Πανεπιστήμιο Πατρών

Τμήμα Μηχανικών Η/Υ και Πληροφορικής

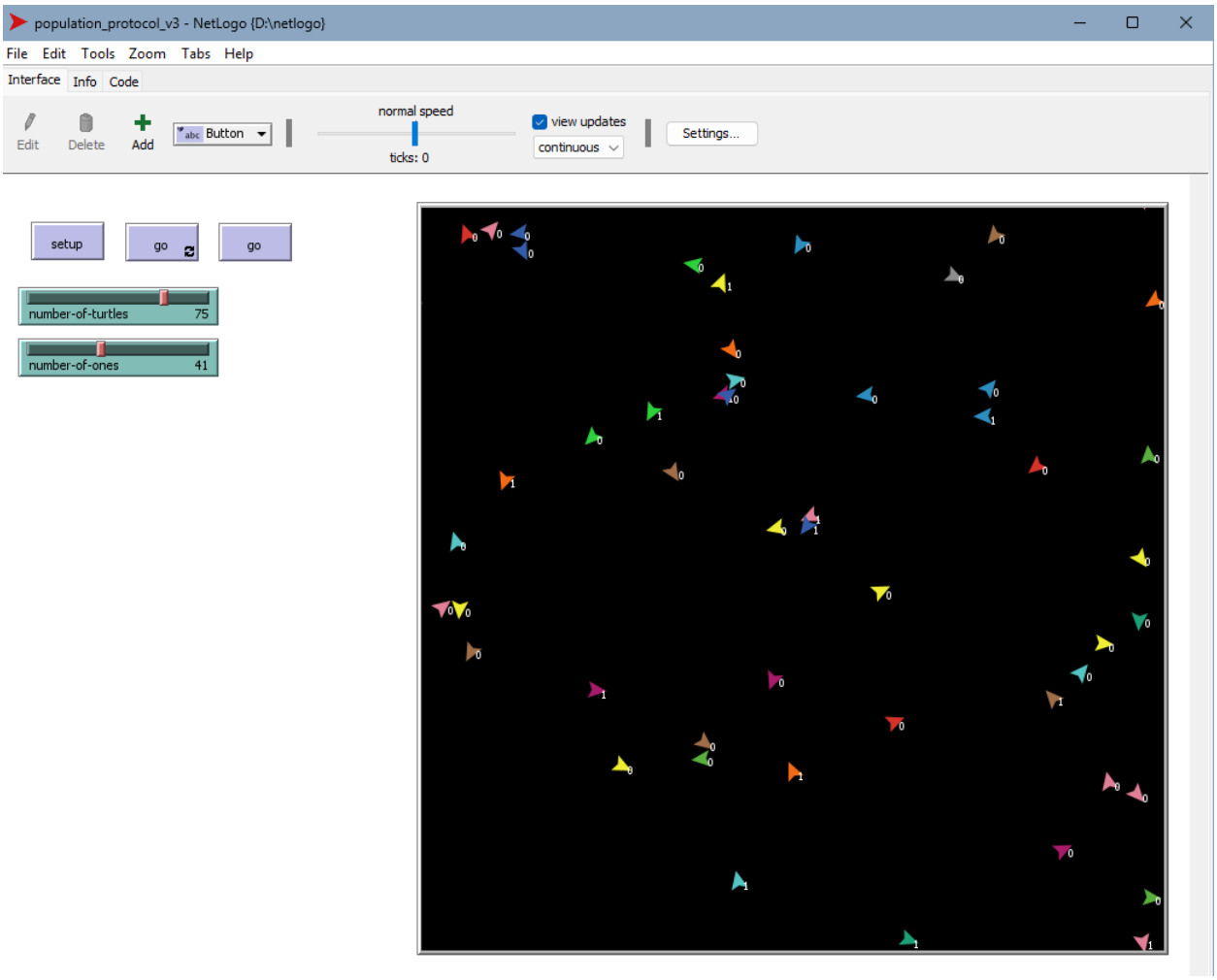
2ο Σύνολο Προγραμματιστικών Ασκήσεων

Θεόφραστος Παξιμάδης 1093460

Κωνσταντίνος Αναστασόπουλος 1093320

Άσκηση 1

Το παραπάνω πρωτόκολλο είναι ακριβώς αυτό που έχει υλοποιηθεί και στο περιβάλλον της netlogo.

