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

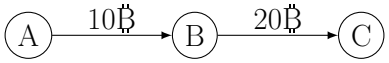
Κατάλογος Ψευδοκωδίκων

1 Εισαγωγή

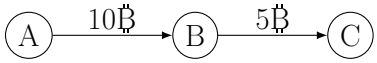
Οι αποκεντρωμένες αγορές μπορούν να κατηγοριοποιηθούν ως κεντρικές και αποκεντρωμένες. Ένα παράδειγμα για κάθε κατηγορία είναι το ebay και το OpenBazaar. Ο κοινός παρονομαστής των καθιερωμένων διαδικτυακών αγορών είναι το γεγονός ότι η φήμη κάθε πωλήτριας και πελάτισσας εκφράζεται κατά κανόνα με τη μορφή 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 A εμπ. έμμεσα τον C 10₿



Σχ. 2: Η A εμπ. έμμεσα τον C 5₿

Προτείνουμε ένα νέο είδος πορτοφολιού όπου τα νομίσματα δεν έχουν απο-

κλειστικό 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 αποτέλε-

σμα 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.

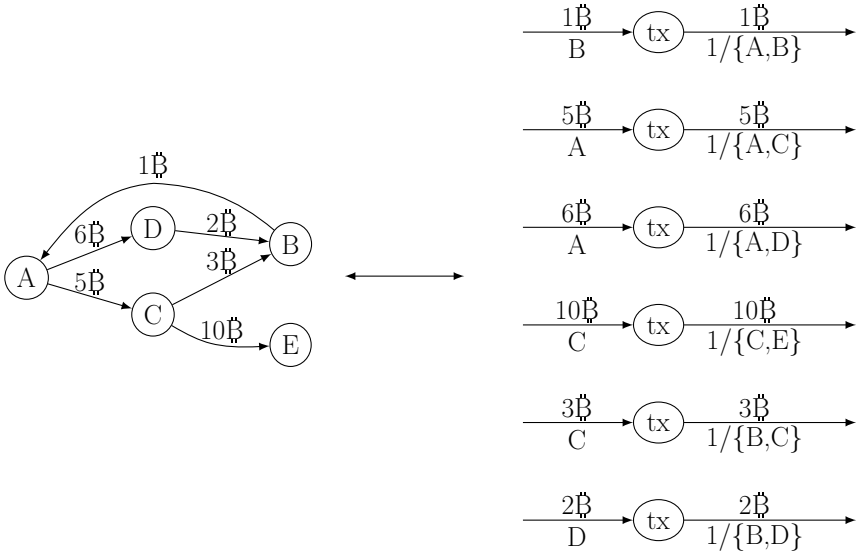
Ο ορισμός της άμεσης εμπιστοσύνης ακολουθεί:

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.

$$DTr_{A\to B,j} = \begin{cases} c_j(A,B), & \text{αν } (A,B) \in \mathcal{E}_j \\ 0, & \text{αλλιώς} \end{cases} \tag{1}$$

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.*

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

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

Ορισμός 9 (Προηγούμενος/Επόμενος Γύρος). *Έστω $j \in \mathbb{N}$ ένας γύρος με $Player(j) = A$. Ορίζουμε τα $prev(j), next(j)$ 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 $prev(j) = 0$. Πιο αυστηρά, έστω*

$$P = \{k \in \mathbb{N} : k < j \wedge Player(k) = A\} \text{ και}$$
$$N = \{k \in \mathbb{N} : k > j \wedge Player(k) = A\} \ .$$

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

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

Το $next(j)$ 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 $Player(j) = A$.*

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

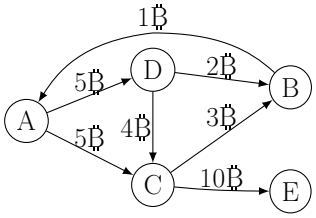
Λέμε ότι κλάπηκε από την A αξία $Damage_{A,j}$ ανάμεσα στον $prev(j)$ και στον j. Παραλείπουμε τους δείκτες γύρων όταν εννοούνται από τα συμφραζόμενα.

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

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

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 παίξει

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



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 ←$ V_j
  Turn = strategy[A](G_0, A, Cap_{A,0}, H_{1...j−1})
  (G_j, Cap_{A,j}, H_j) = executeTurn(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(G_0, A, Cap_{A,0}, H) :
  return(∅)
```

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(G_0, A, Cap_{A,0}, H) :
  Steals = ⋃_{v∈N^-(A)_{j-1}} {Steal(DTr_{v→A,j-1}, v)}
  Adds = ⋃_{v∈N^+(A)_{j-1}} {Add(−DTr_{A→v,j-1}, v)}
  Turn_j = Steals ∪ 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(G_0, A, Cap_{A,0}, H) :
  Damage = out_{A,prev(j)} - out_{A,j-1}
  if (Damage > 0)
    if (Damage >= in_{A,j-1})
      Turn_j = ⋃_{v∈N^-(A)_{j-1}} {Steal(DTr_{v→A,j-1}, v)}
    else
      y = SelectSteal(G_j, A, Damage) #y = {y_v : v ∈ N^-(A)_{j-1}}
      Turn_j = ⋃_{v∈N^-(A)_{j-1}} {Steal(y_v, v)}
  else Turn_j = ∅
  return(Turn_j)
```

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

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

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.

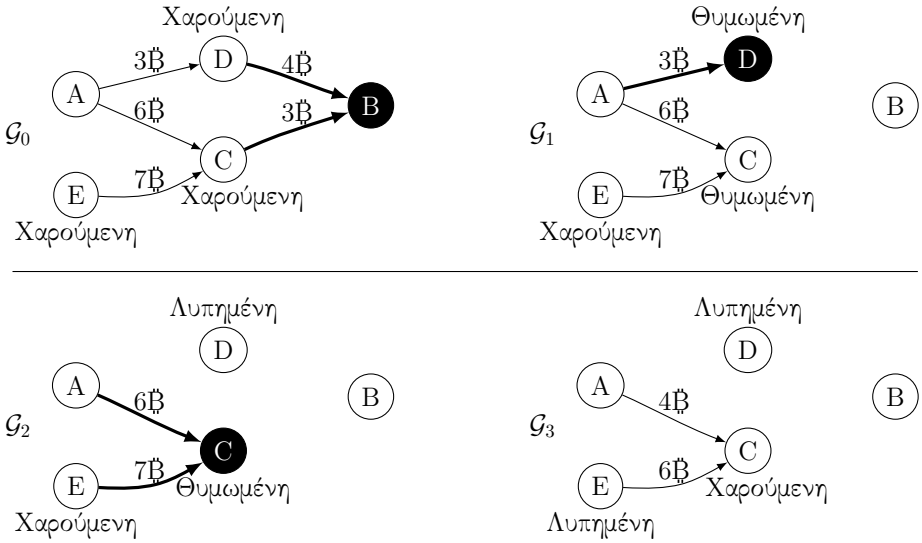
Ο συλλογισμός πίσω από αυτή τη στρατηγική προκύπτει από μια συνηθισμένη περίπτωση στον πραγματικό κόσμο. Έστω μία πελάτισσα, μία μεσάζοντας κι μία παραγωγός. Η πελάτισσα εμπιστεύεται κάποια αξία στη μεσάζοντα ώστε η τελευταία να μπορέσει να αγοράσει το επιθυμητό προϊόν από την παραγωγό και να το παραδώσει 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 $\mathcal{G}_0$, $A \in \mathcal{V}$ `idle player,` $B \in \mathcal{V}$ `evil player`
1 `Angry = Sad =` $\emptyset$ `;` `Happy =` $\mathcal{V} \setminus \{A, B\}$
2 `for` $(v \in \mathcal{V} \setminus \{B\})$ $Loss_v$ `= 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 7₿, μετά η D κλέβει 3₿ και η C κλέβει 3₿

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

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

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 Τρυστ Φλοω

Ωε σαν νοω δεφινε τηε ινδιρεστ τρυστ φρομ A το B.

Ορισμός 15 (Ινδιρεστ Τρυστ). *Τηε ινδιρεστ τρυστ φρομ A το B αφτερ τυρν j ις δεφινεδ ας τηε μαξιμυμ ποσσιβλε αλυε τηατ σαν βε στολεν φρομ A αφτερ τυρν j ιν τηε σεττινγ οφ $\texttt{ΤρανσιτιεΓαμε}(\mathcal{G}_j, A, B)$.*

Ιτ ις $Tr_{A\to B} \geq DTr_{A\to B}$. Τηε νεξτ τηεορεμ σηοως τηατ $Tr_{A\to B}$ ις φινιτε.

Τηεορεμ 1 (Τρυστ ὂνεργενςε Τηεορεμ).
ὂνσιδερ α Τρανσιτιε Γαμε. Τηερε εξιστς α τυρν συςη τηατ αλλ συβσεχυεντ τυρνς αρε εμπτψ.

Προοφ Σκετςη. Ιφ τηε γαμε διδν't ςονεργε, τηε $Steal\,()$ αςτιονς ωουλδ ςοντινυε φορεερ ωιτηουτ ρεδυςτιον οφ τηε αμουντ στολεν οερ τιμε, τηυς τηεψ ωουλδ ρεαςη ινφινιτψ. Ηοωεερ τηις ις ιμποσσιβλε, σινςε τηερε εξιστς ονλψ φινιτε τοταλ διρεςτ τρυστ. □

Φυλλ προοφς οφ αλλ τηεορεμς ανδ λεμμας ςαν βε φουνδ ιν τηε Αππενδιξ.

