ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σύγκριση σύγχρονων μηχανισμών συναίνεσης blockchain και μοντέλα εμπιστοσύνης και κύρους

Κούκιος Πανόπουλος Σωτήριος

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ
Βαρβαρίγου Θεοδώρα

Αθήνα, Ιούνιος 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σύγκριση σύγχρονων μηχανισμών συναίνεσης blockchain και μοντέλα εμπιστοσύνης και κύρους

Κούκιος Πανόπουλος Σωτήριος

Επιβλέπουσα: Βαρβαρίγου Θεοδώρα
Καθηγήτρια Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 20/06/2023

(Υπογραφή)	(Υπογραφή)	(Υπογραφή)
.....	.....	.....
Βαρβαρίγου Θεοδώρα	Βαρβαρίγος Εμμανουήλ	Δουλάμης Αναστάσιος
Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αναπλ. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2023

(Υπογραφή)

.....

Κούκιος Πανόπουλος Σωτήριος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Σε σύγχρονες serverless αρχιτεκτονικές blockchain δημιουργείται η ανάγκη για υιοθέτηση καινοτόμων μηχανισμών συναίνεσης μεταξύ των συμμετεχόντων. Κύριος λόγος αποτελεί η τρομακτικά ακριβή κατανάλωση πόρων που απαιτείται για τη διατήρηση αμετάβλητων δεδομένων σε τέτοια συστήματα (Immutability). Πιο συγκεκριμένα, νέοι μηχανισμοί βασιζόμενοι σε μοντέλα εμπιστοσύνης και κύρους αποσκοπούν να επιτύχουν την αμεταβλητότητα των δεδομένων προσδίδοντας στο serverless σύστημα την ασφάλεια και την χρηστικότητα που το καθιστά υιοθετήσιμο.

Στην παρούσα εργασία γίνεται ανάλυση της σημασίας και της επίδρασης των υπαρχόντων μηχανισμών συναίνεσης, και ουσιαστική σύγκριση των πιο ακμαίων μεθόδων που βασίζονται σε μοντέλα εμπιστοσύνης και κύρους.

Λέξεις κλειδιά

Blockchain, μέθοδοι συναίνεσης, μοντέλα εμπιστοσύνης, κύρος, Proof of Reputation, Proof of Trust

Abstract

In modern blockchain architectures the need arises to adopt innovative consensus mechanisms among participants. The main reason is the frighteningly expensive resource consumption required to maintain immutable data in such systems. More specifically, new mechanisms based on trust and reputation models aim to achieve data immutability by giving the blockchain the security and usability that makes it adoptable.

In this paper we analyze the importance and impact of existing consensus mechanisms, and perform a substantial comparison of the most popular ones.

Keywords

Blockchain, consensus mechanism, reputation models, trust, Proof of Reputation, Proof of Trust

Ευχαριστίες

Σε αυτό το σημείο, θα ήθελα να εκφράσω τις θερμές ευχαριστίες μου σε όλους όσους συνέβαλαν στην επιτυχή εκπόνηση της παρούσας διπλωματικής εργασίας. Πρώτα από όλα, θα ήθελα να ευχαριστήσω την επιβλέπουσα Καθηγήτρια Θεοδώρα Βαρβαρίγου και τον ερευνητή κ. Αντώνη Λίτκε, για το ενδιαφέρον και τη συνεχή και πολύτιμη υποστήριξη και καθοδήγησή τους στην προσπάθεια αυτή, όποτε και αν την χρειάστηκα.

Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου και όλα τα κοντινά μου πρόσωπα για την πολύτιμη υπομονή και ενθάρρυνσή τους καθ’ όλη τη διάρκεια αυτής της διαδρομής μου.

Περιεχόμενα

Κεφάλαιο 1. Εισαγωγή

1.1. Αντικείμενο – Σκοπός

Αντικείμενο της διπλωματικής εργασίας αυτής είναι η επισκόπηση της τεχνολογίας blockchain και των μηχανισμών συναίνεσης που εφαρμόζονται σε διαφορετικές αρχιτεκτονικές. Η τεχνολογία blockchain αποτελεί μια από τις πιο επαναστατικές τεχνολογίες των τελευταίων ετών, με σημαντικό σημείο στην ιστορία να είναι το 2008 με την εισαγωγή του Bitcoin, μέσα από τη δημοσίευση του Satoshi Nakamoto [1]. Αποτελεί ακόμα και σήμερα μυστήριο η πραγματική ιδιότητα του ατόμου αυτού, ή αν είναι και ένα άτομο ή ομάδα ατόμων. Η τεχνολογία blockchain αναμένεται να επιφέρει επανάσταση στον τρόπο με τον οποίο πραγματοποιούνται οι συναλλαγές, και ως επακόλουθο να επηρεάσει μια μεγάλη ποικιλία από πιθανά πεδία εφαρμογής.

Η δομή της τεχνολογίας blockchain βασίζεται σε ένα δίκτυο ομότιμων χρηστών (peer to peer network) και μπορούμε να το σκεφτούμε ως μια πλήρως αποκεντρωμένη βάση δεδομένων, όπου οι συμμετέχοντες κρατούν ένα αντίγραφο από όλες τις συναλλαγές εντός του δικτύου [2]. Για να επιτευχθεί μια συνέπεια μεταξύ των κόμβων, εφαρμόζεται ένα κατανεμημένο πρωτόκολλο συναίνεσης σε κάθε κόμβο, το οποίο διαχειρίζεται τα μηνύματα που ανταλλάσσονται και τις αποφάσεις που παίρνει ο κάθε κόμβος ανεξάρτητα [3]. Οι μηχανισμοί αυτοί και τα πρωτόκολλα συναίνεσης είναι ένα σύνολο από κανόνες που χρησιμοποιούν οι κόμβοι του δικτύου για να αποφασίσουν σχετικά με την εγκυρότητα των συναλλαγών [4], και αυτό διαβεβαιώνει ότι όλοι οι συμμετέχοντες συλλογικά θα διατηρούν ένα κοινό καθολικό συναλλαγών (transaction ledger). Το πιο διαδεδομένο σύστημα συναίνεσης αποτελεί το Proof of Work (PoW), το οποίο χρησιμοποιείται στο δίκτυο του Bitcoin [5], αλλά χρησιμοποιήθηκε αρχικά σε τεχνολογία κρυπτονομισμάτων με την εισαγωγή του HashCash [6]. Εξαιτίας της υψηλής ενεργειακής κατανάλωσης αλλά και της χαμηλής αποδοτικότητας του Proof of Work, εμφανίστηκαν εναλλακτικοί μηχανισμοί συναίνεσης, οι οποίοι είχαν ως στόχο να βελτιώσουν κάποια από τα αρνητικά χαρακτηριστικά του PoW, το καθένα με διαφορετικό τρόπο και κύριο χαρακτηριστικό.

Ορισμένοι μηχανισμοί έχουν ως κύριο χαρακτηριστικό την επίτευξη της συναίνεσης με κριτήρια την εμπιστοσύνη και το κύρος, κριτήριο το οποίο συχνά χρησιμοποιούμε και στις πραγματικές συναλλαγές μας. Ως περαιτέρω στόχο λοιπόν της παρούσας εργασίας έχουμε την επισκόπηση με μεγαλύτερη λεπτομέρεια των μεθόδων αυτών συναίνεσης που βασίζονται σε μοντέλα εμπιστοσύνης και κύρους.

1.2. Εμπιστοσύνη και Κύρος

Αν και εκδηλώσεις εμπιστοσύνης είναι εύκολο να τις αναγνωρίσουμε καθώς τις βιώνουμε και βασιζόμαστε σε αυτές καθημερινά, η εμπιστοσύνη είναι μια πολύπλευρη έννοια, και ο ακριβής ορισμός της μπορεί να είναι απαιτητικός. Συμπεριλαμβάνει έννοιες ηθικής, αξιών, συναισθημάτων, και συνδυάζει μια ποικιλία από πεδία. Επίσης, η εμπιστοσύνη πάντα εξαρτάται και από την κατάσταση στην οποία βρισκόμαστε. Για παράδειγμα, μπορούμε να εμπιστευτούμε έναν πωλητή σε ένα ηλεκτρονικό κατάστημα για να μας πουλήσει ένα προϊόν, αλλά δεν μπορούμε να τον εμπιστευτούμε για να εκτελέσει μια ιατρική εξέταση.

Σύμφωνα με τον Luhmann [7], η εμπιστοσύνη είναι ένας αποτελεσματικός μηχανισμός για να μειώσουμε την πολυπλοκότητα και το ρίσκο. Παρουσιάζει την εμπιστοσύνη ως ένα συνεχή βρόχο ανάδρασης, με τα σήματα εισόδου στο σύστημα αυτό να αποτυπώνουν αν αυτή η εμπιστοσύνη είναι δικαιολογημένη ή όχι. Αντίστοιχα ο Gambetta [8] ορίζει την εμπιστοσύνη ως την υποκειμενική πιθανότητα κατά την οποία ένα άτομο A αναμένει πως ένα διαφορετικό άτομο B θα εκτελέσει μια ενέργεια που θα επηρεάσει τον ίδιο. Όταν λέμε ότι εμπιστευόμαστε κάποιον, εννοούμε ότι η πιθανότητα να εκτελέσει μια ενέργεια που είναι ευεργετική για εμάς, ή τουλάχιστον όχι επιβλαβής, είναι αρκετά υψηλή ώστε να αποφασίσουμε να συνεργαστούμε με αυτό το άτομο.

Έχει επισημανθεί στο [9] πως η εμπιστοσύνη παίζει σημαντικό ρόλο όταν ένας χρήστης αποτιμά την εγκυρότητα του πληροφοριακού περιεχομένου που βρίσκει στο διαδίκτυο ή όταν επιλέγει ένα κατάστημα για να αγοράσει ένα προϊόν. Οι χρήστες δεν θα πιστέψουν ή δεν θα αποφασίσουν να προχωρήσουν τη συναλλαγή με ένα άτομο που δεν εμπιστεύονται. Έτσι, η εμπιστοσύνη ορίζεται ως η αντίληψη του βαθμού κατά τον οποίο ένα άτομο θα ολοκληρώσει τις συναλλακτικές του υποχρεώσεις σε περιπτώσεις που διέπονται από ρίσκο και αβεβαιότητα. Αναφέρονται επτά διαστάσεις εμπιστοσύνης σε ψηφιακά περιβάλλοντα: έλξη (attraction), δυναμισμός (dynamism), εξειδίκευση (expertness), πίστη (faith), προθέσεις (intentions), εντοπιότητα (localness) και αξιοπιστία (reliability).

Γενικά, η εμπιστοσύνη απαιτεί την προθυμία από ένα δράστη (actor), να μπει σε μια θέση πολυπλοκότητας και αβεβαιότητας και κατά συνέπεια να γίνει ευάλωτος μέσα στη σχέση μεταξύ αυτού και ενός διαφορετικού δράστη, τον οποίο πρέπει να εμπιστευτεί. Έτσι, έχουμε δύο διαφορετικά προαπαιτούμενα για να προκύψει εμπιστοσύνη: ρίσκο και αλληλεξάρτηση. Χωρίς αυτές τις δύο συνθήκες, δεν υπάρχει ανάγκη για εμπιστοσύνη [10].

Επομένως, η εμπιστοσύνη μπορεί να παρουσιαστεί σαν μια λογική μορφή συνεργασίας κάτω από κίνδυνο συμπεριφοράς, ζυγίζοντας τα πιθανά κόστη και οφέλη, και είναι σχετική με την αξιολόγηση και τη διαχείριση των κινδύνων που αντιλαμβάνεται κάθε φορέας που συνάπτει μια σχέση.

Σαν επέκταση, η φήμη ή το κύρος είναι μια σφαιρική αντίληψη της συμπεριφοράς ενός φορέα, που βασίζεται στην εμπιστοσύνη που έχουν εδραιώσει άλλοι φορείς προς αυτόν [11].

1.3. Οργάνωση Εργασίας

Η παρούσα εργασία έχει αναπτυχθεί σε 6 συνολικά κεφάλαια. Η διάρθρωσή της είναι η εξής:

- Κεφάλαιο 1
  Καθορίζεται το αντικείμενο και ο σκοπός της διπλωματικής εργασίας, και γίνεται μια εισαγωγή στην έννοια της εμπιστοσύνης και του κύρους
- Κεφάλαιο 2
  Παρουσιάζεται με λεπτομέρεια η τεχνολογία Blockchain. Τα γενικά χαρακτηριστικά της, η αρχιτεκτονική και τα βασικά δομικά στοιχεία (blocks, consensus, είδη δικτύων)
- Κεφάλαιο 3
  Εξηγείται η χρήση των μηχανισμών συναίνεσης και παρουσιάζονται ορισμένοι βασικοί μηχανισμοί, οι οποίοι δεν χρησιμοποιούν μοντέλα ή έννοιες εμπιστοσύνης και κύρους.
- Κεφάλαιο 4
  Αναλύονται οι μηχανισμοί συναίνεσης που βασίζονται σε μοντέλα εμπιστοσύνης και κύρους, και παρουσιάζονται οι κυριότεροι των τελευταίων ετών
- Κεφάλαιο 5
  Σύγκριση και αξιολόγηση των μηχανισμών συναίνεσης που αναφέρθηκαν στο κεφάλαιο 4
- Κεφάλαιο 6
  Συμπεράσματα & Μελλοντική Εργασία
- Κεφάλαιο 7
  Βιβλιογραφία & Αναφορές

Κεφάλαιο 2. Θεωρητικό Υπόβαθρο – Τεχνολογία Blockchain

2.1. Ορισμός και Ιστορική Αναδρομή

Το Blockchain, όπως αναφέραμε και στην εισαγωγή, είναι ένα ανοιχτό κατανεμημένο ημερολόγιο στο οποίο καταγράφονται με αποτελεσματικό και έγκυρο τρόπο συναλλαγές μεταξύ των μερών που συμμετέχουν. Οι συναλλαγές αυτές οργανώνονται σε μια αλυσίδα από μπλοκ (blocks). Η αλυσίδα αυτή αναπτύσσεται και μεγαλώνει συνεχώς όσο πραγματοποιούνται νέες συναλλαγές και προστίθενται μπλοκ σε αυτή. Το blockchain μπορεί να θεωρηθεί ως μια κατανεμημένη βάση δεδομένων όπου καταγράφονται συναλλαγές. Κάθε συναλλαγή επικυρώνεται με τη συναίνεση της πλειοψηφίας των φορέων που συμμετέχουν στην αλυσίδα, και από τη στιγμή που εισέρχεται στην αλυσίδα, δεν μπορεί να επεξεργαστεί ή να διαγραφεί. Η χρήση τεχνολογιών όπως η κρυπτογραφία, οι ψηφιακές υπογραφές και ο κατανεμημένος μηχανισμός συναίνεσης καθιστά το περιβάλλον στο οποίο στηρίζεται η τεχνολογία Blockchain ένα αποκεντρωμένο περιβάλλον. Έτσι, περιορίζεται σε μεγάλο βαθμό το κόστος και βελτιώνεται η αποδοτικότητα του συστήματος συναλλαγών [12].

Όπως επίσης αναφέραμε στην εισαγωγή, η πρώτη εμφάνιση της τεχνολογίας Blockchain σαν έννοια ήταν με την εισαγωγή του Bitcoin το 2008, όταν ένα άτομο (ή μια ομάδα ατόμων) δημοσίευσαν το “Bitcoin: A Peer-To-Peer Electronic Cash System” [1] υπό το όνομα Satoshi Nakamoto. Κατά τη συγγραφή της παρούσας εργασίας, η ταυτότητα πίσω από το όνομα Satoshi Nakamoto παραμένει ακόμα άγνωστη [12]. Στην δημοσίευση αυτή περιγράφονται οι τεχνολογίες που υποστηρίζουν συναλλαγές με ψηφιακό νόμισμα που θα επέτρεπαν διαδικτυακές συναλλαγές να ολοκληρωθούν χωρίς κάποιο ενδιάμεσο χρηματοπιστωτικό ίδρυμα. Μερικούς μήνες αργότερα, στις 3 Ιανουαρίου 2009 το Bitcoin μπήκε σε λειτουργία σαν ψηφιακή υπηρεσία [13], και δημιουργήθηκε το Genesis μπλοκ ή Μπλοκ 0, ένα ειδικό μπλοκ που δεν περιέχει αναφορά σε κάποιο προηγούμενο του.

2.2. Bitcoin

Το Bitcoin είναι ένα δίκτυο συναίνεσης που αποτελεί ένα νέο σύστημα πληρωμών. Παρέχει μια πλήρως ψηφιακή μορφή χρημάτων, και είναι το πρώτο αποκεντρωμένο δίκτυο πληρωμών μεταξύ ομότιμων χρηστών (peer-to-peer) που λειτουργεί χωρίς να υπάρχει κάποια κεντρική αρχή ή κάποιος ενδιάμεσος. Από την πλευρά του χρήστη, το Bitcoin μπορεί να θεωρηθεί σαν τα μετρητά χρήματα του Διαδικτύου (electronic cash).

Μια βασική αρχή του δικτύου Bitcoin είναι πως δεν υπάρχει ιδιοκτήτης. Ο έλεγχος του δικτύου ανήκει στους χρήστες του. Για τις ενημερώσεις και βελτιώσεις στο

λογισμικό του δικτύου, δεν μπορεί να πραγματοποιηθεί καμία αλλαγή στο πρωτόκολλο του Bitcoin. Αντ' αυτού, οι χρήστες είναι ελεύθεροι να επιλέξουν την έκδοση του λογισμικού που χρησιμοποιούν, και θα πρέπει να υπακούν τους ίδιους κανόνες, προκειμένου να διατηρείται η συμβατότητα μεταξύ των συναλλαγών και των μπλοκ. Ως επέκταση, το Bitcoin λειτουργεί σωστά μόνο όταν υπάρχει πλήρης συναίνεση και συμφωνία μεταξύ όλων των χρηστών.

Σαν υποδομή, οι χρήστες του δικτύου Bitcoin μοιράζονται ένα δημόσιο ημερολόγιο, το blockchain, που περιλαμβάνει κάθε συναλλαγή που έχει επεξεργαστεί από το δίκτυο. Έτσι, ο κάθε χρήστης του δικτύου μπορεί ανά πάσα στιγμή να εξακριβώσει την εγκυρότητα της κάθε συναλλαγής ανεξάρτητα. Για την προστασία της αυθεντικότητας των συναλλαγών χρησιμοποιείται η τεχνολογία των ψηφιακών υπογραφών, και κάθε μια υπογραφή αντιστοιχεί σε μια διεύθυνση αποστολής. Επίσης, δίνεται η δυνατότητα στον καθένα να επιβεβαιώσει συναλλαγές και να επιχειρήσει να παράξει ένα μπλοκ, με χρήστη της υπολογιστικής ισχύος του, και με ανταμοιβή ένα ποσό σε bitcoin. Η διαδικασία αυτή ονομάζεται εξόρυξη (mining) και αποτελεί τον μηχανισμό συναίνεσης Proof of Work που χρησιμοποιεί το Bitcoin. Ο μηχανισμός αυτός μαζί με άλλους θα αναλυθούν περισσότερο στο Κεφάλαιο 3.

2.3. Η τεχνολογία Blockchain

Ενώ η έννοια του Blockchain εμφανίστηκε πρώτη φορά με εφαρμογή το Bitcoin σαν ψηφιακό νόμισμα, πολλοί θεωρούν πως η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί σε πολύ μεγαλύτερο βαθμό, καθώς μπορεί να εφαρμοστεί σαν ένα δημόσιο ημερολόγιο για κάθε είδους συναλλαγές, εκτός των ψηφιακών νομισμάτων [13] [14]. Για παράδειγμα, στην επιστημονική κοινότητα θεωρείται πως η τεχνολογία Blockchain έχει μεγάλο αντίκτυπο στον ενεργειακό τομέα [15] [16], στις αλυσίδες εφοδιασμού και την εφοδιαστική [17] [18] [19], στην μουσική βιομηχανία [20], στον τομέα υγείας [21], αλλά βρίσκει εφαρμογή και σε άλλους τομείς.

Έχει επίσης αναφερθεί στην βιβλιογραφία [22] ένας διαχωρισμός της τεχνολογίας Blockchain σε γενιές:

- Blockchain 1.0 (ψηφιακό νόμισμα). Περιλαμβάνει κρυπτονομίσματα όπως το Bitcoin, πρωτοεμφανίστηκε το 2009.
- Blockchain 2.0 (ψηφιακή οικονομία). Περιλαμβάνει οικονομικές υπηρεσίες, χρηματοδότηση από το πλήθος (crowdfunding), αγορές προβλέψεων, έξυπνη ιδιοκτησία και έξυπνα συμβόλαια (smart contracts). Εμφανίστηκε με την κυκλοφορία της υπηρεσίας NXT το 2013.

- Blockchain 3.0 (ψηφιακή κοινωνία). Περιλαμβάνει Ψηφιακή Ταυτότητα (Digital Identity), Προστασία Πνευματικής Ιδιοκτησίας (Intellectual Property Protection), υπηρεσίες διακυβέρνησης, και εκλογές. Ξεκινούν να διαμορφώνονται λύσεις μέσα σε αυτά τα πεδία εφαρμογής.

Δεν υπάρχει κάποιος γενικά αποδεκτός ορισμός της έννοιας του blockchain μέχρι στιγμής από ερευνητές και επαγγελματίες, καθώς έχει χρησιμοποιηθεί υπό διαφορετικές οπτικές σε διαφορετικούς τομείς, και έχει προσεγγιστεί από πολλούς διαφορετικούς κλάδους. Ένας πιο τεχνικός ορισμός αναφέρει πως το Blockchain είναι μια κατανεμημένη και αποκεντρωμένη βάση δεδομένων από αμετάβλητες εγγραφές, όπου οι συναλλαγές είναι προστατευμένες από ισχυρούς κρυπτογραφικούς αλγορίθμους και η κατάσταση του δικτύου διατηρείται από τον αλγόριθμο συναίνεσης. Ωστόσο, η πλειοψηφία των ερευνητών τείνει να συμφωνεί στα κοινά στοιχεία πως το Blockchain είναι ένα συνδεδεμένο σύνολο από κατατμημένες (hashed) συναλλαγές, οι οποίες αναπαράγονται στους συμμετέχοντες.

Η αποκεντρωμένη δομή του Blockchain διαθέτει ορισμένα βασικά χαρακτηριστικά, που αντικρούονται με τις παραδοσιακές συγκεντρωτικές προσεγγίσεις, και είναι τα εξής:

- *Διαφάνεια*: οποιοσδήποτε μπορεί ανά πάσα στιγμή να παρακολουθήσει τις συναλλαγές του δικτύου
- *Αμεταβλητότητα*: αφού επιβεβαιωθεί, μια συναλλαγή δεν μπορεί να αντιστραφεί, και κανείς δεν μπορεί να παρέμβει σε μια ολοκληρωμένη μεταφορά
- *Χαμηλό κόστος*: τα τέλη των συναλλαγών είναι ελάχιστα
- *Διασυνοριακή επικοινωνία*: τα χρήματα (ή εν γένει η πληροφορία του δικτύου) μπορεί να μεταφερθεί σε οποιοδήποτε μέρος, είτε είναι η άλλη άκρη του κόσμου ή το ίδιο δωμάτιο
- *Ταχύτητα*: λόγω της επίπεδης και διαφανούς φύσης του Blockchain, οι μεταφορές εμφανίζονται σχεδόν άμεσα και συνήθως επιβεβαιώνονται σε λεπτά, αντί για ώρες ή ημέρες

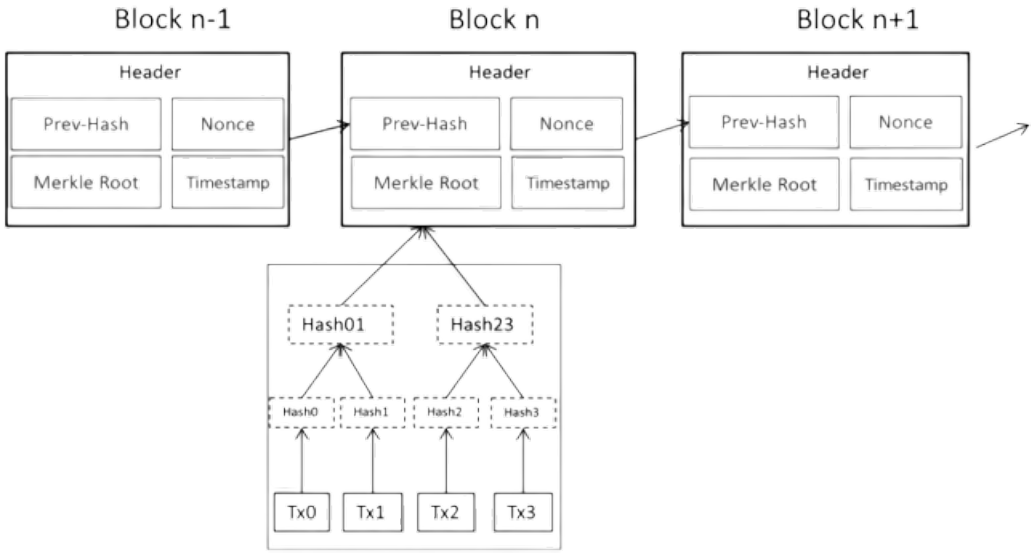
Σε αυτό το σημείο αξίζει να αναφέρουμε πως, παρότι το blockchain είναι δημόσιο και διαφανές, τα στοιχεία των χρηστών του δικτύου παραμένουν ως ένα σημείο ιδιωτικά [23]. Οι συμμετέχοντες στο δίκτυο έχουν στην κατοχή τους δύο κρυπτογραφημένα κλειδιά, ένα ιδιωτικό και ένα δημόσιο, με τα οποία μπορούν να αποδεικνύουν την κυριότητα των συναλλαγών τους. Συγκεκριμένα, το δημόσιο κλειδί ενός χρήστη, συσχετίζεται με το ιδιωτικό κλειδί του, και παράγονται από μια σειρά

πολύπλοκων αριθμητικών διαδικασιών, οι οποίες είναι αδύνατο να αναστραφούν. Για αυτό το λόγο η τεχνολογία blockchain θεωρείται και εμπιστευτική (confidential).

Για να αναλύσουμε τα κύρια δομικά στοιχεία του blockchain, θα δούμε πρώτα τις *συναλλαγές (transactions).* Σε ένα δίκτυο όπως το bitcoin, μια συναλλαγή λέει στο δίκτυο ότι ο ιδιοκτήτης ενός αριθμού νομισμάτων, επιτρέπει τη μεταφορά ορισμένων από αυτά σε κάποιον άλλο χρήστη. Ο νέος ιδιοκτήτης μπορεί έπειτα να ξοδέψει αυτά τα νομίσματα δημιουργώντας μια νέα συναλλαγή που επιτρέπει τη μμεταφορά σε άλλον ιδιοκτήτη και ούτω καθεξής. Οι συναλλαγές συνδέονται με ένα δημόσιο κλειδί που αντιστοιχεί στη διεύθυνση του παραλήπτη και νέου ιδιοκτήτη. Για τη μεταφορά αυτής της αξίας, ο νέος κάτοχος πρέπει να υπογράψει με το ιδιωτικό του κλειδί για να εγκρίνει τη συναλλαγή που πρόκειται να πραγματοποιηθεί.

Οι συναλλαγές εν γένει είναι υπογεγραμμένα (signed) τμήματα πληροφορίας, που δημιουργούνται από τους συμμετέχοντες κόμβους ενός δικτύου και αναμεταδίδονται στο υπόλοιπο δίκτυο. Οι συναλλαγές είναι κρυπτογραφημένες και πρέπει να επαληθευτούν πριν κατακερματιστούν και κωδικοποιηθούν σε ένα δέντρο Merkle, του οποίου η ρίζα είναι το υπολογισμένο hash του υποψήφιου block [24]. Μέχρι όμως να ενταχθεί στο δίκτυο, η συναλλαγή αυτή ορίζεται ως «αίτημα συναλλαγής» και αναμεταδίδεται στο δίκτυο με αυτό το τρόπο.

