Κρυπτο-νομίσματα

- Νόμισμα του οποίου η οργάνωση στηρίζεται σε τεχνικές κρυπτογράφησης
- Συγκεκριμένη οργάνωση επικύρωσης και διασφάλισης των συναλλαγών (blockchain)

Κρυπτονομίσματα

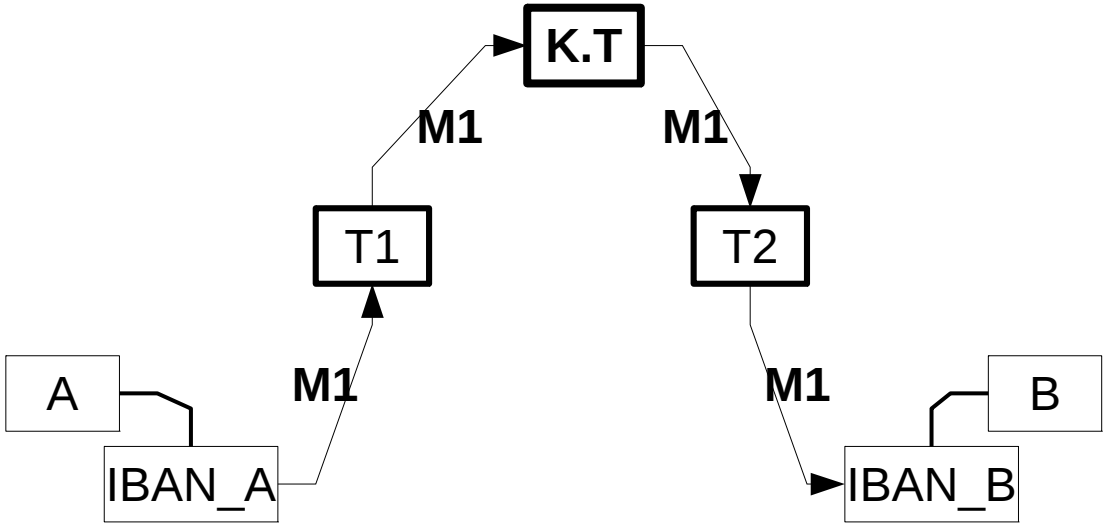
- Όρο δυνατότητας της ύπαρξής τους αποτελεί η εμπορευματική και χρηματική μορφή έκφρασης της αξίας. Δηλαδή ότι η σχέση εμπόρευμα-χρήμα αποτελεί αναγκαία *σχέση* και διατεταγμένη σχέση έκφρασης των καπιταλιστικών σχέσεων παραγωγής και αναπαραγωγής.
- Θεμελιώδες οργανωτικό στοιχείο τους είναι ο τρόπος με τον οποίο επικυρώνονται και διασφαλίζεται το αδιάβλητο των συναλλαγών (blockchain) ή με άλλα λόγια, το σύστημα και οι τεχνικές διασφάλισης και συγκεκριμένης οργάνωσης της έκφρασης των καπιταλιστικών σχέσεων παραγωγής και αναπαραγωγής στη χρηματική μορφή.
- Επομένως η ανάλυσή των κρυπτονομισμάτων πρέπει να κινηθεί α) στο επίπεδο ανάλυσης της χρηματικής μορφής και β) στο επίπεδο ανάλυσης του τρόπου οργάνωσης και επικύρωσης των πληρωμών

