ΠΜΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τεχνολογία Blockchain και Συναλλαγές σε Περιβάλλοντα ιστού και Κινητών Συσκευών

Μπούτσκας Εμμανουήλ
AM: mai20044

Επιβλέπων Καθηγητής
Γεωργιάδης Χρήστος

Τεχνολογία Blockchain

Το **Blockchain** είναι ένα αρχείο καταγραφής **συναλλαγών** που αναπαράγεται σε ένα σύνολο συμμετεχόντων κόμβων.

Κάθε συναλλαγή αποθηκεύεται στο **κοινόχρηστο δημόσιο καθολικό** (Public ledger)

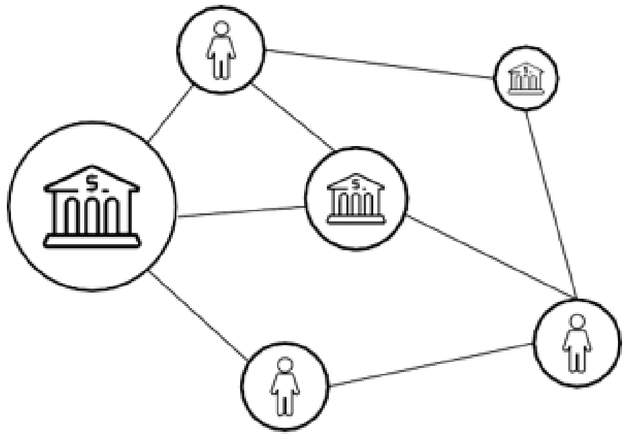
Όλοι οι κόμβοι του δικτύου κατέχουν ξεχωριστά και από κοινού ταυτόχρονα ένα **πανομοιότυπο αντίγραφο** από ένα κοινό αρχείο. Το αρχείο αυτό δεν είναι στατικό σε περιεχόμενο, αλλά **εμπλουτίζεται συνεχώς** με καινούργιο περιεχόμενο.

Οι συναλλαγές τοποθετούνται σε μπλοκ, τα οποία συνδέονται με μια προσέγγιση προς τα πίσω (**one way hashes**)

Αυτοί οι κόμβοι λειτουργούν από κοινού το σύστημα Blockchain, **χωρίς το κεντρικό έλεγχο** οποιουδήποτε μεμονωμένου τρίτου μέρους.

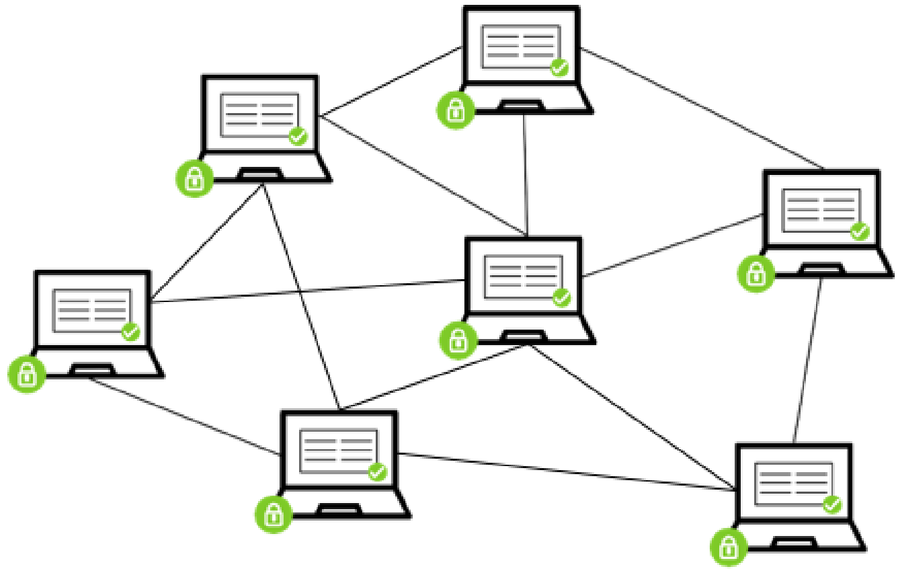
Οι κόμβοι του συστήματος ελέγχουν την **ακεραιότητα** των συναλλαγών και αναλαμβάνουν την **καταγραφή** τους σε νέα μπλοκ στο καθολικό

Τρέχον Χρηματοοικονομικό Σύστημα



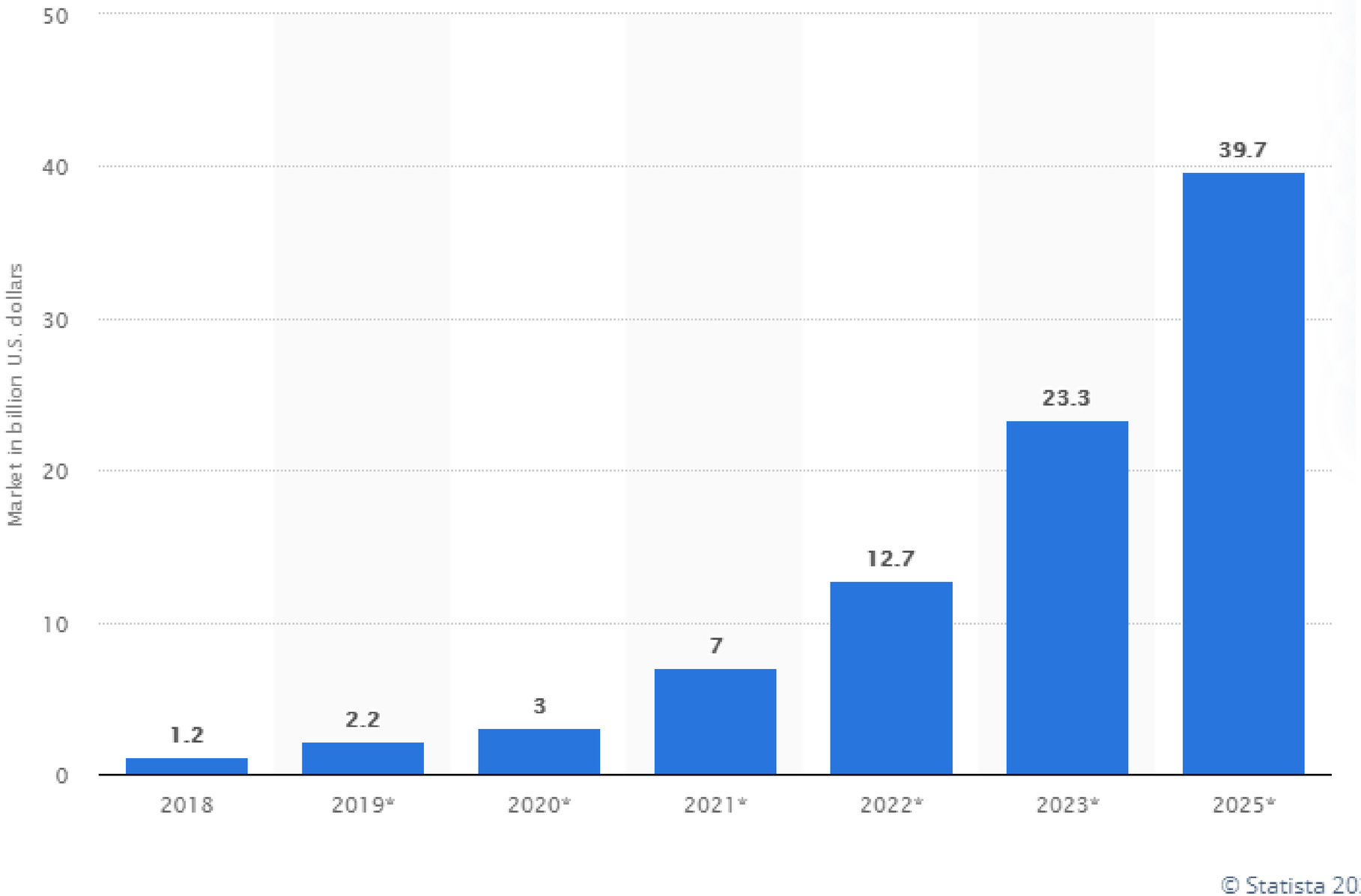
- Οι κεντρικές αρχές (τράπεζα, συμβολαιογράφοι κ.λπ.) αναλαμβάνουν τη μεταφορά αξίας μεταξύ μερών
- Απαιτούνται πολλαπλοί διαμεσολαβητές και τήρηση αρχείων για τη διευκόλυνση της μεταφοράς περιουσιακών στοιχείων και τη δημιουργία εμπιστοσύνης

Σύστημα Blockchain



- Κατανεμημένο δίκτυο υπολογιστών (κόμβοι) που διατηρούν μια κοινή πηγή πληροφοριών
- Τα δεδομένα συναλλαγών είναι αμετάβλητα
- Συναλλαγές Peer-to-Peer χρησιμοποιώντας ψηφιακά νομίσματα για την αναπαράσταση αξίας

Μέγεθος αγοράς τεχνολογίας blockchain παγκοσμίως από το 2018 έως το 2025



Βασικά Χαρακτηριστικά

Αποκέντρωση

- Όλοι οι κόμβοι αποθηκεύουν ένα αντίγραφό του καθολικού κάτι που εξασφαλίζει την *ασφάλεια* και την *διαφάνεια* των συναλλαγών.

Ανωνυμία

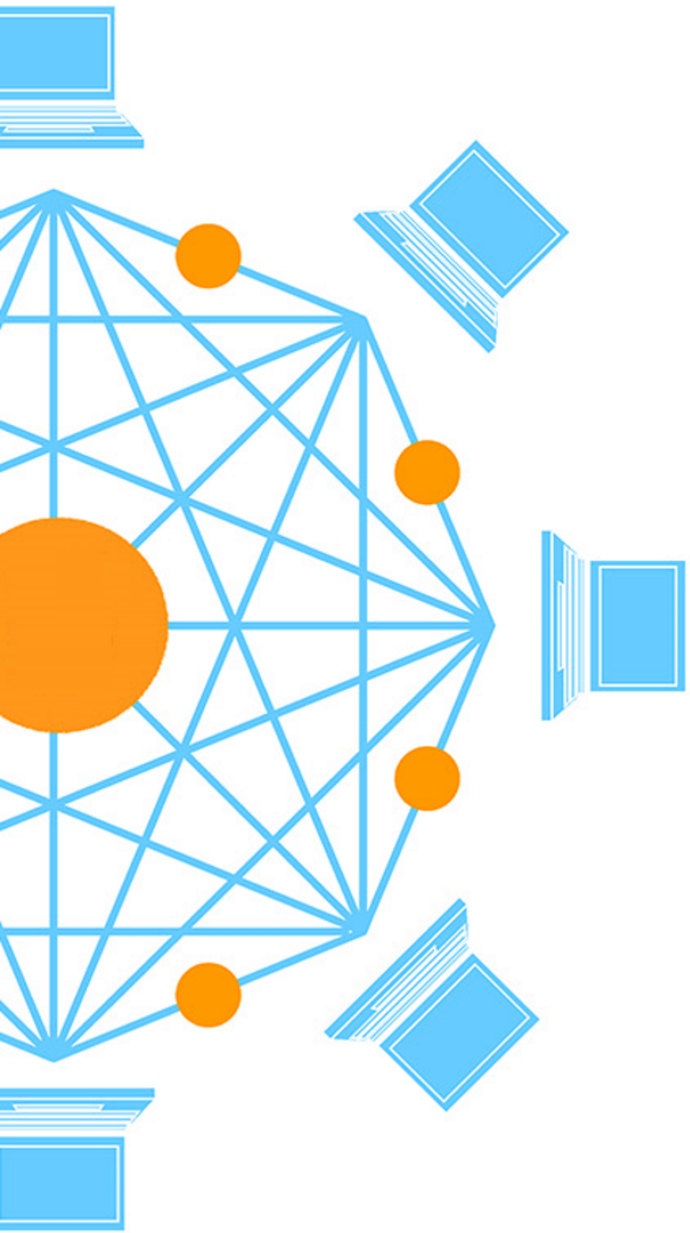
- Κάθε χρήστης μπορεί να αλληλοεπιδράσει με το Blockchain μέσω μιας δημιουργημένης *διεύθυνσης*, η οποία δεν αποκαλύπτει την πραγματική ταυτότητα του.

Δυνατότητα Ελέγχου

- Δεδομένου ότι κάθε μία από τις συναλλαγές στο Blockchain επικυρώνεται και *έχει καταγραφεί με χρονική σήμανση*, οι χρήστες μπορούν εύκολα να επαληθεύσουν και να εντοπίσουν τις προηγούμενες εγγραφές μέσω της πρόσβασης σε οποιονδήποτε κόμβο στο κατανεμημένο δίκτυο.

Ανθεκτικότητα

- Είναι σχεδόν αδύνατο να *διαγραφούν* ή να *αλλοιωθούν* οι συναλλαγές *μόλις προστεθούν* στο Blockchain. Μπορούν να εντοπιστούν αμέσως τα μπλοκ που περιέχουν μη έγκυρες συναλλαγές.

