ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟΣΧΟΛΗ
ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

«Σύγκριση Τεχνολογιών Κατανεμημένης Εγγραφής “Blockchain”»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Μπεκρή Ελένης

Επιβλέπων : Δημήτριος Ασκούνης

Καθηγητής ΕΜΠ

Αθήνα, Ιούνιος 2020

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟΣΧΟΛΗ
ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ
ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

«Σύγκριση Τεχνολογιών Κατανεμημένης Εγγραφής “Blockchain”»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Μπεκρή Ελένης

Επιβλέπων : Δημήτριος Ασκούνης

Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την …….

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χάρης Δούκας
Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ

Αθήνα, Ιούνιος 2020

.....

Ελένη Μπεκρή

Διπλωματούχος Ηλεκτρολόγος Μηχανικός & Μηχανικός Υπολογιστών Ε.Μ.Π

Περίληψη

Τα τελευταία χρόνια η ραγδαία εξέλιξη της τεχνολογίας, αλλά και η συνεχόμενη ανάγκη για πραγμάτωση απομακρυσμένων και γρήγορων συναλλαγών και ανταλλαγής δεδομένων καθιστούν τα θέματα της ασφάλειας και αμεσότητας πιο καίρια από ποτέ.

Στη παρούσα διπλωματική εργασία λοιπόν εξετάζεται η σχετικά νέα τεχνολογία BlockChain, η οποία «υπόσχεται» ασφάλεια και μείωση κόστους συναλλαγών, ανωνυμία χρηστών, αμεσότητα και αποκέντρωση. Στα κεφάλαια που ακολουθούν γίνεται μια αναλυτική παρουσίαση των αρχών του BlockChain καθώς και της αρχιτεκτονικής αυτών των δικτύων και γίνεται επίσης μια βασική αρχική κατηγοριοποίηση βάσει των δικαιωμάτων των χρηστών.

Ακολουθεί η δεύτερη φάση κατηγοριοποίησης των δικτύων BlockChain η οποία στηρίζεται σε διαφορετικές παραμέτρους. Οι βασικότερες αυτών είναι η ιδιοκτησία του δικτύου, τα δικαιώματα του χρήστη καθώς και ο μηχανισμός συναίνεσης. Οι δύο μεγάλες κατηγορίες είναι τα public και τα private blockchains, ανάλογα με το αν το δίκτυο ανήκει σε κάποιο φυσικό πρόσωπο, οργανισμό ή επιχείρηση. Υπάρχουν επίσης και τα consortium τα οποία έχουν λογική για χρήση μεταξύ πολλαπλών εταίρων ή οργανισμών. Συγκεκριμένα τα public blockchains μπορούν να είναι permissioned ή permissionless ανάλογα με την ύπαρξη ή όχι περιορισμών στα δικαιώματα των χρηστών.

Στην συνέχεια γίνεται διάκριση λαμβάνοντας υπόψιν τον μηχανισμό συναίνεσης που χρησιμοποιείται σε διάφορες πλατφόρμες. Οι πιο διαδεδομένοι μηχανισμοί συναίνεσης είναι οι εξής: Proof-of-Work, Proof-of-X, Proof-of-Stake, Proof-of-Capacity, Proof-of-Elapsed Time [36]. Καθώς η τεχνολογία BlockChain εξελίσσεται, προκύπτουν διαφορετικές απαιτήσεις που αναπόφευκτα οδηγούν σε ανάπτυξη νέων πρωτοκόλλων. Γενικεύοντας διακρίνουμε 3 κατηγορίες: Πρωτόκολλα εκλογής βάσει εργασίας (PoW), πρωτόκολλα εκλογής βάσει ιδιότητας (PoX) και υβριδικά πρωτόκολλα.

Τέλος βάσει των παραπάνω κατηγοριοποιήσεων και διαφορών, αναλύουμε τα χαρακτηριστικά ορισμένων διαδεδομένων πλατφορμών BlockChain -Bitcoin, Ripple, Hyperledger Fabric, Corda, Quorum- καλύπτοντας τον συνδυασμό των παραμέτρων που προαναφέρθηκαν αλλά και κάποιων επιπλέον. Στο τελευταίο κεφάλαιο καταγράφονται αναλυτικά τα συμπεράσματα αυτής της έρευνας, το ενδεχόμενο για μελλοντική επέκτασης της, όπως επίσης οι περιορισμοί και οι δυσκολίες που προέκυψαν κατά την υλοποίηση της.

Λέξεις Κλειδιά

Τεχνολογία Κατανεμημένης Εγγραφής, Έξυπνα Συμβόλαια, Συναίνεση, Κρυπτογραφία, Κατακερματισμός, Ψηφιακή Υπογραφή, Εξόρυξη, Ιδιωτικά-Δημόσια Δίκτυα, Χρονοσφραγίδα

Abstract

In recent years, the rapid development of technology, as well as the continuing need for remote and fast transactions and data exchange make the issues of security and immediacy more crucial than ever.

The present dissertation examines the relatively new BlockChain technology, which "promises" security and reduced transaction costs, anonymity of users, immediacy and decentralization. The following chapters provide a detailed presentation of the principles of BlockChain as well as the architecture of these networks and a basic initial categorization based on users' rights.

Following, is the second phase of BlockChain network categorization, which is based on different parameters. The most basic are the ownership of the network, the rights of the user and the consent mechanism. The two major categories are the public and private blockchains, depending on whether the network belongs to an individual, organization or business. There are also consortiums that make sense for use between multiple partners or organizations. In particular, public blockchains can be permissioned or permissionless depending on whether or not there are restrictions on users' rights.

Then, a distinction is made taking into account the consensus mechanism used on various platforms. The most common consent mechanisms are: Proof-of-Work, Proof-of-X, Proof-of-Stake, Proof-of-Capacity, Proof-of-Elapsed Time [36]. As BlockChain technology evolves, different requirements arise that inevitably lead to the development of new protocols. In general, we distinguish 3 categories: Work-Based Selection Protocols (PoW), Property-Based Selection Protocols (PoX) and Hybrid Protocols.

Finally, based on the above categorizations and differences, we analyze the characteristics of some common BlockChain platforms -Bitcoin, Ripple, Hyperledger Fabric, Corda, Quorum- covering the combination of the above-mentioned parameters and some more. In the last chapter, the conclusions of this research are recorded in detail, the possibility for its future expansion, and also the limitations and difficulties that arose during its implementation.

KeyWords

Blockchain, Block, Consensus, Consortium Blockchains, Cryptography, Digital Signature, Ethereum, Genesis block, Merkle tree, Mining, Private Blockchain, Proof of Work (PoW), Public Blockchain, SHA, Smart contracts

Πρόλογος

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο ολοκλήρωσης του προπτυχιακού κύκλου σπουδών της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου. Η εργασία ανατέθηκε από το Εργαστήριο Συστημάτων Αποφάσεων και Διοίκησης και έχει ως θέμα τη σύγκριση υπαρχουσών τεχνολογιών κατανεμημένης εγγραφής Blockchain .

Στόχος της διπλωματικής εργασίας είναι η οικειοποίηση του αναγνώστη με τη λογική στην οποία έχουν βασιστεί τα δίκτυα Blockchain, με μια βαθύτερη ματιά στις αρχές της λειτουργίας τους, δίνοντας του τελικά τη δυνατότητα να μελετήσει τις διαφορές των υπαρχουσών τεχνολογιών, να βγάλει τα δικά του συμπεράσματα και να μπορέσει να βοηθηθεί σε περίπτωση που επιθυμεί να συμμετάσχει σε κάποιο δίκτυο ή ακόμα και να δημιουργήσει ένα νέο δικό του.

