ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΜΗΧΑΝΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ

ΤΟΜΕΑΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΕΡΕΥΝΑΣ

ΤΙΤΛΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ: Αλγόριθμοι Συναίνεσης και ο Ρόλος τους στις Σύγχρονες Εφαρμογές Αλυσίδων Κοινοποιήσεων (Blockchain)

ΟΝΟΜΑ: ΤΣΑΠΟΓΑΣ ΧΡΗΣΤΟΣ

ΕΠΙΒΛΕΠΩΝ: ΣΤΑΥΡΟΣ ΠΟΝΗΣ, ΚΑΘΗΓΗΤΗΣ ΕΜΠ

ΑΘΗΝΑ, ΟΚΤΩΒΡΙΟΣ 2022

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της διπλωματικής εργασίας κ.Σ.Πόνη. Η καθοδήγηση, οι συμβουλές και η βοήθεια του υπήρξαν καταλυτικοί παράγοντες στην εκπόνηση της συγκεκριμένης εργασίας.

Ακόμη, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στους φίλους μου και στην οικογένεια μου για την στήριξη και τη συμπαράσταση τους σε όλη τη διάρκεια των σπουδών μου.

Τσαπόγας Χρήστος

Οκτώβριος 2022

Έχω διαβάσει και κατανοήσει τους κανόνες για τη λογοκλοπή και τον τρόπο σωστής αναφοράς των πηγών που περιέχονται στον Οδηγό συγγραφής Διπλωματικών εργασιών. Δηλώνω ότι, από όσα γνωρίζω, το περιεχόμενο της παρούσας Διπλωματικής εργασίας είναι προϊόν δικής μου δουλειάς και υπάρχουν αναφορές σε όλες τις πηγές που χρησιμοποίησα.

ΧΡΗΣΤΟΣ ΤΣΑΠΟΓΑΣ

Περίληψη

Αδιαμφισβήτητα, το περιβάλλον της αγοράς στις μέρες μας απαιτεί υψηλό επίπεδο εξυπηρέτησης πελατών και παράλληλα το ελάχιστο δυνατό κόστος προϊόντων. Για την επίτευξη των στόχων αυτών, οι εταιρείες ψάχνουν ολοένα και περισσότερες τεχνολογίες οι οποίες μπορούν να βοηθήσουν. Το Blockchain είναι μια τέτοια τεχνολογία η οποία επιτρέπει την ασφαλή, ακριβή και κρυπτογραφημένη καταγραφή συναλλαγών αλλά και την επίτευξη συμφωνιών μεταξύ δύο μερών. Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο ενός έργου για την μείωση της σπατάλης των τροφίμων, για το οποίο θα φτιαχτεί μια εφαρμογή που θα λειτουργεί με δίκτυο Blockchain. Πιο συγκεκριμένα, αναλύεται αρχικά η τεχνολογία Blockchain, ενώ παράλληλα αναφερόμαστε στις εφαρμογές των δικτύων αυτών όπως και στην ασφάλεια την οποία παρέχουν. Ακόμη, αναλύουμε αρκετά από τα γνωστά κρυπτονομίσματα, τα οποία κυριαρχούν τη περίοδο αυτή. Το σημαντικότερο όμως κομμάτι της εργασίας είναι η ανάλυση των αλγορίθμων συναίνεσης που υποστηρίζουν ένα δίκτυο Blockchain και η πρόταση ενός από αυτούς για να χρησιμοποιηθεί στην εφαρμογή του ζητούμενου έργου. Τέλος, έχει γίνει μια δομημένη βιβλιογραφική ανασκόπηση και έρευνα των παραπάνω πεδίων μέσω της πλατφόρμας Scopus, με σκόπο να προκύψουν χρήσιμα συμπεράσματα για τα ζητήματα που μας ενδιαφέρουν.

Abstract

Undoubtedly, the market environment today demands high level of client service, while the cost of products should be maintained as low as possible. To achieve such goals, business entities (companies) seek a growing number of available technologies to assist them. Blockchain is such a technology that allows for safe, precise, and encrypted trades to be recorded, while enabling agreements between two parties to be arranged. This diploma thesis was conducted in the context of a project on the reduction of food waste, for which an application will be developed that operates based on a Blockchain network. Specifically, the Blockchain technology is first analyzed, while relevant topics on Blockchain-enabled networks and the safety that these networks provide are also discussed. Moreover, several popular crypto-currencies, which are currently dominant in the crypto-market, are analyzed. The most significant part of this thesis, though, is the study of consensus algorithms that support a Blockchain network and the proposition of such an algorithm for direct deployment in the food waste project. Lastly, a structured literature review and study of the abovementioned fields powered by the Scopus platform has been performed, to extract useful conclusions on the topics of interest.

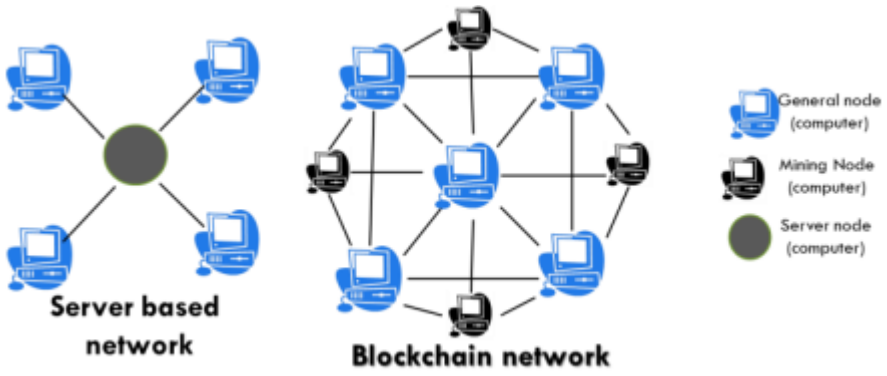
Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Εισαγωγή

Το Blockchain είναι μια κατανεμημένη τεχνολογία που βασίζεται σε υπολογιστές σε ένα αξιόπιστο δίκτυο, όπου μπλοκ δεδομένων προς διαχείριση αποθηκεύονται σε κατανεμημένες βάσεις δεδομένων που φιλοξενούνται σε δίκτυα peer-to-peer (P2P), τα οποία επιτρέπουν σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Σχηματίζονται αλυσίδες μεταξύ των μπλοκ έτσι ώστε τα μπλοκ να μην μπορούν να αναθεωρηθούν αυθαίρετα και να είναι δυνατή η πρόσβαση στα αποτελέσματα τυχόν αλλαγών. Με άλλα λόγια, το Blockchain είναι μια τεχνολογία κατανεμημένης λογιστικής (DLT). Όλα τα δεδομένα προς διαχείριση αποθηκεύονται και διαχειρίζονται πληροφορίες συναλλαγών στους υπολογιστές των συμμετεχόντων που είναι συνδεδεμένοι στο δίκτυο P2P αντί σε έναν κεντρικό διακομιστή ενός συγκεκριμένου οργανισμού (Tang et al, 2022). Στα αριστερά στην **Εικόνα 1** απεικονίζεται ένα τρέχον και παραδοσιακό δίκτυο υπολογιστών στο διαδίκτυο, ενώ στα δεξιά φαίνεται ένα δίκτυο Blockchain.



Εικόνα 1: Δίκτυο που βασίζεται σε διακομιστή και δίκτυο Blockchain (Kim, 2020).

Τα κύρια χαρακτηριστικά της τεχνολογίας Blockchain περιλαμβάνουν αξιοπιστία που επιτυγχάνεται μέσω διαδικασιών συναίνεσης σε μη αξιόπιστα περιβάλλοντα, ασφάλεια, οικονομική αποδοτικότητα, ευελιξία, αποκέντρωση, απουσία ενδιάμεσων, διαφάνεια, αποτελεσματικότητα και επεκτασιμότητα (Kim, 2020). Στόχος της παρούσας εργασίας είναι η μελέτη της τεχνολογίας Blockchain πίσω από τα κρυπτονομίσματα.

Κεφάλαιο 1: Βιβλιογραφική Ανασκόπηση

Το κεφάλαιο αυτό έχει δομηθεί ως εξής: Στις **Ενότητες 1.1 και 1.2** περιγράφεται η μέθοδος, η οποία ακολουθήθηκε για τη διεξαγωγή της βιβλιογραφικής ανασκόπησης και ο τρόπος παρουσίασης της. Στη συνέχει έχουμε την ανάλυση και την εξήγηση των εννοιών που παρουσιάζονται στις **Ενότητες 1.3 εώς 1.7.**

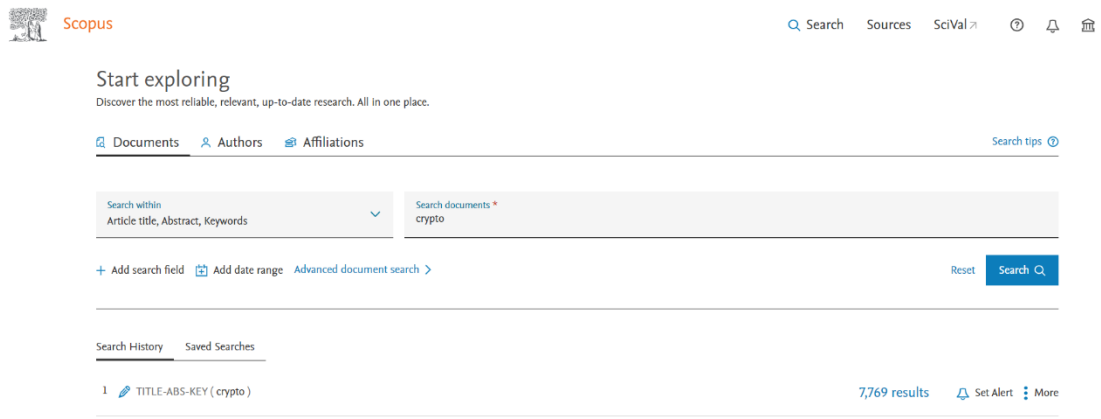
1.1 Μέθοδος Έρευνας

Ο πιο σημαντικός παράγοντας για να χαρακτηριστεί μια ανασκόπηση βιβλιογραφικού πεδίου επιτυχής είναι η δομημένη και συνεκτική προδιαγραφή της μεθόδου προσέγγισης της βιβλιογραφίας. Στο επίκεντρο της διπλωματικής εργασίας βρίσκεται η τεχνολογία Blockchain με έμφαση στην ανάλυση των αλγορίθμων συναίνεσης και των ίδιων των κρυπτονομισμάτων που υπάρχουν και χρησιμοποιούνται. Ακόμη, η έρευνα επικεντρώνεται και στην ασφάλεια των δικτύων Blockchain.

1.1.1 Επιλογή Βιβλιογραφικών Πηγών

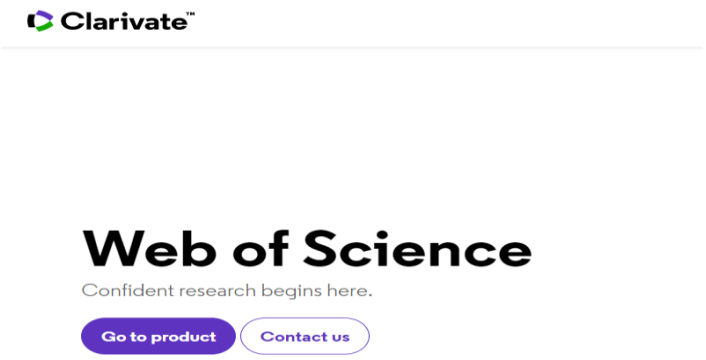
Το πρώτο βήμα που πραγματοποιείται είναι η επιλογή των πηγών άντλησης βιβλιογραφικών δεδομένων. Οι επιλογές που έχουμε διαθέσιμες και έχουμε διαρκή πρόσβαση σε αυτές είναι οι ακόλουθες:

I) Scopus: Η βιβλιογραφική βάση Scopus είναι από τις πιο δημοφιλείς και αντιπροσωπευτικές βάσεις δεδομένων αναζήτησης βιβλιογραφίας. Καλύπτει σχεδόν 36.377 τίτλους από 11.678 εκδότες, από τους οποίους (τίτλους), οι 34.346 είναι έγκριτα αξιολογημένα περιοδικά στις Επιστημονικές, Τεχνολογικές, Φαρμακευτικές και Κοινωνικές επιστήμες, συμπεριλαμβανομένων των Τεχνών και των Ανθρωπιστικών σπουδών. Οι αναζητήσεις στη βάση δεδομένων Scopus ενσωματώνουν αναζητήσεις από επιστημονικές ηλεκτρονικές ιστοσελίδες μέσω του Scirus, ενός προϊόντος της Elsevier, καθώς και βάσεις δεδομένων με ευρεσιτεχνίες. Η πρόσβαση εξασφαλίζεται μέσω του ακαδημαϊκού δικτύου Heal Link από την ιστοσελίδα της Κεντρικής Βιβλιοθήκης του Ε.Μ.Π.



Εικόνα 2: Η οθόνη αναζήτησης του Scopus

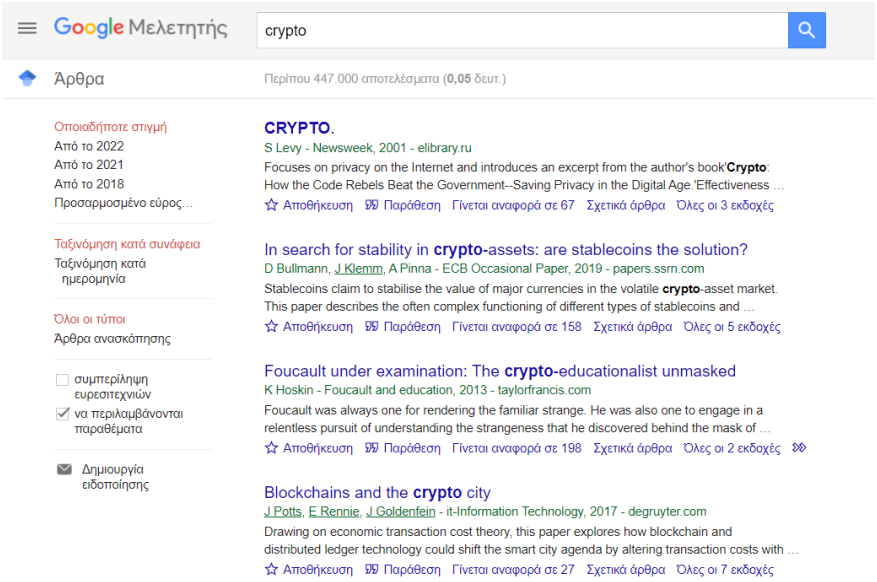
II) Web of Sciense (WoS)- Clarivate Analytics: Το Web of Science (WoS, παλαιότερα γνωστό ως Web of Knowledge) είναι μια πλατφόρμα πληρωμένης πρόσβασης που παρέχει (συνήθως μέσω Διαδικτύου) πρόσβαση σε πολλαπλές βάσεις δεδομένων που παρέχουν δεδομένα αναφοράς και παραπομπών από ακαδημαϊκά περιοδικά, πρακτικά συνεδρίων και άλλα έγγραφα σε διάφορους ακαδημαϊκούς κλάδους. Δημιουργήθηκε αρχικά από το Ινστιτούτο Επιστημονικών Πληροφοριών. Επί του παρόντος ανήκει στην Clarivate, όπου προηγουμένως ήταν η επιχείρηση Πνευματικής Ιδιοκτησίας και Επιστήμης της Thomson Reuters.



Εικόνα 3: Οθόνη στο site του Web of Science

III) Google Scholar: Η Google Scholar είναι ελεύθερα προσβάσιμη μηχανή αναζήτησης ιστού που εντοπίζει το πλήρες κείμενο ή τα μεταδεδομένα των ακαδημαϊκών δημοσιεύσεων που έχουν υλοποιηθεί σε μία εκτεταμένη σειρά επιστημονικών και τεχνικών εκδόσεων, σε παγκόσμια κλίμακα. Η βάση αυτή αφορά δημοσιεύσεις που έχουν γίνει αποκλειστικά με χρήση της αγγλικής γλώσσας. Η

πρόσβαση στη συγκεκριμένη μηχανή αναζήτησης παρέχεται από τη Βιβλιοθήκη του Ε.Μ.Π.



Εικόνα 4: Οθόνη αναζήτησης του Google Scholar

Ύστερα από την ανάλυση των παραπάνω βάσεων δεδομένων και μηχανών αναζήτησης στη παρούσα διπλωματική εργασία αποφασίστηκε να προχωρήσει η βιβλιογραφική έρευνα με τη βάση **Scopus**. Με δεδομένα τα αυστηρότερα κριτήρια ένταξης ενός τίτλου στο ISI WoS, υπάρχει δε η σχετική βεβαιότητα πως οι τίτλοι, οι οποίοι συμμετέχουν σε αυτό, είναι ήδη ενταγμένοι στο SCOPUS και κατά συνέπεια, η πιθανότητα απώλειας χρήσιμων για την έρευνα δημοσιεύσεων είναι πολύ μικρή. Ακόμη εκτός της έρευνας στο **Scopus**, βιβλιογραφικές πηγές αναζητήθηκαν και στο **Google Scholar** με σκοπό να συμπληρωθούν οποιαδήποτε κενά υπήρχαν στη μελέτη της θεματικής μας ενότητας.

1.1.2 Επιλογή Λέξεων Κλειδιών

Το δεύτερο βήμα της μεθόδου αυτής περιλαμβάνει την επιλογή των λέξεων κλειδιών με βάση τις οποίες θα αναζητηθεί η σχετική βιβλιογραφία. Οι φράσεις που επιλέχθηκαν για τη βέλτιστη διερεύνηση του θέματος είναι οι εξής: **1) consensus algorithms, 2) blockchain 3) crypto***. Η χρήση του αστερίσκου (*) υποδηλώνει την αναζήτηση τόσο της λέξης "crypto", όσο και παραγώγων αυτής (π.χ. "cryptocurrency"). Η ενοποίηση των φράσεων κατά την αναζήτηση διενεργήθηκε χρήσει του λογικού τελεστή "OR". Κάθε αποτέλεσμα της εν λόγω αναζήτησης περιείχε τουλάχιστον μία από τις προαναφερθείσες φράσεις.

1.1.3 Επιλογή Πεδίων Αναζήτησης και Χρονικού Εύρους Μελέτης

Τα πεδία αναζήτησης, τα οποία χρησιμοποιηθήκαν στη βιβλιογραφική έρευνα, ήταν ο 'Τίτλος', η 'Περίληψη' και οι 'Λέξεις Κλειδιά' κάθε δημοσίευσης. Το **Scopus** παρέχει αυτή τη δυνατότητα αναζήτησης. Στη συνέχεια όσον αφορά το χρονικό εύρος της μελέτης, τα αποτελέσματα κατά την διάρκεια της αναζήτησης αφορούσαν τη περίοδο από το 2018 και μετά πέρα από δύο δημοσιεύσεις που ήταν πριν από τότε. Καθώς το ζήτημα που αναλύουμε έχει ραγδαία ανάπτυξη τα τελευταία χρόνια και ταυτόχρονα όλες οι δημοσιεύσεις είναι αρκετά πρόσφατες θα τις εξετάσουμε όλες για την διπλωματική εργασία.

1.1.4 Επιλογή Κατηγοριών Δημοσιεύσεων

Το επόμενο βήμα της μεθόδου είναι η επιλογή της κατηγορίας των πηγών ή αλλιώς των δημοσιεύσεων που τελικά θα χρησιμοποιήσουμε. Με βάση το κριτήριο των αξιολογημένων βιβλιογραφικών πηγών, οι οποίες παρουσιάζουν ώριμα και αξιόπιστα ερευνητικά αποτελέσματα, αλλά και τεκμηριωμένες αναλύσεις καταλήγουμε στις εξής βασικές κατηγορίες δημοσιεύσεων, που συμμετείχαν στη μελέτη:

- Άρθρα σε επιστημονικά περιοδικά (**Article**)
- Άρθρα επισκόπησης επιστημονικού πεδίου με σύστημα κριτών (**Review Papers**)
- Κεφάλαια σε βιβλία (**Book Chapters**)

1.1.5 Επιλογή Ερευνητικής Περιοχής

Το τελευταίο βήμα της μεθόδου έρευνας είναι η επιλογή της ερευνητικής περιοχής του θέματος των δημοσιεύσεων. Το θέμα των κρυπτονομισμάτων έχει μελετηθεί κυρίως τα τελευταία χρόνια από επιστήμονες αρκετών και διαφορετικών κλάδων. Η βιβλιογραφική ανασκόπηση έχει σκοπό να εξάγει αποτελέσματα συναφή με το θέμα που εξετάζουμε. Έτσι λοιπόν, τα φίλτρα που ορίζουν την ερευνητική περιοχή που εξετάζουμε είναι τα εξής: **1) Engineering, 2) Decision Sciences, 3) Multidisciplinary, 4) Business, Management and Accounting.**

Στο παρακάτω σχήμα παρουσιάζονται τα διακριτά βήματα της μεθόδου βιβλιογραφικής επισκόπησης.

Εικόνα 5: Μεθοδολογία βιβλιογραφικής ανασκόπησης

1.2 Αποτελέσματα Βιβλιογραφικής Ανασκόπησης

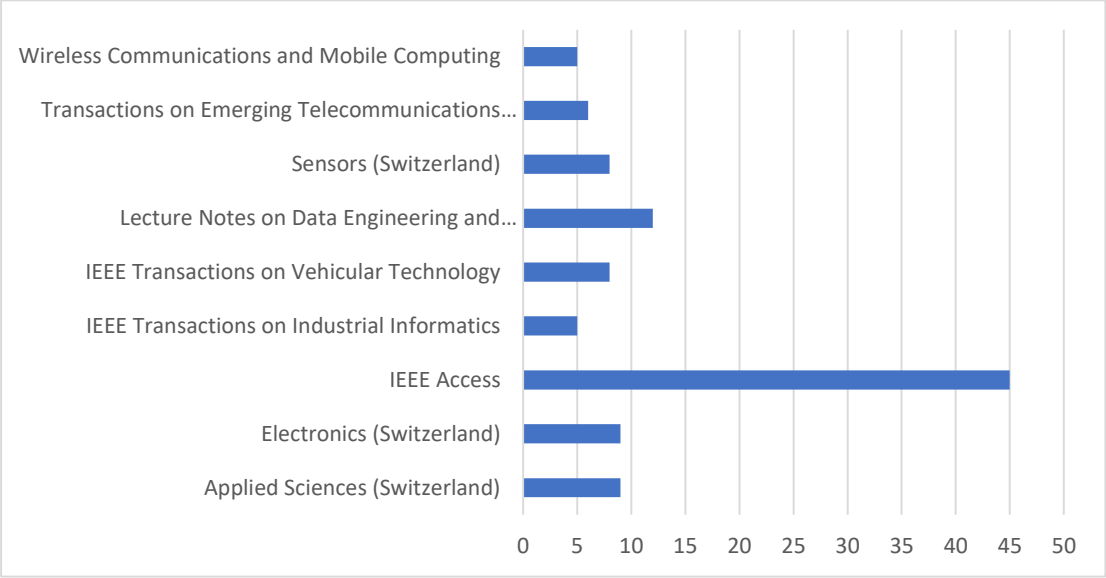
Στην παράγραφο αυτή θα παρουσιάσουμε τα αποτελέσματα της βιβλιογραφικής ανασκόπησης

1.2.1 Ερευνητικοί Στόχοι Βιβλιογραφικής Ανασκόπησης

Στόχος της ανασκόπησης αυτής είναι η ανάλυση και η κατανόηση της τεχνολογίας των Blockchain και των κρυπτονομισμάτων. Συνεπώς, κατά τη διάρκεια της ανάγνωσης των περιλήψεων των δημοσιεύσεων ορίζουμε μερικές κατηγορίες που θα καταταχτούν τα αποτελέσματα μας. Οι κατηγορίες ενδιαφέροντος είναι οι εξής: **α)** Τεχνολογία και Κατηγορίες Blockchain, **β)** Εφαρμογές του Blockchain σε διάφορους κλάδους, **γ)** Κρυπτονομίσματα, **δ)** Ασφάλεια Δικτύων Blockchain. Προφανώς αρκετά άρθρα αποδεικνύεται στη συνέχεια ότι ανήκουν σε παραπάνω από μία κατηγορίες, παρόλα αυτά εμείς τα κατατάσσουμε στην κατηγορία που θεωρούμε ότι ταιριάζουν σύμφωνα με την περίληψη τους.

1.2.2 Στατιστικά Αποτελέσματα Βιβλιογραφικής Ανασκόπησης

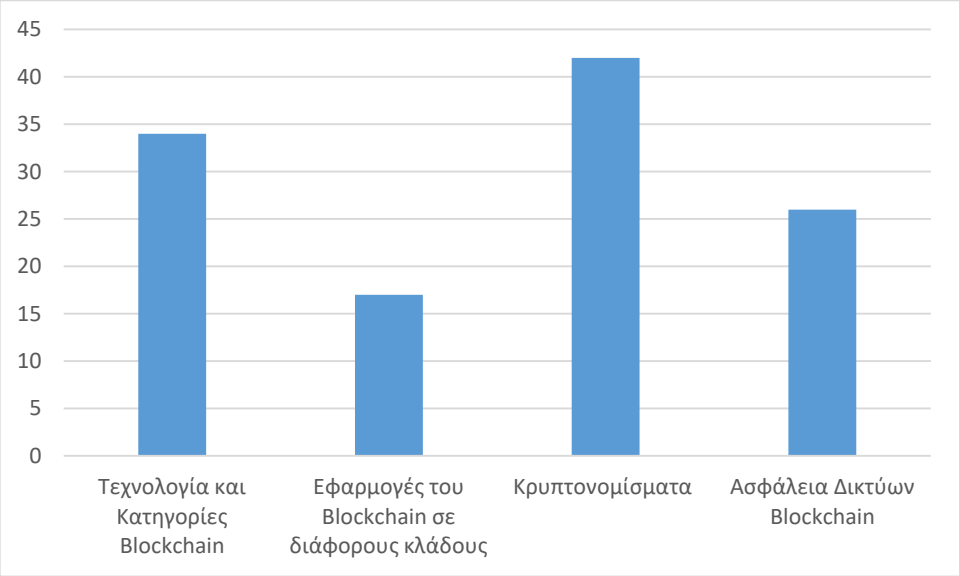
Η βιβλιογραφική ανασκόπηση είχε ως αποτέλεσμα 268 δημοσιεύσεις. Στο παρακάτω διάγραμμα αποτυπώνεται ο αριθμός των δημοσιεύσεων ανά επιστημονική πηγή.



Εικόνα 6: Γραφική απεικόνιση πλήθους αποτελεσμάτων βιβλιογραφικής ανασκόπησης

Έπειτα από την ανάγνωση των περιλήψεων των αρχικών αποτελεσμάτων της ανασκόπησης κρίθηκε ότι πολλά από τα άρθρα δεν έχουν άμεση σχέση με τις κατηγορίες ενδιαφέροντος. Πιο συγκεκριμένα από τα 268 άρθρα, ο αριθμός των

σχετικών άρθρων είναι 119. Έτσι λοιπόν, τα άρθρα αυτά κατηγοριοποιούνται στις 4 θεματικές ενότητες και παρακάτω παρουσιάζονται τα στατιστικά αποτελέσματα της βιβλιογραφικής ανασκόπησης.



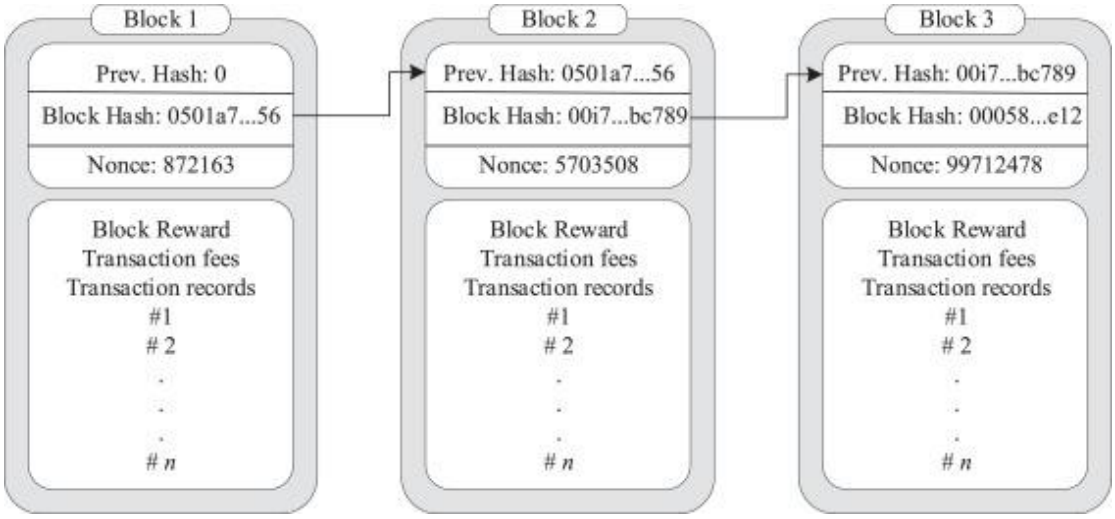
Εικόνα 7: Πλήθος άρθρων ανά κατηγορία μελέτης με βάση τις περιλήψεις τους

1.3 Ανάπτυξη της τεχνολογίας Blockchain

Η τεχνολογία Blockchain εισήχθη για πρώτη φορά από μια ομάδα ερευνητών (Haber et al, 1991) και μέχρι την ίδρυση του Bitcoin από τον Satoshi Nakamoto το 2008 (Nakamoto, 2017), δεν είχε κοινές εφαρμογές. Ωστόσο, πρέπει να σημειωθεί ότι τα τελευταία χρόνια έχει χρησιμοποιηθεί σε διαφορετικούς τομείς όπως η βιοϊατρική και η διαχείριση της εφοδιαστικής αλυσίδας (Solanki, 2021).

Το Blockchain ως κατανεμημένη και αποκεντρωμένη βάση δεδομένων είναι μια ακολουθία μπλοκ που σε κάθε μπλοκ συγκεντρώνεται μια λίστα συναλλαγών. Κάθε μπλοκ έχει τρεις κύριες ενότητες: δεδομένα, μπλοκ κατακερματισμού και προηγούμενο μπλοκ κατακερματισμού. Ο κατακερματισμός καθορίζει την ταυτότητα κάθε μπλοκ σαν δακτυλικό αποτύπωμα και είναι μοναδικός για κάθε μπλοκ. Οι πληροφορίες κάθε μπλοκ υποδεικνύονται με Hash. Όταν μια συναλλαγή καταχωρείται σε ένα μπλοκ, ο αριθμός κατακερματισμού της υπολογίζεται σε ένα μπλοκ κρυπτογράφησης που περιέχει πληροφορίες και λαμβάνεται με μαθηματικούς κανόνες. Κάθε μπλοκ περιέχει τον κατακερματισμό του προηγούμενου μπλοκ. έτσι τα μπλοκ συνδέονται μεταξύ τους. Οποιεσδήποτε αλλαγές γίνονται στις πληροφορίες ενός μπλοκ προκαλούν αλλαγές

στον αριθμό κατακερματισμού του. Επομένως, τυχόν παράνομες αλλαγές στις πληροφορίες των μπλοκ μπορεί να αλλάξει τον αριθμό κατακερματισμού του και αυτό θα κάνει το μπλοκ να καταστεί άκυρο για τα επόμενα μπλοκ (Solanki, 2021). Η **Εικόνα 8**, απεικονίζει τη δομή του Blockchain Bitcoin για τρία μπλοκ.



