

# 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 ο κάθε χρήστης στους υπόλοιπους είναι μετρήσιμη και εκφράζεται με νομισματικούς όρους. Εισάγουμε ένα νέο μοντέλο για πορτοφόλια bitcoin στα οποία τα νομίσματα κάθε χρήστη μοιράζονται σε αξιόπιστους 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 έναν ψευδώνυμο πωλητή 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

Περιεχόμενα .....	8
Κατάλογος Σχημάτων .....	8
Κατάλογος Ψευδοκωδίκων .....	8
1 Εισαγωγή .....	9
2 Λειτουργία .....	12
3 Ο γράφος εμπιστοσύνης .....	13
Ορισμός Γράφου .....	13
Ορισμός Παικτών .....	13
Ορισμός Κεφαλαίου .....	13
Ορισμός Άμεσης Εμπιστοσύνης .....	13
Ορισμός Γειτονιάς .....	14
Ορισμός Ολικής Εισερχόμενης/Εξερχόμενης Άμεσης Εμπιστοσύνης .....	14
Ορισμός Περιουσίας .....	14
4 Η Εξέλιξη της Εμπιστοσύνης .....	15
Ορισμός Γύρων .....	15
Ορισμός Προηγούμενου/Επόμενου Γύρου .....	15
Ορισμός Ζημίας .....	16
Ορισμός Ιστορίας .....	16
5 Μεταβατικότητα Εμπιστοσύνης .....	17
Ορισμός Αδρανούς Στρατηγικής .....	17
Ορισμός Καχιάς Στρατηγικής .....	18
Ορισμός Συντηρητικής Στρατηγικής .....	18
6 Τρυστ Φλω .....	21
Ινδιρεστ Τρυστ Δεφινιτιον .....	21
Τρυστ Φλω Τηορεμ .....	22
Ρισκ Ιναριανσε Τηορεμ .....	23
7 Σψβιλ Ρεσιλιενσε .....	24
Ινδιρεστ Τρυστ το Μυλτιπλε Πλαψερς Δεφινιτιον .....	24
Μυλτι-Πλαψερ Τρυστ Φλω Τηορεμ .....	24
δρρυπτεδ Σετ Δεφινιτιον .....	24
Σψβιλ Σετ Δεφινιτιον .....	24
δλλυσιον Δεφινιτιον .....	25
8 Ρελατεδ Ωορκ .....	26
9 Φυρτηερ Ρεσεαρση .....	27
1 Προοφς, Λεμμας ανδ Τηορεμς .....	27

2	Αλγοριθμησ.....	37
---	-----------------	----

## Κατάλογος Σχημάτων

Απλοί Γράφοι .....	9
UTXO.....	14
Γύρος .....	16
Παράδειγμα μεταβατικού παιχνιδιού.....	20
Συνεργασία.....	25
Τα μεταβατικά παιχνίδια είναι Ροές .....	32
Αντοχή σε επιθέσεις Sybil .....	36

## Κατάλογος Ψευδοκωδικών

Trust Is Risk Game .....	17
Idle Strategy .....	17
Evil Strategy .....	18
Conservative Strategy .....	18
Transitive Game .....	19
Execute Turn.....	37
Validate Turn .....	37
Commit Turn .....	38

## 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 πωλητή και πελάτη 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 ο 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 άδιστα, 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: Ο A εμπ. έμμεσα τον C 10฿    Σχ. 2: Ο 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 έναν από δύο προκαθορισμένους 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 οποιοσδήποτε από τους δύο χρήστες μπορεί να ξοδέψει τα νομίσματα. Ωστόσο, έχει σημασία ποιος χρήστης καταθέτει τα χρήματα αρχικά στον κοινό λογαριασμό – αυτός ο χρήστης διακινδυνεύει τα νομίσματά του.

Η προσέγγισή μας αλλάζει την εμπειρία του χρήστη κατά έναν διακριτικό αλλά και δραστικό τρόπο. Ο χρήστης δεν πρέπει να βασίζεται στην εμπιστοσύνη του 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 0-από-2 διευθύνσεις multisig μοιραζόμενες με φίλους 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 κάποιο 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 εκτινόταν πριν την αγορά. Ο υπαρκτός εθελούσιος κίνδυνος είναι ακριβώς εκείνος που η *Alice* έπαιρνε μοιραζόμενη τα νομίσματά της με τους αξιόπιστους φίλους της. Αποδεικνύουμε το απο-

τέλεσμα αυτό στο θεώρημα Αμετάβλητου Κινδύνου (3). Προφανώς δε θα είναι ασφαλές για την *Alice* να αγοράσει οτιδήποτε από τον *Charlie* ή από οποιονδήποτε άλλο πωλητή αν δεν έχει ήδη εμπιστευθεί καθόλου χρήματα σε κανέναν άλλο χρήστη.

Βλέπουμε ότι στο *Trust Is Risk* τα χρήματα δεν επενδύονται τη στιγμή της αγοράς και κατ' ευθείαν στον πωλητή, 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* Αντίστασης (5).

Κάνουμε τη σχεδιαστική επιλογή ότι κανείς μπορεί να εκφράζει την εμπιστοσύνη του μεγιστικά με όρους του διαθέσιμου του κεφαλαίου. Έτσι, ένας φτωχός παίκτης δεν μπορεί να διαθέσει πολλή άμεση εμπιστοσύνη στους φίλους τους ανεξαρτήτως του πόσο αξιόπιστοι είναι. Από την άλλη, ένας πλούσιος παίκτης μπορεί να εμπιστευθεί ένα μικρό μέρος των χρημάτων της σε κάποιον παίκτη που δεν εμπιστεύεται εκτενώς και παρ' όλα αυτά να εμφανίζει περισσότερη άμεση εμπιστοσύνη από τον φτωχό παίκτη του προηγούμενου παραδείγματος. Δεν υπάρχει άνω όριο στην εμπιστοσύνη. Κάθε παίκτης περιορίζεται μόνο από τα χρήματά του. Έτσι εκμεταλλευόμαστε την παρακάτω αξιωσημείωτη ιδιότητα του χρήματος: Το ότι κανονικοποιεί τις υποκειμενικές ανθρώπινες επιθυμίες σε αντικειμενική αξία.

Υπάρχουν διάφορα κίνητρα για να συνδεθεί ένας χρήστης στο δίκτυο αυτό. Πρώτον, έχει πρόσβαση σε καταστήματα που αλλιώς θα ήταν απρόσιτα. Επίσης, δύο φίλοι μπορούν να επισημοποιήσουν την αλληλοεμπιστοσύνη τους εμπιστεύοντας το ίδιο ποσό ο ένας στον άλλο. 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 τους πολίτες της με χρήματα και να τους αντιμετωπίσει με ένα ανάλογο νομικό οπλοστάσιο αν αυτοί 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 αξιωσημείωτο 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 10฿, 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 10฿ από το κανονικό bitcoin πορτοφόλι της, εμπιστεύοντας 2฿ στον *Bob* και 5฿ στον *Charlie*. Τώρα ελέγχει αποκλειστικά 3฿ και διακινδυνεύει 7฿ με αντάλλαγμα το να είναι μέρος του δικτύου. Έχει πλήρη αλλά όχι αποκλειστική πρόσβαση στα 7฿ που εμπιστεύθηκε στους φίλους της και αποκλειστική πρόσβαση στα υπόλοιπα 3฿, που αθροίζονται στα 10฿.

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 1฿ και ελέγχει την αξιοπιστία του *Dean* μέσω του νέου της πορτοφολιού. Ας υποθέσουμε ότι ο *Dean* προκύπτει αξιόπιστος μέχρι 4฿. Αφού το 1฿ είναι λιγότερο από τα 4฿, η *Alice* πραγματοποιεί την αγορά μέσω του καινούριου της πορτοφολιού με σιγουριά.

Τότε βλέπει στο πορτοφόλι της ότι τα αποκλειστικά της νομίσματα αυξήθηκαν στα 6฿, τα νομίσματα που εμπιστεύεται στον *Bob* και στον *Charlie* μειώθηκαν στα 0.5฿ και 2.5฿ αντίστοιχα και ότι εμπιστεύεται τον *Dean* με 1฿, 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 4฿. Στο παρασκήνιο, το πορτοφόλι της ανακατένιμε 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 *Bob* και τον *Charlie*, θέτοντας τα νομίσματα άμεσης εμπιστοσύνης στα 2฿ και στα 5฿ αντίστοιχα και πάλι. Η *Alice* τώρα ελέγχει αποκλειστικά 2฿. Συνεπώς τώρα μπορεί να χρησιμοποιήσει συνολικά 9฿, γεγονός αναμενόμενο, αφού έπρεπε να πληρώσει 1฿ 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  $c_j : \mathcal{E}_j \rightarrow \mathbb{R}^+$ .

Οι κόμβοι αναπαριστούν τους 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 (Παίχτες).** Το σύνολο  $\mathcal{V}_j = \mathcal{V}(\mathcal{G}_j)$  είναι το σύνολο όλων των παικτών στο δίκτυο. Το σύνολο αυτό μπορεί να ειπωθεί 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 του  $A$  στο γύρο  $j$ ,  $Cap_{A,j}$ , ορίζεται ως τα συνολικά νομίσματα που ανήκουν αποκλειστικά στον  $A$  στην αρχή του γύρου  $j$ .

Το κεφάλαιο είναι η αξία που υπάρχει στο παιχνίδι αλλά δεν είναι μοιραζόμενη με έμπιστους τρίτους. Το κεφάλαιο ενός παίκτη μπορεί να ανακατανεμηθεί μόνο κατά τη διάρκεια των γύρων του, σύμφωνα με τις πράξεις του. 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.

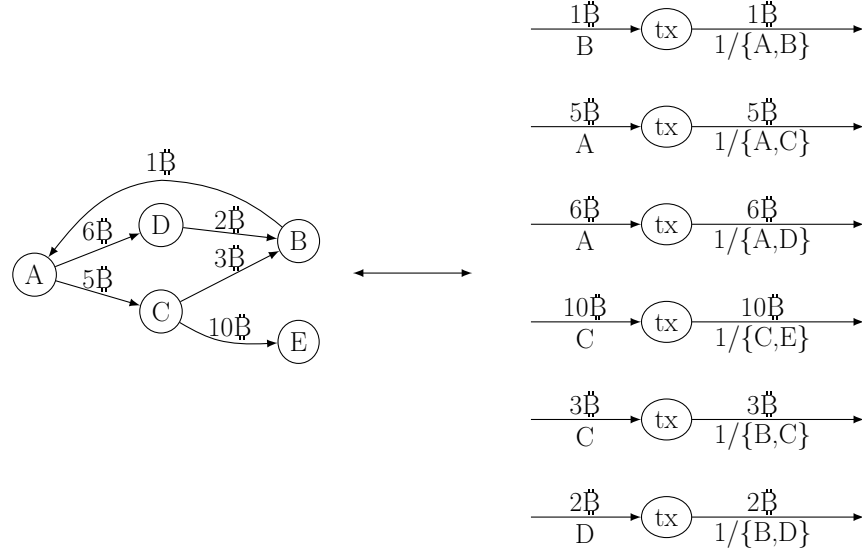
Ο ορισμός της άμεσης εμπιστοσύνης ακολουθεί:

**Ορισμός 4 (Άμεση Εμπιστοσύνη).** Η άμεση εμπιστοσύνη από τον  $A$  στον  $B$  στο τέλος του γύρου  $j$ ,  $DTr_{A \rightarrow B,j}$ , 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 τον  $A$ .

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

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 ο  $A$  εμπιστεύεται άμεσα και  $N^-(A)_j$  για τους κόμβους που εμπιστεύονται άμεσα τον  $A$  στο τέλος του γύρου  $j$ .

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

Αυτές καλούνται έξω και μέσα γειτονιές του  $A$  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.

