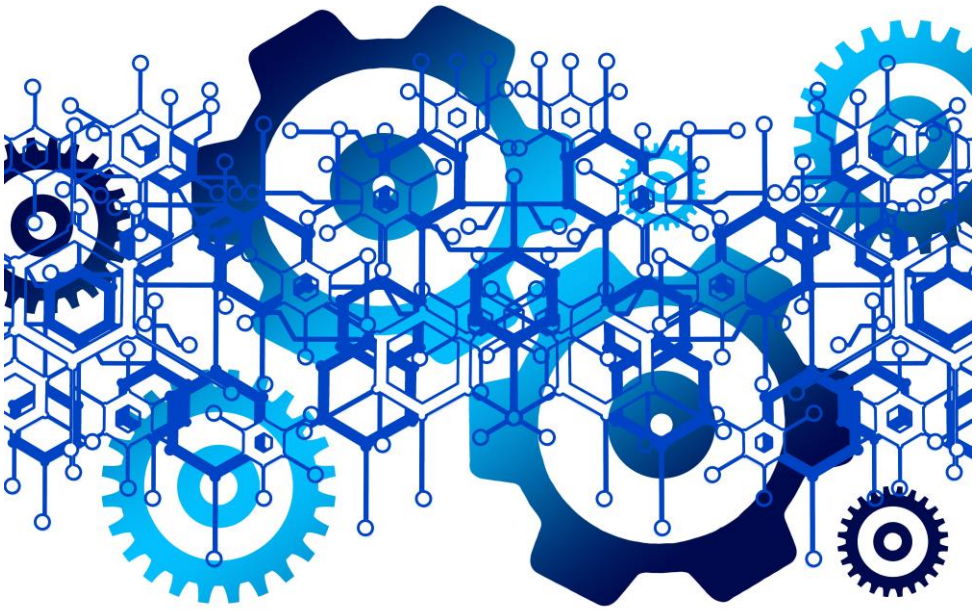
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Ανάλυση και Σύγκριση Μηχανισμών Συναίνεσης σε Blockchain Περιβάλλον



Φοιτητής: Παναγιώτης Τσεσμελής
ΑΜ: 50345070

Επιβλέπων Καθηγητής

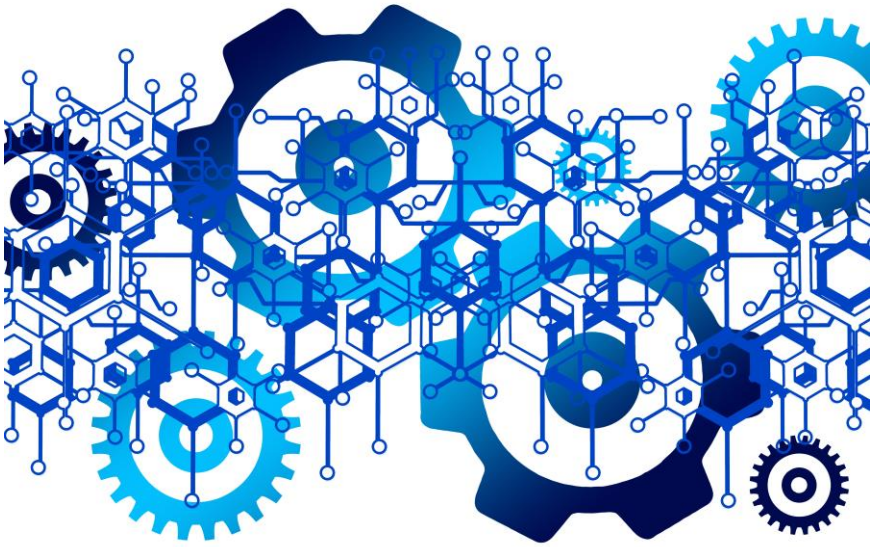
Γρηγόριος Κουλούρας
Αναπληρωτής Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, ΟΚΤΩΒΡΙΟΣ 2021

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

Diploma Thesis

Analysis and Comparison of Consensus Mechanisms in Blockchain Environment



Student: Panagiotis Tsesmelis
Registration Number: 50345070

Supervisor

Grigorios Koulouras
Associate Professor

ATHENS-EGALEO, OCTOBER 2021

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

Γρηγόριος Κουλούρας Αναπληρωτής Καθηγητής	**Ευάγγελος Ζέρβας** Καθηγητής	**Σωτήριος Καραμπέτσος** Αναπληρωτής Καθηγητής
Digitally signed by Grigorios Koulouras DN: c=GR, o=University of West Attica, ou=Class A - Private Key created and stored in hardware CSP, sn=Koulouras, givenName=Grigorios, serialNumber=5281068459, cn=Grigorios Koulouras, email=gregkoul@uniwa.gr Date: 2021.10.07 18:15:43 +03'00' (Υπογραφή)	Evangelos Zervas Digitally signed by Evangelos Zervas Date: 2021.10.07 11:02:13 +03'00' (Υπογραφή)	Sotirios Karampetsos Digitally signed by Sotirios Karampetsos Date: 2021.10.07 15:31:39 +03'00' (Υπογραφή)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Παναγιώτης Τσεσμελής του Σπυρίδων, με αριθμό μητρώου 50345070 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα ότι:

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

Ο Δηλών

ΤΣΕΣΜΕΛΗΣ ΠΑΝΑΓΙΩΤΗΣ;PANAGIOTIS TSESMELIS
Digitally signed by ΤΣΕΣΜΕΛΗΣ ΠΑΝΑΓΙΩΤΗΣ;PANAGIOTIS TSESMELIS
Date: 2021.10.07 10:44:14 +03'00'

Παναγιώτης Τσεσμελής

Περίληψη

Σύμφωνα με την κοινή γνώμη της πλειοψηφίας των επιστημόνων του συγκεκριμένου κλάδου, η τεχνολογία Blockchain αποτελεί ίσως την μεγαλύτερη "εφεύρεση" μετά το ίδιο το διαδίκτυο. Η δημοφιλέστερη εφαρμογή της που την έκανε γνωστή στον κόσμο το 2008 αποτέλεσε το κρυπτονόμισμα Bitcoin, ακολουθώντας στην συνέχεια στην δημιουργία ολοένα και περισσότερων εφαρμογών και κρυπτονομισμάτων βασισμένα στην συγκεκριμένη πρωτοπόρα τεχνολογία. Οι λόγοι που το Blockchain θεωρείται τόσο σημαντικό είναι το γεγονός ότι αποτελεί ένα διανεμημένο σύστημα ομότιμων κόμβων, με κρυπτογραφημένα στοιχεία, κάνοντας χρήση ψηφιακών υπογραφών, αλλά κυρίως η αποκεντρωμένη βάση του, η οποία προσφέρει ανωνυμία και αμεταβλητότητα, καθώς και βελτιστοποίηση στην διαδικασία της πραγματοποίησης συναλλαγών ανάμεσα στους χρήστες του. Οι εφαρμογές του όμως δεν περιορίζονται μόνο στον οικονομικό τομέα αλλά λόγω του συνεχούς πειραματισμού πολλών ατόμων πάνω σε αυτήν την τεχνολογία ανακαλύπτονται καθημερινά καινούργιες χρήσεις του, οι οποίες μπορούν να ωφελήσουν εταιρίες, πελάτες και απλούς χρήστες αντίστοιχα. Τον βασικότερο ρόλο όμως κατέχουν οι μηχανισμοί συναίνεσης, οι οποίοι θέτουν σε σωστή λειτουργία τους κόμβους του συστήματος κάνοντας χρήση ενός συνόλου αλγοριθμικών διαδικασιών και κανόνων, όπως σύνθετες μαθηματικές συναρτήσεις και διαδικασίες ψηφοφορίας ανάμεσα στους χρήστες.

Στην συγκεκριμένη διπλωματική εργασία θα γίνει μία συνοπτική ανάλυση της λειτουργίας της τεχνολογίας Blockchain, της δομής του Bitcoin αλλά και άλλων γνωστών κρυπτονομισμάτων, της αποκέντρωσης και των Blockchain συστημάτων. Θα επικεντρωθούμε περισσότερο όμως στην μελέτη των επικρατέστερων μηχανισμών συναίνεσης ως προς τον τρόπο εκτέλεσης των διαδικασιών τους και θα τους συγκρίνουμε μεταξύ τους ως προς την αποδοτικότητα τους. Σκοπός μας, έπειτα από βιβλιογραφική μελέτη, είναι ο αναγνώστης να κατανοήσει σωστά τον τρόπο λειτουργίας του Blockchain και των μηχανισμών του.

Λέξεις – κλειδιά

Blockchain, μηχανισμοί συναίνεσης, διανεμημένα δίκτυα, δίκτυα ομότιμων κόμβων, σύγχρονα και ασύγχρονα συστήματα, κρυπτογράφηση, συγκεντρωτισμός και αποκέντρωση, δημόσια-ιδιωτικά-κοινοπρακτικά συστήματα, ασφάλεια.

Abstract

According to the general opinion of the majority of scientists in this field, Blockchain technology is perhaps the greatest "invention" after the Internet itself. Its most popular application that made it known to the world in 2008 was the Bitcoin cryptocurrency, followed by the creation of more and more applications and cryptocurrencies based on this pioneering technology. The reasons Blockchain is considered so important is that it is a distributed system of peer nodes, with encrypted data, using digital signatures, but mainly its decentralized database, which offers anonymity and immutability, as well as optimization in the transaction process among its users. However, its applications are not limited only to the financial sector but due to the constant experimentation of many people on this technology, new uses are discovered every day which can benefit companies, customers and ordinary users respectively. The most important role, however, is played by the consent mechanisms, which put the nodes of the system into proper operation using a set of algorithmic procedures and rules, such as complex mathematical functions and voting procedures between users.

In this bachelor's thesis will be a brief analysis of the operation of Blockchain technology, the structure of Bitcoin and other known cryptocurrencies, decentralization and Blockchain systems. However, we will focus more on the study of the prevailing consensus mechanisms in terms of how their procedures are performed and will compare them with each other in terms of their efficiency. Our aim, after a bibliographic study, is for the reader to properly understand how Blockchain and its mechanisms work.

Keywords

Blockchain, consensus mechanisms, distributed networks, peer-to-peer networks, synchronous and asynchronous systems, cryptography, centralization and decentralization, public-private-consortium systems, security.

Περιεχόμενα

Κατάλογος Πινάκων 9

Κατάλογος Εικόνων 10

Αλφαβητικό Ευρετήριο 11

ΕΙΣΑΓΩΓΗ 12

Αντικείμενο της διπλωματικής εργασίας 12
Σκοπός και στόχοι 13
Μεθοδολογία 13
Καινοτομία 13
Δομή της διπλωματικής εργασίας 14

ΚΕΦΑΛΑΙΟ 1 : Χαρακτηριστικά Blockchain δικτύων 15

1.1 Τεχνολογία Διανεμημένων Κατάστιχων (Distributed Ledger Technology) 15
1.2 Κατηγορίες διανεμημένων δικτύων 16
1.2.1 Δίκτυα Πελάτη – Διακομιστή (Client – Server Networks) 16
1.2.2 Δίκτυα Ομότιμων Κόμβων (Peer-to-Peer Networks) 17
1.2.3 Υβριδικά Δίκτυα Ομότιμων Κόμβων (Hybrid Peer-to-Peer Networks) 18
1.2.4 Σφάλματα στα Διανεμημένα Συστήματα 19
1.3 Σύγχρονα και Ασύγχρονα Συστήματα 20
1.4 Κρυπτογράφηση (Cryptography) 21
1.4.1 Κρυπτογράφηση Δημοσίου Κλειδιού (Public Key Cryptography) 21
1.4.2 Ψηφιακή Υπογραφή (Digital Signature) 22
1.4.3 Συναρτήσεις Κατακερματισμού (One-way hash Functions) 22

ΚΕΦΑΛΑΙΟ 2 : Συγκεντρωτισμός και Αποκέντρωση 23

2.1 Συγκεντρωτικά Συστήματα (Centralized Systems) 23
2.2 Αποκεντρωμένα Συστήματα (Decentralized Systems) 23
2.3 Τύποι Συγκεντρωτισμού και Αποκέντρωσης 24

ΚΕΦΑΛΑΙΟ 3 : Μηχανισμοί Συναίνεσης (Consensus Mechanisms) 26

3.1 Proof of Work (PoW) 27
3.1.1 Λειτουργία 27
3.1.2 Block 29
3.1.3 Merkle Tree 30
3.1.4 Forks 31
3.2 Proof of Stake (PoS) 32
3.2.1 Μορφές Πρωτοκόλλων PoS 32
3.2.2 Delegated Proof of Stake (DPoS) 34
3.2.3 Leased Proof of Stake (LPoS) 35
3.2.4 Proof of Importance (PoI) 36
3.3 Υβριδικά Συστήματα (PoW/PoS) – Proof of Activity (PoA) 36
3.4 Proof of Elapsed Time (PoET) 37
3.5 Proof of Trust (PoT) 38
3.6 Proof of Vote (PoV) 40
3.7 Vote-based Consensus Mechanisms 41
3.8 Byzantine Fault Tolerance (BFT) 42
3.8.1 Practical Byzantine Fault Tolerance (PBFT) 42
3.8.2 Stellar Consensus Protocol (SCP) 44
3.8.3 Ripple Protocol Consensus Algorithm (RPCA) 45
3.9 Επιθέσεις και Ασφάλεια στο Blockchain 46
3.9.1 Long Range 46

3.9.2 Nothing at Stake **47**
3.9.3 51% **48**
3.9.4 Sybil **49**
3.9.5 Double-Spending **49**
3.9.6 Eclipse **50**
3.9.7 Distributed Denial of Service (DDoS) **50**
3.9.8 Border Gateway Protocol (BGP) **51**
3.10 Blockchain Συστήματα **51**
3.10.1 Δημόσια **52**
3.10.2 Ιδιωτικά **53**
3.10.3 Κοινοπρακτικά **54**
3.11 Χαρακτηριστικά Blockchain **55**
3.11.1 Εμπιστοσύνη **55**
3.11.2 Ομοφωνία **56**
3.11.3 Ταχύτητα συναλλαγών και έξοδα **56**
3.11.4 Ανωνυμία **57**
3.11.5 Ασφάλεια **58**
3.12 Σύγκριση Μηχανισμών Συναίνεσης **58**
3.12.1 Οριστικότητα **59**
3.12.2 Εμπιστοσύνη κόμβων **60**
3.12.3 Συναίνεση **60**
3.12.4 Δημιουργία επόμενου block **61**
3.12.5 Εχθρική ανοχή και ασφάλεια **62**
3.12.6 Δυνατότητα επέκτασης **63**
3.12.7 Άλλα κριτήρια σύγκρισης **64**
ΣΥΜΠΕΡΑΣΜΑΤΑ **65**

Κατάλογος Πινάκων

Πίνακας 1 - Ασφάλεια μηχανισμών συναίνεσης σε Long range επίθεση 47

Πίνακας 2 - Ασφάλεια μηχανισμών συναίνεσης σε Nothing at stake επίθεση 47

Πίνακας 3 - Ασφάλεια μηχανισμών συναίνεσης σε 51% επίθεση 48

Πίνακας 4 - Ασφάλεια μηχανισμών συναίνεσης σε Sybil επίθεση 49

Πίνακας 5 - Ασφάλεια μηχανισμών συναίνεσης σε Double-spending επίθεση 49

Πίνακας 6 - Ασφάλεια μηχανισμών συναίνεσης σε Eclipse επίθεση 50

Πίνακας 7 - Ασφάλεια μηχανισμών συναίνεσης σε Distributed Denial of Service επίθεση 51

Πίνακας 8 - Ασφάλεια μηχανισμών συναίνεσης σε Border Gateway Protocol επίθεση 51

Πίνακας 9 - Σύγκριση επιπέδου εμπιστοσύνης στα blockchain συστήματα 55

Πίνακας 10 - Μηχανισμοί ομοφωνίας στα blockchain συστήματα 56

Πίνακας 11 - Σύγκριση κόστους και ταχύτητας των blockchain συστημάτων 56

Πίνακας 12 - Σύγκριση απορρήτου στα blockchain συστήματα 57

Πίνακας 13 - Σύγκριση βαθμού ασφαλείας στα blockchain συστήματα 58

Πίνακας 14 - Σύγκριση οριστικότητας των δημοφιλέστερων εφαρμογών μηχανισμών συναίνεσης 59

Πίνακας 15 - Σύγκριση συναίνεσης των δημοφιλέστερων μηχανισμών συναίνεσης 61

Πίνακας 16 - Σύγκριση δυνατότητας επέκτασης των δημοφιλέστερων εφαρμογών των μηχανισμών συναίνεσης 63

Πίνακας 17 - Σύγκριση των δημοφιλέστερων μηχανισμών συναίνεσης 64

Κατάλογος Εικόνων

Εικόνα 1 - Διανεμημένο δίκτυο 16

Εικόνα 2 - Τοπολογία δικτύου Πελάτη-Διακομιστή 16

Εικόνα 3 - Τοπολογία δικτύου ομότιμων κόμβων 17

Εικόνα 4 - Τοπολογία υβριδικού δικτύου ομότιμων κόμβων 18

Εικόνα 5 - Κρυπτογράφηση δημοσίου κλειδιού 21

Εικόνα 6 - Συγκεντρωτικό δίκτυο 23

Εικόνα 7 - Αποκεντρωμένο δίκτυο 24

Εικόνα 8 - Παραγωγή Bitcoin διεύθυνσης 28

Εικόνα 9 - Δομή block 29

Εικόνα 10 - Δομή Merkle Tree 30

Εικόνα 11 - Παράδειγμα soft fork 31

Εικόνα 12 - Παράδειγμα hard fork 31

Εικόνα 13 - Λειτουργία αλγορίθμου Raft 40

Εικόνα 14 - Λειτουργία PBFT αλγορίθμου 43

Εικόνα 15 - Δύο Quorums διασταυρώνονται σε ένα 44

Εικόνα 16 - Διαδικασία επικύρωσης και επιβεβαίωσης αξίας 45

Εικόνα 17 - Δημόσιο blockchain σύστημα 52

Εικόνα 18 - Ιδιωτικό blockchain σύστημα 53

Εικόνα 19 - Κοινοπρακτικό blockchain σύστημα 54

Αλφαβητικό Ευρετήριο

Ακρωνύμιο	**Ετυμολογία**
DLT	Distributed Ledger Technology
P2P	Peer-to-Peer
PoW	Proof of Work
ECDSA	Elliptic Curve Digital Signature Algorithm
SHA-256	Secure Hash Algorithm 256 bit
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
LPoS	Leased Proof of Stake
PoI	Proof of Importance
PoA	Proof of Activity
PoET	Proof of Elapsed Time
SGX	Software Guard Extensions
PoUW	Proof of Useful Work
PoT	Proof of Trust
RPCs	Remote Procedure Calls
CFT	Crash Fault Tolerance
BFTF	Byzantine Fault Tolerance Failures
PoV	Proof of Vote
BFT	Byzantine Fault Tolerance
BA	Byzantine Agreement
PBFT	Practical Byzantine Fault Tolerance
SCP	Stellar Consensus Protocol
RPCA	Ripple Protocol Consensus Algorithm
UNL	Unique Node List
LCL	Last Closed Ledger
IP	Internet Protocol
DDoS	Distributed Denial of Service
BGP	Border Gateway Protocol
ISPs	Internet Service Providers
ASes	Autonomous Systems

ΕΙΣΑΓΩΓΗ

Η blockchain τεχνολογία θεωρείται μία από τις σημαντικότερες σύγχρονες καινοτομίες, με το Bitcoin να αποτελεί την δημοφιλέστερη εφαρμογή που την έκανε γνωστή στο ευρύ κοινό. Έπειτα, ολοένα και περισσότερες εφαρμογές ανά τα έτη βρίσκουν χρήσεις για την συγκεκριμένη τεχνολογία, με την πλειοψηφία παρόλα αυτά να αποτελούν ακόμα τα κρυπτονομίσματα. Αυτό οφείλεται στο γεγονός ότι το blockchain αποτελεί ένα κρυπτογραφημένο και αποκεντρωμένο σύστημα ομότιμων κόμβων, βελτιώνοντας την πραγματοποίηση συναλλαγών μεταξύ των χρηστών, ανώνυμα και αμετάβλητα. Ένα δίκτυο υπολογιστών που ακολουθεί την λογική των ομότιμων κόμβων διαμοιράζει ισοδύναμα τις εργασίες σε όλους τους χρήστες του, οι οποίοι έχουν ίσα δικαιώματα. Εκτός όμως από τα δίκτυα ομότιμων κόμβων που χρησιμοποιείται κυρίως στην δεδομένη περίπτωση, υπάρχουν και τα δίκτυα πελάτη-διακομιστή και τα υβριδικά. Στο blockchain τα δεδομένα προφυλάσσονται κυρίως μέσω της κρυπτογράφησης δημοσίου κλειδιού, σε συνδυασμό με τις ψηφιακές υπογραφές και τις συναρτήσεις κατακερματισμού. Ένα αποκεντρωμένο σύστημα κατανέμει τον έλεγχο σε περιφέρειες και όλοι οι χρήστες του δικτύου είναι υπεύθυνοι για την λήψη αποφάσεων. Υπάρχει όμως και μία ακόμη κατηγορία συστημάτων, η οποία χρησιμοποιούνταν κυρίως σε αποκλειστικότητα μέχρι και πριν μερικά χρόνια και αυτή είναι τα συγκεντρωτικά συστήματα. Ο πυρήνας όμως της συγκεκριμένης τεχνολογίας είναι ο εκάστοτε μηχανισμός συναίνεσης, ο οποίος οργανώνει τους κόμβους του δικτύου, μέσω διάφορων μορφών διαγωνισμών και ψηφοφοριών μεταξύ τους. Ορισμένοι από τους μηχανισμούς που θα αναλυθούν και θα συγκριθούν μεταξύ τους είναι οι Proof of Work, Proof of Stake, Proof of Activity, Proof of Elapsed Time, Proof of Trust, Proof of Vote, Practical Byzantine Fault Tolerance, Stellar Consensus Protocol, Ripple Protocol Consensus Algorithm. Η εφαρμογή της συγκεκριμένης τεχνολογίας δεν περιορίζεται μόνο στα κρυπτονομίσματα, αλλά με συνεχή πειραματισμό ολοένα και περισσότεροι χρήστες ανακαλύπτουν καινούργιες χρήσεις της σε διάφορους κλάδους.

Αντικείμενο της διπλωματικής εργασίας

Το κύριο θέμα της διπλωματικής εργασίας είναι η τεχνολογία blockchain, εμβαθύνοντας στους μηχανισμούς συναίνεσης της. Ένας αναγνώστης που δεν έχει σχέση με το συγκεκριμένο αντικείμενο και θα ενδιαφερθεί να μελετήσει την δεδομένη εργασία θα καταφέρει να μάθει και να κατανοήσει με απλά λογία τον τρόπο λειτουργίας του blockchain, καθώς στην συνέχεια και τους μηχανισμούς συναίνεσης του, για τους οποίους δίνεται μεγαλύτερη βαρύτητα. Από την άλλη πλευρά, ένας έμπειρος αναγνώστης του κλάδου θα έχει την ευκαιρία να μάθει μερικές ακόμη λεπτομέρειες για τα βασικά χαρακτηριστικά της συγκεκριμένης τεχνολογίας και θα ενημερωθεί για τις θεωρητικές και πρακτικές εξελίξεις στους μηχανισμούς συναίνεσης της, σύμφωνα με τα τωρινά δεδομένα. Επιπλέον, αποτελεί μια μελέτη στην οποία βρίσκονται συσσωρευμένες συγκρίσεις από διαφορές πλευρές για τους βασικότερους εν ενεργεία blockchain μηχανισμούς συναίνεσης. Με αυτόν τον τρόπο, οποιοσδήποτε επιθυμεί να ξεκινήσει από την αρχή ή να επεκτείνει τις γνώσεις του στην blockchain τεχνολογία, θα βρει κάτι ενδιαφέρον στην ακόλουθη διπλωματική εργασία, διευρύνοντας τις γνώσεις του.

Σκοπός και στόχοι

Η συγκεκριμένη διπλωματική εργασία συντάχθηκε με σκοπό την συμβολή στην επιστήμη σχετικά με την τεχνολογία blockchain και τους μηχανισμούς συναίνεσης της. Κατά την διάρκεια της ανάγνωσης της θα απαντηθούν ορισμένα ερωτήματα του χώρου, όπως η έννοια των διανεμημένων καταστίχων και δικτύων, τα σύγχρονα και ασύγχρονα συστήματα, ο συγκεντρωτισμός και η αποκέντρωση, καθώς και πολλούς από τους σημαντικότερους εν ενεργεία μηχανισμούς συναίνεσης με τις διαφορές τους. Αρχικά, ο αναγνώστης μελετώντας την θα κατανοήσει, με όσο το δυνατόν πιο απλές έννοιες και ορολογίες, τον γενικό τρόπο λειτουργίας του blockchain. Στην συνέχεια, θα περάσει στο κεφάλαιο της ανάλυσης των μηχανισμών συναίνεσης της συγκεκριμένης τεχνολογίας, όπου και περιγράφεται με σαφήνεια η δομή τους. Στο τελευταίο υποκεφάλαιο πραγματοποιούνται συγκρίσεις των βασικότερων μηχανισμών συναίνεσης σε διαφορετικούς τομείς σύμφωνα με τα δεδομένα των τελευταίων ετών. Με την ολοκλήρωση της διπλωματικής εργασίας στοχεύεται η επιμόρφωση του αναγνώστη ως προς την ραγδαία εξελισσόμενη blockchain τεχνολογία και η ενημέρωση του με τα νεότερα δεδομένα, σε θεωρητικό και πρακτικό επίπεδο, για τους μηχανισμούς συναίνεσης της και τις διαφοροποιήσεις μεταξύ τους.

Μεθοδολογία

Στην συγκεκριμένη διπλωματική εργασία, δεδομένου ότι πραγματοποιείται ανάλυση των μηχανισμών συναίνεσης της τεχνολογίας blockchain και στην συνέχεια σύγκριση μεταξύ τους, είναι απαραίτητη η άντληση πληροφοριών από έγκυρες και όσο το δυνατόν πιο πρόσφατα ενημερωμένες διεθνείς πηγές. Η βιβλιογραφία που χρησιμοποιήθηκε για την συγγραφή της εργασίας αποτελείται από άρθρα σε επιστημονικά περιοδικά, διεθνή συνέδρια και επιστημονικά βιβλία ή τμήματα αυτών. Για την υλοποίηση της ανάλυσης και της σύγκρισης των μηχανισμών συναίνεσης και της υπόλοιπης τεχνολογίας, ήταν απαραίτητο τόσο το θεωρητικό υπόβαθρο όσο και τα πρακτικά αποτελέσματα. Αυτό οφείλεται στο γεγονός ότι αρχικά πρέπει να μάθουμε για τον τρόπο λειτουργίας της τεχνολογίας blockchain. Στην συνέχεια, όταν περάσουμε στο τμήμα της ανάλυσης και σύγκρισης πιο συγκεκριμένων εννοιών πρέπει να γνωρίζουμε και τις θεωρητικές προδιαγραφές τους, αλλά και τα αποτελέσματα που προκύπτουν τελικά στην πράξη κατά της εφαρμογή τους σε πραγματικές συνθήκες χρήσης. Για αυτόν τον λόγο, όλες οι αναφορές είναι εγκεκριμένες από διεθνείς και παγκοσμίου φήμης επιστήμονες του χώρου και ανάλογους θεσμούς, ενώ καμία πηγή δεν είναι στα πλαίσια ερασιτεχνικής σύνταξης ή προπτυχιακής εργασίας. Στο τέλος της διπλωματικής εργασίας αναφέρεται αναλυτικά το σύνολο της βιβλιογραφίας που χρησιμοποιήθηκε για την σύνταξη της.

Καινοτομία

Η συγκεκριμένη διπλωματική εργασία αποτελεί μία συμβολή στην γνώση και στην επιστήμη μέσω της ενιαίας μελέτης της τεχνολογίας blockchain, εμβαθύνοντας στους μηχανισμούς συναίνεσης της. Μέσω αυτής, ο αναγνώστης μπορεί να κατανοήσει με όσο το δυνατόν πιο απλή επεξήγηση τον τρόπο λειτουργίας της συγκεκριμένης τεχνολογίας και των μηχανισμών της. Καθώς αποτελεί ενημέρωση για τις πιο πρόσφατες εξελίξεις στον συγκεκριμένο κλάδο, μέσω της σύγκρισης των μηχανισμών συναίνεσης, σε θεωρητικό και πρακτικό επίπεδο. Ο ενδιαφερόμενος με τον κλάδο αναγνώστης, κατά την ολοκλήρωση της συγκεκριμένης διπλωματικής εργασίας θα έχει αποκομίσει μία πιο εμπεριστατωμένη άποψη και γνώση πάνω σε αυτήν την τεχνολογία με τα σύγχρονα δεδομένα.

Δομή της διπλωματικής εργασίας

Στο πρώτο κεφάλαιο της διπλωματικής εργασίας αναφέρονται τα χαρακτηριστικά των blockchain δικτύων, καθώς και μια περιγραφή τους. Στο πρώτο υποκεφάλαιο αναλύεται η τεχνολογία διανεμημένων κατάστιχων. Στο δεύτερο περιγράφονται οι κατηγορίες στις οποίες χωρίζονται τα διανεμημένα δίκτυα, οι οποίες είναι τα δίκτυα πελάτη-διακομιστή, τα δίκτυα ομότιμων κόμβων και τα υβριδικά δίκτυα, ενώ στο τέλος αναφέρονται και ορισμένα σφάλματα που μπορούν τα προκύψουν. Στο τρίτο αναλύονται τα σύγχρονα και ασύγχρονα συστήματα και ο ρόλος τους. Στο τέταρτο και τελευταίο υποκεφάλαιο περιγράφεται συνοπτικά η κρυπτογράφηση που χρησιμοποιείται στην συγκεκριμένη τεχνολογία, αναφέροντας και ορισμένες μεθόδους που συντελείται η συγκεκριμένη διαδικασία, την κρυπτογράφηση δημοσίου κλειδιού, την ψηφιακή υπογραφή και τις συναρτήσεις κατακερματισμού.