Blockchain

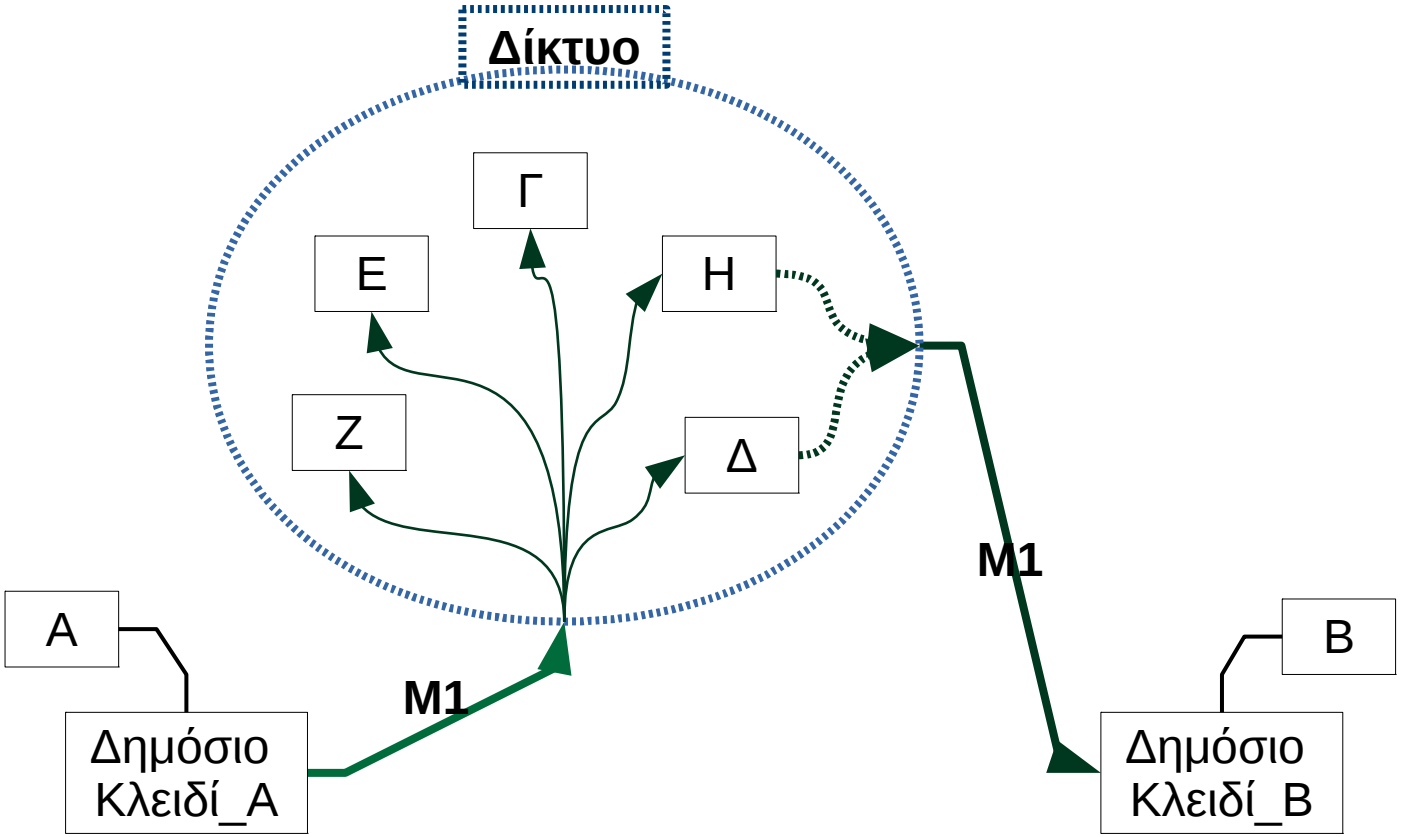
- Ιεραρχημένη αλυσίδα ομαδοποιημένων συναλλαγών

  Θα ξεκινήσουμε με μία ανάλυση του blockchain μέσω της αντιπαραβολής του τρόπου με τον οποίο διενεργούνται πληρωμές μέσω του τραπεζικού συστήματος και του τρόπου με τον οποίο διενεργούνται συναλλαγές στον ‘κόσμο’ των κρυπτονομισμάτων.

