

Μηδενική Γνώση, Άπειρη Εμπιστοσύνη

Όλο το Βιβλίο, σε Απλά Ελληνικά

Το βιβλίο του Eli Ben-Sasson — συνεφευρέτη της απόδειξης STARK και συνιδρυτή της StarkWare — για το πώς το blockchain και οι κρυπτογραφικές αποδείξεις ξαναχτίζουν αθόρυβα την **εμπιστοσύνη** στο διαδίκτυο. Συνοψισμένο κεφάλαιο προς κεφάλαιο σε **δεκαπέντε σύντομους, κατανοητούς οδηγούς**. Χωρίς υπερβολές. Γραμμένο ώστε ο καθένας να καταλάβει το blockchain και να προστατέψει τα χρήματά του.

ΣΥΝΕΡΓΑΣΤΕΙΤΕ ΜΕ ΤΗΝ PANOPTICPROTOCOL

Συμβουλευτική για Ιδιώτες — προσωπική καθοδήγηση για κρύπτο, ένας προς έναν, χτισμένη γύρω από τους στόχους και το ρίσκο σας.

Συμβουλευτική για Επιχειρήσεις — στρατηγική, υιοθέτηση και σύμβουλοι για κρύπτο, για εταιρείες και ομάδες.

Περιεχόμενα

Το βιβλίο, κεφάλαιο προς κεφάλαιο. Κάθε ένα είναι ένας σύντομος, αυτοτελής οδηγός — διαβάστε τα στη σειρά ή πηγαίνετε σε όποιο θέλετε.

—	Εισαγωγή — Ο Ιστός της Ακεραιότητας	3
1	Γιατί Έχει Σημασία το Blockchain	4
2	Ο Νέος Κόσμος του Bitcoin	5
3	Μια Επισκόπηση του Blockchain	6
4	Οι Τομές του Bitcoin	7
5	Πέρα από το Νόμισμα: Το Blockchain ως Υποδομή	8
6	Μέσα Κοινωνικής Δικτύωσης, AI και Gig Economy	9
7	Εμπόδια στη Μαζική Υιοθέτηση	10
8	Η Μαγεία των Αποδείξεων	11
9	Υποδομή για τους Ατραπέζιτους	12
10	Ευχρηστία, Κλιμάκωση και Ιδιωτικότητα	13
11	Η Έρευνα Ζωντανεύει	14
12	StarkWare: Από την Ιδέα στα \$8 Δισ.	15
13	Χρειαζόμαστε Καν τα Κρύπτο;	16
14	Stablecoins και Meme Coins	17
15	Ο Ιστός της Ακεραιότητας	18
∞	Παράρτημα — Αποδείξεις STARK, Απαντήσεις	19
§	Γλωσσάρι — Το Α-Ω του Blockchain	20
★	Σχετικά με τους Συγγραφείς	20

Ο Ιστός της Ακεραιότητας

Για τι πραγματικά μιλάει αυτό το βιβλίο — και γιατί αφορά εσάς, όχι μόνο τους μηχανικούς.

Ζούμε στο διαδίκτυο, αλλά δεν βλέπουμε πώς λειτουργεί τίποτα. Εμπιστευόμαστε τις τράπεζες να μετρούν τα χρήματά μας, τις πλατφόρμες να μας δείχνουν την αλήθεια, τις εταιρείες να κρατούν ασφαλή τα αρχεία μας — και απλώς ελπίζουμε ότι τα κάνουν σωστά. Αυτό το βιβλίο μιλάει για έναν άλλο τρόπο: αντί να **εμπιστεύεσαι** ότι ένα σύστημα είναι έντιμο, μπορείς να το **ελέγξεις**, με μαθηματικά.

Ο Eli Ben-Sasson βοήθησε να εφευρεθεί το εργαλείο που το κάνει αυτό εφικτό — ένα είδος κρυπτογραφικής **απόδειξης** που επιτρέπει στον καθένα, ακόμη και από το κινητό, να επαληθεύσει ότι ένας τεράστιος υπολογισμός έγινε σωστά, χωρίς να τον ξανακάνει. Ονομάζει το αποτέλεσμα **Ιστός της Ακεραιότητας**: ένα διαδίκτυο όπου η εντιμότητα είναι ενσωματωμένη, όχι απλώς υποσχέμενη. Οι δεκαπέντε οδηγοί που ακολουθούν λένε αυτή την ιστορία σε απλά ελληνικά — από το «τι είναι το Bitcoin;» μέχρι το πώς οι αποδείξεις προστατεύουν αθόρυβα τα χρήματα και τα δικαιώματά σας.

Δεν χρειάζεστε τεχνικές γνώσεις για να τα παρακολουθήσετε. Κάθε οδηγός είναι σύντομος, στέκεται μόνος του και κλείνει με λίγα απλά συμπεράσματα που μπορείτε να αξιοποιήσετε. Διαβάστε τους στη σειρά για όλη την ιστορία, ή πηγαίνετε σε ό,τι σας ενδιαφέρει.

Η ΜΙΑ ΙΔΕΑ ΠΟΥ ΝΑ ΚΡΑΤΗΣΕΤΕ

Μην εμπιστεύεσαι — επαλήθευε. Όλο το βιβλίο στηρίζεται στο να αντικαταστήσεις την τυφλή εμπιστοσύνη με απόδειξη που ο καθένας μπορεί να ελέγξει.

Γιατί Έχει Σημασία το Blockchain

Σχεδόν ό,τι έχετε στο διαδίκτυο είναι στην πραγματικότητα μια εγγραφή στη βάση δεδομένων κάποιου άλλου.

Από πού ξεκινάμε: πριν από κάθε ορολογία, το πιο απλό ερώτημα — τι κατέχετε στ' αλήθεια σε έναν ψηφιακό κόσμο, και ποιος πραγματικά τα ελέγχει;

Το υπόλοιπο του λογαριασμού σας δεν είναι μετρητά σε ένα συρτάρι — είναι ένας αριθμός στον υπολογιστή της τράπεζας. Οι πόντοι σας, ο λογαριασμός σας, τα αρχεία σας: όλα είναι απλώς εγγραφές που κάποιος άλλος ελέγχει και μπορεί να αλλάξει, να παγώσει ή να χάσει. Συνήθως αυτό λειτουργεί μια χαρά. Όταν όμως δεν λειτουργεί — ένας παγωμένος λογαριασμός, μια χρεοκοπία τράπεζας, μια κυβέρνηση που κατάσχει αποταμιεύσεις — δεν έχετε αντίγραφο ούτε λόγο.