Εικόνα 8 Η δομή του Blockchain Bitcoin (Bamakan et al, 2020).

Όπως παρουσιάζεται στην **Εικόνα 8**, το πρώτο μπλοκ ονομάζεται μπλοκ Genesis και επειδή δεν υπάρχει άλλο μπλοκ πριν από αυτό, το προηγούμενο ποσό κατακερματισμού είναι ίσο με μηδέν. Κάθε μπλοκ μπορεί να περιέχει χιλιάδες εγγραφές συναλλαγών που κωδικοποιούνται από μια συνάρτηση κατακερματισμού πριν από τη μετάδοση στο δίκτυο (Bamakan et al, 2020).

Το Blockchain χρησιμοποιεί τη λειτουργία δέντρου Merkle για να δημιουργήσει μια τελική τιμή κατακερματισμού ως δείκτη κατακερματισμού (κατακερματισμός του τρέχοντος μπλοκ) και κάθε μπλοκ περιέχει τον κατακερματισμό του προηγούμενου μπλοκ για τη διατήρηση της συνδεσιμότητας των μπλοκ. Το δέντρο Merkle είναι μια δομή δεδομένων σαν δέντρο κατακερματισμού που αποθηκεύει τις συναλλαγές σε μια δυαδική δενδρική μορφή. Κάθε κόμβος φύλλου του δέντρου αποθηκεύει την τιμή κατακερματισμού των συναλλαγών και ένας κόμβος χωρίς φύλλα περιέχει τον κατακερματισμό των κατακερματισμών των δύο αντίστοιχων θυγατρικών κόμβων και, τέλος, τη ρίζα αυτού του δέντρου που ονομάζεται Merkle digest/root. Η χρήση μιας συνάρτησης δέντρου Merkle θα μειώσει το κόστος μετάδοσης δεδομένων και υπολογιστικών πόρων. Συνοπτικά, η διαδικασία εξόρυξης ή επικύρωσης ενός νέου μπλοκ με τον αλγόριθμο απόδειξης εργασίας απαιτείται για να γίνει μια εξαντλητική αναζήτηση μιας συνάρτησης κατακερματισμού κρυπτογράφησης για να βρεθεί ένας

αριθμός που χρησιμοποιείται μόνο μια φορά με τέτοιο τρόπο που να ικανοποιεί μια προκαθορισμένη συνθήκη (Bamakan et al, 2020).

1.4 Τεχνολογία Blockchain και εφαρμογές

Αναμφίβολα, η τεχνολογία Blockchain είναι μια από τις μεγαλύτερες τεχνολογίες. Αν και η πρώτη εφαρμογή της τεχνολογίας Blockchain ήταν το Bitcoin ως κρυπτονόμισμα, άλλες εφαρμογές αυτής της τεχνολογίας έχουν επίσης κερδίσει την προσοχή από κυβερνητικούς και βιομηχανικούς τομείς. Αναμένεται ότι μέχρι το 2027, το Blockchain θα αποθηκεύει το δέκα τοις εκατό του παγκόσμιου Ακαθάριστου Εθνικού Προϊόντος (ΑΕΠ) (Bamakan et al, 2020).

Λόγω της εξάπλωσης των Τεχνολογιών Πληροφοριών και Επικοινωνίας (ΤΠΕ) τις τελευταίες δεκαετίες, υπάρχει μια εκθετική αύξηση στη χρήση διαφόρων έξυπνων εφαρμογών όπως η έξυπνη γεωργία, η έξυπνη υγειονομική περίθαλψη, η εφοδιαστική αλυσίδα και η εφοδιαστική, οι επιχειρήσεις, ο τουρισμός και η φιλοξενία αλλά και η διαχείριση ενέργειας. Για όλες τις προαναφερθείσες εφαρμογές, η ασφάλεια και το απόρρητο αποτελούν βασικές ανησυχίες, λαμβάνοντας υπόψη τη χρήση του ανοιχτού καναλιού, δηλαδή του διαδικτύου για μεταφορά δεδομένων. Αν και πολλές λύσεις και πρότυπα ασφαλείας έχουν προταθεί όλα αυτά τα χρόνια για την ενίσχυση των επιπέδων ασφαλείας των προαναφερθέντων έξυπνων εφαρμογών, οι υπάρχουσες λύσεις είτε βασίζονται στην κεντρική αρχιτεκτονική (με ένα μόνο σημείο αστοχίας) είτε έχουν υψηλό κόστος υπολογισμού και επικοινωνίας. Επιπλέον, οι περισσότερες από τις υπάρχουσες λύσεις ασφάλειας έχουν επικεντρωθεί μόνο σε λίγες πτυχές και αποτυγχάνουν να αντιμετωπίσουν την επεκτασιμότητα, την ευρωστία, την αποθήκευση δεδομένων, την καθυστέρηση δικτύου, τη δυνατότητα ελέγχου, την αμετάβλητη και την ιχνηλασιμότητα. Για τον χειρισμό των προαναφερθέντων ζητημάτων, η τεχνολογία Blockchain μπορεί να είναι μία από τις λύσεις (Bodkhe et al, 2018).

Το Blockchain προσελκύει την προσοχή ως μια νέα λύση για προβλήματα όπως η παράνομη αντιγραφή, η διανομή κερδών και η πλαστογραφία και η παραποίηση στο περιβάλλον εμπορίας ψηφιακού περιεχομένου, το οποίο έχει γίνει βασικό στοιχείο στην εποχή της πληροφορίας. Ωστόσο, ένα πρόβλημα είναι ότι είναι δύσκολο να διαδοθεί ψηφιακό περιεχόμενο στο δίκτυο Blockchain λόγω της περιορισμένης χωρητικότητας μεταφόρτωσης στο Blockchain. Η ακεραιότητα και η διαφάνεια του Blockchain θεωρούνται επίσης ως αδύναμα σημεία όσον αφορά το απόρρητο. Το ψηφιακό περιεχόμενο που διαπραγματεύεται διαθέτει ένα ψηφιακό δακτυλικό αποτύπωμα που

έχει εισαχθεί, οπότε αν υπάρξει παράνομη διαρροή, ο προορισμός μπορεί να εντοπιστεί. Επιπλέον, το περιεχόμενο είναι κρυπτογραφημένο και διαπραγματεύεται και μόνο ο νόμιμος χρήστης μπορεί να χρησιμοποιήσει το ψηφιακό περιεχόμενο, εξασφαλίζοντας έτσι το εισόδημα για τον νόμιμο συγγραφέα περιεχομένου. Στη συνέχεια, το δίκτυο on-chain έχει άδεια χρήσης ψηφιακού περιεχομένου και εκτελείται μια διαδικασία επαλήθευσης χρησιμοποιώντας έναν αλγόριθμο συναίνεσης. Ο εξουσιοδοτημένος καταναλωτής δημιουργεί ένα μυστικό μπλοκ της συναλλαγής του και το καταγράφει μόνο στο βιβλίο τους. Σε ένα ιδιωτικό μέρος, η μυστική δημιουργία μπλοκ εξασφαλίζει την προστασία της ιδιωτικής ζωής και επιλύει την υπερφόρτωση του δικτύου που μπορεί να συμβεί κατά τη μεταφόρτωση ψηφιακού περιεχομένου στο Blockchain. Τέλος, μέσω της επαλήθευσης και της συμφωνίας όλων των συμμετεχόντων στο Blockchain δημιουργείται και καταγράφεται στο βιβλίο για να ολοκληρώσει τη συναλλαγή. Κατά συνέπεια, προτείνουμε το σύστημα SBBC κατάλληλο για περιβάλλοντα συναλλαγών ψηφιακού περιεχομένου και ένα ασφαλές και αξιόπιστο σύστημα μέσω ενός αλγορίθμου συναίνεσης σε τέτοια περιβάλλοντα (Heo et al, 2021).

Ακόμη, το Blockchain έχει εφαρμογές στο περιβάλλον. Η επιτόπια παρακολούθηση της περιβαλλοντικής παρακολούθησης (OCEM) μπορεί να βοηθήσει στη διέγερση των συμπεριφορών των φορέων κατασκευής όσον αφορά τις εκπομπές ρύπων και την προστασία του περιβάλλοντος. Τα τρέχοντα συστήματα OCEM, ωστόσο, χτίστηκαν χρησιμοποιώντας μια κεντρική αρχιτεκτονική, όπως η τοπική βάση δεδομένων της κυβέρνησης, η οποία οδηγεί σε ανισορροπία και διαφορές μεταξύ των πολλαπλών ενδιαφερομένων. Όταν δεν υπάρχουν αξιόπιστα αρχεία δεδομένων για να δικαιολογήσουν τη συμμόρφωση των κατασκευαστικών εταιρειών, για παράδειγμα, τα επιχειρήματα ή ακόμη και οι συγκρούσεις μπορεί να προκύψουν μεταξύ γειτονικών κατοίκων και των εργολάβων. Το Blockchain έχει τη δυνατότητα να είναι μια αξιόπιστη πλατφόρμα για την παρακολούθηση του περιβάλλοντος λόγω της αποκέντρωσης, της αμετάβλητης, της διαφάνειας και της αυτόνομης επιβολής των συμφωνιών (Zhong et al, 2022).

Επιπλέον, αυτή η νέα τεχνολογία έχει αναπτυχθεί για να διακόψει μια ποικιλία πεδίων που βασίζονται σε δεδομένα, συμπεριλαμβανομένου του τομέα της υγείας. Ωστόσο, το Blockchain αναφέρεται στην τεχνολογία κατανεμημένης βιβλιοθήκης, η οποία αποτελεί καινοτομία στην καταγραφή και την κοινή χρήση πληροφοριών χωρίς αξιόπιστο τρίτο (Liu et al, 2020).

Αξίζει να σημειωθεί ότι το Internet of Things (IoT) και οι τεχνολογίες Blockchain χρησιμοποιούνται σε μεγάλο βαθμό για την ηλεκτρονική φροντίδα. Στην υγειονομική περίθαλψη, οι συσκευές IoT έχουν τη δυνατότητα να παρέχουν αισθητήρια δεδομένα σε πραγματικό χρόνο από τους ασθενείς για να υποβληθούν σε επεξεργασία και να αναλυθούν. Τα συλλεχθέντα δεδομένα IoT υποβάλλονται σε κεντρικό υπολογισμό, επεξεργασία και αποθήκευση. Αυτή η συγκέντρωση μπορεί να είναι προβληματική, καθώς μπορεί να είναι ένα ενιαίο σημείο αποτυχίας, δυσπιστίας, χειρισμός δεδομένων και παραβίαση και φοροδιαφυγή για την προστασία της ιδιωτικής ζωής. Το Blockchain μπορεί να λύσει τέτοια σοβαρά προβλήματα παρέχοντας αποκεντρωμένο υπολογισμό και αποθήκευση για δεδομένα IoT. Ως εκ τούτου, οι τεχνολογίες ενσωμάτωσης IoT και Blockchain μπορούν να γίνουν μια λογική επιλογή για το σχεδιασμό ενός αποκεντρωμένου συστήματος ηλεκτρονικής φροντίδας με βάση το IoT. Σε αυτό το άρθρο, πρώτον, δίνουμε ένα σύντομο υπόβαθρο στο Blockchain. Δεύτερον, οι δημοφιλείς αλγόριθμοι συναίνεσης που χρησιμοποιούνται στο Blockchain συζητούνται στο πλαίσιο της ηλεκτρονικής υγείας. Τέλος, οι πλατφόρμες Blockchain εξετάζονται για την καταλληλότητά τους στη φροντίδα ηλεκτρονικής υγείας με βάση το IoT (Ray et al, 2020).

1.5 Κατηγορίες Blockchain

Μια γενική ταξινόμηση χωρίζει το Blockchain σε τρεις κατηγορίες. Πιο συγκεκριμένα σε δημόσιο Blockchain, σε Blockchain κοινοπραξίας και σε ιδιωτικού Blockchain (Korpela et al, 2017):

- Οι δημόσιες αλυσίδες μπλοκ θεωρούνται ως ένα είδος αποκεντρωμένης αλυσίδας μπλοκ χωρίς άδεια στην οποία οι πληροφορίες είναι εμφανίσιμες για όλα τα μέλη του δικτύου και όλοι μπορούν να συμμετέχουν στην αποδοχή τους. Το Bitcoin και το Ethereum αποτελούν παραδείγματα δημόσιου Blockchain. Αυτός ο τύπος Blockchain είναι ασφαλής λόγω του μηχανισμού συναίνεσης που επιτυγχάνει συμφωνία μεταξύ όλων των ομότιμων. Αυτοί οι αλγόριθμοι συναίνεσης περιλαμβάνουν απόδειξη εργασίας (PoW) και απόδειξη στοιχήματος (PoS) (Bamakan et al, 2020).
- Οι μπλοκ αλυσίδες κοινοπραξίας είναι επίσης γνωστές ως ομοσπονδιακές αλυσίδες μπλοκ στις οποίες οι πληροφορίες είναι εμφανίσιμες για όλους τους ανθρώπους, αλλά η αλλαγή και η αποδοχή τους είναι δυνατή μόνο για καθορισμένες ομάδες. Για παράδειγμα, η παρουσίαση προϊόντων μάρκετινγκ μέσω Blockchain. Τα Blockchains κοινοπραξιών χρησιμοποιούνται κυρίως στον τραπεζικό τομέα. Εδώ, η ιδέα είναι να κατανεμηθεί η εξουσία σε έναν αριθμό αρχών αντί να υπάρχει μια ενιαία πλήρης αρχή ελέγχου για τη λήψη

μιας συλλογικής και αμερόληπτης απόφασης. Τα R3 (Τράπεζες), EWF (Ενέργεια) και B3i (Ασφάλειες) είναι μερικά παραδείγματα Blockchain κοινοπραξιών (Dib et al, 2018).

- Οι ιδιωτικές αλυσίδες μπλοκ είναι επιτρεπόμενες αλυσίδες μπλοκ στις οποίες οι πληροφορίες είναι εμφανίσιμες για μια ειδική ομάδα και η αποδοχή της αλλαγής είναι δυνατή μόνο από εξουσιοδοτημένη ομάδα, π.χ. σύστημα μισθοδοσίας μέσω Blockchain. Πρόκειται για ένα κεντρικό Blockchain που υπάρχει μια κεντρική αρχή που καθορίζει την άδεια για το ποιος μπορεί να διαβάζει, να γράφει ή να συμμετέχει στο Blockchain. Ως εκ τούτου, ο μηχανισμός συναίνεσης στις ιδιωτικές αλυσίδες μπλοκ ορίζεται από μια ενιαία κεντρική αρχή (Bamakan et al, 2020).

Αυτά τα τρία είδη Blockchain έχουν διαφορές με βάση τον τρόπο επίτευξης συναίνεσης μεταξύ των συμμετεχόντων. Για παράδειγμα, στο δημόσιο Blockchain όλοι οι εξορύκτες καθορίζουν τη συναίνεση, ωστόσο, στο Blockchain κοινοπραξίας και στο private Blockchain, ο συναινετικός προσδιορισμός μπορεί να γίνει από ένα επιλεγμένο σύνολο κόμβων ή έναν οργανισμό, αντίστοιχα (Bamakan et al, 2020).

1.6 Blockchain και κρυπτονομίσματα

1.6.1 Bitcoin

Το Bitcoin είναι ένα από τα πιο επιτυχημένα σενάρια εφαρμογής του Blockchain μέχρι στιγμής. Μέχρι το 2018, ο αριθμός των Bitcoin που είχαν εξορυχθεί και ήταν σε κυκλοφορία ήταν περίπου 17 εκατομμύρια, και η παγκόσμια οικονομία Bitcoin είναι 185,8 δισεκατομμύρια δολάρια, περίπου το μέγεθος του ΑΕΠ της Νέας Ζηλανδίας το 2016. Με άλλα λόγια, το αποκεντρωμένο Bitcoin έχει δημιουργήσει ένα παγκόσμια οικονομία με το μέγεθος μιας μεσαίου μεγέθους αναπτυγμένης χώρας που βασίζεται απλώς στην εμπιστοσύνη και τη συναίνεση που επικυρώνεται από αλγόριθμους. Ως εκ τούτου, εκτιμάται ότι περίπου το 10% του παγκόσμιου ΑΕΠ θα είναι αποθηκευμένο σε Blockchain μέχρι το 2027 (Nakamoto, 2017).

Το Bitcoin και τα περισσότερα άλλα κρυπτονομίσματα διαφέρουν από τα παραδοσιακά ηλεκτρονικά μετρητά στις ακόλουθες πέντε πτυχές. Πρώτον, το Bitcoin είναι πλήρως αποκεντρωμένο χωρίς κεντρικό έλεγχο ή ιεραρχική δομή. Στην πραγματικότητα, το Bitcoin ελέγχεται από κατανεμημένους αλγόριθμους συναίνεσης που εκτελούνται μεταξύ των υπολογιστικών κόμβων σε δίκτυα P2P. Τα παραδοσιακά ηλεκτρονικά μετρητά, ωστόσο, χρειάζονται συνήθως κεντρικούς παρόχους υπηρεσιών και, επομένως, ελέγχονται κεντρικά από κυβερνήσεις ή συγκεκριμένες εταιρείες. Δεύτερον,

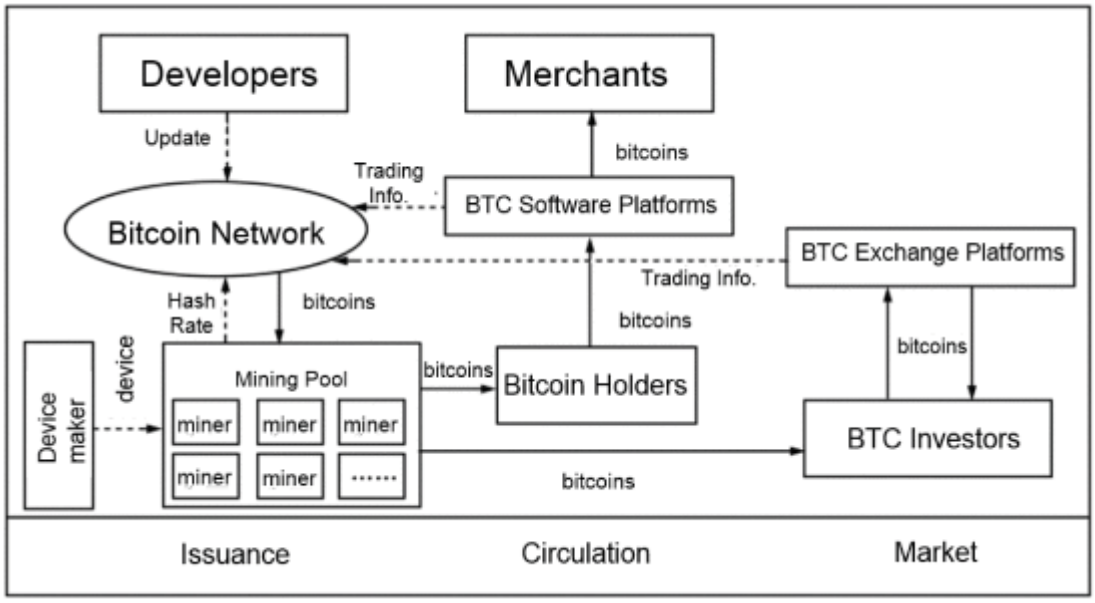
το Bitcoin είναι ψευδο-ανώνυμο όπως το ηλεκτρονικό ταχυδρομείο. Κάποιος μπορεί να γνωρίζει τη διεύθυνση ενός χρήστη Bitcoin, αλλά δεν μπορεί να γνωρίζει ακριβώς ποιος είναι. Αντίθετα, τα περισσότερα παραδοσιακά ηλεκτρονικά μετρητά είναι ανώνυμα και οι ταυτότητες των χρηστών θα καταγράφονται από τους κεντρικούς παρόχους υπηρεσιών. Τρίτον, το Bitcoin έχει περιορισμένη έκδοση νομίσματος με ανώτατο όριο περίπου 21 εκατομμύρια bitcoin. Ενώ τα περισσότερα παραδοσιακά ηλεκτρονικά μετρητά έχουν απεριόριστη έκδοση νομισμάτων. Ο κεντρικός πάροχος υπηρεσιών μπορεί να λάβει την απόφασή του να αυξήσει ή να μειώσει την προσφορά μετρητών, κάτι που μπορεί να προκαλέσει πληθωρισμό ή αποπληθωρισμό. Τέταρτον, το Bitcoin είναι ανοιχτού κώδικα για το κοινό. Ο καθένας μπορεί να ελέγξει τον πηγαίο κώδικα του Bitcoin και έτσι ο καθένας από αυτούς θα κατανοήσει τους υποκείμενους μηχανισμούς της έκδοσης Bitcoin. Ωστόσο, τα περισσότερα παραδοσιακά ηλεκτρονικά μετρητά είναι κλειστού κώδικα και η κρίσιμη επιχειρηματική λογική παραμένει πάντα μυστική στους χρήστες. Τέλος, το ίδιο το Bitcoin δεν έχει αξία, είναι μόνο μια ακολουθία μηδενικών και μονάδων. Ωστόσο, το Bitcoin μπορεί να αποκτήσει αξία αυξάνοντας τους χρήστες. Όσο περισσότεροι χρήστες εμπιστεύονται και χρησιμοποιούν το Bitcoin, τόσο μεγαλύτερη αξία θα έχει το Bitcoin (Yuan et al, 2018).

Όπως αναφέρθηκε, το πρώτο μπλοκ Blockchain Bitcoin, γνωστό και ως, το genesis block, δημιουργήθηκε στις 4 Ιανουαρίου 2009 από τον Nakamoto, ο οποίος έστειλε 10 bitcoin σε έναν κρυπτογράφο Finney μία εβδομάδα αργότερα. Αυτή θεωρείται ευρέως ως η πρώτη συναλλαγή στην ιστορία του Bitcoin. Το Bitcoin είναι στην ουσία ένα ηλεκτρονικό μετρητό που δημιουργείται στα κατανεμημένα συστήματα. Η έκδοση του Bitcoin βασίζεται σε έναν συναινετικό ανταγωνισμό μεταξύ των κατανεμημένων κόμβων δικτύου, γνωστό ως εξόρυξη με βάση την απόδειξη της εργασίας (PoW), αντί για μια συγκεκριμένη κεντρική αρχή. Στη διαδικασία συναίνεσης που βασίζεται σε PoW, κάθε υπολογιστικός κόμβος στο δίκτυο P2P συνεισφέρει τον υπολογιστικό του πόρο (CPU) και ανταγωνίζεται για να λύσει ένα μαθηματικά δύσκολο παζλ με δυναμικά ρυθμιζόμενες δυσκολίες. Πιο συγκεκριμένα, σε κάθε γύρο της διαδικασίας συναίνεσης, νέες συναλλαγές Bitcoin θα μεταδίδονται στο δίκτυο P2P. Κάθε κόμβος συνεχίζει να ακούει το δίκτυο και προσθέτει τις ληφθείσες συναλλαγές σε μια δεξαμενή μνήμης. Κάθε κόμβος ανταγωνίζεται για να υπολογίσει ένα nonce που ικανοποιεί ορισμένες απαιτήσεις. Ο εξορύκτης που θα βρει για πρώτη φορά με επιτυχία ένα τέτοιο σωστό nonce θα κερδίσει τον διαγωνισμό συναίνεσης και επίσης θα κερδίσει το δικαίωμα δημιουργίας του επόμενου νέου μπλοκ. Ο νικητής θα συσκευάσει τις συναλλαγές στη δεξαμενή μνήμης σε ένα νέο μπλοκ, εν μέρει σύμφωνα με μια φθίνουσα σειρά των σχετικών τελών συναλλαγής και, στη συνέχεια, θα μεταδώσει αυτό το νέο μπλοκ σε

ολόκληρο το δίκτυο Blockchain. Το μπλοκ θα γίνει αποδεκτό από άλλους κόμβους εάν και μόνο εάν οι συναλλαγές σε αυτό είναι έγκυρες και δεν έχουν ληφθεί πριν. Τέλος, άλλοι κόμβοι προσαρτούν αυτό το μπλοκ στην κύρια αλυσίδα και ξεκινούν τον επόμενο γύρο της διαδικασίας συναίνεσης που ανταγωνίζονται για το δικαίωμα συσκευασίας νέων συναλλαγών. Σε αυτή τη διαδικασία, το σύστημα Bitcoin θα δημιουργήσει μια συγκεκριμένη ποσότητα bitcoin ως ανταμοιβή στον νικητή εξορύκτη και επίσης ως κίνητρο για να ενθαρρύνει άλλους εξορύκτες να συνεχίσουν να συνεισφέρουν την υπολογιστική τους ισχύ. Η διαδικασία κυκλοφορίας του Bitcoin θα διασφαλίζεται με κρυπτογραφία, με κάθε συναλλαγή Bitcoin να κατακερματίζεται, να κρυπτογραφείται και να εγγράφεται στο καθολικό Blockchain μετά από επικύρωση από όλους τους εξορύκτες. Εν τω μεταξύ, η συναλλαγή μπορεί να προγραμματιστεί και να ελεγχθεί από σενάρια που βασίζονται σε αλγόριθμους και πλήρη έξυπνα συμβόλαια μη Turing, έτσι ώστε να πραγματοποιηθεί η προγραμματιζόμενη και αυτόματη κυκλοφορία για το Bitcoin. Συνοψίζοντας, συμπεραίνεται ότι το Blockchain Bitcoin έχει συνήθως τα ακόλουθα πέντε βασικά στοιχεία, δηλαδή ένα δημόσιο κοινόχρηστο καθολικό Blockchain, ένα κατανεμημένο σύστημα δικτύωσης P2P, έναν αποκεντρωμένο αλγόριθμο συναίνεσης, έναν καλά σχεδιασμένο μηχανισμό οικονομικών κινήτρων και προγραμματιζόμενα έξυπνα συμβόλαια (Nakamoto, 2017).

Το Bitcoin, όπως και τα περισσότερα άλλα κρυπτονομίσματα, είναι ένα αυτόνομο οικοσύστημα που αποτελείται από την έκδοση, την κυκλοφορία και την αγορά ανταλλαγής bitcoin, όπως απεικονίζεται στην **Εικόνα 9**. Στο κομμάτι της έκδοσης, το δίκτυο Bitcoin διατηρείται και ενημερώνεται από τους προγραμματιστές και το δίκτυο λαμβάνει υπολογιστική ισχύ βασισμένη σε hash από το mining pool ή μεμονωμένους εξορύκτες και παράγει Bitcoin ως ανταμοιβές σε αυτούς τους εξορύκτες. Οι εξορύκτες μπορούν να συμμετάσχουν στη διαδικασία εξόρυξης μεμονωμένα, και μπορούν επίσης να συνεργαστούν μπαίνοντας στο mining pool ώστε να αυξηθεί η πιθανότητα επιτυχούς δημιουργίας μπλοκ. Ο κατασκευαστής συσκευών παράγει και πουλά υπολογιστές εξόρυξης στους ανθρακωρύχους. Στο κομμάτι της κυκλοφορίας, οι κάτοχοι ή οι χρήστες Bitcoin αγοράζουν συγκεκριμένους τύπους αγαθών ή υπηρεσιών από τους εμπόρους μέσω των πλατφορμών λογισμικού Bitcoin, όπως πορτοφόλια Bitcoin. Οι πληροφορίες συναλλαγών θα μεταδοθούν στο δίκτυο Bitcoin και θα επικυρωθούν επίσης από τους εξορύκτες. Στο κομμάτι της αγοράς συναλλάγματος, καθώς η τιμή του Bitcoin παρουσιάζει συχνές διακυμάνσεις, γεγονός που οδηγεί σε μια καλή επενδυτική ευκαιρία για τους επενδυτές. Έτσι θα αγοράζουν και θα πωλούν bitcoin από την πλατφόρμα ανταλλαγής Bitcoin και οι πληροφορίες συναλλαγών θα

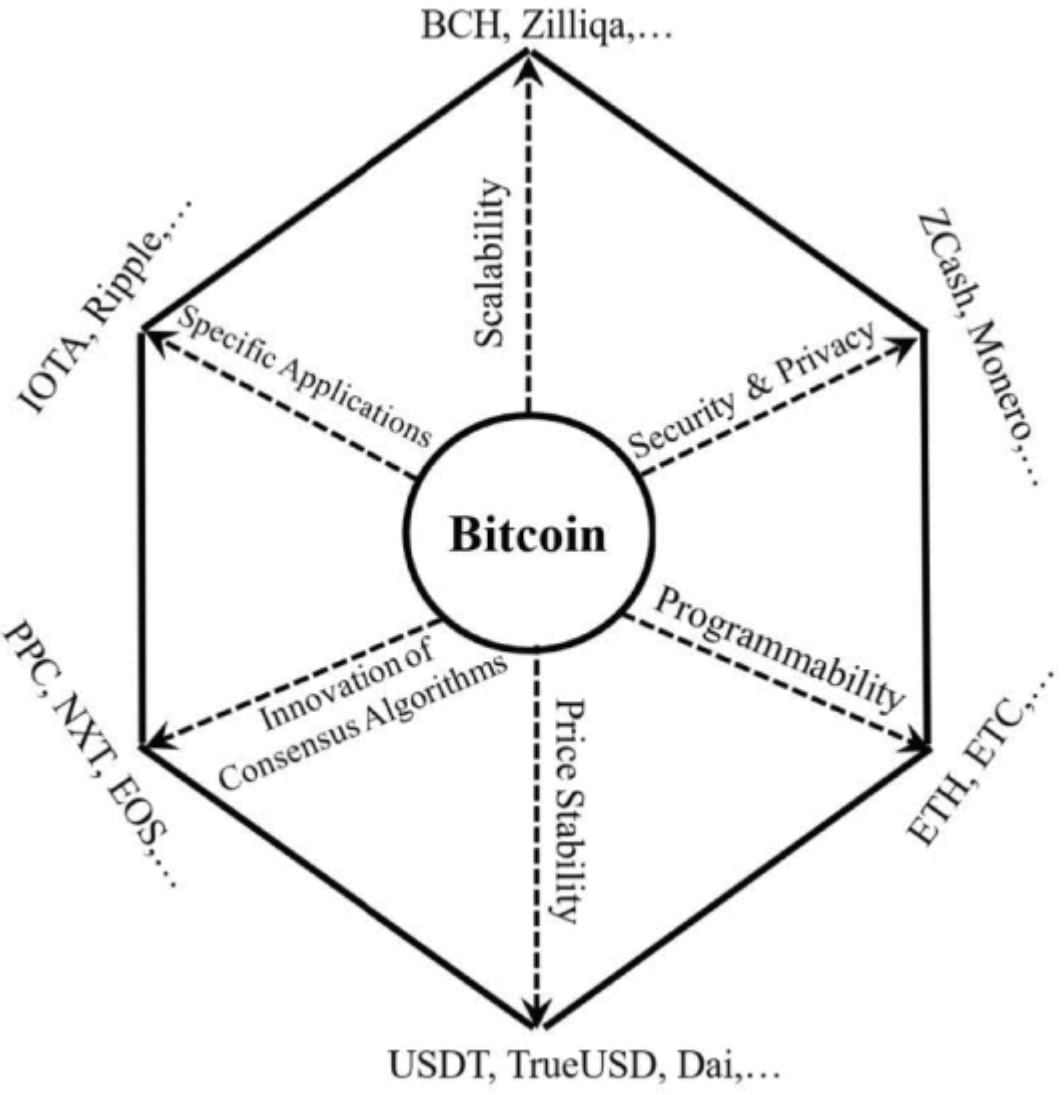
μεταδίδονται επίσης στο δίκτυο Bitcoin και θα επικυρώνονται από τους εξορύκτες (Yuan et al, 2018).



