ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Μεταπτυχιακό Πρόγραμμα Σπουδών
Οικονομική & Επιχειρησιακή Στρατηγική

Διπλωματική Εργασία

Blockchain & Cryptocurrencies: Marketing Strategies

Διονυσία Σπυροπούλου

Επιβλέπων Καθηγητής
Ι. Πολλάλης
(Professor of Strategic Management, Director of iLeads Lab)

Πειραιάς, 2020

Ευχαριστίες

Με την περάτωση της παρούσας διπλωματικής εργασίας θα ήθελα να απευθύνω θερμές ευχαριστίες στον επιβλέποντα καθηγητή Ιωάννη Πολλάλη για την εμπιστοσύνη, την καθοδήγηση, την κατανόηση και την ενθάρρυνσή του καθ'όλη τη διάρκεια της εκπόνησης της παρούσας διπλωματικής εργασίας. Η συμβολή του έπαιξε καθοριστικό ρόλο στην ολοκλήρωση μιας άρτιας έρευνας και συγγραφής.

Ιδιαίτερες ευχαριστίες στους γονείς μου Γιώργο και Αθηνά για την αμέριστη συμπαράσταση τους και για όλα τα πολύτιμα εφόδια που μου έχουν προσφέρει όλα αυτά τα χρόνια. Η παρουσία τους στη ζωή μου είναι μοναδικό και αναντικατάστατο στήριγμα.

Περιεχόμενα

Περίληψη

Η τεχνολογία Blockchain έχει προχωρήσει ως λύση στην παγκόσμια κρίση εμπιστοσύνης. Πράγματι, οι μοναδικές δυνατότητες του Blockchain, ορισμένοι υποστηρίζουν, παρακάμπτουν την ανάγκη εμπιστοσύνης, γι 'αυτό και μερικές φορές ονομάζεται τεχνολογία «χωρίς εμπιστοσύνη». Αντ 'αυτού, προσφέρει έναν νέο τρόπο αντικατάστασης των πληροφοριών που δεν έχει κάποιος από άλλες πηγές, προκειμένου να εμπιστευτεί κάτι ή κάποιον και, κατ' επέκταση, να αναλάβει δράση βάσει του ότι έχει αυτήν την εμπιστοσύνη.

Η αντικατάσταση των πληροφοριών που είναι απαραίτητες για την εμπιστοσύνη επιτυγχάνεται σε συστήματα Blockchain με τα ακόλουθα:

1) Μηχανισμοί κινήτρων: η τεχνολογία Blockchain έχει σχεδιαστεί για να ενθαρρύνει τους κοινωνικούς φορείς να συμπεριφέρονται σωστά (π.χ. μέσω μηχανισμών ανταμοιβής που βασίζονται σε κρυπτονομίσματα σε ορισμένα Blockchain). Τα αλληλεπιδρώντα μέρη το γνωρίζουν αυτό και, ως εκ τούτου, έχουν την εμπιστοσύνη να ενεργήσουν χωρίς πλήρη γνώση μεταξύ τους, 2) Δημιουργία και τήρηση αρχείων: η τεχνολογία Blockchain προορίζεται να παράγει τελικούς, οριστικούς και αμετάβλητους δίσκους, χρησιμοποιώντας κρυπτογραφία, δημιουργώντας έτσι ανθεκτικότητα σε παραβίαση ενεργειών που έχουν πραγματοποιηθεί και 3) Αποκέντρωση: η τεχνολογία Blockchain λειτουργεί ως ένα κατανεμημένο δίκτυο peer-to-peer στο οποίο οι συμμετέχοντες συνήθως δεν λειτουργούν υπό οποιαδήποτε κεντρική αρχή · Αντίθετα, οι συμμετέχοντες είναι αυτόνομοι, αν και λειτουργούν με συντονισμένο τρόπο, επειδή έχουν κίνητρα να το πράξουν. Επειδή είναι αυτόνομοι, γεγονός που καθιστά δύσκολη την απάτη, οι εγγραφές που δημιουργούνται σε αυτά τα συστήματα μπορούν να είναι αξιόπιστες.

Στο παραπάνω πλαίσιο η ανάδειξη της τεχνολογίας Blockchain συντελεί σε μια νέα πραγματικότητα, αυτή της αλλαγής των συναλλακτικών ηθών και της εμπιστοσύνης.

Η τεχνολογία αυτή θα επηρεάσει όλη τη κοινωνία και όχι μόνον την οικονομία. Στα επόμενα κεφάλαια αναδεικνύονται οι δυναμικές αυτής της προοπτικής.

Εισαγωγή

Οι Blockchain υποδομές είναι ψηφιακοί δίσκοι που είναι ανθεκτικοί σε παραβιάσεις και εφαρμόζονται κατανεμημένα χωρίς κεντρικό αποθετήριο και συνήθως χωρίς κεντρική αρχή (δηλαδή, τράπεζα, εταιρεία ή κυβέρνηση). Στο βασικό τους επίπεδο, επιτρέπουν σε μια κοινότητα χρηστών να καταγράφει συναλλαγές σε ένα κοινό μητρώο εντός αυτής της κοινότητας, έτσι ώστε υπό κανονική λειτουργία του δικτύου αυτού (Blockchain) καμία συναλλαγή να μην μπορεί να αλλάξει μετά τη δημοσίευσή της.

Το 2008, η ιδέα του Blockchain συνδυάστηκε με αρκετές άλλες τεχνολογίες και υπολογιστικές έννοιες με σκοπό τη δημιουργία σύγχρονων Cryptocurrencies: Κρυπτόνομισμάτων: ηλεκτρονικά μετρητά που προστατεύονται μέσω κρυπτογραφικών μηχανισμών αντί να διασφαλίζονται από ένα κεντρικό αποθετήριο ή δημόσια αρχή. Το πρώτο τέτοιου είδους κρυπτο-νόμισμα που βασίζεται σε Block chain τεχνολογία είναι το Bitcoin.

Εντός του Blockchain, οι πληροφορίες που αντιπροσωπεύουν τα ηλεκτρονικά μετρητά επισυνάπτονται σε μια ψηφιακή διεύθυνση. Οι χρήστες του Bitcoin επί παραδείγματι μπορούν να υπογράψουν ψηφιακά και να μεταφέρουν δικαιώματα αυτών των πληροφοριών σε άλλον χρήστη ενώ το Bitcoin καταγράφει αυτή τη μεταφορά δημόσια, επιτρέποντας σε όλους τους συμμετέχοντες στο δίκτυο να ελέγχουν την εγκυρότητα των συναλλαγών. Το Bitcoin αποθηκεύεται και συντηρείται από μια κατανεμημένη ομάδα συμμετεχόντων. Αυτό, μαζί με ορισμένους κρυπτογραφικούς μηχανισμούς, κάνει το Blockchain ανθεκτικό σε προσπάθειες αλλαγής μετέπειτα ως προς τις οικονομικές συναλλαγές.

Η τεχνολογία Blockchain είναι το θεμέλιο των σύγχρονων κρυπτονομισμάτων, τα οποία ονομάστηκαν έτσι λόγω της έντονης χρήσης των κρυπτογραφικών λειτουργιών. Οι χρήστες χρησιμοποιούν δημόσιο και ιδιωτικό κλειδί για την ψηφιακή υπογραφή τους και την ασφαλή διαπραγμάτευση εντός του συστήματος. Τα δίκτυα Blockchain είναι βασισμένα σε δίκτυα τα οποία χρησιμοποιούν χρήστες «εξόρυξης». Υφίσταται η δυνατότητα επιβράβευσης με μια σταθερή ποσότητα κρυπτο-νομισμάτων μέσω της χρησιμοποίησης κρυπτογραφικών λειτουργιών. Ωστόσο, η τεχνολογία Blockchain μπορεί να εφαρμοστεί ευρύτερα από τα κρυπτονομίσματα. Σε αυτή την εργασία, εστιάζουμε στην περίπτωση χρήσης κρυπτονομισμάτων, καθώς αυτή είναι η

πρωταρχική χρήση της τεχνολογίας σήμερα. Ωστόσο, υπάρχει αυξανόμενο ενδιαφέρον για άλλους τομείς.

Οι υλοποιήσεις Blockchain τεχνολογίας σχεδιάζονται συχνά με συγκεκριμένο σκοπό ή λειτουργία. Οι λειτουργίες των παραδειγμάτων στη διεθνή βιβλιογραφία περιλαμβάνουν κρυπτονομίσματα, έξυπνες συμβάσεις (λογισμικό που αναπτύσσεται στο Blockchain και εκτελείται από υπολογιστές που λειτουργούν με αυτό το Block chain) και κατανεμημένα συστήματα λογιστικών βιβλίων μεταξύ επιχειρήσεων. Υπήρξε μια συνεχής ροή εξελίξεων στον τομέα της τεχνολογίας Blockchain, με νέες πλατφόρμες που ανακοινώνονται συνεχώς - το τοπίο στο αντικείμενο αυτό μεταβάλλεται συνεχώς.

Παρά τις πολλές παραλλαγές των δικτύων Blockchain και την ταχεία ανάπτυξη νέων τεχνολογιών που σχετίζονται με τα Blockchain, τα περισσότερα δίκτυα Blockchain χρησιμοποιούν κοινές βασικές έννοιες. Οι δομές αυτές είναι ένας κατανεμημένος κύκλος που αποτελείται από μπλοκ [blocks]. Κάθε μπλοκ αποτελείται από μια κεφαλίδα μπλοκ που περιέχει μετα-δεδομένα σχετικά με το μπλοκ. Κάθε κεφαλίδα του μπλοκ περιέχει μια κρυπτογραφική σύνδεση με την κεφαλίδα ενός διαφορετικού μπλοκ. Κάθε συναλλαγή περιλαμβάνει έναν ή περισσότερους χρήστες δικτύων μπλοκ και μια καταγραφή του τι υπογράφεται ψηφιακά από τον χρήστη που εμπλέκεται στη κάθε συναλλαγή.

Η τεχνολογία Blockchain λαμβάνει τις υπάρχουσες, αποδεδειγμένες έννοιες δικτύων και τις συγχωνεύει σε μια ενιαία τεχνική λύση. Η τεχνολογία Blockchain είναι ακόμα νέα και θα πρέπει να διερευνηθεί με την οπτική της πιθανής ωφέλειας αντί της αναγκαστικής συμμόρφωσης υφισταμένων δομών με τα πρότυπα της τεχνολογίας Blockchain. Οι οργανισμοί, όπως εξάγεται ως συμπέρασμα στη παρούσα εργασία πρέπει να αντιμετωπίζουν την τεχνολογία Blockchain όπως και οποιαδήποτε άλλη τεχνολογική λύση που διαθέτουν και να την χρησιμοποιήσουν σε κατάλληλες καταστάσεις. Στόχος λοιπόν αυτής της εργασίας αποτελεί η κατάδειξη της σύνδεσης και της χρησιμότητας των Blockchain τεχνολογιών στις αποφάσεις περί της στρατηγικής στο marketing.

Εννοιολογήσεις [Blockchain – Cryptocurrencies – Marketing Strategies]

Το 2008, η ιδέα του Blockchain συνδυάστηκε με αρκετές άλλες τεχνολογίες και υπολογιστικές έννοιες για τη δημιουργία σύγχρονων cryptocurrencies: η τεχνολογία αυτή έγινε ευρέως γνωστή το 2009 με την κυκλοφορία του δικτύου Bitcoin, το πρώτο από τα πολλά σύγχρονα κρυπτονομίσματα.

Η τεχνολογία Blockchain επέτρεψε την ανάπτυξη πολλών συστημάτων κρυπτονομίσματος όπως το Bitcoin και το Ethereum. Εξαιτίας αυτού, η τεχνολογία Blockchain συχνά θεωρείται ότι δεσμεύεται με το νόμισμα Bitcoin ή πιθανώς με παρόμοιες λύσεις κρυπτογράφησης γενικά. Ωστόσο, η τεχνολογία είναι διαθέσιμη για μια ευρύτερη ποικιλία εφαρμογών και διερευνάται για διάφορους τομείς της οικονομίας.

Τα συστατικά της τεχνολογίας Blockchain μαζί με την εξάρτησή της από τα κρυπτογραφικά πρωτογενή και τα κατανεμημένα συστήματα μπορούν να τα καταστήσουν δύσκολο ως προς την κατανόηση τους. Ωστόσο, κάθε συστατικό μπορεί να περιγραφεί απλά και να χρησιμοποιηθεί ως δομικό στοιχείο για την κατανόηση ενός πολύπλοκου συστήματος.

Τα Blockchains μπορούν να οριστούν ανεπίσημα ως:

Τα Blockchains είναι κατανεμημένες ψηφιακές δομές κρυπτογραφικά υπογεγραμμένων συναλλαγών που ομαδοποιούνται σε μπλοκ. Κάθε block είναι κρυπτογραφικά συνδεδεμένο με το προηγούμενο αφού επικυρωθεί και υποβληθεί σε απόφαση συναίνεσης στο πλαίσιο μιας συναλλαγής. Καθώς προστίθενται νέα μπλοκς, γίνονται πιο δύσκολα να τροποποιηθούν τα παλαιότερα μπλοκ.

Είναι γεγονός ότι πολλά συστήματα ηλεκτρονικών μετρητών υπήρχαν πριν από την εμφάνιση του Bitcoin (π.χ. ecash και NetCash), αλλά κανένα από αυτά δεν κατόρθωσε να απολαύσει μιας ευρείας χρήσης λειτουργία. Η χρήση ενός Blockchain επέτρεψε τη λειτουργία του Bitcoin με κατανεμημένο τρόπο έτσι ώστε κανένας χρήστης να μην ελέγχει τα ηλεκτρονικά μετρητά αυτονόμως. Το κύριο πλεονέκτημα του ήταν ότι επέτρεπε άμεσες συναλλαγές μεταξύ χρηστών χωρίς την ανάγκη διαμεσολάβησης ενός αξιόπιστου τρίτου μέρους, όπως για παράδειγμα μια κεντρική τράπεζα. Επίσης, επέτρεψε την έκδοση μιας νέας κατεύθυνσης κρυπτογράφησης με καθορισμένο τρόπο

σε εκείνους τους χρήστες που καταφέρνουν να δημοσιεύουν νέα μπλοκ και να διατηρούν αντίγραφα. Αυτοί οι χρήστες ονομάζονται «ανθρακωρύχοι» στο Bitcoin. Η αυτοματοποιημένη πληρωμή των «ανθρακωρύχων» επέτρεψε την κατανεμημένη διαχείριση του συστήματος χωρίς να χρειάζεται να οργανωθεί κεντρικά. Χρησιμοποιώντας ένα Blockchain και μια συναινετική πολιτική συντήρησης, δημιουργήθηκε ένας μηχανισμός αυτο-αστυνόμευσης που εξασφάλισε την προσθήκη μόνο έγκυρων συναλλαγών και μπλοκ στο πλαίσιο του Blockchain.

Στο Bitcoin για παράδειγμα, το Blockchain επέτρεψε στους χρήστες να χρησιμοποιούν ψευδώνυμο. Αυτό σημαίνει ότι οι χρήστες είναι ανώνυμοι, αλλά τα αναγνωριστικά λογαριασμού τους δεν είναι. Επιπλέον, όλες οι συναλλαγές είναι δημόσια ορατές. Αυτό έχει επιτρέψει στην Bitcoin να προσφέρει μια ψευδο-ανωνυμία επειδή οι λογαριασμοί μπορούν να δημιουργηθούν χωρίς καμία διαδικασία αναγνώρισης ή εξουσιοδότησης.

Για τα δίκτυα Blockchain που επιτρέπουν σε οποιονδήποτε να δημιουργεί λογαριασμούς και να συμμετέχει ανώνυμα (αποκαλούμενα δίκτυα Blockchain χωρίς άδεια), αυτές οι δυνατότητες παρέχουν ένα επίπεδο εμπιστοσύνης μεταξύ των μερών χωρίς προηγούμενη γνώση του άλλου-ετέρου μέρους ως χρήστη. Αυτή η εμπιστοσύνη μπορεί να επιτρέψει σε ιδιώτες και οργανισμούς να πραγματοποιήσουν απευθείας συναλλαγές, γεγονός που μπορεί να οδηγήσει σε ταχύτερες και λιγότερο δαπανηρές συναλλαγές. Για ένα δίκτυο Blockchain που ελέγχει πιο στενά την πρόσβαση (καλούμενα δίκτυα Blockchain με άδεια χρήσης), όπου μπορεί να υπάρχει κάποια εμπιστοσύνη μεταξύ των χρηστών, αυτές οι δυνατότητες συμβάλλουν στην ενίσχυση αυτής της εμπιστοσύνης.

Η ορολογία για την τεχνολογία Blockchain ποικίλλει από τη μια εφαρμογή στην άλλη. Σε όλο το κείμενο της εργασίας θα χρησιμοποιηθούν οι ακόλουθοι όροι:

• *Blockchain*

• *Τεχνολογία Blockchain* - ένας όρος που περιγράφει την τεχνολογία με τη γενικότερη μορφή

• *Δίκτυο αποκλεισμού* - το δίκτυο στο οποίο χρησιμοποιείται ένα Blockchain

• *Εφαρμογή Blockchain* - ένα συγκεκριμένο Blockchain

• *Χρήστης δικτύου Blockchain* - άτομο, οργανισμός, οντότητα, επιχείρηση, κυβέρνηση, κλπ.

• *Κόμβος* - ένα μεμονωμένο σύστημα εντός ενός δικτύου Blockchain

Ο πλήρης κόμβος είναι ένας κόμβος που αποθηκεύει ολόκληρο το Blockchain, εξασφαλίζοντας ότι οι συναλλαγές είναι έγκυρες. Ο κόμβος δημοσίευσης αποτελεί έναν πλήρη κόμβο που δημοσιεύει επίσης νέα μπλοκ. Ο ελαφρύς κόμβος τέλος, είναι ένας κόμβος που δεν αποθηκεύει ή διατηρεί ένα αντίγραφο του Blockchain και πρέπει να μεταφέρει τις συναλλαγές του σε πλήρεις κόμβους

Τα δίκτυα Blockchain μπορούν να κατηγοριοποιηθούν με βάση το μοντέλο άδειας, το οποίο καθορίζει ποιος μπορεί να τα διατηρήσει (π.χ. να λειτουργεί - δημοσιεύει μπλοκ). Με απλά λόγια, ένα εξουσιοδοτημένο δίκτυο αποκλεισμού είναι όπως ένα εταιρικό intranet που ελέγχεται, ενώ ένα αδέσμευτο δίκτυο Blockchain είναι σαν το δημόσιο διαδίκτυο, όπου μπορεί κανείς να συμμετάσχει. Τα αδειοδοτημένα δίκτυα Blockchain αναπτύσσονται συχνά προς χάριν μιας ομάδας οργανισμών και ατόμων, και τυπικά αναφέρεται ως κοινοπραξία.

Η τεχνολογία Blockchain μπορεί να φαίνεται πολύπλοκη. Ωστόσο, μπορεί να απλοποιηθεί εξετάζοντας κάθε στοιχείο ξεχωριστά. Σε υψηλό επίπεδο, η τεχνολογία Blockchain χρησιμοποιεί γνωστούς μηχανισμούς πληροφορικής και κρυπτογραφικά στοιχεία (κρυπτογραφικές λειτουργίες κατακερματισμού, ψηφιακές υπογραφές, κρυπτογράφηση ασύμμετρου κλειδιού) σε συνδυασμό με την υιοθέτηση εννοιών όπως της τήρησης αρχείων.

Μια συναλλαγή στο Blockchain αντιπροσωπεύει μια αλληλεπίδραση μεταξύ των μερών. Με τα κρυπτονομίσματα για παράδειγμα, μια συναλλαγή αντιπροσωπεύει μια μεταφορά του κρυπτονομίσματος (αριθμού κρυπτονομισμάτων) μεταξύ των χρηστών δικτύου Blockchain. Όσον αφορά στα σενάρια μεταξύ επιχειρήσεων, μια συναλλαγή μπορεί να είναι ένας τρόπος καταγραφής των δραστηριοτήτων που πραγματοποιούνται σε ψηφιακά ή φυσικά περιουσιακά στοιχεία. Για ορισμένες υλοποιήσεις Blockchain, μια σταθερή προσφορά νέων blocks (ακόμη και με μηδενικές συναλλαγές) είναι κρίσιμη για τη διατήρηση της ασφάλειας του συγκεκριμένου δικτύου Blockchain. Μέσω μιας διαρκούς διάθεσης νέων blocks, αποτρέπονται οι κακόβουλοι χρήστες από

το να "προφθάσουν" και να κατασκευάσουν ένα μακρύτερο, τροποποιημένο Blockchain.

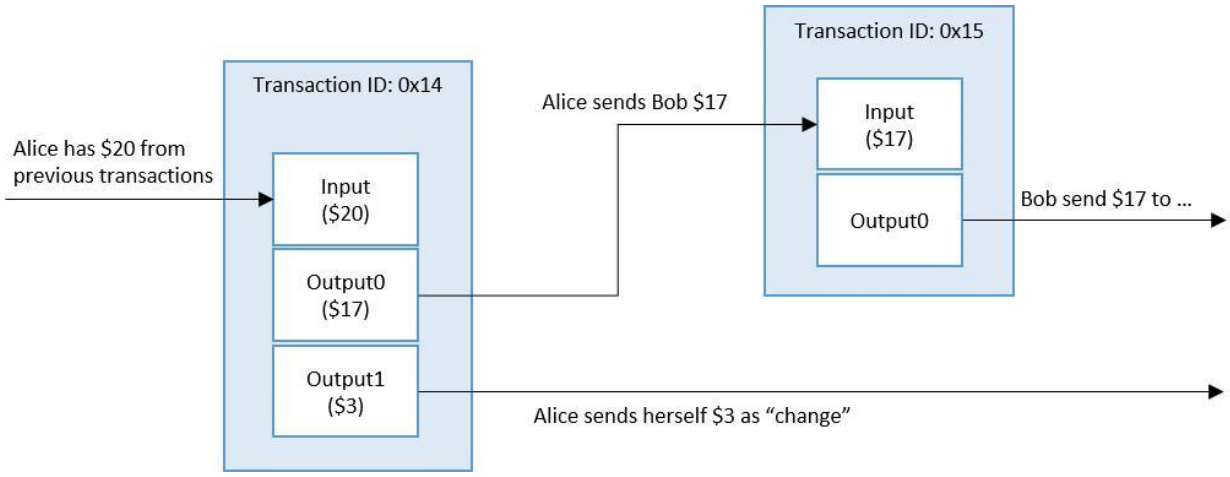
Τα δεδομένα που περιλαμβάνουν μια συναλλαγή μπορεί να είναι διαφορετικά για κάθε εφαρμογή Blockchain, ωστόσο ο μηχανισμός διαπραγμάτευσης είναι σε μεγάλο βαθμό είναι ο ίδιος. Ένας χρήστης δικτύου στέλνει πληροφορίες στο δίκτυο Blockchain. Οι πληροφορίες που αποστέλλονται μπορεί να περιλαμβάνουν τη διεύθυνση του αποστολέα (ή άλλο σχετικό αναγνωριστικό), το δημόσιο κλειδί του αποστολέα, την ψηφιακή υπογραφή, τις εισροές συναλλαγών και τις εξερχόμενες συναλλαγές.

Μια ενιαία συναλλαγή κρυπτογράφησης απαιτεί τουλάχιστον τις ακόλουθες πληροφορίες:

• **Είσοδοι** - Οι είσοδοι είναι συνήθως μια λίστα των ψηφιακών στοιχείων που πρόκειται να μεταφερθούν. Μια συναλλαγή θα αναφέρεται στην πηγή του ψηφιακού στοιχείου (προέλευση) - είτε στην προηγούμενη συναλλαγή η οποία δόθηκε από τον αποστολέα, είτε στην περίπτωση νέων ψηφιακών στοιχείων. Δεδομένου ότι η είσοδος στη συναλλαγή αποτελεί σταθερή αναφορά σε παρελθόντα γεγονότα, τα ψηφιακά στοιχεία ενεργητικού δεν αλλάζουν. Στην περίπτωση των κρυπτονομισμάτων αυτό σημαίνει ότι η αξία δεν μπορεί να προστεθεί ή να αφαιρεθεί από τα υπάρχοντα ψηφιακά περιουσιακά στοιχεία. Αντίθετα, ένα ενιαίο ψηφιακό στοιχείο μπορεί να χωριστεί σε πολλαπλά νέα ψηφιακά στοιχεία (καθένα με μικρότερη αξία) ή πολλαπλά ψηφιακά στοιχεία μπορούν να συνδυαστούν για να σχηματίσουν λιγότερα νέα ψηφιακά στοιχεία (με αντίστοιχα μεγαλύτερη τιμή). Ο διαχωρισμός ή ο συνδυασμός περιουσιακών στοιχείων θα προσδιοριστεί στο πλαίσιο της παραγωγής της συναλλαγής.Ο αποστολέας πρέπει επίσης να παρέχει απόδειξη ότι έχει πρόσβαση στις αναφερόμενες εισόδους, γενικά υπογράφοντας ψηφιακά τη συναλλαγή - αποδεικνύοντας την πρόσβαση στο ιδιωτικό κλειδί.

• **Έξοδοι** - Οι εκροές είναι συνήθως οι λογαριασμοί οι οποίοι αποτελούν τους παραλήπτες των ψηφιακών στοιχείων καθώς και το ποσό του ψηφιακού στοιχείου που θα λάβουν. Κάθε έξοδος προσδιορίζει τον αριθμό των ψηφιακών στοιχείων που μεταφέρονται στους νέους ιδιοκτήτες, το αναγνωριστικό του νέου ιδιοκτήτη (ών) και ένα σύνολο προϋποθέσεων που πρέπει να πληρούν οι νέοι ιδιοκτήτες για να

δαπανήσουν την τιμή αυτή. Εάν τα ψηφιακά στοιχεία που παρέχονται είναι περισσότερα από αυτά που απαιτούνται, τα επιπλέον κεφάλαια πρέπει να αποστέλλονται ρητά στον αποστολέα (αυτός είναι ένας μηχανισμός για την "πραγματοποίηση αλλαγών").



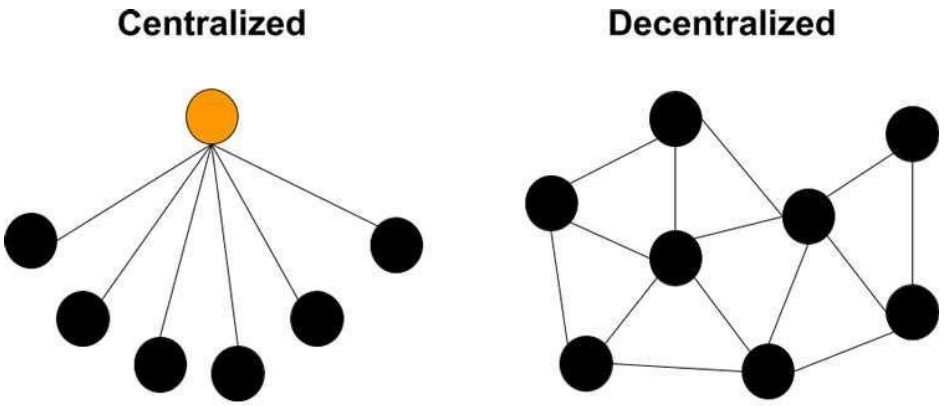
Example Cryptocurrency Transaction

Η διακυβέρνηση των δικτύων Blockchain ασχολείται με τους κανόνες, τις πρακτικές και τις διαδικασίες με τις οποίες κατευθύνεται και ελέγχεται το δίκτυο Blockchain. Μια κοινώς εσφαλμένη αντίληψη είναι ότι τα δίκτυα Blockchain αποτελούν συστήματα χωρίς έλεγχο και ιδιοκτησία. Αυτό όμως δεν ισχύει σε αυστηρά πλαίσια. Τα εξουσιοδοτημένα δίκτυα Blockchain είναι γενικά εγκατεστημένα και λειτουργούν από έναν ιδιοκτήτη ή κοινοπραξία, ο οποίος έχει αναλάβει τη διακυβέρνηση του δικτύου Blockchain. Τα δίκτυα Blockchain χωρίς άδεια διέπονται συχνά από χρήστες του δικτύου εκδότες κόμβων και προγραμματιστές λογισμικού. Κάθε ομάδα έχει ένα επίπεδο ελέγχου που επηρεάζει την κατεύθυνση της εξέλιξης του δικτύου Block chain.

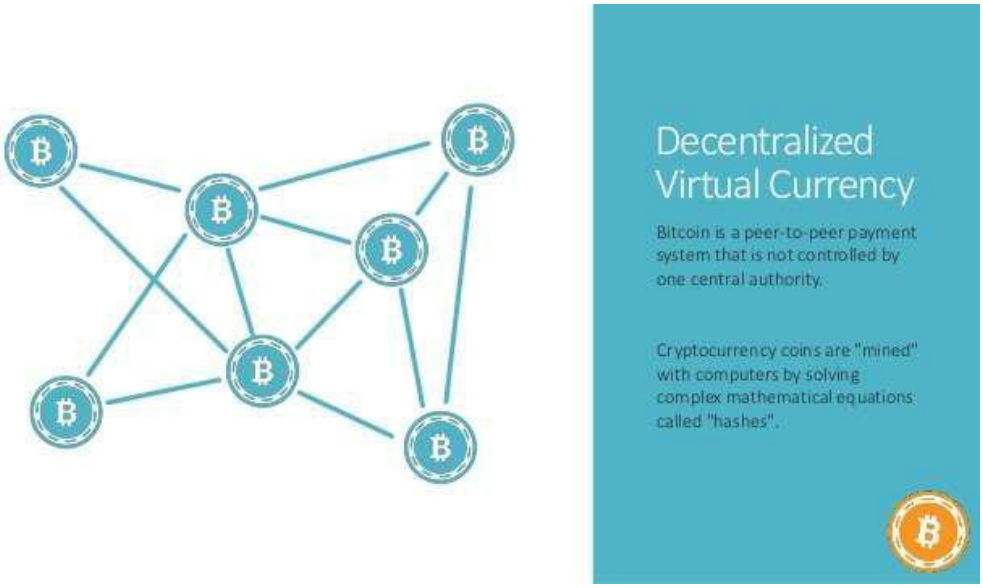
Για να κατανοήσουμε πλήρως την έννοια των κρυπτονομισμάτων, είναι απαραίτητο να κατανοήσουμε την έννοια των αποκεντρωμένων νομισμάτων. Η έννοια των αποκεντρωμένων νομισμάτων είναι το καθοριστικό χαρακτηριστικό των κρυπτονομισμάτων. Σήμερα, τα κρυπτονομίσματα προσφέρουν πρωτοποριακές προόδους που είναι ποικίλες και μεταμορφωτικές. Επιπλέον, θα μπορούσε επίσης να θεωρηθεί επένδυση στο αυριανό χρηματοπιστωτικό σύστημα - αποκεντρωμένη χρηματοδότηση (DeFi).

Το DeFi είναι ένα αναδυόμενο εναλλακτικό χρηματοπιστωτικό σύστημα που βασίζεται σε ένα δημόσιο blockchain, το οποίο επιτρέπει μεγαλύτερη προσβασιμότητα, επειδή ο καθένας έχει τη δυνατότητα να συνδεθεί σε αυτό. Επιπλέον, οι συναλλαγές είναι δημόσια ορατές, επιτρέποντας μεγαλύτερη διαφάνεια σε όλο το σύστημα.

Η δυνατότητα των συναλλασσομένων κρυπτονομισμάτων να παρακάμπτουν κυβερνητικά εγκεκριμένα χρηματοπιστωτικά ιδρύματα διακρίνει τα κρυπτονομίσματα από τα επίσημα κεντρικά νομίσματα των χρηματοπιστωτικών ιδρυμάτων. Το παρακάτω σχήμα (King, 2018) απεικονίζει αυτή την αρχή για κρυπτονομίσματα (η πορτοκαλί κουκίδα). Το αμέσως επόμενο σχήμα (Gagliardi, 2014) απεικονίζει αυτή την κεντρική ιδέα για το Bitcoin.