Οι κόμβοι του δικτύου συλλέγουν τα αιτήματα συναλλαγών και αφού επιβεβαιώσουν την εγκυρότητά τους, τα τοποθετούν σε ένα block. Εκτός από τα αιτήματα συναλλαγών, κάθε block περιέχει και μια χρονοσφραγίδα (timestamp), ένα μοναδικό αναγνωριστικό (ID, για παράδειγμα το hash ενός δέντρου Merkle), και το αναγνωριστικό του προηγούμενου block στην αλυσίδα, που αποτελεί το συνδετικό κρίκο μεταξύ τους.



Εικόνα 1: Περιεχόμενα block στην αλυσίδα

Το κάθε block στην αλυσίδα μπορεί να περιέχει οποιουδήποτε είδους δεδομένα, ανάλογα πάντα τον σκοπό που εξυπηρετεί το σύστημα και την εφαρμογή του. Το blockchain είναι μια κατανεμημένη εφαρμογή διότι σε αυτό συμμετέχουν πολλοί υπολογιστές, οι οποίοι συμμετέχουν στη συνέχιση της αλυσίδας, συνήθως με κάποιο κίνητρο κέρδους. Η πιο ευρεία χρήση του αφορά την οικονομική σκοπιά και κυρίως τα κρυπτονομίσματα. Ωστόσο, τα τελευταία χρόνια δημιουργούνται νέοι τύποι blockchain οι οποίοι έχουν και διαφορετική στόχευση.

Επόμενο δομικό στοιχείο είναι το κατανεμημένο καθολικό (distributed ledger), το οποίο περιέχει τα δημιουργημένα blocks που απαρτίζουν το δίκτυο. Οι επικυρωμένες συναλλαγές πρώτα θα προστεθούν στο τέλος της υπάρχουσας αλυσίδας από block, έπειτα θα συγχρονιστούν, και τελικά θα κατανεμηθούν σε όλο το δίκτυο. Ως αποτέλεσμα, κάθε κόμβος του δικτύου έχει το ίδιο αντίγραφο της βάσης δεδομένων.

Τέλος, ο μηχανισμός συναίνεσης, που θα αναλύσουμε και στη συνέχεια, χρησιμοποιείται για να αποφασιστεί ποιο block θα προστεθεί στην αλυσίδα. Είναι γνωστός επίσης και ως αλγόριθμος συναίνεσης, και είναι ο ασφαλής τρόπος συνεργασίας των υπολογιστών που αποτελούν μέρος ενός δικτύου, που ανήκουν δηλαδή στο κατανεμημένο σύστημα. Στις υλοποιήσεις blockchain, μια συναλλαγή θεωρείται έγκυρη μόνο εφόσον το 50% των κόμβων του δικτύου φτάσουν σε συμφωνία σχετικά με την εγκυρότητα, ακολουθώντας την αρχή «η μεγαλύτερη αλυσίδα κερδίζει» [1].

2.4. Είδη Blockchain

Μπορούμε να ορίσουμε κάποιες κατηγορίες blockchain με διαφορετικούς άξονες κάθε φορά, συγκεκριμένα ως προς την ανοικτότητα (openness) και ως προς τα δικαιώματα (permissions).

2.4.1. Με βάση το Openness

Έχοντας ως άξονα το πόσο ανοιχτό είναι ένα δίκτυο blockchain, μπορεί να κατηγοριοποιηθεί ως δημόσιο, ιδιωτικό, ή υβριδικό [25] [26].

Το Δημόσιο (public) blockchain αποτελεί τις πιο δημοφιλείς υλοποιήσεις κρυπτονομισμάτων, όπου τόσο ο πηγαίος κώδικας όσο και τα δεδομένα της αλυσίδας είναι προσβάσιμα από τον καθένα. Παραδείγματα δημόσιων blockchain αποτελούν το Bitcoin και το Ethereum, που είναι από τα μεγαλύτερα δίκτυα σε αριθμό συμμετεχόντων.

Ο κάθε χρήστης έχει πρόσβαση στο δίκτυο, και μπορεί να συμμετέχει στο σύστημα στο επίπεδο λειτουργειών που διαλέγει. Μπορεί να συμμετέχει σαν απλός χρήστης, ή και να λάβει μέρος σε πιο σύνθετες λειτουργίες, όπως η επαλήθευση και επικύρωση των συναλλαγών. Υπάρχει διαφάνεια και ένα από τα χαρακτηριστικά των δικτύων αυτών είναι ότι η συμμετοχή από τους χρήστες σε αυτά τα δίκτυα παροτρύνεται με μια ανταμοιβή που θα τους αποδοθεί, για παράδειγμα κατά την επίτευξη εξόρυξης ενός block.

Είναι αξιοσημείωτο πως τα δημόσια blockchain δίκτυα τείνουν να είναι πιο ασφαλή από τους υπόλοιπους τύπους blockchain, λόγω του γεγονότος ότι κανένας οργανισμός ή κυβέρνηση δεν ελέγχει το δίκτυο, και η συμμετοχή γίνεται ανώνυμα. Από το σχεδιασμό τους είναι πλήρως αποκεντρωμένα, και ο κώδικας του δικτύου επίσης ανανεώνεται από την κοινότητα στην οποία συμμετέχουν εθελοντικά προγραμματιστές.

Στα μειονεκτήματα των δημόσιων blockchain μπορούμε να καταλογίσουμε το ότι απαιτούνται σημαντικά ποσά υπολογιστικής ισχύος για να επιτευχθεί η συναίνεση και η διατήρηση ενός κατανεμημένου βιβλιαρίου. Επίσης, τα δημόσια blockchain δίκτυα είναι συχνά πιο αργά σε σχέση με τα υπόλοιπα είδη blockchain, και με τη συνεχόμενη αύξηση των συναλλαγών, αντιμετωπίζει προβλήματα αποθηκευτικού χώρου. [27]

Τα Ιδιωτικά (private) blockchain είναι μια επίσης δημοφιλής κατηγορία δικτύων, όπου οι συμμετέχοντες χρειάζονται έγκριση για να γίνουν μέλη του δικτύου, οι συναλλαγές είναι ιδιωτικές και ορατές μόνο στο οικοσύστημα του δικτύου (δηλαδή όχι

από εξωτερικούς κόμβους) και η λειτουργία τους βασίζεται περισσότερο σε κεντρικές αρχές. Είναι πιο μικρά σε αριθμό συμμετεχόντων σε σχέση με τους υπόλοιπους τύπους blockchain, και θα πρέπει να αναφερθεί πως είναι πολύ πιο γρήγορα από τα υπόλοιπα είδη blockchain, καθώς ενδέχεται να έχουν έως και μηδενικές καθυστερήσεις στο χρόνο επικύρωσης των δεδομένων. Έχουν επίσης χαμηλό κόστος λειτουργίας, απεριόριστη χωρητικότητα, και μπορούν να κατασκευαστούν σε πολύ γρήγορο χρονικό διάστημα.

Αξίζει να σημειωθεί πως τα περισσότερα ιδιωτικά δίκτυα blockchain δεν χρησιμοποιούν κάποιο κρυπτονόμισμα, και δεν έχουν την ίδια ασφάλεια που παρέχει ένα αποκεντρωμένο blockchain δίκτυο [28]. Το μεγαλύτερο ίσως παράδειγμα ιδιωτικού δικτύου blockchain αποτελεί το Hyperledger Fabric [29]. Τέτοιου είδους υλοποιήσεις επιλέγονται κυρίως από οργανισμούς και οντότητες που μέσα στο δίκτυο έχουν αυξημένο έλεγχο.

Τα υβριδικά (hybrid) blockchain δίκτυα, συνδυάζουν χαρακτηριστικά τόσο από τα δημόσια όσο και από τα ιδιωτικά δίκτυα, και ονομάζονται επίσης δίκτυα κοινοπραξίας (consortium) [30]. Πρόκειται για κλειστά δίκτυα, που διοικούνται από μια ομάδα οργανισμών που έχουν συμφωνήσει να συνεργαστούν. Οι κοινοπραξιακές αλυσίδες παρέχουν περισσότερο έλεγχο και προστασία από τα δημόσια blockchain, ενώ εξακολουθούν να προσφέρουν ορισμένα από τα οφέλη της, όπως η αποκέντρωση και η διαφάνεια. Σε ένα κοινοπρακτικό δίκτυο, οι συμμετέχοντες ελέγχονται προτού τους επιτραπεί να ενταχθούν σε αυτό, και οι συναλλαγές επικυρώνονται από μια επιλεγμένη ομάδα εξουσιοδοτημένων επικυρωτών.

Οι κοινοπρακτικές αλυσίδες χρησιμοποιούνται πιο συχνά σε κλάδους όπου πολλαπλοί οργανισμοί επιθυμούν να μοιράζονται πληροφορίες και να συνεργάζονται, όπως στα χρηματοοικονομικά συστήματα ή στη διαχείριση εφοδιαστικών αλυσίδων. Αυτή τη στιγμή, υπάρχουν οι δημοφιλείς υλοποιήσεις από τα δίκτυα Hyperledger [31] και Ethereum [32] για κατασκευή υποδομών κοινοπραξιακών δικτύων.

2.4.2. Με βάση τα Permissions

Με γνώμονα τα permissions, τα δίκτυα χωρίζονται στα permissioned και permissionless.

Τα permissioned [33] blockchain δίκτυα βασίζουν την ομαλή λειτουργία τους σε συγκεκριμένους κόμβους κλειδιά, όπως τους μετόχους ενός οργανισμού. Πρόκειται για ένα συνδυασμό των καλύτερων χαρακτηριστικών από τα ιδιωτικά και δημόσια blockchain δίκτυα. Σε αυτό το τύπο δικτύων, ο κόμβος που συμμετέχει μπορεί να μη

χρειάζεται εξουσιοδότηση για να συνδεθεί στο δίκτυο, αλλά σίγουρα θα χρειαστεί συγκεκριμένη άδεια για να συνδιαλλαχθεί με τους υπόλοιπους κόμβους, δηλαδή να περάσει από έγκριση από τις οντότητες που ελέγχουν το δίκτυο [34]. Παράδειγμα τέτοιου δικτύου αποτελεί και το δίκτυο Ripple, που βασίζεται στο XRP πρωτόκολλο συναίνεσης [35].

Αντίθετα, στα permissionless blockchain δίκτυα είναι ελεύθερη τόσο η σύνδεση όσο και οι συναλλαγές που μπορούν να πραγματοποιηθούν από έναν κόμβο, αφού ο καθένας μπορεί να δημιουργήσει λογαριασμό και στη συνέχεια να μεταφέρει ή να του μεταφερθούν ποσά. Permissionless υλοποιήσεις αποτελούν τα Bitcoin και Ethereum.

2.4.3. Χαρακτηριστικά των διαφορετικών ειδών Blockchain

Αξίζει να συγκεντρώσουμε τα βασικά χαρακτηριστικά των διαφορετικών ειδών Blockchain που επικρατούν στη βιβλιογραφία, και να γίνει μια αναφορά στα προτερήματα και τα μειονεκτήματά τους. Σε κάθε περίπτωση, ισχύουν τα βασικά χαρακτηριστικά του blockchain που έχουμε αναφέρει. Η χρήση μιας κοινής βάσης δεδομένων αλλά και όλων των λειτουργιών σε αυτό είναι το πιο σημαντικό χαρακτηριστικό ενός blockchain δικτύου, και ενισχύει την διαφάνεια μέσα στο δίκτυο, ως προς την εκτέλεση των συναλλαγών. Επίσης, η αδυναμία μεταβολής των δεδομένων, δημιουργεί μια αμετάβλητη βάση δεδομένων στο δίκτυο.

Public Permissionless Blockchain

Οι κατανεμημένες δημόσιες πλατφόρμες πληρωμών τείνουν να έχουν τα εξής χαρακτηριστικά:

(1) Βασίζονται στο διαδίκτυο και συγκεκριμένα σε όσους θέλουν να διαθέσουν την επεξεργαστική ισχύ του υπολογιστή τους για τη λειτουργία του δικτύου (χωρίς να υπάρχει κάποιος περιορισμός ως προς τη συμμετοχή), σε αντίθεση με άλλες πλατφόρμες που χρησιμοποιούν ιδιωτικά δίκτυα (όπως π.χ. Visa)

(2) Βασίζονται σε ένα πρωτόκολλο που είναι απαραίτητο για τη μεταφορά των ποσών και την αποθήκευσή τους στο δίκτυο, το οποίο με τη σειρά του βασίζεται στη κρυπτογραφία.

(3) Περιέχουν τα εικονικά νομίσματα τα οποία χρησιμοποιούνται για τη μεταφορά αξιών

(4) Υπάρχει ένα ανταποδοτικό σύστημα, το οποίο ανταμείβει τους συμμετέχοντες για την επεξεργαστική ισχύ και τους πόρους που δαπανούν.

(5) Χρησιμοποιούν λογισμικό ανοιχτού κώδικα, και επιτρέπουν τη χρήση του και την συμμετοχή στην επεξεργασία του από τον καθένα.

(6) Το σύστημα διακυβέρνησης που χρησιμοποιούν είναι παρόμοιο με αυτό του ανοιχτού κώδικα, και βασίζεται σε εθελοντές για την εξέλιξή του

(7) Στα δίκτυα αυτά μπορεί να προστεθεί η δυνατότητα απόκρυψης των στοιχείων των χρηστών, μέσω της τεχνολογίας δημόσιου/ιδιωτικού κλειδιού. Η τεχνολογία κρυπτογραφίας αυτή επιτρέπει τη διατήρηση της ανωνυμίας στο δίκτυο, αφού δεν υπάρχει κάποιος κεντρικός παράγοντας που μπορεί να ελέγχει και να ταυτοποιεί τους χρήστες της εκάστοτε πλατφόρμας.

Πλεονεκτήματα & Μειονεκτήματα public permissionless blockchain

Το βασικό πλεονέκτημα μιας public permissionless blockchain αρχιτεκτονικής είναι η ετοιμότητά τους να χρησιμοποιηθούν ως μέσο συναλλαγών. Είναι έτοιμες πλατφόρμες και ο χρήστης μπορεί να ενταχθεί εύκολα εφόσον διαθέτει ένα ψηφιακό πορτοφόλι, δηλαδή ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού. Σε πολλές περιπτώσεις επίσης το κόστος συναλλαγής είναι πολύ χαμηλό και οι συναλλαγές έχουν αυξημένη ταχύτητα σε σχέση με ορισμένες συμβατικές μεθόδους συναλλαγών.

Από την αντίθετη πλευρά, υπάρχουν και ορισμένα μειονεκτήματα στις συγκεκριμένες αρχιτεκτονικές, τα οποία βασίζονται κυρίως στην έλλειψη μιας κεντρικής αρχής και στην ανωνυμία των χρηστών.

Η κατασκευή ενός δικτύου όπου η εμπιστοσύνη μεταξύ των κόμβων που συμμετέχουν δεν είναι απαραίτητη, όμως έχει και αρκετά μειονεκτήματα. Ένας από τους πιο δημοφιλείς μηχανισμούς συναίνεσης στις αρχιτεκτονικές αυτές, το Proof of Work, αποτελεί εμπόδιο στην επέκταση του δικτύου και στην ευελιξία ως προς το πόσο γρήγορα μπορούν να εφαρμοστούν αλλαγές σε αυτό. Στην περίπτωση του bitcoin, υπάρχει μια ταχύτητα παραγωγής κατά μέσο όρο 1 block ανά 10 λεπτά, ενώ ο αριθμός συναλλαγών ανά δευτερόλεπτο (Transactions Per Second – TPS) κυμαίνεται από 3.3 έως 7 [36], τη στιγμή που παραδοσιακά συστήματα πληρωμών (π.χ. Visa) φτάνουν κατά μέσο όρο τις 1700 συναλλαγές το δευτερόλεπτο.

Η συνεχόμενη επέκταση ενός public permissionless blockchain δημιουργεί έντονο ανταγωνισμό μεταξύ των κόμβων που συμμετέχουν στη διαδικασία της επικύρωσης (mining). Ταυτόχρονα, έχοντας υπόψη τον σταθερό μέσο αριθμό των παραγόμενων blocks, η διαδικασία Proof of Work καθίσταται εξαιρετικά ενεργειακά δαπανηρή. Συγκεκριμένα για το Bitcoin, η ετήσια κατανάλωση ενέργειας υπολογίζεται για το 2023 περίπου στις 130TWh [37], μέγεθος συγκρίσιμο με την ετήσια κατανάλωση ενέργειας της Σουηδίας και των Ηνωμένων Αραβικών Εμιράτων,

Η δυσκολία ως προς την κατανόηση του τρόπου λειτουργίας και τη συμμετοχή σε πλατφόρμες κρυπτονομισμάτων είναι επίσης ένα βασικό μειονέκτημα των public

permissionless blockchain δικτύων, καθώς αυτό μπορεί να οδηγήσει και σε παρανοήσεις ή και ζημίες για τους χρήστες [38]. Η έλλειψη μιας κεντρικής αρχής που να ελέγχει τα κρυπτονομίσματα, σε αντιστοιχία με τις Κεντρικές Τράπεζες ή το Διεθνές Νομισματικό Ταμείο, δημιουργεί κινδύνους ως προς τη χρήση τους. Η συνέχεια της λειτουργίας μιας public permissionless blockchain πλατφόρμας βασίζεται στην ύπαρξη των κόμβων επικύρωσης. Τα κίνητρά τους για να συνεχίσουν να διαθέτουν τους υπολογιστικούς πόρους τους στο σύστημα στηρίζεται κυρίως σε οικονομικά κίνητρα που τους παρέχονται από το δίκτυο, χωρίς να υπάρχει κάποιος δεσμευτικός όρος για να συνεχίσουν την διαδικασία. Για το λόγο αυτό, υπάρχει ο κίνδυνος διακοπής της λειτουργίας, αφήνοντας τους ιδιοκτήτες των κρυπτονομισμάτων με νομίσματα χωρίς κάποια αξία. Επίσης, η μείωση των miners στο δίκτυο είναι δυνατό να συμβεί και από άλλες διαδικασίες, όπως το hard-fork, όπου μια ριζική αλλαγή στο πρωτόκολλο του δικτύου έχει ως αποτέλεσμα δύο παρακλάδια – ένα που ακολουθεί τη καινούργια έκδοση του πρωτοκόλλου και ένα την παλιά. Στην αλλαγή αυτή, υπάρχει πιθανότητα να βρεθούν blocks και συναλλαγές που προηγουμένως είχαν επικυρωθεί, σε μια μη επικυρωμένη κατάσταση, και οι miners δεν είναι υποχρεωμένοι να αλλάξουν το παρακλάδι στο οποίο εκτελούν την διεργασία της επικύρωσης.

Ένα ακόμα υπαρκτό πρόβλημα είναι η πιθανότητα χρεοκοπίας ή κλοπής νομισμάτων σε ανταλλακτήρια κρυπτονομισμάτων σε αυτές τις πλατφόρμες, και μπορεί να οδηγήσει σε απώλεια των νομισμάτων των χρηστών. Τα περισσότερα ανταλλακτήρια δεν ελέγχονται από κάποια ρυθμιστική αρχή και είναι πολύ πιθανό η απώλεια αυτή να είναι μη αναστρέψιμη. Χαρακτηριστικό παράδειγμα μιας τέτοιας περίπτωσης αποτελεί η χρεοκοπία του ανταλλακτηρίου Mt Gox το 2014, που οδήγησε σε απώλεια εκατοντάδων χιλιάδων bitcoins από τους χρήστες [39].

Η έλλειψη μιας κεντρικής αρχής καθιστά αδύνατη την επίλυση περιπτώσεων συναλλαγών που δεν έχουν εγκριθεί από τον χρήστη, μεταφορές λανθασμένου ποσού ή μεταφορές νομισμάτων σε λάθος χρήστη. Επιπλέον, η αδυναμία αναγνώρισης του παραλήπτη, οδηγεί σε μη αντιστρέψιμη απώλεια για τον αποστολέα. Αντίστοιχα, στα έξυπνα συμβόλαια που βασίζονται σε αυτές τις αρχιτεκτονικές, η έλλειψη κάποιου ρυθμιστικού πλαισίου που ρυθμίζει την σύναψη σχέσεων συμβολαίων δημιουργεί αμφιβολίες ως προς την αξιοπιστία και τη χρηστικότητά τους, ιδιαίτερα σε περιπτώσεις διαφωνιών μεταξύ των συναλλασσόμενων.

Ενώ υπάρχει διαφάνεια στις συναλλαγές, αφού αποθηκεύονται στην κατανεμημένη και αμετάβλητη βάση δεδομένων του blockchain δικτύου, ουσιαστικά αποθηκεύονται μόνο τα ψευδώνυμα (alias) των χρηστών, και συγκεκριμένα οι διευθύνσεις των ψηφιακών πορτοφολιών τους – τα δημόσια κλειδιά τους, και μάλιστα κάποιος χρήστης

μπορεί να διαθέτει περισσότερα από ένα πορτοφόλια. Η αδυναμία σύνδεσης των χρηστών με κάποιο ψευδώνυμο, επιτρέπει και τη χρήση ορισμένων πλατφορμών για παράνομες και δόλιες δραστηριότητες, όπως αγοραπωλησίες παράνομων ουσιών ή ξέπλυμα χρημάτων [40].

Public Permissioned Blockchain

Τα κύρια χαρακτηριστικά μιας public permissioned blockchain αρχιτεκτονικής είναι τα εξής:

(1) Η λειτουργία του δικτύου βασίζεται σε ένα συγκεκριμένο διαχειριστή που είναι και ο ιδιοκτήτης του.

(2) Βασίζεται στην κρυπτογραφία για τη μεταφορά, την αποθήκευση και την συναίνεση μεταξύ των κόμβων που συμμετέχουν σε αυτό, και υιοθετούν ένα πρωτόκολλο συναίνεσης το οποίο διαφοροποιείται σε σχέση με το αντίστοιχο των permissionless δικτύων, καθώς οι κόμβοι που επικυρώνουν τα blocks καθορίζονται από τον ιδιοκτήτη του δικτύου.

(3) Είναι πιθανή η χρήση εικονικών νομισμάτων για τη μεταφορά αξίας αλλά όχι απαραίτητη.

(4) Δεν υπάρχει άμεσο ανταποδοτικό σύστημα σε όσους συμμετέχουν στην αποθήκευση και επικύρωση των συναλλαγών του δικτύου.

(5) Χρησιμοποιούν λογισμικό ανοιχτού κώδικα, και επιτρέπουν την συμμετοχή αλλά όχι την επικύρωση από τον οποιοδήποτε.

(6) Η διακυβέρνηση του συστήματος γίνεται από τον ιδιοκτήτη της πλατφόρμας.

(7) Παρά το γεγονός ότι χρησιμοποιείται η τεχνολογία του δημόσιου/ιδιωτικού κλειδιού, η ανωνυμία είναι περιορισμένη, καθώς οι πάροχοι των κλειδιών για τη συμμετοχή στο δίκτυο είναι ορισμένοι από τον ιδιοκτήτη και ακολουθούν τις διαδικασίες αναγνώρισης του πελάτη.

Πλεονεκτήματα & Μειονεκτήματα public permissioned blockchain

Το βασικό πλεονέκτημα μιας public permissioned blockchain αρχιτεκτονικής, όπως και στην προηγούμενη περίπτωση, είναι ότι πρόκειται για πλατφόρμες έτοιμες προς χρήση, που διεκπεραιώνουν συναλλαγές εντός πολύ λίγων δευτερολέπτων και με χαμηλότερο κόστος σε σχέση με τις συμβατικές μεθόδους συναλλαγών. Παράλληλα, επιτρέπει τις συναλλαγές εντός και εκτός του δικτύου με τη χρήση πυλών (gateways).

Τα μειονεκτήματα των public permissioned blockchain δικτύων είναι αρκετά και έχουν να κάνουν κυρίως με την εμπιστοσύνη ως προς τον ιδιοκτήτη της συγκεκριμένης πλατφόρμας και την ασφάλεια των δεδομένων των συναλλαγών.

Η χρήση ενός εικονικού νομίσματος για την επίτευξη των συναλλαγών που δεν ελέγχεται από κάποια κεντρική αρχή και δεν υπόκειται σε κάποιο ρυθμιστικό πλαίσιο, μπορεί να οδηγήσει σε δυσμενείς συνέπειες για τους χρήστες. Χαρακτηριστικά, οι αυξομειώσεις της συναλλαγματικής αξίας των νομισμάτων από πιθανή χειραγώγηση της αγοράς, αλλά και προβλήματα όπως η μη εγκεκριμένη αποστολή νομισμάτων ή η αποστολή νομισμάτων σε λάθος χρήστη είναι αδύνατο να επιλυθούν λόγω της έλλειψης μιας κεντρικής αρχής. Παράλληλα η δυσκολία ως προς την κατανόηση του τρόπου λειτουργίας και τη συμμετοχή σε πλατφόρμες κρυπτονομισμάτων ισχύει και σε αυτή την κατηγορία πλατφορμών.

Η πιθανότητα χρεωκοπίας ή κλοπής των εικονικών νομισμάτων, από ανταλλακτήρια που δεν υπόκεινται σε κάποιο ρυθμιστικό πλαίσιο, υπάρχει και σε αυτή τη περίπτωση, όπως και η πιθανότητα απώλειας ή κλοπής των ιδιωτικών κλειδιών των χρηστών. Και στις δύο περιπτώσεις ο χρήστης οδηγείται σε μη αντιστρέψιμη απώλεια των εικονικών νομισμάτων. Επιπλέον, χρήση των συγκεκριμένων πλατφορμών για συναλλαγές που σχετίζονται με παράνομες δραστηριότητες είναι επίσης πιθανή, λόγω της δυσκολίας ταυτοποίησης των χρηστών λόγω της ανωνυμίας του δημόσιου/ιδιωτικού κλειδιού. Αν και η πλατφόρμα Ripple [35], που αποτελεί υλοποίηση της συγκεκριμένης αρχιτεκτονικής, δεν ενδείκνυται για τέτοια χρήση, ο κίνδυνος είναι ακόμα ορατός.

Επειδή ο ιδιοκτήτης του δικτύου ορίζει συγκεκριμένους κόμβους υπεύθυνους για την επικύρωση των συναλλαγών, η λειτουργία και η σταθερότητα της πλατφόρμας είναι αρμοδιότητα του παρόχου. Τίθεται έτσι το θέμα της αξιοπιστίας ως προς τον πάροχο για τη συνέχεια της λειτουργίας του δικτύου. Αν και οι κόμβοι επικύρωσης δεν έχουν κάποιο οικονομικό κίνητρο όπως στη περίπτωση του permissionless δικτύου, η «σύμβαση» για την λειτουργία των κόμβων επικύρωσης γίνεται με τον πάροχο της κάθε πλατφόρμας. Τέλος, όσον αφορά την ακεραιότητα και την ιδιωτικότητα των δεδομένων των συναλλαγών, ένα στοιχείο που επιζητούν οι επιχειρήσεις και τα χρηματοπιστωτικά ιδρύματα, το πρόβλημα της προηγούμενης περίπτωσης εξακολουθεί να ισχύει, καθώς τα δεδομένα αποστέλλονται σε όλους τους κόμβους επικύρωσης, αλλά είναι προσβάσιμα και από το ευρύ κοινό.

Private Blockchain

Τα χαρακτηριστικά μιας private blockchain αρχιτεκτονικής είναι τα εξής:

(1) Αποτελεί framework το οποίο εφαρμόζεται εντός ενός οργανισμού ή μεταξύ οργανισμών για την βελτίωση συγκεκριμένων διαδικασιών. Στην περίπτωση του project Ubin [41], αρχικός στόχος ήταν η δημιουργία μιας αποκεντρωμένης πλατφόρμας για την επίτευξη διακανονισμών σε συνεχή χρόνο.

(2) Χρησιμοποιούνται και σε αυτή τη περίπτωση πρωτόκολλα που βασίζονται στην κρυπτογραφία δημόσιου/ιδιωτικού κλειδιού για την επίτευξη συμφωνίας των συμμετεχόντων στο δίκτυο.

(3) Δεν περιέχει εικονικά νομίσματα όπως στις προηγούμενες κατηγορίες. Στην περίπτωση του Ubin όμως, δημιουργήθηκε ένα ψηφιακό νόμισμα για το οποίο υπεύθυνη για την έκδοσή του ήταν η Κεντρική Τράπεζα της Σιγκαπούρης και αντικατόπτριζε το συμβατικό νόμισμα.

(4) Δεν υπάρχει ανταποδοτικό σύστημα για τους κόμβους επικύρωσης καθώς οι ίδιοι οι συμμετέχοντες αναλαμβάνουν την συγκεκριμένη διαδικασία.

