

21 Μαθήματα — Κεφάλαιο Ι: Φιλοσοφία

 **nikos** Jan 16, 2020 · 17 min read

Το παρακάτω κείμενο βασίζεται στο βιβλίο “21 Lessons” του [Gigi](#). Για να βρείτε την αρχική πηγή του κειμένου επισκευθείτε την ιστοσελίδα: 21lessons.com

Μετάφραση: [niclick](#)

. . .





Πρόλογος

“ Η μικρή Αλίκη έπεσε μέσα στην τρύπα, χτύπησε το κεφάλι της και τραυμάτισε την ψυχή της”

Η πτώση στο λαγούμι του Bitcoin είναι μια περίεργη εμπειρία. Όπως πολλοί άλλοι, αισθάνομαι ότι έχω μάθει περισσότερα τα τελευταία δύο χρόνια μελετώντας το Bitcoin απ’ ό,τι έχω μάθει κατά τη διάρκεια των δύο δεκαετιών της επίσημης εκπαίδευσής μου.

Τα ακόλουθα μαθήματα είναι το απόσταγμα όσων έχω μάθει. Πρώτα δημοσιευμένο ως σειρά άρθρων με τίτλο “Τι έμαθα από το Bitcoin”, αυτό που ακολουθεί μπορεί να θεωρηθεί ως δεύτερη έκδοση της αρχικής σειράς.

Όπως και το Bitcoin, αυτά τα μαθήματα δεν είναι ένα στατικό πράγμα. Σκοπεύω να τα επεξεργάζομαι ανά διαστήματα, δημοσιεύοντας μελλοντικά ανανεωμένες εκδόσεις και πρόσθετο υλικό.

Σε αντίθεση με το Bitcoin, οι μελλοντικές εκδόσεις αυτού του έργου δεν χρειάζεται να είναι αναδρομικά συμβατές. Ορισμένα μαθήματα μπορεί να επεκταθούν, άλλα μπορεί να επαναγραφούν ή να αντικατασταθούν. Ελπίζω ότι μια από τις μελλοντικές εκδόσεις θα είναι κάτι που θα μπορείτε να κρατήσετε στα χέρια σας,¹ αλλά δεν θέλω να υποσχεθώ ακόμα πολλά. ¹Τελικά το τύπωσε.

Το Bitcoin είναι ένας ανεξάντλητος δάσκαλος, γι' αυτό δεν ισχυρίζομαι ότι τα μαθήματα αυτά είναι ολοκληρωμένα ή πως περιλαμβάνουν τα πάντα. Είναι μια αντανάκλαση του προσωπικού μου ταξιδιού μέσα στο λαγούμι. Υπάρχουν πολλά ακόμα μαθήματα που πρέπει να μάθει κανείς και κάθε άτομο θα μάθει κάτι διαφορετικό μετά από την είσοδο στον κόσμο του Bitcoin.

Ελπίζω να σας φανούν χρήσιμα αυτά τα μαθήματα και ότι η διαδικασία εκμάθησης αυτών μέσα από ανάγνωση δεν θα είναι τόσο κουραστική και επίπονη όσο η μάθηση από πρώτο χέρι.

-Gigi

. . .

Εισαγωγή

“Μα δεν θέλω να βρεθώ ανάμεσα σε τρελούς ανθρώπους”, παρατήρησε η Αλίκη.

“Ω, δεν μπορείς να κάνεις κάτι γι' αυτό”, είπε ο Γάτος: “είμαστε όλοι τρελοί εδώ. Εγώ είμαι τρελός. Εσύ είσαι τρελή”.

“Πώς ξέρεις ότι είμαι τρελή;” είπε η Αλίκη.

“Πρέπει να είσαι,” είπε ο Γάτος, “αλλιώς δεν θα είχες έρθει εδώ.”

Τον Οκτώβριο του 2018, ο Arjun Balaji ρώτησε την ακίνδυνη ερώτηση: Τι μάθατε από το Bitcoin; Αφότου προσπάθησα να απαντήσω σε αυτή την ερώτηση με ένα σύντομο tweet, αποτυγχάνοντας παταγοδώς, συνειδητοποίησα ότι τα πράγματα που έχω μάθει είναι πάρα πολλά για να απαντήσω γρήγορα, έως και καθόλου.

Τα πράγματα που έχω μάθει είναι, προφανώς, για το Bitcoin — ή τουλάχιστον σχετίζονται με αυτό. Παρ' όλα αυτά, ενώ εξηγούνται μερικές από τις εσωτερικές λειτουργίες του Bitcoin, τα ακόλουθα μαθήματα δεν αποτελούν εξήγηση για το πώς λειτουργεί το Bitcoin ή για το τί είναι, θα μπορούσαν όμως να βοηθήσουν στην εξερεύνηση μερικών πραγμάτων με τα οποία *συνδέεται*: τις φιλοσοφικές ερωτήσεις, οικονομικές πραγματικότητες, και τεχνολογικές καινοτομίες.

Τα 21 μαθήματα είναι δομημένα σε δέσμες των επτά, από τις οποίες προκύπτουν τρία κεφάλαια. Κάθε κεφάλαιο μελετά το Bitcoin μέσα από έναν διαφορετικό φακό και εξάγει τα μαθήματα που μπορεί να πάρει κανείς, εξετάζοντας το περιεργο αυτό δίκτυο μέσα από μία άλλη οπτική γωνία.

Το Κεφάλαιο 1 διερευνά τις φιλοσοφικές διδασκαλίες του Bitcoin. Η αλληλεπίδραση της αμεταβλητότητας και της αλλαγής, η έννοια της πραγματικής σπανιότητας, η άψογη σύλληψη του Bitcoin, το πρόβλημα της ταυτότητας, η αντίφαση της αναπαραγωγής και της τοπικότητας, η δύναμη του ελεύθερου λόγου και τα όρια της γνώσης.

Το Κεφάλαιο 2 διερευνά τις οικονομικές διδασκαλίες του Bitcoin. Μαθήματα σχετικά με την οικονομική άγνοια, τον πληθωρισμό, την αξία, το χρήμα και την ιστορία του χρήματος, το τραπεζικό σύστημα κλασματικών αποθεμάτων και τον τρόπο με τον οποίο το Bitcoin επανεισάγει τα “υγιή” χρήματα μέσω ενός πονηρού, έμμεσου τρόπου.

Το Κεφάλαιο 3 διερευνά μερικά από τα μαθήματα που διδάχτηκαν, μέσω της εξέτασης της τεχνολογίας του Bitcoin. Γιατί υπάρχει δύναμη στους αριθμούς, σκέψεις σχετικά με την εμπιστοσύνη, γιατί απαιτεί έργο ο προσδιορισμός της ώρας, γιατί το να κινείσαι αργά και να μην χαλάς πράγματα είναι ένα χαρακτηριστικό και όχι ελλάτωμα, τι μπορεί να μας διδάξει το Bitcoin σχετικά με την ιδιωτικότητα, γιατί οι cypherpunks γράφουν κώδικα (και όχι νόμους), και ποιες μεταφορές μπορεί να σας φανούν χρήσιμες για να εξερευνήσετε το μέλλον του Bitcoin.

Κάθε μάθημα περιέχει αρκετά αποσπάσματα και συνδέσμους καθ' όλη τη διάρκεια του κειμένου. Εάν έχω εξερευνήσει περαιτέρω μια ιδέα, μπορείτε να βρείτε συνδέσμους με τα σχετικά μου έργα στην ενότητα “Through the Looking-Glass”. Εάν θέλετε να εμβαθύνετε περισσότερο, συνδέσμοι με το πιο σχετικό υλικό παρατίθενται στην ενότητα “Down the Rabbit Hole”. Και τα δύο μπορούν να βρεθούν στο τέλος του κάθε μαθήματος.

Παρ' όλο που κάποια προηγούμενη γνώση σχετικά με το Bitcoin να είναι ωφέλιμη, ελπίζω ότι αυτά τα μαθήματα θα μπορούν να αφομοιωθούν από κάθε περίεργο αναγνώστη. Ενώ μερικά συνδέονται μεταξύ τους, το κάθε μάθημα θα πρέπει να είναι σε θέση να σταθεί από μόνο του και να διαβαστεί ανεξάρτητα. Έβαλα τα δυνατά μου για να αποφύγω την τεχνική φρασεολογία, παρ' όλο που μερικό λεξιλόγιο αποκληστικά και μόνο κάποιων συγκεκριμένων τομέων, είναι αναπόφευκτο.

Ελπίζω πως τα γραπτά μου να λειτουργήσουν ως έμπνευση για άλλους με σκοπό να δουν κάτω από την επιφάνεια και να εξετάσουν μερικά από τα βαθύτερα ερωτήματα

που εγείρει το Bitcoin. Η δική μου έμπνευση προέρχεται από ένα πλήθος συγγραφέων και δημιουργών περιεχομένου, σε όλους τους οποίους είμαι αιώνια ευγνώμων.

Τέλος, στόχος όσων γράφω δεν είναι να σας πείσουν για κάτι. Στόχος μου είναι να σας κάνω να σκεφτείτε και να σας δείξω ότι κρύβονται πολλά περισσότερα πράγματα πίσω από το Bitcoin από ό,τι μπορεί να φαντάζεστε αρχικά. Δεν μπορώ καν να σας πω τι είναι το Bitcoin ή τι θα σας διδάξει. Είναι κάτι που θα πρέπει να ανακαλύψετε οι ίδιοι.

“Μετά από αυτό, δεν υπάρχει επιστροφή. Παίρνεις το μπλε χάπι — η ιστορία τελειώνει, ξυπνάς στο κρεβάτι σου και πιστεύεις ό,τι θέλεις να πιστεύεις. Παίρνεις το κόκκινο χάπι — μένεις στη χώρα των θαυμάτων και σου δείχνω πόσο βαθιά φτάνει το λαγούμι.” -Μορφέας



. . .

Κεφάλαιο 1: Φιλοσοφία

Το ποντίκι την κοίταξε κάπως διεξοδικά και της φάνηκε σαν να της έκλεινε το ένα από τα μικρά του μάτια, αλλά δεν είπε τίποτα.

Κοιτάζοντας το Bitcoin επιφανειακά, θα μπορούσε κανείς να συμπεράνει ότι είναι αργό, σπάταλο, άσκοπα περιττό και υπερβολικά παρανοϊκό. Κοιτάζοντας το Bitcoin

διεξοδικά, μπορεί κανείς να ανακαλύψει ότι τα πράγματα δεν είναι όπως φαίνονται με την πρώτη ματιά.

Το Bitcoin έχει έναν τρόπο να παίρνει τις υποθέσεις που κάνεις και να τις αντιστρέφει πλήρως. Μετά από λίγο, καθώς ήσουν έτοιμος να βουλευτείς και πάλι, έρχεται το Bitcoin και σαν ταύρος σπάει τον τοίχο ενός καταστήματος με πορσελάλινα είδη και διαλύει τις υποθέσεις που είχες κάνει, για ακόμη μια φορά.



Τυφλοί μοναχοί εξετάζουν έναν ταύρο ονόματι Bitcoin

Το Bitcoin είναι παιδί πολλών επιστημονικών κλάδων. Όπως οι τυφλοί μοναχοί που εξετάζουν έναν ελέφαντα, έτσι όποιος προσεγγίζει αυτή τη νέα τεχνολογία το κάνει και από διαφορετική οπτική γωνία. Και όλοι θα καταλήξουν σε διαφορετικά συμπεράσματα σχετικά με τη φύση του θηρίου αυτού.

Τα ακόλουθα μαθήματα αφορούν μερικές από τις υποθέσεις μου τις οποίες το Bitcoin κατέστρεψε και τα συμπεράσματα στα οποία έφτασα. Κατά τα πρώτα τέσσερα μαθήματα εξετάζονται τα φιλοσοφικά ζητήματα της αμεταβλητότητας, της σπανιότητας, της τοπικότητας και της ταυτότητας.

- Μάθημα 1: Αμεταβλητότητα και αλλαγή
- Μάθημα 2: Η σπανιότητα της σπανιότητας

- Μάθημα 3: Αναπαραγωγή και τοπικότητα
- Μάθημα 4: Το πρόβλημα της ταυτότητας
- Μάθημα 5: Μία άφογη σύλληψη
- Μάθημα 6: Η δύναμη του ελεύθερου λόγου
- Μάθημα 7: Τα όρια της γνώσης

Το μάθημα 5 διερευνά το πώς η ιστορία γέννησης του Bitcoin δεν είναι μόνο συναρπαστική αλλά απολύτως απαραίτητη για ένα σύστημα χωρίς ηγέτες. Τα δύο τελευταία μαθήματα αυτού του κεφαλαίου διερευνούν τη δύναμη της ελευθερίας του λόγου και τα όρια της ατομικής μας γνώσης, πράγμα που φαίνεται στο εκπληκτικό βάθος του λαγουμιού του Bitcoin.

Ελπίζω ότι θα βρείτε τον κόσμο του Bitcoin εξίσου εκπαιδευτικό, συναρπαστικό, αλλά και διασκεδαστικό, όπως τον βρήκα ο ίδιος και εξακολουθώ να βρίσκω. Σας προσκαλώ να ακολουθήσετε το λευκό κουνέλι και να εξερευνήσετε τα βάθη αυτού του λαγουμιού. Τώρα, κρατήστε μόνο καλά το ρολόι τσέπης σας, πέστε μέσα και απολαύστε την πτώση.

. . .

Μάθημα 1: Αμεταβλητότητα και αλλαγή

Αναρωτιέμαι αν άλλαξα μέσα στη νύχτα. Ασε με να σκεφτώ. Ήμουν το ίδιο όταν σηκώθηκα σήμερα το πρωί; Σχεδόν πιστεύω ότι μπορώ να θυμηθώ να αισθάνομαι λίγο διαφορετικά. Αλλά αν δεν είμαι το ίδιο, η επόμενη ερώτηση είναι «Ποιά στο καλό είμαι εγώ;» Αα, αυτό είναι το σπουδαίο ερώτημα!

Το Bitcoin είναι εκ φύσεως δύσκολο να περιγραφεί. Πρόκειται για ένα νέο πράγμα και κάθε προσπάθεια να συγκριθεί με προηγούμενες ιδέες — είτε ονομάζοντάς το ως τον ψηφιακό χρυσό, είτε ως το διαδίκτυο των χρημάτων — είναι αναπόφευκτα καταδικασμένη να αποτύχει στην δημιουργία μίας πλήρους εικόνας. Όποια και αν είναι η αγαπημένη σας αναλογία, δύο πτυχές του Bitcoin είναι απολύτως απαραίτητες: αποκέντρωση και αμεταβλητότητα.

Ένας τρόπος να καταλάβουμε το Bitcoin είναι να το φανταστούμε ως ένα αυτοματοποιημένο κοινωνικό συμβόλαιο. Το λογισμικό είναι μόνο ένα κομμάτι του παζλ. Η ελπίδα πως το Bitcoin μπορεί να αλλαχθεί μέσω της αλλαγής του λογισμικού, αποτελεί μάταιη πράξη. Κάποιος θα πρέπει να πείσει το υπόλοιπο δίκτυο να υιοθετήσει τις αλλαγές, κάτι που είναι περισσότερο θέμα ψυχολογίας παρά μηχανικής λογισμικού.

Το παρακάτω μπορεί να ακούγεται παράλογο, όπως πολλά άλλα πράγματα σε αυτόν το χώρο, πιστεύω όμως ότι αληθεύει: Δεν πρόκειται να αλλάξεις το Bitcoin, το Bitcoin όμως θα αλλάξει εσένα.

“Το Bitcoin θα μας αλλάξει περισσότερο από όσο θα το αλλάξουμε εμείς.” -Marty Bent

Χρειάστηκε πολύς χρόνος για να συνειδητοποιήσω τη βαθύτητά του. Δεδομένου ότι το Bitcoin είναι απλώς λογισμικό και εξ ολοκλήρου ανοικτού κώδικα, μπορείτε απλά να αλλάξετε τα πράγματα κατά βούληση, σωστά; Λάθος. Πολύ λάθος. Δεν προκαλεί έκπληξη το γεγονός ότι ο δημιουργός του Bitcoin το γνώριζε πολύ καλά αυτό.

“Η φύση του Bitcoin είναι τέτοια ώστε από τη στιγμή που κυκλοφόρησε η έκδοση 0.1, ο σχεδιασμός του πυρήνα ήταν οριστικός για το υπόλοιπο της ζωής του.”
— Satoshi Nakamoto

Πολλοί άνθρωποι προσπάθησαν να αλλάξουν τη φύση του Bitcoin. Μέχρι στιγμής όλοι τους απέτυχαν. Ενώ υπάρχει μια ατελείωτη θάλασσα από Forks (παρακλάδια) και Altcoins, το δίκτυο του Bitcoin εξακολουθεί να κάνει τη δουλειά του, ακριβώς όπως την έκανε όταν ο πρώτος κόμβος συνδέθηκε στο δίκτυο. Μακροπρόθεσμα, τα Altcoins δεν θα έχουν καμία σημασία. Τα forks τελικά θα λιμοκτονήσουν και θα πεθάνουν. Το Bitcoin είναι αυτό που έχει σημασία. Όσο η θεμελιώδης κατανόηση των μαθηματικών ή/και της φυσικής δεν αλλάξει, το Bitcoin Honeybadger θα συνεχίσει να αδιαφορεί.

“Το Bitcoin είναι το πρώτο παράδειγμα μιας νέας μορφής ζωής. Ζει και αναπνέει στο διαδίκτυο. Ζει επειδή μπορεί να πληρώσει τους ανθρώπους για να το κρατήσουν ζωντανό. [...] Δεν μπορεί να αλλαχθεί. Δεν μπορείς να λογομαχήσεις μαζί του. Δεν μπορεί να παραβιαστεί. Δεν μπορεί να αλλοιωθεί. Δεν μπορεί να σταματήσει. [...] Εάν ένας πυρηνικός πόλεμος κατέστρεφε αύριο τον μισό μας πλανήτη, εκείνο θα συνέχιζε να ζει, αναλλοίωτο.” — Ralph Merkle

Η καρδιά του δικτύου του Bitcoin θα συνεχίσει να χτυπάει ακόμα και όταν θα έχουν σταματήσει πια οι δικές μας.

Η συνηθειοποίηση των παραπάνω με έκανε να αλλάξω πολύ περισσότερο απ' όσο θα μπορούσαν ποτέ τα περασμένα μπλοκ του Bitcoin Blockchain. Μου άλλαξε την προτίμησή μου για το χρόνο, την κατανόησή μου για τα οικονομικά, τις πολιτικές μου απόψεις και τόσα πολλά άλλα. Μπορεί ακόμα και να αλλάξει την διατροφή των ανθρώπων. Εάν όλα αυτά σας ακούγονται τρελά, είστε σε καλή παρέα. Όλα αυτά τρελά, κι όμως συμβαίνουν.

Το Bitcoin μου έμαθε ότι δεν θα αλλάξει. Εγώ θα αλλάξω.

Through the Looking-Glass

- [Bitcoin's Gravity: How idea-value feedback loops are pulling people in](#)
- [Proof of Life: Why Bitcoin is a Living Organism](#)
- [Lesson 18: Move slowly and don't break things](#)

Down the Rabbit Hole

- [There is no Bitcoin 2.0](#) by Pete Dushenski
- [DAOs, Democracy and Governance](#) by Ralph C. Merkle
- [Inside the World of the Bitcoin Carnivores — Why a small community of Bitcoin users is eating meat exclusively](#) by Jordan Pearson
- [Bitcoin is a Decentralized Organism](#) by Brandon Quittem
- [Bitcoin is a Social Creature](#) by Brandon Quittem
- [It's the settlement assurances, stupid](#) by Nic Carter
- [Technical Discussion on Bitcoin's Transactions and Scripts](#) by Satoshi Nakamoto, Gavin Andresen, and others
- [Marty's Bent — A daily newsletter highlighting signal in Bitcoin](#) by Marty Bent
- [👂 Tales From the Crypt](#) by Marty Bent
- [📖 Antifragile — Things That Gain From Disorder](#) by Nassim Nicholas Taleb

. . .

Σε γενικές γραμμές, η πρόοδος της τεχνολογίας φαίνεται να κάνει τα πράγματα πιο άφθονα. Όλο και περισσότεροι άνθρωποι έχουν τη δυνατότητα να απολαύσουν προϊόντα που παλαιότερα θεωρούνταν πολυτέλεια. Σύντομα, όλοι θα ζούμε σαν βασιλιάδες. Οι περισσότεροι από εμάς ήδη το κάνουν. Όπως έγραψε και ο Peter Diamandis στο Abundance: “Η τεχνολογία είναι ένας μηχανισμός που απελευθερώνει πόρους. Μπορεί να μετατρέψει το σπάνιο σε άφθονο.”

Το Bitcoin, μια προηγμένη τεχνολογία από μόνη της, σπάει αυτή την τάση και δημιουργεί ένα νέο αγαθό που είναι πραγματικά σπάνιο. Κάποιοι ακόμη ισχυρίζονται ότι είναι ένα από τα πιο σπάνια πράγματα στο σύμπαν. Η προσφορά δεν μπορεί να πληθωριστεί, όσο κόπο και αν δαπανήσει κάποιος στην προσπάθεια δημιουργίας περισσότερων.

“Μόνο δύο πράγματα είναι πραγματικά σπάνια: ο χρόνος και τα bitcoin.” — Saifedean Ammous

Παραδόξως, τα κάνει όλα αυτά μέσω ενός μηχανισμού αντιγραφής. Οι συναλλαγές μεταδίδονται, τα blocks προωθούνται, το διανεμημένο Ledger/βιβλίο ταμείου — καλά το μαντέψατε — διανέμεται. Όλα αυτά είναι απλά κομψά συνώνυμα της αντιγραφής. Το Bitcoin αντιγράφει τον εαυτό του σε όσο το δυνατόν περισσότερους υπολογιστές μπορεί, μέσω της παροχής κινήτρων σε άτομα που τρέχουν τα δικά τους Full Nodes και εξορύσσουν νέα block.


Όλο αυτό το σύστημα αντιγραφής δουλεύει θαυμάσια μεταξύ του σε μία συντονισμένη προσπάθεια να παραχθεί σπανιότητα.

Σε μια εποχή αφθονίας, το Bitcoin μου έμαθε τι σημαίνει πραγματική σπανιότητα.

Through the Looking-Glass

- Lesson 14: Sound money

Down the Rabbit Hole

- Modeling Bitcoin's Value with Scarcity by PlanB
- Bitcoin Can't Be Copied by Parker Lewis
- Presentation on The Bitcoin Standard by Saifedean Ammous
-  Misir Mahmudov on the Scarcity of Time and Bitcoin
TFTC#60 hosted by Marty Bent

- 🎧 [Plan B on Modelling Bitcoin's Scarcity through Stock-to-Flow Techniques](#)
SLP#67 hosted by Stephan Livera
- 🎧 [BTCDCAs on Dollar Cost Averaging Bitcoin](#)
BEC#20 hosted by Collin
- 🎧 [Misir Mahmudov on Bitcoin as Stored Time](#)
OTC#126 hosted by Pomp
- 📖 [Abundance — The Future is Better Than You Think](#) by Peter Diamandis
- 📖 [The Bitcoin Standard — The Decentralized Alternative to Central Banking](#) by Saifedean Ammous

. . .

Μάθημα 3: Αναπαραγωγή και τοπικότητα

Στη συνέχεια ακούστηκε μια θυμωμένη φωνή — το κουνέλι — “Πατ, Πατ! Που είσαι;”

Πέρα από την κβαντική μηχανική, η τοπικότητα δεν αποτελεί ζήτημα στον φυσικό κόσμο. Η ερώτηση “Πού είναι το X;” μπορεί να απαντηθεί με τρόπο που βγάζει νόημα, ανεξάρτητα αν το X είναι ένα άτομο ή ένα αντικείμενο. Στον ψηφιακό κόσμο, το ζήτημα του πού είναι κάτι, είναι δύσκολο αλλά όχι αδύνατον να απαντηθεί. Πού είναι τα e-mail σας, πραγματικά όμως; Μια κακή απάντηση θα ήταν “στο cloud”, το οποίο απλά είναι ο υπολογιστής κάποιου άλλου. Παρ’ όλα αυτά, εάν θέλατε να βρείτε κάθε συσκευή αποθήκευσης που έχει αποθηκευμένα τα μηνύματά σας, θα μπορούσατε, θεωρητικά, να την εντοπίσετε.

Στο Bitcoin, το “που” είναι *πραγματικά* ένα δύσκολο ερώτημα να απαντηθεί. Πού ακριβώς είναι τα bitcoin σας;

«Άνοιξα τα μάτια μου, κοίταξα γύρω μου και ρώτησα την αναπόφευκτη, την παραδοσιακή, την θλιβερά τετριμμένη μετεγχειρητική ερώτηση: « Πού είμαι; » -
Daniel Dennett

Το πρόβλημα είναι διττό: Κατ’ αρχάς, το κατανομημένο ledger κατανέμεται μέσω πλήρους αναπαραγωγής, που σημαίνει ότι το ledger βρίσκεται παντού. Δεύτερον, δεν υπάρχουν bitcoins. Όχι μόνο από φυσικής άποψης, αλλά και από τεχνικής.

Το Bitcoin καταγράφει ένα σύνολο μη δαπανημένων εξόδων συναλλαγής (unspent transaction outputs), χωρίς να χρειάζεται ποτέ να αναφερθεί σε κάποια οντότητα που αντιπροσωπεύει ένα bitcoin. Η ύπαρξη ενός bitcoin συμπεραίνεται εξετάζοντας το σύνολο των μη δαπανημένων εξόδων συναλλαγής και καλώντας κάθε είσοδο με 100 εκατομμύρια μονάδες βάσης ένα bitcoin.

“Πού βρίσκεται, αυτή τη στιγμή, υπό μεταφορά; [...] Πρώτον, δεν υπάρχουν bitcoins. Πραγματικά δεν υπάρχουν. Απλά δεν υφίστανται. Υπάρχουν καταχωρήσεις στο ledger, σε ένα ledger που διαμοιράζεται [...] Δεν υπάρχουν σε κάποια φυσική τοποθεσία. Ουσιαστικά, το ledger υπάρχει σε κάθε φυσική τοποθεσία. Η γεωγραφία δεν έχει νόημα εδώ — δεν πρόκειται να σε βοηθήσει στην ανακάλυψη της πολιτικής σου.» — Peter Van Valkenburgh

Τελικά, τι πραγματικά κατέχεις όταν λες “έχω ένα bitcoin” εάν δεν υπάρχουν bitcoins; Λοιπόν, θυμάσαι όλες αυτές τις παράξενες λέξεις που αναγκάστηκες να γράφεις όταν χρησιμοποίησες το πορτοφόλι σου; Όπως αποδεικνύεται, οι μαγικές αυτές λέξεις είναι τελικά αυτό που κατέχεις: ένα μαγικό ξόρκι που μπορεί να χρησιμοποιηθεί για να προσθέσεις μερικές καταχωρήσεις στο δημόσιο ledger — τα κλειδιά για να “μετακινήσεις” κάποια bitcoins. Αυτός είναι ο λόγος για τον οποίο, ουσιαστικά, τα ιδιωτικά σου κλειδιά τα bitcoins σου. Αν νομίζεις ότι τα έχω βγάλει όλα αυτά από το μυαλό μου, μην διστάσεις να μου στείλεις τα ιδιωτικά σου κλειδιά.

Το Bitcoin μου έμαθε ότι η τοπικότητα δεν είναι μία απλή υπόθεση.

Through the Looking-Glass

- [The Magic Dust of Cryptography: How digital information is changing our society](#)

Down the Rabbit Hole

- [Where Am I?](#) by Daniel Dennett
- 🎧 [Peter Van Valkenburg on Preserving the Freedom to Innovate with Public Blockchains](#)

WBD#49 hosted by Peter McCormack

Μάθημα 4: Το πρόβλημα της ταυτότητας

“Ποιά είσαι?” είπε η κάμπια.

Ο Νικ Κάρτερ, σαν φόρο τιμής στο κείμενο του Thomas Nagel “ What is it like to be a bat”, έγραψε ένα εξαιρετικό άρθρο το οποίο απαντά στην ακόλουθη ερώτηση: What is it like to be a bitcoin? Με έξοχο τρόπο δείχνει ότι τα ανοικτά, δημόσια blockchain γενικότερα, και πió συγκεκριμένα το Bitcoin, υποφέρουν υπό το ίδιο αίνιγμα με το πλοίο του Θησέα: ποιο Bitcoin είναι το πραγματικό Bitcoin;

“Παρατηρήστε μόνο πόσο μικρή παραμονή έχουν τα διάφορα συστατικά μέρη του Bitcoin. Ολόκληρος ο κώδικας βάσης έχει αναθεωρηθεί, τροποποιηθεί και επεκταθεί έτσι ώστε να μοιάζει ελάχιστα πια με την αρχική του έκδοση. [...] Το μητρώο στο οποίο αναγράφεται το ποιός κατέχει τι, το ίδιο το ledger δηλαδή, είναι ουσιαστικά το μοναδικό επιμένων χαρακτηριστικό του δικτύου [...]