Απώτερος σκοπός είναι η διάδοση των νέων αυτών ευκαιριών οι οποίες είναι πολλές τόσο για τους πολίτες όσο και για τις επιχειρήσεις λόγω των νέων τρόπων ανταλλαγής δεδομένων που προσφέρει το blockchain και των συναλλαγών, που προσφέρουν τα ψηφιακά νομίσματα. Επίσης είναι γνωστό πως οι μεγαλύτερες κεντρικές τράπεζες έχουν προβάλει πλήθος ανακοινώσεων για τους κινδύνους που κρύβονται πίσω από τις Blockchain τεχνολογίες, αφού όπως είναι λογικό έχουν θορυβηθεί από την ραγδαία ανάπτυξη των ψηφιακών νομισμάτων. Για το λόγο αυτό η μελέτη του συγκεκριμένου θέματος έχει γίνει απαραίτητη, ώστε να αποφευχθούν τυχούσες προσπάθειες παραπληροφόρησης που μπορεί να οδηγήσουν στη «βύθιση» του Blockchain πριν προλάβουμε να γνωρίσουμε τα όρια και της προοπτικές εξέλιξης και εφαρμογής του.

Ευχαριστίες

Θέλω αρχικά να ευχαριστήσω εγκάρδια τον κύριο Σκαλιδάκη Σταύρο και το Εργαστήριο Συστημάτων Αποφάσεων και Διοίκησης του Εθνικού Μετσόβιου Πολυτεχνείου, τόσο για την ευκαιρία που μου παρείχαν να ασχοληθώ με ένα τόσο ενδιαφέρον και καινοτόμο θέμα, όσο και για την στήριξη που μου προσέφεραν κατά τη διάρκεια εκπόνησης της εν λόγω διπλωματικής εργασίας.

Θα ήθελα επίσης να εκφράσω την ευγνωμοσύνη μου στην οικογένεια μου και στους φίλους μου, για την αμέριστη στήριξη και συμπαράσταση τους καθ' όλη την διάρκεια των σπουδών μου και κυρίως στους γονείς μου που δεν σταμάτησαν να πιστεύουν σε εμένα.

Μπεκρή Δ. Ελένη

Αθήνα, Ιούλιος 2020

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

1 ΚΕΦΑΛΑΙΟ 1ο – ΕΙΣΑΓΩΓΗ

1.1 Αντικείμενο και Σκοπός

Η επικοινωνία των ανθρώπων, η εξέλιξη της και τα μέσα που χρησιμοποιούνται για την επίτευξη της είναι ένα διαχρονικό επιστημονικό ζήτημα που απασχολεί και θα απασχολεί πάντα την επιστημονική κοινότητα. Στις μέρες μας λοιπόν η μοντέρνα τεχνολογία επιτρέπει στους ανθρώπους να επικοινωνούν άμεσα με την χρήση φωνητικών και βίντεο κλήσεων, emails, άμεσα μηνύματα τα οποία ταξιδεύουν από μία συσκευή σε μία άλλη. Η επικοινωνία γίνεται διατηρώντας την εμπιστοσύνη ο ένας στον άλλο, χωρίς την παρουσία τρίτου, ανεξάρτητα από το πόσο μακριά βρίσκονται.

Όταν όμως σε μία επικοινωνία μεταξύ δύο σημείων χρειάζεται να γίνει μία συναλλαγή, τότε οι διαδικασίες απαιτούν την εμπιστοσύνη ενός τρίτου για εδραίωση της εμπιστοσύνης, όπως ένα δικηγορικό γραφείο ή μία τράπεζα, με αποτέλεσμα το υψηλό κόστος, το ενδεχόμενο απάτης και την πιθανή περίπτωση αναποτελεσματικότητας.

Η τεχνολογία blockchain έρχεται να αλλάξει ριζικά αυτό το καθεστώς. Χρησιμοποιώντας μαθηματικά και κρυπτογραφία, το blockchain παρέχει μία ανοιχτή και αποκεντρωμένη βάση δεδομένων σε κάθε συναλλαγή που περιέχει αξία όπως χρήματα, αγαθά, ακίνητη περιουσία, εργασία ή ακόμα και σημειώσεις[58]. Δημιουργεί μία καταγραφή για κάθε συναλλαγή η οποία μπορεί να επαληθευτεί από όλη την κοινότητα. Το blockchain συνδυάζοντας την κρυπτογραφία και τα κατανεμημένα υπολογιστικά συστήματα παρέχει ασφαλείς, άμεσες peer-to-peer συναλλαγές, χωρίς την ανάγκη για παρέμβαση τρίτων.

Αν σωστά κατασκευασμένη, η blockchain τεχνολογία προσφέρει λύση στο πρόβλημα της ασφάλειας και της ιδιωτικότητας στο Internet of Things (IoT) περιβάλλον, παρέχοντας ένα νέο υπολογιστικό στρώμα, όπου τα δεδομένα μπορούν να υποβάλλονται σε επεξεργασία να αναλύονται με ασφάλεια, παραμένοντας ιδιωτικά. Το blockchain μπορεί επίσης να επιτρέψει τις μικρό-πληρωμές μεταξύ ψηφιακών συσκευών, μέσω ultra-light cryptocurrencies και έξυπνων συμβάσεων. Η υλοποίηση των χαρακτηριστικών αυτών αναμένεται να εξασφαλίσει μια πιο αποτελεσματική κατανομή των πόρων σε παγκόσμιο επίπεδο, αν και μπορεί επίσης να οδηγήσει σε ανεπιθύμητες συνέπειες - όπως ένα hyper-tokenization της κοινωνίας και μια δυνητικά καταστροφική συγκέντρωση ισχύος στις μεγάλες παγκόσμιες πλατφόρμες. Επομένως, τα συνολικά οφέλη και τα μειονεκτήματα του blockchain πρέπει να συμπεριληφθούν, για την εύρεση μιας ισορροπίας μεταξύ της ανάγκης για την καινοτομία, την οικονομική ανάπτυξη και την κοινωνική βιωσιμότητα.

Οι εφαρμογές πολλές: Ψηφιακά νομίσματα, ταυτότητες, κτηματολόγιο, συμβόλαια, κλειδαριές, διακρατικό εμπόριο, χρηματοπιστωτικές συναλλαγές και στο μέλλον ακόμα και αυτόνομες επιχειρηματικές λειτουργίες μπορούν να υλοποιηθούν αλλάζοντας τα πάντα.

Για μερικούς ανθρώπους, η τεχνολογία blockchain που βασίζεται στα Bitcoin και Ethereum θεωρείται ως η σημαντικότερη καινοτομία από το Διαδίκτυο. Ωστόσο, εξακολουθεί να είναι σε αρχικά στάδια. Επιπλέον, ο συνδυασμός με το IoT και άλλες τεχνολογίες απαιτεί ακόμα ουσιαστικές γνώσεις σχετικά με τους συγκεκριμένους τομείς εφαρμογής, την επεκτασιμότητα, τα ζητήματα ιδιωτικού απορρήτου, τις επιδόσεις και τα πιθανά οικονομικά οφέλη.

