Bitcoin: Ένα Peer-to-Peer Ηλεκτρονικό Σύστημα Μετρητών

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Translated in Greek from bitcoin.org/bitcoin.pdf
by @chdimosthenis

Περιληπτικά: Μία καθαρά peer-to-peer έκδοση ηλεκτρονικών μετρητών που θα επιτρέπει σε διαδικτυακές πληρωμές να στέλνονται απευθείας από έναν συμβεβλημένο σε έναν άλλον χωρίς την ανάγκη διαμεσολάβησης ενός οικονομικού ιδρύματος. Οι ψηφιακές υπογραφές παρέχουν ένα μέρος της λύσης, αλλά τα κύρια οφέλη χάνονται εάν απαιτείται ένας τρίτος για να αποτρέπει διπλό-ξοδέματα (double-spend). Εμείς προτείνουμε μία λύση στο πρόβλημα του διπλό-ξοδέματος χρησιμοποιώντας ένα peer-to-peer δίκτυο. Το δίκτυο χρονοσφραγίζει (timestamps) συναλλαγές κατακερματίζοντας (transaction hash) τις μέσα σε μία εξελισσόμενη αλυσίδα απόδειξης εργασίας (proof-of-work) βασισμένη σε κατακερματισμούς (hash-based), σχηματίζοντας ένα αρχείο καταγραφής το οποίο δεν μπορεί να αλλαχτεί χωρίς να επαναληφθεί ξανά όλη η απόδειξη της εργασίας που έχει προηγηθεί. Η μακρύτερη αλυσίδα δεν εξυπηρετεί μόνο ως απόδειξη της ακολουθίας των συμβάντων που έχουν δημόσια καταγραφεί, αλλά και απόδειξη ότι προήλθε από τη μεγαλύτερη πηγή επεξεργαστικής ισχύος που έχει καταβληθεί για αυτόν το σκοπό. Όσο η πλειοψηφία της επεξεργαστικής ισχύος ελέγχεται από κόμβους που δεν συνεργάζονται για να επιτεθούν το δίκτυο, αυτοί θα ανά-σχηματίζουν τη μακρύτερη αλυσίδα και θα αφήνουν πίσω τους επιτιθέμενους. Οι απαιτήσεις αυτού του δικτύου είναι ελάχιστες. Τα μηνύματα μεταδίδονται με βάση την καλύτερη δυνατή προσπάθεια του δικτύου (best-effort basis) και οι κόμβοι μπορούν να συνδεθούν ή να ανά-συνδεθούν στο δίκτυο κατά βούληση, αποδεχόμενοι τη μακρύτερη proof-of-work αλυσίδα ως απόδειξη για ο,τι συνέβη κατά την απουσία τους.

1. Εισαγωγή

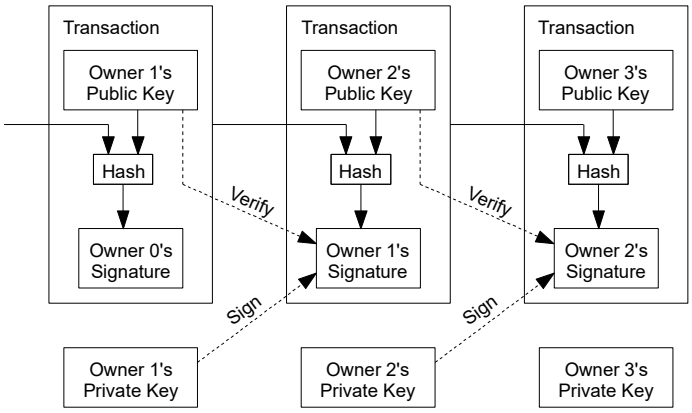
Το εμπόριο στο Διαδίκτυο έχει φθάσει σε ένα σημείο όπου πρέπει να βασιστεί σχεδόν αποκλειστικά σε οικονομικά ιδρύματα να εξυπηρετούν ως έμπιστοι διαμεσολαβητές επεξεργασίας ηλεκτρονικών πληρωμών. Ενώ το σύστημα λειτουργεί αρκετά καλά για τις περισσότερες συναλλαγές, αυτό πάσχει από την εγγενή του αδυναμία, την εμπιστοσύνη ως βάση του. Εξ' ολοκλήρου μη-αναστρέψιμες συναλλαγές δεν είναι στην πραγματικότητα εφικτές, καθ' όσον τα οικονομικά ιδρύματα δεν μπορούν να αποφύγουν τη διαμεσολάβηση διαφορών. Το κόστος της διαμεσολάβησης αυξάνει τα κόστη των συναλλαγών, περιορίζοντας το ελάχιστο πρακτικό μέγεθος αυτών και αποκόβοντας τη δυνατότητα για μικρές απλές πληρωμές, ενώ υπάρχει και ένα ευρύτερο κόστος στην απώλεια της δυνατότητας για πραγματοποίηση μη-αναστρέψιμων πληρωμών για μη-αναστρέψιμες υπηρεσίες. Με τη δυνατότητα για αντιστροφή, η ανάγκη για εμπιστοσύνη εξαπλώνεται. Οι έμποροι πρέπει να είναι επιφυλακτικοί όσον αφορά τους πελάτες τους, ενοχλώντας τους για όλο και περισσότερες πληροφορίες που σε αντίθετη

περίπτωση δεν θα χρειαζόντουσαν. Ένα δεδομένο ποσοστό εξαπάτησης λαμβάνεται ως αναπόφευκτο. Αυτά τα κόστη και οι αβεβαιότητες πληρωμών μπορούν αυτοπροσώπως να αποφευχθούν χρησιμοποιώντας φυσικά νομίσματα, αλλά δεν υπάρχει κανένας μηχανισμός για την πραγματοποίηση πληρωμών σε κάποιο κανάλι επικοινωνίας χωρίς έναν έμπιστο τρίτο.

