Bitcoin

Μία εξήγηση της λειτουργίας του κρυπτονομίσματος

Διονύσης "dionyziz" Ζήνδρος <dionyziz@gmail.com>

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Εθνικό Μετσόβιο Πολυτεχνείο

Φεβρουάριος 2012

Περιεχόμενα

Εισαγωγή

Το Bitcoin αποτελεί ένα πειραματικό αποκεντρωμένο κρυπτονόμισμα, ένα νομισματικό σύστημα δηλαδή χωρίς κεντρικό έλεγχο που η αρτιότητά του στηρίζεται στις αρχές της κρυπτογραφίας. Στο παρόν, αφού θίξουμε το πρόβλημα και τους λόγους ύπαρξης ενός αποκεντρωμένου κρυπτονομίσματος, θα παρουσιάσουμε τις βασικές αρχές λειτουργίας του συστήματος, καθώς και τη θεμελίωσή του τόσο από οικονομικής όσο και μαθηματικής άποψης. Θα παρουσιαστούν οι τεχνικές λεπτομέρειες του πρωτοκόλλου λειτουργίας του και η διαίσθηση ορθότητας και πληρότητας χωρίς τυπική μαθηματική απόδειξη. Θα δειχθούν επίσης οι λόγοι που το πρωτόκολλο επιτυγχάνει ασφάλεια συναλλαγών, αποφεύγει συναλλαγές που δεν επιτρέπονται και επιτυγχάνει ανωνυμία. Στόχος του παρόντος είναι η παρουσίαση του κρυπτονομίσματος και η παρουσίαση των βασικών αρχών λειτουργίας του και επιχειρείται μία απλή αλλά πλήρης εξήγηση των τεχνικών αρχών, χωρίς όμως να μπαίνουμε σε βάθος λεπτομερειών που δεν χρειάζονται. Απευθύνεται σε αναγνώστες με βασικές γνώσεις πολυπλοκότητας και υπολογιστικής δυσκολίας, κρυπτογραφίας και λειτουργίας κρυπτογραφικών συστημάτων, συμπεριλαμβανομένων αποκεντρωμένων συστημάτων, συστημάτων ψηφιακών υπογραφών και hashing.

Το πρόβλημα

Στην κρυπτογραφική κοινότητα, ιδιαίτερα στην κοινότητα των cypherpunks, υπάρχει η επιθυμία της προληπτικής χρήσης της κρυπτογραφίας ώστε να αποφεύγεται η δυνατότητα παραβίασης της ιδιωτικότητας από κρατικούς ή άλλους φορείς που έχουν τη δυνατότητα να κρυφακούνε σε ανταλλαγές δεδομένων, νόμιμα ή παράνομα. Οι παραδοσιακές online πληρωμές σήμερα δεν έχουν τα πλεονεκτήματα των offline πληρωμών. Συγκεκριμένα, απουσιάζει η δυνατότητα της ανώνυμης ανταλλαγής χρημάτων, αφού όλες οι online συναλλαγές γίνονται μέσω ειδικών, κεντρικών υπηρεσιών που έχουν πρόσβαση στην ταυτότητα των συμμετεχόντων. Τέτοιες υπηρεσίες όπως το PayPal απαιτούν να γνωρίζουν την ταυτότητα των ατόμων που συνδιαλλάσσονται με αποτέλεσμα να μην υπάρχει ανωνυμία. Το ίδιο ισχύει και για κάθε μορφής ηλεκτρονικές πληρωμές, ακόμη και αυτές που γίνονται χρησιμοποιώντας πιστωτικές κάρτες που απαιτούν υπηρεσίες όπως Visa και Mastercard. Σε κάθε περίπτωση, είναι αδύνατη η ανταλλαγή χρημάτων χρησιμοποιώντας κάποια ψευδώνυμη ταυτότητα, αφού απαιτείται η πιστοποίηση της πραγματικής ταυτότητας κάποιου μέσω αυστηρών μηχανισμών όπως το άνοιγμα τραπεζικού λογαριασμού που χρειάζεται προσωπική κρατικά πιστοποιημένη ταυτότητα με φωτογραφία, καθώς και πιστοποίηση της διεύθυνσης κατοικίας.

Οι υπηρεσίες αυτές που προσφέρουν δυνατότητες online πληρωμών διασφαλίζουν τις συναλλαγές των συμμετεχόντων, αλλά δεν επιτρέπουν τις ανώνυμες συναλλαγές όπως αυτές γίνονται χρησιμοποιώντας μετρητά και ταυτόχρονα χρεώνουν ένα μικρό ποσό για κάθε συναλλαγή, με αποτέλεσμα να είναι αδύνατη η χρήση online πληρωμών για μικροποσά.

Τέλος, ακόμη και η χρήση μετρητών ή κλασικών νομισμάτων όπως το ευρώ και το δολάριο έχει τα προβλήματά της, καθώς σε αυτή την περίπτωση το αντίστοιχο νόμισμα τυπώνεται από μία κυβέρνηση, με αποτέλεσμα να μπορεί να υπάρχει κεντρικός μακροοικονομικός έλεγχος ο οποίος ενδέχεται να είναι ανεπιθύμητος. Ακολουθώντας την παράδοση της κρυπτογραφικής κοινότητας στην προληπτική χρήση της κρυπτογραφικής τεχνολογίας χωρίς να θεωρεί κανείς δεδομένη την εμπιστοσύνη σε τρίτους φορείς όπως το κράτος, τα συστήματα του παρόντος θεωρούνται μη ικανοποιητικά.

Λύσεις που έχουν προκύψει για το συγκεκριμένο πρόβλημα κατά καιρούς είναι η χρήση χρυσού ή άλλων πολύτιμων υλικών που έχουν πραγματική αξία ώστε να μην υπάρχει η δυνατότητα μακροοικονομικού ελέγχου, αλλά οι τιμές τους να καθορίζονται από την ελεύθερη αγορά. Όμως κάτι τέτοιο δεν μπορεί να χρησιμοποιηθεί σε online πληρωμές καθώς είναι δύσχρηστο, χρονοβόρο και ανασφαλές αφού υπάρχει περίπτωση κλοπής ή απώλειας.