Για όλους αυτούς τους λόγους αναμφίβολα η εμφάνιση της τεχνολογίας BlockChain έχει ταράξει τα νερά της επιστημονικής κοινότητας και όπως όλα δείχνουν ήρθε για να μείνει, καθώς ήδη έχει τραβήξει το ενδιαφέρον χιλιάδων χρηστών , επιχειρήσεων, οργανισμών αλλά και κυβερνήσεων. Προσεγγίζει το ζήτημα της ασφάλειας με έναν καινοτόμο τρόπο, ο οποίος γεννάει τελικά σε πολλούς το ερώτημα αν μπορεί μια τεχνολογία να καταφέρει να γίνει «αήττητη»…

Αντικείμενο αυτής της εργασίας λοιπόν είναι σε αρχική φάση η οικειοποίηση του αναγνώστη με τη λογική στην οποία έχουν βασιστεί τα δίκτυα Blockchain, με μια βαθύτερη ματιά στις αρχές της λειτουργίας τους και στην συνέχεια η κατηγοριοποίηση αυτών των δικτύων βάσει της αξιολόγησης διάφορων παραμέτρων, όπως είναι για παράδειγμα, ο τρόπος συμμετοχής των ενδιαφερομένων σε μια πλατφόρμα, τα δικαιώματα τους μέσα σε αυτήν, ο τρόπος επαλήθευσης των συναλλαγών, η εξασφάλιση της ανωνυμίας, τα επίπεδα ασφαλείας, το κόστος, η ταχύτητα συναλλαγών κ.α. Μετά το πέρας των παραπάνω φάσεων, ακολουθεί η σύγκριση ορισμένων από τις πιο διαδεδομένες τεχνολογίες Blockchain βάσει της κατηγοριοποίησης που προηγήθηκε .

Στόχος είναι η ενημέρωση των ενδιαφερόμενων για τις υπάρχουσες πλατφόρμες κατανεμημένης εγγραφής και η καθοδήγηση τους σχετικά με το ποια τεχνολογία πρέπει να επιλέξουν για να συμμετάσχουν, ανάλογα με τα δικές τους απαιτήσεις από το δίκτυο. Επιπρόσθετα η παρούσα διπλωματική εργασία θα μπορούσε να αποτελέσει έναν οδηγό για οργανισμούς, εταιρείες και ιδιωτικές επιχειρήσεις που μελετούν την περίπτωση υλοποίησης μιας νέας πλατφόρμας. Στην παρούσα εργασία μπορούν να ενημερωθούν για τις παραμέτρους που πρέπει να λάβουν υπόψιν, για την συμπεριφορά κάποιων από τις ήδη χρησιμοποιούμενες και διαδεδομένες πλατφόρμες, για τα πλεονεκτήματα και τα μειονεκτήματα του κάθε δικτύου βάσει των χαρακτηριστικών του.

1.2 Φάσεις Υλοποίησης

Η υλοποίηση της εργασίας χωρίστηκε στις παρακάτω έξι φάσεις:

- **<u>Έρευνα - Συλλογή δεδομένων.</u>**

  Γενικότερη έρευνα για τις αρχές της τεχνολογίας Blockchain, τα οφέλη της, τα πλεονεκτήματα και τους περιορισμούς της χρήσης της. Στην συνέχεια κατηγοριοποίηση υπαρχουσών διαδεδομένων πλατφορμών βάσει διάφορων παραμέτρων, με σκοπό την απόκτηση μιας σφαιρικής εικόνας σχετικά με το ζητούμενο της εργασίας που είναι η σύγκριση τεχνολογιών Blockchain. Τέλος συλλογή αξιόπιστων δεδομένων από peppers και επιστημονικά sites μέσω κατάλληλων μηχανών αναζήτησης επικεντρωμένα στα ζητούμενα του θέματος.

- **Διασταύρωση και κατηγοριοποίηση πληροφοριών.**

Επαλήθευση της ορθότητας της συλλεγόμενης πληροφορίας, διασταυρώνοντας την αξιοπιστία των πηγών προέλευσης της και συγκρίνοντας τα δεδομένα με εκείνα άλλων αξιόπιστων πηγών.

- **Σχεδιασμός Δομής της Διπλωματικής εργασίας.**

Σχεδιασμός της δομής της διπλωματικής εργασίας, με τέτοιο τρόπο ώστε να είναι ευανάγνωστη, λογικά κατανεμημένη η καταγεγραμμένη πληροφορία και ομαλή η μετάβαση μεταξύ των κεφαλαίων, σύμφωνα με το περιεχόμενο τους.

- **Επεξεργασία της συγκεντρωμένης πληροφορίας και αντιστοίχιση της στα κεφάλαια της Διπλωματικής.**

Ομαδοποίηση, επεξεργασία και διαχωρισμός της συγκεντρωμένης πληροφορίας βάσει των κεφαλαίων στα οποία θα ενταχθούν.

- **Διεξαγωγή Συμπερασμάτων από την ερευνητική διαδικασία.**

Παρατήρηση και επεξεργασία των δεδομένων που προέκυψαν από την ερευνητική διαδικασία. Στην συνέχεια καταγραφή των συμπερασμάτων της εργασίας βάσει της επεξεργασμένης πληροφορίας που συλλέχθηκε.

- **Συγγραφή διπλωματικής και παρουσίαση αποτελεσμάτων.**

Συγγραφή της διπλωματικής σύμφωνα με τα παραπάνω στοιχεία.

Αξίζει να σημειωθεί πως λόγω του αντικειμένου της εργασίας η φάση της συλλογής δεδομένων στην συνέχεια σχεδόν παραλληλοποιήθηκε με τις υπόλοιπες φάσεις , καθώς αρκετά συχνά αναρτιόνταν νέες πληροφορίες και δεδομένα σχετικά με διάφορες τεχνολογίες Blockchain!

1.3 Οργάνωση Τόμου

Η παρούσα διπλωματική εργασία θα αναπτυχθεί σε επτά συνολικά κεφάλαια. Η διάρθρωση της εργασίας είναι η εξής:

- *Κεφάλαιο 1:* Καθορίζεται το αντικείμενο και ο σκοπός της διπλωματικής εργασίας, που είναι η σύγκριση τεχνολογιών κατανεμημένης εγγραφής blockchain και η κατηγοριοποίηση των υπαρχουσών πλατφορμών βάσει συγκεκριμένων χαρακτηριστικών. Αναλύονται επίσης οι φάσεις υλοποίησης της και η οργάνωση των κεφαλαίων της.
- *Κεφάλαιο 2:* Ορίζονται με σαφήνεια τα δομικά στοιχεία – Block, Consensus, Hashing κ.α.- , τα γενικά χαρακτηριστικά, η αρχιτεκτονική και οι βασικές αρχές της τεχνολογίας Blockchain. Μελετώνται επίσης τα οφέλη , οι περιορισμοί της χρήσης αυτών των δικτύων που οφείλονται κυρίως σε λόγους ασφάλειας.

