Trust Is Risk: Μία Αποκεντρωμένη Πλατφόρμα Οικονομικής Εμπιστοσύνης

Ορφέας Στέφανος Θυφρονίτης Λήτος

Εθνικό Μετσόβιο Πολυτεχνείο
olitos@corelab.ntua.gr

Περίληψη Κεντρικά συστήματα φήμης χρησιμοποιούν αστέρια και κριτικές και επομένως χρειάζονται απόκρυψη αλγορίθμων για να αποφεύγουν τον αθέμιτο χειρισμό. Σε αυτόνομα αποκεντρωμένα συστήματα ανοιχτού κώδικα αυτή η πολυτέλεια δεν είναι διαθέσιμη. Στο παρόν κατασκευάζουμε ένα δίκτυο φήμης για αποκεντρωμένες αγορές όπου η εμπιστοσύνη που δίνει η κάθε χρήστης στις υπόλοιπες είναι μετρήσιμη και εκφράζεται με νομισματικούς όρους. Εισάγουμε ένα νέο μοντέλο για πορτοφόλια bitcoin στα οποία τα νομίσματα κάθε χρήστη μοιράζονται σε αξιόπιστες συνεργάτες. Η άμεση εμπιστοσύνη ορίζεται χρησιμοποιώντας μοιραζόμενους λογαριασμούς μέσω των 1-από-2 multisig του bitcoin. Η έμμεση εμπιστοσύνη ορίζεται έπειτα με μεταβατικό τρόπο. Αυτό επιτρέπει να επιχειρηματολογούμε με αυστηρό παιγνιοθεωρητικό τρόπο ως προς την ανάλυση κινδύνου. Αποδεικνύουμε ότι ο κίνδυνος και οι μέγιστες ροές είναι ισοδύναμα στο μοντέλο μας και ότι το σύστημά μας είναι ανθεκτικό σε επιθέσεις Sybil. Το σύστημά μας επιτρέπει τη λήψη σαφών οικονομικών αποφάσεων ως προς την υποκειμενική χρηματική ποσότητα με την οποία μπορεί ένας παίκτης να εμπιστευθεί μία ψευδώνυμη οντότητα. Μέσω ανακατανομής της άμεσης εμπιστοσύνης, ο κίνδυνος που διατρέχεται κατά την αγορά από μία ψευδώνυμη πωλήτρια παραμένει αμετάβλητος.

Keywords: αποκεντρωμένο · εμπιστοσύνη · δίκτυο εμπιστοσύνης · γραμμές πίστωσης · εμπιστοσύνη ως κίνδυνος · ροή · φήμη · decentralized · trust · web-of-trust · bitcoin · multisig · line-of-credit · trust-as-risk · flow · reputation

Abstract. Centralized reputation systems use stars and reviews and thus require algorithm secrecy to avoid manipulation. In autonomous open source decentralized systems this luxury is not available. We create a reputation network for decentralized marketplaces where the trust each user gives to the rest of the users is quantifiable and expressed in monetary terms. We introduce a new model for bitcoin wallets in which user coins are split among trusted associates. Direct trust is defined using shared bitcoin accounts via bitcoin's 1-of-2 multisig. Indirect trust is subsequently defined transitively. This enables formal game theoretic arguments pertaining to risk analysis. We prove that risk and maximum flows are equivalent in our model and that our system is Sybil-resilient. Our system allows for concrete financial decisions on the subjective monetary amount a pseudonymous party can be trusted with. Through direct trust redistribution, the risk incurred from making a purchase from a pseudonymous vendor in this manner remains invariant.

Περιεχόμενα

Κατάλογος Σχημάτων

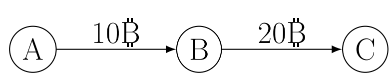
Κατάλογος Ψευδοκωδίκων

1 Εισαγωγή

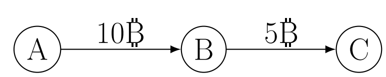
Οι αποκεντρωμένες αγορές μπορούν να κατηγοριοποιηθούν ως κεντρικές και αποκεντρωμένες. Ένα παράδειγμα για κάθε κατηγορία είναι το ebay και το OpenBazaar. Ο κοινός παρονομαστής των καθιερωμένων διαδικτυακών αγορών είναι το γεγονός ότι η φήμη κάθε πωλήτριας και πελάτισσας εκφράζεται κατά κανόνα με τη μορφή αστεριών και κριτικών των χρηστών, ορατές σε όλο το δίκτυο.

Ο στόχος μας είναι να δημιουργήσουμε ένα σύστημα φήμης για αποκεντρωμένες αγορές όπου η εμπιστοσύνη που η κάθε χρήστης δίνει στους υπόλοιπους είναι ποσοτικοποιήσιμη με νομισματικούς όρους. Η κεντρική παραδοχή που χρησιμοποιείται σε όλο το μήκος της παρούσας εργασίας είναι ότι η εμπιστοσύνη είναι ισοδύναμη με τον κίνδυνο, ή η θέση ότι η *εμπιστοσύνη* της *Alice* προς το χρήστη *Charlie* ορίζεται ως το *μέγιστο χρηματικό ποσό* που η *Alice* μπορεί να χάσει όταν ο *Charlie* είναι ελεύθερος να διαλέξει όποια στρατηγική θέλει. Για να υλοποιήσουμε αυτή την ιδέα, θα χρησιμοποιήσουμε τις *πιστωτικές γραμμές* όπως προτάθηκαν από τον Washington Sanchez [1]. Η *Alice* συνδέεται στο δίκτυο όταν εμπιστεύεται ενεργητικά ένα συγκεκριμένο χρηματικό ποσό σε έναν άλλο χρήστη, για παράδειγμα το φίλο της τον *Bob*. Αν ο *Bob* έχει ήδη εμπιστευθεί ένα χρηματικό ποσό σε έναν τρίτο χρήστη, τον *Charlie*, τότε η *Alice* εμπιστεύεται έμμεσα τον *Charlie* αφού αν ο τελευταίος ήθελε να παίξει άδικα, θα μπορούσε να έχει κλέψει ήδη τα χρήματα που του εμπιστεύθηκε ο *Bob*. Θα δούμε αργότερα ότι η *Alice* μπορεί τώρα να εμπλακεί σε οικονομική δραστηριότητα με τον *Charlie*.

Για να υλοποιήσουμε τις πιστωτικές γραμμές, θα χρησιμοποιήσουμε το Bitcoin [2], ένα αποκεντρωμένο κρυπτονόμισμα που διαφέρει από τα συμβατικά νομίσματα γιατί δεν βασίζεται σε αξιόπιστους τρίτους. Όλες οι συναλλαγές δημοσιεύονται σε ένα αποκεντρωμένο "λογιστικό βιβλίο", το blockchain. Κάθε συναλλαγή παίρνει κάποια νομίσματα ως είσοδο και παράγει ορισμένα νομίσματα ως έξοδο. Αν η έξοδος μιας συναλλαγής δεν συνδέεται στην είσοδο μιας άλλης, τότε η έξοδος αυτή ανήκει στο UTXO, το σύνολο των αξόδευτων εξόδων συναλλαγών. Διαισθητικά, το UTXO περιέχει όλα τα αξόδευτα νομίσματα.



Σχ. 1: Η Α εμπ. έμμεσα τον C 10₿



Σχ. 2: Η Α εμπ. έμμεσα τον C 5₿

Προτείνουμε ένα νέο είδος πορτοφολιού όπου τα νομίσματα δεν έχουν αποκλειστικό ιδιοκτήτη, αλλά τοποθετούνται σε μοιραζόμενους λογαριασμούς που υλοποιούνται μέσω των 1-από-2 multisig, μια κατασκευή του bitcoin που επιτρέπει σε μία από δύο προκαθορισμένες χρήστες να ξοδέψουν τα νομίσματα που περιέχονται σε έναν κοινό λογαριασμό [3]. Θα χρησιμοποιήσουμε το συμβολισμό $1/\{Alice, Bob\}$ για να αναπαραστήσουμε ένα 1-από-2 multisig που μπορεί να ξοδευτεί είτε από την $Alice$, είτε από τον Bob. Με αυτό το συμβολισμό, η σειρά των ονομάτων δεν έχει σημασία, εφ΄ όσον οποιαδήποτε από τις δύο χρήστες μπορεί να ξοδέψει τα νομίσματα. Ωστόσο, έχει σημασία ποια χρήστης καταθέτει τα χρήματα αρχικά στον κοινό λογαριασμό – αυτή η χρήστης διακινδυνεύει τα νομίσματά της.

Η προσέγγισή μας αλλάζει την εμπειρία της χρήστη κατά έναν διακριτικό αλλά και δραστικό τρόπο. Η χρήστης δεν πρέπει να βασίζει πια την εμπιστοσύνη της προς ένα κατάστημα σε αστέρια ή κριτικές που δεν εκφράζονται με οικονομικές μονάδες. Μπορεί απλά να συμβουλευθεί το πορτοφόλι της για να αποφασίσει αν το κατάστημα είναι αξιόπιστο και, αν ναι, μέχρι ποια αξία, μετρημένη σε bitcoin. Το σύστημα αυτό λειτουργεί ως εξής: Αρχικά η $Alice$ μεταφέρει τα χρήματά της από το ιδιωτικό της bitcoin πορτοφόλι σε 1-από-2 διευθύνσεις multisig μοιραζόμενες με φίλες που εμπιστεύεται άνετα. Αυτό καλείται άμεση εμπιστοσύνη. Το σύστημά μας δεν ενδιαφέρεται για τον τρόπο με τον οποίο οι παίκτες καθορίζουν ποιος είναι αξιόπιστος γι΄ αυτές τις απ΄ ευθείας 1-από-2 καταθέσεις. Αυτό το αμφιλεγόμενο είδος εμπιστοσύνης περιορίζεται στην άμεση γειτονιά κάθε παίκτη. Η έμμεση εμπιστοσύνη προς άγνωστους χρήστες υπολογίζεται από έναν ντετερμινιστικό αλγόριθμο. Συγκριτικά, συστήματα με αντικειμενικές αξιολογήσεις δε διαχωρίζουν τους γείτονες από τους υπόλοιπους χρήστες, προσφέροντας έτσι αμφιλεγόμενες ενδείξεις εμπιστοσύνης για όλους.

Ας υποθέσουμε ότι η $Alice$ βλέπει τα προϊόντα του πωλητή $Charlie$. Αντί για τα αστέρια του $Charlie$, η $Alice$ θα δει ένα θετικό αριθμό που υπολογίζεται από το πορτοφόλι της και αναπαριστά τη μέγιστη χρηματική αξία που η $Alice$ μπορεί να πληρώσει με ασφάλεια για να ολοκληρώσει μια αγορά από τον $Charlie$. Αυτή η αξία, γνωστή ως έμμεση εμπιστοσύνη, υπολογίζεται με το θεώρημα Εμπιστοσύνης – Ροής (2). Σημειώστε ότι η έμμεση εμπιστοσύνη προς κάποια χρήστη δεν είναι ενιαία αλλά υποκειμενική. Κάθε χρήστης βλέπει μια ιδιαίτερη έμμεση εμπιστοσύνη που εξαρτάται από την τοπολογία του δικτύου. Η έμμεση εμπιστοσύνη που εμφανίζεται από το σύστημά μας διαθέτει την ακόλουθη επιθυμητή ιδιότητα ασφαλείας: Αν η $Alice$ πραγματοποιήσει μια αγορά από τον $Charlie$, τότε εκτίθεται το πολύ στον ίδιο κίνδυνο στον οποίον εκτιθόταν πριν την αγορά. Ο υπαρκτός εθελούσιος κίνδυνος είναι ακριβώς εκείνος που η $Alice$ έπαιρνε μοιραζόμενη τα νομίσματά της με τις αξιόπιστες φίλες της. Αποδεικνύουμε το αποτέλεσμα αυτό στο θεώρημα Αμετάβλητου Κινδύνου (3). Προφανώς δε θα είναι ασφαλές για την *Alice* να αγοράσει οτιδήποτε από τον *Charlie* ή από οποιαδήποτε άλλη πωλήτρια αν δεν έχει ήδη εμπιστευθεί καθόλου χρήματα σε καμία άλλη χρήστη.

Βλέπουμε ότι στο Trust Is Risk τα χρήματα δεν επενδύονται τη στιγμή της αγοράς και κατ΄ ευθείαν στην πωλήτρια, αλλά σε μια προγενέστερη χρονική στιγμή και μόνο προς άτομα που είναι αξιόπιστα για λόγους εκτός παιχνιδιού. Το γεγονός ότι το σύστημα αυτό μπορεί να λειτουργήσει με έναν εξ ολοκλήρου αποκεντρωμένο τρόπο θα γίνει σαφές στις επόμενες ενότητες. Θα αποδείξουμε το αποτέλεσμα αυτό στο θεώρημα Sybil Αντίσταστης (5).

Κάνουμε τη σχεδιαστική επιλογή ότι η κάθε παίκτης μπορεί να εκφράζει την εμπιστοσύνη της μεγιστικά με όρους του διαθέσιμού της κεφαλαίου. Έτσι, μία φτωχή παίκτης δεν μπορεί να διαθέσει πολλή άμεση εμπιστοσύνη στις φίλες της ανεξαρτήτως του πόσο αξιόπιστες είναι. Από την άλλη, μία πλούσια παίκτης μπορεί να εμπιστευθεί ένα μικρό μέρος των χρημάτων της σε κάποια παίκτη που δεν εμπιστεύεται εκτενώς και παρ΄ όλα αυτά να εμφανίζει περισσότερη άμεση εμπιστοσύνη από τη φτωχή παίκτη του προηγούμενου παραδείγματος. Δεν υπάρχει άνω όριο στην εμπιστοσύνη. Κάθε παίκτης περιορίζεται μόνο από τα χρήματά της. Έτσι εκμεταλλευόμαστε την παρακάτω αξιοσημείωτη ιδιότητα του χρήματος: Το ότι κανονικοποιεί τις υποκειμενικές ανθρώπινες επιθυμίες σε αντικειμενική αξία.

Υπάρχουν διάφορα κίνητρα για να συνδεθεί μία χρήστης στο δίκτυο αυτό. Πρώτον, έχει πρόσβαση σε καταστήματα που αλλιώς θα ήταν απρόσιτα. Επίσης, δύο φίλες μπορούν να επισημοποιήσουν την αλληλοεμπιστοσύνη τους εμπιστεύοντας το ίδιο ποσό η μία στην άλλη. Μια μεγάλη εταιρεία που πραγματοποιεί συχνά συμβάσεις υπεργολαβίας με άλλες εταιρείες μπορεί να εκφράσει την εμπιστοσύνη της προς αυτές. Μια κυβέρνηση μπορεί να εμπιστευθεί άμεσα τις πολίτες της με χρήματα και να τις αντιμετωπίσει με ένα ανάλογο νομικό οπλοστάσιο αν αυτές κάνουν ανεύθυνη χρήση της εμπιστοσύνης αυτής. Μια τράπεζα μπορεί να προσφέρει δάνεια ως εξερχόμενες και να χειρίζεται τις καταθέσεις ως εισερχόμενες άμεσες εμπιστοσύνες. Τέλος, το δίκτυο μπορεί να ειδωθεί ως ένα πεδίο επένδυσης και κερδοσκοπίας αφού αποτελεί ένα εντελώς νέο πεδίο οικονομικής δραστηριότητας.

