Blockchain: Ουτοπία ή επιτόπια στροφή;

Βασικές έννοιες

Block

Τα μπλοκ είναι συνώνυμα με τις ψηφιακές σελίδες ενός *καθολικού*, το οποίο λέγεται και λογιστικό βιβλίο. Εκεί φυλάσσονται τα αμετάβλητα δεδομένα που σχετίζονται με το δίκτυο. Ένα μπλοκ είναι ένα αρχείο στην αλυσίδα των μπλοκ (block chain) το οποίο περιέχει και επικυρώνει πολλές συναλλαγές σε αναμονή. Περίπου κάθε 10 λεπτά, κατά μέσο όρο, ένα νέο μπλοκ που συμπεριλαμβάνει συναλλαγές επισυνάπτεται στο αλυσίδα των μπλοκ μέσω εξόρυξης.

Block Height

Το ύψος των μπλοκ είναι το άθροισμα των ατομικών μπλοκ σε κάθε αλυσίδα. Το πρώτο μπλοκ έχει μηδενικό ύψος και είναι γνωστό και ως πρώτη συναλλαγή (genesis block).

Blockchain

Είναι ένα διανεμημένο καθολικό, το οποίο καταγράφει όλες τις συναλλαγές και τα έξυπνα συμβόλαια για ένα κρυπτονόμισμα ή μια πλατφόρμα. Το blockchain αναπαράγεται σε πολλούς χιλιάδες κόμβους παγκοσμίως. Η αλυσίδα των μπλοκ (block chain) είναι ένα δημόσιο αρχείο συναλλαγών Bitcoin με χρονολογική σειρά. Η αλυσίδα των μπλοκ διαμοιράζεται μεταξύ όλων των χρηστών Bitcoin. Χρησιμοποιείται για να επαληθεύσει την μονιμότητα των συναλλαγών Bitcoin και για να αποτρέψει διπλές δαπάνες (double spending).

Bitcoin

Το bitcoin είναι το επώνυμο κρυπτονόμισμα με το οποίο είναι εξοικειωμένοι οι περισσότεροι χρήστες. Το κρυπτονόμισμα αυτό λειτουργεί ως ένα αποκεντρωμένο, παγκόσμιο δίκτυο ομότιμων κόμβων, στο οποίο δεν υπάρχει καμία εκδοτική αρχή και κανένας αγοραστής. Αυτό συνεπάγεται πως δεν μπορεί να το ελέγξει κανένας φορέας, εφόσον η κεντρική εξουσία παρακάμπτεται. Το νόμισμα είναι ανοιχτό, δηλαδή έχει πιστοποίηση για πορτοφόλι και πιστοποίηση συναλλαγών. Αλλά το καλύτερο είναι το εξής: οποιοσδήποτε μπορεί να κάνει χρήση του Bitcoin μέσω smartphone ή ηλεκτρονικού υπολογιστή. Το Bitcoin δημιουργήθηκε από τον Satoshi Nakamoto το 2008 και αποτελεί την πρώτη εφαρμογή της τεχνολογίας του blockchain και το πρώτο κρυπτονόμισμα. Παραμένει μέχρι σήμερα το πιο διαδεδομένο κρυπτονόμισμα. Το παγκόσμιο απόθεμα σε bitcoin έχει οριστεί στα 21 εκατομμύρια – αυτή είναι η χρηματιστηριακή αξία όλων των bitcoins.

Cypherpunk

Με τον όρο «**Cypherpunk»** περιγράφεται κάθε ακτιβιστής που υποστηρίζει την ευρεία χρήση της ισχυρής κρυπτογράφησης και της τεχνολογίας ενίσχυσης της ασφάλειας (δεδομένων), ως μέσου επίτευξης της κοινωνικής και πολιτικής αλλαγής. Αυτές οι άτυπες ομάδες ακτιβιστών, οι οποίες επικοινωνούσαν αρχικά μέσα από λίστες ηλεκτρονικής αλληλογραφίας που κατάρτιζαν οι ίδιοι, έχουν στόχο την προστασία της ιδιωτικότητας και της ασφάλειας, μέσω της ενεργής χρήσης της κρυπτογραφίας. Οι Cypherpunks έχουν οργανωθεί σ’ ένα ενεργό κίνημα από τα

τέλη της δεκαετίας του ’80.

