

ΤΟ BITCOIN ΣΕ

1



ΛΕΠΤΑ

Όλα όσα θα θέλατε να ξέρετε για το Bitcoin

Brought to you by **Relai**

ΤΙ ΕΙΝΑΙ ΤΟ BITCOIN?

Το Bitcoin, το πιο επιτυχημένο κρυπτονόμισμα στον κόσμο, απασχολεί τα πρωτοσέλιδα παγκοσμίως. Πολλοί θέλουν να επωφεληθούν από την επιτυχία του, άλλοι είναι αδιάφοροι ή και δύσπιστοι. Το ψηφιακό νόμισμα έχει πυροδοτήσει αμέτρητες συζητήσεις σχετικά με τα χρήματα, τις επενδύσεις και την τεχνολογία. Κάποιοι βλέπουν το Bitcoin ως ένα καθαρό όχημα κερδοσκοπίας ή το καταγγέλλουν ως φούσκα, ενώ άλλοι μιλούν για καινοτομία, νομισματική επανάσταση ή ακόμα και απαγκίστρωση από το τρέχον νομισματικό σύστημα.

Διάφορες χώρες, συμπεριλαμβανομένης της Κίνας, βλέπουν το Bitcoin ως απειλή και έχουν κηρύξει πόλεμο στο

κρυπτονόμισμα. Άλλες κυβερνήσεις, όπως αυτή του Ελ Σαλβαδόρ, έχουν εισαγάγει το Bitcoin ως επίσημο μέσο πληρωμής με την ελπίδα της οικονομικής ανάπτυξης.

Τι είναι όμως το Bitcoin; Είναι χρήμα; Ψηφιακός χρυσός; Μια πρόσκαιρη μόδα για επιστήμονες υπολογιστών και κερδοσκόπους; Ή κάτι εντελώς διαφορετικό; Στις επόμενες παραγράφους, θα απαντήσουμε σε βαθos αυτές τις ερωτήσεις και θα ρίξουμε μια πιο προσεκτική ματιά στο ψηφιακό νόμισμα για να κατανοήσουμε καλύτερα τη φιλοσοφία και τη λειτουργικότητα πίσω από το Bitcoin. Για να το πετύχουμε αυτό, είναι σημαντικό να ξεκινήσουμε από την αρχή: με την ιστορία της προέλευσης του Bitcoin.

Η ΙΣΤΟΡΙΑ ΤΟΥ BITCOIN

Η αρχή του Bitcoin χρονολογείται από τις αρχές της δεκαετίας του '90. Το 1992, μια ομάδα επιστημόνων υπολογιστών στην Καλιφόρνια ξεκίνησε μια λίστα email για να ανταλλάξει ιδέες με ομοϊδεάτες τους σχετικά με την κρυπτογραφία, τα μαθηματικά, την πολιτική και τη φιλοσοφία. Αυτοαποκαλούνταν «Cypherpunks» - ένα λογοπαίγνιο από το cyberpunk (άτομο στη λογοτεχνία επιστημονικής φαντασίας που αντιμετωπίζει με σκεπτικισμό την κοινωνία για την κοινωνία - και δικαίως) και cipher (για την κρυπτογραφία).

Οι Cypherpunks

Οι Cypherpunks σύντομα μεγάλωσαν σε μία ποικιλόμορφη ομάδα. Παρά το διαφορετικό υπόβαθρό τους, τους

ένωνε η πεποίθηση ότι το Διαδίκτυο θα γινόταν σύντομα ένας από τους πιο αμφισβητούμενους χώρους για την ανθρώπινη ελευθερία.

Για να προστατευτούν από την απειλή ελέγχου, παρακολούθησης και λογοκρισίας του Διαδικτύου και να διατηρήσουν ένα ελεύθερο και ανοικτό Διαδίκτυο, οι Cypherpunks χρησιμοποίησαν ένα ισχυρό όπλο: την Κρυπτογραφία, την κρυπτογράφηση των πληροφοριών.

Στο [μανιφέστο](#) τους το 1993, δήλωσαν: «Οι Cypherpunks γράφουν κώδικα στον υπολογιστή. Γνωρίζουμε ότι κάποιος πρέπει να γράψει λογισμικό για να υπερασπιστεί το απόρρητο, και [...] θα το γράψουμε.

Αλλά η κρυπτογραφία από μόνη της δεν θα ήταν αρκετή για ένα ελεύθερο

Διαδίκτυο. Επειδή, και οι Cypherunks ήταν πεπεισμένοι για αυτό, το Διαδίκτυο δεν μπορεί να είναι πραγματικά ελεύθερο εάν δεν έχει τη δική του μορφή χρήματος. Χρήμα που είναι ανεξάρτητο από κράτη, κεντρικές τράπεζες και εταιρείες. ένα κρυπτονόμισμα τόσο δίκαιο και αποκεντρωμένο όσο το ίδιο το Διαδίκτυο.

Νομισματικά Πειράματα

Αλλά η δημιουργία ανεξάρτητου, ψηφιακού χρήματος παρουσίασε τεχνικές προκλήσεις στους Cypherunks. Ήδη από το 1990, ο κρυπτολόγος David Chaum είχε δημιουργήσει το eCash, το πρώτο κρυπτονόμισμα, το οποίο δεν ήταν αποκεντρωμένο αλλά εξασφάλιζε την ανωνυμία χάρη στην κρυπτογραφία. Ωστόσο, το eCash δεν μπόρεσε να επιβληθεί έναντι άλλων διαδικτυακών συστημάτων πληρωμών μακροπρόθεσμα. Η εταιρεία πίσω από το έργο έπρεπε να κηρύξει πτώχευση μετά από 8 χρόνια λειτουργίας και το eCash εξαφανίστηκε.

Ακολούθησαν και άλλες προσπάθειες, από τις οποίες ξεχώρισε το E-Gold. Το E-Gold ήταν ένα κρυπτονόμισμα υποστηριζόμενο από το χρυσό και ανοιχτό σε όλους. Η εταιρεία ιδρύθηκε κατά την εποχή του dot-com το 1996, και εντυπωσίασε, επεξεργάζοντας συναλλαγές αξίας άνω των δύο δισεκατομμυρίων δολαρίων ετησίως

στο απόγειό της.

Αλλά το E-gold ελεγχόταν από ένα κεντρικό ίδρυμα και επομένως ήταν ευάλωτο σε επιθέσεις. Σύντομα ακολούθησαν νομικά προβλήματα και η κυβέρνηση των ΗΠΑ έλαβε νομικά μέτρα κατά της E-Gold. Το 2008, η E-Gold κρίθηκε ένοχη από δικαστήριο των ΗΠΑ για ξέπλυμα βρώμικου χρήματος και παραβιάσεις του Patriot Act. Όλα τα περιουσιακά στοιχεία δεσμεύτηκαν και η E-Gold έπρεπε να σταματήσει τη λειτουργία της.

Αυτές οι αποτυχημένες προσπάθειες απέδειξαν δύο γεγονότα στους Cypherunks. Πρώτον, τόσο το eCash όσο και το E-gold είχαν υποστηριχθεί από εξασφαλίσεις. Αυτή η εξασφάλιση είχε αποδειχθεί αδύναμο σημείο, καθώς θα μπορούσε να κατασχεθεί από τα κράτη. Επομένως, ένα δωρεάν κρυπτονόμισμα δεν θα πρέπει να έχει κεντρικά σημεία επίθεσης, όπως μια εγγεγραμμένη εταιρεία, έναν τραπεζικό λογαριασμό ή μια κεντρική τοποθεσία διακομιστή (server). Και δεύτερον, τόσο οι κυβερνήσεις όσο και οι ρυθμιστικές αρχές δεν ενδιαφέρονται για το ανεξάρτητο από το κράτος ψηφιακό χρήμα.

Για τους Cypherunks το βασικό ερώτημα, για το οποίο δεν είχε βρεθεί ακόμη λύση, παρέμενε: Πώς μπορεί ένα ανεξάρτητο ψηφιακό χρήμα να λειτουργήσει χωρίς μια κεντρική

αρχή να καταγράφει τις λογιστικές συναλλαγές και να διασφαλίζει ότι τα χρήματα δεν δαπανώνται δύο φορές; Σε τελική ανάλυση, αν ήταν δυνατό να λυθεί το πρόβλημα της διπλής δαπάνης χωρίς να βασιζόμαστε σε μια κεντρική αρχή, θα ήταν ίσως δυνατό να δημιουργηθεί ελεύθερο ψηφιακό χρήμα που είναι εγγενές στο Διαδίκτυο.

Μια μυστικιστική Πράξη Δημιουργίας

Για αυτούς τους λόγους, οι Cypherpunks άρχισαν να συζητούν σχέδια για ένα κρυπτονόμισμα χωρίς κεντρική διοίκηση και εξασφαλίσεις. Δύο από τις πιο σημαντικές ιδέες ήταν το b-money (1998) και το BitGold (2005). Αυτές οι θεωρητικές ιδέες, που δεν εφαρμόστηκαν ποτέ στην πράξη, ήταν ήδη πολύ παρόμοιες με το Bitcoin στο σχεδιασμό τους. Για την κρυπτογραφία προβλεπόταν ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού και για τη δημιουργία πρόσθετων ψηφιακών νομισμάτων θα προβλεπόταν μια τεκμηρίωση εργασίας (Proof-of-Work), όπως συμβαίνει και με το Bitcoin. Στο Whitepaper του, ο εφευρέτης του Bitcoin επιβεβαίωσε επίσης ότι γνώριζε το b-money και το BitGold.

Ωστόσο, επειδή το b-money και το BitGold βασίζονταν σε ένα σύστημα ψηφοφορίας για συναίνεση (η συμφωνία για το ποιος κατέχει ποιες νομισματικές μονάδες επί του παρόντος), ήταν ευάλωτα σε κακόβουλες επιθέσεις που θα

μπορούσαν να χειραγωγήσουν τέτοιες ψηφοφορίες και έτσι να στρεβλώσουν την ιδιοκτησία.

Για αυτό το τελευταίο πρόβλημα, το οποίο παρέμενε εμπόδιο στη δημιουργία νέων Διαδικτυακών χρημάτων, παρουσιάστηκε μια λύση την Παρασκευή, 31 Οκτωβρίου 2008. Εκείνη την ημέρα, το [Whitepaper του Bitcoin](#), στο οποίο ο Satoshi Nakamoto εξηγεί την ιδέα του για ένα αποκεντρωμένο δίκτυο πληρωμών, στάλθηκε με email στους Cypherpunks. Δύο μήνες αργότερα, στις 3 Ιανουαρίου 2009, το δίκτυο του Bitcoin άρχισε να λειτουργεί.

Οι αρχικές αντιδράσεις για το νέο δίκτυο ήταν συγκρατημένες. Κάποιοι ενθουσιώδεις άρχισαν να δοκιμάζουν το δίκτυο και να αναφέρουν σφάλματα που έβρισκαν. Στην αρχή, ωστόσο, ήταν κυρίως ο ίδιος ο Satoshi Nakamoto που κράτησε το δίκτυο σε λειτουργία. Αλλά σιγά σιγά τα νέα για το νέο Διαδικτυακό χρήμα εξαπλώθηκαν σε φόρουμ υπολογιστών και τεχνολογίας και το ενδιαφέρον για το δίκτυο του Bitcoin αυξήθηκε. Μετά από ένα χρόνο, το δίκτυο Bitcoin μετρούσε ήδη ορισμένους χρήστες. Το ίδιο το Bitcoin, ωστόσο, δεν είχε αξία ακόμη.