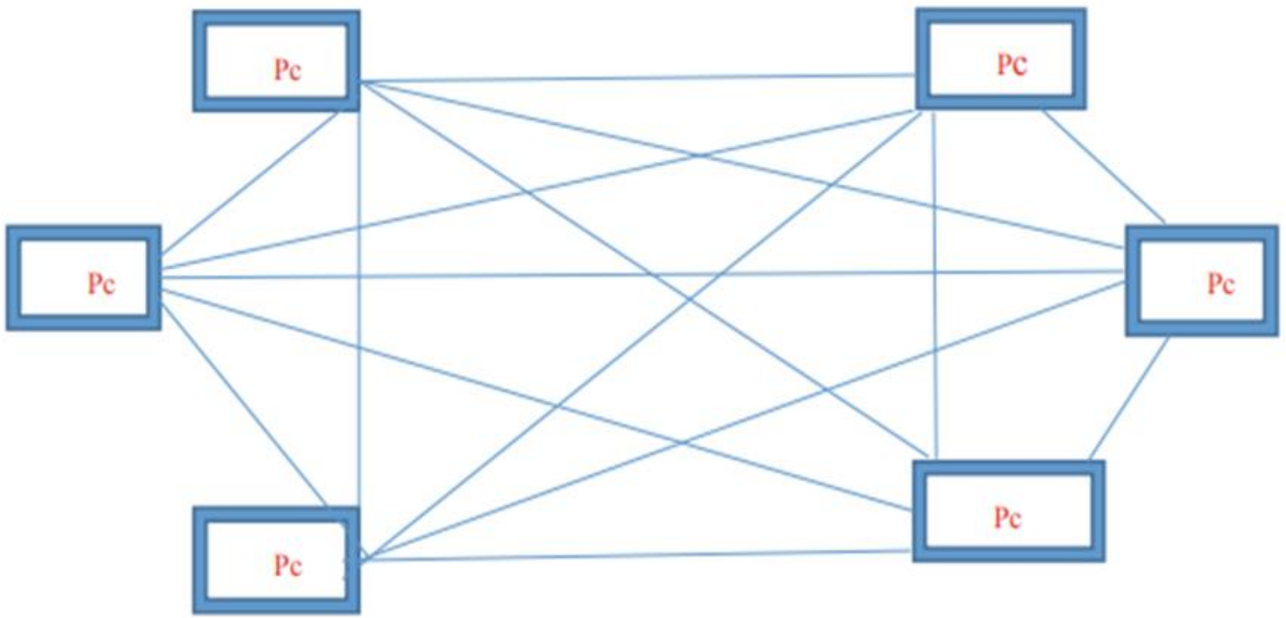


ΤΟΠΟΛΟΓΙΕΣ BLOCKCHAIN

Μια βασική παράμετρος που λαμβάνεται υπόψη στο σχεδιασμό μιας πλατφόρμας Blockchain είναι η κατηγοριοποίηση των κόμβων που αποτελούν μέρος της.

Η κύρια κατηγοριοποίηση των συστημάτων Blockchain διακρίνεται σε δημόσια (public), ιδιωτική (private), με κοινοπραξία (consortium).

Public Blockchain



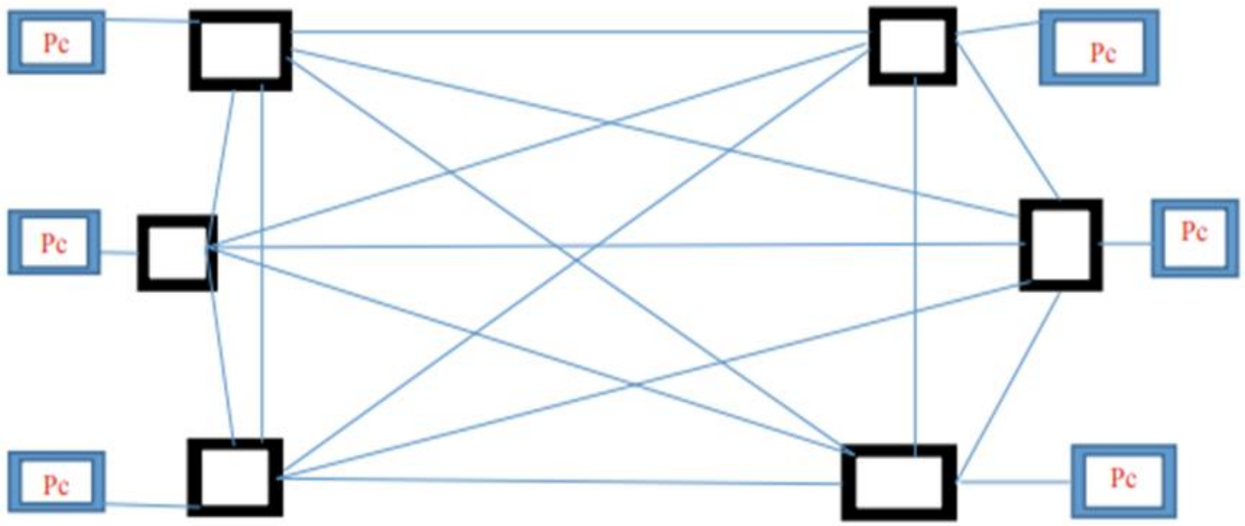
Εικόνα: Public Blockchain

- Τα δημόσια Blockchain λειτουργούν **χωρίς** κεντρικές αρχές και μεσάζοντες.

- Το μεγαλύτερο πλεονέκτημα αυτού του είδους Blockchain είναι ότι **δεν μπορεί κανένας να ελέγξει το δίκτυο πλήρως**. Ως εκ τούτου, διασφαλίζει ότι τα δεδομένα είναι **ασφαλή** και βοηθά στο **αμετάβλητο** των εγγραφών.

- Από την άλλη πλευρά, ένα από τα μειονεκτήματα τους είναι ότι υποφέρουν από **έλλειψη ταχύτητας** στις συναλλαγές. Μπορεί να χρειαστούν μερικά λεπτά έως ώρες πριν ολοκληρωθεί μια συναλλαγή. Για παράδειγμα, το Bitcoin μπορεί να διαχειρίζεται μόνο επτά συναλλαγές ανά δευτερόλεπτο σε σύγκριση με 24.000 συναλλαγές ανά δευτερόλεπτο που πραγματοποιούνται από τη VISA

Private Blockchain

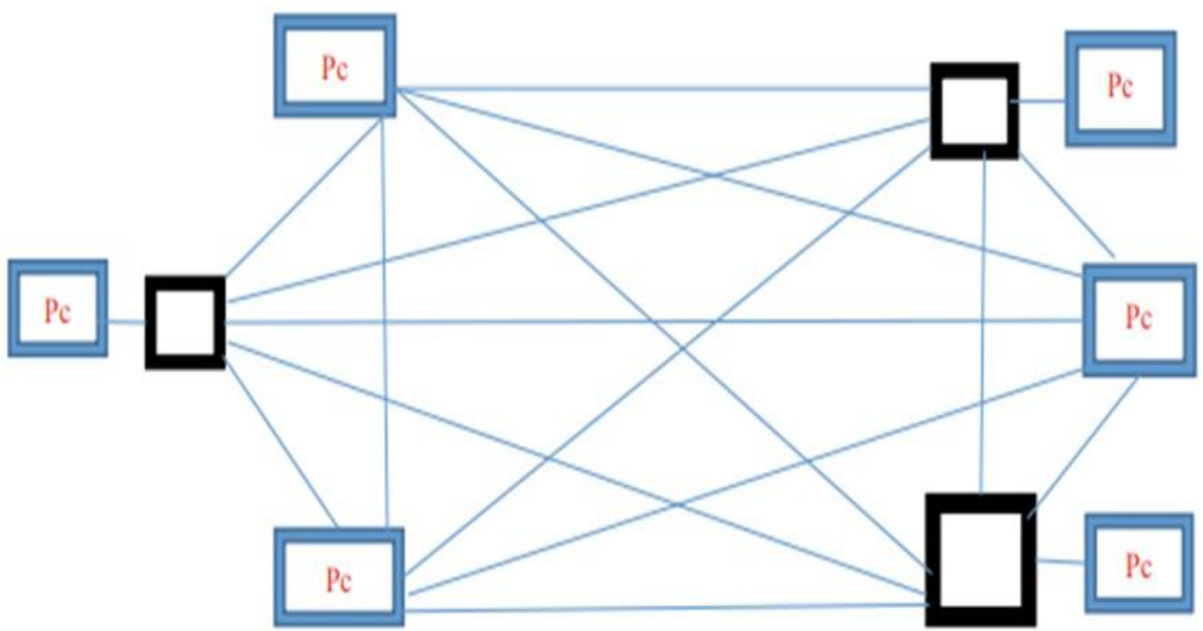


Εικόνα: Private Blockchain

- Τα ιδιωτικά Blockchain έχουν έναν **διαχειριστή δικτύου** που μπορεί να ορίζει τα δικαιώματα χρήστη και παραμέτρους του δικτύου, όπως προσβασιμότητα, εξουσιοδότηση και ούτω καθεξής.

- Η κύρια διαφορά τους με τα δημόσια Blockchain εμφανίζεται στον τρόπο πρόσβασης και στην ταχύτητα. Τα ιδιωτικά Blockchain είναι **γρηγορότερα**. Αυτό συμβαίνει επειδή υπάρχουν λιγότεροι συμμετέχοντες σε σύγκριση με τα δημόσια Blockchain.

Consortium Blockchain

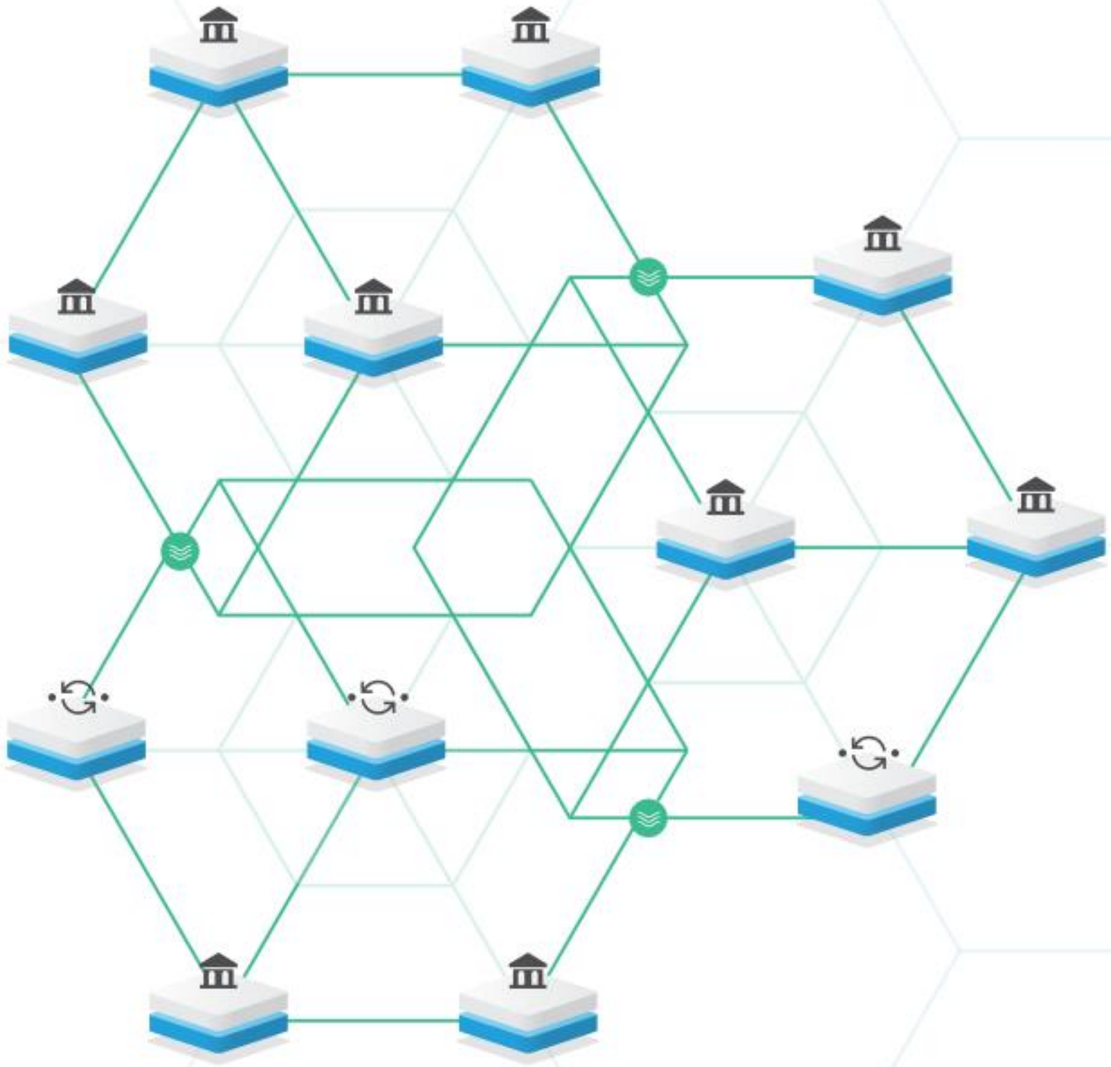


Εικόνα: Consortium Blockchain

- Είναι εν μέρει δημόσιο και εν μέρει ιδιωτικό και ως εκ τούτου ένας **συνδυασμός** τόσο **δημόσιου** όσο και **ιδιωτικού** Blockchain. Ο διαχωρισμός μεταξύ δημόσιου και ιδιωτικού χαρακτήρα συμβαίνει βάσει της συναίνεσης.

- Σε με Blockchain κοινοπραξία, μόνο λίγοι κόμβοι ή χρήστες έχουν το δικαίωμα να εξουσιοδοτούν συναλλαγές και να επιβλέπουν τη διαδικασία συναίνεσης.

