2021-1-IE01-KA220-VET-000032943

Co-funded by the Erasmus+ Programme of the European Union

TrainChain
Blockchain Training for Start Ups

PR1-T3 Βασικό περιεχόμενο

Ενότητα 0 – Εισαγωγή στην Blockchain Τεχνολογία

Συντάκτης: CCSDE

Ταυτότητα project:

Συμφωνία επιχορήγησης	2021-1-IE01-KA220-VET-000032943
Πρόγραμμα	Erasmus+
Βασική δράση	KA220-VET - Cooperation partnerships in vocational education and training
Πεδίο	Vocational Education and Training
Ακρωνύμιο έργου	TrainChain
Τίτλος του έργου	TrainChain - Blockchain Training for Start Ups
Ημερομηνία έναρξης του έργου	28/02/2022
Διάρκεια του έργου	24 μήνες
Ημερομηνία λήξης του έργου	27/02/2024

ΙΣΤΟΡΙΚΌ ΑΝΑΘΕΏΡΗΣΗΣ

Έκδοση	Ημερομηνία	Συγγραφέας	Περιγραφή	Δράση	Σελίδες
1.0	31/07/2022	CCSDE	Δημιουργία	C	8

(*) Action: C = Creation, I = Insert, U = Update, R = Replace, D = Delete

ΑΝΑΦΕΡΌΜΕΝΑ ΈΓΓΡΑΦΑ

ID	Πηγές	Τίτλος
1	2021-1-IE01-KA220-VET-000032943	TrainChain Agreement

ΙΣΧΎΟΝΤΑ ΈΓΓΡΑΦΑ

ID	Reference		Title
1			
2			

Contents

1. Introduction ..... **Error! Bookmark not defined.**
1.1 Module Description ..... **Error! Bookmark not defined.**
1.2 Module Goals 5
1.3 Learning Objectives ..... **Error! Bookmark not defined.**
1.4 Learning Outcomes ..... **Error! Bookmark not defined.**
2. Main Content ..... **Error! Bookmark not defined.**
2.1 Blockchain 5
2.2 Main Blockchain Applications & Evolution ..... **Error! Bookmark not defined.**
2.3 Other Blockchains in use ..... **Error! Bookmark not defined.**
3. Knowledge Assessment ..... **Error! Bookmark not defined.**
4. Module Summary ..... **Error! Bookmark not defined.**
5. References ..... **Error! Bookmark not defined.**

1. Εσαγωγή

1.1 Περιγραφή ενότητας

Στο πρώτο μέρος της ενότητας, θα...

- Ανακαλύψτε τον νέο κόσμο των αλυσίδων μπλοκ,

- Καταλάβετε γιατί έχουν σημασία,

Στο δεύτερο μέρος της ενότητας, θα...

- Προσδιορίστε τους τρεις τύπους αλυσίδων μπλοκ,
- Να εμβαθύνουμε τις γνώσεις μας σχετικά με τον τρόπο λειτουργίας των αλυσίδων μπλοκ.

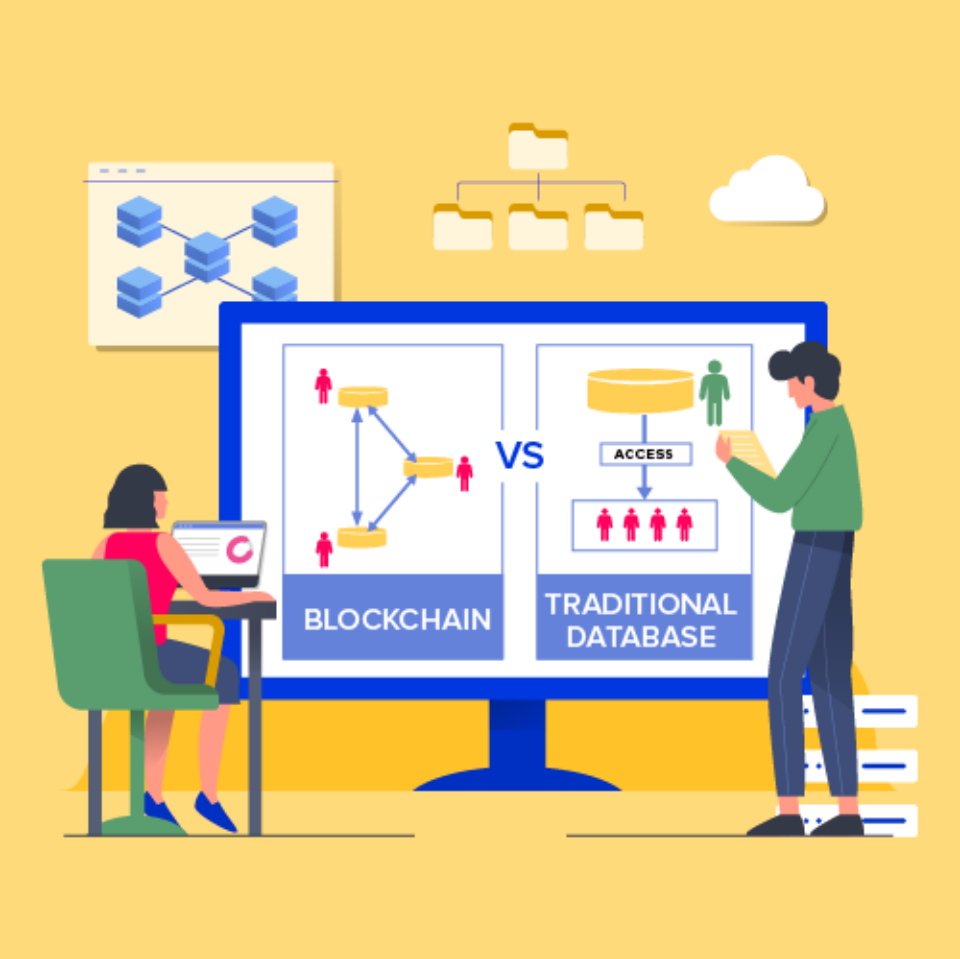
2. Βασικό περιεχόμενο

2.1 Blockchain

Αρχικά, η αλυσίδα μπλοκ ήταν απλώς ο όρος της επιστήμης των υπολογιστών για τον τρόπο διάρθρωσης και διαμοιρασμού δεδομένων. Σήμερα οι αλυσίδες μπλοκ χαρακτηρίζονται ως η πέμπτη εξέλιξη της πληροφορικής.

Οι αλυσίδες μπλοκ αποτελούν μια νέα προσέγγιση της κατανεμημένης βάσης δεδομένων. Η καινοτομία προέρχεται από την ενσωμάτωση παλαιάς τεχνολογίας με νέους τρόπους. Μπορείτε να σκεφτείτε τις αλυσίδες μπλοκ ως κατανεμημένες βάσεις δεδομένων που ελέγχει μια ομάδα ατόμων και οι οποίες αποθηκεύουν και μοιράζονται πληροφορίες.