Ποιός είναι ο Satoshi Nakamoto;

Το Whitepaper του Bitcoin, καθώς και η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου του εφευρέτη του Bitcoin, υπογράφηκαν με το όνομα Satoshi Nakamoto.



Ωστόσο, η πραγματική ταυτότητα του εφευρέτη Bitcoin παραμένει άγνωστη μέχρι σήμερα, καθώς το όνομά του φαίνεται να είναι ψευδώνυμο. Για να απευθυνθεί σε ομοϊδεάτες και αργότερα στην κοινότητα προγραμματιστών του Bitcoin, ο Nakamoto χρησιμοποίησε τουλάχιστον τρεις διαφορετικές διευθύνσεις e-mail, τις οποίες κρυπτογραφούσε επιμελώς για να κρύψει την πραγματική ταυτότητα του αποστολέα.

Διάφοροι άνθρωποι έχουν ήδη ισχυριστεί ότι είναι ο Satoshi Nakamoto. Αλλά μέχρι σήμερα, ο καθένας τους δεν το έχει αποδείξει. Γιατί η απόλυτη απόδειξη, δηλαδή η αποστολή Bitcoin από μια από τις διευθύνσεις πορτοφολιού που πιθανότατα ανήκουν στον Satoshi, δεν έχει πραγματοποιηθεί ακόμη από κανέναν.

Εξάλλου, η ομάδα όσων έχουν επικοινωνήσει «προσωπικά» με τον Satoshi Nakamoto μέσω Διαδικτύου είναι πολύ μικρή. Ο Satoshi Nakamoto έγραψε το τελευταίο του μήνυμα στην κοινότητα του Bitcoin στις 12 Δεκεμβρίου 2010, αλλά αυτό δεν ήταν σε καμία περίπτωση ένα

αποχαιρετιστήριο μήνυμα - ο Satoshi απλά σταμάτησε να επικοινωνεί μετά από αυτό.

Η απόσυρσή του, ωστόσο, ήταν μόνο για την ευρύτερη κοινότητα. Ο Nakamoto συνέχισε να συγκεντρώνει μια μικρή ομάδα βασικών προγραμματιστών γύρω του και τους ενημέρωσε για την περαιτέρω ανάπτυξη του δικτύου Bitcoin. Όμως τον Απρίλιο του 2011 έστειλε ένα τελευταίο μήνυμα και σε αυτή την ομάδα. Εξίσου μυστηριωδώς όπως εμφανίστηκε ο Nakamoto το 2008, εξαφανίστηκε ξανά τρία χρόνια αργότερα.

Η “Pizza Day” του Bitcoin

Πώς όμως απέκτησε αξία το Bitcoin εξ αρχής; Στην αρχή, το Bitcoin μπορούσε να εξορύσσεται και να στέλνεται μεταξύ των μελών του δικτύου, αλλά οι ψηφιακές μονάδες του δεν είχαν καμία αξία. Επίσης, η ομάδα όσων γνώριζαν το Bitcoin, πόσο μάλλον που μπορούσαν να το στείλουν και να το παραλάβουν, ήταν ακόμα πολύ μικρή.

Αυτό άλλαξε στις 22 Μαΐου 2010, όταν εμφανίστηκε ένα ασυνήθιστο αίτημα στο διαδικτυακό φόρουμ bitcointalk.org. Ένας 28χρονος ονόματι

Laszlo Hanyecz από τη Φλόριντα πρόσφερε 10.000 Bitcoin στο άτομο που θα παρέδιδε δύο πίτσες στο σπίτι του. Ένας φοιτητής από την Καλιφόρνια δέχθηκε την προσφορά και του παρέδωσε δύο μεγάλες πίτσες αξίας \$41 στο σπίτι του. Σε αντάλλαγμα, ο Hanyecz του έστειλε τα 10.000 Bitcoin.

Από εκείνη την ημέρα, η 22η Μαΐου γιορτάζεται κάθε χρόνο από τους Bitcoiners ως Bitcoin «Pizza Day». Η ημέρα έγινε δημοφιλής επειδή σηματοδοτεί τρία πράγματα:

- Το Bitcoin έχει αξία
- Το Bitcoin είναι κατάλληλο ως μέσο συναλλαγών και πληρωμών
- Το Bitcoin ως νόμισμα είναι αποπληθωριστικό. Ο αριθμός των επιπλέον Bitcoin που τίθενται σε κυκλοφορία μειώνεται σταθερά, γεγονός που μπορεί να οδηγήσει σε αύξηση της αξίας.

Οι δύο πίτσες έχουν μείνει στην ιστορία ως οι πιο ακριβές πίτσες στον

κόσμο. Υπολογίζοντας το κόστος τους με την τιμή του Bitcoin από τον Δεκέμβριο του 2021, πληρώθηκε γι' αυτές το απίστευτο ποσό των 460 εκατομμυρίων δολαρίων ΗΠΑ. Αυτά είναι πολλά χρήματα. Αλλά ο παραλήπτης των 10.000 Bitcoin τα έχει ήδη ξοδέψει επίσης. Σε συνέντευξή του, δήλωσε ότι είχε πουλήσει το Bitcoin λίγο αργότερα για να πληρώσει για ένα οδικό ταξίδι - στη σημερινή τιμή του Bitcoin ίσως το πιο ακριβό οδικό ταξίδι στην ανθρώπινη ιστορία.

Η Bitcoin «Pizza Day» δείχνει επίσης εντυπωσιακά γιατί το «hodling» - που προέρχεται από το «to hold» - (κρατώ) είναι τόσο δημοφιλές μεταξύ των Bitcoiners. «Hodling» σημαίνει να διατηρεί κανείς τα Bitcoin του για μεγάλα χρονικά διαστήματα με σκοπό (ενδεχομένως) να μην τα πουλήσει ποτέ. Σε τελική ανάλυση, ποιος θέλει να ξοδέψει το Bitcoin του σήμερα όταν θα μπορούσε να αξίζει διπλάσια, τριπλάσια ή και δεκαπλάσια τα επόμενα χρόνια;

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ ΤΟ BITCOIN?

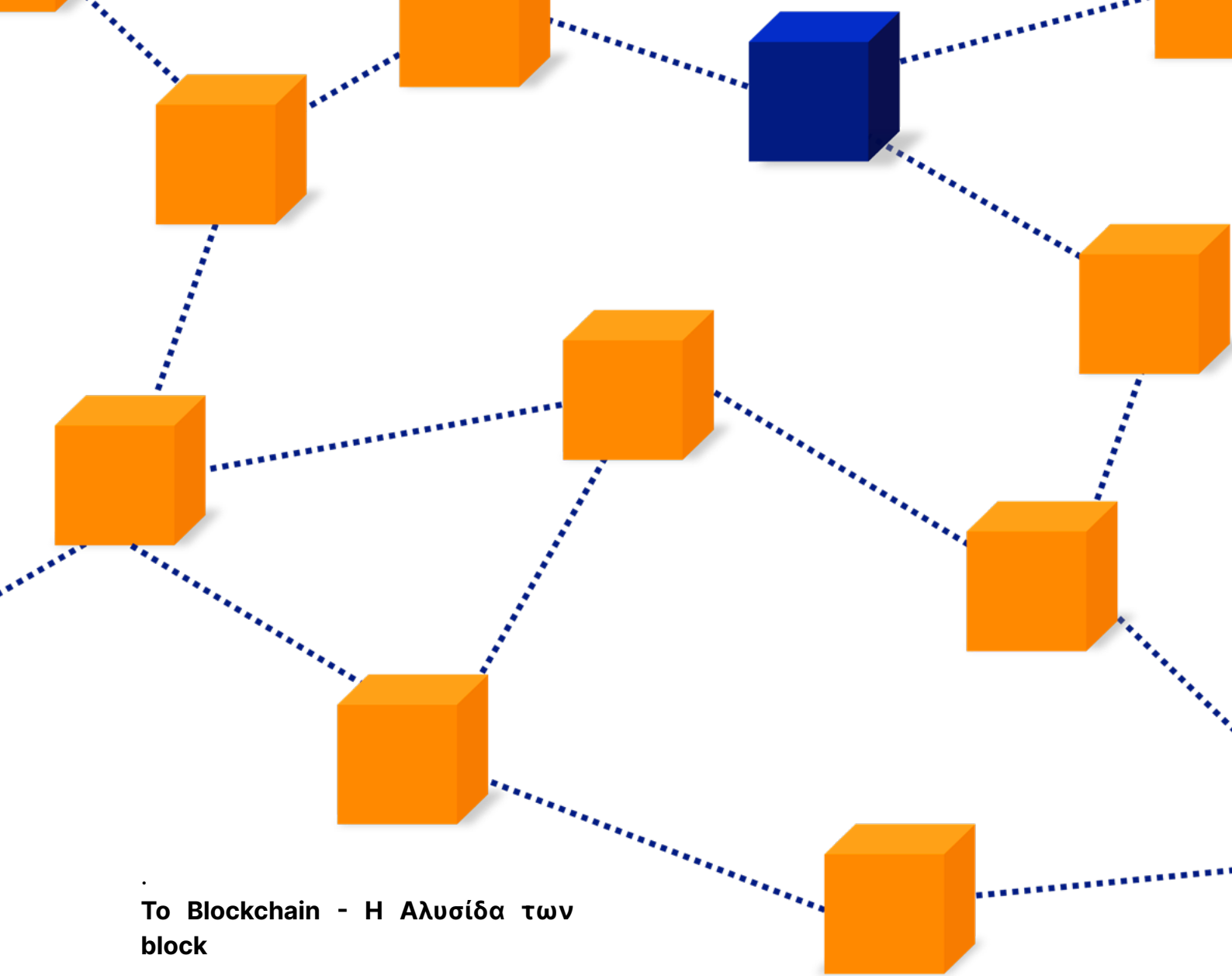
Αφού μάθουμε για την ιστορία του Bitcoin, θα εξετάσουμε τώρα τον τρόπο λειτουργίας του. Ο στόχος είναι να κατανοήσουμε πώς λειτουργεί το δίκτυο του Bitcoin, ποια προβλήματα επιλύει και ποια είναι τα πρακτικά οφέλη του.

Η πρόθεση πίσω από το Bitcoin είναι να είναι ένα αποκεντρωμένο δίκτυο. Κανένας από τους συμμετέχοντες στο δίκτυο δεν θα πρέπει να είναι σε θέση να κυβερνά μόνος του το δίκτυο - η εξουσία λήψης αποφάσεων και η εποπτεία κατανέμονται μεταξύ όλων των συμμετεχόντων. Αυτό είναι σημαντικό γιατί κανένα άτομο, καμία κυβέρνηση και καμία εταιρεία δεν μπορεί να αλλάξει το δίκτυο ανεξάρτητα, αλλά οι αλλαγές είναι δυνατές μόνο συλλογικά.

Το Bitcoin λειτουργεί με τέτοιο τρόπο ώστε κάθε συμμετέχων στο δίκτυο να έχει ένα πανομοιότυπο αντίγραφο της πιο ενημερωμένης συνολικής καταγραφής (ledger, καθολικό)

ιδιοκτησίας ανά πάσα στιγμή - ως αποτέλεσμα, όλοι γνωρίζουν πάντα ποιος κατέχει ποια Bitcoin. Έτσι, κανείς δεν μπορεί να ισχυριστεί ότι κατέχει περισσότερο Bitcoin από ό,τι έχει, επειδή κάθε συμμετέχων στο δίκτυο μπορεί να ελέγξει αυτήν την αξίωση έναντι του αντιγράφου της συνολικής καταγραφής (ledger, καθολικό) του και να αποδείξει ότι είναι ψευδής.