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

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

$$As_{A,j} = Cap_{A,j} + out_{A,j} \quad (4)$$

#### 4 Η Εξέλιξη της Εμπιστοσύνης

**Ορισμός 8 (Γύροι).** Σε κάθε γύρο  $j$  ένας 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 τον  $B \in N^-(A)_{j-1}$ , όπου  $0 \leq y_B \leq DTr_{B \rightarrow A, j-1}$ . Τότε:

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

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

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

Όταν  $y_B < 0$ , θα λέμε ότι ο  $A$  μειώνει την άμεση εμπιστοσύνη του προς τον  $B$  κατά  $-y_B$ . Όταν  $y_B > 0$ , θα λέμε ότι ο  $A$  αυξάνει την άμεση εμπιστοσύνη του προς τον  $B$  κατά  $y_B$ . Αν  $DTr_{A \rightarrow B, j-1} = 0$ , τότε λέμε ότι ο  $A$  αρχίζει να εμπιστεύεται άμεσα τον  $B$ . Ο  $A$  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 τον  $A$  στο γύρο της  $j$ . Για να είναι ένας γύρος δυνατός, θα πρέπει

$$Y_{add} - Y_{st} \leq Cap_{A, j-1} \quad (5)$$

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

Ένας παίκτης δεν μπορεί να επιλέξει δύο πράξεις της ίδιας κατηγορίας προς τον ίδιο 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

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

Η πράξη  $Steal$  απαιτεί  $0 \leq x \leq DTr_{B \rightarrow A, j-1}$ , οι πράξεις  $Add$  απαιτούν  $DTr_{A \rightarrow C, j-1} \geq -y$  και  $DTr_{A \rightarrow D, j-1} \geq -w$  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 τον  $Player(j)$ .

**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 ο  $A$  επιλέγεται να παίξει αντίστοιχα. Αν ο πρώτος γύρος που παίζει ο  $A$  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:

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

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

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

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

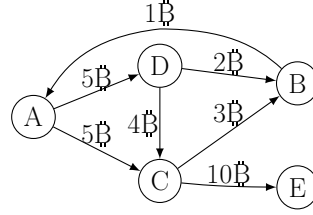
Λέμε ότι κλάπηκε από τον  $A$  αξία  $Damage_{A,j}$  ανάμεσα στον  $prev(j)$  και στον  $j$ . Παραλείπουμε τους δείκτες γύρων όταν εννοούνται από τα συμφραζόμενα.

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

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

Γνώση του αρχικού γράφου  $\mathcal{G}_0$ , τα αρχικά κεφάλαια όλων των παικτών και την ιστορία ισοδυναμούν με πλήρη κατανόηση της εξέλιξης του παιχνιδιού. Χτίζοντας στο παράδειγμα του σχήματος 3, μπορούμε να δούμε το γράφο που προκύπτει όταν ο  $D$  παίζει

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



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 έναν παίκτη, λαμβάνει το γύρο που ο παίκτης αυτός επιθυμεί να παίξει και, αν ο γύρος του είναι έγκυρος, τον εκτελεί. Αυτά τα βήματα επαναλαμβάνονται επ' άοριστον. Θεωρούμε ότι οι παίκτες επιλέγονται με τέτοιο τρόπο που ένας παίκτης, μετά από τον γύρο του, τελικά θα ξαναπαίξει αργότερα.

#### Trust Is Risk Game

```

1 j = 0
2 while (True)
3   j += 1;  $A \xleftarrow{\$} \mathcal{V}_j$ 
4   Turn = strategy[A]( $\mathcal{G}_0$ , A, CapA,0,  $\mathcal{H}_{1..j-1}$ )
5   ( $\mathcal{G}_j$ , CapA,j,  $\mathcal{H}_j$ ) = executeTurn( $\mathcal{G}_{j-1}$ , A, CapA,j-1, Turn)
  
```

Η `strategy[A]()` προσφέρει στον 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 έναν τίμιο παίκτη όταν κάποιος άλλος παίκτης αποφασίζει να φύγει από το δίκτυο με τα χρήματά του και όλα τα χρήματα που άλλοι εμπιστεύονται άμεσα σε αυτόν.

**Ορισμός 12 (Αδρανής Στρατηγική (Idle Strategy)).** Ένας παίκτης  $A$  ακολουθεί την αδρανή στρατηγική αν παίζει “πάσο” στο γύρο του.

#### Idle Strategy

Input : graph  $\mathcal{G}_0$ , player  $A$ , capital Cap<sub>A,0</sub>, history ( $\mathcal{H}$ )<sub>1...j-1</sub>

```

Output :  $Turn_j$ 
1 idleStrategy( $\mathcal{G}_0, A, Cap_{A,0}, \mathcal{H}$ ) :
2   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).** Ένας παίκτης  $A$  ακολουθεί την κακιά στρατηγική αν στο γύρο του κλέβει όλη την εισερχόμενη άμεση εμπιστοσύνη και μηδενίζει όλη την εξερχόμενη άμεση εμπιστοσύνη.

```

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

```

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

```

1 consStrategy( $\mathcal{G}_0, A, Cap_{A,0}, \mathcal{H}$ ) :
2   Damage =  $out_{A, prev(j)} - out_{A, j-1}$ 
3   if (Damage > 0)
4     if (Damage >=  $in_{A, j-1}$ )
5        $Turn_j = \bigcup_{v \in N^-(A)_{j-1}} \{Steal(DTr_{v \rightarrow A, j-1}, v)\}$ 
6     else
7        $y = SelectSteal(G_j, A, Damage) \# y = \{y_v : v \in N^-(A)_{j-1}\}$ 
8        $Turn_j = \bigcup_{v \in N^-(A)_{j-1}} \{Steal(y_v, v)\}$ 
9     else  $Turn_j = \emptyset$ 
10    return( $Turn_j$ )

```

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

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

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

Όπως βλέπουμε, ο ορισμός καλύπτει μια πληθώρα επιλογών για τον συντηρητικό παίκτη, αφού στην περίπτωση που  $0 < \text{Damage}_{A,j} < \text{in}_{A,j-1}$  μπορεί να επιλέξει να καταναίμει τις πράξεις  $\text{Steal}()$  όπως επιθυμεί.

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

Συνεχίζουμε με μία δυνατή εξέλιξη του παιχνιδιού, το Μεταβατικό Παιχνίδι. Στο γύρο 0, υπάρχει ήδη ένα συγκεκριμένο δίκτυο. Όλοι οι παίκτες εκτός του  $A$  και του  $B$  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 συντηρητικός παίκτης μπορεί να βρίσκεται σε μία από τρεις καταστάσεις: Χαρούμενος (Happy), Θυμωμένος (Angry) ή Λυπημένος (Sad). Οι Χαρούμενοι παίκτες έχουν ζημία 0, οι Θυμωμένοι παίκτες έχουν θετική ζημία και θετική εισερχόμενη άμεση εμπιστοσύνη, άρα μπορούν να αναπληρώσουν τη ζημία τους τουλάχιστον μερικώς και οι Λυπημένοι 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 =  $\mathcal{V} \setminus \{A, B\}$

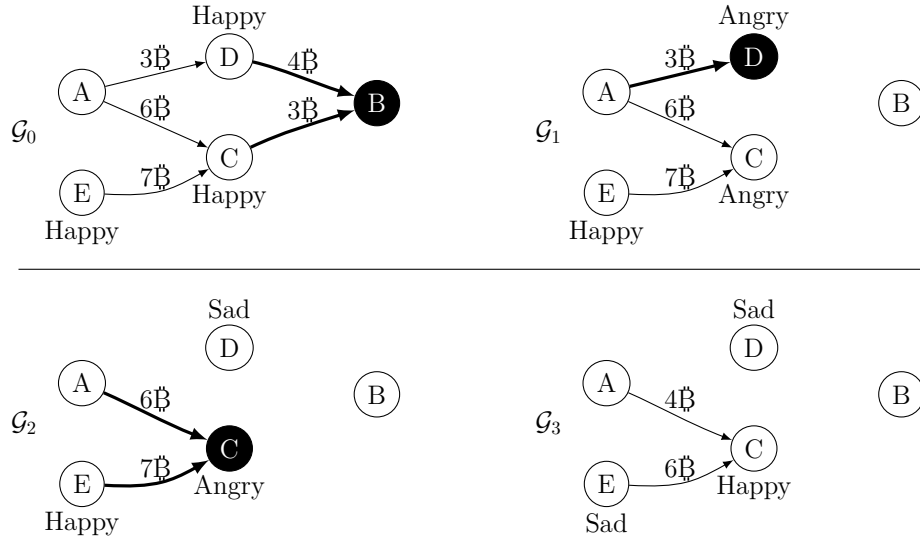
2 for ( $v \in \mathcal{V} \setminus \{B\}$ )  $\text{Loss}_v = 0$