Ένα **blockchain** είναι ένα κοινό αρχείο που δεν το κατέχει καμία εταιρεία. Χιλιάδες υπολογιστές κρατούν το ίδιο αντίγραφο, ώστε κανείς να μην μπορεί να το ξαναγράψει κρυφά ή να το κλείσει. Αυτό ακριβώς είναι το νόημά του: όχι για να πλουτίσεις γρήγορα, αλλά για να κρατάς αρχεία που δεν εξαρτώνται από το να εμπιστεύεσαι έναν ισχυρό μεσάζοντα να είναι έντιμος και ικανός για πάντα.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Κατέχετε λιγότερα απ' όσα νομίζετε.** Τα περισσότερα «δικά σας» χρήματα και δεδομένα είναι εγγραφές που κάποιος άλλος μπορεί να αλλάξει.
- 2 Το blockchain αφαιρεί τον μοναδικό ιδιοκτήτη.** Το αρχείο είναι κοινό, οπότε κανείς δεν μπορεί μόνος του να το αλλοιώσει ή να το μπλοκάρει.
- 3 Είναι ασφάλεια, όχι λαχείο.** Η πραγματική αξία είναι ο έλεγχος που δεν μπορεί να σας αφαιρεθεί.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Το blockchain δεν αφορά τον γρήγορο πλουτισμό. Αφορά το να μη χρειάζεται να εμπιστεύεσαι κάποιον άλλο να είναι έντιμος με τα χρήματά σου.

Ο Νέος Κόσμος του Bitcoin

Η πρώτη φορά που τα χρήματα λειτούργησαν online χωρίς τράπεζα στη μέση.

Η ιστορία μέχρι τώρα: το Κεφάλαιο 1 έδειξε πόσα από τα χρήματά σας είναι στην ουσία μια εγγραφή που ελέγχει κάποιος άλλος. Το Bitcoin ήταν το πρώτο σύστημα φτιαγμένο για να επιστρέψει αυτόν τον έλεγχο στα χέρια σας.

Πριν το 2009, η αποστολή χρημάτων online χρειαζόταν πάντα έναν έμπιστο μεσάζοντα — μια τράπεζα ή το PayPal — για να μη μπορείς να ξοδέψεις το ίδιο ευρώ δύο φορές. Το Bitcoin, δημιούργημα του ανώνυμου **Satoshi Nakamoto**, το έλυσε χωρίς καμία εταιρεία. Αντί μία τράπεζα να κρατά το καθολικό, όλοι κρατούν ένα αντίγραφο και το δίκτυο συμφωνεί για αυτό μαζί.

Το Bitcoin έχει ανώτατο όριο **21 εκατομμύρια νομίσματα** — κανείς δεν μπορεί να τυπώσει κι άλλα — γι' αυτό το λένε «ψηφιακό χρυσό». Ξεκίνησε ως μια ιδέα που κυκλοφορούσε ανάμεσα σε κρυπτογράφους, και μια πίτσα που κάποτε αγοράστηκε για 10.000 νομίσματα· σήμερα αξίζει τρισεκατομμύρια. Το μάθημα δεν είναι η τιμή. Είναι ότι τα χρήματα μπορούν πλέον να κινούνται οπουδήποτε στον κόσμο χωρίς να ζητούν την άδεια κανενός.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Χωρίς μεσάζοντα.** Το Bitcoin επέτρεψε σε αγνώστους να στέλνουν αξία απευθείας, για πρώτη φορά στην ιστορία.
- 2 Σπάνιο εκ σχεδιασμού.** Μόνο 21 εκατομμύρια θα υπάρξουν ποτέ — κανείς δεν μπορεί να το υποτιμήσει τυπώνοντας κι άλλα.
- 3 Χωρίς άδεια.** Ο καθένας με ένα κινητό μπορεί να το κρατήσει και να το στείλει, χωρίς καμία έγκριση.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Η πραγματική εφεύρεση του Bitcoin δεν ήταν ένα νόμισμα. Ήταν χρήμα που δεν χρειάζεται την άδεια κανενός.

Μια Επισκόπηση του Blockchain

Πώς μια «αλυσίδα από μπλοκ» κρατά στην πράξη όλους έντιμους.

Η ιστορία μέχρι τώρα: γνωρίσατε το Bitcoin και γιατί έχει σημασία. Τώρα, δείτε πώς λειτουργεί η μηχανή από κάτω — το ίδιο το blockchain — με απλά λόγια.

Φανταστείτε ένα κοινό τετράδιο. Οι συναλλαγές μπαίνουν μαζί σε μια σελίδα (ένα **μπλοκ**) και κάθε νέα σελίδα σφραγίζεται πάνω στην προηγούμενη — αυτή είναι η **αλυσίδα**. Αν αλλάξεις μια παλιά σελίδα, χαλάει κάθε επόμενη σελίδα, οπότε η παραποίηση γίνεται ολοφάνερη σε όλους. Αυτό κάνει το αρχείο αξιόπιστο χωρίς αφεντικό.

Για να προστεθεί μια σελίδα, το δίκτυο πρέπει να **συμφωνήσει** ότι είναι έγκυρη. Το Bitcoin το κάνει με **εξόρυξη (mining)** (υπολογιστές που τρέχουν να λύσουν έναν γρίφο, το λεγόμενο proof-of-work)· νεότερες αλυσίδες χρησιμοποιούν **staking** (άνθρωποι κλειδώνουν νομίσματα ως εγγύηση που χάνουν αν εξαπατήσουν, το proof-of-stake). Και τα δύο κάνουν την εντιμότητα φθηνότερη από την απάτη. Δεν χρειάζεστε τους μηχανισμούς — μόνο το αποτέλεσμα: ένα αρχείο που κανείς δεν μπορεί να επεξεργαστεί κρυφά.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Τα μπλοκ συνδέονται μεταξύ τους.** Η παραποίηση παλιών εγγραφών σπάει την αλυσίδα και εντοπίζεται αμέσως.
- 2 Το δίκτυο πρέπει να συμφωνήσει.** Καμία εγγραφή δεν προστίθεται αν δεν την αποδεχτεί η πλειοψηφία.
- 3 Η απάτη κοστίζει πιο ακριβά από την εντιμότητα.** Αυτό είναι όλο το κόλπο — εκ σχεδιασμού, όχι με εμπιστοσύνη.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Η μαγεία δεν είναι η πολυπλοκότητα. Είναι ένα σύστημα όπου η απάτη απλώς κοστίζει πιο ακριβά από το τίμιο παιχνίδι.

Οι Τομές του Bitcoin

Το Bitcoin απέδειξε την ιδέα. Μετά, άλλοι ρώτησαν: τι άλλο μπορεί να κάνει αυτό;

Η ιστορία μέχρι τώρα: με τη μηχανή του blockchain εξηγημένη, το φυσικό επόμενο ερώτημα είναι τι μπορεί να κινήσει πέρα από απλές πληρωμές.