- Τέτοιου είδους Blockchain συνδέονται με επιχειρηματική χρήση, όπου μια ομάδα οργανισμών συνεργάζεται για να αξιοποιήσει την τεχνολογία Blockchain για τη βελτίωση των δραστηριοτήτων της.



Ενεργειακή Κατανάλωση Blockchain

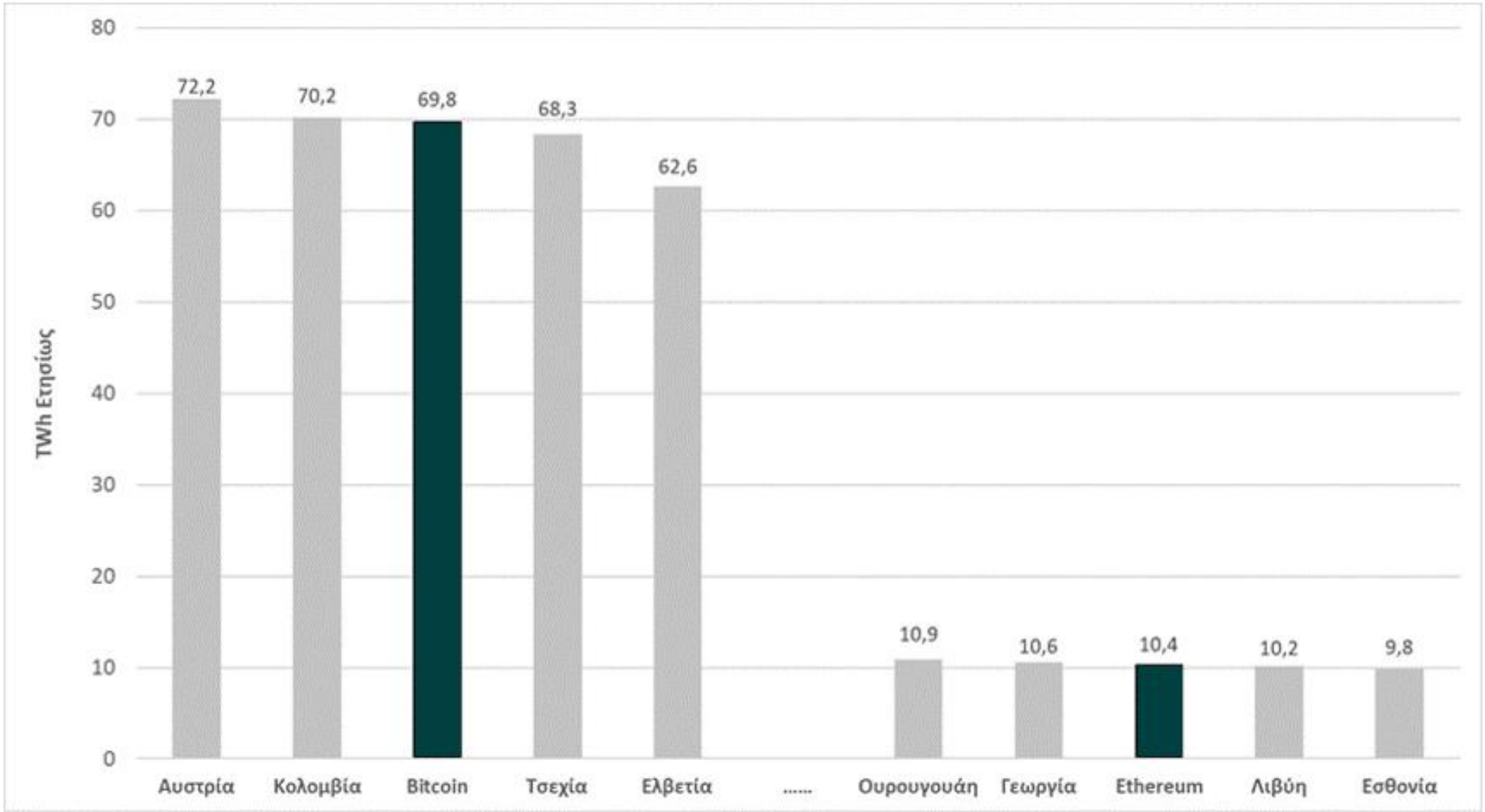
- Μια από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει η τεχνολογία του Blockchain είναι η υψηλή κατανάλωση ενέργειας.

- Ο κύριος λόγος για την υψηλή κατανάλωση ενέργειας των Blockchains οφείλεται σε μεγάλο βαθμό στην χρήση του Proof of Work και στη διαδικασία εκτέλεσης του.

- Έρευνες έχουν δείξει ότι τα Blockchains χρησιμοποιούν ετησίως ενέργεια που είναι περίπου ίση με την κατανάλωση ενέργειας ενός έθνους ετησίως.

- Ολόκληρο το δίκτυο του Bitcoin καταναλώνει λίγο περισσότερη ενέργεια από τη Τσεχία και ελαφρώς μικρότερη από την Κολομβία και την Αυστρία.

- Ταυτόχρονα, ολόκληρο το δίκτυο του Ethereum καταναλώνει περίπου 6,7 φορές λιγότερη ενέργεια από το δίκτυο του Bitcoin.



Εικόνα: Σύγκριση της κατανάλωσης ενέργειας μεταξύ των δικτύων Bitcoin και Ethereum και επιλεγμένων χωρών σε TWh / έτος, από το 2020-09-28

Αποκεντρωμένες Εφαρμογές

Οι αποκεντρωμένες εφαρμογές (DApps) είναι ψηφιακές εφαρμογές ή προγράμματα που υπάρχουν και εκτελούνται σε δίκτυο υπολογιστών Blockchain ή peer-to-peer (P2P). Αυτές οι εφαρμογές διαδόθηκαν από κατανεμημένες τεχνολογίες καθολικών (Distributed Ledger Technology) όπως το Ethereum Blockchain και δεν εμπίπτουν στο πεδίο αρμοδιοτήτων και ελέγχου μιας μεμονωμένης αρχής.

Τύποι Αποκεντρωμένων Εφαρμογών

1

Χρηματοοικονομικές Εφαρμογές (Financial Applications)

(Bitcoin, Ethereum, Litecoin etc.)

2

Ημι-Χρηματοοικονομικές Εφαρμογές (Semi-Financial Applications)

(Πρωτόκολλο Omni)

3

Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (Decentralized Autonomous Organizations)

(Δίκτυο S.A.F.E - Secure Access For Everyone Network)

Κρυπτονομίσματα και Κοινωνικά Δίκτυα: Facebook Libra

Σύμφωνα με το White Paper του Libra (2019), το Libra θεωρείται ως μια χρηματοοικονομική υποδομή που θα αποτελείται από τρία μέρη:

- Πρώτον, το Libra θα είναι ένα ψηφιακό νόμισμα που βασίζεται στη τεχνολογία Blockchain.

- Δεύτερον, θα υποστηρίζεται από ένα αποθεματικό κεφάλαιο που έχει σχεδιαστεί για να διατηρεί την αξία του σταθερή, καθιστώντας το ως ένα stable coin στην αγορά των ψηφιακών νομισμάτων.

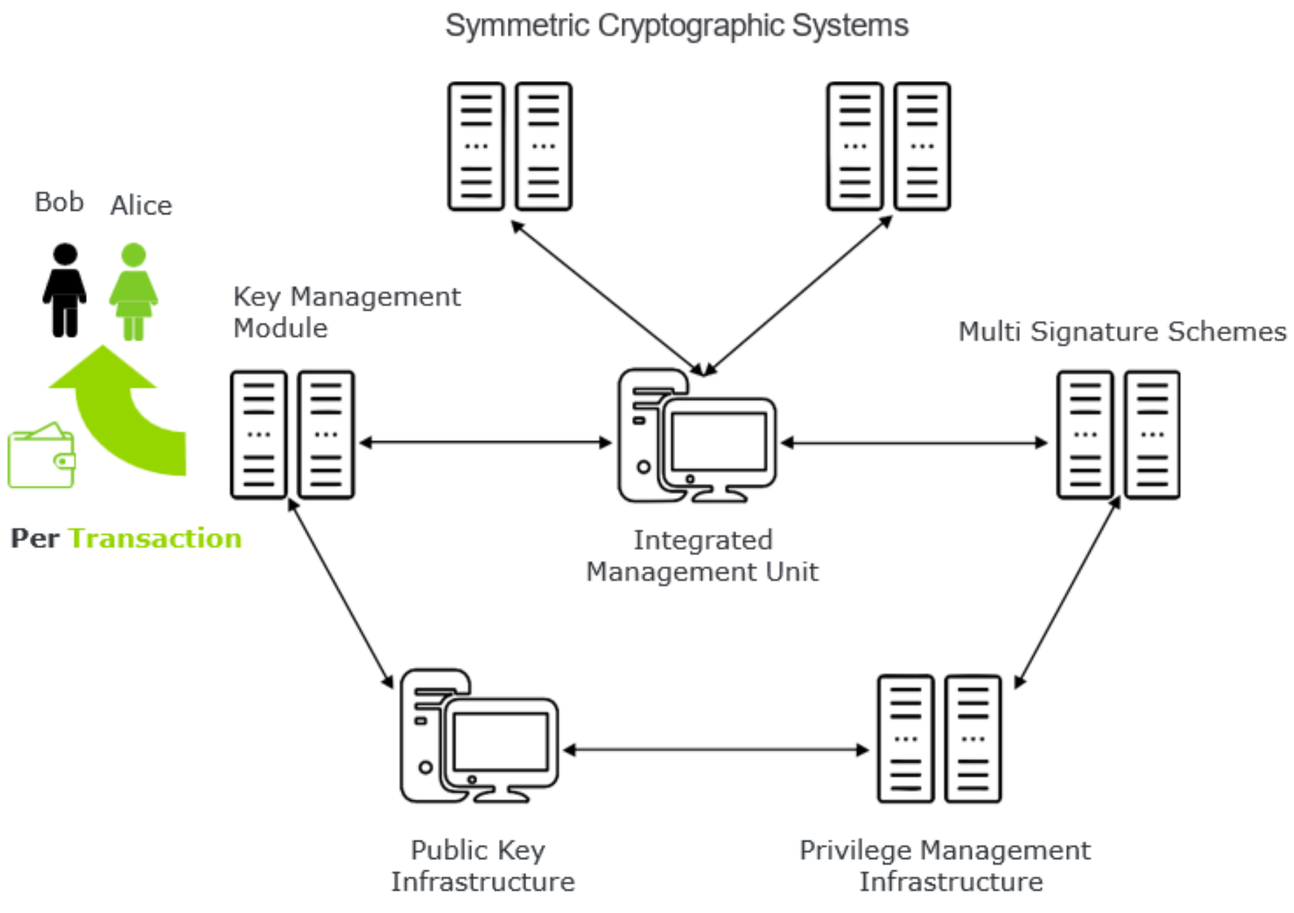
- Τρίτον, θα διαχειρίζεται από έναν ανεξάρτητο οργανισμό (Libra Association) στον οποίο έχει ανατεθεί η ανάπτυξη του οικοσυστήματος του νομίσματος.

Τα ιδρυτικά μέλη του οργανισμού αυτή τη στιγμή απαρτίζουν 24 εταιρίες και ο στόχος τους είναι να φτάσουν τα 100 μέλη μέσα στα επόμενα χρόνια.

libra

Εικόνα: Μέλη-Εταιρίες του Libra Association

ΣΥΝΑΛΛΑΓΕΣ



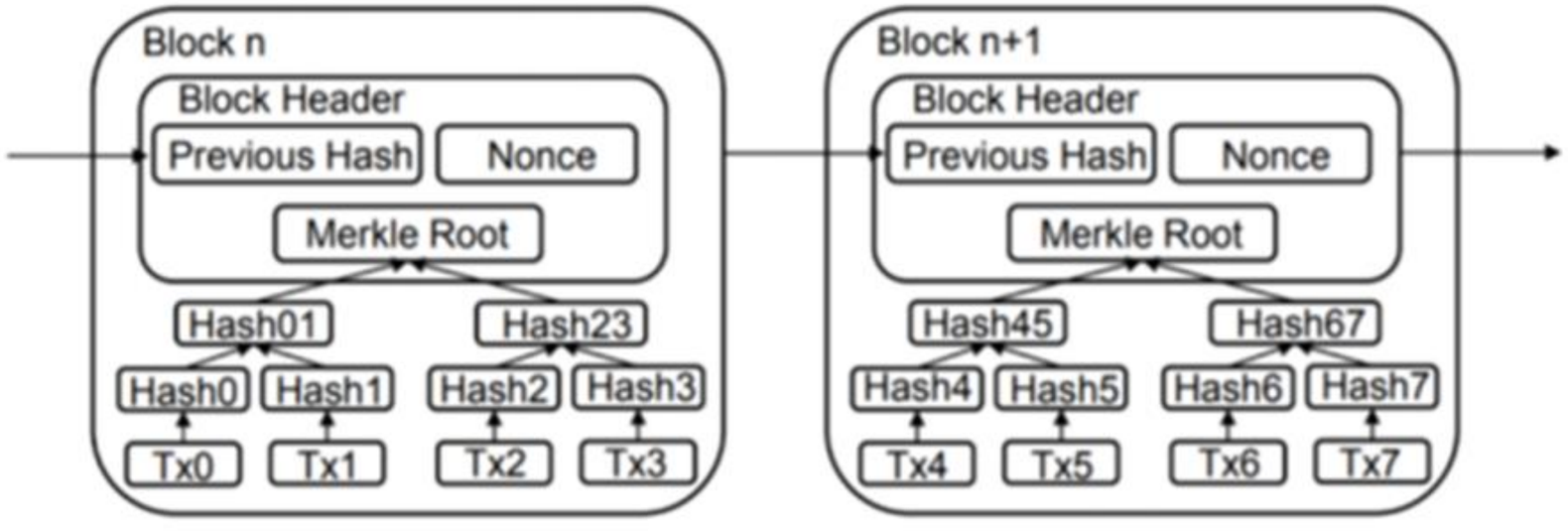
Μια συναλλαγή είναι μια δομή δεδομένων που κωδικοποιεί μια μεταφορά νομισμάτων από μια πηγή κεφαλαίων, που ονομάζεται είσοδος, σε έναν προορισμό που ονομάζεται έξοδος.