Το πρόβλημα αυτό αποτέλεσε το κίνητρο για την αναζήτηση μίας καλύτερης λύσης η οποία βασίζεται στα ψηφιακά νομίσματα.

Ιστορία

Το Bitcoin ξεκίνησε από τον Wei Dai που το 1998 δημοσίευσε στην mailing list της γνωστής κοινότητας πρακτικής κρυπτογραφίας και ανωνυμίας ”cypherpunks” ένα σκιαγράφημα που εξηγούσε την ιδέα με την οποία θα ήταν εφικτή μια οικονομία που δεν απαιτεί κεντρική

διοίκηση. Οι cypherpunks είναι γνωστοί για την προσπάθειά τους για χρήση της κρυπτογραφίας προληπτικά ώστε να πετύχουν ανωνυμία, ιδιωτικότητα και κατ' επέκταση πολιτικοοικονομική αλλαγή μέσω της ανάπτυξης εφαρμοσμένων και όχι ακαδημαϊκών συστημάτων τα οποία στοχεύουν σε πραγματική και ευρεία χρήση. Το σκιαγράφημα του Wei Dai με τίτλο "bmoney" έθεσε τα θεμέλια για την ανάπτυξη του Bitcoin.

Το 2009, ο Satoshi Nakamoto ανέπτυξε την πρώτη έκδοση του λογισμικού σε C++ και ταυτόχρονα δημοσίευσε το paper του με τίτλο "Bitcoin: A Peer-to-Peer Electronic Cash System". Το paper αυτό θεμελίωσε πλέον όλη τη θεωρία που ήταν απαραίτητη για την ανάπτυξη του συστήματος μαζί με μία σύντομη μαθηματική ανάλυση της ασφάλειας του συστήματος. Το λογισμικό σχεδιάστηκε όχι σαν απλό proof-of-concept, αλλά ως ένα ολοκληρωμένο σύστημα με σκοπό να χρησιμοποιηθεί άμεσα σε μεγάλη κλίμακα, μία κίνηση που ακολουθεί την παράδοση των cypherpunks. Το λογισμικό είναι ανοιχτού κώδικα κάτω από την άδεια χρήσης MIT. Ο Satoshi Nakamoto μετά την ολοκλήρωση της πρώτης έκδοσης του Bitcoin εξαφανίστηκε. Πολλές φήμες περιβάλλουν την προσωπικότητά του, καθώς λέγεται – όπως είναι παράδοση σε ανθρώπους που ασχολούνται με την κρυπτογραφία – ότι λόγω παράνοιας δεν αποκάλυψε ποτέ το πραγματικό του όνομα, και ότι η συγκεκριμένη ταυτότητα δεν είναι παρά ένα ψευδώνυμο. Κανείς δεν τον έχει συναντήσει από κοντά, δεν υπάρχουν πληροφορίες γι' αυτόν ή κάποια φωτογραφία και, παρ' όλο που δήλωνε Ιάπωνας στην καταγωγή, ο κώδικάς του και τα λεγόμενά του δεν περιείχαν ποτέ ούτε μία λέξη Ιαπωνικών.

Το σύστημα του Bitcoin συντηρείται και αναπτύσσεται σήμερα υπό τη μορφή ανοιχτού κώδικα από την κοινότητα των προγραμματιστών του Bitcoin.

Η ιδέα του Bitcoin

Το Bitcoin έρχεται να λύσει το πρόβλημα του κεντρικού νομισματικού ελέγχου. Προσφέρει γρήγορες πληρωμές που ολοκληρώνονται εντός 10 λεπτών, απουσία της απαίτησης για την ύπαρξη έμπιστης κεντρικής αρχής, καθώς η αξία του νομίσματος προέρχεται από την ελεύθερη αγορά, διασφαλίζει τις συναλλαγές χρησιμοποιώντας σύγχρονη, αποδεδειγμένα ισχυρή κρυπτογραφία, και παρέχει ανωνυμία στους ανθρώπους που συναλλάσσονται.

Το Bitcoin στηρίζεται στην ιδέα ότι ένα σύγχρονο νόμισμα είναι εικονικό. Δεν έχει δηλαδή πραγματικά την αξία που αντιπροσωπεύει. Καθώς κάτι τέτοιο μπορεί να είναι οποιοδήποτε αντικείμενο, πραγματικό ή ψηφιακό, για το οποίο υπάρχει συμφωνία ότι θα χρησιμοποιείται σε συναλλαγές, με την προϋπόθεση ότι δεν μπορεί να αντιγραφεί αυθαίρετα, το Bitcoin προτείνει τη χρήση ψηφιακής πληροφορίας ως νόμισμα.

Αποκέντρωση

Η αποκέντρωση του δικτύου επιτυγχάνεται με τη χρήση ενός peer-to-peer δικτύου στο οποίο συνδέονται όλοι οι συμμετέχοντες που θέλουν να χρησιμοποιήσουν το Bitcoin για τη διεξαγωγή των πληρωμών τους. Οι συμμετέχοντες τρέχουν το πρόγραμμα του Bitcoin στον υπολογιστή τους.

Αυτό μπορεί να είναι είτε το κλασικό Bitcoin client του Satoshi το οποίο έχει πλέον βελτιωθεί αισθητά από άλλους προγραμματιστές, είτε κάποιο από τα άλλα προγράμματα που υλοποιούν το πρωτόκολλο του Bitcoin σε κάποια άλλη γλώσσα. Καθώς τόσο το πρωτόκολλο όσο και το πρόγραμμα είναι ανοιχτού κώδικα, όπως απαιτείται στη σύγχρονη κρυπτογραφία, οι χρήστες μπορούν να ελέγξουν το κατά πόσο ο κώδικας ακολουθεί το θεωρητικό μοντέλο και ανταποκρίνεται στις αποδείξεις ασφάλειας που καταγράφονται στη θεωρία, ή τουλάχιστον να θεωρήσουν ότι αυτό μπορεί να γίνει από οποιονδήποτε ειδικό το επιθυμήσει. Το λογισμικό είναι διαθέσιμο για όλα τα σύγχρονα λειτουργικά συστήματα.

