Πολυτεχνειο Κρητης

Σχολη Μηχανικων Παραγωγης και Διοικησης

Η Συνεισφορά των Κρυπτονομισμάτων στη Λειτουργία της Εφοδιαστικής Αλυσίδας και ο Ρόλος των Έξυπνων Συμβολαίων

Αριστείδης Ε. Σκουλάκης

Εξεταστική Επιτροπή

Βασίλης Σ. Μουστάκης, Καθηγητής (ΜΠΔ)

Γεώργιος Ε. Σταυρουλάκης, Καθηγητής (ΜΠΔ)

Μαρία Μπακατσάκη, ΕΔΙΠ (ΜΠΔ)

Χανιά, Μάιος 2019

Abstract

Nowadays Cryptocurrencies are a rapidly evolving field that attracts the interest of many people. These are virtual coins that use some form of encryption. The most famous of these coins is 'Bitcoin'. Cryptocurrencies can make a significant contribution to the role of the Supply Chain.

The Supply Chain (SC) is, in principle, defined as an integrated network or value creation system, including closely associated business units, producers, traders, retailers and consumers. SC therefore includes the flow of materials from the raw material supplier or the producer of the final product to the final consumer alongside the flow of information between the chain members. Using Cryptocurrencies, any difficulties in its operation can be eliminated, as in the form of encryption - digital form of money, the payment system at each stage can be implemented much more easily and selflessly.

Smart contracts are also primarily used in the Cryptographic Networks. Smart contracts use cryptographic code to impose a relationship between two parties. These parties should not be individuals or institutions. The relationship imposed by a smart contract can be between an application and a network. In fact, smart contracts are self-control commands that can be programmed to be triggered under specific circumstances. This function is a major object of study as it enters the market and can change it.

In this thesis, the contribution of Cryptocurrencies in the Supply Chain and in particular its function on it is analyzed. The role of Smart Contracts in the Cryptographic Network will also be studied.

Περίληψη

Στις μέρες μας, τα Κρυπτονομίσματα (Cryptocurrencies) αποτελούν ένα ραγδαία εξελισσόμενο τομέα, που ελκύει το ενδιαφέρον πολλών ανθρώπων ανά την υφήλιο. Πρόκειται για εικονικά νομίσματα, που χρησιμοποιούν κάποια μορφή κρυπτογράφησης. Το πιο διαδεδομένο από αυτά τα νομίσματα είναι το Bitcoin. Τα Κρυπτονομίσματα μπορούν να συνεισφέρουν σημαντικά στο ρόλο της Εφοδιαστικής Αλυσίδας.

Η Εφοδιαστική Αλυσίδα (ΕΑ) ορίζεται καταρχήν, σαν ένα ολοκληρωμένο δίκτυο ή ένα σύστημα δημιουργίας αξίας, που περιλαμβάνει στενά συνεργαζόμενες επιχειρηματικές μονάδες, παραγωγούς, εμπόρους, λιανοπωλητές αλλά και τους καταναλωτές. Η Εφοδιαστική Αλυσίδα λοιπόν, συμπεριλαμβάνει τη ροή των υλικών από τον προμηθευτή των πρώτων υλών ή τον παραγωγό του προϊόντος μέχρι τον τελικό καταναλωτή, παράλληλα με τη ροή των πληροφοριών μεταξύ των μελών της αλυσίδας. Χρησιμοποιώντας τα Κρυπτονομίσματα, μπορούν να εξαλειφθούν οποιεσδήποτε δυσκολίες στην λειτουργία της αλυσίδας, καθώς με τα κρυπτονομίσματα, το σύστημα πληρωμών σε κάθε στάδιο του μπορεί και υλοποιείται πολύ πιο εύκολα, πιο γρήγορα και ανιδιοτελώς.

Τα έξυπνα συμβόλαια χρησιμοποιούνται επίσης κατά κύριο λόγο στη λειτουργία του δικτύου των Κρυπτονομισμάτων. Οι έξυπνες συμβάσεις χρησιμοποιούν κρυπτογραφικό κώδικα για την επιβολή μιας σχέσης μεταξύ δύο μερών. Αυτά τα μέρη δεν χρειάζεται να είναι ούτε ιδιώτες, ούτε ιδρύματα. Η σχέση που επιβάλλεται από μια έξυπνη σύμβαση μπορεί να είναι μεταξύ μιας εφαρμογής και ενός δικτύου. Ουσιαστικά, οι έξυπνες συμβάσεις είναι εντολές ή καταστάσεις αυτοελέγχου που μπορούν να προγραμματιστούν και να ενεργοποιηθούν υπό συγκεκριμένες συνθήκες. Αυτή η λειτουργία αποτελεί μείζον αντικείμενο μελέτης, καθώς η τεχνολογία αυτή εισέρχεται ταχύτατα στην αγορά και μπορεί να την αλλάξει άρδην.

Στην παρούσα διπλωματική εργασία, θα αναλυθεί η συνεισφορά των Κρυπτονομισμάτων στην Εφοδιαστική Αλυσίδα και συγκεκριμένα η λειτουργία τους πάνω σε αυτήν. Επίσης, θα μελετηθεί ο ρόλος των Έξυπνων Συμβολαίων στο δίκτυο των Κρυπτονομισμάτων.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Τα "χρήματα" έχουν τρία βασικά χαρακτηριστικά: αποτελούν ένα αποθηκευτικό μέσο αξίας, μια λογιστική μονάδα και ένα μέσο ανταλλαγής - αν και το χρήμα δεν είναι υποχρεωτικό να αποτελεί νόμιμη μονάδα. Εκ πρώτης όψεως τα κρυπτονομίσματα μπορεί να θεωρηθεί ότι πληρούν όλα τα χαρακτηριστικά του χρήματος, όπως ορίστηκαν παραπάνω. Αποτελούν μια πιθανή αποθήκη αξίας, αν και πολύ ασταθή. Θα μπορούσαν να χρησιμοποιηθούν ως λογιστική μονάδα και με την πρώτη γνωστή μορφή τους - το Bitcoin, μπορούν να χρησιμοποιηθούν ως μέσο ανταλλαγής για όποιον επιθυμεί να τα αποδεχθεί. Σε αυτό τον τελευταίο ρόλο, έχουν σημαντικά πλεονεκτήματα, δεδομένου ότι μπορούν να χωριστούν ψηφιακά για κάθε μέγεθος συναλλαγής και να αποφεύγουν τα υψηλά τέλη που χρεώνονται από εταιρείες πιστωτικών καρτών. Αλλά είναι πιθανό ότι ο κύριος λόγος που τα κρυπτονομίσματα "απογειώνονται" σε δημοτικότητα ως μέσο πληρωμής, οφείλεται στην δυνατότητα της ανωνυμίας. Ο υψηλός βαθμός ανωνυμίας, αποτελεί χαρακτηριστικό με μεγάλα πλεονεκτήματα για παράνομες δραστηριότητες, όπως το ξέπλυμα χρήματος, η αποφυγή των δημοσιονομικών κανονισμών, η χρηματοδότηση της τρομοκρατίας και η φοροδιαφυγή.

Η οικονομική κρίση οδήγησε σε απώλεια εμπιστοσύνης σε πολλούς ενδιάμεσους χρηματοπιστωτικούς οργανισμούς, πλατφόρμες συναλλαγών και συστήματα πληρωμών. Η βασική καινοτομία στην οποία βασίστηκαν τα κρυπτονομίσματα είναι το χαρακτηριστικό των συναλλαγών που δεν βασίζονται στην εμπιστοσύνη (η δυνατότητα να αποφευχθεί η ανάγκη για ένα έμπιστο τρίτο μέρος). Η ανταλλαγή είναι πάντα δυνατή ; για παράδειγμα οι υαλοκαθαριστές μπορούν να διαπραγματευτούν με τα καταστήματα και τα ιατρεία για την ανταλλαγή ωρών καθαρισμού με αγαθά και υπηρεσίες. Ωστόσο, η ανταλλαγή είναι ένα φτωχό μέσο σε μια υπηρεσία, όπως ο καθαρισμός, δεν μπορεί να αποθηκευτεί επιτυχώς (και ως εκ τούτου

Εικόνα 1.1: Διαφορετικά κρυπτονομίσματα που κυκλοφορούν στην αγορά. https://medium.com/@jimmysong/why-bitcoin-is-different-than-other-cryptocurrencies-e16b17d48b94 (10/3/2019)

δεν υπάρχει αποθήκευση της αξίας). Μάρκες καζίνο, αεροπορικά μίλια, πιστώσεις Paypal, χρήματα λούνα πάρκ, θα μπορούσαν επίσης να χρησιμοποιηθούν για ορισμένες λειτουργίες εκτός της πρωτογενούς σκοπούμενης χρήσης τους, αλλά όχι με τα πιθανά χαρακτηριστικά ευχρηστίας των κρυπτονομισμάτων στην ψηφιακή εποχή.

Από την άλλη πλευρά, τα κρυπτονομίσματα δεν μπορούν να αποτελέσουν μια εναλλακτική λύση για το νόμιμο νόμισμα, για τον απλό λόγο, ότι οι άνθρωποι πρέπει να πληρώνουν τους φόρους τους. Αυτό προστατεύει τα υπάρχοντα νομίσματα από αντικατάσταση, και ο φόβος της απώλειας του νομισματικού ελέγχου δεν θα πρέπει να χρησιμοποιείται ως επιχείρημα για την πρόληψη της κυκλοφορίας των Bitcoins, ως παράλληλα νομίσματα. Ωστόσο, η τεχνολογία των ψηφιακών πρωτοκόλλων πληρωμών δεν θα πρέπει να συγχέεται με το θέμα "παράλληλο νόμισμα". Όσον αφορά τη λειτουργία του νομίσματος, υπάρχουν δύο πιθανά ζητήματα πολιτικής: (α) θέματα προστασίας των καταναλωτών: π.χ. ηλεκτρονική κλοπή, ή η κατάρρευση της αξίας των κρυπτονομισμάτων, για παράδειγμα λόγω της εμφάνισης των υποκατάστατων, η χρήση της εξουσίας της κυβέρνησης για την απαγόρευσή τους, κλπ .και (β) τα χαρακτηριστικά της ανωνυμίας που επιτρέπει την επέκταση των παράνομων δραστηριοτήτων, όπως η φοροδιαφυγή και το ξέπλυμα χρήματος. Η ψηφιακή τεχνολογία μεταφοράς, από την άλλη πλευρά, θα μπορούσε να παίξει κοινωνικά χρήσιμους ρόλους.

Όσον αφορά το Bitcoin, οι ιδρυτές του παρείχαν στην αγορά αλγορίθμους για την πρόωρη εξόρυξη (mining) και έχουν συγκεντρώσει το πρώτο απόθεμα Bitcoins. Οι κάτοχοι των αποθεμάτων αυτών επωφελήθηκαν από τις μεταγενέστερες αυξήσεις των τιμών. Με τη χρήση ηλεκτρονικών υπολογιστών και εντατικά αναλαμβάνοντας το υψηλό κόστος ηλεκτρικής

ενέργειας, εν συνεχεία οι συμμετέχοντες μπορούσαν να εξορύξουν Bitcoins, εκ των οποίων συνολικά 21 εκατομμύρια είναι ο σταθερός τους αριθμός. Η συνάρτηση προσφοράς για τα νομίσματα απλώνεται με τη μείωση του μεγέθους του μπλοκ και μέσω ενός αλγόριθμου με τον οποίο η εύρεση τους γίνεται πολύ πιο δύσκολη, αν βρίσκονται πολύ γρήγορα. Μπορεί να πάρει πολλά χρόνια για να γίνει εξόρυξη όλων των Bitcoin. Οι συναλλαγές με Bitcoins γίνονται στην ονλινε αγορά και ο καθένας μπορεί να τα αγοράσει στη συναλλαγματική ισοτιμία με το δολάριο από τις πλατφόρμες αγορες Bitcoin (όπως η Coinbase), αν και η τιμή έχει αποδειχθεί ότι είναι πολύ ασταθής μέχρι σήμερα.

Η ψηφιακή τεχνολογία μεταφοράς είναι πολύ ενδιαφέρουσα. Υπάρχει ένα open source κλειδί κρυπτογραφιας, ένα δημόσιο και ένα ιδιωτικό. Οι συναλλαγές μεταβιβάζουν την κυριότητα του νομίσματος από τη μια δημόσια διεύθυνση στην άλλη, αλλά απαιτείται ένα ιδιωτικό κλειδί για την αποκρυπτογράφηση των Bitcoins και την περαιτέρω κατανάλωση τους. Τα δημόσια και τα ιδιωτικά κλειδιά είναι αλφαριθμητικές ακολουθίες που βασίζονται σε εξελιγμένη κρυπτογράφηση: Οι τυχαίοι αριθμοί και τα γράμματα στα δημόσια κλειδιά προέρχονται από την εφαρμογή της συνάρτησης "hash". Η ταυτοποίηση είναι σαν τη λήψη δακτυλικών αποτυπωμάτων - μπορεί να υπάρχει μόνο μία γεννήτρια μεταβίβασης από μια δεδομένη διεύθυνση (αν και φυσικά η αποθήκευση ιδιωτικών ακολουθιών ταυτοποίησης σε απευθείας σύνδεση ανοίγει το δρόμο για την κλοπή και την απάτη, όπως σε όλα τα ζητήματα, όπου εμπλέκονται με τα χρήματα και το διαδίκτυο). Τα Bitcoins με τη μορφή των δημόσιων κλειδιών αποθηκεύονται σε "πορτοφόλια", στο σκληρό δίσκο του υπολογιστή και μπορούν να προσπελαστούν μόνο με το ιδιωτικό κλειδί. Η ασφάλεια από hacking αυξάνεται με την χρήση της off-line ψυχρής αποθήκευσης, και οι υπηρεσίες αυτές παρέχονται από τις πλατφόρμες συναλλαγών. Τα πορτοφόλια που αποθηκεύονται με σύνδεση στο Διαδίκτυο, ή συνδέονται με μια εφαρμογή smartphone, είναι παρόμοια με τα μετρητά, και τα Bitcoins μπορούν να μετακινηθούν από την ψυχρή αποθήκευση στα κινητά πορτοφόλια, όταν απαιτείται.

Οι συναλλαγές καταγράφονται στην "αλυσίδα μπλοκ", η οποία είναι το κλειδί για την καινοτομία στην τεχνολογία αυτή - δηλαδή, μια τεχνολογία που εξαλείφει την ανάγκη για ένα έμπιστο τρίτο μέρος και ενδιάμεσες δαπάνες που συνδέονται με τα εν λόγω ιδρύματα (τράπεζες, εταιρείες πιστωτικών καρτών, εταιρείες πληρωμής, μη τραπεζικούς χρηματοπιστωτικούς διαμεσολαβητές).

Η αλυσίδα μπλοκ είναι μια δημόσια βάση δεδομένων (γιγάντιο καθολικό βιβλίο), που συντηρείται ανοιχτά από τους υπολογιστές σε όλο τον κόσμο - είναι μια διαδοχική καταγραφή όλων των συναλλαγών και της τρέχουσας ιδιοκτησίας. Αυτή η παρακολούθηση και ο έλεγχος των συναλλαγών υποστηρίζονται από την αποκεντρωμένη υπολογιστική ισχύ που

παράγεται από τη δραστηριότητα της «εξόρυξης», και αυτή η δραστηριότητα ανταμείβεται σε Bitcoin. Η αλυσίδα των μπλοκ επιτρέπει στους συμμετέχοντες να ελέγξουν κατά πόσον οι διαβιβάσεις νομισμάτων προέρχονται από τους πραγματικούς τους ιδιοκτήτες και αποφεύγει προβλήματα όπως οι διπλές δαπάνες. Το ίδιο κλάσμα Bitcoin δεν μπορεί να σταλεί πάνω από μία φορά. Αυτή η τεχνολογία του Bitcoin έχει γεννήσει μια ταχέως αναπτυσσόμενη βιομηχανία καινοτόμων κρυπτονομισμάτων που χρησιμοποιούν ανεξάρτητες μεθόδους αλυσίδας μπλοκ.

Άλλα πρωτόκολλα είναι χτισμένα στην αλυσίδα μπλοκ του Bitcoin και εκτελούν ενδιαφέροντα πράγματα, όπως οι μάρκες που ταυτίζονται με συγκεκριμένα στοιχεία ενεργητικού για εμπορικούς σκοπούς (Coloured Coins, Mastercoin, και Counterparty). Η τεχνολογία της Αλυσίδας των Μπλόκ έχει ένα σημαντικό πρόβλημα επεκτασιμότητας, όμως, σχετίζεται με την υπολογιστική ισχύ που απαιτείται για να υπολογίσει εκ νέου το ιστορικό όλων των συναλλαγών, ένα πρόβλημα το οποίο μεγαλώνει καθώς η χρήση Bitcoins γίνεται πιο διαδεδομένη.

Κεφάλαιο 2

Ιστορική Αναδρομή

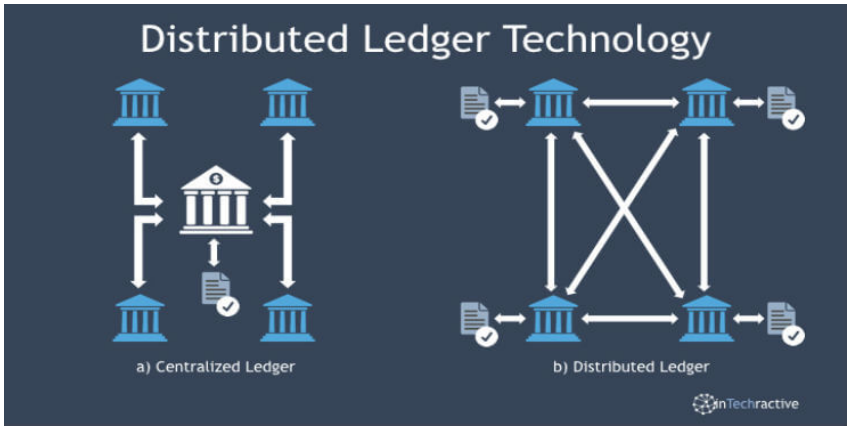
2.1 Ιστορική Αναδρομή Κρυπτονομισμάτων

Το 1983, ο Αμερικανός κρυπτογράφος και προγραμματιστής David Chaum είχε την ιδέα για το πρώτο ανώνυμο κρυπτογραφικό ηλεκτρονικό νόμισμα που ονομάζεται E-cash. Αργότερα, το 1995, το έθεσε σε λειτουργία μέσω του Digicash, μιας πρώιμης μορφής κρυπτογραφικών ηλεκτρονικών πληρωμών που απαιτούσε λογισμικό για την ανάληψη ώστε να μπορέσει να ορίσει συγκεκριμένα κρυπτογραφημένα κλειδιά για να σταλεί σε κάποιον παραλήπτη μια πληρωμή. Αυτό επέτρεψε στο ψηφιακό νόμισμα να μην είναι εντοπίσιμο από την τράπεζα, την κυβέρνηση ή οποιοδήποτε άλλο τρίτο μέρος. [1]

Το 1996, η Εθνική Υπηρεσία Ασφαλείας (National Security Agency - NSA) εξέδωσε μία δημοσίευση με τίτλο: «Πώς να δημιουργήσετε νομίσματα: Η κρυπτογραφία των ανώνυμων ηλεκτρονικών νομισμάτων», περιγράφοντας ένα σύστημα κρυπτονομισμάτων, αφού πρώτα τη δημοσίευσε σε μια λίστα αλληλογραφίας του MIT και αργότερα το 1997, τη δημοσίευσε στο «The American Law Review».

Το 1998, ο Wei Dai δημοσίευσε μια περιγραφή του "B-money", που χαρακτηρίζεται ως ένα ανώνυμο, κατανεμημένο ηλεκτρονικό σύστημα μετρητών. Λίγο αργότερα, ο Nick Szabo περιέγραψε το bit gold. Όπως το bitcoin και άλλα κρυπτονομίσματα που θα ακολουθούσαν, το bit gold (που δεν πρέπει να συγχέεται με την μεταγενέστερη ιδέα ανταλλαγής με βάση το χρυσό, με το όνομα BitGold) περιγράφηκε ως ένα σύστημα ηλεκτρονικού νομίσματος το οποίο απαιτούσε από τους χρήστες να συμπληρώνουν μια απόδειξη εργασίας με τη λύση αλγορίθμων και αποδείξεις κρυπτογραφημένες και δημοσιευμένες. Ένα σύστημα συναλλάγματος βασισμένο στην απόδειξη εργασίας δημιουργήθηκε αργότερα από τον Hal Finney ο

οποίος ακολούθησε το έργο των Wei Dai και Nick Szabo.



