ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ & ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΝΑΛΥΣΗ ΑΛΓΟΡΙΘΜΩΝ ΚΑΙ ΜΗΧΑΝΙΣΜΩΝ ΣΥΝΑΙΝΕΣΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αγγελόπουλος Ιωάννης

Επιβλέπουσα : Θεοδώρα Βαρβαρίγου

Αθήνα, Ιούλιος 2019

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ & ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΝΑΛΥΣΗ ΑΛΓΟΡΙΘΜΩΝ ΚΑΙ ΜΗΧΑΝΙΣΜΩΝ ΣΥΝΑΙΝΕΣΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αγγελόπουλος Ιωάννης

Επιβλέπουσα : Θεοδώρα Βαρβαρίγου

Καθηγήτρια Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 20η Ιουλίου 2019.

.....	.....	.....
Θεοδώρα Βαρβαρίγου	Δημήτριος Ασκούνης	Συμεών Παπαβασιλείου
Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2019

.....

Ιωάννης Αγγελόπουλος

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

Περίληψη

Η blockchain τεχνολογία αποτελεί κατά κοινή ομολογία ένα από τα πιο περιζήτητα και επίκαιρα θέματα στον επιστημονικό και ερευνητικό κόσμο. Η τεχνολογία αυτή, η οποία έγινε γνωστή μέσα από την εφαρμογή των κρυπτονομισμάτων και συγκεκριμένα του Bitcoin, αποτελεί στις μέρες μας αντικείμενο συνεχούς μελέτης αλλά και αμφισβήτησης. Ο αποκεντρωτικός χαρακτήρας που διέπει τη λειτουργία της σε συνδυασμό με τις έννοιες της ανωνυμίας, αμεταβλητότητας και βελτιστοποίησης των συναλλαγών που προσφέρει έχουν μετατοπίσει το ενδιαφέρον της τεχνολογίας αυτής πέρα από τις διαδικτυακές συναλλαγές κρυπτονομισμάτων και διάφορων περιουσιακών στοιχείων σε ένα γενικότερο και ευρύτερο πλαίσιο ανοίγοντας το δρόμο της εφαρμογής της blockchain τεχνολογίας σε ποικίλες οικονομικές, πολιτιστικές και κοινωνικές υλοποιήσεις. Ο πυρήνας της blockchain τεχνολογίας είναι ο μηχανισμός συναίνεσης που χρησιμοποιείται, μία σειρά αλγοριθμικών διαδικασιών και κανόνων που ρυθμίζουν και καθορίζουν την ομαλή και βέλτιστη λειτουργία του αντίστοιχου blockchain συστήματος. Σκοπός αυτής της διπλωματικής εργασίας είναι να παρουσιάσουμε και να συγκρίνουμε ποιοτικά και ποσοτικά τους κυριότερους μηχανισμούς συναίνεσης που χρησιμοποιούνται στα δημοφιλέστερα blockchain συστήματα αλλά και να προσδιορίσουμε κάποια από τα πιο θεμελιώδη ζητήματα της ευρύτερης τεχνολογίας, όπως η επεκτασιμότητα των διάφορων blockchain συστημάτων και η κατηγοριοποίησή τους σε δημόσια, ιδιωτικά και κοινοπρακτικά.

Κατά τη διάρκεια εκπόνησης της διπλωματικής εργασίας μελετήθηκαν σε βάθος διάφορες επιστημονικές πηγές καθώς και η ίδια η blockchain τεχνολογία, με σκοπό να παρέχουμε στον αναγνώστη τόσο μία ολοκληρωμένη, οργανωμένη και ορθολογική επισκόπηση των μηχανισμών συναίνεσης της τεχνολογίας αυτής όσο και μία ουσιαστική και πλήρη βάση για περαιτέρω μελέτη και ενασχόληση με την blockchain τεχνολογία.

Λέξεις Κλειδιά: blockchain, μηχανισμοί συναίνεσης, επεκτασιμότητα, ψηφοφορία, κόμβος, πλατφόρμα, P2P δίκτυο, οριστικότητα, διακίνηση συναλλαγών, χρονική καθυστέρηση, βελτιστοποίηση, δημοσίευση μπλοκ, proof-based, vote-based, δημόσια-ιδιωτικά-κοινοπρακτικά, ασφάλεια

Abstract

Blockchain technology is widely recognized as one of the most famous and topical issues in the scientific and research world. This technology, which became known through the application of cryptocurrencies and Bitcoin in particular, is now a subject of continuous study and questioning. The decentralized nature of its operation, coupled with the notions of anonymity, immutability and optimization of its transactions, have shifted the interest of this technology beyond the online transactions of cryptos and various assets in a broader and wider context opening its way implementation of blockchain technology in a variety of economic, cultural and social implementations. The core of blockchain technology is the consensus mechanism used, a series of algorithmic processes and rules that regulate and determine the smooth and optimal operation of the corresponding blockchain system. The purpose of this diploma thesis is to present and compare qualitatively and quantitatively the major consensus mechanisms used in the most popular blockchain systems and to identify some of the most fundamental issues of wider technology, such as the scalability of various blockchain systems and their categorization into public, private and consortium.

During the development of the diploma thesis, a number of scientific sources were explored in depth as well as the blockchain technology itself, in order to provide the reader with an integrated, organized and rational overview of the consensus mechanisms of this technology as well as a substantial and complete basis for further study and engaging in blockchain technology.

Keywords: blockchain, consensus methods, scalability, voting, node, platform, peer-to-peer network, finality, transaction throughput, latency, optimization, block publication, proof-based, vote-based, public-private-consortium, security

Ευχαριστίες

Η διπλωματική αυτή εργασία εκπονήθηκε στον τομέα Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής στη σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου. Η υπόδειξη του θέματος έγινε σε συνεργασία με την καθηγήτρια κυρία Θεοδώρα Βαρβαρίγου, καθώς και με τον Δρ. Αντώνη Λίτκε και τον Δρ. Γιώργο Παλαιοκρασσά.

Θα ήθελα να ευχαριστήσω από καρδιάς την οικογένεια και τους φίλους μου, οι οποίοι κατά τη διάρκεια του χρονικού διαστήματος της φοίτησης και της ολοκλήρωσης της διπλωματικής μου εργασίας με στήριξαν και με ενθάρρυναν να συνεχίσω υπερπηδώντας κάθε εμπόδιο και δυσκολία.

Οφείλω ένα μεγάλο ευχαριστώ στην καθηγήτρια και επιβλέπουσα κυρία Θεοδώρα Βαρβαρίγου για την ανάθεση μιας τόσο ενδιαφέρουσας διπλωματικής εργασίας, καθώς και στους Δρ. Αντώνη Λίτκε και Γιώργο Παλαιοκρασσά για την αμέριστη βοήθεια και υποστήριξη που μου παρείχαν αλλά και για την άψογη καθοδήγηση κατά την διάρκεια εκπόνησης της διπλωματικής μου εργασίας.

Τέλος απευθύνω θερμές ευχαριστίες σε όλο το διδακτικό προσωπικό του Εθνικού Μετσόβιου Πολυτεχνείου για τις γνώσεις που μου παρείχαν όλα αυτά τα χρόνια.

Πίνακας περιεχομένων

Πίνακας εικόνων

Πίνακας πινάκων

Πίνακας διαγραμμάτων

Κεφάλαιο 1. Εισαγωγή

1.1. Αντικείμενο-Σκοπός

Αντικείμενο της εργασίας αυτής είναι η επισκόπηση της τεχνολογίας blockchain, ή κατά ευθεία, αλλά όχι δόκιμη μετάφραση στα ελληνικά, τεχνολογία αλυσίδας μπλοκ, η οποία αποτελεί αδιαμφισβήτητα μία από τις πιο καινοτόμες και επαναστατικές τεχνολογίες των τελευταίων ετών. Γνωστή από την εφαρμογή της στο πρωτόκολλο του συστήματος του Bitcoin το 2008, η τεχνολογία αυτή πρωταγωνιστεί στην επιστημονική και μη κοινότητα αποτελώντας αντικείμενο συνεχούς μελέτης και διαμάχης. Κάποια από τα μοναδικά χαρακτηριστικά που παρέχει, όπως η αμεταβλητότητα και η ακεραιότητα των δεδομένων, ο αποκεντρωτικός συναλλακτικός χαρακτήρας και η ανωνυμία, εξύψωσαν τη φήμη της τεχνολογίας αυτής δίνοντάς της παράλληλα τη δυνατότητα να ενσωματωθεί σε ένα τεράστιο εύρος εφαρμογών, που ποικίλουν από τα κλασσικά συναλλακτικά συστήματα μέχρι την παιδεία, την υγεία και τον πολιτισμό.

Η δομή της blockchain τεχνολογίας στηρίζεται σε ένα δίκτυο ομότιμων χρηστών(*peer-to-peer network*) οι οποίοι πραγματοποιούν συναλλαγές μεταξύ τους στηριζόμενοι σε έναν αποκεντρωτικό τρόπο λειτουργίας. Αυτό σημαίνει πως η ολοκλήρωση των συναλλαγών δεν απαιτεί την έγκριση κάποιας ανώτερης αρχής, αλλά προϋποθέτει την ταυτόχρονη ομοφωνία ολόκληρου του δικτύου, εισάγοντας την έννοια της συνάινεσης. Η αποδέσμευση από κάθε μορφή κεντρικού ελέγχου αποτελεί την κύρια διαφορά μεταξύ της τεχνολογίας blockchain και των παραδοσιακών συναλλακτικών συστημάτων, όπου η τελική μορφή μιας συναλλαγής πρέπει να εγκριθεί από έναν ή ένα σύνολο οργανισμών που επιβλέπουν το σύστημα.

Τα επίπεδα της συναίνεσης είναι καθοριστικής σημασίας σε κάθε διανεμημένο σύστημα. Τα blockchain συστήματα επιβάλλουν την επίτευξη της συναίνεσης με μία σειρά από αλληλένδετες ενέργειες που συνεπάγονται την συνεργασία των διάφορων συμμετεχόντων στο δίκτυο, οπότε προκύπτει η έννοια των συστημάτων συναίνεσης. Το δημοφιλέστερο σύστημα συναίνεσης είναι το Proof of Work(PoW), το οποίο χρησιμοποιείται στο πρωτόκολλο του Bitcoin, ενώ με την πάροδο του χρόνου εφαρμόστηκε από διάφορα blockchain συστήματα. Το PoW στηρίζει την επίτευξη ομοφωνίας στην δέσμευση τεράστιας υπολογιστικής ισχύος για την επίλυση σύνθετων μαθηματικών προβλημάτων κατακερματισμού, προσδίδοντας στο εκάστοτε σύστημα υψηλά επίπεδα προστασίας έναντι διαφόρων μορφών επιθέσεων, διαφάνειας και αποκεντρωτισμού.

Ωστόσο λόγω των αμφιλεγόμενων επιπέδων ασφάλειας, της υπερβολικής ενεργειακής κατανάλωσης αλλά και της χαμηλής αποδοτικότητας με τον καιρό εμφανίστηκαν εναλλακτικά συστήματα συναίνεσης τα οποία βελτίωσαν κάποια από τα ελαττώματα του PoW, με χαρακτηριστικά παραδείγματα το PoS και τα BFT συστήματα.

Η χρησιμότητα και το πεδίο εφαρμογής των διαφορετικών blockchain συστημάτων οδήγησε στον διαχωρισμό τους στα δημόσια και τα ιδιωτικά-κοινοπρακτικά συστήματα. Ο διαχωρισμός αυτός οφείλεται στο γεγονός πως η τεχνολογία του Bitcoin ενέχει βασικούς περιορισμούς κατά την εφαρμογή της στον εταιρικό τομέα. Συγκεκριμένα οι μεγάλες χρονικές καθυστερήσεις και η περιορισμένη διακίνηση των δεδομένων αποτελούν κάποιους από τους κυριότερους αστάθμητους παράγοντες για τη χρησιμοποίηση του κλασσικού PoW στον ιδιωτικό και τον εταιρικό τομέα, έχοντας ως αποτέλεσμα την δημιουργία νέων βελτιωμένων μηχανισμών συναίνεσης.

Ωστόσο καθώς στις μέρες μας η τεχνολογία blockchain έρχεται αντιμέτωπη με την εφαρμογή της στον πραγματικό κόσμο, τα υπάρχοντα μοντέλα συναίνεσης

αντιμετωπίζουν συνεχή αμφισβήτηση λόγω της περιορισμένης επεκτασιμότητας, της συνεχής ζήτησης για μηδαμινές καθυστερήσεις και της μέτριας αποδοτικότητας. Ως αποτέλεσμα η επιστημονική κοινότητα έχει στρέψει το ενδιαφέρον της σε νέες πρωτοπόρες μεθόδους προσέγγισης και βελτίωσης των υπαρχόντων blockchain μοντέλων αλλά στην δημιουργία νέων επαναστατικών μεθόδων και συστημάτων, εισάγοντας την Blockchain 3.0 εποχή.

Η ακόλουθη εργασία είναι δομημένη ως εξής: στη συνέχεια του **Κεφαλαίου 1** παρουσιάζεται μία εισαγωγή στην δομή της blockchain τεχνολογίας τόσο σε θεωρητικό όσο και σε τεχνικό επίπεδο, αναλύοντας και παρουσιάζοντας βασικές έννοιες και αρχές που είναι απαραίτητες για την κατανόηση της ευρύτερης blockchain τεχνολογίας. Ακολουθεί το **Κεφάλαιο 2** στο οποίο παρατίθενται και αναλύονται οι κυριότεροι μηχανισμοί συναίνεσης, ενώ ακολουθεί μία συγκριτική ανάλυση μεταξύ τους. Στο **Κεφάλαιο 3** προσδιορίζεται το πρόβλημα της επεκτασιμότητας, ενώ έπειτα παρουσιάζονται, αναλύονται και συγκρίνονται οι πιθανές λύσεις έναντι στο πρόβλημα αυτό. Στο **Κεφάλαιο 4** ακολουθεί η ταξινόμηση των διάφορων blockchain συστημάτων σε δημόσια, ιδιωτικά και κοινοπρακτικά. Συγκεκριμένα παρουσιάζονται τα επιμέρους χαρακτηριστικά της κάθε μορφής, οι τομείς εφαρμογής τους και η χρησιμότητά τους, ενώ ακολουθεί μία συγκριτική ανάλυση που διασαφηνίζει πληρέστερα τον διαχωρισμό μεταξύ τους. Στο **Κεφάλαιο 5** παραθέτουμε τα συμπεράσματά μας από την έρευνα και την ανάλυση που έχουμε ολοκληρώσει στην υπόλοιπη εργασία, παρουσιάζοντας την προσωπική μας άποψη σε κάποια θέματα. Τέλος στο **Κεφάλαιο 6** ολοκληρώνεται η εργασία μας.

1.2. Επιστημονικό υπόβαθρο

Η τεχνολογία blockchain, όπως αναφέρουμε παραπάνω, έγινε ευρέως γνωστή από την εφαρμογή του Bitcoin. Αξίζει να αναφέρουμε πως δεν υπάρχει ένας αυθεντικός συγκεκριμένος ορισμός που να καθορίζει την ακριβή έννοια του blockchain. Ακόμα και στην παρουσίαση του Bitcoin[1] η λέξη blockchain δεν αναφέρεται αυτή καθεαυτή. Ουσιαστικά η έννοια του blockchain αναφέρεται σε μία διανεμημένη δομή δεδομένων στην οποία τα δεδομένα συνυπάρχουν αναλλοίωτα και αλληλένδετα δημιουργώντας μία συνεχή αλυσίδα από μπλοκ. Κάθε ένα από τα μπλοκ αυτά περιλαμβάνει τα δεδομένα των συναλλαγών τα οποία αποθηκεύονται με τέτοιο τρόπο ώστε η αυθεντικότητα τους να μην μπορεί να αμφισβητηθεί και να υποβαθμιστεί. Παρακάτω θα αναλύσουμε το επιστημονικό υπόβαθρο της μοναδικής αυτής τεχνολογίας στηριζόμενοι στο πρωτόκολλο του Bitcoin, με σκοπό να παρουσιάσουμε στον αναγνώστη μία ολοκληρωμένη εικόνα της λειτουργίας της blockchain τεχνολογίας και να αναλύσουμε κάποιες βασικές έννοιες-αρχές που είναι απαραίτητες για τις υπόλοιπες ενότητες της εργασίας.

1.2.1.Αναπαραγωγή μηχανογραφικού μηχανήματος

Αναζητώντας την έννοια του blockchain στην ευρύτερη διαθέσιμη βιβλιογραφία συχνά συναντάμε την έννοια της αναπαραγωγής μηχανογραφικού μηχανήματος(*state-machine replication*), κυρίως αναφορικά με τα BFT πρωτόκολλα. Η έννοια αυτή αποτελεί μία μορφή αναπαραγωγής λογισμικού, όπου η υπηρεσία διαμορφώνεται ως μια μηχανή ντετερμινιστικής κατάστασης των οποίων οι μεταβάσεις κατάστασης συνίστανται στην εκτέλεση αιτημάτων πελάτη[2][3]. Στη συνέχεια, η υπηρεσία εκτελείται σε κάθε αντίγραφο, ενώ το λογισμικό αναπαραγωγής ελέγχει την εκτέλεση των αιτημάτων, εξασφαλίζοντας ότι όλα τα αντίγραφα εκτελούν την ίδια ακολουθία αιτήσεων, η οποία μαζί με την ντετερμινιστική φύση της υπηρεσίας εξασφαλίζει ότι η κατάσταση τους παραμένει συνεπής.
Συνεπώς τα συστήματα αναπαραγωγής μηχανογραφικού μηχανήματος αποτελούν ένα μέσο εξασφάλισης συνέπειας και ανεκτικότητας ενδεχόμενων σφαλμάτων στα υπολογιστικά συστήματα. Αντιγράφοντας μία υπηρεσία σε πολλαπλούς διακομιστές το σύστημα παρέχει την εγγύηση της διαθεσιμότητας ακόμα και σε περίπτωση αποτυχίας κάποιων αντιγράφων. Ωστόσο τα συστήματα αυτά ενέχουν βασικούς περιορισμούς που ενδέχεται να υποβαθμίσουν την απόδοση τους, όπως ο αυξημένος χρόνος απόκρισης των εντολών, που οδηγεί το σύστημα σε ανεπιθύμητες χρονικές καθυστερήσεις, αλλά και οι περιορισμοί που προκύπτουν στην διακίνηση του συστήματος με τη συμμετοχή περισσότερων πελατών σε αυτό.

1.2.2.Διανεμημένα συστήματα- Δίκτυα ομότιμων κόμβων(Peer-to-Peer networks)

Ασχολούμενοι με την τεχνολογία blockchain, μία από τις πρώτες έννοιες που συναντάμε είναι η έννοια των διανεμημένων συστημάτων. Αναφερόμενοι στην έννοια αυτή θα χρησιμοποιήσουμε τον ορισμό που έδωσαν οι G.Coulouris κ.ά.[4] :

"Ένα διανεμημένο σύστημα είναι ένα σύστημα στο οποίο τα στοιχεία βρίσκονται σε δικτυωμένους υπολογιστές, επικοινωνούν και συντονίζουν τις ενέργειές του μέσω μόνο της μετάδοσης μηνυμάτων. Ο ορισμός αυτός οδηγεί στα ακόλουθα ιδιαίτερα σημαντικά χαρακτηριστικά των διανεμημένων συστημάτων: την ταυτότητα των στοιχείων, την απουσία παγκόσμιου ρολογιού και τις ανεξάρτητες αποτυχίες των στοιχείων".

Σε ένα τέτοιο σύστημα οι κόμβοι(*peers*), οι οποίοι είναι οι ίδιοι οι χρήστες του συστήματος που συμμετέχουν σε αυτό μέσω ενός υπολογιστή, οργανώνονται σύμφωνα με το μοντέλο πελάτη-εξυπηρετητή(*client-server model*)[5] ή σύμφωνα με την αρχιτεκτονική των δικτύων ομότιμων κόμβων, γνωστά και ως P2P δίκτυα(*peer-to-peer networks*)[6].
Ο ορισμός των δύο παραπάνω δομών διατυπώθηκε από τον R. Schollmeier, ο οποίος παρουσίασε και τη μεταξύ τους διαφοροποίηση[7].
Όσον αφορά τη μελέτη της blockchain τεχνολογίας θα μας απασχολήσει η έννοια των δικτύων ομότιμων κόμβων, τα οποία αποτελούν πυλώνα της τεχνολογίας αυτής και σε αντίθεση με το μοντέλο πελάτη-εξυπηρετητή εκτελούνται χωρίς την υποστήριξη κάποιου κεντρικού εξυπηρετητή, διαθέτουν ευρύτερα επίπεδα κλιμάκωσης και επεκτασιμότητας και παρέχουν ανοχή σε αποτυχίες, όπως η χαρακτηριστική περίπτωση του μοναδικού σημείου αποτυχίας(*single point of failure*).

1.2.3.Σύγχρονα-Ασύγχρονα συστήματα

Η επίτευξη ομοφωνίας αποτελεί τον απώτερο σκοπό κάθε διανεμημένου συστήματος, συνεπώς και οποιασδήποτε πλατφόρμας που χρησιμοποιεί την blockchain τεχνολογία. Ένας από τους παράγοντες που καθορίζουν την επίτευξη της ομοφωνίας σε ένα τέτοιο σύστημα είναι οι παραδοχές που αφορούν τον συγχρονισμό. Ο συγχρονισμός συνίσταται στη λειτουργία ενός συστήματος αναφορικά με τον χρονισμό των γεγονότων που συμβαίνουν μέσα σε αυτό και αναφέρεται στην σχετική ταχύτητα ολοκλήρωσης των απαιτούμενων διαδικασιών και στον χρόνο διάδοσης ενός μηνύματος στο δίκτυο. Οι παραδοχές σχετικά με τον συγχρονισμό σε ένα διανεμημένο σύστημα αποτελούν αναπόσπαστο κομμάτι του ίδιου του συστήματος, καθώς καθορίζουν τα προβλήματα που μπορεί να αντιμετωπιστούν αλλά και το είδος του αλγορίθμου που είναι ανά περίπτωση κατάλληλος. Υπάρχουν δύο κύριες κατηγορίες στις οποίες διαχωρίζονται τα συστήματα με βάση τους περιορισμούς του συγχρονισμού τους, οι οποίες είναι τα ασύγχρονα(*asynchronous systems*) και τα σύγχρονα συστήματα(*synchronous systems*).

Τα ασύγχρονα συστήματα διακρίνονται από την έλλειψη επιβολής ορίων χρονισμού. Συγκεκριμένα χαρακτηρίζονται από απουσία ορίων τόσο στις ταχύτητες των διαδικασιών όσο και στις ταχύτητες μετάδοσης των μηνυμάτων. Το πρόβλημα με το ασύγχρονο περιβάλλον είναι ότι λόγω της απουσίας χρονικών περιορισμών το σύστημα δεν μπορεί να διαχωρίσει μία αργή διαδικασία από μία λανθασμένη διαδικασία, με αποτέλεσμα την αδυναμία αντιμετώπισης μιας σειράς σοβαρών επακόλουθων προβλημάτων, με κυριότερο την αδυναμία επίτευξης ομοφωνίας με ντετερμινιστικό τρόπο παρουσία σφαλμάτων[8]. Το παραπάνω συμπέρασμα αποτελεί μία στοιχειώδη παραδοχή στην εφαρμογή των διανεμημένων συστημάτων, γνωστή ως το FLP αποτέλεσμα αδυναμίας (*FLP impossibility result*).
Στον αντίποδα έχουμε τα σύγχρονα συστήματα τα οποία σύμφωνα με την N. A. Lynch[9] επιτρέπουν την επίτευξη ομοφωνίας, καθώς σε πλήρη αντίθεση με τα ασύγχρονα συστήματα επιβάλλουν χρονικά όρια στις ταχύτητες του συστήματος. Τα όρια αυτά είναι αυστηρά και καθορισμένα από την αρχή και δεν μπορούν να παραβιαστούν και για το λόγο αυτό θα μπορούσαμε να χαρακτηρίσουμε τα σύγχρονα συστήματα ως πιο συντηρητικά. Ακόμα κατά τη λειτουργία ενός συστήματος υπό τους κανόνες του σύγχρονου χρονισμού υπάρχει ο κίνδυνος να υποβαθμιστεί η απόδοση και η λειτουργικότητα. Αυτό οφείλεται στο γεγονός ότι τα διανεμημένα συστήματα συχνά κατά τη λειτουργία τους παρουσιάζουν χρονικές αστάθειες, οι οποίες λόγω του περιορισμένου χρονισμού μπορούν να επιφέρουν λανθασμένα αποτελέσματα και επιπλοκές στην επίτευξη της ομοφωνίας.
Οι αυστηροί χρονικοί περιορισμοί των σύγχρονων μοντέλων προσδίδουν σε αυτά έναν συντηρητικό χαρακτήρα ώστε να διατηρούν την ομοφωνία κάτω από τις χειρότερες περιστάσεις. Μία εναλλακτική προσέγγιση έδωσαν οι C. Dwork κ.ά.[10] με την εισαγωγή των εν μέρει σύγχρονων συστημάτων(*partially synchronous systems*), όπου τα όρια για την ταχύτητα επεξεργασίας και την καθυστέρηση των μηνυμάτων είναι μεν καθορισμένα αλλά διατηρούνται μόνο τελικά. Τα συστήματα αυτά αποτελούν μια παραλλαγή των σύγχρονων συστημάτων με ασθενέστερα όρια χρονισμού που παράλληλα διατηρούν την επίτευξη ομοφωνίας ασφαλή. Μία ακόμα εναλλακτική ιδέα αποτελεί το μοντέλο ανιχνευτή αστοχίας(*failure detector model*), το οποίο παρουσίασαν οι T. Deepak Chandra και S. Toueg[11]. Σκοπός είναι η ενίσχυση ενός ασύγχρονου συστήματος παρέχοντας στις διαδικασίες τις σωστές πληροφορίες σχετικά με την κατάσταση του συστήματος παρέχοντας την ικανότητα επίλυσης ενός ευρύτερου φάσματος προβλημάτων.

1.2.4.Σφάλματα στα διανεμημένα συστήματα

Ένα σφάλμα στα διανεμημένα συστήμστα αποτελεί μία μη αποδεκτή απόκλιση μίας ή περισσότερων χαρακτηριστικών ιδιοτήτων του συστήματος από την επιθυμητή, συνηθισμένη τυπική κατάσταση[12]. Σε οποιοδήποτε διανεμημένο σύστημα διάφορα είδη σφαλμάτων μπορούν να προκύψουν ανά πάσα στιγμή οδηγώντας το ίδιο το σύστημα σε ανεπιθύμητες καταστάσεις που υπονομεύουν την αποδοτικότητα, την συνέχεια και τη λειτουργικότητά του. Μία τέτοια κατάσταση είναι γνωστή ως αποτυχία και ουσιαστικά ισοδυναμεί με μία μόνιμη διακοπή της ικανότητας του συστήματος να εκτελέσει κάποια διαδικασία υπό συγκεκριμένες συνθήκες λειτουργίας. Κάθε σύστημα οφείλει να διαθέτει κατάλληλους μηχανισμούς οι οποίοι

είναι ικανοί να εντοπίζουν, να εποπτεύουν και να αντιμετωπίζουν τα σφάλματα προφυλάσσοντας το σύστημα από καταστάσεις αποτυχίας. Ανάλογα με το είδος του σφάλματος ένα σύστημα μπορεί να οδηγηθεί στις εξής καταστάσεις αποτυχίας:

- *Fail-stop/Crash failures*: το σύστημα καταλήγει σε αυτή τη μορφή αποτυχίας όταν η διαδικασία εκτέλεσης σταματά μόνιμα την αποστολή και αποδοχή μηνυμάτων μεταξύ των κόμβων του δικτύου, οι οποίοι αδυνατούν να συμμετέχουν στην εφαρμογή του πρωτοκόλλου. Πρόκειται ουσιαστικά για σφάλματα και αστοχίες λογισμικού και υλικού(*software and hardware crashes*) που έχουν ως αποτέλεσμα τη μη απόκριση των κόμβων στο δίκτυο.
- *Omission failures*: αυτός ο τύπος αποτυχίας συμβαίνει όταν μια ελαττωματική διαδικασία παραλείπει την αποστολή μηνύματος που θα έπρεπε να έχει αποστείλει σύμφωνα με το πρωτόκολλο. Μπορούμε πιο απλά να πούμε πως μία διαδικασία "ξέχασε"(παρέλειψε) να αποστείλει ή να λάβει το απαραίτητο μήνυμα[13].
- *Byzantine/Non-crash failures*: αυτή είναι η γενικότερη μορφή αποτυχίας η οποία εντοπίστηκε και διατυπώθηκε από τον L. Lamport ως το πρόβλημα των Βυζαντινών στρατηγών[14] και αναφέρεται στην κακόβουλη συμπεριφορά ενός κόμβου του δικτύου. Συγκεκριμένα σε μια τέτοια αποτυχία ένας κόμβος μπορεί να λειτουργήσει αιρετικά έναντι στο σύστημα, παραλείποντας βασικούς κανόνες του πρωτοκόλλου, διαδίδοντας λανθασμένα μηνύματα, ακόμα και παραπλανώντας και άλλους χρήστες που συμμετέχουν στο σύστημα με αποτέλεσμα την ενδεχόμενη υπεραριθμία βυζαντινών χρηστών, άρα και την αποτυχία επίτευξης ομοφωνίας.

Όλα τα διανεμημένα συστήματα οφείλουν να εξασφαλίζουν την βιωσιμότητά τους κάτω από τις ανεπιθύμητες συνθήκες αποτυχιών. Για τον λόγο αυτό χρησιμοποιούν το κατάλληλο μοντέλο συναίνεσης[1], ή και συνδυασμούς αυτών, που παρέχει τα απαραίτητα επίπεδα προστασίας και ανεκτικότητας έναντι κάθε μορφής σφαλμάτων.

1.2.5.Κρυπτογράφηση

Σε αυτή την ενότητα θα παρουσιάσουμε κάποιες βασικές θεωρητικές αρχές της κρυπτογραφίας που θα βοηθήσουν στην πληρέστερη κατανόηση της blockchain τεχνολογίας.

Κρυπτογραφία είναι η επιστήμη της οποίας αντικείμενο αποτελεί ο μετασχηματισμός ενός απλού κειμένου από την αρχική, κανονική του μορφή μέσω της κρυπτογράφησης(*encryption*) σε ένα τελικό κείμενο, το κρυπτογράφημα, το οποίο στη συνέχεια μπορεί να επανέλθει στην αρχική του μορφή μέσω της αποκρυπτογράφησης(*decryption*).

Η παραπάνω διαδικασία υλοποιείται είτε με την ιδέα του συμμετρικού κλειδιού(*symmetric key*), όπου ένα και μόνο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση, είτε με την ιδέα των

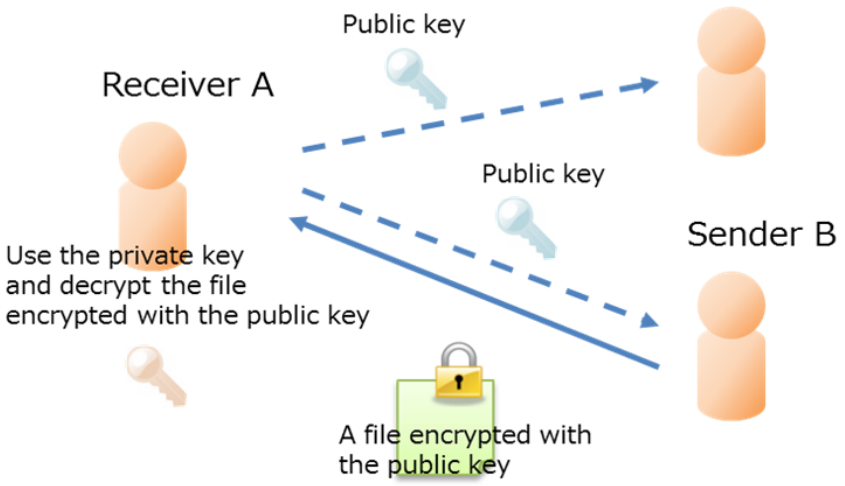
[1] Τα διάφορα μοντέλα συναίνεσης περιγράφονται αναλυτικά στο Κεφάλαιο 2 που ακολουθεί.

ασύμμετρων κλειδιών(*asymmetric key pairs*), όπου η κάθε διαδικασία χρειάζεται ξεχωριστό κλειδί.

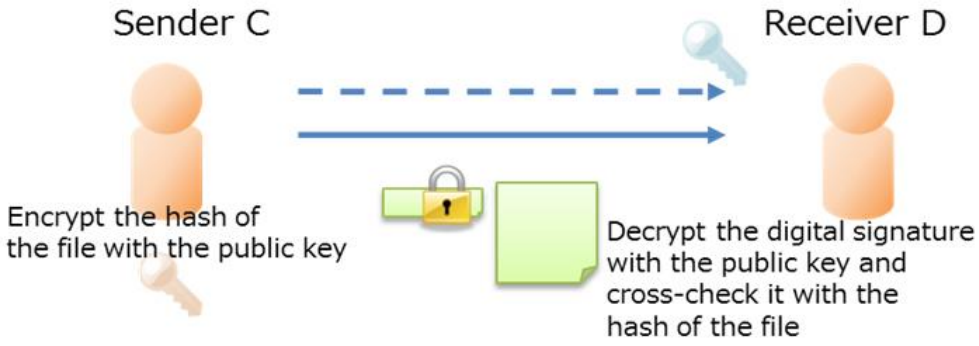
Η ιδέα της ασύμμετρης κρυπτογράφησης, γνωστής και ως κρυπτογράφηση του δημόσιου κλειδιού(*public key cryptography*), παρουσιάστηκε από τους W. Diffie και M.Hellman[15] και λειτουργεί περιληπτικά ως εξής: ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του αποδέκτη, το οποίο είναι γνωστό σε όλους, για να κρυπτογραφήσει το μήνυμα που θέλει να στείλει, ενώ ο αποδέκτης χρησιμοποιεί το ιδιωτικό του κλειδί, το οποίο είναι γνωστό μόνο στον ίδιο, για να αποκρυπτογραφήσει το μήνυμα στην αρχική του μορφή. Η διαδικασία αυτή παρέχει ασφάλεια και ιδιωτικότητα στις συναλλαγές μεταξύ δύο χρηστών, οι οποίοι δεν γνωρίζουν ο ένας τον άλλον, η οποία ασφάλεια ενισχύεται από το γεγονός ότι ενώ η κρυπτογράφηση ενός μηνύματος αποτελεί απλή διαδικασία η αντιστροφή της μέσω της αποκρυπτογράφησης είναι υπολογιστικά ανέφικτη για οποιονδήποτε άλλο πέρα του κατόχου του ιδιωτικού κλειδιού. Συνεπώς η κρυπτογραφία αποτελεί αναπόσπαστο κομμάτι της blockchain τεχνολογίας, καθώς διασφαλίζει την ακεραιότητα των δεδομένων, η οποία αφορά την ικανότητα του συστήματος να εντοπίζει πιθανές παραβιάσεις σε αυτό.

Τα blockchain συστήματα χρησιμοποιούν σε συνδυασμό με την κρυπτογράφηση-αποκρυπτογράφηση τις ψηφιακές υπογραφές(*digital signatures*), οι οποίες εξασφαλίζουν στο σύστημα την αυθεντικότητα των συναλλασσόμενων μηνυμάτων και ενισχύουν την ακεραιότητα έναντι των κακόβουλων επιθέσεων[16]. Μία ψηφιακή υπογραφή επισυνάπτεται από τον αποστολέα μέσω του ιδιωτικού του κλειδιού. Έτσι ο παραλήπτης, γνωρίζοντας το δημόσιο κλειδί του αποστολέα, μπορεί να επικυρώσει την αυθεντικότητα του μηνύματος, το οποίο πλέον είναι καθολικά αποδεκτό από το υπόλοιπο δίκτυο ως προς την αυθεντικότητά του.

Οι αλγόριθμοι στην κρυπτογραφία και στις ψηφιακές υπογραφές χρησιμοποιούν συναρτήσεις κατακερματισμού(*one-way hash functions*), των οποίων τα χαρακτηριστικά, την χρησιμότητα και τις εφαρμογές στην κρυπτογραφία περιέγραψαν με αναλυτικό τρόπο οι M. Naor και M. Yung[17]. Οι συναρτήσεις αυτές μετατρέπουν δεδομένα εισόδου τυχαίου μεγέθους σε δεδομένα εξόδου σταθερού μικρότερου μεγέθους και στηρίζουν τη λειτουργία τους στο γεγονός ότι για κάθε είσοδο η έξοδος είναι μοναδική, παρέχοντας με αυτόν τον τρόπο ανθεκτικότητα σε καταστάσεις σύγκρουσης.



Εικόνα 1-Κρυπτογράφηση του δημόσιου κλειδιού [18]



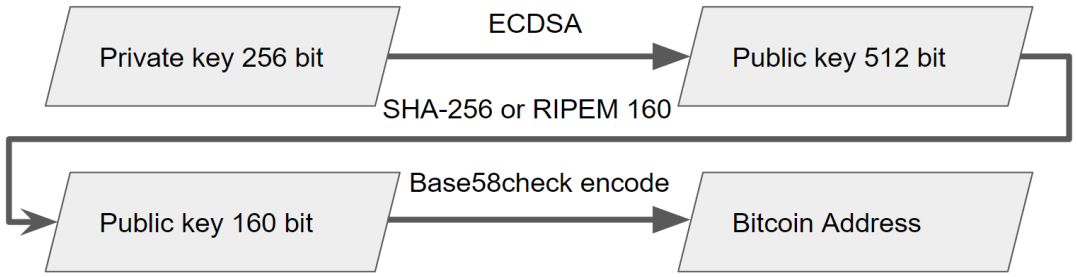
Εικόνα 2-Ψηφιακές υπογραφές[18]

1.3. Επισκόπηση του Bitcoin

Το Bitcoin πρωτόκολλο[1] είναι το πρώτο ψηφιακό σύστημα που ενσάρκωσε την blockchain τεχνολογία, αποτελώντας ένα δίκτυο από ομότιμους χρήστες που αλληλεπιδρούν μεταξύ τους πραγματοποιώντας συναλλαγές με βάση το ομώνυμο κρυπτονόμισμα. Ο σκοπός του S. Nakamoto ήταν να δημιουργήσει ένα σύστημα ψηφιακών συναλλαγών αποδεσμευμένο από κάθε μορφή ελέγχου και επιρροής τρίτων προσώπων, το οποίο στηρίζεται στην ανωνυμία και εξασφαλίζει την ασφάλεια και την ιδιωτικότητα. Παρακάτω θα περιγράψουμε τη λειτουργία του Bitcoin πρωτοκόλλου δίνοντας στον αναγνώστη μία πλήρη και ξεκάθαρη εικόνα της blockchain τεχνολογίας.

1.3.1.Περιληπτική λειτουργία του Bitcoin

Στο δίκτυο του Bitcoin η ολοκλήρωση μίας συναλλαγής είναι αποτέλεσμα μιας διαδικασίας κρυπτογράφησης και ψηφιακών υπογραφών, όπως περιγράφεται στην Ενότητα 1.2.5. Συγκεκριμένα το δημόσιο κλειδί αρχικά παράγεται από το ιδιωτικό κλειδί μέσω της ECDSA(*Elliptic Curve Digital Signature algorithm*) μεθόδου[19], μετασχηματίζεται συνήθως μέσω της SHA-256(*Secure Hash Algorithm 256 bit*) συνάρτησης κατακερματισμού και τελικά οδηγεί στην δημιουργία μιας μοναδικής διεύθυνσης(*Bitcoin address*). Η μοναδική αυτή διεύθυνση αντιπροσωπεύει τα συναλλασσόμενα Bitcoin νομίσματα. Οι συναλλαγές για να ολοκληρωθούν πρέπει να επιλεχθούν από τους κόμβους που είναι υπεύθυνοι για την δημιουργία και την συμπλήρωση των μπλοκ, γνωστούς ως ανθρακωρύχους(*miners*). Οι κόμβοι αυτοί επιλέγουν ποιες συναλλαγές επιθυμούν να συμπεριλάβουν στο δικό τους μπλοκ, ακολουθώντας μία διαδικασία διαγωνισμού υπολογιστικής ισχύος, γνωστής ως Proof of Work(PoW). Η λογική του PoW βασίζεται στο Hashcash πρωτόκολλο[20] του A. Back, το οποίο αποτελεί έναν μηχανισμό αντιμετώπισης ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, η επιτυχία του οποίου εξαρτάται από την αποστολή ενός τεράστιου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου, χρησιμοποιώντας ένα δυσανάλογα μικρό χρονικό διάστημα και την προσπάθεια της κεντρικής μονάδας επεξεργασίας(*Central Processing Unit*)[21]. Κατά την PoW διαδικασία οι κόμβοι συναγωνίζονται στο να επιλύσουν σύνθετες μαθηματικές λειτουργίες κατακερματισμού χρησιμοποιώντας την κατακερματισμένη αξία(*hash value*) του προηγούμενου υπάρχοντος μπλοκ και τα δεδομένα των συναλλαγών σε συνδυασμό με έναν τυχαίο ακέραιο αριθμό που χρησιμοποιείται μόνο μία φορά(*nonce*). Νικητής σε αυτή την επαναλαμβανόμενη διαδικασία είναι ο κόμβος εκείνος που θα εξορύξει μία νέα κατακερματισμένη αξία, μικρότερη από ένα συγκεκριμένο όριο(*target*), την οποία θα χρησιμοποιήσει στο νέο μπλοκ που θα συμπεριλάβει στην ευρύτερη αλυσίδα. Την αξία αυτή στη συνέχεια θα χρησιμοποιήσει ο επόμενος κόμβος που θα ολοκληρώσει με την ίδια PoW διαδικασία το δικό του μπλοκ.



Εικόνα 3-Μετασχηματισμός των κλειδιών και παραγωγή μίας Bitcoin διεύθυνσης[22]

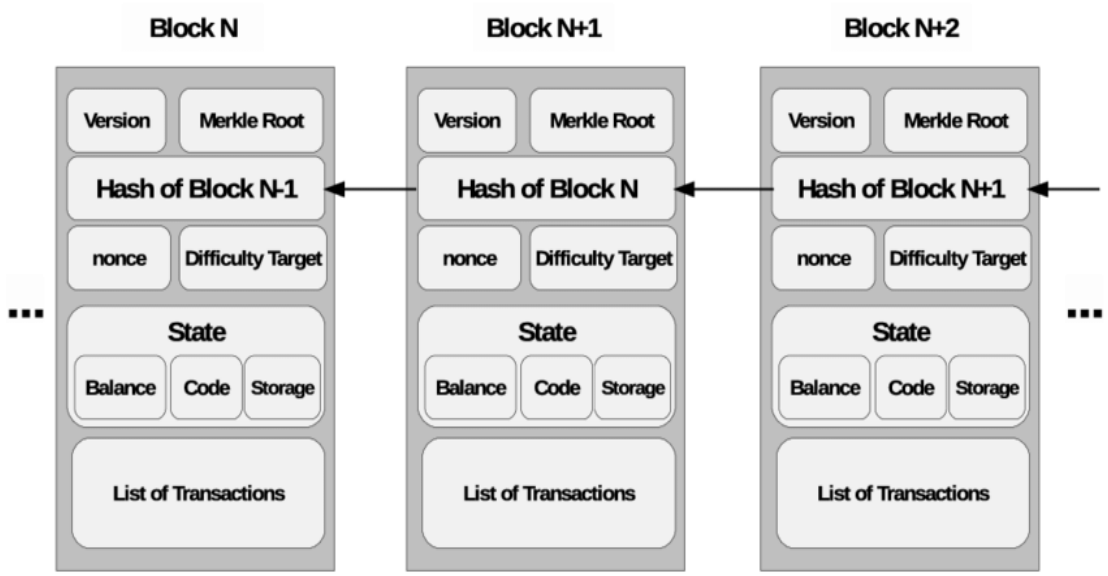
Οι ανθρακωρύχοι επιλέγουν τις συναλλαγές που θα επιβεβαιώσουν στηριζόμενοι στα τέλη συναλλαγών που προσφέρουν οι συναλλασσόμενοι χρήστες του δικτύου, ενώ για κάθε νέο μπλοκ που προσάπτεται κερδίζουν και μερικά νέα Bitcoin ως επιβράβευση της δαπανώμενης υπολογιστικής ισχύος που διέθεσαν.
Κάθε νέο μπλοκ τοποθετείται στην συνεχή αλυσίδα των προηγούμενων μπλοκ, τα οποία συνδέονται μέσω των κατακερματιστικών λειτουργιών, δημιουργώντας μία αδιάσειστη αλυσίδα που διατηρεί αναλλοίωτο όλο το ιστορικό των παρελθοντικών συναλλαγών, εξού και η ορολογία blockchain.
Ο ρόλος του PoW είναι να εξασφαλίζει την ολοκλήρωση των συναλλαγών επιβάλλοντας στο σύστημα μία αυστηρή χρονολογική σειρά. Ωστόσο αν και η εφαρμογή του PoW σε συνδυασμό με τον ρόλο των ανθρακωρύχων παρέχουν σχετική ασφάλεια έναντι πολλαπλών τύπων επιθέσεων και απειλών[2], όπως για παράδειγμα οι *double spending* και *sybil* επιθέσεις, ένα από τα μείζονα ζητήματα του PoW ως αλγόριθμος συναίνεσης είναι ο πιθανολογικός του τερματισμός, που αρκετές φορές μπορεί να οδηγήσει το σύστημα στην διάσπαση της μέχρι τότε μοναδικής αλυσίδας σε δύο υποαλυσίδες(*forks*), όπως θα εξηγήσουμε παρακάτω.

