ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Μελέτη και Ανάλυση των Τεχνικών Συναίνεσης σε Δίκτυα Blockchain

Φοιτητής: Γεώργιος Φωκάς
ΑΜ: ene45468

Επιβλέπων Καθηγητής

Κόγιας Δημήτριος

Διδάσκων ΕΣΠΑ

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, Σεπτέμβριος 2020

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

Study and Analysis of Consensus Techniques in Blockchain Networks

Student: GEORGIOS FOKAS
Registration Number: ene45468

Supervisor

KOGIAS DIMITRIOS

ATHENS-EGALEO, September 2020

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

(Ονοματεπώνυμο), (βαθμίδα)	(Ονοματεπώνυμο), (βαθμίδα)	(Ονοματεπώνυμο), (βαθμίδα)
ΔΗΜΗΤΡΙΟΣ Γ. ΚΟΓΙΑΣ (Υπογραφή)	Digitally signed by Charalampos Patrikakis Date: 2021.04.12 11:35:39 +03'00' ΧΑΡΑΛΑΜΠΟΣ ΠΑΤΡΙΚΑΚΗΣ (Υπογραφή)	Periklis Papadopoulos Digitally signed by Periklis Papadopoulos Date: 2021.04.12 10:42:28 +03'00' ΠΕΡΙΚΛΗΣ ΠΑΠΑΔΟΠΟΥΛΟΣ (Υπογραφή)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Γεώργιος Φωκάς του Δημητρίου, με αριθμό μητρώου ene45468 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.
Δεν επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου έπειτα από αίτησή μου στη Βιβλιοθήκη και έγκριση του επιβλέποντος καθηγητή.»

Ο Δηλών
Γεώργιος Φωκάς

Ευχαριστίες

Η διπλωματική αυτή πραγματοποιήθηκε στην κατεύθυνση επικοινωνιών και δικτύων του τμήματος Ηλεκτρολόγων και Ηλεκτρονικών μηχανικών του Πανεπιστημίου Δυτικής Αττικής. Το θέμα αυτό επιλέχθηκε ύστερα από υπόδειξη και σε συνεργασία με τον Κύριο Δημήτριο Κόγια, οπού ήταν και ο επιβλέπων της διπλωματικής αυτής.
Οφείλω ένα μεγάλο ευχαριστώ στον Επιβλέπων καθηγητή μου, αρχικά για την ανάθεση της διπλωματικής αυτής αλλά και την βοήθεια που μου προσέφερε κατά την διεξαγωγή της.
Τέλος θέλω να ευχαριστήσω το προσωπικό του Πανεπιστημίου Δυτικής Αττικής για τις γνώσεις που μου παρείχαν στα χρόνια της φοίτησης μου.

Περίληψη

Σκοπός της διπλωματικής αυτής είναι η μελέτη και ανάλυση των βασικών και πιο διαδεδομένων μηχανισμών και τεχνικών συναίνεσης, μέσω βιβλιογραφικής έρευνας. Το Blockchain αποτελεί ένα κατανεμημένο σύστημα, αποτελούμενο από ομότιμους κόμβους, ασφαλές λόγω του αποκεντρωτικού χαρακτήρα του, της κρυπτογράφησης των δεδομένων καθώς και της χρήσης ψηφιακών υπογραφών που χρησιμοποιεί. Στον πυρήνα του έχει αποκεντρωτικό χαρακτήρα και λειτουργεί με βασικές αρχές όπως ανωνυμία και αμεταβλητότητα. Η τεχνολογία Blockchain έγινε γνωστό και περιζήτητο θέμα έρευνας για τον επιστημονικό τομέα αρχικά το 2008 μέσω της πλατφόρμας κρυπτο-νομισμάτων Bitcoin. Βασικό γνώρισμα της τεχνολογίας αυτής είναι οι μηχανισμοί και οι τεχνικές που πραγματοποιούνται ώστε να υπάρξει ομοφωνία στο σύστημα. Οι μηχανισμοί αυτοί αναλώνονται σε κανόνες και αλγοριθμικές διεργασίες που πρέπει να τηρούν οι συμμετέχοντες κόμβοι για ομαλή και αποδοτική λειτουργία σε ένα σύστημα Blockchain. Οι διεργασίες αυτές μεταξύ άλλων συνήθως αφορούν επίλυση πολύπλοκων μαθηματικών συναρτήσεων ή εκτέλεσης γύρων ψηφοφορίας ανάμεσα στους κόμβους, αναλόγως του μηχανισμού συναίνεσης που χρησιμοποιείται.

Λέξεις – Κλειδιά

Blockchain, κατανεμημένα συστήματα, Δίκτυα ομότιμων κόμβων, συγκεντρωτικά/αποκεντρικοποιημένα συστήματα, δημιουργία μπλοκ, κρυπτο-νομίσματα, μηχανισμοί συναίνεσης, κόμβος, χρόνος συναλλαγών, δημόσιο-ιδιωτικό κοινοπρακτικό, οριστικότητα συναλλαγών, αποδοτικότητα, μεταβλητότητα, εφαρμογές

Abstract

Blockchain technology became a well-known and sought-after research topic in the scientific field initially in 2008 through the Bitcoin cryptocurrency platform. Blockchain usually refers to a distributed system, consisting of peer nodes, secure due to data encryption, digital signature and distributed nature. At its core it has a decentralized character and operates with basic principles such as anonymity and immutability. This fact makes it an interesting candidate to act as a medium for conducting online transactions through cryptocurrencies or other applications in the wider context of technology (e.g. smart contracts). The key feature of this technology is the mechanisms and techniques that are taking place in order to have consensus in the system. These mechanisms are referred to the rules and algorithmic processes that must be followed by the participating nodes for the smooth and efficient operation in a Blockchain system. These processes, among other things, usually involve solving mathematical functions or performing voting rounds between nodes, depending on the consensus mechanism used. The purpose of this thesis is the study and analysis of the basic and most widespread mechanisms and techniques of consensus, through literature research.

Starting from Byzantine Generals problem, the necessity for the existence of a consensus mechanism in distributed environments is strongly depicted. To the end, we have studied some of the basic and most common consensus mechanisms such as PoW, PoS, PBFT, DPoS etc. which are analyzed. in terms of efficiency, security, finality and speed of transactions. Finally, the three basic types of Blockchain systems, Public-Private-Consortium, are studied in terms of the differences that govern them in characteristics such as decentralization/centralization rate, anonymity, request for permission to participate in the consensus algorithm, etc.

The results of the analysis of the consensus techniques and the systems were summarized in corresponding tables for easier reading of their most essential characteristics.

Keywords

Blockchain, distributed systems, Peer-to-peer networks, centralized / decentralized systems, blockchain, cryptocurrencies, consensus mechanisms, nodes, transaction time, , public-private consortium, transaction finality, efficiency, variability

Περιεχόμενα

1 ΕΙΣΑΓΩΓΗ

1.1 Αντικείμενο της Διπλωματικής εργασίας

Το αντικείμενο αυτής της εργασίας είναι η ανάλυση των διαφόρων τεχνικών συναίνεσης των δικτύων Blockchain μέσω της ευρύτερης ανάλυσης των χαρακτηριστικών του. Οι μηχανισμοί και τεχνικές συναίνεσης είναι βασικό κομμάτι της τεχνολογίας Blockchain. Είναι ο τρόπος με τον οποίο το δίκτυο καταφέρνει να έρθει σε ομοφωνία στην πλειοψηφία του και να λειτουργεί ομαλά. Ένας από τους πρώτους μηχανισμός συναίνεσης, το Proof of Work (PoW) χρησιμοποιήθηκε από την εφαρμογή Bitcoin. Το PoW χαρακτηρίζεται από τον αποκεντρωτικό του χαρακτήρα καθώς όλοι οι κόμβοι του συστήματος θεωρούνται ομότιμοι, ισάξιοι και δεν επιβλέπονται από κάποια κεντρική αρχή, όμως με το πέρασμα του χρόνου παρατηρήθηκε προσαρμογή τις τεχνολογίας σε άλλου είδους μηχανισμούς όπως π.χ. το Raft. Το Raft διαθέτει έναν ηγετικής φύσης μηχανισμό συναίνεσης (θα αναλυθεί σε παρακάτω υποενότητα) και σύστημα που δεν προάγει της αρχές της αποκεντρικοποίησης αφού για την λήψη αποφάσεων το σύστημα βασίζεται σε μία κεντρική ηγετική αρχή ή ηγετικό κόμβο. Πλέον, σήμερα παρατηρείται πληθώρα μηχανισμών συναίνεσης, ο καθένας με διαφορετικά χαρακτηριστικά τα οποία έχουν σκοπό να καλύψουν εφαρμογές ανάλογες των τύπων του συστήματος που χρησιμοποιείται αλλά και των αναγκών που απαιτούνται. Οι πιο διαδεδομένοι μηχανισμοί και τεχνικές θα αποτελέσουν το κύριο θέμα της παρούσας διπλωματικής εργασίας.

1.2 Μεθοδολογία

Για την συγγραφή της παρακάτω εργασίας πραγματοποιήθηκε βιβλιογραφική μελέτη κυρίως επιστημονικών άρθρων σχετικών του θέματος σε συνδυασμό με άντληση πληροφοριών από ηλεκτρονικές πηγές αλλά και βιβλία. Χρησιμοποιήθηκε μικρός αριθμός εικόνων για την περαιτέρω επεξήγηση συγκεκριμένων υποενοτήτων, οι οποίες αναφέρονται συνολικά στον πίνακα εικόνων. Τέλος έγινε η χρήση δύο πινάκων για την παρουσίαση των πιο βασικών και ουσιωδών χαρακτηριστικών των μηχανισμών που αναφέρθηκαν.

1.3 Δομή

Όσον αφορά την δομή της εργασίας στην 1η ενότητα έγινε μια εισαγωγή σχετικά με το αντικείμενο τις εργασίας. Στην συνέχεια στην 2η ενότητα αναλύθηκαν τα βασικά χαρακτηριστικά και γνωρίσματα των Blockchain δικτύων όπως τα κατανεμημένα δίκτυα, τα δίκτυα ομότιμων κόμβων. Στην 3η αναλύθηκαν χαρακτηριστικά όπως οι έννοιες τις αποκεντροποίησης και του συγκεντρωτισμού. Στην 4η αναφέρθηκε το γνωστό πρόβλημα των στρατηγών του Βυζαντινού στρατού το οποίο μας δείχνει την αναγκαιότητα ενός μηχανισμού συναίνεσης σε κατανεμημένα συστήματα. Έπειτα στην ίδια ενότητα αναλύθηκαν κάποιοι από τους βασικούς και πιο διαδεδομένους μηχανισμούς συναίνεσης όπως PoW, PoS, PBFT, DPoS κ.α. ως προς την αποδοτικότητα, ασφάλεια, οριστικότητα αλλά και ταχύτητα πραγματοποίησης συναλλαγών. Τέλος στην 5η έγινε μελέτη των τριών βασικών τύπων Blockchain συστημάτων, Δημόσια-Ιδιωτικά-Κοινοπρακτικά ως προς τις διαφορές που τα διέπουν σε χαρακτηριστικά όπως ποσοστό αποκεντρικοποίησης ή συγκεντρωτισμού, ανωνυμία, απαίτηση άδειας για συμμέτοχή στην διαδικασία του αλγορίθμου συναίνεσης κ.α.

Τα αποτελέσματα της ανάλυσης των τεχνικών συναίνεσης αλλά και των συστημάτων τοποθετήθηκαν περιληπτικά σε αντίστοιχους πίνακες για την ευκολότερη ανάγνωση των πιο ουσιωδών χαρακτηριστικών τους.

2 Βασικά χαρακτηριστικά των δικτύων Blockchain

2.1 Τεχνολογία κατανεμημένων κατάστιχων (Distributed ledger technology (DLT))

2.1.1 Ορισμός ενός κατανεμημένου κατάστιχου (Distributed Ledger)

Ένα κατανεμημένο κατάστιχο (DLT) είναι ένας τύπος βάσης δεδομένων που είναι κατανεμημένη σε όλη την έκταση ενός δικτύου η πολλών τοποθεσιών, και μπορει να είναι δημόσιο. Τα αρχεία που καταχωρούνται σε αυτήν την βάση αποθηκεύονται το ένα μετά το άλλο σε ένα βιβλίο η κατάστιχο (συνήθως παρομοιάζεται με λογιστικό φύλλο) και κάθε μέλος του δικτύου διαθέτει αντίγραφο ολόκληρου του κατάστιχου. [1]

Ακόμα πρέπει να σημειωθεί πως ένα DLT είναι ένας γενικός όρος για να περιγράψουμε μια διαμοιρασμένη βάση δεδομένων, και όπως θα δούμε παρακάτω το blockchain ανήκει σε αυτήν την κατηγορία των διαμοιρασμένων βάσεων δεδομένων ή κατανεμημένων κατάστιχων. Αν και όλα τα blockchain προέρχονται από ένα Distributed ledger, δεν είναι αναγκαίο πως ένα Distributed ledger είναι blockchain. [2]

Κύρια διαφορά των δύο είναι πως τα DLTs δεν περιέχουν αναγκαστικά blocks συναλλαγών για να μεγαλώνει το μέγεθος του κατάστιχου. Από την άλλη το blockchain είναι ένας ειδικός τύπος βάσης δεδομένων όπου αποτελείτε από blocks συναλλαγών.

Παράδειγμα του ότι ένα Distributed ledger δεν χρησιμοποιεί blocks συναλλαγών είναι το Distributed ledger της Corda [3]. Το Corda είναι σχεδιασμένο να καταγράφει και να διαχειρίζεται συναλλαγές και ειδικεύεται στις υπηρεσίες της οικονομικής βιομηχανίας. Από την άλλη οι πιο γνωστές εφαρμογές του Blockchain όπως το Bitcoin [4] και το Ethereum [5] χρησιμοποιούν τα blocks για να ενημερώνουν μια διαμοιρασμένη βάση δεδομένων για την κατάσταση, αυθεντικότητα και την σωστή χρονολογική σειρά των συναλλαγών που λαμβάνουν μέρος σε αυτήν την βάση.

2.1.2 Βασική αρχή λειτουργείας ενός κατανεμημένου κατάστιχου (Distributed Ledger)

Στην βασική της μορφή η DLT τεχνολογία εφαρμόζεται σε εφαρμογές του blockchain ως εξής:

- Πρώτον, η συμφωνία μεταξύ των μελών του δικτύου για την παρούσα κατάσταση του κατάστιχου επιτυγχάνεται μόνο μέσω κοινής συναίνεσης των μελών αυτού, παρά να βασίζονται σε ένα τρίτο ή μεσάζοντα.
- Δεύτερον, οι χρήστες μπορούν να ‘καταθέσουν’ ψηφιακά στοιχεία (όπως αρχεία και καταστάσεις) , τα οποία είναι αμετάβλητα αφού γίνουν κομμάτι του κατάστιχου, τα οποία επίσης είναι διαφανή και ελέγξιμα. Καταφέρνουν όμως να είναι ανθεκτικά στην αλλαγή και χειραγώγησή τους, λόγω της κρυπτογραφικής και κατανεμημένης φύσης των κατάστιχων.

Αφού οι συναλλαγές που καταγράφονται είναι πλέον αμετάβλητες, το σύστημα μπορεί να επιτρέψει ανωνυμία μεταξύ των συναλλασσόμενων μελών, καθιστώντας τις συναλλαγές ανθεκτικές σε παραβιάσεις, κάνοντας όμως των εντοπισμό μελών δύσκολο σε περίπτωση όπου αυτό είναι αναγκαίο.

2.2 Κατηγορίες Δικτύων

2.2.1 P2P μοντέλο

Ένα δίκτυο υπολογιστών peer-to-peer (ή P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα (χωρίς την βοήθεια κεντρικού διακομιστή). Το δίκτυο αυτό χωρίζει ισοδύναμα τις εργασίες η το φόρτο εργασίας στους κόμβους (μέλη του δικτύου). Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα. Αναφέρεται και ως δίκτυο ομότιμων κόμβων. [6]

Όλοι οι κόμβοι παρέχουν μέρος των πόρων τους, όπως υπολογιστική ισχύς, χώρος στο δίσκο ή εύρος ζώνης του δικτύου άμεσα σε οποιονδήποτε άλλον κόμβο χωρίς την ανάγκη κεντρικού συντονισμού από διακομιστές (servers) η σταθερούς υπολογιστές.

Οι κόμβοι είναι ταυτόχρονα καταναλωτές αλλά και προμηθευτές των πόρων σε αντίθεση με το μοντέλο πελάτη εξυπηρετητή(client-server),που βασίζεται σε έναν διακομιστή να διαιρεί το φόρτο εργασίας και να εξυπηρετεί τους κόμβους.

Τα δίκτυα peer to peer (P2P) ή δίκτυα ομότιμων κόμβων καθιερώθηκαν από την εφαρμογή Napster. Πρόκειται για μια εφαρμογή όπου μέσω της φιλοσοφίας των P2P δικτύων σκοπός ήταν ο διαμοιρασμός και ανταλλαγή αρχείων όπως συμπιεσμένων MPEG 3 audio αρχείων (γνωστό και ως MP3).Για την ακρίβεια η συγκεκριμένη εφαρμογή λειτουργούσε κάτω από Hybrid (Υβριδικό) P2P δίκτυο. [7]

2.2.1.1 Τοπολογία P2P δικτύων

Τα συστήματα ομότιμων κόμβων είναι κατανεμημένα συστήματα διασυνδεδεμένων κόμβων, ικανά να αυτό-οργανωθούν σε διάφορες τοπολογίες δικτύων με σκοπό να διαμοιράζονται πόρους χωρίς την βοήθεια κάποιου διακομιστή. [2]

Η τοπολογία ενός τέτοιου εικονικού δικτύου καθώς και οι μηχανισμοί δρομολόγησης του έχουν σημαντική επιρροή σε ιδιότητες εφαρμογής όπως απόδοση, λόγω της συνδυαζόμενης υπολογιστικής ισχύς, αξιοπιστία, διότι ακόμα και αν έναν κόμβος καταρρεύσει το δίκτυο δεν σταματά να λειτουργεί, απλά τα αρχεία που υπήρχαν στον κόμβο αυτό δεν θα είναι προσβάσιμα την στιγμή που κατέρρευσε και κάποιες περιπτώσεις ανωνυμία μέσω διαφόρων τεχνικών κρυπτογράφησης. [8]

2.2.2 Δίκτυα πελάτη-διακομιστή/εξυπηρετητή (Client-Server)

Ένα κατανεμημένο δίκτυο θεωρείται πως λειτουργεί με το μοντέλο Client-Server όταν αυτό απαρτίζεται από ένα υψηλής απόδοσης σύστημα ,τον Server (διακομιστή), και πολλά άλλα μικρότερης απόδοσης, τους clients (εξυπηρετητές) . Ο διακομιστής είναι η κεντρική μονάδα εγγραφής όπως και ο μόνος πάροχος περιεχομένου και υπηρεσιών. Ο εξυπηρετητής ζητά μόνο περιεχόμενο ή υπηρεσίες χωρίς να διαμοιράζεται τους πόρους του. [8]

2.2.2.1 Τοπολογία Client-Server μοντέλου

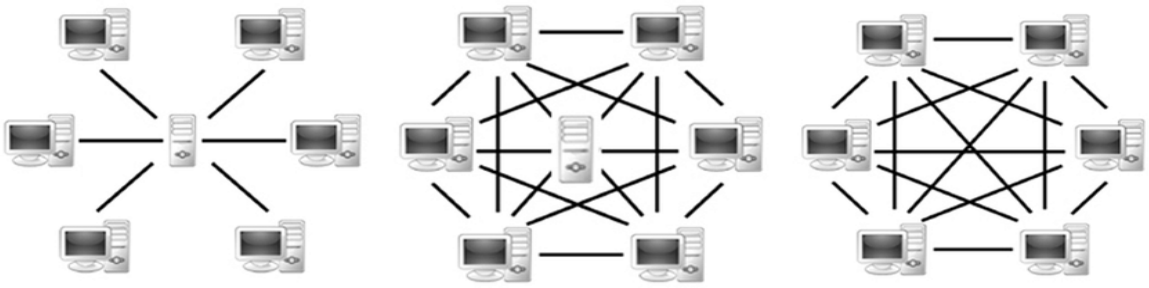
Η τοπολογία ενός δικτύου **Client-Server** δίνει την δυνατότητα στους κόμβους να έχουν πρόσβαση στους διακομιστές από απομακρυσμένα σημεία. Επίσης δεν υπάρχει ανάγκη για χωρητικότητα στον δίσκο των κόμβων καθώς το μοντέλο αυτό δεν το απαιτεί. Τέλος η

αναβάθμιση σε αυτά τα δίκτυα είναι εύκολη καθώς ο server είναι αυτός που αναβαθμίζεται. [9]

2.2.3 Υβριδικά δίκτυα ομότιμων κόμβων Hybrid Peer to Peer

Ένα κατανεμημένο δίκτυο θεωρείται Hybrid όταν πρώτα θεωρείται P2P δίκτυο όπως αναφέρεται παραπάνω και δεύτερον εκμεταλλεύεται μια κεντρική οντότητα αναγκαία ώστε να παρέχει μέρη των υπηρεσιών του δικτύου(σαν το μοντέλο client server) [7]

Το μοντέλο του **Hybrid peer to peer θεωρείται** υβρίδιο των δύο παραπάνω μοντέλων καθώς συνδυάζει βασικά χαρακτηριστικά τους. Από την μία τα δίκτυα αυτά έχουν μια κεντρική οντότητα (**Client-Server**), από την άλλη το να διαμοιράζονται τους πόρους τους οι κόμβοι (**P2P**) είναι βασικό στοιχείο των hybrid P2P δικτύων.



Εικόνα 1 (Αριστερά-Τοπολογία Client-Server, στο κέντρο-Τοπολογία Hybrid P2P, δεξιά-Τοπολογία P2P) [7]

3 Αποκεντρικοποίηση/Συγκεντρωτισμός

3.1 Βασική έννοια αποκεντρικοποιημένων συστημάτων.

Η βασική ιδέα πίσω από τα αποκεντροποιημένα συστήματα είναι η κατανομή ελέγχου και εξουσιοδότησης σε περιφέρειες ,σε αντίθεση με μια κεντρική οντότητα να είναι υπεύθυνη για τον πλήρη έλεγχο μιας εκάστοτε οργάνωσης. Αυτή η ιδέα επιφέρει σημαντικά προτερήματα για μία οργάνωση όπως αυξημένη αποδοτικότητα, ταχύτερο χρόνο λήψης αποφάσεων και μειωμένο φόρτο στις υψηλές θέσεις του management. [2]

3.2 Αποκεντρικοποίηση (Decentralazation) στο Blockchain

Η αποκεντροποίηση είναι ένα από τα βασικά προτερήματα που παρέχονται στην Blockchain τεχνολογία και συγκεκριμένα συνήθως στα δημόσιου τύπου Blockchain συστήματα . Ο σχεδιασμός ενός Blockchain συστήματος είναι ιδανικός στο να στο να παρέχει μια πλατφόρμα που δεν χρειάζεται ενδιάμεσους παράγοντες. Στα κεντρικοποιημένα συστήματα υπάρχει συνήθως ένας ηγετικής φύσης χρήστης ο οποίος δρα ως αρωγός για την εξυπηρέτηση μεταξύ μελών ενός συστήματος ή ενός δικτύου, και είναι υπεύθυνος για την λήψη αποφάσεων στο σύστημα [2] . Σε παρακάτω κεφάλαια θα αναλυθούν συστήματα που λειτουργούν και με τους δυο τρόπους (αποκεντρωτικό ή συγκεντρωτικό χαρακτήρα).
Ένα σύστημα Blockchain το οποίο έχει αποκεντρωτικό χαρακτήρα επιτρέπει σε οποιονδήποτε συμμετέχοντα στο δίκτυο να αποκτήσει τη δυνατότητα να γίνει υπεύθυνος ως προς την λήψη αποφάσεων του συστήματος μέσω ανταγωνισμού. Μια τέτοια διαδικασία ανταγωνισμού ανήκει στους μηχανισμούς κοινής συναίνεσης.
Οι συνήθεις τεχνολογίες επικοινωνιών και πληροφορίας ως τώρα λειτουργούσαν συμβατικά βασισμένες σε κεντρικοποιημένες ή συγκεντρωτικές μεθόδους, όπου οι διακομιστή (servers) υπηρεσιών ή βάσεων δεδομένων λειτουργούσαν υπό τον έλεγχο μια κεντρικής οντότητας, γεγονός που τις έκανε ευάλωτες σε περίπτωση αποτυχίας της κεντρικής αυτής οντότητας. Η εφαρμογή του Blockchain αρχικά με την άφιξη του κρυπτονομίσματος (cryptocurrency) Bitcoin , έδωσε ένα μεγάλο έναυσμα για ανοιχτά προς τους χρήστες συστήματα που λειτουργούν με αποκεντρωτικό χαρακτήρα.