Εικόνα 2.1: Δίκτυο λειτουργίας της οικονομίας. https://whichblockchain.com/uncategorized/distributed-ledger-technology-regulatory-sandbox-in-uk-attracts-attention-from-business-owners/ (10/3/2019)

Το πρώτο επιτυχημένο κρυπτονόμισμα, με το όνομα Bitcoin, δημιουργήθηκε το 2009 από τον προγραμματιστή ή την ομάδα προγραμματιστών με το ψευδώνυμο Satoshi Nakamoto. Χρησιμοποιεί τον αλγόριθμο SHA-256, μια κρυπτογραφική λειτουργία κατακερματισμού, ως το προσχέδιο για την απόδειξη της εργασίας. [2]

Τον Απρίλιο του 2011, δημιουργήθηκε το Namecoin ως την προσπάθεια δημιουργίας ενός αποκεντρωμένου συστήματος DNS, το οποίο θα καθιστούσε πολύ πιο δύσκολη τη λογοκρισία στο Διαδίκτυο. Λίγο αργότερα, τον Οκτώβριο του 2011, κυκλοφόρησε το Litecoin.

Ήταν το πρώτο επιτυχημένο κρυπτονόμισμα που χρησιμοποίησε τον αλγόριθμο Scrypt ως λειτουργία εξόρυξης αντί του SHA-256. Ένα άλλο αξιόλογο κρυπτονόμισμα είναι το Peercoin, το πρώτο που κάνει χρήση ενός υβριδικού συστήματος απόδειξης εργασίας / απόδειξης επιτοκίου.

Στις 6 Αυγούστου 2014, το Ηνωμένο Βασίλειο ανακοίνωσε ότι το Υπουργείο Οικονομικών του είχε αναθέσει τη διενέργεια μελέτης σχετικά με τα κρυπτονομίσματα και ποιο ρόλο μπορούν να διαδραματίσουν στην οικονομία του Ηνωμένου Βασιλείου. Η μελέτη αναφέρει ότι πρέπει να ληφθούν υπόψη συγκεκριμένοι κανονισμοί, όρια και να γίνουν έλεγχοι στο νέο αυτό σύστημα.

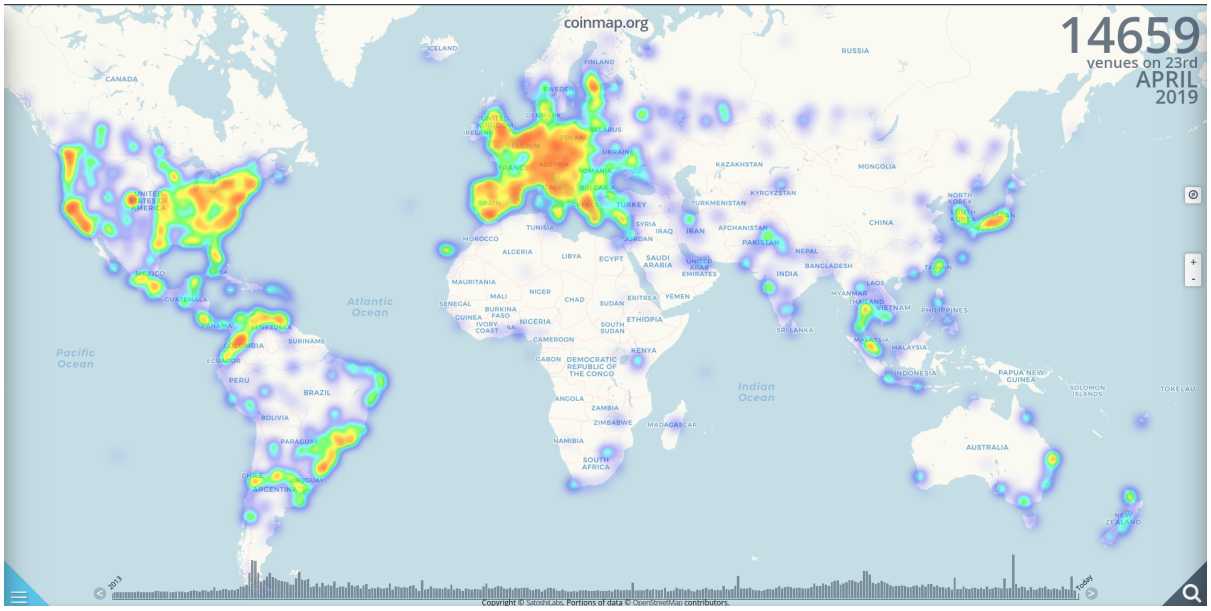
2.2 Bitcoin

Το Bitcoin είναι ένα κρυπτονόμισμα, ένα ψηφιακό στοιχείο που έχει σχεδιαστεί για να λειτουργεί ως μέσο ανταλλαγής, χρησιμοποιώντας την κρυπτογραφία για τον έλεγχο της δημιουργίας και της διαχείρισης του, αντί να βασίζεται στις κλασικές αρχές της δημιουργίας νομισμάτων. Ο φερόμενος δημιουργός του με το ψευδώνυμο «Satoshi Nakamoto» συνδύασε πολλές υπάρχουσες ιδέες σχετικά με την κρυπτογράφηση των νομισμάτων και λειτουργικές ιδέες από το κίνημα των Anonymous και των Cypherpunks κατά τη δημιουργία του Bitcoin. [3]

Εικόνα 2.2: Κρυπτονόμισμα Bitcoin. https://www.theverge.com/2018/1/17/16900448/bitcoin-drop-below-100000-half-peak-bitconnect (10/3/2019)

Το κρυπτονόμισμα αυτό έχει ταχεία ανάπτυξη και έχει γίνει ένα σημαντικό νόμισμα. Από τα μέσα της δεκαετίας του 2010 και μετά ορισμένες επιχειρήσεις άρχισαν να δέχονται το Bitcoin και άλλα κρυπτονομίσματα, εκτός από τα παραδοσιακά χρήματα.

Στις μέρες μας οι παρακάτω εταιρείες (Microsoft, Newegg, ExpressVPN, Cheapair, Overstock, Egifter, Reeds Jewelers, Gyft) και πολλές άλλες δέχονται τα Bitcoin και άλλα κρυπτονομίσματα για αγορές στα διαδικτυακά και μη καταστήματα τους. Επίσης ένας χάρτης των επιχειρήσεων που δέχονται bitcoin ανά την υφήλιο μπορεί κάποιος να τον βρει στο coinmap (Εικόνα 2.3).



Εικόνα 2.3: Coinmap. https://coinmap.org/ (11/3/2019)

2.2.1 Satoshi Nakamoto

Το όνομα «Satoshi Nakamoto» (Εικόνα 2.4) είναι αυτό που χρησιμοποιείται από το άγνωστο άτομο ή άτομα που ανέπτυξαν το Bitcoin. Οι ίδιοι συνέταξαν τις οδηγίες για να κατανοήσει κάποιος τι είναι το Bitcoin, πως μπορεί να του χρησιμεύσει και γιατί να πάρει την απόφαση να το χρησιμοποιήσει. Δημιούργησαν επίσης και κωδικοποίησαν την βασική εφαρμογή του (το πορτοφόλι) αλλά και την σχετική τεκμηρίωση για όλα τα παραπάνω. Στο πλαίσιο της υλοποίησης του, επινόησαν επίσης την πρώτη αποκεντρωμένη βάση δεδομένων φερόμενη ως «Blockchain». Κατά την υλοποίηση, ήταν οι πρώτοι που έλυσαν το πρόβλημα της διπλής δαπάνης στο ψηφιακό νόμισμα χρησιμοποιώντας ένα δίκτυο «peer-to-peer». Ο κώδικας του Bitcoin αναπτύσσεται ενεργά από την ομάδα του Bitcoin Core μετά την αποχώρηση του Satoshi Nakamoto τον Δεκέμβριο του 2010.

Το Bitcoin Core είναι δωρεάν λογισμικό ανοιχτού κώδικα που χρησιμεύει ως κόμβος και ώς πορτοφόλι του bitcoin (το σύνολο των οποίων αποτελεί το δίκτυο του bitcoin) και παρέχει ένα πορτοφόλι bitcoin που ελέγχει πλήρως τις πληρωμές. Θεωρείται ότι είναι η εφαρμογή αναφοράς για το bitcoin και είναι η πιο χρησιμοποιούμενη υλοποίηση. Αρχικά, το λογισμικό δημοσιεύθηκε από τον Satoshi Nakamoto με την επωνυμία "Bitcoin" και αργότερα μετονομάστηκε σε "Bitcoin Core" για να διαφέρει από το όνομα του δικτύου. Για το λόγο αυτό, είναι επίσης γνωστός ως πρόγραμμα- πελάτης Satoshi. Από το 2018, τα

Εικόνα 2.4: «Satoshi Nakamoto», δημιουργός/δημιουργοί του Bitcoin. https://coingambling.io/truth-bitcoins-anonymous/ (13/3/2019)

αποθετήρια του Bitcoin Core διατηρούνται από μια ομάδα συντηρητών, με τον Wladimir J. van der Laan να οδηγεί τη διαδικασία. Η Πρωτοβουλία Ψηφιακής Νομισματικής Μονάδας του MIT χρηματοδοτεί μέρος της ανάπτυξης του Bitcoin Core.

Ο Nakamoto δεν έχει αποκαλύψει καμία προσωπική του πληροφορία κατά τη συζήτηση στα Φόρουμ. Στις αναρτήσεις του για το P2P Foundation το 2010, ο Nakamoto ισχυρίστηκε ότι είναι άντρας ηλικίας 37 ετών που έζησε στην Ιαπωνία, αλλά ορισμένοι πίστευαν ότι ήταν απίθανο να είναι Ιάπωνας λόγω της χρήσης του τέλειου αγγλικού λόγου και της τεκμηρίωσης που παρέχει στα Αγγλικά.

Επιπλέον το πρώτο μπλόκ της αλυσίδας του Bitcoin θα μπορούσε να εξορυχθεί μόνο από τον Satoshi και περιέχει το κωδικοποιημένο μήνυμα "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" κάτι που μας δείχνει ότι ο δημιουργός διαβάζει την εφημερίδα The Times του Λονδίνου κατα την έναρξη του Bitcoin.

Ο Στέφαν Τόμας, είναι Ελβετός και ενεργό μέλος της κοινότητας ο οποίος συγκέντρωσε τις χρονικές σφραγίδες για κάθε μία από τις αναρτήσεις στο φόρουμ του Bitcoin (περισσότερες από 500) για τον Satoshi. Το προκύπτον διάγραμμα παρουσιάζει μια απότομη πτώση σε αναρτήσεις μεταξύ των ωρών 5 π.μ. και 11 μ.μ. ώρα Γκρίνουιτς. Αυτό το χρονικό διάστημα είναι μεταξύ τις 2 μ.μ. και τις 8 μ.μ. σε σχέση με την Ιαπωνική ώρα, υποδεικνύοντας ένα

ασυνήθιστο πρότυπο ύπνου για κάποιον που υποτίθεται ότι ζει στην Ιαπωνία. Δεδομένου ότι αυτό το μοτίβο ισχύει και τα Σάββατα και τις Κυριακές, πρότεινε ότι ο Nakamoto πιθανόν κοιμόταν αυτές τις ώρες. Ο Gavin Andresen είπε για τον κώδικα που έγραψε ο Nakamoto: "Ήταν ένας λαμπρός προγραμματιστής, αλλά ήταν πραγματικά περίεργος". [3]

2.2.2 Mining

Οι καταναλωτές τείνουν να εμπιστεύονται τα παραδοσιακά νομίσματα, τουλάχιστον στις Ηνωμένες Πολιτείες. Αυτό συμβαίνει επειδή το δολάριο των ΗΠΑ υποστηρίζεται από μια κεντρική τράπεζα που ονομάζεται Federal Reserve. Πέρα από μια σειρά άλλων αρμοδιοτήτων, το Federal Reserve ρυθμίζει την παραγωγή νέων νομισμάτων και διώκει τη χρήση πλαστών.

Ακόμη και οι ψηφιακές πληρωμές που χρησιμοποιούν το δολάριο των ΗΠΑ υποστηρίζονται από μια κεντρική αρχή. Όταν πραγματοποιείτε μια ηλεκτρονική αγορά χρησιμοποιώντας χρεωστική ή πιστωτική κάρτα, για παράδειγμα, η συναλλαγή αυτή υποβάλλεται για επεξεργασία από μια εταιρεία επεξεργασίας πληρωμών, όπως η Mastercard ή η Visa. Εκτός από την καταγραφή του ιστορικού των συναλλαγών, οι εταιρείες αυτές επαληθεύουν ότι οι συναλλαγές δεν είναι δόλιες, γεγονός που αποτελεί και έναν λόγο για τον οποίο η χρεωστική ή η πιστωτική κάρτα μπορεί να μην λειτουργεί κατά τη διάρκεια ενός ταξιδιού.

Το Bitcoin, από την άλλη πλευρά, δεν ρυθμίζεται από μια κεντρική αρχή. Αντί για αυτό, το Bitcoin υποστηρίζεται από εκατομμύρια υπολογιστές σε όλο τον κόσμο που ονομάζονται «Miners». Αυτό το δίκτυο υπολογιστών εκτελεί την ίδια λειτουργία με το Federal Reserve, τη Visa και τη Mastercard, αλλά με μερικές βασικές διαφορές. Όπως η Federal Reserve, η Visa και η Mastercard, έτσι και οι «Miners» καταγράφουν συναλλαγές και ελέγχουν την ακρίβειά τους. Αντίθετα όμως με τις κεντρικές αρχές, οι «Miners» βρίσκονται σε ολόκληρο τον κόσμο και καταγράφουν δεδομένα συναλλαγών σε έναν δημόσιο κατάλογο ο οποίος μπορεί να προσεγγιστεί από οποιονδήποτε.

Όταν κάποιος πραγματοποιεί μια αγορά ή μια πώληση χρησιμοποιώντας Bitcoin, διενεργείται μια συναλλαγή. Οι συναλλαγές που γίνονται σε κατάστημα και στο διαδίκτυο τεκμηριώνονται από τις τράπεζες, τα συστήματα σημείων πώλησης και τα φυσικά έσοδα. Οι «Miners» του Bitcoin επιτυγχάνουν το ίδιο αποτέλεσμα χωρίς αυτούς τους φορείς, συγκεντρώνοντας τις συναλλαγές σε ομάδες μπλοκ και προσθέτοντάς τες σε ένα δημόσιο αρχείο που ονομάζεται «Blockchain».

Όταν οι «Miners» προσθέτουν ένα νέο μπλοκ συναλλαγών στο «Blockchain», μέρος της δουλειάς τους είναι να βεβαιωθούν ότι οι συναλλαγές αυτές είναι ακριβείς. Ειδικότερα, οι

«Miners» του Bitcoin φροντίζουν να μην ξοδεύονται τα Bitcoin δυο φορές, με έναν τρόπο που ονομάζεται «διπλή δαπάνη». Με τα κανονικά νομίσματα, η αντιγραφή χρημάτων δεν είναι πρόβλημα. Μόλις ξοδέψει κανείς κάποια χρήματα σε ένα κατάστημα τα χρήματα αυτά βρίσκονται στα χέρια του υπαλλήλου. Με τα ψηφιακά νομίσματα δεν είναι έτσι.

Οι ψηφιακές πληροφορίες μπορούν να αναπαράγονται σχετικά εύκολα, έτσι ώστε με το Bitcoin και άλλα ψηφιακά νομίσματα, δεν υπάρχει ο κίνδυνος ότι ένας καταναλωτής μπορεί να δημιουργήσει ένα αντίγραφο του Bitcoin και να το στείλει σε ένα άλλο μέρος, ενώ κρατάει το πρωτότυπο.

Με περισσότερες από 600.000 συναλλαγές σε μια μόνο ημέρα, η επαλήθευση καθεμιάς από αυτές τις συναλλαγές μπορεί να είναι μια πολύ βαριά εργασία για τους «Miners», κάτι που είναι άλλη μια βασική διαφορά μεταξύ των «Miners» και των Federal Reserve, Mastercard και Visa.

Ως αποζημίωση για τις προσπάθειές τους, οι «Miners» λαμβάνουν Bitcoin, όποτε προσθέτουν ένα νέο μπλοκ συναλλαγών στο Blockchain. Η ποσότητα των νέων Bitcoin που απελευθερώνεται κάθε 10 λεπτά ονομάζεται "ανταμοιβή μπλοκ". Η ανταμοιβή των μπλοκ μειώνεται κατά το ήμισυ κάθε 210.000 μπλοκ, ή περίπου κάθε 4 χρόνια. Το 2009, ήταν 50. Το 2013, ήταν 25, το 2018 ήταν 12,5, και κάποια στιγμή στα μέσα του 2020 η ανταμοιβή θα μειωθεί στο μισό σε 6,25 νομίσματα ανά 10 λεπτά. [4]

Με αυτό το ρυθμό μείωσης κατά το ήμισυ, ο συνολικός αριθμός των Bitcoin σε κυκλοφορία θα προσεγγίσει το όριο των 21 εκατομμυρίων, καθιστώντας το νόμισμα πιο σπάνιο και πολύτιμο με την πάροδο του χρόνου, αλλά και πιο δαπανηρό για τους «Miners» στο να το παράγουν.

Σαν αποτέλεσμα λοιπόν μιας αμιγώς ομότιμης έκδοσης ηλεκτρονικών νομισμάτων θα επιτρέπει την απευθείας αποστολή των πληρωμών στο διαδίκτυο απευθείας από το ένα συμβαλλόμενο μέρος στο άλλο, χωρίς να διέρχεται από κάποιο χρηματοπιστωτικό ίδρυμα. Οι ψηφιακές υπογραφές αποτελούν μέρος της λύσης, αλλά τα κύρια οφέλη χάνονται εάν απαιτείται ακόμη ένας αξιόπιστο τρίτο μέρος για να αποτρέψει τη διπλή δαπάνη.

Ο Satoshi προτείνει μια λύση στο πρόβλημα των διπλών δαπανών χρησιμοποιώντας ένα δίκτυο peer-to-peer. Οι συναλλαγές χρονικής σήμανσης του δικτύου, οι οποίες περιλαμβάνουν την εξάπλωση τους σε μια συνεχή αλυσίδα απόδειξης εργασίας που βασίζεται στον κατακερματισμό, σχηματίζει μια εγγραφή που δεν μπορεί να αλλάξει χωρίς να επαναληφθεί η απόδειξη εργασίας.

Η μεγαλύτερη αλυσίδα όχι μόνο χρησιμεύει ως απόδειξη της σειράς των γεγονότων που παρατηρήθηκαν, αλλά και απόδειξη ότι προέρχεται από τη μεγαλύτερη δεξαμενή ισχύος των

CPU (Εικόνα 2.5). Το ίδιο το δίκτυο απαιτεί ελάχιστη δομή. Τα μηνύματα μεταδίδονται με βάση την καλύτερη δυνατή προσπάθεια και οι κόμβοι μπορούν να εγκαταλείψουν και να επανέλθουν στο δίκτυο κατά βούληση, αποδεχόμενοι τη μεγαλύτερη αλυσίδα απόδειξης της εργασίας ως απόδειξη του τι συνέβη όταν είχαν φύγει. [5]

Εικόνα 2.5: Απαιτούμενα συστήματα για την διαδικασία του Mining. https://www.coindesk.com/gmo-quits-selling-mining-machines-after-crypto-market-downturn (15/3/2019)

2.3 Αλγόριθμοι Εξόρυξης

Εκτός από το μηχανισμό ασφαλείας του δικτύου, οι αλγόριθμοι κατακερματισμού (hash) επηρεάζουν επίσης τα κρυπτονομίσματα. Για τον μηχανισμό POW, ο αλγόριθμος κατακερματισμού και η δυσκολία του υπαγορεύουν πόσα hashes - πόση ενέργεια - αναμένεται να δαπανηθεί. Επειδή οι χρήστες που εξορύσσουν κρυπτονομίσματα έχουν κίνητρα να βρίσκουν και να χρησιμοποιούν όλο και πιο ισχυρό εξοπλισμό, έχει δημιουργηθεί μεγάλος ανταγωνισμός σχετικά με τον εξοπλισμό. Για παράδειγμα, η εξόρυξη αρχικά γινόταν από την CPU (Κεντρική Μονάδα Επεξεργασίας).

Ωστόσο, οι ίδιες λειτουργίες θα μπορούσαν να εκτελούνται από τη GPU (Graphics Processing Unit) με πολύ ταχύτερο ρυθμό. Οι GPUs, στη συνέχεια, έδωσαν τη θέση τους

στα ολοκληρωμένα κυκλώματα ειδικού σκοπού (ASIC), με απώτερο σκοπό τη διενέργεια εξόρυξης κρυπτονομισμάτων με απίστευτες ταχύτητες - μεγέθη πολύ υψηλότερα από ότι θα μπορούσαν μέσω GPUs. Ο αλγόριθμος SHA-256 που χρησιμοποιείται στο δίκτυο του Bitcoin και σε διάφορα εναλλακτικά κρυπτονομίσματα, δεν μπορεί να ανταποκριθεί στις εναλλαγές εξοπλισμού, και πολλά νομίσματα έχουν εισαγάγει εναλλακτικούς αλγορίθμους εξόρυξης που συχνά έχουν ως πλεονέκτημα την ανθεκτικότητα στα ASIC. Ωστόσο, αυτό δεν ισχύει ολοκληρωτικά, καθώς τα ASICs μπορούν να σχεδιαστούν για την εκτέλεση κάθε αλγορίθμου.