Εικόνα 9: Οικοσύστημα Bitcoin (Yuan et al, 2018).

Εμπνευσμένα από τη μεγάλη επιτυχία του Bitcoin, χιλιάδες άλλα κρυπτονομίσματα που τροφοδοτούνται από Blockchain εμφανίζονται και αναπτύσσονται γρήγορα σε αυτή τη νέα αγορά. Τα περισσότερα από αυτά τα κρυπτονομίσματα, γνωστά και ως altcoins, επινοούνται με στόχο τη βελτίωση της απόδοσης του συστήματος Bitcoin. Επί του παρόντος, υπάρχουν έξι κύριες διαστάσεις και κατευθύνσεις στην καινοτομία των altcoin, όπως φαίνεται στην **Εικόνα 10**. Η πρώτη διάσταση εστιάζει στην επεκτασιμότητα. Για παράδειγμα, το Bitcoin cash, που διαχωρίζεται από την αλυσίδα μπλοκ Bitcoin, επεκτείνει το μέγεθος του μπλοκ από 1 σε 8 MB. Αυτό επιτρέπει περισσότερες συναλλαγές να συσκευάζονται σε ένα ενιαίο μπλοκ σε κάθε γύρο συναινετικού ανταγωνισμού, και έτσι έχει ως αποτέλεσμα βελτιωμένη ικανότητα επεξεργασίας συναλλαγών και μειωμένο χρόνο στην επιβεβαίωση της συναλλαγής. Η Zilliqa μπορεί να βελτιώσει την απόδοση χρησιμοποιώντας την τεχνική κοινής χρήσης δικτύου, η οποία μπορεί να χωρίσει αυτόματα το δίκτυο Blockchain σε πολλά θραύσματα που επικυρώνουν τις συναλλαγές παράλληλα. Η δεύτερη διάσταση στοχεύει στη βελτίωση της ασφάλειας και της προστασίας της ιδιωτικής ζωής με κρυπτογραφικές τεχνικές, συμπεριλαμβανομένης της απόδειξης μηδενικής γνώσης και της ομομορφικής κρυπτογράφησης. Παραδείγματα περιλαμβάνουν το ZCash (ZEC)

και το Monero (XMR), μεταξύ άλλων. Η τρίτη διάσταση ενισχύει τη δυνατότητα προγραμματισμού των συστημάτων Blockchain και το πιο γνωστό παράδειγμα είναι το ETH, το οποίο υποστηρίζει πλήρεις έξυπνες συμβάσεις Turing και στη συνέχεια DApps. Η τέταρτη διάσταση στοχεύει στη σταθερότητα των τιμών. Για παράδειγμα, το USDT και άλλα νομίσματα Tether είναι εγκεκριμένα από και ισοδύναμα σε αξία με το δολάριο ΗΠΑ και μπορούν να βοηθήσουν στη διευκόλυνση της μεταφοράς εθνικών νομισμάτων, να παρέχουν στους χρήστες μια σταθερή εναλλακτική λύση στο Bitcoin. Η πέμπτη διάσταση βασίζεται στην καινοτομία συναινετικών αλγορίθμων, όπως το PeerCoin και το EOS. Τέλος, ο έκτος τύπος κρυπτονομισμάτων είναι αφιερωμένος σε συγκεκριμένα σενάρια εφαρμογών, όπως το IOTA προσανατολισμένο στο Internet of Things, το Ripple που χρησιμοποιείται για παγκόσμιο χρηματοοικονομικό διακανονισμό, καθώς και το Augur που δημιουργήθηκε για εφαρμογές στην αγορά προβλέψεων (Yuan et al, 2018).



Εικόνα 10: Έξι διαστάσεις στην καινοτομία κρυπτονομισμάτων (Yuan et al, 2018).

1.6.2 Ethereum

Όπως αναφέρθηκε, οι κατανεμημένες πλατφόρμες συναίνεσης που βασίζονται σε Blockchain έχουν σημειώσει μια σταθερή ανάπτυξη τα τελευταία χρόνια. Σε αυτό το πλαίσιο, το κρυπτονόμισμα είναι μία από τις κύριες εφαρμογές αυτής της τεχνολογίας, ενώ το Bitcoin είναι η πρώτη και πιο αξιοσημείωτη πλατφόρμα που βασίζεται σε Blockchain. Από την άνοδο του Bitcoin και παρά τη φήμη του, εμφανίστηκαν πολλές άλλες πλατφόρμες που βασίζονται σε Blockchain. Το Bitcoin εξακολουθεί να οδηγεί στην κατάταξη των πλατφορμών κρυπτονομισμάτων που βασίζονται σε Blockchain. Ωστόσο, χάνει τον τομέα του στην αγορά. Για παράδειγμα, το Ethereum, μια πιο πρόσφατη πλατφόρμα συναίνεσης που βασίζεται σε Blockchain, κερδίζει σημαντικό μερίδιο αγοράς στο σενάριο των κρυπτονομισμάτων (Buterin, 2014).

Το Ethereum έκανε το ντεμπούτο του το 2015 και εμφανίστηκε ως βασικός παίκτης στο πλαίσιο των κρυπτονομισμάτων που βασίζεται σε Blockchain μέχρι τα τέλη του 2017 και τις αρχές του 2018. Έχει διαταράξει την τεχνολογία Blockchain εισάγοντας την έννοια των έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια είναι αυτοεκτελέσιμα προγράμματα με προκαθορισμένους κανόνες. Τον τελευταίο καιρό, το Ethereum είναι η δεύτερη πιο χρησιμοποιούμενη πλατφόρμα κρυπτονομισμάτων και οδηγεί στην αγορά των έξυπνων συμβολαίων. Πράγματι, η μελέτη των Sigaki et al, 2019 θεώρησε ότι το Ethereum, είναι πιο αποτελεσματικό από το Bitcoin (όσον αφορά την υπόθεση της αποτελεσματικής αγοράς). Παρά το πρόσφατο και αυξανόμενο ενδιαφέρον για το Blockchain, εξακολουθεί να λείπει η εις βάθος ανάλυση των πραγματικών συστημάτων που χρησιμοποιούν αυτήν την τεχνολογία ως δομικό στοιχείο. Οι περισσότερες από τις υπάρχουσες εργασίες επικεντρώνονται στο Bitcoin και, μόνο πολύ πρόσφατες εργασίες αφορούν συγκεκριμένα χαρακτηριστικά νέων πλατφορμών, όπως το Ethereum. Επιπλέον, τα συστήματα κρυπτονομισμάτων που βασίζονται σε Blockchain είναι εξαιρετικά δυναμικά. Οι εσωτερικοί τους μηχανισμοί και οι αλγόριθμοι συναίνεσης εξελίσσονται. Οι χρήστες αλλάζουν επίσης τα ενδιαφέροντά τους σε μια δεδομένη πλατφόρμα, η οποία με τη σειρά της αντανακλά τη συμπεριφορά τους (Sigaki et al, 2019).

Κατά την ανάλυση της χρονικά μεταβαλλόμενης συμπεριφοράς ενός σύνθετου συστήματος, μπορεί κανείς να εντοπίσει μια ακολουθία συναλλαγών στο σύστημα κρυπτονομισμάτων που βασίζεται στο Ethereum, να συνδέσει διακριτές περιόδους, δεδομένες συγκεκριμένες συναλλαγές ή συμβόλαια και να καθορίσει συγκεκριμένες σημαντικές περιόδους του δικτύου (Christidis et al, 2016).

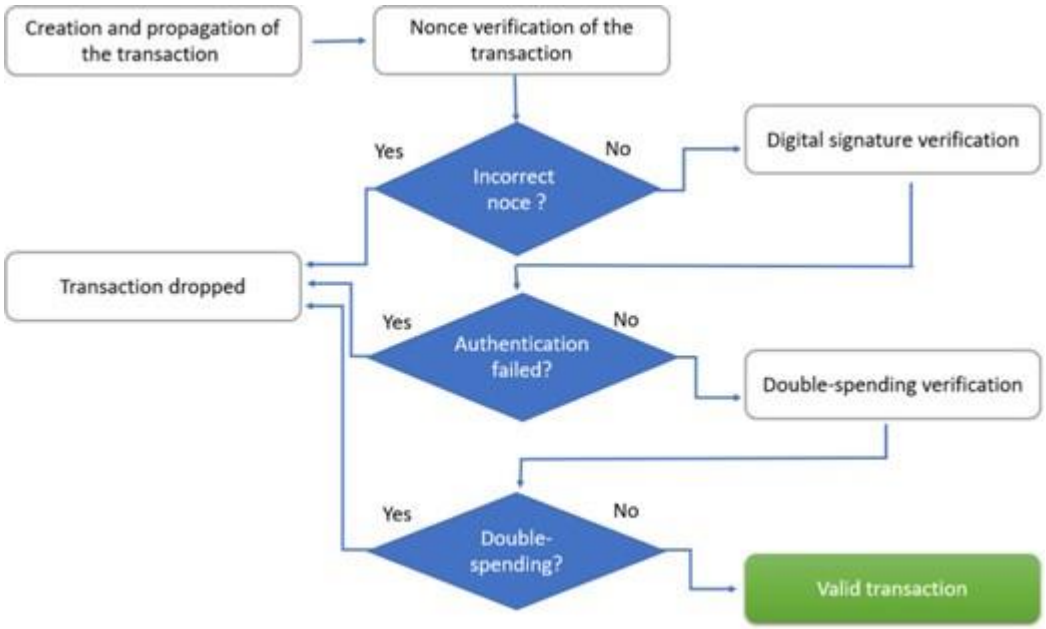
Γενικά, το Ethereum λειτουργεί όπως οι περισσότερες πλατφόρμες που βασίζονται σε Blockchain. Είναι μια πλατφόρμα με πολλά χαρακτηριστικά παρόμοια με το Bitcoin αφού βασίζεται σε συναλλαγές και χρησιμοποιεί ως δομή το Blockchain. Για παράδειγμα, σε μια συναλλαγή, οι απλοί χρήστες ανταλλάσσουν αξία (χρήματα) μεταξύ τους. Αρκετές συναλλαγές ομαδοποιούνται και επικυρώνονται από ειδικούς χρήστες, γνωστούς και ως miners. Αυτές οι ομάδες συναλλαγών, γνωστές ως μπλοκ, συνδέονται γραμμικά σε μια αλυσίδα μπλοκ (Sigaki et al, 2019).

Το Blockchain Ethereum ορίζεται ως ένα πρότυπο μηχανής συναλλαγών ενιαίας κοινής κατάστασης. Έτσι, το Ethereum είναι μια γενική υλοποίηση αυτού του παραδείγματος. Το Ethereum είναι η πρώτη πλατφόρμα που βασίζεται σε Blockchain που εφαρμόζει μια πλήρη κατανεμημένη συναινετική μηχανή Turing μέσω της τεχνολογίας έξυπνων συμβολαίων. Η πλατφόρμα Ethereum αποτελείται από αποκεντρωμένες εικονικές μηχανές, γνωστές ως Ethereum Virtual Machines (EVM), οι οποίες εκτελούν έξυπνες συμβάσεις. Ένα έξυπνο συμβόλαιο προσδιορίζεται από μια διεύθυνση και ενεργοποιείται όταν η διεύθυνσή του αναφέρεται ως προορισμός από μια συναλλαγή. Μόλις ενεργοποιηθεί, το έξυπνο συμβόλαιο εκτελείται αυτόματα σε κάθε κόμβο δικτύου EVM (Christidis et al, 2016).

Υπάρχουν ειδικά αντικείμενα κατάστασης στο Ethereum, δηλαδή «λογαριασμοί». Οι μεταβάσεις κατάστασης σημαίνουν άμεση μεταφορά αξιών μεταξύ λογαριασμών. Υπάρχουν δύο τύποι λογαριασμών: λογαριασμοί εξωτερικής ιδιοκτησίας (EOA), που ελέγχονται από τα ιδιωτικά κλειδιά των χρηστών. και των λογαριασμών συμβολαίου, που ελέγχονται από τους κωδικούς συμβολαίου τους. Τα συμβόλαια είναι διευθύνσεις που ορίζονται τη στιγμή της δημιουργίας τους. Αυτά είναι ικανά να εκτελούν διάφορες λειτουργίες εκτός από τη μεταφορά αιθέρα μεταξύ λογαριασμών. Οι λογαριασμοί μπορούν να ανήκουν σε δύο τύπους χρηστών: miners και traders (δηλαδή απλούς χρήστες). Ένας χρήστης εξόρυξης στοχεύει στο οικονομικό κέρδος από τη διαδικασία εξόρυξης μπλοκ. Οι χρήστες εξόρυξης λαμβάνουν μια αμοιβή λόγω της υπολογιστικής τους εργασίας σε ένα μπλοκ. Ωστόσο, αυτή η τιμή μεταφέρεται μόνο μετά την εισαγωγή του μπλοκ στην αλυσίδα μπλοκ. Οι απλοί χρήστες, από την άλλη πλευρά, χρησιμοποιούν την πλατφόρμα Ethereum κυρίως για την εκτέλεση συμβάσεων ή για τη μεταφορά τιμών μεταξύ λογαριασμών. Ωστόσο, οι απλοί χρήστες και οι εξορύκτες ενδέχεται να ανταλλάξουν τους ρόλους τους (Zanelatto et al, 2020).

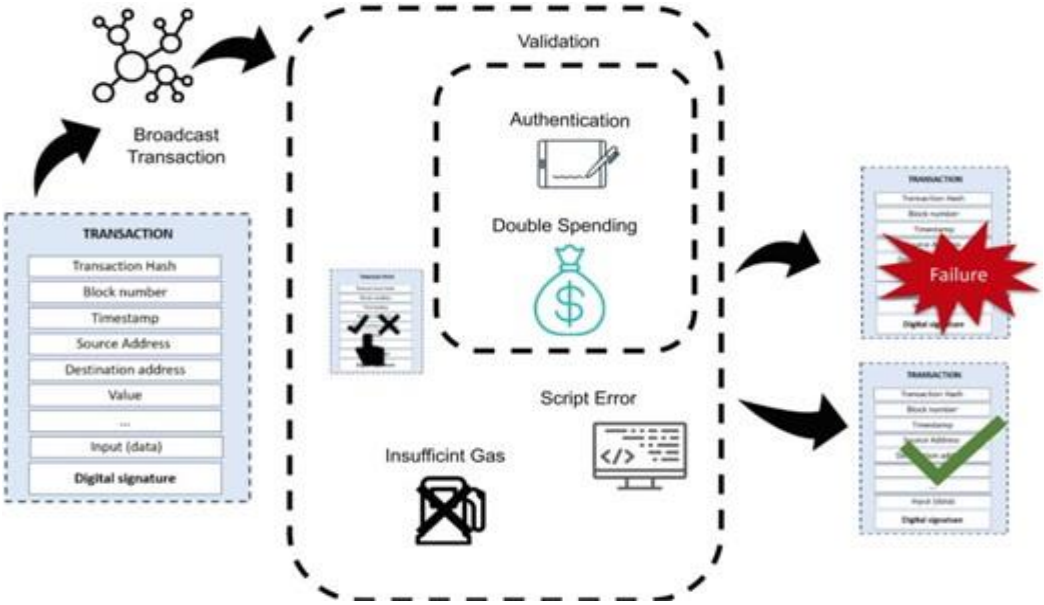
Όπως φαίνεται στην **Εικόνα 11**, οι συναλλαγές, αφού πραγματοποιηθούν, περνούν από διάφορα βήματα για να επικυρωθούν. Αυτά τα βήματα περιλαμβάνουν την επαλήθευση της ψηφιακής υπογραφής των χρηστών, την επαλήθευση του nonce

(ακέραιος αριθμός που αντιστοιχεί στο σύνολο των συναλλαγών που εκτελούνται από τον αποστολέα) της συναλλαγής,· επαλήθευση του ορίου αερίου που δεν πρέπει να είναι μικρότερο από το εγγενές αέριο, το οποίο είναι η ποσότητα αερίου που απαιτείται για την εκτέλεση της συναλλαγής· και, επαλήθευση του υπολοίπου του λογαριασμού του αποστολέα που πρέπει να έχει τουλάχιστον το κόστος συναλλαγής. Πιο συγκεκριμένα, το αέριο, στο Ethereum, είναι μια μέτρηση που χρησιμοποιείται για τον προσδιορισμό της μέγιστης υπολογιστικής εργασίας που θα δαπανηθεί για την επικύρωση μιας συναλλαγής. Η ποσότητα του αερίου και η τιμή του αερίου, που είναι η τιμή του Ethereum για κάθε μονάδα αερίου, αντιπροσωπεύει τη μέγιστη ποσότητα αιθέρα που σκοπεύει να ξοδέψει ένας χρήστης για την εξόρυξη της συναλλαγής του. Εάν το δηλωμένο αέριο είναι ανεπαρκές, η συναλλαγή δεν εξορύσσεται (Zanelatto et al, 2020).



Εικόνα 11: Διάγραμμα ροής διαδικασίας επαλήθευσης συναλλαγών (Zanelatto et al, 2020).

Η **Εικόνα 12** παρουσιάζει τα βήματα που ορίζουν την κατάσταση μιας συναλλαγής ως επιτυχημένη ή αποτυχημένη. Αυτές οι συναλλαγές (που δημιουργούνται από EOAs) εισάγονται στο Blockchain. Άλλες συναλλαγές, που ονομάζονται ανεπίσημα εσωτερικές συναλλαγές, δεν έχουν αρχεία (Zanelatto et al, 2020).



Εικόνα 12: Κατάσταση συναλλαγής στο Ethereum (Zanelatto et al, 2020).

Μόλις επικυρωθεί μια συναλλαγή, είναι διαθέσιμη για εισαγωγή σε ένα μπλοκ από έναν εξορύκτη. Αυτή η διαδικασία είναι παρόμοια με αυτή που συμβαίνει στο Bitcoin, όπου οι συναλλαγές εξορύσσονται πριν εισαχθούν στο Blockchain. Ωστόσο, το Ethereum έχει κάποιες διαφορές σε σύγκριση με το Bitcoin. Για παράδειγμα, το Ethereum ανταμείβει τους εξορύκτες που δεν εξόρυξαν με επιτυχία τη συναλλαγή. Σήμερα, το Ethereum εξακολουθεί να χρησιμοποιεί το γνωστό proof-of-work (PoW) που υιοθετείται από το Bitcoin. Ωστόσο, το Ethereum 2.0 πρόκειται να εφαρμόσει μια μετατόπιση πρωτοκόλλου από το PoW, στο Proof of Stake (PoS). Με μια ματιά, σε ένα PoS, αντί για εξορύκτες, οι επικυρωτές συναλλαγών, γνωστοί ως επικυρωτές, κλειδώνουν (ή ποντάρουν) την κρυπτογράφηση τους ως εγγύηση για το δικαίωμα επαλήθευσης συναλλαγών (Zanelatto et al, 2020).

1.6.3 Litecoin (LTC)

Το Litecoin (LTC) είναι ένα νόμισμα ανοιχτού κώδικα διανεμημένο κρυπτονόμισμα. Κυκλοφόρησε τον Οκτώβριο του 2011. Η συναίνεση του Litecoin βασίζεται στον αλγόριθμο Scrypt PoW χρησιμοποιώντας τον αλγόριθμο SHA-256 PoW που χρησιμοποιείται από το bitcoin. Συνήθως, ο χρυσός του bitcoin ορίζεται ως «ασήμι» (Emeç et al, 2020).

Διαφέρει από το Bitcoin με δύο τρόπους. Η χρήση του αλγόριθμου Scrypt PoW στο Litecoin είναι πολύ πιο γρήγορη από το Bitcoin. Ένα Blockchain σε bitcoin μπορεί να δημιουργηθεί κατά μέσο όρο σε 10 λεπτά. Στο Litecoin, χρειάζονται κατά μέσο όρο 2,5

λεπτά για να δημιουργηθεί ένα Blockchain. Μια άλλη διαφορετική πτυχή είναι το όριο προσφοράς. Είναι 84 εκατομμύρια σε Litecoin και όριο προσφοράς 21 εκατομμύρια σε Bitcoin [10]. Όταν δημιουργείται ένα μπλοκ στο Litecoin, λαμβάνεται μια διαφορετική κεφαλίδα μπλοκ κάθε φορά. Μια κεφαλίδα μπλοκ περιέχει τα ακόλουθα πεδία: Έκδοση, hashPrevBlock, hashMerkleRoot, Time, Bit, Nonce. Συνδυάζοντας ένα μόνο μπλοκ στο Litecoin, καταβάλλεται η ίδια προσπάθεια για να συνδυαστεί ένα μπλοκ 10.000 λειτουργιών. Το πεδίο Bits αντιπροσωπεύει τον στόχο χρησιμοποιώντας μια κωδικοποίηση κινητής υποδιαστολής. Χρησιμοποιούνται τρία byte για αυτήν την κωδικοποίηση και ένα 256 byte βάσης. Χρησιμοποιούνται μόνο 5 χαμηλότερα bit. Το Nonce ξεκινά από το 0 και αυξάνεται για κάθε κλήση προς συνάρτηση κατακερματισμού. Καθώς συμβαίνει η υπερχείλιση, το τμήμα extraNonce της διαδικασίας παραγωγής αυξάνεται, γεγονός που προκαλεί την αλλαγή της ρίζας Merkle. Απλώς κοιτάζοντας αυτές τις περιοχές, οι χρήστες συχνά επιλύουν το χάος το ένα μετά το άλλο και οι πιο γρήγοροι εξορύκτες θα κερδίζουν πάντα. Η κρυπτογράφηση (N = 1024, r = 1, p = 1 παράμετροι) χρησιμοποιείται για τον υπολογισμό των συνδυασμών εργασίας-στόχων και για όλους τους άλλους σκοπούς για τον έλεγχο του SHA-256d (SHA-256 δύο φορές). Κατά τον υπολογισμό των λειτουργιών κατακερματισμού, δίνεται ιδιαίτερη προσοχή στη σειρά των byte (Emeç et al, 2020).

1.6.4 Ripple (XRP)

Το Ripple κυκλοφόρησε το 2012 από την Ripple (Labs) Inc. Παρέχει μεταφορές κοντά στο νόμισμα, ανεξάρτητα από τη μορφή. Το κρυπτονόμισμα είναι το XRP. Στην πλατφόρμα Ripple, το XRP μπορεί να επεξεργαστεί περισσότερες από 1500 λειτουργίες ανά δευτερόλεπτο. Το Ripple χρησιμοποιεί τη δική του ιδιωτική συναίνεση για την επικύρωση συναλλαγών αντί για PoW ή PoS. Το ερώτημα πώς είναι το XRP ή πώς θα διανεμηθεί στο μέλλον παραμένει ασαφές (Emeç et al, 2020).

Στο XRP, η ψηφιακή υπογραφή αποδεικνύει ότι μια συναλλαγή είναι εξουσιοδοτημένη να ορίσει ένα συγκεκριμένο σύνολο ενεργειών. Μόνο υπογεγραμμένες συναλλαγές αποστέλλονται στο δίκτυο και εγκρίνονται. Κάθε ψηφιακή υπογραφή βασίζεται σε ένα κρυπτογραφημένο ζεύγος κλειδιών που σχετίζεται με τον λογαριασμό αποστολής. Ένα ζεύγος κλειδιών μπορεί να δημιουργηθεί χρησιμοποιώντας έναν από τους υποστηριζόμενους αλγόριθμους υπογραφής κρυπτογράφησης του XRP Ledger (Emeç et al, 2020).

Τα αντικείμενα του καθολικού έχουν ένα μοναδικό αναγνωριστικό στο XRP. Η ταυτότητα προκύπτει από την ανάμειξη του σημαντικού περιεχομένου του αντικειμένου με ένα αναγνωριστικό χώρου ονομάτων. Ο τύπος αντικειμένου καθολικού καθορίζει το αναγνωριστικό χώρου ονομάτων που θα χρησιμοποιηθεί και το περιεχόμενο που θα συμπεριληφθεί στο μικτό περιεχόμενο. Με αυτόν τον τρόπο, κάθε ταυτότητα γίνεται μοναδική. Το SHA-512 χρησιμοποιείται για τον υπολογισμό της τιμής κατακερματισμού και το αποτέλεσμα προστίθεται στα πρώτα 256 byte. Αυτός ο αλγόριθμος που ονομάζεται SHA-512 half παρέχει αποτελέσματα ασφαλείας παρόμοια με του SHA-256, αλλά λειτουργεί πιο γρήγορα σε επεξεργαστές 64-bit (Emeç et al, 2020).

1.6.5 Dash

Το Dash (DASH), γνωστό και ως Darkcoin, κυκλοφόρησε για πρώτη φορά τον Ιανουάριο του 2014. Με συνέπεια, χρησιμοποιείται ο αλγόριθμος X11 PoW. Εκτός από το PoW, το Dash χρησιμοποιεί επίσης υποδομή Masternode. Ο Masternode είναι ένας διακομιστής συνδεδεμένος στο δίκτυο Dash, ο οποίος εγγυάται ορισμένες ελάχιστες επιδόσεις για την εκτέλεση ορισμένων εργασιών με το PrivateSend και οι κλήσεις InstantSend μπορούν να γίνουν για να καθιερωθεί η εξουσία ψήφου ελέγχοντας την εγκυρότητα μιας συναλλαγής που αποστέλλεται χρησιμοποιώντας το δίκτυο masternode Dash και εάν αυτό υπάρχει, οι πληροφορίες μεταφέρονται στο δίκτυο. Αυτό σημαίνει ότι το Dash μπορεί να επεξεργαστεί σχεδόν αμέσως, όπως συναλλαγές με πιστωτική κάρτα (Emeç et al, 2020).

Το X11 έχει σχεδιαστεί και αναπτυχθεί για να κάνει τη δημιουργία ολοκληρωμένων κυκλωμάτων για συγκεκριμένες εφαρμογές (ASIC) πολύ πιο δύσκολη. Αυτή η προσέγγιση βασίζεται σε μεγάλο βαθμό. Στις αρχές του 2016, τα ASIC για το X11 αποτελούν πλέον σημαντικό μέρος της τρέχουσας πολυπλοκότητας του δικτύου, αλλά δεν μπορούν ακόμη να οδηγήσουν στο επίπεδο συγκέντρωσης που υπάρχει στο Bitcoin (Emeç et al, 2020).

Εμπνευσμένο από την αλυσιδωτή προσέγγιση του Quark, προστίθεται περισσότερη πολυπλοκότητα, αυξάνοντας τον αριθμό των κατακερματισμών. Ωστόσο, σε αντίθεση με το Quark, αντί να επιλέγουμε τυχαία ορισμένους κατακερματισμούς, είναι διαφορετικός από τον προσδιορισμό των μικτών περιηγήσεων ως a priori. Στον αλγόριθμο X11, 11 διαφορετικοί κατακερματισμοί χρησιμοποιούν περισσότερους από έναν γύρους, καθιστώντας έτσι ένα από τα ασφαλέστερα και πιο σύνθετα μείγματα κρυπτογράφησης που χρησιμοποιούνται σήμερα (Emeç et al, 2020).

1.6.6 Monero (XMR)

Το Monero (XMR) κυκλοφόρησε τον Απρίλιο του 2014. Το Monero έχει αναπτυχθεί κρυπτογραφικά για να διατηρεί τις λειτουργίες με απόλυτη ασφάλεια. Οι διευθύνσεις αποστολής και λήψης των δεδομένων και το ποσό των συναλλαγών που εκτελούνται κωδικοποιούνται στη διαδικασία για λόγους ασφαλείας (Vukolić, 2015).

Η συναίνεση του Monero βασίζεται στον αλγόριθμο CryptoNote PoW. Τα μη επιβεβαιωμένα κρυπτονομίσματα, όπως το Bitcoin και το Litecoin, βρίσκονται στη μαύρη λίστα. Εάν έχουν χρησιμοποιηθεί για παράνομες λειτουργίες στο παρελθόν, αυτό είναι για πάντα στη γραμμή αποκλεισμού. Σε αντίθεση με άλλα νομίσματα στην αγορά, το Monero (XMR) δεν έχει κυκλοφορήσει στο παρελθόν (Emeç et al, 2020).

Το Monero, σε αντίθεση με τον ασφαλή αλγόριθμο κατακερματισμού 256 bit (SHA-256) που χρησιμοποιείται από το Bitcoin, αποτρέπει την ανάπτυξη ASIC χρησιμοποιώντας έναν αλγόριθμο σκληρής μνήμης (CryptoNight) που κάνει την ανάπτυξη ASIC πιο δύσκολη από ό,τι. Οι μικτές συναρτήσεις είναι εργαλεία κρυπτογράφησης που μπορούν να δημιουργήσουν έναν μοναδικό αριθμό για κάθε καταχώρηση. Αυτοί οι αλγόριθμοι έχουν σχεδιαστεί για να προκαλούν μια εντελώς διαφορετική έξοδο με τυχόν αλλαγές στην είσοδο. Ο όρος "hash" χρησιμοποιείται για να αναφέρεται τόσο στην ίδια τη συνάρτηση όσο και στην έξοδο της για μια συγκεκριμένη είσοδο (Emeç et al, 2020).

Ως αποτέλεσμα, η εξόρυξη CPU και GPU είναι κατάλληλη για το Monero ακόμη και το 2018. Το Monero έχει δισεκατομμύρια διαθέσιμες συσκευές με δυνατότητα εξόρυξης. Είναι ακόμη δυνατή η εξόρυξη του Monero από οποιοδήποτε τηλέφωνο ή υπολογιστή με πρόγραμμα περιήγησης ιστού (Emeç et al, 2020).

1.6.7 NEO

Το NEO κυκλοφόρησε για πρώτη φορά ως έργο Antshares τον Φεβρουάριο του 2014. Αργότερα κυκλοφόρησε ως NEO τον Ιούνιο του 2017. Το NEO, μερικές φορές αναφέρεται ως το "Κινεζικό Ethereum". Το NEO, όπως το Ethereum και το Cardano, είναι μια πλατφόρμα στην οποία πραγματοποιούνται έξυπνες συμβάσεις και αποκεντρωμένες συναλλαγές. Το NEO είναι ένα έργο που δημιουργήθηκε με σκοπό μια «έξυπνη οικονομία» που τεχνικά δεν είναι κρυπτονόμισμα. Το NEO μπορεί να υποστηρίξει έως και 10.000 συναλλαγές ανά δευτερόλεπτο. Ως μηχανισμός συναίνεσης, χρησιμοποιείται το dBFT (Vukolić, 2015).

