₿itcoin
Ο Απόλυτος Οδηγός

THE BITCOIN GUIDEBOOK

Όλα τα μυστικά για το πρώτο
αποκεντρωμένο κρυπτονόμισμα στον κόσμο

Ian DeMartino

[2]

Πρακτικός οδηγός αγοράς, αποθήκευσης και ανάλωσης bitcoins

> «Επιλέξαμε να τοποθετήσουμε τα χρήματά μας και την πίστη μας σε ένα μαθηματικό πλαίσιο ελεύθερο από την πολιτική και το ανθρώπινο σφάλμα».
>
> — Tyler Winklevoss, επιχειρηματίας και ολυμπονίκης

Αποφασίσατε, λοιπόν, ότι θέλετε μερικά bitcoins. Ακούγεται αρκετά απλό, αλλά τι γίνεται τώρα; Μία σημαντική απόφαση που πρέπει να λάβετε είναι τι ακριβώς θέλετε να κάνετε με τα bitcoins που αποκτάτε.

Ας τα πάρουμε από την αρχή: Ξεχάστε ότι μπορείτε να αποκτήσετε ένα σημαντικό αριθμό bitcoins δωρεάν. Για λόγους που θα εξηγήσω σε επόμενο κεφάλαιο, δεν είναι πλέον εφικτό για τον μέσο χρήστη να αποκτήσει bitcoins μέσω εξόρυξης, δηλαδή της διαδικασίας που παράγει bitcoins. Υπάρχουν κάποια πράγματα που ονομάζονται «πηγές», που προσφέρουν μικρές ποσότητες bitcoins δωρεάν ή ως αντάλλαγμα για την παρακολούθηση διαφημίσεων, όμως κάθε φορά παράγουν κλάσματα ενός σεντ.

Είναι πολύ καλύτερη ιδέα να αγοράσετε απλώς bitcoins. Και τώρα, το ερώτημα είναι: πού και πώς θα τα αγοράσετε και τι θέλετε να τα κάνετε όταν τα αποκτήσετε;

Ας ασχοληθούμε με το πρώτο ερώτημα. Μπορείτε να αγοράσετε bitcoins είτε δωρεάν, είτε μέσω κάποιου άλλου, είτε από ένα ανταλλακτήριο. Επί του παρόντος, τα πιο ευυπόληπτα ανταλλακτήρια στις Η.Π.Α. είναι το Circle και το Coinbase. Η συμμετοχή σε αυτά σημαίνει ότι θα πρέπει να ακολουθείτε τους σχετικούς κανονισμούς, κυρίως τον Know-Your-Customer (KYC) και τον Anti-Money-Laundering (AML). Αυτό σημαίνει ότι θα υπάρχει κάποιο επίπεδο ταυτοποίησης. Αυτό σημαίνει ότι θα υπάρξει κάποιο επίπεδο επιβεβαίωσης της ταυτότητας, τυπικά μια σκαναρισμένη ταυτότητα και ένας λογαριασμός που αποδεικνύει τη διεύθυνση κατοικίας.

Και τα δύο ανταλλακτήρια, και το Circle και το Coinbase, θα συνδεθούν με τον τραπεζικό λογαριασμό σας, την πιστωτική σας κάρτα ή και με τα δύο. Όταν επιβεβαιωθεί η ταυτότητά σας, μπορείτε να αγοράσετε bitcoins. Συνήθως μεταφέρονται σχεδόν αυτόματα στον λογαριασμό σας, αν και η μεταφορά μπορεί να καθυστερήσει κάποιες μέρες εάν κάποιο από τα δύο ανταλλακτήρια εντοπίσει κάτι ύποπτο στην αγορά ή εάν πρόκειται για μεγάλο ποσό.

Και τα δύο ανταλλακτήρια —όπως και τα περισσότερα που επιτρέπουν τις συναλλαγές μεταξύ παραστατικού χρήματος και bitcoins— θα σας εφοδιάσουν με κάτι που ονομάζεται «web wallet» (διαδικτυακό πορτοφόλι). Στις περιπτώσεις αυτών των συναλλαγών, λειτουργούν ως τράπεζες του Bitcoin. Θα φυλάσσουν τα ιδιωτικά κλειδιά σας —τους μοναδικούς και τυχαιοποιημένους αριθμούς που επιτρέπουν στον χρήστη να στέλνει bitcoins από ένα συγκεκριμένο πορτοφόλι— και, παρότι μπορείτε ελεύθερα να στέλνετε bitcoins όπου επιθυμείτε, κάθε ανταλλακτήριο έχει τη δυνατότητα, θεωρητικά, να κλειδώσει τον λογαριασμό σας. Εάν το ανταλλακτήριο αντιμετωπίσει πρόβλημα ρευστότητας, τα bitcoins σας πιθανότατα θα χαθούν.