1.3.2.Δομική σύσταση των μπλοκ

Η αλυσίδα των συνεχόμενων μπλοκ που συνθέτουν το δίκτυο του Bitcoin είναι μία χρονολογικά άρρηκτη κατασκευή. Κάθε μπλοκ αποτελείται από την κεφαλή(*block header*) και το σώμα(*block body*)[23]. Η κεφαλή του μπλοκ περιλαμβάνει τις απαραίτητες πληροφορίες που καθορίζουν την μοναδικότητα του μπλοκ, όπως η κατακερματισμένη του αξία(*merkle root block hash*), η κατακερματισμένη αξία του προηγούμενου μπλοκ(*parent block hash*), μία χρονική ένδειξη-σφραγίδα που δηλώνει τη χρονική δημιουργία του μπλοκ(*block timestamp*), έναν τυχαίο ακέραιο αριθμό που χρησιμοποιείται στην επίλυση των μαθηματικών διαδικασιών κατά την εξόρυξη(*nonce*), έναν αριθμό έκδοσης που ελέγχει πιθανές αναβαθμίσεις(*version number*), το μέγεθος του μπλοκ(*block size*) και ένα αριθμητικό όριο που χρησιμεύει στην διατήρηση του ρυθμού δημιουργίας του επόμενου μπλοκ στα επιθυμητά χρονικά όρια(*difficulty target*), το οποίο μεταβάλλεται περιοδικά και αναλογικά με την

[2] Οι διάφορες περιπτώσεις απειλών αναλύονται αργότερα στο Κεφάλαιο 2.

αύξηση της υπολογιστικής ισχύος εξόρυξης. Το σώμα του μπλοκ περιλαμβάνει μία λίστα συναλλαγών.



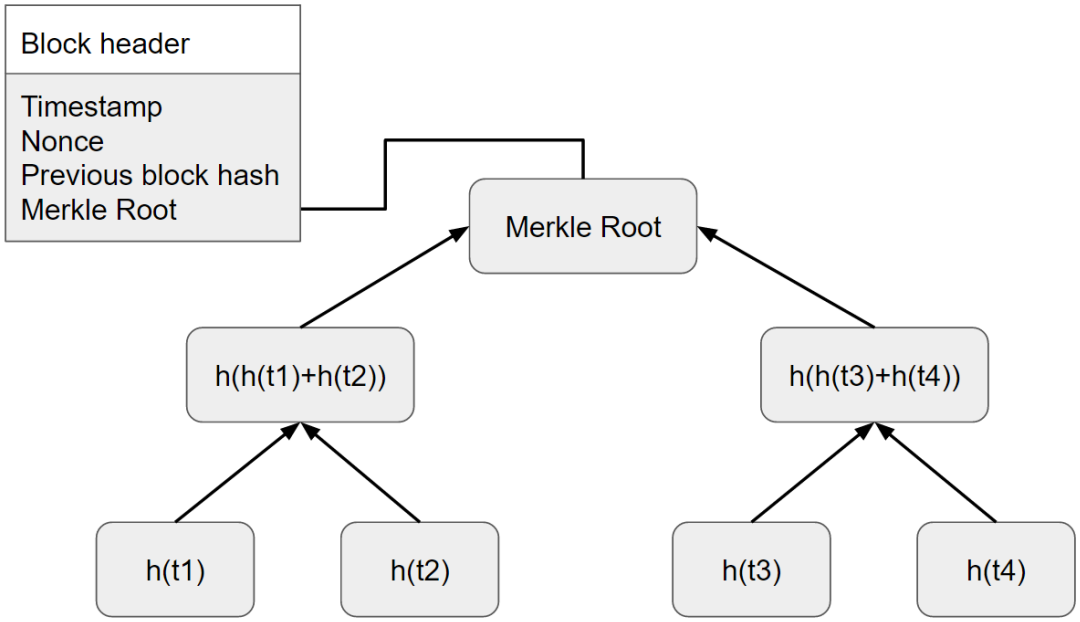
Εικόνα 4-Δομή ενός μπλοκ[23]

Κάθε μπλοκ συνδέεται με το προηγούμενο μέσω της SHA-256 συνάρτησης κατακερματισμού, δημιουργώντας μία αλληλένδετη και αδιάσπαστη αλυσίδα. Με αυτό τον τρόπο κατακερματιστικής διασύνδεσης οποιαδήποτε τροποποίηση σε κάποιο μπλοκ της αλυσίδας μεταδίδεται στην πιο πρόσφατη εκδοχή του συστήματος παρέχοντας τη δυνατότητα εντοπισμού κακόβουλων ενεργειών[24].

1.3.3.Merkle Tree Scheme

Το σχήμα του *Merkle Tree*[25] χρησιμοποιείται στο σύστημα του Bitcoin για να εξασφαλίζει τον εντοπισμό οποιασδήποτε εισερχόμενης αλλαγής σε κάποια συναλλαγή. Συγκεκριμένα ένα δένδρο τύπου Merkle είναι ένα δυαδικό δένδρο στο οποίο οι πληροφορίες αποθηκεύονται στα φύλλα του. Κάθε συναλλαγή κατακερματίζεται μέσω των συναρτήσεων κατακερματισμού, έστω $h(t_i)$, που αναφέρουμε παραπάνω. Το αποτέλεσμα της διαδικασίας αυτής είναι μία κατακερματισμένη αξία που χρησιμοποιείται ως η ταυτότητα της κάθε συναλλαγής (*transaction ID*). Όπως φαίνεται και στην Εικόνα 5 οι συναλλαγές σχηματίζουν ζευγάρια και η νέα συνδυασμένη ταυτότητα επανακατακερματίζεται. Η διαδικασία αυτή συνεχίζεται μέχρις ότου καταλήξει στο τελικό φύλλο του δένδρου, που αποτελεί και τη ρίζα αυτού(*Merkle root*), η οποία με τη σειρά της αποτελεί δομικό στοιχείο του μπλοκ. Οποιαδήποτε αλλαγή σε κάποια από τις συναλλαγές t_i μεταδίδεται στην ρίζα

του δένδρου και αναπαράγεται στο μπλοκ οδηγώντας με αυτόν τον τρόπο στην ακύρωση ολόκληρου του μπλοκ συναλλαγών.
Σύμφωνα με τον G. Becker το μεγάλο πλεονέκτημα του Merkle Signature Scheme είναι ότι η ασφάλεια εξασφαλίζεται μέσω των συναρτήσεων κατακερματισμού και των ψηφιακών υπογραφών και δεν εξαρτάται από σύνθετα μαθηματικά προβλήματα[26].

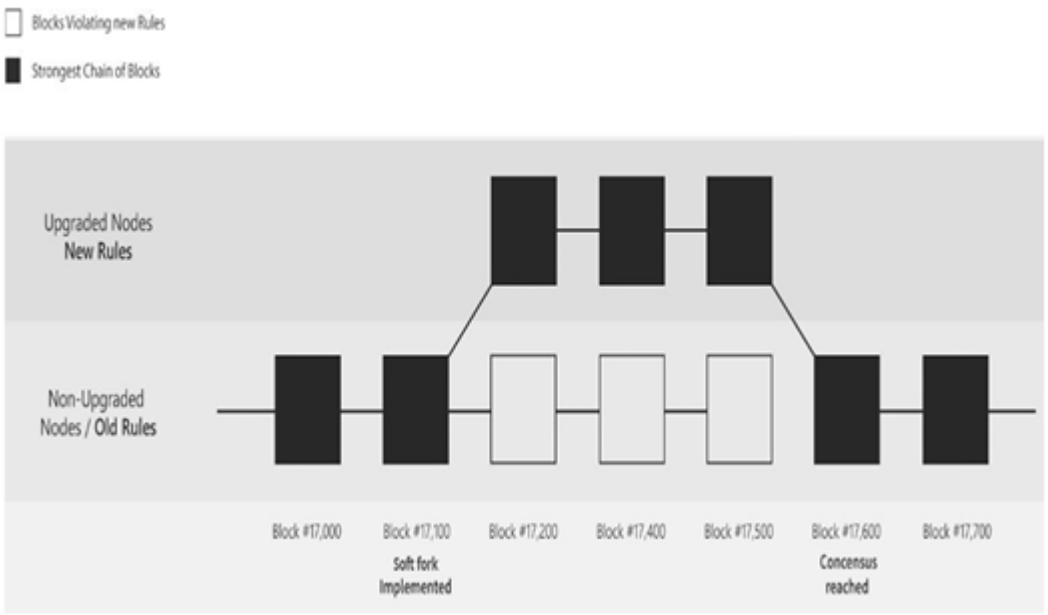


Εικόνα 5-Η δομή ενός Merkle Tree με τις κατακερματισμένες συναλλαγές h(t_i)[22]

1.3.4.Forks

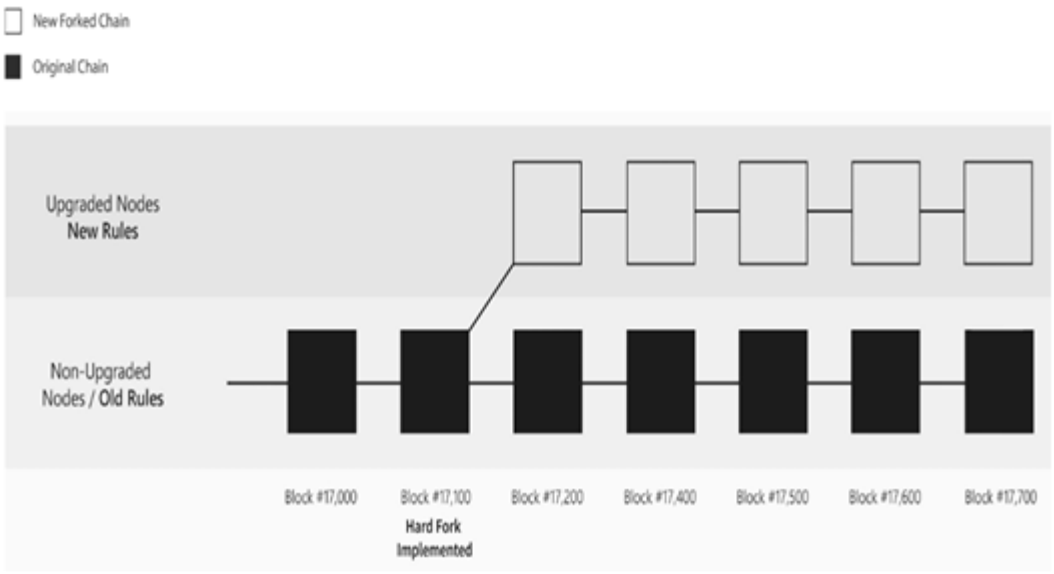
Το "πιρούνισμα"(*forking*) είναι ένα φαινόμενο που υποδηλώνει την αδυναμία του Bitcoin να εξασφαλίζει την απόλυτη οριστικότητα των συναλλαγών και τη συνολική συνέπεια του ίδιου του συστήματος. Η κατάσταση των *blockchain forks* μπορεί να λάβει χώρα ανά πάσα στιγμή δημιουργώντας μία προσωρινή ανεπιθύμητη κατάσταση στο σύστημα. Τα blockchain forks προσδιόρισαν και ανέλυσαν με σαφήνεια οι C. Decker και R. Wattenhofer[27]. Ουσιαστικά πρόκειται για έναν προσωρινό διαχωρισμό την ευρύτερης αλυσίδας του συστήματος σε δύο αλυσίδες-εκδοχές,εξού και ο χαρακτηρισμός *fork*, που συμβαίνει όταν δύο κόμβοι επιχειρούν να τοποθετήσουν ταυτόχρονα στην αλυσίδα ο καθένας το δικό του μπλοκ. Το αποτέλεσμα αυτού είναι ο διαχωρισμός της ενιαίας αλυσίδας σε δύο εκδοχές. Έτσι οι υπόλοιποι κόμβοι του δικτύου πρέπει να επιλέξουν μία από τις δύο αλυσίδες ως έγκυρη και να συνεχίσουν να εργάζονται πάνω σε αυτή με την κλασσική διαδικασία. Εν τέλει μία αλυσίδα θα υπερισχύσει, οπότε λέμε πως το *blockchain fork* έχει επιλυθεί, ενώ τα μπλοκ της αλυσίδας που απορρίφθηκε(*orphan blocks*) ανήκουν πλέον στο σύνολο των εκκρεμών συναλλαγών.

Αξίζει να αναφέρουμε πως στην blockchain τεχνολογία συναντώνται δύο περιπτώσεις blockchain forks: τα *soft forks* και τα *hard forks*.
Ένα soft fork είναι μία μεταβολή στην τεχνολογία, όπως μία αναβάθμιση της πιο πρόσφατης εκδοχής, η οποία δεν απαιτεί την αποδοχή από όλους τους κόμβους του δικτύου, επιτρέποντας εν μέρει στους μη αναβαθμισμένους κόμβους τη συμμετοχή στο σύστημα.



Εικόνα 6-Παράδειγμα ενός soft fork[28]

Ένα hard fork είναι μία μεταβολή στην τεχνολογία, όπως μία αλλαγή στη δομή ενός μπλοκ, η οποία δεν επιτρέπει στους μη αναβαθμισμένους χρήστες να συμμετέχουν στο νέο σύστημα, δίνοντάς τους την επιλογή την αναβάθμισης παράλληλα με το σύστημα ή την παραμονή στην παλιά μη αναβαθμισμένη εκδοχή.



Εικόνα 7-Παράδειγμα ενός hard fork[28]

Επιπροσθέτως οι A.Kiayias κ.ά.[29] όρισαν μία παραλλαγμένη μορφή του soft fork, το οποίο ονόμασαν *velvet fork*.
Η εκτεταμένη ανάλυση των παραπάνω διάφορων περιπτώσεων των blockchain forks δεν αποτελεί αντικείμενο της εργασίας μας, ωστόσο για μία πιο αναλυτική επισκόπηση και σύγκριση ο αναγνώστης μπορεί να ανατρέξει στην εργασία των A. Zamyatin κ.ά.[30].

Κεφάλαιο 2. Μηχανισμοί συναίνεσης

Σε κάθε blockchain σύστημα απώτερος σκοπός είναι η επίτευξη ομοφωνίας μεταξύ των διάφορων κόμβων του δικτύου. Η ομοφωνία, ή αλλιώς συναίνεση(*consensus*), επιτυγχάνεται μέσω διάφορων μηχανισμών και πρωτοκόλλων που στην ευρύτερη βιβλιογραφία είναι γνωστά ως μέθοδοι συναίνεσης(*consensus methods*). Η δημοφιλέστερη μέθοδος συναίνεσης είναι το πρωτόκολλο PoW, το οποίο αποτελεί τον πυρήνα της λειτουργίας του Bitcoin αλλά και άλλων ευρέως εφαρμοσμένων συστημάτων, όπως το Ethereum. Όπως εξηγήσαμε στην Ενότητα 1.3.1 το PoW εξασφαλίζει στο Bitcoin την ομαλή λειτουργία και την ολοκλήρωση των συναλλαγών σε ένα περιβάλλον ασφάλειας και αμεταβλητότητας στηριζόμενο στην μη αναστρέψιμη φύση των κατακερματιστικών τεχνικών και στην πολυπλοκότητα των μαθηματικών λειτουργιών.

Ωστόσο λόγω της συνεχόμενης τάσης για εξέλιξη αλλά και τις αυξανόμενες απαιτήσεις των χρηστών το Bitcoin έρχεται συνεχώς αντιμέτωπο με διάφορα θέματα που χαρακτηρίζουν την εγγενή δομή του, όπως τα υπέρογκα ποσά υπολογιστικής ισχύος, το υψηλό κόστος εγκατάστασης και οι αμφιλεγόμενοι παράμετροι επεκτασιμότητας και χωρητικότητας.

Για το λόγο αυτό με την πάροδο των χρόνων δημιουργήθηκαν νέοι βελτιωμένοι μηχανισμοί συναίνεσης με σκοπό να ξεπεράσουν τα εμπόδια του PoW αλλά και να επεκτείνουν τη χρήση της blockchain τεχνολογίας σε ευρύτερους τομείς, πέρα από τις ψηφιακές συναλλαγές με κρυπτονομίσματα.

Στη βιβλιογραφία σχετικά με την blockchain τεχνολογία υπάρχουν αρκετά επιστημονικά και μη έγγραφα που προσδιορίζουν με σαφήνεια τους διάφορους μηχανισμούς συναίνεσης αλλά και συγκρίσεις μεταξύ αυτών. Σκοπός μας είναι να παραθέσουμε όλους τους υπάρχοντες μηχανισμούς και πρωτόκολλα συναίνεσης, άλλα από τα οποία βρίσκονται ήδη σε εφαρμογή και άλλα υπό μελέτη και βελτίωση, και να παρουσιάσουμε μία πλήρη και εκτεταμένη σύγκριση μεταξύ αυτών προσδιορίζοντας έτσι τη χρησιμότητα, τη διαφοροποίηση και τους τομείς εφαρμογής τους.

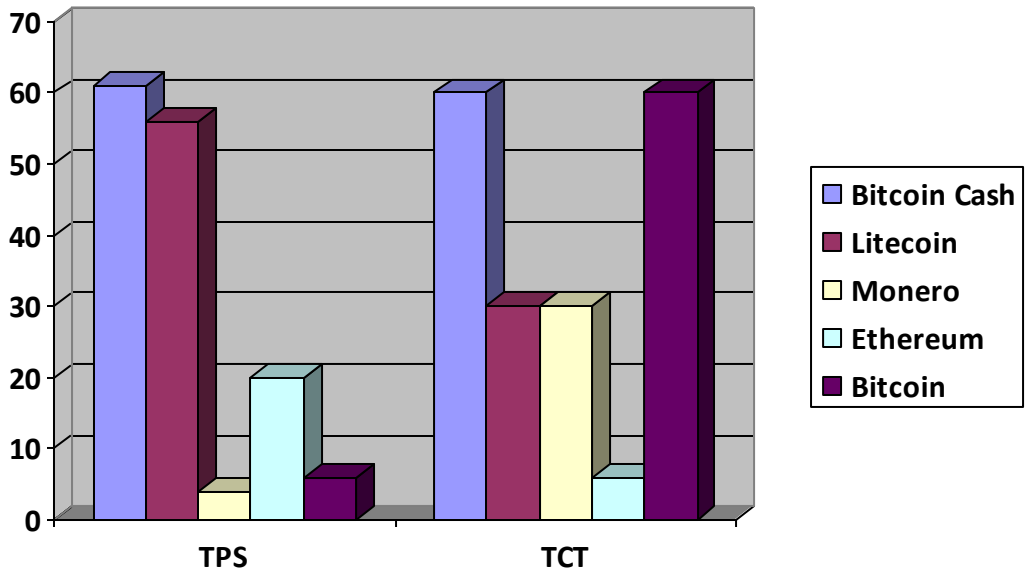
Παρακάτω θα παρουσιάσουμε τους κυριότερους μηχανισμούς συναίνεσης, περιγράφοντας τον τρόπο λειτουργίας και τα χαρακτηριστικά τους, και στη συνέχεια θα παραθέσουμε μία αναλυτική σύγκριση μεταξύ αυτών.

2.1. Proof of Work (PoW)

Το PoW αποτελεί τον πρώτο και δημοφιλέστερο μηχανισμό συναίνεσης που χρησιμοποιείται στο Bitcoin, όπως περιγράψαμε στην Ενότητα 1.3. Οι miners συναγωνίζονται σε μία δύσκολη διαδικασία επίλυσης ενός παζλ κατακερματισμού με σκοπό να βρουν το κατάλληλο nonce value για να δημοσιεύσουν το επόμενο μπλοκ στην αλυσίδα. Η σπατάλη ενεργειακών πόρων, υπολογιστικής ισχύος και χρόνου αποτελούν την απόδειξη της εργασίας τους, ενώ ο κάθε κόμβος λειτουργεί ανεξάρτητα χωρίς να υπάρχει ουσιαστικά καμία προϋπόθεση εμπιστοσύνης μεταξύ των εργαζόμενων κόμβων στο δίκτυο. Το PoW παρέχει υψηλά επίπεδα ασφάλειας, καθώς μια ενδεχόμενη απόπειρα ελέγχου του δικτύου είναι σχεδόν αδύνατη λόγω της απαιτούμενης ενεργειακής δαπάνης. Επίσης τα PoW συστήματα χαρακτηρίζονται από την πιθανολογική οριστικότητα των συναλλαγών, λόγω της πιθανής εμφάνισης των

forks. Όσον αφορά τα επίπεδα επεκτασιμότητας και διακίνησης με χρήση του PoW, αν και στον αριθμό των χρηστών που μπορούν να συμμετέχουν στο δίκτυο δεν υπάρχει περιορισμός, το Bitcoin δυσφημίζεται για τις ελάχιστες 3-7 συναλλαγές ανά δευτερόλεπτο που μπορεί να πραγματοποιήσει. Ακόμα κάθε μπλοκ προστίθεται ανά 10 λεπτά και συνυπολογίζοντας πως για να οριστικοποιηθούν οι συναλλαγές απαιτούνται 6 στάδια επιβεβαίωσης ο συνολικός χρόνος πραγματοποίησης των συναλλαγών ανέρχεται στα 60 λεπτά, μία ταχύτητα που στην ερευνητική κοινότητα αποτελεί ίσως το μεγαλύτερο μειονέκτημα του Bitcoin. Ωστόσο δεν πρέπει να συγχέουμε απαραίτητα το PoW με το Bitcoin, καθώς τα τελευταία χρόνια εμφανίστηκαν στο προσκήνιο αρκετά συστήματα που χρησιμοποιούν ακόμα και σήμερα το PoW πρωτόκολλο πιο αποδοτικά απ' το Bitcoin. Κλασσικό είναι το παράδειγμα του Ethereum, μίας blockchain πλατφόρμας που χρησιμοποιεί το κρυπτονόμισμα Ether και παρέχει την υλοποίηση έξυπνων συμβάσεων(*smart contracts*)[31][32]. Στο Ethereum ο μέσος όρος των πραγματοποιούμενων συναλλαγών είναι 15-20. Επιπροσθέτως οι συναλλαγές ολοκληρώνονται ανά 6 λεπτά(12 δευτ. x 30 επιβεβ.).
Βέβαια υπάρχουν και άλλες παρόμοιες πλατφόρμες που χρησιμοποιούν το PoW πρωτόκολλο, η καθεμία με αντίστοιχες παραλλαγές και βελτιώσεις, οι σημαντικότερες εκ των οποίων παρουσιάζονται στο παρακάτω Διάγραμμα 1.

Διάγραμμα 1-Σύγκριση διακίνησης των συναλλαγών των κυριότερων συστημάτων που χρησιμοποιούν το PoW



TPS: συναλλαγές ανά δευτερόλεπτο
TCT: χρόνος επιβεβαίωσης συναλλαγών σε λεπτά

Αν και η λογική του PoW αυτή καθεαυτή θεσπίζει τη διασφάλιση του αποκεντρωτισμού κατά την επίτευξη της ομοφωνίας έχουν παρατηρηθεί φαινόμενα που απειλούν το χαρακτηριστικό αυτό. Συγκεκριμένα οι I.Eyal και E.Sirer παρουσίασαν το *Selfish-Mine*[33], μία στρατηγική εξόρυξης που επιτρέπει στους

miners να δημιουργούν οργανωμένες ομάδες(*mining pools*) ώστε να έχουν περισσότερα έσοδα αναλογικά με την ενεργειακή συμμετοχή τους. Οι ομάδες αυτές εισάγουν ένα είδος κεντρικού ελέγχου στο δίκτυο και λειτουργούν εις βάρος του διαταράσσοντας τις ισορροπίες μέσα σε αυτό.

2.2. Proof of Stake (PoS)

Το PoS πρωτόκολλο αποτελεί το δεύτερο δημοφιλέστερο μετά το PoW. Η λειτουργία του είναι παρόμοια με αυτή του PoW με μία ουσιαστική διαφορά: στο PoS ο κόμβος(*stakeholder*) που θα τοποθετήσει το επόμενο μπλοκ στην κύρια αλυσίδα επιλέγεται με βάση το "ποντάρισμα"(*stake*) που έχει διαθέσει και όχι με βάση την υπολογιστική του δύναμη, όπως στο PoW. Το stake αυτό αφορά την περιουσία, για παράδειγμα το συνολικό ποσό κρυπτονομισμάτων που διαθέτει ένας κόμβος. Έτσι οι πιθανότητες εκλογής ενός κόμβου ως επικυρωτής(*validator*) του επόμενου μπλοκ είναι ανάλογες με το stake που διαθέτει, το οποίο αντιπροσωπεύει το ποσοστό του κόμβου αυτού ως μέρος του συστήματος, μιας και τα συνολικά νομίσματα είναι διαθέσιμα από την πρώτη μέρα χωρίς την έκδοση νέων με το πέρασμα του χρόνου. Η αμοιβή για τη δημιουργία νέων μπλοκ είναι αποκλειστικά τα τέλη συναλλαγών, ενώ οι κάτοχοι των νομισμάτων λαμβάνουν συγκεκριμένες αμοιβές ανάλογα με την περίοδο της νομισματικής τους κατοχής.
Το PoS πρωτόκολλο εμφανίζεται υπό τρεις βασικές μορφές ανάλογα με τον τρόπο που επιλέγεται από το σύστημα ο κόμβος που θα δημιουργήσει το επόμενο μπλοκ[34]:

- *Chain-based PoS*
- *Byzantine Fault Tolerant PoS*
- *Coin age PoS*

Το PoS πρωτόκολλο υλοποιήθηκε πρώτη φορά μέσω του κρυπτονομίσματος Peercoin το 2012, το οποίο λειτουργεί ως υβριδική πλατφόρμα των PoW και PoS. Στο Peercoin οι S.King και S.Nadal χρησιμοποίησαν την ιδέα του *coin age*[35], η οποία υπολογίζεται από τον γινόμενο του stake ενός κόμβου επί τη χρονική διάρκεια που κατέχει το stake αυτό. Όσο μεγαλύτερο είναι το coin age τόσο ισχυρότερος είναι ένας κόμβος στο δίκτυο, ενώ για κάθε συναλλασσόμενο ποσό κρυπτονομισμάτων το αντίστοιχο coin age καταστρέφεται.
Σε μια άλλη κρυπτονομισματική πλατφόρμα, το Blackckoin[36], ο P.Vasin υποθέτοντας ότι η εφαρμογή του coin age στο PoS θα μπορούσε να ενισχύσει την πιθανότητα κλοπής την αντικατέστησε με την ιδέα του *raw stake*, εξασφαλίζοντας παράλληλα ότι οι κόμβοι θα παραμένουν περισσότερο ενεργοί στο δίκτυο, αποθαρρύνοντάς τους έτσι απ' το να διευρύνουν τη δύναμή τους παραμένοντας ανενεργοί.

Κλασσικές εφαρμογές του PoS παρατηρούνται επίσης στην πλατφόρμα Nextcoin[3] και στην εργασία των I.Bentov κ.ά. σχετικά με τα *pure PoS* πρωτόκολλα[37].
Το πρωτόκολλο Ouroboros των A.Kiayias κ.ά.[38], το οποίο χρησιμοποιεί η πλατφόρμα του κρυπτονομίσματος Cardano, αποτελεί μία εκδοχή του PoS με αναβαθμισμένες παροχές ασφάλειας. Μέσω μίας διαδικασίας ανάθεσης(*delegation process*) του διαχωρισμού των χρηστών του δικτύου σε *leaders* και *endorsers* και τη χρήση χρονικών διαστημάτων(*epochs*) οι δημιουργοί του Ouroboros επιχείρησαν να αυξήσουν την ισότητα στο σύστημα δίνοντας έμφαση στη διασφάλιση των θεμελιωδών εννοιών της επιμονής και ζωτικότητας. Επιπροσθέτως ο χρόνος επιβεβαίωσης των συναλλαγών κινείται στα 10 λεπτά, ενώ πραγματοποιούνται 5-7 συναλλαγές ανά δευτερόλεπτο.
Μία πιο προχωρημένη εκδοχή του PoS αποτελεί ο αλγόριθμος Casper των V.Buterin και V.Griffith[39], η εφαρμογή του οποίου αναμένεται να αποδεσμεύσει την πλατφόρμα του Ethereum οριστικά από το PoW. Σκοπός του Casper είναι η οριστική αντικατάσταση των miners του PoW με τους validators του PoS και λειτουργεί ως εξής: μέσω μίας ειδικής συνθήκης(*Casper contract*) εκλέγονται οι validators, οι οποίοι διαθέτουν ένα μέρος των κρυπτονομισμάτων τους (στο Ethereum τα Ethers) ως stake, το οποίο θα χρησιμοποιήσουν για να επικυρώσουν το μπλοκ που επιθυμούν. Όταν ένα μπλοκ προστεθεί οι validators λαμβάνουν μία αμοιβή ανάλογη του stake που διέθεσαν. Αυτό που κάνει το Casper ιδιαίτερα ενδιαφέρον είναι πως σε περίπτωση κακόβουλης συμπεριφοράς ο χρήστης τιμωρείται με το stake του να μειώνεται από το ίδιο το σύστημα. Με την παραπάνω λειτουργία τα αρχικά stakes παίρνουν τη μορφή καταθέσεων ασφαλείας ως προς την ακεραιότητα του συστήματος, ενώ οι χρήστες αποθαρρύνονται από την πραγματοποίηση ανεπιθύμητων ενεργειών, καταπολεμώντας έτσι την *nothing-at-stake* συμπεριφορά, μία από τις μεγαλύτερες εγγενής απειλές του PoS πρωτοκόλλου. Ο αλγόριθμος Casper σε συνδυασμό με την τεχνική *sharding* αναμένεται υλοποιήσουν την εκδοχή Ethereum 2.0 μέσα στο 2019[40], ενισχύοντας τα υπάρχοντα επίπεδα οριστικότητας και επεκτασιμότητας και μειώνοντας το κόστος επίτευξης ομοφωνίας.
Παρακάτω θα περιγράψουμε κάποια πρωτόκολλα τα οποία στηρίζονται μεν στη λογική του PoS αλλά παρουσιάζουν κάποιες διαφοροποιήσεις στον τρόπο επίτευξης ομοφωνίας.

2.2.1.Delegated Proof of Stake (DPoS)

Η βασική διαφορά του DPoS με το PoS είναι πως οι stakeholders χρησιμοποιούν το stake που έχουν διαθέσει όχι για την διεκδίκηση του δικαιώματος δημιουργίας νέων μπλοκ αλλά για τη συμμετοχή τους σε μία διαδικασία ψηφοφορίας εκλογής. Μέσω της ψηφοφορίας αυτής εκλέγονται κάποιοι αντιπροσωπευτικοί κόμβοι του δικτύου(*witnesses-delegates*) στους οποίους παρέχεται η αποκλειστική ευθύνη της επιβεβαίωσης των συναλλαγών και της δημιουργίας νέων μπλοκ. Οι κόμβοι αυτοί αντιπροσωπεύουν τους stakeholders στο δίκτυο και εκλέγονται ανά εκλογικούς γύρους από μία λίστα η οποία συνεχώς ανακατεύεται, ενώ για κάθε μπλοκ που ολοκληρώνουν λαμβάνουν αμοιβή. Ωστόσο ο κάθε delegate οφείλει να ολοκληρώσει

[3] https://nxtwiki.org/wiki/Whitepaper:Nxt

τις έγκυρες συναλλαγές μέσα σε ένα συγκεκριμένο χρονικό διάστημα, που σημαίνει ότι η υπέρβαση αυτού θα αναθέσει την διαδικασία στον επόμενο delegate και ίσως στερήσει από τον κόμβο που απέτυχε να ολοκληρώσει το έργο του την συμμετοχή σε μελλοντικές εκλογές. Δύο δημοφιλείς πλατφόρμες που χρησιμοποιούν το DPoS πρωτόκολλο είναι οι EOS.IO[41] και BitShares[42].
Στο BitShares οι witnesses εκλέγονται από τους χρήστες του δικτύου αναλογικά με το ποσό των BTS tokens που έχουν στη διάθεσή τους. Ο κάθε witness που επιλέγεται εγκρίνει το νέο μπλοκ, με τα μπλοκ να παράγονται ανά 2-3 δευτερόλεπτα, ενώ η πλατφόρμα Graphene του BitShares 2.0 μπορεί θεωρητικά να ολοκληρώσει 100000 συναλλαγές ανά δευτερόλεπτο.
Το EOS.IO συγκροτείται από 21 κόμβους, οι οποίοι λειτουργούν ως παραγωγοί μπλοκ και ψηφίζονται από του κατόχους των EOS tokens. Το σύστημα είναι δομημένο με τέτοιο τρόπο ώστε ένας κόμβος που δεν εκτελεί σωστά τα καθήκοντά του να τιμωρείται με τον αποκλεισμό του από την εκλογική διαδικασία. Κάθε μπλοκ δημιουργείται ανά 3 δευτερόλεπτα από τον επιλεγμένο κόμβο, ενώ σύμφωνα με το EOS network monitor η πλατφόρμα αυτή έχει καταγράψει μέχρι και 3996 συναλλαγές ανά δευτερόλεπτο[43], νούμερο αξιοσημείωτο συγκριτικά με τα αντίστοιχα δεδομένα για το Bitcoin και το Ethereum, ενώ η εκτέλεση των συναλλαγών πραγματοποιείται σχεδόν αμέσως.
Το DPoS πρωτόκολλο συγκρινόμενο με τα PoW και PoS καθιστά τις παραπάνω blockchain πλατφόρμες πιο αποδοτικές, καθώς με την ανάθεση της δημιουργίας των μπλοκ σε πολύ μικρότερο αριθμό χρηστών οι ταχύτητες και οι συχνότητες πραγματοποίησης των συναλλαγών βελτιστοποιούνται, ενώ το ίδιο το δίκτυο αποδεσμεύεται από την τεράστια ενεργειακή σπατάλη. Ωστόσο στον αντίποδα η διαχείριση των συναλλαγών απ' τους λίγους θίγει τη διασφάλιση του αποκεντρωτικού χαρακτήρα της γενικότερης blockchain λογικής, καθιστώντας το DPoS αντιπροσωπευτικά δημοκρατικό σε αντίθεση με το άμεσα δημοκρατικό PoS[44].

2.2.2.Proof of Importance (PoI)

Ο συγκεκριμένος μηχανισμός ομοφωνίας αποτελεί μία τροποποιημένη εκδοχή του PoS και χρησιμοποιήθηκε πρώτη φορά από το δίκτυο NEM, στο οποίο οι συναλλαγές χρησιμοποιούν το κρυπτονόμισμα XEM[45]. Αυτό που διαφοροποιεί το PoI από το PoS και το PoW είναι το γεγονός ότι η χρησιμότητα ενός ενεργού κόμβου στο δίκτυο δεν κρίνεται ούτε από το ποσό της υπολογιστικής ισχύος ούτε από το συνολικό stake που διαθέτει, αλλά διαμορφώνεται συνυπολογίζοντας επιπλέον παραμέτρους που καθορίζουν την καθολική συνεισφορά στο δίκτυο. Συγκεκριμένα κάθε λογαριασμός διαχωρίζει το ποσό XEM που διαθέτει σε δύο μέρη, *vested* και *unvested balance*, και ανάλογα με τη συναλλαγή διατηρείται μία σχετική αναλογία μεταξύ αυτών. Ένας κόμβος μπορεί να δημιουργήσει ένα μπλοκ(*harvesting*) και να λάβει τα τέλη συναλλαγών ως αμοιβή ανάλογα με το *importance score* του μέσα στο δίκτυο, με την προϋπόθεση να διαθέτει τουλάχιστον 10000 vested XEM. Το importance score είναι αυτό που ουσιαστικά καθορίζει τη συμμετοχή των κόμβων στην διαδικασία ομοφωνίας και συνυπολογίζεται από διάφορες παραμέτρους μέσα στο δίκτυο, όπως η φήμη που χαρακτηρίζει έναν κόμβο και το πλήθος των συναλλαγών που αυτός έχει ολοκληρώσει. Με τη χρήση του PoI στο δίκτυο του NEM οι ταχύτητες δημιουργίας

των μπλοκ κινούνται κατά μέσο όρο γύρω στο 1 λεπτό, ενώ σημειώνονται κατά μέσο όρο 3085 συναλλαγές ανά δευτερόλεπτο.

2.2.3.Leased Proof of Stake (LPoS)

Το LPoS είναι ένας μηχανισμός συναίνεσης που λειτουργεί παρόμοια με το PoS, αλλά παρουσιάζει κάποιες βελτιώσεις συγκριτικά με αυτό. Σύμφωνα με την πλατφόρμα Waves, μία blockchain πλατφόρμα που στηρίζει τη λειτουργία της στο LPoS και έχει συνεργαστεί με την Deloitte για την blockchain τεχνολογία[46], οι κόμβοι μπορούν να συμμετέχουν σε αυτή λειτουργώντας είτε ως *full nodes*, οι οποίοι θα προσθέσουν το επόμενο μπλοκ, είτε ως κάτοχοι των κεφαλαίων τους δανείζοντας μέρος αυτών στους full nodes(*leasers*)[47]. Μέσω της διαδικασίας αυτής μίσθωσης, γνωστής ως *leasing*, οι κόμβοι του δικτύου με λίγα κεφάλαια αποκτούν το δικαίωμα συμμετοχής στην παραγωγή των μπλοκ καθώς μισθώνονται κεφάλαια των πλουσιότερων κόμβων, οι οποίοι λαμβάνουν αναλογικά μέρος των τελών που εισπράττονται από τα μπλοκ. Με τη χρήση του LPoS μία blockchain πλατφόρμα καθίσταται πιο ασφαλής μέσω της ενίσχυσης των επιπέδων αποκεντρωτισμού, ο οποίος είναι αμφιλεγόμενος στην λογική του DPoS αλλά και του κλασσικού PoS εν μέρει.

2.3. Υβριδικά PoW-PoS συστήματα

Τα υβριδικά συστήματα συναίνεσης αποτελούν μία προσπάθεια δημιουργίας νέων μηχανισμών που θα βελτιώσουν τα μειονεκτήματα των κλασσικών PoW και PoS συστημάτων. Οι G.Nguyen, K.Kim[48] παρουσίασαν διάφορες παραλλαγές των PoW και PoS μηχανισμών, παραθέτοντας και κάποιες υβριδικές μορφές. Παρακάτω παρουσιάζουμε το βασικότερο για την ώρα υβριδικό σύστημα, το Proof of Activity(PoA).

Το PoA αποτελεί ένα συνδυαστικό μοντέλο συναίνεσης των κλασσικών PoW και PoW το οποίο παρουσίασαν οι I.Bentov κ.ά.[49] Σκοπός του PoA είναι ο περιορισμός της υπέρμετρης ενεργειακής σπατάλης που χαρακτηρίζει το Bitcoin, διαμερίζοντας την επίτευξη ομοφωνίας σε δύο στάδια. Αρχικά, στο πρώτο στάδιο(*proof of work mining*), οι PoW κόμβοι(*miners*) συναγωνίζονται σε έναν κατακερματιστικό μαραθώνιο με σκοπό τη δημιουργία του επόμενου μπλοκ, το οποίο με τη δημιουργία του θα περιλαμβάνει μόνο την κεφαλή και τη διεύθυνση του δημιουργού του χωρίς συναλλαγές. Στη συνέχεια ακολουθεί το επόμενο στάδιο(*proof of stake voting*), στο οποίο ορισμένοι PoS κόμβοι(*validators*) αποκτούν το δικαίωμα να εγκρίνουν το μπλοκ τοποθετώντας την υπογραφή τους σε αυτό, ενώ ο τελευταίος από αυτούς τοποθετεί στο μπλοκ και τις συναλλαγές που επιθυμεί[48].

Από τη μία μεριά το υβριδικό αυτό μοντέλο συναίνεσης παρέχει ασφάλεια έναντι κλασσικών απειλών, όπως οι 51% και οι double-spending επιθέσεις. Ακόμα διαμοιράζει τις αμοιβές που προκύπτουν από την ολοκλήρωση των συναλλαγών

μεταξύ όλων των κόμβων που συμμετείχαν στη διαδικασία, αποτελώντας μία πιο δίκαιη εκδοχή συγκριτικά με το κλασσικό PoS, όπου ο πλούσιος γίνεται πλουσιότερος[48]. Από την άλλη μιας και στηρίζεται αρχικά στο κλασσικό PoW διατηρεί, έστω και σε μικρότερα επίπεδα, την κατανάλωση πόρων και ακριβού εξοπλισμού, ενώ οι χρονικές καθυστερήσεις κατά την ολοκλήρωση των συναλλαγών ενδέχεται να είναι μεγαλύτερες απ' ότι στα κλασσικά PoW και PoS συστήματα[50].

2.4. Proof of Elapsed Time (PoET)

Η ιδέα του PoET ανήκει στην Intel, ενώ χρησιμοποιείται ως βασικός μηχανισμός συναίνεσης στην πλατφόρμα Hyperledger Sawtooth της Linux[51]. Ο μηχανισμός αυτός είναι σχεδιασμένος για να λειτουργεί μέσα σε ένα έμπιστο περιβάλλον εκτέλεσης(*trusted execution environment-TEE*) όπως το *Software Guard Extensions(SGX)* της Intel[52] και η βασική ιδέα είναι πως ένας κόμβος του δικτύου πρέπει να περιμένει ένα συγκεκριμένο χρονικό διάστημα ώστε να αποκτήσει το δικαίωμα έκδοσης του επόμενου μπλοκ. Η διαφορά με το PoW είναι πως αν και οι κόμβοι θα χρειαστεί να επιλύσουν παρόμοια προβλήματα κατακερματισμού δεν απαιτείται ο συναγωνισμός υπολογιστικής ισχύος, καθώς το σύστημα χρησιμοποιεί ένα μοντέλο τυχαίας εκλογής μέσω του SGX, όπου νικητής είναι ο κόμβος εκείνος με τον μικρότερο χρόνο αναμονής. Το σύστημα διανέμει τους χρόνους αναμονής μεταξύ των κόμβων εντελώς τυχαία,, ενώ κάθε κόμβος που θα ολοκληρώσει ένα μπλοκ οφείλει να αποδείξει τον χρόνο αναμονής του, ώστε το μπλοκ του να μπορεί εύκολα να εγκριθεί από το υπόλοιπο δίκτυο. Με τη διαδικασία αυτή το PoET παρέχει μια μορφή ισότητας και δικαιοσύνης μεταξύ των κόμβων. Ακόμα η χρήση ειδικού hardware καθιστά το PoET ένα γενικά ανθεκτικό μοντέλο συναίνεσης.
Ωστόσο ένα βασικό μειονέκτημα του PoET είναι η εγγενής εξάρτησή του από τη χρήση του ειδικού αυτού hardware. Συγκεκριμένα μία πλατφόρμα που λειτουργεί στηριζόμενη σε ένα έμπιστο περιβάλλον εκτέλεσης παρέχει αμφιλεγόμενη ασφάλεια έναντι κακόβουλων ενεργειών και στρατηγικών επίθεσης. Σε μία έρευνα των L.Chen κ.ά.[53] θίγονται τα όρια ασφαλείας στο blockchain πρωτόκολλο της SGX πλατφόρμας της Intel και αποδεικνύεται ότι το σύστημα μπορεί να υπερνικηθεί αν οι πιθανοί εχθρικοί κόμβοι ξεπεράσουν το Θ{[log(logn)]/logn} μέρος των n συνολικών κόμβων. Από την άλλη το ίδιο το σύστημα μετράει πόσες φορές ο κάθε κόμβος εκλέγεται ως νικητής της SGX λοτταρίας, οπότε είναι πιο εύκολο να εντοπιστούν κακόβουλες ενέργειες χειραγώγισης.

2.5. Άλλα proof-based συστήματα

Στην ενότητα αυτή αναφέρουμε και σχολιάζουμε κάποια εναλλακτικά συστήματα συναίνεσης τα οποία είτε δεν τόσο δημοφιλή συγκρινόμενα με τα προαναφερθέντα είτε δεν έχουν βρει ακόμα ουσιαστική εφαρμογή στον blockchain κόσμο.

2.5.1.Proof of Burn (PoB)

Το PoB πρωτόκολλο αποτελεί μία λύση στο πρόβλημα της χρονοβόρας και δαπανηρής διαδικασίας εξόρυξης του PoW και χρησιμοποιήθηκε για την παραγωγή νέων νομισμάτων στο κρυπτονόμισμα Slimcoin[54]. Αντί να συμμετέχουν στην διαδικασία της εξόρυξης οι κόμβοι στο PoB ακολουθούν μία διαδικασία κατά την οποία στέλνουν τα νομίσματά τους σε μία διεύθυνση με σκοπό να τα ‘‘κάψουν’’(*coin burning*). Αυτό πρακτικά σημαίνει πως τα νομίσματα αυτά δεν μπορούν πλέον να χρησιμοποιηθούν από κανέναν άλλον, ενώ ο κάθε κόμβος μπορεί να δημιουργήσει ένα μπλοκ ανάλογα με το πόσα νομίσματα έχει κάψει. Επιπλέον οι κόμβοι ανάλογα με το ποσό των νομισμάτων που έχουν θυσιάσει στην διαδικασία του PoB λαμβάνουν και τις αντίστοιχες αμοιβές. Συνεπώς ενθαρρύνοντας τους κόμβους να κάψουν όλο και περισσότερα νομίσματα το PoB επιδιώκει να ενισχύσει την σταθερότητα και την αποκέντρωση δημιουργώντας ένα ιδανικά διανεμημένο δίκτυο συναλλαγών.
Ουσιαστικά το PoB αποτελεί απλά μία βελτιωμένη έκδοση του PoW σχετικά με τον περιορισμό των δαπανών που καταβάλουν οι κόμβοι αλλά και τον τρόπο διανομής των αμοιβών. Ωστόσο η εφαρμογή του είναι περιορισμένη και αποκλειστική μόνο στο Slimcoin.