3.2.1 Πλεονεκτήματα απόκεντρικοποιημένων συστημάτων

- **Οι χρήστες δεν είναι αναγκασμένοι να εμπιστεύονται μία κεντρική αρχή**: Διάφορες εταιρίες/οργανώσεις (μέσα κοινωνικής δικτύωσης) έχουν δικαίωμα να χρησιμοποιούν προσωπικά δεδομένα των χρηστών τους. Σε ένα αποκεντρικοποιημένο σύστημα η απαιτούμενη εμπιστοσύνη μεταξύ τρίτων είναι ελάχιστη και συνεχίζει μειώνεται.
- **Πολύ μικρότερη πιθανότητα αποτυχίας του δικτύου λόγω αποτυχίας ενός κόμβου-μέλους:** Σε ένα αποκεντροποιημένο σύστημα η περίπτωση αποτυχίας ενός μέλους δεν σημαίνει πως θα καταρρεύσει ολόκληρο το σύστημα, καθώς δεν υπάρχει κεντρική αρχή η οποία είναι υπεύθυνη για την λειτουργία όλου του συστήματος. Αυτό σημαίνει πως το σύστημα δεν επηρεάζεται με την τυχόν εμφάνιση νέου χρήστη ή την αποτυχία ενός παλαιότερου.
- **Γρηγορότεροι χρόνοι πραγματοποίησης συναλλαγών:**

Οι συναλλαγές που βασίζονται σε αποκεντροποιημένα συστήματα ,όπως συστήματα που βασίζονται στην τεχνολογία Blockchain, χρειάζονται συνήθως μερικά λεπτά για να πραγματοποιήσουν μια συναλλαγή, σε σχέση με παλαιότερα κεντρικοποιημένα συστήματα όπως συναλλαγές τράπεζας.

3.3 Συγκεντρωτικά/Κεντρικοποιημένα Συστήματα (Centralized Systems)

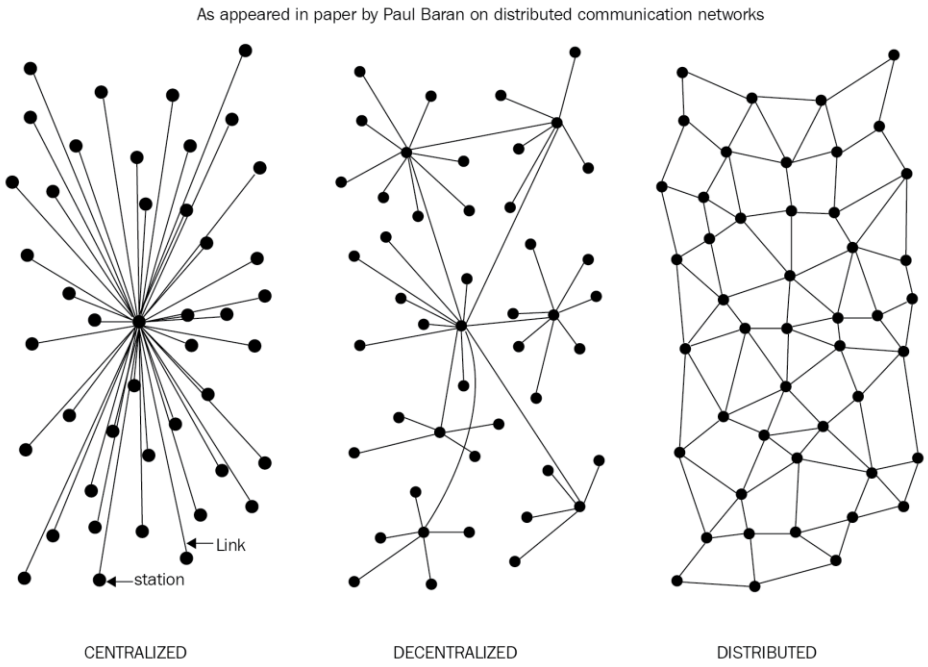
Η ίδια η λέξη (κεντρικοποιημένο/centralized) 'προδίδει' πως ένα τέτοιο σύστημα δομείται. Ένα τέτοιο σύστημα παρέχει τις υπηρεσίες στους στα μέλη του μέσω μια κεντρικής οντότητας, όπως μία τράπεζα παρέχει υπηρεσίες για συναλλαγές και πληροφορίες. Αυτό σημαίνει πως τα δεδομένα και οι συναλλαγές είναι γνωστά, κάτι που καθιστά την εμπιστοσύνη υψίστη προτεραιότητα.
Πιο συγκεκριμένα τα κεντρικοποιημένα συστήματα βασίζονται στο μοντέλο client-server, στο οποίο μια κεντρική οντότητα έχει την εξουσία να ελέγχει το σύστημα και είναι η μόνη υπεύθυνη για όλες τις διεργασίες ενός κεντρικοποιημένου συστήματος. Όλοι οι χρήστες του συστήματος εξαρτώνται από μία μόνο πηγή υπηρεσιών [2]. Στον κόσμο των blockchain συγκεντρωτικό χαρακτήρα έχουν συνήθως τα ιδιωτικά δίκτυα λόγω υψηλότερης απαίτησης ελέγχου και ασφάλειας με μηχανισμούς συναίνεσης όπως το Raft [10] και το PBFT [11]. Πολλοί πάροχοι υπηρεσιών όπως οι Google, Amazon, eBay και άλλοι χρησιμοποιούν αυτό το σύνηθες μοντέλο για να παραδίδουν τις υπηρεσίες τους.

3.4 Τρεις τύποι συγκεντρωτισμού/αποκεντρικοποίησης

Όσον αφορά την αποκεντροποίηση λογισμικού υπάρχουν τρεις σκοπιές ή πτυχές που μπορούμε να ξεχωρίσουμε. Αν και πολλές φορές είναι δύσκολο να καταλάβουμε την μία χωρίς την άλλη, σε γενικές γραμμές είναι ανεξάρτητες. [12]

- Αρχιτεκτονικός συγκεντρωτισμός/αποκεντρικοποίηση: Αναφέρεται στο πόσους υπολογιστές ή φυσικούς κόμβους αποτελείται ένα σύστημα.
- Πολιτική κεντρικοποίηση/αποκεντρικοποίηση: Αναφέρεται στο πόσες οργανώσεις ή ξεχωριστά άτομα τελικά ελέγχουν τους υπολογιστές που αποτελούν το σύστημα.
- Λογική κεντρικοποίηση/αποκεντρικοποίηση: Αναφέρεται στο κατά πόσο οι διεπαφές και η δομή του συστήματος μοιάζει περισσότερο σαν να λειτουργεί υπό την επιρροή ενός μονολιθικού αντικειμένου ή μια άμορφης μάζας. Δηλαδή αν κάποιος 'κόψει' το σύστημα στην μέση, κατά πόσο θα συνεχίσουν τα μισά να λειτουργούν σαν ανεξάρτητες μονάδες.

Για παράδειγμα η τεχνολογία Blockchain είναι πολιτικά αποκεντρωποιημένη γιατί κανείς δεν ελέγχει την αλυσίδα, αρχιτεκτονικά αποκεντρωποιημένα καθώς δεν υπάρχει κεντρικό σημείο αποτυχίας της υποδομής του ενώ είναι λογικά κεντρικοποιημένη διότι υπάρχει μόνο μια κοινή και αποδεκτή κατάσταση από όλο το σύστημα το οποίο συμπεριφέρεται σαν μονάδα. [12]



Εικόνα 2 Διαφορετικοί τύποι δικτύων-συστημάτων [2]

Μια βασική διαφορά που παρατηρείται μεταξύ των αποκεντροποιημένων και κατανεμημένων συστημάτων, είναι πως στα κατανεμημένα πολλές φορές υπάρχει ακόμα μια κεντρική οντότητα όπου ‘διοικεί’ το σύστημα ενώ στα αποκεντροποιημένα μια τέτοια οντότητα δεν υπάρχει. [2] Σε ένα αποκεντροποιημένο σύστημα ο έλεγχος κατανέμεται ανάμεσα στου κόμβους του, χωρίς να εξαρτώνται από κάποιον κύριο κόμβο που θα έχει παραπάνω δικαιοδοσίες.

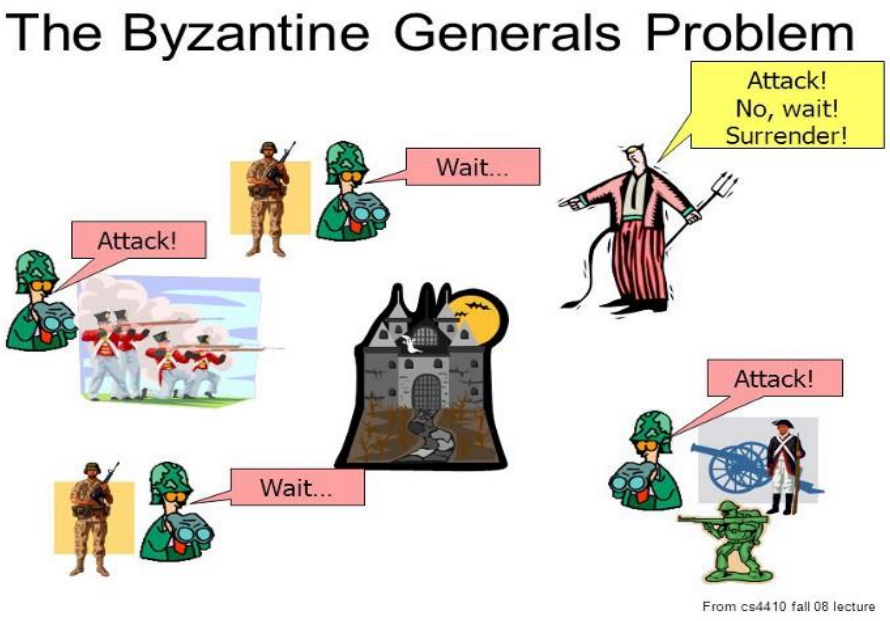
4 Ανάλυση μηχανισμών συναίνεσης σε Δίκτυα Blockchain

4.1 Εισαγωγικά: Το πρόβλημα των στρατηγών του Βυζαντίου

Το Πρόβλημα των Στρατηγών του Βυζαντίου (Byzantine Generals' Problem, BGP) δημοσιεύτηκε αρχικά από τον Leslie Lamport [13] το 1982 και αναφέρεται στο πρόβλημα εύρεσης ενός αλγορίθμου συναίνεσης σε κατανεμημένα συστήματα που πιθανόν να συμπεριλαμβάνουν κακόβουλους κόμβους, με παράδειγμα την προσπάθεια του Βυζαντινού στρατού να καταλάβει μια αντίπαλή πόλη.

Πιο συγκεκριμένα υποθέτουμε πως ο Βυζαντινός στρατός έχει χωριστεί σε διμοιρίες ή τμήματα με σκοπό να περικυκλώσει και να πολιορκήσει μια αντίπαλη πόλη. Ο μόνος τρόπος να καταφέρουν να πολιορκήσουν την πόλη είναι να επιτεθούν όλα τα τμήματα μαζί και ταυτόχρονα. Κάθε τμήμα έχει και έναν στρατηγό, όπου κάθε στρατηγός επικοινωνεί με τα άλλα τμήματα αλλά και με τους υπολοχαγούς του μόνο μέσω μηνυμάτων, λόγω της ιδιομορφίας του χώρου που βρίσκεται η αντίπαλη πόλη. Έτσι στόχος των στρατηγών είναι να συμφωνήσουν σε ακριβή ώρα για επίθεση ή για υποχώρηση λόγω αντεπίθεσης του αντιπάλου. Αν η επίθεση ή η υποχώρηση δεν εκπληρωθεί με την πλήρη ισχύ του Βυζαντινού στρατού, η ήττα είναι σίγουρη.

Σε περίπτωση όπου όλα τα μέλη του στρατού είναι έντιμα και έμπιστα πρόκειται για μια απλή επικοινωνία όπου και στις δύο περιπτώσεις θα υπάρξει εύκολα λύση . Το πρόβλημα παρουσιάζεται στην περίπτωση όπου κάποιοι από τους στρατηγούς ή μέλη στου Βυζαντινού στρατού είναι προδότες ή κατάσκοποι των αντιπάλων. Η πιθανότητα αποτυχία εκπλήρωσης της επίθεσης αυξάνεται όταν οποιοδήποτε μέλος του στρατού δράσει κακόβουλα και εναντίον του στρατού του διαδίδοντας εσφαλμένα μηνύματα, με σκοπό την παραπλάνηση για λήψη μη έγκυρων αποφάσεων.



Εικόνα 3 https://gauthamzz.github.io/tendermint.html#byzantine-fault-tolerant [14]

Το BGP [13] είναι πρόβλημα που μπορεί να εμφανιστεί σε πολλά κατανεμημένα δίκτυα ή δίκτυα Blockchain όπου η εμπιστοσύνη ανάμεσα στους κόμβους δεν είναι δεδομένη. Μια αποτυχία λόγω κακόβουλων ή 'βυζαντινών' κόμβων οφείλεται στην αιρετική προς το σύστημα συμπεριφορά ενός ή περισσότερων κόμβων. Πιο συγκεκριμένα ένας κακόβουλος κόμβος παραβλέπει τους βασικούς κανόνες του πρωτοκόλλου στο οποίο είναι ενεργός και εκπέμπει λανθασμένα μηνύματα. Έτσι μπορεί ακόμα και να καταφέρει να επηρεάσει τις αποφάσεις των υπόλοιπων κόμβων παραπλανώντας τους ώστε και αυτοί να δράσουν κακόβουλα σύμφωνα με τα παραπλανητικά μηνύματα που δέχθηκαν, με απώτερο σκοπό την αποτυχία επίτευξης ομοφωνίας και κοινής συναίνεσης στην λήψη αποφάσεων. Για να υπάρξει συναίνεση (consensus) πρέπει η πλειοψηφία των στρατηγών και μελών του στρατού (κόμβοι ενός δικτύου) να συμφωνήσουν σε ένα κοινό μεταδιδόμενο μήνυμα, χωρίς να επηρεάζονται από τους προδότες (κακόβουλους ή ΄Βυζαντινούς΄ κόμβους). Το πρόβλημα των στρατηγών του Βυζαντίου αναφέρεται για να δείξει την αναγκαιότητα ύπαρξης ενός μηχανισμού συναίνεσης σε κατανεμημένα δίκτυα, όπως είναι αυτά του Blockchain.

4.2 Proof of work (PoW) (Απόδειξη εργασίας)

Το Proof of Work (απόδειξη εργασίας) ή PoW είναι το πρώτο consensus protocol (πρωτόκολλο κοινής συναίνεσης) για crypto-currency (κρυπτονομίσματα) που δημιουργήθηκε σε εφαρμογή Blockchain και πιο συγκεκριμένα στο δίκτυο του Bitcoin [4] . Το πρωτόκολλο αυτό βασίζεται κυρίως σε απαιτητικές και δαπανηρές σε υπολογιστική ισχύ, λύσεις μαθηματικών προβλημάτων, που περιλαμβάνουν συναρτήσεις όπως η SHA-256 (Secure Hash Algorithm-256 bits) [15], και βασίζεται στην P-2-P τοπολογία δικτύων (τοπολογία ομότιμων κόμβων) στηριζόμενο σε ένα αποκεντρωτικό τρόπο λειτουργίας για την δημιουργία, εκπομπή και επαλήθευση των μπλοκ στο δίκτυο. Οι κόμβοι λειτουργούν ανεξάρτητα χωρίς να υπάρχει ανάγκη εμπιστοσύνης ανάμεσά τους.

Στο PoW οι κόμβοι ανταγωνίζονται μεταξύ τους για το ποιος θα είναι αυτός που θα δημοσιοποιήσει ένα μπλοκ με τις συναλλαγές προσθέτοντας το σε μία αλυσίδα με τις όλες ως τώρα συναλλαγές του δικτύου [16]. Για να αποδείξει ένας κόμβος πως δεν έχει σκοπό να επιτεθεί στο δίκτυο και να κρατά αυτός τις συναλλαγές χρειάζεται να εργαστεί σκληρά. Σε γενικά πλαίσια αυτή η εργασία αναφέρεται σε μαθηματικούς υπολογισμούς που απαιτούν μεγάλη υπολογιστική ισχύ.

4.2.1 Transactions (Συναλλαγές)

Στα πλαίσια του Blockchain ένα ηλεκτρονικό νόμισμα ορίζεται ως μια αλυσίδα ψηφιακών υπογραφών [4]. Κάθε ιδιοκτήτης μεταφέρει ένα νόμισμα στον επόμενο υπογράφοντας ψηφιακά με ένα hash που περιέχει πληροφορίες από προηγούμενες συναλλαγές μαζί με το public key (δημόσιο κλειδί) του επόμενου ιδιοκτήτη, προσθέτοντάς το στο νόμισμα. Ο επί πληρωμή χρήστης επικυρώνοντας τις υπογραφές μπορεί να βεβαιωθεί για την εγκυρότητα της αλυσίδας.

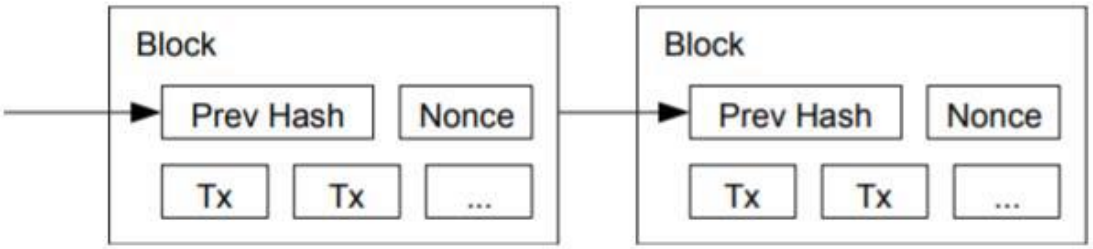
Ένα βασικό πρόβλημα με αυτόν τον τρόπο πραγματοποίησης συναλλαγών είναι ότι ο επί πληρωμή χρήστης δεν μπορεί να ξέρει αν ο ιδιοκτήτης του νομίσματος δεν έχει

χρησιμοποιήσει το νόμισμα αυτό και για άλλες συναλλαγές, το οποίο ορίζεται ως double-spend.
Χρειάζεται λοιπόν ένας τρόπος ώστε να ξέρει ο αποστολέας πως ο προηγουμένως ιδιοκτήτης του νομίσματος δεν υπέγραψε άλλες συναλλαγές με αυτό. Υποθέτουμε πως η πρώτη χρονολογικά συναλλαγή είναι αυτή που είναι έγκυρη, θεωρώντας έτσι τις μετέπειτα συναλλαγές με το ίδιο νόμισμα ως double spend. Έτσι ο μοναδικός τρόπος να επιβεβαιωθεί η απουσία μια συναλλαγής είναι να είναι όλες γνωστές. [4] Καθώς το PoW λειτουργεί σαν ένα αποκεντροποιημένο δίκτυο θέλουμε να μπορούμε να το κάνουμε αυτό χωρίς την χρήση μεσάζοντα. Έτσι οι συναλλαγές ανακοινώνονται δημόσια σε όλο το δίκτυο, με σκοπό να μπορούν οι συμμετέχοντες κόμβοι του να συμφωνήσουν σε μία μοναδική σειρά λήψης των συναλλαγών. Ο επί πληρωμή κόμβος χρειάζεται να έχει απόδειξη πως για κάθε χρονική στιγμή πραγματοποίησης μίας συναλλαγής, το μεγαλύτερο μέρος των κόμβων συμφωνεί για την πραγματοποίηση της εν λόγω συναλλαγής.
Η λύση που προτείνεται ξεκινά με την λειτουργία χρονικής αποτύπωσης (timestamp server). Ένα timestamp (χρονική αποτύπωση) ορίζει την χρονική στιγμή επιτυχημένης επίλυσης συνάρτησης τύπου SHA-256 και περιλαμβάνει το προηγούμενο timestamp στο hash του, διαμορφώνοντας έτσι μια αλυσίδα, όπου κάθε επιπρόσθετο timestamp ενισχύει το προηγούμενό του.

4.2.2 Τρόπος λειτουργίας του Proof of work

Η διαδικασία ανταγωνισμού εύρεσης του επόμενου block ξεκινά δίνοντας σαν είσοδο σε μία συνάρτηση, όπως η SHA-256, μία αξία η οποία θα μας δίνει μια έξοδο καθορισμένου μήκους με πλήθος μηδενικών στην αρχή της.
Ως είσοδο στην συνάρτηση δίνουμε το hash του παρόντος block, το Merkle root hash, πρόκειται για ένα hash που αν αντιστραφεί οδηγεί στις προηγούμενες ως τώρα συναλλαγές (χρησιμοποιείται για επαλήθευση και εξοικονόμηση χώρου), και το Nonce, έναν αριθμό που ξεκινά από το μηδέν και αυξάνεται κατά ένα για κάθε προσπάθεια επίλυσης της συνάρτησης μέχρι να βρεθεί το επιθυμητό αποτέλεσμα. Το Nonce είναι αυτό που βοηθά να γίνει αντιληπτή η απόδειξη εργασίας καθώς ορίζει τον αριθμό επαναλήψεων επίλυσης της συνάρτησης.
Σκοπός της διαδικασίας αυτής είναι το hash που παίρνουμε βάζοντας τις παραπάνω παραμέτρους να μας δώσει για έξοδο μια αξία που θα είναι ίση ή μικρότερη με τον ζητούμενο βαθμό δυσκολίας που μετριέται βάσει του αριθμού μηδενικών στην αρχή του παραγόμενου αριθμού (N-bits ήtarget), ο οποίος θα ικανοποιεί την απόδειξη της εργασίας. Πρόκειται για μια απαιτητική από άποψη υπολογιστικής ισχύος διαδικασία. Ακόμα θεωρείται και χρονοβόρα διότι μια απλή συναλλαγή για παράδειγμα στο δίκτυο bitcoin χρειάζεται δέκα λεπτά για το νέο block να προστεθεί χωρίς καν να έχει επικυρωθεί και από τους υπόλοιπους κόμβους του

δικτύου.



Εικόνα 4 Εικονική απεικόνιση αλυσίδας απο δύο μπλοκ [14]

Στην παραπάνω εικόνα φαίνεται μια αλυσίδα από blocks με τις απαραίτητες τιμές για τον υπολογισμό του hash για το επόμενο block. Εξαίρεση αυτών των blocks θεωρείται το genesis block, το οποίο είναι το πρώτο block που δημιουργείται αναγκάστηκα από το σύστημα και το hash του αποτελείται αποκλειστικά από μηδενικά. [17]

Για να μην υπάρχει κατάχρηση του δικτύου από τους κόμβους, το PoW λειτουργεί με ψήφο ανά CPU. Αυτό λύνει το πρόβλημα στον καθορισμό για την λήψη αποφάσεων μέσω πλειοψηφίας καθώς βασίζεται καθαρά στην υπολογιστική ισχύ του κάθε κόμβου και όχι στο πόσες IP διευθύνσεις μπορεί να παράγει (‘ξεγελώντας’ έτσι το δίκτυο) [16]. Οι αποφάσεις μέσω πλειοψηφίας αντιπροσωπεύονται από την πιο ‘μακριά’ (σε μήκος συναλλαγών) αλυσίδα, η οποία έχει και την μεγαλύτερη απόδειξη εργασίας. Εάν η πλειοψηφία της υπολογιστικής ισχύος κατέχεται από τίμιους και ειλικρινής κόμβους, η ειλικρινής αλυσίδα μεγαλώνει γρηγορότερα από τυχόν ανεπιθύμητους ανταγωνιστές.