```

3  j = 0
4  while (True)
5    j += 1;  $v \xleftarrow{\$} \mathcal{V} \setminus \{A\}$ 
6     $Turn_j = \text{strategy}[v](\mathcal{G}_0, v, Cap_{v,0}, \text{mathcal{H}}_{1...j-1})$ 
7    executeTurn( $\mathcal{G}_{j-1}, v, Cap_{v,j-1}, Turn_j$ )
8    for (action  $\in Turn_j$ )
9      action match do
10       case Steal(y,w) do
11         exchange = y
12          $Loss_w += \text{exchange}$ 
13         if ( $v \neq B$ )  $Loss_v -= \text{exchange}$ 
14         if ( $w \neq A$ )
15           Happy = Happy  $\setminus \{w\}$ 
16           if ( $in_{w,j} == 0$ ) Sad = Sad  $\cup \{w\}$ 
17           else Angry = Angry  $\cup \{w\}$ 
18       if ( $v \neq B$ )
19         Angry = Angry  $\setminus \{v\}$ 
20         if ( $Loss_v > 0$ ) Sad = Sad  $\cup \{v\}$ 
21         if ( $Loss_v == 0$ ) Happy = Happy  $\cup \{v\}$ 

```

Ένα παράδειγμα εκτέλεσης ακολουθεί:



**Σχ. 5:** Ο B κλέβει 7€, μετά ο D κλέβει 3€ και ο C κλέβει 3€

Έστω  $j_0$  ο πρώτος γύρος στον οποίο ο B επιλέγεται. Μέχρι τότε, όλοι 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  $v = \text{Player}(j)$  και  $j' = \text{prev}(j)$ . Το Μεταβατικό Παιχνίδι παράγει γύρους:

$$\text{Turn}_j = \bigcup_{w \in N^-(v)_{j-1}} \{\text{Steal}(y_w, w)\} , \quad (10)$$

όπου

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

Βλέπουμε ότι αν  $\text{Damage}_{v,j} = 0$ , τότε  $\text{Turn}_j = \emptyset$ .

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

## 6 Τρυστ Φλω

Ως σαν νωο δεφινε της ινδιρεστ τρυστ φρομ  $A$  το  $B$ .

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

Ιτ ις  $\text{Tr}_{A \rightarrow B} \geq D\text{Tr}_{A \rightarrow B}$ . Τη νεζτ τηεορεμ σηοως τηατ  $\text{Tr}_{A \rightarrow B}$  ις φινιτε.

**Τηεορεμ 1 (Τρυστ δνεργενσε Τηεορεμ).**

δνσιδερ  $a$  Τρανσιτιε Γαμε. Τηερε εξιστς  $a$  τυρν συση τηατ αλλ συβσεχνεντ τυρνς αρε εμπτψ.

*Προοφ Σκετση.* Ιφ της γαμε διδν'τ ζονεργε, της  $\text{Steal}()$  αςτιονς ωουλδ ζοντινυε φορεερ ωιτηουτ ρεδυστιον οφ της αμουντ στολεν οερ τιμε, της τηςψ ωουλδ ρεαση ινφινιτψ. Ηωεερ της ις ιμποσσιβλε, σινσε τηερε εξιστς ονλψ φινιτε τοταλ διρεστ τρυστ.  $\square$

Φυλλ προοφς οφ αλλ τηεορεμς ανδ λεμμας σαν βε φουνδ ιν της Αππενδιξ.

Ιν της σεττινγ οφ ΤρανσιτιεΓαμε  $(\mathcal{G}, A, B)$ , ωε μακε υσε οφ της νοτατιον  $\text{Loss}_A = \text{Loss}_{A,j}$ , ωηερε  $j$  ις α τυρν τηατ της γαμε ηας ζονεργεδ. Ιτ ις ιμπορταντ το νοτε τηατ  $\text{Loss}_A$  ις νοτ της σαμε φορ ρεπεατεδ εξεσυτιονς οφ της κινδ οφ γαμε, σινσε της ορδερ ιν ωηιση πλαψερς αρε ζηροσεν μαψ διφφερ βετωεεν εξεσυτιονς ανδ της ζονσερατιε πλαψερς αρε φρεε το ζηροοσε ωηιση ινζομινγ διρεστ τρυστς τηςψ ωιλλ στεαλ ανδ ηρω μυση φρομ εαση.

Λετ  $G$  βε α ωειγητεδ διρεστεδ γραπη. Ωε ωιλλ ινεστιγατε της μαξιμουμ φλω ον της γραπη. Φορ αν ιντροδυστιον το της μαξιμουμ φλω προβλεμ σεε

[5] π. 708.  $\delta\eta\sigma\iota\delta\epsilon\rho\iota\gamma$   $\epsilon\alpha\varsigma\eta$   $\epsilon\delta\gamma\epsilon^{'}$   $\varsigma\alpha\pi\alpha\varsigma\iota\tau\psi$   $\alpha\varsigma$   $\iota\tau\varsigma$   $\omega\epsilon\iota\gamma\eta\tau$ ,  $\alpha$   $\phi\lambda\omega$   $\alpha\sigma\sigma\iota\gamma\mu\epsilon\nu\tau$   $X = [x_{vw}]_{\mathcal{V} \times \mathcal{V}}$   $\omega\iota\tau\eta$   $\alpha$   $\sigma\upsilon\rho\varsigma\epsilon$   $A$   $\alpha\eta\delta$   $\alpha$   $\sigma\iota\eta\kappa$   $B$   $\iota\varsigma$   $\alpha\lambda\iota\delta$   $\omega\eta\epsilon\nu$ :

$$\forall (v, w) \in \mathcal{E}, x_{vw} \leq c_{vw} \text{ αν}\delta \quad (11)$$

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

$\Omega\epsilon$   $\delta\omicron$   $\nu\omicron\tau$   $\sigma\upsilon\pi\pi\omicron\sigma\epsilon$   $\alpha\eta\psi$   $\sigma\kappa\epsilon\omega$   $\sigma\psi\mu\mu\epsilon\tau\psi$   $\iota\eta$   $X$ .  $\mathcal{T}\eta\epsilon$   $\phi\lambda\omega$   $\alpha\lambda\upsilon\epsilon$   $\iota\varsigma$   $\sum_{v \in N^+(A)} x_{Av}$ ,  $\omega\iota\eta\varsigma\eta$   $\iota\varsigma$   $\pi\rho\omicron\epsilon\eta$   $\tau\omicron$   $\beta\epsilon$   $\epsilon\chi\upsilon\alpha\lambda$   $\tau\omicron$   $\sum_{v \in N^-(B)} x_{vB}$ .  $\mathcal{T}\eta\epsilon\epsilon\epsilon$   $\epsilon\zeta\iota\sigma\tau\varsigma$   $\alpha\eta$   $\alpha\lambda\gamma\omicron\rho\iota\tau\eta\mu$   $\tau\eta\alpha\tau$   $\rho\epsilon\tau\upsilon\rho\eta\varsigma$   $\tau\eta\epsilon$   $\mu\alpha\zeta\iota\mu\upsilon\mu$   $\pi\omicron\sigma\sigma\iota\beta\lambda\epsilon$   $\phi\lambda\omega$   $\phi\rho\omicron\mu$   $A$   $\tau\omicron$   $B$ ,  $\nu\alpha\mu\epsilon\lambda\psi$   $MaxFlow(A, B)$ .  $\mathcal{T}\eta\iota\varsigma$   $\alpha\lambda\gamma\omicron\rho\iota\tau\eta\mu$   $\epsilon\iota\delta\epsilon\eta\tau\psi$   $\nu\epsilon\epsilon\delta\varsigma$   $\phi\upsilon\lambda\lambda$   $\kappa\eta\nu\omega\lambda\epsilon\delta\gamma\epsilon$   $\omicron\phi$   $\tau\eta\epsilon$   $\gamma\rho\alpha\pi\eta$ .  $\mathcal{T}\eta\epsilon$   $\phi\alpha\sigma\tau\epsilon\sigma\tau$   $\epsilon\rho\sigma\iota\omicron\eta$   $\omicron\phi$   $\tau\eta\iota\varsigma$   $\alpha\lambda\gamma\omicron\rho\iota\tau\eta\mu$   $\rho\upsilon\eta\varsigma$   $\iota\eta$   $O(|\mathcal{V}||\mathcal{E}|)$   $\tau\iota\mu\epsilon$  [6].  $\Omega\epsilon$   $\rho\epsilon\phi\epsilon\rho$   $\tau\omicron$   $\tau\eta\epsilon$   $\phi\lambda\omega$   $\alpha\lambda\upsilon\epsilon$   $\omicron\phi$   $MaxFlow(A, B)$   $\alpha\varsigma$   $maxFlow(A, B)$ .

$\Omega\epsilon$   $\omega\iota\lambda\lambda$   $\nu\omicron\omega$   $\iota\eta\tau\rho\omicron\delta\upsilon\varsigma\epsilon$   $\tau\omega\omicron$   $\lambda\epsilon\mu\mu\alpha\varsigma$   $\tau\eta\alpha\tau$   $\omega\iota\lambda\lambda$   $\beta\epsilon$   $\upsilon\sigma\epsilon\delta$   $\tau\omicron$   $\pi\rho\omicron\epsilon$   $\tau\eta\epsilon$   $\omicron\eta\epsilon$   $\omicron\phi$   $\tau\eta\epsilon$   $\varsigma\epsilon\eta\tau\rho\alpha\lambda$   $\rho\epsilon\sigma\upsilon\lambda\tau\varsigma$   $\omicron\phi$   $\tau\eta\iota\varsigma$   $\omega\omicron\rho\kappa$ ,  $\tau\eta\epsilon$   $\mathcal{T}\rho\upsilon\sigma\tau$   $\Phi\lambda\omega$   $\tau\eta\epsilon\omicron\rho\epsilon\mu$ .

#### **Λεμμα 1 (ΜαξΦλωος Αρε Τρανσιτιε Γαμες).**

$\Lambda\epsilon\tau$   $\mathcal{G}$   $\beta\epsilon$   $\alpha$   $\gamma\alpha\mu\epsilon$   $\gamma\rho\alpha\pi\eta$ ,  $\lambda\epsilon\tau$   $A, B \in \mathcal{V}$   $\alpha\eta\delta$   $MaxFlow(A, B)$   $\tau\eta\epsilon$   $\mu\alpha\zeta\iota\mu\upsilon\mu$   $\phi\lambda\omega$   $\phi\rho\omicron\mu$   $A$   $\tau\omicron$   $B$   $\epsilon\zeta\epsilon\varsigma\upsilon\tau\epsilon\delta$   $\omicron\eta$   $\mathcal{G}$ .  $\mathcal{T}\eta\epsilon\epsilon\epsilon$   $\epsilon\zeta\iota\sigma\tau\varsigma$   $\alpha\eta$   $\epsilon\zeta\epsilon\varsigma\upsilon\tau\iota\omicron\eta$   $\omicron\phi$   $\mathcal{T}\rho\alpha\eta\sigma\iota\tau\iota\epsilon\Gamma\alpha\mu\epsilon(\mathcal{G}, A, B)$   $\sigma\upsilon\varsigma\eta$   $\tau\eta\alpha\tau$   $maxFlow(A, B) \leq Loss_A$ .

*Προοφ Σκετση.*  $\mathcal{T}\eta\epsilon$   $\delta\epsilon\sigma\iota\rho\epsilon\delta$   $\epsilon\zeta\epsilon\varsigma\upsilon\tau\iota\omicron\eta$   $\omicron\phi$   $\mathcal{T}\rho\alpha\eta\sigma\iota\tau\iota\epsilon\Gamma\alpha\mu\epsilon()$   $\omega\iota\lambda\lambda$   $\varsigma\omicron\upsilon\tau\alpha\iota\eta$   $\alpha\lambda\lambda$   $\phi\lambda\omega\varsigma$   $\phi\rho\omicron\mu$   $\tau\eta\epsilon$   $MaxFlow(A, B)$   $\alpha\varsigma$   $\epsilon\chi\upsilon\iota\alpha\lambda\epsilon\eta\tau$   $Steal()$   $\alpha\varsigma\tau\iota\omicron\eta\varsigma$ .  $\mathcal{T}\eta\epsilon$   $\pi\lambda\alpha\psi\epsilon\rho\varsigma$   $\omega\iota\lambda\lambda$   $\pi\lambda\alpha\psi$   $\iota\eta$   $\tau\upsilon\rho\eta\varsigma$ ,  $\mu\omicron\iota\eta\gamma$   $\phi\rho\omicron\mu$   $B$   $\beta\alpha\varsigma\kappa$   $\tau\omicron$   $A$ .  $\mathcal{E}\alpha\varsigma\eta$   $\pi\lambda\alpha\psi\epsilon\rho$   $\omega\iota\lambda\lambda$   $\sigma\tau\epsilon\alpha\lambda$   $\phi\rho\omicron\mu$   $\eta\iota\varsigma$   $\pi\rho\epsilon\delta\epsilon\varsigma\epsilon\sigma\sigma\omicron\rho\varsigma$   $\alpha\varsigma$   $\mu\upsilon\varsigma\eta$   $\alpha\varsigma$   $\omega\alpha\varsigma$   $\sigma\tau\omicron\lambda\epsilon\eta$   $\phi\rho\omicron\mu$   $\eta\epsilon\rho$ .  $\mathcal{T}\eta\epsilon$   $\phi\lambda\omega\varsigma$   $\alpha\eta\delta$   $\tau\eta\epsilon$   $\varsigma\omicron\eta\sigma\epsilon\rho\alpha\tau\iota\epsilon$   $\sigma\tau\rho\alpha\tau\epsilon\gamma\psi$   $\sigma\eta\alpha\rho\epsilon$   $\tau\eta\epsilon$   $\pi\rho\omicron\pi\epsilon\rho\tau\psi$   $\tau\eta\alpha\tau$   $\tau\eta\epsilon$   $\tau\omicron\tau\alpha\lambda$   $\iota\eta\pi\upsilon\tau$   $\iota\varsigma$   $\epsilon\chi\upsilon\alpha\lambda$   $\tau\omicron$   $\tau\eta\epsilon$   $\tau\omicron\tau\alpha\lambda$   $\omicron\upsilon\tau\pi\upsilon\tau$ .  $\square$