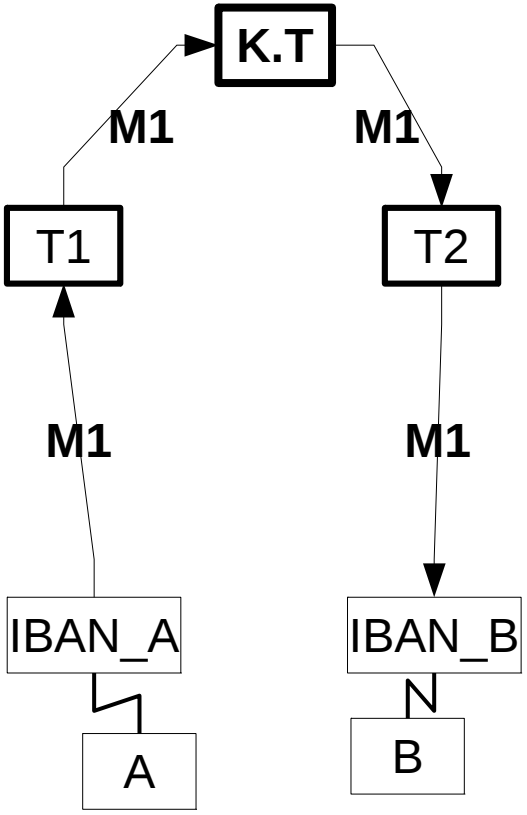
Πληρωμή του Α στον Β μέσω τραπεζών

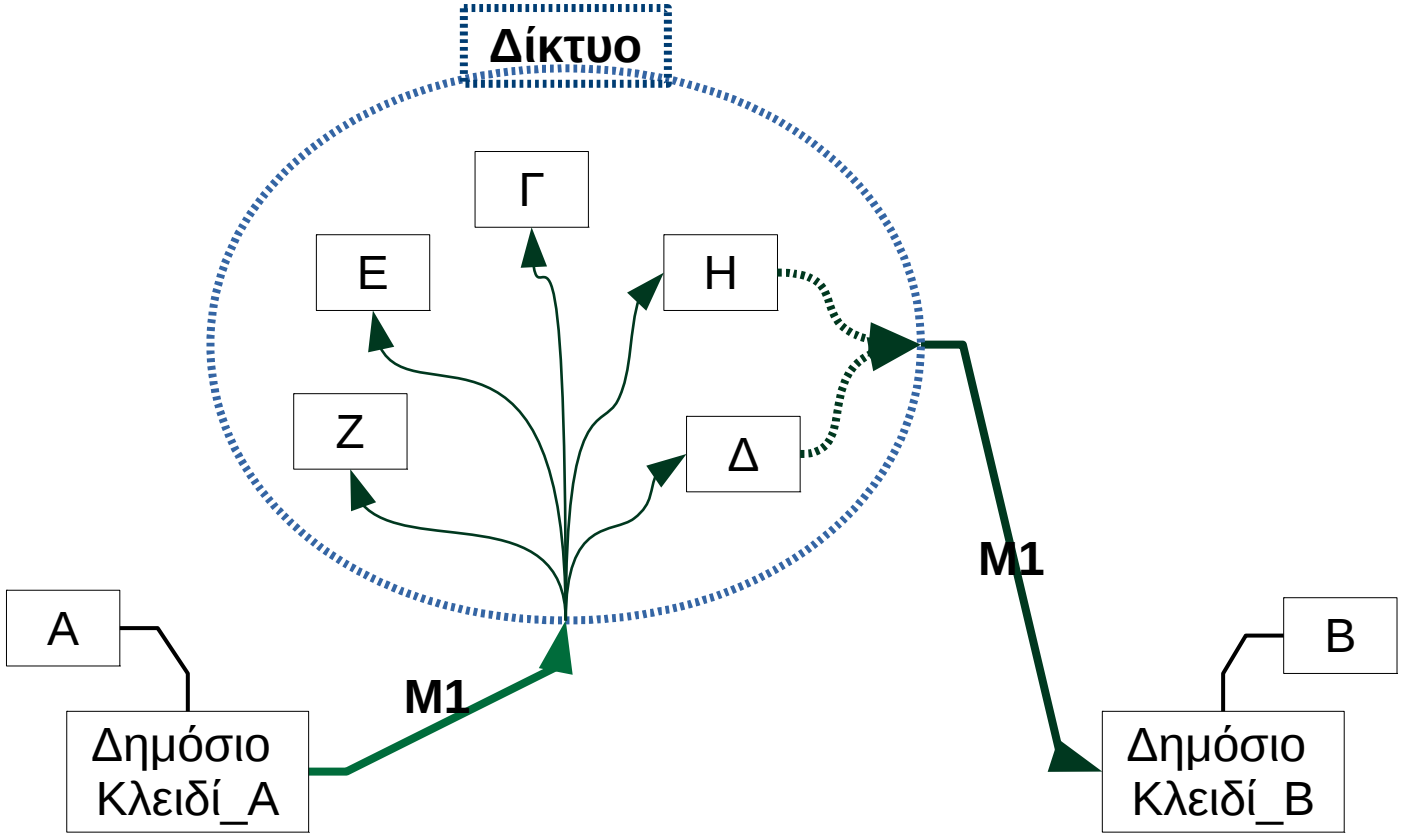


Πληρωμή του Α στον Β μέσω blockchain



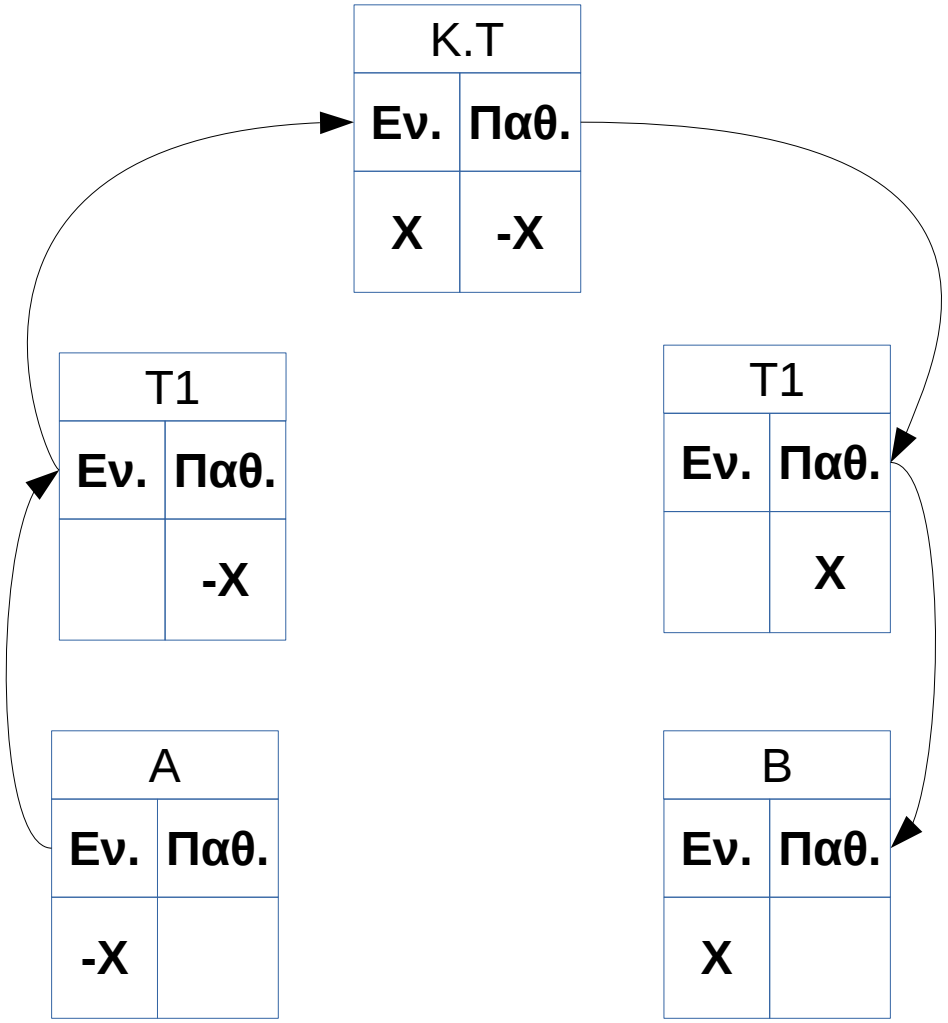
Συγκριτικά και οι δύο τρόποι μαζί



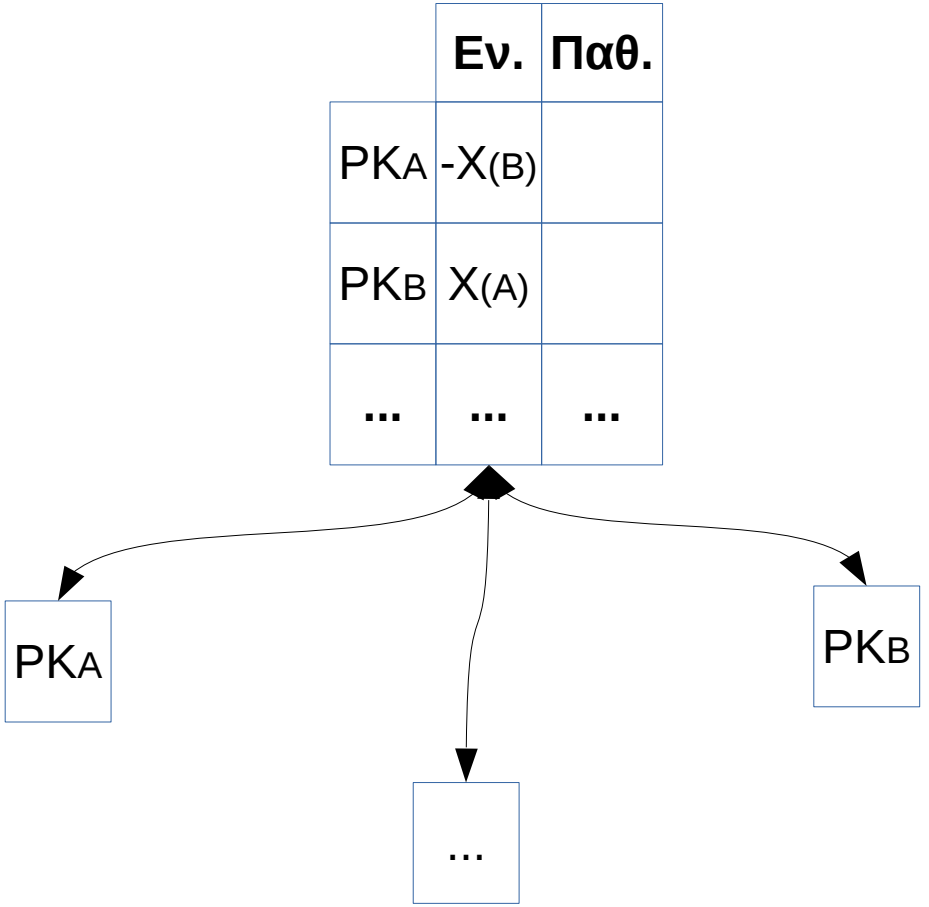


Η πληρωμή ως αλλαγή εγγραφών σε βιβλία λογαριασμών

Τρέχον τρόπος με βάση το τραπεζικό σύστημα



Δημόσιο λογιστικό βιβλίο στα κρυπτονομίσματα



Χρήμα

- Μορφή έκφρασης των κοινωνικών σχέσεων παραγωγής και αναπαραγωγής
- Μορφή συμπύκνωσης των κοινωνικών συγκρούσεων
- Οργανωτικό στοιχείο της ‘πολιτικής’ οργάνωσης της καπιταλιστικής εξουσίας
- Το χρήμα παράγεται αυτοφυώς ως διατεταγμένο ζεύγος που μόνο τελικά οργανωνέται/ επικυρώνεται από το κράτος

Χρήμα

- Μετρητής αξίας – γενικό ισοδύναμο
- Μονάδα μέτρησης – λογιστική μονάδα
- Μέσο συναλλαγών
- Μέσο αποθεματοποίησης (‘αποθήκευσης’) αξίας

Χρήμα

- Η περιγραφή των ποσοτικών χαρακτηριστικών της κυκλοφορίας μέσω μίας σχέσης:

  MV = PT + Ληξιπρόθεσμες Συναλλαγές (για μία περίοδο)

  Η αιτιότητα τρέχει από το δεύτερο μέλος πρός το πρώτο
- Τραπεζικό σύστημα
- Κρατική οργάνωση των συστημάτων πληρωμών και της Πίστης (Κεντρική Τράπεζα)

Το bitcoin σε σχέση με άλλα νομίσματα

1) Πόσα κρυπτονομίσματα κυκλοφορούν (coins-tokens):

