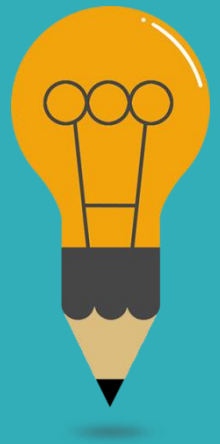
ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

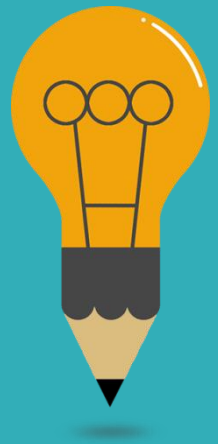
Τι είναι τα κρυπτονομίσματα;

Τα κρυπτονομίσματα είναι μία κατηγορία ψηφιακού χρήματος που έχει σχεδιαστεί για να είναι ασφαλής και σε πολλές περιπτώσεις, ανώνυμη. Πρόκειται για νομίσματα που συνδέονται με το Διαδίκτυο και χρησιμοποιούν την επιστήμη της κρυπτογραφίας για την επαλήθευση των συναλλαγών

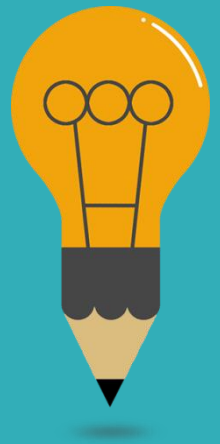


Τι είναι τα κρυπτονομίσματα;

Αφορούν καταχωρήσεις σε μία βάση δεδομένων που δεν μπορεί να αλλάξει, παρά μόνο υπό προϋποθέσεις. Η βασική διαφορά μεταξύ των υπαρχόντων νομισμάτων και των κρυπτονομισμάτων είναι πως τα δεύτερα δεν ελέγχονται από κάποιον κυβερνητικό μηχανισμό ή τραπεζικό σύστημα



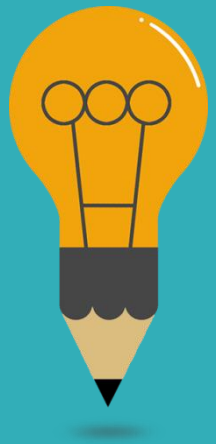
Τι είναι τα κρυπτονομίσματα;



Η **Παγκόσμια Τράπεζα** έχει ταξινομήσει τα κρυπτονομίσματα ως ένα υποσύνολο ψηφιακών νομισμάτων, το οποίο ορίζεται ως ψηφιακές αναπαραστάσεις αξίας που εκφράζονται στη δική τους λογιστική μονάδα (διαφορετική από το ηλεκτρονικό χρήμα) και τα οποία βασίζονται σε κρυπτογραφικές τεχνικές για την επίτευξη συναίνεσης

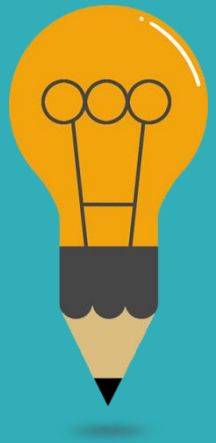
Πλεονεκτήματα Κρυπτονομισμάτων

1. ΧΡΗΣΤΗΣ



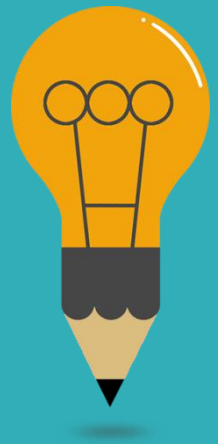
Ιδιωτικότητα	Απόλυτη ανωνυμία. Κάθε χρήστης προσδιορίζεται από έναν μόνο αριθμό και δεν υπάρχει καμία ταύτιση με τα προσωπικά του στοιχεία
Διαφάνεια	Το ιστορικό όλων των συναλλαγών (λογιστικό βιβλίο) είναι διαθέσιμο ανά πάσα στιγμή στον καθένα Λογισμικό ανοικτού κώδικα (open-source)
Συμμετοχή	Δυνατότητα συμμετοχής στη διαδικασία παραγωγής νομίσματος και στον έλεγχο συναλλαγών Δυνατότητα διορθώσεων και βελτιστοποιήσεων του συστήματος μέσω του open-source κώδικα
Εύκολη προσβασιμότητα	Δεν απαιτείται τραπεζικός λογαριασμός για τη συμμετοχή στο οικονομικό σύστημα

2. ΣΥΝΑΛΛΑΓΕΣ



Μηδενικό ή ελάχιστο κόστος	Δεν υπάρχουν έξοδα διαμεσολαβητή για την επιβεβαίωση της συναλλαγής Μηδενικά έξοδα παρόχου προστασίας
Υψηλή ταχύτητα	Οι συναλλαγές πραγματοποιούνται σε διάστημα μερικών δευτερολέπτων έως και κάποιων λεπτών, ακόμη κι αν πρόκειται για διασυνοριακές συναλλαγές μεγάλων ποσών
Χωρίς όρια	Οπουδήποτε Σε οποιονδήποτε Οποιοδήποτε ποσό
Υποδιαιρέσεις	Τα περισσότερα κρυπτονομίσματα έχουν έως και χιλιάδες υποδιαιρέσεις

3. ΟΙΚΟΝΟΜΙΑ



Δεν υπάρχει πληθωρισμός

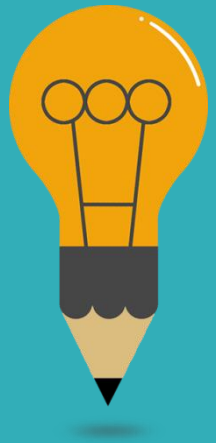
Τα περισσότερα κρυπτονομίσματα έχουν ελεγχόμενο και προγραμματισμένο ρυθμό παραγωγής, ο οποίος στοχεύει στην αποφυγή φαινομένων πληθωρισμού