Centralized and decentralized currencies



Bitcoin - a decentralized cryptocurrency brand

Βασικά, το κρυπτογραφικό χρήμα είναι ένα προηγμένο ή εικονικό χρήμα που προορίζεται να αποτελέσει συμπλήρωμα του εμπορικού μηχανισμού. Χρησιμοποιεί την κρυπτογραφία για να επαληθεύει και να επιβεβαιώνει τις ανταλλαγές, ακριβώς για να ελέγχει τη δημιουργία νέων μονάδων συγκεκριμένου ψηφιακού χρήματος. Βασικά, τα περίφημα «cryptocurrencies» είναι περιορισμένες ενότητες σε μια βάση δεδομένων που κανείς δεν μπορεί να αλλάξει εκτός εάν πληρούνται ρητές προϋποθέσεις. Διαφορετικοί υποστηρικτές όπως η καινοτομία Blockchain πίσω από τα κρυπτονομίσματα, διατηρούν το σκεπτικό ότι είναι ένα αποκεντρωμένο πλαίσιο προετοιμασίας και καταγραφής και μπορεί να είναι πιο ασφαλές από τα συμβατικά πλαίσια νομισμάτων. Ακολουθεί μια λίστα για ορισμένα από τα πρακτικά πλεονεκτήματα που εφαρμόζονται στα κρυπτονομίσματα.

Περιπτώσεις χρήσεις	Ονομασία	Περιγραφή
Πληρωμές	Bitcoin Ripple (XRP) Stellar Dash	Χρησιμοποιείται για την αγορά αγαθών χωρίς την ανάγκη αξιόπιστου τρίτου μέρους
Αποθήκευση αξίας	Bitcoin Litecoin	Καθώς η συνολική προσφορά πολλών κρυπτονομισμάτων είναι περιορισμένη, αυτή η έλλειψη επηρεάζει την αξία τους
Σταθερά νομίσματα	DAI USDC GeminiUSD	Ψηφιακό χρήμα που συνήθως συνδέεται με ένα νόμισμα ή ένα εμπόρευμα, όπως ο χρυσός
Ιδιωτικότητα	Monero Zcash	Η κρυπτογραφία, η τεχνολογία πίσω από το crypto, μπορεί να επιτρέψει την ανωνυμία των κατόχων της
Ψηφιακή Ιδιοκτησία	Bitcoin Ripple (XRP) Stellar	Μπορεί να εξουσιοδοτήσει αυτούς που δεν έχουν πρόσβαση σε τράπεζα να εισέλθουν στο χρηματοοικονομικό σύστημα

Ψηφιακός Χρυσός	Bitcoin	Το Bitcoin μοιράζεται παρόμοια χαρακτηριστικά με τα χρήματα: ένα μέσο ανταλλαγής, μονάδα λογαριασμού και αποθήκευση αξίας
Αποκεντρωμένες Εφαρμογές (DApps)	EOS Tezos Ethereum (ETH)	Επιτρέπει σε άτομα να δημιουργούν εφαρμογές χωρίς κεντρική αρχή, συνδέοντας απευθείας τον χρήστη και τον δημιουργό

Σε κάθε περίπτωση, χωρίς το Blockchain, δεν θα είχαμε μεθόδους για την καταγραφή αυτών των ανταλλαγών. Παρά τις εγγενείς αντιθέσεις ως προς τη χρησιμότητα μεταξύ των δύο οντοτήτων, το κρυπτογραφικό χρήμα και το Blockchain μπορούν να συλλειτουργούν με αξιοθαύμαστο τρόπο.

Τα περίφημα "Cryptocurrencies" προσφέρουν μια μέθοδο για την αμοιβή των πελατών του Blockchain. Τα ICOs (Initial Coin Offerings) έχουν καταλήξει να αποτελούν μια πρακτική μέθοδο με σκοπό την άντληση περιουσιακών στοιχείων. Το συνολικό σχήμα μοιάζει με την έκδοση ομολόγων μεταξύ συμβαλλόμενων μερών στο πλαίσιο μιας οικονομικής ανταλλαγής, αλλά στην προκειμένη περίπτωση οι πελάτες καθίστανται ταυτόχρονα επενδυτές.

Το Cryptocurrency είναι σημαντικό να "εκτελεστεί" σε ένα Blockchain διότι χωρίς το Blockchain, δεν θα είχαμε μεθόδους για την καταγραφή αυτών των ανταλλαγών.

Το 2017 ήταν ένα σημαντικό μεταιχμιακό έτος για τα ψηφιακά νομίσματα, καθώς η κεφαλαιοποίηση της αγοράς εξελίχθηκε από περίπου 18 δισεκατομμύρια δολάρια τον Ιανουάριο του 2017 σε 800 δισεκατομμύρια δολάρια τον Ιανουάριο του 2018. Από το έτος όμως αυτό και έπειτα παρατηρήθηκε μια τεράστια τροποποίηση, καθώς το κόστος σχεδόν όλων των ψηφιακών μορφών χρημάτων μειώθηκε και η κεφαλαιοποίησή τους στην αγορά έφθασε σε ένα υποβαθμισμένο σημείο ύψους 254 δισεκατομμυρίων δολαρίων προς την αρχή του Απριλίου 2018. Σύμφωνα με εκτιμήσεις, «*το 2019-2020*

θα είναι η περίοδος κατά την οποία οι μεγάλοι παίκτες μπαίνουν στον κόσμο του crypto "(H. Aslanian, 2019).

Cryptocurrencies

1. Bitcoin (BTC)

Το ενδιαφέρον για το πρώτο crypto - Bitcoin το οποίο δημιουργήθηκε το 2008, είναι ότι κανείς δεν ξέρει ποιος το δημιούργησε. (P. Vinga, 2017). "Το BTC είναι η πιο σημαντική εφεύρεση στον κόσμο από το Διαδίκτυο" (RogerVer, 2017)

Θετικές πλευρές του Bitcoin

• Είναι το πλέον εδραιωμένο ψηφιακό χρήμα, διαθέτει το μεγαλύτερο δίκτυο μηχανικών και χρηματοοικονομικών ειδικών που το υποστηρίζουν για περαιτέρω ανάπτυξη.

• Το Bitcoin λαμβάνεται υπόψιν από την τυπική οικονομία. Οι εταιρείες Bloomberg, Microsoft, Overstock.com, Expedia.com και πολλές άλλες έχουν αρχίσει να συναλλάσσονται με το BTC.

Αρνητικές πλευρές του Bitcoin

• Το Bitcoin αντιμετωπίζει τεράστιες δυσκολίες στην χρονική κλιμάκωση στη συναλλαγή. Μια ανταλλαγή Bitcoin διαρκεί περίπου 9-10 λεπτά, και το σύστημα μπορεί να επεξεργαστεί μόνο περίπου 7 ανταλλαγές για κάθε δευτερόλεπτο.

• Το «ορυχείο», το οποίο αποτελεί σημαντική δράση για οποιοδήποτε ψηφιακό νόμισμα, έχει κινηθεί προς την κατεύθυνση της βαθιάς συγκέντρωσης. Η εξόρυξη

Bitcoin είναι προς το παρόν αντιληπτή μόνο με δαπανηρό, πολύ απίστευτο εξοπλισμό που χρησιμοποιεί υπολογιστική ισχύ.

• Οι χρεώσεις συναλλαγών για την αποστολή του Bitcoin είναι επίσης σε ένα αξεπέραστο βαθμό υψηλές.

2. Ethereum (Ether)

Το Ethereum είναι το δεύτερο πιο κερδοφόρο κρυπτογραφικό χρήμα μετά το Bitcoin. Κατασκευάστηκε το 2015 από τον Vitalik Buterin, και είναι στην πραγματικότητα πολύ περισσότερο από ηλεκτρονικά μετρητά. Το Ethereum είναι ένα στάδιο νομίσματος θεμελιωμένο σε Blockchain τεχνολογία με σκοπό τη δημιουργία αποκεντρωμένων εφαρμογών.

Θετικές πλευρές του Ethereum

• Είναι το πιο γνωστό στάδιο το οποίο σχετίζεται με συμβόλαια κατανόησης δομών, κάτι που θεωρείται ως το πολύ σημαντικό στο σύμπαν του ψηφιακού νομίσματος.

Το Ethereum έχει μεγαλύτερη ταχύτητα ανταλλαγής σε σχέση με το Bitcoin.

Αρνητικές πλευρές του Ethereum

Όπως το Bitcoin, το Ethereum αντιμετωπίζει επιπλέον δύσκολα ζητήματα όσον αφορά στην ευελιξία. Παρ 'όλα αυτά χρησιμοποιεί ένα ξεπερασμένο όργανο (Proof-of-Work) για να ελέγξει τις ανταλλαγές του συστήματος. Το Ethereum απλά υποστηρίζει μια γλώσσα κωδικοποίησης

3. Bitcoin Cash (BCH)

Το Bitcoin Cash έχει αποσπασθεί από το ίδιο το Bitcoin το 2016.

Το κίνητρο πίσω από το BCH ήταν να φροντίσει ένα μέρος των σημερινών ζητημάτων του Bitcoin, ιδιαίτερα όσον αφορά την ευελιξία και τις χρεώσεις ανταλλαγής.

Πλεονεκτήματα του Bitcoin Cash

• Τα χρηματιστήρια σε Bitcoin Cash είναι ταχύτερα όσον αφορά στις ανταλλαγές Bitcoin ως αποτέλεσμα της επέκτασης σε μεγέθη MB σε αντίθεση με το Bitcoin.

• Οι μέσες δαπάνες ανταλλαγής Bitcoin είναι αυτή τη στιγμή γύρω στα 1,8 δολάρια που έχουν μειωθεί στα 0,067 δολάρια για λογαριασμό του Bitcoin Cash.

Μειονεκτήματα του Bitcoin Cash

• Το Bitcoin Cash, όπως το Bitcoin, απαιτείται να είναι αποκεντρωμένο.

• Η εξόρυξη BCH είναι τόσο δαπανηρή όσο η εξόρυξη Bitcoin, ωστόσο, δίνει λιγότερες αποδόσεις

• Το Bitcoin Cash δεν είναι τόσο αποτελεσματικά προσβάσιμο στις συναλλαγές ψηφιακού χρήματος όπως και τα άλλα διάσημα κρυπτονομίσματα.

4. Litecoin (LTC)

Το Litecoin δημιουργήθηκε το 2011 από τον Charlie Lee, πρώην στέλεχος της Google. Βασίστηκε στο Blockchain του ίδιου του Bitcoin, με σκοπό τη βελτίωση του. Με αυτόν τον τρόπο, το Litecoin είναι μόνο μηχανογραφημένα μετρητά. Το Litecoin έχει καταφέρει να ανέλθει στα καλύτερα κρυπτονομίσματα.

Θετικές πλευρές του Litecoin

• Η συναλλαγή σε Litecoin διαρκεί περίπου 150 δευτερόλεπτα, ενώ χρειάζονται περισσότερα από 9-10 λεπτά για να ολοκληρωθεί η ανταλλαγή Bitcoin. Αυτός είναι ο λόγος για τον οποίο το όνομά του αρχίζει με το "Φως".

• Οι μέσες χρεώσεις ανταλλαγής Litecoin είναι περίπου 0,179 δολάρια που είναι 100 φορές φθηνότερες από τις αντίστοιχες του Bitcoin.

Αρνητικές πλευρές του Litecoin

• Εκτός από την ταχύτητα ανταλλαγής, δεν υπάρχει άλλο προτέρημα του Litecoin, το οποίο μπορεί να το διαχωρίσει ουσιαστικά από τα άλλα κρυπτονομίσματα.

• Όπως η «εξόρυξη» Bitcoin, έτσι και η «εξόρυξη» Litecoin είναι επιπλέον δαπανηρή και περιορίζεται σε εκείνους με ιδιαίτερα απίστευτο εξοπλισμό.

Η κρυπτογραφία χρησιμοποιείται επίσης για να διαχειριστεί την παραγωγή επιπλέον κρυπτο-μονάδων. Ένα από τα πιο σημαντικά προτερήματα των ψηφιακών μορφών χρημάτων είναι ότι δεν τα διαχειρίζονται κάποιου είδους γραφεία. Τα κρυπτονομίσματα μπορούν να ανταλλάσσονται μέσω κρυπτογραφικών πλατφορμών. Αυτές οι συναλλαγές των περίφημων "Cryptocurrencies" είναι στάδια μέσω των οποίων μπορεί να αγοράσει κάποιος ή να πωλήσει ηλεκτρονικά νομισματικά πρότυπα για δολάρια, ευρώ και λίρες.

Η μεγάλη εικόνα:

Καθώς το crypto συνεχίζει να κερδίζει δυναμική, οι μακροπρόθεσμες επιπτώσεις του θα επικεντρωθούν. Βασικά, το κρυπτογραφικό ίδρυμά θέτει το στάδιο για μελλοντικές εξελίξεις στη χρηματοδότηση.

1. **Ιδωτικότητα.** Οι ανώνυμες συναλλαγές προστατεύουν τα δεδομένα των χρηστών μέσω κρυπτογραφικών τεχνικών.
2. **Προσβασιμότητα.** Παροχή νός νέου χρηματοοικονομικού μοντέλου για 1,7B άτομα που δεν έχουν τραπεζική πρόσβαση σε όλο τον κόσμο.
3. **Αποδοτικότητα.** Οι απότομες μειώσεις του χρόνου διακανονισμού και της αποτελεσματικότητας θα μπορούσαν να εξοικονομήσουν στους καταναλωτές 16 δισεκατομμύρια δολάρια ετησίως.
4. **Ασφάλεια.** Παροχή αμετάβλητων, ανιχνεύσιμων αρχείων δικτύων συναλλαγών πλούσιων σε ασφάλεια.
5. **Προγραμματιζόμενα χρήματα.** Οι έξυπνες συμβάσεις θα μπορούσαν να εξαλείψουν δραστικά τη χειρωνακτική και διοικητική εργασία - τελικά παρακάμπτοντάς τις εντελώς.

Βασισμένα σε αποκεντρωμένα και αυτόνομα συστήματα, τα κρυπτονομίσματα δημιουργούν ένα second-order effect στον χρηματοοικονομικό κόσμο. Τελικά, τα κρυπτονομίσματα βοηθούν στη μετατροπή των χρηματοοικονομικών όπως το γνωρίζουμε - ξεκλειδώνοντας αμέτρητες επενδυτικές ευκαιρίες σε ολόκληρη την παγκόσμια οικονομία.

Η εμφάνιση των κρυπτονομισμάτων και των συναφών τεχνολογιών είναι μέρος ενός ευρύτερου κύματος τεχνολογιών που διευκολύνουν το εμπόριο peer-to-peer (P2P), την εξατομίκευση των προϊόντων και την ευελιξία των μεθόδων παραγωγής. Για διάφορους

λόγους, αυτό το τεχνολογικό κύμα απέκτησε ένα συλλογικό θαυμασμό μετά την παγκόσμια οικονομική κρίση πριν από μια δεκαετία (2010) . Μεγάλες ψηφιακές πλατφόρμες, όπως οι Alibaba, Amazon, Uber και Airbnb, αντικαθιστούν πολλά καταστήματα τσιμέντου, εταιρείες παροχής υπηρεσιών και μακροχρόνιες εργασιακές σχέσεις.

Οι τεχνολογίες Blockchain στοχεύουν να προχωρήσουν ένα βήμα μακρύτερα. Οργανώνουν τις πράξεις P2P και τις ροές πληροφοριών P2P χωρίς εταιρίες που λειτουργούν ψηφιακές πλατφόρμες. Το εάν οι τεχνολογίες αυτές θα εξαλείψουν εντελώς τους μεσάζοντες ή αν προκύψουν νέες μορφές αξιόπιστων διαμεσολαβητών παραμένει προς συζήτηση.

Τα κρυπτονομίσματα τελικά είναι η πρώτη - και ως εκ τούτου η πιο ανεπτυγμένη - εφαρμογή τεχνολογιών Blockchain. Δημιουργούν χρήματα χωρίς κεντρικές τράπεζες και διευκολύνουν πληρωμές χωρίς χρηματοπιστωτικά ιδρύματα. Η επιτυχία πολλών κρυπτονομισμάτων θέτει ανταγωνιστικές πιέσεις στις μεθόδους συναλλαγών από τα υφιστάμενα χρηματοπιστωτικά ιδρύματα.

Ωστόσο, έχουν αναδυθεί εμφανείς σοβαροί περιορισμοί. Η αποκεντρωμένη οργάνωση των αγορών χωρίς εμπιστευμένους μεσάζοντες μπορεί να είναι πολύ δαπανηρή και η αστάθεια της αξίας των κρυπτονομισμάτων αποτελεί σημαντικό εμπόδιο για να νομιμοποιηθούν ως εναλλακτικές λύσεις τα κρυπτονομίσματα έναντι του νόμιμου χρήματος.

Τα κρυπτονομίσματα έχουν προκαλέσει έντονες αντιδράσεις. Οι κριτικοί ονομάζουν αυτές τις εικονικές συναλλαγές μια φούσκα, μια απάτη (Krugman 2013, Popper 2018). Οι υποστηρικτές αντιθέτως προβλέπουν ότι τα κρυπτονομίσματα θα αντικαταστήσουν τελικά τα χρήματα (Rooney 2018).

Δεν είναι σαφές πώς αυτές οι τεχνολογίες θα αναπτυχθούν μακροπρόθεσμα. Πιθανόν να απορροφηθούν από τα υπάρχοντα θεσμικά όργανα, οι κεντρικές τράπεζες θα εκδίδουν ψηφιακά μετρητά, οι κυβερνήσεις θα χρησιμοποιούν το Blockchain για τη διατήρηση των συστημάτων πληροφορικής και οι εμπορικές τράπεζες θα θέτουν συστήματα πληρωμών στο Blockchain.

Το γεγονός ότι το Bitcoin δημιουργήθηκε το 2009 λίγο μετά την κρίση, δεν ήταν πιθανώς σύμπτωση. Η εμπιστοσύνη στα χρηματοπιστωτικά ιδρύματα είχε διαβρωθεί

και ο χρόνος ήταν πλέον ώριμος για να διερευνηθούν θεμελιωδώς διαφορετικές προσεγγίσεις. Όποιο και αν είναι το μέλλον των τεχνολογιών κρυπτογράφησης και τεχνολογίας Blockchain, οι τάσεις προς την αποκέντρωση και τις συναλλαγές P2P είναι αδιαμφισβήτητα ισχυρές.

Το Cryptocurrency έχει ξεσπάσει σε μια βιομηχανία 200 δισεκατομμυρίων δολαρίων, πυροδοτώντας ένα κύμα παγκόσμιας αναστάτωσης. Στην καρδιά της κρυπτογράφησης υπάρχει μια πλούσια ιστορία καινοτομίας. Εκτείνεται από τη δεκαετία του 1980 με τις εξελίξεις στον τομέα της κρυπτογραφίας - οδηγώντας τελικά στην τεχνολογία που σχηματίζει τεχνικές κρυπτογράφησης που έχουν σχεδιαστεί για την προστασία του δικτύου.

Από τότε, μια σειρά από βασικά γεγονότα συνέχισαν να διαμορφώνουν τον τομέα.

Έτος	Συμβάν
2009	Ο Satoshi Nakamoto εξορύσσει το πρώτο Bitcoin σε αποκεντρωμένο δίκτυο
2011	Κυκλοφορεί το Litecoin
2012	Ιδρύθηκε το Ripple
2013	Η τιμή ενός μόνο Bitcoin φτάνει τα 1.000 $
2015	Το Ethereum κυκλοφορεί το εισάγοντας έξυπνα συμβόλαια στο κρυπτοσύστημα
2017	Πάνω από 1.000 κρυπτονομίσματα παρατίθενται
2017	Οι τιμές του Bitcoin ξεπερνούν τα 10.000 $, φτάνοντας σε μια κορυφή μόλις 20.000 $
2018	Το EOS 2018 προσφέρει μια υποδομή βασισμένη σε blockchain για αποκεντρωμένες εφαρμογές (DApps)

Τώρα, κυκλοφορούν πάνω από 5.000 κρυπτονομίσματα, με πολλές ενσωματωμένες καινοτόμες εφαρμογές και περιπτώσεις χρήσης καθώς το οικοσύστημα εξελίσσεται γρήγορα.

Οι δραστηριότητες κρυπτονομισμάτων είναι ευρέως διαδεδομένες στην Ευρώπη και την Κεντρική Ασία. Η μαζική εξόρυξη κρυπτονομισμάτων πραγματοποιείται πλέον μέχρι και στην Ισλανδία και τη Γεωργία. Πολλοί Ρώσοι διαθέτουν ψηφιακά

πορτοφόλια και χρησιμοποιούν την τεχνολογία Blockchain για να καταστήσουν την αποστολή εμβασμάτων πιο αποτελεσματική (UNDP 2018). Η Εσθονία χρησιμοποιεί πια λογισμικό Blockchain στα μητρώα και σχεδιάζει να επεκτείνει τη χρήση της (https://e-estonia.com/).

Ο ανταγωνισμός για το δικαίωμα προσθήκης «μπλοκ» στο σχήμα Blockchain επιλύει επίσης το πρόβλημα της δημιουργίας νέων ηλεκτρονικών κερμάτων. Οι άνθρωποι που επιλύουν το παζλ αναλαμβάνουν έναν συνδυασμό νεοαποκτηθέντων νομισμάτων και αμοιβών συναλλαγών. Η μεγαλύτερη επιτυχία της Bitcoin έχει γίνει η πιο ανησυχητική αδυναμία της. Η έννοια της απόδειξης εργασίας που εξασφάλισε την επίτευξη μιας αποκεντρωμένης συναίνεσης έχει καταστεί υπερβολικά δαπανηρή και σπάταλη. Ελκυσμένοι από την ανταμοιβή των νεοσύστατων ψηφιακών κερμάτων, οι επενδυτές δημιούργησαν τεράστια δύναμη στον υπολογιστή με ειδικές μάρκες για να αγωνιστούν για να επιτρέψουν την προσθήκη ενός μπλοκ στο Blockchain.

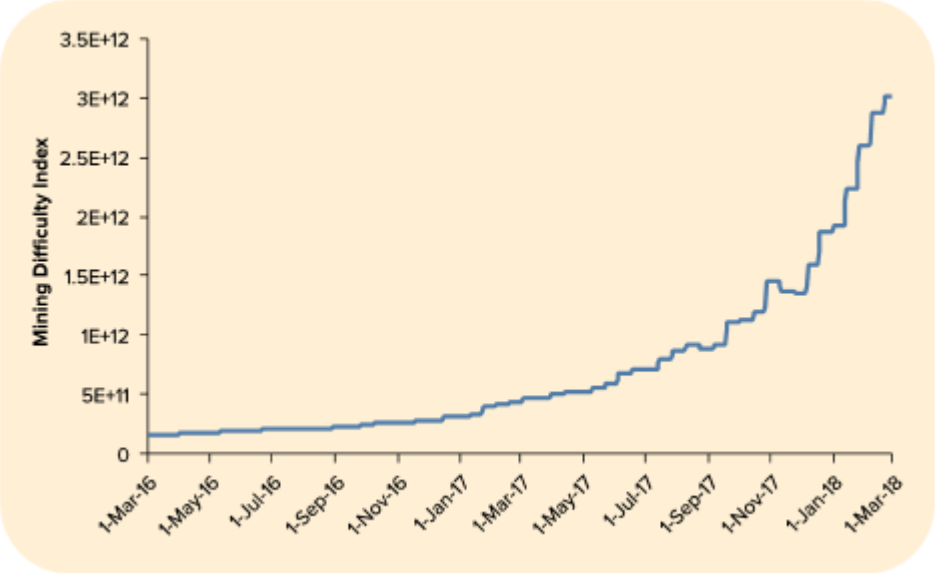
Το σύστημα καταναλώνει σήμερα περίπου 53 TWh ηλεκτρικής ενέργειας ετησίως - σχεδόν όσο καταναλώνει ολόκληρη η χώρα του Μπαγκλαντές. Το κόστος της ηλεκτρικής ενέργειας που χρησιμοποιείται για την επεξεργασία μίας μόνο μέσης συναλλαγής (περίπου $ 20) μπορεί να τροφοδοτήσει περίπου πέντε νοικοκυριά σε μια χώρα υψηλού εισοδήματος για μια ημέρα.

Αυτά τα έξοδα ηλεκτρικής ενέργειας είναι πιθανό να αυξηθούν. Επειδή τα κέρδη των «ανθρακωρύχων» είναι ακόμη μεγάλα, προστίθεται περισσότερη δύναμη στον υπολογιστή. Όμως, το κόστος από την άποψη της χρήσης ηλεκτρικής ενέργειας και η προκύπτουσα επιβάρυνση για το περιβάλλον είναι πραγματικές.

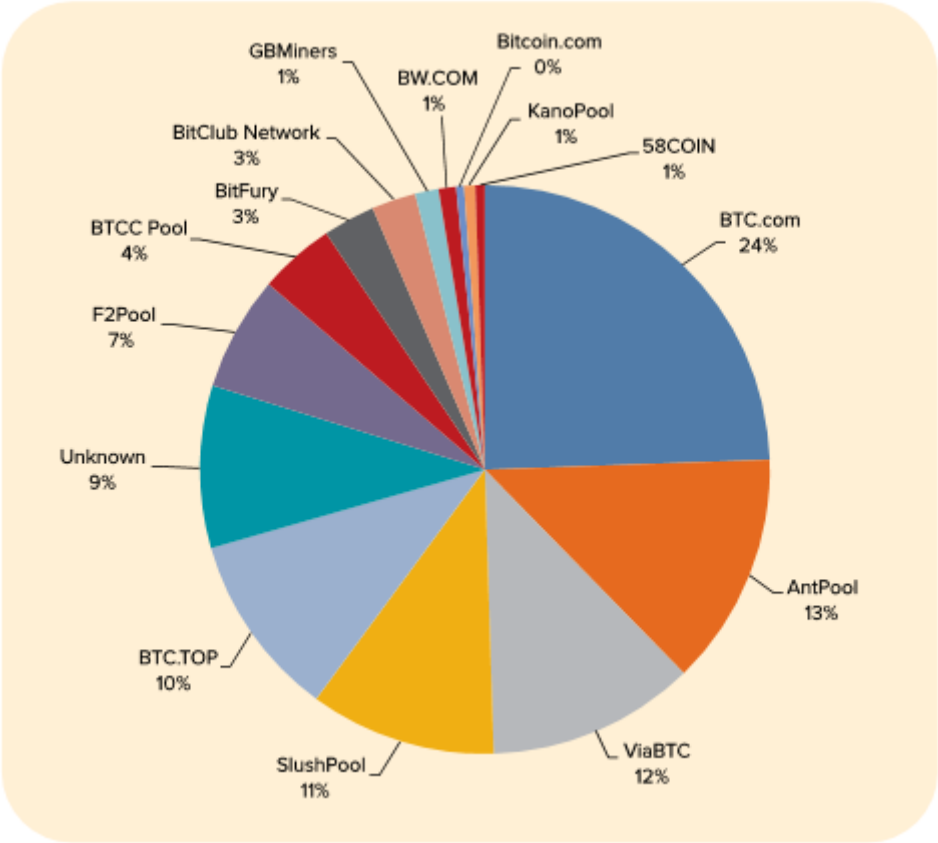
Μια παράδοξη παρενέργεια της ταχείας αύξησης της υπολογιστικής ισχύος είναι ότι η ισχύς του υπολογιστή έχει γίνει πιο συγκεντρωμένη. Μερικές εταιρείες έχουν εγκαταστήσει τεράστιας χωρητικότητας υπολογιστές σε μεγάλα εργοστάσια που χρησιμοποιούν ειδικά υπολογιστικά τσιπ. Η εκμετάλλευση των οικονομιών κλίμακας οδηγεί στη συγκέντρωση της ισχύος στην αγορά.

Αυτή η συγκέντρωση της ισχύος του υπολογιστή καθιστά το δίκτυο πιο ευάλωτο σε κακόβουλες επιθέσεις. Ακόμη και χωρίς επιθέσεις, αν η αγορά γίνει ολιγοπώλιο, οι περίφημοι «ανθρακωρύχοι» θα μπορούσαν να χειραγωγήσουν τέλη συναλλαγών, να

αρνηθούν να επεξεργαστούν ορισμένους τύπους συναλλαγών ή να αρνηθούν την εξυπηρέτηση των χρηστών στο πλαίσιο των συναλλαγών αυτών.



As the price of bitcoin soared in 2017, so did competition among miners



Three large mining pools provide half of all network blocks

Εισαγωγή στην τεχνολογία Blockchain/Cryptocurrency

Ένα Blockchain, κυριολεκτικά μιλώντας, είναι απλά μια αλυσίδα ψηφιακών μπλοκ. Κάθε μπλοκ περιέχει έναν ορισμένο όγκο δεδομένων και η αλυσίδα συνδέει αυτά τα δεδομένα για να σχηματίσει μια κατανεμημένη βάση δεδομένων. Ένα μπλοκ που δημιουργήθηκε περιλαμβάνει πολλές συναλλαγές που συλλέγονται από κόμβους και εκπομπές σε κάθε κόμβο της εργασίας. Μπορεί να γίνει αποδεκτό και να προστεθεί στο Blockchain από κόμβους που έχουν το ίδιο πρωτόκολλο συναίνεσης. Κάθε πρόσθετο μπλοκ περιλαμβάνει πληροφορίες του προηγούμενου μπλοκ στην αλυσίδα. Ως εκ τούτου, εάν το μπλοκ αλλάξει, όλα τα μπλοκ πριν από αυτό το μπλοκ θα είναι άκυρα επίσης. Οι στρατηγικές για την επίτευξη συμφωνίας για το νέο μπλοκ (συναίνεση) ποικίλλουν σε διαφορετικούς τύπους Blockchain. Η μαθηματική δομή του Blockchain συνεπάγεται δύο βασικές ιδιότητες: (i) τα δεδομένα (σε μπλοκ) είναι αμετάβλητα[1](ii) το κατανεμημένο δίκτυο με συναίνεση επιτρέπει στους χρήστες να επικοινωνούν απευθείας μεταξύ τους και να κατεβάζουν ένα αντίγραφο του τρέχοντος καθολικού Blockchain, πράγμα που σημαίνει ότι υπάρχει συνεχής παρακολούθηση και πλεονασμός των δεδομένων στο δίκτυο. Επομένως, το Blockchain είναι πιο ανθεκτικό σε μεμονωμένες κυβερνοεπιθέσεις.

Ανάλογα με το ποιός μπορεί να έχει πρόσβαση στο Blockchain και ποιός μπορεί να επικυρώσει δεδομένα, το Blockchain μπορεί να κατηγοριοποιηθεί σε δημόσιες αλυσίδες, ιδιωτικές αλυσίδες και αλυσίδες κοινοπραξίας. Τα περισσότερα κρυπτονομίσματα βασίζονται σε δημόσιες αλυσίδες. Παρόλο που ένα πλήρως διανεμημένο δημόσιο Blockchain, το οποίο επιτρέπει σε όλους να συμμετάσχουν στο δίκτυο, είναι σχεδόν αδύνατο να πλαστογραφηθεί, τα μειονεκτήματα περιλαμβάνουν υψηλή κατανάλωση ενέργειας κατά την επικύρωση συναλλαγών και χαμηλή απόδοση για την καταγραφή συναλλαγών που μπορεί να συμβούν ταυτόχρονα. Κατά τη χρήση σε επίπεδο επιχειρήσεων, αναπτύσσονται ιδιωτικές αλυσίδες και κοινοπραξίες για υψηλότερη απόδοση. Μια ιδιωτική αλυσίδα ελέγχεται και λειτουργεί από έναν οργανισμό ή έναν ιδρυτή που αναλαμβάνει ευθύνες για την επικύρωση και την επεξεργασία συναλλαγών. Οι νέοι χρήστες πρέπει να υποβάλουν αίτηση για δικαιώματα από τον οργανισμό για να συμμετάσχουν στο δίκτυο. Εκτός από τις

[1] MIT Technology Review Editor. \Explainer: What is a Blockchain?"
In: (2018). url: https://www.technologyreview.com/s/610833/ explainer-what-is-a-Blockchain/

συναλλαγές που είναι ορατές στον οργανισμό, ένας χρήστης μπορεί να καθορίσει ποιος μπορεί να έχει πρόσβαση στη συναλλαγή του και όχι σε κάθε χρήστη στο δίκτυο. Ένα παράδειγμα ιδιωτικής αλυσίδας Blockchain είναι το IBM Hyperledger Fabric[2]

Πρόκειται για μια πλατφόρμα Blockchain με σκοπό την παροχή αποκεντρωμένων λύσεων αποθήκευσης δεδομένων χρησιμοποιώντας έξυπνα συμβόλαια, που ονομάζονται Chaincode, για επιχειρήσεις που εγγράφονται στο δίκτυο μέσω ενός αξιόπιστου παρόχου υπηρεσιών μέλους. Η αλυσίδα κοινοπραξίας είναι παρόμοια με την ιδιωτική αλυσίδα, εκτός από τη διαχείρισή της από πολλούς χρήστες ή οργανισμούς. Οι συναλλαγές συνήθως επικυρώνονται και υποβάλλονται σε επεξεργασία από όλους ή ένα υποσύνολο χρηστών.