Για να μπορέσει να θεωρηθεί κάτι πραγματικά πως δεν έχει ηγέτες, πρέπει να ξεχάσει κανείς την εύκολη λύση της ύπαρξης μιας οντότητας που μπορεί να χαρακτηρίζει μία αλυσίδα ως την μόνη αποδεκτή.” — Nic Carter

Φαίνεται ότι η πρόοδος της τεχνολογίας μας υποχρεώνει να πάρουμε αυτά τα φιλοσοφικά ζητήματα στα σοβαρά. Αργά ή γρήγορα, τα αυτοκατευθυνόμενα αυτοκίνητα θα χρειαστεί να αντιμετωπίσουν πραγματικές εκδοχές του προβλήματος του τρόλεϊ, αναγκάζοντάς τα να λάβουν ηθικές αποφάσεις σχετικά με το ποιές ζωές έχουν σημασία και ποιές όχι.

Τα κρυπτονομίσματα, ειδικά από το πρώτο αμφιλεγόμενο hard-fork, μας ωθούν να σκεφτούμε και να συμφωνήσουμε σχετικά με τη μεταφυσική της ταυτότητας. Είναι

ενδιαφέρον, ότι τα δύο μεγαλύτερα παραδείγματα που έχουμε μέχρι στιγμής έχουν οδηγήσει σε δύο διαφορετικές απαντήσεις. Την 1η Αυγούστου 2017, το Bitcoin χωρίστηκε σε δύο στρατόπεδα. Η αγορά αποφάσισε ότι η αναλλοίωτη αλυσίδα είναι το αυθεντικό Bitcoin. Ένα χρόνο νωρίτερα, στις 25 Οκτωβρίου 2016, το Ethereum χωρίστηκε σε δύο στρατόπεδα. Η αγορά αποφάσισε ότι η αλλοιωμένη αλυσίδα είναι το αρχικό Ethereum.

Υπο σωστή αποκέντρωση, τα ερωτήματα που θέτει το *Πλοίο του Θησέα* θα πρέπει να απαντώνται διαρκώς για όσο διάστημα υπάρχουν αυτά τα δίκτυα μεταφοράς αξίας.

Το Bitcoin μου έμαθε ότι η αποκέντρωση και η ταυτότητα δεν συνάδουν μεταξύ τους.

Down the Rabbit Hole

- [What Is It Like to be a Bat?](#) by Thomas Nagel
- [What is it like to be a Bitcoin?](#) by Nic Carter
- [Ship of Theseus](#) by Wikipedia Authors
- [Trolley Problem](#) by Wikipedia Authors
- 🎧 [Luke Dashjr on 300k Blocks and Full Nodes](#)
WBD#109 hosted by Peter McCormack
- 🎧 [Giacomo Zucco on Bitcoin's Identity and Copycats](#)
SLP#75 hosted by Stephan Livera

. . .

Μάθημα 5: Μία άψογη σύλληψη

“Δεν έχουν πια κεφάλια,” απάντησαν φωναχτά οι στρατιώτες...

Όλοι αγαπούν μια καλή ιστορία. Η ιστορία γέννησης του Bitcoin είναι συναρπαστική και οι λεπτομέρειες αυτού είναι πιο σημαντικές από ό,τι μπορεί να σκέφτεται κανείς αρχικά. Ποιος είναι ο Satoshi Nakamoto; Ήταν ένα άτομο ή μια ομάδα ανθρώπων; Ήταν γυναίκα; Εξωγήινος χρονοταξιδιώτης ή προηγμένο AI; Αφήνωτας στην άκρη τις εξωπραγματικές θεωρίες, πιθανότατα δεν θα μάθουμε πότε. Και αυτό είναι σημαντικό.

Ο Satoshi επέλεξε να είναι ανώνυμος. Φύτεψε τον σπόρο του Bitcoin. Παρέμεινε για αρκετό καιρό για να βεβαιωθεί ότι το δίκτυο δεν θα πεθάνει στη βρεφική ηλικία του. Και τότε εξαφανίστηκε.

Κάτι που θα μπορούσε να φανεί ως ένα περίεργο κόλπο ανωνυμίας είναι ειλικρινά κρίσιμο για ένα πραγματικά αποκεντρωμένο σύστημα. Κανένας κεντρικός έλεγχος. Καμία κεντρική αρχή. Κανένας εφευρέτης. Κανείς που μπορεί να εκδιωχθεί, να βασανισθεί ή να εκβιασθεί. Μια άφογη σύλληψη της τεχνολογίας.

“Ένα από τα σπουδαιότερα πράγματα που έκανε ο Satoshi, ήταν να εξαφανιστεί.” — [Jimmy Song](#)


Από την ημέρα γέννησης του Bitcoin μέχρι σήμερα έχουν δημιουργηθεί χιλιάδες άλλα κρυπτονομίσματα. Κανένας από αυτούς τους κλώνους δεν έχει την ιστορία γέννησής του. Εάν θέλετε να αντικαταστήσετε το Bitcoin, θα πρέπει να υπερβείτε την ιστορία γέννησής του. Σε έναν πόλεμο ιδεών, οι αφηγήσεις καθορίζουν την επιβίωση.

“Ο χρυσός μορφοιήθηκε πρώτα ως κόσμημα και χρησιμοποιήθηκε ως μέσο ανταλλαγής πάνω από 7.000 χρόνια πριν. Η μαγευτική λάμψη του χρυσού οδήγησε στο να θεωρηθεί δώρο από τους θεούς.” — [Gold: The Extraordinary Metal](#)

Όπως και ο χρυσός στην αρχαιότητα, το Bitcoin μπορεί να θεωρηθεί δώρο από τους θεούς. Σε αντίθεση με τον χρυσό, η προέλευση του Bitcoin παραείναι ανθρώπινη. Και αυτή τη φορά, γνωρίζουμε ποιοί είναι οι θεοί ανάπτυξης και συντήρησης: άνθρωποι σε όλο τον κόσμο, ανώνυμοι ή μη.

Το Bitcoin μου έμαθε ότι οι αφηγήσεις είναι σημαντικές.

Down the Rabbit Hole

- [Catallaxy — the origins of Bitcoin, innovation and spontaneous order](#) by Francis Pouliot
- [Why Bitcoin is Different](#) by Jimmy Song
- [Gold — The Extraordinary Metal](#) by the Austrian Mint
-  [The Black Swan — The Impact of the Highly Improbable](#) by Nassim Nicholas Taleb

“Με συγχωρείτε?” είπε το ποντίκι, συνοφριώνοντας, αλλά πολύ ευγενικά, “μιλήσατε;”

Το Bitcoin είναι μια ιδέα. Μια ιδέα η οποία, στη σημερινή της μορφή, είναι η εκδήλωση ενός μηχανήματος που λειτουργεί καθαρά με κείμενο. Κάθε πτυχή του Bitcoin είναι κείμενο: Το whitepaper είναι κείμενο. Το λογισμικό που εκτελείται από τους κόμβους του είναι κείμενο. Το ledger είναι κείμενο. Οι συναλλαγές είναι κείμενο. Τα δημόσια και ιδιωτικά κλειδιά είναι κείμενο. Κάθε πτυχή του Bitcoin είναι κείμενο και ως εκ τούτου ισοδυναμεί με ομιλία.

“Το Κογκρέσο δεν θα θέσει κανένα νόμο για τη θέσπιση ή τον περιορισμό της δημιουργίας θρησκείας ή για περιορισμό της ελευθερίας του λόγου, του Τύπου ή τον περιορισμό του δικαιώματος του λαού να συγκεντρώνεται ειρηνικά και να ζητάει από την κυβέρνηση την αποκατάσταση των παραπτόνων του.”
— First Amendment to the United States Constitution

Παρόλο που δεν έχει δοθεί ακόμα η τελική μάχη των Κρύπτο-Πολέμων, θα είναι πολύ δύσκολο να ποινικοποιηθεί μια ιδέα, πόσο μάλλον μια ιδέα που βασίζεται στην ανταλλαγή μηνυμάτων κειμένου. Κάθε φορά που μια κυβέρνηση επιχειρεί να απαγορεύσει το κείμενο ή την ομιλία, κατηγορίζουμε μια πορεία παραλογισμού, η οποία αναπόφευκτα οδηγεί σε αποτροπιασμούς όπως οι παράνομοι αριθμοί και οι παράνομοι πρώτοι αριθμοί.

Όσο υπάρχει ένα μέρος του κόσμου όπου ο λόγος είναι ελεύθερος, με την έννοια της *Ελευθερίας*, τόσο το Bitcoin είναι ασταμάτητο.

“Δεν υπάρχει κανένα σημείο σε οποιαδήποτε συναλλαγή του Bitcoin όπου το Bitcoin παύει να είναι κείμενο. Όλα είναι κείμενο, όλη την ώρα. [...]

Το Bitcoin είναι κείμενο. Το Bitcoin είναι ομιλία. Δεν μπορεί να ρυθμιστεί σε μια ελεύθερη χώρα όπως οι

ΗΠΑ με εγγυημένα αναφαίρετα δικαιώματα και ένα First Amendment που αποκλείει ρητά την κρατική εποπτοία στην δημοσίευση.“ — Beautyon

Το Bitcoin μου έμαθε ότι σε μια ελεύθερη κοινωνία, η ελευθερία του λόγου και το ελεύθερο λογισμικό είναι ασταμάτητα.

Through the Looking-Glass

- The Magic Dust of Cryptography: How digital information is changing our society
- The Rise of the Sovereign Individual: How power is re-aligning itself in an internet-native world

Down the Rabbit Hole

- Why America Can't Regulate Bitcoin by Beautyon
- Why Bitcoin Matters for Freedom by Alex Gladstein
- A most peaceful revolution by Nic Carter
- Crypto Wars by Wikipedia Contributors
- Illegal Numbers by Wikipedia Contributors
- Illegal Primes by Wikipedia Contributors
- First Amendment to the United States Constitution by Wikipedia Contributors
- 🎧 Jameson Lopp on Freedom-Enabling Technologies like Bitcoin
TFTC#29 hosted by Marty Bent
- 🎧 Alex Gladstein on Bitcoin's Role in the Fight for Human Rights
TFTC#76 hosted by Marty Bent

. . .

Μάθημα 7: Τα όρια της γνώσης

Κάτω, κάτω, κάτω. Δεν θα τελειώνει ποτέ αυτή η πτώση;

Η είσοδος στο Bitcoin είναι μια συγκλονιστική εμπειρία. Νόμιζα ότι ήξερα πράγματα. Νόμιζα ότι ήμουν μορφωμένος. Νόμιζα ότι τουλάχιστον ήξερα την πληροφορική μου.

Την μελετώ εδώ και χρόνια, οπότε θα πρέπει να γνωρίζω τα πάντα για τις ψηφιακές υπογραφές, τα hashes, την κρυπτογράφηση, τη λειτουργική ασφάλεια(OPSEC) και τα δίκτυα, σωστά;

Λάθος.

Η εκμάθηση όλων των βασικών στοιχείων που κάνουν το Bitcoin να λειτουργεί είναι δύσκολη. Η πλήρης κατανόησή τους είναι οριακά αδύνατη.

“Κανείς δεν έχει βρει το τέλος του λαγουμιού του Bitcoin.” — Jameson Lopp

Η λίστα με τα βιβλία που θέλω να διαβάσω επεκτείνεται πιο γρήγορα απ' ό,τι θα μπορούσα να τα διαβάσω. Η λίστα με τις επιστημονικές δημοσιεύσεις και τα άρθρα για ανάγνωση είναι σχεδόν ατελείωτη. Υπάρχουν περισσότερα podcast για όλα αυτά τα θέματα από ό,τι θα μπορούσα ποτέ να ακούσω. Σε κάνει πραγματικά πιο ταπεινό. Επιπλέον, το Bitcoin εξελίσσεται και είναι σχεδόν αδύνατον να παραμείνεις ενήμερος με τον επιταχυνόμενο ρυθμό καινοτομίας. Δεν έχει καθαρίσει ακόμα το πεδίο στο επίπεδο του πρώτου στρώματος, και άτομα έχουν ήδη χτίσει το δεύτερο στρώμα και εργάζονται στο τρίτο.

Το Bitcoin μου έμαθε ότι ξέρω πολύ λίγα για σχεδόν οτιδήποτε. Μου έμαθε ότι αυτό το λαγούμι είναι απύθμενο.

Through the Looking-Glass

- [Bitcoin-Resources.com](#) by Gigi

Down the Rabbit Hole

- [Bitcoin Information & Resources](#) by Jameson Lopp
- [Bitcoin Literature](#) by Satoshi Nakamoto Institute
- [Educational Resources](#) by Bitcoin Only
- [Bitcoin Intro](#) by 6102bitcoin
- 🎧 [Matt Corallo on how Everyone is Ignorant when it comes to Bitcoin](#)
TFTC#7 hosted by Marty Bent
- 🎧 [Ben Prentice on the Bitcoin Spectrum](#)
BEC#14 hosted by Collin
- 🎧 [Yan Pritzker on Inventing Bitcoin and Bitcoin Education](#)
BRF#16 hosted by John Vallis

21 Μαθήματα — Κεφάλαιο II: Οικονομικά



nikos Jan 28, 2020 · 31 min read

Μετάφραση: [niclick](#)

. . .

Κεφάλαιο II: Οικονομικά

Μία μεγάλη τριανταφυλλιά βρισκόταν κοντά στην είσοδο του κήπου: τα τριαντάφυλλά της ήταν λευκά, αλλά υπήρχαν και τρεις κηπουροί μαζί της, απασχολημένοι στο να τα ζωγραφίζουν κόκκινα. Αυτό φάνηκε πολύ περίεργο στην Αλίκη...

Το χρήμα δεν φυτρώνει στα δέντρα. Το να πιστεύουμε ότι το κάνει είναι ανόητο και οι γονείς μας βεβαιώνονται ότι το γνωρίζουμε, επαναλαμβάνοντας το ρητό αυτό σαν μάντρα. Μας ενθαρρύνουν να χρησιμοποιήσουμε τα χρήματά μας σοφά, να μην τα ξοδεύουμε επιπόλαια και να τα βάζουμε στην άκρη σε καλές εποχές για να μας βοηθήσουν στις κακές. Το χρήμα, εξάλλου, δεν φυτρώνει στα δέντρα.

Το Bitcoin μου δίδαξε περισσότερα για τα χρήματα απ' όσα πίστευα ότι θα χρειαζόταν ποτέ να μάθω. Χάρη σε αυτό, αναγκάστηκα να εξερευνήσω την ιστορία του χρήματος, τις τράπεζες, τις διάφορες σχολές οικονομικής σκέψης και πολλά άλλα πράγματα. Ο στόχος μου να κατανοήσω το Bitcoin με έκανε να ακολουθήσω μια πληθώρα από μονοπάτια, μερικά από τα οποία προσπαθώ να εξερευνήσω σε αυτή τη σειρά.

Στα πρώτα επτά μαθήματα συζητήθηκαν μερικές από τις φιλοσοφικές ερωτήσεις που θίγει το Bitcoin. Τα επόμενα επτά μαθήματα θα ρίξουν μια πιο προσεκτική ματιά στο χρήμα και τα οικονομικά.

- Μάθημα 8: Οικονομική Άγνοια
- Μάθημα 9: Πληθωρισμός
- Μάθημα 10: Αξία
- Μάθημα 11: Χρήμα
- Μάθημα 12: Η ιστορία και πτώση του χρήματος
- Μάθημα 13: Η παραφροσύνη των κλασματικών αποθεμάτων
- Μάθημα 14: Υγιές χρήμα

Επαναλαμβάνω, η εξέταση θα μπορέσει να γίνει μόνο επιφανειακά. Το Bitcoin δεν είναι μόνο φιλόδοξο αλλά επίσης αντικείμενο με ευρύ πεδίο εφαρμογής, καθιστώντας αδύνατη τη κάλυψη όλων των σχετικών θεμάτων σε ένα μόνο μάθημα, δοκίμιο, άρθρο ή βιβλίο. Αμφιβάλλω εάν κάτι τέτοιο είναι καν δυνατόν να συμβεί.

Το Bitcoin είναι μια νέα μορφή χρήματος, το οποίο καθιστά τη μάθηση των οικονομικών πρωτίστης σημασίας. Ασχολούμενο με τη φύση της ανθρώπινης δράσης και τις αλληλεπιδράσεις των οικονομικών παραγόντων, τα οικονομικά είναι ίσως ένα από τα μεγαλύτερα και πιο συγκεχυμένα κομμάτια παζλ του Bitcoin.

Επαναλαμβάνω, αυτά τα μαθήματα είναι μια εξερεύνηση των διαφόρων πραγμάτων που έχω μάθει μέσα από το Bitcoin. Πρόκειται για μια προσωπική αντανάκλαση του ταξιδιού μου πέφτοντας στο λαγούμι. Μην έχοντας κάποιο υπόβαθρο στα οικονομικά, είμαι σίγουρα έξω από τη ζώνη άνεσής μου, με ιδιαίτερη επίγνωση ότι κάθε κατανόηση που μπορεί να έχω να είναι ελλιπής. Θα βάλω τα δυνατά μου για να περιγράψω όσα έχω μάθει, ακόμη και με τον κίνδυνο να φανώ ανόητος. Ούτως ή άλλως, ακόμα προσπαθώ να απαντήσω στην ερώτηση: “Τι μάθατε από το Bitcoin;”

Μετά την εξέταση των επτά μαθημάτων μέσω του φακού της φιλοσοφίας, ας χρησιμοποιήσουμε τον φακό των οικονομικών για να δούμε άλλα επτά. Η Economy Class είναι το μόνο που μπορώ να προσφέρω αυτή τη φορά. Τελικός προορισμός: **υγιή χρήματα.**

. . .

Μάθημα 8: Οικονομική Άγνοια

Και πόσο αδαή μικρό κοριτσάκι θα με θεωρήσει για να ρωτάω! Όχι, θα ήταν απαράδεκτο να ρωτήσω: ίσως να το δω γραμμένο κάπου.

Ένα από τα πιο εκπληκτικά πράγματα, για εμένα, ήταν το μέγεθος των χρηματοοικονομικών, των οικονομικών και της ψυχολογίας που απαιτούνται για να κατανοηθεί αυτό που με μια πρώτη ματιά φαίνεται να είναι ένα καθαρά *τεχνικό* σύστημα — ένα δίκτυο υπολογιστών. Παραφράσοντας έναν μικρόσωμο τύπο με τριχωτά πόδια: “Είναι ένα επικίνδυνο εγχείρημα, Frodo, η είσοδος στο Bitcoin. Διαβάζεις το *Whiterpaper*, και αν δεν κρατιέσαι καλά από κάπου, δεν υπάρχει τρόπος να γνωρίζεις μέχρι πού μπορεί να παρασυρθείς.”

Για να κατανοήσεις ένα νέο νομισματικό σύστημα, πρέπει να εξοικειωθείς με το παλιό. Άρχισα πολύ σύντομα να συνειδητοποιώ ότι η ποσότητα της οικονομικής εκπαίδευσης που απολάμβανα εντός του εκπαιδευτικού συστήματος ήταν ουσιαστικά *μηδενική*.

Όπως ένα πεντάχρονο παιδί, έτσι κι εγώ άρχισα να αναρωτιέμαι πολλές ερωτήσεις: Πώς λειτουργεί το τραπεζικό σύστημα; Πώς λειτουργεί το χρηματιστήριο; Τι είναι το παραστατικό χρήμα; Τι είναι το κλασικό χρήμα; Γιατί υπάρχει τόσο μεγάλο χρέος; Πόσο χρήμα τυπώνεται πραγματικά και ποιός το αποφασίζει;

Μετά από έναν μικρό πανικό απλά και μόνο από το μέγεθος της άγνοιάς μου, καθησυχάστηκα όταν συνειδητοποίησα ότι βρισκόμουν μεταξύ ομοίων μου.

“Δεν είναι ειρωνικό το γεγονός ότι το Bitcoin μου έχει διδάξει περισσότερα για τα χρήματα από όλα αυτά τα χρόνια που έχω ξοδέψει δουλεύοντας για τα χρηματοπιστωτικά ιδρύματα; ... συμπεριλαμβανομένης της έναρξης της καριέρας μου σε μια κεντρική τράπεζα” — [aarontaycc](#)

“Έχω μάθει περισσότερα για τα οικονομικά, την οικονομία, την τεχνολογία, την κρυπτογραφία, την ανθρώπινη ψυχολογία, την πολιτική, τη θεωρία παιγνίων, τη νομοθεσία και τον εαυτό μου τους τελευταίους τρεις μήνες στον χώρο του crypto σε σχέση με τα τελευταία τρισήμιση χρόνια κολλεγίου” — [bitcoindunny](#)

Αυτές είναι μόνο δύο από τις πολλές ομολογίες σε όλο το Twitter. Το Bitcoin, όπως εξετάστηκε στο Μάθημα 1, είναι ένα ζωντανό πράγμα. Ο Mises ισχυρίστηκε ότι τα οικονομικά είναι επίσης ένα ζωντανό πράγμα. Και όπως όλοι γνωρίζουμε από προσωπική εμπειρία, τα έμβια όντα είναι εγγενώς δυσνόητα.

“Ένα επιστημονικό σύστημα είναι ένας μόνο σταθμός σε μια αδιάκοπα εξελισσόμενη αναζήτηση για γνώση. Είναι αναγκαστικά επηρεασμένο από την εγγενή ανεπάρκεια εντός κάθε ανθρώπινης προσπάθειας. Αλλά η αναγνώριση αυτών των γεγονότων δεν σημαίνει ότι τα σημερινά οικονομικά είναι οπισθοδρομικά. Σημαίνει απλώς ότι τα οικονομικά είναι ένα ζωντανό πράγμα — και το να ζεις συνεπάγεται τόσο με ατέλεια όσο και αλλαγή.” — Ludwig von Mises

Όλοι μας διαβάζουμε στις ειδήσεις για τις διάφορες οικονομικές κρίσεις, αναρωτιόμαστε για το πώς λειτουργούν αυτά τα μεγάλα προγράμματα διάσωσης και απορροούμε με το γεγονός ότι κανείς δεν φαίνεται να θεωρείται υπεύθυνος για ζημιές που ανέρχονται στα τρισεκατομμύρια. Ο προβληματισμός μου αυτός συνεχίζει να υπάρχει, τουλάχιστον όμως έχω αρχίσει να παίρνω μια γενική ιδέα των όσων συμβαίνουν στον κόσμο των χρηματοοικονομικών.

Μερικοί άνθρωποι μάλιστα φτάνουν μέχρι και να αποδώσουν τη γενική άγνοια αυτών των θεμάτων σε συστημική, εσκεμμένη άγνοια. Ενώ η ιστορία, η φυσική, η βιολογία, τα μαθηματικά και οι γλώσσες είναι όλα μέρος της εκπαίδευσής μας, ο κόσμος του χρήματος και του χρηματοπιστωτικού τομέα, με μεγάλη έκπληξη, διερευνάται μόνο επιφανειακά έως και καθόλου. Αναρωτιέμαι αν οι άνθρωποι θα εξακολουθούσαν να είναι πρόθυμοι να συσσορεύουν τόσο χρέος όσο κάνουν σήμερα, εάν όλοι εκπαιδεύονταν στον προσωπικό οικονομικό προγραμματισμό και στη λειτουργία του χρήματος και του χρέους. Έπειτα αναρωτιέμαι πόσες στρώσεις αλουμινίου φτιάχνουν ένα αποτελεσματικό καπέλο αλουμινόχαρτου. Πιθανώς τρεις.

“Αυτά τα κραχ, αυτά τα προγράμματα διάσωσης, δεν είναι τυχαία. Ούτε είναι τυχαίο το γεγονός ότι δεν

υπάρχει χρηματοοικονομική εκπαίδευση στο σχολείο [...] Είναι προμελετημένο. Ακριβώς όπως πριν από τον εμφύλιο πόλεμο ήταν παράνομο να εκπαιδεύσεις έναν σκλάβο, έτσι δεν μας επιτρέπεται να μαθαίνουμε για τα χρήματα στο σχολείο. “ — Robert Kiyosaki

Όπως και στον Μάγο του Οζ, μας λένε να μην δώσουμε προσοχή στον άνθρωπο στο παρασκήνιο. Σε αντίθεση με τον Μάγο του Οζ, έχουμε πραγματική μαγεία τώρα: ένα ανθεκτικό στη λογοκρισία, ανοιχτό, χωρίς σύνορα δίκτυο μεταφοράς αξίας. Δεν υπάρχει παρασκήνιο και η μαγεία είναι ορατή σε όλους.

Το Bitcoin μου έμαθε να κοιτάζω το παρασκήνιο και να αντιμετωπίζω την χρηματοοικονομική μου άγνοια.

Down the Rabbit Hole

- [Why the Rich are Getting Richer](#) by Robert Kiyosaki
- 🎧 [Stephan Livera — Intro to Bitcoin Austrian thought](#)
SLP#71 hosted by Stephan Livera
- 🎧 [Paranoid Bull on the World's Current Disconnection from Reality](#)
TFTC#85 hosted by Marty Bent
- 📖 [Economic Depressions — Their Cause and Cure](#) by Murray N. Rothbard
- 📖 [Human Action](#) by Ludwig von Mises

. . .

Μάθημα 9: Πληθωρισμός

Αγαπητή μου, εδώ πρέπει να τρέξουμε όσο πιο γρήγορα μπορούμε, απλά και μόνο για να παραμείνουμε στη θέση μας. Και αν επιθυμείς να πας οπουδήποτε, πρέπει να τρέξεις δύο φορές πιο γρήγορα.

Η προσπάθειά μου να κατανοήσω το νομισματικό πληθωρισμό και πώς ένα μη πληθωριστικό σύστημα όπως το Bitcoin μπορεί να αλλάξει τον τρόπο με τον οποίο λειτουργούμε, ήταν το σημείο εκκίνησής μου στην εξερεύνηση των οικονομικών. Ήξερα ότι ο πληθωρισμός ήταν ο ρυθμός με τον οποίο δημιουργείται το νέο χρήμα, πέρα από αυτό όμως δεν γνώριζα κάτι παραπάνω.

Ενώ ορισμένοι οικονομολόγοι υποστηρίζουν ότι ο πληθωρισμός κάνει καλό, άλλοι ισχυρίζονται ότι το «σκληρό» χρήμα που δεν μπορεί να πληθωριστεί εύκολα — όπως είχαμε στις μέρες του χρυσού κανόνα— είναι απαραίτητο για μια υγιή οικονομία. Το Bitcoin, έχοντας σταθερή προσφορά 21 εκατομμυρίων, συμφωνεί με το δεύτερο στρατόπεδο.

Συνήθως, οι επιπτώσεις του πληθωρισμού δεν είναι άμεσα προφανείς. Ανάλογα με το ρυθμό πληθωρισμού (καθώς και άλλους παράγοντες) ο χρόνος μεταξύ αιτίας και αποτελέσματος μπορεί να είναι αρκετά χρόνια. Όχι μόνο αυτό, αλλά ο πληθωρισμός επηρεάζει διαφορετικές ομάδες ανθρώπων περισσότερο από άλλες. Όπως επισημαίνει ο Henry Hazlitt στο *Economics in One Lesson*: “Η τέχνη των οικονομικών συνίσταται στην εξέταση όχι μόνο των άμεσων, αλλά και των μακροπρόθεσμων αποτελεσμάτων οποιασδήποτε πράξης ή πολιτικής. Συνίσταται στον εντοπισμό των συνεπειών της πολιτικής αυτής όχι μόνο για μια ομάδα αλλά για όλες τις ομάδες.”