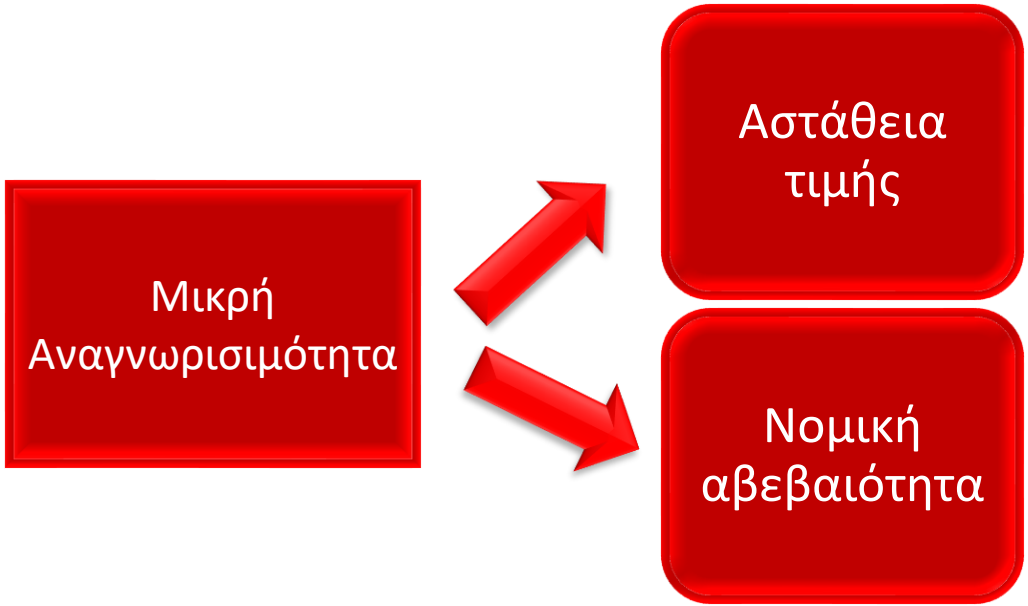
Νομίσματα χωρίς εθνικότητα

Μπορούν να αναγνωριστούν σε οποιοδήποτε μέρος του πλανήτη καθώς το Διαδίκτυο δεν έχει σύνορα. Εξυπηρετούν μονάχα τους συναλλασσόμενους και την εξέλιξη του διεθνούς εμπορίου

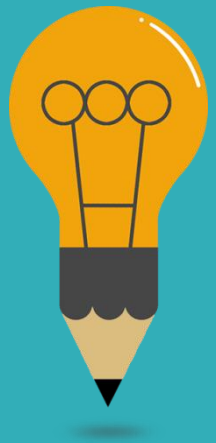
Μειονεκτήματα & Κίνδυνοι

1. Κλίμα αβεβαιότητας





2. Λειτουργία



- **Κατάλληλα για εγκληματική δραστηριότητα** → Ανωνυμία και αποκέντρωση αποτελούν κάποια από τα χαρακτηριστικά που επιθυμούν οι εγκληματίες
- **Στόχος hackers** → Η αποκλειστική ψηφιακή τους μορφή τα καθιστά στόχο για hackers, οι οποίοι επιθυμούν να κλέψουν τα ψηφιακά πορτοφόλια των χρηστών ή να εκμεταλλευτούν πιθανά λάθη στον ανοικτό κώδικα
- **Μη αντιστρέψιμες συναλλαγές** → Οι ολοκληρωμένες συναλλαγές δεν έχουν επιστροφή και δεν αντιστρέφονται. Ενδεχόμενο λάθος δεν μπορεί να διορθωθεί
- **Η θεωρία της επίθεσης του 51%**

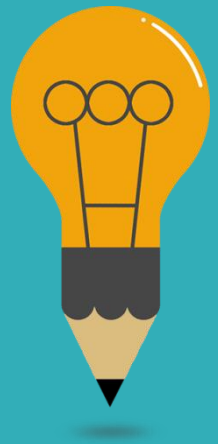
Η θεωρία της επίθεσης του 51%

Η θεωρία αυτή αναφέρει ότι, εάν μία ομάδα κακόβουλων miners μπορέσουν να αποκτήσουν την απαραίτητη υπολογιστική ισχύ στο δίκτυο (αν και αποδεδειγμένα είναι οικονομικά ασύμφορο), θα είναι σε θέση να ελέγχουν ποιες συναλλαγές επιβεβαιώνονται και ποιες όχι,
και συνεπώς τη συνολική πορεία του νομίσματος

3. Ψηφιακή μορφή

Απαραίτητος ο Η/Υ

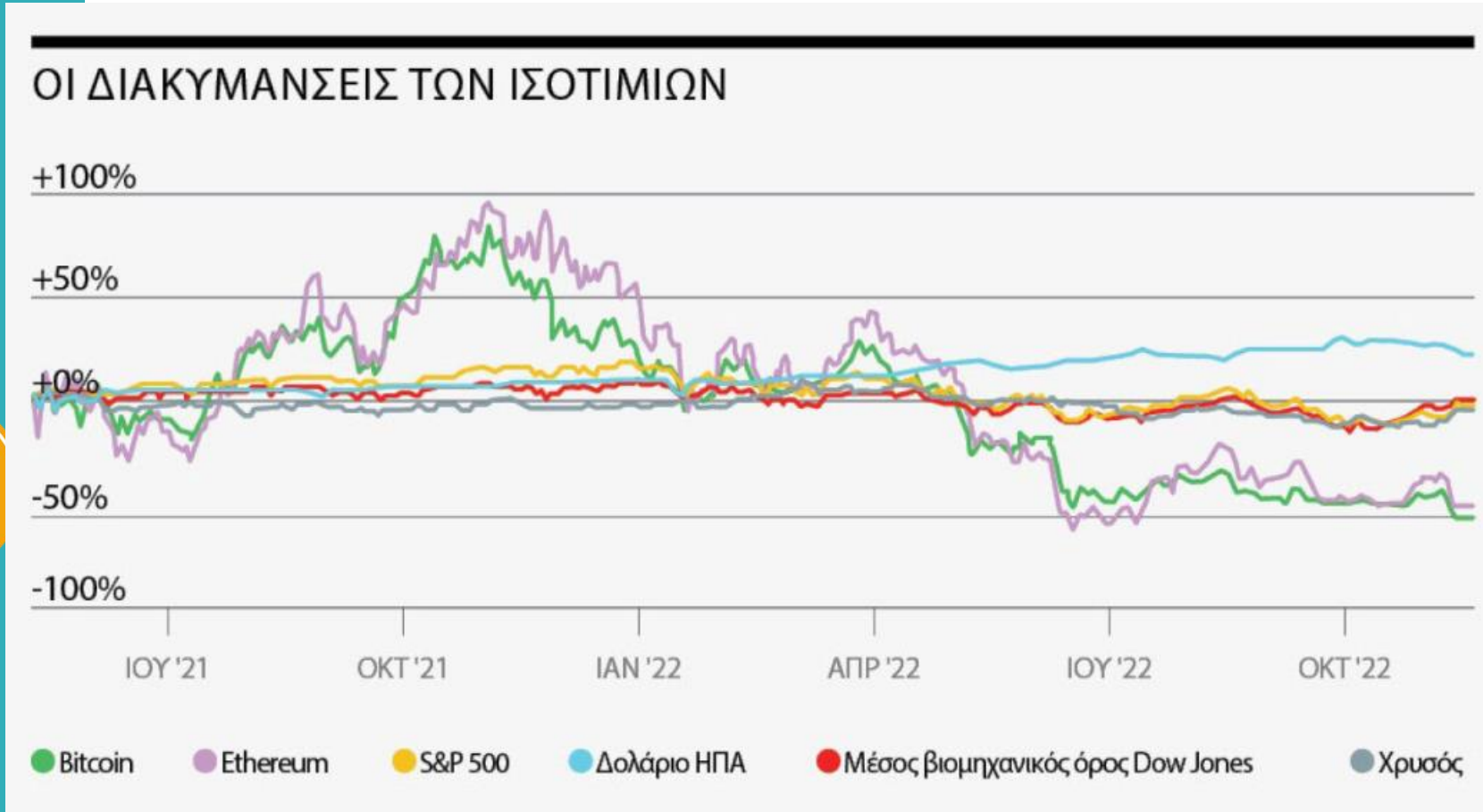
Απαραίτητες γνώσεις πληροφορικής και των τεχνικών στοιχείων που χαρακτηρίζουν το εκάστοτε νόμισμα



