερους από έναν κόμβο. Συνήθως, οι πραγματικοί αλγόριθμοι DHT επιλέγουν *i* κατάλληλους κόμβους, όπου το *i* αποτελεί παράμετρο που ορίζεται ανάλογα με την εφαρμογή του DHT. Σε ορισμένους DHT σχεδιασμούς, οι κόμβοι αναλαμβάνουν ένα συγκεκριμένο εύρος κλειδιών, το μέγεθος του οποίου μπορεί να επιλέγεται δυναμικά.
- Ορισμένα πιο εξελιγμένα DHTs, όπως το Kademlia [31], εφαρμόζουν αρχικά μέθοδος επαναληπτικής αναζήτησης (iterative lookup) για την επιλογή των κατάλληλων κόμβων και στη συνέχεια στέλνουν το μήνυμα κατευθείαν σε αυτούς, μειώνοντας δραστικά την αποστολή

αχρείαστων μηνυμάτων· την ίδια στιγμή η μέθοδος επαναληπτικής αναζήτησης διατρέχει ένα μικρό σύνολο κόμβων αντί του συνολικού DHT, μειώνοντας κατά πολύ τις προωθήσεις μηνυμάτων. Σε τέτοιας μορφής DHTs, η προώθηση των *put(k, data)* μηνυμάτων γίνεται μόνο ως αποτέλεσμα ενός αυτοθεραπευόμενου (self-healing) αλγορίθμου: στην περίπτωση που ο κόμβος-στόχος λάβει μήνυμα *put(k, data)*, αλλά πιστεύει πως το *k* είναι εκτός του εύρους κλειδιών που του αναλογούν και γνωρίζει κάποιον κόμβο που βρίσκεται πιο κοντά στο *k* (πάντα σε όρους απόστασης στο πεδίο κλειδιών του DHT), το προωθεί σε αυτόν. Διαφορετικά, τα δεδομένα αποθηκεύονται τοπικά. Βέβαια, ένας τέτοιος αλγόριθμος προϋποθέτει οι κόμβοι να δημοσιοποιούν την παρουσία τους στο DHT, ώστε να είναι δυνατή η μέθοδος επαναληπτικής αναζήτησης.

4.3 Chord

Το Chord είναι ένα από τα τέσσερα αρχικά πρωτόκολλα DHT, μαζί με τα CAN [23], Tapestry [32] και Pastry [33]. Παρουσιάστηκε το 2001 από τους Ion Stoica, Robert Morris, David Karger, Frans Kaashoek και Hari Balakrishnan και αναπτύχθηκε στο MIT [24].

Γενικά

Οι κόμβοι και τα κλειδιά λαμβάνουν *m*-bit αναγνωριστικά *IDs* με τη χρήση *consistent hashing* [34], για το οποίο η βασική hash συνάρτηση είναι ο αλγόριθμος SHA-1. Το *consistent hashing* είναι απαραίτητο για την ευρωστία και την υψηλή απόδοση του Chord επειδή τόσο τα κλειδιά όσο και οι κόμβοι κατανέμονται ομοιόμορφα στο ίδιο πεδίο *IDs* με αμελητέα πιθανότητα να συμπέφτουν.

Με βάση το πρωτόκολλο αναζήτησης του Chord, οι κόμβοι και τα κλειδιά διατάσσονται σε έναν κύκλο από αναγνωριστικά ο οποίος περιέχει το 2^m θέσεις, με τιμές από 0 έως 2^m-1 (το *m* θα πρέπει να είναι αρκετά μεγάλο, ώστε να αποφεύγονται οι συγκρούσεις). Κάθε κόμβος έχει έναν διάδοχο (*successor*) κι έναν προκάτοχο (*predecessor*). Ο διάδοχος ενός κόμβου είναι ο αμέσως επόμενός του στον κύκλο αναγνωριστικών με ωρολογιακή φορά. Αντίστοιχα, ο προκάτοχός του είναι ο αμέσως προηγούμενος (με την ίδια φορά). Αν υπάρχει ένας κόβος για κάθε πιθανό ID, τότε διάδοχος του κόμβου 0 είναι ο κόμβος 1 και ο προκάτοχός του ο κόμβος 2^m-1. Βέβαια, κατά κανόνα υπάρχουν “κενά” στις ακολουθίες των κόμβων. Για παράδειγμα, ο διάδοχος του κόμβου 159 μπορεί να είναι ο

κόμβος 200 (δεν υπάρχουν κόμβοι με IDs μεταξύ 159 και 200), κάτι που σημαίνει πως ο προκάτοχος του κόμβου 200 είναι ο κόμβος 159.

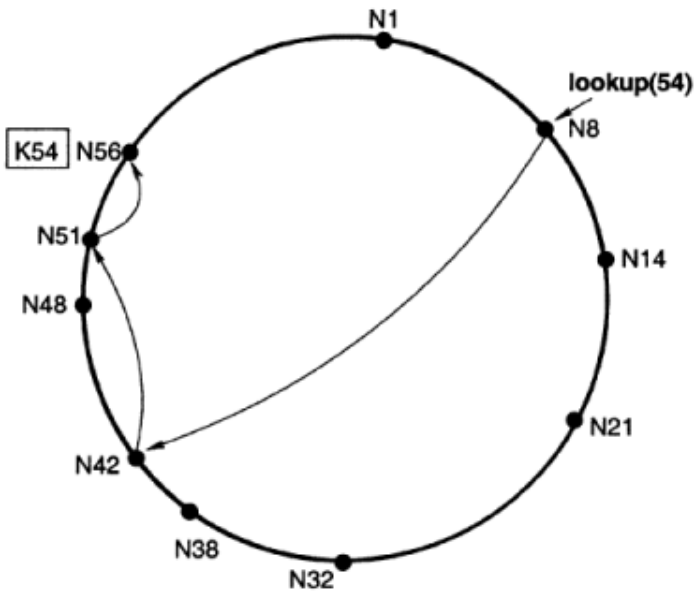
Η ίδια λογική μπορεί να χρησιμοποιηθεί και για τα κλειδιά. Ο διάδοχος κόμβος ενός κλειδιού *k* είναι ο πρώτος κόμβος του οποίου το ID είναι ίσο με *k* ή ακολουθεί το *k* στον κύκλο των αναγνωριστικών, συμβολιζόμενος ως *successor(k)*. Κάθε κλειδί ανατίθεται (αποθηκεύεται) στον διάδοχο κόμβο του, επομένως η αναζήτηση ενός κλειδιού *k* είναι ένα ερώτημα στον *successor(k)*.

Καθώς ο διάδοχος ή ο προκάτοχος ενός κόμβου μπορεί να χαθεί από το δίκτυο (λόγω αποτυχίας ή αναχώρησης), κάθε κόμβος καταγράφει ένα τμήμα του κύκλου αναγνωριστικών εκατέρωθέν του π.χ. τους *r* που προηγούνται αυτού και τους *r* που τον ακολουθούν. Η διατήρηση αυτών των λιστών εξασφαλίζει με μεγάλη πιθανότητα ότι ο κάθε κόμβος είναι σε θέση να γνωρίζει ανά πάσα στιγμή τον προκάτοχο και το διάδοχό του, ακόμη κι αν το δίκτυο βρίσκεται σε συνθήκες υψηλού ρυθμού αποτυχιών ή αναχωρήσεων.

Αναζήτηση

Η κύρια χρήση του πρωτοκόλλου Chord είναι η εφαρμογή ερωτημάτων για κλειδιά από χρήστες/πελάτες (ή ακόμη κι από κόμβους), π.χ. να ευρεθεί ο *successor(k)*. Η βασική προσέγγιση είναι πως σε περίπτωση που ένας κόμβος λάβει το ερώτημα και δε διαθέτει το κλειδί *k* θα προωθήσει το μήνυμα στο διάδοχό του. Αυτό οδηγεί σε χρόνο *O(n)*, όπου *n* το πλήθος των κόμβων στο δακτύλιο του Chord.

Για να αποφευχθεί η γραμμική αναζήτηση, το Chord εφαρμόζει μια ταχύτερη μέθοδο αναζήτησης η οποία απαιτεί από κάθε κόμβο να διατηρεί ένα *finger table*. Το *finger table* περιέχει *m* εγγραφές, όπου *m* το πλήθος των bits του hash key. Η *i*-οστή εγγραφή του κόμβου *n* θα περιέχει τον *successor*$((n + 2^{i-1}) \bmod 2^m)$. Η πρώτη εγγραφή του *finger table* είναι ο διάδοχος του κόμβου. Κάθε φορά που ένας κόμβος επιθυμεί να αναζητήσει ένα κλειδί *k*, προωθεί το ερώτημα στον κόμβο του *finger table* του που είναι κοντινότερος στο *k*. Κάνοντας χρήση ενός τέτοιου *finger table*, το πλήθος των κόμβων με τους οποίους πρέπει κανείς να έρθει σε επαφή για την εύρεση του κατόχου ενός κλειδιού σε δίκτυο *n* κόμβων είναι *O(log n)*.



Σχήμα 8: *Η αναζήτηση με finger table σε Chord DHT.*

Είσοδος κόμβου

Όταν ένας νέος κόμβος εισέρχεται, τρεις ιδιότητες θα πρέπει να διατηρηθούν:

- Ο διάδοχος κάθε κόμβου θα πρέπει να δείχνει σωστά στον αμέσως επόμενό του.
- Κάθε κλειδί *k* θα πρέπει να είναι αποθηκευμένο από τον *successor(k).*
- Το *finger table* κάθε κόμβου θα πρέπει να είναι σωστό.