Υπάρχουν πολλοί διαφορετικοί τύποι αλυσίδων μπλοκ και εφαρμογών αλυσίδας μπλοκ. Η αλυσίδα μπλοκ είναι μια ολοκληρωμένη τεχνολογία που ενσωματώνεται σε όλες τις πλατφόρμες και το υλικό σε όλο τον κόσμο.



Τι είναι οι αλυσίδες μπλοκ

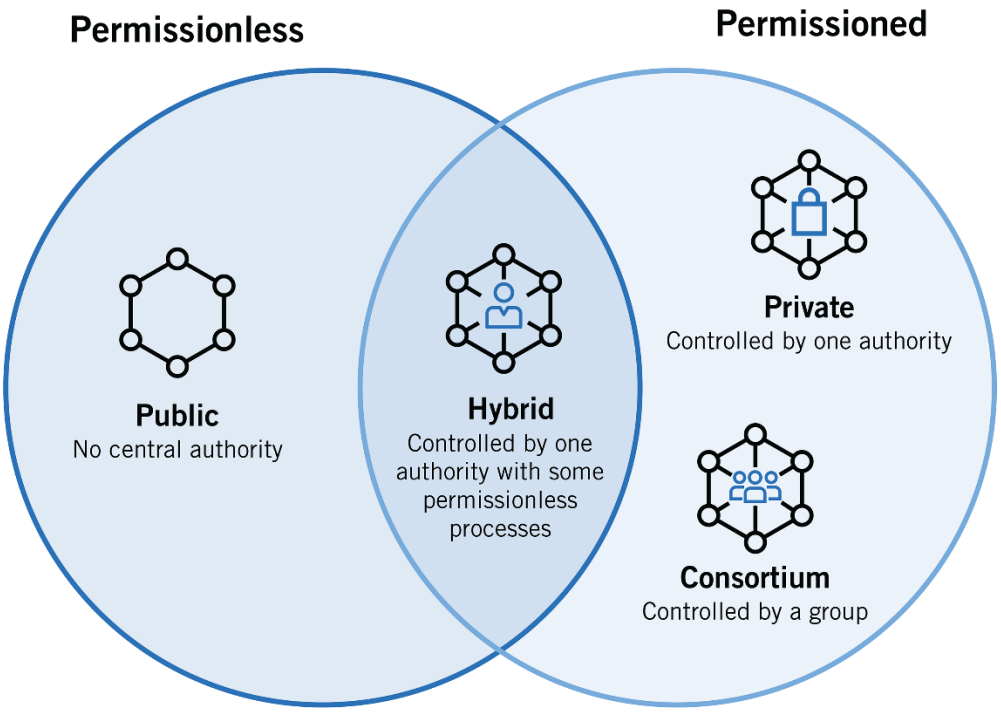
Η αλυσίδα μπλοκ είναι μια δομή δεδομένων που καθιστά δυνατή τη δημιουργία ενός ψηφιακού βιβλίου δεδομένων και τη διανομή του σε ένα δίκτυο ανεξάρτητων μερών. Υπάρχουν πολλοί διαφορετικοί τύποι αλυσίδων μπλοκ.

- Δημόσιες αλυσίδες μπλοκ: Οι δημόσιες αλυσίδες μπλοκ, όπως το Bitcoin, είναι μεγάλα κατανεμημένα δίκτυα που λειτουργούν μέσω ενός εγγενούς κρυπτονομίσματος. Ένα κρυπτονόμισμα είναι ένα μοναδικό κομμάτι δεδομένων που μπορεί να αποτελέσει αντικείμενο συναλλαγής μεταξύ δύο μερών. Οι δημόσιες αλυσίδες μπλοκ είναι ανοικτές για οποιονδήποτε να συμμετέχει σε οποιοδήποτε επίπεδο και διαθέτουν κώδικα ανοικτού κώδικα που συντηρεί η κοινότητά τους.

- Οι αλυσίδες μπλοκ με άδεια χρήσης: Οι αλυσίδες μπλοκ με άδεια, όπως η Ripple, ελέγχουν τους ρόλους που μπορούν να διαδραματίσουν τα άτομα στο δίκτυο. Εξακολουθούν να είναι μεγάλα και κατανεμημένα συστήματα που χρησιμοποιούν ένα εγγενές token. Ο βασικός τους κώδικας μπορεί να είναι ή να μην είναι ανοιχτού κώδικα.

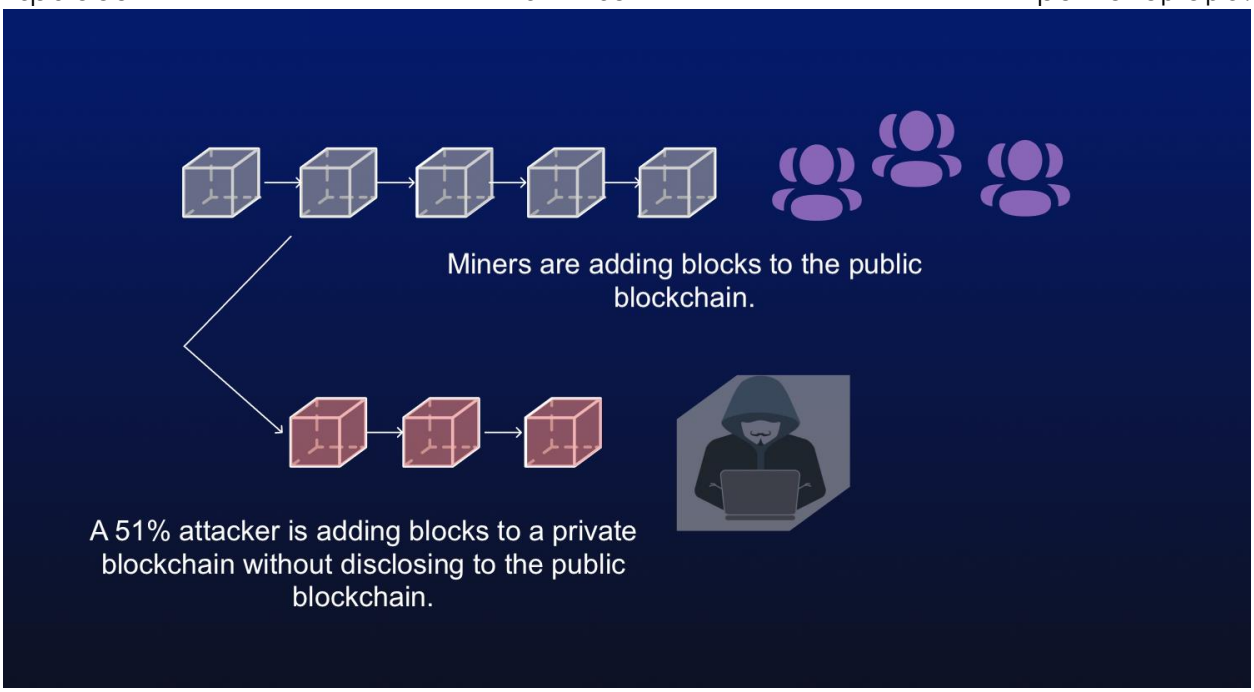
- Ιδιωτικές αλυσίδες μπλοκ: Οι ιδιωτικές αλυσίδες μπλοκ, γνωστές και ως τεχνολογία κατανεμημένου βιβλίου (DLT), τείνουν να είναι μικρότερες και δεν χρησιμοποιούν κάποιο κουπόνι ή κρυπτονόμισμα. Τα μέλη τους ελέγχονται στενά. Αυτού του είδους οι αλυσίδες μπλοκ προτιμώνται από κοινοπραξίες που έχουν έμπιστα μέλη και ανταλλάσσουν εμπιστευτικές πληροφορίες.