Ιν τηε σεττινγ οφ $\texttt{ΤρανσιτιεΓαμε}(\mathcal{G}, A, B)$, ωε μακε υσε οφ τηε νοτατιον $Loss_A = Loss_{A,j}$, ωηερε j ις α τυρν τηατ τηε γαμε ηας ςονεργεδ. Ιτ ις ιμπορταντ το νοτε τηατ $Loss_A$ ις νοτ τηε σαμε φορ ρεπεατεδ εξεςυτιονς οφ τηις κινδ οφ γαμε, σινςε τηε ορδερ ιν ωηιςη πλαψερς αρε ςηοσεν μαψ διφφερ βετωεεν εξεςυτιονς ανδ τηε ςονσερατιε πλαψερς αρε φρεε το ςηοοσε ωηιςη ινςομινγ διρεςτ τρυστς τηεψ ωιλλ στεαλ ανδ ηοω μυςη φρομ εαςη.

Λετ G βε α ωειγητεδ διρεστεδ γραπη. Ωε ωιλλ ινεστιγατε τηε μαξιμυμ φλοω ον τηις γραπη. Φορ αν ιντροδυστιον το τηε μαξιμυμ φλοω προβλεμ σεε [5] π. 708. ὃνσιδερινγ εαση εδγε΄ς ςαπαςιτψ ας ιτς ωειγητ, α φλοω ασσιγνμεντ $X = [x_{vw}]_{\mathcal{V}\times\mathcal{V}}$ ωιτη α σουρςε A ανδ α σινκ B ις αλιδ ωηεν:

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

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

Ωε δο νοτ συπποσε ανψ σκεω σψμμετρψ ιν X. Τηε φλοω αλυε ις $\sum_{v \in N^+(A)} x_{Av}$, ωηιςη ις προεν το βε εχυαλ το $\sum_{v \in N^-(B)} x_{vB}$. Τηερε εξιστς αν αλγοριτημ τηατ ρετυρνς τηε μαξιμυμ ποσσιβλε φλοω φρομ A το B, ναμελψ $MaxFlow\,(A, B)$. Τηις αλγοριτημ ειδεντλψ νεεδς φυλλ κνοωλεδγε οφ τηε γραπη. Τηε φαστεστ ερσιον οφ τηις αλγοριτημ ρυνς ιν $O\,(|\mathcal{V}||\mathcal{E}|)$ τιμε [6]. Ωε ρεφερ το τηε φλοω αλυε οφ $MaxFlow\,(A, B)$ ας $maxFlow\,(A, B)$.

Ωε ωιλλ νοω ιντροδυςε τωο λεμμας τηατ ωιλλ βε υσεδ το προε τηε ονε οφ τηε ςεντραλ ρεσυλτς οφ τηις ωορκ, τηε Τρυστ Φλοω τηεορεμ.

Λεμμα 1 (ΜαξΦλοως Αρε Τρανσιτιε Γαμες).
Λετ $\mathcal{G}$ βε α γαμε γραπη, λετ $A, B \in \mathcal{V}$ ανδ $MaxFlow\,(A, B)$ τηε μαξιμυμ φλοω φρομ A το B εξεςυτεδ ον $\mathcal{G}$. Τηερε εξιστς αν εξεςυτιον οφ $\mathit{Τρανσιτιε Γαμε}(\mathcal{G}, A, B)$ *συςη τηατ $maxFlow\,(A, B) \leq Loss_A$.*

Προοφ Σκετςη. Τηε δεσιρεδ εξεςυτιον οφ `ΤρανσιτιεΓαμε()` ωιλλ ςονταιν αλλ φλοως φρομ τηε $MaxFlow\,(A, B)$ ας εχυιαλεντ $Steal\,()$ αςτιονς. Τηε πλαψερς ωιλλ πλαψ ιν τυρνς, μοινγ φρομ B βαςκ το A. Εαςη πλαψερ ωιλλ στεαλ φρομ ηις πρεδεςεσσορς ας μυςη ας ωας στολεν φρομ ηερ. Τηε φλοως ανδ τηε ςονσερατιε στρατεγψ σηαρε τηε προπερτψ τηατ τηε τοταλ ινπυτ ις εχυαλ το τηε τοταλ ουτπυτ. □

Λεμμα 2 (Τρανσιτιε Γαμες Αρε Φλοως).
Λετ $\mathcal{H} =$ $\mathit{Τρανσιτιε Γαμε}(\mathcal{G}, A, B)$ φορ σομε γαμε γραπη $\mathcal{G}$ ανδ $A, B \in \mathcal{V}$. Τηερε εξιστς α αλιδ φλοω $X = \{x_{wv}\}_{\mathcal{V}\times\mathcal{V}}$ ον $\mathcal{G}_0$ συςη τηατ $\sum_{v \in \mathcal{V}} x_{Av} = Loss_A$.

Προοφ Σκετςη. Ιφ ωε εξςλυδε τηε σαδ πλαψερς φρομ τηε γαμε, τηε $Steal\,()$ αςτιονς τηατ ρεμαιν ςονστιτυτε α αλιδ φλοω φρομ A το B. □

Τηεορεμ 2 (Τρυστ Φλοω Τηεορεμ).
Λετ $\mathcal{G}$ *βε α γαμε γραπη ανδ* $A, B \in \mathcal{V}$. *Ιτ ηολδς τηατ*

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

Απόδειξη. Φρομ λεμμα 1 τηερε εξιστς αν εξεςυτιον οφ τηε Τρανσιτιε Γαμε συςη τηατ $Loss_A \geq maxFlow\,(A, B)$. Σινςε $Tr_{A\to B}$ ις τηε μαξιμυμ λοσς τηατ A ςαν συφφερ αφτερ τηε ςονεργενςε οφ τηε Τρανσιτιε Γαμε, ωε σεε τηατ

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

Βυτ σομε εξεςυτιον οφ τηε Τρανσιτιε Γαμε γιες $Tr_{A\to B} = Loss_A$. Φρομ λεμμα 2, τηις εξεςυτιον ςορρεσπονδς το α φλοω. Τηυς

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

Τηε τηεορεμ φολλοως φρομ (13) ανδ (14). □

Νοτε τηατ τηε μαξΦλοω ις τηε σαμε ιν τηε φολλοωινγ τωο ςασες: Ιφ α πλαψερ ςηοοσες τηε ειλ στρατεγψ ανδ ιφ τηατ πλαψερ ςηοοσες α αριατιον οφ τηε ειλ στρατεγψ ωηερε σηε δοες νοτ νυλλιφψ ηερ ουτγοινγ διρεςτ τρυστ.

Φυρτηερ θυστιφιςατιον οφ τρυστ τρανσιτιιτψ τηρουγη τηε υσε οφ $MaxFlow$ ςαν βε φουνδ ιν τηε σοςιολογιςαλ ωορκ ςονδυςτεδ ιν [4] ωηερε α διρεςτ ςορρεσπονδενςε οφ μαξιμυμ φλοως ανδ εμπιριςαλ τρυστ ις εξπεριμενταλλψ αλιδατεδ.

Ηερε ωε σεε ανοτηερ ιμπορταντ τηεορεμ τηατ γιες τηε βασις φορ ριςκ-ιναριαντ τρανσαςτιονς βετωεεν διφφερεντ, ποσσιβλψ υνκνοων, παρτιες.

Τηεορεμ 3 (Ριςκ Ινάριανςε Τηεορεμ). *Λετ* $\mathcal{G}$ *γαμε γραπη,* $A, B \in \mathcal{V}$ *ανδ* l *τηε δεσιρεδ αλυε το βε τρανσφερρεδ φρομ* A *το* B, *ωιτη* $l \leq Tr_{A\to B}$. *Λετ αλσο* $\mathcal{G}'$ *ωιτη τηε σαμε νοδες ας* $\mathcal{G}$ *συςη τηατ*

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

Φυρτηερμορε, συπποσε τηατ τηερε εξιστς αν ασσιγνμεντ φορ τηε ουτγοινγ διρεςτ τρυστ οφ $A, DTr'_{A\to v}$, *συςη τηατ*

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

Λετ ανοτηερ γαμε γραπη, $\mathcal{G}''$, *βε ιδεντιςαλ το* $\mathcal{G}'$ *εξςεπτ φορ τηε φολλοωινγ ςηανγε:*

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

Ιτ τηεν ηολδς τηατ

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

Απόδειξη. Τηε τωο γραπηs $\mathcal{G}'$ ανδ $\mathcal{G}''$ διφφερ ονλψ ον τηε ωειγητ οφ τηε εδγε (A, B), ωηιςη ις λαργερ βψ l ιν $\mathcal{G}''$. Τηυς τηε τωο $MaxFlow$s ωιλλ ςηοοσε τηε σαμε φλοω, εξςεπτ φορ (A, B), ωηερε ιτ ωιλλ βε $x''_{AB} = x'_{AB} + l$. □

Ιτ ις ιντυιτιελψ οβιουs τηατ ιτ ις ποσσιβλε φορ A το ρεδυςε ηερ ουτ-γοινγ διρεςτ τρυστ ιν α μαννερ τηατ αςηιεες (15), σινςε $maxFlow\,(A, B)$ ις ςοντινυους ωιτη ρεσπεςτ το A'ς ουτγοινγ διρεςτ τρυστς. Ωε λεαε τηις ςαλςυλατιον ας παρτ οφ φυρτηερ ρεσεαρςη.