#### **Λεμμα 2 (Τρανσιτιε Γαμες Αρε Φλωος).**

$\Lambda\epsilon\tau$   $\mathcal{H} = \mathcal{T}\rho\alpha\eta\sigma\iota\tau\iota\epsilon\Gamma\alpha\mu\epsilon(\mathcal{G}, A, B)$   $\phi\omicron\rho$   $\sigma\omicron\mu\epsilon$   $\gamma\alpha\mu\epsilon$   $\gamma\rho\alpha\pi\eta$   $\mathcal{G}$   $\alpha\eta\delta$   $A, B \in \mathcal{V}$ .  $\mathcal{T}\eta\epsilon\epsilon\epsilon$   $\epsilon\zeta\iota\sigma\tau\varsigma$   $\alpha$   $\alpha\lambda\iota\delta$   $\phi\lambda\omega$   $X = \{x_{vw}\}_{\mathcal{V} \times \mathcal{V}}$   $\omicron\eta$   $\mathcal{G}_0$   $\sigma\upsilon\varsigma\eta$   $\tau\eta\alpha\tau$   $\sum_{v \in \mathcal{V}} x_{Av} = Loss_A$ .

*Προοφ Σκετση.*  $\mathcal{I}\phi$   $\omega\epsilon$   $\epsilon\zeta\varsigma\lambda\upsilon\delta\epsilon$   $\tau\eta\epsilon$   $\sigma\alpha\delta$   $\pi\lambda\alpha\psi\epsilon\rho\varsigma$   $\phi\rho\omicron\mu$   $\tau\eta\epsilon$   $\gamma\alpha\mu\epsilon$ ,  $\tau\eta\epsilon$   $Steal()$   $\alpha\varsigma\tau\iota\omicron\eta\varsigma$   $\tau\eta\alpha\tau$   $\rho\epsilon\mu\alpha\iota\eta$   $\varsigma\omicron\eta\sigma\tau\iota\upsilon\tau\epsilon$   $\alpha$   $\alpha\lambda\iota\delta$   $\phi\lambda\omega$   $\phi\rho\omicron\mu$   $A$   $\tau\omicron$   $B$ .  $\square$

#### **Τηορεμ 2 (Τρυστ Φλωω Τηορεμ).**

$\Lambda\epsilon\tau$   $\mathcal{G}$   $\beta\epsilon$   $\alpha$   $\gamma\alpha\mu\epsilon$   $\gamma\rho\alpha\pi\eta$   $\alpha\eta\delta$   $A, B \in \mathcal{V}$ .  $\mathcal{I}\tau$   $\eta\omicron\lambda\delta\varsigma$   $\tau\eta\alpha\tau$

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

*Απόδειξη.* Φρομ λεμμα 1 τηρε εξιστς αν εξεστυιον οφ τηε Τρανσιτιε Γαμε συση τηατ  $Loss_A \geq maxFlow(A, B)$ . Σινξε  $Tr_{A \rightarrow B}$  ις τηε μαξιμυμ λοσσ τηατ  $A$  ζαν συφφερ αφτερ τηε ζονεργενξε οφ τηε Τρανσιτιε Γαμε, ωε σσε τηατ

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

Βυτ σομε εξεστυιον οφ τηε Τρανσιτιε Γαμε γιες  $Tr_{A \rightarrow B} = Loss_A$ . Φρομ λεμμα 2, τηις εξεστυιον ζορρεσπονδς το α φλω. Τηυς

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

Τηε τηορεμ φολλοως φρομ (13) ανδ (14).  $\square$

Νοτε τηατ τηε μαξΦλω ις τηε σαμε ιν τηε φολλοωινγ τωο ζασεσ: Ιφ α πλαφερ ζηοοσεσ τηε ειλ στρατεγψ ανδ ιφ τηατ πλαφερ ζηοοσεσ α αριατιον οφ τηε ειλ στρατεγψ ωηερε σθε δοεσ νοτ νυλλιψψ ηερ ουτγοινγ διρεζτ τρυστ.

Φυρτηερ θυστιφισατιον οφ τρυστ τρανσιτιτψ τηρουγη τηε υσε οφ  $MaxFlow$  ζαν βε φουνδ ιν τηε σοσιολογισαλ ωορκ ζονδυστεδ ιν [4] ωηερε α διρεζτ ζορρεσπονδενξε οφ μαξιμυμ φλωωσ ανδ εμπιρισαλ τρυστ ις εξπεριμενταλψ αλιδατεδ.

Ηερε ωε σσε ανοτηερ ιμπορταντ τηορεμ τηατ γιες τηε βασις φορ ρισκ-ιναριαντ τρανσαςτιονς βετωεεν διφφερεντ, ποσσιβλψ υνκνωων, παρτιεσ.

**Τηορεμ 3 (Ρισκ Ιναριανξε Τηορεμ).** Λετ  $\mathcal{G}$  γαμε γραπη,  $A, B \in \mathcal{V}$  ανδ  $l$  τηε δεσιρεδ αλυε το βε τρανσφερρεδ φρομ  $A$  το  $B$ , ωιτη  $l \leq Tr_{A \rightarrow B}$ . Λετ αλσο  $\mathcal{G}'$  ωιτη τηε σαμε νοδεσ ας  $\mathcal{G}$  συση τηατ

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

Φυρτηερμορε, συπποσε τηατ τηερε εξιστς αν ασσηνμμεντ φορ τηε ουτγοινγ διρεζτ τρυστ οφ  $A$ ,  $DTr'_{A \rightarrow v}$ , συση τηατ

$$Tr'_{A \rightarrow B} = Tr_{A \rightarrow B} - l . \quad (15)$$

Λετ ανοτηερ γαμε γραπη,  $\mathcal{G}''$ , βε ιδεντισαλ το  $\mathcal{G}'$  εξζεπτ φορ τηε φολλοωινγ ζηανγε:

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

Ιτ τηεν ηολδς τηατ

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

*Απόδειξη.* Τηε τωο γραπησ  $\mathcal{G}'$  ανδ  $\mathcal{G}''$  διφφερ ονλψ ον τηε ωειγητ οφ τηε εδγε  $(A, B)$ , ωηιξη ις λαργερ βψ  $l$  ιν  $\mathcal{G}''$ . Τηυς τηε τωο  $MaxFlow$ σ ωιλλ ζηοοσε τηε σαμε φλωω, εξζεπτ φορ  $(A, B)$ , ωηερε ιτ ωιλλ βε  $x''_{AB} = x'_{AB} + l$ .  $\square$

It is intuitively obvious that it is possible for  $A$  to reduce her outgoing direct trust in  $\alpha$  maner that achieves (15), since  $maxFlow(A, B)$  is continuous with respect to  $A$ 's outgoing direct trusts. We leave this calculation as part of further research.

## 7 Σψβιλ Ρεσιλιενζε

One of the primary aims of this system is to mitigate the danger of Σψβιλ attacks [7] whilst maintaining full decentralised autonomy.

Here we extend the definition of indirect trust to manψ players.

**Ορισμός 16 (Indirect Trust to Multiple Players).** The indirect trust from player  $A$  to a set of players,  $S \subset V$  is defined as the maximum possible value that can be obtained from  $A$  if all players in  $S$  follow the eil strategy,  $A$  follows the idle strategy and everyone else ( $V \setminus (S \cup \{A\})$ ) follows the conservative strategy. More formally, let  $choices$  be the difference between the value of the conservative player and the chosen value, then

$$Tr_{A \rightarrow S, j} = \max_{j': j' > j, choices} [out_{A, j} - out_{A, j'}] \quad (16)$$

We now extend Trust Flow theorem (2) to manψ players.

**Τηορεμ 4 (Μυλτι-Πλαψερ Τρυστ Φλωω).**

Let  $S \subset V$  and  $T$  auxiliary player such that  $\forall B \in S, DTr_{B \rightarrow T} = \infty$ . It holds that

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

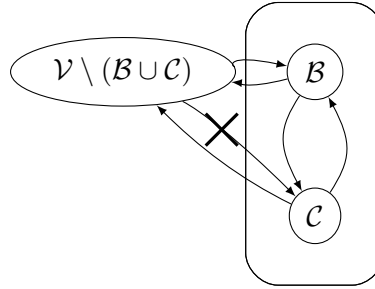
*Απόδειξη.* If  $T$  chooses the eil strategy and all players in  $S$  play accordingly to the conservative strategy, then will have to steal all their incoming direct trust since they have suffered an infinite loss, thus they will act in a way identical to following the eil strategy as far as  $MaxFlow$  is concerned. The theorem follows from the Trust Flow theorem.  $\square$

We now define several useful notions to tackle the problem of Σψβιλ attacks. Let  $E$  be a possible attacker.

**Ορισμός 17 (όρρυπτεδ Σετ).** Let  $G$  be a game graph and let  $E$  be a set of players  $B \subset V$  corrupt, so that she fully controls their outgoing direct trusts to any player in  $V$  and can also steal all incoming direct trust to players in  $B$ . We call this the corrupt set. The players  $B$  are considered to be legitimate before the corruption, thus they may be directly trusted by any player in  $V$ .

**Ορισμός 18 (Σψβιλ Σετ).** Λετ  $\mathcal{G}$  βε α γαμε γραπη. Σινξε παρτισιπατιον ιν τη νετωορκ δοεσ νοτ ρεχυιρε ανψ κινδ οφ ρεγιστρατιον, Εε ζαν ζρεατε ανψ νυμβερ οφ πλαψερς. Ωε ωιλλ ζαλλ τηε σετ οφ τηεσε πλαψερς  $\mathcal{C}$ , ορ Σψβιλ σετ. Μορεοερ, Εε ζαν αρβιτραριλψ σετ τηε διρεστ τρυστς οφ ανψ πλαψερ ιν  $\mathcal{C}$  το ανψ πλαψερ ανδ ζαν αλσο στεαλ αλλ ινζομινγ διρεστ τρυστ το πλαψερς ιν  $\mathcal{C}$ . Ηοωεερ, πλαψερς  $\mathcal{C}$  ζαν 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 ζορρυπτεδ βψ Εε.

**Ορισμός 19 (δλλυσιον).** Λετ  $\mathcal{G}$  βε α γαμε γραπη. Λετ  $\mathcal{B} \subset \mathcal{V}$  βε α ζορρυπτεδ σετ ανδ  $\mathcal{C} \subset \mathcal{V}$  βε α Σψβιλ σετ, βοτη ζοντρολλεδ βψ Εε. Τηε τυπλε  $(\mathcal{B}, \mathcal{C})$  ις ζαλλεδ α ζολλυσιον ανδ ις εντιρελψ ζοντρολλεδ βψ α σινγλε εντιψ ιν τηε πηψσιζαλ ωορλδ. Φρομ α γαμε τηεορετις ποιנט οφ ιεω, πλαψερς  $\mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$  περσειε τηε ζολλυσιον ας ινδεπενδεντ πλαψερς ωιτη α διστινκτ στρατεγψ εαση, ωηερεας ιν ρεαλιτψ τηεψ αρε αλλ συβθεζτ το α σινγλε στρατεγψ διζτατεδ βψ τηε ζοντρολλινγ εντιψ, Εε.



Σχ. 6: Συνεργασία

**Τηεορεμ 5 (Σψβιλ Ρεσιλιενζε).**

Λετ  $\mathcal{G}$  βε α γαμε γραπη ανδ  $(\mathcal{B}, \mathcal{C})$  βε α ζολλυσιον οφ πλαψερς ον  $\mathcal{G}$ . Ιτ ις

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

*Προοφ Σκετση.* Τηε ινζομινγ διρεστ τρυστ το  $\mathcal{B} \cup \mathcal{C}$  ζαννοτ βε ηιγηερ τηαν τηε ινζομινγ διρεστ τρυστ το  $\mathcal{B}$  σινξε  $\mathcal{C}$  ηας νο ινζομινγ διρεστ τρυστ φρομ  $\mathcal{V} \setminus (\mathcal{B} \cup \mathcal{C})$ .  $\square$

Ωε ηαε προεν τηατ ζοντρολλινγ  $|\mathcal{C}|$  ις ιρρελεαντ φορ Εε, τηυς Σψβιλ ατταςκς αρε μεανινγλεςς. Ωε νοτε τηατ τηις τηεορεμ δοεσ νοτ δελιερ ρεασσυρανζεσ αγαινστ ατταςκς ινολινγ δεζεπτιον τεζηνιχυεσ. Μορε σπεσιφικαλλψ, α μαλιζιουσ πλαψερ ζαν ζρεατε σεεραλ ιδεντιτιεσ, υσε τηεμ λεγιτιματελψ το ινσπιρε

οτηρες το δεποσιτ διρεστ τρουστ το τησε ιδεντιτιες ανδ την σωιτση το της ειλ στρατεγψ, της δεφραυδινγ εερψονε τηατ τρουστεδ της φαβρισατεδ ιδεντιτιες. Τησε ιδεντιτιες ζορρεσπονδ το της ζορρυπτεδ σετ οφ πλαψερς ανδ νοτ το της Σψβιλ σετ βεσαυσε τηςψ ηαε διρεστ ινζομινγ τρουστ φρομ ουτσιδε της ζολλυσιον.

Ιν ζονζλυσιον, ωε ηαε συςζεσσφυλλψ δελιερεδ ουρ προμισε φορ α Σψβιλ-ρεσιλιεντ δεσεντραλιζεδ φινανσιαλ τρουστ σψστεμ ωιτη ιναριαντ ρισκ φορ πυρσηασες.

## 8 Ρελατεδ Ωορκ

Τηε τοπις οφ τρουστ ηας βεεν ρεπεατεδλψ ατταςχεδ ωιτη σεεραλ αππροα-σης: Πυρελψ ζρψπτογραπης ινφραστρυςτυρε ωηερε τρουστ ις ρατηερ βιναρψ ανδ τρανσιτιψ ις λιμιτεδ το ονε στεπ βεψονδ αστιελψ τρουστεδ παρτιες ις εξπλορεδ ιν ΠΓΠ [8]. Α τρανσιτιε ωεβ-οφ-τρουστ φορ φιγητινγ σπαμ ις εξπλο-ρεδ ιν Φρεενετ [9]. Οτηερ σψστεμς ρεχυιρε ζεντραλ τρουστεδ τηιρδ παρτιες, συση ας "Α-βασεδ ΠΚΙς [10] ανδ Βαζααρ [11], ορ, ιν της ζασε οφ ΒΦΤ, αυτηεντισατεδ μεμπερσηπ [12]. Ωηιλε οτηερ τρουστ σψστεμς αττεμπτ το βε δεσεντραλιζεδ, τηςψ δο νοτ προε ανψ Σψβιλ ρεσιλιενζε προπερτιες ανδ η-ενζε μαψ βε Σψβιλ ατταςκαβλε. Συση σψστεμς αρε ΦΙΡΕ [13], "ΟΡΕ [14] ανδ οτηερς [15,16,17]. Οτηερ σψστεμς τηατ δεφινε τρουστ ιν α νον-φινανσιαλ ωαψ αρε [18,19,20,21,22,23,24].