Το πρόβλημα του dBFT είναι το εξής.ότι υπάρχουν 9 στρατηγοί στη Βυζαντινή Αυτοκρατορία και περιβάλλουν την πόλη της Ρώμης. Κάθε στρατηγός έχει τον δικό του στρατό. Για να καταλάβουν τη Ρώμη, οι στρατηγοί πρέπει να δράσουν στρατηγικά. Αν κάποιος στρατηγός δεν εφαρμόσει τη συναινετική απόφαση, ο στρατός του θα ηττηθεί. Υπάρχουν δύο επιλογές επίθεσης και αποχώρησης και τους προσφέρεται να ψηφίζουν κάθε μέρα. Εάν η επιλογή υπερβαίνει το 50%, εφαρμόζεται η απόφαση. Κάθε στρατηγός βρίσκεται σε διαφορετική περιοχή. Ως εκ τούτου, οι στρατηγοί κοινοποιούν τις αποφάσεις τους μεταξύ τους με κούριερ. Αυτό το σύστημα έχει κάποια προβλήματα. Πρώτο πρόβλημα, οι Ρωμαίοι μπορούν να δωροδοκήσουν τους βυζαντινούς αγγελιαφόρους και μπορούν να μάθουν το σχέδιο. Δεύτερο πρόβλημα, μπορεί να υπάρχουν στρατηγοί που δεν έχουν συναίνεση. Τρίτο πρόβλημα, οι Ρωμαίοι μπορούν να δωροδοκήσουν για να αλλάξουν ψήφους σε οποιονδήποτε από τους αγγελιαφόρους. Το τέταρτο πρόβλημα, οι ταχυμεταφορείς μπορεί να παραδώσουν το μήνυμα λανθασμένα ή να μην παραδώσουν το μήνυμα. Το πρόβλημα είναι παρόμοιο με το πρόβλημα στα κατανεμημένα συστήματα υπολογιστών. Υπάρχουν πολλά πρωτόκολλα για την επίλυση αυτού του προβλήματος. Οι δημιουργοί του NEO επέλεξαν το dBFT. Επειδή, αυτή η μέθοδος έχει καλή επεκτασιμότητα και η επεκτασιμότητα είναι ένα πολύ σημαντικό ζήτημα (Emeç et al, 2020).

Η υποκείμενη λογική του dBFT μπορεί να εξηγηθεί ως: Ας υποθέσουμε ότι υπάρχουν εκπρόσωποι και πολίτες σε μια χώρα. Οι πολίτες ψηφίζουν εκλέγοντας τον εκπρόσωπο ως πρόεδρό τους. Ο επιλεγμένος εκπρόσωπος κάνει ό,τι θέλουν οι πολίτες και τους σώζει. Εάν οι πολίτες δεν είναι ικανοποιημένοι, μπορούν να αλλάξουν ομόφωνα τον εκπρόσωπο. Όταν γίνεται μια νέα πρόταση, ένας τυχαίος ομιλητής από κάθε ομάδα λέει τον αριθμό ευτυχίας στην κοινότητα και το αποτέλεσμα παρουσιάζεται στους συνέδρους. Εάν το αποτέλεσμα είναι μεγαλύτερο από 66% ή ίσο με 66%, και εάν οι εκπρόσωποι επαληθεύσουν το αποτέλεσμα, τότε αποδέχονται τη νέα πρόταση. Αυτή η αναλογία είναι η συναίνεση του Blockchain NEO. Εδώ, ο αριθμός ευτυχίας είναι η τιμή κατακερματισμού στο Blockchain NEO (Vukolić, 2015).

1.6.8 Cardano (ADA)

Το Cardano (ADA) κυκλοφόρησε τον Σεπτέμβριο του 2015. Αναπτύχθηκε ως πλατφόρμα για έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές όπως το Ethereum και το NEO. Ο Cardano πήρε πολλά μαθήματα από τις κοινότητες Bitcoin και Ethereum και στόχευσε στην ασφάλεια, την επεκτασιμότητα και τη διαλειτουργικότητα. Το νόμισμα του Cardanon είναι η ADA. Με την ADA, η αποστολή και η λήψη συναλλαγών

από ψηφιακά κεφάλαια μπορούν να πραγματοποιηθούν. Το Cardano είναι το πρώτο έργο Blockchain που σχεδιάστηκε από μια ομάδα με επικεφαλής ακαδημαϊκούς και μηχανικούς, που διαφέρει από το Ethereum και άλλα κρυπτονομίσματα. Η βάση της συναίνεσης Cardano βασίζεται στον αλγόριθμο PoS. Πιο ιδιαίτερο όνομα είναι Ouroboros. Στο πρωτόκολλο Ouroboros, κάθε ενότητα περιέχει ένα σύνολο εγκρίσεων. Τα μπλοκ παράγονται από αυτούς που ονομάζονται ηγέτες. Οι διαδικασίες που πρέπει να περιλαμβάνονται σε αυτά τα τμήματα πρέπει να εγκρίνονται από τον κατάλληλο αριθμό εγκρίσεων. Για τη δημιουργία ισορροπίας, οι εγκρίοντες ανταμείβονται από τους ηγέτες σε ορισμένες περιόδους (Emeç et al, 2020).

1.7 Ασφάλεια

Το Blockchain είναι ένα σύστημα που επιτρέπει στους χρήστες να συνδέονται σε διαφορετικά δίκτυα και να δημιουργούν μια σύνδεση μέσω αυτού του δικτύου. Υπάρχουν δύο τύποι συστημάτων Blockchain που ονομάζονται μη εξουσιοδοτημένα συστήματα και χορηγούμενα συστήματα. Τα τελευταία χρόνια, κρυπτονομίσματα όπως το Bitcoin και το Ethereum, που αποτελούν αντικείμενο περιέργειας από όλους, είναι μερικά παραδείγματα μη εξουσιοδοτημένων συστημάτων. Σε τέτοια συστήματα, οι συμμετέχοντες μπορούν να περιορίσουν τις συναλλαγές και να συμμετέχουν στη συναίνεση του Blockchain. Παραδείγματα χορηγούμενων συστημάτων περιλαμβάνουν το Hyperledger και το multichain. Σε τέτοια συστήματα, οι συμμετέχοντες πρέπει να λάβουν άδεια για τις δραστηριότητές τους, ενώ ταυτόχρονα υπάρχουν αρκετοί περιορισμοί για το Blockchain να αναλάβει το προβάδισμα. Δεδομένου ότι τα μη εξουσιοδοτημένα συστήματα είναι ανοιχτά στο κοινό, οποιοσδήποτε χρήστης μπορεί εύκολα να ενταχθεί στο Blockchain, επομένως θα προέκυπταν προβλήματα ασφάλειας λόγω του μεγέθους του Blockchain. Τα πρωτόκολλα συναίνεσης αναπτύσσονται για τη διατήρηση του συστήματος με ασφάλεια. Για παράδειγμα, ένας συμμετέχων στο σύστημα μπορεί να ενταχθεί στο Blockchain με περισσότερες από μία ταυτότητες ταυτόχρονα και να προκαλέσει την αποτυχία του συστήματος κατά τη διαδικασία συναίνεσης (Narayanan et al, 2016).

Είναι σημαντικό να αναπτυχθούν πρωτόκολλα συναίνεσης, να αποκαλυφθούν θετικές και αρνητικές πτυχές των υπαρχουσών προσεγγίσεων ή να δημιουργηθούν εναλλακτικές προσεγγίσεις σε ανεπαρκή συστήματα, προκειμένου να ελαχιστοποιηθούν τα προβλήματα που αντιμετωπίζουν οι συμμετέχοντες, το δίκτυο ή άλλοι λόγοι. Η ασφάλεια του πρωτοκόλλου συναίνεσης θα πρέπει να λαμβάνεται υπόψη στην αρχή κατά την επιλογή της πλατφόρμας Blockchain. Οι αρνητικές πτυχές

του επιλεγμένου πρωτοκόλλου επηρεάζουν επίσης τη χρηστικότητα και την αποτελεσματικότητα του συστήματος Blockchain. Η ασφάλεια μιας τεχνολογίας Blockchain μπορεί να εκφραστεί με το μέγεθος της κατανεμημένης βάσης δεδομένων (Emeç et al, 2020).

1.7.1 Επιθέσεις στο Blockchain

Τα Blockchain, παρά την ισχυρή δομή δεδομένων τους και άλλα οφέλη, έχουν ορισμένες αδυναμίες, όπως το υπολογιστικό κόστος για την εκτέλεση των συναινετικών αλγορίθμων του Blockchain, που απαιτεί την επίλυση σύνθετων μαθηματικών προβλημάτων παράλληλα από μεγάλο αριθμό χρηστών, που όλοι ανταγωνίζονται για να τερματίσουν πρώτοι σε ένα παγκόσμια φυλή (Aponte-Novoa et al, 2021).

Παρά το γεγονός ότι η προσπάθεια που απαιτείται για την επίλυση των προβλημάτων είναι υψηλή, υπάρχουν χρήστες με αρκετή υπολογιστική ισχύ που όχι μόνο θα μπορούσαν να τα λύσουν γρήγορα και με κατανεμημένο τρόπο, αλλά και να προσπαθήσουν να κυριαρχήσουν στο δίκτυο δημιουργώντας μια νέα έκδοση του Blockchain που θα επέτρεπε να ξοδέψουν έναν συγκεκριμένο αριθμό νομισμάτων τουλάχιστον δύο φορές, παραβιάζοντας μία από τις αρχές σχεδιασμού των ψηφιακών νομισμάτων. Αυτό ονομάζεται επίθεση διπλής δαπάνης και ενέχει υψηλό κίνδυνο για την ασφάλεια του Blockchain. Συγκεκριμένα, αυτή η επίθεση μπορεί να πραγματοποιηθεί από έναν εξορύκτη εάν αυτός ο εξορύκτης έχει περισσότερο από το 51% της συνολικής ισχύος εξόρυξης. Αυτή είναι επίσης γνωστή ως επίθεση 51%, η οποία μπορεί να οριστεί ως επίθεση που βασίζεται σε κατακερματισμό που συμβαίνει σε μια αλυσίδα μπλοκ όταν ένας ή περισσότεροι εξορύκτες αναλαμβάνουν τον έλεγχο τουλάχιστον του 51% του συνόλου της εξόρυξης του κατακερματισμού ή του υπολογισμού στο δίκτυο της αλυσίδας μπλοκ. Με αυτήν την υπολογιστική ισχύ, ένας εξορύκτης μπορεί να αλλάξει τις συναλλαγές σε ένα δίκτυο Blockchain και ως εκ τούτου να εμποδίσει τη διαδικασία αποθήκευσης ενός νέου μπλοκ (Aponte-Novoa et al, 2021).

Εκτελώντας μια επίθεση 51%, ένας εξορύκτης μπορεί αυθαίρετα να χειραγωγήσει και να τροποποιήσει τις πληροφορίες στο Blockchain. Συγκεκριμένα, ένας εισβολέας μπορεί να εκμεταλλευτεί αυτή την ευπάθεια για να πραγματοποιήσει τις ακόλουθες επιθέσεις: α) να αντιστρέψει τις συναλλαγές και να ξεκινήσει μια επίθεση διπλής δαπάνης. Δηλαδή ξοδεύοντας τα ίδια νομίσματα πολλές φορές. β) εξαιρεί και τροποποιεί τη σειρά των συναλλαγών· γ) να παρεμποδίσει τις κανονικές εργασίες εξόρυξης άλλων εξορύκτων και δ) αποτρέπει τη λειτουργία επιβεβαίωσης των κανονικών συναλλαγών (Guo et al, 2022).

Εάν μερικοί εξορύκτες συγκεντρώσουν την ισχύ εξόρυξης σε ένα Blockchain που χρησιμοποιεί τον μηχανισμό συναίνεσης Proof of Work (PoW), τότε μπορεί να προκύψει φόβος μιας ακούσιας κατάστασης, όπως μια ομάδα να ελέγχει περισσότερο από το 50% του κατακερματισμού υπολογιστικής ισχύος. Τον Ιανουάριο του 2014, ο όμιλος εξόρυξης ghash.io έφτασε το 42% της συνολικής ισχύος κατακερματισμού σε Bitcoin, γεγονός που προκάλεσε οικειοθελώς αποχώρηση από εξορύκτες από τον όμιλο, ενώ το ghash.io σε ένα δελτίο τύπου διαβεβαίωσε την κοινότητα του Bitcoin ότι θα αποφύγει να φτάσει το 51% κατώφλι ισχύος κατακερματισμού. Σε αυτή την περίπτωση, υπήρχε ένας μηχανισμός αυτοελέγχου βασισμένος στην τιμή. Ωστόσο, αυτό το είδος ζητήματος δεν μπορεί να αφεθεί στην τύχη εάν το Blockchain θέλει να γίνει μια ευρύτερα αποδεκτή υποδομή για συναλλαγές (Aponte-Novoa et al, 2021).

1.7.2 Αξιόπιστος έλεγχος ταυτότητας με βάση το Blockchain

Γενικά, η χρήση του Blockchain μπορεί να συμπεράνει ως τρεις τύπους: ενεργώντας ως κατανεμημένο καθολικό, πραγματοποίηση αποκεντρωμένης αποθήκευσης ή υποστήριξη κατανεμημένων υπηρεσιών που βασίζονται σε έξυπνα συμβόλαια. Για παράδειγμα, έχει εισαχθεί ένα αυτόνομο Blockchain για να επιλέξει τον πιο βολικό σταθμό φόρτισης ηλεκτρικού τερματικού, ενώ έχουν προταθεί ηλεκτρικές συναλλαγές που βασίζονται σε Blockchain σε μικροδίκτυα (Guo et al, 2020).

Ωστόσο, η αποτελεσματικότητα του ελέγχου ταυτότητας είναι μια πρόκληση που πρέπει να επιλυθεί στο δίκτυο Blockchain που βασίζεται σε σύννεφο. Οι Tselios et al, 2017 θεώρησαν το Blockchain ως σημαντικό παράγοντα ασφάλειας για την υποδομή υπολογιστικού νέφους που βασίζεται σε δίκτυο καθορισμένου λογισμικού (SDN). Αν και είναι αφιερωμένες στη διασφάλιση της εγκυρότητας των δεδομένων, αυτές οι εργασίες αγνοούν το τεράστιο κόστος για την ενέργεια και τους υπολογιστικούς πόρους. Για την προώθηση της επεξεργασίας ακμών, ο υπολογισμός ακμών θεωρείται ως ένα νέο υπολογιστικό παράδειγμα (Tselios et al, 2017).

Χρησιμοποιώντας υπολογιστική και χωρητικότητα αποθήκευσης υπολογιστικών άκρων, τα σταθερά και κινητά τερματικά μπορούν να λειτουργήσουν με κατανεμημένους τρόπους. Οι Zhu et al., 2019 ανέλυσαν τα πλεονεκτήματα της διευκόλυνσης των εφαρμογών Blockchain στο μελλοντικό κινητό σύστημα IoT. Οι Liu et al, 2018 πρότειναν ένα νέο πλαίσιο ασύρματης αλυσίδας μπλοκ με δυνατότητα υπολογιστικής ακμής για φορητές συσκευές, όπου οι εργασίες εξόρυξης που απαιτούν υπολογισμό μπορούν να εκφορτωθούν σε κοντινούς κόμβους άκρης. Ωστόσο, αυτές οι εργασίες δεν έλαβαν υπόψη την αποτελεσματικότητα του ελέγχου ταυτότητας.

Συνοπτικά, η υπάρχουσα βιβλιογραφία για συστήματα Blockchain έχει επιτύχει μια ποικιλία ιδιοτήτων, όπως η ανωνυμία, η αποκέντρωση και η διαφάνεια του συστήματος. Ωστόσο, έχει δοθεί λιγότερη προσοχή στην επίτευξη αποτελεσματικού ελέγχου ταυτότητας μεταξύ διαφορετικών πλατφορμών IoT. Ως εκ τούτου, αυτό το άρθρο προτείνει ένα κατανεμημένο και αξιόπιστο σύστημα ελέγχου ταυτότητας που βασίζεται σε Blockchain και υπολογιστές άκρων. Με την τεχνολογία υπολογιστών άκρων, οι κόμβοι άκρων της αλυσίδας μπλοκ μπορούν να προσφέρουν ανάλυση ονομάτων και υπηρεσία ελέγχου ταυτότητας άκρων. Εν τω μεταξύ, μια στρατηγική προσωρινής αποθήκευσης έχει σχεδιαστεί για να βελτιώσει περαιτέρω την αποτελεσματικότητα του ελέγχου ταυτότητας (Guo et al, 2020).

Το Blockchain κοινοπραξίας υιοθετείται για τη δημιουργία ενός αξιόπιστου συστήματος ελέγχου ταυτότητας σε αυτό το άρθρο. Με βάση το Blockchain της κοινοπραξίας, έχουν σχεδιαστεί διάφοροι αλγόριθμοι συναίνεσης όπως φαίνεται στον **Πίνακα Ι**, όπως απόδειξη εργασίας, απόδειξη συμμετοχής (PoS), εκχωρημένο PoS (dPoS), casper, απόδειξη του παρελθόντος χρόνου (PoET) και PBFT. Συνήθως, το καθένα μπορεί να χωριστεί σε τρία μέρη: επαλήθευση ταυτότητας, επιλογή βασικών ομότιμων και συγχρονισμός δεδομένων στην αλυσίδα μπλοκ. Για να ικανοποιηθεί η υψηλή απαίτηση σε πραγματικό χρόνο, εφαρμόζεται ο αλγόριθμος PBFT χωρίς να απαιτείται διακριτικό (Guo et al, 2020).

Πίνακας 1 Σύγκριση αλγορίθμων συναίνεσης (Guo et al, 2020).

Algorithm	PoS	DPoS	Casper	PoET	PBFT
Decentralized	complete	complete	complete	semi	semi
Tokens	yes	yes	yes	no	no
Evil number	51%	51%	51%	51%	33%
Performance	relatively high	high	relatively high	high	high
Technical maturity	mature	mature	not applied	not applied	mature

Τα περισσότερα μέλη της συμμαχίας που αποτελούν το Blockchain της κοινοπραξίας είναι αξιόπιστα και έγκυρα, όπως κυβερνήσεις, φορείς εκμετάλλευσης υπηρεσιών και μεγάλες επιχειρήσεις. Επιπλέον, για την ελάφρυνση του φόρτου αποθήκευσης και υπολογισμού του Blockchain, οι εργασίες επίλυσης και καταγραφής δεδομένων που παράγονται από πολυάριθμα τερματικά εκτελούνται από κόμβους ακμών. Με αυτόν

τον τρόπο, ο αλγόριθμος συναίνεσης εκτελείται μόνο για την επαλήθευση της ταυτότητας και την αποθήκευση αρχείων καταγραφής ελέγχου ταυτότητας στο Blockchain, επιτυγχάνοντας την ιχνηλασιμότητα των δεδομένων και αποτρέποντας την παραβίαση δεδομένων (Guo et al, 2020).

Κεφάλαιο 2: Αλγόριθμοι Συναίνεσης και Κρυπτονομίσματα

Η συγκεκριμένη διπλωματική εργασία αποτελεί κομμάτι ενός έργου που στοχεύει στην μείωση της σπατάλης των τροφίμων (food waste) σε επιχειρήσεις, εστιατόρια, μαγαζιά με τρόφιμα και οποιουδήποτε τύπου χώρο εστιάσης. Η βασική ιδέα του παραπάνω έργου είναι η δημιουργία μιας εφαρμογής, η οποία θα επιτρέπει συναλλαγές μεταξύ επιχειρήσεων μέσω ενός δικτύου Blockchain, με σκοπό οι συναλλαγές αυτές να είναι άμεσες, ασφαλείς και καταγεγραμμένες. Έτσι λοιπόν, στο κεφάλαιο αυτό θα αναλύσουμε αρκετούς αλγορίθμους συναίνεσης δικτύων Blockchain, με σκοπό να βρεθεί κάποιος κατάλληλος για το έργο μας. Ακόμη, θα αναλύσουμε την έννοια του Tokenization και αναφέρουμε μερικά κρυπτονομίσματα, τα οποία είναι αρκετά επίκαιρα και ανεβαίνουν συνεχώς η αξία, αλλά και η φήμη τους.

2.1 Αλγόριθμοι συναίνεσης

Στο πλαίσιο των κρυπτονομισμάτων, οι αλγόριθμοι συναίνεσης είναι ένα κρίσιμο μέρος κάθε δικτύου blockchain, καθώς είναι υπεύθυνοι για τη διατήρηση της ακεραιότητας και της ασφάλειας αυτών των κατανεμημένων (Distributed) συστημάτων. Ένας αλγόριθμος συναίνεσης μπορεί να οριστεί ως ο μηχανισμός μέσω του οποίου ένα δίκτυο blockchain φτάνει στη συναίνεση. Τα δημόσια (αποκεντρωμένα) blockchains δημιουργούνται ως κατανεμημένα συστήματα και, δεδομένου ότι δεν βασίζονται σε μία κεντρική αρχή, οι κατανεμημένοι κόμβοι πρέπει να συμφωνήσουν σχετικά με την εγκυρότητα των συναλλαγών. Έτσι, οι αλγόριθμοι συναίνεσης διαβεβαιώνουν ότι ακολουθούνται οι κανόνες πρωτοκόλλου και εγγυώνται ότι όλες οι συναλλαγές πραγματοποιούνται με έναν βέβαιο τρόπο, επομένως το κάθε κρυπτονόμισμα μπορεί να χρησιμοποιηθεί μόνο μία φορά. Παρακάτω θα αναλυθούν αρκετοί αλγόριθμοι συναίνεσης που υπάρχουν στα δίκτυα blockchain των περισσοτέρων και των πιο γνωστών κρυπτονομισμάτων.

2.1.1 Proof of work

Το Proof-of-work είναι ο αλγόριθμος που χρησιμοποιούν πολλά κρυπτονομίσματα, συμπεριλαμβανομένων των Bitcoin και Ethereum. Τα περισσότερα ψηφιακά νομίσματα έχουν μια κεντρική οντότητα ή έναν ηγέτη ο οποίος παρακολουθεί κάθε χρήστη και πόσα χρήματα έχει. Στο Bitcoin όμως δεν υπάρχει τέτοιος ηγέτης ή υπεύθυνος για τα κρυπτονομίσματα. Έτσι λοιπόν, απαιτείται απόδειξη της εργασίας

για να λειτουργήσει το διαδικτυακό νόμισμα χωρίς εταιρεία ή κυβέρνηση να εκτελεί την παράσταση.

Πιο συγκεκριμένα, η απόδειξη εργασίας είναι η λύση του «προβλήματος των διπλών δαπανών», το οποίο είναι πιο δύσκολο να επιλυθεί χωρίς υπεύθυνο ηγέτη. Εάν οι χρήστες μπορούν να ξοδέψουν διπλά τα κέρματά τους, αυτό αυξάνει τη συνολική προσφορά, υποβαθμίζοντας τα κέρματα όλων των άλλων χρηστών και καθιστώντας το νόμισμα απρόβλεπτο και άχρηστο.

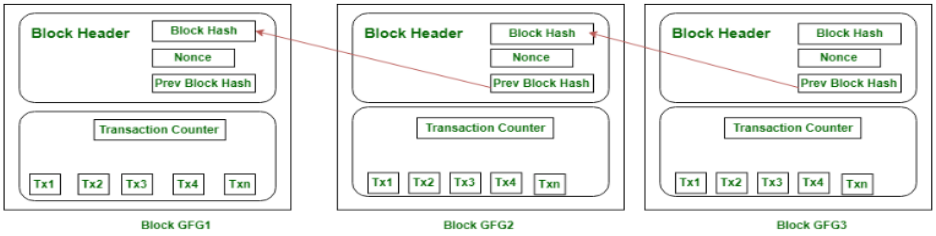
Η διπλή δαπάνη είναι ένα ζήτημα για διαδικτυακές συναλλαγές, επειδή οι ψηφιακές ενέργειες είναι πολύ εύκολο να αναπαραχθούν, γεγονός που το καθιστά ασήμαντο να αντιγράφετε και να επικολλάτε ένα αρχείο ή να στέλνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε περισσότερα από ένα άτομα. Η απόδειξη της εργασίας καθιστά τον διπλασιασμό του ψηφιακού χρήματος εξαιρετικά δύσκολο. Είναι ακριβώς όπως ακούγεται: απόδειξη ότι κάποιος έχει κάνει σημαντικό αριθμό υπολογισμών.

Το Bitcoin είναι ένα blockchain, ένα κοινόχρηστο καθολικό που περιέχει ένα ιστορικό κάθε συναλλαγής Bitcoin που πραγματοποιήθηκε ποτέ. Αυτό το blockchain, όπως υποδηλώνει το όνομα, αποτελείται από μπλοκ. Κάθε μπλοκ έχει αποθηκεύσει τις πιο πρόσφατες συναλλαγές. Η απόδειξη της εργασίας είναι απαραίτητο μέρος της προσθήκης νέων μπλοκ στο blockchain Bitcoin. Τα μπλοκ ζωντανεύουν από τους εξορύκτες, τους παίκτες στο οικοσύστημα που εκτελούν την απόδειξη της εργασίας. Ένα νέο μπλοκ γίνεται αποδεκτό από το δίκτυο κάθε φορά που ένας ανθρακωρύχος έρχεται με μια νέα κερδοφόρα απόδειξη εργασίας, η οποία συμβαίνει περίπου κάθε 10 λεπτά.

Η εύρεση της κερδοφόρας απόδειξης εργασίας είναι δύσκολη και ο μόνος τρόπος για να γίνει η δουλειά που χρειάζονται οι εξορύκτες για να κερδίσουν το bitcoin είναι με ακριβούς, εξειδικευμένους υπολογιστές. Οι εξορύκτες θα κερδίσουν bitcoin εάν μαντέψουν έναν αντίστοιχο υπολογισμό. Όσο περισσότεροι υπολογισμοί λαμβάνουν χώρα, τόσο περισσότερα bitcoin είναι πιθανό να κερδίσουν.

Ο στόχος των εξορυκτών είναι να δημιουργήσουν ένα hash που να ταιριάζει με τον τρέχοντα στόχο του Bitcoin. Αυτό το hash πρέπει να έχει αρκετά μηδενικά μπροστά. Η πιθανότητα να πάρει πολλά μηδενικά στη σειρά είναι όμως πολύ χαμηλή. Οι εξορύκτες όμως σε όλο τον κόσμο κάνουν τρισεκατομμύρια τέτοιου είδους υπολογισμούς το δευτερόλεπτο, οπότε χρειάζονται περίπου 10 λεπτά κατά μέσο όρο για να επιτύχουν ο στόχος. Όποιος πετύχει το στόχο κερδίζει πρώτα μια παρτίδα κρυπτογράφησης Bitcoin. Στη συνέχεια, το πρωτόκολλο Bitcoin δημιουργεί μια νέα αξία που οι εξορύκτες θα πρέπει να επιλύσουν, για να επιτύχουν το στόχο τους. Ο στόχος της

απόδειξης εργασίας είναι να αποτρέψει τους χρήστες από την εκτύπωση επιπλέον νομισμάτων που δεν κέρδισαν ή με τη μέθοδο των διπλών δαπανών. Εάν οι χρήστες μπορούσαν να ξοδέψουν τα κέρματά τους περισσότερες από μία φορές, αυτό θα έκανε πραγματικά το νόμισμα άχρηστο.



Εικόνα 13: Ακολουθία των μπλοκ στον αλγόριθμο συναίνεσης PoW

Στα περισσότερα ψηφιακά νομίσματα, αυτό το πρόβλημα είναι εύκολο να λυθεί. Η τράπεζα που είναι υπεύθυνη για το σύστημα παρακολουθεί πόσα χρήματα έχει κάθε άτομο. Εάν ο Α στέλνει στον Β $ 1, τότε η τράπεζα αφαιρεί $ 1 από την Α και δίνει $ 1 στον Β. Αλλά στα κρυπτονομίσματα δεν υπάρχει τέτοια οντότητα. Η απόδειξη εργασίας όμως παρέχει μια λύση.

Υπάρχουν ορισμένα προβλήματα με τον αλγόρθμο PoW:

- Υψηλή κατανάλωση ενέργειας: Το Bitcoin για παράδειγμα χρησιμοποιεί τόση ενέργεια όσο όλη η Ελβετία λόγω της απόδειξης εργασίας. Και η χρήση της ενέργειας αυξάνεται καθώς περισσότεροι εξορύκτες συμμετέχουν στο κυνήγι bitcoin, παρόλο που μερικά από αυτά τροφοδοτούνται από ανανεώσιμες πηγές ενέργειας.
- 51% επιθέσεις: Εάν μια οντότητα εξόρυξης είναι σε θέση να συσσωρεύσει το 51% του hashrate εξόρυξης Bitcoin, τότε μπορεί να παραβιάσει τους κανόνες προσωρινά, να δαπανήσει διπλά κέρματα και να εμποδίσει συναλλαγές.
- Συγκέντρωση ορυχείων: Η απόδειξη της εργασίας έχει να κάνει με τη δημιουργία ενός νομίσματος χωρίς έναν μόνο φορέα. Λέγοντας αυτό, στην πράξη το σύστημα είναι κάπως συγκεντρωτικό, με μόλις τρεις ομάδες από εξορύκτες να ελέγχουν σχεδόν το 50% της υπολογιστικής ισχύος του Bitcoin. Ωστόσο, οι προγραμματιστές προσπαθούν να μετριάσουν τουλάχιστον αυτό το ζήτημα.

Η απόδειξη εργασίας είναι αλγόριθμος συναίνεσης, του οποίου η χρήση στο blockchain έχει φέρει επανάσταση στην ασφάλεια δεδομένων. Το PoW είναι δημοφιλές στα κρυπτονομίσματα λαμβάνοντας υπόψη τη διασφάλιση υψηλής ασφάλειας του. Λειτουργεί βάσει ενός ενεργοβόρου μοντέλου ασφαλείας που απαιτεί από τους εξορύκτες να επικυρώνουν όλες τις συναλλαγές και να τις οργανώνουν σε blockchains.

Το PoW έχει δεχθεί επικρίσεις λόγω της αναποτελεσματικότητας του κόστους, της υπερβολικής κατανάλωσης χρόνου και των υψηλών ηλεκτρονικών αποβλήτων. Οι αλγόριθμοι συναίνεσης όπως το PoS και άλλοι που θα αναλυθούν παρακάτω είναι ανώτεροι σε αυτές τις πτυχές, διότι είναι οικονομικά αποδοτικοί και επεκτάσιμοι. Παρόλα αυτά, η μεγαλύτερη ασφάλεια του PoW παραμένει το πιο σημαντικό του πλεονέκτημα και για αυτό τα κρυπτονομίσματα ακόμη το επιλέγουν κατά κύριο λόγο.

2.1.2 Proof of stake

Ένας αλγόριθμος συναίνεσης Proof of Stake (PoS) είναι ένα σύνολο κανόνων που διέπουν ένα δίκτυο blockchain και τη δημιουργία του εγγενούς νομίσματός του, δηλαδή έχει τον ίδιο στόχο με έναν αλγόριθμο Proof of Work (PoW) με την έννοια ότι είναι μέσο για την επίτευξη συναίνεσης. Σε αντίθεση όμως με το PoW, δεν συμμετέχουν εξορύκτες στη διαδικασία. Αντ 'αυτού, οι συμμετέχοντες του δικτύου που θέλουν να ενταχθούν στην απόδειξη της εγκυρότητας των συναλλαγών δικτύου και τη δημιουργία μπλοκ σε ένα δίκτυο PoS πρέπει να κρατήσουν ένα συγκεκριμένο μερίδιο στο δίκτυο. Ένα παράδειγμα είναι η τοποθέτηση ενός συγκεκριμένου ποσού νομίσματος ενός δικτύου σε ένα συνδεδεμένο πορτοφόλι του blockchain του.

Αυτό είναι γνωστό ως «τοποθέτηση πονταρίσματος» ή «στοίχημα». Ένας δημιουργός μπλοκ σε ένα σύστημα PoS περιορίζεται στη δημιουργία μπλοκ ανάλογων με το μερίδιό του στο δίκτυο.