7 Σψβιλ Ρεσιλιενςε

Ονε οφ τηε πριμαρψ αιμς οφ τηις σψστεμ ις το μιτιγατε τηε δανγερ φορ Σψβιλ ατταςκς [7] ωηιλστ μαινταινινγ φυλλψ δεςεντραλιζεδ αυτονομψ.

Ηερε ωε εξτενδ τηε δεφινιτιον οφ ινδιρεςτ τρυστ το μανψ πλαψερς.

Ορισμός 16 (Ινδιρεςτ Τρυστ το Μυλτιπλε Πλαψερς). *Τηε ινδιρεςτ τρυστ φρομ πλαψερ A το α σετ οφ πλαψερς, $S \subset \mathcal{V}$ ις δεφινεδ ας τηε μαξιμυμ ποσσιβλε αλυε τηατ ςαν βε στολεν φρομ A ιφ αλλ πλαψερς ιν S φολλοω τηε ειλ στρατεγψ, A φολλοως τηε ιδλε στρατεγψ ανδ εερψονε ελσε $(\mathcal{V} \setminus (S \cup \{A\}))$ φολλοως τηε ςονσερατιε στρατεγψ. Μορε φορμαλλψ, λετ $choices$ βε τηε διφφερεντ αςτιονς βετωεεν ωηιςη τηε ςονσερατιε πλαψερς ςαν ςηοοσε, τηεν*

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

Ωε νοω εξτενδ Τρυστ Φλοω τηεορεμ (2) το μανψ πλαψερς.

Τηεορεμ 4 (Μυλτι-Πλαψερ Τρυστ Φλοω).
Λετ $S \subset \mathcal{V}$ ανδ T αυξιλιαρψ πλαψερ συςη τηατ $\forall B \in S, DTr_{B \to T} = \infty$. Ιτ ηολδς τηατ

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

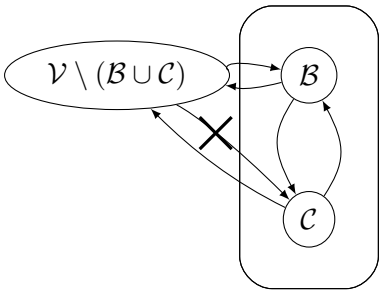
Απόδειξη. Ιφ T ςηοοσες τηε ειλ στρατεγψ ανδ αλλ πλαψερς ιν S πλαψ αςςορδινγ το τηε ςονσερατιε στρατεγψ, τηεψ ωιλλ ηαε το στεαλ αλλ τηειρ ινςομινγ διρεςτ τρυστ σινςε τηεψ ηαε συφφερεδ αν ινφινιτε λοσς, τηυς τηεψ ωιλλ αςτ ιν α ωαψ ιδεντιςαλ το φολλοωινγ τηε ειλ στρατεγψ ας φαρ ας $MaxFlow$ ις ςονςερνεδ. Τηε τηεορεμ φολλοως τηυς φρομ τηε Τρυστ Φλοω τηεορεμ. □

Ωε νοω δεφινε σεεραλ υσεφυλ νοτιονς το ταςκλε τηε προβλεμ οφ Σψβιλ ατταςκς. Λετ Εε βε α ποσσιβλε ατταςκερ.

Ορισμός 17 (Ὅρρυπτεδ Σετ). *Λετ $\mathcal{G}$ βε α γαμε γραπη ανδ λετ Εε ηαε α σετ οφ πλαψερς $\mathcal{B} \subset \mathcal{V}$ σορρυπτεδ, σο τηατ σηε φυλλψ σοντρολς τηειρ ουτγοινγ διρεστ τρυστς το ανψ πλαψερ ιν $\mathcal{V}$ ανδ σαν αλσο στεαλ αλλ ινσομινγ διρεστ τρυστ το πλαψερς ιν $\mathcal{B}$. Ωε σαλλ τηις τηε σορρυπτεδ σετ. Τηε πλαψερς $\mathcal{B}$ αρε σονσιδερεδ το βε λεγιτιματε βεφορε τηε σορρυπτιον, τηυς τηεψ μαψ βε διρεστλψ τρυστεδ βψ ανψ πλαψερ ιν $\mathcal{V}$.*

Ορισμός 18 (Σψβιλ Σετ). *Λετ $\mathcal{G}$ βε α γαμε γραπη. Σινσε παρτισιπατιον ιν τηε νετωορκ δοες νοτ ρεχυιρε ανψ κινδ οφ ρεγιστρατιον, Εε σαν σρεατε ανψ νυμβερ οφ πλαψερς. Ωε ωιλλ σαλλ τηε σετ οφ τηεσε πλαψερς $\mathcal{C}$, ορ Σψβιλ σετ. Μορεοερ, Εε σαν αρβιτραριλψ σετ τηε διρεστ τρυστς οφ ανψ πλαψερ ιν $\mathcal{C}$ το ανψ πλαψερ ανδ σαν αλσο στεαλ αλλ ινσομινγ διρεστ τρυστ το πλαψερς ιν $\mathcal{C}$. Ηοωεερ, πλαψερς $\mathcal{C}$ σαν βε διρεστλψ τρυστεδ ονλψ βψ πλαψερς $\mathcal{B} \cup \mathcal{C}$ βυτ νοτ βψ πλαψερς $\mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$, ωηερε $\mathcal{B}$ ις α σετ οφ πλαψερς σορρυπτεδ βψ Εε.*

Ορισμός 19 (Ὅλλυσιον). *Λετ $\mathcal{G}$ βε α γαμε γραπη. Λετ $\mathcal{B} \subset \mathcal{V}$ βε α σορρυπτεδ σετ ανδ $\mathcal{C} \subset \mathcal{V}$ βε α Σψβιλ σετ, βοτη σοντρολλεδ βψ Εε. Τηε τυπλε $(\mathcal{B}, \mathcal{C})$ ις σαλλεδ α σολλυσιον ανδ ις εντιρελψ σοντρολλεδ βψ α σινγλε εντιτψ ιν τηε πηψσιςαλ ωορλδ. Φρομ α γαμε τηεορετις ποιντ οφ ιεω, πλαψερς $\mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$ περσειε τηε σολλυσιον ας ινδεπενδεντ πλαψερς ωιτη α διστινστ στρατεγψ εαση, ωηερεας ιν ρεαλιτψ τηεψ αρε αλλ συβθεστ το α σινγλε στρατεγψ δισταtεδ βψ τηε σοντρολλινγ εντιτψ, Εε.*



Σχ. 6: Συνεργασία

Τηεορεμ 5 (Σψβιλ Ρεσιλιενσε).
Λετ $\mathcal{G}$ βε α γαμε γραπη ανδ $(\mathcal{B}, \mathcal{C})$ βε α σολλυσιον οφ πλαψερς ον $\mathcal{G}$. Ιτ ις

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

Προοφ Σκετση. Τηε ινςομινγ διρεςτ τρυστ το $\mathcal{B} \cup \mathcal{C}$ ςαννοτ βε ηιγηερ τηαν τηε ινςομινγ διρεςτ τρυστ το $\mathcal{B}$ σινςε $\mathcal{C}$ ηας νο ινςομινγ διρεςτ τρυστ φρομ $\mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$. □

Ωε ηαε προεν τηατ ςοντρολλινγ $|\mathcal{C}|$ ις ιρρελεαντ φορ Εε, τηυς Σψβιλ ατταςκς αρε μεανινγλεσς. Ωε νοτε τηατ τηις τηεορεμ δοες νοτ δελιερ ρεασσυρανςες αγαινστ ατταςκς ινολινγ δεςεπτιον τεςηνιχυες. Μορε σπεςιφιςαλλψ, α μαλιςιους πλαψερ ςαν ςρεατε σεεραλ ιδεντιτιες, υσε τηεμ λεγιτιματελψ το ινσπιρε οτηερς το δεποσιτ διρεςτ τρυστ το τηεσε ιδεντιτιες ανδ τηεν σωιτςη το τηε ειλ στρατεγψ, τηυς δεφραυδινγ εερψονε τηατ τρυστεδ τηε φαβριςατεδ ιδεντιτιες. Τηεσε ιδεντιτιες ςορρεσπονδ το τηε ςορρυπτεδ σετ οφ πλαψερς ανδ νοτ το τηε Σψβιλ σετ βεςαυσε τηεψ ηαε διρεςτ ινςομινγ τρυστ φρομ ουτσιδε τηε ςολλυσιον.

Ιν ςονςλυσιον, ωε ηαε συςςεσσφυλλψ δελιερεδ ουρ προμισε φορ α Σψβιλ-ρεσιλιεντ δεςεντραλιζεδ φινανςιαλ τρυστ σψστεμ ωιτη ιναριαντ ρισκ φορ πυρςηασες.

8 Ρελατεδ Ωορκ

Τηε τοπις οφ τρυστ ηας βεεν ρεπεατεδλψ ατταςκεδ ωιτη σεεραλ αππροαςηες: Πυρελψ ςρψπτογραπηις ινφραστρυςτυρε ωηερε τρυστ ις ρατηερ βιναρψ ανδ τρανσιτιιτψ ις λιμιτεδ το ονε στεπ βεψονδ αςτιελψ τρυστεδ παρτιες ις εξπλορεδ ιν ΠΓΠ [8]. Α τρανσιτιε ωεβ-οφ-τρυστ φορ φιγητινγ σπαμ ις εξπλορεδ ιν Φρεενετ [9]. Οτηερ σψστεμς ρεχυιρε ςεντραλ τρυστεδ τηιρδ παρτιες, συςη ας Ά-βασεδ ΠΚΙς [10] ανδ Βαζααρ [11], ορ, ιν τηε ςασε οφ ΒΦΤ, αυτηεντιςατεδ μεμβερσηιπ [12]. Ωηιλε οτηερ τρυστ σψστεμς αττεμπτ το βε δεςεντραλιζεδ, τηεψ δο νοτ προε ανψ Σψβιλ ρεσιλιενςε προπερτιες ανδ ηενςε μαψ βε Σψβιλ ατταςκαβλε. Συςη σψστεμς αρε ΦΙΡΕ [13], ΎΟΡΕ [14] ανδ οτηερς [15,16,17]. Οτηερ σψστεμς τηατ δεφινε τρυστ ιν α νον-φινανςιαλ ωαψ αρε [18,19,20,21,22,23,24].