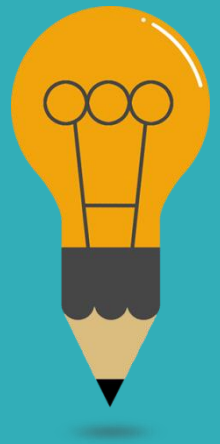
Τα 10 κορυφαία κρυπτονομίσματα με βάση την κεφαλαιοποίηση της αγοράς (27/10/23)

1	**Bitcoin** [BTC]	€32,283	-1,11%	630,32 Δις
2	**Ethereum** [ETH]	€1,692.1	-3,03%	203,48 Δις
3	**Tether USDt** [USDT]	€0.94675	-0,02%	80,01 Δις
4	**BNB** [BNB]	€212.7	-0,29%	32,27 Δις
5	**XRP** [XRP]	€0.52189	-1,86%	27,95 Δις
6	**USDC** [USDC]	€0.94661	-0,02%	23,77 Δις
7	**Solana** [SOL]	€31.074	1,89%	13,02 Δις
8	**Cardano** [ADA]	€0.27072	-2,58%	9,54 Δις
9	**Dogecoin** [DOGE]	€0.067236	-0,87%	9,52 Δις
10	**TRON** [TRX]	€0.088247	-0,43%	7,84 Δις

Οι διακυμάνσεις Ισοτιμιών (Bitcoin, Ethereum, S&P 500, Δολάριο ΗΠΑ, Dow Jones, Χρυσός)

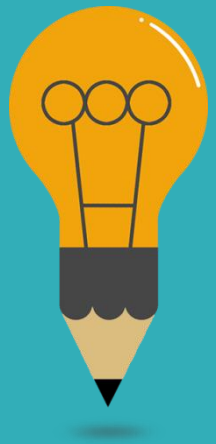


Βασικοί πυλώνες των κρυπτονομισμάτων:



- Κρυπτογραφία
- Ιδιωτικότητα
- Αποκέντρωση

Βασικές διαφορές μεταξύ των κρυπτονομισμάτων:



- Πρωτόκολλα – Κώδικας
- Αναγνώριση – Αξία
- Μετατρεψιμότητα σε fiat χρήμα

Bitcoin (μέρος Ι)

Το νόμισμα που έφερε επανάσταση στον κόσμο των κρυπτονομισμάτων

Το Bitcoin είναι το πιο γνωστό κρυπτονόμισμα του κόσμου

Η αξία μόνο του Bitcoin αντιστοιχεί στο 50% της συνολικής αξίας της αγοράς κρυπτονομισμάτων!

Τι είναι το Bitcoin;

Το Bitcoin είναι το **πρώτο πλήρως αποκεντρωμένο** ψηφιακό νόμισμα. Η ονομασία του προέρχεται από την ένωση των λέξεων: ***bit***, που είναι η βασική μονάδα πληροφορίας στον κλάδο της πληροφορικής και ***coin*** που σημαίνει νόμισμα

Τι είναι το Bitcoin;

Είναι το πρώτο αποκεντρωμένο δίκτυο ανταλλαγής ψηφιακού χρήματος. Οι μεταφορές χρήματος γίνονται μεταξύ ομότιμων και δεν υπάρχει μία κεντρική αρχή που μπορεί αυθαίρετα να εκδόσει νέα Bitcoins. Ο κάθε χρήστης μπορεί απλά να συμμετέχει στις συναλλαγές ή να συμβάλλει στην παραγωγή νέων Bitcoins, με την αντίστοιχη υπολογιστική ισχύ που θα συνεισφέρει στο δίκτυο του Bitcoin

Τι είναι το Bitcoin;

Peer-to-peer:

Είναι ένα **peer-to-peer** (P2P) δίκτυο, που σημαίνει ότι οι συναλλαγές πραγματοποιούνται **απευθείας μεταξύ των χρηστών, χωρίς μεσάζοντα.** Αυτό σημαίνει ότι είναι το πρώτο εντελώς ανοικτό χρηματοπιστωτικό δίκτυο του κόσμου

Ένα **P2P** δίκτυο αποτελείται από ένα σύνολο υπολογιστών (**κόμβων**), οι οποίοι είναι συνδεδεμένοι μεταξύ τους μέσω Διαδικτύου. Όλοι οι κόμβοι του δικτύου έχουν **ίσα δικαιώματα**, καθώς μοιράζονται τους πόρους τους (αποθηκευτικός χώρος, υπολογιστική ισχύς, εύρος ζώνης) ισοδύναμα. Τα αρχεία μπορούν να μοιράζονται απευθείας μέσω του δικτύου στο οποίο είναι συνδεδεμένα αυτά τα συστήματα. Δεν απαιτείται κεντρικός διακομιστής γι’ αυτό

Τι είναι το Bitcoin;

Βασίζεται σε **λογισμικό ανοιχτού κώδικα**, που σημαίνει ότι ο πηγαίος κώδικας του λογισμικού είναι δημόσιος και διαθέσιμος σε όποιον επιθυμεί να ελέγξει τις λεπτομέρειες της λειτουργίας του.