Το υψηλό κόστος αυτής της διαδικασίας είναι ένα μειονέκτημα, και πρέπει να δοθούν επαρκή κίνητρα σε αυτούς που κάνουν εξόρυξη κρυπτονομισμάτων, για την κατασκευή μηχανημάτων ASIC για ένα συγκεκριμένο αλγόριθμο πλην του SHA-256, όπως το Scrypt. Έτσι υπήρξε μια δραματική αύξηση στον αριθμό των gigahashes ανά δευτερόλεπτο στο δίκτυο του Bitcoin. Ένα άλλο πρόβλημα είναι οι οικονομίες κλίμακας που δημιουργούνται. Για να είναι αποκεντρωμένος ο έλεγχος, τα νομίσματα πρέπει να έχουν κατανεμημένη ασφάλεια μεταξύ πολλών χρηστών.

Ωστόσο, οι επενδυτές μικρής κλίμακας βλέπουν πλέον ως επικερδή τη σύνδεση των υπολογιστών του σπιτιού τους στο δίκτυο των κρυπτονομισμάτων, δεδομένου ότι τότε θα αναγκαστούν να ανταγωνιστούν με πολύ πιο γρήγορα ASICs. Ως εκ τούτου, αυτός ο ανταγωνισμός των εξοπλισμών είχε ως αποτέλεσμα, τη συγκέντρωση του ελέγχου του δικτύου στα χέρια των μεγαλύτερων «Miners».

2.3.1 Αλγόριθμος SHA-256

Το SHA-256 είναι μέρος των κρυπτογραφικών λειτουργιών κατακερματισμού SHA-2, που έχει σχεδιάσει η NSA. Το SHA σημαίνει Secure Hash Algorithm. Οι κρυπτογραφικές λειτουργίες είναι μαθηματικές λειτουργίες που εκτελούνται πάνω στα ψηφιακά δεδομένα. με τη σύγκριση του υπολογιζόμενου "hash" (του αποτελέσματος από την εκτέλεση του αλγορίθμου), με μια γνωστή και αναμενόμενη τιμή, ένα άτομο μπορεί να καθορίσει την ακεραιότητα των δεδομένων. Μπορεί να δημιουργηθεί ένα hash μονής κατεύθυνσης από οποιοδήποτε κομμάτι δεδομένων, αλλά τα δεδομένα δεν μπορούν να δημιουργηθούν από το hash. [6]

Εικόνα 2.6: Σύστημα υλοποίησης Mining, της εταιρίας SFARDS, για τους αλγορίθμους SHA-256 και Scrypt. https://cryptomining-blog.com/5284-sfards-sf100-asics-coming-soon-but-too-expensive/ (20/3/2019)

2.3.2 Αλγόριθμος Scrypt

Στην κρυπτογραφία, το Scrypt είναι μια λειτουργία εξόρυξης που βασίζεται σε κάποιον κωδικό πρόσβασης. Ο αλγόριθμος σχεδιάστηκε ειδικά για να καταστήσει δαπανηρές τις εκτελέσεις επιθέσεων μεγάλης κλίμακας με υλικό υπολογιστών που απαιτούν μεγάλες ποσότητες μνήμης. Το 2012, ο αλγόριθμος Scrypt δόθηκε στη δημοσιότητα από το IETF ως σχέδιο. Μια απλοποιημένη εκδοχή του Scrypt χρησιμοποιείται ως ένα σύστημα απόδειξης της εργασίας από μια σειρά κρυπτονομισμάτων, όπως το Litecoin. [7]

Μια λειτουργία προέλευσης κλειδιών που βασίζεται σε κωδικό πρόσβασης (με βάση τον κωδικό KDF) έχει σχεδιαστεί για να είναι υπολογιστικά εντατική, ώστε να χρειαστεί ένα σχετικά μεγάλο χρονικό διάστημα για να υπολογιστεί (της τάξης των μερικών εκατοντάδων χιλιοστών του δευτερολέπτου). Εξουσιοδοτημένοι χρήστες πρέπει να εκτελέσουν τη συνάρτηση μία φορά ανά λειτουργία (π.χ. έλεγχος ταυτότητας), και έτσι ο χρόνος που απαιτείται είναι αμελητέος. Ωστόσο, κατά την διάρκεια μιας επίθεσης είναι πιθανόν να χρειαστεί να εκτελεστεί η λειτουργία δισεκατομμύρια φορές, οπότε οι απαιτήσεις χρόνου θα γίνουν σημαντικές έως και απαγορευτικές.

Προηγούμενες λειτουργίες που βασίζονται σε κωδικό πρόσβασης KDFs (όπως το δημοφιλές PBKDF2) έχουν σχετικά χαμηλές απαιτήσεις πόρων, που σημαίνει ότι δεν χρειάζονται

Εικόνα 2.7: Σύστημα υλοποίησης Mining, της εταιρίας Zeus Integrated Systems Limited, για τον αλγόριθμο Scrypt. https://cryptomining-blog.com/tag/zeusminer-blizzard-review/ (25/3/2019)

περίτεχνο υλικό ή πολύ μνήμη για να εκτελεστούν. Είναι, συνεπώς, εύκολο και φθηνό να υλοποιηθούν από την άποψη του υλικού (για παράδειγμα, σε ένα ASIC ή ακόμα και ένα FPGA). Αυτό επιτρέπει σε έναν εισβολέα με επαρκείς πόρους να ξεκινήσει μια μεγάλης κλίμακας επίθεση, παράλληλα με την οικοδόμηση εκατοντάδων ή ακόμα και χιλιάδων εφαρμογών του αλγορίθμου σε υλικό και με κάθε αναζήτηση να υπάρχει ένα διαφορετικό υποσύνολο. Αυτό χωρίζει το ποσό του χρόνου που απαιτείται για να ολοκληρωθεί μια επίθεση από τον αριθμό των διαθέσιμων εφαρμογών, πολύ πιθανόν αξιοποιώντας τες σε ένα εύλογο χρονικό διάστημα.

Η λειτουργία Scrypt έχει σχεδιαστεί για να εμποδίσει τέτοιες προσπάθειες, αυξάνοντας τις απαιτήσεις των πόρων του αλγορίθμου. Συγκεκριμένα, ο αλγόριθμος έχει σχεδιαστεί για να χρησιμοποιεί ένα μεγάλο ποσό της μνήμης σε σύγκριση με τα άλλα KDFs, καθιστώντας το μέγεθος και το κόστος μιας εφαρμογής υλικού πολύ πιο ακριβή, και επομένως περιορίζει

την ποσότητα του παραλληλισμού ενός εισβολέα, για μια δεδομένη ποσότητα χρηματικών πόρων.

2.3.3 Αλγόριθμος X11

Αυτός είναι ένας σχετικά νέος και κερδοφόρος αλγόριθμος, πολύ δημοφιλής από το 2014 στην εξόρυξη με GPU. Έχουν δημιουργηθεί ειδικά για την εξόρυξη GPU και είναι σε θέση να παρέχουν καλή κερδοφορία στην κοινότητα μετά την έλευση των μεγάλων ASICs για τον αλγόριθμο Scrypt. Κάθε αποτέλεσμα από έναν υπο-αλγόριθμο, περνιέται στον επόμενο υπο-αλγόριθμο. [8]

Εικόνα 2.8: Απαιτούμενο σύστημα για την υλοποίηση του αλγορίθμου X11. https://cryptomining-blog.com/7117-the-first-x11-mining-asic-ibelink-dm384m-asic-dash-miner/ (27/3/2019)

Η δημιουργία ASIC, αφιερωμένων σε αυτή την οικογένεια αλγορίθμων δυσχεραίνει την εξόρυξη με το γεγονός ότι το υλικό θα πρέπει να έχει λογικές πύλες για κάθε αλγόριθμο σε ολόκληρο το τσιπ, αυξάνοντας έτσι δραστικά τη πολυπλοκότητα της κατασκευής.

Από την άλλη πλευρά, οι αλγόριθμοι X11-X15 χρησιμοποιούν μόνο 536mb RAM (περίπου), και αυτό μπορεί να αποσβέσει ένα μέρος του κόστους των λογικών πυλών. X11 είναι το όνομα μιας αλυσίδας συναλλαγών, η οποία χρησιμοποιείται για τους υπολογισμούς στον μηχανισμό απόδειξης εργασίας, ώστε να υπάρχει ασφάλεια στο δίκτυο ορισμένων κρυπτονομισμάτων.

Είναι γνωστός ως αλυσιδωτός αλγόριθμος, επειδή χρησιμοποιεί 11 διαφορετικούς αλγορίθμους που είναι συνδεδεμένοι μεταξύ τους. Αυτοί είναι: Blake, Bmw, Groestl, JH, Keccak, Skein, Luffa, Cubehash, Shavite, Simd, και Echo. Είναι ανθεκτικός στην υλοποίηση ASIC και κατάλληλος τόσο για την εξόρυξη με CPU όσο και για την εξόρυξη με GPU. Το πρώτο κρυπτονόμισμα που χρησιμοποίησε τον X11 στο δίκτυο του ήταν το Darkcoin, που από τότε έχει αλλάξει το όνομα του σε «Dash».

Ο X11 αναπτύχθηκε προκειμένου να ξεπεραστούν κάποια σημαντικά μειονεκτήματα που συνδέονται με τους ήδη υπάρχοντες αλγορίθμους κατακερματισμού, όπως ο SHA-256 (Bitcoin) ή ο Scrypt (Litecoin, Dogecoin). Το μεγαλύτερο από αυτά τα μειονεκτήματα ήταν το γεγονός ότι οι εταιρείες ηλεκτρονικών ειδών είχαν αναπτύξει ειδικό υλικό, που ονομάζεται ASICs, για την εξόρυξη νομισμάτων όπου χρησιμοποιούνται οι αλγόριθμοι εξόρυξης SHA-256 και Scrypt.

Αυτό είχε ως αποτέλεσμα να καταστήσει τα δίκτυα πιο συγκεντρωτικά - να ελέγχονται δηλαδή από μια μικρή ομάδα ισχυρών «Miners», ενώ το αρχικό όραμα των δικτύων των κρυπτονομισμάτων ήταν διαφορετικό. Στόχος ήταν αρχικά, οι απλοί χρήστες να μπορούν να πάρουν μέρος στην ενίσχυση της ασφάλειας του δικτύου και να κερδίζουν ανταμοιβές μέσω της εξόρυξης.

Ο συγκεντρωτισμός της εξόρυξης μειώνει την ασφάλεια του δικτύου, μειώνει τον αριθμό των ανθρώπων που συμμετέχει στη λειτουργία του δικτύου και γίνονται φυσικά υποστηρικτές του και μπορεί να αυξήσει την πιθανότητα τα κρυπτονομίσματα που εξορύσσονται να υφίστανται την άμεση πώληση, καθώς οι επιχειρήσεις θα πρέπει να καλύπτουν το κόστος και να λαμβάνουν τα κέρδη, ενώ οι ιδιώτες όχι.

2.3.4 Αλγόριθμος Dagger - Hashimoto

Ο Dagger-Hashimoto σχεδιάστηκε από τον Vitalik Buterin και την ομάδα του Ethereum συνδυάζοντας τα χαρακτηριστικά γνωρίσματα του αλγορίθμου Hashimoto και του αλγόριθμο Dagger. Ο Dagger-Hashimoto σχεδιάστηκε για να είναι ανθεκτικός στα ASIC. Και οι δύο αλγόριθμοι (Dagger-Hashimoto και Ethash) ενημερώθηκαν αργότερα ξεχωριστά και δεν

θεωρούνται σήμερα ο ίδιος αλγόριθμος. Ωστόσο, εξακολουθούν να αναφέρονται μερικές φορές ως συνώνυμα. [9]

Ο Hashimoto επιλέχθηκε ως μέρος του αλγορίθμου λόγω του γεγονότος ότι χρησιμοποιεί το blockchain ως πηγή δεδομένων και έχει σχεδιαστεί για να επιτύχει αντοχή στα ASIC κάνοντας τη μνήμη τον περιοριστικό παράγοντα στην εξαγωγή των νομισμάτων, που καθιστά τον Hashimoto ικανοποιητικό σαν λύση.

Εικόνα 2.9: Απαιτούμενο σύστημα για την υλοποίηση του αλγορίθμου Dagger - Hashimoto. https://cryptosrus.com/ethereum-mining-rig/ (15/3/2019)

Ο Dagger είναι μια εναλλακτική λύση για το Scrypt που παρέχει υπολογιστική μνήμη και γρήγορη επαλήθευση. Ο Dagger, όπως και ο Hashimoto, έχει ως στόχο να χρησιμοποιηθεί για τη δημιουργία δικτύων ανθεκτικών στα ASIC απαιτώντας ένα σημαντικό ποσό μνήμης RAM. Βασίζεται σε DAG, από τα οποία προέκυψε το όνομα Dagger. Τα DAGs είναι γραφήματα που δεν έχουν κατευθυνόμενους κύκλους που συνδέουν τις άκρες του γραφήματος. Ο Dagger, χρειάζεται 512 MB για την εξόρυξη, 112 KB μνήμης και 4078 hashes για την επαλήθευση, πράγμα που σημαίνει, ότι ο πρωταρχικός φορέας του Mining είναι η μνήμη και όχι η επεξεργαστική ισχύς. [9]

2.3.5 Αλγόριθμος CryptoNight

Ο CryptoNight είναι ένας αλγόριθμος απόδειξης της εργασίας (PoW). Είναι σχεδιασμένος για να είναι κατάλληλος για τους απλούς επεξεργαστές των υπολογιστών, ενώ προς το παρόν δεν υπάρχουν συσκευές ειδικού σκοπού για την εξόρυξη. Ως εκ τούτου, ο CryptoNight μπορεί να εξορύσσεται μόνο μέσω της CPU. Ο CryptoNight εφαρμόστηκε αρχικά στη βάση του κώδικα CryptoNote.

Ο CryptoNight βασίζεται στην τυχαία πρόσβαση στην αργή μνήμη και δίνει έμφαση στη λανθάνουσα κατάσταση εξάρτησης. Κάθε νέο μπλοκ εξαρτάται από όλα τα προηγούμενα μπλοκ (σε αντίθεση, για παράδειγμα, με τον Scrypt). Ο αλγόριθμος απαιτεί περίπου 2 MB ανά περίπτωση. [10]

Εικόνα 2.10: Απαιτούμενο σύστημα για την υλοποίηση του αλγορίθμου CryptoNight. https://www.youtube.com/watch?v=9dDrSSveXV4 (19/3/2019)

2.4 Blockchain

Ένα Blockchain είναι μια αυξανόμενη λίστα αρχείων, που ονομάζεται μπλοκ, τα οποία συνδέονται χρησιμοποιώντας κρυπτογραφία. Κάθε μπλοκ περιέχει ένα κρυπτογραφικό hash του προηγούμενου μπλοκ, μια σφραγίδα χρόνου και δεδομένα της συναλλαγής. Από τον σχεδιασμό του, ένα Blockchain είναι ανθεκτικό στην τροποποίηση των δεδομένων. Είναι ένας ανοικτός, κατανεμημένος φορέας που μπορεί να καταγράφει τις συναλλαγές μεταξύ δύο μερών αποτελεσματικά και με επαληθεύσιμο και μόνιμο τρόπο.

Για να χρησιμοποιηθεί ένα Blockchain χρειάζεται συνήθως ένα δίκτυο peer-to-peer που ακολουθεί ένα πρωτόκολλο για την επικοινωνία μεταξύ των κόμβων και την επικύρωση νέων μπλοκ. Μόλις καταγραφούν, τα δεδομένα σε οποιοδήποτε μπλοκ δεν μπορούν να τροποποιηθούν αναδρομικά, χωρίς αλλοίωση όλων των επόμενων μπλοκ, πράγμα που απαιτεί τη συναινετική πλειοψηφία του δικτύου.

Παρόλο που τα αρχεία μπλοκ αλυσίδων δεν είναι αναλλοίωτα, τα Blockchains μπορεί να θεωρηθούν ασφαλή από το σχεδιασμό τους και να αποτελέσουν παράδειγμα ενός κατανεμη-

μένου συστήματος υπολογιστών με υψηλή ανοχή βλαβών. Συνεπώς, έχει αποκατασταθεί η αποκεντρωμένη συναίνεση με ένα Blockchain. [11]

2.5 Συναλλαγές

Η μεταφορά χρημάτων μεταξύ δύο ψηφιακών πορτοφολιών ονομάζεται συναλλαγή. Η συναλλαγή αυτή υποβάλλεται στο δημόσιο βιβλίο και αναμένει επιβεβαίωση. Τα πορτοφόλια χρησιμοποιούν μια κρυπτογραφημένη ηλεκτρονική υπογραφή όταν γίνεται μια συναλλαγή.

Η υπογραφή είναι ένα κρυπτογραφημένο κομμάτι δεδομένων που ονομάζεται κρυπτογραφική υπογραφή και παρέχει μια μαθηματική απόδειξη ότι η συναλλαγή ήρθε από τον ιδιοκτήτη του πορτοφολιού. Η διαδικασία επιβεβαίωσης διαρκεί λίγο χρόνο (δέκα λεπτά για το bitcoin). Η εξόρυξη επιβεβαιώνει τις συναλλαγές και τις προσθέτει στο δημόσιο βιβλίο.

Όλες οι επιβεβαιωμένες συναλλαγές από την αρχή της δημιουργίας του νομίσματος αποθηκεύονται στο δημόσιο βιβλίο. Οι ταυτότητες των κατόχων είναι κρυπτογραφημένες και το σύστημα χρησιμοποιεί άλλες κρυπτογραφικές τεχνικές για να εξασφαλίσει τη νομιμότητα της τήρησης των αρχείων. Ο λογαριασμός εξασφαλίζει ότι τα αντίστοιχα "ψηφιακά πορτοφόλια" μπορούν να έχουν ένα ακριβές διαθέσιμο υπόλοιπο. Επίσης, μπορούν να ελεγχθούν νέες συναλλαγές για να διασφαλιστεί ότι κάθε συναλλαγή χρησιμοποιεί μόνο νομίσματα που ανήκουν εκείνη τη στιγμή στον εκδότη.

Στα κρυπτονομίσματα μια συναλλαγή DEX είναι μια αποκεντρωμένη συναλλαγή peer-to-peer. Πρόκειται για ένα χρηματιστήριο με κωδικό. Συνήθως υπάρχει ως αποκεντρωμένη εφαρμογή (DApp). Είναι ένας τρόπος, που οι άνθρωποι μπορούν να εμπορεύονται κρυπτονομίσματα απευθείας, χωρίς μεσάζοντα. [12]

Σε μια συναλλαγή DEX, κάθε κίνηση καταγράφεται στο Blockchain. Το DEX αντικαθιστά την ανάγκη ενός κεντρικού ανταλλακτηρίου που θα ενεργεί ως μεσάζων. Ένα παράδειγμα DEX είναι το EtherDelta. Το EtherDelta είναι ένα ανταλλακτήριο που υπάρχει ως DApp και χρησιμοποιεί την αλυσίδα συναλλαγών του Ethereum. [13]

2.5.1 Εναλλακτικές χρήσεις των Συναλλαγών

Μια εναλλακτική χρήση των κρυπτονομισμάτων είναι οι συναλλαγές από το εξωτερικό στην πατρίδα για άτομα το οποία είναι μετανάστες στις περιοχές αυτές και θέλουν να έχουν ασφάλεια και ταχύτητα στις συναλλαγές χωρίς να έχουν χρηματικές απώλειες και καθυστερήσεις από τα παραδοσιακά συστήματα τραπεζών και συναλλάγματος.

Άλλη μια εναλλακτική χρήση των κρυπτονομισμάτων είναι ότι σε πολλές χώρες όπου το νόμισμα της χώρας δεν είναι σταθερό και υπάρχει κίνδυνος υπονομευσης του νομίσματος αυτού, οι πολίτες τείνουν να επενδύουν σε κρυπτονομίσματα για να έχουν ασφάλεια στα χρήματα τους σε περίπτωση κατάρρευσης του οικονομικού συστήματος της χώρας αυτής.

