

Monero

Αργυροπούλου Μαρία : Π18011

Στεργίου Χρήστος : Π18147

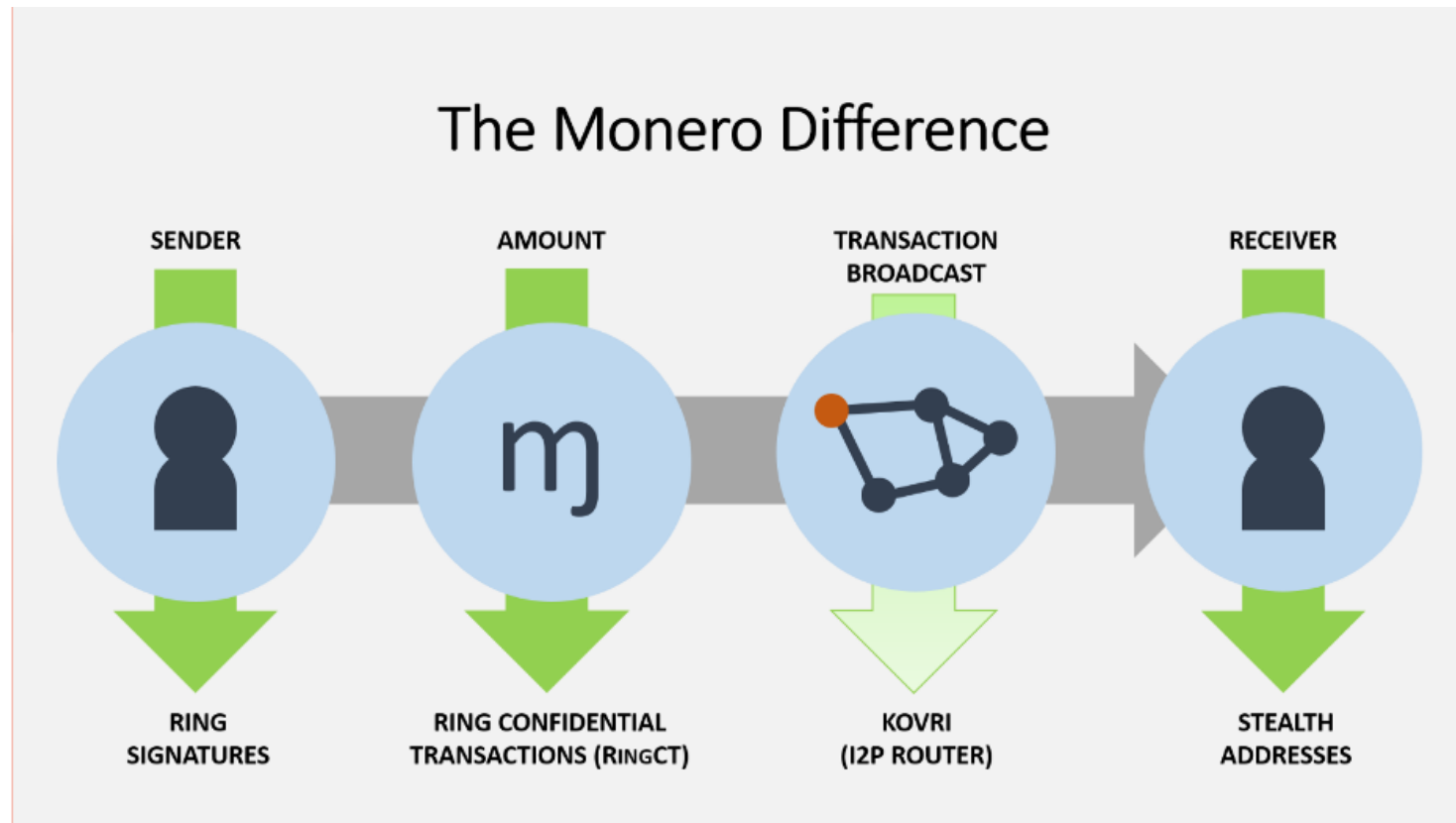


Εισαγωγή

-
- Το Monero αποτελεί ένα κρυπτονόμισμα με έμφαση στην ιδιωτικότητα και το απόρρητο. Αποσκοπεί στη διευκόλυνση των συναλλαγών των χρηστών του και επιδιώκει την εξάλειψη περιστατικών διακρίσεων με βάση το εισόδημα τους, την παρακολούθηση των προσωπικών τους δραστηριοτήτων και την ταυτοποίησή τους.