Αυτό που χρειάζεται είναι ένα ηλεκτρονικό σύστημα πληρωμών βασισμένο σε απόδειξη κρυπτογραφίας αντί για εμπιστοσύνη, επιτρέποντας σε όποιους δύο συμβεβλημένους να κάνουν συναλλαγή απευθείας μεταξύ τους χωρίς την ανάγκη για έναν έμπιστο τρίτο. Συναλλαγές να είναι υπολογιστικά μη-πρακτικά να αντιστραφούν θα προστατεύουν τους πωλητές από εξαπάτηση, ενώ απλοί μηχανισμοί μεσεγγύησης θα μπορούν εύκολα να υλοποιούνται για την προστασία των αγοραστών. Σε αυτό το έγγραφο, προτείνουμε μία λύση στο πρόβλημα του διπλό-ξοδέματος χρησιμοποιώντας έναν peer-to-peer κατανεμημένο χρονοσφραγισμένο εξυπηρετητή για τη δημιουργία υπολογιστικής απόδειξης της χρονολογικής σειράς των συναλλαγών. Το σύστημα είναι ασφαλές όσο οι έντιμοι κόμβοι (nodes) συγκεντρώνουν από κοινού περισσότερη επεξεργαστική ισχύ από οποιαδήποτε συνεργατική ομάδα επιτιθέμενων.

2. Συναλλαγές

Ορίζουμε ένα ηλεκτρονικό νόμισμα ως μία αλυσίδα ψηφιακών υπογραφών. Κάθε ιδιοκτήτης μεταφέρει το νόμισμα στον επόμενο υπογράφοντας ψηφιακά έναν κατακερματισμό της προηγούμενης συναλλαγής και το δημόσιο κλειδί του επόμενου ιδιοκτήτη, προσθέτοντας αυτά στο τέλος του νομίσματος. Ένας δικαιούχος πληρωμής μπορεί να επιβεβαιώσει τις υπογραφές για να επιβεβαιώσει την αλυσίδα της ιδιοκτησίας.



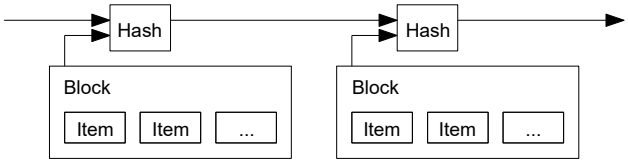
Το πρόβλημα είναι φυσικά ότι ο δικαιούχος πληρωμής δεν μπορεί να επιβεβαιώσει ότι ένας από τους ιδιοκτήτες δεν διπλό-ξόδεψε το νόμισμα. Η κοινή λύση είναι να εισάγουμε μία έμπιστη κεντρική αρχή -ή νομισματοκοπείο- η οποία ελέγχει κάθε συναλλαγή για διπλό-ξόδεμα. Το πρόβλημα με αυτήν τη λύση είναι ότι η μοίρα ολόκληρου του χρηματικού συστήματος εξαρτάται από την εταιρία που λειτουργεί το νομισματοκοπείο, με κάθε συναλλαγή να πρέπει να περνάει μέσα από αυτούς, όπως ακριβώς με μία τράπεζα.

Χρειαζόμαστε έναν τρόπο για τον δικαιούχο πληρωμής να γνωρίζει ότι οι προηγούμενοι ιδιοκτήτες δεν υπόγραψαν νωρίτερα άλλες πληρωμές. Για τον σκοπό μας, η παλαιότερη συναλλαγή είναι αυτή που μετράει, έτσι δεν ενδιαφερόμαστε για μεταγενέστερες απόπειρες διπλό-ξοδέματος. Ο μόνος τρόπος για επιβεβαίωση απουσίας μιας συναλλαγής είναι να γνωρίζουμε για όλες τις συναλλαγές. Στο σύστημα εμπιστοσύνης του νομισματοκοπείου, αυτό είναι που γνωρίζει για όλες τις συναλλαγές και αποφασίζει ποια έχει ληφθεί πρώτη. Για να το επιτύχουμε αυτό χωρίς κάποιον τρίτο έμπιστο, οι συναλλαγές πρέπει να ανακοινώνονται δημόσια [1], ενώ χρειαζόμαστε ένα σύστημα για τους συμμετέχοντες να συμφωνούν σε μία ενιαία ιστορία

της σειράς με την οποία αυτές έχουν ληφθεί. Ο δικαιούχος πληρωμής χρειάζεται απόδειξη ότι τη στιγμή της κάθε συναλλαγής, η πλειοψηφία των κόμβων συμφώνησε ότι ήταν η πρώτη που ελήφθη.