2.6 ICO/STO

Μια αρχική προσφορά νομισμάτων, κοινώς αναφερόμενη ως ICO, είναι ένας μηχανισμός συλλογής κεφαλαίων κατά τον οποίο πωλούνται τα υποκείμενα κρυπτογραφικά νομίσματα σε αντάλλαγμα για άλλα κρυπτονομίσματα όπως το Bitcoin και το Ethereum. Μοιάζει με μια αρχική δημόσια εγγραφή (IPO) στην οποία οι επενδυτές αγοράζουν μετοχές μιας εταιρείας. [14]

Πρόκειται για ένα σχετικά νέο φαινόμενο, αλλά έχει γίνει ένα κυρίαρχο θέμα συζήτησης μέσα στην κοινότητα του Blockchain. Πολλοί θεωρούν ότι τα σχέδια των ICO είναι ως μη ελεγχόμενα χρεόγραφα που επιτρέπουν στους ιδρυτές να αυξήσουν ένα ποσό κεφαλαίου, ενώ άλλοι υποστηρίζουν ότι είναι μια καινοτομία στο παραδοσιακό μοντέλο χρηματοδότησης επιχειρηματικών πρωτοβουλιών.

Η Αμερικανική Επιτροπή Κεφαλαιαγοράς (SEC) κατέληξε πρόσφατα σε μια απόφαση σχετικά με την κατάσταση των νομισμάτων που έχουν εκδοθεί στο περίφημο DAO ICO, η οποία ανάγκασε πολλά έργα και επενδυτές να επανεξετάσουν τα μοντέλα χρηματοδότησης πολλών ICO. Τα πιο σημαντικά κριτήρια που πρέπει να ληφθούν υπόψη είναι εάν το νόμισμα μπορεί να περάσει τη δοκιμασία Howey. Αν συμβαίνει αυτό, πρέπει να αντιμετωπίζεται ως εγγύηση και υπόκειται σε ορισμένους περιορισμούς που επιβάλλει η Επιτροπή Κεφαλαιαγοράς.

Τα ICO είναι εύκολο να δομηθούν λόγω τεχνολογιών, όπως το πρότυπο ERC20 Token, το οποίο αφαιρεί πολλές από τις αναπτυξιακές διαδικασίες που είναι απαραίτητες για τη δημιουργία ενός νέου κρυπτογραφικού στοιχείου. Οι περισσότεροι οργανισμοί λειτουργούν με το να αποστέλλουν κεφάλαια (συνήθως bitcoin) σε ένα έξυπνο συμβόλαιο, που αποθηκεύει τα κεφάλαια και διανέμει μια ισοδύναμη αξία στο νέο νόμισμα σε μεταγενέστερο χρονικό διάστημα.

Υπάρχουν λίγοι περιορισμοί σχετικά με το ποιος μπορεί να συμμετέχει σε ένα ICO, υποθέτοντας ότι το νόμισμα δεν παρέχει στην πραγματικότητα ασφάλεια. Δεδομένου ότι λαμβάνονται χρήματα από μια παγκόσμια ομάδα επενδυτών, τα ποσά που συγκεντρώνονται στα ICO μπορεί να είναι αστρονομικά. Ένα βασικό ζήτημα με τα ICO είναι το γεγονός ότι

τα περισσότερα από αυτά συγκεντρώνουν χρήματα προ-παρασκευής.

Αυτό κάνει την επένδυση εξαιρετικά κερδοσκοπική και επικίνδυνη. Το αντίθετο επιχείρημα είναι ότι αυτό το στυλ συλλογής κεφαλαίων είναι ιδιαίτερα χρήσιμο (έως και απαραίτητο) για την παροχή κινήτρων για την ανάπτυξη πρωτοκόλλων.

2.7 Security Token Offering (STO)

Τα Security Token Offering (STO) είναι παρόμοια με τη συμμετοχή σε ένα ICO. Μπορεί κανείς να αγοράσει νομίσματα, κατά τη διάρκεια της προσφοράς που μπορεί να εμπορευτεί ή να κρατήσει. Ωστόσο, επειδή τα νομίσματα ασφαλείας είναι πραγματικοί χρηματοοικονομικοί τίτλοι, υποστηρίζονται δηλαδή από κάτι απτό, όπως τα περιουσιακά στοιχεία, τα κέρδη ή τα έσοδα μιας εταιρείας. [15]

Όταν οι εταιρείες εκδίδουν τα STO τους στην πλατφόρμα, έχουν καθοδηγήσει τις σύνθετες νομικές και τεχνολογικές διαδικασίες πριν από την έκδοση. Οι μάρκες που κυκλοφορούν με αυτόν τον τρόπο προορίζονται να συμμορφώνονται με τις απαιτήσεις KYC / AML και τους νόμους περί τίτλων σε όλες τις περιοχές.

Οι μάρκες ασφαλείας που δημιουργήθηκαν χρησιμοποιώντας το πρότυπο ST-20 του Polymath και άλλων αλυσίδων όπως το Ethereum είναι σε θέση να εμποδίσουν το εμπόριο μεταξύ αποκλεισμένων ατόμων, μέσω της χρήσης ισχυρών έξυπνων συμβολαίων και της τεχνολογίας διευθύνσεων για την καταχώρηση τους.

2.8 Εφοδιαστική αλυσίδα

Με τον όρο Εφοδιαστική Αλυσίδα (Εικόνα 2.11) εννοούμε σε γενικές γραμμές την διαδικασία μεταφοράς ενός προϊόντος ή μιας υπηρεσίας από το σημείο παραγωγής στο σημείο παράδοσης. Σκοπός της εφοδιαστικής αλυσίδας είναι η μείωση του λειτουργικού κόστους της μεταφοράς των προϊόντων και η αύξηση της ικανοποίησης του πελάτη. Το δίκτυο της εφοδιαστικής αλυσίδας επιτρέπει να έχει κανείς γενικότερη εικόνα της αγοράς, έχοντας καλύτερη κατανόηση της ροής των υλικών και των πληροφοριών. [16]

Οι εταιρίες συχνά επικεντρώνονται μόνο στην οργάνωσή τους, τι παράγουν ή παρέχουν και όχι τι λαμβάνει ο τελικός πελάτης. Η εξέταση ενός δικτύου εφοδιαστικής αλυσίδας επιτρέπει στις επιχειρήσεις να εξετάζουν τη συνολική κίνηση υλικών / πληροφοριών, από την αρχή μέχρι το τέλος. Έτσι, έχουν τη δυνατότητα να δουν την αξία στη δημιουργία εταιρικών σχέσεων και την αξία στη συνεργασία, για να εξασφαλιστεί η καλύτερη δυνατή παροχή

Εικόνα 2.11: Παράδειγμα Εφοδιαστικής Αλυσίδας. https://www.open.edu/openlearn/money-business/leadership-management/supply-chain-sustainability/content-section-0 (16/3/2019)

στον τελικό πελάτη. Οι εφοδιαστικές αλυσίδες και τα δίκτυα προμήθειας περιγράφουν τη ροή και την κυκλοφορία των υλικών και των πληροφοριών, συνδέοντας τις εταιρείες για να εξυπηρετήσουν τον τελικό πελάτη.

Το «δίκτυο» περιγράφει μια πιο σύνθετη δομή, όπου οι εταιρείες μπορούν να συνδεθούν και να υπάρχουν αμφίδρομες ανταλλαγές μεταξύ τους. Η «αλυσίδα» περιγράφει ένα απλούστερο, διαδοχικό σύνολο δεσμών. Προκειμένου να κατανοηθεί ένα δίκτυο εφοδιαστικής αλυσίδας, πρέπει να καταλάβει κανείς τι είναι μια εφοδιαστική αλυσίδα. Μια εφοδιαστική αλυσίδα είναι μια σειρά διαδικασιών που συνδέονται μαζί για να σχηματίσουν μια «αλυσίδα».

Κεφάλαιο 3

Εφοδιαστική αλυσίδα, η λειτουργία της στον πραγματικό κόσμο

3.1 Πως λειτουργεί η εφοδιαστική αλυσίδα

Οι βασικές λειτουργίες της Εφοδιαστικής Αλυσίδας περιλαμβάνουν:

- Προμήθειες
- Παραγωγή
- Μεταφορές
- Αποθήκευση
- Διανομή
- Εξυπηρέτηση Πελατών

Η διαχείριση της εφοδιαστικής αλυσίδας (ΔΕΑ) είναι η διαχείριση ενός δικτύου εσωτερικά συνδεδεμένων επιχειρήσεων που συμμετέχουν στην παροχή πακέτων προϊόντων και υπηρεσιών, τα οποία απευθύνονται στους τελικούς καταναλωτές. Η διαχείριση της εφοδιαστικής αλυσίδας εκτείνεται σε όλη τη διαδικασία μεταφοράς και αποθήκευσης των πρώτων υλών και των ολοκληρωμένων αγαθών από τα σημεία προέλευσης προς τα σημεία κατανάλωσης.

Ένας άλλος ορισμός αναφέρει την ΔΕΑ ως το σχεδιασμό, την εκτέλεση, τον έλεγχο και την παρακολούθηση των δραστηριοτήτων της εφοδιαστικής αλυσίδας με στόχο τη δημιουργία καθαρής αξίας, τη δόμηση μιας ανταγωνιστικής υποδομής, τη μόχλευση της διεθνούς επιμελητείας (logistics), τον συγχρονισμό της παροχής με τη ζήτηση και τη μέτρηση της απόδοσης παγκοσμίως. [16]

3.2 Το πρόβλημα

Το μέγεθος της βιομηχανίας των μεταφορών είναι τεράστιο - η παγκόσμια αξία του εμπορίου ναυτιλίας είναι πάνω από 12 τρισεκατομμύρια δολάρια (στατιστικές του ΠΟΕ). Η αξία των ναύλων είναι 380 δισεκατομμύρια δολάρια ΗΠΑ για το 2017 (UNCTAD). Αν και η ναυτιλιακή βιομηχανία είναι ένας από τους μεγαλύτερους οικονομικούς τομείς, είναι ο λιγότερο προηγμένος τεχνολογικά. Σήμερα τα έγγραφα εκδίδονται για όλα τα φορτία σε χαρτί, ανεξάρτητα από τα μέσα μεταφοράς. Όλα τα πρωτότυπα έγγραφα στέλνονται από ταχυμεταφορείς, το οποίο απαιτεί χρόνο και χρήμα. Όλα τα φορτία μεταφέρονται με παραδοσιακούς τρόπους - μέσω τραπεζικών εμβασμάτων ή πιστωτικών επιστολών. Αυτές είναι ακριβές, αργές και μη έμπιστες μέθοδοι.

Όλο και συχνότερα οι συναλλαγές σε δολάρια ΗΠΑ και ευρώ εμποδίζονται για εβδομάδες από τις ΗΠΑ. Όλοι στη βιομηχανία αντιμετώπισαν αυτό το πρόβλημα. Οι καθυστερήσεις παράδοσης των εγγράφων και οι καθυστερήσεις μεταφοράς των χρημάτων προκαλούν ένα μη υπολογιζόμενο επιπλέον κόστος, κόστος ευκαιρίας και απόσβεση περιουσιακών στοιχείων, ενώ διαταράσσουν μια μακρά αλυσίδα εφοδιασμού. Η τεχνολογία της αλυσίδας προσφέρει την επανάσταση του εμπορίου και των μεταφορών, προωθώντας τη βελτιστοποίηση.

Η νέα αυτή τεχνολογία θα εξαλείψει ορισμένα προβλήματα:

- Μείωση της Απάτης - Μειώνει τον κίνδυνο απάτης και σε πολλές περιπτώσεις την εξαλείφει πλήρως, μη αποδεσμεύοντας τις πληρωμές έως ότου ολοκληρωθούν οι προκαθορισμένες προϋποθέσεις των μελών και αποδεικνύεται δημόσια η απόδειξη ότι η πληρωμή έχει πραγματοποιηθεί ή εξασφαλιστεί σε ένα σημείο μεσεγγύησης. Οι πληρωμές θα είναι εγγυημένες ως προεπιλογή. Η αθέμιτη επικύρωση και η επικάλυψη εγγράφων ιδιοκτησίας αποκλείονται.

- Μείωση του κόστους - Θα μειώσει σημαντικά το κόστος, σε σύγκριση με τα υψηλά ποσοστά και άλλα τέλη εκτύπωσης που χρεώνονται μέσω της διαδικασίας από τράπε-

ζες, ταχυμεταφορείς, ασφαλιστές, μεσίτες, πράκτορες, γραμμές, κ.λπ. Τράπεζα L/C αυτή τη στιγμή.

- Ελαχιστοποίηση των καθυστερήσεων - Αποφεύγει τις καθυστερήσεις, παρέχοντας άμεση ανταλλαγή, εξέταση και έγκριση εγγράφων και πληρωμών μεταξύ των εμπλεκόμενων μερών. Περαιτέρω καθυστερήσεις προκαλούνται από διαφορετικές ζώνες ώρας, διαφορετικές δημόσιες αργίες κλπ. Η αλυσίδα λειτουργεί πάντα 24 ώρες το 24ωρο και δεν εξαρτάται από ανθρώπινη παρέμβαση/παρουσία. Εκτιμάται ότι οι καθυστερήσεις πληρωμών κοστίζουν περίπου 19 δισεκατομμύρια δολάρια ετησίως (UNCATD) σε ζημίες.

- Αύξηση της εμπιστοσύνης - Βασίζεται στη δημόσια υποδομή του μπλοκ αλυσίδας, υποστηριζόμενη από χιλιάδες ανθρώπους σε μια αποκεντρωμένη υποδομή από ομότιμους χρήστες. Η χρήση μιας αποδεδειγμένης και αξιόπιστης τεχνολογίας μιλάει από μόνη της.

- Διασφάλιση πληροφοριών - Είναι φυσικά ασφαλές. Βασίζεται στην αποδεδειγμένη τεχνολογία αλγορίθμου των μπλόκ. Δεν υπάρχει πιθανότητα διαρροής ευαίσθητων εμπορικών πληροφοριών από μεσάζοντες, όπως τράπεζες, μεσίτες, πράκτορες κ.λπ. Ενώ είναι απόλυτα εμπιστευτικό, επιτρέποντας επίσης την πλήρη δημοσιοποίηση των λεπτομερειών των συναλλαγών που πρέπει να είναι ορατες από όλα τα μέρη και το κοινό.

- Ασφαλής αρχειοθέτηση - Βασίζεται πλήρως στην ιστορική αποθήκευση όλων των συναλλαγών που πραγματοποιήθηκαν ποτέ, αποφεύγοντας έτσι τους κινδύνους σωματικής απώλειας ή καταστροφής εγγράφων που βρίσκονται σε χαρτί, επιτρέποντας παράλληλα την εύκολη αναζήτηση και ανασκόπηση προηγούμενων πληροφοριών που αποθηκεύονται.

3.3 Παραδοσιακή Φορτωτική (B/L).

Το Bill of Landing (B/L - Παραδοσιακή Φορτωτική) είναι το βασικό έγγραφο για το διεθνές εμπόριο. Εκδίδεται από τον μεταφορέα ή τους αντιπροσώπους του για κάθε μεταφορά αγαθών. Οι τρεις κύριες λειτουργίες ενός B/L είναι:

1. Έγγραφο Τίτλου. Δείχνει τον ιδιοκτήτη του φορτίου. (παραλήπτης)

2. Σύμβαση Μεταφοράς.

3. Έγγραφο Παραλαβής, το οποίο βεβαιώνει ότι ο μεταφορέας έλαβε τα εμπορεύματα από τον αποστολέα.

Η Παραδοσιακή φορτωτική είναι ένα τυποποιημένο έντυπο, το οποίο μπορεί να μεταβιβαστεί με την επικύρωση. Η ιδιοκτησία του φορτίου μπορεί να αλλάξει χέρια κατά τη μεταφορά. Τα αποδεικτικά στοιχεία της αλλαγής κυριότητας είναι μια απλή χειρόγραφη θεώρηση σε ένα χαρτί B/L από τον παραλήπτη.

Τα 3 κύρια μέρη που εμπλέκονται στο B/L είναι ο αποστολέας, ο μεταφορέας (ή αντιπρόσωπός του) και ο παραλήπτης. Στο παρακάτω, απλοποιημένο μοντέλο μας έχουμε τις εξής λειτουργίες:

1. Ο αποστολέας (πωλητής ή εξαγωγέας) στέλνει το φορτίο με πλοίο ή με εμπορευματοκιβώτια.

2. Ο Μεταφορέας (ναυτιλιακή γραμμή, γραμμή εμπορευματοκιβωτίων, NVOCC,) λαμβάνει το φορτίο για μεταφορά και αναλαμβάνει την ευθύνη για την ποσότητα και την ποιότητα.

3. Ο Παραλήπτης (αγοραστής ή παραλήπτης).

Το διάγραμμα εξετάζει πώς λειτουργεί το σύστημα εδώ και αιώνες, συμπεριλαμβανομένου του τμήματος των κούριερ. Τα B/L αποστέλλονταν από την Ευρώπη στην Ινδία και ανάποδα ταχυδρομικώς στους παραλήπτες, ώστε οι πλοίαρχοι να μπορούν να δώσουν το φορτίο στον πραγματικό παραλήπτη! Τα πρωτότυπα τιμολόγια εξακολουθούν να εκδίδονται σε χαρτί με τον παλιό τρόπο. Υπάρχουν όμως και ορισμένα μειονεκτήματα που μπορούν να βελτιωθούν με την εισαγωγή της έξυπνης αλυσίδας και του B/L.

3.4 Μειονεκτήματα της παραδοσιακής φορτωτικής B/L.

- Ανασφαλές. Η φορτωτική B/L δεν γίνεται με ασφαλή τρόπο:

  Οι ευαίσθητες και εμπιστευτικές εμπορικές πληροφορίες μπορεί να αλλοιωθούν καθώς περνούν από τα χέρια πολλών ατόμων.

Το πρωτότυπο B/L μπορεί να χαθεί από τον κούριερ, ή στα χαρτιού του γραφείου ή μεταξύ των τμημάτων.

- Αργό. Χρειάζεται πολύ χρόνο για να παραδοθεί:

  Η παράδοση των διεθνών ταχυμεταφορών μπορεί να διαρκέσει από 3 έως και 5 ημέρες. Σε περιπτώσεις κατά τις οποίες το B/L κατατίθεται σε μια Τράπεζα σύμφωνα με τους Όρους της Συμφωνίας, έχει πολύ λίγες πιθανότητες να παραδοθεί πριν από την άφιξη του πλοίου στον προορισμό.

  Σε πολλές περιπτώσεις τα πλοία ή τα εμπορευματοκιβώτια φτάνουν πριν από το B/L. Η αργή παράδοση του B/L προκαλεί καθυστερήσεις σε ολόκληρη την αλυσίδα του εφοδιασμού.

- Κόστος. Ακριβό στην έκδοση και στην παράδοση:

  Οι διεθνείς μεταφορείς κοστίζουν από 50 έως 75 Δολάρια. Οι εμπορικές εταιρείες αποστέλλουν χιλιάδες τιμολόγια ετησίως.

  Η συμβολή στην υπερθέρμανση του πλανήτη και το σταθερό κόστος είναι σημαντικά. Σύμφωνα με την πρακτική για κάθε B/L 3 πρωτότυπα και 7 αντιτυπα εκτυπώνονται και εκδίδονται σε χαρτί. Τα σχέδια για έγκριση, εγκρίνονται εκ των προτέρων από τους φορτωτές, τους μεταφορείς, τους δέκτες και τους παραλήπτες.

  Δεν υπάρχουν στατιστικά στοιχεία σε παγκόσμια κλίμακα σχετικά με το πόσο κοστίζει η παράδοση μέσω του B/L, ποια είναι η ποσότητα των χρησιμοποιούμενων σημείων και το μέγεθος των εκτυπώσεων που δημιουργούνται από την παράδοση. Λαμβάνοντας υπόψη ότι το διεθνές εμπόριο και οι μεταφορές είναι μια βιομηχανία πολλών δισεκατομμυρίων, τα στατιστικά στοιχεία θα ανέρχονταν σε δισεκατομμύρια δολάρια ΗΠΑ και σε εκατομμύρια τόνους διοξειδίου του άνθρακα.

3.5 Μειονεκτήματα εφοδιαστικής αλυσίδας

Υπάρχουν πολλά μειονεκτήματα στην εφοδιαστική αλυσίδα που θα μπορούσαν να επισημανθούν. Στο σημείο αυτό το ενδιαφέρον θα επικεντρωθεί στη διαδικασία που υλοποιείται και πως το "έγγραφο" αυτό καθαυτό επηρεάζει την συνολική διαδικασία. Αυτό αποτελεί μήλο της Έριδος για όποιον προσπαθεί να βελτιστοποιήσει την εφοδιαστική και την παγκόσμια βιομηχανία του εμπορίου. Ο κανόνας 80/20 ισχύει: με 20% προσπάθεια μπορεί να λυθεί το 80% του προβλήματος.

Οι άνθρωποι εξακολουθούν να δαπανούν δισεκατομμύρια δολάρια κάθε χρόνο για έγγραφα που μετακινούνται σε όλο τον κόσμο. Ακολουθούν τον ίδιο ακριβώς τρόπο όπως οι πρόγονοί τους, με ταχυδρομικές εταιρείες. Τα έγγραφα που υπάρχουν στην εφοδιαστική αλυσίδα που θα μεταφερθούν είναι πολλά.