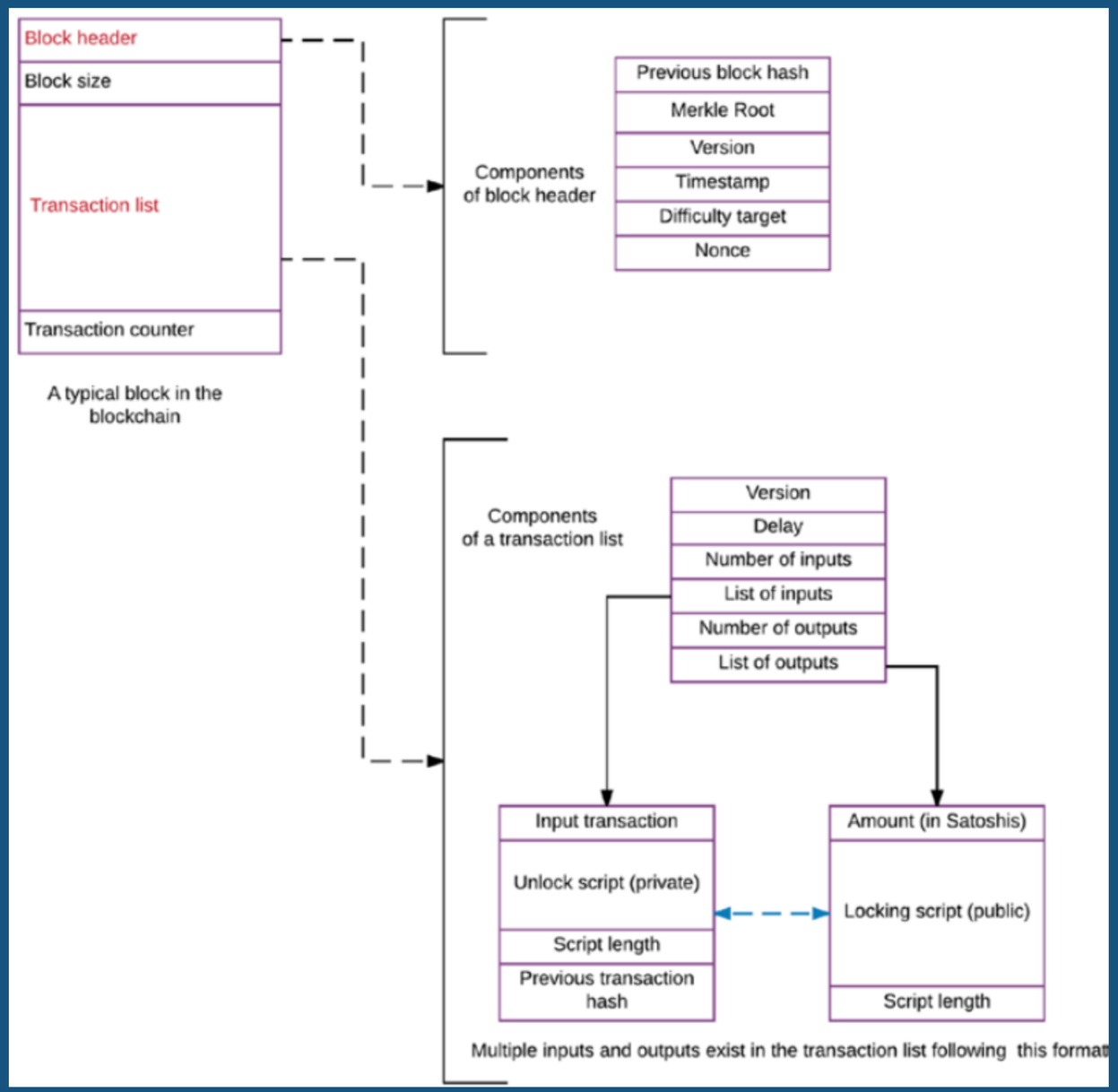
Πραγματοποιούνται σε πραγματικό χρόνο σε αποκεντρωμένο δίκτυο για να διασφαλιστεί η ασφάλεια και η αξιοπιστία ολόκληρου του συστήματος.

Μια συναλλαγή είναι ουσιαστικά μια δομή δεδομένων που μεταφέρεται και υπάρχει μέσα σε ένα μπλοκ

Ο Ρόλος των Block

Τα μπλοκ αποτελούν το μέρος όπου αποθηκεύονται όλες οι συναλλαγές. Είναι αρχεία όπου καταγράφονται μόνιμα δεδομένα που σχετίζονται με το δίκτυο. Κάθε μπλοκ μπορεί να θεωρηθεί ως σελίδα στο καθολικό. Το δίκτυο Blockchain αποτελείται από εκατομμύρια μπλοκ που βρίσκονται σε συνεχή κατάσταση ροής. Επομένως ένα μπλοκ είναι μια μόνιμη αποθήκευση αρχείων που, μόλις γράφονται, δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν.





Κάθε μπλοκ έχει τουλάχιστον δύο μοναδικά στοιχεία.

1. Το πρώτο είναι η κεφαλίδα του μπλοκ (block header), η οποία περιέχει ένα μοναδικό κατακερματισμό που ονομάζεται ρίζα merkle και προσδιορίζει μοναδικά το μπλοκ.

2. Το δεύτερο είναι η λίστα συναλλαγών (transaction list) η οποία περιέχει νέες συναλλαγές.

Σε αυτό το απλοποιημένο μοντέλο, υπάρχουν δύο επιπλέον στοιχεία ενός μπλοκ: το μέγεθος του μπλοκ (block size), το οποίο διατηρείται συνεπή για ολόκληρο το δίκτυο και τέλος ένας μετρητής (transaction counter) που χρησιμοποιείται για να μετράει τον αριθμό των συναλλαγών σε κάθε μπλοκ.

Block

1 block deep

659,083

00000000000000000097727ff80963b3f94ae799fb19e51a880440679ad9af4

version	0x20800000
previousblock	00000000000000000e996233114d60d4248e9740af4d096dcf3d9bd360e662
merkleroot	68e463df247d837a54bec75572cd09dc1bef71e422f0d429b4461b58829ef64a
time	28 Nov 2020, 14:55:32
bits	170ffedd
nonce	229,420,194 ↗

Serialized | Table

2354 transactions

1287.75 KB

3,993,485 WU

+6.25	2e4aa58b9a8a15f8e8c843fd22b0f20f1fe9f682364d58257a24e53a1a7b5251	
2.	1e9fc467238076d64637648dbdb369a18433ef4db015ed1944ffc874adfb0430	
3.	b547778e9a027ffbac57592e049257d9203f5342a4dcc55b02bc71becc0803ad	SEGWIT
...	...	
2351.	cbcc6099daed41ab6500565e26937ef7d3d4d5fb04f6c0fde42ed710c0d58658	
2352.	daf40111807d792008a74a1568cbba69f56c4611cab4d56a9dcf30ddf9d064c1	
2353.	7857ecec88f83d09fd94b46a74b1b2e45b41e9660a9090db74b2f9c529d1cbf2	SEGWIT
2354.	f51f54d9120b0bb5ec07b665513035342bb3a0e8dd77e16637f22fba803ddfba	SEGWIT

↗ Unknown

Tx Sizes:

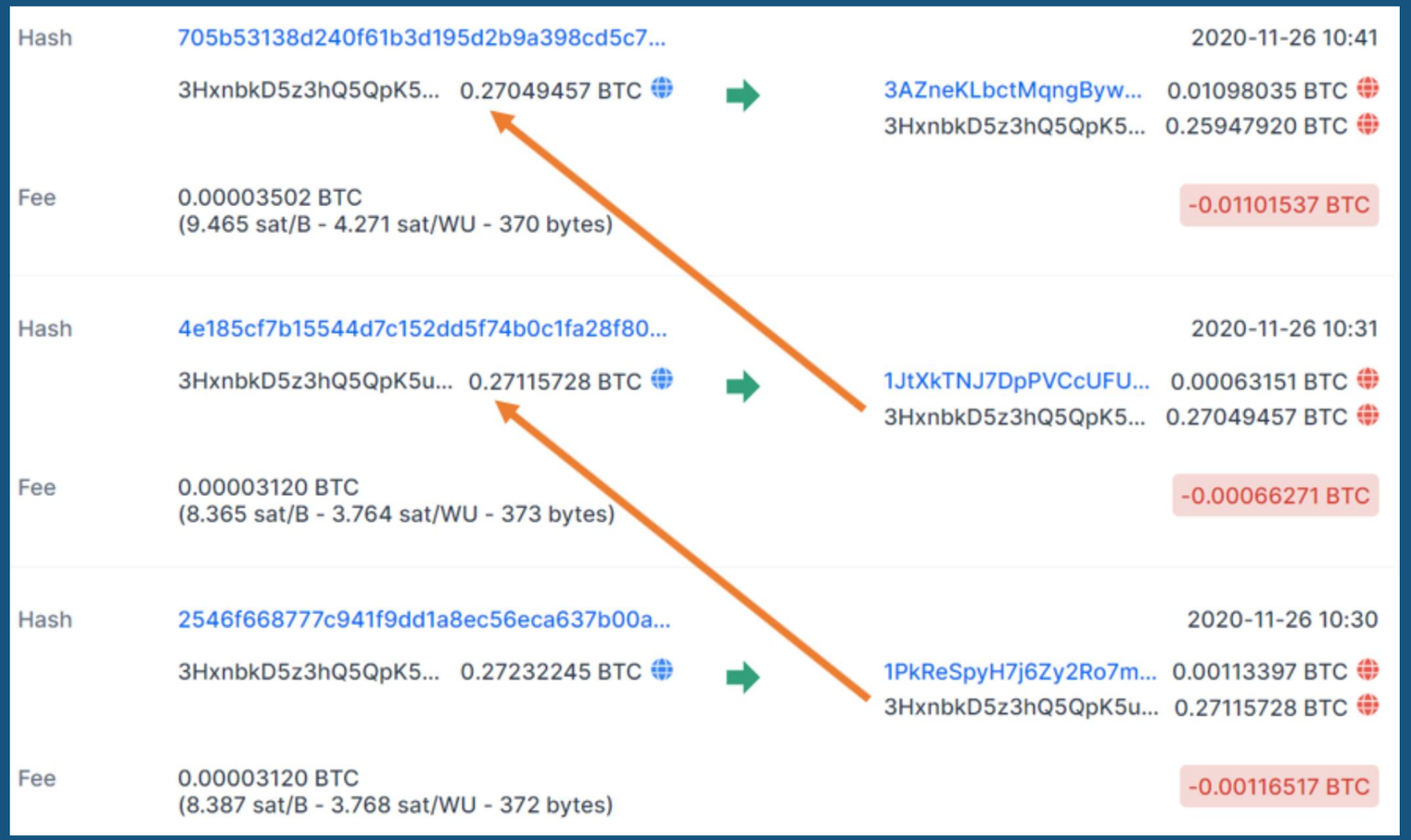
Show | Hide

Εικόνα: Αναπαράσταση πληροφοριών block # 659083, το οποίο περιέχει 2354 συναλλαγές

Κύκλος Ζωής Συναλλαγών	• Η αρχική δημιουργία μιας συναλλαγής ξεκινά συνήθως από κάποια εφαρμογή πορτοφόλι (wallet). Εν συνεχεία, υπογράφεται με την ψηφιακή υπογραφή του δημιουργού προκειμένου να ξεκλειδωθεί η χρηματική αξία των κρυπτονομισμάτων που θέλει να μεταφέρει. Έπειτα διαδίδεται σε ολόκληρο το δίκτυο μέχρι να φτάσει σε όλους τους κόμβους. Στο τελευταίο στάδιο θα επικυρωθεί από κάποιον Mining κόμβο και θα συμπεριληφθεί σε ένα μπλοκ συναλλαγών το οποίο θα καταγραφεί στο Blockchain
Μετάδοση Συναλλαγών στο Δίκτυο	• Προκειμένου μία συναλλαγή να συμπεριληφθεί και να διαδοθεί στο Blockchain πρέπει πρώτα να φτάσει στο δίκτυο. Κάθε συναλλαγή έχει μέγεθος περίπου 300 - 400 byte δεδομένων τα οποία πρέπει να φτάσουν σε κάποιον από τους κόμβους του δικτύου.
Διάδοση Συναλλαγών στο Δίκτυο	• Από την στιγμή που μια συναλλαγή σταλεί σε κάποιον κόμβο του δικτύου, επικυρώνεται από αυτόν και στην συνέχεια ο ίδιος κόμβος αναλαμβάνει να την διαβιβάσει στους κόμβους με τους όποιους συνδέεται • Όταν μία συναλλαγή σταλθεί σε κάποιον κόμβο αυτός με την σειρά του θα την στείλει σε 4 με 5 γειτονικούς κόμβους όπου με την σειρά τους ο καθένας θα την στείλει σε άλλους 4 με 5 κόμβους κ.ο.κ. Μέσα σε λίγα δευτερόλεπτα η συναλλαγή μεταβιβάζεται με έναν εκθετικά αυξανόμενο ρυθμό σε ολόκληρο το δίκτυο μέχρι να την λάβουν όλοι οι συνδεδεμένοι κόμβοι.