Έτσι, τα δίκτυα PoS βασίζονται σε ντετερμινιστικούς αλγόριθμους, που σημαίνει ότι οι επικυρωτές των μπλοκ επιλέγονται ανάλογα με τη φύση του στοιχήματος. Για παράδειγμα, η επιλογή υπολοίπου λογαριασμού ως το μοναδικό κριτήριο στο οποίο ορίζεται το επόμενο έγκυρο μπλοκ σε ένα blockchain θα μπορούσε δυνητικά να οδηγήσει σε ανεπιθύμητη συγκέντρωση. Αυτό θα σήμαινε ότι τα πλούσια μέλη ενός δικτύου θα απολάμβαναν μεγάλα πλεονεκτήματα. Για το λόγο αυτό, υπάρχουν διάφορες μέθοδοι επιλογής για τον ορισμό ενός στοιχήματος ή ενός συνδυασμού τους. Διαφορετικά κρυπτονομίσματα που χρησιμοποιούν PoS χρησιμοποιούν διαφορετικές παραλλαγές για να ορίσουν τα «μερίδια».

Παραδείγματα για τέτοιες παραλλαγές περιλαμβάνουν το πραγματικό υπόλοιπο των νομισμάτων σε έναν λογαριασμό, τα σταθερά χρονικά διακριτικά πρέπει να είναι σε ένα blockchain για να συμβάλλουν στη δημιουργία μπλοκ, ηλικία νομισμάτων (ο αριθμός των νομισμάτων που κρατούνται σε ένα πορτοφόλι πολλαπλασιασμένος επί τον αριθμό ημερών έχουν βρεθεί σε αυτό το πορτοφόλι), και άλλους παράγοντες.

Ακόμη ένα από τα πλεονεκτήματα του PoS είναι πως επιλύει μερικές από τις αδυναμίες ενός συστήματος PoW πίσω από κρυπτονομίσματα όπως το Bitcoin. Το PoS ουσιαστικά εξαλείφει τα εμπόδια στην είσοδο της διαδικασίας επικύρωσης. Οι χρήστες δεν χρειάζεται πλέον να αγοράζουν εξειδικευμένους υπολογιστές μόνο για να έχουν την ευκαιρία να κερδίσουν όλα αυτά τα αόριστα μπλοκ ως ανταμοιβή. Κατά συνέπεια, το PoS απαιτεί λιγότερη υπολογιστική ισχύ από το PoW και επομένως έχει επίσης λιγότερες επιπτώσεις στο περιβάλλον.

Από την άλλη πλευρά, ορισμένα δίκτυα PoS έχουν σημαντικές αδυναμίες, ανάλογα με τις παραλλαγές που χρησιμοποιούνται για τον καθορισμό της συμμετοχής σε ένα δίκτυο. Οι παραγωγοί μπλοκ ορισμένων νομισμάτων ενδέχεται να διαθέτουν απίστευτη ισχύ εάν ο αριθμός των παραγωγών μπλοκ σε ένα δίκτυο είναι χαμηλός και μπορούν να επικυρώσουν όλες τις συναλλαγές. Ωστόσο, η ισχύς ενός παραγωγού μπορεί να ανακληθεί αυτόματα κάθε φορά που κάνει κάτι ενάντια στα συμφέροντα του δικτύου. Εάν, για παράδειγμα, ένας παραγωγός νομίσματος EOS αποτύχει να εργαστεί σε οποιοδήποτε μπλοκ για 24 ώρες, ένα αντίγραφο ασφαλείας παίρνει γρήγορα τη θέση του.

Η δεύτερη μεγάλη αδυναμία είναι ότι ορισμένα συστήματα PoS ευνοούν τους πλούσιους χρήστες - όσο περισσότερα νομίσματα στοιχηματίζετε, τόσο περισσότερα μπορείτε να ψηφίσετε. Δίκτυα όπως η Cardano έχουν ήδη αντιμετωπίσει αυτό το ζήτημα με την εφαρμογή τυχαιοποιημένης επιλογής παραγωγών μπλοκ. Σε αυτήν την περίπτωση, οι πλουσιότεροι χρήστες εξακολουθούν να έχουν περισσότερες πιθανότητες να γίνουν παραγωγοί μπλοκ, αλλά η εξωτερική επιρροή των συμμετεχόντων που κατέχουν πολύ περισσότερα νομίσματα ενός συγκεκριμένου δικτύου από τον μέσο χρήστη μειώνεται.

Τέλος, καταλήγουμε ότι ο PoS είναι ένας αλγόριθμος, ο οποίος δεν είναι κοστοβόρος ούτε ενεργειακά, αλλά ούτε και σε θέμα εξοπλισμού. Ακόμη, τον χαρακτηρίζει μια τυχαιότητα όσον αφορά την επιλογή των επικυρωτών των συναλλαγών του δικτύου και διαθέτει μηχανισμούς που αποτρέπουν τους χρήστες από το να πραγματοποιήσουν μη έγκυρες συναλλαγές, αλλά ταυτόχρονα τους ωθεί να συμμετέχουν καθημερινά στις διαδικασίες επικύρωσης συναλλαγών. Καταλήγουμε

δηλαδή σύμφωνα με τα παραπάνω και συμφωνούμε με την επιστημονική κοινότητα ότι πρόκειται για τον πιο σημαντικό αλγόριθμο συναίνεσης και αυτόν που από ότι φαίνεται θα αντικαταστήσει και θα ξεπεράσει τον αλγόριθμο Proof-of-Work.

2.1.3 Delegated Proof Of Stake (DPoS)

Το Delegated Proof Of Stake (DPoS) είναι ένας αλγόριθμος συναίνεσης που αποτελεί την πρόοδο των θεμελιωδών εννοιών του Proof Of Stake. Στο σύστημα συναίνεσης Proof of Stake, κάθε άτομο που ποντάρει ένα διακριτικό μπορεί να συμμετάσχει στη διαδικασία «molding» που σημαίνει ότι έχει την ευκαιρία να επιλέξει δύο κόμβους επιπέδου που επικυρώνουν περαιτέρω το μπλοκ και ανταμείβονται για την προσθήκη ενός μπλοκ στο blockchain. Το σύστημα DPos διατηρείται από ένα εκλογικό σύστημα για την επιλογή κόμβων που επαληθεύουν μπλοκ. Αυτοί οι κόμβοι ονομάζονται «μάρτυρες» ή «παραγωγοί αποκλεισμού».

Στη συναίνεση DPoS οι χρήστες μπορούν είτε να ψηφίσουν άμεσα είτε να δώσουν την ψήφο τους σε άλλη οντότητα για να ψηφίζει εκ μέρους τους. Ο επιλεγμένος μάρτυρας είναι υπεύθυνος για τη δημιουργία μπλοκ επαληθεύοντας τις συναλλαγές. Εάν επαληθεύσουν και υπογράψουν όλες τις συναλλαγές σε ένα μπλοκ, λαμβάνουν μια ανταμοιβή, η οποία συνήθως κοινοποιείται σε εκείνους που έχουν ψηφίσει. Εάν ένας μάρτυρας αποτύχει να επαληθεύσει όλες τις συναλλαγές στο δεδομένο χρονικό διάστημα, χάνει το μπλοκ. Συνεπώς, όλες οι συναλλαγές παραμένουν μη επαληθευμένες και δεν διανέμεται ανταμοιβή σε αυτόν τον μάρτυρα. Η ανταμοιβή προστίθεται ως ανταμοιβή του επόμενου μάρτυρα που επαληθεύει αυτό το μπλοκ. Τέτοιες συναλλαγές συλλέγονται από τον επόμενο μάρτυρα και ένα τέτοιο μπλοκ ονομάζεται κλεμμένο.

Ακόμη, οι ψήφοι είναι ανάλογοι με το μέγεθος του ποσοστού κάθε ψηφοφόρου. Ένας χρήστης δεν χρειάζεται να έχει μεγάλο ποντάρισμα για να εισέλθει στην πρώτη κατηγορία μαρτύρων. Αντίθετα, οι ψήφοι από χρήστες με μεγάλα στοιχήματα μπορούν να έχουν ως αποτέλεσμα οι χρήστες με σχετικά μικρά στοιχήματα να ανεβαίνουν στην κορυφαία κατηγορία μαρτύρων.

Οι χρήστες σε συστήματα DPoS ψηφίζουν επίσης μια ομάδα αντιπροσώπων που επιβλέπουν τη διακυβέρνηση blockchain, οι οποίοι δεν διαδραματίζουν ρόλο στον έλεγχο συναλλαγών. Οι προηγούμενοι ονομάζονται πληρεξούσιοι και μπορούν να προτείνουν αλλαγή μεγέθους ενός μπλοκ ή του ποσού που πρέπει να πληρώσει ένας

μάρτυρας ως αντάλλαγμα για την επικύρωση ενός μπλοκ. Μόλις οι εκπρόσωποι προτείνουν τέτοιες αλλαγές, οι χρήστες του blockchain ψηφίζουν εάν θα τις εγκρίνουν.

Οι επικυρωτές μπλοκ στο DPoS αναφέρονται σε πλήρεις κόμβους που επαληθεύουν ότι τα μπλοκ που δημιουργήθηκαν από μάρτυρες ακολουθούν τους κανόνες συναίνεσης. Οποιοσδήποτε χρήστης μπορεί να εκτελέσει ένα πρόγραμμα επικύρωσης μπλοκ και να επαληθεύσει το δίκτυο, παρόλα αυτά όμως δεν υπάρχει κίνητρο να γίνει κάποιος επικυρωτής μπλοκ.

Πλεονεκτήματα :

- Τα μπλοκ DPoS έχουν καλή προστασία από τις διπλές δαπάνες.
- Το DPoS είναι πιο δημοκρατικό και οικονομικά χωρίς αποκλεισμούς λόγω του μικρότερου ποσού στοιχηματισμού που απαιτείται από έναν χρήστη / κόμβο.
- Το DPoS παρέχει περισσότερη αποκέντρωση καθώς περισσότερα άτομα συμμετέχουν στη συναίνεση λόγω του χαμηλού ορίου εισόδου.
- Το DPoS δεν απαιτεί μεγάλη ισχύ για την εκτέλεση δικτύου, γεγονός που το καθιστά πιο βιώσιμο.
- Οι συναλλαγές στο DPoS δεν εξαρτώνται από την υπολογιστική ισχύ που απαιτείται για την εκτέλεση του δικτύου, επομένως είναι πιο επεκτάσιμη.
- Η DPoS διαχωρίζει την εκλογή παραγωγών μπλοκ από την ίδια την παραγωγή μπλοκ που ανοίγει την πόρτα για πιο δημιουργικά μοντέλα για την επίλυση και των δύο προβλημάτων μεμονωμένα.
- Η μέθοδος DPoS παρέχει τη βάση για την εφαρμογή ενδιαφέρων μοντέλων διακυβέρνησης σε εφαρμογές blockchain. Κατά μία έννοια, σχηματίζει ένα είδος δημοκρατίας.

Μειονεκτήματα:

- Η αποτελεσματική λειτουργία και λήψη αποφάσεων του δικτύου απαιτεί από τους αντιπροσώπους να είναι καλά ενημερωμένοι και να διορίζουν έντιμους μάρτυρες.
- Ο περιορισμένος αριθμός μαρτύρων μπορεί να οδηγήσει σε συγκέντρωση δικτύου.
- Το blockchain DPoS είναι ευαίσθητο σε προβλήματα σταθμισμένης ψηφοφορίας. Οι χρήστες με μικρότερο ποσοστό μπορούν να αρνηθούν να συμμετάσχουν σε ψηφοφορίες αφού θεωρήσουν ότι η ψήφος τους είναι ασήμαντη.

Έτσι λοιπόν, καταλήγουμε ότι αυτή η ιδέα δίνει μια τεράστια υπόσχεση για την αύξηση της αποτελεσματικότητας, της ταχύτητας των συναλλαγών και της απόδοσης των πρωτοκόλλων blockchain, κάτι που είναι απαραίτητο για εταιρικές χρήσεις καθώς ο κλάδος αναπτύσσεται και προσπαθεί να διαταράξει πιο περίπλοκες και μεγαλύτερες αγορές. Η μετάβαση από το PoW σε μηχανισμούς συναίνεσης που βασίζονται σε PoS είναι μια σημαντική εξέλιξη για την τεχνολογία blockchain και η επανάληψη του PoS πιθανότατα θα γίνει η κυρίαρχη μορφή συναίνεσης στο μέλλον.

2.1.4 Proof of Elapsed Time

Το Proof of Elapsed Time (PoET) είναι μια αποτελεσματική εναλλακτική λύση στον αλγόριθμο της απόδειξης της εργασίας (PoW). Στην περίπτωση του PoW, απαιτείται ένας ακριβός υπολογισμός για τη δημιουργία ενός υποψηφίου μπλοκ και τη διάδοση του μηνύματος σε άλλους κόμβους του δικτύου. Είναι ακριβό, διότι συνεπάγεται κόστος για την ηλεκτρική ενέργεια που χρησιμοποιείται από το ειδικό υλικό εξόρυξης (που έχει σχεδιαστεί ειδικά για τον υπολογισμό της τιμής κατακερματισμού) για να εξορύξει το επόμενο μπλοκ στο blockchain. Ο κόμβος που μπορεί να βρει την τιμή κατακερματισμού γίνεται πρώτα ο νέος ηγέτης και παίρνει μια ανταμοιβή με τη μορφή Bitcoin.

Ωστόσο, στο PoET, ένας ξεχωριστός τυχαίος χρονοδιακόπτης που λειτουργεί ανεξάρτητα σε κάθε κόμβο καθορίζει εάν αυτός ο κόμβος δημιουργεί ή όχι το νέο μπλοκ του blockchain και λαμβάνει την ανταμοιβή. Αυτή η τυχαιοποίηση διασφαλίζει επίσης ότι κάθε κόμβος είναι εξίσου πιθανό να είναι ο νικητής.

Ο αλγόριθμος PoET προορίζεται για δίκτυα blockchain που ζητούν άδεια. Δηλαδή, απαιτείται ειδική επαλήθευση από έναν κόμβο όταν προσπαθεί να συνδεθεί στο δίκτυο. Αυτή η επαλήθευση επιτυγχάνεται χρησιμοποιώντας την τεχνολογία Software Guard Extension (SGX) της Intel. Δημιουργεί μια βεβαίωση για ένα κομμάτι κώδικα και προστατεύει τον κώδικα από εξωτερική πρόσβαση.

Το δίκτυο λειτουργεί λοιπόν με τον ακόλουθο τρόπο. Ένας κόμβος κατεβάζει τον κωδικό PoET και δημιουργεί μια βεβαίωση (κλειδί) για τον κωδικό χρησιμοποιώντας SGX. Στη συνέχεια, ο κόμβος προωθεί αυτό το κλειδί όταν ζητάτε εγγραφή στο δίκτυο. Οι κόμβοι που αποτελούν ήδη μέρος του δικτύου επαληθεύουν αυτό το κλειδί και ο νέος κόμβος έχει το δικό του χρονοδιακόπτη που αρχικοποιείται σε μια τυχαία τιμή. Αυτή η τυχαιότητα διασφαλίζεται από την προστασία κώδικα που προσφέρει η SGX.

Όλοι οι κόμβοι αρχικοποιούνται με τυχαίο χρόνο και ο πρώτος που λήγει παίρνει τον νικητή. Αυτό σημαίνει ότι δημιουργεί ένα νέο μπλοκ, το συνδέει με το τρέχον μπλοκ αλυσίδας και λαμβάνει την ανταμοιβή. Στη συνέχεια, οι κόμβοι αρχικοποιούνται ξανά και η διαδικασία επαναλαμβάνεται.

Το αρνητικό του αλγορίθμου που αναλύουμε έχει να κάνει με την ασφάλεια του. Το σπάσιμο ενός κομματιού hardware δίνει τη δυνατότητα στον εισβολέα να κερδίζει πάντα το λαχείο. Βέβαια, υποστηρίζεται ότι μια στατιστική ανάλυση των μπλοκ που κόπηκαν πρόσφατα αρκεί για να ανιχνεύσει εάν ένα τσιπ μπορεί να τεθεί σε κίνδυνο. Συνεπώς, πρόκειται για έναν αλγόριθμο που τα κύρια και σημαντικότερα πλεονεκτήματα του είναι η τυχαιότητα της επιλογής των νικητών σε συνδυασμό με το χαμηλό ενεργειακό κόστος.

2.1.5 Proof of Weight

Το Proof-of-Weight (PoWeight) είναι ένας μηχανισμός συναίνεσης blockchain που δίνει στους χρήστες ένα «βάρος» με βάση το πόσα κρυπτονομίσματα κατέχουν. Οι μηχανισμοί συναίνεσης Proof-of-Weight βασίζονται στο πρώτο μοντέλο συναίνεσης Proof-of-Weight που χρησιμοποιήθηκε στον αλγόριθμο κρυπτογράφησης Algorand.

Ο μηχανισμός συναίνεσης Proof-of-Weight παραμένει ασφαλής, αρκεί η πλειοψηφία των σταθμισμένων χρηστών να είναι ειλικρινείς και να προστατεύει το δίκτυο από επιθέσεις διπλών δαπανών. Κάθε φορά που πραγματοποιείται μια συναλλαγή σε ένα blockchain χρησιμοποιώντας τον μηχανισμό συναίνεσης Proof-of-Weight, το δίκτυο δημιουργεί μια επιτροπή τυχαίων μελών του δικτύου και εκχωρεί σε κάθε μέλος το «βάρος» τους, με βάση το πόσο νόμισμα κατέχουν στο δίκτυο, το οποίο ελαφρώς συγκεντρώνει τη διαδικασία συναίνεσης στο πλαίσιο της τυχαίας επιτροπής.

Με μια πρώτη ματιά φαίνεται ότι οι αλγόριθμοι Proof-of-Weight και Proof-of-Stake είναι αρκετά παρόμοιοι, παρόλα αυτά έχουν μια βασική διαφορά. Σε ένα δίκτυο Proof-of-Stake, ο αριθμός των νομισμάτων που διατηρούνται στο πορτοφόλι καθορίζει το βάρος του χρήστη και στη συνέχεια τη πιθανότητα να λάβει ο χρήστης την ανταμοιβή του μπλοκ. Από την άλλη μεριά, στο μηχανισμό συναίνεσης Proof-of-Weight οποιαδήποτε τιμή και όχι μόνο η ποσότητα των κερμάτων μπορεί να χρησιμοποιηθεί ως προσδιορισμός του βάρους ενός χρήστη.

Ακόμη, ο μηχανισμός συναίνεσης που αναλύουμε είναι εξαιρετικά προσαρμόσιμος και ικανός να κλιμακωθεί σε μεγάλο αριθμό χρηστών. Οι προγραμματιστές μπορούν να προσαρμόσουν τον βασικό αλγόριθμο έτσι ώστε να επιτρέπει τη δημιουργία

επιτροπών. Μια επιτροπή αποτελείται από τυχαίους χρήστες δικτύου, η δουλειά των οποίων είναι να εκτελέσουν ένα ορισμένο βήμα του πρωτοκόλλου συναίνεσης.

Η δομή της επιτροπής εισάγει κάποιο επίπεδο συγκέντρωσης, ενώ εξακολουθεί να διατηρεί ένα ασφαλές και συνολικά αποκεντρωμένο δίκτυο. Παρά τα πλεονεκτήματα του Proof-of-Weight, αποδείχθηκε πολύ δύσκολο να πειστούν οι χρήστες με αυτό το μοντέλο λόγω έλλειψης κινήτρων, καθώς το πρωτόκολλο δεν ανταμείβει τους χρήστες του για την εκτέλεση ενός κόμβου και την επιβεβαίωση συναλλαγών.

2.1.6 Proof of Importance

Η απόδειξη σπουδαιότητας (POI) είναι ένα σύστημα που χρησιμοποιείται για τον προσδιορισμό των χρηστών που μπορούν να εκτελέσουν τους απαραίτητους υπολογισμούς για να προσθέσουν ένα νέο μπλοκ δεδομένων σε ένα blockchain και να λάβουν τη σχετική πληρωμή.

Ένας αλγόριθμος απόδειξης σπουδαιότητας δίνει προτεραιότητα στους ανθρακωρύχους (εξορύκτες) με βάση τον αριθμό των συναλλαγών στην αντίστοιχη κρυπτογράφηση που εκτελούν. Όσο περισσότερες συναλλαγές γίνονται από και προς το πορτοφόλι κρυπτογράφησης μιας οντότητας, τόσο υψηλότερες είναι οι πιθανότητες να δοθούν έργα εξόρυξης σε μια οντότητα.

Οι αλγόριθμοι απόδειξης εργασίας δίνουν προτεραιότητα στις οντότητες με βάση τον αριθμό των νομισμάτων που κατέχουν. Αυτό σημαίνει ότι όσο περισσότερη υπολογιστική ισχύς μπορεί να προσφέρει μια οντότητα σε ένα αποδεικτικό του δικτύου κρυπτογράφησης εργασίας, τόσο περισσότερα νομίσματα θα είναι σε θέση να εκμεταλλευτεί. Η απόδειξη του συστήματος εργασίας δεν ενθαρρύνει την κυκλοφορία του κρυπτονομίσματος. Μια καθαρή απόδειξη του συστήματος εργασίας δεν είναι απαλλαγμένη από τη συγκέντρωση, επειδή προτεραιότητα δίνεται αυτόματα στην οντότητα που είναι ικανή να παρέχει την υψηλότερη ποσότητα υπολογιστικής ισχύος.

Το σύστημα απόδειξης σπουδαιότητας ξεχωρίζει επίσης από το σύστημα απόδειξης πονταρίσματος. Η απόδειξη του συστήματος πονταρίσματος δίνει προτεραιότητα στις οντότητες με βάση το πόσο από τα αντίστοιχα κρυπτονομίσματα που ποντάρεται. Μια απόδειξη αλγόριθμου στοιχήματος εκχωρεί αυτόματα εργασίες εξόρυξης σε ανθρακωρύχους με βάση το ποσό του αντίστοιχου κρυπτονομίσματος στα πορτοφόλια τους. Αυτό παρέχει λίγα κίνητρα για τη χρήση του κρυπτονομίσματος ως μέσου ανταλλαγής.

Τα συστήματα απόδειξης σπουδαιότητας έχουν σχεδιαστεί για την επιβράβευση χρηστών που πραγματοποιούν ενεργά συναλλαγές σε κρυπτογράφηση με προτεραιότητα στους ανθρακωρύχους με βάση τα ποσά και τα μεγέθη των συναλλαγών που πραγματοποιούνται από τα πορτοφόλια τους. Ένα σύστημα απόδειξης σπουδαιότητας μπορεί να αντιπροσωπεύει πρόσθετους παράγοντες, όπως τα πορτοφόλια από και προς τα οποία πραγματοποιούνται συναλλαγές.

2.1.7 Proof of Believability

Η απόδειξη της αξιοπιστίας (PoB) διασφαλίζει ότι οι κόμβοι έχουν αμελητέα πιθανότητα σφάλματος, αυξάνοντας έτσι σημαντικά τον όγκο των συναλλαγών που μπορούν να εκτελεστούν χάρη στη διακύμανση του μεγέθους των shards. Το Sharding χωρίζει ολόκληρο το δίκτυο μιας εταιρείας blockchain σε μικρότερα διαμερίσματα, γνωστά ως "shards".

Το πρωτόκολλο που βασίζεται σε PoB χρησιμοποιεί μια προσέγγιση που βασίζεται στο Believable-First. Αυτό σημαίνει ότι το πρωτόκολλο χωρίζει όλους τους επικυρωτές σε δύο ομάδες: από τη μία πλευρά, τους αξιόπιστους επικυρωτές και από την άλλη, τους κανονικούς.

Ως αποτέλεσμα, οι αξιόπιστοι επικυρωτές επεξεργάζονται συναλλαγές πολύ γρήγορα στην πρώτη φάση. Στη συνέχεια, οι κανονικοί επικυρωτές δοκιμάζουν και επαληθεύουν τις συναλλαγές στη δεύτερη φάση, έτσι ώστε να οριστικοποιηθεί η λειτουργία και να διασφαλιστεί η νομιμότητα των συναλλαγών.

Η πιθανότητα να επιλεγεί ένας κόμβος ως αξιόπιστος από άλλους αξιόπιστους επικυρωτές καθορίζεται από τη βαθμολογία αξιοπιστίας του κόμβου. Αυτό υπολογίζεται χρησιμοποιώντας πολλαπλές παραμέτρους, όπως ισορροπία διακριτικών, συνεισφορές κοινότητας κ.λπ. Όσο υψηλότερη είναι η βαθμολογία, τόσο πιθανότερο είναι να επιλεγεί ο κόμβος.

Αυτό σημαίνει ότι υπάρχουν αξιόπιστοι επικυρωτές που διαχειρίζονται τις απαραίτητες διαδικασίες για να αποφασίσουν το σύνολο των συναλλαγών που θα υποβληθούν σε επεξεργασία και τη σειρά με την οποία θα υποβληθούν σε επεξεργασία. Αυτοί οι επικυρωτές μπορούν να συγκεντρωθούν, σχηματίζοντας τις δικές τους ομάδες επικύρωσης. Ωστόσο, αυτές οι ομάδες μπορεί επίσης να είναι πολύ μικρές, τόσο ώστε να αποτελούνται από μόνο έναν επικυρωτή ανά ομάδα.

Αυτό θα έχει ως αποτέλεσμα την τυχαία κατανομή των συναλλαγών προς επεξεργασία μεταξύ των διαφόρων αξιόπιστων επικυρωτών. Κατά συνέπεια, παράγονται μικρότερα μπλοκ με εξαιρετικά χαμηλό λανθάνοντα χρόνο.

Ωστόσο, ενδέχεται να υπάρχουν ορισμένα ζητήματα ασφαλείας, καθώς η επαλήθευση γίνεται μόνο από έναν κόμβο. Ως εκ τούτου, ορισμένες κακόβουλες συναλλαγές ενδέχεται να εκτελούνται από αξιόπιστους κακόβουλους επικυρωτές. Για την επίλυση αυτού του προβλήματος, καθορίζεται ένα ορισμένο διάστημα δειγματοληψίας που καθορίζει πόσο συχνά οι κανονικοί επικυρωτές θα πρέπει να επαληθεύουν συναλλαγές στη δεύτερη φάση, εντοπίζοντας έτσι τυχόν ασυνέπειες. Έτσι λοιπόν, εάν ένας επικυρωτής εντοπιστεί ως κακόβουλος, θα χάσει όλα τα διακριτικά και τη φήμη του στο σύστημα.

2.1.8 Proof of Activity

Το Proof-of-Activity (PoA) είναι ένας αλγόριθμος συναίνεσης blockchain που χρησιμοποιείται σε κρυπτονομίσματα και παρόμοια συστήματα. Χρησιμοποιείται για να διασφαλίσει ότι όλες οι συναλλαγές που πραγματοποιούνται στο blockchain είναι γνήσιες, καθώς και για να διασφαλιστεί ότι όλοι οι εξορύκτες καταλήγουν σε συναίνεση. Το PoA είναι ένας συνδυασμός δύο άλλων αλγορίθμων συναίνεσης blockchain: proof-of-work (PoW) και proof-of-stake (PoS).

Το σύστημα PoA είναι μια προσπάθεια συνδυασμού των καλύτερων πτυχών τόσο των συστημάτων PoW όσο και των συστημάτων PoS. Στο PoA, η διαδικασία εξόρυξης ξεκινά με τον ίδιο τρόπο όπως σε μια διαδικασία PoW, με διάφορους ανθρακωρύχους να προσπαθούν να ξεπεράσουν ο ένας τον άλλον με μεγαλύτερη υπολογιστική ισχύ για να βρουν ένα νέο μπλοκ. Όταν βρεθεί ένα νέο μπλοκ (ή εξορύσσεται), το σύστημα αλλάζει σε PoS, με το μπλοκ που βρέθηκε πρόσφατα να περιέχει μόνο μια κεφαλίδα και τη διεύθυνση ανταμοιβής του ανθρακωρύχου.

Με βάση τις λεπτομέρειες της κεφαλίδας, επιλέγεται μια νέα, τυχαία ομάδα επικυρωτών από το δίκτυο blockchain, η οποία υποχρεούται να επικυρώσει ή να υπογράψει το νέο μπλοκ. Όσο περισσότερα νομίσματα κατέχει ένας επικυρωτής, τόσο περισσότερες πιθανότητες έχει να επιλεγεί ως υπογράφων.

Μόλις όλοι οι επικυρωτές υπογράψουν το μπλοκ που βρέθηκε, εντοπίζεται και προστίθεται στο δίκτυο blockchain και οι συναλλαγές αρχίζουν να καταγράφονται σε αυτό. Σε περίπτωση που ορισμένοι από τους επιλεγμένους υπογράφοντες δεν είναι διαθέσιμοι για να υπογράψουν το μπλοκ στην ολοκλήρωση, η διαδικασία μετακινείται

στο επόμενο μπλοκ νίκης με ένα νέο σετ επικυρωτών, το οποίο επιλέγεται τυχαία, με γνώμονα το ποσό των κερμάτων τους. Αυτή η διαδικασία συνεχίζεται έως ότου ένα νικητήριο μπλοκ λάβει τον απαιτούμενο αριθμό υπογραφών και γίνει πλήρες μπλοκ. Τα έξοδα εξόρυξης ή ανταμοιβές κατανέμονται μεταξύ του ανθρακωρύχου και των διαφόρων επικυρωτών που συνέβαλαν στους αντίστοιχους ρόλους τους για να εγγραφούν στο μπλοκ.

Δεδομένου ότι το σύστημα PoA παντρεύει τα PoW και PoS, επικρίνει την μερική χρήση και των δύο. Απαιτείται πάρα πολύ δύναμη για την εξόρυξη μπλοκ κατά τη φάση PoW και οι κερματοδέκτες εξακολουθούν να έχουν περισσότερες πιθανότητες να μπουν στη λίστα των υπογραφόντων και να συγκεντρώσουν περισσότερες ανταμοιβές εικονικού νομίσματος.

Παράδειγμα απόδειξης δραστηριότητας (PoA)

Το Decred (DCR) είναι το πιο γνωστό δίκτυο κρυπτογράφησης που χρησιμοποιεί τον μηχανισμό συναίνεσης PoA. Με το Decred, δημιουργούνται μπλοκ κάθε πέντε λεπτά. Η διαδικασία εξόρυξης του Decred ξεκινά με κόμβους (υπολογιστές που συμμετέχουν στο δίκτυο) αναζητώντας μια λύση σε ένα κρυπτογραφικό παζλ με γνωστό επίπεδο δυσκολίας για τη δημιουργία ενός νέου μπλοκ. Μέχρι στιγμής, αυτή η διαδικασία μοιάζει με σύστημα PoW. Μόλις βρεθεί η λύση, μεταδίδεται στο δίκτυο και στη συνέχεια, το δίκτυο επαληθεύει τη λύση. Σε αυτό το σημείο, το σύστημα γίνεται PoS. Όσο περισσότερο DCR έχει εξορύξει ένας κόμβος, τόσο πιθανότερο είναι να επιλεγούν να ψηφίσουν στο μπλοκ. Στο blockchain του DCR, οι ενδιαφερόμενοι κερδίζουν εισιτήρια που τους παρέχουν δικαίωμα ψήφου σε αντάλλαγμα για την εξόρυξη DCR. Πέντε εισιτήρια επιλέγονται ψευδο-τυχαία από την ομάδα εισιτηρίων. Εάν τουλάχιστον τρεις από τις πέντε ψήφους είναι "ναι" για την επικύρωση του μπλοκ, προστίθεται μόνιμα στο blockchain. Τέλος, τόσο οι ανθρακωρύχοι όσο και οι ψηφοφόροι ανταμείβονται με DCR.