(5) Τα δίκτυα χρησιμοποιούν πρωτόκολλα που μπορεί να βασίζονται και σε ανοιχτό κώδικα, αλλά στα δίκτυα έχουν πρόσβαση μόνο οι συμμετέχοντες.

(6) Η διακυβέρνηση του δικτύου γίνεται από τον χρήστη ή τους χρήστες που είναι υπεύθυνοι για τη σταθερότητα και την εξέλιξή του.

(7) Η χρήση κρυπτογραφίας για την ενίσχυση της ανωνυμίας δεν ισχύει σε αυτή τη περίπτωση, καθώς πρόκειται για ένα δίκτυο που δημιουργήθηκε από τους ίδιους τους χρήστες και δεν επιτρέπει την συμμετοχή σε νέους χωρίς έγκριση.

Πλεονεκτήματα & Μειονεκτήματα private blockchain

Το βασικό πλεονέκτημα μιας private blockchain αρχιτεκτονικής είναι ότι έχει αυξημένη διαλειτουργικότητα και ταχύτητα στις συναλλαγές. Αυτό συμβαίνει επειδή αναφερόμαστε σε κλειστά δίκτυα, τα οποία έχουν ως στόχο να αντικαταστήσουν ορισμένα υπάρχοντα κεντρικά συστήματα οργανισμών, βελτιώνοντας προβλήματα όπως σφάλματα που οφείλονται στην δομή ενός κεντρικού συστήματος. Επιπλέον, η ιδιωτικότητα και η ασφάλεια των δεδομένων και των συναλλαγών μεταξύ των συμμετεχόντων είναι αυξημένη σε σχέση με τις προηγούμενες αρχιτεκτονικές.

Τα μειονεκτήματα ενός δικτύου αυτής της φύσης σχετίζονται κυρίως με την σύνδεσή τους στο υπάρχον σύστημα των οργανισμών. Καθώς στις περισσότερες περιπτώσεις οι πλατφόρμες αυτές αντικαθιστούν κεντρικά συστήματα συγκεκριμένων διαδικασιών, η προσαρμογή και η σύνδεση ενός κατανεμημένου δικτύου στα υπάρχοντα συστήματα μπορεί να παρουσιάσει αρκετές δυσκολίες. Συγκεκριμένα, θα πρέπει να αναπτυχθεί ένα ρυθμιστικό πλαίσιο που να ορίζει τον τρόπο λειτουργίας της πλατφόρμας αλλά και την εγκυρότητα των συναλλαγών εντός αυτής. Επιπλέον, η

πιθανή μεγέθυνση ή τροποποίηση ενός κατανεμημένου δικτύου μπορεί να αυξήσει την πολυπλοκότητα των διαδικασιών. Σε αυτή τη περίπτωση, η ταχύτητα των διαδικασιών αυτών μπορεί να μειωθεί σημαντικά.

Για την λειτουργία και την χρήση ενός κατανεμημένου δικτύου οι οργανισμοί θα πρέπει να υιοθετήσουν νέες δεξιότητες σχετικά με το λογισμικό και τον εξοπλισμό που χρησιμοποιείται από το κατανεμημένο δίκτυο. Συγκεκριμένα, απαιτούνται δεξιότητες σχετικές με τις τεχνολογίες πληροφοριών και με την κρυπτογραφία. Παράλληλα, οι πάροχοι υπηρεσιών σύννεφου πρέπει να προσαρμόσουν και τον εξοπλισμό τους για την εφαρμογή ενός κατανεμημένου δικτύου. Οι δομές σε αυτή την περίπτωση αναπτύσσονται από εταιρίες πληροφορικής ή συμβουλευτικές. Επομένως και αυτές οι εταιρείες με τη σειρά τους θα πρέπει να αναπτύξουν νέες δεξιότητες σχετικές με τη δημιουργία δομών blockchain για κάθε περίπτωση εφαρμογής.

Κεφάλαιο 3. Μηχανισμοί Συναίνεσης

Στις τεχνολογίες που βασίζονται στο blockchain, το πώς μπορεί να επιτευχθεί μια συμφωνία μεταξύ αναξιόπιστων κόμβων, αποτελεί μια παραλλαγή του προβλήματος των Βυζαντινών Στρατηγών, όπως αναφέρθηκε για πρώτη φορά στη βιβλιογραφία το 1982 [42]. Το πρόβλημα αυτό είναι ένα πρόβλημα θεωρίας παιγνίων, όπου περιγράφει τη δυσκολία που έχουν αποκεντρωμένα μέρη να καταλήξουν σε συναίνεση χωρίς να βασίζονται σε κάποιο αξιόπιστο τρίτο παράγοντα. Σε ένα δίκτυο όπου κανένα μέλος δεν μπορεί να επαληθεύσει την ταυτότητα των άλλων μελών, πώς μπορούν τα μέλη να συμφωνήσουν συλλογικά σε μια συγκεκριμένη αλήθεια;

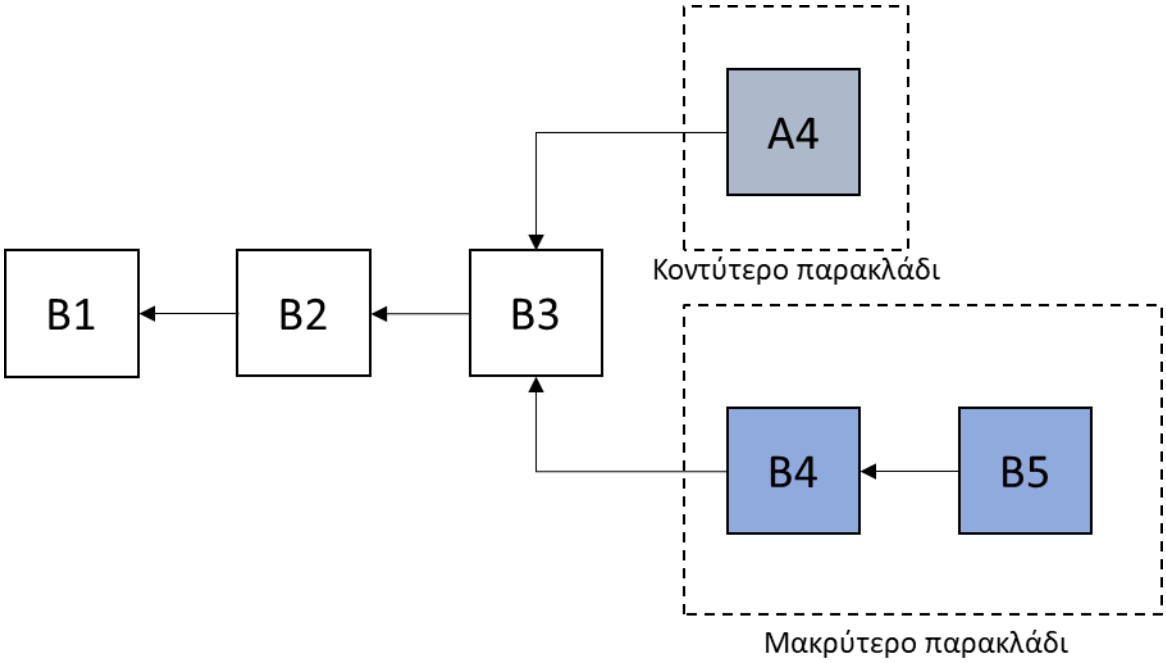
Η αναλογία της θεωρίας παιγνίων πίσω από το Πρόβλημα των Βυζαντινών Στρατηγών (Byzantine Generals Problem – BGP / BG) είναι ότι διάφοροι στρατηγοί πολιορκούν το Βυζάντιο. Έχουν περικυκλώσει την πόλη, αλλά πρέπει να αποφασίσουν συλλογικά για το πότε θα επιτεθούν. Αν όλοι οι στρατηγοί επιτεθούν την ίδια στιγμή, θα κερδίσουν, αλλά αν επιτεθούν σε διαφορετικές χρονικές στιγμές, θα χάσουν. Οι στρατηγοί δεν έχουν ασφαλείς διαύλους επικοινωνίας μεταξύ τους, διότι τα μηνύματα που στέλνουν μπορεί να έχουν υποκλαπεί ή να έχουν σταλεί με δόλο από τους υπερασπιστές του Βυζαντίου. Το πώς μπορεί να επιτευχθεί μια συμφωνία σε ένα κατανεμημένο περιβάλλον σαν και αυτό αποτελεί μια πρόκληση. Η ίδια πρόκληση ισχύει και στο blockchain που είναι επίσης ένα κατανεμημένο δίκτυο. Στο blockchain, δεν υπάρχει κάποιος κεντρικός κόμβος που διαβεβαιώνει πως η κατάσταση των κατανεμημένων κόμβων είναι πάντα ίδια. Απαιτούνται ορισμένα πρωτόκολλα για να βεβαιώσουμε πως τα κατανεμημένα καθολικά στους διαφορετικούς κόμβους είναι συνεπή. Στη συνέχεια θα παρουσιάσουμε κάποιες κοινές προσεγγίσεις για να φτάσουμε στην επιθυμητή συναίνεση όπως έχουν εφαρμοστεί ανά τα χρόνια σε πραγματικά δίκτυα blockchain.

3.1. Proof of Work

Το Proof of Work (PoW) είναι μια στρατηγική συναίνεσης που χρησιμοποιείται στο δίκτυο Bitcoin [1]. Σε ένα αποκεντρωμένο δίκτυο, κάποιος πρέπει να επιλεχθεί για να καταγράφει τις συναλλαγές. Ο ευκολότερος τρόπος είναι η τυχαία επιλογή. Ωστόσο, η τυχαία επιλογή είναι ευάλωτη σε επιθέσεις. Επομένως, αν ένας κόμβος θέλει να δημοσιεύσει ένα μπλοκ από συναλλαγές, πρέπει να γίνει πολλή δουλειά για να αποδείξει ότι ο κόμβος δεν είναι πιθανό να επιτεθεί στο δίκτυο. Γενικά η δουλειά αυτή

είναι πράξεις με τον υπολογιστή. Στο Proof of Work, κάθε κόμβος του δικτύου υπολογίζει μια τιμή κατακερματισμού της επικεφαλίδας του block. Η επικεφαλίδα του block περιέχει μια μη-επαναλαμβανόμενη τιμή (nonce) και οι κόμβοι – επικυρωτές (miners) δοκιμάζουν πολλές διαφορετικές τιμές με μεγάλη συχνότητα ώστε να παράξουν διαφορετικές τιμές κατακερματισμού (hash values). Η συναίνεση απαιτεί η τιμή που θα υπολογιστεί να είναι μικρότερη ή ίση από μια δεδομένη τιμή. Μόλις ένας κόμβος φτάσει την τιμή-στόχο, αναμεταδίδει το block στους υπόλοιπους κόμβους του δικτύου και όλοι οι κόμβοι πρέπει να επιβεβαιώσουν από κοινού την ορθότητα της τιμής κατακερματισμού που μεταδόθηκε. Αν το block θεωρηθεί έγκυρο, οι υπόλοιποι κόμβοι προσθέτουν το block αυτό στο τέλος της αλυσίδας τους. Το να βρεθεί μια λύση στο αρχικό πρόβλημα συχνά παρομοιάζεται με την διεργασία εξόρυξης χρυσού από μεταλλωρύχους [43], και έτσι οι κόμβοι που υπολογίζουν τις τιμές κατακερματισμοί ονομάζονται miners και η διαδικασία Proof of Work που εκτελείται στο Bitcoin ονομάζεται αντίστοιχα εξόρυξη (mining).

Στο κατανεμημένο δίκτυο, υπάρχει πιθανότητα να προκύψουν ταυτόχρονα δύο ή και περισσότερα έγκυρα block, όταν πολλαπλοί miners υπολογίσουν μία σωστή τιμή σε πολύ κοντινό χρόνο. Σαν αποτέλεσμα, μπορεί να δημιουργηθούν παρακλάδια όπως στο παρακάτω σχήμα.



Εικόνα 2: Σενάριο επιλογής μεγαλύτερου παρακλαδιού στο Proof of Work

Ωστόσο, είναι απίθανο ότι δύο αντικρουόμενα παρακλάδια θα παράξουν ένα νέο block ταυτόχρονα. Στο Proof of Work πρωτόκολλο, μια αλυσίδα που γίνεται μεγαλύτερη στη συνέχεια κρίνεται ως η αυθεντική. Ας σκεφτούμε δύο παρακλάδια (branches / forks) που έχουν δημιουργηθεί μέσω των block B4 και A4, τα οποία επικυρώθηκαν ταυτόχρονα. Οι miners συνεχίζουν να κάνουν εξόρυξη στα block τους

μέχρι να προκύψει ένα μακρύτερο παρακλάδι. Τα block B4 και B5 σχηματίζουν μακρύτερη αλυσίδα, και έτσι οι miners του A4 θα αλλάξουν και θα συνεχίσουν την εργασία τους στο μακρύτερο παρακλάδι.

Οι miners πρέπει να ξοδέψουν πολλή υπολογιστική ισχύ για τους υπολογισμούς του Proof of Work, και αυτές οι εργασίες σπαταλούν υπερβολικά πολλούς πόρους. Για να μειωθεί αυτή η απώλεια, έχουν σχεδιαστεί ορισμένα Proof of Work πρωτόκολλα στα οποία η εργασία που εκτελείται μπορεί ταυτόχρονα να χρησιμοποιηθεί σε διαφορετικές εφαρμογές. Για παράδειγμα, οι miners στο Primecoin [44] εκτελούν αναζητήσεις για αλυσίδες ειδικών πρώτων αριθμών, που μπορούν να χρησιμοποιηθούν σε μαθηματική έρευνα.

Για έναν αντίπαλο (adversary) να παρακάμψει το πρωτόκολλο Proof of Work και να διαταράξει την συναίνεση του δικτύου, πρέπει να συγκεντρώσει συνολικά περισσότερη υπολογιστική ισχύ από όλους τους έντιμους κόμβους εξόρυξης μαζί. Αυτό αναφέρεται ως επίθεση 51% (51% attack), όπου πρέπει να αποκτήσει την απόλυτη πλειοψηφία του δικτύου ώστε να το πάρει στον έλεγχό του [45]. Πολλοί πιστεύουν πως αυτή η επίθεση δεν είναι οικονομικά εφικτή να εκτελεστεί σε ένα δίκτυο blockchain, ωστόσο η έλευση των pool εξόρυξης (mining pools) και η χρήση ολοκληρωμένων κυκλωμάτων ειδικών εφαρμογών (ASIC – application-specific integrated circuits) έχουν αποδείξει το αντίθετο. Ορισμένα παραδείγματα κρυπτονομισμάτων που βασίζονται στο Proof of Work είναι το Bitcoin, το Ethereum, το Litecoin και το Dogecoin.

3.1.1. Delayed Proof of Work

Το πρωτόκολλο συναίνεσης Delayed Proof of Work (dPoW) χρησιμοποιείται από το Komodo, μια πλατφόρμα πολλαπλών αλυσίδων [46] και έχει ως βάση τον μηχανισμό Proof of Work. Όπως υπονοεί και το όνομα, μια πλατφόρμα πολλαπλών αλυσίδων αξιοποιεί την ασφάλεια που προσφέρεται από την δευτερεύουσα αλυσίδα (στη συγκεκριμένη περίπτωση, η ασφάλεια που παρέχεται από την επίλυση προβλημάτων με hashing του Proof of Work) για να ασφαλίσει blocks στην κύρια αλυσίδα. Αυτή η διαδικασία εκτελείται από 64 συμβεβλημένους κόμβους που εκλέγονται σε ετήσια βάση, με σκοπό τους να είναι να γράφουν στην Proof of Work αλυσίδα. Κάνοντας αυτή τη διαφοροποίηση, το Delayed Proof of Work αποφεύγει την επιπλέον κατανάλωση ενέργειας και τα επιπλέον κόστη. Το Delayed Proof of Work χρησιμοποιεί μια Proof of Work αλυσίδα για να αποθηκεύσει τις συναλλαγές. Εκτός από το να είναι οικονομικά αποδοτικό, το Delayed Proof of Work είναι επίσης ανθεκτικό

απέναντι στην επίθεση 51%, καθώς ένας αντίπαλος πρέπει να επιτεθεί και στην κύρια και στην δευτερεύουσα αλυσίδα για να επιτύχει το σκοπό του.

3.2. Proof of Stake

Ο μηχανισμός Proof of Stake (PoS) είναι μια λιγότερο ενεργοβόρα εναλλακτική του μηχανισμού Proof of Work. Οι miners στο Proof of Stake πρέπει να αποδείξουν την ιδιοκτησία μιας ποσότητας χρημάτων. Για να συμμετέχουν στη διαδικασία, οι οντότητες πρέπει να έχουν ένα ποντάρισμα (stake) στο σύστημα ώστε να συμμετέχουν στην εξόρυξη ή την επικύρωση των blocks. Αν ένας συμμετέχων κόμβος έχει στην κατοχή του για παράδειγμα το 10% των συνολικών stake, τότε η πιθανότητα να επιλεγεί για να εξορύξει ένα block είναι 10%. Θεωρείται ότι τα άτομα που συγκεντρώνουν μεγαλύτερα χρηματικά ποσά θα είναι λιγότερο πιθανό να επιτεθούν στο δίκτυο. Η επιλογή αυτή που βασίζεται μόνο στο υπόλοιπο του λογαριασμού είναι αρκετά άδικη διότι μπορεί ένα μόνο άτομο με το μεγαλύτερο υπόλοιπο να καταλήξει να είναι κυρίαρχο στο δίκτυο. Ως αποτέλεσμα, έχουν προταθεί πολλές λύσεις με το συνδυασμό του μεγέθους του πονταρίσματος (stake) για να αποφασιστεί ποιος θα κατασκευάσει το επόμενο block. Το Blackcoin [47] χρησιμοποιεί τυχαιότητα για να προβλέψει τον επόμενο κόμβο που θα παράξει ένα block. Χρησιμοποιεί μια μέθοδο που ελέγχει τη χαμηλότερη τιμή κατακερματισμού σε συνδυασμό με το μέγεθος του πονταρίσματος. Το Peercoin [48] δίνει περισσότερη βάση στην επιλογή με βάση το χρόνο ζωής ενός νομίσματος. Παλαιότερα και μεγαλύτερα σύνολα από νομίσματα έχουν αυξημένη πιθανότητα να επιλεγούν για να εξορύξουν το επόμενο block.

Σε σύγκριση με τον Proof of Work μηχανισμό, ο Proof of Stake εξοικονομεί περισσότερη ενέργεια και είναι πιο αποτελεσματικός. Δυστυχώς, επειδή το κόστος της εξόρυξης είναι σχεδόν μηδαμινό, έχουμε ως αποτέλεσμα αυξημένο πλήθος επιθέσεων, αν και μια επίθεση 51% είναι οικονομικά ασύμφορη. Το βασικότερο μειονέκτημα του Proof of Stake είναι το nothing-at-stake, καθώς πολλαπλές αλυσίδες μπορούν να ψηφιστούν από κόμβους που παράγουν block, καθώς δεν έχουν κάτι να χάσουν. Η ψήφιση πολλαπλών αλυσίδων αποτρέπει τη συναίνεση σε αυτή τη περίπτωση, και δημιουργεί πολλά παρακλάδια (forks).

Πολλά blockchains υιοθετούν το Proof of Work στην αρχή, και μεταφέρονται σε Proof of Stake στη συνέχεια. Για παράδειγμα, το Ethereum μεταφέρθηκε από το πρωτόκολλο Ethash (που είναι υλοποίηση του Proof of Work) στο Casper (ένα είδος Proof of Stake) το 2022 [49]. Άλλα παραδείγματα blockchain, εκτός από αυτά που έχουν αναφερθεί ήδη, που βασίζονται στο Proof of Stake είναι το Ouroboros [50], το Gridcoin και το Nxt.

3.2.1. Delegated Proof of Stake

Ο αλγόριθμος αυτός παρουσιάστηκε από τον Daniel Larimer [51]. Είναι άλλο ένα πρωτόκολλο που βασίζεται σε εκλογές και είναι παράγωγο του Proof of Stake. Περιλαμβάνει μια εκλογική διαδικασία ανάλογη με τα διοικητικά συμβούλια (board of directors / stakeholders), όπου τα μέλη του διοικητικού συμβουλίου είναι περιορισμένα σε πλήθος και εκλέγονται από το κοινό. Επιπρόσθετα, έχουν την εντολή από το εκλογικό σώμα για να ασκήσουν τα δικαιώματά του. Εκτός από το ποσό των πονταρισμένων κρυπτονομισμάτων, τα μέλη που έχουν δικαίωμα ψήφου επιλέγονται μέσω μιας διαδικασίας εκλογής και αντικαθίστανται στην πορεία [52]. Ο πλούτος που συγκεντρώνεται στο πρωτόκολλο κατά τους γύρους εκλογών είναι κλειδωμένος σε έξυπνα συμβόλαια (smart contracts). Οι επικυρώσεις συναλλαγών, η δημιουργία νέων block, εργασίες δικτύου και συντήρηση εκτελούνται από εκλεγμένους αντιπροσώπους. Αυτοί οι αντιπρόσωποι είναι οι block producers (BPs), που αμείβονται ανάλογα με την εργασία που ολοκληρώνουν. Υπάρχει επίσης μια ομάδα από εφεδρικούς BP που λαμβάνουν μικρότερες ανταμοιβές. Για κάθε αρνητική ενέργεια ή χαμένο γύρο, ένας BP μπορεί να καταψηφιστεί και να φύγει από την ομάδα των BP. Ο πλούτος και τα κρυπτονομίσματα που έχουν συγκεντρωθεί στο smart contract για το μέλος αυτό, μπορεί να παγώσει ή να κατασχεθεί ως ποινή για τις αρνητικές του ενέργειες. Ο μηχανισμός Delegated Proof of Stake επιχειρεί να αντιμετωπίσει ορισμένα βασικά μειονεκτήματα, όπως το nothing-at-stake πρόβλημα, τις long-range επιθέσεις, και την ασθενή υποκειμενικότητα ενός βασικού Proof of Stake μηχανισμού [53].

Το Delegated Proof of Stake είναι πιο ενεργειακά αποδοτικό και έχει υψηλή απόδοση (throughput – στο EOS παράγεται ένα μπλοκ κάθε 0,5 sec). Ταυτόχρονα, ορισμένες παράμετροι του δικτύου, όπως το μέγεθος του block (block size) και το πόσος χρόνος θα περάσει μεταξύ δυο block (block interval), μπορούν να καθοριστούν από τους αντιπροσώπους. Επίσης, οι χρήστες δεν χρειάζεται να ανησυχούν για ανέντιμους αντιπροσώπους, καθώς μπορούν να καταψηφιστούν εύκολα από το δίκτυο. Ένα από τα μεγάλα αρνητικά του Delegated Proof of Stake είναι πως έχει τη τάση προς συγκεντρωτισμό, και συμμετέχοντες που έχουν μεγάλα ποσά για ποντάρισμα στο δίκτυο μπορούν να ψηφίσουν τους εαυτούς τους ώστε να γίνουν κόμβοι-επικυρωτές. Ορισμένες δημοφιλείς πλατφόρμες που χρησιμοποιούν το πρωτόκολλο Delegated Proof of Stake είναι οι EOS.IO [54], Steemit, List, Ark και BitShares [55].

3.2.2. Leased Proof of Stake

Το Leased Proof of Stake είναι ένας μηχανισμός συναίνεσης που λειτουργεί επίσης παρόμοια με το Proof of Stake, αλλά παρουσιάζει ορισμένες βελτιώσεις. Σύμφωνα με την πλατφόρμα Waves [56], μια blockchain πλατφόρμα που βασίζεται στο Leased Proof of Stake, οι κόμβοι μπορούν να συμμετέχουν σε αυτή λειτουργώντας είτε ως πλήρεις κόμβοι (full nodes), οι οποίοι θα προσθέσουν πληροφορία στο επόμενο block, είτε ως κάτοχοι των κεφαλαίων τους, δανείζοντας μέρος αυτών στους πλήρεις κόμβους (οι ονομαζόμενοι leasers). Μέσω της διαδικασίας αυτής μίσθωσης, γνωστής ως leasing, οι κόμβοι του δικτύου με λίγα κεφάλαια αποκτούν το δικαίωμα συμμετοχής στην παραγωγή των μπλοκ καθώς μισθώνονται κεφάλαια των πλουσιότερων κόμβων, οι οποίοι λαμβάνουν αναλογικά μέρος των τελών που εισπράττονται από τα μπλοκ. Με τη χρήση του Leased Proof of Stake, μία blockchain πλατφόρμα καθίσταται πιο ασφαλής μέσω της ενίσχυσης των επιπέδων αποκεντρωτισμού, ο οποίος είναι αμφιλεγόμενος στην λογική του Delegated Proof of Stake αλλά και του κλασσικού Proof of Stake.

3.3. Practical Byzantine Fault Tolerance (PBFT)

Ο μηχανισμός PBFT παρουσιάστηκε από τους M.Castro και B.Liskov [57] με στόχο την αντιμετώπιση του προβλήματος των Βυζαντινών απειλών στα κατανεμημένα συστήματα. Το Hyperledger Fabric [29] χρησιμοποιεί το PBFT ως το μηχανισμό συναίνεσής του, καθώς το PBFT μπορεί να διαχειριστεί έως και 1/3 των κόμβων του δικτύου να είναι κακόβουλα Βυζαντινά αντίγραφα (byzantine replicas). Λόγω της δομής του, το PBFT αποτελεί ένα μοντέλο συναίνεσης ιδανικό για Blockchain συστήματα με περιορισμένο πλήθος κόμβων, ώστε να επιτυγχάνονται γρήγορες συναλλαγές μεταξύ έμπιστων κόμβων, γνωστών σε όλο το δίκτυο.

Συγκεκριμένα, σε ένα blockchain σύστημα που λειτουργεί με βάση το PBFT πρότυπο οι συναλλαγές ολοκληρώνονται αφού περάσουν μέσα από μία διαδικασία πολλαπλών γύρων ψηφοφορίας την οποία απαρτίζουν ο ηγετικός κόμβος (leader node) και οι υπόλοιποι κόμβοι του δικτύου (validating nodes). Η διαδικασία αυτή αποτελείται από πέντε στάδια-φάσεις: request, pre-prepare, prepare, commit, και reply. Στην πρώτη φάση ο πελάτης στέλνει την συναλλαγή στον ηγετικό κόμβο, ο οποίος επιβεβαιώνει χρονολογικά το αίτημα αυτό, στη συνέχεια ακολουθούν τα επόμενα στάδια επεξεργασίας-ψηφοφορίας, ενώ στο τελευταίο στάδιο ο ηγετικός κόμβος ενημερώνει τον πελάτη για την ολοκλήρωση της συναλλαγής [58]. Για τη συμμετοχή στα στάδια αυτά οι validating nodes πρέπει να συγκεντρώσουν την

αποδοχή των ψήφων των 2/3 του υπόλοιπου δικτύου, ενώ ο ηγετικός κόμβος συντονίζει τις ενέργειες της διαδικασίας.

Η επίτευξη ομοφωνίας μέσω του PBFT δεν απαιτεί ιδιαίτερη ενεργειακή δαπάνη, ενώ το περιβάλλον εμπιστοσύνης που απαιτείται να κυριαρχεί στην αλληλεπίδραση μεταξύ των κόμβων καθιστά το δίκτυο ιδιαίτερα αποδοτικό με μηδαμινές χρονικές καθυστερήσεις και θεωρητικά δεκάδες χιλιάδες συναλλαγές ανά δευτερόλεπτο [59].

Το PBFT είναι ουσιαστικά χρήσιμο σε πλατφόρμες που λειτουργούν σε ιδιωτικό περιβάλλον με περιορισμένους και επιλεγμένους χρήστες, σε αντίθεση για παράδειγμα με τα δημόσια δίκτυα του Bitcoin ή Ethereum, όπου η συμμετοχή είναι ανοιχτή στον καθένα. Η IBM έχει εισαγάγει και λειτουργεί το ιδιωτικό της blockchain δίκτυο στηριζόμενη στο Hyperledger Fabric [31] της Linux Foundation, το οποίο αποτελεί και την δημοφιλέστερη υλοποίηση του PBFT. Μέσω του PBFT το Hyperledger Fabric επιτυγχάνει 2000-3500 συναλλαγές ανά δευτερόλεπτο, ενώ για την ολοκλήρωση των συναλλαγών απαιτείται χρόνος μικρότερος του ενός δευτερολέπτου.