Η συναλλαγή Bitcoin ορίζεται ως μεταφορά του κρυπτονομίσματος από έναν κόμβο (διεύθυνση εισόδου) στον άλλο κόμβο (διεύθυνση εξόδου) χωρίς ένα τρίτο μέρος να συμμετέχει. Εδώ οι κόμβοι είναι συσκευές συνδεδεμένες στο δίκτυο Blockchain, οι οποίες είναι υπεύθυνες για την αποθήκευση, την επαλήθευση και τη μετάδοση μπλοκ συναλλαγών συνεχώς, προκειμένου να διατηρούν ενημερωμένα όλα τα δεδομένα.

Στο παραδοσιακό κεντρικό τραπεζικό σύστημα, η συναλλαγή γίνεται από άτομο ή μηχανή της τράπεζας. Στο σύστημα Bitcoin, η συναλλαγή θα μεταδοθεί σε όλους τους χρήστες του δικτύου για επικύρωση και τήρηση βιβλίων. Κάθε συναλλαγή έχει ένα μοναδικό κατακερματισμό που χρησιμεύει ως αναγνωριστικό συναλλαγής. Το Hash δημιουργείται από τη συνάρτηση κατακερματισμού, η οποία μετατρέπει οποιαδήποτε συμβολοσειρά ή αριθμό σε μια μοναδική έξοδο σταθερού μήκους. Μια μικρή αλλαγή στην είσοδο οδηγεί σε σημαντική διαφορά στην έξοδο. Το Bitcoin χρησιμοποιεί τον αλγόριθμο κατακερματισμού SHA-256 για τη δημιουργία κατακερματισμού συναλλαγών που ξεκινούν πάντα με πολλά μηδενικά. Κάτω από τον αλγόριθμο SHA-256, οποιοδήποτε μήκος της εισόδου μεταφέρεται σε μια σταθερή έξοδο 256-bit.

Το επίπεδο δικτύου σε συστήματα Blockchain περιέχει τους κόμβους στο δίκτυο, τις γεωγραφικές και σχετικές θέσεις τους και τη συνδεσιμότητα μεταξύ τους. Καθορίζει

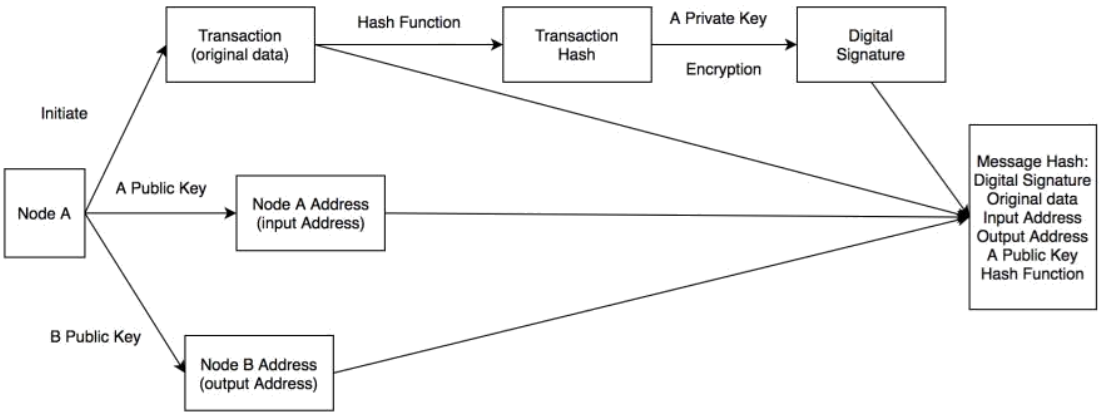
[2] Thang N Dinh and My T Thai. \AI and Blockchain: A Disruptive Integration". eng. In: Computer 51.9 (2018), pp. 48{53. issn: 0018-9162.

ποιες πληροφορίες πρέπει να διαδίδονται καθώς και τον μηχανισμό διάδοσης αυτών των πληροφοριών.

Consensus Layer

Το επίπεδο συναίνεσης στα συστήματα Blockchain καθορίζει τους αλγόριθμους και τους κανόνες για την επίτευξη συμφωνίας σχετικά με την κατάσταση του Blockchain μεταξύ των κόμβων του δικτύου. Αυτοί οι κανόνες καθορίζουν ποιος κόμβος είναι κατάλληλος για δημιουργία και προσθήκη του επόμενου μπλοκ στο μπλοκ Blockchain, πόσο συχνά δημιουργούνται μπλοκ καθώς και πώς να επιλύονται πιθανές διενέξεις που μπορεί να προκύψουν όταν οι κόμβοι έχουν πολλαπλά, διαφορετικά αντίγραφα του καθολικού.

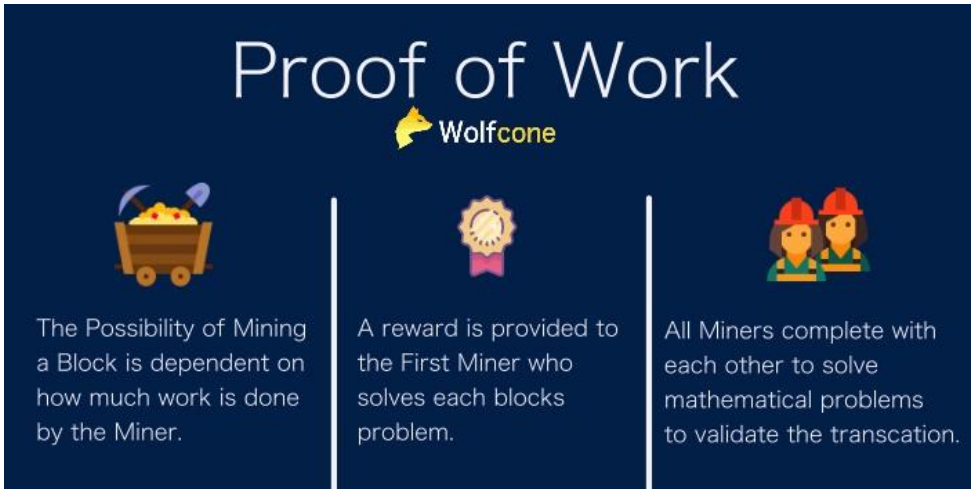
Το κύριο συστατικό στο επίπεδο δικτύου είναι ένας κόμβος. Ένας κόμβος μπορεί να είναι ένας απλός χρήστης που θέλει να δημιουργήσει και να υποβάλει μια συναλλαγή που θα εκτελεστεί και συμπεριληφθεί στο καθολικό ή έναν ειδικό κόμβο, γνωστό ως «ανθρακωρύχος», ο οποίος διατηρεί και επεκτείνει το καθολικό μπλοκ προσθέτοντας νέα μπλοκ.



Ένας κόμβος έχει ένα μοναδικό αναγνωριστικό και διατηρεί την ισορροπία του ως ένα τοπικό αντίγραφο του Blockchain και, εάν ο κόμβος είναι «ανθρακωρύχος», ένα μεμονωμένο σύνολο συναλλαγών. Το σύνολο συναλλαγών διατηρεί τις εκκρεμείς συναλλαγές που λαμβάνονται από άλλους κόμβους στο δίκτυο.

Οι κόμβοι επικοινωνούν μεταξύ τους τις ακόλουθες πληροφορίες. Εάν ένας κόμβος δημιουργεί μια νέα συναλλαγή, τον υπογράφει κρυπτογραφικά και τον διαδίδει στους ομολόγους του για να τον επιβεβαιώσει και να εγγράψει στο καθολικό Blockchain. Σε περίπτωση που ο κόμβος είναι «ανθρακωρύχος», κάθε φορά που δημιουργεί ένα μπλοκ, ειδοποιεί τους ομολόγους του ώστε να μπορούν να το επικυρώσουν και να τον προσαρτήσουν στα αντίγραφα του καθολικού τους. Ως μηχανισμός διάδοσης πληροφοριών για Blockchains έχουν προταθεί διάφορα πρωτόκολλα, συμπεριλαμβανομένων δικτύων αναμετάδοσης και πρωτοκόλλων που βασίζονται σε διαφημίσεις.

Η συναλλαγή μεταξύ δύο κόμβων ολοκληρώνεται σε δύο στάδια, το στάδιο κόμβου και το στάδιο μπλοκ. Το σχήμα παραπάνω δείχνει πώς λειτουργεί το Blockchain στο επίπεδο του κόμβου. Τόσο το Α όσο και το Β λαμβάνουν ένα μοναδικό ζεύγος κλειδιών (συμβολοσειρές χαρακτήρων), το ιδιωτικό κλειδί που χρησιμοποιείται για κρυπτογράφηση και το δημόσιο κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση και τη δημιουργία διευθύνσεων. Ας υποθέσουμε ότι μια συναλλαγή ΤΑΒ ξεκινά από τον κόμβο Α που θέλει να στείλει ψηφιακά νομίσματα στον κόμβο Β. Τα πρωτότυπα δεδομένα συναλλαγών μεταφέρονται πρώτα σε κατακερματισμό συναλλαγής μέσω μιας λειτουργίας κατακερματισμού. Στη συνέχεια, δημιουργείται μια ψηφιακή υπογραφή κρυπτογραφώντας το κατακερματισμό της συναλλαγής. Στη συνέχεια, η ψηφιακή υπογραφή μαζί με τη διεύθυνση συναλλαγής εισόδου (διεύθυνση κόμβου Α) που δημιουργήθηκε από το δημόσιο κλειδί του κόμβου Α, τη διεύθυνση συναλλαγής εξόδου (διεύθυνση κόμβου Β) που δημιουργήθηκε από το δημόσιο κλειδί του κόμβου Β και τα αρχικά δεδομένα συναλλαγών με αντίστοιχη συνάρτηση κατακερματισμού, κατακερματίζεται και αποστέλλεται στον κόμβο Β.



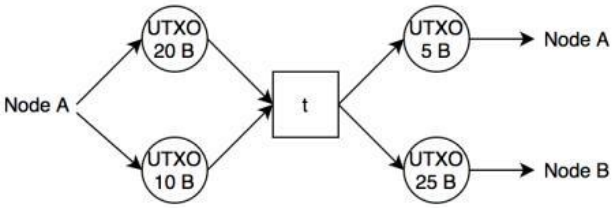
Μετά τη λήψη της συναλλαγής TAB από τον κόμβο Α, ο κόμβος Β την επαληθεύει συγκρίνοντας δύο τιμές κατακερματισμού που δημιουργούνται από την ψηφιακή υπογραφή και τα αρχικά δεδομένα συναλλαγής.

Μετά την επαλήθευση της συναλλαγής, μεταφορτώνεται σε μια ομάδα συναλλαγών για προσθήκη στα μπλοκ.

Στο δεύτερο στάδιο, οι ενεργοί συμμετέχοντες του δικτύου θα συγκεντρώσουν συναλλαγές για να σχηματίσουν μπλοκ και θα ανταγωνίζονται για να προσθέσουν το δικό τους μπλοκ στο δίκτυο Blockchain. Η διαδικασία είναι επίσης γνωστή ως «εξόρυξη». Ο μηχανισμός για να προσδιοριστεί εάν ένα μπλοκ μπορεί να προστεθεί στην αλυσίδα ονομάζεται «συναίνεση».

Το Bitcoin Blockchain εφαρμόζει το proof-of-work (PoW) ως πρωτόκολλο συναίνεσης. Διαισθητικά, οι κόμβοι εξόρυξης ανταγωνίζονται ο ένας τον άλλον για την επίλυση ενός σκληρού μαθηματικού προβλήματος, δηλαδή, για να εντοπίσουν μια συγκεκριμένη τιμή κατακερματισμού που είναι χαμηλότερη από το κατακερματισμό στόχου. Ο κόμβος μεταδίδει το μπλοκ του σε ολόκληρο το δίκτυο όταν εντοπίσει τον απαιτούμενο κατακερματισμό. Μόλις οι πληροφορίες σχετικά με το νέο μπλοκ επικυρωθούν από την πλειοψηφία των κόμβων, το νέο μπλοκ προσαρτάται στο Blockchain και στον κόμβο που δημιουργεί πρώτα το μπλοκ απονέμεται ένας ορισμένος αριθμός Bitcoin.

Το Bitcoin ανήκει στον τύπο Blockchain που βασίζεται σε έξοδο συναλλαγών (UTXOs). Κάθε κόμβος μπορεί να εισάγει μόνο ολόκληρες (όχι κλασματικές) εξόδους που δεν έχουν δαπανηθεί (UTXOs) σε μια συναλλαγή. Τα αθροιστικά UTXO χρησιμεύουν ως το υπόλοιπο κάθε κόμβου. Για παράδειγμα, ας υποθέσουμε ότι ένας Κόμβος Α έχει δύο UTXO που καταγράφουν 10 Bitcoins και 20 Bitcoins αντίστοιχα και σκοπεύει να στείλει 25 Bitcoins στον Κόμβο Β. Ο κόμβος Α πρέπει να δαπανήσει και τα δύο UTXO ως συναλλαγή εισόδου. Στο τέλος της συναλλαγής, δύο UTXO εισόδου δαπανώνται και αφαιρούνται από το σύνολο UTXO του κόμβου Α. Ένα νέο UTXO που καταγράφει 5 Bitcoins επιστρέφεται στον κόμβο Α ενώ ένα άλλο νέο UTXO που καταγράφει 25 Bitcoins αποστέλλεται στον κόμβο Β. Η διαδικασία φαίνεται στο σχήμα παρακάτω. Η διεύθυνση που χρησιμοποιεί ο κόμβος Α για να λάβει την αλλαγή της ονομάζεται διεύθυνση αλλαγής Bitcoin.



Ένας άλλος τύπος δημόσιου Blockchain είναι το Blockchain που βασίζεται σε λογαριασμό, π.χ. Ethereum. Σε σύγκριση με τις συναλλαγές bitcoin, οι συναλλαγές Ethereum περιλαμβάνουν όχι μόνο ψηφιακά νομίσματα (Ether), αλλά και έξυπνα συμβόλαια. Ένα έξυπνο συμβόλαιο είναι ένα κομμάτι κώδικα που εκτελείται αυτόματα και επιτρέπει την εκτέλεση μιας συναλλαγής αυτόματα. Πιο συγκεκριμένα, το έξυπνο συμβόλαιο φορτώνεται σε μια διεύθυνση κόμβου. Άλλοι κόμβοι μπορούν να καλέσουν μια συνάρτηση αυτού του έξυπνου συμβολαίου για τη δημιουργία μιας συναλλαγής. Το Ethereum χρησιμοποιεί επί του παρόντος το PoW ως το πρωτόκολλο συναίνεσης, αλλά σχεδιάζει να υιοθετήσει στο μέλλον την απόδειξη της συμμετοχής (PoS). Οι ανθρακωρύχοι αντικαθίστανται από επικυρωτές και ψηφίζουν ποιό μπλοκ θα προστεθεί δίπλα στην αλυσίδα. Όσο περισσότερα στοιχήματα (συνήθως μέσω κρυπτογράφησης) έχουν έναν κόμβο, τόσο περισσότερη δύναμη ψήφου θα έχουν. Επομένως, στο PoW, η πιθανότητα δημιουργίας ενός νέου μπλοκ εξαρτάται από το πόση υπολογιστική ισχύ που χρησιμοποιεί κάθε κόμβος. Στο PoS (Proof of Stake), η πιθανότητα δημιουργίας ενός νέου μπλοκ εξαρτάται από το πόσα νομίσματα έχει κάθε κόμβος. Ο κόμβος που αποκτά μεγαλύτερο αριθμό κερμάτων έχει μεγαλύτερη πιθανότητα να δημιουργήσει ένα νέο μπλοκ.

Proof of work VS Proof stake

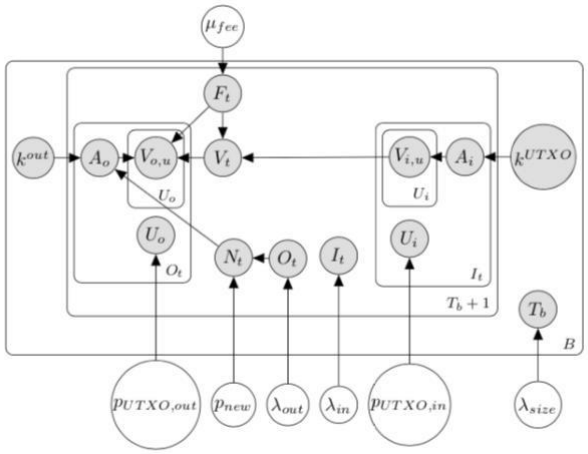
Στο δίκτυο Bitcoin, είναι σημαντικό να αναγνωρίζουμε οντότητες πίσω από αυτές τις δυνητικά παράνομες οντότητες. Η μελέτη του εντοπισμού οντοτήτων πίσω από διευθύνσεις ονομάζεται ομαδοποίηση διευθύνσεων Οι Yin et al. (2017) εφαρμόζουν την περίφημη «εποπτευόμενη μάθηση» για την ταξινόμηση οντοτήτων συναλλαγών που ενδέχεται να εμπλέκονται σε εγκληματικές δραστηριότητες στον κυβερνοχώρο. Το μοντέλο ταξινόμησης εκπαιδεύεται με βάση 854 παρατηρήσεις με κατηγορηματικά αναγνωριστικά και στη συνέχεια εφαρμόζεται για τη μελέτη 10000 μη κατηγοριοποιημένων παρατηρήσεων που λαμβάνουν το 31,62% των μοναδικών διευθύνσεων και το 28,99% των συνολικών νομισμάτων στο συνολικό Bitcoin Blockchain. Τα αναγνωριστικά κατηγορίας αντιπροσωπεύουν 12 κατηγορίες οντοτήτων, πέντε από τις οποίες σχετίζονται με εγκληματικές δραστηριότητες στον κυβερνοχώρο. Εφαρμόζονται δεκατρείς ταξινομητές από το πακέτο μηχανικής εκμάθησης Python \ scikit-learn.

Συγκρίνοντας τις βαθμολογίες ακρίβειας όλων των ταξινομητών, διαπιστώνεται ότι τα τυχαία πακέτα (77,38%), τα εξαιρετικά τυχαία πακέτα (76,47%), το Bagging (78,46%) και το Gradient Boosting (80,76%) ξεχωρίζουν ως οι τέσσερις καλύτεροι ταξινομητές. Μετά από περαιτέρω σύγκριση της ακρίβειας, της ανάκλησης και της βαθμολογίας αυτών των ταξινομητών, το bagging και το gradient boosting ξεχωρίζουν, τα οποία στη συνέχεια εφαρμόζονται για την ανάλυση των παρατηρήσεων. Το αποτέλεσμα της ταξινόμησης δείχνει ότι 5,79% (3,16%) διευθύνσεις και 10,02% (1,45%) από τα ελεγχθέντα νομίσματα προέρχονται από κυβερνοεγκληματικές οντότητες σύμφωνα με τη μέθοδο bagging (μέθοδος ενίσχυσης κλίσης).

Τα Bitcoin είναι ένας κοινός τρόπος για την πληρωμή του ransomware. Προκειμένου να εντοπιστούν διευθύνσεις που σχετίζονται με την πληρωμή ransomware, οι Akcora et al. (2019) εφαρμόζουν μια προσέγγιση τοπολογικής ανάλυσης δεδομένων (TDA) για να δημιουργήσουν το γράφημα διευθύνσεων Bitcoin ομαδοποιώντας πρώτα παρόμοιες διευθύνσεις σε κόμβους και έπειτα τοποθετώντας κοινές διευθύνσεις μεταξύ δύο κόμβων στο σύνολο των άκρων. Το TDA είναι μια προσέγγιση που χρησιμοποιείται συνήθως για τη μείωση των διαστάσεων. Αντιπροσωπεύει το σύνολο δεδομένων σε ένα γράφημα διαιρώντας πρώτα τα δεδομένα σε υποδείγματα με βάση διαφορετικά κριτήρια φιλτραρίσματος και στη συνέχεια συγκεντρώνοντας παρόμοια σημεία σε κάθε υπόδειγμα.

Τα UTXO καταγράφουν τον αριθμό των Bitcoin σε συναλλαγές, γεγονός που μας επιτρέπει να παρακολουθούμε πληροφορίες αγοράς και πώλησης για να προβλέψουμε την τιμή του Bitcoin. Μια άλλη συνεισφορά των Jourdan et al. (2018) μας βοηθά να προβλέψουμε την αξία των UTXO δημιουργώντας πιθανολογικά γραφικά μοντέλα. Το πρώτο μοντέλο ονομάζεται μοντέλο διεύθυνσης αποκλεισμού συναλλαγών (BT-A) που είναι ένα σταθερό γραφικό μοντέλο ενός μπλοκ Bitcoin με δομές εξάρτησης υπό όρους. Ως επέκταση του BT-A, ένα μοντέλο αποκλειστικής συναλλαγής οντότητας-διεύθυνσης (BT-EA) αναπτύσσεται περαιτέρω προσθέτοντας μια κατηγορηματική οντότητα σε κάθε διεύθυνση. Όσον αφορά στα MSE, RMSE, MAE, τα αποτελέσματα προσομοίωσης στο σχήμα παρακάτω δείχνουν ότι αυτή η επέκταση ξεπερνά σημαντικά το μοντέλο BT-A σε όλες τις κατηγορίες εκτός από το Exchange.

Metric	BT-EA				BT-A
	E	S	G	M	All
MSE	1.22	-0.30	-0.02	0.06	1.12
RMSE	125	53.3	1.15	5.19	90.5
MAE	15.6	0.94	0.20	2.42	7.47
RMAE	1.82	1.74	1.86	1.93	1.69
NRMSE	1.34	1.28	1.42	1.22	1.29



Block-transaction Address Model[3]

Οι Zhu et al. (2019) ανέπτυξαν ένα πλαίσιο προστασίας της ιδιωτικής ζωής που βασίζεται σε Blockchain. Ο αλγόριθμος Federated Learning αναπτύσσεται με τρόπο ο οποίος επιτρέπει σε κάθε κινητή συσκευή να υπολογίζει και να ανεβάζει ενημερώσεις στο παγκόσμιο μοντέλο πρόβλεψης βάσει των τοπικών συνόλων δεδομένων τους. Ένα ζήτημα ασφαλείας προκύπτει όταν υπάρχουν «βυζαντινές αποσβέσεις» στο δίκτυο. Σε αυτήν την περίπτωση, ο μηχανισμός συναλλαγών Blockchain υιοθετείται για να διασφαλίσει την ασφάλεια της κοινής χρήσης και της ενημέρωσης των αλλαγών. Συγκεκριμένα, οι ενημερώσεις μοντέλων γράφονται σε μια συναλλαγή Blockchain από κόμβους. Μαζί με την ψηφιακή υπογραφή ενός κόμβου, μια συναλλαγή μεταδίδει σε άλλους κόμβους σε σχηματισμό, συμπεριλαμβανομένων αλλαγών υπερπαραμέτρων, τα δημόσια κλειδιά (διευθύνσεις των συμμετεχόντων). Άλλοι κόμβοι επικυρώνουν τη συναλλαγή και ελέγχουν τις ενημερώσεις σύμφωνα με τα τοπικά σύνολα δεδομένων τους. Εάν οι περισσότεροι κόμβοι επιβεβαιώνουν ότι η βαθμολογία απόδοσης του

[3] Marc Jourdan et al. \A Probabilistic Model of the Bitcoin Blockchain". In: CoRR abs/1812.05451 (2018).

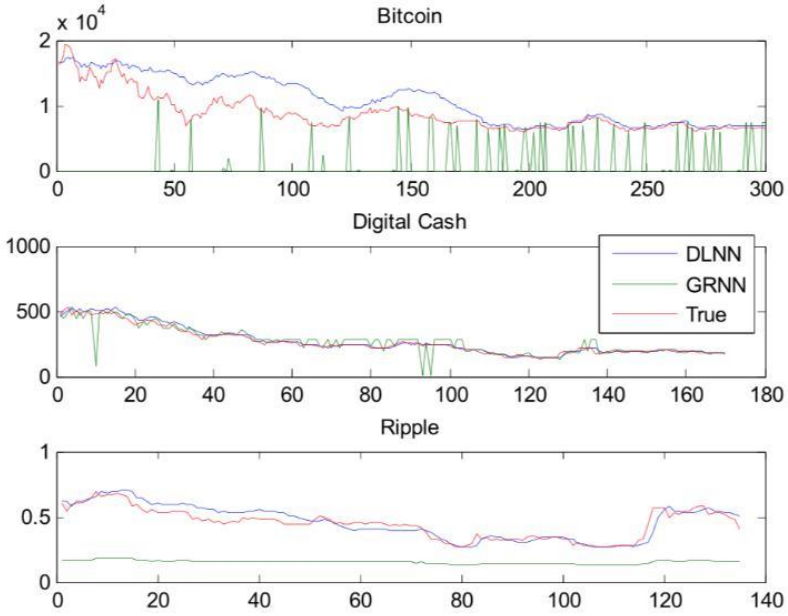
ενημερωμένου μοντέλου είναι υψηλότερη από το υπάρχον μοντέλο στα τοπικά σύνολα δεδομένων τους, οι ενημερώσεις εφαρμόζονται στο τρέχον μοντέλο.

Για την πρόβλεψη της τιμής του Bitcoin, οι McNally et al. (2018) συνέκριναν τις επιδόσεις δύο αλγορίθμων βαθιάς μάθησης, δηλαδή του Recurrent Neural Network (RNN) και της Long-Short Term Memory (LSTM). Είναι ενδιαφέρον να σημειωθεί ότι δύο κρυφά στρώματα με 20 κόμβους ανά επίπεδο είναι επαρκή και στα δύο μοντέλα. Συγκεκριμένα, το μοντέλο RNN υιοθετεί τη λειτουργία ως λειτουργία ενεργοποίησης ενώ το LSTM εφαρμόζει λειτουργίες για διαφορετικές πύλες, οι οποίες έχουν ως αποτέλεσμα μεγαλύτερο χρόνο προπόνησης. Το σύνολο δεδομένων που χρησιμοποιείται για την εκπαίδευση και τη δοκιμή μοντέλων LSTM και RNN είναι η τιμή bitcoin από 19 Αυγούστου 2013 έως 19 Ιουλίου 2016. Χαρακτηριστικά που περιλαμβάνουν την τιμή ανοίγματος, το ημερήσιο υψηλό, το ημερήσιο χαμηλό, την τιμή κλεισίματος, το ποσοστό κατακερματισμού και τη δυσκολία εξόρυξης χρησιμοποιείται στο μοντέλο. Η σημασία των χαρακτηριστικών αξιολογείται από τον αλγόριθμο Boruta, ο οποίος είναι ένα πλαίσιο το οποίο βασίζεται στον τυχαίο αλγόριθμο ταξινόμησης πακέτων. Το παραδοσιακό μοντέλο χρονοσειρών, το Auto Regression Integrated Moving Average (ARIMA), συγκρίνεται εμπειρικά με αυτά τα μοντέλα μάθησης (deep learning) . Τα αποτελέσματα της προσομοίωσης δείχνουν ότι τα LSTM, RNN και ARIMA έχουν παρόμοια ακρίβεια, τα οποία είναι 52,78%, 50,25% και 50,05%.

Ωστόσο, τα μοντέλα αυτά έχουν πολύ χαμηλότερες τιμές RMSE. Επιπλέον, το μοντέλο LSTM είναι ικανό να αναγνωρίζει μακροπρόθεσμες εξαρτήσεις σε αντίθεση με το μοντέλο RNN.

Σε αντίθεση με άλλες μελέτες κυρίως για μοντέλα πρόβλεψης, οι Lahmiri et al. (2019) αντ 'αυτού, διεξάγουν μια χαοτική ανάλυση χρονοσειρών πριν δημιουργήσουν μοντέλα μάθησης. Ως εκ τούτου, το πρώτο τους βήμα είναι να υπολογίσουν τον μεγαλύτερο εκθετή Lyapunov (LLE) και, στη συνέχεια, να εφαρμόσουν αναλυτική ανάλυση διακύμανσης (DFA) για να ανιχνεύσουν τα χαρακτηριστικά χάους των δεδομένων τιμών κρυπτογράφησης χωρίς να έχουν την παραδοχή της σταθερότητας.

	LLE		HE	
	Training sub-sample	Testing sub-sample	Training sub-sample	Testing sub-sample
Bitcoin	0.1250	−7.8711	1.0087	0.9776
Digital Cash	0.3205	−10.7333	0.9559	1.0901
Ripple	0.8181	−0.0065	1.0741	0.8715



Chaotic Analysis and Prediction Result

Η έρευνα που εξετάζουμε είτε εφαρμόζει το Blockchain σε μια βάση δεδομένων για τη βελτίωση του απορρήτου των χρηστών στη διαδικασία εκμάθησης είτε χρησιμοποιεί μηχανική εκμάθηση για τη βελτιστοποίηση της κατανομής πόρων υπολογιστών ή των επενδυτικών αποφάσεων κρυπτογράφησης. Η πλειοψηφία μπορεί να κατηγοριοποιηθεί ως εφαρμογή μιας τεχνικής στην άλλη. Λίγη είναι η πραγματική ολοκλήρωση των δύο τεχνολογιών. Ως εκ τούτου, είναι δίκαιο να πούμε ότι η τρέχουσα έρευνα είναι ακόμη πολύ προκαταρκτική από διεπιστημονική άποψη.

Ωστόσο, αναμένουμε να εμφανιστούν νέες ερευνητικές γραμμές στους ακόλουθους τομείς:

Σχεδιασμός smart agents με μαθησιακές ικανότητες για τη ρύθμιση του Blockchain και τον εντοπισμό μη φυσιολογικών συμπεριφορών. Ο σχεδιασμός αυτός είναι ιδιαίτερα σημαντικός για την αλυσίδα κοινοπραξιών και την ιδιωτική αλυσίδα που απαιτεί συντονισμό μεταξύ των χρηστών. Η ανάλυση που βασίζεται στη μάθηση του συστήματος που βασίζεται σε Blockchain είναι σπάνια. Από τα χρηματοοικονομικά συστήματα έως τις αλυσίδες εφοδιασμού, υπάρχει ένας τεράστιος αριθμός διαθέσιμων δεδομένων για την αξιολόγηση της απόδοσης της αποκεντρωμένης δομής του

Blockchain σε σύγκριση με την παραδοσιακή κεντρική. Η ανάλυση που βασίζεται στη μάθηση μπορεί να φωτίσει το ερευνητικό πεδίο σχετικά με το σχεδιασμό του μηχανισμού των δομών Blockchain και να παρέχει μοντέλα έγκαιρης πρόβλεψης.

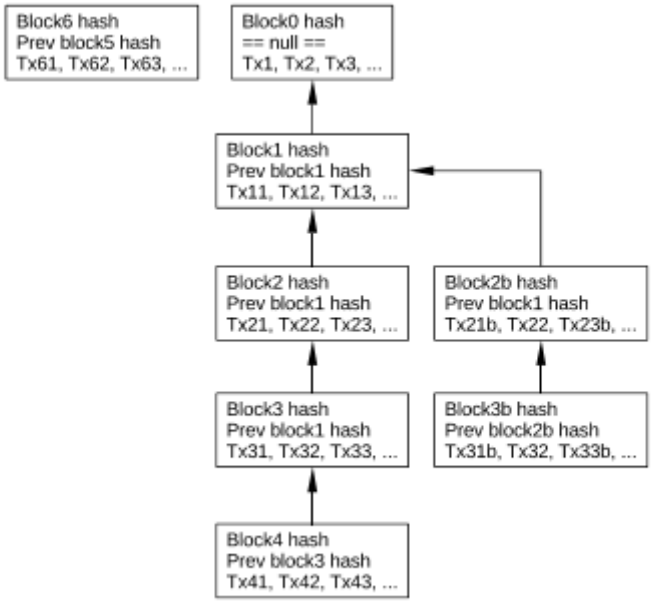
Ζητήματα Οφέλους και Κόστους

Με την ανάπτυξη του Internet Of Things και της φορητής συσκευής, το ζήτημα του απορρήτου προσελκύει όλο και περισσότερο την προσοχή των χρηστών. Σε συνδυασμό με τη συγχώνευση δεδομένων, μπορούμε να σχεδιάσουμε δομές Blockchain πολλαπλών επιπέδων που επιτρέπουν εξελιγμένη εξουσιοδότηση δεδομένων για διαφορετικούς χρήστες.