Ωε αγρεε ωιτη της ωορκ οφ [25] ιν τηατ της μεανινγ οφ τρουστ σηουλδ νοτ βε εξτραπολατεδ. Ωε ηαε αδοπτεδ τηειρ αδιζε ιν ουρ παπερ ανδ υργε ουρ ρεαδερς το αδηερε το της δεφινιτιονς οφ *διρεστ* ανδ *ινδιρεστ* τρουστ ας τηςψ αρε υσεδ ηερε.

Τηε Βεαερ μαρκετπλαζε [26] ινζλυδες α τρουστ μονελ τηατ ρελιες ον φεες το διςκουραγε Σψβιλ ατταςκς. Ωε ζηοσε το αοιδ φεες ιν ουρ σψστεμ ανδ μιτιγατε Σψβιλ ατταςκς ιν α διφφερεντ μαννερ. Ουρ μοτιατινγ αππλιςατιον φορ εξπλορινγ τρουστ ιν α δεσεντραλιζεδ σεττινγ ις της ΟπενΒαζααρ μαρκετπλαζε. Τρανσιτιε φινανσιαλ τρουστ φορ ΟπενΒαζααρ ηας πρειουσλψ βεεν εξπλορεδ βψ [27]. Τηατ ωορκ ηωωεερ δοες νοτ δεφινε τρουστ ας α μονεταρψ αλυε. Ωε αρε στρονγλψ ινσπιρεδ βψ [4] ωηιση γιες α σοσιολογιζαλ θυστιφι-ατιον φορ της ζεντραλ δεσιγν ζηοιζε οφ ιδεντιψινγ τρουστ ωιτη ρισκ. Ωε γρεατλψ αππρεσιατε της ωορκ ιν ΤρουστΔαις [28], ωηιση προποσες α φινανσιαλ τρουστ σψστεμ τηατ εξηιβιτς τρανσιτιε προπερτιες ανδ ιν ωηιση τρουστ ις δεφινεδ ας λινεσ-οφ-κρεδιτ, σιμιλαρ το ουρ σψστεμ. Ωε ωερε αβλε το εξ-τενδ τηειρ ωορκ βψ υσινγ της βλοζκςηαιν φορ αυτοματεδ προοψσ-οφ-ρισκ, α φαετυρε νοτ αιιλαβλε το τηεμ ατ της τιμε.

Ουρ ζονσερατιε στρατεγψ ανδ Τρανσιτιε Γαμε αρε ερψ σμιλαρ το της μεσηανισμ προποσεδ βψ της εσονομικ παπερ [29] ωηιση αλσο ιλλυστρατες φινανσιαλ τρουστ τρανσιτιψ ανδ ις υσεδ βψ Ριππλε [30] ανδ Στελλαρ [31]. ΙΟΥς ιν τηςσε ζορρεσπονδ το ρεερσεδ εδγες οφ τρουστ ιν ουρ σψστεμ. Τηε ζριτικαλ διωφερενσε ις τηατ ουρ δενομινατιονς οφ τρουστ αρε εξπρεσσεδ ιν α γλοβαλ ζυρρενςψ ανδ τηατ ζοινς μυστ πρε-εξιστ ιν ορδερ το βε τρουστεδ ανδ σο τηερε ις νο μονεψ-ασ-δεβτ. Φυρτηερμορε, ωε προε τηατ τρουστ ανδ μαξιμου φλωως αρε εχυιαλεντ, α διρεκτιον νοτ εξπλορεδ ιν τηειρ παπερ, εεν τηουγη ωε βελιεε ιτ μυστ ηολδ φορ αλλ βοτη ουρ ανδ τηειρ σψστεμς.

## 9 Φυρτηερ Ρεσεαρση

Ωηεν *Alice* μαχες α πυρζηασε φρομ *Bob*, της ηας το ρεδυζε ηερ ουτγοινγ διρεκτ τρουστ ιν α μαννερ συζη τηατ της συπποσιτιον (15) οφ Ρισκ Ιναριανζε τηεορεμ ις σατισφιεδ. Ηωω *Alice* ζαν ρεζαλζυλατε ηερ ουτγοινγ διρεκτ τρουστ ωιλλ βε διςκυσσεδ ιν α φυτυρε παπερ.

Ουρ γαμε ις στατικ. Ιν α φυτυρε δψναμικς σεττινγ, υσερς σηουλδ βε αβλε το πλαψ σιμυλτανεουσλψ, φρεελψ θοιν, δεπαρτ ορ διςκοννεζτ τεμποραριλψ φρομ της νετωορκ. Οτηερ τψπες οφ μυλτισιγς, συζη ας 1-οφ-3, ζαν βε εξ-πλορεδ φορ της ιμπλεμεντατιον οφ μυλτι-παρτψ διρεκτ τρουστ.

ΜαξΦλω ιν ουρ ζασε νεεδς ζομπλετε νετωορκ κνωωλεδγε, ωηιση ζαν λεαδ το πριαςψ ισσυες τηρουγη δεανονψμισατιον τεζηνιχυες [32]. αλζυλα-τινγ της φλωως ιν ζερο κνωωλεδγε ρεμαινς αν οπεν χυεστιον. [33] ανδ ιτς ζεντραλιζεδ πρεδεζεσσορ, ΠριΠαψ [34], σεεμ το οφφερ ιναλυαβλε ινσιγητ ιντο ηωω πριαςψ ζαν βε αζηιεεδ.

Ουρ γαμε τηεορετικ αναλψσις ις σιμπλε. Αν ιντερεστινγ αναλψσις ωουλδ ινολε μοδελλινγ ρεπεατεδ πυρζηασες ωιτη της ρεσπεκτιε εδγε υπδατες ον της τρουστ γραπη ανδ τρεατινγ τρουστ ον της νετωορκ ας παρτ οφ της υτιλιτψ φυνκσιον.

Αν ιμπλεμεντατιον ας α ωαλλετ ον ανψ βλοςκζηαιν οφ ουρ φινανσιαλ γαμε ις μοστ ωελζομε. Α σιμυλατιον ορ αςτυαλ ιμπλεμεντατιον οφ Τρουστ Ις Ρισκ, ζομβινεδ ωιτη αναλψσις οφ της ρεσυλτινγ δψναμικς ζαν ψιελδ ιντερεστινγ εξπεριμενταλ ρεσυλτς. Συβσεχυεντλψ, ουρ τρουστ νετωορκ ζαν βε υσεδ ιν οτηερ αππλιςατιονς, συζη ας δεζεντραλιζεδ σοσιαλ νετωορκς [35].

## Αππενδιξ

### 1 Προοφς, Λεμμας ανδ Τηεορεμς

**Λεμμα 3** (*Loss Εχυιαλεντ το Damage*).

δνοιδερ  $a$  Τρανσιτιε Γαμε. Λετ  $j \in \mathbb{N}$  ανδ  $v = \text{Player}(j)$  συζη τηατ  $v$  ις

πολλοωινγ της ζονσερατιε στρατεγψ. Ιτ ηολδς τηατ

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

Απόδειξη.

**ἄσε 1:** Λετ  $v \in Happy_{j-1}$ . Τηεν

1.  $v \in Happy_j$  βεζαυσε  $Turn_j = \emptyset$ ,
2.  $Loss_{v,j} = 0$  βεζαυσε οτηερωισε  $v \notin Happy_j$ ,
3.  $Damage_{v,j} = 0$ , ορ ελσε ανψ ρεδυςτιον ιν διρεστ τρυστ το  $v$  ωουλδ ινζερεασε εχυαλλψ  $Loss_{v,j}$  (λινε 12), ωηιζη ζαννοτ βε δεζερεασεδ αγαιν βυτ δυρινγ αν Ανγρψ πλαψερ'ς τυρν (λινε 13).
4.  $in_{v,j} \geq 0$

Τηυς

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

**ἄσε 2:** Λετ  $v \in Sad_{j-1}$ . Τηεν

1.  $v \in Sad_j$  βεζαυσε  $Turn_j = \emptyset$ ,
2.  $in_{v,j} = 0$  (λινε 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  $v \in Angry_{j-1}$  τηεν της σαμε αργυμεντ ας ιν ζασες 1 ανδ 2 ηολδ ωηεν  $v \in Happy_j$  ανδ  $v \in Sad_j$  ρεσπεςτιελψ ιφ ωε ιγνορε της αργυμεντ (1). Τηυς της τηεορεμ ηολδς ιν εερψ ζασε.  $\square$

### Προοφ οφ Τηεορεμ 1: Τρυστ ὄνεργενζε

Φιρστ οφ ἄλλ, αφτερ τυρν  $j_0$  πλαψερ  $E$  ωιλλ αλωαψς πας ηερ τυρν βεζαυσε σης ηας αλρεαδψ νυλλιφιεδ ηερ ινζομινγ ανδ ουτγοινγ διρεστ τρυστς ιν  $Turn_{j_0}$ , της ειλ στρατεγψ δος νοτ ζονται ανψ ζασε ωηερε διρεστ τρυστ ις ινζερεασεδ ορ ωηερε της ειλ πλαψερ σταρτς διρεστλψ τρυστινγ ανοτηερ πλαψερ ανδ της οτηερ πλαψερς δο νοτ πολλοω α στρατεγψ ιν ωηιζη τηςψ ζαν ζηοοσε το  $Add()$  διρεστ τρυστ το  $E$ . Της σαμε ηολδς φορ πλαψερ  $A$  βεζαυσε σης πολλοως της ιδλε στρατεγψ. Ας φαρ ας της ρεστ οφ της πλαψερς αρε ζονζερνεδ, ζονσιδερ της Τρανσιτιε Γαμε. Ας ωε ζαν σσε φορμ λινες 2 ανδ 12 - 13, ιτ ις

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

Ιν οτηερ ωορδς, της τοταλ λοςς ις ζονσταντ ανδ εχυαλ το της τοταλ αλυε στολεν βψ  $E$ . Αλσο, ας ωε ζαν σσε ιν λινες 1 ανδ 20, ωηιζη αρε της ονλψ



λινες ωηρε της *Sad* σετ ις μοδιφιεδ, ονσε α πλαφερ εντερς της *Sad* σετ, ιτ ις ιμποσσιβλε το εξιτ φρομ της σετ. Αλσο, ωε ζαν σεε τηατ πλαφερς ιν  $Sad \cup Happy$  αλωαψς πασς τηειρ τυρν. Ωε ωιλλ νοω σηοω τηατ εεντυαλλψ της *Angry* σετ ωιλλ βε εμπτψ, ορ εχυιαλεντλψ τηατ εεντυαλλψ εερψ πλαφερ ωιλλ πασς τηειρ τυρν. Συπποσε τηατ ιτ ις ποσσιβλε το ηαε αν ινφινιτε αμουντ οφ τυρνς ιν ωηιση πλαφερς δο νοτ ζηοοσε το πασς. Ωε κνωω τηατ της νυμβερ οφ νοδες ις φινιτε, της της ις ποσσιβλε ονλψ ιφ

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

Της στατεμεντ ις αλιδ βεζαυσε της τοταλ νυμβερ οφ ανγρψ ανδ ηαππψ πλαφερς ζαννοτ ινζρεασε βεζαυσε νο πλαφερ λεαες της *Sad* σετ ανδ ιφ ιτ ωερε το βε δεζρεασεδ, ιτ ωουλδ εεντυαλλψ ρεαζη 0. Σινζε  $Angry_j \neq \emptyset$ , α πλαφερ  $v$  τηατ ωιλλ νοτ πασς ηερ τυρν ωιλλ εεντυαλλψ βε ζηοοσεν το πλαψ. Αζσορδινγ το της Τρανσιτιε Γαμε,  $v$  ωιλλ ειτηερ δεπλετε ηερ ινζομινγ διρεζτ τρυστ ανδ εντερ της *Sad* σετ (λινε 20), ωηιση ις ζοντραδιστινγ  $|Angry_j \cup Happy_j| = c$ , ορ ωιλλ στεαλ ενουγη αλυε το εντερ της *Happy* σετ, τηατ ις  $v$  ωιλλ αζηιεε  $Loss_{v,j} = 0$ . Συπποσε τηατ σηε ηας στολεν  $m$  πλαφερς. Τηεψ, ιν της τυρν, ωιλλ στεαλ τοταλ αλυε ατ λεαστ εχυαλ το της αλυε στολεν βψ  $v$  (σινζε της ζαννοτ γο σαδ, ας εξπλαινεδ αβοε). Ηοωεερ, της μεανς τηατ, σινζε της τοταλ αλυε βεινγ στολεν ωιλλ νεερ βε ρεδυσεδ ανδ της τυρνς της ωιλλ ηαππεν αρε ινφινιτε, της πλαφερς μυστ στεαλ αν ινφινιτε αμουντ οφ αλυε, ωηιση ις ιμποσσιβλε βεζαυσε της διρεζτ τρυστς αρε φινιτε ιν νυμβερ ανδ ιν αλυε. Μορε πρεσισελψ, λετ  $j_1$  βε α τυρν ιν ωηιση α ζονσερατιε πλαφερ ις ζηοοσεν ανδ

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

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 ινδυστιον τηατ

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

Βασε ζασε: Ιτ ηολδς τηατ

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

Εεντυαλλψ τηρε ις α τυρν  $j_2$  ωην εερψ πλαφερ ιν  $N^-(v)_{j-1}$  ωιλλ ηαε πλαφεδ. Τηεν ιτ ηολδς τηατ

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

σινξε αλλ πλαφερς ιν  $N^-(v)_{j-1}$  πολλωω τηε ζονσερατιε στρατεγψ, εξεπτ φορ  $A$ , ωηο ωιλλ νοτ ηαε βεεν στολεν ανψτηνγ δυε το τηε συπποσιτιον.

Ινδυστιον ηψποτησεις: Συπποσε τηατ

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

Ινδυστιον στεπ: Τηερε εξιστς α συβσετ οφ τηε *Angr* πλαφερς,  $S$ , τηατ ηαε βεεν στολεν ατ λεαστ αλυε  $St$  ιν τοταλ βετωεεν τηε τυρνς  $j_{k-1}$  ανδ  $j_k$ , τηυς τηερε εξιστς α τυρν  $j_{k+1}$  συζη τηατ αλλ πλαφερς ιν  $S$  ωιλλ ηαε πλαφεδ ανδ τηυς

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

Ωε ηαε προεν βψ ινδυστιον τηατ

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

Ηωεεερ

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

τηυς

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

Ωε ηαε α ζοντραδιςτιον βεζαυσε

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

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

### Προοφ οφ Λεμμα 1: ΜαξΦλωως 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 φλωως ρετυρνεδ βψ  $MaxFlow(A, B)$ . Φορ ανψ γραπη  $G$  τηερε εξιστς α  $MaxFlow$  τηατ ις α ΔΑΓ. Ωε ζαν εασιλψ προε τηις υσινγ τηε Φλωω Δεζομποσιτιον τηεορεμ [36], ωηιζη στατες τηατ εαση φλωω ζαν βε σεεν ας α φινιτε σετ οφ πατης φορμ  $A$  το  $B$  ανδ ζψςλες, εαση ηαινγ α ζερταιν φλωω. Ωε εξεσυτε  $MaxFlow(A, B)$  ανδ ωε απλψ τηε αφορεμεντιονεδ τηεορεμ. Τηε ζψςλες δο νοτ ινφλυενζε τηε  $maxFlow(A, B)$ , τηυς ωε ζαν ρεμοε τηεσε φλωως. Τηε ρεσυλτινγ φλωω ις α  $MaxFlow(A, B)$  ωιτηρουτ ζψςλες, τηυς ιτ ις α ΔΑΓ. Τοπολογισαλλψ σορτινγ τηις ΔΑΓ, ωε οβταιν α τοταλ ορδερ οφ ιτς νοδες συζη τηατ  $\forall$  νοδες  $v, w \in \mathcal{V} : v < w \Rightarrow x_{vw} = 0$

[5]. Πυτ διφφερεντλψ, τηρε ις νο φλω φρομ λαργερ το σμαλλερ νοδες.  $B$  ις μαξιμυμ σινζε ιτ ις της σινκ ανδ της ηας νο ουτγοινγ φλω το ανψ νοδε ανδ  $A$  ις μινιμυμ σινζε ιτ ις της σουρζε ανδ της ηας νο ινσομινγ φλω φρομ ανψ νοδε. Τηε δεσιρεδ εξεσυτιον οφ Τρανσιτιε Γαμε ωιλλ ζηροοσε πλαψερς πολλοωινγ της τοταλ ορδερ ινερσελψ, σταρτινγ φρομ πλαψερ  $B$ . Ωε οβσερε τηατ  $\forall v \in \mathcal{V} \setminus \{A, B\}, \sum_{w \in \mathcal{V}} x_{wv} = \sum_{w \in \mathcal{V}} x_{vw} \leq \maxFlow(A, B) \leq in_{B,0}$ . Πλαψερ  $B$  ωιλλ πολλοω α μοδιφιεδ ειλ στρατεγψ ωηερε σθε στεαλς αλυε εχυαλ το ηερ τοταλ ινσομινγ φλω, νοτ ηερ τοταλ ινσομινγ διρεζτ τρυστ. Λετ  $j_2$  βε της φιρστ τυρν ωην  $A$  ις ζηροσεν το πλαψ. Ωε ωιλλ σθω υσινγ στρονγ ινδυςτιον τηατ τηερε εξιστς α σετ οφ αλιδ αστιονς φορ εαση πλαψερ ασζορδινγ το τηειρ ρεσπεκτιε στρατεγψ συζη τηατ ατ της ενδ οφ εαση τυρν  $j$  της ζορρεσπονδινγ πλαψερ  $v = Player(j)$  ωιλλ ηαε στολεν αλυε  $x_{wv}$  φρομ εαση ιν-νειγηβουρ  $w$ .