Αδαπάνητα Δεδομένα Εξόδου (Unspent Transaction Output)

- Το σημαντικότερο στοιχείο μιας συναλλαγής είναι τα αδαπάνητα δεδομένα εξόδου (Unspent Transaction Output).
- Στην πραγματικότητα το υπόλοιπο των λογαριασμών των χρηστών δεν είναι αποθηκευμένο κάπου. Αυτό που υπάρχει μόνο, είναι διάσπαρτα UTXO κλειδωμένα σε διάφορους ιδιοκτήτες. Το υπόλοιπο που εμφανίζεται στα πορτοφόλια κρυπτονομισμάτων είναι ουσιαστικά το άθροισμα των UTXO που υπάρχουν στο Blockchain που ανήκουν στον συγκεκριμένο χρήστη.
- Σε περίπτωση που ένα UTXO είναι μεγαλύτερο της αξίας της συναλλαγής τότε αυτό πρέπει να καταναλωθεί όλο και εκ νέου να δημιουργηθούν τα ρέστα της συναλλαγής.
- Τα UTXO μπορούν να ονομαστούν ως δεδομένα εισόδου αν καταναλώνονται από κάποια συναλλαγή, και ως δεδομένα εξόδου αν δημιουργούνται από κάποια συναλλαγή.



Για να κατανοήσουμε καλύτερα πως λειτουργούν όλα αυτά στον πραγματικό κόσμο ας δούμε για παράδειγμα το στιγμιότυπο κάποιων συναλλαγών που ανακτήθηκαν από το Blockchain.com

Όπως φαίνεται στην παρακάτω εικόνα ο χρήστης με διεύθυνση ***3HxnbkD5z3hQ5QpK5uNKaPdc7VbZ6AZ7qW*** στέλνει 0.00063151 BTC σε έναν άλλο χρήστη με διεύθυνση ***1JtXkTNJ7DpPVCcUFUGrr9H4967hwp1T9S*** και χρησιμοποιεί μια προηγούμενη έξοδο **0.27115728 BTC**. Η συναλλαγή αποτελείται από μία έξοδο **0.00063151 BTC** και άλλη μια **0.27049457 BTC** ως UTXO πίσω στον αρχικό αποστολέα. Μια καλή πρακτική ασφάλειας είναι να χρησιμοποιείται ένα νέο ζεύγος κλειδιών για κάθε νέα συναλλαγή.

Πορτοφόλια Κρυπτονομισμάτων

- Τα πορτοφόλια κρυπτονομισμάτων είναι ψηφιακά πορτοφόλια που χρησιμοποιούνται για τη λήψη, αποστολή και αποθήκευση ψηφιακών νομισμάτων.

- Χρησιμοποιούν μηχανισμούς κρυπτογράφησης και περιλαμβάνουν τη χρήση ιδιωτικών και δημόσιων κλειδιών.

- Ένας αποστολέας θα απαιτήσει τη δημόσια διεύθυνση του παραλήπτη για να του στείλει κρυπτονομίσματα και ο παραλήπτης με τη σειρά του για να αποκτήσει πρόσβαση σε αυτά θα χρησιμοποιήσει το ιδιωτικό του κλειδί.

- Παρόλο, που τα κλειδιά είναι συνδεδεμένα μεταξύ τους δεν μπορεί να προκύψει το ένα από το άλλο. Με άλλα λόγια, αν ο αποστολέας γνωρίζει το δημόσιο κλειδί του παραλήπτη, δεν μπορεί να προσδιορίσει το ιδιωτικό του κλειδί.

Τύποι Πορτοφολιών

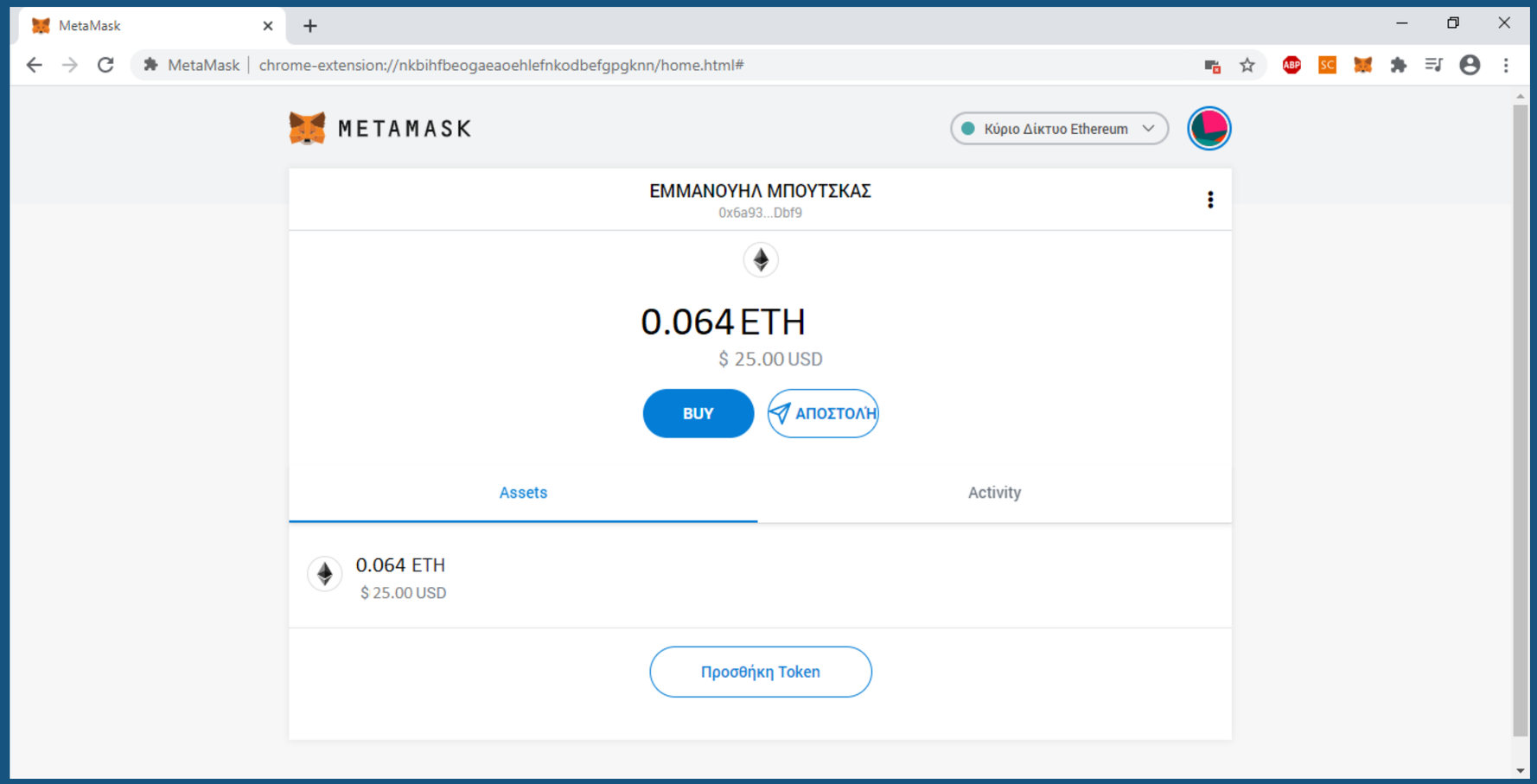
- Τα πορτοφόλια κρυπτονομισμάτων χωρίζονται ως επί πρωτίστως σε «Ζεστά» (διαδικτυακά πορτοφόλια) και «Κρύα» (μη συνδεδεμένα στο διαδίκτυο).

- Τα πορτοφόλια που είναι αποθηκευμένα σε οποιονδήποτε ιστότοπο/βάση δεδομένων ονομάζονται διαδικτυακά πορτοφόλια (online wallets).

- Από την άλλη πλευρά, ένα πορτοφόλι λέγεται ότι είναι ένα πορτοφόλι χωρίς σύνδεση (offline wallet) όταν δεν είναι συνδεδεμένο στο Διαδίκτυο. Για παράδειγμα, πορτοφόλια που είναι αποθηκευμένα σε μονάδες usb, χαρτιά, αρχεία κειμένου και ούτω καθεξής. Τα offline wallets ονομάζονται επίσης «κρύα» πορτοφόλια (cold wallets).

Πορτοφόλια Ιστού (Web wallets)

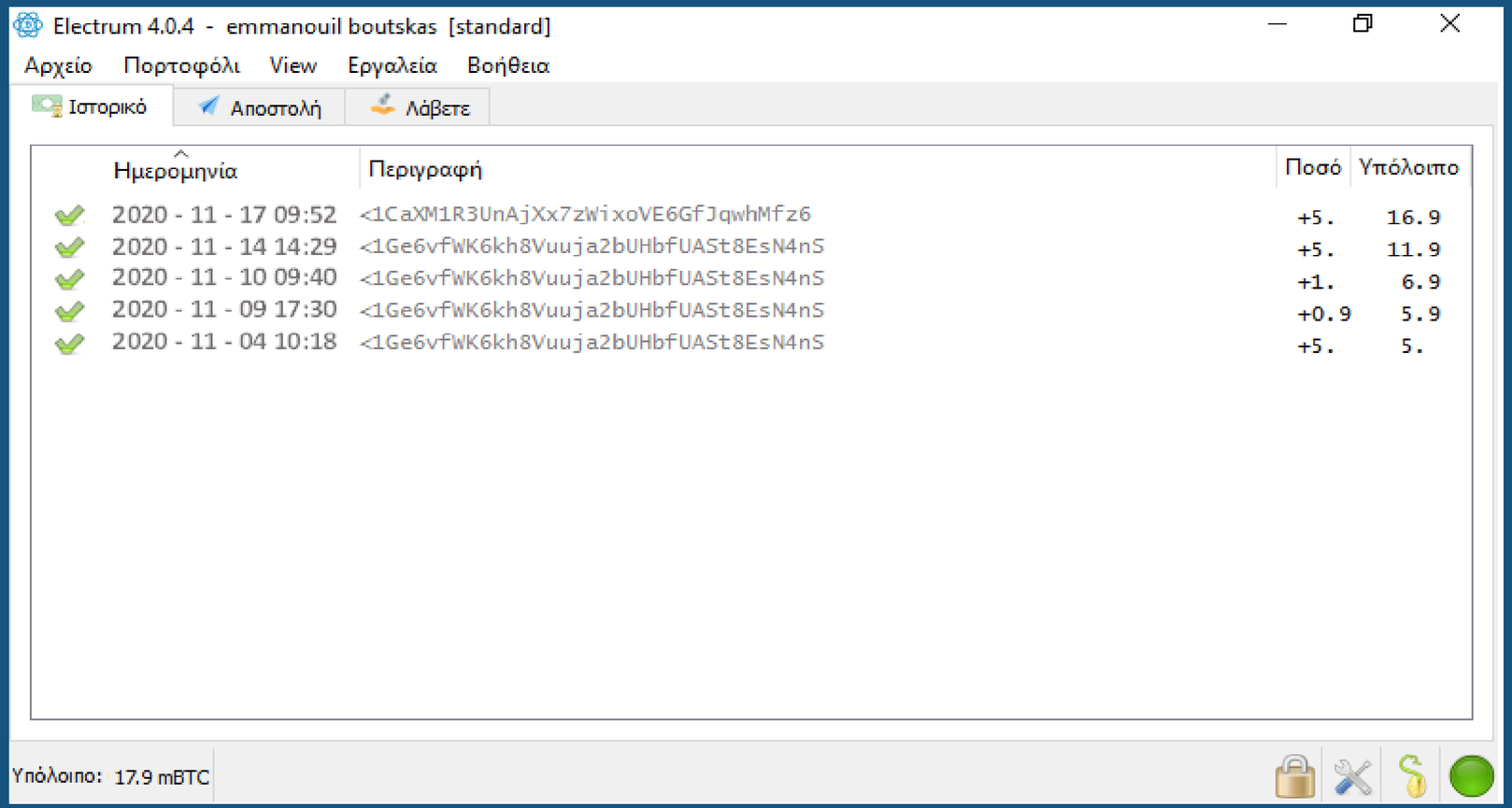
Τα πορτοφόλια ιστού λειτουργούν ως διαδικτυακές πλατφόρμες για συναλλαγές κρυπτονομισμάτων και είναι προσβάσιμα μέσω προγραμμάτων περιήγησης ιστού όπως το Google Chrome, το Mozilla Firefox, το Opera κ.λπ . Παρέχουν μια εμπειρία παρόμοια με τις διαδικτυακές τραπεζικές υπηρεσίες και μπορούν να συνδεθούν αυτόματα στον τραπεζικό λογαριασμό του χρήστη.



Εικόνα: MetaMask Web wallet

Πορτοφόλια Επιφάνειας Εργασίας (Desktop Wallets)

Τα πορτοφόλια υπολογιστή θεωρούνται ασφαλέστερα σε σύγκριση με τα διαδικτυακά και κινητά πορτοφόλια και σε γενικές γραμμές, προσφέρουν έναν καλό συνδυασμό ασφάλειας και ευκολίας χρήσης. Ο βαθμός ασφάλειας ωστόσο, σχετίζεται άμεσα με την ποιότητα της προστασίας του υπολογιστή από διαδικτυακές απειλές, όπως ιούς υπολογιστών και κακόβουλο λογισμικό. Το κύριο πλεονέκτημα τους πηγάζει από την διαχείριση των ιδιωτικών κλειδιών, καθώς δεν αποθηκεύονται σε διακομιστή τρίτου μέρους αλλά στον ίδιο τον υπολογιστή, εξαλείφοντας την ανάγκη να βασίζονται σε τρίτους.