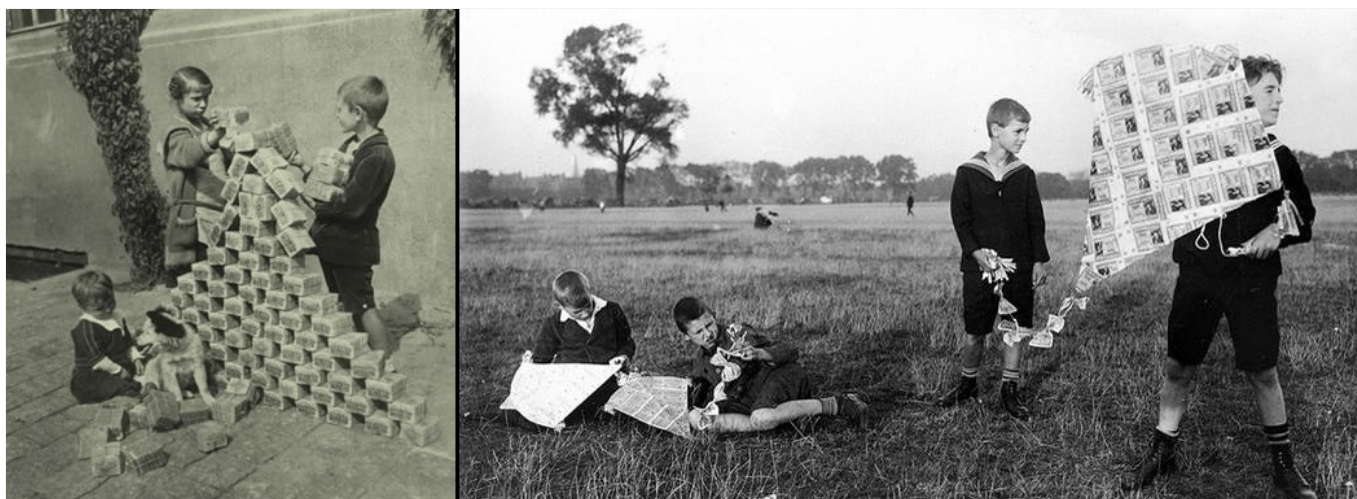
Μία από τις προσωπικές μου στιγμές αναλαμπής ήταν η συνειδητοποίηση ότι η έκδοση νέων νομισμάτων — η εκτύπωση περισσότερων χρημάτων — είναι μια εντελώς διαφορετική οικονομική δραστηριότητα από όλες τις άλλες. Ενώ τα πραγματικά αγαθά και οι πραγματικές υπηρεσίες παράγουν πραγματική αξία για τους πραγματικούς ανθρώπους, στην ουσία η εκτύπωση χρημάτων κάνει το αντίθετο: αφαιρεί αξία από όλους όσους κρατούν το νόμισμα που πληθωρίζεται.

“Ο απλός πληθωρισμός — δηλαδή η απλή έκδοση περισσότερων χρημάτων, με συνέπεια υψηλότερων μισθών και τιμών — μπορεί να μοιάζει με δημιουργία μεγαλύτερης ζήτησης. Αλλά όσον αφορά την πραγματική παραγωγή και την ανταλλαγή πραγματικών αντικειμένων, δεν είναι.” — Henry Hazlitt

Η καταστροφική δύναμη του πληθωρισμού καθίσταται εμφανής μόλις ο λιγοστός πληθωρισμός μετατραπεί σε πολύς. Εάν τα χρήματα υπερπληθωριστούν, τα πράγματα γίνονται άσχημα πραγματικά γρήγορα. Καθώς το πληθωριζόμενο νόμισμα διαλύεται, θα αποτύχει να αποθηκεύει αξία μέσα στον χρόνο και οι άνθρωποι θα σπεύσουν να αποκτήσουν οποιαδήποτε αγαθά επιτελούν αυτή τη λειτουργία.

Μια ακόμα συνέπεια του υπερπληθωρισμού είναι ότι όλα τα χρήματα που έχουν αποταμιέψει οι άνθρωποι κατά τη διάρκεια της ζωής τους, ουσιαστικά θα

εξαφανιστούν. Τα χαρτονομίσματα στο πορτοφόλι σου φυσικά θα είναι ακόμα εκεί. Αλλά θα είναι ακριβώς αυτό: άχρηστο χαρτί.



Υπερπληθωρισμός στην Δημοκρατία της Βαϊμάρης (1921–1923)

Το χρήμα χάνει επίσης σε αξία με τον λεγόμενο “ήπιος” πληθωρισμό. Αυτό συμβαίνει τόσο αργά ώστε οι περισσότεροι άνθρωποι δεν παρατηρούν τη μείωση της αγοραστικής τους δύναμης. Μόλις ξεκινήσουν να λειτουργούν οι μηχανές εκτύπωσης, το νόμισμα μπορεί να πληθωριστεί εύκολα και αυτό που ήταν κάποτε ήπιος πληθωρισμός μπορεί με το πάτημα ενός κουμπιού να μετατραπεί σε υψηλό. Όπως ανέφερε ο Friedrich Hayek σε ένα από τα δοκίμιά του, ο ήπιος πληθωρισμός συνήθως οδηγεί σε πλήρη πληθωρισμό.

“Ο ‘ήπιος’ σταθερός πληθωρισμός δεν μπορεί να βοηθήσει — μπορεί να οδηγήσει μόνο σε πλήρη πληθωρισμό.” — Friedrich Hayek

Ο πληθωρισμός είναι ιδιαίτερα ύπουλος, καθώς ευνοεί όσους είναι πιο κοντά στα εκτυπωτήρια. Απαιτείται χρόνος για να κυκλοφορήσουν τα νεοαφιχθέντα χρήματα και να προσαρμοστούν οι τιμές, οπότε αν είστε σε θέση να αποκτήσετε περισσότερα χρήματα πριν υποτιμηθούν αυτά των υπολοίπων, θα βρίσκεστε ένα βήμα μπροστά από την πληθωριστική καμπύλη. Αυτός είναι και ο λόγος για τον οποίο ο πληθωρισμός μπορεί να θεωρηθεί ως κρυμμένος φόρος επειδή τελικά οι κυβερνήσεις επωφελούνται από αυτόν ενώ όλοι οι υπόλοιποι καταλήγουν να πληρώνουν το τίμημα.

“Δεν νομίζω ότι είναι υπερβολή να πούμε ότι η ιστορία είναι σε μεγάλο βαθμό μια ιστορία πληθωρισμού και συνήθως πληθωρισμών που έχουν σχεδιαστεί από τις

κυβερνήσεις για το κέρδος των κυβερνήσεων”. —

Friedrich Hayek

Μέχρι στιγμής, όλα τα κυβερνητικά ελεγχόμενα νομίσματα έχουν τελικά αντικατασταθεί ή έχουν καταρρεύσει εντελώς. Ανεξάρτητα από το πόσο μικρός είναι ο ρυθμός πληθωρισμού, η “σταθερή” ανάπτυξη είναι απλώς ένας άλλος τρόπος να λέμε εκθετική ανάπτυξη. Στη φύση, όπως και στην οικονομία, όλα τα συστήματα που αναπτύσσονται εκθετικά θα πρέπει τελικά να σταθεροποιηθούν ή να υποστούν καταστροφική κατάρρευση.

“Δεν μπορεί να συμβεί στη χώρα μου”, είναι πιθανώς αυτό που σκέφτεστε. Δεν το σκέφτεστε όμως αν είστε από τη Βενεζουέλα, η οποία σήμερα υποφέρει από υπερπληθωρισμό. Με ρυθμό πληθωρισμού άνω του 1 εκατομμυρίου τοις εκατό, τα χρήματα είναι ουσιαστικά άχρηστα.

Μπορεί να μην συμβεί τα επόμενα δύο χρόνια ή στο συγκεκριμένο νόμισμα που χρησιμοποιείται στη χώρα σας. Αλλά μια ματιά στη λίστα των ιστορικών νομισμάτων δείχνει ότι θα συμβεί αναπόφευκτα στην πάροδο ενός αρκετά μεγάλου χρονικού διαστήματος. Θυμάμαι και χρησιμοποίησα πολλά από αυτά που αναφέρονται στη λίστα: το αυστριακό σίλιγκ, το γερμανικό μάρκο, την ιταλική λίρα, το γαλλικό φράγκο, την ιρλανδική λίρα, το κροατικό δηνάριο κλπ. Η γιαγιά μου χρησιμοποίησε ακόμη και την αυστρο-ουγγρική κορώνη. Με την πάροδο του χρόνου, τα νομίσματα που χρησιμοποιούνται σήμερα θα μετακινούνται αργά αλλά σταθερά στα αντίστοιχα νεκροταφεία τους. Θα υπερπληθωριστούν ή θα αντικατασταθούν. Σύντομα θα αποτελούν ιστορικά νομίσματα. Θα τα καταστήσουμε παρωχημένα.

“Η ιστορία έχει δείξει ότι οι κυβερνήσεις αναπόφευκτα θα υποκύψουν στον πειρασμό του πληθωρισμού της προσφοράς χρήματος.” — Saifedean Ammous

Γιατί διαφέρει το Bitcoin; Σε αντίθεση με τα κυβερνητικά καθορισμένα νομίσματα, τα νομισματικά αγαθά που δεν ρυθμίζονται από τις κυβερνήσεις αλλά από τους νόμους της φυσικής τείνουν να επιβιώνουν και να διατηρούν την αντίστοιχη αξία τους με την πάροδο του χρόνου. Το καλύτερο παράδειγμα μέχρι στιγμής είναι ο χρυσός, ο οποίος όπως δείχνει το εύστοχο Gold to Decent-Suit Ratio, κρατά την αξία του εκατοντάδες ή και χιλιάδες χρόνια. Ίσως να μην είναι απόλυτα “σταθερός” — μια αμφισβητήσιμη ιδέα καταρχάς— αλλά η αξία που κρατάει θα είναι τουλάχιστον της ίδιας τάξης μεγέθους.

Εάν ένα νομισματικό αγαθό ή νόμισμα διατηρεί την αξία του με την πάροδο του χρόνου και του χώρου, θεωρείται ότι είναι *σκληρό*. Εάν δεν μπορεί να διατηρήσει την αξία του, επειδή φθείρεται εύκολα ή πληθωρίζεται, θεωρείται *μαλακό* νόμισμα. Η έννοια της σκληρότητας είναι απαραίτητη για την κατανόηση του Bitcoin και αξίζει να εξεταστεί εις βάθος. Θα επιστρέψουμε σε αυτή στο τελευταίο οικονομικό μάθημα: υγιές χρήμα.




Καθώς όλο και περισσότερες χώρες υποφέρουν από υπερπληθωρισμό, όλο και περισσότεροι άνθρωποι θα πρέπει να αντιμετωπίσουν την πραγματικότητα του σκληρού και του μαλακού χρήματος. Αν είμαστε τυχεροί, ίσως ακόμη και μερικοί κεντρικοί τραπεζίτες θα αναγκαστούν να επαναξιολογήσουν τις νομισματικές τους πολιτικές. Ό,τι κι αν συμβεί, οι γνώσεις που έχω κερδίσει χάρη στο Bitcoin θα είναι πιθανότατα ανεκτίμητες, ανεξάρτητα από το αποτέλεσμα.

Το Bitcoin μου έμαθε για το κρυφό φόρο του πληθωρισμού και τη καταστροφή του υπερπληθωρισμού.

Through the Looking-Glass

- [Bitcoin's Energy Consumption — A shift in perspective](#)

Down the Rabbit Hole

- [Economic Crisis in Venezuela](#) by Wikipedia Contributors
- [Hyperinflation](#) by Wikipedia Contributors
- [List of Currencies](#) by Wikipedia Contributors
- [List of Historical Currencies](#) by Wikipedia Contributors
-  [1980S Unemployment And The Unions — Essays on the Impotent Price Structure of Britain and Monopoly in the Labour Market](#) by Friedrich von Hayek
-  [Economics In One Lesson](#) by Henry Hazlitt
-  [Good Money, Part 2 — The Standard](#) by Friedrich von Hayek

. . .

Μάθημα 10: Αξία

Ήταν το λευκό κουνέλι, περπατώντας αργά προς τα πίσω και κοιτάζοντας αγωνιωδώς καθώς πήγαινε, σαν να είχε χάσει κάτι...

Η αξία είναι κάπως παράδοξη και υπάρχουν πολλές θεωρίες που προσπαθούν να εξηγήσουν γιατί εκτιμούμε ορισμένα πράγματα περισσότερο σε σχέση με άλλα. Οι άνθρωποι γνώριζαν αυτό το παράδοξο για χιλιάδες χρόνια. Όπως έγραψε ο Πλάτωνας στο διάλογό του με τον Ευθύδημο, εκτιμούμε μερικά πράγματα επειδή είναι σπάνια και όχι μονάχα βάση της αναγκαιότητάς τους προς την επιβίωσή μας.

Εάν ηξεύρετε το συμφέρον σας, θα συμβουλευέστε και τους μαθητάς σας, ποτέ με κανένα άλλον άνθρωπον να μη συζητούν, παρά μόνον με σας ή μεταξύ των· διότι το σπάνιον, Ευθύδημε, είναι εκείνο που κάμνει πολύτιμον ένα πράγμα· το νερό βλέπεις, είναι πάμφθηνον, αν και είναι το καλύτερον από όλα τα πράγματα, καθώς το λέγει και ο Πίνδαρος. — Πλάτων


Το παράδοξο αυτό της αξίας δείχνει κάτι ενδιαφέρον για εμάς τους ανθρώπους: φαίνεται ότι εκτιμούμε τα πράγματα σε υποκειμενική βάση, αλλά το πράττουμε με ορισμένα μη αυθαίρετα κριτήρια. Μπορεί κάτι να είναι πολύτιμο για εμάς για διάφορους λόγους, αλλά τα πράγματα που εκτιμούμε μοιράζονται μεταξύ τους ορισμένα χαρακτηριστικά. Αν μπορούμε να αντιγράψουμε κάτι πολύ εύκολα ή αν είναι φυσικά άφθονο, δεν το εκτιμούμε.

Φαίνεται ότι δίνουμε αξία σε κάτι επειδή είναι σπάνιο (χρυσός, διαμάντια, χρόνος), δύσκολο ή θέλει σκληρή δουλειά για να παραχθεί, δεν μπορεί να αντικατασταθεί (μια παλιά φωτογραφία ενός αγαπημένου προσώπου), είναι χρήσιμο με τέτοιο τρόπο ώστε να επιτρέπει να κάνουμε πράγματα που διαφορετικά δεν μπορούσαμε να κάνουμε ή ένας συνδυασμός αυτών, όπως τα σπουδαία έργα τέχνης.

Το Bitcoin είναι όλα τα παραπάνω: είναι υπερβολικά σπάνιο (21 εκατομμύρια), όλο και πιο δύσκολο να παραχθεί (υποδιπλασιασμός ανταμοιβής), δεν μπορεί να αντικατασταθεί (ένα χαμένο ιδιωτικό κλειδί χάνεται για πάντα) και μας επιτρέπει να κάνουμε κάποια πολύ χρήσιμα πράγματα. Είναι αναμφισβήτητο το καλύτερο εργαλείο για τη μεταφορά αξίας μεταξύ συνόρων, πρακτικά ανθεκτικό στη λογοκρισία και τη κατάσχεση, καθώς και αυτοκυρίαρχο μέσο αποθήκευσης αξίας που επιτρέπει σε άτομα να αποθηκεύουν τον πλούτο τους ανεξάρτητα από τράπεζες και κυβερνήσεις.

Το Bitcoin μου έμαθε ότι η αξία είναι υποκειμενική αλλά όχι αυθαίρετη.

Down the Rabbit Hole

- [Bitcoin Has No Intrinsic Value — and That’s Great](#) by Conner Brown
- [Bitcoin Is Not Too Volatile](#) by Parker Lewis
- [Euthydemus](#) by Plato
- [Paradox of Value](#) by Wikipedia Contributors
- [Subjective Theory of Value](#) by Wikipedia Contributors
- [Theory of Value](#) by Wikipedia Contributors
-  [Skin In The Game — Hidden Asymmetries in Daily Life](#) by Nassim Nicholas Taleb

. . .

Μάθημα 11: Χρήμα

«Στη νιάτα μου,» είπε ο σοφός, καθώς κούνησε τα γκρίζα του μαλλιά, “κρατούσα όλα τα άκρα μου πολύ ευλύγιστα, με τη χρήση αυτής της αλοιφής, πέντε σελίνια το κουτί — Επιτρέψτε μου να σας πουλήσω μερικά.”

Τι είναι το χρήμα; Το χρησιμοποιούμε καθημερινά, όμως αυτή η ερώτηση είναι εκπληκτικά δύσκολη να απαντηθεί. Είμαστε εξαρτημένοι από εκείνο για μεγάλους και μικρούς λόγους, και αν έχουμε πολύ λίγα από αυτά, η ζωή μας γίνεται πολύ δύσκολη. Ωστόσο, σπάνια σκεφτόμαστε το πράγμα που υποτίθεται ότι κάνει τον κόσμο να περιστρέφεται. Το Bitcoin με ανάγκασε να απαντήσω ξανά και ξανά σε αυτή την ερώτηση: Τι στο καλό είναι το χρήμα;

Στον “σύγχρονο” κόσμο μας, οι περισσότεροι άνθρωποι πιθανότατα θα σκεφτούν κομμάτια χαρτιού όταν μιλάνε για χρήματα, αν και το μεγαλύτερο μέρος των χρημάτων μας είναι απλά ένας αριθμός σε έναν τραπεζικό λογαριασμό. Χρησιμοποιούμε ήδη μηδενικά και ένα ως τα χρήματά μας, άρα πώς διαφέρει το Bitcoin; Το Bitcoin διαφέρει επειδή κατ’ ουσίαν είναι ένα πολύ διαφορετικό είδος χρήματος από αυτά που χρησιμοποιούμε σήμερα. Για να γίνει κατανοητό αυτό, θα πρέπει να εξετάσουμε πιο προσεκτικά τι είναι το χρήμα, πώς ξεκίνησε να υφίσταται, και γιατί ο χρυσός και ο άργυρος χρησιμοποιήθηκαν για το μεγαλύτερο μέρος της εμπορικής ιστορίας.

“Με αυτή την έννοια, αντιπροσωπεύει περισσότερο ένα πολύτιμο μέταλλο. Αντί να αλλάζει η προσφορά για να διατηρηθεί η ίδια τιμή, η προσφορά είναι προκαθορισμένη και η τιμή αλλάζει.” — Satoshi Nakamoto

Κοχύλια, χρυσός, άργυρος, χαρτί, bitcoin. Στο τέλος, **το χρήμα είναι ό,τι χρησιμοποιούν οι άνθρωποι ως χρήμα**, ανεξάρτητα από το σχήμα και τη μορφή του, ή την έλλειψη αυτών.

Το χρήμα, ως εφεύρεση, είναι μεγαλοφυής. Ένας κόσμος χωρίς χρήματα είναι απίστευτα περίπλοκος: Πόσα ψάρια θα μου αγοράσουν νέα παπούτσια; Πόσες αγελάδες θα μου αγοράσουν ένα σπίτι; Τι θα συμβεί αν δεν χρειάζομαι τίποτα αυτή τη στιγμή, αλλά πρέπει να απαλλαγώ από τα σύντομα σάπια μήλα μου; Δεν χρειάζεστε πολλή φαντασία για να συνειδητοποιήσετε ότι μια ανταλλακτική οικονομία είναι εξοργιστικά αναποτελεσματική.

Το φοβερό πράγμα με τα χρήματα είναι ότι μπορεί να ανταλλάγουν για *οτιδήποτε άλλο* — αυτό κι αν είναι εφεύρεση! Όπως άψογα συνοψίζει ο Nick Szabo στο Shelling Out: The Origins of Money, εμείς οι άνθρωποι έχουμε χρησιμοποιήσει όλων των ειδών τα πράγματα ως χρήματα: χάντρες από σπάνια υλικά όπως το ελεφαντόδοντο, κοχύλια ή ειδικά οστά, διάφορα είδη κοσμημάτων και αργότερα σπάνια μέταλλα όπως ο άργυρος και ο χρυσός.

Όντας τα τεμπέλικα πλάσματα που είμαστε, δεν ξοδεύουμε πολύ σκέψη για πράγματα που απλά λειτουργούν. Τα χρήματα, για τους περισσότερους από εμάς, λειτουργούν μιά χαρά. Όπως με τα αυτοκίνητα ή τους υπολογιστές μας, οι περισσότεροι από εμάς αναγκαζόμαστε να σκεφτούμε τις εσωτερικές διεργασίες αυτών των πραγμάτων μόνο αν καταρρεύσουν. Οι άνθρωποι που είδαν τις οικονομίες μιας ζωής να εξαφανίζονται λόγω υπερπληθωρισμού γνωρίζουν την αξία των σκληρών χρημάτων, ακριβώς όπως εκείνοι που είδαν τους φίλους και την οικογένειά τους να εξαφανίζονται εξαιτίας των θηριωδιών της ναζιστικής Γερμανίας ή της Σοβιετικής Ρωσίας γνωρίζουν την αξία της ιδιωτικότητας.

Το θέμα με το χρήμα είναι ότι περιβάλλει τα πάντα. Το χρήμα είναι το ήμισυ της κάθε συναλλαγής. Ως αποτέλεσμα, οι υπεύθυνοι για τη δημιουργία των χρημάτων κατέχουν τεράστια δύναμη.

“Δεδομένου ότι τα χρήματα είναι το ήμισυ της κάθε εμπορικής συναλλαγής και πως η άνοδος και η πτώση ολόκληρων πολιτισμών κυριολεκτικά βασίζεται στην ποιότητα των χρημάτων τους, μιλάμε για μια φοβερή δύναμη. Μία δύναμη που καλύπτεται από ένα πυκνό πέπλο μυστηρίου. Είναι η δύναμη να δημιουργείς ψευδαισθήσεις που φαίνονται πραγματικές όσο διαρκούν. Αυτός ακριβώς είναι ο πυρήνας της δύναμης της Fed.” — Ron Paul

Το Bitcoin απομακρύνει ειρηνικά αυτή την εξουσία, καθώς εξαλείφει τη δημιουργία χρημάτων και το κάνει χωρίς τη χρήση βίας.

Το χρήμα πέρασε από πολλαπλές επαναλήψεις. Οι περισσότερες από αυτές ήταν καλές. Βελτίωσαν τα χρήματά μας με τον ένα ή τον άλλο τρόπο. Πολύ πρόσφατα ωστόσο, οι εσωτερικές διεργασίες των χρημάτων μας αλλοιώθηκαν. Την σήμερα ημέρα, σχεδόν όλα μας τα χρήματα δημιουργούνται απλά από το πουθενά από τις δυνάμεις εξουσίας. Για να καταλάβω πώς συνέβη αυτό έπρεπε να μάθω για την ιστορία και την επακόλουθη πτώση των χρημάτων.

Μένει να διαπιστωθεί εάν θα χρειαστεί μια σειρά από καταστροφές ή απλώς μια μεγαλειώδης εκπαιδευτική προσπάθεια για να διορθωθεί αυτή η αλλοίωση. Προσεύχομαι στους θεούς του υγιές χρήματος ότι θα είναι το δεύτερο.

Το Bitcoin μου έμαθε τι είναι το χρήμα.

Down the Rabbit Hole

- [Money, blockchains, and social scalability](#) by Nick Szabo
- [Gradually, Then Suddenly](#) by Parker Lewis
- 🎧 [Ansel Lindner on Why Ether is Bad Money](#)
POV#22 hosted by Christian
- 🎧 [Tuur Demeester — Bitcoin 101](#)
TIP#244 hosted by Preston Pysh and Stig Brodersen
- 🎧 [Conner Brown on the intersubjective nature of Bitcoin](#)
TFTC#87 hosted by Marty Bent

- 📖 End The Fed by Ron Paul
- 📖 What Has Government Done To Our Money by Murray Rothbard

. . .

Μάθημα 12: Η ιστορία και πτώση του χρήματος

Δεν θα θυμόντουσαν τους απλούς κανόνες που τους είχαν δώσει οι φίλοι τους, όπως ότι, αν μπειτε στη φωτιά, θα σας κάψει, και πως εάν κόψετε πολύ βαθιά το δάχτυλό σας με ένα μαχαίρι, γενικά αιμορραγεί και ποτέ δεν είχε ξεχάσει ότι, εάν πεις ένα μπουκάλι με την ένδειξη «δηλητήριο», είναι σχεδόν βέβαιο ότι θα σε πειράξει αργά ή γρήγορα.

Πολλοί άνθρωποι πιστεύουν ότι τα χρήματα καλύπτονται από αποθέματα χρυσού, ο οποίος φυλάγεται εντός μεγάλων θησαυροφυλακίων, προστατευόμενος από τεράστιους τοίχους. Αυτό έπαψε να ισχύει πριν από πολλές δεκαετίες. Δεν είμαι σίγουρος τι σκεφτόμουν, δεδομένου ότι είχα πολύ μεγαλύτερα προβλήματα να λύσω, έχοντας ουσιαστικά μηδενική κατανόηση του χρυσού, των χαρτονομισμάτων ή γιατί θα έπρεπε ευθύς εξαρχής να καλύπτονται από κάτι.

Ένα μέρος της μάθησης σχετικά με το Bitcoin είναι αυτό του παραστατικού χρήματος (fiat money): τι σημαίνει, πως ξεκίνησε να υφίσταται και γιατί ίσως δεν είναι η καλύτερη ιδέα που έχει υπάρξει. Λοιπόν, τι ακριβώς είναι το παραστατικό χρήμα; Και πώς καταλήξαμε να το χρησιμοποιήσουμε;

Εάν κάτι επιβάλλεται μέσω *fiat*, σημαίνει απλώς ότι επιβάλλεται μέσω επίσημης εξουσιοδότησης ή πρότασης. Έτσι, το παραστατικό χρήμα είναι χρήμα απλά επειδή κάποιος λέει ότι είναι. Δεδομένου ότι όλες οι σημερινές κυβερνήσεις χρησιμοποιούν παραστατικά νομίσματα, αυτός ο κάποιος είναι η κυβέρνησή σας. Δυστυχώς, δεν έχετε το δικαίωμα να διαφωνείτε με αυτήν την πρόταση αξίας. Θα αισθανθείτε γρήγορα ότι αυτή η πρόταση δεν είναι μη βίαια. Εάν αρνηθείτε να χρησιμοποιήσετε τα χαρτονομίσματα αυτά για τις επιχειρήσεις σας και την πληρωμή των φόρων, οι μόνοι άνθρωποι με τους οποίους θα μπορέσετε να συζητήσετε περί οικονομικών θα είναι οι συγκρατούμενοί σας.

Η αξία του παραστατικού χρήματος δεν προέρχεται από τις εγγενείς ιδιότητές του. Το πόσο καλό είναι κάποιο είδος παραστατικού χρήματος, συνδέεται μόνο με την πολιτική και δημοσιονομική α/ευ-στάθεια εκείνων που τα δημιουργούν. Η αξία του επιβάλλεται, αυθαίρετα, μέσω διατάγματος.

Origin



late Middle English: from Latin, 'let it be done,' from *feri* 'be done or made.'

fi·at /'fē,ät,'fēət/ — — 'Let it be done'

Μέχρι πρόσφατα γινόταν χρήση δύο τύπων χρήματος: χρήματα προϊόντων, κατασκευασμένα από πολύτιμα αντικείμενα, και αντιπροσωπευτικά χρήματα, τα οποία απλά αντιπροσωπεύουν το πολύτιμο αντικείμενο, κυρίως γραπτώς.

Αναφερθήκαμε ήδη στα χρήματα προϊόντων παραπάνω. Οι άνθρωποι χρησιμοποίησαν ως χρήματα ειδικά οστά, κοχύλια και πολύτιμα μέταλλα. Αργότερα χρησιμοποιήθηκαν ως χρήματα κυρίως κέρματα φτιαγμένα από πολύτιμα μέταλλα όπως ο χρυσός και ο άργυρος. Το παλαιότερο νόμισμα που έχει βρεθεί μέχρι στιγμής είναι φτιαγμένο από ένα φυσικό μίγμα χρυσού και αργύρου και κατασκευάστηκε πάνω από 2700 χρόνια πριν. Εάν προσφέρει κάτι καινούριο το Bitcoin, σίγουρα δεν είναι η έννοια του νομίσματος.



Λυδικό νόμισμα ήλεκτρου. Picture cc-by-sa Classical Numismatic Group, Inc.

Προκύπτει ότι η αποταμίευση νομισμάτων, ή αλλιώς *Hodling*, για να χρησιμοποιήσουμε και το σημερινό ιδίωμα, είναι σχεδόν τόσο παλιά όσο τα νομίσματα. Ένας από τους πρώτους hodler νομισμάτων ήταν κάποιος που έβαλε σχεδόν εκατό από αυτά τα νομίσματα σε ένα δοχείο και τα έθαψε στα θεμέλια ενός ναού, μόνο και μόνο για να βρεθούν 2500 χρόνια αργότερα. Αρκετά καλό “cold storage” κατά τη γνώμη μου.

Ένα από τα μειονεκτήματα της χρήσης πολύτιμων μετάλλων ως νόμισμα είναι ότι μπορούν να περικοπούν, μειώνοντας ουσιαστικά κατ' αυτό τον τρόπο την αξία τους. Νέα κέρματα μπορούν να εκδοθούν από τα αποκόμματα, πληθωρίζοντας με την πάροδο του χρόνου την ποσότητα χρήματος, υποτιμώντας παράλληλα το κάθε ένα κέρμα. Οι

άνθρωποι κυριολεκτικά έκοβαν όσο περισσότερο μπορούσαν από τα δολάρια αργύρου. Αναρωτιέμαι τι είδους “Dollar Shave Club” διαφημίσεις είχαν στις μέρες τους.