Και οι τρεις τύποι αλυσίδων μπλοκ χρησιμοποιούν κρυπτογραφία για να επιτρέπουν σε κάθε συμμετέχοντα σε οποιοδήποτε δίκτυο να διαχειρίζεται το λογιστικό βιβλίο με ασφαλή τρόπο, χωρίς να απαιτείται κεντρική αρχή για την επιβολή των κανόνων. Η απομάκρυνση της κεντρικής αρχής από τη δομή της βάσης δεδομένων είναι μία από τις πιο σημαντικές και ισχυρές πτυχές των αλυσίδων μπλοκ.



Οι αλυσίδες μπλοκ δημιουργούν μόνιμα αρχεία και ιστορικά των συναλλαγών, αλλά τίποτα δεν είναι πραγματικά μόνιμο. Η μονιμότητα του αρχείου βασίζεται στην αξιοπιστία και την υγεία του δικτύου. Στο πλαίσιο των αλυσίδων μπλοκ, αυτό σημαίνει ότι αν ένα μεγάλο μέρος της κοινότητας των αλυσίδων μπλοκ ήθελε να αλλάξει τις πληροφορίες που έχουν εγγραφεί στην αλυσίδα μπλοκ, θα μπορούσε να το κάνει. Το κρυπτονόμισμα χρησιμοποιείται ως ανταμοιβή για να δώσει κίνητρα σε πολλούς χρήστες να διευκολύνουν την υγιή λειτουργία του δικτύου μέσω του ανταγωνισμού. Εάν οι εγγραφές αλλάξουν με ακατάλληλο τρόπο, αυτό είναι γνωστό ως επίθεση 51%. Τα μικρά δίκτυα με λίγους ανεξάρτητους miners είναι ευάλωτα, επειδή δεν χρειάζεται μεγάλη προσπάθεια για να αλλάξουν τα στοιχεία τους και οι ισχυροί miners θα μπορούσαν να το κάνουν και να

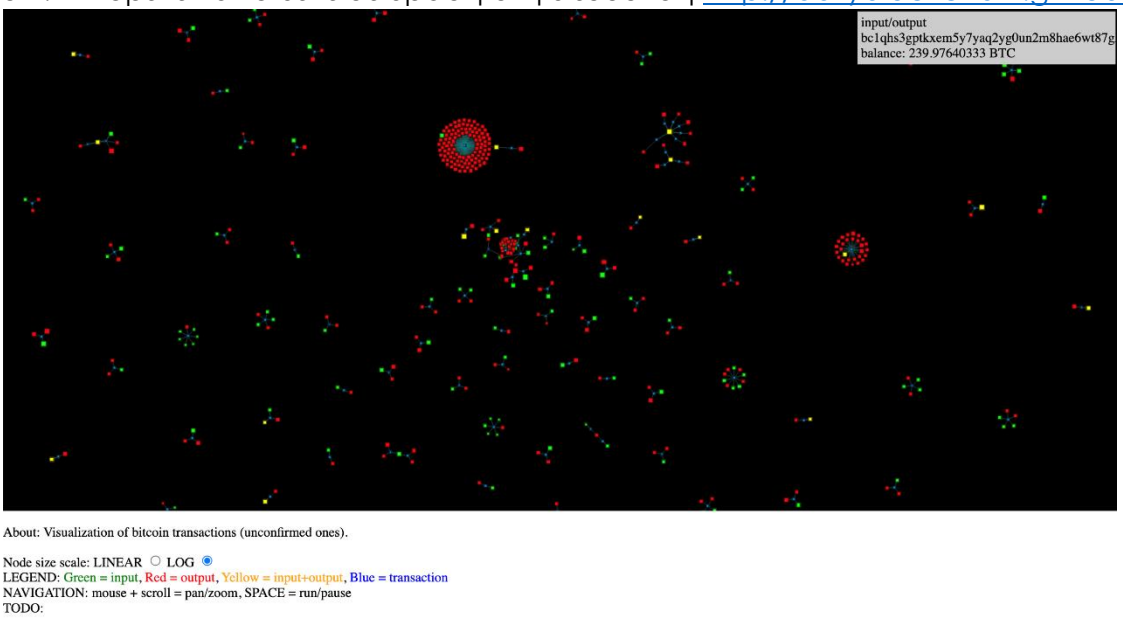
κερδίσουν επιπλέον κρυπτονόμισμα.



Τι κάνουν τα blockchains

Η αλυσίδα μπλοκ είναι ένα σύστημα peer-to-peer χωρίς κεντρική αρχή που διαχειρίζεται τη ροή δεδομένων. Ένας από τους βασικούς τρόπους για την άρση του κεντρικού ελέγχου με ταυτόχρονη διατήρηση της ακεραιότητας των δεδομένων είναι η ύπαρξη ενός μεγάλου κατανεμημένου δικτύου ανεξάρτητων χρηστών. Αυτό σημαίνει ότι οι υπολογιστές που απαρτίζουν το δίκτυο βρίσκονται σε περισσότερες από μία τοποθεσίες. Αυτοί οι υπολογιστές αναφέρονται συχνά ως πλήρεις κόμβοι".

"Στην Εικόνα 1-1 παρουσιάζεται μια οπτικοποίηση της δομής του δικτύου blockchain του Bitcoin. Μπορείτε να το δείτε σε δράση στη διεύθυνση http://dailyblockchain.github.io."