Εικόνα: Electrum Desktop wallet

Πορτοφόλια Κινητών Συσκευών (Mobile Wallets)

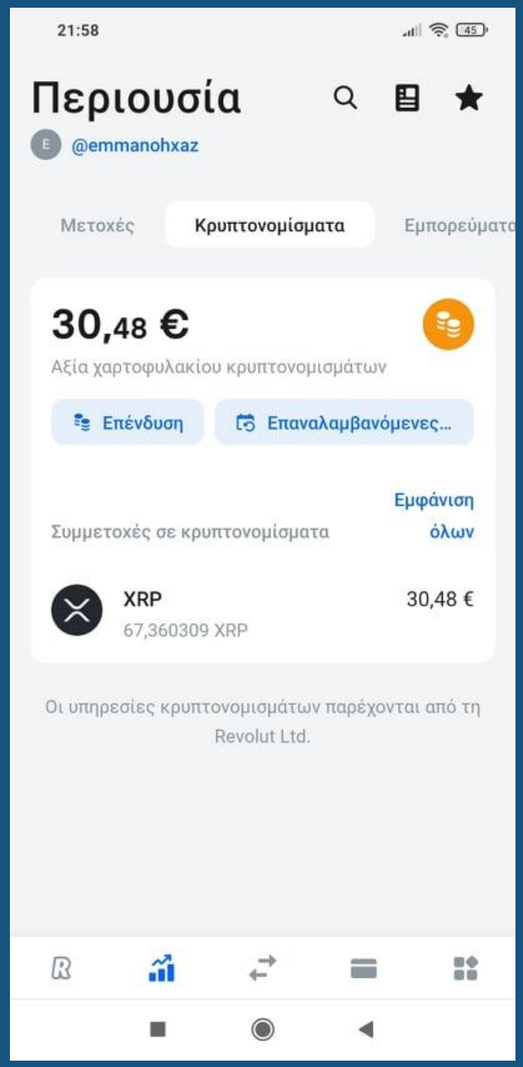
- Τα κινητά πορτοφόλια λειτουργούν ακριβώς όπως τα πορτοφόλια επιτραπέζιων υπολογιστών, αλλά είναι εφαρμογές ειδικά σχεδιασμένες για κινητά τηλέφωνα. Είναι ιδιαίτερα κατάλληλα για την ολοκλήρωση καθημερινών συναλλαγών και πληρωμών, καθιστώντας τα μια βιώσιμη επιλογή για περιπτώσεις όπου οι χρήστες βρίσκονται σε εξωτερικούς χώρους, προσπαθώντας να υλοποιήσουν μία συναλλαγή σε κάποιο φυσικό κατάστημα.

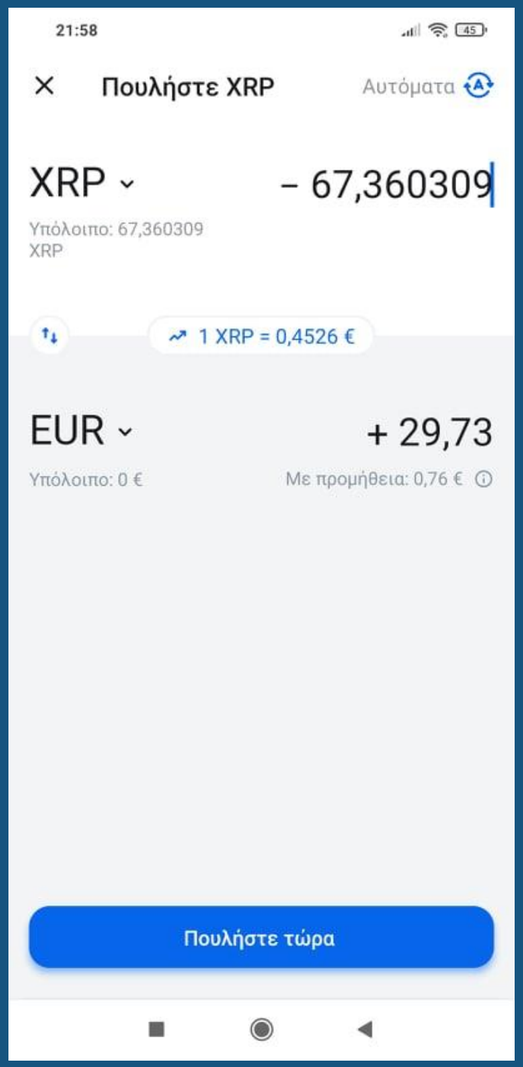
- Ένα κοινό χαρακτηριστικό των mobile wallets είναι ότι δεν είναι πλήρεις πελάτες (full clients). Οι πλήρεις clients είναι σε θέση να κατεβάζουν ολόκληρο το Blockchain το οποίο έχει χωρητικότητα αρκετά gigabyte.

- Ως εκ τούτου, ένα κινητό τηλέφωνο δεν είναι σε θέση να φέρει εις πέρας κάτι τέτοιο, καθώς αυτό θα οδηγήσει στην εμφάνιση προβλημάτων ως προς την λειτουργικότητα και την χωρητικότητα του. Αυτός είναι και ο λόγος που η σχεδίαση τους βασίζεται σε απλή επαλήθευση πληρωμής (Simple Payment Verification – SPV).

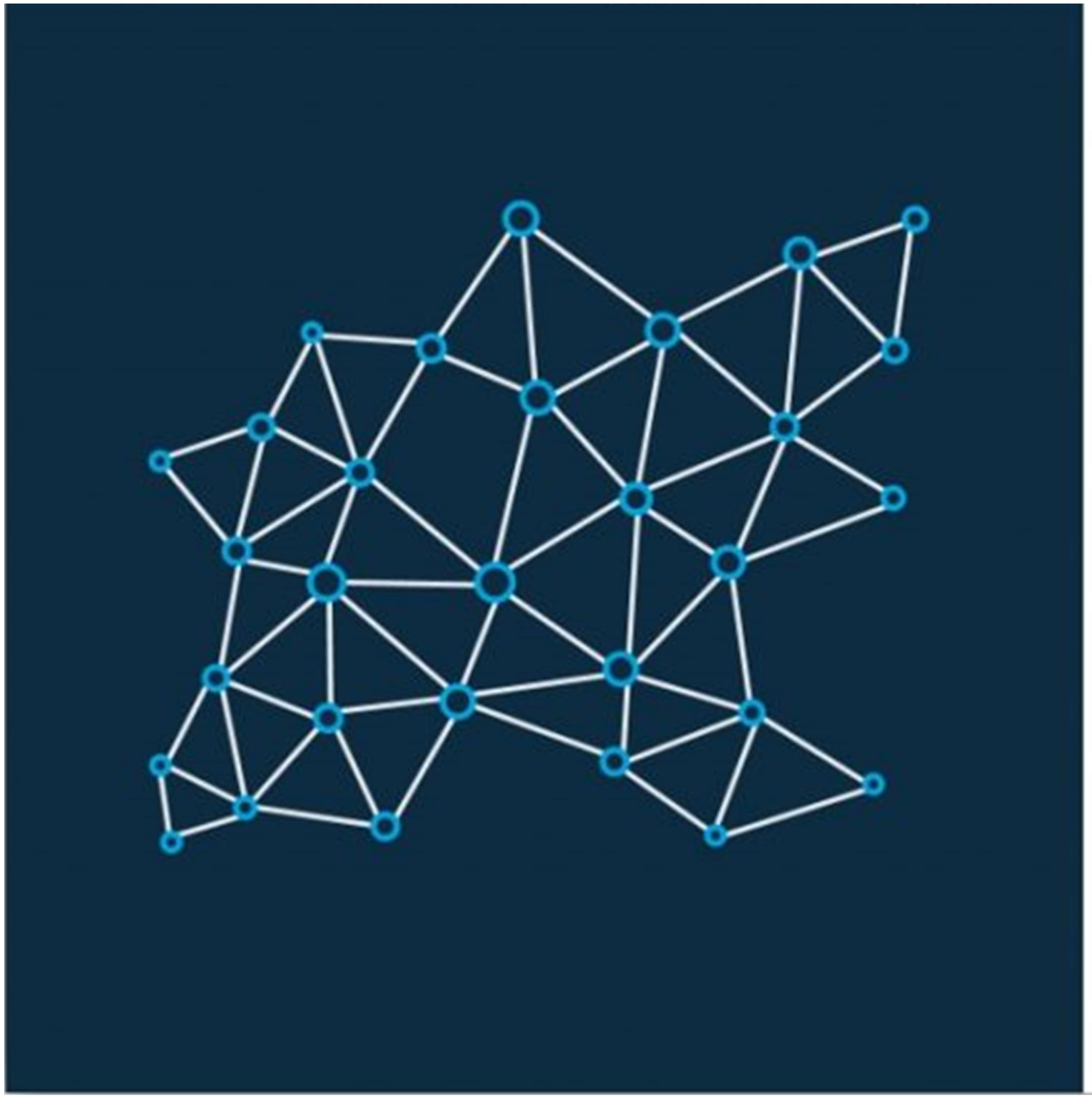
- Κατεβάζουν μόνο ένα μικρό κομμάτι του Blockchain. Για να το επιτύχουν αυτό βασίζονται σε έμπιστους κόμβους του δικτύου, με αυτό τον τρόπο σιγουρεύονται ότι έχουν τις σωστές πληροφορίες που χρειάζονται.

Πορτοφόλια Κινητών Συσκευών (Mobile Wallets)





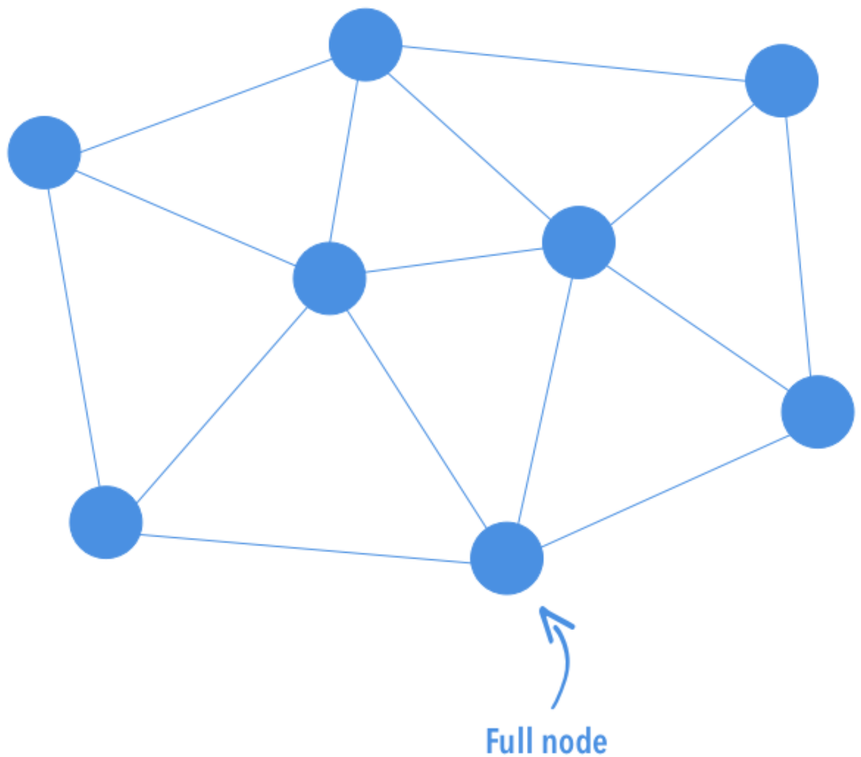
Εικόνα: Mobile wallet



Blockchain

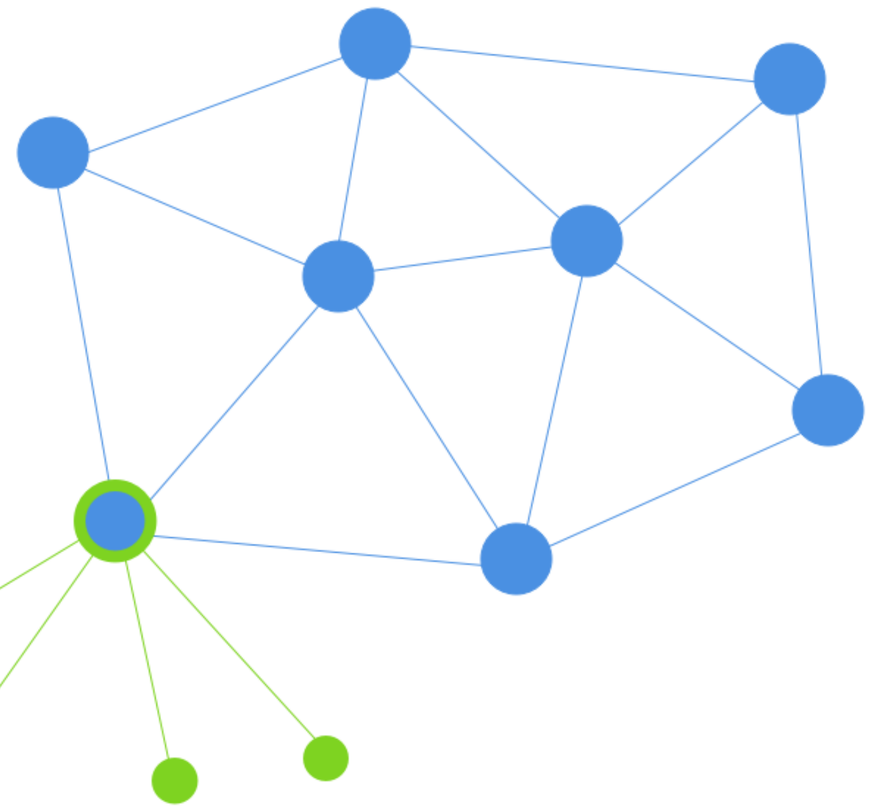
Ταξινόμηση Πορτοφολιών με Βάση τον Τρόπο Σύνδεσης στο Δίκτυο