3. Timestamp Server (Δημιουργία εξυπηρετητή για χρονική επαλήθευση – Χρονοσφραγίδες)

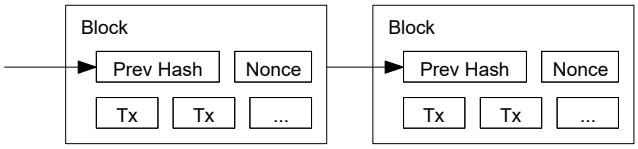
Η πρόταση που προτείνουμε ξεκινάει με τη δημιουργία ενός εξυπηρετητή για χρονική επαλήθευση (ή χρονοσφράγισμα) (timestamp). Ένας τέτοιος εξυπηρετητής λειτουργεί παίρνοντας έναν κατακερματισμό ενός μπλοκ από αντικείμενα, χρονοσφραγίζοντας το και δημοσιεύοντας ευρέως τον κατακερματισμό, όπως δηλαδή σε μία εφημερίδα ή σε μια ανάρτηση σε ένα σύστημα Usenet [2-5]. Η χρονοσφραγίδα αποδεικνύει ότι τα δεδομένα πρέπει να υπήρχαν τη δεδομένη χρονική στιγμή, προφανώς, ώστε να περιληφθούν μέσα στον κατακερματισμό. Κάθε χρονοσφραγίδα περιλαμβάνει την προηγούμενη χρονοσφραγίδα μέσα στον κατακερματισμό της, σχηματίζοντας μία αλυσίδα, με κάθε επιπρόσθετη χρονοσφραγίδα να ενισχύει τις προηγούμενες.



4. Proof-of-Work (Απόδειξη της Εργασίας)

Για να υλοποιήσουμε έναν κατανεμημένο εξυπηρετητή με χρονική επαλήθευση σε ένα peer-to-peer πλαίσιο, θα πρέπει να χρησιμοποιήσουμε ένα σύστημα απόδειξης εργασίας (proof-of-work) παρόμοιο με το Hashcash του Adam Back [6], σε σύγκριση με την εφημερίδα ή τις αναρτήσεις στο Usenet. Η απόδειξη εργασίας περιλαμβάνει τη σάρωση μιας τιμής η οποία όταν είναι κατακερματισμένη, όπως με τον αλγόριθμο SHA-256, ο κατακερματισμός να ξεκινάει με έναν αριθμό από μηδενικά μπιτ. Η μέση εργασία που απαιτείται είναι εκθετική στον αριθμό των μηδενικών μπιτ που απαιτούνται και μπορεί να επαληθευτεί με την εκτέλεση ενός μόνο κατακερματισμού.

Για το δικό μας χρονικά επαληθευμένο δίκτυο, υλοποιούμε την απόδειξη της εργασίας προσαυξάνοντας μία τιμή nonce (κρυπτογραφική περιστασιακή τιμή) στο μπλοκ μέχρι την εύρεση μίας τιμής που δίνει στον κατακερματισμό του μπλοκ τα απαιτούμενα μηδενικά μπιτ. Από τη στιγμή που έχει καταναλωθεί προσπάθεια του επεξεργαστή (CPU) ώστε να ικανοποιεί την απόδειξη εργασίας, το μπλοκ δεν μπορεί να αλλαχθεί χωρίς να επαναληφθεί ξανά η εργασία. Καθώς νέα μπλοκ προστίθενται μετά από αυτό στην αλυσίδα, η εργασία για να αλλαχθεί το μπλοκ περιλαμβάνει την επανάληψη όλης της εργασίας για όλα τα μπλοκ που έχουν προστεθεί μετά από αυτό.



Η απόδειξη της εργασίας (proof-of-work) λύνει επίσης το πρόβλημα καθορισμού της αντιπροσωπευτικής πλειοψηφίας στη λήψη αποφάσεων. Εάν η πλειοψηφία καθορίζονταν με βάση το σχήμα «μία διεύθυνση IP ανά ψήφο», θα μπορούσε να ανατραπεί από οποιονδήποτε σε θέση να διαθέσει πολλές IP διευθύνσεις. Η απόδειξη εργασίας είναι στην ουσία «ένας

επεξεργαστής CPU ανά ψήφο». Η απόφαση της πλειοψηφίας αντιπροσωπεύεται από τη μακρύτερη αλυσίδα, η οποία έχει τη μεγαλύτερη προσπάθεια απόδειξης εργασίας επενδεδυμένη σε αυτήν. Εάν η πλειοψηφία της επεξεργαστικής ισχύος ελέγχεται από έντιμους κόμβους (nodes), η έντιμη αλυσίδα θα αναπτύσσεται ταχύτερα και θα ξεπερνάει όποιες ανταγωνιστικές αλυσίδες. Για να τροποποιήσει ένα μπλοκ που έχει περάσει, ένα επιτιθέμενος θα πρέπει να ξανακάνει όλη την απόδειξη εργασίας του μπλοκ και όλων των μπλοκ μετά από αυτό και τότε να προλάβει και να υπερβεί την εργασία των έντιμων κόμβων. Θα δείξουμε αργότερα ότι η πιθανότητα ενός βραδύτερου επιτιθέμενου για να προλάβει μειώνεται εκθετικά καθώς προστίθενται μεταγενέστερα μπλοκ.