Επειδή οι κυβερνήσεις δεν έχουν θέμα με τον πληθωρισμό μόνο εάν τον εφαρμόζουν οι ίδιοι, έγιναν προσπάθειες για να σταματήσει αυτή η αντισυμβατική υποτίμηση. Με τον κλασικό τρόπο του κυνηγητού μεταξύ κλέφτη κι αστυνόμου, όσοι περιέκοβαν κέρματα γινόντουσαν όλο και πιο δημιουργικοί με τις τεχνικές τους, αναγκάζοντας τους «κύριους του νομισματοκοπείου» να γίνουν εξίσου δημιουργικοί με τα αντίμετρα τους. Ο Ισαάκ Νεύτων, ο παγκοσμίως γνωστός φυσικός για την φήμη του Principia Mathematica, ήταν ένας από αυτούς τους κύριους. Του αποδίδεται η προσθήκη των μικρών λωρίδων περιμετρικά των νομισμάτων που εξακολουθούν να υπάρχουν ακόμα και σήμερα. Η εποχή της εύκολης περικοπής νομισμάτων είχε πια τελειώσει.



Ακόμη και με αυτές τις μεθόδους υποτιμήσεως των νομισμάτων να διατηρούνται υπό έλεγχο, τα κέρματα εξακολουθούν να υποφέρουν από άλλα προβλήματα. Είναι ογκώδη και η μεταφορά τους δεν είναι πολύ βολική, ειδικά όταν πρέπει να συμβούν μεγάλες μεταφορές αξίας. Εμφανίζοντας μια τεράστια τσάντα από δολάρια αργύρου κάθε φορά που θέλετε να αγοράσετε μια Mercedes δεν είναι ιδιαίτερα πρακτικό.

Μιλώντας για Γερμανικά πράγματα: ενδιαφέρουσα είναι επίσης η ιστορία του πώς το δολάριο των ΗΠΑ πήρε το όνομά του. Η λέξη “δολάριο” προέρχεται από τη γερμανική λέξη *Thaler*, μια συντομογραφία του *Joachimsthaler*. Το Joachimsthaler ήταν ένα νόμισμα που κοβόταν στην πόλη Sankt Joachimsthal. Η λέξη Thaler είναι απλά μια συντομογραφία για κάποιον (ή κάτι) που προέρχεται από την κοιλάδα και επειδή το Joachimsthal ήταν η κοιλάδα για την παραγωγή νομισμάτων αργύρου, οι άνθρωποι απλά αναφέρονταν σε αυτά τα νομίσματα αργύρου ως *Thaler*. Τα Thaler (Γερμανικά) μετατράπηκαν σε daalders (Ολλανδικά), και τέλος δολάρια (Αγγλικά).



Το αρχικό «δολάριο». Ο Άγιος Ιωακείμ απεικονίζεται με το ράσο και το καπέλο του οδηγού. Picture cc-by-sa Berlin-George

Η εισαγωγή των αντιπροσωπευτικών χρημάτων προανήγγειλε την πτώση των σκληρών χρημάτων. Τα πιστοποιητικά χρυσού εισήχθησαν το 1863 και περίπου δεκαπέντε χρόνια αργότερα το δολάριο αργύρου άρχισε, αργά αλλά σταθερά, να αντικαθίσταται από ένα χάρτινο πληρεξούσιο: το πιστοποιητικό αργύρου.

Χρειάστηκαν περίπου 50 χρόνια από την εισαγωγή των πρώτων πιστοποιητικών αργύρου μέχρι αυτά τα κομμάτια χαρτιού να μεταμορφωθούν σε κάτι που θα αναγνωρίζαμε σήμερα ως ένα δολάριο των ΗΠΑ.



Ένα δολάριο αργύρου των ΗΠΑ του 1928 . «Πληρωτέο στον κομιστή κατόπιν αιτήσεως». Picture credit to the National Numismatic Collection at the Smithsonian Institution

Παρατηρήστε ότι το παραπάνω αμερικάνικο δολάριο αργύρου του 1928 εξακολουθεί να ονομάζεται *πιστοποιητικό αργύρου*, υποδεικνύοντας ότι στην ουσία είναι απλά ένα έγγραφο που δηλώνει την ύπαρξη οφειλής ενός κομματιού αργύρου στον κομιστή αυτού του χαρτιού. Είναι επίσης ενδιαφέρον να παρατηρήσουμε ότι το κείμενο που υποδεικνύει αυτή την οφειλή ξεκίνησε σταδιακά να μικραίνει. Η ένδειξη του “πιστοποιητικού” εξαφανίστηκε εντελώς μετά από λίγο. Αντικαταστάθηκε με την καθησυχαστική δήλωση ότι πρόκειται για τραπεζογραμμάτια του Federal Reserve.

Όπως αναφέρθηκε παραπάνω, το ίδιο συνέβη και με το χρυσό. Το μεγαλύτερο μέρος του κόσμου λειτουργούσε με το διμεταλλικό σύστημα, δηλαδή τα νομίσματα κατασκευάζονταν κυρίως από χρυσό και άργυρο. Η χρήση πιστοποιητικών χρυσού, εξαργυρώσιμα σε χρυσά νομίσματα, ήταν αναμφισβήτητα μια τεχνολογική βελτίωση. Το χαρτί είναι πιο βολικό, ελαφρύτερο, και από τη στιγμή που μπορεί να διαιρεθεί αυθαίρετα με την απλή εκτύπωση ενός μικρότερου αριθμού σε αυτό, είναι ευκολότερο να χωριστεί σε μικρότερες μονάδες.

Για να υπενθυμίσει στους κομιστές (χρήστες) ότι αυτά τα πιστοποιητικά ήταν αντιπροσωπευτικά πραγματικού χρυσού και αργύρου, έφεραν τις αντίστοιχες χρωματικές ενδείξεις και δήλωναν με σαφήνεια την ιδιότητα αυτή. Μπορείτε με ευκολία να διαβάσετε από πάνω προς τα κάτω την παρακάτω αναγραφή:

“Το παρόν πιστοποιεί ότι έχουν κατατεθεί στο
θησαυροφυλάκιο των Ηνωμένων Πολιτειών της
Αμερικής εκατό δολάρια σε χρυσό νόμισμα πληρωτέα
στον κομιστή κατόπιν αιτήσεως”.



Picture credit to National Numismatic Collection, National Museum of American History.

Το 1963, η φράση “ΠΛΗΡΩΤΕΑ ΣΤΟΝ ΚΟΜΙΣΤΗ ΚΑΤΟΠΙΝ ΑΙΤΗΣΕΩΣ” αφαιρέθηκε από όλα τα νεοεκδοθέντα χαρτονομίσματα. Πέντε χρόνια αργότερα, η εξαργύρωση των χαρτονομισμάτων σε χρυσό και άργυρο τελείωσε.

Οι λέξεις που υπονοούν την προέλευση και την ιδέα πίσω από το χαρτονόμισμα αφαιρέθηκαν. Το χρυσό χρώμα εξαφανίστηκε. Το μόνο που απέμεινε ήταν το χαρτί και μαζί του η ικανότητα της κυβέρνησης να τυπώνει όσο εκείνη επιθυμεί.

Με την κατάργηση του χρυσού κανόνα το 1971, το τέχνασμα διαρκείας ενός περίπου αιώνα είχε πλέον ολοκληρωθεί. Το χρήμα έγινε μια ψευδαισθησι κοινή σε όλους μέχρι σήμερα: το παραστατικό χρήμα. Αξίζει κάτι επειδή κάποιος που διοικεί ένα στρατό και λειτουργεί φυλακές λέει ότι αξίζει κάτι. Όπως μπορεί με ευκολία να διαβαστεί σε κάθε δολάριο που κυκλοφορεί σήμερα, “ΤΟ ΠΑΡΟΝ ΧΑΡΤΟΝΟΜΙΣΜΑ ΑΠΟΤΕΛΕΙ ΝΟΜΙΜΟ ΧΡΗΜΑ”. Με άλλα λόγια: Είναι πολύτιμο επειδή το χαρτονόμισμα λέει ότι είναι.



Ένα χαρτονόμισμα 20 δολαρίων των ΗΠΑ του 2004 που χρησιμοποιείται σήμερα. ‘THIS NOTE IS LEGAL TENDER’


Παρεμπιπτόντως, υπάρχει ένα άλλο ενδιαφέρον δίδαγμα σχετικά με τα σημερινά χαρτονομίσματα, κρυμμένο σε εμφανές σημείο. Η δεύτερη γραμμή αναφέρει ότι

αποτελεί νόμιμο χρήμα “ΓΙΑ ΟΛΑ ΤΑ ΔΗΜΟΣΙΑ ΚΑΙ ΙΔΙΩΤΙΚΑ ΧΡΕΗ. Κάτι που μπορεί να είναι προφανές στους οικονομολόγους αποτέλεσε έκπληξη για μένα: Όλα τα χρήματα είναι χρέος. Το κεφάλι μου εξακολουθεί να πονάει εξαιτίας αυτού, και θα αφήσω την εξερεύνηση της σχέσης των χρημάτων και του χρέους ως άσκηση στον αναγνώστη.

Όπως είδαμε, ο χρυσός και ο άργυρος χρησιμοποιήθηκαν ως χρήματα για χιλιετίες. Με την πάροδο του χρόνου, κέρματα από χρυσό και άργυρο αντικαταστάθηκαν από χαρτί. Το χαρτί έγινε σιγά σιγά αποδεκτό ως πληρωμή. Αυτή η αποδοχή δημιούργησε μια ψευδαίσθηση — την ψευδαίσθηση ότι το ίδιο το χαρτί έχει αξία. Η τελική κίνηση ήταν η πλήρης αποκόπη του δεσμού μεταξύ της εκπροσώπησης και του πραγματικού: καταργώντας το χρυσό κανόνα και πείθοντας όλους ότι το χαρτί από μόνο του είναι πολύτιμο.

Το Bitcoin μου έμαθε για την ιστορία των χρημάτων και το μεγαλύτερο τέχνασμα στην ιστορία των οικονομικών: το παραστατικό χρήμα.

Down the Rabbit Hole

- [Bimetallism](#) by Wikipedia Contributors
- [Methods of Coin Debasement](#) by Wikipedia Contributors
- [Thaler](#) by Wikipedia Contributors
- [U.S. Silver Certificate](#) by Wikipedia Contributors
-  [How Is Fiat Money Possible](#) by Hans-Hermann Hoppe

. . .

Μάθημα 13: Η παραφροσύνη των κλασματικών αποθεμάτων

Αλίμονο! ήταν πια πολύ αργά: συνεχίσε να μεγαλώνει όλο και περισσότερο και πολύ σύντομα έπρεπε να γονατίσει: μέσα στο επόμενο λεπτό δεν υπήρχε χώρος ούτε γι ‘αυτό και προσπάθησε να ξαπλώσει, με τον έναν αγκώνα στην πόρτα και το άλλο χέρι τυλιγμένο γύρω από το κεφάλι της. Συνέχισε παρ’ όλα αυτά να μεγαλώνει και ως τελευταία βοήθεια έβγαλε το χέρι της από το παράθυρο και το πόδι της από την καμινάδα, και είπε στον εαυτό της: Δεν μπορώ να κάνω τίποτα άλλο τώρα — τι θα απογίνω;”

Η αξία και τα χρήματα δεν αποτελούν ασήμαντα θέματα, ειδικά στη σημερινή εποχή. Η διαδικασία δημιουργίας χρημάτων στο τραπεζικό μας σύστημα είναι εξίσου

σημαντική και εξακολουθώ να έχω την αίσθηση ότι είναι σκόπιμα περίπλοκη. Αυτά που στο παρελθόν έχω συναντήσει μόνο στον ακαδημαϊκό κόσμο και στα νομικά κείμενα φαίνεται να είναι συνήθως πρακτική στο χρηματοοικονομικό κόσμο: τίποτα δεν εξηγείται με απλούς όρους, όχι επειδή είναι πραγματικά πολύπλοκο, αλλά επειδή η αλήθεια κρύβεται πίσω από πολλά στρώματα ορολογίας και προφανής πολυπλοκότητας. “Επεκτατική νομισματική πολιτική, ποσοτική χαλάρωση, δημοσιονομικά κίνητρα για την οικονομία.” Ο ακροατής γνέφει μαζί καταφατικά, υπνωτισμένος από τις πολύπλοκες λέξεις.

Το τραπεζικό σύστημα κλασματικών αποθεμάτων και η ποσοτική χαλάρωση είναι δύο από αυτές τις εξεζητημένες λέξεις, που περιπλέκουν αυτό που πραγματικά συμβαίνει, καμουφλάροντάς το ως περίπλοκο και δυσνόητο. Εάν τις εξηγήσετε σε ένα πεντάχρονο, η παραφροσύνη και των δύο θα γίνει γρήγορα φανερή.

Ο Godfrey Bloom, απευθυνόμενος στο Ευρωπαϊκό Κοινοβούλιο κατά τη διάρκεια μιας κοινής συζήτησης, το έθεσε πολύ καλύτερα από όσο θα μπορούσα ποτέ ο ίδιος:

“[...] δεν καταλαβαίνετε πραγματικά την έννοια του τραπεζικού συστήματος. Όλες οι τράπεζες έχουν χρεοκοπήσει. Bank Santander, Deutsche Bank, Royal Bank of Scotland— όλες έχουν χρεοκοπήσει! Και γιατί έχουν χρεοκοπήσει; Δεν αποτελεί θεομηνία. Δεν είναι κάποιου είδους τσουνάμι. Έχουν χρεοκοπήσει επειδή έχουμε ένα σύστημα που ονομάζεται «fractional reserve banking» που σημαίνει ότι οι τράπεζες μπορούν να δανείσουν χρήματα που δεν έχουν στην πραγματικότητα! Είναι ένα εγκληματικό σκάνδαλο και έχει διαρκέσει για πολύ καιρό. [...]

Έχουμε πλαστογράφηση— μερικές φορές καλείται ποσοτική χαλάρωση — αλλά πλαστογράφηση με οποιοδήποτε άλλο όνομα. Η τεχνητή εκτύπωση χρημάτων που, αν ένα συνηθισμένο άτομο το έκανε, θα πήγαινε στη φυλακή για πολύ καιρό [...] και μέχρι να

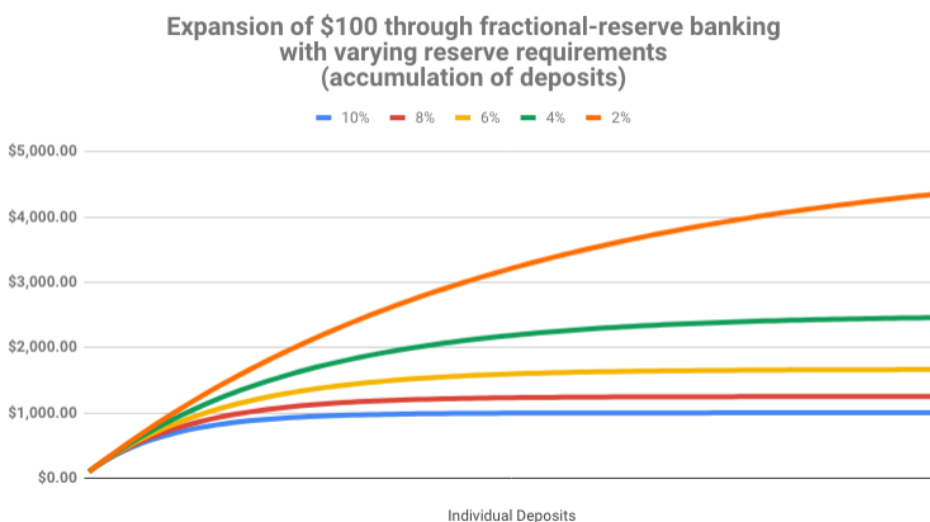
αρχίσουμε να στέλνουμε τραπεζίτες — και συμπεριλαμβάνω τους κεντρικούς τραπεζίτες και τους πολιτικούς — στη φυλακή για αυτά τα αίσχη, θα συνεχίσει.“ — Godfrey Bloom

Επιτρέψτε μου να επαναλάβω το πιο σημαντικό κομμάτι: οι τράπεζες μπορούν να δανείσουν χρήματα που στην πραγματικότητα δεν έχουν.

Χάρη στο τραπεζικό σύστημα κλασματικών αποθεμάτων, μια τράπεζα χρειάζεται μόνο να κρατήσει ένα μικρό μέρος του κάθε δολαρίου που δέχεται. Είναι κάπου μεταξύ 0 και 10%, συνήθως στο κατώτερο άκρο, γεγονός που κάνει τα πράγματα ακόμη χειρότερα.

Ας χρησιμοποιήσουμε ένα σαφές παράδειγμα για να κατανοήσουμε καλύτερα αυτή τη τρελή ιδέα: Ένα κλάσμα 10% θα μας βοηθήσει να είμαστε σε θέση να κάνουμε όλους τους υπολογισμούς στο κεφάλι μας. Ωφέλιμο για όλους. Έτσι, αν μεταφέρετε 100 δολάρια σε μια τράπεζα — επειδή δεν θέλετε να τα φυλάξετε κάτω από το στρώμα σας — θα χρειάζεται να κρατήσει μόνο το συμφωνηθέν κλάσμα του. Στο παράδειγμά μας, θα ήταν \$10, επειδή το 10% των \$100 είναι \$10. Εύκολο, σωστά;

Τι κάνουν λοιπόν οι τράπεζες με τα υπόλοιπα χρήματα; Τι συμβαίνει με τα \$90 σας; Κάνουν αυτό που κάνουν οι τράπεζες, τα δανείζουν σε άλλους ανθρώπους. Το αποτέλεσμα είναι ένας τραπεζικός πολλαπλασιαστής, ο οποίος αυξάνει υπερβολικά την προσφορά χρήματος στην οικονομία. Η αρχική σας κατάθεση των \$100 θα μετατραπεί σύντομα σε \$190. Δανείζοντας ένα κλάσμα 90% των νεοδημιουργημένων \$90, σύντομα θα υπάρχουν \$271 στην οικονομία. Και 343,90 δολάρια μετά από αυτό. Η προσφορά χρήματος αυξάνεται επαναλαμβανόμενα, καθώς οι τράπεζες δανείζουν χρήματα που κυριολεκτικά δεν έχουν. Χωρίς να πουν ούτε ένα μόνο αμπρακατάμπρα, οι τράπεζες μετατρέπουν με μαγικό τρόπο τα 100 δολάρια σε χίλια δολάρια ή και περισσότερα. Αποδεικνύεται ότι ένα 10x είναι εύκολο. Απαιτούνται μόνο μερικοί γύροι δανεισμού.



Χωρίς παρεξήγηση: Δεν υπάρχει τίποτα το κακό με το δανεισμό. Ούτε με το επιτόκιο. Δεν υπάρχει καν τίποτα το κακό με τις παλιές καλές κλασικές τράπεζες για να αποθηκεύσετε τον πλούτο σας κάπου ασφαλέστερα απ' ότι στο συρτάρι σας.

Οι κεντρικές τράπεζες, ωστόσο, αποτελούν ένα διαφορετικό κτήνος. Βδελύγματα δημοσιονομικού κανονισμού, μισό δημόσιες μισό ιδιωτικές, υποδύονται το θεό σε κάτι που επηρεάζει όλους όσους είναι μέρος του παγκόσμιου πολιτισμού μας, χωρίς καμία συνείδηση, ενδιαφέρονται μόνο για το άμεσο μέλλον και απ' ότι φαίνεται χωρίς να φέρουν καμία ευθύνη ή ικανότητα να ελεγχθούν.

Ενώ το Bitcoin εξακολουθεί να είναι πληθωριστικό, θα πάψει να είναι σχετικά σύντομα. Η αυστηρά περιορισμένη προσφορά 21 εκατομμυρίων bitcoins θα εξαλείψει τελικά τον πληθωρισμό εντελώς. Τώρα έχουμε δύο νομισματικούς κόσμους: ένα πληθωριστικό, όπου το χρήμα τυπώνεται αυθαίρετα, και τον κόσμο του Bitcoin, όπου η τελική προσφορά είναι σταθερή και εύκολα ελέγξιμη για όλους. Ο ένας μας επιβάλλεται μέσω βίας, ο άλλος επιτρέπει να συμμετάσχει όποιος το επιθυμεί. Κανένα εμπόδιο κατά την είσοδο, κανείς για να ζητήσετε άδεια. Εθελοντική συμμετοχή. Αυτή είναι η ομορφιά του Bitcoin.

Υποστηρίζω ότι η διαφωνία μεταξύ των Κεϊνσιανών και των Αυστριακών οικονομολόγων δεν είναι πλέον καθαρά ακαδημαϊκή. Ο Satoshi κατάφερε να αναπτύξει ένα σύστημα για τη μεταφορά αξίας υπό στεροειδή, δημιουργώντας επί τη ευκαιρία το πιο υγιές χρήμα που έχει υπάρξει. Με τον ένα ή τον άλλο τρόπο, όλο και περισσότεροι άνθρωποι θα μάθουν για την απάτη του τραπεζικού συστήματος κλασματικών αποθεμάτων. Αν καταλήξουν σε παρόμοια συμπεράσματα με αυτά των περισσότερων Αυστριακών και Bitcoiners, ίσως να ενταχθούν στο συνεχώς αυξανόμενο διαδίκτυο των χρημάτων. Κανείς δεν μπορεί να τους σταματήσει αν το επιλέξουν.

Το Bitcoin μου έμαθε ότι το τραπεζικό σύστημα κλασματικών αποθεμάτων είναι σκέτη παραφροσύνη.

Down the Rabbit Hole

- [Austrian School](#) by Wikipedia Contributors
- [Keynesian Economics](#) by Wikipedia Contributors
- [Money Multiplier](#) by Wikipedia Contributors
- [Why the whole banking system is a scam](#) by Godfrey Bloom
- [🎧 Jörg Guido Hülsmann on Fiat Money and Fractional Reserve](#)
- [Banking SLP#51](#) hosted by Stephan Livera

. . .

Μάθημα 14: Υγιές Χρήμα

«Το πρώτο πράγμα που έχω να κάνω», είπε η Αλίκη στον εαυτό της, καθώς περιπλανιόταν στο δάσος »είναι να φτάσω στο σωστό μου μέγεθος και το δεύτερο είναι να βρω τον δρόμο μου να μπω σε αυτόν τον υπέροχο κήπο. Νομίζω αυτό είναι το καλύτερο σχέδιο.»

Το πιο σημαντικό μάθημα που έχω διδαχθεί από το Bitcoin είναι ότι μακροπρόθεσμα, το σκληρό χρήμα είναι ανώτερο του μαλακού. Σκληρό χρήμα, που επίσης αναφέρεται ως υγιές χρήματα, είναι οποιοδήποτε διεθνώς συναλλάξιμο νόμισμα το οποίο χρησιμεύει ως αξιόπιστη αποθήκη αξίας.

Ομολογουμένως, το Bitcoin είναι ακόμα νέο και ασταθές. Οι κριτικοί θα πουν ότι δεν αποθηκεύει αξιόπιστα την αξία. Το επιχείρημα της μεταβλητότητας αποτυγχάνει να θίξει την ουσία του θέματος. Η μεταβλητότητα είναι αναμενόμενη. Η αγορά θα χρειαστεί λίγο χρόνο για να ανακαλύψει τη δίκαιη τιμή αυτού του νέου χρήματος. Επίσης, όπως συχνά αστειευόμενα επισημαίνεται, στηρίζεται σε ένα σφάλμα μέτρησης. Εάν σκέφτεστε σε δολάρια θα αποτύχετε να δείτε ότι ένα bitcoin θα αξίζει πάντα ένα bitcoin.

«Μια σταθερή προσφορά χρήματος ή μια προσφορά που αλλάζει μόνο σύμφωνα με αντικειμενικά και υπολογίσιμα κριτήρια είναι απαραίτητη προϋπόθεση για μια ουσιώδης δίκαιη τιμή του χρήματος». — Fr. Bernard W. Dempsey, S.J.

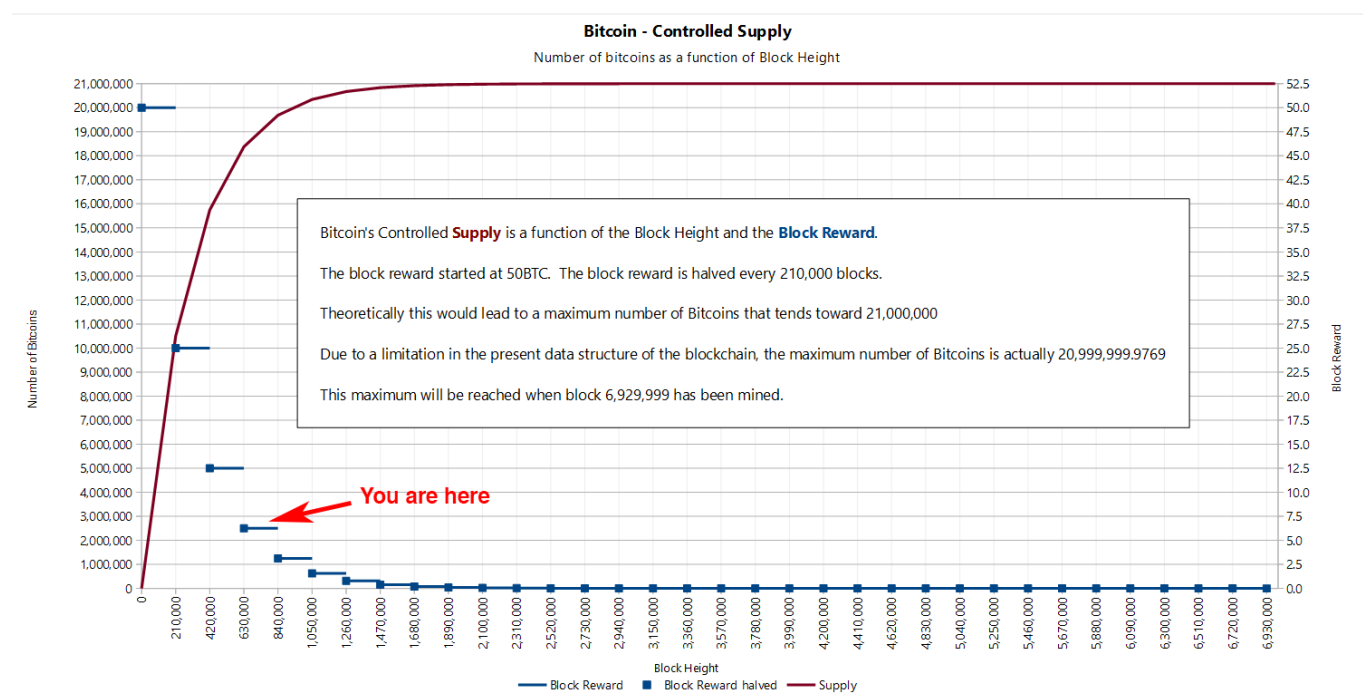
Όπως μας έχει δείξει ένα γρήγορος περίπατος μέσα από το νεκροταφείο των ξεχασμένων νομισμάτων, το χρήμα που μπορεί να τυπωθεί θα τυπωθεί. Μέχρι στιγμής, κανένας άνθρωπος στην ιστορία δεν ήταν σε θέση να αντισταθεί σε αυτόν τον πειρασμό.

Το Bitcoin απομακρύνει τον πειρασμό της εκτύπωσης χρημάτων μέσω ενός ιδιοφυή τρόπου. Ο Satoshi γνώριζε για την απληστία μας και την δυνατότητα να σφάλουμε — αυτός είναι ο λόγος για τον οποίο επέλεξε κάτι πιο αξιόπιστο από την ανθρώπινη αυτοσυγκράτηση: τα μαθηματικά.

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50 \cdot 10^8}{2^i} \right\rfloor}{10^8}$$

Ο τύπος προσφοράς του Bitcoin

Αν και ο τύπος αυτός είναι χρήσιμος για να περιγράψουμε τη προσφορά του Bitcoin, δεν μπορεί να βρεθεί πουθενά στο κώδικα. Η έκδοση νέων bitcoin γίνεται με αλγοριθμικά ελεγχόμενο τρόπο, μειώνοντας την ανταμοιβή που πληρώνονται οι miners κάθε τέσσερα χρόνια. Ο παραπάνω τύπος χρησιμοποιείται για να συνοψίσουμε γρήγορα αυτό που συμβαίνει στο παρασκήνιο. Αυτό που πραγματικά συμβαίνει μπορεί να παρατηρηθεί καλύτερα εξετάζοντας την αλλαγή της ανταμοιβής των block, την ανταμοιβή δηλαδή που δίνεται σε όποιον βρίσκει ένα έγκυρο block, το οποίο συμβαίνει περίπου κάθε 10 λεπτά.