Αφού ο χρήστης τρέξει το πρόγραμμα στον υπολογιστή του, αυτό συνδέεται με άλλους κόμβους του δικτύου χρησιμοποιώντας τυπικούς μηχανισμούς εύρεσης άλλων κόμβων σε peer-to-peer σχήματα. Αυτά περιλαμβάνουν τη χρήση μίας λίστας από προκαθορισμένες διευθύνσεις IP από γνωστούς Bitcoin clients για την αρχική σύνδεση, τη χρήση κάποιων δημόσιων server για την εύρεση άλλων κόμβων (π.χ. μέσω IRC), και φυσικά τη δυνατότητα χειρωνακτικής σύνδεσης με γνωστή IP διεύθυνση. Έτσι, κάθε κόμβος συνδέεται με ένα πλήθος άλλων ομότιμων κόμβων στο δίκτυο. Επιπλέον, κάθε κόμβος παράγει ένα δημόσιο κλειδί το οποίο δημοσιεύει στο δίκτυο, και κρατάει το αντίστοιχο ιδιωτικό του κλειδί κρυφό στο τοπικό σύστημα. Το ιδιωτικό κλειδί του χρήστη είναι απαραίτητο για να γίνουν οι πληρωμές, συνεπώς θα πρέπει να προστατευθεί κατάλληλα, αφού κάποιος αντίπαλος θα μπορούσε, χρησιμοποιώντας το, να διεξάγει πληρωμές χρησιμοποιώντας τα χρήματα του χρήστη.

Σχήμα πληρωμών

Έχοντας δεδομένο ότι ένας χρήστης στο δίκτυο έχει στην κατοχή του ένα συγκεκριμένο πλήθος νομισμάτων, η βασική ιδέα στην ανταλλαγή τους είναι η χρήση ψηφιακών υπογραφών. Συγκεκριμένα, ο αποστολέας των χρημάτων (Bob) υπογράφει ψηφιακά την επιθυμία του να πραγματοποιήσει μία συναλλαγή, περιλαμβάνοντας το όνομα του παραλήπτη (Alice) στο μήνυμά του. Επιβεβαιώνοντας την υπογραφή του Bob, η Alice μπορεί να σιγουρευτεί ότι αυτός έκανε πράγματι τη συγκεκριμένη πληρωμή. Οι υπογραφές στο σύστημα γίνονται πάνω σε hashes των μηνυμάτων και όχι στα ίδια τα μηνύματα για λόγους ταχύτητας αλλά και παράδοσης.

Το πρώτο πρόβλημα σε ένα τέτοιο σχήμα είναι ότι τα χρήματα δεν πρέπει να είναι αυτοδημιούργητα. Δηλαδή είναι επιθυμητό ο κάθε χρήστης να μην μπορεί αυθαίρετα να εκδόσει χρήματα τα οποία στη συνέχεια να υπογράψει ώστε να πραγματοποιήσει μία πληρωμή. Με λίγα λόγια, θέλουμε κάθε κόμβος στο δίκτυο να μπορεί να επιβεβαιώσει ότι ο εκάστοτε χρήστης πράγματι έχει στην κατοχή του τα χρήματα που δίνει όταν τα δίνει. Ο μόνος τρόπος να επιτευχθεί κάτι τέτοιο, αφού δεν υπάρχει κάποια έμπιστη αρχή, είναι γνωστοποιώντας σε όλο το δίκτυο το ποιος έχει τι. Αυτό είναι απαραίτητο ώστε να μπορούμε να βεβαιωθούμε ότι ένα νόμισμα είναι έγκυρο και ότι πρόκειται να ξοδευτεί από τον κάτοχό του μόνο μία φορά.

Το δίκτυο αποθηκεύει συλλογικά ποιος έχει τι. Έτσι, κάθε παραλήπτης μπορεί να επιβεβαιώσει ότι τα χρήματα που λαμβάνει από τον αποστολέα ήταν στην κατοχή του αποστολέα πριν την αποστολή τους. Όταν κάποιος νέος κόμβος συνδέεται στο δίκτυο, οι

κόμβοι με τους οποίους συνδέεται (γείτονες) τον ενημερώνουν για το πού ανήκουν τα νομίσματα που υπάρχουν στο δίκτυο. Πιο συγκεκριμένα, όταν ένας κόμβος συνδέεται στο δίκτυο ενημερώνεται για το πλήρες ιστορικό της ανταλλαγής χρημάτων που έχει διενεργηθεί στο δίκτυο από την αρχή της ύπαρξης του δικτύου μέχρι και τη στιγμή της σύνδεσής του κόμβου σε αυτό, διαδικασία που ονομάζεται συγχρονισμός.

Για να μπορέσει να διατηρήσει κάθε κόμβος τη γνώση για το τι χρήματα υπάρχουν στο δίκτυο είναι απαραίτητο να γνωστοποιούνται και οι νέες συναλλαγές. Αυτό επιτυγχάνεται με ένα μηχανισμό που είναι γνωστός ως broadcasting. Κατά το broadcasting, όταν δύο κόμβοι πραγματοποιήσουν μία συναλλαγή, γνωστοποιούν στους γείτονές τους τις λεπτομέρειες αυτής της συναλλαγής. Αυτές περιλαμβάνουν τον αποστολέα, τον παραλήπτη, καθώς και το ποσό της συναλλαγής. Οι γείτονες, με τη σειρά τους, γνωστοποιούν αναδρομικά τις συναλλαγές σε όλο το δίκτυο.