Γύρω στα 1564 κρυπτονομίσματα

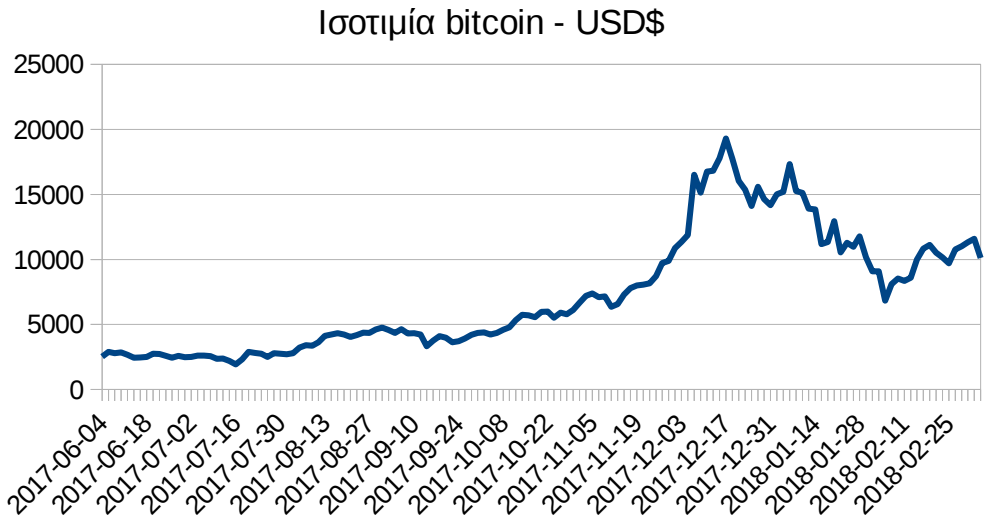
2) Ογκος αξίας σε κυκλοφορία: $290.339.541.962

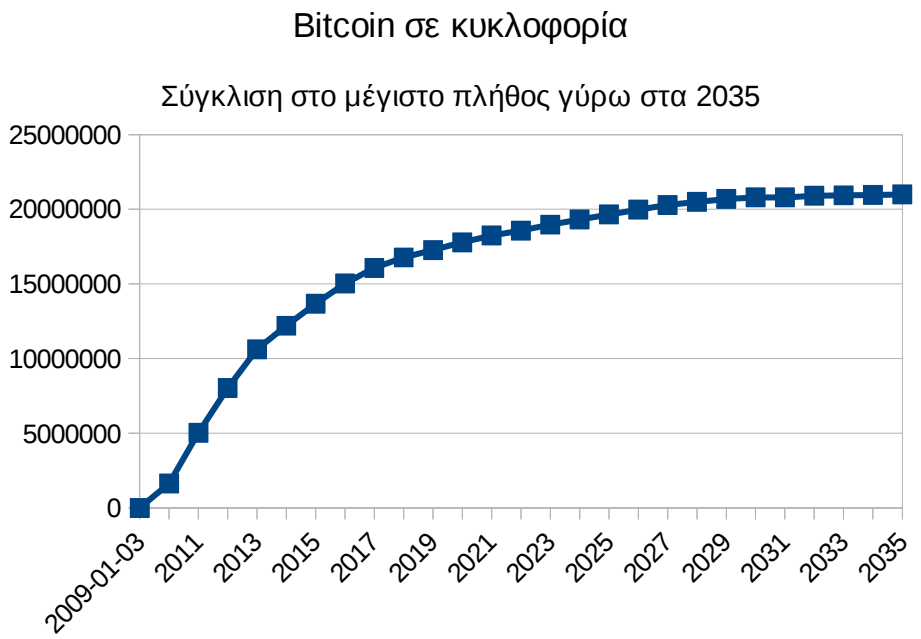
Πηγή: https://coinmarketcap.com/ 2018-03-18

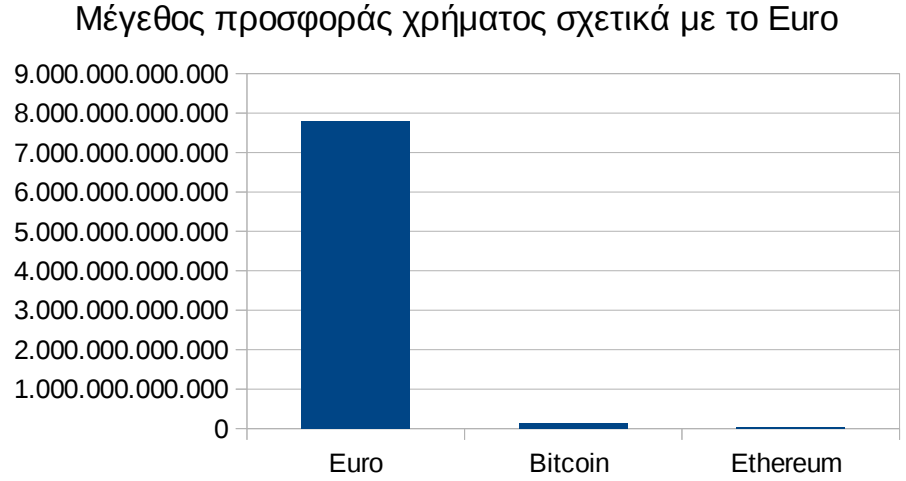
3) Συναλλαγές ανά δευτερόλεπτο:

Μέσο πληρωμής	Συναλλαγές ανά δευτερόλεπτο
Bitcoin	4
Ethereum	20
paypal	193
Visa	1670

Το bitcoin σε σχέση με άλλα νομίσματα







Το bitcoin σε σχέση με άλλα νομίσματα: Θεσμικό Πλαίσιο

- Ζητήματα φορολογίας (έμμεση σε συναλλαγές και άμεση σε εισοδήματα)
- Ζητήματα νομιμότητας
- Τρόποι χρήσης (εμβάσματα, παράνομες δραστηριότητες, στοιχείο χαρτοφυλακίων)