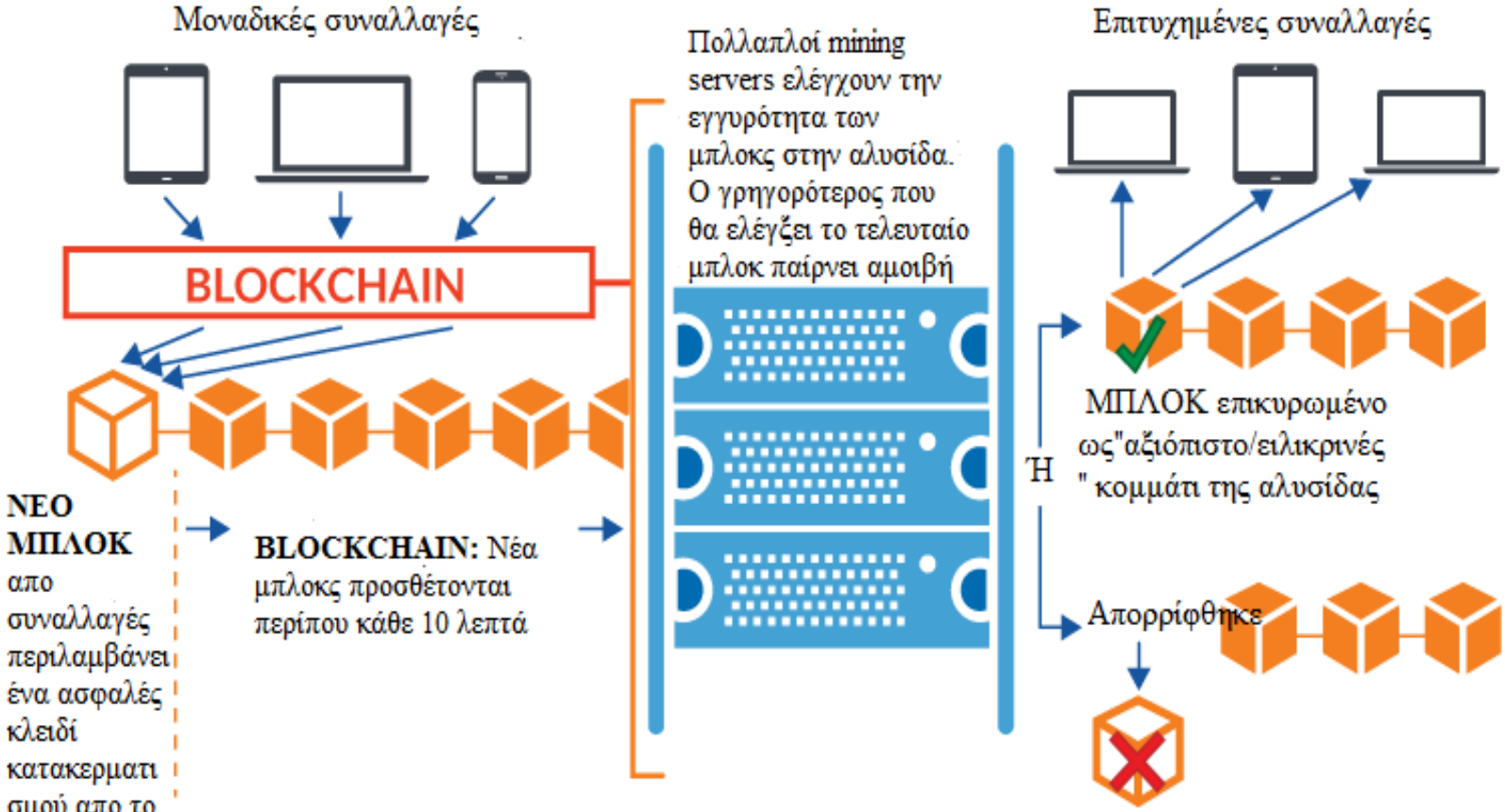
Η αρχή αυτή επιτρέπει σε οποιονδήποτε την ελεύθερη και δωρεάν αντιγραφή και ανάπτυξη δικού του λογισμικού βασισμένου στο υπάρχον

Total Bitcoins over time

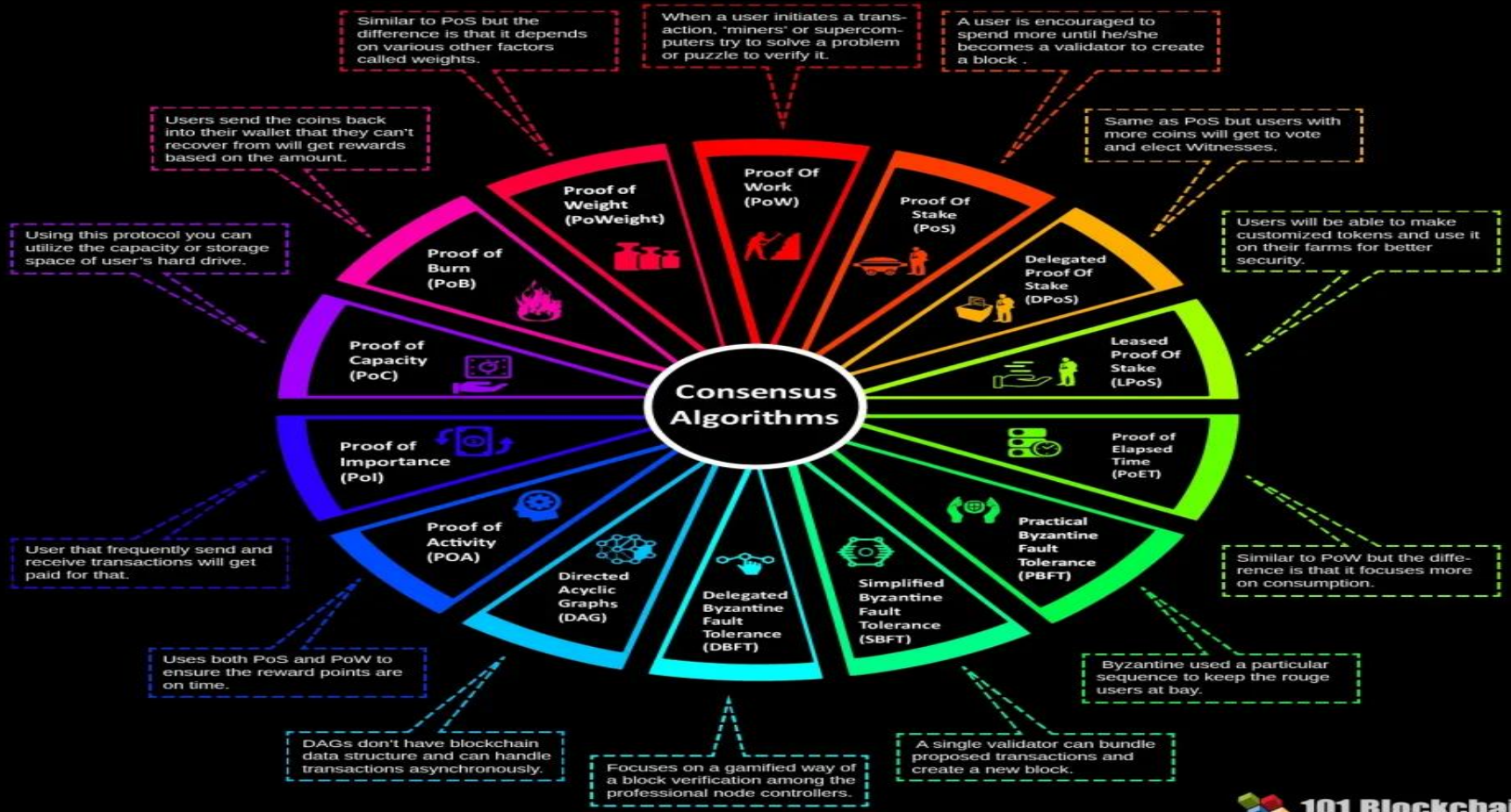
Total Coins (millions)