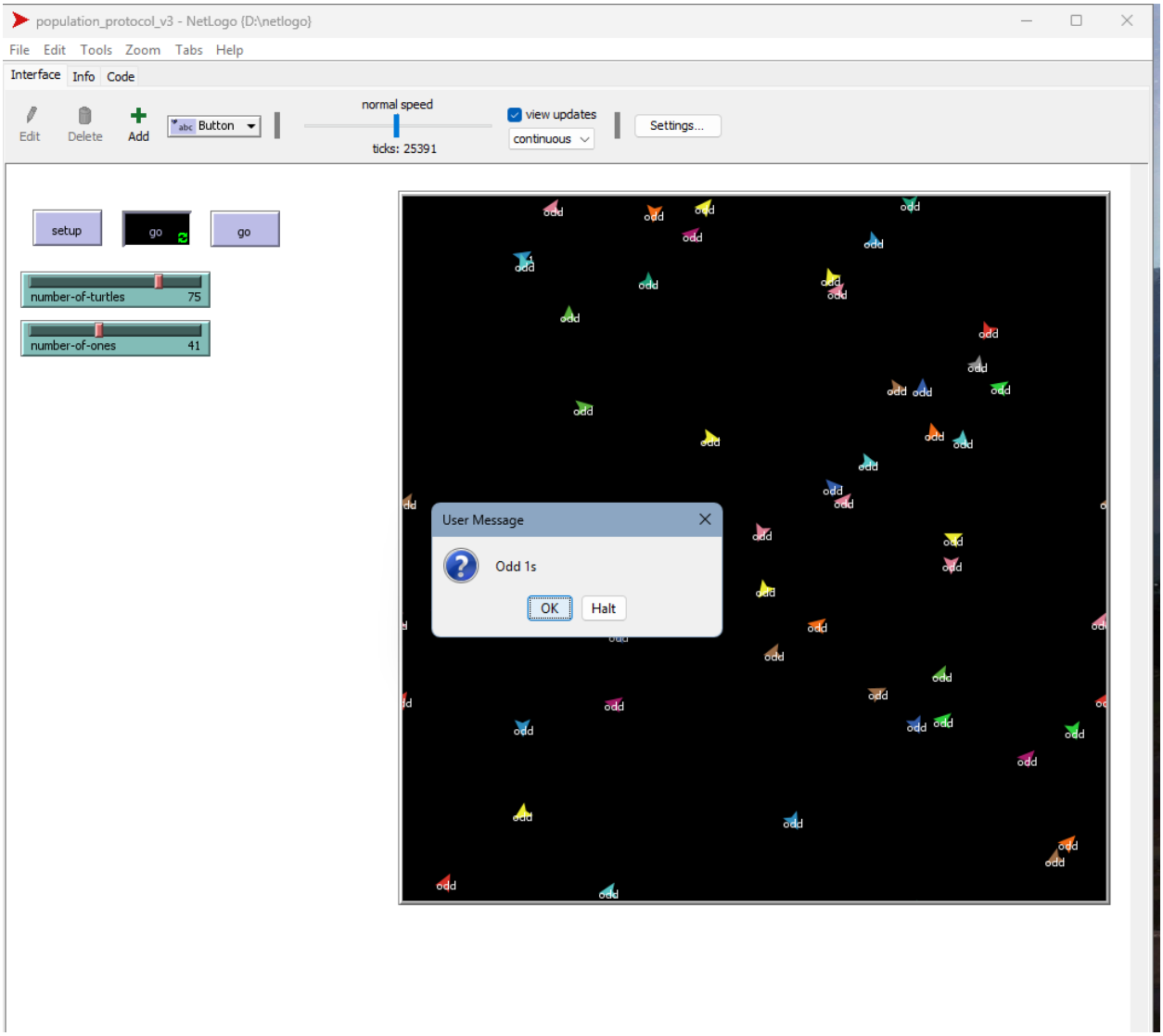


Επιλέγοντας το setup, δημιουργούνται χελώνες ίσες με το slider number-of-turtles σε τυχαίες θέσεις και με τυχαίες κατευθύνσεις. Το slider number-of-ones καθορίζει πόσες από αυτές αρχικά θα είναι με τιμή 1.