Οι τύποι, οι λογαριθμικές συναρτήσεις και οι εκθετικοί αριθμοί δεν είναι ακριβώς διαισθητικά κατανοησιμοι. Η έννοια της ευρωστίας (υγιές χρήμα) μπορεί να είναι ευκολότερη στην κατανόησή της εάν την εξετάσουμε λίγο διαφορετικά. Εφόσον

γνωρίζουμε την ποσότητα που υπάρχει από κάτι, αλλά και την δυσκολία να παραχθεί ή να κατέχουμε αυτό το κάτι, μπορούμε να καταλάβουμε αμέσως την αξία του. Αυτό που ισχύει για τις ζωγραφιές του Πικάσο, τις κιθάρες του Elvis Presley και τα βιολιά Stradivarius είναι επίσης αληθές για το παραστατικό χρήμα, το χρυσό και τα bitcoins.

Η σκληρότητα του παραστατικού χρήματος εξαρτάται από το ποιός είναι υπεύθυνος για τις αντίστοιχες τυπωτικές μηχανές. Ορισμένες κυβερνήσεις ενδέχεται να είναι πιο πρόθυμες να εκτυπώσουν μεγάλες ποσότητες νομισματικών μονάδων από άλλες, το οποίο οδηγεί σε ένα ασθενέστερο νόμισμα. Άλλες κυβερνήσεις ενδέχεται να είναι πιο περιοριστικές στην εκτύπωση των χρημάτων τους, με αποτέλεσμα ένα σκληρότερο νόμισμα.

Προτού υπάρξουν παραστατικά νομίσματα, η ευρωστία των χρημάτων καθοριζόταν από τις φυσικές ιδιότητες των υλικών που χρησιμοποιούσαμε ως χρήμα. Η ποσότητα του χρυσού στη γη περιορίζεται από τους νόμους της φυσικής. Ο χρυσός είναι σπάνιος, διότι οι υπερκαινοφανείς αστέρες και οι συγκρούσεις αστέρων νετρονίων είναι σπάνιες. Η “ροή” του χρυσού είναι περιορισμένη επειδή η εξόρυξη απαιτεί αρκετά μεγάλο κόπο. Όντας βαρέο στοιχείο είναι κατά κύριο λόγο θαμμένο βαθιά κάτω από τη γη.

Η κατάργηση του χρυσού κανόνα παραχώρησε τη θέση του σε μια νέα πραγματικότητα: η προσθήκη νέων χρημάτων απαιτεί μόνο μια σταγόνα μελάνης. Στον σύγχρονο κόσμο μας, η επισύναψη μερικών μηδενικών στο υπόλοιπο ενός τραπεζικού λογαριασμού απαιτεί ακόμη λιγότερη προσπάθεια: η αντιστροφή μερικών bit σε ένα τραπεζικό υπολογιστή αρκεί.

“Μια σημαντική πτυχή αυτής της νέας πραγματικότητας είναι ότι ιδρύματα όπως η Fed δεν μπορούν να χρεοκοπήσουν. Μπορούν να τυπώσουν οποιοδήποτε χρηματικό ποσό που μπορεί να χρειαστούν για τον εαυτό τους με σχεδόν μηδενικό κόστος.” — Jörg Guido Hülsmann

Η αρχή που περιγράφεται παραπάνω μπορεί να εκφραστεί γενικότερα ως ο λόγος του “αποθέματος” προς τη “ροή”. Με απλά λόγια, το απόθεμα είναι η ποσότητα από κάτι που υπάρχει σήμερα. Για τις δικές μας ανάγκες, το απόθεμα αποτελεί μέτρο της τρέχουσας προσφοράς χρήματος. Η ροή είναι η ποσότητα που παράγεται σε μια χρονική περίοδο

(π.χ. ανά έτος). Το κλειδί για την κατανόηση του υγιούς χρήματος είναι η κατανόηση αυτού του λόγου αποθέματος-ροής.

Ο υπολογισμός του λόγου αποθέματος-προς-ροή για το παραστατικό χρήμα είναι δύσκολος, επειδή η ποσότητα των χρημάτων που υπάρχουν εξαρτάται από το πώς βλέπει κανείς τα πράγματα. Θα μπορούσατε να μετρήσετε μόνο τραπεζογραμμάτια και κέρματα (M0), να προσθέσετε ταξιδιωτικές επιταγές και να επιταγές καταθέσεων (M1), να προσθέσετε αποταμιευτικούς λογαριασμούς, αμοιβαία κεφάλαια και κάποια άλλα πράγματα (M2), ακόμα και να προσθέσετε πιστοποιητικά καταθέσεων σε όλα αυτά (M3). Επιπλέον, το πώς ορίζονται και μετριοούνται όλα αυτά αλλάζει από χώρα σε χώρα και από τη στιγμή που η Ομοσπονδιακή Τράπεζα των ΗΠΑ (Fed) σταμάτησε να δημοσιεύει αριθμούς για το M3, θα πρέπει να αρκεστούμε με τη νομισματική προσφορά M2. Θα ήθελα πολύ να επαληθεύσω αυτούς τους αριθμούς, αλλά υποθέτω ότι πρέπει να εμπιστευθούμε την Fed για την ώρα.

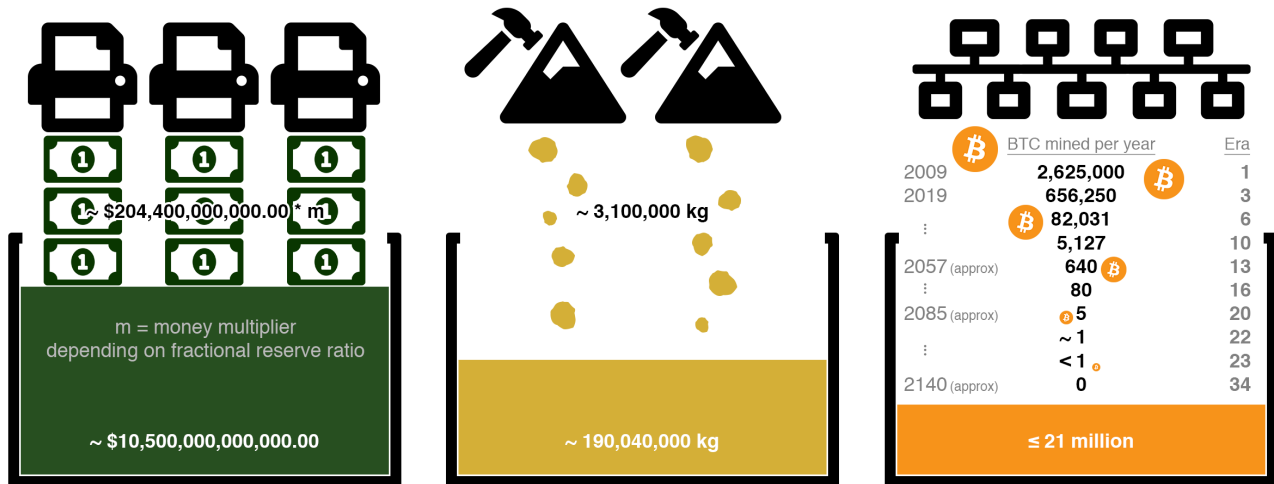
Ο χρυσός, ένα από τα σπανιότερα μέταλλα στη γη, έχει το μεγαλύτερο λόγο αποθέματος-προς-ροή. Σύμφωνα με την US Geological Survey, έχουν εξορυχθεί λίγο περισσότεροι από 190.000 τόνοι. Τα τελευταία χρόνια περίπου 3100 τόνοι χρυσού εξορύσσονται ετησίως.

Χρησιμοποιώντας τους παραπάνω αριθμούς, μπορούμε εύκολα να υπολογίσουμε το λόγο αποθέματος-προς-ροή του χρυσού: $190.000 \text{ τόνοι} / 3.100 \text{ τόνοι} = \sim 61$.

Τίποτα δεν έχει υψηλότερο λόγο αποθέματος-προς-ροή από το χρυσό. Αυτός είναι ο λόγος για τον οποίο ο χρυσός, μέχρι στιγμής, ήταν το πιο σκληρό και υγιές χρήμα που υπήρχε. Συχνά λέγεται ότι η συνολική ποσότητα χρυσού που έχει εξορυχθεί μέχρι τώρα θα μπορούσε να γεμίσει δυο πισίνες ολυμπιακών διαστάσεων. Σύμφωνα με τους υπολογισμούς μου, θα χρειαζόμασταν τέσσερεις. Οπότε ίσως να χρειάζονται μια ενημέρωση οι αριθμοί τους, ή οι πισίνες ολυμπιακών διαστάσεων μικρυναν.

Και τώρα το Bitcoin. Όπως πιθανότατα γνωρίζετε, το bitcoin mining (εξόρυξη) ήταν πολύ δημοφιλές τα τελευταία δύο χρόνια. Αυτό οφείλεται στο γεγονός ότι βρισκόμαστε ακόμα στα πρώτα στάδια από κάτι που ονομάζεται εποχή ανταμοιβής, όπου τα mining nodes (κόμβοι εξόρυξης) ανταμείβονται με αρκετά bitcoin για τον υπολογιστικό τους φόρτο. Αυτή τη στιγμή βρισκόμαστε στην εποχή ανταμοιβής αριθ.3, η οποία ξεκίνησε το 2016 και θα λήξει στις αρχές του 2020, πιθανώς τον Μάιο. Ενώ η προσφορά των bitcoin είναι προκαθορισμένη, οι εσωτερικές λειτουργίες του Bitcoin επιτρέπουν μόνο κατά προσέγγιση ημερομηνίες. Παρ' όλα αυτά, μπορούμε να προβλέψουμε με βεβαιότητα πόσο μεγάλος θα είναι ο λόγος αποθέματος-προς-ροή του Bitcoin. Spoiler Alert: θα είναι υψηλός.

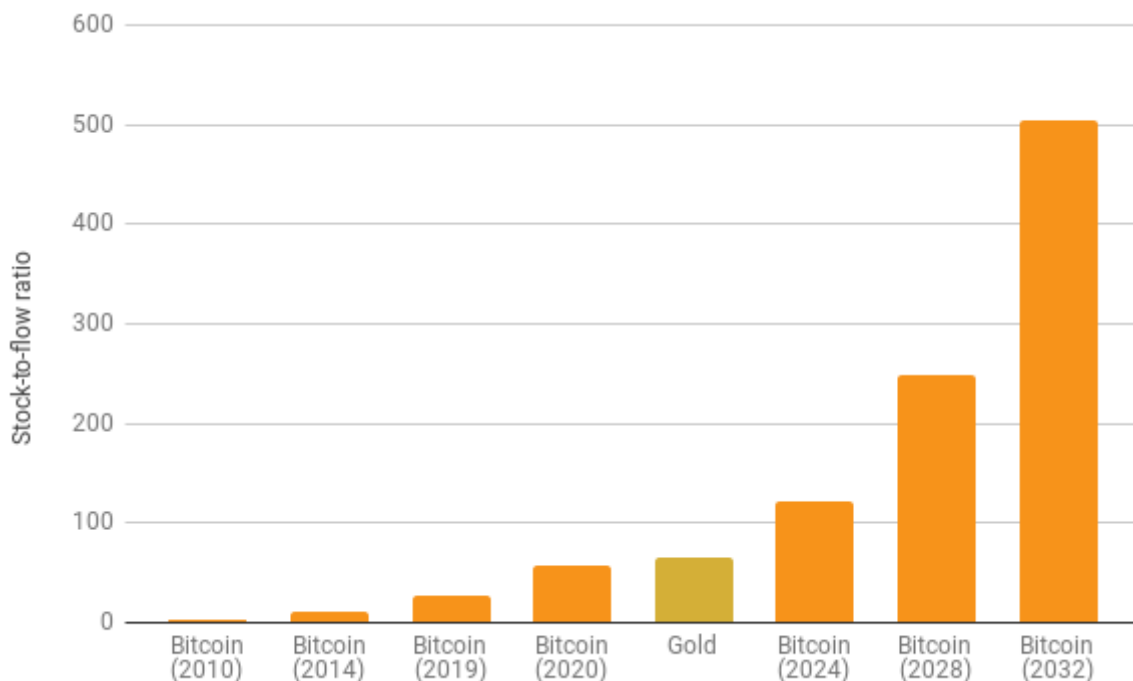
Πόσο υψηλός? Λοιπόν, προκύπτει ότι το Bitcoin θα γίνει απείρωσ σκληρό.



Fiat production according to U.S. Department of the Treasury [0], Gold production according to U.S. Geological Survey [1], Bitcoin supply according to calculations by the author [2]
 © dergigi [0] https://www.treasury.gov/resource-center/faqs/Currency/Pages/edu_faqs_currency_production.aspx [1] <https://minerals.usgs.gov/minerals/pubs/mcs/2018/mcs2018.pdf> [2] <http://bit.ly/btc-stock-to-flow>

Απεικόνιση του αποθέματος και της ροής για το USD, χρυσό και Bitcoin

Λόγω μιας εκθετικής μείωσης στην ανταμοιβή από mining, η ροή των νέων bitcoin θα μειωθεί με αποτέλεσμα έναν εκτοξευόμενο λόγο αποθέματος-προς-ροή. Θα φθάσει αυτό του χρυσού το 2020, μόνο για να το ξεπεράσει τέσσερα χρόνια αργότερα διπλασιάζοντας ξανά την ευρωστία του. Αυτός ο διπλασιασμός θα συμβεί 64 φορές συνολικά. Χάρη στη δύναμη των εκθετικών αριθμών, ο αριθμός των bitcoin που εξορύσσεται ετησίως θα πέσει κάτω από 100 bitcoin σε 50 χρόνια και κάτω από 1 bitcoin σε 75 χρόνια. Η παγκόσμια “βρύση” που είναι η ανταμοιβή των block θα στερεύσει κάποια στιγμή γύρω στο έτος 2140, σταματώντας ουσιαστικά την παραγωγή των bitcoin. Αποτελεί μακροπρόθεσμο παιχνίδι. Εάν το διαβάζετε αυτό, σημαίνει ότι έχετε έρθει νωρίς.



Αυξανόμενος λόγος αποθέματος-προς-ροή bitcoin σε σύγκριση με το χρυσό

Καθώς το bitcoin θα προσεγγίζει τον άπειρο λόγο αποθέματος-προς-ροή, θα είναι το υγιέστερο χρήμα που υπάρχει. Η άπειρη ευρωστέια είναι δύσκολο να ηττηθεί.

Θεωρούμενο υπό τον φακό των οικονομικών, η προσαρμογή δυσκολίας (difficulty adjustment) του Bitcoin είναι ίσως το πιο σημαντικό του στοιχείο. Το πόσο δύσκολο είναι να εξορυχθούν τα bitcoin εξαρτάται από το πόσο γρήγορα εξορύσσονται τα νέα bitcoins*. Χάρη στη δυναμική προσαρμογή της δυσκολίας εξόρυξης του δικτύου, μας επιτρέπεται η προβλέψη της μελλοντικής του προσφοράς.

(* Εξαρτάται πραγματικά από το πόσο γρήγορα βρίσκονται έγκυρα block, αλλά για τους σκοπούς μας, ισοδυναμεί με την “εξόρυξη bitcoin” και θα είναι έτσι για τα επόμενα 120 χρόνια.)

Η απλότητα του αλγορίθμου προσαρμογής δυσκολίας μπορεί να μας κάνει να ξεχάσουμε τη σπουδαιότητά της, αλλά η προσαρμογή δυσκολίας είναι πραγματικά μια επανάσταση Αϊνσταϊνικών διαστάσεων. Εξασφαλίζει ότι, ανεξάρτητα από το πόσο πολύς ή πόσο λίγος φόρτος δαπανάται σε εξόρυξη, η ελεγχόμενη προσφορά του Bitcoin δεν θα διαταραχθεί. Σε αντίθεση με κάθε άλλο πόρο, ανεξάρτητα από το πόσο πολύ ενέργεια θέτει κάποιος για εξόρυξη bitcoin, η συνολική ανταμοιβή δεν θα αυξηθεί.

Ακριβώς όπως το $E = mc^2$ υπαγορεύει το παγκόσμιο όριο ταχύτητας στο σύμπαν μας, η προσαρμογή δυσκολίας του Bitcoin υπαγορεύει το παγκόσμιο χρηματικό όριο στο Bitcoin.

Αν δεν υπήρχε αυτή η προσαρμογή δυσκολίας, όλα τα bitcoins θα είχαν ήδη εξορυχθεί. Αν δεν υπήρχε αυτή η προσαρμογή δυσκολίας, το Bitcoin πιθανότατα δεν θα είχε επιβιώσει στην παιδική του ηλικία. Είναι αυτό που ασφαρίζει το δίκτυο στην εποχή ανταμοιβής του. Είναι αυτό που εξασφαλίζει μια σταθερή και δίκαιη κατανομή νέων bitcoin. Είναι ο θερμοστάτης που ρυθμίζει τη νομισματική πολιτική του Bitcoin.

Ο Αϊνστάιν μας έδειξε κάτι πρωτόγνωρο: όσο δυνατά κι αν σπρώξεις ένα αντικείμενο, κάποια στιγμή δεν θα μπορείς να το κάνεις να μετακινηθεί πιο γρήγορα. Ο Satoshi μας έδειξε επίσης κάτι πρωτόγνωρο: όσο δυνατά κι αν “σκάψεις” για το ψηφιακό αυτό χρυσό, κάποια στιγμή δεν θα μπορείς να το κάνεις να βγάλει περισσότερα bitcoin. Για πρώτη φορά στην ανθρώπινη ιστορία, έχουμε ένα νομισματικό αγαθό που, ανεξάρτητα από το πόσο σκληρά προσπαθήσεις, δεν θα μπορέσεις να παράξεις περισσότερα.

Το Bitcoin μου έμαθε ότι το υγιές χρήμα είναι απαραίτητο.

Through the Looking-Glass

- [Bitcoin's Energy Consumption: A Shift in Perspective](#)

Down the Rabbit Hole

- [Bitcoin's distribution was fair](#) by Dan Held
- [Bitcoin's Controlled Supply](#) by Bitcoin Wiki Contributors
- [Mineral Commodity Summaries 2019](#) by the United States Geological Survey
- [Money Supply](#) by Wikipedia Contributors
- [Speed of Light](#) by Wikipedia Contributors
- 🎧 [Saifedean Ammous on Bitcoin as Sound Money](#)
Noded#3 hosted by Michael Goldstein and Pierre Rochard
- 🎧 [Murad Mahmudov on Bitcoin as the World Reserve Currency](#)
TFTC#34 hosted by Marty Bent
- 📖 [Money, Sound And Unsound](#) by Joseph Salerno
- 📖 [The Ethics Of Money Production](#) by Jörg Guido Hülsmann

. . .

21 Μαθήματα — Κεφάλαιο III: Τεχνολογία



nikos Mar 17, 2020 · 31 min read

Μετάφραση: [niclick](#)

. . .

Κεφάλαιο III: Τεχνολογία

“Τώρα, θα τα καταφέρω καλύτερα αυτή τη φορά”, είπε στον εαυτό της και άρχισε παίρνοντας το μικρό χρυσό κλειδί και ξεκλειδώνοντας την πόρτα που οδηγούσε στον κήπο.

Χρυσά κλειδιά, ρολόγια που λειτουργούν μόνο τυχαία, αγώνες για να λυθούν περίεργα αινίγματα και χτίστες που δεν έχουν πρόσωπα ή ονόματα. Αυτό που μοιάζει με παραμύθι από τη χώρα των θαυμάτων αποτελεί καθημερινή δραστηριότητα στον κόσμο του Bitcoin.

Όπως διερευνήσαμε στο [Κεφάλαιο 2](#), μεγάλα τμήματα του τρέχοντος χρηματοπιστωτικού συστήματος καταρρέουν συστηματικά. Όπως και η Αλίκη, μπορούμε μόνο να ελπίζουμε πως θα τα καταφέρουμε καλύτερα αυτή τη φορά. Όμως, χάρη σε έναν ψευδώνυμο εφευρέτη, έχουμε μια εξαιρετικά προηγμένη τεχνολογία που μας υποστηρίζει αυτή τη φορά: το Bitcoin.

Η επίλυση προβλημάτων σε ένα ριζικά αποκεντρωμένο και ανταγωνιστικό περιβάλλον απαιτεί πρωτοφανείς λύσεις. Αυτά που υπό άλλες συνθήκες θα θεωρούνταν επουσιώδη προβλήματα είναι κάθε άλλο παρά ασήμαντα σε αυτό τον περίεργο κόσμο των nodes. Το Bitcoin βασίζεται σε ισχυρή κρυπτογραφία για τις περισσότερες λύσεις του,

τουλάχιστον όταν μελετάται μέσα από τον φακό της τεχνολογίας. Το πόσο ισχυρή είναι αυτή η κρυπτογραφία θα εξερευνηθεί σε ένα από τα ακόλουθα μαθήματα.

Η κρυπτογραφία είναι αυτό που χρησιμοποιεί το Bitcoin για να απομακρύνει την εμπιστοσύνη σε αρχές. Αντί να βασίζεται σε κεντρικά ιδρύματα, το σύστημα αυτό βασίζεται στην τελική εξουσία του σύμπαντός μας: τη φυσική. Ορισμένα ίχνη εμπιστοσύνης παραμένουν ωστόσο. Θα εξετάσουμε αυτά τα ίχνη στο δεύτερο μάθημα αυτού του κεφαλαίου.

- Μάθημα 15: Δύναμη σε αριθμούς
- Μάθημα 16: Στοχασμοί πάνω στο “Μην εμπιστεύεστε, επαληθεύστε”
- Μάθημα 17: Ο προσδιορισμός της ώρας απαιτεί έργο
- Μάθημα 18: Κινηθείτε αργά και μην σπάσετε πράγματα
- Μάθημα 19: Η ιδιωτικότητα δεν έχει πεθάνει
- Μάθημα 20: Οι Cypherpunks γράφουν κώδικα
- Μάθημα 21: Μεταφορές για το μέλλον του Bitcoin

Τα τελευταία δύο μαθήματα διερευνούν το ήθος της τεχνολογικής ανάπτυξης στο Bitcoin, το οποίο είναι αναμφισβήτητα εξίσου σημαντικό με την ίδια τη τεχνολογία. Το Bitcoin δεν είναι η επόμενη φανταχτερή εφαρμογή στο κινητό σας. Είναι το θεμέλιο μιας νέας οικονομικής πραγματικότητας, το οποίο είναι ο λόγος που το Bitcoin πρέπει να αντιμετωπίζεται ως χρηματοοικονομικό λογισμικό “πυρηνικής-ποιότητας”.

Πού βρισκόμαστε σε αυτή τη χρηματοοικονομική, κοινωνική και τεχνολογική επανάσταση; Τα δίκτυα και οι τεχνολογίες του παρελθόντος μπορούν να χρησιμεύσουν ως μεταφορές για το μέλλον του Bitcoin, τα οποία διερευνώνται στο τελευταίο μάθημα αυτού του κεφαλαίου.

Για μια ακόμη φορά, βάλτε ζώνη και απολαύστε τη βόλτα. Όπως όλες οι εκθετικές τεχνολογίες, είμαστε έτοιμοι να πάμε παραβολικά.

. . .

Μάθημα 15: Δύναμη σε αριθμούς

Για να δω: τέσσερις φορές το πέντε κάνει δώδεκα, και τέσσερις φορές το έξι δεκατρία, και τέσσερις φορές το επτά δεκατέσσερα — Ω, Θεέ μου! Δεν θα φτάσω ποτέ στο είκοσι

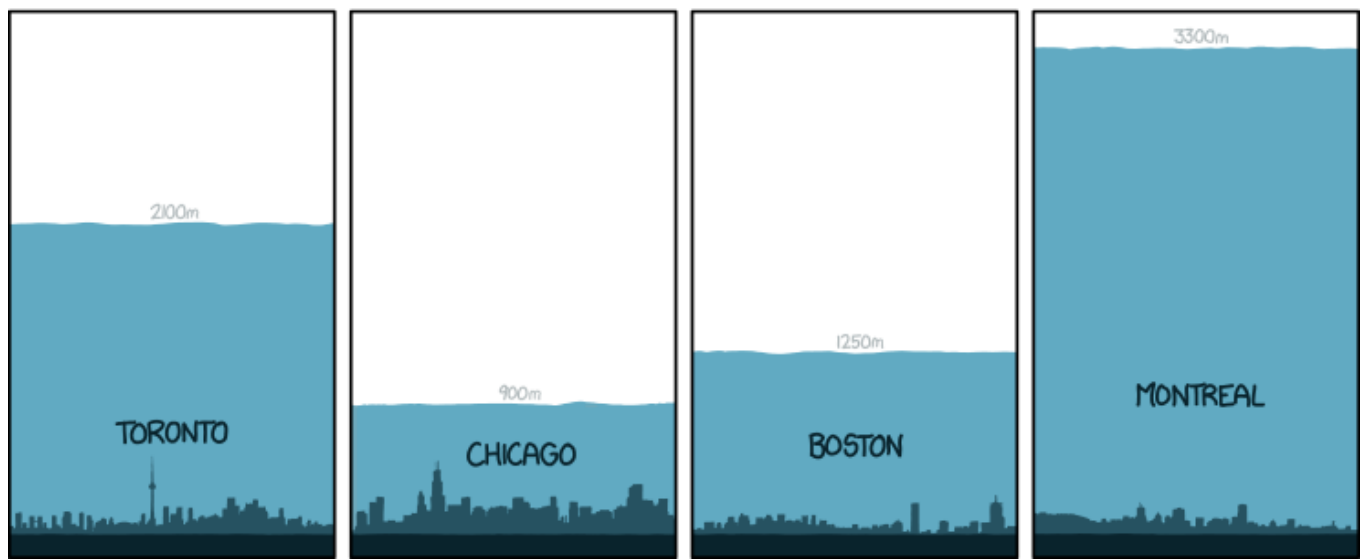
Οι αριθμοί αποτελούν ουσιαστικό μέρος της καθημερινής μας ζωής. Οι μεγάλοι αριθμοί, ωστόσο, δεν είναι κάτι με το οποίο οι περισσότεροι από εμάς είμαστε αρκετά εξοικειωμένοι. Οι μεγαλύτεροι αριθμοί που μπορεί να συναντήσουμε στην καθημερινή μας ζωή είναι της τάξης των εκατομμυρίων, δισεκατομμυρίων ή τρισεκατομμυρίων. Μπορεί να διαβάσουμε για εκατομμύρια ανθρώπους που βρίσκονται υπό συνθήκες φτώχειας, δισεκατομμύρια δολάρια που δαπανώνται για τη διάσωση τραπεζών και τρισεκατομμύρια δημόσιου χρέους. Αν και είναι δύσκολο να κατανοήσουμε τις ειδήσεις αυτές, είμαστε κάπως άνετοι με το μέγεθος αυτών των αριθμών.

Παρόλο που μπορεί να φαινόμαστε άνετοι με τα δισεκατομμύρια και τα τρισεκατομμύρια, η διαίσθησή μας ήδη αρχίζει να αποτυγχάνει με αριθμούς αυτού του μεγέθους. Έχετε την διαίσθηση του πόσο καιρό θα έπρεπε να περιμένετε για να περάσει ένα εκατομμύριο/δισεκατομμύριο/τρισεκατομμύριο δευτερόλεπτα; Εάν είστε έστω και λίγο σαν εμένα, είστε εντελώς χαμένοι εάν δεν κάνετε πραγματικά τον υπολογισμό.

Ας ρίξουμε μια πιο προσεκτική ματιά σε αυτό το παράδειγμα: η διαφορά μεταξύ του καθενός είναι μια αύξηση κατά τρεις τάξεις μεγέθους: 10^6 , 10^9 , 10^{12} . Το να σκεφτόμαστε σε δευτερόλεπτα δεν βοηθάει ιδιαίτερα, οπότε ας το μεταφράσουμε σε κάτι που μπορούμε να κατανοήσουμε καλύτερα:

- 10^6 : Ένα εκατομμύριο δευτερόλεπτα ήταν πριν από $1\frac{1}{2}$ εβδομάδα.
- 10^9 : Ένα δισεκατομμύριο δευτερόλεπτα ήταν σχεδόν 32 χρόνια πριν.
- 10^{12} : Ένα τρισεκατομμύριο δευτερόλεπτα πριν, το Μανχάταν ήταν καλυμμένο κάτω από ένα παχύ στρώμα πάγου.