Στο δεύτερο κεφάλαιο περιγράφονται οι όροι συγκεντρωτισμός και αποκέντρωση και η θέση τους στην τεχνολογία blockchain. Το πρώτο υποκεφάλαιο είναι μια ανάλυση των συγκεντρωτικών συστημάτων, ενώ το δεύτερο των αποκεντρωμένων συστημάτων. Το τρίτο αποτελεί μια αναφορά στους 3 τύπους που χωρίζονται τα συγκεκριμένα συστήματα με βάση το λογισμικό τους.

Στο τρίτο κεφάλαιο αναλύονται οι μηχανισμοί συναίνεσης, οι οποίοι αποτελούν τον πυρήνα της συγκεκριμένης τεχνολογίας. Στο πρώτο υποκεφάλαιο περιγράφεται ο μηχανισμός συναίνεσης Proof of Work και συγκεκριμένα η λειτουργία του, η δημιουργία των blocks του, τα Merkle trees και τα forks. Στο δεύτερο αναλύεται το Proof of Stake και οι πιο γνωστές μορφές πρωτοκόλλων του, το Delegated Proof of Stake, το Leased Proof of Stake και το Proof of Importance. Στο τρίτο γίνεται περιγραφή των υβριδικών συστημάτων, δηλαδή των μηχανισμών που αποτελούνται από συνδυασμό του PoW και του PoS, με έμφαση στο Proof of Activity. Στα επόμενα 3 υποκεφάλαιο γίνεται ανάλυση μερικών ακόμα μηχανισμών ως προς τον τρόπο λειτουργίας τους, του Proof of Elapsed Time, του Proof of Trust και του Proof of Vote. Στο έβδομο περιγράφονται οι Vote-based μηχανισμοί συναίνεσης και διαφοροποιούνται σε σχέση με τους προηγούμενους Proof-based μηχανισμούς. Στο όγδοο αναλύονται οι Byzantine Fault Tolerance μηχανισμοί και γίνεται περιγραφή των 3 κορυφαίων μηχανισμών αυτού του είδους, το Practical Byzantine Fault Tolerance, το Stellar Consensus Protocol και το Ripple Protocol Consensus Algorithm. Στο ένατο περιγράφεται η δυνατότητα ασφάλειας έναντι ορισμένων πιθανών επιθέσεων που μπορεί να δεχτεί ένα blockchain σύστημα και εξετάζονται οι 9 πιο γνωστές μορφές. Στο δέκατο αναφέρονται και διαχωρίζονται τα blockchain συστήματα σε 3 κατηγορίες, τα δημόσια, τα ιδιωτικά και τα κοινοπρακτικά. Στο ενδέκατο συγκρίνονται οι κατηγορίες των blockchain συστημάτων μεταξύ τους ως προς τα βασικά χαρακτηριστικά τους, δηλαδή την εμπιστοσύνη των κόμβων του δικτύου, την ομοφωνία τους στην λήψη αποφάσεων, την ταχύτητα πραγματοποίησης συναλλαγών και διεκπεραίωσης εξόδων, την ανωνυμία των χρηστών και την ασφάλεια της εφαρμογής. Στο δωδέκατο και τελευταίο υποκεφάλαιο πραγματοποιείται σύγκριση μεταξύ των βασικότερων μηχανισμών συναίνεσης ως προς τα πιο σημαντικά κριτήρια, όπως την οριστικότητα, την εμπιστοσύνη των κόμβων, την συναίνεση, τον τρόπο δημιουργίας του επομένου block, την ασφάλεια και την εχθρική ανοχή, τις δυνατότητες επέκτασης.

ΚΕΦΑΛΑΙΟ 1 : Χαρακτηριστικά Blockchain δικτύων

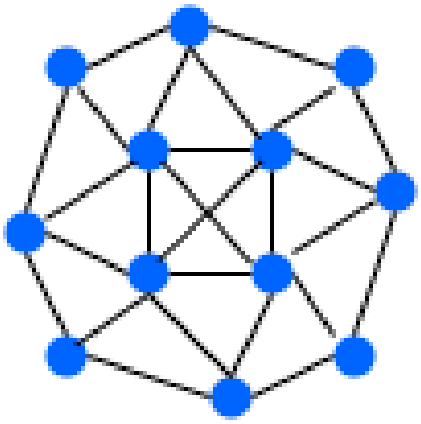
1.1 Τεχνολογία Διανεμημένων Κατάστιχων (Distributed Ledger Technology)

Ένα διανεμημένο κατάστιχο της τεχνολογίας Distributed Ledger Technology (DLT) αποτελεί ένα είδος βάσης δεδομένων η οποία διανέμεται σε όλο το δίκτυο ή σε πολλές τοποθεσίες, με την δυνατότητα να είναι δημόσιο. Σε αυτή τη βάση δεδομένων καταχωρούνται τα αρχεία των χρηστών και αποθηκεύονται σε σειρά σε ένα κατάστιχο (βιβλίο), με κάθε χρήστη του δικτύου να έχει στην κατοχή του ένα αντίγραφο αυτού του κατάστιχου [1]. Τα διανεμημένα κατάστιχα είναι πιο γενικός όρος από το blockchain, μιας και περιγράφουν μία διανεμημένη βάση δεδομένων, έτσι δεν είναι όλα τα διανεμημένα συστήματα blockchain, διότι το blockchain ανήκει σε αυτήν την τεχνολογία. Οι δύο αυτές τεχνολογίες διαφέρουν μεταξύ τους με βασικότερο να είναι το γεγονός ότι τα διανεμημένα δεν είναι απαραίτητο να περιέχουν blocks για συναλλαγές ώστε να μεγαλώσει το μέγεθος του κατάστιχου, ενώ στο blockchain είναι απαραίτητη η ύπαρξη τους μιας και είναι ένα ειδικό είδος βάσης δεδομένων αποτελούμενη από τέτοια blocks για τις συναλλαγές που πραγματοποιούνται. Μία εφαρμογή DLT χωρίς την χρήση blocks αποτελεί το Corda, όπου ειδικεύεται στις υπηρεσίες της οικονομικής βιομηχανίας καθώς είναι σχεδιασμένο να καταγράφει και να διαχειρίζεται συναλλαγές. Πιο γνωστή εφαρμογή DLT με χρήση blocks αποτελεί φυσικά το Bitcoin (BTC), όπου η διανεμημένη βάση δεδομένων του τα χρησιμοποιεί ώστε να ενημερώνεται ως προς την αυθεντικότητα, την κατάσταση και την σωστή χρονολογική σειρά των συναλλαγών που παίρνουν μέρος σε αυτή [2].

Τα διανεμημένα κατάστιχα κατά την κύρια λειτουργία τους και στην βασική τους μορφή εκτελούν μία διαδικασία στις blockchain εφαρμογές. Αρχικά, επιτυγχάνεται μέσω κοινής συναίνεσης μία συμφωνία ανάμεσα στους χρήστες του δικτύου, ανεξάρτητα μεσάζοντα. Στη συνέχεια μπορεί να πραγματοποιηθεί το ανέβασμα των καταστάσεων ή των αρχείων των χρηστών, τα οποία αποτελούν τα ψηφιακά τους στοιχεία, με διαφάνεια και δυνατότητα ελέγχου, καθώς και από την στιγμή που γίνουν μέρος του κατάστιχου θεωρούνται αμετάβλητα. Τέλος, από την στιγμή που οι συναλλαγές θεωρούνται αμετάβλητες, τα μέλη μπορούν να αλληλοεπιδράσουν ανώνυμα. Από την μία, η αμεταβλητότητα προσδίδει ανθεκτικότητα σε περίπτωση παραβίασης κατά τις συναλλαγές, από την άλλη, σε περίπτωση που χρειαστεί να βρεθεί ένα ή και τα δύο μέλη μίας συναλλαγής (π.χ. λόγω μίας παράνομης πώλησης), ο εντοπισμός τους είναι αδύνατος [3].

1.2 Κατηγορίες διανεμημένων δικτύων

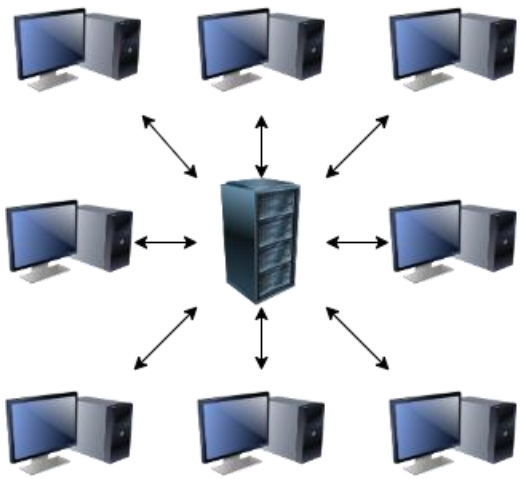
Οι χρήστες αποτελούν τους κόμβους (peers) του συστήματος και οργανώνονται με δύο διαφορετικούς τρόπους. Ο ένας είναι το μοντέλο πελάτη-διακομιστή (client-server model) και ο άλλος η αρχιτεκτονική δικτύων ομότιμων κόμβων ή αλλιώς Peer-to-Peer (P2P). Ωστόσο υπάρχει και μία τρίτη κατηγορία, τα υβριδικά δίκτυα ομότιμων κόμβων (hybrid P2P networks), που αποτελούν έναν συνδυασμό των προηγούμενων δύο [4].



Εικόνα 1 - Διανεμημένο δίκτυο

1.2.1 Δίκτυα Πελάτη – Διακομιστή (Client – Server Networks)

Τα διανεμημένα δίκτυα που αποτελούνται από έναν διακομιστή (server), δηλαδή ένα σύστημα υψηλής απόδοσης, σε συνδυασμό με τους εξυπηρετητές (clients), δηλαδή πολλά συστήματα χαμηλότερης απόδοσης, ονομάζονται δίκτυα πελάτη – διακομιστή. Ο διακομιστής αποτελεί τον μοναδικό πάροχο υπηρεσιών και περιεχομένου, καθώς και την κεντρική μονάδα εγγραφής, ενώ ο εξυπηρετητής δεν διαμοιράζεται τους πόρους του και ζητάει υπηρεσίες και περιεχόμενο. Ένας κόμβος της συγκεκριμένης κατηγορίας δικτύων έχει την δυνατότητα απομακρυσμένης σύνδεσης με τους διακομιστές και δεν απαιτείται από τους κόμβους χωρητικότητα στους δίσκους τους, ενώ αν είναι απαραίτητη οποιαδήποτε βελτίωση, τότε μόνο ο διακομιστής χρειάζεται να αναβαθμιστεί [5].



Εικόνα 2 - Τοπολογία δικτύου Πελάτη-Διακομιστή

1.2.2 Δίκτυα Ομότιμων Κόμβων (Peer-to-Peer Networks)

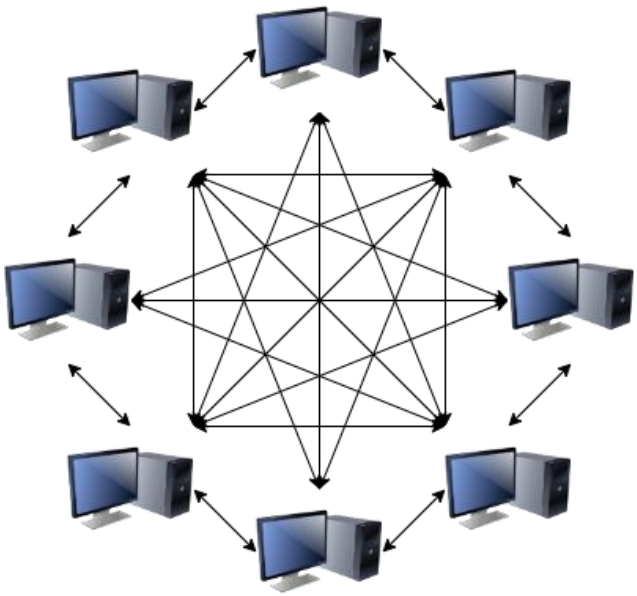
Ένα δίκτυο που επιτρέπει ισοδύναμα σε τουλάχιστον δύο υπολογιστές τον διαμοιρασμό των πόρων τους, χωρίς την βοήθεια κάποιου κεντρικού διακομιστή, ονομάζεται δίκτυο ομότιμων κόμβων. Οι κόμβοι του δικτύου, δηλαδή τα μέλη του, έχουν όλοι τα ίδια δικαιώματα και οι εργασίες χωρίζονται ισάξια. Ο κάθε χρήστης μπορεί να διαβάσει όλες τις πληροφορίες οποιουδήποτε κόμβου, αναλόγως τα δικαιώματα που θεσπίζονται.

Οι κόμβοι του δικτύου παρέχουν άμεσα σε άλλους κόμβους ένα μέρος των πόρων τους, χωρίς να είναι απαραίτητη η ύπαρξη κάποιου κεντρικού συντονιστή, όπως ενός διακομιστή. Αυτοί οι πόροι μπορεί να είναι εύρος ζώνης του δικτύου, υπολογιστική ισχύς ή και χώρος στο δίσκο. Σε αντίθεση με τα δίκτυα πελάτη – εξυπηρετητή, οι κόμβοι των P2P δικτύων μπορούν να είναι προμηθευτές αλλά και καταναλωτές ταυτόχρονα.

Η εφαρμογή που έκανε γνωστά τα P2P δίκτυα ήταν το Napster, όπου οι χρήστες της μπορούσαν να ανταλλάξουν και να διαμοιράσουν αρχεία, όπως συμπιεσμένα MPEG 3 audio αρχεία (MP3). Συγκεκριμένα, το Napster λειτουργούσε με υβριδικό P2P δίκτυο, στα οποία θα τα αναφερθούμε στην συνέχεια [6].

Ένα σύστημα που υλοποιείται μέσω P2P δικτύου είναι διανεμημένο, οι κόμβοι του διασυνδέονται μεταξύ τους και οργανώνονται σε ποικίλες τοπολογίες δικτύων ώστε να επιτυγχάνεται ο διαμοιρασμός πόρων ανάμεσα τους, χωρίς την ύπαρξη διακομιστή [2]. Η επιρροή ενός P2P δικτύου και των μηχανισμών δρομολόγησης του είναι αισθητή σε ιδιότητες εφαρμογής, όπως:

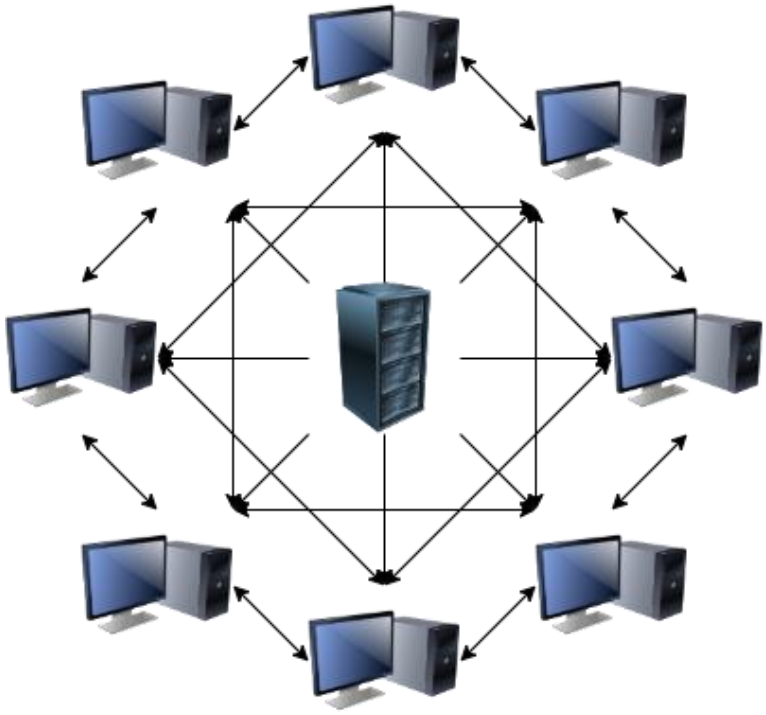
- απόδοση, εξαιτίας της συνδυασμένης υπολογιστικής ισχύς
- ανωνυμία, σε κάποιες περιπτώσεις, μέσω διάφορων τεχνικών κρυπτογράφησης
- αξιοπιστία, όπου ακόμα και στην περίπτωση που ένας κόμβος καταρρεύσει, το δίκτυο συνεχίζει να λειτουργεί, όμως δεν θα είναι προσβάσιμα τα αρχεία του συγκεκριμένου κόμβου εκείνη τη στιγμή [5].



Εικόνα 3 - Τοπολογία δικτύου ομότιμων κόμβων

1.2.3 Υβριδικά Δίκτυα Ομότιμων Κόμβων (Hybrid Peer-to-Peer Networks)

Τα διανεμημένα P2P δίκτυα που εκμεταλλεύονται μία κεντρική οντότητα, με σκοπό την παροχή μέρους των υπηρεσιών του δικτύου, ονομάζονται υβριδικά δίκτυα ομότιμων κόμβων. Το συγκεκριμένο μοντέλο συνδυάζει το βασικό χαρακτηριστικό των P2P δικτύων, δηλαδή το διαμοιρασμό των πόρων ανάμεσα στους κόμβους και το αντίστοιχο των δικτύων πελάτη - διακομιστή, δηλαδή την ύπαρξη μίας κεντρικής οντότητας.



Εικόνα 4 - Τοπολογία υβριδικού δικτύου ομότιμων κόμβων

Στην δική μας περίπτωση, ως προς το Blockchain, μας ενδιαφέρουν περισσότερο τα δίκτυα ομότιμων κόμβων μιας και είναι βασικό κομμάτι της τεχνολογίας. Ο βασικότερος λόγος που αποτελεί και την κύρια διαφορά των δύο βασικών μεθόδων είναι η έλλειψη ανάγκης κάποιου κεντρικού διακομιστή, διαθέτοντας μεγαλύτερα επίπεδα κλιμάκωσης και επεκτασιμότητας, καθώς είναι και ανεκτικά έναντι αποτυχιών, όπως του μοναδικού σημείου αποτυχίας (single point of failure), που είναι και το πιο συνηθισμένο [6].

1.2.4 Σφάλματα στα Διανεμημένα Συστήματα

Σφάλμα σε ένα διανεμημένο σύστημα μπορούμε να πούμε ότι είναι μία μη αποδεκτή απόκλιση μίας ή περισσότερων χαρακτηριστικών ιδιοτήτων του συστήματος από την επιθυμητή, συνηθισμένη τυπική κατάσταση. Διάφορα είδη σφαλμάτων μπορούν να προκύψουν σε οποιοδήποτε τέτοιο σύστημα ανά πασά στιγμή, το οποίο θα οδηγήσει το σύστημα να καταλήξει σε ανεπιθύμητες καταστάσεις ως προς την λειτουργικότητα, την συνέχεια και την αποδοτικότητα 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. Υπάρχουν κατάλληλοι μηχανισμοί, όπου κάθε σύστημα οφείλει να διαθέτει, οι οποίοι είναι ικανοί να εντοπίζουν, να εποπτεύουν και να αντιμετωπίζουν τα σφάλματα προφυλάσσοντας το σύστημα από καταστάσεις αποτυχίας [7]. Ορισμένα είδη σφαλμάτων που μπορεί να οδηγήσει ένα σύστημα σε κατάσταση αποτυχίας είναι τα εξής:

- Fail-stop/Crash failures, το οποίο αποτελεί την κατάληξη του συστήματος 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. Οφείλονται σε σφάλματα και αστοχίες λογισμικού και υλικού (software and hardware crashes) που έχουν ως αποτέλεσμα τη μη απόκριση των κόμβων στο δίκτυο.

- Omission failures, η οποία αποτυχία πραγματοποιείται όταν η αποστολή μηνύματος, που σε κανονικές συνθήκες θα έπρεπε να έχει αποσταλεί σύμφωνα με το πρωτόκολλο, παραλείπεται εξαιτίας μίας ελαττωματικής διαδικασίας [8].

Τα διανεμημένα συστήματα χρησιμοποιούν το κατάλληλο μοντέλο συναίνεσης, ή και συνδυασμό (για τα οποία θα αναφερθούμε στη συνέχεια), ώστε να παρέχεται η απαραίτητη προστασία και ανεκτικότητα σε κάθε μορφή σφάλματος, διότι είναι όφελος τους η εξασφάλιση της βιωσιμότητας του συστήματος κάτω από πιθανές ανεπιθύμητες συνθήκες αποτυχίας.

1.3 Σύγχρονα και Ασύγχρονα Συστήματα

Τα διανεμημένα συστήματα, κατεπέκταση και όλες οι πλατφόρμες που χρησιμοποιούν την τεχνολογία blockchain, έχουν ως στόχο την επίτευξη ομοφωνίας. Οι παραδοχές που αφορούν τον συγχρονισμό αποτελούν έναν από τους παράγοντες που καθορίζουν την επίτευξη της ομοφωνίας. Η λειτουργία ενός συστήματος προτείνεται να είναι συγχρονισμένη αναφορικά με τον χρονισμό των γεγονότων που πραγματοποιούνται ως προς την σχετική ταχύτητα ολοκλήρωσης των απαιτούμενων διαδικασιών και τον χρόνο διάδοσης ενός μηνύματος στο δίκτυο. Σε κάθε διανεμημένο σύστημα, αναπόσπαστο κομμάτι του αποτελούν οι παραδοχές του σχετικά με τον συγχρονισμό του μιας και το είδος του αλγορίθμου που είναι κατάλληλος αναλόγως την περίπτωση και τα προβλήματα που μπορεί να αντιμετωπιστούν. Τα συστήματα χωρίζονται ανάλογα τους περιορισμούς του συγχρονισμού τους σε δύο κατηγορίες:

1. Σύγχρονα, τα οποία επιτρέπουν την επίτευξη ομοφωνίας επιβάλλοντας χρονικά όρια στις ταχύτητες του συστήματος. Τα συγκεκριμένα συστήματα μπορούν τα θεωρηθούν πιο συντηρητικά μιας και τα όρια τους είναι αυστηρά και προκαθορισμένα από την αρχή χωρίς ενδεχόμενο παραβίασης. Υπάρχει βέβαια πάντα στα διανεμημένα συστήματα η πιθανότητα κατά την λειτουργία τους να παρουσιαστούν χρονικές αστάθειες. Αυτές μπορούν να επιφέρουν λανθασμένα αποτελέσματα και επιπλοκές στην επίτευξη της ομοφωνίας λόγω του περιορισμένου χρονισμού. Σε αυτή τη περίπτωση θα παρατηρηθεί υποβιβασμός της απόδοσης και της λειτουργικότητας του συστήματος κατά τη λειτουργία του υπο τους κανόνες του σύγχρονου χρονισμού.

2. Ασύγχρονα, τα οποία διακρίνονται από την έλλειψη επιβολής ορίων χρονισμού. Τα συγκεκριμένα συστήματα χαρακτηρίζονται από απουσία ορίων στις ταχύτητες των διαδικασιών και στην μετάδοση των μηνυμάτων. Βέβαια, η απουσία χρονικών περιορισμών επιφέρει στο σύστημα τον μη διαχωρισμό μίας λάθος διαδικασίας από μία απλά αργή. Ως αποτέλεσμα, η αδυναμία αντιμετώπισης μίας σειράς σοβαρών προβλημάτων που θα ακολουθήσουν, με πιο βασικό την αδυναμία επίτευξης ομοφωνίας με ντετερμινιστικό τρόπο παρουσία σφαλμάτων. Αυτό αποτελεί το FLIP αποτέλεσμα αδυναμίας (FLIP impossibility result), μία στοιχειώδης παραδοχή στην εφαρμογή των διανεμημένων συστημάτων [9].

Ο συντηρητικός τους χαρακτήρας προσδίδεται από τους αυστηρούς χρονικούς περιορισμούς των συγχρόνων μοντέλων, με σκοπό την διατήρηση της ομοφωνίας υπο τις χειρότερες περιστάσεις. Έχει προταθεί μία εναλλακτική προσέγγιση με τα εν μέρει σύγχρονα συστήματα (partially synchronous systems), όπου τα όρια ταχύτητας είναι προκαθορισμένα για την επεξεργασία και την καθυστέρηση των μηνυμάτων, αλλά διατηρούνται μόνο στο τέλος. Αυτά τα συστήματα αποτελούν μία παραλλαγή των συγχρόνων συστημάτων με πιο ασθενή όρια χρονισμού, ενώ παράλληλα διατηρούν ασφαλή την επίτευξη ομοφωνίας [10]. Μία ακόμη εναλλακτική πρόταση είναι το μοντέλο ανιχνευτή αστοχίας (failure detector model), το οποίο έχει ως στόχο την ενίσχυση ενός ασύγχρονου συστήματος παρέχοντας στις διαδικασίες τις σωστές πληροφορίες σχετικά με την κατάσταση του συστήματος, έχοντας παράλληλα την δυνατότητα επίλυσης ενός ευρύτερου φάσματος προβλημάτων [11].

1.4 Κρυπτογράφηση (Cryptography)

Η κρυπτογράφηση είναι το πρώτο μέρος μίας διαδικασίας της κρυπτογραφίας κατά την οποία ένα κείμενο από κανονική μορφή μετασχηματίζεται σε μορφή που δεν είναι δυνατό να διαβαστεί από τον οποιοδήποτε. Πάρα μόνο όμως εάν μπορεί να το αποκρυπτογραφήσει (decryption) ώστε να το επαναφέρει στην αρχική του κανονική μορφή ώστε να μπορεί να αναγνωστεί, όπου είναι και το δεύτερο μέρος της διαδικασίας. Υπάρχουν δύο τρόποι με τους οποίους μπορεί να πραγματοποιηθεί η διαδικασία της κρυπτογράφησης. Ο ένας είναι μέσω του συμμετρικού κλειδιού (symmetric key), όπου και για την κρυπτογράφηση αλλά και για την αποκρυπτογράφηση χρησιμοποιείται μόνο ένα κλειδί. Ο άλλος μέσω των ασύμμετρων κλειδιών (asymmetric key pairs), όπου είναι απαραίτητο διαφορετικό κλειδί για την διεξαγωγή της κάθε διαδικασίας [12].

1.4.1 Κρυπτογράφηση Δημοσίου Κλειδιού (Public Key Cryptography)

Ο τρόπος κρυπτογράφησης που μας ενδιαφέρει περισσότερο στην τεχνολογία blockchain, το οποίο και κάνει χρήση του, είναι ο δεύτερος που λέγεται αλλιώς και κρυπτογράφηση δημοσίου κλειδιού. Αναλυτικά, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του αποδέκτη, το οποίο είναι γνωστό σε όλους, ώστε να κρυπτογραφήσει το μήνυμα που θέλει να στείλει, ενώ ο αποδέκτης χρησιμοποιεί το ιδιωτικό του κλειδί, το οποίο είναι γνωστό μόνο στον ίδιο, ώστε να αποκρυπτογραφήσει το μήνυμα στην αρχική κανονική του μορφή. Η συγκεκριμένη διαδικασία προσφέρει ασφάλεια, διατηρώντας και την ιδιωτικότητα μεταξύ αποστολέα και παραλήπτη κατά τις συναλλαγές τους μιας και δεν γνωρίζει κανένας από τους δύο την ταυτότητα του αλλού. Επίσης, η ασφάλεια σφραγίζεται από το γεγονός ότι είναι αδύνατη η αποκρυπτογράφηση του κρυπτογραφημένου περιεχομένου από οποιονδήποτε δεν κατέχει το κλειδί. Έτσι διασφαλίζεται η ακεραιότητα των δεδομένων των χρηστών εντοπίζοντας πιθανές παραβάσεις κατά τις συναλλαγές.

Εικόνα 5 - Κρυπτογράφηση δημοσίου κλειδιού

1.4.2 Ψηφιακή Υπογραφή (Digital Signature)

Ένα blockchain σύστημα εκτός από την κρυπτογραφία χρησιμοποιεί παράλληλα και τις ψηφιακές υπόγραφες. Μέσω αυτών διασφαλίζεται η αυθεντικότητα των μηνυμάτων κατά τις συναλλαγές και η ακεραιότητα ενάντια σε επιθέσεις. Με την δημιουργία ενός ιδιωτικού κλειδιού από τον αποστολέα επισυνάπτεται και μία ψηφιακή υπογραφή. Έπειτα, αφού γνωρίζει ο παραλήπτης το δημόσιο κλειδί του αποστολέα, είναι σε θέση να επιβεβαιώσει ότι το μήνυμα είναι αυθεντικό, θέτοντας το έτσι αποδεκτό από το δίκτυο.

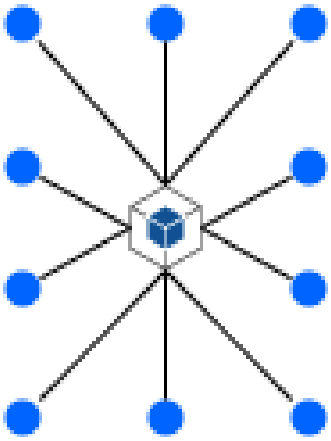
1.4.3 Συναρτήσεις Κατακερματισμού (One-way hash Functions)

Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται από τους αλγορίθμους κατά την κρυπτογραφία και τις ψηφιακές υπογραφές. Ο ρόλος τους είναι η μετατροπή δεδομένων εισόδου με τυχαίο μέγεθος σε δεδομένα εξόδου με σταθερό και μικρότερο μέγεθος. Η λειτουργία τους στηρίζεται στο γεγονός ότι για κάθε είσοδο η αντίστοιχη έξοδος της είναι μοναδική, ώστε να διασφαλίζεται η ανθεκτικότητα του συστήματος σε περίπτωση κακόβουλης ενέργειας [13].