Charlie Lee
Ο Τσάρλι Λι είναι ο δημιουργός του Litecoin και, πριν από αυτό, επικεφαλής μηχανικός του Coinbase. Αν και είναι ο πρωτεργάτης του Litecoin, ο Λι έχει αφοσιωθεί σε πολυάριθμα πρότζεκτ που αφορούν αποκλειστικά το Bitcoin. Πριν από τις εξορμήσεις του στον κόσμο των κρυπτονομισμάτων, ο Λι εργαζόταν ως μηχανικός υπολογιστών σε πολλές εταιρείες, όπως στην Google και την Guidewire Software.

David Lee Chaum
Ο Ντέιβιντ Λι Τσομ είναι Αμερικανός επιστήμονας των Η/Υ και κρυπτογράφος. Έγινε διάσημος για την ανάπτυξη του ecash, μιας εφαρμογής ηλεκτρονικών «μετρητών», η οποία έχει στόχο τη διατήρηση της ανωνυμίας του χρήστη. Έχει επίσης εφεύρει πολλά κρυπτογραφικά πρωτόκολλα, ενώ ίδρυσε και το DigiCash, μια εταιρεία ηλεκτρονικού χρήματος. Το άρθρο του «Μη ανιχνεύσιμη ηλεκτρονική αλληλογραφία, διεύθυνση αποστολέα και ψηφιακά ψευδώνυμα» (1981), προλείανε το έδαφος για την έρευνα στην ανώνυμη επικοινωνία.

Cryptocurrency
Το κρυπτονόμισμα είναι ένα αποκεντρωμένο ψηφιακό συνάλλαγμα, το οποίο μπορεί να χρησιμοποιηθεί για εμπορεύματα, υπηρεσίες και μεταφορές επενδυτικών αγαθών. Το πρώτο κρυπτονόμισμα ήταν το Bitcoin. Πρωτοκυκλοφόρησε στην αγορά τον Ιανουάριο του 2009.

Ανταλλακτήρια κρυπτονομισμάτων (Cryptocurrency Exchange)
Τα ανταλλακτήρια κρυπτονομισμάτων είναι ιστοσελίδες ή υπηρεσίες που επιτρέπουν την ανταλλαγή ψηφιακών κρυπτο-αγαθών με κρυπτονομίσματα και αντιστρόφως, ή την ανταλλαγή παραστατικού χρήματος (π.χ. δολάρια Ηνωμένων Πολιτειών) με κρυπτο-επενδυτικά αγαθά). Δύο από τα πιο χαρακτηριστικά παραδείγματα τέτοιων ανταλλακτηρίων είναι το Coinbase και το Binance.

Πορτοφόλια κρυπτονομισμάτων (Cryptocurrency Wallets)
Το πορτοφόλι κρυπτονομίσματος είναι ένας τρόπος αποθήκευσης των ιδιωτικών και δημόσιων κλειδιών για τα επενδυτικά αγαθά. Κάθε πορτοφόλι είναι ένα χρηματοφυλάκιο όπου μπορεί κανείς να καταφύγει για να εντοπίσει κλειδιά. Ένα Bitcoin πορτοφόλι είναι γενικώς **το ισοδύναμο ενός φυσικού πορτοφολιού στο δίκτυο Bitcoin**. Στην πραγματικότητα, το πορτοφόλι περιέχει τα δικά σας ιδιωτικό(ά) κλειδί(ά) τα οποία σας επιτρέπουν να ξοδεύετε τα bitcoins που κατανέμονται σε αυτή την αλυσίδα των μπλοκ (block chain). Το κάθε Bitcoin πορτοφόλι μπορεί να σας δείξει το συνολικό υπόλοιπο όλων των bitcoins που ελέγχει και σας αφήνει να πληρώσετε ένα συγκεκριμένο ποσό σε ένα συγκεκριμένο άτομο, όπως συμβαίνει και με ένα αληθινό πορτοφόλι. Αυτό διαφέρει από τις πιστωτικές κάρτες όπου χρεώνεστε από τον έμπορο.