Για την αντιστάθμιση της αυξημένης ταχύτητας hardware και του διαφορετικού ενδιαφέροντος για τη διατήρηση κόμβων με την πάροδο του χρόνου, η δυσκολία απόδειξης της εργασίας καθορίζεται από έναν μεταβλητό μέσο όρο στοχεύοντας έναν αριθμό μπλοκ ανά ώρα. Εάν δημιουργούνται πολύ γρήγορα, η δυσκολία αυξάνει.

5. Δίκτυο

Τα βήματα για να τρέξουν το δίκτυο είναι ως ακολούθως:

1) Νέες συναλλαγές μεταδίδονται σε όλους τους κόμβους.
2) Κάθε κόμβος συλλέγει νέες συναλλαγές μέσα σε ένα μπλοκ.
3) Κάθε κόμβος εργάζεται στην εύρεση μιας δύσκολης απόδειξης εργασίας (proof-of-work) για το μπλοκ του.
4) Όταν ένας κόμβος βρίσκει μία απόδειξη εργασίας, μεταδίδει το μπλοκ σε όλους τους κόμβους.
5) Οι κόμβοι αποδέχονται το μπλοκ μόνο εάν όλες συναλλαγές είναι έγκυρες και δεν έχουν ήδη ξοδευτεί.
6) Οι κόμβοι εκφράζουν την αποδοχή του μπλοκ εργαζόμενοι στη δημιουργία του επόμενου μπλοκ στην αλυσίδα, χρησιμοποιώντας τον κατακερματισμό του αποδεκτού μπλοκ ως προηγούμενο κατακερματισμό.

Οι κόμβοι πάντα θεωρούν τη μακρύτερη αλυσίδα να είναι η σωστή και εξακολουθούν να εργάζονται για να την επεκτείνουν. Εάν δύο κόμβοι μεταδώσουν διαφορετικές εκδόσεις του ίδιου μπλοκ ταυτόχρονα, μερικοί κόμβοι μπορεί να λάβουν το ένα ή το άλλο πρώτα. Σε αυτήν την περίπτωση, εργάζονται στο πρώτο που έχουν λάβει, αλλά αποθηκεύουν τον άλλον κλάδο (branch) σε περίπτωση που γίνει μακρύτερος. Ο δεσμός θα αποκοπεί όταν βρεθεί η επόμενη απόδειξη της εργασίας και ο ένας κλάδος γίνει μακρύτερος· οι κόμβοι που εργάζονταν στον άλλον κλάδο θα στραφούν τότε στον μακρύτερο.

Οι μεταδόσεις νέων συναλλαγών δεν χρειάζεται να φτάσουν απαραίτητα σε όλους τους κόμβους. Μόλις φθάσουν σε πολλούς κόμβους, θα μπουν μέσα σε ένα μπλοκ πολύ σύντομα. Οι μεταδόσεις μπλοκ δεν επηρεάζονται επίσης από μη-επιτυχημένα μηνύματα. Εάν ένας κόμβος δεν λάβει ένα μπλοκ, θα το αιτηθεί με την λήψη του επόμενου μπλοκ και καταλαβαίνοντας ότι του λείπει ένα.

6. Κίνητρο

Συμβατικά, η πρώτη συναλλαγή σε ένα μπλοκ είναι μια ειδική συναλλαγή που ξεκινάει ένα καινούριο νόμισμα στην κυριότητα του δημιουργού του μπλοκ. Αυτό προσδίδει ένα κίνητρο στους κόμβους να υποστηρίζουν το δίκτυο και παρέχει έναν τρόπο για αρχική διανομή νομισμάτων στην κυκλοφορία, αφού δεν υπάρχει καμία κεντρική αρχή να τα εκδίδει. Η σταθερή πρόσθεση ενός ποσού νέων νομισμάτων είναι ανάλογη με τους εξορύκτες (miners) χρυσού που καταναλώνουν πόρους για να προσθέσουν χρυσό στην κυκλοφορία. Στην περίπτωση μας, είναι

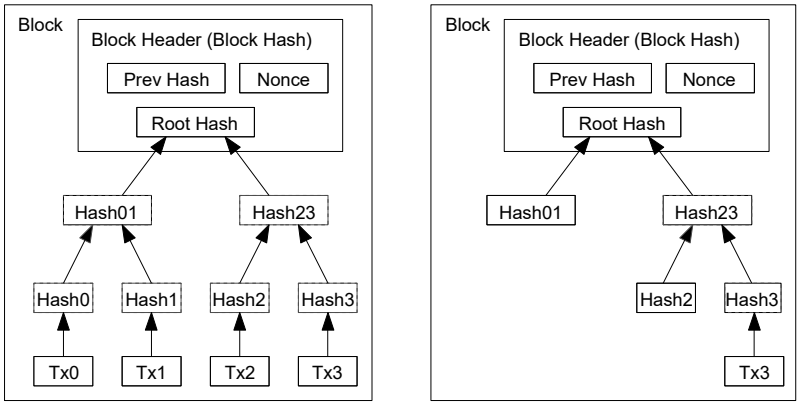
επεξεργαστικός χρόνος και ηλεκτρισμός που καταναλώνεται.