ΚΕΦΑΛΑΙΟ 2 : Συγκεντρωτισμός και Αποκέντρωση

2.1 Συγκεντρωτικά Συστήματα (Centralized Systems)

Ένα συγκεντρωτικό ή κεντρικοποιημένο σύστημα, όπως φαίνεται και από την ονομασία του, δομείται γύρω από ένα κέντρο. Τα συστήματα αυτού του τύπου βασίζονται στο μοντέλο πελάτη-διακομιστή όπου μία κεντρική εξουσία παρέχει υπηρεσίες στους χρήστες, ελέγχει το σύστημα και είναι υπεύθυνη για όλες τις διεργασίες του. Οι συναλλαγές και τα δεδομένα τους όμως από τον κάθε χρήστη είναι φανερά, το οποίο συνεπάγει ότι είναι αναγκαία η εμπιστοσύνη στο σύστημα ανάμεσα σε χρήστες και εξουσία. Όσον αφορά το blockchain, τα ιδιωτικά δίκτυα κυρίως έχουν συγκεντρωτικό χαρακτήρα λόγω μεγαλύτερης ανάγκης ασφάλειας και ελέγχου με τη χρήση μηχανισμών συναίνεσης. Οι δημοφιλέστεροι αυτοί μηχανισμοί είναι ο PBFT (Ενότητα 3.8.1) και ο Raft (Ενότητα3.5), καθώς και πάροχοι όπως η Google, το eBay και η Amazon κάνουν χρήση αυτού του μοντέλου για την παροχή των υπηρεσιών τους [14].



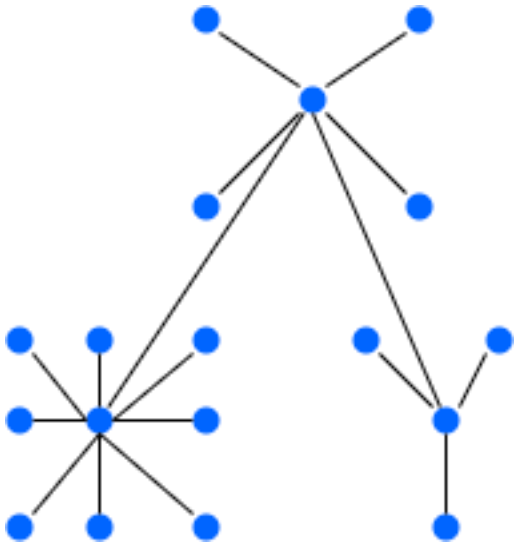
Εικόνα 6 - Συγκεντρωτικό δίκτυο

2.2 Αποκεντρωμένα Συστήματα (Decentralized Systems)

Θα σταθούμε περισσότερο στην αποκέντρωση μιας και η πλειοψηφία των blockchain εφαρμογών "χτίζονται" πάνω σε αυτόν τον τύπο συστημάτων. Ο βασικός λόγος που συμβαίνει αυτό είναι το γεγονός ότι ο έλεγχος κατανέμεται σε περιφέρειες σε αντίθεση με τα συγκεντρωτικά συστήματα. Σε ένα αποκενρτωμένο blockchain σύστημα δίνεται η δυνατότητα σε όλους τους χρήστες του δικτύου να γίνουν υπεύθυνοι για την λήψη των αποφάσεων που αφορούν το σύστημα σαν σύνολο. Μέχρι πριν μερικά χρόνια τα περισσοότερα μέσα μετάδοσης πληροφορίας και επικοινωνίας έκαναν χρήση του συγκεντρωτισμού. Στην περίπτωση όμως που η μοναδική κεντρική υπεύθυνη εξουσία αποτύχει να εκτελέσει σωστά το ρόλο της τότε όλο το σύστημα γίνεται ευάλωτο σε επιθέσεις. Γι' αυτό και το blockchain επένδυσε πάνω στην αποκέντρωση, αρχικά με τα κρυπτονομίσματα και συγκεκριμένα το BTC, και στη συνέχεια ακολουθώντας ολοένα και περισσότερα καινούργια κρυπτονομίσματα και άλλες εφαρμογές. Με αυτόν τον τρόπο θέλησε να δώσει στον κόσμο ανοιχτά και πιο ασφαλοί συστήματα μιας και η ευθύνη δεν παραμένει σε έναν αλλά μοιράζεται σε πολλούς και συγκεκριμένα σε όλους τους εμπλακώμενους χρήστες [2].

Τα κύρια πλεονεκτήματα των αποκεντρωμένων συστημάτων έναντι των συγκεντρωτικών είναι:

- Η εξουσία βρίσκεται στα χέρια του κάθε χρήστη, έτσι κανένας άλλος χρήστης του δικτύου δεν μπορεί να χρησιμοποιήσει προς όφελος του δεδομένα οποιουδήποτε άλλου χρήστη χωρίς την συνέναιση του.
- Βασισμένοι στο προηγούμενο πλεονέκτημα, η κατάρρευση ενός κόμβου δεν θα προκαλέσει την πτώση ολόκληρου του συστήματος μιας και όλοι οι κόμβοι είναι ανεξάρτητοι. Επίσης δεν θα δημιουργηθεί πρόβλημα ούτε στην περίπτωση που ένας καινούργιος χρήστης εισέλθει στο δίκτυο ή ένας παλαιότερος υποστεί κάποια αποτυχία. Έτσι αυτά συντελούν στην μείωση της πιθανότητας αποτυχίας όλου του δικτύου εξαιτίας ορισμένων μεμονωμένων αποτυχιών.
- Ο χρόνος πραγματοποίησης μίας συναλλαγής έχει γίνει αισθητά ταχύτερος (και συγκεκριμένα σε μερικά λεπτά) σε σχέση με παλαιότερα συστήματα που βασίζονταν στον συγκεντρωτισμό.



Εικόνα 7 - Αποκεντρωμένο δίκτυο

2.3 Τύποι Συγκεντρωτισμού και Αποκέντρωσης

Τα συγκεντρωτικά και τα αποκεντρωμένα συστήματα χωρίζονται σε 3 τύπους ως προς το λογισμικό τους:

- Αρχιτεκτονικός, όπου αφορά το πλήθος των κόμβων του κάθε συστήματος.
- Πολιτική, όπου αφορά το πλήθος των χρηστών σαν σύνολο πίσω από κάθε κόμβο του συστήματος.
- Λογική, όπου αφορά την περίπτωση που ακόμα και ένα μεγάλο ποσοστό του συστήματος καταρρεύσει, εάν οι υπόλοιποι κόμβοι θα επηρεαστούν ή θα παραμείνουν ανεξάρτητοι και λειτουργικοί.

Οι παραπάνω τύποι μπορεί να θεωρούνται ανεξάρτητοι μεταξύ τους αλλά εξαρτώνται ο ένας με τον άλλο ως προς την κατανόηση τους. Όσον αφορά την τεχνολογία blockchain μπορούμε να την χαρακτηρίσουμε ως:

- Αρχιτεκτονικά αποκεντρωμένη, μιας και ο κάθε κόμβος ξεχωριστά συντελεί την εξουσία.
- Πολιτικά αποκεντρωμένη, μιας και ο έλεγχος της αλυσίδας δεν υφίσταται.
- Λογικά συγκεντρωτική, μιας και η κατάσταση εν τέλη που θα επικρατήσει θα είναι μία στην οποία θα συμφωνήσουν όλοι οι κόμβοι του συστήματος.

Πολλοί συγκρίνουν τα αποκεντρωμένα με τα διανεμημένα συστήματα με τη κύρια διαφορά τους να είναι ότι στα πρώτα δεν υπάρχει μία κεντρική εξουσία που ευθύνεται και παίρνει αποφάσεις για όλο το σύστημα, ενώ στα δεύτερα αυτή η εξουσία μπορεί να χωρηγείται σε έναν ή δύο κόμβους. Έτσι καταλαβαίνουμε ότι τα διανεμημένα συστήματα τείνουν λίγο περισσότερο προς το μοντέλο του συγκεντρωτισμού παρά προς την αποκέντρωση [2].

ΚΕΦΑΛΑΙΟ 3 : Μηχανισμοί Συναίνεσης (Consensus Mechanisms)

Ένα σημαντικό πρόβλημα που αντιμετωπίζουν τα διανεμημένα συστήματα είναι η αξιοπιστία της πληροφορίας, άρα και των χρηστών εάν κάτι πάει στραβά. Αυτό το γεγονός αναφέρεται ως "Πρόβλημα Συναίνεσης" και είναι ουσιαστικά η ανάγκη για επιτυχής συμφωνία μεταξύ των ασύγχρονων κόμβων. Για την αποτροπή του έχουν δημιουργηθεί ανά τα χρόνια όλο και περισσότερα πρωτόκολλα τα οποία έχουν σαν τελικό σκοπό την λήψη μίας κοινής απόφασης σε μία δυαδική τιμή. Προκειμένου να καταλήξουμε σε αυτό το αποτέλεσμα τα πρωτόκολλα θα πρέπει να διενεργούν σωστά ακόμα και στην περίπτωση ενός οποιουδήποτε σφάλματος. Η κύρια διαδικασία που εκτελείται είναι αρχικά η διαμοίραση των εναλλακτικών τιμών από τους κόμβους στο δίκτυο και εν συνεχεία η αλληλεπίδραση μεταξύ τους ώστε να καταλήξουμε στην τελική μας απόφαση. Για να φτάσουμε όμως στην τελική απόφαση πρέπει να συμφωνεί η πλειοψηφία των κόμβων ανάμεσα στις προτεινόμενες τιμές, καθώς και να ικανοποιούνται οι ακόλουθες προϋποθέσεις:

- Τερματισμός: Κάθε λειτουργικά σωστή διαδικασία δίνει μία τιμή.
- Εγκυρότητα: Εάν οι περισσότερες διαδικασίες δίνουν την ίδια τιμή σημαίνει ότι όλες οι λειτουργικές διαδικασίες έδωσαν κοινή τιμή.
- Ακεραιότητα: Κάθε λειτουργική διαδικασία δίνει μία μοναδική τιμή, το οποίο σημαίνει στην περίπτωση που μας δοθεί η συγκεκριμένη τιμή τότε αυτή έχει προταθεί από κάποια διαδικασία.
- Συμφωνία: Όλες οι λειτουργικές διαδικασίες είναι απαραίτητο να δίνουν την ίδια τιμή.

Επίσης οι δύο βασικές ιδιότητες όλων των πρωτοκόλλων συναίνεσης είναι:

- Ο χρόνος, που έχει να κάνει με το σύνολο των απαιτούμενων γύρων ανταλλαγής μηνυμάτων συναρτήσει του συνόλου διαδικασιών και μεγέθους του κάθε τομέα εισόδου.
- Η πολυπλοκότητα των μηνυμάτων, τα οποία είναι ουσιαστικά το σύνολο των μηνυμάτων που κυκλοφορούν.

Ο βασικότερος λόγος ύπαρξης των πρωτοκόλλων συναίνεσης όπως είπαμε και προηγουμένως είναι η απαίτηση μας να λειτουργεί σωστά το σύστημα ακόμα και σε περίπτωση σφάλματος, όπως η αποτυχία κάποιου κόμβου ο οποίος έχει αντίγραφα της κοινής βάσης δεδομένων. Ο κύριος διαχωρισμός τους είναι ανάλογα:

- τον τρόπο αντιμετώπισης ενός πιθανού σφάλματος. Το πρώτο είναι η συντριπτική αποτυχία (crash failure), όπου οι κόμβοι δεν είναι ικανοί να επεξεργαστούν, να στείλουν ή και να λάβουν μηνύματα. Το δεύτερο είναι η βυζαντινή αποτυχία (byzantine failure), όπου οι κόμβοι λαμβάνουν αόριστες αποφάσεις που συνήθως δεν συμβαδίζουν με το ανάλογο πρωτόκολλο.
- τον τρόπο αλληλεπίδρασης ανάμεσα στους κόμβους, όπου χωρίζουμε τα δίκτυα σε σύγχρονα και ασύγχρονα με κύρια διαφορά να είναι η καθυστέρηση διαλογής των μηνυμάτων.

3.1 Proof of Work (PoW)

Το πρωτόκολλο PoW, ή απόδειξη εργασίας, είναι το πρώτο που δημιουργήθηκε βασισμένο στο Blockchain μέσω του κρυπτονομίσματος BTC από τον Satoshi Nakamoto το 2009 και αποτελεί από τότε μέχρι και σήμερα το πιο δημοφιλή ανάμεσα στους συναγωνιστές του που έχουν δημιουργηθεί με το πέρασμα των χρόνων. Βασικό ρόλο σε αυτόν τον μηχανισμό κατέχουν οι miners οι οποίοι ανταγωνίζονται ο ένας τον άλλο ως προς το ποιος θα καταφέρει να λύσει ένα κατακερματισμένο πρόβλημα, βρίσκοντας έτσι το nonce value που είναι κατάλληλο για την δημιουργία ενός νέου block. Ο κάθε κόμβος ενεργεί ανεξάρτητα λόγω της φύσης τους και απόδειξη της δουλείας τους αποτελεί ο χρόνος, η υπολογιστική ισχύς και η ενέργεια που δαπανήθηκε κατά το έργο τους, αιτίες που συντελούν και στην ασφάλεια που προσφέρεται μιας και τα υψηλά κόστοι κάνουν το ρίσκο επιτυχίας μίας κακόβουλης ενέργειας να μην αξίζει τον κόπο. Επίσης, η πιθανή εμφάνιση των forks προσφέρει ένα χαρακτηριστικό του PoW την παθολογική οριστικότητα των συναλλαγών. Το PoW πλέον όμως έχει αρχίσει να αποσπάτε από το BTC σαν ονομασία μιας και τα τελευταία χρονιά ολοένα και περισσότερα συστήματα πειραματίζονται με τον συγκεκριμένο μηχανισμό κάνοντας χρήση του σε ποικίλες εφαρμογές προσπαθώντας να τον κάνουν πιο αποδοτικό. Τα κύρια μειονεκτήματα του που γίνεται προσπάθεια να βελτιωθούν είναι ο μικρός αριθμός συναλλαγών το δευτερόλεπτο (3-7) και ο αργός χρόνος δημιουργίας καινούργιου block που μαζί με τον χρόνο επιβεβαίωσης από τα 6 στάδια του κυμαίνεται στην μία ώρα για κάθε block. Παρόλα αυτά, η περιγραφή του BTC είναι ο καλύτερος τρόπος για την κατανόηση της λειτουργίας του PoW, όπως και θα γίνει παρακάτω [3].

3.1.1 Λειτουργία

Το BTC αποτελείται από ένα δίκτυο στο οποίο συντελούνται συναλλαγές μεταξύ των χρηστών του, όμως για την ολοκλήρωση τους είναι απαραίτητη η πραγματοποίηση μίας συγκεκριμένης διαδικασίας:

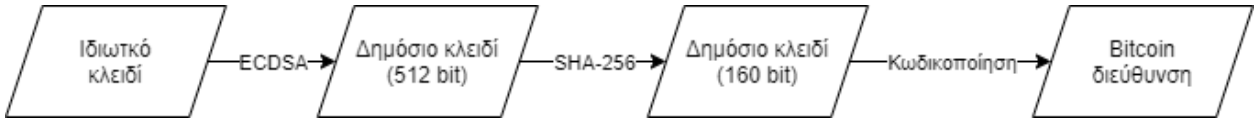
1. Παραγωγή του δημοσίου κλειδιού από το ιδιωτικό κλειδί με χρήση της μεθόδου Elliptic Curve Digital Signature Algorithm (ECDSA),
2. Μετασχηματισμός του με τη συνάρτηση κατακερματισμού Secure Hash Algorithm 256 bit (SHA-256),
3. Δημιουργία μίας διεύθυνσης (BTC address) η οποία είναι μοναδική και αντιπροσωπεύει τα νομίσματα BTC που χρησιμοποιήθηκαν κατά την συναλλαγή [15].

Τέλος, οι κόμβοι που έχουν αναλάβει την δημιουργία των blocks πρέπει να επιλέξουν τις συναλλαγές που θέλουν να προσθέσουν στο block τους, συναγωνίζοντας ο ένας τον άλλο ως προς την υπολογιστική ισχύ. Οι συγκεκριμένοι κόμβοι ονομάζονται miners και η ανταγωνιστική διαδικασία που εκτελούν είναι το λεγόμενο PoW.

Ο μηχανισμός συναίνεσης PoW σαν λογική έχει βασιστεί πάνω στο πρωτόκολλο Hashcash, το οποίο είναι ένας μηχανισμός με στόχο την αντιμετώπιση ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το πρωτόκολλο αυτό για να θεωρείται ότι λειτουργεί σωστά πρέπει να στείλει ένα πολύ μεγάλο ποσό μηνυμάτων στο ηλεκτρονικό ταχυδρομείο, σε συνεργασία με τον επεξεργαστή του υπολογιστή (CPU) κατά ένα σύντομο χρόνο. Κατά τη διάρκεια της διαδικασίας του PoW, οι κόμβοι ανταγωνίζονται μεταξύ τους στην επίλυση δύσκολων μαθηματικών κατακερματιστικών λειτουργιών κάνοντας χρήση της κατακερματισμένης αξίας (hash value) του προηγούμενου block και το περιεχόμενο των συναλλαγών που θα συνδυαστούν με έναν ακέραιο, μοναδικό και τυχαίο αριθμό (nonce). Κατά το τέλος αυτής της διαδικασίας, ο κόμβος που θα καταφέρει να "εξορύξει" (mining) μία καινούργια κατακερματισμένη αξία και μικρότερη από ένα ορισμένο όριο-στόχο (target) θα είναι ο επικρατέστερος. Η εξορυγμένη αυτή αξία θα χρησιμοποιηθεί στο καινούργιο block που θα δημιουργηθεί, το οποίο θα συμπεριληφθεί στην γενικότερη αλυσίδα. Έπειτα, αυτή η αξία θα χρησιμοποιηθεί από τον επόμενο κόμβο με την ίδια διαδικασία από την αρχή στο επερχόμενο block, ο οποίος κύκλος θα επαναλαμβάνεται συνέχεια [16].

Οι miners είναι αυτοί που θα τεθούν να επιλέξουν ποιες συναλλαγές επιθυμούν να επιβεβαιώσουν. Η απόφαση τους εξαρτάται από τα τέλη συναλλαγών που θα προσφέρουν οι χρήστες που θα συμμετέχουν στην συναλλαγή στο δίκτυο. Ο βασικότερος λόγος όμως του να καταφέρεις να γίνεις miner είναι ότι στο τέλος αυτής της διαδικασίας και στην δημιουργία δηλαδή ενός καινούργιου block, εισπράττει ως αμοιβή ορισμένα BTCs σε αντάλλαγμα για την υπολογιστική ισχύ που σπαταλήθηκε. Το καινούργιο block που δημιουργείται θα τοποθετηθεί στην αλυσίδα, η οποία αποτελείται από προηγούμενα δημιουργημένα blocks και συνδέονται μεταξύ τους μέσω λειτουργιών κατακερματισμού. Από αυτήν την αλυσίδα έχει πάρει και την ονομασία της η τεχνολογία Blockchain, όπου και το ιστορικό των συναλλαγών της παραμένει ανεπηρέαστο [17].

Κατά το μηχανισμό συναίνεσης PoW εξασφαλίζεται η ολοκλήρωση των συναλλαγών των χρηστών του δικτύου, ενώ παράλληλα διατηρείται μία συγκεκριμένη χρονολογική σειρά. Το PoW και οι ενέργειες των miners προσφέρουν ασφάλεια στο σύστημα έναντι πιθανών απειλών. Παρόλα αυτά, υπάρχει πάντα η πιθανότητα τερματισμού του, το οποίο θα έχει ως αποτέλεσμα της διάσπαση της αλυσίδας σε δύο υποαλυσίδες (forks).



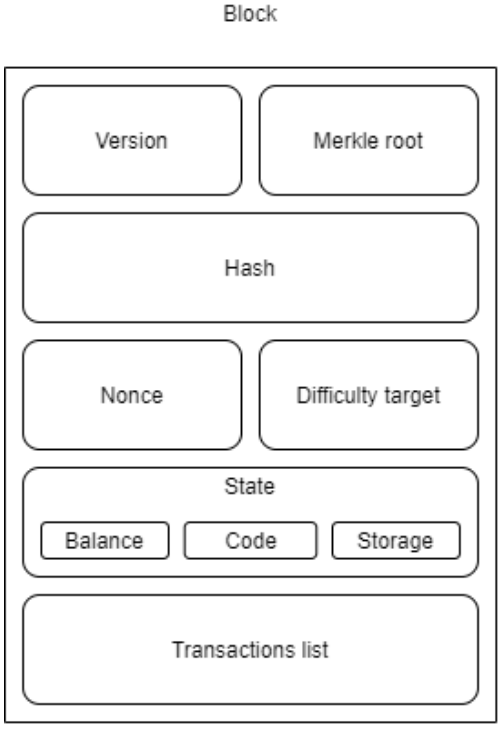
Εικόνα 8 - Παραγωγή Bitcoin διεύθυνσης

3.1.2 Block

Το δίκτυο του κρυπτονομίσματος BTC αποτελείται από blocks που συγκεντρώνονται στη σειρά σε μία αλυσίδα η οποία μπορεί να σπάσει. Το κάθε block αποτελείται από δύο μέρη:

- Την κεφαλή (header), στην οποία περιλαμβάνονται σημαντικά δεδομένα που συντελούν στην μοναδικότητα του κάθε block, όπως:
    - Την αξία κατακερματισμού του (merkle root block hash)
    - Την αξία κατακερματισμού του προηγούμενου block (parent block hash)
    - Την χρονική ένδειξη η οποία δηλώνει το πότε δημιουργήθηκε το block (block timestamp)
    - Έναν ακέραιο τυχαίο αριθμό για την επίλυση των περίπλοκων μαθηματικών διαδικασιών κατά τη διαδικασία του mining (nonce)
    - Τον αριθμό έκδοσης όπου ελέγχει αναβαθμίσεις που ίσως χρειάζεται το σύστημα (version number)
    - Το μέγεθος του κάθε block (block size)
    - Ένα αριθμητικό όριο, το οποίο είναι χρήσιμο για να διατηρηθεί ο ρυθμός με τον οποίο δημιουργείται το επόμενο block στον ορισμένο επιθυμητό χρόνο (difficulty number) που η μεταβολή του είναι περιοδική και ανάλογη της αύξησης της υπολογιστικής ισχύς του miner.
- Το σώμα (body), στο οποίο περιλαμβάνεται μία λίστα με τις συναλλαγές που έχουν πραγματοποιηθεί από τους χρήστες του δικτύου [18].

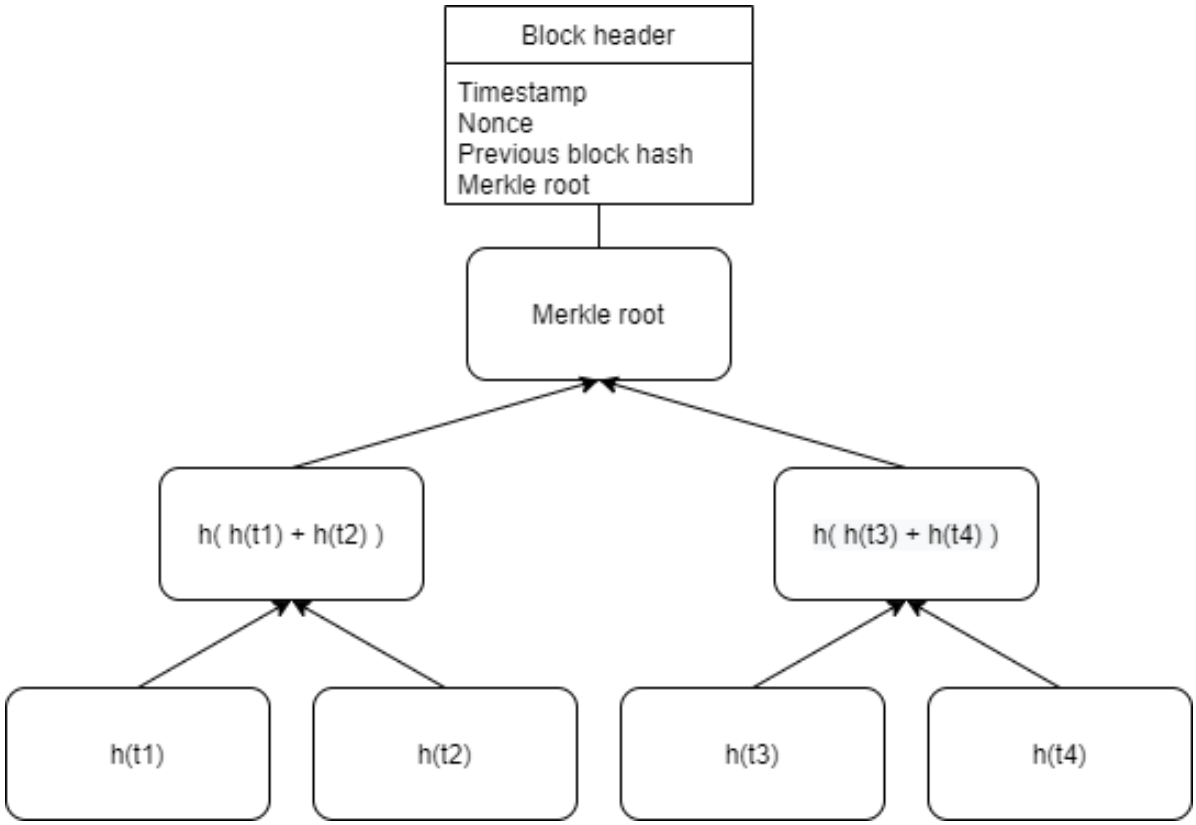
Η αλυσίδα που συντελούν τα blocks δεν διασπάτε και είναι συνεχής λόγω του ότι κάθε block συνδέεται με το προηγούμενο του με τη χρήση της συνάρτησης κατακερματισμού SHA-256. Καθώς και με αυτήν την συνάρτηση επιτυγχάνεται η ανίχνευση πιθανών κακόβουλων ενεργειών στο δίκτυο μιας και όποια τροποποίηση γίνει σε οποιοδήποτε block θα μεταδοθεί στην πιο πρόσφατη έκδοση του συστήματος [19].



Εικόνα 9 - Δομή block

3.1.3 Merkle Tree

Το κρυπτονόμισμα BTC κάνει χρήση των δένδρων Merkle με σκοπό να εντοπίζει όλες τις εισερχόμενες αλλαγές κατά την διαδικασία της συναλλαγής. Δεδομένου της ονομασίας του μπορούμε να πούμε ότι είναι ένα δένδρο αποτελούμενο από δυαδικά ψηφιά όπου τα φύλλα του είναι οι πληροφορίες που έχουν αποθηκευτεί. Κατά τη διάρκεια οποιασδήποτε συναλλαγής χρησιμοποιούνται συναρτήσεις κατακερματισμού ($h(t_i)$) όπου κατά την ολοκλήρωση της διαδικασίας να μας δοθεί μία κατακερματισμένη αξία η οποία και θα αντιπροσωπεύει την ταυτότητα της συναλλαγής (transaction ID). Κάθε συναλλαγή συνδυάζεται με μία άλλη σχηματίζοντας ζευγάρια και μία καινούργια ταυτότητα η οποία κατακερματίζεται ξανά. Ο κατακερματισμός συνεχίζει να επαναλαμβάνεται μέχρι να φτάσει στη ριζά του δένδρου (Merkle root) όπου αποτελεί και βασικό μέρος της δομής του block. Στην περίπτωση που πραγματοποιηθεί κάποια αλλαγή σε μία συναλλαγή (t_i), τότε αυτή η μεταβολή θα μεταδοθεί μέχρι τη ρίζα του δένδρου με αποτέλεσμα να αναπαραχθεί στο ίδιο το block, το οποίο θα αποτελέσει το σύνολο του block συναλλαγών να ακυρωθεί. Το βασικότερο πλεονέκτημα των Merkle Trees βλέπουμε πως είναι η ασφάλεια που προσφέρουν στο σύστημα η οποία επιτυγχάνεται με τις συναρτήσεις κατακερματισμού που χρησιμοποιεί αλλά και τις ψηφιακές υπογραφές, που σε αντίθεση με άλλες μεθόδους δεν γίνεται χρήση περίπλοκων μαθηματικών προβλημάτων [20].