Παρά την αρνητική δημοσιότητα, πολλοί χρήστες συνεχίζουν να φυλάσσουν τα bitcoins τους σε αυτά τα ανταλλακτήρια. Το Coinbase και το Circle, όπως όλα δείχνουν, δεν πρόκειται να κλείσουν σύντομα. Και τα δύο έχουν τροφοδοτηθεί με εκατομμύρια σε χρηματοδοτικά κεφάλαια, και τα δύο στοχεύουν να γίνουν οι ηγέτες στον χώρο του Bitcoin κατά τις επόμενες δεκαετίες.

Σε κάθε περίπτωση, τα πλεονεκτήματα των διαδικτυακών πορτοφολιών είναι η ευκολία που παρέχουν. Είναι εύκολα προσβάσιμα από ηλεκτρονικό υπολογιστή ή κινητό τηλέφωνο και αμφότερα έχουν πολύ φιλικό UI (διεπαφή χρήστη). Το μειονέκτημα είναι κάποιες «θυσίες» ως προς τα προσωπικά στοιχεία και την ασφάλεια. Και οι δύο υπηρεσίες διαθέτουν πιστοποίηση δύο παραγόντων, η οποία συστήνεται ως απαραίτητη. «Η πιστοποίηση δύο παραγόντων» είναι ένας όρος που χρησιμοποιείται για να περιγράψει οποιοδήποτε σύστημα ασφαλείας απαιτεί δύο τύπους πληροφοριών: έναν κωδικό πρόσβασης και κάτι άλλο. Αυτό το «κάτι άλλο» συνήθως μεταφέρεται μέσω μηνύματος sms ή μέσω των δημοφιλών εφαρμογών για κινητά τηλέφωνα Authy και Google Authenticator.

Τώρα που έχουμε bitcoins, τι τα κάνουμε; Αν σκοπεύετε να αγοράσετε έναν σημαντικό αριθμό bitcoins, πιθανόν να θέλετε να τα μεταφέρετε σε ένα πιο ασφαλές μέρος από το Coinbase και το Circle. Υπάρχουν διαδικτυακά πορτοφόλια πολλαπλών υπογραφών που παρέχουν κατά τι περισσότερη ασφάλεια, ενώ παραμένουν βολικά για τους χρήστες. Το Coinkite και το BitGo, στα οποία έχω πείρα, θα σας δώσουν πολλές επιλογές στο πώς να προσδιορίσετε το κλειδί σας. Μπορεί να δημιουργηθεί τυχαία από τον πλοηγό σας, μπορεί να δημιουργηθεί από κάποιον τρίτο, μπορεί να διαθέτετε μια εφαρμογή —προς το παρόν, μόνο iOS— για την παραγωγή του, ή μπορείτε να το δημιουργήσετε μόνοι σας. Η δημιουργία του μέσω τρίτου σημαίνει ότι αν χάσετε το κλειδί, μπορείτε να το

επαναφέρετε. Όμως, αυτό σημαίνει ότι θα πρέπει να έχετε εμπιστοσύνη στον τρίτο ότι θα προστατεύσει σωστά το κλειδί.

Οι ανωτέρω επιλογές είναι σχετικά απλές, εκτός από την εκτός σύνδεσης παραγωγή, δηλαδή την παραγωγή ενός κρυπτογραφημένου κλειδιού όταν δεν είστε συνδεδεμένοι στο Διαδίκτυο. Σε αυτή την περίπτωση, θα πρέπει να βρείτε κάποιο λογισμικό γεννήτριας κλειδιών BIP32. Σας προτείνω το bit32.org. Παράγετε το κλειδί σας ακολουθώντας τις οδηγίες, παίρνετε το κλειδί BIT32 και το αντιγράφετε στο BitGo. Για περισσότερη ασφάλεια, αυτό το τελευταίο βήμα καλό θα είναι να γίνεται σε έναν υπολογιστή διαφορετικό από αυτόν που χρησιμοποιείτε συνήθως.