Για να αποφευχθεί η αλλοίωση του δικτύου, οι αλυσίδες μπλοκ δεν είναι μόνο αποκεντρωμένες, αλλά συχνά χρησιμοποιούν και ένα κρυπτονόμισμα. Τα δίκτυα blockchain παράγουν κρυπτονομίσματα ως κίνητρο για τη διατήρηση της ακεραιότητας του δικτύου. Πολλά κρυπτονομίσματα διαπραγματεύονται σε χρηματιστήρια όπως οι μετοχές.

Τα κρυπτονομίσματα λειτουργούν λίγο διαφορετικά σε κάθε αλυσίδα μπλοκ. Βασικά, το λογισμικό πληρώνει το υλικό για να λειτουργήσει. Το λογισμικό είναι το πρωτόκολλο της αλυσίδας μπλοκ. Τα γνωστά πρωτόκολλα blockchain περιλαμβάνουν το Bitcoin, το Ethereum, το Ripple, το Bitcoin Cash, το Stellar και το EOS. Το υλικό αποτελείται από τους πλήρεις κόμβους που διασφαλίζουν τα δεδομένα στο δίκτυο.

Γιατό το blockchains έχει σημασία

Οι αλυσίδες μπλοκ αναγνωρίζονται ως η "πέμπτη εξέλιξη" της πληροφορικής, επειδή αποτελούν ένα νέο επίπεδο εμπιστοσύνης για το Διαδίκτυο. Πριν από τις αλυσίδες μπλοκ, η εμπιστοσύνη εδραιωνόταν από κεντρικές αρχές που εξέδιδαν πιστοποιητικά. Ένα από αυτά που ίσως γνωρίζετε είναι τα πιστοποιητικά πελάτη Secure Sockets Layer (SSL). Ένα πιστοποιητικό SSL είναι η "πράσινη κλειδαριά" που βρίσκεται δίπλα σε έναν διαδικτυακό τομέα. Σας ενημερώνει ότι βρίσκεστε σε έναν ασφαλή ιστότοπο. Τα πιστοποιητικά SSL έχουν αποδειχθεί ότι δεν είναι αξιόπιστα. Πιστοποιητικά έχουν κλαπεί από τους τομείς της Κεντρικής Υπηρεσίας Πληροφοριών (CIA), της Μυστικής Υπηρεσίας Πληροφοριών του Ηνωμένου Βασιλείου (κοινώς γνωστή ως MI6), της Microsoft, της Yahoo!, του Skype, του Facebook και του Twitter. Η εξάρτηση από ένα τρίτο μέρος επιτρέπει την ύπαρξη ενός μοναδικού σημείου αποτυχίας.

Οι αλυσίδες μπλοκ, από την άλλη πλευρά, εγκαθιδρύουν την εμπιστοσύνη με νέους τρόπους. Οι αλυσίδες μπλοκ με απόδειξη εργασίας (POW) απαιτούν από τους ανθρακωρύχους να έχουν ένα πλήρες και ακριβές ιστορικό των συναλλαγών τους για να συμμετέχουν στο δίκτυο. Οι μπλοκ αλυσίδες απόδειξης συμμετοχής (POS) δημιουργούν εμπιστοσύνη απαιτώντας από τους κόμβους που επεξεργάζονται συναλλαγές να "ποντάρουν" κάποιο κρυπτονόμισμα το οποίο μπορεί να καταπέσει αν συλληφθούν να εξαπατούν το δίκτυο. Οι ιδιωτικές αλυσίδες μπλοκ δημιουργούν εμπιστοσύνη με τη διανομή δεδομένων σε ένα δίκτυο συνδεδεμένων αλλά ανεξάρτητων συμμετεχόντων που είναι γνωστοί μεταξύ τους και μπορούν να λογοδοτήσουν. Κάθε τύπος blockchain χρησιμοποιεί διαφορετικά συστήματα κινήτρων για να εδραιώσει την εμπιστοσύνη ότι κάθε συμμετέχων στο δίκτυο θα συνεργαστεί για την τήρηση ενός πλήρους και αναλλοίωτου ιστορικού "κάθε συναλλαγής ή καταχώρησης που γίνεται στη βάση δεδομένων που μοιράζονται.

Όταν τα δεδομένα είναι μόνιμα και αξιόπιστα σε ψηφιακή μορφή, μπορείτε να πραγματοποιείτε συναλλαγές στο διαδίκτυο με τρόπους που, στο παρελθόν, ήταν δυνατοί μόνο εκτός σύνδεσης. Όλα όσα μέχρι τώρα παρέμεναν αναλογικά, συμπεριλαμβανομένων των δικαιωμάτων ιδιοκτησίας και της ταυτότητας, μπορούν πλέον να δημιουργηθούν και να διατηρηθούν στο διαδίκτυο. Οι αργές επιχειρηματικές και τραπεζικές διαδικασίες, όπως οι μεταφορές χρημάτων και οι διακανονισμοί κεφαλαίων, μπορούν πλέον να γίνονται σχεδόν ακαριαία. Οι επιπτώσεις των ασφαλών ψηφιακών αρχείων είναι τεράστιες για την παγκόσμια οικονομία".

Οι αλυσίδες μπλοκ είναι σημαντικές επειδή επιτρέπουν νέα αποτελεσματικότητα και αξιοπιστία στην ανταλλαγή πολύτιμων και ιδιωτικών πληροφοριών που κάποτε απαιτούσαν τη διευκόλυνση ενός τρίτου μέρους, όπως η διακίνηση χρημάτων και η αυθεντικότητα της ταυτότητας. Αυτό είναι μεγάλη υπόθεση, επειδή μεγάλο μέρος της κοινωνίας και της οικονομίας μας έχει δομηθεί γύρω από την εγκαθίδρυση εμπιστοσύνης, την επιβολή της εμπιστοσύνης όταν αυτή παραβιάζεται και τα τρίτα μέρη που διευκολύνουν την εμπιστοσύνη. Μπορείτε να φανταστείτε πώς αυτό το απλό λογισμικό blockchain μπορεί να αξιοποιηθεί για να διορθώσει τομείς που έχουν αποδειχθεί ότι δεν είναι αλάνθαστοι, όπως οι ψηφοφορίες, η διαχείριση της εφοδιαστικής αλυσίδας, η κίνηση χρημάτων και η ανταλλαγή περιουσιακών στοιχείων.