Στον τομέα της ναυτιλίας ένα έγγραφο που έχει σημαντικό ρόλο είναι τα τιμολόγια (Bill of Landing - B/L). Τα τιμολόγια χρησιμοποιούνται για τη μεταφορά δικαιωμάτων ιδιοκτησίας στο παγκόσμιο εμπόριο για αιώνες, διατηρώντας την τάξη σε ένα περίπλοκο ιστό εμπορικών δικτύων και εταιρικών σχέσεων.

Ένα άλλο επίσης ευρέως χρησιμοποιούμενο έγγραφο που υποστηρίζει το παγκόσμιο εμπόριο είναι η επιστολή πίστωσης (Letter of Credit - L/C). Τόνοι χαρτί χρησιμοποιούνται για τις πολύπλοκες αυτές διαδικασίες οι οποίες είναι δαπανηρές, απαιτούν χρόνο για να ολοκληρωθούν και εκδίδονται μόνο από τράπεζες. Η διαδικασία L/C είναι εξ ολοκλήρου σε χαρτί και απαιτεί πολλές εισροές έγγραφων, συμπεριλαμβανομένου σχεδόν πάντα ενός Bill of Lading.

Το τρίτο βασικό έγγραφο στο παγκόσμιο εμπόριο είναι το Πιστοποιητικό Ασφάλισης.

Όπως φαίνεται από την παρακάτω εικόνα (Εικόνα 3.1), οι κυριότεροι παράγοντες στο παγκόσμιο εμπόριο είναι:

- Παραγωγός - Κατασκευαστής - Εξαγωγέας - Αποστολέας (παραγγέλνουν και πληρώνουν για την μεταφορά)
- NVOCC - Εταιρεία Μεταφορών- Ναυλωτής
- Μεταφορική γραμμή - Μεταφορέας
- Εισαγωγέας - Αγοραστής
- Αντιπρόσωπος Απαλλαγής
- Τράπεζα Εισαγωγέων
- Τράπεζα Εξαγωγέα
- Ασφαλιστικός φορέας

Επειδή τα έγγραφα που σχετίζονται με το παγκόσμιο εμπόριο είναι φυσικά έγγραφα (χαρτί), δημιουργούν μια σχετική ταλαιπωρία στη διαχείριση και την αποστολή ενός φυσικού αντικειμένου.

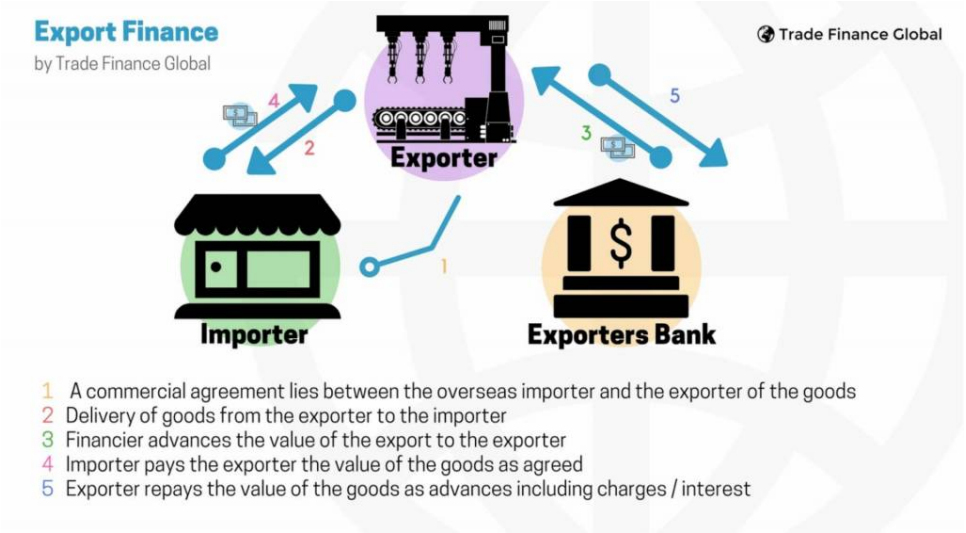
- Προβλήματα σχετικά με την ταχύτητα.

  Χρειάζεται πολύ μεγάλο χρονικό διάστημα για να σταλεί ένα B/L με συμβατικό τρόπο. Ο εκδότης (μεταφορέας ή NVOCC) το αποστέλλει στον αποστολέα (1-2 ημέρες), ο αποστολέας το αποστέλλει στον παραλήπτη/ή σε μια τράπεζα του παραλήπτη (3-5 ημέρες), τέλος, ο παραλήπτης το στέλνει σε (1-2 ημέρες). Συνολικά, κάθε B/L ταξιδεύει με τουλάχιστον 3 υπηρεσίες ταχυμεταφορών και η διαδικασία αποστολής-παραλαβής είναι από 5-10 ημέρες, καθιστώντας το πιο επιρρεπές σε απώλεια ή ακόμα και κλοπή.

- Προβλήματα σχετικά με τα φυσικά έγγραφα.

  Το αρχικό έγγραφο B/L μπορεί να χαθεί, να σταλεί σε λάθος χέρια ή ακόμα και να κλαπεί. Αυτό το πρόβλημα γίνεται αισθητό κυρίως από τους παραλήπτες, που πρέπει να δηλώσουν επισήμως το B/L χαμένο και να περιμένουν εβδομάδες ένα νέο. Ακόμα χειρότερα, αυτό μπορεί να απαιτεί επιπρόσθετα έξοδα, όπως η απόσβεση και η κράτηση στο λιμάνι του προορισμού, οι ποινές άφιξης αργοπορημένου φορτίου και ακόμη χειρότερα και την παύση εργασιών του εργοστασίου, γεγονός που μπορεί να οδηγήσει σε απώλεια πολλών εκατομμυρίων δολαρίων.

- Προβλήματα σχετικά με το κόστος.



Εικόνα 3.1: Κυριότεροι παράγοντες παγκοσμίου εμπορίου. https://www.tradefinanceglobal.com/export-finance/ (22/3/2019)

Στις μέρες μας κάθε έγγραφο πρέπει να εκτυπώνεται σε χαρτί. Αυτό το φυσικό αντικείμενο (το οποίο έχει υψηλή αξία) πρέπει να αποσταλεί κατ΄Α ελάχιστο 3 φορές μέσω εταιρειών ταχυμεταφορών, όπως οι UPS, Fedex, και άλλες, μια διαδικασία που είναι τόσο χρονοβόρα όσο και εξαιρετικά ακριβή. Η απώλεια ή η εσφαλμένη τοποθέτηση ενός εγγράφου αυξάνει το κόστος, πράγμα που σημαίνει ότι πολλά φορτία επηρεάζονται. Ο μέσος όρος των εξόδων ταχυμεταφοράς είναι 100 δολάρια ΗΠΑ, για κάθε B/L.

- Προβλήματα σχετικά με την νοθεία.

  Τα έγγραφα B/L εκτυπώνονται συνήθως σε εταιρικά επιστολόχαρτα (με το λογότυπο του εκδότη). Αυτό το επιστολόχαρτο μπορεί να κλαπεί ή να χαθεί και στις μέρες μας αποτελεί τη βάση για απάτη και εγκληματική δραστηριότητα. Η εκδότρια εταιρεία "μπλέκει" και ενδέχεται να αντιμετωπίσει ποινική έρευνα ή τουλάχιστον αρνητική δημοσιότητα και διατάραξη ή υπονόμευση της λειτουργικότητας της. Αντικαθιστώντας την μεταφορά των εγγράφων B/L από φυσικό χαρτί μέσω της εφοδιαστικής αλυσίδας, αυτό αποφεύγεται τελείως.

Κεφάλαιο 4

Κρυπτονομίσματα και η εφοδιαστική αλυσίδα

4.1 Προσέγγιση του προβλήματος

Η εφοδιαστική αλυσίδα έχει γίνει πολύπλοκη. Χρειάζονται αρκετές ημέρες για να πραγματοποιηθεί μια πληρωμή μεταξύ ενός κατασκευαστή και ενός προμηθευτή ή ενός πελάτη και ενός πωλητή. Οι συμβατικές συμφωνίες απαιτούν τις υπηρεσίες δικηγόρων και τραπεζιτών, καθεμία από τις οποίες προσθέτει επιπλέον κόστος και καθυστέρηση. Τα προϊόντα και τα εξαρτήματα συχνά είναι δύσκολο να εντοπιστούν στους προμηθευτές, καθιστώντας τα προβλήματα, δύσκολα στην επίλυση.

Η αύξηση της αβεβαιότητας εμποδίζει τις εφοδιαστικές αλυσίδες να λειτουργούν σωστά. Οι προμηθευτές, οι πωλητές και οι πελάτες πρέπει να αλληλεπιδρούν μέσω κεντρικών οντοτήτων τρίτου μέρους, αντί να συνδέονται άμεσα μεταξύ τους. Φαινομενικά απλές συναλλαγές μετατρέπονται σε μακροχρόνιες διαδικασίες πολλαπλών βημάτων.

Το Blockchain θα μπορούσε να είναι η απάντηση σε πολλά από αυτά τα ζητήματα. Αυτή η τεχνολογία είναι αυτή που οδηγεί στην εξέλιξη των κρυπτονομισμάτων. Το Blockchain μπορεί να διαχειριστεί οποιαδήποτε μορφή ανταλλαγής, συμφωνίας ή παρακολούθησης. Σε μια εφοδιαστική αλυσίδα, μπορεί να εφαρμοστεί σε οποιαδήποτε από τις συμβάσεις εφοδιασμού που πραγματοποιούνται με την αυτοματοποιημένη διαχείριση της αλυσίδας. [17]

4.2 Μηχανισμοί Ασφάλειας Δικτύου

Το μεγαλύτερο τεχνολογικό επίτευγμα του Bitcoin (και η εκ των ων ουκ άνευ για κάθε κρυπτονόμισμα) είναι η κατασκευή ενός συστήματος συναλλαγών peer-to-peer που στηρίζεται στην κρυπτογραφική απόδειξη αντί για την εμπιστοσύνη. Ωστόσο, αντικαθιστώντας μια κεντρική αρχή, παρουσιάζει ένα μοναδικό πρόβλημα με μια λύση που δεν είναι προφανής.

Πρώτον, το νόμισμα θα πρέπει να είναι σε θέση να αλλάζει κατόχους. Οι συναλλαγές καταγράφονται με το συνδυασμό των ψηφιακών υπογραφών από κάθε μέλος και μία χρονοσήμανση, έτσι ώστε η ημερομηνία της συναλλαγής να καταγράφεται. Ο νέος αυτός κώδικας αντιπροσωπεύει το νόμισμα και τη διαδρομή του μέσω του δικτύου. Αυτός ο κώδικας στη συνέχεια μεταδίδεται σε όλους τους κόμβους του δικτύου (υπολογιστές που είναι συνδεδεμένοι και τρέχουν το λογισμικό του δικτύου των κρυπτονομισμάτων).

Ωστόσο, είναι απαραίτητο η πλειοψηφία των κόμβων να συμφωνήσουν σχετικά με τις συναλλαγές που έχουν συμβεί, αλλιώς μπορεί να προκύψουν διπλές δαπάνες και denial-of-service (DoS). Ο μηχανισμός που χρησιμοποιείται για την επίτευξη συναίνεσης μεταξύ των κόμβων ενισχύει την ακεραιότητα του συστήματος επαληθεύοντας ότι η συναλλαγή είναι πράγματι νόμιμη.

Ως εκ τούτου, οι συναλλαγές επαληθεύονται, και το σύστημα καθίσταται ασφαλές, από την εφαρμογή ορισμένων μηχανισμών που καθιστούν υπερβολικά δαπανηρή την παραβίαση της ακεραιότητας του συστήματος. Η βασική αρχή ενός τέτοιου μηχανισμού είναι η αναγκαιότητα της δαπάνης πόρων κατά την επιβεβαίωση των συναλλαγών.

Διάφορα κρυπτονομίσματα έχουν αναπτύξει νέα εργαλεία για τη χρήση ως μέσο ασφάλειας του δικτύου. Ο πόρος που πρέπει να καταναλώνεται μπορεί να είναι ένας συνδυασμός ηλεκτρικής ενέργειας, χρόνου, ή η προσωρινή παράδοση του νομίσματος, και αντιπροσωπεύει το κόστος για την ασφάλεια του δικτύου. Οι χρήστες που κάνουν εξόρυξη κρυπτονομισμάτων - εκείνοι που κατέχουν τον υποκείμενο πόρο, και ως εκ τούτου μπορούν να τον δαπανήσουν - εργάζονται για την ασφάλεια του δικτύου, και αμείβονται για την εργασία τους με τη μορφή συναλλαγών ή νέων κρυπτονομισμάτων.

Ο μηχανισμός που χρησιμοποιείται για την εξασφάλιση της ακεραιότητας του δικτύου καθορίζει τον πόρο και τη μέθοδο που χρησιμοποιείται για την αμοιβή τους. Έτσι, ο υποκείμενος μηχανισμός της ασφάλειας του δικτύου κάθε κρυπτονομίσματος έχει σημαντική επίπτωση επί της υποκείμενης οικονομίας του νομίσματος. Στις επόμενες παραγράφους παρουσιάζονται αναλυτικά οι πιο ευρέως χρησιμοποιούμενοι μηχανισμοί στη βιομηχανία των κρυπτονομισμάτων.

4.2.1 Proof-of-work (POW).

Ένα σύστημα απόδειξης εργασίας (POW) ή πρωτόκολλο, ή λειτουργία, είναι ένα οικονομικό μέτρο για την αποτροπή επιθέσεων άρνησης παροχής υπηρεσίας και άλλων καταχρήσεων των υπηρεσιών, όπως το spam σε ένα δίκτυο, απαιτώντας κάποια εργασία από τον αιτούντα υπηρεσία, που συνήθως σημαίνει μεγαλύτερο χρόνο επεξεργασίας από έναν υπολογιστή.

Ένα βασικό χαρακτηριστικό των συστημάτων αυτών είναι η ασυμμετρία τους: η εργασία πρέπει να είναι μέτρια έως σκληρή (αλλά εφικτή) από την πλευρά του αιτούντος, αλλά εύκολη να ελεγχθεί και από τον πάροχο των υπηρεσιών. Η ιδέα αυτή είναι επίσης γνωστή ως μια συνάρτηση κόστους. Είναι διαφορετική από το CAPTCHA, το οποίο προορίζεται για έναν άνθρωπο, ώστε να το λύσει γρήγορα, παρά έναν υπολογιστή.

Υπάρχουν δύο κατηγορίες πρωτοκόλλων απόδειξης της εργασίας:

1. Πρωτόκολλα πρόκλησης-απόκρισης που αναλαμβάνουν μια άμεση διαδραστική σχέση μεταξύ του αιτούμενου (client) και του παρόχου (server). Ο πάροχος επιλέγει μια πρόκληση, δηλαδή ένα στοιχείο σε ένα σύνολο με μια ιδιότητα, ο αιτών κρίνει τη σχετική απόκριση στο σύνολο, η οποία αποστέλλεται πίσω και να ελέγχεται από τον πάροχο. Δεδομένου ότι η πρόκληση θα επιλεγεί επί τόπου από τον πάροχο, η δυσκολία της μπορεί να προσαρμοστεί άμεσα. Οι εργασίες από την πλευρά του αιτούντος δύνανται να ορίζονται εάν το πρωτόκολλο πρόκλησης-απόκρισης έχει μια γνωστή λύση (επιλέγεται από τον πάροχο), ή είναι γνωστό ότι υπάρχει μέσα σε ένα οριοθετημένο χώρο αναζήτησης.

2. Τα πρωτόκολλα επίλυσης-επαλήθευσης δεν δεσμεύουν μια τέτοια σύνδεση: ως εκ τούτου το πρόβλημα πρέπει να επιβληθεί πριν αναζητηθεί λύση από τον αιτούντα, και ο πάροχος πρέπει να ελέγχει τόσο την επιλογή του προβλήματος όσο και τη λύση. Τα περισσότερα τέτοια συστήματα είναι μη οριοθετημένα με πιθανολογικές επαναληπτικές διαδικασίες, όπως οι μετρητές κατακερματισμού (Hashcash).

Πρωτόκολλα γνωστής λύσης τείνουν να έχουν ελαφρώς χαμηλότερη διακύμανση από τα πιθανολογικά πρωτόκολλα, επειδή η διακύμανση της ορθογώνιας διανομής είναι μικρότερη από την διακύμανση της κατανομής Poisson (με την ίδια μέση τιμή). Μια γενική τεχνική για τη μείωση της διακύμανσης είναι η χρήση πολλαπλών ανεξάρτητων υπο-προκλήσεων, καθώς ο μέσος όρος των πολλαπλών δειγμάτων που θα έχει χαμηλότερη διακύμανση.

Υπάρχουν επίσης συναρτήσεις σταθερού κόστους. Επιπλέον, οι βασικές λειτουργίες που χρησιμοποιούνται από τα συστήματα αυτά μπορεί να είναι:

- Συνδεδεμένα με τη CPU εφόσον ο υπολογισμός τρέχει με την ταχύτητα του επεξεργαστή, η οποία ποικίλλει σημαντικά σε χρόνο, καθώς και από υψηλής ταχύτητας σέρβερ έως χαμηλής ταχύτητας φορητές συσκευές.

- Συνδεδεμένα με τη μνήμη όταν η ταχύτητα υπολογισμού δεσμεύεται από κύριες προσβάσεις μνήμης (είτε λανθάνουσες ή στο εύρος ζώνης), η απόδοση των οποίων αναμένεται να είναι λιγότερο ευαίσθητη στην εξέλιξη του υλικού.

- Συνδεδεμένα με το Δίκτυο, εάν ο πελάτης πρέπει να εκτελέσει μερικούς υπολογισμούς, αλλά πρέπει να μαζέψει κάποια στοιχεία από απομακρυσμένους διακομιστές πριν απευθυνθεί στον τελικό φορέα παροχής υπηρεσιών. Με αυτή την έννοια το έργο δεν εκτελείται από τον αιτούντα, αλλά συνεπάγεται καθυστερήσεις ούτως ή άλλως.

Τέλος, ορισμένα συστήματα POW προσφέρουν συντόμευση υπολογισμών που επιτρέπουν στους συμμετέχοντες που γνωρίζουν το μυστικό, συνήθως ιδιωτικό κλειδί, για να δημιουργήσουν φτηνές αποδείξεις εργασίας. Το σκεπτικό είναι ότι οι κάτοχοι μιας λίστας αλληλογραφίας μπορούν να δημιουργήσουν σφραγίδες για κάθε δικαιούχο, χωρίς αυτό να συνεπάγεται υψηλό κόστος. Αν ένα τέτοιο χαρακτηριστικό είναι επιθυμητό εξαρτάται από το εκάστοτε σενάριο χρήσης.

Ο επιστήμονας υπολογιστών Hal Finney (2007) βασίστηκε στην ιδέα της απόδειξης της εργασίας, αποδίδοντας ένα σύστημα που εκμεταλλεύεται την επαναχρησιμοποιήσιμη απόδειξη της εργασίας «RPOW». Είχε ήδη καθιερωθεί η ιδέα της δημιουργίας επαναχρησιμοποιήσιμων αποδείξεων-τησ-εργασίας για κάποιο πρακτικό σκοπό από το 1999.

Σκοπός του Finney με τη χρήση του RPOW ήταν ως συμβολικά χρήματα. Ακριβώς όπως η τιμή χρυσού νομίσματος είναι πιθανό να υποστηρίζεται από την αξία του χρυσού που απαιτείται για να κατασκευαστεί το νόμισμα, η αξία ενός νομίσματος RPOW είναι εγγυημένη από την αξία των πραγματικών πόρων που απαιτούνται για την δημιουργία του. Στην έκδοση της RPOW του Finney, η POW αποτελεί ένα κομμάτι του μετρητή κατακερματισμού.

Ένας δικτυακός τόπος μπορεί να απαιτήσει ένα συμβολικό POW αντάλλαγμα της υπηρεσίας. Η απαίτηση του συμβολικού POW από τους χρήστες θα αναστείλει την επιπόλαιη ή υπερβολική χρήση της υπηρεσίας, απαλλάσσοντας υποκείμενους πόρους της υπηρεσίας, όπως το εύρος ζώνης στο Internet, ο υπολογισμός, ο χώρος στο δίσκο, η ηλεκτρική ενέργεια και τα συνολικά διοικητικά έξοδα.