Είναι αξισημείωτο το ότι το ίδιο φυσικό πρόσωπο μπορεί να διατηρεί πολλαπλές ψευδώνυμες ταυτότητες στο ίδιο δίκτυο εμπιστοσύνης και ότι πολλά ανεξάρτητα δίκτυα εμπιστοσύνης διαφορετικών σκοπών μπορούν να συνυπάρχουν. Από την άλλη, η ίδια ψευδώνυμη ταυτότητα μπορεί να χρησιμοποιηθεί για να αναπτύξει σχέσεις εμπιστοσύνης σε διαφορετικά περιβάλλοντα.

2 Λειτουργία

Θα ακολουθήσουμε τώρα τα βήματα της *Alice* από τη σύνδεση με το δίκτυο μέχρι να ολοκληρώσει επιτυχώς μια αγορά. Ας υποθέσουμε ότι αρχικά όλα τα νομίσματά της, ας πούμε 10Ƀ, είναι αποθηκευμένα έτσι που αποκλειστικά εκείνη μπορεί να τα ξοδέψει.

Δύο αξιόπιστοι φίλοι, ο *Bob* και ο *Charlie*, την πείθουν να δοκιμάσει το Trust Is Risk. Εγκαθιστά το πορτοφόλι Trust Is Risk και μεταφέρει τα 10Ƀ από το κανονικό bitcoin πορτοφόλι της, εμπιστεύοντας 2Ƀ στον *Bob* και 5Ƀ στον *Charlie*. Τώρα ελέγχει αποκλειστικά 3Ƀ και διακινδυνεύει 7Ƀ με αντάλλαγμα το να είναι μέρος του δικτύου. Έχει πλήρη αλλά όχι αποκλειστική πρόσβαση στα 7Ƀ που εμπιστεύθηκε στους φίλους της και αποκλειστική πρόσβαση στα υπόλοιπα 3Ƀ, που αθροίζονται στα 10Ƀ.

Μερικές ημέρες αργότερα, ανακαλύπτει ένα διαδικτυακό κατάστημα παπουτσιών του *Dean*, ο οποίος είναι συνδεδεμένος επίσης στο Trust Is Risk. Η *Alice* βρίσκει ένα ζευγάρι παπούτσια που κοστίζει 1Ƀ και ελέγχει την αξιοπιστία του *Dean* μέσω του νέου της πορτοφολιού. Ας υποθέσουμε ότι ο *Dean* προκύπτει αξιόπιστος μέχρι 5Ƀ. Αφού το 1Ƀ είναι λιγότερο από τα 5Ƀ, η *Alice* πραγματοποιεί την αγορά μέσω του καινούριου της πορτοφολιού με σιγουριά.

Τότε βλέπει στο πορτοφόλι της ότι τα αποκλειστικά της νομίσματα παρέμειναν στα 3Ƀ, τα νομίσματα που εμπιστεύεται στον *Charlie* μειώθηκαν στα 4Ƀ και ότι εμπιστεύεται τον *Dean* με 1Ƀ, όσο και η αξία των παπουτσιών. Επίσης, η αγορά της είναι σημειωμένη ως "σε εξέλιξη". Αν η *Alice* ελέγξει την έμμεση εμπιστοσύνη της προς τον *Dean*, θα είναι και πάλι 4Ƀ. Στο παρασκήνιο, το πορτοφόλι της ανακατένειμε τα νομίσματα που εμπιστευόταν με τρόπο ώστε εκείνη να εμπιστεύεται άμεσα στον *Dean* τόσα νομίσματα όσο κοστίζει το αγορασμένο προϊόν και η εμπιστοσύνη που εμφανίζει το πορτοφόλι να είναι ίση με την αρχική.

Τελικά όλα πάνε καλά και τα παπούτσια φτάνουν στην *Alice*. Ο *Dean* επιλέγει να εξαργυρώσει τα νομίσματα που του εμπιστεύθηκε η *Alice* κι έτσι το πορτοφόλι της δε δείχνει ότι εμπιστεύεται κανένα νόμισμα στον *Dean*. Μέσω του πορτοφολιού της, σημειώνει την αγορά ως επιτυχή. Αυτό επιτρέπει στο σύστημα να αναπληρώσει τη μειωμένη εμπιστοσύνη προς τον *Charlie*, θέτοντας τα νομίσματα άμεσης εμπιστοσύνης στα 5Ƀ και πάλι. Η *Alice* τώρα ελέγχει αποκλειστικά 2Ƀ. Συνεπώς τώρα μπορεί να χρησιμοποιήσει συνολικά 9Ƀ, γεγονός αναμενόμενο, αφού έπρεπε να πληρώσει 1Ƀ για τα παπούτσια.

3 Ο γράφος εμπιστοσύνης

Ας ξεκινήσουμε μια αυστηρή περιγραφή του προτεινόμενου συστήματος, συνοδευόμενη από βοηθητικά παραδείγματα.

Ορισμός 1 (Γράφος). *Το Trust Is Risk αναπαρίσταται από μια ακολουθία κατευθυνόμενων γράφων με βάρη* $(\mathcal{G}_j)$ *όπου* $\mathcal{G}_j = (\mathcal{V}_j, \mathcal{E}_j), j \in \mathbb{N}$. *Επίσης, αφού οι γράφοι έχουν βάρη, υπάρχει μία ακολουθία συναρτήσεων βάρους* (c_j) *με* $c_j : \mathcal{E}_j \to \mathbb{R}^+$.

Οι κόμβοι αναπαριστούν τις παίκτες, οι ακμές αναπαριστούν τις υπάρχουσες άμεσες εμπιστοσύνες και τα βάρη το ποσό αξίας συνδεδεμένης με την αντίστοιχη άμεση εμπιστοσύνη. Όπως θα δούμε, το παιχνίδι εξελίσσεται σε γύρους. Ο δείκτης του γράφου αναπαριστά τον αντίστοιχο γύρο.

Ορισμός 2 (Παίκτες). *Το σύνολο* $\mathcal{V}_j = \mathcal{V}(\mathcal{G}_j)$ *είναι το σύνολο όλων των παικτών στο δίκτυο. Το σύνολο αυτό μπορεί να ειδωθεί ως το σύνολο όλων των ψευδώνυμων ταυτοτήτων.*

Κάθε κόμβος έχει έναν αντίστοιχο μη αρνητικό αριθμό που αναπαριστά το κεφάλαιό του. Το κεφάλαιο ενός κόμβου είναι η συνολική αξία που ο κόμβος κατέχει αποκλειστικά και κανείς άλλος δεν μπορεί να ξοδέψει.

Ορισμός 3 (Κεφάλαιο). *Το κεφάλαιο της* A *στο γύρο* j, $Cap_{A,j}$, *ορίζεται ως τα συνολικά νομίσματα που ανήκουν αποκλειστικά στην* A *στην αρχή του γύρου* j.

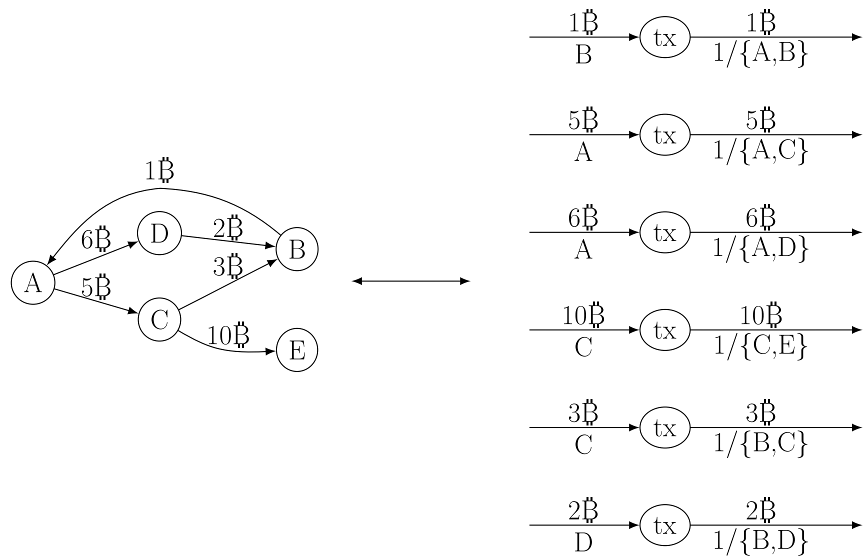
Το κεφάλαιο είναι η αξία που υπάρχει στο παιχνίδι αλλά δεν είναι μοιραζόμενη με έμπιστες τρίτες. Το κεφάλαιο μίας παίκτη μπορεί να ανακατανεμηθεί μόνο κατά τη διάρκεια των γύρων της, σύμφωνα με τις πράξεις της. Μοντελοποιούμε το σύστημα με τέτοιο τρόπο ώστε να είναι αδύνατο να προστεθεί κεφάλαιο στην πορεία του παιχνιδιού με εξωτερικά μέσα. Η χρήση του κεφαλαίου θα ξεκαθαρίσει μόλις οι γύροι ορισθούν με ακρίβεια.

Ο ορισμός της άμεσης εμπιστοσύνης ακολουθεί:

Ορισμός 4 (Άμεση Εμπιστοσύνη). *Η άμεση εμπιστοσύνη από την* A *στη* B *στο τέλος του γύρου* j, $DTr_{A\to B,j}$, *ορίζεται ως το συνολικό ποσό αξίας που υπάρχει σε* $1/\{A,B\}$ *multisigs στο UTXO στο τέλος του γύρου* j, *όπου τα χρήματα έχουν κατατεθεί από την* A.

$$DTr_{A\to B,j} = \begin{cases} c_j(A,B), & \alpha\nu\ (A,B) \in \mathcal{E}_j \\ 0, & \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases} \tag{1}$$

Ο ορισμός αυτός συμφωνεί με τον τίτλο του παρόντος κειμένου και συμπίπτει με τη διαίσθηση και τα κοινωνιολογικά πειραματικά αποτελέσματα του [4] ότι η εμπιστοσύνη που η *Alice* δείχνει στον *Bob* σε κοινωνικά δίκτυα του φυσικού κόσμου αντιστοιχεί με την έκταση του κινδύνου στην οποία η *Alice* τοποθετεί τον εαυτό της με σκοπό να βοηθήσει τον *Bob*. Ένας γράφος παράδειγμα με τις αντίστοιχες συναλλαγές στο UTXO φαίνεται παρακάτω.



Σχ. 3: Ο Γράφος του Trust Is Risk το αντίστοιχο Bitcoin UTXO

Όποιος αλγόριθμος έχει πρόσβαση στο γράφο $\mathcal{G}_j$ έχει επίσης πρόσβαση σε όλες της άμεσες εμπιστοσύνες του γράφου αυτού.

Ορισμός 5 (Γειτονιά). *Χρησιμοποιούμε το συμβολισμό* $N^+(A)_j$ *για να αναφερθούμε σε κόμβους που η* A *εμπιστεύεται άμεσα και* $N^-(A)_j$ *για τους κόμβους που εμπιστεύονται άμεσα την* A *στο τέλος του γύρου* j.

$$\begin{aligned} N^+(A)_j &= \{B \in \mathcal{V}_j : DTr_{A\to B,j} > 0\} \\ N^-(A)_j &= \{B \in \mathcal{V}_j : DTr_{B\to A,j} > 0\} \end{aligned} \tag{2}$$

Αυτές καλούνται έξω και μέσα γειτονιές της A *στο γύρο* j *αντίστοιχα.*

Ορισμός 6 (Ολική Εισερχόμενη/Εξερχόμενη Άμεση Εμπιστοσύνη). *Χρησιμοποιούμε το συμβολισμό* $in_{A,j}, out_{A,j}$ *για να αναφερθούμε στη συνολική εισερχόμενη και εξερχόμενη άμεση εμπιστοσύνη αντίστοιχα.*

$$in_{A,j} = \sum_{v \in N^-(A)_j} DTr_{v\to A,j} \quad , \qquad out_{A,j} = \sum_{v\in N^+(A)_j} DTr_{A\to v,j} \tag{3}$$

Ορισμός 7 (Περιουσία). *Το άθροισμα του κεφαλαίου και της εξερχόμενης άμεσης εμπιστοσύνης της* A.

$$As_{A,j} = Cap_{A,j} + out_{A,j} \tag{4}$$

4 Η Εξέλιξη της Εμπιστοσύνης

Ορισμός 8 (Γύροι). *Σε κάθε γύρο* j *μία παίκτης* $A \in \mathcal{V}, A = Player(j)$, *επιλέγει μία ή περισσότερες πράξεις εκ των δύο ακόλουθων κατηγοριών:*
Steal(y_B, B***)***: *Να κλέψει αξία* y_B *από τη* $B \in N^-(A)_{j-1}$, *όπου* $0 \leq y_B \leq DTr_{B \to A, j-1}$. *Τότε:*

$$DTr_{B \to A, j} = DTr_{B \to A, j-1} - y_B$$

Add(y_B, B***)***: *Να προσθέσει αξία* y_B *στη* $B \in \mathcal{V}$, *όπου* $-DTr_{A \to B, j-1} \leq y_B$. *Τότε:*

$$DTr_{A \to B, j} = DTr_{A \to B, j-1} + y_B$$

Όταν $y_B < 0$, *θα λέμε ότι η* A *μειώνει την άμεση εμπιστοσύνη του προς την* B *κατά* $-y_B$. *Όταν* $y_B > 0$, *θα λέμε ότι η* A *αυξάνει την άμεση εμπιστοσύνη της προς τη* B *κατά* y_B. *Αν* $DTr_{A \to B, j-1} = 0$, *τότε λέμε ότι η* A *αρχίζει να εμπιστεύεται άμεσα τη* B. *Η* A *επιλέγει "πάσο" αν δεν επιλέξει καμία πράξη. Επίσης, έστω* Y_{st}, Y_{add} *η συνολική αξία που πρόκειται να κλαπεί και να προστεθεί αντίστοιχα από την* A *στο γύρο της* j. *Για να είναι ένας γύρος δυνατός, θα πρέπει*

$$Y_{add} - Y_{st} \leq Cap_{A,j-1} \ . \tag{5}$$

Το κεφάλαιο ανανεώνεται σε κάθε γύρο: $Cap_{A,j} = Cap_{A,j-1} + Y_{st} - Y_{add}$.

Μία παίκτης δεν μπορεί να επιλέξει δύο πράξεις της ίδιας κατηγορίας προς την ίδια παίκτη σε ένα γύρο. Το σύνολο πράξεων το γύρο j *συμβολίζεται* $Turn_j$. *Ο γράφος που προκύπτει εφαρμόζοντας τις πράξεις στον* $\mathcal{G}_{j-1}$ *είναι ο* $\mathcal{G}_j$.

Για παράδειγμα, έστω $A = Player(j)$. Ένας έγκυρος γύρος μπορεί να είναι

$$Turn_j = \{Steal\,(x, B)\,, Add\,(y, C)\,, Add\,(w, D)\} \ .$$

Η πράξη $Steal$ απαιτεί $0 \leq x \leq DTr_{B \to A, j-1}$, οι πράξεις Add απαιτούν $DTr_{A \to C, j-1} \geq -y$ και $DTr_{A \to D, j-1} \geq -w$ και ο περιορισμός του κεφαλαίου $y + w - x \leq Cap_{A,j-1}$.

Χρησιμοποιούμε $prev\left(j\right)$ και $next\left(j\right)$ για να δηλώσουμε τον προηγούμενο και τον επόμενο γύρο που παίχθηκε αντίστοιχα από την $Player\left(j\right)$.