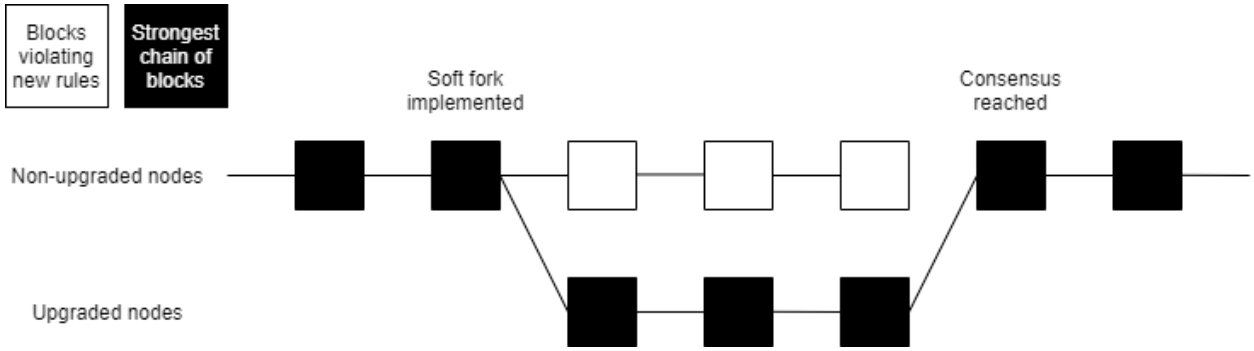


Εικόνα 10 - Δομή Merkle Tree

3.1.4 Forks

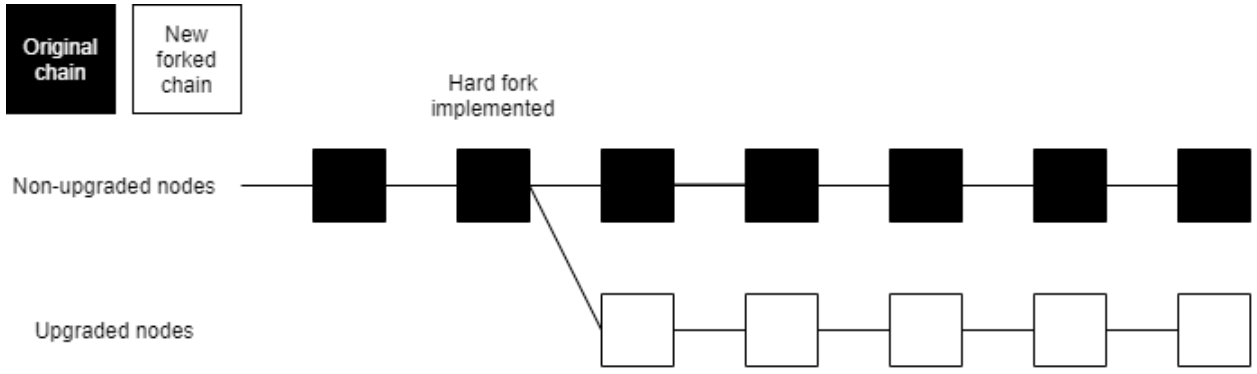
Στην περίπτωση που δεν μπορεί να εξασφαλιστεί η οριστικότητα κάποιας συναλλαγής άρα κατεπέκταση και η συνέπεια του συστήματος τότε λεμέ ότι εμφανίζεται το φαινόμενο του forking. Η συγκεκριμένη κατάσταση οφείλεται σε αδυναμία του κρυπτονομίσματος BTC και μπορεί να δημιουργηθεί οποτεδήποτε. Κατά την συγκεκριμένη διαδικασία, όταν δύο διαφορετικοί κόμβοι θελήσουν να θέσουν και οι δύο την ίδια στιγμή από ένα block στην αλυσίδα τότε εκείνη διασπάται στα δύο δημιουργώντας δύο υποαλυσίδες (forks). Στην συνέχεια το σύνολο των κόμβων του δικτύου που δεν συμμετείχαν στο πρόβλημα καλούνται να διαλέξουν μία από τις δύο υποαλυσίδες, η οποία θα θεωρηθεί έγκυρη και η διαδικασία θα συνεχιστεί κανονικά. Τα blocks της αλυσίδας που θα περισσέψουν τα λέμε ορφανά (orphan blocks) και τα αφήνουμε ως συναλλαγές που εκκρεμούν. Υπάρχει όμως και μία διαφοροποίηση ανάμεσα στα forks τα οποία τα διαχωρίζει σε δύο κατηγορίες:

- Τα soft forks, όπου οφείλονται σε μία μεταβολή κατά την οποία δεν είναι απαραίτητη η αποδοχή της από το σύνολο των κόμβων, όπως μία αναβάθμιση του συστήματος, δίνοντας έτσι την δυνατότητα να συμμετάσχουν στο δίκτυο και κόμβοι που δεν έχουν αναβαθμιστεί.



Εικόνα 11 - Παράδειγμα soft fork

- Τα hard forks, όπου οφείλονται σε μία μεταβολή κατά την οποία είναι απαραίτητη η αποδοχή της από το σύνολο των κόμβων, όπως οποιαδήποτε αλλαγή στην δομή κάποιου block, διότι όσοι κόμβοι δεν αναβαθμιστούν δεν θα συμμετάσχουν στο καινούργιο δίκτυο και θα παραμείνουν στην προηγούμενη έκδοση [21].



Εικόνα 12 - Παράδειγμα hard fork

3.2 Proof of Stake (PoS)

Το πρωτόκολλο PoS ή απόδειξη μεριδίου είναι το δεύτερο σε δημοτικότητα και δημιουργήθηκε το 2012 μέσω του κρυπτονομίσματος Peercoin, ως ένας συνδυασμός του PoW και του PoS [22]. Ο σχεδιασμός του είναι για δημόσια Blockchain συστήματα, βασισμένο σε P2P τοπολογία δικτύου και έχει αρκετά κοινά με τον κύριο ανταγωνιστή του, το PoW, με μία βασική διαφορά. Ο κόμβος (stakeholder) ποντάρει το μερίδιο του (stake) και βάση αυτού μπορεί να γίνει η επιλογή του για να τοποθετήσει στην κύρια αλυσίδα ένα καινούργιο block και όχι σύμφωνα με την υπολογιστική δύναμη του χρήστη, όπως συμβαίνει στο PoW. Το μερίδιο του κόμβου, εάν αναφερόμαστε για παράδειγμα σε cryptocurrency, είναι το σύνολο των κρυπτονομισμάτων που έχει στην κατοχή του. Όσο μεγαλύτερο είναι το μερίδιο του χρήστη, τόσες περισσότερες οι πιθανότητες να επιλεγεί να γίνει επικυρωτής (validator) του νέου block, αντίστοιχα με τους miners του PoW. Επίσης, το σύνολο των νομισμάτων είναι διαθέσιμα εξαρχής στο σύστημα και δεν εκδίδονται άλλα. Το κέρδος των χρηστών που επιλέχθηκαν για να δημιουργήσουν το καινούργιο block είναι τα τέλη συναλλαγής, το οποίο διαφέρει ανάλογα με το χρονικό διάστημα που παρέμειναν στην κατοχή τους τα νομίσματα [23].

Τα τελευταία χρονιά το PoS πρωτόκολλο έχει αρχίσει να πλησιάζει την αντικατάσταση του PoW, μιας και οι ενεργειακές δαπάνες του είναι συγκριτικά πολύ λιγότερες, αφού δεν απαιτεί μεγάλη υπολογιστική ισχύ. Η ισχύς αυτή αντικαταστείτε από την χρήση εικονικών πόρων που εξαρτώνται από το ποντάρισμένο μερίδιο του επικυρωτή ώστε να λυθούν περίπλοκα μαθηματικά προβλήματα. Βασικό παράδειγμα της αναβάθμισης του PoS αποτελεί το κρυπτονόμισμα Cardano, στο οποίο έχουν πραγματοποιηθεί ενέργειες βελτιστοποίησης των επιπέδων ασφαλείας του [24].

3.2.1 Μορφές Πρωτοκόλλων PoS

Κάθε σύστημα που κάνει χρήση του πρωτοκόλλου PoS ως μηχανισμό συναίνεσης του, τις περισσότερες των περιπτώσεων υιοθέτησε και από μία εναλλακτική τεχνική ως προς τον τρόπο δημιουργίας ενός καινούργιου block. Παρακάτω θα πραγματοποιηθεί μία ανάλυση των τριών πιο βασικών μορφών τέτοιων παραλλαγών σύμφωνα με την δημοτικότητα και το ποσοστό χρήσης τους.

3.2.1.1 Byzantine Fault Tolerance PoS

Στην περίπτωση ενός Byzantine Fault Tolerance-based συστήματος (Ενότητα 3.8) οι υποψήφιοι κόμβοι που επιθυμούν να δημιουργήσουν ένα καινούργιο block επιλέγονται τυχαία από το δίκτυο και στη συνέχεια ψηφίζουν το block εκείνο που θέλουν να συμπεριληφθεί στην αλυσίδα. Η προηγούμενη διαδικασία γίνεται με γύρους και μπορεί να πραγματοποιηθεί πολλές φορές μέχρι να κυριαρχήσει μόνο ένα block. Κυρίο χαρακτηριστικό των BFT-based συστημάτων που τα κάνουν να διαφέρουν σε σχέση με τα υπόλοιπα είναι το γεγονός ότι η συμφωνία ανάμεσα στους κόμβους για την δημιουργία ενός καινούργιου block είναι ανεπηρέαστη από οποιοδήποτε χαρακτηριστικό του blockchain, όπως το μήκος ή το μέγεθος του [25].

Μία εφαρμογή που χρησιμοποιεί το πρωτόκολλο BFT είναι η Algorand με χρήση PoS συστήματος. Κατά την ψηφοφορία του επόμενου block, οι πιθανότητες να εμφανιστούν forks είναι σχεδόν μηδενικές. Η διαδικασία της ψηφοφορίας όμως πρέπει να εκτελεστεί για τουλάχιστον 3 γύρους ώστε όλοι οι κόμβοι που συμμετέχουν να είναι σύμφωνοι με το αποτέλεσμα και η ειλικρίνεια και εγκυρότητα του προτεινόμενου block να είναι βέβαιη [26].

3.2.1.2 Coin age PoS

Το πρωτόκολλο coin age ξεκίνησε να χρησιμοποιείται το 2012 στο πρώτο PoS κρυπτονόμισμα το Peercoin [22]. Το coin age ουσιαστικά είναι το χρονικό διάστημα όπου τα κρυπτονομίσματα ενός κόμβου παρέμειναν σταθερά χωρίς να χρησιμοποιηθούν για οποιαδήποτε συναλλαγή. Ο τίτλος του προκύπτει από το γεγονός ότι αυτό το χρονικό διάστημα αποτελεί την ηλικία του νομίσματος, όπου και μηδενίζεται κάθε φορά που ένα ποσό κρυπτονομισμάτων του κόμβου αξιοποιείται. Τα συγκεκριμένα νομίσματα όμως του κόμβου που δημιούργησε ένα καινούργιο block αποκτούν μεγαλύτερη αξία όσο περισσότερο τα έχει κρατήσει χωρίς να τα ξοδέψει, έχοντας δηλαδή περισσότερο κέρδος. Το γεγονός αυτό όμως αποτελεί ίσως και το πιο βασικό μειονέκτημα του πρωτοκόλλου διότι πολλοί κόμβοι δεν συμμετέχουν στις διαδικασίες ομοφωνίας μιας και προτιμούν να κρατήσουν τα κρυπτονομίσματα τους ώστε η αξία τους να αυξηθεί. Η εφαρμογή Vericoin προσέφερε μία λύση σε αυτό το πρόβλημα με το να ενημερώνεται και για το χρονικό διάστημα (stake time) που τα κρυπτονομίσματα βρίσκονται στην κατοχή του κόμβου. Μία άλλη λύση προσφέρθηκε από την πλατφόρμα Blackcoin εφαρμόζοντας το raw stake, όπου κατά το οποίο όσο περισσότερο ενεργοί παραμένουν οι κόμβοι, με την πραγματοποίηση συναλλαγών, τόσο μικρότερες γίνονται οι πιθανότητες να πέσουν θύματα κλοπής [27]. Η εφαρμογή αυτή μεταβάλει την είσοδο στο ζητούμενο hash για τη δημιουργία ενός νέου block (stake modifier) ώστε ο χρόνος δημιουργίας του να μεταβάλλεται άρα και να μην μπορεί να προβλεφθεί από κακόβουλους χρήστες, αντιμετωπίζοντας έτσι μία pre-computing επίθεση. Το Novacoin είναι μία ακόμη coin age-based εφαρμογή, υβριδική PoW-PoS και λειτουργεί λύνοντας την SHA-256 συνάρτηση, διαφέροντας όμως από τις υπόλοιπες μιας και χρησιμοποιεί δικό της αλγόριθμο PoS σε συνδυασμό με μία καινούργια παράμετρο το coin age weight. Η συγκεκριμένη παράμετρος μοιάζει με το coin age μιας και η χρησιμότητα του είναι η εύρεση του στόχου με σκοπό να δημιουργηθεί στο δίκτυο το νέο block. Από αυτό συνεπάγεται ότι όσο πιο μεγάλο είναι το coin age weight τόσες περισσότερες οι πιθανότητες να δημιουργηθεί το καινούργιο block [2].

3.2.1.3 Deposit based PoS

Το deposit based PoS λειτουργεί αποκόπτοντας την άμεση παραλαβή της αμοιβής του κόμβου κατά την δημιουργία ενός καινούργιου block εμποδίζοντας τον να πραγματοποιήσει αμέσως μία καινούργια συναλλαγή με το νέο του ποσό. Το συγκεκριμένο πρωτόκολλο δημιουργήθηκε για την ενίσχυση της ασφάλειας του δικτύου, μιας και με αυτήν την ενέργεια, αν αμφιβάλλουμε για την εγκυρότητα των συναλλαγών ενός κόμβου και αποδειχθεί αυτό το σενάριο τότε η αμοιβή του κρατάτε από το σύστημα. Με αυτόν τον τρόπο μπορεί να αντιμετωπιστεί μία ενδεχόμενη nothing at stake επίθεση (Ενότητα 3.9.2) μιας και έτσι δεν δίνεται η δυνατότητα δημιουργίας ενός block ώστε να το αντικρούσει. Στην περίπτωση όμως που ένας κακόβουλος κόμβος πάρει το ρίσκο και δοκιμάσει να πραγματοποιήσει μία double spend επίθεση, υπάρχει η πιθανότητα να μην το καταλάβει το σύστημα, λαμβάνοντας έτσι μία μεγάλη αμοιβή λόγω των forks που χρησιμοποιήθηκαν. Μία τέτοια εφαρμογή που αντιμετωπίζει nothing at stake επιθέσεις υλοποίησε ο δημιουργός του Ethereum (ETH), το Casper. Προσπαθώντας επίσης να αντικαταστήσει το PoW, εκτός από το ETH 2.0 που προβλέπεται να κυκλοφορήσει στο άμεσο μέλλον [28].

3.2.2 Delegated Proof of Stake (DPoS)

Το πρωτόκολλο DPoS είναι μία παραλλαγή του PoS με σκοπό την αντικατάσταση του PoW δίνοντας λύση στα μειονεκτήματα του. Σε μεγάλο ποσοστό είναι παρόμοιο με το PoS με μία όμως ειδοποιό διαφορά. Το ποντάρισμα (stake) των κόμβων (stakeholders) του δικτύου χρησιμοποιείται για να λάβουν μέρος σε μία διαδικασία ψηφοφορίας, σε αντίθεση με το κλασσικό PoS που χρησιμοποιείται κατευθείαν για να διεκδικήσουν το δικαίωμα της δημιουργίας καινούργιου block. Κατά την ψηφοφορία πραγματοποιείται η εκλογή των κόμβων εκπροσώπων/υποψηφίων (delegates/witnesses) που θα έχουν την δυνατότητα αρχικά να επιβεβαιώνουν τις πραγματοποιούμενες συναλλαγές και στη συνέχεια να δημιουργούν νέα blocks. Η εκλογή των stakeholders γίνεται τυχαία με γύρους, έχοντας την δυνατότητα ψήφου σε παραπάνω από έναν υποψήφιο. Επίσης, οι stakeholders μπορούν να παραχωρήσουν το μερίδιο τους σε άλλους κόμβους ώστε να αυξήσουν τις πιθανότητες του δεύτερου να εκλεγεί και να δημιουργήσει block, λαμβάνοντας αυτός και την αντίστοιχη αμοιβή. Η διαδικασία της ψηφοφορίας όμως για να λειτουργεί σωστά προϋποθέτει ότι τουλάχιστον το 51% των συμμετέχοντων κόμβων επιβεβαιώνουν ότι το δίκτυο είναι αποκεντρωμένο ως προς τους εκλεγόμενους. Η παραγωγή του κάθε block πρέπει να πραγματοποιείται σε συγκεκριμένο χρόνο ανά εφαρμογή, με την αδυναμία τήρησης του χρονικού περιθωρίου να σημαίνει ακύρωση του block, πιθανή απαγόρευση επιλογής αυτού του κόμβου στο μέλλον και αντικατάστασή του. Η παραγωγή blocks γίνεται πολύ γρηγορά λόγω του μικρού αριθμού συμμετέχων κόμβων και θεωρείται συγκριτικά πιο αποδοτικό πρωτόκολλο. Επίσης, το DPoS θεωρείται αρκετά ασφαλές μιας και παραδείγματος χάριν στην περίπτωση μίας επίθεσης διπλής δαπάνης (double spend attack) (Ενότητα 3.9.5) είναι σχεδόν αμελητέα η πιθανότητα βλάβης επικοινωνίας ώστε να πραγματοποιηθεί επιτυχώς η επίθεση. Το υψηλό ποσοστό ασφαλείας οφείλεται στο γεγονός ότι εάν υπάρξουν απώλειες κατά την επικοινωνία, το δίκτυο το καταλαβαίνει αμέσως, λόγω της αποτυχίας παραγωγής block στο χρονικό όριο από τους κόμβους. Σε ένα τέτοιο σενάριο, στην χειρότερη των περιπτώσεων το δίκτυο θα μπει σε κατάσταση αναμονής μέχρι να επιβεβαιώσουν οι μισοί κόμβοι τις συναλλαγές τους. Ένα μειονέκτημα του DPoS είναι το γεγονός ότι χάνει τον αποκεντρωμένο χαρακτήρα του, λόγω της παραχώρησης ευθυνών σε ένα σχετικά μικρό αριθμό

κόμβων, μη θεωρώντας το δημοκρατικό αλλά αντιπροσωπευτικό, πηγαίνοντας κόντρα στην αρχική ιδέα του blockchain [29].

Μία γνωστή εφαρμογή του DPoS είναι η πλατφόρμα EOS.IO. Οι κάτοχοι EOS tokens εκλέγουν 21 κόμβους που ονομάζονται παραγωγοί (producers), οι οποίοι θα έχουν την ευθύνη παραγωγής blocks και την αντάμειψη τους για κάθε νέο block. Για να αποφευχθεί κάποια κακόβουλη ενέργεια, με την ολοκλήρωση κάθε γύρου επιλέγονται καινούργοι παραγωγοί. Στην περίπτωση που κάποιος κόμβος δεν ακολουθεί σωστά τις ευθύνες του τότε αποκλείεται από την διαδικασία εκλογής. Η δημιουργία καινούργιων blocks πραγματοποιείται ταχύτατα συγκριτικά με πιο δημοφιλείς εφαρμογές (ETH, BTC) και συγκεκριμένα ανά 3 δευτερόλεπτα για κάθε block με το ρεκόρ της να είναι οι 3996 συναλλαγές το δευτερόλεπτο, σύμφωνα με το EOS network monitor [30].

Μία άλλη εφαρμογή του DPoS είναι το Lick, το οποίο επιδιώκει να αυξήσει την ασφάλεια του δικτύου με ορισμένες τροποποιήσεις. Για να το επιτύχει αυτό, κατά την ψηφοφορία το ποντάρισμα του κάθε κόμβου κρατάτε από το σύστημα και δεν μπορεί να χρησιμοποιηθεί μέχρι το τέλος της. Επίσης, μία ακόμα αλλαγή είναι η μείωση των ψήφων σε μία ανά χρήστη τη φορά.

Μία τρίτη εφαρμογή του DPoS είναι η πλατφόρμα BitShares κατά την οποία οι εκλεγμένοι κόμβοι προκύπτουν ανάλογα με το πόσα tokens κατέχουν. Ο αριθμός των εκπροσώπων καθορίζεται σε κάθε γύρο από τους stakeholders, αλλά δεν μπορούν να είναι λιγότεροι από 11. Η έγκριση και δημιουργία του κάθε block από τους κόμβους γίνεται και σε αυτήν πολύ γρηγορά (2-3 δευτερόλεπτα ανά block), με μέγιστο θεωρητικό όριο τις 100.000 συναλλαγές το δευτερόλεπτο, σύμφωνα με την πλατφόρμα Graphene [31].

3.2.3 Leased Proof of Stake (LPoS)

Το πρωτόκολλο LPoS λειτουργεί κατά ένα μεγάλο ποσοστό όμοια με το πρωτόκολλο PoS, δημιουργήθηκε όμως με στόχο την λύση ορισμένων μειονεκτημάτων του. Ένα χαρακτηριστικό του συγκεκριμένου μηχανισμού συναίνεσης είναι η δυνατότητα δανεισμού ενός μέρους του μεριδίου των κόμβων σε άλλους χρήστες, με σκοπό την αύξηση του stake των δεύτερων άρα και την αύξηση των πιθανοτήτων επιλογής για την δημιουργία block. Το LPoS θεωρείται πιο αποκεντρωμένο συγκριτικά με το προαναφερθέν DPoS, μιας και οι κόμβοι που συμμετέχουν στην διαδικασία δημιουργίας block είναι περισσότεροι.

Μία εφαρμογή βασισμένη στο LPoS είναι η ShareRing, κατά την οποία εάν ένας κόμβος επιθυμεί να δανείσει ένα μέρος του μεριδίου του σε έναν άλλο κόμβο τότε μπορεί να του ζητήσει ως αντάλλαγμα ένα ποσοστό από την αμοιβή που θα λάβει ο δεύτερος κόμβος εάν επιλεχθεί να δημιουργήσει block. Η ψήφος ενός κόμβου (mastenode) είναι ανάλογη με τις πιθανότητες να ψηφιστεί για να παράγει block (proposer), ενώ αυτές μπορούν να αυξηθούν σύμφωνα με το μερίδιο που του έχουν δανείσει άλλοι κόμβοι, με ένα προκαθορισμένο όριο όμως από το σύστημα ισότητας των ψηφοφόρων.

Μία δεύτερη LPoS-based εφαρμογή είναι η Waves, όπου σε συνεργασία με την Deloitte παρέχει στους κόμβους δύο επιλογές ενέργειας. Η μία είναι η κλασσική συμμετοχή τους για την δημιουργία block (full nodes) και η άλλη είναι η παραχώρηση του μεριδίου τους με μορφή δανείου σε άλλους κόμβους (leasers), μοιράζοντας την αμοιβή παραγωγής block ανάμεσα σε δανειστές και δανειζόμενους. Ειδικά η δεύτερη μέθοδος (leasing) συνεισφέρει στον αποκεντρωτισμό του συστήματος, χάρης την αύξηση του αριθμού των επιλεγόμενων κόμβων που οδηγεί στην ελάττωση των πιθανοτήτων συγκέντρωσης του ελέγχου από μία συγκεκριμένη μικρή ομάδα κόμβων του δικτύου [32].

3.2.4 Proof of Importance (PoI)

Ο μηχανισμός συναίνεσης PoI είναι ακόμη μία παραλλαγή του πρωτοκόλλου PoS και η πρώτη χρήση του ήταν μέσω του κρυπτονομίσματος XEM στο δίκτυο που διαθέτει, το NEM. Μία σημαντική διαφοροποίηση του είναι ο διαχωρισμός των κρυπτονομισμάτων του κάθε χρήστη σε καταχωρημένα (vested balance) και μη καταχωρημένα (unvested balance). Η αναλογία ανάμεσα στα δύο μέρη παραμένει σχετικά σταθερή, καθώς με την πραγματοποίηση κάθε συναλλαγής τα δύο μέρη μεταβάλλονται κάθε φορά ώστε να έρθουν σε ισορροπία. Ο κάθε κόμβος μπορεί να χρησιμοποιήσει 10.000 καταχωρημένα XEMs για να του δοθεί το δικαίωμα να δημιουργήσει ένα block, που εδώ αυτή η διαδικασία ονομάζεται συγκομιδή (harvesting), λαμβάνοντας την ανάλογη αμοιβή που του ισοδυναμεί σύμφωνα με την βαθμολογία σπουδαιότητας (importance score) που κατέχει μέσα στο δίκτυο. Η συμμετοχή των κόμβων στην διαδικασία ομοφωνίας καθορίζεται και αυτή από τη βαθμολογία σπουδαιότητας, η οποία εξαρτάται από πολλές παραμέτρους (σύνολο ολοκληρωμένων συναλλαγών κόμβου, συμπεριφορά κόμβου μέσα στο δίκτυο). Άρα καταλαβαίνουμε ότι το importance score του κάθε κόμβου είναι το στοιχείο που κάνει το PoI να διαφέρει από το PoS. Η διαδικασία αυτή το κάνει να είναι λίγο πιο αργό από το DPoS με την ταχύτητα παραγωγής του κάθε block να κυμαίνεται στο 1 λεπτό περίπου και οι συναλλαγές το δευτερόλεπτο να είναι γύρω στις 3085 [33].

3.3 Υβριδικά Συστήματα (PoW/PoS) – Proof of Activity (PoA)

Τα τελευταία χρόνια έχουν δημοσιευθεί διάφορα υβριδικά συστήματα μαζί με πληθώρα παραλλαγών του PoW και του PoS, με σκοπό την πρόταση βελτιωμένων μηχανισμών, έχοντας διορθώσει κάποια από τα μειονεκτήματα που υστερούσαν οι κλασσικοί μηχανισμοί. Ο πιο γνωστός όμως υβριδικός μηχανισμός συναίνεσης είναι το PoA, το οποίο και θα αναλυθεί στην συνέχεια [34].

Το PoA αποτελεί ένα συνδυασμό των PoW και PoS μηχανισμών, με στόχο να περιορίσει την μεγάλη ενεργειακή δαπάνη του πιο δημοφιλούς κρυπτονομίσματος, του BTC. Για να το επιτύχει αυτό, αποφάσισε να διαχωρίσει την διαδικασία επίτευξης ομοφωνίας σε δύο μέρη, το mining και το voting:

1. Αρχικά, οι PoW κόμβοι, οι λεγόμενοι miners, για να δημιουργήσουν το επόμενο στη σειρά block ανταγωνίζονται ο ένας τον άλλο. Όταν δημιουργηθεί, το καινούργιο block θα κατέχει μόνο την διεύθυνση και την κεφαλή του κόμβου που το δημιούργησε, χωρίς να αναφέρεται οποιαδήποτε συναλλαγή.
2. Στη συνέχεια, κάποιοι PoS κόμβοι, οι λεγόμενοι validators, κερδίζουν το δικαίωμα της έγκρισης του καινούργιου block με την τοποθέτηση της υπογραφής τους και ο τελευταίος κόμβος τοποθετεί σε αυτό τις επιθυμητές συναλλαγές.

Η παραπάνω διαδικασία δημιουργίας νέων block στηρίζεται στον παράγοντα coinage, που ουσιαστικά είναι το γινόμενο μίας ποσότητας νομισμάτων ενός χρήστη επί το χρονικό διάστημα που βρίσκονται στην ιδιοκτησία του. Με την ολοκλήρωση της δημιουργίας τα block πριμοδοτούνται με το μεγαλύτερο coinage και τα νομίσματα που μπαίνουν σε κυκλοφορία είναι το 1% εκείνων που έχουν δαπανηθεί μέσα σε ένα coin-year [35].

Ο παραπάνω διαχωρισμός, προσφέρει μία ασφάλεια ως προς ορισμένες γνωστές απειλές των μηχανισμών συναίνεσης, με πιο σημαντικές το 51% Attack (Ενότητα 3.9.3) και το Double-spending (Ενότητα 3.9.5). Επίσης, είναι πιο δίκαιο, διότι η τελική ανταμοιβή μοιράζεται ανάμεσα σε όλους τους συμμετέχων κόμβους, σε αντίθεση με το PoS που η αμοιβή πάει μόνο στον ισχυρότερο κόμβο. Παρόλα αυτά, ενώ απώτερος σκοπός της δημιουργίας του είναι η μείωση της ενεργειακής σπατάλης, δεν το καταφέρνει στο έπακρο. Αυτό οφείλεται στο ότι είναι βασισμένο στον PoW μηχανισμό σε κύρια σημεία και έτσι χρειάζεται ακόμη ακριβό εξοπλισμό για το mining και η κατανάλωση πόρων είναι αναπόφευκτη. Επιπλέον, λόγω της υβριδικής μορφής του χρειάζεται και περισσότερο χρόνο για την ολοκλήρωση των συναλλαγών συγκριτικά με τους δύο κλασσικούς μηχανισμούς στους οποίους στηρίζεται μεμονωμένα [36].

3.4 Proof of Elapsed Time (PoET)

Ένας λίγο διαφορετικός μηχανισμός συναίνεσης αποτελεί το PoET της Intel, του οποίου η βασικότερη χρήση πραγματοποιείται στην πλατφόρμα Hyperledger Sawtooth της Linux. Ο συγκεκριμένος μηχανισμός λειτουργεί μέσα σε ένα έμπιστο περιβάλλον εκτέλεσης, το Software Guard Extensions (SGX), με αυξημένες επεκτάσεις ασφαλείας, τις SGX CPUs (2017). Οι συγκεκριμένες επεκτάσεις παρέχουν προστασία για εκτέλεση αξιόπιστου κώδικα και σε δεδομένα γνωστοποίησης ή τροποποίησης. Σε κάθε κόμβο του δικτύου ορίζεται ένας χρόνος αναμονής για το δικαίωμα δημιουργίας του επόμενου block. Ένα σημαντικό προτέρημα σε σύγκριση με τον μηχανισμό PoW είναι η μείωση ανάγκης συναγωνισμού ως προς την υπολογιστική ισχύ του κάθε χρήστη. Ένας σημαντικός παράγοντας της επιτυχίας αυτού του στόχου είναι η αύξηση της απόδοσης των συστημάτων λόγω της διάθεσης σε άλλα έργα των επεξεργαστών όταν δεν συμμετέχουν στην διαδικασία. Παρόλα αυτά, οι κόμβοι θα χρειαστούν όμως να επιλύσουν προβλήματα κατακερματισμού παρόμοια με το PoW. Αυτό ευθύνεται στο SGX και το τυχαίο μοντέλο εκλογής που έχει τεθεί, ώστε να ωφελείται ο κόμβος με τον συγκριτικά μικρότερο χρόνο αναμονής, οι οποίοι χρόνοι διανέμονται τυχαία από το σύστημα. Κατά την ολοκλήρωση δημιουργίας του κάθε block, για να γίνει αποδεκτό από το σύνολο του δικτύου, χρειάζεται ο υπεύθυνος κόμβος να αποδείξει τον χρόνο που έμεινε σε κατάσταση αναμονής και ότι δεν εξέπεμπε το νέο block πρόωρα. Οι αποδείξεις αυτές όμως πραγματοποιούνται μόνο μέσω της Υπηρεσίας Πιστοποιήσεων της Intel (IAS), το οποίο θέτει τον όλο μηχανισμό ως μερικώς αποκεντρωμένος. Η προηγούμενη διαδικασία είναι αναγκαία για την παροχή δικαιοσύνης και ισότητας ανάμεσα στο δίκτυο, που σε συνδυασμό με την χρήση ειδικού hardware μετατρέπεται σε ένα αρκετά ανθεκτικό μοντέλο. Αυτός ο ειδικός εξοπλισμός hardware όμως αποτελεί παράλληλα και ένα βασικό μειονέκτημα του μηχανισμού, διότι εξαρτώνται αλληλένδετα μεταξύ τους. Μία κακόβουλη επίθεση είναι πιο πιθανόν να είναι επιτυχημένη όταν μία πλατφόρμα στηρίζεται καθαρά και μόνο στο έμπιστο περιβάλλον εκτέλεσης του PoET. Στην περίπτωση που οι κακόβουλοι κόμβοι ξεπεράσουν τους:

$$\Theta\{[\frac{\log(logn)}{logn}\}$$

όπου n το σύνολο των κόμβων, τότε το σύστημα μπορεί να κινδυνέψει. Ωστόσο, η Intel έχει μεριμνήσει για τον εντοπισμό κακόβουλων ενεργειών με το να θέσει ένα μετρητή που σημειώνει τις φορές που κέρδισε ο κάθε κόμβος στο SGX.
Το συγκεκριμένο μειονέκτημα, χωρίζεται σε δύο περιπτώσεις:

- Broken Chip Problem: Στην περίπτωση παραβίασης της ασφάλειας του συστήματος, ο επιτιθέμενος κόμβος μπορεί να κερδίζει συνέχεια στην κλήρωση. Το πρόβλημα όμως επιλύεται με την χρήση στατιστικής ανάλυσης στους νέους κόμβους.
- Stale Chip Problem: Θεωρητικά, σε κάθε καινούργιο ολοκληρωμένο που εισάγεται στο δίκτυο προσφέρεται και μία ακόμη ψήφος για την κλήρωση, το οποίο μπορεί να οδηγήσει σε συγκεντρωτισμό [37].