Ανωνυμία

Η δημοσίευση των συναλλαγών στο δίκτυο καταστρέφει την ανωνυμία τους, καθώς κάθε κόμβος έχει πρόσβαση στο πλήρες ιστορικό όλων των συναλλαγών που έχουν γίνει στο παρελθόν από όλους τους άλλους. Παρ' όλα αυτά, είναι εύκολο να δημιουργήσουμε ένα σχήμα στο οποίο η ανωνυμία διατηρείται παρ' όλο που όλες οι συναλλαγές δημοσιεύονται. Παραλλάσσουμε το σύστημα χρησιμοποιώντας ένα διαφορετικό ιδιωτικό κλειδί για κάθε συναλλαγή. Αυτό σημαίνει ότι χρησιμοποιούμε ένα συγκεκριμένο κλειδί για να λάβουμε ένα ποσό χρημάτων και στη συνέχεια το ίδιο κλειδί για να πληρώσουμε χρησιμοποιώντας τα χρήματα που λάβαμε με το συγκεκριμένο κλειδί. Όμως, όταν θα λάβουμε ένα άλλο ποσό χρημάτων από κάποιον άλλο κόμβο του δικτύου και θα το χρησιμοποιήσουμε για να κάνουμε μία πληρωμή κάπου αλλού, θα χρησιμοποιηθεί ένα διαφορετικό κλειδί για τη συναλλαγή.

Η δημιουργία ενός κλειδιού ανά συναλλαγή είναι εύκολη και μπορεί να γίνεται αυτόματα. Φροντίζοντας να μην υπάρχει αντιστοιχία μεταξύ IP διεύθυνσης και κλειδιών και καθώς κάθε κόμβος δεν έχει όνομα, το δίκτυο μπορεί έτσι να πετύχει απόλυτη ανωνυμία. Αυτό είναι εφικτό διότι δεν είναι δυνατή η αντιστοίχηση δύο κλειδιών με το γεγονός ότι χρησιμοποιήθηκαν από το ίδιο πρόσωπο.

Σε αυτό το σχήμα, ο κάθε χρήστης έχει μία πλήρη γνώση των στατιστικών στοιχείων της συνολικής οικονομίας, με κάθε λεπτομέρεια, αλλά ανώνυμα. Μπορεί δηλαδή να μάθει το τζίρο που πραγματοποιείται σε ολόκληρο το δίκτυο, τα ποσά που ανταλλάσσονται, τη συχνότητα με την οποία γίνονται συναλλαγές, κ.ό.κ. αλλά όχι τις ταυτότητες αυτών που πραγματοποιούν τις συναλλαγές. Αυτού του τύπου η ανωνυμία μοιάζει με την ανωνυμία που υπάρχει σε χρηματιστηριακές αγορές όπου ανακοινώνεται μία πώληση ή αγορά μετοχών όσον αφορά τα χρηματιστηριακά της στοιχεία, χωρίς όμως να φαίνεται η ταυτότητα του αγοραστή ή του πωλητή.

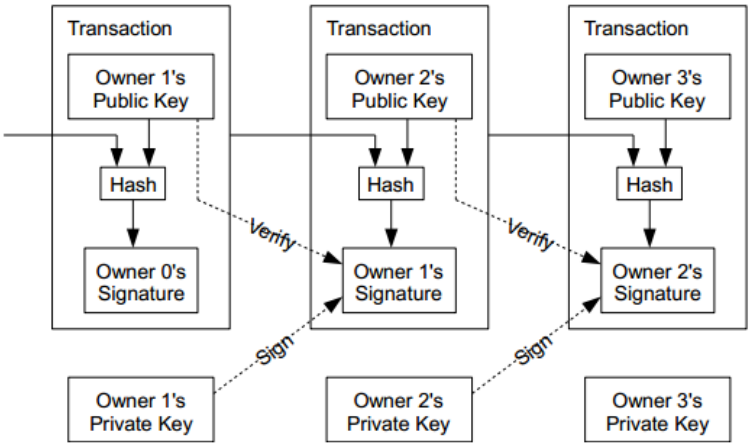
Ορισμός νομίσματος

Ας προχωρήσουμε, τώρα, σε μία πιο τεχνική ανάλυση της φύσης των νομισμάτων του συστήματος και των υπογραφών με λεπτομέρεια. Αυτό είναι απαραίτητο για την εξήγηση του πώς ακριβώς είναι εφικτό να μπορεί κανείς να αποδείξει ότι έχει στην κατοχή του ένα νόμισμα που πράγματι του ανήκει και δεν το παρήγαγε μόνος του αυθαίρετα. Μας επιτρέπει επίσης να δούμε ότι ένα νόμισμα μπορεί να ξοδευτεί αποκλειστικά από τον κάτοχό του και να αποδείξουμε ότι η πιθανότητα διπλού ξοδέματος του ίδιου νομίσματος μπορούμε να πετύχουμε να είναι όσο μικρή επιθυμούμε. Για να πετύχουμε αυτές τις ιδιότητες που είναι απαραίτητες για ένα σύστημα που διασφαλίζει τις συναλλαγές, είναι χρήσιμο κάθε νόμισμα να έχει μία ταυτότητα και να οριστεί σαν οντότητα. Καθώς πρόκειται για ένα αποκεντρωμένο δίκτυο, δεν είναι δυνατόν κάθε νόμισμα να έχει έναν αύξοντα αριθμό ή η ταυτότητά του να παράγεται από μία κεντρική αρχή, αλλά θα πρέπει να δημιουργείται και να ελέγχεται αποκεντρωμένα.

Το νόμισμα στο σύστημα του Bitcoin ορίζεται ως μία αλυσίδα ψηφιακών υπογραφών. Το νόμισμα ξεκινάει τη ζωή του με την εξόρυξη (βλ. παρακάτω ενότητα) η οποία έχει ως αποτέλεσμα τη δημιουργία του νομίσματος που είναι ένα αλφαριθμητικό από δεδομένα που περιλαμβάνουν πληροφορίες για το νόμισμα όπως για παράδειγμα η αξία του. Κατά την ανταλλαγή του νομίσματος από τον πρώτο κάτοχο, τον Bob, στον δεύτερο, την Alice, ο Bob παραθέτει (με απλή παράθεση αλφαριθμητικών) το αρχικό νόμισμα με το δημόσιο κλειδί της Alice. Στη συνέχεια εφαρμόζει τη συνάρτηση κατακερματισμού (hash function) στο αποτέλεσμα και το υπογράφει χρησιμοποιώντας το ιδιωτικό του κλειδί. Αυτό είναι και το νόμισμα που ανήκει στην Alice.