Τεχνολογία απορρήτου

- Το Monero δίνει έμφαση στην ιδιωτικότητα και την ανωνυμία, με την χρήση διαφόρων μοναδικών τεχνολογιών κρυπτογράφησης που προστατεύουν την ταυτότητα των χρηστών και των δραστηριοτήτων τους



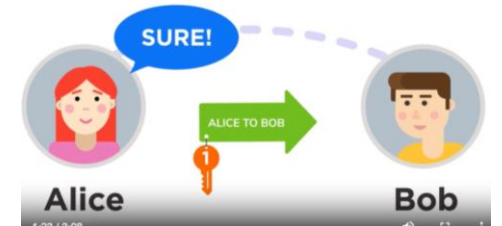


5 XMR



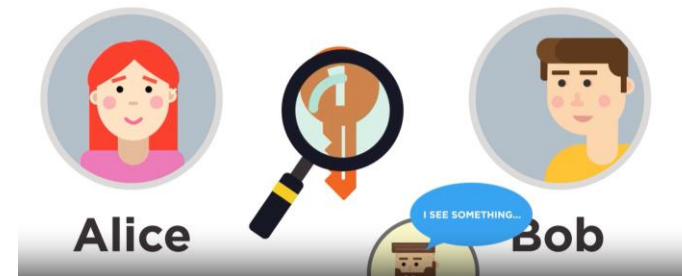
Stealth address

- Σε κάθε συναλλαγή δημιουργείται αυτόματα μια μυστική διεύθυνση, γνωστή και ως one time public key, η οποία καταγράφεται ως μέρος της συναλλαγής για να υποδείξει ποιος μπορεί να ξοδέψει αυτή την έξοδο σε μια μεταγενέστερη συναλλαγή.
- Ένας εξωτερικός παρατηρητής δεν μπορεί να δει τον αποστολέα και τον παραλήπτη των κεφαλαίων που κινούνται, ούτε να συνδέσει τις διευθύνσεις πορτοφολιών μεταξύ τους κοιτάζοντας απλώς την αλυσίδα συστοιχιών.
- Αν χρειαστεί ποτέ να αποδείξει ο αποστολέας ότι πράγματι έστειλε monero, μπορεί να επαληθεύσει ότι η πληρωμή στάλθηκε κοινοποιώντας το κλειδί συναλλαγής του (transaction key).



Stealth address

- Οι διευθύνσεις ενός πορτοφολιού Monero είναι μια συμβολοσειρά 95 χαρακτήρων που αποτελούνται από ένα δημόσιο κλειδί προβολής (public view key) και ένα δημόσιο κλειδί αποστολής (public send key).
- Για να πραγματοποιηθεί μια αποστολή, το πορτοφόλι του αποστολέα θα συνδυάσει το δημόσιο κλειδί προβολής και το δημόσιο κλειδί αποστολής του παραλήπτη καθώς και κάποια τυχαία δεδομένα για να δημιουργήσει ένα μοναδικό δημόσιο κλειδί μίας χρήσης (one time public key) για τη νέα έξοδο.
- Όλοι μπορούν να δουν το one time public key στην blockchain αλλά μόνο ο αποστολέας και ο παραλήπτης θα γνωρίζουν ποιος έστειλε monero σε ποιον.
- Η έξοδος δημιουργείται με τέτοιο τρόπο ώστε ο Bob να είναι σε θέση να εντοπίσει την έξοδο που προορίζεται γι' αυτόν σαρώνοντας την αλυσίδα μπλοκ με το ιδιωτικό κλειδί προβολής του πορτοφολιού του