Η δραστηριότητα εξόρυξης Blockchain θα μπορούσε να θεωρηθεί ως διαδικασία MDP. Παρόλο που υπάρχουν μερικά έργα που σχετίζονται με την εξεύρεση της βέλτιστης στρατηγικής εξόρυξης με χρήση εκμάθησης ενίσχυσης ενός πράκτορα, η ατομική εξόρυξη δεν είναι τόσο δημοφιλής όσο η εξόρυξη «δεξαμενών» στην πραγματικότητα. Συγκεκριμένα, οι «ανθρακωρύχοι» συνεργάζονται και ανταγωνίζονται μεταξύ τους για να εξορύξουν μπλοκ. Μια μάθηση ενίσχυσης πολλαπλών παραγόντων (MARL) με μικτή ρύθμιση συνεργατικών και ανταγωνιστικών πρακτόρων είναι πιο κατάλληλη για τη μοντελοποίηση της σύνθετης δραστηριότητας εξόρυξης δεξαμενών και βοηθά τους ανθρακωρύχους να βρουν τις βέλτιστες στρατηγικές εξόρυξης στο μέλλον.

Το κρυπτονόμισμα (Cryptocurrency) παίζει σημαντικό ρόλο, ειδικά στη δημόσια αλυσίδα. Διαφορετικές αλυσίδες έχουν τη μοναδική κρυπτογράφηση τους. Τώρα το χαρτοφυλάκιο cryptocurrency είναι μια επενδυτική επιλογή παρόμοια με άλλα χρηματοοικονομικά προϊόντα. Ορισμένα έργα έχουν μελετήσει την πρόβλεψη τιμών κρυπτογράφησης χρησιμοποιώντας εποπτευόμενες τεχνικές μάθησης, αλλά μόνο μερικά από αυτά διερευνούν τις δυνατότητες του RL ή του βαθύ RL. Σε πολλές περιπτώσεις, η RL παρουσιάζει καλύτερα αποτελέσματα στις χρηματοοικονομικές προβλέψεις, π.χ. την πρόβλεψη των τιμών των μετοχών, καθώς τα ιστορικά δεδομένα δεν μπορούν να αντικατοπτρίζουν την τρέχουσα αγορά, η οποία οδηγεί περαιτέρω σε χαμηλή απόδοση προβλέψεων για μελλοντικές αλλαγές τιμών. Αναμένεται στην ερευνητική κοινότητα ότι θα εμφανιστούν σύντομα περισσότερα έργα που υιοθετούν RL, βαθιά RL ή αντίστροφα RL για να μελετήσουν την απόδοση επένδυσης των κρυπτονομισμάτων.

Σε ένα κατανεμημένο Blockchain, νέα μπλοκ και συναλλαγές κατανέμονται μεταξύ ομοτίμων. Κάθε ομότιμος διατηρεί ένα σύνολο συναλλαγών που θα συμπεριληφθούν σε μελλοντικά μπλοκ. Οι νέες συναλλαγές που θα προστεθούν σε αυτήν την ομάδα επικυρώνονται, δηλαδή διασφαλίζεται ότι επιτρέπονται λογικά. Στην αλυσίδα Bitcoin αυτό συνεπάγεται τη διασφάλιση ότι οι εισροές συναλλαγών αναφέρουν μη εκχωρημένες συναλλαγές. Στο πλαίσιο της ροής εργασίας αυτό μπορεί να σημαίνει ότι η εκτέλεση μιας δραστηριότητας ροής εργασίας επιτρέπεται στην τρέχουσα κατάσταση μιας διαδικασίας.



Η ασύμμετρη κρυπτογραφία χρησιμοποιείται εντατικά σε Blockchains συστήματα. Σε αντίθεση με τη συμμετρική κρυπτογραφία όπου χρησιμοποιείται ένα κοινόχρηστο κλειδί, η ασύμμετρη κρυπτογραφία χρησιμοποιεί ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού. Συνήθως, το δημόσιο κλειδί αντιστοιχεί στη δημόσια διεύθυνση του χρήστη στο Blockchain. Αυτό επιτρέπει στον χρήστη να υπογράψει μια συναλλαγή με το ιδιωτικό του κλειδί έτσι ώστε όλοι να μπορούν να επαληθεύσουν την αυθεντικότητά της στο Blockchain (όπως αντιστοιχεί στη διεύθυνσή του). Το ιδιωτικό κλειδί χρησιμοποιείται επομένως για την εξουσιοδότηση ενεργειών στον λογαριασμό χρήστη, καθώς πρόκειται για μια απλή μέθοδο ελέγχου ταυτότητας.

Τα Blockchain μπορούν να ταξινομηθούν σε Blockchains με άδειες και Blockchains χωρίς άδεια. Σε ένα Blockchain χωρίς άδεια, οποιαδήποτε οντότητα μπορεί να γίνει κόμβος και να συμμετάσχει στη γενική συναίνεση Blockchain (π.χ. προσθήκη

συναλλαγών). Αντιθέτως, το Blockchain που επιτρέπεται (είναι αδειοδοτημένο) αυξάνει τον έλεγχο περιορίζοντας τη συμμετοχή μόνο σε συγκεκριμένες αποδεκτές οντότητες [4] Συνήθως, ένα εγκεκριμένο Blockchain περιορίζει τους κόμβους που συμμετέχουν στο πρωτόκολλο συναίνεσης σε ειδικά σύνολα κόμβων. Ανάλογα με την εφαρμογή, μπορεί να χρησιμοποιηθεί ο ένας τύπος ή ο άλλος. Για παράδειγμα, κρυπτονομίσματα όπως το Bitcoin δεν επιτρέπονται, ενώ οι επιχειρηματικές λύσεις που χρησιμοποιούνται σε οργανισμούς συνήθως επιτρέπονται.

Οι λύσεις διαχείρισης ταυτότητας που βασίζονται στο Blockchain επωφελούνται των εγγενών πλεονεκτημάτων της τεχνολογίας Blockchain. Εξαλείφουν την ανάγκη για την ύπαρξη μιας κεντρικής αρχής η οποία θα ελέγχει και θα διαχειρίζεται το σύστημα και εν τέλει θα μεταβιβάζει την ευθύνη στον χρήστη. Αυτά τα πλεονεκτήματα αναμένεται να λύσουν (σε κάποιο βαθμό) ορισμένα από τα προβλήματα που εμφανίζονται σε κεντρικά συστήματα, όπως απάτη ταυτότητας ή διαρροές δεδομένων. Ωστόσο, αυτό είναι συζητήσιμο επειδή οι λύσεις διαχείρισης ταυτότητας είτε δεν επιτυγχάνουν πλήρη αποκέντρωση, είτε απαιτούν υψηλό επίπεδο εμπιστοσύνης. Από την κατασκευή του αυτή καθαυτή, το Blockchain επιφέρει διαφάνεια στις αλλαγές δεδομένων και το ιστορικό δεδομένων δεν μπορεί να ελεγχθεί διαφορετικά (εκτός εάν η πλειοψηφία των κόμβων συμφωνήσει σχετικά με την αλλαγή). Από την άλλη, το Blockchain εισάγει προκλήσεις όσον αφορά στην αποτελεσματικότητα της εφαρμογής και στην ασφάλεια.

Μια λύση διαχείρισης ταυτότητας με βάση το Blockchain θα πρέπει να επιτρέπει επιλεκτική αποθήκευση ταυτοτήτων στο Blockchain. Οι ταυτότητες πρέπει να πιστοποιούνται από αρχές ή άλλες οντότητες στο Blockchain. Αυτό συνήθως λειτουργεί ως εξής: μια οντότητα διεκδικεί ταυτότητα με επαληθεύσιμη αξίωση, η οποία επιβεβαιώνεται μετά την επαλήθευση ορισμένων χαρακτηριστικών που διαφοροποιούν τον χρήστη (π.χ. αριθμός τηλεφώνου, ηλεκτρονικό ταχυδρομείο, κυβερνητικά έγγραφα ταυτότητας (αναγνωριστικά), βιομετρικά στοιχεία).

Μέσα στη διαχείριση ταυτότητας στο Blockchain λειτουργεί μια σαφής διαφορά μεταξύ του ψηφιακού αναγνωριστικού (μια τιμή που προσδιορίζει μοναδικά την

[4] *NISTIR 8202 Blockchain Technology Overview*, October 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

οντότητα) και των χαρακτηριστικών που σχετίζονται με αυτήν[5]. Καθώς η μη εξουσιοδοτημένη ή ανεξέλεγκτη αποκάλυψη χαρακτηριστικών οδηγεί σε διαρροές ασφάλειας και απορρήτου, έτσι η αποθήκευση χαρακτηριστικών (εάν ισχύει) πρέπει να αντιμετωπίζεται ανάλογα με τις καθορισμένες αρχές.

Στη βιβλιογραφία, παρατηρήθηκαν προσπάθειες χρησιμοποίησης μοντέλων προσομοίωσης για την αξιολόγηση διαφόρων πτυχών των συστημάτων Blockchain[6] Οι μελετητές χρησιμοποιούν αρχιτεκτονική μοντελοποίηση και προσομοίωση για τη μέτρηση του λανθάνοντος χρόνου σε συστήματα Blockchain υπό διαφορετικές διαμορφώσεις. Οι συγγραφείς προτείνουν ένα μοντέλο προσομοίωσης για να διερευνήσουν τον αντίκτυπο της αβεβαιότητας των κερδών στο Ethereum Blockchain. Διαπίστωσαν τελικά ότι οι ανθρακωρύχοι στο Ethereum δεν είναι σε θέση να λάβουν τεκμηριωμένες αποφάσεις σχετικά με τις συναλλαγές που πρέπει να συμπεριληφθούν στα μπλοκ τους για να μεγιστοποιήσουν τα έσοδά τους[7]. Σε άλλες έρευνες[8] οι συγγραφείς χρησιμοποιούν προσομοίωση διακριτών συμβάντων για να μελετήσουν τη συμπεριφορά των «ανθρακωρύχων» Bitcoin (συμπεριλαμβανομένων των στρατηγικών εξόρυξης) όταν υπάρχει καθυστέρηση στη διάδοση πληροφοριών μεταξύ των «ανθρακωρύχων». Εκτός από αυτές τις προτάσεις, υπάρχουν ορισμένοι προσομοιωτές Blockchain που προτείνονται στη βιβλιογραφία.

Στη βιβλιογραφία προτείνονται επίσης αρκετοί άλλοι προσομοιωτές δικτύου που μοιάζουν με Bitcoin[9] Ωστόσο, αυτές οι προτάσεις χρησιμοποιούν μοντέλα που βασίζονται σε προσομοίωση για να μελετήσουν συγκεκριμένες πτυχές των συστημάτων Blockchain. Δεν διασχίζουν διαφορετικά επίπεδα ούτε καλύπτουν όλα τα

[5] P. DUNPHY, F. A. P. PETITCOLAS, *A First Look at Identity Management Schemes on the Blockchain*, IEEE Security & Privacy, **16,** 4**,** pp. 20-29, 2018.

[6] R. Yasaweerasinghelage, M. Staples, and I. Weber, \Predicting latency of Blockchain-based systems using architectural modelling and simulation," in 2017 IEEE International Conference on Software Architecture (ICSA). IEEE, 2017, pp. 253{256.

[7] M. Alharby and A. Van Moorsel, \The impact of pro t uncertainty on miner de-cisions in Blockchain systems," Electronic Notes in Theoretical Computer Science, vol. 340, pp. 151{167, 2018.

[8] T. Neudecker, P. Andel nger, and H. Hartenstein, \A simulation model for analysis of attacks on the bitcoin peer-to-peer network," in 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, 2015, pp. 1327{1332.

[9] L. Stoykov, K. Zhang, and H.-A. Jacobsen, \Vibes: fast Blockchain simulations for large-scale peer-to-peer networks," in Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. ACM, 2017, pp. 19{20.

κοινά λειτουργικά δομικά στοιχεία (π.χ. μπλοκ και συναλλαγές) για συστήματα Blockchain.

Το παράδειγμα Blockchain παρέχει έναν μηχανισμό διάδοσης περιεχομένου και κατανεμημένης συναίνεσης σε δίκτυα Peer-to-Peer (P2P). Παρόλο που αυτό το παράδειγμα έχει υιοθετηθεί ευρέως στη βιομηχανία, δεν έχει αναλυθεί προσεκτικά όσον αφορά στην κλιμάκωση του δικτύου σε σχέση με τον αριθμό των ομολόγων. Οι εφαρμογές για συστήματα Blockchain, όπως κρυπτονομίσματα και IoT, απαιτούν αυτήν τη μορφή κλιμάκωσης δικτύου.

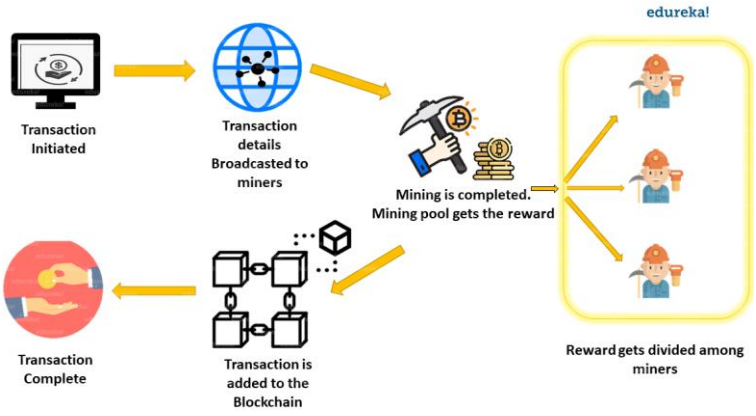
Το παράδειγμα Blockchain, επιτρέπει την κατανεμημένη συναίνεση μέσω ενός δικτύου peer-to-peer. Κάθε ομόλογος εξορύσσει συνεχώς νέες πληροφορίες που ονομάζονται μπλοκ, οι οποίες μπορούν να αποτελούνται από πιο λεπτομερείς πληροφορίες που ονομάζονται συναλλαγές. Έτσι, δημιουργούνται μπλοκ στο δίκτυο με την πάροδο του χρόνου. Κάθε ομόλογος που δημιουργεί (ορυχεία) ένα μπλοκ δημιουργεί επίσης αναφορές σε ένα ή περισσότερα μπλοκ που δημιουργήθηκαν προηγουμένως. Οι ομόλογοι επικοινωνούν επίσης μπλοκ για να συγχρονίσουν τα σύνολα πληροφοριών τους, δηλαδή τα σύνολα μπλοκ και τις αναφορές που γνωρίζουν οι ομόλογοι.

Εμπιστοσύνη

Ένας από τους κύριους στόχους ενός συστήματος Blockchain είναι να επιτρέψει τη συναίνεση μέσω κατανεμημένης εμπιστοσύνης. Η εμπιστοσύνη επιτυγχάνεται με τις αναφορές {ένα peer αναφέρεται μόνο σε ένα μπλοκ για το οποίο έχουν επαληθεύσει το περιεχόμενο}. Προκειμένου να επιτευχθεί κατανεμημένη συναίνεση, όλοι οι ομόλογοι πρέπει να εμπιστεύονται τα ίδια τμήματα. Εάν όλοι οι ομόλογοι εμπιστεύονται ένα μπλοκ, αυτό ονομάζεται επιβεβαιωμένο. Μια φυσική απαίτηση απόδοσης ενός συστήματος Blockchain είναι ότι το υποσύνολο των μπλοκ που επιβεβαιώνονται αυξάνεται με το χρόνο καθώς δημιουργούνται μπλοκ. Αυτό, ωστόσο, δεν είναι εγγυημένο καθώς δημιουργούνται μπλοκ με την πάροδο του χρόνου σε διαφορετικές τοποθεσίες στο δίκτυο και, στη συνέχεια, πρέπει να διαδοθούν. Λόγω περιορισμών εύρους ζώνης, οι επικοινωνίες στο δίκτυο δεν είναι στιγμιαίες και αντιμετωπίζουν καθυστερήσεις. Εάν δημιουργούνται μπλοκ πολύ γρήγορα [10] οι καθυστερήσεις

[10] Serguei Foss and Takis Konstantopoulos. An overview of some stochastic stability methods (< special issue> network design, control and optimization). Journal of the Operations Research Society of Japan, 47(4):275{303, 2004

προκαλούν συμφόρηση δικτύου και μπορούν να εμποδίσουν ένα σύστημα Blockchain να επιβεβαιώσει ένα μπλοκ. Καθώς η τεχνολογία Blockchain ωριμάζει και εξελίσσεται [11] είναι φυσιολογικό να μελετήσουμε τις προκλήσεις κλιμάκωσης που προκύπτουν λόγω της υιοθέτησής της. Η επεκτασιμότητα των κατανεμημένων πρωτοκόλλων συναίνεσης έχει μελετηθεί και σε διάφορα άλλα πλαίσια.



Block chain network

Bitcoin και το πρόβλημα των διπλών δαπανών

Γενικά

Οι τεχνολογίες Industry 4.0 αρχίζουν σταδιακά να επιφέρουν σημαντικό στρατηγικό αντίκτυπο σε εφαρμογές στη βιομηχανία μεταποίησης και υπηρεσιών, όπως ο προγραμματισμός (Dolgui et al. 2019b), και οι στρατηγικές διεργασίας και παγκοσμιοποίησης (Stentoft και Rajkumar 2019). Η τεχνολογία Blockchain έχει συγκεντρώσει μεγάλη προσοχή τα τελευταία χρόνια ως λύση για μια σειρά από επιχειρησιακές προκλήσεις σε διάφορους επιχειρηματικούς τομείς. Η έρευνα εντός του τομέα Blockchain επικεντρώνεται γενικά στην κρυπτογράφηση και στο Bitcoin. Υπάρχει αυξημένο ενδιαφέρον για τη χρήση του παραδείγματος Blockchain για την επίλυση επιχειρησιακών προκλήσεων στον κλάδο της μεταποίησης και των υπηρεσιών.

[11] Vivek Bagaria, Sreeram Kannan, David Tse, Giulia Fanti, and Pramod Viswanath. Prism: Deconstructing the Blockchain to approach physical limits. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pages 585{602. ACM, 2019

Σε αυτό το κεφάλαιο, παρουσιάζεται μια νέα επίπτωση της χρήσης της τεχνολογίας Blockchain. Πρώτον, παρουσιάζεται η έννοια του υπολογιστικού κόστους ως ουσιαστικό μηχανισμό για την ολοκλήρωση των επιχειρησιακών συναλλαγών στο περιβάλλον Blockchain. Δεύτερον, συζητείται η χρήση έξυπνων συμβάσεων και η επίδρασή τους στις επιχειρησιακές συναλλαγές.

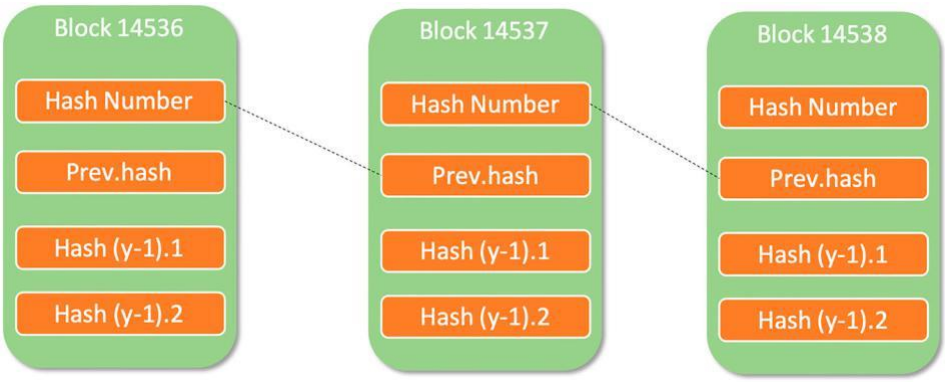
Αυτές οι δύο συνεισφορές βασίζονται στο έργο διαφόρων επιρροών από συγγραφείς (Roeck, Sternberg και Hofmann 2019; Stentoft and Rajkumar 2019; Dolgui et al. 2019a; 2019b) που έχουν συνεισφέρει στον τομέα του Industry 4.0, των έξυπνων συμβάσεων και των Blockchains. Προσδιορίζεται η πτυχή του υπολογιστικού κόστους σε ένα περιβάλλον Blockchain ως μια αναδυόμενη περιοχή έρευνας που έχει τη δυνατότητα να αλλάξει τις απόψεις μας σχετικά με το κόστος συναλλαγών, τα διαδικτυακά επιχειρηματικά μοντέλα, τις ταχύτητες επικοινωνίας της αλυσίδας εφοδιασμού και τις υπηρεσίες προστιθέμενης αξίας στους πελάτες. Η έννοια του υπολογιστικού κόστους βασίζεται στην υπολογιστική ισχύ και ταχύτητα, που είναι παραδοσιακά θέματα αρχιτεκτονικής υπολογιστών. Ωστόσο, ορισμένοι ερευνητές στον τομέα θεωρούν το υπολογιστικό κόστος ως κίνδυνο ασφάλειας (Cheng et al. 2019). Αν και αυτή είναι μια αναδυόμενη ιδέα στο περιβάλλον Blockchain, η άποψη του κόστους συναλλαγής στην αλληλεπίδραση μεταξύ οργανισμών σε υπολογιστικό επίπεδο είναι νέα. Ενώ τα οφέλη του Blockchain έχουν συζητηθεί εκτενώς (Kim και Laskowski 2018), υπάρχει μικρή ή καθόλου συζήτηση σχετικά με το υπολογιστικό κόστος ως παράγοντα που μπορεί να αυξήσει το κόστος των δημόσιων συναλλαγών Blockchain για αγοραστές και προμηθευτές, ειδικά από μια επιχειρησιακή συναλλαγή προοπτική.

Οι Roeck, Sternberg και Hofmann (2019) υιοθετούν μια προσέγγιση απαγωγικής περιπτωσιολογικής μελέτης για να μελετήσουν τις συναλλαγές που βασίζονται στην τεχνολογία μεταξύ οργανωτικών πακέτων μεταξύ αγοραστή και προμηθευτή σε μια αλυσίδα εφοδιασμού φυσικών αγαθών. Ερευνάται η χρήση υπολογιστικών δαπανών, που είναι εγγενείς σε συναλλαγές που ολοκληρώνονται σε ένα δημόσιο Blockchain, χρησιμοποιώντας μια πειραματική μεθοδολογία για να διερευνήσουμε τη σημασία τους για το Industry 4.0 και το λειτουργικό κόστος συναλλαγών. Ορίζεται το υπολογιστικό κόστος ως το συνολικό κόστος που απαιτείται για την ολοκλήρωση μιας συναλλαγής στο Blockchain. Σύμφωνα με τους κανόνες του Ethereum Blockchain, αυτό το κόστος πρέπει να καταβληθεί από τον εκκινητή (Wood 2017).

Αναπτύσσεται λοιπόν και εφαρμόζεται ένα πλήρως λειτουργικό εικονικό δημόσιο Blockchain σε μια πλατφόρμα γνωστή ως Ethereum (Wood 2017) για αποθήκευση, επικύρωση και συντήρηση συναλλαγών. Αυτή η μεθοδολογία παρέχει μια διαδικασία για τη μέτρηση του υπολογιστικού κόστους, της συχνότητας και της έντασης των συναλλαγών. Το Ethereum επιλέγεται λόγω της δημοτικότητάς του στην αγορά τόσο για χρήστες όσο και για επιχειρήσεις. Οι πληροφορίες από τις συνεισφορές συγκεντρώνονται μέσω της ανάλυσης 30 συναλλαγών που πραγματοποιούνται και καταγράφονται στο εικονικό Ethereum Blockchain. Η υπάρχουσα βιβλιογραφία σε αυτόν τον τομέα υποδηλώνει ότι η εισαγωγή και η εφαρμογή του Blockchain μπορεί να επηρεάσει αρνητικά τις δραστηριότητες σε τομείς όπως η παραγωγή (Dolgui et al. 2019b), logistics (Fran-cisco and Swanson 2018), ιχνηλασιμότητα (Hastig and Sodhi 2019), προμήθειες (White 2017), χρηματοδότηση, διακυβέρνηση (Shermin 2017), αλυσίδες εφοδιασμού (Yanling, Eleftherios και Weidong 2019) και η βιομηχανία γεωργικών τροφίμων (Zhao et al. 2019). Η τεχνολογία Blockchain προσφέρει επίσης ένα πλούσιο περιβάλλον για ακαδημαϊκή έρευνα. Ωστόσο, οι περισσότερες έρευνες σε αυτόν τον τομέα είναι ακόμη θεωρητικές, με ελάχιστες ή καθόλου εμπειρικές αποδείξεις ή περιπτώσεις πραγματικής χρήσης. Ο Lakhani (2017) προτείνει ότι ορισμένοι ερευνητές έχουν συζητήσει τις ανησυχίες τους σχετικά με το απόρρητο, την ασφάλεια και το κόστος λόγω της διαφημιστικής εκστρατείας γύρω από τη χρήση και την εφαρμογή του Blockchain.

Η εμφάνιση του Blockchain δημιούργησε τη δυνατότητα να μεταβάλλει πολλές βιομηχανίες. Για παράδειγμα, ο Min (2019) υποστηρίζει ότι έχει τη δυνατότητα να επηρεάσει τους οργανισμούς και τον τρόπο που πραγματοποιούν συναλλαγές με παρόμοιο τρόπο με τον τρόπο με τον οποίο η μορφή αρχείου MP3 επηρέασε τη μουσική βιομηχανία. Αυτή η διαταραχή επεκτείνεται επίσης στην κοινωνική χρήση, την οργανωτική στρατηγική, την τεχνολογική καινοτομία, τη διακυβέρνηση, την παραγωγή, την αποδοτικότητα, το κόστος και την εμπιστοσύνη (Pazaitis, De Filippi και Kostakis 2017; Sullivan and Burger 2017; Dolgui et al. 2019a; Dolgui et al. 2019b). Μέσα σε αυτό το πλήθος εφαρμογών, υπάρχουν πολλές βιομηχανίες για τις οποίες μπορεί να εφαρμοστεί το Blockchain, όπως η αλυσίδα εφοδιασμού και η κατασκευή (Olsen και Borit 2018; Min 2019; Stentoft and Rajkumar 2019; Dolgui et al. 2019a), χρηματοοικονομικές υπηρεσίες (Mori 2016 ; Gai, Qiu και Sun 2018), φαγητό (Zhao et al. 2019) και διακυβέρνηση (Shermin 2017).

Η σκόπιμη έλλειψη συγκέντρωσης διαφοροποιεί ένα Blockchain από μια παραδοσιακή σχεσιακή βάση δεδομένων (Jabbar, Akhtar και Dani 2019), κυρίως όσον αφορά τον τρόπο με τον οποίο τα άτομα και οι οργανισμοί βλέπουν και αποθηκεύουν δεδομένα. Αυτό έχει σχεδιαστεί για να δημιουργεί εμπιστοσύνη στα συστήματα και να διασφαλίζει ότι όλες οι προστιθέμενες συναλλαγές επαληθεύονται από άλλα μέλη του δημόσιου Blockchain (ανθρακωρύχοι) που ελέγχουν κόμβους. Κατ 'αρχήν, αυτός ο τύπος προσέγγισης επιτρέπει στους οργανισμούς να ολοκληρώνουν συναλλαγές χωρίς την ανάγκη για μεσάζοντες (Yeoh 2017), ελαχιστοποιώντας το κόστος και αυξάνοντας την αποτελεσματικότητα. Άλλες μελέτες σε αυτόν τον τομέα θεωρούν την τεχνολογία Blockchain ως αξιόλογη από επιχειρησιακή σκοπιά. Οι Bai και Sarkis (2020) συζητούν μεθόδους αξιολόγησης για την επιλογή της κατάλληλης τεχνολογίας Blockchain. Οι Yoon et al. (2020) χρησιμοποιούν ένα μοντέλο προσομοίωσης και ανάλυσης για να υποδείξουν ότι η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για τη διαχείριση της αστάθειας στο διεθνές εμπόριο. Οι Manupati et al. (2020) επικεντρώθηκαν στην παρακολούθηση αλυσίδων εφοδιασμού για εκπομπές άνθρακα και λειτουργικού κόστους στο πλαίσιο μιας προσέγγισης μοντελοποίησης εμπνευσμένης από Blockchain. Οι Kamble, Gunasekaran και Arha (2019) από την άλλη μεριά διεξάγουν μια εμπειρική μελέτη των προοπτικών της υιοθέτησης τεχνολογίας Blockchain.



Συμπληρωματικές Μεταφορές στο Blockchain

Στον πυρήνα του, ένα Blockchain βασίζεται στην έννοια μιας παραδοσιακής σχεσιακής βάσης δεδομένων (Zhao et al. 2019), με μερικές σημαντικές διαφορές. Πρώτον, υπάρχουν σημαντικές διαφορές στους τύπους δεδομένων που μπορούν να διατηρηθούν: δομημένα, ημι-δομημένα και μη δομημένα (Jabbar, Akhtar και Dani 2019). Δεύτερον, το χαρακτηριστικό αποκέντρωσης αλλάζει όπου βρίσκεται η βάση

δεδομένων. Τέλος, λόγω του αμετάβλητου χαρακτηριστικού του, ένα Blockchain μπορεί να λειτουργήσει ως μόνιμος δίσκος. Από την οπτική γωνία των συστημάτων πληροφοριών (DeLone και McLean 2003), αυτό μπορεί να φαίνεται ως κακή πρακτική, καθώς υπάρχει πιθανότητα επικάλυψης δεδομένων. Ωστόσο, αυτός ο κίνδυνος εξαλείφεται χρησιμοποιώντας τον αλγόριθμο συναίνεσης και τους «ανθρακωρύχους».

Η διαδικασία προσθήκης συναλλαγών σε ένα Blockchain είναι πολύπλοκη, με πολλούς παράγοντες και σημαντική απαιτούμενη δύναμη επεξεργασίας για διασύνδεση με αποτελεσματικό τρόπο. Υπάρχουν διαφορετικά στάδια για τους ανθρακωρύχους να επαληθεύσουν και να επικυρώσουν τις συναλλαγές και τις υπολογιστικές εργασίες μόλις προστεθούν στο Blockchain (Ankalkoti και Santhosh 2017). Προκειμένου οι οργανισμοί να έχουν πρόσβαση ή να αλληλεπιδρούν με ένα Blockchain, εμπλέκονται πέντε βασικά βήματα:

• Υπάρχει μια αρχική κλήση στο Blockchain για την έναρξη της συναλλαγής.

• Αυτή η συναλλαγή γίνεται αντικείμενο επεξεργασίας ως μπλοκ έτοιμο για διανομή.

• Το μπλοκ διανέμεται έπειτα σε κάθε μέρος του δικτύου.

• Μέσω της διαδικασίας εξόρυξης, το δίκτυο εγκρίνει αυτήν τη συναλλαγή.

• Το επαληθευμένο μπλοκ προστίθεται τώρα στο Blockchain και δημιουργείται ένας κατακερματισμός που συνδέει το τρέχον μπλοκ με το προηγούμενο μπλοκ, δημιουργώντας έτσι μια αλυσίδα.

Τόσο τα ιδιωτικά όσο και τα δημόσια Blockchains όπως γράψαμε στο προηγούμενο κεφάλαιο έχουν διαφορετικούς ρόλους στο οικοσύστημα Ethereum και έχουν διαφορετικά χαρακτηριστικά. Η κύρια διαφορά μεταξύ τους είναι η βάση για την άδεια. Ένα δημόσιο Blockchain από τη φύση του είναι «άδειο»: οποιοσδήποτε μπορεί να συμμετάσχει στο δίκτυο και να διαβάσει, να γράψει και να συμμετάσχει σε συναλλαγές. Αυτό παρουσιάζει αποκέντρωση στη δράση (Pazaitis, De Filippi και Kostakis 2017). Αντίθετα, ένα ιδιωτικό Blockchain έχει περιορισμούς για το ποιος επιτρέπεται να συμμετάσχει. Το βασικό ζήτημα και στα δύο αυτά σενάρια είναι ο τρόπος με τον οποίο τα δύο συστήματα βλέπουν τους χρήστες και ο ρόλος του κινήτρου έναντι της ταυτότητας. Για ιδιωτικά Blockchains, και αναμφισβήτητα για πολλούς κλάδους, είναι σημαντικό να γνωρίζουμε τους χρήστες (ποιοι είναι και τι κάνουν).