Σε κάθε go, οι χελώνες προχωράνε κατά μία θέση σε μία τυχαία κατεύθυνση. Όταν έρθουν σε επαφή με άλλη χελώνα, δηλαδή βρεθούνε στο ίδιο patch, τότε εξετάζονται οι τιμές τους και αλλάζουν σύμφωνα με τα transitions του πρωτοκόλλου. Αυτό επιτυγχάνεται με πολλαπλά ifs στην go. Επίσης, στο τέλος της

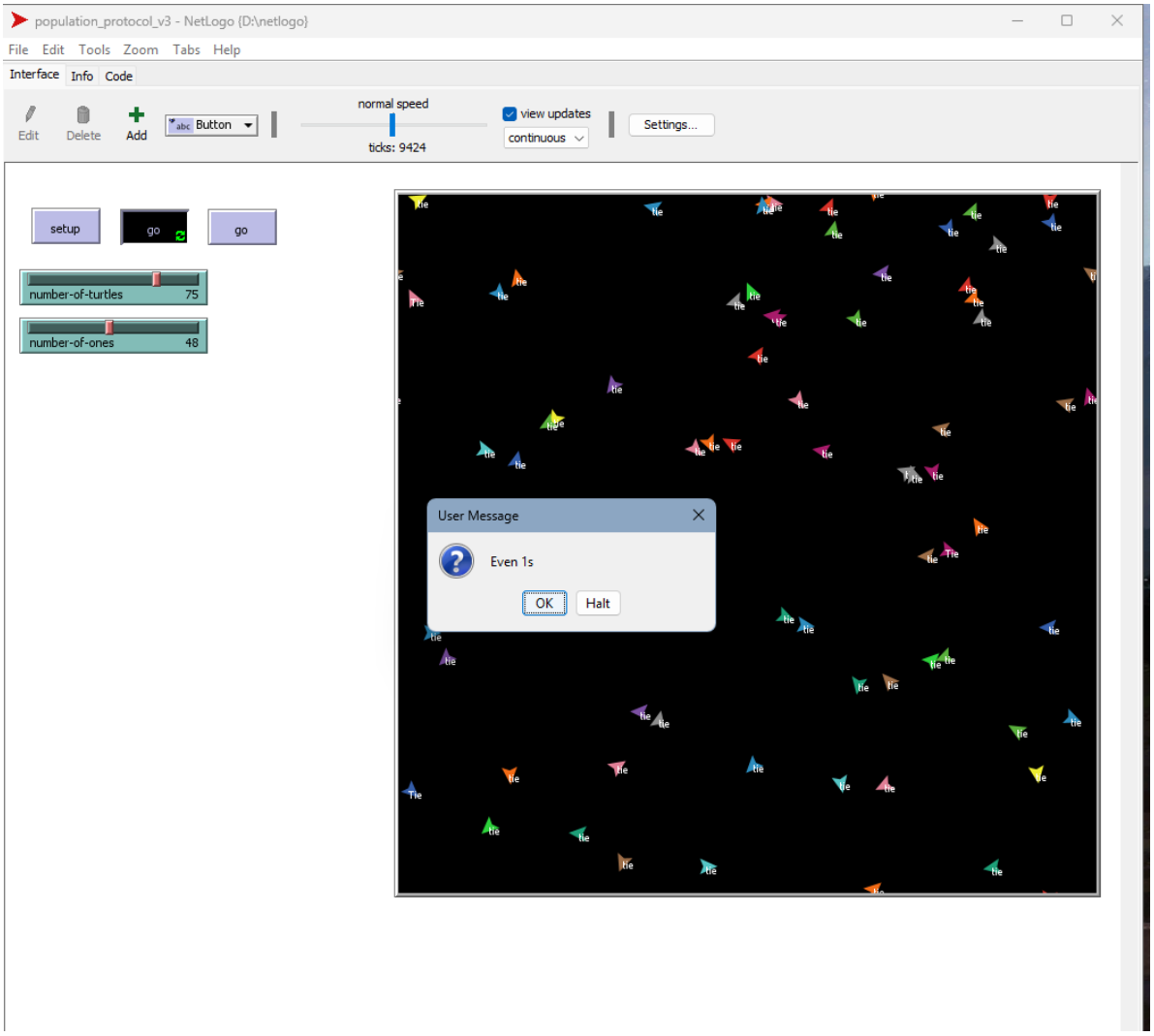
go, εξετάζεται εάν όλες οι χελώνες είναι σε τιμή 1 και odd, ή αλλιώς σε 0, even, Tie και tie. Εάν ισχύει κάποια από τις δύο περιπτώσεις, τότε σημαίνει ότι έχει επιτευχθεί το consensus.