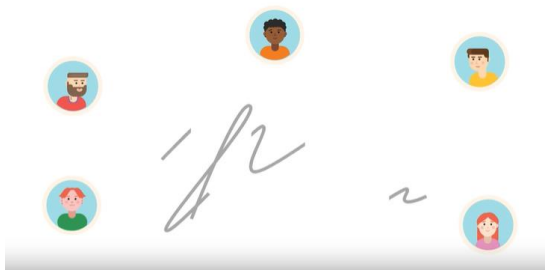


5 XMR



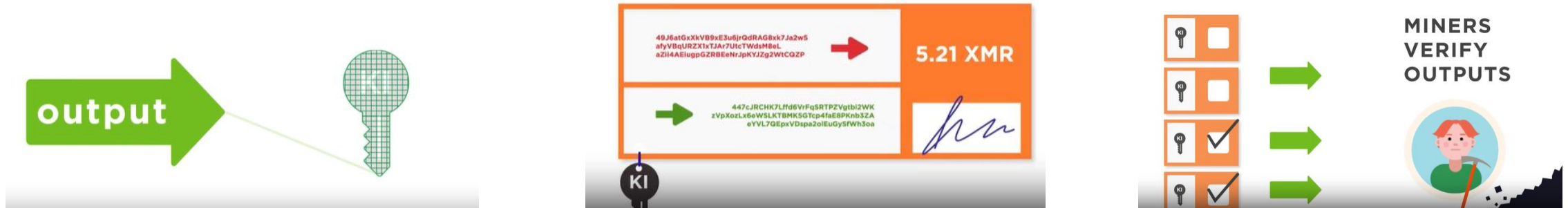
Ring signatures

- Όσο αφορά την είσοδο (input) της συναλλαγής, το απόρρητο του αποστολέα προστατεύεται με τη χρήση υπογραφών δακτυλίου (ring signatures). Είναι ένας τύπος ψηφιακής υπογραφής κατά τον οποίο μια ομάδα πιθανών υπογραφόντων συγχωνεύεται για να δημιουργήσει μια διακριτή υπογραφή που εξουσιοδοτεί μια συναλλαγή.
- Η ψηφιακή υπογραφή αποτελείται από το ιδιωτικό κλειδί του πραγματικού αποστολέα σε συνδυασμό με τα δημόσια κλειδιά άλλων χρηστών έτσι ώστε να σχηματίσει ένας δακτύλιος όπου όλα τα μέλη είναι ίσα και έγκυρα. Η πραγματική υπογραφή είναι ένα κλειδί που ξοδεύεται μια φορά και αντιστοιχεί στην έξοδο της συναλλαγής.



Ring signatures

- Αν δεν υπάρχει τρόπος για έναν τρίτο να επαληθεύσει ποια έξοδος δαπανάται τι θα εμπόδιζε κάποιον να δαπανήσει την ίδια έξοδο δύο φορές;
- Αυτό το πιθανό ζήτημα αντιμετωπίζεται με τη χρήση των key images (εικόνων των κλειδιών). Μπορεί να υπάρχει μόνο μία εικόνα κλειδιού για κάθε έξοδο στην αλυσίδα μπλοκ. Ωστόσο, λόγω των κρυπτογραφικών ιδιοτήτων της δεν είναι δυνατόν να προσδιοριστεί ποια έξοδος δημιούργησε ποια εικόνα κλειδιού. Μια λίστα όλων των χρησιμοποιημένων εικόνων κλειδιού διατηρείται στην αλυσίδα μπλοκ επιτρέποντας στους miners να επαληθεύουν ότι καμία έξοδος δεν δαπανάται δύο φορές.





5 XMR



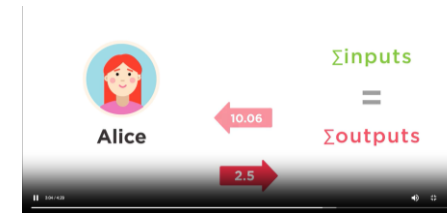
RingCT

- Για να αυξηθεί το απόρρητο και των δύο μελών μιας συναλλαγής εφαρμόζεται το ring CT, Ring Confidential Transactions. Το ring CT αποτρέπει τις διαρροές απορρήτου αποκρύπτοντας τα ποσά των συναλλαγών.
- Όταν νέα moneroj μεταφέρονται για πρώτη φορά, δημιουργούνται ring CT outputs με κρυμμένα ποσά. Ωστόσο δεδομένου ότι οι έξοδοι δεν μπορούν να ξοδευτούν δύο φορές, ο αποστολέας πρέπει να στείλει το output στο σύνολό του, επιστρέφοντας τα ρέστα στον εαυτό του.