Όταν η Alice με τη σειρά της θελήσει να πληρώσει τον Charlie χρησιμοποιώντας τα χρήματα που πήρε από τον Bob, θα παραθέσει το δικό της νόμισμα με το δημόσιο κλειδί του Charlie, θα κατακερματίσει το αποτέλεσμα, και θα το υπογράψει με το ιδιωτικό της κλειδί. Καθώς μόνο η Alice έχει στην κατοχή της το ιδιωτικό της κλειδί, το νόμισμα μπορεί να ξοδευτεί μόνο από την Alice και από κανέναν άλλο. Το ότι το νόμισμα προορίζεται πράγματι για τον Charlie μπορεί να το επιβεβαιώσει ο ίδιος απλώς κοιτάζοντας τα περιεχόμενα του νομίσματος που έλαβε, καθώς αυτό θα πρέπει να περιλαμβάνει το δημόσιο κλειδί του. Αν δεν το περιλαμβάνει, τότε ο Charlie μπορεί να αρνηθεί τη συναλλαγή. Το ότι το νόμισμα προήλθε πράγματι από την Alice μπορεί ο Charlie να το ελέγξει εύκολα κάνοντας πιστοποίηση της υπογραφής της Alice. Θα πρέπει, φυσικά, εκτός από απλή πιστοποίηση να ελέγξει και ότι το νόμισμα ήταν πράγματι στην κατοχή της Alice πριν περιέλθει στην κατοχή του επιβεβαιώνοντας ότι το δημόσιο κλειδί που περιλαμβάνεται στο προηγούμενο νόμισμα αντιστοιχεί στο ιδιωτικό κλειδί με το οποίο υπογράφηκε ψηφιακά το νέο νόμισμα που του στάλθηκε.

Η αλληλουχία αυτή υπογραφών φαίνεται στο παρακάτω σχήμα:



Εικόνα 1: Αλληλουχία νομισματικών συναλλαγών στο σύστημα Bitcoin

Διπλό ξόδεμα

Παρ' όλο που έχουμε εγγυηθεί ότι μόνο οι κάτοχοι ενός νομίσματος μπορούν να το ξοδέψουν και ότι ο παραλήπτης του νομίσματος μπορεί να επικυρώσει ότι το νόμισμα προήλθε από τον αποστολέα στον οποίο ανήκει καθώς και ότι ο παραλήπτης είναι πράγματι ο ίδιος, δεν έχουμε ακόμη πετύχει καμία εγγύηση σε σχέση με το διπλό ξόδεμα νομισμάτων. Το πρόβλημα έγκειται στο ότι ένας αποστολέας μπορεί να ξοδέψει το ίδιο νόμισμα δύο φορές. Καθώς το δίκτυο είναι αποκεντρωμένο, ένα διπλό ξόδεμα μπορεί να μην γίνει άμεσα αντιληπτό, αλλά να χρειαστεί μερικά λεπτά μέχρι να φανεί στο δίκτυο.

Σημαντικότερο, δε, πρόβλημα, αποτελεί το διπλό ξόδεμα που ενδέχεται να γίνει μετά από ένα μεγαλύτερο χρονικό διάστημα όπως ένας μήνας ή ένα έτος. Σε αυτή την περίπτωση δεν είναι εφικτό να ελεγχθεί με σιγουριά ο πραγματικός παραλήπτης ενός νομίσματος, καθώς ένας κακόβουλος αντίπαλος μπορεί να ισχυριστεί ότι μία συναλλαγή έλαβε χώρα πολύ νωρίτερα στο παρελθόν, αφού δεν υπάρχει κάποια έμπιστη αρχή που να αποθηκεύει τη χρονική αλληλουχία με την οποία συνέβησαν οι συναλλαγές. Είναι, επιπλέον, πρόβλημα που δεν μπορεί να λυθεί χωρίς κάποια αλλαγή του σχήματος. Η προφανής λύση που απορρίπτει μία συναλλαγή αν γίνει πολλαπλές φορές δεν είναι αποδεκτή, καθώς κάτι τέτοιο επιτρέπει σε κάποιον κακόβουλο να ακυρώσει τις συναλλαγές του παρελθόντος διπλοξοδεύοντας στο μέλλον, κάτι που θα έχει ως αποτέλεσμα να χάσει τα χρήματά του και ο ίδιος αλλά και ο παραλήπτης των χρημάτων, αλλά παραμένει ανεπιθύμητο, αφού θα θέλαμε οι συναλλαγές να πιστοποιούνται και ο παραλήπτης να μπορεί με σιγουριά να λάβει τα χρήματά του και να τα ξοδέψει με τη σειρά του. Επιπλέον, ένας κακόβουλος παίκτης δεν μπορεί να εντοπιστεί και να απομονωθεί, αφού, λόγω ανωνυμίας, είναι αδύνατο να ξέρουμε σε ποια διεύθυνση IP αντιστοιχεί, και μπορεί να συνεχίσει να πράττει κακόβουλα χρησιμοποιώντας κάθε φορά ένα νέο δημόσιο κλειδί.