- *Κεφάλαιο 3:* Καταγράφονται τομείς εφαρμογής της, όπως για παράδειγμα ο συνδυασμός του Blockchain με IoT, αναλύονται τα χαρακτηριστικά των επικρατέστερων πλατφορμών και γίνεται μια βασική αρχική κατηγοριοποίηση βάσει των δικαιωμάτων των χρηστών.
- *Κεφάλαιο 4:* Γίνεται η διάκριση των δικτύων Blockchain βάσει συγκεκριμένων παραμέτρων, όπως η ιδιοκτησία του δικτύου (public, private, consortium), η διαδικασία συμμετοχής ενός ενδιαφερόμενου στο δίκτυο, τα δικαιώματα των χρηστών (permissioned, permissionless) και οι μηχανισμοί συναίνεσης (PoW, PoS, PoX κ.α.).
- *Κεφάλαιο 5:* Πραγματοποιείται σύγκριση ορισμένων από των πιο διαδεδομένων τεχνολογιών κατανεμημένης εγγραφής, όπως είναι οι Bitcoin, Corda, Ripple, Quorum, βάσει των παραμέτρων που κατηγοριοποιήθηκαν στο κεφάλαιο 4.
- *Κεφάλαιο 6:* Παρουσιάζονται αναλυτικά τα συμπεράσματα που προκύπτουν από τη μελέτη των τεχνολογιών Blockchain, οι πιθανές προοπτικές της παρούσας διπλωματικής εργασίας καθώς και οι περιορισμοί που αντιμετωπίστηκαν κατά την υλοποίηση της.
- *Κεφάλαιο 7:* Καταγράφεται η βιβλιογραφία και οι ιστότοποι από τα οποία συλλέχθηκε το υλικό της εργασίας.

2 ΚΕΦΑΛΑΙΟ 2ο - ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

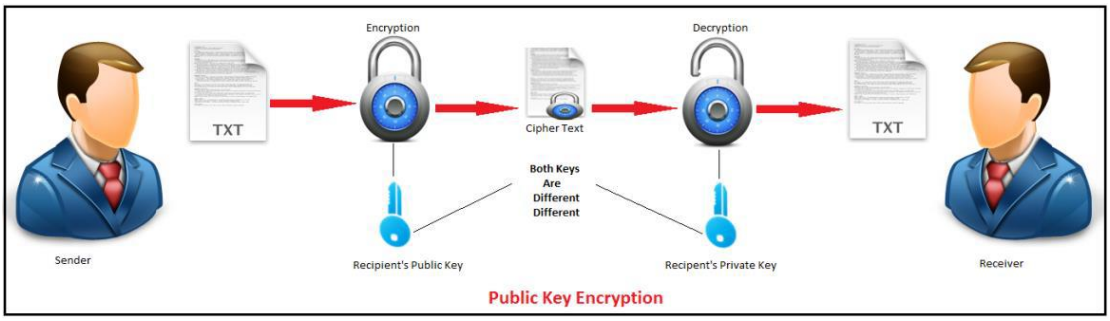
2.1 Κρυπτογραφία

Ιστορικά καταγόμενη από απλές εκδοχές κωδικοποίησης με μόνο στόχο την απόκρυψη στρατιωτικών ή ευαίσθητων γενικά πληροφοριών από μη εκλεπτυσμένους αντιπάλους, όπως ο Κώδικας του Καίσαρα, η κρυπτογραφία εξελίχτηκε [1] κατ' αντιστοιχία με την εξέλιξη της πληροφορικής και κατ' επέκταση της αποκρυπτογράφησης. Η διαχρονική ανάγκη για εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα και μη αποκήρυξη της πληροφορίας [2] τους βασικούς πυλώνες, δηλαδή, της ασφάλειας πληροφοριών, οδήγησε σταδιακά την κρυπτογραφία στην υιοθέτηση όλο και πολυπλοκότερων τεχνικών, που ενίοτε καθίστανται συμπληρωματικές. Με στόχο την ανταλλαγή μηνυμάτων, των οποίων το περιεχόμενο μπορεί να κατανοήσει μόνο ο παραλήπτης και ο αποστολέας (κρυπτολογία), γίνεται χρήση ενός προσυμφωνημένου μετασχηματισμού του μηνύματος (κρυπτογράφηση) με μία μέθοδο/μαθηματική συνάρτηση (κρυπτογραφικός αλγόριθμος), όπου το αρχικό κείμενο μετασχηματίζεται με τη χρήση ενός κλειδιού στο κωδικοποιημένο.

2.1.1 **Ασύμμετρη Κρυπτογραφία**

Η σύγχρονη κρυπτογραφία, αν και χρησιμοποιείται σε μία πλειάδα επιστημών, αποτελεί ουσιαστικά έναν τομέα έρευνας και εφαρμογής που συγκεράζει την μαθηματική με την επιστήμη των υπολογιστών. Στην παρούσα ανάλυση, δε, θα μας απασχολήσει το πλέον διαδεδομένο μέρος της, η χρήση ασύμμετρων κρυπτογραφικών συστημάτων.

Τα ασύμμετρα κρυπτογραφικά συστήματα, ονομάζονται και συστήματα δημόσιου κλειδιού. Η διαφορά τους είναι ότι, σε αντίθεση με τα συμμετρικά, χρησιμοποιείται ένα ζευγάρι κλειδιών, εκ των οποίων το ένα (δημόσιο) κωδικοποιεί το μήνυμα προς παραλαβή, ενώ το δεύτερο (ιδιωτικό) το αποκωδικοποιεί. Η διαδικασία δύναται να είναι και αντίστροφη ή ακόμα και να υπάρχει σύνδεση των δύο κλειδιών. Στην εικόνα που ακολουθεί παρουσιάζεται συνοπτικά η κρυπτογράφηση δημοσίου κλειδιού.



Εικόνα 1: Κρυπτογράφηση Δημοσίου Κλειδιού

Με βασική προϋπόθεση, σε κάθε περίπτωση, ότι το ιδιωτικό κλειδί παραμένει ιδιωτικό και άρα δεν υποκλέπτεται, είναι κοινή παραδοχή, αν και όχι αποδεδειγμένο μαθηματικά [3], ότι η αντιστροφή των συναρτήσεων δημιουργίας των κλειδιών στα πλέον σύγχρονα κρυπτογραφικά

συστήματα είναι αδύνατη πλην περιπτώσεων όπου απαιτείται κάποια ειδική είσοδος, η οποία καθίσταται γνωστή στον επιτιθέμενο.

Οι μαθηματικές συναρτήσεις που χρησιμοποιούνται ως βάση, ονομάζονται μίας κατεύθυνσης (trapdoor functions). Η πολυπλοκότητα τους (εκθετική ή πολυωνυμική) καθώς και η εκάστοτε είσοδος τις καθιστά λιγότερο ή περισσότερο προβλέψιμες και αντιστρεφόμενες, αναλόγως φυσικά και των τεχνολογικών πόρων που διατίθενται ή εξελίσσονται προς τούτο. Μία βασική, για την παρούσα ανάλυση, χρήση των παραπάνω είναι η κατασκευή ψηφιακών υπογραφών.