Αυτό δημιουργεί βεβαιότητα και ένα πλαίσιο εμπιστοσύνης (Anoaica and Levard 2018). Η εμπιστοσύνη είναι μια σημαντική αιτία ανησυχίας για τους περισσότερους διαχειριστές που ανησυχούν για τις επιπτώσεις της ασφάλειας στην ακεραιότητα δεδομένων εσωτερικών και εξωτερικών δικτύων (Wang et al. 2019). Για να οικοδομήσουμε εμπιστοσύνη σε ένα δημόσιο Blockchain και να ελαχιστοποιήσουμε τα ζητήματα απάτης και ασφάλειας, η εστίαση είναι στη χρήση θεωρίας παιχνιδιού και κινήτρων (κρυπτογράφηση) μέσω εξόρυξης για την ενθάρρυνση καλής συμπεριφοράς (Ankalkoti and Santhosh 2017). Τόσο τα ιδιωτικά όσο και τα δημόσια συστήματα έχουν διαφορετικά σενάρια χρήσης και συναφείς αλγόριθμους. Η έρευνα σε αυτόν τον τομέα είναι καινοτόμος και πολλές λύσεις προτείνονται σε διαφορετικά πλαίσια. Για παράδειγμα, η ανάπτυξη του Manuchain είναι ένα καινοτόμο βήμα προς τα εμπρός που διερευνά τη χρήση του Blockchain στην έξυπνη κατασκευή (Leng et al. 2020). Ωστόσο, για να ελαχιστοποιηθεί ο χρόνος επεξεργασίας συναλλαγών και τα μεγάλα σημεία συμφόρησης, το Manuchain πρέπει να ενσωματωθεί σε άλλα κυβερνο-συστήματα (Leng et al. 2020, 184). Επιπλέον, το Makerchain έχει προταθεί ως Blockchain με υπογραφές που εξετάζουν τη διαδικασία αυτο-οργάνωσης στην κοινωνική κατασκευή (Leng et al. 2019). Και οι δύο λύσεις βασίζονται σε δικαιώματα και έχουν πρωτότυπα βασισμένα σε ψηφιακά «δίδυμα». Όταν τα ιδιωτικά Blockchains χρειάζονται πρόσβαση σε άλλους φορείς σε έναν οργανισμό και γίνουν «ημι-ιδιωτικά», θα πρέπει να εξεταστεί ο αλγόριθμος συναίνεσης ο οποίος θα πρέπει να αλλάξει για να δώσει κίνητρα στους «ανθρακωρύχους».

Στον πυρήνα της οικονομικής λογικής των κρυπτονομισμάτων βρίσκεται το πρόβλημα της υπέρβασης του προβλήματος των διπλών δαπανών, το οποίο θέτει μια πρόκληση λογιστικής και λογοδοσίας που προσπάθησαν να ξεπεράσουν τα αποτελεσματικά κρυπτονομίσματα (βλ. πίσης συζητήσεις στο Decourt et al., 2017; Chohan 2017a, 2017b , 2017c, 2017d, 2017e, 2017f, 2017g, 2017h, 2017i, 2017j). Αυτό το κεφάλαιο εξετάζει τη συμβολή της βιβλιογραφίας, προκειμένου να καταδείξει καλύτερα την έρευνα σχετικά με τα προβλήματα διπλής δαπάνης σε κρυπτονομίσματα με μια ελαφριά κλίση προς θέματα διακυβέρνησης και λογοδοσίας (βλ. συζητήσεις διακυβέρνησης και λογοδοσίας στο Chohan 2017k, 2017l, 2017m, 2017n και Karame et al. (2015). Για τους σκοπούς του ορισμού, το πρόβλημα της διπλής δαπάνης είναι ένα πιθανό ελάττωμα σε μια κρυπτογράφηση ή σε άλλο σύστημα ψηφιακών μετρητών, με το οποίο το ίδιο ενιαίο ψηφιακό διακριτικό μπορεί να δαπανηθεί περισσότερες από

μία φορές, και αυτό είναι δυνατό επειδή ένα ψηφιακό διακριτικό αρχείο μπορεί να αναπαραχθεί ή να παραποιηθεί. Ο υποτιθέμενος δημιουργός του Bitcoin με το ψευδώνυμο Satoshi Nakamoto, προσανατολίστηκε στο πρόβλημα των διπλών δαπανών, και το συμπεριέλαβε στη λευκή βίβλο που περιγράφει την ανάπτυξη του Bitcoin (2008). Επομένως, το πρόβλημα των διπλών δαπανών εγείρει ερωτήματα σχετικά με την προστασία του ψηφιακού νομίσματος με τον ίδιο τρόπο που τα παραδοσιακά νομίσματα πρέπει να προστατεύονται από την απάτη ή την πλαστογραφία, με υποκείμενα ζητήματα λογοδοσίας στην προστασία των ψηφιακών πληροφοριών.

Όπως σημειώνει ο Rosenfeld (2014) «Ενώ η ποιοτική φύση αυτού του συστήματος είναι καλά κατανοητή, υπάρχει ευρεία σύγχυση σχετικά με τις ποσοτικές πτυχές του και τον τρόπο με τον οποίο σχετίζονται με τους φορείς επίθεσης και τα αντίμετρά τους». Αναλογικά για την παραχάραξη του παραδοσιακού χρήματος, το πρόβλημα των διπλών δαπανών ασκεί πληθωριστική πίεση δημιουργώντας μια νέα προσφορά δόλιου νομίσματος που δεν υπήρχε προηγουμένως, μειώνοντας έτσι την αξία του ψηφιακού νομίσματος σε σχέση με το γενικό επίπεδο τιμών (ή άλλες νομισματικές μονάδες σύγκρισης). Με τη σειρά του, αυτό θέτει σε κίνδυνο τη διακυβέρνηση και την υπευθυνότητα που σχετίζονται με την εμπιστοσύνη των χρηστών στο νόμισμα και μπορεί να θέσει σε κίνδυνο την προθυμία των χρηστών να διατηρήσουν το νόμισμα, γεγονός που μπορεί να αποτρέψει την κυκλοφορία της προσφοράς νομίσματος. Για την αντιμετώπιση αυτού του προβλήματος διπλών δαπανών, διάφορες κρυπτογραφικές τεχνικές μπορούν και χρησιμοποιούνται, οι οποίες αποτελούν μέρος της βιβλιογραφικής επισκόπησης αυτού του κεφαλαίου. Ο φερόμενος ως δημιουργός του Bitcoin, Satoshi Nakamoto, προσανατολίστηκε έντονα στο πρόβλημα των διπλών δαπανών και το συμπεριέλαβε στο λευκό χαρτί που περιγράφει την ανάπτυξη του Bitcoin (2008), υποδεικνύοντας ότι θα μπορούσε να επιλυθεί «να επιλυθεί χρησιμοποιώντας έναν διακομιστή κατανεμημένης χρονικής σήμανσης P2P δημιουργήστε υπολογιστική απόδειξη της χρονολογικής σειράς συναλλαγών. "

Ωστόσο, από το 1993, η Brands παρουσίασε μια μέθοδο για κρυπτογραφικές διεργασίες γνωστές ως περιοριστικές τυφλές υπογραφές, οι οποίες αποτελούν τη ραχοκοκαλιά του συνόλου των κρυπτονομισμάτων. Αφού αντιπαρέθεσε τις τυφλές υπογραφές μίας προβολής με τη μέθοδο των πορτοφολιών (portfolios) για τους παρατηρητές, διατύπωσε περιοριστικές υπογραφές (blinded) «σε συνδυασμό με το

λεγόμενο πρόβλημα εκπροσώπησης σε ομάδες πρώτης τάξης» που θα δημιουργούσαν «εξαιρετικά αποτελεσματικά συστήματα μετρητών εκτός σύνδεσης που μπορούν να επεκταθούν ουσιαστικά χωρίς επιπλέον κόστος σε «πορτοφόλια» με παρατηρητές σύμφωνα με τις πιο αυστηρές απαιτήσεις απορρήτου.

Ο φόρτος εργασίας για τον παρατηρητή είναι τόσο μικρός που μπορεί να εκτελεστεί από μια έξυπνη κάρτα ανθεκτική σε παραβίαση ικανή να εκτελέσει το σχήμα αναγνώρισης Schnorr »(Brands 1993). Ο Ferguson (1993) τόνισε ότι ένα καλύτερο σύστημα θα χρησιμοποιούσε έναν μόνο όρο για μεγάλο αριθμό πιθανών προκλήσεων, και έτσι αντί να χρησιμοποιήσει ένα πρωτόκολλο απόσυρσης.

Οι Medvinsky et al. (1993), ενώ χρησιμοποίησαν ως προϋπόθεση τα ηλεκτρονικά μετρητά ("Netcash") τόνισαν την ανάγκη για ισχυρά πρωτόκολλα πρόσβασης σε μια τέτοια αρχιτεκτονική. Οι Krsul et al. (1998) κατοχύρωσαν με δίπλωμα ευρεσιτεχνίας μια μέθοδο ηλεκτρονικών πληρωμών που θα αντιμετώπιζε το πρόβλημα των διπλών δαπανών εισάγοντας «Μια μέθοδο δημιουργίας ηλεκτρονικών νομισματικών μαρκών» όπου η δημιουργία κάθε «ηλεκτρονικού μάρκου από έναν πάροχο χρηματοπιστωτικών υπηρεσιών ξεκινά ως απάντηση σε αίτημα ενός αγοραστή για τη δημιουργία ηλεκτρονικών νομισμάτων με σκοπό τη χρήση από έναν αναγνωρισμένο πωλητή. Σε αυτήν τη διαδικασία, ο πάροχος χρηματοοικονομικών υπηρεσιών θα «δημιουργούσε πολλαπλότητα ηλεκτρονικών νομισματικών διακριτικών» και στη συνέχεια «θα διαιρούσε κάθε ηλεκτρονικό νομισματικό διακριτικό σε δύο ηλεκτρονικά διηρημένα κατά το ήμισυ σύμβολα και θα συσχετιζόταν με τον ίδιο σειριακό αριθμό» (Krsul et al., 1998). Αυτά τα μισά ηλεκτρονικών διακριτικών, όταν συνδυάζονται, θα αναδημιουργήσουν το ηλεκτρονικό νομισματικό διακριτικό από το οποίο δημιουργήθηκαν.

Μετά την κατανομή των μισών μεταξύ των μερών αγοραστή και πωλητή, θα ήταν δυνατό για τον αγοραστή και τον πωλητή να πραγματοποιήσει πολλαπλές συναλλαγές εκτός σύνδεσης του παρόχου χρηματοοικονομικών υπηρεσιών (Krsul et al., 1998). Περίπου αυτήν την περίοδο, οι Pointcheval et al., στο περιοδικό Journal of Cryptology, αναγνώρισαν ότι ένας κρυπτογραφικός αλγόριθμος που μπορεί να αντέξει κρυπτοαναλυτικές επιθέσεις για αρκετά χρόνια θεωρείται συχνά ως ένα είδος διαδικασίας επικύρωσης, Οι Pointcheval et al. (2000) προσέφερε επιχειρήματα ασφαλείας για μια μεγάλη κατηγορία γνωστών σχεδίων υπογραφήςes, εξετάζοντας

ειδικότερα την ασφάλεια των τυφλών υπογραφών (που χρησιμοποιούνται σήμερα), τα οποία υποστήριξαν ότι ήταν «το πιο σημαντικό συστατικό για την ανωνυμία στα ηλεκτρονικά συστήματα μετρητών εκτός σύνδεσης», με έμφαση στην «κατάλληλη έννοια της ασφάλειας που σχετίζεται με τη ρύθμιση των ηλεκτρονικών μετρητών.».

Ο Karame et al. μελέτησαν το πρόβλημα των διπλών δαπανών στο πλαίσιο του Bitcoin συγκεκριμένα, και κατέδειξαν ότι «το σύστημα επαλήθευσης πληρωμών Bitcoin έχει σχεδιαστεί για να αποτρέπει τις διπλές δαπάνες (2012α, 2012β). Αυτό το πρόβλημα, από αυτήν την άποψη τονίζεται ιδιαίτερα από την εξαιρετικά υψηλή πίεση στο εύρος ζώνης του δικτύου Bitcoin (Chohan 2017a-d). Οι Karame et al., διαπίστωσαν επίσης κατά τη διάρκεια της έρευνάς τους ότι, εκτός της ενσωμάτωσης κατάλληλων τεχνικών ανίχνευσης στην αρχιτεκτονική εφαρμογής του Bitcoin, «οι επιθέσεις διπλών δαπανών σε γρήγορες πληρωμές επιτυγχάνουν με συντριπτική πιθανότητα και μπορούν να τοποθετηθούν με χαμηλό κόστος» (2012a , 2012β), και ως επακόλουθο «τα μέτρα που συνιστώνται από τους προγραμματιστές.

Η χρήση των Bitcoin σε γρήγορες πληρωμές δεν είναι πάντα αποτελεσματική στον εντοπισμό των διπλών δαπανών, γι 'αυτό ακόμη και αν οι συστάσεις τους ενσωματώθηκαν σε μελλοντικές υλοποιήσεις Bitcoin, "*Οι επιθέσεις διπλών δαπανών στο Bitcoin θα εξακολουθούν να είναι δυνατές*" (Karame et al., 2012a, 2012b). Από την άλλη μεριά ο Rozenfeld παρατήρησε ότι «*Αν και η ποιοτική φύση αυτού του συστήματος είναι καλά κατανοητή, υπάρχει ευρεία σύγχυση σχετικά με τις ποσοτικές πτυχές του και τον τρόπο με τον οποίο σχετίζονται με τους φορείς επίθεσης και τα αντίμετρά τους*», και έτσι προσπάθησε να περιγράψει και να αναλύσει τις διεργασίες στις οποίες βασίζονται οι τυπικές επιθέσεις και οι πιθανότητες επιτυχίας τους (2014). Τέλος οι Karame et al. (2015) διεξήγαγαν μια σημαντική μελέτη για την «*κακή συμπεριφορά στο Bitcoin*», επισημαίνοντας τα ζητήματα υπευθυνότητας που προέκυψαν από αυτό. Όπως σημειώνουν, αναπόφευκτα, σε ένα τέτοιο περιβάλλον, η ασφάλεια των συναλλαγών έρχεται σε αντίθεση με το απόρρητο των συναλλαγών.

Η χρήση τεχνολογίας Block chain με συμπληρωματικές τεχνολογίες.

Με την ταχεία ανάπτυξη βιώσιμων ενεργειακών τεχνολογιών και τεχνολογιών δικτύου, το Ενεργειακό Διαδίκτυο που εκπροσωπείται από το «New Energy + Internet» έχει γίνει το νέο σύνορο της τεχνολογικής καινοτομίας στη διεθνή ενεργειακή ακαδημαϊκή και βιομηχανία. Επιπλέον, αποτελεί επίσης σημαντική κατεύθυνση ανάπτυξης στον τομέα της ενέργειας μετά το έξυπνο δίκτυο. Ωστόσο, το Διαδίκτυο Ενέργειας περιλαμβάνει περισσότερες μορφές ενέργειας και περισσότερους συμμετέχοντες, η ενέργεια και οι πληροφορίες του είναι καλά ενσωματωμένες και ορισμένες προκλήσεις είναι δύσκολο να ξεπεραστούν, όπως ο έλεγχος και η διαχείριση των κατανεμημένων μορφών βιώσιμης ενέργειας. Μέχρι στιγμής, η έρευνα στο Διαδίκτυο Ενέργειας βρίσκεται ακόμη στο επίπεδο της θεωρητικής έρευνας και του σχεδιασμού της αρχιτεκτονικής. Το Energy Internet που λειτουργεί είναι ακόμα σπάνιο. Επομένως, χρειάζονται επειγόντως νέες τεχνολογίες για να βοηθήσουν στην κατασκευή και την εμπορευματοποίηση του Διαδικτύου Ενέργειας.

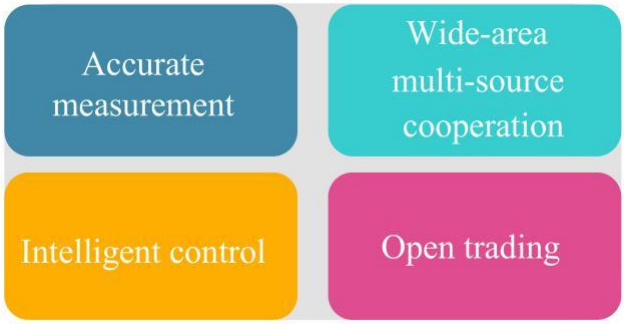
Το Blockchain θεωρείται ως η πέμπτη επαναστατική καινοτομία του υποδείγματος υπολογιστών, μετά από τους υπολογιστές mainframe, προσωπικούς υπολογιστές, Διαδίκτυο και κινητά / κοινωνικά δίκτυα. Προς το παρόν, η εξερεύνηση της τεχνολογίας Blockchain είναι κορυφαία στον χρηματοπιστωτικό κλάδο, ενώ οι εφαρμογές σε άλλους κλάδους επεκτείνονται γρήγορα. Οι βασικές τεχνολογίες στο Blockchain όπως οι μηχανισμοί συναίνεσης, οι αλγόριθμοι κρυπτογράφησης, οι έξυπνες συμβάσεις και η κατανεμημένη αποθήκευση δεδομένων μπορούν να χρησιμοποιηθούν για την επίλυση ορισμένων από τα δύσκολα προβλήματα στην κατασκευή του Energy Internet.

Τα μικροδίκτυα και η κατανεμημένη βιώσιμη ενέργεια περιλαμβάνονται στο Διαδίκτυο Ενέργειας. Αυτά τα δύο στοιχεία αντιπροσωπεύουν τόσο τον παραγωγό όσο και τον πελάτη. Επιπλέον, οι δραστηριότητες παραγωγής, κατανάλωσης και συναλλαγών τους πρέπει να καθίστανται αντικείμενο διαχείρισης ανεξάρτητα. Η ενέργεια και οι πληροφορίες μεταξύ των συστημάτων είναι πολύ αλληλένδετες και η διαφάνεια και η ασφάλεια των δεδομένων πρέπει να αφορούν τη βάση των έξυπνων συναλλαγών. Σύμφωνα με αυτήν την αρχή, εάν το Ενεργειακό Διαδίκτυο χρησιμοποιεί μια παραδοσιακή λύση για τη δημιουργία ενός κεντρικού ιδρύματος ως αξιόπιστου κέντρου, όλες οι συναλλαγές θα μεταφέρονται μέσω του κεντρικού ιδρύματος. Σε

αυτήν την περίπτωση, εάν το κεντρικό όργανο μπορεί να ελέγξει ή να διαχειριστεί αποτελεσματικά θα ήταν απρόβλεπτο ερώτημα. Επιπλέον, το Ενεργειακό Διαδίκτυο επιτρέπει την πρόσβαση σε διάφορες μορφές ενέργειας, δηλαδή το άνοιγμα του Ενεργειακού Διαδικτύου, το οποίο δείχνει μια μεγάλη πρόκληση για τη διαφάνεια του κεντρικού θεσμού

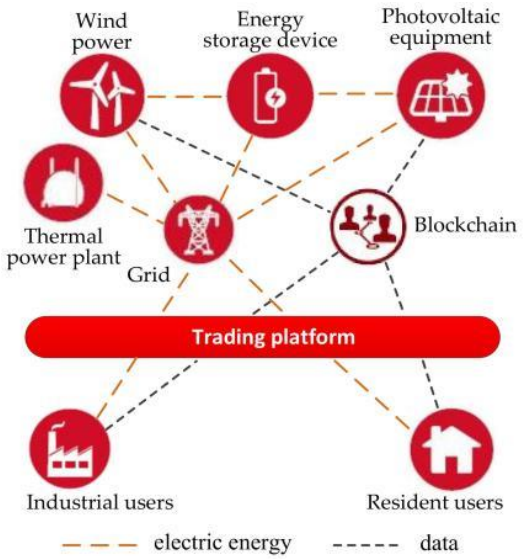
Τα χαρακτηριστικά του Energy Internet και των τεχνολογιών Blockchain αφορούν στη συνοχή. Σε αυτό το σενάριο, εάν το Blockchain εφαρμόζεται στο Internet Energy, μπορεί να οριστεί ως μια αποκεντρωμένη πλατφόρμα συναλλαγών ενέργειας που βασίζεται στον μηχανισμό συναίνεσης. Εν τω μεταξύ, η αυτοματοποιημένη και αποτελεσματική διαπραγμάτευση διασφαλίζεται από την εφαρμογή έξυπνων αντιθέσεων. Οι συμμετέχοντες επιτρέπεται να υποβάλλουν ερωτήματα για δεδομένα συναλλαγών στο Blockchain, το οποίο διασφαλίζει τη διαφάνεια ολόκληρης της πλατφόρμας. Επιπλέον, τα δεδομένα στο σύστημα προστατεύονται από αλγόριθμους κρυπτογράφησης και αποθήκευση διανεμητικών δεδομένων. Πάνω απ 'όλα όμως, η τεχνολογία Blockchain μπορεί να εφαρμοστεί στο Energy Internet και είναι εφικτή.

Με την εξάντληση της παραδοσιακής ορυκτής ενέργειας και τα ολοένα και πιο σοβαρά περιβαλλοντικά προβλήματα, ο τρόπος ανάπτυξης της ενέργειας που βασίζεται στην παραδοσιακή ορυκτή ενέργεια είναι δύσκολο να διατηρηθεί. Είναι μια γενική τάση αντικατάστασης της ορυκτής ενέργειας με καθαρή και βιώσιμη ενέργεια. Προς το παρόν, αν και η έρευνα στον τομέα της αειφόρου ενέργειας έχει σημειώσει κάποια πρόοδο, οι σχετικά ώριμες τεχνολογίες όπως η αιολική ενέργεια και η ηλιακή ενέργεια έχουν τα προβλήματα της αποκεντρωμένης γεωγραφικής κατανομής, των χαμηλών ποσοστών διαχείρισης και χρήσης και του υψηλού κόστους μετατροπής ενέργειας, οδηγώντας σε μεγάλο περιορισμό στη χρήση νέας ενέργειας σε εφαρμογές μεγάλης κλίμακας και στην εμπορία. Το 2008, το «Σύστημα διαχείρισης ενέργειας μελλοντικής ενέργειας από ανανεώσιμες πηγές ενέργειας», με το έργο του Εθνικού Ιδρύματος Επιστημών (NSF), πρότεινε την έννοια του Διαδικτύου Ενέργειας. Αυτή η ακαδημαϊκή ιδέα επισημαίνει ότι το Διαδίκτυο Ενέργειας είναι ένας νέος τύπος δομής ηλεκτρικού δικτύου που βασίζεται στην παραγωγή ανανεώσιμων πηγών ενέργειας, σε συσκευές αποθήκευσης κατανεμημένης ενέργειας και στο υπάρχον Διαδίκτυο.



The characteristics of the Energy Internet

Η παραδοσιακή εμπορία ενέργειας γίνεται μέσω ενός κεντρικού οργανισμού. Με την πρόσβαση μεγάλου αριθμού καταναλωτών, το Energy Internet έχει γίνει πιο περίπλοκο. Εάν δημιουργηθεί ένας κεντρικός οργανισμός, υπάρχουν προβλήματα όπως το υψηλό λειτουργικό κόστος και η κακή ασφάλεια των πληροφοριών. Εάν δεν υπάρχει κεντρικός οργανισμός διαχείρισης, θα υπάρχει το πρόβλημα της δυσπιστίας της εμπορικής οντότητας. Η εισαγωγή της τεχνολογίας blockchain στο εμπόριο ενέργειας μπορεί να ξεπεράσει αυτά τα προβλήματα. Το μοντέλο εμπορίας ενέργειας P2P που βασίζεται σε Blockchain μπορεί να προσφέρει μια αποτελεσματική, φθηνή, ανοιχτή και αξιόπιστη πλατφόρμα συναλλαγών για το Energy Internet. Το σχήμα παρακάτω δείχνει τη διαδικασία διαπραγμάτευσης ισχύος με βάση το Blockchain.



Ταυτόχρονα, η παραδοσιακή διαδικασία ανάπτυξης στοιχείων άνθρακα διαρκεί πολύ χρόνο, με τη συμμετοχή εταιρειών, κυβερνητικών ρυθμιστικών αρχών, ανταλλαγών περιουσιακών στοιχείων άνθρακα, οργανισμών επαλήθευσης και πιστοποίησης τρίτων

και ούτω καθεξής. Ο μέσος χρόνος ανάπτυξης είναι περισσότερο από ένα έτος και κάθε κόμβος που συμμετέχει θα έχει μεγάλο αριθμό μεταφορών αρχείων, οι οποίες είναι επιρρεπείς σε σφάλματα. Το Blockchain μπορεί επίσης να λύσει αυτό το πρόβλημα.

Τα εργαστήρια Energy Blockchain της IBM και της Κίνας έχουν δημιουργήσει την πρώτη πλατφόρμα διαχείρισης πράσινων περιουσιακών στοιχείων που βασίζεται σε Blockchain για την υποστήριξη τεχνολογιών χαμηλών εκπομπών άνθρακα. Η πλατφόρμα θα μειώσει δραματικά τον κύκλο ανάπτυξης των περιουσιακών στοιχείων διοξειδίου του άνθρακα και θα μειώσει το κόστος ανάπτυξης των περιουσιακών στοιχείων διοξειδίου του άνθρακα κατά 20% σε 30%.

Η τεχνολογία Blockchain έχει τα χαρακτηριστικά της αποκέντρωσης και της αμοιβαίας συμπληρωματικότητας, η οποία είναι παρόμοια με τη γεωγραφική διασπορά και τον προγραμματισμό εικονικών σταθμών παραγωγής ενέργειας. Ωστόσο, το κόστος συναλλαγής είναι υψηλότερο μεταξύ εικονικών μονάδων παραγωγής ενέργειας και χρηστών. Επιπλέον, ο μηχανισμός κατανομής κερδών κάθε VPP δεν είναι ανοιχτός. Η αμφίδρομη επιλογή συμμετρίας πληροφοριών δεν μπορεί να διαμορφωθεί μεταξύ κατανεμημένης ενέργειας και VPP, γεγονός που αυξάνει το πιστωτικό κόστος στη διαδικασία συναλλαγής. Η τεχνολογία Blockchain έχει τα πλεονεκτήματά της στις εφαρμογές συναλλαγών λόγω των δικών της χαρακτηριστικών και μπορεί να παρέχει μια διαφανή, δίκαιη, αξιόπιστη και χαμηλού κόστους πλατφόρμα συναλλαγών για εικονικούς σταθμούς παραγωγής ενέργειας. Επομένως, η τεχνολογία Blockchain είναι κατάλληλη για χρήση σε δίκτυα ενέργειας.

Το παραπάνω παράδειγμα αποδεικνύει ότι η τεχνολογία BlockChain συναρτάται με άλλες τεχνολογίες.

PI Cryptocurrency

Το π (pi) το δημιούργησε ο Ελληνας Δρ Νικόλαος Κόκκαλης μαζί με τηνDr. Chengdiao Fan και τον Vincent McPhillip στο πανεπιστήμιο Στάνφορτ. Για να αποκτήσει κάποιος το νέο κρυπτονόμισμα π δεν χρειάζεται να ξοδέψει χρήματα για να αγοράσει τον εξοπλισμό με τον οποίο θα κάνει mining όπως χρειάζεται στα υπόλοιπα, αρκεί να κατεβάσει δωρεάν την εφαρμογή Pi network από το App store ή το Google play. Η εφαρμογή δεν καταναλώνει μπαταρία, δεν δεσμεύει μνήμη από τη συσκευή(όπως τα άλλα κρυπτονομίσματα), το μόνο που χρειάζεται είναι να πατάτε ένα κουμπί μια φορά το 24ωρο ώστε να συνεχίζεται το mining....12

Το Pi Cryptocurrency είναι μια πρωτοποριακή πλατφόρμα. Αποτελεί το μόνο κρυπτονομισμα που δίνει την ευκαιρία να εξορύξει κάποιος κρυπτονόμισμα στο smartphone του χωρίς να εξαντλείται απαραίτητα η διάρκεια ζωής της μπαταρίας ή τα δεδομένα του κινητού.

Θεμελιωμένο στην προηγμένη τεχνολογία blockchain, το Pi Cryptocurrency είναι ασφαλές, αμετάβλητο, λειτουργικό και νόμιμο κρυπτονόμισμα. Αυτό το κρυπτονομισμα έχει την ιδιότητα να είναι αμετάβλητο πράγμα που σημαίνει απλώς ότι όλες οι πληροφορίες που καταγράφονται στο δίκτυο δεν μπορούν να τροποποιηθούν από οποιονδήποτε στο δίκτυο.

Ένα ενδιαφέρον χαρακτηριστικό του Pi Cryptocurrency είναι ότι δίνει την ευκαιρία να κλιμακώσει κάποιος τις αγορές του χωρίς μεγάλη κατανάλωση ενέργειας. Όπως ορθά δήλωσε η ομάδα προγραμματιστών του κρυπτονομίσματος αυτού, αυτή η οντότητα

κρυπτογράφησης τυγχάνει να απέχει αρκετά από το Bitcoin με διάφορους τρόπους. Θα χρησιμοποιήσουμε ένα παράδειγμα για να υποστηρίξουμε αυτόν τον ισχυρισμό.

Οι ανθρακωρύχοι στο δίκτυο Bitcoin μπορούν εύκολα να εξορύξουν πάνω από 50 BTC, απλά εκτελώντας λογισμικό εξόρυξης στους υπολογιστές τους. Με τη πάροδο του χρόνου και καθώς η αγοραία αξία του Bitcoin συνέχισε να αυξάνεται προσελκύοντας περισσότερους επενδυτές, οι εταιρείες με εξελιγμένους υπολογιστές και εξοπλισμό άρχισαν να αναδύονται.

Αυτές οι εταιρείες συνέχισαν να αναπτύσσουν και να προωθούν εξελιγμένες τεχνολογίες εξόρυξης μετά την άλλη. Η εισροή αυτών των προηγμένων και εξελιγμένων εγκαταστάσεων εξόρυξης σήμαινε ότι οι αγωνιζόμενοι ανθρακωρύχοι χωρίς κεφάλαια για να αποκτήσουν αυτές τις προηγμένες εξέδρες έπρεπε να σταματήσουν, καθώς δεν μπορούσαν να ανταγωνιστούν τους καλά εξοπλισμένους ομολόγους τους.

Αυτό οδήγησε στη δημιουργία εκμεταλλεύσεων εξόρυξης που απαιτούσαν επαρκή ισχύ και υπολογιστικούς πόρους για την εξόρυξη. Το δίκτυο Bitcoin που σχεδιάστηκε για να αποκεντρωθεί έγινε συγκεντρωτικό με τους περισσότερους ανθρακωρύχους να μην γνωρίζουν αυτήν τη μαζική αλλαγή.

Επί του παρόντος, μόνο το 1% περίπου των συνολικών χρηστών Bitcoin ελέγχει το 87% του συνολικού αριθμού BTC. Οι προγραμματιστές του Pi Cryptocurrency που είναι καινοτόμοι και καθοδηγούνται προς τα εμπρός, ενσωμάτωσαν το Stellar Consensus Protocol, το οποίο είναι εντελώς διαφορετικό από τον αλγόριθμο συναίνεσης εργασίας του περιβάλλοντος του Bitcoin.

Οι δημιουργοί του Δικτύου Pi ήθελαν να το κάνουν διαφορετικό και πιο αποτελεσματικό από οποιοδήποτε άλλο κρυπτογραφικό στοιχείο. Βέβαια ήταν κρίσιμο για αυτούς το γεγονός ότι ότι το Pi Cryptocurrency δεν εμπίπτει στα ίδια προβλήματα που αντιμετωπίζουν σήμερα το Bitcoin και άλλα κρυπτο-νομίσματα.