0 3 6 9 12 15 18 21

2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033


Μοναδικές συναλλαγές
BLOCKCHAIN
ΝΕΟ ΜΠΛΟΚ απο συναλλαγές περιλαμβάνει ένα ασφαλές κλειδί κατακερματισμού απο το προηγούμενο μπλοκ
BLOCKCHAIN: Νέα μπλοκς προσθέτονται περίπου κάθε 10 λεπτά
Πολλαπλοί mining servers ελέγχουν την εγγυρότητα των μπλοκς στην αλυσίδα. Ο γρηγορότερος που θα ελέγξει το τελευταίο μπλοκ παίρνει αμοιβή
Η
Επιτυχημένες συναλλαγές
ΜΠΛΟΚ επικυρωμένο ως"αξιόπιστο/ειλικρινές " κομμάτι της αλυσίδας
Απορρίφθηκε

Different Types of Consensus Algorithms



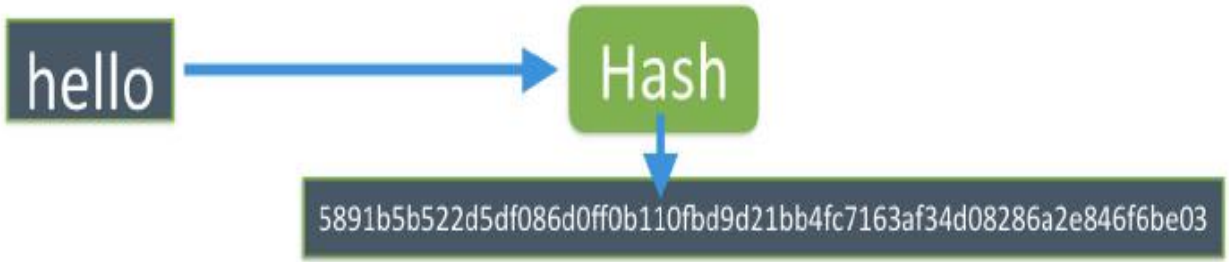
Μηχανισμός συναίνεσης Bitcoin: Proof of Work (PoW)

Για να δημιουργηθεί ένα νέο block, οι miners σε ένα δίκτυο PoW ανταγωνίζονται ο ένας τον άλλον για να λύσουν πολύπλοκα μαθηματικά προβλήματα σε μία διαδικασία που ονομάζεται **hashing**

Το **hash function** είναι μία **μονόδρομη** συνάρτηση: δεν μπορεί να χρησιμοποιηθεί για τη λήψη των αρχικών δεδομένων, μόνο για να ελεγχθεί ότι τα δεδομένα που δημιούργησαν το συγκεκριμένο hash ταιριάζουν με τα αρχικά δεδομένα

Συνάρτηση Κατακερματισμού

Hash
(sha256)



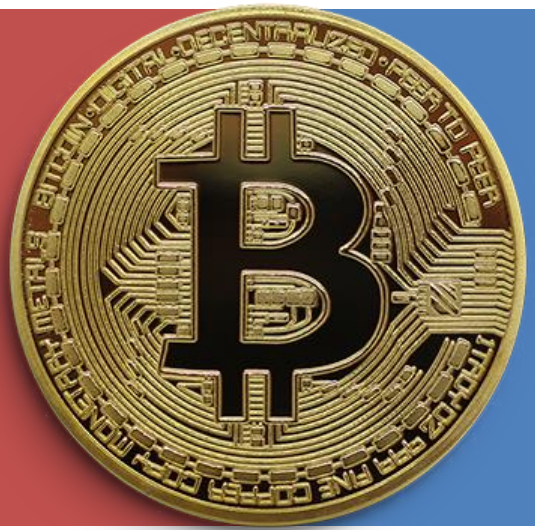
Το output είναι ένα σταθερού μήκους σύνολο από αριθμούς και χαρακτήρες

Το μέγεθός του είναι 256-bit, επομένως οι διαφορετικές τιμές είναι 2^{256}, δηλ. $1,158 \times 10^{77}$

Μηχανισμός συναίνεσης Bitcoin: Proof of Work (PoW)

Στόχος κάθε miner είναι να βρει πρώτος το σωστό hash, επειδή θα είναι αυτός που μπορεί να ενημερώσει το blockchain, δηλαδή να προσθέσει το νέο block και να λάβει ανταμοιβή με τη μορφή Bitcoins

Ο λόγος που το PoW λειτουργεί καλά είναι επειδή η εύρεση του hash είναι δύσκολη, αλλά η επαλήθευση όχι. Η διαδικασία είναι πολύ δύσκολη για να αποτρέψει τον έλεγχο των συναλλαγών. Μόλις όμως βρεθεί ένα hash, είναι εύκολο για τους άλλους miners να το ελέγξουν



Πλεονεκτήματα

Ελευθερία

Με το Bitcoin μπορεί ο καθένας να λάβει ή να αποστείλει ένα ποσό ανεξαρτήτως μεγέθους άμεσα και σε οποιοδήποτε σημείο του κόσμου υπάρχει σύνδεση στο Internet, οποιαδήποτε στιγμή

Ταχύτητα Συναλλαγών & Διεθνής Φύση

Οι συναλλαγές σε Bitcoin συμβαίνουν άμεσα και ανακοινώνονται ταυτόχρονα σε όλο το δίκτυο ανά τον πλανήτη. Αυτό δεν απαιτεί άλλες υποδομές πέρα από κάποια μορφή του δωρεάν λογισμικού σε υπολογιστή ή σε smartphone και σύνδεση στο Διαδίκτυο.
Η επιβεβαίωση μιας συναλλαγής στο Bitcoin απαιτεί κατά μέσο όρο 10 λεπτά

Εξαιρετικά χαμηλό κόστος συναλλαγών

Κάθε συναλλαγή με Bitcoin έχει τέλη αλλά είναι χαμηλά και δεν επηρεάζονται από την αξία που μεταφέρει κανείς. Μπορώ να στείλω χρήματα αξίας ενός εκατομμυρίου ευρώ από την Ελλάδα στη Νιγηρία, η συναλλαγή να πραγματοποιηθεί σε μερικά λεπτά και το κόστος μου να είναι ίσο με μερικά λεπτά του ευρώ. Το κόστος συναλλαγής είναι προαιρετικό, αν δεν υπάρχει βιασύνη επιβεβαίωσης της συναλλαγής

Ιδιωτικότητα συναλλαγών (Ι)

Κάθε χρήστης μπορεί να δημιουργήσει, μέσω του λογισμικού, σχεδόν απεριόριστο αριθμό διευθύνσεων μέσω των οποίων θα εκτελεί τις συναλλαγές του. Αυτές οι διευθύνσεις είναι ψευδώνυμες, δεν έχουν δηλαδή κάποια άμεση σχέση με τα πραγματικά στοιχεία ή την τοποθεσία του χρήστη. Με αυτόν τον τρόπο μπορεί ο χρήστης να διατηρήσει την ιδιωτικότητά του απεμπλέκοντας τις συναλλαγές του από τα προσωπικά του στοιχεία