Πριν από την κυκλοφορία του Bitcoin, τα αποκεντρωμένα δίκτυα αντιμετώπιζαν δύο μεγάλες προκλήσεις. Πρώτον, πώς μπορεί να διασφαλιστεί ότι όλοι οι συμμετέχοντες λαμβάνουν τις πιο πρόσφατες ενημερώσεις σχετικά με τις αλλαγές στην ιδιοκτησία - δηλαδή τις πληροφορίες σχετικά με το ποια Bitcoin έχουν μεταφερθεί και σε ποιον. Και δεύτερον, πώς μπορούν οι συμμετέχοντες να επαληθεύσουν με απόλυτη βεβαιότητα ότι οι πληροφορίες που λαμβάνουν είναι σωστές.

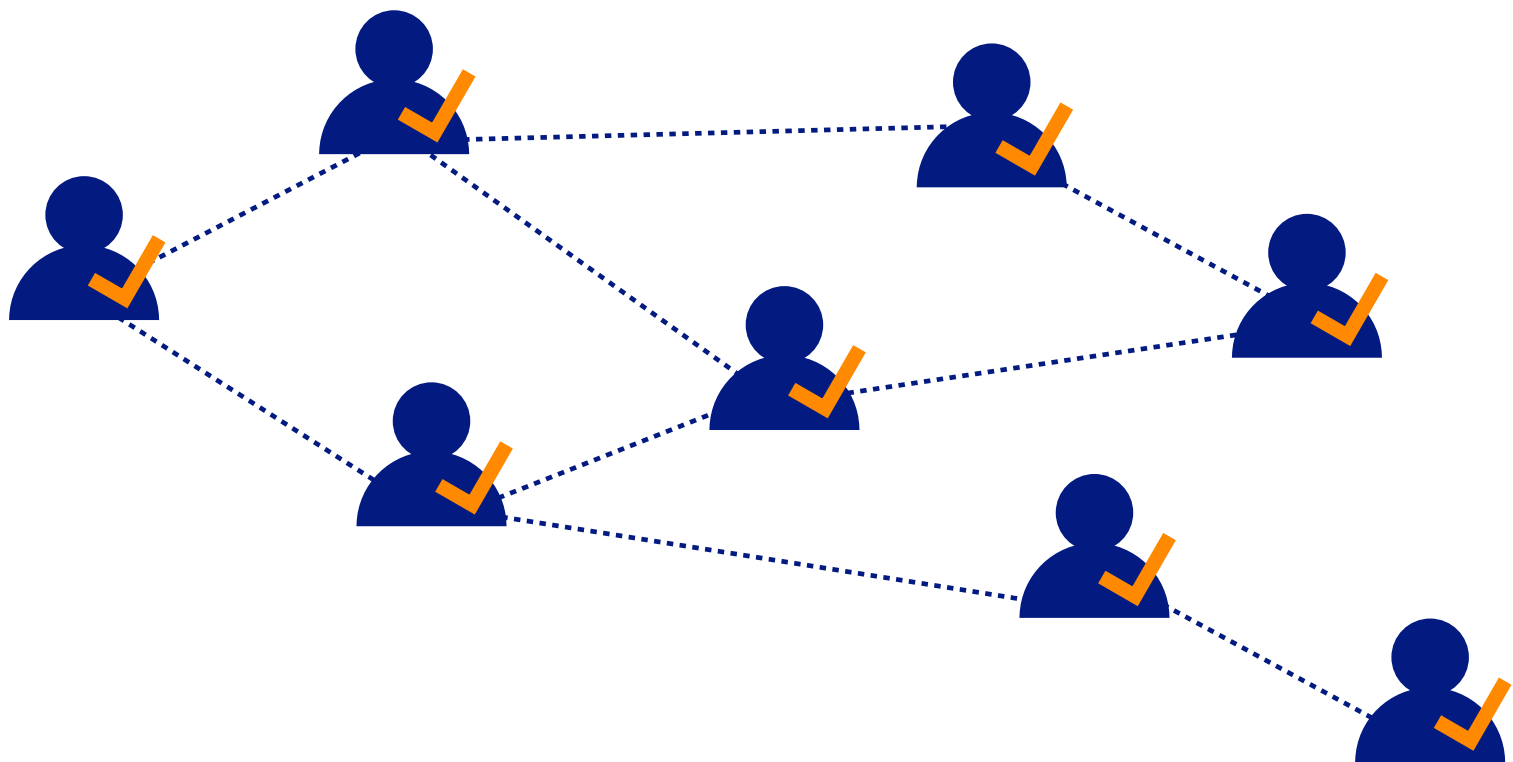


To Blockchain - Η Αλυσίδα των block

Αυτές οι δυσκολίες έχουν ξεπεραστεί χάρη στην εφεύρεση του blockchain. Ένα blockchain αποθηκεύει πληροφορίες και δεδομένα με χρονολογική σειρά. Στην περίπτωση του Bitcoin, όλες οι συναλλαγές από τη δημιουργία του Bitcoin αποθηκεύονται με χρονολογική σειρά σε δεκάδες χιλιάδες block, τα οποία μαζί δημιουργούν το blockchain του Bitcoin. Οποιοσδήποτε συμμετέχων στο δίκτυο που θέλει να μάθει σε ποιον ανήκει ποιο Bitcoin μπορεί να εντοπίσει το ιστορικό συναλλαγών στο blockchain και να γνωρίζει ακριβώς σε ποιον ανήκουν και πόσα Bitcoin αυτή τη στιγμή.

Έτσι, εάν κάποιος θέλει να στείλει ένα Bitcoin, οποιοσδήποτε μπορεί να ελέγξει αν αυτό το Bitcoin ανήκει πραγματικά στο εν λόγω άτομο.

Μέχρι στιγμής, αυτός ο μηχανισμός δεν είναι κάτι καινούργιο αφού οι τράπεζες χρησιμοποιούν παρόμοια διαδικασία. Εάν ένας πελάτης θέλει να δαπανήσει ένα ελβετικό φράγκο, η τράπεζα αναζητά το ιστορικό συναλλαγών για να δει εάν το φράγκο εξακολουθεί να ανήκει στον πελάτη ή αν έχει ήδη

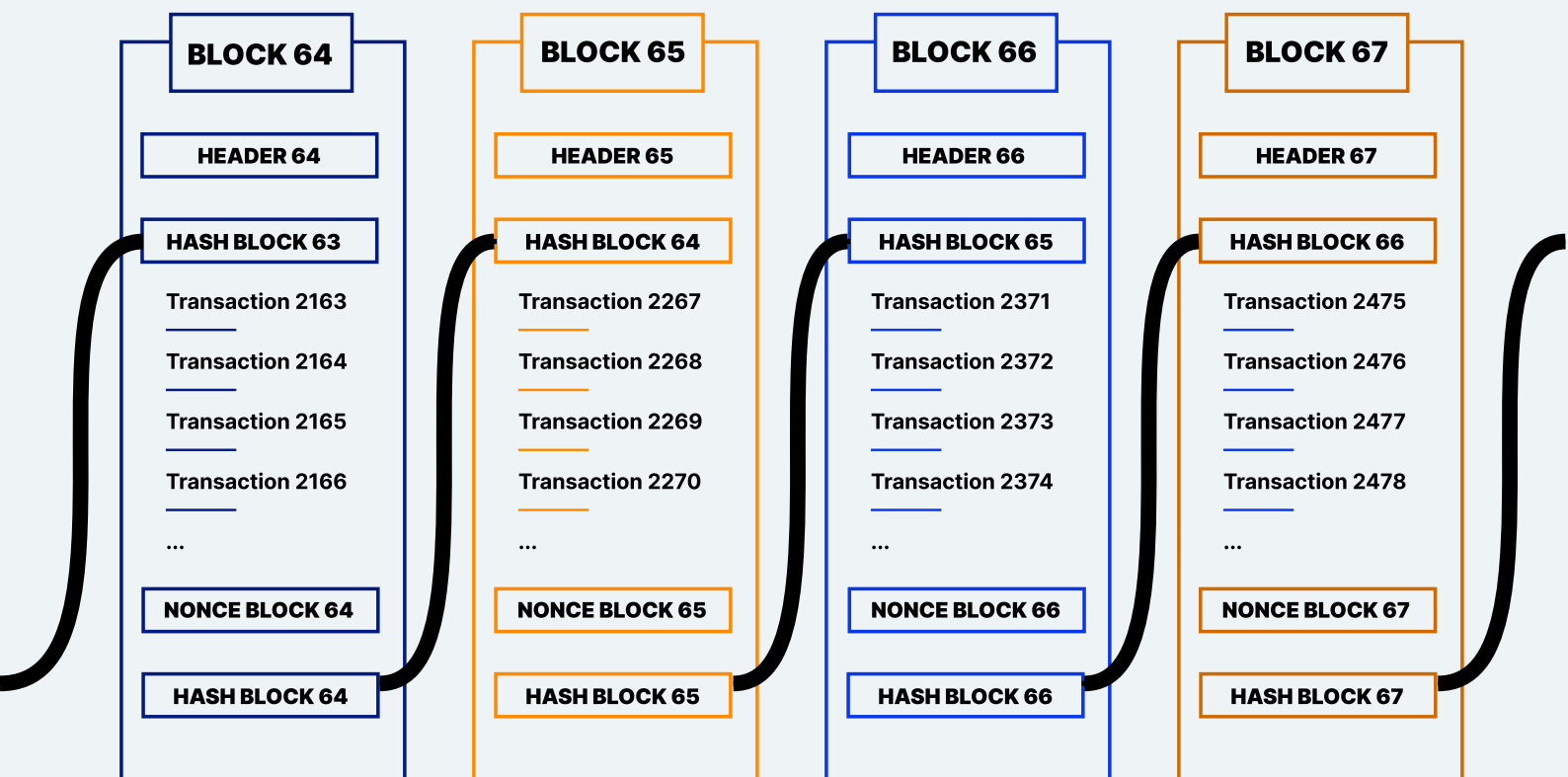


δαπανηθεί (σταλεί σε κάποιον άλλο). Το μοναδικό χαρακτηριστικό ενός blockchain, ωστόσο, είναι ότι αυτές οι πληροφορίες δεν αποθηκεύονται σε διακομιστή (server) κεντρικής τράπεζας, αλλά στους υπολογιστές όλων των συμμετεχόντων στο δίκτυο (τα λεγόμενα full nodes - πλήρεις κόμβοι) και έτσι υπάρχουν σε δεκάδες χιλιάδες αντίγραφα παγκοσμίως. Αυτός είναι επίσης ο λόγος για τον οποίο το Bitcoin δεν μπορεί απλώς να διαγραφεί - για να γίνει αυτό, θα πρέπει να διαγραφεί το αντίγραφο του blockchain από όλους τους συμμετέχοντες υπολογιστές παγκοσμίως ταυτόχρονα.

Ωστόσο, η πρόκληση που αντιμετωπίζουν τα blockchain είναι ότι κάθε συμμετέχων στο δίκτυο πρέπει να είναι σε θέση να προσδιορίσει με απόλυτη βεβαιότητα ότι το αντίγραφο του blockchain είναι σωστό και ότι καμία εσφαλμένη ή δόλια συναλλαγή δεν εισάγεται στο αντίγραφο του καθολικού (ledger).