2.5.2.Proof of EXercise (PoX)

Σύμφωνα με τους δημιουργούς του, το PoX είναι ένα μοντέλο το οποίο αντικαθιστά τα μειονεκτήματα των κατακερματιστικών εργασιών του PoW με επιστημονικά υπολογιστικά προβλήματα που επιλύονται με τη χρήση πινάκων[55]. Οι *employers* του συστήματος παρέχουν τέτοιου είδους προβλήματα τα οποία αναθέτονται στους *miners*. Τόσο οι employers όσο και οι miners καταθέτουν αντίστοιχα κάποιο ποσό, το οποίο θα λάβουν πίσω με την ολοκλήρωση της διαδικασίας επίλυσης, στο σύστημα για την εξασφάλιση της βιωσιμότητας και της διατήρησης του συστήματος. Με την επίλυση ενός προβλήματος οι *verifiers* του συστήματος αναλαμβάνουν την επιβεβαίωση αυτού ώστε να συμπεριληφθεί στο blockchain σύστημα, ενώ για την αποφυγή συγκρούσεων μεταξύ των παραπάνω ομάδων κόμβων οι λύσεις διέρχονται από μία υπηρεσία ανακατεύθυνσης(*shuffling service*).
Η ιδέα του PoX δεν έχει ακόμα εφαρμοστεί σε κάποιο σύστημα, ενώ οι ίδιοι οι δημιουργοί του προτείνουν μια πιο εκτεταμένη μελέτη και ανάλυση ώστε να μπορεί να συγκριθεί με τα υπόλοιπα επικρατέστερα συστήματα συναίνεσης. Ακόμα βασικό μειονέκτημα αποτελεί η ιδιαίτερα μεγάλη πολυπλοκότητα του PoX που καθιστά αρκετά δύσκολη την βέλτιστη επίλυση προβλημάτων στον απαιτούμενο χρόνο.

2.5.3.Proof of Luck (PoL)

Παρόμοια με το PoET το PoL αποτελεί έναν μηχανισμό ομοφωνίας που λειτουργεί σε ένα TEE, όπως το SGX της Intel, και χωρίζεται σε δύο λειτουργικές διαδικασίες, τις

PoLRound και *PoLMine*[56]. Οι κόμβοι που εργάζονται στη δημιουργία των μπλοκ προτιμούν την αλυσίδα εκείνη που το σύστημα ορίζει ως πιο 'τυχερή'. Ο καθορισμός του βαθμού της τύχης αφορά έναν αριθμό μεταξύ του 0 και του 1(*luck value*), ο οποίος παράγεται στο TEE και προστίθεται σε κάθε νέο μπλοκ, με κάθε μεγαλύτερο αριθμό να αντιστοιχεί σε μεγαλύτερο δείκτη τύχης. Πιο τυχερή, άρα και προτιμότερη, είναι η αλυσίδα εκείνη με το υψηλότερο άθροισμα αριθμών τύχης, αρχής γενομένης από το genesis block μέχρι το τελευταίο μπλοκ. Ακόμα το PoL επιβάλει κάποια χρονική καθυστέρηση πριν την τελική έκδοση του επόμενου μπλοκ, η οποία είναι μικρότερη για τα πιο τυχερά μπλοκ, με σκοπό τη βελτιστοποίηση της επικοινωνίας στο σύστημα.
Το PoL παρέχει, σύμφωνα με τους δημιουργούς του, βελτιωμένη διακίνηση των συναλλαγών(15 δευτερόλεπτα για κάθε νέο μπλοκ) και μειωμένη κατάχρηση υπολογιστικής ισχύος. Ωστόσο αποτελεί έναν μηχανισμό ο οποίος παραμένει σε θεωρητικό επίπεδο και φαινομενικά δεν έχει να προσφέρει κάτι ιδιαίτερο πέραν μιας ακόμη προσπάθειας βελτίωσης των μειονεκτημάτων του PoW.

2.5.4.Proof of Space-Proof of Capacity (PoC)

Το Proof of Space[57][58], γνωστό και ως Proof of Capacity(PoC), χρησιμοποιείται στα κρυπτονομίσματα SpaceMint[59] και Burst[60] παρέχοντας πιο διανεμημένη και οικονομική συμμετοχή και μικρότερη κατανάλωση πόρων συγκριτικά με το PoW. Αντί για υπολογιστικές μονάδες οι χρήστες πρέπει να επενδύσουν σε, δεδομένα φθηνότερο, αποθηκευτικό χώρο για να μπορέσουν να ολοκληρώσουν τα απαραίτητα υπολογιστικά προβλήματα στο σύστημα. Ο PoC αλγόριθμος κατά τη διάρκεια της εργασίας δημιουργεί πολλά μεγάλα σύνολα δεδομένων στο σκληρό δίσκο(*plots*), με τους κόμβους να διεκδικούν το δικαίωμα του επόμενου μπλοκ ανάλογα με την ποσότητα των δεδομένων που διαθέτουν[48]. Εφόσον ένας κόμβος δεν διαθέτει επαρκή αποθηκευτικό χώρο αποκλείεται από την συμμετοχή στη διαδικασία συναίνεσης[61].
Συνεπώς, αν και το PoC είναι μία ενεργειακά και χρηματικά περισσότερο συμφέρουσα επιλογή από το PoW, η διαδικασία ομοφωνίας που ακολουθείται φαίνεται να ευνοεί τους κόμβους εκείνους που διαθέτουν περισσότερο αποθηκευτικό χώρο στις υπολογιστικές τους μονάδες δημιουργώντας πρόβλημα στην έννοια της αποκέντρωσης. Επίσης η ασφάλεια δεν είναι δεδομένη καθώς οι κακόβουλοι χρήστες δεν ελέγχονται από το σύστημα με αποτέλεσμα να μπορούν πιθανώς να το εκμεταλλευτούν, εισάγωντας για παράδειγμα κακόβουλο λογισμικό εξόρυξης.

2.5.5.Proof of Familiarity (PoF)

Το PoF αποτελεί έναν συγκεντρωτικό αλγόριθμο συναίνεσης ο οποίος σχεδιάστηκε για να αφομοιώνει ιατρικές αποφάσεις των ενδιαφερόμενων κόμβων(ασθενείς, γιατροί, ασφαλιστικές εταιρίες κ.ά.) για την υγειονομική περίθαλψη[62]. Ακολουθώντας τις βασικές αρχές της blockchain τεχνολογίας το PoF διασφαλίζει την

ακεραιότητα, το ιδιωτικό απόρρητο και υψηλά επίπεδα ασφάλειας στον τομέα της υγείας, παρέχοντας τα επιθυμητά επίπεδα διαφάνειας και διαλειτουργικότητας μεταξύ των κόμβων. Το PoF έχει δοκιμαστεί από την blockchain πλατφόρμα Multichain 2.0[63], η οποία κατέδειξε κάποιες προνομιακές πτυχές του αλγορίθμου, όπως το μειωμένο κόστος χρήσης, η μη εξάρτηση από το μεγάλο μέγεθος των μπλοκ, τα περιθώρια βελτίωσης της επεκτασιμότητας μέσω του κοινοπρακτικού blockchain χαρακτήρα, οι τεράστιες δυνατότητες διακίνησης μέχρι και 2000000 συναλλαγές ανά δευτερόλεπτο και η άμεση οριστικότητα.
Ωστόσο το PoF είναι ένα μοντέλο συναίνεσης με αποκλειστική εφαρμογή στον υγειονομικό τομέα, το οποίο αναμένεται να δοκιμαστεί σε πραγματικό περιβάλλον στο Inje University Hospital στην Κορέα[64].

2.5.6.Proof of Trust (PoT)

Το PoT αποτελεί μία αρχιτεκτονική συναίνεσης η οποία ενσωματώνει ένα κοινοπρακτικό blockchain σύστημα σε ένα δημόσιο δίκτυο υπηρεσιών[65]. Στο PoT η συναίνεση πραγματοποιείται σε τέσσερα στάδια: αρχικά(*phase 1*) πραγματοποιείται η εκλογή του ηγέτη(*leader*) της ομάδας διαχείρισης του κοινοπρακτικού συστήματος(*ledger management group*), στηριζόμενη στον αλγόριθμο εκλογικής ηγεσίας Raft[66], μεταξύ των μελών της ομάδας(*leader, candidates, followers*). Στη συνέχεια(*phase 2*) ο ηγέτης επιλέγει μία ομάδα επικύρωσης συναλλακτικών υπηρεσιών(*service transaction validation group*) από μία λίστα επικυρωτών που ο ίδιος έχει συνθέσει στηριζόμενος σε κάποια απαραίτητα κριτήρια(*πχ trust value*), η οποία ομάδα προχωράει στην επιλογή-εκλογή των συναλλαγών που θα συμπεριληφθούν στο επόμενο μπλοκ(*phase 3*). Τέλος ακολουθεί η επανεκλογή των συναλλαγών από την ομάδα διαχείρισης, ενώ ο ηγέτης συγκεντρώνει, αξιολογεί και ολοκληρώνει την εγκατάσταση του νέου μπλοκ συναλλαγών στο σύστημα. Με την παραπάνω διαδικασία οι δημιουργοί του PoT ισχυρίζονται πως η προσέγγισή τους αποτελεί μία καινοτομία στον κλάδο των ηλεκτρονικών υπηρεσιών, κάτι που θεωρούμε πως σε πρώτο στάδιο επιβεβαιώνεται με την παροχή διανεμημένης διακυβέρνησης και βελτιωμένης διακίνησης και επεκτασιμότητας συγκριτικά με άλλα ευρέως διαδεδομένα blockchain συστήματα. Πρόκειται για ένα πολύ ενδιαφέρον μοντέλο συναίνεσης και μένει η εφαρμογή του στον πραγματικό κόσμο της blockchain βιομηχανίας για να αξιολογηθεί πιο πρακτικά και ουσιαστικά.

2.5.7.Proof of Authority (PoA)

Το PoA[67] είναι ένα μοντέλο συναίνεσης το οποίο αποτελεί μία πιο αποδοτική μορφή του κλασσικού PoS και μπορεί να εφαρμοστεί τόσο στα δημόσια(*Ethereum testnet Krovan*) όσο και στα ιδιωτικά blockchain συστήματα(*Parity*[68]). Το PoA δεν στηρίζεται ούτε στην επίλυση πολύπλοκων και χρονοβόρων μαθηματικών προβλημάτων, όπως στο PoW, ούτε στην κατοχή κάποιας μορφής stake, όπως στο PoS. Αντίθετα χρησιμοποιεί ένα σύνολο αξιών-κόμβων(*authorities*) οι οποίοι είναι

υπεύθυνοι για τη δημιουργία νέων μπλοκ και την ασφάλεια του συστήματος. Οι κόμβοι αυτοί εκλέγονται στα διάφορα στάδια(*steps*) και διαθέτουν ο καθένας μία μοναδική ταυτότητα. Σύμφωνα με τους συγγραφείς κατά την ανάλυση και τη σύγκριση του PoA με το PBFT, το οποίο θα αναλύσουμε σε επόμενη ενότητα, το PoA φαίνεται πως θυσιάζει τη θεμελιώδη έννοια της συνεκτικότητας προς όφελος της διαθεσιμότητας, το οποίο σημαίνει πως σε συνθήκες όπου η ακεραιότητα των δεδομένων είναι ζωτικής σημασίας το PBFT θεωρείται προτιμότερη επιλογή[67]. Ακόμα το PoA με σκοπό να γίνει ταχύτερο βελτιώνοντας την αποδοτικότητά του θυσιάζει σε ένα μεγάλο βαθμό την έννοια της εμπιστοσύνης στο δίκτυο.
Επομένως το PoA χρειάζεται μελλοντικά μεγαλύτερη ανάλυση και δοκιμή σε πραγματικό χρόνο ώστε να μπορεί να αξιολογηθεί πιο ουσιαστικά και ως προς τη διακίνηση και την επεκτασιμότητα.

2.5.8.Proof of Authentification (PoAh)

Αποτελώντας έναν επιπλεόν μηχανισμό συναίνεσης με σκοπό να αντικαταστήσει το PoW, το PoAh[69] ολοκληρώνει την δημιουργία των μπλοκ μέσω μίας διαδικασίας επαλήθευσης. Ένα PoAh μοντέλο διαχωρίζει τους κόμβους σε *individual nodes* και *trusted nodes*. Οι individual nodes δημιουργούν τα μπλοκ με τις απαραίτητες συναλλαγές και δεδομένα τα οποία προωθούνται για επιπλέον αξιολόγηση στους trusted nodes, οι οποίοι αξιολογούν τα δεδομένα των μπλοκ σε δύο στάδια και με βάση την αξία εμπιστοσύνης που έχουν κερδίσει στο σύστημα επιστρέφουν στους αρχικούς κόμβους την επαληθευμένη τελική έκδοση των μπλοκ.
Σύμφωνα με θεωρητικές προσεγγίσεις αλλά και πειράματα σε περιβάλλοντα προσομοίωσης το PoAh παρέχει χρονικές καθυστερήσεις της τάξης των 3-4.5 δευτερολέπτων, τιμές καθόλου αδιάφορες συγκριτικά με το PoW. Βέβαια να αναφέρουμε ότι οι παραπάνω ενδείξεις επιτεύχθηκαν με τη συμμετοχή μόνο 5 αντιπροσωπευτικών κόμβων. Το συμπέρασμα των παραπάνω είναι πως αν και το PoAh παρέχει σχετικά χαμηλή σπατάλη ενέργειας και πόρων αλλά και σημαντικές ενδείξεις βελτιωμένης απόδοσης και προοπτικές επεκτασιμότητας, οφείλουμε να αναμένουμε την εφαρμογή του σε πλατφόρμες με μεγαλύτερο πλήθος χρηστών και πιο ρεαλιστικές συνθήκες υλοποίησης ώστε να μπορέσουμε να το αξιολογήσουμε πιο ορθά.

2.5.9.Proof of Possession (PoP)

Το PoP, ή αλλιώς *Provable Data Possession(PDP)*, είναι ένα μοντέλο που χρησιμοποιείται για απομακρυσμένο έλεγχο δεδομένων σε μεγάλα σύνολα δεδομένων στα ευρέως διανεμημένα συστήματα αποθήκευσης[70]. Ο M.Jones κατέδειξε διάφορα πεδία και εφαρμογές χρήσης καθώς και τη χρησιμότητα του PoP στο διαδίκτυο[71]. Στη blockchain πραγματικότητα το PoP έχει υλοποιηθεί σε smart contracts του Ethereum καταδεικνύοντας την ελάττωση του κόστους σε ιδιωτικό αλλά όχι σε δημόσιο περιβάλλον[72].

Το PoP δεν μοιάζει να είναι ένα μοντέλο συναίνεσης που θα μπορέσει να απασχολήσει περεταίρω τα blockchain συστήματα, ενώ σε περιπτώσεις που το πρωτόκολλο έχει σχεδιαστεί σωστά το PoP δεν προσφέρει κάτι ουσιαστικό, όπως για παράδειγμα ενίσχυση της ασφάλειας, πέραν της μερικής μείωσης του κόστους[73].

2.5.10. Proof of Vote (PoV)

Το PoV αποτελεί έναν μηχανισμό συναίνεσης που αναφέρεται αποκλειστικά στα κοινοπρακτικά blockchain συστήματα, με κύρια χαρακτηριστικά την ασφάλεια, τη χαμηλή ενεργειακή κατανάλωση και την υψηλή απόδοση[74]. Με τον μηχανισμό ψηφοφορίας και το διαχωρισμό των συμμετέχοντων κόμβων-συνεταίρων σε τέσσερις ρόλους, *commissioner, butler candidate, butler, and ordinary user*, το PoV διαμοιράζει τα δικαιώματα και επιτυγχάνει την αποκεντρωμένη συναίνεση. Συγκρινόμενο με άλλα δημοφιλή PoW συστήματα, το PoV παρέχει μικρές χρονικές καθυστερήσεις και πολύ καλή διακίνηση, καθώς κάθε μπλοκ δημοσιεύεται ανά 15 δευτερόλεπτα, ενώ η οριστικότητα είναι άμεση καθώς απαιτείται μόνο η πρώτη επιβεβαίωση για τα μπλοκ.

2.5.11. Proof of Bandwidth (PoBw)

Το PoBw χρησιμοποιείται σε συστήματα όπου οι διαδικασίες μεταβατικών καταστάσεων κατανέμονται πιθανολογικά ανάλογα με το εύρος ζώνης που διαθέτουν οι συμμετέχοντες κόμβοι στο δίκτυο. Η λειτουργία του PoBw περιγράφεται στο πρωτόκολλο TorCoin και στο TorPath σχέδιο[75] που χρησιμοποιούνται στο Tor[76], μία διαδικτυακή υπηρεσία ανώνυμης επικοινωνίας. Όπως περιγράφεται στο TorCoin, οι κόμβοι συνδέονται με τη βοήθεια υπο-γραφικών μέσων(*paths*) στο ευρύτερο δίκτυο. Τα μέσα αυτά συνδέονται σύμφωνα με κάποια σταθμισμένα άκρα, η στάθμιση των οποίων υπολογίζεται και υπογράφεται από αποκεντρωμένους εξυπηρετητές σύμφωνα με τη διακίνηση της μεταφοράς πληροφοριών σε μία διαδρομή. Έτσι το PoBw πρωτόκολλο απαιτεί από τους κόμβους του δικτύου να συνεισφέρουν σε αυτό με τη δέσμευση εύρους ζώνης και να συνδέονται με άλλους κόμβους που διαθέτουν υψηλό εύρος ζώνης. Συνεπώς η απόδειξη συνεισφοράς στο δίκτυο είναι αναλογική του εύρους ζώνης ενός κόμβου.

2.6. Byzantine Aggreement (BA)

Όπως γίνεται εύκολα αντιληπτό οι μέθοδοι συναίνεσης που έχουμε περιγράψει παραπάνω χρησιμοποιούν ένα μέσο ή μία διαδικασία απόδειξης που επιτρέπει στους κόμβους να συνεχίζουν το αντίστοιχο blockchain σύστημα προσθέτοντας το επόμενο μπλοκ στην αλυσίδα. Ωστόσο υπάρχει μία οικογένεια συστημάτων που διαφοροποιείται από τα προαναφερθέντα μοντέλα καθώς η διαδικασία επίτευξης ομοφωνίας βασίζεται αποκλειστικά στην ολοκλήρωση διάφορων μορφών και σταδίων ψηφοφορίας στο δίκτυο, οδηγώντας σε μία σαφή διάκριση των μοντέλων συναίνεσης στα *proof-based* και *vote-based* μοντέλα[48]. Τα BA ή BFT(*Byzantine Fault Tolerant*) πρωτόκολλα έχουν ως σκοπό την επίτευξη της ομοφωνίας μέσα σε ένα περιβάλλον που περιλαμβάνει την υπόθεση εμφάνισης τόσο των crash όσο και των Byzantine failures που έχουμε περιγράψει στην Ενότητα 1.2.4.

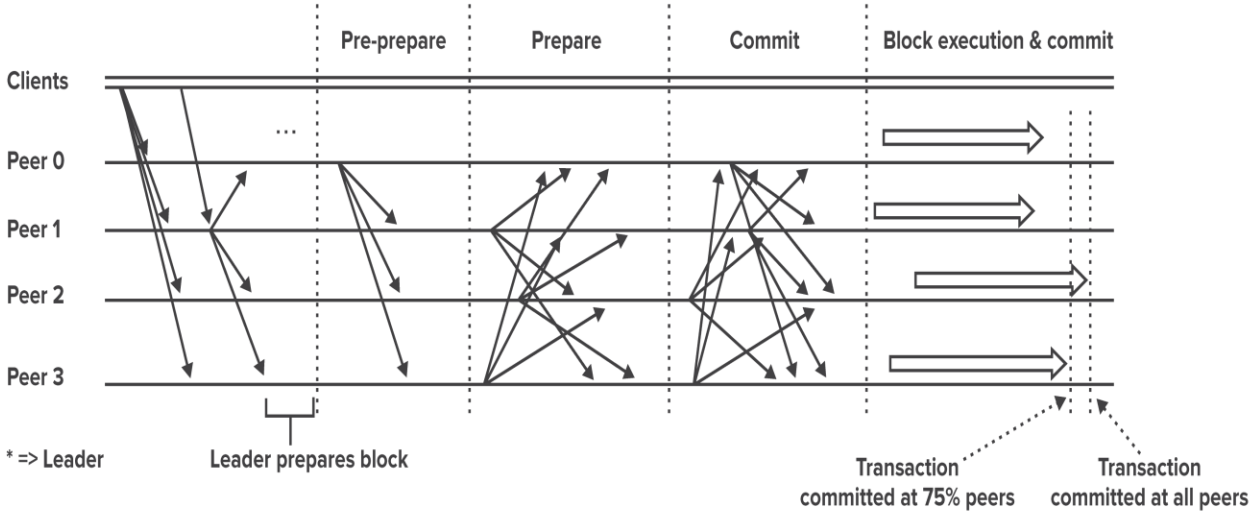
2.6.1.Practical Byzantine Fault Tolerance (PBFT)

Ο αλγόριθμος αυτός παρουσιάστηκε από τους M.Castro και B.Liskov[77] με σκοπό την αντιμετώπιση του προβλήματος των Βυζαντινών απειλών στα διανεμημένα συστήματα. Λόγω της δομής του το PBFT αποτελεί ένα μοντέλο ομοφωνίας ιδανικό για blockchain συστήματα με περιορισμένο πλήθος κόμβων, ώστε να επιτυγχάνονται γρήγορες συναλλαγές μεταξύ έμπιστων κόμβων γνωστών σε ολόκληρο το δίκτυο. Συγκεκριμένα σε ένα blockchain σύστημα που λειτουργεί με βάση το PBFT πρότυπο οι συναλλαγές ολοκληρώνονται αφού περάσουν μέσα από μία διαδικασία πολλαπλών γύρων ψηφοφορίας την οποία απαρτίζουν ο ηγετικός κόμβος(*leader node*) και οι υπόλοιποι κόμβοι του δικτύου(*validating nodes*). Η διαδικασία αυτή αποτελείται από πέντε στάδια-φάσεις: *request*, *pre-prepare*, *prepare*, *commit*, *reply*. Στην πρώτη φάση ο πελάτης στέλνει την συναλλαγή στον leader node, ο οποίος επιβεβαιώνει χρονολογικά το αίτημα αυτό, στη συνέχεια ακολουθούν τα επόμενα στάδια επεξεργασίας-ψηφοφορίας όπως φαίνεται στην Εικόνα 8, ενώ στο τελευταίο στάδιο ο leader node ενημερώνει τον πελάτη για την ολοκλήρωση της συναλλαγής[78]. Για τη συμμετοχή στα στάδια αυτά οι validating nodes πρέπει να συγκεντρώσουν την αποδοχή των ψήφων των 2/3 του υπόλοιπου δικτύου, ενώ ο leader node συντονίζει τις ενέργειες της διαδικασίας.

Η επίτευξη ομοφωνίας μέσω του PBFT δεν απαιτεί ιδιαίτερη ενεργειακή δαπάνη, ενώ το περιβάλλον εμπιστοσύνης που απαιτείται να κυριαρχεί στην αλληλεπίδραση μεταξύ των κόμβων καθιστά το δίκτυο ιδιαίτερα αποδοτικό με μηδαμινές χρονικές καθυστερήσεις και θεωρητικά δεκάδες χιλιάδες συναλλαγών[79]. Αναφέρουμε τη λέξη θεωρητικά καθώς το PBFT έχει δοκιμαστεί σε δίκτυα της τάξεως των 10-20 κόμβων όπου οι συναλλαγές δεν μπορούν να επιτύχουν τόσο μεγάλες επιδόσεις.

Το PBFT είναι ουσιαστικά χρήσιμο σε πλατφόρμες που λειτουργούν σε ιδιωτικό περιβάλλον με περιορισμένους και επιλεγμένους χρήστες, σε αντίθεση για παράδειγμα με το δημόσιο δίκτυο του Bitcoin και του Ethereum, όπου η συμμετοχή είναι ανοιχτή στον καθένα. Η IBM λειτουργεί το ιδιωτικό της blockchain δίκτυο στηριζόμενη στο πρόγραμμα Hyperledger Fabric[80] της Linux Foundation[81], το οποίο αποτελεί τη δημοφιλέστερη υλοποίηση του PBFT. Μέσω του PBFT το

Hyperledger Fabric ολοκληρώνει 2000-3500 συναλλαγές ανά δευτερόλεπτο, ενώ για την ολοκλήρωση των συναλλαγών απαιτείται χρόνος λιγότερος του 1 δευτερολέπτου.



Εικόνα 8-Διάγραμμα ροής των συναλλαγών στο PBFT[82]

2.6.2.HoneyBadger BFT

Οι A.Miller κ.ά. παρουσίασαν το HoneyBadger BFT[83], ένα αποδοτικό και με μεγάλη διακίνηση σύγχρονο πρωτόκολλο, με σκοπό να αντικαταστήσουν το παγιωμένο μερικώς ασύγχρονο PBFT πρωτόκολλο. Σε πειραματικές μετρήσεις που πραγματοποιήθηκαν στο Amazon EC2 καταγράφηκαν περίπου 20000 συναλλαγές ανά δευτερόλεπτο σε δίκτυο 40 κόμβων και 1500 σε πιο επεκτάσιμα δίκτυα με 104 κόμβους. Συγκρινόμενο με το PBFT το HoneyBadger BFT κατέγραψε περισσότερες συναλλαγές ανά δευτερόλεπτο παράλληλα με την αύξηση των κόμβων στο δίκτυο, με τα δύο πρωτόκολλα να χαρακτηρίζονται μεν από την ίδια πολυπλοκότητα στην δικτυακή επικοινωνία, αλλά το HoneyBadger BFT να παρουσιάζει πιο σταθερή διακίνηση.

Ωστόσο δεν μπορούμε ακόμα να τοποθετήσουμε το πρωτόκολλο αυτό ανάμεσα στα πιο σημαντικά και να το συγκρίνουμε με αυτά, καθώς όπως τα περισσότερα εναλλακτικά blockchain πρωτόκολλα περιορίζονται είτε σε πειραματικές και ερευνητικές μετρήσεις είτε σε ποιοτικές μελέτες, καθιστώντας την ουσιαστική τους αξιολόγησή αδύνατη.

2.6.3.Delegated Byzantine Fault Tolerance (DBFT)

Το DBFT αποτελεί έναν αλγόριθμο ο οποίος χρησιμοποιεί την ίδια λογική και κανόνες με το PBFT με τη διαφορά ότι δεν απαιτείται η καθολική συμμετοχή όλων των κόμβων του δικτύου στη διαδικασία επίτευξης ομοφωνίας. Συγκεκριμένα σε ένα DBFT σύστημα, όπως η κρυπτονομισματική πλατφόρμα NEO, οι κόμβοι διαχωρίζονται σε δύο κατηγορίες, τους *ordinary nodes* και τους *bookkeepers*[84]. Οι κόμβοι της πρώτης κατηγορίας δεν συμμετέχουν στην διαδικασία ομοφωνίας, αλλά εκλέγουν τους κόμβους της δεύτερης κατηγορίας, οι οποίοι είναι εκείνοι που θα συμφωνήσουν για την εγκυρότητα η μη των συναλλαγών και προχωρούν σε κάθε ένα από τα διαδοχικά στάδια ψηφοφορίας αρκεί να συγκεντρώσουν την αποδοχή των 2/3 του δικτύου. Ουσιαστικά θα μπορούσαμε να χαρακτηρίσουμε το DBFT ως έναν αλγόριθμο που συνδυάζει το DPoS με την γενικότερη BA λογική, αποτελώντας μία υβριδική συναινετική μέθοδο στην blockchain τεχνολογία. Κάποια από τα ιδιαίτερα χαρακτηριστικά που προσφέρει το DBFT είναι οι χαμηλές ενεργειακές απαιτήσεις και η άμεση οριστικότητα των συναλλαγών[85]. Ακόμα κάθε νέο μπλοκ συναλλαγών δημιουργείται ανά 15-20 δευτερόλεπτα, ενώ οι συναλλαγές ανά δευτερόλεπτο στην πλατφόρμα του NEO μπορούν να προσεγγίσουν τις 1000.
Οι Y.Wang κ.ά.[86] πρότειναν μία βελτιωμένη εκδοχή του DBFT, το credit-delegated Byzantine fault tolerance(CDBFT), το οποίο μέσω της πιστοληπτικής αξιολόγησης βελτιώνει την απόδοση του υπό χρήση συστήματος, καθώς επιτυγχάνει την μείωση των επιπέδων επικοινωνίας και της συμμετοχής ανεπιθύμητων κόμβων.

2.6.4.Simplified Byzantine Fault Tolerance (SBFT)

Στον συγκεκριμένο μηχανισμό συναίνεσης, το οποίο χρησιμοποιεί η πλατφόρμα Chain, η ολοκλήρωση των συναλλαγών πραγματοποιείται μέσα από πέντε διαδοχικά στάδια[87]: αρχικά, στο *creation phase*, το κάθε μπλοκ συναλλαγών δημιουργείται από έναν και μόνο κόμβο(*block generator*). Στη συνέχεια ακολουθούν τα *submission, validation, signing* και *pulling into nodes phases,* στα οποία οι συναλλαγές ελέγχονται, εγκρίνονται και προωθούνται στους υπόλοιπους κόμβους του δικτύου μέχρι την τελική φάση, όπου οι συναλλαγές έχουν ολοκληρωθεί. Η λειτουργία του SBFT στηρίζεται αποκλειστικά στην εμπιστοσύνη μεταξύ των κόμβων και καταλήγει σε ομοφωνία υπό την προϋπόθεση ότι αν υπάρχουν n ελλαττωματικοί κόμβοι, το κάθε μπλοκ συναλλαγών πρέπει να εγκριθεί από τουλάχιστον 2n+1 κόμβους.
Ως μηχανισμός συναίνεσης είναι ταχύτερος και διαθέτει μεγαλύτερη επεκτασιμότητα από το PoW. Από την άλλη, παρόμοια με το PBFT, είναι κατάλληλος σε ιδιωτικά συστήματα και χαρακτηρίζεται από χαμηλά επίπεδα αποκεντρωτισμού. Συν τοις άλλοις ως μηχανισμός έχει ελάχιστη εφαρμογή μέχρι σήμερα στον blockchain κόσμο, οπότε δεν μπορεί να αξιολογηθεί ουσιαστικά.

2.6.5.Probabilistic Byzantine Voting-Ripple Protocol Consensus Algorithm (RPCA)

Το RPCA[88] είναι μία ιδέα των C.Schwartz, N.Youngs και A.Britto με σκοπό την επίτευξη ομοφωνίας σε ένα περιβάλλον που διασφαλίζει την ορθότητα, την χρησιμότητα και τη μέγιστη δυνατή αποδοτικότητα. Το Ripple λειτουργεί σε ένα δίκτυο, το RippleNet[89], με το όραμα της σύνδεσης των τραπεζικών οντοτήτων, των πλατφορμών ανταλλαγής και των παρόχων πληρωμών χρησιμοποιώντας ως μέσο συναλλαγής το τοπικό του κρυπτονόμισμα XRP. Στο δίκτυο του Ripple κάθε κόμβος που συμμετέχει στη διαδικασία ομοφωνίας(*server node*) ορίζει μία λίστα από έμπιστους κόμβους(*Unique Node List-UNL*). Κάθε κόμβος δημοσιοποιεί τις υπό έγκριση συναλλαγές στους υπόλοιπους κόμβους της UNL, οι οποίες συναλλαγές συλλέγονται σε μία δομή δεδομένων(*candidate set*). Η ομοφωνία επιτυγχάνεται σε πολλαπλούς γύρους ψηφοφορίας, στους οποίους για να θεωρηθούν έγκυρες οι συναλλαγές πρέπει να συγκεντρώσουν το 80% των ψήφων αποδοχής σε κάθε UNL. Στον τελευταίο γύρο το candidate set που έχει υπερψηφιστεί από την απαιτούμενη πλειοψηφία αποτελεί το *Last Closed Ledger(LCL)* και τοποθετείται από όλους τους κόμβους στην ευρύτερη αλυσίδα του Ripple blockchain. Μέσω της λειτουργίας αυτής το Ripple διαμοιράζει την εργασία στο δίκτυο σε πολλαπλές ομάδες κόμβων, οι οποίοι εργάζονται παράλληλα μέσα στο ίδιο δίκτυο χωρίς να απαιτείται η συνολική εμπιστοσύνη και ιδιαίτερη συνδεσιμότητα μεταξύ αυτών, όπως συμβαίνει για παράδειγμα στα προαναφερθέντα BA μοντέλα. Έτσι το RPCA επιτυγχάνει την ολοκλήρωση των συναλλαγών παρέχοντας μηδαμινές χρονικές καθυστερήσεις(μέση ταχύτητα συναλλαγών στα 4 δευτερόλεπτα), απεριόριστη συμμετοχή και εντυπωσιακούς δείκτες απόδοσης(1500 συναλλαγές ανά δευτερόλεπτο με δυνατότητα επέκτασης στις 50000) που μπορούν να ανταγωνιστούν ή και να προσπεράσουν τα δημοφιλέστερα δίκτυα διαδικτυακών συναλλαγών, όπως η Visa και το Paypal.

2.6.6.Federated Byzantine Aggreement-Stellar Consensus Protocol (SCP)

Το SCP[90] εισάχθηκε από τον D.Mazieres και αποτελεί μία βελτιωμένη εκδοχή των BA πρωτοκόλλων εισάγοντας τις έννοιες των *quorum* και *quorum slices*. Συγκεκριμένα στο SCP ο κάθε κόμβος επιλέγει ελεύθερα τους υπόλοιπους κόμβους που επιθυμεί να εμπιστευτεί, με αποτέλεσμα τη δημιουργία των quorum slices, τα οποία αποτελούν ομάδες κόμβων που λειτουργούν σε ένα περιβάλλον εμπιστοσύνης και συνεργασίας προς όφελος του συστήματος. Η συμμετοχή σε μία τέτοια ομάδα είναι, σε αντίθεση με τα UNL στο δίκτυο του Ripple, ανοιχτή σε όλους και απεριόριστη, γεγονός που σημαίνει πως ένας κόμβος μπορεί να συμμετέχει παράλληλα σε περισσότερα από ένα quorum slices[91]. Το δίκτυο που συνθέτουν τα διάφορα quorum slices οδηγεί στην έννοια των quorums τα οποία αποτελούν ομάδες κόμβων οι οποίες είναι ικανές και επαρκείς για να οδηγήσουν στην επίτευξη συμφωνίας.

Το SCP αποτελεί ένα ομοσπονδιακό BA πρωτόκολλο(*Federated Byzantine Aggreement*) όπου η επίτευξη ομοφωνίας πραγματοποιείται σε δύο στάδια

υποψηφιότητας(*nomination protocol*) και ψηφοφορίας(*ballot protocol*). Αρχικά ο κάθε κόμβος καλείται να ψηφίσει μία μόνο αξία ανάμεσα σε ένα πλήθος υποψήφιων αξιών(*candidate set*) ως έγκυρη. Οι αξίες που υπερψηφίζονται ομόφωνα προάγονται στο δεύτερο στάδιο, όπου πραγματοποιείται μία νέα ψηφοφορία σχετικά με το αν οι επιλεγμένες αξίες θα επικυρωθούν στο δίκτυο ή αν θα απορριφθούν. Σε περίπτωση που οι κόμβοι δεν μπορούν να αποφανθούν σχετικά με την κατάληξη μιας εκκρεμούς αξίας, το σύστημα οδηγεί στην έναρξη νέας ψηφοφορίας ώστε να αποφεύγονται καταστάσεις που το σύστημα "παγώνει"(*stuck states*)[92].
Στο SCP η ομοφωνία στο σύστημα απαιτεί την διασταύρωση των quorums(*quorum intersection*), κατά την οποία πρέπει να υπάρχει τουλάχιστον ένας λειτουργικός και ειλικρινής κόμβος στο δίκτυο, καθώς και τη διαθεσιμότητα των quorums(*quorum availability*), η οποία αναφέρεται στην ύπαρξη μέσα στο συνολικό δίκτυο ενός τουλάχιστον quorum που δεν περιέχει κακόβουλους ή μη λειτουργικούς κόμβους, [93]. Οι δύο παραπάνω έννοιες συνεισφέρουν στη διασφάλιση της συνέχειας και της συνέπειας του SCP προστατεύοντας το από πιθανά stuck states και forks.
Αν και το SCP θεωρείται γενικά ως ένα πρωτόκολλο που πέραν των πολλών πλεονεκτημάτων του εξασφαλίζει την αποκέντρωση, μία πρόσφατη έρευνα των M.Kim κ.ά. πάνω στη δομή των quorum slices κατέδειξε πως το SCP χαρακτηρίζεται από σημαντικά επίπεδα συγκεντρωτισμού, κάτι που οδηγεί και σε σημαντικές επιπλοκές στην γενικότερη ασφάλεια του δικτύου[94].
Όσον αφορά τα επίπεδα διακίνησης στο SCP οι συναλλαγές ολοκληρώνονται άμεσα(ανά 2-5 δευτερόλεπτα) παρόμοια με το Ripple και είναι κατά μέσο όρο 1000 ανά δευτερόλεπτο[95].

2.7. Σύγκριση των κυριότερων μηχανισμών συναίνεσης

Έχοντας περιγράψει τους βασικότερους μηχανισμούς συναίνεσης ως προς τον τρόπο λειτουργίας και τα κύρια χαρακτηριστικά τους θα προχωρήσουμε σε μία αναλυτική σύγκριση μεταξύ τους, παρουσιάζοντας στοιχειώδης διαφορές και προσπαθώντας να δώσουμε μία πιο ξεκάθαρη εικόνα αναφορικά με το πότε, το γιατί και το πού μπορεί να εφαρμοστεί ο κάθε μηχανισμός στον κόσμο της blockchain τεχνολογίας. Η σύγκριση που ακολουθεί δεν περιλαμβάνει όλους τους μηχανισμούς συναίνεσης που έχουμε παρουσιάσει παραπάνω αλλά αφορά τους μηχανισμούς PoW, PoS, DPoS, PoET, PFBT, RPCA και SCP. Οι υπόλοιποι μηχανισμοί δεν συμπεριλαμβάνονται στην παρακάτω σύγκριση καθώς τα δεδομένα που είναι διαθέσιμα για αυτούς αναφορικά με κάποια βασικά ποιοτικά-ποσοτικά χαρακτηριστικά, το εύρος χρήσης και τον αντίκτυπό τους στην επιστημονική κοινότητα είναι για την ώρα ελλιπή και ανεπαρκώς αξιολογημένα.

2.7.1.Οριστικότητα συναλλαγών (transaction finality)

Η οριστικότητα ή τελικότητα σε ένα blockchain σύστημα αναφέρεται στην επιβεβαίωση ότι ένα μπλοκ, άρα και οι συναλλαγές που περιλαμβάνει, που έχει προστεθεί στην ευρύτερη αλυσίδα του συστήματος δεν μπορεί να ανακαλεστεί. Οι χρήστες που πραγματοποιούν συναλλαγές σε ένα blockchain δίκτυο θέλουν να διασφαλίσουν ότι οι συναλλαγές που πραγματοποιούνται δεν μπορούν να μεταβληθούν ή να αντιστραφούν, καθώς σε μία τέτοια περίπτωση θα οδηγηθούν σε εναλλακτικές μεθόδους πληρωμών προκαλώντας τη δυσφήμιση της εκάστοτε blockchain πλατφόρμας. Συνεπώς η οριστικότητα παίζει καταλυτικό ρόλο κατά την επιλογή ενός μηχανισμού ομοφωνίας καθώς με απλά λόγια διασφαλίζει ότι οι παρελθοντικές συναλλαγές έχουν οριστικά ολοκληρωθεί και δεν διατρέχουν τον κίνδυνο να καταλήξουν σε κάποιο *orphan block*[96].
Ωστόσο η έννοια της οριστικότητας δεν είναι αμοιβαία σε όλα τα blockchain συστήματα, με αποτέλεσμα να διαχωρίζουμε την οριστικότητα σε πιθανολογική(*probabilistic finality*) και απόλυτη ή καθοριστική(*absolute-deterministic finality).*

2.7.1.1. Πιθανολογική οριστικότητα (probabilistic finality)

Η πιθανολογική οριστικότητα χαρακτηρίζει τα πρωτόκολλα εκείνα που στηρίζουν την επίτευξη ομοφωνίας τους στον κανόνα της μεγαλύτερης αλυσίδας. Αυτό σημαίνει πως μία συναλλαγή που περιέχεται σε ένα μπλοκ που είναι τοποθετημένο βαθύτερα στην ευρύτερη κύρια αλυσίδα των συναλλαγών έχει πολύ λίγες πιθανότητες να αναστραφεί καθώς η "μακρύτερη αλυσίδα" είναι αυτή που επιλέγεται από τους κόμβους για την ολοκλήρωση των μπλοκ έναντι των υπόλοιπων πιθανών forks. Μία παράμετρος που είναι κομβικής σημασίας για την κατανόηση της πιθανολογικής οριστικότητας είναι το χρονικό διάστημα που απαιτείται ώστε μία συναλλαγή να οριστικοποιηθεί για πάντα. Το χρονικό αυτό διάστημα είναι ευρέως γνωστό ως χρονική καθυστέρηση(*latency*) η οποία προηγείται του τερματισμού μιας συναλλαγής. Παίρνοντας ως παράδειγμα το πρωτόκολλο του Bitcoin μία συναλλαγή από τη χρονική στιγμή που δημιουργείται θεωρείται αμετάβλητη. Ωστόσο δυστυχώς δεν είναι την ίδια χρονική στιγμή οριστική. Αντιθέτως ένας χρήστης πρέπει να περιμένει περίπου 60 λεπτά, καθώς κάθε μπλοκ δημιουργείται ανά 10 λεπτά και για να μεγιστοποιηθεί η πιθανότητα ολοκλήρωσης των συναλλαγών πρέπει να ολοκληρωθούν 6 επιβεβαιώσεις, που σημαίνει ότι ο χρήστης πρέπει να περιμένει να τοποθετηθούν στην αλυσίδα 6 μπλοκ από τη δημιουργία της συναλλαγής του[97]. Βέβαια ακόμα και μετά από 60 λεπτά η πιθανότητα μη αναστρεψιμότητας δεν φτάνει το 100%, αλλά σύμφωνα με μετρήσεις το προσεγγίζει τόσο πολύ ώστε ο χρόνος αυτός σε συνδυασμό με την υπόθεση πως ένας κακόβουλος χρήστης δεν ελέγχει περισσότερο από το 25% του δικτύου να θεωρείται ικανός για την πιθανολογική οριστικότητα[98]. Εννοείται πως η αναμονή για περισσότερες επιβεβαιώσεις αυξάνει ακόμα περισσότερο την πιθανότητα της οριστικότητας, η οποία από την άλλη μειώνεται όσο αυξάνεται το ποσοστό του δικτύου που ελέγχουν οι κακόβουλοι χρήστες.

Γενικά τα συστήματα που χρησιμοποιούν proof-based αλγόριθμους χαρακτηρίζονται από τέτοιες χρονικές καθυστερήσεις με σκοπό να ελαχιστοποιούν την πιθανότητα ανατροπής μίας συναλλαγής. Όπως περιγράψαμε παραπάνω οι καθυστερήσεις αυτές ισοδυναμούν με την χρονική διάρκεια που απαιτείται ώστε να ολοκληρωθούν μερικές επιβεβαιώσεις, οπότε μπορούμε να αναφερόμαστε στους χρόνους αυτούς και με τον όρο χρόνος επιβεβαίωσης συναλλαγών(*transaction confirmation time*) που αναφέραμε στην Ενότητα 2.1.

2.7.1.2. Απόλυτη οριστικότητα (absolute finality)

Η απόλυτη οριστικότητα παρατηρείται κυρίως στα BA πρωτόκολλα τα οποία λειτουργούν στηριζόμενα σε ένα μοντέλο ψηφοφορίας, όπως έχουμε περιγράψει αναλυτικά στην Ενότητα 2.6. Στα πρωτόκολλα αυτά μία συναλλαγή τερματίζεται σχεδόν άμεσα. Συγκεκριμένα όταν μία συναλλαγή δημιουργηθεί προωθείται από τον υπεύθυνο ηγετικό κόμβο σε μία διαδικασία ψηφοφορίας, κατά την οποία μία επαρκής και όχι κακόβουλη ομάδα κόμβων εγκρίνει και τοποθετεί την συναλλαγή στο ευρύτερο μπλοκ με αποτέλεσμα η συναλλαγή να θεωρείται την ίδια στιγμή οριστική όντας απαλλαγμένη από χρονικές αναμονές και καθυστερήσεις.
Στον παρακάτω Πίνακα 1 έχουμε παραθέσει την οριστικότητα κάποιων βασικών blockchain συστημάτων. Ο χρόνος επιβεβαίωσης, που ισοδυναμεί με την χρονική καθυστέρηση(*latency*) που είναι απαραίτητη ώστε μία συναλλαγή να θεωρηθεί κατά το μέγιστο οριστική, προκύπτει από το γινόμενο του χρόνου δημιουργίας του επόμενου μπλοκ(*block time*) επί τις συνεχόμενες επιβεβαιώσεις(*confirmations*) που ένας χρήστης προτείνεται να περιμένει για να σιγουρέψει κατά ένα μεγάλο ποσοστό την ολοκλήρωση της συναλλαγής του.

Latency = block time x confirmations

Εξίσωση 1-Υπολογισμός των χρονικών καθυστερήσεων στα blockchain συστήματα

Παρατηρούμε ότι τα proof-based συστήματα, με εξαίρεση το EOS.IO με το DPoS, χαρακτηρίζονται από ποικίλες αλλά σημαντικές χρονικές καθυστερήσεις, σε αντίθεση με τα BA συστήματα που ολοκληρώνουν τις συναλλαγές σε μικρά έως ελάχιστα χρονικά διαστήματα.
Ακόμα να αναφέρουμε πως τα αριθμητικά δεδομένα του Πίνακα 1 δεν είναι απόλυτα, καθώς οι χρόνοι πραγματοποίησης των συναλλαγών στα διάφορα blockchain συστήματα δεν είναι σταθεροί αλλά μεταβάλλονται με το χρόνο καθώς επηρεάζονται από διάφορους παράγοντες, όπως για παράδειγμα την κατάσταση του δικτύου κάθε φορά, τον όγκο των συναλλαγών και τις αυξανόμενες απαιτήσεις για επεκτασιμότητα. Τα δεδομένα που παραθέτουμε στον Πίνακα 1 αντλήθηκαν σε ένα εύρος χρόνου από τα μέσα του 2018 μέχρι και τις αρχές του 2019 με τη βοήθεια των online πλατφορμών

του κάθε συστήματος και κάποιων αξιόπιστων συναλλακτικών πλατφορμών (Kraken, Coinbase).