2.1.2 **Ψηφιακές Υπογραφές**

Οι ψηφιακές υπογραφές είναι τεχνικές για αυθεντικοποίηση των επικοινωνούντων μερών με σκοπό την επαλήθευση της πηγής της προέλευσης δεδομένων, την ακεραιότητα τους και την παροχή δυνατότητας μη αμφισβήτησης τόσο της αποστολής ή λήψης μηνυμάτων όσο και της δημιουργίας ή τροποποίησης τους [4]. Όπως αναφέρει και ο Menezes, *«μία από τις πιο σημαντικές εφαρμογές των ψηφιακών υπογραφών είναι η πιστοποίηση των δημοσίων κλειδιών σε μεγάλα δίκτυα».*

Εννοιολογικά, η ψηφιακή υπογραφή είναι ένα αλφαριθμητικό που συσχετίζει ένα (ψηφιακό) μήνυμα με την πηγή του και η οποία προκύπτει από έναν αλγόριθμο, ο οποίος ενίοτε συμπεριλαμβάνει το ίδιο το μήνυμα. Ο ανωτέρω αλγόριθμος, συνεργαζόμενος με έναν άλλο, επαλήθευσης της αυθεντικότητας της υπογραφής, συνθέτουν έναν μηχανισμό ψηφιακής ταυτότητας, ο οποίος εν συνεχεία, συνδυάζεται με μία μέθοδο μετασχηματισμού των δεδομένων του μηνύματος σε μορφή υπογράψιμη για να ολοκληρωθεί μία διαδικασία ψηφιακής υπογραφής.

Πιο αναλυτικά, η διαδικασία εκκινεί από τη δημιουργία ενός ζεύγους κλειδιών, του υπογράφοντος (αντίστοιχο του ιδιωτικού) και του επαληθεύοντος (αντίστοιχο του δημόσιου). Το μήνυμα μετασχηματίζεται σε μορφή υπογράψιμη, συνδυάζεται με το ιδιωτικό κλειδί και με χρήση του αλγορίθμου υπογραφής, παράγει την υπογραφή του μηνύματος. Ο αποδέκτης επαληθεύει το μήνυμα αναλύοντας το ίδιο, την υπογραφή και το ‘δημόσιο’ κλειδί [2]. Αυτονόητα με τα παραπάνω, δεν πρέπει να είναι δυνατό να υπολογιστεί η υπογραφή́ ενός μηνύματος μόνο από το κλειδί επαλήθευσης, να υφίστανται δύο μηνύματα με την ιδία υπογραφή́ και να εξάγεται ή να εκτιμάται το κλειδί υπογραφής από τα υπογεγραμμένα μηνύματα.

Η επικρατούσα επιλογή στην πλειοψηφία των υπαρχόντων blockchains για τη εξαγωγή του δημόσιου κλειδιού από το ιδιωτικό είναι ο Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικής Καμπύλης, ECDSA. Προέρχεται από τη σύγκλιση των μαθηματικών τομέων των πεπερασμένων πεδίων και των ελλειπτικών καμπυλών και χρησιμοποιεί το ιδιωτικό κλειδί των 256 ψηφίων που μπορεί να δημιουργηθεί χειροκίνητα, τυχαία ή με κάποιο αλγόριθμο, για να εξάγει το αντίστοιχο δημόσιο.

Στην περίπτωση του bitcoin, εκτιμάται ότι απαιτούνται τρισεκατομμύρια υπολογιστές που να εκτελούν συνεχόμενες προσπάθειες τυχαίας επιλογής ιδιωτικών κλειδιών για τρισεκατομμύρια χρόνια για να βρουν από ποιο μυστικό κλειδί εξάγεται ένα γνωστό δημόσιο κλειδί [3]. Σαν

υποσημείωση, αξίζει να αναφερθεί ότι ένα ψηφιακό νόμισμα είναι ουσιαστικά μία αλυσίδα ψηφιακών υπογραφών.

2.1.3 **Κατακερματισμός (Hashing)**

Εμβαθύνοντας στα συστατικά στοιχεία, μία συνάρτηση κατακερματισμού είναι ένας μαθηματικός αλγόριθμος που έχοντας ως είσοδο μία αυθαίρετου μεγέθους ομάδα δεδομένων, παράγει ως έξοδο μία καθορισμένου μεγέθους στοιχειοσειρά (string), σχεδιασμένη επιπλέον να είναι μονόδρομη, ήτοι αδύνατο να αντιστραφεί. *'Μία συνάρτηση κατακερματισμού H δέχεται ένα μπλοκ μεταβλητού μήκους δεδομένων M ως είσοδο και παράγει μια τιμή κατακερματισμού σταθερού μεγέθους h = H (M), που ονομάζεται σύνοψη (digest) ή κατακερματισμός (hash)'* [7].

Η ποιότητα των ανωτέρω συναρτήσεων καθορίζεται από το αν τα αποτελέσματα εφαρμογής τους είναι τυχαία και ομοιόμορφα κατανεμημένα για ένα επαρκές σύνολο εισόδων. Η ασφάλεια έγκειται στο χαρακτηριστικό η μικρότερη δυνατή αλλαγή των δεδομένων εισόδου (ένα bit), να οδηγεί σε μεγάλη διαφοροποίηση της παραχθείσας σύνοψης. Επιπλέον, μία ομάδα τέτοιων αλγορίθμων με συγκεκριμένες, όμως, ιδιότητες που τις καθιστούν ασφαλείς, συγκροτούν τις κρυπτογραφικές συναρτήσεις κατακερματισμού. Οι ιδιότητες αυτές είναι:

- Είναι προσδιοριστικοί. Η ίδια είσοδος πάντα εξάγει την ίδια σύνοψη.
- Είναι αποδοτικοί. Για κάθε είσοδο, η σύνοψη εξάγεται γρήγορα.
- Είναι μονόδρομοι. Είναι ανέφικτο να υπολογιστεί η είσοδος από τη σύνοψη.
- Είναι συγκρουσιακά ανθεκτικοί. Δύο διαφορετικές είσοδοι δεν μπορούν να εξάγουν ίδια σύνοψη.
- Είναι ασυνεχείς. Μία μικρή αλλαγή επιφέρει τελείως διαφορετική σύνοψη.

Η πρώτη ιδιότητα (προσδιοριστικοί) αφορά στην εμφάνιση του ίδιου αποτελέσματος, όσες φορές και αν εισάγεις τα ίδια δεδομένα στην ίδια συνάρτηση. Η ύπαρξη της εξασφαλίζει τη δυνατότητα να ανατρέξεις στα δεδομένα εισόδου, κάτι που θα ήταν ανέφικτο αν κάθε φορά άλλαζε η σύνοψη. Η δεύτερη ιδιότητα (αποδοτικοί) αφορά στην ταχύτητα υπολογισμού της σύνοψης από τα εκάστοτε σύγχρονα μέσα ώστε να μην αποτελεί τροχοπέδη η χρήση τους σε πραγματικό χρόνο, δεδομένου φυσικά της ενίοτε καθορισθείσας δυσκολίας.

Η τρίτη ιδιότητα (μονόδρομοι) επισημαίνει το ακατόρθωτο του αντίστροφου υπολογισμού των δεδομένων εισόδου από τη σύνοψη. Η χρήση του επιθέτου, αντί του 'αδύνατου' γίνεται λόγω της θεωρητικής δυνατότητας εύρεσης των δεδομένων εισόδου με χρήση μεθόδων 'ωμής δύναμης' (brute force attacks). Ωστόσο αποδεικνύεται ότι, προς το παρόν και για τις σύγχρονες συναρτήσεις, απαιτείται υπέρμετρος χρόνος και πόροι, τόσο που η προσπάθεια καθίσταται άνευ νοήματος.

