Κατανεμημένα Συστήματα

9ο εξάμηνο
Εξαμηνιαία Εργασία

Τερέζα Άννα Βασιλείου 03120403
Παντελής Εμμανουήλ 03119018
Γιώργος Κυριάκος 03119204

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Η.Μ.Μ.Υ.

Ακαδημαϊκό Έτος 2023-2024

Σχεδιασμός Συστήματος

Στην παρούσα εργασία υλοποιήθηκε ένα σύστημα χρηματικών συναλλαγών και ανταλλαγής μηνυμάτων μεταξύ χρηστών σε απομακρυσμένα συστήματα χρησιμοποιώντας τη τεχνολογία Blockchain. Η τεχνολογία αυτή εξασφαλίζει στο σύστημα συνέπεια, ιδιωτικότητα και αξιοπιστία για όλα τα είδη συναλλαγών. Σκόπος είναι η συμφωνία όλων των χρηστών για την κατάσταση του συστήματος. Οι συναλλαγές λαμβάνονται και επιβεβαιώνονται από όλους τους κόμβους, οι οποίοι επιλέγουν από κοινού τον validator, ο οποίος κατασκευάζει ένα block, όπου τοποθετεί τις συναλλαγές που έχουν επικυρωθεί, και στη συνέχεια το στέλνει στους υπόλοιπους για να προστεθεί στην αλυσίδα.
Κάθε κόμβος διαθέτει ένα δημόσιο και ένα ιδιωτικό ψηφιακό κλειδί, όπως και ένα αναγνωριστικό (id). Τα κλειδιά αυτά δημιουργούνται μέσω του αλγορίθμου RSA. Επίσης, διατηρεί λίστα με τα υπόλοιπα των λογαριασμών όλων των χρηστών, τα στοιχεία επικοινωνίας τους και την αλυσίδα με τις μέχρι τώρα επικυρωμένες συναλλαγές. Η επικοινωνία μεταξύ των κόμβων έχει υλοποιηθεί με sockets και ξεχωριστά threads για αποστολή και λήψη μηνυμάτων.

Αρχικοποίηση

Αρχικά, δημιουργείται ο κόμβος bootstrap, ο οποίος δημιουργεί το genesis block, το πρώτο block της αλυσίδας. Στη συνέχεια, κάθε κόμβος που δημιουργείται στέλνει στον bootstrap τα στοιχεία επικοινωνίας του και τη δημόσια διεύθυνσή του, και λαμβάνει το id και την παρούσα κατάσταση του συστήματος (αλυσίδα που επικυρώνεται, υπόλοιπα κλπ). Όταν εισαχθούν όλοι οι κόμβοι, ο bootstrap τους στέλνει επίσης τα στοιχεία επικοινωνίας τους για να μπορούν να επικοινωνήσουν μεταξύ τους.

Transactions

Ένα transaction μπορεί να είναι μήνυμα κειμένου ή μεταφορά χρηματικού ποσού και κοστολογείται ανάλογα με το μήκος του κειμένου ή ενός ποσοστού επί του μεταφερόμενου ποσού, αντίστοιχα. Η συναλλαγή υπογράφεται από τον αποστολέα χρησιμοποιώντας το ιδιωτικό κλειδί του με τον αλγόριθμο PKCS1_v1_5, και “ασφαλίζεται” με ένα hash, ώστε να μην μπορεί να τροποποιηθεί. Έπειτα, οι υπόλοιποι χρήστες μπορούν να επαληθεύσουν την εγκυρότητα του αποστολέα χρησιμοποιώντας την υπογραφή του και το δημόσιο κλειδί του. Επίσης, ελέγχει την επάρκεια του balance κάθε αποστολέα, καθώς και το ότι το μήνυμα δεν επαναποστέλεται από κακόβουλους χρήστες. Αυτό εξασφαλίζεται με τη μεταβλητή nonce, που αντιστοιχεί στον αύξοντα αριθμό του αποστολέα κάθε transaction, και καθώς αυξάνεται σε κάθε λήψη μηνύματος αποτρέπει την λήψη του μηνύματος δεύτερη φορά. Αν μια συναλλαγή επιβεβαιωθεί, ενημερώνεται το soft balance του (προσωρινό χρηματικό υπόλοιπο κάθε κόμβου, που μπορεί να αλλάξει αν τελικά το transaction δεν εισαχθεί στο blockchain).