Η πραγματική τομή του Bitcoin ήταν κοινωνική, όχι μόνο τεχνική: έδειξε ότι άγνωστοι μπορούν να συμφωνήσουν σε μια κοινή αλήθεια χωρίς καμία αρχή στο τιμόνι. Αλλά το Bitcoin κάνει κυρίως ένα πράγμα — μετακινεί νομίσματα. Οι άνθρωποι σύντομα ήθελαν ένα blockchain που να μπορεί να τρέχει **προγράμματα**, όχι μόνο πληρωμές.

Αυτό έγινε το **Ethereum**: ένα blockchain πάνω στο οποίο μπορείς να χτίσεις εφαρμογές, χρησιμοποιώντας **έξυπνα συμβόλαια (smart contracts)** — κανόνες γραμμένους σε κώδικα που εκτελούνται μόνοι τους. Αυτό άνοιξε την πόρτα σε όλα όσα ακολούθησαν: δανεισμό, αγορές, ψηφιακή ιδιοκτησία, και τη δουλειά κλιμάκωσης που βρίσκεται στην καρδιά αυτού του βιβλίου. Το Bitcoin ήταν η απόδειξη της ιδέας· το Ethereum την έκανε πλατφόρμα.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Η μεγάλη νίκη ήταν η εμπιστοσύνη ανάμεσα σε αγνώστους.** Η συμφωνία χωρίς αρχή ήταν η πραγματική εφεύρεση.
- 2 Το Bitcoin είναι χρήμα· το Ethereum είναι πλατφόρμα.** Το ένα μετακινεί νομίσματα, το άλλο τρέχει προγράμματα.
- 3 Τα έξυπνα συμβόλαια άλλαξαν το παιχνίδι.** Κώδικας που επιβάλλει τους δικούς του κανόνες άνοιξε τα πάντα από κει και πέρα.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Το Bitcoin απέδειξε ότι η εμπιστοσύνη ανάμεσα σε αγνώστους ήταν εφικτή. Το Ethereum έκανε αυτή την απόδειξη πλατφόρμα.

Πέρα από το Νόμισμα: Το Blockchain ως Υποδομή

Τα χρήματα είναι μόνο η αρχή. Στην ουσία μιλάμε για αρχεία, συμβόλαια, και ποιος κρατά το «πραγματικό αντίγραφο» της ζωής σου.

Η ιστορία μέχρι τώρα: ο συν-συγγραφέας Nathan Jeffay αναλαμβάνει για να απαντήσει στο ερώτημα που κάνει κάθε ξένος — εντάξει, αλλά για τι πράγμα χρησιμεύει αυτό;

Ο Nathan κάνει μια απλή παρατήρηση: τα χρήματα είναι μόνο ένα είδος αρχείου. Τίτλοι ιδιοκτησίας, ταυτότητες, διαθήκες, ψήφοι — κι αυτά ορίζουν τη ζωή σου, κι είναι εύθραυστα. Ένας συγγενής του δεν μπόρεσε να πουλήσει ένα κληρονομημένο σπίτι επειδή η υπηρεσία έχασε τους τίτλους. Ολόκληρα αποικιακά αρχεία κάποτε κάηκαν επίτηδες. Η αποτυχία δεν είναι ποτέ ότι ένα αρχείο *δεν μπορεί* να υπάρξει — είναι ποιος το ελέγχει και αν θα επιβιώσει.

Ένα blockchain δεν βάζει τα ιδιωτικά σας χαρτιά σε δημόσια θέα. Αγκυρώνει την **απόδειξη** — μια χρονοσφραγίδα κι ένα δακτυλικό αποτύπωμα — ώστε να μπορείτε να δείξετε ότι ένα έγγραφο είναι γνήσιο και αναλλοίωτο, χρόνια αργότερα. Και ένα **έξυπνο συμβόλαιο** μπορεί να κάνει ένα αρχείο να *δράσει*: να μοιράσει έναν μισθό τη στιγμή που φτάνει, ή να χωρίσει τα έσοδα ενός podcast 50/50 αυτόματα, χωρίς δικηγόρους και χωρίς περιθώριο απάτης. Οι άνθρωποι στρέφονται σε αυτό, διαπιστώνει ο Nathan, όχι για να πλουτίσουν αλλά για να νιώσουν λιγότερο έρμια συστημάτων που δεν βλέπουν.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Τα χρήματα είναι μόνο ένα αρχείο.** Τίτλοι, ταυτότητες και συμβόλαια είναι κι αυτά αρχεία — και εξίσου χάνονται.
- 2 Αποδεικνύει, δεν εκθέτει.** Μπορείτε να δείξετε ότι ένα αρχείο είναι γνήσιο χωρίς να αποκαλύψετε τι περιέχει.
- 3 Το έξυπνο συμβόλαιο αφαιρεί την επιλογή της απάτης.** Εκτελείται ακριβώς όπως γράφτηκε, για όλους.

ΜΕ ΜΙΑ ΦΡΑΣΗ

«Απλώς αφαιρεί την επιλογή της απάτης.» — για το πώς λειτουργεί ένα έξυπνο συμβόλαιο

Μέσα Κοινωνικής Δικτύωσης, AI και Gig Economy

Τρία σημεία όπου ένας αόρατος αλγόριθμος διευθύνει αθόρυβα τη ζωή σας: το feed σας, το AI που σας κρίνει, και η εφαρμογή για την οποία δουλεύετε.

Η ιστορία μέχρι τώρα: το Κεφάλαιο 5 έδειξε το blockchain ως ουδέτερη υποδομή. Τώρα το ίδιο ερώτημα — ποιος πραγματικά αποφασίζει; — στραμμένο στο feed σας, τη δουλειά σας, και το AI που σας αξιολογεί.

Στα μέσα κοινωνικής δικτύωσης, δεν μιλάτε πραγματικά στους φίλους σας — μιλάτε σε έναν **αλγόριθμο** που αποφασίζει ποιος βλέπει τι. Δεν είναι ρυθμισμένος για την αλήθεια ή την καλοσύνη· είναι ρυθμισμένος για την **αλληλεπίδραση (engagement)**, γιατί η προσοχή σας πουλιέται σε διαφημιστές. Η ίδια αόρατη εξουσία φιλτράρει την αίτησή σας για δουλειά και ορίζει την αμοιβή σας στις εφαρμογές gig — κι όταν σας κρίνει λάθος, συνήθως δεν υπάρχει έφεση.