Το σύστημα RPOW του Finney διαφέρει από ένα POW σύστημα στο ότι επιτρέπει τη τυχαία ανταλλαγή νομισμάτων χωρίς να επαναληφθούν οι εργασίες που απαιτούνται για τη

δημιουργία του. Αφού κάποιος περάσει μια συμβολική POW σε μια ιστοσελίδα, ο φορέας εκμετάλλευσης του δικτυακού τόπου θα μπορούσε να ανταλλάξει το POW για ένα νέο, μη χρησιμοποιημένο συμβολικό RPOW, το οποίο θα μπορούσε στη συνέχεια να δαπανηθεί σε κάποια ιστοσελίδα τρίτου ομοίως εξοπλισμένη για να δεχτεί νομίσματα RPOW. Αυτό θα εξοικονομήσει πόρους που διαφορετικά θα χρειαζόταν για τη δημιουργία μιας συμβολικής POW.

Η μη πλαστή περιουσία του διακριτικού RPOW είναι εγγυημένη από την απομακρυσμένη πιστοποίηση. Ο διακομιστής RPOW που ανταλλάσσει ένα μεταχειρισμένο RPOW κουπόνι με ένα νέο ίσης αξίας χρησιμοποιεί απομακρυσμένη πιστοποίηση για να επιτρέψει σε κάθε ενδιαφερόμενο να εξακριβώσει τι λογισμικό εκτελείται στον διακομιστή RPOW. Δεδομένου ότι ο πηγαίος κώδικας για το λογισμικό RPOW του Finney δόθηκε στη δημοσιότητα (στο πλαίσιο μιας άδειας τύπου BSD), κάθε προγραμματιστής με επαρκή γνώση θα μπορούσε, κατά την επιθεώρηση του κώδικα, να βεβαιωθεί ότι το λογισμικό (και, κατ έπέκταση, ο διακομιστής RPOW) ουδέποτε εξέδωσε ένα νέο κουπόνι εκτός σε αντάλλαγμα για μια συμβολική RPOW ίσης αξίας.

Μέχρι το 2009, το σύστημα Finney ήταν το μόνο σύστημα RPOW που είχε υλοποιηθεί, αλλά ποτέ δεν είδε οικονομικά σημαντική χρήση. Το 2009, το δίκτυο του Bitcoin βγήκε στην κυκλοφορία. Το Bitcoin είναι ένα κρυπτονόμισμα απόδειξης εργασίας, όπως το RPOW του Finney, αλλά βασίζεται επίσης στον μετρητή κατακερματισμού POW.

Η προστασία στο Bitcoin παρέχεται από ένα αποκεντρωμένο P2P πρωτόκολλο για την παρακολούθηση της μεταφοράς των νομισμάτων, σε αντίθεση με το υλικό εμπιστοσύνης στη λειτουργία των υπολογιστών που χρησιμοποιούνται από το RPOW. Το Bitcoin έχει καλύτερη αξιοπιστία, επειδή προστατεύεται από τους υπολογισμούς. Το RPOW προστατεύεται από τα ιδιωτικά κλειδιά που αποθηκεύονται στο υλικό TPM και οι κατασκευαστές κατέχουν τα ιδιωτικά κλειδιά του TPM.

Οι χάκερ που κλέβουν ένα κλειδί TPM, ή οποιοσδήποτε ικανός να αποκτήσει το κλειδί με την εξέταση του ίδιου του TPM chip, θα μπορούσαν να ανατρέψουν αυτή τη διαβεβαίωση. Τα Bitcoins εξορύσσονται χρησιμοποιώντας το μετρητή κατακερματισμού με τη λειτουργία απόδειξης της εργασίας από μεμονωμένους κόμβους και επαληθεύοντας το με το αποκεντρωμένο δίκτυο P2P του Bitcoin.

4.2.2 Proof-of-stake

Η απόδειξη της συμμετοχής ή επιτοκίου (proof-of-stake) είναι μια μέθοδος με την οποία ένα δίκτυο κρυπτονομισμάτων αποσκοπεί στην επίτευξη κατανεμημένης συναίνεσης. Αν και η μέθοδος απόδειξης της εργασίας ζητά από τους χρήστες να τρέχουν επανειλημμένα αλγόριθμους κατακερματισμού για την επικύρωση των ηλεκτρονικών συναλλαγών, η απόδειξη της συμμετοχής ζητά από τους χρήστες να αποδείξουν την κυριότητα σε ένα ορισμένο ποσό του νομίσματος («συμμετοχής» τους στο νόμισμα). Το Peercoin ήταν το πρώτο κρυπτονόμισμα που χρησιμοποίησε την απόδειξη του επιτοκίου. Άλλες εξέχουσες αλυσίδες είναι τα BitShares, NXT, BlackCoin, NuShares / NuBits και Qora.

Η απόδειξη της εργασίας βασίζεται στη χρήση της ενέργειας. Σύμφωνα με τον διαχειριστή εξόρυξης Bitcoin, η κατανάλωση ενέργειας ανήλθε στις 240 kWh ανά Bitcoin το 2014 (ισοδύναμο με 16 γαλόνια φυσικού αερίου). Επιπλέον, οι δαπάνες της ενέργειας σχεδόν πάντα καταβάλλονται σε παραδοσιακό χρήμα, εισάγοντας μια σταθερή πτωτική πίεση στην τιμή. Η μέθοδος απόδειξης επιτοκίου μπορεί να είναι αρκετές χιλιάδες φορές πιο αποδοτική.

Τα κίνητρα της γεννήτριας μπλοκ είναι επίσης διαφορετικά. Υπό την απόδειξη της εργασίας, η γεννήτρια μπορεί δυνητικά να μην κατέχει κανένα από τα νομίσματα που παράγονται από την εξόρυξη. Το κίνητρο του ανθρακωρύχου είναι μόνο να μεγιστοποιήσει τα δικά του κέρδη. Δεν είναι σαφές αν αυτή η ανισότητα μειώνει ή αυξάνει τους κινδύνους ασφαλείας. Στην Απόδειξη της συμμετοχής, αυτοί που φυλάσσουν τα νομίσματα είναι πάντα αυτοί που κατέχουν τα νομίσματα (αν και αρκετά κρυπτονομίσματα επιτρέπουν ή επιβάλλουν τον δανεισμό της δυνατότητας συμμετοχής σε άλλους κόμβους).

4.2.3 Υβριδικός μηχανισμός POW/POS

Ένα υβριδικό σύστημα Pow / POS χρησιμοποιεί τον μηχανισμό Pow για την αρχική κοπή και διανομή κερμάτων. Δηλαδή, ο Pow επιτρέπει στο δίκτυο τη διανομή των νέων νομισμάτων προς εκείνους που εξορύσουν τα νομίσματα. Ωστόσο, με την πάροδο του χρόνου, ο μηχανισμός PoS σβήνει τον μηχανισμό Pow, δημιουργώντας ένα μακροπρόθεσμα ενεργειακά αποδοτικό κρυπτονόμισμα.

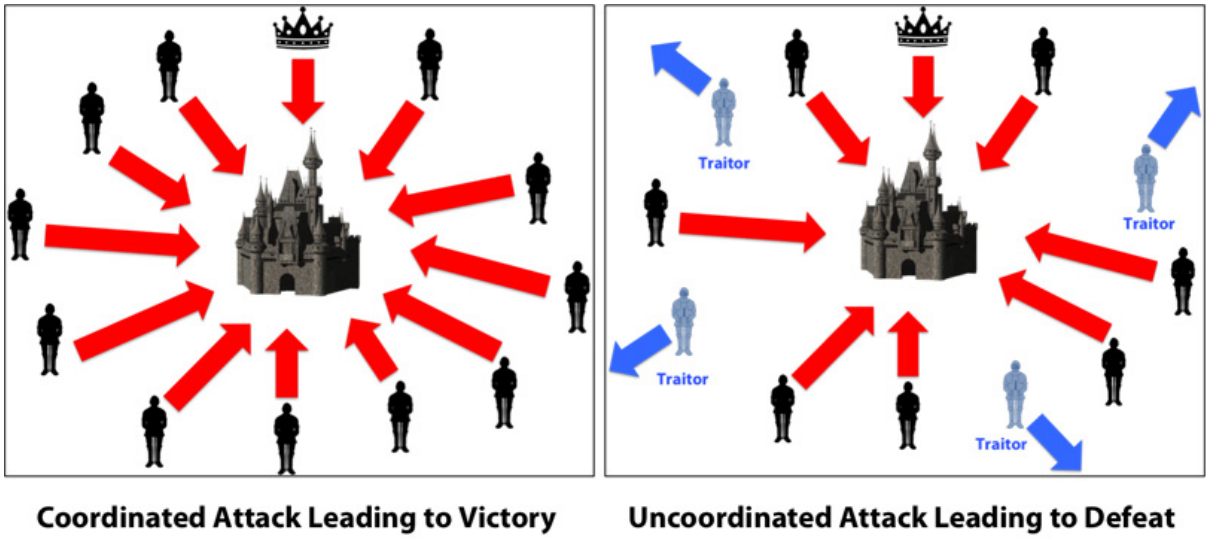
Οι Sunny King και Scott Nadal (2013), στο εγχειρίδιο "PPCoin: Peer-to-Peer Crypto-Νόμισμα με απόδειξη-τησ-Συμμετοχής", είναι οι πρώτοι που προτείνουν και στη συνέχεια εφαρμόζουν ένα τέτοιο υβριδικό σύστημα POW / POS. Σε αυτόν τον υβριδικό σχεδιασμό, η παραγωγή μπλοκ, αντί να βασίζεται σε μία CPU ανά ψήφο, βασίζεται στην έννοια του πλήθους νομισμάτων ή coinage.

Το coinage είναι περίπου το πλήθος νομισμάτων ενός ιδιοκτήτη πολλαπλασιασμένο με το χρόνο της κυριότητας από τον σημερινό ιδιοκτήτη του νομίσματος. Η παραγωγή μπλοκ πηγαίνει έτσι στο μπλοκ με το πιο πολλά νομίσματα (ανάλογα με το coinage). Περαιτέρω, τα νομίσματα δημιουργούνται κατά μία ποσοστιαία μονάδα της κατανάλωσης ανά έτος, η οποία λειτουργεί ως επιτόκιο για το νόμισμα. Το κύριο πλεονέκτημα, ωστόσο, είναι ότι αυτό το σύστημα δεν βασίζεται σε υψηλή κατανάλωση ενέργειας μακροπρόθεσμα. Ως εκ τούτου, το σχέδιο είναι οικονομικά ανταγωνιστικό σε σύγκριση με εκείνο που βασίζεται σε Pow και αποφεύγει το πρόβλημα της διανομής.

4.2.4 Μηχανισμός συναίνεσης (Byzantine Consensus)

Τα κρυπτονομίσματα Ripple και Stellar διαθέτουν έναν εξ ολοκλήρου εναλλακτικό μηχανισμό ασφαλείας, που αποτελεί υλοποίηση του πρωτοκόλλου «Byzantine Consensus» (Εικόνα 4.1). Η υποδομή των νομισμάτων είναι αυτή ενός κατανεμημένου δικτύου, όπου κάθε server του δικτύου είναι αντιμέτωπος με το πρόβλημα του να αποφασίσει αν οι άλλοι διακομιστές στο δίκτυο αποστέλλουν έγκυρα μηνύματα. Τα μηνύματα σε αυτή την περίπτωση είναι συναλλαγές. Αυτό το σύστημα είναι ανθεκτικό στην κατηγορία των αποτυχιών που είναι γνωστή ως προβλήματα Byzantine Generals και ως εκ τούτου θεωρείται ανθεκτικό στην οικογένεια αυτή προβλημάτων. Σε αυτού του τύπου τα προβλήματα, ο "βυζαντινός στρατός" σαν παράδειγμα διχάζεται ανάμεσα σε πολλούς υπαξιωματικούς που λαμβάνουν εντολή για επίθεση ή υποχώρηση από έναν γενικό διοικητή. Ωστόσο, υπάρχει ένας αριθμός των προδοτών - ενδεχομένως ο ίδιος ο γενικός διοικητής - ενώ όλοι οι πιστοί στρατηγοί πρέπει να καταλήξουν σε συμφωνία μεταξύ τους, ενώ θα πρέπει να αποκλείσουν τους προδότες για να αποτρέψουν τα σχέδια τους. Το πρόβλημα είναι ότι οι πιστοί υπαξιωματικοί πρέπει να καταλήξουν σε συναίνεση σχετικά με το ποια εντολή να υπακούσουν, στέλνοντας μεταξύ τους υπογεγραμμένα μηνύματα. Διάφοροι αλγόριθμοι έχουν προταθεί ως αποτελεσματικοί για το ανωτέρω πρόβλημα.

Τα κατανεμημένα δίκτυα που δημιουργούνται από τα κρυπτονομίσματα Ripple και Stellar αντιμετωπίζουν ένα πρόβλημα ανάλογο με το παραπάνω. Πρώτον, άτομα που εμπλέκονται με ένα από αυτά τα νομίσματα θα πρέπει να ενταχθούν σε ένα διακομιστή. Κάθε διακομιστής στο δίκτυο βρίσκεται αντιμέτωπος με το πρόβλημα του να αποφασίσει αν άλλοι servers στο δίκτυο στέλνουν ακριβή "μηνύματα", το οποίο στην προκειμένη περίπτωση είναι συναλλαγές. Το πρωτόκολλο του Ripple απαιτεί οι οικονομικές οντότητες να εντάσσονται σε ένα διακομιστή. Κάθε διακομιστής διατηρεί μια λίστα με μοναδικούς Κόμβος (UNL), σύμφωνα



Εικόνα 4.1: Μηχανισμός συναίνεσης - Byzantine Consensus. https://blockonomi.com/practical-byzantine-fault-tolerance/ (23/3/2019)

με την οποία ο διακομιστής επικοινωνεί μόνο με τους κόμβους στο UNL του. Αυτό επιτρέπει στους διακομιστές να είναι σε επαφή μόνο με αξιόπιστους διακομιστές. Κάθε διακομιστής μπορεί να μεταδώσει τις συναλλαγές, και οι διακομιστές ψηφίζουν επί των συναλλαγών. Ωστόσο, οι διακομιστές ψηφίζουν μόνο για συναλλαγές που προέρχονται από άλλους κόμβους του UNL.

Κάθε λίγα δευτερόλεπτα, όλοι οι διακομιστές στέλνουν μηνύματα εμπρός και πίσω, έως ότου ο αλγόριθμος να τερματιστεί με συναίνεση ή αδυναμία να επιτευχθεί συναίνεση. Ο συγκεκριμένος αλγόριθμος που χρησιμοποιείται στο δίκτυο Ripple απαιτεί ότι η συναλλαγή γίνεται αποδεκτή από το 80 τοις εκατό των servers, για την επίτευξη συναίνεσης. Αυτός ο μηχανισμός ασφαλείας είναι πιο ενεργειακά αποδοτικός από το μηχανισμό Pow, απαιτεί τουλάχιστον μια επίθεση 80% στο δίκτυο, προκειμένου να παραβιαστεί η ασφάλεια του δικτύου (ο αλγόριθμος τερματίζει χωρίς συναίνεση, εάν δεν υπάρχει συμφωνία 80%), επιτρέπει ευέλικτη εμπιστοσύνη, και προσφέρει ταχύτερους χρόνους συναλλαγής.

Κεφάλαιο 5

Έξυπνα συμβόλαια και κρυπτονομίσματα

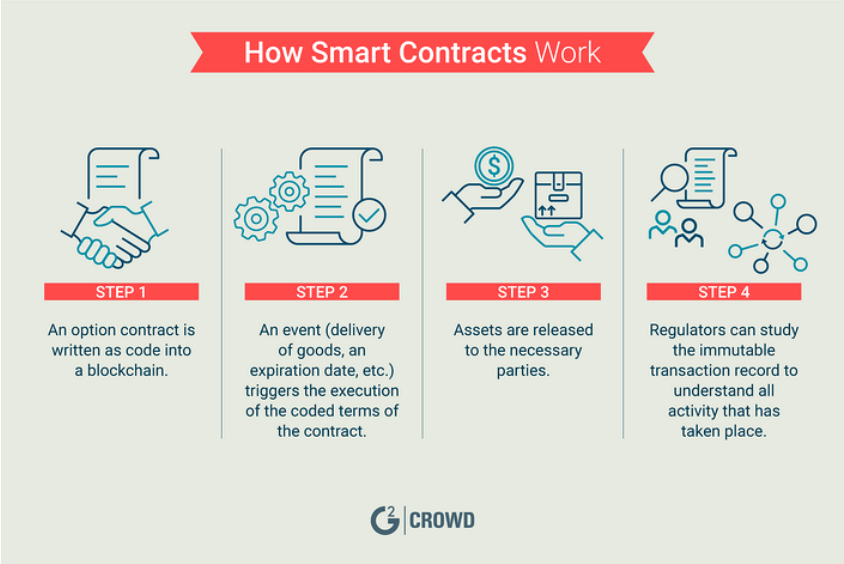
5.1 Ορισμός έξυπνων συμβολαίων

Ένα έξυπνο συμβόλαιο είναι ένα πρωτόκολλο ηλεκτρονικού υπολογιστή προοριζόμενο να διευκολύνει ψηφιακά, να επαληθεύσει ή να επιβάλει τη διαπραγμάτευση ή την εκτέλεση ενός συμβολαίου. Τα έξυπνα συμβόλαια επιτρέπουν την εκτέλεση αξιόπιστων συναλλαγών χωρίς τρίτους. Οι συναλλαγές αυτές είναι παρακολουθούμενες και μη αναστρέψιμες (Εικόνα 5.1).

Ο στόχος των έξυπνων συμβολαίων είναι να παρέχουν ενισχυμένη ασφάλεια και να μειώσουν τα άλλα κόστη συναλλαγών που συνδέονται με τη σύναψη συμβολαίων. Πολλά κρυπτονομίσματα έχουν εφαρμόσει τύπους έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια σχεδιάστηκαν αρχικά από τον Nick Szabo, ο οποίος και δημιούργησε τον όρο. Για παράδειγμα, σύμφωνα με τον Οργανισμό του Ethereum ή την IBM, ένα έξυπνο συμβόλαιο δεν συνδέεται κατΆ ανάγκη με την κλασική έννοια του συμβολαίου, αλλά μπορεί να είναι οποιοδήποτε είδος προγράμματος ηλεκτρονικού υπολογιστή. [18]

Το 2018, σε ένα δημοσίευμα της Γερουσίας των ΗΠΑ αναρτήθηκε η εξής δήλωση: "Παρόλο που τα έξυπνα συμβόλαια μπορεί να φαίνονται ως ένας νέος όρος, η έννοια βασίζεται στο βασικό δίκαιο των συμβολαίων. Συνήθως, το δικαστικό σύστημα εκδικάζει συμβατικές διαφορές και επιβάλλει όρους, αλλά είναι επίσης συνηθισμένο να υπάρχει και άλλος τρόπος επίλυσης ζητημάτων για διεθνείς συναλλαγές. Με τα έξυπνα συμβόλαια, εισάγονται οι όροι του συμβολαίου, όπως υπάρχουν στα νομικά πλαίσια. "

Ένα παράδειγμα έξυπνου συμβολαίου αποτελεί το Σύστημα Αλυσίδας της Thomson



Εικόνα 5.1: Έξυπνα Συμβόλαια - Smart Contracts (1/2). https://learn.g2crowd.com/smart-contracts (19/3/2019)

Reuters για τη διαχείριση της ταυτότητας των χρηστών. [19]

5.2 Πλεονεκτήματα έξυπνων συμβολαίων

Τα έξυπνα συμβόλαια (Εικόνα 5.2) υλοποιούν διαφορετικές διαδικασίες αυτόματα, χωρίς να χρειάζεται να εποπτεύεται η υλοποίηση του συμβολαίου. [20] Οι διαδικασίες γίνονται:

- Αυτόματα - ό, τι προδιαγράφεται σε ένα συμβόλαιο θα γίνει.
- Γρήγορα - ο χρόνος υλοποίησης είναι της τάξης των δευτερολέπτων.
- Άμεσα - δεν εμπλέκονται μεσάζοντες.
- Οικονομικά - δεν πληρώνονται τέλη.
- Με διαφάνεια - όλες οι πληροφορίες καταχωρούνται στο blockchain.

Πολλά παραδείγματα εφαρμογής έξυπνων συμβολαίων αποδεικνύουν πόσο επωφελή είναι όταν υλοποιούνται σωστά. [21]

Εικόνα 5.2: Έξυπνα Συμβόλαια - Smart Contracts (2/2). https://cryptooa.com/what-is-smart-contract/ (24/3/2019)

5.3 Ψηφιακή Ταυτότητα (Digital Identity)

Στη σύγχρονη εποχή, διαφορετικοί οργανισμοί έχουν πολλές λεπτομέρειες για τη ζωή των ανθρώπων - τραπεζικά αρχεία, δικαιώματα ιδιοκτησίας, λεπτομέρειες εργασίας, δημογραφικά γεγονότα, ενδιαφέροντα, χόμπι κλπ. Για να συγκεντρωθούν όλες αυτές οι πληροφορίες σε ένα φάκελο, χρειάζεται να μεταφερθεί τεράστιος όγκος χαρτιών, αναφορών και αντιγράφων. Είναι μια αρκετά δυσάρεστη διαδικασία, ειδικά όταν πρέπει να γίνει επαλήθευση των στοιχείων.