Blocks

Όταν συμπληρωθεί ο απαραίτητος αριθμός επικυρωμένων transactions, οι κόμβοι αποφασίζουν ποιός θα είναι ο validator του επόμενου block με την ακόλουθη διαδικασία. Κάθε κόμβος θέτει

ένα ποσό ως stake, το οποίο αντιστοιχεί στην πιθανότητά του να γίνει validator. Η επιλογή του validator γίνεται τυχαία με λοταρία, με κοινό seed για όλους τους κόμβους ίσο με το hash του προηγούμενου επικυρωμένου block της αλυσίδας. Με τον τρόπο αυτό, εξασφαλίζεται ότι όλοι οι κόμβοι θα υπολογίσουν τον ίδιο validator. Αφού καθοριστεί, ο validator σχηματίζει ένα block και προσθέτει σε αυτό τα τελευταία transactions που έχει επικυρώσει. Το block αποστέλλεται σε όλους τους κόμβους, οι οποίοι επικυρώνουν τη γνησιότητα του validator και του hash και εφόσον επικυρωθεί το προσθέτουν στην αλυσίδα. Επιπλέον, ανανεώνουν τα hard balances που διατηρούν, και ανανεώνουν τα soft balances με τις τιμές των hard. Όλα τα transactions που έχουν ληφθεί πριν την λήψη του νέου block διαγράφονται, αφού υπάρχει περίπτωση να μην είναι πλέον εφικτά παρόλο που έχουν επικυρωθεί, δεδομένων των νέων τιμών των balances. Με τη διαδικασία αυτή, διασφαλίζεται ότι ακόμα κι αν χαθούν κάποια transactions, όλοι οι κόμβοι θα διαθέτουν το ίδιο blockchain, και θα υπάρχει συμφωνία μεταξύ τους σχετικά με το ποιες συναλλαγές έχουν πραγματοποιηθεί και ποιες όχι.

Αποτελέσματα πειραμάτων

Για 5 κόμβους:

	Transaction Throughput
5	98.600
10	99.162
20	91.416

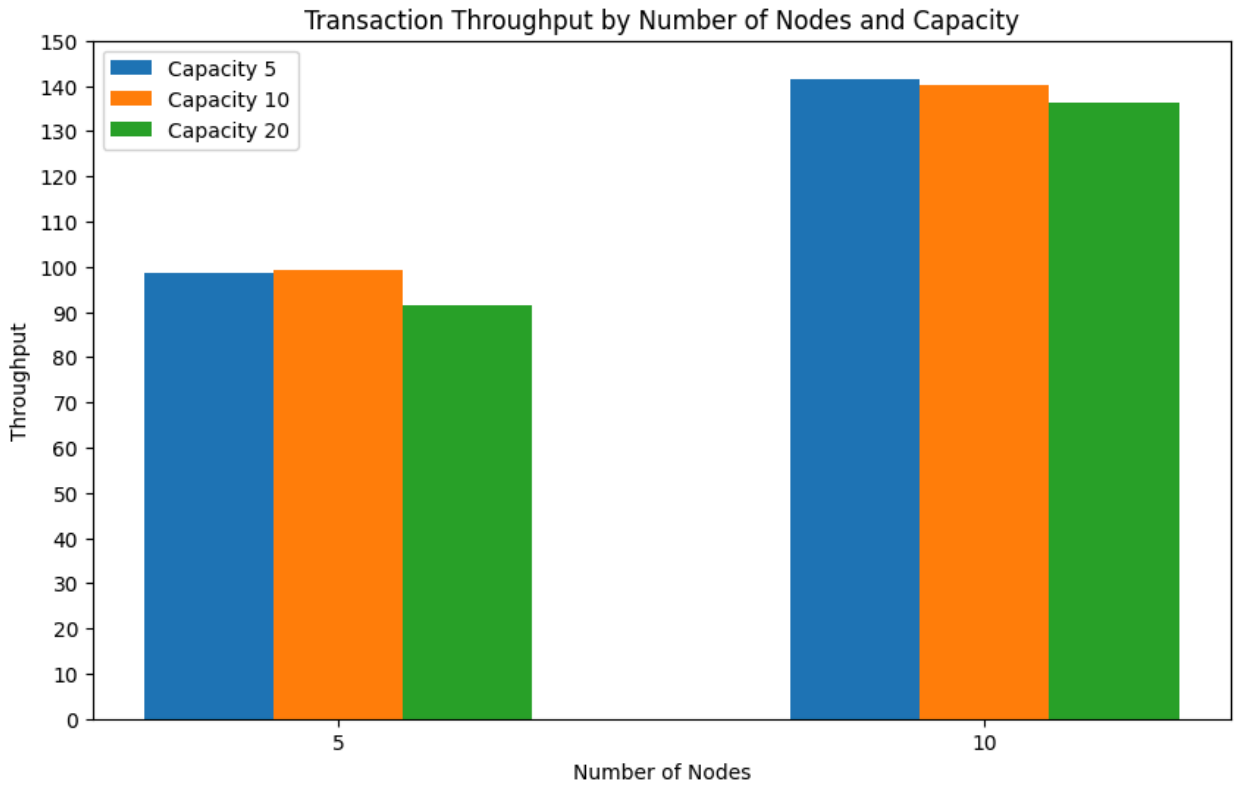
	Block Throughput
5	19.900
10	10.116
20	4.386

Για 10 κόμβους:

	Transaction Throughput
5	141.580
10	140.300
20	136.302

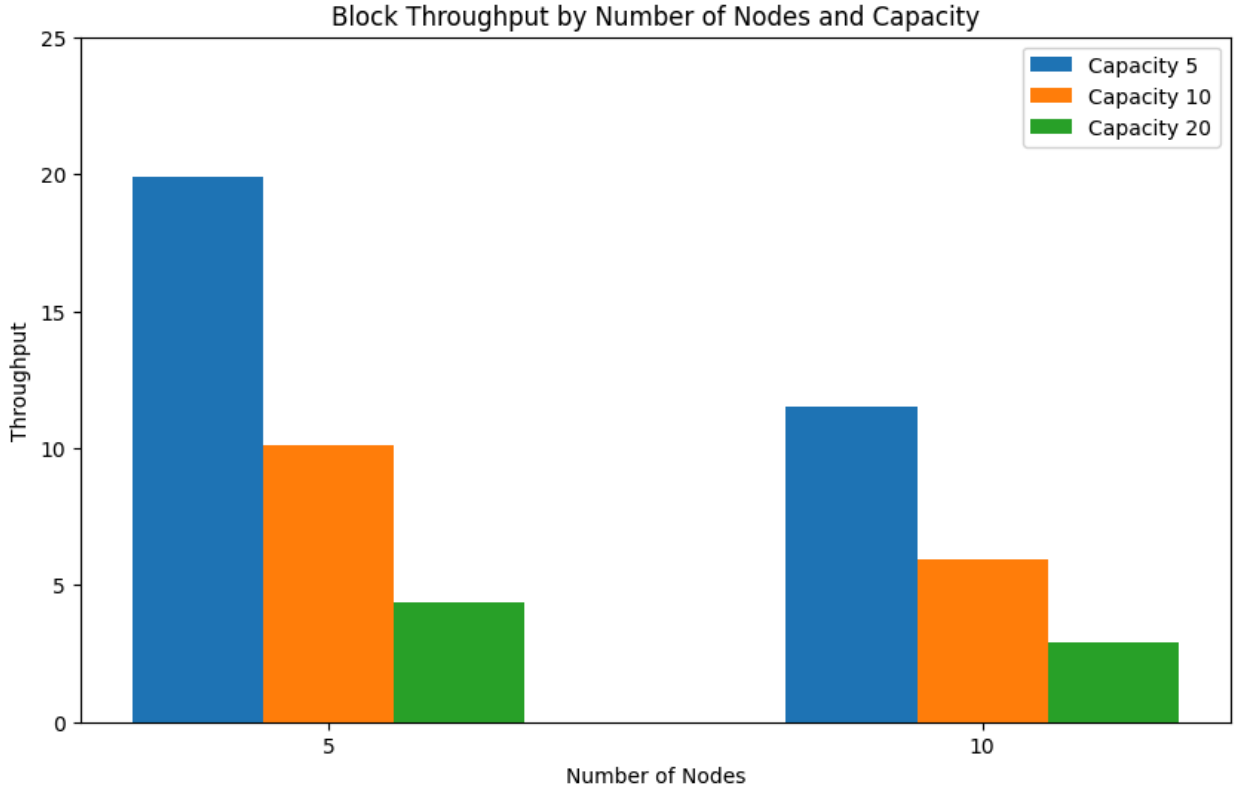
	Block Throughput
5	11.490
10	5.920
20	2.882