Εάν πατήσουμε το κουμπί go forever με 75 χελώνες και 41 από αυτές με την τιμή 1:



Τότε βλέπουμε ότι το consensus επιτυγχάνεται μετά από 25391 ticks και όλες οι χελώνες έχουν την τιμή odd, εκτός από μία με την τιμή 1, το οποίο είναι το αναμενόμενο.

Αντίστοιχο αποτέλεσμα λαμβάνουμε και στην περίπτωση των άρτιων άσσων.

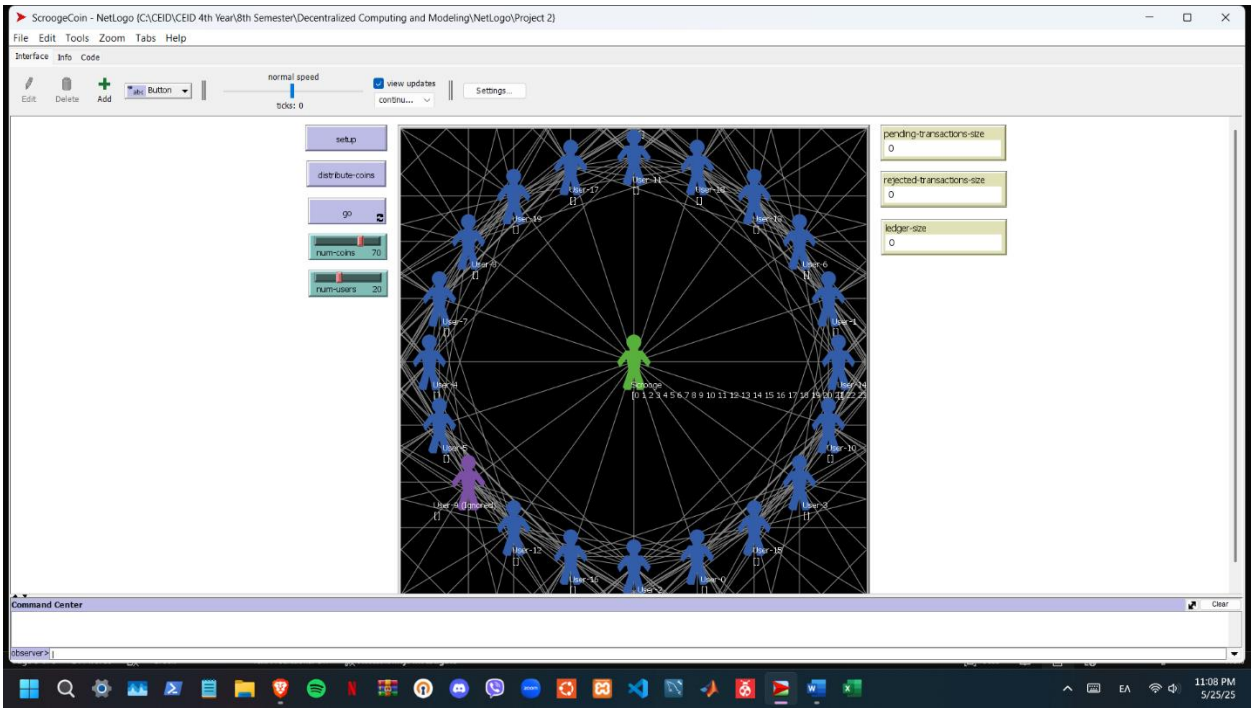


Μία παρατήρηση είναι πως στην περίπτωση των άρτιων άσσων, ο κώδικας τερματίζει αναλογικά γρηγορότερα, διότι δεν σημειώνεται η αναδρομή με τα Tie και 1.

Τέλος, να σημειωθεί πως στο αρχικό πρωτόκολλο, το consensus για να επιτευχθεί χρειαζόταν χρόνο τρομερά μεγαλύτερο.