THICKNESS OF THE ICE SHEETS AT VARIOUS LOCATIONS 21,000 YEARS AGO COMPARED WITH MODERN SKYLINES



Μόλις εισέλθουμε στην υπερ-αστρονομική σφαίρα της σύγχρονης κρυπτογραφίας, η διαίσθησή μας αποτυγχάνει καταστροφικά. Το Bitcoin είναι χτισμένο γύρω από μεγάλους αριθμούς και την ουσιαστική αδυναμία να τους μαντέψουμε. Αυτοί οι αριθμοί είναι κατά πολύ μεγαλύτεροι από οτιδήποτε μπορεί να συναντήσουμε στην καθημερινή μας ζωή. Πολλές τάξεις μεγέθους μεγαλύτεροι. Το να κατανοήσουμε πόσο μεγάλοι είναι αυτοί οι αριθμοί είναι πραγματικά απαραίτητο για την κατανόηση του Bitcoin στο σύνολό του.

Ας πάρουμε το SHA-256, μία από τις συναρτήσεις κατακερματισμού (hash functions) που χρησιμοποιείται στο Bitcoin, ως συγκεκριμένο παράδειγμα. Είναι φυσικό να αναλογιζόμαστε τα 256 bit ως “διακόσια πενήντα έξι”, το οποίο δεν είναι καθόλου μεγάλος αριθμός. Ωστόσο, ο αριθμός αυτός στο SHA-256 μιλάει για *τάξεις μεγέθους* — κάτι που οι εγκέφαλοί μας δεν είναι καλά εξοπλισμένοι για να διαχειριστούν.

Ενώ το μήκος bit είναι μια βολική μέθοδος μέτρησης, το πραγματικό νόημα των 256-bit ασφάλειας χάνεται στη μετάφραση. Παρόμοια με τα εκατομμύρια (10^6) και τα δισεκατομμύρια (10^9) παραπάνω, ο αριθμός στο SHA-256 αναφέρεται σε τάξεις μεγέθους (2^{256}).

Άρα, πόσο ισχυρό είναι το SHA-256, ακριβώς;

“Το SHA-256 είναι πολύ ισχυρό. Δεν είναι σαν το σταδιακό αυξητικό βήμα από MD5 σε SHA1. Μπορεί να διαρκέσει αρκετές δεκαετίες, εκτός και αν υπάρξει κάποια σημαντικά πρωτοποριακή επίθεση.” — Satoshi Nakamoto

Ας το κάνουμε πιο ξεκάθαρο. Το 2^{256} ισούται με τον ακόλουθο αριθμό:

```
115 quattuorvigintillion 792 trevigintillion 89 duovigintillion 237
unvigintillion 316 vigintillion 195 novemdecillion 423 octodecillion
570 septendecillion 985 sexdecillion 8 quindecillion 687
quattuordecillion 907 tredecillion 853 duodecillion 269 undecillion
984 decillion 665 nonillion 640 octillion 564 septillion 39
sextillion 457 quintillion 584 quadrillion 7 trillion 913 billion 129
million 639 thousand 936.
```

Μιλάμε για πολλά nonillions! Το να κατανοήσουμε αυτό τον αριθμό είναι σχεδόν αδύνατο. Δεν υπάρχει τίποτα στο φυσικό σύμπαν με το οποίο μπορούμε να το συγκρίνουμε. Είναι κατά πολύ μεγαλύτερος από τον αριθμό των ατόμων στο παρατηρήσιμο σύμπαν. Ο ανθρώπινος εγκέφαλος απλά δεν έχει εξελιχθεί για να τον συλλάβει.

Μια από τις καλύτερες απεικονίσεις της πραγματικής δύναμης του SHA-256 είναι το ακόλουθο βίντεο του Grant Sanderson. Εύστοχα ονομαζόμενο “Πόσο ασφαλής είναι η ασφάλεια 256 bit;” δείχνει πολύ όμορφα πόσο μεγάλος είναι ένας χώρος 256 bit. Κάντε στον εαυτό σας την χάρη και αφιερώστε πέντε λεπτά για να το παρακολουθήσετε. Όπως όλα τα άλλα βίντεο του [3Blue1Brown](#) δεν είναι μόνο συναρπαστικό αλλά και εξαιρετικά καλοφτιαγμένο. Προειδοποίηση: Μπορεί να πέσετε σε ένα λαγούμι μαθηματικών.



Απάντηση: Αρκετά ασφαλής.

Ο [Bruce Schneier](#) χρησιμοποίησε τα φυσικά όρια του υπολογισμού για να θέσει τον αριθμό αυτό υπό προοπτική: ακόμη και αν μπορούσαμε να φτιάξουμε έναν βέλτιστο υπολογιστή, ο οποίος θα χρησιμοποιούσε κάθε παρεχόμενη ενέργεια για να αναστρέφει τα bit τέλεια, να κατασκευάσουμε μια [σφαίρα Dyson](#) γύρω από τον ήλιο μας, και να τον αφήσουμε να λειτουργεί για 100 δισεκατομμύρια δισεκατομμυρίων χρόνια, θα εξακολουθούσαμε να έχουμε μόνο 25% πιθανότητα να βρούμε ένα ψύλλο σε έναν αχυρώνα 256-bit.

“Αυτοί οι αριθμοί δεν έχουν καμία σχέση με την τεχνολογία των συσκευών· είναι τα μέγιστα που επιτρέπει η θερμοδυναμική. Και υπονοούν έντονα ότι οι επιθέσεις brute-force ενάντια σε κλειδιά 256-bit θα είναι ανέφικτες έως ότου οι υπολογιστές κατασκευάζονται από κάτι άλλο πέρα από ύλη και καταλαμβάνουν κάτι διαφορετικό του χώρου». — Bruce Schneier

Είναι δύσκολο να μεγαλοποιήσουμε την βαθύτητα αυτού. Η ισχυρή κρυπτογραφία ανατρέπει την ισορροπία δυνάμεων του φυσικού κόσμου που έχουμε τόσο συνηθίσει. Αδιάρρηκτα πράγματα δεν υπάρχουν στον πραγματικό κόσμο. Εφάρμοσε αρκετή δύναμη και θα μπορέσεις να ανοίξεις οποιαδήποτε θύρα, κουτί ή σεντούκι.

Το σεντούκι του Bitcoin είναι πολύ διαφορετικό. Ασφαλίζεται από ισχυρή κρυπτογραφία, η οποία δεν καταρρέει μέσω brute-force. Και όσο διατηρούνται οι υποκείμενες μαθηματικές υποθέσεις, το brute-force είναι το μόνο που έχουμε. Ομολογουμένως, υπάρχει επίσης η επιλογή μίας παγκόσμιας επίθεσης με κλειδί των 5\$. Τα βασανιστήρια όμως δεν θα λειτουργήσουν για όλες τις διευθύνσεις bitcoin, και οι κρυπτογραφικοί τοίχοι του bitcoin θα εμποδίσουν τις επιθέσεις brute-force. Ακόμη και αν του επιτεθείτε με τη δύναμη χιλίων ήλιων. Κυριολεκτικά.

Το γεγονός αυτό και οι συνέπειές του συνοψίζονταν ξεκάθαρα στην έκκληση για κρυπτογραφικά όπλα: “Κανένα ποσό καταναγκαστικής δύναμης δεν θα λύσει ποτέ ένα μαθηματικό πρόβλημα”.

“Δεν είναι προφανές ότι ο κόσμος έπρεπε να λειτουργεί κατ’ αυτό το τρόπο. Αλλά με κάποιον τρόπο το σύμπαν ευνοεί την κρυπτογράφηση.” — Julian Assange

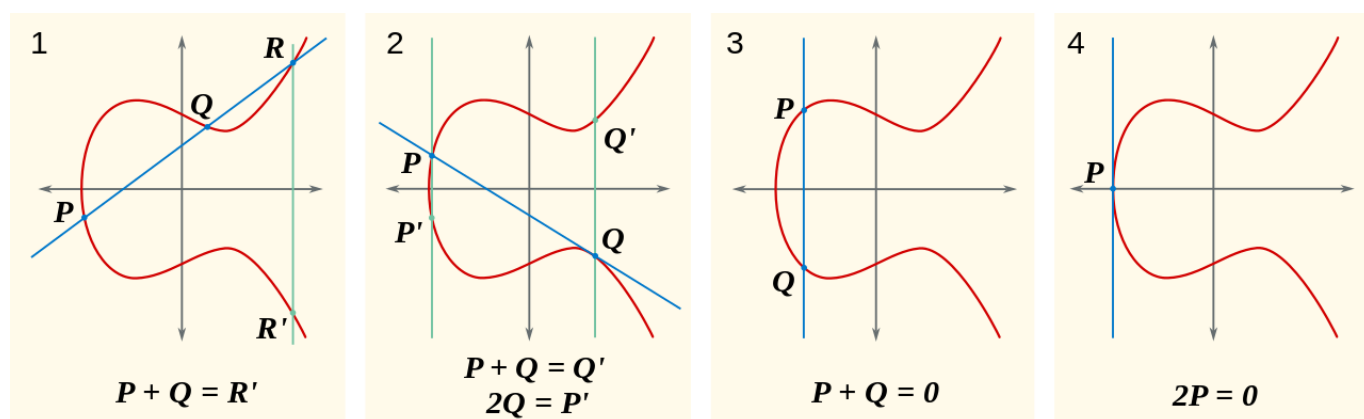
Κανείς δεν γνωρίζει ακόμα με βεβαιότητα αν η εύνοια αυτή του σύμπαντος είναι γνήσια ή όχι. Είναι πιθανό ότι η υπόθεσή μας για μαθηματικές ασυμμετρίες είναι λανθασμένη και να διαπιστώσουμε ότι το P στην πραγματικότητα ισοδυναμεί με NP, ή να βρούμε εκπληκτικά γρήγορες λύσεις σε συγκεκριμένα προβλήματα τα οποία προς το παρόν θεωρούμε ότι είναι δύσκολα. Εάν έχουν έτσι τα πράγματα, η κρυπτογραφία

όπως την γνωρίζουμε θα σταματήσει να υφίσταται, και οι επιπτώσεις θα έκαναν πιθανότατα τον κόσμο αγνώριστο.

“Vires in Numeris” = “Δύναμη σε Αριθμούς” — επι

Το *Vires in numeris* δεν αποτελεί μόνο πιασάρικο σλόγκαν που χρησιμοποιείται από τους bitcoiners. Η συνειδητοποίηση ότι υπάρχει μια ανυπέρβλητη δύναμη που βρίσκεται στους αριθμούς είναι ουσιαστική. Η κατανόηση αυτού του γεγονότος και η ανατροπή των υφιστάμενων ισορροπιών δυνάμεων που επιτρέπει, άλλαξε την άποψή μου για τον κόσμο και το μέλλον που βρίσκεται μπροστά μας.

Ένα άμεσο αποτέλεσμα αυτού είναι το γεγονός ότι δεν χρειάζεται να ζητήσετε από κανέναν άδεια για συμμετοχή στο Bitcoin. Δεν υπάρχει σελίδα για εγγραφή, καμία αρμόδια εταιρεία, καμία κρατική υπηρεσία στην οποία να στείλετε έντυπο αίτησης. Δημιουργήστε απλά έναν μεγάλο αριθμό και θα είστε πάνω-κάτω έτοιμοι να ξεκινήσετε. Η κεντρική αρχή για τη δημιουργία λογαριασμού είναι τα μαθηματικά. Και ένας Θεός μόνο γνωρίζει ποιός είναι υπεύθυνος για αυτά.



Παραδείγματα Ελλειπτικών Καμπυλών (cc-by-sa Emmanuel Boutet)


Το Bitcoin βασίζεται στην καλύτερη κατανόηση της πραγματικότητας που έχουμε. Ενώ υπάρχουν ακόμη πολλά ανοιχτά προβλήματα στη φυσική, την επιστήμη των υπολογιστών και τα μαθηματικά, είμαστε αρκετά σίγουροι για κάποια πράγματα. Το ότι υπάρχει μια ασυμμετρία μεταξύ της εύρεσης λύσεων και της επαλήθευσης της ορθότητας αυτών των λύσεων είναι ένα τέτοιο πράγμα. Το ότι ο υπολογισμός απαιτεί ενέργεια είναι άλλο ένα. Με άλλα λόγια: η εύρεση ενός φύλλου στ' άχυρα είναι πιο δύσκολη από το να ελέγξετε αν το πράγμα στο χέρι σας είναι όντως φύλλος ή όχι. Και η εύρεση του φύλλου απαιτεί έργο.

Η απεραντοσύνη του χώρου διευθύνσεων του Bitcoin είναι πραγματικά εντυπωσιακή. Ο αριθμός των ιδιωτικών κλειδιών ακόμα περισσότερο. Είναι συναρπαστικό το πόσο πολύ ο σύγχρονος κόσμος μας συνοψίζεται στην αδυναμία της εύρεσης ενός φύλλου

σε έναν ακατάλυπτα μεγάλο αχυρώνα. Αντιλαμβάνομαι το γεγονός αυτό περισσότερο από ποτέ.

Το Bitcoin μου έμαθε ότι υπάρχει δύναμη σε αριθμούς.

Down the Rabbit Hole

- [Block hashing algorithm](#) by Bitcoin Wiki Contributors
- [Discrete Logarithm](#) by Wikipedia Contributors
- [Dyson Sphere](#) by Wikipedia Contributors
- [How secure is 256 bit security?](#) by 3Blue1Brown
- [Landauer's Principle](#) by Wikipedia Contributors
- [Last Glacial Maximum](#) by Wikipedia Contributors
- [P versus NP](#) by Wikipedia Contributors
- [SHA-2](#) by Wikipedia Contributors
-  [Fooled By Randomness — The Hidden Role of Chance in Life and in the Markets](#) by Nassim Nicholas Taleb

. . .

Μάθημα 16: Στοχασμοί πάνω στο “Μην εμπιστεύεστε, επαληθεύστε”

“Τώρα για τα αποδεικτικά στοιχεία,” είπε ο βασιλιάς, “και στη συνέχεια η ποινή.”

Το Bitcoin στοχεύει στην αντικατάσταση, ή τουλάχιστον την παροχή εναλλακτικής λύσης, των συμβατικών νομισμάτων. Τα συμβατικά νομίσματα συνδέονται με μια κεντρική αρχή, ανεξάρτητα αν μιλάμε για νόμιμο χρήμα όπως το δολάριο των ΗΠΑ ή σύγχρονα χρήματα τύπου Μονόπολης όπως τα V-Bucks του Fortnite. Και στα δύο παραδείγματα, θα πρέπει να εμπιστευτείτε την κεντρική αρχή για να εκδίδει, να διαχειρίζεται και να κυκλοφορεί τα χρήματά σας. Το Bitcoin λύνει αυτόν τον δεσμό, και το βασικό πρόβλημα που επλύει το Bitcoin είναι το θέμα της *εμπιστοσύνης*.

“Το βασικό πρόβλημα με το συμβατικό νόμισμα είναι όλη η εμπιστοσύνη που απαιτείται για να λειτουργήσει. [...] Αυτό που χρειάζεται είναι ένα ηλεκτρονικό

σύστημα πληρωμών βασισμένο στην κρυπτογραφική απόδειξη αντί της εμπιστοσύνης.“ — Satoshi

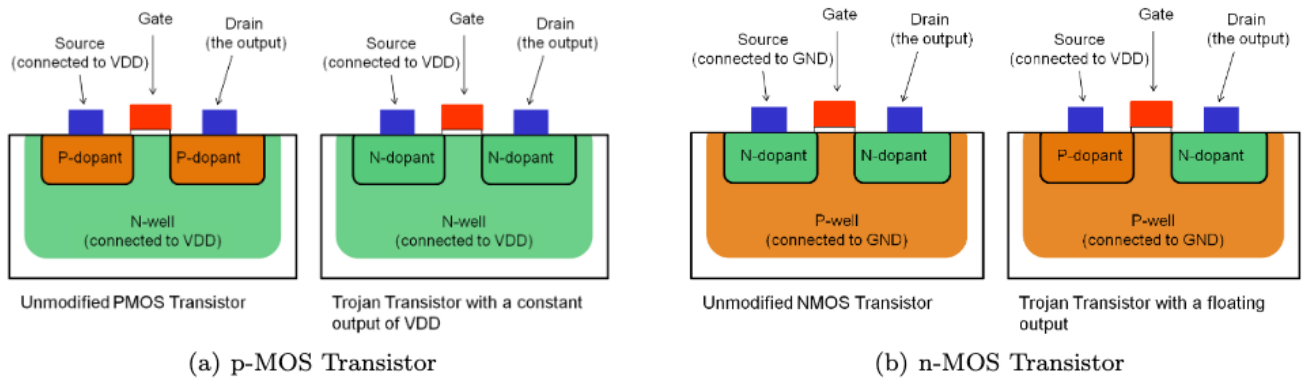
Το Bitcoin λύνει το πρόβλημα της εμπιστοσύνης με το να είναι πλήρως αποκεντρωμένο, χωρίς κεντρικό server ή έμπιστα μέρη. Ούτε καν έμπιστα τρίτα μέρη, αλλά έμπιστα μέρη, τελεία και παύλα. Όταν δεν υπάρχει κεντρική αρχή, απλά δεν υπάρχει κανείς που μπορείς να εμπιστευτείς. Η πλήρης αποκέντρωση είναι η καινοτομία. Είναι η ρίζα της ανθεκτικότητας του Bitcoin, ο λόγος για τον οποίο είναι ακόμα ζωντανό. Η αποκέντρωση είναι επίσης ο λόγος για τον οποίο έχουμε την εξόρυξη (mining), τους κόμβους (nodes), τα υλισμικά πορτοφόλια (hardware wallets) και ναι, το blockchain. Το μόνο που πρέπει να “εμπιστευτείτε” είναι ότι η κατανόηση που έχουμε των μαθηματικών και της φυσικής δεν είναι εντελώς λανθασμένη και ότι η πλειοψηφία των miners ενεργεί ειλικρινά (κάτι που τους δίνεται κίνητρο να κάνουν).

Ενώ ο κανονικός κόσμος λειτουργεί υπό την υπόθεση του «*εμπιστεύσου, αλλά επαλήθευσε*», το Bitcoin λειτουργεί υπό την υπόθεση του «*μην εμπιστεύεσαι, επαλήθευσε*». Ο Satoshi έκανε τη σημασία της άρσης της εμπιστοσύνης πολύ ξεκάθαρη τόσο στην εισαγωγή όσο και στον επίλογο του Bitcoin whitepaper.

“Επίλογος: Έχουμε προτείνει ένα σύστημα για ηλεκτρονικές συναλλαγές χωρίς να στηρίζεται σε εμπιστοσύνη”. — Satoshi Nakamoto

Παρατηρήστε ότι το “χωρίς να στηρίζεται σε εμπιστοσύνη” χρησιμοποιείται εντός ενός πολύ συγκεκριμένου πλαισίου εδώ. Μιλάμε για έμπιστα τρίτα μέρη, δηλαδή για άλλες οντότητες στις οποίες εμπιστεύεστε την παραγωγή, κατοχή και επεξεργασία των χρημάτων σας. Υποτίθεται, για παράδειγμα, ότι μπορείτε να εμπιστευτείτε τον υπολογιστή σας.

Όπως έδειξε ο Ken Thompson στη διάλεξη του βραβείου Turing του, η εμπιστοσύνη είναι ένα εξαιρετικά δύσκολο πράγμα στον υπολογιστικό κόσμο. Κατά την εκτέλεση ενός προγράμματος, πρέπει να εμπιστεύεστε όλων των ειδών τα λογισμικά (και υλικά) τα οποία, θεωρητικά, θα μπορούσαν να αλλάξουν με κακόβουλο τρόπο το πρόγραμμα που προσπαθείτε να εκτελέσετε. Όπως συνοψίζει και ο Thompson στο Reflections on Trusting Trust: “Το ηθικό δίδαγμα είναι προφανές. Δεν μπορείτε να εμπιστεύεστε κώδικα που δεν δημιουργήσατε πλήρως οι ίδιοι.”



Stealthy Dopant-Level Hardware Trojans by Becker, Regazzoni, Paar, Burleson

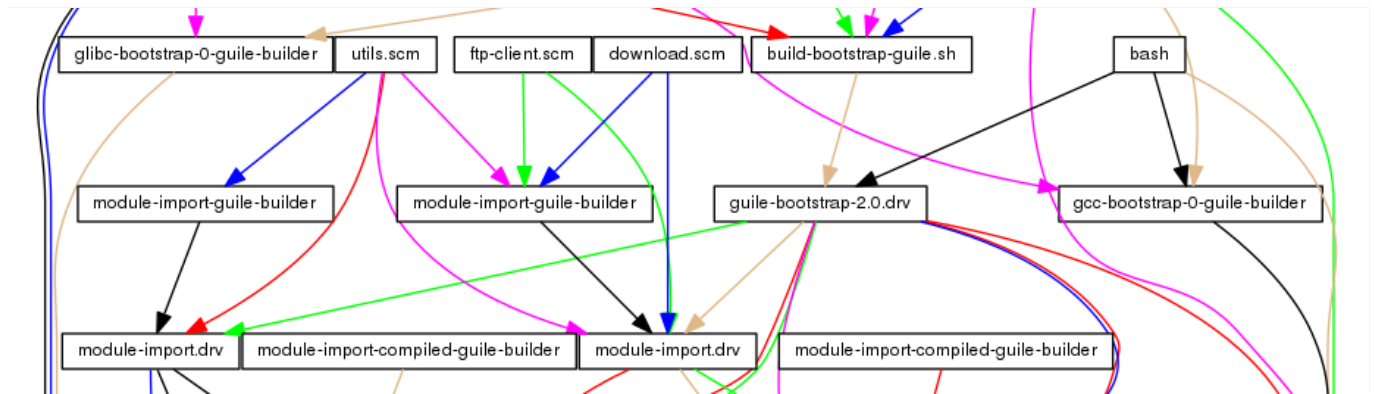
Ακούγεται τρομακτικό; Λοιπόν, ακόμη και αν μπορούσατε να κατασκευάσετε τα πάντα από το μηδέν, θα έπρεπε παρ' όλα αυτά να εμπιστευτείτε τα υποκείμενα μαθηματικά. Θα πρέπει να εμπιστευτείτε ότι το [secr256k1](#) είναι μια ελλειπτική καμπύλη χωρίς backdoors. Ναι, κακόβουλα backdoors μπορούν να εισαχθούν στα μαθηματικά θεμέλια των κρυπτογραφικών λειτουργιών και θα μπορούσε να ισχυριστεί κανείς ότι έχει ήδη συμβεί τουλάχιστον μία φορά. Υπάρχουν σοβαροί λόγοι να είστε παρανοϊκοί, και το γεγονός ότι όλα, από το υλικό σας, μέχρι το λογισμικό σας και τις ελλειπτικές καμπύλες που χρησιμοποιούνται μπορούν να έχουν backdoors είναι μερικοί από αυτούς.

“Μην εμπιστεύεστε. Επαληθεύστε.”

Τα παραπάνω παραδείγματα δείχνουν ότι ο υπολογισμός που δεν απαιτεί εμπιστοσύνη είναι ουτοπικός. Το Bitcoin είναι ίσως το μόνο σύστημα που πλησιάζει περισσότερο αυτή την ουτοπία, παρ' όλα αυτά εξακολουθεί να χρησιμοποιεί την ελάχιστη δυνατή εμπιστοσύνη, με στόχο την άρση αυτής όπου αυτό είναι δυνατό. Αναμφισβήτητα, η “αλυσίδα” εμπιστοσύνης είναι ατελείωτη, καθώς θα πρέπει να εμπιστευτείτε ότι ο υπολογισμός απαιτεί ενέργεια, ότι το P δεν ισοδυναμεί με NP και ότι βρίσκεστε στην θεμελιώδη πραγματικότητα και όχι φυλακισμένοι σε κάποια προσομοίωση από κακόβουλους αυτοργούς.

Προγραμματιστές εργάζονται σε εργαλεία και διαδικασίες για να ελαχιστοποιήσουν περαιτέρω οποιαδήποτε εναπομείνουσα εμπιστοσύνη. Για παράδειγμα, προγραμματιστές του Bitcoin δημιούργησαν το [Gitian](#), το οποίο είναι μια μέθοδος διανομής λογισμικού για τη δημιουργία ντετερμινιστικών εκδόσεων. Η ιδέα είναι ότι αν πολλαπλοί προγραμματιστές είναι σε θέση να αναπαράγουν πανομοιότυπα δυαδικά αρχεία, μειώνεται η πιθανότητα κακόβουλης παρέμβασης. Τα εξεζητημένα backdoors δεν είναι ο μόνος τρόπος επίθεσης. Ο απλός εκβιασμός είναι επίσης μια πραγματική απειλή. Όπως και στο κύριο πρωτόκολλο, η αποκέντρωση χρησιμοποιείται για την ελαχιστοποίηση της εμπιστοσύνης.

Καταβάλλονται διάφορες προσπάθειες για να βελτιωθεί το πρόβλημα της κότας και του αβγού όσον αφορά το bootstrapping, το οποίο τόσο εξαιρετικά επισήμανε το hack του Ken Thompson. Μια τέτοια προσπάθεια είναι το Guix (προφερόμενο geeks), το οποίο χρησιμοποιεί μια συναρτησιακά δηλωθείσα διαχείριση πακέτων που οδηγεί σε αναπαραγωγίμες κατασκευές bit-for-bit εκ σχεδιασμού. Το αποτέλεσμα είναι ότι δεν χρειάζεται να εμπιστευέστε πλέον κανέναν διακομιστή παροχής λογισμικού, αφού μπορείτε να επαληθεύσετε ότι το δυαδικό αρχείο που σας παρέχεται δεν έχει παραποιηθεί μέσω της ανακατασκευής του από το μηδέν. Πρόσφατα, συγχωνεύθηκε ένα pull-request για να ενσωματώσει το Guix στη διαδικασία κατασκευής του Bitcoin.



Ποιό ήταν πρώτο, η κότα ή το αβγό;

Ευτυχώς, το Bitcoin δεν βασίζεται σε ένα μόνο αλγόριθμο ή κομμάτι υλικού. Ένα αποτέλεσμα της ριζικής αποκέντρωσης του Bitcoin είναι ένα κατανομημένο μοντέλο ασφάλειας. Παρόλο που τα παραπάνω περιγραφόμενα backdoors δεν πρέπει να υποτιμούνται, είναι απίθανο ότι κάθε λογισμικό πορτοφόλι, κάθε υλισμικό πορτοφόλι, κάθε κρυπτογραφική βιβλιοθήκη, κάθε εφαρμογή κόμβου και κάθε μεταγλωττιστής κάθε γλώσσας έχει υπονομευθεί. Δυνατό, αλλά εξαιρετικά απίθανο.

Σημειώστε ότι μπορείτε να δημιουργήσετε ένα ιδιωτικό κλειδί χωρίς να βασίζεστε σε οποιοδήποτε υπολογιστικό υλικό ή λογισμικό. Μπορείτε να ρίξετε ένα νόμισμα μερικές φορές, αν και ανάλογα με το νόμισμά σας και το στυλ ριζήματος, η πηγή της τυχαιότητας αυτής μπορεί να μην είναι επαρκώς τυχαία. Υπάρχει λόγος για τον οποίο πρωτόκολλα αποθήκευσης όπως το Glacier συμβουλεύουν να χρησιμοποιείτε ζάρια ποιότητας καζίνο ως μία εκ των δύο πηγών εντροπίας.

Το Bitcoin με ανάγκασε να σκεφτώ με τι πραγματικά συνεπάγεται το να μην εμπιστεύεσαι κανέναν. Αύξησε την αντίληψή μου στο πρόβλημα του bootstrapping και την έμμεση “αλυσίδα” εμπιστοσύνης στην ανάπτυξη και εκτέλεση λογισμικού. Αύξησε επίσης την αντίληψή μου στους πολλούς τρόπους με τους οποίους μπορεί να υπονομευθεί το λογισμικό και το υλικό.

Το Bitcoin μου έμαθε να μην εμπιστεύομαι, αλλά να επαληθεύω.

Down the Rabbit Hole

- [Reflections on Trusting Trust](#) by Ken Thompson
- [51% Attack](#) by Bitcoin Developer Guide Contributors
- [Bootstrapping](#) by Guix Manual Contributors
- [Dual EC DRBG](#) by Wikipedia Contributors
- [ECC Backdoors](#) by Wikipedia Contributors
- [Secp256k1](#) by Bitcoin Wiki Contributors

. . .

Μάθημα 17: Ο προσδιορισμός της ώρας απαιτεί έργο

“Θεέ μου, Θεέ μου! Θα έχω αργήσει!”