Ορισμός 9 (Προηγούμενος/Επόμενος Γύρος). *Έστω $j \in \mathbb{N}$ ένας γύρος με $Player\left(j\right) = A$. Ορίζουμε τα $prev\left(j\right), next\left(j\right)$ ως τον προηγούμενο και τον επόμενο γύρο που η A επιλέγεται να παίξει αντίστοιχα. Αν ο πρώτος γύρος που παίζει η A είναι ο j, είναι $prev\left(j\right) = 0$. Πιο αυστηρά, έστω*

$$\begin{aligned} P &= \left\{k \in \mathbb{N} : k < j \wedge Player\left(k\right) = A\right\} \text{ και} \\ N &= \left\{k \in \mathbb{N} : k > j \wedge Player\left(k\right) = A\right\} \ . \end{aligned}$$

Τότε ορίζουμε $prev\left(j\right), next\left(j\right)$ ως εξής:

$$prev\left(j\right) = \begin{cases} \max P, & P \neq \emptyset \\ 0, & P = \emptyset \end{cases} \ , \ next\left(j\right) = \min N$$

Το $next\left(j\right)$ είναι πάντα καλώς ορισμένο με την παραδοχή ότι μετά από κάθε γύρο όλες οι παίκτες ξαναπαίζουν τελικά.

Ορισμός 10 (Ζημία). *Έστω j γύρος τέτοιος ώστε $Player\left(j\right) = A$.*

$$Damage_{A,j} = out_{A,prev(j)} - out_{A,j-1} \tag{6}$$

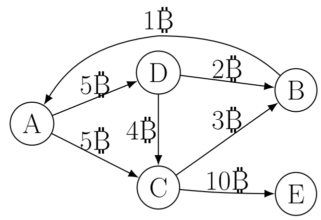
Λέμε ότι κλάπηκε από την A αξία $Damage_{A,j}$ ανάμεσα στον $prev\left(j\right)$ και στον j. Παραλείπουμε τους δείκτες γύρων όταν εννοούνται από τα συμφραζόμενα.

Ορισμός 11 (Ιστορία). *Ορίζουμε την Ιστορία, $\mathcal{H} = \left(\mathcal{H}_j\right)$, ως την ακολουθία όλων των διατεταγμένων ζευγών που περιέχουν τα σύνολα κινήσεων και την αντίστοιχη παίκτη.*

$$\mathcal{H}_j = \left(Player\left(j\right), Turn_j\right) \tag{7}$$

Γνώση του αρχικού γράφου $\mathcal{G}_0$, των αρχικών κεφαλαίων όλων των παικτών και της ιστορίας ισοδυναμούν με πλήρη κατανόηση της εξέλιξης του παιχνιδιού. Χτίζοντας στο παράδειγμα του σχήματος 3, μπορούμε να δούμε το γράφο που προκύπτει όταν η D παίζει

$$Turn_1 = \left\{Steal\left(1, A\right), Add\left(4, C\right)\right\} \ . \tag{8}$$



Σχ. 4: Ο Γράφος του Παιχνιδιού μετά τον $Turn_1$ (8) στο γράφο του Σχ. 3

Το Trust Is Risk ελέγχεται από έναν αλγόριθμο που επιλέγει μία παίκτη, λαμβάνει το γύρο που η παίκτης αυτή επιθυμεί να παίξει και, αν ο γύρος της είναι έγκυρος, τον εκτελεί. Αυτά τα βήματα επαναλαμβάνονται επ΄ αόριστον. Θεωρούμε ότι οι παίκτες επιλέγονται με τέτοιο τρόπο που μία παίκτης, μετά από τον γύρο της, τελικά θα ξαναπαίξει αργότερα.

`Trust Is Risk Game`

`j = 0`

`while (True)`

  `j += 1;` $A \xleftarrow{\$} \mathcal{V}_j$

  `Turn = strategy[`A`](`$\mathcal{G}_0$`, `A`, `$Cap_{A,0}$`, `$\mathcal{H}_{1\dots j-1}$`)`

  `(`$\mathcal{G}_j$`, `$Cap_{A,j}$`, `$\mathcal{H}_j$`) = executeTurn(`$\mathcal{G}_{j-1}$`, `A`, `$Cap_{A,j-1}$`, Turn)`

Η `strategy[`A`]()` προσφέρει στην παίκτη A πλήρη γνώση του παιχνιδιού, εκτός από τα κεφάλαια των άλλων παικτών. Αυτή η παραδοχή μπορεί να μην είναι πάντα ρεαλιστική.

Η `executeTurn()` ελέγχει την εγκυρότητα του γύρου `Turn` και τον αντικαθιστά με έναν κενό γύρο αν είναι άκυρος. Ακόλουθα, δημιουργεί ένα νέο γράφο $\mathcal{G}_j$ και ανανεώνει την ιστορία αναλόγως. Για τους αντίστοιχους ψευδοκώδικες, δείτε το Παράρτημα.

5 Μεταβατικότητα Εμπιστοσύνης

Στην ενότητα αυτή ορίζουμε μερικές στρατηγικές και δείχνουμε τους ανάλογους αλγορίθμους. Μετά ορίζουμε το Μεταβατικό Παιχνίδι (Transitive Game) που αναπαριστά το σενάριο χειρότερης περίπτωσης για μία τίμια παίκτη όταν κάποια άλλη παίκτης αποφασίζει να φύγει από το δίκτυο με τα χρήματά της και όλα τα χρήματα που άλλες εμπιστεύονται άμεσα σε αυτήν.

Ορισμός 12 (Αδρανής Στρατηγική (Idle Strategy)). *Μία παίκτης A ακολουθεί την αδρανή στρατηγική αν παίζει "πάσο" στο γύρο της.*

Idle Strategy
Input : graph $\mathcal{G}_0$, player A, capital $Cap_{A,0}$, history $(\mathcal{H})_{1\ldots j-1}$
Output : $Turn_j$

`idleStrategy(`$\mathcal{G}_0$, A, $Cap_{A,0}$, $\mathcal{H}$`) :`
  `return(`$\emptyset$`)`

Οι είσοδοι και οι έξοδοι είναι πανομοιότυποι με αυτούς της `idleStrategy()` στις υπόλοιπες στρατηγικές, συνεπώς αποφεύγουμε την επανάληψή τους.

Ορισμός 13 (Κακιά Στρατηγική). *Μία παίκτης A ακολουθεί την κακιά στρατηγική αν στο γύρο της κλέβει όλη την εισερχόμενη άμεση εμπιστοσύνη και μηδενίζει όλη την εξερχόμενη άμεση εμπιστοσύνη.*

`evilStrategy(`$\mathcal{G}_0$, A, $Cap_{A,0}$, $\mathcal{H}$`) :`
  `Steals =` $\bigcup_{v \in N^-(A)_{j-1}} \{Steal(DTr_{v \to A,j-1}, v)\}$
  `Adds =` $\bigcup_{v \in N^+(A)_{j-1}} \{Add(-DTr_{A \to v,j-1}, v)\}$
  $Turn_j$ `=` `Steals` $\cup$ `Adds`
  `return(`$Turn_j$`)`

Ορισμός 14 (Συντηρητική Στρατηγική). *Μία παίκτης A ακολουθεί τη συντηρητική στρατηγική αν αναπληρώνει την αξία που έχασε από τον προηγούμενο γύρο, $Damage_A$, κλέβοντας από άλλες που την εμπιστεύονται άμεσα τόσο όσο μπορεί μέχρι την τιμή $Damage_A$ και δεν εκτελεί άλλη πράξη.*

`consStrategy(`$\mathcal{G}_0$, A, $Cap_{A,0}$, $\mathcal{H}$`) :`
  `Damage =` $out_{A,prev(j)}$ `-` $out_{A,j-1}$
  `if (Damage > 0)`
    `if (Damage >=` $in_{A,j-1}$`)`
      $Turn_j$ `=` $\bigcup_{v \in N^-(A)_{j-1}} \{Steal\left(DTr_{v \to A,j-1}, v\right)\}$
    `else`
      y `= SelectSteal(`G_j, A, `Damage) #`y `=` $\{y_v : v \in N^-\left(A\right)_{j-1}\}$
      $Turn_j$ `=` $\bigcup_{v \in N^-(A)_{j-1}} \{Steal\left(y_v, v\right)\}$
  `else` $Turn_j$ `=` $\emptyset$
  `return(`$Turn_j$`)`

Η `SelectSteal()` επιστρέφει y_v με $v \in N^-\left(A\right)_{j-1}$ τέτοιο ώστε

$$\sum_{v \in N^-(A)_{j-1}} y_v = Damage_{A,j} \land \forall v \in N^-\left(A\right)_{j-1}, y_v \leq DTr_{v \to A,j-1} \ . \quad (9)$$

Η παίκτης A μπορεί να ορίσει κατά βούληση πώς η `SelectSteal()` θα κατανείμει τις πράξεις $Steal\,()$ κάθε φορά που καλεί τη συνάρτηση, εφ' όσον ο περιορισμός (9) είναι σεβαστός.

Όπως βλέπουμε, ο ορισμός καλύπτει μια πληθώρα επιλογών για τη συντηρητική παίκτη, αφού στην περίπτωση που $0 < Damage_{A,j} < in_{A,j-1}$ μπορεί να επιλέξει να κατανείμει τις πράξεις $Steal\,()$ όπως επιθυμεί.

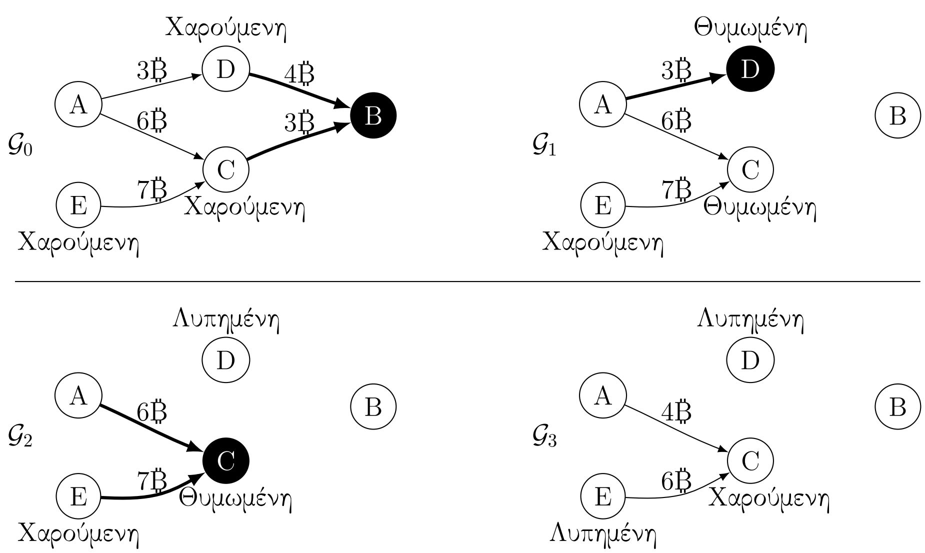
Ο συλλογισμός πίσω από αυτή τη στρατηγική προκύπτει από μια συνηθισμένη περίπτωση στον πραγματικό κόσμο. Έστω μία πελάτισσα, μία μεσάζοντας κι μία παραγωγός. Η πελάτισσα εμπιστεύεται κάποια αξία στη μεσάζοντα ώστε η τελευταία να μπορέσει να αγοράσει το επιθυμητό προϊόν από την παραγωγό και να το παραδώσει στην πελάτισσα. Η μεσάζοντας με τη σειρά της εμπιστεύεται ίση αξία στην παραγωγό, η οποία απαιτεί την προκαταβολή του ποσού για να μπορέσει να ολοκληρώσει τη διαδικασία παραγωγής. Ωστόσο, η παραγωγός τελικά δε δίνει το προϊόν ούτε επιστρέφει το ποσό λόγω πτώχευσης ή επιλογής να φύγει από την αγορά με ένα άδικο όφελος. Η μεσάζοντας τότε μπορεί να επιλέξει είτε να αποζημιώσει την πελάτισσα και να υποστεί τη ζημία, ή να αρνηθεί την αποζημίωση και να χάσει την εμπιστοσύνη της πελάτισσας. Η τελευταία επιλογή για τη μεσάζοντα είναι ακριβώς η συντηρητική στρατηγική. Χρησιμοποιείται στη συνέχεια του παρόντος ως η στρατηγική για όλες τις ενδιάμεσες παίκτες γιατί μοντελοποιεί με επιτυχία το σενάριο χειρότερης περίπτωσης που μία πελάτισσα μπορεί να αντιμετωπίσει αφού μία κακιά παίκτης αποφασίσει να κλέψει ό,τι μπορεί και οι υπόλοιπες παίκτες δεν εμπλέκονται σε κακή δράση.

Συνεχίζουμε με μία δυνατή εξέλιξη του παιχνιδιού, το Μεταβατικό Παιχνίδι. Στο γύρο 0, υπάρχει ήδη ένα συγκεκριμένο δίκτυο. Όλες οι παίκτες εκτός της A και της B ακολουθούν τη συντηρητική στρατηγική. Επιπλέον, το σύνολο των παικτών δε μεταβάλλεται κατά τη διάρκεια του Μεταβατικού Παιχνιδιού, συνεπώς μπορούμε να αναφερθούμε στο $\mathcal{V}_j$ για κάθε γύρο j ως $\mathcal{V}$. Επίσης, κάθε συντηρητική παίκτης μπορεί να βρίσκεται σε μία από τρεις καταστάσεις: Χαρούμενη (Happy), Θυμωμένη (Angry) ή Λυπημένη (Sad). Οι Χαρούμενες παίκτες έχουν ζημία 0, οι Θυμωμένες παίκτες έχουν θετική ζημία και θετική εισερχόμενη άμεση εμπιστοσύνη, άρα μπορούν να αναπληρώσουν τη ζημία τους τουλάχιστον μερικώς και οι Λυπημένες παίκτες έχουν θετική ζημία, αλλά 0 εισερχόμενη άμεση εμπιστοσύνη, άρα δεν μπορούν να αναπληρώσουν τη ζημία. Αυτές οι συμβάσεις θα ισχύουν όποτε χρησιμοποιούμε το Μεταβατικό Παιχνίδι.

```
Transitive Game
Input : graph G_0, A ∈ V idle player, B ∈ V evil player
Angry = Sad = ∅ ; Happy = V \ {A, B}
for (v ∈ V \ {B}) Loss_v = 0
```

```
j = 0
while (True)
  j += 1; v ←$ 𝒱 \ {A}
  Turn_j = strategy[v](𝒢_0, v, Cap_{v,0}, mathcalH_{1...j−1})
  executeTurn(𝒢_{j−1}, v, Cap_{v,j−1}, Turn_j)
  for (action ∈ Turn_j)
    action match do
      case Steal(y, w) do
        exchange = y
        Loss_w += exchange
        if (v != B) Loss_v -= exchange
        if (w != A)
          Happy = Happy \ {w}
          if (in_{w,j} == 0) Sad = Sad ∪ {w}
          else Angry = Angry ∪ {w}
  if (v != B)
    Angry = Angry \ {v}
    if (Loss_v > 0)  Sad = Sad ∪ {v}       #in_{v,j} should be zero
    if (Loss_v == 0) Happy = Happy ∪ {v}
```

Ένα παράδειγμα εκτέλεσης ακολουθεί:



Σχ. 5: Η B κλέβει 7Ƀ, μετά η D κλέβει 3Ƀ και η C κλέβει 3Ƀ

Έστω j_0 ο πρώτος γύρος στον οποίο η B επιλέγεται. Μέχρι τότε, όλες οι παίκτες θα παίζουν "πάσο" αφού τίποτα δεν έχει κλαπεί ακόμα (βλέπε το

Παράρτημα (Θεώρημα 6) για μια αυστηρή απόδειξη αυτού του απλού γεγονότος). Επιπλέον, έστω $v = Player(j)$ και $j' = prev\,(j)$. Το Μεταβατικό Παιχνίδι παράγει γύρους:

$$Turn_j = \bigcup_{w \in N^-(v)_{j-1}} \{Steal\,(y_w, w)\}\ , \tag{10}$$

όπου

$$\sum_{w \in N^-(v)_{j-1}} y_w = \min\left(in_{v,j-1}, Damage_{v,j}\right)\ .$$

Βλέπουμε ότι αν $Damage_{v,j} = 0$, τότε $Turn_j = \emptyset$.