Άσκηση 2

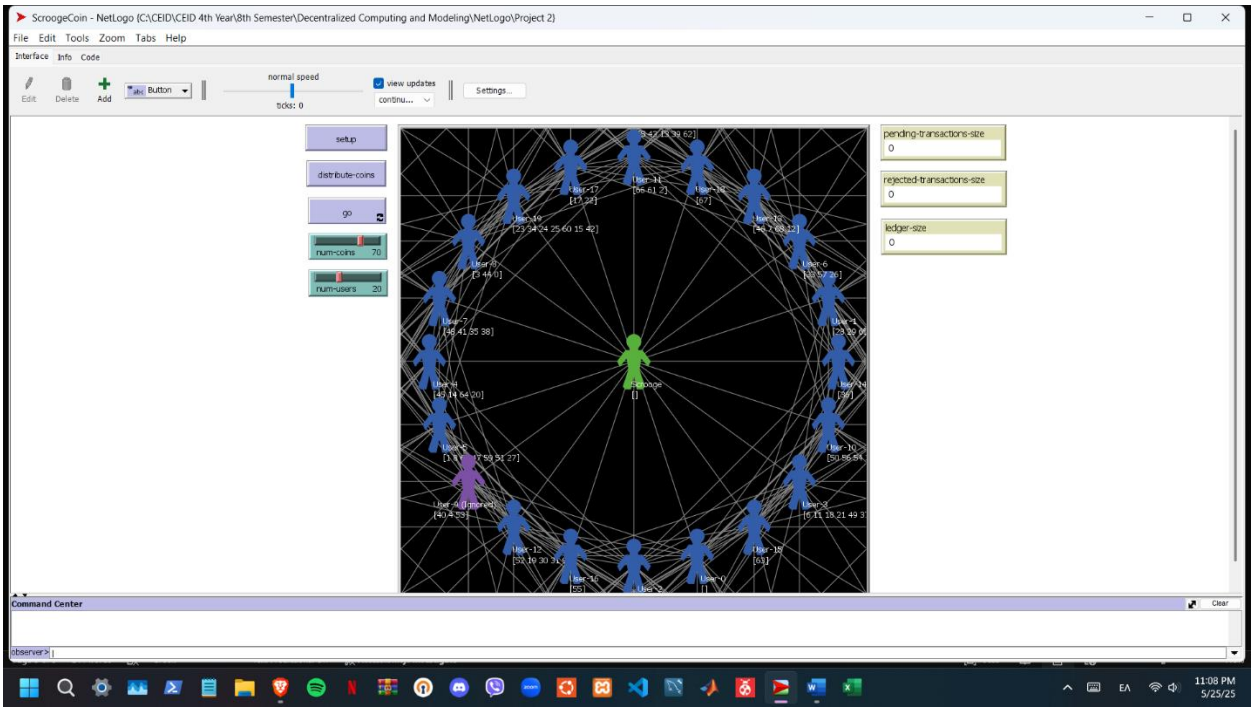
Ο τρόπος που προσομοιώνεται το scrooge coin είναι ένα γράφημα. Οι χρήστες είναι κόμβοι τοποθετημένοι σε διάταξη κύκλου και ο scrooge βρίσκεται στη μέση του κύκλου. Όλοι οι κόμβοι είναι συνδεδεμένοι μεταξύ τους για να κάνουν συναλλαγές. Κάθε κόμβος έχει ένα όνομα και ένα πορτοφόλι, το περιεχόμενο του οποίου προβάλλεται κάτω από το όνομα. Το περιβάλλον προσομοίωσης φαίνεται παρακάτω.