Decentralized network



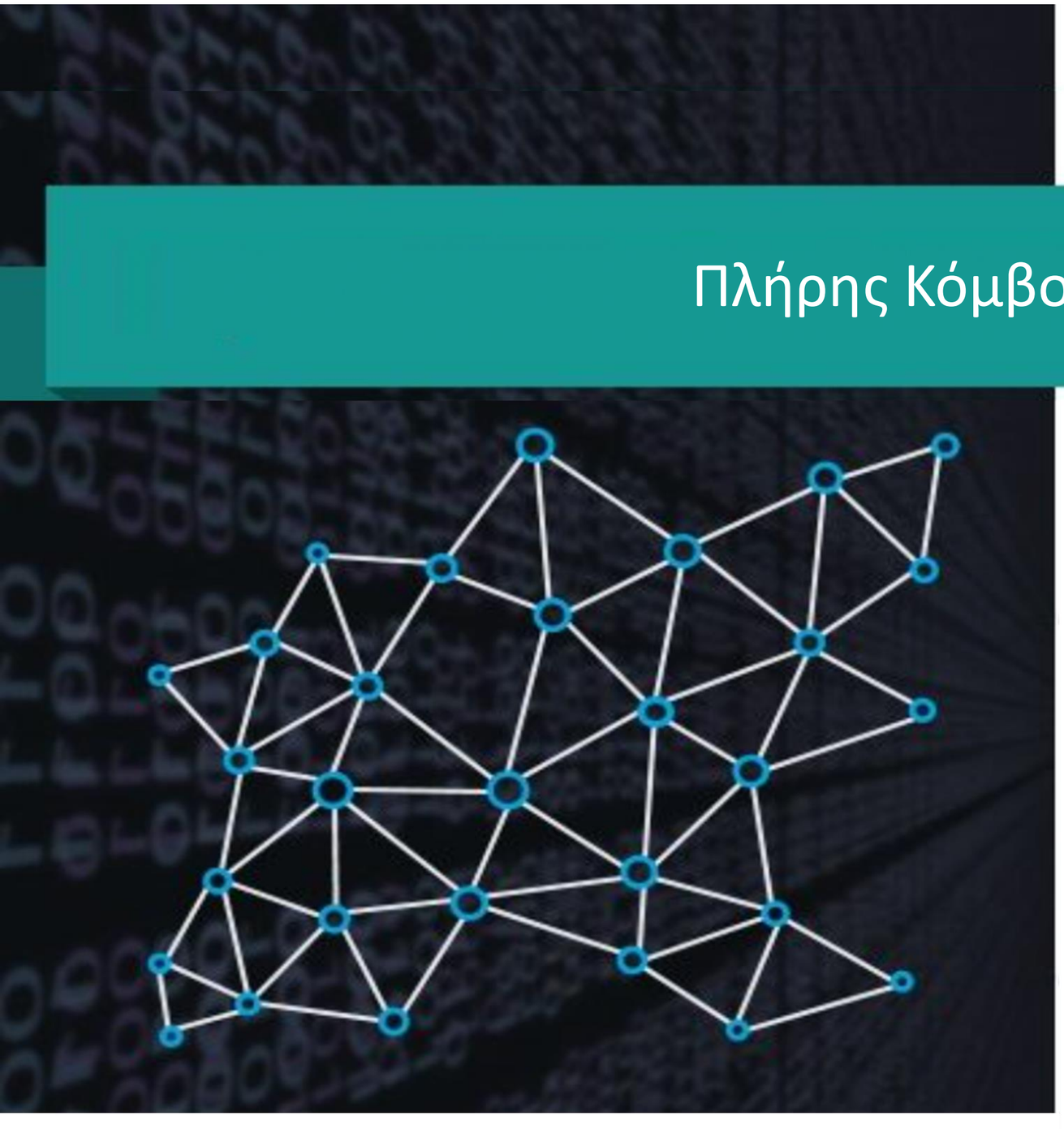
Full node

Decentralized network with light clients



Light client

Πλήρης Κόμβος (Full Node)



Τα πορτοφόλια που διατηρούν ένα πλήρες αντίγραφο του Blockchain ονομάζονται πλήρεις κόμβοι. Αυτά τα πορτοφόλια έχουν το πλεονέκτημα ότι δεν χρειάζεται να βασίζονται σε οποιονδήποτε τρίτο διακομιστή, αντιθέτως αποθηκεύουν και επεξεργάζονται ολόκληρη τη βάση δεδομένων των συναλλαγών, καθιστώντας τα περισσότερο ασφαλή σε σχέση με τα ελαφριά πορτοφόλια (light nodes).

Ελαφρύς Κόμβος (Lightweight Node)

Οι ελαφριοί κόμβοι βοηθούν στην επαλήθευση συναλλαγών χρησιμοποιώντας μια μέθοδο που ονομάζεται απλοποιημένη επαλήθευση πληρωμής (Simplified Payment Verification - SPV). Αυτή η μέθοδος επιτρέπει σε έναν κόμβο να επαληθεύσει εάν μια συναλλαγή έχει συμπεριληφθεί σε ένα μπλοκ, χωρίς να χρειάζεται να κάνει λήψη ολόκληρου του Blockchain. Χρησιμοποιώντας την απλοποιημένη επαλήθευση πληρωμής, οι ελαφριοί κόμβοι συνδέονται σε πλήρεις κόμβους και μεταδίδουν συναλλαγές σε αυτούς για επαληθεύσεις. Οι ελαφριοί κόμβοι αποθηκεύουν μόνο τις κεφαλίδες όλων των μπλοκ του Blockchain.

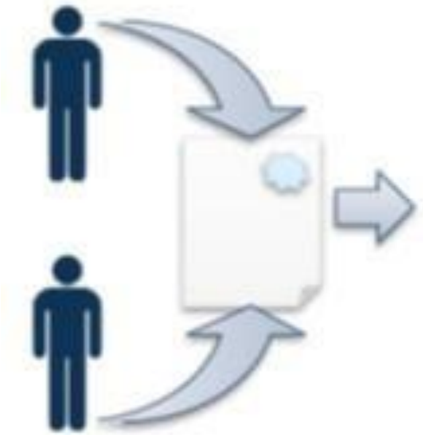
ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ

SMART CONTRACTS

Ένα “έξυπνο συμβόλαιο” αποτελεί μια «σύμβαση» μεταξύ δύο ή περισσότερων αντισυμβαλλομένων, το οποίο έχει συναφθεί μέσω ηλεκτρονικού κώδικα σε μια ηλεκτρονική πλατφόρμα εκτελώντας αυτομάτως τις υποχρεώσεις με τις οποίες δεσμεύονται στη συμφωνία οι συναλλασσόμενοι. Δεν υπάρχει ανάγκη για άμεση ανθρώπινη εμπλοκή στην σύναψη και εκτέλεση της μέσω των δυνατοτήτων κρυπτογραφικής ασφάλειας-πιστοποίησης των προσωπικών στοιχείων των συναλλασσόμενων που παρέχει η τεχνολογία Blockchain.

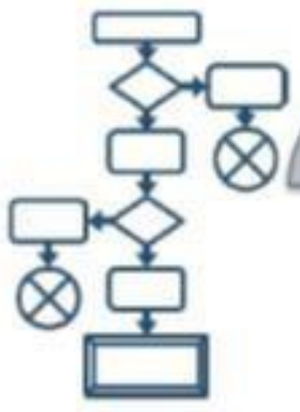
Εκτελούνται στο Blockchain, ακριβώς όπως έχουν προγραμματιστεί, χωρίς δυνατότητα λογοκρισίας, διακοπή λειτουργίας ή παρέμβασης τρίτων. Λειτουργούν εκτελώντας εντολές «if…then…else» που είναι γραμμένες σε κώδικα σε ένα Blockchain. Το δίκτυο υπολογιστών του Blockchain μπορεί να εκτελέσει ενέργειες όπως: αποδέσμευση χρημάτων στα κατάλληλα μέρη, αποστολή ειδοποιήσεων, έκδοση εισιτηρίων κλπ., μόνο όταν πληρούνται και έχουν επαληθευτεί οι προκαθορισμένες προϋποθέσεις που έχουν οριστεί στο συμβόλαιο. Στη συνέχεια, το Blockchain ενημερώνεται όταν ολοκληρωθεί η συναλλαγή.

Κύκλος Ζωής Έξυπνου Συμβολαίου



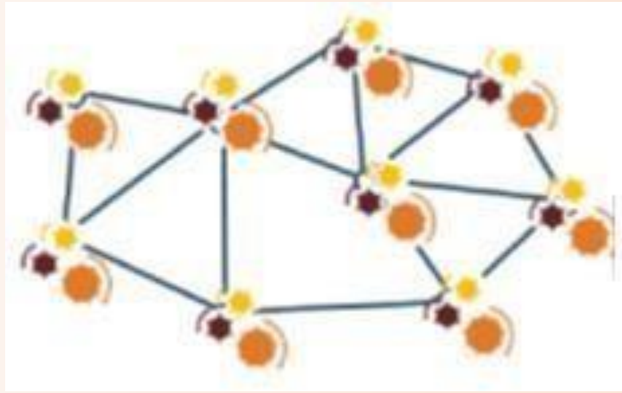
Τα μέρη συμφωνούν στη δημιουργία ενός συμβολαίου

Το συμβόλαιο καθορίζει ένα σύνολο κανόνων.



Οι κανόνες κωδικοποιούνται σε ένα πρόγραμμα

Το πρόγραμμα αποθηκεύεται στους κόμβους του Blockchain



Οι κόμβοι του Blockchain εκτελούν το πρόγραμμα του Έξυπνου Συμβολαίου

Πλεονεκτήματα έξυπνων συμβολαίων

1

Ταχύτητα: Τα έξυπνα συμβόλαια είναι ψηφιακά και αυτοματοποιημένα, επομένως δεν χρειάζεται επιπλέων χρόνος επεξεργασίας εγγράφων και διόρθωσης σφαλμάτων που συχνά παρατηρούνται σε έγγραφα που έχουν συμπληρωθεί με μη αυτόματο τρόπο.

2

Εμπιστοσύνη: Τα έξυπνα συμβόλαια εκτελούν αυτόματα συναλλαγές σύμφωνα με προκαθορισμένους κανόνες και οι κρυπτογραφημένες εγγραφές αυτών των συναλλαγών κοινοποιούνται σε όλους τους συμμετέχοντες. Επομένως, κανείς δεν μπορεί να αμφισβητεί ότι έχουν αλλάξει πληροφορίες για προσωπικό όφελος.

3

Ασφάλεια: Τα αρχεία συναλλαγών Blockchain είναι κρυπτογραφημένα και αυτό τα καθιστά πολύ δύσκολο να τροποποιηθούν από κακόβουλους χρήστες. Επειδή κάθε μεμονωμένη εγγραφή συνδέεται με προηγούμενες και επόμενες εγγραφές σε ένα κατανεμημένο καθολικό, ολόκληρη η αλυσίδα θα πρέπει να αλλάξει για να μεταβληθεί μία μόνο εγγραφή.

ethereum

Σήμερα, η δημοφιλέστερη πλατφόρμα ανάπτυξης έξυπνων συμβολαίων είναι η Ethereum Virtual Machine (EVM). Πρόκειται, για μία αποκεντρωμένη εικονική μηχανή που παρέχεται από το Ethereum ως περιβάλλον για εκτέλεση έξυπνων συμβολαίων. Η EVM μπορεί να θεωρηθεί ως ένας παγκόσμιος αποκεντρωμένος υπολογιστής στον οποίο εκτελούνται όλα τα έξυπνα συμβόλαια. Ένα έξυπνο συμβόλαιο στην EVM γράφετε σε γλώσσα προγραμματισμού Solidity (παρόμοια με την JavaScript) και ανεβαίνει στο Blockchain. Μόλις προστεθεί στο Blockchain, στο έξυπνο συμβόλαιο εκχωρείται μια διεύθυνση, η οποία αποτελεί μοναδικό αναγνωριστικό του.

Συναλλαγή Δημιουργίας Συμβολαίου

Μια ειδική περίπτωση που πρέπει να αναφέρουμε είναι μια συναλλαγή που δημιουργεί ένα νέο συμβόλαιο στο Blockchain, αναπτύσσοντας το για μελλοντική χρήση. Δεν υπάρχει κανένα αντίστοιχο ζεύγος ιδιωτικού-δημόσιου κλειδιού, όπως γίνεται με μία κανονική συναλλαγή. Αυτή η συναλλαγή είναι μηδενική και δεν περιέχει καμία ποσότητα Ether.