3.3.1. Honeybadger BFT

Οι A. Miller κ.ά. παρουσίασαν το HoneyBadger BFT [60], ένα αποδοτικό και με μεγάλη διακίνηση σύγχρονο πρωτόκολλο, με στόχο να αντικαταστήσουν το παγιωμένο μερικώς ασύγχρονο PBFT πρωτόκολλο. Σε πειραματικές μετρήσεις που πραγματοποιήθηκαν, καταγράφηκαν περίπου 20000 συναλλαγές ανά δευτερόλεπτο σε δίκτυο 40 κόμβων και 1500 συναλλαγές σε δίκτυα μεγαλύτερης κλίμακας, με 100 περίπου κόμβους. Συγκρινόμενο με το PBFT, το Honeybadger BFT κατέγραψε περισσότερες συναλλαγές ανά δευτερόλεπτο παράλληλα με την αύξηση των κόμβων στο δίκτυο, με τα δύο πρωτόκολλα να χαρακτηρίζονται μεν από την ίδια πολυπλοκότητα στην δικτυακή επικοινωνία, αλλά το Honeybadger BFT να παρουσιάζει πιο σταθερή απόδοση σε throughput.

3.3.2. Delegated Byzantine Fault Tolerance (DBFT)

Το Delegated Byzantine Fault Tolerance (DBFT) αποτελεί ένα πρωτόκολλο όπου χρησιμοποιείται ή ίδια λογική και κανόνες με το PBFT με τη διαφορά ότι δεν απαιτείται η καθολική συμμετοχή όλων των κόμβων του δικτύου στη διαδικασία επίτευξης ομοφωνίας. Συγκεκριμένα, σε ένα DBFT σύστημα, όπως η πλατφόρμα κρυπτονομισμάτων NEO, οι κόμβοι διαχωρίζονται σε δύο βασικές κατηγορίες, τους ordinary nodes και τους bookkeepers [61]. Οι κόμβοι της πρώτης κατηγορίας δεν συμμετέχουν στην διαδικασία συναίνεσης, αλλά εκλέγουν τους κόμβους της δεύτερης

κατηγορίας, οι οποίοι θα είναι και εκείνοι που θα συμφωνήσουν για την εγκυρότητα ή μη των συναλλαγών και προχωρούν σε κάθε ένα διαδοχικά στάδια της ψηφοφορίας, αρκεί να συγκεντρώσουν την αποδοχή του 2/3 του συνόλου των κόμβων του δικτύου. Ουσιαστικά το DBFT είναι ένας αλγόριθμος που συνδυάζει το Delegated Proof of Stake με τη γενικότερη λογική της Βυζαντινής Συμφωνίας (Byzantine Agreement – BA), αποτελώντας έναν υβριδικό μηχανισμό συναίνεσης στην blockchain τεχνολογία. Κάποια από τα ιδιαίτερα χαρακτηριστικά που προσφέρει το DBFT είναι το χαμηλό ενεργειακό κόστος και η άμεση οριστικοποίηση των συναλλαγών [62]. Επίσης, κάθε νέο μπλοκ συναλλαγών δημιουργείται ανά 15-20 δευτερόλεπτα, ενώ οι συναλλαγές ανά δευτερόλεπτο στην πλατφόρμα NEO μπορούν να φτάσουν και τις 1000.

Οι Y.Wang κ.ά. [63] προτείνουν μια βελτιωμένη εκδοχή του DBFT, το Credit-Delegated Byzantine Fault Tolerance (CDBFT), το οποίο μέσω της πιστοληπτικής αξιολόγησης βελτιώνει την απόδοση του συστήματος, καθώς πετυχαίνει την μείωση των επιπέδων επικοινωνίας και της συμμετοχής ανεπιθύμητων κόμβων.

3.3.3. Ripple

Το πρωτόκολλο Ripple ή XRP ledger όπως ονομάζεται διαφορετικά, είναι επίσης ένας μηχανισμός συναίνεσης που ανήκει στην κατηγορία BFT [35]. Ένα σύνολο από κόμβους-επικυρωτές (που επίσης ονομάζεται unique node list – UNL) επιλέγεται από τους συμμετέχοντες στο δίκτυο για να αξιολογεί τις συναλλαγές. Αυτοί οι επικυρωτές θα πρέπει να είναι έντιμοι κόμβοι που είναι απίθανο να συνωμοτήσουν μεταξύ τους. Όταν ένα μεγάλο ποσοστό από τους επικυρωτές συμφωνεί σε ένα δεδομένο σετ από συναλλαγές, αυτό το σετ συμπεριλαμβάνεται στην επόμενη έκδοση του λογιστικού (ledger). Διαφορετικά, οι επικυρωτές αλλάζουν τις προτάσεις τους για τις έγκυρες συναλλαγές για να συμφωνούν με τις προτάσεις άλλων αξιόπιστων επικυρωτών. Αυτή η αλλαγή μπορεί να είναι αφαίρεση συναλλαγών ή ένταξη νέων. Είναι μια επαναληπτική διαδικασία που εκτελείται μέχρι να σχηματιστεί ομοφωνία. Η ομοφωνία μπορεί να ισχύσει με την προϋπόθεση ότι τουλάχιστον το 80% των επικυρωτών δεν είναι προβληματικοί ή κακόβουλοι. Ωστόσο, αν αυτή η συνθήκη δεν ικανοποιείται, η πρόοδος όλου του δικτύου απλώς καθυστερεί, αντί να είναι ευπαθής σε επιθέσεις.

3.4. Federated Byzantine Agreement

Το δίκτυο Stellar έχει σχεδιαστεί για να διεκπεραιώνει συναλλαγές με κουπόνια (tokens) από διαφορετικούς εκδότες. Ο μηχανισμός συναίνεσης στον οποίο στηρίζεται, το Stellar Consensus Protocol (SCP) είναι βασισμένο στο Federated Byzantine Agreement (FBA), το οποίο με τη σειρά του αποτελεί γενίκευση της

Βυζαντινής Συμφωνίας (Byzantine Agreement – BA) που υποστηρίζει ανοιχτή ένταξη μελών [64]. Οι εκδότες των tokens μπορούν να ορίσουν επικυρωτές για να επιβάλλουν την ολοκλήρωση των συναλλαγών, ενώ επικυρωτές από διαφορετικούς εκδότες token πρέπει να φτάσουν σε κατάσταση συναίνεσης και ομοφωνίας προτού ο οποιοσδήποτε μπορεί να προσθέσει στο ιστορικό συναλλαγών.

Για να διευκολύνει τη διαδικασία της συναίνεσης, το SCP εισαγάγει την έννοια των τμημάτων απαρτίας (quorum slices). Τα quorum slices είναι υποσύνολα από κόμβους και κάθε ζευγάρι από τα τμήματα αυτά έχουν τουλάχιστον ένα κοινό κόμβο. Τα quorum slices έχουν ζωτικής σημασίας ρόλο για την επίτευξη συμφωνίας στο αποκεντρωμένο σύστημα, όπου οι ενημερώσεις της κατάστασης πραγματοποιούνται μόνο αν υπάρχει μια απαρτία σε συμφωνία. Παραδοσιακά, οι απαρτίες είναι σταθερές και ομοιόμορφες, όμως στο SCP αυτό δεν μπορεί να εφαρμοστεί, καθώς υπάρχει η πιθανότητα να έχουμε κόμβους που δεν γνωρίζουν για την ύπαρξη άλλων κόμβων. Αντ'αυτού, κάθε κόμβος v μπορεί να δηλώσει τα δικά του τμήματα απαρτίας (δηλαδή σύνολο από κόμβους) με τις εξής προϋποθέσεις:

- Εάν όλοι οι κόμβοι σε ένα τμήμα είναι σε συμφωνία για την κατάσταση του συστήματος, ο κόμβος v θεωρεί πως έχουν δίκιο
- Πληροφορίες για το σύστημα μπορούν να αντληθούν από τον v έγκαιρα από ένα από τα τεμάχια απαρτίας, ανά πάσα χρονική στιγμή.

Τα τμήματα απαρτίας του κόμβου v μπορούν να περιέχουν κόμβους με τους οποίους ο v πρέπει να βρίσκεται σε συμφωνία. Οι κόμβοι σε αυτά τα τμήματα μπορούν επίσης να έχουν τα δικά τους τμήματα απαρτίας. Η συμφωνία μεταξύ των κόμβων από διαφορετικά τμήματα απαρτίας (που δεν γνωρίζουν για την ύπαρξη ο ένας του άλλου) συνάγεται μέσω των κοινών κόμβων τους, οι οποίοι έτσι σχηματίζουν απαρτία.

Το πρωτόκολλο SCP έχει δύο βασικές φάσεις: υποβολή υποψηφιότητας (nomination) και ψηφοφορία (balloting). Κατά τη διάρκεια της φάσης υποβολής υποψηφιότητας, οι κόμβοι θέτουν υποψήφιες τιμές για να προστεθούν στο σύνολο συναλλαγών. Με μια διαδικασία που ονομάζεται echoing, αναμεταδίδουν τις υποψηφιότητες των ομότιμων κόμβων στο δίκτυο, και εν τέλει όλοι οι κόμβοι συγκλίνουν σε μια κοινή υποψήφια τιμή. Αυτή η υποψήφια τιμή στη συνέχεια ορίζεται σε ένα ψηφοδέλτιο (ballot), και ψηφίζεται από τους κόμβους. Μπορούν να υπάρχουν πολλαπλά ψηφοδέλτια, για πολλαπλούς υποψήφιους, που μπορούν να ψηφίζονται ταυτόχρονα. Η συναίνεση επιτυγχάνεται όταν οι κόμβοι μπορούν να βρουν ένα τμήμα απαρτίας που αποδέχεται ένα συγκεκριμένο ψηφοδέλτιο.

3.5. Proof of Elapsed Time

Το 2016, η Intel παρουσίασε το Proof of Elapsed Time ως εναλλακτική για το πρωτόκολλο Proof of Work [65]. Τελευταία, το project Sawtooth του Hyperledger (HYP16) χρησιμοποιεί το PoET πρωτόκολλο [66]. Αντί να υπάρχει ανταγωνισμός μεταξύ των κόμβων με βάση τους υπολογιστικούς πόρους ή το ποντάρισμα κρυπτονομισμάτων, το Proof of Elapsed Time υλοποιεί ένα ανταγωνιστικό σύστημα βασισμένο στον μηχανισμός τυχαίας υπαναχώρησης (random back-off) που έχει προηγουμένως υιοθετηθεί στα τοπικά δίκτυα, και συγκεκριμένα για διαδικασίες που αφορούν τον έλεγχο πρόσβασης στο μέσο [67].

Εν γένει, οι συμμετέχοντες κόμβοι αιτούνται να τους ανατεθεί ένας τυχαίος χρόνος αναμονής, και ο κόμβος στον οποίο έχει ανατεθεί η μικρότερη χρονική διάρκεια επιλέγεται για να γίνει ο κόμβος-αρχηγός του block (block leader). Εκτός από το να δημοσιεύσει το νέο block, ο αρχηγός πρέπει επίσης να παρέχει πειστήρια για τον σύντομο χρόνο αναμονής του, και ότι δεν έχει δημοσιεύσει το block του πριν παρέλθει ο χρόνος αυτός [68]. Το Proof of Elapsed Time είναι πιο αποκεντρωμένο λόγω του χαμηλού κόστους που έχει για τη συμμετοχή των κόμβων, κάτι που επιτρέπει περισσότερες οντότητες να συμμετέχουν ευκολότερα. Είναι επίσης αρκετά ευκολότερο για τις οντότητες που συμμετέχουν, να επιβεβαιώσουν πως ο αρχηγός έχει επιλεγεί νόμιμα και ότι το κόστος της εκλογής του αρχηγού είναι αντίστοιχο με το κέρδος που αντλείται από αυτή. Ωστόσο, δεν είναι κατάλληλο για δημόσια συστήματα blockchain και δεν μπορεί να υιοθετηθεί μαζικά, καθώς απαιτεί εξειδικευμένο hardware της Intel. Εκτός από αυτό, προϋποθέτει επίσης εμπιστοσύνη στο υλικό αυτό καθ'αυτό, κάτι που βρίσκεται αντιμέτωπο με μια από τις βασικές ιδέες της τεχνολογίας blockchain, ότι το σύστημα πρέπει να είναι χωρίς εμπιστοσύνη (trustless).

3.6. Proof of Burn

Αντί να γίνεται επένδυση φυσικών πόρων για να πραγματοποιηθούν διαδικασίες εξόρυξης, όπως γίνεται στο πρωτόκολλο Proof of Work, το Proof of Burn (PoBr) εσκεμμένα «καίει» ή καταστρέφει κρυπτονομίσματα ως το μέσο για την επιλογή των αρχηγών του επόμενου block [69]. Στα δίκτυα που είναι βασισμένα στο Proof of Burn για την διαδικασία της επικύρωσης των block δεν χρειάζονται ισχυροί υπολογιστικοί πόροι, και έτσι δεν είναι αναγκαία τα ισχυρά εξειδικευμένα ASIC που χρησιμοποιούνται σε Proof of Work δίκτυα για την εξόρυξη block. Η ενέργεια της καύσης κρυπτονομισμάτων μπορεί να θεωρηθεί και ως η ενέργεια αγοράς μιας εικονικής μηχανής εξόρυξης. Επιτρέπει σε ένα κόμβο να δείξει τη δέσμευσή του στο

δίκτυο, αναλαμβάνοντας μια βραχυπρόθεσμη απώλεια για να λάβει ένα μακροπρόθεσμο κέρδος.

Τα κρυπτονομίσματα μπορούν να καούν στέλνοντάς τα σε μια προκαθορισμένη ειδική διεύθυνση, και δεν μπορούν να ανακτηθούν. Αυτές οι συναλλαγές καύσης έχουν ως αποτέλεσμα ορισμένες τιμές κατακερματισμού καύσης, που είναι ανάλογες με τις τιμές κατακερματισμού που χρησιμοποιούνται για να επιλεγούν οι αρχηγοί block στα δίκτυα Proof of Work.

Ένα παράδειγμα δικτύου που χρησιμοποιεί το Proof of Burn ως το υποκείμενο πρωτόκολλο συναίνεσης είναι το Slimcoin [70].

3.7. Proof of Capacity

Το Proof of Capacity (ή Proof of Space) αποτελεί ένα πρωτόκολλο που ως κύριο χαρακτηριστικό έχει την κατανομή μη τετριμμένου πλήθους από μνήμη ή χώρου αποθήκευσης για να λύσει ένα πρόβλημα που παρουσιάζεται από έναν πάροχο υπηρεσιών [71]. Το Proof of Capacity είναι ένα τμήμα δεδομένων που αποστέλλεται από έναν Prover σε έναν Verifier για να δείξει πως ο Prover έχει δεσμεύσει ένα συγκεκριμένο ποσό χωρητικότητας. Για παράδειγμα, ένας συμμετέχων που αιτείται μιας συγκεκριμένης υπηρεσίας, πρέπει να δεσμεύσει ή να αφιερώσει ένα συγκεκριμένο χώρο στον σκληρό του δίσκο, κάτι το οποίο πρέπει να επιβεβαιωθεί από μια διαδικασία επιβεβαίωσης που θα εκτελέσει ο verifier. Η διαδικασία αυτή πρέπει να είναι σύντομη, αποδοτική και πρέπει να καταναλώνει ένα εύλογο ποσό χωρητικότητας δίσκου.

Όπως και στο Proof of Burn, ο δεσμευμένος χώρος μνήμης αποδεικνύει την υποχρέωση του κόμβου προς το δίκτυο, κάτι το οποίο διαβεβαιώνει πως το κόμβος που ζητάει μια υπηρεσία είναι γνήσιος και έντιμος. Στην πραγματικότητα, είναι δύσκολο για ένα κόμβο να περάσει την διαδικασία επιβεβαίωσης χωρίς να δεσμεύσει το χώρο μνήμης που έχει ισχυριστεί.

Το Proof of Capacity συχνά υλοποιείται χρησιμοποιώντας ένα είδος γράφων που ανήκουν στην κατηγορία hard-to-pebble. Ο κόμβος που εκτελεί την επικύρωση ζητά από τον prover κόμβο να εκτελέσει μια σήμανση (labeling) ενός hard-to-pebble γράφου, και ο prover κόμβος δεσμεύεται σε αυτό. Ο verifier κόμβος με τη σειρά του ζητά από τον prover κόμβο ένα πλήθος τυχαίων τοποθεσιών στον δεσμευμένο αποθηκευτικό χώρο ως απόδειξη ότι έχει εκτελεστεί η σήμανση [72] [73].

Το πιο διαδεδομένο δίκτυο που βασίζεται στο Proof of Capacity είναι το Chia [74], με άλλα παραδείγματα να αποτελούν το Burstcoin και το Spacemint [73].

Κεφάλαιο 4. Μηχανισμοί Συναίνεσης βασισμένοι σε μοντέλα εμπιστοσύνης και κύρους

Έχοντας υπόψη όσα έχουν αναφερθεί στα προηγούμενα κεφάλαια, σχετικά με τα μειονεκτήματα και τους περιορισμούς των πιο δημοφιλών μηχανισμών συναίνεσης που χρησιμοποιούνται, όπως το Proof of Work, έχουν παρουσιαστεί και προταθεί διάφορες εναλλακτικές μέθοδοι για την αντιμετώπιση του προβλήματος της Βυζαντινής Συμφωνίας (Byzantine Agreement). Με την ανοιχτή και δυναμική φύση των peer-to-peer (P2P) δικτύων αυτών που βασίζονται σε blockchain αρχιτεκτονικές, το ρίσκο ασφαλείας σε αυτά τα περιβάλλοντα αυξάνεται σημαντικά, ειδικά όταν κόμβοι μπορούν να εισέρχονται και να αποχωρούν με ευκολία. Είναι σημαντικό να υπάρχει ένα σύστημα που ελέγχει και να αντιμετωπίζει κακόβουλες συμπεριφορές.

Στο κεφάλαιο αυτό θα παρουσιάσουμε μια επισκόπηση ορισμένων μηχανισμών συναίνεσης που επιχειρούν να λύσουν το πρόβλημα της συναίνεσης βασιζόμενα στις έννοιες της εμπιστοσύνης και του κύρους σε ένα δίκτυο, αντικατοπτρίζοντας τις κοινωνικές έννοιες αυτές στην blockchain αρχιτεκτονική. Για τους σκοπούς αυτούς, πολλές από τις επόμενες λύσεις βασίζονται σε συστήματα φήμης (reputation system) για να διευκολυνθεί η εμπιστοσύνη μεταξύ των οντοτήτων του δικτύου [75].

4.1. Συστήματα Φήμης (Reputation Systems)

Μπορούμε να ορίσουμε την στατιστική εκτίμηση της αξιοπιστίας ενός κόμβου από την προοπτική των υπόλοιπων κόμβων του δικτύου ως την φήμη του (reputation). Η φήμη αυτή έχει μια προγνωστική ικανότητα, καθώς είναι μια ένδειξη για την μελλοντική συμπεριφορά του κόμβου σε ένα σύστημα από κόμβους που αλληλοεπιδρούν μεταξύ τους. Σύμφωνα με τη συστημική αυτή περιγραφή, μια καλή φήμη συσχετίζεται με καλή συμπεριφορά, ενώ η κακή φήμη συσχετίζεται με κακή συμπεριφορά. Η φήμη βασίζεται σε κριτικές ή βαθμολογίες που λαμβάνονται σχετικά με μια συγκεκριμένη αλληλεπίδραση. Οι κόμβοι συνήθως βαθμολογούν άλλους κόμβους με βάση την εκάστοτε αλληλεπίδραση, και πιο συγκεκριμένα, μια βαθμολογία είναι μια κρίση από έναν κόμβο (προέλευση – origin) προς έναν διαφορετικό κόμβο (στόχος – target) σε ένα συγκεκριμένο πεδίο εφαρμογής.

Τα συστήματα φήμης είναι μηχανισμοί που σχεδιάζονται για την αξιολόγηση και αναπαράσταση της φήμης ή της αξιοπιστίας ατόμων, οργανισμών ή οντοτήτων σε ένα συγκεκριμένο πλαίσιο. Αυτά τα συστήματα χρησιμοποιούν ανατροφοδότηση,

αξιολογήσεις, κριτικές και άλλα σχετικά δεδομένα για να αξιολογήσουν το βαθμό εμπιστοσύνης, την αξιοπιστία και την ποιότητα των αξιολογούμενων οντοτήτων.

Ο βασικός σκοπός των συστημάτων φήμης είναι να παρέχουν στους χρήστες πληροφορίες και καθοδήγηση κατά τη λήψη αποφάσεων σχετικά με τη συνεργασία ή την εξάρτησή τους από συγκεκριμένες οντότητες. Αυτά τα συστήματα χρησιμοποιούνται συνήθως σε online πλατφόρμες, όπως ιστοσελίδες ηλεκτρονικού εμπορίου, κοινωνικά δίκτυα, διαδικτυακές αγορές και συνεργατικά περιβάλλοντα.

Τα συστήματα φήμης επιτρέπουν στους χρήστες να αξιολογήσουν και να παρέχουν ανατροφοδότηση για τις εμπειρίες τους με άλλους συμμετέχοντες. Αυτή η ανατροφοδότηση συνοψίζεται και επεξεργάζεται για τη δημιουργία μιας βαθμολογίας ή κατάταξης φήμης για κάθε οντότητα. Οι χρήστες μπορούν να χρησιμοποιήσουν αυτές τις βαθμολογίες ή κατατάξεις για να αξιολογήσουν την αξιοπιστία και την εμπιστοσύνη των άλλων πριν από την εμπλοκή σε συναλλαγές ή αλληλεπιδράσεις.

Τα συστήματα φήμης προωθούν επιθυμητές συμπεριφορές και αποθαρρύνουν αρνητικές ή πρακτικές εξαπάτησης μέσω της δημιουργίας ενός συστήματος υπευθυνότητας. Αυτά ενθαρρύνουν τους συμμετέχοντες να ενεργούν υπεύθυνα και ηθικά προκειμένου να διατηρήσουν ή να βελτιώσουν τη φήμη τους. Επιπλέον, τα συστήματα φήμης μπορούν να ενισχύσουν την εμπιστοσύνη των χρηστών, να διευκολύνουν τις διαδικασίες λήψης αποφάσεων και να προάγουν το αίσθημα κοινότητας και συνεργασίας στις online πλατφόρμες.

Υπάρχουν τρία διακριτά μέρη σε ένα σύστημα φήμης: η διαμόρφωση (formulation), ο υπολογισμός (calculation) και η διάδοση (dissemination). Η διαμόρφωση (formulation) περιγράφει το μαθηματικό ή το στατιστικό μοντέλο και το σύνολο εισόδων για την αξιολόγηση των τιμών φήμης. Τα δύο επιμέρους μέρη για τη διαμόρφωση είναι: το μέτρο της φήμης, και το μαθηματικό μοντέλο που χρησιμοποιείται για την συγκέντρωση των βαθμολογιών. Ο υπολογισμός (calculation) χειρίζεται το σχεδιασμό και την υλοποίηση του αλγορίθμου για την αξιολόγηση της φήμης και τέλος, η διάδοση (dissemination) έχει να κάνει με την αποθήκευση και τη διανομή της φήμης στο υπόλοιπο δίκτυο. Δύο δημοφιλείς προσεγγίσεις για τη διαχείριση της διάδοσης είναι είτε μέσω μιας κεντροποιημένης αρχής ή μέσω αποκεντρωμένων κόμβων σε ένα δίκτυο. Επιπλέον, η φήμη μπορεί να μετρηθεί χρησιμοποιώντας συνεχείς ή διακριτές τιμές.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι τα συστήματα φήμης δεν είναι απαλλαγμένα από περιορισμούς. Μπορούν να επηρεαστούν από την εκμετάλλευση ή την παραπληροφόρηση των ανατροφοδοτήσεων και ενδέχεται να μην αποτυπώνουν πάντα την πλήρη πολυπλοκότητα των αξιολογούμενων ατόμων ή οντοτήτων.

Επιπλέον, οι βαθμολογίες φήμης μπορεί να επηρεαστούν από έναν περιορισμένο αριθμό αξιολογήσεων ή προκαταλήψεις, με αποτέλεσμα δυνητικές ανακρίβειες.

Οι Josang κ.ά. το 2002 [76] εισήγαγαν το Beta Reputation System (BRS). Στο σχήμα αυτό, οι βαθμολογίες είναι είτε θετικές ή αρνητικές για μια οντότητα, και οι βαθμολογίες αυτές με τη σειρά τους θεωρούνται ως δύο γεγονότα σε μια κατανομή πιθανότητας βήτα. Η φήμη μιας οντότητας υπολογίζεται ως η αναμενόμενη τιμή της θετικής αξιολόγησης στο μέλλον, προκύπτοντας από την αντικατάσταση του πλήθους αρνητικών και θετικών αξιολογήσεων στην συνάρτηση πυκνότητας πιθανότητας beta που έχει σχεδιαστεί. Το σχήμα αυτό χρησιμοποιεί επίσης έναν παράγοντα λήθης, για να διασφαλίσει ότι οι παλαιότερες αξιολογήσεις έχουν μικρότερη βαρύτητα στον υπολογισμό της συνολικής φήμης της οντότητας. Αφορά επίσης ένα κεντροποιημένο σύστημα, αν και αναφέρουν πως μπορεί να προσαρμοστεί και να αποκτήσει μια κατανεμημένη μορφή.

Στην στατιστική προσέγγιση που πρότειναν οι Weng κ.ά. το 2009 [77], το μοντέλο αξιοπιστίας (credibility model) βασίζεται στις καταθέσεις πολλαπλών μαρτύρων (οι οντότητες που προσφέρουν την κριτική τους) για κάθε οντότητα, και τις χρησιμοποιεί ως ένα συνολικό προφίλ που αποθηκεύεται τοπικά από κάθε οντότητα που προσφέρει την κριτική του. Στο μοντέλο αξιολογείται μεταξύ άλλων και η αξιοπιστία του κάθε μάρτυρα, με βάση το ιστορικό επιτυχίας του. Με την αποκεντρωμένη μέθοδο αυτή στο μοντέλο αξιοπιστίας επιχειρείται να μειωθεί το πρόβλημα των αρνητικών αποτελεσμάτων από άδικες μαρτυρίες.

Άλλες προσεγγίσεις έχουν εμφανιστεί, βασισμένες σε ασαφή λογική [78], [79], Bayesian συστήματα [80]–[82], και υποκειμενική λογική [83]–[85].

4.2. Μηχανισμοί συναίνεσης βασισμένοι στη Φήμη

Όπως έχουμε προαναφέρει, η φήμη ορίζεται ως μια ποσότητα που προέρχεται από το υποκείμενο κοινωνικό δίκτυο, η οποία είναι καθολικά ορατή σε όλα τα μέλη του δικτύου [86]–[88]. Ιστορικά, τα συστήματα φήμης έχουν γνωστοποιηθεί ως ένας τρόπος αξιοποίησης κάποιου είδους δεδομένων φήμης. Λειτουργούν διευκολύνοντας τη συλλογή, τη συγκέντρωση και την κατανομή δεδομένων σχετικά με μια συγκεκριμένη οντότητα. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για να χαρακτηρίσουν και να προβλέψουν τις μελλοντικές ενέργειες αυτής της οντότητας [89], [90]. Ουσιαστικά, οι χρήστες εντός ενός δικτύου μπορούν να αποφασίσουν ποιον θα εμπιστευθούν και με ποιο βαθμό βασιζόμενοι σε δεδομένα φήμης. Ένα σύστημα φήμης, εκτός από τα προηγούμενα, αποτελεί έναν κοινωνικά διορθωτικό μηχανισμό, καθώς το κίνητρο της θετικής φήμης και η αποθάρρυνση της αρνητικής φήμης εν γένει

ενθαρρύνουν την καλή συμπεριφορά μακροπρόθεσμα. Αφού ένα σύστημα φήμης συλλέξει δεδομένα φήμης, αυτά μπορούν να μοιραστούν μεταξύ των χρηστών, οι οποίοι μπορούν στη συνέχεια να τα χρησιμοποιήσουν για να αξιολογήσουν άλλους χρήστες πριν πάρουν αποφάσεις σχετικά με προοριζόμενες ή μελλοντικές αλληλεπιδράσεις, χωρίς να έχουν προηγουμένως αλληλοεπιδράσει. Παραδείγματα πρακτικής εφαρμογής αυτού του συστήματος μπορούν να βρεθούν σε ιστοσελίδες ηλεκτρονικού εμπορίου όπως η Amazon ή το eBay, όπου η φήμη που αποδίδεται σε έναν πωλητή επηρεάζεται από αξιολογήσεις από προηγούμενες συναλλαγές. Ένα άλλο παράδειγμα είναι η κυβέρνηση, όπου χώρες όπως η Κίνα παρακινούν τη συμπεριφορά των πολιτών μέσω ενός συστήματος κοινωνικού πιστοποιητικού σκορ.