Για να αντισταθμιστεί η πιθανή αύξηση τις ισχύος λόγω βελτίωσης hardware, η δυσκολία του PoW μεταβάλετε αλλάζοντας (μεγαλώνοντας συνήθως) το μέγεθος του επιζητούμενου στόχου (N-bits ή target) με σκοπό να κάνει την διαδικασία του hash πιο δύσκολη ή χρονοβόρα (λόγω αύξησής της απαίτησης ισχύος) , κάτι που ποικίλει αναλόγως την εφαρμογή blockchain. Εάν δηλαδή ένα νέο block δημιουργείται πολύ γρήγορα, η δυσκολία αυξάνεται (πρακτικά η πιθανότητα να βρεθεί ο στόχος μικραίνει καθώς αυξάνεται ο αριθμός των μηδενικών που το αποτελούν). [18]

Αν και το bitcoin είναι η πρώτη εφαρμογή που χρησιμοποίεισαι το PoW σαν πρωτόκολλο συνέναισης, δεν θα ήταν σωστό να τα συγχέουμε μεταξύ τους καθώς πληθώρα συστημάτων το χρησιμοπούν σήμερα, κάποια ακόμα ίσως και με πιο αποδοτικά αποτελέσματα. Για παράδειγμα μια άλλη διαδεδομένη εφαρμογή που χρησιμοποιεί PoW είναι το Ethereum με το κρυπτο-νόμισμα Ether που ποικοίλει σε χρήση, ανταμοιβή και χρόνους δημιουργίας των νέων block από το Bitcoin. Στη παρακάτω εικόνα φαίνοται διάφορες εφαρμογές του PoW σε ποικιλία συστημάτων.

#	Name	Algorithm	Block Time	Marketcap	Price	Volume
1	Bitcoin BTC	SHA256	10 minutes	$201.67B	$11,283.09	$13,777,018,442
2	Ethereum ETH	Ethash	~14 seconds	$22.66B	$211.200	$5,408,334,702
3	Bitcoin Cash BCH	SHA256	10 minutes	$6.1B	$339.673	$1,169,109,935
4	Litecoin LTC	Scrypt	~2.5 minutes	$5.44B	$86.2888	$2,563,360,701
5	Bitcoin SV BSV	SHA256	10 minutes	$2.56B	$143.223	$255,455,373
6	Monero XMR	CryptoNight	120 seconds	$1.54B	$89.8280	$81,035,742
7	Dash DASH	X11	~2.6 minutes	$937.99M	$104.477	$193,384,986
8	Ethereum Classic ETC	Ethash	N/A	$654.99M	$5.81325	$434,128,819
9	Zcash ZEC	Equihash	2.5 minutes	$406.12M	$56.5466	$91,213,064
10	Dogecoin DOGE	Scrypt	60 Seconds	$345.11M	$0.00286	$24,613,670

Εικόνα 5 Παράδειγμα συστημάτων που λειτουργούν με PoW [16]

4.2.3 Εξόρυξη για δημιουργία Μπλοκ (Mining)

Η εξόρυξη είναι μια ανταγωνιστική διαδικασία ανάμεσα στους κόμβους του δικτύου. Οι κόμβοι ανταγωνίζονται μεταξύ τους στο ποιος θα είναι αυτός που θα δημιουργήσει πρώτος το επόμενο block. Αυτό σημαίνει πως ο πρώτος που θα λύσει πρώτος ένα δύσκολο μαθηματικό πρόβλημα, αυτός δηλαδή που θα φτάσει πρώτος στον στόχο που δίνεται από το δίκτυο θα είναι και αυτός που θα δημιουργήσει το νέο block και θα ενημερώσει όλους τους κόμβους για αυτό, καθώς και θα παραλάβει ανταμοιβή αντίστοιχη της εργασίας του. Η πλειοψηφία των κόμβων πρέπει να συμφωνήσει για την ορθότητα της αξίας του εκπεμπόμενου hash. Αν το hash εγκριθεί εγκρίνεται και το νέο block. Τότε όλοι οι κόμβοι εμπεριέχουν το block αυτό στην δική τους αλυσίδα. Οι κόμβοι που υπολογίζουν την τιμή του hash ονομάζονται miners. [16]

4.2.4 Mining pools

Η δημιουργία νέων block μπορεί να γίνει είτε αυτόνομα από miners, είτε με συνεργασία πολλών μαζί. Στην δεύτερη περίπτωση, οι miners εργάζονται συγκεντρωτικά με σκοπό την ανακάλυψη ενός νέου block. Πρόκειται για μια διαδεδομένη πρακτική, λόγω της υψηλής δυσκολίας και απαίτησης υπολογιστικής ισχύος από ένα miner να ανακαλύψει ένα νέο block μονός του. Το έπαθλο που κερδίζεται με την εύρεση νέου block διαμοιράζεται σε όλους του συμμετέχοντες του εκάστοτε mining pool,ανάλογα με την προσπάθεια που κατέβαλαν. [19]
Λόγω αυτού του φαινομένου παρατηρούμε αδυναμία του PoW στην γνωστή ως 51% attack (επίθεση πλειοψηφίας). Αν το ποσοστό υπολογιστικής ισχύος των κόμβων σε ένα mining pool ξεπεράσει το 51% του δικτύου ,τότε αυτοί μπορούν να πάρουν τον έλεγχο του Blockchain αυτού [20]. Παρατηρείται πως κάποιος που έχει την πλειοψηφία της υπολογιστικής ισχύος του δικτύου μπορεί να βρεί την αξία του στόχου γρηγορότερα από άλλους, έχοντας έτσι την

δυνατότητα να δημιουργεί αυτός νέα μπλοκ είναι στην αλυσίδα [21].Έχει δηλαδή την δυνατότητα:

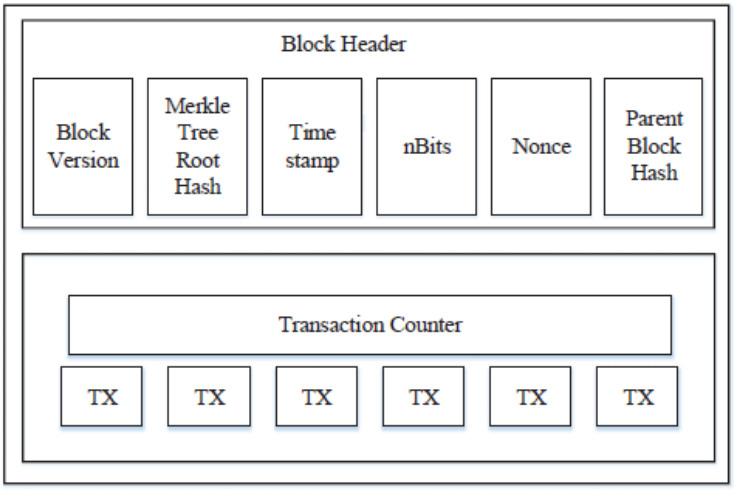
- Να τροποποιήσει τα δεδομένα της συναλλαγής, μπορεί να προκαλέσει πρόβλημα διπλής δαπάνης (double spending)
- Να σταματήσει τη συναλλαγή επαλήθευσης μπλοκ.
- Να σταματήσει την διαδικασία του mining οποιουδήποτε διαθέσιμου μπλοκ.

4.2.5 **Δομής ενός μπλοκ (Block structure)**

Αρχικά ένα block αποτελείται από το block header (επικεφαλίδα), και το block body (το περιεχόμενο του ίδιου του μπλοκ). Έχουμε ως εξής πρώτα για την επικεφαλίδα ενός block:

- **Έκδοση μπλοκ**- Ο αριθμός έκδοσης του μπλοκ υποδεικνύει τους κανόνες εγκυρότητας της εκάστοτε έκδοσης.
- **Previous block**- Το αποτέλεσμα της λύσης του SHA-256 αλγορίθμου του προηγούμενου σε σειρά block.
- **Merkle root hash**-Το αποτέλεσμα ενός SHA-256 αλγορίθμου όλων των συναλλαγών των block.
- **Timestamp**- Η χρονική στιγμή όπου άρχισε η διαδικασία επίλυσης του SHA-256 (η στιγμή που ξεκίνησε το mining).
- **Nbits ή target**- Ο στόχος ή η τιμή που πρέπει ένας miner να φτάσει πρώτος (επιλύοντας την SHA-256) ώστε αυτός να είναι αυτός που θα εκπέμψει την νεότερη συναλλαγή στο δίκτυο.
- Nonce- Πρόκειται για τον αριθμό των επαναλήψεων που οι miners επιλύουν τον SHA-256 μέχρις ότου να φτάσουν στον ζητούμενο στόχο (Nbits).

Το σώμα ενός block αποτελείται από το transaction counter (μετρητής συναλλαγών) και τα transaction (τις συναλλαγές). Ο μέγιστος αριθμός συναλλαγών που μπορούν να εμπεριέχονται σε ένα block ποικίλει ανάλογα με το μέγεθος του εκάστοτε block αλλά και με τον όγκο πληροφορίας της κάθε συναλλαγής. [16]



Εικόνα 6 An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends [13]

4.2.6 Βασικοί όροι και χαρακτηρίστηκα του PoW

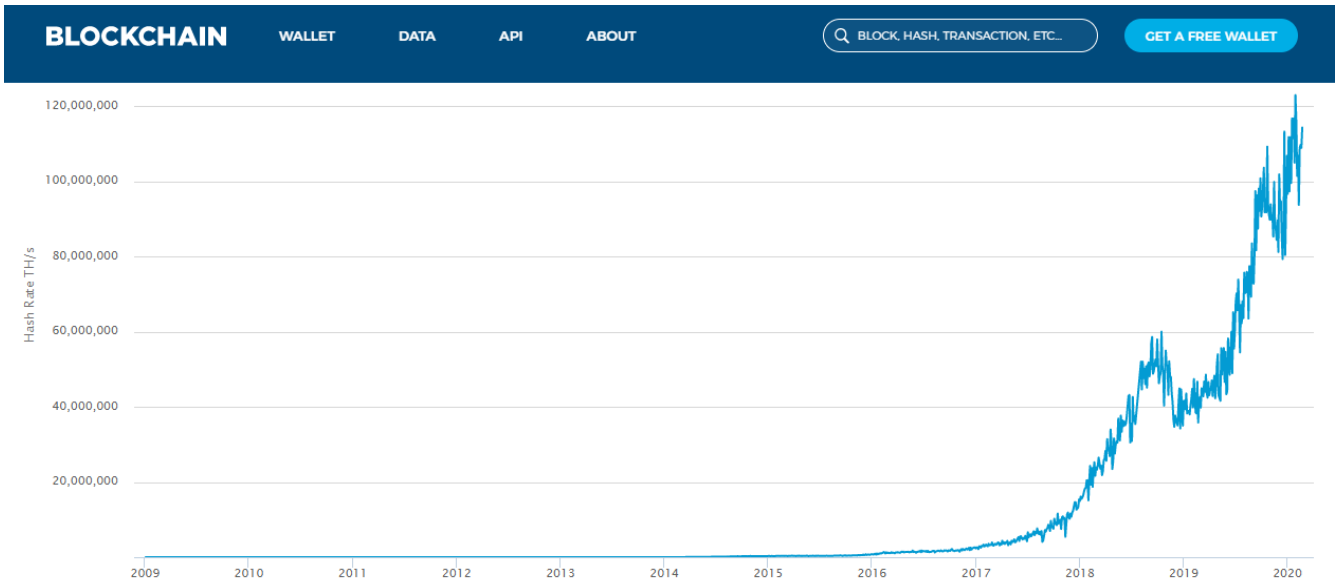
4.2.6.1 Hash

Αποτέλεσμα συνάρτησης που μετατρέπει μια ανεξαρτήτου μεγέθους είσοδο αριθμών και χαρακτήρων σε μια κωδικοποιημένη έξοδο προκαθορισμένου μήκους. Ένα hash για να δημιουργηθεί χρησιμοποιεί έναν αλγόριθμο (στο PoW τον SHA-256) .

ASICs: Ειδικό ολοκληρωμένο κύκλωμα που σχεδιάστηκε για να εκτελεί την SHA-256.

4.2.6.2 Hashing rate (Ρυθμός Hash)

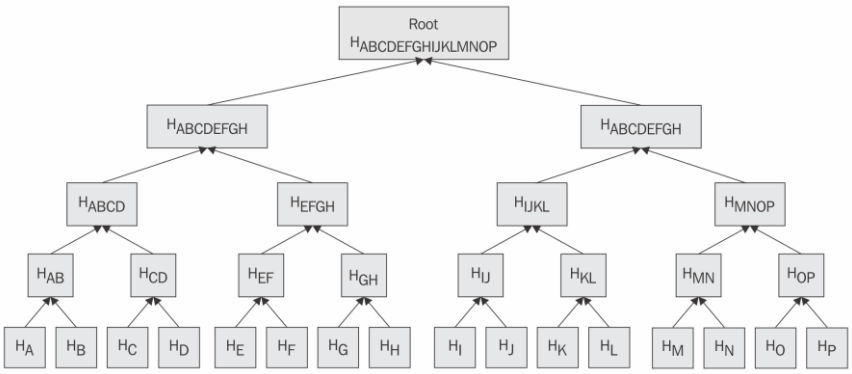
Το hashing rate η hashrate δείχνει πως αυξάνεται η δυσκολία στο mining με την πάροδο του χρόνου, και πρακτικά υπολογίζει τον ρυθμό των υπολογιζόμενων hashes ανά δευτερόλεπτο. Στις πρώτες μέρες λειτουργίας του Bitcoin το mining απαιτούσε πολύ μικρότερη υπολογιστική ισχύ, αλλά με την δημιουργία των mining pools και των ASICs το hashrate έχει ανέβει σημαντικά, έτσι και η δυσκολία του mining. Στο παρακάτω γράφημα φαίνεται πως το hashrate αυξάνεται με την πάροδο του χρόνου. [22]



Εικόνα 7 https://www.blockchain.com/el/charts/hash-rate?timespan=all [21]

4.2.6.3 Merkle tree root

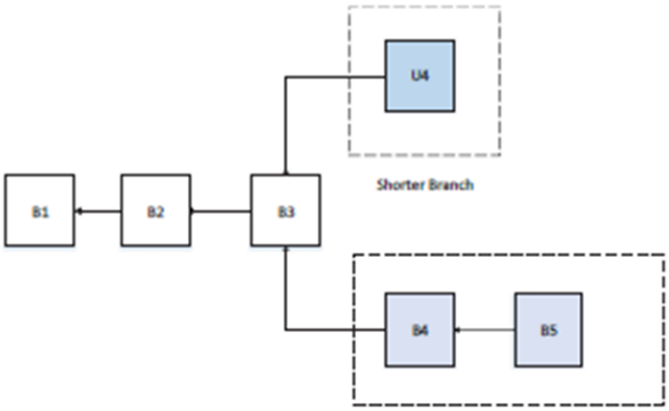
Η ιδέα των Merkle trees (δέντρων merkle) προήλθε από τον Ralph Merkle. Τα δέντρα αυτά επιτρέπουν την ασφαλή και αποδοτική επαλήθευση σε αρχεία μεγάλου όγκου δεδομένων. Πρόκειται για ένα τύπο δυαδικού δέντρου όπου αρχικά οι είσοδοι τοποθετούνται τα 'φύλλα' (κομβόι χωρίς παιδιά ή παρακλάδια), και έπειτα το περιεχόμενο των ζευγαριών γίνεται hashed σε ένα νέο κόμβο γονέα (περιέχει δηλαδή σαν παιδιά του το ζευγάρι των κόμβων αυτών), έως ότου να καταλήξουμε σε ένα μοναδικό hash που θεωρείται η ρίζα του Merkle δέντρου. [2]



Εικόνα 8 Mastering Blockchain Distributed ledgers, decentralization and smart contracts explained Imran Bashir [2]

4.2.6.4 Forks

Σε ένα αποκεντροποιημένο δίκτυο, έγκυρα blocks μπορεί να δημιουργηθούν ταυτόχρονα εάν παραπάνω από ένας κόμβοι βρουν το προκαθορισμένο στόχο σχεδόν την ίδια χρονική στιγμή. Ως αποτέλεσμα μπορεί να δημιουργηθούν forks (διακλαδώσεις) όπως φαίνεται στην παρακάτω εικόνα. Όμως είναι σχεδόν απίθανο τα ανταγωνιζόμενα forks να φτάσουν ξανά ταυτόχρονά στον ίδιο στόχο. Στο PoW η πιο ΄μακριά΄ αλυσίδα, αυτή δηλαδή με τον μεγαλύτερο αριθμό blocks κρίνεται ως η αυθεντική.



Εικόνα 9 An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends [13]

Όπως φαίνεται στην εικόνα τα Blocks U4,B4 δημιουργήθηκαν ταυτόχρονα. Η διαδικασία συνεχίζεται έως ότου να βρεθεί το νέο block (B5). Πλέον όλοι αλλάζουν από το U4 στην πιο μακριά αλυσίδα (B5). [16]

4.3 Proof of Stake (PoS)/Απόδειξη μεριδίου

Το Proof of stake (PoS) είναι ένα ακόμα πρωτόκολλο κοινής συναίνεσης, το δημοφιλέστερο μετά το PoW. Είναι σχεδιασμένο για δημόσια blockchain, τα οποία είναι ανοιχτά για οποιονδήποτε θελήσει να γίνει μέλος του δικτύου ως κόμβος . Χρησιμοποιήθηκε για πρώτη φορά από την εφαρμογή κρυπτονομισμάτων Peercoin [23] το 2011 σε συνδυασμό με το PoW πρωτόκολλο. Όπως και το Peercoin παρακάτω θα διαπιστώσουμε πως πολλές από τις πιο γνωστές PoS εφαρμογές λειτουργούν με παραλλαγές, κυρίως στον τρόπο επιλογής κόμβου για δημιουργία νέων block, κρατώντας όμως τις βασικές αρχές που αποτελούν ένα PoS-based blockchain .

Ο τρόπος λειτουργίας του έχει πολλά κοινά χαρακτηριστικά με το PoW καθώς και τα δύο λειτουργούν σε δημόσια blockchain, βασίζονται σε τοπολογία P2P δικτύου, με μία όμως ειδοποιός διαφορά. Στο PoS οι κόμβοι που θα δημιουργήσουν το επόμενο block στην αλυσίδα βασίζονται στο ‘stake ’ (μερίδιο ή ποντάρισμα) που διαθέτουν , αλλά όχι στην επεξεργαστική ισχύ τους (όπως είδαμε στο PoW) [24].

Στο PoS οι κόμβοι που συμμετέχουν στην διαδικασία εύρεσης νέου block συνήθως ονομάζονται επικυρωτές (validators) αντιστοίχως με τους miners στο PoW, και είναι αυτοί που ‘επενδύουν’ το stake (το μερίδιο τους) στο δίκτυο [21]. Οι επικυρωτές επενδύουν με το stake τους στο σύστημα για να έχουν πιθανότητες να δημιουργήσουν το νέο block. Αυτός που καταχωρεί το μεγαλύτερο stake έχει και την μεγαλύτερη πιθανότητα να είναι αυτός που θα δημιουργήσει το νέο block (χωρίς να του εγγυείται ότι θα επιλεχτεί σίγουρα). Ο κόμβος που δημιουργεί το block συνήθως ανταμείβεται με τα τέλη της συναλλαγής των αντίστοιχων στο stake του νομισμάτων στο σύστημα. Ως αποτέλεσμα αποφεύγεται η δημιουργία επιπλέον νομισμάτων στο δίκτυο (με την δημιουργία του δικτύου ορίζεται και ο αριθμός των κρυπτονομισμάτων ο οποίος παραμένει αμετάβλητος).

Το PoS θεωρείται ένας από του λίγους πιθανούς υποψηφίους για να αντικαταστήσουν το PoW ,το οποίο θεωρείται πολύ δαπανηρό λόγω της μεγάλης απαιτούμενης υπολογιστικής ισχύς. Το Proof of Stake χρησιμοποιεί εικονικούς πόρους αντίστοιχους του stake του κάθε επικυρωτή για να λύσει δύσκολα μαθηματικά προβλήματα όπως είδαμε και στο PoW. Για τον λόγο αυτό αντιθέτως με το PoW το PoS δεν απαιτεί την δαπανηρή χρήση υπολογιστικών πόρων. Η ιδέα πίσω από αυτήν την λογική πληροί τα παραπάνω λεγόμενα καθώς ο κόμβος ή επικυρωτής με το υψηλότερο stake θα έχει και την μεγαλύτερη εικονική υπολογιστική ισχύ, ώστε να καταφέρει να δημιουργήσει το επόμενο block [24] . Η ονομασία της διαδικασίας αυτής ποικίλει από εφαρμογή σε εφαρμογή (minting, forging…). Θεωρείται πιο ασφαλείς, καθώς οι πιθανότητες κάποιος να διαθέτει μεγάλο ποσοστό του κρυπτονομίσματος σε αντίθεση με το να ‘αγοράσει’ υπολογιστική ισχύ (όπως τα ASICs) είναι μικρότερες. Τέλος σε σχέση με το PoW θεωρείται και πιο ενεργειακά αποδοτικό λόγω της απουσία των δαπανηρών υπολογιστικών πόρων.

4.3.1 ΒΑΣΙΚΕΣ ΜΟΡΦΕΣ POS ΠΡΟΤΟΚΌΛΛΩΝ

Παρατηρείται πως υπάρχει πληθώρα συστημάτων που υιοθετούν το PoS σαν consensus πρωτόκολλο, το καθένα όμως με μια δική του παραλλαγή συνήθως πάνω στον τρόπο όπου επιλέγεται και δημιουργείται από το σύστημα ένα νέο block. Κάποιες από αυτές τις παραλλαγές είναι PoS πρωτόκολλα με χρήση λογικής Coin-Age για το Mining ή minting των block,άλλα με deposit-based λογική, άλλα Byzantine fault tolerant(BFT) PoS συστήματα και πολλά ακόμα καθώς συνεχώς δημιουργούνται νέες προσαρμογές σε τωρινά πρωτόκολλα, τα οποίο εξηγούνται παρακάτω.

4.3.1.1 'Ηλικία νομίσματος' (Coin Age)

Ο όρος coin age αναγνωρίζεται ως ο χρόνος που έχει περάσει από την τελευταία φορά που χρησιμοποίησε ένας κόμβος τα κρυπτονομίσματα του για την πραγματοποίηση συναλλαγής. Σε ένα σύστημα που λειτουργεί βασιζόμενο σε μια τέτοια προσέγγιση, η 'ηλικία' (age) του νομίσματος (coin) ενός κόμβου μηδενίζεται κάθε φορά που ο κόμβος αυτός πραγματοποιεί μια συναλλαγή. Ο κόμβος ο οποίος δημιούργησε το block βραβεύεται όταν κρατά τα νομίσματα του για μεγάλο χρονικό διάστημα και όχι αν τα ξοδεύει. Αυτό σημαίνει πως για όσο περισσότερο χρονικό διάστημα κρατά τα νομίσματα του αυτά αποκτούν μεγαλύτερη αξία [2]. Μειονέκτημα της προσέγγισης αυτής καθιστά το γεγονός πως κόμβοι αποθαρρύνονται από το να συμμετέχουν στις διεργασίες ομοφωνίας του δικτύου καθώς κρατώντας τα νομίσματά τους για μεγάλο χρονικό διάστημα αυτά αποκτούν μεγαλύτερη αξία. Για να αποφύγει τέτοια φαινόμενα η εφαρμογή VeriCoin [25] μαζί με το Coin age λαμβάνει υπόψιν και τον χρόνο που κρατάει ένας κόμβος τα νομίσματά του (stake time) .Τέτοια πρακτική έχει υιοθετηθεί από πολλές εφαρμογές του blockchain με consensus το PoS όπως πρώτα από όλες το Peercoin [23] αλλά και άλλες όπως το Cloakcoin [26] , Novacoin [27].