Μία ακόμη ενδιαφέρουσα υλοποίηση μέσω του PoET είναι το REM, το οποίο είναι μία υβριδική προσέγγιση με το PoW, δημιουργώντας το πρωτόκολλο Proof of Useful Work (PoUW). Μέσω αυτού, δίνεται η δυνατότητα χρήσης των SGX CPUs για χρήσιμους υπολογισμούς, παράλληλα με τη συμμετοχή τους στον μηχανισμό. Επιπλέον, οι δημιουργοί του υποστηρίζουν ότι η πλατφόρμα τους έχει αντιμετωπίσει το stale chip problem, λειτουργώντας έτσι ώστε πριμοδοτείτε η εργασία και όχι η κατοχή ολοκληρωμένων [38].

3.5 Proof of Trust (PoT)

Το πρωτόκολλο PoT αποτελεί ένα κοινοπρακτικό σύστημα, μέσα σε ένα δημόσιο δίκτυο και στηρίζεται στον αλγόριθμο εκλογικής ηγεσίας Raft (2014) [39]. Ο αλγόριθμος δέχεται εντολές από έναν χρήστη-πελάτη (client) τη φορά, οι οποίες εκτελούνται εάν υπάρξει συμφωνία ανάμεσα στο μεγαλύτερο μέρος των κόμβων του συστήματος διακομιστών (server). Οι διακομιστές έχουν στην διάθεσή τους:

- Αρχεία καταγραφής (logs), όπου μέσα σε ένα τέτοιο αρχείο η εντολή του πελάτη αποθηκεύεται και διαμοιράζεται στα αρχεία όλων των διακομιστών.
- Μηχανές κατάστασης (state machines), όπου μία τέτοια μπορεί να είναι ένα μηχάνημα, μία εφαρμογή ή ακόμη και ένα πρόγραμμα, στοχεύοντας, έπειτα από ομοφωνία στην πλειοψηφία του δικτύου, στην εκτέλεση της εντολής του πελάτη από το αρχείο [40].

Η συναίνεση σε ένα τέτοιο σύστημα επιτυγχάνεται με την εκτέλεση 4 φάσεων:

1. Εκλέγεται αποκλειστικά ένας κόμβος-ηγέτης από τα μέλη της ομάδας, των οποίων ο αριθμός είναι προκαθορισμένος από το σύστημα και χωρίζονται στις εξής κατηγορίες:

- Ηγέτης (Leader), ο οποίος ηγείται της ομάδας διαχείρισης του κοινοπρακτικού συστήματος (ledger management group), καθώς επιβλέπει και διαχειρίζεται τις αλληλεπιδράσεις του συστήματος, δηλαδή τα αναπαραγόμενα καταγεγραμμένα αρχεία (replicated logs). Επίσης, είναι ο κόμβος που δέχεται τις καταχωρήσεις καταγραφής (log entries), δηλαδή τις εντολές των πελατών, τοποθετώντας τες στα αρχεία των διακομιστών.

- Υποψήφιοι (Candidates), οι οποίοι αναμένουν την εκλογή τους ως ηγέτες.

- Ακόλουθοι (Followers), οι οποίοι είναι παθητικοί διακομιστές και η θέση από την οποία ξεκινούν όλοι οι κόμβοι, όπου αναμένουν από τον ηγέτη τις κλήσεις απομακρυσμένων διαδικασιών, ή αλλιώς Remote Procedure Calls (RPCs), που χωρίζονται σε δύο είδη:

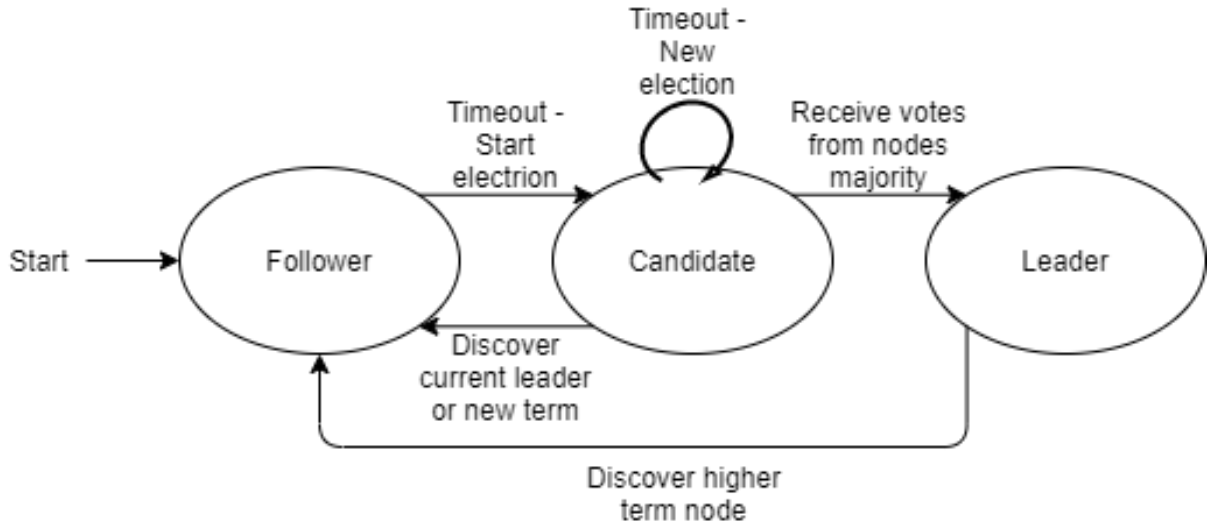
   A. AppendEntries RPCs, τα οποία τα χρησιμοποιεί ο ηγέτης ώστε να αναπαράγει σε όλους τους διακομιστές τα αρχεία καταγραφής και να αποστέλλουν ενημερώσεις για την κατάσταση τους (heartbeat), δηλαδή αν είναι πλέον εκλεγμένοι ως ηγέτες ή αν είναι γενικά ακόμα ενεργοί.
   B. RequestVote RPCs, τα οποία τα χρησιμοποιούν οι υποψήφιοι ηγέτες στην διαδικασία εκλογής καινούργιου ηγέτη.
2. Στη συνέχεια, ο ηγέτης συνθέτει μία λίστα με επικυρωτές, βασισμένος σε βασικά κριτήρια, όπως ο βαθμός εμπιστοσύνης (trust value). Έπειτα, διαλέγει από την συγκεκριμένη λίστα ορισμένους χρήστες οι οποίοι θα αποτελέσουν την ομάδα επικύρωσης συναλλακτικών υπηρεσιών (service transaction validation group).
3. Η ομάδα επικύρωσης από το προηγούμενο στάδιο έχει ως στόχο την επιλογή και εκλογή των συναλλαγών, οι οποίες θα συμπεριληφθούν στο καινούργιο block.
4. Στο τελευταίο βήμα, η ομάδα διαχείρισης του συστήματος εκλέγει ξανά τις συναλλαγές και ο ηγέτης αναλαμβάνει την συγκέντρωση, αξιολόγηση και εγκατάσταση του καινούργιου block [41].

Ο κάθε γύρος ξεκινάει εκλέγοντας τον καινούργιο ηγέτη και τερματίζει όταν εκτελεστεί η εντολή που έδωσε, με τα χρονικά διαστήματα να είναι διαχωρισμένα με διαδοχικά αριθμημένους ακέραιους αριθμούς σε όρους (terms). Αν η εκλογή του ηγέτη δεν είναι επιτυχής τότε η όλη διαδικασία ξεκινάει πάλι από την αρχή με καινούργιο όρο, ενώ ο διακομιστής αποθηκεύει τον πιο πρόσφατο όρο του (current term), σε περίπτωση που ο ηγέτης δεν είναι ενημερωμένος ή μπει σε ανενεργή κατάσταση. Επίσης, ο αριθμός του όρου μπορεί συνεισφέρει στην επίλυση μίας αντικρουόμενης απόφασης δύο ή περισσοτέρων διακομιστών, μιας και ο συγκεκριμένος αριθμός καθορίζει την πιο πρόσφατη απόφαση του ηγέτη που έχει ληφθεί από το σύστημα.

Στην περίπτωση που ο ηγέτης σταματήσει να φαίνεται ενεργός για ένα συγκεκριμένο χρονικό διάστημα, τότε οι υπόλοιποι κόμβοι επανεκλέγουν καινούργιο ηγετικό κόμβο. Ένας ακόλουθος που επιθυμεί να γίνει υποψήφιος ηγέτης πρέπει να αλλάξει τον πρόσφατο όρο του, στη συνέχεια να ψηφίσει τον εαυτό του και τέλος να στείλει σε όλους τους διακομιστές RequestVote RPCs. Στη συνέχεια, υπάρχουν 3 περιπτώσεις που μπορούν να πραγματοποιηθούν στον κόμβο:

- Να ψηφισθεί από την πλειοψηφία των κόμβων και να εκλεγεί ηγέτης, όπου έπειτα πρέπει να ενημερώσει όλους τους υπόλοιπους διακομιστές, ώστε να τερματίσει η διαδικασία της εκλογής.
- Άλλος υποψήφιος κόμβος να εκλεγεί, όπου τότε όλοι οι υπόλοιποι υποψήφιοι δέχονται AppendEntries RPC από έναν άλλο διακομιστή και αλλάζουν την θέση τους πάλι σε ακόλουθοι.
- Να περάσει ένα προκαθορισμένο, από το σύστημα, χρονικό διάστημα (100-500ms) και κανένας υποψήφιος κόμβος να μην συλλέξει την πλειοψηφία των ψήφων ώστε να εκλεγεί, με την διαδικασία ψηφοφορίας να ξεκινάει πάλι από την αρχή με καινούργιο όρο.

Ο νέος εκλεγμένος ηγετικός κόμβος πρέπει να στείλει με AppendEntries RPCs τις εντολές που θα δέχεται, από τους πελάτες που τον ψήφισαν, στα αρχεία των διακομιστών. Στη συνέχεια, επιβεβαιώνεται ότι όλοι οι διακομιστές έλαβαν τα αρχεία και μόνο τότε οι μηχανές κατάστασης εκτελούν την εντολή, με τον πελάτη να λαμβάνει το αποτέλεσμα.



Εικόνα 13 - Λειτουργία αλγορίθμου Raft

Η διαδικασία λειτουργίας του μηχανισμού PoT παρέχει βελτιωμένη διακίνηση και επεκτασιμότητα, καθώς και διανεμημένη διακυβέρνηση, σε σχέση με δημοφιλέστερα πρωτόκολλα. Λόγω της ανάγκης για εμπιστοσύνη ανάμεσα στους κόμβους του δικτύου, το PoT χρησιμοποιείται περισσότερο σε ιδιωτικές blockchain εφαρμογές, μιας και λειτουργεί πιο αποδοτικά για προκαθορισμένο μικρό αριθμό κόμβων. Ο αλγόριθμος μπορεί να αντιμετωπίσει μόνο αποτυχίες εξαρτημάτων, λογισμικού και κακής επικοινωνίας των κόμβων, αλλιώς Crash Fault Tolerance (CFT), μένοντας εκτεθειμένος στους κακόβουλους κόμβους, αλλιώς Byzantine Fault Tolerance Failures (BFTF). Η δημοφιλέστερη εφαρμογή του πρωτοκόλλου είναι το Quorum, η οποία είναι βασισμένη στο ETH και λειτουργεί παράλληλα με το PoW [14].

3.6 Proof of Vote (PoV)

Το πρωτόκολλο συναίνεσης PoV δημιουργήθηκε με στόχο την αύξηση των επιδόσεων, την μείωση της ενεργειακής δαπάνης και την θωράκιση της ασφάλειας εφαρμογών οι οποίες είναι σχεδιασμένες βασισμένες αποκλειστικά σε κοινοπρακτικό σύστημα. Η αποκέντρωση επιτυγχάνεται, κατά την διαδικασία ψηφοφορίας, με τον διαμοιρασμό των δικαιωμάτων στους κόμβους που συμμετέχουν στον μηχανισμό, οι οποίοι χωρίζονται σε 4 κατηγορίες:

- απλός χρήστης (ordinary user)
- βοηθός (butler)
- υποψήφιος βοηθός (butler candidate)
- επίτροπος (commissioner).

Μόνο η πρώτη επιβεβαίωση είναι αρκετή για την δημιουργία κάθε block, καθιστώντας την οριστικότητα του συστήματος άμεση. Η διακίνηση λειτουργεί πολύ θετικά, όπως και οι χρονικές καθυστερήσεις που είναι ελάχιστες, γεγονός που φαίνεται από τον χρόνο παραγωγής των blocks ο οποίος κυμαίνεται στα 15 δευτερόλεπτα ανά block, δεδομένο που καθιστά το PoV πολύ ταχύτερο από το κατά πολύ δημοφιλέστερο PoW. Ο κύριος λόγος αναφοράς του μηχανισμού συναίνεσης PoV είναι η κατανόηση της λειτουργίας του και η διαφοροποίηση του με τα vote-based συστήματα που θα αναφερθούν στην επόμενη ενότητα [42].

3.7 Vote-based Consensus Mechanisms

Τα vote-based συστήματα είναι μία λίγο διαφορετική κατηγορία μηχανισμού συναίνεσης σε σχέση με τα proof-based συστήματα ως προς την επίτευξη ομοφωνίας στο δίκτυο. Στο συγκεκριμένο μηχανισμό, η κοινή συναίνεση μεταξύ των κόμβων του δικτύου επιτυγχάνεται μέσω μίας διαδικασία ψηφοφορίας, η οποία διαφέρει από εφαρμογή σε εφαρμογή αναλόγως την χρήση της. Η πιο γνωστή εφαρμογή vote-based πρωτοκόλλου είναι το Tendermint, η οποία λειτουργεί με γύρους ψηφοφορίας [43]. Ο κάθε γύρος αποτελείται από 5 φάσεις:

1. Propose: Στο πρώτο στάδιο του γύρου προτείνεται ο κόμβος που θα διεξάγει πρόταση για δημιουργία νέου block στο δίκτυο (Proposer), με τους κόμβους που τον συνορεύουν να πρέπει να την μεταδώσουν σε όλο το υπόλοιπο δίκτυο.

2. Prevote: Στο δεύτερο στάδιο, διεξάγεται η ψηφοφορία, κατά την οποία κάθε κόμβος ψηφίζει για το καινούργιο block που θέλει να προστεθεί και το μοιράζεται με όλους τους κόμβους στο δίκτυο.
3. Precommit: Στην τρίτη φάση, μία πρόταση block από το προηγούμενο στάδιο για να θεωρηθεί έγκυρη χρειάζεται να έχει ψηφισθεί τουλάχιστον από τα 2/3 των κόμβων του δικτύου. Τον έλεγχο αυτής της διαδικασίας αναλαμβάνει ο επικυρωτής και όσες προτάσεις διαπιστωθούν ότι δεν έχουν συλλέξει το κατάλληλο αριθμό ψήφων επιστρέφουν πάλι στο πρώτο στάδιο (Propose) που θα διαδεχθεί τον επόμενο γύρο.

4. Commit: Στο τέταρτο στάδιο, οι υπόλοιποι κόμβοι του δικτύου αποφασίζουν και δεσμεύονται για την ένταξη του block που ψηφίστηκε και πέρασε από την προηγούμενη φάση. Εάν υπάρξει συμφωνία μεταξύ τους, το block δεν εντάσσεται αμέσως, αλλά διατηρείται μία αναμονή στο δίκτυο για ένα συγκεκριμένο χρονικό διάστημα για πιθανούς ψήφους που δεν έφτασαν εγκαίρως εξαιτίας κάποιας καθυστέρησης.

5. NewHeight: Κατά το πέμπτο και τελευταίο στάδιο, το block του κόμβου που προέκυψε από την διαδικασία της ψηφοφορίας εντάσσεται στην κορυφή και ξεκινάει πάλι από την αρχή με την έναρξη του επόμενου γύρου [44].

Έχει ήδη γίνει αναφορά σε προηγούμενες ενότητες στα πρωτόκολλα LPoS (3.2.3) και DPoS (3.2.2), γι'αυτό και θα τα περιγράψουμε για ακόμη μία φορά συνοπτικά ώστε να γίνουν αντιληπτές οι διαφορές τους σε σχέση με την διαδικασία ψηφοφορίας των vote-based συστημάτων:

- Η διαδικασία της ψηφοφορίας στις LPoS εφαρμογές πραγματοποιείται μεταξύ των κόμβων, δίνοντας τους επιπλέον την δυνατότητα δανεισμού του μεριδίου τους σε άλλους κόμβους. Η διαδικασία του δανεισμού σε εκπροσώπους τους πραγματοποιείται μέσω ψηφοφορίας των κόμβων του δικτύου, αυξάνοντας τις πιθανότητες του επιλεγμένου κόμβου να ψηφισθεί για την δημιουργία του νέου block. Η αμοιβή όμως της παραγωγής block του επιλεγμένου κόμβου θα μοιραστεί ισάξια ανάμεσα σε αυτόν και στους κόμβους που του δάνεισαν το μερίδιο τους, εάν υπήρξαν.

- Στις DPoS εφαρμογές πρέπει να πραγματοποιείται η διαδικασία ψηφοφορίας, διότι συντελεί στην ομοφωνία μεταξύ των κόμβων του δικτύου ώστε να παραχθεί το καινούργιο block και να προστεθεί στην αλυσίδα. Οι κόμβοι ψηφίζουν, ανά εκλογικούς γύρους, ανάμεσα από μία ομάδα χρηστών οι οποίοι έχουν εκλεχθεί από το σύστημα, με ένα ορισμένο από την εφαρμογή αριθμητικό μέγεθος, χρησιμοποιώντας το μερίδιο τους. Ο κόμβος που θα συλλέξει τις περισσοτέρους ψήφους θα του δοθεί το δικαίωμα να δημιουργήσει το επόμενο block της αλυσίδας, εισπράττοντας και την αντίστοιχη αμοιβή.

3.8 Byzantine Fault Tolerance (BFT)

Οι αλγόριθμοι που είναι ανθεκτικοί σε βυζαντινές αποτυχίες, ή αλγόριθμοι βυζαντινής συμφωνίας, ή αλλιώς Byzantine Agreement (BA), είναι μία διαφορετική μορφή μηχανισμών συναίνεσης σε σχέση με τα proof-based πρωτόκολλα. Στα BFT και BA συστήματα κατά την διαδικασία επίτευξης ομοφωνίας, οι κόμβοι του δικτύου εκτελούν διάφορα στάδια και μορφές ψηφοφοριών. Αυτό συμβαίνει για την αποτροπή κάποιου κακόβουλου κόμβου που θα επιχειρήσει να επιτεθεί στο σύστημα ή ακόμη και να παροτρύνει άλλους κόμβους να τον βοηθήσουν έμμεσα, στέλνοντας τους λανθασμένες εντολές. Τα βυζαντινά πρωτόκολλα σκοπεύουν στην επίτευξη ομοφωνίας μεταξύ των χρηστών, καταπολεμώντας παράλληλα κλασσικά σφάλματα του blockchain, αλλά και γενικότερα των διανεμημένων συστημάτων, όπως τις βυζαντινές αποτυχίες (byzantine failures) και τις αποτυχίες σύγκρουσης (crash failures) [34].

3.8.1 Practical Byzantine Fault Tolerance (PBFT)

Ο αλγόριθμος PBFT δημιουργήθηκε λόγω της ανάγκης ενός μηχανισμού συναίνεσης στα διανεμημένα συστήματα για την καταπολέμηση των Βυζαντινών επιθέσεων. Το κύριο δομικό χαρακτηριστικό του αποτελεί η απαραίτητη εμπιστοσύνη που πρέπει να υπάρχει ανάμεσα στους κόμβους του δικτύου. Για αυτό το λόγο λειτουργεί βέλτιστα σε σχετικά μικρό αριθμό χρηστών, ώστε οι συναλλαγές να πραγματοποιούνται ταχύτατα. Η λειτουργία του PBFT συντελείται με την λήψη αιτημάτων πελατών από τον ηγέτη σε συνδυασμό με ένα μοντέλο ψηφοφορίας επαναλαμβανόμενων μηχανημάτων κατάστασης (replicated state machines). Στην ψηφοφορία λαμβάνουν μέρος ο κόμβος-ηγέτης (leader node) και οι απλοί κόμβοι του δικτύου (validating nodes), ενώ η ολοκλήρωση των συναλλαγών πραγματοποιείται έπειτα από πολλούς γύρους ψηφοφοριών [45].

Η πραγματοποίηση των συναλλαγών εκτελείται μέσα από 5 στάδια:

1. Αίτηση (Request): Ο πελάτης στέλνει ένα αίτημα συναλλαγής και το αποδέχεται ο κόμβος-ηγέτης, ή αλλιώς πρωταρχικός κόμβος (primary node). Στη συνέχεια ο ηγέτης προσάπτει στο αίτημα μία χρονική σήμανση (timestamp) και το προωθεί στους υπόλοιπους πανομοιότυπους κόμβους (replicas).

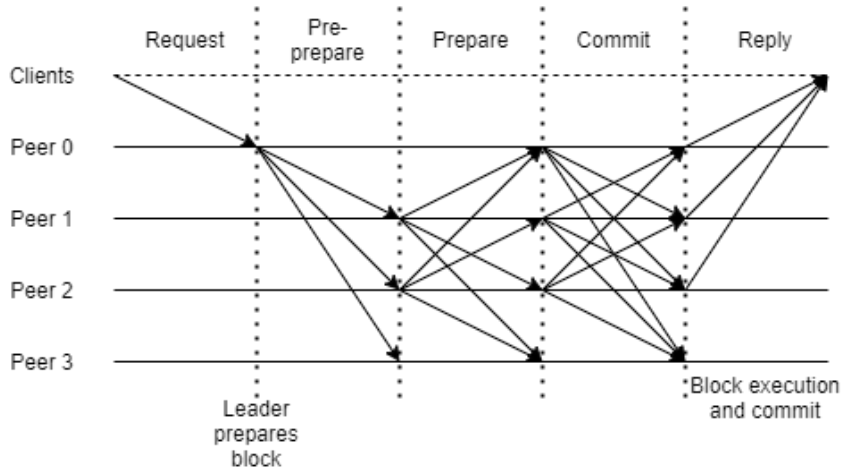
2. Προ-Προετοιμασία (Pre-Prepare): Ο κόμβος-ηγέτης στέλνει στους υπόλοιπους κόμβους του δικτύου ένα μήνυμα μόνο με την χρονική σήμανση του αιτήματος (χωρίς το ίδιο το αίτημα) για να αποδείξει την εγκυρότητα του, ώστε και εκείνοι έπειτα να το αποδεχτούν ή να το απορρίψουν.

3. Προετοιμασία (Prepare): Οι κόμβοι που έχουν λάβει το μήνυμα του κόμβου-ηγέτη στέλνουν και εκείνοι από ένα μήνυμα αποδοχής ή απόρριψης ο καθένας σε όλους τους κόμβους του δικτύου, ενώ αν η πλειοψηφία (2/3) δεχτεί το αίτημα, τότε η διαδικασία προχωράει.

4. Δεσμεύω (Commit): Οι κόμβοι που αποδέχτηκαν το αίτημα στέλνουν ένα ακόμη μήνυμα προς όλους τους υπόλοιπους κόμβους του δικτύου και όταν ληφθεί από την πλειοψηφία των κόμβων τότε εκτελείται.

5. Απάντηση (Reply): Ο πελάτης δέχεται την απάντηση του αιτήματος του από τον κόμβο-ηγέτη με την ολοκληρωμένη συναλλαγή του [43].

Στην περίπτωση όμως που ο ισχύον κόμβος-ηγέτης δεν δείχνει σημάδια ότι είναι πλέον διαθέσιμος με το να στέλνει αιτήματα και το αντιληφθεί τουλάχιστον η πλειοψηφία των κόμβων του δικτύου στέλνοντας μηνύματα στους υπόλοιπους, τότε ενεργοποιείται το πρωτόκολλο view change για την εκλογή καινούργιου. Το συγκεκριμένο πρωτόκολλο έχει 3 στάδια εκτέλεσης, επιλέγοντας αρχικά έναν κόμβο από το δίκτυο ώστε να αντικαταστήσει τον ηγέτη. Στην συνέχεια, εκείνος στέλνει από ένα μήνυμα σε όλους τους υπόλοιπους κόμβους για την επιβεβαίωση ότι ο κόμβος-ηγέτης είναι σίγουρα εκτός λειτουργίας. Εάν η πλειοψηφία των κόμβων του απαντήσουν με δικό τους μήνυμα με την επιβεβαίωση του γεγονότος τότε εκείνος εκλέγεται ως ο νέος ηγετικός κόμβος [46].



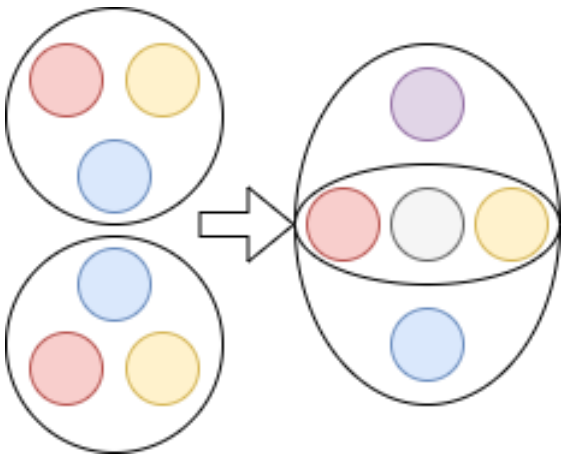
Εικόνα 14 - Λειτουργία PBFT αλγορίθμου

Στο συγκεκριμένο πρωτόκολλο η ομοφωνία επιτυγχάνεται μέσα από την συμφωνία της πλειοψηφίας, γεγονός που το κάνει αρκετά αποδοτικό, με σχεδόν ανύπαρκτες καθυστερήσεις και ελάχιστο κόστος ενέργειας. Παρόλα αυτά, η εφαρμογή του αλγορίθμου σε ένα δημόσιο δίκτυο θα τον καθιστούσε ευάλωτο σε επιθέσεις λόγω την ελεύθερης εισόδου χρηστών, όπως και η εφαρμογή του σε ένα δίκτυο με πολλούς χρήστες θα μείωνε την απόδοση του [47]. Για αυτό το λόγο ο PBFT εφαρμόζεται κυρίως σε ιδιωτικά δίκτυα με ορισμένο αριθμό χρηστών, με πιο γνωστό το Hyperledger Fabric (2016), εκτελώντας μέχρι και 3500 συναλλαγές το δευτερόλεπτο [48].

3.8.2 Stellar Consensus Protocol (SCP)

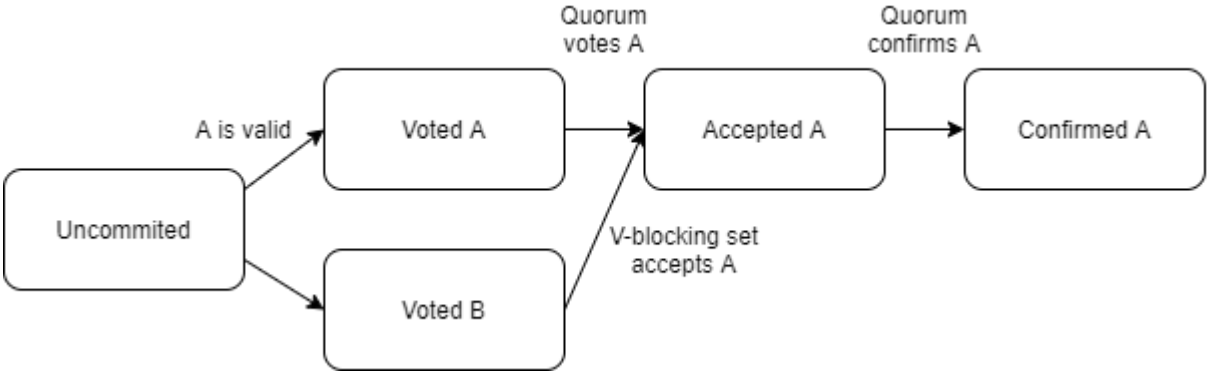
Το SCP πρωτόκολλο δημιουργήθηκε για την επίτευξη ομοφωνίας της πλειοψηφίας μεταξύ των χρηστών της πλατφόρμας Stellar, βασισμένο στο πρωτόκολλο ομοσπονδιακής βυζαντινής συμφωνίας (Federated Byzantine Agreement). Στο FBA πρωτόκολλο οι συμμετέχοντες κόμβοι διαλέγουν τα μέλη της ομάδας έμπιστων κόμβων τους (quorums), όπου το κάθε μέλος αποτελεί ένα quorum slice και συνεργάζονται μεταξύ τους για την πραγματοποίηση της κάθε συναλλαγής. Η είσοδος στα quorum slices, αλλά και γενικότερα στο δίκτυο, είναι ελεύθερη, απεριόριστη και δεν απαιτείται έλεγχος (permissionless), γεγονός που επιτρέπει σε έναν κόμβο να ανήκει σε παραπάνω από μία ομάδα ταυτόχρονα. Το σύστημα είναι αποκεντρωμένο λόγω της απουσίας κεντρικού ελέγχου των συναλλαγών και τον ρόλο του επικυρωτή κατέχουν όλοι οι κόμβοι [49]. Η ομοφωνία στο δίκτυο επιτυγχάνεται μέσα από 3 φάσεις:

1. Φάση αρχικής ψηφοφορίας (Initial Voting): Ο κάθε κόμβος καλείται να ψηφίσει μία μόνο φορά οποιαδήποτε αξία επιθυμεί μέσα από ένα σύνολο υποψήφιων (candidate set) και εκείνες που θα συλλέξουν τις περισσότερες ψήφους του quorum slice περνούν στην επόμενη φάση.
2. Φάση αποδοχής (Acceptance): Τα quorum slices των οποίων οι αξίες που ψήφισαν δεν πέρασαν, αποδέχονται τις υπερψηφισμένες αξίες από την πλειοψηφία των quorums. Αυτή η ενέργεια θα περάσει από την έγκριση των V-blocking κόμβων, οι οποίοι είναι ένα σύνολο επιλεγμένων quorum slices από κάθε quorum που έχουν ψηφίσει τις προαγμένες αξίες. Η συγκεκριμένη διαδικασία θα επιτευχθεί με την διασταύρωση των quorum (quorum intersection), κατά την οποία εξασφαλίζεται ότι ανά δύο quorums θα υπάρχει σίγουρα ένας ή περισσότεροι κοινοί κόμβοι, οι οποίοι προφανώς θα πρέπει να έχουν την ίδια απόφαση. Τα quorum slices θα δράσουν έτσι ώστε να συμφωνήσουν όλοι οι κόμβοι σε μία μόνο αξία, δημιουργώντας ένα quorum.