Το bitcoin σε σχέση με άλλα νομίσματα: Πλεονεκτήματα

Από την πλευρά του χρήστη

α) Μικρός χρόνος για επαλήθευση και τελική πληρωμή συναλλαγών. Λιγότερο από μία ώρα για αποκεντρωμένες πλατφόρμες και σχεδόν άμεσα για κεντροποιημένες

β) Δεν απαιτείται συμφωνίας μέ ειδικούς όρους όρους ή πληρώμη αντιτίμου/τελών για τη χρήση της υπηρεσίας (όπως στις τράπεζες)

γ) σχετική ανωνυμία (ψευδωνυμία)

δ) Πολύ μικρά κόστη για να συμμετέχεις και να συναλλάσσεσαι (μηδενικό αν συντηρείς ο ίδιος το πορτοφόλι σου και μικρά μέχρι στιγμής αντίτιμο συναλλαγών σχετικά με τα τέλη των τραπεζών) και φυσικά δεν υπάρχει κόστος για πληρωμές παγκόσμια,

Ωστόσο υπάρχει κόστος για τη μετατροπή σε τοπικό νόμισμα και μεγάλος κίνδυνος λόγω της μεταβλητότητας της ισοτιμίας των κρυπτονομισμάτων με κρατικά ελεγχόμενα νομίσματα

Ειδικό πλεονέκτημα για τον πωλητή:

Μη-αντιστρεπτό των συναλλαγών (αυτό είναι γενικά ένα αμφισβητούμενο σημείο) λόγω αλγοριθμικής εκτέλεσης και επικύρωσης – αποτελεί στοιχείο σχεδιασμού των κρύπτο-νομισμάτων μέχρι σήμερα τουλάχιστον το οποίο του ενισχύει την θέση σε σχέση με τον πληρωτή (μη-υπαναχώρηση)

Το bitcoin σε σχέση με άλλα νομίσματα: Πλεονεκτήματα

Δύο άλλα χαρακτηριστικά:

1) Ο συλλογικός χαρακτήρας διαμοιρασμού του κόστους το οποίο επιτρέπει να διαχέεται το κόστος επενδύσεων για επαλήθευση των συναλλαγών και συγκρότηση του βιβλίου συναλλαγών.

2) Το ότι είναι **προγράμματα ανοιχτού κώδικα** τα οποία είναι ελεύθερα και το σημαντικότερο ο κάθε ένας (ο οποίος γνωρίζει ανάγνωση κώδικα) μπορεί να διαβάσει τον κώδικα και να προτείνει τροποποιήσεις – οι πολλοί σκέφτονται καλύτερα από τον ένα. Επομένως πιο δημοκρατικά χαρακτηριστικά από αυτήν την πλευρά σε σχέση με το λογισμικό κλειστού κώδικα ή την παρουσία άλλων στεγανών στη συμμετοχή πολλών στη διαδικασία αποφάσεων) και πιο συμβατά με τη δυναμική διαδικασία ανάπτυξης των γνώσεων.

Το bitcoin σε σχέση με άλλα νομίσματα: Μειονεκτήματα και κίνδυνοι

1) Έλλειψη διαφάνειας στη λειτουργία τους (τεχνική γνώση, παραγωγή και ποιότητα αλγορίθμων, δυνατότητα απάτης).

2) Δεν υπάρχει ρύθμιση και επίβλεψη:
Αυτό σημαίνει ότι δεν υπάρχει εγγύηση ‘καταθέσεων’ και δυνατότητα αποδέσμευσης από μία ‘κακή’ συμφωνία. Δεν υπάρχει επίσης ρυθμισμένο νομικό πλαίσιο: επομένως α) συμβάσεις που γίνονται μπορεί με ένα άλλο νομικό πλαίσιο να καταστούν άκυρες, β) το καθεστώς φορολόγησης δεν είναι καθαρό, επομένως μπορεί να υπάρξουν επιπλέον κόστη χωρίς να έχεις τη δυνατότητα αποδέσμευσης ή άλλων διευθετήσεων. Δεν υπάρχουν ελάχιστες απαιτήσεις κεφαλαίου κλπ για όσους ‘τρέχουν’ μία τέτοια πλατφόρμα.

3) Έλλειψη συνέχειας και πιθανής έλλειψης ρευστότητας
Για πολλούς λόγους, η συνέχεια ενός κρυπτονομίσματος δεν είναι εγγυημένη. Οι χρήστες αντιμετωπίζουν τον κίνδυνο μιας απότομη άρση της εμπιστοσύνης στην κοινότητα. Επίσης Οι δραστηριότητες βασικών φορέων μπορεί να διακοπούν, όχι μόνο ως αποτέλεσμα της πτώχευσης, αλλά και για οποιονδήποτε άλλο λόγο (π.χ. έλλειψη κερδοφορίας).

4) Υψηλή εξάρτηση από τεχνολογίες πληροφορικής και δικτύου

5) Ανωνυμία (στην πραγματικότητα δεν υπάρχει ανωνυμία αλλά ‘ψευδωνυμία’ η οποία μπορεί να αρθεί.)