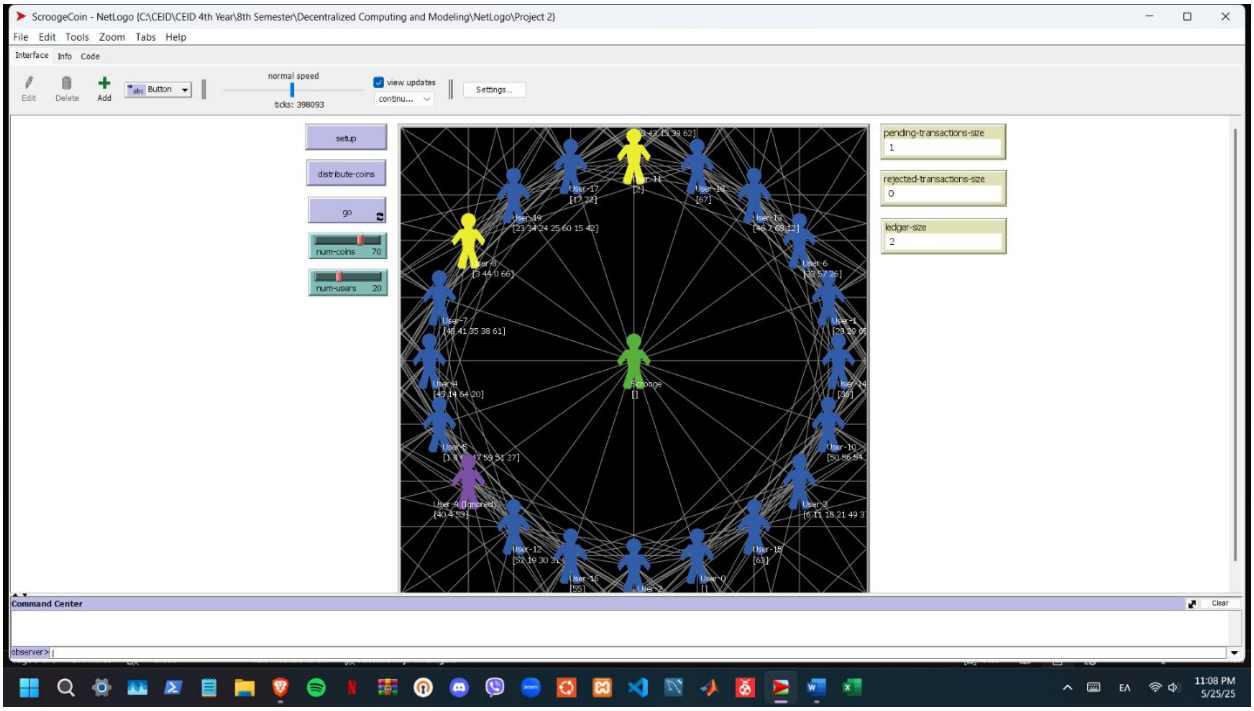
Ο χρήστης μπορεί μέσω των sliders να ρυθμίσει τον αριθμό των χρηστών του δικτύου και τον αριθμό των διαθέσιμων νομισμάτων.

Με το πάτημα του κουμπιού setup, δημιουργείται το γράφημα και ο scrooge κατασκευάζει όσα νομίσματα όρισε ο χρήστης και τα αποθηκεύει στο πορτοφόλι του.

Με το πάτημα του κουμπιού distribute-coins, ο scrooge μοιράζει τα νομίσματα τυχαία στους χρήστες. Το κάθε νόμισμα είναι ξεχωριστό και έχει μοναδικό id.