Δεδομένου ότι νέα block με νέες συναλλαγές προστίθενται στο blockchain κάθε 10 λεπτά, το blockchain αυξάνεται συνεχώς και πρέπει να ενημερώνεται συνεχώς σε όλους τους συμμετέχοντες κόμβους (nodes) παγκοσμίως.

Τα block που προσαρτήθηκαν πρόσφατα πρέπει να είναι επαληθεύσιμα από όλους. Η επαλήθευση γίνεται χρησιμοποιώντας αμετάβλητους κανόνες που ορίζονται στον κώδικα του δικτύου Bitcoin. Αυτοί οι κανόνες ορίζουν ακριβώς ποιες συναλλαγές επιτρέπονται και ποιες όχι. Κάθε χρήστης που κατεβάζει το αντίγραφο του blockchain μπορεί επομένως να επαληθεύσει εάν όλες οι συναλλαγές συμμορφώνονται με τους δεδομένους κανόνες. Εάν μια συναλλαγή παραβιάζει τους κανόνες, δηλαδή εάν είναι εσφαλμένη ή δόλια, απορρίπτεται από τους συμμετέχοντες στο δίκτυο (full nodes) και δεν περιλαμβάνεται στο blockchain.



Η επικεφαλίδα (header), το αποτέλεσμα της συνάρτησης κατακερματισμού (hash function) του προηγούμενου block, όλες οι συναλλαγές του τρέχοντος block και ένας τυχαίος αριθμός (nonce) τοποθετούνται σε μια μαθηματική συνάρτηση. Ο τυχαίος αριθμός αλλάζει μέχρι το αποτέλεσμα της συνάρτησης κατακερματισμού να έχει αρκετά μηδενικά μπροστά. Αυτή η διαδικασία ονομάζεται εξόρυξη (mining).

Proof-of-Work (PoW) Mining -Τεκμηρίωση Εργασίας (PoW) Εξόρυξη

Επιπλέον, το δίκτυο Bitcoin διαθέτει έναν μηχανισμό για τον περιορισμό της προσθήκης νέων block. Εάν μπορούσαν να προστεθούν νέες συναλλαγές και block στο blockchain από οποιονδήποτε, το δίκτυο θα κατέληγε σε χάος, καθώς το blockchain δεν θα μπορούσε να ενημερωθεί σε όλο τον κόσμο στην ίδια κατάσταση αρκετά γρήγορα.

Για να αποφευχθεί αυτό, το Bitcoin λειτουργεί με έναν μηχανισμό τεκμηρίωσης εργασίας. Για να κερδίσει κάποιος το δικαίωμα

να προσθέσει ένα νέο block στο blockchain, πρέπει να παράσχει τεκμηρίωση εργασίας (Proof-Of-Work). Μια απλή απεικόνιση αυτής της διαδικασίας είναι μια ομάδα ανθρώπων που ψάχνουν για βελόνες στα άχυρα. Όποιος βρει πρώτος μια βελόνα, επιτρέπεται να προσθέσει ένα νέο block στο blockchain. Επιπλέον, αυτός του τη βρήκε ανταμείβεται με νέες μονάδες Bitcoin καθώς και με τα τέλη συναλλαγών (transaction fees) που περιέχονται σε αυτό το block. Μόλις συνδεθεί το block στο blockchain, αυτή η διαδικασία ξεκινά ξανά.

Στην πραγματικότητα, οι εξορύκτες (miners) εκτελούν μια μαθηματική συνάρτηση

κατακερματισμού (hash function) (αλγόριθμος κατακερματισμού SHA-256) με σκοπό την αναζήτηση συγκεκριμένων αριθμών. Ο αριθμός κατακερματισμού του προηγούμενου block, οι συναλλαγές του τρέχοντος block και ένας τυχαίος αριθμός (nonce) κατακερματίζονται μαζί. Ο τυχαίος αριθμός αλλάζει έως ότου η συνάρτηση κατακερματισμού εμφανίσει ένα αποτέλεσμα με έναν ελάχιστο αριθμό αρχικών μηδενικών. Για παράδειγμα, το block #700000, που δημιουργήθηκε στις 11 Σεπτεμβρίου 2021, είχε τον έγκυρο αριθμό κατακερματισμού (hash number): 0000000000000000000590fc0f3e-ba193a278534220b2b37e 9849e1a-770ca959.

Η αναζήτηση αυτού του αριθμού, που ονομάζεται επίσης εξόρυξη (mining), έχει δύο κύριες λειτουργίες: Πρώτον, συνδέει τα block μεταξύ τους με μαθηματικό-κρυπτογραφικό τρόπο, ώστε ο καθένας να μπορεί εύκολα να επαληθεύσει τη σωστή σειρά. Ταυτόχρονα, ο μηχανισμός Τεκμηρίωσης Εργασίας (Proof-of-Work) καθιστά σχεδόν αδύνατη την αλλαγή αυτής της σειράς. Δεύτερον, αυτός ο μηχανισμός καθυστερεί την προσθήκη νέων block, έτσι ώστε, κατά μέσο όρο, ένα νέο block να προστίθεται στο blockchain μόνο κάθε 10 λεπτά. Έτσι, όλοι οι συμμετέχοντες στο δίκτυο παγκοσμίως έχουν αρκετό χρόνο για να ενημερωθούν στην ίδια, τελευταία κατάσταση του blockchain.

Συνοπτικά, οι εξορύκτες (miners) διατηρούν το δίκτυο Bitcoin σε λειτουργία. Χάρη σε αυτούς, νέες συναλλαγές υποβάλλονται σε επεξεργασία και προστίθενται στο blockchain. Οι πλήρεις κόμβοι (full nodes) διατηρούν αντίγραφα της συνολικής καταγραφής, βεβαιώνουν ότι τηρούνται οι κανόνες και διασφαλίζουν ότι δεν εισέρχονται δόλιες συναλλαγές στο blockchain.

21 εκατομμύρια Bitcoin

Παρόλο που προστίθενται συνεχώς περισσότερα block στο blockchain του Bitcoin και οι εξορύκτες (miners) ανταμείβονται για αυτήν τη δουλειά με νέα Bitcoin, ο συνολικός αριθμός Bitcoin περιορίζεται στα 21 εκατομμύρια. Δεν θα υπάρξουν ποτέ περισσότερα από 21 εκατομμύρια Bitcoin. Όμως αυτά τα 21 εκατομμύρια νομίσματα δεν ήταν σε κυκλοφορία από την αρχή. Αντίθετα, απελευθερώνονται από τον κώδικα Bitcoin σύμφωνα με ένα αυστηρό χρονοδιάγραμμα έκδοσης.

Όταν κυκλοφόρησε το Bitcoin, ο κώδικας απελευθέρωνε 50 νέα Bitcoin στους εξορύκτες (miners) περίπου κάθε 10 λεπτά. Τέσσερα χρόνια μετά την κυκλοφορία, ο αριθμός των Bitcoin που κυκλοφόρησαν ανά δέκα λεπτά μειώθηκε στο μισό. Αυτή η διαδικασία ονομάζεται «halving» (υποδιπλασιασμός) και περιγράφει το γεγονός ότι η ανταμοιβή παραγωγής block για τους εξορύκτες (miners)

μειώνεται κατά το ήμισυ κάθε 4 χρόνια. Επί του παρόντος, υπάρχουν ήδη 19 εκατομμύρια Bitcoin σε κυκλοφορία. Το υπόλοιπο Bitcoin θα εξορύσσεται μέχρι το έτος 2140. Μετά από αυτό, οι εξορύκτες (miners) θα αποζημιώνονται μόνο μέσω τελών συναλλαγών.

Η αυστηρά περιορισμένη ποσότητα μονάδων Bitcoin είναι μια από τις θεμελιώδεις ιδιότητες του κρυπτονομίσματος και καθιστά το Bitcoin ένα εξαιρετικά σπάνιο αγαθό. Αυτή η απόλυτη ψηφιακή σπανιότητα είναι επίσης μια σημαντική προϋπόθεση για τη λειτουργία του Bitcoin ως μέσο αποθήκευσης αξίας για μεγάλες χρονικές περιόδους και είναι ο λόγος που το Bitcoin ονομάζεται συχνά ψηφιακός χρυσός ή χρυσός 2.0.

Το αποτέλεσμα: Ψηφιακή Ιδιοκτησία

Εξετάζοντας όλα τα χαρακτηριστικά του δικτύου Bitcoin συνδυαστικά, μπορεί κανείς να δει τη σημασία αυτής της εφεύρεσης. Για πρώτη φορά στην ιστορία, υπάρχει ένα ψηφιακό αγαθό που είναι διαθέσιμο μόνο σε αυστηρά περιορισμένο αριθμό. Τα Bitcoin δεν μπορούν να αντιγραφούν ή να παραχθούν δύο φορές.

Χάρη σε αυτό το επίτευγμα, το Bitcoin αναφέρεται συχνά ως ψηφιακή ιδιοκτησία. Επειδή ακριβώς όπως κάθε κομμάτι γης σε αυτή τη γη είναι μοναδικό και υπάρχει μόνο μία φορά, κάθε μονάδα Bitcoin είναι επίσης μοναδική και υπάρχει μόνο μία φορά στον ψηφιακό χώρο.

Και αυτές οι μονάδες Bitcoin μπορούν να ανήκουν πραγματικά. Μόνο το άτομο που έχει στην κατοχή του το αντίστοιχο ιδιωτικό κλειδί (private key), το οποίο είναι ένας συνδυασμός αριθμών και γραμμάτων που αποτελείται από 64 χαρακτήρες, μπορεί να μεταφέρει το Bitcoin που του αναλογεί. Με άλλα λόγια, χωρίς αυτό το ιδιωτικό κλειδί, το Bitcoin δεν μπορεί να κλαπεί, να κατασχεθεί ή να αποκλειστεί. Αυτό επιτρέπει στον ιδιοκτήτη να έχει τον απόλυτο έλεγχο των οικονομικών του πόρων, ανεξάρτητα από το αν είναι εκατομμυριούχος, πολιτικός πρόσφυγας ή διωκόμενος πιστωτής. Για πρώτη φορά από την εφεύρεση του υπολογιστή, είναι δυνατή η πραγματική κατοχή ψηφιακών περιουσιακών στοιχείων.

ΓΙΑΤΙ ΤΟ BITCOIN;

Γιατί όμως όλη αυτή η μανία γύρω από το Bitcoin; Η δυνατότητα πραγματικής κατοχής ενός ψηφιακού στοιχείου μπορεί να είναι επαναστατική. Αλλά γιατί κάποιος θα ήθελε να κατέχει το Bitcoin εξ αρχής;

Το καλύτερο και των δύο κόσμων

Στους περασμένους αιώνες, πολύτιμα μέταλλα και αργότερα μετρητά με τη μορφή νομισμάτων και τραπεζογραμμάτων χρησιμοποιήθηκαν ως μέσα πληρωμής. Αυτά είχαν το πλεονέκτημα ότι μπορούσαν να αποθηκευτούν και να δαπανηθούν ανεξάρτητα από τρίτους. Το ρητό «τα μετρητά είναι τυπωμένη ελευθερία» το συνοψίζει πολύ καλά. Ωστόσο, το μειονέκτημα των πολύτιμων μετάλλων και των μετρητών είναι ότι είναι δύσκολο να χρησιμοποιηθούν στον ψηφιακό χώρο του Διαδικτύου. Το αργότερο από την εμφάνιση

των ηλεκτρονικών αγορών, οι χρεωστικές και πιστωτικές κάρτες έχουν καθιερωθεί στο γενικό πληθυσμό.