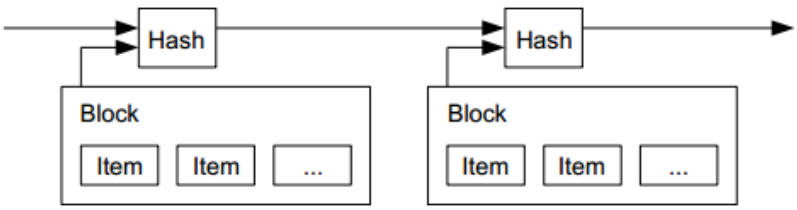
Το πρόβλημα αυτό λύνεται στο Bitcoin χρησιμοποιώντας ένα σύστημα βέλους του χρόνου που μας επιτρέπει να γνωρίζουμε με σιγουριά την χρονική αλληλουχία των συναλλαγών. Υποθέτοντας ότι είναι εφικτό να γνωρίζουμε ποια συναλλαγή έγινε πριν από ποια άλλη, το σύστημά μας διορθώνεται εύκολα θεωρώντας έγκυρη μόνο την πρώτη συναλλαγή στην

οποία βρέθηκε ένα νόμισμα. Έτσι, όταν το νόμισμα ξοδευτεί, ο παραλήπτης μπορεί να ελέγξει ότι το νόμισμα δεν ξοδεύτηκε ξανά στο παρελθόν και να δεχτεί τη συναλλαγή, ή να την απορρίψει αν το νόμισμα έχει ξαναξοδευτεί.

Φυσικά, είναι αδύνατο να στηριχθεί κανείς στην ψηφιακή υπογραφή ως εγγύηση της ημερομηνίας διεξαγωγής μίας συναλλαγής, αφού κάποιος κακόβουλος αντίπαλος μπορεί να υπογράψει ψευδή μηνύματα. Σε παραδοσιακά ακαδημαϊκά κρυπτοσυστήματα, το βέλος του χρόνου υλοποιείται με μία δημοσίευση (για παράδειγμα σε κάποια εφημερίδα ή το Usenet), κάτι που μπορεί κανείς να επιβεβαιώσει ανεξάρτητα. Κάτι τέτοιο δεν μπορεί να γίνει στην περίπτωση του Bitcoin, αφού καταφεύγουμε στη χρήση έμπιστης αρχής που είναι αυτό που προσπαθήσαμε από την αρχή να αποφύγουμε. Το Bitcoin χρησιμοποιεί ένα καινοτόμο σύστημα βέλους του χρόνου που λειτουργεί χρησιμοποιώντας αλυσίδες απόδειξης εργασίας.

Απόδειξη εργασίας

Οι κόμβοι του δικτύου του Bitcoin μοιράζονται μία κοινή αλυσίδα που περιλαμβάνει τις συναλλαγές με τη σειρά που έγιναν. Αυτή η αλυσίδα είναι κοινή για όλους και αποτελείται από μία συνδεδεμένη λίστα από blocks. Κάθε block περιλαμβάνει μία λίστα από συναλλαγές που έγιναν κοντά σε μία δεδομένη χρονική στιγμή. Η διαδικασία της αλυσίδας κατακερματίζει κάθε block και κάθε επόμενο block περιλαμβάνει τον κατακερματισμό του προηγούμενου block μέσα στα δεδομένα του, με αποτέλεσμα κάθε επόμενο block που προστίθεται στην αλυσίδα να μην μπορεί να δημιουργηθεί χωρίς να γνωρίζει την ύπαρξη του προηγούμενου block, αφού θα πρέπει να το κατακερματίσει για να υπολογίσει την τιμή του τελικού κατακερματισμού.



Εικόνα 2: Αλληλουχία blocks απόδειξης εργασίας στο σύστημα Bitcoin

Παρ' όλο που τα blocks μπορούν να τοποθετηθούν χρονολογικά, κάποιος κόμβος μπορεί εύκολα να αλλάξει τη σειρά εμφάνισης δύο blocks μέσα στην αλυσίδα αλλάζοντας τους αντίστοιχους κατακερματισμούς και παράγοντας νέους όπου χρειάζεται, πράγμα ανεπιθύμητο, αφού θα μπορούσε να ισχυριστεί ψευδή σειρά γεγονότων μέσα στο χρόνο. Για την αποφυγή αυτού του προβλήματος, εισάγουμε ένα τεχνητά δύσκολο κρυπτογραφικό πρόβλημα στην παραγωγή κάθε block.

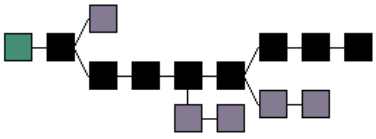
Υποθέτοτας ότι το πρόβλημα της αντιστροφής της συνάρτησης κατακερματισμού είναι δυσεπίλυτο, απαιτούμε την εύρεση μερικού αντιστρόφου της συνάρτησης για την παραγωγή ενός block. Συγκεκριμένα, ζητάμε ο κατακερματισμός του block που θα παραχθεί να είναι μικρότερος από ένα δεδομένο αριθμό που παράγεται συλλογικά από το peer-to-peer δίκτυο. Ο τρόπος που μπορεί ο κόμβος που παράγει το εκάστοτε block να αλλάξει τον

κατακερματισμό του είναι μέσω ενός nonce, μίας τιμής που παρατίθεται στο block και χρησιμεύει απλώς για να αλλάξει την τιμή του κατακερματισμού. Καθώς η συνάρτηση κατακερματισμού πιστεύουμε ότι είναι μίας κατεύθυνσης, ο μόνος τρόπος για να δημιουργηθεί ο κατακερματισμός εντός των επιθυμητών ορίων είναι με αλλεπάλληλες δοκιμές διαφορετικών nonces, διαδικασία που είναι υπολογιστικά εκθετική ως προς το πλήθος των ψηφίων του κατακερματισμού. Θέτοντας συλλογικά το peer-to-peer δίκτυο κατάλληλα όρια για τον επιθυμητό κατακερματισμό, μπορεί να καθορίσει το βαθμό δυσκολίας αυτής της διαδικασίας.

Τα όρια στον κατακερματισμό ορίζονται συλλογικά από το δίκτυο από έναν προκαθορισμένο αλγόριθμο. Στη συνέχεια, όλοι οι κόμβοι του δικτύου επιχειρούν ταυτόχρονα να παραγάγουν ένα νέο block που περιλαμβάνει όλες τις συναλλαγές που δεν περιλαμβάνονται στην μέχρι τώρα γνωστή αλυσίδα και έχει τις απαιτούμενες ιδιότητες που αποδεικνύουν την εργασία του κόμβου. Καθώς το δίκτυο μπορεί να ελέγξει κατά βούληση τη δυσκολία διεκπεραίωσης της απόδειξης εργασίας, μπορεί να ελέγξει συλλογικά τη συχνότητα παραγωγής νέων blocks.