4.2.1. Proof of Authority

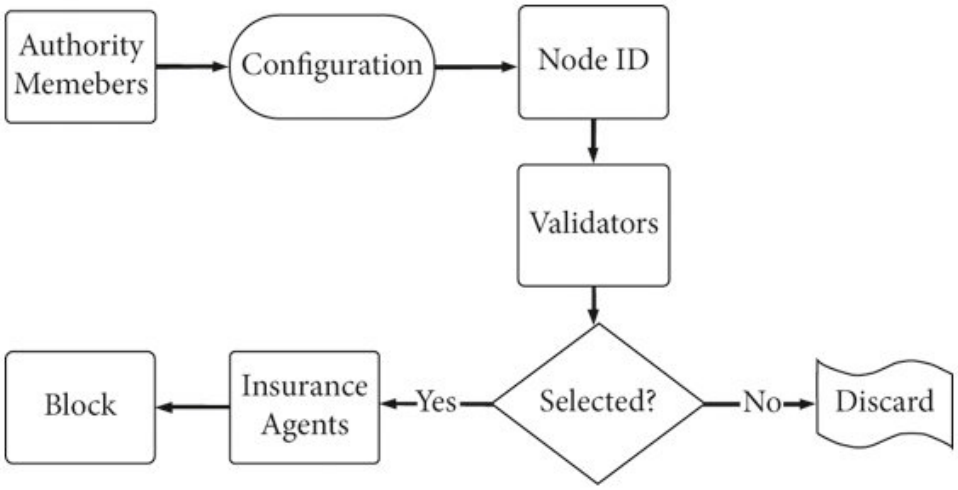
Το Proof of Authority (PoA) είναι άλλη μια παραλλαγή του Proof of Stake [91], [92], και αποτελεί ένα συνδυασμό μεταξύ του Proof of Work και Proof of Stake. Βασίζεται σε μια επιλεγμένη ομάδα εξουσιοδοτημένων επαληθευτών ή κόμβων για την επαλήθευση συναλλαγών και τη δημιουργία νέων μπλοκ. Στο PoA, η συναίνεση επιτυγχάνεται με βάση την ταυτότητα των επαληθευτών αντί για την υπολογιστική ισχύ ή το συνολικό μερίδιο που κατέχουν.

Το πρωτόκολλο λειτουργεί με την αρχή ότι οι επαληθευτές με γνωστές ταυτότητες και φήμες έχουν μεγαλύτερη πιθανότητα να ενεργούν ειλικρινώς και να διατηρούν την ακεραιότητα του δικτύου του blockchain. Οι επαληθευτές συνήθως επιλέγονται με βάση την εμπειρία, την αξιοπιστία ή το μερίδιο που έχουν στο δίκτυο. Στο PoA, οι επαληθευτές εναλλάσσονται για τη δημιουργία μπλοκ και οι ταυτότητές τους είναι γνωστές δημόσια. Κάθε επαληθευτής έχει έναν καθορισμένο χρονικό διάστημα κατά το οποίο έχει την εξουσία να δημιουργεί μπλοκ. Η ταυτότητα του επαληθευτή χρησιμοποιείται ως μια μορφή ψηφιακής υπογραφής, παρέχοντας αποδοτικότητα για τις ενέργειές του.

Μόλις δημιουργηθεί ένα μπλοκ, προστίθεται στο blockchain και οι άλλοι επαληθευτές επαληθεύουν την αυθεντικότητά του πριν το αποδεχθούν. Σε περίπτωση που ένας επαληθευτής ενεργεί κακόβουλα ή ανενδοίαστα, υπάρχουν μηχανισμοί για να τον απομακρύνουν από την ομάδα εξουσιοδοτημένων επαληθευτών και να τον αντικαταστήσουν με νέους.

Το πρωτόκολλο PoA προσφέρει αρκετά πλεονεκτήματα, συμπεριλαμβανομένης της υψηλής ροής συναλλαγών, της χαμηλής καθυστέρησης και της ενεργειακής αποδοτικότητας σε σύγκριση με άλλους μηχανισμούς συναίνεσης όπως το Proof of Work. Ωστόσο, εισάγει έναν βαθμό κεντροποίησης καθώς η εξουσία που επαληθεύει

τις συναλλαγές ανήκει σε έναν περιορισμένο αριθμό επαληθευτών. Συνολικά, το PoA είναι ένα πρωτόκολλο συναίνεσης κατάλληλο για ιδιωτικά ή κοινοπρακτικά blockchain όπου η εμπιστοσύνη μεταξύ των συμμετεχόντων κόμβων μπορεί να θεσπιστεί και να διατηρηθεί μέσω μιας προκαθορισμένης ομάδας εξουσιοδοτημένων επαληθευτών.



Εικόνα 3: Διάγραμμα ροής Proof of Authority [93]

4.2.2. Proof of Reputation

Στο Proof of Reputation (PoR), που αποτελεί επέκταση του Proof of Authority, η εμπιστοσύνη και η φήμη αποτελούν κίνητρα για την επιβολή επιθυμητής συμπεριφοράς στους συμμετέχοντες του πρωτοκόλλου [94]. Οι συμμετέχοντες που δημοσιεύουν μπλοκ εγκαίρως όταν επιλέγονται ανταμείβονται με αξιοπιστία, η οποία οδηγεί στη φήμη για αυτούς τους συμμετέχοντες κόμβους. Όπως και σε άλλα πρωτόκολλα όπου οι συμμετέχοντες ή οι miners ανταμείβονται με νομίσματα του δικτύου για τη δημιουργία μπλοκ ή την καλή συμπεριφορά, το PoR ανταμείβει τους συμμετέχοντες με εμπιστοσύνη, η οποία δεν είναι μεταφερόμενη.

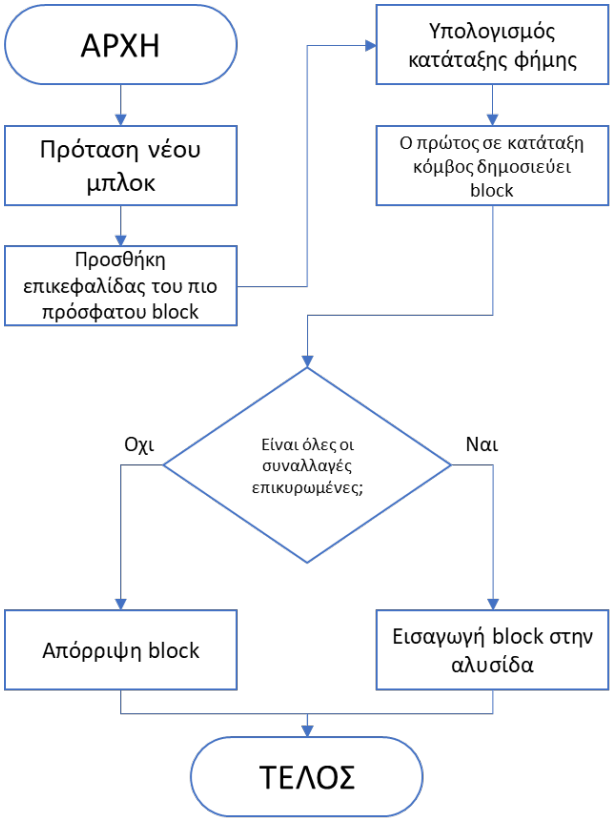
Η εμπιστοσύνη αποτελεί μέτρο της φήμης. Οι συμμετέχοντες κόμβοι με συνεχώς υψηλές τιμές αξιοπιστίας μπορούν να παρέχουν καλύτερες και πιο σταθερές υπηρεσίες από αυτούς που δεν έχουν. Σε αντίθεση με το Proof of Work, όπου οι κόμβοι που λύνουν το κρυπτογραφικό πρόβλημα με τον συντομότερο χρόνο επιλέγονται για να δημοσιεύσουν ένα μπλοκ, το PoR επιλέγει τους συμμετέχοντες κόμβους με την υψηλότερη φήμη ή αξία εμπιστοσύνης στην ομάδα. Με τη δημοσίευση ενός μπλοκ, ο επιλεγμένος κόμβος αυξάνει αυτόματα τη συνολική θέση της φήμης του. Η φήμη των ειλικρινών επαληθευτών αυξάνεται επίσης.

Η τροποποίηση της αλυσίδας blockchain στο Proof of Work θα απαιτούσε υπολογιστική ισχύ αντίστοιχη του 51% της συνολικής υπολογιστικής ισχύος του

δικτύου. Παρόλο που αυτό φαίνεται αδύνατο για την παρούσα στιγμή, η ύπαρξη μεγάλων ομάδων εξόρυξης υποδηλώνει ότι μπορεί να αποτελέσει μια εφικτή απειλή στο μέλλον. Για να αποφευχθεί αυτό το πρόβλημα, τα δημόσια κλειδιά όλων των συμμετεχόντων στο PoR αποθηκεύονται τοπικά. Κάθε συμμετέχοντας κόμβος έχει ένα τοπικό αντίγραφο όλων των δημόσιων κλειδιών, καθιστώντας δύσκολο για οποιονδήποτε κακόβουλο κόμβο να προσπαθήσει να πλαστογραφήσει ταυτότητες χωρίς να ανιχνευθεί αμέσως. Το πρωτόκολλο PoR έχει τρία βήματα:

1. Εκπομπή συναλλαγών: Ο αιτών της υπηρεσίας καταγράφει τον ρυθμό της υπηρεσίας μέσω ανατροφοδότησης στο τέλος κάθε αλληλεπίδρασης. Αυτό το μήνυμα μεταδίδεται μαζί με την υπογραφή του σε άλλους κόμβους που το επαληθεύουν και το αποθηκεύουν στη μνήμη.
2. Δημιουργία μπλοκ: Οι κόμβοι λαμβάνουν συναλλαγές μέχρι να φτάσουν ένα καθορισμένο όριο. Όταν φτάσουν σε αυτό το όριο, ο κόμβος σταματάει να λαμβάνει συναλλαγές και κατατάσσει κάθε πάροχο υπηρεσίας βάσει αυτού του συνόλου των συναλλαγών. Αν ο τρέχων κόμβος είναι ο πάροχος υπηρεσίας με την υψηλότερη κατάταξη, κατασκευάζει και δημοσιεύει ένα μπλοκ, υπογεγραμμένο με το ιδιωτικό του κλειδί.
3. Επαλήθευση μπλοκ: Το μπλοκ προστίθεται στο blockchain μετά την επαλήθευση ότι ο αποστολέας είναι πραγματικά ο πιο αξιόπιστος κόμβος. Αυτό γίνεται από όλους τους κόμβους που λαμβάνουν το μπλοκ, οι οποίοι επίσης επαληθεύουν τις υπογραφές των συναλλαγών χρησιμοποιώντας το δημόσιο κλειδί του υπογράφοντα κόμβου. Αν η επαλήθευση είναι επιτυχής, το μπλοκ προστίθεται στο blockchain.

Το Proof of Reputation είναι ένας μηχανισμός συναίνεσης για permissioned blockchain δίκτυα, ενώ έχει και ορισμένα χαρακτηριστικά που το κάνουν κατάλληλο και για κοινοπρακτικά δίκτυα. Μπορεί να είναι ένα στοιχείο κατάλληλο για συναλλακτικές εφαρμογές, που απαιτούν να λαμβάνουν αποφάσεις με βάση τη φήμη των κόμβων. Το Proof of Reputation χρησιμοποιείται αυτή τη στιγμή από το δίκτυο GoChain [95].



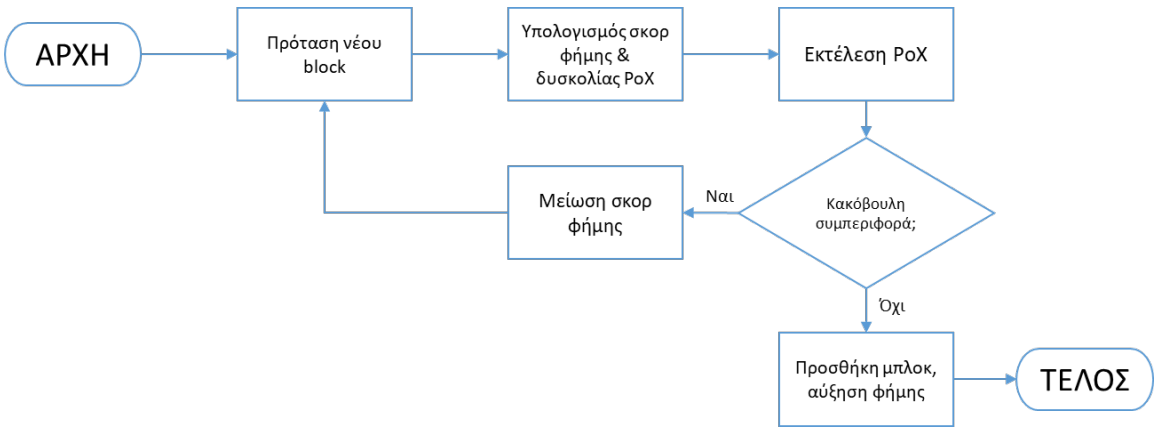
Εικόνα 4: Διάγραμμα ροής Proof of Reputation

4.2.3. Proof of Reputation X

Ο μηχανισμός Proof of Reputation X (PoRX) ενσωματώνει το στοιχείο φήμης του βασικού Proof of Reputation μηχανισμού σε άλλα Proof of X πρωτόκολλα, όπως το Proof of Work [96]. Οι κόμβοι με καλή συμπεριφορά και ιστορικό συμπεριφοράς επιλέγονται βάσει των συγκεντρωμένων πόρων φήμης τους. Αυτοί οι πόροι, που αποκτήθηκαν μέσω καλής συμμετοχικής συμπεριφοράς, αποθηκεύονται στην ενότητα φήμης (reputation module) που βοηθά το σύστημα να μειώσει τις δυσκολίες επίλυσης γρίφων για τα κάτω επίπεδα πρωτοκόλλων PoX και εξαλείφει τον κίνδυνο της κεντρικοποίησης από τη χρήση ASIC και mining pools. Στο PoRX, οι κόμβοι με υψηλότερη φήμη έχουν μικρότερη δυσκολία εξόρυξης σε σύγκριση με τους κόμβους με χαμηλότερη φήμη. Μετά από έναν επιτυχημένο γύρο εξόρυξης, ένας κόμβος ανταμείβεται με περισσότερη φήμη μαζί με τα τέλη εξόρυξης. Ωστόσο, εάν ένας κόμβος αποτύχει να παράγει ένα μπλοκ εντός καθορισμένου χρόνου, αντιμετωπίζει μείωση στη φήμη του, η οποία αντανακλάται στην ενότητα φήμης. Αυτή η φήμη υποβαθμίζεται επίσης με την πάροδο του χρόνου.

Το Proof of X-repute (PoX-R) είναι άλλο ένα πρωτόκολλο συναίνεσης βασισμένο στη φήμη, που συνδυάζει πρωτόκολλα Proof of X με ένα επίπεδο φήμης [97]. Εδώ, χρησιμοποιούμε τον όρο PoX-R για να αναφερθούμε σε αυτό το πρωτόκολλο, αντί για PoRX, προκειμένου να διαφοροποιηθούν σαφώς οι δύο μέθοδοι. Τόσο το PoX-R όσο

και το PoRX αναπτύχθηκαν από την ίδια ομάδα ερευνητών και παρουσιάζουν ορισμένα κοινά χαρακτηριστικά. Το PoX-R εφαρμόζει ένα δημοφιλές πρωτόκολλο X, όπως για παράδειγμα το PoW, με ένα επίπεδο φήμης που ανταμείβει την καλή συμπεριφορά και τιμωρεί τους κόμβους που εμφανίζουν αρνητική συμπεριφορά. Σε κάθε συμμετέχοντα κόμβο ανατίθεται μια τιμή φήμης που αποθηκεύει τις βαθμολογίες φήμης που προκύπτουν από τη συμπεριφορά του. Οι κόμβοι με θετικές συνεισφορές και καλή συμπεριφορά ανταμείβονται με αυξημένες βαθμολογίες φήμης, ενώ αυτοί που ενεργούν κακόβουλα ή είναι αναξιόπιστοι βλάπτονται στις βαθμολογίες φήμης τους. Όπως και στο PoRX, οι κόμβοι με υψηλότερες τιμές φήμης ανταμείβονται με μειωμένη δυσκολία στη διαδικασία εξόρυξης του επιλεγμένου PoX. Οι συμμετέχοντες κόμβοι που συνεισφέρουν θετικά στο σύστημα καταλήγουν να δημοσιεύουν περισσότερα μπλοκ από τους κόμβους που δεν το κάνουν. Το PoX-R βελτιώνει την συνολική αποδοτικότητα του πρωτοκόλλου συναίνεσης PoX, αντιστέκεται σε ισχυρότερες επιθέσεις και παρέχει στους χρήστες με μικρότερη υπολογιστή ισχύ μια καλύτερη ευκαιρία για να συμμετάσχουν στη διαδικασία εξόρυξης. Τα πειραματικά αποτελέσματα δείχνουν ότι το πρωτόκολλο συναίνεσης αυτό που είναι βασισμένο στη φήμη έχει πλεονεκτήματα όσον αφορά την ασφάλεια και ότι η αντοχή του δικτύου κατά των επιθέσεων παρουσιάζει βελτίωση σε σύγκριση με τα δημοφιλή πρωτόκολλα.



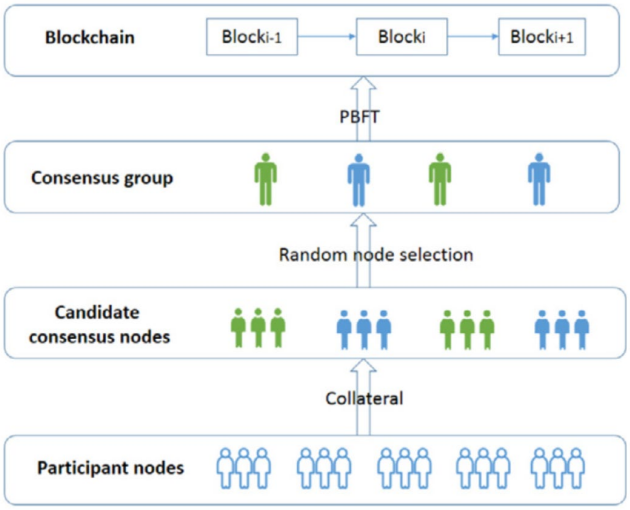
Εικόνα 5: Διάγραμμα ροής πρωτοκόλλου Proof of X-repute

Μια ακόμα εναλλακτική για το Proof of Reputation X πρωτόκολλο, αποτελεί το Permissionless Proof of Reputation X (PL-PoRX) [98], το οποίο παρουσιάζεται ως αναβαθμισμένη έκδοση του Proof of Reputation X. Στο PoRX, ο μηχανισμός με τον οποίο εντάσσονται κόμβοι στο δίκτυο βασίζεται συνήθως σε μια ήδη έμπιστη βάση δεδομένων που συγκρατεί πληροφορίες για την ταυτότητα των χρηστών. Αυτός ο μηχανισμός κάνει το PoRX ημι-κεντροποιημένο, και κατ' επέκταση, permissioned. Στο PL-PoRX αντικαθίσταται η διαδικασία αυτή με μια νέα, με στόχο την πλήρη

αποκεντροποίηση και τη χρήση του πρωτοκόλλου σε permissionless δίκτυα. Ο μηχανισμός που προτείνεται είναι η χρήση μιας κατάθεσης εγγύησης και τιμωρίας. Η εγγύηση χρησιμοποιείται για να προωθηθεί η σωστή συμπεριφορά των κόμβων και να αποτραπούν κακόβουλες συμπεριφορές. Για κόμβους που παρουσιάζουν κακόβουλες συμπεριφορές, η εγγύηση που έχει κατατεθεί είναι δυνατό να μειωθεί ως τιμωρία για την συμπεριφορά τους. Το ποσό που έχει εναπομείνει από την αρχική κατάθεση εγγύησης, επιστρέφεται στον κόμβο από το δίκτυο μόλις αποσυνδεθεί.

4.2.4. Fair Proof of Reputation

Μια πρόσφατη ερευνητική προσθήκη, το Fair proof-of-reputation (FPoR) [99] αποτελεί ένα πρωτόκολλο συναίνεσης που σαν στόχο έχει να ισορροπήσει την ασφάλεια, την αποκεντροποίηση, και την επεκτασιμότητα, και ταυτόχρονα να αυξήσει την δικαιοσύνη μεταξύ των κόμβων. Είναι ένα πρωτόκολλο συναίνεσης που είναι επίσης βασισμένο στην φήμη και βρίσκει εφαρμογή σε permissionless blockchain δίκτυα, και συνδυάζει μηχανισμούς εξασφαλίσεων (collateral), ομάδες συναίνεσης βασισμένες σε επιτροπές, το πρωτόκολλο PBFT, και ανταποδοτικούς μηχανισμούς. Η ομάδα συναίνεσης σχηματίζεται από τυχαία επιλεγμένους κόμβους του δικτύου, γεγονός που βελτιώνει τη δικαιοσύνη του δικτύου και την αποκέντρωσή του, αλλά ταυτόχρονα και την ασφάλεια και τη συμμετοχή των κόμβων. Οι κόμβοι που συμμετέχουν στην διαδικασία συναίνεσης εκτελούν τον μηχανισμό PBFT εντός της ομάδας συναίνεσης στην οποία συμμετέχουν, και βεβαιώνουν την οριστικότητα του κάθε block. Έχοντας ως συστατικά μηχανισμούς εξασφαλίσεων και φήμης, η φήμη χρησιμοποιείται ως κίνητρο για να ενισχύσει καλές συμπεριφορές και να τιμωρήσει τις αρνητικές.



Εικόνα 6: Επισκόπηση του μηχανισμού συναίνεσης Fair Proof of Reputation [99]

Σε πειραματικά αποτελέσματα των ερευνητών για το συγκεκριμένο πρωτόκολλο, αναδείχτηκε πως το FPoR παρουσιάζει μεγάλη απόδοση και επεκτασιμότητα, και μπορεί να χρησιμοποιηθεί τόσο σε permissionless όσο και σε permissioned blockchain δίκτυα.

4.2.5. Proof of Importance

Ο συγκεκριμένος μηχανισμός συναίνεσης αποτελεί μια τροποποιημένη εκδοχή του Proof of Stake και χρησιμοποιήθηκε για πρώτη φορά στο δίκτυο NEM, όπου οι συναλλαγές χρησιμοποιούν το κρυπτονόμισμα XEM [100]. Αυτό που διαφοροποιεί το Proof of Importance από το Proof of Stake και το Proof of Work είναι το γεγονός ότι η χρησιμότητα ενός ενεργού κόμβου στο δίκτυο δεν κρίνεται ούτε από το ποσό της υπολογιστικής ισχύος του ούτε από το συνολικό stake που διαθέτει, αλλά διαμορφώνεται συνυπολογίζοντας επιπλέον παραμέτρους που καθορίζουν την συνολική συνεισφορά του στο δίκτυο. Συγκεκριμένα, κάθε λογαριασμός διαχωρίζει το ποσό XEM που διαθέτει σε δύο μέρη, κατοχυρωμένο (vested) και μη κατοχυρωμένο (unvested) υπόλοιπο, και ανάλογα με τη συναλλαγή διατηρείται μια σχετική αναλογία μεταξύ αυτών. Ένας κόμβος μπορεί να δημιουργήσει ένα μπλοκ, με μια διαδικασία που ονομάζεται συγκομιδή (harvesting) και να λάβει τα τέλη συναλλαγών ως αμοιβή, ανάλογα με το importance score του μέσα στο δίκτυο. Το importance score (βαθμός σπουδαιότητας) είναι αυτό που ουσιαστικά καθορίζει τη συμμετοχή των κόμβων στη διαδικασία συναίνεσης και συνυπολογίζεται από διάφορες παραμέτρους μέσα στο δίκτυο, όπως η φήμη που χαρακτηρίζει τον κόμβο και το πλήθος των συναλλαγών που αυτός έχει ολοκληρώσει. Με τη χρήση του Proof of Importance στο δίκτυο NEM οι ταχύτητες δημιουργίας block κυμαίνονται κατά μέσο όρο στο 1 λεπτό, ενώ σημειώνονται κατά μέσο όρο 3000 συναλλαγές ανά δευτερόλεπτο.

4.2.6. RepuCoin

Ο μηχανισμός συναίνεσης που χρησιμοποιείται στην υλοποίηση του RepuCoin [101], είναι ένας μηχανισμός συναίνεσης που έχει ως γνώμονα μια σταθμισμένη ψηφοφορία με βάση την φήμη. Η συναίνεση στο σύστημα RepuCoin επιτυγχάνεται μέσω της συλλογικής προσπάθειας αξιόπιστων κόμβων συναίνεσης. Αυτοί οι κόμβοι διαθέτουν υψηλή φήμη, η οποία καθορίζεται βάσει της συνεχούς συνεισφοράς τους στο δίκτυο του blockchain. Για τη διατήρηση της ακεραιότητας του συστήματος, υπάρχουν μηχανισμοί τιμωρίας για τους κόμβους που εκδηλώνουν συμπεριφορές που αποκλίνουν από τους καθορισμένους κανόνες. Οι τιμωρίες αυτές μειώνουν

αποτελεσματικά τη φήμη αυτών των κόμβων, λειτουργώντας ως αποτρεπτικός παράγοντας έναντι πιθανών κακόβουλων ενεργειών.

Με την εφαρμογή αυτού του μηχανισμού τιμωρίας, η συναίνεση του RepuCoin εξασφαλίζει ότι το δίκτυο παραμένει ανθεκτικό σε γνωστές επιθέσεις. Αυτή η προσέγγιση αποτρέπει αποτελεσματικά τους κινδύνους που συνδέονται με γνωστές επιθέσεις, συμπεριλαμβανομένης της φημισμένης επίθεσης 51%. Ως αποτέλεσμα, το RepuCoin επιτυγχάνει υψηλή απόδοση, διευκολύνοντας την αποτελεσματική επεξεργασία συναλλαγών, ενώ παράλληλα προστατεύει το σύστημα από πιθανούς κινδύνους.

Συνολικά, ο συνδυασμός των αξιόπιστων κόμβων συναίνεσης και του μηχανισμού τιμωρίας στον αλγόριθμο συναίνεσης του RepuCoin όχι μόνο διατηρεί την ακεραιότητα του δικτύου, αλλά προάγει επίσης την ασφάλεια, καθιστώντας το μια ελκυστική επιλογή για εφαρμογές blockchain.

4.2.7. Υβριδικό PoR/PoS

Οι Kleinrock κ.ά. [87] παρουσίασαν ένα μηχανισμό μάθησης βασιζόμενο στη φήμη, που παρουσίαζε υψηλή επεκτασιμότητα και απόδοση. Στο μηχανισμό αυτό, υλοποίησαν μια επέκταση του Proof of Reputation πρωτοκόλλου, και σχεδίασαν ένα υβριδικό σύστημα όπου σαν εφεδρική λύση χρησιμοποιείται ένα blockchain που βασίζεται σε Nakamoto στρατηγικές. Πιο συγκεκριμένα, χρησιμοποιήθηκε ένας Proof of Stake μηχανισμός για την υποστήριξη της κύριας αλυσίδας. Η προσέγγισή τους δίνει έμφαση στη δικαιοσύνη της φήμης ως βασικό χαρακτηριστικό των πρωτοκόλλων που βασίζονται στη φήμη. Εισήγαγαν ένα τροποποιημένο μοντέλο τυχαίου μαντείου (random oracle) για να προωθήσουν την δικαιοσύνη της φήμης που εξασφαλίζει δίκαιη συμμετοχή, δίνοντας ευκαιρίες σε νεοεισερχόμενους κόμβους στο δίκτυο να συμμετέχουν και ενδεχομένως να χτίσουν τη φήμη τους στο δίκτυο αυτό.