Η τέταρτη ιδιότητα (συγκρουσιακά ανθεκτικοί) καθορίζει την, κατά μεγάλη πλειοψηφία, μη πιθανότητα ταύτισης δύο συνόψεων που εξάγονται από διαφορετικά δεδομένα εισόδου. Για τον καθορισμό της πιθανότητας αυτής, σε συνάρτηση με το μήκος της σύνοψης, θα πρέπει να λαμβάνεται υπόψη και το λεγόμενο 'παράδοξο των γενεθλίων'. Τις επιπλοκές αυτού στον

κατακερματισμό καθώς και τις αδυναμίες έναντι επιθέσεων που το εκμεταλλεύονται αναλύονται επαρκώς στο έργο των A. Narayanan, J. Bonneau και E. Felten[8].

Η πέμπτη και πιο απλή ιδιότητα (ασυνεχείς) υπογραμμίζει ότι η παραμικρή αλλαγή των δεδομένων εισόδου, έστω κατά ένα bit, οδηγεί σε τελείως διαφορετική σύνοψη. Στα ανωτέρω θα προσθέσουμε και μία έκτη και ενδιαφέρουσα ιδιότητα με μεγάλη επίδραση στην τεχνολογία blockchain και τα κρυπτονομίσματα.

Αξίζει να σημειωθεί ότι πλέον, οι γλώσσες προγραμματισμού́ (ενδεικτικά C++, Java, Python, Javascript κ.α.) χρησιμοποιούν βιβλιοθήκες με έτοιμες προς χρήση συναρτήσεις κατακερματισμού́, καθιστώντας εύκολη τη χρήση τους χωρίς την ανάγκη κατανόησης τους. Παράδειγμα σύγχρονων συναρτήσεων αποτελούν οι:

- MD 5: Παράγει σύνοψη 128-bit ενώ η ανθεκτικότητα της σπάει μετά από περίπου 2^{21} κατακερματισμούς.
- SHA 120: Παράγει σύνοψη 160-bit ενώ η ανθεκτικότητα της σπάει μετά από περίπου 2^{61} κατακερματισμούς.
- SHA 25620: Παράγει σύνοψη 256-bit και χρησιμοποιείται στο Bitcoin.
- Keccak-256: Παράγει σύνοψη 256-bit και χρησιμοποιείται στο Ethereum.

Για παράδειγμα, στο Hashcash του A. Back, ο αποστολέας ενός email πρέπει να παράγει μία επικεφαλίδα της οποίας η σύνοψη με χρήση της συνάρτησης SHA-1 έχει τιμή που ξεκινά με είκοσι μηδενικά. Κατά μέσο όρο, απαιτούνται 219 προσπάθειες για εύρεση μίας τέτοιας έγκυρης επικεφαλίδας.

Επεκτείνοντας αυτή την προσέγγιση, ο ‘Nakamoto’, συνοπτικά, στην περίπτωση του bitcoin εφηύρε την εξόρυξη (mining) ως προσπάθεια εύρεσης ενός τυχαίου αριθμού (nonce) με τον οποίο ο κατακερματισμός κατά SHA-256 ενός block αποφέρει μία σύνοψη με τιμή μικρότερη μίας τεθείσας τιμής στόχου. Η εξόρυξη αποτελεί την επικύρωση της εγκυρότητας του block και αναλαμβάνεται από αφοσιωμένους σε αυτό, ή όχι, κόμβους, τους miners.

2.2 Το Block

Το block αποτελεί, αυτονόητα, το δομικό στοιχείο της αλυσίδας, μία ιδιότυπη μονάδα πληροφορίας. Η βασικότερη ιδιότητα ενός block είναι το μέγεθος της επικεφαλίδας του και του ιδίου ως σύνολο. Στην περίπτωση του bitcoin, η επικεφαλίδα αποτελείται από 80 bytes, ενώ το μέγεθος των block έχει εγγενές όριο το 1 MB[17]. Στην περίπτωση του ethereum, του δεύτερου πιο διαδεδομένου blockchain σήμερα, το μέγεθος της επικεφαλίδας είναι 508 bytes, το μέγεθος του εκάστοτε block διαχρονικά έλαβε τιμές από 575 bytes έως 34MB, ενώ σήμερα κυμαίνεται περί τα 20MB. Το μέγεθος της επικεφαλίδας αφορά ουσιαστικά στις διαδικασίες επικύρωσης που διέπουν το πρωτόκολλο, ενώ εκείνο του σώματος (body) του block, στη χωρητικότητα του για πληροφορία.

Τα μέσα που χρησιμοποιούνται για την επεξεργασία και κανονικοποίηση της πληροφορίας, θα εξεταστούν στη συνέχεια εκτενώς, δεδομένου ότι αφορούν στο πλαίσιο της επικεφαλίδας του block. Η ουσία είναι ότι τη στιγμή κατά την οποία η ύπαρξη τους κατοχυρώθηκε με την εισαγωγή τους στο block, είναι εξαιρετικά δύσκολο έως αδύνατο να αλλάξουν, να διαγραφούν ή έστω να αμφισβητηθούν με κάποιο τρόπο. Αυτά είναι ένα σύνολο μηνυμάτων / συναλλαγών που αποτελούν τις εγγραφές της διευρυμένης αυτής βάσης δεδομένων, αναφερόμενες σε συναλλαγές άυλων (κρυπτονομίσματα) και υλικών αγαθών (τίτλοι), σε ψηφιακά πιστοποιητικά, σε έξυπνα συμβόλαια και λοιπά. Ένα ακόμη παράδειγμα αποτελεί η αποθήκευση επικυρωμένων ψηφιακών αντιγράφων πτυχίων φοιτητών, υπηρεσία που παρουσιάστηκε τόσο από το Πανεπιστήμιο Λευκωσίας, όσο και από το MIT. Είναι προφανές ότι οι πιθανές χρήσεις εξαντλώνται στο όριο του μεγέθους του block κάθε εφαρμογής Blockchain [4].

2.2.1 **Συναλλαγές (transactions)**

Μία συναλλαγή (transaction) είναι, κατ' ουσία, ένα μήνυμα που περιέχει το δημόσιο κλειδί του παραλήπτη επισυναπτόμενο στο ποσό που μεταφέρεται και υπογεγραμμένο από το ιδιωτικό κλειδί του αποστολέα. Το σύνολο των συναλλαγών (ή άλλου τύπου δεδομένων εάν δεν αφορά σε κρυπτονόμισμα η εφαρμογή Blockchain), δημιουργούν τα blocks που σχηματίζουν το blockchain.

Οι εγγραφές αυτές αφορούν συναλλαγές αγαθών, έξυπνων συμβολαίων και ψηφιακών πιστοποιητικών. Τα αγαθά́ μπορεί́ να είναι οικονομικές αξίες, όπως στην περίπτωση των κρυπτονομισμάτων ή τίτλοι ιδιοκτησίας υλικών αγαθών. Αυτά́ τα δεδομένα μετασχηματίζονται κρυπτογραφικά σε ένα δένδρο Merkle, του οποίου η ρίζα καταχωρείται στην επικεφαλίδα και το οποίο θα αναλύσουμε στη συνέχεια. Επιγραμματικά, η εντολή εκτέλεσης μίας συναλλαγής εκκινεί την εξής διαδικασία [5]:

- Ένας αριθμός συναλλαγών συσσωρεύεται στη δομή που ονομάζουμε block.
- Οι miners αναλαμβάνουν να επικυρώσουν την νομιμότητα των συναλλαγών.
- Η επικύρωση έρχεται μέσα από την επίλυση ενός μαθηματικού γρίφου με το όνομα.
- Ο πρώτος miner που επιλύει το γρίφο κάθε block, δέχεται μία ανταμοιβή.
- Τα επικυρωμένα block εισάγονται άμεσα στο blockchain.