Τώρα που έχετε εξοπλιστεί με ένα διαδικτυακό πορτοφόλι πολλαπλών υπογραφών και έχετε κάποιον έλεγχο στα ιδιωτικά κλειδιά, το επόμενο βήμα είναι να στείλετε εκείνα τα bitcoins στο πορτοφόλι από το πορτοφόλι που έχετε στο Circle ή το Coinbase. Απλώς πάρτε το «δημόσιο κλειδί» —το κλειδί που μπορείτε να δίνετε δημοσίως και επιτρέπει στους άλλους να σας στέλνουν bitcoins— που αρχίζει με 3 και μοιάζει λίγο με 3Bi1fng5LfoDzue5M TfGw9PgHNKKgRkVt. (Το δημόσιο κλειδί σας στο Circle ή το Coinbase, το οποίο εξ ορισμού δεν διαθέτει πολλές υπογραφές, θα είναι παρόμοιο, αλλά θα ξεκινάει με το ψηφίο 1). Πατήστε το πλήκτρο «send» ή «send bitcoins» στο πορτοφόλι σας στο Circle ή το Coinbase και κατόπιν αντιγράψτε τη διεύθυνση του BitGo, του Coinkite ή του χάρτινου πορτοφολιού στον χώρο «Το» και πατήστε το «Send».

Από εκείνο το σημείο, μπορείτε να στέλνετε και να παραλαμβάνετε bitcoins σε οποιαδήποτε διεύθυνση στο Bitcoin ενώ παράλληλα θα διατηρείτε τα bitcoins σας σχετικά ασφαλή. Αυτό είναι αποδεκτό για μεσαίου μεγέθους ποσότητες χρημάτων —όποιο ποσό και αν είναι αυτό για εσάς— που επιθυμείτε να ξοδέψετε, αλλά δεν θέλετε να το μετατρέψετε άμεσα σε παραστατικό χρήμα.

Πρόσφατα, το Coinbase ξεκίνησε τη δική του υπηρεσία πορτοφολιών με πολλαπλές υπογραφές, η οποία ονομάζεται Vault. Είναι μία φιλική προς τον χρήστη επιλογή, που σας επιτρέπει να δίνετε κλειδιά στον εαυτό σας ή σε άλλους. Το BitGo χρειάζεται ακόμα μερικά χρόνια εμπειρίας —και φήμης— στον χώρο, αλλά είναι μια βιώσιμη επιλογή.

Αν και όποτε επιθυμήσετε να εξαργυρώσετε αυτά τα bitcoins σε παραστατικό χρήμα, οι επιλογές σας θα είναι ή να τα πουλήσετε σε κάποιον άμεσα για μετρητά (δεν σας προτείνω να δεχτείτε το PayPal ή οποιασδήποτε άλλη αναστρέψιμη συναλλαγή, εκτός αν σκοπεύετε να πουλήσετε bitcoins ως επιχείρηση) ή να τα ξαναβάλετε στο Circle ή στο Coinbase και να τα πουλήσετε εκεί, όπου τα μετρητά θα μπουν άμεσα στον τραπεζικό λογαριασμό σας, ύστερα από μερικές εργάσιμες ημέρες. Θα καλύψω την πρακτική διαδικασία αγοράς και πώλησης bitcoins για μετρητά —και άλλες μεθόδους πώλησης— με περισσότερες λεπτομέρειες στο 10ο κεφάλαιο.

Για μακροπρόθεσμη αποταμίευση, καλή ιδέα είναι η εκτύπωση ενός «χάρτινου πορτοφολιού». Για να το κάνετε αυτό, το λογισμικό με τον καλύτερο συνδυασμό ασφάλειας και χρηστικότητας είναι, κατά τη γνώμη μου, το bitaddress.org. Δημιουργεί διευθύνσεις στο Bitcoin βάσει τυχαίων πράξεων που εκτελείτε στον πλοηγό σας —κίνηση του ποντικιού, πληκτρολόγηση κλειδιών, οτιδήποτε— και σας επιτρέπει να δημιουργήσετε μία διεύθυνση από αυτό. Για ένα πιο ασφαλές πορτοφόλι, σας συστήνω να κάνετε λήψη του προγράμματος (στον ιστότοπο παρέχεται σύνδεσμος που σας επιτρέπει να το κάνετε).

Μετά από αυτό, εκτυπώστε το πορτοφόλι και χρησιμοποιήστε το διαδικτυακό πορτοφόλι που δημιουργήσατε νωρίτερα για να στείλετε bitcoins στη δημόσια διεύθυνση που δημιουργήθηκε για

το χάρτινο πορτοφόλι σας χρησιμοποιώντας τον κωδικό QR (ή εισάγοντας οι ίδιοι τη δημόσια διεύθυνση).

Υπάρχει, φυσικά, και η επιλογή να κάνετε τα πάντα εσείς. Άλλωστε, αυτή είναι η έννοια του Bitcoin: χρήματα χωρίς τρίτους. Κάνοντας λήψη του δικού σας αντιγράφου από το Bitcoin Core —για το οποίο θα μιλήσουμε παρακάτω— και την αλυσίδα των μπλοκ, μπορείτε να αποκτήσετε ένα διαδικτυακό πορτοφόλι το οποίο είναι τόσο ασφαλές όσο ο υπολογιστής που το εισάγετε και βοηθάει στο να γίνεται ασφαλές το δίκτυο του Bitcoin όσο βρίσκεστε σε αυτό. Αυτό ονομάζεται «τοπικό πορτοφόλι». Ένα τοπικό πορτοφόλι που είναι αποσυνδεδεμένο από το Διαδίκτυο ονομάζεται «εκτός σύνδεσης» (offline) και συχνά αναφέρεται ως «cold storage».