Αλλά τώρα που οι περισσότεροι άνθρωποι χρησιμοποιούν ψηφιακό χρήμα σε τραπεζικούς λογαριασμούς αντί για μετρητά, οι κίνδυνοι αντισυμβαλλομένου που αντιμετωπίζουν αυξάνονται. Εάν, για παράδειγμα, ένα χρηματοπιστωτικό ίδρυμα κηρύξει πτώχευση, οι αποταμιεύσεις των πελατών ενδέχεται να χαθούν. Ή, όπως συνέβη στην Κύπρο το 2013, εάν οι αναλήψεις μετρητών περιοριστούν σοβαρά, τεθούν σε εφαρμογή έλεγχοι κεφαλαίων (capital controls) και πραγματοποιηθεί αναγκαστική κατάσχεση σε αποταμιευτικούς λογαριασμούς, τότε οι άνθρωποι δεν έχουν πλέον τον έλεγχο των χρημάτων τους. Ή, όπως συμβαίνει σήμερα σε πολλές δυτικές χώρες, εάν οι πελάτες τραπεζών δεν

επιτρέπεται να στέλνουν χρήματα σε συγγενείς τους επειδή ζουν στην Κούβα ή το Ιράν, εξαρτώνται από τρίτους για την έγκριση όλων των συναλλαγών τους.

Με τη μετάβαση από το χαρτί στο ψηφιακό χρήμα, που είναι αποθηκευμένο σε τραπεζικούς λογαριασμούς, τελικά δεν έχουμε πλέον τον έλεγχο των δικών μας χρημάτων. Μέχρι τώρα, ωστόσο, αυτό το μειονέκτημα ήταν το τίμημα που έπρεπε να πληρώσουμε για να συμμετάσχουμε σε μια ψηφιοποιημένη ζωή.

Το Bitcoin προσφέρει μια λύση σε αυτό το δίλημμα. Ως ψηφιακό χρήμα, είναι ιδανικά κατάλληλο για χρήση στον ψηφιακό χώρο. Ταυτόχρονα, το Bitcoin μπορεί να αποθηκευτεί

ως ψηφιακή ιδιοκτησία χωρίς να χρειάζεται να βασιστείτε σε τρίτα μέρη (τράπεζες) για φύλαξη. Έτσι, οι ιδιοκτήτες Bitcoin μπορούν να αποθηκεύουν τα νομίσματά τους - με τη μορφή ιδιωτικών κλειδιών - κάτω από το στρώμα ή οπουδήποτε πιστεύουν ότι είναι πιο ασφαλές.

Τέλειος Συγχρονισμός

Το Bitcoin δημιουργήθηκε εν μέσω της παγκόσμιας οικονομικής κρίσης του 2008/09. Στο πρώτο block της αλυσίδας (blockchain) Bitcoin - που ονομάζεται επίσης Genesis block - ο Satoshi Nakamoto άφησε ένα ισχυρό μήνυμα. Παρέθεσε έναν τίτλο που δημοσιεύτηκε στην εφημερίδα The Times λέγοντας: «Η καγκελάριος στα πρόθυρα του

Bitcoin Genesis Block

Raw Hex Version

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	;f1ýz{.²zç,>
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.È.Ã^ŠQ2:Ÿ,ª
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.ˆ^J)«_IŸŸ...¬+
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ŸŸŸŸM.ŸŸ..
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Times 03/
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 Chancel
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brink of
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bailout f
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksŸŸŸŸ..ð.
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠŸ°pUH'
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"(à9.
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybàê.aB¶IÖ¿?Lİ8Ä
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.â.Ā.ß\8M+ø..W
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._¬....

δεύτερου προγράμματος διάσωσης για τις τράπεζες».

Με αυτή την πράξη, ο Satoshi εξέφρασε την φιλοσοφία των Cypherpunks σχετικά με την κριτική τους προς οτιδήποτε κρατικό. Στη χρηματοπιστωτική κρίση του 2008, οι κεντρικές τράπεζες έβγαλαν τεράστια ποσά νέου χρήματος σε κυκλοφορία για να σώσουν τις τράπεζες. Στο τέλος, ωστόσο, οι αποταμιευτές το πλήρωσαν, καθώς οι αποταμιεύσεις τους έχασαν την αξία τους λόγω του πληθωρισμού από την αύξηση του χρήματος. Αυτό το γεγονός επιβεβαίωσε για άλλη μια φορά τους Cypherpunks, τη δυσπιστία τους προς το κράτος και τις κεντρικές τράπεζες, και ενίσχυσε την πεποίθησή τους ότι χρειαζόνταν επείγοντως μία μορφή χρήματος ανεξάρτητη από το κράτος.

Η ίδια διαδικασία, μόνο σε μεγαλύτερη κλίμακα, έχει επαναληφθεί και από το ξέσπασμα της πανδημίας Covid-19. Μόνο το 2020, η προσφορά χρήματος στις ΗΠΑ αυξήθηκε κατά 50% και σε άλλες χώρες - συμπεριλαμβανομένης της Ελβετίας - το ψηφιακή εκτύπωση χρήματος λειτουργεί συνεχώς. Άμεση συνέπεια αυτού είναι τα χαμηλά επιτόκια ρεκόρ - ακόμη και τα αρνητικά επιτόκια στην Ελβετία - και ο ισχυρός πληθωρισμός περιουσιακών στοιχείων.

Αντιστάθμισμα έναντι της υποτίμησης του νομίσματος

Το Bitcoin λοιπόν κυκλοφόρησε την καλύτερη δυνατή στιγμή. Σπάνια το θέμα των χρημάτων ήταν πιο επίκαιρο και τα ερωτηματικά μεγαλύτερα από σήμερα. Με την περιορισμένη προσφορά του στα 21 εκατομμύρια, το Bitcoin προσφέρει μια ευχάριστη αντίθεση σε σχέση με τους συνεχώς αυξανόμενους ισολογισμούς των κεντρικών τραπεζών. Η περιορισμένη προσφορά του προσφέρει προστασία από τη μείωση του κεφαλαίου, όπως έχει παρατηρηθεί με όλα τα νομίσματα παγκοσμίως τις τελευταίες δεκαετίες.

Από τη δημιουργία του λοιπόν, το Bitcoin έχει σχεδιαστεί για να διασφαλίζει τη διατήρηση της αγοραστικής δύναμης για μεγάλες περιόδους. Δεδομένου ότι το Bitcoin είναι σπάνιο, είναι ακόμη καλύτερο σε αυτό από τον χρυσό, ο οποίος έχει καθαρή εισροή 1-2% κάθε χρόνο. Επιπλέον, το κόστος αποθήκευσης και μεταφοράς Bitcoin είναι επίσης σημαντικά χαμηλότερο σε σύγκριση με τον χρυσό, γεγονός που επιτρέπει επίσης την καλύτερη διατήρηση της αξίας με την πάροδο του χρόνου.

Προστασία της Περιουσίας

Ένα άλλο ζήτημα που εξαλείφει το Bitcoin είναι η προστασία της ιδιοκτησίας. Ενώ ο χρυσός ή τα μετρητά συνήθως πρέπει να αποθηκεύονται με ασφάλεια και με μεγάλο κόστος για να προστατευτούν από κλοπή, το Bit-

coin μπορεί να αποθηκευτεί και να μεταφερθεί με σχεδόν μηδενικό κόστος. Ακόμη και σημαντικά ποσά μπορούν να ληφθούν οπουδήποτε στον κόσμο με έναν κωδικό που αποτελείται από δώδεκα ή είκοσι τέσσερις λέξεις. Μόλις απομνημονευθεί και καταστραφεί η φυσική μορφή του, αυτός ο κωδικός δεν μπορεί να κλαπεί από κανέναν, καθιστώντας το Bitcoin πίσω από τον κωδικό ασφαλές και επιτρέποντας στον ιδιοκτήτη του να τα πάρει μαζί του στον τάφο, εάν το επιθυμεί.

ΑΓΟΡΑ BITCOIN

Υπάρχουν δύο τρόποι για να αποκτήσετε το Bitcoin. Είτε με το να κερδίζετε Bitcoin ως εξορύκτης (miner) - κάνοντας mining - είτε αγοράζοντας Bitcoin από άλλο άτομο. Δεδομένου ότι η εξόρυξη με οικιακές συσκευές έχει γίνει ουσιαστικά αδύνατη στις μέρες μας, ο μόνος τρόπος που απομένει για τους νεοφερμένους είναι να αγοράσουν Bitcoin.

Ανταλλακτήρια Bitcoin & μεσίτες

Ο ευκολότερος τρόπος για να αγοράσετε Bitcoin είναι μέσω ενός ανταλλακτηρίου crypto ή ενός μεσίτη. Αυτά λειτουργούν παρόμοια με τις πλατφόρμες συναλλαγών μετοχών. Μετά το άνοιγμα ενός προσωπικού λογαριασμού, μπορούν να μεταφερθούν ελβετικά φράγκα, ευρώ ή δολάρια ΗΠΑ μέσω τραπεζικού εμβάσματος ή πιστωτικής κάρτας. Μόλις φτάσουν τα χρήματα στον προσωπικό σας

λογαριασμό στο ανταλλακτήριο, το Bitcoin μπορεί να αγοραστεί 24/7 με μερικά κλικ στην τρέχουσα τιμή της αγοράς. Στην Ευρώπη, είναι δυνατό να αγοράσετε Bitcoin χωρίς εγγραφή, επαλήθευση στοιχείων ή κατάθεση χρημάτων μπροστά με τη δημοφιλή επενδυτική εφαρμογή [Re-lai](#) που υποστηρίζει μόνο Bitcoin.

Peer-to-peer

Ως εναλλακτική λύση στα ανταλλακτήρια crypto, το Bitcoin μπορεί επίσης να αγοραστεί απευθείας από άλλους συμμετέχοντες στην αγορά μέσω πλατφορμών peer-to-peer χωρίς να μεσολαβεί κάποιο ανταλλακτήριο. Αυτό επιτρέπει μεγαλύτερη ανωνυμία, καθώς δεν χρειάζεται να αποκαλύπτονται προσωπικά δεδομένα κατά τη διαδικασία.

Bitcoin ATMs

Υπάρχει επίσης η δυνατότητα ανάληψης Bitcoin μέσω ATM. Αυτά

είναι ήδη διαθέσιμα σε πολλές χώρες, όπως η [Ελβετία](#), η [Γερμανία](#), η [Αυστρία](#) και η [Ελλάδα](#). Στα Bitcoin ATM, μπορεί κάποιος να αγοράσει Bitcoin ανώνυμα με μετρητά ή με χρήση πιστωτικής κάρτας. Δεν είναι απαραίτητος λογαριασμός ούτε πορτοφόλι crypto.