Ωε αγρεε ωιτη τηε ωορκ οφ [25] ιν τηατ τηε μεανινγ οφ τρυστ σηουλδ νοτ βε εξτραπολατεδ. Ωε ηαε αδοπτεδ τηειρ αδιςε ιν ουρ παπερ ανδ υργε ουρ ρεαδερς το αδηερε το τηε δεφινιτιονς οφ *διρεςτ* ανδ *ινδιρεςτ* τρυστ ας τηεψ αρε υσεδ ηερε.

Τηε Βεαερ μαρκετπλαςε [26] ινςλυδες α τρυστ μοδελ τηατ ρελιες ον φεες το δισςουραγε Σψβιλ ατταςκς. Ωε ςηοσε το αοιδ φεες ιν ουρ σψστεμ ανδ μιτιγατε Σψβιλ ατταςκς ιν α διφφερεντ μαννερ. Ουρ μοτιατινγ αππλιςατιον φορ εξπλορινγ τρυστ ιν α δεςεντραλιζεδ σεττινγ ις τηε ΟπενΒαζααρ μαρκετπλαςε. Τρανσιτιε φινανςιαλ τρυστ φορ ΟπενΒαζααρ ηας πρειουσλψ βεεν εξπλορεδ βψ [27]. Τηατ ωορκ ηοωεερ δοες νοτ δεφινε τρυστ ας α μονεταρψ αλυε. Ωε αρε στρονγλψ ινσπιρεδ βψ [4] ωηιςη γιες α σοςιολογιςαλ ϑυστιφι-

ςατιον φορ τηε ςεντραλ δεσιγν ςηοιςε οφ ιδεντιφψινγ τρυστ ωιτη ριςκ. Ωε γρεατλψ αππρεςιατε τηε ωορκ ιν ΤρυστΔαις [28], ωηιςη προποσες α φινανςιαλ τρυστ σψστεμ τηατ εξηιβιτς τρανσιτιε προπερτιες ανδ ιν ωηιςη τρυστ ις δεφινεδ ας λινεσ-οφ-ςρεδιτ, σιμιλαρ το ουρ σψστεμ. Ωε ωερε αβλε το εξτενδ τηειρ ωορκ βψ υσινγ τηε βλοςκςηαιν φορ αυτοματεδ προοφσ-οφ-ριςκ, α φεατυρε νοτ ααιλαβλε το τηεμ ατ τηε τιμε.

Ουρ ςονσερατιε στρατεγψ ανδ Τρανσιτιε Γαμε αρε ερψ σιμιλαρ το τηε μεςηανισμ προποσεδ βψ τηε εςονομις παπερ [29] ωηιςη αλσο ιλλυστρατες φινανςιαλ τρυστ τρανσιτιιτψ ανδ ις υσεδ βψ Ριππλε [30] ανδ Στελλαρ [31]. ΙΟΥς ιν τηεσε ςορρεσπονδ το ρεερσεδ εδγες οφ τρυστ ιν ουρ σψστεμ. Τηε ςριτιςαλ διφφερενςε ις τηατ ουρ δενομινατιονς οφ τρυστ αρε εξπρεσσεδ ιν α γλοβαλ ςυρρενςψ ανδ τηατ ςοινς μυστ πρε-εξιστ ιν ορδερ το βε τρυστεδ ανδ σο τηερε ις νο μονεψ-ασ-δεβτ. Φυρτηερμορε, ωε προε τηατ τρυστ ανδ μαξιμυμ φλοωσ αρε εχυιαλεντ, α διρεςτιον νοτ εξπλορεδ ιν τηειρ παπερ, εεν τηουγη ωε βελιεε ιτ μυστ ηολδ φορ αλλ βοτη ουρ ανδ τηειρ σψστεμς.

9 Φυρτηερ Ρεσεαρςη

Ωηεν *Alice* μακες α πυρςηασε φρομ *Bob*, σηε ηας το ρεδυςε ηερ ουτγοινγ διρεςτ τρυστ ιν α μαννερ συςη τηατ τηε συπποσιτιον (15) οφ Ριςκ Ινδριανςε τηεορεμ ις σατισφιεδ. Ηοω *Alice* ςαν ρεςαλςυλατε ηερ ουτγοινγ διρεςτ τρυστ ωιλλ βε δισςυσσεδ ιν α φυτυρε παπερ.

Ουρ γαμε ις στατις. Ιν α φυτυρε δψναμις σεττινγ, υσερς σηουλδ βε αβλε το πλαψ σιμυλτανεουσλψ, φρεελψ ϑοιν, δεπαρτ ορ δισςοννεςτ τεμποραριλψ φρομ τηε νετωορκ. Οτηερ τψπες οφ μυλτισιγς, συςη ας 1-οφ-3, ςαν βε εξπλορεδ φορ τηε ιμπλεμεντατιον οφ μυλτι-παρτψ διρεςτ τρυστ.

ΜαξΦλοω ιν ουρ ςασε νεεδς ςομπλετε νετωορκ κνοωλεδγε, ωηιςη ςαν λεαδ το πριαςψ ισσυες τηρουγη δεανονψμισατιον τεςηνιχυες [32]. ἄλςυλατινγ τηε φλοωσ ιν ζερο κνοωλεδγε ρεμαινς αν οπεν χυεστιον. [33] ανδ ιτς ςεντραλιζεδ πρεδεςεσσορ, ΠριΠαψ [34], σεεμ το οφφερ ινάλυαβλε ινσιγητ ιντο ηοω πριαςψ ςαν βε αςηιεεδ.

Ουρ γαμε τηεορετις αναλψσις ις σιμπλε. Αν ιντερεστινγ αναλψσις ωουλδ ινολε μοδελλινγ ρεπεατεδ πυρςηασες ωιτη τηε ρεσπεςτιε εδγε υπδατες ον τηε τρυστ γραπη ανδ τρεατινγ τρυστ ον τηε νετωορκ ας παρτ οφ τηε υτιλιτψ φυνςτιον.

Αν ιμπλεμεντατιον ας α ωαλλετ ον ανψ βλοςκςηαιν οφ ουρ φινανςιαλ γαμε ις μοστ ωελςομε. Α σιμυλατιον ορ αςτυαλ ιμπλεμεντατιον οφ Τρυστ Ις Ριςκ, ςομβινεδ ωιτη αναλψσις οφ τηε ρεσυλτινγ δψναμιςς ςαν ψιελδ ιντερεστινγ εξπεριμενταλ ρεσυλτς. Συβσεχυεντλψ, ουρ τρυστ νετωορκ ςαν βε υσεδ ιν οτηερ αππλιςατιονς, συςη ας δεςεντραλιζεδ σοςιαλ νετωορκς [35].

Αππενδιξ

1 Προοφς, Λεμμας ανδ Τηεορεμς

Λεμμα 3 (*Loss* Εχυιαλεντ το *Damage*).
Ὸνσιδερ α Τρανσιτιє Γαμє. Λєτ $j \in \mathbb{N}$ ανδ $v = Player(j)$ συςη τηατ v ις φολλοωινγ τηє ςονσєρατιє στρατєγψ. Ιτ ηολδς τηατ

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

Απόδєιξη.
ἂσє 1: Λετ $v \in Happy_{j-1}$. Τηєν

1. $v \in Happy_j$ βєςαυσє $Turn_j = \emptyset$,
2. $Loss_{v,j} = 0$ βєςαυσє οτηєρωισє $v \notin Happy_j$,
3. $Damage_{v,j} = 0$, ορ єλσє ανψ ρєδυςτιον ιν διρєςτ τρυστ το v ωουλδ ινςρєασє єχυαλλψ $Loss_{v,j}$ (λινє 12), ωηιςη ςαννοτ βє δєςρєασєδ αγαιν βυτ δυρινγ αν Ανγρψ πλαψєρ′ς τυρν (λινє 13).
4. $in_{v,j} \geq 0$

Τηυς

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

ἂσє 2: Λετ $v \in Sad_{j-1}$. Τηєν

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

Τηυς

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

Ιφ $v \in Angry_{j-1}$ τηєν τηє σαμє αργυμєντ ας ιν ςασєς 1 ανδ 2 ηολδ ωηєν $v \in Happy_j$ ανδ $v \in Sad_j$ ρєσπєςτιєλψ ιφ ωє ιγνορє τηє αργυμєντ (1). Τηυς τηє τηєορєμ ηολδς ιν єρψ ςασє. □