Από τον ορισμό του $Damage_{v,j}$ και γνωρίζοντας ότι καμία στρατηγική σε αυτή την περίπτωση δεν μπορεί να αυξήσει καμία άμεση εμπιστοσύνη, βλέπουμε ότι $Damage_{v,j} \geq 0$. Επίσης, είναι $Loss_{v,j} \geq 0$ γιατί αν $Loss_{v,j} < 0$, τότε η v θα είχε κλέψει περισσότερη αξία απ' ότι της έχει κλαπεί, συνεπώς δε θα ακολουθούσε τη συντηρητική στρατηγική.

6 Ροή Εμπιστοσύνης

Μπορούμε τώρα να ορίσουμε την έμμεση εμπιστοσύνη από την A στη B.

Ορισμός 15 (Έμμεση Εμπιστοσύνη). *Η έμμεση εμπιστοσύνη από την A στη B μετά το γύρο j ορίζεται ως η μέγιστη δυνατή αξία που μπορεί να κλαπεί από την A μετά το γύρο j στο* `TransitiveGame(`$\mathcal{G}_j$`,`A`,`B`)`.

Είναι $Tr_{A\rightarrow B} \geq DTr_{A\rightarrow B}$. Το επόμενο θεώρημα δείχνει ότι η $Tr_{A\rightarrow B}$ είναι πεπερασμένη.

Θεώρημα 1 (Θεώρημα Σύγκλισης Εμπιστοσύνης).
Έστω ένα Μεταβατικό Παιχνίδι. Υπάρχει γύρος τέτοιος ώστε όλοι οι επόμενοι γύροι να είναι κενοί.

Διάγραμμα Απόδειξης. Αν το παιχνίδι δεν συνέκλινε, οι πράξεις $Steal\,()$ θα συνέχιζαν για πάντα χωρίς μείωση του συνολικού κλεμμένου ποσού σε βάθος χρόνου, συνεπώς το ποσό αυτό θα απειριζόταν. Αυτό ωστόσο είναι αδύνατο, αφού υπάρχει μόνο πεπερασμένη συνολική άμεση εμπιστοσύνη. □

Πλήρεις αποδείξεις όλων των θεωρημάτων και λημμάτων υπάρχουν στο Παράρτημα.

Στην περίπτωση ενός `TransitiveGame(`$\mathcal{G}$`,`A`,`B`)`, χρησιμοποιούμε το συμβολισμό $Loss_A = Loss_{A,j}$, όπου j είναι ένας γύρος στον οποίο το παιχνίδι έχει συγκλίνει. Είναι σημαντικό να σημειώσουμε ότι η $Loss_A$ δεν είναι η ίδια για επανειλημμένες εκτελέσεις αυτού του είδους παιχνιδιού, αφού η σειρά με την οποία επιλέγονται οι παίκτες μπορεί να διαφέρει ανάμεσα σε εκτελέσεις και οι συντηρητικές παίκτες έχουν το περιθώριο να επιλέξουν ποιες εισερχόμενες άμεσες εμπιστοσύνες θα κλέψουν και πόσο από την καθεμία.

Έστω ένας κατευθυνόμενος γράφος με βάρη G. Θα μελετήσουμε τη μέγιστη ροή στο γράφο αυτό. Για μία εισαγωγή στο πρόβλημα μέγιστης ροής βλέπε [5] σελ. 708. Θεωρώντας το βάρος κάθε ακμής ως τη χωρητικότητά της, μία απόδοση ροής $X = [x_{vw}]_{\mathcal{V}\times\mathcal{V}}$ με πηγή A και καταβόθρα B είναι έγκυρη όταν:

$$\forall (v, w) \in \mathcal{E}, x_{vw} \leq c_{vw} \text{ και} \tag{11}$$

$$\forall v \in \mathcal{V} \setminus \{A, B\}, \sum_{w \in N^+(v)} x_{wv} = \sum_{w \in N^-(v)} x_{vw} \ . \tag{12}$$

Δεν υποθέτουμε συμμετρία κατεύθυνσης στην απόδοση X. Η τιμή ροής είναι $\sum\limits_{v \in N^+(A)} x_{Av}$, η οποία προκύπτει ίση με $\sum\limits_{v \in N^-(B)} x_{vB}$. Υπάρχει αλγόριθμος που επιστρέφει τη μέγιστη δυνατή ροή από την A στη B, γνωστός ως $MaxFlow\,(A, B)$. Αυτός ο αλγόριθμος χρειάζεται πλήρη γνώση του γράφου. Η γρηγορότερη εκδοχή του έχει χρονική πολυπλοκότητα $O\,(|\mathcal{V}||\mathcal{E}|)$ [6]. Η τιμή ροής του $MaxFlow\,(A, B)$ συμβολίζεται $maxFlow\,(A, B)$.

Θα εισάγουμε τώρα δύο λήμματα που θα χρησιμοποιηθούν για την απόδειξη ενός από τα κεντρικά αποτελέσματα αυτής της εργασίας, το θεώρημα Εμπιστοσύνης – Ροής.

Λήμμα 1 (Οι Μέγιστες Ροές είναι Μεταβατικά Παιχνίδια). *Έστω $\mathcal{G}$ γράφος παιχνιδιού, $A, B \in \mathcal{V}$ και $MaxFlow\,(A, B)$ η μέγιστη ροή από την A στη B εκτελεσμένη στον $\mathcal{G}$. Τότε υπάρχει εκτέλεση του `TransitiveGame(`$\mathcal{G}, A, B$`)` τέτοια ώστε $maxFlow\,(A, B) \leq Loss_A$.*

Διάγραμμα Απόδειξης. Η επιθυμητή εκτέλεση του `TransitiveGame()` θα περιέχει όλες τις ροές από την $MaxFlow\,(A, B)$ ως ισοδύναμες πράξεις $Steal\,()$. Οι παίκτες θα παίζουν η μία μετά την άλλη, από την B προς την A. Κάθε παίκτης θα κλέψει από τις προκατόχους της τόσο όσο κλάπηκε από αυτή. Οι ροές και η συντηρητική στρατηγική μοιράζονται την ιδιότητα ότι η συνολική είσοδος είναι ίση με τη συνολική έξοδο. □

Λήμμα 2 (Τα Μεταβατικά Παιχνίδια είναι Μέγιστες Ροές). *Έστω $\mathcal{H} =$`TransitiveGame(`$\mathcal{G}, A, B$`)` για κάποιο γράφο $\mathcal{G}$ και $A, B \in \mathcal{V}$. Υπάρχει έγκυρη ροή $X = \{x_{wv}\}_{\mathcal{V}\times\mathcal{V}}$ στον $\mathcal{G}_0$ τέτοια ώστε $\sum\limits_{v \in \mathcal{V}} x_{Av} = Loss_A$.*

Διάγραμμα Απόδειξης. Αν αποκλείσουμε τις Λυπημένες παίκτες από το παιχνίδι, οι πράξεις $Steal\,()$ που απομένουν συνιστούν μία έγκυρη ροή από την A στη B. □

Θεώρημα 2 (Θεώρημα Εμπιστοσύνης – Ροής).
Έστω $\mathcal{G}$ ένας γράφος παιχνιδιού και $A, B \in \mathcal{V}$. Ισχύει ότι

$$Tr_{A \to B} = maxFlow\,(A, B) \enspace .$$

Απόδειξη. Από το Λήμμα 1 υπάρχει εκτέλεση του Μεταβατικού Παιχνιδιού τέτοια ώστε $Loss_A \geq maxFlow\,(A, B)$. Αφού η $Tr_{A \to B}$ είναι η μέγιστη ζημία που μπορεί να έχει υποστεί η A μετά τη σύγκλιση του Μεταβατικού Παιχνιδιού, βλέπουμε ότι

$$Tr_{A \to B} \geq maxFlow\,(A, B) \enspace . \tag{13}$$

Όμως κάποια εκτέλεση του Μετατβατικού Παιχνιδιού δίνει $Tr_{A \to B} = Loss_A$. Από το Λήμμα 2, αυτή η εκτέλεση αντιστοιχεί σε μία ροή. Συνεπώς

$$Tr_{A \to B} \leq maxFlow\,(A, B) \enspace . \tag{14}$$

Το θεώρημα προκύπτει από το (13) και το (14). □

Ας σημειωθεί ότι η μέγιστη ροή είναι η ίδια στις ακόλουθες δύο περιπτώσεις: Αν μία παίκτης επιλέξει την κακιά στρατηγική και αν αυτή η παίκτης επιλέξει μία παραλλαγή της κακιάς στρατηγικής στην οποία δεν μηδενίζει την εξερχόμενη άμεση εμπιστοσύνη της.

Επιπλέον δικαιολόγηση της μεταβατικότητας της εμπιστοσύνης με χρήση της μέγιστης ροής μπορεί να βρεθεί στην κοινωνιολογική εργασία [4] όπου η άμεση αντιστοίχιση των μέγιστων ροών και της εμπειρικής εμπιστοσύνης επαληθεύεται πειραματικά.

Εδώ βλέπουμε ένα ακόμη σημαντικό θεώρημα που δίνει τη βάση για συναλλαγές αμετάβλητου κινδύνου μεταξύ διαφορετικών, πιθανώς αγνώστων, ατόμων.

Θεώρημα 3 (Θεώρημα Αμετάβλητου Κινδύνου). *Έστω $\mathcal{G}$ γράφος παιχνιδιού, $A, B \in \mathcal{V}$ και l η επιθυμητή αξία προς μεταφορά από την A στην B, με $l \leq Tr_{A \to B}$. Έστω επίσης $\mathcal{G}'$ με τους ίδιους κόμβους με τον $\mathcal{G}$ τέτοιος ώστε*

$$\forall v \in \mathcal{V}' \setminus \{A\}, \forall w \in \mathcal{V}', DTr'_{v \to w} = DTr_{v \to w} \enspace .$$

Επιπλέον, υποθέτουμε ότι υπάρχουν τιμές για τις εξερχόμενες άμεσες εμπιστοσύνες της A, $DTr'_{A \to v}$, τέτοιες ώστε

$$Tr'_{A \to B} = Tr_{A \to B} - l \enspace . \tag{15}$$

Έστω ένας άλλος γράφος παιχνιδιού, $\mathcal{G}''$, ταυτόσημος με τον $\mathcal{G}'$ εκτός της παρακάτω διαφοράς:

$$DTr''_{A\to B} = DTr'_{A\to B} + l \ .$$

Ισχύει τότε ότι

$$Tr''_{A\to B} = Tr_{A\to B} \ .$$

Απόδειξη. Οι δύο γράφοι $\mathcal{G}'$ και $\mathcal{G}''$ διαφέρουν μόνο στο βάρος της ακμής (A, B), το οποίο είναι μεγαλύτερο κατά l στον $\mathcal{G}''$. Συνεπώς οι δύο αλγόριθμοι $MaxFlow$ θα επιλέξουν την ίδια ροή, εκτός από την ακμή (A, B), όπου θα είναι $x''_{AB} = x'_{AB} + l$. □

Είναι διαισθητικά προφανές ότι η A μπορεί να μειώσει την εξερχόμενη άμεση εμπιστοσύνη με τρόπου που να επιτυγχάνει το (15), αφού το $maxFlow\,(A, B)$ είναι συνεχές ως προς τις εξερχόμενες άμεσες εμπιστοσύνες της A. Αφήνουμε αυτόν τον υπολογισμό ως μέρος μελλοντικής έρευνας.

7 Sybil Αντίσταση

Ένας από τους κεντρικούς στόχους αυτού του συστήματος είναι να περιορίσει τον κίνδυνο για επιθέσεις Sybil διατηρώντας ταυτόχρονα πλήρως αποκεντρωμένη αυτονομία.

Εδώ επεκτείνουμε τον ορισμό της έμμεσης εμπιστοσύνης σε πολλούς παίκτες.

Ορισμός 16 (Έμμεση Εμπιστοσύνη προς Πολλούς Παίκτες). *Η έμμεση εμπιστοσύνη από την παίκτη A σε ένα σύνολο παικτών, $S \subset \mathcal{V}$ ορίζεται ως η μέγιστη δυνατή αξία που μπορεί να κλαπεί από την A αν όλοι οι παίκτες στο S ακολουθούν την κακιά στρατηγική, η A ακολουθεί την αδρανή στρατηγική και όλοι οι υπόλοιποι ($\mathcal{V} \setminus (S \cup \{A\})$) ακολουθούν τη συντηρητική στρατηγική. Πιο αυστηρά, έστω $choices$ οι διαφορετικές δράσεις μεταξύ των οποίων μπορούν να επιλέξουν οι συντηρητικοί παίκτες. Τότε*

$$Tr_{A\to S,j} = \max_{j':j'>j, choices} \left[out_{A,j} - out_{A,j'}\right] \tag{16}$$

Τώρα επεκτείνουμε το θεώρημα Εμπιστοσύνης – Ροής (2) σε πολλούς παίκτες.

Θεώρημα 4 (Εμπιστοσύνη – Ροή Πολλών Παικτών).
Έστω $S \subset \mathcal{V}$ *και* T *βοηθητική παίκτης τέτοια ώστε* $\forall B \in S, DTr_{B \to T} = \infty$. *Ισχύει ότι*

$$\forall A \in \mathcal{V} \setminus S, Tr_{A \to S} = maxFlow\,(A, T) \quad .$$

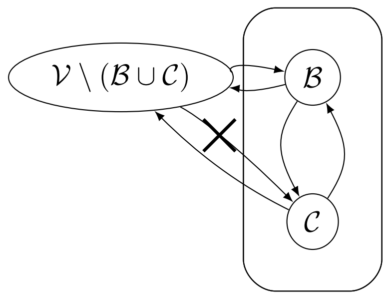
Απόδειξη. Αν η T επιλέξει την κακιά στρατηγική και όλες οι παίκτες στο S παίξουν σύμφωνα με τη συντηρητική στρατηγική, θα πρέπει να κλέψουν όλη την εισερχόμενη άμεση εμπιστοσύνη αφού έχουν υποστεί άπειρη ζημία, συνεπώς θα δράσουν ταυτόσημα με την κακιά στρατηγική όσον αφορά τον αλγόριθμο $MaxFlow$. Το θεώρημα προκύπτει συνεπώς από το θεώρημα Εμπιστοσύνης – Ροής. □

Ορίζουμε τώρα διάφορες χρήσιμες έννοιες για να αντιμετωπίσουμε το πρόβλημα των επιθέσεων Sybil. Έστω μία πιθανή επιτιθέμενη, η Eve.