Ασφαλής Αποθήκευση του Bitcoin

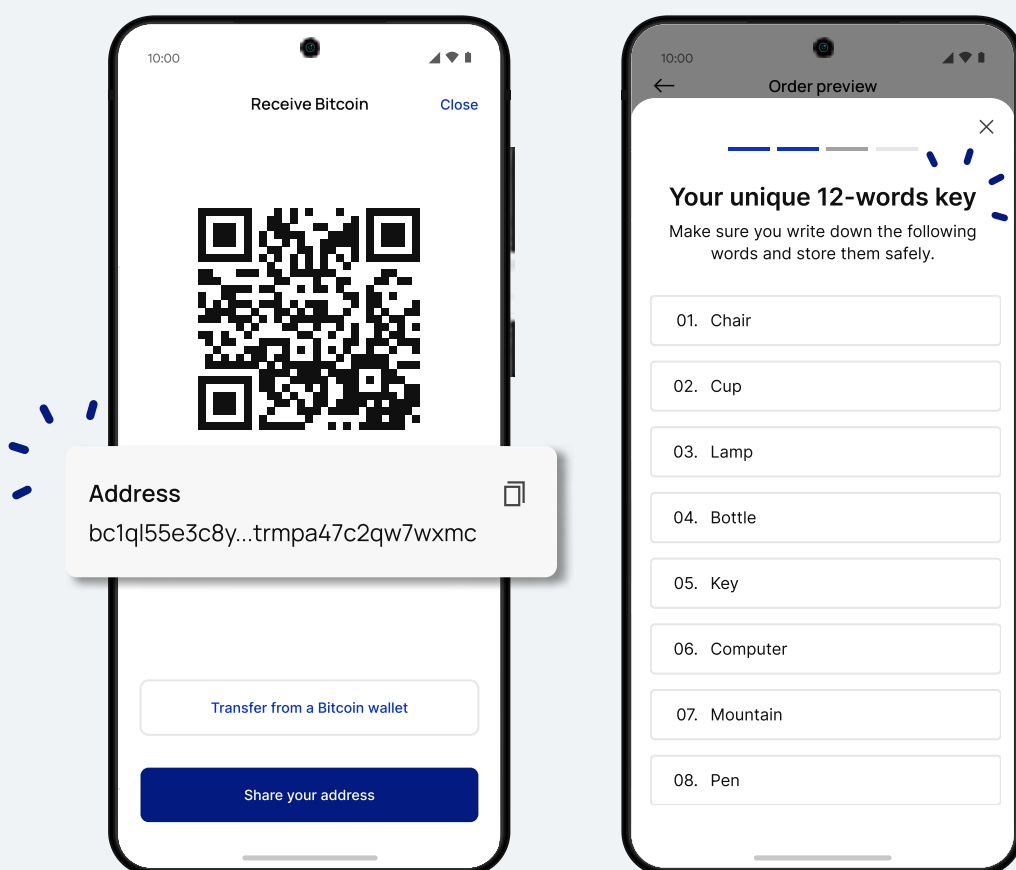
Μόλις αποκτηθούν τα Bitcoins, τίθεται το ζήτημα του ασφαλούς χειρισμού και αποθήκευσης τους. Το Bitcoin και τα κρυπτονομίσματα διέπονται από την αρχή: «όχι τα κλειδιά σας, όχι τα νομίσματά σας» ή «not your keys, not your coins». Για να έχετε στην κατοχή σας πραγματικά τα Bitcoin σας, πρέπει να έχετε στην κατοχή σας τα αντίστοιχα ιδιωτικά κλειδιά (private keys). Αυτή η κάπως

τεχνική έκφραση σημαίνει ότι έχετε πραγματικά τον έλεγχο του Bitcoin σας, μόνο εάν τα αποθηκεύσετε σε ένα προσωπικό ψηφιακό πορτοφόλι στο οποίο έχετε τα ιδιωτικά κλειδιά.

Όσο τα Bitcoin κατατίθενται σε ένα ανταλλακτήριο crypto, είναι υπό τον έλεγχο του ανταλλακτηρίου. Εάν το ανταλλακτήριο παραβιαστεί, χρεοκοπήσει ή είναι δόλιο, τα Bitcoin σας μπορεί να χαθούν για πάντα.

Self-Custody - Αυτοδιαχείριση

Σε αντίθεση με έναν τραπεζικό λογαριασμό, το Bitcoin σας δίνει την επιλογή να αποθηκεύσετε τις χρηματικές σας μονάδες σε ένα προσωπικό πορτοφόλι. Αυτό σας επιτρέπει να είστε η δική σας τράπεζα και έχει το πλεονέκτημα ότι έχετε τον απόλυτο έλεγχο του Bitco-



in σας. Σε αντάλλαγμα, αυτό έρχεται επίσης με κάποιες ευθύνες. Το ιδιωτικό κλειδί, το οποίο συχνά έχει τη μορφή δώδεκα ή είκοσι τεσσάρων λέξεων, πρέπει να αποθηκεύεται και να διατηρείται με ασφάλεια από τον ίδιο τον ιδιοκτήτη του αντίστοιχου Bitcoin. Ο εσφαλμένος ή αμελής χειρισμός μπορεί να οδηγήσει σε αμετάκλητη απώλεια του Bitcoin.

Πορτοφόλια: Ψηφιακά Πορτοφόλια - Digital Wallets

Τα ψηφιακά πορτοφόλια βοηθούν στην ασφαλή αποθήκευση του Bitcoin, ή πιο συγκεκριμένα, των ιδιωτικών κλειδιών. Το ίδιο το Bitcoin αποθηκεύεται πάντα στο blockchain και δεν μπορεί να μεταφερθεί σε πορτοφόλι. Μόνο τα κλειδιά πρόσβασης στο Bitcoin μπορούν να αποθηκευτούν σε ένα πορτοφόλι.

Έτσι, δημιουργήθηκαν πορτοφόλια για την αποθήκευση των ιδιωτικών κλειδιών με ασφάλεια και με απλό τρόπο. Επιπλέον, επιτρέπουν την αποστολή και λήψη Bitcoin με λίγα μόνο κλικ. Έτσι, τα πορτοφόλια είναι ένα χρήσιμο εργαλείο για το χειρισμό του Bitcoin.

Πορτοφόλι λογισμικού - Software Wallet

Τα πιο κοινά πορτοφόλια είναι τα πορτοφόλια λογισμικού ή Software Wallets. Τα πορτοφόλια λογισμικού μπορούν να εγκατασταθούν ως εφαρμογές επιτραπέζιου υπολογιστή

ή ως εφαρμογές smartphone. Κατά την διάρκεια της εγκατάστασης, τα ιδιωτικά κλειδιά του πορτοφολιού παρατίθενται με τη μορφή δώδεκα ή είκοσι τεσσάρων λέξεων (seed phrase). Αυτές οι λέξεις είναι συνώνυμες με το Bitcoin στο συγκεκριμένο πορτοφόλι. Όποιος ξέρει αυτές τις λέξεις έχει τον έλεγχο των νομισμάτων. Επομένως, οι λέξεις πρέπει να γράφονται με σωστή σειρά, κατά προτίμηση σε χαρτί, και να διατηρούνται ασφαλείς σε κρυφή τοποθεσία. Σε περίπτωση που χαθεί ή κλαπεί ο υπολογιστής ή το smartphone, το πορτοφόλι μπορεί να αποκατασταθεί ανά πάσα στιγμή με αυτές τις λέξεις.

Τα πορτοφόλια λογισμικού έχουν το πλεονέκτημα ότι μπορούν να ρυθμιστούν γρήγορα και είναι εύκολα στη χρήση. Ωστόσο, δεδομένου ότι τα πορτοφόλια λογισμικού είναι προγράμματα υπολογιστών που είναι εγκατεστημένα σε μια συσκευή και συνδέονται απευθείας στο Διαδίκτυο, υπάρχει πάντα ο κίνδυνος επιθέσεων χάκερ.

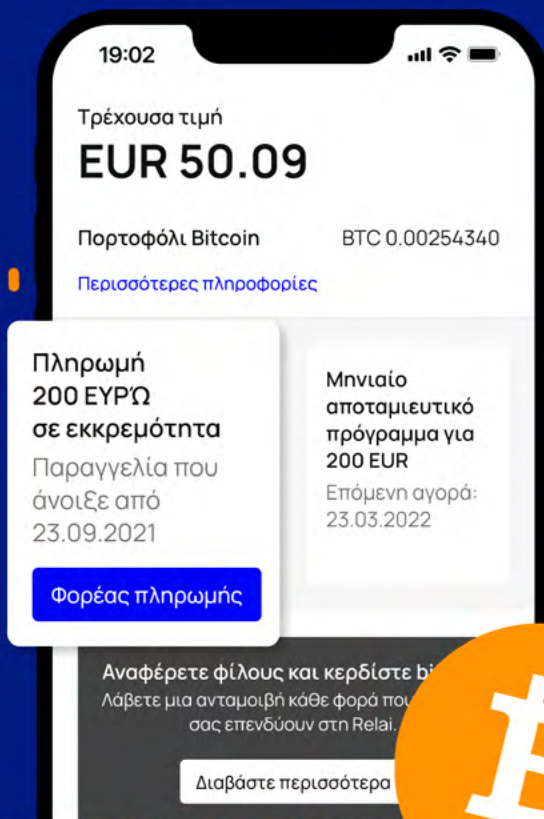
Πορτοφόλι Υλικού - Hardware Wallet

Εάν εκτιμάτε την ασφάλεια, θα πρέπει να χρησιμοποιήσετε ένα πορτοφόλι υλικού (hardware wallet). Αυτές οι μικρές συσκευές αποθηκεύουν τους κωδικούς πρόσβασης για το Bitcoin σε μια συσκευή που μοιάζει με USB me-

mory stick και που συνδέεται με τον υπολογιστή μόνο όταν χρειάζεται. Η συσκευή έχει σχεδιαστεί με τέτοιο τρόπο ώστε ακόμη και ένας υπολογιστής που έχει μολυνθεί με κακόβουλο λογισμικό δεν μπορεί να έχει πρόσβαση στους κωδικούς.

Κατά τη δημιουργία ενός πορτοφολιού υλικού (hardware wallet), δημιουργούνται δώδεκα ή είκοσι τέσσερις λέξεις (seed phrase), οι οποίες πρέπει να καταγράφονται με τη σωστή σειρά και να αποθηκεύονται με ασφάλεια. Εάν χαθεί ποτέ το πορτοφόλι υλικού (hardware wallet), μπορεί να ανακτηθεί με τη βοήθεια των λέξεων. Παραδείγματα πορτοφολιών υλικού (hardware wallet) είναι τα BitBox και Trezor.

 Made in Switzerland



Η ΠΙΟ ΑΠΛΗ ΕΦΑΡΜΟΓΗ ΓΙΑ ΑΓΟΡΑ BITCOIN ΣΤΗΝ ΕΥΡΩΠΗ



Bitcoins που ελήφθησαν BTC 0.00254340
24.09.2021 CHF 50.65

Relai



Αγοράστε bitcoins σε ένα λεπτό από
μόλις 10 EUR/CHF, χωρίς επαλήθευση.



**ΔΗΜΟΣΙΟ
ΚΛΕΙΔΙ**
Γραμματοκιβώτιο

**ΙΔΙΩΤΙΚΟ
ΚΛΕΙΔΙ**
Κλειδιά για το
γραμματοκιβώτιο

**ΔΗΜΟΣΙΟ
ΔΙΕΥΘΥΝΣΗ**
ΔΗΜΟΣΙΑ
ΔΙΕΥΘΥΝΣΗ

Αποστολή και λήψη Bitcoin

Η αποστολή και λήψη Bitcoin είναι πολύ εύκολη. Κάθε πορτοφόλι Bitcoin έχει τη δημόσια διεύθυνση (public address) του που δημιουργείται από το λεγόμενο δημόσιο κλειδί (public key). Αυτό χρησιμεύει ως διεύθυνση λήψης, παρόμοια με ένα IBAN. Όποιος έχει αυτή τη διεύθυνση μπορεί να στείλει Bitcoin στο αντίστοιχο πορτοφόλι. Η διεύθυνση εμφανίζεται συχνά ως κωδικός QR, γεγονός που απλοποιεί περαιτέρω τον χειρισμό.