Το κίνητρο μπορεί επίσης να χρηματοδοτείται με χρεώσεις συναλλαγών (transaaction fees). Εάν η τιμή εξόδου (output) μίας συναλλαγής είναι μικρότερη από την τιμή εισόδου (input), η διαφορά είναι μία χρέωση συναλλαγής που προστίθεται στην αξία κινήτρου του μπλοκ που περιέχει τη συναλλαγή. Μόλις ένας προκαθορισμένος αριθμός νομισμάτων έχει εισέλθει στην κυκλοφορία, το κίνητρο μπορεί να μεταβεί εξ' ολοκλήρου στις χρεώσεις συναλλαγών, και να είναι ολοκληρωτικά ανεξάρτητος από πληθωρισμό.

Το κίνητρο μπορεί να ενθαρρύνει κόμβους να παραμένουν έντιμοι. Εάν ένας άπληστος επιτιθέμενος είναι σε θέση να συναρμολογήσει περισσότερη επεξεργαστική ισχύ από όλους τους έντιμους κόμβους, θα πρέπει να επιλέξει μεταξύ της χρήσης της για εξαπάτηση ανθρώπων κλέβοντας πίσω τις πληρωμές του, ή χρησιμοποιώντας την για δημιουργία νέων νομισμάτων. Αυτός θα πρέπει να το θεωρήσει πιο επικερδές να παίξει με τους κανόνες, αυτούς τους κανόνες που τον ευνοούν με περισσότερα νέα νομίσματα από όλους τους άλλους μαζί, αντί να υπονομεύσει το σύστημα και την εγκυρότητα της ίδιας του της περιουσίας.

7. Εξοικονόμηση αποθηκευτικού χώρου

Μόλις η τελευταία συναλλαγή σε ένα νόμισμα έχει θαφτεί κάτω από αρκετά μπλοκ, οι συναλλαγές που έχουν ξοδευτεί πριν από αυτήν μπορούν να παραμεριστούν για εξοικονόμηση χώρου στο δίσκο. Για να γίνει αυτό δυνατό χωρίς να καταστρέψουμε τον κατακερματισμό του μπλοκ, οι συναλλαγές κατακερματίζονται σε ένα δέντρο Merkle [7][2][5], με την ρίζα (root) μόνο να περιλαμβάνεται στον κατακερματισμό του μπλοκ. Τα παλαιότερα μπλοκ μπορούν τότε να συμπτυχθούν δημιουργώντας κλάδους του δέντρου. Οι εσωτερικοί κατακερματισμοί δεν χρειάζεται να αποθηκευτούν.



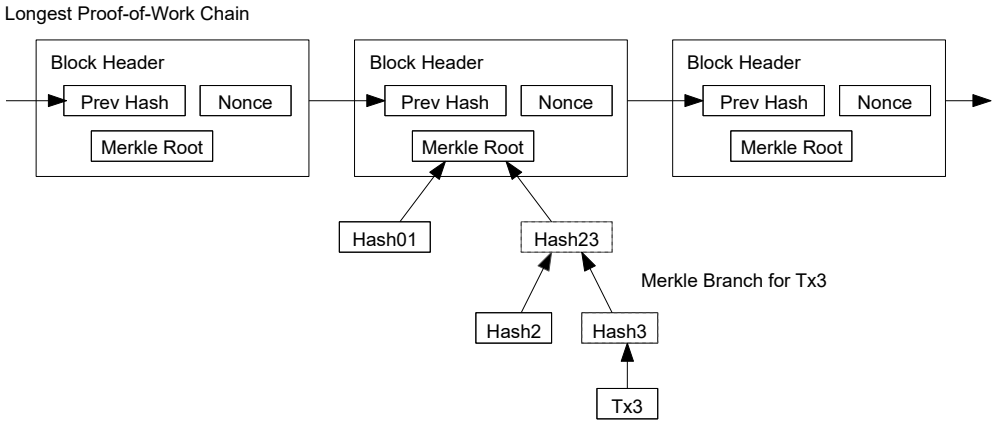
Transactions Hashed in a Merkle Tree | After Pruning Tx0-2 from the Block

Μία κεφαλίδα μπλοκ (block header) με καθόλου συναλλαγές θα είναι περίπου 80 μπάιτ. Εάν υποθέσουμε ότι δημιουργούνται μπλοκ κάθε 10 λεπτά, 80 μπάιτ * 6 * 24 * 365 = 4,2 MB. Με τα υπολογιστικά συστήματα να πωλούνται την τρέχουσα χρονική περίοδο με 2GB μνήμης RAM και το νόμο του Μουρ να προβλέπει τωρινή αύξηση 1,2GB ανά χρόνο, ο αποθηκευτικός χώρος δεν θα πρέπει να είναι πρόβλημα ακόμα και αν οι κεφαλίδες των μπλοκ πρέπει να κρατούνται στην μνήμη.