4.3.1.2 Βάση της κατάθεσης (Deposit Based)

Ένα δίκτυο λειτουργεί με deposit-based λογική κυρίως για λόγους ασφαλείας. Deposit-based σημαίνει πως η ανταμοιβή για την δημιουργία ενός νέου block δεν θα είναι άμεσα διαθέσιμη για να χρησιμοποιηθεί για άλλες συναλλαγές. Έτσι σε περίπτωση που υπάρξει αμφιβολία για την εγκυρότητα των συναλλαγών ενός κόμβου το μερίδιο που κρατείται από το σύστημα θα αφαιρεθεί από αυτόν, αποτρέποντας τον να δημιουργήσει αντικρουόμενα block, αντιμετωπίζοντας με αυτόν τον τρόπο το πρόβλημα μιας 'nothing at stake' επίθεσης. Μειονέκτημα της λογικής αυτής είναι πως η τιμωρία αφαίρεσης του stake πολλές φορές δεν αποθαρρύνει κακόβουλους κόμβους, καθώς αν 'ρισκάρουν' να πραγματοποιήσουν μια double spend επίθεση, χωρίς να γίνουν αντιληπτοί, θα κερδίσουν μεγάλο ποσοστό stake μέσω των πιθανών forks που θα χρησιμοποιήσουν.

4.3.1.3 Byzantine fault tolerant based, BFT-based

Σε ένα Byzantine Fault tolerant τύπου σύστημα, στους επικυρωτές (υποψήφιους κόμβους για δημιουργία νέων block) η δυνατότητα της πρότασης νέου μπλοκ είναι τυχαία επιλογή του δικτύου. Οι κόμβοι αυτοί έπειτα πρέπει να συμφωνήσουν στο ποιο θα είναι το νέο block μέσω μίας διαδικασίας πολλών γύρων, όπου κάθε ένας τους στέλνει μια 'ψήφο' για ένα συγκεκριμένο block σε κάθε γύρο. Στο τέλος της διαδικασίας αυτής οι κόμβοι αποφασίζουν από κοινού και οριστικά για το ένταξη ή όχι ενός block στην αλυσίδα. Πρέπει όμως να

σημειωθεί πως ακόμα και αν υπάρχει αλυσίδα από blocks, η διαφορά ενός τέτοιου πρωτοκόλλου με τα chain based πρωτόκολλά που αναφέρθηκαν παραπάνω είναι πως η συμφωνία που απαιτείται για την δημιουργία νέου block (consensus) δεν επηρεάζεται από χαρακτηριστικά όπως το μέγεθος ή το μήκος του υπόλοιπου blockchain. [28] [29]

Το Peercoin αποτελεί την πρώτη εφαρμογή PoS πρωτοκόλλου. Εάν ένας κόμβος Α μέσω πραγματοποίησης μιας συναλλαγής ανταμειφθεί με 10 νομίσματα από έναν κόμβο Β και τα κρατήσει (δεν πραγματοποιήσει κάποια συναλλαγή με αυτά) ας πούμε για 90 μέρες υπολογίζεται πως ο κόμβος Α έχει τώρα 10*90=900 νομίσματα*μέρες (Coin-days). Όταν όμως ο κόμβος Α χρησιμοποιήσει τα 10 αυτά νομίσματα που πήρε από τον κόμβο Β θεωρείται πως το Coin Age που συσσώρευσε ο κόμβος Α πλέον καταναλώνεται ή καταστρέφεται και επιστρέφει στο αρχικό ποσό (10 νομίσματα) . [23]

Μια άλλη εφαρμογή blockchain το Novacoin [27] , χρησιμοποιεί το coin age μαζί με το Coin Day Weight στον δικό του PoS αλγόριθμο. Όπως και στο PoW η δυσκολία του αλγορίθμου προσαρμόζεται ώστε οι κόμβοι να μπορούν να βρουν το ζητούμενο hash περίπου σε διάρκεια 10 λεπτών. Το Coin Day Weight είναι μια παρόμοια παράμετρος με το Coinage και χρησιμοποιείται για να βρεθεί ο ζητούμενος στόχος που απαιτείται για την δημιουργία block από το δίκτυο, κάτι που σημαίνει πως όσο μεγαλύτερο είναι τόσες πιο πολλές οι πιθανότητες για την δημιουργία νέου block. Το Novacoin είναι υβρίδιο ανάμεσα στα PoS και PoW και λειτουργεί και αυτό λύνοντας την SHA-256 συνάρτηση.

Το πρωτόκολλο Nxt [30] βασίζεται στο ποσοστό του stake, όπου κάθε κρυπτονόμισμα μπορεί να θεωρηθεί σαν ένα αντίστοιχο ποσοστό ισχύς για mining. Σαν αποτέλεσμα αυτού όσο πιο πολλά νομίσματα διαθέτει ένας κόμβος έχει και τις μεγαλύτερές πιθανότητες να κερδίσει το δικαίωμα να δημιουργήσει αυτός νέο block. Για να αντιμετωπίσει την πιθανή επίθεση κακόβουλων κόμβων το Nxt λειτουργεί με έναν αλγόριθμο εκλογής ηγετικών κόμβων για την αντίστοιχη διαδικασία mining. Κάτι τέτοιο γίνεται για να αποφευχθεί η δημιουργία νέων μπλοκ στο δίκτυο από κακόβουλους κόμβους οι οποίοι έχουν καταφέρει να διαθέσουν μεγάλο ποσοστό του stake. Η αντίστοιχη διαδικασία του mining στο Nxt ονομάζεται Forging, στην οποία ένας ενεργός κόμβος βρίσκει το hash με είσοδο το hash προηγούμενου block και του δημόσιου κλειδιού του με την βοήθεια της γνωστής συνάρτησης SHA-256 για να βρεθεί ο ζητούμενος στόχος για την δημιουργία νέων blocks.

Εφαρμογές όπως το Casper [31] και το Slasher [32] είναι deposit based μοντέλα και έχουν δημιουργηθεί από τους δημιουργούς του Ethereum [5] με απώτερο σκοπό την αντικατάσταση του PoW μοντέλου που λειτουργεί ως τώρα, κάτι που έχει προγραμματιστεί να γίνε με το Ethereum 2.0 μέσα στο 2020 με 2021 [33]. Το Casper θα εισάγει τους επικυρωτές στο Ethereum οι οποίοι όπως προαναφέρθηκε διαθέτουν μερίδιο των κρυπτονομισμάτων τους ως stake για να έχουν πιθανότητες να δημιουργήσουν νέα blocks. Σε περίπτωση εμφάνισης κακόβουλης συμπεριφοράς, το Casper εισάγει κυρώσεις μειώνοντας το μερίδιο των κρυπτονομισμάτων του κακόβουλου χρήστη από το σύστημα. Έτσι καταπολεμώνται επιθέσεις τύπου nothing at stake, λόγω αποθάρρυνσης τέτοιων χρηστών.

Άλλη μια PoS εφαρμογή είναι το Blackcoin [34] που μεταβάλει το stake modifier (είσοδος στο ζητούμενο hash δημιουργίας ενός block). Σκοπός του είναι εισάγει μια μεταβλητότητα στον χρόνο δημιουργίας νέων block ώστε να μην είναι προβλέψιμος. Έτσι αντιμετωπίζει την pre-computatation επίθεση. Μια τέτοια επίθεση έχει σκοπό να εντοπίσει την χρονική περίοδο

που γίνονται τα ΄πονταρίσματα ΄ από τους ειλικρινής κόμβους προς όφελος κακόβουλων για το δίκτυο κόμβων.
Η εφαρμογή Algorand [35] είναι ένα PoS σύστημα όπου για να δημιουργεί νέα block στην αλυσίδα χρησιμοποιεί ένα Byzantine Fault tolerant πρωτόκολλο. Πρόκειται για πρόταση νέων block μέσω ψηφοφορίας μιας επιτροπής από μέλη του δικτύου και χάρη σε αυτό το πρωτόκολλο η πιθανότητα εμφάνισης Forks στο Algorand είναι ελάχιστη έως αμελητέα. Μειονέκτημα του πρωτοκόλλου αυτού είναι το ότι απαιτεί τουλάχιστον τρεις γύρους ψηφοφορίας (Byzantine agreement ψηφοφορίας) για να σιγουρευτεί η εγκυρότητα και η ειλικρίνεια της πρότασης νέου block, καθώς και για να επιτευχθεί κοινή συναίνεση από όλους τους κόμβους για το νέο block στο σύστημα [36].

4.3.2 Βασικά χαρακτηριστικά και θέματα ασφάλειας του PoS

4.3.2.1 The Nothing at Stake Attack

Μια τέτοια επίθεση είναι δυνατό να πραγματοποιηθεί σε περίπτωσής ύπαρξης ενός ή περισσοτέρων forks σε ένα PoS δίκτυο. Οι κόμβοι σε ένα PoS δίκτυο για να συμμετέχουν στην διαδικασία δημιουργίας ενός block δεν χρειάζεται πάρα να διαθέτουν μία ψηφιακή υπογραφή με το περιεχόμενο του μεριδίου που διαθέτουν (σε αντίθεση με το PoW που απαιτεί κατανάλωση υπολογιστικής ισχύος). Έτσι παρατηρείται πως κακόβουλοι χρήστες ‘ποντάρουν’ σε πολλαπλά forks με την πρόθεση να δημιουργήσουν block (χωρίς να είναι γνωστό ότι ποντάρουν σε παραπάνω από ένα) μεγιστοποιώντας έτσι τις πιθανότητες τους. Κάτι τέτοιο θεωρείται διπλή δαπάνη (ένας κόμβος να χρησιμοποιεί τα ίδια κρυπτονομίσματα σε παραπάνω από μια συναλλαγές).Καθώς οι περισσότερες PoS εφαρμογές δεν τιμωρούν τους κόμβους σε περίπτωση κακόβουλης συμπεριφοράς (όπως κι δεν τους ανταμείβουν για την δημιουργία νέων block) , κακόβουλοι κόμβοι έχουν ως σκοπό να δημιουργούν πολλαπλά forks ώστε να εκμεταλλευτούν την αδυναμία αυτή του δικτύου. [24] [28]

4.3.2.2 The Long Range Attack

Σε ένα σενάριο μιας τέτοιας επίθεσης, ένας κακόβουλος χρήστης έχει ως σκοπό την δημιουργία ενός fork στο υπάρχον blockchain το οποίο θα ξεκινά αν όχι από το genesis block, από κάποιο από τα αρχικά blocks της υπάρχουσας μακρύτερης αλυσίδας με σκοπό να την προσπεράσει. Η αλυσίδα αυτή δεν είναι ανάγκη να εμπεριέχει τα ίδια block με την αρχική. Όταν το fork καταφέρει να γίνει μεγαλύτερο από την αρχική αλυσίδα τότε θα έχει καταφέρει να την προσπεράσει και να αναγνωριστεί αυτή ως η ισχύουσα αφού αυτή τώρα θα είναι η μεγαλύτερη.

Σκοπός του επιτιθέμενου είναι να βρει έναν τρόπο να καταφέρει να δημιουργήσει πιο πολλά blocks από την κύρια αλυσίδα στα ίδια χρονικά πλαίσια. Για να συμβεί κάτι τέτοιο ΄θα μπορούσε να αυξήσει τις πιθανότητές της αν ‘συνεργαζόταν’ με κάποιον άλλο κόμβο του δίκτυο.
Εδώ πρέπει να σημειωθεί πως οι κόμβοι έχουν συνήθως την δυνατότητα να αποσυρθούν από ένα PoS δίκτυο οποιαδήποτε στιγμή θελήσουν, αποσύροντας το μερίδιο τους. Ενώ όμως ο αποσυρόμενος κόμβος ήταν σε λειτουργία έπρεπε να προστατεύει τα προσωπικά του του δεδομένα (private key). Αφού πλέον δεν είναι ενεργός στο σύστημα η ασφάλεια των κλειδιών του δεν είναι προτεραιότητα ούτε του συστήματος αλλά ούτε του ίδιου αποσυρμένου πλέον

κόμβου. Ακόμα και εκτός του δικτύου όμως ο κόμβος αυτός θα ήταν ικανός να επικυρώσει τα blocks που είχε καταγεγραμμένα ως την στιγμή που σταμάτησε [37].
Ο επιτιθέμενος κόμβος μπορεί να εκμεταλλευτεί την παραπάνω ιδιότητα με δύο τρόπους. Πρώτον να καταχραστεί παράνομα τα κλειδιά του αποσυρόμενου κόμβου για να ενισχύσει την αλυσίδα του (παραβιάζοντας τα, αφού πλέον η ασφάλεια τους δεν είναι προτεραιότητα) ή δεύτερον να δωροδοκήσει τον αποσυρόμενο για τα δεδομένα του ώστε να τα χρησιμοποιήσει. Πλέον ο επιτιθέμενος κόμβος θα μπορεί να προσθέσει block στην αλυσίδα στο fork του ως τα block του αποσυρόμενου block, αυξάνοντας έτσι τις πιθανότητές της να ξεπεράσει την κύρια αλυσίδα.

4.4 Delegated Proof of Stake (DPoS)

Το Delegated Proof of Stake (DPoS) είναι ένα ακόμα consensus πρωτόκολλο το οποίο δημιουργήθηκε με σκοπό να λύσει προβλήματα που παρουσίαζαν παλαιοτέρα πρωτόκολλα όπως το PoW και το PoS.
Ένα σύστημα που βασίζεται σε DPoS πρωτόκολλο λειτουργεί με ένα σύστημα ψηφοφορίας, όπου κόμβοι του δικτύου (stakeholders) παρέχουν το μερίδιο τους σε άλλους κόμβους [38]. Συγκεκριμένα οι κόμβοι (stakeholders) ψηφίζουν για εκπροσώπους (delegates ή witnesses) τους στο δίκτυο, οι οποίοι θα έχουν την δυνατότητα να παράγουν και να εκπέμπουν νέα blocks. Η διαδικασία πραγματοποίησης ενός τέτοιου συστήματος χωρίζεται σε δύο μέρη. Το πρώτο μέρος απαρτίζεται από την διαδικασία εκλογής των εκπροσώπων ή υποψηφίων, και το δεύτερο από την επιβεβαίωσή των συναλλαγών και την δημιουργία των νέων block. Παρέχοντας το stake τους μέσω της ψηφοφορίας οι stakeholders αυξάνουν την πιθανότητα δημιουργίας νέων block στους υποψηφίους όπου αυτοί εμπιστεύονται. [39]Η ψηφοφορία πραγματοποιείται ψήφος ανά υποψήφιο και οι stakeholders μπορούν να ψηφίσουν παραπάνω από έναν υποψήφιο. Προϋπόθεση αυτού όμως είναι ότι το 51% των ψηφοφόρων να εκτιμούν πως το δίκτυο παραμένει αποκεντροποιημένο με τον αριθμό των υποψηφίων που εκλέχθηκαν. Κάτι τέτοιο πρακτικά σημαίνει πως ο αριθμός των υποψηφίων καθώς και το ποσοστό που διαθέτουν από κάθε stakeholder πρέπει να εκπροσωπούν ολόκληρο το δίκτυο ή τουλάχιστον παραπάνω από το 51% αυτού. το δίκτυο.. Αναλόγως την εφαρμογή που υιοθετεί το DPoS , οι υποψήφιοι επιλέγονται ανά προκαθορισμένα χρονικά διαστήματα ημέρας ή βδομάδας. Υπό κανονικές συνθήκες η παραγωγή νέων block πραγματοποιείται ανά προκαθορισμένα χρονικά διαστήματα [40]. Αν ένας υποψήφιος δεν καταφέρει να δημιουργήσει νέο block σε αυτό το διάστημα το block θεωρείται άκυρο και άλλος υποψήφιος παίρνει την θέση του, με πιθανό αποκλεισμό μελλοντικής επιλογής του πρώτου. Για κάθε block που δημιουργούν οι υποψήφιοι λαμβάνουν και ανάλογη ανταμοιβή [41] .
Το DPoS λόγω του μειωμένου αριθμού κόμβων που λαμβάνουν μέρος στην δημιουργία νέων block, καταφέρνει να προσθέτει block στην αλυσίδα της εκάστοτε εφαρμογής σε μικρότερο χρονικό διάστημα (π.χ. σε σχέση με το PoS) , και θεωρείται πιο αποδοτικό από προαναφερθέντα πρωτόκολλα ΄πως το Pow. Παρατηρείται πως το χαρακτηριστικό του αυτό, να λαμβάνονται δηλαδή αποφάσεις για τα νέα blocks από περιορισμένο αριθμό χρηστών του δικτύου, αντικρούεται στον αποκεντρωτικό χαρακτήρα των blockchain εφαρμογών. Ως αποτέλεσμα το DPoS δεν προάγει την άμεση δημοκρατία (PoS), όπου οι όλοι οι κόμβοι

συμμετέχουν στην διαδικασία ομοφωνίας και λαμβάνουν όλες τις αποφάσεις, αλλά την αντιπροσωπευτική, όπου μια συγκεκριμένη ομάδα κόμβων εκπροσωπεί όλο το δίκτυο λαμβάνοντας τις τελικές αποφάσεις .

Γνωστές εφαρμογές που λειτουργούν με DPoS πρωτόκολλο είναι οι Bitshares [42], Lisk [43] και EOS.IO [44].

Στο Lisk έχει εισαχθεί νέος τρόπος ψηφοφορίας όπου το stake των stakeholder που ψηφίζουν κλειδώνεται όταν ψηφίσουν. Το ποσό που κλειδώνεται ανήκει ακόμα στον stakeholder και ο υποψήφιος δεν θα έχει πρόσβαση σε αυτό. Κάτι τέτοιο γίνεται για λόγους ασφάλειας όπως είδαμε και σε παρόμοιες τεχνικές PoS πρωτοκόλλων. Επίσης για την πιο ομαλή και αποδοτική ροή του συστήματος δίνεται η δυνατότητα ψήφου μόνο σε έναν υποψήφιο ανά κόμβο. Κάτι τέτοιο γίνεται για λόγους ασφάλειας όπως είδαμε και σε παρόμοιες τεχνικές PoS πρωτοκόλλων.

Το πρωτόκολλο του EOS.IO χρησιμοποιεί μια δομή δύο μερών για την λειτουργία του. Αρχικά στο πρώτο μέρος εκλέγονται οι υποψήφιοι του συστήματος , 21 σε αριθμό, μόνο που στο EOS.IO οι αντίστοιχοι κόμβοι ονομάζονται παραγωγοί (producers). Οι producers είναι υπεύθυνοι για την παραγωγή νέων μπλοκ (ένα block/παραγωγό σε κάθε γύρο). Οι παραγωγοί ανταμείβονται για την δημιουργία και την επικύρωση των νέων block. Το δεύτερο μέρος αφορά την επιλογή των producers. Νέοι producers επιλέγονται στο τέλος κάθε γύρου με σκοπό την αποφυγή εμφάνισης κακόβουλων κόμβων. Κόμβος που θα θεωρηθεί κακόβουλος από το σύστημα τιμωρείται και αποκλείεται από την διαδικασία εκλογής και δημιουργίας νέων block. Στο EOS.IO νέα μπλοκς παράγονται περίπου κάθε 3 δευτερόλεπτα από κάθε κόμβο, αριθμό αξιοσημείωτο με προηγούμενα πρωτόκολλα και εφαρμογές (όπως το Bitcoin ή το Ethereum).

Στο BitShares [45]το ποσό που έχουν επενδύσει οι stakeholders είναι αυτό που θα κρίνει ποιοι θα είναι οι witnesses του συστήματος .Το ποσοστό των witnesses ανά γύρο επιλέγεται από τους stakeholders, ή πιο σωστά από την πλειοψηφία αυτών με ελάχιστο αριθμό τους 11 witnesses [42].

Όσον αφορά σε θέματα ασφάλειας όπως μια επίθεση διπλής δαπάνης (double spend) η πιθανότητα μιας βλάβης επικοινωνίας που επιτρέπει τέτοια επίθεση είναι πολύ χαμηλή. Το δίκτυο μπορεί να ανιχνεύσει αμέσως οποιαδήποτε απώλεια στην επικοινωνία, καθώς οι witnesses αποτυγχάνουν να παράγουν τα μπλοκ μέσα στο προκαθορισμένο χρονικό διάστημα. Το δίκτυο μπορεί να ‘πέσει’, ώστε οι χρήστες να πρέπει να περιμένουν έως ότου οι μισοί από τους witnesses επιβεβαιώσουν τις συναλλαγές τους.

4.5 Leased Proof of Stake (LPoS))

Το LPoS είναι ακόμα ένα consensus πρωτόκολλο που δημιουργήθηκε με σκοπό να φέρει βελτιώσεις σε προηγούμενα πρωτόκολλα, και λειτουργεί σε μεγάλο βαθμό όπως το PoS. Η ειδοποιός διαφορά των δύο είναι πως στις LPoS-based εφαρμογές στους χρήστες επιτρέπει να ΄δανείζουν΄ ποσοστό από το stake σε άλλους κόμβους. Οι κόμβοι με μεγαλύτερο συνολικά stake έχουν μεγαλύτερες πιθανότητες επιλογής για να παράγουν το επόμενο μπλοκ. Καθώς περισσότεροι κόμβοι λαμβάνουν μέρος στην διαδικασία παραγωγής block (μέσω του ‘δανεισμού’) το πρωτόκολλο αυτό θεωρείται πως είναι σε μεγαλύτερο ποσοστό αποκεντροποιημένο από το DPoS το οποίο χρησιμοποιεί περιορισμένο αριθμό κόμβων.

Στην εφαρμογή Waves [46] οι χρήστες μπορούν να συμμετέχουν είτε ως κόμβοι με σκοπό να δημιουργήσουν block ,είτε παρέχοντας το stake τους ως ΄δάνειο΄. Αυτό ως αποτέλεσμα μειώνει την πιθανότητα συγκέντρωσης ελέγχου του δικτύου από μία ομάδα κόμβων, αυξάνοντας τον αριθμό των επιλεγέντων μελών. Οι ανταμοιβές μοιράζονται μεταξύ των δημιουργών των block και των δανειστών.
Στην εφαρμογή ShareRing [47] οι κόμβοι μπορούν να δεχτούν προσφορές από άλλους stakeholders για να αυξήσουν την πιθανότητα τους, με αντίτιμο την επιστροφή ποσοστού από την ανταμοιβή για την δημιουργία ενός block. Η πιθανότητα ενός κόμβου (Masternode) να επιλεγεί ως proposer (αυτός που θα δημιουργήσει νέο block) είναι ανάλογη με την ψήφο του. Η πιθανότητα του να δημιουργήσει νέο block αυξάνεται ανάλογα με τον αριθμό του stake που έχουν επενδύσει ή 'δανείσει' στον εν δυνάμει proposer άλλοι κόμβοι, μέχρι τα όρια που προτείνονται από το σύστημα ισότητας των ψηφοφόρων.