Η δομή των Blockchains

Κάθε αλυσίδα μπλοκ είναι δομημένη ελαφρώς διαφορετικά. Ωστόσο, το Bitcoin είναι μια εξαιρετική αλυσίδα μπλοκ για μελέτη, επειδή χρησιμοποιήθηκε ως πρότυπο για τις περισσότερες μεταγενέστερες αλυσίδες μπλοκ. Τα δεδομένα στο Bitcoin είναι δομημένα έτσι ώστε κάθε πλήρης κόμβος (οι υπολογιστές που εκτελούν το δίκτυο) να περιέχει όλα τα δεδομένα του δικτύου. Αυτό το μοντέλο είναι συναρπαστικό από την άποψη της εμμονής των δεδομένων. Εξασφαλίζει ότι τα δεδομένα θα παραμείνουν άθικτα ακόμη και αν μερικοί από τους κόμβους εκτεθούν. Ωστόσο, επειδή κάθε κόμβος έχει ένα πλήρες αντίγραφο του ιστορικού των συναλλαγών, από την αρχή, και κάθε συναλλαγής στο μέλλον, απαιτεί οι καταχωρήσεις να είναι όσο το δυνατόν μικρότερες από άποψη αποθηκευτικής ικανότητας.

Συγκριτικά, άλλα κατανεμημένα δίκτυα που μπορεί να έχετε ακούσει, όπως το Napster και το Pirate Bay, αποτελούν ένα διαδικτυακό ευρετήριο δεδομένων. Τα μεμονωμένα αρχεία διαμοιράζονται από συγκεκριμένους κόμβους του δικτύου. Αυτό επιτρέπει τον διαμοιρασμό μεγάλων αρχείων. Ωστόσο, επειδή τα δεδομένα που μπορεί να σας ενδιαφέρουν δεν είναι διαθέσιμα σε όλους τους συμμετέχοντες στο δίκτυο, η απόκτηση των δεδομένων που σας ενδιαφέρουν είναι προβληματική. Είναι επίσης δύσκολο να γνωρίζετε αν τα δεδομένα που κατεβάζετε είναι άθικτα και δεν έχουν καταστραφεί ή και/και δεν περιέχουν πληροφορίες που δεν θέλετε, όπως π.χ. έναν ιό.

Ο τρόπος με τον οποίο το Bitcoin συντονίζει την οργάνωση και την εισαγωγή νέων δεδομένων περιλαμβάνει τρία βασικά στοιχεία:

1. **Block**: Κατάλογος των συναλλαγών που καταγράφονται σε ένα λογιστικό βιβλίο κατά τη διάρκεια μιας δεδομένης περιόδου. Το μέγεθος, η περίοδος και το γεγονός ενεργοποίησης των μπλοκ είναι διαφορετικά για κάθε αλυσίδα μπλοκ.

Δεν είναι σε όλες τις αλυσίδες μπλοκ η καταγραφή και η διασφάλιση ενός αρχείου της κίνησης του κρυπτονομίσματος ως πρωταρχικός στόχος τους. Αλλά όλες οι αλυσίδες μπλοκ καταγράφουν την κίνηση του κρυπτονομίσματος ή του συμβόλου τους. Σκεφτείτε ότι η συναλλαγή είναι απλώς η καταγραφή δεδομένων. Η απόδοση μιας αξίας σε αυτά (όπως συμβαίνει σε μια χρηματοοικονομική συναλλαγή) χρησιμοποιείται για να ερμηνεύσει τι σημαίνουν αυτά τα δεδομένα.

2. **Chain**: Ένας κατακερματισμός που συνδέει ένα μπλοκ με ένα άλλο, "αλυσοδένοντάς" τα μαθηματικά μεταξύ τους. Αυτή είναι μία από τις πιο δύσκολες έννοιες στην αλυσίδα μπλοκ για να κατανοηθεί. Είναι επίσης η μαγεία που συγκολλάει τις αλυσίδες μπλοκ μεταξύ τους και τους επιτρέπει να δημιουργούν μαθηματική εμπιστοσύνη.

Ο κατακερματισμός στο blockchain δημιουργείται από τα δεδομένα που υπήρχαν στο προηγούμενο μπλοκ. Το hash είναι ένα δακτυλικό αποτύπωμα αυτών των δεδομένων και κλειδώνει τα μπλοκ κατά σειρά και χρόνο".

Αν και οι αλυσίδες μπλοκ είναι μια σχετικά νέα καινοτομία, το hashing δεν είναι. Το hashing εφευρέθηκε πριν από 30 χρόνια. Αυτή η παλιά καινοτομία χρησιμοποιείται επειδή δημιουργεί μια μονόδρομη συνάρτηση που δεν μπορεί να αποκρυπτογραφηθεί. Μια συνάρτηση κατακερματισμού δημιουργεί έναν μαθηματικό αλγόριθμο που αντιστοιχίζει δεδομένα οποιουδήποτε μεγέθους σε μια συμβολοσειρά bit σταθερού μεγέθους. Μια συμβολοσειρά bit έχει συνήθως μήκος 32 χαρακτήρων, η οποία στη συνέχεια αντιπροσωπεύει τα δεδομένα που κατακερματιστήκαν. Ο αλγόριθμος ασφαλούς κατακερματισμού (SHA) είναι μία από ορισμένες κρυπτογραφικές συναρτήσεις κατακερματισμού που χρησιμοποιούνται στις αλυσίδες μπλοκ. Ο SHA-256 είναι ένας κοινός αλγόριθμος που παράγει έναν σχεδόν μοναδικό, σταθερού μεγέθους κατακερματισμό 256 bit (32 byte). Για πρακτικούς σκοπούς, σκεφτείτε ένα hash" "ως ένα

ψηφιακό δακτυλικό αποτύπωμα των δεδομένων που χρησιμοποιείται για να τα κλειδώσει στη θέση τους μέσα στην αλυσίδα μπλοκ".

3. **Δίκτυο**: Το δίκτυο αποτελείται από "πλήρεις κόμβους". Σκεφτείτε τους ως τον υπολογιστή που εκτελεί έναν αλγόριθμο που διασφαλίζει το δίκτυο. Κάθε κόμβος περιέχει ένα πλήρες αρχείο όλων των συναλλαγών που καταγράφηκαν ποτέ στο συγκεκριμένο blockchain.

Οι κόμβοι βρίσκονται σε όλο τον κόσμο και μπορούν να λειτουργούν από οποιονδήποτε. Είναι δύσκολο, ακριβό και χρονοβόρο να λειτουργήσει κάποιος έναν πλήρη κόμβο, γι' αυτό και οι άνθρωποι δεν το κάνουν δωρεάν. Έχουν κίνητρο να λειτουργήσουν έναν κόμβο επειδή θέλουν να κερδίσουν κρυπτονόμισμα. Ο υποκείμενος αλγόριθμος της αλυσίδας μπλοκ τους ανταμείβει για τις υπηρεσίες τους. Η ανταμοιβή είναι συνήθως ένα token ή ένα κρυπτονόμισμα, όπως το Bitcoin".