Εικόνα 15 - Δύο Quorums διασταυρώνονται σε ένα

3. Φάση επικύρωσης (Confirmation): Κάθε κόμβος ενημερώνει το υπόλοιπο δίκτυο με την απόφαση του, ώστε να επικυρωθεί πως η τελική απόφαση είναι συλλογική, άρα επιτεύχθηκε ομοφωνία [50].



Εικόνα 16 - Διαδικασία επικύρωσης και επιβεβαίωσης αξίας

Για την αποφυγή μίας κατάστασης όπου οι κόμβοι του δικτύου δεν μπορούν να αποφασίσουν αν μία αξία γίνει δεκτή ή όχι (stuck state), τότε πραγματοποιείται καινούργια ψηφοφορία. Επίσης, για την αποφυγή του stuck state, αλλά και των forks, είναι αναγκαία σε κάθε SCP σύστημα η διαθεσιμότητα των quorums (quorum availability), κατά την οποία πρέπει να υπάρχει τουλάχιστον ένα quorum που δεν θα έχει μη λειτουργικούς ή κακόβουλους κόμβους. Κάθε συναλλαγή στο Stellar πραγματοποιείται ανά 4 περίπου δευτερόλεπτα, ενώ σημειώνονται κατά μέσο όρο 1000 συναλλαγές το δευτερόλεπτο [51].

3.8.3 Ripple Protocol Consensus Algorithm (RPCA)

Το πρωτόκολλο Ripple, μέσω του κρυπτονομίσματος XRP, δρα στο δικό του ανοικτό δίκτυο, το RippleNet, κάνοντας χρήση της πιθανοτικής βυζαντινής ψηφοφορίας (probabilistic byzantine voting) [52]. Το RPCA επικεντρώνεται κυρίως στον οικονομικό τομέα και συγκεκριμένα εστιάζει στην επίτευξη ενός αποκεντρωμένου και αποδοτικού δικτύου όπου οι συναλλαγές ανάμεσα σε πελάτες και "τράπεζα" θα είναι άμεσες. Ο κάθε κόμβος του δικτύου μπορεί να είναι χρήστης (user), επικυρωτής διακομιστή (validating server) ή κατασκευαστής αγοράς (market maker). Ο ρόλος του κόμβου χρήστη είναι η αποδοχή και κατάθεση πληρωμών. Ο επικυρωτής διακομιστή ελέγχει τις συναλλαγές του συστήματος και τις επικυρώνει, μέσω του πρωτοκόλλου RPCA. Ο κατασκευαστής αγοράς είναι βοηθητικός κόμβος για την επίτευξη συναλλαγών όλων των ειδών νομισμάτων. Ο κάθε χρήστης του RippleNet διαθέτει ένα δημόσιο και ένα ιδιωτικό κλειδί για λόγους ασφαλείας κατά τις συναλλαγές, ενώ οι πληρωμές κρυπτογραφούνται με τον αλγόριθμο ECDSA [53]. Η ποσότητα των XRP του δικτύου καταγράφεται στο ανοικτό κατάστιχο (open ledger) ενός χρήστη, στο οποίο όμως δεν μπορούν να καταχωρηθούν ολοκληρωμένες συναλλαγές [54]. Οι επικυρωτές διακομιστή πρέπει να θέσουν μία λίστα με ορισμένους κόμβους που θεωρούν μοναδικούς και αξιόπιστους, την Unique Node List (UNL), και στη συνέχεια πραγματοποιούν πολλούς γύρους ψηφοφορίας ώσπου να επιτύχουν την ομοφωνία μεταξύ των κόμβων [55].

Το RPCA επιτυγχάνει την συγκεκριμένη διαδικασία μέσω τριών σταδίων:

1. Συλλογή (Collection): Αρχικά, οι συναλλαγές εξετάζονται από τους επικυρωτές ως προς την αυθεντικότητα του δημοσίου κλειδιού τους και την οικονομική δυνατότητα του χρήστη να εκπληρώσει το ποσό. Όσες περάσουν τον έλεγχο αποθηκεύονται σε μία δομή δεδομένων συνόλου υποψηφίων (candidate set), πριν δημοσιευθούν στο δίκτυο. Οι χρήστες που ανήκουν στην UNL των επικυρωτών μπορούν να προτείνουν συναλλαγές, οι οποίες στην συνέχεια προστίθενται σε μία λίστα και ψηφίζονται μόνο οι αξιόπιστες.
2. Συναίνεση (Consensus): Στη συνέχεια, οι επικυρωτές εξακολουθούν να λαμβάνουν συναλλαγές, όμως εγκρίνουν μόνο εκείνες που συλλέξανε τουλάχιστον τα 4/5 των ψήφων των κόμβων της UNL και αυτές αποθηκεύονται στο διανεμημένο κατάστιχο του αντίστοιχου κόμβου που τις επικύρωσε.
3. Κλείσιμο κατάστιχου (Ledger closing): Τέλος, οι συναλλαγές που ψηφίστηκαν από την πλειοψηφία και εγκρίθηκαν από τους επικυρωτές συντελούν το τελευταίο κλειστό κατάστιχο, ή αλλιώς Last Closed Ledger (LCL). Το κάθε LCL τίθεται προς εκτέλεση, προσθέτοντας το στην αλυσίδα του Ripple και στη συνέχεια ξεκινάει ένα καινούργιος γύρος ψηφοφορίας [3].

Στο πρωτόκολλο Ripple, η συνεργασία και η εμπιστοσύνη ανάμεσα στου κόμβους δεν είναι εξολοκλήρου απαραίτητη, μιας και οι εργασίες μοιράζονται μέσα στο δίκτυο, ενώ ο κανόνας της συμφωνίας της πλειοψηφίας το καθιστά ανθεκτικό ενάντια βυζαντινών αποτυχιών. Με αυτόν τον τρόπο επιτυγχάνονται υψηλές ταχύτητες πραγματοποίησης συναλλαγών χωρίς καθυστερήσεις (4 δευτερόλεπτα ανά συναλλαγή) και αποδοτικότητα που προς το παρών φθάνει τις 1500 συναλλαγές το δευτερόλεπτο. Παρόλα αυτά, η απόδοση μπορεί να επεκταθεί ακόμα και στις 50.000-65.000 συναλλαγές το δευτερόλεπτο, ανταγωνίζοντας κορυφαία δίκτυα συναλλαγών, όπως η Visa.

3.9 Επιθέσεις και Ασφάλεια στο Blockchain

Η αποτελεσματικότητα, η αποκέντρωση και κυρίως η ασφάλεια είναι τα βασικότερα κριτήρια με τα οποία επιλέγεται ένας μηχανισμός συναίνεσης ώστε να υλοποιηθεί πάνω του μία εφαρμογή. Με την πάροδο του χρόνου, η αύξηση της δημοσιότητας του blockchain έχει κεντρίσει το ενδιαφέρον πολλών κακόβουλων χρηστών, οι οποίοι επιχειρούν με διάφορους τρόπους όλο και πιο εντατικά να παραβιάσουν τα συστήματα, εξελίσσοντας στην πορεία τις τεχνικές τους. Καθήκον του δημιουργού μίας blockchain εφαρμογής είναι να βρει το κατάλληλο πρωτόκολλο που καλύπτει τις ανάγκες των χρηστών της πλατφόρμας του, ενώ παράλληλα θα βρίσκονται σε ένα περιβάλλον προστατευμένο από όσο το δυνατόν περισσότερες πιθανές κακόβουλες επιθέσεις [56].

3.9.1 Long Range

Η επίθεση μεγάλης εμβέλειας συναντάται αποκλειστικά στα PoS και DPoS συστήματα. Ένας κακόβουλος χρήστης που θέλει να επιχειρήσει μία long range επίθεση για να ξεκινήσει με την δημιουργία ενός fork, είτε στο αρχικό block της αλυσίδας (genesis) που θα δημιουργεί, είτε σε ένα από τα πρώτα αν δεν τα καταφέρει. Στόχος αυτού του κόμβου είναι η προσπέραση της κυρίας αλυσίδας από την δικιά του σε μέγεθος και η θεώρηση της πλέον ως την ισχύουσα, χωρίς απαραίτητα να πρέπει να περιέχει ίδια blocks με την πρώτη αλυσίδα. Για να το πέτυχει αυτό πρέπει να καταφέρει να δημιουργήσει στον ίδιο χρόνο περισσότερα blocks, αυξάνοντας τις πιθανότητες επιτυχίας του με μία πιθανή συνεργασία με κάποιον άλλο κόμβο του δικτύου.

Μία ιδιότητα των κόμβων των PoS δικτύων είναι η δυνατότητα απόσυρσης του μεριδίου τους οποιαδήποτε χρονική στιγμή επιθυμεί ο χρήστης. Τα ιδιωτικά δεδομένα (private key) των συμμετέχων κόμβων προστατεύονται από το σύστημα, όμως όταν επιλέξουν να αποχωρήσουν παύει να είναι προτεραιότητα η ασφάλεια τους. Ένας κόμβος όμως που επέλεξε να αποχωρήσει μπορεί ακόμα να επικυρώσει τα blocks που είχε μέχρι την στιγμή της αποχώρησης. Εκεί στοχεύει ένας κακόβουλος χρήστης που θα κάνει long range επίθεση ακολουθώντας δύο προσεγγίσεις:

1. Αγορά των δεδομένων του κόμβου που αποχώρησε,
2. Παράνομη κατάχρηση των κλειδιών του κόμβου που αποχώρησε, μιας και πλέον είναι πιο εύκολο να παραβιάσει την ασφάλεια.

Με αυτές τις τεχνικές ο κόμβος που επιτίθεται θα καταφέρει να προσθέσει στην αλυσίδα του περισσότερα blocks χωρίς να τα παράγει ο ίδιος, αυξάνοντας το μήκος της αλυσίδας του με μεγαλύτερο ρυθμό από αυτό που παράγει η κύρια αλυσίδα [57].

	PoW	**PoS**	**DPoS**	**PoET**	**PBFT**	**SCP**	**RPCA**
Long Range	Ασφαλές	Ευάλωτο	Ευάλωτο	Ασφαλές	Ασφαλές	Ασφαλές	Ασφαλές

Πίνακας 1 - Ασφάλεια μηχανισμών συναίνεσης σε Long range επίθεση

3.9.2 Nothing at Stake

Η nothing at stake επίθεση συναντάται αποκλειστικά στα PoS συστήματα και είναι πιθανό να πραγματοποιηθεί εάν υπάρχει τουλάχιστον ένα fork. Οι κόμβοι του δικτύου είναι απαραίτητο να διαθέτουν μία ψηφιακή υπογραφή, η οποία περιέχει το μερίδιο που έχουν στην διάθεσή τους, ώστε να μπορέσουν να συμμετάσχουν στην διαδικασία δημιουργίας ενός νέου block. Μία τέτοια επίθεση μπορεί να εκτελεστεί με το ποντάρισμα ορισμένων κακόβουλων χρηστών σε παραπάνω από ένα fork, με σκοπό την αύξηση των πιθανοτήτων να επιλεχθούν αυτοί για την δημιουργία του καινούργιου block. Το να χρησιμοποιείς τα κρυπτονομίσματα σου σε πολλαπλές συναλλαγές ταυτόχρονα είναι γνωστό ως διπλή δαπάνη (double spend). Μειονέκτημα του PoS αποτελεί η έλλειψη τιμωρίας αυτών των χρηστών μιας και το μόνο που τους κάνει σε περίπτωση που γίνουν αντιληπτοί είναι απλά να μην τους παρέχει την αμοιβή τους, πράγμα που δεν τους σταματά από το να συνεχίσουν να προσπαθούν να δημιουργήσουν πολλά forks, αφού δεν έχουν κάτι να χάσουν [24].

	PoW	**PoS**	**DPoS**	**PoET**	**PBFT**	**SCP**	**RPCA**
Nothing at Stake	Ασφαλές	Ευάλωτο	Ασφαλές	Ασφαλές	Ασφαλές	Ασφαλές	Ασφαλές

Πίνακας 2 - Ασφάλεια μηχανισμών συναίνεσης σε Nothing at stake επίθεση

3.9.3 51%

Ένας μόνο κόμβος ή μία ομάδα κόμβων μπορεί να πραγματοποιήσει μία 51% επίθεση, ή αλλιώς majority attack, με σκοπό τον έλεγχο της πλειοψηφίας της ισχύος ενός δικτύου [56]. Αυτός ο τύπος επίθεσης αποτελεί τον πιο συνηθισμένο στο blockchain, ενώ δεν είναι καθόλου εύκολο να παρατηρηθεί πριν την ολοκλήρωση της. Η ύπαρξη της σχετίζεται με την P2P δομή της τεχνολογίας blockchain και με τους μηχανισμούς συναίνεσης της [58]. Κατά την ολοκλήρωση μίας 51% επίθεσης, ο επιτιθέμενος δημιουργεί μία δική του αλυσίδα στο δίκτυο, χωρίς να τον καταλάβουν οι υπόλοιποι κόμβοι, στοχεύοντας να την ακολουθήσουν άθελα τους [59]. Στην περίπτωση που η αλυσίδα τους γίνει η μεγαλύτερη στο δίκτυο τότε η επίθεση θεωρείται επιτυχής και ο έλεγχος του δικτύου περνά στα χεριά των κακόβουλων χρηστών. Από εκείνο το σημείο και μετά οι επιτιθέμενοι έχουν την δυνατότητα να επηρεάσουν το δίκτυο όπως επιθυμούν, με σοβαρότερο την υποκλοπή κρυπτονομισμάτων άλλων χρηστών. Επίσης, μπορούν να προωθήσουν και να εγκρίνουν πλαστές συναλλαγές, να διαχωρίσουν το σύστημα με την δημιουργία forks, να μεταβάλλουν την εγκυρότητα των blocks παρεμποδίζοντας την επικύρωση των συναλλαγών τους και να διαταράξουν την αμεταβλητότητα με την αντιστροφή συναλλαγών. Στη συνέχεια, μπορούν να πραγματοποιηθούν επιθέσεις κι άλλων μορφών μιας και το δίκτυο είναι ήδη ευάλωτο [60].

Η πιθανότητα επιτυχίας μίας 51% επίθεσης σε ένα proof-based σύστημα είναι μικρή, αλλά όχι μηδενική, μιας και ο έλεγχος της πλειοψηφίας του δικτύου είναι πιο δύσκολος, ενώ όσο πιο μεγάλο είναι, τόσο η δυσκολία αυξάνεται [61]. Μία επίθεση σε ένα PoW σύστημα θα στοχεύσει την κατακερματιστική ισχύ του δικτύου, ενώ σε ένα PoS την αξία των περιουσιακών στοιχείων των χρηστών. Παρόλα αυτά έχουν πραγματοποιηθεί ελάχιστες επιθέσεις σε τέτοιου είδους συστήματα, ενώ αυτές ήταν σε μικρότερα συστήματα με μικρά ποσοστά κατακερματισμού. Έχουν παρουσιαστεί αρκετές τεχνικές περιορισμού, αποφυγής και αντιμετώπισης μίας 51% επίθεσης, όμως καμία προς το παρών δεν μπορεί να αποτρέψει απόλυτα μία τέτοια επίθεση [62]. Από την άλλη πλευρά, στα BA-based συστήματα η πιθανότητα επιτυχίας αυτού του είδους επιθέσεων είναι σχεδόν μηδενική, λόγω του ότι η ταυτότητα όλων των χρηστών του δίκτυο κατά την επίτευξη της διαδικασίας ομοφωνίας είναι γνωστή και οι κόμβοι έχουν εμπιστοσύνη μεταξύ τους, μιας και οποιαδήποτε κακόβουλη ενέργεια θα γινόταν φανερή [63].

	PoW	**PoS**	**DPoS**	**PoET**	**PBFT**	**SCP**	**RPCA**
51%	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ασφαλές	Ασφαλές	Ασφαλές

Πίνακας 3 - Ασφάλεια μηχανισμών συναίνεσης σε 51% επίθεση

3.9.4 Sybil

Στα P2P δίκτυα ο κάθε κόμβος έχει μία μοναδική ψηφιακή ταυτότητα και υπογραφή [64]. Μία sybil επίθεση στοχεύει στην δημιουργία πολλών διαφορετικών ψεύτικων ψηφιακών ταυτοτήτων και κατεπέκταση υπογράφων. Με αυτόν τον τρόπο, ο κακόβουλος κόμβος θα έχει περισσότερες πιθανότητες να επηρεάσει το δίκτυο προς όφελος του. Μία τέτοιου είδους επίθεση είναι αναπόφευκτη σε όλα τα P2P blockchain δίκτυα, οποιοδήποτε μηχανισμό συναίνεσης και αν χρησιμοποιούν, εξαιτίας της δομής των δικτύων P2P. Πάρα το γεγονός όμως ότι δεν είναι ποτέ δυνατόν οι πιθανότητες μίας sybil επίθεσης να φθάσουν στο μηδέν, υπάρχουν ορισμένοι μηχανισμοί που μειώνουν κατά πολύ το ποσοστό επιτυχίας, όπως το PoW λόγω του μεγάλου κόστους του. Ξεκινώντας με μία sybil attack, ο επιτιθέμενος κόμβος μπορεί να επιχειρήσει στην συνέχεια και άλλες επιθέσεις, όπως τις double spending και distributed denial of service που θα αναφερθούν στη συνέχεια [65].

	PoW	**PoS**	**DPoS**	**PoET**	**PBFT**	**SCP**	**RPCA**
Sybil	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο

Πίνακας 4 - Ασφάλεια μηχανισμών συναίνεσης σε Sybil επίθεση

3.9.5 Double-Spending

Οι double-spending επιθέσεις αφορούν κυρίως κρυπτονομίσματα μιας και ο σκοπός του επιτιθέμενου είναι η χρήση του ίδιου μεριδίου του για παραπάνω από μία συναλλαγές [66]. Ο κακόβουλος χρήστης ξεκινά μία συναλλαγή με έναν άλλο χρήστη του δικτύου, όμως για όσο χρόνο η πρόταση του πρώτου μένει σε ένα block ώσπου να ολοκληρωθεί, εκείνος επιχειρεί να πραγματοποιήσει όσες περισσότερες συναλλαγές καταφέρει με το ίδιο μερίδιο μέσα σε αυτό το χρονικό διάστημα [67]. Τα PoW και PoET συστήματα είναι περισσότερο ευάλωτα σε τέτοιου είδους επιθέσεις μιας και οι χρονικές καθυστερήσεις κατά την οριστικότητα των blocks είναι αισθητή, ενώ στα PoS συστήματα ο κίνδυνος είναι μικρότερος [59]. Τα BA συστήματα είναι ανθεκτικά σε τέτοιες επιθέσεις λόγω της απολυτής οριστικότητας τους, όπως και στα DPoS που εξαιτίας της συνεχής ανίχνευσης για πιθανές απώλειες η πιθανότητα κίνδυνου είναι ελάχιστη [68]. Ωστόσο, μία double-spending επίθεση μπορεί να εκτελεστεί συνδυαστικά με άλλες επιθέσεις, όπως η eclipse, η BGP, η sybil και η 51% [58].

	PoW	**PoS**	**DPoS**	**PoET**	**PBFT**	**SCP**	**RPCA**
Double-Spending	Ευάλωτο	Ευάλωτο	Ασφαλές	Ευάλωτο	Ασφαλές	Ασφαλές	Ασφαλές

Πίνακας 5 - Ασφάλεια μηχανισμών συναίνεσης σε Double-spending επίθεση

3.9.6 Eclipse

Μία Eclipse επίθεση μπορεί να πραγματοποιηθεί από έναν ή περισσοτέρους χρήστες ταυτόχρονα σε ένα σύστημα δημοσίου δικτύου, όπου δεν ελέγχονται ούτε περιορίζονται οι ταυτότητες των χρηστών του [69]. Ο επιτιθέμενος έχει ως σκοπό την απομόνωση ενός συγκεκριμένου κόμβου καθιστώντας αδύνατη την πραγματοποίηση συναλλαγών με τους πλησίον κόμβους του. Για να πέτυχει τον στόχο του δεσμεύει τις διευθύνσεις Internet Protocol (IP) των κόμβων του δικτύου, ενώ παράλληλα βοηθά στην επίτευξη κι άλλων επιθέσεων (double-spending, 51%). Το δίκτυο του Ripple αποτελεί εξαίρεση στον κανόνα μιας και ενώ είναι δημόσιο, παρουσιάζει ορισμένους περιορισμούς στην συμμετοχή που το καθιστούν ασφαλές έναντι μίας τέτοιας επίθεσης. Τα πρωτόκολλα που λειτουργούν σε ιδιωτικό ή κοινοπρακτικό δίκτυο θεωρούνται ασφαλή, καθώς και όσα είναι δυνατόν να εφαρμοστούν και σε δημόσιο και σε ιδιωτικό αλλά και σε κοινοπρακτικό δίκτυο [70].

	PoW	**PoS**	**DPoS**	**PoET**	**PBFT**	**SCP**	**RPCA**
Eclipse	Ευάλωτο	Ασφαλές	Ασφαλές	Ασφαλές	Ασφαλές	Ευάλωτο	Ασφαλές

Πίνακας 6 - Ασφάλεια μηχανισμών συναίνεσης σε Eclipse επίθεση

3.9.7 Distributed Denial of Service (DDoS)

Οι DDoS επιθέσεις αποτελούν μία συνηθισμένη μορφή κακόβουλης ενέργειας, ενώ υπήρχαν από πριν την δημιουργία του blockchain, προσβάλλοντας τόσο διαδικτυακές πλατφόρμες όσο και εφαρμογές [68]. Ένας κακόβουλος χρήστης που θα επιχειρήσει μία τέτοιου είδους επίθεση αρχικά θα προσπαθήσει να πάρει υπο τον έλεγχο του διάφορα υπολογιστικά συστήματα που συνδέονται με τον στόχο του, παρεμβάλλοντας την λειτουργία του [71]. Για την επίτευξη του στόχου του θα μολύνει αυτά τα συστήματα με ένα λογισμικό ώστε να μπορεί να τα ελέγξει (botnet) και στη συνέχεια μέσω αυτών θα ξεκινήσει να στέλνει επανειλημμένα πολλαπλά αιτήματα στον στόχο του [59]. Με αυτόν τον τρόπο, το σύστημα θα γεμίσει από αιτήματα με συνέπεια να αρνείται στο εξής την περαιτέρω εξυπηρέτηση άλλων αιτημάτων και να σταματήσει να ανταποκρίνεται [72]. Οι DDoS επιθέσεις δεν είναι εύκολο να είναι επιτυχημένες στις blockchain εφαρμογές, αφού είναι αποκεντρωμένες και διανεμημένες, όμως αυτό δεν σημαίνει ότι οι πιθανότητες είναι μηδενικές, μιας και στο παρελθόν τέτοιες επιθέσεις έχουν προκαλέσει σοβαρά προβλήματα στο BTC και στο ETH [58]. Οι πιθανότητες ολοκλήρωσης μίας τέτοιας επίθεσης στα δημόσια proof-based συστήματα είναι πολύ μικρότερες σε σχέση με τα ιδιωτικά, κοινοπρακτικά και BA [73]. Τα κρυπτονομίσματα αποτελούν τον πιο πιθανό στόχο στο blockchain και συγκεκριμένα τα ηλεκτρονικά πορτοφόλια και οι συναλλαγές [74]. Ένας ακόμη πολύ συχνός στόχος των επιτιθέμενων είναι τα mining pools, καθώς και τα memory pools (mempools), ώστε να αυξήσουν τα τέλη εξόρυξης. Επίσης, ένας κακόβουλος χρήστης μπορεί να επιχειρήσει μία DDoS επίθεση από μόνη της, είτε έπειτα από μία άλλη μορφή επίθεσης [75]. Ακόμη δεν υπάρχουν κατάλληλα μέτρα προστασίας ώστε οι πιθανότητες επιτυχίας μίας τέτοιας επίθεσης να πέσουν στο μηδέν, όμως είναι απαραίτητο να δημιουργηθούν μιας και μπορούν να προκληθούν σοβαρές συνέπειες [76].

	PoW	PoS	DPoS	PoET	PBFT	SCP	RPCA
DDoS	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο	Ευάλωτο

Πίνακας 7 - Ασφάλεια μηχανισμών συναίνεσης σε Distributed Denial of Service επίθεση

3.9.8 Border Gateway Protocol (BGP)

Στα blockchain συστήματα τα οποία αλληλοεπιδρούν με το διαδίκτυο είναι πιθανό να πραγματοποιηθεί μία BGP επίθεση (αλλιώς Routing Attack) [58]. Αυτό οφείλεται στην χωρική συγκέντρωση των κόμβων στους Internet Service Providers (ISPs) και Autonomous Systems (ASes), οι οποίοι είναι υπεύθυνοι για την διαδικτυακή ροή και δρομολόγηση της κυκλοφορίας στο σύστημα. Μία επιτυχημένη BGP επίθεση δίνει στον κακόβουλο χρήστη τον έλεγχο του 51% του δικτύου, ενώ παράλληλα προκαλούνται χρονικές καθυστερήσεις στην παραγωγή των blocks, το οποίο κάνει τους χρήστες πιο ευάλωτους σε double-spending επιθέσεις και τους miners να χάνουν την υπολογιστική τους ισχύ [77]. Συστήματα στα οποία είναι πιθανή μία τέτοια επίθεση λόγω της πραγματοποίησης διάφορων διαδικασιών τους μέσω διαδικτύου είναι όλα όσα είναι βασισμένα στον μηχανισμό συναίνεσης PoW και στο πρωτόκολλο BA [78].

	PoW	PoS	DPoS	PoET	PBFT	SCP	RPCA
BGP	Ευάλωτο	Ασφαλές	Ασφαλές	Ασφαλές	Ευάλωτο	Ευάλωτο	Ευάλωτο

Πίνακας 8 - Ασφάλεια μηχανισμών συναίνεσης σε Border Gateway Protocol επίθεση

3.10 Blockchain Συστήματα

Όταν αναφερόμαστε στην τεχνολογία blockchain δεν γίνεται κατεπέκταση να μην αναφερθούμε στα διανεμημένα και αποκεντρωμένα συστήματα διαχείρισης δεδομένων που αποτελούν τον κορμό του. Αρχικά ξεκίνησε από το BTC με τα δημόσια συστήματα, όμως με την πάροδο του χρόνου η τεχνολογία εξελίχτηκε, η ζήτηση τέτοιων εφαρμογών αυξήθηκε και έχουμε φτάσει σε ένα επίπεδο όπου πολλά από τα καινούργια συστήματα να μην ακολουθούν αρκετά από τα πρότυπα των πρώτων συστημάτων [79].

Πλέον έχουμε καταλήξει να τα κατηγοριοποιούμε σε 3 τύπους:

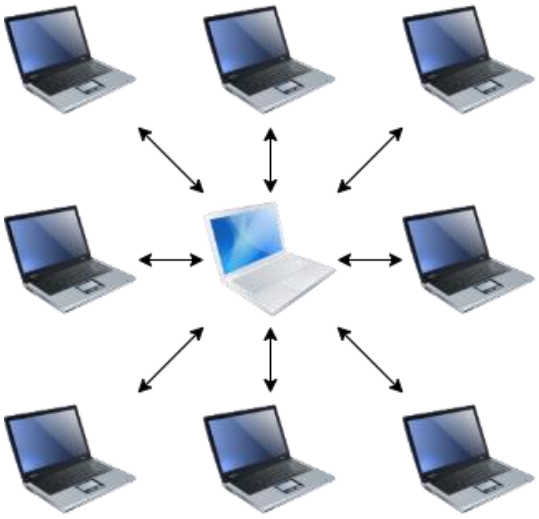
1. τα δημόσια (public),
2. τα ιδιωτικά (private) και
3. τα κοινοπρακτικά (consortium) [1].

Αυτός ο διαχωρισμός πραγματοποιήθηκε για την αποτελεσματικότερη διαχείριση τους ως προς τις ανάγκες της κάθε εφαρμογής, με βάση [80]:

1. την πρόσβαση στα δεδομένα του συστήματος,
2. την συμμετοχή στην διαδικασία ομοφωνίας και
3. την εξασφάλιση της συνέχειας και της ασφάλειας του συστήματος [81].