2.2.2 **Έξυπνα συμβόλαια (smart contracts)**

Ο Nick Szabo [6], εισήγαγε στην πληροφορική τα έξυπνα συμβόλαια ως «ένα μηχανογραφημένο πρωτόκολλο συναλλαγής που εκτελεί τους όρους μιας σύμβασης». Σκοπός του ήταν η μεταφορά συμβάσεων σε κώδικα ώστε να αποφεύγονται πιθανές εξαιρέσεις από τις επιταγές των ρητρών (κακόβουλες ή μη) και να ελαχιστοποιείται η απαίτηση διαμεσολάβησης έμπιστου τρίτου μέρους. Σήμερα, αποτελούν ένα είδος συναλλαγής εντός κάποιων blockchains.

Η κωδικοποίηση αυτή, στο πλαίσιο των blockchains, επιτυγχάνεται με τη μορφή αυτόνομων δεσμών ενεργειών που τοποθετούνται εντός της αλυσίδας και εκτελούν περίπλοκες διεργασίες υπό συγκεκριμένους όρους. Συνήθως, αντιμετωπίζονται ως ανεξάρτητες οντότητες με ξεχωριστή διεύθυνση και ιδίους πόρους. Ενεργοποιούνται με τη λήψη συναλλαγών στη διεύθυνση τους και

εφόσον οι τεθέντες, κατά τη δημιουργία τους, όροι ικανοποιούνται από τα επισυναπτόμενα στην συναλλαγή δεδομένα. Έχουν, δε, ιδιαίτερα και σημαντικά χαρακτηριστικά[7]:

- Αυτονομία: Εκτελούνται σε κάθε περίπτωση που τα κριτήρια τους καλύπτονται και με δεδομένη την ακεραιότητα καθώς το δίκτυο στο οποίο εδρεύουν δεν έχει κεντρικό σημείο ελέγχου.
- Αιτιοκρατία: Κάθε εκτέλεση τους οδηγεί στο ίδιο αποτέλεσμα με τα δίκτυα να καθιστούν αδύνατη την αποθήκευση κώδικα με μη αιτιοκρατικές ιδιότητες.
- Διαφάνεια: Οποιοσδήποτε μπορεί να ελέγξει με απλό τρόπο τον κώδικα καθώς και το αποτέλεσμα τους χωρίς να τα ενεργοποιήσεις.
- Ευελιξία: Η εφαρμογή τους δεν περιορίζεται στο blockchain που εδρεύουν, καθώς δύναται να εκτελεστούν με έξωθεν εντολή αλλά και να παράξουν αποτέλεσμα σε άλλο blockchain.

2.2.3 **Χρονοσφραγίδα (timestamp)**

Αν και το Blockchain δεν θα μπορούσε να υπάρξει χωρίς την παράλληλη χρήση όλων των αναφερόμενων σε αυτό το κεφάλαιο εφευρέσεων, μία εξ αυτών και ίσως η πιο απλή, εισήχθη ως ένα πεδίο τεσσάρων μόνο bytes στο block, με μερικές πολύ ενδιαφέρουσες ιδιότητες. Η χρονοσφραγίδα Unix 'Epoch' (Εποχή) ήταν η πρώτη που χρησιμοποιήθηκε και βασίζεται στον αριθμό δευτερολέπτων που έχουν παρέλθει από τα μεσάνυχτα της 1ης Ιανουαρίου 1970 [8].

Κάθε block λοιπόν, περιέχει και μία μοναδική χρονοσφραγίδα της στιγμής που δημιουργείται, η οποία αφενός πιστοποιεί το χρόνο, αφετέρου δε, επιδρά στον κατακερματισμό του block καθώς συμμετέχει σε αυτόν. Άλλωστε, ήδη έχουμε εξετάσει το ότι ακόμα και ένα bit να αλλάζει στα προς κατακερματισμό δεδομένα, αλλάζει άρδην η σύνοψη. Τη στιγμή που πραγματοποιείται σύνδεση μεταξύ δύο κόμβων, λαμβάνουν ο ένας από τον άλλο μία χρονοσφραγίδα σε UTC και αποθηκεύουν την απόκλιση της από την τοπική ώρα του κόμβου.

Η network-adjusted time αποτελεί το άθροισμα της τοπικής ώρας συν τον διάμεσο όλων των αποκλίσεων των χρονοσφραγίδων που αποστέλλονται στον κόμβο από τους υπόλοιπους κόμβους, ο οποίος ωστόσο δεν υπερβαίνει τα 70 λεπτά. Μία χρονοσφραγίδα λοιπόν, είναι έγκυρη εφόσον υπερβαίνει σαν τιμή τον διάμεσο (median) των προηγούμενων έντεκα blocks και είναι μικρότερη από τον χρόνο δικτυακής προσαρμογής προσαυξημένο κατά δύο ώρες. Αποτέλεσμα αυτού να μην υπάρχει ακρίβεια ως προς τον απόλυτο χρόνο, αλλά και να μην τηρείται απόλυτη χρονολογική σειρά ως προς τις χρονοσφραγίδες των block. Η ακρίβεια περιορίζεται σε εύρος μίας ή δύο ωρών. Τέλος, αναλόγως του τύπου δεδομένων που χρησιμοποιείται για την απεικόνιση της χρονοσφραγίδας, τίθενται περιορισμοί. Για παράδειγμα, στα συστήματα που χρησιμοποιούνται signed integers, τα 4 bytes εξαντλούνται το 2038 [9].

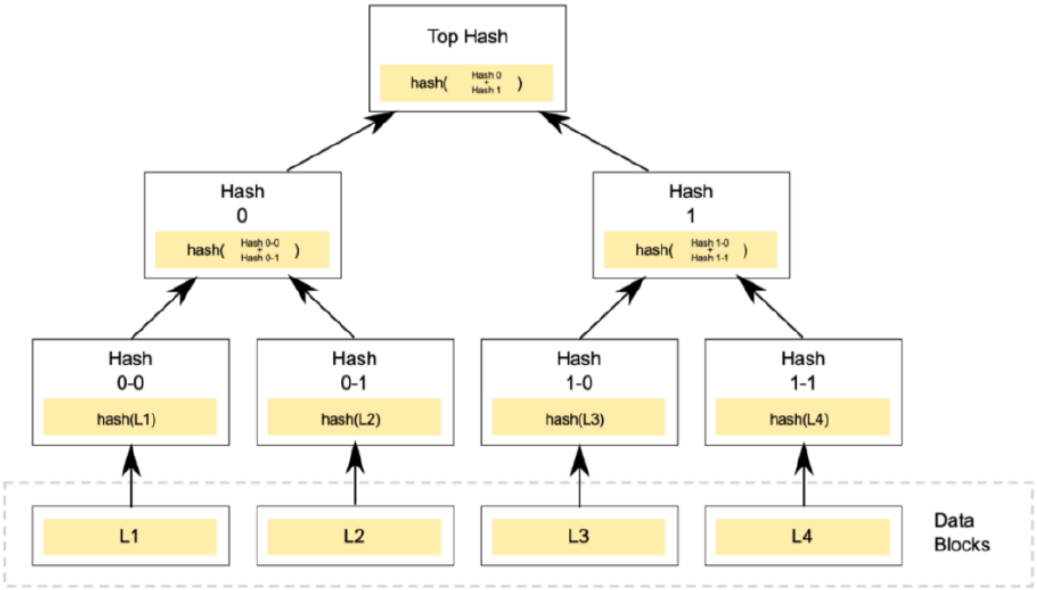
2.3 Δέντρα Merkle

Τα δέντρα Merkle (ή δέντρα κατακερματισμού) είναι δυαδικά δέντρα τα οποία ονομάστηκαν έτσι προς τιμήν του επιστήμονα που τα πρότεινε [10] με σκοπό την ανάπτυξη μίας νέας μεθόδου