Η λύση του blockchain δεν είναι να ξαναχτίσει αυτές τις εφαρμογές — είναι να προσθέσει ένα **αρχείο**. Να καταγράφει γιατί αφαιρέθηκε μια ανάρτηση, να αποδεικνύει ότι οι κανόνες κατάταξης ήταν οι δημοσιευμένοι, να δίνει πραγματικές εφέσεις, και να επιτρέπει τον έλεγχο των αποφάσεων AI (με αποδείξεις μηδενικής γνώσης που ελέγχουν ότι τηρήθηκαν οι κανόνες χωρίς να εκτεθεί ο ιδιωτικός κώδικας). Η gig εργασία μπορεί να πάει παραπέρα: **συνεταιρισμοί** οδηγών όπου τα μέλη ψηφίζουν για τις προμήθειες και η φήμη σας σας ακολουθεί από εφαρμογή σε εφαρμογή. Ο στόχος είναι απλός — ορατές αποτυχίες και εξουσία που λογοδοτεί.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Μιλάτε στον αλγόριθμο, όχι στους φίλους σας.** Αυτός αποφασίζει ποιος σας ακούει, για να συνεχίζετε το scroll.
- 2 Λογοδοσία χωρίς έκθεση.** Οι αποδείξεις δείχνουν ότι τηρήθηκαν οι κανόνες, χωρίς να αποκαλύψουν τον κώδικα.
- 3 Οι εργαζόμενοι μπορούν να γίνουν ιδιοκτήτες.** Συνεταιρισμοί και μεταφερόμενη φήμη αντικαθιστούν το αόρατο αφεντικό.

ΜΕ ΜΙΑ ΦΡΑΣΗ

«Δεν μιλάμε πια στους φίλους μας. Μιλάμε στον σερβιτόρο — τον αλγόριθμο.»

Εμπόδια στη Μαζική Υιοθέτηση

Αν το blockchain είναι τόσο χρήσιμο, γιατί δεν είναι παντού; Τρία ειλικρινή εμπόδια.

Η ιστορία μέχρι τώρα: τα Κεφάλαια 5 και 6 έστρωσαν την υπόσχεση. Το Κεφάλαιο 7 είναι ο ρεαλισμός του Eli — οι πρακτικοί λόγοι που δεν έχει επικρατήσει ακόμη.

Πρώτον, η **ρύθμιση** είναι μπάλωμα: το ίδιο νόμισμα αντιμετωπίζεται ως μετοχή σε μία χώρα και ως εμπόρευμα σε μία άλλη, με βαριά γραφειοκρατία από πάνω. Δεύτερον, η **ευχρηστία** είναι δύσκολη — αντί για κωδικό, παίρνετε μια **φράση ανάκτησης (seed phrase)** 12-24 λέξεων, κι αν τη χάσετε τα χρήματά σας χάνονται για πάντα, χωρίς επαναφορά και χωρίς γραμμή υποστήριξης. Αν στείλετε σε λάθος διεύθυνση, χάνονται κι αυτά.

Τρίτο και βαθύτερο είναι το **τρίλημμα της κλιμάκωσης**: όλοι θέλουν ένα δίκτυο που να είναι αποκεντρωμένο, ασφαλές και γρήγορο — αλλά ο παλιός σχεδιασμός σας αφήνει να κρατήσετε μόνο δύο. Το blockchain είναι αργό **επίτηδες**, ανταλλάσσοντας την ταχύτητα με την ασφάλεια και το άνοιγμα. Το 2017 ένα και μόνο χαριτωμένο παιχνίδι, το CryptoKitties, μπλόκαρε ολόκληρο το Ethereum. Ο δρόμος μπροστά δεν είναι να θυσιάσεις ένα από τα τρία — είναι να αλλάξεις το ίδιο το τρίλημμα, κι αυτό λύνει το υπόλοιπο βιβλίο.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Η φράση ανάκτησης είναι το παν.** Αν τη χάσετε, δεν υπάρχει κουμπί επαναφοράς ούτε εξυπηρέτηση πελατών.
- 2 Το αργό είναι επιλογή.** Το blockchain ανταλλάσσει την ταχύτητα με την ασφάλεια — χαρακτηριστικό, όχι ελάττωμα.
- 3 Διάλεξε δύο από τρία — προς το παρόν.** Αποκέντρωση, ασφάλεια, ταχύτητα: τα επόμενα κεφάλαια σπάνε αυτό το όριο.

ΜΕ ΜΙΑ ΦΡΑΣΗ

«Είναι χαρακτηριστικό, όχι ελάττωμα.» — για το γιατί το blockchain είναι σκόπιμα αργό

Η Μαγεία των Αποδείξεων

Η καρδιά του βιβλίου: πώς μπορείς να ελέγξεις ότι ένας τεράστιος υπολογισμός είναι σωστός χωρίς να τον ξανακάνεις.

Η ιστορία μέχρι τώρα: το Κεφάλαιο 7 έκλεισε με το τρίλημμα — δεν μπορείς να τα έχεις όλα μαζί. Αυτή είναι η απάντηση του Eli, και η ιδέα πάνω στην οποία χτίστηκε ολόκληρη η εταιρεία του.

Κανονικά, για να είσαι σίγουρος ότι ένας υπολογισμός είναι σωστός, πρέπει να τον **ξανακάνεις** βήμα προς βήμα. Το πεδίο του Eli σπάει αυτόν τον κανόνα. Με μια **απόδειξη εγκυρότητας**, ένας τεράστιος υπολογισμός — ας πούμε ένας ολόκληρος χρόνος συναλλαγών — μπορεί να ελεγχθεί ελέγχοντας μόνο μερικούς αριθμούς. Είναι σαν εξέταση αίματος: μία σταγόνα αποκαλύπτει το σάκχαρό σου, γιατί είναι ουσιαστικά αδύνατο εκείνη η σταγόνα να «λέει ψέματα» για το σύνολο. Αν αλλοιώσεις έστω κι ένα ψηφίο, ο έλεγχος σχεδόν σίγουρα το πιάνει.