Για να αντιμετωπιστούν οι πιθανές ανησυχίες ασφάλειας και ευελιξίας που προκύπτουν από την υποκειμενική και απρόβλεπτη φύση της φήμης, χρησιμοποιείται ένα λογιστικό στυλ Nakamoto ως εφεδρική λύση. Η πρότασή τους αποτελεί το πρώτο κρυπτογραφικά ασφαλές σχέδιο ενός blockchain βασισμένο σε απόδειξη φήμης (PoR-based) που ενισχύει την ασφάλεια του βασισμένου σε PoR μέσω βελτιστοποιημένης συναίνεσης Nakamoto. Το αποτέλεσμα είναι ένα πρωτόκολλο που είναι αποδεδειγμένα ασφαλές όταν το σύστημα φήμης είναι αξιόπιστο, και διατηρεί τις βασικές ιδιότητες ασφάλειας ακόμα κι αν αυτό δεν συμβαίνει, με την προϋπόθεση ότι το εναλλακτικό blockchain δεν αποτυγχάνει. Με αυτήν την προσέγγιση

αντιμετωπίζονται αποτελεσματικά οι ανησυχίες που προκύπτουν από την υποκειμενικότητα και την αστάθεια των συστημάτων φήμης.

4.3. Μηχανισμοί συναίνεσης με βάση την εμπιστοσύνη

Την τελευταία δεκαετία, ένας αυξανόμενος αριθμός επιχειρήσεων έχει μετασχηματίσει τα μοντέλα τους προς την κατεύθυνση του διαδικτύου. Τα τελευταία χρόνια, η διαδικασία αυτή της μετασχηματιστικής αλλαγής έχει επιταχυνθεί και οι επιχειρήσεις έχουν εισέλθει στην εποχή του cloud computing, όπου η δυνατότητα να μετατραπεί σχεδόν οτιδήποτε σε online υπηρεσία (XaaS) έχει γίνει μια ξεχωριστή πιθανότητα. Ένα σημαντικό παράδειγμα είναι η εμφάνιση των ιστότοπων crowdsourcing. Ένας ιστότοπος crowdsourcing επιτρέπει την αποτελεσματική αντιστοίχιση προσφοράς και ζήτησης υπηρεσιών σε μεγάλη κλίμακα, που δεν μπορεί ποτέ να επιτευχθεί από την παραδοσιακή αποκλειστικά εκτός σύνδεσης αγορά υπηρεσιών. Ενώ η τεχνολογική ανάπτυξη και οι αλλαγές στα μοντέλα επιχειρηματικότητας προχωρούν με ραγδαίους ρυθμούς, η υποδομή που υποστηρίζει την ακεραιότητα και την ευθύνη των επιχειρηματικών υπηρεσιών παραμένει πολύ πίσω. Η υποδομή αυτή αναφέρεται στο θεμέλιο που παρέχει τις λειτουργίες της καταγραφής αποδεικτικών στοιχείων, της ελέγχου και της επίλυσης διαφορών.

Το θεμελιώδες πρόβλημα είναι ότι η παραδοσιακή υποδομή των επιχειρήσεων βασίζεται σε ένα μοντέλο διαπροσωπικής επικοινωνίας και σε ένα εκτός σύνδεσης περιβάλλον, με έναν κεντρικό φορέα που εποπτεύει ορισμένες πτυχές της επιχειρηματικής συμπεριφοράς. Αυτός ο τύπος μοντέλου δεν είναι πλέον κατάλληλος για το Διαδίκτυο και το περιβάλλον των cloud υπηρεσιών, όπως για παράδειγμα οι ιστότοποι crowdsourcing. Αυτό συμβαίνει επειδή το Διαδίκτυο έχει μια ενσωματωμένη κατανομή και οι υπηρεσίες διεκπεραιώνονται κυρίως αυτόματα από υπηρεσίες λογισμικού.

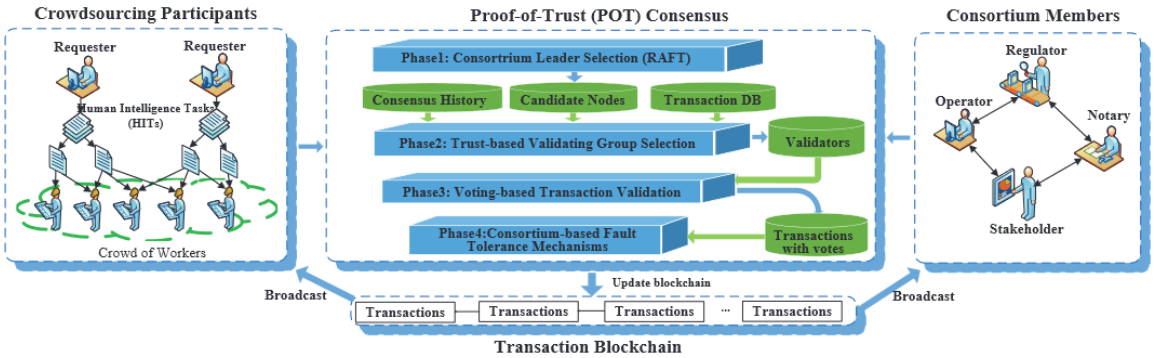
Σε ένα διανεμημένο περιβάλλον, ούτε η έκδοση του πάροχου υπηρεσιών για την παρακολούθηση της εκτέλεσης συμβολαίων υπηρεσιών ούτε η έκδοση του καταναλωτή μπορεί να θεωρηθεί ως η πηγή της αλήθειας. Εάν προκύψει διαφωνία μεταξύ του παρόχου και του καταναλωτή κατά τη διάρκεια της εκτέλεσης ενός συμβολαίου υπηρεσίας, είναι πολύ δύσκολο να επιλυθεί, καθώς ο πάροχος και ο καταναλωτής μπορεί να έχουν διαφορετική έκδοση των αρχείων καταγραφής ή επιχειρημάτων τους. Συνεπώς, υπάρχει επείγουσα ανάγκη για μια υποδομή που διασφαλίζει την ευθύνη στο περιβάλλον των online υπηρεσιών. Χωρίς μια τέτοια υποδομή, οι συμμετέχοντες στις υπηρεσίες δεν μπορούν να είναι βέβαιοι για την δικαιοσύνη των συναλλαγών υπηρεσιών και την ευθύνη της παράδοσης των

υπηρεσιών, κάτι που θα εμποδίσει σοβαρά την υγιή ανάπτυξη της οικονομίας υπηρεσιών στην εποχή του cloud computing.

Για το λόγο αυτό έχουν προταθεί λύσεις στο χώρο των υλοποιήσεων δικτύων blockchain που επιχειρούν να αντιμετωπίσουν το πρόβλημα αυτό, και εν γένει το πρόβλημα της εμπιστοσύνης μεταξύ των κόμβων σε ένα κατανεμημένο σύστημα.

4.3.1. Proof of Trust

Στην δημοσίευση των Zou κ.ά. [2] προτείνεται ένας αλγόριθμος συναίνεσης για τις υπηρεσίες crowdsourcing, ονομαζόμενος Proof of Trust (PoT), όπου οι επαληθευτές συναλλαγών εκλέγονται με βάση τις τιμές εμπιστοσύνης των κόμβων. Στον μηχανισμό αυτό, η συντήρηση του δικτύου blockchain γίνεται από μια ομάδα διαχείρισης λογιστικού (ledger management group), και από αυτή την ομάδα επιλέγεται ένας αρχηγός, χρησιμοποιώντας έναν αλγόριθμο ψηφοφορίας. Έπειτα, ο επιλεγμένος αρχηγός επιλέγει μια ομάδα η οποία είναι υπεύθυνη για την επικύρωση των συναλλαγών που θα εισαχθούν στο blockchain. Η λίστα με τους κόμβους που συμμετέχουν στην ομάδα αυτή κοινοποιείται σε όλο το δίκτυο, και οι κόμβοι του δικτύου ψηφίζουν βασιζόμενοι σε μια βάση δεδομένων που αντιστοιχίζει κόμβους με τιμές εμπιστοσύνης. Ο αρχηγός υπολογίζει τις ψήφους του δικτύου και σχηματίζει την τελική ομάδα επικύρωσης (transaction validation group) και την κοινοποιεί στο δίκτυο. Κάθε κόμβος αυτής της ομάδας επιλέγει υποψήφιες συναλλαγές προς ένταξη στο επόμενο block, και τις κοινοποιεί σε άλλους κόμβους. Οι κόμβοι αυτοί ονομάζονται κόμβοι κοινοπραξίας (consortium nodes) και ψηφίζουν επί των προτεινόμενων συναλλαγών από τους κόμβους επικύρωσης. Οι ψήφοι από την ομάδα κοινοπραξίας και επικύρωσης συνυπολογίζονται από τον κόμβο αρχηγό, και με βάση αυτές επιλέγει τις συναλλαγές που θα μπουν στο επόμενο block.



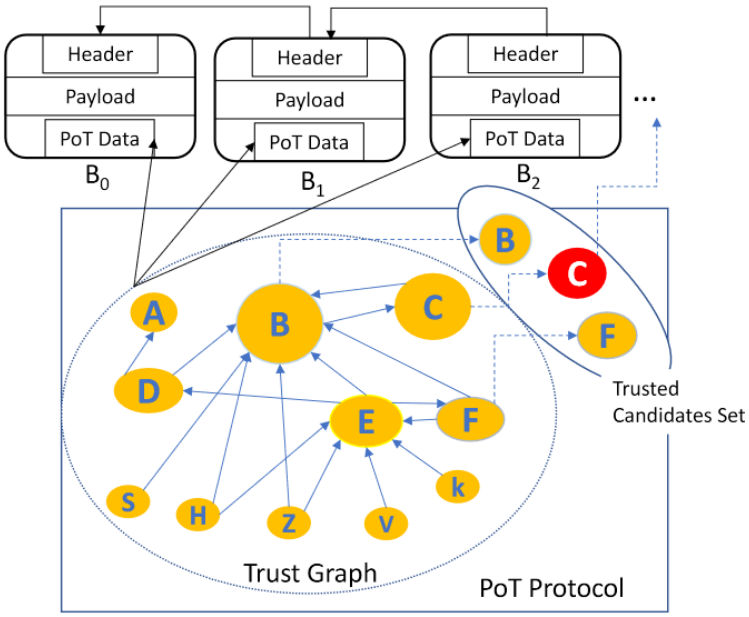
Εικόνα 7: Η αρχιτεκτονική του μηχανισμού Proof of Trust των Zou κ.ά.[2]

Ο μηχανισμός συναίνεσης Proof of Trust των Zou κ.ά. αποφεύγει τη χρήση του Proof of Work, και προσθέτει την έννοια της εμπιστοσύνης σε όλη τη διεργασία.

Ωστόσο, η απόφαση για ένα μοναδικό κόμβο – αρχηγό οδηγεί σε προβλήματα κεντροποίησης και σε ένα μοναδικό πιθανό σημείο αποτυχίας. Επιπλέον, στην δημοσίευση αυτή δεν αναφέρεται το κίνητρο που έχουν οι κόμβοι για συμμετοχή στο δίκτυο, ούτε προσδιορίζονται πληροφορίες για τις βάσεις δεδομένων εμπιστοσύνης που συγκρατούν οι κόμβοι, και αν διαφέρουν μεταξύ τους.

Για να λυθούν ορισμένα από τα προβλήματα αυτά, οι ερευνητές στο [102] παρουσίασαν μια βελτιωμένη εκδοχή του μηχανισμού συναίνεσης Proof of Trust. Ο βελτιωμένος αλγόριθμος Proof of Trust χρησιμοποιεί ένα αλγόριθμο υποκειμενικής λογικής (subjective logic) για να βελτιστοποιήσει την επιλογή των κόμβων που θα συμμετέχουν στην διαδικασία συναίνεσης, και χρησιμοποιεί χρονοσφραγίδες και ψηφιακές υπογραφές για να αυξήσει την απροβλεψιμότητα των κόμβων που παράγουν blocks. Για την εκλογή των κόμβων, χρησιμοποιείται επίσης μεταβλητότητα στην τιμή της φήμης των κόμβων, και έτσι ο αλγόριθμος διαβεβαιώνει πως οι συμμετέχοντες κόμβοι έχουν ίσες ευκαιρίες για να συμμετέχουν στο δίκτυο. Επίσης, προτείνεται ένας μηχανισμός κινήτρων βασισμένος στην θεωρία παιγνίων, όπου η ειλικρίνεια είναι η καλύτερη στρατηγική για κάθε κόμβο. Σε προσομοιώσεις που διεξήχθησαν, τα αποτελέσματα δείχνουν πως ο μηχανισμός αυτός παρουσιάζει βελτίωση σε σύγκριση με τον παραδοσιακό Proof of Trust μηχανισμό, όσον αφορά την εγκυρότητα, την δικαιοσύνη, και την ασφάλεια.

Η ονομασία Proof of Trust επίσης συναντάται στην βιβλιογραφία και από άλλη ομάδα ερευνητών. Οι Bahri κ.ά [103] προτείνουν έναν μηχανισμό συναίνεσης όπου συνδυάζεται ένας «γράφος εμπιστοσύνης» (trust graph) και ο μηχανισμός Proof of Work.



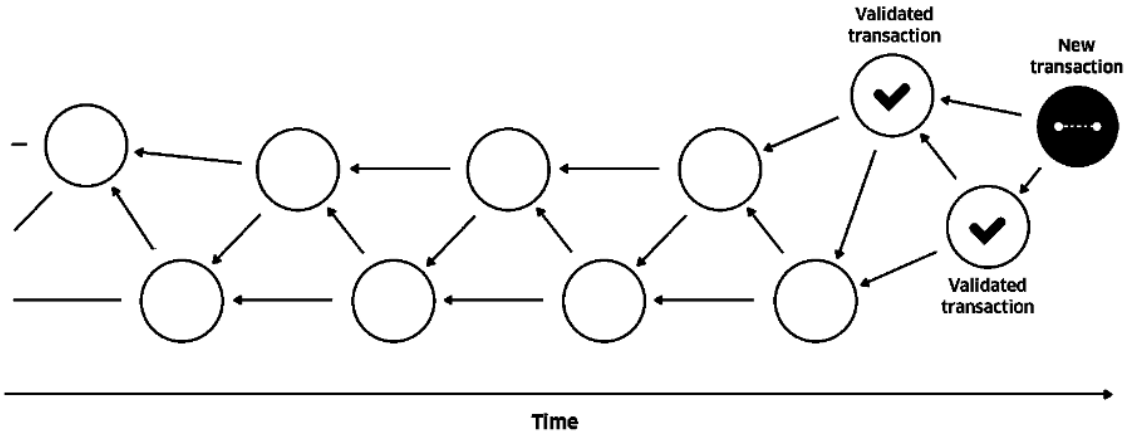
Εικόνα 8: Επισκόπηση του μηχανισμού Proof of Trust των Bahri κ.ά.[103]

Με βάση τον γράφο εμπιστοσύνης προκύπτει η τιμή εμπιστοσύνης (trust score) κάθε κόμβου, και η τιμή αυτή χρησιμοποιείται για να καθορίσει την δυσκολία του κόμβου για την εκτέλεση μιας διεργασίας αντίστοιχης του Proof of Work. Έτσι, όσο πιο έμπιστος είναι ένας κόμβος, τόση λιγότερο έργο θα χρειαστεί να ξοδέψει. Ωστόσο, στην πρότασή τους η επιλογή των κόμβων για την διαδικασία συναίνεσης δεν είναι απόλυτα ντετερμινιστική, και προτείνουν ένα συνδυασμό από μεθόδους. Σε κάθε γύρο, ο κόμβος που πρόσθεσε τελευταίος block στην αλυσίδα, προτείνει ένα τυχαίο σύνολο από υποψήφιους κόμβους, και μέσα σε αυτό το σύνολο οι κόμβοι ανταγωνίζονται για την προσθήκη του επόμενου μπλοκ, εκτελώντας την εργασία Proof of Work μειωμένη αντιστρόφως ανάλογα με την τιμή εμπιστοσύνης τους. Έτσι αποφεύγεται το φαινόμενο της κεντροποίησης και κατάληψης του δικτύου από τους πιο έμπιστους κόμβους. Αυτή η προσέγγιση διατηρεί την δομή του μηχανισμού Proof of Work, και είναι κατάλληλη για δημόσια blockchain δίκτυα, καθώς ο γράφος εμπιστοσύνης βρίσκεται κωδικοποιημένος στα δεδομένα των block, και δεν υπάρχει κάποια κεντρική δομή.

4.3.2. Trustchain

Οι συγγραφείς στο [104] προτείνουν ένα μηχανισμό συναίνεσης που λειτουργεί σε έναν κατευθυνόμενο ακυκλικό γράφο (Directed Acyclic Graph – DAG), όπου οι ίδιες οι συναλλαγές λαμβάνουν ένα σκορ εμπιστοσύνης, με βάση το σκορ εμπιστοσύνης του αποστολέα κόμβου. Ο μηχανισμός αυτός χρησιμοποιείται στην πλατφόρμα COTI, και έχει την ονομασία Proof of Trust, αλλά αναφέρεται επίσης και ως TrustChain. Για να

προστεθεί μια συναλλαγή στο δίκτυο, πρέπει να συνδεθεί με δύο προηγούμενες συναλλαγές με παρόμοιο σκορ εμπιστοσύνης, και να εκτελεστεί μια ελαφριά μορφή του Proof of Work αλγορίθμου για να αντιμετωπιστούν επιθέσει διπλής δαπάνης, δηλαδή να μην μπορεί να ξοδευτεί δύο φορές το ίδιο ποσό. Η προσθήκη των συναλλαγών με αυτό το τρόπο οδηγεί στη δημιουργία αλυσίδων από έμπιστες συναλλαγές, που αναφέρονται ως “trustchain”.



Εικόνα 9: Προσθήκη νέας συναλλαγής στο δίκτυο [104]

Το συνολικό σκορ εμπιστοσύνης της κάθε αλυσίδας προκύπτει από το σκορ εμπιστοσύνης των συναλλαγών που την απαρτίζουν, και για να ελεγχθεί πως μια συναλλαγή έχει επιβεβαιωθεί, το συνολικό σκορ εμπιστοσύνης της αλυσίδας πρέπει να ξεπερνά ένα προκαθορισμένο καθολικό κατώφλι. Στα πλεονεκτήματα της προσέγγισης αυτής έχουμε πως λαμβάνονται υπόψη τα σκορ εμπιστοσύνης τόσο του αποστολέα της συναλλαγής όσο και της ίδιας της συναλλαγής. Ωστόσο, η υλοποίηση αυτή μπορεί να χρησιμοποιηθεί μόνο σε ιδιωτικά δίκτυα περιορισμένου αριθμού κόμβων, και η διαδικασία της συναίνεσης διεκπεραιώνεται κυρίως από ένα μικρό αριθμό κόμβων με υψηλά σκορ εμπιστοσύνης, κάτι που οδηγεί σε κεντροποίηση και μονοπώλιο της διαδικασίας.

4.3.3. Proof of Random Trust

Έχοντας ως βάση το μηχανισμό Proof of Trust, οι ερευνητές στο [105] παρουσιάζουν τον μηχανισμό συναίνεσης Proof of Random Trust (PoRT), που βρίσκει εφαρμογή σε κατανεμημένα δίκτυα διαμοιρασμού ηλεκτρικής ενέργειας. Στόχος της προσέγγισης αυτής ήταν η δημιουργία ενός μηχανισμού με πρωτίστως μεγάλη απόδοση και υψηλή επεκτασιμότητα.

Ο αλγόριθμος του μηχανισμού χρησιμοποιεί τυχαιότητα στις τιμές εμπιστοσύνης για να λύσει τους περιορισμούς των μηχανισμών συναίνεσης που έβρισκαν χρήση

μέχρι πρότινος σε παρόμοια συστήματα. Η υλοποίησή του βασίζεται επίσης στον διαχωρισμό των διαδικασιών της επικύρωσης συναλλαγών και της επικύρωσης των block, και έχει σαφή διαχωρισμό μεταξύ των χρηστών και της επιτροπής κοινοπραξίας. Για την επικοινωνία μεταξύ των κόμβων που είναι χρήστες του δικτύου (π.χ. αγοραστές και πωλητές ενέργειας) και του δικτύου της επιτροπής, χρησιμοποιούνται κόμβοι πύλες (gateway nodes), που μεταφέρουν τα δεδομένα των συναλλαγών. Στο consortium μέρος του δικτύου, ο αρχηγός σε κάθε γύρο προκύπτει από εκλογή και με βάση μια τιμή εμπιστοσύνης του κόμβου, η οποία υπολογίζεται από παλαιότερες τιμές εμπιστοσύνης και από έναν παράγοντα τυχαιότητας. Η τυχαιότητα αυτή επιτρέπει περισσότερες ευκαιρίες εκλογής σε κόμβους που δεν θα είχαν αρκετά υψηλή τιμή εμπιστοσύνης.

Στο δίκτυο των χρηστών γίνεται ο έλεγχος των συναλλαγών, από ένα σύνολο επικυρωτών κόμβων που δημιουργείται δυναμικά, πάλι με εκλογή από το consortium δίκτυο, και μετά από πρόταση από τον κόμβο-αρχηγό. Η εκλογή ακολουθεί παρόμοιο τρόπο υπολογισμού με βάση την ημι-τυχαία τιμή εμπιστοσύνης για κάθε κόμβο του δικτύου των χρηστών. Η επικοινωνία για την σύσταση της ομάδας επικύρωσης γίνεται μέσω των gateway κόμβων προς το δίκτυο των χρηστών, όπου εκτελείται η επικύρωση των συναλλαγών και το αποτέλεσμα μεταβιβάζεται στον κόμβο-αρχηγό του consortium δικτύου, για να παράξει το block και να το προσθέσει στο blockchain.

Στον αλγόριθμο Proof of Random Trust υπάρχει επίσης και μηχανισμός ανταπόδοσης και τιμωρίας, που επηρεάζει την τιμή εμπιστοσύνης που έχει κάθε κόμβος. Σε κάθε γύρο, όλοι οι συμμετέχοντες, δηλαδή ο κόμβος-αρχηγός του consortium δικτύου όσο και οι κόμβοι στο δίκτυο των χρηστών που επιλέγονται στην ομάδα επικύρωσης, ποντάρουν την εμπιστοσύνη τους και ανάλογα την συμπεριφορά τους ανταμείβονται ή τιμωρούνται με ανάλογη αναδιαμόρφωση της τιμής εμπιστοσύνης τους.

4.3.4. Proof of Accumulated Trust

Ο μηχανισμός συναίνεσης Proof of Accumulated Trust (PoAT) [106] παρουσιάστηκε ως μέρος μιας λύσης που αντιμετωπίζει τα θέματα ασφαλείας σε δίκτυα Internet of Vehicles (IoV), όπου διασυνδεδεμένα αυτοκίνητα επικοινωνούν μεταξύ τους και με άλλες έξυπνες συσκευές σχετικές με την υποδομή, και ανταλλάσσουν δεδομένα και υπηρεσίες. Το ιδιωτικό δίκτυο που σχεδιάστηκε, ασφαλίζει τις συναλλαγές που παράγονται από τα αυτοκίνητα, και στο δίκτυο αυτό ένα από τα είδη κόμβων που παίζουν σημαντικό ρόλο είναι τα road side units (RSUs), που

είναι μονάδες στην άκρη του δρόμου και λειτουργούν ως αναμεταδότες και επεξεργαστές για τα δεδομένα που ανταλλάσσονται.

Το μοντέλο που προτείνεται για τον μηχανισμό Proof of Accumulated Trust αφορά την δυναμική επιλογή των miners, με βάση την αλλαγή στα επίπεδα εμπιστοσύνης του κάθε κόμβου – miner. Στο μοντέλο υπολογίζονται τα επίπεδα εμπιστοσύνης με βάση την ορθότητα και τη νομιμότητα των συναλλαγών που ανταλλάχθηκαν και επιλέγονται τα πιο έμπιστα RSU για να δράσουν ως miners. Εφαρμόζεται επίσης ένας μηχανισμός πλεονασμού, για την ανίχνευση απειλών σε ένα ή περισσότερα οχήματα ή RSU. Ορισμένα αξιόπιστα και μη RSU συμμετέχουν στην ανταλλαγή πολλαπλών αντιγράφων κάθε συναλλαγής. Αν έστω και ένας κόμβος που συμμετέχει στην ανταλλαγή αυτή είναι εκτεθειμένος σε κάποιον επιτιθέμενο, τότε η επίθεση θα ανιχνευτεί.

Προκειμένου ένας κόμβος RSU να επιλεγεί ως έμπιστος κόμβος (Trusted Node – TN), πρέπει να πληροί δύο προϋποθέσεις: α) να έχει συσσωρεύσει ένα συνολικό ποσό πόντων εμπιστοσύνης (trust points) μεγαλύτερο από ένα κατώφλι για μια συγκεκριμένη περίοδο, και β) να έχει συσσωρεύσει ένα πλήθος πόντων εμπιστοσύνης μεγαλύτερο από ένα μικρότερο κατώφλι για κάθε υποπερίοδο της περιόδου για την προϋπόθεση (α) – αυτό εξασφαλίζει τη νομιμότητα του RSU σε κάθε υποπερίοδο. Κάθε RSU κόμβος κερδίζει πόντους εμπιστοσύνης συμμετέχοντας σε νόμιμες και αληθείς λειτουργίες, και χάνει πόντους εμπιστοσύνης συμμετέχοντας σε κακόβουλες ενέργειες.

Μια περαιτέρω τροποποίηση του μηχανισμού Proof of Accumulated Trust από την ίδια ομάδα ερευνητών, είναι ο Parallel Multi-Miner Proof of Accumulated Trust (PROACT) [107], και όπως υποδηλώνει η πλήρης ονομασία του, επιτρέπει παράλληλη επεξεργασία του blockchain. Βρίσκει εφαρμογή σε δίκτυα Internet of Drones (IoD), όπου οι υπολογιστικοί πόροι των drones είναι περιορισμένοι, και χρησιμοποιούνται σε λύσεις που είναι ευαίσθητες σε καθυστερήσεις και λειτουργούν σε πραγματικό χρόνο. Έτσι αποκτά βαρύνουσα σημασία η γρήγορη ένταξη μιας συναλλαγής δεδομένων στο blockchain. Το PROACT προτείνεται ως παραλλαγή του PoAT και επιτρέπει πολλαπλούς κόμβους miners να παράγουν τα block τους παράλληλα και να τα προσθέτουν στο δίκτυο με βάση έναν κόμβο που ονομάζεται Block Orderer που συντονίζει τη σειρά τους.

Κεφάλαιο 5. Σύγκριση και Αξιολόγηση

Στην παρούσα εργασία, στόχος είναι η σύγκριση και αξιολόγηση των εναλλακτικών αυτών μηχανισμών συναίνεσης που έχουν ως βάση τα μοντέλα εμπιστοσύνης και φήμης ή κύρους. Έγινε μελέτη της σχετικής βιβλιογραφίας σχετικά με δίκτυα blockchain, τους μηχανισμούς συναίνεσης που χρησιμοποιούνται, και έπειτα έγινε εμβάθυνση στους μηχανισμούς συναίνεσης που βασίζονται στην εμπιστοσύνη και τη φήμη. Έγινε εξερεύνηση της βιβλιογραφίας αρχικά από συγκεντρωτικές και συγκριτικές δημοσιεύσεις και η ανακάλυψη περαιτέρω μεθόδων έγινε μέσω αναζήτησης και εξερεύνηση των αναφορών των μελετημένων εργασιών. Έχει μελετηθεί η βιβλιογραφία των τελευταίων ετών (μέχρι και το μέσο του 2023) και έχουν παρατεθεί συνολικά 15 μηχανισμοί συναίνεσης σχετικοί με την εμπιστοσύνη και το κύρος, οι οποίοι χωρίστηκαν σε δύο κατηγορίες, με βάση την έμφασή τους στην εκάστοτε έννοια, εμπιστοσύνης ή κύρους. Η επιλογή τους έγινε με βάση την μεθοδολογία που χρησιμοποιούν, και έγινε επίσης φιλτράρισμα με βάση την ποιότητα των δημοσιεύσεων. Για παράδειγμα, αποφεύγουμε την χρήση δημοσιεύσεων όπου δεν έχει γίνει ανάλυση της προτεινόμενης μεθόδου που παρουσιάζεται. Κατά την συγγραφή της εργασίας έγινε επίσης αναθεώρηση ορισμένων αναφορών που είχαν προηγουμένως χρησιμοποιηθεί, και είτε αφαιρέθηκαν, ή έγινε αντικατάστασή τους με ποιοτικότερες δημοσιεύσεις.