6) Υψηλή μεταβλητότητα

Το bitcoin σε σχέση με άλλα νομίσματα

- Κανόνες vs αποφάσεις σχετικά με τη συγκυρία (πολιτική)
- Δανειστής ύστατης προσφυγής
- Θεσμικό πλαίσιο προστασίας χρηστών από απάτες ή πτωχεύσεις

άρθρο Nakamoto: Στόχοι και μέθοδος

Εισαγωγή

Το εμπόριο στο Διαδίκτυο έχει καταλήξει να βασίζεται σχεδόν αποκλειστικά σε χρηματοπιστωτικά ιδρύματα που λειτουργούν ως αξιόπιστα τρίτα μέρη {ενδιάμεσοι} για να διεκπεραιώνουν τις ηλεκτρονικές πληρωμές.

Αν και το σύστημα λειτουργεί αρκετά καλά για το μεγαλύτερο όγκο των συναλλαγών {επομένως συμπλήρωμα}, εξακολουθεί να πάσχει από τις εγγενείς αδυναμίες ενός υποδείγματος που βασίζεται στην εμπιστοσύνη *{στόχος: ένα υπόδειγμα που δεν θα βασίζεται εκεί, και ο οποίος αποτυγχάνει λόγω μη-επαρκούς εννοιολόγησης της 'εμπιστοσύνης'}.* Μη-αναστρέψιμες συναλλαγές {επομένως ενίσχυση της θέσης των πωλητών} δεν είναι ουσιαστικά δυνατές, δεδομένου ότι τα χρηματοπιστωτικά ιδρύματα δεν μπορούν να αποφύγουν τη διαμεσολάβηση στην επίλυση διαφορών *{επομένως ένα σύστημα το οποίο δεν διαμεσολαβεί διαφορές: ό,τι έγινε - έγινε}*. Το κόστος της διαμεσολάβησης αυξάνει το κόστος συναλλαγών, θέτει ένα όριο στο πιο μπορεί να είναι το ελάχιστο μέγεθος των συναλλαγών και επομένως δεν δίνει τη δυνατότητα να λαμβάνουν χώρα μικρές απλές συναλλαγές και συγχρόνως δημιουργεί ένα ευρύτερο κόστος από την απώλεια της δυνατότητας οι πληρωμές να μην είναι δυνατό να αναστραφούν για υπηρεσίες που παρασχέθηκαν και των οποίων η παροχή είναι πρακτικά μη-αναστρέψιμη. Με τη δυνατότητα αντιστροφής, διευρύνονται οι ανάγκες ύπαρξης εμπιστοσύνης.

Αυτό που χρειάζεται είναι ένα σύστημα ηλεκτρονικών πληρωμών βασισμένο στην κρυπτογραφική απόδειξη αντί της εμπιστοσύνης, επιτρέποντας σε δυο ενδιαφερόμενα μέρη να συνάψουν συναλλαγές απευθείας μεταξύ τους χωρίς την ανάγκη μεσολάβησης ενός αξιόπιστου τρίτου μέρους. Οι συναλλαγές οι οποίες θα είναι μη-πρακτικό υπολογιστικά να αναστραφούν, θα προστατεύσουν τους πωλητές από απάτες και μηχανισμοί συστηματικής μεσεγγύησης θα μπορούσαν εύκολα να εφαρμοστούν για την προστασία των αγοραστών. Σε αυτή την εργασία προτείνουμε μια λύση στο πρόβλημα της *διπλής δαπάνης* χρησιμοποιώντας έναν διακομιστή/εξυπηρετητή οργανωμένο με βάση την ομότιμη σχέση χρηστών ο οποίο διανέμεται μεταξύ τους και έχει χρονική σήμανση μέσω του οποίου παράγεται υπολογιστικά απόδειξη της χρονολογικής διάταξης των συναλλαγών. Το σύστημα είναι ασφαλές στο βαθμό που οι 'τίμιοι' κόμβοι του δικτύου ελέγχουν συλλογικά περισσότερη υπολογιστική σε σχέση με οποιαδήποτε ομάδα συνεργαζόμενων κόμβων του δικτύου οι οποία 'επιτίθεται' στο σύστημα πρός όφελός της.

αρθρο Nakamoto: Στόχοι και μέθοδος

Συμπέρασμα

Έχουμε προτείνει ένα σύστημα ηλεκτρονικών συναλλαγών το οποίο δεν στηρίζεται στην εμπιστοσύνη *{δεν το έχει αποδείξει, λόγω μη-επαρκούς εννοιολόγησης. Εχει αποδείξει ότι δεν χρειάζεται ένας τρίτος για να κρατήσει το βιβλίο συναλλαγών, αλλά ζητήματα εμπιστοσύνης προβάλλουν τουλάχιστον σε δύο σημεία: προστασία αγοραστών, και 51% της υπολογιστικής ισχύος. Η εμπειρία του bitcoin δείχνει ότι υπάρχουν και άλλα σημεία που εμφανίζεται η ανάγκη εμπιστοσύνης}*.