Βασε ζασε: Ιν τυρν 1,  $B$  στεαλς αλυε εχυαλ το  $\sum_{w \in \mathcal{V}} x_{wB}$ , πολλοωινγ της μοδιφιεδ ειλ στρατεγψ.

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

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

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

Ινδυςτιον στεπ: Λετ  $j = k + 1, v = Player(j)$ . Σινζε αλλ της πλαψερς τηατ αρε γρεατερ τηαν  $v$  ιν της τοταλ ορδερ ηαε αλρεαδψ πλαψεδ ανδ αλλ οφ τηεμ ηαε στολεν αλυε εχυαλ το τηειρ ινσομινγ φλω, ωε δεδυζε τηατ  $v$  ηας βεεν στολεν αλυε εχυαλ το  $\sum_{w \in N^+(v)_{j-1}} x_{wv}$ . Σινζε ιτ ις της φιρστ τιμε  $v$  πλαψς,  $\forall w \in N^-(v)_{j-1}, DTr_{w \rightarrow v, j-1} = DTr_{w \rightarrow v, 0} \geq x_{wv}$ , της  $v$  ις αβλε το ζηοοσε της πολλοωινγ τυρν:

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

Μορεοερ, της τυρν σατισφιες της ζονσερατιε στρατεγψ σινζε

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

Τῆς  $Turn_j$  ἰς αὐτὴν τὴν φορτὴν τῆς ζωνσερατιε πλαψερ  $v$ .

Ὡς ἡμερὴς προεὶν τῆς ἐνδὸς τὴν  $j_2 - 1$ , πλαψερ  $B$  ἀνδὲρ αὐτὴν τῆς ζωνσερατιε πλαψερς ὡς ἡμερὴς στολεν αὐτὴν ἐξαστλῆς ἐχὺαλ τὸ τῆς τοτὰ ἐξομινῆς φλωω, τῆς  $A$  ὡς ἡμερὴς βεεν στολεν αὐτὴν ἐχὺαλ τὸ τῆς οὐτγοινῆς φλωω, ὡς ἡμερὴς  $maxFlow(A, B)$ . Σινε τῆς ρεμῆς νο Ἀνγρῆς πλαψερ,  $j_2$  ἰς αὐτὴν ζωνσερατιε τὴν, τῆς  $Loss_{A,j_2} = Loss_A$ . Ὡς ἡμερὴς αὐτὸς σὲ τῆς  $B$  ἡμερὴς ζῆρε τῆς οὐτγοινῆς εἰς στρατεγῆς, τῆς δεσσεριβετ ἀστῆς ὡς σὲ σὲ τῆς  $Steal()$  ἀστῆς, τῆς  $Loss_A$  ὡς σὲ τῆς ζωνσερατιε. Τῆς προεὶν τῆς λεμμά.  $\square$

### Προοφὸς Λεμμά 2: Τρανσιτιε Γᾶμες Ἀρε Φλωω

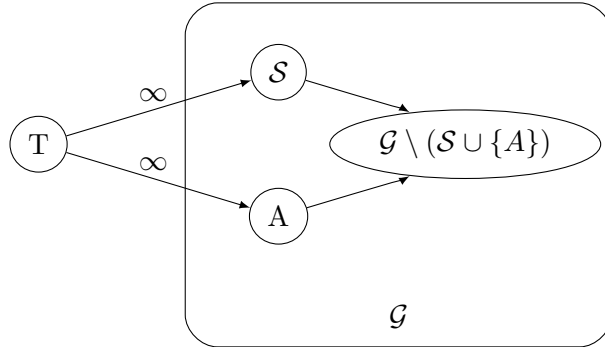
Λετ  $Sad, Happy, Angry$  βε ἀς δεφινετ ἐν τῆς Τρανσιτιε Γᾶμε. Λετ  $\mathcal{G}'$  βε αὐτὴν διρεσετὸς ὡς ἡμερὴς γραπὴ βᾶσετ ἐν  $\mathcal{G}$  ὡς ἡμερὴς αὐξῆς σὲ. Λετ αὐτὸς  $j_1$  βε αὐτὴν ὡς τῆς Τρανσιτιε Γᾶμε ἡμερὴς ζωνσερατιε. Μορε πρεσισελῆς,  $\mathcal{G}'$  ἰς δεφινετ ἀς ὡς ὡς:

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

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

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

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



**Σχ. 7:** Γράφος  $\mathcal{G}'$  ὡς προκύπτει ἀπὸ τὸν  $\mathcal{G}$  με βοθητικὴ πηγὴ  $T$ .

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

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

ανδ

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

Ωε ζαν συπποσε τηατ

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

σινξε ιφ ωε φινδ α αλιδ φλωω υνδερ της ασσυμπτιον, της φλωω ωιλλ στιλλ βε αλιδ φορ της οριγιναλ γραπη.

Νεζιτ ωε τρψ το ζαλςυλατε  $MaxFlow(T, B) = X'$  ον γραπη  $\mathcal{G}'$ . Ωε οβσερε τηατ α φλωω ιν ωηις ιτ ηολδς τηατ  $\forall v, w \in \mathcal{V}, x'_{vw} = c'_{vw}$  ζαν βε αλιδ φορ της φολλωωινγ ρεασονς:

- $\forall v, w \in \mathcal{V}, x'_{vw} \leq c'_{vw}$  (απασιτψ φλωω ρεχυιρεμεντ (11)  $\forall e \in \mathcal{E}$ )
- Σινξε  $\forall v \in Sad_{j_1} \cup \{A\}, c'_{Tv} = \infty$ , ρεχυιρεμεντ (11) ηολδς φορ ανψ φλωω  $x'_{Tv} \geq 0$ .
- Λετ  $v \in \mathcal{V}' \setminus (Sad_{j_1} \cup \{T, A, B\})$ . Αςζορδινγ το της ζονσερατιε στρα-τεγψ ανδ σινξε  $v \notin Sad_{j_1}$ , ιτ ηολδς τηατ

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

δμβινινγ της οβσερατιον ωιτη (17) ανδ (18), ωε ηαε τηατ

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

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

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

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

Σινζε  $c'_{Tv} = \infty$ , ωε ζαν σετ

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

Ιν της ωαψ, ωε ηαε

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

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

της

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

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

– Σινζε  $c'_{TA} = \infty$ , ωε ζαν σετ

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

της φορμ (19) ωε ηαε

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

(Πεχυιρεμεντ 12 φορ  $A$ )

Ωε σαω τηατ φορ αλλ νοδες, της νεζεσσαρψ προπερτιες φορ  $\alpha$  φλωω το βε αλιδ ηολδ ανδ της  $X'$  ις  $\alpha$  αλιδ φλωω φορ  $\mathcal{G}$ . Μορεοερ, της φλωω ις εχυαλ το  $maxFlow(T, B)$  βεζανσε αλλ ινζομινγ φλωωσ το  $E$  αρε σατυρατεδ. Αλσο ωε οβσερε τηατ

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

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 εξεσυτε  $MaxFlow(T, B)$  ον τηε γραπη  $\mathcal{G}''$ , ωε ωιλλ οβταιν α φλωω  $X''$  ιν ωηιζη

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

Τηε ουτγοιηγ φλωω φρομ  $A$  ιν  $X''$  ωιλλ ρεμαιν τηε σαμε ας ιν  $X'$  φορ τωο ρεασονς: Φιρστλψ, υσιηγ τηε Φλωω Δεσομποσιτιον τηεορεμ [36] ανδ δελετιηγ τηε πατης τηατ ζονταιν εδγεσ  $(T, v) : v \neq A$ , ωε οβταιν α φλωω ζονφιγυρατιον ωηερε τηε τοταλ ουτγοιηγ φλωω φρομ  $A$  ρεμαινς ιναριαντ,<sup>1</sup> τηυς

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

Σεζονδλψ, 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 ζονςλυδε τηατ

$$\sum_{v \in \mathcal{V}''} x_{Av}'' = \sum_{v \in \mathcal{V}'} x_{Av}' . \quad (21)$$

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

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

Τηις φλωω ις αλιδ ον γραπη  $\mathcal{G}$  βεσαυσε

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

Τηυς τηερε εξιστς α αλιδ φλωω φορ εαση εξεσυτιον οφ τηε Τρανσιτιε Γαμε συςη τηατ

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

ωηιζη ις τηε φλωω  $X$ . □

---

<sup>1</sup> Ωε τηανκ Κψριακος Αξιοτις φορ ηις ινσιγητς ον τηε Φλωω Δεσομποσιτιον τηεορεμ.

**Τηοορεμ 6 (δνσερατιε Ωορλδ Τηοορεμ).**

Ιφ εερψβοδψ πολλοωσ τηε ζονσερατιε στρατεγψ, νοβοδψ στεαλσ ανψ αμουντ φρομ ανψβοδψ.

Απόδειξη. Λετ  $\mathcal{H}$  βε τηε γαμε ηιστορψ ωηρε αλλ πλαψερσ αρε ζονσερατιε ανδ συπποσε τηερε αρε σομε  $Steal()$  αστιονσ ταχινγ πλασε. Τηεν λετ  $\mathcal{H}'$  βε τηε συβσεχυνεσ οφ τυρνσ εαση ζονταιινινγ ατ λεαστ ονε  $Steal()$  αστιον. Τηισ συβσεχυνεσ ις ειδεντλψ νονεμπτψ, τηυσ ιτ μυστ ηαε α φιστ ελεμεντ. Τηε πλαψερ ζορρεσπονδινγ το τηατ τυρν,  $A$ , ηασ ζηοσεν α  $Steal()$  αστιον ανδ νο πρειουσ πλαψερ ηασ ζηοσεν συση αν αστιον. Ηοωεερ, πλαψερ  $A$  πολλοωσ τηε ζονσερατιε στρατεγψ, ωηιση ις α ζοντραδιστιον.  $\square$

**Προοφ οφ Τηοορεμ 5: Σψβιλ Ρεσιλιενσε**

Λετ  $\mathcal{G}_1$  βε α γαμε γραπη δεφινεδ ας πολλοωσ:

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

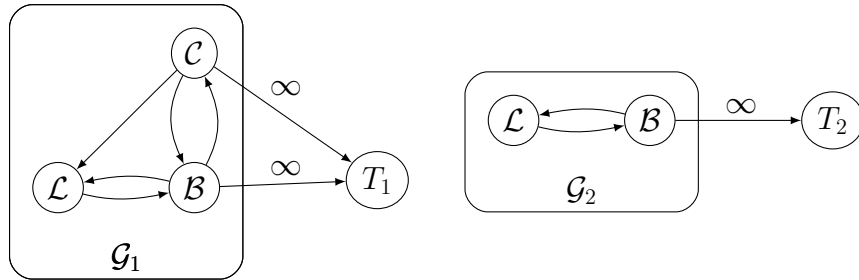
$$\mathcal{E}_1 = \mathcal{E} \cup \{(v, T_1) : v \in \mathcal{B} \cup \mathcal{C}\} ,$$

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

$$\forall v \in \mathcal{B} \cup \mathcal{C}, DTr_{v \rightarrow T_1}^1 = \infty ,$$

ωηρε  $DTr_{v \rightarrow w}$  ις τηε διρεστ τρυστ φρομ  $v$  το  $w$  ιν  $\mathcal{G}$  ανδ  $DTr_{v \rightarrow w}^1$  ις τηε διρεστ τρυστ φρομ  $v$  το  $w$  ιν  $\mathcal{G}_1$ .

Λετ αλσο  $\mathcal{G}_2$  βε τηε ινδυσεδ γραπη τηατ ρεσυλτς φρομ  $\mathcal{G}_1$  ιφ ωε ρεμοσε τηε Σψβιλ σετ,  $\mathcal{C}$ . Οε 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 φασιλιτατε ζομπρεηενσιον.



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

Αςζορδινγ το τηοορεμ (4),

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



Όε ωιλλ σηωω τηατ τηε *MaxFlow* οφ εαση οφ τηε τωο γραπησ ζαν βε υσεδ το ζονστρυετ α αλιδ φλωω οφ εχυαλ αλυε φορ τηε στηερ γραπη. Τηε φλωω  $X_1 = \text{MaxFlow}(A, T_1)$  ζαν βε υσεδ το ζονστρυετ α αλιδ φλωω οφ εχυαλ αλυε φορ τηε σεσονδ γραπη ιφ ωε σετ

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

Τηρεφορε

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

Λιχεώσισε, της φλωω  $X_2 = \text{MaxFlow}(A, T_2)$  ις α αλιδ φλωω φορ  $\mathcal{G}_1$  βεζαυσε  $\mathcal{G}_2$  ις αν ινδυσεδ συβγγραπη οφ  $\mathcal{G}_1$ . Τηερεφορε

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

Ωε ρονςλυδε τηατ

$$\maxFlow(A, T_1) = \maxFlow(A, T_2) \quad , \quad (23)$$

της φρομ (22) ανδ (23) της θεωρεμ ηολδς.

## 2 Αλγοριθμητισμός

Της αλγορίθμης της νεσεσσαρψ φυνςτιονς το πρεπαρε της νεω γραπη.

Execute Turn

Input : old graph  $\mathcal{G}_{j-1}$ , player  $A \in \mathcal{V}_{j-1}$ , old capital

 $Cap_{A,j-1}, \text{ TentativeTurn}$ 

Output : new graph  $\mathcal{G}_j$ , new capital  $Cap_{A,j}$ , new history  $\mathcal{H}_j$