Τα αποτελέσματα των πειραμάτων φαίνονται στα ακόλουθα διαγράμματα.



Παρατηρούμε ότι για μεγαλύτερες τιμές capacity, το throughput μειώνεται ελαφρώς, αλλά οι διαφορές είναι πολύ μικρές. Αυτό συμβαίνει επειδή η καθυστέρηση εξυπηρέτησης των transactions οφείλεται κυρίως στον χρόνο αποστολής των μηνυμάτων στο δίκτυο, και όχι στον χρόνο υπολογισμού των κρυπτογραφικών συναρτήσεων για τα blocks. Επιπλέον, βλέπουμε ότι η αύξηση του πλήθους των κόμβων οδηγεί σε μεγαλύτερο throughput, αφού περισσότερα transactions αποστέλλονται και εξυπηρετούνται ταυτόχρονα (από 10 κόμβους αντί για 5).

Ωστόσο, αν λάβουμε υπόψη τον διπλασιασμό των transactions, παρατηρούμε ότι το throughput δεν έχει διπλασιαστεί. Άρα η συνολική απόδοση του συστήματος μειώνεται.



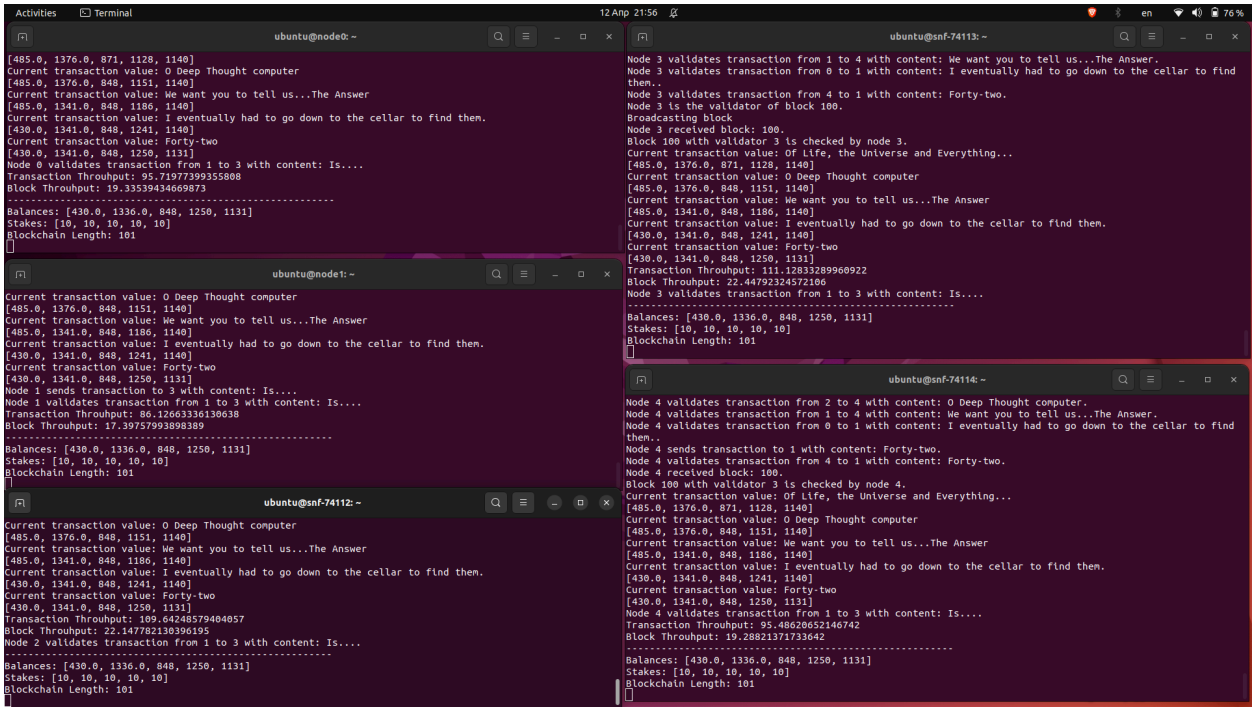
Το throughput των blocks βλέπουμε ότι γενικά μειώνεται καθώς αυξάνεται το capacity, αφού κάθε block θα περιέχει περισσότερα transactions, τα οποία απαιτούν περισσότερο χρόνο για να εξυπηρετηθούν. Παράλληλα, ο αριθμός των block μειώνεται. Τέλος, βλέπουμε ότι με περισσότερους κόμβους, το throughput των blocks είναι χαμηλότερο. Αυτό εξηγείται από το γεγονός ότι με περισσότερους κόμβους, παρατηρούμε περισσότερα χαμένα transactions, οπότε το συνολικό μήκος του blockchain στο τέλος είναι μικρότερο. Αυτό