Στο κεφάλαιο αυτό, εκτελούμε μια αξιολόγηση των μηχανισμών αυτών και μια σύγκριση μεταξύ τους, έχοντας ως βάση τον μηχανισμό Proof of Work.

5.1. Επιλογή Κριτηρίων

Για την ανάλυση των μεθόδων, θα εστιάσουμε στην αξιολόγησή τους με βάση ορισμένα από τα κριτήρια που έχουμε στη διάθεσή μας. Ενώ στην βιβλιογραφία οι μηχανισμοί αναλύονται με διάφορους επιπλέον γνώμονες, όπως η ασφάλεια, η δικαιοσύνη, η κατανάλωση ενέργειας, η οριστικότητα των συναλλαγών, εστιάσαμε στα πιο κοινά χαρακτηριστικά που εφαρμόζονται σε όλους τους τύπους μηχανισμών συναίνεσης, παρά τις ιδιαιτερότητές τους. Επιλέγουμε λοιπόν τα κριτήρια της απόδοσης και της επεκτασιμότητας για την αξιολόγησή μας:

- Απόδοση (Throughput): Η απόδοση συμπεριλαμβάνει τόσο την διαδικασία επικύρωσης ενός block όσο και την διαδικασία τοποθέτησης αυτού στο blockchain. Ως σύνολο, μπορεί να υπολογιστεί με τον αριθμό συναλλαγών που επεξεργάζονται στο δίκτυο ανά δευτερόλεπτο (Transactions per second – TPS)

- Επεκτασιμότητα (Scalability): Η μετρική αυτή αναφέρεται στη δυνατότητα ενός δικτύου blockchain να υποστηρίζει ένα μεγάλο σύνολο από χρήστες και δεδομένα. Ένας μηχανισμός συναίνεσης με υψηλή επεκτασιμότητα έχει το χαρακτηριστικό πως η γενική επίδοσή του δεν επηρεάζεται από την προσθήκη νέων κόμβων.

Με βάση τα κριτήρια αυτά, παρουσιάζουμε στον ακόλουθο πίνακα μια συνοπτική σύγκριση των μηχανισμών συναίνεσης που παρατέθηκαν στο προηγούμενο κεφάλαιο, οι οποίοι εστιάζουν στη χρήση μηχανισμών εμπιστοσύνης και κύρους. Να σημειωθεί πως ο χαρακτηρισμός σε κάθε κριτήριο για τους διαφορετικούς μηχανισμούς προκύπτει από τις μελέτες των αντίστοιχων δημοσιεύσεων.

Μηχανισμός Συναίνεσης	Απόδοση (TPS)	Επεκτασιμότητα
Proof of Authority	Υψηλή	Υψηλή
Proof of Reputation	Υψηλή	Υψηλή
Proof of Reputation-X	Εξάρτηση από PoX	Εξάρτηση από PoX
Proof of X-Repute	Εξάρτηση από PoX	Εξάρτηση από PoX
Fair Proof of Reputation	Υψηλή	Υψηλή
Proof of Importance	Πολύ Υψηλή	Υψηλή
RepuCoin	Πολύ Υψηλή	Υψηλή
Proof of Trust	Υψηλή	Υψηλή
TrustChain	Πολύ Υψηλή	Πολύ Υψηλή
Proof of Random Trust	Υψηλή	Υψηλή
Proof of Accumulated Trust	Υψηλή	Υψηλή

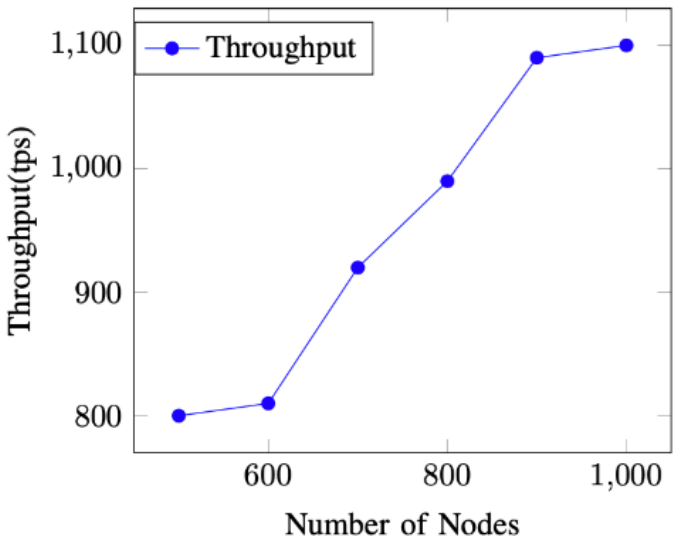
5.2. Σύγκριση μηχανισμών

5.2.1. Απόδοση

Για τον χαρακτηρισμό της απόδοσης ενός μηχανισμού συναίνεσης, χρησιμοποιούμε ως βάση σύγκρισης τον μηχανισμό Proof of Work, ο οποίος, αν και ο πιο δημοφιλής μηχανισμός, παρουσιάζει χαμηλή απόδοση όσον αφορά το συνολικό πλήθος συναλλαγών ανά δευτερόλεπτο. Αν ένας μηχανισμός συναίνεσης μετριέται να έχει σημαντικά μεγαλύτερο αριθμό συναλλαγών ανά δευτερόλεπτο (TPS) από το Proof of Work, το χαρακτηρίζουμε ως υψηλής απόδοσης, ενώ αν παρουσιάζει παρόμοιο TPS τον χαρακτηρίζουμε ως χαμηλής απόδοσης.

Ο μηχανισμός Proof of Authority θεωρείται συνδυασμός των πρωτοκόλλων Proof of Work και Proof of Stake, με τέτοιο τρόπο που δεν απαιτεί μεγάλα ποσά από υπολογιστική ισχύ. Η ανάλυση της απόδοσης του μηχανισμού αυτού δεν πραγματοποιείται στην αρχική δημοσίευση, αλλά η δημοσίευση των De Angelis κ.ά. [108] προχωρά στην σύγκριση με το PBFT και αξιολογούνται με βάση το θεώρημα CAP. Στην ανάλυσή τους, επισημαίνεται πως η δομή του αλγορίθμου δεν χρειάζεται την υπολογιστική ισχύ του Proof of Work, αλλά εξαρτάται από τους γύρους που χρειάζεται να ολοκληρωθούν για να επιτευχθεί η συναίνεση. Η μειωμένη ανάγκη για υπολογιστική ισχύ προκύπτει από τους λιγότερους κόμβους στο δίκτυο που εκτελούν την διαδικασία της επικύρωσης και της συναίνεσης. Έτσι, μπορεί να πετύχει απόδοση μεγαλύτερη σε σύγκριση με το πρωτόκολλο Proof of Work.

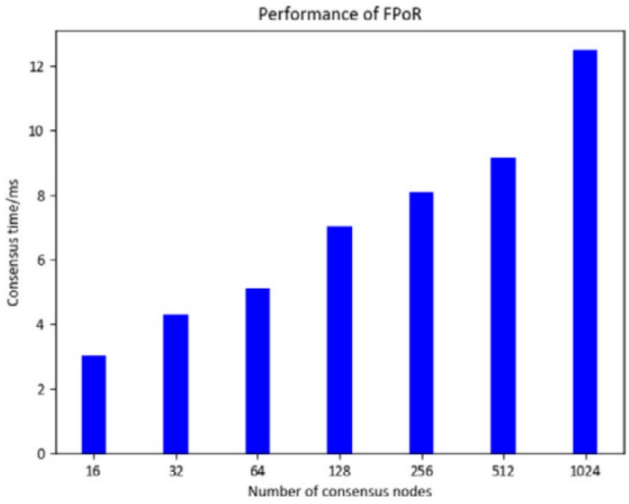
Η απόδοση του μηχανισμού Proof of Reputation ποικίλει, κυρίως με βάση το μέγεθος του block, το οποίο μπορεί να κυμαίνεται ανάμεσα σε 200 και 1000 συναλλαγές ανά block, για δίκτυα μεγέθους από 100 έως 500 κόμβους. Η απόδοση του δικτύου παρουσιάζει μια αναλογία με το μέγεθος του δικτύου, δηλαδή τους συμμετέχοντες σε αυτό. Αυτή η αναλογική αύξηση οφείλεται στο γεγονός ότι τα μπλοκ μεγαλύτερου μεγέθους μπορούν να υποστηρίξουν μεγαλύτερο όγκο συναλλαγών, αλλά με το μειονέκτημα πως αυξάνεται αντίστοιχα ο χρόνος επεξεργασίας του κάθε μπλοκ. Οι υπεύθυνοι ερευνητές πίσω από το Proof of Reputation σε αντίστοιχες προσομοιώσεις με δίκτυα με χιλιάδες κόμβους, πέτυχαν ένα πλήθος επεξεργασμένων συναλλαγών ανά δευτερόλεπτο στην τάξη των χιλιάδων (>1000 TPS). Αυτό το μέγεθος ξεπερνά κατά πολύ το αντίστοιχο TPS του μηχανισμού Proof of Work, που κυμαίνεται ανάμεσα σε 7 και 15 TPS.



Εικόνα 10: Απόδοση Proof of Reputation συναρτήσει του πλήθους των κόμβων [94]

Τα σχετιζόμενα πρωτόκολλα με το Proof of Reputation, τα Proof of Reputation-X (PoRx) και Proof of X-Repute (PoXR), εισάγουν ένα μηχανισμό φήμης στην αρχιτεκτονική ενός ήδη υπάρχοντος μηχανισμού Proof of X, ο οποίος επηρεάζει την δυσκολία εξόρυξης για τον κάθε μηχανισμό. Η απόδοσή τους λοιπόν είναι δυσκολότερο να καθοριστεί, καθώς εξαρτάται από τον αντίστοιχο μηχανισμό συναίνεσης Proof of X που χρησιμοποιείται. Παρόμοια αποτελέσματα εμφανίζει και ο μηχανισμός Permissionless Proof of Reputation – X (PL-PoRX), με μια πιθανή αύξηση της απόδοσης λόγω της χαμηλότερης πιθανότητας εμφάνισης block στο δίκτυο από κακόβουλους χρήστες, μειώνοντας έτσι τον χρόνο που ξοδεύεται άσκοπα για την διαδικασία της επικύρωσης. Αντίστοιχα στον υβριδικό μηχανισμό συναίνεσης PoR/PoS, αξιοποιούνται τα οφέλη στην απόδοση και των δύο μηχανισμών, με αποτέλεσμα την συνολικά υψηλή απόδοση του μηχανισμού.

Στον μηχανισμό συναίνεσης Fair Proof of Reputation (FPoR) οι ερευνητές εφαρμόζουν μια λύση που συνδυάζει τον μηχανισμό Proof of Reputation με το PBFT, με στόχο να αυξήσουν την δικαιοσύνη της διαδικασίας, αλλά εφαρμόζοντας αντίστοιχα ένα κόστος στην απόδοση. Συγκρίνουν την απόδοση του προτεινόμενου μηχανισμού με την απόδοση του PBFT, και παρουσιάζουν σημαντική βελτίωση. Η απόδοση παρουσιάζει επίσης παρόμοια χαρακτηριστικά με τον βασικό μηχανισμό Proof of Reputation, όπου ο χρόνος για να επιτευχθεί η συναίνεση αυξάνεται με την προσθήκη περισσότερων κόμβων, αλλά η χρήση block μεγαλύτερου μεγέθους αντισταθμίζει το κόστος αυτό.

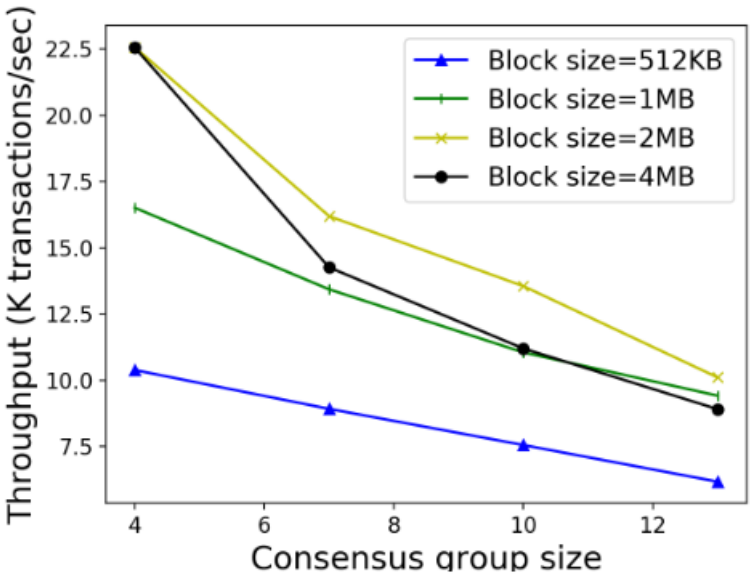


Εικόνα 11: Χρόνος επίτευξης συναίνεσης για το FPoR, συναρτήσει του πλήθους των κόμβων συναίνεσης [99]

Ο μηχανισμός Proof of Importance που χρησιμοποιείται στο δίκτυο NEM, έχει ως βάση τον μηχανισμό Proof of Stake μαζί με έναν μηχανισμό που υπολογίζει έναν βαθμό σπουδαιότητας ανά κόμβο και αντιστοιχεί στην φήμη του. Η ομοιότητα του

δικτύου με την αρχιτεκτονική του μηχανισμού Proof of Stake επιτρέπει την υψηλή απόδοση, και την επίτευξη μέχρι και 4000 TPS.

Στον μηχανισμό συναίνεσης RepuCoin, οι ερευνητές σε προσομοιώσεις δικτύων κατάφεραν να πετύχουν σημαντικά μεγάλο TPS (~10.000) σε πολλές παραμέτρους υπό διερεύνηση. Με την προσθήκη περισσότερων κόμβων στην ομάδα που εκτελεί την διαδικασία της συναίνεσης, ο χρόνος για την επίτευξη της συναίνεσης παρουσιάζει αύξηση, και έτσι μειώνεται η συνολική απόδοση του δικτύου.



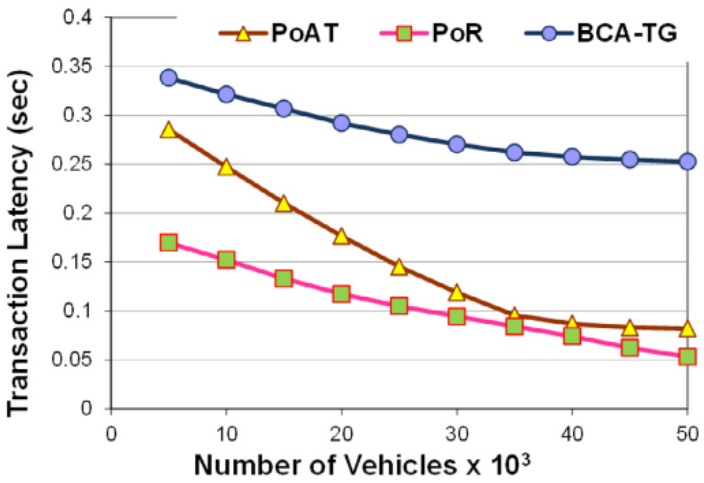
Εικόνα 12: Απόδοση του μηχανισμού RepuCoin συναρτήσει του μεγέθους της ομάδας συναίνεσης και του μεγέθους του block [101]

Στους μηχανισμούς που βασίζονται στην έννοια της εμπιστοσύνης, έχουμε τους μηχανισμούς Proof of Trust, που συναντώνται σε πολλαπλές υλοποιήσεις με την ίδια ονομασία. Από άποψη απόδοσης έχουν παρόμοια συμπεριφορά, καθώς μειώνουν την ανάγκη για δαπανηρούς υπολογισμούς όπως στο Proof of Work, και παρουσιάζουν σημαντική βελτίωση στην απόδοση. Πιο συγκεκριμένα, το Proof of Trust των Zou κ.ά. και η βελτιωμένη εκδοχή της από τους Zhu κ.ά. έχουν παρόμοια απόδοση μεταξύ τους, έχοντας υψηλή απόδοση, χωρίς να αναφέρονται ωστόσο αποτελέσματα σχετικά με τις τιμές TPS που επιτυγχάνουν. Αξίζει να σημειωθεί πως οι μηχανισμοί αυτοί βρίσκουν κυρίως χρήση σε ιδιωτικά δίκτυα με περιορισμένο πλήθος κόμβων και μπορούν να επιτύχουν υψηλές τιμές σε TPS. Το ίδιο ισχύει και για την υλοποίηση του μηχανισμού Proof of Trust από τους Bahri κ.ά.

Για τον μηχανισμό TrustChain του δικτύου COTI, λόγω του τρόπου υλοποίησης στον ακυκλικό γράφο, η ύπαρξη πολλαπλών αλυσίδων εμπιστοσύνης οδηγεί σε μια είδους παραλληλοποίηση στο δίκτυο. Αντίθετα με τις υπόλοιπες υλοποιήσεις που έχουμε μελετήσει μέχρι τώρα, ο μηχανισμός αυτός παρουσιάζει σημαντική επεκτασιμότητα, και ο αριθμός των συναλλαγών ανά δευτερόλεπτο στο δίκτυο μπορεί

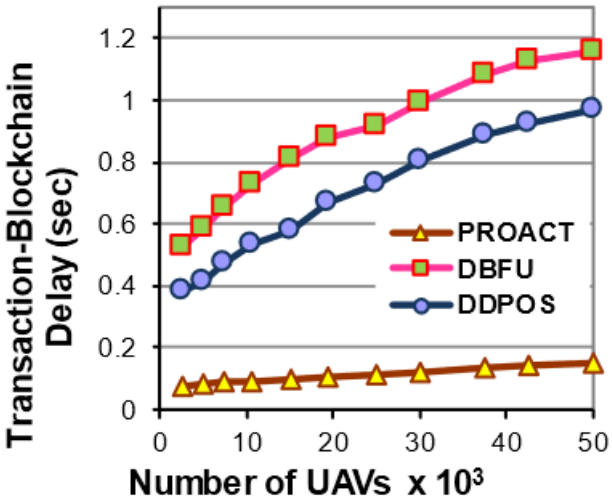
να αυξάνεται όσο συμμετέχουν περισσότεροι κόμβοι στο δίκτυο. Οι ερευνητές σε πειράματα προσομοίωσης είχαν απόδοση περίπου 1000 TPS, ενώ υποστηρίζουν πως το θεωρητικό όριο για την απόδοση του δικτύου είναι ο ρυθμός άφιξης συναλλαγών στο δίκτυο αυτό, με εκτιμήσεις για υποστήριξη άνω των 10,000 TPS.

Για τους μηχανισμούς Proof of Random Trust και Proof of Accumulated Trust που παρουσιάστηκαν στο κεφάλαιο 4, η βιβλιογραφία δεν αναφέρει στα πειραματικά αποτελέσματα την απόδοση μετρημένη σε TPS. Αναγράφονται, ωστόσο, τα αποτελέσματα μετρημένα σε Transaction Latency, δηλαδή τον χρόνο που χρειάζεται μια συναλλαγή για να ολοκληρωθεί – από την στιγμή που εκδίδεται μέχρι να γίνει οριστικοποιηθεί και να αποθηκευτεί στο δίκτυο. Μελετώντας σε προσομοιώσεις την απόδοση του Proof of Accumulated Trust υπό διαφορετικές παραμέτρους, μετρήθηκαν για παράδειγμα χρόνοι Transaction Latency από 0,3 έως 0,1 δευτερόλεπτα, με τις αντίστοιχες τιμές για το πρωτόκολλο Proof of Reputation με το οποίο έγινε σύγκριση να είναι μεταξύ 0,17 και 0,05 δευτερόλεπτα, όσο αυξανόταν το πλήθος των κόμβων στο δίκτυο. Αυτό τοποθετεί την απόδοση του PoAT σε παρόμοια, αλλά λίγο χαμηλότερα επίπεδα, με τον μηχανισμό Proof of Reputation.



Εικόνα 13: Transaction Latency του Proof of Accumulated Trust, συναρτήσει του πλήθους των κόμβων, σε σύγκριση με το Proof of Reputation [106]

Για τον μηχανισμό Parallel multi-miner proof of Accumulated Trust (PROACT) τα αποτελέσματα ήταν από την ίδια ομάδα ερευνητών και ήταν μια εναλλακτική και πιο αποδοτική υλοποίηση του μηχανισμού Proof of Accumulated Trust. Σε αντίστοιχες μετρικές για Transaction Latency, παρουσιάστηκαν πιο θετικά αποτελέσματα, με το latency να κυμαίνεται μεταξύ 0,14 και 0,07 δευτερόλεπτα, πλησιάζοντας περισσότερο στην απόδοση του μηχανισμού Proof of Reputation.



Εικόνα 14: Transaction Latency για τον μηχανισμό PROACT συναρτήσει του πλήθους των κόμβων [107]

5.2.2. Επεκτασιμότητα

Όπως και στην περίπτωση της μελέτης των μηχανισμών συναίνεσης με βάση την απόδοσή τους, αξιολογούμε την επεκτασιμότητά τους συγκρίνοντάς την με την αντίστοιχη επεκτασιμότητα του μηχανισμού συναίνεσης Proof of Work.

Ξεκινώντας με τον μηχανισμό συναίνεσης Proof of Authority, παρατηρούμε μια υψηλή επεκτασιμότητα, καθώς ο μηχανισμός βασίζεται σε ένα μικρότερο σύνολο κόμβων για να φτάσει σε συναίνεση. Η προσθήκη νέων κόμβων στο δίκτυο δεν επηρεάζει την γενική απόδοση του δικτύου.

Για τον μηχανισμό Proof of Reputation, όπως αναφέραμε και στην ανάλυση για την απόδοση, η προσθήκη περισσότερων κόμβων στο δίκτυο επηρεάζει θετικά την συνολική απόδοση του δικτύου, καθώς μειώνεται ο χρόνος που απαιτείται για να επιτευχθεί η συναίνεση. Ως αποτέλεσμα, όσο αυξάνεται το πλήθος συμμετεχόντων στο δίκτυο, μειώνεται ο χρόνος που απαιτείται για την παραγωγή ενός νέου μπλοκ. Έτσι μπορούμε να χαρακτηρίσουμε τον μηχανισμό Proof of Reputation ως μηχανισμό υψηλής επεκτασιμότητας. Για τους μηχανισμούς Proof of Reputation – X και Proof of X-Repute, ισχύουν οι ίδιες παρατηρήσεις με την απόδοσή τους. Η επεκτασιμότητά τους ακολουθεί παρόμοια συμπεριφορά με το υποκείμενο μηχανισμό Proof of X που χρησιμοποιούν. Η επέκταση του Proof of Reputation-X στην permissionless μορφή του, Permissionless Proof of Reputation-X, έχει επίσης παρόμοια χαρακτηριστικά με τον Proof of Reputation – X όσον αφορά την επεκτασιμότητά του, όμως η βελτίωση της permissionless μορφής του το καθιστά πιο ανοιχτό σε περισσότερους κόμβους.

Ο μηχανισμός Fair Proof of Reputation αποσκοπεί στο να πετύχει μια ισορροπία μεταξύ πολλαπλών χαρακτηριστικών, με κύριο γνώμονα την ασφάλεια και την δικαιοσύνη στην συμμετοχή των χρηστών. Στην δημοσίευσή τους οι ερευνητές συγκρίνουν την υλοποίησή τους με τον μηχανισμό PBFT και αναφέρουν βελτιωμένη επεκτασιμότητα, καθώς η διαδικασία της συναίνεσης εκτελείται από ένα μικρότερο

σύνολο κόμβων. Οι μηχανισμοί Proof of Importance και hybrid PoR/PoS παρουσιάζουν επίσης υψηλή επεκτασιμότητα, καθώς έχουν και οι δύο χαρακτηριστικά του μηχανισμού Proof of Stake, έναν μηχανισμό συναίνεσης που παρουσιάζει ήδη υψηλή επεκτασιμότητα.

Στον μηχανισμό συναίνεσης RepuCoin, όπως αναφέρθηκε και στην ενότητα για την αξιολόγηση της απόδοσης, η προσθήκη περισσότερων κόμβων στο δίκτυο βελτιώνει την απόδοση του δικτύου, και έτσι ο μηχανισμός RepuCoin μπορεί να χαρακτηριστεί σαν μηχανισμός συναίνεσης υψηλής επεκτασιμότητας.

Στους μηχανισμούς Proof of Trust έχουμε επίσης σχετικά υψηλή επεκτασιμότητα. Στην υλοποίηση των Zou κ.ά. η υβριδική αρχιτεκτονική του μηχανισμού επιτρέπει το μέγεθος του συνόλου των κόμβων που συμμετέχουν στη συναίνεση να παραμείνει σχετικά σταθερό, ακόμα και αν το πλήθος των κόμβων στο ανοιχτό μέρος του δικτύου αυξάνεται σημαντικά. Έτσι η απόδοση παραμένει σταθερή με την αύξηση της έκτασης του δικτύου, και έτσι χαρακτηρίζεται από υψηλή επεκτασιμότητα σε σύγκριση με άλλα πρωτόκολλα που χρησιμοποιούνται σε δίκτυα ιδιωτικά ή κοινοπραξίας. Στην υλοποίηση των Bahri κ.ά. δεν παρουσιάζονται αποτελέσματα σχετικά με την επεκτασιμότητα του μηχανισμού συναίνεσης. Ωστόσο, μπορούμε να αποφανθούμε ότι παρουσιάζει επίσης υψηλή επεκτασιμότητα, καθώς για την διαδικασία της συναίνεσης χρησιμοποιείται ένα υποσύνολο των κόμβων του δικτύου. Αυτό ενισχύεται επίσης από το γεγονός ότι η πληροφορία για τον γράφο εμπιστοσύνης που χρησιμοποιεί ο συγκεκριμένος μηχανισμός βρίσκεται κωδικοποιημένη μέσα στην αλυσίδα blockchain, και δεν υπάρχει κάποια κεντρική αρχή που να αποφασίζει σχετικά με τις τιμές εμπιστοσύνης των κόμβων.

Για τον μηχανισμό συναίνεσης Trustchain του δικτύου COTI έχουμε επίσης να αναφέρουμε την εξαιρετικά υψηλή επεκτασιμότητά του. Η αρχιτεκτονική του μηχανισμού που βασίζεται σε έναν κατευθυνόμενο ακυκλικό γράφο (DAG) εξυπηρετεί στην παράλληλη προσθήκη συναλλαγών στο δίκτυο, σε αντίθεση με την κλασική αρχιτεκτονική blockchain όπου νέο block μπορεί να προστεθεί μόνο στο τέλος της αλυσίδας.

Στον μηχανισμό Proof of Random Trust, πραγματοποιείται σύγκριση για τα χαρακτηριστικά του με τον παραδοσιακό αλγόριθμο BFT, όπου ο μηχανισμός Proof of Random Trust παρουσιάζει μεγαλύτερη επεκτασιμότητα. Με την αύξηση του πλήθους των κόμβων στο δίκτυο, το μέγεθος της ομάδας επαλήθευσης παραμένει σχετικά σταθερός. Έτσι η αύξηση των συμμετεχόντων στο δίκτυο δεν θα επηρεάσει την απόδοση του μηχανισμού συναίνεσης.

Τέλος, στον μηχανισμό Proof of Accumulated Trust έχουμε επίσης υψηλή επεκτασιμότητα. Σε πειραματικές προσομοιώσεις, η αύξηση των κόμβων στο δίκτυο είχε ως αποτέλεσμα σχετικά σταθερό χρόνο δημιουργίας ενός block, και το Transaction Latency παρουσίαζε μείωση. Ως αποτέλεσμα, μπορούμε να αποφανθούμε πως ο συγκεκριμένος μηχανισμός συναίνεσης παρουσιάζει υψηλή επεκτασιμότητα. Παρόμοια και μάλιστα ακόμα καλύτερη επεκτασιμότητα παρουσιάζει και ο μηχανισμός συναίνεσης PROACT, έχοντας ως πλεονέκτημα την παραλληλοποίηση των συναλλαγών στο δίκτυο.