First-time transfer



Masked RingCT output generated



Range Proof

- Μια άλλη σημαντική πτυχή μιας συναλλαγής ring CT είναι το range proof (απόδειξη εύρους), το οποίο εμποδίζει τους αποστολείς να δεσμευτούν σε αρνητικές τιμές. Προκειμένου να διασφαλιστεί η προμήθεια του monero, η απόδειξη εύρους αποδεικνύει κρυπτογραφικά ότι τα ποσά που χρησιμοποιούνται στη συναλλαγή είναι μεγαλύτερα από 0 και μικρότερα από κάποιον αυθαίρετο αριθμό.
- Ένας εξωτερικός παρατηρητής δεν είναι σε θέση να δει τα πραγματικά ποσά και τα αποτελέσματα μιας συναλλαγής, είναι σε θέση να επιβεβαιώσει ότι η συναλλαγή είναι νόμιμη και ότι το δίκτυο πρέπει να την αποδεχτεί.

commitment



YES



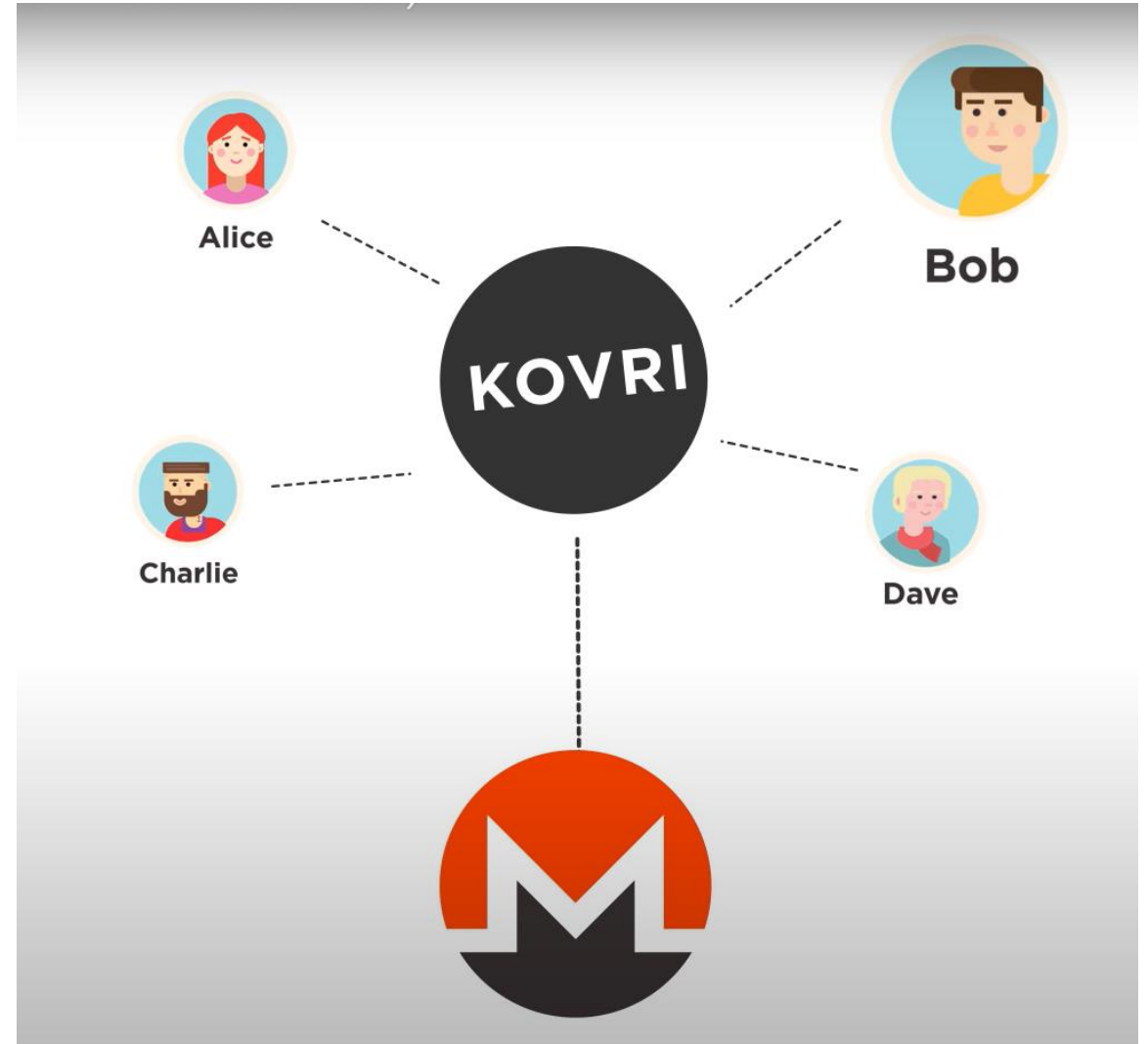
**RING
SIGNATURES**

**RING
CONFIDENTIAL
TRANSACTIONS**

**STEALTH
ADDRESSES**

Kovri

- Τεχνολογία I2P (Invisible Internet Project) που χρησιμοποιεί κρυπτογράφηση και διάφορες τεχνικές δρομολόγησης για να δημιουργήσει ένα ιδιωτικό δίκτυο, αποκρύπτοντας τη γεωγραφική θέση και τη διεύθυνση IP των χρηστών.



RandomX

- Η κοινότητα Monero αποδοκιμάζει την λειτουργία των ASICs (Application-specific Integrated Circuits) στο δίκτυό της και αντιστέκεται έμπρακτα στην καταπολέμησή τους, υλοποιώντας τον αλγόριθμο proof of work, randomX. Αυτός ο αλγόριθμος έχει υψηλές απαιτήσεις σε μνήμη και εισάγει το στοιχείο της τυχαιότητας. Έτσι απωθούνται οι κατασκευαστές από το να σχεδιάσουν κυκλώματα ειδικού σκοπού καθώς με βάση τις απαιτήσεις του randomX θα κοστίζουν ακριβά και δεν θα μπορεί να εξασφαλιστεί η αποδοτικότητά τους.

Monero vs Bitcoin

Ομοιότητες με το Bitcoin

- Αποκέντρωση: Και το Bitcoin και το Monero λειτουργούν χωρίς την ανάγκη μιας κεντρικής αρχής, όπως μιας κυβέρνησης ή ενός χρηματοπιστωτικού ιδρύματος.