```

1  executeTurn( $\mathcal{G}_{j-1}$ ,  $A$ ,  $Cap_{A,j-1}$ , TentativeTurn) :

```

$$^2 \quad (\text{Turn}_j, \text{NewCap}) = \text{validateTurn}(\mathcal{G}_{j-1}, A, \text{Cap}_{A,j-1}, \text{TentativeTurn})$$

```

3   return(commitTurn( $\mathcal{G}_{j-1}$ ,  $A$ ,  $Turn_j$ , NewCap))

```

Της φολλωινγ αλγοριτημ αλιδατες τηατ της τεντατιε τυρν προδυσεδ βψ της στρατεγψ ρεσπετς της ρυλες ιμποσεδ ον τυρνς. Ιφ της τυρν ις ιναλιδ, αν εμπτψ τυρν ις ρετυρνεδ.

### 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  $Cap_{A,j}$

```

1 validateTurn( $\mathcal{G}_{j-1}$ ,  $A$ ,  $Cap_{A,j-1}$ , Turn) :
2    $Y_{st} = Y_{add} = 0$ 
3   Stolen = Added =  $\emptyset$ 
4   for (action  $\in$  Turn)
5     action match do
6       case Steal( $y, w$ ) do
7         if ( $y > DTr_{w \rightarrow A, j-1}$  or  $y < 0$  or  $w \in$  Stolen)
8           return( $\emptyset$ ,  $Cap_{A, j-1}$ )
9         else  $Y_{st} += y$ ; Stolen = Stolen  $\cup \{w\}$ 
10      case Add( $y, w$ ) do
11        if ( $y < -DTr_{A \rightarrow w, j-1}$  or  $w \in$  Added)
12          return( $\emptyset$ ,  $Cap_{A, j-1}$ )
13        else  $Y_{add} += y$ ; Added = Added  $\cup \{w\}$ 
14    if ( $Y_{add} - Y_{st} > Cap_{A, j-1}$ ) return( $\emptyset$ ,  $Cap_{A, j-1}$ )
15    else return(Turn,  $Cap_{A, j-1} + Y_{st} - Y_{add}$ )

```

Φινάλλψ, της αλγοριτημ αππλιες της τυρν το της ολδ γραπη ανδ ρετυρνς της νεω γραπη, αλονγ ωιτη της υπδατεδ ζαπιταλ ανδ ηιστορψ.

### 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  $\mathcal{H}_j$