Ιδιωτικότητα συναλλαγών (II)

Αυτό δεν συνεπάγεται εξ' ορισμού ανωνυμία συναλλαγών καθώς όλες οι συναλλαγές δημοσιεύονται και έστω και μία συναλλαγή να έχει γνωστό (δημόσιο) αποδέκτη, ίσως μπορεί να εξαχθεί από συμπληρωματικά στοιχεία η ταυτότητα του χρήστη. **Αυτός είναι και ο κύριος λόγος για τον οποίο η χρήση Bitcoins δεν ενδείκνυται για συναλλαγές παράνομων δραστηριοτήτων**, καθώς το ίχνος των συναλλαγών όχι μόνο δεν διαγράφεται με το πέρασμα του χρόνου, αλλά παραμένει διαθέσιμο για εξέταση απ' όλους και για πάντα

Έλεγχος από τον χρήστη

Ο χρήστης είναι ο μόνος που έχει τη δυνατότητα να εκτελέσει συναλλαγές με τα Bitcoins του και εφόσον δεν έχει παραχωρήσει αυτό το δικαίωμα και έχει προστατεύσει την πρόσβαση σε αυτά, είναι πρακτικά αδύνατο να κλαπούν από τρίτους

Διαφάνεια Συναλλαγών/Κανόνων

Όλοι οι κανόνες και οι συναλλαγές που έχουν εκτελεστεί ποτέ στο δίκτυο είναι δημόσια διαθέσιμες και διαφανείς. Έτσι, ο οποιοσδήποτε μπορεί να εξετάσει οποιαδήποτε διεύθυνση και να δει τις προηγούμενες συναλλαγές που έχουν εκτελεστεί με αυτήν, το πλήθος των Bitcoins που έχουν μετακινηθεί, όπως και το που έχουν σταλεί

Φορητότητα & αντίγραφα ασφαλείας

Ανεξάρτητα από το πλήθος τους, τα Bitcoins και τα «πορτοφόλια» αποθήκευσης ή οι κωδικοί πρόσβασης σε αυτά είναι ουσιαστικά πάρα πολύ μικρά σε μέγεθος και μπορούν να μεταφερθούν εύκολα, να καταγραφούν σε χαρτί, ακόμη και να απομνημονευθούν. Βέβαια, αν παραβιαστεί οποιοδήποτε από τα αντίγραφα, τα υπόλοιπα είναι επίσης παραβιασμένα

Συναινετική φύση χρήσης και αλλαγών

Η αλλαγή οποιουδήποτε χαρακτηριστικού του λογισμικού ή των κανόνων του, έχει ουσιαστικά εφαρμογή μόνο όταν τις δεχτεί η κοινότητα που απαρτίζει το δίκτυο. Με αυτόν τον τρόπο αποφεύγονται κακόβουλες αλλαγές που θα μπορούσαν να αλλάξουν θεμελιωδώς το λογισμικό, αλλά και μεγάλη ευελιξία και ταχύτητα αντίδρασης σε περίπτωση εντοπισμού σφαλμάτων ή απρόβλεπτων αστοχιών κατά τη λειτουργία

Αποκεντρωμένη Φύση

Δεν απαιτείται καμία κεντρική αρχή ελέγχου ή επιβεβαίωσης. Κάθε κόμβος του δικτύου το ενισχύει περαιτέρω, αλλά αν προσβληθεί με κάποιο τρόπο, η λειτουργία του συνολικού δικτύου δεν επηρεάζεται ανάλογα. Ο μόνος τρόπος να σταματήσει να δουλεύει το δίκτυο είναι να αποκοπούν όλοι οι υπολογιστές του δικτύου μεταξύ τους, με άλλα λόγια να κοπεί το Διαδίκτυο σε όλο τον πλανήτη, κάτι που σήμερα είναι πέρα από τις δυνάμεις οποιουδήποτε

Μη αντιστρέψιμη φύση

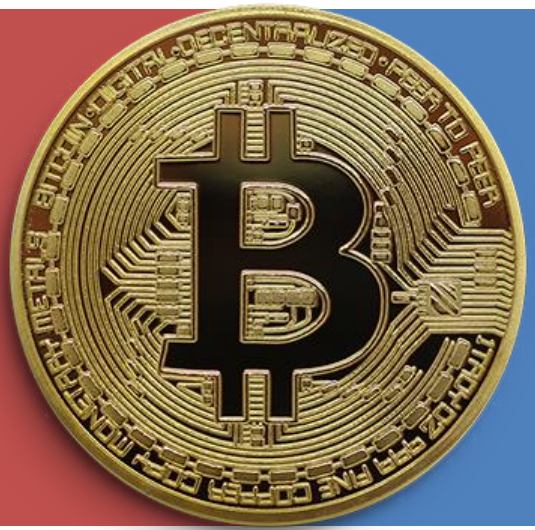
Όλες οι συναλλαγές με Bitcoin είναι τελικές και μη αντιστρέψιμες. Αυτό έχει το επιπλέον πλεονέκτημα προς όσους διαθέτουν προϊόντα για Bitcoin, ότι δεν είναι δυνατόν να ανακληθούν συναλλαγές. Συνεπώς, δίνει επιπλέον κίνητρα σε επιχειρήσεις να προσφέρουν τα προϊόντα τους σε χαμηλότερες τιμές, εξαιτίας της άμεσης και αμετάκλητης πληρωμής

Υποδιαιρέσεις

Κάθε Bitcoin είναι υποδιαιρέσιμο έως και 8 δεκαδικά ψηφία (0,00000001) που ονομάζονται Satoshi, επιτρέποντας μικροσυναλλαγές που δεν είναι δυνατές με άλλα μέσα ή συμβατικά νομίσματα. Η προσθήκη περισσότερων ακόμη δεκαδικών επαφίεται στη συναίνεση του δικτύου, αν αυτό χρειαστεί στο μέλλον

Αποπληθωριστικό νόμισμα

Ο πληθωρισμός του Bitcoin είναι γνωστός εκ των προτέρων και είναι προγραμματισμένο να μειώνεται με το πέρασμα του χρόνου με σκοπό κάποια στιγμή να μηδενιστεί



Ρίσκα/Κίνδυνοι & Μειονεκτήματα

Δεν είναι ευρέως γνωστό και αποδεκτό

Παγκοσμίως μέχρι και σήμερα υπάρχει αμέτρητος κόσμος που δεν γνωρίζει τον τρόπο χρήσης του ή ακόμη και την ίδια την ύπαρξή του. Ταυτόχρονα, αν και με αυξητικές τάσεις, είναι λίγοι οι επίσημοι φορείς και οργανισμοί που το αποδέχονται ως μέσο συναλλαγής και αποπληρωμής