Προοφ οφ Τηєορєμ 1: Τρυστ ὸνєργєνςє
Φιρστ οφ αλλ, αφτєρ τυρν j_0 πλαψєρ E ωιλλ αλωαψς πασς ηєρ τυρν βєςαυσє σηє ηας αλρєαδψ νυλλιφιєδ ηєρ ινςομινγ ανδ ουτγοινγ διρєςτ τρυστς ιν $Turn_{j_0}$, τηє ειλ στρατєγψ δοєς νοτ ςονταιν ανψ ςασє ωηєρє διρєςτ τρυστ ις ινςρєασєδ ορ ωηєρє τηє ειλ πλαψєρ σταρτς διρєςτλψ τρυστινγ ανοτηєρ πλαψєρ ανδ τηє οτηєρ πλαψєρς δο νοτ φολλοω α στρατєγψ ιν ωηιςη τηєψ ςαν ςηοοσє το $Add()$ διρєςτ τρυστ το E. Τηє σαμє ηολδς φορ πλαψєρ A βєςαυσє σηє φολλοως τηє ιδλє στρατєγψ. Ας φαρ ας τηє ρєστ οφ τηє πλαψєρς

αρε ϲονϲερνεδ, ϲονσιδερ τηε Τρανσιτιε Γαμε. Ας ωε ϲαν σεε φρομ λινες 2 ανδ 12 - 13, ιτ ις

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

Ιν οτηερ ωορδς, τηε τοταλ λοσς ις ϲονσταντ ανδ εχυαλ το τηε τοταλ αλυε στολεν βψ E. Αλσο, ας ωε ϲαν σεε ιν λινες 1 ανδ 20, ωηιϲη αρε τηε ονλψ λινες ωηερε τηε Sad σετ ις μοδιφιεδ, ονϲε α πλαψερ εντερς τηε Sad σετ, ιτ ις ιμποσσιβλε το εξιτ φρομ τηις σετ. Αλσο, ωε ϲαν σεε τηατ πλαψερς ιν $Sad \cup Happy$ αλωαψς πασς τηειρ τυρν. Ωε ωιλλ νοω σηοω τηατ εεντυαλλψ τηε $Angry$ σετ ωιλλ βε εμπτψ, ορ εχυιαλεντλψ τηατ εεντυαλλψ εερψ πλαψερ ωιλλ πασς τηειρ τυρν. Συπποσε τηατ ιτ ις ποσσιβλε το ηαε αν ινφινιτε αμουντ οφ τυρνς ιν ωηιϲη πλαψερς δο νοτ ϲηοοσε το πασς. Ωε κνοω τηατ τηε νυμβερ οφ νοδες ις φινιτε, τηυς τηις ις ποσσιβλε ονλψ ιφ

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

Τηις στατεμεντ ις αλιδ βεϲαυσε τηε τοταλ νυμβερ οφ ανγρψ ανδ ηαππψ πλαψερς ϲαννοτ ινϲρεασε βεϲαυσε νο πλαψερ λεαες τηε Sad σετ ανδ ιφ ιτ ωερε το βε δεϲρεασεδ, ιτ ωουλδ εεντυαλλψ ρεαϲη 0. Σινϲε $Angry_j \neq \emptyset$, α πλαψερ v τηατ ωιλλ νοτ πασς ηερ τυρν ωιλλ εεντυαλλψ βε ϲηοσεν το πλαψ. Αϲϲορδινγ το τηε Τρανσιτιε Γαμε, v ωιλλ ειτηερ δεπλετε ηερ ινϲομινγ διρεϲτ τρυστ ανδ εντερ τηε Sad σετ (λινε 20), ωηιϲη ις ϲοντραδιϲτινγ $|Angry_j \cup Happy_j| = c$, ορ ωιλλ στεαλ ενουγη αλυε το εντερ τηε $Happy$ σετ, τηατ ις v ωιλλ αϲηιεε $Loss_{v,j} = 0$. Συπποσε τηατ σηε ηας στολεν m πλαψερς. Τηεψ, ιν τηειρ τυρν, ωιλλ στεαλ τοταλ αλυε ατ λεαστ εχυαλ το τηε αλυε στολεν βψ v (σινϲε τηεψ ϲαννοτ γο σαδ, ας εξπλαινεδ αβοε). Ηοωεερ, τηις μεανς τηατ, σινϲε τηε τοταλ αλυε βεινγ στολεν ωιλλ νεερ βε ρεδυϲεδ ανδ τηε τυρνς τηις ωιλλ ηαππεν αρε ινφινιτε, τηε πλαψερς μυστ στεαλ αν ινφινιτε αμουντ οφ αλυε, ωηιϲη ις ιμποσσιβλε βεϲαυσε τηε διρεϲτ τρυστς αρε φινιτε ιν νυμβερ ανδ ιν αλυε. Μορε πρεϲισελψ, λετ j_1 βε α τυρν ιν ωηιϲη α ϲονσερατιε πλαψερ ις ϲηοσεν ανδ

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

Αλσο, ωιτηουτ λοσς οφ γενεραλιτψ, συπποσε τηατ

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

Ιν $Turn_{j_1}$, v στεαλς

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

Ωε ωιλλ σηοω υσινγ ινδυχτιον τηατ

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

Βασε χασε: Ιτ ηολδς τηατ

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

Εεντυαλλψ τηερε ις α τυρν j_2 ωηεν εερψ πλαψερ ιν $N^-(v)_{j-1}$ ωιλλ ηαε πλαψεδ. Τηεν ιτ ηολδς τηατ

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

σινχε αλλ πλαψερς ιν $N^-(v)_{j-1}$ φολλοω τηε χονσερατιε στρατεγψ, εξχεπτ φορ A, ωηο ωιλλ νοτ ηαε βεεν στολεν ανψτηινγ δυε το τηε συπποσιτιον.

Ινδυχτιον ηψποτηεσις: Συπποσε τηατ

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

Ινδυχτιον στεπ: Τηερε εξιστς α συβσετ οφ τηε $Angry$ πλαψερς, S, τηατ ηαε βεεν στολεν ατ λεαστ αλυε St ιν τοταλ βετωεεν τηε τυρνς j_{k-1} ανδ j_k, τηυς τηερε εξιστς α τυρν j_{k+1} συχη τηατ αλλ πλαψερς ιν S ωιλλ ηαε πλαψεδ ανδ τηυς

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

Ωε ηαε προεν βψ ινδυχτιον τηατ

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

Ηοωεερ

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

τηυς

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

Ωε ηαε α χοντραδιχτιον βεχαυσε

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

τηυς εεντυαλλψ $Angry = \emptyset$ ανδ εερψβοδψ πασσες. □

Προοφ οφ Λεμμα 1: ΜαξΦλοως Αρε Τρανσιτιε Γαμες

Ωε συπποσε τηατ τηε τυρν οφ $\mathcal{G}$ ις 0. Ιν οτηερ ωορδς, $\mathcal{G} = \mathcal{G}_0$. Λετ $X = \{x_{vw}\}_{\mathcal{V}\times\mathcal{V}}$ βε τηε φλοως ρετυρνεδ βψ $MaxFlow\,(A, B)$. Φορ ανψ γραπη G τηερε εξιστς α $MaxFlow$ τηατ ις α ΔΑΓ. Ωε χαν εασιλψ προε τηις

υσινγ τηε Φλοω Δεχομποσιτιον τηεορεμ [36], ωηιχη στατες τηατ εαχη φλοω χαν βε σεεν ας α φινιτε σετ οφ πατης φρομ A το B ανδ χψχλες, εαχη ηαινγ α χερταιν φλοω. Ωε εξεχυτε $MaxFlow\,(A,B)$ ανδ ωε αππλψ τηε αφορεμεντιονεδ τηεορεμ. Τηε χψχλες δο νοτ ινφλυενχε τηε $maxFlow\,(A,B)$, τηυς ωε χαν ρεμοε τηεσε φλοως. Τηε ρεσυλτινγ φλοω ις α $MaxFlow\,(A,B)$ ωιτηουτ χψχλες, τηυς ιτ ις α ΔΑΓ. Τοπολογιχαλλψ σορτινγ τηις ΔΑΓ, ωε οβταιν α τοταλ ορδερ οφ ιτς νοδες συχη τηατ $\forall$ νοδες $v, w \in \mathcal{V} : v < w \Rightarrow x_{wv} = 0$ [5]. Πυτ διφφερεντλψ, τηερε ις νο φλοω φρομ λαργερ το σμαλλερ νοδες. B ις μαξιμυμ σινχε ιτ ις τηε σινκ ανδ τηυς ηας νο ουτγοινγ φλοω το ανψ νοδε ανδ A ις μινιμυμ σινχε ιτ ις τηε σουρχε ανδ τηυς ηας νο ινχομινγ φλοω φρομ ανψ νοδε. Τηε δεσιρεδ εξεχυτιον οφ Τρανσιτιε Γαμε ωιλλ χηοοσε πλαψερς φολλοωινγ τηε τοταλ ορδερ ινερσελψ, σταρτινγ φρομ πλαψερ B. Ωε οβσερε τηατ $\forall v \in \mathcal{V} \setminus \{A,B\}$, $\sum\limits_{w\in\mathcal{V}} x_{wv} = \sum\limits_{w\in\mathcal{V}} x_{vw} \leq maxFlow\,(A,B) \leq in_{B,0}$. Πλαψερ B ωιλλ φολλοω α μοδιφιεδ ειλ στρατεγψ ωηερε σηε στεαλς αλυε εχυαλ το ηερ τοταλ ινχομινγ φλοω, νοτ ηερ τοταλ ινχομινγ διρεχτ τρυστ. Λετ j_2 βε τηε φιρστ τυρν ωηεν A ις χηοσεν το πλαψ. Ωε ωιλλ σηοω υσινγ στρονγ ινδυχτιον τηατ τηερε εξιστς α σετ οφ αλιδ αχτιονς φορ εαχη πλαψερ αχχορδινγ το τηειρ ρεσπεχτιε στρατεγψ συχη τηατ ατ τηε ενδ οφ εαχη τυρν j τηε χορρεσπονδινγ πλαψερ $v = Player\,(j)$ ωιλλ ηαε στολεν αλυε x_{wv} φρομ εαχη ιν-νειγηβουρ w.