Για να ικανοποιούνται αυτές οι ιδιότητες, κάθε κόμβος διατηρεί ένα πεδίο *predecessor.* Καθώς ο *successor* είναι η πρώτη εγγραφή στο *finger table*, δε χρειάζεται διατήρηση ενός ξεχωριστού πεδίου. Σε περίπτωση εισόδου ενός νέου κόμβου *n* θα πρέπει να γίνουν οι ακόλουθες ενέργειες:

- Γίνεται αρχικοποίηση του *n* (του *predecessor* και του *finger table*).
- Ειδοποιούνται οι υπόλοιποι κόμβοι, ώστε να ενημερώσουν τους *predecessors* και τα *finger tables* τους.
- Ο νέος κόμβος αναλαμβάνει τα *keys* που του αναλογούν από τον *successor* του.

Ο *predecessor* του *n* μπορεί εύκολα να αποκτηθεί μέσω του *predecessor* του *successor* (σύμφωνα με τα δεδομένα πριν την είσοδο του *n*). Αναφορικά με το *finger table*, υπάρχουν διάφορες μέθοδοι αρχικοποίησης [24].

4.4 Ασφάλεια σε DHT

4.4.1 Sybil επίθεση

Η Sybil επίθεση μελετήθηκε πρώτη φορά από τον Douceur το 2002 [35]. Αυτός ο τύπος επίθεσης εκμεταλλεύεται το γεγονός ότι σε ένα κατανεμημένο σύστημα οι απομακρυσμένες οντότητες αντιμετωπίζονται ως αφηρημένες πληροφοριακές οντότητες γνωστές ως ταυτότητες. Όταν το σύστημα αποτυγχάνει να εγγυηθεί ότι η κάθε λογική οντότητα αναφέρεται σε διαφορετική φυσική οντότητα, ένας επιτιθέμενος μπορεί να δημιουργήσει ένα μεγάλο αριθμό από ταυτότητες και να κυριαρχήσει στο δίκτυο ανώτερου στρώματος κοροϊδεύοντας τα πρωτόκολλα και να υποβιβάζει μηχανισμούς βασιζόμενος στον πλεονασμό του. Η Sybil επίθεση δε βλάπτει το DHT αυτό καθ' αυτό, αλλά μπορεί να χρησιμοποιηθεί για την τεχνητή δημιουργία μιας πλειοψηφίας κακόβουλων συνωμοτούντων κόμβων σε επίπεδο overlay. Έχουν σχεδιαστεί διάφοροι τύποι άμυνας για DHTs, υπό την υπόθεση ότι οι κακόβουλοι κόμβοι αποτελούν ένα μικρό ποσοστό *f* του συνόλου. Μια Sybil επίθεση, όμως, σπάει αυτές τις άμυνες αυξάνοντας το *f*. Αν, για παράδειγμα, υπάρχουν πολλές κακόβουλες ταυτότητες στο σύστημα, γίνεται ευκολότερη η καταχώρηση ψευδών στοιχείων στους πίνακες δρομολόγησης των έντιμων κόμβων και ο έλεγχος της πλειοψηφίας των αντιγράφων ενός δεδομένου κλειδιού. Το σημαντικότερο συμπέρασμα της μελέτης του Douceur είναι ότι, σε ένα peer-to-peer σύστημα, ο μόνος τρόπος για να υπάρχει εγγύηση της ένα προς ένα αντιστοίχησης ταυτοτήτων σε φυσικές οντότητες που λειτουργούν τους συμμετέχοντες κόμβους είναι η χρήση μιας κεντρικής, έμπιστης αρχής για την έκδοση ταυτοτήτων.

4.4.2 Eclipse επίθεση

Οι κόμβοι σε ένα overlay δίκτυο διατηρούν συνδέσεις με ορισμένους άλλους peers, οι οποίοι αναφέρονται ως γείτονες. Αν ένας επιτιθέμενος ελέγχει ένα επαρκώς μεγάλο μέρος των γειτόνων έντιμων κόμβων, τότε οι κόμβοι αυτοί μπορεί να "επισκιαστούν" (*eclipse*) από τους κακόβουλους. Αυτό το είδος επίθεσης είναι επίσης γνωστό ως δηλητηριασμός του πίνακα δρομολόγησης (*routing table poisoning*). Η Eclipse επίθεση μπορεί να χρησιμοποιηθεί για να προωθήσει άλλων ειδών επιθέσεις, κυρίως επιθέσεις δρομολόγησης και αποθήκευσης. Οι Sit και Morris (2002) ήταν οι πρώτοι που μελέτησαν αυτήν την επίθεση στα πλαίσια των DHTs. Ισχυρίστηκαν ότι τα συστήματα στα οποία οι γείτονες δε διαθέτουν ειδικές απαιτήσεις επιβεβαίωσης ταυτότητας είναι τα πιο ευάλωτα σε αυτού

του τύπου την επίθεση. Ο ευκολότερος τρόπος εκμετάλλευσης αυτής της αδυναμίας είναι μέσω εσφαλμένων ενημερώσεων δρομολόγησης. Για παράδειγμα, τα ανώτερα στρώματα του πίνακα δρομολόγησης του Pastry απαιτούν ένα κοινό πρόθεμα μόλις μερικών ψηφίων. Αυτό αυξάνει τον αριθμό των έγκυρων αναγνωριστικών που μπορεί να διαθέσει ένας επιτιθέμενος κατά τη διάρκεια της ενημέρωσης πινάκων δρομολόγησης σε σύγκριση με συστήματα που επιβάλλουν ισχυρούς περιορισμούς, όπως το Chord [24]. Αυτή η συγκεκριμένη επίθεση μπορεί να κάνει το ποσοστό των κακόβουλων εγγραφών στον πίνακα δρομολόγησης των έντιμων κόμβων να τείνει στο 100%, καθώς το πλήθος των κακόβουλων εγγραφών μπορεί να αυξηθεί με κάθε νέα ενημέρωση. Ένα άλλο πιθανό σενάριο επίθεσης είναι η υπονόμευση του μηχανισμού μέτρησης της εγγύτητας στο δίκτυο. Για παράδειγμα, οι Hildrum και Kubiatowicz (2003) έδειξαν ότι ένας επιτιθέμενος μπορεί να μειώσει τη φαινόμενη απόστασή του χρησιμοποιώντας ένα συνωμότη που βρίσκεται σε μια συντομότερη οδό, ώστε να προωθεί παραπλανητικές απαντήσεις σε ένα μήνυμα παλμού (heartbeat). Οι Castro et al. διατύπωσαν ότι οι μετρήσεις μπορούν επίσης να υπονομευτούν με μηχανισμούς εναλλακτικών οδών, όπως το IPv6 κινητής, ή αν ο επιτιθέμενος ελέγχει μια μεγάλη υποδομή, όπως ένα ISP η μια μεγάλη εταιρία. Θα πρέπει επίσης να σημειωθεί ότι αν υποτεθεί ότι η υπονόμευση των μετρήσεων εγγύτητας δικτύου δεν είναι εφικτή σε μεγάλη κλίμακα, τότε η μετρική της εγγύτητας δικτύου μπορεί να χρησιμοποιηθεί για να βοηθήσει στην πρόληψη της επίθεσης Eclipse [Hildrum and Kubiatowicz 2003]. Ένα άλλο προφανές σενάριο επίθεσης σε DHTs βασιζόμενα στην εγγύτητα στο δίκτυο είναι η τοποθέτηση πολλών κακόβουλων κόμβων στις κοντινές περιοχές δύο κόμβων. Στο εξής, οι κακόβουλοι κόμβοι μπορούν εύκολα να συνωμοτήσουν και να επιτεθούν και σε άλλους κοντινούς κόμβους. Μία άμυνα κατά της επίθεσης Eclipse μπορεί να θεωρείται επιτυχής αν το ποσοστό των κακών εγγραφών στους πίνακες δρομολόγησης των έντιμων κόμβων δε διαφέρει πολύ από το ποσοστό f των κακόβουλων κόμβων στο σύστημα, καθώς αυτό είναι το αναμενόμενο ποσοστό των κακών εγγραφών σε ένα τυχαίο δείγμα κόμβων, δεδομένου ότι τα αναγνωριστικά γεννιούνται με τυχαίο τρόπο. Ωστόσο, η δρομοολόγηση μέσω ενός μονοπατιού μπορεί εύκολα να αποτυγχάνει με μεγάλη πιθανότητα. Για παράδειγμα, αν το ποσοστό f είναι 25% και το μονοπάτι είναι μήκου 5, η πιθανότητα επιτυχούς δρομολόγησης είναι $(1 – 0.25)^5 \approx 0.24$, που θα ήταν απαράδεκτη για τις περισσότερες εφαρμογές. Για το λόγο αυτό, τα πρωτόκολλα ενημέρωσης των πινάκων δρομολόγησης είναι πάντα ενισχυμένα με κάποιου είδους πλεονάζουσας δρομολόγησης, που είναι η βάση της άμυνας εναντίον των επιθέσεων δρομολόγησης και αποθήκευσης. Το πιο κοινό μοντέλο επίθεσης, στο οποίο βασίζεται και η λύση της πλεονάζουσας δρομολόγησης, είναι αυτό κατά το οποίο οι κακόβουλοι κόμβου προσπαθούν να

μεγιστοποιήσουν τις κακές εγγραφές στους πίνακες δρομολόγησης όλων των έντιμων κόμβων προσφέροντας λανθασμένες αναφορές κατά την εφαρμογή των πρωτοκόλλων ενημέρωσης. Βέβαια, αυτό δεν είναι απαραίτητα και το μοναδικό πιθανό σενάριο. Επί παραδείγματι, ο επιτιθέμενος μπορεί να επιχειρήσει την επίθεση σε ένα μόνο μικρό υποσύνολο των κόμβων, σε ένα συγκεκριμένο κλειδί ή σε μια συγκεκριμένη γραμμή των πινάκων δρομολόγησης. Θα μπορούσε επίσης να διαδίδει λανθασμένες πληροφορίες με αργό τρόπο, κάνοντας επίθεση σε διαφορετικούς κόμβους σειριακά και συμπεριφερόμενος σωστά τις περισσότερες φορές. Μεταξύ των λύσεων που έχουν προταθεί, καμία δεν είναι αποτελεσματική εναντίον τέτοιων πιο περίτεχνων επιθέσεων. Οι Singh et al. [36] αναφέρθηκαν σε επιθέσεις τοπικού χαρακτήρα, κατά τις οποίες ένας έντιμος κόμβος περιβάλλεται – με όρους τοπολογίας δικτύου – από κακόβουλους κόμβους. Το συμπέρασμά τους ήταν ότι η άμυνα εναντίον τέτοιου είδους επιθέσεων παραμένει ανοιχτό πρόβλημα.