Είναι φανερό ότι, παρ’ όλο που απαιτείται απόδειξη εργασίας από τον εκάστοτε κόμβο που παράγει το κάθε block ως τελευταίο της αλυσίδας απόδειξης εργασίας, το block αυτό πρέπει κατά τα γνωστά να περιέχει μόνο έγκυρες συναλλαγές. Αυτό είναι εγγυημένο διότι οι υπόλοιποι κόμβοι δεν θα κάνουν ποτέ δεκτό ένα block στο τέλος μίας αλυσίδας που περιέχει διπλό ξόδεμα του ίδιου νομίσματος ή ξόδεμα νομίσματος που δεν ανήκει σε κάποιον.

Όταν ένα νέο block υπολογίζεται από κάποιον κόμβο, αυτό γίνεται broadcast σε όλους τους γείτονές του οι οποίοι με τη σειρά τους το μεταφέρουν σε όλο το δίκτυο. Παρ’ όλο που η συχνότητα παραγωγής blocks ελέγχεται ώστε να είναι αρκετά χαμηλή (π.χ. 1 block κάθε 10 λεπτά) για να μην παράγονται δύο blocks ταυτόχρονα από δύο διαφορετικούς κόμβους, αυτό μπορεί σε ορισμένες περιπτώσεις να συμβεί, αφού η αντιστροφή της συνάρτησης κατακερματισμού δεν είναι προβλέψιμη. Σε αυτή την περίπτωση, όποιος κόμβος λάβει και τα δύο αυτά blocks που επιμηκύνουν την αλυσίδα των blocks, διαλέγει εκείνη την αλυσίδα που περιέχει τις περισσότερες συναλλαγές. Αν έχουν το ίδιο μήκος, τότε διαλέγει αυθαίρετα κάποια από όλες και την αποδέχεται. Ένας κόμβος δηλώνει την αποδοχή ενός block δουλεύοντας πάνω στη δημιουργία ενός νέου block ξεκινώντας από την αλυσίδα που τελειώνει σε αυτό. Σε περίπτωση που κάποιος έχει λάβει δύο εναλλακτικές πραγματικότητες σε σχέση με τη μορφή της αλυσίδας και επιλέξει να δουλέψει στην επέκταση μίας από αυτές, οι συναλλαγές που υπάρχουν στην άλλη θα συμπεριληφθούν στο αμέσως επόμενο block της τρέχουσας αλυσίδας και έτσι δεν θα χαθούν. Ο κόμβος που θα παραγάγει το επόμενο block είναι εκείνος που θα αποφασίσει από πού τελικά θα συνεχιστεί η πραγματική αλυσίδα και ποιο μέρος της αλυσίδας θα μείνει ορφανό.



Εικόνα 3: Η αλυσίδα απόδειξης εργασίας του συστήματος Bitcoin με ορφανούς κόμβους

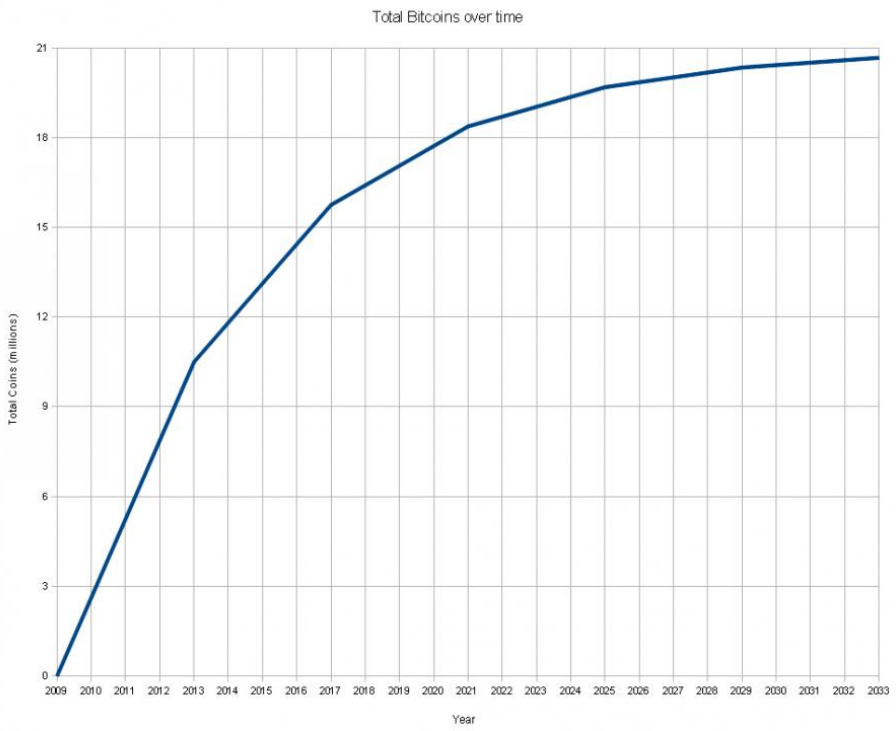
Στο παραπάνω σχήμα, κάθε τετράγωνο αποτελεί ένα block που περιέχει πολλαπλές συναλλαγές που έγιναν σε κοντινές χρονικές στιγμές. Η τρέχουσα αλυσίδα εμφανίζεται με μαύρο χρώμα. Με μοβ χρώμα εμφανίζονται οι ορφανές αλυσίδες, αλυσίδες που δημιουργήθηκαν επεκτείνοντας την τρέχουσα αλυσίδα ταυτόχρονα με άλλες επεκτάσεις, αλλά που τελικά δεν επιλέχθηκαν ως η τρέχουσα αλυσίδα. Με πράσινο φαίνεται το αρχικό block.