2.2 Κύριες εφαρμογές Blockchain & εξέλιξη

Οι εφαρμογές blockchain βασίζονται στην ιδέα ότι το δίκτυο είναι ο διαιτητής. Αυτός ο τύπος συστήματος είναι ένα ασυγχώρητο και τυφλό περιβάλλον. Ο κώδικας του υπολογιστή γίνεται νόμος και οι κανόνες εκτελούνται όπως γράφτηκαν και ερμηνεύτηκαν από το δίκτυο. Οι υπολογιστές δεν έχουν τις ίδιες κοινωνικές προκαταλήψεις και συμπεριφορές με τους ανθρώπους.

Το δίκτυο δεν μπορεί να ερμηνεύσει την πρόθεση (τουλάχιστον όχι ακόμη). Τα ασφαλιστήρια συμβόλαια που διαιτητεύονται σε μια αλυσίδα μπλοκ έχουν διερευνηθεί σε μεγάλο βαθμό ως περίπτωση χρήσης που βασίζεται σε αυτή την ιδέα.

Ένα άλλο ενδιαφέρον πράγμα που επιτρέπουν οι αλυσίδες μπλοκ είναι η άψογη τήρηση αρχείων. Μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός σαφούς χρονοδιαγράμματος για το ποιος έκανε τι και πότε. Πολλές βιομηχανίες και ρυθμιστικοί φορείς ξοδεύουν αμέτρητες ώρες προσπαθώντας να αξιολογήσουν αυτό το πρόβλημα. Η τήρηση αρχείων με δυνατότητα blockchain θα απαλλάξει από κάποια από τα βάρη που δημιουργούνται όταν προσπαθούμε να ερμηνεύσουμε το παρελθόν.

Ο κύκλος ζωής του Blockchain

Οι αλυσίδες μπλοκ προέκυψαν με τη δημιουργία του Bitcoin. Απέδειξε ότι μια ομάδα ατόμων που δεν είχαν συναντηθεί ποτέ μπορούσε να λειτουργήσει διαδικτυακά μέσα σε ένα σύστημα που ήταν απευαισθητοποιημένο στην εξαπάτηση άλλων που συνεργάζονταν στο δίκτυο.

Το αρχικό δίκτυο Bitcoin δημιουργήθηκε για να εξασφαλίσει το κρυπτονόμισμα Bitcoin. Διαθέτει περίπου 5.000 πλήρεις κόμβους και είναι κατανεμημένο σε παγκόσμιο επίπεδο. Χρησιμοποιείται κυρίως για την εμπορία Bitcoin και την ανταλλαγή αξίας, αλλά η κοινότητα είδε τη δυνατότητα να κάνει πολύ περισσότερα με το δίκτυο. Λόγω του μεγέθους του και της δοκιμασμένης στο χρόνο ασφάλειας, χρησιμοποιείται επίσης για την ασφάλεια άλλων μικρότερων αλυσίδων μπλοκ και εφαρμογών blockchain.

Το δίκτυο Ethereum είναι μια δεύτερη εξέλιξη της έννοιας της αλυσίδας μπλοκ. Παίρνει την παραδοσιακή δομή του blockchain και προσθέτει αρκετές νέες γλώσσες προγραμματισμού που είναι ενσωματωμένες στο εσωτερικό του. Όπως και το Bitcoin, διαθέτει πάνω από 10.000 πλήρεις κόμβους και είναι παγκοσμίως κατανεμημένο. Το Ethereum χρησιμοποιείται κυρίως για το εμπόριο Ether και τη δημιουργία έξυπνων συμβάσεων. Το πιο δημοφιλές έξυπνο συμβόλαιο του Ethereum είναι το ERC 20. Επιτρέπει τη δημιουργία ανταλλάξιμων μάρκων. Αυτά τα tokens μπορούν να χρησιμοποιηθούν για σκοπούς συγκέντρωσης κεφαλαίων.

Υπάρχει μια τρίτη εξέλιξη στην τεχνολογία blockchain που βρίσκεται υπό ενεργή ανάπτυξη και αντιμετωπίζει τους περιορισμούς της ταχύτητας και του μεγέθους των δεδομένων. Η διόρθωση αυτών των ζητημάτων θα επιτρέψει στην τεχνολογία blockchain να χρησιμοποιηθεί πιο "ρεαλιστικά με mainstream εφαρμογές. Θα χρειαστούν αρκετά χρόνια προτού καταστεί σαφές ποια δομή θα επικρατήσει.

Οι δημοφιλείς νέες εξελίξεις περιλαμβάνουν το sharding, ένα είδος διαμερισμού βάσεων δεδομένων που διαχωρίζει μεγάλες βάσεις δεδομένων σε μικρότερα τμήματα που ονομάζονται data shards. Μια αναπτυξιακή προσπάθεια του Ethereum που ονομάζεται fork choice rule χωρίζει την αλυσίδα μπλοκ του Ethereum σε διάφορα παράλληλα δίκτυα. Μπορεί να επιτρέψει στο Ethereum να κλιμακωθεί πιο αποτελεσματικά και να μειώσει τη συμφόρηση στο δίκτυο, αυξάνοντας τις ταχύτητες των συναλλαγών και μειώνοντας το κόστος των συναλλαγών.

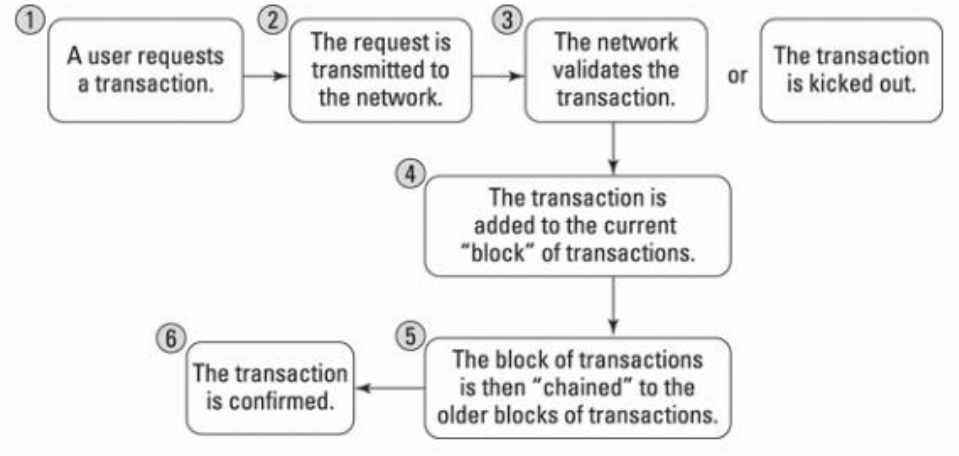
Μια άλλη δημοφιλής θεωρία κλιμάκωσης ονομάζεται POS. Σε γενικές γραμμές, το POS είναι η έννοια της τοποθέτησης tokens ή κρυπτονομισμάτων ως εγγύηση για την επεξεργασία των συναλλαγών. Εάν ο κόμβος είναι διεφθαρμένος και δεν επεξεργάζεται τις συναλλαγές με ακρίβεια, ο κόμβος μπορεί να χάσει τα token ή το κρυπτονόμισμα.