- Ψηφιακό νόμισμα: Το Bitcoin και το Monero είναι ψηφιακά νομίσματα που μπορούν να χρησιμοποιηθούν για διαδικτυακές συναλλαγές και ως μέσο αποθήκη αξίας. Μπορούν να αποστέλλονται και να λαμβάνονται παγκοσμίως, χωρίς την ανάγκη διαμεσολαβητών.
- Τεχνολογία blockchain: Και τα δύο κρυπτονομίσματα χρησιμοποιούν την τεχνολογία blockchain για την καταγραφή και την επικύρωση των συναλλαγών. Ωστόσο, διαφέρουν ως προς το επίπεδο ιδιωτικότητας και διαφάνειας που παρέχουν οι αντίστοιχες αλυσίδες μπλοκ.

Διαφορές με το Bitcoin

(1/2)



- **Ιδιωτικότητα και ανωνυμία:** Ενώ το Bitcoin είναι πιο διαφανές. Το Monero επιτυγχάνει την ιδιωτικότητα μέσω προηγμένων κρυπτογραφικών τεχνικών. Το Bitcoin, προσφέρει ψευδωνυμία, που σημαίνει ότι ενώ οι συναλλαγές είναι δημόσιες, οι ταυτότητες του πραγματικού κόσμου πίσω από τις διευθύνσεις μπορεί να είναι δύσκολο να εντοπιστούν, αλλά δεν είναι εντελώς ανώνυμες.
- **Ιχνηλασιμότητα:** Η αλυσίδα μπλοκ του Bitcoin είναι διαφανής, επιτρέποντας σε οποιονδήποτε να δει τα στοιχεία των συναλλαγών και τις διευθύνσεις. Ενώ οι διευθύνσεις Bitcoin δεν αποκαλύπτουν άμεσα προσωπικές πληροφορίες, το ιστορικό των συναλλαγών μπορεί να αναλυθεί για να συνδεθούν οι διευθύνσεις με άτομα ή οντότητες. Αντίθετα, τα χαρακτηριστικά απορρήτου του Monero καθιστούν σημαντικά πιο δύσκολο τον εντοπισμό των συναλλαγών και τη σύνδεσή τους με συγκεκριμένους συμμετέχοντες.
- **Ανταλλαξιμότητα :** Το Monero δίνει μεγάλη έμφαση στη ανταλλαξιμότητα, πράγμα που σημαίνει ότι όλα τα νομίσματα θεωρούνται ίσα και ανταλλάξιμα. Δεδομένου ότι οι συναλλαγές του Monero είναι ιδιωτικές, δεν υπάρχει τρόπος να γίνει διάκριση μεταξύ διαφορετικών νομισμάτων με βάση το ιστορικό τους. Στο Bitcoin, ορισμένα νομίσματα μπορεί να θεωρηθούν λιγότερο πολύτιμα ή μολυσμένα εάν έχουν εμπλακεί σε παράνομες δραστηριότητες, γεγονός που οδηγεί σε πιθανά προβλήματα με τη δυνατότητα ανταλλαγής.