Επέλεξαν λοιπόν το αστρικό πρωτόκολλο ως μηχανισμό συναίνεσης για το Pi. Πριν εξερευνήσουμε πλήρως τα διάφορα επίπεδα εξόρυξης που είναι διαθέσιμα στο Pi

Cryptocurrency, είναι καλύτερο να λάβουμε μια ιδέα για το τι είναι το Stellar Consensus Protocol και πώς διαφέρει από την απόδειξη της συναίνεσης εργασίας.

Αυτός ο αλγόριθμος συναίνεσης είναι απλά ένα σύστημα FBA (Federated Byzantine Agreement) που προσφέρει σε όλα τα αποκεντρωμένα δίκτυα στο δίκτυο Cry Cryptocurrency την ευκαιρία να επιτύχουν συναίνεση όσο το δυνατόν γρηγορότερα.

Σε αυτόν τον αλγόριθμο συναίνεσης, οι κόμβοι δεν ανταγωνίζονται μεταξύ τους, αλλά κάθε κόμβος φέρει την ευθύνη να καθορίσει εάν μια συναλλαγή που πραγματοποιείται από έναν χρήστη είναι έγκυρη ή όχι. Μόλις ένα μπλοκ (συναλλαγή) εντοπιστεί από έναν κόμβο, ένα μήνυμα αποστέλλεται σε άλλους στο δίκτυο και θα ακολουθήσει μια σειρά ψηφοφορίας για να προσδιοριστεί ποιο μπλοκ θα καταγραφεί στο blockchain του δικτύου.

Το Πρωτόκολλο Stellar Consensus παρέχει στο δίκτυο τέσσερις διαφορετικές προσαρμογές που αντιπροσωπεύουν τα διαφορετικά επίπεδα εξόρυξης στο δίκτυο Pi Cryptocurrency. Αυτά τα επίπεδα εξόρυξης είναι:

1. Επίπεδο πρωτοπόρου · σχετικά με το Pi Cryptocurrency, αυτό απλά αναφέρεται σε ένα ανθρακωρύχο ο οποίος στο πλαίσιο του δικτύου παρέχει ουσιαστική απόδειξη ότι δεν είναι ρομπότ. Για να αποδείξουν αυτό, οι πρωτοπόροι ανθρακωρύχοι θα πρέπει απλώς να ξεκινήσουν μια συνεδρία εξόρυξης στο δίκτυο. Οι ανθρακωρύχοι επιπέδου Pioneer – Πρωτοπόρου μπορούν επίσης να ξεκινήσουν συναλλαγές peer-to-peer (P2P) στο δίκτυο.

2. Επίπεδο συντελεστών Οι συνεργάτες είναι πρωτοπόροι που συμβάλλουν στην ανάπτυξη του δικτύου παρέχοντας μια λίστα με πρωτοπόρους που είναι αξιόπιστοι. Αυτοί οι αξιόπιστοι πρωτοπόροι θα βοηθήσουν στη δημιουργία του γραφήματος εμπιστοσύνης.

3. Επίπεδο πρέσβη · Αυτός είναι απλά ένας χρήστης του δικτύου του οποίου η αρμοδιότητα στο δίκτυο είναι να εισαγάγει νέα μέλη στο Pi Cryptocurrency.

4. Κόμβοι αυτοί είναι χρήστες που είναι τόσο συνεισφέροντες όσο και πρωτοπόροι στο δίκτυο. Βοηθούν επίσης στην εκτέλεση κόμβων Pi στους προσωπικούς τους υπολογιστές. Αυτοί οι κόμβοι είναι εκείνοι που είναι υπεύθυνοι για την επικύρωση

των μπλοκ στο δίκτυο. Οι πρωτοπόροι και οι συνεργάτες μπορούν να εκτελέσουν το λογισμικό Pi node στον υπολογιστή τους.

Εφαρμογές Pl Cryptocurrency

Ως προς την εμπορικότητα του Pi Cryptocurrency υπάρχουν πολλές πιθανές περιπτώσεις χρήσης του δικτύου στην αγορά.

1. Κοινή αγορά Πρόκειται για μια πλατφόρμα κοινωνικών μέσων μορφής Instagram όπου τα μέλη μπορούν να δημοσιεύουν στο δίκτυο και είτε να ποντάρουν είτε να ξοδεύουν το Pi για να τραβήξουν την προσοχή άλλων στο δίκτυο. Αυτό σημαίνει απλώς ότι οι χρήστες σε αυτήν την πλατφόρμα κοινωνικών μέσων μπορούν να δημοσιεύουν αναρτήσεις και να πληρώνουν το δίκτυο, ώστε οι χρήστες να βλέπουν αυτές τις αναρτήσεις. Αυτό λειτουργεί ακριβώς όπως η λειτουργία "Προώθηση διαφημίσεων" στο Instagram.

2. Εμπιστοσύνη γραφημάτων. Αυτή η λειτουργία είναι απλώς ένας χάρτης που περιέχει την αξιολόγηση των κόμβων, των πρωτοπόρων και των συντελεστών στο δίκτυο με βάση τον αριθμό των ατόμων που προσλαμβάνουν και επίσης τη συνολική συμπεριφορά του κόμβου. Αυτό το γράφημα αξιοπιστίας θα συνδέει νέους χρήστες στον καλύτερο ή στον πλησιέστερο κόμβο κάθε φορά που λαμβάνουν ή θέλουν να στείλουν το Pi σε όλο το δίκτυο.

3. Αποκεντρωμένο App Store. Αυτό αποτελεί ένα κατάστημα εφαρμογών όπου οι προγραμματιστές στο δίκτυο μπορούν να αναπτύξουν και να πουλήσουν τις πρόσφατα αναπτυγμένες εφαρμογές τους χωρίς να χρειάζεται να κάνουν bootstrap. Αυτό το πρόγραμμα – εφαρμογή είναι παρόμοιο με το δημοφιλές Google Playstore.

4. Διακυβέρνηση – Διαχείριση του Pi κάτω των 5 εκατομμυρίων · Αυτή αποτελεί μια παρόμοια αρχή διακυβέρνησης που υιοθετήθηκε από τα δίκτυα Bitcoin και Ethereum. η μόνη διαφορά είναι ότι το PI είναι η κλειστή πηγή, ενώ, στα δίκτυα Ethereum και Bitcoin, οι προγραμματιστές μπορούν να δημιουργήσουν κωδικούς για τη βελτίωση του δικτύου.

5. Διακυβέρνηση – Διαχείριση του Pi πάνω από 5 εκατομμύρια χρήστες Αυτή αποτελεί μια επιτροπή στο δίκτυο. Αυτή η επιτροπή θα καθορίσει πού οδεύει το δίκτυο στη

διάρκεια του έτους. Μόνο οι συνεισφέροντες, οι κόμβοι και οι πρωτοπόροι που κατατάσσονται ψηλά στο γράφημα εμπιστοσύνης δύνανται να αποτελούν αυτήν την επιτροπή.

Ενώ δεν υπάρχουν συγκεκριμένες ημερομηνίες του χάρτη πορείας, υπάρχει μια περίληψη για το τι σχεδιάζουν να κάνουν οι προγραμματιστές αυτού του δικτύου κρυπτογράφησης. Αυτοί λειτουργούν σε φάσεις.

1. Φάση 1 · Είναι η πρώτη φάση και περιλαμβάνει την ανάπτυξη του εμπλουτισμένου γραφήματος εμπιστοσύνης. Καλύπτει επίσης την πρόσληψη περισσότερων χρηστών για το δίκτυο, ενώ αυξάνει τον αριθμό των εφαρμογών που λαμβάνονται.

2. Φάση 2 - Testnet. Αυτή η φάση εκτελείται αυτήν τη στιγμή μαζί με το στάδιο 1. Όποιος ήδη τρέχει τον κόμβο στον υπολογιστή του εκτελείται ταυτόχρονα και στο Testnet.

3. Φάση 3 - Mainnet. Αφορά στην τελική φάση αυτού του έργου,

Ενώ οι περισσότεροι άνθρωποι εξακολουθούν να είναι δύσπιστοι για αυτό το κρυπτονόμισμα, το επίπεδο εμπειρογνωμοσύνης και προηγμένων χαρακτηριστικών που προσφέρει είναι ο λόγος ο οποίος το καθιστά αξιόπιστο.

Bootstrapping Δίκτυο και Επιδράσεις Μέσω Blockchain Τεχνολογίας και Cryptoeconomics

Τα κρυπτονομίσματα είναι μια πολλά υποσχόμενη προσέγγιση για αποκεντρωμένες ηλεκτρονικές πληρωμές, έξυπνες συμβάσεις και άλλες εφαρμογές. Ωστόσο, η υποστήριξη μεγάλου αριθμού χρηστών και συναλλαγών θα απαιτήσει κρυπτονομίσματα για την αντιμετώπιση δύο κρίσιμων και συναφών σημείων συμφόρησης: αποθήκευσης (πόσα δεδομένα πρέπει να αποθηκεύσει κάθε συμμετέχων) και εκκίνησης (πόσα δεδομένα πρέπει να κατεβάσει κάθε συμμετέχων για να συμμετάσχει στο σύστημα).

Για παράδειγμα, στο Bitcoin, ένας νέος πελάτης που επιθυμεί να συμμετάσχει στο δίκτυο και να επιβεβαιώσει ότι έλαβε τη σωστή απόφαση, πρέπει να πραγματοποιήσει λήψη περίπου 150 GB δεδομένων, από τον Ιανουάριο του 2018. Το κόστος αποθήκευσης και εκκίνησης σχετίζεται, επειδή, σε αποκεντρωμένο σχεδιασμό, οι

κόμβοι πρέπει να αποθηκεύουν αρκετή κατάσταση για να βοηθήσουν τους νέους κόμβους να ενταχθούν στο σύστημα.

Ο σχεδιασμός ενός κρυπτονομίσματος του οποίου το κόστος αποθήκευσης και bootstrapping κλιμακώνεται με τον αριθμό των χρηστών και των συναλλαγών.

Πρώτον, ένα κρυπτονόμισμα πρέπει να αποτρέπει τη διπλή δαπάνη, δηλαδή να εμποδίζει έναν χρήστη να ξοδεύει τα ίδια χρήματα δύο φορές ή να εκδίδει την ίδια συναλλαγή πολλές φορές. Αυτό γίνεται συνήθως παρακολουθώντας προηγούμενες συναλλαγές. Για παράδειγμα, το Bitcoin αποθηκεύει όλες τις προηγούμενες συναλλαγές, οι οποίες δεν κλιμακώνονται καλά (το κόστος αυξάνεται γραμμικά με τον αριθμό των συναλλαγών). Ως άλλο παράδειγμα, το Ethereum δεν αποθηκεύει όλες τις συναλλαγές, αλλά παρακολουθεί τον αριθμό ακολουθίας ("nonce") της τελευταίας συναλλαγής που εκδόθηκε από έναν δεδομένο λογαριασμό[12].Αυτό το nonce πρέπει να αποθηκευτεί ακόμη και αν ο λογαριασμός δεν έχει υπόλοιπο.

Ο στόχος επί παραδείγματι της εταιρείας Vault είναι να μειώσει το κόστος αποθήκευσης και να κάνει bootstrapping σε κρυπτογράφηση. Υπάρχουν δύο σημαντικές πτυχές σε αυτόν τον στόχο, που αντιστοιχούν σε δύο μεγάλες κατηγορίες εργασίας.

Το πρώτο είναι αυτό που ονομάζουμε «πλάτος» του καθολικού: πόσα δεδομένα χρειάζεται κάθε συμμετέχων να αποθηκεύσει για να επικυρώσει τις συναλλαγές (συμπεριλαμβανομένης της ανίχνευσης διπλών δαπανών); Στην περίπτωση του Bitcoin, για παράδειγμα, το "πλάτος" είναι το σύνολο όλων των προηγούμενων μη χρησιμοποιημένων συναλλαγών. Οι τεχνικές που αντιμετωπίζουν το πλάτος ενός καθολικού εστιάζουν στη διαχείριση του σημαντικού κόστους αποθήκευσης της διατήρησης του ιστορικού όλων των συναλλαγών σε κάθε πελάτη.

Το δεύτερο είναι αυτό που αποκαλούμε «μήκος» του καθολικού: πόσα δεδομένα πρέπει να μεταδοθούν σε έναν νέο συμμετέχοντα ως απόδειξη της τρέχουσας κατάστασης του καθολικού; Στην περίπτωση του Bitcoin, η απόδειξη αποτελείται από όλες τις κεφαλίδες μπλοκ που ξεκινούν από το μπλοκ γένεσης, που συνδέονται μεταξύ τους με

[12] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, pp. 1–32, 2014.

κατακερματισμούς στις κεφαλίδες μπλοκ, καθώς και από όλα τα αντίστοιχα περιεχόμενα μπλοκ (για να αποδείξουν ποιες συναλλαγές έχουν ή δεν έχουν ξοδευτεί ακόμη). Οι τεχνικές που αντιμετωπίζουν το μήκος του καθολικού επιτρέπουν συνήθως στους πελάτες να παραλείπουν τις καταχωρήσεις κατά την επαλήθευση των κεφαλίδων μπλοκ, γεγονός που μειώνει το συνολικό κόστος λήψης.

Πολλά κρυπτονομίσματα παρατηρούν ότι το αρχείο καταγραφής συναλλαγών καθίσταται ανέφικτο να αποθηκεύεται και να μεταδίδεται με την πάροδο του χρόνου. Επιδιώκουν να μειώσουν το μέγεθος αυτού του αρχείου καταγραφής, το οποίο μειώνει το μέγεθος του εύρους ζώνης που απαιτείται για τη συμμετοχή στο πρωτόκολλο (ως επαληθευτής) και επίσης το ποσό αποθήκευσης που απαιτείται για την εκτέλεση του πρωτοκόλλου.

Το Ethereum υποστηρίζει τη συνοπτική σύνοψη των ισοζυγίων account και άλλων καταστάσεων σε μια σύντομη πέψη. Σε κάθε μπλοκ, οι συγγραφείς του βιβλίου χρησιμοποιούν το Patricia Merkle Trees για να δεσμευτούν για το τρέχον σύνολο υπολοίπων. Ένα δέντρο Merkle[13] επιτρέπει σε ένα συμβαλλόμενο μέρος να παράγει αποτελεσματικά αποδεικτικά στοιχεία για την ιδιότητα μέλους ενός αντικειμένου σε κάποιο σύνολο. Αυτά τα «σημεία ελέγχου» της Merkle επιτρέπουν σε νέους πελάτες να αποκτήσουν κατάσταση ισορροπίας από οποιονδήποτε μη αξιόπιστο κόμβο και, στη συνέχεια, να επαληθεύσουν γρήγορα αυτήν την κατάσταση έναντι μιας γνωστής ρίζας Merkle. Για να αποτρέψουν έναν εισβολέα από την επανάληψη μιας συναλλαγής που εκδίδεται από έναν χρήστη, οι χρήστες ενσωματώνουν έναν αριθμό ακολουθίας (που ονομάζεται συναλλαγή nonce) σε κάθε συναλλαγή. Οι πελάτες Ethereum πρέπει να παρακολουθούν την τελευταία έκδοση που έχει εκδοθεί από κάθε λογαριασμό στο δέντρο του υπολοίπου, ακόμα και αν ο λογαριασμός είναι κενός (δηλαδή, το υπόλοιπό του είναι 0). Διαφορετικά, μια παλιά συναλλαγή θα μπορούσε να αναπαραχθεί (π.χ., εάν ένας άδειος λογαριασμός λάβει κατάθεση στο μέλλον).

Με λίγα λόγια, το πρωτόκολλο είναι μια γενίκευση του πρωτοκόλλου, το οποίο ενισχύεται με δύο τρόπους: (1) προσπάθειες παικτών, και (2) μια διαδικασία κατάταξης και μια αλυσίδα επικύρωσης προβλέπουν ότι, εκτός από τη βασική λειτουργία της

[13] D. E. Knuth, The art of computer programming. Pearson Education, 1997, vol. 3.

(έλεγχος της εγκυρότητας του περιεχομένου μιας αλυσίδας), επιτρέπεται ο εντοπισμός νέων υποψηφίων ομάδων.

Πριν περιγράψουμε λεπτομερώς το πρωτόκολλο backbone του bootstrapped, επισημαίνουμε τα μοναδικά χαρακτηριστικά του.

Δεν υπάρχει αξιόπιστη εγκατάσταση και εξατομικευμένη εξαγωγή αποκλεισμού. Τα συμβαλλόμενα μέρη ξεκινούν χωρίς προηγούμενο συντονισμό και εισέρχονται σε μια αρχική φάση ανταλλαγής πρόκλησης, όπου θα ανταλλάξουν τυχαίες τιμές που θα χρησιμοποιηθούν για την κατασκευή αποδείξεων για υποψήφια μπλοκ. Τα μέρη θα τρέξουν την αρχική φάση ανταλλαγής πρόκλησης για έναν μικρό αριθμό γύρων και στη συνέχεια θα προσπαθήσουν να εξορύξουν τα δικά τους μπλοκ γένεσης ξεχωριστά. Μόλις εξορύξουν ή αποδεχθούν ένα μπλοκ από το δίκτυο, θα ασχοληθούν με την εξόρυξη περαιτέρω μπλοκ και την ανταλλαγή Blockchains όπως στο πρωτόκολλο Blockchain του Bitcoin. Περιστασιακά μπορεί να στραφούν σε αλυσίδα με διαφορετικό μπλοκ. Ωστόσο, όπως θα δείξουμε, πολύ σύντομα θα σταθεροποιηθούν σε ένα κοινό μόνο μπλοκ.

Η χρονική «φρεσκάδα» των ομάδων επηρεάζει το συνολικό βάρος των αλυσίδων. Οι αλυσίδες που έχουν τις ρίζες τους σε ένα μπλοκ θα ενσωματώσουν το βάρος τους στη συνολική αποτίμησή τους. Το μπλοκ μπορεί να είναι αρκετά βαρύ σε σύγκριση με τα κανονικά μπλοκ. Το βάρος τους γενικά μπορεί να είναι όσο ένας γραμμικός αριθμός κανονικών μπλοκ στην παράμετρο ασφαλείας. Επιπλέον, κάθε κανονικό μπλοκ σε μια αλυσίδα αντιστοιχεί σε 3 μονάδες ως προς το συνολικό βάρος της αλυσίδας, κάτι που, όπως δείχνουμε, θα είναι ζωτικής σημασίας για να ληφθούν υπόψη οι διαφορές όσον αφορά το βάρος που αντιστοιχίζονται στο ίδιο μπλοκ γένεσης από διαφορετικά συμβαλλόμενα μέρη που εκτελούν το πρωτόκολλο

Εξατομικευμένος κανόνας επιλογής αλυσίδας. Δεδομένης της συνύπαρξης πολλαπλών μπλοκ γένεσης, μια διαδικασία κατάταξης ενσωματώνεται στον κανόνα επιλογής αλυσίδας που, εκτός από τη βασική λειτουργία του (έλεγχος της εγκυρότητας του περιεχομένου μιας αλυσίδας) και επιλέγοντας τη μεγαλύτερη αλυσίδα, τώρα λαμβάνει επίσης υπόψη το βαθμό ενός μπλοκ γένεσης από την προοπτική κάθε παίκτη-δρώντα που εκτελεί το πρωτόκολλο.

Η διαδικασία κατάταξης αποδίδει αποτελεσματικά μια βαθμολογημένη λίστα μπλοκ γένεσης και εμπνέεται από το βασικό πρωτόκολλο κατάταξης, όπου χρησιμοποιείται για την παραγωγή βαθμολογημένου PKI.

Το πρωτόκολλο backbone Bitcoin εκτελείται από έναν αυθαίρετο αριθμό συμβαλλομένων μερών σε μη εξουσιοδοτημένο δίκτυο. Για τις ανάγκες συγκεκριμένης υπόθεσης, υποθέτουμε ότι ο αριθμός των μερών που εκτελούν το πρωτόκολλο είναι n. Ωστόσο, τα μέρη δεν χρειάζεται να γνωρίζουν αυτόν τον αριθμό όταν εκτελούν το πρωτόκολλο. Η επικοινωνία μέσω του δικτύου επιτυγχάνεται με τη χρήση μιας λειτουργίας αποστολής σε όλους «Diffuse» που είναι διαθέσιμη σε όλα τα μέρη (και μπορεί να γίνει κατάχρηση από τον αντίπαλο με την έννοια της παράδοσης διαφορετικών μηνυμάτων σε διαφορετικά μέρη). Μετά από μια αρχική φάση (πρόκληση), κάθε μέρος πρέπει να διατηρήσει μια δομή δεδομένων που ονομάζεται Blockchain, όπως ορίζεται παραπάνω. Η αλυσίδα κάθε συμβαλλόμενου μέρους μπορεί να είναι διαφορετική, αλλά, όπως θα αποδείξουμε, υπό ορισμένες σαφώς καθορισμένες συνθήκες, οι αλυσίδες των ειλικρινών κομμάτων θα μοιράζονται ένα μεγάλο κοινό.

Η παραπάνω διαδικασία ονομάζεται Bootstrapping και αποτελεί ασφαλιστική δικλείδα του Blockchain.

Στρατηγικές Μάρκετινγκ και Νέοι Τύποι Ψηφιακών Πλατφορμών – Η περίπτωση των Tokens

Τα κρυπτονομίσματα επαναπροσδιορίζουν το μέλλον της οικονομίας. Το Cryptocurrency είναι ένα ακμάζον οικοσύστημα, που καταπατά ήσυχα την επικράτεια της συμβατικής χρηματοδότησης.

Τα τελευταία πέντε χρόνια, οι χρήστες και οι συναλλαγές Bitcoin έχουν μέσο όρο ρυθμού ανάπτυξης περίπου 60% ετησίως. Ομοίως, ιδιωτικοί και δημόσιοι επενδυτές έχουν εμβαθύνει τη δέσμευσή τους για κρυπτονομίσματα, συμπεριλαμβανομένων των Ethereum, Ripple (XRP) και Stellar - και ορισμένων άλλων σε ολόκληρο τον κλάδο.

Το Bitcoin είναι ένα παγκόσμιο νόμισμα, επομένως το κοινό-στόχος δεν είναι μόνο μία ομάδα ή είδος ατόμου. Όμως, οι κύριοι χρήστες είναι άτομα που εκτιμούν την

ιδιωτικότητα, την παγκοσμιοποίηση και την αποκέντρωση. Ξεκίνησε να είναι δημοφιλής στους χώρους επαναστατών ερευνητών περί το νόμισμα, αλλά έχει επεκταθεί σε ένα διαφορετικό κοινό καθώς όλο και περισσότεροι άνθρωποι ενδιαφέρονται για αυτό και γίνεται ευκολότερο στη χρήση.

Ποιοί είναι οι παίκτες κλειδιά στο τοπίο των Crypto ?

Ιδιωτικοί παίκτες:

1. Θεσμικοί επενδυτές
   Harvard Endowment Fund, Crypto Hedge Funds
2. Ανταλλαγές κρυπτονομισμάτων
   Coinbase, Bitstamp
3. Τράπεζες και Χρηματοοικονομικά
   J.P. Morgan, Fidelity Investments, Swissquote
4. Ισχύς και βοηθητικά προγράμματα
   RWE
5. Τεχνολογία
   IBM, Microsoft

Δημοσιοι παίκτες:

1. Κυβερνήσεις
   Βενεζουέλα
2. Οργανισμοί
   Crypto Valley Association, Global Digital Finance
3. Κεντρικές τράπεζες
   Κίνα, Σουηδία, Σαουδική Αραβία

Παρακάτω ακολουθεί η λίστα των καταναλωτών-στόχων:

1. Καζίνο

2. Επιχειρήσεις

3. Τουρίστες

4. Ρυθμιστές

5. Επενδυτές

6. Έμποροι

7. Ανθρακωρύχοι

8. Φοιτητές πανεπιστημίου

Το δίκτυο Blockchain είναι αποκεντρωμένο. Μια αρχή όπως η κεντρική τράπεζα δεν καθορίζει την παροχή της επαληθευμένης συναλλαγής ενώ το Blockchain δημιουργεί ένα διαφανές και αμετάβλητο ιστορικό σημείων συνάντησης ή συναλλαγών μεταξύ σημείων Α και Β, δεν έχει κόστος συναλλαγής και δεν απαιτεί μεσάζοντα. Εξαλείφει την ανάγκη για τέλη συναλλαγής τρίτων, ούτε την απαίτηση για πλατφόρμα τρίτου μέρους που να ταιριάζει με αγοραστές και πωλητές.

Τι σημαίνουν όλα αυτά όταν εφαρμόζονται στο επιχειρηματικό περιβάλλον; Η τεχνολογία Blockchain θα μπορούσε να αλλάξει δραστικά την υπάρχουσα δομή της αγοράς και τους παίκτες της, καθώς και την οικονομία.

Το Spotify, για παράδειγμα, που λειτουργεί ως μεσάζων μεταξύ καλλιτεχνών και συνδρομητών, θα μπορούσε τελικά να χάσει το μερίδιο αγοράς του εάν οι καλλιτέχνες αποφάσισαν να αποθηκεύσουν τη μουσική τους σε μια υποδομή που βασίζεται σε iCloud Blockchain, χρεώνοντας απευθείας τους συνδρομητές για να ακούσουν τη μουσική τους. Αυτό θα καθιστούσε το επιχειρηματικό μοντέλο της Spotify ξεπερασμένο.

Ομοίως, εταιρείες όπως η Uber που χρησιμοποιούν την πλατφόρμα τους για να ταιριάξουν τους οδηγούς με τους πελάτες θα μπορούσαν να χάσουν το μερίδιο αγοράς τους εάν η επικοινωνία μεταξύ προγραμμάτων οδήγησης και πελατών πραγματοποιούνταν απευθείας μέσω μιας πλατφόρμας Blockchain. Αυτή η τεχνολογία θα μπορούσε επίσης να διαταράξει εταιρείες όπως η Amazon εάν τα καταστήματα, μέσω του μάρκετινγκ, επικοινωνούν απευθείας με τους πελάτες μέσω μιας δωρεάν πλατφόρμας Blockchain για να πουλήσουν τα προϊόντα τους και να αντιληφθούν τις αντίστοιχες χρεώσεις τους. Το OpenBazaar χρησιμοποιεί αυτήν τη στιγμή μια πλατφόρμα Blockchain που επιτρέπει δωρεάν σύνδεση μεταξύ εμπόρων και πελατών.

Αυτό δημιουργεί ένα κίνητρο για τους εμπόρους να προσφέρουν 100% ικανοποίηση στους πελάτες, καθώς η ιστορία του Blockchain είναι αμετάβλητη και μόνιμη.

Οι τράπεζες θα μπορούσαν να εφαρμόσουν αυτήν την τεχνολογία στις προσφορές παράδοσης προϊόντων και υπηρεσιών του πελάτη τους μέσω της εκτέλεσης και του διακανονισμού σημαντικών συναλλαγών (πληρωμές, διακανονισμοί τίτλων, δάνεια κ.λπ.)

Επιτρέπει περαιτέρω τη δημιουργία και τη χρήση έξυπνων συμβάσεων ή συμφωνιών μεταξύ των μερών, που ενεργοποιούνται με κλειδιά πρόσβασης για τη μεταφορά οτιδήποτε αξίας χωρίς τη χρήση διαμεσολαβητή.

Ως αποτέλεσμα, τα τέλη συναλλαγών θα μπορούσαν να εξαλειφθούν μειώνοντας έτσι τα έσοδα και τα κέρδη των τραπεζών.

Η SIX (Ελβετικό Χρηματιστήριο) ανακοίνωσε πρόσφατα σχέδια για τη μεταφορά των μετοχών σε ένα σύστημα Blockchain. Ο διευθύνων σύμβουλος της SIX Jos Dijsselhoff δηλώνει ότι «*το μεγαλύτερο πλεονέκτημα μιας τέτοιας λύσης θα είναι το κέρδος στο χρόνο. Το πραγματικό εμπόριο ενός αποθέματος σήμερα διαρκεί λιγότερο από ένα δευτερόλεπτο. Αλλά η πραγματική διευθέτηση στο back office μπορεί να διαρκέσει έως και δύο ημέρες για να ολοκληρωθεί* ».

Αυτό θα μπορούσε ενδεχομένως να εξαλείψει τα υψηλότερα χρονοδιαγράμματα χρεώσεων της τράπεζας στο εμπόριο μετοχών, καθώς οι αγοραστές και οι πωλητές θα ταιριάζουν απευθείας μέσω της πλατφόρμας SIX blockchain, με αποτέλεσμα η τράπεζα να λειτουργεί μόνο ως θεματοφύλακας για το απόθεμα.

Το Blockchain μπορεί να μειώσει το κόστος και να εξοικονομήσει χρόνο και ενέργεια όταν εφαρμόζεται σε καθημερινές τράπεζες καθημερινές εργασίες και συναλλαγές. Για παράδειγμα, τα ίδια τραπεζικά τμήματα που εργάζονται για τον διακανονισμό μεταβιβάσεων κινητών αξιών θα μπορούσαν να συντονιστούν και να συναντηθούν εξ αποστάσεως σε μια κοινή κρυπτογραφημένη πλατφόρμα με δυνατότητες ροής βίντεο και να ανταλλάσσουν δεδομένα ενώ προβάλλουν και εργάζονται στο ίδιο έργο ή λογαριασμό πελάτη, εξαλείφοντας ταυτόχρονα την ανάγκη ανταλλαγής email, γραφικών, και εσωτερικό ταχυδρομείο. Ομοίως, δύο διαφορετικές τράπεζες με δύο ξεχωριστά φυσικά γραφεία μπορούν να συναντηθούν στην ίδια πλατφόρμα, να εκτελούν πανομοιότυπες εργασίες και να επιτρέψουν την ολοκλήρωση του έργου.

Το Blockchain προσφέρει λύσεις με τη δυνατότητα να διαταράξει τα υπάρχοντα πρωτόκολλα και τις διαδικασίες που χρησιμοποιούνται στις τραπεζικές συναλλαγές σήμερα, όπως το SWIFT, ένα ρυθμιζόμενο παγκοσμίως που χρησιμοποιείται από χρηματοοικονομικές οντότητες για δεκαετίες, πλατφόρμα.

Ενώ η τεχνολογία Blockchain βρίσκεται στα πρώτα στάδια ανάπτυξης, εφαρμογής και ρύθμισης, το SWIFT παρέχει εγγύηση ασφάλειας και αξιοπιστίας παρά το γεγονός ότι είναι πιο αργό και λιγότερο τεχνολογικά προηγμένο σε σύγκριση με τις πλατφόρμες Blockchain.

Η SWIFT προσαρμόστηκε πρόσφατα στις ψηφιακές απαιτήσεις της εποχής δημιουργώντας μια πλατφόρμα Corporate Global Know Your Customer ή το KYC Registry, ένα βασικό βήμα για τον εξορθολογισμό των τραπεζικών πληρωμών μέσω ανταποκριτών-όπου τα μέλη της πλατφόρμας της τράπεζας μπορούν να ανεβάσουν τα αντίστοιχα KYC του πελάτη τους και να τα μοιραστούν με τις αντίστοιχες τράπεζες, μείωση του χρόνου επεξεργασίας και επιτάχυνση των πληρωμών - ένα καινοτόμο βήμα κλειδί για τη διασφάλιση της επιβίωσής του.

Ο πολλαπλασιασμός εξελιγμένων πλατφορμών ηλεκτρονικού εμπορίου σε συνδυασμό με εφαρμογές για κινητές συσκευές προκάλεσε την ανάπτυξη του εμπορίου από επιχείρηση σε καταναλωτή (B2C), αναδιαμόρφωσε τις οργανωτικές δομές και ανανέωσε τις διαδικασίες δημιουργίας αξίας.