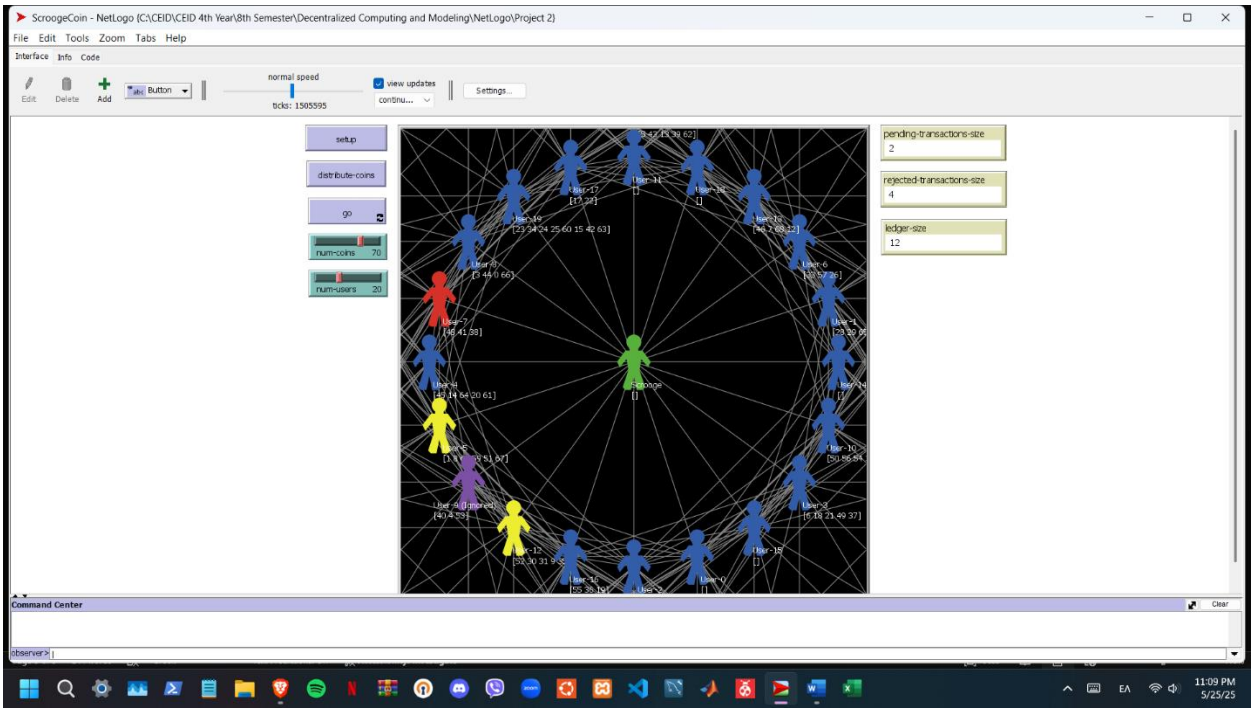


Όταν ο χρήστης πατήσει go, επαναληπτικά, κάθε 100.000 ticks, ένας τυχαίος χρήστης επιλέγει στην τύχη έναν άλλο χρήστη και προσπαθεί να εκτελέσει συναλλαγή, δηλαδή να μεταφέρει ένα από τα νομίσματά του από το πορτοφόλι του στο πορτοφόλι του άλλου. Οι εμπλεκόμενοι στη συναλλαγή χρήστες μαρκάρονται με κίτρινο χρώμα.



Τότε η συναλλαγή (sender-id, receiver-id, coin-id) εισάγεται σε μια λίστα pending-transactions.

Κάθε 500.000 ticks, ένας κακόβουλος χρήστης αποφασίζει να κάνει double spending attack. Δημιουργεί ένα duplicate coin με ίδιο id με κάποιο άλλο coin που έχει στο πορτοφόλι του και προσπαθεί να κάνει συναλλαγή με δύο άλλους τυχαία επιλεγμένους χρήστες. Και οι δύο συναλλαγές εισάγονται στη λίστα pending-transactions. Ο κακόβουλος χρήστης μαρκάρεται με κόκκινο χρώμα, ενώ οι δύο δέκτες με κίτρινο.



Κάθε 100.000 ticks ο scrooge ελέγχει τα pending-transactions. Μετράει τα συνολικά coins στο δίκτυο μέσω της μεταβλητής total-value. Αν το total-value του δικτύου παραμένει σταθερό, η συναλλαγή που είναι στη λίστα pending-transactions υπογράφεται από τον scrooge. Αν έχουν προκύψει παραπάνω coins μέσω double spending attack, υπογράφει μόνο τη μία συναλλαγή, ενώ την άλλη τη μεταφέρει στη λίστα rejected-transactions και καταστρέφει το duplicate coin. Η συναλλαγή που υπογράφεται μεταφέρεται από τη λίστα pending-transactions, στο ιστορικό ledger, που έχει το ρόλο ενός append-only blockchain.

Κατά το τρέξιμο, βλέπουμε στα monitors δεξιά ότι ανά 500.000 ticks αυξάνεται το μέγεθος του rejected-transactions λόγω μη υπογραφής συναλλαγών που αποτελούν απόπειρες double spending. Αντίστοιχα το μέγεθος του ledger αυξάνεται κάθε 100.000 ticks, δηλαδή κάθε μία συναλλαγή.

Στο γράφημα φαίνεται επίσης ένας μωβ χρήστης με ετικέτα Ignored. Ο χρήστης αυτός επιλέγεται τυχαία κατά το setup από τον scrooge και τα αιτήματά του αγνοούνται, δηλαδή δεν υπογράφονται ποτέ και μένουν για πάντα στη λίστα pending-transactions. Εδώ φαίνεται και ένα αρνητικό ενός συστήματος με μία κεντρική οντότητα που είναι εξουσιοδοτημένη να ελέγχει τις συναλλαγές. Οι χρήστες βασίζονται στο ότι η οντότητα θα είναι δίκαιη, αλλά αυτή έχει εξουσία πάνω στους χρήστες και αν αποφασίσει να στερήσει το δικαίωμα συναλλαγής από κάποιο χρήστη, αυτός είναι καταδικασμένος να μη συμμετέχει στο δίκτυο συναλλαγών.