Πίνακας 1-Οριστικότητα των blockchain συστημάτων

Blockchain Σύστημα	Μηχανισμός Ομοφωνίας	Χρόνος επόμενου μπλοκ	Απαραίτητες επιβεβαιώσεις	Χρόνος επιβεβαίωσης
Bitcoin	PoW(SHA-256 hashing algorithm)	10 λεπτά	6	60 λεπτά
Litecoin	PoW(Scrypt hashing algorithm)	2.5 λεπτά	6-12	15-30 λεπτά
Monero	PoW(CryptoNight)	2 λεπτά	10-15	20-30 λεπτά
Ethereum	PoW(Ethash)	12 δευτ.	10-30	2-6 λεπτά
Cardano	PoS(Ouroboros)	40 δευτ	15	10 λεπτά
Nextcoin	PoS(Nxt PoS)	80 δευτ	10	13 λεπτά
EOS.IO	DPoS	3 δευτ	1	Σχεδόν άμεσα
NEM	PoI(SHA3-512)	1 λεπτό	-	1-2 λεπτά
Hyperledger Fabric	PBFT	<1 δευτ	1	<1 δευτ
NEO	DBFT	15-20 δευτ	1	15-20 δευτ
Ripple	Probabilistic Byzantine Voting(RPCA)	4 δευτ	1	4 δευτ
Stellar	Federated Byzantine Aggreement(SCP)	2-5 δευτ	1	2-5 δευτ

2.7.2.Διαδικασία έκδοσης επόμενου μπλοκ

Στα PoW συστήματα η δημιουργία ενός μπλοκ είναι αποτέλεσμα της εξόρυξης μέσω της υπολογιστικής δύναμης και της κατακερματιστικής ισχύος που διαθέτουν οι κόμβοι. Στο PoS οι κόμβοι συμμετέχουν στην έκδοση νέων μπλοκ αναλογικά με το coin age του stake που διαθέτουν, ενώ στο DPoS η ισχύς του stake σε συνδυασμό με ένα πρωτόκολλο ψηφοφορίας καθορίζουν τον κόμβο που θα προτείνει το επόμενο μπλοκ. Η συμμετοχή στο PoET προδιαθέτει την χρήση ειδικευμένου hardware καθώς οι χρήστες λειτουργούν σε ένα έμπιστο περιβάλλον εκτέλεσης(TEE). Τα BA πρωτόκολλα καθορίζουν τον υπεύθυνο κόμβο για το επόμενο μπλοκ στηριζόμενα σε πρωτόκολλα ψηφοφορίας πολλαπλών γύρων(PBFT), σε πρωτόκολλα ομοσπονδιακής ψηφοφορίας(SCP) ή σε πρωτόκολλα πιθανολογικής ψηφοφορίας(RPCA).

2.7.3.Προσδιορισμός της συναίνεσης

Ένα σύστημα συναίνεσης πρέπει να παρέχει στους χρήστες του έναν τρόπο ώστε να μπορούν να γνωρίζουν την κατάσταση του συστήματος ώστε να συμμετέχουν σε αυτό. Στα blockchain συστήματα οι κόμβοι πρέπει να προμηθεύονται από το ίδιο το σύστημα με κάποια αντικειμενικά κριτήρια για να μπορούν να έχουν μια εικόνα της σωστής λειτουργίας του συστήματος στηριζόμενοι σε πληροφορίες που παίρνουν από τους υπόλοιπους ενεργούς κόμβους του δικτύου. Ωστόσο οι πληροφορίες που διακινούνται μεταξύ των κόμβων μέσα στο ίδιο το σύστημα δεν είναι απαραίτητα αυθεντικές καθώς πάντα υπάρχει για παράδειγμα ο κίνδυνος μία οργανωμένη κακόβουλη μερίδα των κόμβων να επιχειρήσει μία *Sybil attack*, όπως θα εξηγήσουμε παρακάτω[99].
Συνεπώς με βάση τα κριτήρια και την εικόνα που έχει ένας νέος χρήστης σε κάποιο σύστημα η συναίνεση διαχωρίζεται στις παρακάτω μορφές[100]:

1. **Αντικειμενική(*objective*)** : ένας νέος χρήστης που εισέρχεται στο δίκτυο γνωρίζοντας αποκλειστικά τον ορισμό του πρωτοκόλλου και το σύνολο όλων των μπλοκ και άλλων σημαντικών μηνυμάτων που έχουν δημοσιευτεί μπορεί ανεξάρτητα να καταλήξει στο ίδιο συμπέρασμα με το υπόλοιπο το δίκτυο για την τρέχουσα κατάσταση.

2. **Υποκειμενική(*subjective*)** : το σύστημα έχει σταθερές καταστάσεις όπου διαφορετικοί χρήστες καταλήγουν σε διαφορετικά συμπεράσματα και απαιτείται μεγάλη ποσότητα κοινωνικών πληροφοριών (π.χ. φήμη) για να συμμετάσχουν.

3. **Ασθενώς υποκειμενική(*weakly subjective*)** : ένας νέος χρήστης που εισέρχεται στο δίκτυο γνωρίζοντας αποκλειστικά τον ορισμό του πρωτοκόλλου, το σύνολο όλων των μπλοκ και άλλων σημαντικών μηνυμάτων που έχουν δημοσιευτεί και μία κατάσταση με λιγότερα από κάποια μπλοκ τα οποία είναι γνωστό ότι είναι έγκυρα μπορεί ανεξάρτητα να καταλήξει στο ίδιο συμπέρασμα με το υπόλοιπο δίκτυο στην τρέχουσα κατάσταση, εκτός εάν υπάρχει κάποιος κακόβουλος κόμβος που κατέχει μόνιμα ένα σημαντικό ποσοστό ελέγχου πάνω από το σύνολο συναίνεσης.

Με βάση τα παραπάνω χαρακτηρίζουμε το PoW ως απόλυτα αντικειμενικό καθώς η ομοφωνία ακολουθεί τον κοινώς αποδεκτό προς όλους και απαραβίαστο κανόνα της μακρύτερης αλυσίδας, ενώ αντικειμενικό θεωρούμε και το PoET που ακολουθεί σχεδόν την ίδια λογική. Αντίθετα το κλασσικό PoS παρουσιάζει μικρό βαθμό αντικειμενικότητας στην διαδικασία ομοφωνίας. Αυτό συμβαίνει καθώς ένας κακόβουλος χρήστης με ικανό stake μπορεί να διατηρεί το δικό του fork πιο εύκολα απ' ότι στο PoW με αποτέλεσμα ένας νέος κόμβος στο σύστημα να αδυνατεί να διασφαλίσει απευθείας με την είσοδό του πως έχει επιλέξει τη σωστή εκδοχή του blockchain. Στο DPoS με τον διαχωρισμό των stakeholders από τους delegates και το ρόλο αυτών παρατηρούμε μία ασθενώς υποκειμενική ομοφωνία. Όσον αφορά το σύνολο των BA συστημάτων η ομοφωνία σε αυτά είναι καθαρά υποκειμενική καθώς προκύπτει εξ' ολοκλήρου από το βαθμό εμπιστοσύνης μεταξύ των κόμβων.

2.7.4.Βαθμός ευελιξίας εμπιστοσύνης

Με τον όρο ευελιξία στην εμπιστοσύνη αναφερόμαστε στο βαθμό ελευθερίας που έχει ο κάθε κόμβος σε ένα blockchain σύστημα για να επιλέξει τους υπόλοιπους κόμβους που εμπιστεύεται[93]. Όπως έχουμε αναφέρει και παραπάνω η εμπιστοσύνη στα ΒΑ συστήματα είναι ζωτικής σημασίας για τη λειτουργία τους. Άλλωστε ολόκληρη η δομή τους στηρίζεται στις σχέσεις αλληλεπίδρασης μεταξύ των κόμβων και στην εμπιστοσύνη που απαιτείται, όχι πάντα στον ίδιο βαθμό, ώστε να επέλθει ομοφωνία. Εμπιστοσύνη μεταξύ των κόμβων χρειάζεται και στα DPoS συστήματα όπου οι stakeholders ψηφίζουν τους delegates που θα τους εκπροσωπήσουν στο δίκτυο. Έτσι μπορούμε να πούμε πως οι παραπάνω μηχανισμοί συναίνεσης χαρακτηρίζονται από μεγάλο βαθμό ευελιξίας όσον αφορά την εμπιστοσύνη, καθώς ένας χρήστης μπορεί να επιλέξει ελεύθερα και ανεξάρτητα ποιόν θα εμπιστευτεί. Στους υπόλοιπους μηχανισμούς συναίνεσης δεν παρατηρείται ευελιξία στην εμπιστοσύνη μιας και οι μηχανισμοί αυτοί φτάνουν στην ομοφωνία είτε χωρίς να απαιτείται εμπιστοσύνη είτε με τέτοιο τρόπο ώστε η εμπιστοσύνη να είναι καθορισμένη. Συγκεκριμένα στο PoW η ομοφωνία επιτυγχάνεται κατά μήκος όλου του δικτύου μέσω της έμμεσης συνεργασίας και των επιλογών των κόμβων χωρίς να απαιτείται να γνωρίζουν ο ένας την ταυτότητα του άλλου και να επιχειρούν σχέσεις εμπιστοσύνης. Στο PoS η εμπιστοσύνη που υπάρχει στο δίκτυο είναι αναλογική με το stake του κάθε κόμβου, ενώ στο DPoS η εμπιστοσύνη περιορίζεται σε ένα μόνο μέρος του συνολικού δικτύου. Στο PoET δεν παρατηρούμε ιδιαίτερο βαθμό εμπιστοσύνης παρά μόνο την στοιχειώδη εμπιστοσύνη των κόμβων στο hardware που απαιτείται.

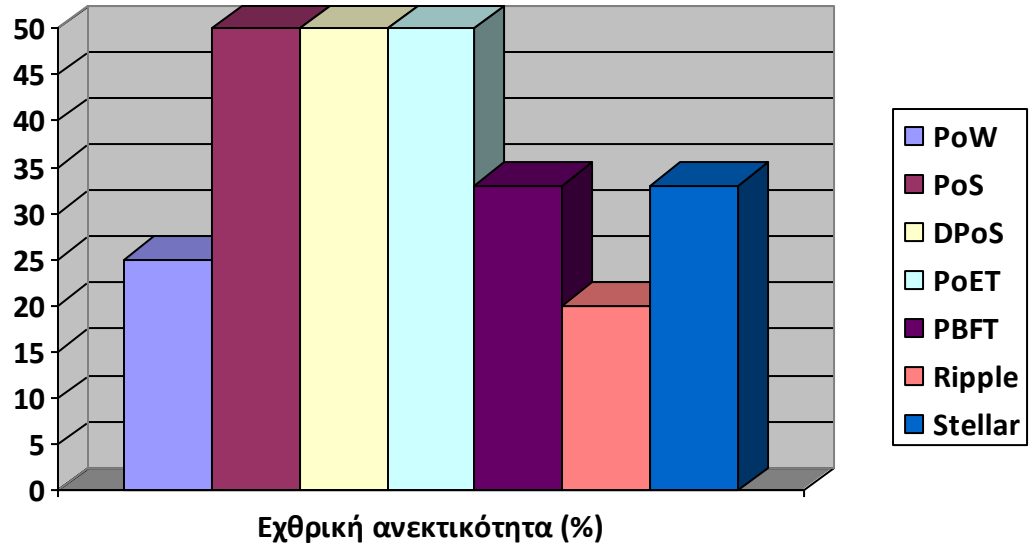
2.7.5.Ανοχή έναντι κακόβουλης συμπεριφοράς

Όπως γνωρίζουμε στα blockchain συστήματα υπάρχει πάντα η πιθανότητα ένας μεμονωμένος χρήστης ή συνηθέστερα μία ομάδα χρηστών να επιχειρήσουν κάποια μορφή επίθεσης έναντι στο σύστημα με σκοπό να προκαλέσουν σύγχυση και δυσλειτουργία σε αυτό ή στην ακραία περίπτωση να μπορέσουν να ελέγξουν ολόκληρο το δίκτυο. Μιας και αρκετά από τα συστήματα είναι αποκεντρωμένα και στηρίζονται στην αρχή της ισότητας των κόμβων που συμμετέχουν σε αυτά, μία κακόβουλη ενέργεια απειλεί την ίδια τη σύσταση του πυρήνα της blockchain λογικής. Συνεπώς κάθε μηχανισμός συναίνεσης πρέπει να παρέχει ασφάλεια και ανοχή στις κακόβουλες ενέργειες. Στο PoW η δράση των κόμβων συνάδει με την υπολογιστική ισχύ που είναι διατεθειμένοι να ξοδέψουν για να προσθέσουν το επόμενο μπλοκ. Καθώς τα ενεργειακά ποσά που σπαταλούνται είναι τεράστια η ίδια η φύση του PoW αποθαρρύνει έναν μεμονωμένο κόμβο να επιχειρήσει επίθεση λόγω των τεχνολογικών και οικονομικών συνεπειών. Για να κατανοήσει κανείς το οικονομικό κόστος μιας επίθεσης στο δίκτυο αρκεί να λάβει υπ' όψη πως στα μέσα του 2018 το συνολικό δίκτυο του Bitcoin κατανάλωσε περίπου ίση ενέργεια με την Ρουμανία και το Ουζμπεκιστάν[101], ενώ το Ethereum με την Αιθιοπία και την Κόστα Ρίκα[102]. Βέβαια με την συνεχώς αυξανόμενη δράση των mining pools το υπέρογκο κόστος μιας επίθεσης διαμοιράζεται στα μέλη αυτής. Έτσι αν και τα PoW συστήματα θεωρούνται ευρέως πως λειτουργούν σωστά αν ένας κόμβος κατέχει λιγότερο από το 51% της συνολικής ισχύος, η δράση των mining pools περιορίζει την ανοχή αυτή στο

25%[103]. Δύο προσεγγίσεις κατά της επιζήμιας δράσης των mining pools παρουσίασαν οι A. Miller κά[104] μέσω της δομής των *"nonoutsourceable" puzzles* και οι L. Luu κά[105] μέσω του *SmartPool* πρωτοκόλλου για τη εισαγωγή της αποκέντρωσης στα mining pools. Τα PoS συστήματα λειτουργούν κανονικά υπό την προυπόθεση ότι κανένας κόμβος δεν διαθέτει τέτοιο stake που να ξεπερνά το 50% του αρχικού συνολικού stake, ενώ το DPoS είναι παρόμοια ευάλωτο σε 51% επιθέσεις, καθώς μόνο μερικοί και όχι όλοι οι κόμβοι του δικτύου είναι υπεύθυνοι για την διατήρηση της ομαλής λειτουργίας του. Ο PoET μηχανισμός είναι ευάλωτος υπό την έννοια ότι κάποιος μπορεί θεωρητικά να απειλήσει το σύστημα αν καταφέρει να πάρει με το μέρος του ένα Θ[log(logn)/logn] κλάσμα των n συνολικών κόμβων, το οποίο είναι ένα μεταβλητό μέγεθος σε αντίθεση με τους προηγούμενους μηχανισμούς. Βέβαια καθώς στο PoET οι κόμβοι επενδύουν σε TEE hardwares ενδέχεται ένας κόμβος που μπορεί να διαθέσει μεγάλα ποσά στο hardware να μπορέσει να εξαπατήσει το σύστημα και να το απειλήσει με μία επίθεση της μορφής 50%[106].

Στα BFT συστήματα, όπου οι κόμβοι είναι γνωστοί αναμεταξύ τους και χρειάζεται να εμπιστεύονται ο ένας τον άλλον, η διαδικασία ομοφωνίας μπορεί να θεωρηθεί ασφαλής αν και μόνο αν το σύνολο των κακόβουλων κόμβων δεν ξεπερνά τα 2/3 του συνολικού αριθμού των κόμβων του δικτύου. Ωστόσο το δίκτυο του Ripple λειτουργεί κανονικά εφόσον το 80% των κόμβων είναι μη κακόβουλοι. Στην περίπτωση που το ποσοστό των κακόβουλων χρηστών κινείται μεταξύ 20-80% η ομοφωνία στο δίκτυο διακυβεύεται, με αποτέλεσμα το δίκτυο να μπορεί να αντέξει μέχρι 20% εχθρικών κόμβων[93]. Βέβαια σύμφωνα με μεταγενέστερη ανεξάρτητη ανάλυση[107] το ποσοστό αυτό μπορεί να φτάσει το 40%, ενώ σε μία ακόμα πιο πρόσφατη μελέτη[108] οι B.Chase και E.MacBrough έδειξαν πως κάτω από ένα γενικότερο πρότυπο σφάλματος, το οποίο χρησιμοποιείται κανονικά στην ερευνητική βιβλιογραφία, το ποσοστό αυτό ανέρχεται στο 90% στις UNL.

Διάγραμμα 2-Ποσοστιαία ανεκτικότητα των blockchain μηχανισμών έναντι κακόβουλων χρηστών



2.7.6.Επεκτασιμότητα

Η επεκτασιμότητα αποτελεί ένα από τα κυριότερα ζητήματα στον τομέα της τεχνολογίας blockchain, καθώς η αντιμετώπιση-επίλυση των ζητημάτων που την αφορούν απασχολεί την επιστημονική (και μη) κοινότητα εδώ και πολύ καιρό. Η συνεχώς αυξανόμενη πίεση που δέχονται τα δημοφιλέστερα blockchain συστήματα (πχ Bitcoin,Ethereum) λόγω της περιορισμένης επεκτασιμότητας που διαθέτουν σε συνδυασμό με τον συνεχώς αυξανόμενο αριθμό χρηστών τους καθιστά την επεκτασιμότητα ένα μείζον ζήτημα.
Η επεκτασιμότητα είναι ένας όρος που κατά καιρούς έχει ερμηνευθεί και προσδιοριστεί με τη βοήθεια διάφορων εννοιών[109][110][79]: αριθμός συμμετεχόντων κόμβων(*nodes*), απόδοση του συστήματος (*performance*), χρονικές καθυστερήσεις κατά την επιβεβαίωση(*latency*), χρόνος επιβεβαίωσης συναλλαγής(*transaction confirmation time*), συναλλαγές ανά δευτερόλεπτο(*transactions per second*), μέγεθος-χωρητικότητα και συχνότητα παραγωγής μπλοκ(*block time*), ταχύτητα επεξεργασίας εκτέλεσης και διακίνηση(*throughput*).
Σε μία ενδιαφέρουσα προσέγγιση ο Vitalik Buterin αναφέρθηκε στην έννοια της επεκτασιμότητας μέσω του όρου "*Scalability Trilemma*"[111]. Ο όρος αυτός θίγει το πρόβλημα του τρόπου ανάπτυξης μιας τεχνολογίας blockchain που προσφέρει δυνατότητα επεκτασιμότητας, αποκέντρωσης και ασφάλειας, χωρίς να διακυβεύει τίποτα από τα παραπάνω.
Με βάση τα παραπάνω καταλήγουμε πως η επεκτασιμότητα είναι στην ουσία μία πολυσύνθετη έννοια. Συνεπώς για την ανάλυση και κατανόησή της οφείλουμε να αναφερθούμε σε όλες τις απαραίτητες έννοιες-χαρακτηριστικά της τεχνολογίας blockchain ώστε να παρέχουμε μία πλήρη εικόνα επί του θέματος. Έχοντας αναλύσει κάποιες έννοιες που σχετίζονται με την επεκτασιμότητα σε προηγούμενες ενότητες(ταχύτητα συναλλαγών, χρονικές καθυστερήσεις κά), στην ενότητα αυτή θα αναφερθούμε στην επεκτασιμότητα των υπό σύγκριση μηχανισμών συναίνεσης επικεντρώνοντας σε δύο σημαντικές ποσοτικές παραμέτρους: στην ικανότητα του συστήματος να καταλήξει σε ομοφωνία παράλληλα με το αυξανόμενο πλήθος των χρηστών που συμμετέχουν και στη διακίνηση των συναλλαγών παραθέτοντας τις συναλλαγές ανά δευτερόλεπτο που μπορεί να προσφέρει το κάθε δίκτυο. Παρακάτω, στον Πίνακα 2, παρουσιάζουμε μία ποσοτική σύγκριση μεταξύ των μηχανισμών συναίνεσης, ενώ στο επόμενο κεφάλαιο θα ασχοληθούμε εκτενώς με την ανάλυση διάφορων προσεγγίσεων που μπορούν να συμβάλλουν στην αντιμετώπιση του προβλήματος της επεκτασιμότητας.
Στα δημοφιλέστερα PoW και PoS συστήματα δεν υπάρχει περιορισμός στον αριθμό των κόμβων που μπορούν να συμμετέχουν πραγματοποιώντας συναλλαγές. Αυτό σημαίνει ότι το σύστημα θα καταλήξει τελικά στην πολυπόθητη ομοφωνία, αν και η διακίνηση των συναλλαγών κινείται σε μικρά επίπεδα λόγω της ίδιας της δομής των αλγορίθμων συναίνεσης. Στις DPoS και PoI παραλλαγές του PoS ενώ δεν υπάρχει αντίστοιχα περιορισμός στο πλήθος των χρηστών η διαφοροποίησή τους από το κλασσικό PoS επιτρέπει πολύ περισσότερες συναλλαγές, αυξάνοντας τη διακίνηση και ουσιαστικά την απόδοση των συστημάτων στα οποία χρησιμοποιούνται. Για το PoET αν και δεν έχουμε ενδεικτικά στοιχεία για τη διακίνηση, θεωρείται ότι παρέχει μεγάλη επεκτασιμότητα ως προς το πλήθος των συμμετεχόντων χρηστών[53]. Όσον αφορά το σύνολο των BA συστημάτων η διακίνηση κινείται μεταξύ 1000-3500 συναλλαγών ανά δευτερόλεπτο και συχνά αναφέρεται η προοπτική των μερικών

δεκάδων χιλιάδων. Ωστόσο οι συναλλαγές αυτές επιτυγχάνονται συνήθως με περιορισμένο και πολύ μικρότερο πλήθος κόμβων. Συγκεκριμένα στο PBFT η λειτουργία και η συναίνεση στηρίζεται στο πλήθος των μηνυμάτων που ανταλλάσσονται μεταξύ των κόμβων δημιουργώντας ένα περιβάλλον εμπιστοσύνης που στηρίζεται σε πολλαπλούς γύρους ψηφοφορίας. Έτσι η αύξηση των κόμβων ακόμα και σε εκατοντάδες συνεπάγεται μεγαλύτερη πολυπλοκότητα στο επίπεδο της επικοινωνίας, πλήττοντας έτσι την απόδοση του συστήματος, με αποτέλεσμα ένα PBFT δίκτυο να λειτουργεί αποδοτικά με 30-64 κόμβους[93][96]. Τα ίδια ισχύουν και για το δίκτυο του Ripple και του Stellar των οποίων οι ενεργοί κόμβοι δεν ξεπερνούν τους 200[4][5] .

Πίνακας 2-Επεκτασιμότητα και διακίνηση στα κυριότερα blockchain συστήματα

Blockchain σύστημα	Μηχανισμός συναίνεσης	Διακίνηση (Συναλλαγές ανά δευτερόλεπτο)	Επεκτασιμότητα ως προς το πλήθος χρηστών
Bitcoin	PoW	3-7	Υψηλή
Litecoin	PoW	56	-//-
Monero	PoW	4	-//-
Ethereum	PoW	15-20	-//-
Cardano	PoS	5-7	-//-
EOS.IO	DPoS	50[112] (μέγιστο 3996)	-//-
NEM	PoI	Μέγιστο 3085	-//-
NEO	DBFT	1000	Χαμηλή
Hyperledger Fabric	PBFT	2000-3500	Ελάχιστη (μέχρι 64)
Ripple	RPCA	1500	Περιορισμένη (<200)
Stellar	SCP	1000	Περιορισμένη (<200)

2.7.7.Δημόσια-Ιδιωτικά blockchain συστήματα

Όπως θα αναλύσουμε εκτενέστερα σε επόμενο κεφάλαιο τα blockchain συστήματα διακρίνονται σε τρείς μεγάλες κατηγορίες: τα δημόσια, τα ιδιωτικά και τα κοινοπρακτικά blockchain συστήματα. Ο διαχωρισμός αυτός γίνεται με βάση την άδεια που έχουν οι συμμετέχοντες για[113]:

[4] https://xrpcharts.ripple.com/#/topology
[5] https://stellarbeat.io/

- απλή πρόσβαση(ανάγνωση) στα δεδομένα του συστήματος(*read permission*)

- συμμετοχή στην διεκπεραίωση συναλλαγών(*write permission*)

- συμμετοχή στη δημιουργία νέων μπλοκ συναλλαγών, στην διατήρηση και αναβάθμιση του συστήματος(*commit permission*)

Ο J. Garzik σε συνεργασία με το BitFury Group κατηγοριοποίησαν με βάση τα παραπάνω κριτήρια το σύνολο των blockchain συστημάτων στις παρακάτω κατηγορίες[114][115]:

- **Δημόσια**: τα συστήματα στα οποία η απλή πρόσβαση στα δεδομένα του συστήματος δεν έχει περιορισμούς. Τα δημόσια συστήματα διαχωρίζονται σε εκείνα όπου δεν υπάρχουν περιορισμοί ούτε στη δημιουργία συναλλαγών ούτε στη δημιουργία μπλοκ(***public permissionless***) και σε εκείνα που η ολοκλήρωση των συναλλαγών περιορίζεται μόνο σε εξουσιοδοτημένους από το σύστημα χρήστες(***public permissioned***).

- **Ιδιωτικά(*private permissioned*)**: τα συστήματα στα οποία η απλή πρόσβαση στα δεδομένα είναι μερικώς ή πλήρως περιορισμένη, ενώ η συμμετοχή και ολοκλήρωση των συναλλαγών είναι αποκλειστική ευθύνη μίας μορφής κεντρικής εξουσίας που ελέγχει και καθορίζει το δίκτυο.

- **Κοινοπρακτικά(*consortium*)**: τα συστήματα που αποτελούν μία ενδιάμεση μορφή των δύο παραπάνω κατηγοριών, μιας και η συμμετοχή σε αυτά είναι περιορισμένη σε μία ομάδα εξουσιοδοτημένων χρηστών.

Με βάση τους παραπάνω ορισμούς μπορούμε να χαρακτηρίζουμε τα PoW συστήματα ως δημόσια, λόγω της έλλειψης κάθε μορφής ελέγχου στη συμμετοχή ενός χρήστη σε αυτά, ενώ το PoS με τις παραλλαγές τους και το PoET μπορούν να εφαρμοστούν τόσο στα δημόσια όσο και στα ιδιωτικά δίκτυα. Όσον αφορά το PBFT είναι ιδανικό για εφαρμογή σε ιδιωτικές πλατφόρμες, λόγω της περιορισμένης προσβασιμότητας και των υψηλών δεικτών απόδοσης που παρέχει. Τα δίκτυο του Ripple και του Stellar ανήκουν στην κατηγορία των δημόσιων blockchain, αλλά σε διαφορετική υποκατηγορία το καθένα. Συγκεκριμένα στο δίκτυο του Stellar δεν υπάρχει κανένας περιορισμός στη δράση ενός κόμβου(*public permissionless*), σε αντίθεση με το δίκτυο του Ripple όπου η απλή συμμετοχή είναι ανοιχτή αλλά η συμμετοχή στην ολοκλήρωση των συναλλαγών είναι περιορισμένη(*public permissioned*).

2.7.8.Ασφάλεια έναντι διάφορων μορφών κακόβουλων επιθέσεων

Η ασφάλεια σε ένα blockchain σύστημα είναι αν όχι το κυριότερο ένα από τα κυριότερα και πρωταρχικά ζητήματα. Κάθε blockchain σύστημα επιλέγει τον μηχανισμό συναίνεσης και το περιβάλλον λειτουργίας του με κύριο σκοπό την ασφάλεια, την αποκέντρωση και την αποτελεσματικότητα[116]. Ακόμα και αν ένα blockchain σύστημα παρέχει τα επιθυμητά επίπεδα αποκέντρωσης και υψηλή διακίνηση και επεκτασιμότητα, οφείλει να εξασφαλίζει στους χρήστες που θα το χρησιμοποιήσουν και που θα επενδύσουν σε αυτό ένα ασφαλές περιβάλλον. Ωστόσο λόγω της δημοσιότητας που έχει κερδίσει η blockchain τεχνολογία, οι κακόβουλες ενέργειες έναντι αυτής γίνονται όλο και πιο ισχυρές, με τους εχθρικούς χρήστες να οργανώνονται ακόμα και σε πολυάριθμες ομάδες με σκοπό να καταφέρουν να ελέγξουν και να αντιστρέψουν προς όφελός τους τα blockchain δίκτυα. Οι επιθέσεις που έχουν παρατηρηθεί εις βάρος των δημοφιλέστερων, πχ Bitcoin, πλατφορμών ποικίλουν και ανθίζουν, καθιστώντας την ανάγκη για ασφάλεια το μείζον μέλημα κάθε blockchain συστήματος. Συνεπώς η κατανόηση και η αξιολόγηση των επιθέσεων αυτών είναι απαραίτητες προϋποθέσεις για την αποδεκτικότητα και την χρησιμοποίηση της blockchain τεχνολογίας από τους πιθανούς ενδιαφερόμενους χρήστες[117].
Παρακάτω θα παραθέσουμε τις κυριότερες μορφές εχθρικών επιθέσεων που παρατηρούνται στα διάφορα blockchain συστήματα ανάλογα με τον μηχανισμό συναίνεσης που χρησιμοποιείται, ώστε να μπορέσουμε να αξιολογήσουμε κατά πόσο ένα τέτοιο σύστημα μπορεί να θεωρηθεί ασφαλές.

2.7.8.1. Sybil attack

Η sybil attack, η οποία συζητήθηκε για πρώτη φορά από τον J.R. Douceur[118], είναι μία στοχευμένη και οργανωμένη επιθετική ενέργεια κατά την οποία κάποιος μπορεί να απειλήσει και να διαφθείρει ένα P2P δίκτυο δημιουργώντας πολλαπλές ψεύτικες ταυτότητες. Σε κάθε P2P δίκτυο ο κάθε κόμβος ισοδυναμεί με μία και μοναδική ψηφιακή ταυτότητα. Συνεπώς αν κάποιος καταφέρει να δημιουργήσει πολλαπλές ταυτότητες μπορεί να ασκήσει μεγάλη επιρροή κατέχοντας μεγαλύτερη εξουσία στο δίκτυο από αυτή που του αναλογεί, αντιστρέφοντας έγκυρες και προωθώντας άκυρες συναλλαγές, αλλά και πυροδοτώντας άλλες μορφές επιθέσεων, όπως για παράδειγμα οι *double-spending* και οι *distributed denial-of-service attacks* που θα εξηγήσουμε παρακάτω. Πρόκειται για μία μορφή επίθεσης που υφίσταται λόγω της P2P δομής των blockchain δικτύων και είναι δυνατή σε κάθε blockchain σύστημα ανεξαρτήτως μηχανισμού συναίνεσης. Η προστασία έναντι στις sybil attacks παρέχεται ως ένα μεγάλο βαθμό από τον ίδιο τον μηχανισμό συναίνεσης που υιοθετεί το κάθε σύστημα. Για παράδειγμα στο PoW η εφαρμογή μίας τέτοιας επίθεσης καθίσταται υπερβολικά ακριβή λόγω της ενεργειακής και τεχνολογικής συνεισφοράς στων κόμβων στη διαδικασία εξόρυξης. Όσο κι αν γίνονται αξιόλογες έρευνες και προσπάθειες για την καταπολέμηση των sybil attacks[119], αυτή η μορφή επιθέσεων παραμένει πάντα πιθανή στα blockchain συστήματα.

2.7.8.2. 51% attack

Αυτή η μορφή επίθεσης, γνωστή και ως *majority attack*[116], είναι ίσως η δημοφιλέστερη επίθεση στα blockchain συστήματα και οφείλεται στον ίδιο το μηχανισμό συναίνεσης του εκάστοτε συστήματος[120] και στην P2P δομή του[121]. Μία 51% επίθεση[122] πραγματοποιείται είτε από έναν κόμβο είτε από μία οργανωμένη ομάδα κόμβων(πχ mining pool) και θεωρείται επιτυχής εάν κάποιος καταφέρει να ελέγξει το 51% της ισχύος του συνολικού δικτύου, η οποία μπορεί να είναι η κατακερματιστική ισχύς σε ένα PoW σύστημα ή η αξία των περιουσιακών στοιχείων σε ένα PoS σύστημα. Σε μία επιτυχημένη επίθεση αυτής της μορφής, η οποία είναι εξαιρετικά δύσκολο να εντοπιστεί μέχρι να ολοκληρωθεί[123], οι εχθρικοί κόμβοι δημιουργούν κρυφά τη δική τους αλυσίδα από μπλοκ, την οποία κάποια στιγμή δημοσιοποιούν στο δίκτυο με σκοπό να προσελκύσουν τους υπόλοιπους κόμβους ώστε να ακολουθήσουν την δική τους αλυσίδα. Ως αποτέλεσμα αυτού η κακόβουλη αλυσίδα θα γίνει η μεγαλύτερη στο δίκτυο δίνοντας στους εχθρικούς κόμβους που τη δημιούργησαν τον έλεγχο του συστήματος. Συνεπώς οι επιθέσεις αυτής της μορφής διασπούν τη σταθερότητα ενός blockchain συστήματος επιτρέποντας στους κόμβους που τις επιδιώκουν να[121][124]:

- αντιστρέφουν συναλλαγές διαταράσσοντας την θεμελιώδη ιδιότητα της αμεταβλητότητας της blockchain τεχνολογίας
- επιχειρούν νέες επιθέσεις, όπως η *double-spending*
- μετατρέπουν πολλά μπλοκ σε μη έγκυρα εμποδίζοντας την επικύρωση των συναλλαγών που αυτά περιέχουν από τους υπόλοιπους κόμβους
- δημιουργούν forks στο σύστημα διαχωρίζοντάς το
- προωθούν και εγκρίνουν ψεύτικες συναλλαγές
- κλέβουν κρυπτονομίσματα και γενικότερα περιουσιακά στοιχεία από άλλους κόμβους

Στα proof-based συστήματα μία 51% επίθεση είναι πολύ δύσκολη να πραγματοποιηθεί, λόγω της δυσκολίας που απαιτείται από τους εχθρικούς κόμβους να καταλάβουν το 51% του συνολικού δικτύου. Το δημοφιλέστερο PoW δίκτυο του Bitcoin δεν έχει δεχθεί ποτέ από την δημιουργία του τέτοια επίθεση, σε αντίθεση με άλλα μικρότερα κρυπτονομίσματα με χαμηλά ποσοστά κατακερματισμού που κατά καιρούς βίωσαν την επίθεση αυτή[125][126][127], που σημαίνει ότι όσο μεγαλύτερο και ισχυρότερο είναι ένα δίκτυο τόσο δυσκολότερη είναι η επιτυχία μίας τέτοιας επίθεσης. Βέβαια έστω και σε θεωρητικό επίπεδο τα κυριότερα proof-based συστήματα είναι πάντα ευάλωτα στις 51% επιθέσεις.

Οι S.Sayeed και H.Marco-Gisbert[123] παρουσίασαν μία εκτενή μελέτη και ανάλυση των 51% επιθέσεων στα blockchain συστήματα, παραθέτοντας μία σειρά από τεχνικές και μεθόδους που θα μπορούσαν στην πράξη να μετριάσουν τη συχνότητα και τον αντίκτυπο των 51% επιθέσεων στα blockchain συστήματα, ενώ ενδιαφέρουσες προτάσεις και τεχνικές αντιμετώπισης έχουν διατυπωθεί και τα προηγούμενα χρόνια[128][129]. Ωστόσο, όπως αναφέρουμε και παραπάνω, καμία τεχνική μέχρι σήμερα δεν μπορεί να εγγυηθεί την απόλυτη προστασία έναντι τέτοιων επιθέσεων.

Όσον αφορά τα BA συστήματα, τα κυριότερα από αυτά που έχουμε αναλύσει στην Ενότητα 2.6 δεν έχουν απειληθεί ποτέ στην πράξη από 51% επιθέσεις. Θεωρώντας δεδομένο ότι στα συστήματα αυτά η ταυτότητα των ενεργών στην επίτευξη ομοφωνίας κόμβων είναι γνωστή και η λειτουργία τους στηρίζεται σε διάφορες διαδικασίες ψηφοφορίας ή ομάδες κόμβων που λειτουργολυν σε κλίμα εμπιστοσύνης

και όχι σε συναγωνιστικούς μηχανισμούς εξόρυξης, μπορούμε να κρίνουμε τα συστήματα αυτά ως σχετικά ασφαλή ως προς τις 51% επιθέσεις.

2.7.8.3. Distributed denial-of-service attack (DDoS)

Μία DDoS επίθεση είναι μία μορφή διαδικτυακής επίθεσης που όπως φανερώνει και η ονομασία της έχει ως αποτέλεσμα την άρνηση της εξυπηρέτησης των διαδικτυακών πελατών και εφαρμόζεται τόσο σε διαδικτυακό επίπεδο όσο και σε επίπεδο εφαρμογών[120]. Η επίθεση αυτή είναι μία κοινή μορφή κακόβουλης ενέργειας που ήταν γνωστή πολύ πριν εμφανιστεί η blockchain τεχνολογία[130] προκαλώντας πολλά και σοβαρά προβλήματα σε διάφορες διαικτυακές πλατφόρμες και υπηρεσίες. Για την επίτευξη μίας τέτοιας επίθεσης ο κακόβουλος χρήστης επιχειρεί να φθείρει τη λειτουργία ενός διακομιστή-στόχου μέσω του ελέγχου διάφορων υπολογιστικών συστημάτων που συνδέονται με αυτόν(πχ IoT συσκευές, διαδικτυακές πηγές κτλ). Τα συστήματα αυτά διεγείρονται με κακόβουλο λογισμικό και αποτελούν πλέον μία ομάδα υποκεινούμενων μέσων(*botnet*), μέσω των οποίων ο επιτιθέμενος υποβάλει συνεχώς πολλαπλά αιτήματα στον διακομιστή-στόχο προκαλώντας μία μορφή πληροφοριακής υπερχείλισης που οδηγεί σε μη ανταποκρίσιμη συμπεριφορά. Αν και η διανεμημένη και αποκεντρωμένη φύση των περισσότερων blockchain συστημάτων καθιστά θεωρητικά δύσκολη την επιτυχημένη ολοκλήρωση μίας DDoS επίθεσης με αποτέλεσμα η διακίνηση στο blockchain δίκτυο να επηρεάζεται μόνο μέχρι ένα επίπεδο[123], στον blockchain κόσμο τέτοιες επιθέσεις έχουν καταγραφεί στο παρελθόν προκαλώντας μεγάλα προβλήματα, όπως συνέβη στα δύο δημοφιλέστερα κρυπτονομίσματα, το Bitcoin[131][132] και το Ethereum[133][134], ενώ σύμφωνα με μία εμπειρική ανάλυση των M.Vasek κ.ά.[135] οι DDoS επιθέσεις είναι πολύ πιθανές σε νομισματικές συναλλαγές, ηλεκτρονικά πορτοφόλια και mining pools που χαρακτηρίζουν τα blockchain συστήματα. Αναφορικά με τα mining pools, αξίζει να αναφέρουμε ότι έχουν δεχθεί κατά καιρούς αξιοσημείωτες DDoS επιθέσεις[136], ενώ μία άλλη DDoS μορφή επίθεσης παρατηρείται στα *memory pools(mempools)* με σκοπό την αύξηση των τελών εξόρυξης[121]. Αξίζει να αναφέρουμε πως οι DDoS επιθέσεις πολλές φορές οργανώνονται ως επακόλουθο των μορφών επιθέσεων που έχουμε περιγράψει παραπάνω, γεγονός που ενισχύει την συχνότητα εμφάνισής τους.
Στηριζόμενοι στην εχρθρική ανεκτικότητα των blockchain πρωτοκόλλων σε συνδυασμό με την επεκτασιμότητά τους ως προς το πλήθος των χρηστών που συμμετέχουν σε αυτά, μπορούμε να πούμε πως στα δημόσια proof-based συστήματα μία DDoS επίθεση είναι πιο δύσκολα υλοποιήσιμη συγκρητικά με το ιδιωτικά-κοινοπρακτικά και το σύνολο των BA πρωτοκόλλων.
Αν και κατά καιρούς έχουν δημοσιευτεί πολλές προτάσεις για την καταπολέμηση των DDoS επιθέσεων και την προστασία των blockchain συστημάτων[137][138][139], η μάστιγα των επιθέσεων αυτών παραμένει ιδιαίτερα επιζήμια, ενώ στο άρθρο τους οι E.Osterweil κ.ά.[140] επισήμαναν τον κίνδυνο των DDoS επιθέσεων καιδιευκρίνισαν την απουσία κατάλληλων μέτρων προστασίας καλώντας την άμεση ανταπόκριση της ερευνητικής κοινότητας

2.7.8.4. Double-spending attack

Μία double-spending επίθεση[141] είναι η μορφή της επίθεσης κατά την οποία ο κακόβουλος χρήστης επιχειρεί να πραγματοποιήσει περισσότερες από μία συναλλαγές χρησιμοποιώντας το ίδιο περιουσιακό στοιχείο, με κυριότερο παράδειγμα τα κρυπτονομίσματα[142]. Κατά τη διάρκεια μίας double-spending επίθεσης ένας χρήστης προωθεί μία συναλλαγή, έστω τη συναλλαγή μίας ποσότητας κρυπτονομισμάτων. Η συναλλαγή προωθείται στη διεύθυνση του αγοραστή και περιέχεται σε ένα μπλοκ μέχρις ότου ολοκληρωθεί. Ωστόσο ο κακόβουλος χρήστης εκμεταλλεύεται το χρονικό διάστημα που μεσολαβεί μέχρι η συναλλαγή του να θεωρηθεί ολοκληρωμένη, επιχειρώντας να πραγματοποιήσει νέα συναλλαγή με τα ίδια κρυπτονομίσματα, οπότε και έχουμε την double-spending επίθεση. Σύμφωνα με τους S.Sayeed κά η επιτυχία της ολοκλήρωσης μίας double-spending επίθεσης είναι αντιστρόφως ανάλογη του αριθμού των επιβεβαιώσεων των μπλοκ σε ένα PoW σύστημα[123]. Διαφωνούμε με το γεγονός αυτό, καθώς ακόμα και αν οι σύνθετες υπολογιστικές διαδικασίες του PoW μπορούν να περιορίσουν τις double-spending επιθέσεις, οι χρονικές καθυστερήσεις που συνεπάγονται την οριστικότητα των μπλοκ στα περισσότερα proof-based συστήματα αποτελούν πρόσφορο έδαφος για τη διεξαγωγή των επιθέσεων αυτών. Συνεπώς θεωρούμε πως τα BA συστήματα, καθώς και το DPoS(θεωρώντας ως παράδειγμα το EOS), που παρέχουν απόλυτη οριστικότητα ανθεκτικά στις double-spending επιθέσεις, σε αντίθεση με την πιθανολογική οριστικότητα PoW, PoS και PoET πρωτοκόλλων. Ακόμα στο PoS μία double-spending επίθεση είναι πολύ πιο δύσκολο να ολοκληρωθεί απ' ότι στο PoW[48], ωστόσο πάντα υπάρχει ο κίνδυνος, ενώ στο DPoS το αντίστοιχο δίκτυο ελέγχει και ανιχνεύει πιθανές απώλειες μειώνοντας τον double-spending κίνδυνο σε μεγάλο βαθμό[143].
Αξίζει να αναφέρουμε πως μία double-spending επίθεση μπορεί να προκύψει όχι απαραίτητα ως αυτόνομη εχθρική ενέργεια, αλλά και ως επακόλουθο άλλων επιθετικών ενεργειών, όπως οι προαναφερθείσες 51% και Sybil επιθέσεις, αλλά και οι race, finney, vector76, alternative history, BGP highjacking, flood, eclipse επιθέσεις[120][121].

2.7.8.5. Border Gateway Protocol Hijacking(BGP) attack

Μία BGP επίθεση, γνωστή και ως routing attack, σχετίζεται άμεσα με τη χωρική συγκέντρωση των κόμβων στα *Autonomous Systems(ASes)* και στους *Internet Service Providers(ISPs)*, που είναι υπεύθυνα για τη διαδικτυακή ροή και δρομολόγηση της κυκλοφορίας σε ένα blockchain σύστημα[121]. Σε μία επιστημονική έρευνα οι M.Apostolaki κ.ά.[144] κατέδειξαν τη σοβαρότητα των επιθέσεων αυτής της μορφής στη blockchain τεχνολογία μέσω του αρνητικού αντικτύπου τους στο Bitcoin. Ενδεικτικά μία τέτοια επίθεση μπορεί να δώσει στον επιτιθέμενο 51% έλεγχο του δικτύου και προκαλεί επιπλέον χρονική καθυστέρηση στην δημιουργία των μπλοκ κατά 20 λεπτά, δημιουργώντας κατάλληλες συνθήκες για double-spending επιθέσεις στους χρήστες-εμπόρους και προκαλώντας απώλεια της υπολογιστικής ισχύος των χρηστών-miners.

Συμπερασματικά μία BGP επίθεση αποτελεί όχι ένα πρόβλημα της blockchain τεχνολογίας, αλλά ένα γενικότερο πρόβλημα της φύσης του διαδυκτίου[145]. Τα PoW συστήματα, όπως το Bitcoin, είναι ευάλωτα σε τέτοιες επιθέσεις καθώς χρησιμοποιούν τον παγκόσμιο ιστό με αποτέλεσμα η διακίνηση των πληροφοριών να εμπλέκει τους ISPs. Το ίδιο ισχύει για το σύνολο των BA πρωτοκόλλων, καθώς συστήματα όπως τα Hyperledger Fabric, Ripple και Stellar λειτουργούν επίσης στο παγκόσμιο διαδίκτυο. Όσον αφορά τα PoS, DPoS και PoET πρωτόκολλα δεν υπάρχει κάποια αναφορά που να εμπλέκει αυτά και τα συστήματα στα οποία υλοποιούνται με BGP επιθέσεις.