Αποκέντρωση (Decentralization)
Η αποκέντρωση είναι ένα κριτήριο βάσει του οποίου εκτιμάται πόση εξουσία έχει ένας βασικός δικαιούχος. Μπορεί κανείς να ισχυριστεί πως τα blockchain είναι οπωσδήποτε πολύ

πιο αποκεντρωμένα από άλλες μεθόδους κατανομής δεδομένων, καθώς (τουλάχιστον στις δημόσιες αλυσίδες) δεν υπάρχει κανένας φύλακας να ελέγχει ποιος μπορεί να συμμετάσχει: όποιος κατέχει την υπολογιστική δύναμη μπορεί να γίνει μέρος του blockchain.

Ψηφιακή υπογραφή (Digital Signature)
Η ψηφιακή (κρυπτογραφική) υπογραφή είναι ένας ψηφιακός κώδικας που δημιουργείται από την αποκρυπτογράφηση ενός δημόσιου κλειδιού που είναι με τη σειρά του συνδεδεμένο μ' ένα ηλεκτρονικά κοινοποιημένο έγγραφο, το οποίο εξακριβώνει το περιεχόμενο του εγγράφου και την ταυτότητα του αποστολέα. Μια κρυπτογραφική υπογραφή είναι **ένας μαθηματικός μηχανισμός που επιτρέπει σε κάποιον να αποδείξει την κυριότητα**. Στην περίπτωση του Bitcoin, ένα Bitcoin πορτοφόλι και τα δικά του ιδιωτικό(ά) κλειδί(ά) συνδέονται με κάποια μαθηματική μαγεία. Όταν το λογισμικό σας Bitcoin υπογράψει μια συναλλαγή με το κατάλληλο ιδιωτικό κλειδί, όλο το δίκτυο μπορεί να δει ότι η υπογραφή συμπίπτει με τα bitcoins που ξοδεύονται. Ωστόσο, δεν υπάρχει τρόπος, που να χαλάσει ο κόσμος, κάποιος να μαντέψει το ιδιωτικό κλειδί σας για να κλέψει τα κερδισμένα με κόπο bitcoins σας.

Διανεμημένο καθολικό (Distributed ledger)
Πρόκειται για μια αντιστοιχία που γίνεται συχνά στα blockchain. Αντί για ένα κεντρικό καθολικό, το blockchain υπόσχεται τη διανομή των υπολοίπων μέσω ενός δικτύου διακομιστών.

Ethereum
Το Ethereum είναι μια αποκεντρωμένη πλατφόρμα για εφαρμογές που τρέχουν «έξυπνα συμβόλαια», η οποία βασίζεται στην τεχνολογία του blockchain και έχει στόχο την επίλυση προβλημάτων που σχετίζονται με τη λογοκρισία, την απάτη και την παρέμβαση τρίτων.

Χρηματική εγγύηση (Escrow)
Η χρηματική εγγύηση είναι μια οικονομική συμφωνία, σύμφωνα με την οποία ένα τρίτο μέλος αποταμιεύει και ρυθμίζει την πληρωμή των κεφαλαίων που απαιτείται από τα δύο μέλη που συμμετέχουν σε μια συγκεκριμένη συναλλαγή. Συντελεί στο να κάνει τις συναλλαγές πιο ασφαλείς, διατηρώντας την πληρωμή σ' έναν ασφαλή εγγυητικό λογαριασμό, ο οποίος αποδεσμεύεται μόνο όταν όλοι οι όροι της συμφωνίας έχουν τηρηθεί, υπό την επίβλεψη της εγγυήτριας εταιρείας.

James Dalton Bell
Ο Τζέιμς Ντάλτον Μπελ είναι ένας Αμερικανός κρυπτο-αναρχικός που συνέλαβε την ιδέα των διαδικτυακών πληρωμένων δολοφονιών, τις οποίες αποκαλεί «πολιτική δολοφονίας». Τον Απρίλιο του 1995, ο Μπελ συνέγραψε το πρώτο κεφάλαιο ενός δοκιμίου σε δέκα μέρη με τίτλο «Πολιτική δολοφονίας», στο οποίο περιγράφει εκτενώς μια αγορά φόνων, στην οποία ανώνυμοι δωρητές μπορούν να παραγγείλουν με εχεμύθεια τη δολοφονία μελών της κυβέρνησης ή άλλων προσώπων που καταπατούν τα δικαιώματα των πολιτών. Το 2001 το περιοδικό *Wired* αποκάλεσε τον Μπελ «έναν από τους πιο διάσημους δοκιμιογράφους του Διαδικτύου» και «τον πιο διαβόητο κρυπτο-κατάδικο του κόσμου».