4.6 Χαρακτηριστικά Voting αλγορίθμων

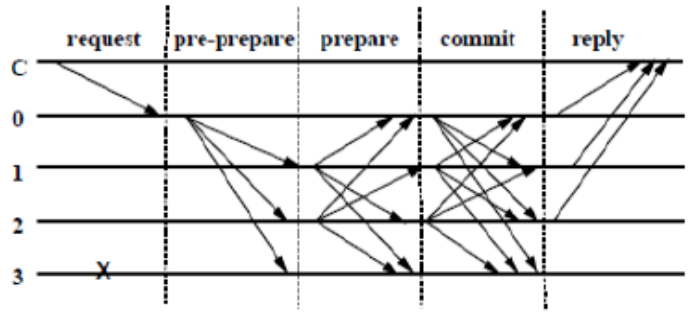
Τόσο στα PoS συστήματα αλλά και στους υπολοίπους αλγορίθμους συναίνεσης παρατηρείται μια βασική διαφορά ανάμεσα στον τρόπο που επιτυγχάνεται ομοφωνία σε ένα δίκτυο blockchain. Από την μία έχουμε τα proof-based συστήματα όπου μια διαδικασία απόδειξης επιτρέπει στους κόμβους να δημιουργούν και να προσθέτουν νέα block στην αλυσίδα (όπως το PoW στο Bitcoin). Από την άλλη υπάρχουν και τα vote-based συστήματα στα οποία κοινή συναίνεση αποκτάτε μέσω ψηφοφορίας μέσα στο εκάστοτε δίκτυο. Κάθε σύστημα διαθέτει διαφορετικό τρόπο διεξαγωγής τη ψηφοφορίας αναλόγως τον σχεδιασμό και την ανάγκη των εφαρμογών που ικανοποιεί.
Στα PoS συστήματα παρατηρείται χρήση γύρων ψηφοφορίας στις BFTή BA (Byzantine Fault tolerant , Byzantine Agreement [13]) εφαρμογές. Η εφαρμογή Tendermint αποτελεί ένα τέτοιο παράδειγμα. Στο Tendemint [48] η διαδικασία δημιουργίας νέων blocks απαρτίζεται από γύρους ψηφοφορίας (5 στάδια σε κάθε γύρο). Τα στάδια με την αντίστοιχη σειρά είναι τα Propose-Prevote-Precommit-Commit-NewHeight [49]. Συνοπτικά η διαδικασία αυτή λειτουργεί ω εξής:Αρχικά στο βήμα Propose προτείνεται ο εκάστοτε proposer (κόμβος που προτείνει νέα block) εκπέμπει την πρότασή του στο δίκτυο, και οι γειτονικοί κόμβοι την μεταδίδουν σε όλο το δίκτυο. Στο στάδιο Prevote βρίσκεται και το κομμάτι της ψηφοφορίας όπου ο κάθε κόμβος ψηφίζει για το νέο block που επιθυμεί και τον μοιράζεται με τους υπόλοιπους κόμβους του δικτύου. Στην συνέχεια στο στάδιο precommit, ο επικυρώτής ελέγχει εάν ένα προτεινόμενο block έχει μαζέψει παραπάνω από τα 2/3 των ψήφων στο στάδιο prevote, ώστε να μπορεί να θεωρηθεί έγκυρο. Αφού τα αποτελέσματα εκπεμφθούν στο δίκτυο και διαπιστωθεί πως έχουν ληφθεί παραπάνω από το 2/3 των ψήφων το αντίστοιχο block θα συνεχίσει στο στάδιο Commit. Αν όχι η πρόταση αυτή επιστρέφει στο στάδιο Propose του επόμενου γύρου. Στο στάδιο commit οι κόμβοι πρέπει να αποφασίσουν και να δεσμευτούν για το νέο block που θα ενταχθεί. Όταν αυτό πραγματοποιηθεί οι κόμβοι έχουν επιλέξει το νέο block αλλά περιμένουν ένα προκαθορισμένο διάστημα χρόνου για τυχόν ψήφους που άργησαν να φτάσουν λόγω καθυστέρησης εξυπηρέτησης του δικτύου.
Στα DPoS συστήματα μια διαδικασία ψηφοφορίας καθιστάτε αναγκαία καθώς μέσω ψηφοφορίας επιτυγχάνεται ομοφωνία και εντάσσεται το επόμενο block στην αλυσίδα. Οι

κόμβοι ενός DPoS δικτύου χρησιμοποιούν το stake τους για να 'ψηφίσουν' υποψηφίους κόμβους (delegates) οι οποίοι θα δημιουργήσουν νέα block. Πιο συγκεκριμένα μια εκλεγμένη από το σύστημα ομάδα υποψήφιους, το μέγεθος της οποίας εξαρτάται από την κάθε εφαρμογή, είναι οι υποψήφιοι εκπρόσωποι όπου οι κόμβοι του δικτύου θα 'ψηφίσουν' παραχωρώντας κομμάτι από το stake τους. Η διαδικασία αυτή συνήθως πραγματοποιείται ανά εκλογικούς γύρους και ο υποψήφιος με τις περισσότερες ψήφους, άρα και το μεγαλύτερο ποσοστό σε stake θα είναι αυτός που θα δημιουργήσει και προσθέσει το επόμενο block στην αλυσίδα.
Στις εφαρμογές όπου λειτουργούν βασισμένες σε LPoS πρωτόκολλο, ψηφοφορία πραγματοποιείται ανάμεσα στους κόμβους. Σκοπός αυτής της διαδικασίας ψηφοφορίας είναι οι κόμβοι να έχουν την δυνατότητα να δανείσουν ποσό από το stake τους σε οποιοδήποτε έμπιστο κόμβο της επιλογής τους. Όπως και στα κλασσικά PoS-based συστήματα ο κόμβος με το μεγαλύτερο stake θα έχει την μεγαλύτερη πιθανότητα να δημιουργήσει το νέο block. Η διαφορά όμως σε τέτοιου τύπου συστήματα είναι πως η ανταμοιβή για την δημιουργία του νέου block διαμοιράζεται στον κόμβο που το δημιούργησε αλλά και σε αυτούς που με το stake τους τον 'βοήθησαν' , δανείζοντας του stake αυξάνοντας έτσι τις πιθανότητές του. Το δάνειο αυτό του stake πραγματοποιείται στο δίκτυο μέσω ψηφοφορίας των κόμβων για εκπροσώπους τους.

4.7 Αλγόριθμοι συναίνεσης ανθεκτικοί σε 'Βυζαντινές' αποτυχίες (Byzantine Fault tolerant Consensus algorithms, BFT)

4.7.1 Practical Byzantine Fault tolerance (PBFT)

Το PBFT αποτελεί ένα από τα δημοφιλέστερα πρωτόκολλα συναίνεσης όσον αφορά Blockchain συστήματα. Δημοσιεύτηκε από τους Miguel Castro και Barbara Liskov [11] με σκοπό την πραγματοποίηση ενός αλγορίθμου κοινή συναίνεσης σε κατανεμημένα συστήματα. Πιο συγκεκριμένα ο αλγόριθμος δημιουργήθηκε με κίνητρο μία πρακτική λύση του προβλήματος των στρατηγών του Βυζαντίου (BGP). Έχει παρόμοιες αρχές λειτουργίας με πρωτόκολλα που θα αναλυθούν παρακάτω, όπως για παράδειγμα το Raft, καθώς λειτουργεί μέσω ενός μοντέλου ψηφοφορίας από επαναλαμβανόμενα μηχανήματα κατάστασης (replicated state machines) με την βοήθεια ενός ηγετικού κόμβου ο οποίος δέχεται αιτήματα από πελάτες [20].Η βασική διαφορά είναι πως για να προστατευτούν από κακόβουλους ΄Βυζαντινούς΄ κόμβους τα PBFT-based πρωτόκολλα απαιτούν τουλάχιστον τα 2/3 του συστήματος να συμφωνούν για την επίτευξη ομοφωνίας.
Ο αλγόριθμος εκτελείται ανά γύρο ως εξής: Ο ηγετικός κόμβος αναφέρεται ως primary (βασικός ή πρωταρχικός) και είναι αυτός που δέχεται τα αιτήματα των πελατών, τα 'υπογράφει' με ένα timestamp (χρονική αποτύπωση) και τα προωθεί στους υπολοίπους κόμβους οι οποίοι ονομάζονται και replicas (αναπαραγώμενοι κόμβοι) καθώς σε αυτούς αναπαράγεται το αίτημα του πελάτη. Ηγέτης επιλέγεται μόνο σε περίπτωση υποψίας μη διαθεσιμότητας του τρέχοντος ηγέτη.
Το πρωτόκολλο λειτουργεί με μία διαδικασία τριών φάσεων: Pre-Prepare, Prepare, Commit. Για να ξεκινήσουν όμως οι διεργασίες αυτές πρέπει πρώτα ο ηγετικός κόμβος να δεχτεί το αίτημα του πελάτη.

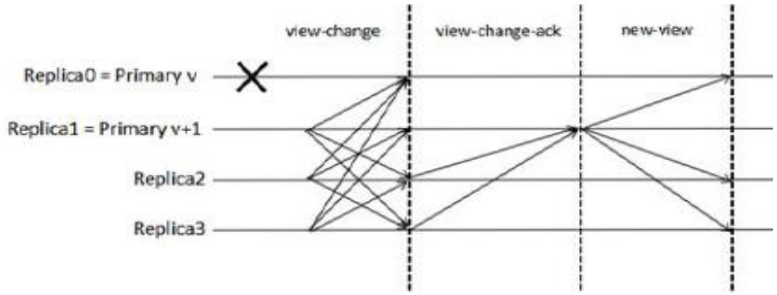


Εικόνα 10 Βήματα του PBFT αλγόριθμου [8]

Αρχικά στο στάδιο Pre-Prepare όπως αναφέρθηκε νωρίτερα ο ηγέτης βάζει το timestamp στο αίτημα και εκπέμπει ένα pre-prepare μήνυμα με την υπογεγραμμένη χρονική αποτύπωση σε όλους τους κόμβους. Το μήνυμα αυτό δεν περιέχει το αίτημα αλλά στέλνεται από τον ηγέτη ως απόδειξη εγκυρότητας ώστε να μπορέσουν να αποφασίσουν οι υπόλοιποί κόμβοι του δικτύου αν θα δεχτούν το επακόλουθο αίτημα.
Στο στάδιο Prepare οι κόμβοι που δέχονται το αίτημα του ηγέτη, εκπέμπουν με την σειρά τους ένα prepare μήνυμα σε όλο το δίκτυο καθώς και δέχονται τέτοια μηνύματα από παρόμοιους κόμβους. Αν ένα μήνυμα έχει εκπεμφθεί και αποδεχτεί από τα 2/3 του δικτύου τότε προχωράει στο τελευταίο στάδιο (Commit). Τα δύο παραπάνω στάδια ή φάσεις είναι αυτά που ικανοποιούν το κριτήριο της ομοφωνίας μέσω πλειοψηφίας από έναν γύρο ψηφοφορίας σε ένα PBFT σύστημα.
Στο στάδιο commit παρομοίως με στάδιο Prepare οι κόμβοι που έχουν φτάσει ως εδώ εκπέμπουν ένα μήνυμα commit σε όλο το δίκτυο. Μόλις ένας κόμβος λάβει το μήνυμα αυτό από ποσοστό που ξεπερνά τα 2/3 του δικτύου πιστεύει πως το σύστημα ήρθε σε συμφωνία και εκτελεί το αίτημα. Τελικά ο ηγετικός κόμβος απαντά στον πελάτη με το εκτελεσμένο αίτημα. [48]

4.7.1.1 ***View Change πρωτόκολλο***

Ο αλγόριθμος εκτελείται με εκλογικούς γύρους (views). Ο ηγετικός κόμβος αλλάζει ανά γύρο και σε περίπτωση που έχει περάσει ένα προκαθορισμένο διάστημα χωρίς ο ηγέτης να εκπέμπει το αίτημα, δηλαδή χωρίς να είναι ενεργός ή να υπολειτουργεί, καλείται το πρωτόκολλο View Change. Το πρωτόκολλο αυτό σκοπεύει να κρατήσει ζωντανή την διαδικασία εκτέλεσης του αλγορίθμου και ενεργοποιείται μόνο αν παραπάνω από τα 2/3 των μελών του δικτύου αντιληφθούν και ειδοποιήσουν τους γύρω κόμβους για αδυναμία του ηγετικού κόμβου. Αν οι κόμβοι συμφωνήσουν το view change εκτελείται προχωρώντας σε νέο εκλογικό γύρο και ορίζοντας νέο ηγετικό κόμβο [50].



Εικόνα 11 Εκτέλεση του View Change πρωτοκόλλου [51]

Στην εικόνα 3 φαίνεται η εκτέλεση του View Change πρωτοκόλλου. Έστω πως το View change ενεργοποιείται λόγω αποτυχίας του ως τώρα ηγετικού κόμβου στον γύρο **v**. Σε νέο **v+1** γύρο ένας κόμβος του δικτύου (Replica 1) ορίζεται ως ηγέτης (primary node) και εκπέμπει ένα μήνυμα 'View Change' σε όλο τι δίκτυο για να σιγουρευτεί πως ο ως τώρα ηγετικός κόμβος είναι ανενεργός. Έπειτα ο νέος ηγέτης επιβεβαιώνει τη αποτυχία του προηγούμενου αποτυχημένου ηγέτη όταν λάβει το μήνυμα View Change Ack από τουλάχιστον τα 2/3 του δικτύου, συμπεριλαμβανομένου και τον εαυτό του. Τέλος σε νέο γύρο ο καινούριος πλέον ηγετικός κόμβος εκτελεί τον BFT αλγόριθμο κοινής συναίνεσης όπως αναλύθηκε παραπάνω.
Άλλοι αλγόριθμοι κοινής συναίνεσης όπως το Paxos [51] και το Raft [10] χρησιμοποιούνται σε συστήματα με περιορισμένους κόμβους και μόνο για Crash fault τύπου αποτυχίες, και απαιτείται εμπιστοσύνη ανάμεσα στους χρήστες ώστε να πραγματοποιούνται συναλλαγές αποδοτικά και χωρίς καθυστερήσεις. Τα PBFT-based συστήματα από την άλλη έχουν λιγότερους περιορισμούς σε θέματα εμπιστοσύνης καθώς καταφέρνουν να λειτουργούν έως ότου το ποσοστό των κακόβουλων κόμβων δεν ξεπερνά το 1/3 του εκάστοτε συστήματος. Υλοποιήσεις PBFT-based συστημάτων συνήθως δεν εφαρμόζονται σε μεγάλη κλίμακα (για μεγάλο αριθμό κόμβων) και για ανοιχτά δημόσιου τύπου δίκτυα για τους δύο παρακάτω λόγους:
Σε ανοικτού τύπου δημόσια δίκτυα η πρόσβαση συνήθως είναι ελεύθερη για όποιο νέο μέλος θέλει να συμμετέχει σε αυτό, γεγονός που δίνει την δυνατότητα σε κακόβουλους κόμβους να συμμετέχουν εύκολα και με μικρό κόστος πρόσβασης. Ως αποτέλεσμα κακόβουλοι κόμβοι θα έχουν την δυνατότητα να δημιουργούν μη εγκεκριμένες αλλαγές αφού δεν υπάρχει μηχανισμός ελέγχου για την ένταξη τους στο σύστημα.
Η διαδικασία εκτέλεσης του αλγορίθμου απαιτεί την συνεχή επανεκπομπή μηνυμάτων και στις τρεις φάσεις του. Το γεγονός αυτό καθιστά την απόδοση του αλγορίθμου σε μεγάλη κλίμακα χαμηλή καθώς το σύστημα βομβαρδίζεται από τον όγκο των μηνυμάτων που στέλνονται σε όλες τις φάσεις πραγματοποίησης του. Κάτι τέτοιο περιορίζει PBFT-based συστήματα με υλοποιήσεις τους συνήθως να μην ξεπερνούν τους 100 κόμβους.
Οι δύο παραπάνω λόγοι κάνουν φανερό πως PBFT-based αλγόριθμοι συναίνεσης λειτουργούν βέλτιστα σε δίκτυα που απαιτούν έλεγχο άδειας αλλά και μικρό αριθμό συμμετεχόντων. Γνωστές υλοποιήσεις του PBFT είναι το Hyperledger Fabric, R3 Corda αλλά και η πλατφόρμα Zilliqa

4.7.1.2 *PBFT-based Εφαρμογές*

Το Hyperledger Fabric [52] αποτελεί μια πλατφόρμα τεχνολογίας blockchain για ιδιωτικά δίκτυα με σκοπό να εκτελεί ‘έξυπνα συμβόλαια’ (smart contracts ή chaincodes). Η πλατφόρμα αυτή είναι μέρος της οικογένειας προγραμμάτων Hyperleldger [53] με την πρώτη έκδοση v0.5 του Fabric να έχει δημοσιευτεί τον Ιούνιο του 2016. Η αρχιτεκτονική του Fabric του δίνει την δυνατότητα να εναλλάσσει μηχανισμούς συναίνεσης εκμεταλλευόμενοι γνωστές και αποτελεσματικές τεχνολογίες. Στην πρώτη του έκδοση το Fabric χρησιμοποιούσε το PBFT ως μηχανισμό συναίνεσης, αφού οι κόμβοι επικύρωσης των συναλλαγών του συστήματος το χρησιμοποιούσαν για τον εντοπισμό κακόβουλων κόμβων. Ένα chaincode είναι αντίστοιχο ενός Smart Contract. Πρόκειται δηλαδή για ένα κομμάτι κώδικα που γράφεται συνήθως σε γλώσσα προγραμματισμού Go (golang.org). Ο κώδικας αυτός περιέχει μια διαδικασία ή έναν συμβιβασμό που πρέπει να εκτελεστεί ώστε να μπορέσει να εκπληρωθεί μια συναλλαγή ανάμεσα σε δύο κόμβους. Είναι οι όροι συμφωνίας για την εκπλήρωσή μίας συναλλαγής. [54]
Η πλατφόρμα Zilliqa [55] υλοποιεί blockchain εφαρμογές χρησιμοποιώντας ως αλγόριθμο συναίνεσης το PBFT. Είναι η πρώτη πλατφόρμα που χρησιμοποιεί την τεχνική κοπής (sharding), η οποία αντιμετωπίζει το πρόβλημα της επεκτασιμότητας που αντιμετωπίζουν τα περισσότερα blockchain συστήματα. Με λίγα λόγια το sharding είναι μια τεχνική αποσυμφόρησης του δικτύου καθώς διαιρεί το δίκτυο σε μικρότερές ομάδες κόμβων. Διαιρώντας το δίκτυο το συνολικό μέρος των συναλλαγών διαμοιράζεται στις αντίστοιχες μικρότερες ομάδες χωρίς να χρειάζεται πλέον όλα τα μέλη του δικτύου να επικυρώνουν όλες τις συναλλαγές. Αφού πλέον οι συναλλαγές ελέγχονται παράλληλα από κάθε ομάδα η επεκτασιμότητα του δικτύου αυξάνεται καθώς είναι δυνατό να διευθετηθεί μεγαλύτερο πλήθος συναλλαγών στον ίδιο χρόνο. Το Zilliqa χρησιμοποιεί το PoW για ασφάλεια από επιθέσεις Sybil και το PBFT σαν μηχανισμό συναίνεσης το οποίο προσφέρει επιπλέον ασφάλεια στην πλατφόρμα. Μια Sybil επίθεση έχει στόχο την δημιουργία πολλών πλαστών ταυτοτήτων δημιουργώντας πλαστές ψηφιακές υπογραφές [56] . Έτσι ο επιτιθέμενος κόμβος θα έχει μεγάλη επιρροή στο σύστημα αφού θα κατέχει μεγάλο ποσοστό αυτού λόγω των πλαστών ταυτοτήτων. Κάτι τέτοιο αποφεύγεται σε PoW συστήματα καθώς η συνεχής και δαπανηρή διαδικασία εξόρυξης καθιστά την επίθεση αυτή πολύ χρονοβόρα και κοστοβόρα. Το Zilliqa έχει καταγράψει σε δοκιμαστικά στάδια με μέγιστο αριθμό κόμβων τους 3600 χωρισμένους σε 6 τμήματα (shards) τις 2488 συναλλαγές το δευτερόλεπτο [57].

4.8 Πρωτόκολλο συναίνεσης της πλατφόρμας Ripple (Ripple Protocol Consensus algorithm, RPCA)

Το RPCA δημοσιεύτηκε από τους David Schwartz, Noah Youngs και Arthur Britto [58]. Με το κρυπτονόμισμα XPR το Ripple λειτουργεί στο δίκτυο Ripplenet με σκοπό την δημιουργία μιας πλατφόρμας άμεσης πληρωμής σε ένα παγκόσμιο αποκεντροποιημένο δίκτυο συναλλαγών, συνδέοντας τα μέλη του δικτύου, για παράδειγμα τραπεζικές οντότητες, με απλούς χρήστες ή πελάτες, όπως μικρές εταιρίες και επιχειρηματίες, για την διευθέτηση των μεταξύ τους συναλλαγών.

Το Ripple είναι ένα αποκεντρικοποιημένο σύστημα πληρωμών, με ελεύθερη πρόσβαση στο κοινό. Οι συμμετέχοντες κόμβοι στο Ripplenet μπορεί να έχουν ένας από τους τρεις παρακάτω ρόλους:

- **Χρήστες (Users):** Κόμβοι που καταθέτουν και δέχονται πληρωμές,
- **Εξυπηρετητές αγοράς (Market makers):** Κόμβοι που δρουν ως παράγοντες και αρωγοί των συναλλαγών του συστήματος. Χρειάζονται ώστε να πραγματοποιούν συναλλαγές από οποιοδήποτε κρυπτονόμισμα ή συνάλλαγμα στο δίκτυο του Ripple,
- **Διακομιστές επικύρωσης ή επικυρωτές κόμβοι (Validating servers):** Κόμβοι που εκτελούν το RPCA πρωτόκολλο συναίνεσης ελέγχοντας και επικυρώνοντας όλες τις συναλλαγές που πραγματοποιούνται στο σύστημα.

Κάθε χρήστης διαθέτει ένα ζευγάρι κλειδιών (ιδιωτικό/δημόσιο) τα οποία χρησιμοποιεί για να πραγματοποιήσει συναλλαγές με ασφάλεια, κρυπτογραφώντας τις πληρωμές του μέσω του ECDSA αλγορίθμου (Elliptic curved digital signature algorithm) όπως γίνεται και στο δίκτυο του Bitcoin [59]. Ακόμα ένας χρήστης κατέχει ένα ανοιχτό κατάστιχο που καταγράφει το ποσοστό του XPR [60] στον λογαριασμό του (open ledger) και ονομάζεται ανοιχτό καθώς σε αυτό δεν καταχωρούνται ολοκληρωμένες συναλλαγές.
Οι συναλλαγές που πραγματοποιούνται στο δίκτυο του Ripple καταχωρούνται σε ένα κατανεμημένο κατάστιχο. Μόλις αυτές επικυρωθούν από την πλειοψηφία των διακομιστών επικύρωσης αποθηκεύονται στο ολοκληρωμένο ή ΄τελευταίο κατάστιχο΄(last closed ledger) [58]. Το κατάστιχο αυτό περιέχει την τελευταία συναλλαγή που επικυρώθηκε και αντιπροσωπεύει την παρούσα κατάσταση του δικτύου.
Κάθε κόμβος που λαμβάνει μέρος στο πρωτόκολλο συναίνεσης (validating servers) συντηρεί μια λίστα από έμπιστους κόμβους (προκαθορισμένη από τους δημιουργούς του Ripple) γνωστή ως Unique Node list (UND). Κατά την διάρκεια εκτέλεσης του RPCA πρωτοκόλλου οι διακομιστές επικύρωσης λαμβάνουν υπόψιν τους ψήφους μόνο μέσα από αυτήν την λίστα.
Στο Ripple επιτυγχάνεται κοινή συναίνεση μέσα σε γύρους ψηφοφορίας που πραγματοποιείται από τους διακομιστές επικύρωσης. Πιο συγκεκριμένα το πρωτόκολλο συναίνεσης εμπεριέχετε σε τρείς φάσεις: Την φάση συλλογής (collection phase),την φάση κοινής συναίνεσης (consensus phase) και τέλος την φάση του ολοκληρωμένου κατάστιχου(ledger closing phase) [59].
Στην πρώτη φάση οι επικυρωτές κόμβοι μαζεύουν όλες τις υποψήφιες συναλλαγές που βρίσκονται στο σύστημα και τις ελέγχουν όσον αφορά την αυθεντικότητα του δημόσιου κλειδιού που περιέχουν. Ακόμα οι συναλλαγές αυτές ελέγχονται ως προς την εγκυρότητα του χρήστη. Πιο συγκεκριμένα ελέγχεται αν ο κόμβος που έχει προτείνει μία συναλλαγή διαθέτει στον λογαριασμό του το ποσό που απαιτείται για την εκπλήρωσή της. Οι συναλλαγές που θεωρούνται αυθεντικές και έγκυρες αποθηκεύονται προσωρινά σε μια λίστα υποψηφίων ως προς εκτέλεση συναλλαγών (candidate set), με σκοπό στην συνέχεια να εκπεμφθούν σε όλο το δίκτυο [59]. Οι επικυρωτές κόμβοι δέχονται προτάσεις μόνο από κόμβους που περιέχονται στην UNL λίστα τους και τις αποθηκεύουν σε μία λίστα συναλλαγών προσθέτοντας μία ψήφο για κάθε νέα έμπιστη υποψήφια συναλλαγή που λαμβάνουν.