Τέλος, είναι δεδομένο πως δεν υπάρχει λύση που να ταιριάζει σε όλους, ειδικά όταν πρόκειται για Blockchain. Ο αλγόριθμος Proof of Stake είναι ένα εξαιρετικό παράδειγμα αυτής της δήλωσης, όμως το Proof of Activity έχει κάθε ευκαιρία να το αποδείξει ότι είναι λάθος. Ήδη ανταγωνίζεται το PoS όσον αφορά την ασφάλεια και την επεκτασιμότητα, έχοντας την ευκαιρία να γίνει ένας από τους ηγέτες στον κόσμο της αποκέντρωσης.

2.1.9 Proof of Authority

Σε ένα εγκεκριμένο blockchain, όλοι οι κόμβοι έχουν προ-πιστοποιηθεί. Αυτό το πλεονέκτημα επιτρέπει τη χρήση τύπων συναίνεσης που παρέχουν υψηλό ποσοστό συναλλαγών εκτός από άλλα οφέλη. Ένας από αυτούς τους τύπους συναίνεσης είναι η συναίνεση Proof-of-Authority (PoA).

Το Proof-of-Authority (PoA) είναι μια οικογένεια αλγορίθμων συναίνεσης που παρέχει υψηλή απόδοση και ανοχή σφαλμάτων. Στο PoA, τα δικαιώματα δημιουργίας νέων μπλοκ απονέμονται σε κόμβους που έχουν αποδείξει την εξουσία τους να το κάνουν. Για να αποκτήσετε αυτήν την εξουσία και το δικαίωμα δημιουργίας νέων μπλοκ, ένας κόμβος πρέπει να περάσει από έναν προκαταρκτικό έλεγχο ταυτότητας.

Σε σύγκριση με άλλους τύπους συναίνεσης που απαιτούν απόδειξη των εξαντλημένων υπολογιστικών πόρων (Proof-of-Work) ή ένα υπάρχον "μερίδιο" (Proof-of-Stake), η συναίνεση PoA έχει αρκετά αξιοσημείωτα πλεονεκτήματα. Αρχικά, δεν απαιτείται υψηλής απόδοσης hardware. Σε σύγκριση με τη συναίνεση PoW, η συναίνεση PoA δεν απαιτεί κόμβους για να δαπανήσουν υπολογιστικούς πόρους για την επίλυση πολύπλοκων μαθηματικών εργασιών. Ακόμη, το χρονικό διάστημα στο οποίο δημιουργούνται νέα μπλοκ είναι προβλέψιμο, ενώ για τα PoW και PoS, αυτό διαφέρει.

Τα δίκτυα που λειτουργούν με Proof-of-Authority έχουν υψηλό ποσοστό συναλλαγών, δηλαδή τα μπλοκ δημιουργούνται σε μια σειρά σε ένα καθορισμένο χρονικό διάστημα από εξουσιοδοτημένους κόμβους δικτύου. Αυτό αυξάνει την ταχύτητα επικύρωσης των συναλλαγών. Επίσης ο συγκεκριμένος αλγόριθμος προσφέρει ανοχή σε παραβιασμένους και κακόβουλους κόμβους, εφόσον το 51% των κόμβων δεν έχει παραβιαστεί.

Η αντίληψη του μηχανισμού PoA είναι ότι απέχει από την αποκέντρωση. Θα μπορούσε λοιπόν κανείς να πει ότι αυτό το μοντέλο αλγορίθμου συναίνεσης είναι απλώς μια προσπάθεια να γίνουν τα κεντρικά συστήματα πιο αποτελεσματικά. Αν και αυτό καθιστά το PoA μια ελκυστική λύση για μεγάλες εταιρείες με υλικοτεχνικές ανάγκες, όντως φέρνει κάποιο δισταγμό ειδικά στο πεδίο εφαρμογής των κρυπτονομισμάτων. Τα συστήματα PoA έχουν υψηλή απόδοση, αλλά οι πτυχές της σταθερότητας τίθονται υπό αμφισβήτηση όταν πράγματα όπως η ανιχνευσιμότητα μπορούν να επιτευχθούν εύκολα.

Μια άλλη κοινή κριτική είναι ότι οι ταυτότητες των επικυρωτών PoA είναι ορατές σε οποιονδήποτε. Το επιχείρημα εναντίον αυτού είναι ότι μόνο καθιερωμένοι παίκτες που μπορούν να κατέχουν αυτή τη θέση θα επιδιώκουν να γίνουν επικυρωτές ως δημόσια

γνωστοί συμμετέχοντες. Ωστόσο, η γνώση της ταυτότητας των επικυρωτών θα μπορούσε ενδεχομένως να οδηγήσει σε χειραγώγηση τρίτων. Για παράδειγμα, εάν ένας ανταγωνιστής θέλει να διακόψει ένα δίκτυο που βασίζεται σε PoA, μπορεί να προσπαθήσει να επηρεάσει γνωστούς δημόσιους επικυρωτές να ενεργήσουν ανέντιμα προκειμένου να διακυβεύσει το σύστημα εκ των έσω.

Το PoW, το PoS ή το PoA έχουν όλα τα δικά τους μοναδικά πλεονεκτήματα και μειονεκτήματα. Είναι γνωστό ότι η αποκέντρωση εκτιμάται ιδιαίτερα στην κοινότητα των κρυπτονομισμάτων και η PoA, ως μηχανισμός συναίνεσης, θυσιάζει την αποκέντρωση προκειμένου να επιτύχει υψηλή απόδοση και επεκτασιμότητα. Τα εγγενή χαρακτηριστικά των συστημάτων PoA είναι μια έντονη αντίθεση με το πώς λειτουργούσαν μέχρι τώρα τα blockchain. Ωστόσο, το PoA παρουσιάζει μια ενδιαφέρουσα προσέγγιση και δεν μπορεί να αγνοηθεί ως μια αναδυόμενη λύση blockchain, η οποία μπορεί να ταιριάζει καλά για ιδιωτικές εφαρμογές blockchain.

2.1.10 Proof of Capacity

Ένας άλλος αλγόριθμος συναίνεσης είναι το Proof-of-Capacity (PoC), επίσης γνωστό ως Proof-of-Space (PoSpace). Μία απ’τις λίγες πλατφόρμες blockchain, η οποία προς το παρόν υποστηρίζει αυτόν τον αλγόριθμο είναι η Burstcoin.

Το PoC λειτουργεί χρησιμοποιώντας την ακόλουθη προσέγγιση. Κάθε ανθρακωρύχος υπολογίζει αρκετά μεγάλο αριθμό δεδομένων, τα οποία καταγράφονται σε ένα υποσύστημα δίσκου ενός κόμβου: σκληρός δίσκος, αποθήκευση cloud ή άλλα. Αυτό το αρχικό σύνολο δεδομένων στο PoC ονομάζεται space. Στη συνέχεια για κάθε νέο μπλοκ στο blockchain, ο ανθρακωρύχος διαβάζει ένα μικρό σύνολο δεδομένων που ισούται με το 1/4096, το οποίο είναι περίπου 0,024% όλων των αποθηκευμένων δεδομένων. Έτσι λοιπόν, επιστρέφει το αποτέλεσμα ή προθεσμία ως το χρόνο που έχει παρέλθει από τη δημιουργία του τελευταίου μπλοκ, μετά από τον οποίο ο ανθρακωρύχος μπορεί να δημιουργήσει ένα νέο μπλοκ. Τέλος, ο ανθρακωρύχος που έλαβε ελάχιστη προθεσμία υπογράφει το μπλοκ και λαμβάνει ανταμοιβή για συναλλαγές.

Έτσι, οι υπολογιστικοί πόροι που απαιτούνται για αυτήν την εργασία περιορίζονται από το χρόνο που απαιτείται για την ανάγνωση αρχείων από ένα υποσύστημα δίσκου. Αυτό είναι το κύριο πράγμα που επιτρέπει την εκτέλεση εξόρυξης με αρκετά υψηλή ενεργειακή απόδοση. Οι ανθρακωρύχοι ανταγωνίζονται μεταξύ τους για το ποσό των

αποθηκευμένων δεδομένων και όχι για την ταχύτητα του εξοπλισμού, η οποία καθορίζει την εξόρυξη στο PoW.

Κάποια προβλήματα τα οποία παρατηρούνται στο συγκεκριμένο αλγόριθμο θα αναλυθούν παρακάτω. Αρχικά, οι μονάδες δίσκου που χρησιμοποιούνται για την αποθήκευση δεδομένων έχουν πολύ ελεύθερο χώρο, το οποίο καθιστά δύσκολο τον εντοπισμό τυχόν κακόβουλης αποθήκευσης υπολογισμού από εισβολείς δικτύου. Ακόμη, η μαζική υιοθέτηση αυτής της προσέγγισης μπορεί να οδηγήσει σε ανταγωνισμό μεταξύ των πωλητών σκληρών δίσκων υψηλής χωρητικότητας. Τέλος, είναι επιτακτική ανάγκη να αναφέρουμε πως ο PoC εξακολουθεί να μην χρησιμοποιείται σε μαζική χρήση όπως για παράδειγμα ο αλγόριθμος PoW.

2.1.11 Proof of Burn

Ο αλγόριθμος συναίνεσης Proof-of-burn έχει χρησιμοποιηθεί ως μηχανισμός για την καταστροφή των κρυπτονομισμάτων με επαληθεύσιμο τρόπο. Παρά τη γνωστή χρήση του, ο μηχανισμός δεν έχει προηγουμένως μελετηθεί επίσημα ως πρωτόγονος. Έτσι λοιπόν, παρουσιάζουμε τον πρώτο κρυπτογραφικό ορισμό του τι είναι ένα πρωτόκολλο PoB. Αποτελείται από δύο λειτουργίες: Πρώτον, μια συνάρτηση που δημιουργεί μια διεύθυνση κρυπτονομίσματος. Όταν ένας χρήστης στέλνει χρήματα σε αυτή τη διεύθυνση, τα χρήματα καταστρέφονται αμετάκλητα. Δεύτερον, μια συνάρτηση επαλήθευσης που ελέγχει ότι μια διεύθυνση είναι πραγματικά μη αναλώσιμη.

Προτείνουμε τις ακόλουθες ιδιότητες για πρωτόκολλα εγγραφής. Η **απαγόρευση δαπάνης**, η οποία επιβάλλει ότι μια διεύθυνση που επαληθεύεται σωστά ως διεύθυνση εγγραφής δεν μπορεί να χρησιμοποιηθεί για δαπάνες. Η **δεσμευτική**, η οποία επιτρέπει τη συσχέτιση μεταδεδομένων με μια συγκεκριμένη εγγραφή. Ακόμη η **αδυναμία ανίχνευσης**, η οποία επιβάλλει ότι μια διεύθυνση εγγραφής δεν διακρίνεται από μια κανονική διεύθυνση κρυπτονομίσματος. Ο ορισμός μας καταγράφει όλα τα προηγουμένως γνωστά πρωτόκολλα απόδειξης καύσης. Στη συνέχεια, σχεδιάζουμε μια νέα κατασκευή για καύση, η οποία είναι απλή και ευέλικτη, καθιστώντας την συμβατή με όλα τα υπάρχοντα δημοφιλή κρυπτονομίσματα. Αποδεικνύουμε ότι το σχήμα μας είναι ασφαλές στο μοντέλο Random Oracle. Εξερευνούμε την εφαρμογή της καταστροφής αξίας σε ένα κρυπτονόμισμα παλαιού τύπου για την εκκίνηση ενός νέου. Ο χρήστης καίει νομίσματα στο blockchain προέλευσης και στη συνέχεια δημιουργεί μια απόδειξη καύσης, μια σύντομη συμβολοσειρά που αποδεικνύει ότι η καύση έγινε, την οποία στη συνέχεια υποβάλλει στο blockchain προορισμού για να ανταμειφθεί με το αντίστοιχο ποσό. Ο χρήστης μπορεί να χρησιμοποιήσει ένα τυπικό

πορτοφόλι για να πραγματοποιήσει την εγγραφή χωρίς να χρειάζεται εξειδικευμένο λογισμικό, καθιστώντας το πρόγραμμά μας φιλικό προς τον χρήστη. Προτείνουμε μηχανισμούς επαλήθευσης καψίματος με διαφορετικές εγγυήσεις ασφαλείας, σημειώνοντας ότι οι στοχευόμενοι εξορύκτες blockchain δεν χρειάζεται απαραίτητα να παρακολουθούν το blockchain προέλευσης.

Όπως αναφέραμε και προηγουμένως, η μέθοδος λειτουργεί πολύ καλά για τη μεταφορά από ένα "παλιό" σε ένα "νέο" κρυπτονόμισμα. Πιο συγκεκριμένα, όταν το παλιό κρυπτονόμισμα βρίσκεται στο τελικό σημείο της εξόρυξής του, μπορούμε να χρησιμοποιήσουμε τη μέθοδο PoB για να κάψουμε το παλιό, προκειμένου να περάσουμε στο νέο. Αυτός ο αλγόριθμος χρησιμοποιείται στην πλατφόρμα Slimcoin.

Ορισμένα προβλήματα που προκύπτουν με αυτή τη μέθοδο είναι πως οι χρήστες που διαθέτουν πολλά κρυπτονομίσματα ευνοούνται στην μελλοντική εξόρυξη μπλοκ, με αποτέλεσμα να χρειάζεται τεράστιο κεφάλαιο αγοράς για να βελτιωθεί η ασφάλεια και η τυχαιότητα του αλγορίθμου. Τέλος, όπως και στο PoS, η αρχή που διέπει τον αλγόριθμο δεν είναι κατάλληλη για τη διανομή των πρώτων νομισμάτων στο δίκτυο.

2.1.12 Proof of Existence

Η απόδειξη της ύπαρξης (PoE) έχει γίνει ένα πολύ βολικό εργαλείο όταν πρόκειται για δημόσια απόδειξη και γνησιότητα οποιουδήποτε αρχείου ή εγγράφου, επειδή ακόμη και σήμερα, ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα υπογεγραμμένο μήνυμα μπορεί μερικές φορές να μην είναι αρκετό για να αποδείξει κάτι.

Η απόδειξη της ύπαρξης παίρνει απλώς ένα hash και το αποθηκεύει στο Blockchain. Δεδομένου ότι το Blockchain αποθηκεύει όλες τις συναλλαγές που έχουν επιβεβαιωθεί και όλα τα hashes είναι μοναδικά, αφού επιβεβαιωθεί αυτή η συναλλαγή, μπορεί να αναφερθεί ξανά για να αποδειχθεί ότι υπάρχει ένα συγκεκριμένο έγγραφο.

Οι άνθρωποι μπορούν να αποκαλύψουν δημόσια τι έχουν βρει και αν προκύψει σύγκρουση μπορούν να αποδείξουν ότι είχαν τα δεδομένα που δημιούργησαν εξαρχής. Η απόδειξη ύπαρξης είναι χρήσιμη για υλικό που προστατεύεται από πνευματικά δικαιώματα, διπλώματα ευρεσιτεχνίας κ.λπ. Έτσι λοιπόν, ένα άτομο μπορεί να αποδείξει ότι ορισμένα δεδομένα υπάρχουν σε μια συγκεκριμένη στιγμή του χρόνου. Καθώς χρησιμοποιούμε το Bitcoin Blockchain για να αποθηκεύσουμε την απόδειξη του εγγράφου, ο καθένας μπορεί να πιστοποιήσει την ύπαρξη ενός εγγράφου χωρίς την ανάγκη να πιστοποιηθεί από μια κεντρική αρχή. Η υπολογιστική ισχύς ολόκληρου του δικτύου bitcoin χρησιμοποιείται για την πιστοποίηση δεδομένων.

Μερικές από τις κοινές χρήσεις για PoE είναι:

- Επίδειξη ιδιοκτησίας δεδομένων χωρίς αποκάλυψη πραγματικών δεδομένων.
- Σφραγίδα χρόνου εγγράφου.
- Παροχή ιδιοκτησίας και μεταφορά πράξης
- Πραγματοποίηση περιουσιακών στοιχείων
- Έλεγχος ακεραιότητας εγγράφου

Εάν ένα άτομο αποθηκεύσει μια απόδειξη για το έγγραφό του και αργότερα το ανεβάσει ξανά, το σύστημα θα το αναγνωρίσει μόνο εάν είναι πλήρως το ίδιο έγγραφο. Η παραμικρή αλλαγή να έχει γίνει και το Blockchain αναγνωρίζει ότι είναι διαφορετική. Αυτό παρέχει στον χρήστη την απαιτούμενη ασφάλεια ότι τα πιστοποιημένα δεδομένα δεν μπορούν να αλλάξουν.

Είναι προφανές ότι τα δίκτυα Blockchain δεν προορίζονται μόνο για περιπτώσεις οικονομικής χρήσης και στην πραγματικότητα, λόγω της γενικής φύσης τους, μπορούν να χρησιμοποιηθούν σχεδόν σε κάθε σενάριο. Αξίζει επίσης να σημειωθεί ότι τα δίκτυα που λειτουργούν με PoE, που αρχικά προσφέρθηκε από το Bitcoin Blockchain, όχι μόνο επέτρεψε στους προγραμματιστές και τους επιχειρηματίες να δημιουργήσουν περαιτέρω περιπτώσεις χρήσης αυτής της τεχνολογίας, αλλά μπορούμε επίσης να παρατηρήσουμε μια πληθώρα αλυσίδων κοινοπραξιών που έχουν δημιουργηθεί σε blockchain εταιρικής ποιότητας.

Οι «bull runs» για κρυπτονομίσματα έχουν επίσης κλιμακώσει τη δημοτικότητα των blockchain και είναι μια αξιοπρεπής χειρονομία που οι κυβερνήσεις άρχισαν να υιοθετούν. Ο όρος «bull run» είναι η χρονική περίοδος κατά την οποία η πλειονότητα των επενδυτών αγοράζει, η ζήτηση υπερτερεί της προσφοράς και οι τιμές αυξάνονται. Η χειρονομία αυτή όχι μόνο θα προωθήσει τις δραστηριότητές τους, αλλά θα επέτρεπε και σε πολλές άλλες χώρες να αναλάβουν την ηγεσία και να χρησιμοποιήσουν την τεχνολογία blockchain για να παρέχουν καλύτερες λύσεις για τους πολίτες τους.

2.1.13 Proof of Practical Byzantine Fault Tolerance

Το Practical Byzantine Fault Tolerance είναι ένας αλγόριθμος συναίνεσης που εισήχθη στα τέλη της δεκαετίας του '90. Το pBFT σχεδιάστηκε για να λειτουργεί αποτελεσματικά σε ασύγχρονα συστήματα (χωρίς ανώτερο όριο όταν θα ληφθεί η απόκριση στην αίτηση). Βελτιστοποιείται για χαμηλό γενικό χρόνο και έχει ως στόχο του να επιλύει πολλά προβλήματα που σχετίζονται με ήδη διαθέσιμες λύσεις βυζαντινής βλάβης. Οι περιοχές εφαρμογών περιλαμβάνουν κατανεμημένους υπολογιστές και blockchain.

Το Byzantine Fault Tolerance (BFT) είναι το χαρακτηριστικό ενός κατανεμημένου δικτύου για την επίτευξη συναίνεσης ακόμη και όταν ορισμένοι από τους κόμβους του δικτύου δεν ανταποκρίνονται ή ανταποκρίνονται με εσφαλμένες πληροφορίες. Ο στόχος ενός μηχανισμού BFT είναι η προστασία από τις αστοχίες του συστήματος χρησιμοποιώντας συλλογική λήψη αποφάσεων που στοχεύει στη μείωση της επιρροής των ελαττωματικών κόμβων. Προσπαθεί δηλαδή να παρέχει μια πρακτική αναπαραγωγή βυζαντινής κατάστασης που μπορεί να λειτουργήσει ακόμα και όταν λειτουργούν κακόβουλοι κόμβοι στο σύστημα.

Οι κόμβοι σε ένα κατανεμημένο σύστημα με δυνατότητα pBFT ταξινομούνται διαδοχικά με έναν κόμβο να είναι ο κύριος (ή ο κόμβος οδηγός) και άλλοι που αναφέρονται ως δευτερεύοντες (ή οι εφεδρικοί κόμβοι). Εδώ χρειάζεται να σημειωθεί ότι οποιοσδήποτε κατάλληλος κόμβος στο σύστημα μπορεί να γίνει ο πρωτεύων με μετάβαση από δευτερεύοντα σε πρωτεύοντα, το οποίο συμβαίνει στην περίπτωση αποτυχίας πρωτεύοντος κόμβου. Ο στόχος είναι ότι όλοι οι ειλικρινείς κόμβοι να βοηθούν στην επίτευξη συναίνεσης σχετικά με την κατάσταση του συστήματος χρησιμοποιώντας τον κανόνα της πλειοψηφίας.

Ένα πρακτικό σύστημα βυζαντινού σφάλματος μπορεί να λειτουργήσει με την προϋπόθεση ότι ο μέγιστος αριθμός κακόβουλων κόμβων δεν πρέπει να είναι μεγαλύτερος ή ίσος με το ένα τρίτο όλων των κόμβων του συστήματος. Προφανώς, καθώς ο αριθμός των κόμβων αυξάνεται, το σύστημα γίνεται πιο ασφαλές.

Οι γύροι συναίνεσης του pBFT χωρίζονται σε 4 φάσεις:

- Ο πελάτης στέλνει ένα αίτημα στον κύριο κόμβο (leader).
- Ο κύριος κόμβος (ηγέτης) μεταδίδει το αίτημα σε όλους τους δευτερεύοντες (εφεδρικούς) κόμβους.
- Οι κόμβοι (πρωτογενείς και δευτερεύοντες) εκτελούν την ζητούμενη υπηρεσία και, στη συνέχεια, στέλνουν μια απάντηση στον πελάτη.
- Το αίτημα προβάλλεται με επιτυχία όταν ο πελάτης λαμβάνει απαντήσεις «m + 1» από διαφορετικούς κόμβους στο δίκτυο με το ίδιο αποτέλεσμα, όπου m είναι ο μέγιστος επιτρεπόμενος αριθμός ελαττωματικών κόμβων.

Ακόμη, υπάρχουν μερικά προβλήματα ή αλλιώς όρια, τα οποία μας απασχολούν για τον αλγόριθμο pBFT. Το συναινετικό μοντέλο pBFT λειτουργεί αποτελεσματικά μόνο όταν ο αριθμός των κόμβων στο κατανεμημένο δίκτυο είναι μικρός λόγω του υψηλού κόστους επικοινωνίας που αυξάνεται εκθετικά με κάθε επιπλέον κόμβο στο δίκτυο. Οι μηχανισμοί pBFT είναι επιρρεπείς σε επιθέσεις Sybil, όπου μια οντότητα

(συμβαλλόμενο μέρος) ελέγχει πολλές ταυτότητες. Καθώς ο αριθμός των κόμβων στο δίκτυο αυξάνεται, οι επιθέσεις Sybil γίνονται όλο και πιο δύσκολο να πραγματοποιηθούν.

Τέλος, υπάρχει το βασικό πρόβλημα της κλιμάκωσης. Το pBFT δεν κλιμακώνεται καλά λόγω της επιβάρυνσης της επικοινωνίας του με όλους τους άλλους κόμβους σε κάθε βήμα. Καθώς ο αριθμός των κόμβων στο δίκτυο αυξάνεται (αυξάνεται ως O(n^k), όπου n είναι τα μηνύματα και k είναι ο αριθμός των κόμβων), τόσο αυξάνεται και ο χρόνος που απαιτείται για την απάντηση στο αίτημα. Καθώς όμως, οι μηχανισμοί pBFT έχουν προβλήματα επεκτασιμότητας, ο μηχανισμός pBFT χρησιμοποιείται πολύ επιτυχημένα σε συνδυασμό με άλλους μηχανισμούς.

2.1.14 DAGs consensus algorithm

Το DAG είναι ένα διαφορετικό είδος δομής δεδομένων το οποίο είναι σαν μια βάση δεδομένων που συνδέει διαφορετικά κομμάτια πληροφοριών μαζί.

Τέτοιες δομές δεδομένων χρησιμοποιούνται γενικά για τη μοντελοποίηση δεδομένων. Μπορεί να βασιστείτε σε μια DAG σε επιστημονικούς ή ιατρικούς τομείς για να παρατηρήσετε τη σχέση μεταξύ των μεταβλητών και να προσδιορίσετε πώς επηρεάζουν ο ένας τον άλλον. Για παράδειγμα, θα μπορούσατε να πάρετε πράγματα όπως η διατροφή, οι κύκλοι ύπνου και τα σωματικά συμπτώματα, έτσι ώστε να μπορείτε να σχεδιάσετε συνδέσμους μεταξύ τους για να διαπιστώσετε πώς επηρεάζουν έναν ασθενή. Για τους σκοπούς μας, ενδιαφερόμαστε περισσότερο για το πώς μπορούν να συμβάλουν στην επίτευξη συναίνεσης σε ένα κατανεμημένο δίκτυο κρυπτογράφησης. Σε ένα τέτοιο σύστημα με βάση το DAG, κάθε κορυφή στη δομή αντιπροσωπεύει μια συναλλαγή. Δεν υπάρχει έννοια των μπλοκ εδώ, ούτε απαιτείται εξόρυξη για την επέκταση της βάσης δεδομένων. Έτσι, αντί να συλλέγονται συναλλαγές σε μπλοκ, κάθε συναλλαγή είναι χτισμένη η μία πάνω στην άλλη. Ακόμα, υπάρχει μια μικρή λειτουργία Proof-of-Work που γίνεται όταν ένας κόμβος υποβάλλει μια συναλλαγή και έτσι διασφαλίζεται ότι το δίκτυο δεν είναι ανεπιθύμητο και επικυρώνει προηγούμενες συναλλαγές.

Πλεονεκτήματα των DAGs

- Ταχύτητα
  Χωρίς περιορισμούς από τους χρόνους αποκλεισμού, ο καθένας μπορεί να μεταδώσει και να επεξεργαστεί τις συναλλαγές του ανά πάσα στιγμή. Δεν

υπάρχει όριο στον αριθμό των συναλλαγών που υποβάλλουν οι χρήστες, υπό την προϋπόθεση ότι επιβεβαιώνουν τις παλαιότερες όπως κάνουν.

- Δεν υπάρχει εξόρυξη

  Οι DAG δεν χρησιμοποιούν αλγόριθμους συναίνεσης PoW με τον τρόπο που έχουμε συνηθίσει. Το αποτύπωμα άνθρακα τους είναι, συνεπώς, ένα κλάσμα εκείνου των κρυπτονομισμάτων που βασίζονται στην εξόρυξη για να διασφαλίσουν το δίκτυο blockchain

- Δεν υπάρχουν χρεώσεις συναλλαγής

  Επειδή δεν υπάρχουν ανθρακωρύχοι, οι χρήστες δεν χρειάζεται να πληρώνουν τέλη για τη μετάδοση των συναλλαγών τους. Τούτου λεχθέντος, ορισμένοι απαιτούν να καταβάλλεται μια μικρή χρέωση σε ειδικά είδη κόμβων. Τα χαμηλά τέλη (ή καλύτερα, μηδενικά τέλη) είναι δελεαστικά για τις μικροπληρωμές, καθώς ο σκοπός τους νικά με σημαντικές χρεώσεις δικτύου.

- Δεν υπάρχουν προβλήματα επεκτασιμότητας

  Χωρίς περιορισμούς από τους χρόνους αποκλεισμού, οι DAG μπορούν να επεξεργαστούν πολλές περισσότερες συναλλαγές ανά δευτερόλεπτο από τα παραδοσιακά δίκτυα blockchain. Πολλοί υποστηρικτές πιστεύουν ότι αυτό θα τους κάνει πολύτιμους σε περιπτώσεις χρήσης του Internet of Things (IoT), όπου όλα τα είδη μηχανών θα αλληλεπιδρούν μεταξύ τους.

Μειονεκτήματα των DAG

- Δεν είναι πλήρως αποκεντρωμένο

  Τα πρωτόκολλα που βασίζονται σε DAG έχουν διάφορα στοιχεία συγκέντρωσης. Για μερικούς, υποτίθεται ότι είναι μια βραχυπρόθεσμη λύση για την εκκίνηση του δικτύου, αλλά απομένει να δούμε αν οι DAG μπορούν να ευδοκιμήσουν χωρίς την παρέμβαση τρίτων. Εάν όχι, ανοίγουν για να επιτεθούν σε διανύσματα που θα μπορούσαν τελικά να καταστρέψουν τα δίκτυά τους.

- Δεν έχει δοκιμαστεί σε μεγάλη κλίμακα

  Αν και τα κρυπτονομίσματα που βασίζονται στο DAG υπάρχουν εδώ και μερικά χρόνια, έχουν πολύ δρόμο να διανύσουν προτού να δουν ευρεία χρήση. Ως εκ τούτου, είναι δύσκολο να προβλέψουμε ποια κίνητρα ενδέχεται να έχουν οι χρήστες για να εκμεταλλευτούν το σύστημα στο μέλλον.

Στη συνέχεια, θα συγκρίνουμε τα δίκτυα Blockchain με τα δίκτυα DAG. Το Blockchain είναι ένα κατανεμημένο καθολικό, που αναπαράγεται από όλους τους κόμβους του δικτύου. Αυτό το κατανεμημένο καθολικό σχηματίζει μια αλυσίδα μπλοκ συναλλαγών με αμετάβλητη, χρονολογική σειρά. Οι συναλλαγές ομαδοποιούνται σε μπλοκ προς επικύρωση. Τα επικυρωμένα μπλοκ σφραγίζονται και προστίθενται σε μια αλυσίδα προηγουμένως επικυρωμένων μπλοκ.

Συγκριτικά, ένα DAG είναι ένα δίκτυο μεμονωμένων συναλλαγών που συνδέονται με πολλές άλλες συναλλαγές. Δεν υπάρχουν μπλοκ συναλλαγών στα δίκτυα DAG. Εάν το blockchain είναι μια συνδεδεμένη λίστα, ένα DAG είναι ένα δέντρο, που διακλαδώνεται από τη μια συναλλαγή στην άλλη, στην άλλη και ούτω καθεξής.

2.2 Κρυπτονομίσματα με μέλλον

2.2.1 Ripple

Η Ripple είναι μια τεχνολογία που λειτουργεί τόσο ως κρυπτονόμισμα αλλά και ψηφιακό δίκτυο πληρωμών σε χρηματοοικονομικές συναλλαγές. Κυκλοφόρησε για πρώτη φορά το 2012 και ιδρύθηκε από τους Chris Larsen και Jeb McCaleb. Η βασική λειτουργεία της Ripple είναι η ανταλλαγή περιουσιακών στοιχείων και εμβασμάτων διακανονισμού πληρωμών παρόμοιο με το σύστημα Switch για διεθνείς μεταφορές χρημάτων και ασφαλείας, το οποίο χρησιμοποιείται από τράπεζες και χρηματοπιστωτικούς μεσάζοντες που συναλλάσονται σε διάφορα νομίσματα. Το διακριτικό που χρησιμοποιείται ως κρυπτονόμισμα είναι προεγκατεστημένο και χρησιμοποιεί το σύμβολο XRP. Η Ripple είναι το όνομα της εταιρείας και του δικτύου και το XRP είναι το διακριτικό κρυπτογράφησης. Ο σκοπός του XRP είναι να χρησιμεύει ως ένα ενδιάμεσος μηχανισμός ανταλλαγής μεταξύ δύο νομισμάτων ή δικτύων ως ένα είδος προσωρινής ονομαστικής αξίας διακανονισμού.