Δύο ρόλοι το κάνουν να δουλεύει. Ο **αποδεικνύων (prover)** κάνει όλη τη βαριά δουλειά και παράγει μια απόδειξη που δεν μπορεί να αλλάξει αργότερα· ο **επαληθευτής (verifier)** ελέγχει δειγματοληπτικά μόνο μερικά σημεία — γρήγορα, και αδύνατο να πλαστογραφηθεί. Το σύστημα του Eli, το **STARK**, δεν χρειάζεται «έμπιστη αρχικοποίηση (trusted setup)», δηλαδή κανένα μυστικό κύριο κλειδί που θα μπορούσε κάποιος να καταχραστεί. Η φράση του τα λέει όλα: δώστε του ένα αργό αλλά έμπιστο blockchain, και μία μόνο απόδειξη μπορεί να κρατά έντιμα ακόμη και κράτη — ελέγξιμη από τον καθένα με ένα κινητό.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 **Έλεγχος χωρίς επανάληψη.** Λίγοι δειγματοληπτικοί αριθμοί επαληθεύουν έναν τεράστιο υπολογισμό.
- 2 **Επαληθεύεις τα μαθηματικά, όχι τα δεδομένα σου.** Μπήκε στους λογαριασμούς κάθε λεπτό — χωρίς να αποκαλυφθεί τι αγόρασες.
- 3 **Ένα κινητό κρατά έντιμους τους γίγαντες.** Μια πλαστή απόδειξη απλώς δεν περνά τον έλεγχο.

ΜΕ ΜΙΑ ΦΡΑΣΗ

«Δώστε μου ένα αργό, αδύναμο, αλλά έμπιστο blockchain, και θα επιβάλουμε ακεραιότητα σε όλους τους υπολογισμούς στη Γη.» — Eli Ben-Sasson

Υποδομή για τους Ατραπέζιτους

Για 1,4 δισεκατομμύρια ανθρώπους χωρίς τράπεζα, ένα κινητό κι ένα πορτοφόλι μπορεί να είναι όλο το χρηματοπιστωτικό σύστημα.

Η ιστορία μέχρι τώρα: με τις αποδείξεις να κάνουν το blockchain αξιόπιστο και κλιμακώσιμο, αυτό το κεφάλαιο στρέφεται σε όσους το χρειάζονται περισσότερο.

Περίπου **1,4 δισεκατομμύρια ενήλικες** δεν έχουν τραπεζικό λογαριασμό — όχι από απροσεξία με τα χρήματα, αλλά επειδή τα υποκαταστήματα, η γραφειοκρατία και τα ελάχιστα υπόλοιπα τους αποκλείουν. Κι όμως πολλοί έχουν κινητό. Ένα πορτοφόλι κρύπτο δεν χρειάζεται άδεια, ούτε υποκατάστημα, ούτε πιστωτικό ιστορικό: μπορείτε να λαμβάνετε, να αποταμιεύετε και να στέλνετε χρήματα από παντού, και κανείς δεν μπορεί να σας αποκλείσει επειδή δεν έχετε τα σωστά έγγραφα.

Αυτό αλλάζει ζωές εκεί όπου το τοπικό νόμισμα είναι ασταθές. Άνθρωποι σε χώρες με υψηλό πληθωρισμό κρατούν **stablecoins** (κρύπτο συνδεδεμένα με το δολάριο) για να μην εξατμιστούν οι αποταμιεύσεις τους μέσα σε μια νύχτα, και εργαζόμενοι στο εξωτερικό στέλνουν χρήματα στην πατρίδα σε λεπτά αντί να χάνουν μέρες και βαριές προμήθειες. Δεν αφορά την κερδοσκοπία — αφορά το να δώσεις σε απλούς ανθρώπους έναν δρόμο εισόδου που το παλιό σύστημα ποτέ δεν πρόσφερε.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 **Το πορτοφόλι δεν ζητά άδεια.** Χωρίς υποκατάστημα, χωρίς χαρτιά, χωρίς ελάχιστο υπόλοιπο για να συμπεριληφθείτε.
- 2 **Τα stablecoins προστατεύουν τις αποταμιεύσεις.** Ένα νόμισμα δεμένο στο δολάριο νικά ένα νόμισμα που χάνει αξία κάθε βδομάδα.
- 3 **Η αποστολή χρημάτων στην πατρίδα φθηναίνει.** Λεπτά και σεντς αντί για μέρες και βαριές προμήθειες.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Για 1,4 δισ. ανθρώπους, ένα πορτοφόλι δεν είναι επένδυση — είναι η πρώτη τράπεζα που είπε ποτέ «ναι».

Ευχρηστία, Κλιμάκωση και Ιδιωτικότητα

Πώς οι αποδείξεις μετατρέπουν ένα αργό, δύσχρηστο *blockchain* σε κάτι που μπορούν να χρησιμοποιήσουν εκατομμύρια.

Η ιστορία μέχρι τώρα: οι αποδείξεις έλυσαν το πρόβλημα της εμπιστοσύνης. Αυτό το κεφάλαιο δείχνει πώς η ίδια ιδέα λύνει τα πρακτικά — κόστος, ταχύτητα και ιδιωτικότητα.

Οι αποδείξεις δεν επαληθεύουν απλώς — **κλιμακώνουν**. Αντί κάθε υπολογιστής να ξανατρέχει κάθε συναλλαγή, ένα **rollup** μαζεύει χιλιάδες συναλλαγές στην άκρη, κάνει τη δουλειά μία φορά, και στέλνει πίσω στην κύρια αλυσίδα μία μικρή απόδειξη. Η αλυσίδα ελέγχει την απόδειξη, όχι τις χιλιάδες συναλλαγές. Το αποτέλεσμα: πολύ μεγαλύτερη χωρητικότητα, πολύ χαμηλότερες προμήθειες, και η ίδια ασφάλεια όπως πριν.

Τα ίδια μαθηματικά προστατεύουν αθόρυβα την **ιδιωτικότητα**. Μια **απόδειξη μηδενικής γνώσης (zero-knowledge)** σας επιτρέπει να αποδείξετε ότι κάτι ισχύει — ότι είστε άνω των 18, ότι έχετε τα χρήματα, ότι περάσατε έναν έλεγχο — χωρίς να αποκαλύψετε τις υποκείμενες λεπτομέρειες. Και η ευχρηστία βελτιώνεται συνεχώς: πιο ομαλά πορτοφόλια, ονόματα κατανοητά από ανθρώπους, επιλογές ανάκτησης, ώστε να μη χρειάζεται πια να είσαι ειδικός για να μένεις ασφαλής.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Τα rollups σημαίνουν χαμηλότερες προμήθειες.** Κάνε τη δουλειά μία φορά, απόδειξέ την, και ωφελούνται όλοι.
- 2 Απόδειξέ το χωρίς να το αποκαλύψεις.** Δείξε ότι πληροίς τις προϋποθέσεις χωρίς να παραδώσεις τα ιδιωτικά σου δεδομένα.
- 3 Γίνεται πιο εύκολο.** Καλύτερα πορτοφόλια και ανάκτηση κλείνουν το χάσμα της ευχρηστίας.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Οι αποδείξεις δεν ελέγχουν απλώς τη δουλειά. Είναι αυτό που κάνει εφικτά τα φθηνά, ιδιωτικά, καθημερινά κρύπτο.