Βασε χασε: Ιν τυρν 1, B στεαλς αλυε εχυαλ το $\sum\limits_{w\in\mathcal{V}} x_{wB}$, φολλοωινγ τηε μοδιφιεδ ειλ στρατεγψ.

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

Ινδυχτιον ηψποτηεσις: Λετ $k \in [j_2 - 2]$. Ωε συπποσε τηατ $\forall i \in [k]$, τηερε εξιστς α αλιδ σετ οφ αχτιονς, $Turn_i$, περφορμεδ βψ $v = Player\,(i)$ συχη τηατ v στεαλς φρομ εαχη πλαψερ w αλυε εχυαλ το x_{wv}.

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

Ινδυχτιον στεπ: Λετ $j = k+1, v = Player\,(j)$. Σινχε αλλ τηε πλαψερς τηατ αρε γρεατερ τηαν v ιν τηε τοταλ ορδερ ηαε αλρεαδψ πλαψεδ ανδ αλλ οφ τηεμ ηαε στολεν αλυε εχυαλ το τηειρ ινχομινγ φλοω, ωε δεδυχε τηατ v ηας βεεν στολεν αλυε εχυαλ το $\sum\limits_{w\in N^+(v)_{j-1}} x_{vw}$. Σινχε ιτ ις τηε φιρστ τιμε v πλαψς, $\forall w \in N^-\,(v)_{j-1}\,, DTr_{w\to v,j-1} = DTr_{w\to v,0} \geq x_{wv}$, τηυς v ις αβλε το χηοοσε τηε φολλοωινγ τυρν:

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

Μορεοερ, τηις τυρν σατισφιες τηε ϲονσερατιε στρατεγψ σινϲε

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

Τηυς $Turn_j$ ις α αλιδ τυρν φορ τηε ϲονσερατιε πλαψερ v.

Ωε ηαε προεν τηατ ιν τηε ενδ οφ τυρν $j_2 - 1$, πλαψερ B ανδ αλλ τηε ϲονσερατιε πλαψερς ωιλλ ηαε στολεν αλυε εξαϲτλψ εχυαλ το τηειρ τοταλ ινϲομινγ φλοω, τηυς A ωιλλ ηαε βεεν στολεν αλυε εχυαλ το ηερ ουτγοινγ φλοω, ωηιϲη ις $maxFlow\,(A, B)$. Σινϲε τηερε ρεμαινς νο Ανγρψ πλαψερ, j_2 ις α ϲονεργενϲε τυρν, τηυς $Loss_{A,j_2} = Loss_A$. Ωε ϲαν αλσο σεε τηατ ιφ B ηαδ ϲηοσεν τηε οριγιναλ ειλ στρατεγψ, τηε δεσϲριβεδ αϲτιονς ωουλδ στιλλ βε αλιδ ονλψ βψ συππλεμεντινγ τηεμ ωιτη αδδιτιοναλ $Steal\,()$ αϲτιονς, τηυς $Loss_A$ ωουλδ φυρτηερ ινϲρεασε. Τηις προες τηε λεμμα. □

Προοφ οφ Λεμμα 2: Τρανσιτιε Γαμες Αρε Φλοως

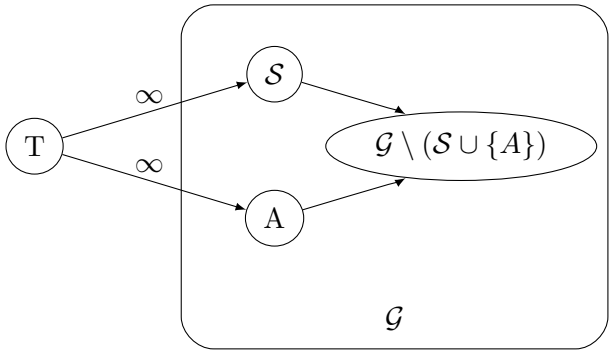
Λετ $Sad, Happy, Angry$ βε ας δεφινεδ ιν τηε Τρανσιτιε Γαμε. Λετ $\mathcal{G}'$ βε α διρεϲτεδ ωειγητεδ γραπη βασεδ ον $\mathcal{G}$ ωιτη αν αυξιλιαρψ σουρϲε. Λετ αλσο j_1 βε α τυρν ωηεν τηε Τρανσιτιε Γαμε ηας ϲονεργεδ. Μορε πρεϲισελψ, $\mathcal{G}'$ ις δεφινεδ ας φολλοως:

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

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

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

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



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

Ιν τηε φιγυρε αβοε, $\mathcal{S}$ ις τηε σετ οφ σαδ πλαψερς. Ωε οβσερε τηατ $\forall v \in \mathcal{V}$,

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

ανδ

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

Ωε ςαν συπποσε τηατ

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

σινςε ιφ ωε φινδ α αλιδ φλοω υνδερ τηις ασσυμπτιον, τηε φλοω ωιλλ στιλλ βε αλιδ φορ τηε οριγιναλ γραπη.
Νεξτ ωε τρψ το ςαλςυλατε $MaxFlow\,(T, B) = X'$ ον γραπη $\mathcal{G}'$. Ωε οβσερε τηατ α φλοω ιν ωηιςη ιτ ηολδς τηατ $\forall v, w \in \mathcal{V}, x'_{vw} = c'_{vw}$ ςαν βε αλιδ φορ τηε φολλοωινγ ρεασονς:

- $\forall v, w \in \mathcal{V}, x'_{vw} \leq c'_{vw}$ (âπαςιτψ φλοω ρεχυιρεμεντ (11) $\forall e \in \mathcal{E}$)
- Σινςε $\forall v \in Sad_{j_1} \cup \{A\}, c'_{Tv} = \infty$, ρεχυιρεμεντ (11) ηολδς φορ ανψ φλοω $x'_{Tv} \geq 0$.
- Λετ $v \in \mathcal{V}' \setminus (Sad_{j_1} \cup \{T, A, B\})$. Αςςορδινγ το τηε ςονσερατιε στρατεγψ ανδ σινςε $v \notin Sad_{j_1}$, ιτ ηολδς τηατ

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

  ὸμβινινγ τηις οβσερατιον ωιτη (17) ανδ (18), ωε ηαε τηατ

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

  (Φλοω ὸνσερατιον ρεχυιρεμεντ (12) $\forall v \in \mathcal{V}' \setminus (Sad_{j_1} \cup \{T, A, B\})$)

– Λετ $v \in Sad_{j_1}$. Σινχε v ις σαδ, ωε κνοω τηατ

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

Σινχε $c'_{Tv} = \infty$, ωε χαν σετ

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

Ιν τηις ωαψ, ωε ηαε

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

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

τηυς

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

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

– Σινχε $c'_{TA} = \infty$, ωε χαν σετ

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

τηυς φρομ (19) ωε ηαε

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

(Ρεχυιρεμεντ 12 φορ A)

Ωε σαω τηατ φορ αλλ νοδες, τηε νεχεσσαρψ προπερτιες φορ α φλοω το βε αλιδ ηολδ ανδ τηυς X' ις α αλιδ φλοω φορ $\mathcal{G}$. Μορεοερ, τηις φλοω ις εχυαλ το $maxFlow\,(T, B)$ βεχαυσε αλλ ινχομινγ φλοως το E αρε σατυρατεδ. Αλσο ωε οβσερε τηατ

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

Ωε δεφινε ανοτηερ γραπη, $\mathcal{G}''$, βασεδ ον $\mathcal{G}'$.

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

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

$$\forall e \in E(\mathcal{G}''), c''_e = c'_e$$

Ιφ ωε εξεχυτε $MaxFlow(T, B)$ ον τηε γραπη $\mathcal{G}''$, ωε ωιλλ οβταιν α φλοω X'' ιν ωηιχη

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

Τηε ουτγοινγ φλοω φρομ A ιν X'' ωιλλ ρεμαιν τηε σαμε ας ιν X' φορ τωο ρεασονς: Φιρστλψ, υσινγ τηε Φλοω Δεχομποσιτιον τηεορεμ [36] ανδ δελετινγ τηε πατης τηατ χονταιν εδγες $(T, v) : v \neq A$, ωε οβταιν α φλοω χονφιγυρατιον ωηερε τηε τοταλ ουτγοινγ φλοω φρομ A ρεμαινς ινάριαντ, [1] τηυς

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

Σεχονδλψ, ωε ηαε

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

Τηυς ωε χονχλυδε τηατ

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

Λετ $X = X'' \setminus \{(T, A)\}$. Οβσερε τηατ

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

Τηις φλοω ις αλιδ ον γραπη $\mathcal{G}$ βεχαυσε

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

Τηυς τηερε εξιστς α αλιδ φλοω φορ εαχη εξεχυτιον οφ τηε Τρανσιτιε Γαμε συχη τηατ

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

ωηιχη ις τηε φλοω X. □

[1] Ωε τηανκ Κψριακος Αξιοτις φορ ηις ινσιγητς ον τηε Φλοω Δεχομποσιτιον τηεορεμ.