Διακύμανση ισοτιμίας

Καθώς το Bitcoin δεν έχει κάποια κεντρική αρχή να παρεμβαίνει στις διακυμάνσεις μεταξύ προσφοράς και ζήτησης -όπως συμβαίνει με τα κρατικά νομίσματα- είναι επιρρεπές σε μεγαλύτερες διακυμάνσεις της ισοτιμίας του με τα περισσότερα νομίσματα

Βρίσκεται σε συνεχείς μεταβολές και εξελίξεις

Όπως το Internet με τη δημιουργία του το 1991, έτσι και τώρα το Bitcoin σε επίπεδο λογισμικού και υπηρεσιών συνεχώς εξελίσσεται και αλλάζει. Το γεγονός αυτό υποδηλώνει ότι το δίκτυο του Bitcoin είναι ακόμη σε διαδικασία ωρίμανσης με αποτέλεσμα να δημιουργεί αβεβαιότητα για το τι μέλλει γενέσθαι και ανησυχία για πιθανούς κινδύνους

Ασφάλεια δικτύου

Το νεαρό της ηλικίας του δικτύου δημιουργεί ανησυχίες για πιθανούς κινδύνους που σχετίζονται με:

1. Έλεγχο μεγάλου μέρος του δικτύου από μία κακόβουλη οντότητα (51%)

2. Παραβίαση των αλγόριθμων κρυπτογράφησης του δικτύου

3. Αντικατάσταση από κάποιο λογισμικό ανώτερης σχεδίασης και μεγαλύτερου δικτύου από το υπάρχον, με ό,τι αυτό συνεπάγεται

Ασαφές νομικό πλαίσιο

Παρόλο που η Ευρωπαϊκή νομοθεσία έχει λάβει μέτρα για τη θέσπιση όρων σε ό,τι αφορά κεντρικά ελεγχόμενα ή εκδιδόμενα ψηφιακά νομίσματα, η αποκεντρωμένη φύση του Bitcoin, όπως και άλλα από τα χαρακτηριστικά του, εισάγουν νέες παραμέτρους που δεν έχουν ακόμη εξεταστεί σε όλο τους το εύρος σε καμία χώρα

Απώλεια ιδιωτικών κλειδιών

Το μόνο που χρειάζεται ένας κακόβουλος χρήστης ώστε να αποκτήσει τον έλεγχο των Bitcoins ενός άλλου χρήστη, είναι η γνώση των ιδιωτικών κλειδιών ή πιο απλά των προσωπικών κωδικών του. Συνεπώς, κάθε χρήστης έχει την απόλυτη ευθύνη για την προστασία των δικών του Bitcoins

Μη αντιστρέψιμες συναλλαγές

Οι ολοκληρωμένες συναλλαγές δεν έχουν επιστροφή και δεν αντιστρέφονται. Ενδεχόμενο λάθος δεν μπορεί να διορθωθεί

Λίγες Εμπορικές Συναλλαγές

Ένα πολύ μικρό ποσοστό των συναλλαγών που γίνονται στο Bitcoin αφορούν εμπορικές συναλλαγές. Οι περισσότερες συναλλαγές γίνονται για επενδύσεις ή για αποθήκευση αξίας (όπως στον χρυσό). Αυτό σημαίνει ότι το νόμισμα βρίσκεται ακόμη σε αρχικά στάδια

Ιστορική Αναδρομή

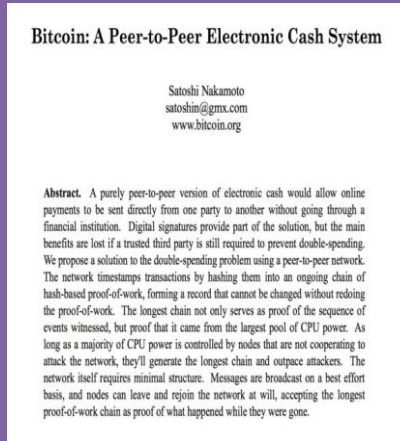
2008

•Στις 18 Αυγούστου δημιουργήθηκε η ηλεκτρονική διεύθυνση **www.bitcoin.org** (η διεύθυνση παραμένει ενεργή)

•Τη διεύθυνση κατοχύρωσαν οι Neal King, Vladimir Oksman και Charles Bry, αρνούμενοι ωστόσο οποιαδήποτε σχέση με τον δημιουργό του νομίσματος, τον πασίγνωστο και συνάμα αφανή **Satoshi Nakamoto**

2008

Στις 31 Οκτωβρίου δημοσιεύθηκε από τον **Satoshi Nakamoto** το μανιφέστο του Bitcoin μέσω μιας κρυπτογραφημένης λίστας αλληλογραφίας, εντός της οποίας περιγράφεται η λογική πίσω από το νέο ψηφιακό νόμισμα, η λειτουργία του, καθώς και η επίλυση σε ένα πρόβλημα που αντιμετώπιζαν όλα τα ψηφιακά νομίσματα έως τότε (**double spending**), γεγονός που κατέστησε άμεσα το Bitcoin πρωτοποριακό



Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

2009

•Στις 3 Ιανουαρίου δημιουργήθηκε το πρώτο μπλοκ (**block 0**) που περιείχε τα πρώτα 50 Bitcoins

•Λίγες μέρες αργότερα κυκλοφόρησε η **πρώτη έκδοση του λογισμικού** που απαιτείται για την παραγωγή Bitcoins

•Στις 12 Ιανουαρίου πραγματοποιήθηκε η πρώτη συναλλαγή σε Bitcoin ανάμεσα στον Satoshi Nakamoto και τον Hal Finney (ένα από τα πρώτα μέλη των Cypherpunks)

•Τον Οκτώβριο, ανακοινώθηκε η πρώτη ισοτιμία του Bitcoin (***1 δολάριο = 1.309,03 BTC***)

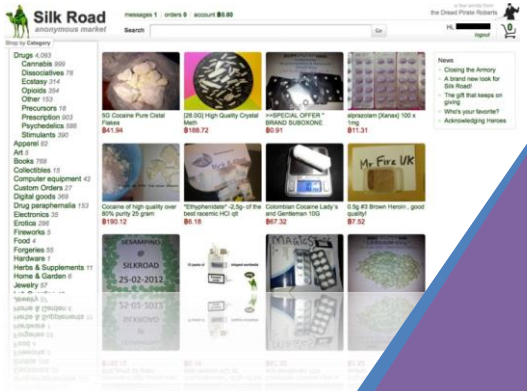
2010

•Η πρώτη συναλλαγή στον πραγματικό κόσμο έλαβε χώρα στις 22 Μαΐου, καθώς ο προγραμματιστής Laszlo Hanyecz διέθεσε 10.000 Bitcoins για να αγοράσει 2 πίτσες αξίας $ 25 !!!