3.10.1 Δημόσια

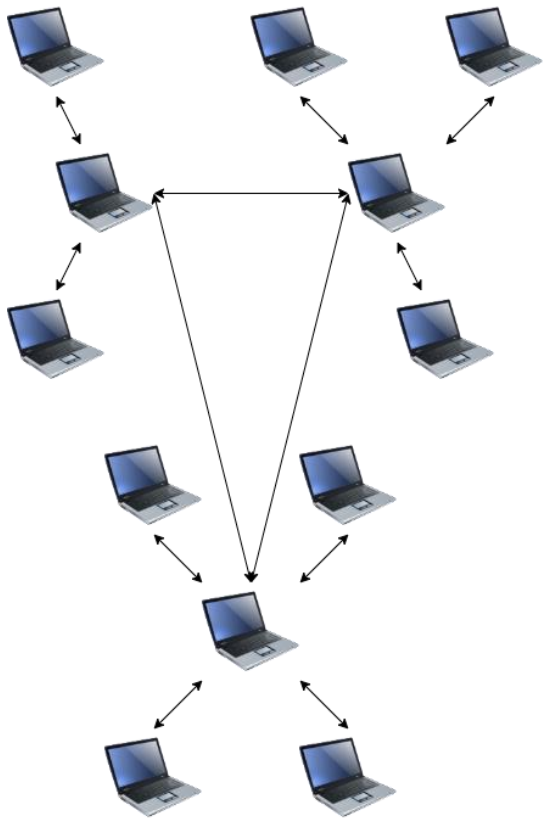
Τα δημόσια Blockchain συστήματα έχουν ως κύριο χαρακτηριστικό την ελεύθερη πρόσβαση στα δεδομένα σε όποιον επιθυμεί να γίνει μέλος του [82]. Αναλυτικά, όποιος έχει την δυνατότητα να γίνει χρήστης ή πιο συγκεκριμένα να συμμετέχει στην παραγωγή blocks, στην ολοκλήρωση συναλλαγών και στην επίτευξη ομοφωνίας με το κατάλληλο λογισμικό, ώστε να εξυπηρετήσει το σύστημα. Δεν χρειάζεται κάποια έγκριση για να συμμετάσχεις στο σύστημα, ούτε περνάς από κάποιον έλεγχο από έναν υπεύθυνο. Συμπεριλαμβανομένων όλων αυτών των χαρακτηριστικών καταλήγουμε στο γεγονός ότι είναι εξολοκλήρου αποκεντρωμένα, ενώ παράλληλα διατηρείται η ανωνυμία και η διασφάλιση του απορρήτου όλων των χρηστών. Αυτό επιτυγχάνεται μέσω της ψευδωνυμίας, όπου ο κάθε χρήστης έχει μία μοναδική και τυχαία ταυτότητα με την οποία φαίνεται στο δίκτυο. Η ομαλότητα και η λειτουργικότητα του συστήματος επιτυγχάνεται μέσα από τον ενεργό ρόλο των χρηστών, για αυτό και τα συγκεκριμένα συστήματα παρέχουν υψηλά επίπεδα ασφάλειας. Πέρα από όλα τα πλεονεκτήματα όμως που αναφέρθηκαν, τα δημόσια συστήματα έχουν μερικά μειονεκτήματα ώστε να καταφέρουν να τα επιτύχουν. Αυτά είναι, η υψηλή σπατάλη ενέργειας και τα έξοδα για εξοπλισμό, που συντελούν στην μεγάλη χρηματική δαπάνη, καθώς και οι χαμηλές ταχύτητες λειτουργίας σε σχέση με τα άλλα blockchain συστήματα. Ωστόσο το μεγαλύτερο ποσοστό τα επιλέγει και κυρίως κρατικοί οργανισμοί και τράπεζες, ενώ είναι και χρονικά τα πρώτα συστήματα, στηριζόμενα στους αρχικούς αλγορίθμους PoW (Υποκεφάλαιο 3.1) και PoS, με βασικότερα παραδείγματα το BTC και το ETH αντίστοιχα [81].



Εικόνα 17 - Δημόσιο blockchain σύστημα

3.10.2 Ιδιωτικά

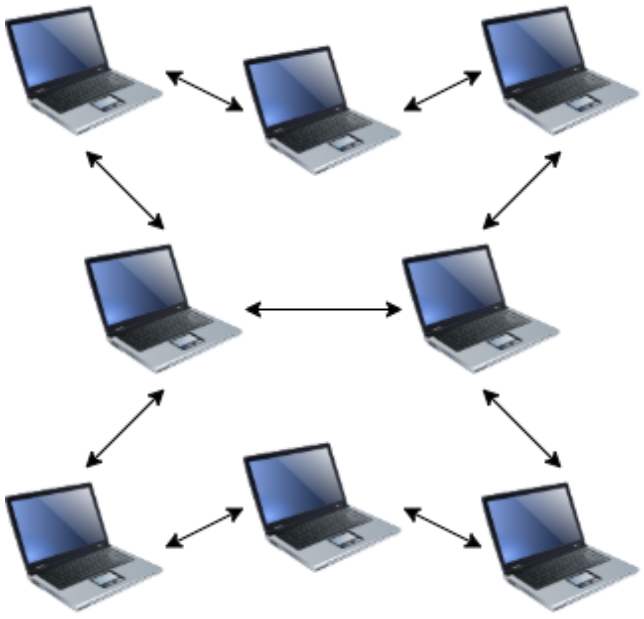
Τα ιδιωτικά blockchain συστήματα διαφέρουν από τα δημόσια ως προς την έγκριση που απαιτείται από έναν διαχειριστή (admin) κατά την είσοδο ενός χρήστη, η οποία μπορεί να είναι σαν μία ιδιωτική πρόσκληση, όπου οι συναλλαγές του χρήστη πραγματοποιούνται σε ένα περιορισμένο περιβάλλον [46]. Ο διαχειριστής, ένας οργανισμός ή μία τράπεζα, καθορίζει την πρόσβαση για ανάγνωση δεδομένων και στη μεταβολή τους, όπως δημιουργία καινούργιων blocks για συναλλαγές, από συγκεκριμένους χρήστες. Η πρώτη διαδικασία, που λέγεται και πρόσβαση ανάγνωσης (read access), έχει την δυνατότητα να είναι και δημόσια, ενώ η δεύτερη, που λέγεται και πρόσβαση εγγραφής (write access), εξαρτάται από τον διαχειριστή. Τα ιδιωτικά συστήματα χαρακτηρίζονται από την μεταβλητότητα και αναστρεψιμότητας τους, διότι ο καθορισμός ομοφωνίας ελέγχεται αποκλειστικά από τον διαχειριστή, ο οποίος μπορεί να παρέμβει τροποποιώντας τον. Σημαντικό πλεονέκτημα, σε αντίθεση με τα δημόσια συστήματα, αποτελεί επίσης η μεγαλύτερη αποδοτικότητα τους λόγω της φθηνότερης και ταχύτερης ολοκλήρωσης των συναλλαγών. Ωστόσο, η ταυτότητα του χρήστη δεν είναι κρυφή, όπως στα δημόσια, όμως υπάρχει εμπιστοσύνη μεταξύ διαχειριστή και χρήστη ως προς την ανωνυμία του, το οποίο τα κάνει να θεωρούνται κεντρωποιημένα [83]. Ο πιο γνωστός αλγόριθμος συναίνεσης βασισμένος σε ιδιωτικό σύστημα είναι ο PBFT και οι πιο γνωστές εφαρμογές το Blockstack, το Hyperledger Fabric, το Ziliqa και το Quorum [84].



Εικόνα 18 - Ιδιωτικό blockchain σύστημα

3.10.3 Κοινοπρακτικά

Τα κοινοπρακτικά Blockchain συστήματα αποτελούν έναν συνδυασμό των δημοσίων και ιδιωτικών συστημάτων, με μία τάση περισσότερο προς τα ιδιωτικά [85]. Αυτό οφείλεται στο ότι μία προκαθορισμένη και διανεμημένη ομάδα χρηστών είναι υπεύθυνη για τη διαδικασία της ομοφωνίας και η πρόσβαση είναι ελεύθερη, αλλά η εγγραφή είναι περιορισμένη σε συγκεκριμένους χρήστες. Το μέγεθος αυτών των δικτύων είναι μικρότερο σε σχέση με τα δύο προηγούμενα λόγω του περιορισμένου αριθμού χρηστών που επιβάλλουν. Τα συγκεκριμένα συστήματα θεωρούνται μεταβλητά λόγω της δυνατότητας αντιστρεπτότητας, διότι μπορούν να πραγματοποιηθούν αλλαγές, αλλά μόνο έπειτα από συμφωνία του μεγαλύτερου ποσοστού των χρηστών. Ένας ακόμη λόγος που θεωρούνται υβρίδιο των προηγούμενων συστημάτων είναι η διατήρηση ορισμένων πλεονεκτημάτων του κάθε συστήματος, όπως την ασφάλεια των δημοσίων συστημάτων και την ταχύτητα και αποδοτικότητα των ιδιωτικών συστημάτων, με το οποίο επιτυγχάνεται οργανωτική συνεργασία μεταξύ διάφορων επιμέρους οργανισμών. Παρόλα αυτά, ενώ υιοθετεί κάποια στοιχεία των δημοσίων συστημάτων, παραμένει πιο κοντά στα ιδιωτικά λόγω των αρκετών τεχνικών ομοιοτήτων που κατέχουν [86]. Ωστόσο ο κύριος λόγος διαχωρισμού τους είναι σε διοικητικό και αρχιτεκτονικό επίπεδο, το οποίο βοηθάει στην αξιοποίηση και των δύο συστημάτων [52]. Δημοφιλέστερη εφαρμογή κοινοπρακτικού συστήματος αποτελεί το Ripple με την χρήση του αλγορίθμου συναίνεσης RPCA και το Cobra [87].



Εικόνα 19 - Κοινοπρακτικό blockchain σύστημα

3.11 Χαρακτηριστικά Blockchain

Στα διανεμημένα συστήματα έχει θεσπισθεί ένα θεώρημα, το λεγόμενο θεώρημα CAP, του οποίου τα αρχικά προέρχονται από το Consistency (Συνεκτικότητα) – Availability (Διαθεσιμότητα) - Portion tolerance (Ανοχή διαχωρισμού) [88]. Τα αρχικά του υποδηλώνουν 3 ιδιότητες και σύμφωνα με αυτό το θεώρημα δεν μπορούν να παρέχονται πάνω από 2 τη φορά σε ένα τέτοιο σύστημα [89]. Συνεκτικότητα σημαίνει ότι όλοι οι χρήστες του διανεμημένου συστήματος κατέχουν τα πιο πρόσφατα εγγεγραμμένα δεδομένα. Διαθεσιμότητα σημαίνει ότι όλοι οι χρήστες θα είναι συνέχεια διαθέσιμοι για ανταλλαγή πληροφοριών, δίχως αστοχίες κατά την αποστολή και λήψη δεδομένων. Ανοχή διαχωρισμού σημαίνει ότι στην περίπτωση που αποτύχει ή αποσυνδεθεί ένα σύνολο κόμβων από το δίκτυο τότε το σύστημα θα διασφαλίσει την ορθή λειτουργία του [90]. Επίσης, τα συστήματα blockchain μπορούν να λάβουν πάλι το πολύ μόνο 2 από τις 3 παρακάτω ιδιότητες τη φορά: την αποκέντρωση (decentralization), την συνεκτικότητα (consistency) και την επεκτασιμότητα (scalability) [91]. Οι συγκεκριμένες δύο περιπτώσεις σε συνδυασμό με μερικές ακόμα, όπως η επεκτασιμότητα, οι χρονικές καθυστερήσεις και εύρος και μέγεθος των blocks, αποτελούν προβλήματα του blockchain τα οποία προσπαθούν να λυθούν. Σε αντίθεση με άλλα εμπόδια του παρελθόντος, όπως η σπατάλη πόρων, η ιδιωτικότητα, η ασφάλεια, που έχουν πλέον κατά ένα μεγάλο ποσοστό αντιμετωπιστεί [2].

3.11.1 Εμπιστοσύνη

Γνωρίζουμε ήδη ότι στα δημόσια Blockchain συστήματα η πρόσβαση είναι ελεύθερη και στην συνέχεια όταν ο χρήστης εισέλθει και γίνει μέλος του δικτύου τίθεται να δημιουργήσει block συναλλαγών, εάν μπορεί να παρέχει μία ορισμένη υπολογιστική ισχύ, συμμετέχοντας έτσι στην διαδικασία του ανταγωνισμού, διατηρώντας την σωστή λειτουργία του δικτύου. Σύμφωνα με τα προηγούμενα προκύπτει ότι ανάμεσα στους κόμβους του δικτύου δεν υπάρχει εμπιστοσύνη ούτε και συνεργασία μεταξύ τους λόγω της ανεξαρτησίας τους.

Αντιθέτως, στα ιδιωτικά Blockchain συστήματα υπάρχει εμπιστοσύνη ανάμεσα στους κόμβους οι οποίοι και συνεργάζονται μεταξύ τους για την ομαλή λειτουργία του δικτύου ώστε να διατηρείται παράλληλα και η ιδιωτικότητα τους.

Τα κοινοπρακτικά δίκτυα όμως κάνουν κάτι ενδιάμεσο καθώς ενώ υπάρχει εμπιστοσύνη ανάμεσα στους κόμβους διατηρείται παρόλα αυτά η ανεξαρτησία τους, πραγματοποιώντας ο καθένας τις δίκες του υποχρεώσεις υπακούοντας συγκεκριμένους κανόνες.

	Δημόσια	**Ιδιωτικά**	**Κοινοπρακτικά**
Εμπιστοσύνη	Δεν απαιτείται	Απαιτείται ανάμεσα σε υπεύθυνο και μέλη	Απαιτείται κατά την επιλογή υπευθύνων χρηστών

Πίνακας 9 - Σύγκριση επιπέδου εμπιστοσύνης στα blockchain συστήματα

3.11.2 Ομοφωνία

Η πλειοψηφία των δημοσίων Blockchain συστημάτων χρησιμοποιεί τον μηχανισμό συναίνεσης PoW, όμως εξαιτίας της υψηλής κατανάλωσής ενέργειας έχουν στραφεί και προς άλλους μηχανισμούς, όπως τον PoS με πιο γνωστή εφαρμογή του το κρυπτονόμισμα ETH [92].

Στην περίπτωση των ιδιωτικών συστημάτων αποφεύγεται η χρήση αλγορίθμου PoW λόγω των κινδύνων που ενδέχεται να προκύψουν εξαιτίας κάποιας πιθανής ανωμαλίας (blockchain anomaly) κατά τον τερματισμό της διαδικασίας της ομοφωνίας [93]. Επίσης, για την αποφυγή της ενεργειακής σπατάλης γίνεται χρήση του μηχανισμού PoA σε ορισμένες εφαρμογές, καθώς συχνά χρησιμοποιούνται και οι PoS, PBFT και Raft που πλησιάζουν στην νοοτροπία που πρεσβεύουν τα ιδιωτικά συστήματα [46]. Τέλος, στα κοινοπρακτικά συστήματα εκτελείται μία διαδικασία ψηφοφορίας ανάμεσα στους χρήστες του δικτύου, όπως συμβαίνει στα PBFT και UNL [43].

	Δημόσια	**Ιδιωτικά**	**Κοινοπρακτικά**
Μηχανισμός Ομοφωνίας	PoW PoS	PoS PoA PoT PBFT	Πρωτόκολλα Ψηφοφορίας, RPCA

Πίνακας 10 - Μηχανισμοί ομοφωνίας στα blockchain συστήματα

3.11.3 Ταχύτητα συναλλαγών και έξοδα

Στα δημόσια Blockchain συστήματα κατά την ολοκλήρωση μίας συναλλαγής μεταξύ δύο χρηστών είναι απαραίτητη η επικύρωση της εγκυρότητας της ώστε στη συνέχεια να γίνει μέρος της αλυσίδας μέσα σε ένα block της. Η διαδικασία αυτή πραγματοποιείται μέσω μίας δυνατότητας του P2P συστήματος κατά την οποία η συναλλαγή χρειάζεται να γίνει αποδεκτή από όλους τους κόμβους του δικτύου. Η συγκεκριμένη όμως διαδικασία είναι χρονοβόρα και δαπανηρή, μιας και ο αριθμός των κόμβων είναι μεγάλος το οποίο συνεπάγει και υψηλές χρονικές καθυστερήσεις κατά την επιβεβαίωση.

Στα ιδιωτικά και στα κοινοπρακτικά Blockchain συστήματα ένας καθορισμένος αριθμός εξουσιοδοτημένων ατόμων είναι υπεύθυνος για την επικύρωση της κάθε συναλλαγής. Αποτέλεσμα του οποίου είναι η μείωση των εξόδων συναλλαγών και η ταχύτερη εκτέλεση των διαδικασιών το οποίο συνεπάγει και στην μείωση των χρονικών καθυστερήσεων αναμονής.

	Δημόσια	**Ιδιωτικά**	**Κοινοπρακτικά**
Κόστος συναλλαγών	Μεγάλο	Μικρό	Περιορισμένο
Ταχύτητα συναλλαγών	Μικρή	Μεγάλη	Μέτρια

Πίνακας 11 - Σύγκριση κόστους και ταχύτητας των blockchain συστημάτων

3.11.4 Ανωνυμία

Τα συστήματα Blockchain τεχνολογίας χωρίζονται σε δύο περιπτώσεις ως προς το πόσο απόρρητα είναι τα στοιχεία του κάθε χρήστη. Η πρώτη περίπτωση είναι αυτή που ισχύει στα δημόσια συστήματα όπου η είσοδος είναι ελεύθερη προς όλους όσους επιθυμούν να συμμετάσχουν χωρίς την ζήτηση προσωπικών στοιχείων. Η δεύτερη περίπτωση είναι αυτή που ισχύει στα κοινοπρακτικά και ιδιωτικά συστήματα όπου κατά την είσοδο απαιτείται η υποβολή προσωπικών στοιχείων ως προς την ταυτότητα του χρήστη, όμως τα συγκεκριμένα στοιχεία είναι δυνατόν να μπορούν να αναγνωστούν από επιλεγμένα άτομα ώστε να διατηρείται έτσι η ιδιωτικότητα των μελών.

	Δημόσια	**Ιδιωτικά**	**Κοινοπρακτικά**
Απόρρητο	Ελεύθερη είσοδος νέων μελών, Ελεύθερη ανάγνωση δεδομένων, Ελεύθερη εγγραφή δεδομένων, Καθορισμός ομοφωνίας και πραγματοποίηση συναλλαγών από τους ενεργούς χρήστες.	Είσοδος νέων μελών έπειτα από έγκριση, Ελεύθερη ή περιορισμένη ανάγνωση δεδομένων από χρήστες, Εγγραφή δεδομένων μόνο από τον υπεύθυνο, Καθορισμός ομοφωνίας και πραγματοποίηση συναλλαγών μόνο από τον υπεύθυνο.	Περιορισμένη είσοδος νέων μελών, Ελεύθερη ή περιορισμένη ανάγνωση δεδομένων από χρήστες, Εγγραφή δεδομένων μόνο από επιλεγμένους χρήστες, Καθορισμός ομοφωνίας και πραγματοποίηση συναλλαγών μόνο από επιλεγμένους χρήστες.

Πίνακας 12 - Σύγκριση απορρήτου στα blockchain συστήματα

3.11.5 Ασφάλεια

Τα επίπεδά ασφαλείας στα Blockchain συστήματα εξαρτώνται από τους κανονισμούς της διαδικασίας επίτευξης ομοφωνίας ανάμεσα στους κόμβους του δικτύου. Τα δημόσια συστήματα προσφέρουν ασφάλεια κυρίως μέσω της κρυπτογράφησης που καθιστά σχεδόν αδύνατη την αποκρυπτογράφηση των συναλλαγών και των χρηστών. Η κρυπτογράφηση που χρησιμοποιείται είναι ασύμμετρη και διατηρεί τα προσωπικά στοιχεία των χρηστών ιδιωτικά. Ακόμη όμως και αν κάποιος θέληση να επιχειρήσει την αποκρυπτογράφηση αυτών των δεδομένων για κακόβουλο σκοπό, θα χρειαστεί μεγάλη υπολογιστική ισχύ και ενέργεια για να το καταφέρει, κάνοντας το έργο του πιθανόν μη κερδοφόρο. Επιπλέον, τα δημόσια συστήματα δεν έχουν ανταγωνισμό σε σχέση με τα υπόλοιπα συστήματα στην περίπτωση του μοναδικού σημείου αποτυχίας (single point of failure) ή του κεντρικού σημείου αποτυχίας (central point of failure) μιας και δεν αποτελούν κίνδυνο για τα συγκεκριμένα.

Από την άλλη πλευρά, τα ιδιωτικά και κοινοπρακτικά συστήματα παρέχουν υψηλή ασφάλεια, η οποία όμως δεν είναι απόλυτα αδιαπέραστη εξαιτίας της στήριξης της στην σωστή συμπεριφορά και ειλικρίνεια των χρηστών. Επίσης, υπάρχει πιθανότητα να υπάρξουν καθυστερήσεις στο σύστημα, δυσκολίες κατά την ολοκλήρωση των συναλλαγών και επιπλοκές στην βεβαίωση της ταυτότητας του κάθε χρήστη, εξαιτίας κάποιας αποτυχίας της κεντρικής εξουσίας που είναι υπεύθυνη για όλο το δίκτυο. Παρόλα αυτά, στα κοινοπρακτικά συστήματα αυτή η πιθανότητα είναι μικρότερη σε σχέση με τα ιδιωτικά μιας και η εξουσία δεν ανήκει σε μία οντότητα αλλά σε περισσότερες μέσα στο δίκτυο και η αναπαραγωγή των δεδομένων γίνεται στους επιλεγμένους χρήστες και όχι ταυτόχρονα σε όλους [94].

	Δημόσια	**Ιδιωτικά**	**Κοινοπρακτικά**
Ασφάλεια	Κρυπτογράφηση	Ευπρέπεια χρηστών, Single Point of Failure	Μικρότερη αναπαραγωγή δεδομένων στο δίκτυο

Πίνακας 13 - Σύγκριση βαθμού ασφαλείας στα blockchain συστήματα

3.12 Σύγκριση Μηχανισμών Συναίνεσης

Γνωρίζοντας πλέον αρκετές δομικές και λειτουργικές λεπτομέρειες για διάφορους μηχανισμούς συναίνεσης του blockchain, θα προσπαθήσουμε πλέον να τους συγκρίνουμε μεταξύ τους σε διάφορους τομείς, συμπυκνώνοντας έτσι τα σημαντικότερα χαρακτηριστικά τους. Σε κάθε στάδιο θα χρησιμοποιηθούν οι βασικότεροι μηχανισμοί για τους οποίους έχουμε επαρκή και αξιολογημένα δεδομένα, μιας και ορισμένοι δεν είναι τόσο διαδεδομένοι και δεν χρησιμοποιούνται πρακτικά σε πραγματικές συνθήκες, για αυτό και δεν μπορούμε να αρκεστούμε μόνο στα θεωρητικά στοιχεία τους.

3.12.1 Οριστικότητα

Με τον όρο οριστικότητα αναφερόμαστε στην διαβεβαίωση από το σύστημα ότι από την στιγμή που ένα block προστεθεί στην αλυσίδα, αυτό δεν μπορεί ακυρωθεί. Ένας χρήστης θα προτιμήσει την εφαρμογή που θα του εξασφαλίσει με μεγαλύτερη βεβαιότητα ότι τα χρήματα του δεν θα χαθούν εξαιτίας κάποιας μεταβολής σε μία συναλλαγή του. Η έλλειψη οριστικότητας μπορεί να οδηγήσει μία συναλλαγή να καταλήξει σε ένα orphan block, για το οποίο αναφέρθηκα στην ενότητα του PoW (3.1.4). Η οριστικότητα, αναλόγως το σύστημα, χωρίζεται σε δύο κατηγορίες:

- Πιθανοτική (Probabilistic): Ένα block που περιέχει μία συναλλαγή για εκτέλεση και βρίσκεται πιο "μέσα" στην αλυσίδα είναι πιο πιθανό να επιλεγεί για ολοκλήρωση από τους κόμβους, σε σχέση με ένα άλλο block που βρίσκεται πιο "επιφανειακά" (Κανόνας μακρύτερης αλυσίδας). Σημαντικός παράγοντας αυτής της επιλογής είναι η καθυστέρηση (latency), η οποία είναι ο χρόνος που χρειάζεται μία συναλλαγή για να οριστικοποιηθεί. Ο χρόνος καθυστέρησης προκύπτει από τον χρόνο δημιουργίας κάθε block επί τον χρόνο εκτέλεσης ενός αριθμού επιβεβαιώσεων, όπου όσο μεγαλύτερος είναι, τόσο μικρότερη είναι η πιθανότητα ολοκλήρωσης της συναλλαγής. Μεγαλύτερες καθυστερήσεις παρατηρούνται κυρίως στα proof-based συστήματα για την αποφυγή της μεταβολής κάποιας συναλλαγής.

- Καθοριστική (Absolute): Κάθε συναλλαγή περνάει από μία διαδικασία ψηφοφορίας μεταξύ μίας ομάδας έμπιστων κόμβων, όπου αν την εγκρίνουν τότε περνάει στο block άμεσα και οριστικοποιείται. Τα BA συστήματα βασίζονται κυρίως σε αυτόν τον τύπο οριστικοποίησης χωρίς την ύπαρξη καθυστερήσεων [95].

Σύστημα Blockchain	**Bitcoin**	**Ethereum**	**Cardano**	**EOS.IO**	**NEM**	**Hyperledger Fabric**	**Stellar**	**Ripple**
Μηχανισμός Συναίνεσης	PoW	PoW	PoS	DPoS	PoI	PBFT	SCP	RPCA
Αριθμός Επιβεβαιώσεων	6	10-30	15	1	0	1	1	1
Χρόνος επόμενου block (λεπτά)	10	0.12	0.4	0.03	1	< 1	<0.05	0.04
Συνολικός Χρόνος Επιβεβαίωσης (λεπτά)	60	2-6	10	1	1	< 1	<0.05	0.04

Πίνακας 14 - Σύγκριση οριστικότητας των δημοφιλέστερων εφαρμογών μηχανισμών συναίνεσης

3.12.2 Εμπιστοσύνη κόμβων

Η εμπιστοσύνη μεταξύ των κόμβων σε ορισμένα συστήματα δεν χρειάζεται να υπάρχει, ενώ σε αλλά χρήζει απαραίτητη, με τον βαθμό της να διαφέρει ανά σύστημα [51]. Συγκεκριμένα, μηχανισμοί όπου η εμπιστοσύνη δεν είναι απαραίτητη ή είναι πολύ απαραίτητα τυπική:

- PoW: Επίτευξη ομοφωνίας μέσω ανώνυμης συνεργασίας μεταξύ των κόμβων του δικτύου.
- PoS: Ανάλογη του μεριδίου του κάθε κόμβου.
- DPoS: Περιορισμένη στο δίκτυο.
- LPoS: Τυπική μεταξύ του δανειζόμενου κόμβου και του δανειστή.
- PoET: Αποκλειστικά στην υπολογιστική ισχύ του κάθε κόμβου.

Μηχανισμοί όμως που η εμπιστοσύνη υπάρχει σε μεγαλύτερο βαθμό μέσα στο δίκτυο ή ακόμη είναι αναπόσπαστο κομμάτι τους:

- DPoS: Μεταξύ των stakeholders και των delegates που εκείνοι ψηφίζουν για να τους εκπροσωπήσουν μέσα στο δίκτυο.
- PoT: Σημαντικός παράγοντας για την επίτευξη ομοφωνίας στο δίκτυο.
- PBFT: Απαραίτητη για λήψη αποφάσεων και επίτευξη ομοφωνίας μεταξύ των κόμβων του δικτύου.
- SCP: Απαραίτητη για αλληλεπίδραση και συμμετοχή σε quorum slices και quorums.
- RPCA: Απαραίτητη για συμμετοχή στην λίστα έμπιστων κόμβων.

3.12.3 Συναίνεση

Κάθε χρήστης που είναι μέλος ενός blockchain συστήματος αλληλοεπιδρά με τους υπόλοιπους κόμβους του δικτύου λαμβάνοντας πληροφορίες για την κατάσταση του συστήματος, δηλαδή την διαβεβαίωση ότι λειτουργεί σωστά. Αυτή η πληροφορία μπορεί να είναι όμως λάθος μιας και υπάρχει πιθανότητα στο δίκτυο να ενεργούν κακόβουλοι κόμβοι. Για αυτό το λόγο η συναίνεση ενός συστήματος ως προς τις απόψεις των χρηστών του χωρίζεται σε:

- Υποκειμενική, κατά την οποία οι απόψεις των χρηστών διίστανται και στο σύστημα εισέρχονται καινούργοι χρήστες κυρίως μέσω της κοινωνικής αναγνωσιμότητας του.
- Ελαφρώς Υποκειμενική, κατά την οποία ο κάθε χρήστης μπορεί να εκφέρει άποψη ως προς την συναίνεση του συστήματος, μιας και όλα τα απαραίτητα δεδομένα που χρειάζεται είναι ελεύθερα για ανάγνωση, γνωρίζοντας και έναν αριθμό έμπιστων κόμβων μέσα στο δίκτυο, όμως υπάρχει περίπτωση οι υπόλοιποι άγνωστοι κόμβοι να είναι κακόβουλοι.
- Αντικειμενική, κατά την οποία η άποψη όλων των χρηστών του συστήματος είναι κοινή, μιας και όλα τα απαραίτητα δεδομένα για την εξακρίβωση της συναίνεσης του δικτύου είναι ελεύθερα για ανάγνωση προς όλους [96].

Σύστημα Blockchain	**Συναίνεση**
Proof of Work	Αντικειμενική
Proof of Stake	Αντικειμενική
Delegated Proof of Stake	Ελαφρώς Υποκειμενική
Proof of Elapsed Time	Αντικειμενική
Practical Byzantine Fault Tolerance	Υποκειμενική
Stellar Consensus Protocol	Υποκειμενική
Ripple Protocol Consensus Algorithm	Υποκειμενική

Πίνακας 15 - Σύγκριση συναίνεσης των δημοφιλέστερων μηχανισμών συναίνεσης

3.12.4 Δημιουργία επόμενου block

Η διαδικασία έκδοσης του επόμενου block της αλυσίδας διαφέρει ανά μηχανισμό συναίνεσης και συγκεκριμένα:

- PoW: Εξόρυξη με χρήση hardware και κατακερματιστικής ισχύς των κόμβων.
- PoS: Ανάλογα την δύναμη του μεριδίου του κάθε συμμετέχον κόμβου (coin age).
- DPoS: Πρωτόκολλο ψηφοφορίας και ισχύς του stake.
- PoET: Χρήση εξιδεικευμένης υπολογιστικής δύναμης και έμπιστο περιβάλλον εκτέλεσης.
- PoT: Πρωτόκολλο ψηφοφορίας με γύρους.
- PBFT: Πρωτόκολλο ψηφοφορίας πολλών γύρων.
- SCP: Πρωτόκολλο ομοσπονδιακής ψηφοφορίας.
- RPCA: Πρωτόκολλο πιθανοτικής ψηφοφορίας.