Ταυτόχρονα, οι νέες τεχνολογίες έχουν αλλάξει τη δυναμική του μάρκετινγκ μάρκας, επιτρέποντας μια ευρύτερη προσέγγιση και πιο εξατομικευμένη στόχευση με στόχο την αύξηση της εμπιστοσύνης της μάρκας και την ενίσχυση της αφοσίωσης των πελατών. Σήμερα, το Διαδίκτυο επιτρέπει στους εμπόρους να διεισδύσουν βαθύτερα στις υπάρχουσες αγορές τους, να δημιουργήσουν νέες διαδικτυακές αγορές και να δημιουργήσουν νέα ζήτηση. Αυτή η δυναμική δέσμευση στην αγορά χρησιμοποιεί νέες τεχνολογίες για την αποτελεσματικότερη στόχευση των καταναλωτών Σε αυτό το εννοιολογικό κεφάλαιο, συζητείται πώς η τεχνολογία Blockchain μπορεί δυνητικά να επηρεάσει τις δραστηριότητες μάρκετινγκ μιας εταιρείας. Πιο συγκεκριμένα, απεικονίζεται πώς η τεχνολογία Blockchain δρα ως σταδιακή καινοτομία, ενισχύοντας το καταναλωτικό-κεντρικό παράδειγμα. Επιπλέον, η τεχνολογία Blockchain προάγει τη διαμεσολάβηση, βοηθά στην καταπολέμηση της απάτης, ενισχύει την εμπιστοσύνη και τη διαφάνεια, επιτρέπει την ενισχυμένη προστασία της ιδιωτικής ζωής, ενισχύει

την ασφάλεια και επιτρέπει δημιουργικά προγράμματα αφοσίωσης. Παρουσιάζονται επίσης προτάσεις που θα καθοδηγήσουν τη μελλοντική έρευνα που σχετίζεται με το Blockchain στον τομέα του μάρκετινγκ.

Το πελατοκεντρικό μάρκετινγκ είναι ζωτικής σημασίας για εταιρείες που θέλουν να επιβιώσουν σε έντονα αμφισβητούμενα περιβάλλοντα B2C (Sheth et al., 2000). Το μάρκετινγκ βοηθά τις εταιρείες να κατανοήσουν και να εξηγήσουν την αξία που ένας καταναλωτής αντιλαμβάνεται και προέρχεται από ένα προϊόν ή μια υπηρεσία (Larivière et al., 2013). Οι μέθοδοι επικοινωνίας που επιλέγει μια εταιρεία ενδέχεται να διαφέρουν από τη μία βιομηχανία στην άλλη. Ωστόσο, οι θεμελιώδεις στόχοι και προκλήσεις που σχετίζονται με τη δέσμευση των καταναλωτών παραμένουν οι ίδιοι. Ο πολλαπλασιασμός των νέων τεχνολογιών έχει συχνά αποτέλεσμα ένα πλαίσιο εκδημοκρατισμού για εταιρείες και καταναλωτές, υπερβαίνοντας την εμβέλεια και το μέγεθος της εταιρείας και καθιστώντας τις νέες τεχνολογίες πιο προσιτές σε μικρότερες εταιρείες. Παρά τις αβέβαιες οικονομικές αποδόσεις, οι μικρές επιχειρήσεις επενδύουν τώρα σε τεχνολογίες και πλατφόρμες βάσει αμοιβών που θεωρούν απαραίτητες για τη διατήρηση μιας ανταγωνιστικής θέσης στις αγορές τους (Rishel and Burns, 1997). Δεδομένης αυτής της τάσης, η εμφάνιση της «Mar-tech» ως συνδυασμού λύσεων αυτοματισμού και τεχνολογίας μάρκετινγκ επηρέασε θετικά τον τρόπο με τον οποίο οι εταιρείες προσεγγίζουν και αλληλεπιδρούν με τους πελάτες τους (Cvitanović, 2018). Όχι μόνο αναδιαμορφώνουν το modus operandi για μια προσέγγιση της εταιρείας, αλλά αλλάζουν και αυξάνουν τις προσδοκίες των πελατών, αλλάζοντας έτσι τη δυναμική των σχέσεων με τους πελάτες (Treiblmaier και Strebinger, 2008).

Στη νέα οικονομία, οι επωνυμίες δεν εστιάζουν πλέον αποκλειστικά στην εκτέλεση μιας καμπάνιας μετά την άλλη. Αντ 'αυτού, αξιοποιούν νέες μορφές δέσμευσης και διαλόγου των καταναλωτών για να επεκτείνουν την κάλυψη της αγοράς τους και να επιβάλουν μια πιο συνεργατική και συντονισμένη στρατηγική επικοινωνίας μάρκετινγκ (Santomier, 2008). Οι εταιρείες σήμερα χτίζουν ένα χαρτοφυλάκιο τεχνολογιών και εκμεταλλεύονται διάφορα κανάλια μέσων και μεθόδους δημοσιότητας για να τοποθετήσουν τις μάρκες τους, καθώς και να πουλήσουν τα προϊόντα, τις υπηρεσίες και τις ιδέες τους (McAllister και Turow, 2002). Το ψηφιακό μάρκετινγκ αξιοποιεί νέα κανάλια σε όλα τα μέσα κοινωνικής δικτύωσης που παρέχουν στις εταιρείες νέες, καινοτόμες, οικονομικά αποδοτικές και σημαντικές δυνατότητες για να αλληλεπιδράσουν με τους πελάτες (Melewar et al., 2017). Με τη σειρά τους, οι πελάτες

γίνονται αναπόσπαστο μέρος του εξελισσόμενου διαλόγου εμπλοκής στη διαδικασία και ενισχύουν την επιρροή τους στη διαδικασία μάρκετινγκ (Berman και McClellan, 2002).

Η ανάπτυξη του Διαδικτύου, μαζί με τις αναδυόμενες τεχνολογίες, έχει επηρεάσει σημαντικά τον παραδοσιακό συνδυασμό μάρκετινγκ (δηλαδή, προϊόν, τιμή, μέρος και προώθηση). Για παράδειγμα, οι προηγμένες τεχνολογίες που συχνά αναφέρονται ως μεγάλα αναλυτικά δεδομένα έχουν επιτρέψει στις εταιρείες να συγκεντρώσουν μεγάλα και περίπλοκα σύνολα δεδομένων και να χρησιμοποιήσουν εξελιγμένα αναλυτικά στοιχεία για να αποκτήσουν πρόσθετες γνώσεις καταναλωτών (Stone and Woodcock, 2014). Ομοίως, οι λιανοπωλητές και οι διαδικτυακές επιχειρήσεις επενδύουν όλο και περισσότερο στα μέσα κοινωνικής δικτύωσης ως μέρος των πρακτικών επικοινωνίας μάρκετινγκ και προσπαθούν να ξεπεράσουν τους ανταγωνιστές τους (Vend, 2018).

Από αυτή την άποψη, η DeMers (2016) προέβλεψε ότι η τάση προς τις αγορές στον κυβερνοχώρο είναι πιθανό να ενταθεί λόγω της αυξημένης μελλοντικής τάσης των καταναλωτών να συμμετάσχουν σε διαδικτυακές αγορές. Κατά συνέπεια, περισσότεροι άνθρωποι στις Ηνωμένες Πολιτείες προτιμούν να κάνουν τις αγορές τους στο διαδίκτυο παρά να κάνουν αγορές σε φυσικά καταστήματα (Marketo, 2017).

Οι σύγχρονες τεχνολογίες θέτουν τους καταναλωτές στην πρώτη γραμμή διαλόγου περί τα θέματα της ασφάλειας, της ιδιωτικής ζωής, της εμπιστοσύνης και της μετάβασης στις νέες προκλήσεις. Ο Prabhaker (2000) υποστηρίζει ότι κάθε φορά που τα άτομα συμμετέχουν σε μια διαδικτυακή συναλλαγή, αφήνουν πίσω τους ένα ψηφιακό ίχνος λεπτομερών πληροφοριών σχετικά με την ταυτότητά τους, τις προτιμήσεις αγορών τους, τις συνήθειες δαπανών, τα στοιχεία της πιστωτικής κάρτας και άλλες προσωπικά αναγνωρίσιμες πληροφορίες (δηλ., δεδομένα που μπορούν να χρησιμοποιηθούν για την ταυτοποίηση ενός συγκεκριμένου ατόμου). Από πλευράς απορρήτου, αυτή η κατάσταση επιδεινώθηκε με την πάροδο των ετών καθώς οι πρακτικές συλλογής δεδομένων έχουν γίνει πιο ευέλικτες και πανταχού παρούσες. Οι διαδικτυακές επιχειρήσεις συχνά δεν πληρούν τις κανονιστικές απαιτήσεις και οι διαρροές απορρήτου είναι συχνές και έχουν μόνιμο αντίκτυπο στην εμπιστοσύνη των καταναλωτών (Ingram et al., 2018; Martin, 2018; Bodoni, 2019).

Ως αποτέλεσμα, η ευαισθητοποίηση των καταναλωτών αυξάνεται, οι υποψίες τους αυξάνονται και είναι πιο συνετές για τις διαδικτυακές συναλλαγές, καθώς το PII τους

μπορεί να χρησιμοποιηθεί ή να πωληθεί για χρηματικό κέρδος χωρίς την άδειά τους (Norman et al., 2016). Η αποφυγή διαδικτυακών αγορών δεν αποτελεί λύση, καθώς οι λιανοπωλητές σε φυσικά καταστήματα ενθαρρύνουν επίσης τη χρήση καρτών επιβράβευσης και διατηρούν μια κεντρική βάση δεδομένων που μπορεί να είναι ευάλωτη σε εισβολή ή κατάχρηση. Επιπλέον, πολλές αναπτυσσόμενες χώρες δεν διαθέτουν κανονισμούς απορρήτου για την προστασία των καταναλωτών PII. Επομένως, οι επωνυμίες πρέπει να ενημερώνονται για τους τελευταίους κανονισμούς απορρήτου, να κατανοούν τις προσδοκίες των καταναλωτών και να ενημερώνονται για την τεχνολογική καινοτομία και τις βέλτιστες πρακτικές. Οι υποστηρικτές για ενισχυμένη προστασία της ιδιωτικής ζωής των καταναλωτών προτείνουν ότι τα συστήματα θα πρέπει να δημιουργηθούν με ένα πλαίσιο «απόρρητο κατά σχεδιασμό» (Cavoukian, 2011).

Η πρόσφατη διαφημιστική εκστρατεία γύρω από την τεχνολογία Blockchain οδήγησε σε πολλά υποσχόμενες περιπτώσεις χρήσης σε τομείς όπως χρηματοδότηση, διαχείριση αλυσίδας εφοδιασμού, υγειονομική περίθαλψη, τουρισμός, ακίνητα. Το πεδίο μάρκετινγκ δεν δύναται να αποτελεί εξαίρεση.

Αρχικά ξεκίνησε για τη στήριξη του Bitcoin κρυπτογράφησης, το κύριο χαρακτηριστικό της τεχνολογίας Blockchain είναι η επικοινωνία, εξαλείφοντας την ανάγκη κεντρικών τρίτων για τον έλεγχο της ροής των συναλλαγών (Yli-Huumo et al., 2016). Ο Treiblmaier (2018, σελ. 547) ορίζει το Blockchain ως "ψηφιακό, αποκεντρωμένο και κατανεμημένο καθολικό σύστημα στο οποίο οι συναλλαγές καταγράφονται και προστίθενται με χρονολογική σειρά με στόχο τη δημιουργία μόνιμων αρχείων." Μια συγκεκριμένη διαμόρφωση Blockchain είναι συνήθως ένας συνδυασμός πολλαπλών τεχνολογιών, εργαλείων και μεθόδων που αντιμετωπίζουν ένα συγκεκριμένο πρόβλημα ή μια περίπτωση επιχειρηματικής χρήσης (Rejeb et al., 2018). Έτσι, οι διαχειριστές μάρκετινγκ πρέπει να κατανοήσουν τις δυνατότητες της τεχνολογίας Blockchain ως πρωτόκολλο επικοινωνίας που σηματοδοτεί τη μετάβαση από το Διαδίκτυο των πληροφοριών στο Διαδίκτυο της αξίας και της εμπιστοσύνης (Twesige, 2015; Zamani and Giaglis, 2018).

Οι αγορές κρυπτονομισμάτων είναι ένα φαινόμενο. Κατά τη διάρκεια του έτους 2017, το Bitcoin έφτασε σε μια συνολική κεφαλαιοποίηση αγοράς άνω των 300 δισεκατομμυρίων δολαρίων - δίπλα σε περισσότερα από χίλια μικρότερα

κρυπτονομίσματα με λιγότερο σημαντική κεφαλαιοποίηση (coinmarketcap.com 2018). Παρά αυτά τα ύψη, η αγορά παρέμεινε αρκετά ανεξέλεγκτη από κυβερνητικά ιδρύματα (Dyhrberg 2016). Υποθέτουμε ότι αυτό το μοναδικό περιβάλλον πρώιμου σταδίου μπορεί να εμφανίζει αναποτελεσματικές τιμές που μπορούν δυνητικά να εντοπιστούν και να αξιοποιηθούν από στατιστικές στρατηγικές arbitrage. Μέχρι στιγμής, λίγες μόνο ακαδημαϊκές μελέτες έχουν αγγίξει αυτό το ζήτημα και οι περισσότερες από αυτές επικεντρώνονται μόνο σε μερικά επιλεγμένα κρυπτονομίσματα.

Ένα από τα πρώτα έργα που αντιμετωπίζουν αυτήν την ερώτηση είναι οι Shah και Zhang (2014). Συγκεκριμένα, οι συγγραφείς στοχεύουν στην πρόβλεψη αλλαγών τιμών του Bitcoin κατά τη διάρκεια μιας περιόδου έξι μηνών το 2014 με ένα μοντέλο παλινδρόμησης Bayesian. Τα αποτελέσματα είναι εκπληκτικά, με απόδοση 89% και αναλογία Sharpe 4,10 για περίοδο μόλις 50 ημερών διαπραγμάτευσης. Ωστόσο, δεν λαμβάνονται υπόψη έξοδα συναλλαγής, υποτίθεται η τέλεια ρευστότητα και λαμβάνεται υπόψη μόνο ένα κρυπτονόμισμα.

Χρησιμοποιώντας μερικές από τις ιδέες που πρότειναν οι Shah και Zhang (2014), οι Madan et al. (2015) ανέπτυξαν διάφορα μοντέλα ταξινόμησης για να προβλέψουν το σημείο των αλλαγών τιμών του Bitcoin, αξιοποιώντας πληροφορίες σχετικά με τις τιμές, τον όγκο συναλλαγών και τα δεδομένα σχετικά με το υποκείμενο Blockchain. Ένα διωνυμικό γενικευμένο γραμμικό μοντέλο απέδωσε εξαιρετικά καλά με 98,7% και 95,0% ακρίβεια για το ημερήσιο σύμβολο, αντίστοιχα.

Οι ακαδημαϊκές μελέτες για εφαρμογές Blockchain για την υποστήριξη δραστηριοτήτων μάρκετινγκ είναι σπάνιες. Παρόλα αυτά, στη βιβλιογραφία που βασίζεται σε επαγγελματίες, τα οφέλη του Blockchain θεωρούνται αδιαμφισβήτητα (Ghose, 2018). Σε αυτό το κείμενο, τίθενται τα θεμέλια για μελλοντικές ακαδημαϊκές μελέτες εντοπίζοντας αρκετούς σημαντικούς ερευνητικούς τομείς.

Πρώτα απ 'όλα, η τεχνολογία Blockchain βασίζεται στην επικοινωνία peer-to-peer, η οποία μεταβάλλει τις δομές της αγοράς προωθώντας την αποδιαμεσολάβηση, δηλαδή την απομάκρυνση διαμεσολαβητών που επεξεργάζονται και φιλτράρουν ροές δεδομένων και προσθέτουν κόστος. Δημιουργώντας αμετάβλητα και κοινόχρηστα αρχεία δεδομένων, η τεχνολογία Blockchain μπορεί επίσης να βοηθήσει στη βελτίωση της ποιότητας των δεδομένων και στη διευκόλυνση της πρόσβασης στα δεδομένα. Από την πλευρά των καταναλωτών, η τεχνολογία Blockchain έχει τη δυνατότητα να

μεταμορφώσει ουσιαστικά τις σχέσεις των καταναλωτών με την ενίσχυση της διαφάνειας δεδομένων και πληροφοριών και τη βελτίωση της ιδιωτικής ζωής και της ασφάλειας. Επιτρέπει επίσης καινοτόμες μορφές προγραμμάτων αφοσίωσης των καταναλωτών που θα μπορούσαν να βοηθήσουν στη δημιουργία πρόσθετης αξίας.

Καθοριστικό ρόλο στην προστασία των προσωπικών δεδομένων μπορούν να παίξουν τα Tokens. Ως token μπορεί να οριστεί ένα digital asset και ουσιαστικά είναι ένα κλειδί που πιστοποιεί με μονοσήμαντο τρόπο ότι το πρόσωπο που το κατέχει ειναι ιδιοκτήτης μίας αξίας. Τα tokens μπορούν να αντιστοιχούν σε φυσικά assets τα οποία μπορεί να τα χρησιμοποιήσει ή να τα καταναλώσει ο ιδιοκτήτης του έναντι κάποιου προϊόντος, υπηρεσίας ή πλατφόρμας. Ένα token μπορεί να αναπαρασταθεί μέσα σε ένα Blockchain και να είναι διαθέσιμο μέσω ενός marketplace. Αυτή η διαδικασία προβλέπει αρχικά την αγορά tokens με fiat currency ή με συμβατό κρυπτονόμισμα. Τα tokens είναι κατά βάση διαθέσιμα σε μια κατανεμημένη βάση δεδομένων τύπου Blockchain ώστε να διέπονται από τη διαφάνεια και την πιστοποίηση των συναλλαγών. Σε όλα αυτά ακολουθούνται πρότυπα ώστε να έχουν χαρακτηριστικά ανταλλαξιμότητας. Ένα τέτοιο πρότυπο και το πιο διαδεδομένο είναι το ERC 20 της πλατφόρμας Ethereum. Θα έλεγε κανείς ότι η μετατροπή ενός digital asset σε token μοιάζει με τη διαδικασία έκδοσης ενός χρεογράφου με τεχνολογική βέβαια διαφοροποίηση.

Η χρήση των tokens μπορεί να μετασχηματίσει τους παραδοσιακούς κλάδους της οικονομίας:

- Μετατροπή παραδοσιακών αγαθών σε ρευστοποιήσιμα, ανταλλάξιμα και εμπορεύσιμα αγαθά.
- Διαφάνεια στις συναλλαγές - Λογοδοσία.
- Ταχύτητα – Ελαχιστοποίηση της γραφειοκρατίας.
- Τα δυνατά brands θα έχουν τη δυνατότητα να κάνουν πραγματικά συμμέτοχους τους καταναλωτές και να ενισχύσουν τις επιχειρηματικές διαδικασίες λαμβάνοντας χρηματοδότηση.
- Οι start ups ή και οι εδραιωμένες εταιρείες μπορούν να χρηματοδοτήσουν ένα επιχειρηματικό σχέδιο με δυναμικό τρόπο.

Μεταφερόμαστε σταδιακά από τις πλατφόρμες διαμεσολάβησης και τα κεντρικοποιημένα marketplaces σε αποκεντρωμένα δίκτυα ανταλλαγής αξίας που βασίζονται σε ψηφιακές αναπαραστάσεις αγαθών σε μορφή ειδικών κλειδιών (tokens) και της τεχνολογίας Blockchain.

Η αλλαγή ή η δημιουργία νέν μοντέλων τιτλοποίησης (securititation) στη νέα εποχή Blockchain (tokenization) μπορεί να επιφέρει τα παρακάτω:

1. Επιχειρηματικά οφέλη για τους ιδιοκτήτες αξιών σε μορφή tokens (Asset token issuers)
2. Δυνατότητα ευρύτερης συμμετοχής από διεθνές κοινό επενδυτών και με λιγότερα εμπόδια.
3. Δημιουργία δευτερών αγορών για αγαθά που δεν είναι εμπορεύσιμα (asset backed tokens).
4. Αποτελεσματική διαχείριση πόρων ενεργητικού με μηχανισμούς διαφάνειας και εμπιστοσύνης.

Όλα τα παραπάνω καθώς και ένα σχέδιο μετάβασης στην «οικονομία των tokens» ενέχει θεσμικές, νομικές, επιχειρησιακές και τεχνολογικές προκλήσεις για τη σωστή χρήση των tokens καθώς και την προετοιμασίου του εδάφους σε διάφορους τομείς.

Ενδεικτικά:

- Ανάπτυξη μηχανισμών διακυβέρνησης κατανεμημένης ιδιοκτησίας ενός αγαθού, ώστε αυτό να είναι εμπορεύσιμο με τη μορφή tokens (fractional ownership)
- Αναγνώριση αι συμβατότητα με το θεσμικό πλαίσιο των ηλεκτρονικών συναλλαγών και διαδικασιών. Δημιουργία εταιρειών επενδυτικών υπηρεσιών που θα παρέχουν υπηρεσίες tokenization.
- Συνεργασία και διαβούλευση με ρυθμιστικούς και ελεγκτικούς φορείς με σκοπό την αξιοποίηση των νέων ευκαιριών που αναδεικνύονται με οικονομικό και κοινωνικό όφελος.

Τεχνητή Νοημοσύνη και Ιδιωτικότητα- Οι σχέσεις τους με την Τεχνολογία Blockchain

Ένα υποδειγματικό παράδειγμα για το πώς ένα σύστημα τεχνητής νοημοσύνης μπορεί να είναι ένα μεταιχμιακό τεχνολογικό πρότυπο μέσω της χρήσης του Blockchain προέρχεται απευθείας από τον κόσμο της ακαδημαϊκής έρευνας. Οι επιστήμονες δεδομένων αγωνίζονται εδώ και πολύ καιρό να διατηρήσουν την ποιότητα ενός συνόλου δεδομένων για μηχανική μάθηση από μια οντότητα Artificial Inteligence.

Τα σύνολα δεδομένων μπορεί να είναι πολύ ακριβά για την αγορά, καθώς, ανάλογα με την σωστή επιλογή των στοιχείων και την ομοιογένεια των δεδομένων που περιέχονται μέσα, η κατασκευή και η διατήρηση της ακεραιότητας ενός συνόλου δεδομένων είναι δύσκολη. Το Blockchain ως ένα εξαιρετικά ασφαλές μέσο αποθήκευσης παρουσιάζει ένα τεχνολογικό άλμα στη διατήρηση της ακεραιότητας των δεδομένων. Επιπλέον, το αμετάβλητο του Blockchain δημιουργεί ένα γόνιμο περιβάλλον για τη δημιουργία υψηλής ποιότητας, μόνιμων και αναπτυσσόμενων συνόλων δεδομένων για βαθιά μάθηση. Ο συνδυασμός τεχνητής νοημοσύνης και Blockchain θα μπορούσε να επηρεάσει πεδία όπως το Internet of Things (IoT), την ταυτότητα, τις χρηματοπιστωτικές αγορές, την πολιτική διακυβέρνηση, τις έξυπνες πόλεις, τις μικρές κοινότητες, τις αλυσίδες εφοδιασμού, την εξατομικευμένη ιατρική και άλλους τομείς και, ως εκ τούτου, να προσφέρει οφέλη σε πολλούς ανθρώπους.

Το Blockchain ως σύστημα δεδομένων και πλαισίων παρουσιάζει ορισμένα πλεονεκτήματα μέσω του Διαδικτύου. Μέσω δύο παραδειγμάτων - προκλήσεων στον κόσμο της τεχνητής νοημοσύνης, παρουσιάζεται πώς το Blockchain μπορεί να τα αντιμετωπίσει με νέους τρόπους.

Μία από τις μεγαλύτερες προκλήσεις στην επιστήμη των δεδομένων σήμερα είναι η συλλογή ενός κατάλληλου συνόλου δεδομένων, το οποίο μπορεί να χρησιμοποιηθεί για την εκπαίδευση ενός νευρωνικού δικτύου. Ο πλουραλισμός των δεδομένων μέσω του Διαδικτύου είναι τεράστιος, αλλά η ποιότητα είναι ελάχιστη λόγω της συνήθειας των ανθρώπων να δημοσιεύουν ανακριβή πράγματα, κυρίως επειδή δεν υπάρχει έλεγχος. Χαρακτηριστικό παράδειγμα είναι η έκρηξη των «ψεύτικων ειδήσεων» (fake news) τα τελευταία χρόνια, η οποία τείνει να διαδίδεται ταχύτερα από τα τεκμηριωμένα και επαληθευμένα νέα. Οι γίγαντες του Διαδικτύου όπως το Facebook και το Google έχουν προσπαθήσει να αντιμετωπίσουν το πρόβλημα μέσω αρκετών υπολογιστικών

μεθόδων, αλλά παρόλο που φαίνεται να υπάρχει επαρκής θεωρητική βάση για το διαχωρισμό του «σήματος» από το «θόρυβο» , το πρόβλημα εξακολουθεί να ευδοκιμεί έως σήμερα.

Μια δεύτερη πρόκληση είναι η εχθρική παρέμβαση απέναντι στην επεξεργασία. Το αυτόματο πιλοτικό πρόγραμμα του Tesla αποδείχθηκε ότι είναι ευάλωτο σε επιθέσεις απομακρυσμένων δικαιωμάτων root που θα μπορούσαν να ελέγξουν το σύστημα διεύθυνσης και να διαταράξουν τη λειτουργία "autowipers".Τα Blockchains μπορούν να αντιμετωπίσουν αυτά τα ζητήματα με έναν ολοκληρωμένο τρόπο μέσω της ακεραιότητας, της ασφάλειας, της τριπλής εισόδου και του ελέγχου της προέλευσης.

Επίσης οι κρυπτογραφικές εφευρέσεις ψηφιακών υπογραφών και κατακερματισμών έχουν οδηγήσει σε μια γενική τεχνική με σκοπό να καταστούν τα δεδομένα αξιόπιστα στο πλαίσιο και τους περιορισμούς των τεχνικών μέσων, ένα χαρακτηριστικό που ονομάζεται ακεραιότητα. Στην πράξη, αυτό σημαίνει ότι μπορούμε να δηλώσουμε με (κρυπτογραφική) βεβαιότητα ότι ένα κομμάτι δεδομένων υπήρχε εδώ και μια συγκεκριμένη ώρα και ότι παραμένει ανεμπόδιστο ως προς τη λειτουργία του. Αυτές οι κρυπτογραφικές τεχνικές χρειάζονται κάποιο λογισμικό για να αποφέρουν αποτελέσματα. Η χρονική σήμανση περιλαμβάνει τη λήψη του κατακερματισμού ενός εγγράφου και την τοποθέτησή του σε μια χρονομετρημένη ακολουθία κατακερματισμού που διατηρείται ζωντανή ουσιαστικά χωρίς περιορισμό χρόνου. Ο κατακερματισμός κάθε νέου εγγράφου τοποθετείται σε ένα μπλοκ, το οποίο στη συνέχεια κατακερματίζεται, μαζί με ένα κατακερματισμό του τελευταίου μπλοκ. Δεδομένου ότι ο κρυπτογραφικός κατακερματισμός είναι ουσιαστικά ασήμαντος χωρίς το πραγματικό μπλοκ, αυτό διασφαλίζει τόσο τη συμπερίληψη των νέων εγγράφων όσο και την απόδειξη ότι το τελευταίο μπλοκ, και με επαγωγή όλων των προηγούμενων μπλοκ και των συμπεριλαμβανόμενων εγγράφων, σφραγίζεται με ασφάλεια τη δεδομένη χρονική στιγμή. Η αξιοπιστία της σφραγίδας του χρόνου είναι η αξιοπιστία της καταγραφής του χρόνου σε κάθε μπλοκ και του χώρου μεταξύ των μπλοκ.

Η ψηφιακή υπογραφή παίρνει την απόδειξη ενός κατακερματισμού ένα βήμα παραπέρα δείχνοντας ποιος ήταν αυτός που έκανε αυτή τη σφραγίδα. Οι ψηφιακές υπογραφές γίνονται από ένα ιδιωτικό κλειδί και επαληθεύονται από ένα δημόσιο κλειδί, το οποίο έχει επίσης τη μορφή αναγνωριστικού για το ιδιωτικό κλειδί που ονομάζεται ψευδώνυμο. Αυτό το μοντέλο ασφαλείας είναι απαραίτητο για ένα

Blockchain, καθώς διασφαλίζει ότι μόνο ο κατάλληλος ψευδώνυμος πράκτορας, ως κάτοχος του ιδιωτικού κλειδιού, μπορεί να κάνει νέες συναλλαγές. Το χρήμα είναι ίσως η πιο σκληρή απάντηση της ανθρωπότητας μετά από τους πολέμους, και ως εκ τούτου μπορεί να επιβιώσει μόνο εάν προστατεύεται από ισχυρή ασφάλεια. Το κρυπτογραφικό μοντέλο ασφάλειας της ψευδώνυμης ψηφιακής υπογραφής που χρησιμοποιείται σε Blockchains είναι ανθεκτικό και είναι διαθέσιμο δωρεάν για όλες τις άλλες εφαρμογές πέρα από τις μεταφορές αξίας. Αυτό δεν είναι ασήμαντο όφελος, καθώς το Διαδίκτυο έχει αρκετά κακόφημα μοντέλα ασφαλείας, και οι μεγάλες εφαρμογές Διαδικτύου, όπως οι διαδικτυακές τραπεζικές συναλλαγές και τα αυτόνομα οχήματα, έχουν γενικά προβλήματα στην ανάπτυξη ισχυρής ασφάλειας στους χρήστες. Η έγχυση πληροφοριών από άγνωστες πηγές είναι ανεξέλεγκτη και η απλή προσθήκη σφραγίδων δεδομένων και υπογραφής όπως χρησιμοποιείται στο Blockchain καθιστά τη δουλειά του εισβολέα πιο δύσκολη.

Μια τεχνική γνωστή ως λογιστική τριπλής καταχώρησης προσθέτει ένα επιπλέον πλεονέκτημα που αποτυπώνεται από τον αφορισμό «*Ξέρω ότι αυτό που βλέπετε είναι αυτό που βλέπω*». Η τριπλή καταχώριση λαμβάνει τις παραπάνω τεχνικές ακεραιότητας και δημιουργεί αρχεία όπως παραγγελίες και αποδοχές, πληρωμές, αποδείξεις και τιμολόγια, τόσο κοινόχρηστα όσο και αξιόπιστα το ίδιο σε όλα τα σχετικά μέρη, γεγονός που επιτρέπει στο λογισμικό να λειτουργεί με αξιόπιστα ανεπεξέργαστα δεδομένα ως γεγονότα που παράγονται από άλλα μέρη. η λογιστική τριπλής καταχώρησης κάνει για τους εμπορικούς ομίλους τι έκανε η λογιστική διπλής εισόδου για την εταιρεία.

Αυτό που απομένει είναι η προέλευση των δεδομένων κατά τη δημοσίευση. Το Blockchain υποστηρίζει ένα απαιτητικό έλεγχο. Πρώτον, εάν τα δεδομένα είναι μια χρηματοοικονομική συναλλαγή σε ένα Blockchain, σε ένα περιουσιακό στοιχείο που διαμεσολαβείται από το Blockchain, τότε το αρχείο συναλλαγών μπορεί να υποστηρίξει τη δική του προέλευση. Δεύτερον, η χρήση των ψευδώνυμων ψηφιακών υπογραφών παρέχει μια ελάχιστη μορφή συστήματος ταυτότητας.

Εν κατακλείδι ένα Blockchain σχηματίζει μια νέα μέθοδο για την αποθήκευση πληροφοριών σε δημόσιο χώρο, μέσω μιας διαδικασίας πληρωμής. Εκτός από τις στατικές πληροφορίες, θα μπορούσαμε επίσης να αποθηκεύσουμε τον κώδικα για προγράμματα όπως το Github, και μάλιστα, το υποκείμενο σύστημα git μοιάζει πολύ

με ένα Blockchain από πολλές απόψεις. Αυτά τα προγράμματα μπορούν να διαβαστούν ελεύθερα καθώς αποτελούν μέρος των αμετάβλητων δεδομένων της αλυσίδας. Κάθε συναλλαγή που δημοσιεύει δεδομένα στο Blockchain κοστίζει χρήματα.

Οι συνέπειες του COVID 19 σε Blockchain και Cryptocurrencies

Στις αρχές του 2020 παρατηρήθηκε η εμφάνιση του κορονaϊού που προκλήθηκε από έναν νέο ιό που ονομάζεται SARS-CoV.

Η ξαφνική έκρηξη και η ανεξέλεγκτη παγκόσμια εξάπλωση του COVID-19 δείχνουν τους περιορισμούς των υπαρχόντων συστημάτων υγειονομικής περίθαλψης για την έγκαιρη αντιμετώπιση καταστάσεων έκτακτης ανάγκης στη δημόσια υγεία. Σε τέτοια πλαίσια, καινοτόμες τεχνολογίες όπως το Blockchain και η Τεχνητή Νοημοσύνη (AI) έχουν αναδειχθεί ως πολλά υποσχόμενες λύσεις για την καταπολέμηση της επιδημίας του κορονaϊού.