Ορισμός 17 (Διεφθαρμένο Σύνολο). *Έστω* $\mathcal{G}$ *γράφος παιχνιδιού και η Eve έχει διαφθείρει ένα σύνολο παικτών* $\mathcal{B} \subset \mathcal{V}$*, έτσι που ελέγχει πλήρως τις εξερχόμενες άμεσες εμπιστοσύνες προς οποιαδήποτε παίκτη στο* $\mathcal{V}$ *και που μπορεί επίσης να κλέψει όλη την εισερχόμενη άμεση εμπιστοσύνη προς τις παίκτες στο* $\mathcal{B}$*. Αυτό αποκαλείται το διεφθαρμένο σύνολο. Θεωρούμε ότι οι παίκτες* $\mathcal{B}$ *ήταν νόμιμες πριν τη διαφθορά, συνεπώς μπορεί να έχουν άμεση εισερχόμενη εμπιστοσύνη από οποιαδήποτε παίκτη στο* $\mathcal{V}$*.*

Ορισμός 18 (Σύνολο Sybil). *Έστω* $\mathcal{G}$ *γράφος παιχνιδιού. Αφού η συμμετοχή στο δίκτυο δε χρειάζεται κανενός είδους εγγραφή, η Eve μπορεί να δημιουργήσει όσες παίκτες θέλει. Θα αποκαλούμε το σύνολο αυτών των παικτών* $\mathcal{C}$*, ή σύνολο Sybil. Επιπλέον, η Eve μπορεί να θέτει κατά βούληση τις άμεσες εμπιστοσύνες οποιασδήποτε παίκτη στο* $\mathcal{C}$ *προς οποιαδήποτε παίκτη και επίσης μπορεί να κλέψει όλη την εισερχόμενη άμεση εμπιστοσύνη προς παίκτες στο* $\mathcal{C}$*. Ωστόσο, μόνο οι παίκτες στο* $\mathcal{B} \cup \mathcal{C}$ *εμπιστεύονται άμεσα τους παίκτες στο* $\mathcal{C}$ *και όχι οι παίκτες στο* $\mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$*, όπου* $\mathcal{B}$ *είναι ένα σύνολο παικτών που η Eve έχει διαφθείρει.*

Ορισμός 19 (Συνεργασία). *Έστω* $\mathcal{G}$ *γράφος παιχνιδιού. Έστω* $\mathcal{B} \subset \mathcal{V}$ *ένα διεφθαρμένο σύνολο και* $\mathcal{C} \subset \mathcal{V}$ *ένα Sybil σύνολο, ελεγχόμενα και τα δύο από την Eve. Το διατεταγμένο ζεύγος* $(\mathcal{B}, \mathcal{C})$ *αποκαλείται συνεργασία και ελέγχεται εξ ολοκλήρου από μία μοναδική οντότητα στο φυσικό κόσμο. Από παιγνιοθεωρητική οπτική, οι παίκτες* $\mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$ *εκλαμβάνουν τη συνεργασία ως ανεξάρτητες παίκτες με διαφορετική στρατηγική η καθεμία, ενώ στην* *πραγματικότητα υπάγονται όλες σε μία μοναδική στρατηγική που ορίζεται από την οντότητα που ελέγχει, την Eve.*



Σχ. 6: Συνεργασία

Θεώρημα 5 (Sybil Αντίσταση).
Έστω $\mathcal{G}$ γράφος παιχνιδιού και $(\mathcal{B}, \mathcal{C})$ μια συνεργασία παικτών στον $\mathcal{G}$. Είναι

$$Tr_{A \to \mathcal{B} \cup \mathcal{C}} = Tr_{A \to \mathcal{B}} \ .$$

Διάγραμμα Απόδειξης. Η εισερχόμενη άμεση εμπιστοσύνη στη $\mathcal{B} \cup \mathcal{C}$ δεν μπορεί να είναι μεγαλύτερη από την εισερχόμενη άμεση εμπιστοσύνη στο $\mathcal{B}$ αφού το $\mathcal{C}$ δεν έχει εισερχόμενη άμεση εμπιστοσύνη από τους παίκτες στο $\mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$. □

Αποδείξαμε ότι ο έλεγχος του $|\mathcal{C}|$ δεν αφορά την Eve, συνεπώς οι επιθέσεις Sybil δεν έχουν νόημα. Σημειώνουμε ότι αυτό το θεώρημα δεν προσφέρει διαβεβαιώσεις ενάντια σε επιθέσεις που συμπεριλαμβάνουν τεχνικές εξαπάτησης. Πιο συγκεκριμένα, μία κακεντρεχής παίκτης μπορεί να δημιουργήσει πολλές ταυτότητες, να τις χρησιμοποιήσει με δίκαιο τρόπο ούτως ώστε να πείσει άλλες να καταθέσουν άμεση εμπιστοσύνη σε αυτές τις ταυτότητες και μετά να μεταβεί στην κακιά στρατηγική, εξαπατώντας έτσι όλες όσες εμπιστεύθηκαν τις κατασκευασμένες ταυτότητες. Αυτές οι ταυτότητες αντιστοιχούν στο διεφθαρμένο σύνολο παικτών και όχι στο σύνολο Sybil γιατί διαθέτουν εισερχόμενη άμεση εμπιστοσύνη από παίκτες έξω από τη συνεργασία.

Συμπερασματικά, έχουμε δημιουργήσει με επιτυχία ένα αποκεντρωμένο σύστημα οικονομικής εμπιστοσύνης με αντίσταση σε επιθέσεις Sybil και αμετάβλητο κίνδυνο για αγορές, όπως υποσχεθήκαμε.

8 Σχετικές Εργασίες

Το θέμα της εμπιστοσύνης έχει προσεγγιστεί επανειλημμένα από διάφορες οπτικές: Καθαρά κρυπτογραφική υποδομή στην οποία η εμπιστοσύνη είναι σχεδόν δυαδική και η μεταβατικότητα περιορίζεται σε ένα βήμα πέρα από άτομα που εμπιστεύεται κανείς ενεργητικά εξερευνάται στο PGP [7]. Ένας μεταβατικός ιστός εμπιστοσύνης για την αντιμετώπιση ανεπιθύμητης αλληλογραφίας μελετάται στο Freenet [8]. Άλλα συστήματα απαιτούν κεντρικούς αξιόπιστους τρίτους, όπως PKI βασιζόμενα σε αρχές πιστοποίησης [9] και το Bazaar [10], ή, στην περίπτωση της Βυζαντινής ανοχής στα σφάλματα, πιστοποιημένη συμμετοχή [11]. Ενώ άλλα συστήματα εμπιστοσύνης επιχειρούν να είναι αποκεντρωμένα, δεν αποδεικνύουν καμία ιδιότητα αντίστασης σε Sybil επιθέσεις και συνεπώς ίσως να δέχονται τέτοιες επιθέσεις. Τέτοια συστήματα είναι το FIRE [12], το CORE [13] και άλλα [14,15,16]. Άλλα συστήματα που ορίζουν την εμπιστοσύνη με έναν μη οικονομικό τρόπο είναι τα [17,18,19,20,21,22,23].

Συμφωνούμε με την εργασία [24] στο ότι η σημασία της εμπιστοσύνης δεν πρέπει να προεκτείνεται απρόσεκτα. Έχουμε υιοθετήσει τις συμβουλές τους στην παρούσα εργασία και παροτρύνουμε τον αναγνώστη να παραμένει στους ορισμούς της *άμεσης* και *έμμεσης* εμπιστοσύνης.

Η αγορά Beaver [25] περιλαμβάνει ένα μοντέλο εμπιστοσύνης που βασίζεται σε χρεώσεις για να αποθαρρύνει τις επιθέσεις Sybil. Επιλέξαμε να αποφύγουμε τις χρεώσεις στο σύστημά μας και να αντιμετωπίσουμε τις επιθέσεις Sybil με άλλο τρόπο. Η κινητήριος εφαρμογή για την έρευνα στο θέμα της εμπιστοσύνης σε ένα αποκεντρωμένο περιβάλλον είναι η αγορά OpenBazaar. Η μεταβατική οικονομική εμπιστοσύνη για το OpenBazaar έχει μελετηθεί παλαιότερα στο [26]. Η εργασία αυτή ωστόσο δεν ορίζει την εμπιστοσύνη σαν οικονομική αξία. Έχουμε εμπνευστεί ισχυρά από το [4] το οποίο δίνει μια κοινωνιολογική επιβεβαίωση για την κεντρική σχεδιαστική επιλογή της ταύτησης της εμπιστοσύνης με τον κίνδυνο. Εκτιμούμε ιδιαιτέρως την εργασία στο TrustDavis [27], το οποίο προτείνει ένα σύστημα οικονομικής εμπιστοσύνης που εμφανίζει μεταβατικές ιδιότητες και στο οποίο η εμπιστοσύνη ορίζεται ως πιστωτικές γραμμές, όμοια με το δικό μας σύστημα. Μπορέσαμε να επεκτείνουμε την εργασία τους χρησιμοποιώντας το blockchain για αυτόματες αποδείξεις κινδύνου, ένα εργαλείο που δεν είχαν στη διάθεσή τους τότε.

Η συντηρητική μας στρατηγική και το Μεταβατικό Παιχνίδι είναι πολύ παρόμοια με το μηχανισμό που προτείνεται στην οικονομική εργασία [28] η οποία επίσης περιγράφει μεταβατικότητα οικονομικής εμπιστοσύνης και χρησιμοποιείται από το Ripple [29] και το Stellar [30]. Τα IOU στις προαναφερθείσες εργασίες αντιστοιχούν σε ανεστραμμένες ακμές εμπιστοσύνης στο δικό μας σύστημα. Η κρίσιμη διαφορά είναι ότι η δική μας εμπιστοσύνη εκφράζεται με ένα ενιαίο νόμισμα και τα ότι τα νομίσματα πρέπει να προϋπάρχουν για να τα εμπιστευθεί κάποια σε κάποια άλλη, άρα δεν υπάρχει χρήμα ως χρέος. Επιπλέον, αποδεικνύουμε ότι η εμπιστοσύνη και οι μέγιστες ροές είναι ισοδύναμες, μία ανεξερεύνητη κατεύθυνση από τις εργασίες τους, παρ΄ όλο που πιστεύουμε ότι θα πρέπει να ισχύει και για τα δικά τους συστήματα.

9 Μελλοντική Έρευνα

Όταν η *Alice* πραγματοποιεί μία αγορά από τον *Bob*, η πρώτη πρέπει να μειώσει την εξερχόμενη άμεση εμπιστοσύνη της με τρόπο ώστε η προϋπόθεση (15) του θεωρήματος Αμετάβλητου Κινδύνου να ικανοποιείται. Το πώς η *Alice* μπορεί να επανυπολογίσει την εξερχόμενη άμεση εμπιστοσύνη της θα συζητηθεί σε μελλοντική εργασία.

Το παιχνίδι μας είναι στατικό. Σε ένα μελλοντικό δυναμικό περιβάλλον, οι χρήστες πρέπει να μπορούν να παίζουν ταυτόχρονα, να συνδέονται, να αποχωρούν ή να αποσυνδέονται προσωρινά από το δίκτυο. Άλλα είδη multisig, όπως 1-από-3, μπορούν να ερευνηθούν για την υλοποίηση άμεσης εμπιστοσύνης πολλών παικτών.

Ο αλγόριθμος MaxFlow χρειάζεται πλήρη γνώση του δικτύου, κάτι που μπορεί να οδηγήσει σε προβλήματα ιδιωτικότητας μέσω τεχνικών αποανωνυμοποίησης [31]. Ο υπολογισμός των ροών με μηδενική γνώση παραμένει ένα ανοιχτό ερώτημα. Το [32] και ο κεντροποιημένος προκάτοχός του, το PrivPay [33], φαίνεται να προσφέρουν ανεκτίμητες ιδέες ως προς το πώς μπορεί να επιτευχθεί η ιδιωτικότητα.

Η παιγνιοθεωρητική μας ανάλυση είναι απλή. Μία ενδιαφέρουσα ανάλυση θα περιλάμβανε τη μοντελοποίηση επαναλαμβανόμενων αγορών με τις σχετικές ανανεώσεις ακμών στο γράφο εμπιστοσύνης και την αντιμετώπιση της εμπιστοσύνης στο δίκτυο ως μέρος της συνάρτησης χρησιμότητας.

Η υλοποίηση του οικονομικού μας παιχνιδιού ως πορτοφόλι σε οποιοδήποτε blockchain θα ήταν ευπρόσδεκτη. Μία προσομοίωση ή πραγματική υλοποίηση του Trust Is Risk, σε συνδυασμό με μία ανάλυση των δυναμικών που προκύπτουν μπορεί να προσφέρουν ενδιαφέροντα πειραματικά αποτελέσματα. Στη συνέχεια, το δίκτυο εμπιστοσύνης μπορεί να χρησιμοποιηθεί σε άλλες εφαρμογές, όπως αποκεντρωμένα κοινωνικά δίκτυα [34].

10 Ευχαριστίες

Ευχαριστούμε θερμά το Διονύση Ζήνδρο, χωρίς τον οποίο η παρούσα εργασία δε θα ήταν δυνατή. Επίσης ευχαριστούμε τους καθηγητές Άρη Παγουρτζή, Δημήτρη Φωτάκη και Άγγελο Κιαγιά για την υποστήριξή τους και τις κατευθύνσεις που μας έδωσαν. Ευχαριστίες οφείλονται στο Εθνικό Μετσόβιο Πολυτεχνείο, το οποίο μας πρόσφερε τις απαραίτητες γνώσεις για την περάτωση της παρούσας εργασίας. Ο Κυριάκος Αξιώτης πρόσφερε απαραίτητη βοήθεια για την κατανόηση λεπτών σημείων σε σχέση με τις μέγιστες ροές και σχετικά θεωρήματα. Τέλος ευχαριστούμε θερμά την οικογένεια του συντάκτη για την υπομονή και την ένθερμη υποστήριξη που έδειξε κατά τη διάρκεια της έρευνας, τόσο σε συναισθηματικό όσο και σε πρακτικό επίπεδο.

Παράρτημα

1 Αποδείξεις, Λήμματα και Θεωρήματα

Λήμμα 3 (*Loss* ισοδύναμη με *Damage*).
Έστω ένα Μεταβατικό Παιχνίδι. Έστω $j \in \mathbb{N}$ και $v = Player\left(j\right)$ έτσι ώστε η v να ακολουθεί τη συντηρητική στρατηγική. Ισχύει ότι

$$\min\left(in_{v,j}, Loss_{v,j}\right) = \min\left(in_{v,j}, Damage_{v,j}\right) \quad .$$

Απόδειξη.
1η περίπτωση: Έστω $v \in Happy_{j-1}$. Τότε

1. $v \in Happy_j$ γιατί $Turn_j = \emptyset$,
2. $Loss_{v,j} = 0$ γιατί αλλιώς $v \notin Happy_j$,
3. $Damage_{v,j} = 0$, ειδάλλως οποιαδήποτε μείωση σε άμεση εμπιστοσύνη προς τη v θα αύξανε κατά ίσο ποσό τη $Loss_{v,j}$ (λινε 12), η οποία δεν μπορεί να μειωθεί ξανά παρά μόνο κατά τη διάρκεια του γύρου μιας Θυμωμένης παίκτη (γραμμή 13).
4. $in_{v,j} \geq 0$

Συνεπώς

$$\min\left(in_{v,j}, Loss_{v,j}\right) = \min\left(in_{v,j}, Damage_{v,j}\right) = 0 \quad .$$

2η περίπτωση: Έστω $v \in Sad_{j-1}$. Τότε

1. $v \in Sad_j$ γιατί $Turn_j = \emptyset$,
2. $in_{v,j} = 0$ (γραμμή 20),
3. $Damage_{v,j} \geq 0 \wedge Loss_{v,j} \geq 0$.

