**Αποκεντρωμένος Υπολογισμός & Μοντελοποίηση**

**3ο σύνολο Προγραμματιστικών/Θεωρητικών Ασκήσεων**

**Θεωρητικές Ασκήσεις**

**Άσκηση 1:**

𝑥1(𝑡 + 1) = 𝑥1(𝑡)

𝑥2(𝑡 + 1) = 𝑎𝑥1(𝑡) + (1 − 𝑎)𝑥2(𝑡)

1. Ο παίκτης 1 βλέπουμε ότι ποτέ δεν αλλάζει άποψη. Αντιθέτως, ο παίκτης 2 επηρεάζεται από τον παίκτη 1.

Άρα,

Για να δείξουμε ότι το μητρώο Α είναι στοχαστικό ως προς τις γραμμές θα πρέπει το άθροισμα της κάθε γραμμής να είναι ίσο με 1. Πράγματι, για την γραμμή 1 έχουμε ότι 1+0=1 και για την γραμμή 2 έχουμε α+1-α=1.

Άρα, ιδιοτιμές του Α είναι οι λ1 = 1 και λ2 = 1 – α

Για λ=1:

Για λ=1-α:

Άρα τα ιδιοδιανύσματα του Α είναι τα:

1. Το γράφημα είναι συνεκτικό, όχι ισχυρά όμως, γιατί δεν υπάρχει κατευθυνόμενο μονοπάτι από τον κόμβο 2 στον κόμβο 1.

1-α

α

1

2

1

1. Για παίκτη 1:

Για παίκτη 2:

**Άσκηση 2:**

1. Όταν το 80% της υπολογιστικής ισχύος στο δίκτυο Bitcoin τρέχει την υλοποίηση Α, εφόσον υπερβαίνει το 50%, υπερισχύει η λάθος πλειοψηφία κατά την διαδικασία επαλήθευσης. Έτσι, θα υπάρχει η δυνατότητα αλλαγής του ledger (υπολογισμός νέων headers). Ως αποτέλεσμα, στο blockchain θα καταγραφεί το μπλοκ με την διπλοξοδευμένη συναλλαγή ως έγκυρο.
2. Όταν το 80% της υπολογιστικής ισχύος στο δίκτυο Bitcoin τρέχει την υλοποίηση Β, εφόσον υπερβαίνει το 50%, υπερισχύει η σωστή πλειοψηφία κατά την διαδικασία επαλήθευσης. Έτσι, δεν θα υπάρχει η δυνατότητα αλλαγής του ledger (υπολογισμός νέων headers). Ως αποτέλεσμα, στο blockchain δεν θα καταγραφεί το μπλοκ με την διπλοξοδευμένη συναλλαγή ως έγκυρο.

**Άσκηση 3:**

Ο Bob δεν πρέπει να δεχτεί το συγκεκριμένο πρωτόκολλο, καθώς η Alice μπορεί να στείλει το s πριν λήξει το συμβόλαιο του Bob (CM), αλλά μετά την λήξη του συμβολαίου της Alice (CA). Έτσι, ο Bob δεν θα λάβει το κόκκινο νόμισμα από την Alice και θα της επιστραφεί, ενώ η Alice θα λάβει το πράσινο νόμισμα από τον Bob, αφού θα ενεργοποιηθεί το CM.