2.7.8.6. Eclipse attack

Οι επιθέσεις αυτές στηρίζονται στην ιδέα ότι ένας κακόβουλος χρήστης ή μία ομάδα από κακόβουλους χρήστες επιδιώκουν να απομονώσουν τον στοχευμένο κόμβο-θύμα από τους γειτονικούς του κόμβους εμποδίζοντας την παράδοση εισερχόμενων και εξερχόμενων συναλλαγών μεταξύ αυτών. Η παραπάνω ενέργεια επιτυγχάνεται από τους κακόβουλους χρήστες μέσω της δέσμευσης των IP διευθύνσεων των κόμβων στο δίκτυο και μπορεί να δημιουργήσει τις κατάλληλες συνθήκες για επιπλέον επιθέσεις, όπως η 51% επίθεση και η double-spending επίθεση που περιφράφουμε παραπάνω. Επομένως, λόγω της φύσης της, μία eclipse επίθεση ευδοκιμεί στα δημόσια δίκτυα(public permissionlees) όπου δεν απαιτείται καμία μορφή ελέγχου ή περιοριστικών μέτρων στις ταυτότητες των χρηστών, με χαρακτηριστικό παράδειγμα τις επιθέσεις στο Bitcoin[146] και στο Ethereum[147]. Επομένως οι επιθέσεις αυτές μπορούν να βλάψουν τα PoW συστήματα, καθώς και το δίκτυο του Stellar. Αντίθετα δεν μπορούν να βλάψουν τα ιδιωτικά δίκτυα, επομένως το PBFT πρωτόκολλο παρέχει προστασία στα συστήματα όπου χρησιμοποιείται, αλλά ούτε το δίκτυο του Ripple το οποίο αν και δημόσιο παρουσιάζει περιορισμούς στη συμμετοχή(όπως αναφέρουμε στην Ενότητα 2.7.7). Τα PoS, DPoS και PoET πρωτόκολλα μιας και μπορούν να εφαρμοστούν τόσο σε δημόσια όσο και σε ιδιωτικά και κοινοπρακτικά συστήματα θεωρούμε πως είναι επίσης ασφαλή απέναντι στις eclipse επιθέσεις.

Πίνακας 3-Διάφορες μορφές κακόβουλων επιθέσεων

	Sybil attack	*51% attack*	*DDoS attack*	*Double-spending attack*	*BGP attack*	*Eclipse attack*
PoW	✓	✓	✓	✓	✓	✓
PoS	✓	✓	✓	✓	×	×
DPoS	✓	✓	✓	×	×	×
PoET	✓	✓	✓		×	×
PBFT	✓	×	✓	×	✓	×
RPCA	✓	×	✓	×	✓	×
SCP	✓	×	✓	×	✓	✓

2.7.8.7. Άλλες επιθέσεις

Πέρα από τις επιθέσεις που έχουμε αναλύσει παραπάνω για τους κυριότερους blockchain μηχανισμούς συναίσεσης, υπάρχει μία πληθώρα από επιθέσεις που οφείλονται στην P2P δομή των blockchain συστημάτων, στους ίδιους τους μηχανισμούς συναίνεσης, στη διαδικτυακή φύση των συστημάτων, στις εφαρμογές όπου συναντάται η blockchain τεχνολογία κτλ. Για παράδειγμα δύο πολύ κλασσικές μορφές επιθέσεων που αφορούν αποκλειστικά τα PoS συστήματα είναι η nothing-at-stake επίθεση[148] και η long-range επίθεση[149], η οποία συναντάται και στο DPoS. Άλλες γνωστές επιθέσεις που κατά καιρούς έχουν προσβάλλει τα διάφορα blockchain συστήματα είναι οι balance, refund, replay, short-address, finney, vector76, overflow, reentrancy, wallet theft, time-jacking, block-withholding, fork-after-withhold, bribery, pool hopping, consensus delay, selfish mining, DNS highjacks, partition routing, transaction malleability, P+Epsilon, alternative history, race, record hacking, identity theft, DAO, liveness επιθέσεις κά. Για πιο αναλυτική μελέτη των παραπάνω επιθέσεων υπάρχει αναλυτική έρευνα στην ευρύτερη βιβλιογραφία [121][120][123][124][150][151][152].

Πίνακας 4-Αναλυτική σύγκριση των κύριων μηχανισμών συναίνεσης

	POW	***POS***	***DPOS***	***POET***	***PBFT***	***RPCA***	***SCP***
ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΣΥΝΑΙΝΕΣΗΣ	Απόλυτη αντικειμενικότητα	Ελάχιστη αντικειμενικότητα	Ασθενώς υποκειμενικός	Απόλυτη αντικειμενικότητα	Απόλυτη υποκειμενικότητα	Απόλυτη υποκειμενικότητα	Απόλυτη υποκειμενικότητα
ΔΙΑΚΡΙΣΗ ΜΟΝΤΕΛΟΥ ΣΥΝΑΙΝΕΣΗΣ	Proof-based	Και τα δύο	Proof-based με διαδικασία ψηφοφορίας	Proof-based	Vote-based	Vote-based	Vote-based
ΕΠΟΜΕΝΟ ΜΠΛΟΚ-ΔΙΑΔΙΚΑΣΙΑ ΕΞΟΡΥΞΗΣ	Εξόρυξη κατακερματιστικής ισχύος	Δύναμη stake (πχcoin age)	Stake-vote πρωτόκολλο	Έμπιστο περιβάλλον εκτέλεσης	Πολλαπλοί γύροι ψηφοφορίας	Πιθανολογική ψηφοφορία	Ομοσπονδιακή ψηφοφορία
ΚΑΤΗΓΟΡΙΑ BLOCKCHAIN	Δημόσια	Όλα	Όλα	Ιδιωτικά-κοινοπρακτικά συστήματα	Ιδιωτικά	Δημόσια	Δημόσια
ΕΥΕΛΙΞΙΑ ΕΜΠΙΣΤΟΣΥΝΗΣ ΜΟΝΤΕΛΟΥ	Έλλειψη βαθμού ατομικής εμπιστοσύνης-Μη ευέλικτο	Εμπιστοσύνη αναλογική με το stake-Μη ευέλικτο	Πλήρης εμπιστοσύνη στους delegates-Ευέλικτο	Τυχαίο μοντέλο εκλογής λοταρίας-Μη ευέλικτο	Ομοφωνία σε περιβάλλον εμπιστοσύνης-Απόλυτη ευελιξία	Συμμετοχή σε UNL-Απόλυτη ευελιξία	Συμμετοχή σε quorums, quorum slices-Απόλυτη ευελιξία
ΕΝΕΡΓΕΙΑΚΗ ΚΑΤΑΝΑΛΩΣΗ	Υψηλή	Μέτρια(χαμηλότερη από PoW)	Μέτρια(χαμηλότερη από PoW, PoS)	Χαμηλή	Ελάχιστη	Ελάχιστη	Ελάχιστη
ΒΑΘΜΟΣ ΑΠΟΚΕΝΤΡΩΤΙΣΜΟΥ	Τάσεις συγκεντρωτισμού (mining pools)	Μερική αποκέντρωση-Οι πλούσιοι πλουσιότεροι	Μερική αποκέντρωση-Αντιπροσωπευτικά δημοκρατικό	Μάλλον συγκεντρωτικό-Κεντρική ηγεσία	Πλήρης συγκεντρωτισμός	Αποκεντρωμένο δίκτυο	Αποκεντρωμένο δίκτυο
ΕΧΘΡΙΚΗ ΑΝΟΧΗ	25%	50%	50%	50%	33%	Ίσως κοντά στο 90%	33%
ΚΟΣΤΟΣ ΣΥΜΜΕΤΟΧΗΣ	Υψηλό(σπατάλη ηλ. Ενέργειας-πόρων)	Μέτριο(πχ αγορά αρχικών κρυπτονομισμάτων)	Χαμηλό(λιγότερο από PoW, PoS)	Χαμηλό(κατανάλωση χρόνου αναμονής και απαραίτητου εξοπλισμού)	Μηδενικό	Μηδαμινό (της τάξης των $4x10^{-7}$ $)	Παρόμοια με RCPA
ΟΡΙΣΤΙΚΟΤΗΤΑ ΣΥΝΑΛΛΑΓΩΝ	Πιθανολογική	Πιθανολογική	Πιθανολογική	Πιθανολογική	Απόλυτη	Απόλυτη	Απόλυτη
ΕΠΙΠΕΔΟ ΔΙΑΚΙΝΗΣΗΣ ΣΥΝΑΛΛΑΓΩΝ(TPS)	Περιορισμένη(3-56)	Χαμηλό(λιγότερες από 10)	Μέχρι περίπου 4000-Δυνατότητα 100000 (EOS, Bitshares)		Μέχρι 3500-Δυνατότητα δεκάδων χιλιάδων	1500	1000
ΕΠΙΠΕΔΟ ΑΠΟΚΕΝΤΡΩΣΗΣ	Αποκεντρωτικό	Αποκεντρωτικό	Μερικώς συγκεντρωτικό	Κεντρική ηγεσία(SGX)	Συγκεντρωτικό	Αποκεντρωτικό	Αμφιλεγόμενο

2.8. Συμπεράσματα και αξιολόγηση

Συνοψίζοντας όλα τα παραπάνω ποιοτικά και ποσοτικά δεδομένα μπορούμε να καταλήξουμε στο συμπέρασμα πως το σύνολο των proof-based μηχανισμών συναίνεσης χαρακτηρίζεται από χαμηλή διακίνηση συναλλαγών και μεγάλες χρονικές καθυστερήσεις, σε πλήρη αντίθεση με τα BA μοντέλα τα οποία παρέχουν μεγαλύτερη διακίνηση και ταχύτητες συναλλαγών και μικρές χρονικές καθυστερήσεις. Έτσι χαρακτηρίζουμε τα BA μοντέλα ως πιο αποδοτικά. Επιπλέον η παραπάνω σύγκριση μπορεί να γενικευτεί και στη διαφοροποίηση των δημόσιων από τα ιδιωτικά και κοινοπρακτικά blockchain συστήματα. Αναφορικά με την επεκτασιμότητα αναλύσαμε τους διάφορους μηχανισμούς συναίνεσης με βάση τη διακίνηση και τον αριθμό των συμμετέχοντων κόμβων. Οι PoW, PoS μηχανισμοί παρέχουν πολύ φτωχή διακίνηση συγκριτικά με το DPoS και τα κυριότερα BA συστήματα. Βέβαια στον αντίποδα τα BA συστήματα είναι σημαντικά λιγότερο επεκτάσιμα ως προς το πλήθος των κόμβων που μπορούν να διαχειριστούν, λόγω της σύνθετης και μεγάλης πολυπλοκότητας που συνεπάγεται η ανταλλαγή μηνυμάτων στο δίκτυό τους. Αναφορικά με την ασφάλεια που παρέχεται στο πλαίσιο της blockchain εφαρμογής σε διάφορα πρωτόκολλα, συστήματα και δίκτυα, αναλύσαμε τόσο την εχθρική ποσοστιαία ανεκτικότητα όσο και την ανοχή στις πιο κλασσικές και επιζήμιες επιθέσεις. Καταλήγουμε στο συμπέρασμα πως κανένας μηχανισμός συναίνεσης δεν μπορεί να θεωρηθεί 100% ασφαλής απέναντι στην κακόβουλη συμπεριφορά των εχθρικών κόμβων. Επιπλέον αν και ο δημοφιλέστερος μηχανισμός συναίνεσης, το PoW, έχει επικρατήσει ως ένας απ' τους ασφαλέστερους λόγω της τεράστιας υπολογιστικής ισχύος που δαπανάται, με βάση την ανάλυσή μας παρατηρούμε πως είναι επιρρεπής σε όλες τις βασικές μορφές επιθέσεων που αναλύσαμε. Γενικεύοντας τη συζήτηση περί ασφάλειας μπορούμε να πούμε πως τα δημόσια συστήματα έχουν στο σύνολό τους καλύτερη ανοχή ποσοστιαίας εχθρικότητας, αλλά όχι απαραίτητα και εχθρικών επιθέσεων, από τα ιδιωτικά και κοινοπρακτικά. Απ' την άλλη τα ιδιωτικά κυρίως και πολλά κοινοπρακτικά δίκτυα λειτουργούν στηριζόμενα σε ένα αυστηρό μποντέλο εμπιστοσύνης, οπότε από αυτή την άποψη μπορούν να προβλέψουν και να αναχαιτίσουν με μεγαλύτερη ευκολία περισσότερα ήδη εχθρικών επιθέσεων. Συμπερασματικά λοιπόν, δεν μπορούμε να χαρακτηρίσουμε σε γενικό πλαίσιο κάποιο μοντέλο συναίνεσης ως ασφαλέστερο ή μη συγκριτικά με τα υπόλοιπα. Κάθε μοντέλο συναίνεσης έχει τα δικά του πλεονεκτήματα και περιορισμούς. Συνεπώς ανάλογα με το σύστημα και την εφαρμογή που πρόκειται να χρησιμοποιήσει την blockchain τεχνολογία, επιλέγεται και διαφορετικό μοντέλο συναίνεσης. Κλασσικό παράδειγμα είναι η χρήση του PoW σε δημόσιες πλατφόρμες, όπως το Bitcoin και το Ethereum, και η εφαρμογή του PBFT σε ιδιωτικά συστήματα, όπως το Hyperledger Fabric.

Κεφάλαιο 3. Επεκτασιμότητα

.

3.1. Προσδιορισμός του προβλήματος

Γιατί η επεκτασιμότητα αποτελεί ένα τεράστιο πρόβλημα για την τεχνολογία blockchain; Πώς η επεκτασιμότητα επηρεάζει την εξέλιξη και τη διάδοση της τεχνολογίας blockchain σε ένα ακόμα μεγαλύτερο φάσμα εφαρμογών; Ένα σύστημα με ιδανική επεκτασιμότητα θα έχει την ίδια λειτουργικότητα με τα υπάρχοντα συστήματα και τα επίπεδα επεκτασιμότητας τους;
Προσπαθώντας να βρούμε απάντηση στα παραπάνω ερωτήματα θα προσδιορίσουμε πιο αναλυτικά τα προβλήματα-θέματα που σχετίζονται με την επεκτασιμότητα:

- Εγγενής περιορισμοί: Εξ' ορισμού σε κάθε σύστημα blockchain η ολοκλήρωση νέων συναλλαγών συνεπάγεται την προσθήκη ενός νέου μπλοκ στην αλυσίδα του συστήματος. Το γεγονός αυτό σε συνδυασμό με το τεχνικό χαρακτηριστικό της τεχνολογίας να μεταφέρει ολόκληρο το ιστορικό των συναλλαγών(άρα ένα σύνολο από ήδη γεμάτα μπλοκ) αλλά και την αυξανόμενη ζήτηση οδηγούν το ίδιο το σύστημα να "λυγίσει" υπό τη δική του εγγενή δομή.

- Όγκος δεδομένων: Το δημοφιλέστερο κρυπτονόμισμα στις μέρες μας(Bitcoin) έχει αρχικό περιορισμό χωρητικότητας κάθε μπλοκ στο 1MB το οποίο ισοδυναμεί με περίπου 2.020 συναλλαγές, αλλά με τον καιρό υπήρξαν προτάσεις αύξησης του παραπάνω ορίου(όπως θα δούμε παρακάτω), ενώ άλλα νομίσματα όπως το Ethereum δεν περιλαμβάνουν αντίστοιχο περιορισμό των μπλοκ.
  Σε κάθε περίπτωση και ανεξαρτήτως περιορισμών χωρητικότητας ο όγκος των συναλλαγών αυξάνεται συνεχώς, το δίκτυο δέχεται ολοένα και περισσότερους χρήστες και συνεπώς ο όγκος των δεδομένων οδηγεί το ίδιο το σύστημα σε διαρκή αύξηση του μεγέθους των μπλοκ: κάτι το οποίο δεν αποτελεί ουσιαστική αλλά προσωρινή λύση.

- Χρονικές καθυστερήσεις: Η ολοκλήρωση κάθε συναλλαγής απαιτεί peer-to-peer επιβεβαίωση. Ο χρόνος που απαιτείται για τη διαδικασία αυτή επηρεάζεται από τον αριθμό των μπλοκ που συμμετέχουν στη διαδικασία.
  Έτσι καθώς το σύνολο των χρηστών μεγαλώνει πραγματοποιώντας συνεχώς περισσότερες συναλλαγές οι χρονικές καθυστερήσεις και οι χρόνοι αναμονής αυξάνονται σημαντικά, δημιουργώντας πρόβλημα στην ζήτηση και τη λειτουργικότητα του συστήματος.
  Το Bitcoin παρέχει 3-7 συναλλαγές ανά δευτερόλεπτο, ο χρόνος επιβεβαίωσης συναλλαγών είναι περίπου 60 λεπτά ενώ κάθε νέο μπλοκ δημιουργείται κάθε 10 λεπτά. Το Ethereum παρέχει 15-20 συναλλαγές ανά δευτερόλεπτο με χρόνο επιβεβαίωσης 2-6 λεπτά και χρόνο δημιουργίας επόμενου μπλοκ στα 12 δευτερόλεπτα.
  Τα παραπάνω δεδομένα των δύο δημοφιλέστερων κρυπτονομισμάτων αυτή τη στιγμή στην αγορά μοιάζουν πενιχρά συγκριτικά με τα νούμερα που παρέχουν κάποια από τα επικρατέστερα συγκεντρωτικά συστήματα συναλλαγών όπως η

Visa(1.667 κατά μέσο όρο, μέχρι και 24.000-56.000 συναλλαγές ανά δευτερόλεπτο[153][154])το Paypal(193 κατά μέσο όρο[6]) και η MasterCard.

- Κόστος συναλλαγών: Ο συνωστισμός που προκαλείται σε ένα blockchain σύστημα λόγω της μεγάλης ζήτησης οδηγεί στον αυξανόμενο αριθμό χρηστών που προωθούν τις συναλλαγές. Μιας και τα λειτουργικά έξοδα είναι σημαντικά καταλαβαίνουμε εύκολα πως όσο διευρύνεται η κλιμάκωση τόσο τα έξοδα αυτά θα αποτελούν όλο και μεγαλύτερο αγκάθι στην εξέλιξη της τεχνολογίας blockchain.
  Συν της άλλοις οι miners προτιμούν να ολοκληρώνουν τις συναλλαγές των χρηστών εκείνων που προσφέρουν μεγαλύτερα τέλη συναλλαγών, μετατρέποντας την όλη διαδικασία σ΄ ένα παιχνίδι συναγωνισμού στο οποίο νικητής είναι εκείνος που έχει να προσφέρει περισσότερα. Αν σκεφτούμε μία ιδανική τεχνολογία blockchain με τεράστια περιθώρια επεκτασιμότητας τότε το παιχνίδι αυτό ζήτησης συναλλαγών-τελών θα έχει ως αποτέλεσμα τεράστια ποσά χρέωσης ακόμα και για μια απλή συναλλαγή μετατρέποντας τον αποκεντρωτικό χαρακτήρα της τεχνολογίας σε συγκεντρωτικό και κερδοφόρο.

3.2. Συναλλαγές ανά δευτερόλεπτο-Χρόνος επιβεβαίωσης συναλλαγών

Η έννοια της επεκτασιμότητας συνδέεται άμεσα με την ταχύτητα εκτέλεσης συναλλαγών του εκάστοτε συστήματος. Για μας η έννοια της ταχύτητας εκτέλεσης περιλαμβάνει δύο βασικά χαρακτηριστικά της τεχνολογίας blockchain:

1. *Συναλλαγές ανά δευτερόλεπτο (Transactions per second)*

2. *Χρόνος επιβεβαίωσης συναλλαγών (Transaction confirmation time)*

Οι ταχύτητες των διάφορων κρυπτονομισμάτων δεν αποτελούν σταθερό αλλά χρονικά μεταβαλλόμενο μέγεθος και εξαρτώνται από μία σειρά χρονικών παραγόντων[7] όπως:

- Μέση τιμή τελών συναλλαγών
- Όγκος των συναλλαγών
- Ο τύπος συναλλαγής περιλαμβάνεται στη δημιουργία μπλοκ
- Συνθήκες του διαδικτύου

Άξιο αναφοράς είναι το γεγονός πως αν και μερικά κρυπτονομίσματα χρησιμοποιούν το ίδιο ή παρόμοια συστήματα συναίνεσης τα δεδομένα τους όσον αφορά τις

[6] https://altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/
[7] https://cryptocomes.com/which-cryptocurrencies-have-fastest-transaction-speeds

ταχύτητες εκτέλεσης παρουσιάζουν μεγάλη διαφορετικότητα, γεγονός που φανερώνει την ξεκάθαρη εξάρτηση των νομισμάτων από τους παραπάνω παράγοντες.
Οφείλουμε να αναφέρουμε ότι τα ποσοτικά δεδομένα που αφορούν τις συναλλαγές ανά δευτερόλεπτο και τους χρόνους επιβεβαίωσης των συναλλαγών σε αρκετές περιπτώσεις βρίσκονται σε θεωρητικό επίπεδο ή σε πιλοτικό στάδιο. Ακόμα μία πρόχειρη έρευνα στο διαδίκτυο για την εύρεση των μεγεθών αυτών θα μας οδηγήσει σε πηγές που παρουσιάζουν διαφορετικά δεδομένα ακόμα και για τα ίδια κρυπτονομίσματα. Για το λόγο αυτό στους συγκριτικούς Πίνακες 1 και 2 της Ενότητας 2.7 συμπεριλάβαμε αριθμητικά δεδομένα που κατά βάση αναφέρονται σε υπάρχουσες, εξακριβωμένες και δοκιμασμένες περιστάσεις.
Ακόμα ένας άλλος παράγοντας που συνδέεται άμεσα με την επεκτασιμότητα είναι ο αριθμός των κόμβων που μπορεί να αντέξει ένα blockchain σύστημα, καθώς ανάλογα με το πλήθος των κόμβων επηρεάζεται πολλές φορές καθοριστικά η απόδοση του ίδιου του συστήματος. Για παράδειγμα τα δημόσια blockchain δίκτυα επιτρέπουν συνήθως απεριόριστη συμμετοχή, σε αντίθεση με τα ιδιωτικά δίκτυα που μπορούν να διαχειριστούν περιορισμένο πλήθος κόμβων για να διατηρήσουν τους δείκτες αποδοτικότητάς τους σε ικανοποιητικά επίπεδα.

3.3. Πιθανές λύσεις-προτάσεις

Έχοντας προσδιορίσει παραπάνω τα διάφορα θέματα που απασχολούν την επιστημονική κοινότητα σχετικά με την επεκτασιμότητα των blockchain συστημάτων θα παραθέσουμε μια σειρά από διάφορες προτάσεις(άλλες ήδη σε εφαρμογή, άλλες σε επίπεδο δοκιμών και άλλες σε θεωρητικό επίπεδο) οι οποίες μπορούν να συμβάλουν στην επίλυση των θεμάτων αυτών. Στο παρελθόν έχουν γίνει αρκετές προσπάθειες βελτίωσης της επεκτασιμότητας, ωστόσο η ερευνητική κοινότητα δεν έχει καταλήξει σε κάποια επαρκή-τελική λύση. Θα αναφέρουμε κάποιες προσπάθειες που έχουν γίνει στο παρελθόν για την επίλυση του προβλήματος της επεκτασιμότητας και στη συνέχεια θα παραθέσουμε μια σειρά από προτάσεις που προσεγγίζουν το θέμα με τον βέλτιστο δυνατό τρόπο.

3.3.1.Πρώιμες προσεγγίσεις του προβλήματος

Οι πρώτες προσπάθειες αντιμετώπισης του προβλήματος της επεκτασιμότητας τοποθετούνται στην δεκαετία του 1990, όταν ο G. Bracha[155] εισήγαγε την ιδέα της διαίρεσης του συνόλου των χρηστών σε μικρότερες ομάδες-επιτροπές. Έκτοτε υπάρχουν αναρίθμητες προσεγγίσεις στην υπάρχουσα βιβλιογραφία που βελτίωσαν σε κάποιο βαθμό την επεκτασιμότητα και παρουσίασαν διάφορες πρωτοπόρες τεχνικές κατά καιρούς. Η αναφορά σε αυτές τις προσεγγίσεις είναι χρονοβόρα και για τον λόγο αυτό θα αναφερθούμε μόνο σε μερικές σύγχρονες περιπτώσεις που παρουσιάζουν μεγάλο ενδιαφέρον:

Το πρωτόκολλο GHOST[156] επιτρέπει περισσότερες συναλλαγές απ' ότι το Bitcoin καθώς τροποποιεί τον κανόνα καθορισμού της κύριας-έγκυρης αλυσίδας. Συγκεκριμένα αντί να ακολουθεί τον κανόνα της μεγαλύτερης αλυσίδας του Bitcoin "βάζει στο παιχνίδι της επικράτησης" και τα μπλοκ τα οποία αν και δεν είναι τα πρωταρχικά(χρονικά) περιλαμβάνουν περισσότερο φόρτο εργασίας από τα μπλοκ που ολοκληρώθηκαν πρώτα, επιτρέποντας έτσι τη συμμετοχή των orphaned blocks και παρέχοντας με αυτή τη διαδικασία μεγαλύτερη ασφάλεια στην αύξηση του μεγέθους και της συχνότητας παραγωγής των μπλοκ. Ακόμα η παραπάνω διαδικασία προσφέρει καλύτερη αξιοποίηση στο τομέα της ισχύος εξόρυξης αλλά και υψηλότερο επίπεδο δικαιοσύνης.
Ωστόσο αν και προσφέρει βελτιωμένη επεκτασιμότητα, καθώς ουσιαστικά παρέχει στο δίκτυο τον παραλληλισμό των μπλοκ, δεν διαχωρίζει τον όγκο των δεδομένων από την διαδικασία ομοφωνίας, καθώς όλα τα δεδομένα από τα μπλοκ μεταδίδονται στο δίκτυο προκαλώντας συνωστισμό και την μείωση της λειτουργικότητας του. Ακόμα για έναν χρήστη δεν είναι δεδομένο πως μπορεί να διακρίνει ποια αλυσίδα είναι η έγκυρη καθώς σε αντίθεση με το Bitcoin στο πρωτόκολλο GHOST υπάρχει πιθανότητα κανένας χρήστης να μην έχει τις απαραίτητες πληροφορίες ώστε να αναγνωρίσει την κύρια αλυσίδα. Επίσης οι περισσότερες συναλλαγές ακολουθούνται από τη δαπάνη μεγαλύτερης υπολογιστικής ισχύος, καθυστερώντας τη διαδικασία της ομοφωνίας στο σύστημα[157].
Σε μία μεταγενέστερη προσπάθεια βελτίωσης της επεκτασιμότητας, στο πρωτόκολλο Bitcoin-NG[158] ο ηγέτης της κάθε εποχής(*epoch*) του συστήματος μπορεί να περιλαμβάνει στην εποχή του περισσότερα μπλοκ. Το πρωτόκολλο αυτό χαρακτηρίζει ο διαχωρισμός των μπλοκ σε *key blocks* και *microblocks*. Στα key blocks πραγματοποιείται η εκλογή των ηγετών οι οποίοι παράλληλα μπορούν να προσθέτουν στην αλυσίδα τα microblocks τα οποία περιλαμβάνουν τις συναλλαγές του ηγέτη κάθε εποχής. Με την διαδικασία αυτή το παραπάνω πρωτόκολλο παρέχει επίσης μια μορφή παραλληλισμού στο σύστημα βελτιώνοντας το επίπεδο επεκτασιμότητας και μειώνοντας τα επίπεδα αφάνειας.
Ωστόσο παρόμοια με το GHOST δεν υπάρχει διαχωρισμός μεταξύ δεδομένων-ομοφωνίας υπερφορτώνοντας έτσι το σύστημα και δυσχεραίνοντας την επίτευξη ομοφωνίας. Ακόμα η εκλογή των ηγετών ακολουθεί τη λογική του κλασσικού PoW αλγορίθμου ρισκάροντας έτσι την εμφάνιση forks και ενέχοντας κινδύνους ασφάλειας[79]. Τέλος η διαδικασία επίτευξης ομοφωνίας επιβραδύνεται σημαντικά λόγω της αναλογικής εξάρτησης συναλλαγών-υπολογιστικής ισχύος όπως και στο GHOST.
Ακόμα πιο πρόσφατα, το Ιούλιο του 2017, ενεργοποιήθηκε το Segregated Witness(SegWit)[8] το οποίο αποτελεί ένα soft fork του Bitcoin. Αν και η αναβάθμιση αυτή αρχικά αποσκοπούσε στην αντιμετώπιση της μαλακότητας των συναλλαγών(*transaction malleability*)[159], ένα χαρακτηριστικό πρόβλημα του Bitcoin, ουσιαστικά συντέλεσε και στην αντιμετώπιση του προβλήματος της επεκτασιμότητας. Πιο αναλυτικά το SegWit,σε αντίθεση με τα προηγούμενα πρωτόκολλα διαχωρίζει τον όγκο των δεδομένων που περιέχουν τις ψηφιακές υπογραφές και καταλαμβάνουν το 65-70% των δεδομένων συναλλαγών από τα δεδομένα των συναλλαγών, μετριάζοντας έτσι το πρόβλημα του περιορισμού του μεγέθους των μπλοκ και επιτρέποντας περισσότερες συναλλαγές σε ένα μπλοκ χωρίς

[8] https://en.wikipedia.org/wiki/SegWit

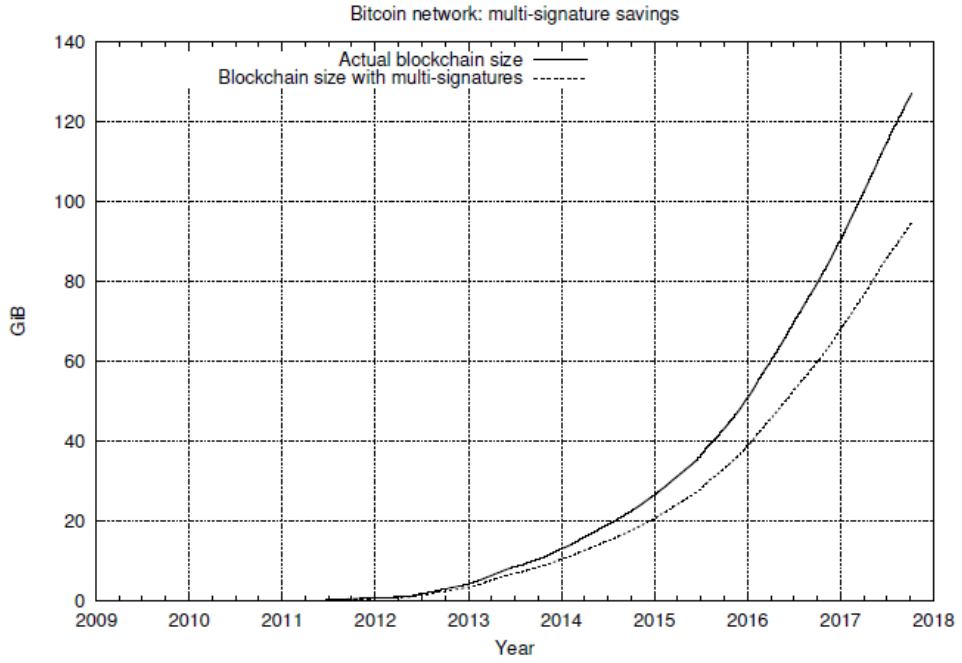
την αύξηση της χωρητικότητάς του. Ακόμα το SegWit διευκολύνει την υλοποίηση του Lightning Network, το οποίο θα αναλύσουμε παρακάτω.
Μία παρόμοια εκδοχή του SegWit, το SegWit2x προσπάθησε να συντελέσει στο πρόβλημα της επεκτασιμότητας προτείνοντας αύξηση του μεγέθους των μπλοκ στα 2MB, ωστόσο δεν έχει εφαρμοστεί ακόμα από την πλειοψηφία.
Στις αρχές του Αυγούστου του 2017,πραγματοποιήθηκε μία αλλαγή-hard fork στο Bitcoin που είχε ως αποτέλεσμα τον διαχωρισμό του υπάρχοντος blockchain συστήματος σε δύο μέρη και τη δημιουργία ενός νέου κρυπτονομίσματος, το Bitcoin Cash[9], το οποίο συντέλεσε στο ζήτημα της επεκτασιμότητας αυξάνοντας το όριο των μπλοκ μέχρι και 8 MB.
Βέβαια η αύξηση του ορίου στο μέγεθος των μπλοκ δεν αποτελεί ουσιαστική παρά μόνο προσωρινή λύση σε ένα γενικότερο δομικό πρόβλημα της blockchain τεχνολογίας. Για παράδειγμα το όριο των 8MB προσφέρει μια γραμμική αύξηση στις συναλλαγές ανά δευτερόλεπτο αυξάνοντάς τες στις 56 (7 TPS x 8 MB) που σημαίνει ότι η ανάγκη της επιπλέον διεύρυνσης του ορίου των μπλοκ δεν θα σταματήσει ποτέ κρίνοντας με βάση την ασταμάτητα αυξανόμενη ζήτηση.
Όπως γίνεται εύκολα αντιληπτό οι παραπάνω προσεγγίσεις αν και προσφέρουν εμφανή βελτίωση στην επεκτασιμότητα των blockchain συστημάτων δεν παρέχουν μία επαρκή αλλά μία μερική και προσωρινή λύση. Για το λόγο αυτό παρακάτω παρουσιάζουμε κάποιες λύσεις, αναλύοντας τα χαρακτηριστικά και τα μειονεκτήματά τους, οι οποίες τόσο ατομικά όσο και σε συνδυαστικό επίπεδο προσφέρουν τη βέλτιστη δυνατή προσέγγιση:

3.3.2.Schnorr signatures

Το σχέδιο των Schnorr signatures παρουσιάστηκε το 1991[160] και η λογική του μπορεί να αποτελέσει ένα διέξοδο στην επεκτασιμότητα του Bitcoin[161]. Συγκεκριμένα για την ολοκλήρωση συναλλαγών μέσω Bitcoin οι ψηφιακές υπογραφές και κλειδιά είναι απαραίτητα, καθώς αποτελούν αναπόσπαστο κομμάτι της έγκρισης και της διασφάλισης της ιδιωτικότητας των συναλλαγών. Συνεπώς τα ψηφιακά αυτά δεδομένα αποτελούν κομμάτι των συναλλαγών με αποτέλεσμα να καταλαμβάνουν αποθηκευτικό χώρο στα μπλοκ του blockchain. Κατά την εκτέλεσή της μεταξύ ενός αποστολέα κι ενός αποδέκτη, κάθε μεμονωμένη συναλλαγή απαιτεί και ένα ζευγάρι ψηφιακών κλειδιών αλλά και την αντίστοιχη ψηφιακή υπογραφή. Το ουσιαστικό πρόβλημα έγκειται στην περίπτωση που κάποιος χρήστης(ή ομάδα χρηστών) επιθυμεί να πραγματοποιήσει συναλλαγές από πολλαπλές διευθύνσεις προς τον ίδιο παραλήπτη: κάθε συναλλαγή ακολουθείται από έναν συνδυασμό κλειδιών-υπογραφής με αποτέλεσμα τη δέσμευση μεγαλύτερου αποθηκευτικού χώρου που με τη σειρά του οδηγεί σε αυξημένα τέλη συναλλαγών. Η χρήση των Schnorr signatures, με την εφαρμογή μαθηματικών κανόνων, επιτρέπει στον παραπάνω χρήστη να ολοκληρώσει την πολλαπλή αυτή συναλλαγή συνδυάζοντας το ιδιωτικό κλειδί, το δημόσιο κλειδί και την υπογραφή σε ένα αποδεσμεύοντας χώρο και δίνοντας έτσι μία λύση στο πρόβλημα επεκτασιμότητας του Bitcoin . Σύμφωνα με τους προγραμματιστές που εργάζονται πάνω στην συγκεκριμένη τεχνολογία, η εφαρμογή

[9] https://en.wikipedia.org/wiki/Bitcoin_Cash

της μπορεί να οδηγήσει σε μια εκτιμώμενη αύξηση 25% έως 30% στη συναλλακτική ικανότητα του Bitcoin[162]. Η συμβολή των Schnorr signatures στο σύστημα του Bitcoin φαίνεται στο παρακάτω διάγραμμα, όπου παρουσιάζεται μία σύγκριση μεγέθους με και χωρίς την εφαρμογή αυτών.
Το σχέδιο των Schnorr signatures βρίσκεται ακόμα σε πειραματικό στάδιο και συνεπώς δεν μπορούμε για την ώρα να εξάγουμε ασφαλή συμπεράσματα για το πώς θα ενισχύσει την επεκτασιμότητα του Bitcoin. Ωστόσο αν και η αλλαγή που μπορεί να επιφέρει στα υπάρχοντα επίπεδα επεκτασιμότητας μοιάζει πολλά υποσχόμενη, εκφράζονται έντονες ανησυχίες και αμφισβητήσεις σχετικά με τα επίπεδα ασφάλειας που παρέχει[163][164].



Εικόνα 9-Μέγεθος του Bitcoin με και χωρίς την εφαρμογή των Schnorr signatures[161]

3.3.3.Συναλλαγές εκτός αλυσίδας(Off-chain transactions)

Αναφερόμενοι στις συναλλαγές εκτός αλυσίδας θα μπορούσαμε να χρησιμοποιήσουμε επίσης τους όρους τεχνικές δύο στρωμάτων(*layer-2*) και στρατηγικές στηριζόμενες σε κανάλια πληρωμών(*channel-based strategies*). Για να κατανοήσουμε αρχικά την διαφορά των τεχνικών αυτών από τα ήδη υπάρχοντα παγιωμένα συστήματα αρκεί να αναφέρουμε ότι το Bitcoin και το Ethereum τα οποία κυριαρχούν στις ψηφιακές αγορές θεωρούνται στην αρχική τους δομή layer-1 συστήματα. Καθώς δεν υπάρχει κάποιος επίσημος ή επιστημονικός ορισμός για το διαχωρισμό μεταξύ των layer-1 και layer-2 συστημάτων μπορούμε να κάνουμε την εξής διευκρίνηση: το layer-1(*ή root chain*) αποτελεί τον πυρήνα, το πρώτο στάδιο, το αρχικό στρώμα του ευρύτερου αποκεντρωμένου οικοσυστήματος μιας τεχνολογίας blockchain με αποτέλεσμα οι layer-1 στρατηγικές να αφορούν αλλαγές στο βασικό πρωτόκολλο, ενώ οι layer-2 τεχνικές αποτελούν νέα επίπεδα-στρώματα τα οποία προσπαθούν να εφαρμόσουν μια λύση πάνω από την υπάρχουσα υποδομή και μπορούν να πραγματοποιούνται εκτός του layer-1 επιπέδου αλλά η λειτουργικότητα τους στηρίζεται εξ' ολοκλήρου στον πυρήνα της τεχνολογίας, προσφέροντας με αυτόν τον τρόπο μία πρωτοποριακή προσέγγιση στον τομέα της επεκτασιμότητας. Η υλοποίηση των layer-2 τεχνικών αφαιρεί μεγάλο όγκο δεδομένων από κύριο στρώμα του blockchain ελευθερώνοντας έτσι αποθηκευτικό χώρο και βελτιώνοντας την ταχύτητα εκτέλεσης ενώ παράλληλα διατηρούνται η ασφάλεια και ο αποκεντρωτικός χαρακτήρας. Τα κυριότερα layer-2 μοντέλα που μπορούν να αλλάξουν ριζικά τα δεδομένα στα θέματα επεκτασιμότητας είναι :

3.3.3.1. Πεπλατυσμένες πλευρικές αλυσίδες (Pegged Sidechains)

Η τεχνολογία των Pegged Sidechains(ή Sidechains)[165]επιχειρεί την βελτίωση της λειτουργίας του Bitcoin[166]. Ουσιαστικά αποτελεί έναν δίαυλο επικοινωνίας του Bitcoin (και όχι μόνο) με άλλα blockchain συστήματα, καθώς παρέχει την δυνατότητα σε κάποιον χρήστη να διακινήσει τα Bitcoins που κατέχει μεταξύ άλλων ξεχωριστών συστημάτων διατηρώντας αναλλοίωτη την αξία τους σε, επιτρέποντας έτσι στον χρήστη να έχει πρόσβαση σε πλατφόρμες που χρησιμοποιούν διαφορετικά κρυπτονομίσματα. Οι αλυσίδες αυτές αποτελούν μία ξεχωριστή πλατφόρμα ανεξάρτητη από το αρχικό σύστημα και επιτρέπουν την αμφίδρομη αλληλεπίδραση διαφορετικών συστημάτων blockchain χωρίς την δημιουργία νέων κρυπτονομισμάτων και λειτουργικών κανόνων ενισχύοντας την έννοια της διαλειτουργικότητας.
Αν και σαν τεχνολογία προτείνει θεωρητικά μια νέα οπτική για την εξέλιξη της επεκτασιμότητας σύμφωνα με τον ίδιο τον συγγραφέα χαρακτηρίζεται από σημαντικά μειονεκτήματα όπως πολυπλοκότητα, πιθανότητα πραγματοποίησης παράνομων συναλλαγών, κίνδυνος συγκεντρωτισμού και εμφάνισης soft forks, ενώ έντονη είναι η αμφισβήτηση της γενικότερης ασφάλειας που παρέχει[167][168].

3.3.3.2. Lightning Network

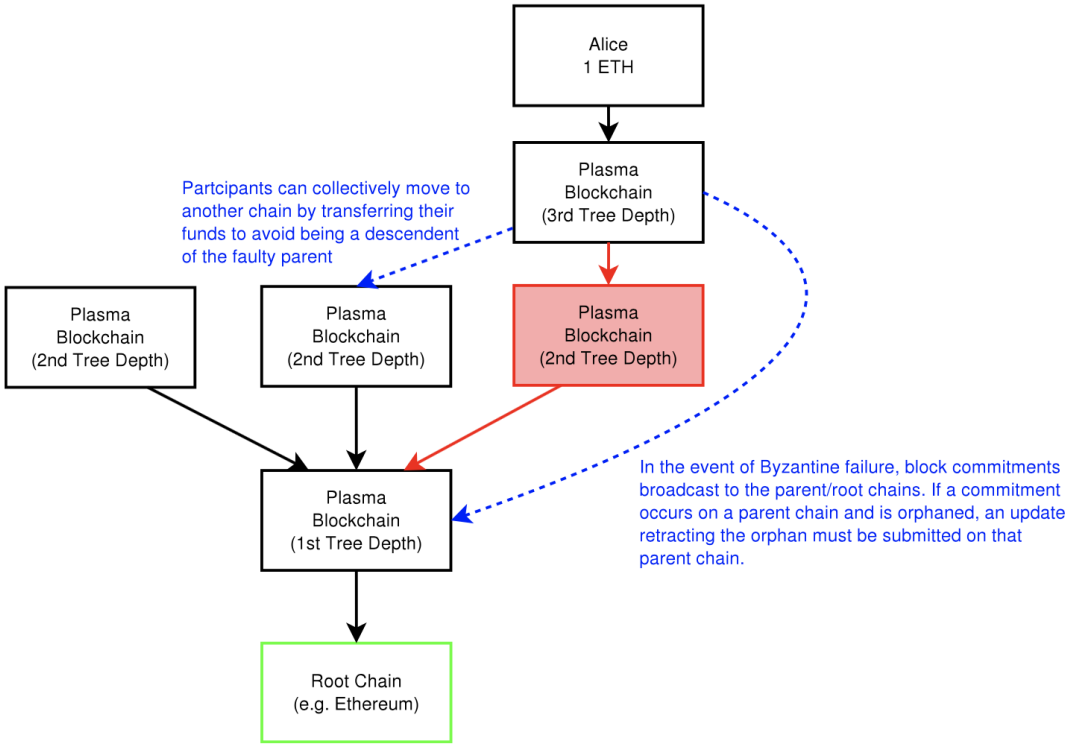
Το Lightning Network[169] στηρίζει τη λειτουργία του σε ένα off-chain πρωτόκολλο και συνιστά ένα δίκτυο καναλιών μικροπληρωμών παρέχοντας σχεδόν άμεσες συναλλαγές. Στηριζόμενο στο SegWit που αναφέραμε παραπάνω το Lightning Network αποτελεί μία ουσιαστική διέξοδο στα υπάρχοντα επίπεδα επεκτασιμότητας του Bitcoin(ενώ το Δεκέμβρη του 2018 αναμένεται να υλοποιηθεί και στο Stellar[10]) με τη χρήση των καναλιών πληρωμών εκτός αλυσίδας: η κύρια αλυσίδα αποφορτίζεται από τον τεράστιο όγκο των συναλλαγών καθώς αυτές λαμβάνουν χώρα σε ξεχωριστά κανάλια τα οποία παραμένουν ανοιχτά διατηρώντας όσες συναλλαγές επιθυμούν οι χρήστες που συμμετέχουν σε αυτά, ενώ στην κύρια αλυσίδα αποθηκεύονται μόνο το άνοιγμα και το κλείσιμο του καναλιού αποτυπώνοντας το συνολικό μέγεθος της συναλλαγής. Ιδιαίτερο ενδιαφέρον παρουσιάζει το γεγονός πως οι συναλλασσόμενοι χρήστες μπορούν να πραγματοποιούν συναλλαγές συμπεριλαμβάνοντας πέρα από τους ίδιους και επιπλέον χρήστες δημιουργώντας έτσι ένα δίκτυο καναλιών πληρωμών εκτός της κύριας αλυσίδας. Το Lightning Network ουσιαστικά δεν επιφέρει αλλαγές στο θεμελιώδες λογισμικό του Bitcoin ούτε απαιτεί την αναβάθμιση του, απλά προσθέτει στην υπάρχουσα τεχνολογία ένα επιπλέον επίπεδο-στρώμα(*layer*) πραγματοποίησης συναλλαγών εκτός του κύριου δικτύου, κάτι το οποίο θα μπορούσε να επιφέρει και μείωση στα τέλη συναλλαγών[170]. Έτσι το επιπλέον αυτό στρώμα διατηρεί τα ήδη υπάρχοντα επίπεδα ασφαλείας ενώ βελτιώνει την επεκτασιμότητα χωρίς να επιφέρει αλλαγές στο μέγεθος των μπλοκ. Βέβαια η μέγιστη ασφάλεια είναι όπως και στο γενικότερο μοντέλο του PoW αμφισβητούμενη, καθώς το Lightning Network είναι ευάλωτο σε τετριμμένες επιθέσεις όπως αυτές στο Bitcoin, με κλασσικό παράδειγμα την DDoS επίθεση τον Μάρτιο του 2018[171].
Ωστόσο παρά τις αρετές του το δίκτυο αυτό δέχεται αμφισβήτηση στην υλοποίηση συναλλαγών μεγαλύτερης αξίας και περιουσιακών στοιχείων, καθώς για την ώρα περιορίζεται σε μικροσυναλλαγές-μικροπληρωμές, και στο εύρος των εφαρμογών που μπορεί να καλύψει[172][173].