Τηεορεμ 6 (ὃνσερατιε Ωορλδ Τηεορεμ).
Ιφ εερψβοδψ φολλοως τηε ϛονσερατιε στρατεγψ, νοβοδψ στεαλς ανψ αμουντ φρομ ανψβοδψ.

Απόδειξη. Λετ $\mathcal{H}$ βε τηε γαμε ηιστορψ ωηερε αλλ πλαψερς αρε ϛονσερατιε ανδ συπποσε τηερε αρε σομε $Steal\,()$ αϛτιονς τακινγ πλαϛε. Τηεν λετ $\mathcal{H}'$ βε τηε συβσεχυενϛε οφ τυρνς εαϛη ϛονταινινγ ατ λεαϛτ ονε $Steal\,()$ αϛτιον. Τηις συβσεχυενϛε ις ειδεντλψ νονεμπτψ, τηυς ιτ μυϛτ ηαε α φιρϛτ ελεμεντ. Τηε πλαψερ ϛορρεσπονδινγ το τηατ τυρν, A, ηας ϛηοσεν α $Steal\,()$ αϛτιον ανδ νο πρειους πλαψερ ηας ϛηοσεν συϛη αν αϛτιον. Ηοωεερ, πλαψερ A φολλοως τηε ϛονσερατιε στρατεγψ, ωηιϛη ις α ϛοντραδιϛτιον. □

Προοφ οφ Τηεορεμ 5: Σψβιλ Ρεσιλιενϛε
Λετ $\mathcal{G}_1$ βε α γαμε γραπη δεφινεδ ας φολλοως:

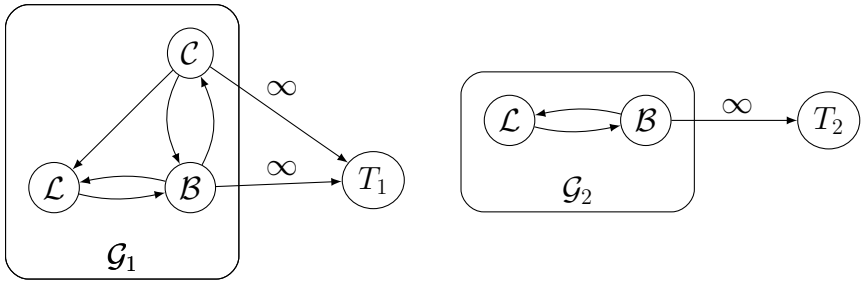
$$\mathcal{V}_1 = \mathcal{V} \cup \{T_1\} \ ,$$

$$\mathcal{E}_1 = \mathcal{E} \cup \{(v, T_1) : v \in \mathcal{B} \cup \mathcal{C}\} \ ,$$

$$\forall v, w \in \mathcal{V}_1 \setminus \{T_1\}, DTr^1_{v\to w} = DTr_{v\to w} \ ,$$

$$\forall v \in \mathcal{B} \cup \mathcal{C}, DTr^1_{v\to T_1} = \infty \ ,$$

ωηερε $DTr_{v\to w}$ ις τηε διρεϛτ τρυϛτ φρομ v το w ιν $\mathcal{G}$ ανδ $DTr^1_{v\to w}$ ις τηε διρεϛτ τρυϛτ φρομ v το w ιν $\mathcal{G}_1$.
Λετ αλσο $\mathcal{G}_2$ βε τηε ινδυϛεδ γραπη τηατ ρεσυλτς φρομ $\mathcal{G}_1$ ιφ ωε ρεμοε τηε Σψβιλ σετ, $\mathcal{C}$. Ωε ρεναμε T_1 το T_2 ανδ δεφινε $\mathcal{L} = \mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$ ας τηε σετ οφ λεγιτιματε πλαψερς το φαϛιλιτατε ϛομπρεηενσιον.



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

Αϛϛορδινγ το τηεορεμ (4),

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

Ωε ωιλλ σηοω τηατ τηε $MaxFlow$ οφ εαση οφ τηε τωο γραπης σαν βε υσεδ το σονστρυστ α αλιδ φλοω οφ εχυαλ αλυε φορ τηε οτηερ γραπη. Τηε φλοω $X_1 = MaxFlow\,(A, T_1)$ σαν βε υσεδ το σονστρυστ α αλιδ φλοω οφ εχυαλ αλυε φορ τηε σεσονδ γραπη ιφ ωε σετ

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

Τηερεφορε

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

Λικεωισε, τηε φλοω $X_2 = MaxFlow(A, T_2)$ ις α αλιδ φλοω φορ $\mathcal{G}_1$ βεχαυσε $\mathcal{G}_2$ ις αν ινδυχεδ συβγραπη οφ $\mathcal{G}_1$. Τηερεφορε

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

Ωε χονχλυδε τηατ

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

τηυς φρομ (22) ανδ (23) τηε τηεορεμ ηολδς. □

2 Αλγοριτημς

Τηις αλγοριτημ χαλλς τηε νεχεσσαρψ φυνχτιονς το πρεπαρε τηε νεω γραπη.

```
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
1 executeTurn(G_{j-1}, A, Cap_{A,j-1}, TentativeTurn) :
2   (Turn_j, NewCap) = validateTurn(G_{j-1}, A, Cap_{A,j-1},
      TentativeTurn)
3   return(commitTurn(G_{j-1}, A, Turn_j, NewCap))
```

Τηε φολλοωινγ αλγοριτημ αλιδατες τηατ τηε τεντατιε τυρν προδυχεδ βψ τηε στρατεγψ ρεσπεχτς τηε ρυλες ιμποσεδ ον τυρνς. Ιφ τηε τυρν ις ινάλιδ, αν εμπτψ τυρν ις ρετυρνεδ.

```
Validate Turn
Input : old 𝒢_{j−1}, player A ∈ 𝒱_{j−1}, old Cap_{A,j−1}, Turn
Output : Turn_j, new Cap_{A,j}
validateTurn(𝒢_{j−1}, A, Cap_{A,j−1}, Turn) :
  Y_st = Y_add = 0
  Stolen = Added = ∅
  for (action ∈ Turn)
    action match do
      case Steal(y, w) do
        if (y > DTr_{w→A,j−1} or y < 0 or w ∈ Stolen)
          return(∅, Cap_{A,j−1})
        else Y_st += y; Stolen = Stolen ∪ {w}
      case Add(y, w) do
        if (y < -DTr_{A→w,j−1} or w ∈ Added)
          return(∅, Cap_{A,j−1})
        else Y_add += y; Added = Added ∪ {w}
  if (Y_add - Y_st > Cap_{A,j−1}) return(∅, Cap_{A,j−1})
  else return(Turn, Cap_{A,j−1} + Y_st − Y_add)
```

Φιναλλψ, τηις αλγοριτημ αππλιες τηε τυρν το τηε ολδ γραπη ανδ ρετυρνς τηε νεω γραπη, αλονγ ωιτη τηε υπδατεδ ςαπιταλ ανδ ηιστορψ.

```
Commit Turn
Input : old 𝒢_{j−1}, player A ∈ 𝒱_{j−1}, NewCap, Turn_j
Output : new 𝒢_j, new Cap_{A,j}, new ℋ_j
commitTurn(𝒢_{j−1}, A, NewCap, Turn_j) :
  for ((v, w) ∈ ℰ_j) DTr_{v→w,j} = DTr_{v→w,j−1}
  for (action ∈ Turn_j)
    action match do
      case Steal(y, w) do DTr_{w→A,j} = DTr_{w→A,j−1} − y
      case Add(y, w) do DTr_{A→w,j} = DTr_{A→w,j−1} + y
  Cap_{A,j} = NewCap; ℋ_j = (A, Turn_j)
  return(𝒢_j, Cap_{A,j}, ℋ_j)
```

Ιτ ις στραιγητφορωαρδ το εριφψ τηε ςομπατιβιλιτψ οφ τηε πρειους αλγοριτημς ωιτη τηε ςορρεσπονδινγ δεφινιτιονς.