Η Έρευνα Ζωντανεύει

Πώς μια αφηρημένη μαθηματική ιδέα έγινε τεχνολογία που δουλεύει — και γιατί αυτό το άλμα είναι τόσο σπάνιο.

Η ιστορία μέχρι τώρα: είδαμε τι μπορούν να κάνουν οι αποδείξεις. Αυτό το κεφάλαιο είναι η ανθρώπινη ιστορία του πώς αυτή η θεωρία έγινε κάτι πραγματικό.

Για χρόνια, οι αποδείξεις του Eli ήταν όμορφη θεωρία που σχεδόν κανείς δεν θεωρούσε χρήσιμη. Το να γίνουν κάτι πραγματικό σήμαινε την επίλυση ενός βουνού πρακτικών προβλημάτων: να γίνουν οι αποδείξεις αρκετά μικρές, αρκετά γρήγορες και αρκετά φθηνές ώστε να τρέχουν στον πραγματικό κόσμο. Οι περισσότερες ακαδημαϊκές τομές δεν επιβιώνουν ποτέ από αυτό το ταξίδι.

Το σημείο καμπής ήταν να αντιμετωπιστεί η έρευνα ως **σχέδιο κατασκευής**, όχι ως δημοσίευση — και να μαζευτεί μια ομάδα πρόθυμη να το χτίσει. Αυτό το κεφάλαιο μιλάει για το χάσμα ανάμεσα σε μια λαμπρή ιδέα και ένα προϊόν που δουλεύει, και για την επίμονη μηχανική που χρειάζεται για να το διασχίσεις. Η απόδειξη που κρατά έντιμες τις συναλλαγές σας υπάρχει επειδή κάποιος αρνήθηκε να την αφήσει στον πίνακα.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Η θεωρία δεν αρκεί.** Το δύσκολο είναι να γίνει μια ιδέα αρκετά μικρή, γρήγορη και φθηνή για να χρησιμοποιηθεί.
- 2 Σχέδια κατασκευής, όχι δημοσιεύσεις.** Η πρόοδος ήρθε από το χτίσιμο, όχι μόνο από τη δημοσίευση.
- 3 Η αληθινή τεχνολογία έχει ανθρώπινη ιστορία.** Η απόδειξη που σας προστατεύει υπάρχει επειδή μια ομάδα την έβγαλε από τον πίνακα.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Μια λαμπρή ιδέα σε έναν πίνακα δεν βοηθά κανέναν. Η πραγματική δουλειά είναι να την κάνεις να τρέχει στον κόσμο.

StarkWare: Από την Ιδέα στα \$8 Δισ.

Τι χρειάζεται για να μετατρέψεις μια απόδειξη σε μια εταιρεία στην οποία στηρίζεται ολόκληρος ο κλάδος.

Η ιστορία μέχρι τώρα: η έρευνα έγινε σχέδιο κατασκευής. Αυτό το κεφάλαιο είναι η ιστορία του ιδρυτή που το έχτισε σε υποδομή στην οποία στηρίζεται πλέον ο κλάδος.

Ο Eli συνίδρυσε την **StarkWare** για να φέρει τις αποδείξεις STARK στον κόσμο. Αυτή είναι η ειλικρινής ιστορία ενός ιδρυτή: άντληση χρημάτων πάνω σε μια υπόσχεση, πρόσληψη ανθρώπων που πίστεψαν σε αυτή, και παράδοση τεχνολογίας που ασφαλίζει πλέον δισεκατομμύρια δολάρια σε συναλλαγές — η εταιρεία αποτιμήθηκε γύρω στα **\$8 δισεκατομμύρια**.

Το μάθημα για τον καθημερινό αναγνώστη δεν είναι η αποτίμηση. Είναι ότι η «μαγεία» πίσω από τα κρύπτο με χαμηλές προμήθειες και ασφάλεια χτίζεται από πραγματικές ομάδες που παίρνουν δύσκολες αποφάσεις, όχι από την υπερβολή. Όταν χρησιμοποιείτε ένα σύγχρονο δικτυο με μικροσκοπικές προμήθειες, στέκεστε πάνω σε χρόνια αυτής της άδοξης δουλειάς.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Οι αποδείξεις έγιναν προϊόν.** Η StarkWare μετέτρεψε την έρευνα του Eli σε υποδομή που χρησιμοποιεί ο κλάδος.
- 2 Πραγματική αξία, όχι μόνο υπερβολή.** Η τεχνολογία ασφαλίζει πλέον δισεκατομμύρια σε πραγματικές συναλλαγές.
- 3 Κοιτάξτε πέρα από την τιμή.** Αυτό που μετράει είναι η τεχνολογία που δουλεύει από κάτω.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Η «μαγεία» των χαμηλών προμηθειών και της άμεσης ασφάλειας είναι στην πραγματικότητα χρόνια άδοξης μηχανικής.

Χρειαζόμαστε Καν τα Κρύπτο;

Το πιο σκληρό κεφάλαιο του βιβλίου: παίρνει τους επικριτές στα σοβαρά αντί να τους απορρίπτει.

Η ιστορία μέχρι τώρα: αφού έχτισε την υπόθεση για την τεχνολογία, ο Eli στρέφεται στο πιο δύσκολο ερώτημα — αυτό που κάνουν οι επικριτές, όχι οι θαυμαστές.

Πολλοί έξυπνοι άνθρωποι λένε ότι τα κρύπτο είναι κυρίως απάτες, τζόγος και σπατάλη — και ο Eli δεν τους αποφεύγει. Μεγάλο μέρος του κλάδου *υπήρξε* υπερβολή, απάτη και κερδοσκοπία. Κάθε ειλικρινής υπεράσπιση της τεχνολογίας πρέπει να το παραδεχτεί αυτό πρώτα, αλλιώς δεν αξίζει εμπιστοσύνης.

Η απάντησή του είναι να ξεχωρίσει το **καζίνο** από την **υποδομή**. Οι απάτες είναι υπαρκτές, αλλά υπαρκτή είναι και η υποκείμενη τομή: ένας τρόπος να επαληθεύεις την αλήθεια χωρίς έμπιστη αρχή. Το ζητούμενο δεν είναι να υπερασπίζεσαι ό,τι έχει ένα νόμισμα κολλημένο πάνω του — είναι να κρατήσεις το κομμάτι που πραγματικά βοηθά τους ανθρώπους και να δεις καθαρά τα υπόλοιπα.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Οι επικριτές έχουν δίκιο σε κάτι.** Πολλά κρύπτο πράγματι είναι υπερβολή και απάτη — μείνετε καχύποπτοι.
- 2 Ξεχωρίστε το καζίνο από την υποδομή.** Η κερδοσκοπία δεν είναι το ίδιο με τη χρήσιμη τεχνολογία.
- 3 Κρίνετε κάθε έργο από τη χρήση του.** Ρωτήστε τι πραγματικό πρόβλημα λύνει, όχι τι υπόσχεται.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Ξεχωρίστε το καζίνο από την υποδομή — και κρίνετε κάθε έργο από το τι πραγματικά κάνει.