Στην ουσία, η Ripple είναι ένα ψηφιακό δίκτυο πληρωμών βασισμένο σε blockchain με πρωτόκολλο που έχει το δικό του κρυπτονόμισμα XRP. Αντί να χρησιμοποιεί εξόρυξη blockchain η Ripple χρησιμοποιεί ένα μηχανισμό συναίνεσης μέσω μιας ομάδας διακομιστών που ανήκουν σε τράπεζες για να επιβεβαιώσει τις συναλλαγές. Οι συναλλαγές κυματισμού χρησιμοποιούν πολύ λιγότερη ενέργεια από το Bitcoin, επιβεβαιώνονται σε δευτερόλεπτα και κοστίζουν ελάχιστα, σε αντίθεση με τις συναλλαγές του Bitcoin που χρειάζονται περισσότερο χρόνο για να πραγματοποιηθούν και έχουν μεγαλύτερο κόστος συναλλαγής.

Το XRP συγκαταλέγεται ανάμεσα στα 5 πιο πολύτιμα tokens που βασίζονται σε blockchain βάση της κεφαλαιοποίησης της αγοράς. Η Ripple λειτουργεί ως μια αποκεντρωμένη πλατφόρμα ανοιχτού κώδικα και «peer to peer» που επιτρέπει την απρόσκοπτη μεταφορά χρημάτων σε οποιαδήποτε μορφή είτε πρόκειται για δολάρια, γιεν, ευρώ ή κρυπτονομίσματα. Η Ripple είναι ένα παγκόσμιο δίκτυο πληρωμών και μετράει μεγάλες τράπεζες και χρηματικο-οικονομικές υπηρεσίες μεταξύ των πελατών του. Το XRP χρησιμοποιείται στα προϊόντα του για να διευκολύνει τη γρήγορα μετατροπή μεταξύ διαφορετικών νομισμάτων. Ο τρόπος που λειτουργεί το σύστημα γίνεται πιο εύκολα κατανοητός εάν αναλογιστούμε πως λειτουργεί μια δομή μεταφοράς χρημάτων όπου τα δύο μέρη σε κάθε άκρο της συναλλαγής χρησιμοποιούν τους προτεινόμενους μεσάζοντες για να λάβουν τα χρήματα. Στη πραγματικότητα η Ripple λειτουργεί ως ψηφιακή υπηρεσία Havala, η οποία είναι μια άτυπη μέθοδος μεταφοράς χρημάτων, συνήθως διασυνοριακά, χωρίς πραγματικά χρήματα να μετακινούνται. Παρόλο που το δίκτυο Ripple είναι αρκετά περίπλοκο καταδεικνύει τα βασικά στοιχεία του τρόπου λειτουργείας του συστήματος. Η Ripple χρησιμοποιεί ένα μέσο γνωστό gateway (πύλη) ως σύνδεσμο στην αλυσίδα εμπιστοσύνης μεταξύ δύο ομάδων που θέλουν να κάνουν μια συναλλαγή. Το gateway ενεργεί ως μεσίτης πιστώσεων που λαμβάνει και στέλνει νομίσματα σε δημόσιες διευθύνσεις μέσω του δικτύου Ripple. Οποιοσδήποτε ή οποιαδήποτε επιχείρηση μπορεί να εγγραφεί και να ανοίξει μια πύλη, η οποία εξουσιοδοτεί τον καταχωρήσα να ενεργεί ως μεσάζων στην ανταλλαγή νομισμάτων, τη διατήρηση ρευστότητας και τη μεταφορά πληρωμών στο δίκτυο. Όσον αφορά το ψηφιακό νόμισμα της Ripple, το XRP, λειτουργεί ως γέφυρα σε άλλα νομίσματα και δεν κάνει διάκριση μεταξύ οποιουδήποτε κρυπτονομίσματος, το οποίο διευκολύνει την ανταλλαγή νομίσματος με άλλα. Κάθε νόμισμα στο οικοσύστημα έχει τη δική του πύλη και για να γίνει μια συναλλαγή σχηματίζεται μία αλυσίδα πυλών, η οποία ονομάζεται αλυσίδα εμπιστοσύνης στους χρήστες. Η διατήρηση υπολοίπων με μία πύλη εκθέτει το χρήστη σε κίνδυνο αντίστοιχο με αυτόν που υπάρχει και στο παραδοσιακό τραπεζικό σύστημα. Εάν η πύλη δεν τηρήσει την ευθύνη της ο χρήστης θα μπορούσε να χάσει την αξία των χρημάτων που διατηρεί σε αυτή τη πύλη. Οι χρήστες που δεν εμπιστεύονται μια πύλη μπορούν να συναλλάσονται σε μια αξιόπιστη πύλη που και αύτη με τη σειρά της ασχολείται με μία άλλη αξιόπιστη πύλη. Έτσι λοιπόν, το IOU θα πραγματοποιείται μέσω της αξιόπιστης ή πιστοποιημένης πύλης και ο κίνδυνος αντισυμβαλλομένου δεν ισχύει για τα Bitcoin και τα περισσότερα AltCoins, καθώς το Bitcoin ενός χρήστη δεν αποτελεί IOU ή ευθύνη άλλου χρήστη. Ο όρος «IOU» είναι ένα οφειλόμενο ή ανεξόφλητο χρέος.

Στη συνέχεια θα εξηγήσουμε πως λειτουργεί το δίκτυο Ripple. Οι συναλλαγές στο δίκτυο αυτό βασίζονται σε ένα πρωτόκολλο συναίνεσης για την επικύρωση των υπολοίπων λογαριασμών και των συναλλαγών στο σύστημα. Η συναίνεση αποσκοπεί στη βελτίωση της ακεραιότητας του συστήματος αποτρέποντας τις διπλές δαπάνες. Ένας χρήστης Ripple που ξεκινά μια συναλλαγή με πολλαπλές πύλες, αλλά προσπαθεί να στείλει ένα χρηματικό ποσό στα συστήματα πύλης θα διαγράψει τα πάντα εκτός από την πρώτη συναλλαγή. Οι μεμονωμένοι κατανεμημένοι κόμβοι αποφασίζουν με συναίνεση ποια συναλλαγή έγινε πρώτα και οι επιβεβαιώσεις είναι άμεσες, διάρκειας λίγων δευτερολέπτων. Δεδομένου ότι δεν υπάρχει κεντρική αρχή που να αποφασίζει ποιος μπορεί να δημιουργήσει ένα κόμβο και να επιβεβαιώσει συναλλαγές η πλατφόρμα Ripple περιγράφεται ως αποκεντρωμένη. Η πλατφόρμα αυτή παρακολουθεί όλα τα IOU σε ένα δεδομένο νόμισμα για οποιοδήποτε χρήστη ή πύλη. Οι πιστώσεις IOU και οι ροές συναλλαγών που συμβαίνουν μεταξύ των πορτοφολιών Ripple είναι διαθέσιμα στο κοινό στο βιβλίο συναίνεσης Ripple. Ωστόσο, παρόλο που το ιστορικό χρηματοοικονομικών συναλλαγών καταγράφεται δημόσια και διατίθεται σε blockchain τα δεδομένα δεν συνδέονται με την ταυτότητα ή το λογαριασμό οποιουδήποτε ατόμου ή επιχείρησης. Παρόλα αυτά, το δημόσιο αρχείο όλων των συναλλαγών, δηλαδή το blockchain καθιστά τις πληροφορίες ευαίσθητες σε μέτρα απονομιμοποίησης. Το σύστημα πληρωμών Ripple προορίζεται κυρίως να χρησιμοποιηθεί από τράπεζες, ενώ πιο συγκεκριμένα υπάρχουν ήδη πολλές τέτοιες συμφωνίες, για παράδειγμα με την τράπεζα της Αμερικής. Η Ripple βελτιώνεται σε ορισμένα από τα μειονεκτήματα που αποδίδονται στις παραδοσιακές τράπεζες. Οι συναλλαγές διευθετούνται εντός δευτερολέπτων, παρόλο που η πλατφόρμα χειρίζεται εκατομμύρια συναλλαγές, σε αντίθεση με τις τράπεζες που θα χρειαζόντουσαν πολύ μεγαλύτερο διάστημα για να ολοκληρώσουν ένα τραπεζικό έμβασμα. Τέλος, η αμοιβή για τη διεξαγωγή συναλλαγών στη Ripple είναι επίσης ελάχιστη, σε σύγκριση όχι μόνο με τις μεγάλες τράπεζες, αλλά και με τα υπόλοιπα κρυπτονομίσματα.

2.2.2 Cardano

Το κρυπτονόμισμα Cardano είναι ένα δίκτυο κρυπτονομισμάτων και κέντρο ανοιχτού κώδικα που στοχεύει σε μια δημόσια blockchain πλατφόρμα για έξυπνα συμβόλαια. Η εσωτερική κρυπτογράφηση του κρυπτονομίσματος Cardano ονομάζεται Ada. Το Cardano είναι μια τρίτη γενιά αποκεντρωμένη πλατφόρμα blockchain απόδειξης πονταρίσματος (proof-of-stake) σχεδιασμένη να είναι μια πιο αποτελεσματική εναλλακτική λύση έναντι των δικτύων proof-of-work. Η επεκτασιμότητα, η διαλειτουργικότητα και η βιωσιμότητα σε δίκτυα proof-of-work περιορίζονται από την

επιβάρυνση της υποδομής του αυξανόμενου κόστους, τη χρήση ενέργειας και τους αργούς χρόνους συναλλαγών σε σύγκριση πάντα με τον κόσμο των κρυπτονομισμάτων. Επίσης, το Cardano στοχεύει να είναι μια αποκεντρωμένη πλατφόρμα ανάπτυξης dap με καθολικό πολλαπλών στοιχείων και επαληθεύσιμα έξυπνα συμβόλαια. Το πρωτόκολλο στο οποίο βασίζεται, Ouroboros Praos, θεωρείται ένα συγκρίσιμο και αναπαραγώγιμα ασφαλές πρωτόκολλο. Αυτό συμβαίνει επειδή είναι το πρώτο πρωτόκολλο που έχει περάσει από ομότιμους χρήστες για αξιολόγηση και μαθηματικές αποδείξεις. Ως πρωτόκολλο PoS, το Ouroboros είναι γρήγορο, εξαιρετικά επεκτάσιμο και ενεργειακά αποδοτικό, ενώ ταυτόχρονα έχει καταφέρει να μειώσει την κατανάλωση ενέργειας σε σύγκριση με άλλα κρυπτονομίσματα όπως το Bitcoin. Το Ouroboros είναι προγραμματισμένο έτσι ώστε κάθε 20 δευτερόλεπτα να εκδίδεται ένα νέο μπλοκ στο blockchain, κάτι που συνεπάγεται υψηλή ταχύτητα επιβεβαίωσης των συναλλαγών. Η επόμενη έκδοση του Ouroboros Praos θα ονομάζεται Ourobors Hydra και αναμένεται να κάνει μια αξιοσημείωτη βελτίωση στην επεκτασιμότητα του Cardano. Με αυτήν την ενημέρωση, περισσότερες συναλλαγές θα πραγματοποιούνται με χαμηλότερες τιμές και κάθε χρήστης του δικτύου θα δημιουργεί 10 επιπλέον κεφαλές, καθεμία από τις οποίες θα μπορεί να πραγματοποιεί 1000 συναλλαγές ανά δευτερόλεπτο, σύμφωνα με προσομοιώσεις που πραγματοποιήθηκαν από το Πανεπιστήμιο του Εδιμβούργου.

Ακόμη, μία ενδιαφέρουσα χρήση του Cardano blockchain είναι το Atala PRISM. Το Atala PRISM είναι μια αποκεντρωμένη λύση για την πιστοποίηση ταυτότητας που βασίζεται στο blockchain Cardano. Δημιουργεί μια νέα προσέγγιση στη διαχείριση ταυτότητας, όπου οι χρήστες κατέχουν την ταυτότητά τους και έχουν πλήρη έλεγχο του τρόπου με τον οποίο την χρησιμοποιούν και έχουν πρόσβαση τα προσωπικά τους δεδομένα. Τα δεδομένα μοιράζονται με άλλα άτομα ή οργανισμούς μέσω ασφαλών, ιδιωτικών διαύλων επικοινωνίας peer-to-peer. Η Cardano παρέχει αποκεντρωμένη υποδομή δημοσίου κλειδιού (DPKI), η οποία είναι το κλειδί για την ενεργοποίηση εγγραφών που μπορούν να επαληθευτούν άμεσα από οποιονδήποτε και οπουδήποτε. Το DKPI δίνει τη δυνατότητα σε όλους να δημιουργήσουν κρυπτογραφικά κλειδιά στο blockchain με τρόπο που δεν παραβιάζεται και με χρονολογική σειρά. Αυτά τα κλειδιά χρησιμοποιούνται για να επιτρέπουν σε άλλους να επαληθεύουν ψηφιακές υπογραφές ή να κρυπτογραφούν δεδομένα στον αντίστοιχο κάτοχο ταυτότητας. Έτσι λοιπόν, το DPKI είναι ένας ενεργοποιητής για επαληθεύσιμα διαπιστευτήρια. Το blockchain Cardano είναι ιδανικό για χρήση ψηφιακών ταυτοτήτων καθώς είναι εξαιρετικά ασφαλές και σχεδιασμένο για μακροπρόθεσμη βιωσιμότητα. Τέλος, το Atala PRISM χρησιμοποιείται κυρίως σε χώρες της Αφρικής και πιο συγκεκριμένα κατά κύριο λόγο

στην Αιθιοπία, καθώς το μεγαλύτερο μέρος του πληθυσμού για να έχει δυνατότητα για εκπαίδευση και νοσηλεία χρειάζεται να διαθέτει ταυτότητα.

2.3 Tokenization

Υπάρχουν περισσότεροι από ένας τρόποι για να απαντήσετε στην ερώτηση, τι είναι το tokenization; Αυτό συμβαίνει επειδή πολλοί άνθρωποι με διαφορετικές τεχνολογικές κλίσεις ορίζουν το tokenization με διαφορετικούς τρόπους. Ουσιαστικά, το tokenization μπορεί να εφαρμοστεί τόσο στην ασφάλεια δεδομένων όσο και στα ψηφιακά στοιχεία, οπότε δίδεται ελαφρώς διαφορετική έννοια και στα δύο. Από τεχνικής άποψης, ένα Token είναι ένας αλγόριθμος που εφαρμόζεται ως μια σύμβαση σε Blockchain. Ο αλγόριθμος ορίζει όλα τα χαρακτηριστικά του Token όπως η αξία του, πώς και πόσα Tokens δημιουργούνται, πώς τα Tokens δαπανώνται και με ποιο όνομα και διεύθυνση μπορούν να χρησιμοποιηθούν.

Το tokenization, όταν εφαρμόζεται στην κωδικοποίηση δεδομένων, είναι η πράξη ανταλλαγής ενός πολύ ευαίσθητου στοιχείου δεδομένων με ένα με λιγότερο ευαίσθητες πληροφορίες. Αυτά τα λιγότερο ευαίσθητα δεδομένα που αναφέρονται συχνά ως Tokens συνήθως δεν έχουν καμία σημαντική αξία την οποία μπορούν να εκμεταλλευτούν οι κακόβουλοι χρήστες. Το token αντιπροσωπεύει τα υποκείμενα δεδομένα, τα οποία θα μπορούσαν να είναι ομόλογα, μετοχές, αριθμός κύριου λογαριασμού, πληρωμές με πιστωτική κάρτα ή πλήθος άλλων πραγμάτων. Το token είναι συνήθως ένα αναγνωριστικό που μπορεί να οδηγήσει πίσω στα υποκείμενα δεδομένα του. Η μεταφορά δεδομένων από το token στα δεδομένα πίσω από αυτό, και το αντίστροφο είναι δυνατή μόνο μέσω ενός συστήματος tokenization.

Η κωδικοποίηση δεδομένων μπορεί επίσης να σχετίζεται με την τεχνολογία blockchain και τα κρυπτονομίσματα. Σε αυτό το πλαίσιο, το tokenization είναι μια διαδικασία κατά την οποία ορισμένα στοιχεία μετατρέπονται σε tokens, τα οποία διαμένουν στο blockchain. Αυτό συνήθως διευκολύνει την αποθήκευση, την καταγραφή και την υποβολή των συνολικών χαρακτηριστικών των στοιχείων που έχουν δημιουργηθεί με τεχνολογία blockchain.

Σχεδόν οτιδήποτε έχει αξία μπορεί να επισημανθεί και να τοποθετηθεί στο blockchain. Η υπολογιστική ισχύς και η ηλεκτρική χρήση του Bitcoin μετατρέπονται σε ψηφιακό νόμισμα. Κάθε Bitcoin μπορεί να συσχετιστεί άμεσα ή να συνδεθεί με τα περίπλοκα μαθηματικά παζλ που λύθηκαν για την παραγωγή του, καθώς και τον ηλεκτρικό ρεύμα που δαπανήθηκε.

Το Tokenization έχει βοηθήσει στην ανάπτυξη του ψηφιακού οικοσυστήματος που αλλάζει γρήγορα σήμερα, ειδικά στον επαναπροσδιορισμό της διαδικασίας πληρωμής. Για παράδειγμα οι εκτυπωμένοι αριθμοί αναπαράγονται σε αστερίσκους και τελειώνουν με τα τελικά ψηφία. Σε αυτό το σενάριο, ο έμπορος έχει το token και όχι ένα πραγματικό αριθμό κάρτας.

Ένα πιο συγκεκριμένο παράδειγμα θα ήταν το εξής: Όταν ένας πελάτης παρέχει τα στοιχεία πληρωμής του, είτε μέσω διαδικτύου μέσω ιστότοπου ηλεκτρονικού εμπορίου είτε με τερματικό POS, κάθε τιμή δεδομένων αντικαθίσταται με ένα τυχαίο δημιουργημένο διακριτικό. Σε όλες σχεδόν τις περιπτώσεις, η πύλη του πωλητή για πληρωμές είναι υπεύθυνη για τη δημιουργία αυτών των διακριτικών.

Μετά από αυτό, οι κωδικοποιημένες πληροφορίες κρυπτογραφούνται περαιτέρω πριν παραδοθούν μέσω άλλων δικτύων στον επεξεργαστή πληρωμών. Τα αρχικά στοιχεία πληρωμής υπόκεινται σε αποθήκευση στο θησαυροφυλάκιο της πύλης πληρωμής για μάρκες. Είναι το μόνο διαμέρισμα που μπορεί να χρησιμοποιηθεί για την αντιστοίχιση αυτού του διακριτικού στα πραγματικά δεδομένα πληρωμής.

Ο πάροχος του προμηθευτή κρυπτογραφεί ξανά τα δεδομένα προτού στείλει τις λεπτομέρειες σε δίκτυα ACH(Automated Clearing House) ή καρτών για επαλήθευση. Εάν η εξουσιοδότηση είναι επιτυχής, η επιβεβαίωση της συναλλαγής αποστέλλεται μέσω των δικτύων ACH ή καρτών σε όλα τα εμπλεκόμενα μέρη (πύλη πληρωμής, επεξεργαστής, προμηθευτής και πελάτης).

Η πιο σημαντική πλατφόρμα για τη δημιουργία των Tokens σήμερα είναι το Ethereum Blockchain. Επιτρέπει την απλή τεχνική εφαρμογή των Tokens μέσω Smart Contracts. Η σύνδεση μεταξύ ενός Token και του περιουσιακού του στοιχείου είναι αρχικά καθαρά πλασματική. Εάν αφορά ψηφιακό στοιχείο, η σύνδεση μπορεί συνήθως να χαρτογραφηθεί μέσω του κωδικού προγράμματος ενός Smart Contract και έτσι να μείνει σταθερά αγκυροβολημένο. Το παιχνίδι Cryptokitties λειτουργεί με βάση το Ethereum και είναι ένα παράδειγμα αυτού. Είναι μια από τις πρώτες περιπτώσεις όπου τα Tokens έχουν εφαρμοστεί σε περιβάλλον παραγωγής. Αυτός είναι ο λόγος που έχει προσελκύσει πολλή προσοχή και πολλά χρήματα έχουν επενδυθεί και επενδύονται σε αυτά τα εικονικά συλλεκτικά αντικείμενα. Τα μεμονωμένα CryptoKitties συναλλάσονται πάνω από 100.000 $. Όπως και με γραμματόσημα ή νομίσματα, η μοναδικότητα και η σπανιότητα καθορίζει την τιμή. Ο αλγόριθμος του Smart Contract εγγυάται τη μοναδικότητα, δεν επιτρέπει την αντιγραφή και περιορίζει τον μέγιστο αριθμό διαθέσιμων token. Σε περίπτωση που έχουμε φυσικά στοιχεία, αυτή η σύνδεση γίνεται πολύ πιο περίπλοκη. Αν και υπάρχουν εταιρείες που, για παράδειγμα, συνδέουν

ακίνητα ή χρυσό με Tokens. Όμως, η απόδειξη της μοναδικότητας και η σταθερότητα τους βασίζεται πάντα στην εμπιστοσύνη εκτός του Blockchain, π.χ. μέσω ελέγχων ή θεματοφυλάκων.

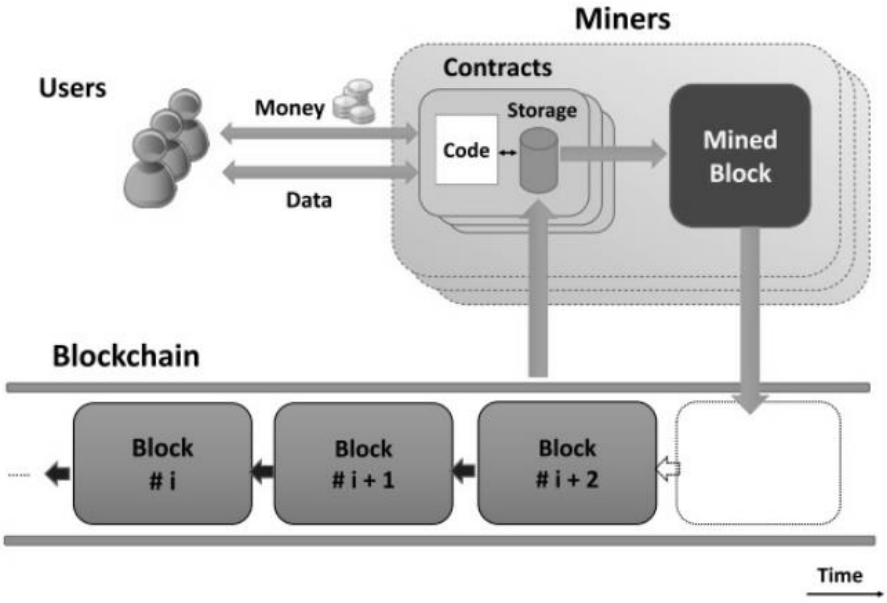
Κεφάλαιο 3: Εφαρμογές Blockchain και Πρόταση Αλγορίθμου

Στο συγκεκριμένο κεφάλαιο θα αναφερθούμε στην αξία που έχουν τα Έξυπνα Συμβόλαια (Smart Contracts) και στο πως αυτά χρησιμοποιούνται. Ακόμη, θα αναφερθούμε στη σύνδεση των δικτύων Blockchain με το IoT και το πως τα δίκτυα αυτά μπορούν να χρησιμοποιηθούν σε βασικούς τομείς από εταιρείες, επιχειρήσεις ακόμα και πολίτες.

3.1 Έξυπνα Συμβόλαια (Smart Contracts) και οι Εφαρμογές τους

3.1.1 Έξυπνα Συμβόλαια (Smart Contracts)

Ένα έξυπνο συμβόλαιο είναι εκτελέσιμος κώδικας που εκτελείται στην αλυσίδα μπλοκ για να διευκολύνει, να εκτελεί και να επιβάλλει τους όρους μιας συμφωνίας. Ο κύριος στόχος ενός έξυπνου συμβολαίου είναι η αυτόματη εκτέλεση των όρων μιας συμφωνίας μόλις πληρούνται οι καθορισμένες προϋποθέσεις. Έτσι, οι έξυπνες συμβάσεις υπόσχονται χαμηλά έξοδα συναλλαγών σε σύγκριση με τα παραδοσιακά συστήματα που απαιτούν ένα αξιόπιστο τρίτο μέρος για την επιβολή και εκτέλεση των όρων μιας συμφωνίας. Η ιδέα των έξυπνων συμβολαίων προήλθε από τον Szabo το 1994. Ωστόσο, η ιδέα δεν είδε το φως της δημοσιότητας μέχρι την εμφάνιση της τεχνολογίας blockchain. Ένα έξυπνο συμβόλαιο μπορεί να θεωρηθεί ως ένα σύστημα που απελευθερώνει ψηφιακά περιουσιακά στοιχεία σε όλους ή σε ορισμένους από τους εμπλεκόμενους μόλις πληρούνται οι αυθαίρετοι προκαθορισμένοι κανόνες. Για παράδειγμα, η Alice στέλνει το νόμισμα X μονάδες στον Bob, αν λάβει Y νομισματικές μονάδες από τον Carl. Πολλοί διαφορετικοί ορισμοί ενός έξυπνου συμβολαίου έχουν συζητηθεί στη βιβλιογραφία. Ταξινομήθηκαν όλοι αυτοί οι ορισμοί σε δύο κατηγορίες, σε κώδικα έξυπνης σύμβασης και σε έξυπνο νομικό συμβόλαιο. Ως κώδικας έξυπνου συμβολαίου νοείται "κώδικας που αποθηκεύεται, επαληθεύεται και εκτελείται σε μια αλυσίδα μπλοκ (blockchain)". Η ικανότητα αυτού του έξυπνου συμβολαίου εξαρτάται εξ ολοκλήρου από τη γλώσσα προγραμματισμού που χρησιμοποιείται για να εκφράσει τη σύμβαση και τα χαρακτηριστικά της αλυσίδας μπλοκ. Έξυπνο νομικό συμβόλαιο σημαίνει κώδικας για να να συμπληρώνει ή να υποκαθιστά νομικές συμβάσεις. Η ικανότητα αυτής της έξυπνης σύμβασης δεν εξαρτάται από την τεχνολογία, αλλά αντίθετα από τους νομικούς, πολιτικούς και επιχειρηματικούς θεσμούς. Το επίκεντρο της παρούσας μελέτης θα επικεντρωθεί στον πρώτο ορισμό, ο οποίος είναι ο κώδικας έξυπνης σύμβασης.



Εικόνα 14: Σύστημα Έξυπνου Συμβολαίου

Ένα έξυπνο συμβόλαιο διαθέτει υπόλοιπο λογαριασμού, ιδιωτικό αποθηκευτικό χώρο και εκτελέσιμο κώδικα. Το συμβόλαιο κατάσταση περιλαμβάνει την αποθήκευση και το υπόλοιπο του συμβολαίου. Η κατάσταση αποθηκεύεται στην αλυσίδα μπλοκ και ενημερώνεται κάθε φορά που γίνεται επίκληση του συμβολαίου. Στην εικόνα 14 απεικονίζεται το σύστημα ενός έξυπνου συμβολαίου.

Κάθε σύμβαση θα εκχωρηθεί σε μια μοναδική διεύθυνση 20 bytes. Μόλις το συμβόλαιο αναπτυχθεί στην αλυσίδα μπλοκ, ο κώδικας της σύμβασης δεν μπορεί να αλλάξει. Για την εκτέλεση ενός συμβολαίου, οι χρήστες μπορούν απλώς να στείλουν μια συναλλαγή στη διεύθυνση του συμβολαίου. Αυτή η συναλλαγή θα εκτελεστεί στη συνέχεια από κάθε κόμβο συναίνεσης, δηλαδή έναν ανθρακωρύχο-χρήστη του συστήματος με σκοπό να επιτευχθεί η συναίνεση στην έξοδο. Η κατάσταση του συμβολαίου στη συνέχεια θα ενημερωθεί αναλόγως. Το συμβόλαιο μπορεί, με βάση τη συναλλαγή που λαμβάνει, να διαβάζει ή να γράφει σε ιδιωτικό αποθηκευτικό χώρο, να αποθηκεύει χρήματα στο υπόλοιπο του λογαριασμού του, να στέλνει και να λαμβάνει μηνύματα ή χρήματα από χρήστες και συμβόλαια ή ακόμη και να δημιουργήσει νέα συμβόλαια. Υπάρχουν δύο τύποι έξυπνων συμβολαίων, τα ντετερμινιστικά και τα μη ντετερμινιστικά έξυπνα συμβόλαια. Ένα ντετερμινιστικό έξυπνο συμβόλαιο είναι ένα έξυπνο συμβόλαιο που όταν εκτελείται, δεν απαιτεί καμία πληροφορία από ένα εξωτερικό μέρος, εκτός της αλυσίδας μπλοκ. Ένα μη ντετερμινιστικό έξυπνο συμβόλαιο είναι ένα συμβόλαιο που εξαρτάται από πληροφορίες, που ονομάζονται oracles ή data feeds, από ένα εξωτερικό μέρος. Για παράδειγμα, ένα συμβόλαιο που απαιτεί τις τρέχουσες πληροφορίες για τον καιρό για να εκτελεστεί είναι ένα μη

ντετερμινιστικό συμβόλαιο, καθώς η πληροφορία που χρειάζεται δεν είναι διαθέσιμη στην αλυσίδα μπλοκ.

3.1.2 Εφαρμογές Έξυπνων Συμβολαίων

Υπάρχουν πολλές και διαφορετικές εφαρμογές που μπορούν να χρησιμοποιηθούν τα έξυπνα συμβόλαια.

- **Διαδίκτυο των πραγμάτων (IoT) και έξυπνη ιδιοκτησία**: υπάρχουν δισεκατομμύρια κόμβοι που μοιράζονται δεδομένα μεταξύ τους μέσω του Διαδικτύου. Μια πιθανή περίπτωση χρήσης της έξυπνης τεχνολογίας που βασίζεται στην αλυσίδα μπλοκ συμβολαίων είναι να επιτραπεί σε αυτούς τους κόμβους να μοιράζονται ή να έχουν πρόσβαση σε διαφορετικές ψηφιακές ιδιότητες χωρίς αξιόπιστο τρίτο μέρος. Υπάρχουν διάφορες εταιρείες που διερευνούν αυτή την περίπτωση χρήσης. Για παράδειγμα, η Slock.it είναι μια γερμανική εταιρεία που χρησιμοποιεί έξυπνες συμβάσεις βασισμένες στο Ethereum για την ενοικίαση, πώληση και κοινή χρήση οποιουδήποτε πράγματος χωρίς την συμμετοχή ενός έμπιστου τρίτου μέρους.
- **Διαχείριση μουσικών δικαιωμάτων**: μια πιθανή περίπτωση χρήσης είναι η καταγραφή των δικαιωμάτων ιδιοκτησίας μιας μουσικής στην αλυσίδα μπλοκ. Ένα έξυπνο συμβόλαιο μπορεί να επιβάλει την πληρωμή των ιδιοκτητών μουσικής μόλις μια μουσική χρησιμοποιηθεί για εμπορικούς σκοπούς. Εξασφαλίζει επίσης ότι η πληρωμή διανέμεται μεταξύ των ιδιοκτητών της μουσικής. Η Ujo είναι μια εταιρεία που διερευνά τη χρήση έξυπνων συμβολαίων βασισμένων στην αλυσίδα μπλοκ στη μουσική βιομηχανία.
- **Ηλεκτρονικό εμπόριο**: μια πιθανή περίπτωση χρήσης είναι η διευκόλυνση των συναλλαγών μεταξύ μη αξιόπιστων μερών (π.χ. πωλητή και αγοραστή) χωρίς αξιόπιστο τρίτο μέρος. Αυτό θα είχε ως αποτέλεσμα τη μείωση του κόστους συναλλαγών. Οι έξυπνες συμβάσεις μπορούν να αποδεσμεύσουν την πληρωμή στον πωλητή μόνο όταν ο αγοραστής είναι ικανοποιημένος με το προϊόν ή την υπηρεσία που έλαβε.