συμβαίνει επειδή αποστέλλονται περισσότερα transactions ταυτόχρονα, οπότε πολλά δεν προλαβαίνουν να εισαχθούν στο block και διαγράφονται. Συνεπώς φτιάχνονται λιγότερα block και το μήκος της αλυσίδας μειώνεται. Παρατηρούμε ότι στην πρώτη περίπτωση εξυπηρετούνται όλα τα transactions, ενώ στην δεύτερη ειδικά στην περίπτωση μικρού block, περίπου τα μισά.

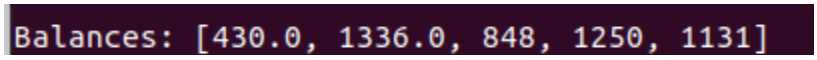
Δικαιοσύνη

Παρακάτω φαίνεται η εκτέλεση των συναλλαγών για 5 κόμβους και capacity = 5. Στην πρώτη περίπτωση έχουμε σταθερό staking = 10 για όλους τους κόμβους. Στην δεύτερη περίπτωση έχουμε staking = 100 για τον κόμβο με id = 1.

Παρατηρούμε ότι ο κόμβος 1 (στον οποίο βάζουμε μεγάλο stake) καταλήγει με αισθητά περισσότερα BCC. Αυτό είναι λογικό καθώς λόγω του δεκαπλάσσου staking έχει 10 φορές μεγαλύτερη πιθανότητα να είναι ο validator σε κάθε block (από τη συνάρτηση POS). Άρα, παίρνει πολύ πιο συχνά τα fees και πλουτίζει ενώ οι υπόλοιποι κόμβοι οδηγούνται σε πτώχευση. Επίσης, βλέπουμε ότι το μήκος της αλυσίδας μειώνεται (blockchain length). Δηλαδή, κατασκευάζονται λιγότερα block. Αυτό είναι λογικό αφού οι υπόλοιποι κόμβοι πτωχεύουν και δεν έχουν επαρκή αριθμό χρημάτων για να εκτελέσουν τις συναλλαγές τους.

<u>Σταθερό staking = 10 BCC για όλους τους κόμβους</u>





Κόμβος 1 με staking = 100