Stablecoins και Meme Coins

Τα δύο πιο πολυσυζητημένα νομίσματα — το ένα πραγματικά χρήσιμο, το άλλο κυρίως στοίχημα.

Η ιστορία μέχρι τώρα: αφού ξεχώρισε το χρήσιμο από την υπερβολή στη θεωρία, αυτό το κεφάλαιο το κάνει για τα δύο νομίσματα για τα οποία μαλώνουν όλοι.

Τα **stablecoins** είναι κρύπτο συνδεδεμένα με ένα σταθερό νόμισμα όπως το δολάριο, ώστε ένα νόμισμα να αξίζει πάντα περίπου ένα δολάριο. Είναι ίσως η πιο ξεκάθαρη πραγματική νίκη των κρύπτο: γρήγορες, φθηνές, διασυννοριακές πληρωμές και καταφύγιο για ανθρώπους των οποίων το τοπικό νόμισμα καταρρέει. Η παγίδα είναι η εμπιστοσύνη — πρέπει να ξέρεις ότι το νόμισμα στηρίζεται πραγματικά σε αληθινά αποθέματα.

Τα **meme coins** είναι το αντίθετο. Γεννημένα από αστεία και διαδικτυακή υπερβολή, δεν έχουν πίσω τους παρά την προσοχή. Λίγοι είναι τυχεροί· οι περισσότεροι αγοράζουν κοντά στην κορυφή και χάνουν. Το θέμα του Eli δεν είναι «μην τα αγγίζετε ποτέ» — είναι να ξέρεις ακριβώς ποιο κρατάς: ένα εργαλείο με χρήση, ή ένα λαχείο μεταμφιεσμένο σε επένδυση.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 **Τα stablecoins είναι η χρήσιμη περίπτωση.** Φθηνές πληρωμές και καταφύγιο στο δολάριο — αν τα αποθέματα είναι αληθινά.
- 2 **Ελέγξτε το αντίκρισμα.** Ένα stablecoin είναι τόσο ασφαλές όσο και αυτό που στέκεται από πίσω του.
- 3 **Τα meme coins είναι στοιχήματα.** Ίσως διασκεδαστικά — αλλά αντιμετωπίστε τα ως τζόγο, όχι αποταμίευση.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Να ξέρετε ποιο κρατάτε: ένα εργαλείο με πραγματική χρήση, ή ένα λαχείο μεταμφιεσμένο.

Ο Ιστός της Ακεραιότητας

Πού οδεύουν όλα: ένα διαδίκτυο όπου μπορείς να επαληθεύεις, όχι απλώς να ελπίζεις.

Η ιστορία μέχρι τώρα: όλα στο βιβλίο οδηγούσαν εδώ — στο διαδίκτυο που θέλει πραγματικά να χτίσει ο Eli, και στον δικό σας ρόλο σε αυτό.

Το όραμα του Eli συνδέει όλο το βιβλίο. Το σημερινό διαδίκτυο λειτουργεί με εμπιστοσύνη — ελπίζουμε ότι εταιρείες, τράπεζες και πλατφόρμες είναι έντιμες. Ο **Ιστός της Ακεραιότητας** είναι η εκδοχή όπου η εντιμότητα είναι αποδείξιμη: κάθε σημαντικός ισχυρισμός μπορεί να ελεγχθεί με μια απόδειξη, από τον καθένα, σε οποιαδήποτε συσκευή. Όχι «εμπιστέψου με», αλλά «να η απόδειξη».

Αυτό φτάνει πολύ πέρα από τα χρήματα. Επαληθευμένες αποφάσεις AI, αναλλοίωτα αρχεία, εκλογές που μπορείς να ελέγξεις, ειδήσεις που μπορείς να ιχνηλατήσεις ως την πηγή τους. Η τεχνολογία ήδη δουλεύει· αυτό που μένει είναι η υιοθέτηση — απλοί άνθρωποι να την καταλάβουν και να την απαιτήσουν. Γι' αυτό ακριβώς υπάρχει αυτός ο οδηγός.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΕΣΑΣ

- 1 Από το «εμπιστέψου με» στο «να η απόδειξη».** Η εντιμότητα γίνεται κάτι που μπορείς να ελέγξεις.
- 2 Μεγαλύτερο από τα χρήματα.** AI, αρχεία, ψήφοι και ειδήσεις μπορούν όλα να γίνουν επαληθεύσιμα.
- 3 Η υιοθέτηση είναι το τελευταίο βήμα.** Η τεχνολογία δουλεύει — αυτό που λείπει είναι να την καταλάβουμε.

ΤΟ ΒΑΣΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Το μέλλον του διαδικτύου δεν είναι «εμπιστέψου με». Είναι «να η απόδειξη».

Αποδείξεις STARK, Απαντήσεις

Γρήγορες, απλές απαντήσεις στις ερωτήσεις που κάνει ο κόσμος για τις αποδείξεις.

Τα ιδιωτικά μου δεδομένα βρίσκονται στο blockchain;

Όχι. Μια απόδειξη ελέγχει ότι τα μαθηματικά «βγαίνουν» — όχι τι αγοράσατε ή τι κατέχετε προσωπικά. Οι λεπτομέρειές σας παραμένουν ιδιωτικές.

Πώς μπορεί ο έλεγχος λίγων αριθμών να αποδείξει το σύνολο;

Με τον ίδιο τρόπο που μία σταγόνα αίματος αποκαλύπτει το σάκχαρό σας. Αν κάτι παραποιήθηκε, η δειγματοληψία σχεδόν σίγουρα το πιάνει.

Τι είναι η «έμπιστη αρχικοποίηση» και γιατί το STARK την αποφεύγει;

Ορισμένα συστήματα αποδείξεων χρειάζονται ένα μυστικό κλειδί στην αρχή — κίνδυνος αν διαρρεύσει ποτέ. Τα STARK δεν χρησιμοποιούν κανένα, οπότε δεν υπάρχει κύριο κλειδί προς κατάχρηση.

Μπορεί πραγματικά ένα κινητό να το επαληθεύσει;

Ναι. Αυτό ακριβώς είναι το νόημα: η βαριά δουλειά γίνεται μία φορά από τον αποδεικνύοντα, και ο καθένας μπορεί να ελέγξει τη μικρή απόδειξη φθηνά.