4.4.3 Επιθέσεις δρομολόγησης και αποθήκευσης

Οι Sybil και Eclipse επιθέσεις δεν επηρεάζουν άμεσα το DHT, αλλά μπορούν να χρησιμοποιηθούν για να υποβοηθήσουν ή να επισχύσουν άλλες, μελλοντικές επιθέσεις. Τέτοιες επιθέσεις μπορεί να επιχειρήσουν την αποτυχία ενός αιτήματος αναζήτησης. Για παράδειγμα, μπορεί ένας επιτιθέμενος να αρνηθεί την προώθηση ενός τέτοιου αιτήματος. Θα μπορούσε επίσης να το προωθήσει σε λάθος, σε ανύπαρκτο ή σε κακόβουλο κόμβο. Ακόμη, θα μπορούσε να προσποιηθεί πως είναι ο υπεύθυνος για το κλειδί που αναζητάται ή να δρομολογεί σωστά τα αιτήματα αλλά να αρνείται την ύπαρξη ενός έγκυρου κλειδιού ή να απαντά προσφέροντας λανθασμένα δεδομένα. Τέτοιες επιθέσεις κατατάσσονται στις επιθέσεις δρομολόγησης, οι οποίες στοχεύουν στη διατάραξη της δρομολόγησης, και στις επιθέσεις αποθήκευσης, που επιχειρούν την αποστολή ψευδών απαντήσεων σε ερωτήματα. Έχουν γίνει πολλές προτάσεις για την αντιμετώπιση τέτοιων επιθέσεων. Ορισμένες από τις πιο ενδεικτικές είναι:

- η χρήση επαναληπτικής αναζήτησης, ώστε ο αιτών να μπορεί να παρακολουθεί την εξέλιξη και να εντοπίζει ανωμαλίες κατά τη δρομολόγηση του αιτήματός του
- η ανάθεση κλειδιών με τρόπο ώστε να μπορεί να γίνεται επαλήθευση και να είναι δύσκολο για έναν κόμβο να ισχυρίζεται την κυριότητα ενός συγκεκριμένου κλειδιού
- η χρήση αναγνωριστικών βασιζόμενων σε δημόσκα κλειδιά, προκειμένου οι παραλήπτες απαντήσεων να μπορούν αν ελέγξουν την εγκυρότητα των περιεχομένων

- η αντιστοίχιση ενός κλειδιού σε πολλαπλούς κόμβους με τη χρήση μιας συνάρτησης κατακερματισμού.

4.4.4 Συμπεράσματα για την ασφάλεια

Έγινε αναφορά στις πιο γνωστές απειλές που αντιμετωπίζουν τα DHTs και σε ορισμένες τεχνικές που έχουν προταθεί για την αντιμετώπιση ή το μετριασμό τους. Η ποικιλία των προτεινόμενων λύσεων και τα αντίτιμα που επιφέρουν είναι ενδεικτικά του πόσο δύσκολη είναι η ασφάλιση ενός συστήματος DHT σε ένα εχθρικό περιβάλλον. Είναι εύλογο το συμπέρασμα ότι η ασφάλιση ενός DHT απαιτεί ασφαλή τρόπο ανάθεσης αναγνωριστικών στους κόμβους, χαμηλό ποσοστό κακόβουλων κόμβων, διασπορά των κακόβουλων κόμβων στο πεδίο των αναγνωριστικών, αντιγραφή δεδομένων και έναν μηχανισμό δρομολόγησης ο οποίος προσφέρει μια υψηλή πιθανότητα ένα αίτημα να φτάσει με επιτυχία σε έναν κατάλληλο κόμβο (κάτοχο αντιγράφου των ζητούμενων δεδομένων).

Οι σημερινές εφαρμογές DHT δεν είναι σχεδιασμένες κατάλληλα, ώστε να έχουν ανέχονται την παρουσία κακόβουλων κόμβων. Ωστόσο, οι περισσότερες βασίζονται στο Kademlia, το οποίο προσφέρει μια σχετική ασφάλεια μέσω της αντιγραφής των δεδομένων και της χρήσης ενός πλεονάζοντα μηχανισμού δρομολόγησης. Παρ’ όλ’ αυτά, παραμένει ευάλωτο σε Sybil επιθέσεις, καθώς οι κόμβοι γεννούν από μόνοι το αναγνωριστικό τους. Η μεγαλύτερη πρόκληση για την επίτευξη ασφαλών DHTs και εν γένει αποκεντρωμένων συστημάτων είναι η εύρωστη και ασφαλής ανάθεση αναγνωριστικών των κόμβων. Το ζήτημα αυτό είναι κρίσιμο για να εξασφαλιστεί ότι οι κακόβουλοι κόμβοι αποτελούν ένα μικρό ποσοστό του δικτύου και δεν μπορούν να επιλέξουν από μόνοι τους την τοποθεσία τους στο overlay, προλαμβάνοντας έτσι τις Sybil και Eclipse επιθέσεις. Αυτό το συμπέρασμα σκιαγραφείται σε μελέτες όπως η [37].

Σε κάθε περίπτωση, παρά τη δυνατότητα επίτευξης ενός πρακτικά αποδεκτού επιπέδου ασφαλείας σε DHT εφαρμογές, είναι προφανές ότι απαιτείται ακόμη πολλή δουλειά στο κομμάτι αυτό αν οι απαιτήσεις είναι υψηλές.

5 Το Bitcoin blockchain σε Chord DHT

Με αφορμή τα όσα αναφέρθηκαν περί αποκέντρωσης του Bitcoin, θα μελετηθεί η δυνατότητα αποθήκευσης του Bitcoin blockchain σε ενα DHT. Μια τέτοια επιλογή έχει ως στόχο να δοθεί η δυνατότητα σε χρήστες με μηχανήματα χαμηλότερων δυνατοτήτων να συμμετέχουν στο δίκτυο του Bitcoin επιβεβαιώνοντας οι ίδιοι τις συναλλαγές τους και την ορθότητα του Bitcoin blockchain, χωρίς να διαθέτουν μεγάλο αποθηκευτικό χώρο στο δίσκο. Αυτό θα επιτυγχάνεται καθώς ο κάθε συμμετέχων κόμβος του DHT θα αποθηκεύει τοπικά στο δίσκο του μόνο ένα μέρος του συνολικού όγκου των δεδομένων του blockchain. Ένα δεύτερο και ακόμη πιο σημαντικό πλεονέκτημα της ύπαρξης ενός blockchain κατανεμημένου σε DHT είναι η συνεισφορά του σε ένα πιο αποκεντρωμένο δίκτυο Bitcoin.

Όπως έχει ήδη αναλυθεί στην Ενότητα 4.4 περί ασφάλειας DHT, ένα DHT δεν μπορεί να εξασφαλίσει ότι δε θα υπάρξουν απώλειες δεδομένων. Ως εκ τούτου, η υλοποίηση ενός DHT για την αποθήκευση του blockchain δεν αποσκοπεί ούτε μπορεί να καταφέρει την αντικατάσταση των full nodes. Όσο υπάρχει το Bitcoin και άνθρωποι συναλλάσσονται μέσω αυτού θα υπάρχει και το κίνητρο για τη διατήρηση ενός full node. Η πρόταση της εργασίας προβλέπει τη δημιουργία DHTs όπου θα συμμετέχει ένα μέρος των σημερινών Bitcoin nodes αλλά και νέοι κόμβοι, οι οποίοι θα διαθέτουν το συμβατικό τους μηχάνημα συνεισφέροντας σε ένα δίκτυο (αυτό του DHT overlay) κατά βάσην απλών χρηστών και σε μια προσπάθεια διατήρησης της αποκέντρωσης του Bitcoin.

Ο τρόπος διατήρησης της αποκέντρωσης του Bitcoin θα βασίζεται στην ιδιότητα της κλιμάκωσης του DHT. Δεδομένης της διαρκούς και σταθερής αύξησης του όγκου δεδομένων του blockchain, καθίσταται ολοένα και πιο κοστοβόρα η αποστολή δεδομένων (chaindata) προς έναν νεοεισερχόμενο κόμβο στο δίκτυο (bootstrapper). Συν αυτού, ένας full node δεν έχει άμεσα ωφέλη ούτε κάποιο κίνητρο για την εξυπηρέτηση ενός bootstrapper. Αυτά τα ζητήματα επιλύει ένα DHT καθώς η κλιμάκωσή του αποτελεί αντισταθμιστικό παράγοντα της αύξησης του όγκου δεδομένων ενώ εκ κατασκευής ωφελείται και από την εξυπηρέτηση bootstrapping κόμβων.