3.3.3.3. Plasma

Τον Αύγουστο του 2017 ο V.Buterin σε συνεργασία με τον συνιδρυτή του Bitcoin Lightning Network J.Poon παρουσίασαν το Plasma[174], μία layer-2 προσέγγιση στην τεχνολογία του Ethereum στηριζόμενη στην λογική του PoS και της λειτουργίας του MapReduce που θα υλοποιεί έξυπνες συμβάσεις ακολουθώντας ένα περισσότερο επεκτάσιμο και αποδοτικό πρωτόκολλο. Συγκεκριμένα μπορούμε να χαρακτηρίσουμε το Plasma ως ένα ιεραρχικό δέντρο αλυσίδων που έχει ως βάση-κύρια αλυσίδα(*root-parent chain*) το αρχικό δημόσιο δίκτυο του Ethereum και ως κλαδιά άλλες αλυσίδες(*child chains*) οι οποίες με τη σειρά τους μπορούν να περιλαμβάνουν επιπλέον παρακλάδια κοκ. Μπορούμε να φανταστούμε το ευρύτερο αυτό δίκτυο αλυσίδων ως ένα δίκτυο πολλών υποδεέστερων blockchain υποσυστημάτων μέσα σε

[10] https://www.stellar.org/blog/lightning-on-stellar-roadmap/

άλλα blockchain συστήματα τα οποία έχουν ως κέντρο ελέγχου το αρχικό δίκτυο. Η κάθε αλυσίδα επεξεργάζεται δεδομένα ανεξάρτητα από το υπόλοιπο δίκτυο στηριζόμενη στους δικούς της κανόνες και αρχές επιστρέφοντας περιστασιακά τις ολοκληρωμένες εργασίες στο κύριο δίκτυο, το οποίο θα χρειαστεί να "παρέμβει" για την αποκατάσταση της ομοφωνίας αν και εφόσον κάτι τέτοιο προκύψει. Έτσι το Plasma διαμοιράζει τον όγκο των δεδομένων σε όλο το δίκτυο των αλυσίδων με αποτέλεσμα να επιτυγχάνει περισσότερες συναλλαγές ανά δευτερόλεπτο και χαμηλότερα τέλη συναλλαγών[175], μεγιστοποίηση της αποδοτικότητας και της διαθεσιμότητας των δεδομένων στο δίκτυο και ταχύτερη εκτέλεση επιδρώντας καταλυτικά στην βελτίωση της επεκτασιμότητας. Επιπροσθέτως μιας και οι συναλλαγές ολοκληρώνονται στις αλυσίδες χωρίς να απαιτείται η έγκριση των miners, το Plasma επιβάλλει ποινές σε περιπτώσεις παραβίασης της ομοφωνίας.
Υπάρχουν βέβαια και κάποια στοιχεία προς βελτίωση στην υλοποίηση του Plasma[176]. Τα κυριότερα εξ' αυτών είναι: η περίπτωση εντοπισμού κατάστασης απάτης(*fraud proof*) σε ένα μπλοκ, οπότε και υπάρχει ο κίνδυνος μαζικής τάσης εξόδου των χρηστών από την αντίστοιχη αλυσίδα οδηγώντας σε πιθανότητα αποκλεισμού μέχρι και υποκλοπής των κεφαλαίων τους και το ερώτημα αν οι αλυσίδες(*child chains*) μπορούν να επιβιώσουν από την 51% επίθεση στην κύρια αλυσίδα(*parent chain*). Το πρωτόκολλο Plasma αν και ήδη συμπεριλαμβάνεται στη λειτουργία κάποιων συστημάτων όπως τα OmiseGo και Cosmos/Polkadot βρίσκεται για την ώρα σε πρώιμο στάδιο.



Εικόνα 10- Σχηματική απεικόνιση της λειτουργίας του Plasma[174]

Συνδυάζοντας τα οφέλη των Plasma και Lightning Network ενδιαφέρον παρουσιάζει η προοπτική ενός συνδυασμένου συστήματος των δύο πρωτοκόλλων στο οποίο το Lightning Network θα ολοκληρώνει τις συναλλαγές ενώ το Plasma θα ασχολείται με την επικύρωση του συστήματος.

3.3.3.4. Raiden

Το Raiden Network[177] αποτελεί την αντίστοιχη εκδοχή του Ethereum για το Lightning Network του Bitcoin: ένα off-chain πρωτόκολλο που στηρίζει την λειτουργία του σε ένα δίκτυο-κανάλι συναλλαγών. Η κύρια διαφορά του με το Lightning Network έγκειται στο γεγονός πως ενώ το Lightning Network στηρίζει τη λειτουργία του στην αποκλειστική ολοκλήρωση πληρωμών στο Bitcoin, το Raiden είναι συμβατό με οποιοδήποτε ERC20 συμβατό token. Το δίκτυο αυτό παρέχει άμεσες off-chain συναλλαγές ,απαλλαγμένες από τα on-chain gas τέλη και είναι ωφέλιμο για συναλλαγές μικρότερης αξίας.
Λόγω της πολυπλοκότητας του το Raiden δεν είναι άμεσα εφαρμόσιμο αλλά μπορεί να αποτελέσει τη βάση για τη λειτουργία παράπλευρων συστημάτων[178] όπως το Trinity[179].
Τα δίκτυα Plasma και Raiden θα μπορούσαν να συνδυαστούν έχοντας ως αποτέλεσμα ένα ακόμα πιο βέλτιστο δίκτυο στην κορυφή του Ethereum blockchain, όπου σε πρώτο στάδιο το Plasma θα ασχολείται με τη διαχείριση των έξυπνων συμβάσεων ενώ στη συνέχεια το Raiden θα ολοκληρώνει τις επικείμενες συναλλαγές.
Παρακάτω παρουσιάζουμε το συγκριτικό Πίνακα 5 των παραπάνω μεθόδων επεκτασιμότητας στον οποίο χρησιμοποιούμε ως μέθοδο σύγκρισης μία κλίμακα από το 1 έως το 3.
Θεωρούμε το Lightning Network το σύστημα με τον μεγαλύτερο βαθμό ασφάλειας, καθώς στηρίζεται στο πρωτόκολλο του PoW ακολουθώντας τη δοκιμασμένη λογική του Bitcoin, ενώ το Raiden έχει το μεγαλύτερο βαθμό πολυπλοκότητας και για το λόγο αυτό δεν έχει εφαρμοστεί αυτό καθαυτό στην blockckain κοινότητα. Όσον αφορά τον βαθμό ιδιωτικότητας όλες οι παραπάνω μέθοδοι χρειάζονται βελτίωση ώστε να εξασφαλίζουν μεγαλύτερα επίπεδα από τα ήδη υπάρχοντα blockchain συστήματα. Για την ελάττωση του κόστους το Raiden υπερτερεί όλων, ενώ τοποθετήσαμε το Lightning Network τελευταίο σε αυτόν τον τομέα, καθώς αν και εξασφαλίζει χαμηλότερα τέλη συναλλαγών μέσω της off-chain διαδικασίας τα χρηματικά ποσά που απαιτούνται για να διατηρείται η λειτουργικότητα του συστήματος είναι τεράστια[180]. Όσον αφορά τη βελτίωση των χρονικών καθυστερήσεων το Raiden υπόσχεται να είναι η καλύτερη επιλογή, αλλά αυτό θα φανεί μεταγενέστερα και όταν έχουμε πρακτικά παραδείγματα πλήρους εφαρμογής του.

Πίνακας 5-Συγκριτική ανάλυση μεθόδων συναλλαγών εκτός αλυσίδας

	Ασφάλεια	**Πολυπλοκότητα**	**Ιδιωτικότητα**	**Εφαρμοσιμότητα**	**Ελάττωση κόστους**	**Καθυστερήσεις**
Pegged Sidechains	1	2	2	2	2	2
Lightning Network	2	1	2	3	1	2
Plasma	1	1	2	2	2	2
Raiden	2	3	2	1	3	1

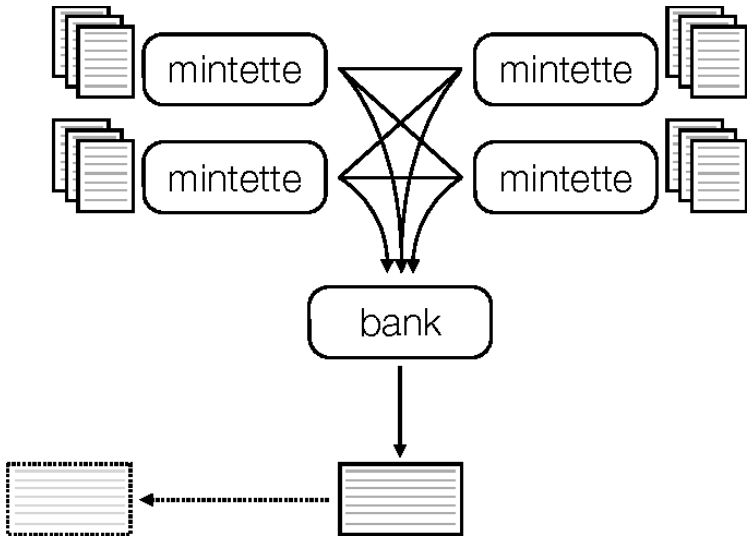
1:ελάχιστος βαθμός 2:ενδιάμεσος βαθμός 3:μέγιστος βαθμός

3.3.4.Υβριδικά συστήματα με την τεχνική κοπής(sharding)

Το sharding είναι εδώ και χρόνια μια ευρέως εφαρμοζόμενη τεχνική στα συστήματα βάσεων δεδομένων και στο cloud computing[181] [182]. Ωστόσο η χρήση της στον τομέα της τεχνολογίας blockchain διαφέρει αρκετά. Η ειδοποιός διαφορά του sharding με τα off-chain συστήματα που περιγράψαμε παραπάνω είναι πολύ απλή: το sharding αποτελεί μία layer-1 τεχνική, όπως υποστηρίζει και ο V. Buterin[183], καθώς οι συναλλαγές πραγματοποιούνται στο αρχικό σύστημα και όχι σε κανάλια η άλλες αλυσίδες. Το sharding, που είναι γνωστό στην blockchain κοινότητα ως μία πρόταση βελτίωσης του Ethereum blockchain[184], αποτελεί μία ιδιαίτερη προοπτική για την επεκτασιμότητα και η λογική είναι η εξής: το δίκτυο διαιρείται σε πολλές μικρότερες ομάδες-τμήματα χρηστών(*shards*), καθένα από τα οποία περιλαμβάνει και διαχειρίζεται ένα μέρος των συνολικών συναλλαγών αποδεσμεύοντας έτσι το σύστημα από τον εγγενή περιορισμό ότι όλοι πρέπει να γνωρίζουν και να επαληθεύουν το ιστορικό των συναλλαγών. Κάθε shard χωρίζεται σε μικρές ομάδες(*collations*) χρηστών(*collators*). Κάθε ομάδα από αυτές διαχειρίζεται το δικό της μερίδιο του συνολικού blockchain ανεξάρτητα από το υπόλοιπο δίκτυο. Ανά χρονικά διαστήματα τα ολοκληρωμένα δεδομένα των collations του κάθε shard συγκεντρώνονται σε ένα μπλοκ στην κύρια αλυσίδα. Έτσι η τεχνική sharding παρέχει στο σύστημα την παράλληλη ολοκλήρωση των συναλλαγών οδηγώντας την επεκτασιμότητα σε νέους ορίζοντες βελτιώνοντας τη διακίνηση και αυξάνοντας τον αριθμό των συναλλαγών ανά δευτερόλεπτο ταυτόχρονα με την αύξηση του δικτύου.
Παρακάτω θα δούμε κάποια συστήματα τα οποία χαρακτηρίζουμε υβριδικά καθώς στηρίζουν τη λειτουργία τους στην τεχνική κοπής που περιγράψαμε παραπάνω σε συνδυασμό με άλλες κλασσικές τεχνικές, όπως PoW και BFT :

3.3.4.1. RSCoin[185]

Το RSCoin αποτελεί ένα πρωτόκολλο που αποσκοπεί στην βελτίωση της επεκτασιμότητας της λειτουργίας συγκεντρωτικών συστημάτων που διαχειρίζονται κρυπτονομίσματα. Στηριζόμενο στο sharding χρησιμοποιεί μία κατανεμημένη μορφή χρηστών επικύρωσης(*mintettes*) με σκοπό να προσδώσει στον συγκεντρωτικό χαρακτήρα των τραπεζικών συστημάτων έναν αυξημένο βαθμό διαφάνειας.
Βέβαια η δομή αυτή καθεαυτή αντικρούει απευθείας αυτήν την προσπάθεια μετρίασης του συγκεντρωτισμού, ενώ το πρωτόκολλο δέσμευσης δύο φάσεων(*two-phase commit protocol*) που εφαρμόζεται στα shards καθιστά το RSCoin πρωτόκολλο μη ανεκτικό στις Βυζαντινές βλάβες ενισχύοντας τον κίνδυνο εμφάνισης απειλών τύπου double-spending και denial-of-service(DoS).



Εικόνα 11-Η δομή του RScoin[185]

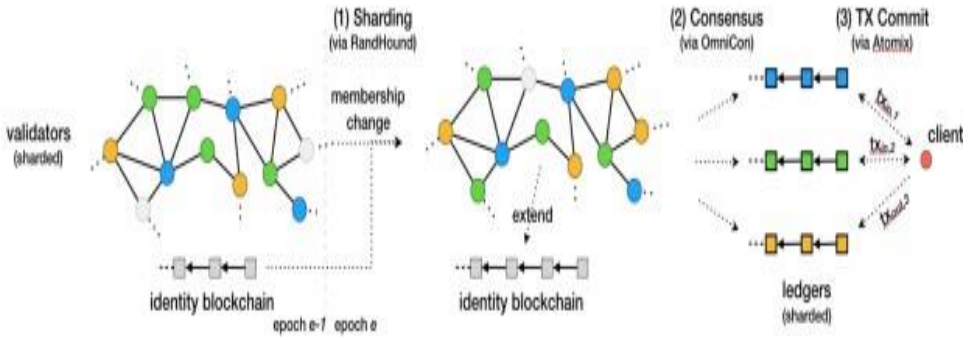
3.3.4.2. Elastico[173]

Σύμφωνα με τη βιβλιογραφία συνιστά το πρώτο πρωτόκολλο που στηρίζεται στο sharding και αφορά τα δημόσια blockchain συστήματα. Ακολουθώντας τη PoW λογική για την επίτευξη ομοφωνίας και μέσω επιτροπών χρηστών(*committees*) πετυχαίνει μία γραμμική αύξηση των συναλλαγών με την δαπανόμενη υπολογιστική ισχύ, ενώ χρησιμοποιεί την PBFT λογική για την αντιμετώπιση των Βυζαντινών σφαλμάτων. Έτσι συνδυάζοντας τις τεχνικές των PoW, PBFT και sharding αυξάνει την επεκτασιμότητα του συστήματος βελτιώνοντας τη διακίνηση και το σύνολο των συναλλαγών.
Βέβαια χαρακτηρίζεται και από κάποια αξιοσημείωτα μειονεκτήματα. Για παράδειγμα με την εφαρμογή του PBFT αλγορίθμου παρέχει μεν 25% προστασία

απέναντι σε Βυζαντινές απειλές αλλά περιορίζεται σε επιτροπές μικρού εύρους(ιδανικά 100) μετριάζοντας την ασφάλεια του συστήματος. Ακόμα με την αύξηση του δικτύου έστω και κατά μερικές εκατοντάδες χρηστών παρατηρείται ταυτόχρονα γραμμική αύξηση στο κόστος και τετραγωνική αύξηση των χρονικών καθυστερήσεων καθιστώντας τη χρήση του PBFT αναποτελεσματική. Να τονίσουμε ότι σύμφωνα με πειραματικά αποτελέσματα τα παραπάνω ισχύουν στο Elastico υπό την προυπόθεση ότι δεν υπάρχουν κακόβουλοι χρήστες. Επίσης ενώ μέσω του sharding η ολοκλήρωση των συναλλαγών διαμοιράζεται στο σύστημα, κάθε χρήστης οφείλει να μεταδίδει τις συναλλαγές του σε ολόκληρο το δίκτυο αποθηκεύοντας παράλληλα το πλήρες ιστορικό. Τέλος ο συνδυασμός της χρήσης PoW αλγορίθμου με τον επαναπροσδιορισμό των επιτροπών σε κάθε κύκλο ομοφωνίας(*epoch*) επιβραδύνουν σε ένα βαθμό τη λειτουργικότητα.

3.3.4.3. Omniledger[186]

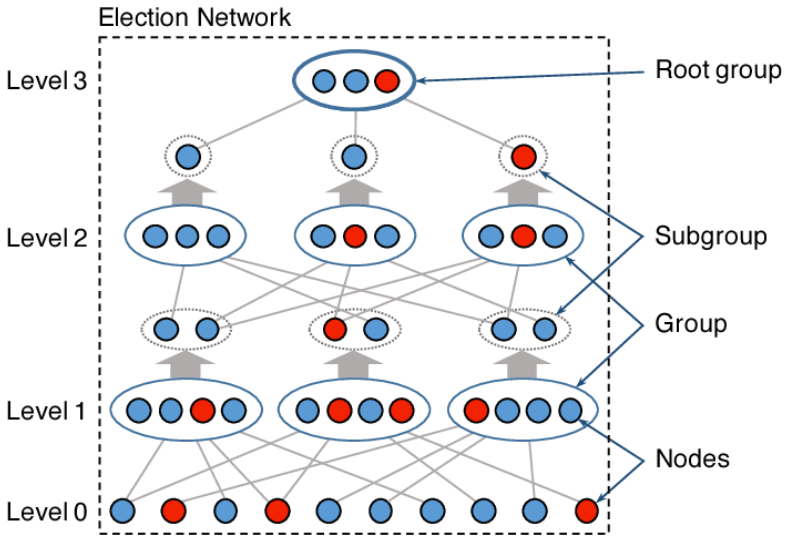
Αποτελεί μία βελτιωμένη έκδοση του Elastico εξασφαλίζοντας μεγαλύτερα επίπεδα ασφάλειας απέναντι στις Βυζαντινές απειλές και μεγάλη επεκτασιμότητα με μικρές καθυστερήσεις, διατηρώντας παράλληλα έναν πλήρη αποκεντρωτικό χαρακτήρα. Τα υψηλά επίπεδα ασφάλειας επιτυγχάνονται με την επέκλυση διαχωριζόμενης τυχαίας ανθεκτικότητας(*scalable bias-resistant distributed randomness*) [187]. Μέσω ενός πρωτοκόλλου αναδιαμόρφωσης το Omniledger αναδιαμορφώνει περιοδικά τις επιτροπές χρηστών(*committees*) διασφαλίζοντας την ακεραιότητα και την αποφυγή παραβιάσεων.
Ωστόσο το Omniledger περιλαμβάνει την εφαρμογή της cross-sharding τεχνικής, που χαρακτηρίζεται από μεγάλο βαθμό πολυπλοκότητας, ενώ δεν είναι πλήρως ανθεκτικό σε επιθέσεις τύπου DoS λόγω του ατομικού πρωτοκόλλου δέσμευσης(*atomic commit protocol*) που χρησιμοποιείται για τη διακίνηση των συναλλαγών μεταξύ των επιτροπών.



Εικόνα 12-Αρχιτεκτονική επισκόπηση του Omniledger[186]

3.3.4.4. RapidChain[188]

Το RapidChain αποτελεί μία πρόσφατη εκδοχή των sharding blockchains και είναι το πρώτο sharding πρωτόκολλο που αυξάνει την ασφάλεια έναντι στα Βυζαντινά σφάλματα στο 33%. Το σύστημα ακολουθεί ένα ενδοεπιχειρησιακό πρωτόκολλο συναίνεσης(*intra-committee consensus protocol*) για να πετύχει ομοφωνία και σε συνδυασμό με ένα pipelining πρωτόκολλο βελτιώνει τη διακίνηση των συναλλαγών στο σύστημα. Με τη χρήση μίας cross-shard τεχνικής για την επιβεβαίωση των συναλλαγών το RapidChain αντιμετωπίζει το πρόβλημα των gossiping transactions που χαρακτηρίζει το Omniledger, ενώ σε αντίθεση με όλα τα παραπάνω sharding συστήματα περιλαμβάνει ένα στάδιο αναδιαμόρφωσης όπου με τη βοήθεια του κανόνα του Κούκου[189] προστατεύει το σύστημα ενάντια σε έναν βραδείας προσαρμογής Βυζαντινό αντίπαλο.



Εικόνα 13-Το δίκτυο εκλογής του RapidChain[188]

Πίνακας 6-Σύγκριση των συστημάτων που χρησιμοποιούν το sharding

	Δοκιμασμένο μέγεθος δικτύου (αριθμός χρηστών)	**Συναλλαγές ανά δευτερόλεπτο**	**Χρονικές καθυστερήσεις(σε sec)**	**Βυζαντινή ανεκτικότητα (στο σύνολο του δικτύου)**	**Ασφάλεια-Αποκέντρωση-Επεκτασιμότητα[11]**
RSCoin	30	Περίπου 2000	1	1/4	Ε>ΑΣ>ΑΠ
Elastico	1600	40	800	1/4	Ε=ΑΠ>ΑΣ
Omniledger	1800(μέχρι και 2400)	3500	63	1/4	Ε=ΑΠ>ΑΣ
RapidChain	4000	7384	8.7	1/3	Ε=ΑΠ=ΑΣ

3.3.5.Blockchain 3.0

Λόγω της συνεχούς εξέλιξής της η τεχνολογία blockchain δεν συναντάται πλέον μόνο στον τομέα των ψηφιακών συναλλαγών μέσω κρυπτονομισμάτων, αλλά εκτείνεται σε ένα τεράστιο φάσμα εφαρμογών. Για το λόγω αυτό συχνά συναντάμε στη βιβλιογραφία τον διαχωρισμό των blockchain σε τρεις γενιές[190][191], ενώ ένας πιο ξεκάθαρος διαχωρισμός με συγκεκριμένα παραδείγματα και ορισμούς παρουσιάστηκε από την M.Swan[192]. Παρακάτω προσδιορίζουμε τις τρεις γενιές των blockchain συστημάτων :

1. **Blockchain 1.0**: η χρήση των κρυπτονομισμάτων, όπως το Bitcoin και άλλα απλά altcoins (πχ Litecoin), για την αποκέντρωση, τις ψηφιακές συναλλαγές, το ιδιωτικό απόρρητο και την ασφάλεια των χρηματικών συναλλαγών. Ωστόσο η γενιά αυτή των blockchain συστημάτων αντιμετωπίζει στις μέρες μας έντονη αμφισβήτηση και πολλά προβλήματα τα κυριότερα από τα οποία αφορούν τα επίπεδα ασφάλειας, αποκέντρωσης, λειτουργικότητας και επεκτασιμότητας.
2. **Blockchain 2.0**: θεωρείται η αποκέντρωση της ευρύτερης οικονομίας, καθώς αποτελεί μια πιο πλήρη-αναβαθμισμένη εκδοχή του Blockchain 1.0 συμπεριλαμβάνοντας τις έξυπνες συμβάσεις(μέσω του Ethereum), οι οποίες έφεραν ένα εντελώς νέο επίπεδο τάξης και πρακτικότητας σε ένα ευρύ φάσμα εφαρμογών, και επιτρέποντας τη λειτουργία στις αποκεντρωμένες εφαρμογές(DApps) και στους αποκεντρωμένους αυτόνομους οργανισμούς(DAOs), οι οποίοι μπορούν να οριστούν ως δίκτυα αυτόνομων μονάδων αποκεντρωτικού χαρακτήρα που στηρίζονται σε μία παραγωγική διαδικασία μεγιστοποίησης της απόδοσης(Peters et al., 2018).. Επίσης για την ώρα τα Blockchain 2.0 συστήματα χρησιμοποιούνται σε ένα πολύ μεγαλύτερο πλήθος εφαρμογών συγκριτικά με τα Blockchain 1.0 και Blockchain 3.0 συστήματα(Kane, 2017).
3. **Blockchain 3.0**: το σύνολο των blockchain εφαρμογών πέρα από τα κρυπτονομίσματα, τη χρηματοδότηση και τις αγορές που εκτείνονται σε νέους

[11] Παρέχουμε για κάθε μέθοδο μία σύγκριση προτεραιότητας μεταξύ τριών βασικών εννοιών: ασφάλεια(ΑΣ), αποκέντρωση(ΑΠ) και επεκτασιμότητα(Ε).

τομείς, όπως οι τομείς της κυβέρνησης, της επιστήμης, της υγείας και της παιδείας[193][194][195],της ενέργειας[196], της φαρμακευτικής βιομηχανίας και των βιβλιοθηκών[197], της κατασκευαστικής βιομηχανίας[198], της βελτίωσης του εκπαιδευτικού συστήματος[199], της νομικής μετρολογίας[200], της διαχείρισης αλυσίδων εφοδιασμού(*supply chain management*)[201], των κτηματολογικών και μεσιτικών γραφείων[202] αλλά και τους τομείς της τέχνης, του πολιτισμού κ.ά. Επίσης τα Blockchain 3.0 συστήματα θα μπορούσαν να ξεπεράσουν τα προβλήματα εφαρμογής της υπάρχουσας blockchain τεχνολογίας στα τραπεζικά συστήματα[203]. Ακόμα η Blockchain 3.0 τεχνολογία δίνει ακόμα μεγαλύτερη έμφαση στους αποκεντρωμένους αυτόνομους οργανισμούς(*DAOs*) και μπορεί να χρησιμοποιηθεί στον τομέα του Internet of Things(*IoT*)[204][205]. Συνεπώς αυτά τα τρίτης γενιάς συστήματα αποτελούν μία γέφυρα της blockchain τεχνολογίας, και γενικότερα της DLT(*distributed ledger technology*) λογικής, με τον φυσικό κόσμο που περιλαμβάνει τόσο το δημόσιο όσο και τον ιδιωτικό τομέα.

Οι μέθοδοι που έχουμε αναλύσει παραπάνω είναι μέθοδοι που θα μπορούσαν να ανήκουν και στις τρεις γενιές των blockchain, ανάλογα την περίπτωση. Ωστόσο έχουμε ταξινομήσει τις παραπάνω μεθόδους με βάση κάποια κοινά χαρακτηριστικά που παρουσιάζουν. Παρακάτω θα αναφέρουμε μερικές ενδιαφέρουσες περιπτώσεις blockchain που ανήκουν αποκλειστικά στην τρίτη γενιά με διαφορετικά χαρακτηριστικά και τρόπο λειτουργίας για να κατανοήσουμε πως μπορούν να συντελέσουν δραστικά στο πρόβλημα της επεκτασιμότητας:

3.3.5.1. EOS.IO-συναλλαγές με DPoS

Το λογισμικό EOS.IO[41] εισάγει μια νέα αρχιτεκτονική blockchain σχεδιασμένη να επιτρέπει την κάθετη και οριζόντια κλιμάκωση αποκεντρωμένων εφαρμογών στηρίζοντας τη λειτουργία του στο DPoS, όπως αναφέρουμε και στην Ενότητα 2.2.1, αλλά και στην BFT λογική, επιτρέποντας τις αποκεντρωμένες εφαρμογές(*Decentralized applications-DApps*) και εξαλείφοντας τα συναλλακτικά τέλη[206]. Το BFT μοντέλο εξασφαλίζει διαφάνεια και προστασία από τις Βυζαντινές απειλές, ενώ το DPoS μοντέλο αποτελεί το ταχύτερο, πιο αποτελεσματικό, πιο αποκεντρωμένο και πιο ευέλικτο μοντέλο συναίνεσης σύμφωνα με το Bitshares[207]. Στο DPoS η διαδικασία εξόρυξης της PoW και PoS λογικής αντικαθίσταται από μία νέα λειτουργία επίτευξης ομοφωνίας και ολοκλήρωσης συναλλαγών κατά την οποία οι stakeholders, όπως στο PoS, ψηφίζουν άλλους χρήστες(*witnesses*) οι οποίοι έχουν την αποκλειστική ευθύνη της δημιουργίας των μπλοκ. Παρόμοια επιλέγονται άλλοι χρήστες(*delegates*) οι οποίοι είναι υπεύθυνοι για τη διατήρηση του δικτύου, ενώ έχουν και τη δυνατότητα να προτείνουν αλλαγές σε αυτό. Μέσω του DPoS ο χρόνος επιβεβαίωσης των συναλλαγών μειώνεται δραστικά με αποτέλεσμα να ολοκληρώνονται πολύ περισσότερες συναλλαγές σε πολύ λιγότερο χρόνο. Τελικά το blockchain λειτουργεί ταχύτερα ενώ οι χρόνοι καθυστέρησης και ολοκλήρωσης των συναλλαγών μειώνονται καθώς η λήψη αποφάσεων είναι υπόθεση λίγων ατόμων και όχι ολόκληρου του δικτύου, όπως στο PoW. Βέβαια για την επίτευξη υψηλών επιπέδων επεκτασιμότητας το EOS.IO δίνει μικρότερη προτεραιότητα στην

αποκέντρωση καθώς για την ώρα περιλαμβάνει μόνο 21 χρήστες για την παραγωγή μπλοκ ανά διάστημα(*epoch*), αλλά αυτό έχει μικρή σημασία συγκριτικά με τους εξαιρετικούς δείκτες επεκτασιμότητας του όπως δημιουργία μπλοκ ανά 0.5-3 δευτερόλεπτα και άμεσος χρόνος επιβεβαίωσης συναλλαγών, ενώ αναμένεται να ξεπεράσει τις 50000 συναλλαγές ανά δευτερόλεπτο[208]. Εδώ αξίζει να σκεφτούμε πως αυτές οι συναλλαγές επιτυγχάνονται μόνο με 21 χρήστες-δημιουργούς, οπότε το EOS.IO μπορεί να φτάσει ακόμη μεγαλύτερα πρωτόγνωρα νούμερα, ενώ το φθινόπωρο του 2018 αναμένεται να ενσωματωθούν στο EOS.IO τεχνικές παραλληλισμού[209] που θα αυξήσουν ακόμα περισσότερο την επεκτασιμότητά του.

3.3.5.2. Zilliqa

Στηριζόμενη στο Elastico που περιγράψαμε στην Υποενότητα 3.3.4.2 μια ομάδα ερευνητών του εθνικού πανεπιστημίου της Σιγκαπούρης ανέπτυξαν την blockchain πλατφόρμα Zilliqa[210], την οποία οι ίδιοι αποκαλούν πλατφόρμα επόμενης γενιάς. Αποτελεί την πρώτη blockchain πλατφόρμα που στηρίζει τη λειτουργία της στην τεχνική της κοπής(*sharding*), την οποία έχουμε περιγράψει παραπάνω, με σκοπό να εξαλείψει τα προβλήματα επεκτασιμότητας που αντιμετωπίζουν όλα τα blockchain συστήματα. Στηρίζεται στην εφαρμογή τόσο του PoW όσο και του PBFT αλγορίθμου για την εγγύηση της ασφάλειας και της διατήρησης της αποκέντρωσης και στοχεύει στην αύξηση των συναλλαγών παράλληλα με το μέγεθος του δικτύου. Ακόμα δημιουργεί μία γλώσσα έξυπνων συμβάσεων η οποία, αν και δεν είναι πλήρως συμβατή με την Turing-machine λογική, επιτρέπει την επεκτασιμότητα και είναι ιδανική για εναλλακτικές εφαρμογές όπως η ψηφιακή διαφήμιση, οι αυτοματοποιημένες δημοπρασίες και γενικότερα οποιαδήποτε MapReduce εργασία. Σύμφωνα με πειραματικά αποτελέσματα προς τα τέλη του 2017[211] η πλατφόρμα Zilliqa κατέγραψε 1389 συναλλαγές ανά δευτερόλεπτο με 2400 χρήστες σε 4 shards και αργότερα 2488 συναλλαγές ανά δευτερόλεπτο με 3600 χρήστες σε 6 shards, ενώ όπως ισχυρίζονται οι ίδιοι οι δημιουργοί της, αν έφταναν έναν αριθμό χρηστών ισάξιο με αυτόν του Ethereum θα μπορούσαν να αγγίξουν τις 15000 συναλλαγές ανά δευτερόλεπτο. Η δοκιμαστική πλατφόρμα βρίσκεται σε δημόσια λειτουργία με τη διακίνηση να αυξάνεται σχεδόν γραμμικά με την αύξηση των χρηστών σημειώνοντας πάνω από 2800 συναλλαγές ανά δευτερόλεπτο[212].

3.3.5.3. Cosmos

Το Cosmos[213] είναι ένα blockchain σύστημα που προάγει την πρωτότυπη αρχιτεκτονική ενός δικτύου πολλαπλών και ανεξάρτητων blockchain. Η αρχιτεκτονική αυτή βασίζεται στο συνδυασμό των λειτουργιών των Tendermint Core[214], Hubs and Zones και IBC(*Inter-blockchain Communication-IBC*) πρωτοκόλλου. Πιο συγκεκριμένα το Cosmos αποτελείται από ένα κύριο blockchain(*Hub*) το οποίο συνδέεται με διάφορα άλλα blockchains(*Zones*). Η λειτουργία των παραπάνω βασίζεται στη λογική του Tendermint Core, το οποίο

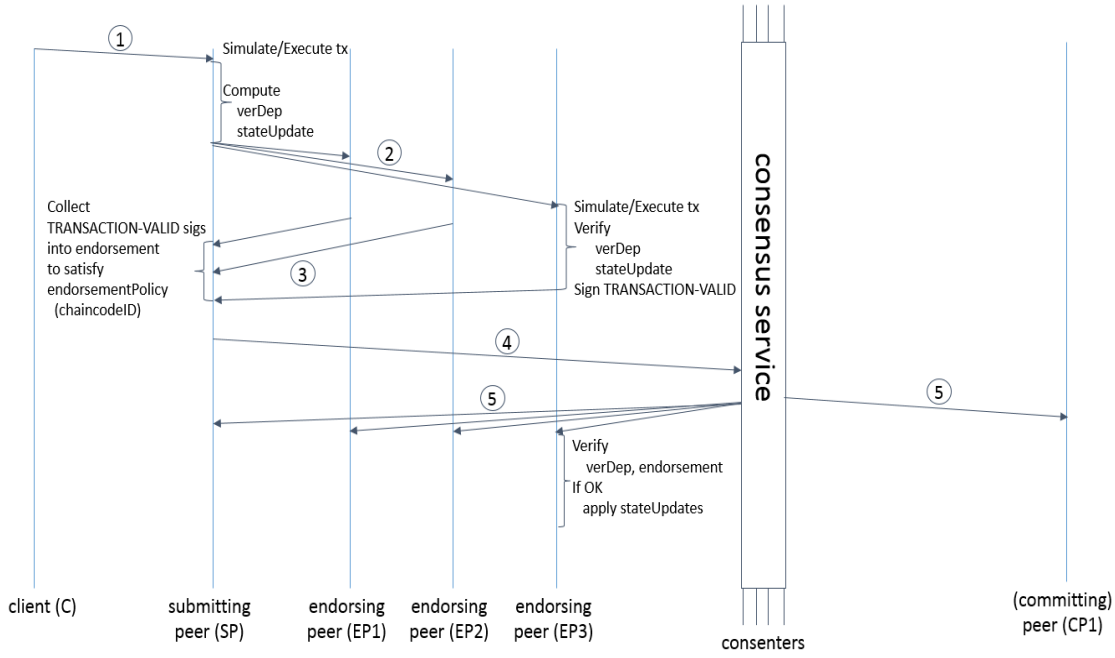
αποτελεί ένα συνεκτικό πρωτόκολλο βασισμένο σε PBFT μηχανισμούς επίτευξης ομοφωνίας. Με τη βοήθεια του IBC πρωτοκόλλου το Cosmos επιτρέπει τις συναλλαγές περιουσιακών στοιχείων μεταξύ διαφορετικών blockchain συστημάτων, υπό την επίβλεψη ενός δημόσιου, κεντρικού, αναβαθμίσιμου και προσαρμόσιμου PoS blockchain συστήματος. Το ενδιαφέρον κομμάτι της όλης λογικής είναι ότι το Cosmos δεν περιορίζεται στην προσαρμογή blockchain συστημάτων στηριζόμενων αποκλειστικά στο Tendermint Core, αλλά οποιουδήποτε blockchain: τα blockchain συστήματα με άμεση οριστικότητα συνδέονται στο Cosmos μέσω του IBC, ενώ εκείνα με πιθανολογική οριστικότητα συνδέονται με μια πιο σύνθετη διαδικασία με τη βοήθεια των *Peg-Zones*. Έτσι το Cosmos επιτυγχάνει τη διαλειτουργικότητα μεταξύ πολλών παράλληλων blockchain συστημάτων τα οποία μπορούν να συναλλάσσονται μεταξύ τους διατηρώντας την ταυτότητα και τα δομικά λειτουργικά χαρακτηριστικά τους. Τα επίπεδα επεκτασιμότητας ενισχύονται από το γεγονός ότι το Cosmos αρχικά θα λειτουργήσει παρέχοντας κλασσική κατακόρυφη επεκτασιμότητα(*vertical scalability*), ενώ αργότερα θα υλοποιήσει τεχνικές πολλαπλών αλυσίδων(*multi-chain*) προσφέροντας οριζόντια επεκτασιμότητα(*horizontal scalability*). Αν και λόγω της λειτουργίας του Tendermint Core το Cosmos χαρακτηρίζεται από περιορισμένο αριθμό χρηστών(100-300), καθώς μεγάλος αριθμός χρηστών σημαίνει περιορισμένη απόδοση, μπορεί να παρέχει χιλιάδες συναλλαγές ανά δευτερόλεπτο(περίπου 4000 με 64 χρήστες) και χρονικές καθυστερήσεις της τάξης των 1-2 δευτερολέπτων.

3.3.5.4. Hedera Hashgraph

Το Hedera Hashgraph[215] αποτελεί μία μορφή διανεμημένης τεχνολογίας η οποία προσφέρει μία εντελώς διαφορετική αρχιτεκτονική συγκριτικά με τα συνήθη blockchain συστήματα. Αντί των διαδεδομένων PoW, PoS και layer-2 μηχανισμών διατηρεί μία ασύγχρονη BFT λογική και βασίζεται στη δομή και λειτουργία του Hashgraph αλγορίθμου[216], ενώ λειτουργεί ως ιδιωτικό blockchain θυσιάζοντας την αποκέντρωση προς όφελος της μεγιστοποίησης της ασφάλειας και της επεκτασιμότητας. Ο μηχανισμός ομοφωνίας αποτελεί το συνδυασμό ενός εικονικού αλγορίθμου ψηφοφορίας(*virtual voting algorithm*) και ενός πρωτοκόλλου κουτσομπολιού(*gossip protocol*). Ο παραπάνω επαναστατικός συνδυασμός επιτρέπει στο σύστημα βέλτιστα επίπεδα ταχύτητας τόσο στη διακίνηση των δεδομένων όσο και στην επίτευξη ομοφωνίας. Αυτό επιτυγχάνεται καθώς η γραμμική σύνδεση των μπλοκ που συναντάται στα κλασσικά blockchain συστήματα αντικαθίσταται από συνδέσεις τύπου πλευρικών αλυσίδων ενώ μέσω του πρωτοκόλλου κουτσομπολιού τα δεδομένα διακινούνται ταυτόχρονα μεταξύ πολλαπλών χρηστών. Επίσης το Hedera Hashgraph παρέχει προστασία έναντι της εμφάνισης forks και είναι σχετικά φθηνό, καθώς είναι αποδεσμευμένο από την PoW εξόρυξη. Σύμφωνα με πειραματικά αποτελέσματα το Hedera Hashgraph αυξάνει τις συναλλαγές ανά δευτερόλεπτο σε νούμερα της τάξης του μισού εκατομμυρίου, ενώ οι χρονικές καθυστερήσεις δεν ξεπερνούν τα 11 δευτερόλεπτα, φτάνοντας ακόμα και κάτω από τα 0.04 δευτερόλεπτα. Βέβαια τα παραπάνω εντυπωσιακά αριθμητικά δεδομένα δεν είναι παρά μόνο πειραματικά αποτελέσματα, αλλά ο επαναστατικός χαρακτήρας της τεχνολογίας μας αφήνει ενθαρρυντικά στοιχεία για την πρακτική τους μελλοντική υλοποίηση.

3.3.5.5. Hyperledger Fabric

Το Hyperledger Fabric[217] είναι ένα αρθρωτό σύστημα γενικού σκοπού και αποτελεί μία ιδιωτική πλατφόρμα στηριζόμενη στις αρχές της blockchain τεχνολογίας. Η πλατφόρμα αυτή είναι μέρος του συνόλου των Hyperledger προγραμμάτων της Linux Foundation και οι πρώτες εκδόσεις, Hyperledger Fabric v0.5 και v0.6, κυκλοφόρησαν το 2016. Οι πρώιμες αυτές εκδόσεις, αν και πολλά υποσχόμενες, υλοποιούν μία state-machine αρχιτεκτονική[217] και περιλαμβάνουν πολλούς από τους εγγενείς σχεδιαστικούς περιορισμούς που χαρακτηρίζουν τα ιδιωτικά blockchain συστήματα[218], γεγονός που οδήγησε σε μία ανανεωμένη εκδοχή, το Hyperledger Fabric v1.0, η οποία σχεδιάστηκε για να παρέχει ακόμα υψηλότερα επίπεδα απόδοσης και μεταξύ άλλων επεκτασιμότητας και για να εξαλείψει τους υπάρχοντες περιορισμούς[219]. Σε αντίθεση με πολλά blockchain συστήματα που διαθέτουν ένα συναλλακτικό μοντέλο παραγγελίας-εκτέλεσης, το Hyperledger Fabric χρησιμοποιεί ένα συνδυαστικό προσομοιωτικό μοντέλο παραγγελίας-επικύρωσης-δέσμευσης, όπως φαίνεται και από την παρακάτω εικόνα, ενώ συγκρινόμενο με άλλες blockchain πλατφόρμες παρουσιάζει αρκετές διαφοροποιήσεις που αναδεικνύουν την χρησιμότητά του στην εφαρμογή της blockchain τεχνολογίας[220][221]. Βασικά χαρακτηριστικά του Hyperledger Fabric είναι η λειτουργία έξυπνων συμβάσεων(*chaincodes*[222]),οι οποίες υλοποιούνται στις γλώσσες Go/JAVA/Nodejs, καθώς και μία πολύπλευρη διαδικασία ομοφωνίας(*pluggable consensus protocol*), όπου ανάλογα με τις ανάγκες και απαιτήσεις της εκάστοτε εφαρμογής μπορούν να χρησιμοποιηθούν διάφορα αλγοριθμικά μοντέλα. Ακόμα υπάρχει μία πολυδιάστατη διανομή ρόλων στους χρήστες , οι οποίοι διακρίνονται σε clients, endorsing peers, committing peers, validators και orderers. Αν και ο καθένας από τους παραπάνω επιτελεί διαφορετικό ρόλο στην πλατφόρμα, το έργο και η εκτελεστική τους λειτουργία συνδυάζονται με σκοπό την βελτιστοποίηση του συνολικού συστήματος. Τα σημαντικά επίπεδα διακίνησης και επεκτασιμότητας φανερώνονται στα πειραματικά αποτελέσματα που διεξήχθησαν στις πλατφόρμες v1.0 και v1.1: στο Hyperledger Fabric v1.0(Thakkar, Nathan, & Vishwanathan, 2018a) παρουσιάστηκαν τρεις απλές βελτιστοποιήσεις οι οποίες οδήγησαν επίτευξη δεκαεξαπλάσιας απόδοσης, καταγράφοντας 2250 συναλλαγές ανά δευτερόλεπτο, ενώ στο Hyperledger Fabric v1.1(Androulaki et al., 2018) επιτεύχθηκαν πάνω από 3560 συναλλαγές ανά δευτερόλεπτο.



Εικόνα 14-Διάγραμμα ροής των συναλλαγών στο Hyperledger Fabric v1.0[223]

Βέβαια υπάρχουν και άλλα συστήματα τρίτης γενιάς που υπόσχονται νέα επίπεδα επεκτασιμότητας, κάποια από τα οποία αξίζει να αναφέρουμε παρακάτω: το Aion Network[224] αποτελεί μία μορφή πολυεπίπεδου blockchain(*multi-tier blockchain*) που επιτρέπει την cross-chain επικοινωνία τόσο σε δημόσιο όσο και σε ιδιωτικό επίπεδο. Το πρωτόκολλο IOTA[225] αποτελεί μία εναλλακτική προσέγγιση καθώς επιχειρεί την βελτίωση της επεκτασιμότητας και άλλων σημαντικών παραμέτρων στον τομέα του IoT(*Internet of Things*) μέσω της εφαρμογής του Tangle[226][227], ενός άμεσου κυκλικού γραφήματος(*Directed Acyclic Graph*)[228] που διαφέρει σημαντικά από την κλασσική blockchain τεχνολογία[229]. Το Cardano είναι ένα ανοιχτού κώδικα, αποκεντρωμένο, και δημόσιο blockchain σύστημα που αντικαθιστά το PoW με το Ouroboros[38], ένα σύγχρονο PoS πρωτόκολλο, αλλά και βελτιωμένες εκδοχές αυτού[230]. Αν και η επεκτασιμότητά του το 2017 ήταν σε χαμηλά επίπεδα(κατά μέσο όρο 7 συναλλαγές ανά δευτερόλεπτο), σκοπός του Cardano είναι να αποτελέσει ένα σύστημα τρίτης γενιάς που θα εκτοξεύσει την επεκτασιμότητα σε νέα επίπεδα με τη βοήθεια του PoS αλγορίθμου που χρησιμοποιεί, ο οποίος έχει σχεδιαστεί για να αυξάνει την επεκτασιμότητα παράλληλα με την αύξηση των χρηστών και του όγκου του δικτύου. Ωστόσο τα παραπάνω συστήματα δεν μπορούν να αξιολογηθούν τη δεδομένη στιγμή καθώς η εφαρμογή τους αναμένεται στο άμεσο μέλλον παράλληλα με τις συνεχής τεχνικές αναβαθμίσεις, ενώ τα πειραματικά τεστ είτε δεν έχουν ξεκινήσει είτε δεν παρέχουν ακόμα επαρκή για την εξαγωγή συμπερασμάτων στοιχεία.