Τα έξυπνα συμβόλαια επιλύουν αυτό το πρόβλημα και επιτρέπουν τη διατήρηση όλων των δεδομένων ενός ατόμου , σε ένα μέρος. Ό,τι συμβαίνει καταχωρείται στην αλυσίδα για να διατηρείται το αρχείο. Λόγω αυτού, η επαλήθευση KYC γίνεται άμεση και το απόρρητο δεν επηρεάζεται, καθώς ο χρήστης αποφασίζει ποιες πληροφορίες θα αποκαλύψει και ποιες όχι.

5.4 Τραπεζικές Εργασίες (Banking)

Όταν κάποιος προσπαθεί να κάνει μεταφορά χρημάτων και πρέπει να καλύψει μια χρέωση, εκτελεί την πληρωμή και στη συνέχεια περιμένει λίγες ημέρες κατά τη διάρκεια των οποίων γίνεται η επεξεργασία της συναλλαγής. Παρόλο που το σύγχρονο τραπεζικό σύστημα λειτουργεί ομαλά, σίγουρα υπάρχουν μειονεκτήματα.

Τα έξυπνα συμβόλαια δεν απαιτούν μεσάζοντες. Ως εκ τούτου, δεν πληρώνονται τέλη, καθώς δεν υπάρχει γραφειοκρατία, οι συναλλαγές γίνονται γρήγορα και οικονομικότερα.

Επιπλέον, η διαφάνεια που εγγυάται η αλυσίδα συναλλαγών μειώνει τους πιθανούς κινδύνους απάτης.

5.5 Φορολογικά Αρχεία (Tax Records)

Ένα πρόβλημα που αντιμετωπίζει πληθώρα πολιτών είναι η συνέπεια στις φορολογικές πληρωμές. Πολλές φορές κάποιοι ξεχνιούνται ακόμα και όταν έχουν όσα έγγραφα χρειάζεται για να πάνε σε μία υπηρεσία, μπορεί να μην προλάβουν ή να αντιμετωπίσουν κάποια απρόσμενη απεργία. Επίσης, είναι σύνηθες να ψάχνει κανείς χρήσιμα έγγραφα και να μην έχει πρόσβαση σε αυτά.

Οι αυτόματες πληρωμές που ενεργοποιούνται από τα έξυπνα συμβόλαια δίνουν τη δυνατότητα σε όποιον τα χρησιμοποιεί να ολοκληρώνει τις οικονομικές του συναλλαγές εμπρόθεσμα, χωρίς τον κίνδυνο να επιβαρυνθεί με κάποιο πρόστιμο. Ταυτόχρονα, όλα τα δεδομένα σχετικά με τους φόρους καταγράφονται στην αλυσίδα και διατίθενται για έλεγχο της βάσης δεδομένων. Η διαδικασία αυτή παρέχει διαφάνεια και είναι σχεδόν αδύνατο να δεχτεί κάποια απειλή - κίνδυνο.

5.6 Ασφάλιση (Insurance)

Έστω για παράδειγμα ένα μικρό τροχαίο ατύχημα, το πρώτο πράγμα που θα σκέφτεται κανείς που ευθύνεται για αυτό, αφού δεν τίθεται θέμα υγείας, θα ήταν αν τον καλύπτει η ασφάλεια του και αν την έχει πληρώσει. Αν για το ατύχημα δεν φταίει κάποιος, περιμένει από την άλλη πλευρά να καλύψει τα έξοδα επισκευής. Πολλές φορές όμως υπάρχει ρήξη μεταξύ των δύο πλευρών και επιρρίπτει ευθύνες ο ένας στον άλλο. Τότε, οι πιθανότητες για επιστροφή χρημάτων μειώνονται αρκετά.

Μπορεί το αυτοκίνητο να είναι εξοπλισμένο με μια συσκευή IoT (Internet of Things) που έχει την δυνατότητα να αναφέρει την τοποθεσία, την ταχύτητα, την ώρα του ατυχήματος, χωρίς ο κάθε οδηγός να έχει λόγους ανησυχίας. Τα δεδομένα της αλυσίδας θα μπορούν να αποδείξουν ποια πλευρά έχει δίκιο και ποια είναι εκείνη που δεν φέρει ευθύνες ώστε να λάβει αυτόματα την πληρωμή που της αναλογεί.

5.7 Διαχείριση ακινήτων και τίτλων γης (Real Estate and Land Titles Recording)

Οι νομικές συμφωνίες για τα ακίνητα, είναι πολύ χρονοβόρες και χρήζουν ειδικής μεταχείρισης. Κανένας δεν θέλει να συμμετέχει σε νομικές διαπραγματεύσεις και γραφειοκρατικές διαδικασίες που σχετίζονται με μεταβιβάσεις δικαιωμάτων ιδιοκτησίας.

Με τη βοήθεια έξυπνων συμβολαίων, αυτή η διαδικασία είναι εύκολο να αποφευχθεί. Το κεντρικό μητρώο ακινήτων επιτρέπει την αγοραπωλησία ακινήτων, χωρίς μεσάζοντες και μπορεί να υλοποιηθεί η μεταβίβαση των δικαιωμάτων κυριότητας μέσα σε λίγα λεπτά. Με μόλις μερικά κλικ, μπορεί κανείς να βρει το διαμέρισμα που επιθυμεί, να πληρώσει για αυτό και να το πάρει στην κυριότητά του χωρίς καν να συναντήσει τον πωλητή.

5.8 Εφοδιαστική αλυσίδα (Supply Chain)

Όταν έρχεστε στο κατάστημα για να αγοράσετε θαλασσινά, δεν γνωρίζετε ποτέ 100% πόσο φρέσκα είναι. Μπορεί να γράφει ότι μόλις έφτασε από τη Δανία. Οι επιλογές σας δεν είναι πάρα πολλές - μπορείτε είτε να το πιστεύετε είτε όχι.

Τα έξυπνα συμβόλαια που συνδυάζονται με συσκευές IoT πρόκειται να φέρουν την επανάσταση στην εφοδιαστική αλυσίδα (Εικόνα 5.3). Με τη βοήθειά τους, η παρακολούθηση του τρόπου με τον οποίο τα προϊόντα μετακινούνται πριν φτάσουν στο σημείο πώλησης γίνεται αυτόματα και ανεπηρέαστα. Σε οποιαδήποτε χρονική στιγμή, ξέρει κανείς που βρίσκονται τα εμπορεύματα, υπό ποιους όρους αποθηκεύονται και πότε θα φτάσουν. Αυτή η τεχνολογία μπορεί να χρησιμοποιηθεί για την παρακολούθηση λιανικών αγαθών, άνθρακα, πετρελαίου, χρυσού, κλπ. Λόγω της αλυσίδας των μπλοκ, οι πωλητές γίνονται πιο αξιόπιστοι και οι κίνδυνοι μιας πιθανής απάτης μειώνονται.

5.9 Internet of Things (IoT)

Η ραγδαία εξέλιξη της τεχνολογίας επιτρέπει στους ανθρώπους να έχουν πολλές ευκολίες στην καθημερινότητά τους. Επιστρέφοντας από τη δουλειά μπορεί να ενεργοποιείται η τηλεόραση και η ταινία που θέλει ο χρήστης να παρακολουθήσει να υπάρχει διαθέσιμη, ενώ παράλληλα να έχουν γίνει όλα του τα επιθυμητά ψώνια και να έχουν φτάσει στην πόρτα του. Ο συναγερμός μπορεί να απενεργοποιείται και οι κουρτίνες να ανοίγουν αυτόματα μόλις γί-

Εικόνα 5.3: Εφοδιαστική Αλυσίδα - Supply Chain. http://ltxsolutions.com/five-challenges-in-food-and-beverage-supply-chains/ (20/3/2019)

νει ανίχνευση κάποιας άφιξης. Ένα έξυπνο σπίτι δεν είναι πλέον ένα περιβάλλον από μια ταινία επιστημονικής φαντασίας και λόγω των έξυπνων συμβολαίων, γίνεται αυτόματα και αξιόπιστα.

Το IoT είναι ένα από τα πιο εμπνευσμένα παραδείγματα έξυπνων συμβολαίων, καθώς είναι στενά συνδεδεμένο με τις καθημερινές μας συνήθειες (Εικόνα 5.4).

Εικόνα 5.4: Internet of Things - IoT. https://www.naftemporiki.gr/story/1402498/summaxia-arm-kai-intel-gia-xari-tou-internet-of-things (20/3/2019)

5.10 Παιχνίδια και τυχερά παιχνίδια (Gaming and Gambling)

Το Διαδίκτυο είναι γεμάτο από προσφορές για διαδικτυακά τυχερά παιχνίδια και για εικονικά δωμάτια τυχερών παιχνιδιών. Όταν παίζει κανείς δωρεάν, δεν τον ενδιαφέρει πάρα πολύ αν κερδίζει ή χάνει. Αλλά όταν παίζει για χρήματα, αρχίζει να σκέφτεται τις πληρωμές και τους τρόπους να κερδίσει.

Εάν μια εικονική χαρτοπαικτική λέσχη υιοθετεί έξυπνα συμβόλαια, δεν θα έχει λόγο κανείς να ανησυχεί: κάθε φορά που κερδίζει παίρνει την ανταμοιβή του, όποτε χάνει δεν μπορεί να ξεγελάσει το σύστημα και να κρατήσει τα χρήματά. Έτσι κάθε μορφή τζόγου γίνεται διαφανής και αξιόπιστη.

5.11 Πνευματικά δικαιώματα ιδιοκτησίας (Authorship and Intellectual Property Rights)

Η πειρατεία και οι παραβιάσεις των πνευματικών δικαιωμάτων είναι ένα μεγάλο ζήτημα στο χώρο της ψυχαγωγίας. Οι μουσικοί, οι φωτογράφοι, οι συγγραφείς και άλλοι καλλιτέχνες στερούνται των δικαιωμάτων τους, λόγω της ανέντιμης εκμετάλλευσης της πνευματικής ιδιοκτησίας τους.

Η δημιουργία ενός διαφανούς μητρώου εγγράφων σε μια blockchain είναι ένα φιλόδοξο παράδειγμα για το πώς τα έξυπνα συμβόλαια μπορούν να βελτιώσουν την τρέχουσα κατάσταση. Για παράδειγμα, κάθε φορά που κάποιος κατεβάζει ένα μυθιστόρημα ενός συγγραφέα

ή κάποια φωτογραφία, ο ιδιοκτήτης αυτού θα λαμβάνει το εκάστοτε αντίτιμο. Επιπλέον, τα πνευματικά δικαιώματά καταχωρούνται με ασφάλεια και κανείς δεν θα μπορεί να τα αλλοιώσει.

5.12 Φροντίδα υγείας και ιατρική περίθαλψη (Life Science and Health Care)

Τα οφέλη που προσφέρουν τα έξυπνα συμβόλαια, δεν είναι μόνο ασφαλείς και γρήγορες συναλλαγές, αυτόματες πληρωμές και βελτιωμένες καθημερινές διαδικασίες. Ένα τέτοιο συμβόλαιο μπορεί να σώσει μία ανθρώπινη ζωή, για παράδειγμα, να αποτρέψει μια καρδιακή προσβολή.

Ας υποθέσουμε ότι φοράει κάποιος ένα βραχιόλι παρακολούθησης της υγείας του που καταγράφει τον καρδιακό παλμό και την αρτηριακή πίεση και μεταφέρει τα δεδομένα αυτά σε μία αλυσίδα τακτικά. Όταν οποιοσδήποτε από τους δείκτες υπερβαίνει τα επιτρεπόμενα όρια, ένα έξυπνο συμβόλαιο ενεργοποιεί μια ειδοποίηση που λαμβάνει ο χρήστης στο τηλέφωνό του. Με αυτόν τον τρόπο, ειδοποιείται ότι κάτι πάει στραβά και έχει αρκετό χρόνο για να πάρει όποια αγωγή χρειάζεται για να αποφύγει μια κρίση.

Επιπλέον, μία blockchain είναι χρήσιμη για την ασφαλή αποθήκευση αποτελεσμάτων κλινικών εξετάσεων, καθώς εγγυάται την ιδιωτικότητα των ασθενών και μπορεί να δημιουργηθεί μία βάση δεδομένων για το προφίλ υγείας του κάθε ατόμου.

Κεφάλαιο 6

Παραδείγματα κρυπτονομισμάτων

6.1 Bitcoin

Το Bitcoin (Εικόνα 6.1) είναι ένα λεγόμενο εικονικό νόμισμα, που έχει επινοηθεί για ανώνυμες πληρωμές που πραγματοποιούνται εξ΄ ολοκλήρου ανεξάρτητα από κυβερνήσεις και τράπεζες. Τα τελευταία χρόνια, το Bitcoin έχει φέρει μεγάλη προσοχή σε διάφορα μέτωπα. Οι πληρωμές βασίζονται σε μια νέα ενδιαφέρουσα τεχνική λύση και λειτουργούν διαφορετικά από τις παραδοσιακές πληρωμές. Σε ορισμένες περιπτώσεις πληρωμής, το Bitcoin μπορεί να φέρει οφέλη με τη μορφή της μείωσης του κόστους, της ταχύτητας, της ανωνυμίας, κλπ πέρα από τις παραδοσιακές μεθόδους πληρωμής. Ωστόσο, η χρήση μπορεί επίσης να είναι πιο επικίνδυνη επειδή το Bitcoin δεν καλύπτεται άμεσα από τους νόμους που διέπουν άλλες πληρωμές. Η ασθενής προστασία των καταναλωτών είναι επίσης ένας λόγος για τον οποίο μπορεί να είναι δύσκολο για το Bitcoin να γίνει γενικά αποδεκτό και βιώσιμο ως μέσο πληρωμής. Η χρήση του Bitcoin για τις πληρωμές είναι σε χαμηλά επίπεδα σήμερα, και παρόλο που το μέλλον του Bitcoin είναι αβέβαιο, είναι μια ενδιαφέρουσα τεχνολογία. [22]

Πολλές περιοχές έχουν υποστεί ταχεία τεχνολογική πρόοδο τα τελευταία χρόνια. Οι ανάγκες μας όσον αφορά την πραγματοποίηση πληρωμών βρίσκονται επίσης στο στάδιο μετασχηματισμού. Για παράδειγμα, τα νοικοκυριά μπορούν να κάνουν online αγορές σε μεγάλη έκταση, καθώς επίσης και το ποσό των διασυνοριακών πληρωμών βρίσκεται σε μεγάλη άνοδο. Οι λύσεις πληρωμών, ιδίως από πρόσωπο-σε-πρόσωπο, είναι ιδανικές, ωστόσο, δεν έχουν εξελιχθεί τόσο γρήγορα. Το Bitcoin μπορεί να θεωρηθεί ως απάντηση στην έλλειψη τέτοιων λύσεων πληρωμών και συχνά αποτελεί θέμα συζήτησης στα μέσα μαζικής ενημέρωσης, στους χώρους εργασίας και μεταξύ φίλων τα τελευταία χρόνια. Διάφοροι παράγοντες

Εικόνα 6.1: Κρυπτονόμισμα Bitcoin. https://www.coindesk.com/6k-ahead-bitcoin-price-rsi-confirms-long-run-bull-reversal (21/3/2019)

έχουν προκάλεσε την περιέργεια για το πώς λειτουργεί το κρυπτονόμισμα, όπως η υποτιθέμενη ανωνυμία για τους χρήστες, το γεγονός ότι οι τράπεζες δεν εμπλέκονται στις πληρωμές και η ικανότητα να υλοποιούνται πληρωμές σε όλο τον κόσμο. Ταυτόχρονα, είναι δύσκολο να καταλάβουμε τι είναι πραγματικά το Bitcoin, και πώς λειτουργεί. Το Bitcoin είναι ένα συναινετικό δίκτυο που παρέχει τη δυνατότητα ενός νέου συστήματος πληρωμών και μιας εντελώς ψηφιακής μορφής χρημάτων. Είναι το πρώτο αποκεντρωμένο δίκτυο πληρωμής μεταξύ ομότιμων (peer-to-peer) που λειτουργεί από τους χρήστες του χωρίς κεντρική αρχή ή μεσάζοντες. Από τη σκοπιά του χρήστη, το Bitcoin είναι λίγο πολύ σαν τα "χρήματα" του Διαδικτύου. Το Bitcoin μπορεί επίσης να θεωρηθεί ως το πιο περίφημο λογιστικό σύστημα τριπλής καταχώρησης που υπάρχει. Οι πληρωμές με Bitcoin είναι ευκολότερο να γίνουν από ότι με χρεωστική ή πιστωτική κάρτα και μπορούν να ληφθούν χωρίς κάποιον εμπορικό λογαριασμό. Οι πληρωμές γίνονται μέσω εφαρμογής πορτοφολιού, είτε στον υπολογιστή ή στο κινητό σας τηλέφωνο, εισάγοντας τη διεύθυνση του παραλήπτη, το ποσό πληρωμής, και πατώντας αποστολή. Για να γίνει καλύτερη η εισαγωγή της διεύθυνσης του παραλήπτη, πολλά πορτοφόλια μπορούν να αποκτήσουν τη διεύθυνση σαρώνοντας ένα κώδικα QR ή φέρνοντας σε επαφή δύο κινητά τηλέφωνα, με χρήση της τεχνολογίας NFC. [23]

6.2 Ethereum

Η πρόθεση του Ethereum (Εικόνα 6.2) είναι να δημιουργήσει ένα εναλλακτικό πρωτόκολλο για την κατασκευή αποκεντρωμένων εφαρμογών, παρέχοντας ένα διαφορετικό σύνολο συμφωνιών που πιστεύεται ότι θα είναι πολύ χρήσιμες για μια μεγάλη κατηγορία αποκεντρωμένων εφαρμογών. Με ιδιαίτερη έμφαση σε καταστάσεις, όπου ο χρόνος ανάπτυξης, η ασφάλεια για μικρές και σπάνια χρησιμοποιούμενες εφαρμογές και η δυνατότητα διαφορετικών εφαρμογών να αλληλεπιδρούν πολύ αποτελεσματικά είναι σημαντικές. Για να το θέσουμε απλά, το Ethereum είναι το Blockchain των πραγμάτων. Το Bitcoin χρησιμοποιείται κυρίως για οικονομικούς λόγους και κατά την άποψή μας θα αποτελεί πάντοτε το βασιλιά των blockchain. [24]

Εικόνα 6.2: Κρυπτονόμισμα Ethereum. https://ethereumworldnews.com/coinbase-kraken-and-huobi-to-support-ethereums-eth-constantinople-hard-fork/ (22/3/2019)

Παρόλα αυτά, το Ethereum είναι ένα πολύ ευρύτερο blockchain το οποίο αρχίζει να γίνεται πολύ χρήσιμο και αποκτά ολοένα και περισσότερη δυναμική. Μπορούν να χτιστούν πολλές εφαρμογές βασισμένες στο blockchain του Ethereum (πράγματα όπως έξυπνα συμβόλαια για αποθήκευση συμφωνιών, ιδιοκτησιακά δικαιώματα, ιατρικά αρχεία, και λίγο πολύ οποιαδήποτε άλλα αρχεία θέλετε να αποθηκεύσετε χρησιμοποιώντας ένα ασφαλές blockchain).

Το Ethereum λειτουργεί βάσει ενός νομίσματος που μοιάζει πολύ με το Bitcoin και ονομάζεται Ether (ETH). Το νόμισμα αυτό μπορεί επίσης να εξορυχθεί, όπως ακριβώς και το Bitcoin.

Αυτή ακριβώς τη στιγμή το Ethereum βρίσκεται στα αρχικά στάδια της υιοθέτησης του. Για την ακρίβεια, απευθύνεται μόνο σε προγραμματιστές και σχεδιαστές αυτή τη στιγμή και δεν απευθύνεται πραγματικά για χρήση από το κοινό (ακόμη). Χρειάζεται να γνωρίζετε πως

να χρησιμοποιείτε μια διασύνδεση γραμμών εντολών για να μπορέσετε να κάνετε κάτι μαζί του, τα εργαλεία και η φιλικότητα προς το χρήστη όμως έρχονται πολύ σύντομα.

Βλέπουμε μια τεράστια ευκαιρία αυτή τη στιγμή για την εξόρυξη των Ether, όμοια με το Bitcoin τον πρώτο καιρό της εξόρυξης του. Το Ether μπορεί να εξορυχθεί χρησιμοποιώντας GPU και εξακολουθεί να είναι αρκετά μικρό για να μπορεί οποιοσδήποτε να μπει στο παιχνίδι.