Οι συμμετέχοντες κόμβοι του DHT πρώτ’ απ’ όλα θα είναι μέλη του δικτύου του Bitcoin, με ό,τι αυτό συνεπάγεται. Πιο συγκεκριμένα, βάσει και των όσων έχουν αναφερθεί στην Ενότητα 2.7 σχετικά με τους full nodes του Bitcoin, οι κόμβοι του DHT θα διατηρούν συνδέσεις με άλλους κόμβους του δικτύου για τη λήψη και τη μετάδοση νέων transactions και blocks. Παράλληλα, όμως, θα είναι υποχρεωτική και η τήρηση του πρωτοκόλλου του DHT, π.χ. η επικοινωνία με τους γείτονες κόμβους και η εξυπηρέτηση ερωτημάτων, λειτουργίες που έχουν πρόσθετες απαιτήσεις πόρων. Είναι

σημαντικό επίσης να οριστεί το βάθος στο blockchain που θα πρέπει να έχει ένα block, ώστε να θεωρείται επιβεβαιωμένο και να εκχωρείται στο DHT. Επομένως, το δίκτυο του DHT θα αποτελεί ουσιαστικά ένα στρώμα δικτύου πάνω στο δίκτυο του Bitcoin.

Το σύστημα ενός DHT έχει ορισμένες σημαντικές παραμέτρους λειτουργίας και συνέπειες στη χρησιμοποίηση των πόρων των κόμβων του. Έτσι, θα πραγματοποιηθούν προσομοιώσεις και θα αξιολογηθεί το κατά πόσον μια τέτοια εφαρμογή είναι πραγματοποιήσιμη, δεδομένων των απαιτήσεων του πρωτοκόλλου του Bitcoin.

5.1 Μέσο και παράμετροι προσομοίωσης

Έχοντας αναφέρει πιθανούς κινδύνους ασφαλείας ενός DHT, θα πρέπει να γίνει αξιολόγηση και κατάλληλη επιλογή παραμέτρων, ώστε να διασφαλίζεται με μεγάλη βεβαιότητα η απρόσκοπτη λειτουργία του συστήματος που θα μελετηθεί. Συν αυτού, η συμμετοχή ενός μηχανήματος σε DHT συνεπάγεται πρόσθετες λειτουργίες και δεσμεύσεις πόρων π.χ. εύρους ζώνης.

Η μελέτη θα γίνει με τη χρήση ενός προσομοιωτή DHT Chord αναπτυγμένου σε περιβάλλον Java. Επίσης, θα γίνουν οι εξής θεωρήσεις για το σημερινό δίκτυο Bitcoin nodes, βάσει στατιστικών και πραγματικών μετρήσεων ενός full node [10]:

- ➔ Καθυστέρηση δικτύου (network latency) με μέση τιμή ***100ms***, μέγιστη ***550ms*** και ελάχιστη ***5ms***.
- ➔ Καθυστέρηση μέχρι να επιβεβαιωθεί μια απροειδοποίητη αναχώρηση: ***10s*** (στις προσομοιώσεις όλες οι αναχωρήσεις θα θεωρούνται απροειδοποίητες).
- ➔ Λαμβάνοντας υπόψιν την κατανομή του 70% των διαθέσιμων full nodes στον παγκόσμιο χάρτη [9] και τις μέσες ταχύτητες internet ανά χώρα κατά το Q1 2016 [36]:
  - ΗΠΑ: 29 % των full nodes με μέση ταχύτητα 15.3Mbps
  - Γερμανία: 18 % των full nodes με μέση ταχύτητα 14Mbps
  - Γαλλία: 7 % των full nodes με μέση ταχύτητα 10Mbps
  - Ολλανδία: 6 % των full nodes με μέση ταχύτητα 18Mbps
  - Καναδάς: 4 % των full nodes με μέση ταχύτητα 14.3Mbps
  - Ην. Βασίλειο: 4 % των full nodes με μέση ταχύτητα 15Mbps
  - Ρωσία: 3 % των full nodes με μέση ταχύτητα 12.2Mbps

Ως μέση ταχύτητα internet των Bitcoin nodes λαμβάνεται αυτή των ***14.5Mbps***.

- ➔ Ρυθμός downloading δεδομένων σχετικών με το δίκτυο του Bitcoin: Max 400Kbps, Avg ***80Kbps***.
- ➔ Ρυθμός uploading δεδομένων σχετικών με το δίκτυο του Bitcoin: Max 24Mbps, Avg **7.2*Mbps***.
- ➔ Μέσος χρόνος επιβεβαίωσης της εγκυρότητας και αποδοχής ενός block: CheckBlock() + AcceptBlock() = 27ms + 24ms ≈ ***50ms***.

Θα θεωρηθεί ως δεδομένο ότι ισχύει ο υπολογισμός που έχει γίνει σχετικά με το πλήθος των κόμβων του δικτύου του Bitcoin, σύμφωνα με τον οποίο υπάρχουν 86,000 Bitcoin nodes, εκ των οποίων οι 7,500 είναι διαθέσιμοι full nodes. Οι 78,500 απρόσιτοι κόμβοι μπορεί να είναι είτε full nodes είτε fast nodes. Δεδομένου, όμως, του κόστους για τη διατήρηση αντιγράφου του Bitcoin blockchain εν αντιθέσει των περιορισμένων απαιτήσεων ενός fast node, είναι λογικό πως το μεγαλύτερο μέρος αυτών θα είναι fast nodes.

Οι fast nodes είναι αυτοί οι οποίοι θα έχουν μεγαλύτερο κίνητρο να συμμετάσχουν στο DHT, καθώς στην πλειοψηφία τους θα ταιριάζουν στο προφίλ που έχει περιγραφεί σχετικά με τους συμμετέχοντες του DHT: χρήστες με μηχανήματα χαμηλών δυνατοτήτων που επιθυμούν τη διατήρηση της αποκέντρωσης του Bitcoin. Για τις προσομοιώσεις του DHT συστήματος που θα γίνουν θα θεωρηθεί πως οι κόμβοι του DHT θα είναι το σύνολο των fast nodes.

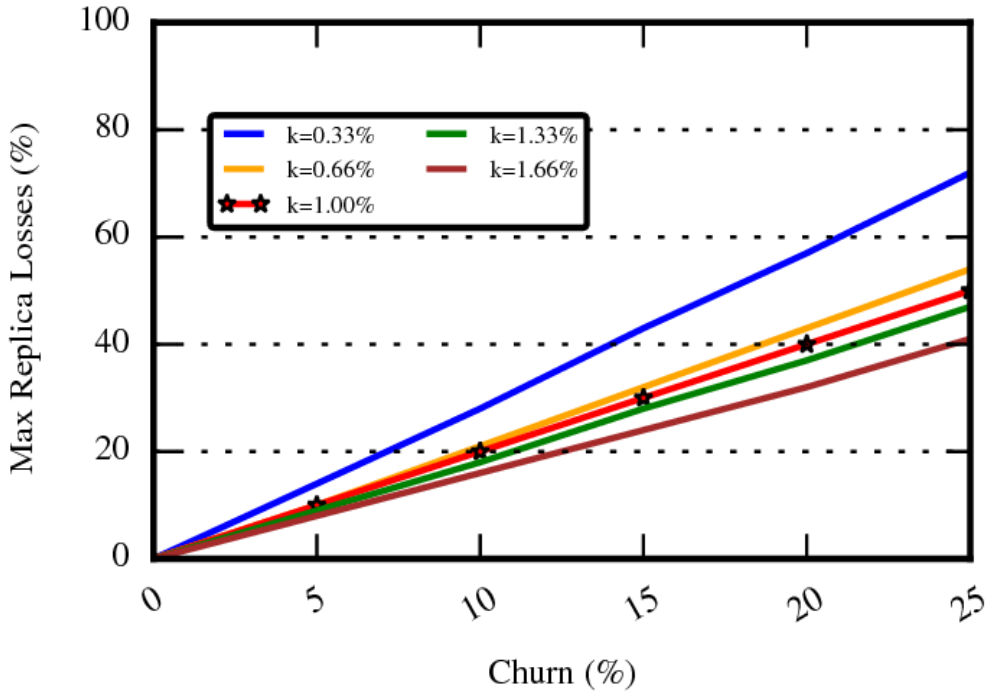
Η χρησιμοποίηση εύρους ζώνης για uploading πρωτοκόλλου Bitcoin προκύπτει από αποστολή δεδομένων σε συγχρονισμένους κόμβους του δικτύου, σε bootstrapping κόμβους και σε lightweight clients και προς το παρόν εξυπηρετείται από τους διαθέσιμους full nodes. Καθώς αναπόσταστο μέρος της λειτουργίας ενός DHT είναι η απάντηση σε ερωτήματα σχετικά με τα δεδομένα που διαθέτει, θα πρέπει οι fast nodes-συμμετέχοντες του DHT να αναλάβουν και μέρος της εξυπηρέτησης uploading. Στις προσομοιώσεις το DHT θα αναλάβει το σύνολο του uploading που καλείται να εξυπηρετεί το δίκτυο του Bitcoin, ενώ θα γίνει η θεώρηση ότι κάθε ερώτημα για uploading αντιστοιχεί στην αποστολή ενός block, δηλαδή 1 MB.