Συνεπώς

$$\min\left(in_{v,j}, Loss_{v,j}\right) = \min\left(in_{v,j}, Damage_{v,j}\right) = 0 \ .$$

Αν $v \in Angry_{j-1}$ τότε ισχύει το ίδιο επιχείρημα με τις περιπτώσεις 1 και 2 όταν $v \in Happy_j$ και $v \in Sad_j$ αντίστοιχα αν αγνοήσουμε το επιχείρημα (1). Συνεπώς το θεώρημα ισχύει σε κάθε περίπτωση. □

Απόδειξη του Θεωρήματος 1: Σύγκλιση Εμπιστοσύνης

Πρώτα απ΄ όλα, μετά το γύρο j_0 η κακιά παίκτης E θα παίζει πάντα "πάσο" γιατί έχει ήδη μηδενίσει την εισερχόμενη και εξερχόμενη εμπιστοσύνη στο γύρο j_0, η κακιά στρατηγική δεν περιέχει καμία περίπτωση κατά την οποία η άμεση εμπιστοσύνη να αυξάνεται ή κατά την οποία η κακιά παίκτης ξεκινά να εμπιστεύεται άμεσα κάποια άλλη παίκτη και οι άλλες παίκτες δεν ακολουθούν κάποια στρατηγική στην οποία να μπορούν να επιλέξουν την πράξη $Add\left(y, E\right)$. Το ίδιο ισχύει για την παίκτη A γιατί ακολουθεί την αδρανή στρατηγική. Όσον αφορά τους υπόλοιπους παίκτες, θεωρήστε το Μεταβατικό Παιχνίδι. Όπως βλέπουμε στις γραμμές 2 και 12 - 13, είναι

$$\forall j, \sum_{v \in \mathcal{V}_j} Loss_v = in_{E,j_0-1} \ .$$

Με άλλα λόγια, η συνολική ζημία είναι σταθερή και ίση με τη συνολική αξία που έκλεψε η E. Επίσης, όπως μπορούμε να δούμε στις γραμμές 1 και 20, οι οποίες είναι οι μόνες γραμμές όπου το σύνολο των Λυπημένων μεταβάλλεται, μόλις μία παίκτης μπει στο Λυπημένο σύνολο, είναι αδύνατο να βγει από αυτό. Επίσης βλέπουμε ότι οι παίκτες στα Λυπημένο και Χαρούμενο σύνολα πάντα παίζουν "πάσο". Θα δείξουμε τώρα ότι τελικά το σύνολο Θυμωμένων θα αδειάσει, ή ισοδύναμα ότι τελικά κάθε παίκτης θα παίζει "πάσο". Ας υποθέσουμε ότι είναι δυνατό να έχουμε άπειρους γύρους κατά τους οποίους οι παίκτες δεν επιλέγουν να παίξουν "πάσο". Γνωρίζουμε ότι ο αριθμός των κόμβων είναι πεπερασμένος, συνεπώς αυτό είναι δυνατό μόνο αν

$$\exists j' : \forall j \geq j', \left|Angry_j \cup Happy_j\right| = c > 0 \wedge Angry_j \neq \emptyset \ .$$

Ο ισχυρισμός αυτός είναι έγκυρος γιατί ο συνολικός αριθμός Θυμωμένων και Χαρούμενων παικτών δεν μπορεί να αυξηθεί γιατί καμία παίκτης δεν αποχωρεί από το σύνολο Λυπημένων και αν μειωνόταν, θα έφτανε τελικά το 0. Αφού $Angry_j \neq \emptyset$, κάποια παίκτης v που δε θα παίξει "πάσο" θα επιλεγεί τελικά για να παίξει. Σύμφωνα με το Μεταβατικό Παιχνίδι, η v είτε θα μηδενίσει την εισερχόμενη άμεση εμπιστοσύνη της και θα μπει στο σύνολο των Λυπημένων (γραμμή 20), το οποίο αντικρούεται στο $|Angry_j \cup Happy_j| = c$, ή θα κλέψει αρκετή αξία ώστε να μπει στο σύνολο Χαρούμενων, δηλαδή η v θα πετύχει $Loss_{v,j} = 0$. Ας υποθέσουμε ότι έχει κλέψει m παίκτες. Εκείνες, στο γύρο τους, θα κλέψουν συνολική αξία τουλάχιστον ίση με την αξία που κλάπηκε από την v (αφού δεν μπορούν να γίνουν Λυπημένες, όπως εξηγήθηκε νωρίτερα). Ωστόσο, αυτο σημαίνει ότι, αφού η συνολική αξία που κλέβεται δε θα μειωθεέι και οι γύροι που αυτό θα συμβεί είναι άπειροι, οι παίκτες πρέπει να κλέψουν ένα άπειρο ποσό αξίας, το οποίο είναι αδύνατο γιατί οι άμεσες εμπιστοσύνες είναι πεπερασμένες σε αριθμό και αξία. Πιο συγκεκριμένα, έστω j_1 ένας γύρος στον οποίο επιλέγεται ένας συντηρητικός παίκτης και

$$\forall j \in \mathbb{N}, DTr_j = \sum_{w,w' \in \mathcal{V}} DTr_{w \to w',j} \enspace .$$

Επίσης, χωρίς βλάβη της γενικότητας, υποθέτουμε ότι

$$\forall j \geq j_1, out_{A,j} = out_{A,j_1} \enspace .$$

Στο γύρο j_1, η v κλέβει

$$St = \sum_{i=1}^{m} y_i \enspace .$$

Θα δείξουμε με χρήση επαγωγής ότι

$$\forall n \in \mathbb{N}, \exists j_n \in \mathbb{N} : DTr_{j_n} \leq DTr_{j_1 - 1} - nSt \enspace .$$

Επαγωγική βάση: Ισχύει ότι

$$DTr_{j_1} = DTr_{j_1 - 1} - St \enspace .$$

Τελικά υπάρχει γύρος j_2 που κάθε παίκτης στο $N^-(v)_{j-1}$ θα έχει παίξει. Τότε ισχύει ότι

$$DTr_{j_2} \leq DTr_{j_1} - St = DTr_{j_1 - 1} - 2St \enspace ,$$

αφού όλες οι παίκτες στο $N^-(v)_{j-1}$ ακολουθούν τη συντηρητική στρατηγική, εκτός της A, από την οποία δεν έχει κλαπεί τίποτα λόγω της υπόθεσης.

Επαγωγική υπόθεση: Υποθέτουμε ότι

$$\exists k > 1 : j_k > j_{k-1} > j_1 \Rightarrow DTr_{j_k} \leq DTr_{j_{k-1}} - St \enspace .$$

Επαγωγικό βήμα: Υπάρχει ένα υποσύνολο των Θυμωμένων παικτών, S, από τους οποίους έχει κλαπεί τουλάχιστον St συνολική αξία μεταξύ των γύρων j_{k-1} και j_k, συνεπώς υπάρχει γύρος j_{k+1} τέτοιος ώστε όλες οι παίκτες στο S να έχουν παίξει και συνεπώς

$$DTr_{j_{k+1}} \leq DTr_{j_k} - St \ .$$

Δείξαμε με επαγωγή ότι

$$\forall n \in \mathbb{N}, \exists j_n \in \mathbb{N} : DTr_{j_n} \leq DTr_{j_1 - 1} - nSt \ .$$

Ωστόσο

$$DTr_{j_1 - 1} \geq 0 \wedge St > 0 \ ,$$

συνεπώς

$$\exists n' \in \mathbb{N} : n'St > DTr_{j_1 - 1} \Rightarrow DTr_{j_{n'}} < 0 \ .$$

Έχουμε άτοπο γιατί

$$\forall w, w' \in \mathcal{V}, \forall j \in \mathbb{N}, DTr_{w \to w', j} \geq 0 \ ,$$

Συνεπώς τελικά $Angry = \emptyset$ και όλοι παίζουν "πάσο". □

Απόδειξη του Λήμματος 1: Οι Μέγιστες Ροές είναι Μεταβατικά Παιχνίδια

Υποθέτουμε ότι ο γύρος του $\mathcal{G}$ είναι ο 0. Με άλλα λόγια, $\mathcal{G} = \mathcal{G}_0$. Έστω $X = \{x_{vw}\}_{\mathcal{V} \times \mathcal{V}}$ οι ροές που επιστρέφονται από τον $MaxFlow\,(A, B)$. Για κάθε γράφο G υπάρχει απόδοση $MaxFlow$ που να είναι κατευθυνόμενος ακυκλικός γράφος (ΚΑΓ). Αυτό μπορεί να αποδειχθεί εύκολα με χρήση του θεωρήματος Αποσύνθεσης Ροής [35], το οποίο δηλώνει ότι κάθε ροή μπορεί να ειδωθεί ως ένα πεπερασμένο σύνολο μονοπατιών από τον A στον B και κύκλων, ο καθένας εκ των οποίων εχει μία συγκεκριμένη ροή. Εκτελούμε το $MaxFlow\,(A, B)$ και εφαρμόζουμε το προαναφερθέν θεώρημα. Οι κύκλοι δεν επηρεάζουν το $MaxFlow\,(A, B)$, συνεπώς μπορούμε να αφαιρέσουμε τις ροές αυτές. Η προκύπτουσα ροή είναι ένα $MaxFlow\,(A, B)$ χωρίς κύκλους, συνεπώς είναι ένας ΚΑΓ. Εκτελώντας τοπολογική ταξινόμηση σε αυτόν τον ΚΑΓ, παίρνουμε μία ολική διάταξη των κόμβων του έτσι που $\forall v, w \in \mathcal{V} : v < w \Rightarrow x_{wv} = 0$ [5]. Θέτοντάς το διαφορετικά, δεν υπάρχει ροή από μεγαλύτερους προς μικρότερους κόμβους. Ο B είναι μέγιστος αφού είναι η καταβόθρα και συνεπώς δεν έχει εξερχόμενη ροή προς άλλους κόμβους και ο A είναι ελάχιστος γιατί είναι η πηγή και συνεπώς δεν έχει καθόλου εισερχόμενη ροή από άλλους κόμβους. Η επιθυμητή εκτέλεση του Μεταβατικού Παιχνιδιού θα διαλέξει παίκτες ακολουθώντας την ολική διάταξη αντίστροφα, ξεκινώντας από την παίκτη B. Παρατηρούμε ότι $\forall v \in \mathcal{V} \setminus \{A, B\}$, $\sum\limits_{w \in \mathcal{V}} x_{wv} = \sum\limits_{w \in \mathcal{V}} x_{vw} \leq maxFlow\,(A, B) \leq in_{B,0}$.

Η παίκτης B θα ακολουθήσει μία τροποποιημένη κακιά στρατηγική στην οποία κλέβει αξία ίση με τη συνολική εισερχόμενη ροή, όχι τη συνολική εισερχόμενη εμπιστοσύνη. Έστω j_2 ο πρώτος γύρος στον οποίο επιλεγεται η A. Θα δείξουμε χρησιμοποιώντας ισχυρή επαγωγή ότι υπάρχει σύνολο έγκυρων πράξεων για κάθε παίκτη ανάλογα με τη στρατηγική της τέτοιο ώστε στο τέλος του γύρου j η αντίστοιχη παίκτης $v = Player\left(j\right)$ θα έχει κλέψει αξία x_{wv} από κάθε μέσα γείτονα w.

Επαγωγική βάση: Στο γύρο 1, η B κλέβει αξία ίση με $\sum\limits_{w \in \mathcal{V}} x_{wB}$, ακολουθώντας την τροποποιημένη κακιά στρατηγική.

$$Turn_1 = \bigcup_{v \in N^-(B)_0} \left\{Steal\left(x_{vB}, v\right)\right\}$$

Επαγωγική υπόθεση: Έστω $k \in [j_2 - 2]$. Υποθέτουμε ότι $\forall i \in [k]$, υπάρχει ένα έγκυρο σύνολο πράξεων, $Turn_i$, εκτελεσμένων από την $v = Player\left(i\right)$ τέτοιο ώστε η v να κλέψει από κάθε παίκτη w αξία ίση με x_{wv}.

$$\forall i \in [k], Turn_i = \bigcup_{w \in N^-(v)_{i-1}} \left\{Steal\left(x_{wv}, w\right)\right\}$$

Επαγωγικό βήμα: Έστω $j = k+1, v = Player\left(j\right)$. Αφού όλες οι παίκτες που είναι μεγαλύτερες από την v στην ολική διάταξη έχουν ήδη παίξει και όλες τους έχουν κλέψει αξία ίση με την εισερχόμενη ροή τους, συμπεραίνουμε ότι από τη v έχει κλαπεί αξία ίση με $\sum\limits_{w \in N^+(v)_{j-1}} x_{vw}$. Αφού αυτή είναι η πρώτη φορά που η v παίζει, $\forall w \in N^-\left(v\right)_{j-1}, DTr_{w \to v, j-1} = DTr_{w \to v, 0} \geq x_{wv}$, συνεπώς η v μπορεί να διαλέξει τον εξής γύρο:

$$Turn_j = \bigcup_{w \in N^-(v)_{j-1}} \left\{Steal\left(x_{wv}, w\right)\right\}$$

Επιπλέον, αυτός ο γύρος ικανοποιεί τη συντηρητική στρατηγική αφού

$$\sum_{w \in N^-(v)_{j-1}} x_{wv} = \sum_{w \in N^+(v)_{j-1}} x_{vw} \ .$$

Άρα ο $Turn_j$ είναι ένας έγκυρος γύρος για τη συντηρητική παίκτη v.

Δείξαμε ότι στο τέλος του γύρου $j_2 - 1$, η παίκτης B και όλες οι συντηρητικές παίκτες θα έχουν κλέψει αξία ακριβώς ίση με την εισερχόμενη ροή, συνεπώς από την A θα έχει κλαπεί αξία ίση με την εξερχόμενη ροή της, η οποία είναι $maxFlow\left(A, B\right)$. Αφού δε μένει άλλη Θυμωμένη παίκτης, ο j_2 είναι γύρος σύγκλισης, συνεπώς $Loss_{A, j_2} = Loss_A$. Μπορούμε επίσης να δούμε ότι αν η B είχε διαλέξει την κανονική κακιά στρατηγική, οι πράξεις που περιγράφηκαν θα εξακολουθούσαν να είναι έγκυρες με απλή προσθήκη επιπλέον πράξεων $Steal\left(\right)$, συνεπώς η $Loss_A$ θα αυξανόταν περαιτέρω. Αυτό αποδεικνύει το λήμμα. $\square$

Απόδειξη του Λήμματος 2: Τα Μεταβατικά Παιχνίδια είναι Μέγιστες Ροές

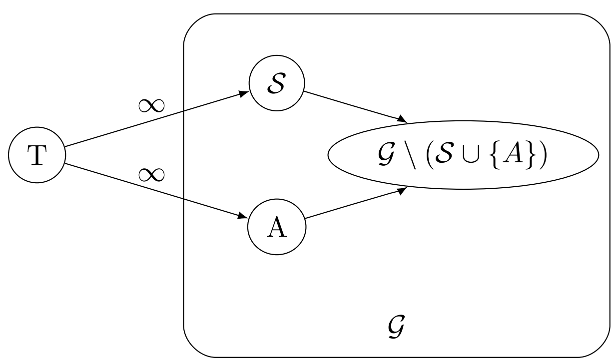
Έστω σύνολα Λυπημένων, Χαρούμενων και Θυμωμένων παικτών όπως ορίστηκαν στο Μεταβατικό Παιχνίδι. Έστω $\mathcal{G}'$ ένας κατευθυνόμενος γράφος με βάρη βασισμένος στον $\mathcal{G}$ με μία βοηθητική πηγή. Έστω επίσης j_1 ένας γύρος που το Μεταβατικό Παιχνίδι έχει συγκλίνει. Πιο συγκεκριμένα, ο $\mathcal{G}'$ ορίζεται ως εξής:

$$\mathcal{V}' = \mathcal{V} \cup \{T\}$$

$$\mathcal{E}' = \mathcal{E} \cup \{(T, A)\} \cup \{(T, v) : v \in Sad_{j_1}\}$$

$$\forall (v, w) \in \mathcal{E}, c'_{vw} = DTr_{v \to w, 0} - DTr_{v \to w, j_1}$$

$$\forall v \in Sad_{j_1}, c'_{Tv} = c'_{TA} = \infty$$



Σχ. 7: Γράφος $\mathcal{G}'$ όπως προκύπτει από τον $\mathcal{G}$ με βοηθητική πηγή T.