Σημαίνει μια απόδειξη ότι ένα έργο είναι ασφαλές για επένδυση;

Όχι. Μια απόδειξη δείχνει ότι ένας υπολογισμός έγινε σωστά — όχι ότι ένα νόμισμα είναι καλή επένδυση. Κρατήστε τα δύο ξεχωριστά.

Είναι το ίδιο με τη «μηδενική γνώση» του τίτλου του βιβλίου;

Ναι. Μια απόδειξη μηδενικής γνώσης σας αφήνει να αποδείξετε ότι κάτι ισχύει χωρίς να αποκαλύψετε τις ιδιωτικές λεπτομέρειες πίσω του — η βασική ιδέα όλου του βιβλίου.

Το Α-Ω του Blockchain

Κάθε βασικός όρος αυτού του οδηγού, σε ένα σημείο — απλά και σύντομα.

Address (διεύθυνση) — ο δημόσιος αριθμός του λογαριασμού σας, σαν email για χρήματα. Ένας λάθος χαρακτήρας και τα χρήματα χάνονται.

Bitcoin — το πρώτο κρυπτονόμισμα· ψηφιακό χρήμα χωρίς εταιρεία στο τιμόνι, με όριο 21 εκατ. νομίσματα.

Block (μπλοκ) — μια δέσμη συναλλαγών που προστίθεται στην αλυσίδα, σφραγισμένη πάνω στο προηγούμενο μπλοκ.

Blockchain — ένα κοινό αρχείο σε χιλιάδες υπολογιστές, που κανείς δεν μπορεί να αλλάξει κρυφά.

Custodial υπηρεσία — εταιρεία που κρατά τα κρύπτο σας για εσάς, σαν τράπεζα — πιο εύκολο, αλλά την εμπιστεύεστε.

Αποκέντρωση — κανένας μοναδικός ιδιοκτήτης ή αφεντικό· ο έλεγχος μοιράζεται σε πολλούς.

Ethereum — ένα blockchain πάνω στο οποίο χτίζεις εφαρμογές, όχι μόνο στέλνεις νομίσματα.

Gas fee (προμήθεια) — η (συχνά απρόβλεπτη) χρέωση για να επεξεργαστεί το δίκτυο τη συναλλαγή σας.

KYC — «Know Your Customer»: έλεγχοι ταυτότητας που κάνει μια υπηρεσία πριν σας αφήσει να συναλλαχθείτε ή να κάνετε ανάληψη.

Meme coin — νόμισμα γεννημένο από αστείο ή υπερβολή, με ελάχιστο αντίκρισμα· αντιμετωπίστε το ως τζόγο.

Mining (εξόρυξη) — υπολογιστές που ανταγωνίζονται για να προσθέσουν το επόμενο μπλοκ (proof-of-work), όπως στο Bitcoin.

NFT — ένα μοναδικό ψηφιακό token που δηλώνει ιδιοκτησία ενός συγκεκριμένου αντικειμένου ή δικαιώματος.

Permissionless (χωρίς άδεια) — ανοιχτό στον καθένα· δεν χρειάζεται έγκριση για να συμμετέχεις.

Απόδειξη (validity proof) — μαθηματικά που δείχνουν ότι ένας υπολογισμός έγινε σωστά, ελέγξιμο χωρίς επανάληψη.

Prover / Verifier — ο αποδεικνύων κάνει όλη τη δουλειά και φτιάχνει την απόδειξη· ο επαληθευτής την ελέγχει γρήγορα δειγματοληπτικά.

Rollup — τρόπος να επεξεργάζεσαι χιλιάδες συναλλαγές στην άκρη και μετά να στέλνεις πίσω μία μικρή απόδειξη — μειώνοντας τις προμήθειες.

Seed phrase (φράση ανάκτησης) — οι 12-24 λέξεις που είναι το κύριο κλειδί του πορτοφολιού σας. Αν τις χάσετε, η πρόσβαση χάνεται οριστικά.

Smart contract (έξυπνο συμβόλαιο) — κώδικας που επιβάλλει τους δικούς του κανόνες αυτόματα, χωρίς περιθώριο απάτης.

Stablecoin — κρύπτο συνδεδεμένο με ένα σταθερό νόμισμα (συνήθως το δολάριο) για να κρατά την αξία του.

Staking — κλείδωμα νομισμάτων ως εγγύηση που χάνετε αν εξαπατήσετε (proof-of-stake).

STARK — το σύστημα αποδείξεων του Eli· δεν χρειάζεται μυστική «έμπιστη αρχικοποίηση».

Trusted setup (έμπιστη αρχικοποίηση) — μυστικό κλειδί που χρειάζονται ορισμένα συστήματα στην αρχή· κίνδυνος διαρροής. Τα STARK το αποφεύγουν.

Wallet (πορτοφόλι) — η εφαρμογή που κρατά τα κλειδιά σας και σας αφήνει να στέλνετε, λαμβάνετε και αποθηκεύετε κρύπτο.

Απόδειξη μηδενικής γνώσης (zero-knowledge) — απόδειξη ότι κάτι ισχύει (π.χ. ότι είστε άνω των 18) χωρίς να αποκαλύψετε τις λεπτομέρειες πίσω του.

ΣΧΕΤΙΚΑ ★

Σχετικά με τους Συγγραφείς & τον Οδηγό

Eli Ben-Sasson

Κρυπτογράφος και συνεφευρέτης της απόδειξης **STARK**, και συνιδρυτής και CEO της **StarkWare**. Πέρασε χρόνια στα μαθηματικά των αποδείξεων πριν βρουν τη χρήση τους στο blockchain — και τώρα δουλεύει για να κάνει την επαληθεύσιμη εμπιστοσύνη πρακτική για όλους.

Nathan Jeffay

Δημοσιογράφος και συν-συγγραφέας του Eli, με δουλειά να μετατρέπει πολύπλοκες ιδέες σε απλά λόγια. Τα κεφάλαιά του γειώνουν την τεχνολογία στην καθημερινή ζωή — feeds, δουλειές, χαμένους τίτλους σπιτιών — ώστε ο καθένας να δει γιατί έχει σημασία.

Σχετικά με τον Οδηγό

Μια δωρεάν σύνοψη κοινότητας του *Zero Knowledge, Infinite Trust*, από την **PanopticProtocol**, για να καταλάβουν απλοί άνθρωποι το blockchain και να προστατέψουν τα χρήματά τους. Συνοδευτικό του βιβλίου, όχι υποκατάστατο — αν σας αγγίζει, διαβάστε το πρωτότυπο. Στόχος μας: υιοθέτηση μέσα από εκπαίδευση.