Συχνά λέγεται ότι τα bitcoin εξορύσσονται επειδή χιλιάδες υπολογιστές εργάζονται για την επίλυση πολύπλοκων μαθηματικών προβλημάτων. Ορισμένα προβλήματα πρέπει να επιλυθούν και αν υπολογίσετε τη σωστή απάντηση, θα “παράγετε” ένα bitcoin. Ενώ αυτή η απλοποιημένη θεώρηση της εξόρυξης των bitcoin μπορεί να επικοινωνηθεί πιο εύκολα, υπερβαίνει κάπως τον ορισθέντα στόχο. Τα bitcoin δεν παράγονται ή δημιουργούνται και η όλη ταλαιπωρία δεν αφορά στην επίλυση συγκεκριμένων μαθηματικών προβλημάτων. Επίσης, τα μαθηματικά δεν είναι ιδιαίτερα περίπλοκα. Αυτό που είναι περίπλοκο είναι ο προσδιορισμός της ώρας σε ένα αποκεντρωμένο σύστημα.

Όπως περιγράφεται στο whitepaper, το σύστημα proof-of-work (επίσης γνωστό ως mining) είναι ένας τρόπος για την υλοποίηση ενός καταναμημένου διακομιστή χρονοσήμανσης.

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.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Όταν έμαθα για πρώτη φορά πώς δουλεύει το Bitcoin, πίστευα επίσης ότι το proof-of-work είναι μη αποδοτικό και σπάταλο. Μετά από λίγο, άρχισα να αλλάζω την αντίληψή μου για την κατανάλωση ενέργειας του Bitcoin. Φαίνεται ότι το proof-of-work παραμένει σήμερα ευρέως παρανοημένο, στο έτος 10 AB (μετά Bitcoin).

Δεδομένου ότι τα προβλήματα που πρέπει να λυθούν στο proof-of-work είναι τεχνητά, πολλοί άνθρωποι φαίνεται να πιστεύουν ότι είναι *άχρηστη* δουλειά. Εάν το σημείο εστίασης βρίσκεται καθαρά στον υπολογισμό, τότε πρόκειται για κατανοητό συμπέρασμα. Αλλά το Bitcoin δεν αφορά τον υπολογισμό. Έχει να κάνει με την *ανεξάρτητη συμφωνία για τη σειρά των πραγμάτων*.

Το proof-of-work είναι ένα σύστημα στο οποίο όλοι μπορούν να επιβεβαιώσουν τι συνέβη και με ποιά σειρά συνέβη. Αυτή η ανεξάρτητη επιβεβαίωση είναι αυτό που οδηγεί σε συναίνεση, μια ατομική συμφωνία από πολλαπλά συμβαλλόμενα μέρη για το ποιός κατέχει τι.

Σε ένα ριζικά αποκεντρωμένο περιβάλλον, δεν έχουμε την πολυτέλεια της απόλυτης ώρας. Οποιοδήποτε ρολόι θα εισήγαγε ένα έμπιστο τρίτο μέρος, ένα κεντρικό σημείο στο σύστημα στο οποίο πρέπει να βασιζόμαστε και που θα μπορούσε να γίνει στόχος επίθεσης. «Ο χρονισμός είναι το βασικό πρόβλημα», όπως τονίζει ο Grisha Trubetskoy. Και ο Satoshi έλυσε με έξοχο τρόπο αυτό το πρόβλημα εφαρμόζοντας ένα αποκεντρωμένο ρολόι μέσω ενός proof-of-work blockchain. Όλοι συμφωνούν εκ των προτέρων ότι η αλυσίδα με το περισσότερο σωρευτικό έργο είναι η πηγή της αλήθειας. Είναι εξ ορισμού αυτό που πραγματικά συνέβη. Η συμφωνία αυτή είναι αυτό που είναι πλέον γνωστό ως συναίνεση Nakamoto.

“Το δίκτυο βάζει χρονοσημάνσεις σε συναλλαγές θέτοντας τις τιμές κατακερματισμού εντός μίας εξελισσόμενης αλυσίδας που χρησιμεύει ως απόδειξη της σειράς των γεγονότων που μαρτυρήθηκαν” — Satoshi Nakamoto

Χωρίς έναν σταθερό τρόπο να καθορίσει κανείς την ώρα, δεν υπάρχει σταθερός τρόπος να ξεχωρίσουμε το πριν από το μετά. Η αξιόπιστη διάταξη είναι αδύνατη. Όπως αναφέρθηκε παραπάνω, η συναίνεση Nakamoto είναι ο τρόπος με τον οποίο το Bitcoin καθορίζει με συνέπεια την ώρα. Η δομή κινήτρων του συστήματος παράγει ένα πιθανοτικό, αποκεντρωμένο ρολόι, χρησιμοποιώντας τόσο την απληστία όσο και το προσωπικό συμφέρον των ανταγωνιζόμενων συμμετεχόντων. Το γεγονός ότι αυτό το

ρολίοι είναι ανακριβές είναι άσχετο, διότι η σειρά των γεγονότων είναι τελικά ξεκάθαρη και μπορεί να επαληθευτεί από οποιονδήποτε.

Χάρη στο proof-of-work, τόσο η εργασία όσο και η επαλήθευση της εργασίας είναι ριζικά αποκεντρωμένες. Όλοι μπορούν να συμμετάσχουν και να αποχωρήσουν κατά βούληση, και όλοι μπορούν να επαληθεύσουν τα πάντα ανά πάσα στιγμή. Όχι μόνο αυτό, αλλά ο καθένας μπορεί να επαληθεύσει την κατάσταση του συστήματος ξεχωριστά, χωρίς να χρειάζεται να βασιστεί σε κανέναν άλλο για επαλήθευση.

Η κατανόηση του proof-of-work απαιτεί χρόνο. Συχνά φαίνεται να είναι παράλογο, και ενώ οι κανόνες είναι απλοί, οδηγούν σε ιδιαίτερα περίπλοκα φαινόμενα. Για μένα, βοήθησε η αλλαγή της αντίληψής μου για την εξόρυξη. Χρήσιμο, όχι άχρηστο. Επαλήθευση, όχι υπολογισμός. Ώρα, όχι block.

Το Bitcoin μου έμαθε ότι ο καθορισμός της ώρας είναι δύσκολος, ειδικά αν είσαι αποκεντρωμένος.

Through the Looking-Glass

- [Bitcoin's Energy Consumption: A shift in perspective](#)

Down the Rabbit Hole

- [Nothing is Cheaper than Proof of Work](#) by Paul Sztorc
- [Bitcoin Doesn't Waste Electricity](#) by Beautyon
- [Blockchain Proof-of-Work Is a Decentralized Clock](#) by Gregory Trubetskoy
- [The Anatomy of Proof-of-Work](#) by Hugo Nguyen
- [Work is Timeless, Stake is Not](#) by Hugo Nguyen
- [Bitcoin Does Not Waste Energy](#) by Parker Lewis
- [Controlled Supply](#) by Bitcoin Wiki Contributors
- [Mining](#) by Bitcoin Wiki Contributors
- 🎧 [Trace Mayer on Bitcoin Valuation, Trust, and Energy Consumption](#)
TIP#252 hosted by Breston Pysh and Stig Brodersen

. . .

Μάθημα 18: Κινηθείτε αργά και μην σπάσετε πράγματα

Έτσι η βάρκα έπλεε αργά, κάτω από την ηλιόλουστη καλοκαιρινή μέρα, με το χαρούμενο πλήρωμά της και τη μουσική από φωνές και γέλιο...

Μπορεί να είναι ένα νεκρό μάντρα, αλλά το “κινηθείτε γρήγορα και σπάστε πράγματα” εξακολουθεί να είναι ο τρόπος με τον οποίο λειτουργεί η πλειοψηφία του τεχνολογικού κόσμου. Η ιδέα ότι δεν έχει σημασία αν επιτύχουμε το σωστό αποτέλεσμα την πρώτη φορά είναι ένας βασικός πυλώνας της νοοτροπίας του “αποτύχετε νωρίς, αποτύχετε συχνά”. Η επιτυχία μετράται σε ανάπτυξη, έτσι ώστε όσο αναπτύξεστε όλα είναι καλά. Εάν κάτι δεν λειτουργεί αρχικά απλά αλλάζετε κατεύθυνση και επαναλαμβάνετε. Με άλλα λόγια: ρίξτε αρκετά σκατά στον τοίχο και δείτε τι κολλάει.

Το Bitcoin είναι πολύ διαφορετικό. Είναι διαφορετικό ήδη από το σχεδιασμό του. Είναι διαφορετικό εξ ανάγκης. Όπως επεσήμανε ο Satoshi, το ηλεκτρονικό χρήμα έχει δοκιμαστεί πολλές φορές στο παρελθόν και όλες οι προηγούμενες προσπάθειες απέτυχαν επειδή υπήρχε πάντοτε ένα κεφάλι που μπορούσε να αποκοπεί. Η καινοτομία του Bitcoin είναι ότι πρόκειται για ένα κτήνος χωρίς κεφάλια.

“Πολλοί άνθρωποι απορρίπτουν αυτόματα το ηλεκτρονικό χρήμα ως χαμένη υπόθεση εξαιτίας όλων των εταιρειών που απέτυχαν από τη δεκαετία του 1990. Ελπίζω πως είναι προφανές ότι μόνο η κεντρικά ελεγχόμενη φύση αυτών των συστημάτων ήταν που τους καταδίκασε”. — Satoshi Nakamoto

Μια συνέπεια αυτής της ριζικής αποκέντρωσης είναι μια εγγενής αντίσταση στην αλλαγή. Το “κινηθείτε γρήγορα και σπάστε πράγματα” δεν λειτουργεί και ούτε πρόκειται ποτέ να λειτουργήσει στο επίπεδο βάσης του Bitcoin. Ακόμα κι αν ήταν επιθυμητό, δεν θα ήταν δυνατό χωρίς να πειστούν *όλοι* να αλλάξουν τον τρόπο λειτουργίας τους. Αυτό σημαίνει κατανεμημένη συναίνεση. Αυτή είναι η φύση του Bitcoin.

“Η φύση του Bitcoin είναι τέτοια που από τη στιγμή που κυκλοφόρησε η έκδοση 0.1, ο σχεδιασμός του πηρύνα κατοχυρώθηκε για το υπόλοιπο της ζωής του.”
— Satoshi Nakamoto

Αυτή είναι μια από τις πολλές παράδοξες ιδιότητες του Bitcoin. Όλοι πιστέψαμε ότι οτιδήποτε είναι λογισμικό μπορεί να αλλάξει εύκολα. Αλλά η φύση του θηρίου αυτού κάνει την αλλαγή του αναθεματισμένα δύσκολη.

Όπως πολύ όμορφα δείχνει ο Hasu στο [Unpacking Bitcoin's Social Contract](#), η αλλαγή των κανόνων του Bitcoin είναι δυνατή μόνο μέσω της πρότασης μιας αλλαγής, και κατόπιν πείθοντας όλους τους χρήστες του Bitcoin να υιοθετήσουν αυτήν την αλλαγή. Αυτό καθιστά το Bitcoin αρκετά ανθεκτικό στην αλλαγή, παρόλο που είναι λογισμικό.

Η ανθεκτικότητα αυτή είναι μία από τις πιο σημαντικές ιδιότητες του Bitcoin. Τα κρίσιμα συστήματα λογισμικού πρέπει να είναι αντι-εύθραυστα (antifragile), πράγμα που εγγυάται η αλληλεπίδραση του κοινωνικού και τεχνικού επιπέδου του Bitcoin. Τα νομισματικά συστήματα είναι από τη φύση τους ανταγωνιστικά και, όπως γνωρίζουμε εδώ και χιλιάδες χρόνια, τα στερεά θεμέλια είναι απαραίτητα σε ένα ανταγωνιστικό περιβάλλον.

“καί κατέβη ἡ βροχή καί ἤλθον οἱ ποταμοί καί ἔπνευσαν οἱ ἄνεμοι καί προσέπεσον τῇ οἰκίᾳ ἐκείνῃ, καί οὐκ ἔπεσε· τεθεμελίωτο γάρ ἐπί τήν πέτραν.” —
[Κατά Ματθαῖον 7:24–27](#)

Μπορεί να υποστηριχθεί ότι σε αυτή την παραβολή των σοφών και των ανόητων οικοδόμων, το Bitcoin δεν είναι το σπίτι. Είναι η πέτρα. Αμετάβλητο, ακίνητο, παρέχοντας τα θεμέλια για ένα νέο χρηματοπιστωτικό σύστημα.

Ακριβώς όπως οι γεωλόγοι, που γνωρίζουν ότι οι σχηματισμοί βράχων συνεχώς κινούνται και εξελίσσονται, μπορεί κανείς να δει ότι το Bitcoin πάντοτε κινείται και εξελίσσεται επίσης. Απλά πρέπει να ξέρετε πού να κοιτάξετε και πώς να το δείτε.

Η εισαγωγή των [pay to script hash](#) και [segregated witness](#) αποτελούν απόδειξη ότι οι κανόνες του Bitcoin μπορούν να αλλάξουν εάν αρκετοί χρήστες είναι πεπεισμένοι ότι η υιοθέτηση της εν λόγω αλλαγής είναι προς όφελος του δικτύου. Το τελευταίο επέτρεψε την ανάπτυξη του [lightning network](#), το οποίο είναι ένα από τα σπίτια που χτίζονται πάνω στα στερεά θεμέλια του Bitcoin. Οι μελλοντικές αναβαθμίσεις, όπως οι [Schnorr signatures](#), θα ενισχύσουν την αποτελεσματικότητα και ιδιωτικότητα καθώς και τα script (που διαβάζονται: smart contracts), τα οποία θα είναι πανομοιότυπα με τις απλές συναλλαγές χάρη στο [Taproot](#). Οι σοφοί οικοδόμοι πράγματι χτίζουν πάνω σε στερεά θεμέλια.

Ο Satoshi δεν ήταν μόνο ένας τεχνολογικά σοφός οικοδόμος. Κατανοούσε επίσης ότι θα ήταν αναγκαίο να ληφθούν *ιδεολογικά* σοφές αποφάσεις.

“Το να είναι ανοιχτού κώδικα σημαίνει ότι ο καθένας μπορεί να ελέγξει ανεξάρτητα τον κώδικα. Εάν ήταν κλειστού κώδικα, κανείς δεν θα μπορούσε να επαληθεύσει την ασφάλεια. Νομίζω ότι είναι απαραίτητο ένα πρόγραμμα αυτής της φύσεως να είναι ανοιχτού κώδικα.” — Satoshi Nakamoto

Η διαφάνεια είναι υψίστης σημασίας για την ασφάλεια καθώς και εγγενής στον ανοικτό κώδικα και στο κίνημα του ελεύθερου λογισμικού. Όπως επεσήμανε ο Satoshi, τα ασφαλή πρωτόκολλα και ο κώδικας που τα εφαρμόζει πρέπει να είναι ανοικτά — δεν υπάρχει ασφάλεια μέσω ασάφειας. Ένα άλλο πλεονέκτημα σχετίζεται και πάλι με την αποκέντρωση: κώδικας ο οποίος μπορεί να εκτελείται, να μελετάται, να τροποποιείται, να αντιγράφεται και να διανέμεται ελεύθερα εξασφαλίζει ότι θα είναι ευρέως διαδεδομένος.

Η ριζικά αποκεντρωμένη φύση του Bitcoin είναι αυτό που το κάνει να κινείται αργά και συνετά. Ένα δίκτυο κόμβων, με τον καθένα εκτελούμενο από ένα κυρίαρχο άτομο, είναι εγγενώς ανθεκτικό στην αλλαγή — κακόβουλη ή μη. Δίχως κάποιον τρόπο για αναγκασμό των χρηστών σε ενημέρωση λογισμικού, η μόνη μέθοδος για να εισαχθούν αλλαγές είναι να πειστούν σιγά σιγά κάθε ένα από αυτά τα άτομα να υιοθετήσουν μια αλλαγή. Αυτή η μη κεντρική διαδικασία εισαγωγής και ανάπτυξης αλλαγών είναι αυτό που καθιστά το δίκτυο εξαιρετικά ανθεκτικό στις κακόβουλες αλλαγές. Είναι επίσης αυτό που κάνει την επισκευή σπασμένων πραγμάτων πιο δύσκολη απ' ό,τι σε ένα κεντρικό περιβάλλον, γι' αυτό όλοι προσπαθούν να μην σπάσουν πράγματα ευθύς εξαρχής.

Το Bitcoin μου έμαθε ότι το να κινείται αργά είναι ένα από τα χαρακτηριστικά του, και όχι σφάλμα.

Through the Looking-Glass

- [Lesson 1: Immutability and Change](#)

Down the Rabbit Hole

- [Bitcoin Is Not Too Slow](#) by Parker Lewis
- [Parable of the Wise and the Foolish Builders](#) by Wikipedia Contributors

- [Segregated Witness \(SegWit\)](#). by Bitcoin Wiki Contributors
- [Pay to Script Hash \(P2SH\)](#). by Bitcoin Wiki Contributors
- [Taproot proposal](#) by Gregory Maxwell
- [Schnorr signatures BIP](#) by Pieter Wuille

. . .

Μάθημα 19: Η ιδιωτικότητα δεν έχει πεθάνει

Οι παίκτες όλοι έπαιζαν ταυτόχρονα χωρίς να περιμένουν για σειρές, και τσακωνώντουσαν όλο αυτό το διάστημα στο μέγιστο της φωνής τους, και σε πολύ λίγα λεπτά η Βασίλισσα ήταν ξέφρενα παθιασμένη και ξεκίνησε να χτυπάει τα πόδια της και να φωνάζει “κόψτε του το κεφάλι!” ή “κόψτε της το κεφάλι!” περίπου μία φορά το λεπτό.

Εάν πρόκειται να πιστέψουμε τους ειδήμονες, τότε η ιδιωτικότητα έχει πεθάνει από τη δεκαετία του 80. Η ψευδώνυμη εφεύρεση του Bitcoin και άλλα γεγονότα της πρόσφατης ιστορίας δείχνουν ότι αυτό δεν ισχύει. Η ιδιωτικότητα είναι ζωντανή, παρόλο που δεν είναι καθόλου εύκολο να δραπετεύσουμε από το κράτος παρακολούθησης.

Ο Satoshi κατέβαλλε μεγάλη προσπάθεια για να καλύψει τα ίχνη του και να αποκρύψει την ταυτότητά του. Δέκα χρόνια μετά, είναι ακόμα άγνωστο αν ο Satoshi Nakamoto ήταν ένα άτομο, μια ομάδα ανθρώπων, αρσενικό, θηλυκό ή χρονοταξιιδιωτικό AI, το οποίο έθεσε τον εαυτό του σε λειτουργία για να κατακτήσει τον κόσμο. Αφήνοντας τις θεωρίες συνωμοσίας στην άκρη, ο Satoshi επέλεξε να ταυτίσει τον εαυτό του με Ιαπωνικό αρσενικό, γι 'αυτό δεν υποθέτω, αλλά σέβομαι το φύλο που επέλεξε και αναφέρομαι σε αυτόν ως *αρσενικού φύλου*.



Δεν είμαι ο Dorian Nakamoto.

Όποια και αν είναι η πραγματική του ταυτότητα, ο Satoshi κατάφερε να την κρύψει. Έθεσε ένα ενθαρρυντικό παράδειγμα για όλους όσους επιθυμούν να παραμείνουν ανώνυμοι: είναι δυνατό να υπάρχει ιδιωτικότητα στο διαδίκτυο.

“Η κρυπτογράφηση λειτουργεί. Με τη σωστή εφαρμογή της, τα ισχυρά συστήματα κρυπτογραφίας είναι ένα από τα λίγα πράγματα στα οποία μπορείτε να βασιστείτε.” — Edward Snowden

Ο Satoshi δεν ήταν ο πρώτος ψευδώνυμος ή ανώνυμος εφευρέτης και δεν θα είναι ο τελευταίος. Μερικοί έχουν μιμηθεί άμεσα αυτό το ψευδώνυμο στυλ δημοσίευσης, όπως ο Tom Elvis Yedusor της φήμης του MimbleWimble, ενώ άλλοι έχουν δημοσιεύσει προηγμένες μαθηματικές αποδείξεις παραμένοντας εντελώς ανώνυμοι.

Είναι ένας παράξενος καινούργιος κόσμος στον οποίο ζούμε. Ένας κόσμος όπου η ταυτότητα είναι προαιρετική, οι συνεισφορές γίνονται αποδεκτές με βάση την αξία τους και οι άνθρωποι μπορούν να συνεργαστούν και να συναλλάσσονται ελεύθερα. Θα χρειαστεί κάποια προσαρμογή για να εξοικιωθούμε με αυτά τα νέα πρότυπα, αλλά πιστεύω ακράδαντα ότι όλα αυτά έχουν τη δυνατότητα να αλλάξουν τον κόσμο προς το καλύτερο.

Πρέπει όλοι να θυμόμαστε ότι η ιδιωτικότητα αποτελεί θεμελιώδες ανθρώπινο δικαίωμα. Και όσο οι άνθρωποι ασκούν και υπερασπίζονται αυτά τα δικαιώματα, η μάχη για την ιδιωτικότητα κάθε άλλο παρά έχει ολοκληρωθεί. Το Bitcoin μου έμαθε ότι η ιδιωτικότητα δεν έχει πεθάνει.

Down the Rabbit Hole

- Digital Cash & Privacy by Hal Finney
- The Case for Privacy by David D. Friedman
- Protect Your Privacy by Bitcoin.org
- How Lightning Layers Privacy on Top of Bitcoin by Aaron van Wirdum
- Dandelions, and a Bright Future for Bitcoin Privacy by Guy Swann
- The Case for Electronic Cash by Jerry Brito
- We Must Protect our Ability to Transact Privately Online by Jerry Brito
- Bitcoin Wiki's Privacy Article by Chris Belcher

- [How Private is Bitcoin?](#) by Eric Wall
- [FAQ for Wasabi Wallet](#) by 6102bitcoin
- [FAQ for Hodl Privacy](#) by 6102bitcoin
- [Bitcoin and Privacy](#) by Edward Snowden
- [FAQ for Samurai Wallet's Whirlpool](#) by 6102bitcoin
- [Universal Declaration of Human Rights](#) by the United Nations
- [A lower bound on the length of the shortest superpattern](#) by Anonymous 4chan Poster, Robin Houston, Jay Pantone, and Vince Vatter
- 🦉 [Jameson Lopp on Privacy, Security, and Personal Sovereignty](#). C&G#35 hosted by CryptoDantes and Stigofthepump

. . .

Μάθημα 20: Οι Cypherpunks γράφουν κώδικα

Βλέπω ότι προσπαθείς να εφεύρεις κάτι.

Όπως πολλές μεγάλες ιδέες, έτσι και το Bitcoin δεν βγήκε από το πουθενά. Έγινε εφικτό χρησιμοποιώντας και συνδυάζοντας πολλές καινοτομίες και ανακαλύψεις στα μαθηματικά, τη φυσική, την πληροφορική και άλλους τομείς. Αν και αναμφισβήτητα μεγαλοφυΐα, ο Satoshi δεν θα μπορούσε να έχει επινοήσει το Bitcoin χωρίς τους γίγαντες στον οποίον τις πλάτες στάθηκε.

«Αυτός που μόνο επιθυμεί και ελπίζει δεν παρεμβαίνει ενεργά στην πορεία των γεγονότων και στη διαμόρφωση του ίδιου του πεπρωμένου». —
Ludwig Von Mises

Ένας από αυτούς τους γίγαντες είναι ο Eric Hughes, ένας από τους ιδρυτές του cypherpunk κινήματος και συγγραφέας του [cypherpunk manifesto](#). Είναι δύσκολο να φανταστούμε ότι ο Satoshi δεν επηρεάστηκε από αυτό το μανιφέστο. Μιλά για πολλά πράγματα που το Bitcoin επιτρέπει και αξιοποιεί, όπως άμεσες και ιδιωτικές συναλλαγές, ηλεκτρονικό χρήμα και μετρητά, ανώνυμα συστήματα και προστασία της ιδιωτικότητας μέσω κρυπτογραφίας και ψηφιακών υπογραφών.

“Η ιδιωτικότητα είναι απαραίτητη για μια ανοιχτή κοινωνία στην ηλεκτρονική εποχή. [...] Δεδομένου ότι επιθυμούμε την ιδιωτικότητα, πρέπει να διασφαλίσουμε ότι κάθε συμβαλλόμενο μέρος μιας συναλλαγής έχει γνώση μόνο αυτού που είναι άμεσα απαραίτητο για τη συγκεκριμένη συναλλαγή. [...]

Επομένως, η ιδιωτικότητα σε μια ανοιχτή κοινωνία απαιτεί ανώνυμα συστήματα συναλλαγών. Μέχρι τώρα, τα μετρητά ήταν το κύριο αυτό σύστημα. Ένα ανώνυμο σύστημα συναλλαγών δεν είναι ένα μυστικό σύστημα συναλλαγών. [...]

Εμείς οι Cypherpunks είμαστε αφοσιωμένοι στην κατασκευή ανώνυμων συστημάτων.

Υπερασπιζόμαστε την ιδιωτικότητά μας με τη χρήση κρυπτογραφίας, με ανώνυμα συστήματα προώθησης αλληλογραφίας, με ψηφιακές υπογραφές και με ηλεκτρονικό χρήμα.

Οι Cypherpunks γράφουν κώδικα. “ — Eric Hughes

Οι Cypherpunks δεν βρίσκουν καταφύγιο στις ελπίδες και τις ευχές. Παρεμβαίνουν ενεργά στην πορεία των γεγονότων και διαμορφώνουν οι ίδιοι το πεπρωμένο τους. Οι Cypherpunks γράφουν κώδικα.

Έτσι, με αληθινά Cypherpunk τρόπο, ο Satoshi κάθισε και άρχισε να γράφει κώδικα. Κώδικα που πήρε μια αφηρημένη ιδέα και απέδειξε στον κόσμο ότι πραγματικά λειτουργούσε. Κώδικα που έσπειρε τον σπόρο μιας νέας οικονομικής πραγματικότητας. Χάρη σε αυτόν τον κώδικα, ο καθένας μπορεί να επιβεβαιώσει ότι αυτό το καινοτόμο σύστημα λειτουργεί πραγματικά, και κάθε 10 λεπτά περίπου, το Bitcoin αποδεικνύει στον κόσμο ότι εξακολουθεί να ζει.

```

23 map<uint256, CBlockIndex*> mapBlockIndex;
24 const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
25 CBlockIndex* pindexGenesisBlock = NULL;
26 int nBestHeight = -1;
27 uint256 hashBestChain = 0;
28 CBlockIndex* pindexBest = NULL;
  :
675 int64 CBlock::GetBlockValue(int64 nFees) const
676 {
677     int64 nSubsidy = 50 * COIN;
678
679     // Subsidy is cut in half every 4 years
680     nSubsidy >>= (nBestHeight / 210000);
681
682     return nSubsidy + nFees;
683 }
684
685 unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
686 {
687     const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
688     const unsigned int nTargetSpacing = 10 * 60;
689     const unsigned int nInterval = nTargetTimespan / nTargetSpacing;
690
691     // Genesis block
692     if (pindexLast == NULL)
693         return bnProofOfWorkLimit.GetCompact();

```

Αποσπάσματα κώδικα από την Bitcoin έκδοση 0.1.0

Για να σιγουρευτεί ότι η καινοτομία του υπερβαίνει τη φαντασία και γίνεται πραγματικότητα, ο Satoshi έγραψε κώδικα για να υλοποιήσει την ιδέα του πριν γράψει το whitpaper. Επιβεβαίωσε επίσης να μην καθυστερήσει οποιαδήποτε κυκλοφορία επ' αόριστον. Εν τέλει, “πάντα θα υπάρχει ένα ακόμα πράγμα που πρέπει να γίνει”.

“Έπρεπε να γράψω όλο τον κώδικα προτού μπορέσω να πείσω τον εαυτό μου ότι θα μπορούσα να λύσω κάθε πρόβλημα, έπειτα έγραψα την εργασία”. — Satoshi Nakamoto

Στον σημερινό κόσμο των ατελείωτων υποσχέσεων και της αμφίβολης εκτέλεσης, μια άσκηση αφιερωμένης κατασκευής ήταν απελπιστικά αναγκαία. Να είστε σκόπιμοι, πείστε τον εαυτό σας ότι μπορείτε πραγματικά να λύσετε τα προβλήματα, και εφαρμόσετε τις λύσεις. Όλοι μας θα έπρεπε να επιδιώκουμε να είμαστε λίγο πιο cypherpunk.

Το Bitcoin μου έμαθε ότι οι cypherpunks γράφουν κώδικα.

Down the Rabbit Hole

- [The Crypto Anarchist Manifesto](#) by Timothy C. May
- [A Cypherpunk's Manifesto](#) by Eric Hughes

- [The Cyphernomicon](#) by Timothy C. May
- [Bitcoin P2P e-cash paper announcement](#) by Satoshi Nakamoto
- [Bitcoin version 0.1.0 announcement](#) by Satoshi Nakamoto

. . .