Στη χρησιμοποίηση εύρους ζώνης θα προστεθεί και uploading/downloading λόγω πρωτοκόλλου DHT, που κατά κύριο λόγο πρόκειται για μεταφορά δεδομένων αντιγράφων, ως συνέπεια αναχώρησης κόμβων. Για τον ορισμό της δυναμικότητας του πληθυσμού των κόμβων θα αξιολόγηση των

δεδομένων [39] που αναφέρονται στους full nodes, καθώς είναι τα μόνα διαθέσιμα. Ο μέσος ρυθμός αφίξεων ή αναχωρήσεων θα οριστεί στο 16% του πληθυσμού ανά ημέρα. Κάθε κόμβος κάνει downloading πληροφορίας chaindata/N όταν γίνεται αναχώρηση ενός εκ των k προκατόχων του και αντίστοιχα uploading της ίδιας πληροφορίας όταν αναχωρεί ένας εκ των k διαδόχων του, όπου chaindata το μέγεθος του blockchain, N το πλήθος των κόμβων και k ο συντελεστής αντιγραφής. Έχοντας N*16% αφίξεις ή αναχωρήσεις ανά ημέρα, στατιστικά ο κάθε κόμβος θα παρατηρεί k/N*N*16% αφίξεις ή αναχωρήσεις ανά ημέρα, που αντιστοιχεί σε χρησιμοποίηση εύρους ζώνης k/N*N*16%/2 MB ανά ημέρα για uploading και ίδιο εύρος για downloading.

Ένας παράγοντας που πρέπει να συνυπολογιστεί είναι η περίπτωση των hot data, δηλαδή δεδομένων τα οποία έχουν ζήτηση πολύ μεγαλύτερη του μέσου όρου. Στην περίπτωση του blockchain γνωρίζουμε ήδη πως τέτοια δεδομένα υπάρχουν και είναι τα πιο πρόσφατα. Είναι κοινή πρακτική όταν γίνεται μια συναλλαγή τόσο ο αποστολέας όσο και ο παραλήπτης να κάνουν έλεγχο για την επιβεβαίωσή της. Ο έλεγχος αυτός για έναν lightweight client είναι ερώτημα προς έναν ή περισσότερους full nodes και αφορά στα πιο πρόσφατα blocks του blockchain. Για να αποφευχθεί το φαινόμενο της συμφόρησης (congestion) σε συγκεκριμένα σημεία του DHT, κάθε κόμβος θα διατηρεί στο δίσκο του τα blocks που προστέθηκαν στο blockchain τις τελευταίες 24 ώρες. Κατ’ αυτόν τον τρόπο, η πλειοψηφία των ερωτημάτων θα μπορεί να απαντηθεί από τον παραλήπτη του ερωτήματος, χωρίς την ανάγκη προώθησής του εντός του DHT και την απαίτηση απάντησής τους από τους σχετικά ολιγάριθμους κατόχους βάσει κατανομής κλειδιών. Στο Bitcoin δημιουργούνται κατά μέσο όρο 144 blocks ανά 24 ώρες, επομένως κάθε κόμβος θα διατηρεί περίπου 144MB επιπλέον. Για τις προσομοιώσεις θα γίνει η θεώρηση πως το 50% των συνολικών ερωτημάτων αναφέρονται σε blocks που δημιουργήθηκαν τις τελευταίες 24 ώρες και γίνονται lightweight clients.

Σχετικά με την ανταλλαγή δεδομένων λόγω πρωτοκόλλου DHT, θα γίνει η θεώρηση ότι η λήψη των δεδομένων ενός κόμβου που αναχώρησε (για τη διατήρηση σταθερού αριθμού αντιγράφων) γίνεται όχι μόνο από το νέο υπεύθυνο κόμβο των δεδομένων, αλλά από όλους τους κόμβους που διατηρούσαν αντίγραφό τους. Κατ’ αυτόν τον τρόπο η χρησιμοποίηση εύρους ζώνης για uploading θα μοιράζεται στους κατόχους αντιγράφων.



Σχήμα 9: *Ποσοστό μέγιστων απωλειών αντιγράφων δεδομένων σε περιπτώσεις συντονισμένων αναχωρήσεων.*

Θα γίνει κατάλληλη επιλογή του συντελεστή αντιγράφων k, ώστε οι μέγιστες απώλειες αντιγράφων να μην ξεπερνούν -στατιστικά- το 50%, για συνθήκες συντονισμένης αναχώρησης κόμβων που φτάνουν το 25% του συνόλου των κόμβων. Όπως φαίνεται στο *Σχήμα 9*, για την ικανοποίηση αυτής της απαίτησης ο συντελεστής k αρκεί να είναι τουλάχιστον το 1% του πλήθους των κόμβων.

Καθώς δεν μπορεί να γίνει πρόβλεψη του πλήθους των κόμβων ενός τέτοιου συστήματος, οι προσομοιώσεις θα γίνουν για πέντε διαφορετικά μεγέθη, 3,750, 7,500, 41,250, 75,000 και 150,000 κόμβων, ούτως ώστε να έχουμε εικόνα τόσο των μεγεθών όπως το εύρος ζώνης ή οι απώλειες αντιγράφων, για μικρά και μεγάλα δίκτυα όσο και του επιπέδου κλιμάκωσης του συστήματος.

- πλήθος κόμβων: 3,750 7,500 41,250 75,000 150,000
- μέγεθος blockchain: 130GB
- συντελεστής αντιγραφής: k = 1% επί του πλήθους των κόμβων
- ρυθμός ερωτημάτων (1MB / ερώτημα): μέχρι 120,000 qps (μέσος όρος Bitcoin: 7.2Mbps * 7,500 διαθέσιμοι κόμβοι = 54,000Mbps ⇒ 6.750 qps)

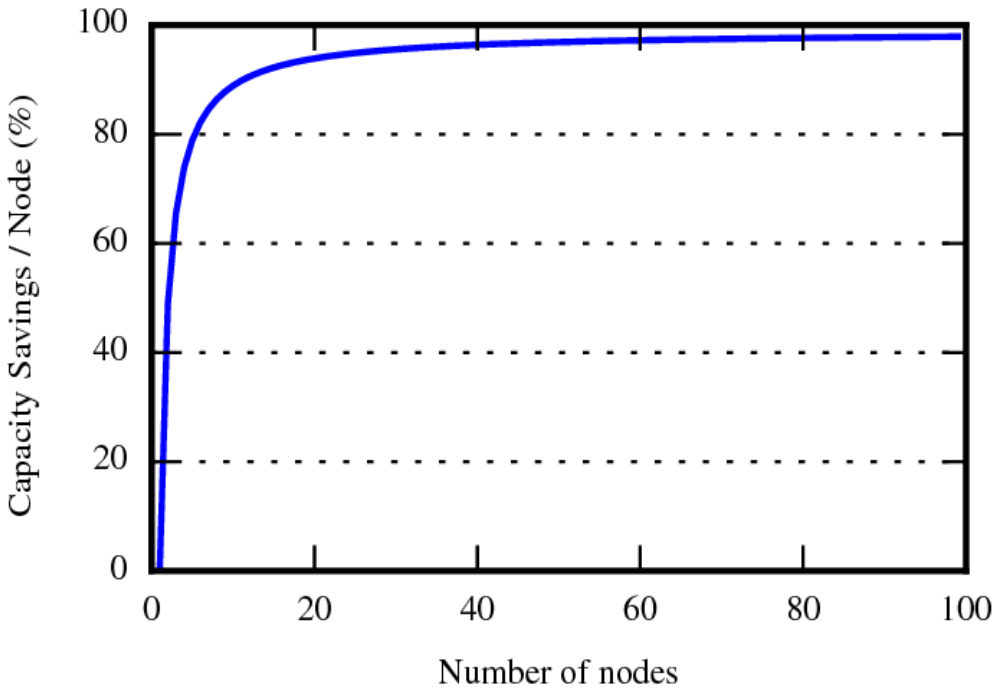
- ρυθμός αφίξεων – αναχωρήσεων εκπεφρασμένος ως ποσοστό επί του πλήθους των κόμβων: μέχρι 48% / ώρα
- μέση ταχύτητα internet: 14.5Mbps
- μέσος χρόνος επιβεβαίωσης και αποδοχής ενός block: 50ms

5.2 Προσομοιώσεις

Έχει αξία να μελετήσουμε τη λειτουργία του DHT σε επίπεδα κινητικότητας και εξυπηρέτησης ερωτημάτων αρκετά υψηλότερα των μέσων ρυθμών, καθώς η συμπεριφορά τόσο των κόμβων ενός peer-to-peer δικτύου όσο και των χρηστών που υποβάλλουν ερωτήματα είναι απρόβλεπτη και μπορεί να παρουσιάζει σημαντικές διακυμάνσεις. Σκοπός αυτών των προσομοιώσεων είναι να παρατηρηθούν και να αξιολογηθούν μετρικές όπως οι απώλειες αντιγράφων δεδομένων, η χρησιμοποίηση εύρους ζώνης των κόμβων και τα επίπεδα συμφόρησης στο σύστημα.

- ***Capacity***

Ακολουθεί διάγραμμα που απεικονίζει τα κέρδη σε capacity που έχει ένας κόμβος του DHT, ως ποσοστό επί του όγκου δεδομένων που αποθηκεύει ένας full node.