Παραστατικό χρήμα (Fiat)
Το παραστατικό χρήμα είναι το μέσο πληρωμής που σχετίζεται με το εθνικό νόμισμα, όπως το αμερικανικό δολάριο, τη λίρα Αγγλίας ή το ευρώ. Θεωρείται νόμιμο χρήμα από μια κυβέρνηση, αλλά η αξία του δεν δικαιολογείται από φυσικούς πόρους, όπως από χρυσό.

Διχάλα (Fork)
Η διχάλα είναι μια πράξη λειτουργικού συστήματος που δημιουργεί μια εναλλακτική εκδοχή του blockchain, επιτρέποντας σε δύο αλυσίδες να τρέχουν παράλληλα σε διαφορετικές περιοχές του δικτύου.

Πρώτη συναλλαγή (Genesis Block)
Πρόκειται για την πρώτη συστοιχία/μπλοκ ενός blockchain.

Hodl
Το Hodl είναι ένα meme κρυπτονομισμάτων για αποταμίευση, και όχι για την πώληση των επενδυτικών αγαθών. Το meme δημιουργήθηκε τον Δεκέμβριο του 2013, όταν ένας χρήστης που είχε κατεβάσει μερικά ποτηράκια δαχτυλογράφησε κάτι λάθος σ' ένα δημοφιλές φόρουμ για το Bitcoin. Μπορείτε να βρείτε το σχετικό πρωτότυπο thread στη σελίδα bitcointalk.org.

Αρχική νομισματική προσφορά (ICO)
Καθώς τα κρυπτονομίσματα γίνονται ολοένα και πιο δημοφιλή, αυξάνεται και ο αριθμός των πρώτων νομισμάτων. Κάθε ένα από αυτά υπόσχεται να διορθώσει, να αναδείξει ή να βελτιώσει μια συγκεκριμένη όψη του τοπίου των κρυπτονομισμάτων. Αυτά τα νέα νομίσματα διατίθενται μέσω των ICO. Μ' άλλα λόγια, είναι η κρυπτο-παραλλαγή ενός χρηματιστηρίου προσφοράς νέων χρεογράφων με δημόσια εγγραφή.

Εξόρυξη (Mining)
Εξαιτίας της κρυπτογραφημένης φύσης των κρυπτονομισμάτων, η εξακρίβωση των συναλλαγών απαιτεί ένα τεράστιο ποσό υπολογιστικής δύναμης και εξειδικευμένου υλισμικού. Ως αντάλλαγμα για την υπολογιστική δύναμη, οι άνθρωποι που λύνουν (και συνεπώς εγκρίνουν) μια συναλλαγή) πληρώνονται σε κρυπτονομίσματα. Αυτή η διαδικασία ονομάζεται *εξόρυξη*. Η εξόρυξη είναι η διεργασία που δημιουργεί το υλισμικό υπολογιστή (computer hardware) για να κάνει μαθηματικούς υπολογισμούς ώστε το δίκτυο Bitcoin να επιβεβαιώσει τις συναλλαγές και να αυξήσει την ασφάλεια. Ως αμοιβή για τις υπηρεσίες τους, όσοι κάνουν εξόρυξη μπορούν να συλλέγουν τα τέλη συναλλαγών για τις συναλλαγές που επιβεβαιώνουν, μαζί με τα πρόσφατα δημιουργημένα bitcoins. Η εξόρυξη είναι μια εξειδικευμένη και ανταγωνιστική αγορά όπου οι αμοιβές χωρίζονται ανάλογα με το πόσος υπολογισμός έχει γίνει. Δεν κάνουν όλοι οι χρήστες Bitcoin mining και δεν είναι εύκολος τρόπος να βγάλετε χρήματα.