8. Απλοποιημένη επαλήθευση πληρωμής

Είναι δυνατό να επαληθευτούν πληρωμές χωρίς τη διατήρηση ενός πλήρους κόμβου (full node) του δικτύου. Ένας χρήστης χρειάζεται μόνο να διατηρεί ένα αντίγραφο των κεφαλίδων μπλοκ της μακρύτερης proof-of-work αλυσίδας, το οποίο μπορεί να πάρει στέλνοντας αιτήματα στους

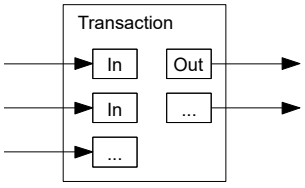
κόμβους του δικτύου μέχρι να είναι πεπεισμένος ότι έχει τη μακρύτερη αλυσίδα, αποκτώντας τον κλάδο Merkle που συνδέει τη συναλλαγή στο μπλοκ που είναι χρονοσφραγισμένη. Αυτός δεν μπορεί να ελέγξει τη συναλλαγή από μόνος του, αλλά μέσω της σύνδεσης σε μία τοποθεσία στην αλυσίδα, μπορεί να δει ότι ένας κόμβος δικτύου την έχει αποδεχτεί, με τα μπλοκ που έχουν προστεθεί μετά από αυτήν να επιβεβαιώνουν επιπλέον ότι το δίκτυο την έχει αποδεχτεί.



Ως εκ τούτου, η επαλήθευση είναι αξιόπιστη όσο έντιμοι κόμβοι ελέγχουν το δίκτυο, αλλά είναι πιο ευάλωτη εάν στο δίκτυο υπερισχύει ένας επιτιθέμενος. Ενώ οι κόμβοι του δικτύου μπορούν να επαληθεύουν πληρωμές από μόνοι τους, η απλοποιημένη μέθοδος μπορεί να εξαπατηθεί από τις επινοημένες συναλλαγές του επιτιθέμενου για όσο αυτός συνεχίζει να υπερισχύει στο δίκτυο. Μία στρατηγική για προστασία απέναντι σε αυτό θα ήταν η αποδοχή προειδοποιήσεων από κόμβους δικτύου όταν ανιχνεύουν ένα άκυρο μπλοκ, προτρέποντας το λογισμικό του χρήστη να κάνει λήψη το πλήρες μπλοκ και τις προειδοποιημένες συναλλαγές για την επιβεβαίωση της ασυμφωνίας. Επιχειρήσεις που λαμβάνουν συχνές πληρωμές θα θέλουν πιθανότατα να τρέχουν τους δικούς τους κόμβους για πιο ανεξάρτητη ασφάλεια και γρηγορότερη επαλήθευση.

9. Συνδυάζοντας και Χωρίζοντας Τιμές

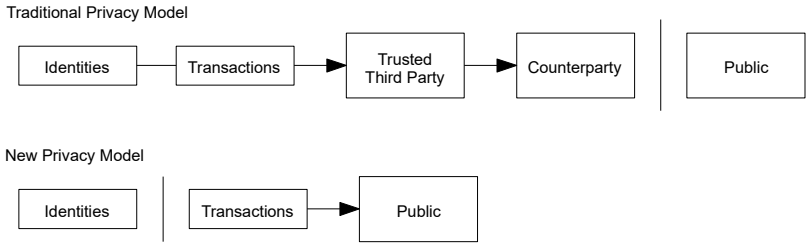
Αν και θα ήταν δυνατός ο ανεξάρτητος χειρισμός των νομισμάτων, θα ήταν δύσχρηστη η πραγματοποίηση ξεχωριστής συναλλαγής για κάθε σεντ που μεταφέρεται. Για να επιτρέπουν στις τιμές να χωρίζονται και να συνδυάζονται, οι συναλλαγές περιέχουν πολλαπλές εισόδους και εξόδους. Συνήθως θα υπάρχει μία μοναδική είσοδος από μία προηγούμενη μεγαλύτερη συναλλαγή ή πολλαπλές είσοδοι συνδυάζοντας μικρότερα ποσά, και το περισσότερο δύο έξοδοι: μία για την πληρωμή, και μία επιστροφής για τα ρέστα (change), εάν υπάρχουν, πίσω στον αποστολέα.



Πρέπει να σημειωθεί ότι ο αριθμός των εισόδων που συνδέονται με την έξοδο, όπου η συναλλαγή εξαρτάται από πολλές συναλλαγές, και αυτές οι συναλλαγές εξαρτώνται από πολλές περισσότερες, δεν αποτελεί πρόβλημα εδώ. Δεν υπάρχει ποτέ η ανάγκη για εξαγωγή ενός ολόκληρου ανεξάρτητου αντιγράφου του ιστορικού μια συναλλαγής.