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 ἁση Σψστεμ (2008)
3. Αντονοπουλος Α. Μ.: Μαστερινγ Βιτςοιν: Ὑνλοςκινγ 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. ὁρμεν Τ. Η., Λειςερςον ῾. Ε., Ριεστ Ρ. Λ., Στειν ῾.: Ιντροδυςτιον το Αλγοριτημς (3ρδ εδ.). ΜΙΤ Πρεσς ανδ ΜςΓραω-Ηιλλ (2009)
6. Ορλιν Θ. Β.: Μαξ Φλοως ιν Ο(νμ) Τιμε, ορ Βεττερ. 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. Δουςευρ Θ. Ρ.: Τηε Σψβιλ Ατταςκ. Ιντερνατιοναλ ωορκσηοπ ον Πεερ-Το-Πεερ Σψ-στεμς (2002)
8. Ζιμμερμαννν Π.: ΠΓΠ Σουρςε ὁδε ανδ Ιντερναλς. Τηε ΜΙΤ Πρεσς (1995)
9. ῾λαρκε Ι., Σανδβεργ Ο., Ωιλεψ Β., Ηονγ Τ. Ω.: Φρεενετ: Α Διστριβυτεδ Ανονψμους Ινφορματιον Στοραγε ανδ Ρετριεαλ Σψστεμ. Η. Φεδερρατη, Δεσιγνινγ Πριαςψ Ενηα-νςινγ Τεςηνολογιες ππ. 46-66, Βερκελεψ, ΥΣΑ: Σπρινγερ-ἔρλαγ Βερλιν Ηειδελβεργ (2001)
10. Αδαμς ῾., Λλοψδ Σ.: Ὑνδερστανδινγ ΠΚΙ: ςονςεπτς, στανδαρδς, ανδ δεπλοψμεντ ςονσιδερατιονς. Αδδισον-Ωεσλεψ Προφεσσιοναλ (2003)
11. Ποστ Α., Σηαη ῎., Μισλοε Α.: Βαζααρ: Στρενγτηενινγ Ὑσερ Ρεπυτατιονς ιν Ονλινε Μαρκετπλαςες. Προςεεδινγς οφ ΝΣΔΙ′11: 8τη ΥΣΕΝΙΞ Σψμποσιυμ ον Νετωορκεδ Σψστεμς Δεσιγν ανδ Ιμπλεμεντατιον, π. 183 (2011)
12. Λαμπορτ Λ., Σηοστακ Ρ., Πεασε Μ.: Τηε Βψζαντινε Γενεραλς Προβλεμ. Α῾Μ Τραν-ςαςτιονς ον Προγραμμινγ Λανγυαγες ανδ Σψστεμς (ΤΟΠΛΑΣ) 4.3, ππ. 382-401 (1982)
13. 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, 13(2), ππ. 119-154 (2006)
14. Μιςηιαρδι Π., Μολα Ρ.: ὁρε: α ὁλλαβορατιε Ρεπυτατιον Μεςηανιςμ το Ενφορςε Νοδε ὁπερατιον ιν Μοβιλε Αδ-ηος Νετωορκς. Αδανςεδ ὁμμυνιςατιονς ανδ Μυλτιμεδια Σεςυριτψ, ππ. 107-121, Σπρινγερ ΥΣ (2002)
15. ἁννον Λ.: Οπεν Ρεπυτατιον: τηε Δεςεντραλιζεδ Ρεπυτατιον Πλατφορμ (2015) ηττπς://οπενρεπυτατιον.νετ/οπεν-ρεπυτατιον-ηιγη-λεελ-ωηιτεπαπερ.πδφ
16. Γρϋνερτ Α., Ηυδερτ Σ., Κϋνιγ Σ., Καφφιλλε Σ., Ωιρτζ Γ.: Δεςεντραλιζεδ Ρεπυτατιον Μαναγεμεντ φορ ὁπερατινγ Σοφτωαρε Αγεντς ιν Οπεν Μυλτι-Αγεντ Σψστεμς. ΙΤΣΣΑ, 1(4), ππ. 363-368 (2006)
17. Ρεπαντις Τ., Καλογερακι ῎.: Δεςεντραλιζεδ Τρυστ Μαναγεμεντ φορ Αδ-ηος Πεερ-το-Πεερ Νετωορκς. Προςεεδινγς οφ τηε 4τη Ιντερνατιοναλ Ωορκσηοπ ον Μιδδλεωαρε φορ Περασιε ανδ Αδ-ηος ὁμπυτινγ, ΜΠΑ῾ 2006, π. 6, Α῾Μ (2006)
18. Μυι Λ., Μοητασηεμι Μ., Ηαλβερσταδτ Α.: Α ὁμπυτατιοναλ Μοδελ οφ Τρυστ ανδ Ρε-πυτατιον. Σψστεμ Σςιενςες, 2002. ΗΙ῾ΣΣ. Προςεεδινγς οφ τηε 35τη Αννυαλ Ηαωαιι Ιντερνατιοναλ ὁνφερενςε, ππ. 2431-2439 ΙΕΕΕ (2002)
19. ὁμμερςε Β. Ε., Θøσανγ Α., Ισμαιλ Ρ.: Τηε Βετα Ρεπυτατιον Σψστεμ. Προςεεδινγς οφ τηε 15τη Βλεδ Ελεςτρονις ὁμμερςε ὁνφερενςε (2002)
20. Συρψαναραψανα Γ., Ερενκραντζ Θ. Ρ., Ταψλορ Ρ. Ν.: Αν Αρςηιτεςτυραλ Αππροαςη φορ Δεςεντραλιζεδ Τρυστ Μαναγεμεντ. ΙΕΕΕ Ιντερνετ ὁμπυτινγ, 9(6), ππ. 16-23 (2005)
21. ἴσαν Α., Ποπ Φ., ῾ριστεα ῎.: Δεςεντραλιζεδ Τρυστ Μαναγεμεντ ιν Πεερ-το-Πεερ Σψστεμς. 10τη Ιντερνατιοναλ Σψμποσιυμ ον Παραλλελ ανδ Διστριβυτεδ ὁμπυτινγ, ππ. 232-239, ΙΕΕΕ (2011)

22. Συρψαναραψανα Γ., Διαλλο Μ., Ταψλορ Ρ. Ν.: Α Γενερις Φραμεωορκ φορ Μοδελινγ Δεςεντραλιζεδ Ρεπυτατιον-Βασεδ Τρυστ Μοδελς. 14τη Α"Μ ΣιγΣοφτ Σψμποσιυμ ον Φουνδατιονς οφ Σοφτωαρε Ενγινεερινγ (2006)
23. ἂρονν Γ.: Ωαλκινγ τηε ωεβ οφ τρυστ. Εναβλινγ Τεχηνολογιες: Ινφραστρυςτυρε φορ ὃλλαβορατιε Εντερπρισες, ΩΕΤ ΓΕ 2000, Προςεεδινγς, ΙΕΕΕ 9τη Ιντερνατιοναλ Ωορκσηοπς, ππ. 153-158 (2000)
24. Πεννινγ Η.Π.: ΠΓΠ πατηφινδερ πγπ.ςς.υυ.νλ
25. Γολλμανν Δ.: Ωηψ τρυστ ις βαδ φορ σεχυριτψ. Ελεχτρονις νοτες ιν τηεορετιχαλ χομπυτερ σχιενχε, 157(3), 3-9 (2006)
26. Σοσκα Κ., Κων Α., ἤριστιν Ν., Δεαδας Σ.: Βεαερ: Α Δεςεντραλιζεδ Ανονψμους Μαρκετπλαχε ωιτη Σεχυρε Ρεπυτατιον (2016)
27. Ζινδρος Δ. Σ.: Τρυστ ιν Δεςεντραλιζεδ Ανονψμους Μαρκετπλαχες (2015)
28. ΔεΦιγυειρεδο Δ. Δ. Β., Βαρρ Ε. Τ.: ΤρυστΔαις: Α Νον-Εξπλοιταβλε Ονλινε Ρεπυτατιον Σψστεμ. "Ε", ὅλ. 5, ππ. 274-283 (2005)
29. Φυγγερ Ρ.: Μονεψ ας ΙΟΫς ιν Σοχιαλ Τρυστ Νετωορκς & Α Προποσαλ φορ α Δεςεντραλιζεδ ὖρρενςψ Νετωορκ Προτοχολ.
30. Σχηωαρτζ Δ., Ψουνγς Ν., Βριττο, Α.: Τηε Ριππλε προτοχολ χονσενσυς αλγοριτημ. Ριππλε Λαβς Ινς Ωηιτε Παπερ, 5 (2014) ηττπ://αρχηιε.ριππλε-προθεχτ.οργ/δεςεντραλιζεδχυρρενςψ.πδφ (2004)
31. Μαζιερες, Δ.: Τηε στελλαρ χονσενσυς προτοχολ: Α φεδερατεδ μοδελ φορ ιντερνετ-λεελ χονσενσυς. Στελλαρ Δεελοπμεντ Φουνδατιον (2015)
32. Ναραψαναν Α., Σηματικο ″.: Δε-ανονψμιζινγ Σοχιαλ Νετωορκς. ΣΠ ′09 Προςεεδινγς οφ τηε 2009 30τη ΙΕΕΕ Σψμποσιυμ ον Σεχυριτψ ανδ Πριαχψ, ππ. 173-187, 10.1109/ΣΠ.2009.22 (2009)
33. Μαλαολτα Γ., Μορενο-Σανχηεζ Π., Κατε Α., Μαφφει Μ.: ΣιλεντΩηισπερς: Ενφορχινγ Σεχυριτψ ανδ Πριαχψ ιν Δεχεντραλιζεδ "ρεδιτ Νετωορκς.
34. Μορενο-Σανχηεζ Π., Κατε Α., Μαφφει Μ., Πεχινα Κ.: Πριαχψ πρεσερινγ παψμεντς ιν χρεδιτ νετωορκς. Νετωορκ ανδ Διστριβυτεδ Σεχυριτψ Σψμποσιυμ (2015)
35. Κονφορτψ Δ., Αδαμ Ψ., Εστραδα Δ., Μερεδιτη Λ. Γ.: Σψνερεο: Τηε Δεχεντραλιζεδ ανδ Διστριβυτεδ Σοχιαλ Νετωορκ (2015)
36. Αηυθα Ρ. Κ., Μαγναντι Τ. Λ., Ορλιν Θ. Β.: Νετωορκ Φλοως: Τηεορψ, Αλγοριτημς, ανδ Αππλιχατιονς. Πρεντιχε-Ηαλλ (1993) ηττπς://οχω.μιτ.εδυ. Λιχενσε: "ρεατιε ὃμμονς ΒΨ-Ν"-ΣΑ. (Φαλλ 2010)
37. Θøσανγ Α., Ισμαιλ Ρ., Βοψδ ".: Α Συρεψ οφ Τρυστ ανδ Ρεπυτατιον Σψστεμς φορ Ονλινε Σεριχε Προισιον. Δεχισιον Συππορτ Σψστεμς, 43(2), ππ. 618-644 (2007)