Μια συναλλαγή δημιουργίας συμβολαίου πρέπει να περιέχει το μεταγλωττισμένο bytecode που θα δημιουργήσει το συμβόλαιο. Όπως φαίνεται στη παρακάτω εικόνα αυτό εμφανίζεται στο πεδίο Input Data. Το μόνο αποτέλεσμα αυτής της συναλλαγής είναι η δημιουργία του συμβολαίου και τίποτα παραπάνω.

Transaction Details

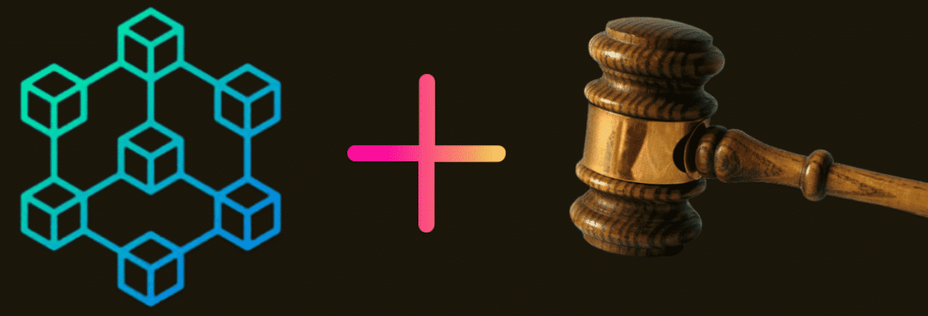
Buy | Exchange | Earn | Crypto Credit

Overview | Internal Txns | State | Comments

Transaction Hash:	0x44ecbe6614b27b60b73b6b0f456c76d77003085aee53d1db154d14fc3ef6a1df
Status:	Success
Block:	11354685 694 Block Confirmations
Timestamp:	2 hrs 41 mins ago (Nov-29-2020 04:20:49 PM +UTC) | Confirmed within 7 secs
From:	0xf827ac3a510eca8d7f356c9c9d78699d5848cabf
To:	[Contract 0xf1ca03aae24c4865d09643cb929141d8d3c60a75 Created]
Value:	0 Ether ($0.00)
Transaction Fee:	0.0583840376 Ether ($32.34)
Gas Price:	0.0000000211 Ether (21.1 Gwei)
Gas Limit:	2,767,016
Gas Used by Transaction:	2,767,016 (100%)
Nonce Position	98 7
Input Data:	0x60e06040523480156200001157600080fd5b50604051620033eb380380620033eb833981016040819052620000349162000182565b6001600055600160160160601b0319606083901b1660a0526040805163 5a2f760e11b8152905160016001600160a01b0384169163aca345ee916004808301926020929190829003018186803b1580156200008c57600080fd5b505afa158015620000a1573d6000803e3d6000fd5b505050506040513d601f19601f820116820180604052508101906200 00c791906200015c565b6001600160a01b031663fbfa77cf6040518163ffffffff1660e01b8152600401602060405180830381 86803b1580156200001005760008fd5b505afa158015620001157573d6000803e3d6000fd5b505050506040513d601f19601f820116820180604052508

View Input As | Decode Input Data

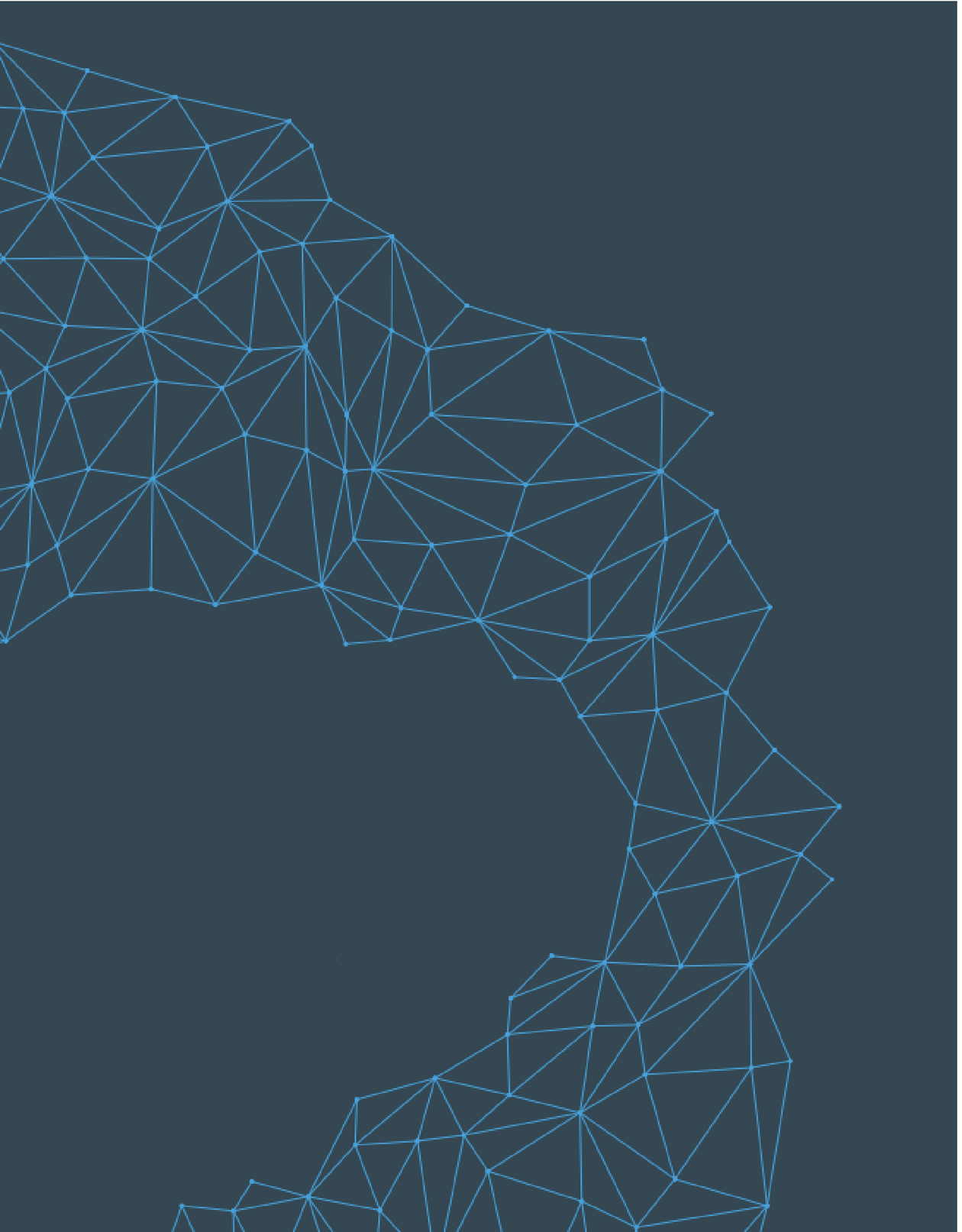
Νομικά Ζητήματα και Περιορισμοί



- Μέχρι στιγμής, τα έξυπνα συμβόλαια δεν είναι νομικά εκτελεστέα, αν και έχουν γίνει προσπάθειες προς αυτή την κατεύθυνση.

- Συγκεκριμένα, η ειδική επιτροπή για θέματα δικαιοδοσίας του Ηνωμένου Βασιλείου (UK Jurisdiction Taskforce) δημοσίευσε νομική δήλωση σχετικά με το καθεστώς των κρυπτονομισμάτωνν και των έξυπνων συμβάσεων, σύμφωνα με το δίκαιο της Αγγλίας και της Ουαλίας.

- Εν ολίγοις, η νομική της δήλωση καταλήγει στο συμπέρασμα ότι τα κρυπτονομίσματα μπορούν να αποτελέσουν νομική μορφή ιδιοκτησίας και ότι τα έξυπνα συμβόλαια μπορούν, ανάλογα με τα γεγονότα, να πληρούν τις προϋποθέσεις για έγκυρη σύναψη δεσμευτικής σύμβασης μεταξύ των μερών.

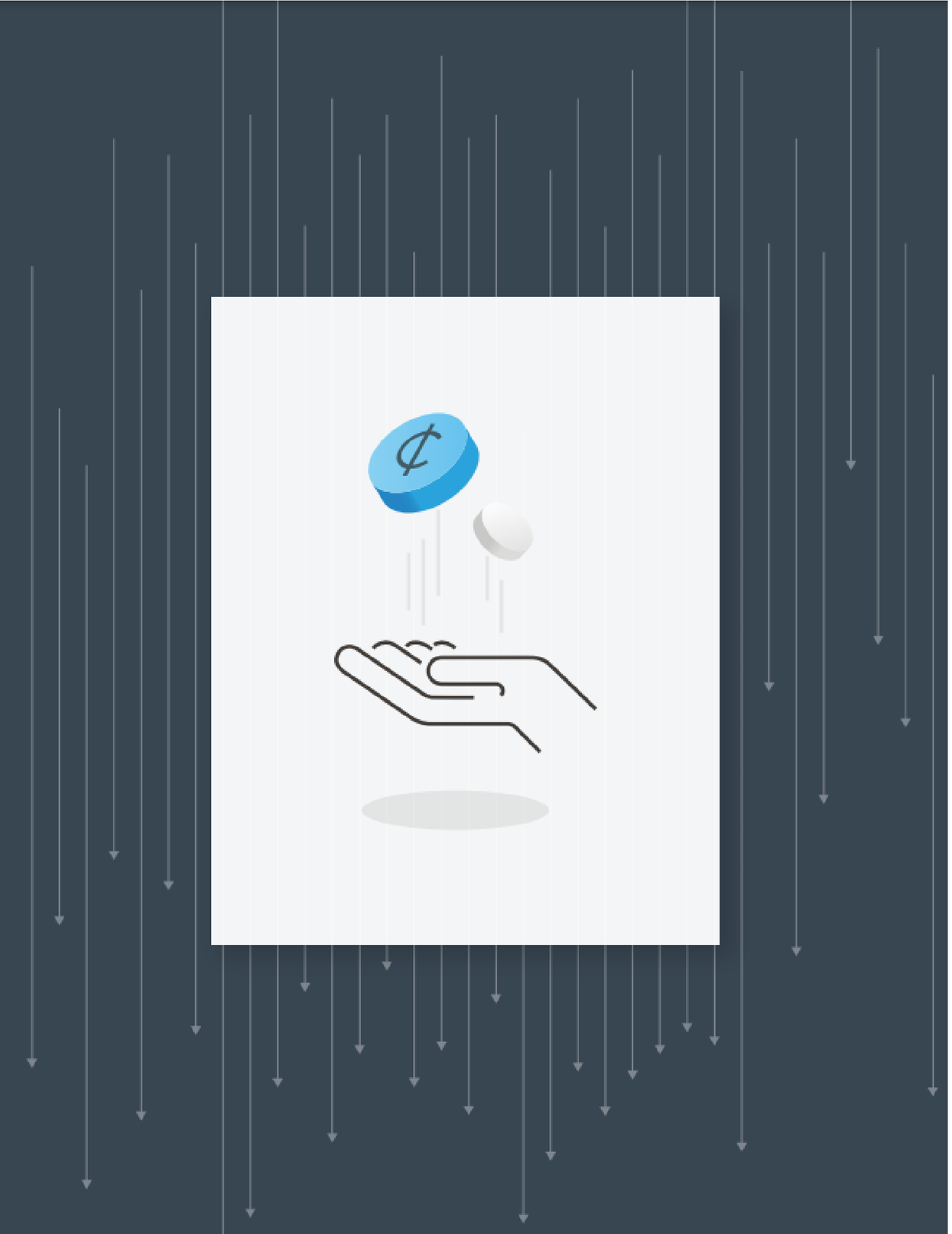


Συμπεράσματα

- Το Blockchain βρίσκεται στην παγκόσμια αγορά για περισσότερα από δέκα χρόνια και έχει εισβάλλει στη χρηματοοικονομική αγορά με σκοπό να αλλάξει τον τρόπο με τον οποίο υλοποιούνται οι ψηφιακές συναλλαγές.

- Οι τεχνολογίες γύρω από το blockchain μετασχηματίζουν ριζικά τον τρόπο οργάνωσης και λειτουργίας της οικονομίας καθώς δημιουργούν την τεχνολογική δυνατότητα για ύπαρξη κατανεμημένης μορφής εμπιστοσύνης.

- Τα κρυπτονομίσματα εξακολουθούν να εμφανίζουν σημαντικά εμπόδια που πρέπει να ξεπεραστούν προτού μπορέσουν να συνυπάρξουν πλήρως με τα τρέχοντα νομισματικά συστήματα.



- Το μεγαλύτερο όλων είναι η αντίθεση των υφιστάμενων χρηματοπιστωτικών ιδρυμάτων, τα οποία ασκούν μεγάλη πίεση και έχουν κίνητρα για να αποθαρρύνουν τον πολλαπλασιασμό των κρυπτονομισμάτων.

- Έχοντας αυτό κατά νου, η Ripple η οποία παρέχει υπηρεσίες πληρωμών που χρησιμοποιούν το ψηφιακό νόμισμα XRP έχει ξεκινήσει να συνεργάζεται με κεντρικές τράπεζες ανά τον κόσμο για να βοηθήσει στην επίτευξη διαλειτουργικότητας μεταξύ διαφόρων περιουσιακών στοιχείων όπως σταθερά νομίσματα και κρυπτονομίσματα.

Ευχαριστώ


Digital Wallet
International Bank
Local Bank
Correspondent Bank
Payment Provider
Correspondent Bank
Local Bank
Payment Provider
Local Bank
Digital Wallet
International Bank