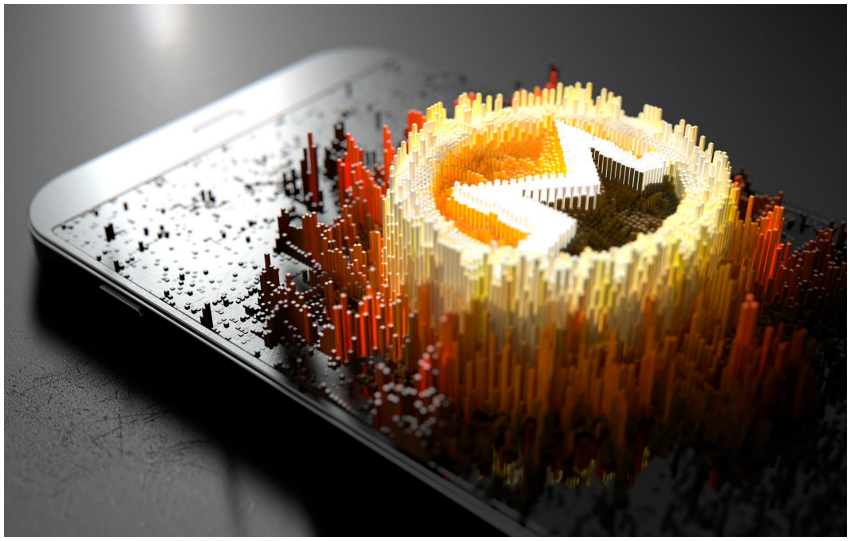
Το Ethereum το κάνει αυτό κατασκευάζοντας αυτό που είναι ουσιαστικά το θεμελιώδες στρώμα του: ένα blockchain με μια ενσωματωμένη γλώσσα προγραμματισμού Turing, επιτρέποντας σε οποιονδήποτε να γράψει έξυπνες συμβάσεις και αποκεντρωμένες εφαρμογές, όπου μπορούν να δημιουργήσουν τους δικούς τους αυθαίρετους κανόνες ιδιοκτησίας και μεταβατικές λειτουργίες.

Μια εκδοχή του Namecoin μπορεί να γραφτεί σε δύο σειρές κώδικα και σε άλλα πρωτόκολλα, όπως νομίσματα και συστήματα επανάληψης που μπορούν να κατασκευαστούν σε κάτω από είκοσι γραμμές κώδικα. Έξυπνα συμβόλαια, κρυπτογραφικά "κουτιά" που περιέχουν αξία και ξεκλειδώνουν μόνο αν πληρούνται ορισμένες προϋποθέσεις, μπορούν επίσης να χτιστούν στην πλατφόρμα, με πολύ περισσότερη δύναμη από αυτή που προσφέρει το Bitcoin scripting, λόγω των πρόσθετων δυνατοτήτων και πληρότητας του Turing, σε θέματα σχετικά με την αξία και την εφοδιαστική αλυσίδα.

6.3 Monero

Το Monero (XM - Εικόνα 6.3) είναι ανοικτού κώδικα κρυπτονόμισμα το οποίο δημιουργήθηκε τον Απρίλιο του 2014 και είναι εστιασμένο στην ιδιωτικότητα, την αποκέντρωση και την επεκτασιμότητα. Αντίθετα με τα περισσότερα κρυπτονομίσματα που είναι εκδόσεις ή αντίγραφα του Bitcoin, το Monero είναι βασισμένο στο πρωτόκολλο CryptoNote και έχει αλγοριθμικές διαφορές που σχετίζονται με την ανάλυση της αλυσίδας συναλλαγών. [25]

Το Monero κυκλοφόρησε στις 18 Απριλίου 2014 αρχικά με την ονομασία BitMonero, η οποία είναι μια ένωση Bit (όπως στην περίπτωση του Bitcoin) και Monero (που σημαίνει κυριολεκτικά "χρήμα"). Πέντε ημέρες αργότερα επιλέχθηκε να μειωθεί το μήκος του ονόματος του μόνο στο Monero. Η πρώτη έκδοση του ξεκίνησε βασιζόμενη στο CryptoNote νόμισμα Bytecoin, ωστόσο κυκλοφόρησε με δύο μεγάλες διαφορές. Πρώτον, ο χρόνος του μπλοκ-στόχου μειώθηκε από 120 σε 60 δευτερόλεπτα, και δεύτερον, η ταχύτητα εκπομπής επιβραδύνθηκε κατά 50% (αργότερα το Monero επανήλθε σε χρόνο μπλόκ 120 δευτερολέπτων διατηρώντας το πρόγραμμα εκπομπών, διπλασιάζοντας την ανταμοιβή του μπλοκ για κάθε νέο μπλοκ). Επιπλέον, οι προγραμματιστές του Monero βρήκαν πολυάριθμα προβλήματα



Εικόνα 6.3: Κρυπτονόμισμα Monero. https://bitcoinist.com/when-moonero-the-mystery-of-moneros-declining-price/ (24/3/2019)

που στη συνέχεια διορθώθηκαν.

Το Monero διαθέτει μια «αδιαφανή» αλυσίδα (με ένα ρητό σύστημα δικαιωμάτων που ονομάζεται viewkey), σε έντονη αντίθεση με το «διαφανές» blockchain που χρησιμοποιείται από οποιαδήποτε άλλη κρυπτογράφηση που δεν βασίζεται στο CryptoNote. Έτσι, το Monero λέγεται ότι είναι «ιδιωτικό και προαιρετικά διαφανές». Πέρα από την πολύ ισχυρή προστασία της ιδιωτικότητας των συναλλαγών, ένα τέτοιο σύστημα επιτρέπει την ουδετερότητα του δικτύου στο blockchain (οι εξορύκτες δεν μπορούν να λογοκρίνουν, αφού δεν γνωρίζουν πού πηγαίνει η συναλλαγή ή τι περιέχει), επιτρέποντας ταυτόχρονα τον έλεγχο, όταν χρειαστεί.

Το Monero είναι ίσως το πιο ανώνυμο κρυπτονόμισμα που έχει δημιουργηθεί , είναι ένα κρυπτονόμισμα πού βασίζεται στην ιδιωτικότητα και την ανωνυμία.

Δημιουργήθηκε από μια ανώνυμη ομάδα προγραμματιστών.

Ο στόχος της δημιουργίας του ήταν να συμπληρώσει την αδυναμία του Bitcoin σχετικά με την ψευδο-ανωνυμία των συναλλαγών, προστατεύοντας σε μεγάλο βαθμό την ιδιωτικότητα και την ανωνυμία.

Το Monero προστατεύει την ιδιωτικότητα, την ανωνυμία των συναλλαγών για όλες τις συναλλαγές στο δίκτυο με τρεις τρόπους:

1. Οι υπογραφές δακτυλίων κρύβουν τη διεύθυνση αποστολής.

2. Το RingCT κρύβει το ποσό της συναλλαγής.

3. Οι διευθύνσεις αποκρύπτουν τη διεύθυνση παραλαβής της συναλλαγής.

6.4 Tether

Το Tether (Εικόνα 6.4) είναι ένα εναλλακτικό νόμισμα. Ένα από τα παλαιότερα από αυτά, με ένα μοναδικό χαρακτηριστικό: έχει τη σταθερή αξία 1$. Αυτό οφείλεται στο ότι η εταιρεία τυπώνει ένα Tether για κάθε δολάριο που έχει στους τραπεζικούς της λογαριασμούς. Λόγω της σταθερής του αυτής αξίας, χρησιμοποιείται πάρα πολύ από ανταλλακτήρια που έχουν μόνο κρύπτο και δεν έχουν σύνδεση με μετρητά. Η αξία του Tether δημοσιεύεται καθημερινά. [26]

Εικόνα 6.4: Κρυπτονόμισμα Tether. https://www.coindesk.com/tether-says-customers-can-once-again-deposit-and-redeem-fiat (30/3/2019)

Η αξία των αποθεμάτων αντιστοιχεί ή υπερβαίνει την αξία όλων των Tether που κυκλοφορούν. Οποιοσδήποτε έχει βασικές γνώσεις εργασίας σχετικά με την κρυπτογράφηση θα ειναι εξοικειωμένος με τις διακυμάνσεις της αγοράς και την αστάθεια που σχετίζεται με την κατηγορία στοιχείων ενεργητικού. Εντούτοις, αυτό που θέτει σταθερές βάσεις εκτός από άλλα ψηφιακά νομίσματα είναι ότι έχουν σχεδιαστεί ώστε να χρησιμοποιούνται ως αποθήκη αξίας με ελάχιστη διακύμανση των τιμών. Αυτό εξυπηρετεί έναν πρακτικό σκοπό σε ταραχώδεις εποχές ή φέρει αγορές όταν οι έμποροι θέλουν να αποφύγουν να χάσουν χρήματα από τις επενδύσεις τους. Για να διατηρηθούν αυτές οι λειτουργίες, οι ψηφιακές μάρκες συνδέονται με την αξία ενός άλλου σταθερού στοιχείου, συνήθως ένα σημαντικό παραδοσιακό νόμισμα, όπως το δολάριο ΗΠΑ.

Η πλατφόρμα του Tether είναι δομημένη με βάση τις ανοικτές τεχνολογίες της αλυσίδας, αξιοποιώντας την ασφάλεια και τη διαφάνεια που παρέχουν. Η τεχνολογία αλυσίδας του Tether παρέχει ασφάλεια παγκόσμιας κλάσης, ενώ πληροί τα διεθνή πρότυπα και τους κανονισμούς συμμόρφωσης.

6.5 VeChain

Το VeChain (Εικόνα 6.5) είναι μια πλατφόρμα βασισμένη στην αλυσίδα που καταγράφει τι συμβαίνει σε κάθε στάδιο της εφοδιαστικής αλυσίδας. Συνδυάζει τη φυσική παρακολούθηση με τα αρχεία του μπλοκ αλυσίδας, για να διατηρεί τις καρτέλες σε προϊόντα από την παραγωγή έως την παράδοση, συμβάλλοντας στην πρόληψη της απάτης και στην αύξηση της διαφάνειας. [27]

Εικόνα 6.5: Κρυπτονόμισμα VeChain. https://hackernoon.com/china-on-the-blockchain-how-the-vechain-thor-blockchain-is-set-to-revolutionize-governance-2c640b7c512c (1/4/2019)

Το VeChain είναι ένα blockchain που έχει σχεδιαστεί για να διευκολύνει τη διαχείριση της εφοδιαστικής αλυσίδας. Αρχικά, σχεδιάστηκε ως ένας τρόπος να προσδιοριστεί αν ένα πραγματικό προϊόν είναι ψεύτικο ή όχι - αποτρέποντας φαινόμενα απάτης. Έχει χρησιμοποιηθεί από μεγάλες εταιρείες για να βοηθήσει στην παρακολούθηση πολλών προϊόντων από την παραγωγή κρασιού έως την κατασκευή αυτοκινήτων.

Ο τρόπος που το κάνει αυτό είναι απλός: δίνει σε κάθε προϊόν μια μοναδική ταυτότητα και μετά χρησιμοποιεί αισθητήρες για να παρακολουθεί τι συμβαίνει σε κάθε στάδιο της εφοδιαστικής αλυσίδας. Με αυτόν τον τρόπο, οι εταιρείες μπορούν να είναι βέβαιες, ότι τα

προϊόντα χειρίζονται σωστά και οι καταναλωτές μπορούν να ελέγξουν αν οι αγορές τους είναι ασφαλείς και νόμιμες.

6.6 Zcash

Το Zcash (Εικόνα 6.6) είναι ένα κρυπτονόμισμα που προσφέρει ιδιωτικότητα και επιλεκτική διαφάνεια των συναλλαγών. Οι πληρωμές με το Zcash δημοσιεύονται σε μια δημόσια αλυσίδα, αλλά ο αποστολέας, ο παραλήπτης και το ποσό μιας συναλλαγής παραμένουν ιδιωτικές πληροφορίες. Όπως και το Bitcoin, το Zcash έχει σταθερή συνολική προσφορά 21 εκατομμυρίων μονάδων.

Το Zcash προσφέρει πλήρη εμπιστευτικότητα πληρωμής, ενώ πάλι διατηρεί ένα αποκεντρωμένο δίκτυο χρησιμοποιώντας μια δημόσια αλυσίδα από μπλοκ. Αντίθετα από το Bitcoin, οι συναλλαγές Zcash μπορούν να προστατευθούν αποκρύβοντας τον αποστολέα, παραλήπτη και αξία για όλες τις συναλλαγές στην αλυσίδα των μπλοκ.

Εικόνα 6.6: Κρυπτονόμισμα Zcash. https://medium.com/swlh/how-to-mine-for-zcash-a-profitable-business-for-everyone-da32d42e2535 (3/4/2019)

Μόνο αυτοί με το σωστό κλειδί εμφάνισης μπορούν να δουν τα περιεχόμενα. Οι χρήστες έχουν τον πλήρη έλεγχο και είναι στην κρίση τους στο να επιλέξουν να παρέχουν σε άλλους το κλειδί. Οι συναλλαγές Zcash δεν εξαρτώνται από τη συνεργασία άλλων μερών.

Στα παραδοσιακά blockchains, όπως το Bitcoin και το Ethereum, κάθε είσοδος στην αλυσίδα αποκαλύπτει τόσο το ποσό της συναλλαγής όσο και τα μέρη που συμμετέχουν στη

συναλλαγή. Το CoinJoin του Bitcoin κατακλύζει τα ποσά και τους παραλήπτες επιτρέποντας στους χρήστες να συγκεντρώνουν τις συναλλαγές. Δεν κρύβει την αξία του συνολικού ποσού των συγκεντρωτικών συναλλαγών, μόνο το πώς κατανέμεται το συνολικό ποσό μεταξύ των μελλοντικών συναλλαγών. Απαιτεί επίσης την ενεργό συμμετοχή μεταξύ των πελατών.

Κεφάλαιο 7

Συμπεράσματα

Παρά το γεγονός ότι η ιδέα των ηλεκτρονικών νομισμάτων χρονολογείται από τα τέλη της δεκαετίας του 1980, το Bitcoin, που ξεκίνησε το 2009, είναι το πρώτο επιτυχημένο αποκεντρωμένο κρυπτονόμισμα. Εν ολίγοις, ένα κρυπτονόμισμα είναι ένα εικονικό σύστημα κερμάτων που λειτουργεί σαν ένα τυπικό νόμισμα, επιτρέποντας στους χρήστες να κάνουν εικονικές πληρωμές για αγαθά και υπηρεσίες χωρίς κεντρική και αξιόπιστη αρχή. Τα κρυπτονομίσματα βασίζονται στην μετάδοση των ψηφιακών πληροφοριών, με τη χρήση κρυπτογραφικών μεθόδων για τη διασφάλιση της νομιμότητας των συναλλαγών. Το Bitcoin ενίσχυσε την ανάπτυξη της ψηφιακής αγοράς νομισμάτων, αποκεντρώνοντας το κρυπτονόμισμα και απελευθερώνοντας το από ιεραρχικές δομές εξουσίας. Οι ιδιώτες και οι επιχειρήσεις συναλλάσσονται με το ηλεκτρονικά νομίσματα σε ένα δίκτυο peer-to-peer. Το Bitcoin προσέλκυσε τη προσοχή του ευρύ κοινού από το 2011, και διάφορα εναλλακτικά κρυπτονομίσματα - μια γενική ονομασία για όλα τα άλλα ψηφιακά νομίσματα μετά το Bitcoin - εμφανίστηκαν σύντομα.

Η βιομηχανία των κρυπτονομισμάτων αποτελείται από περίπου 550 νομίσματα με διαφορετικές βάσεις χρηστών και όγκο εμπορικών συναλλαγών. Λόγω της υψηλής μεταβλητότητας της ίδιας της αγοράς και των συνεχώς νέων εισαγόμενων νομισμάτων, η μεταβλητότητα της απόδοσης του κάθε κρυπτονομίσματος είναι μεγάλη. Επίσης, λόγω της έλλειψης ρυθμιστικών πλαισίων, της περιορισμένης αποδοχής και του μικρού χρόνου ωρίμανσης της αγοράς, δεν γίνεται συστηματική ακαδημαϊκή έρευνα και δεν υπάρχει μεγάλος όγκος επιστημονικής βιβλιογραφίας σχετικά με την αξιολόγηση των νομισμάτων.

Στην παρούσα διπλωματική εργασία, στόχος ήταν η διερεύνηση της συνεισφοράς των Κρυπτονομισμάτων στη λειτουργία της Εφοδιαστικής Αλυσίδας και ο ρόλος των Έξυπνων

Συμβολαίων.

Ενώ η πλατφόρμα blockchain του Bitcoin δημιουργήθηκε και μέχρι σήμερα αφορά κυρίως συναλλαγές με το ομώνυμο κρυπτονόμισμα, η αντίστοιχη του Ethereum έχει τη δυνατότητα να ενσωματώσει και πιο σύνθετες πληροφορίες, όπως τα λεγόμενα έξυπνα συμβόλαια (smart contracts). Όλοι αυτοί οι όροι λειτουργίας ενσωματώνονται στο πρωτόκολλο (whitepaper) της εκάστοτε πλατφόρμας blockchain, το οποίο είναι διαθέσιμο στο κοινό μέσω του διαδικτύου.

Η τεχνολογία blockchain όχι μόνο καταργεί την ανάγκη για την ύπαρξη τρίτων μερών, αλλά εξασφαλίζει ότι όλοι οι συμμετέχοντες γνωρίζουν τις λεπτομέρειες του συμβολαίου και ότι οι συμβατικοί όροι θα εκπληρώνονται αυτόματα, όταν ισχύουν ορισμένες προϋποθέσεις. Τα συμβαλλόμενα μέρη σε ένα έξυπνο συμβόλαιο διαπραγματεύονται τους βασικούς όρους, όπως τις προδιαγραφές των προϊόντων, την ποσότητα, το τίμημα, τον χρόνο και τον τόπο εκπλήρωσης μέσω της blockchain, σε μία διαδικασία η οποία μοιάζει με την διαπραγμάτευση παραγώγων συμβολαίων σε ηλεκτρονική πλατφόρμα.

Οι νέες τεχνολογίες, η ψηφιοποίηση της Εφοδιαστικής Αλυσίδας, των Logistics και τα Έξυπνα Συμβόλαια, αποτελούν το «κλειδί» για το μέλλον του κλάδου. Οι επιχειρήσεις θα πρέπει να προσαρμοστούν, ενσωματώνοντας την τεχνολογία και εξελίσσοντας την εφοδιαστική τους αλυσίδα, προκειμένου να πετύχουν μια βιώσιμη ανάπτυξη.

Βιβλιογραφία

[1] : https://en.wikipedia.org/wiki/Cryptocurrency [10/03/2019]

[2] : https://en.wikipedia.org/wiki/History_of_bitcoin [10/03/2019]

[3] : https://en.wikipedia.org/wiki/Satoshi_Nakamoto [10/03/2019]

[4] : https://www.investopedia.com/terms/b/bitcoin-mining.asp [12/03/2019]

[5] : https://www.buybitcoinworldwide.com/mining/ [12/03/2019]

[6] : https://en.bitcoinwiki.org/wiki/SHA-256 [15/03/2019]

[7] : https://en.bitcoinwiki.org/wiki/Scrypt [15/03/2019]

[8] : https://en.bitcoinwiki.org/wiki/X11 [15/03/2019]

[9] : https://en.bitcoinwiki.org/wiki/Dagger-Hashimoto [15/03/2019]

[10] : https://en.bitcoinwiki.org/wiki/CryptoNight [15/03/2019]

[11] : https://en.m.wikipedia.org/wiki/Blockchain [15/03/2019]

[12] : https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-exchange/ [16/03/2019]

[13] : https://cryptocurrencyfacts.com/what-is-a-dex/ [15/03/2019]

[14] : https://bitcoinmagazine.com/guides/what-ico/ [16/03/2019]

[15] : https://blog.polymath.network/what-is-a-security-token-offering-sto-4e5a92bf6bca [16/03/2019]

[16] : https://www.aalhysterforklifts.com.au/index.php/about/blog-post/what_is_a_supply_chain_network [20/03/2019]

[17] : https://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/ [26/03/2019]

[18] : https://coinsutra.com/smart-contracts/ [30/03/2019]

[19] : https://en.wikipedia.org/wiki/Smart_contract [01/04/2019]

[20] : https://coinsutra.com/ethereum-smart-contract-usecases/ [04/04/2019]

[21] : https://ambisafe.com/blog/smart-contracts-10-use-cases-business/ [03/04/2019]

[22] : https://bitcoin.org/bitcoin.pdf [10/04/2019]

[23] : https://etherscan.io/tokens [10/04/2019]

[24] : https://github.com/ethereum/wiki/wiki/White-Paper

[25] : https://cryptonote.org/whitepaper.pdf

[26] : https://tether.to/ [12/04/2019]

[27] : https://cdn.vechain.com/vechainthor_development_plan_and_whitepaper_en_v1.0.pdf [15/04/2019]