Μια τρίτη προσπάθεια για την κλιμάκωση της τεχνολογίας blockchain χρησιμοποιεί αξιόπιστους κόμβους. Για παράδειγμα, το δίκτυο Factom λειτουργεί με ομοσπονδιακούς κόμβους και απεριόριστο αριθμό κόμβων ελέγχου. Αυτοί οι κόμβοι είναι έμπιστοι με τη διασφάλιση του συστήματος. Το εκλεγμένο δίκτυο της Factom είναι μικρό, μόλις πάνω από 60 κόμβους. Για να αντισταθμίσει τους κινδύνους ασφαλείας, το Factom αγκυρώνεται σε άλλα κατανεμημένα δίκτυα για να στηριχθεί στην ασφάλεια πιο εκτεταμένων συστημάτων. Το Factom χωρίζει επίσης το δίκτυό του σε μικρότερα, ταχύτερα και ευκολότερα διαχειρίσιμα μέρη που ονομάζονται αλυσίδες. Το Factom έχει ταχύτερες ταχύτητες συναλλαγών και χαμηλότερο κόστος συναλλαγών από τις αλυσίδες μπλοκ POW.

Συναίνεση: Blockchains

Οι αλυσίδες μπλοκ είναι ισχυρά εργαλεία επειδή δημιουργούν έντιμα συστήματα που αυτοδιορθώνονται χωρίς την ανάγκη ενός τρίτου μέρους να επιβάλλει τους κανόνες. Επιτυγχάνουν την επιβολή των κανόνων μέσω του αλγορίθμου συναίνεσής τους.

Στον κόσμο της αλυσίδας μπλοκ, η συναίνεση είναι η διαδικασία ανάπτυξης μιας συμφωνίας μεταξύ μιας ομάδας κοινώς δυσπιστούντων μετόχων. Αυτοί είναι οι πλήρεις κόμβοι του δικτύου. Οι πλήρεις κόμβοι επικυρώνουν τις συναλλαγές που εισάγονται στο δίκτυο για να καταγραφούν ως μέρος του λογιστικού βιβλίου.



Κάθε αλυσίδα μπλοκ έχει τους δικούς της αλγορίθμους για τη δημιουργία συμφωνίας στο δίκτυό της σχετικά με τις εγγραφές που προστίθενται. Υπάρχουν πολλά διαφορετικά μοντέλα για τη δημιουργία συναίνεσης επειδή κάθε blockchain δημιουργεί διαφορετικά είδη καταχωρήσεων. Ορισμένες αλυσίδες μπλοκ ανταλλάσσουν αξίες, άλλες αποθηκεύουν δεδομένα και άλλες διασφαλίζουν συστήματα και συμβάσεις.

Το Bitcoin, για παράδειγμα, εμπορεύεται την αξία του token του μεταξύ των μελών του δικτύου του. Τα token έχουν αγοραία αξία, οπότε οι απαιτήσεις που σχετίζονται με τις επιδόσεις, την επεκτασιμότητα, τη συνέπεια, το μοντέλο απειλών και το μοντέλο αποτυχίας θα είναι υψηλότερες. Το Bitcoin λειτουργεί με την υπόθεση ότι ένας κακόβουλος επιτιθέμενος μπορεί να θέλει να αλλοιώσει το ιστορικό των συναλλαγών προκειμένου να κλέψει μάρκες. Το Bitcoin αποτρέπει αυτό το ενδεχόμενο χρησιμοποιώντας ένα μοντέλο συναίνεσης που ονομάζεται "απόδειξη εργασίας", το οποίο επιλύει το πρόβλημα του βυζαντινού γενικού: "Πώς ξέρετε ότι οι πληροφορίες που εξετάζετε δεν έχουν αλλάξει εσωτερικά ή εξωτερικά;". Επειδή η αλλαγή ή η χειραγώγηση των δεδομένων είναι σχεδόν πάντα δυνατή, η αξιοπιστία των δεδομένων αποτελεί μεγάλο πρόβλημα για την επιστήμη των υπολογιστών.

Οι περισσότερες αλυσίδες μπλοκ λειτουργούν υπό την προϋπόθεση ότι θα δεχθούν επιθέσεις από εξωτερικές δυνάμεις ή από τους χρήστες του συστήματος. Η αναμενόμενη

απειλή και ο βαθμός εμπιστοσύνης που έχει το δίκτυο στους κόμβους που διαχειρίζονται την αλυσίδα μπλοκ θα καθορίσουν τον τύπο του αλγορίθμου συναίνεσης που χρησιμοποιούν για τη διευθέτηση του βιβλίου τους. Για παράδειγμα, το Bitcoin και το Ethereum αναμένουν πολύ υψηλό βαθμό απειλής και χρησιμοποιούν έναν ισχυρό αλγόριθμο συναίνεσης που ονομάζεται απόδειξη εργασίας. Δεν υπάρχει εμπιστοσύνη στο δίκτυο.

Στο άλλο άκρο του φάσματος, οι αλυσίδες μπλοκ που χρησιμοποιούνται για την καταγραφή οικονομικών συναλλαγών μεταξύ γνωστών μερών μπορούν να χρησιμοποιήσουν μια πιο ελαφριά και ταχύτερη συναίνεση. Η ανάγκη τους για συναλλαγές υψηλής ταχύτητας είναι πιο σημαντική. Η απόδειξη εργασίας είναι πολύ αργή και δαπανηρή για τη λειτουργία τους λόγω των συγκριτικά λίγων συμμετεχόντων στο δίκτυο και της ανάγκης άμεσης οριστικοποίησης κάθε συναλλαγής. Επίσης, δεν χρειάζονται ένα συμβολικό ή κρυπτονόμισμα για να δώσουν κίνητρα για την επεξεργασία των συναλλαγών. Έτσι, εξαλείφουν αυτά τα πράγματα από το σύστημά τους και λειτουργούν ταχύτερα και φθηνότερα από τα συστήματα POW".