10. Ιδιωτικότητα

Το παραδοσιακό τραπεζικό μοντέλο επιτυγχάνει ένα επίπεδο ιδιωτικότητας περιορίζοντας την πρόσβαση στις πληροφορίες για τα εμπλεκόμενα μέρη και τον έμπιστο τρίτο. Η αναγκαιότητα για ανακοίνωση όλων των συναλλαγών δημόσια αποκλείει αυτήν τη μέθοδο, αλλά η ιδιωτικότητα μπορεί ακόμα να διατηρείται σπάζοντας τη ροή της πληροφορίας σε μία άλλη τοποθεσία: κρατώντας τα δημόσια κλειδιά ανώνυμα. Το κοινό μπορεί να δει ότι κάποιος στέλνει ένα ποσό σε κάποιον άλλον, αλλά χωρίς πληροφορίες να συνδέουν συναλλαγές σε οποιονδήποτε. Αυτό είναι παρόμοιο με το επίπεδο πληροφορίας που απελευθερώνεται από τα χρηματιστήρια, όπου ο χρόνος και το μέγεθος των μεμονωμένων συναλλαγών, η «ταινία» συναλλαγών, δημοσιοποιείται, αλλά χωρίς να λέει ποια ήταν τα εμπλεκόμενα μέρη.



Σαν επιπλέον τοίχος προστασίας, πρέπει να χρησιμοποιείται ένα νέο κλειδί για κάθε συναλλαγή για να τα προφυλάξει από τη σύνδεση τους με ένα κοινό ιδιοκτήτη. Μερική σύνδεση είναι πάλι αναπόφευκτη με συναλλαγές πολλαπλών εισόδων, οι οποίες αναγκαστικά αποκαλύπτουν ότι οι είσοδοι ήταν στην κυριότητα του ίδιου ιδιοκτήτη. Ο κίνδυνος είναι ότι εάν ένας ιδιοκτήτης κλειδιού αποκαλυφθεί, η σύνδεση μπορεί να αποκαλύψει άλλες συναλλαγές που άνηκαν στον ίδιο ιδιοκτήτη.

11. Υπολογισμοί

Εξετάζουμε το σενάριο ενός επιτιθέμενου να προσπαθεί να δημιουργήσει μία εναλλακτική αλυσίδα γρηγορότερη από την έντιμη αλυσίδα. Ακόμα και αν αυτό επιτευχθεί, το σύστημα δεν είναι ανοιχτό σε αυθαίρετες αλλαγές, όπως δημιουργία αξίας από το τίποτα ή ανάληψη χρημάτων που δεν άνηκαν ποτέ στον επιτιθέμενο. Οι κόμβοι δεν πρόκειται να αποδεχτούν μία άκυρη συναλλαγή ως πληρωμή, και οι έντιμοι κόμβοι δεν θα αποδεχτούν ποτέ ένα μπλοκ να περιέχει τέτοιες. Ένας επιτιθέμενος μπορεί μόνο να προσπαθήσει να αλλάξει μία από τις δικές του συναλλαγές για να πάρει πίσω χρήματα που πρόσφατα ξόδεψε.

Ο αγώνας δρόμου μεταξύ της έντιμης αλυσίδας και της αλυσίδας του επιτιθέμενου μπορεί να χαρακτηριστεί ως ένας «διωνυμικός τυχαίος περίπατος» (Binomial Random Walk). Το επιτυχές αποτέλεσμα είναι η έντιμη αλυσίδα να επεκταθεί ένα μπλοκ, αυξάνοντας το προβάδισμα της +1, και το ανεπιτυχές αποτέλεσμα είναι η αλυσίδα του επιτιθέμενου να επεκταθεί ένα μπλοκ, μειώνοντας το χάσμα κατά -1.

Η πιθανότητα ενός επιτιθέμενου να προλάβει από ένα συγκεκριμένο έλλειμμα είναι ανάλογο με το πρόβλημα χρεοκοπίας του στοιχηματιστή (Gambler's ruin problem). Υποθέτουμε ότι ένας στοιχηματιστής με απεριόριστη πίστωση ξεκινάει από ένα έλλειμμα και παίζει δυνητικά έναν απεριόριστο αριθμό προσπαθειών ώστε να φτάσει στο νεκρό σημείο. Μπορούμε να υπολογίσουμε την πιθανότητα που θα φτάσει ποτέ στο νεκρό σημείο, ή την πιθανότητα που ο επιτιθέμενος θα προφτάσει ποτέ την έντιμη αλυσίδα, ως ακολούθως [8]:

p = πιθανότητα ένας έντιμος κόμβος να βρει το επόμενο μπλοκ
q = πιθανότητα ο επιτιθέμενος να βρει το επόμενο μπλοκ
q_z = πιθανότητα ο επιτιθέμενος να προλάβει ποτέ από z μπλοκ πίσω

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

Δεδομένης της υπόθεσης μας ότι p > q, η πιθανότητα πέφτει εκθετικά καθώς ο αριθμός των μπλοκ που πρέπει να προφτάσει μεγαλώνει. Με τις πιθανότητες εναντίον του, εάν δεν κάνει από νωρίς μία τυχερή εξόρμηση προς τα μπροστά, οι πιθανότητες του γίνονται ανύπαρκτα μικρές καθώς μένει κι άλλο πίσω.