Σεληνιασμός (Mooning)
Το 2017, τα κρυπτονομίσματα έμελλε να αποκτήσουν πολλαπλάσια αξία εν μία νυκτί. Ολόκληρη η κεφαλαιακή αξία του τομέα αυξήθηκε από 15 δισεκατομμύρια δολάρια τον Ιανουάριο σε 600 δισεκατομμύρια δολάρια τον Δεκέμβριο του ίδιου χρόνου. Το Ripple ήταν ο

μεγαλύτερος νικητής. Η αξία του αυξήθηκε κατά 28,963% αυτούς τους 12 μήνες. Συγκριτικά, το S&P 500 ανέβηκε κατά 19,4%. Το φαινόμενο του πολλαπλασιασμού των κερδών με ένα και μόνο κέρμα είναι γνωστό ως «σεληνιασμός».

Κόμβος (Node)
Ο κόμβος είναι μια υπολογιστική συσκευή στο blockchain. Είναι υπεύθυνος για την πιστοποίηση των συναλλαγών, αλλά και για τη διατήρηση και επικαιροποίηση του διανεμημένου καθολικού.

Ομότιμη σύνδεση (Peer to Peer)
Η ομότιμη σύνδεση ή P2P αναφέρεται στις αποκεντρωμένες αλληλεπιδράσεις ανάμεσα σε δύο ή περισσότερα μέλη σ' ένα έντονα διασυνδεδεμένο δίκτυο. Οι συμμετέχοντες ενός δικτύου P2P ασχολούνται απευθείας ο ένας με τον άλλο, μέσα από ένα και μοναδικό σημείο διαμεσολάβησης. Η ομότιμη σύνδεση (peer-to-peer) αναφέρεται σε συστήματα που λειτουργούν όπως μια οργανωμένη συλλογική επιτρέποντας στο κάθε άτομο να αλληλοεπιδρά άμεσα με τους άλλους. Στην περίπτωση του Bitcoin, το δίκτυο είναι φτιαγμένο με τέτοιο τρόπο ώστε ο κάθε χρήστης να εκπέμπει τις συναλλαγές των άλλων χρηστών. Και, κυρίως, δεν απαιτείται καμία τράπεζα ως τρίτος.

Αρκετά Καλό Απόρρητο / Pretty Good Privacy (**PGP**)
Πρόκειται για ένα πρόγραμμα κρυπτογράφησης το οποίο παρέχει απόρρητο κρυπτογράφησης και επαλήθευσης για την επικοινωνία δεδομένων. Το PGP χρησιμοποιείται για την υπογραφή, την κρυπτογράφηση και την αποκρυπτογράφηση κειμένων, e-mail, φακέλων, καταλόγων και διαμερισμάτων σκληρών δίσκων, αλλά και για την ενίσχυση της ασφάλειας της ηλεκτρονικής αλληλογραφίας. Ο Φιλ Ζίμερμαν ανέπτυξε το PGP το 1991.

Απόδειξη κυριότητας (Proof-of-stake)
Η απόδειξη κυριότητας ενθαρρύνει τους ανθρώπους που έχουν στην ιδιοκτησία τους μια πλειάδα από μάρκες blockchain να λάβουν αποφάσεις για την επικύρωση της αλυσίδας. Στην πράξη, είναι αισθητά λιγότερο ενεργοβόρα πρακτική σε σχέση με την εξόρυξη.

Απόδειξη εργασίας (Proof-of-work)
Είναι ένα σύστημα στο οποίο μπλοκ δεδομένων συναλλαγών στο blockchain εξορύσσονται και επικυρώνονται από εξειδικευμένους υπολογιστές που επιβραβεύονται για την επίλυση μαθηματικών εξισώσεων.

Δημόσια/Ιδιωτικά κλειδιά (Public/Private Keys)
Τα κλειδιά είναι τα εργαλεία πρόσβασης στις ισοτιμίες και στη λήψη/αποστολή αξίας ή δεδομένων στο κρυπτονόμισμα. Το δημόσιο κλειδί είναι εφάμιλλο της ηλεκτρονικής διεύθυνσης. Είναι αυτό που επιτρέπει την αποστολή κεφαλαίων σε τρίτους. Μπορείς να μοιραστείς το δημόσιο κλειδί σου με ένα γενικό κοινό.