Εάν θέλετε να στείλετε Bitcoin σε κάποιον, μπορείτε είτε να εισαγάγετε τη διεύθυνση Bitcoin του παραλήπτη στο πορτοφόλι σας κάτω από το ,send' είτε να σαρώσετε τον αντίστοιχο κωδικό QR. Τα τέλη συναλλαγής (transactions fees) που προκύπτουν αφαιρούνται αυτόματα

από το πορτοφόλι του αποστολέα. Το ποσό των χρεώσεων συναλλαγής ποικίλλει ανάλογα με το φόρτο του δικτύου και μπορείτε να το αναζητήσετε [εδώ](#). Χρειάζονται κατά μέσο όρο 10 λεπτά για να φτάσει η μεταφορά στον παραλήπτη. Ωστόσο, μπορεί επίσης να διαρκέσει περισσότερο, ανάλογα με το ύψος των προμηθειών που είστε διατεθειμένοι να πληρώσετε.

Πληρωμές με Bitcoin

Όταν δημιουργήθηκε το Bitcoin, υπήρχε η ελπίδα ότι το Bitcoin θα μπορούσε μια μέρα να χρησιμοποιηθεί για την πληρωμή καθημερινών αγαθών. Και θεωρητικά, αυτό είναι δυνατό σήμερα. Ορισμένες κρατικές φορολογικές υπηρεσίες, μη κερδοσκοπικοί οργανισμοί και ένας αυξανόμενος αριθμός

εταιρειών δέχονται το Bitcoin ως μέσο πληρωμής. Επειδή όμως οι συναλλαγές μέσω του δικτύου Bitcoin μπορεί να κοστίζουν αρκετά φράγκα και να διαρκούν τουλάχιστον 10 λεπτά, αυτό έχει νόημα μόνο για μεγαλύτερα ποσά. Για να στείλετε Bitcoin φθηνά και γρήγορα, χρειάζεται μια εναλλακτική λύση.

Lightning network - Ταχύτερα και Φθηνότερα

Ως εκ τούτου, ένα πρόσθετο επίπεδο δημιουργήθηκε πάνω από το δίκτυο Bitcoin. Αυτό το δίκτυο, που ονομάζεται Lightning, επιτρέπει την πληρωμή με Bitcoin σε δευτερόλεπτα με ελάχιστο κόστος. Σε χώρες όπως το Ελ Σαλβαδόρ, το Lightning network χρησιμοποιείται ήδη ενεργά και επιτυχώς.

Έτσι, η πληρωμή για καθημερινά αγαθά με Bitcoin θα πραγματοποιείται σε μεγάλο βαθμό μέσω του δικτύου Lightning στο

μέλλον. Οι εξελίξεις σε αυτόν τον τομέα τρέχουν ολοταχώς. Το Twitter, για παράδειγμα, παρουσίασε πρόσφατα μια λειτουργία «tipping» που χρησιμοποιεί το δίκτυο Lightning. Επιπλέον, η εφαρμογή Strike προσφέρει πληρωμές παγκοσμίως σε διάφορα νομίσματα με μηδενικό κόστος μέσω του δικτύου Lightning. Είναι, λοιπόν, αναμενόμενο ότι στο μέλλον μόνο μεγαλύτερα ποσά θα διακανονίζονται απευθείας μέσω του δικτύου Bitcoin, ενώ όλες οι άλλες συναλλαγές θα εκτελούνται μέσω του δικτύου Lightning.

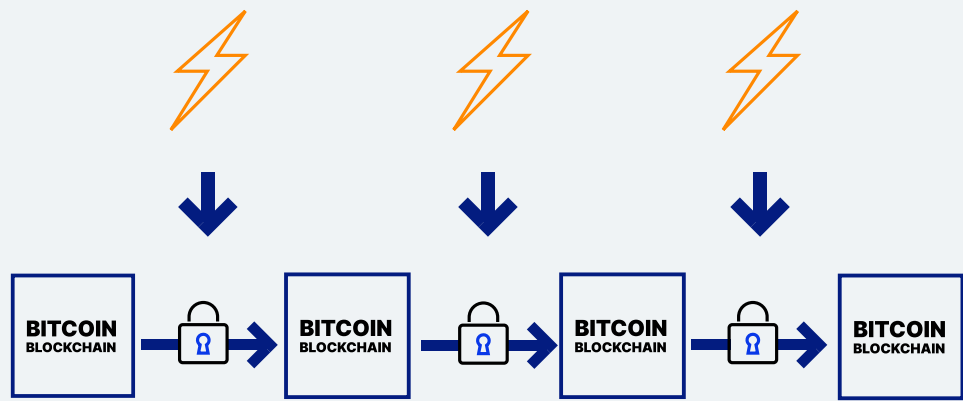
Δεδομένου ότι κυρίως μικρότερα ποσά αποστέλλονται μέσω του δικτύου Lightning, τα Satoshis ή σύντομα Sats, χρησιμοποιούνται ως λογιστική μονάδα αντί για το Bitcoin. 1 Bitcoin ισούται με 100.000.000 Satoshis (Sats). Για να χρησιμοποιήσετε το Lightning Network, πρέπει να δημιουργήσετε ένα πορτοφόλι Lightning.

ΜΙΑ ΜΑΤΙΑ ΣΤΟ ΜΕΛΛΟΝ

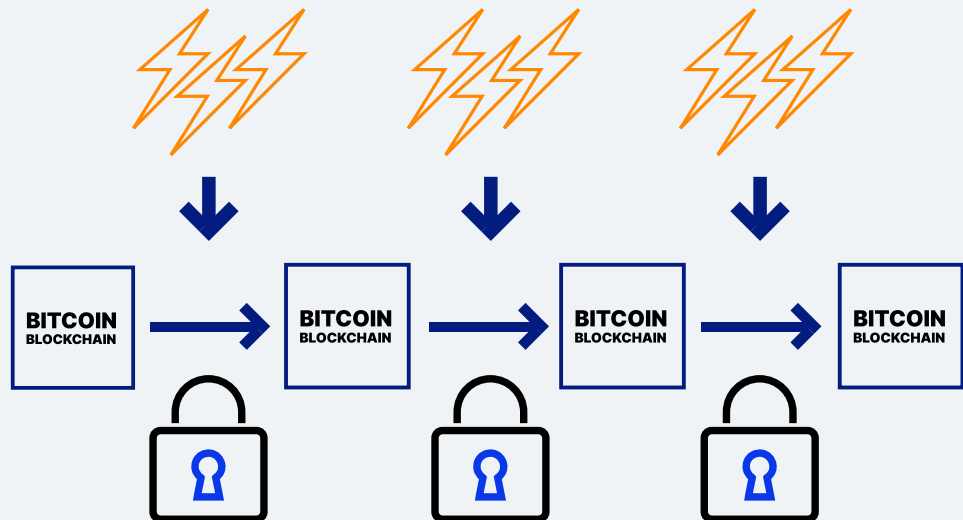
Στα λίγο πάνω από δέκα χρόνια ύπαρξής του, το Bitcoin έχει περάσει από πολλές καλές και κακές στιγμές. Το κρυπτονόμισμα κηρύχθηκε νεκρό ή έπεσε στη λήθη στο ευρύ κοινό

αρκετές φορές μετά από μεγάλες απώλειες σχετικά με την τιμή του. Ωστόσο, το Bitcoin έχει διαδοθεί σε όλο τον κόσμο την τελευταία δεκαετία.

Όσο λιγότερη ενέργεια με τη μορφή υπολογιστικής ισχύος χρησιμοποιείται για τη δημιουργία της αλυσίδας μπλοκ του Bitcoin, τόσο ευκολότερη είναι η μεταβολή της αργότερα.



Όσο περισσότερη ενέργεια με τη μορφή υπολογιστικής ισχύος χρησιμοποιείται για τη δημιουργία του Bitcoin Blockchain, τόσο πιο δύσκολο είναι να τροποποιηθεί αργότερα.



Bitcoin και ενέργεια

Μία από τις πρώτες ανησυχίες που εγείρονται συχνά σχετικά με την ανάπτυξη του Bitcoin είναι η κατανάλωση ενέργειας του Bitcoin Network. Η εξόρυξη Bitcoin (mining) καταναλώνει ήδη σημαντική ποσότητα ηλεκτρικής ενέργειας παγκοσμίως. Και αυτή η κατανάλωση είναι πιθανό να αυξηθεί στο μέλλον καθώς περισσότεροι άνθρωποι μπαίνουν στην εξόρυξη Bitcoin.

Όταν μιλάμε για το Bitcoin και την ενέργεια, είναι σημαντικό να κατανοήσουμε ότι η ποσότητα ενέργειας που ρέει στο δίκτυο Bitco-

in είναι κρίσιμη για την ασφάλεια του δικτύου. Όσο περισσότερη ενέργεια ρέει στο δίκτυο, τόσο πιο ασφαλές είναι. Αυτό συμβαίνει επειδή, για να αλλάξει το blockchain του Bitcoin, πρέπει να δαπανηθεί ξανά το ίδιο ποσό υπολογιστικής ισχύος (computing power) - και επομένως ενέργειας - που επενδύθηκε για τη δημιουργία του blockchain εξ αρχής. Ωστόσο, με εκατομμύρια υπολογιστές σε όλο τον κόσμο να παρέχουν υπολογιστική ισχύ στο δίκτυο Bitcoin, είναι σχεδόν αδύνατο για ένα άτομο, έναν οργανισμό ή ένα κράτος να συγκεντρώσει ποτέ αρκετή υπολογιστική ισχύ για να κάνει ακόμη και τις πιο μικρές αλλαγές

στο blockchain. Επομένως, η ισχύς κατακερματισμού (hashpower) και η σχετική κατανάλωση ενέργειας είναι ένα σημαντικό χαρακτηριστικό ασφαλείας του δικτύου Bitcoin.

Επιπλέον, οι υπολογιστές εξόρυξης Bitcoin έχουν το πλεονέκτημα ότι μπορούν να βρίσκονται οπουδήποτε στον κόσμο. Δεδομένου ότι οι εξορύκτες (miners) χρειάζονται τη φθηνότερη δυνατή ηλεκτρική ενέργεια για να είναι κερδοφόροι, συχνά εντοπίζουν μέρη όπου υπάρχει πλεονάσμα ισχύος, άρα και φθηνή, ηλεκτρική ενέργεια. Μακροπρόθεσμα, είναι πιθανό το mining να γίνεται σε μέρη όπου υπάρχει ενέργεια, ως επί το πλείστον από ανανεώσιμες πηγές καθώς αυτό καθιστά φθηνότερη την παραγωγή της.

Σύμφωνα με το Συμβούλιο Εξόρυξης Bitcoin (Bitcoin Mining Council), οι εξορύκτες Bitcoin (miners) χρησιμοποιούν αυτήν τη στιγμή περίπου κατά 56% ανανεώσιμες πηγές ενέργειας και υπάρχει η τάση να αυξηθεί αυτό το ποσοστό. Πολλοί ειδικοί του Bitcoin πιστεύουν ότι η εξόρυξη Bitcoin θα τροφοδοτείται από έως και 100% ανανεώσιμες πηγές ενέργειας στο μέλλον.