Στο παραπάνω σχήμα, το $\mathcal{S}$ είναι το σύνολο των Λυπημένων παικτών. Παρατηρούμε ότι $\forall v \in \mathcal{V}$,

$$\begin{aligned} &\sum_{w \in N^-(v)' \setminus \{T\}} c'_{wv} = \\ &= \sum_{w \in N^-(v)' \setminus \{T\}} (DTr_{w \to v,0} - DTr_{w \to v,j_1}) = \\ &= \sum_{w \in N^-(v)' \setminus \{T\}} DTr_{w \to v,0} - \sum_{w \in N^-(v)' \setminus \{T\}} DTr_{w \to v,j-1} = \\ &= in_{v,0} - in_{v,j_1} \end{aligned} \tag{17}$$

και

$$\begin{aligned} &\sum_{w \in N^+(v)' \setminus \{T\}} c'_{vw} = \\ &= \sum_{w \in N^+(v)' \setminus \{T\}} (DTr_{v \to w,0} - DTr_{v \to w,j_1}) = \\ &= \sum_{w \in N^+(v)' \setminus \{T\}} DTr_{v \to w,0} - \sum_{w \in N^+(v)' \setminus \{T\}} DTr_{v \to w,j-1} = \\ &= out_{v,0} - out_{v,j_1} \ \ . \end{aligned} \tag{18}$$

Μπορούμε να υποθέσουμε ότι

$$\forall j \in \mathbb{N}, in_{A,j} = 0 \ \ , \tag{19}$$

αφού αν βρύμε μία έγκυρη ροή υπό αυτήν την υπόθεση, η ροή θα εξακολουθεί να είναι έγκυρη για τον αρχικό γράφο.
Στη συνέχεια θα υπολογίσουμε το $MaxFlow\,(T, B) = X'$ στο γράφο $\mathcal{G}'$. Παρατηρούμε ότι μία ροή για την οποία ισχύει $\forall v, w \in \mathcal{V}, x'_{vw} = c'_{vw}$ μπορεί να είναι έγκυρη για τους ακόλουθους λόγους:

- $\forall v, w \in \mathcal{V}, x'_{vw} \leq c'_{vw}$ (Περιορισμός χωρητικότητας (11) $\forall e \in \mathcal{E}$)
- Αφού $\forall v \in Sad_{j_1} \cup \{A\}, c'_{Tv} = \infty$, ο περιορισμός (11) ισχύει για κάθε ροή $x'_{Tv} \geq 0$.
- Έστω $v \in \mathcal{V}' \setminus (Sad_{j_1} \cup \{T, A, B\})$. Σύμφωνα με τη συντηρητική στρατηγική και αφού $v \notin Sad_{j_1}$, ισχύει ότι

$$out_{v,0} - out_{v,j_1} = in_{v,0} - in_{v,j_1} \ \ .$$

Συνδυάζοντας αυτή την παρατήρηση με το (17) και το (18), έχουμε ότι

$$\sum_{w \in \mathcal{V}'} c'_{vw} = \sum_{w \in \mathcal{V}'} c'_{wv} \ \ .$$

(Περιορισμός Διατήρησης Ροής (12) $\forall v \in \mathcal{V}' \setminus (Sad_{j_1} \cup \{T, A, B\})$)

– Έστω $v \in Sad_{j_1}$. Αφού η v είναι Λυπημένη, ξέρουμε ότι

$$out_{v,0} - out_{v,j_1} > in_{v,0} - in_{v,j_1} \quad .$$

Αφού $c'_{Tv} = \infty$, μπορούμε να θέσουμε

$$x'_{Tv} = (out_{v,0} - out_{v,j_1}) - (in_{v,0} - in_{v,j_1}) \quad .$$

Κατ΄ αυτόν τον τρόπο έχουμε

$$\sum_{w \in \mathcal{V}'} x'_{vw} = out_{v,0} - out_{v,j_1} \text{ και}$$

$$\sum_{w \in \mathcal{V}'} x'_{wv} = \sum_{w \in \mathcal{V}' \setminus \{T\}} c'_{wv} + x'_{Tv} = in_{v,0} - in_{v,j_1} +$$
$$+ (out_{v,0} - out_{v,j_1}) - (in_{v,0} - in_{v,j_1}) = out_{v,0} - out_{v,j_1} \quad .$$

συνεπώς

$$\sum_{w \in \mathcal{V}'} x'_{vw} = \sum_{w \in \mathcal{V}'} x'_{wv} \quad .$$

(Περιορισμός 12 $\forall v \in Sad_{j_1}$)

– Αφού $c'_{TA} = \infty$, μπορούμε να θέσουμε

$$x'_{TA} = \sum_{v \in \mathcal{V}'} x'_{Av} \quad ,$$

συνεπώς από το (19) έχουμε

$$\sum_{v \in \mathcal{V}'} x'_{vA} = \sum_{v \in \mathcal{V}'} x'_{Av} \quad .$$

(Περιορισμός 12 για την A)

Είδαμε ότι για όλους τους κόμβους, οι απαραίτητες ιδιότητες για να είναι μία ροή έγκυρη ισχύουν και συνεπώς η X' είναι μία έγκυρη ροή για τον $\mathcal{G}$. Επιπλέον, η ροή αυτή είναι ίση με το $maxFlow\,(T,B)$ γιατί όλες οι εισερχόμενες ροές στην E είναι κορεσμένες. Επίσης παρατηρούμε ότι

$$\sum_{v \in \mathcal{V}'} x'_{Av} = \sum_{v \in \mathcal{V}'} c'_{Av} = out_{A,0} - out_{A,j_1} = Loss_A \quad . \tag{20}$$

Ορίζουμε έναν ακόμη γράφο, τον $\mathcal{G}''$, με βάση τον $\mathcal{G}'$.

$$\mathcal{V}'' = \mathcal{V}'$$

$$E(\mathcal{G}'') = E(\mathcal{G}') \setminus \{(T,v) : v \in Sad_j\}$$
$$\forall e \in E(\mathcal{G}''), c''_e = c'_e$$

Αν εκτελέσουμε τον $MaxFlow\,(T,B)$ στο γράφο $\mathcal{G}''$, θα αποκτήσουμε μια ροή X'' στην οποία

$$\sum_{v \in \mathcal{V}''} x''_{Tv} = x''_{TA} = \sum_{v \in \mathcal{V}''} x''_{Av} \ .$$

Η εξερχόμενη ροή από την A στη X'' θα παραμείναι ίδια με αυτή στην X' για δύο λόγους: Πρώτον, χρησιμοποιώντας το θεώρημα Αποσύνθεσης Ροών [35] και διαγράφοντας τα μονοπάτια που περιέχουν ακμές $(T,v) : v \neq A$, αποκτούμε μία νέα απόδοση ροών όπου η συνολική εξερχόμενη ροή από την A παραμένει αμετάβλητη, συνεπώς

$$\sum_{v \in \mathcal{V}''} x''_{Av} \geq \sum_{v \in \mathcal{V}'} x'_{Av} \ .$$

Κατά δεύτερον, έχουμε

$$\left.\begin{array}{l} \sum_{v \in \mathcal{V}''} c''_{Av} = \sum_{v \in \mathcal{V}'} c'_{Av} = \sum_{v \in \mathcal{V}'} x'_{Av} \\ \sum_{v \in \mathcal{V}''} c''_{Av} \geq \sum_{v \in \mathcal{V}''} x''_{Av} \end{array}\right\} \Rightarrow \sum_{v \in \mathcal{V}''} x''_{Av} \leq \sum_{v \in \mathcal{V}'} x'_{Av} \ .$$

Καταλήγουμε συνεπώς ότι

$$\sum_{v \in \mathcal{V}''} x''_{Av} = \sum_{v \in \mathcal{V}'} x'_{Av} \ . \tag{21}$$

Έστω $X = X'' \setminus \{(T,A)\}$. Παρατηρούμε ότι

$$\sum_{v \in \mathcal{V}''} x''_{Av} = \sum_{v \in \mathcal{V}} x_{Av} \ .$$

Αυτή η ροή είναι έγκυρη στο γράφο $\mathcal{G}$ γιατί

$$\forall e \in \mathcal{E}, c_e \geq c''_e \ .$$

Συνεπώς υπάρχει έγκυρη ροή για κάθε εκτέλεση του Μεταβατικού Παιχνιδιού έτσι ώστε

$$\sum_{v \in \mathcal{V}} x_{Av} = \sum_{v \in \mathcal{V}''} x''_{Av} \overset{(21)}{=} \sum_{v \in \mathcal{V}'} x'_{Av} \overset{(20)}{=} Loss_{A,j_1} \ ,$$

η οποία είναι η ροή X. □

Θεώρημα 6 (Θεώρημα Συντηρητικού Κόσμου).
Αν όλες ακολουθούν τη συντηρητική στρατηγική, καμία δεν κλέβει κανένα ποσό από καμία άλλη.

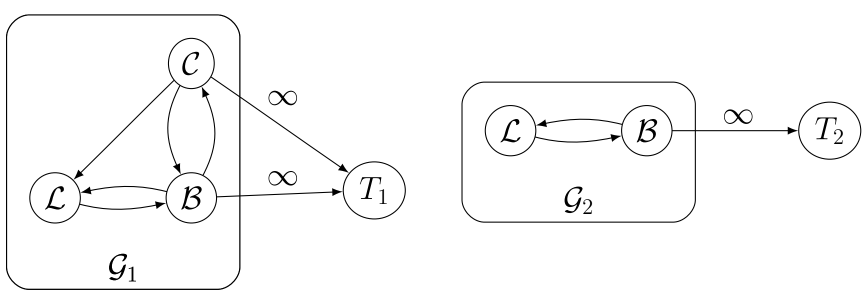
Απόδειξη. Έστω $\mathcal{H}$ η ιστορία του παιχνιδιού όπου όλοι οι παίκτες είναι συντηρητικοί και ας υποθέσουμε ότι συμβαίνουν κάποιες πράξεις $Steal\,()$. Τότε έστω $\mathcal{H}'$ η υπακολουθία των γύρων που περιέχουν τουλάχιστον μία πράξη $Steal\,()$. Αυτή η υπακολουθία είναι προφανώς μη κενή, συνεπώς θα πρέπει να περιέχει πρώτο στοιχείο. Η παίκτης που αντιστοιχεί σε αυτόν το γύρο, A, έχει επιλέξει μία πράξη $Steal\,()$ και καμία προηγούμενη παίκτης δεν έχει επιλέξει τέτοια πράξη. Ωστόσο, η παίκτης A ακολουθεί τη συντηρητική στρατηγική, το οποίο είναι αντίφαση. □

Απόδειξη του Θεωρήματος 5: Sybil Αντίσταση
Έστω $\mathcal{G}_1$ γράφος παιχνιδιού που ορίζεται ως εξής:

$$\mathcal{V}_1 = \mathcal{V} \cup \{T_1\}\ ,$$

$$\mathcal{E}_1 = \mathcal{E} \cup \{(v, T_1) : v \in \mathcal{B} \cup \mathcal{C}\}\ ,$$
$$\forall v, w \in \mathcal{V}_1 \setminus \{T_1\}, DTr^1_{v \to w} = DTr_{v \to w}\ ,$$
$$\forall v \in \mathcal{B} \cup \mathcal{C}, DTr^1_{v \to T_1} = \infty\ ,$$

όπου η $DTr_{v \to w}$ είναι η άμεση εμπιστοσύνη από την v στην w στον $\mathcal{G}$ και η $DTr^1_{v \to w}$ είναι η άμεση εμπιστοσύνη από την v στην w στον $\mathcal{G}_1$.
Έστω επίσης $\mathcal{G}_2$ ο παράγωγος γράφος που προκύπτει από τον $\mathcal{G}_1$ αν αφαιρέσουμε το σύνολο Sybil, $\mathcal{C}$. Μετονομάζουμε τη T_1 σε T_2 και ορίζουμε $\mathcal{L} = \mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$ ως το σύνολο των τίμιων παικτών για να διευκολύνουμε την κατανόηση.



Σχ. 8: Οι γράφοι $\mathcal{G}_1$ και $\mathcal{G}_2$

Σύμφωνα με το Θεώρημα 4,

$$Tr_{A \to \mathcal{B} \cup \mathcal{C}} = maxFlow_1\left(A, T_1\right) \wedge Tr_{A \to \mathcal{B}} = maxFlow_2\left(A, T_2\right) \quad . \tag{22}$$

Θα δείχουμε ότι το $MaxFlow$ του καθενός από τους δύο γράφους μπορεί να χρησιμοποιηθεί για να κατασκευαστεί μία έγκυρη ροή ίσης τιμής για τον άλλο γράφο. Η ροή $X_1 = MaxFlow\left(A, T_1\right)$ μπορεί να χρησιμοποιηθεί για να κατασκευαστεί μία έγκυρη ροή ίσης τιμής για το δεύτερο γράφο αν θέσουμε

$$\forall v \in \mathcal{V}_2 \setminus \mathcal{B}, \forall w \in \mathcal{V}_2, x_{vw,2} = x_{vw,1} \ ,$$
$$\forall v \in \mathcal{B}, x_{vT_2,2} = \sum_{w \in N_1^+(v)} x_{vw,1} \ ,$$
$$\forall v, w \in \mathcal{B}, x_{vw,2} = 0 \ .$$

Έτσι

$$maxFlow_1\left(A, T_1\right) \leq maxFlow_2\left(A, T_2\right)$$

Ομοίως, η ροή $X_2 = MaxFlow(A, T_2)$ είναι μία έγκυρη ροή για τον $\mathcal{G}_1$ γιατί ο $\mathcal{G}_2$ είναι ένας παράγωγος υπογράφος του $\mathcal{G}_1$. Συνεπώς

$$maxFlow_1\left(A, T_1\right) \geq maxFlow_2\left(A, T_2\right)$$

Συμπεραίνουμε ότι

$$maxFlow\left(A, T_1\right) = maxFlow\left(A, T_2\right) \quad , \tag{23}$$

άρα από το (22) και το (23) το θεώρημα ισχύει. □

2 Αλγόριθμοι

Αυτός ο αλγόριθμος καλεί τις απαραίτητες συναρτήσεις για να προετοιμάσει το νέο γράφο.

```
Execute Turn
Input : old graph 𝒢_{j−1}, player A ∈ 𝒱_{j−1}, old capital
    Cap_{A,j−1}, TentativeTurn
Output : new graph 𝒢_j, new capital Cap_{A,j}, new history ℋ_j
executeTurn(𝒢_{j−1}, A, Cap_{A,j−1}, TentativeTurn) :
  (Turn_j, NewCap) = validateTurn(𝒢_{j−1}, A, Cap_{A,j−1},
      TentativeTurn)
  return(commitTurn(𝒢_{j−1}, A, Turn_j, NewCap))
```