Υπάρχουν και άλλες πιθανές εφαρμογές όπου ταιριάζει η χρήση των έξυπνων συμβολαίων, όπως η ηλεκτρονική ψηφοφορία, η πληρωμή υποθηκών, η διαχείριση ψηφιακών δικαιωμάτων, η ασφάλιση αυτοκινήτων, η κατανεμημένη αποθήκευση αρχείων, η διαχείριση ταυτότητας και η εφοδιαστική αλυσίδα.

3.2 Σύνδεση των δικτύων Blockchain με το IoT (Internet of Things)

Οι αισθητήρες που συνδέονται στο δίκτυο και οι συσκευές IoT είναι η προϋπόθεση για τη σύνδεση του ψηφιακού δίδυμου με τη φυσική του προέλευση. Μεταφέρουν τη στατική αναπαράσταση σε ένα δυναμικό αντίγραφο. Οι αισθητήρες παρέχουν πληροφορίες σχετικά με το περιβάλλον στο οποίο βρίσκονται ή το αντικείμενο στο οποίο είναι προσαρτημένοι. Η τεχνολογία blockchain εισάγει την εμπιστοσύνη, την αυτοματοποίηση και την υπευθυνότητα σε αυτό το σύστημα. Για να καταδειχθεί η σημασία του Blockchain για το IoT, παρακάτω παρουσιάζονται πέντε τομείς περιπτώσεων χρήσης.

3.2.1 Διαχείριση Εφοδιαστικής Αλυσίδας (Supply Chain Management)

Η εμπιστοσύνη είναι ένα από τα πιο σημαντικά χαρακτηριστικά στη διαχείριση της αλυσίδας εφοδιασμού. Όταν πρόκειται για την παρακολούθηση των εμπορευμάτων, την παρακολούθηση των συνθηκών και την εγγύηση της προέλευσης, οι συσκευές IoT σε συνδυασμό με μια αλυσίδα μπλοκ έχουν μεγάλα πλεονεκτήματα. Για παράδειγμα, τα ευπαθή προϊόντα σε ψυγείο μπορούν να εντοπιστούν από αισθητήρες IoT και να τεκμηριωθούν στην αλυσίδα μπλοκ. Αυτό βοηθά στο να εντοπίζονται μεγαλύτερες διαδρομές μεταφοράς. Επίσης, η προέλευση των εμπορευμάτων μπορεί να καταγραφεί και να εντοπιστεί μπρος και πίσω από το τελικό προϊόν. Νεοσύστατες επιχειρήσεις όπως η Modum4, η ZetoChain5 ή η VeChain6 επικεντρώνονται σε αυτές τις επιχειρηματικές δραστηριότητες. Τα tokens των δικτύων αυτών μπορούν να χρησιμοποιηθούν για πληρωμή ή ως αναπαράσταση ενός φυσικού αγαθού. Σπάνια ακόμα χρησιμοποιούνται και ως αναπαράσταση άυλων αξιών όπως τα δικαιώματα. Στην αλυσίδα εφοδιασμού διαχείρισης κάθε σημείο μεταφοράς παρακολουθεί την κατάσταση των συσκευών IoT και αποθηκεύει τα δεδομένα στην αλυσίδα μπλοκ, με αποτέλεσμα να οικοδομείται εμπιστοσύνη.

3.2.2 Οικονομία Διαμοιρασμού (Sharing)

Όπως οι συμμετέχοντες σε μια αλυσίδα εφοδιασμού, έτσι και οι συμμετέχοντες στην οικονομία διαμοιρασμού βασίζονται στη φήμη και την εμπιστοσύνη. Κανείς δεν δίνει την περιουσία του σε έναν ξένο χωρίς καμία εμπιστοσύνη. Εμπιστοσύνη μπορεί να αντιπροσωπεύεται είτε από μια κατάθεση είτε από μια καλή φήμη. Και τα δύο μπορούν να επιτευχθούν με τη χρήση μιας αλυσίδας μπλοκ. Ένα παράδειγμα θα μπορούσε να είναι ένα γενικό σύστημα ενοικίασης. Αντικείμενα ή δωμάτια σε φυσικό κόσμο μπορούν να ενοικιάζονται μέσω έξυπνων συμβολαίων, έτσι ώστε η εγγραφή του αντικειμένων, η απελευθέρωση για τον ενοικιαστή, ο διακανονισμός της μίσθωσης και η επιστροφή

του αντικειμένου μπορεί να διεκπεραιώνεται μέσω της αλυσίδας μπλοκ. Η εφαρμογή Lokkit7 που βραβεύτηκε με το Siemens Excellence Award είναι ένα παράδειγμα. Πολλαπλές θυρίδες ενός κιβωτίου κλειδώματος συστήματος ελέγχονται από έξυπνα συμβόλαια. Οι συσκευές IoT χρησιμοποιούνται για την ανίχνευση της κατάστασης και για την το άνοιγμα και το κλείσιμο των θυρίδων. Το συμβόλαιο ενοικίασης περιλαμβάνει άμεση πρόσβαση στο χρησιμοποιούμενο Token ή κρυπτονόμισμα για την πληρωμή της μίσθωσης και της εγγύησης. Δεδομένου ότι το η υπολογιστική ισχύς και η αποθήκευση στην αλυσίδα μπλοκ είναι δαπανηρή το πρωτόκολλο Whisper χρησιμοποιήθηκε για τον μηχανισμό ανοίγματος μετά τη σύναψη της σύμβασης ενοικίασης. Αυτό το τύπος εφαρμογής αποκλείει τα έμπιστα τρίτα μέρη και δημιουργεί ένα βασισμένο στην εμπιστοσύνη Peer-to-Peer σύστημα. Η προσέγγιση αυτή ανοίγει νέους τομείς εφαρμογής για την οικονομία του διαμοιρασμού (αμοιβαία κοινή χρήση εργαλείων και αγαθών) ή αλλάζει ριζικά τα υφιστάμενα επιχειρηματικά μοντέλα (AirBnB, Uber, κ.λπ.). Και πάλι, τα tokens παίζουν θεμελιώδη ρόλο για την ανταλλαγή αξίας και την αναπαράσταση των δικαιωμάτων στον φυσικό κόσμο. Ιδιαίτερη προσοχή πρέπει να δοθεί στο πρωτόκολλο ανταλλαγής. Δεδομένου ότι οι αλλαγές στην κατάσταση του έξυπνου συμβολαίου προκαλούνται αυτόματα από εξωτερικά γεγονότα, πρέπει να αμφισβητηθεί το κίνητρο των χρηστών ή των συσκευών για την αποστολή αυτών των γεγονότων. Τα περισσότερα πρωτόκολλα λειτουργούν με καταθέσεις ή θεματοφύλακες για να μειωθεί ο κίνδυνος για αδιέξοδα. Εταιρείες όπως η Slock.it8, η HireGo9 ή η MixRent10 επικεντρώνονται σε αυτή την περίπτωση χρήσης.

3.2.3 Εμπορία Δεδομένων

Ένας άλλος τομέας εφαρμογής είναι η εμπορία και η νομισματοποίηση των δεδομένων. Δεδομένου ότι τα δεδομένα που συλλέγονται από αισθητήρες IoT αντιπροσωπεύουν μεγάλη αξία, μπορούν να προσφερθούν δημοσίως προς πώληση. Για παράδειγμα, τα μετεωρολογικά δεδομένα μπορούν να προσφέρονται και να πληρώνονται μέσω Tokens όπως το WXB από το Weatherblock11. Η τεχνολογία Blockchain εκπληρώνει δύο καθήκοντα σε αυτή την περίπτωση: Από τη μία αφενός, τη συμβατική διεκπεραίωση μεταξύ του προμηθευτή και του παραλήπτη δεδομένων με τη χρήση Smart Contracts και αφετέρου την πληρωμή με τη χρήση Tokens. Με αυτόν τον τρόπο οι αισθητήρες IoT μπορούν να ενεργούν αυτόνομα και οι συναλλαγές δεν εξαρτώνται από την ανθρώπινη επιρροή. Κατά μία έννοια, ο IoT αισθητήρας μετατρέπεται σε έναν συμμετέχοντα στην αγορά.

3.2.4 Διαχείριση Ταυτότητας και Δικτύου

Η ταυτότητα γίνεται το πιο σημαντικό αγαθό στο μέλλον. Από τη μία πλευρά, η ταυτότητα των προσώπων ή των φυσικών αντικειμένων, αφετέρου η ταυτότητα των συσκευών IoT. Οι αισθητήρες μπορούν να εξασφαλίσουν ταυτότητα χρησιμοποιώντας διάφορες τεχνικές όπως δακτυλικά αποτυπώματα, σαρωτή ίριδας, αναγνώριση προσώπου, υποδομή ιδιωτικού κλειδιού (PKI), ανιχνευτές GPS, ενσωματωμένους αισθητήρες ή δείκτες. Επιπλέον, οι συσκευές ή τα αντικείμενα που εντάσσονται σε ένα δίκτυο πρέπει να ταυτοποιούνται και να δημιουργείται επικοινωνία. Τα μη ανταλλάξιμα tokens μπορούν να βοηθήσουν στην υλοποίηση αυτής της μοναδικότητας. Μια αδιάβλητη σύνδεση μεταξύ αντικειμένου και Token θα βοηθήσει στην οικοδόμηση εμπιστοσύνης και αποτελεί προϋπόθεση για κάθε περαιτέρω περίπτωση χρήσης.

3.2.5 Αυτοματοποίηση

Τέλος, η αυτοματοποίηση των διαδικασιών και των ροών εργασίας δημιουργεί έντονη ζήτηση για αισθητήρες αντικειμένων σε αυτές τις διαδικασίες, καθώς και για την παρακολούθηση και την καταγραφή της προόδου τους. Ο συνδυασμός συσκευών IoT και έξυπνων συμβάσεων σε μια αλυσίδα μπλοκ επιτρέπει πλήρως αυτοματοποιημένη επικοινωνία και σύναψη συμβάσεων μεταξύ μηχανών. Ακόμη και οι πληρωμές μπορούν να πραγματοποιηθούν με χρήση Tokens. Αυτό οδηγεί την αυτοματοποίηση σε ένα νέο επίπεδο, αφού οι απομονωμένες μονάδες παραγωγής γίνονται ξαφνικά ικανές να αλληλεπιδρούν. Οι διασυνδέσεις μπορούν να περιοριστούν στη διαπραγμάτευση έξυπνων συμβάσεων και στην εκτέλεσή τους.

3.3 Ανάλυση Έργου και Πρόταση Αλγορίθμου

3.3.1 Έργο Food Waste

Όπως αναφέραμε και προηγουμένως η συγκεκριμένη διπλωματική εργασία πραγματοποιείται με αφετηρία ένα έργο, το οποίο στοχεύει στην μείωση της σπατάλης τροφίμων αρχικά από επιχειρήσεις, εστιατόρια και άλλες τέτοιου τύπου δομές. Ο περιορισμός αυτός αποτελεί επιτακτική ανάγκη και έχει ως στόχο την ελαχιστοποίηση περιβαλλοντικών και κοινωνικοοικονομικών επιπτώσεων. Το έργο επικεντρώνεται κυρίως στις κοινωνικές επιπτώσεις του ζητήματος της σπατάλης των τροφίμων και στοχεύει στην ανακούφιση των επισιτιστικά ανασφάλιστων συμπολιτών μας μέσω της διάθεσης δωρεάν γευμάτων από τους προερχόμενους ποικίλους χώρους εστίασης. Η τεχνολογία Blockchain θα είναι η σύνδεση μεταξύ των χώρων εστίασης και των εν

λόγω ατόμων με τη χρήση ενός διαδικτυακού μητρώου, μέσω του οποίου θα γνωστοποιείται η ποσότητα και το είδος των προσφερόμενων γευμάτων. Επιπλέον, μέσω της τεχνολογίας Blockchain θα παρέχονται tokens ως επιβράβευση στους συμβαλλόμενους χώρους εστίασης, δημιουργώντας έτσι ένα κίνητρο συνεργασίας. Μέσω της κρυπτογράφησης, που παρέχει μια τεχνολογία Blockchain, εξασφαλίζεται η εμπιστευτικότητα και η ανωνυμία των εμπλεκόμενων σε κάθε συναλλαγή. Όλα τα παραπάνω θα καταστούν εφικτά με την ανάπτυξη μιας πλατφόρμας ή αλλιώς εφαρμογής, λόγω της δημιουργίας ενός δικτύου αξιόπιστης πληροφόρησης.

Οι χώροι εστίασης, με την εγγραφή τους στην πλατφόρμα, θα συνδέονται σε ένα δίκτυο και θα διοχετεύουν δεδομένα εικόνας σε μια υποδομή υπολογιστικού νέφους. Τα δεδομένα αυτά σε συνδυασμό με τα δεδομένα που θα παρέχουν οι χρήστες θα υπόκεινται σε ανάλυση και θα λαμβάνονται αποφάσεις για την δωρεάν διάθεση μερίδων φαγητού. Έτσι λοιπόν, η ενέργεια αυτή θα μεταφράζεται σε tokens για την επιχείρηση εστίασης, η οποία θα μπορεί να τα χρησιμοποιήσει σε διάφορες συναλλαγές με άλλες επιχειρήσεις.

Η πλατφόρμα που πραγματευόμαστε αποτελείται από τρία βασικά υποσυστήματα: το υποσύστημα συλλογής και ανάλυσης δεδομένων, το υποσύστημα ανταμοιβής και το υποσύστημα της εφαρμογής. Το κυριότερο από αυτά τα υποσυστήματα, το οποίο έχει άμεση σχέση με τη συγκεκριμένη διπλωματική εργασία είναι το υποσύστημα ανταμοιβής και θα αναλυθεί παρακάτω.

Το υποσύστημα ανταμοιβής της πλατφόρμας λαμβάνει χώρα χάρης το ψηφιακό νόμισμα επιβράβευσης, το οποίο θα δημιουργηθεί. Στόχος του νομίσματος αυτού θα είναι η νομισματοποίηση των μερίδων φαγητού και η δημιουργία ενός δικτύου Blockchain για την καταγραφή της διάθεσης και απόκτησης μερίδων φαγητού. Οι καταχωρήσεις στο δίκτυο αυτό δεν δύναται να μεταβληθούν, για αυτό κιόλας θεωρείται μια εξαιρετικά ασφαλής επιλογή.

Τα βασικά χαρακτηριστικά του ψηφιακού νομίσματος στο οποίο αναφερόμαστε επιθυμούμε να είναι τα ακόλουθα:

1. Σπανιότητα: Τα ψηφιακά νομίσματα που εκδίδονται έχουν συγκεκριμένο αριθμό και αυτό τα καθιστά ιδιαίτερα σπάνια. Για παράδειγμα, το bitcoin που αποτελεί ένα από τα δημοφιλέστερα ψηφιακά νομίσματα έχει 21 εκατομμύρια μονάδες (ενώ τα αντίστοιχα ψηφιακά νομίσματα, όπως το ευρώ, έχουν 7 τρισεκατομμύρια μονάδες).

2. Διαιρεσιμότητα: Τα ψηφιακά νομίσματα μπορούν να διαιρεθούν σε πολλαπλά δεκαδικά ψηφία, το οποίο σε συνδυασμό με τη σπανιότητα αποτελεί μια αξιοσημείωτη

ιδιότητα, ειδικά στο περιβάλλον της τεχνητής νοημοσύνης, στο οποίο μηχανές εκτελούν συναλλαγές και πληρωμές σε νανο-ποσότητες (machine-to-machine commerce και nano-payments).

3. Αποθηκευσιμότητα: Τα ψηφιακά νομίσματα δίνουν τη δυνατότητα να αποθηκευθούν εύκολα, φθηνά και για μεγάλο χρονικό διάστημα, καθώς είναι ψηφιακά και επομένως δε φθείρονται, όπως τα χαρτονομίσματα, ενώ δεν καταλαμβάνουν καθόλου φυσικό αποθηκευτικό χώρο.

4. Φορητότητα / Μεταφερσιμότητα: Η δυνατότητα μεταφοράς των νομισματικών μονάδων εύκολα και χωρίς περιορισμούς αποτελεί, επίσης, σημαντικό παράγοντα.

5. Επαληθευσιμότητα: Το γεγονός ότι το κρυπτονόμισμα που θα αναπτυχθεί βασίζεται σε τεχνολογία blockchain, το καθιστά απόλυτα επαληθεύσιμο, καθώς όλες οι συναλλαγές που λαμβάνουν χώρα στο blockchain παραμένουν αμετάβλητες και προσβάσιμες.

6. Αποδοχή: Τα κρυπτονομίσματα δεν έχουν καμία εσωτερική αξία αν δεν χρησιμοποιούνται σε συναλλαγές. Στο πλαίσιο του έργου θα δημιουργήσουμε μια πρώτη μάζα χρηστών, οι οποίοι θα αξιοποιούν το νόμισμα.

Ως εκ τούτου, η προτεινόμενη ιδέα δίνει ιδιαίτερη έμφαση στη γεφύρωση της τεχνολογικής προόδου και της εφαρμογής στην αγορά, ενώ παράλληλα προσαρμόζεται στο τρίπτυχο της εξισορρόπησης και μεγιστοποίησης των περιβαλλοντικών, οικονομικών και κοινωνικών αξιών. Το προτεινόμενο επιχειρηματικό μοντέλο σε συνδυασμό με την ανάπτυξη της πλατφόρμας αγοράς blockchain θα εξυπηρετήσει ενεργά αυτόν τον σκοπό, διεγείροντας τις διατομεακές συνδέσεις, επιτρέποντας τη συμβατότητα της ροής υλικών και οδηγώντας στη διαμόρφωση βιομηχανικών συνεργειών. Στην ουσία, η προτεινόμενη αγορά θα χρησιμοποιεί την τεχνολογία Blockchain για την ψηφιοποίηση του εμπορίου αποβλήτων/παραπροϊόντων, επιτρέποντας σε πολλαπλούς συμμετέχοντες να συνεργάζονται και να πραγματοποιούν συναλλαγές χρησιμοποιώντας κοινές απόψεις της βάσης γνώσεων του συστήματος. Τέλος, επιτρέπει στους συμμετέχοντες την επιλογή προμηθευτών και προϊόντων (είδος και ποσότητα αποβλήτων ή παραπροϊόντων) και τρέχουσων πληροφοριών συναλλαγής, συμπεριλαμβανομένων των λεπτομερειών αποστολής και των αναμενόμενων ημερομηνιών παράδοσης.

3.3.2 Πρόταση Αλγορίθμου για την Εφαρμογή

Στο συγκεκριμένο κεφάλαιο θα προκρίνουμε έναν αλγόριθμο συναίνεσης από αυτούς που αναλύσαμε σε προηγούμενη ενότητα. Θα λάβουμε υπόψιν, αφενός τα θετικά και τα αρνητικά όλων των αλγορίθμων συναίνεσης που αναλύσαμε και αφετέρου τις ανάγκες που προκύπτουν από το ζητούμενο έργο και τους εμπλεκόμενους του.

Όπως είναι γνωστό, ο πιο διαδεδομένος αλγόριθμος συναίνεσης είναι ο αλγόριθμος Proof-of-Work, ο οποίος όμως είναι ιδιαίτερα κοστοβόρος, για αυτό κιόλας δεν θα επιλεγεί για το συγκεκριμένο έργο, διότι πέρα από τις περιβαλλοντικές του συνέπειες απαιτεί και τεχνολογικό εξοπλισμό που δεν είναι εφικτό να διαθέτουν όλοι οι εμπλεκόμενοι. Ο προαναφερθέντας αλγόριθμος μνημονεύτηκε καθώς το 64% των κρυπτονομισμάτων που υπάρχουν λειτουργούν με αλγόριθμο συναίνεσης που έχει ως βάση το Proof-of-Work. Στη συνέχεια, πολλοί αλγόριθμοι απορρίπτονται καθώς είτε έχουν ζητήματα επεκτασιμότητας και ασφάλειας, τα οποία καθιστούν τους αλγορίθμους ακατάλληλους για το εγχείρημα μας, είτε δεν είναι τόσο διαδεδομένοι με αποτέλεσμα να μην έχουν δοκιμαστεί σε εφαρμογές ή να έχουν δοκιμαστεί και να έχουν αποτύχει, λόγω αδυναμίας να δώσουν κίνητρα στους χρήστες τους να τους χρησιμοποιούν.

Ο αλγόριθμος που η διπλωματική προκρίνει έναντι των υπολοίπων είναι ο **Proof-of-Stake**. Σύμφωνα με την έρευνα που πραγματοποιήθηκε και τις προβλέψεις των επιστημόνων για τα επόμενα χρόνια φαίνεται πως ο παραπάνω αλγόριθμος θα αποτελέσει το κέντρο του ενδιαφέροντος όσον αφορά τους αλγορίθμους συναίνεσης.

Πιο συγκεκριμένα, η διπλωματική εργασία προτείνει τον παραπάνω αλγόριθμο για να χρησιμοποιηθεί ως βάση με σκοπό να φτιαχτεί και να προταθεί ένας αλγόριθμος λίγο αλλαγμένος, άλλα με τα θεμελιώδη χαρακτηριστικά του **PoS.** Αρχικά, η πιθανότητα εξόρυξης του επόμενου block για μια επιχείρηση εστίασης δεν θα είναι ανάλογη ούτε της υπολογιστικής της δύναμης, αλλά ούτε και των χρημάτων της. Η παραπάνω πιθανότητα θα είναι ανάλογη των μερίδων δωρεάν φαγητού που θα προσφέρει η εν λόγω επιχείρηση. Με αυτόν τον τρόπο οι επιχειρήσεις που δίνουν τα περισσότερα γεύματα θα έχουν και τις περισσότερες πιθανότητες να εξορύξουν το επόμενο block, συνεπώς δεν θα υπάρχει προβάδισμα ούτε για τις πιο εύπορες επιχειρήσεις, ούτε για τις πιο τεχνολογικά προηγμένες.

Στη συνέχεια, ο προτεινόμενος αλγόριθμος θα έχει ορισμένους χρήστες/επιχειρήσεις, οι οποίοι θα επιβεβαιώνουν μια συναλλαγή στο οικοσύστημα του αλγορίθμου. Κάθε συναλλαγή που πραγματοποιείται στο δίκτυο θα επικυρώνεται και θα εισέρχεται στην αλυσίδα των μπλοκ αμέσως μετά την προσφορά του γεύματος ή του προϊόντος. Οι

χρήστες που θα επικυρώνουν μια συναλλαγή ή ένα μπλοκ θα είναι μέλη του δικτύου Blockchain με υψηλή αξιοπιστία. Για παράδειγμα, θα μπορούσε την αξιοπιστία των χρηστών αυτών να την ορίζει ο συνδυασμός ορισμένων παραγόντων, όπως το σύνολο των tokens που έχουν διαχειριστεί και ο αριθμός των συμβολαίων που έχουν πιστοποιήσει ως έγκυρα. Ακόμη, θα ήταν επιτακτική ανάγκη οι παραπάνω παράγοντες να προστατεύουν τον αλγόριθμο από τυχόν μη έγκυρες συναλλαγές, δηλαδή να μην είναι δυνατόν κάποια ομάδα χρηστών να αποκτήσει το 51% του οικοσυστήματος και ταυτόχρονα να έχει υψηλή αξιοπιστία για να επικυρώνουν συναλλαγές.

Επιπλέον, η αγορά θα διαθέτει ένα ιδιωτικό σύστημα πληρωμών και ένα σύστημα εκτέλεσης συναλλαγών, οι οποίες θα εκτελούνται μέσω των έξυπνων συμβάσεων (Smart Contracts) σε πλατφόρμα Blockchain. Οι συμβάσεις που θα εκτελούνται θα είναι πλήρεις, διαφανείς, επαληθεύσιμες και μόνιμα εγγεγραμμένες στο δίκτυο Blockchain. Η δυνατότητα των χρηστών του οικοσυστήματος να προχωρούν στο κλείσιμο ενός προκαθορισμένου διαθέσιμου έξυπνου συμβολαίου είναι ζωτικής σημασίας για την οικονομική βιωσιμότητα του οικοσυστήματος. Το προαναφερθέν συμβαίνει καθώς με αυτό το τρόπο ο σχεδιασμός και η υλοποίηση των συμβάσεων θα μπορεί να επιτευχθεί με ελάχιστο κόστος, αρκετά δε μικρότερο από το κόστος λειτουργίας των παραδοσιακών αγορών. Η αγορά που βασίζεται στο Blockchain θα αποτελέσει το επίκεντρο του προτεινόμενου επιχειρηματικού μοντέλου, το οποίο θα εκμεταλλευτεί το πλεονέκτημα της λειτουργικότητάς του, προκειμένου να διασφαλίσει την άψογη και απρόσκοπτη λειτουργία του, δημιουργώντας παράλληλα ένα αξιόπιστο περιβάλλον συνεργασίας για όλους τους συμμετέχοντες του οικοσυστήματος.

Συνοψίζοντας τα παραπάνω, καταλήγουμε σε έναν «πειραγμένο» αλγόριθμο συναίνεσης Proof-of-Stake με τα χαρακτηριστικά και τις λειτουργίες που αναλύσαμε, αντιμετωπίζοντας τις αδυναμίες του κλασσικού αλγορίθμου Proof-of-Stake και προσαρμόζοντας τον αλγόριθμο στις συνθήκες και ιδιαιτερότητες του έργου.

Βιβλιογραφία

Aponte-Novoa, F., Orozco, A., Villanueva-Polanco, R. and Wightman, P., 2021. The 51% Attack on Blockchains: A Mining Behavior Study. IEEE Access, 9, pp.140549-140564.

Bamakan, S., Motavali, A. and Babaei Bondarti, A., 2020. A survey of blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications, 154(1), pp.113-115.

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N. and Alazab, M., 2020. Blockchain for Industry 4.0: A Comprehensive Review. IEEE Access, 8, pp.764-800.

Buterin, V. 2014. A next-generation smart contract and decentralized application platform. White Paper.

Christidis, K., Devetsikiotis, M. 2016. Blockchains and smart contracts for the internet of things. IEEE Access, 4(1), pp. 2292–2303.

Dib, O., Brousmiche, K., Durand, A., Thea, E., Hamida, B. 2018. Consortium blockchains: Overview, applications and challenges International Journal On Advances in Telecommunications, 11 (1).

Emeç, M., Karatay, M., Dalkılıç, G., Alkım, E. 2020. Consensus Approaches of High-Value Crypto Currencies and Application in SHA-3. In: Hemanth, D., Kose, U. (eds) Artificial Intelligence and Applied Mathematics in Engineering Problems. ICAIAME 2019. Lecture Notes on Data Engineering and Communications Technologies, 43(1). Springer, Cham.

Guo, H. and Yu, X., 2022. A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), p.10-67.

Guo, S., Hu, X., Guo, S., Qiu, X. and Qi, F., 2020. Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. IEEE Transactions on Industrial Informatics, 16(3), pp.1972-1983.

Haber, S. and Stornetta, W., 1991. How to time-stamp a digital document. Journal of Cryptology, 3(2), pp.99-111.

Heo, G., Yang, D., Doh, I. and Chae, K., 2021. Efficient and Secure Blockchain System for Digital Content Trading. IEEE Access, 9, pp.438-450.

Kim, J., 2020. Blockchain Technology and Its Applications: Case Studies. Journal of System and Management Sciences.

Korpela, K., Hallikas, J., Dahlberg, T. 2017. Digital supply chain transformation toward blockchain integration. Paper presented at the proceedings of the 50th Hawaii international conference on system sciences.

Liu, M., Yu, F., Teng, V. 2018. Computation offloading and content caching in wireless blockchain networks with mobile edge computing, IEEE Trans. Veh. Technol., 67(11), pp. 11008-11021.

Liu, H., Crespo, R. and Martínez, O., 2020. Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts. Healthcare, 8(3), p.243.

Nakamoto, N., 2017. Centralised Bitcoin: A Secure and High Performance Electronic Cash System. SSRN Electronic Journal.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: 2016. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, Princeton.

Ray, P., Dash, D., Salah, K. and Kumar, N., 2021. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. IEEE Systems Journal, 15(1), pp.85-94.

Sigaki, H., Perc, M., Ribeiro, H. 2019. Clustering patterns in efficiency and the coming-of-age of the cryptocurrency market. Sci. Rep., 9(1), pp. 1–9.

Solanki, M., 2021. Overview of Blockchain Technology: Consensus, Architecture, and Its Future Trends. International Journal of Innovative Research in Computer Science & Technology, pp.47-51.

Tang, S., Wang, Z., Jiang, J., Ge, S. and Tan, G., 2022. Improved PBFT algorithm for high-frequency trading scenarios of alliance blockchain. Scientific Reports, 12(1).

Tselios, C., Politis, I., Kotsopoulos, A. 2017. Enhancing SDN security for IoT-related deployments through blockchain, Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN), pp. 303-308.

Yuan, Y. and Wang, F., 2018. Blockchain and Cryptocurrencies: Model, Techniques, and Applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48(9), pp.1421-1428.

Vukolić, M. 2015. The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: International Workshop on Open Problems in Network Security, pp. 112–125. Springer, Cham.

Zanelatto Gavião Mascarenhas, J., Ziviani, A., Wehmuth, K. and Vieira, A., 2020. On the transaction dynamics of the Ethereum-based cryptocurrency. Journal of Complex Networks, 8(4).

Zhu, Y., Zheng, G., Wong, K. 2019. Blockchain-empowered decentralized storage in air-to-ground industrial networks, IEEE Trans. Ind. Inform., 15(6), pp. 3593-3601.

Zhong, B., Guo, J., Zhang, L., Wu, H., Li, H. and Wang, Y., 2022. A blockchain-based framework for on-site construction environmental monitoring: Proof of concept. Building and Environment, 217, p.109.

Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. arXiv preprint arXiv:1710.06372.

Ανακτήθηκε από https://getbtcz.com/

Ανακτήθηκε από https://www.coindesk.com/

Ανακτήθηκε από https://www.investopedia.com/

Ανακτήθηκε από https://www.algorand.com/

Ανακτήθηκε από https://www.educative.io/

Ανακτήθηκε από https://academy.binance.com/

Ανακτήθηκε από https://www.geeksforgeeks.org/

Ανακτήθηκε από https://www.newsbtc.com/proof-of-existence/

Ανακτήθηκε από https://apla.readthedocs.io/

Ανακτήθηκε από https://digiforest.io/

Ανακτήθηκε από https://en.cryptonomist.ch/

Ανακτήθηκε από https://golden.com/

Ανακτήθηκε από https://www.moneyland.ch/

Ανακτήθηκε από https://www.golden.com/

Ανακτήθηκε από https://tokens-economy.gitbook.io/

Ανακτήθηκε από https://www.techtarget.com/

Ανακτήθηκε από https://originstamp.com/

Ανακτήθηκε από https://www.forbes.com/advisor/

Ανακτήθηκε από https://www.eublockchainforum.eu/