Μέχρι να συμβεί αυτό, ωστόσο, η κατανάλωση ενέργειας του Bitcoin συνοψίζεται στο ερώτημα εάν μία μορφή ασφαλούς και μη παραχαράξιμου χρήματος και αποθήκευσης αξίας όπως το Bitcoin

αξίζει αυτή τη δαπάνη ενέργειας - ή όχι.

Ελ Σαλβαδόρ - Το Bitcoin ως Εθνικό Νόμισμα

Πριν από μερικά χρόνια, οι οραματιστές πίστευαν ήδη ότι το Bitcoin θα αναγνωριστεί μια μέρα ως νόμιμο χρήμα από τα έθνη-κράτη. Το καλοκαίρι του 2021, είχε έρθει η ώρα: το Ελ Σαλβαδόρ ήταν η πρώτη χώρα στον κόσμο που εισήγαγε το Bitcoin ως νόμιμο χρήμα. Σε καταστήματα, εστιατόρια και σε εταιρίες παροχής υπηρεσιών κάθε είδους, η πληρωμή δεν μπορεί να γίνει μόνο με δολάρια ΗΠΑ αλλά και με Bitcoin. Για το σκοπό αυτό, οι πολίτες έλαβαν ένα προσαρμοσμένο πορτοφόλι Bitcoin, το οποίο επιτρέπει πληρωμές μέσω του δικτύου Lightning σε ελάχιστα δευτερόλεπτα και με ελάχιστο κόστος.

Άλλες χώρες όπως η Ουκρανία, η Βραζιλία και ο Παναμάς συζητούν επί του παρόντος παρόμοια νομοσχέδια. Εάν και άλλες χώρες ακολουθήσουν το παράδειγμα του Ελ Σαλβαδόρ, αυτό αφενός θα αύξανε περαιτέρω τη ζήτηση για Bitcoin και ακόμη πιο σημαντικό, θα υποστήριζε την αξιοπιστία του Bitcoin ως «χρήμα». Ως εκ τούτου, η αποδοχή του Bitcoin ως νόμιμο χρήμα σε όλο και περισσότερες χώρες αντιπροσωπεύει μια αποφασιστική φάση στην παγκόσμια υιοθέτηση του Bitcoin.

Νόμοι και κανονισμοί

Αυτές οι εξελίξεις οδήγησαν τα κράτη, τις κεντρικές τράπεζες και τις εταιρείες να ασχοληθούν εντατικά με τα κρυπτονομίσματα. Διάφορα κράτη, συμπεριλαμβανομένης της [Ελβετίας](#), έχουν εκδώσει κανονισμούς και οδηγίες σχετικά με τα κρυπτονομίσματα. Αυτό το βήμα χαιρετίζεται από πολλούς συμμετέχοντες στην αγορά, καθώς δημιουργεί νομοθετική ασφάλεια τόσο για τα crypto projects όσο και για τους εμπλεκόμενους επενδυτές.

Ρυθμίσεις βρίσκονται επίσης στον ορίζοντα στις ΗΠΑ, οι οποίες μέχρι στιγμής έχουν υιοθετήσει μια προσέγγιση laissez-faire. Η ακριβής μορφή που θα πάρουν αυτοί οι νέοι κανονιστικοί νόμοι στις ΗΠΑ παρακολουθείται στενά από την παγκόσμια κοινότητα crypto, καθώς θα έχουν σημαντικό αντίκτυπο σε ολόκληρο τον τομέα των κρυπτονομισμάτων.

Άλλα κρυπτονομίσματα

Το Bitcoin δεν είναι το μόνο κρυπτονόμισμα στις μέρες μας. Υπάρχουν πλέον πάνω από 16.000 διαφορετικά κρυπτονομίσματα και περιουσιακά στοιχεία. Αυτά τα νομίσματα και tokens έχουν διαφορετικά χαρακτηριστικά και λειτουργίες και δεν έχουν σχεδιαστεί όλα ως «νομίσματα» ή χρήματα. Ορισμένα μοιάζουν περισσότερο με μετοχές, καθώς η αξία τους

αντανακλά την επιτυχία ενός crypto project. Άλλα υποχρεούνται να κάνουν χρήση μιας συγκεκριμένης υπηρεσίας. Και ακόμα άλλα - τα λεγόμενα meme tokens - είναι κυρίως νομίσματα με σκοπό τη διασκέδαση.

Για να αποφύγετε τυχόν οικονομικές απώλειες, καλό είναι, να ρίξετε μια πιο προσεκτική ματιά στο αντίστοιχο νόμισμα και το project που υποστηρίζει πριν κάνετε οποιαδήποτε επένδυση.

Ψηφιακά Νομίσματα Κεντρικών Τραπεζών (CBDCs) (Central Bank Digital Currencies)

Τα κρυπτονομίσματα βρίσκονται σε μετάβαση από μια μη ελεγχόμενη φάση της Άγριας Δύσης σε έναν ρυθμιζόμενο χρηματοοικονομικό κόσμο κρυπτονομισμάτων. Αυτή η εξέλιξη δεν άφησε αλώβητες τις κεντρικές τράπεζες και έχουν διατυπωθεί ιδέες ότι οι κεντρικές τράπεζες πρέπει να εκδίδουν τα δικά τους κρυπτονομίσματα. Αυτά τα «ψηφιακά νομίσματα Κεντρικών Τραπεζών», ή CBDC, θα συνδύαζαν, λένε οι υποστηρικτές, τη σταθερότητα ενός κρατικού νομίσματος με τα οφέλη ενός νομίσματος που βασίζεται σε blockchain. Με λίγα λόγια, θα δημιουργούσαν ψηφιακά μετρητά, κατά κάποιον τρόπο.

Ωστόσο, ανάλογα με το σχεδιασμό του, ένα CBDC μπορεί να λάβει

θεμελιωδώς διαφορετικές μορφές. Διάφορες χώρες έχουν ξεκινήσει πιλοτικές δοκιμές με διαφορετικούς τύπους CBDC και σε λίγες χώρες έχουν ήδη ξεκινήσει να χρησιμοποιούνται. Ωστόσο, αναμένεται με ανυπομονησία εάν και με ποια μορφή θα λανσάρουν τα CBDC τους οικονομικά ισχυρές περιοχές όπως οι ΗΠΑ, η ΕΕ ή η Κίνα.

Ανταγωνισμός του Χρήματος

Η κοινωνία μας έχει συνηθίσει τόσο πολύ στα κρατικά νομίσματα τις τελευταίες δεκαετίες, που άλλα είδη χρημάτων ήταν σχεδόν αδιανόητα για πολλούς μέχρι πρόσφατα. Αλλά όχι πολύ καιρό πριν, ήταν μέρος της καθημερινής ζωής να κυκλοφορούν παράλληλα διάφορα είδη χρημάτων. Υπήρχαν τραπεζογραμμάτια από διάφορες τράπεζες, νομίσματα από διαφορετικά μέταλλα και άλλες χρηματικές αξίες που μπορούσαν να χρησιμοποιηθούν ως μέσα πληρωμής.

Με το Bitcoin, τα μη κρατικά νομίσματα είναι πλέον διαθέσιμα ξανά ως εναλλακτική λύση απέναντι στα κρατικά νομίσματα. Μέχρι τώρα, η πλειοψηφία των κυβερνήσεων ανέχονταν το Bitcoin. Σε κάποιο βαθμό, αυτό μπορεί να οφείλεται στην αποκεντρωμένη φύση του, η οποία καθιστά δύσκολη την επίθεση στο Bitcoin. Για τους πολίτες, αυτό σημαίνει ότι μια ψηφιακή εναλλακτική λύση για το κρατικό χρήμα είναι πλέον διαθέσιμη μαζί με το χρυσό και το ασήμι. Τα αποτελέσματα αυτού του πρόσθετου νομισματικού ανταγωνισμού θα είναι ένα συναρπαστικό θέμα που θα παρακολουθήσουμε στο μέλλον.

BITCOIN, ΚΑΙ ΤΩΡΑ ΤΙ;

Αν αναρωτιέστε τι πρέπει να κάνετε με όλες αυτές τις πληροφορίες, επιτρέψτε μου να κάνω μια πρόταση. Η είσοδος στον κόσμο του Bitcoin δεν κοστίζει τίποτα, ούτε χρόνο ούτε χρήματα. Αλλά θα γνωρίσετε μια τεχνολογία που πρόκειται να αλλάξει τον κόσμο μας και το μέλλον.

Επομένως: Δημιουργήστε έναν λογαριασμό σε ένα ανταλλακτήριο crypto ή κατεβάστε ένα πορτοφόλι στο smartphone σας και αγοράστε Bitcoin για 50€. Ή ζητήστε από έναν συνάδελφο να σας στείλει λίγα Bit-

coin στο πορτοφόλι σας. Αλλά πάρτε στα χέρια σας το Bitcoin τουλάχιστον μία φορά.

Επειδή εάν το Bitcoin φέρει την επανάσταση και γίνει τόσο διαδεδομένο όσο το Διαδίκτυο, όχι μόνο θα το γνωρίζετε θεωρητικά, αλλά θα έχετε χρησιμοποιήσει και εσείς το Bitcoin. Μερικές φορές αυτό κάνει τη διαφορά, καθώς αυτό σας δίνει μια ματιά και αίσθηση για την τεχνολογία, η οποία σας βάζει μπροστά σχετικά με την πλειοψηφία των ανθρώπων.

ΣΧΕΤΙΚΑ

ΜΕ ΤΟΝ ΣΥΓΓΡΑΦΕΑ

Ο Daniel Jungen είναι οικονομολόγος και χρηματοοικονομικός δημοσιογράφος με εξειδίκευση στα crypto. Ο Daniel είναι συνιδρυτής της [InsightDeFi](#), μιας ερευνητικής μπουτίκ που ειδικεύεται σε όλα τα

θέματα που αφορούν τα crypto. Μαζί με τους συνεργάτες του στο Insight-DeFi, δημοσιεύουν ένα [ενημερωτικό δελτίο](#) δύο φορές την εβδομάδα (στα γερμανικά) σχετικά με το Bitcoin, το DeFi και το Crypto.

ΣΧΕΤΙΚΑ ΜΕ ΤΗ RELAI

Ιδρύθηκε στην Ελβετία από τον Julian Liniger και τον Adem Biliçan, αφού προσπάθησαν να βρουν έναν ασφαλή, χωρίς προβλήματα χώρο για την αγορά bitcoin, η Relai κάνει την αποταμίευση και την επένδυση σε bitcoin προσβάσιμη σε όλους. Η εφαρμογή μόνο για bitcoin έχει σχεδιαστεί για να είναι απλή και διαισθητική, επιτρέποντας σε οποιονδήποτε στην Ευρώπη να

αγοράζει και να πουλάει bitcoin μέσα σε λίγα λεπτά, χωρίς να χρειάζεται εγγραφή, επαλήθευση ή χρηματική κατάθεση. Ελεγχμένη ανεξάρτητα και με πάνω από 35 εκατομμύρια CHF επενδεδυμένα σε Bitcoin μέσω της πλατφόρμας, η Relai δίνει στους καταναλωτές την ευκαιρία να ξεκλειδώσουν νέα μέσα αποταμίευσης και επένδυσης.

Μάθετε περισσότερα στο [Relai.app](#).

Ευχαριστούμε τον [@BonViveur.x](#) που μετέφρασε αυτό το e-book από τα αγγλικά στα ελληνικά. Τέλος, ευχαριστώ την [@MiaThalassa](#) για τις σημειώσεις και τα σχόλια.