Η ύπαρξη μίας συναλλαγής σε ένα block στην αλυσίδα πιστοποιεί ότι η συναλλαγή έχει πραγματοποιηθεί. Όσο βαθύτερα βρίσκεται ένα block μέσα στην αλυσίδα, τόσο περισσότερο πιστοποιημένη είναι η συναλλαγή. Αυτό γίνεται εμφανές από τον υπολογισμό του χρόνου που χρειάζεται για να αλλάξει κανείς την αλυσίδα ώστε να αναδιατάξει τις συναλλαγές, να ακυρώσει μία συναλλαγή, ή να προσθέσει μία συναλλαγή πριν από κάποια δεδομένη συναλλαγή, ο οποίος είναι εκθετικός ως προς το πλήθος των blocks που έχουν προστεθεί μετά από το block που περιέχει τη δεδομένη συναλλαγή. Έτσι, κάποιος που θέλει να επιβεβαιώσει ότι η συναλλαγή του θα είναι πιστοποιημένη, μπορεί να περιμένει έως ότου εμφανιστούν 5 ή 6 blocks που πιστοποιούν τη συναλλαγή του ώστε να είναι σίγουρος πως δεν θα μπορέσει να μεταβληθεί στο μέλλον. Ο ακριβής υπολογισμός της πιθανότητας να ακυρωθεί μία συναλλαγή από έναν κακόβουλο παίκτη δεδομένου ότι έχει προστεθεί ένα συγκεκριμένο πλήθος από blocks στην τρέχουσα αλυσίδα και με δεδομένη CPU δύναμη παρουσιάστηκε από τον Nakamoto.

Η αλλαγή της αλυσίδας απόδειξης εργασίας είναι δύσκολη για έναν αντίπαλο, καθώς η αλυσίδα επεκτείνεται διαρκώς. Για να μπορέσει να έχει έλεγχο της αλυσίδας ο κακόβουλος παίκτης, θα πρέπει να ελέγχει την πλειοψηφία της CPU δύναμης του δικτύου. Στην υπόθεση ότι κάτι τέτοιο δεν πρόκειται να συμβεί στηρίζεται και η ασφάλεια του συστήματος Bitcoin.

Εξόρυξη

Η παραγωγή νέων blocks ονομάζεται εξόρυξη. Η πρώτη εξόρυξη έγινε από τον Satoshi και ονομάζεται block γέννησης (genesis block). Κάθε έγκυρη αλυσίδα ξεκινά από αυτό το block γέννησης. Κάθε εξόρυξη που γίνεται υπογράφεται από τον κόμβο που την πραγματοποίησε. Η εξόρυξη, εκτός από την πιστοποίηση συναλλαγών που περιλαμβάνει, ανταμοίβει και τον κόμβο που την πραγματοποίησε με ένα ποσό Bitcoin που δημιουργούνται από τη συγκεκριμένη εξόρυξη. Αυτός είναι και ο τρόπος με τον οποίο παράγονται τα Bitcoin. Το ποσό που παράγεται από κάθε εξόρυξη είναι προσυμφωνημένο από το δίκτυο και μειώνεται σταδιακά ώστε ο διαθέσιμος αριθμός Bitcoin στην αγορά να συγκλίνει στα 21,000,000 Bitcoin. Η συνάρτηση σύγκλισης φαίνεται στο παρακάτω σχήμα:



Εικόνα 4: Συνάρτηση συνολικής διαθεσιμότητας Bitcoin ανά έτος

Τεχνικές λεπτομέρειες

Το σχήμα υπογραφής που χρησιμοποιείται είναι η υπογραφή ελλειπτικών καμπυλών DSA, μία παραλλαγή του σχήματος Elgamal πάνω σε ελλειπτικές καμπύλες, ενώ η συνάρτηση κατακερματισμού που χρησιμοποιείται είναι μονό ή διπλό SHA256 κατά περίπτωση. Η υλοποίηση του αρχικού client χρησιμοποιεί C++ με εκτενή χρήση των βιβλιοθηκών STL και boost, καθώς και της κρυπτογραφικής βιβλιοθήκης OpenSSL.

Στατιστικά στοιχεία

Το Φεβρουάριο του 2012, το Bitcoin έχει μία τρέχουσα αλυσίδα που περιέχει 167,000 blocks. Η ισοτιμία Bitcoin και ευρώ είναι 1BTC = 3.27€, ενώ μπορεί κανείς εύκολα να αγοράσει και να πουλήσει Bitcoin είτε με ιδιώτες είτε μέσω εταιριών που παρέχουν υπηρεσίες ForEx. Υπάρχουν 8,354,750BTC σε κυκλοφορία, συνολικής αξίας 27,000,000€. Η συνολική συχνότητα κατακερματισμού του δικτύου αυτή τη στιγμή ανέρχεται στα 9THz, ρυθμός που επιτυγχάνεται με τη συμμετοχή πολλών μηχανημάτων που είναι πλήρως αφιερωμένα στην εξόρυξη Bitcoin με χρήση διάφορων μεθόδων όπως κατακερματισμός μέσω GPU παραλληλισμού. Καθώς το σύστημα του Bitcoin είναι ακόμη σε μικρή χρήση σε σχέση με άλλα νομίσματα, παρ' όλο που έχει υιοθετηθεί και από ανθρώπους έξω από την κρυπτογραφική κοινότητα, αναμένεται εν τέλει να φανεί αν το πείραμα του κρυπτονομίσματος θα μπορέσει να λειτουργήσει, τόσο από οικονομικής και πολιτικής όσο και από τεχνικής πλευράς, όπως η κοινότητα των cypherpunks οραματιζόταν από την αρχή της δημιουργίας της.

Βιβλιογραφία

1. **The Bitcoin community**, 2009 - 2012: Bitcoin Wiki
2. **Satoshi Nakamoto**, 2009: ”Bitcoin: A Peer-to-Peer Electronic Cash System”
3. **Wei Dai**, 1998: “Bmoney”
4. **The Bitcoin developers**, 2009 - 2012: Πηγαίος κώδικας του Bitcoin
5. **The Bitcoin developers**, 2009 - 2012: Bitcoin client website