Διαφορές με το Bitcoin

(2/2)

- Κοινότητα και διάδοση: Το Bitcoin έχει σημαντικά μεγαλύτερη βάση χρηστών και είναι πιο διαδεδομένο σε σύγκριση με το Monero. Το Bitcoin θεωρείται συχνά ως ψηφιακή αποθήκευση αξίας και έχει κερδίσει την αναγνώριση της κοινής γνώμης. Το Monero, από την άλλη πλευρά, έχει μικρότερη κοινότητα, αλλά εκτιμάται ιδιαίτερα από άτομα που αναζητούν αυξημένη ιδιωτικότητα και εμπορευσιμότητα.
- Μέγεθος μπλοκ και επεκτασιμότητα: Το Bitcoin έχει ένα σταθερό όριο μεγέθους μπλοκ (επί του παρόντος 1MB) που μπορεί να περιορίσει τον αριθμό των συναλλαγών που υποβάλλονται σε επεξεργασία ανά μπλοκ, οδηγώντας ενδεχομένως σε συμφόρηση του δικτύου. Το Monero, από την άλλη πλευρά, προσαρμόζει δυναμικά το μέγεθος των μπλοκ ανάλογα με τη ζήτηση, επιτρέποντας τη συμπερίληψη περισσότερων συναλλαγών σε κάθε μπλοκ και βελτιώνοντας την επεκτασιμότητα.
- Αλγόριθμος εξόρυξης: Το Bitcoin χρησιμοποιεί τον αλγόριθμο Proof-of-Work (PoW), SHA-256, ενώ το Monero χρησιμοποιεί έναν διαφορετικό αλγόριθμο PoW που ονομάζεται RandomX. Ο αλγόριθμος του Monero έχει σχεδιαστεί για να είναι πιο ανθεκτικός σε εξειδικευμένο υλικό εξόρυξης, προωθώντας ένα πιο αποκεντρωμένο σύστημα εξόρυξης.



Bitcoin	Monero
	

Cryptocurrency Symbol	BTC	XMR
Cryptocurrency Used	Bitcoin	Monero
Founder	Satoshi Nakamoto	Group of 7 core developers
Release Date	9 Jan 2008	18 April 2014
Release Method	Genesis Block Mined	Crowdfunded group of 7 developers
Total Coin Supply	21 Million	Unlimited
Blockchain	Proof of Work	Proof of Work
Useage	Digital Currency	Digital Currency
Mining	ASICs	GPUs, CPU
Minnig Software	MinerGate, ECOS DeFi, NiceHash, and Salad	XMR-Stak
Intended Purpose	To be store of value/ medium of exchange	Decentralized, secure, private and untraceable cryptocurrency
Algorithm	SHA-256	CryptoNote (Random X)
Blocks Time	10 minutes	120 seconds

Βιβλιογραφικές πηγές

- SerHack, December 2018, Mastering Monero The future of private transactions First edition, Monero Community,
<https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf>
- Koe, Kurt M. Alonso, Sarang Noether, April 4 2020, Zero to Monero: Second Edition,
<https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf>
- Monero's RandomX, 5 6 2019,
<https://www.monerooutreach.org/stories/RandomX.html>