Πίνακας 7-Σύγκριση των κυριότερων Blockchain 3.0 συστημάτων

	Τεχνική αύξησης επεκτασιμότητας	**Συναλλαγές ανά δευτερόλεπτο**
EOS.IO	DPoS	3996[12]
Cosmos	IBC πρωτόκολλο-Hubs and Zones	4000 (64 χρήστες)
Zilliqa	Τεχνική κοπής(sharding)	2828-2488 (3600 χρήστες)
Hedera Hashgraph	Virtual voting algorithm-Gossip protocol	Περίπου 500000 (1 region, 32 computers)
Hyperledger Fabric	MSP cache, παράλληλη VSCC επικύρωση, μαζική ανάγνωση-εγγραφή κατά τη διάρκεια της MVCC φάσης επικύρωσης και δέσμευσης	2250 (στην έκδοση v1.0) Πάνω από 3560(στην έκδοση v1.1)

[12] Σύμφωνα με το http://eosnetworkmonitor.io/# στις 15-08-2018.

Κεφάλαιο 4. Κατηγοριοποίηση των blockchain συστημάτων

4.1. Κατηγορίες των blockchain συστημάτων

Η έννοια του blockchain συνδέεται με την έννοια ενός δημόσιου, διανεμημένου, αποκεντρωμένου συστήματος διαχείρισης δεδομένων. Ωστόσο με την πάροδο των χρόνων και με τη συνεχή εξέλιξη στον τομέα στης ευρύτερης τεχνολογίας, τα διάφορα blockchain συστήματα που λειτουργούν δεν ακολουθούν όλα πλέον το κλασσικό μοτίβο του δημόσιου χαρακτήρα που χαρακτηρίζει το θεμελιώδες σύστημα του Bitcoin. Τα blockchain συστήματα πλέον χρησιμοποιούνται σε ένα τεράστιο φάσμα εφαρμογών και τομέων με αποτέλεσμα πολλές φορές να παραμερίζουν κάποια απ' τα θεμελιώδη γνωρίσματα της τεχνολογίας, όπως τα επίπεδα συγκεντρωτισμού. Συνεπώς για την καλύτερη και αποτελεσματικότερη διαχείριση τους, τα συστήματα αυτά διακρίνονται σε τρείς μεγάλες κατηγορίες: δημόσια(*public-permissionless*), ιδιωτικά(*private-permissioned*) και κοινοπρακτικά(*consortium-federated-semi private*). Ο διαχωρισμός αυτός, που διασαφηνίστηκε από τον V.Buterin τον Αύγουστο του 2015[231], συναντάται πλέον σε όλη την επιστημονική κοινότητα αλλά και στην πρακτική εφαρμογή των blockchain συστημάτων και γίνεται με βάση το ποιος έχει πρόσβαση στα δεδομένα του συστήματος, ποιος συμμετέχει στην διαδικασία ομοφωνίας και ποιος εξασφαλίζει τη συνέχεια και την ασφάλεια του συστήματος. Στην Ενότητα 2.7.7 προσδιορίσαμε την κατηγοριοποίηση των blockchain συστημάτων προς όφελος της σύγκρισης των μηχανισμών συναίνεσης. Σε αυτή την ενότητα θα ασχοληθούμε πιο αναλυτικά με την κατηγοριοποίηση αυτή.

4.1.1.Δημόσια blockchain συστήματα

Αυτά τα συστήματα, γνωστά από το Bitcoin και το Ethereum, χαρακτηρίζονται από το γεγονός ότι η πρόσβαση στα δεδομένα είναι ανοιχτή σε όλους. Οποιοσδήποτε μπορεί να είναι χρήστης ή να εξυπηρετεί το ίδιο το σύστημα συμμετέχοντας στην διαδικασία της παραγωγής μπλοκ, της ολοκλήρωσης των συναλλαγών και της επίτευξης ομοφωνίας χρησιμοποιώντας μόνο το κατάλληλο λογισμικό. Τα συστήματα αυτά είναι απαλλαγμένα από κάθε μορφή έγκρισης και αδειοδότησης συμμετοχής, καθώς χαρακτηρίζονται από παντελή απουσία οποιασδήποτε μορφής ελέγχου και εξουσίας. Συνεπώς αποτελούν συστήματα που προάγουν κατά βάση έναν πλήρως αποκεντρωτικό τρόπο λειτουργίας παρέχοντας παράλληλα σε κάθε χρήστη την δυνατότητα διατήρησης της ανωνυμίας και διασφάλισης του απορρήτου. Συγκεκριμένα χρησιμοποιείται η ψευδωνυμία, αφού ο κάθε χρήστης αντιπροσωπεύεται στο δημόσιο δίκτυο από μία τυχαία ταυτότητα(*random ID*). Επίσης καθώς όλοι οι συμμετέχοντες χρήστες του δικτύου παίζουν ενεργό ρόλο στην ομαλότητα και τη σωστή λειτουργία του συστήματος, τα δημόσια blockchain συστήματα παρέχουν υψηλά επίπεδα ασφάλειας. Ωστόσο τα συστήματα αυτά χαρακτηρίζονται από υψηλά κόστη συμμετοχής, λόγω της απαιτούμενης ενεργειακής σπατάλης και λειτουργικών εξόδων, και από χαμηλές ταχύτητες εκτέλεσης και λειτουργίας συγκριτικά με τα υπόλοιπα είδη blockchain συστημάτων. Παρ' όλ' αυτά υπερέχουν συγκρινόμενα με τα υπάρχοντα κρατικά και μη συστήματα, όπως οι τράπεζες και διάφοροι κρατικοί οργανισμοί. Τα δημόσια είναι ιστορικά τα πρώτα blockchain συστήματα τα οποία λειτουργούν και στηρίζονται ακόμα στους

κλασσικούς PoW, PoS αλγορίθμους, όπως για παράδειγμα το Bitcoin και το Ethereum.
Σε μία ερευνητική εργασία της[232], η EY μεταξύ άλλων προχώρησε σε μία ενδιαφέρουσα παρουσίαση των δημόσιων blockchain σχετικά με το πώς και σε ποιες περιπτώσεις αυτά μπορούν να χρησιμοποιηθούν από τους εκάστοτε ενδιαφερόμενους.

4.1.2.Ιδιωτικά blockchain συστήματα

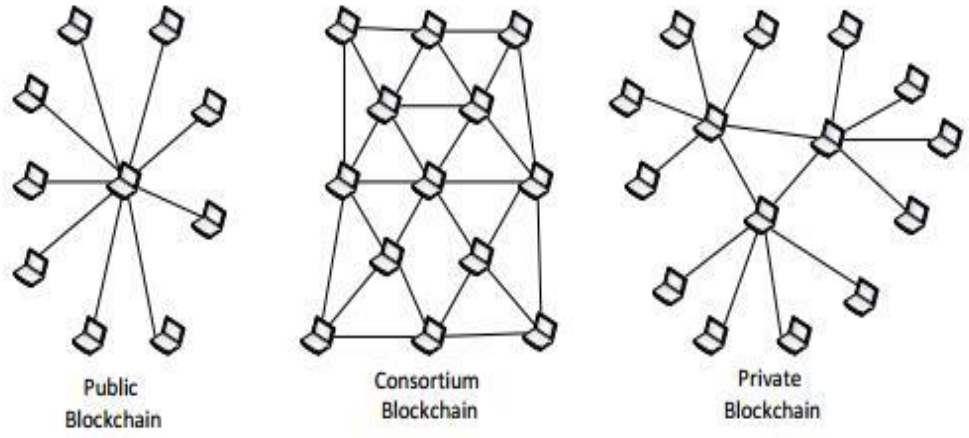
Η ειδοποιός διαφορά με τα δημόσια block chain συστήματα είναι πως η είσοδος σε ένα τέτοιο σύστημα απαιτεί την έγκριση μίας ανώτερης αρχής. Η έγκριση αυτή μπορεί να έχει τη μορφή ιδιωτικής πρόσκλησης και οι συναλλαγές ολοκληρώνονται σε ένα περιορισμένο περιβάλλον. Η ανώτερη αυτή αρχή, που μπορεί να είναι για παράδειγμα μία εταιρία ή ένας οργανισμός, ορίζει τόσο ποιος μπορεί να έχει πρόσβαση στην απλή ανάγνωση των δεδομένων όσο και ποιος μπορεί να συμμετέχει στην μεταβολή αυτών δημιουργώντας για παράδειγμα νέα μπλοκ συναλλαγών: η πρόσβαση ανάγνωσης(*read access*) μπορεί να είναι και δημόσια, αλλά η πρόσβαση εγγραφής(*write access*) περιορίζεται στην ίδια την αρχή και μόνο. Επίσης η ανώτερη αρχή έχει τον αποκλειστικό έλεγχο του καθορισμού της ομοφωνίας και μπορεί να παρεμβαίνει άμεσα στο σύστημα πραγματοποιώντας τροποποιήσεις, προσδίδοντας έτσι στα ιδιωτικά συστήματα την ιδιότητα της αναστρεψιμότητας και της μεταβλητότητας. Τα συστήματα αυτά πέραν της ευκαμψίας επιτρέπουν την ταχύτερη και φθηνότερη ολοκλήρωση συναλλαγών ανεβάζοντας τα ποσοστά αποδοτικότητας συγκριτικά με τα δημόσια συστήματα. Όπως αναφέραμε παραπάνω, η συμμετοχή ενός ατόμου σε ένα τέτοιο σύστημα προδιαθέτει ότι ο χρήστης αυτός έχει γνωστοποιήσει την ταυτότητά του. Συνεπώς εδώ έχουμε απουσία ανωνυμίας και απορρήτου αλλά παρουσία εμπιστοσύνης μεταξύ αρχής και χρηστών. Συνεπώς γίνεται αντιληπτό πως τα ιδιωτικά blockchain συστήματα είναι ιδανικά σε περιπτώσεις όπου η αποκέντρωση δεν έχει τόσο μεγάλη σημασία, καθώς η λειτουργία τους είναι στην ευθύνη των λίγων και όχι του συνόλου των χρηστών του δικτύου. Χαρακτηριστικές ιδιωτικές πλατφόρμες είναι τα Hyperledger Fabric, Blockstack[233] και Multichain[234].

4.1.3.Κοινοπρακτικά blockchain συστήματα

Θα μπορούσαμε να τοποθετήσουμε τον ορισμό των συστημάτων αυτό ενδιάμεσα στα δύο προηγούμενα είδη συστημάτων. Συγκεκριμένα η διαδικασία ομοφωνίας δεν εξαρτάται ούτε από όλους τους συμμετέχοντες στο δίκτυο ούτε από μία κεντρική μεμονωμένη μονάδα, αλλά απευθύνεται σε μία προκαθορισμένη, διανεμημένη ομάδα χρηστών. Η απλή πρόσβαση είναι ανοιχτή σε όλους σε αντίθεση με τις αλλαγές στο δίκτυο που πραγματοποιούνται από τους επιλεγμένους χρήστες. Λόγω του περιοριστικού χαρακτήρα που επιβάλλουν, τα δίκτυα αυτού του είδους των blockchain συστημάτων είναι πολύ μικρότερα παρόμοια με τα ιδιωτικά και συγκρινόμενα με

τα δημόσια δίκτυα, καθώς το πλήθος των χρηστών είναι συγκεκριμένο και όχι απεριόριστο. Επίσης αν η πλειοψηφία της κοινοπραξίας συμφωνήσει μπορούν να πραγματοποιηθούν αλλαγές στο σύστημα, καθιστώντας δυνατή την αντιστρεπτότητα και συνεπώς τα κοινοπρακτικά συστήματα μεταβλητά. Ακόμα τα κοινοπρακτικά blockchain συστήματα διατηρούν τα επιθυμητά επίπεδα ασφάλειας που χαρακτηρίζουν τα δημόσια συστήματα ενώ παράλληλα παρέχουν την ταχύτητα και την αποδοτικότητα των ιδιωτικών συστημάτων. Συνεπώς διατηρούν τα κύρια πλεονεκτήματα και των δύο παραπάνω κατηγοριών των blockchain συστημάτων και είναι ιδανικά για την επίτευξη οργανωτικής συνεργασίας μεταξύ διάφορων επιμέρους οργανισμών. Κλασσικά παραδείγματα κοινοπρακτικών blockchain συστημάτων είναι το Ripple[88] και το Corda[235].

Αξίζει να σημειώσουμε πως ο διαχωρισμός μεταξύ των ιδιωτικών και κοινοπρακτικών blockchain συστημάτων αποτελεί ένα αμφιλεγόμενο θέμα, καθώς τα εν λόγω συστήματα παρουσιάζουν αρκετές τεχνικές ομοιότητες. Ωστόσο οι διαφορές που παρατηρούνται σε διοικητικό και αρχιτεκτονικό επίπεδο μεταξύ τους μας οδηγούν σ' έναν διαχωρισμό που θα βοηθήσει στην καλύτερη κατανόηση και σε μια πιο ουσιαστική προσέγγιση στον τρόπο λειτουργίας της γενικότερης blockchain τεχνολογίας[236].



Εικόνα 15-Σχηματική αναπαράσταση διασύνδεσης των κόμβων στα δημόσια, κοινοπρακτικά και ιδιωτικά blockchain συστήματα[237]

4.2. Βασικά χαρακτηριστικά της τεχνολογίας blockchain

Σύμφωνα με το *θεώρημα CAP*[238][239] κανένα διανεμημένο σύστημα δεν μπορεί να εξασφαλίζει ταυτόχρονα τα τρία παρακάτω θεμελιώδη χαρακτηριστικά:

- Συνεκτικότητα-Συνέπεια(*Consistency*)
- Διαθεσιμότητα(*Availability*)
- Ανοχή διαχωρισμού(*Partition tolerance*)

Όσον αφορά την blockchain τεχνολογία ως μορφή διανεμημένων συστημάτων ο J. Garzik σε συνεργασία με το BitFury group, θέλοντας να επιβεβαιώσει το παραπάνω θεώρημα, εξέφρασε την αμφιβολία του σχετικά με την συνεκτικότητα των blockchain συστημάτων [115].
Παρόμοια με το θεώρημα CAP, τα blockchain συστήματα αδυνατούν να υιοθετήσουν ταυτόχρονα και τις τρείς παρακάτω ιδιότητες:

- Αποκέντρωση(*Decentralization*)
- Συνεκτικότητα(*Consistency*)
- Επεκτασιμότητα(*Scalability*)

Η αδυναμία της blockchain τεχνολογίας να ενσωματώσει ταυτόχρονα τα παραπάνω χαρακτηριστικά, γνωστά ως οι *DCS* αρχές, αποτελεί ένα ακόμα μελανό σημείο στον κόσμο της blockchain κοινότητας[191], καθώς τα blockchain συστήματα μπορούν να διαθέτουν το πολύ δύο από τα παραπάνω βασικά χαρακτηριστικά.
Σε ένα ερευνητικό άρθρο οι J. Yli-Huumo κ.ά.[240] αναφέρονται σε μία σειρά από αναγνωρισμένες προκλήσεις που αντιμετωπίζουν τα διάφορα blockchain συστήματα. Ενώ πολλές από τις προκλήσεις αυτές έχουν διευθετηθεί σε μεγάλο βαθμό(όπως η ασφάλεια, η ιδιωτικότητα και η σπατάλη πόρων), καθώς υπάρχουν προτάσεις και λύσεις, υπάρχουν άλλες για τις οποίες η επιστημονική κοινότητα, παρά τις συνεχείς προσπάθειες, δεν έχει βρει ακόμα επαρκή λύση(όπως οι χρονικές καθυστερήσεις, η επεκτασιμότητα, το μέγεθος και το εύρος των μπλοκ).
Παρακάτω, στον Πίνακα 8, παρουσιάζουμε μία βασική σύγκριση των διαφορετικών ειδών των blockchain συστημάτων ως προς κάποια στοιχειώδη χαρακτηριστικά που θεωρούμε πως αυτά πρέπει να διαθέτουν.
Στη συνέχεια θα αναλύσουμε κάποια χαρακτηριστικά της blockchain τεχνολογίας με βάση των διαχωρισμό τους στα τρία είδη συστημάτων που περιγράφουμε παραπάνω για να κατανοήσουμε πως η κάθε μορφή συστήματος ανταποκρίνεται στις απαιτήσεις της ευρύτερης τεχνολογίας, ενώ παραθέτουμε έναν πίνακα που συνοψίζει την σύγκριση αυτή.

Πίνακας 8-Θεμελιώδη χαρακτηριστικά της blockchain τεχνολογίας στα δημόσια, ιδιωτικά και κοινοπρακτικά blockchain συστήματα

	ΔΗΜΟΣΙΑ	***ΙΔΙΩΤΙΚΑ***	***ΚΟΙΝΟΠΡΑΚΤΙΚΑ***
ΑΝΩΝΥΜΙΑ	Ναι	Όχι	Όχι
ΑΜΕΤΑΒΛΗΤΟΤΗΤΑ	Ναι	Όχι	Όχι
ΑΠΟΔΟΤΙΚΟΤΗΤΑ	Χαμηλή	Υψηλή	Υψηλή
ΔΙΑΦΑΝΕΙΑ	Απόλυτη	Σχετική	Σχετική
ΑΠΟΚΕΝΤΡΩΣΗ	Πλήρης	Μηδενική	Μερική
ΣΥΝΕΚΤΙΚΟΤΗΤΑ	Ναι	Ναι	Ναι
ΕΠΕΚΤΑΣΙΜΟΤΗΤΑ	Ελάχιστη	Υψηλή	Υψηλή
ΕΥΚΑΜΨΙΑ	Χαμηλή	Υψηλή	Μέτρια
ΔΙΑΘΕΣΙΜΟΤΗΤΑ	Πλήρης	Μηδενική	Ελάχιστη
ΕΛΕΓΚΤΙΚΗ ΙΚΑΝΟΤΗΤΑ	Μηδενική	Απόλυτη	Μερική

4.2.1.Απόρρητο

Σε δημόσιο επίπεδο, τα blockchain συστήματα αποτελούν ανοιχτή πηγή πρόσβασης και συμμετοχής σε κάθε ενδιαφερόμενο, ο οποίος δεν χρειάζεται να γνωστοποιήσει τα προσωπικά του στοιχεία. Από την άλλη μεριά, στα άλλα δύο είδη συστημάτων ναι μεν η ταυτότητα απαιτείται, αλλά η πρόσβαση στην ανάγνωση μπορεί να περιοριστεί σε λίγους, αυξάνοντας έτσι τα επίπεδα ιδιωτικότητας.

4.2.2.Βαθμός εμπιστοσύνης

Η είσοδος στα δημόσια συστήματα όπως έχουμε ήδη αναφέρει είναι ανοιχτή σε όλους. Οι χρήστες του δικτύου που διαθέτουν την απαραίτητη υπολογιστική ισχύ μπορούν να δημιουργούν μπλοκ συναλλαγών και να συμμετέχουν στην ομαλή λειτουργία της εκάστοτε δημόσιας πλατφόρμας μέσω μίας διαδικασίας διαγωνισμού-συναγωνισμού που επικρατεί στο δίκτυο. Αυτό σημαίνει πως υπάρχει ανεξαρτησία και απουσία οποιασδήποτε μορφής εμπιστοσύνης μεταξύ των διάφορων κόμβων του δικτύου, σε αντίθεση με τα ιδιωτικά δίκτυα, στα οποία επικρατεί ένα κλίμα εμπιστοσύνης-συνεργασίας μεταξύ των υπεύθυνων χρηστών για την σωστή εκτέλεση και ολοκλήρωση των απαιτούμενων εργασιών. Στα κοινοπρακτικά δίκτυα η εμπιστοσύνη είναι απαραίτητη προυπόθεση κατά την επιλογή των εξουσιοδοτημένων χρηστών, οι οποίοι στη συνέχεια εκτελούν τις απαραίτητες εργασίες ο ένας ανεξάρτητα από τον άλλον, τηρώντας τους κανόνες λειτουργίας και όχι απαιτώντας εμπιστοσύνη από το υπόλοιπο δίκτυο.

4.2.3.Μηχανισμός επίτευξης ομοφωνίας

Ενώ τα περισσότερα δημόσια blockchain δίκτυα λειτουργούν στηριζόμενα κατά βάση στον κλασσικό PoW αλγόριθμο, η χρήση του PoW σε ένα ιδιωτικό δίκτυο ενέχει κινδύνους για τον τερματισμό της ομοφωνίας λόγω μίας ανωμαλίας(*blockchain anomaly*) όπως παρατηρήθηκε σε μία αλυσίδα ιδιωτικής μορφής του Ethereum[241]. Βέβαια τα μεγάλα ποσά ενεργειακής δαπάνης που χαρακτηρίζουν το PoW οδήγησαν κάποια δημόσια δίκτυα στην υιοθέτηση ενναλακτικών μοντέλων, όπως το PoS στο Ethereum, ενώ το PoA μοντέλο μπορεί να εφαρμοστεί για τον ίδιο σκοπό στα ιδιωτικά δίκτυα[196]. Επιπλέον τα ιδιωτικά δίκτυα αν και λόγω της φύσης τους ενσωματώνουν μοντέλα με περιορισμένα χαρακτηριστικά δημόσιας φύσης[78], όπως το PBFT με χαρακτηριστικό παράδειγμα το Hyperledger Fabric αλλά και το ηγετικής φύσης μοντέλο Raft[242], μπορούν να λειτουργήσουν σε κάποιες περιπτώσεις και υπό τη λογική του PoS, όπως για παράδειγμα η ανοιχτού κώδικα μηχανή Tendermint[243]. Τα κοινοπρακτικά δίκτυα στηρίζονται σε μηχανισμούς που ακολουθούν μία διαδικασία ψηφοφορίας ομοσπονδιακού χαρακτήρα, όπως το PBFT και την UNL εφαρμογή στο Ripple.

4.2.4.Επίπεδα ασφαλείας

Αναφερόμενοι στην ασφάλεια των blockchain συστημάτων η βασική διαφορά μεταξύ των δημόσιων με τα άλλα δύο είδη συστημάτων είναι ουσιαστικά απλή και αφορά τους κανόνες που διέπουν τη λειτουργία και την επίτευξη ομοφωνίας: στα δημόσια συστήματα η ασφάλεια παρέχεται από την μαθηματική αδυναμία της αντιστροφής και της κακόβουλης διαχείρισης των συναλλαγών, ενώ στα υπόλοιπα συστήματα η ασφάλεια είναι ουσιαστικά απόλυτη συνάρτηση της ειλικρίνειας και της ορθολογικής συμπεριφοράς των συμμετεχόντων. Πιο αναλυτικά το δημοφιλέστερο δημόσιο σύστημα, το Bitcoin, παρέχει ασφάλεια που στηρίζεται στη δομή της κρυπτογραφικής λογικής του, ενώ η εφαρμογή του PoW εξασφαλίζει τη μέγιστη δυνατή αλλά όχι απόλυτη προστασία απέναντι σε διάφορες γνωστές απειλές, όπως οι 51% και οι sybil επιθέσεις. Η ασύμμετρη κρυπτογράφηση εξασφαλίζει την προστασία των προσωπικών δεδομένων και τη διασφάλιση της ολοκλήρωσης των συναλλαγών, ενώ η λογική της επένδυσης πόρων και λογισμικού του PoW αποθαρρύνει τους κακόβουλους χρήστες να επιχειρήσουν επιθέσεις. Το Bitcoin και τα περισσότερα δημόσια blockchain συστήματα είναι επίσης απαλλαγμένα από κάθε μορφή κεντρικού(*central point of failure*) ή μοναδικού σημείου αποτυχίας(*single point of failure*)[13], σε αντίθεση με τα ιδιωτικά blockchain συστήματα. Συγκεκριμένα σε αυτά μία δυσλειτουργία ή αποτυχία του κεντρικού οργανισμού που ελέγχει τη λειτουργία ολόκληρου του δικτύου μπορεί να οδηγήσει το σύστημα σε καθυστερήσεις, επιπλοκές στην ολοκλήρωση συναλλαγών και εξακρίβωσης της ταυτότητας, διαταράσσοντας έτσι τη διαθεσιμότητα και την ασφάλεια του δικτύου[244]. Συνεπώς τα ιδιωτικά blockchain συστήματα υποφέρουν από το μοναδικό σημείο αποτυχίας. Τα κοινοπρακτικά συστήματα περιορίζουν την παραπάνω μορφή αποτυχίας καθώς η

[13] https://en.wikipedia.org/wiki/Single_point_of_failure

οργάνωση του δικτύου διαμοιράζεται σε περισσότερους από έναν υπεύθυνους, ενώ η ασφάλεια ενισχύεται από το γεγονός ότι τα συνολικά δεδομένα δεν αναπαράγονται ταυτόχρονα σε κάθε χρήστη, αλλά διαμοιράζονται μεμονωμένα στους προεπιλεγμένους χρήστες.
Επιπλέον η εχθρική ανοχή των διάφορων blockchain συστημάτων έχει αναλυθεί εκτενώς στις Ενότητες 2.7.8 και 2.7.5.

4.2.5.Κόστος και ταχύτητα εκτέλεσης συναλλαγών

Τα δημόσια blockchain συστήματα χρησιμοποιούν ένα peer-to-peer σύστημα επικύρωσης των συναλλαγών. Αυτό σημαίνει πως για να θεωρηθεί μία μεμονωμένη συναλλαγή ως έγκυρη και ικανή να συμπεριληφθεί σε ένα μπλοκ της ευρύτερης αλυσίδας, πρέπει να επικυρωθεί από τον κάθε ξεχωριστό κόμβο του δικτύου, γεγονός που με τη σειρά του καθιστά το κόστος συναλλαγών υψηλό και ταυτόχρονα οδηγεί σε μεγάλες καθυστερήσεις επιβεβαίωσης άρα και ολοκλήρωσης των εκκρεμών συναλλαγών. Αντίθετα στα ιδιωτικά και κοινοπρακτικά συστήματα η επικύρωση των συναλλαγών εναποτίθεται σε μία κυρίαρχη οργάνωση ή σε ένα περιορισμένο πλήθος ατόμων, με αποτέλεσμα την βελτίωση της ταχύτητας εκτέλεσης, την μείωση των χρονικών καθυστερήσεων λόγω αναμονής και την ελαχιστοποίηση του κόστους συναλλαγών. Τα παραπάνω συμπεράσματα γίνονται ακόμα πιο κατανοητά χρησιμοποιώντας ένα τυπικό παράδειγμα : το Bitcoin χρειάζεται περίπου 60 λεπτά για την επιβεβαίωση μιας νέας συναλλαγής με τέλη συναλλαγών που κινούνται κατά μέσο όρο στο 1 USD, ενώ το Ripple επιβεβαιώνει τις συναλλαγές με καθυστερήσεις της τάξης των 4 δευτερολέπτων και περιλαμβάνει τέλη συναλλαγών μικρότερα του 0,01 USD. Στα ιδιωτικά δίκτυα οι συναλλαγές συνήθως δεν συνεπάγονται καταβολή επιπλέον φόρων.

Πίνακας 9-Αναλυτική σύγκριση των τριών ειδών των blockchain συστημάτων

	ΔΗΜΟΣΙΑ	***ΙΔΙΩΤΙΚΑ***	***ΚΟΙΝΟΠΡΑΚΤΙΚΑ***
ΕΙΣΟΔΟΣ ΝΕΩΝ ΜΕΛΩΝ	Ελεύθερη σε όλους	Απαιτείται έγκριση	Περιορισμένη
ΠΡΟΣΒΑΣΗ ΑΝΑΓΝΩΣΗΣ	Ανοιχτή σε όλους	Δημόσια ή περιορισμένη σε συγκεκριμένους χρήστες	Δημόσια ή περιορισμένη σε συγκεκριμένους χρήστες
ΠΡΟΣΒΑΣΗ ΕΓΓΡΑΦΗΣ	Ανοιχτή σε όλους	Περιορίζεται στην ανώτερη αρχή	Σύνολο προεπιλεγμένων-εγκεκριμένων χρηστών
ΚΑΘΟΡΙΣΜΟΣ ΟΜΟΦΩΝΙΑΣ-ΔΙΕΚΠΕΡΑΙΩΣΗ ΣΥΝΑΛΛΑΓΩΝ	Όλοι οι ενεργοί χρήστες(πχ miners, stakeholders)	Ανώτερη αρχή αποκλειστικά	Σύνολο προεπιλεγμένων-εγκεκριμένων χρηστών
ΜΗΧΑΝΙΣΜΟΣ ΕΠΙΤΕΥΞΗΣ ΟΜΟΦΩΝΙΑΣ	Κυρίως PoW, PoS	PoS, PBFT, PoA, Raft	Συλλογική ομοφωνία στηριζόμενη συνήθως σε πρωτόκολλα ψηφοφορίας
ΤΑΧΥΤΗΤΑ ΕΚΤΕΛΕΣΗΣ ΣΥΝΑΛΛΑΓΩΝ	Χαμηλή	Υψηλή	Ενδιάμεση
ΤΑΥΤΟΤΗΤΑ	Δεν απαιτείται-Ανωνυμία/ Ψευδωνυμία	Απαραίτητη	Απαραίτητη
ΕΜΠΙΣΤΟΣΥΝΗ	Απουσία οποιασδήποτε μορφής εμπιστοσύνης	Απαραίτητη μεταξύ αρχής-μελών	Απαραίτητη στην προεπιλογή των υπεύθυνων χρηστών
ΠΑΡΟΧΗ ΑΣΦΑΛΕΙΑΣ	Σύνθετες διαδικασίες κρυπτογράφησης-αποκρυπτογράφησης	SPOF (*single point of failure*), Ορθολογική συμπεριφορά χρηστών	Μειωμένη αναπαραγωγή δεδομένων σε ολόκληρο το δίκτυο
ΣΥΝΑΛΛΑΚΤΙΚΟ ΜΕΣΟ	Κρυπτονομίσατα	Δεν απαιτείται	Ανάλογα την πλατφόρμα
ΚΟΣΤΟΣ ΣΥΝΑΛΛΑΓΩΝ	Υψηλό	Χαμηλό	Περιορισμένο
ΚΑΤΑΝΑΛΩΣΗ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ	Υψηλή(PoW υπολογιστική ισχύς)	Χαμηλή(Περιορισμένος αριθμός χρηστών)	Παρόμοια με τα ιδιωτικά συστήματα
ΠΑΡΑΔΕΙΓΜΑΤΑ	Bitcoin, Ethereum, Litecoin, Monero, Dash, Neo, NEM, Stellar	Hyperledger Fabric, Quorum, Monax, Chain INC, Multichain, Exonum, Blockstack	Corda R3, EWF, Ripple

Κεφάλαιο 5. Συζήτηση, ερευνητικά αποτελέσματα και καινοτομίες

5.1. Σύνοψη της εργασίας

Σε αυτή τη διπλωματική εργασία ασχοληθήκαμε με τη μελέτη, την επισκόπηση, την ανάλυση και τη σύγκριση των διάφορων μηχανισμών συναίνεσης της blockchain τεχνολογίας. Αφού παραθέσαμε κάποιες βασικές έννοιες για την ευκολότερη κατανόηση της blockchain τεχνολογίας αναλύσαμε όλους τους κλασσικούς μηχανισμούς συναίνεσης, ενώ παραθέσαμε και άλλους λιγότερο δημοφιλείς. Συγκεκριμένα αναλύσαμε τους PoW, PoS, DPoS, PoET, PBFT, RPCA και SCP μηχανισμούς και προχωρήσαμε σε μία ευρεία σύγκριση μεταξύ τους, προσδιορίζοντας όλες τις βασικές παραμέτρους της blockchain τεχνολογίας, όπως η διακίνηση και η ταχύτητα εκτέλεσης των συναλλαγών, η επεκτασιμότητα, η ασφάλεια έναντι εχθρικών ενεργειών κ.ά. Με βάση την ανάλυσή μας καταλήγουμε στο γενικό συμπέρασμα πως η σύγκριση των παραπάνω μηχανισμών δεν είναι απλό εγχείρημα, καθώς απαιτείται βαθιά γνώση και επαρκή ποσοτικά δεδομένα για να μπορέσουμε να αξιολογήσουμε πλήρως το σύνολο των μηχανισμών συναίνεσης. Επιπροσθέτως η blockchain τεχνολογία, άρα και οι μηχανισμοί συναίνεσης στους οποίους στηρίζεται, εξελίσσεται με την πάροδο του χρόνου με σκοπό την ενσωμάτωσή της σε όλο και περισσότερους τομείς, συνεπώς η σύγκριση και η αξιολόγηση των μηχανισμών συναίνεσης θα είναι ιδανικό να γίνεται ανά τακτά χρονικά διαστήματα ώστε να συμβαδίζει με την πραγματικότητα, η οποία στον blockchain κόσμο είναι συνεχώς μεταβαλλόμενη.

5.2. Συγκριτικά αποτελέσματα και καινοτομίες

Κατά τη διάρκεια εκπόνησης αυτής της διπλωματικής εργασίας ασχοληθήκαμε σχολαστικά με τη μελέτη, την ανάλυση, την αξιολόγηση και τη σύγκριση μίας μεγάλης ποικιλίας ερευνητικών και επιστημονικών εργασιών που πραγματεύονται τη blockchain τεχνολογία καθώς και την ανάλυση και τη σύγκριση των μηχανισμών συναίνεσης[67][50][48][91][92][78][44][245][62][246][247][248][249][250][251].
Θεωρούμε πως για να δομήσει κανείς μία ολοκληρωμένη σύγκριση μεταξύ των διάφορων μηχανισμών συναίνεσης θα πρέπει να συμπεριλάβει στη σύγκρισή του μεταξύ άλλων ποιοτική ανάλυση, έγκυρα ποσοτικά δεδομένα, καθώς και σχολαστική μελέτη και κριτική ανάλυση θεμελιωδών εννοιών, όπως οι δείκτες απόδοσης και ασφάλειας των blockchain συστημάτων. Αν και στην υπάρχουσα βιβλιογραφία υπάρχει πληθώρα συγκριτικών προσεγγίσεων, θεωρούμε πως μέχρι και σήμερα, με εκτίμηση στη διαθέσιμη ερευνητική βιβλιογραφία, δεν υπάρχει κάποια ερευνητική εργασία που να καταπιάνεται με όλες τις απαραίτητες πτυχές των μηχανισμών συναίνεσης, παραθέτοντας πλήρη ανάλυση και σύγκριση. Θεωρούμε πως στην παρούσα διπλωματική εργασία έχουμε προσεγγίσει και αναλύσει όλες τις απαραίτητες πτυχές των μηχανισμών συναίνεσης ώστε να μπορέσουμε να συντάξουμε μία καινοτόμο ανάλυση και σύγκριση, συνδυάζοντας τόσο ποιοτικά όσο και ποσοτικά δεδομένα και παρέχοντας μία κατάλληλη βάση για επιπλέον έρευνα και ανάλυση σε συνδυασμό με τις μελλοντικές τάσεις και προκλήσεις.

5.2.1.Δείκτες απόδοσης

Σε κάθε blockchain σύστημα το βασικό ζητούμενο της επιτυχίας είναι η απόδοση. Προσεγγίσαμε την πολυδιάστατη έννοια της απόδοσης αναλύοντας τις χρονικές καθυστερήσεις των συναλλαγών, τις συναλλαγές ανά δευτερόλεπτο και την επεκτασιμότητα. Πιο αναλυτικά στην Ενότητα 2.7 παρουσιάσαμε μία αναλυτική περιγραφή της οριστικότητας των μηχανισμών συναίνεσης. Αφού ξεκινήσαμε με μία θεωρητική προσέγγιση συνεχίσαμε προσδιορίζοντας την οριστικότητα μέσω των χρονικών καθυστερήσεων που παρατηρούνται κατά την ολοκλήρωση των συναλλαγών στα δίκτυα των blockchain συστημάτων. Ορίσαμε τις καθυστερήσεις αυτές και τις αναλύσαμε με έναν καινοτόμο τρόπο, σύμφωνα και με την Εξίσωση 1 της Υποενότητας 2.7.1.2, παρουσιάζοντας στον Πίνακα 1 αριθμητικά δεδομένα που καταδεικνύουν τις διαφορές ανάμεσα στα κυριότερα blockchain συστήματα. Κατά τη γνώση και τη γνώμη μας παρέχουμε για πρώτη φορά σε ερευνητικό επίπεδο μία αναλυτική και περιεκτική περιγραφή της έννοιας της οριστικότητας των συναλλαγών. Ακόμα ασχοληθήκαμε αναλυτικά με τον βαθμό ευελιξίας εμπιστοσύνης και τον προσδιορισμό της συναίνεσης στα διάφορα blockchain συστήματα, δύο θέματα που αποτελούν πλευρές της blockchain τεχνολογίας που συνήθως προσδιορίζονται επιφανειακά. Στη συνέχεια προσεγγίσαμε την πάντα επίκαιρη έννοια της επεκτασιμότητας επικεντρώνοντας στις συναλλαγές ανά δευτερόλεπτο και στο πλήθος των κόμβων σε κάθε δίκτυο, οργανώνοντας τα δεδομένα που αντλήσαμε από διάφορες πηγές στον Πίνακα 2. Συνδυάζοντας τα δεδομένα των Πινάκων 1 και 2 μπορούμε να καταλήξουμε στο συμπέρασμα πως τα BA πρωτόκολλα κατά κανόνα παρέχουν καλύτερους δείκτες απόδοσης από τα βασικότερα proof-based μοντέλα, ωστόσο μειονεκτούν ως προς την επεκτασιμότητα στο εύρος των χρηστών που συμμετέχουν. Βέβαια κάτι τέτοιο μπορεί να αποτελεί και σκοπό για τις επιχειρήσεις και οργανώσεις που χρησιμοποιούν κατά βάση τα ιδιωτικά και κοινοπρακτικά δίκτυα, διασφαλίζοντας ένα περιβάλλον εμπιστοσύνης στο δίκτυό τους. Οι δείκτες αυτοί αφορούν τις συναλλαγές ανά δευτερόλεπτο σε συνδυασμό με τις χρονικές καθυστερήσεις των συναλλαγών. Όλα τα BA μοντέλα με την απόλυτη οριστικότητα παρέχουν χρονικές καθυστερήσεις της τάξης των 1-20 δευτερολέπτων, ενώ παράλληλα παρέχουν συναλλαγές που κινούνται στις 1000-3500 ανά δευτερόλεπτο. Από την άλλη τα δημοφιλέστερα proof-based συστήματα με την πιθανολογική οριστικότητα χαρακτηρίζονται από ελάχιστες συναλλαγές και χρονικές καθυστερήσεις της τάξης των μερικών δεκάδων λεπτών, καθιστώντας την απόδοσή τους μείζον πρόβλημα υψίστης σημασίας, με μερικές εξαιρέσεις όπως το EOS.IO με το DPoS και το NEM με το PoI.

Να τονίσουμε πάλι πως η καλύτερη αποδοτικότητα των BA συστημάτων έχει έναν αρνητικό αντίκτυπο ως προς την επεκτασιμότητα, καθώς τα δίκτυα αυτά όπως δείξαμε στον Πίνακα 2 λειτουργούν σε μικρό εύρος χρηστών, συγκριτικά με τους αναρίθμητους χρήστες που μπορούν να συμμετάσχουν στα proof-based συστήματα. Αποδίδουμε το γεγονός αυτό στην πολυπλοκότητα των μηνυμάτων που ανταλλάσσονται μεταξύ των κόμβων στα BA συστήματα προκειμένου να επιβεβαιωθούν οι συναλλαγές, με χαρακτηριστικό παράδειγμα την ενδοεπικοινωνιακή δομή του Hyperledger Fabric που στηρίζεται στο PBFT μοντέλο συναίνεσης.

Τέλος η απόδοση των blockchain συστημάτων προφανώς επηρεάζεται από την ασφάλεια που αυτά παρέχουν έναντι εχθρικών και κακόβουλων ενεργειών, που περιγράψαμε στις Ενότητες 2.7.5 και 2.7.8. Η ασφάλεια των πολλών μηχανισμών

συναίνεσης προκύπτει από την ίδια τη δομή τους, όπως για παράδειγμα η καταβολή ενεργειακής κατανάλωσης που αποτελεί απόδειξη της προσπάθειας και εργασίας στο PoW. Άλλοι μηχανισμοί στηρίζουν την ασφάλειά τους σε πρωτόκολλα ψηφοφορίας και εκλογής με σκοπό τη συναίνεση, όπως τα BA πρωτόκολλα. Σε κάθε περίπτωση μία ουσιαστική διαφορά των κυριότερων proof-based από τα vote-based πρωτόκολλα είναι η εχθρική ανεκτικότητα, η οποία στα μεν κινείται κατά κανόνα στο 25-50% ενώ στα δε στο 20-33%. Με βάση αυτό θα μπορούσε κανείς να πει ότι τα vote-based πρωτόκολλα χαρακτηρίζονται από χαμηλότερα επίπεδα ασφαλείας. Διαφωνούμε με αυτή την άποψη, καθώς όπως δείξαμε στον Πίνακα 3 της Ενότητας 2.7.8 τα PBFT, RPCA και SCP συστήματα υποφέρουν από λιγότερες κλασσικές επιθέσεις, γεγονός το οποίο αποδίδουμε στην απόλυτη οριστικότητα που παρέχουν και στο κλίμα συνεργασίας που διέπουν. Συνεπώς μιας και τα δίκτυα της BA λογικής είναι γενικότερα πιο συνεκτικά και δυσμετάβλητα, θεωρούμε πως ίσως τελικά οι θεαματικοί δείκτες απόδοσης που παρέχουν συνδέονται και με τη σταθερότητα της ασφάλειας τους, καθώς η απόδοση δεν χρειάζεται να μετριαστεί προς όφελος της ασφάλειας, κάτι που χαρακτηρίζει σε μεγάλο βαθμό τα περισσότερα proof-based δίκτυα.

5.2.2.Βέλτιστη επεκτασιμότητα

Παρά την πληθώρα μοντέλων και πρωτοκόλλων συναίνεσης δεν υπάρχει κανένας ιδανικός ως προς την επεκτασιμότητα μηχανισμός συναίνεσης και αυτό αποδεικνύεται από το γεγονός ότι τα συστήματα τα οποία παρέχουν ικανοποιητικούς δείκτες διακίνησης με μικρές χρονικές καθυστερήσεις χαρακτηρίζονται από περιορισμό στο εύρος χρήσης, όπως τα ιδιωτικά συστήματα, ενώ στον αντίποδα τα συστήματα με απεριόριστο πλήθος χρηστών χαρακτηρίζονται από χαμηλή απόδοση, όπως το δημόσιο δίκτυο του Bitcoin. Παραθέσαμε και αναλύσαμε για πρώτη φορά διάφορες τεχνικές βελτίωσης της επεκτασιμότητας, οι οποίες αν και όχι ευρέως δοκιμασμένες, διαθέτουν την προοπτική να βοηθήσουν σε σημαντικό βαθμό στην επίλυση του μεγάλου αυτού προβλήματος. Για τις τεχνικές αυτές κινηθήκαμε σε τρείς κατευθύνσεις: τα off-chain συστήματα, την τεχνική του sharding και τα Blockchain 3.0 συστήματα. Συγκεκριμένα τα off-chain συστήματα, όπως το Lightning Network, το Raiden και το Plasma, τα οποία αναμένεται μέσα στο 2019 να τεθούν σε κανονική ή πιο ευρεία ισχύ, εισάγουν την layer-2 δομή ανοίγοντας νέους ορίζοντες στην επεκτασιμότητα. Επίσης η τεχνική του sharding, που ήδη εφαρμόζεται και αποτελεί αντικείμενο μελέτης και υλοποίησης στο Ethereum, έχει ήδη αποδώσει σημαντικά στην βελτίωση της επεκτασιμότητας. Ακόμα μεγάλο ενδιαφέρον παρουσιάζουν τα Blockchain 3.0 συστήματα, τα οποία θεωρητικά θα φέρουν μία επανάσταση ως προς την επεκτασιμότητα και όχι μόνο. Στους συγκριτικούς Πίνακες 5, 6 και 7 που έχουμε δημιουργήσει συμπεριλάβαμε όσο το δυνατόν πιο ασφαλή δεδομένα, καθώς κάποια συστήματα βρίσκονται ακόμα σε πιλοτικό και ερευνητικό στάδιο, και έχουμε ολοκληρώσει την έρευνά μας περί της επεκτασιμότητας σε πρακτικό και όχι θεωρητικό επίπεδο. Οι προτάσεις που αναφέρουμε συνοδεύονται από πλήρη και επαρκή αιτιολόγηση, παρέχοντας έτσι στον αναγνώστη μία πλήρη επισκόπηση των ήδη υπαρχόντων λύσεων και μία πλήρη εικόνα των μελλοντικών τάσεων.
Θεωρούμε πως ένας συνδυασμός των Lightning Network και Plasma θα δημιουργούσε ένα ισχυρό δίκτυο, το οποίο θα εκτόξευε τους επεκτάσιμους

περιορισμούς των PoW και PoS διατηρώντας την αποκέντρωση και διευρύνοντας τις δυνατότητες των συναλλαγών πέρα από τα μικρά ποσά στα οποία κατά βάση περιορίζεται το Lightning Network. Παρομοίως το Ethereum θα μπορούσε να αναβαθμιστεί σημαντικά συνδυάζοντας στο δίκτυό του το Plasma με το Raiden, ωστόσο πρέπει να περιμένουμε μία πιο επίσημη εφαρμογή του Raiden για να αξιολογηθούν οι βελτιώσεις και οι εξαιρετικοί δείκτες που διαθέτει. Συμπερασματικά, στηριζόμενοι στα συγκριτικά δεδομένα του Πίνακα 5 που έχουμε συντάξει, θεωρούμε το Lightning Network ως τη βέλτιστη off-chain επεκτάσιμη λύση, η οποία μάλιστα ήδη εφαρμόζεται και συνεχώς βελτιώνεται.