Μάθημα 21: Μεταφορές για το μέλλον του Bitcoin

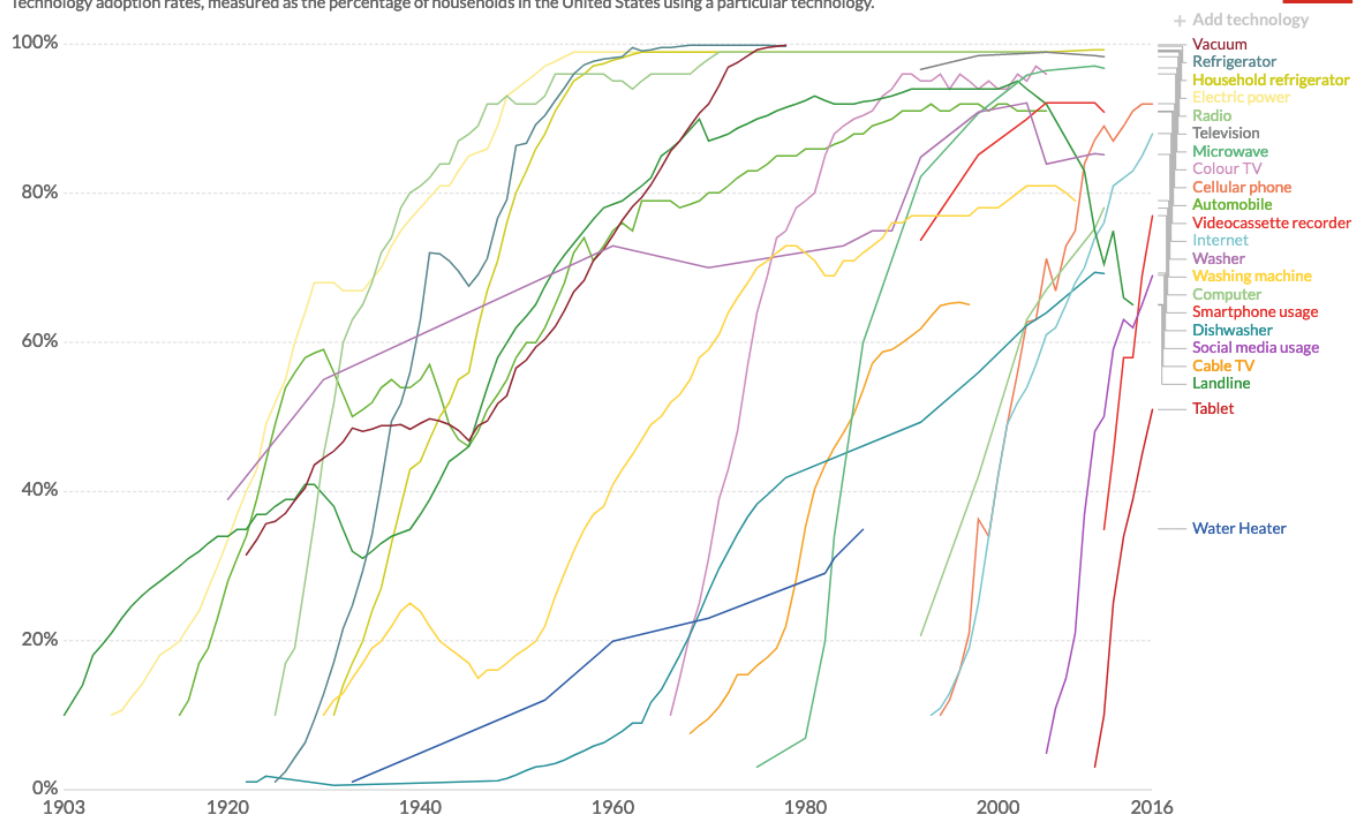
Ξέρω ότι κάτι ενδιαφέρον είναι βέβαιο ότι θα συμβεί...

Τις τελευταίες δεκαετίες, κατέστη προφανές ότι η τεχνολογική καινοτομία δεν ακολουθεί μια γραμμική τάση. Είτε πιστεύετε στην τεχνολογική μοναδικότητα είτε όχι, είναι αναμφισβήτητο ότι η πρόοδος είναι εκθετική σε πολλούς τομείς. Όχι μόνο αυτό, αλλά ο ρυθμός με τον οποίο υιοθετούνται οι τεχνολογίες επιταχύνεται και πριν καν το καταλάβεις, ο θάμνος της τοπικής σχολικής αυλής έχει εξαφανιστεί και τα παιδιά σου χρησιμοποιούν το Snapchat αντ' αυτού. Οι εκθετικές καμπύλες έχουν την τάση να σας ρίχνουν ένα καλό χαστούκι στο πρόσωπο πολύ πριν τις δείτε να έρχονται.

Το Bitcoin είναι μια εκθετική τεχνολογία που βασίζεται σε εκθετικές τεχνολογίες. Το [Our World in Data](#) δείχνει όμορφα την αυξανόμενη ταχύτητα της τεχνολογικής υιοθέτησης, ξεκινώντας το 1903 με την εισαγωγή των σταθερών γραμμών. Σταθερές γραμμές, ηλεκτρισμός, ηλεκτρονικοί υπολογιστές, διαδίκτυο, smartphones όλα ακολουθούν εκθετικές τάσεις στην απόδοση-τιμή και υιοθέτηση. Το Bitcoin επίσης.

Technology adoption in US households

Technology adoption rates, measured as the percentage of households in the United States using a particular technology.



Source: Comin and Hobijn (2004) and others

Note: See the sources tab for definitions of household adoption, or adoption rates, by technology type.

OurWorldInData.org/technology-adoption/ • CC BY

Το Bitcoin είναι κυριολεκτικά εκτός των γραφημάτων.

Το Bitcoin δεν έχει ένα αλλά πολλαπλά δικτυακά φαινόμενα, τα οποία οδηγούν σε εκθετικά μοντέλα ανάπτυξης στον αντίστοιχο τομέα τους: τιμή, χρήστες, ασφάλεια, προγραμματιστές, μερίδιο αγοράς και υιοθέτηση ως παγκόσμιο χρήμα.

Έχοντας επιβιώσει τη βρεφική του ηλικία, το Bitcoin συνεχίζει να αναπτύσσεται καθημερινά σε περισσότερες από μία πτυχές. Ομολογουμένως, η τεχνολογία δεν έχει φτάσει την πλήρης ανάπτυξή της ακόμα. Θα μπορούσε να είναι στην εφηβεία της. Αλλά αν η τεχνολογία είναι εκθετική, ο δρόμος από την αφάνεια στην πανταχού παρουσία σίγουρα είναι σύντομος.



Κινητό τηλέφωνο, περίπου 1965 vs 2019

Στην TED ομιλία του το 2003, ο Jeff Bezos επέλεξε να χρησιμοποιήσει την ηλεκτρική ενέργεια ως μεταφορά για το μέλλον του διαδικτύου. Και τα τρία φαινόμενα — η ηλεκτρική ενέργεια, το Διαδίκτυο, το Bitcoin — είναι τεχνολογίες *ευρείας εφαρμογής*, δίκτυα που επιτρέπουν και άλλα πράγματα. Αποτελούν τις υποδομές πάνω στις οποίες μπορούν να αναπτυχθούν εφαρμογές, θεμελιώδη στη φύση τους.

Η ηλεκτρική ενέργεια υπάρχει εδώ και αρκετό καιρό. Την θεωρούμε δεδομένη. Το διαδίκτυο είναι αρκετά πιο νέο, οι περισσότεροι άνθρωποι όμως το θεωρούν ήδη εξίσου δεδομένο. Το Bitcoin είναι δέκα ετών και έχει εισέλθει στη συνείδηση του κοινού κατά τη διάρκεια του τελευταίου κύκλου ενθουσιασμού. Μόνο οι πρώτοι που το υιοθέτησαν το θεωρούν δεδομένο. Καθώς περνάει κι άλλο ο χρόνος, όλο και περισσότερο οι άνθρωποι θα αναγνωρίσουν το Bitcoin ως κάτι που απλά υπάρχει.

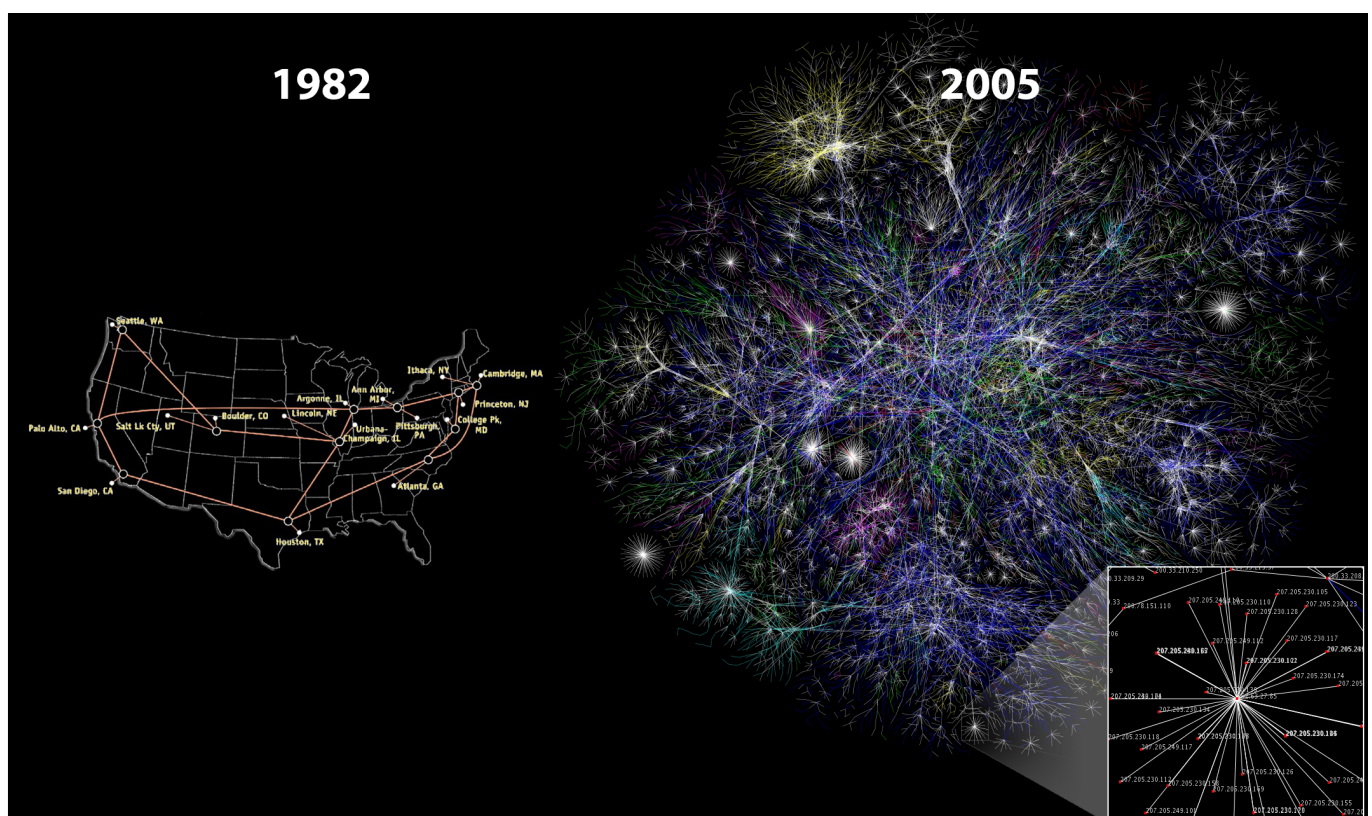
Το 1994, το Διαδίκτυο εξακολουθούσε να είναι συγκεχυμένο και κάθε άλλο παρά ενστικτώδες στη χρήση του. Παρακολουθώντας αυτή την παλιά λήψη του Today Show, είναι προφανές ότι αυτό που τώρα αισθανόμαστε ως φυσικό και διαισθητικό, πράγματι τότε δεν ήταν. Το Bitcoin εξακολουθεί να είναι δυσνόητο και άγνωστο στους

περισσότερους, αλλά όπως και το Διαδίκτυο αποτελεί δεύτερη φύση για τους ψηφιακούς ιθαγενείς, το ξόδεμα και στοίβαγμα των sats θα αποτελεί δεύτερη φύση για τους bitcoin ιθαγενείς του μέλλοντος.

“Το μέλλον είναι ήδη εδώ — απλά δεν είναι αρκετά ομοιόμορφα κατανεμημένο”. — William Gibson

Το 1995, περίπου το 15% των αμερικανών ενηλίκων χρησιμοποιούσαν το Διαδίκτυο. Ιστορικά δεδομένα από το Pew Research Center δείχνουν πώς το Διαδίκτυο έχει πλεχτεί στη ζωή όλων μας. Σύμφωνα με μια έρευνα καταναλωτών από την Kaspersky Lab, το 13% των ερωτηθέντων χρησιμοποίησε το Bitcoin και τους κλώνους του για να πληρώσει για προϊόντα το 2018. Ενώ οι πληρωμές δεν είναι η μόνη περίπτωση χρήσης του bitcoin, είναι μία ένδειξη για το πού βρισκόμαστε όσον αφορά το αντίστοιχο χρονικό σημείο στην εξέλιξη του Internet: κάπου στις αρχές έως μέσα της δεκαετίας του '90.

Το 1997, ο Jeff Bezos δήλωσε σε μια επιστολή προς τους μετόχους ότι «αυτή είναι η 1η Μέρα για το Διαδίκτυο», αναγνωρίζοντας τη μεγάλη ανεκμετάλλευτη δυνατότητα για το Διαδίκτυο και, κατ'επέκταση, την εταιρεία του. Όποια μέρα κι αν είναι αυτή για το Bitcoin, οι τεράστιες ποσότητες αναξιοποίητου δυναμικού είναι σαφείς σε όλους, εκτός από τον πιο απλό παρατηρητή.

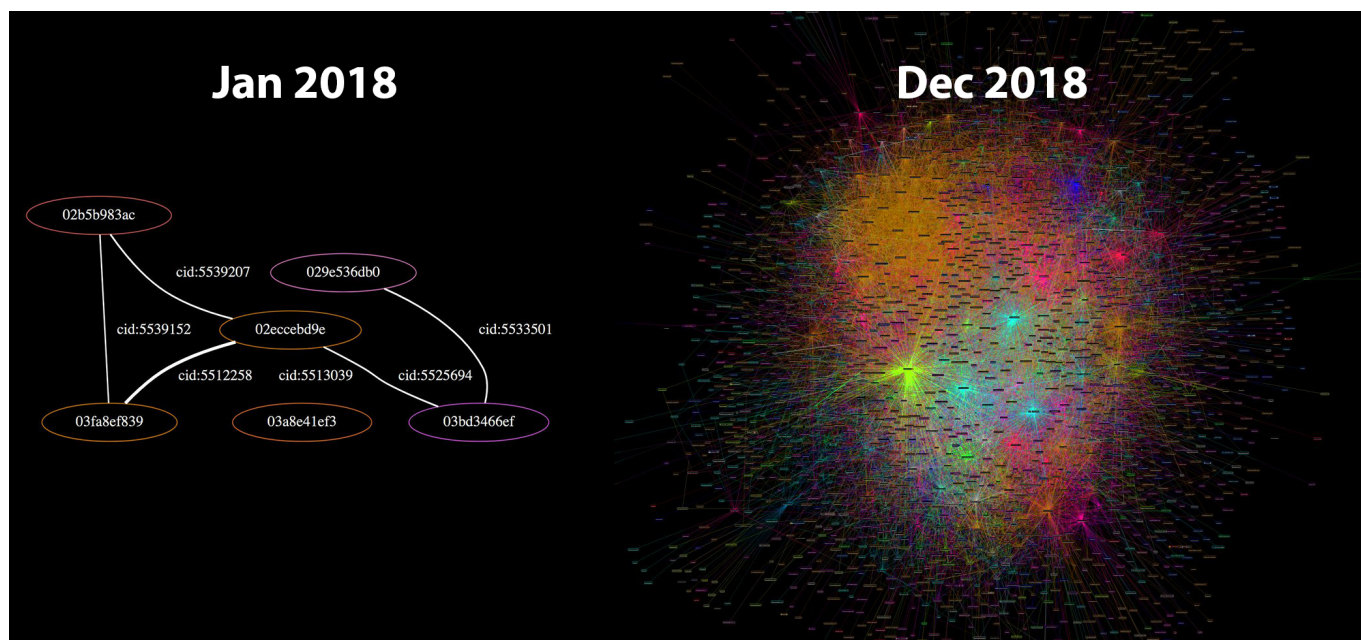


Το Διαδίκτυο, 1982 vs 2005. Source: cc-by Merit Network, Inc. and Barrett Lyon, Opte Project

Ο πρώτος κόμβος του Bitcoin συνδέθηκε το 2009 όταν ο Satoshi εξόρυξε το genesis block και εξέδωσε το λογισμικό στην “άγρια φύση”. Ο κόμβος του δεν έμεινε για πολύ μόνος. Ο Hal Finney ήταν ένας από τους πρώτους ανθρώπους που αντιλήφθηκαν την ιδέα και συμμετείχαν στο δίκτυο. Δέκα χρόνια μετά, κατά τη σύνταξη του παρόντος βιβλίου, πάνω από 75.000 κόμβοι τρέχουν το bitcoin.

Το επίπεδο βάσης του πρωτοκόλλου δεν είναι το μόνο πράγμα που αναπτύσσεται εκθετικά. Το lightning network, μια τεχνολογία δευτέρου επιπέδου, αυξάνεται με ακόμα πιο γρήγορο ρυθμό.

Τον Ιανουάριο του 2018, το lightning network είχε 40 κόμβους και 60 κανάλια (channels). Τον Απρίλιο του 2019, το δίκτυο αυξήθηκε σε περισσότερους από 4000 κόμβους και περίπου 40.000 κανάλια. Λάβετε υπόψη ότι πρόκειται ακόμη για πειραματική τεχνολογία όπου η απώλεια κεφαλαίων μπορεί και έχει συμβεί. Ωστόσο, η τάση είναι σαφής: χιλιάδες άνθρωποι είναι ρυποκίνδυνοι και πρόθυμοι να το χρησιμοποιήσουν.



Lightning Network, Ιανουάριος 2018 vs Δεκέμβριος 2018. Πηγή: Jameson Lopp

Προσωπικά, έχοντας ζήσει τη μετεωρική άνοδο του διαδικτύου, οι παραλληλισμοί μεταξύ του παγκόσμιου ιστού και του Bitcoin είναι προφανείς. Και τα δύο είναι δίκτυα, και τα δύο είναι εκθετικές τεχνολογίες, και τα δύο επιτρέπουν νέες δυνατότητες, νέες βιομηχανίες, νέους τρόπους ζωής. Ακριβώς όπως η ηλεκτρική ενέργεια ήταν η καλύτερη μεταφορά για να καταλάβουμε προς τα πού οδεύει το internet, το διαδίκτυο μπορεί να είναι η καλύτερη μεταφορά για να καταλάβουμε προς τα πού οδεύει το bitcoin. Ή, σύμφωνα με τα λεγόμενα του Ανδρέα Αντωνόπουλου, το Bitcoin είναι Το Διαδίκτυο του Χρήματος. Οι μεταφορές αυτές είναι μια καλή υπενθύμιση ότι, ενώ η ιστορία δεν επαναλαμβάνεται, συχνά δημιουργεί ομοιοκαταληξίες.

Οι εκθετικές τεχνολογίες είναι δύσκολο να κατανοηθούν και συχνά υποτιμώνται. Παρόλο που έχω μεγάλο ενδιαφέρον για τέτοιες τεχνολογίες, εκπλήσσομαι συνεχώς από το ρυθμό της προόδου και της καινοτομίας. Το να παρακολουθείς την ανάπτυξη του Bitcoin οικοσυστήματος είναι σαν να παρακολουθείς την άνοδο του Διαδικτύου σε γρήγορο κίνηση. Είναι συναρπαστικό.

Η αναζήτησή μου της προσπάθειας να κατανοήσω το Bitcoin με οδήγησε μέσα από μονοπάτια της ιστορίας με περισσότερους από έναν τρόπους. Η κατανόηση των αρχαίων κοινωνικών δομών, των χρημάτων του παρελθόντος και της εξέλιξης των δικτύων επικοινωνίας ήταν όλα μέρος του ταξιδιού. Από τον χειροπέλεκυ μέχρι το smartphone, η τεχνολογία έχει αναμφίβολα αλλάξει τον κόσμο μας πολλές φορές. Οι δικτυωμένες τεχνολογίες είναι ιδιαίτερα μετασχηματιστικές: η γραφή, οι δρόμοι, ο ηλεκτρισμός, το διαδίκτυο. Όλα τους άλλαξαν τον κόσμο. Το Bitcoin έχει αλλάξει τον δικό μου και θα συνεχίσει να αλλάζει τα μυαλά και τις καρδιές εκείνων που τολμούν να το χρησιμοποιήσουν.

Το Bitcoin μου έμαθε ότι η κατανόηση του παρελθόντος είναι απαραίτητη για την κατανόηση του μέλλοντός του. Ένα μέλλον που μόλις αρχίζει.

Down the Rabbit Hole

- [The Electricity Metaphor for the Web's Future](#) by Jeff Bezos
- [How the internet has woven itself into American life](#) by Susannah Fox and Lee Rainie
- [The 7 Network Effects of Bitcoin](#) by Trace Mayer
- [The Rising Speed of Technological Adoption](#) by Jeff Desjardins
- [Genesis Block](#) by Bitcoin Wiki Contributors
- [Lindy Effect](#) by Wikipedia Contributors
- 🎧 [Murad Mahmudov on The Ultimate Bitcoin Argument](#)
OTC#25 hosted by Pomp
- 🎧 [BitcoinTina on Why he is Bullish on Bitcoin](#)
TFTC#55 hosted by Marty Bent
- 🎧 [Pierre Rochard on Hyperbitcoinization and Bitcoin Maximalism](#)
HF#75 hosted by Demetri Kofinas

“Ξεκινήστε από την αρχή”, είπε ο βασιλιάς, πολύ σοβαρά, “και συνεχίστε μέχρι να φτάσετε στο τέλος: έπειτα σταματήστε”.

Όπως αναφέρθηκε στην αρχή, νομίζω ότι οποιαδήποτε απάντηση στο ερώτημα “Τι μάθατε από το Bitcoin;” θα είναι πάντοτε ατελής. Η συμβίωση αυτών που μπορούν να θεωρηθούν ως πολλαπλά ζωντανά συστήματα — το Bitcoin, η τεχνόσφαιρα και τα οικονομικά — είναι αρκετά αλληλένδετη, τα θέματα υπερβολικά πολλά και τα πράγματα κινούνται πάρα πολύ γρήγορα για να μπορέσουν να γίνουν πλήρως κατανοητά από ένα μόνο άτομο.

Ακόμη και χωρίς να έχει κατανοηθεί πλήρως, και μάλιστα με όλες τις ιδιοτροπίες και τις φαινομενικές αδυναμίες του, το Bitcoin αναμφισβήτητα λειτουργεί. Συνεχίζει να παράγει block περίπου κάθε δέκα λεπτά και το κάνει τόσο όμορφα. Όσο περισσότερο καιρό λειτουργεί το Bitcoin, τόσο περισσότεροι άνθρωποι θα επιλέξουν να το χρησιμοποιήσουν.

“Είναι αλήθεια ότι τα πράγματα είναι όμορφα όταν δουλεύουν. Τέχνη είναι η λειτουργία.” — [Giannina Braschi](#)

Το Bitcoin είναι παιδί του Διαδικτύου. Μεγαλώνει εκθετικά, θολώνοντας τις διαχωριστικές γραμμές μεταξύ των κλάδων. Δεν είναι ξεκάθαρο, για παράδειγμα, πού τελειώνει ο αμιγώς τεχνολογικός τομέας και πού ξεκινάει ένας άλλος τομέας. Παρόλο που το Bitcoin απαιτεί υπολογιστές για να λειτουργήσει αποτελεσματικά, η επιστήμη των υπολογιστών δεν αρκεί για να το κάνει κατανοητό. Το Bitcoin δεν είναι μόνο δίχως όρια όσον αφορά τις εσωτερικές του λειτουργίες αλλά και χωρίς όρια σχετικά με τους ακαδημαϊκούς κλάδους που συμπεριλαμβάνει.

Τα οικονομικά, η πολιτική, η θεωρία παιγνίων, η νομισματική ιστορία, η θεωρία δικτύων, τα χρηματοοικονομικά, η κρυπτογραφία, η θεωρία πληροφορίας, η λογοκρισία, η νομοθεσία και ο έλεγχος, η ανθρώπινη οργάνωση, η ψυχολογία — όλα αυτά και πολλά άλλα είναι τομείς εμπειρογνωμοσύνης που θα μπορούσαν να βοηθήσουν στην αναζήτηση της κατανόησης του τρόπου λειτουργίας του Bitcoin και του τι είναι το Bitcoin.

Καμία εφεύρεση από μόνη της δεν είναι υπεύθυνη για την επιτυχία της. Είναι ο συνδυασμός πολλαπλών, προηγουμένως άσχετων μεταξύ τους κομματιών, χρησιμοποιώντας ως κόλλα αναμεταξύ τους τα κίνητρα θεωρητικών παιγνίων, τα οποία

αποτελούν την επανάσταση που είναι το Bitcoin. Το όμορφο μείγμα πολλαπλών επιστημονικών κλάδων είναι αυτό που κάνει τον Satoshi μεγαλοφυή.

Όπως κάθε σύνθετο σύστημα, έτσι και το Bitcoin πρέπει να κάνει συμβιβασμούς όσον αφορά την αποδοτικότητα, το κόστος, την ασφάλεια και πολλές άλλες ιδιότητες. Ακριβώς όπως δεν υπάρχει καμία τέλεια λύση για την εξαγωγή ενός τετραγώνου από έναν κύκλο, οποιαδήποτε λύση στα προβλήματα που προσπαθεί να λύσει το Bitcoin θα είναι πάντοτε επίσης ατελής.

“Δεν πιστεύω ότι θα έχουμε ποτέ ξανά καλά χρήματα πριν τα βγάλουμε από τα χέρια της κυβέρνησης, δηλαδή, δεν μπορούμε να τα αφαιρέσουμε βίαια από τα χέρια της κυβέρνησης, το μόνο που μπορούμε να κάνουμε είναι με κάποιον πονηρό έμμεσο τρόπο να εισάγουμε κάτι που δεν μπορούν να σταματήσουν.” — Friedrich Hayek

Το Bitcoin είναι ο πονηρός, έμμεσος τρόπος να επανεισάγουμε τα καλά χρήματα στον κόσμο. Το καταφέρνει τοποθετώντας ένα κυρίαρχο άτομο πίσω από κάθε κόμβο, ακριβώς όπως ο Da Vinci προσπάθησε να λύσει το δυσεπίλυτο πρόβλημα του τετραγωνισμού ενός κύκλου, τοποθετώντας τον Άνθρωπο του Βιτρούβιου στο κέντρο του. Οι κόμβοι αφαιρούν αποτελεσματικά κάθε έννοια ενός κέντρου, δημιουργώντας ένα σύστημα που είναι εκπληκτικά αντι-εύθραστο και εξαιρετικά δύσκολο να απενεργοποιηθεί. Το Bitcoin ζει και ο καρδιακός παλμός του θα ξεπεράσει πιθανών αυτών όλων μας.

Ελπίζω να απολαύσατε αυτά τα εικοσιένα μαθήματα. Ίσως το πιο σημαντικό μάθημα είναι ότι το Bitcoin θα πρέπει να εξεταστεί ολιστικά, από πολλαπλές οπτικές γωνίες, εάν κάποιος επιθυμεί να έχει κάτι που να προσεγγίζει μια πλήρη εικόνα. Ακριβώς όπως η αφαίρεση ενός τμήματος από ένα πολύπλοκο σύστημα καταστρέφει το σύνολο, εξετάζοντας τμήματα του Bitcoin μεμονωμένα φαίνεται να αλλοιώνει την κατανόησή του. Αν έστω και ένα άτομο διαγράψει το “blockchain” από το λεξιλόγιό του και το αντικαταστήσει με “μια αλυσίδα από block” θα μπορέσω να πεθάνω ευτυχισμένος.

Σε κάθε περίπτωση, το ταξίδι μου συνεχίζεται. Σκοπεύω να εξερευνήσω περισσότερο τα βάθη αυτού του λαγουμιού και σας προσκαλώ όλους να με ακολουθήσετε σε αυτή τη περιπέτεια.