Αναλογιζόμαστε τώρα πόσο πολύ πρέπει να περιμένει ο παραλήπτης μίας νέας συναλλαγής πριν να είναι επαρκώς σίγουρος ότι ο αποστολέας δεν μπορεί να αλλάξει τη συναλλαγή. Υποθέτουμε ότι ο αποστολέας είναι ένας επιτιθέμενος που θέλει να κάνει για λίγο τον παραλήπτη να πιστέψει ότι τον έχει πληρώσει, αλλάζοντας μετά από λίγο χρόνο που έχει περάσει την πληρωμή πίσω στον εαυτό του. Ο παραλήπτης θα προειδοποιηθεί όταν συμβαίνει αυτό, αλλά ο αποστολέας ελπίζει να μην είναι πολύ αργά.

Ο παραλήπτης δημιουργεί ένα νέο ζεύγος κλειδιών και δίνει το δημόσιο κλειδί στον αποστολέα λίγο πριν την υπογραφή. Αυτό αποτρέπει τον αποστολέα να δημιουργήσει μία αλυσίδα μπλοκ εκ των προτέρων δουλεύοντας πάνω της μέχρι να είναι αρκετά τυχερός να φτάσει αρκετά μπροστά μακριά, εκτελώντας εκείνη τη στιγμή τότε τη συναλλαγή. Μόλις η συναλλαγή έχει αποσταλεί, ο ανέντιμος κόμβος ξεκινάει να δουλεύει μυστικά σε μία παράλληλη αλυσίδα που περιέχει μία εναλλακτική έκδοση της συναλλαγής του.

Ο παραλήπτης περιμένει μέχρι η συναλλαγή να έχει προστεθεί σε ένα μπλοκ με z μπλοκ να έχουν συνδεθεί μετά από αυτό. Δεν γνωρίζει το ακριβές ποσό προόδου που έχει κάνει ο επιτιθέμενος, αλλά υποθέτοντας ότι στους έντιμους κόμβους χρειάστηκε ο μέσος αναμενόμενος χρόνος ανά μπλοκ, η δυνητική πρόοδος του επιτιθέμενου θα είναι μία Poisson κατανομή με αναμενόμενη τιμή:

$$\lambda = z\frac{q}{p}$$

Για να πάρουμε την πιθανότητα ο επιτιθέμενος να μπορεί τώρα να προφτάσει, πολλαπλασιάζουμε την πυκνότητα Poisson για κάθε ποσό προόδου που θα μπορούσε να έχει κάνει επί την πιθανότητα που θα μπορούσε να προφτάσει από εκείνο το σημείο:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

Αναδιάταξη για να αποφύγουμε την άθροιση της άπειρης ουράς της κατανομής...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Μετατρέποντας σε C κώδικα...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Τρέχοντας μερικά αποτελέσματα, μπορούμε να δούμε την πιθανότητα να πέφτει εκθετικά με το z.

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012

q=0.3
z=0    P=1.0000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

Λύνοντας για P μικρότερο από 0,1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Επίλογος

Έχουμε προτείνει ένα σύστημα για ηλεκτρονικές συναλλαγές χωρίς την ανάγκη για εξάρτηση από εμπιστοσύνη. Ξεκινήσαμε από το σύνηθες πλαίσιο κατασκευής νομισμάτων από ψηφιακές

υπογραφές, το οποίο παρέχει ισχυρό έλεγχο στην ιδιοκτησία, αλλά είναι ατελές χωρίς έναν τρόπο αποφυγής του διπλό-ξοδέματος. Για την επίλυση αυτού, προτείναμε ένα peer-to-peer δίκτυο για την καταγραφή ενός δημόσιου ιστορικού των συναλλαγών το οποίο γίνεται γρήγορα υπολογιστικά μη-πρακτικό για έναν επιτιθέμενο να αλλάξει εάν η πλειοψηφία της επεξεργαστικής ισχύος ελέγχεται από έντιμους κόμβους. Το δίκτυο είναι ανθεκτικό μέσα από τη μη-δομημένη του απλότητα. Οι κόμβοι εργάζονται όλοι ταυτόχρονα με ελάχιστο συντονισμό. Δεν χρειάζεται να αναγνωρίζονται, δεδομένου ότι τα μηνύματα δεν διευθύνονται σε ένα συγκεκριμένο μέρος και χρειάζεται μόνο να παραδίδονται με βάση την καλή θέληση του δικτύου. Οι κόμβοι μπορούν κατά βούληση να αποχωρούν και να ενώνονται ξανά με το δίκτυο, αποδεχόμενοι την αλυσίδα απόδειξης της εργασίας (proof-of-work) ως απόδειξη του τι συνέβη όσο απουσίαζαν. Αυτοί ψηφίζουν με την επεξεργαστική τους ισχύ, εκφράζοντας την αποδοχή τους για έγκυρα μπλοκ εργαζόμενοι για την επέκταση αυτών και απορρίπτοντας τα άκυρα μέσω της άρνησης τους να εργαστούν σε αυτά. Οτιδήποτε κανόνες και κίνητρα χρειάζονται μπορούν να επιβληθούν με αυτόν το μηχανισμό συναίνεσης.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," *In Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. *1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.