Στο δεύτερο στάδιο, οι επικυρωτές κόμβοι συνεχίζουν να στέλνουν και να δέχονται προτάσεις. Η διαφορά εδώ είναι πως ένας κόμβος προωθεί μια πρόταση μόνο αν παραπάνω από το 80% του UNL του την θεωρεί έγκυρη. Οι προτάσεις που τηρούν αυτό το κριτήριο καταχωρούνται στο κατάστιχο του κόμβου που επικυρώθηκαν για να εκτελεστούν.
Στο τελευταίο στάδιο, αφού το κατάστιχο ολοκληρωθεί και ενταχθούν όλες οι εγκεκριμένες από το δεύτερο στάδιο συναλλαγές, αυτές εκτελούνται[4]. Τέλος όταν ολοκληρωθούν οι συναλλαγές αρχίσει νέος γύρος ψηφοφορίας.
Το Ripple καταφέρνει να αντέχει τις BFT αποτυχίες μέσω τις υψηλής απαίτησης ομοφωνίας που απαιτείται από τους κόμβους (μεγαλύτερη του 80%). Με την λειτουργία των UNL η εργασία για την πραγματοποίηση συναλλαγών, επιτυγχάνεται γρήγορα καθώς οι διεργασίες διαμοιράζονται στους κόμβους χωρίς να απαιτείται εμπιστοσύνη μεταξύ τους (εκτός της UNL λίστας). Σύμφωνα με το [61] στο Ripple πραγματοποιείται μια συναλλαγή ανά 4 δευτερόλεπτα, ενώ συνολικά εκτελούνται περίπου 1500 συναλλαγές ταυτόχρονα, με βλέψεις για την επεκτασιμότητα της πλατφόρμας αντίστοιχες με συστήματα πληρωμών όπως η Visa (παρατηρήθηκαν 65,000+ συναλλαγές το δευτερόλεπτο, 15 Ιουλίου 2019).

4.9 Πρωτόκολλο συναίνεσης της πλατφόρμας Stellar (Stellar Consensus Protocol, SPC)

Το πρωτόκολλο SPC δημοσιεύτηκε από τον David Mazieres [62] ως πρωτόκολλο συναίνεσης για την πλατφόρμα συναλλαγών Stellar σε εφαρμογές Blockchain. Πρόκειται για ένα πρωτόκολλο που επιτυγχάνει ομοφωνία μέσω πλειοψηφίας βασιζόμενο στο ομοσπονδιακό BFT πρωτόκολλο (Federated Byzantine Agreement, FBA). Η κύρια διαφορά του FBA με προγενέστερα BFT συστήματα είναι πως στο FBA οι κόμβοι που λαμβάνουν μέρος σε μια συναλλαγή αποφασίζουν ελεύθερα για την ομάδα εμπίστων κόμβων τους (quorums) με τους οποίους θα εκτελέσουν το πρωτόκολλο κοινής συναίνεσης [20] . Ένα FBA-based σύστημα όπως το Stellar θεωρείται αποκεντροποιημένο καθώς δεν απαιτείται ο ορισμός μίας κεντρικής αρχής για την επικύρωση και τον έλεγχο των συναλλαγών. Αντίθετα συνολικά οι κομβόι δρουν ως επικυρωτές και αποφασίζουν για την έγκυρη διεξαγωγή συναλλαγών. Επίσης το δίκτυο του Stellar παρέχει ελεύθερη και χωρίς έλεγχο πρόσβαση σε νέους συμμετέχοντες (Open/Permissionless).
Το SPC εισάγει την έννοια των quorum και των quorum slices. Η έννοια του Quorum αναφέρεται στην δυνατότητα ενός κόμβου να διαλέξει ελεύθερα τα δικά του quorums slices, δηλαδή μια ομάδα εμπίστων κόμβων για την επικύρωση συναλλαγών. Τα quorum slices είναι ομάδες που ανήκουν σε ένα ή περισσότερα Quorums, με σκοπό να βοηθήσουν έναν κόμβο κατά τις διεργασίες που απαιτούνται για να υπάρξει ομοφωνία. Όταν επαρκής ομάδες από quorum slices διαμορφωθούν και δράσουν συνολικά δημιουργείται ένα quorum που μέσω της εκτέλεσης του FBA πρωτοκόλλου επιτυγχάνουν κοινή συναίνεση (consensus).
Σε αντίθεση με το Ripple η δημιουργία των Quorums (αντιθέτως των UNL στο Ripple) είναι ελεύθερη για όλους τους κόμβου που απαρτίζουν το δίκτυο, καθώς και η παράλληλη συμμέτοχή ενός κόμβου σε παραπάνω από ένα quorum slices.

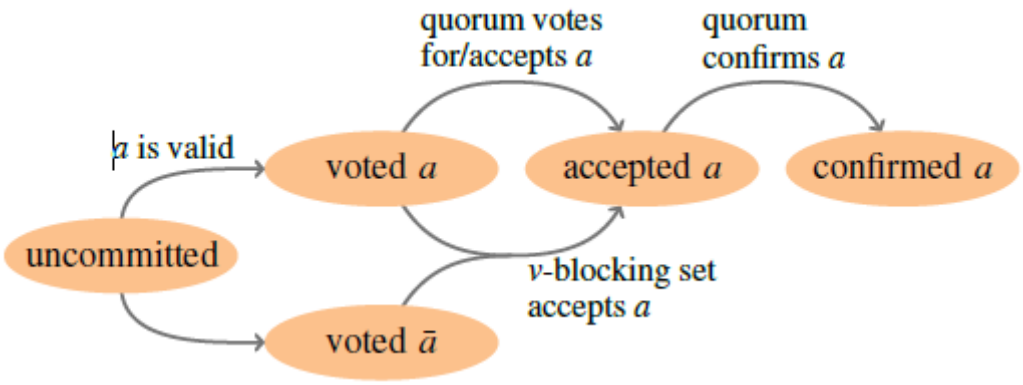
4.9.1 Διαδικασία εκτέλεσης ψηφοφορίας του SPC πρωτοκόλλου

Η διαδικασία εκτέλεσης του FBA πρωτοκόλλου συναίνεσης εκτελείται σε τρία στάδια: Αρχική Ψηφοφορία (Initial Voting), Αποδοχή (Acceptance) και επιβεβαίωση (Confirm) [63].

Στο πρώτο στάδιο κάθε κόμβος ψηφίζει μία αξία ή απόφαση ανάμεσα σε μία λίστα υποψήφιων αξίων (candidate set). Η ψήφος του εκάστοτε κόμβου θα αλλάξει μόνο στην περίπτωση που δεν συμφωνεί με την πλειοψηφία των ψήφων που περιέχετε στο δικό του quorum slice.

Στο επόμενο στάδιο (αποδοχή) ένας κόμβος αποδέχεται μια αξία ή απόφαση εάν δεν έχει ποτέ αποδεχτεί μια αντικρουόμενη σε σχέση με την τωρινή του απόφαση, και αν οι κόμβοι του V-blocking που ανήκει συμφωνούν με την απόφαση αυτή. Ένα σετ V-blocking κόμβων αποτελείται από τους κόμβους κάθε πιθανού quorum slice που ανήκει ο κόμβος με την επιλεγμένη προς αποδοχή απόφαση, κάτι που είναι δυνατό μέσω τις διασταύρωσης των quorums (quorum intersection) [64]. Τα Quorum slices αλληλοεπηρεάζονται οδηγώντας τους κόμβους να συμφωνήσουν σε μία αξία δημιουργώντας έτσι ένα Quorum.

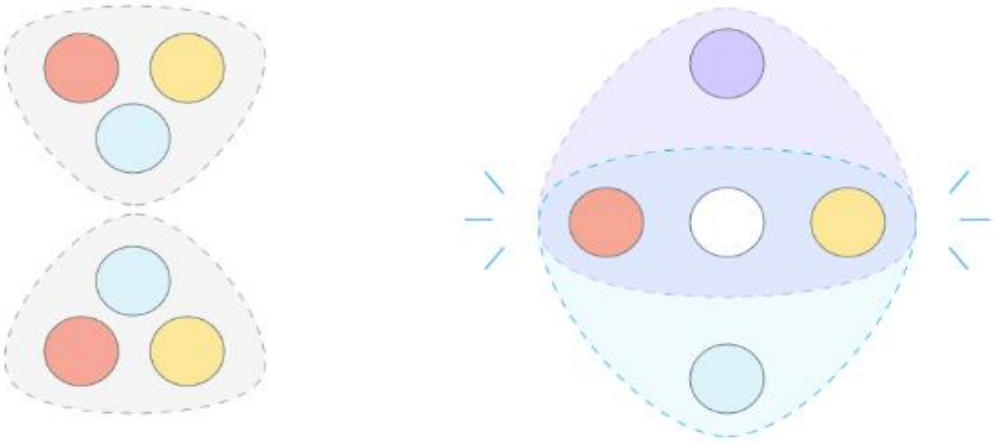
Στο τελευταίο βήμα της διαδικασίας ψηφοφορίας (επιβεβαίωση) επιβεβαιώνεται πως υπάρχει ομοφωνία στο δίκτυο μέσω εναλλαγής μηνυμάτων ανάμεσα σε όλους τους κόμβους του δικτύου ώστε η τελική απόφαση να ληφθεί συνολικά από το δίκτυο.



Εικόνα 12 Διάγραμμα μιας επιτυχημένα επικυρωμένης και επιβεβαιωμένης αξίας [63]

4.9.2 Διασταύρωση Quorum

Η διασταύρωση των Quorum (Quorum intersection) θεωρείται βασική ιδιότητα στο SCP πρωτόκολλο ώστε να μπορέσει να λειτουργήσει αποδοτικά η διαδικασία ψηφοφορίας. Ένα δίκτυο με αυτήν την ιδιότητα εξασφαλίζει πως κάθε δύο πιθανά quorums θα έχουν τουλάχιστον έναν κόμβο που ανήκει και στα δύο [65]. Κάτι τέτοιο σημαίνει πως τα δύο αυτά quorums πρέπει αναγκάστηκα να συμφωνούν καθώς ένας κόμβος δεν μπορεί να λάβει παραπάνω από μία αποφάσεις για διαφορετικά quorums.



Εικόνα 13 Αριστερά: 2 ξεχωριστά Quorums, Δεξιά; Quorum intersection [64]

Όσον αφορά την ταχύτητα εκτέλεσης των συναλλαγών το Stellar δείχνει παρόμοιά αποτελέσματα με το Ripple. Παρατηρείται πως μια συναλλαγή εκτελείται περίπου κάθε 3-5 δευτερόλεπτα με τον συνολικό αριθμό συναλλαγών το δευτερόλεπτο να ξεπερνάει σε αρχικά στάδια τις 1000 ταυτόχρονες συναλλαγές [66].

4.10 Ο αλγόριθμος συναίνεσης Paxos

Το Paxos [51] είναι ένα από τα βασικά πρωτόκολλα συναίνεσης για κατανεμημένα συστήματα, το οποίο δημιουργήθηκε από τον Leslie Lamport. Σε ένα σύστημα Paxos που αποτελείτε από μια ομάδα κόμβων, ο κάθε κόμβος προτείνει μια διαφορετική τιμή ή αξία (value). Σκοπός του αλγορίθμου είναι να σιγουρευτεί πως θα επιλεχτεί μια μόνο από τις προτεινόμενες τιμές η οποία θα είναι κοινώς αποδεκτή σε όλο το σύστημα. Όταν μια τιμή επιλεχτεί πρέπει να γίνει γνωστή σε όλους τους κόμβους του συστήματος. Για την ομαλή και ασφαλή λειτουργία του αλγορίθμου πρέπει να τηρούνται οι τρεις παρακάτω βασικές προϋποθέσεις:

- Μόνο μια αξία που έχει προταθεί από έναν κόμβο μπορεί και να επιλεχθεί.
- Μόνο μία αξία μπορεί τελικά να επιλεχθεί και να εκτελεστεί ανά κάθε γύρο εκτέλεσης του αλγορίθμου.
- Ένας κόμβος δεν γνωρίζει ποια αξία έχει επιλεχτεί έως ότου αυτή επιλεχτεί και γίνει αποδεκτή.

Η απλή εκδοχή του Paxos που αναφέρεται σε ένα σύστημα με περιορισμένους κόμβους λειτουργεί σε δύο ξεχωριστά στάδια. Οι κόμβοι ενός τέτοιου συστήματος χωρίζονται σε τρεις διαφορετικές κατηγορίες, η καθεμία με τον δικό της ρόλο για την επίτευξη επιλογής αξίας και ομοφωνίας στο σύστημα και είναι οι εξής: Προτείνων κόμβοι (Proposers), αποδέκτες κόμβοι (acceptors) και learners.

4.10.1 Διαδικασία επίτευξης ομοφωνίας

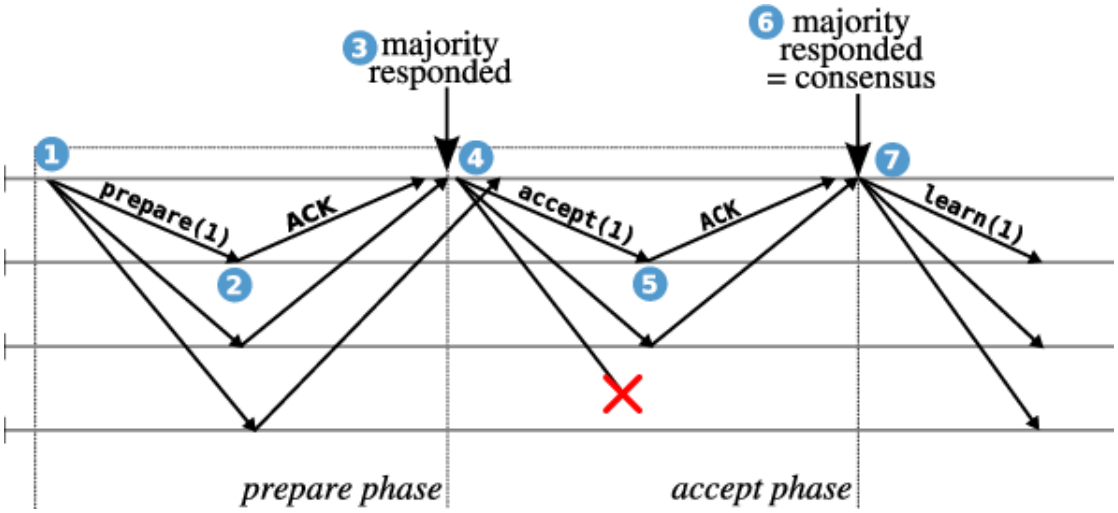
Η επίτευξη συναίνεσης στο Paxos βασίζεται στην πλειοψηφία για την λήψη αποφάσεων. Στην πρώτη φάση ο proposer στέλνει αίτημα στους χρήστες του συστήματος (acceptors) για να

εξασφαλίσει την πλειοψηφία. Πιο συγκεκριμένα στέλνει ένα μήνυμα Prepare το οποίο περιέχει τα στοιχεία του δηλαδή την ταυτότητα του που ορίζεται ως ένας αυξανόμενος ξεχωριστός για κάθε proposer αριθμός. Αν ο αύξοντας αριθμός που περιέχεται στο prepare μήνυμα του proposer είναι ο μεγαλύτερος που έχει λάβει ένας χρήστης (acceptor) , τότε ο acceptor απαντά με το μήνυμα promise το οποίο επιβεβαιώνει στον proposer πως δεν θα δεχτεί αιτήματα (proposals) από άλλους με μικρότερο αύξοντα αριθμό proposers. Κάτι τέτοιο σημαίνει πως ο proposer με τον μεγαλύτερο αύξοντα αριθμό θα είναι αυτός που θα μαζέψει την πλειοψηφία των χρηστών. Αν ένας acceptor έχει λάβει prepare μήνυμα με μικρότερο αύξοντα αριθμό, είναι υποχρεωμένος να ενημερώσει τον αποστολέα του πως υπάρχει proposer με μεγαλύτερο από αυτόν αύξοντα αριθμό [51].

Για να πραγματοποιηθεί η δεύτερη φάση αρχικά πρέπει ο proposer να έχει δεχτεί απάντηση στο αίτημα που έκανε στην πρώτη φάση από την πλειοψηφία των χρηστών. Στην συνέχεια ο proposer στέλνει ένα αίτημα στους acceptors που του έχουν απαντήσει με το μήνυμα accept το οποίο περιλαμβάνει μια προτεινόμενη αξία αλλά και τον αύξοντα αριθμό του proposer. Οι acceptors τότε ελέγχουν αν ο αύξοντας αριθμός του proposer είναι ακόμα ο μεγαλύτερος ανάμεσα στα αιτήματα που έχουν δεχτεί. Αν αυτό ισχύει τότε δέχονται αυτόν ως proposer, αποδέχονται την αξία που έχει προτείνει και τον ενημερώνουν για την απόφαση τους. Με αυτόν τον τρόπο λειτουργίας του αλγορίθμου επιτυγχάνεται κοινή συναίνεση ανάμεσα στους χρήστες του συστήματος και όλοι οι χρήστες ακολουθούν την απόφαση ή την αξία που πρότεινε ο proposer που επιλέχτηκε στις δύο φάσεις επιλογής του.

Είναι σημαντικό να σημειωθεί πως ένας proposer μπορεί να παρατήσει την διαδικασία της πρότασης οποιαδήποτε στιγμή, χωρίς να ξαναχρησιμοποιήσει όμως τον ίδιο αύξοντα αριθμό για μία πρόταση. Εάν ένας acceptor λάβει πρόταση με μικρότερο αύξοντα αριθμό την αγνοεί. Έπειτα ενημερώνει τον proposer που την έστειλε πως υπάρχει άλλος proposer με μεγαλύτερο αύξοντα αριθμό. Έτσι αποφεύγεται η άσκοπη συνέχιση της διαδικασίας του proposer με μικρότερο αύξοντα αριθμό καθώς δεν θα επιλεχθεί η δική του πρόταση και επιτυγχάνεται βελτίωση στην απόδοση του εκάστοτε συστήματος [67].

Η δουλεία των χρηστών Learners είναι να γνωρίζουν ποια πρόταση έχει γίνει αποδεκτή από την πλειοψηφία των χρηστών. Έτσι στο τέλος του γύρου εκτέλεσης του αλγορίθμου οι acceptors στέλνουν την πρόταση επιλέχτηκε από την πλειοψηφία σε όλους του Learners.



Εικόνα 14 Παράδειγμα ενός γύρου εκτέλεσης του BASIC Paxos αλγορίθμου. [69]

Στην παραπονώ εικόνα απεικονίζεται ένας γύρος του Paxos αλγορίθμου στην απλούστερη εκδοχή του (χωρίς να παρουσιαστεί πρόβλημα από κάποιον proposer ή acceptor). Όπως αναλύθηκε παραπάνω, αρχικά ένας proposer (1) στέλνει το μήνυμα prepare. Στην συνέχεια (2) οι acceptors απαντούν και στην βέλτιστη κατάσταση όπου η πλειοψηφία έχει απαντήσει (3) οι proposers στέλνουν το μήνυμα accept (4). Αφού η πλειοψηφία των acceptors ελέγξει την εγκυρότητα του proposer στο μήνυμα accept (5) , επιτυγχάνεται συναίνεση ανάμεσα στους χρήστες (6) και η αξία ή απόφαση του proposer είναι αυτή που επιλέγεται και εκτελείτε από όλο το σύστημα. Τέλος η απόφαση αυτή διαμοιράζεται σε όλο το σύστημα(7).

Αν και το Paxos θεωρείται σημείο αναφοράς και είναι συνώνυμο με την έννοια της κοινής συναίνεσης (consensus) έχει κάποια μεγάλα μειονεκτήματα. Αρχικά το ίδιο το πρωτόκολλο θεωρείται δύσκολο στην κατανόηση του μηχανισμού συναίνεσης με την πρώτη έκδοση που δημοσιεύτηκε[11], αν και έχουν γίνει μετέπειτα προσπάθειες από τον ίδιο τον Leslie Lamport [1] αλλά και από την λοιπή επιστημονική κοινότητα [68].

Ένα άλλο πρόβλημα είναι η υλοποίηση του πρωτοκόλλου σε εφαρμογές. Το βασικό πρωτόκολλο του Paxos δεν καλύπτει την πολυπλοκότητα συστημάτων που έχουν την ανάγκη για λήψη παραπάνω από μία αποφάσεις. Για τον λόγο αυτό ο Lamport σχεδίασε το multi-Paxos, πρωτόκολλο που εκτελεί παραπάνω από μία διεργασίες του Basic Paxos ταυτόχρονα πετυχαίνοντας έτσι λήψη πολλαπλών αποφάσεων. Το πρωτόκολλο όμως ακόμα παραμένει δύσκολο στην κατανόηση αν και έχουν γίνει προσπάθειές εφαρμογής του από κάποιες εφαρμογές.

Υλοποιήσεις του Paxos χρησιμοποιούνται για παράδειγμα από την google στην υπηρεσία Chubby, που λειτουργεί ως διακομιστής χρηστών (name server), εφαρμογή με απαίτηση από τους χρήστες να συμφωνούν για μια συγκεκριμένη διεργασία (κάτι που πετυχαίνει το Paxos) [69].

4.11 Ο αλγόριθμος συναίνεσης Raft

Το Raft είναι ένα πρωτόκολλο συναίνεσης το οποίο δημιουργήθηκε από τους Diego Ongaro και John Ousterhout το 2014 [10].Σκοπός του Raft είναι η επίτευξη ενός αλγόριθμου που θα αναπαράγει εντολές ενός 'πελάτη' (client) σε ένα σύστημα διακομιστών (server) με σκοπό την εκτέλεση τους υπό την συμφωνία της πλειοψηφίας των μελών του συστήματος. Οι δημιουργοί του Raft κατασκεύασαν έναν αντίστοιχο μηχανισμό με το Paxos, δομώντας και αναλύοντας το όμως με πιο κατανοητό τρόπο, με κίνητρο την ευκολότερη πρακτική εφαρμογή του μηχανισμού σε υλοποιήσεις συστημάτων βασιζόμενες σε αυτό.
Το Raft λειτουργεί μέσα σε ένα σύστημα από διακομιστές (servers) οι οποίοι διαθέτουν αρχεία καταγραφής (logs) και μηχανές κατάστασης (state machines). Μέσα σε ένα log αποθηκεύεται η εντολή του πελάτη με τελικό στόχο τον διαμοιρασμό στα logs όλων των servers. Μία μηχανή κατάστασης (state machine) μπορεί να είναι ένα μηχάνημά, ένα πρόγραμμα ή μια εφαρμογή που δέχεται εισόδους και παράγει εξόδους. Στόχος του state machine είναι να εκτελέσει την εντολή που βρίσκεται στο log αφού πρώτα υπάρχει ομοφωνία για αυτήν από την πλειοψηφία του δικτύου.
Για να γίνει δυνατή η επίτευξη κοινής συναίνεσης το Raft υιοθετεί έναν μηχανισμό εκλογής ηγέτη ή ηγετικού κόμβου (leader) του οποίου το καθήκον να επιβλέπει και να διαχειρίζεται τα αναπαραγόμενα καταγεγραμμένα αρχεία (replicated logs). Ο ηγέτης δέχεται τις εντολές των πελατών (καταχωρήσεις καταγραφής) ή log entries και είναι αυτός που τοποθετεί τις εντολές στα logs των servers. Δεν γίνεται να λειτουργούν ταυτόχρονα παραπάνω από ένας ηγέτες. Σε περίπτωση αποτυχίας ή αποσύνδεσης του υπάρχοντος εκλέγεται νέος.
Το πρωτόκολλο δημιουργήθηκε για συστήματα με προκαθορισμένο αριθμό μελών. Οι servers κατά την εκτέλεση του αλγορίθμου ανήκουν σε μία από τις τρείς παρακάτω κατηγορίες αναλόγως με τον ρόλο τους:

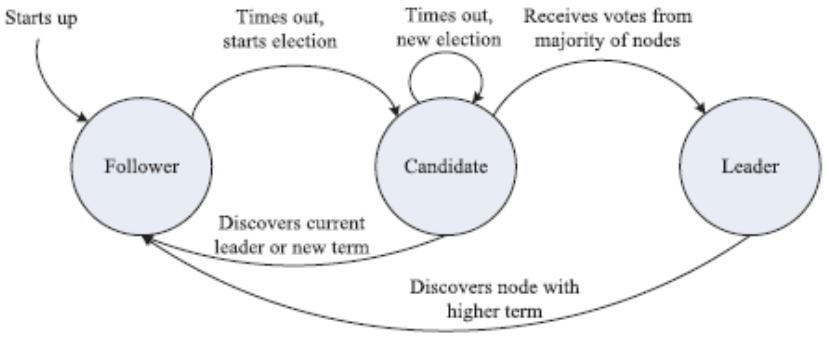
- Ηγέτες ή ηγετικοί κόμβοι (Leaders): Ο ηγέτης διαχειρίζεται όλες τις αλληλεπιδράσεις του συστήματος, τα replicated logs,
- Ακόλουθοι (Followers): Παθητικοί servers, περιμένουν RPCs (remote procedure calls) από τον leader,
- Υποψήφιοι (Candidates): Υποψήφιοι προς εκλογή leaders.