Σχήμα 10: *Ποσοστά εξοικονόμησης capacity.*

Η γραφική παράσταση δείχνει απότομη κλιμάκωση του ποσοστού εξοικονόμησης capacity (capacity savings). Έτσι, η αύξηση του πλήθους των κόμβων δεν έχει ως αποτέλεσμα περαιτέρω κλιμάκωση όταν οι κόμβοι είναι της τάξης των 100. Το ποσοστό των capacity savings τείνει σε μια τιμή κοντά στο 99%. Η συμπεριφορά της καμπύλης εξηγείται λαμβάνοντας υπόψιν ότι ο όγκος δεδομένων ενός DHT distributed blockchain κόμβου προκύπτει ως το άθροισμα:

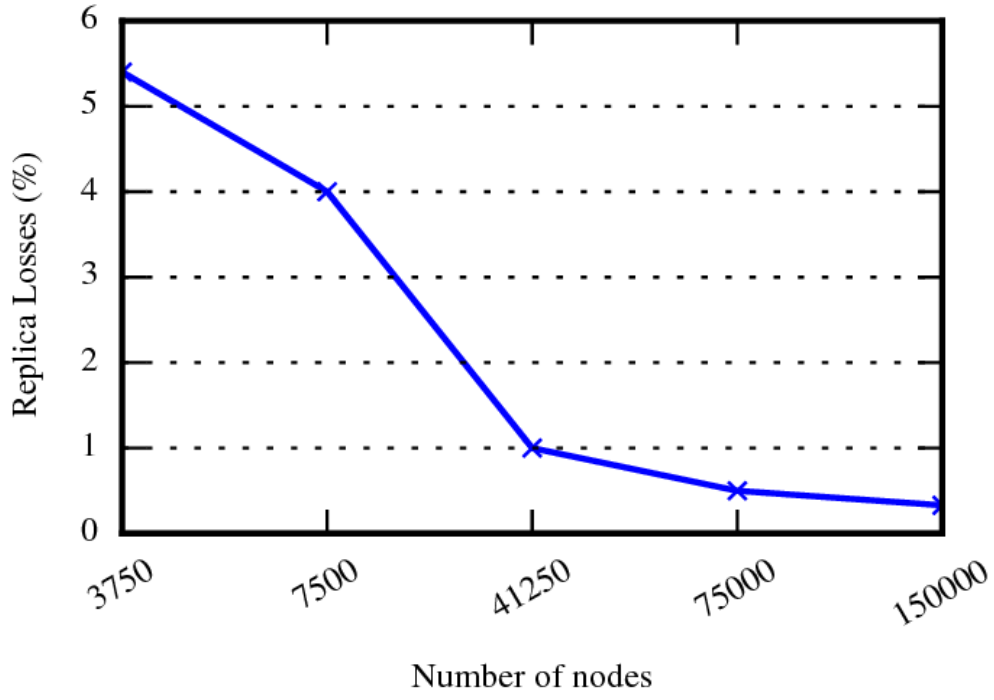
$$\frac{chaindata}{N} + \text{UTXO-set} + \text{hot\_data}$$

όπου chaindata το μέγεθος του blockchain, N το πλήθος των κόμβων, UTXO-set το μέγεθος της βάσης δεδομένων με το σύνολο των unspent transaction outputs και hot_data ο όγκος των blocks που έχουν κατατεθεί στο blockchain έως και 24 ώρες πριν. Ωστόσο, ο ορισμός των hot_data είναι σχετικός, ο ορισμός των 24 ωρών έγινε στα πλαίσια των προσομοιώσεων της εργασίας. Το διάγραμμα αναφέρεται στις τιμές του σημερινού Bitcoin blockchain, δηλαδή: chainada = 130GB, UTXO-set = 1.3GB, hot_data = 144MB.

Επομένως, γίνεται ουσιαστικά πλήρης κλιμάκωση ως προς τον όγκο του blockchain, ενώ κάθε κόμβος θα αποθηκεύει επιπλέον έναν πάγιο όγκο δεδομένων, αυτόν των UTXO-set και hot_data. Αν μπορεί να γίνει ένα σχόλιο σχετικά με τον όγκο των UTXO-set και hot_data, το πρώτο εξαρτάται από το πλήθος των ενεργών διευθύνσεων Bitcoin και την κλίμακα στην οποία συναλλάσσονται (θεωρητικά θα αυξάνεται μέχρι να σταθεροποιηθεί η διάδοση του Bitcoin ως μέσου πληρωμών) και το δεύτερο από το ρυθμό δημιουργίας και το μέγεθος των blocks, αν και όπως αναφέρθηκε παραπάνω πρόκειται για ένα ευέλικτο μέγεθος.

- ***Replicas losses***

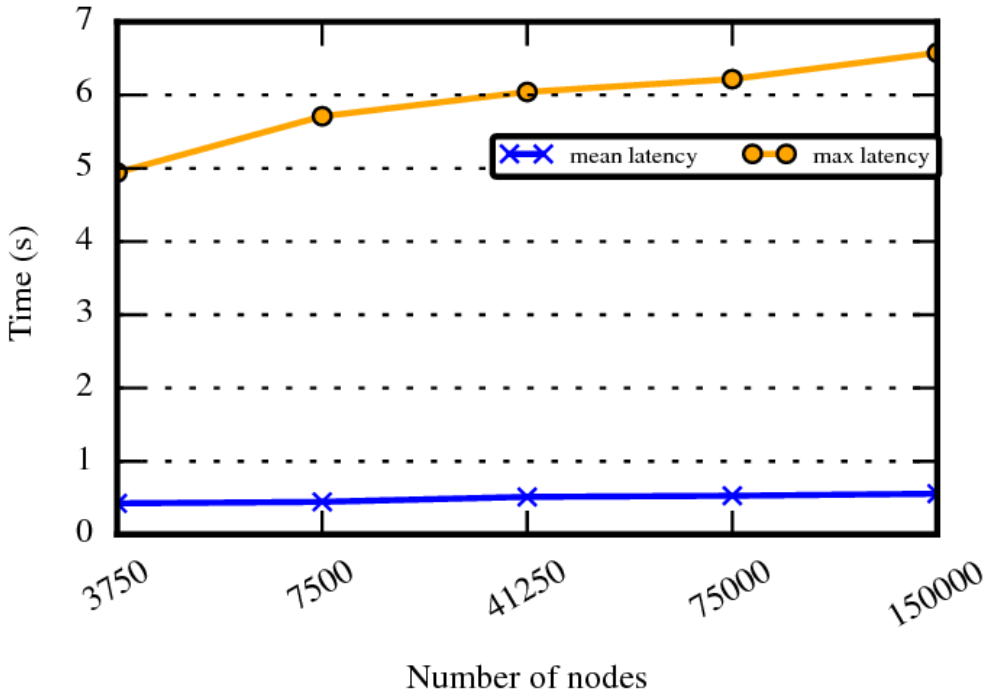
Οι μέγιστες απώλειες αντιγράφων που καταγράφηκαν, οι οποίες προκύπτουν από τις προσομοιώσεις του συστήματος υπό τις συνθήκες του μέγιστου ρυθμού αφίξεων–αναχωρήσεων, δηλαδή της άφιξης ή αναχώρησης πλήθους κόμβων ίσου με το 48 % των κόμβων του DHT ανά ώρα, απεικονίζονται στο παρακάτω διάγραμμα.



Σχήμα 11: *Ποσοστό μέγιστων απωλειών αντιγράφων.*

Οι απώλειες αντιγράφων είναι αντιστρόφως ανάλογες του πλήθους των κόμβων του DHT. Ακόμη και για την περίπτωση του δικτύου των 3,750 κόμβων οι απώλειες δεν ξεπερνούν το 6% σε περιπτώσεις πολύ έντονου ρυθμού αφίξεων-αναχωρήσεων κόμβων. Η παράμετρος αυτή, εκτός από την κινητικότητα του δικτύου, εξαρτάται και από τις ταχύτητες λήψης και αποστολής δεδομένων. Καθώς για τις μετρήσεις η ταχύτητα internet κάθε κόμβου κυμαίνεται γύρω από τη μέση ταχύτητα (που υπολογίστηκε στα 14.5Mbps), είναι ασφαλές να θεωρηθεί ότι ακόμη και σε περίπτωση πολύ συχνών αναχωρήσεων κόμβων το σύστημα ανταποκρίνεται άμεσα, ώστε να είναι ανθεκτικό σε απώλειες δεδομένων. Θεωρητικά, στην περίπτωση απώλειας δεδομένων απ’ το DHT, αυτά αναπληρώνονται εύκολα λαμβάνοντάς τα από έναν full node. Ωστόσο, η ιδέα ενός DHT distributed blockchain ledger είναι μια εναλλακτική του full node. Όπως ένας full node δε βασίζεται σε κανέναν και δεν επιτρέπει την απώλεια των δεδομένων του, έτσι και σε ένα σύστημα DHT η απώλεια δεδομένων θα πρέπει να θεωρείται απαγορευτική.