Ο ακόλουθος αλγόριθμος επικυρώνει ότι ο προετοιμασμένος γύρος που παράχθηκε από τη στρατηγική σέβεται τους κανόνες που επιβάλλονται στους γύρους. Αν ο γύρος είναι άκυρος, επιστρέφεται ένας κενός γύρος.

```
Validate Turn
Input : old $\mathcal{G}_{j-1}$, player $A \in \mathcal{V}_{j-1}$, old $Cap_{A,j-1}$, Turn
Output : $Turn_j$, new $Cap_{A,j}$
validateTurn($\mathcal{G}_{j-1}$, $A$, $Cap_{A,j-1}$, Turn) :
  $Y_{st}$ = $Y_{add}$ = 0
  Stolen = Added = $\emptyset$
  for (action $\in$ Turn)
    action match do
      case $Steal(\mathrm{y}, w)$ do
        if (y > $DTr_{w \to A,j-1}$ or y < 0 or $w \in$ Stolen)
          return($\emptyset$, $Cap_{A,j-1}$)
        else $Y_{st}$ += y; Stolen = Stolen $\cup \{w\}$
      case $Add(\mathrm{y}, w)$ do
        if (y < -$DTr_{A \to w,j-1}$ or $w \in$ Added)
          return($\emptyset$, $Cap_{A,j-1}$)
        else $Y_{add}$ += y; Added = Added $\cup \{w\}$
  if ($Y_{add}$ - $Y_{st}$ > $Cap_{A,j-1}$) return($\emptyset$, $Cap_{A,j-1}$)
  else return(Turn, $Cap_{A,j-1} + Y_{st} - Y_{add}$)
```

Τέλος, αυτός ο αλγόριθμος εφαρμόζει το γύρο στον παλιό γράφο και επιστρέφει τον καινούριο γράφο, μαζί με το ανανεωμένο κεφάλαιο και την ιστορία.

```
Commit Turn
Input : old $\mathcal{G}_{j-1}$, player $A \in \mathcal{V}_{j-1}$, NewCap, $Turn_j$
Output : new $\mathcal{G}_j$, new $Cap_{A,j}$, new $\mathcal{H}_j$
commitTurn($\mathcal{G}_{j-1}$, $A$, NewCap, $Turn_j$) :
  for (($v$, $w$) $\in \mathcal{E}_j$) $DTr_{v \to w,j}$ = $DTr_{v \to w,j-1}$
  for (action $\in Turn_j$)
    action match do
      case $Steal(\mathrm{y}, w)$ do $DTr_{w \to A,j}$ = $DTr_{w \to A,j-1} - y$
      case $Add(\mathrm{y}, w)$ do $DTr_{A \to w,j}$ = $DTr_{A \to w,j-1} + y$
  $Cap_{A,j}$ = NewCap; $\mathcal{H}_j$ = ($A$, $Turn_j$)
  return($\mathcal{G}_j$, $Cap_{A,j}$, $\mathcal{H}_j$)
```

Ο έλεγχος της συμβατότητας των προηγούμενων αλγορίθμων με τους αντίστοιχους ορισμούς είναι πολύ απλός.

Αναφορές

1. Σανςηεζ Ω.: Λινες οφ ῝ρεδιτ. ηττπς://γιστ.γιτηυβ.ςομ/δρωασηο/2ς40β91ε169φ55988618ˆπαρτ-3-ωεβ-οφ-ςρεδιτ (2016)
2. Νακαμοτο Σ.: Βιτςοιν: Α Πεερ-το-Πεερ Ελεςτρονις ῝ἂση Σψστεμ (2008)
3. Αντονοπουλος Α. Μ.: Μαστερινγ Βιτςοιν: Υνλοςκινγ Διγιταλ ῝ρψπτοςυρρενςιες. Ο-Ῥειλλψ Μεδια, Ινς. (2014)
4. Καρλαν Δ., Μοβιυς Μ., Ροσενβλατ Τ., Σζειδλ Α.: Τρυστ ανδ σοςιαλ ςολλατεραλ. Τηε Χυαρτερλψ Θουρναλ οφ Εςονομιςς: ππ. 1307–1361 (2009)
5. ῞ὂρμεν Τ. Η., Λεισερσον ῝. Ε., Ριεστ Ρ. Λ., Στειν ῝.: Ιντροδυςτιον το αλγοριτημς. ΜΙΤ Πρεσς ανδ ΜςΓραω-Ηιλλ: 3ρδ εδ. (2009)
6. Ορλιν Θ. Β.: Μαξ Φλοως ιν Ο(νμ) Τιμε, ορ Βεττερ. Ιν ΣΤΟ῝ ΄13 Προςεεδινγς οφ τηε φορτψ-φιφτη αννυαλ Α῝Μ σψμποσιυμ ον Τηεορψ οφ ςομπυτινγ: ππ. 765–774: Α῝Μ, Νεω Ψορκ: δοι:10.1145/2488608.2488705 (2013)
7. Ζιμμερμανν Π.: ΠΓΠ Σουρςε ῝ὂδε ανδ Ιντερναλς. Τηε ΜΙΤ Πρεσς (1995)
8. ῝λαρκε Ι., Σανδβεργ Ο., Ωιλεψ Β., Ηονγ Τ. Ω.: Φρεενετ: Α Διστριβυτεδ Ανονψμους Ινφορματιον Στοραγε ανδ Ρετριεαλ Σψστεμ. Ιν Η. Φεδερρατη (εδιτορ), Δεσιγνινγ Πριαςψ Ενηανςινγ Τεςηνολογιες: ππ. 46–66: Σπρινγερ-῞ἒρλαγ Βερλιν Ηειδελβεργ, Βερκελεψ, ΥΣΑ (2001)
9. Αδαμς ῝., Λλοψδ Σ.: Υνδερστανδινγ ΠΚΙ: ςονςεπτς, στανδαρδς, ανδ δεπλοψμεντ ςονσιδερατιονς. Αδδισον-Ωεσλεψ Προφεσσιοναλ (2003)
10. Ποστ Α., Σηαη ῞., Μισλοε Α.: Βαζααρ: Στρενγτηενινγ Υσερ Ρεπυτατιονς ιν Ονλινε Μαρκετπλαςες. Ιν Προςεεδινγς οφ ΝΣΔΙ΄11: 8τη ΥΣΕΝΙΞ Σψμποσιυμ ον Νετωορκεδ Σψστεμς Δεσιγν ανδ Ιμπλεμεντατιον: π. 183 (2011)
11. Λαμπορτ Λ., Σηοστακ Ρ., Πεασε Μ.: Τηε Βψζαντινε Γενεραλς Προβλεμ. Ιν Α῝Μ Τρανσαςτιον ον Προγραμμινγ Λανγυαγες ανδ Σψστεμς: ολ. 4.3: ππ. 382–401 (1982)
12. Ηυψνη Τ. Δ., Θεννινγς Ν. Ρ., Σηαδβολτ Ν. Ρ.: Αν Ιντεγρατεδ Τρυστ ανδ Ρεπυτατιον Μοδελ φορ Οπεν Μυλτι-Αγεντ Σψστεμς. Αυτονομους Αγεντς ανδ Μυλτι-Αγεντ Σψστεμς: ολ. 13(2), ππ. 119–154 (2006)
13. Μιςηιαρδι Π., Μολα Ρ.: ῞ὂρε: α ῞ὂλλαβορατιε Ρεπυτατιον Μεςηανισμ το Ενφορςε Νοδε ῞ὂοπερατιον ιν Μοβιλε Αδ-ηος Νετωορκς. Ιν Αδανςεδ ῞ὂμμυνιςατιονς ανδ Μυλτιμεδια Σεςυριτψ: ππ. 107–121: Σπρινγερ ΥΣ (2002)
14. ῞ἂννον Λ.: Οπεν Ρεπυτατιον: τηε Δεςεντραλιζεδ Ρεπυτατιον Πλατφορμ. ηττπς://οπενρεπυτατιον.νετ/οπεν-ρεπυτατιον-ηιγη-λεελ-ωηιτεπαπερ.πδφ (2015)
15. Γρΰνερτ Α., Ηυδερτ Σ., Κὂνινγ Σ., Καφφιλλε Σ., Ωιρτζ Γ.: Δεςεντραλιζεδ Ρεπυτατιον Μαναγεμεντ φορ ῞ὂοπερατινγ Σοφτωαρε Αγεντς ιν Οπεν Μυλτι-Αγεντ Σψστεμς. ΙΤΣΣΑ: ολ. 1(4), ππ. 363–368 (2006)
16. Ρεπαντις Τ., Καλογερακι ῞.: Δεςεντραλιζεδ Τρυστ Μαναγεμεντ φορ Αδ-ηος Πεερ-το-Πεερ Νετωορκς. Ιν Προςεεδινγς οφ τηε 4τη Ιντερνατιοναλ Ωορκσηοπ οφ Μιδδλεωαρε φορ Περασιε ανδ Αδ-ηος ῞ὂμπυτινγ: π. 6: ΜΠΑ῝: Α῝Μ (2006)
17. Μυι Λ., Μοητασηεμι Μ., Ηαλβερσταδτ Α.: Α ῞ὂμπυτατιοναλ Μοδελ οφ Τρυστ ανδ Ρεπυτατιον. Ιν Προςεεδινγς οφ τηε 35τη Αννυαλ Ηαωαιι Ιντερνατιοναλ ῞ὂνφερενςε ον Σψστεμ Σςιενςες: ππ. 2431–2439: ΙΕΕΕ (2002)
18. Θøσανγ Α., Ισμαιλ Ρ.: Τηε Βετα Ρεπυτατιον Σψστεμ. Ιν Προςεεδινγς οφ τηε 15τη Βλεδ Ελεςτρονις ῞ὂμμερςε ῞ὂνφερενςε (2002)
19. Συρψαναραψανα Γ., Ερενκραντζ Θ. Ρ., Ταψλορ Ρ. Ν.: Αν Αρςηιτεςτυραλ Αππροαςη φορ Δεςεντραλιζεδ Τρυστ Μαναγεμεντ. Ιντερνετ ῞ὂμπυτινγ: ολ. 9(6), ππ. 16–23 (2005)
20. Ἶςαν Α., Ποπ Φ., ῝ριστεα ῞.: Δεςεντραλιζεδ Τρυστ Μαναγεμεντ ιν Πεερ-το-Πεερ Σψστεμς. Ιν 10τη Ιντερνατιοναλ Σψμποσιυμ ον Παραλλελ ανδ Διστριβυτεδ ῞ὂμπυτινγ: ππ. 232–239 (2011)

21. Συρψαναραψανα Γ., Διαλλο Μ., Ταψλορ Ρ. Ν.: Α Γενερις Φραμεωορκ φορ Μοδελινγ Δεςεντραλιζεδ Ρεπυτατιον-Βασεδ Τρυστ Μοδελς. Ιν 14τη Σψμποσιυμ ον Φουνδατιονς οφ Σοφτωαρε Ενγινεερινγ: ΣιγΣοφτ: Α̂Μ (2006)
22. ἆροννι Γ.: Ωαλκινγ τηε ωεβ οφ τρυστ. Ιν Εναβλινγ Τεςηνολογιες: Ινφραστρυςτυρε φορ δλλαβορατιε Εντερπρισες, ΙΕΕΕ 9τη Ιντερνατιοναλ Ωορκσηοπς: ππ. 153–158 (2000)
23. Πεννινγ Η. Π.: ΠΓΠ πατηφινδερ. πγπ.ςς.υυ.νλ
24. Γολλμαννν Δ.: Ωηψ τρυστ ις βαδ φορ σεςυριτψ. Ελεςτρονις νοτες ιν τηεορετιςαλ ςομπυτερ σςιενςε: ολ. 157(3), ππ. 3–9 (2016)
25. Σοσκα Κ., Κωον Α., ῆριστιν Ν., Δεαδας Σ.: Βεαερ: Α Δεςεντραλιζεδ Ανονψμους Μαρκετπλαςε ωιτη Σεςυρε Ρεπυτατιον (2016)
26. Ζινδρος Δ.: Τρυστ ιν Δεςεντραλιζεδ Ανονψμους Μαρκετπλαςες (2015)
27. ΔεΦιγυειρεδο Δ. Δ. Β., Βαρρ Ε. Τ.: ΤρυστΔαις: Α Νον-Εξπλοιταβλε Ονλινε Ρεπυτατιον Σψστεμ. ἘἘ: ολ. 5, ππ. 274–283 (2005)
28. Φυγγερ Ρ.: Μονεψ ας ΙΟΥς ιν Σοςιαλ Τρυστ Νετωορκς & Α Προποσαλ φορ α Δεςεντραλιζεδ ῦρρενςψ Νετωορκ Προτοςολ. ηττπ://αρςηιε.ριππλε-προθεςτ.οργ/δεςεντραλιζεδςυρρενςψ.πδφ (2004)
29. Σςηαρτζ Δ., Ψουνγς Ν., Βριττο Α.: Τηε Ριππλε προτοςολ ςονσενσυς αλγοριτημ. Ριππλε Λαβς Ινς Ωηιτε Παπερ: ολ. 5 (2014)
30. Μαζιερες Δ.: Τηε στελλαρ ςονσενσυς προτοςολ: Α φεδερατεδ μοδελ φορ ιντερνετλεελ ςονσενσυς. Στελλαρ Δεελοπμεντ Φουνδατιον (2015)
31. Ναραψαναν Α., Σηματικο ῞.: Δε-ανονψμιζινγ Σοςιαλ Νετωορκς. Ιν Προςεεδινγς οφ τηε 30τη Σψμποσιυμ ον Σεςυριτψ ανδ Πριαςψ: ππ. 173–187: ΙΕΕΕ: 10.1109/ΣΠ.2009.22 (2009)
32. Μαλαολτα Γ., Μορενο-Σανςηεζ Π., Κατε Α., Μαφφει Μ.: ΣιλεντΩηισπερς: Ενφορςινγ Σεςυριτψ ανδ Πριαςψ ιν Δεςεντραλιζεδ ῝ρεδιτ Νετωορκς (2016)
33. Μορενο-Σανςηεζ Π., Κατε Α., Μαφφει Μ., Πεςινα Κ.: Πριαςψ πρεσερινγ παψμεντς ιν ςρεδιτ νετωορκς. Ιν Νετωορκ ανδ Διστριβυτεδ Σεςυριτψ Σψμποσιυμ (2015)
34. Κονφορτψ Δ., Αδαμ Ψ., Εστραδα Δ., Μερεδιτη Λ. Γ.: Σψνερεο: Τηε Δεςεντραλιζεδ ανδ Διστριβυτεδ Σοςιαλ Νετωορκ (2015)
35. Αηυϑα Ρ. Κ., Μαγναντι Τ. Λ., Ορλιν Θ. Β.: Νετωορκ Φλοως: Τηεορψ, Αλγοριτημς, ανδ Αππλιςατιονς. Πρεντιςε-Ηαλλ: ηττπς://οςω.μιτ.εδυ. Λιςενσε: ῝ρεατιε ὂμμονς ΒΨ-Ν῝-ΣΑ. (1993)