Το Raft χωρίζει τα χρονικά διαστήματα σε όρους (terms), οι οποίοι αριθμούνται διαδοχικά με ακέραιους αριθμούς. Κάθε γύρος ξεκινά ,με σκοπό την εκλογή ηγέτη και τελειώνει με την εκτέλεση της εντολής που δόθηκε. Σε περίπτωση μη εκλογής ηγέτη η διαδικασία ξεκινά από την αρχή με νέο όρο. Για τον εντοπισμό ανενεργών ή μη ενημερωμένων ηγετών κάθε server αποθηκεύει τον πιο πρόσφατο όρο του (current term). Το νούμερο του όρου καθορίζει την πιο πρόσφατη λαμβανόμενη απόφαση και είναι βοηθητικό σε περίπτωσης αντίκρουσης δύο ή παραπάνω server.
Η επικοινωνία σε ένα Raft σύστημα πραγματοποιείται μόνο μέσω 2 ειδών κλήσεων απομακρυσμένης διαδικασίας (remote procedure call ή RPC).Τα RequestVote RPCs, τα οποία χρησιμοποιούνται από τους candidates κατά την διαδικασία εκλογών leader, και τα AppendEntries RPCs τα οποία χρησιμοποιούνται από τους leaders για την αναπαραγωγή των

log entries σε όλους τους servers αλλά και για να στέλνουν περιοδικές ειδοποιήσεις πως είναι ακόμα ενεργοί ή πως εκλέχθηκαν και λειτουργούν ως leader (heartbeat) [70].

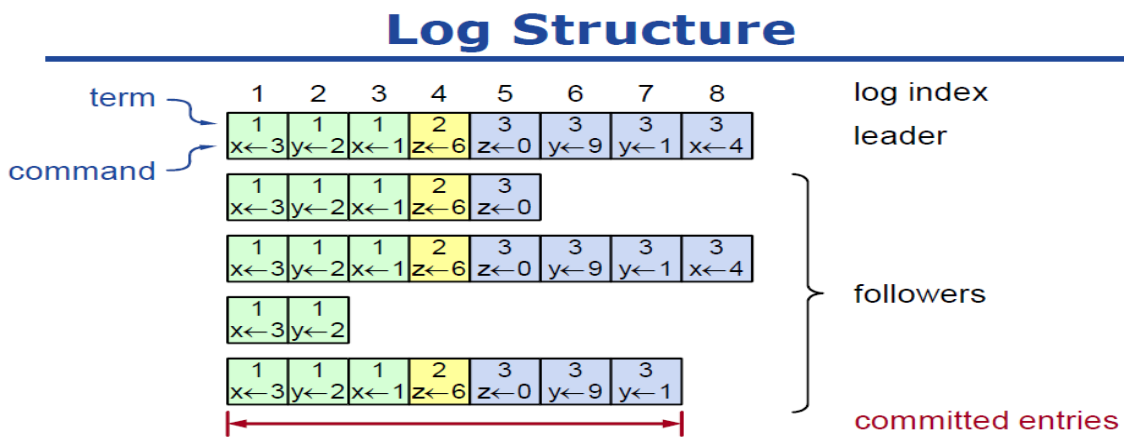
4.11.1 Διαδικασία εκλογής ηγετικού κόμβου

Για να υπάρξει εκλογική περίοδος πρέπει ο ως τώρα ηγετικός κόμβος να μην δίνει σημάδια ζωής ή αλλιώς heartbeat για ένα προκαθορισμένο διάστημα. Όταν περάσει αυτό το διάστημα οι υπόλοιποι κόμβοι υποθέτουν πως δεν υπάρχει ενεργός Leader και ξεκινούν νέα διαδικασία εκλογής. Η διαδικασία ξεκινά με όλους τους servers στον ρόλο του ακόλουθου. Για να αλλάξει την κατάσταση του ένας server σε υποψήφιος αυξάνει το current term του, ψηφίζει τον εαυτό του και στέλνει RequestVote RPCs στους servers όλου του συστήματος. Ο υποψήφιος παραμένει στη ίδια κατάσταση έως ότου είτε νικήσει και εκλεγεί ηγέτης, είτε ειδοποιηθεί πως άλλος ηγετικός κόμβος διαχειρίζεται το σύστημα ή εάν τέλικά περάσει ένα προκαθορισμένο διάστημα και δεν υπάρξει νικητής σε αυτήν την εκλογική περίοδο (χρονικό time out που ποικίλει 100-500ms αναλόγως την εφαρμογή).
Αν ο υποψήφιος λάβει την πλειοψηφία των ψήφων εκλέγεται ως ο ηγέτης του παρόντος όρου και στέλνει heartbeat σε όλους τους servers για δηλώσει τον ρόλο του ως ηγετικός κόμβος και να αποτρέψει την συνέχει της ψηφοφορίας στον παρόν όρο. Σε περίπτωση που ο υποψήφιος δεχτεί AppendEntries RPC από άλλον server ο οποίος υποστηρίζει πως είναι ηγέτης και τον όρο του ηγέτη αυτού είναι ίσο ή μεγαλύτερο (παρομοίως με το Paxos) από του υποψηφίου τότε ο υποψήφιος αλλάζει την κατάστασή του σε ακόλουθος. Τέλος αν περάσει το προκαθορισμένο χρονικό διάστημα που δίνεται από το σύστημα για την εκλογή λόγω διαμοιρασμού των ψήφων ανάμεσα στους υποψήφιους και δεν υπάρξει πλειοψηφία η διαδικασία εκλογής ξεκινά με νέο όρο.



Εικόνα 15 Σύνοψη διαδικασιών του Raft αλγορίθμου [73]

Όταν τελικά εκλεγεί νέος ηγέτης αυτός στέλνει με AppendEntries RPCs τις εντολές που δέχεται από τους πελάτες στα log των server που του έδωσαν την πλειοψηφία. Αφού σιγουρευτεί πως τα logs έχουν αναπαραχθεί επιτυχώς σε όλους του servers η εντολή που δόθηκε εκτελείται από τα state machines παραχωρώντας το αποτέλεσμά της στον πελάτη. Πρέπει να σημειωθεί εδώ πως σε περίπτωση που ο ηγέτης ανακαλύψει server με μεγαλύτερο όρο πρέπει να αλλάξει την κατάστασή του σε ακόλουθος, κάτι που μπορεί να προκληθεί σε περίπτωση που ένας ηγέτης απέτυχε να μείνει ενεργός και όταν επανήλθε στο σύστημα είχε ήδη εκλεχθεί ηγέτης με μεγαλύτερο όρο.

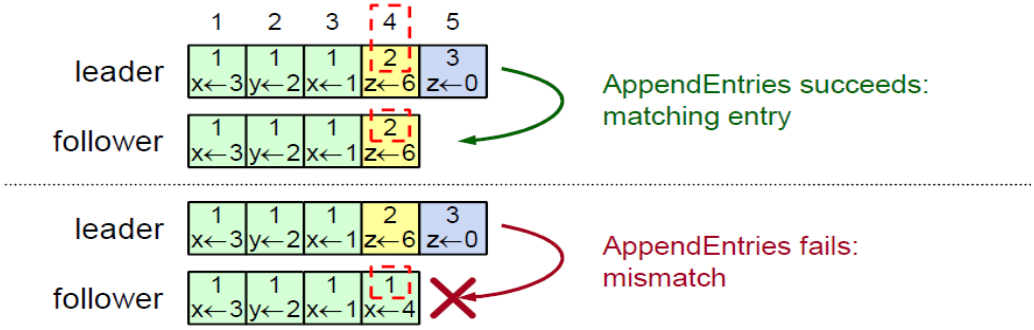


Εικόνα 16 Δομή των αρχείων καταγραφών (Log Structure) [72]

Παραπάνω φαίνεται μια απεικόνιση της δομή των logs τα οποία στοιχίζονται ανά όρους με περιεχόμενο τον αριθμό του τρέχοντος όρου και την προς εκτέλεση εντολή που δίνεται σαν είσοδος από τον πελάτη.

Πιο συγκεκριμένα το log index αναφέρεται στο ποσό των καταγεγραμμένων όρων ξεκινώντας από το 1, το term είναι ο αυξανόμενος όρος που έχει ο ηγέτης του γύρου αυτού και τέλος το command είναι η προς εκτέλεση εντολή. Η αλλαγή του χρώματος με την αύξηση του όρου υποδεικνύει πως έχει εκλεχθεί νέος ηγέτης με τον αριθμό του όρου αυτού στον συγκεκριμένο γύρο.

Πολύ σημαντικός παράγοντας σε ένα τέτοιο σύστημα είναι η ομοιότητα των logs των ηγέτης με τους ακόλουθους. Είναι δουλεία του ηγέτη να διατηρεί ομοιομορφία μέσα στο σύστημα σε περίπτωση πιθανής έλλειψης περιεχομένου στα logs οποιουδήποτε server, σε περίπτωση ύπαρξης παραπάνω σε αριθμό logs σε έναν server ή τέλος σε περίπτωση που το log ενός server δεν συμφωνεί με αυτό του ηγέτη.



Εικόνα 17 The Raft Consensus Algorithm Diego Ongaro and John Ousterhout, Stanford University [72]

Για να είναι σίγουρος ο ηγέτης για την ομοιότητα του log του με αυτό των ακόλουθων ο αλγόριθμος ενσωματώνει ένα βήμα το οποίο ελέγχει την ομοιότητα των logs. Πρακτικά καθώς τα AppendEntries RPCs περιέχουν τον όρο αλλά και το log index των διακομιστών, ελέγχουν για ασυνέπειες ανάμεσα μεταξύ του log του leader και των follower του.

Σε σχέση με το Paxos το Raft [71] θεωρείται πιο κατανοητό, για αυτόν τον λόγο και οι υλοποιήσεις του Raft είναι περισσότερες. Όσον αφορά υλοποίησης του Raft στον κόσμο του Blockchain παρατηρούμε πως συνήθως Raft-based συστήματα υιοθετούνται από ιδιωτικά blockchain, καθώς το πρωτόκολλο βέλτιστα για μικρό και προκαθορισμένο αριθμό κόμβων όπου η εμπιστοσύνη μεταξύ τους είναι απαραίτητη. Κάτι τέτοιο είναι απαραίτητο καθώς το Raft δεν αντιμετωπίζει τις αποτυχίες λόγω κακόβουλων κόμβων (Byzantine Fault Tolerance Failures) αλλά μόνο τις αποτυχίες λόγω κακής επικοινωνίας μεταξύ κόμβων, αποτυχίας του λογισμικού ή και των εξαρτημάτων που εκτελούν τον αλγόριθμο (Crash Fault Tolerance).
Για παράδειγμα Raft χρησιμοποιείται από την εφαρμογή Quorum [72], ένα Ethereum-based πρωτόκολλο, ως εναλλακτική λύση στο PoW πρωτόκολλο του. Το πρωτόκολλο λειτουργεί ταυτόχρονα με το Ethereum καθώς ο ηγέτης θεωρείται ο κόμβος που παράγει νέα blocks και διαχειρίζεται τις συναλλαγές χωρίς όμως την χρήση υπολογιστικών διεργασιών για απόδειξη εργασίας.

4.12 Πίνακας Συγκρίσεων βασικών χαρακτηριστικών των κύριων Μηχανισμών Συναίνεσης.

Στον παρακάτω πίνακα μπορείτε να δείτε συνολικά τα βασικά χαρακτηριστικά των κύριων μηχανισμών συναίνεσης.

Πίνακας 1 Πίνακας Συγκρίσεων βασικών χαρακτηριστικών των κύριων Μηχανισμών Συναίνεσης

	PoW	PoS	DPoS	LPoS	PBFT	RAFT	SCP	XPR (RPCA)	Tendermint
Επίπεδο Αποκέντρωσης	Απεκντρωτικό	Αποκεντρωτικό	Μερικώς αποκεντρωτικό	Αποκεντροτικό	Συγκεντρωτικό	Συγκεντρωτικό	Αποκεντρωτικό	Αποκεντρωτικό	Συγκεντρωτικό
Διαχείριση ταυτότητας κόμβου	Ανοιχτή/Γνωστή σε όλους	Ανοιχτή/Γνωστή σε όλους	Ανοιχτή/Γνωστή σε όλους	Ανοιχτή/Γνωστή σε όλους	Κατόπιν άδειας	Κατόπιν άδειας	Ανοιχτή/Γνωστή σε όλους	Ανοιχτή/Γνωστή σε όλους	Κατόπιν άδειας
Μοντέλο Συναίνεσης	Proof-based	Voted-based/ Proof-based	Proof-based	Voted-based/ Proof-based	Voted-based	Voted-based	Voted-based	Voted-based	Voted-based
Χρόνος πραγματοποίησης συναλλαγών ανά δευτερόλεπτο	3 με 6	11 με 13	EOS,BitShares περίπου 4000	Waves- 1000	Hyperledger-3500, Ziliqa-2000	Quorum-175-180	1000	1500	περίπου 8000
Χρόνος επιβεβαίωσης Συναλλαγών (Λεπτά)	60 (Bitcoin)	13 (Nxt)	Άμεσα (EOS.IO)	1 με 2 (Waves)	Σχεδόν άμεσο, μικρότερο απο 1 δευτερόλεπτο (HyperLedger)	Άμεσα	2 με 4 δευτερόλεπτα	4 δευτερόλεπτα	Άμεσα
Διαδικασία Δημιουργίας νέων block	Εξόρυξη(Mining) με χρήση hardware	Ποσοστό stake/ Coin age	Ποσοστό stake σε συνδυασμό με ψηφοφορία	Ποσοστό stake/Δυνατότητα 'δανεισμού' stake	Γύροι ψηφοφορίας	Γύροι ψηφοφορίας	Ομοσπονδιακή (Federated) ψηφοφορία	Πιθανολογική (PROBABYLISTIC) ψηφοφορία	Byzantine tolerant γύροι ψηφοφορίας
Ανεκτή ισχύς κακόβουλων κόμβων	25% υπολογιστικής ισχύς	50% του Stake	51% των επικυρωτών	50% του Stake	33,3% αναπαραγαγώμενων κόμβων	Βυζαντινούς κόμβους 0%,	Μεταβλητό	<20% κακόβουλων κόμβων του UNL	<33.3% Βυζαντινών κόμβων
Εξοικονόμηση ενέργειας	Μηδαμινή, υψηλή απαίτηση υπολογιστικών πόρων	Μερική,απαιτεί ελάχιστη κατανάλωση υπολογιστικών πόρων	Παρομοίως με PoS	Παρομοίως με PoS	Υψυλή	Υψηλή	Υψηλή	Υψηλή	Υψηλή
Οριστικότητα συναλλαγών	Πιθανολογική	Πιθανολογική	Πιθανολογική	Πιθανολογική	Σίγουρη	Σίγουρη	Σίγουρη	Σίγουρη	Σίγουρη
Επεκτασιμότητα στον αριθμό των κόμβων	Υψηλή (Χιλιάδες κόμβοι)	Υψηλή (Χιλιάδες κόμβοι)	Υψηλή (Χιλιάδες κόμβοι)	Υψηλή (Χιλιάδες κόμβοι)	Χαμηλή	Χαμηλή	Χαμηλή	Μεταβλητή	Χαμηλή
Εμπιστοσύνη μεταξύ κόμβων	Δεν απαιτείται εμπιστοσύνη	Δεν απαιτείται εμπιστοσύνη	Απαιτείται εμπιστοσύνη στους Delegates	Απαιτείται εμπιστοσύνη μεταξύ δανειζόμενου και δανειστή	Απαιτείται εμπιστοσύνη για ομόφωνη λήψη αποφάσεων	Απαιτείται εμπιστοσύνη για ομόφωνη λήψη αποφάσεων	Απαιτείται εμπιστοσύνη μεταξύ quorum, quorums slices	Απαιτείται εμπιστοσύνη μεταξύ UNL	Απαιτείται εμπιστοσύνη για ομόφωνη λήψη αποφάσεων
Παράδειγμα εφαρμογής	Bitcoin, Etereum	Nxt, Cardano	EOS,NEO	Waves, Sharering	Hyperledger, Ziliqa	Quorum	STELLAR	RIPPLE	Tendermint

5 Τύποι Blockchain Συστημάτων

Η τεχνολογία Blockchain είναι άμεσα συνδεδεμένη με συστήματα που έχουν κυρίως δημόσιο και αποκεντρωτικό χαρακτήρα ως προς την διαχείριση των δεδομένων τους. Παρόλα αυτά με το πέρασμα του χρόνου, την εξέλιξη της τεχνολογίας αλλά και τις ανάγκες των εφαρμογών blockchain δημιουργήθηκαν συστήματα που διαφέρουν στον αρχικό αποκεντρωτικό χαρακτήρα τους. Ανάλογα με τις ανάγκες τις εκάστοτε εφαρμογής τα συστήματα αυτά χωρίζονται σε τρεις κατηγορίες: Δημόσια (Public/Permissionless) , Ιδιωτικά (Private/Permissioned) και κοινοπρακτικά (consortium)[1]. Η κατηγοριοποίηση αυτή βασίζεται κυρίως στην διαφορά των συστημάτων ως προς την ελεύθερη ή όχι πρόσβαση στο εκάστοτε δίκτυο , την δυνατότητα συμμετοχής στην διαδικασία κοινής συναίνεσης αλλά και στην γενικότερη ασφάλεια του συστήματος.

5.1 Δημόσια (Public) συστήματα Blockchain

Δημόσιο σύστημα Blockchain σημαίνει πως η πρόσβαση σε τέτοιου είδους δίκτυο είναι ελεύθερη για οποιονδήποτε θελήσει να γίνει μέλος του. Οποιοσδήποτε έχει την δυνατότητα τρέξει έναν κόμβο του δικτύου, να συμμετάσχει στην διαδικασία δημιουργίας νέων μπλοκ και να ανταμειφθεί αντίστοιχα, εφόσον τηρεί τους κανόνες του εκάστοτε συστήματος. Ακόμα αφού δημιουργηθεί νέο μπλοκ και εκτελεστεί η αντίστοιχη συναλλαγή αυτή διαμοιράζεται σε όλο το δίκτυο ούσα ορατή από όλους τους συμμετέχοντες κόμβους.

Πλεονέκτημα αυτού του είδους συστημάτων είναι η ιδιότητα της μη μεταβλητότητάς του. Πιο συγκεκριμένα καθώς οι συναλλαγές είναι γνωστές σε όλους, καθίσταται σχεδόν αδύνατη η παραβίαση και μετατροπή τους από κακόβουλους κόμβους. Από την άλλη καθώς στα δημόσια Blockchain απαιτείται μεγάλο χρονικό διάστημα ώστε να διαδοθεί μια νέα συναλλαγή, λόγω του μεγάλου πλήθους κόμβων, η αποδοτικότητα της ολοκλήρωσης των συναλλαγών μειώνεται.

Το βασικό χαρακτηριστικό που διαχωρίζει τα Δημόσια Blockchain συστήματα από τα δύο υπόλοιπα είναι πως τα Δημόσια θεωρούνται αποκεντροποιημένα, δηλαδή δεν υπάρχει κάποια κεντρική οντότητα η οποία κατέχει παραπάνω δικαιοδοσία και ελέγχει το σύστημα καθώς όλοι οι κόμβοι θεωρούνται ισάξιοι και ομότιμοι [16]. Τα δημόσια Blockchain συστήματα είναι ιστορικά τα πρώτα συστήματα στα οποία αρχικά βασίστηκε η τεχνολογία Blockchain στα ανοιχτά και αποκεντρωτικά χαρακτηριστικά τους για να δημιουργήσει τους πιο γνωστούς αλγόριθμους συναίνεσης όπως το PoW και το PoS. Γνωστές εφαρμογές αλγορίθμων που ακολουθούν τα δημόσια Blockchain είναι το Bitcoin και το Ethereum.

5.2 Ιδιωτικά (Private) Blockchain Συστήματα

Σε ένα Ιδιωτικό Blockchain σύστημα συνήθως ο ιδιοκτήτης του συστήματος (ένας οργανισμός η μία εταιρία) ή μια ομάδα κόμβων καθορισμένη από αυτόν είναι ο κύριος υπόλογος για την τελική λήψη αποφάσεων στο σύστημα. Πιο συγκεκριμένα ένα τέτοιο σύστημα θεωρείται κεντρικοποιημένο καθώς μια ομάδα κόμβων κατέχει την μέγιστη δικαιοδοσία στην τροποποίηση των δεδομένων της αλυσίδας [73]. Οι κόμβοι αυτοί είναι υπεύθυνοι για την διεξαγωγή των συναλλαγών στο δίκτυο. Βασικό χαρακτηριστικό αυτών των συστημάτων είναι πως η είσοδος σε νέους κόμβους πραγματοποιείται μόνο μέσω έγκρισης από την αρχή υπεύθυνή για τον καθορισμό ομοφωνίας στο σύστημα.

Για παράδειγμα στο Raft οι κεντρικοί κόμβοι τρέχουν τον αλγόριθμο συναίνεσης διεξάγοντας γύρους ψηφοφορίας για πραγματοποίηση νέων συναλλαγών υπό την επίβλεψη ενός ηγετικού κόμβου. Ο ηγετικός κόμβος ορίζεται από την κεντρική ομάδα κόμβων και μαζί του εκτελούν την διαδικασία ομοφωνίας. Επίσης είναι και αυτός που δίνει την άδεια σε κόμβους-πελάτες που χρησιμοποιούν την εφαρμογή για διεξαγωγή συναλλαγών, αρχικά να αιτούνται και έπειτα να πραγματοποιήσουν νέες συναλλαγές.

Οι πραγματοποιημένες συναλλαγές είναι ορατές σε όλους τους κόμβους μόνο αν αυτό επιτρέπεται τους κόμβους που τρέχουν την διεργασία ομοφωνίας του συστήματος. Το γεγονός αυτό σε συνδυασμό με τον μικρό αριθμό κόμβων που περιέχουν συνήθως τα ιδιωτικά Blockchain (σε σχέση με τα δημόσια) τους προσδίδει την ιδιότητα της μεταβλητότητας.