Satoshi Nakamoto
Το όνομα Σατόσι Νακαμότο είναι αυτό που χρησιμοποιήθηκε από τον ανώνυμο δημιουργό (ή

τους ανώνυμους δημιουργούς) που συνέλαβαν το bitcoin, υπέγραψαν τη Λευκή Βίβλο του bitcoin, αλλά και συνέλαβαν και ανέπτυξαν την πρώτη υλοποίηση αναφορών (reference implementation) του bitcoin. Ως μέρος της υλοποίησης, οι Σατόσι Νακαμότο ανέπτυξαν επίσης την πρώτη βάση δεδομένων του blockchain. Σε αυτή τη διαδικασία, ήταν οι πρώτοι που έλυσαν το ζήτημα της διπλής δαπάνης, χρησιμοποιώντας ένα δίκτυο ομότιμης σύνδεσης. Ήταν ενεργοί στην ανάπτυξη του bitcoin μέχρι και τον Δεκέμβριο του 2010.

Έξυπνα συμβόλαια (Smart Contracts)
Εκτός από τα κρυπτονομίσματα (μάρκες ή κέρματα), κάποιες αλυσίδες υποστηρίζουν επίσης τα έξυπνα συμβόλαια. Η επικρατέστερη μορφή δικτύου έξυπνων συμβολαίων είναι το Ethereum. Κάποια συμβόλαια επιτρέπουν στα μη συναλλαγματικά επενδυτικά αγαθά να αλλάξουν χέρια στην αλυσίδα, χωρίς τη χρήση μεσαζόντων. Τα αγαθά αυτά μπορεί να περιλαμβάνουν αρχεία συνδρομών, ασφάλειες ή ακόμα και ακίνητα.

Nick Szabo
Ο Νικ Ζάμπο είναι ένας από τους πρωτοπόρους του blockchain και των κρυπτονομισμάτων. Θεωρείται ευρέως ως ο εφευρέτης της έννοιας των έξυπνων συμβολαίων (smart contracts), τα οποία είναι σήμερα ένα θεμελιώδες χαρακτηριστικό των κρυπτονομισμάτων. Ο Ζάμπο είναι επίσης ο δημιουργός του bit gold, μιας αποκεντρωμένης πρόδρομης εκδοχής του Bitcoin, η οποία έθεσε τις βάσεις για την αρχική κατασκευή της αρχιτεκτονικής του Bitcoin.

Timothy C. May
Ο Τίμοθι Σι Μέι, γνωστός ως Tim May (21 Δεκεμβρίου 1951 – 13 Δεκεμβρίου 2018) ήταν ένας Αμερικανός συγγραφέας που εξειδικευόταν σε τεχνικά θέματα και πολιτική, και εργαζόταν ως μηχανικός ηλεκτρονικών υπολογιστών και ανώτατο επιστημονικό προσωπικό στην Intel, τα πρώτα χρόνια της εταιρείας. Ο Μέι ήταν ένα από τα ιδρυτικά στελέχη και ένας από τους πιο γενναιόδωρους συμμετέχοντες της λίστας ηλεκτρονικής αλληλογραφίας των Cypherpunk. Είχε γράψει εκτενώς για ζητήματα κρυπτογράφησης και απορρήτου από τη δεκαετία του ’90 έως το 2003.

Μάρκες (Tokens)
Μια μάρκα είναι μια ψηφιακή μονάδα που μπορεί να προγραμματιστεί, έχοντας τον δικό της κώδικα βάσης (codebase) που σχετίζεται με μια υπάρχουσα αλυσίδα. Οι μάρκες χρησιμοποιούνται για να διευκολύνουν τη δημιουργία αποκεντρωμένων εφαρμογών.

Vitalik Buterin
Ο Βιτάλικ Μπουτέριν είναι ο δημιουργός του Ethereum, της πλατφόρμας blockchain που λειτουργεί ως παγκόσμιος υπολογιστής για αποκεντρωμένες εφαρμογές. Το αντίστοιχο κρυπτονόμισμα, το Ether, είδε την αξία του να εκτοξεύεται το 2017 (η κεφαλαιακή αξία του Ethereu είναι κοντά στα 30 εκατομμύρια δολάρια). Είναι ο συνιδρυτής του περιοδικού *Bitcoin Magazine* και αυτή την περίοδο τρέχει το πρότζεκτ του Ethereum, δουλεύοντας για την αναβάθμιση του πρωτοκόλλου του.

Curated by: Voltnoi Brege & Quetempo