Από τη μία πλευρά, το Blockchain μπορεί να καταπολεμήσει τις πανδημίες επιτρέποντας την έγκαιρη ανίχνευση εστιών, προστατεύοντας το απόρρητο των χρηστών και διασφαλίζοντας αξιόπιστη ιατρική αλυσίδα εφοδιασμού κατά την παρακολούθηση της επιδημίας. Από την άλλη πλευρά, η τεχνητή νοημοσύνη παρέχει έξυπνες λύσεις για τον εντοπισμό συμπτωμάτων που προκαλούνται από τον κορανοϊό για θεραπείες και την υποστήριξη της παρασκευής φαρμάκων.

Με τον θανατηφόρο κορονaϊό να εξαπλώνεται παγκοσμίως, πραγματοποιήθηκε στη διεθνή κοινότητα ένας αγώνας δρόμου για να εξασφαλιστεί η βοήθεια για τα θύματα καθώς και για να σταματήσει η εξάπλωση. Καθώς οι κυβερνήσεις προσπαθούν να

αντιμετωπίσουν αυτά τα προβλήματα, οι τεχνολογικές λύσεις μπορούν να βοηθήσουν στην αντιμετώπιση της παγκόσμιας κρίσης στην υγεία.

Εφαρμογές καινοτόμων τεχνολογικών τεχνολογιών όπως το Blockchain και η Τεχνητή Νοημοσύνη (AI) θα μπορούσαν να δώσουν απαντήσεις στην κρίση του κοροναϊού[14]. Ενώ το Blockchain μπορεί να καταπολεμήσει τις πανδημίες επιτρέποντας την έγκαιρη ανίχνευση εστιών, γρήγορη παράδοση φαρμάκων και προστατεύοντας το απόρρητο των χρηστών κατά τη διάρκεια της θεραπείας, η AI παρέχει έξυπνες λύσεις για τον εντοπισμό συμπτωμάτων που προκαλούνται από τον κοροναϊο για θεραπείες και υποστηρίζοντας την κατασκευή φαρμάκων. Υποστηρίζεται επίσης ότι η παρούσα κρίση κοροναϊού πρέπει να θεωρηθεί ως «έκκληση για όπλα προς την βιομηχανία τεχνολογίας», όπου το Blockchain και η Τεχνητή Νοημοσύνη μπορούν να είναι οι βασικοί παράγοντες για την ριζική αλλαγή του τοπίου της ανταπόκρισης σε κρίσεις και τη διαχείριση της επιδημίας του κοροναϊού. Από την πανδημία του coronavirus θα προκύψει μια νέα κατάσταση της ψηφιακής κοινωνίας - μια που θα επιταχύνει τις σημαντικές τεχνολογικές εξελίξεις που βρίσκονται ήδη σε εξέλιξη. Μεταξύ των πολλών σημαντικών καινοτομιών που θα προωθήσει η πανδημία είναι το blockchain και το cryptocurrency.

Ακολουθούν ορισμένες προβλέψεις για το διάστημα Blockchain και το ψηφιακό νόμισμα για το υπόλοιπο του έτους, καθώς και πώς θα επηρεαστούν από τον κοροναϊό.

Κατά τη διάρκεια του 2020, το Blockchain θα συνεχίσει να αυξάνεται στον χρηματοοικονομικό τομέα, μπροστά από άλλους κλάδους. Εφαρμογές όπως παρακολούθηση τροφίμων, έλεγχος ταυτότητας αγαθών και αποθήκευση ευαίσθητων δεδομένων συνεπάγονται σημαντική κανονιστική εργασία για τη σύνδεση αντικειμένων πραγματικού κόσμου στα αντίστοιχα ισοδύναμα.

Η πιο σημαντική ανακάλυψη σε αυτόν τον τομέα που θα δούμε είναι η εφαρμογή της βασικής τεχνολογίας του Blockchain στα κυρίαρχα νομίσματα. Η Κίνα θα μπορούσε κάλλιστα να επιχειρήσει ένα πείραμα σε μια πρότυπη πόλη όπως το Σενζέν φέτος όπως και η Σουηδία είναι μια άλλη χώρα που ενδιαφέρεται για αυτήν την πιθανότητα.

[14] A. A. Monrat, O. Schelen,´ and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE Access, vol. 7, pp. 117 134–117 151, 2019.

Θα υπάρξει μεγαλύτερη ενοποίηση στο χώρο του Blockchain. Πολλές εταιρείες δεν ήταν προετοιμασμένες για την κρίση, είτε πρόκειται για υποδομές είτε για οικονομικές ρυθμίσεις. Κατά συνέπεια, οι καλά προετοιμασμένες εκκινήσεις θα επιταχυνθούν.

Τα κρυπτονομίσματα θα χρησιμοποιούνται όλο και περισσότερο ως μη συσχετιζόμενες επενδυτικές επιλογές. Εάν κοιτάξετε την πρόσφατη κρίση της αγοράς που προκλήθηκε από τον κοροναϊό, τα κρυπτονομίσματα και το χρηματιστήριο συσχετίστηκαν μόνο για λίγο πάνω από μία εβδομάδα. Η πτώση του Bitcoin ήταν κυρίως ζήτημα ρευστότητας - ο χρυσός είχε την ίδια συμπεριφορά εκείνη την περίοδο - και έγινε γρήγορα εμφανές ότι το νόμισμα είχε υπερπωληθεί. Οι αγορές είναι και πάλι ασυμβίβαστες. Αυτό θα αυξήσει το ενδιαφέρον για χρηματοοικονομικά μέσα που βασίζονται σε Blockchain.

Είναι πολύ πιθανό, μέχρι το τέλος του έτους, να δούμε πώς θα είναι η μαζική υιοθέτηση. Το είδος των υπηρεσιών και των εργαλείων που θα χρησιμοποιηθούν ευρέως στο μέλλον πιθανότατα θα είναι ήδη διαθέσιμο φέτος.

Με τους ανθρώπους που μένουν σπίτι όπως ποτέ άλλοτε, περισσότερα διαδικτυακά τυχερά παιχνίδια σίγουρα θα συμβούν σε παγκόσμια κλίμακα. Αυτό θα έχει ως αποτέλεσμα την αύξηση της χρήσης ψηφιακού νομίσματος στο παιχνίδι και της σχετικής τεχνολογίας Blockchain.

Τα άτομα που μένουν στο σπίτι θα οδηγήσουν σε τεράστια αύξηση των casual παικτών - εκείνων που παίζουν απλά παιχνίδια στα smartphone ή τα tablet τους, παρά σε σοβαρούς χομπίστες με υπολογιστές παιχνιδιών. Αυτά τα παιχνίδια κατασκευάζονται συχνά από μικρές ομάδες και μπορούν να είναι εξαιρετικά κερδοφόρα δεδομένου του μεγέθους της αγοράς τυχερών παιχνιδιών. Ως αποτέλεσμα, υπάρχουν πολλά κίνητρα για να αδράξετε την ευκαιρία.

Επίσης, δεν είναι δύσκολο να φανταστεί κανείς τι θα είναι δημοφιλές: παιχνίδια πάρτι για άτομα σε καραντίνα που θέλουν να διασκεδάσουν κοινωνικά αλλά δεν μπορούν να περάσουν χρόνο μαζί. Η πιο προφανής χρήση είναι για το νόμισμα εντός του παιχνιδιού. Ωστόσο, είναι επίσης δυνατό να θεωρήσετε τα μη εύφλεκτα κουπόνια ως ψηφιακά συλλεκτικά αντικείμενα, είτε ως ειδικά βραβεία είτε για άτομα που θέλουν να προσαρμόσουν τον κόσμο του παιχνιδιού τους.

Οφέλη από τη χρήση Blockchain και AI για την επίλυση της επιδημίας του Coronavirus:

Το Blockchain και η Τεχνητή Νοημοσύνη είναι σε θέση να παρέχουν βιώσιμες λύσεις για την αντιμετώπιση της επιδημίας του coronavirus από διάφορες πτυχές. Το Blockchain που έχει αποδείξει την επιτυχία του σε πολλές εφαρμογές πραγματικού κόσμου, μπορεί να εφαρμοστεί για να υποστηρίξει την καταπολέμηση της εμφάνισης εστιών κοραναϊού. Μια πιθανή εφαρμογή είναι η παρακολούθηση εστιών έτσι ώστε το Blockchain να παρακολουθεί την εξάπλωση των λοιμώξεων του coronavirus μέσω ενός δικτύου Blockchain που αναπτύσσεται σε κινητές συσκευές πολιτών.

Ένα σημαντικό χαρακτηριστικό του Blockchain είναι η δυνατότητα διατήρησης του απορρήτου των χρηστών, η οποία μπορεί να επηρεάσει την παρακολούθηση του coronavirus, επιτρέποντας την έγκαιρη ανίχνευση επιδημιών, αποφεύγοντας ταυτόχρονα την έκθεση πληροφοριών του χρήστη.

Από την άλλη πλευρά, η Τεχνητή Νοημοσύνη μπορεί να βοηθήσει στην αντιμετώπιση της επιδημίας του κοροναϊού με διάφορους τρόπους. Η Τεχνητή Νοημοσύνη μπορεί να χρησιμοποιηθεί για την ανίχνευση του ιού και την πρόβλεψη της εξάπλωσης του ιού αναλύοντας τις συνδυασμένες πληροφορίες για τις περιβαλλοντικές συνθήκες, την πρόσβαση στην υγειονομική περίθαλψη και τον τρόπο μετάδοσής του. Με βάση αυτό, η τεχνητή νοημοσύνη μπορεί να εντοπίσει τον κορανοϊό σε εντοπισμένα κρούσματα της νόσου και να αποκαλύψει τη φύση του ιού . Ο κοροναϊός μπορεί να προκαλέσει σοβαρά συμπτώματα όπως πνευμονία, σοβαρό οξύ αναπνευστικό σύνδρομο και νεφρική ανεπάρκεια. Αλγόριθμοι που βασίζονται σε AI, όπως νευρωνικά δίκτυα που βασίζονται σε γονιδίωμα που έχουν ήδη κατασκευαστεί για εξατομικευμένη θεραπεία, μπορούν να αποδειχθούν πολύ χρήσιμοι στον έλεγχο αυτών των ανεπιθύμητων συμβάντων ή συμπτωμάτων που προκαλούνται από έναν κοροναϊό, ειδικά όταν ο αντίκτυπος του ιού εξαρτάται από την ανοσία και τη δομή του γονιδιώματος των ατόμων και όχι. Η συνήθης θεραπεία μπορεί να αντιμετωπίσει αποτελεσματικά όλα τα συμπτώματα προς το παρόν. Επιπλέον, η χρήση της AI μπορεί να είναι πολύ χρήσιμη για τον εντοπισμό της σχέσης του νέου κοροναϊού και των σχετικών ιών όπως το SARS για να επιταχυνθεί η εύρεση ενός νέου εμβολίου.

Τέλος, η μαζική παρακολούθηση στο κοινό για την παρακολούθηση του κοραναϊού εγείρει κρίσιμα ζητήματα απορρήτου. Για παράδειγμα, η ισραηλινή κυβέρνηση επιβάλλει πρόσφατα στους οργανισμούς υγειονομικής περίθαλψης να παρακολουθούν τα τηλέφωνα των πολιτών χωρίς να απαιτείται δικαστική απόφαση σε μια προσπάθεια

περιορισμού της εξάπλωσης του κορονοϊού COVID-19. Ωστόσο, αυτό το μέτρο αντιμετώπισε κριτική από εμπειρογνώμονες στον τομέα των ανθρωπίνων δικαιωμάτων και της ιδιωτικής ζωής, διότι μπορεί να αποκαλύψει ευαίσθητες προσωπικές πληροφορίες των πολιτών, προκαλώντας σοβαρές ανησυχίες σχετικά με την ιδιωτική ζωή και τις παραβιάσεις της πολιτικής ελευθερίας. Επομένως, ο τρόπος ανάπτυξης λύσεων που επιτρέπουν την άμεση παρακολούθηση της εξάπλωσης του ιού κορανοϊού ενώ ταυτόχρονα προστατεύει το απόρρητο των χρηστών είναι εξαιρετικά απαραίτητος για την επίλυση αυτής της επιδημίας έκτακτης ανάγκης.

Αρχικά, όλα τα δεδομένα από κλινικά εργαστήρια, νοσοκομεία, κοινωνικά μέσα και πολλές άλλες πηγές συγκεντρώνονται και δημιουργούν πρωτογενή δεδομένα που στη συνέχεια αναπτύσσονται σε κλίμακα σε μεγάλα δεδομένα. Αυτά τα δεδομένα πρέπει να διασφαλίζονται ως προς το απόρρητο και την ασφάλεια κατά τη διάρκεια της παρακολούθησης και της ανάλυσης εστιών coronavirus, χρησιμοποιώντας το Blockchain. Εδώ, το Blockchain μπορεί να προσφέρει μια σειρά βιώσιμων λύσεων για υπηρεσίες που σχετίζονται με τον coronavirus, όπως παρακολούθηση εστιών, προστασία απορρήτου χρήστη, ασφαλείς καθημερινές λειτουργίες, ιατρική αλυσίδα εφοδιασμού και παρακολούθηση δωρεών. Τα ασφαλή δεδομένα που συλλέγονται από το δίκτυο Blockchain αναλύονται χρησιμοποιώντας έξυπνες λύσεις που βασίζονται σε AI. Χρησιμοποιώντας αξιόπιστη πρόβλεψη και ικανότητα ακριβούς ανάλυσης σε μεγάλα δεδομένα που συλλέγονται από πηγές coronavirus, το AI μπορεί να παρέχει υποστήριξη για την καταπολέμηση του coronavirus μέσω πέντε κύριων εφαρμογών, όπως εκτίμηση εστίας, ανίχνευση κοραναϊού, αναλυτικά στοιχεία κοροναϊών, ανάπτυξη εμβολίων / ναρκωτικών και πρόβλεψη οποιουδήποτε μέλλοντος εστίας κοροναϊού. Τέλος, στην κορυφή της ιεραρχίας έρχεται το στρώμα των ενδιαφερόμενων μερών που περιλαμβάνει κόμματα όπως κυβερνήσεις, παρόχους υγειονομικής περίθαλψης που επωφελούνται από λύσεις Blockchain-AI. Πρέπει επίσης να ληφθεί υπόψη ότι το Blockchain μπορεί να δημιουργήσει ασφαλή δίκτυα και πρωτόκολλα επικοινωνίας για τη δημιουργία μιας γρήγορης και αξιόπιστης ανταλλαγής δεδομένων που διατηρεί το απόρρητο με τους ενδιαφερόμενους, χάρη στον αποκεντρωμένο χαρακτήρα του.

Συμπεράσματα

Η ταχεία τεχνολογική πρόοδος και η ανάπτυξη του ηλεκτρονικού εμπορίου έχουν διαμορφώσει σημαντικά τη διαδικασία δημιουργίας αξίας. Πολλές επιχειρήσεις επιδεικνύουν μεγάλη εξάρτηση από τεχνολογίες για να προσφέρουν απρόσκοπτα προϊόντα και υπηρεσίες στους πελάτες τους. Οι αναδυόμενες τεχνολογίες μπορούν να βοηθήσουν στον καλύτερο σχεδιασμό νέων προϊόντων και υπηρεσιών, στη βελτίωση της ποιότητας των δεδομένων και στη βελτίωση της απόδοσης και της διαδικασίας παραγωγής. Οι νέες τεχνολογίες έχουν επίσης αναδιαμορφώσει σημαντικά την πειθαρχία μάρκετινγκ και έφεραν νέους όρους και τακτικές μάρκετινγκ. Σήμερα, οι επωνυμίες χρησιμοποιούν όλο και περισσότερο την τεχνολογία για να αξιοποιήσουν την παγκόσμια εμβέλειά τους διεισδύοντας σε νέες αγορές και δημιουργώντας τη ζήτηση των καταναλωτών. Σε αυτήν τη διαδικασία, το Διαδίκτυο έχει επιτρέψει στους εμπόρους να προσεγγίσουν τους καταναλωτές με βελτιωμένες ηλεκτρονικές επικοινωνίες και διαδραστικά μέσα Εν τω μεταξύ, οι καταναλωτές έχουν γίνει πιο ενημερωμένοι για τις διαθέσιμες προσφορές και μπορούν να λάβουν ενημερωμένες αποφάσεις με βολικό τρόπο. Οι επιχειρήσεις επωφελήθηκαν από τεχνικές εξόρυξης δεδομένων και μεγάλα δεδομένα για να εξαγάγουν συμπεράσματα σχετικά με τις ανάγκες και τις επιθυμίες των καταναλωτών. Η ανάλυση μεγάλων συνόλων δεδομένων βοηθά τις επιχειρήσεις να αποκτήσουν ενεργές πληροφορίες μέσω προγνωστικών αναλυτικών στοιχείων. Η τεχνολογία Blockchain είναι μια τεχνολογική πρόοδος που μπορεί να βοηθήσει τις επωνυμίες να αποκτήσουν καλύτερη κατανόηση και να στοχεύσουν τους πελάτες τους, αλλά ταυτόχρονα επιτρέπουν στους πελάτες να ανακτήσουν τον έλεγχο των δραστηριοτήτων τους.

Βιβλιογραφία

Ankalkoti, Prashant, and S. G. Santhosh. 2017. “A Relative Study on Bitcoin Mining.” Imperial Journal of Interdisciplinary Research (IJIR) 3 (5): 1757–1761.

Anoaica, Andra, and Hugo Levard. 2018. “Quantitative Description of Internal Activity on the Ethereum Public Blockchain.” 2018 9th IFIP international conference on New technologies, Mobility and security (NTMS). IEEE, 1–5.

Antonopoulos, Andreas M., and Gavin Wood. 2018. Mastering Ethereum: Building Smart Contracts and Dapps. Sebastopol: O’Reilly Media.

Bai, C., and J. Sarkis. 2020. “A Supply Chain Transparency and Sustainability Technology Appraisal Model for Blockchain Technology.” International Journal of Production Research. doi:10.1080/00207543.2019.1708989.

Bhargavan, Karthikeyan, Antoine Delignat-Lavaud, Cédric Fournet, Anitha Gollamudi, Georges Gonthier, Nadim Kobeissi, Natalia Kula-tova, et al. 2016. “Formal Verification of Smart Contracts: Short Paper.” Proceedings of the 2016 ACM Workshop on programming languages and analysis for security, 91–96.

Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Business, Money and the World” - by D.Tapskott andA.Tapskott, 2017;

Blockchain Technology and Smart Contracts” - by J.Berguist, 2017

Brands, S. (1993, August). Untraceable off-line cash in wallet with observers. In Annual International Cryptology Conference(pp. 302-318). Springer, Berlin, Heidelberg.

Browne, R. 2017. “There Were More Than 26,000 New Blockchain Projects Last Year-Only 8% Are Still Active.” *CNBC*, November 9. Castellanos, J., F. Alejandro, Debora Coll-Mayor, and José Antonio Notholt. 2017. “*Cryptocurrency as Guarantees of Origin: Simulating a Green Certificate Market with the Ethereum Blockchain*.” *2017 IEEE international Conference on smart energy Grid Engineering* (SEGE). IEEE, 367–372.

Cheng, Zhen, Xinrui Hou, Runhuai Li, Yajin Zhou, Xiapu Luo, Jinku Li, and Kui Ren. 2019. “Towards a First Step to Understand the Cryptocurrency Stealing Attack on Ethereum.” 22nd international Symposium on research in Attacks, Intrusions and Defenses ({RAID} 2019), 47–60.

Chohan, U.W. (2017a). Cryptocurrencies: A Brief Thematic Review. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330

Chohan, U.W. (2017b).Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042248

Chohan, U.W. (2017c). A History of Bitcoin. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875

Chohan, U.W. (2017d). Cryptoanarchism and Cryptocurrencies. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3079241

Chohan, U.W. (2017e). Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080098

Chohan, U.W. (2017f). The Cryptocurrency Tumblers: Risks, Legality and Oversight. SSRN.

Chohan, U.W. (2017g). The Decentralized Autonomous Organization and Governance Issues. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055

Chohan, U.W. (2017h). The Leisures of Blockchains: Exploratory Analysis. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3084411

Chohan, U.W. (2017i). Blockchain and Securities Exchanges: Australian Case Study. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085631

Chohan, U.W. (2017j). What is a Ricardian Contract? SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085682

Christensen, Clayton M., and Joseph L. Bower. 1996. "Customer Power, Strategic Investment, and the Failure of Leading Firms." Strategic Management Journal 17 (3): 197–218.

Christidis, Konstantinos, and Michael Devetsikiotis. 2016. "Blockchains and Smart Contracts for the Internet of Things." IEEE Access 4:2292–2303.

Clohessy, T., Acton, T., and Rogers, N. (2019). "Blockchain adoption: technological, organisational and environmental considerations," in Business Transformation Through Blockchain, Vol. I, eds H. Treiblmaier and R. Beck (Cham: Springer International Publishing), 47–76. doi: 10.1007/978-3-319-98911-2_2

Cong, Lin William, and Zhiguo He. 2019. "Blockchain Disruption and Smart Contracts." The Review of Financial Studies 32 (5): 1754– 1797.

Cryptocurrency: The Ultimate Guide to The World of Cryptocurrency"- by N.Hofmann. T.Publisher, 2017;

Decourt, R.F.; Chohan, U.W.; Perugini, M.L. (2017). "Bitcoin returns and the Monday Effect." Conference Proceedings of the 14th Convibra: Administração (Brazil). November. http://www.convibra.com.br/upload/paper/2017/33/2017_33_14675.pdf

DeLone, William H., and Ephraim R. McLean. 2003. "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update." Journal of Management Information Systems 19 (4): 9–30.

Dolgui, Alexandre, Dmitry Ivanov, Semyon Potryasaev, Boris Sokolov, Marina Ivanova, and Frank Werner. 2019a. "Blockchain-Oriented Dynamic Modelling of Smart Contract Design and Execution in the Supply Chain." International Journal of Production Research 57: 1–19.

Dolgui, Alexandre, Dmitry Ivanov, Suresh P. Sethi, and Boris Sokolov. 2019b. "Scheduling in Production, Supply Chain and Industry 4.0 Systems by Optimal Control: Fundamentals, State-of-the-Art and Applications." International Journal of Production Research 57 (2): 411–432.

Forbes.com. 2019. "Forbes Releases 'Top 50 Billion-Dollar Companies Exploring Blockchain' — Over Half are Working with Ethereum." Forbes, November 1.

https://media.consensys.net/forbes-releases-top-50-billion-dollar-companies-exploring-Blockchain-over-half-are-working-with-d4f9e44f144d.

Francisco, Kristoffer, and David Swanson. 2018. “The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency.” Logistics 2 (1): 2.

Gai, Keke, Meikang Qiu, and Xiaotong Sun. 2018. “A Survey on FinTech.” Journal of Network and Computer Applications 103: 262–273.

Ghose, A. (2018). What blockchain could mean for marketing. Harv. Bus. Rev. 2–5. Available online at: https://hbr.org/2018/05/what-blockchain-could-mean-for-marketing

Global Cryptocurrency Benchmarking Study” - by G.Hilerman, M.Raucks. 2017;

Grech, Neville, Michael Kong, Anton Jurisevic, Lexi Brent, Bernhard Scholz, and Yannis Smaragdakis. 2018. “Madmax: Surviving

Groop, J., M. Ketokivi, M. Gupta, and J. Holmstrom. 2017. “Improving Home Care: Knowledge Creation Through Engagement and Design.” Journal of Operations Management 53-56: 9–22.

Hastig, Gabriella M., and ManMohan S. Sodhi. 2019. “Blockchain for Supply Chain Traceability: Business Requirements and Critical Success Factors.” Production and Operations Management. doi:10.1111/poms.13147.

Hukkinen, T., J. Mattila, K. Smolander, T. Seppälä, and T. Goodden. 2019. “Skimping on Gas – Reducing Ethereum Transaction Costs in a Blockchain Electricity Market Application.” Proceedings of the 52nd Hawaii International Conference on System Sciences, URI: https://hdl.handle.net/10125/60123, ISBN: 978-0-9981331-2-6.

Ingram, D., Panchadar, A., and Auchard, E. (2018). Facebook Privacy Scandal Widens as Data Leak Hits 87 Million Users. CIO. Available online at: https://www.cio.com.au/article/635768/facebook-privacy-scandal-widens-data-leak-hits-87-million-users/

Jabbar, Abdul, Pervaiz Akhtar, and Samir Dani. 2019. “Real-Time Big Data Processing for Instantaneous Marketing Decisions: A Problematization Approach.” Industrial Marketing Management. doi:10.1016/j.indmarman.2019.09.001.

Johnston, W. J. (2014). The future of business and industrial marketing and needed research. J. Bus. Mark. Manag. 7, 296–300. Available online at: https://www.econstor.eu/bitstream/10419/96103/1/783119623.pdf

Kamble, S., A. Gunasekaran, and H. Arha. 2019. “Understanding the Blockchain Technology Adoption in Supply Chains-Indian Context.” International Journal of Production Research 57 (7): 2009–2033.

Kim, Henry M., and Marek Laskowski. 2018. “Toward an Ontology-Driven Blockchain Design for Supply-Chain Provenance.” Intelligent Systems in Accounting, Finance and Management 25 (1): 18–27.

Kosba, Ahmed, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. 2016. “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts.” 2016 IEEE symposium on security and privacy (SP). IEEE, 839–858.

Kriptovalyuta” - by “UNEC Ekspert” journal, 2017;

Kumar, V., Dalla Pozza, I., and Ganesh, J. (2013). Revisiting the satisfaction–loyalty relationship: empirical generalizations and directions for future research. J. Retail. 89, 246–262. doi: 10.1016/j.jretai.2013.02.001

Lakhani, K. R. 2017. “the Truth About Blockchain.” Harvard Business Review 95 (1): 119–127.

Leng, Jiewu, Douxi Yan, Qiang Liu, Kailin Xu, J. Leon Zhao, Rui Shi, Lijun Wei, Ding Zhang, and Xin Chen. 2020. “ManuChain: Combining Permissioned Blockchain with a Holistic Optimization Model as Bi-Level Intelligence for Smart Manufacturing.” IEEE Transactions on Systems, Man, and Cybernetics: Systems 50 (1): 182–192.

Leng, Jiewu, Pingyu Jiang, Kailin Xu, Qiang Liu, J. Leon Zhao, Yiyang Bian, and Rui Shi. 2019. “Makerchain: A Blockchain with Chemical Signature for Self-Organizing Process in Social Manufacturing.” Journal of Cleaner Production 234: 767–778.

Lu, Y. (2019). The Blockchain: state-of-the-art and research challenges. J. Ind. Inf. Integr. 15, 80–90. doi: 10.1016/j.jii.2019.04.002

Madan, Isaac, Shaurya Saluja, and Aojia Zhao. 2015. Automated Bitcoin Trading via Machine Learning Algorithms. Working Paper, Stanford University, Stanford, CA, USA.

Manupati, V. K., T. Schoenherr, M. Ramkumar, S. M. Wagner, S. K. Pabba, and R. Inder Raj Singh. 2020. “A Blockchain-Based Approach for a Multi-Echelon Sustainable Supply Chain.” International Journal of Production Research 58 (7): 2222–2241. doi:10.1080/00207543.2019.1683248.

Min, Hokey. 2019. “Blockchain Technology for Enhancing Supply Chain Resilience.” Business Horizons 62 (1): 35–45.

Mondal, Saikat, Kanishka P. Wijewardena, Saranraj Karuppuswami, Nitya Kriti, Deepak Kumar, and Premjeet Chahal. 2019. “Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain.” IEEE Internet of Things Journal 6 (3): 5803–5813.

Mori, Taketoshi. 2016. “Financial Technology: Blockchain and Securities Settlement.” Journal of Securities Operations & Custody 8 (3): 208–227.

Olsen, Petter, and Melania Borit. 2018. “The Components of a Food Traceability System.” Trends in Food Science & Technology 77: 143–149.

Out-of-Gas Conditions in Ethereum Smart Contracts.” Proceedings of the ACM on Programming Languages 2: 1–27.

Pazaitis, Alex, Primavera De Filippi, and Vasilis Kostakis. 2017. “Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed.” Technological Forecasting and Social Change 125: 105–115.

Roeck, Dominik, Henrik Sternberg, and Erik Hofmann. 2019. “Distributed Ledger Technology in Supply Chains: A Transaction Cost Perspective.” International Journal of Production Research. doi:10.1080/00207543.2019.1657247.

Schmidt, Christoph G., and Stephan M. Wagner. 2019. “Blockchain and Supply Chain Relations: A Transaction Cost Theory Perspective.” Journal of Purchasing and Supply Management 25 (4): 100552.

Schniederjans, Dara G., Carla Curado, and Mehrnaz Khalajhedayati. 2020. “Supply Chain Digitisation Trends: An Integration of Knowledge Management.” International Journal of Production Economics 220: 107439.

Shermin, Voshmgir. 2017. “Disrupting Governance with Blockchains and Smart Contracts.” Strategic Change 26 (5): 499–509.

Simon, H. A. 1996. The Science of the Artificial. 3rd ed. Cambridge, MA: MIT Press.

Stentoft, Jan, and Christopher Rajkumar. 2019. “The Relevance of Industry 4.0 and its Relationship with Moving Manufacturing Out, Back and Staying at Home.” International Journal of Production Research. doi:10.1080/00207543.2019.1660823.

Stoll, Christian, Lena Klaaßen, and Ulrich Gallersdörfer. 2019. “The Carbon Footprint of Bitcoin.” Joule 3 (7): 1647–1661.

Sullivan, Clare, and Eric Burger. 2017. “E-Residency and Blockchain.” Computer Law & Security Review 33 (4): 470–481.

Tapscott, Don, and Alex Tapscott. 2017. “How Blockchain Will Change Organizations.” MIT Sloan Management Review 58 (2): 10.

The Age of Cryptocurrency” - by P.Vinga, M.Kasey, 2015;

The Altcoin Trader’s Handbook” - by N.Patell, 2014;

The Financial and economic crisis of 2008-2009 and developing countries - by S.Dulien, D.J.Kote, A.Marquez, J.Prieve, 2010;

The Internet of Money Paperback” - by A.Antonopulos, 2016;

The Trader’s Handbook” - by M.Neufeinde, 2016.

Van Aken, Joan, Aravind Chandrasekaran, and Joop Halman. 2016.“Conducting and Publishing Design Science Research: Inaugural Essay of the Design Science Department of the Journal of Operations Management.” Journal of Operations Management 47-48: 1–8.

Wang, Yingli, Meita Singgih, Jingyao Wang, and Mihaela Rit. 2019. “Making Sense of Blockchain Technology: How Will it Transform Supply Chains?” International Journal of Production Economics 211: 221–236.

White, Gareth RT. 2017. “Future Applications of Blockchain in Business and Management: A Delphi Study.” Strategic Change 26 (5): 439–451.

Wood, Gavin. 2017. “Ethereum: A Secure Decentralised Generalised Transaction Ledger (eip-150 Revision).” Ethereum Project Yellow Paper 151.

Yanling, Chang, Iakovou Eleftherios, and Shi Weidong. 2019. “Blockchain in Global Supply Chains and Cross Border Trade: a Critical Synthesis of the State-of-the-art, Challenges and Opportunities.” International Journal of Production Research. doi:10.1080/00207543.2019.1651946.

Yeoh, Peter. 2017. “Regulatory Issues in Blockchain Technology.” Journal of Financial Regulation and Compliance 25: 196–208.

Ιστοσελίδες

1. https://www.cbinsights.com/research/blockchain-disrupting-banking/
2. www.apiax.com
3. www.apiax.com/use-case/digital-wealth-management/
4. www.apiax.com/digital-cross-border-compliance/
5. www.falconpb.com/en/blockchain-solutions
6. https://blockgeeks.com/guides/smart-contracts/
7. https://en.m.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication
8. https://www.ubs.com/magazines/innovation/en/our-approach/2016/path-finding.html
9. https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp
10. http://fintechnews.ch/regtech/swift-global-know-your-customer-kyc-platform/25514/
11. https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/kyc-solutions/the-kyc-registry
12. https://blockgeeks.com/guides/what-is-blockchain-technology/
13. https://www.finews.com/news/english-news/35078-swiss-exchange-fewer-risks-with-blockchain
14. https://covidathon.devpost.com/
15. https://www.opengovpartnership.org/collecting-open-government-approaches-to-covid-19/
16. https://www.codemotion.com/magazine/articles/stories/covid-19-hackathon/