- ***Query latency***



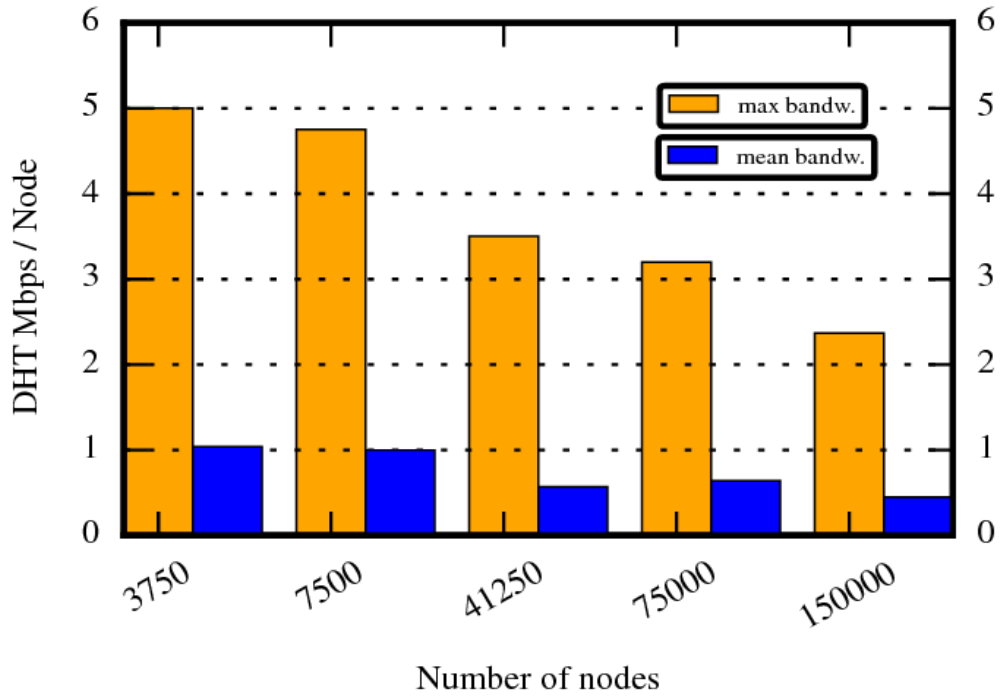
Σχήμα 12: *Καθυστέρηση για την εξυπηρέτηση ενός ερωτήματος.*

Στις προσομοιώσεις έγινε η θεώρηση ότι το 50% των ερωτημάτων αφορά σε blocks τα οποία δημιουργήθηκαν τις τελευταίες 24 ώρες (*hot data*). Καθώς έχει αποφασιστεί ο κάθε κόμβος να διατηρεί την πληροφορία αυτή τοπικά αποθηκευμένη, τα αντίστοιχα ερωτήματα εξυπηρετούνται χωρίς την ανάγκη προώθησης και δρομολόγησης εντός του DHT, δηλαδή χωρίς πρόσθετη καθυστέρηση. Η μέση καθυστέρηση ενός ερωτήματος είναι 450-500ms με ελάχιστη αύξηση αναλογικά με το πλήθος των κόμβων. Η μέγιστη καθυστέρηση που παρατηρείται, μη λαμβάνοντας υπόψιν καθυστερήσεις λόγω αποτυχίας κόμβων, αυξάνεται επίσης αναλογικά με το μέγεθος του DHT και κυμαίνεται μεταξύ 5-6s.

- ***Bandwidth***

Ένας πολύ σημαντικός παράγοντας είναι το bandwidth που απαιτείται από έναν κόμβο για τη συμμετοχή του στο υπό μελέτη σύστημα. Το χρησιμοποιούμενο εύρος προκύπτει από την αποστολή

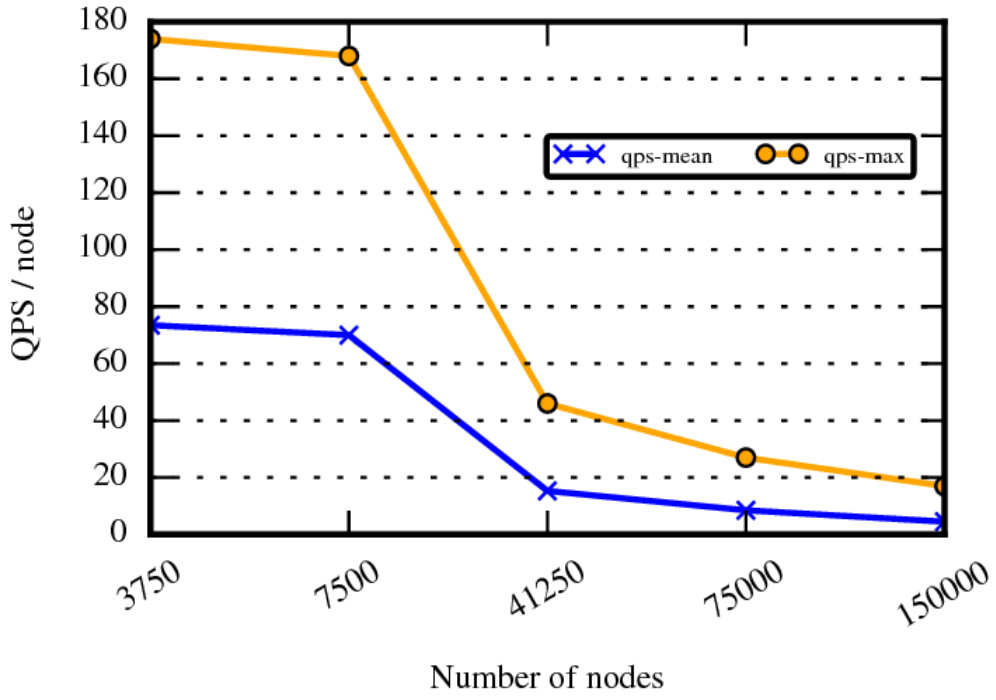
και λήψη δεδομένων αφενός λόγω συμμετοχής στο δίκτυο του Bitcoin και αφετέρου λόγω πρωτοκόλλου DHT. Στο ραβδόγραμμα που ακολουθεί, η χρησιμοποίηση εύρους ζώνης για την εξυπηρέτηση ερωτημάτων θεωρείται λειτουργία του δικτύου Bitcoin και δεν υπάγεται στη χρησιμοποίηση λόγω πρωτοκόλλου DHT.



Σχήμα 13: *Bandwidth ενός κόμβου για ανταλλαγή δεδομένων σε επίπεδο πρωτοκόλλου DHT.*

Το bandwidth που απαιτείται για τη διατήρηση των αντιγράφων του DHT, όπως φαίνεται και στις αντίστοιχη γραφική παράσταση, είναι σχετικά χαμηλό σε σύγκριση με το bandwidth που χρησιμοποιεί ένας σημερινός κόμβος Bitcoin, αλλά και σε σύγκριση με τη μέση ταχύτητα ίντερνετ που υπολογίζεται ότι διαθέτει ένας κοινός χρήστης. Το μέσο bandwidth για την εξυπηρέτηση ερωτημάτων σε επίπεδο δικτύου Bitcoin αυτή τη στιγμή είναι κατά μέσο όρο 7.2Mbps και κατά το μέγιστο 24Mbps, ενώ η διαθέσιμη ταχύτητα ίντερνετ ενός κοινού χρήστη υπολογίζεται περίπου στα 14.5Mbps. Επομένως, το overhead που προκύπτει από τη χρήση του DHT είναι πολύ χαμηλό, ειδικά αν το αντιπαραθέσουμε με το όφελος του capacity που έχουν οι συμμετέχοντες κόμβοι.

- ***Congestion***



Σχήμα 14: *Πλήθος ερωτημάτων ανά κόμβο (qps = queries per second).*

Στην παραπάνω γραφική απεικονίζεται το πλήθος των ερωτημάτων που δέχεται ένας κόμβος του DHT. Οι τιμές αναφέρονται σε σταθερό ρυθμό 120,000 ερωτημάτων ανά δευτερόλεπτο. Η αξία του γραφήματος, βέβαια, δεν έγκειται στις τιμές αυτές καθαυτές, αλλά στη σχέση μεταξύ μέσου και μέγιστου ρυθμού άφιξης ερωτημάτων σε έναν κόμβο, αφού σκοπός είναι ο εντοπισμός πιθανών σημείων συμφόρησης στο DHT. Όπως φαίνεται στα αποτελέσματα ο μέγιστος ρυθμός άφιξης ερωτημάτων που μπορεί να παρατηρηθεί σε έναν κόμβο ανά δευτερόλεπτο μπορεί να είναι 2 ή το πολύ 3 φορές μεγαλύτερος του μέσου ρυθμού. Είναι μία θεωρητικά μικρή απόκλιση, που δεν υποδεικνύει την ύπαρξη σημείων συμφόρησης. Ας σημειωθεί ότι ο ρυθμός των 120,000 ερωτημάτων ανά δευτερόλεπτο ξεπερνά κατά πολύ αυτόν των 6,750, που είναι ο μέσος ρυθμός που υπολογίζεται για το σημερινό δίκτυο Bitcoin.