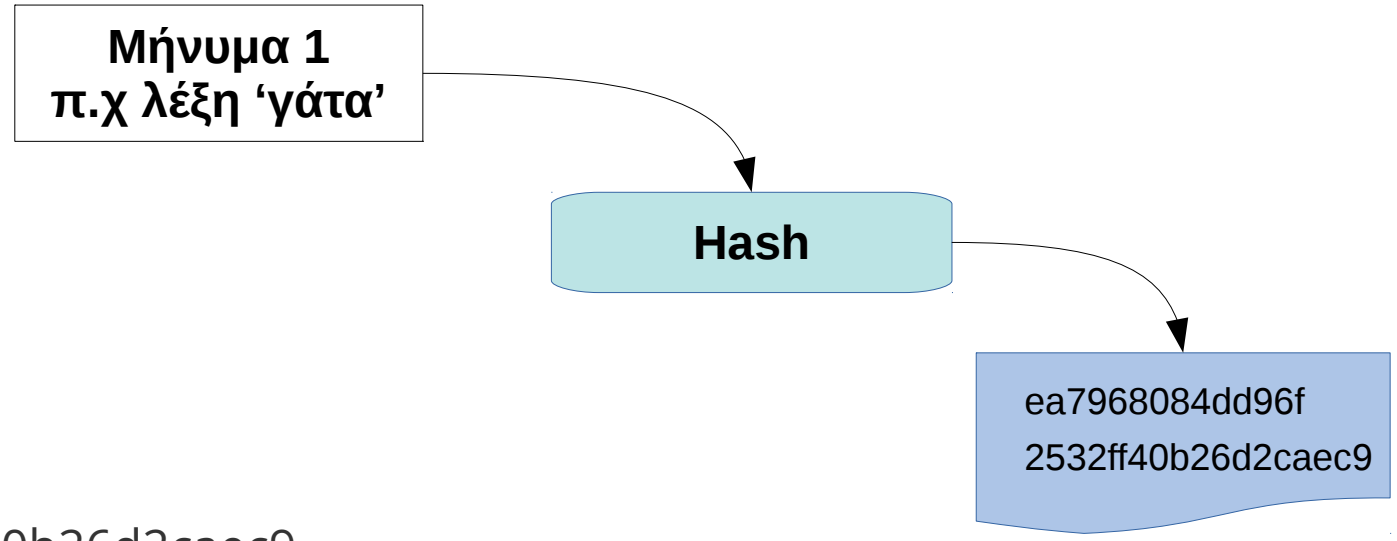
Ξεκινήσαμε με το σύνηθες πλαίσιο νομισμάτων που συγκροτούνται με βάση τις ψηφιακές υπογραφές, το οποίο παρέχει ισχυρό έλεγχο της ιδιοκτησίας, αλλά είναι ελλιπές στο βαθμό που δεν περιέχει ένα τρόπο αποτροπής της διπλής δαπάνης. Για να επιλυθεί αυτό το πρόβλημα, προτείνουμε ένα δίκτυο peer-to-peer οργανωμένο στη βάση της απόδειξης-εργασίας για να καταγράφει ένα δημόσιο ιστορικό των συναλλαγών το οποίο γρήγορα, καθώς αναπτύσσεται, καθιστά υπολογιστικά μη πρακτική την αλλαγή του από έναν εισβολέα αν οι ‘τίμιοι/ειλικρινείς’ κόμβοι ελέγχουν το μεγαλύτερο ποσοστό υπολογιστικής ισχύος.

Το δίκτυο είναι ανθεκτικό στην μη-δομημένη απλότητα του. Οι κόμβοι εργάζονται ταυτόχρονα με ελάχιστο συντονισμό. Δεν χρειάζεται να ταυτοποιηθούν, δεδομένου ότι τα μηνύματά τους δεν μεταφέρονται σε κάποια συγκεκριμένη τοποθεσία και το μόνο απαιτούμενο είναι αυτά να παραδοθούν στη βάση της καλύτερης προσπάθειας. Οι κόμβοι μπορούν να αποσυνδεθούν και να επανασυνδεθούν στο δίκτυο κατά βούληση, αποδεχόμενοι την αλυσίδα απόδειξης εργασίας ως απόδειξη του τι συνέβη όταν είχαν αποσυνδεθεί.

Ψηφίζουν με την υπολογιστική ισχύ τους, εκφράζοντας την αποδοχή τους για έγκυρες ομάδες συναλλαγών, εργαζόμενοι για την επέκτασή τους και απορρίπτοντας μη-έγκυρες ομάδες συναλλαγών αρνούμενοι να εργαστούν πάνω σε αυτές. Όλοι οι αναγκαίοι κανόνες και τα κίνητρα μπορούν να ενισχυθούν με αυτόν τον μηχανισμό συναίνεσης.

https://bitcoin.org/bitcoin.pdf

Hash



Για παράδειγμα

η λέξη «γάτα» έχει hash:

ea7968084dd96f2532ff40b26d2caec9

(MD5 αλγόριθμος και η λέξη γραμμένη με unicode χαρακτήρες),

η λέξη «Γάτα» έχει hash:

8b6de4e0433ec30f35b907fd10dd713f,

η ίδια χωρίς τόνο, «Γατα»:

74fc09fbe10901e7859af99550dda3cd

και η ίδια γραμμένη σε ένα txt αρχείο, το οποίο περιέχει μόνο αυτήν την λέξη και το οποίο έχει τίτλο «γάτα» έχει MD5 hash:

57878a8c183c1184f8a7cb7e46abc685,

ενώ ένα άλλο αρχείο pdf μεγέθους 10 Mb έχει MD5 hash:

0809b9e4527e7765f960b495966619fc.

Ασύμμετρη κρυπτο-γράφηση δημόσιου – ιδιωτικού κλειδιού