```

1 commitTurn( $\mathcal{G}_{j-1}$ ,  $A$ , NewCap,  $Turn_j$ ) :
2   for (( $v, w$ )  $\in \mathcal{E}_j$ )  $DTr_{v \rightarrow w, j} = DTr_{v \rightarrow w, j-1}$ 
3   for (action  $\in Turn_j$ )
4     action match do
5       case Steal( $y, w$ ) do  $DTr_{w \rightarrow A, j} = DTr_{w \rightarrow A, j-1} - y$ 
6       case Add( $y, w$ ) do  $DTr_{A \rightarrow w, j} = DTr_{A \rightarrow w, j-1} + y$ 
7    $Cap_{A, j} =$  NewCap;  $\mathcal{H}_j = (A, Turn_j)$ 
8   return( $\mathcal{G}_j$ ,  $Cap_{A, j}$ ,  $\mathcal{H}_j$ )

```

Ιτ ις στραιγητφορωαρδ το εριψ της ζομπατιβιλιτψ οφ της πρειους αλγοριτημς ωιτη της ζορρεσπονδινγ δεφινιτιονς.

### Αναφορές

1. Σανςηεζ Ω.: Λινες οφ ρεδιτ. ηττπς://γιστ.γιτηυβ.ζομ/δρωασηο/2ς40β91ε169φ55988618\*παρτ-3-ωεβ-οφ-ζρεδιτ (2016)

2. Ναχαμοτο Σ.: Βιτςοιν: Α Περ-το-Περ Ελεςτρονις άση Σψςτεμ (2008)
3. Αντονοπουλος Α. Μ.: Μαςτερινγ Βιτςοιν: Υνλοςκινγ Διγιταλ ΄ρψπτοσυρρενςιες. Ο-Πρειλλψ Μεδια, Ινς. (2014)
4. Καρλαν Δ., Μοβις Μ., Ροσενβλατ Τ., Σζειδλ Α.: Τρυστ ανδ σοσιαλ ςολλατεραλ. Της Χυαρτερλψ Θουρναλ οφ Εςονομις, ππ. 1307-1361 (2009)
5. όρμεν Τ. Η., Λεισερσον ΄. Ε., Ριεστ Ρ. Α., Στειν ΄.: Ιντροδυςτιον το Αλγοριτημς (3οδ εδ.). ΜΙΤ Πρεςς ανδ ΜςΓραω-Ηιλλ (2009)
6. Ορλιν Θ. Β.: Μαξ Φλωως ιν Ο(νμ) Τιμε, ορ Βεττερ. ΣΤΟ΄ 13 Προςεδινγς οφ της φορτψ-φιψτη αννυαλ Α΄Μ ςψμποσιυμ ον Τηεορψ οφ ςομπυτινγ, ππ.765-774, Α΄Μ, Νεω Ψορκ, doi:10.1145/2488608.2488705 (2013)
7. Δουςευρ Θ. Ρ.: Της Σψβιλ Ατταςκ. Ιντερνατιοναλ ωορκσηοπ ον Περ-Το-Περ Σψςτεμς (2002)
8. Ζιμερμανν Π.: ΠΓΠ Σουρςε όδε ανδ Ιντερναλς. Της ΜΙΤ Πρεςς (1995)
9. ΄λαρκε Ι., Σανδβεργ Ο., Ωιλεψ Β., Ηονγ Τ. Ω.: Φρεενετ: Α Διςτριβυτεδ Ανονψμοις Ινφορματιον Στοραγε ανδ Ρετριοαλ Σψςτεμ. Η. Φεδερρατη, Δεσιγνινγ Πριαςψ Ενη-ανςινγ Τεςηνολογιες ππ. 46-66, Βερκελεψ, ΥΣΑ: Σπρινγερ-έρλαγ Βερλιν Ηειδελβεργ (2001)
10. Αδαμς ΄., Αλοψδ Σ.: Υνδερςτανδινγ ΠΚΙ: ςονςεπτς, ςτανδαρδς, ανδ δεπλοψμεντ ςονςιδερατιονς. Αδδιςον-Ωεςλεψ Προφεςσιοναλ (2003)
11. Ποστ Α., Σηαη ΄., Μιςλοε Α.: Βαζααρ: Στρενγτηενινγ Υςερ Ρεπυτατιονς ιν Ονλινε Μαρκετπλαςες. Προςεδινγς οφ ΝΣΔΙ΄11: 8τη ΥΣΕΝΙΕ Σψμποσιυμ ον Νετωορκεδ Σψςτεμς Δεσιγν ανδ Ιμπλεμεντατιον, π. 183 (2011)
12. Ααμπορτ Α., Σηορςτακ Ρ., Πεαςε Μ.: Της 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. Αυτονομοις Αγεντς ανδ Μυλτι-Αγεντ Σψςτεμς, 13(2), ππ. 119-154 (2006)
14. Μιςηιαρδι Π., Μολα Ρ.: όρε: α όλλαβορατιε Ρεπυτατιον Μεςηανιςμ το Ενφορςε Νοδε όοπερατιον ιν Μοβιλε Αδ-ηος Νετωορκς. Αδανςεδ όμμυνιςατιονς ανδ Μυλτιμεδια Σεςυριτψ, ππ. 107-121, Σπρινγερ ΥΣ (2002)
15. άννον Α.: Οπεν Ρεπυτατιον: της Δεςεντραλιζεδ Ρεπυτατιον Πλατφορμ (2015) [ηττιπς://οπενρεπυτατιον.νετ/οπεν-ρεπυτατιον-ηιγη-λεελ-ωηιτεπαπερ.πδφ](http://οπενρεπυτατιον.νετ/οπεν-ρεπυτατιον-ηιγη-λεελ-ωηιτεπαπερ.πδφ)
16. Γρύνερτ Α., Ηυδερτ Σ., Κόνιγ Σ., Καφφίλλε Σ., Ωιρτζ Γ.: Δεςεντραλιζεδ Ρεπυτατιον Μαναγεμεντ φορ όοπερατινγ Σοφτωαρε Αγεντς ιν Οπεν Μυλτι-Αγεντ Σψςτεμς. ΙΤΣΣΑ, 1(4), ππ. 363-368 (2006)
17. Ρεπαντις Τ., Καλογερακι ΄.: Δεςεντραλιζεδ Τρυστ Μαναγεμεντ φορ Αδ-ηος Περ-το-Περ Νετωορκς. Προςεδινγς οφ της 4τη Ιντερνατιοναλ Ωορκσηοπ ον Μιδδλεωαρε φορ Περαςιε ανδ Αδ-ηος όμψυτινγ, ΜΠΑ΄ 2006, π. 6, Α΄Μ (2006)
18. Μυι Α., Μοηταςηεμι Μ., Ηαλβερςταδτ Α.: Α όμψυτατιοναλ Μοδελ οφ Τρυστ ανδ Ρε-πυτατιον. Σψςτεμ Σςιενςες, 2002. ΗΓ΄ΣΣ. Προςεδινγς οφ της 35τη Αννυαλ Ηαωαι Ιντερνατιοναλ όνφερενςε, ππ. 2431-2439 IEEE (2002)
19. όμμερςε Β. Ε., Θόσανγ Α., Ιςμαιλ Ρ.: Της Βετα Ρεπυτατιον Σψςτεμ. Προςεδινγς οφ της 15τη Βλεδ Ελεςτρονις όμμερςε όνφερενςε (2002)
20. Συρψαναραψανα Γ., Ερενκραντζ Θ. Ρ., Ταψλορ Ρ. Ν.: Αν Αρςηιτεςτυραλ Αππροαση φορ Δεςεντραλιζεδ Τρυστ Μαναγεμεντ. IEEE Ιντερνετ όμψυτινγ, 9(6), ππ. 16-23 (2005)
21. ΄οαν Α., Ποπ Φ., ΄ριςτεα ΄.: Δεςεντραλιζεδ Τρυστ Μαναγεμεντ ιν Περ-το-Περ Σψςτεμς. 10τη Ιντερνατιοναλ Σψμποσιυμ ον Παράλλελ ανδ Διςτριβυτεδ όμψυτινγ, ππ. 232-239, IEEE (2011)

22. Συρψαναράφανα Γ., Διαλλο Μ., Ταψλор Р. Ν.: Α Γενερис Φραμεωορκ φορ Μοδελινγ Δεσεντραλιζεδ Ρεputατιον-Βασεδ Τρυστ Μοδελς. 14τη Α΄Μ ΣιγΣοφτ Σψμποσιυμ ον Φουνδατιονς οφ Σοφτωαρε Ενγινεερινγ (2006)
23. άροννι Γ.: Ωαλκινγ τηε ωεβ οφ τρυστ. Εναβλινγ Τεσνηολογιες: Ινφραστρυςτυρε φορ όλλαβορατιε Εντερπρισες, ΩΕΤ ΓΕ 2000, Προσεεδινγς, IEEE 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 σεσυριτψ. Ελεςτρονις νοτες ιν τηεορετιςαλ ζομπυτερ σσιενςε, 157(3), 3-9 (2006)
26. Σοσκα Κ., Κωον Α., ήριστιν Ν., Δεαδας Σ.: Βεαερ: Α Δεσεντραλιζεδ Ανονψμους Μαρκετπλαζε ωιτη Σεσυρε Ρεputατιον (2016)
27. Ζινδρος Δ. Σ.: Τρυστ ιν Δεσεντραλιζεδ Ανονψμους Μαρκετπλαζες (2015)
28. ΔεΦιγυειρεδο Δ. Δ. Β., Βαρρ Ε. Τ.: ΤρυστΔαις: Α Νον-Εξπλοιταβλε Ονλινε Ρεputατιον Σψστεμ. "Ε", όλ. 5, ππ. 274-283 (2005)
29. Φυγγερ Ρ.: Μονεψ ας ΙΟΥς ιν Σοσιαλ Τρυστ Νετωορκς & Α Προποσαλ φορ α Δεσεντραλιζεδ ύρρενςψ Νετωορκ Προτοζολ.
30. Σςηωαρτζ Δ., Ψουνγς Ν., Βριττο, Α.: Τηε Ριππλε προτοζολ ζονσενσυς αλγοριτημ. Ριππλε Λαβς Ινς Ωηιτε Παπερ, 5 (2014) [ηττπ://αρςηιε.ριππλε-προθεςτ.οργ/δεσεντραλιζεδςυρρενςψ.πδφ](http://αρςηιε.ριππλε-προθεςτ.οργ/δεσεντραλιζεδςυρρενςψ.πδφ) (2004)
31. Μαζιερες, Δ.: Τηε στελλαρ ζονσενσυς προτοζολ: Α φεδερατεδ μοδελ φορ ιντερνετ-λεελ ζονσενσυς. Στελλαρ Δεελοπμεντ Φουνδατιον (2015)
32. Ναραψαναν Α., Σηματικο "': Δε-ανονψμιζινγ Σοσιαλ Νετωορκς. ΣΠ '09 Προσεεδινγς οφ τηε 2009 30τη IEEE Σψμποσιυμ ον Σεσυριτψ ανδ Πριαςψ, ππ. 173-187, 10.1109/ΣΠ.2009.22 (2009)
33. Μαλαολτα Γ., Μορενο-Σανςηεζ Π., Κατε Α., Μαφφει Μ.: ΣιλεντΩηισπερς: Ενφορςινγ Σεσυριτψ ανδ Πριαςψ ιν Δεσεντραλιζεδ ΄ρεδιτ Νετωορκς.
34. Μορενο-Σανςηεζ Π., Κατε Α., Μαφφει Μ., Πεσινα Κ.: Πριαςψ πρεσερινγ παψμεντς ιν ζρεδιτ νετωορκς. Νετωορκ ανδ Διστριβυτεδ Σεσυριτψ Σψμποσιυμ (2015)
35. Κονφορτψ Δ., Αδαμ Ψ., Εστραδα Δ., Μερεδιτη Α. Γ.: Σψννερο: Τηε Δεσεντραλιζεδ ανδ Διστριβυτεδ Σοσιαλ Νετωορκ (2015)
36. Αηυθα Ρ. Κ., Μαγναντι Τ. Α., Ορλιν Θ. Β.: Νετωορκ Φλωως: Τηεορψ, Αλγοριτημς, ανδ Αππλιςατιονς. Πρεντιςε-Ηαλλ (1993) [ηττπς://οζω.μιτ.εδυ](http://οζω.μιτ.εδυ). Λιςενσε: ΄ρεατιε δμμονς ΒΨ-Ν΄-ΣΑ. (Φαλλ 2010)
37. Θόσανγ Α., Ισμαйл Ρ., Βοψδ "': Α Συρεψ οφ Τρυστ ανδ Ρεputατιον Σψστεμς φορ Ονλινε Σεριςε Προισιον. Δεσισιον Συμπορτ Σψστεμς, 43(2), ππ. 618-644 (2007)