•Στις 17 Ιουλίου δημιουργήθηκε το μεγαλύτερο ανταλλακτήριο Bitcoin με την ονομασία **Mt. Gox**

•Τον Αύγουστο, χάκερς εκμεταλλεύονται αδυναμία του λογισμικού και παράγουν πολύ μεγάλο αριθμό Bitcoins που στέλνουν σε δύο διευθύνσεις στο δίκτυο. Εντοπίζονται, η συναλλαγή διαγράφεται και παράγεται μία βελτιωμένη έκδοση του λογισμικού

2011



•Τον Ιανουάριο, ιδρύεται το **Silk Road**, site για διακίνηση ναρκωτικών και άλλες παράνομες συναλλαγές. Τον επόμενο μήνα, η αξία του Bitcoin εκτοξεύεται (1 BTC = 1 δολάριο). Τον Ιούνιο, η τιμή του φθάνει τα $ 31!

•Τον Ιούνιο, λαμβάνει χώρα σοβαρή παραβίαση ασφάλειας στο **Mt. Gox**

•Ένα μήνα αργότερα, το **Bitomat**, το τρίτο μεγαλύτερο ανταλλακτήριο εκείνη την εποχή, χακάρεται με αποτέλεσμα την απώλεια 17.000 Bitcoins

2012

•Καταγράφονται πολλές περιπτώσεις παραβίασης ανταλλακτηρίων Bitcoin, όπως για παράδειγμα, το **Bitcoinica** και το **Bitfloor**

•Τον Νοέμβριο, η ανταμοιβή για την εξόρυξη ενός νέου μπλοκ μειώνεται στο μισό (από τα 50 στα 25 Bitcoins)

2013

•Τον Μάρτιο, το Δίκτυο Δίωξης Οικονομικού Εγκλήματος των ΗΠΑ εκδίδει για πρώτη φορά οδηγίες για τους χρήστες του Bitcoin

•Τον ίδιο μήνα, η κεφαλαιοποίηση της αγοράς Bitcoin ξεπερνάει το **1 δις δολάρια**

•Στις 11 Αυγούστου αποκαλύπτεται ένα σφάλμα στο λειτουργικό σύστημα Android που βοήθησε να κλαπούν Bitcoins από ψηφιακά πορτοφόλια που δημιουργήθηκαν μέσω Android apps

•Τον Οκτώβριο, το FBI συνέλαβε τον ιδρυτή του **Silk Road**, **Ross Ulbricht** και του κατάσχεσε περίπου 26.000 Bitcoins

2014

•Τον Ιανουάριο, η **Overstock.com** γίνεται η πρώτη μεγάλη online εταιρία λιανικής που δέχεται Bitcoins

•Τον Φεβρουάριο, το **Mt. Gox** (διαχειριζόταν το 70% του παγκόσμιου εμπορίου σε Bitcoin) οδηγείται σε χρεοκοπία, έχοντας χάσει $ 390 εκατομμύρια

•Τον Ιούλιο, η **Ευρωπαϊκή Τραπεζική Αρχή** αναφέρει ότι τα ανταλλακτήρια ψηφιακών νομισμάτων πρέπει να συμμορφώνονται στις απαιτήσεις για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες

2015

•Το Δίκτυο Δίωξης Οικονομικού Εγκλήματος των ΗΠΑ θεσπίζει κανόνες για τα “αποκεντρωμένα ψηφιακά νομίσματα”, που κατατάσσουν τους εξορύκτες Bitcoin σε **Επιχειρήσεις Χρηματοοικονομικών Υπηρεσιών** που υπόκεινται σε νομικές υποχρεώσεις

•Χάκερς κλέβουν Bitcoins αξίας $ 2,1 εκατομμυρίων από το Κινέζικο ανταλλακτήριο **Bter** και $ 5,1 εκατομμυρίων από το Σλοβένικο ανταλλακτήριο **Bitstamp**

2016

•Τον Ιούλιο, η ανταμοιβή για την εξόρυξη ενός νέου μπλοκ μειώνεται στο μισό (στα 12,5 Bitcoins)

•Χάκερς κλέβουν Bitcoins αξίας $ 72 εκατομμυρίων από το ανταλλακτήριο **Bitfinex** στο Hong Kong. Ο CEO του Αμερικανικού ανταλλακτηρίου **Cryptsy** κατηγορείται ότι έκλεψε Bitcoins αξίας $ 3,3 εκατομμυρίων

2017

•Στις 2 Μαρτίου, για πρώτη φορά, η τιμή του Bitcoin ξεπερνάει την τιμή μιας ουγγιάς χρυσού

•Στις 1 Αυγούστου η αλυσίδα μπλοκ του Bitcoin χωρίζεται στα δύο: την **αλυσίδα Bitcoin (BTC)** με όριο στο μέγεθος μπλοκ 1 MB και την **αλυσίδα Bitcoin Cash (BCH)** με όριο στο μέγεθος μπλοκ 8 MB

2020

•Τον Μάιο, η ανταμοιβή για την εξόρυξη ενός νέου μπλοκ μειώνεται και πάλι στο μισό της προηγούμενης ανταμοιβής (στα 6,25 Bitcoins)

2021

•Στις 19 Φεβρουαρίου η κεφαλαιοποίηση της αγοράς Bitcoin ξεπερνάει για πρώτη φορά το **1 τρις δολάρια**

•Στις 7 Σεπτεμβρίου το **El Salvador** γίνεται η πρώτη χώρα του κόσμου που αναγνωρίζει το Bitcoin ως νόμιμο χρήμα

•Στις 10 Νοεμβρίου το Bitcoin φθάνει τη μέγιστη τιμή του μέχρι σήμερα (**$ 68.789,63**)

2022

•Τον Μάρτιο, η πόλη **Lugano της Ελβετίας** καθιερώνει το Bitcoin ως “*de facto*” νόμιμο χρήμα. Εκτός του ότι επιτρέπει τα κρυπτονομίσματα για την πληρωμή φόρων, στοχεύει να κάνει όλες τις επιχειρήσεις της να χρησιμοποιούν τα κρυπτονομίσματα για τις καθημερινές τους συναλλαγές

•Τον Νοέμβριο, το ανταλλακτήριο-αυτοκρατορία κρυπτονομισμάτων **FTX** του **Sam Bankman-Fried** καταρρέει με αποτέλεσμα να χαθούν δισεκατομμύρια δολάρια

2023

•Τον Απρίλιο, ανακοινώνεται ότι το πτωχευμένο ανταλλακτήριο **FTX** ανέκτησε περιουσιακά στοιχεία αξίας $ 7,3 δις

•Η ταυτόχρονη χρεοκοπία των **Signature Bank** και **Silvergate** (κύριες τράπεζες για την αγορά κρυπτονομισμάτων), καθώς επίσης της **Silicon Valley Bank** (της μεγαλύτερης τράπεζας για *start-ups* τεχνολογίας), αντί να οδηγήσει σε πτώση τιμών, πυροδότησε ένα ράλι στις τιμές των κρυπτονομισμάτων (Bitcoin και Ether), λόγω της απόφασης της Ομοσπονδιακής Κυβέρνησης να εγγυηθεί όλες τις καταθέσεις των πελατών των SVB και Signature Bank