Κεφάλαιο 6. Συμπεράσματα

Στόχος της παρούσας διπλωματικής εργασίας ήταν η διερεύνηση της βιβλιογραφίας σχετικά με τα δίκτυα blockchain και συγκεκριμένα ένα βασικό τμήμα της αρχιτεκτονικής τους, τον μηχανισμό συναίνεσης που χρησιμοποιούν. Έγινε μια παράθεση των πιο κοινών μηχανισμών που βρίσκονται υπό έρευνα τα τελευταία χρόνια και επίσης χρησιμοποιούνται σε πραγματικές υλοποιήσεις, και έπειτα η εστίαση της εργασίας ήταν σε μεθόδους που βασίζονται στην έννοια της εμπιστοσύνης και του κύρους ή της φήμης. Η προσέγγιση αυτή επιλέχθηκε ως μελέτη εναλλακτικών μεθόδων συναίνεσης σε σύγκριση με τις πιο κοινές.

Η επίτευξη συναίνεσης είναι καθοριστικής σημασίας για το σχηματισμό ενός αξιόπιστου κατανεμημένου δικτύου. Οι συμμετέχοντες πρέπει να συντονίζουν τις ενέργειές τους ώστε να πετύχουν κοινές αποφάσεις, και να έχουν συνέπεια στην κατάσταση τους, και το σύστημα να συνεχίζει παρά τα σφάλματα. Οι μηχανισμοί συναίνεσης χρησιμοποιούνται για το σκοπό αυτό στα δίκτυα blockchain. Όταν στα ιδιωτικά ή τα υβριδικά δίκτυα υπάρχει ένα μικρό σύνολο από κόμβους που συμμετέχει στη διαδικασία συναίνεσης, υπάρχει και ο κίνδυνος παραβίασης από κακόβουλους συμμετέχοντες. Το πρόβλημα αυτό επιχειρούν να λύσουν οι μηχανισμοί συναίνεσης που βασίζονται στην εμπιστοσύνη, καθώς αυτοί οι μηχανισμοί μεταξύ άλλων πιστοποιούν την αξιοπιστία του κάθε κόμβου.

Από την έρευνα αυτή, προέκυψαν ορισμένες μέθοδοι οι οποίες βρίσκουν ήδη χρήση σε δίκτυα όλων των ειδών, από ιδιωτικά μέχρι και δημόσια. Συγκεκριμένα, τα πρωτόκολλα Proof of Reputation και Proof of Trust, όσο και οι παραλλαγές τους, θεωρούνται υποσχόμενα πρωτόκολλα τα οποία βρίσκουν και πρακτική εφαρμογή σε διαφορετικά πεδία. Στα κυριότερα κοινά πλεονεκτήματα των μεθόδων αυτών σε σύγκριση με τις συμβατικές μεθόδους, μπορούμε να καταλογίσουμε την χαμηλότερη υπολογιστική ισχύ που απαιτούν συνολικά, και την λύση του προβλήματος αξιοπιστίας των κόμβων στα δίκτυα όπου συμμετέχουν.

Πραγματοποιήθηκε μια σύγκριση και αξιολόγηση των μεθόδων αυτών, έχοντας ως γνώμονα τα κριτήρια της απόδοσης και της επεκτασιμότητας των δικτύων όπου βρίσκουν χρήση τα αντίστοιχα πρωτόκολλα συναίνεσης. Με βάση τα κριτήρια αυτά, η πλειονότητα των μεθόδων συναίνεσης παρουσιάζουν ενθαρρυντικά αποτελέσματα, ενώ και κατά την μελέτη των μεθόδων παρατηρήθηκε και η χρησιμότητα των μεθόδων στην αντιμετώπιση επιθέσεων στα δίκτυα όπου εφαρμόζονται. Θα πρέπει να τονίσουμε, ωστόσο, πως η πλειονότητα των μεθόδων που συγκρίθηκαν, λόγω της φύσης τους, είναι περισσότερο συμβατές για χρήση σε πιο κλειστά δίκτυα, κυρίως

ιδιωτικά και υβριδικά. Ενδιαφέρον παρουσιάζουν οι ακόλουθοι μηχανισμοί: (α) Permissionless Proof of Reputation-X, ως μηχανισμός συναίνεσης που χρησιμοποιεί μοντέλο φήμης και μηχανισμό για χρήση σε δημόσιο permissionless δίκτυο, (β) Trustchain, ως μηχανισμός που παρουσιάζει εξαιρετικά υψηλή απόδοση και εισάγει σε πολλαπλά σημεία της αρχιτεκτονικής την έννοια της εμπιστοσύνης, αν και βασίζεται σε DAG αντί για blockchain.

Ως μελλοντική εργασία, θα μπορούσε να γίνει περαιτέρω ανάλυση των σύγχρονων μηχανισμών συναίνεσης που έχουν ως βάση μηχανισμούς φήμης και κύρους, και έχουν αναφερθεί στην παρούσα εργασία, αλλά και τους αντίστοιχους μηχανισμούς αυτής της κατηγορίας που θα έχουν εμφανιστεί μετά τη συγγραφή της, με περισσότερα κριτήρια. Ένα από τα βασικά κριτήρια για αξιολόγηση είναι η ασφάλεια των μηχανισμών, δηλαδή το πόσο ανθεκτικά είναι σε διαφορετικούς τύπους επιθέσεων. Επιπλέον κριτήρια που μπορούν να χρησιμοποιηθούν είναι η ενεργειακή κατανάλωση των μηχανισμών, και η οριστικότητα των συναλλαγών μέσα σε αυτό. Μια επίσης πιθανή επέκταση της παρούσας εργασίας, θα ήταν και η αποτίμηση της απόδοσης των μηχανισμών όπου δεν υπήρχαν ξεκάθαρα πειραματικά αποτελέσματα, με στόχο τη καταγραφή και δημοσίευση της απόδοσής τους, ως κριτήριο επιλογής από το κοινό, αν ενδιαφέρεται να χρησιμοποιήσει ένα δίκτυο που βασίζεται σε μηχανισμούς φήμης και κύρους, αλλά έχει και ως γνώμονα την υψηλή απόδοσή του.

Κεφάλαιο 7. Βιβλιογραφία - Αναφορές

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” p. 9, 2008.

[2] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, “A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services,” *IEEE Transactions on Services Computing*, vol. 12, no. 3, pp. 429–445, May 2019, doi: 10.1109/TSC.2018.2823705.

[3] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, “Blockchain consensus: An overview of alternative protocols,” *Symmetry*, vol. 13, no. 8, pp. 1–35, 2021, doi: 10/gnz453.

[4] N. Alzahrani and N. Bulusu, “Towards True Decentralization: A Blockchain Consensus Protocol Based on Game Theory and Randomness,” in *GameSec*, 2018. doi: 10/gnz5np.

[5] S. Sharkey and H. Tewari, “Alt-PoW: An Alternative Proof-of-Work Mechanism,” in *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, Newark, CA, USA: IEEE, Apr. 2019, pp. 11–18. doi: 10/ggjkjs.

[6] A. Back, “Hashcash - A Denial of Service Counter-Measure,” p. 10.

[7] N. Luhmann, “Trust: A mechanism for the reduction of social complexity,” in *Trust and Power*, 1979, pp. 4–103.

[8] D. Gambetta, “Can We Trust Trust? Diego Gambetta,” Aug. 2000.

[9] B. P. Bailey, L. J. Gurak, and J. A. Konstan, “Trust in Cyberspace,” in *Human Factors and Web Development*, 2nd ed.CRC Press, 2002.

[10] M. J. Gallivan, “Striking a balance between trust and control in a virtual organization: a content analysis of open source software case studies,” *Inform Syst J*, vol. 11, no. 4, pp. 277–304, Oct. 2001, doi: 10/dq7z7b.

[11] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, “Reputation systems,” *Commun. ACM*, vol. 43, no. 12, pp. 45–48, Dec. 2000, doi: 10/c7973b.

[12] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” *Applied Innovation*, vol. 2, no. 6–10, p. 71, 2016.

[13] S. Ølnes, J. Ubacht, and M. Janssen, “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,” *Government Information Quarterly*, vol. 34, no. 3, pp. 355–364, Sep. 2017, doi: 10/gcsjtt.

[14] J. L. Zhao, S. Fan, and J. Yan, “Overview of business innovations and research opportunities in blockchain and introduction to the special issue,” *Financ Innov*, vol. 2, no. 1, Art. no. 1, Dec. 2016, doi: 10/gfkn4d.

[15] C. Burger, J. Weinmann, A. Kuhlmann, and P. Richard, “Blockchain in the energy transition. A survey among decision-makers in the German energy industry,” Nov. 2016.

[16] S. Lavrijssen and A. Carrilo, “Radical Innovation in the Energy Sector and the Impact on Regulation,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2979206, Jun. 2017. doi: 10.2139/ssrn.2979206.

[17] M. Iansiti and K. R. Lakhani, “The truth about blockchain,” *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, Feb. 2017.

[18] K. Korpela, J. Hallikas, and T. Dahlberg, “Digital Supply Chain Transformation toward Blockchain Integration,” Jan. 2017. doi: 10/gfwwpf.

[19] F. Tian, “An agri-food supply chain traceability system for China based on RFID amp; blockchain technology,” in *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, Jun. 2016, pp. 1–6. doi: 10/gf4v66.

[20] Rethink Music, “Fair Music: Transparency and payment flows in the music industry,” Berklee Institute of Creative Entrepreneurship, Jul. 2015.

[21] M. Hoy, “An Introduction to the Blockchain and Its Implications for Libraries and Medicine,” *Medical Reference Services Quarterly*, vol. 36, pp. 273–279, Jul. 2017, doi: 10/gfzc5z.

[22] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. O'Reilly Media, Inc., 2015.
[23] G. Zyskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, San Jose, CA: IEEE, May 2015, pp. 180–184. doi: 10.1109/SPW.2015.27.
[24] R. C. Merkle, "Protocols for Public Key Cryptosystems," in *1980 IEEE Symposium on Security and Privacy*, Apr. 1980, pp. 122–122. doi: 10.1109/SP.1980.10006.
[25] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pp. 557–564, Sep. 2017, doi: 10/gfgs7b.
[26] "On Public and Private Blockchains," *Ethereum Foundation Blog*. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains (accessed Apr. 26, 2023).
[27] A. Arabo, I. Brown, and F. El-Mousa, "Privacy in the Age of Mobility and Smart Devices in Smart Homes," Sep. 2012, doi: 10.1109/SocialCom-PASSAT.2012.108.
[28] D. Groshoff, "Kickstarter My Heart: Extraordinary Popular Delusions and the Madness of Crowdfunding Constraints and Bitcoin Bubbles," *William & Mary Business Law Review*, vol. 5, no. 2, p. 489, Apr. 2014.
[29] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," 2016. Accessed: Apr. 25, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Architecture-of-the-Hyperledger-Blockchain-Fabric-Cachin/f852c5f3fe649f8a17ded391df0796677a59927f
[30] A. S. M. Irwin and G. Milad, "The use of crypto-currencies in funding violent jihad," *Journal of Money Laundering Control*, vol. 19, no. 4, pp. 407–425, Jan. 2016, doi: 10.1108/JMLC-01-2016-0003.
[31] "Hyperledger – Open Source Blockchain Technologies." https://www.hyperledger.org/ (accessed Apr. 25, 2023).
[32] "Consortium Chain Development," *GitHub*. https://github.com/ethereum/wiki/wiki/Consortium-Chain-Development (accessed Apr. 25, 2023).
[33] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of Empowered IoT Users," in *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Apr. 2016, pp. 13–24. doi: 10.1109/IoTDI.2015.39.
[34] C. Fromknecht, D. Velicanu, and S. Yakoubov, "A Decentralized Public Key Infrastructure with Identity Retention," *IACR Cryptol. ePrint Arch.*, 2014, Accessed: Apr. 26, 2023. [Online]. Available: https://www.semanticscholar.org/paper/A-Decentralized-Public-Key-Infrastructure-with-Fromknecht-Velicanu/57855fea0eea38a503ae58cbb024a2606002f677
[35] B. Chase and E. MacBrough, "Analysis of the XRP Ledger Consensus Protocol." arXiv, Feb. 20, 2018. doi: 10.48550/arXiv.1802.07242.
[36] K. Croman *et al.*, "On Scaling Decentralized Blockchains: (A Position Paper)," in *Financial Cryptography and Data Security*, J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds., in Lecture Notes in Computer Science, vol. 9604. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 106–125. doi: 10.1007/978-3-662-53357-4_8.
[37] "Cambridge Bitcoin Electricity Consumption Index (CBECI)." https://ccaf.io/cbnsi/cbeci (accessed Apr. 30, 2023).
[38] K. Lewison and F. Corella, "Backing Rich Credentials with a Blockchain PKI".

[39] F. Bolici and S. Rosa, “Mt.Gox Is Dead, Long Live Bitcoin!: Analysis of the Rise and Fall of a Leading Virtual Currency Exchange Platform,” vol. 11, pp. 285–296, Oct. 2016, doi: 10.1007/978-3-319-23784-8_22.
[40] M. Baldi, F. Chiaraluce, E. Frontoni, G. Gottardi, D. Sciarroni, and L. Spalazzi, “Certificate Validation Through Public Ledgers and Blockchains,” presented at the Italian Conference on Cybersecurity, 2017. Accessed: Apr. 30, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Certificate-Validation-Through-Public-Ledgers-and-Baldi-Chiaraluce/f4d18995b0b3d76992bccfc761bb0be272cc987c
[41] “Project Ubin: Central Bank Digital Money using Distributed Ledger Technology.” https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin (accessed May 04, 2023).
[42] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982, doi: 10.1145/357172.357176.
[43] “An Effective Randomization Framework to POW Consensus Algorithm of Blockchain (RPoW),” *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, pp. 1793–1797, Aug. 2019, doi: 10.35940/ijeat.f8456.088619.
[44] S. King, “Primecoin: Cryptocurrency with Prime Number Proof-of-Work”.
[45] S. Sayeed and H. Marco-Gisbert, “Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack,” *Applied Sciences*, vol. 9, no. 9, Art. no. 9, Jan. 2019, doi: 10.3390/app9091788.
[46] “Komodo (Advanced Blockchain Technology, Focused On Freedom),” *Komodo Documentation*. https://docs.komodoplatform.com/whitepaper/introduction.html (accessed May 15, 2023).
[47] P. Vasin, “Blackcoin’s proof-of-stake protocol v2,” *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, vol. 71, 2014.
[48] S. King and S. Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,” 2012. Accessed: May 12, 2023. [Online]. Available: https://www.semanticscholar.org/paper/PPCoin%3A-Peer-to-Peer-Crypto-Currency-with-King-Nadal/0db38d32069f3341d34c35085dc009a85ba13c13
[49] E. Kapengut and B. Mizrach, “An Event Study of the Ethereum Transition to Proof-of-Stake.” arXiv, Feb. 28, 2023. doi: 10.48550/arXiv.2210.13655.
[50] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol,” in *Advances in Cryptology – CRYPTO 2017*, J. Katz and H. Shacham, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017, pp. 357–388. doi: 10.1007/978-3-319-63688-7_12.
[51] “Delegated Proof of Stake (DPOS) — BitShares Documentation documentation.” https://how.bitshares.works/en/master/technology/dpos.html (accessed May 13, 2023).
[52] “A New Election Algorithm for DPos Consensus Mechanism in Blockchain | IEEE Conference Publication | IEEE Xplore.” https://ieeexplore.ieee.org/document/8634684 (accessed May 15, 2023).
[53] T. Do, T. Nguyen, and H. Pham, “Delegated Proof of Reputation: a Novel Blockchain Consensus,” in *Proceedings of the 1st International Electronics Communication Conference*, in IECC ’19. New York, NY, USA: Association for Computing Machinery, Jul. 2019, pp. 90–98. doi: 10.1145/3343147.3343160.
[54] I. Grigg, “EOS-An Introduction,” 2017. Accessed: May 13, 2023. [Online]. Available: https://www.semanticscholar.org/paper/EOS-An-Introduction-Grigg/c7a922dffb06ee1a75e1a5527c557da21b3c1d90
[55] F. Schuh and D. Larimer, “BITSHARES 2.0: FINANCIAL SMART CONTRACT PLATFORM,” 2015. Accessed: May 13, 2023. [Online]. Available:

https://www.semanticscholar.org/paper/BITSHARES-2.0%3A-FINANCIAL-SMART-CONTRACT-PLATFORM-Schuh-Larimer/9d628b9c29d66bad1eebc0e197d1e64d7fcea824

[56] "LPoS consensus algorithm — Waves Enterprise master documentation." https://docs.wavesenterprise.com/en/1.1.2/how-the-platform-works/consensus/PoS.html (accessed May 15, 2023).

[57] M. Castro, "Practical Byzantine fault tolerance," 1999. https://www.semanticscholar.org/paper/Practical-Byzantine-fault-tolerance-Castro/8132164f0fad260a12733b9b09cacc5fff970530 (accessed May 13, 2023).

[58] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct. 2017, pp. 2567–2572. doi: 10.1109/SMC.2017.8123011.

[59] M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," in *Open Problems in Network Security*, J. Camenisch and D. Kesdoğan, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016, pp. 112–125. doi: 10.1007/978-3-319-39028-4_9.

[60] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The Honey Badger of BFT Protocols," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, in CCS '16. New York, NY, USA: Association for Computing Machinery, Oct. 2016, pp. 31–42. doi: 10.1145/2976749.2978399.

[61] neo-project, "Neo Documentation." https://docs.neo.org/v2/docs/en-us/basic/whitepaper.html (accessed May 16, 2023).

[62] I. Coelho, V. Coelho, P. Lin, and E. Zhang, "Community yellow paper: A technical specification for neo blockchain," *NeoResearch, March*, 2019.

[63] Y. Wang *et al.*, "Study of blockchains's consensus mechanism based on credit," *IEEE Access*, vol. 7, pp. 10224–10231, 2019, doi: 10.1109/ACCESS.2019.2891065.

[64] M. Lokhava *et al.*, "Fast and secure global payments with Stellar," in *Proceedings of the 27th ACM Symposium on Operating Systems Principles*, in SOSP '19. New York, NY, USA: Association for Computing Machinery, Oct. 2019, pp. 80–96. doi: 10.1145/3341301.3359636.

[65] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On Security Analysis of Proof-of-Elapsed-Time (PoET)," Oct. 2017, pp. 282–297. doi: 10.1007/978-3-319-69084-1_19.

[66] S. Bistarelli, C. Pannacci, and F. Santini, "CapBAC in Hyperledger Sawtooth," 2019, pp. 152–169. doi: 10.1007/978-3-030-22496-7_10.

[67] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "Distributed consensus protocols and algorithms," *Blockchain for Distributed Systems Security*, vol. 25, p. 40, 2019, doi: 10.1002/9781119519621.ch2.

[68] S. Bano *et al.*, "SoK: Consensus in the Age of Blockchains," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, in AFT '19. New York, NY, USA: Association for Computing Machinery, Oct. 2019, pp. 183–198. doi: 10.1145/3318041.3355458.

[69] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-Burn." 2019. Accessed: May 16, 2023. [Online]. Available: https://eprint.iacr.org/2019/1096

[70] "About Slimcoin." https://slimcoin.info/about/ (accessed May 16, 2023).

[71] R. Gennaro and M. Robshaw, Eds., *Advances in Cryptology -- CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, vol. 9216. in Lecture Notes in Computer Science, vol. 9216. Berlin, Heidelberg: Springer, 2015. doi: 10.1007/978-3-662-48000-7.

[72] L. Ren and S. Devadas, "Proof of Space from Stacked Expanders." 2016. Accessed: May 16, 2023. [Online]. Available: https://eprint.iacr.org/2016/333

[73] S. Park, A. Kwon, G. Fuchsbauer, P. Gaži, J. Alwen, and K. Pietrzak, “SpaceMint: A Cryptocurrency Based on Proofs of Space.” 2015. Accessed: May 16, 2023. [Online]. Available: https://eprint.iacr.org/2015/528

[74] H. Abusalah, J. Alwen, B. Cohen, D. Khilko, K. Pietrzak, and L. Reyzin, “Beyond Hellman’s Time-Memory Trade-Offs with Applications to Proofs of Space,” Nov. 2017, pp. 357–379. doi: 10.1007/978-3-319-70697-9_13.

[75] F. Hendrikx, K. Bubendorfer, and R. Chard, “Reputation systems: A survey and taxonomy,” *Journal of Parallel and Distributed Computing*, vol. 75, pp. 184–197, Jan. 2015, doi: 10.1016/j.jpdc.2014.08.004.

[76] A. Jøsang and R. Ismail, “The Beta Reputation System,” *In: Proceedings of the 15th Bled Conference on Electronic Commerce*, Jan. 2002.

[77] J. Weng, Z. Shen, C. Miao, A. Goh, and C. Leung, “Credibility: How Agents Can Handle Unfair Third-Party Testimonies in Computational Trust Models,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 9, pp. 1286–1298, Sep. 2010, doi: 10.1109/TKDE.2009.138.

[78] K. K. Bharadwaj and M. Y. H. Al-Shamri, “Fuzzy computational models for trust and reputation systems,” *Electronic Commerce Research and Applications*, vol. 8, no. 1, pp. 37–47, Jan. 2009, doi: 10.1016/j.elerap.2008.08.001.

[79] S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok, “Trusted P2P transactions with fuzzy reputation aggregation,” *IEEE Internet Computing*, vol. 9, no. 6, pp. 24–34, Nov. 2005, doi: 10.1109/MIC.2005.136.

[80] W. T. L. Teacy, M. Luck, A. Rogers, and N. R. Jennings, “An efficient and versatile approach to trust and reputation using hierarchical Bayesian modelling,” *Artificial Intelligence*, vol. 193, pp. 149–185, Dec. 2012, doi: 10.1016/j.artint.2012.09.001.

[81] M. Tavakolifard and S. J. Knapskog, “A Probabilistic Reputation Algorithm for Decentralized Multi-Agent Environments,” *Electronic Notes in Theoretical Computer Science*, vol. 244, pp. 139–149, Aug. 2009, doi: 10.1016/j.entcs.2009.07.043.

[82] A. Whitby and A. Jøsang, “Filtering Out Unfair Ratings in Bayesian Reputation Systems,” *The Icfain Journal of Management Research*, vol. 4, Jan. 2004.

[83] A. Josang, R. Hayward, and S. Pope, “Trust network analysis with subjective logic,” in *Conference Proceedings of the Twenty-Ninth Australasian Computer Science Conference (ACSW 2006)*, Australian Computer Society, 2006, pp. 85–94.

[84] A. Jøsang, *Subjective logic*, vol. 4. Springer, 2016.

[85] A. Jøsang and T. Bhuiyan, “Optimal trust network analysis with subjective logic,” in *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, IEEE, 2008, pp. 179–184.

[86] L. C. Freeman, “Centrality in social networks conceptual clarification,” *Social Networks*, vol. 1, no. 3, pp. 215–239, Jan. 1978, doi: 10.1016/0378-8733(78)90021-7.

[87] L. Kleinrock, R. Ostrovsky, and V. Zikas, “Proof-of-Reputation Blockchain with Nakamoto Fallback,” in *Progress in Cryptology – INDOCRYPT 2020*, K. Bhargavan, E. Oswald, and M. Prabhakaran, Eds., in Lecture Notes in Computer Science, vol. 12578. Cham: Springer International Publishing, 2020, pp. 16–38. doi: 10.1007/978-3-030-65277-7_2.

[88] J. Horton and J. Golden, “Reputation inflation in an online marketplace,” *New York I*, vol. 1, 2015.

[89] G. Swamynathan, K. C. Almeroth, and B. Y. Zhao, “The design of a reliable reputation system,” *Electronic Commerce Research*, vol. 10, pp. 239–270, 2010, doi: 10.1007/s10660-010-9064-y.

[90] K. Hoffman, D. Zage, and C. Nita-Rotaru, “A survey of attack and defense techniques for reputation systems,” *ACM Computing Surveys (CSUR)*, vol. 42, no. 1, pp. 1–31, 2009, doi: 10.1145/1592451.1592452.
[91] “POA Network Whitepaper,” *GitHub*. https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper (accessed May 15, 2023).
[92] S. Joshi, “Feasibility of proof of authority as a consensus protocol model,” *arXiv preprint arXiv:2109.02480*, 2021.
[93] M. Khan, A. Hassan, and Md. I. Ali, “Secured Insurance Framework Using Blockchain and Smart Contract,” *Scientific Programming*, vol. 2021, pp. 1–11, Nov. 2021, doi: 10.1155/2021/6787406.
[94] F. Gai, B. Wang, W. Deng, and W. Peng, “Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network,” in *Database Systems for Advanced Applications*, J. Pei, Y. Manolopoulos, S. Sadiq, and J. Li, Eds., in Lecture Notes in Computer Science, vol. 10828. Cham: Springer International Publishing, 2018, pp. 666–681. doi: 10.1007/978-3-319-91458-9_41.
[95] GoChain, “GoChain - 100% Ethereum Compatible, 100x faster,” *GoChain*. https://gochain.io/ (accessed May 20, 2023).
[96] E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan, “PoRX: A reputation incentive scheme for blockchain consensus of IIoT,” *Future Generation Computer Systems*, vol. 102, pp. 140–151, 2020, doi: 10.1016/j.future.2019.08.005.
[97] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. K. Khan, “Proof of X-repute blockchain consensus protocol for IoT systems,” *Computers & Security*, vol. 95, p. 101871, 2020, doi: 10.1016/j.cose.2020.101871.
[98] J. Bou Abdo, R. El Sibai, and J. Demerjian, “Permissionless proof-of-reputation-X: A hybrid reputation-based consensus algorithm for permissionless blockchains,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4148, 2021, doi: 10.1002/ett.4148.
[99] T. Zhang and Z. Huang, “FPoR: Fair proof-of-reputation consensus for blockchain,” *ICT Express*, vol. 9, no. 1, pp. 45–50, Feb. 2023, doi: 10.1016/j.icte.2022.11.007.
[100] “NEM XEM whitepapers - whitepaper.io.” https://whitepaper.io/document/583/nem-whitepaper (accessed May 13, 2023).
[101] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo, “RepuCoin: Your Reputation Is Your Power,” *IEEE Transactions on Computers*, vol. 68, no. 8, pp. 1225–1237, Aug. 2019, doi: 10.1109/TC.2019.2900648.
[102] X. Zhu, Y. Li, L. Fang, and P. Chen, “An Improved Proof-of-Trust Consensus Algorithm for Credible Crowdsourcing Blockchain Services,” *IEEE Access*, vol. 8, pp. 102177–102187, 2020, doi: 10.1109/ACCESS.2020.2998803.
[103] L. Bahri and S. Girdzijauskas, “When Trust Saves Energy: A Reference Framework for Proof of Trust (PoT) Blockchains,” Apr. 2018, pp. 1165–1169. doi: 10.1145/3184558.3191553.
[104] “The Trust Chain Consensus COTI : a decentralized , high performance cryptocurrency ecosystem,” 2018. Accessed: Jun. 05, 2023. [Online]. Available: https://www.semanticscholar.org/paper/The-Trust-Chain-Consensus-COTI-%3A-a-decentralized-%2C/9d4c0f029e4b11ecae9a397b20ddabf2dd45860f
[105] Y. Zhang, B. Yan, Y. Yao, and J. Yu, “Proof of Random Trust Consensus Mechanism for Power Resource Sharing System,” *Procedia Computer Science*, vol. 187, pp. 402–407, Jan. 2021, doi: 10.1016/j.procs.2021.04.079.
[106] K. Mershad, O. Cheikhrouhou, and L. Ismail, “Proof of accumulated trust: A new consensus protocol for the security of the IoV,” *Vehicular Communications*, vol. 32, p. 100392, Dec. 2021, doi: 10.1016/j.vehcom.2021.100392.

[107] K. Mershad, “PROACT: Parallel multi-miner proof of accumulated trust protocol for Internet of Drones,” *Vehicular Communications*, vol. 36, p. 100495, Aug. 2022, doi: 10.1016/j.vehcom.2022.100495.

[108] S. De Angelis, L. Aniello, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain,” Jan. 2017.