Αναφορικά με τις το sharding και με βάση την αναλυτική σύγκριση που έχουμε παραθέσει μεταξύ των RSCoin, Elastico, Omniledger και RapidChain στον Πίνακα 6, θεωρούμε το RapidChain ως τη βέλτιστη επεκτάσιμη λύση, καθώς αποτελεί ένα πρωτόκολλο που μέσω του sharding αυξάνει εντυπωσιακά τον αριθμό των χρηστών διατηρώντας παράλληλα υψηλά επίπεδα διακίνησης συναλλαγών, όπως μικρές χρονικές καθυστερήσεις, παρόμοιες με αυτές των BA πρωτοκόλλων, και περίπου 7500 συναλλαγές ανά δευτερόλεπτο.

Τέλος αναφορικά με τα Blockchain 3.0 συστήματα να πούμε πως το πλήθος τους συνεχώς αυξάνεται με την πάροδο του χρόνου και παράλληλα με το συνεχώς διευρυνόμενο εύρος χρήσης του. Για πρακτικούς λόγους ξεχωρίσαμε, αναλύσαμε και συγκρίναμε τα πέντε πιο ενδιαφέροντα συστήματα που συμβαδίζουν με την Blockchain 3.0 εποχή, τα οποία είναι τα EOS.IO, Zilliqa, Cosmos, Hedera Hashgraph και Hyperledger Fabric. Τα EOS.IO και Hyperledger Fabric αποτελούν δύο πολύ δημοφιλή συστήματα που έχουν αποδείξει τις επεκτάσιμες αρετές τους, χρησιμοποιώντας διαφορετικούς μηχανισμούς συναίνεσης και λειτουργώντας το πρώτο σε δημόσιο και το δεύτερο σε ιδιωτικό επίπεδο. Ωστόσο και τα δύο συστήματα αποτελούν διέξοδο στην επεκτασιμότητα με διαφορετικές επεκτάσιμες τεχνικές και εξαιρετικούς δείκτες διακίνησης, αλλά με διαφορετικά όρια στον αριθμό χρηστών και στα επίπεδα αποκέντρωσης. Το EOS.IO είναι μία δημόσια πλατφόρμα στην οποία ωστόσο το DPoS επιτρέπει μόνο σε περιορισμένο αριθμό από το σύνολο των κόμβων να παράγουν τα μπλοκ συναλλαγών, ενώ το Hyperledger Fabric λειτουργεί αυστηρά σε συγκεντρωτικό επίπεδο και μία κλειστή ομάδα γνωστών αναμεταξύ τους κόμβων. Οι υπόλοιπες Blockchain 3.0 προτάσεις είτε κινούνται ακόμα σε πειραματικό-πιλοτικό στάδιο είτε η εφαρμογή τους βρίσκεται σε πρώιμη μορφή, οπότε θεωρούμε πως μία πιο ώριμη αξιολόγηση θα πρέπει να περιμένει μέχρι να περάσει κάποιο χρονικό διάστημα ώστε να εξάγουμε πιο ασφαλή και έγκυρα συμπεράσματα.

5.2.3.Δημόσια-Ιδιωτικά-Κοινοπρακτικά συστήματα

Τέλος ολοκληρώσαμε την ανάλυσή μας ασχολούμενοι με την διάσημη πλέον κατηγοριοποίηση των blockchain συστημάτων σε δημόσια, ιδιωτικά και κοινοπρακτικά, περιγράφοντας πώς και πού μπορεί να εφαρμοστεί το καθένα και γιατί. Συγκεκριμένα καταλήξαμε πως τα ιδιωτικά δίκτυα είναι ιδανικά για εταιρίες, οργανισμούς και επιχειρήσεις οι οποίες επιθυμούν να διατηρήσουν ένα κλειστό δίκτυο με λιγότερους χρήστες αλλά υψηλούς δείκτες αποδοτικότητας. Τα δημόσια δίκτυα είναι ιδανικά για μαζική χρήση χωρίς περιορισμούς, αλλά με μειωμένη απόδοση, ενώ τα κοινοπρακτικά δίκτυα είναι κάπου στη μέση, καθώς με προσαρμογές μπορούν να χρησιμοποιηθούν σε διάφορες περιπτώσεις. Μία

περιληπτική σύγκριση παρουσιάσαμε στον συμπερασματικό Πίνακα 9, όπου έχουμε συμπεριλάβει όλες τις σημαντικές πτυχές της σύγκρισής μας.
Επιπλέον προχωρήσαμε, πέραν της κλασσικής σύγκρισης που υπάρχει στη βιβλιογραφία, σε μία ποιοτική σύγκριση στον Πίνακα 8, καταδεικνύοντας πώς ανταποκρίνεται η κάθε μία από τις τρεις κατηγορίες των blockchain συστημάτων σε θεμελιώδη γνωρίσματα της ταυτότητας της γενικότερης blockchain λογικής. Μέσω της ανάλυσης αυτής εκφράζουμε την πεποίθηση πως τελικά καμία μορφή blockchain συστήματος δεν διατηρεί τις αρχικές ιδιότητες και χαρακτηριστικά της blockchain φύσης. Αντίθετα, μιας και τα blockchain συστήματα συνεχώς μεταβάλλονται και προσαρμόζουν τη δομή τους στις διάφορες εφαρμογές όπου τείνουν να χρησιμοποιηθούν, θεωρούμε πως ακόμα και τα βασικότερα χαρακτηριστικά της blockchain τεχνολογίας, όπως η ιδιωτικότητα, η αποκέντρωση και η ασφάλεια όχι μόνο δεν μπορούν να συνυπάρξουν αρμονικά σε κάποιο σύστημα, αλλά πολλές φορές μπορεί να απουσιάζουν εντελώς από αυτό.

Κεφάλαιο 6. Επίλογος

Κατά γενική ομολογία η blockchain τεχνολογία είναι ένα από τα πιο περιζήτητα θέματα των τελευταίων χρόνων και της επικαιρότητας. Για άλλους η blockchain τεχνολογία είναι μία επαναστατική τάση, η οποία μπορεί να φέρει ριζοσπαστικές αλλαγές στις συναλλακτικές διαδικασίες, στην ανωνυμία των πληρωμών και σε ένα τεράστιο εύρος εφαρμογών που κινούνται από την οικονομία μέχρι και την εκπαίδευση, την υγεία και την πολιτική. Για άλλους πρόκειται απλά για μία τεχνολογική φούσκα με θολό πλαίσιο και πολλές υποσχόμενες προοπτικές στις οποίες δεν μπορεί να ανταποκριθεί.

Ανήκοντας στην πρώτη κατηγορία, θεωρούμε την blockchain τεχνολογία μία πρωτοποριακή τεχνολογία, η οποία μπορεί να αλλάξει ριζικά πολλά πράγματα όπως τα γνωρίζουμε σήμερα στην επιστημονική κοινότητα και στην καθημερινή μας ζωή. Σκοπός της διπλωματικής αυτής εργασίας είναι να προσδιορίσουμε, να αναλύσουμε και να συγκρίνουμε τον πυρήνα των blockchain συστημάτων, που δεν είναι άλλος από τον μηχανισμό συναίνεσης που χρησιμοποιούν.

Αφού περιγράψαμε σε βάθος τους κυριότερους μηχανισμούς συναίνεσης προχωρήσαμε σε μία αναλυτική σύγκριση μεταξύ τους, προσδιορίζοντας κατά τη γνώμη μας όλα τα απαραίτητα πεδία, όπως για παράδειγμα οι δείκτες απόδοσης και η ασφάλεια. Επιπλέον ασχοληθήκαμε εκτενώς με το πρόβλημα της επεκτασιμότητας που αντιμετωπίζουν όλα τα blockchain συστήματα, παραθέτοντας μία σειρά από λύσεις και προτάσεις για την βελτίωση του προβλήματος αυτού και προσδιορίσαμε την κατηγοριοποίηση των blockchain συστημάτων σε δημόσια, ιδιωτικά και κοινοπρακτικά. Συνοψίζουμε τα αποτελέσματα της σύγκρισής μας στους διάφορους Πίνακες και Διαγράμματα που έχουμε δημιουργήσει, για μία πιο εύκολη μελέτη από τον αναγνώστη.

Τέλος, προτείνουμε μελλοντικά τη συνεχή ενασχόληση με τη μελέτη των διάφορων μηχανισμών συναίνεσης, καθώς οι ανάγκες και οι απαιτήσεις εφαρμογής της blockchain τεχνολογίας συνεχώς αυξάνονται, με αποτέλεσμα να αλλάζουν και οι ίδιοι οι μηχανισμοί αυτοί. Επιπλέον θεωρούμε ζωτικής σημασίας την περαιτέρω αξιολόγηση των διάφορων επεκτάσιμων προτάσεων που έχουμε παραθέσει παράλληλα με την πλήρη εφαρμογή τους στον πραγματικό κόσμο και σε αξιόλογο εύρος χρηστών.

Βιβλιογραφία

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9. doi:10.1007/s10838-008-9062-0stem," *J. Gen. Philos. Sci.*, vol. 39, no. 1, pp. 53–67, 2008.

[2] L. Lamport, "time-clocks," vol. 21, no. 7, pp. 1–8, 2000.

[3] F. B. Schneider, "Implementing fault-tolerant services using the state machine approach: a tutorial," *ACM Comput. Surv.*, vol. 22, no. 4, pp. 299–319, 1990.

[4] G. Coulouris, J. Dollimore, and T. Kindberg, *Distributed Systems: Concepts and Design*, 4th ed. 2012.

[5] B. Benatallah, F. Casati, and F. Toumani, "Web service conversation modeling: a cornerstone for e-business automation," *IEEE Internet Comput.*, vol. 8, no. 1, pp. 46–54, 2004.

[6] G. Fox, "Peer-to-Peer Networks," *Comput. Sci. Eng.*, vol. 3, no. 3, pp. 75–77, 2001.

[7] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," *Proc. - 1st Int. Conf. Peer-to-Peer Comput. P2P 2001*, pp. 101–102, 2001.

[8] J. Fischer, A. Lynch, and S. Paterson, "Impossibility of Distributed Consensus," vol. 32, no. 2, pp. 374–382, 1985.

[9] N. A. Lynch, *Distributed Algorithms*. Morgan Kaufmann, 1996, 1996.

[10] C. Dwork, N. Lynch, and L. Stockmeyer, "Consensus in the presence of partial synchrony," *J. ACM*, vol. 35, no. 2, pp. 288–323, 1988.

[11] T. D. Chandra and S. Toueg, "Unreliable failure detectors for reliable distributed systems," *J. ACM*, vol. 43, no. 2, pp. 225–267, 1996.

[12] S. Kumar and M. Kumar, "Distribution System Faults Classification And Location Based On Wavelet Transform," *Int. J. Adv. Comput. Theory Eng.*, no. 4, pp. 86–91, 2013.

[13] P. Raipin Parvedy and M. Raynal, "Uniform agreement despite process omission failures," *Proc. - Int. Parallel Distrib. Process. Symp. IPDPS 2003*, vol. 00, no. C, 2003.

[14] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[15] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[16] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. New York: Chapman and Hall/CRC, 2014.

[17] M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic applications," *Proc. twenty-first Annu. ACM Symp. Theory Comput. - STOC '89*, pp. 33–43, 1989.

[18] Nomura Research Institute, "Survey on Blockchain Technologies and Related Services," *Res. Rep.*, vol. 10, no. March, pp. 1–78, 2015.

[19] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, 2001.

[20] A. Back, "Hashcash - A Denial of Service Counter-Measure," *Tech. Rep.*, no. August, pp. 1–10, 2002.

[21] S. Peng, "BITCOIN : Cryptography , Economics , and the Future," 2013.

[22] A. Piccolo, "Distributed ledger technology in the capital market Shared versus private information in a permissioned blockchain," 2017.
[23] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, no. November, pp. 395–411, 2018.
[24] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, Technology, and Governance," vol. 29, no. 2, pp. 213–238, 2015.
[25] S. Electronics Laboratories and R. C. Merkle, "I Nformat I on Systems Laboratory Secrecy, Authentication, and Public Key Systems," 1979.
[26] G. Becker, "Merkle Signature Schemes," p. 28, 2008.
[27] C. Decker and R. Wattenhofer, "Information Propagation in the Bitcoin Network," *13-th IEEE Int. Conf. Peer-to-Peer Comput.*, p. 10, 2013.
[28] V. Melnychuk, "Ethereum Hard Forks Explained." [Online]. Available: https://applicature.com/blog/ethereum-fork.
[29] A. Kiayias, A. Miller, and D. Zindros, "Non-Interactive Proofs of Proof-of-Work," *IACR Cryptol. ePrint Arch.*, p. 963, 2017.
[30] A. Zamyatin, N. Stifter, A. Judmayer, P. Schindler, E. R. Weippl, and W. J. Knottenbelt, "(Short Paper) A Wild Velvet Fork Appears! Inclusive Blockchain Protocol Changes in Practice.," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 87, 2018.
[31] M. N. O. Sadiku, K. G. Eze, S. M. Musa, R. G. Perry, P. V. A, and P. View, "Smart Contracts : A Primer," *J. Sci. Eng. Res.*, no. June, 2018.
[32] B. K. Mohanta, S. S. Panda, and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," *2018 9th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2018*, no. November, pp. 1–4, 2018.
[33] I. Eyal and E. G. Sirer, "Majority is not enough: bitcoin mining is vulnerable," *Communications of the ACM*, vol. 61, no. 7, New York, USA, pp. 95–102, 2018.
[34] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Draft Blockchain Technology Overview (NISTIR-8202)," *Natl. Inst. Stand. Technol.*, p. 59, 2018.
[35] S. King and S. Nadal, "Peercoin-Paper," 2012.
[36] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2 Pavel," *Self-published*, 2014.
[37] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9604 LNCS, no. 240258, pp. 142–157, 2016.
[38] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10401 LNCS, pp. 357–388, 2017.
[39] V. Buterin and V. Griffith, "Casper the Friendly Finality Gadget," pp. 1–10, 2017.
[40] M. Kramer, "Ethereum Casper Update Expected in 2019, Sharding in 2020," 2018. [Online]. Available: https://unhashed.com/cryptocurrency-news/ethereum-sharding-update-expected-2020/.
[41] I. Grigg, "EOS - An Introduction," no. ii, pp. 1–8, 2017.
[42] F. Schuh and D. Larimer, "Bitshares 2.0: Financial Smart Contract Platform," *Bitshares Financ. Platf.*, p. 12, 2015.
[43] "EOS Network Monitor - by CryptoLions." [Online]. Available: https://eosnetworkmonitor.io/. [Accessed: 02-Mar-2019].

[44] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017.

[45] NEM, "Distributed Ledger Technology (Blockchain)» Foundation." [Online]. Available: https://nem.io/technology/. [Accessed: 17-Apr-2019].

[46] E. Lavrova, "Deloitte and Waves Platform to shape the future of blockchain," 2017. [Online]. Available: https://blog.wavesplatform.com/deloitte-cis-and-waves-platform-to-shape-the-future-of-blockchain-674e17c3b067.

[47] "Leased Proof of Stake (LPoS)." [Online]. Available: https://docs.wavesplatform.com/en/platform-features/leased-proof-of-stake-lpos.html.

[48] G. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018.

[49] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of Activity," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.

[50] M. Salimitari and M. Chatterjee, "A Survey on Consensus Protocols in Blockchain for IoT Networks," 2018.

[51] "Hyperledger Sawtooth." [Online]. Available: https://www.hyperledger.org/projects/sawtooth.

[52] F. McKeen *et al.*, "Innovative instructions and software model for isolated execution," pp. 1–1, 2013.

[53] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10616 LNCS, pp. 282–297, 2017.

[54] "Slimcoin A Peer-to-Peer Crypto-Currency with Proof-of-Burn "Mining without Powerful Hardware"," 2014.

[55] A. Shoker, "Sustainable blockchain through proof of exercise," *2017 IEEE 16th Int. Symp. Netw. Comput. Appl. NCA 2017*, vol. 2017-Janua, pp. 1–9, 2017.

[56] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of Luck: an Efficient Blockchain Consensus Protocol," pp. 2–7, 2017.

[57] G. Ateniese, I. Bonacina, A. Faonio, and N. Galesi, "Proofs of Space: When Space Is of the Essence," pp. 538–557, 2014.

[58] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Poster: Proofs of space," pp. 1–2.

[59] J. Alwen, G. Fuchsbauer, P. Gazi, S. Park, and K. Pietrzak, "Spacecoin : A Cryptocurrency Based on Proofs of Space," *IACR Cryptol. ePrint Arch.*, pp. 1–26, 2015.

[60] S. Gauld, F. Von Ancoina, and R. Stadler, "The Burst Dymaxion An Arbitrary Scalable, Energy Efficient and Anonymous Transaction Network Based on Colored Tangles," *CryptoGuru PoC SIG*, pp. 2017–12, 2017.

[61] S. Gupta and M. Sadoghi, "Blockchain Transaction Processing," *Encycl. Big Data Technol.*, pp. 366–376, 2019.

[62] J. Yang, M. Onik, N.-Y. Lee, M. Ahmed, and C.-S. Kim, "Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making," *Appl. Sci.*, vol. 9, no. 7, p. 1370, 2019.

[63] G. Greenspan, "Scaling blockchains with off-chain data | MultiChain," *MultiChain*, 2018. [Online]. Available: https://www.multichain.com/blog/2018/06/scaling-blockchains-off-chain-data/.

[Accessed: 19-May-2019].
[64] "INJE UNIVERSITY HAEUNDAE PAIK HOSPITAL." [Online]. Available: http://haeundae.paik.ac.kr/eng/main/main.asp. [Accessed: 19-May-2019].
[65] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services," *IEEE Trans. Serv. Comput.*, vol. 1374, no. c, pp. 1–14, 2018.
[66] M. Bakhoff, "Consensus Algorithms for Distributed Systems," *2010 Free. Annu. Conf.*, pp. 222–225, 2010.
[67] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," *CEUR Workshop Proc.*, vol. 2058, pp. 1–11, 2018.
[68] Parity Technologies, "Blockchain Infrastructure for the Decentralised Web | Parity Technologies," 2018. [Online]. Available: https://www.parity.io/. [Accessed: 23-Apr-2019].
[69] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," *2019 IEEE Int. Conf. Consum. Electron. ICCE 2019*, pp. 1–5, 2019.
[70] G. Ateniese *et al.*, "Provable data possession at untrusted stores," p. 598, 2007.
[71] M. B. Jones, "The Increasing Importance of Proof-of-Possession to the Web," 2014.
[72] F. Knirsch, A. Unterweger, K. Karlsson, D. Engel, and S. B. Wicker, "Evaluation of a Blockchain-Based Proof-of-Possession Implementation," vol. 865082, no. 865082, 2018.
[73] N. Asokan, V. Niemi, and P. Laitinen, "On the Usefulness of Proof-of-Possession," *Proc. 2nd Annu. {PKI} Res. Work.*, pp. 122–127, 2003.
[74] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain," *Proc. - 2017 IEEE 19th Intl Conf. High Perform. Comput. Commun. HPCC 2017, 2017 IEEE 15th Intl Conf. Smart City, SmartCity 2017 2017 IEEE 3rd Intl Conf. Data Sci. Syst. DSS 2017*, vol. 2018-Janua, no. December, pp. 466–473, 2018.
[75] M. Ghosh, M. Richardson, B. Ford, and R. Jansen, "A TorPath to TorCoin:Proof-of-Bandwidth Altcoins for Compensating Relays," vol. 2014.
[76] R. Dingledine, "Tor-Design," p. 17, 2004.
[77] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," no. February, pp. 1–14, 1999.
[78] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," *2017 IEEE Int. Conf. Syst. Man, Cybern. SMC 2017*, vol. 2017-Janua, pp. 2567–2572, 2017.
[79] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9591, pp. 112–125, 2016.
[80] "Hyperledger Fabric." [Online]. Available: https://www.hyperledger.org/projects/fabric.
[81] "Linux Foundation." [Online]. Available: https://www.linuxfoundation.org/. [Accessed: 09-Sep-2018].
[82] A. Hyperledger, "Hyperledger Blockchain Performance Metrics."
[83] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The Honey Badger of BFT Protocols," no. Section 3, pp. 31–42, 2016.
[84] "NEO White Paper." [Online]. Available: https://docs.neo.org/en-

us/whitepaper.html. [Accessed: 24-Feb-2019].
[85] I. M. Coelho, V. N. Coelho, P. Lin, and E. Zhang, "Chapter 8 – Delegated Byzantine Fault Tolerance : Technical details , challenges and perspectives," 2019.
[86] Y. Wang *et al.*, "Study of Blockchains's Consensus Mechanism Based on Credit," *IEEE Access*, vol. 7, pp. 10224–10231, 2019.
[87] G. S. Samman, "Chain: Simplified Byzantine Fault Tolerance (SBFT)," *SAMMANTICS*, 2016.
[88] D. Schwartz, N. Youngs, and A. Britto, "The Ripple protocol consensus algorithm," *Ripple Labs Inc White Pap.*, pp. 1–8, 2014.
[89] "RippleNet One frictionless experience to send money globally."
[90] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Dev. Found.*, pp. 1–45, 2015.
[91] A. Baliga, "Understanding Blockchain Consensus Models," *Whitepaper*, no. April, pp. 1–14, 2017.
[92] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," *2017 4th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2017*, 2017.
[93] J. Debus, "Consensus Methods in Blockchain Systems," *FSBC Work. Pap.*, no. May, pp. 1–58, 2017.
[94] M. Kim, Y. Kwon, and Y. Kim, "Is Stellar As Secure As You Think?," vol. 5, 2019.
[95] "Stellar meetup in Singapore - Announcements - Stellar Community Forum." [Online]. Available: https://stellarcommunity.org/t/stellar-meetup-in-singapore/1665/2. [Accessed: 07-Mar-2019].
[96] Bitcoin.org, "Orphan Block." [Online]. Available: https://www.investopedia.com/terms/o/orphan-block-cryptocurrency.asp. [Accessed: 09-Mar-2019].
[97] "Latency and finality in different cryptocurrencies – Hacker Noon." [Online]. Available: https://hackernoon.com/latency-and-finality-in-different-cryptocurrencies-a7182a06d07a. [Accessed: 09-Mar-2019].
[98] "Blockchain Finality In IoT – Coinmonks – Medium." [Online]. Available: https://medium.com/coinmonks/blockchain-finality-in-iot-79e466406133. [Accessed: 20-Mar-2019].
[99] A. Mohaisen and J. Kim, "The Sybil Attacks and Defenses: A Survey," no. December 2013, 2013.
[100] V. Buterin, "Proof of Stake: How I Learned to Love Weak Subjectivity." [Online]. Available: https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/. [Accessed: 22-Mar-2019].
[101] Digiconomist, "Bitcoin Energy Consumption Index," *Digiconomist*. pp. 1–8, 2018.
[102] Digiconomist, "Ethereum Energy Consumption Index (beta) - Digiconomist," *Digiconomist*. 2018.
[103] N. Christin and R. Safavi-Naini, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8437, pp. 436–454, 2014.
[104] A. Miller, A. Kosba, J. Katz, and E. Shi, "Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions," pp. 680–691, 2015.
[105] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "This paper is included in the Proceedings of the 26th USENIX Security Symposium SmartPool: Practical

Decentralized Pooled Mining SMARTPOOL: Practical Decentralized Pooled Mining," 2017.
[106] S. S. Shetty, C. A. Kamhoua, and L. L. Njilla, *Blockchain for Distributed Systems Security*. 2019.
[107] E. Armknecht, F., Karame, G. O., Mandal, A., Youssef, F., & Zenner, "Ripple: Overview and outlook," in *Trust and Trustworthy Computing - 8th International Conference, TRUST 2015, Proceedings*, 2015, vol. 9229, pp. 163–180.
[108] B. Chase and E. Macbrough, "Analysis of the XRP Ledger Consensus Protocol," pp. 1–25, 2018.
[109] V. Buterin, "Notes on Scalable Blockchain Protocols," pp. 1–40, 2015.
[110] K. Croman *et al.*, "On scaling decentralized blockchains (A position paper)," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9604 LNCS, pp. 106–125, 2016.
[111] "(3) BeyondBlock Taipei 2017 | Afternoon - YouTube." [Online]. Available: https://www.youtube.com/watch?v=9RtSod8EXn4. [Accessed: 10-Apr-2019].
[112] "Whiteblock completes industry's first EOS benchmark testing and blockchain investigation." [Online]. Available: https://www.prnewswire.com/news-releases/whiteblock-completes-industrys-first-eos-benchmark-testing-and-blockchain-investigation-300742130.html. [Accessed: 06-May-2019].
[113] G. Hileman and M. Rauchs, "2017 Global Blockchain Benchmarking Study," *Ssrn*, 2017.
[114] Bitfury Group and J. Garzik, "Public versus Private Blockchains. Part 2: Permissionless Blockchains," *Bitfury*, pp. 1–23, 2015.
[115] BitFury Group and J. Garzik, "Public versus Private Blockchains. Part 1: Permissioned Blockchains," *Bitfury*, pp. 1–23, 2015.
[116] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.
[117] F. Olleros, M. Zhegu, and M. Pilkington, "Blockchain technology: principles and applications," *Res. Handb. Digit. Transform.*, pp. 225–253, 2016.
[118] D. John R, "The Sybil Attack," p. 6.
[119] K. Alachkar and D. Gaastra, "Blockchain-based Sybil Attack Mitigation : A Case Study of the I2P Network," 2018.
[120] J. H. Mosakheil, "Security Threats Classification in Blockchains," *Culminating Proj. Inf. Assur.*, 2018.
[121] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Systematic Overview," pp. 1–30, 2019.
[122] learncrytography.com, "Learn Cryptography - 51% Attack," *learncrytography.com*. [Online]. Available: https://learncryptography.com/cryptocurrency/51-attack. [Accessed: 02-Jul-2019].
[123] S. Sayeed and H. Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, 2019.
[124] J. J. Xu, "Are blockchains immune to all malicious attacks?," *Financ. Innov.*, vol. 2, no. 1, 2016.
[125] J. J. Roberts, "Bitcoin Gold Suffers Rare '51% Attack' | Fortune," *Fortune*, 2018. [Online]. Available: https://fortune.com/2018/05/29/bitcoin-gold-hack/. [Accessed: 02-Jul-2019].
[126] A. Hertig, "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular -

CoinDesk," *Coindesk*, 2018. [Online]. Available: https://telegra.ph/Blockchains-Once-Feared-51-Attack-Is-Now-Becoming-Regular-06-08. [Accessed: 02-Jul-2019].
[127] S. Shanaev, A. Shuraeva, M. Vasenin, and M. Kuznetsov, "Cryptocurrency value and 51% attacks: evidence from event studies," p. 43, 2018.
[128] A. Miller, A. Kosba, J. Katz, and E. Shi, "Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions," pp. 680–691, 2015.
[129] M. Bastiaan, "Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin," *Proc. 22nd Twente Student Conf. IT*, 2015.
[130] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajković, "Distributed denial of service attacks," *Proc. IEEE Int. Conf. Syst. Man Cybern.*, vol. 3, no. December 2014, pp. 2275–2280, 2000.
[131] "World's Largest Bitcoin Exchange Bitfinex Crippled by DDoS - Infosecurity Magazine." [Online]. Available: https://www.infosecurity-magazine.com/news/worlds-largest-bitcoin-exchange/. [Accessed: 04-Jul-2019].
[132] "Bitcoin Trader Hit By "Severe DDoS Attack" as Bitcoin Price Nears All-Time High." [Online]. Available: https://www.bleepingcomputer.com/news/security/bitcoin-trader-hit-by-severe-ddos-attack-as-bitcoin-price-nears-all-time-high/. [Accessed: 04-Jul-2019].
[133] J. Wilcke, "The Ethereum network is currently undergoing a DoS attack," *Ethereum Blog*, 2016. [Online]. Available: https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/. [Accessed: 04-Jul-2019].
[134] "Ethereum Responds to Recent DDoS Attack." [Online]. Available: https://www.ccn.com/ethereum-responds-to-recent-ddos-attack/. [Accessed: 04-Jul-2019].
[135] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8438, pp. 57–71, 2014.
[136] "Bitcoin Mining Pools Targeted in Wave of DDOS Attacks." [Online]. Available: https://www.coindesk.com/bitcoin-mining-pools-ddos-attacks. [Accessed: 04-Jul-2019].
[137] M. Saad, M. T. Thai, and A. Mohaisen, "POSTER: Deterring DDoS attacks on blockchain-based cryptocurrencies through mempool optimization," *ASIACCS 2018 - Proc. 2018 ACM Asia Conf. Comput. Commun. Secur.*, pp. 809–811, 2018.
[138] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against bitcoin mining pools," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8438, pp. 72–86, 2014.
[139] C. Dietzel and M. Wichtlhuber, "Stellar : Network Attack Mitigation using Advanced Blackholing," *ACM Conex.*, no. iv, pp. 152–164, 2018.
[140] E. Osterweil, A. Stavrou, and L. Zhang, "20 Years of DDoS: a Call to Action," vol. 1, no. 1, pp. 1–11, 2019.
[141] I. Dilhani and T. N., "Transaction Verification Model over Double Spending for Peer-to-Peer Digital Currency Transactions based on Blockchain Architecture," *Int. J. Comput. Appl.*, vol. 163, no. 5, pp. 24–31, 2017.
[142] Z. Peng and Y. Chen, "All roads lead to Rome: Many ways to double spend

your cryptocurrency," pp. 1–12, 2018.
[143] H. Anwar, "46.Consensus Algorithms: The Root Of The Blockchain Technology," -, 2018. [Online]. Available: https://101blockchains.com/consensus-algorithms-blockchain/#prettyPhoto. [Accessed: 06-Jul-2019].
[144] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," *Proc. 2017 IEEE Symp. Secur. Priv. (SP)*, 2017.
[145] Q. Jacquemart, "Towards uncovering BGP hijacking attacks," 2016.
[146] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse Attacks on Bitcoin{\textquoteright}s Peer-to-Peer Network," *USENIX Secur. Symp.*, pp. 129–144, 2015.
[147] W. Karl and A. Gervais, "Ethereum Eclipse Attacks," *Doi.Org*, pp. 1–7, 2016.
[148] W. Li, G. Karame, S. Andreina, and J.-M. Bohli, "Securing Proof-of-Stake Blockchain Protocols Wenting," *Lect. Notes Comput. Sci.*, 2017.
[149] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, "A survey on long-range attacks for proof of stake protocols," *IEEE Access*, vol. 7, no. February, pp. 28712–28725, 2019.
[150] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Futur. Gener. Comput. Syst.*, no. Xiaoqi Li, pp. 1–25, 2017.
[151] N. Rathod and D. Motwani, "Security threats on Blockchain and its countermeasures," *Int. Res. J. Eng. Technol.*, vol. 05, no. 11, pp. 1636–1642, 2018.
[152] A. Gervais, K. Wüst, and H. Ritzdorf, "On the Security and Performance of Proof of Work Blockchains."
[153] VISA, "Small Business Retail | Visa," 2018. [Online]. Available: https://usa.visa.com/run-your-business/small-business-tools/retail.html. [Accessed: 15-Sep-2018].
[154] J. Vermeulen, "Bitcoin and Ethereum vs Visa and PayPal – Transactions per second," *MyBroadband*, 2017. [Online]. Available: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html. [Accessed: 15-Sep-2018].
[155] G. Bracha, "An O(log n) Expected Rounds Randomized Byzantine Generals Protocol," *Jacm*, vol. 34, no. 4, pp. 910–920, 1987.
[156] Y. Sompolinsky and A. Zohar, "Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains," *IACR Cryptol. ePrint Arch.*, vol. 881, pp. 1–31, 2013.
[157] L. Luu, J. Teutsch, R. Kulkarni, and P. Saxena, "Demystifying Incentives in the Consensus Computer," *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. - CCS '15*, pp. 706–719, 2015.
[158] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," 2015.
[159] G. Pernul, P. Y. A. Ryan, E. W. Eds, and D. Hutchison, *Computer Security – ESORICS 2015*. 2015.
[160] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.
[161] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille, "Simple Schnorr Multi-Signatures with Applications to Bitcoin," pp. 1–35, 2018.
[162] "Funny Name or Not, Schnorr Is a Big Deal for Bitcoin - CoinDesk." [Online]. Available: https://www.coindesk.com/schnorr-signatures-explained-bitcoin-

tech. [Accessed: 07-Aug-2018].
[163] M. Drijvers and G. Neven, "Okamoto Beats Schnorr : On the Provable Security of Multi-Signatures," 2018.
[164] D. J. Bernstein, "Multi-user Schnorr security, revisited," pp. 1–19, 2015.
[165] A. Back, M. Corallo, and L. Dashjr, "Enabling blockchain innovations with pegged sidechains," *URL http//www.*, pp. 1–25, 2014.
[166] Sergio Demian Lerner (RSK Labs), "Drivechains, Sidechains, and Hybrid 2-Way Peg Designs," *Rootstock*, 2016.
[167] A. Bstract, "(19) United States (12) Patent Application Publication," vol. 1, no. 12, 2002.
[168] G. Maxwell, "Bringing New Elements to Bitcoin with Sidechains," *San Fr. Bitcoin Dev. Meetup*, 2015.
[169] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," *Tech. Rep.*, p. 59, 2016.
[170] "Bitcoin's Lightning Network Could Play Havoc With The Bitcoin Price." [Online]. Available: https://www.forbes.com/sites/billybambrough/2018/07/06/bitcoins-lightning-network-could-play-havoc-with-the-bitcoin-price/#6959bdce7f1a. [Accessed: 07-Aug-2018].
[171] "Lightning Network DDoS Sends 20% of Nodes Down." [Online]. Available: https://www.trustnodes.com/2018/03/21/lightning-network-ddos-sends-20-nodes. [Accessed: 07-Aug-2018].
[172] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena, "SCP: A Computationally-Scalable Byzantine Consensus Protocol For Blockchains," *IACR Cryptol. ePrint Arch. 2015*, p. 1168, 2015.
[173] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A Secure Sharding Protocol For Open Blockchains," *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS'16*, pp. 17–30, 2016.
[174] J. Poon and V. Buterin, "Plasma : Scalable Autonomous Smart Contracts Scalable Multi-Party Computation," *Whitepaper*, pp. 1–47, 2017.
[175] "Blockchains and the Scalability Problem." [Online]. Available: https://cryptopotato.com/blockchains-and-the-scalability-problem/. [Accessed: 09-Aug-2018].
[176] "Plasma — Layer 2 Scaling protocol - Coinmonks - Medium." [Online]. Available: https://medium.com/coinmonks/plasma-layer-2-scaling-protocol-5a1263d86bc8. [Accessed: 09-Aug-2018].
[177] B. T. AG, "Raiden Network," 2019. [Online]. Available: https://raiden.network/101.html. [Accessed: 09-Aug-2018].
[178] "The model Raiden Network used for the NEO called Trinity. : raidennetwork." [Online]. Available: https://www.reddit.com/r/raidennetwork/comments/7qejqd/the_model_raiden_network_used_for_the_neo_called/. [Accessed: 10-Aug-2018].
[179] "Trinity." [Online]. Available: https://trinity.tech/blog/index.html?id=2#/. [Accessed: 15-Aug-2018].
[180] "Brave New Coin." [Online]. Available: https://bravenewcoin.com/news/raiden-lightning-and-plasma-arent-the-only-contenders-in-crypto-speed-battle. [Accessed: 11-Aug-2018].
[181] L. Glendenning, I. Beschastnikh, A. Krishnamurthy, and T. Anderson, "Scalable consistency in Scatter," *Proc. Twenty-Third ACM Symp. Oper. Syst. Princ. - SOSP '11*, p. 15, 2011.

[182] J. C. Corbett *et al.*, "Spanner : Google's Globally-Distributed Database," *Proc. OSDI'12 Tenth Symp. Oper. Syst. Des. Implement.*, pp. 251–264, 2012.
[183] G. Georgiev, "Vitalik Buterin: Sharding and Plasma Could Scale Ethereum by 10,000x," *www.bitcoinist.com*, 2018. [Online]. Available: https://bitcoinist.com/vitalik-buterin-sharding-plasma-scale-ethereum-10000-times/. [Accessed: 16-Aug-2018].
[184] "sharding/doc.md at develop · ethereum/sharding · GitHub." [Online]. Available: https://github.com/ethereum/sharding/blob/develop/docs/doc.md. [Accessed: 17-Aug-2018].
[185] G. Danezis and S. Meiklejohn, "Centrally Banked Cryptocurrencies," no. February, pp. 21–24, 2015.
[186] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger.," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 406, 2017.
[187] E. Syta *et al.*, "Scalable Bias-Resistant Distributed Randomness," *Proc. - IEEE Symp. Secur. Priv.*, pp. 444–460, 2017.
[188] M. Zamani, P. Alto, M. Movahedi, P. Alto, M. Raykova, and N. Haven, "RapidChain: A Fast Blockchain Protocol via Full Sharding," pp. 1–31.
[189] O. Street and M. J. Freedman, "Commensal Cuckoo : Secure Group Partitioning for Large-Scale Services," *LADIS Work.*, no. 1, p. 6, 2011.
[190] I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, "Design of the Blockchain Smart Contract: A Use Case for Real Estate," *J. Inf. Secur.*, vol. 09, no. 03, pp. 177–190, 2018.
[191] K. Zhang and H. A. Jacobsen, "Towards dependable, scalable, and pervasive distributed ledgers with blockchains," *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2018-July, pp. 1337–1346, 2018.
[192] M. Swan, *Blockchain-Blueprint for a New Economy*. .
[193] F. Lamberti, V. Gatteschi, C. Demartini, C. Pranteda, and V. Santamaria, "Blockchain or not blockchain, that is the question of the insurance and other sectors," *IT Prof.*, 2017.
[194] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, I. Original, and T. Vieira, "A Case Study for Blockchain in Healthcare: " MedRec " prototype for electronic health records and medical research data MedRec: Using Blockchain for Medical Data Access and Permission Management," *IEEE Technol. Soc. Mag.*, pp. 1–13, 2016.
[195] C. Pirtle and J. Ehrenfeld, "Blockchain for Healthcare: The Next Generation of Medical Records?," *J. Med. Syst.*, vol. 42, no. 9, pp. 1–3, 2018.
[196] S. Albrecht, S. Reichert, J. Schmid, J. Strüker, D. Neumann, and G. Fridgen, "Dynamics of Blockchain Implementation - A Case Study from the Energy Sector," *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, pp. 3527–3536, 2018.
[197] M. B. Hoy, "An Introduction to the Blockchain and Its Implications for Libraries and Medicine," *Med. Ref. Serv. Q.*, vol. 36, no. 3, pp. 273–279, 2017.
[198] J. WANG, P. WU, X. WANG, and W. SHOU, "The outlook of blockchain technology for construction engineering management," *Front. Eng. Manag.*, vol. 4, no. 1, p. 67, 2017.
[199] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learn. Environ.*, vol. 5, no. 1, p. 1, 2018.
[200] D. Peters, J. Wetzlich, F. Thiel, and J. P. Seifert, "Blockchain applications for legal metrology," *I2MTC 2018 - 2018 IEEE Int. Instrum. Meas. Technol. Conf.*

Discov. New Horizons Instrum. Meas. Proc., pp. 1–6, 2018.
[201] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.
[202] P. Rizzo, "Sweden tests blockchain smart contracts for land registry," *URL http//www. coindesk. com/sweden-blockchain …*, 2016.
[203] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financ. Innov.*, vol. 2, no. 1, p. 24, 2016.
[204] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," *Proc. Second Int. Conf. Internet-of-Things Des. Implement. - IoTDI '17*, pp. 173–178, 2017.
[205] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment," *2018 IEEE Int. Conf. Inf. Reuse Integr.*, pp. 15–22, 2018.
[206] "Documentation/TechnicalWhitePaper.md at master · EOSIO/Documentation · GitHub." [Online]. Available: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md. [Accessed: 20-Aug-2018].
[207] "Delegated Proof-of-Stake Consensus | BitShares Blockchain." [Online]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/. [Accessed: 25-Aug-2018].
[208] "EOS [EOS] "should be doing 50,000 transactions per second in a few months", says Novogratz - AMBCrypto." [Online]. Available: https://ambcrypto.com/eos-50k-transactions-per-second-says-novogratz/. [Accessed: 26-Aug-2018].
[209] "Documentation/Roadmap.md at master · EOSIO/Documentation · GitHub." [Online]. Available: https://github.com/EOSIO/Documentation/blob/master/Roadmap.md. [Accessed: 26-Aug-2018].
[210] P. Barrett, "Zilliqa Technical Whitepaper," *Zilliqa*, pp. 1–8, 2017.
[211] X. Dong, "Highlights of fresh experimental results: testnet v0.5," *blog.zilliqa.com*, 2017. [Online]. Available: https://blog.zilliqa.com/highlights-of-fresh-experimental-results-testnet-v0-5-f72bcaefd21b. [Accessed: 28-Aug-2018].
[212] "About Zilliqa." [Online]. Available: https://zilliqa.com/about-us.html. [Accessed: 15-Aug-2018].
[213] C. C. R. Whitepaper, "'A new internet build in a virtual reality metaverse,'" pp. 1–49, 2019.
[214] J. Kwon, "TenderMint : Consensus without Mining," *the-Blockchain.Com*, vol. 6, pp. 1–10, 2014.
[215] L. Baird, M. Harmon, and P. Madsen, "Hedera: A Governing Council & Public Hashgraph Network," pp. 1–27, 2018.
[216] A. Extance, "the Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance," *Nature*, vol. 552, no. 7685, pp. 301–302, 2017.
[217] C. Cachin, "Architecture of the hyperledger blockchain fabric," *IBM Res.*, vol. July, 2016.
[218] M. Vukolić, "Rethinking Permissioned Blockchains," *Proc. ACM Work. Blockchain, Cryptocurrencies Contract. - BCC '17*, pp. 3–7, 2017.
[219] "Next Consensus Architecture Proposal · hyperledger-archives/fabric Wiki · GitHub." [Online]. Available: https://github.com/hyperledger-archives/fabric/wiki/Next-Consensus-Architecture-Proposal. [Accessed: 25-

Aug-2018].
[220] M. Valenta and P. Sandner, "Comparison of Ethereum, Hyperledger Fabric and Corda," 2017.
[221] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," *2017 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017*, 2017.
[222] "Chaincode for Developers — hyperledger-fabricdocs master documentation." [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.1/chaincode4noah.html. [Accessed: 25-Aug-2018].
[223] E. Androulaki *et al.*, "Cryptography and Protocols in Hyperledger Fabric," *Real-World Cryptogr. Conf. 2017*, 2017.
[224] M. D. Industry, "AION White Paper :," no. July, pp. 3–6, 2017.
[225] S. Popov, "The Tangle," *IOTA Whitepaper*, pp. 1–28, 2017.
[226] B. Kusmierz, "The first glance at the simulation of the Tangle : discrete model," pp. 1–10, 2017.
[227] "IN PA Extracting Tangle Properties in Continuous Time," 2018.
[228] Z. A. Lewenberg Y., Sompolinsky Y., *Inclusive Block Chain Protocols*. Springer, Berlin, Heidelberg, 2015.
[229] "The tangle vs blockchain: a comparison between IOTA and bitcoin | IG AU." [Online]. Available: https://www.ig.com/au/trading-opportunities/the-tangle-vs-blockchain--a-comparison-between-iota-and-bitcoin-180709. [Accessed: 29-Aug-2018].
[230] B. David, P. Gaži, A. Kiayias, and A. Russell, "Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10821 LNCS, pp. 66–98, 2018.
[231] V. Buterin, "On public and private Blockchains," *blog.ethereum.org*, pp. 1–4, 2015.
[232] EYGM Limited, "EY research: initial coin offerings (ICOs)," no. December, p. 44, 2017.
[233] M. Ali, R. Shea, J. Nelson, and M. J. Freedman, "Blockstack Technical Whitepaper Blockstack: A New Internet for Decentralized Applications," pp. 1–24, 2017.
[234] P. Thakkar, S. Nathan, and B. Vishwanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," pp. 1–17, 2018.
[235] M. Hearn, "Corda: A distributed ledger," *Whitepaper*, pp. 1–56, 2016.
[236] X. Xu *et al.*, "A Taxonomy of Blockchain-Based Systems for Architecture Design," *Proc. - 2017 IEEE Int. Conf. Softw. Archit. ICSA 2017*, pp. 243–252, 2017.
[237] A. Prashanth Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018.
[238] S. Gilbert and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services," *ACM SIGACT News*, vol. 33, no. 2, p. 51, 2002.
[239] E. Brewer, "Inktomi at a Glance Distributed Systems Understanding Boundaries Where ' s the state ? (not all locations are equal) Santa Clara Cluster Delivering High Availability," *Networks*, vol. 19, pp. 1–12, 2000.
[240] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on Blockchain technology? - A systematic review," *PLoS One*, vol.

11, no. 10, pp. 1–27, 2016.
[241] V. Gramoli, "On the Danger of Private Blockchains," no. ii, pp. 1–4, 2016.
[242] L. Lamport *et al.*, "In Search of an Understandable Consensus Algorithm," *Atc '14*, vol. 22, no. 2, pp. 305–320, 2014.
[243] E. Buchman, "Tendermint: Byzantine Fault Tolerance in the Age of Blockchains," p. 109, 2016.
[244] N. Zhumabekuly Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 5, pp. 1–1, 2016.
[245] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc.*, pp. 1545–1550, 2018.
[246] K. S. N. Murthy, "A Review of Blockchain Technology and Its Application in Internet of Things," *Int. J. Manag. Technol. Eng.*, vol. 8, no. XII, pp. 2714–2722, 2018.
[247] BitFury Group, "Proof of Stake versus Proof of Work," *BitFury Gr.*, vol. 2015, pp. 1–26, 2015.
[248] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," *ICOSST 2018 - 2018 Int. Conf. Open Source Syst. Technol. Proc.*, pp. 54–63, 2019.
[249] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and B. Hamida, "Consortium Blockchains: Overview, Applications and Challenges," *Int. J. Adv. Telecommun.*, vol. 11, no. 1&2, pp. 51–64, 2018.
[250] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," vol. 1, no. 1, 2019.
[251] S. Yang, "Interpretation of Consensus Mechanism in Block Chain and Its Future Development Trend," vol. 86, no. Cecs, pp. 441–446, 2018.