5.3 Αξιολόγηση του DHT blockchain

Οι μετρήσεις που έγιναν σχετικά με κρίσιμες μετρικές που προσδιορίζουν τη λειτουργία ενός συμμετέχοντα κόμβου στο DHT δείχνουν ότι μια τέτοια εφαρμογή θα μπορούσε να λειτουργήσει αποδοτικά. Αυτό σημαίνει πως ο χρήστης ενός κοινού μηχανήματος, στον οποίο κυρίως αναφέρεται η παρούσα πρόταση, θα είχε τη δυνατότητα συμμετοχής σε έναν “αποκεντρωμένο full node” χωρίς υψηλές απαιτήσεις πόρων. Πιο συγκεκριμένα, κάνοντας όσο το δυνατόν πιο ρεαλιστικές υποθέσεις με βάση τα σημερινά χαρακτηριστικά ενός Bitcoin full node και του Bitcoin δικτύου εν γένει, προκύπτουν τα κατωτέρω στοιχεία για δίκτυο Chord με 7,500 ή περισσότερους κόμβους:

- ➔ Δεν υπάρχει ουσιαστικός κίνδυνος απώλειας δεδομένων απ’ το DHT, εφόσον γίνει κατάλληλη επιλογή του συντελεστή αντιγραφής και λαμβάνονται τα απαραίτητα μέτρα ασφαλείας κατά κακόβουλων κόμβων. Για επιλογή συντελεστή 1% επί του πλήθους των κόμβων και για επίπεδα κινητικότητας εντός λογικών πλαισίων (έως 5 φορές μεγαλύτερη από το μέσο όρο), οι μέγιστες απώλειες αντιγράφων μιας εγγραφής του DHT δεν ξεπερνούν το 4%.
- ➔ Η καθυστέρηση εξυπηρέτησης ενός ερωτήματος είναι ικανοποιητικά χαμηλή, αφού έχει μέση τιμή 500ms ενώ στη χειρότερη περίπτωση μπορεί να φτάσει σε τιμές της τάξης των 5-6s.
- ➔ Το bandwidth που προκύπτει ως overhead λόγω DHT κυμαίνεται σε επίπεδα κάτω του 1Mbps, με μέγιστη στιγμιαία τιμή μέχρι 5Mbps. Αναλογιζόμενοι ότι το μέσο διαθέσιμο bandwidth ενός Bitcoin node είναι 14.5Mbps, η μέση χρησιμοποίηση είναι ικανοποιητικά χαμηλή.
- ➔ Επιβάλλοντας στους κόμβους του DHT την τοπική αποθήκευση των blocks του blockchain που δημιουργήθηκαν τις τελευταίες 24 ώρες, δεν παρατηρούνται φαινόμενα συμφόρησης, που σημαίνει ότι δεν επιβαρύνεται δυσανάλογα κανείς κόμβος και το σύστημα μπορεί να παρέχει υψηλή διαθεσιμότητα δεδομένων.

6 Επίλογος

Σε αυτήν τη διπλωματική εργασία έγινε εκτενής αναφορά στο blockchain, με ανάλυση της τεχνολογίας του, αναφορά στο πρόβλημα κλιμάκωσής του και στις κυριότερες λύσεις που έχουν προταθεί μέχρι σήμερα γι’ αυτό. Επιπλέον, έγινε παρουσίαση μιας νέας πρότασης για αποθήκευση ενός blockchain σε DHT, που στοχεύει στη μείωση του όγκου πληροφορίας που αποθηκεύουν οι κόμβοι ενός δικτύου blockchain. Η πρόταση αυτή αξιολογήθηκε βάσει προσομοιώσεων που έγιναν με τη χρήση ενός εργαλείου που αναπτύχθηκε σε γλώσσα Java και αφορούν στην αποθήκευση του Bitcoin blockchain σε ένα Chord DHT. Τα αποτελέσματα δείχνουν πως μια τέτοια υλοποίηση είναι δυνατή, καθώς κρίσιμες μετρικές των κόμβων ενός τέτοιου συστήματος όπως το bandwidth και το congestion κυμαίνονται σε κανονικά επίπεδα και κλιμακώνουν με την αύξηση των κόμβων. Μαλιστα, σύμφωνα με τη μελέτη που έγινε, είναι δυνατή η κατανομή ενός blockchain σε DHT με πολύ σημαντικά επίπεδα εξοικονόμησης αποθηκευτικού χώρου, της τάξεως του 98%.

Ως περαιτέρω έρευνα, θα μπορούσε γίνει πραγματική δοκιμή του συστήματος που προτείνεται στην εργασία, δηλαδή σύσταση ενός Chord DHT. Έτσι, μπορεί να γίνει μελέτη της κλιμάκωσης που επιτυγχάνεται για μεταβλητό αριθμό κόμβων και παρακολούθηση των απωλειών αντιγράφων τού DHT σε πραγματικά μεγέθη.

7 Αναφορές

[1] Dwork, C., Naor, M.: Pricing via processing or combatting junk mail. In: Advances in Cryptology.

[2] Fox, Geoffrey. "Peer-to-peer networks." *Computing in Science & Engineering* 3.3 (2001): 75-77.

[3] https://en.wikipedia.org/wiki/Smart_contract

[4] P. Koshy. Bitcoin and the Byzantine Generals Problem – a Crusade is needed? A Revolution? http://financialcryptography.com/mt/archives/001522.html, November 2014.

[5] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3):382–401, July 1982. http: //research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf.

[6] https://en.bitcoin.it/wiki/Proof_of_work

[7] Villasenor, John (26 April 2014). "Secure Bitcoin Storage: A Q&A With Three Bitcoin Company CEOs". *forbes.com*. Forbes. Retrieved 26 April 2014.

[8] "MtGox gives bankruptcy details". *bbc.com*. BBC. 4 March 2014. Retrieved 13 March 2014.

[9] https://bitnodes.21.co

[10] https://statoshi.info

[11] https://en.bitcoin.it

[12] https://en.wikipedia.org/wiki/SegWit

[13] http://web.archive.org/web/20160121231718/http://apps.usa.visa.com/merchants/become-a merchant/show-a-visa-transaction-works.jsp, 2015.

[14] Croman, Kyle, et al. "On scaling decentralized blockchains." *International Conference on Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2016.

[15] https://en.bitcoin.it/wiki/Confirmation

[16] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system, 2008." *URL: http://www. bitcoin. org/bitcoin. Pdf* (2012).

[17] https://en.bitcoin.it/wiki/Scalability

[18] http://www.investopedia.com/terms/p/proof-stake-pos.asp

[19] Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." *Technical Report (draft)* (2015).

[20] https://bitcoin.org/en/glossary/mainnet

[21] Oram, A. (Ed.). (2001). Peer-to-peer: Harnessing the Benefits of a Disruptive Technologies. O'Reilly Media, Inc.

[22] Filali, Imen; et al. (2011). "A Survey of Structured P2P Systems for RDF Data Storage and Retrieval". In Hameurlain, Abdelkader; et al. *Transactions on Large-Scale Data- and Knowledge-Centered Systems III: Special Issue on Data and Knowledge Management in Grid and PSP Systems*. Springer. p. 21.

[23] Ratnasamy et al. (2001). "A Scalable Content-Addressable Network". In Proceedings of ACM SIGCOMM 2001. Retrieved 2013-05-20.

[24] Stoica, I.; Morris, R.; Karger, D.; Kaashoek, M. F.; Balakrishnan, H. (2001). "Chord: A scalable peer-to-peer lookup service for internet applications". *ACM SIGCOMM Computer Communication Review*.

[25] Cohen, David (October 1, 2002). "New P2P network funded by US government". *New Scientist*. Retrieved November 10, 2013.

[26] "MIT, Berkeley, ICSI, NYU, and Rice Launch the IRIS Project". *Press release*. MIT. September 25, 2002. Retrieved November 10, 2013.

[27] https://en.wikipedia.org/wiki/BitTorrent

[28] *https://en.wikipedia.org/wiki/Coral_Content_Distribution_Network*

[29] Naor, Moni and Wieder, Udi. Novel Architectures for P2P Applications: the Continuous-Discrete Approach. Proc. SPAA, 2003.

[30] Manku, Gurmeet Singh. Dipsea: A Modular Distributed Hash Table. Ph. D. Thesis (Stanford University), August 2004.

[31] Maymounkov P., Mazières D. (2002) Kademlia: A Peer-to-Peer Information System Based on the XOR Metric. In: Druschel P., Kaashoek F., Rowstron A. (eds) Peer-to-Peer Systems. IPTPS 2002. Lecture Notes in Computer Science, vol 2429. Springer, Berlin, Heidelberg

[32] Ben Y. Zhao, John Kubiatowicz, and Anthony D. Joseph (2001) Tapestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing. Computer Science Division University of California, Berkeley.

[33] Rowstron A., Druschel P. (2001) Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems. In: Guerraoui R. (eds) Middleware 2001. Middleware 2001. Lecture Notes in Computer Science, vol 2218. Springer, Berlin, Heidelberg

[34] https://en.wikipedia.org/wiki/Consistent_hashing

[35] Douceur, John R. "The sybil attack." *International Workshop on Peer-to-Peer Systems*. Springer, Berlin, Heidelberg, 2002

[36] Singh, Atul. "Eclipse attacks on overlay networks: Threats and defenses." *In IEEE INFOCOM*. 2006.

[37] Baumgart, Ingmar, and Sebastian Mies. "S/kademlia: A practicable approach towards secure key-based routing." *Parallel and Distributed Systems, 2007 International Conference on*. IEEE, 2007.

[38] https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf

[39] https://coin.dance/nodes/all

[40] Economist Staff (31 October 2015). "Blockchains: The great chain of being sure about things". *The Economist*. Retrieved 18 June 2016.

[41] https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/

[42] https://bitcoin.org/en/developer-guide#block-chain

[43] Bradbury, Danny. "The problem with Bitcoin." *Computer Fraud & Security* 2013.11 (2013): 5- 8.

[44] Luu, Loi, et al. "Demystifying incentives in the consensus computer." *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015.

[45] https://www.cryptocompare.com/mining/guides/what-are-mining-rewards-in-ethereum/

[46] https://blog.ethereum.org/2016/05/09/on-settlement-finality/

[47] https://blockchain.info/

[48] https://etherscan.io/

[49] Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". *Harvard Business Review*. Harvard University.

[50] Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." *International Workshop on Open Problems in Network Security*. Springer International Publishing, 2015.

[51] Pilkington, Marc. "Blockchain technology: principles and applications." *University of Burgundy, France* (2015).

[52] Antonopoulos, Andreas M. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media Inc.", 2014.

[53] https://bitcoinwisdom.com/bitcoin/difficulty

[54] Nielsen, Jakob. "Nielsen’s law of internet bandwidth." *Online at http://www.useit.com/alertbox/980405. Html* (1998).