Δεν πρόκειται ακριβώς για μια διαδικασία φιλική προς τον χρήστη και δεν είναι κάτι που προτείνω να κάνει κάποιος για το πρώτο του πορτοφόλι στο Bitcoin. Τούτου λεχθέντος, υπάρχει κάτι που κάθε χρήστης του Bitcoin θα πρέπει να κάνει τουλάχιστον μία φορά εάν σκοπεύει να κρατήσει τα bitcoins μακροπρόθεσμα. Όποιος σκοπεύει να αποθηκεύσει μεγάλες ποσότητες χρημάτων με στόχο να έχει αποταμιεύσει χρήματα όταν βγει στη σύνταξη, θα πρέπει οπωσδήποτε να δημιουργήσει ένα τοπικό πορτοφόλι και ένα εκτός σύνδεσης πορτοφόλι — αν δεν τοποθετήσει τις μακροπρόθεσμες οικονομίες του σε ένα χάρτινο πορτοφόλι.

Το Bitcoin Core και το Armory, που προσφέρουν υπηρεσίες πολλαπλών υπογραφών για εκτός σύνδεσης και τοπικά πορτοφόλια, αποτελούν τα δύο δημοφιλέστερα τοπικά πορτοφόλια. Κάνετε λήψη από τους αντίστοιχους ιστότοπους —bitcoin.org και bitcoinarmory.org— και εγκαταστήστε το πρόγραμμα. Κατά την εφαρμογή, θα ξεκινήσει η μακρά (πάνω από 50MB) λήψη της αλυσίδας των μπλοκ του Bitcoin. Όταν ολοκληρωθεί, θα είστε νόμιμο μέλος του δικτύου του Bitcoin ως κάτι που ονομάζεται πλήρης κόμβος.

Θα διατηρείτε μια συνεχώς ενημερούμενη έκδοση της αλυσίδας των μπλοκ και θα συμμετέχετε σε συναλλαγές επιβεβαιωμένες από τους εξορύκτες (περισσότερα για την εξόρυξη σε μετέπειτα κεφάλαιο). Δεν είναι απαραίτητο να είστε ένας πλήρης κόμβος — όμως, κάθε κόμβος βοηθά ώστε το δίκτυο του Bitcoin να κινείται πιο ομαλά και με περισσότερη ασφάλεια. Το λογισμικό θα πρέπει να τα αναλάβει όλα μόνο του αλλά, αν αντιμετωπίσετε προβλήματα, βεβαιωθείτε ότι ο δίαυλος 8333 είναι ανοικτός. Θα πρέπει να ανατρέξετε στις ρυθμίσεις του router σας για να δείτε πώς γίνεται αυτό.

Από εκείνο το σημείο και μετά, η διαδικασία είναι σχετικά απλή και δεν μοιάζει καθόλου με τη χρήση ενός διαδικτυακού πορτοφολιού. Αν θελήσετε να μετατρέψετε το πορτοφόλι σας σε πορτοφόλι εκτός σύνδεσης, βρείτε το αρχείο «wallet.dat» στον φάκελο του προγράμματος και μεταφέρετέ το σε ένα στικάκι USB ή σε κάποια παρόμοια συσκευή αποθήκευσης.

Μία τελευταία επιλογή που αξίζει να αναφερθεί είναι το «hardware wallet» (πορτοφόλι υλισμικού). Πρόκειται για πορτοφόλια που έχουν δημιουργηθεί από διάφορες εταιρείες και επιτρέπουν στους χρήστες να διατηρούν και να ξοδεύουν bitcoins με ελάχιστη σύνδεση στο δίκτυο του Bitcoin. Δυστυχώς, δεν έχω χρησιμοποιήσει κάποιο από αυτά, επομένως δεν μπορώ να μιλήσω άμεσα για την αποτελεσματικότητά τους. Τα KeepKey, TREXOR και Ledger είναι οι πρωτοπόροι αυτής της βιομηχανίας.

Τώρα γνωρίζετε πώς να αποκτήσετε, πώς να αποθηκεύσετε και πώς να αναλώνετε bitcoins. Γιατί, όμως, να θέλετε να το κάνετε αυτό; Η εξήγηση απαιτεί περισσότερο χρόνο. Θα ξεκινήσω με μια σύντομη ιστορία του Bitcoin.