3.12.5 Εχθρική ανοχή και ασφάλεια

Ένα σύστημα blockchain μπορεί να λεηλατηθεί από διάφορες μορφές επιθέσεων, όπως αναφέραμε και σε προηγούμενη παράγραφο (Ενότητα 3.9), από έναν ή περισσοτέρους κακόβουλους χρήστες ενός δικτύου με βασικότερο απώτερο σκοπό το κέρδος. Για τον λόγο αυτό, είναι υποχρέωση όλων των μηχανισμών συναίνεσης να προσφέρουν ένα ασφαλές περιβάλλον στον εκάστοτε χρήστη, το οποίο θα μπορεί να αμυνθεί σε όσο το δυνατόν περισσότερες μορφές επιθέσεων και συγκεκριμένα:

- Στα PoW συστήματα, ένας κόμβος για να καταφέρει να προσθέσει το επόμενο block στην αλυσίδα πρέπει να κατέχει την κατάλληλη υπολογιστική ισχύ. Αυτό συνεπάγεται με μεγάλη ενεργειακή δαπάνη, γεγονός που αποθαρρύνει έναν επίδοξο κακόβουλο χρήστη, μιας και είναι ασύμφορο. Τα τελευταία όμως χρονιά, τα mining pools πληθαίνουν όλο και περισσότερο, εξαιτίας του ότι τα μέλη μοιράζονται τα ενεργειακά έξοδα. Η ύπαρξη τους και η πιθανότητα ένας κόμβος να ελέγχει πάνω από το 51% της ισχύς του δικτύου έχει συντελέσει στην ανοχή του μηχανισμού κατά 25% σε εχθρικές ενέργειες [97].
- Το PoS προσφέρει ανοχή της τάξης του 50% μιας και δεν παρουσιάζονται προβλήματα όταν δεν υπάρχει κόμβος που να έχει μερίδιο παραπάνω από το μισό του συνολικού.
- Το DPoS παρέχει επίσης 50% ανοχή, αφού η σωστή λειτουργία του συστήματος είναι ευθύνη ορισμένων κόμβων και μπορεί να φτάσει σε έναν κακόβουλο χρήστη που θα ελέγξει την πλειοψηφία του δικτύου.
- Στο LPoS είναι και αυτό ανεκτικό κατά 50%, ακολουθώντας την μη κατοχή μεριδίου ενός κόμβου περισσοτέρου από το 50% του συνολικού.
- Το PoET είναι και αυτό ανεκτικό κατά 50%, εξαιτίας της πιθανότητας ελέγχου ενός μεταβλητού μέρους του συνόλου από έναν κόμβο, το οποίο αλλάζει ανά περίπτωση, καθώς και με χρήση πολύ μεγάλης υπολογιστικής ισχύς [98].
- Το PoT διαθέτει μηδενική ανοχή, καθώς μπορεί να ανταπεξέλθει μόνο σε αποτυχίες λογισμικού, εξαρτημάτων και επικοινωνίας μεταξύ των κόμβων, αλλά όχι κακόβουλες επιθέσεις.
- Στο PBFT η ανοχή ανέρχεται περίπου στο 33%, μιας και έμπιστοι κόμβοι πρέπει να καλύπτουν τα 2/3 του δικτύου για την επίτευξη ομοφωνίας.
- Και στο SCP ισχύει το ίδιο, δηλαδή περίπου 33% ανοχή, λόγω απαραίτητης εμπιστοσύνης μεταξύ της πλειοψηφίας των κόμβων.
- Στο RPCA όμως η ανοχή είναι μέχρι 20%, εξαιτίας της απαίτησης έμπιστων κόμβων κατά τουλάχιστον 80% του δικτύου, ενώ αν αυτό το ποσοστό είναι μικρότερο τότε η ομοφωνία του συστήματος δεν είναι σίγουρη. Σύμφωνα όμως με πρόσφατες μελέτες, η ανοχή του συστήματος μπορεί να φτάσει θεωρητικά το 90% βασιζόμενοι στην λίστα έμπιστων κόμβων [51].

3.12.6 Δυνατότητα επέκτασης

Με την πάροδο του χρόνου κάθε blockchain σύστημα πορεύεται προς την αναβάθμιση της πλατφόρμας του για την καλύτερη, γρηγορότερη και αποτελεσματικότερη εξυπηρέτηση όλο και περισσοτέρων χρηστών [99]. Η επεκτασιμότητα όμως διαφέρει ανά εφαρμογή καθώς ορισμένες έχουν περισσότερες δυνατότητες και προοπτικές από άλλες [100]. Οι κυριότεροι παράγοντες που την καθορίζουν είναι ο μηχανισμός συναίνεσης που είναι βασισμένη η κάθε πλατφόρμα, το μέγιστο όριο πλήθους κόμβων που μπορούν να είναι ταυτόχρονα συνδεδεμένοι και ο αριθμός συναλλαγών που μπορούν να πραγματοποιηθούν το δευτερόλεπτο ακόμη και όταν το σύστημα είναι στο όριο του [47]. Επίσης, σημαντικό ρόλο έχουν και η μείωση των χρονικών καθυστερήσεων, όπως και η αύξηση των ταχυτήτων για πραγματοποίηση συναλλαγών, οι οποίες έχουν αναφερθεί σε προηγούμενες παραγράφους [38]. Παρακάτω αναφέρονται ορισμένα χαρακτηριστικά παραδείγματα ορισμένων εφαρμογών των βασικότερων μηχανισμών συναίνεσης με τις δυνατότητες επέκτασης τους, ενώ παράλληλα η απόδοση τους δεν θα μειώνεται [51].

Σύστημα Blockchain	**Μηχανισμός Συναίνεσης**	**Αριθμός συναλλαγών το δευτερόλεπτο**	**Επεκτασιμότητα πλήθους κόμβων**
Bitcoin	PoW	3-7	Απεριόριστη (Θεωρητικά) Χιλιάδες (Πρακτικά)
Ethereum	PoW	15-20	Απεριόριστη (Θεωρητικά) Χιλιάδες (Πρακτικά)
Cardano	PoS	5-7	Απεριόριστη (Θεωρητικά) Χιλιάδες (Πρακτικά)
EOS.IO	DPoS	50 (πρακτικά) 3996 (θεωρητικά)	Απεριόριστη (Θεωρητικά) Χιλιάδες (Πρακτικά)
NEM	PoI	Έως 3085	Απεριόριστη (Θεωρητικά) Χιλιάδες (Πρακτικά)
Hyperledger Fabric	PBFT	2000-3500	Πολύ Μικρή (30-64)
Stellar	SCP	1000	Μικρή (έως 200)
Ripple	RPCA	1500	Μικρή (έως 200)

Πίνακας 16 - Σύγκριση δυνατότητας επέκτασης των δημοφιλέστερων εφαρμογών των μηχανισμών συναίνεσης

3.12.7 Άλλα κριτήρια σύγκρισης

Υπάρχουν και αλλά όμως κριτήρια που μπορούν να συγκριθούν μεταξύ τους οι βασικότεροι μηχανισμοί συναίνεσης, όπως το μοντέλο συναίνεσης τους, ο τύπος του blockchain συστήματος που εφαρμόζεται, η διαχείριση της ταυτότητας κάθε κόμβου, το επίπεδο αποκεντρωτισμού, η ενέργεια που καταναλώνουν και το κόστος συμμέτοχης για κάθε κόμβο, τα οποία φαίνονται στον ακόλουθο πίνακα.

Σύστημα Blockchain	**Μοντέλο Συναίνεσης**	**Κατηγορία Εφαρμογής Συστήματος**	**Ταυτότητα Κόμβου**	**Βαθμός Αποκέντρωσης/ Συγκέντρωσης**	**Κατανάλωση Ενέργειας**	**Κόστος Εισόδου**	**Εφαρμογή**
PoW	Proof-based	Δημόσιο	Δημόσια	Αποκεντρωτικό (προς Συγκεντρωτικό)	Μεγάλη	Μεγάλο	Bitcoin
PoS	Proof-based και Vote-based	Δημόσιο και Ιδιωτικό	Δημόσια	Αποκεντρωτικό (Μερικώς)	Μέτρια προς μεγάλη	Μέτριο	Cardano
DPoS	Proof-based	Δημόσιο και Ιδιωτικό	Δημόσια	Μεταβλητό	Μέτρια	Μικρό	EOS
LPoS	Proof-based και Vote-based	Δημόσιο και Ιδιωτικό	Δημόσια	Αποκεντρωτικό	Μέτρια	Μικρό	Waves
PoET	Proof-based	Δημόσιο και Ιδιωτικό	Δημόσια	Συγκεντρωτικό (προς Κεντρικό)	Μικρή	Μικρό	Hyperledger Sawtooth
PoT	Vote-based	Ιδιωτικό	Ιδιωτική	Συγκεντρωτικό	Πολύ μικρή	Πολύ μικρό	Quorum
PBFT	Vote-based	Ιδιωτικό	Ιδιωτική	Συγκεντρωτικό	Πολύ μικρή	Μηδενικό	Hyperledger Fabric
SCP	Vote-based	Δημόσιο	Δημόσια	Αποκεντρωτικό	Πολύ μικρή	Σχεδόν Μηδενικό	Stellar
RPCA	Vote-based	Δημόσιο	Δημόσια	Αποκεντρωτικό	Πολύ μικρή	Σχεδόν Μηδενικό	Ripple

Πίνακας 17 - Σύγκριση των δημοφιλέστερων μηχανισμών συναίνεσης

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην συγκεκριμένη διπλωματική αναφέραμε αρχικά τα κυριότερα δομικά χαρακτηριστικά της τεχνολογίας blockchain, όπως τα διανεμημένα δίκτυα και την κρυπτογράφηση, ενώ αναλύσαμε και την διαφορά μεταξύ συγκεντρωτισμού και αποκέντρωσης. Στην συνέχεια, αφού κατανοήσαμε τα βασικά για τον τρόπο λειτουργίας του blockchain, περάσαμε στον κορμό της εργασίας, τους μηχανισμούς συναίνεσης. Πρώτα μελετήσαμε τους δημοφιλέστερους μηχανισμούς ως προς την δομή τους, ενώ έπειτα, περνώντας στον τομέα της ασφάλειας, περιγράψαμε ορισμένες πιθανές επιθέσεις που μπορούν να προκύψουν σε τέτοιου είδους συστήματα. Δεύτερον, διαφοροποιήσαμε τους 3 τύπους blockchain συστημάτων, αναφέροντας και μερικά στοιχεία που τα χαρακτηρίζουν. Τέλος, με όλες τις γνώσεις που διαθέταμε, προχωρήσαμε σε μία σύγκριση των βασικότερων εν χρήση μηχανισμών συναίνεσης από διάφορες πτυχές.

Έπειτα από όλη αυτή τη μελέτη πλέον έχουμε σχηματίσει μία πιο εμπεριστατωμένη άποψη για το blockchain και τους μηχανισμούς του. Γενικά, μπορούμε να συμπεράνουμε ότι από θέμα ταχύτητας και διακίνησης συναλλαγών, τα BFT συστήματα είναι πιο αποδοτικά, ενώ από πλευράς εξυπηρέτησης περισσοτέρων κόμβων τα proof-based μοντέλα θεωρούνται πιο επεκτάσιμα. Ως προς τον τομέα της ασφάλειας, ενώ ορισμένοι μηχανισμοί είναι πιο ανεκτικοί σε σχέση με άλλους, κανένας τους δεν παρέχει απόλυτη προστασία σε όλες τις μορφές κακόβουλων επιθέσεων. Τελικά, συμπεραίνουμε πως δεν υπάρχει ένας μηχανισμός συναίνεσης που στο σύνολο του να είναι καλύτερος από τους υπόλοιπους, αλλά αυτή η επιλογή διαφέρει ανάλογα την εφαρμογή που θέλουμε να το χρησιμοποιήσουμε.

Η blockchain τεχνολογία, ενώ έγινε γνωστή μέσω των κρυπτονομισμάτων ως ένας τρόπος αποκεντρωμένες πραγματοποίησης συναλλαγών μέσα σε δίκτυα ομότιμων κόμβων, πλέον έχει αρχίσει να αποσπάται καθαρά από τον κλάδο της οικονομίας και να επεκτείνεται σε διάφορους τομείς, όπως της πολιτικής, της εκπαίδευσης και της υγείας. Με το πέρασμα των χρονών η συγκεκριμένη τεχνολογία θα συνεχίσει μόνο να εξελίσσεται βελτιώνοντας τα ήδη υπάρχων μοντέλα, δημιουργώντας καινούργια και ανακαλύπτοντας νέους τρόπους εφαρμογής της.

Βιβλιογραφία – Αναφορές – Διαδικτυακές Πηγές

[1] R. Maull, P. Godsiff, C. Mulligan, A. Brown και B. Kewell, «Distributed ledger technology: Applications and implications,» *Strategic Change*, τόμ. 26, αρ. 5, pp. 481-489, 2017.

[2] I. Bashir, Mastering blockchain, Packt Publishing Ltd, 2017.

[3] S. Nakamoto, «Bitcoin: A peer-to-peer electronic cash system,» 2019.

[4] G. F. Coulouris, J. Dollimore και T. Kindberg, Distributed systems: concepts and design, pearson education, 2005.

[5] M. Ripeanu, «Peer-to-peer architecture case study: Gnutella network,» σε *Proceedings first international conference on peer-to-peer computing*, 2001, pp. 99-100.

[6] R. Schollmeier, «A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications,» σε *Proceedings First International Conference on Peer-to-Peer Computing*, Miinchen, 2001, pp. 101-102.

[7] S. K. G. MukeshThakre και M. K. Mishra, «Distribution System faults Classification and Location Based on Wavelet Transform,» *International Journal on Advanced Computer Theory and Engineering*, τόμ. 2, αρ. 4, pp. 2319-2526, 2013.

[8] P. R. Parvedy και M. Raynal, «Uniform agreement despite process omission failures,» σε *Proceedings of the 17th International Symposium on Parallel and Distributed Processing*, 2003.

[9] M. J. Fischer, N. A. Lynch και M. S. Paterson, «Impossibility of distributed consensus with one faulty process,» *Journal of the ACM(JACM)*, τόμ. 32, αρ. 2, pp. 374-382, 1985.

[10] C. Dwork, N. Lynch και L. Stockmeyer, «Consensus in the presence of partial synchrony,» *Journal of the ACM (JACM)*, τόμ. 35, αρ. 2, pp. 288-323, 1988.

[11] T. D. Chandra και S. Toueg, «Unreliable failure detectors for reliable distributed systems,» *Journal of the ACM (JACM)*, τόμ. 43, αρ. 2, pp. 225-267, 1966.

[12] W. Diffie και M. Hellman, «New directions in cryptography,» *IEEE transactions on Information Theory*, τόμ. 22, αρ. 6, pp. 644-654, 1976.

[13] M. Naor και M. Yung, «Universal one-way hash functions and their cryptographic applications,» σε *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, 1989, pp. 33-43.

[14] D. Ongaro και J. Ousterhout, «In search of an understandable consensus algorithm,» σε *2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14*, 2014, pp. 305-319.

[15] D. Johnson, A. Menezes και S. Vanstone, «The elliptic curve digital signature algorithm (ECDSA)}„» *International journal of information security*, τόμ. 1, αρ. 1, pp. 36-63, 2001.

[16] A. Back, «Hashcash-a denial of service counter-measure,» 2002.

[17] S. Peng, «BITCOIN: Cryptography, Economics, and the Future,» *Senior Capstone Thesis School of Engineering and Applied Science,* 2013.

[18] M. A. Khan και K. Salah, «IoT security: Review, blockchain solutions, and open challenges,» *Future Generation Computer Systems,* τόμ. 82, pp. 395-411, 2018.

[19] R. Böhme, N. Christin, B. Edelman και T. Moore, «Bitcoin: Economics, technology, and governance,» *Journal of economic Perspectives,* τόμ. 29, αρ. 2, pp. 213-238, 2015.

[20] G. Becker, «Merkle signature schemes, merkle trees and their cryptanalysis,» *Ruhr-University Bochum, Tech. Rep,* 2008.

[21] C. Decker και R. Wattenhofer, «Information propagation in the bitcoin network,» σε *IEEE P2P 2013 Proceedings,* IEEE, 2013, pp. 1-10.

[22] S. King και S. Nadal, «Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,» *self-published paper, August,* τόμ. 19, p. 1, 2012.

[23] A. Wahab και W. Mehmood, «Survey of consensus protocols,» *arXiv preprint arXiv:1810.03357,* 2018.

[24] J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein και J. Herrera-Joancomartí, Data privacy management, cryptocurrencies and blockchain technology, τόμ. 10436, Springer, 2017.

[25] J. Chen και S. Micali, «Algorand,» *arXiv preprint arXiv:1607.01341,* 2016.

[26] Y. Gilad, R. Hemo, S. Micali, G. Vlachos και N. Zeldovich, «Algorand: Scaling byzantine agreements for cryptocurrencies,» σε *Proceedings of the 26th Symposium on Operating Systems Principles,* 2017, pp. 51-68.

[27] P. Vasin, «Blackcoin's proof-of-stake protocol v2,» τόμ. 71, 2014.

[28] V. Buterin και V. Griffith, «Casper the friendly finality gadget,» *arXiv preprint arXiv:1710.09437,* 2017.

[29] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong και M. Zhou, «Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism,» *IEEE Access,* τόμ. 7, pp. 118541-118555, 2019.

[30] I. Grigg, «Eos-an introduction,» *White paper,* 2017.

[31] F. Schuh και D. Larimer, «Bitshares 2.0: Financial smart contract platform,» *Accessed: Jan,* τόμ. 15, p. 2017, 2015.

[32] Y. Kwon, J. Liu, M. Kim, D. Song και Y. Kim, «Impossibility of full decentralization in permissionless blockchains,» σε *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 110-123.

[33] K. Janowicz, B. Regalia, P. Hitzler, G. Mai, S. Delbecque, M. Fröhlich, P. Martinent και T. Lazarus, «On the prospects of blockchain and distributed ledger technologies for open science and academic publishing,» *Semantic web*, τόμ. 9, αρ. 5, pp. 545-555, 2018.

[34] G.-T. Nguyen και K. Kim, «A survey about consensus algorithms used in blockchain,» *Journal of Information processing systems*, τόμ. 14, αρ. 1, pp. 101-128, 2018.

[35] I. Bentov, C. Lee, A. Mizrahi και M. Rosenfeld, «Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y,» *ACM SIGMETRICS Performance Evaluation Review*, τόμ. 42, αρ. 3, pp. 34-37, 2014.

[36] M. Salimitari και M. Chatterjee, «A survey on consensus protocols in blockchain for iot networks,» *arXiv preprint arXiv:1809.05613*, 2018.

[37] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue και U. R. Savagaonkar, «Innovative instructions and software model for isolated execution.,» *Hasp@ isca*, τόμ. 10, αρ. 1, 2013.

[38] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu και W. Shi, «On security analysis of proof-of-elapsed-time (poet),» σε *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, Springer, 2017, pp. 282-297.

[39] M. Bakhoff, «Consensus algorithms for distributed systems,» σε *2010 Free. Annu. Conf*, 2010, pp. 222-225.

[40] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun και L. Li, «A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services,» *IEEE Transactions on Services Computing*, τόμ. 12, αρ. 3, pp. 429-445, 2018.

[41] D. Ongaro και J. Ousterhout, «The raft consensus algorithm,» 2015.

[42] K. Li, H. Li, H. Hou, K. Li και Y. Chen, «Proof of vote: A high-performance consensus protocol based on vote mechanism \& consortium blockchain,» σε *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, IEEE, 2017, pp. 466-473.

[43] E. Buchman, «Tendermint: Byzantine fault tolerance in the age of blockchains,» 2016.

[44] W. Y. M. M. Thin, N. Dong, G. Bai και J. S. Dong, «Formal analysis of a proof-of-stake blockchain,» σε *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*, IEEE, 2018, pp. 197-200.

[45] M. Castro και B. Liskov, «Practical byzantine fault tolerance,» *OSDI,* τόμ. 99, αρ. 1999, pp. 173-186, 1999.

[46] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei και C. Qijun, «A review on consensus algorithm of blockchain,» σε *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, IEEE, 2017, pp. 2567-2572.

[47] M. Vukolić, «The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication,» σε *International workshop on open problems in network security*, Springer, 2015, pp. 112-125.

[48] C. Cachin, «Architecture of the hyperledger blockchain fabric,» *Workshop on distributed cryptocurrencies and consensus ledgers,* τόμ. 310, αρ. 4, 2016.

[49] D. Mazieres, «The stellar consensus protocol: A federated model for internet-level consensus,» *Stellar Development Foundation,* τόμ. 32, 2015.

[50] L. S. Sankar, M. Sindhu και M. Sethumadhavan, «Survey of consensus protocols on blockchain applications,» σε *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, 2017, pp. 1-5.

[51] J. Debus, «Consensus methods in blockchain systems,» *Frankfurt School of Finance \& Management, Blockchain Center, Tech. Rep,* 2017.

[52] D. Schwartz, N. Youngs και A. Britto, «The ripple protocol consensus algorithm,» *Ripple Labs Inc White Paper,* τόμ. 5, αρ. 8, p. 151, 2014.

[53] M. Dehghani, A. Mashatan και R. W. Kennedy, «Innovation within networks--patent strategies for blockchain technology,» *Journal of Business \& Industrial Marketing,* 2020.

[54] B. Chase και E. MacBrough, «Analysis of the XRP ledger consensus protocol,» *arXiv preprint arXiv:1802.07242,* 2018.

[55] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef και E. Zenner, «Ripple: Overview and outlook,» σε *International Conference on Trust and Trustworthy Computing*, Springer, 2015, pp. 163-180.

[56] I.-C. Lin και T.-C. Liao, «A survey of blockchain security issues and challenges.,» *IJ Network Security,* τόμ. 19, αρ. 5, pp. 653-659, 2017.

[57] Y. Takefuji, «Security Protection Mechanisms Must Be Embedded in Blockchain Applications,» *Journal of Chemical Education,* τόμ. 97, αρ. 7, pp. 1819-1820, 2020.

[58] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang και A. Mohaisen, «Exploring the attack surface of blockchain: A systematic overview,» *arXiv preprint arXiv:1904.03487,* 2019.

[59] S. Sayeed και H. Marco-Gisbert, «Assessing blockchain consensus and security mechanisms against the 51\% attack,» *Applied Sciences,* τόμ. 9, αρ. 9, p. 1788, 2019.

[60] J. J. Xu, «Are blockchains immune to all malicious attacks?,» *Financial Innovation,* τόμ. 2, αρ. 1, pp. 1-9, 2016.

[61] S. Shanaev, A. Shuraeva, M. Vasenin και M. Kuznetsov, «Cryptocurrency value and 51\% attacks: evidence from event studies,» *The Journal of Alternative Investments,* τόμ. 22, αρ. 3, pp. 65-77, 2019.

[62] A. Miller, A. Kosba, J. Katz και E. Shi, «Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions,» σε *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security,* 2015, pp. 680-691.

[63] M. Bastiaan, «Preventing the 51\%-attack: a stochastic analysis of two phase proof of work in bitcoin,» σε *Availab le at http://referaat. cs. utwente. nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-oftwo-phase-proof-of-work-in-bitcoin. pdf,* 2015.

[64] J. R. Douceur, «The sybil attack,» σε *International workshop on peer-to-peer systems,* Springer, 2002, pp. 251-260.

[65] K. Alachkar και D. Gaastra, *Blockchain-based Sybil Attack Mitigation: A Case Study of the I2P Network,* Semanticscholar Seattle, Washington, 2018.

[66] I. D. Rubasinghe και T. De Zoysa, «Transaction verification model over double spending for peer-to-peer digital currency transactions based on blockchain architecture,» *International Journal of Computer Applications,* τόμ. 975, p. 8887, 2012.

[67] Z. Peng και Y. Chen, «All roads lead to Rome: Many ways to double spend your cryptocurrency,» *arXiv preprint arXiv:1811.06751,* 2018.

[68] J. H. Mosakheil, «Security threats classification in blockchains,» 2018.

[69] E. Heilman, A. Kendler, A. Zohar και S. Goldberg, «Eclipse attacks on bitcoin's peer-to-peer network,» σε *24th {USENIX} Security Symposium ({USENIX} Security 15)*, 2015, pp. 129-144.

[70] K. Wüst και A. Gervais, «Ethereum eclipse attacks,» 2016.

[71] F. Lau, S. H. Rubin, M. H. Smith και L. Trajkovic, «Distributed denial of service attacks,» σε *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0*, τόμ. 3, IEEE, 2000, pp. 2275--2280.

[72] M. Vasek, M. Thornton και T. Moore, «Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem,» σε *International conference on financial cryptography and data security*, Springer, 2014, pp. 57-71.

[73] M. Saad, M. T. Thai και A. Mohaisen, «POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization,» σε *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, 2018, pp. 809-811.

[74] B. Johnson, A. Laszka, J. Grossklags, M. Vasek και T. Moore, «Game-theoretic analysis of DDoS attacks against Bitcoin mining pools,» σε *International Conference on Financial Cryptography and Data Security*, Springer, 2014, pp. 72-86.

[75] C. Dietzel, M. Wichtlhuber, G. Smaragdakis και A. Feldmann, «Stellar: network attack mitigation using advanced blackholing,» σε *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies*, 2018, pp. 152-164.

[76] E. Osterweil, A. Stavrou και L. Zhang, «20 years of ddos: a call to action,» *arXiv preprint arXiv:1904.02739*, 2019.

[77] M. Apostolaki, A. Zohar και L. Vanbever, «Hijacking bitcoin: Routing attacks on cryptocurrencies,» σε *2017 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2017, pp. 375-392.

[78] Q. Jacquemart, «Towards uncovering BGP hijacking attacks,» 2015.

[79] J. Garzik, «Public versus private blockchains,» *BitFury Group, San Francisco, USA, White Paper*, τόμ. 1, 2015.

[80] G. Hileman και M. Rauchs, «2017 global blockchain benchmarking study,» *SSRN 3040224*, 2017.

[81] L. Arnold, M. Brennecke, P. Camus, G. Fridgen, T. Guggenberger, S. Radszuwill, A. Rieger, A. Schweizer και N. Urbach, «Blockchain and initial coin offerings: blockchain's implications for crowdfunding,» σε *Business transformation through blockchain*, Springer, 2019, pp. 233-272.

[82] Z. Zheng, S. Xie, H. Dai, X. Chen και H. Wang, «An overview of blockchain technology: Architecture, consensus, and future trends,» σε *2017 IEEE international congress on big data (BigData congress)*, IEEE, 2017, pp. 557-564.

[83] M. Ali, R. Shea, J. Nelson και M. J. Freedman, «Blockstack: A new internet for decentralized applications,» *Technical whitepaper version*, τόμ. 1, 2017.

[84] P. Thakkar, S. Nathan και B. Viswanathan, «Performance benchmarking and optimizing hyperledger fabric blockchain platform,» σε *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, IEEE, 2018, pp. 264-276.

[85] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea και E. B. Hamida, «Consortium blockchains: Overview, applications and challenges,» *International Journal On Advances in Telecommunications,* τόμ. 11, αρ. 1&2, pp. 51-64, 2018.

[86] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso και P. Rimba, «A taxonomy of blockchain-based systems for architecture design,» σε *2017 IEEE international conference on software architecture (ICSA)*, IEEE, 2017, pp. 243-252.

[87] M. Hearn, «Corda: A distributed ledger,» *Corda Technical White Paper,* τόμ. 2016, 2016.

[88] S. Gilbert και N. Lynch, «Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services,» *Acm Sigact News,* τόμ. 33, αρ. 2, pp. 51-59, 2002.

[89] E. Brewer, «CAP twelve years later: How the" rules" have changed,» *Computer,* τόμ. 45, αρ. 2, pp. 23-29, 2012.

[90] K. Zhang και H.-A. Jacobsen, «Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains.,» σε *ICDCS*, 2018, pp. 1337-1346.

[91] J. Yli-Huumo, D. Ko, S. Choi, S. Park και K. Smolander, «Where is current research on blockchain technology?—a systematic review,» *PloS one,* τόμ. 11, αρ. 10, p. e0163477, 2016.

[92] V. Gramoli, «On the danger of private blockchains,» σε *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16)*, 2016.

[93] S. Albrecht, S. Reichert, J. Schmid, J. Strüker, D. Neumann και G. Fridgen, «Dynamics of blockchain implementation-a case study from the energy sector,» σε *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[94] N. Z. Aitzhan και D. Svetinovic, «Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,» *IEEE Transactions on Dependable and Secure Computing,* τόμ. 15, αρ. 5, pp. 840-852, 2016.

[95] A. Grigorean, «Latency and finality in different cryptocurrencies,» *Accessed: Jan,* τόμ. 4, 2019.

[96] V. Buterin, «Proof of stake: how I learned to love weak subjectivity,» *Ethereum Blog,* 2014.

[97] I. Eyal και E. G. Sirer, «Majority is not enough: Bitcoin mining is vulnerable,» *International conference on financial cryptography and data security*, pp. 436-454, 2014.

[98] S. Shetty, C. A. Kamhoua και L. L. Njilla, Blockchain for distributed systems security, John Wiley & Sons, 2019.

[99] V. Buterin, J. Coleman και M. Wampler-Doty, *Notes on Scalable Blockchain Protocols (verson 0.3)*, 2015.

[100] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi και E. G. Sirer, «On scaling decentralized blockchains,» σε *International conference on financial cryptography and data security*, Springer, 2016, pp. 106-125.