Ποια από τα προβλήματα θα μπορούσε να αντιμετωπίσει;

2.3 Άλλες χρησιμοποιούμενες αλυσίδες μπλοκ

Σήμερα υπάρχουν χιλιάδες αλυσίδες μπλοκ και εφαρμογές αλυσίδας μπλοκ. Όλος ο κόσμος έχει παθιαστεί με τις ιδέες της ταχύτερης διακίνησης χρημάτων, της ενσωμάτωσης και της διακυβέρνησης σε ένα κατανεμημένο δίκτυο και της δημιουργίας ασφαλών εφαρμογών και υλικού.

Μπορείτε να δείτε πολλές από αυτές τις δημόσιες αλυσίδες μπλοκ πηγαίνοντας σε ένα ανταλλακτήριο κρυπτονομισμάτων.

Το παρακάτω σχήμα δείχνει το ανταλλακτήριο altcoin για την Poloniex (https://poloniex.com), μια πλατφόρμα συναλλαγών κρυπτονομισμάτων".

Οι αλυσίδες μπλοκ κινούνται πέρα από την αγορά εμπορικών αξιών και ενσωματώνονται σε όλα τα είδη των βιομηχανιών. Οι αλυσίδες μπλοκ προσθέτουν ένα νέο επίπεδο εμπιστοσύνης που καθιστά πλέον την εργασία στο διαδίκτυο ασφαλή με τρόπο που δεν ήταν εφικτός προηγουμένως.

Τρέχουσες χρήσεις blockchain

Οι περισσότερες ανερχόμενες εφαρμογές blockchain περιστρέφονται γύρω από τη διακίνηση χρημάτων ή άλλων μορφών αξίας γρήγορα και φθηνά. Αυτό περιλαμβάνει τη διαπραγμάτευση μετοχών δημόσιας εταιρείας, την πληρωμή εργαζομένων σε άλλες χώρες και την ανταλλαγή ενός νομίσματος με ένα άλλο.

Οι αλυσίδες μπλοκ χρησιμοποιούνται επίσης πλέον ως μέρος μιας στοίβας ασφάλειας λογισμικού. Το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ διερευνά λογισμικό blockchain που διασφαλίζει συσκευές του Διαδικτύου των Πραγμάτων (IoT). Ο κόσμος του IoT έχει μερικά από τα περισσότερα να κερδίσει από αυτή την καινοτομία, επειδή είναι ιδιαίτερα ευάλωτος στην παραποίηση και σε άλλες μορφές πειρατείας. Οι συσκευές IoT έχουν επίσης γίνει πιο διαδεδομένες και η ασφάλεια έχει γίνει πιο εξαρτημένη από αυτές. Τα νοσοκομειακά συστήματα, τα αυτοοδηγούμενα αυτοκίνητα και τα συστήματα ασφαλείας αποτελούν κορυφαία παραδείγματα.

Οι αρχικές προσφορές νομισμάτων (ICOs) είναι μια άλλη συναρπαστική καινοτομία blockchain. Πρόκειται για ένα είδος έξυπνης σύμβασης που επιτρέπει στον εκδότη να προσφέρει ένα token σε αντάλλαγμα για επενδυτικά κεφάλαια. Συχνά χρησιμοποιούνται ως επιλογή άντλησης κεφαλαίων που δεν επιφέρει διαλυτικά κέρδη, οι επιχειρηματίες σε παγκόσμιο επίπεδο έχουν συγκεντρώσει δισεκατομμύρια δολάρια. Οι κυβερνήσεις και οι ρυθμιστικές αρχές έσπευσαν να πατάξουν τις ICO. Τα κουπόνια μπορεί να είναι μη αδειοδοτημένοι τίτλοι και η προσφορά μπορεί να εξαπατά τους επενδυτές. Η τεχνολογία είναι εντυπωσιακή, ακόμη και αν τα ζητήματα συμμόρφωσης εξακολουθούν να αντιμετωπίζονται.

Μία από τις φανταστικές καινοτομίες που ενυπάρχουν στα μάρκες ICO είναι ότι είναι ένα μέσο αυτοεκκαθάρισης και αυτοδιακανονισμού. Στο σημερινό μας σύστημα διαπραγμάτευσης τίτλων, υπάρχουν δύο τύποι οργανισμών εκκαθάρισης: οι εταιρείες εκκαθάρισης και τα αποθετήρια. Οι εταιρείες εκκαθάρισης ελέγχουν τις συναλλαγές και ενεργούν ως μεσάζοντες στην πραγματοποίηση διακανονισμών. Οι θεματοφύλακες κατέχουν πιστοποιητικά τίτλων και διατηρούν αρχεία ιδιοκτησίας των τίτλων. Οι αλυσίδες μπλοκ εκτελούν και τις δύο αυτές λειτουργίες για τα μάρκες χωρίς να χρειάζονται τρίτους για τον έλεγχο και τη διατήρηση της κατοχής των περιουσιακών στοιχείων

.Μελλοντικές εφαρμογές blockchain

Τα μεγαλύτερα και πιο μακροπρόθεσμα έργα blockchain που διερευνώνται τώρα περιλαμβάνουν κυβερνητικά υποστηριζόμενα συστήματα κτηματολογίου, ταυτότητας και εφαρμογές διεθνούς ταξιδιωτικής ασφάλειας.

Οι δυνατότητες ενός μέλλοντος εμπλουτισμένου με blockchain έχουν εξάψει τη φαντασία επιχειρηματιών, κυβερνήσεων, πολιτικών ομάδων και ανθρωπιστών σε όλο τον κόσμο. Χώρες όπως το Ηνωμένο Βασίλειο, η Σιγκαπούρη και τα Ηνωμένα Αραβικά Εμιράτα το βλέπουν ως έναν τρόπο για τη μείωση του κόστους, τη δημιουργία νέων χρηματοπιστωτικών μέσων και την τήρηση καθαρών αρχείων. Έχουν ενεργές επενδύσεις και πρωτοβουλίες που διερευνούν το blockchain.

Οι αλυσίδες μπλοκ έχουν θέσει τα θεμέλια όπου η ανάγκη για εμπιστοσύνη έχει αφαιρεθεί από την εξίσωση. Εκεί που πριν το να ζητάς "εμπιστοσύνη" ήταν μεγάλη υπόθεση, με τις αλυσίδες μπλοκ είναι μικρή υπόθεση. Επίσης, η υποδομή που επιβάλλει τον κανόνα εάν αυτή η εμπιστοσύνη παραβιαστεί μπορεί να είναι ελαφρύτερη. Μεγάλο μέρος της κοινωνίας βασίζεται στην εμπιστοσύνη και την επιβολή των κανόνων. Οι κοινωνικές και οικονομικές επιπτώσεις των εφαρμογών blockchain μπορεί να είναι

συναισθηματικά και πολιτικά πολωτικές, επειδή το blockchain θα αλλάξει τον τρόπο με τον οποίο δομούμε τις συναλλαγές με βάση τις αξίες και την κοινωνία.