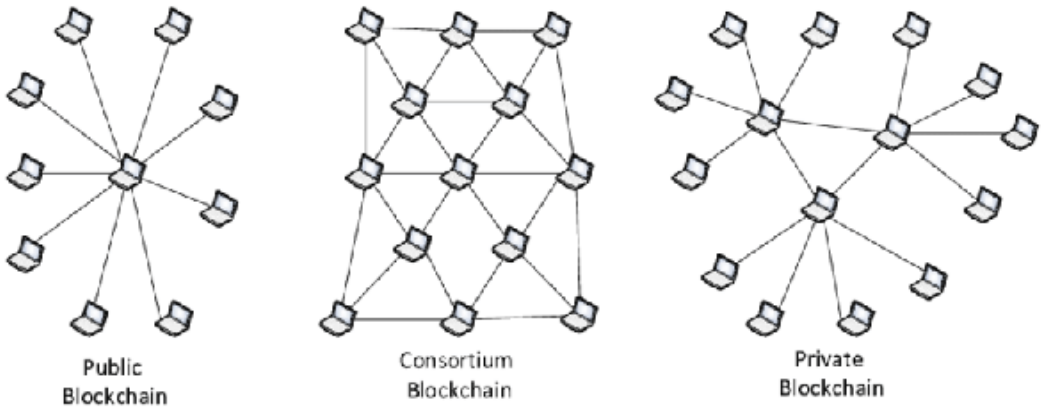
Ακόμα όσον αφορά την αποδοτικότητα του συστήματος τα ιδιωτικά Blockchain συστήματα θεωρούνται πιο ταχύτερα καθώς ο περιορισμένος αριθμός κόμβων που τα απαρτίζουν καθιστά την ολοκλήρωση των συναλλαγών αρκετά πιο σίγουρη και αποτελεσματική σε σχέση με τα Δημόσια [18]. Από τα παραπάνω γίνεται κατανοητό πως τα Ιδιωτικά Blockchain συστήματα χρησιμοποιούνται για εφαρμογές όπου η αποκέντρωση δεν παίζει σημαντικό ρόλο, δηλαδή σε περιπτώσεις που απαιτείται η επίβλεψη του συστήματος από έναν κεντρικό με ηγετικό ρόλο κόμβο. Αλγόριθμοι συναίνεσής που χρησιμοποιούνται σε ιδιωτικά συστήματα είναι το Raft και το PBFT με τις αντίστοιχες εφαρμογές τους Hyperledger Fabric, Ziliqa, Quorum.

5.3 Κοινοπρακτικά (Consortium) Blockchain Συστήματα

Κοινοπρακτικό σύστημα Blockchain θεωρείται ένα σύστημα στο οποίο ο αλγόριθμος κοινής συναίνεσης εκτελείται από προκαθορισμένους από το σύστημα κόμβους. Πληροφορίες για τα δεδομένα του συστήματος (π.χ. εκτελεσμένες συναλλαγές) μπορεί να είναι ορατές σε όλους τους κόμβους, αλλά συνήθως μόνο οι προκαθορισμένοι από το σύστημα κόμβοι έχουν την δυνατότητα να τα επεξεργαστούν και να επικυρώνουν συναλλαγές. Ανάλογα με την εφαρμογή σε πολλές περιπτώσεις μπορούν και οι μη προκαθορισμένοι κόμβοι να λάβουν μέρος στην διαδικασία επικύρωσης αλλά προτεραιότητα έχουν πάντα οι προκαθορισμένοι κόμβοι [74].

Παρομοίως με τα ιδιωτικά συστήματα η ολοκλήρωση των συναλλαγών θεωρείται πολύ πιο αποδοτική και σίγουρη λόγω των περιορισμένων κόμβων ενός κοινοπρακτικού συστήματος. Λόγω τις απαίτησης για μία μικρή ομάδα επικυρωτών , τα κοινοπρακτικά συστήματα είναι περιορισμένα στο πλήθος κόμβων, όπως τα ιδιωτικά μικραίνοντας έτσι και τις πιθανότητες για πρόσβαση σε κακόβουλους κόμβους. Ένα τέτοιο σύστημα θεωρείται μερικώς αποκεντρωτικό καθώς λειτουργεί με ένα υβριδικό μοντέλο που βασίζεται στα θετικά στοιχεία των δύο προαναφερθέντων μοντέλων

συστημάτων. Γνωστά κοινοπρακτικά συστήματα στον κόσμο του Blockchain θεωρούνται οι πλατφόρμες Ripple με τον αλγόριθμο συναίνεσης RPCA και Multichain [75].
Κανένα από τα τρία συστήματα δεν θεωρείται ανώτερο του αλλού καθώς η επιλογή ενός από τα τρία τους εξαρτάται από την εφαρμογή. Για παράδειγμα τα κοινοπρακτικά και τα ιδιωτικά συστήματα θεωρούνται κατάλληλα για οργανισμούς και επιχειρήσεις που απαιτούν έλεγχο των συμμετεχόντων κόμβων, παρέχοντας ταυτόχρονα γρηγορότερους χρόνους διεξαγωγής συναλλαγών σε σχέση με τα δημόσια. Από την άλλη τα δημόσια συστήματα λόγω του ανοιχτού προς το κοινό χαρακτήρα τους ελκύουν πληθώρα χρηστών για νέες εφαρμογές.



Εικόνα 18 Σχεδιάγραμμά των κόμβων για τα διαφορετικά συστήματα Blockchain [79]

5.4 Θεώρημα CAP

Το θεώρημα CAP το οποίο προτάθηκε από τον Eric Brewer, αναφέρεται σε τρεις βασικές ιδιότητες που πρέπει παρέχει να παρέχει ένα κατανεμημένο σύστημα. Πιο συγκεκριμένα αναφέρεται στο ότι ένα κατανεμημένο σύστημα πρακτικά μπορεί να έχει μόνο δυο από τις τρεις ιδιότητες ταυτόχρονα [76]. Οι ιδιότητες αναφέρονται ως εξής:

- Σταθερότητα/Συνεκτικότητα (Consistency): Όλοι οι χρήστες του συστήματος να κατέχουν τα πιο πρόσφατα εγγεγραμμένα δεδομένα στο σύστημα,
- Διαθεσιμότητα (Availability): Οι χρήστες θα είναι πάντα διαθέσιμοι στην ανταλλαγή πληροφοριών, χωρίς αποτυχίες αποστολής ή λήψης δεδομένων
- Ανοχή διαχωρισμού (Partition tolerance): Διασφαλίζει πως αν μία ομάδα κόβων αποσυνδεθεί ή αποτύχει να επικοινωνήσει με το υπόλοιπο δίκτυο το σύστημα θα συνεχίσει να λειτουργεί ορθά.

Όσον αφορά τον κόσμο του Blockchain το θεώρημα CAP ισχύει σε μεγάλο βαθμό παρομοίως με τα κατανεμημένα συστήματα και λειτουργεί ως εξής:
Αρχικά ο διαχωρισμός είναι εγγενές χαρακτηριστικό κάθε κατανεμημένου συστήματος, άρα η ιδιότητα της ανοχής διαχωρισμού θεωρείται δεδομένη. Έπειτα σαν την δεύτερη από τις τρεις ιδιότητες που συνήθως επιλέγονται παρατηρείται πως στις εφαρμογές Blockchain η Διαθεσιμότητα

επιλέγεται μαζί με την ανοχή διαχωρισμού. Κάτι τέτοιο γίνεται καθώς σε περίπτωση διαχωρισμού του δικτύου και μη ύπαρξης διαθεσιμότητας παραβιάζεται η διαδικασία συναίνεσης του συστήματος [77].

Η διαφορά των Blockchain συστημάτων είναι πως εξασφαλίζοντας την διαθεσιμότητα και την ανοχή διαχωρισμού, τελικά μέσω της διαδικασίας εκτέλεσης των αλγορίθμων συναίνεσης εξασφαλίζεται και η συνεκτικότητα [2].Κάτι τέτοιο γίνεται για παράδειγμα στο PoW μέσω του mining, ή μέσω των vote-based αλγορίθμων, χάρης στην επικύρωση των πιο πρόσφατων και ορθών συναλλαγών έπειτα από αρκετούς γύρους ψηφοφορίας.

5.5 Πίνακας σύγκρισης βασικών χαρακτηριστικών των τριών τύπων Blockchain συστημάτων

Πίνακας 2 ΣΥΣΓΚΡΙΣΗ ΒΑΣΙΚΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΤΩΝ ΤΡΙΩΝ ΤΥΠΩΝ BLOCKCHAIN ΣΥΣΤΗΜΑΤΩΝ

Σύστημα	ΔΗΜΌΣΙΟ	ΙΔΙΩΤΙΚΌ	ΚΟΙΝΟΠΡΑΚΤΙΚΌ
Ποσοστό κεντρικοποίησης	Μηδαμινό (Θεωρητικά)	Απόλυτο	Μεταβλητό, Μερικό
Συμμέτοχή στην διαδικασία κοινής συναίνεσης	Χωρίς άδεια	Απαιτείται άδεια	Απαιτείται άδεια
Μεταβλητότητά	Όχι	Ναι	Ναι
Ανωνυμία	Ναι	Όχι	Όχι
Αποδοτικότητα	Χαμηλή	Υψηλή	Υψηλή
Εμπιστοσύνη μεταξύ κόμβων	Όχι	Ναι	Μερική
Δυνατότητα Ελέγχου	Μηδαμινή	Απόλυτη	Μερική
Αλγόριθμοι συναίνεσης	Συνήθως PoS, PoW	PBFT, RAFT PoS κ.α	Εξαρτάται από την εφαρμογή (πχ Ripple)
Παράδειγμα εφαρμογής	Ethereum, Bitcoin	Quorum, Hyperledger Fabric	Ripple

Επίλογος

Η τεχνολογία Blockchain έγινε ευρέως γνωστή τα τελευταία χρόνια μέσω των κρυπτο-νομισμάτων. Αρχικά το Blockchain ταυτίστηκε με την πραγματοποίηση συναλλαγών σε δίκτυα ομότιμων κόμβων με αποκεντρικοποιημένο χαρακτήρα. Όμως όπως είδαμε και μέσα από την ανάλυση των μηχανισμών συναίνεσης η τεχνολογία αυτή είναι ικανή να ανταπεξέλθει και σε άλλα πεδία εκτός τον οικονομικού, έχοντας την δυνατότητα εφαρμογής σε μεγάλο εύρος του επιστημονικού τομέα. Για να γίνει κάτι τέτοιο αρκεί να διαμορφωθεί ο αναγκαίος μηχανισμός συναίνεσης που θα ανταποκρίνεται στις ανάγκες της εκάστοτε εφαρμογής.

Ο ενθουσιασμός που περιτριγυρίζει την έρευνα στον κόσμο του Blockchain, αλλά και οι προσδοκώμενες δυνατότητες των πλατφορμών που το χρησιμοποιούν, το καθιστούν παράγοντα που θεωρείται πως θα αλλάξει ριζικά τα πράγματα όπως είναι τώρα στην επιστημονική κοινότητα με επέκταση την μαζική τεχνολογία στην καθημερινότητά μας.

Με την διπλωματική αυτή προσπαθήσαμε να αναλύσουμε τους κύριους μηχανισμούς συναίνεσης που διέπουν σήμερα την τεχνολογία Blockchain αλλά και να δείξουμε την προσαρμοστικότητα των μηχανισμών αυτών αναλόγως με το πεδίο και την εφαρμογή που υπηρετούν.

Βιβλιογραφία

[1] R. Maull, R. Maull, C. Mulligan, A. Brown και B. Kewell, «Distributed ledger technology: Applications DOI: 10.1002/jsc.2148».*WILEY*.

[2] I. Bashir, Mastering Blockchain Distributed ledgers, decentralization and smart contracts explained, Livery Place 35 Livery Street Birmingham: Packt Publishing Ltd., 2017.

[3] M. Hearn και R. Brown, «Corda: A distributed ledger,» 20 August 2019.

[4] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» *www.cryptovest.co.uk,* 31 October 2008.

[5] «Ethereum Whitepaper,» [Ηλεκτρονικό]. Available: https://ethereum.org/en/whitepaper/.

[6] «el.wikipedia.org/Peer-to-peer,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Peer-to-peer.

[7] R. Schollmeier, «Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications,» Miinchen, Germany.

[8] M. Ripeanu, «Peer-to-Peer Architecture Case Study: Gnutella Network».

[9] «www.orosk.com/client-server-topology,» pp. http://www.orosk.com/client-server-topology.

[10] D. Ongaro και J. Ousterhout, «In Search of an Understandable Consensus Algorithm,» σε *2014 USENIX Annual Technical Conference*, 19-20, 2014, p. June.

[11] M. Castr και B. Liskov, «Practical Byzantine Fault Tolerance,» σε *Operating Systems Design and Implementation*, 1999.

[12] V. Buterin, «medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274#0387,» 6 February 2017. [Ηλεκτρονικό]. Available: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274#0387.

[13] L. LAMPORT, R. SHOSTAK και M. PEASE, «The Byzantine Generals Problem,» *ACM Transactions on Programming Languages and Systems,* 3 July 1982.

[14] BGP, «gauthamzz.github.io/tendermint.html,» [Ηλεκτρονικό]. Available: https://gauthamzz.github.io/tendermint.html#byzantine-fault-tolerant.

[15] «The cryptographic hash function SHA-256».*CRIPTOGRAFIA MAII - FIB.*

[16] Z. Zheng, S. Xie, H. Dai, X. Chen και a. H. Wang, «An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends,» *IEEE 6th International Congress on Big Data*, 2017.

[17] B. a. M. Z. L.M.Bach, «Comparative Analysis of Blockchain Consenus Algorithms,» *MIPRO 2018, Opatijs Croatia,* 21-25 May 2018.

[18] D. Mingxiao*, M. Xiaofeng*, Z. Zhe*, W. Xiangwei* και C. Qijun*, «A Review on Consensus Algorithm of Blockchain,» *IEEE International Conference on Systems, Man, and Cybernetics (SMC) Banff Center, Banff, Canada,* 5-8 October 2017.

[19] «bitcoinx.gr,» 2020. [Ηλεκτρονικό]. Available: https://bitcoinx.gr/mining-pools/.

[20] A. Baliga, «Understanding Blockchain Consensus Models,» *Persistent Systems (BSE & NSE: PERSISTENT),* April 2017.

[21] A. Wahab και W. Mehmood, «Survey of Consensus Protocols,» *https://arxiv.org/abs/1810.03357v1,* 8 October 2016.

[22] «thenextweb.com/hardfork/2019/08/05/ugh-this-is-what-bitcoins-hash-rate-means-and-why-it-matters/,» 5 August 2019. [Ηλεκτρονικό]. Available: https://thenextweb.com/hardfork/2019/08/05/ugh-this-is-what-bitcoins-hash-rate-means-and-why-it-matters/.

[23] S. King και S. Nadal, «PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,» 19 August 2012.

[24] L. Wenting, A. S´ebastien, Bohli, Jens-Matthias και K. Ghassan, Securing Proof-of-Stake Blockchain Protocols, DOI: 10.1007/978-3-319-67816-0 17: Springer International Publishing, 2017.

[25] D. Pike, P. Nosker, D. Boehm, D. Grisham, S. Woods και J. Marston, Vericoin/ Proof of stake.

[26] CLOAK, ENIGMA A PR IVATE , SECURE AND UNTRACEABLE TRANSACTION SYSTEM FOR CLOAKCOIN V 2.1, 2018.

[27] novacoin, «/github.com/novacoin-project/novacoin/wiki,» [Ηλεκτρονικό]. Available: https://github.com/novacoin-project/novacoin/wiki.

[28] «github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#how-does-proof-of-stake-fit-into-traditional-byzantine-fault-tolerance-research,» [Ηλεκτρονικό]. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#how-does-proof-of-stake-fit-into-traditional-byzantine-fault-tolerance-research.

[29] «github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#so-how-does-this-relate-to-byzantine-fault-tolerance-theory,» [Ηλεκτρονικό]. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#so-how-does-this-relate-to-byzantine-fault-tolerance-theory.

[30] «nxtdocs.jelurida.com/Nxt_Whitepaper,» [Ηλεκτρονικό]. Available: https://nxtdocs.jelurida.com/Nxt_Whitepaper.

[31] V. Buterin και V. Griffith, «Casper the Friendly Finality Gadget,» 22 January 2019.

[32] V. Buterin, «https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/,» 15 January 2014. [Ηλεκτρονικό]. Available: https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/.

[33] D. Won, «www.exodus.io/blog/ethereum,» [Ηλεκτρονικό]. Available: https://www.exodus.io/blog/ethereum-proof-of-stake-date/.

[34] P. Vasin, «BlackCoin's Proof-of-Stake Protocol v2».*www.blackcoin.co.*

[35] J. Chen και S. Micali, «Algorand,» 26 May 2017.

[36] Y. Gilad, R. Hemo, S. Micali, G. Vlachos και N. Zeldovich, «Algorand: Scaling Byzantine Agreements for Cryptocurrencies».

[37] «POSITIVE.COM/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9,» 31 May 2018. [Ηλεκτρονικό]. Available: https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9.

[38] F. YANG, W. ZHOU, Q. WU, R. LONG, N. N. XIONG και M. ZHOU, «Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism,» *IEEE Access SPECIAL SECTION ON EMERGING APPROACHES TO CYBER SECURITY,* 30 June 2019.

[39] Foundation και BitShares, «how.bitshares.works,» 2019. [Ηλεκτρονικό]. Available: https://how.bitshares.works/en/master/technology/dpos.html.

[40] «www.mycryptopedia.com/delegated-proof-stake-dpos-explained/,» 1 November 2018. [Ηλεκτρονικό]. Available: https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/.

[41] «steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper,» 2017. [Ηλεκτρονικό]. Available: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper.

[42] «bitshares.org/technology/delegated-proof-of-stake-consensus/,» [Ηλεκτρονικό]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

[43] M. Gagnebin, «lisk.io/blog/research/3-new-dpos-lips-changing-voting-system-lisk,» 30 September 2019. [Ηλεκτρονικό]. Available: https://lisk.io/blog/research/3-new-dpos-lips-changing-voting-system-lisk.

[44] I. Grigg, «EOS,» Creative Commons Attribution 4.0 International License (CC BY).

[45] bitshares.org, «bitshares.org/technology/delegated-proof-of-stake-consensus/,» [Ηλεκτρονικό]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

[46] Waves, «wavesprotocol.org,» [Ηλεκτρονικό]. Available: https://docs.wavesprotocol.org/en/blockchain/leasing#leasing-benefits-for-the-node-owner.

[47] T. BOS, R. L. PAGE, T. TRA και T. DO, «LEASED PROOF-OF-STAKE/SHARERING,» 2019.

[48] E. Buchman, «Tendermint: Byzantine Fault Tolerance in the Age of Blockchains,» June 2016.

[49] W. Y. M. M. Thin, N. Don, G. Bai και J. S. Dong, «Formal Analysis of a Proof-of-Stake Blockchain,» International Conference on Engineering of Complex Computer Systems (ICECCS), 2018.

[50] «medium.com/thundercore/consensus-series-pbft-3e011e7f3691,» 2019. [Ηλεκτρονικό]. Available: https://medium.com/thundercore/consensus-series-pbft-3e011e7f3691.

[51] L. Lamport, «Paxos Made Simple,» 1 November 2001.

[52] C. Cachin, «Architecture of the Hyperledger Blockchain Fabric,» *cca@zurich.ibm.com,* July 2016.

[53] «Hyperledger Whitepaper,» [Ηλεκτρονικό]. Available: https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/edit#heading=h.m6iml6hqrnm2.

[54] J. FRANKENFIELD, «investopedia.com,» 2019. [Ηλεκτρονικό]. Available: https://www.investopedia.com/terms/s/smart-contracts.asp.

[55] «The ZILLIQA Technical Whitepaper,» *The ZILLIQA Team,* 1 August 2017.

[56] «medium.com/chainrift-research/bitcoins-attack-vectors-sybil-eclipse-attacks-d1b6679963e5,» 2018. [Ηλεκτρονικό]. Available: https://medium.com/chainrift-research/bitcoins-attack-vectors-sybil-eclipse-attacks-d1b6679963e5. [Πρόσβαση 26 November].

[57] D. XINSHU και J. YAOQI, «ZILLIQA NEXT GEN HIGH-THROUGHPUT BLOCKCHAIN PLATFORM».

[58] D. Schwartz, N. Youngs και A. Britto, «The Ripple Protocol Consensus Algorithm».

[59] F. Armknecht, G. Karame, A. Mandal, F. Youssef και E. Zenner, «Ripple: Overview and Outlook,» Springer International Publishing Switzerland, 2015.

[60] B. Chase και E. MacBrough, «Analysis of the XRP Ledger Consensus Protocol,» *@ripple.com,* 21 February 2018.

[61] «ripple.com/xrp/,» [Ηλεκτρονικό]. Available: https://ripple.com/xrp/.

[62] D. Mazières, «The Stellar Consensus Protocol A federated model for Internet-level consensus,» *Stellar Development Foundation,* 6 December 2017.

[63] S. D. Foundation, «medium.com,» 8 April 2015. [Ηλεκτρονικό]. Available: https://medium.com/stellar-development-foundation/on-worldwide-consensus-359e9eb3e949.

[64] L. S. Sankar, S. M και M. Sethumadhavan, «Survey of Consensus Protocols on Blockchain Applications,» *International Conference on Advanced Computing and Communication Systems (ICACCS -2017)*, 6-7 January 2017.

[65] B. Glickstein, «medium.com/interstellar/understanding-the-stellar-consensus-protocol-423409aad32e,» 13 May 2019. [Ηλεκτρονικό]. Available: https://medium.com/interstellar/understanding-the-stellar-consensus-protocol-423409aad32e.

[66] E. Posnak, «medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-stellar,» 3 February 2019. [Ηλεκτρονικό]. Available: https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-stellar-b19190b26776.

[67] L. Rajendran, «medium.com/@logeshrajendran/paxos-a9d76ebf04f3,» 15 May 2019. [Ηλεκτρονικό]. Available: https://medium.com/@logeshrajendran/paxos-a9d76ebf04f3.

[68] B. W. Lampson, «The ABCD's of Paxos,» 180 Lake View Ave Cambridge.

[69] Wikipedia, «en.wikipedia.org/wiki/Distributed_lock_manager,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Distributed_lock_manager.

[70] D. Ongaro και J. Ousterhout, «The Raft Consensus Algorithm,» October 2013.

[71] «raft.github.io/#implementations,» [Ηλεκτρονικό]. Available: https://raft.github.io/#implementations.

[72] Quorum-Raft, «docs.goquorum.com/en/latest/Consensus/raft/raft/,» [Ηλεκτρονικό]. Available: https://docs.goquorum.com/en/latest/Consensus/raft/raft/.

[73] 7sevencoin, «medium.com/types-of-blockchain-public-private-and-consortium-blockchain-e190604df820,» 14 June 2018. [Ηλεκτρονικό]. Available: https://medium.com/7sevencoin/types-of-blockchain-public-private-and-consortium-blockchain-e190604df820.

[74] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea και E. B. Hamida, «Consortium Blockchains: Overview, Applications and Challenges,» *International Journal on Advances in Telecommunications, vol 11 no 1 & 2,* 2018.

[75] G. Greenspan, «MultiChain Private Blockchain».

[76] E. Brewer, «infoq.com/cap-twelve-years-later-how-the-rules-have-changed,» 30 May 2012. [Ηλεκτρονικό]. Available: https://www.infoq.com/articles/cap-twelve-years-later-how-the-rules-have-changed/.

[77] K. Nelaturi, «www.mangoresearch.co,» 5 February 2018. [Ηλεκτρονικό]. Available: https://www.mangoresearch.co/understanding-blockchain-tech-cap-theorem/.

[78] «www.researchgate.net/figure/Comparison-of-network-architectures-Client-server-hybrid-P2P-real-P2P,» [Ηλεκτρονικό]. Available: https://www.researchgate.net/figure/Comparison-of-network-architectures-Client-server-hybrid-P2P-real-P2P-from_fig1_315677975.

[79] «cryptoslate.com/cryptos/proof-of-work,» [Ηλεκτρονικό]. Available: (https://cryptoslate.com/cryptos/proof-of-work/).

[80] «blockchain.com/el/charts/hash-rate?timespan=all,» [Ηλεκτρονικό]. Available: https://www.blockchain.com/el/charts/hash-rate?timespan=all.

Πίνακας Εικόνων

Πίνακας Πινάκων