ψηφιακής υπογραφής βασιζόμενης σε συμβατικές συναρτήσεις κρυπτογράφησης. Η ιδιότητα τους είναι ότι κάθε κόμβος-φύλλο (leaf node) περιέχει μία σύνοψη δεδομένων, κάθε κόμβος-πατέρας (non-leaf node) περιέχει το αποτέλεσμα κρυπτογραφικού κατακερματισμού των περιεχομένων των κόμβων-παιδιών. Η ανωτέρω μεθόδευση κατακερματισμού, έχει ως αποτέλεσμα τη ρίζα του δέντρου (Merkle root) η οποία περιέχει μία σύνοψη όλων των δεδομένων του δέντρου, σχηματιζόμενη από συνεχείς κατακερματισμούς. Με τον τρόπο αυτό, είναι εφικτή η ασφαλής και εύκολη επαλήθευση της αυθεντικότητας και ακεραιότητας δεδομένων χωρίς να απαιτείται η αποστολή, κατοχή και έλεγχος όλου του δέντρου. Εφόσον η ρίζα είναι διαθέσιμη, οποιοσδήποτε μπορεί να επαληθεύσει τα δεδομένα κάθε κόμβου με υπολογισμό ενός αριθμού κατακερματισμών ανάλογου με τον λογάριθμο του αριθμού κόμβων φύλλων του δέντρου, ακολουθώντας την αντίστοιχη διαδρομή κατακερματισμού (Merkle branch).

Έτσι, το σύνολο των συναλλαγών δημιουργεί τα blocks που σχηματίζουν το blockchain. Έχουμε, λοιπόν, έναν αριθμό συναλλαγών που περιλαμβάνονται σε ένα block, η καθεμία από τις οποίες κατακερματίζεται σε μία σύνοψη (Transaction ID) και οι οποίες σχηματίζουν ζεύγη που αποτελούν τα φύλλα του δέντρου (leaf nodes). Για κάθε ζευγάρι δημιουργείται ένας ‘πατέρας’ με δύο δείκτες κατακερματισμού που δείχνουν σε κάθε συναλλαγή.

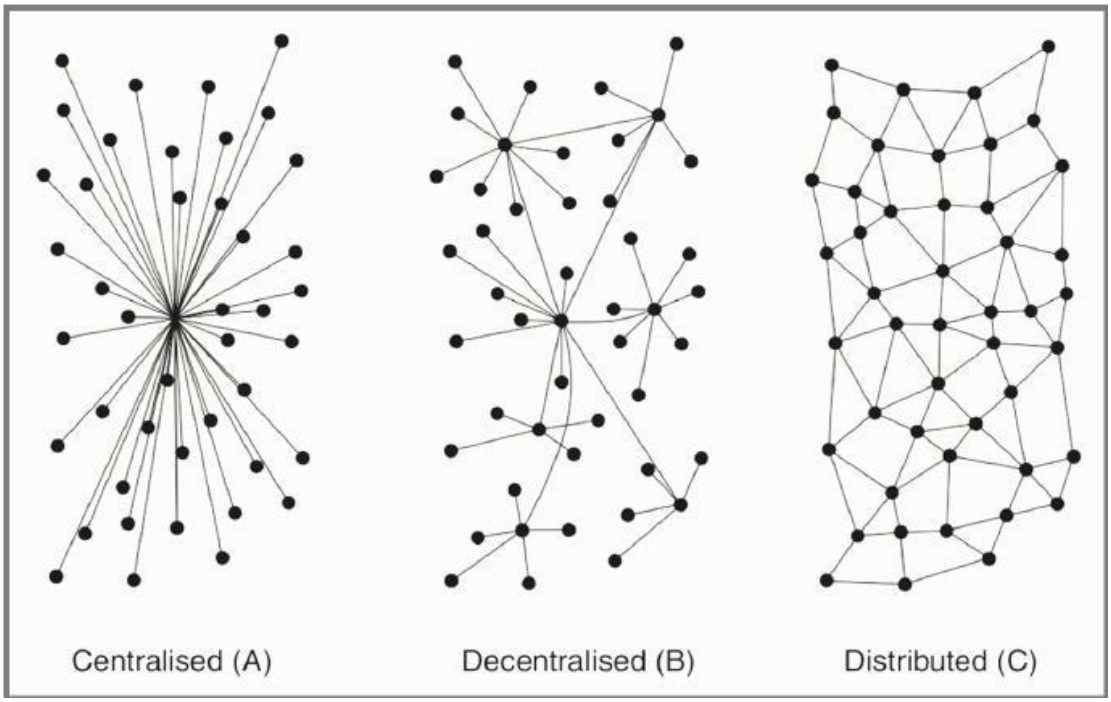
Αυτοί οι κόμβοι/πατέρες σχηματίζουν το επόμενο επίπεδο του δέντρου και η ζευγοποίηση και κατακερματισμός συνεχίζεται μέχρι την εμφάνιση ενός και μοναδικού κόμβου (Merkle Root). Δεδομένου ότι κάθε block περιέχει εκατοντάδες συναλλαγές, αλλά μία και μόνο ρίζα Merkle, θα ήταν εξαιρετικά αναποτελεσματικό να αποθηκεύονται όλα τα δεδομένα τους, έστω και κατακερματισμένα. Η εύρεση μίας συγκεκριμένης συναλλαγής μέσα σε ένα block, θα απαιτούσε υπέρμετρο χρόνο. Με τα Δέντρα Merkle, ο χρόνος αυτός μειώνεται δραστικά δεδομένου ότι απαιτείται συνήθως να επιβεβαιωθεί η ύπαρξη της συναλλαγής στο block.



Εικόνα 2: Ένα τυπικό δέντρο Merkle

2.4 Αρχιτεκτονική Δικτύου

Το σύνολο της επικοινωνίας μεταξύ των κόμβων που συμμετέχουν σε ένα blockchain διενεργείται, αυτονόητα, μέσω ενός δικτύου. Αν και μπορούμε να σχεδιάσουμε μία πληθώρα δικτύων, τα κύρια είδη, όσον αφορά την αρχιτεκτονική ελέγχου και λήψης αποφάσεων, είναι δύο, τα κεντρικοποιημένα (centralized) και τα κατανεμημένα (distributed). Η βασική διαφορά είναι ο τρόπος που λαμβάνεται η κάθε απόφαση και πώς διαμοιράζεται η πληροφορία στους κόμβους [11]. Αν και στην πράξη, συνήθως γίνεται χρήση μικτών αρχιτεκτονικών, είναι εποικοδομητικό να γίνει μια επιγραμματική αναφορά στις ιδιαιτερότητες των δικτύων και μέσα από αυτήν να επιδειχθεί και η χρησιμοποιούμενη τεχνική στα δίκτυα Blockchain.



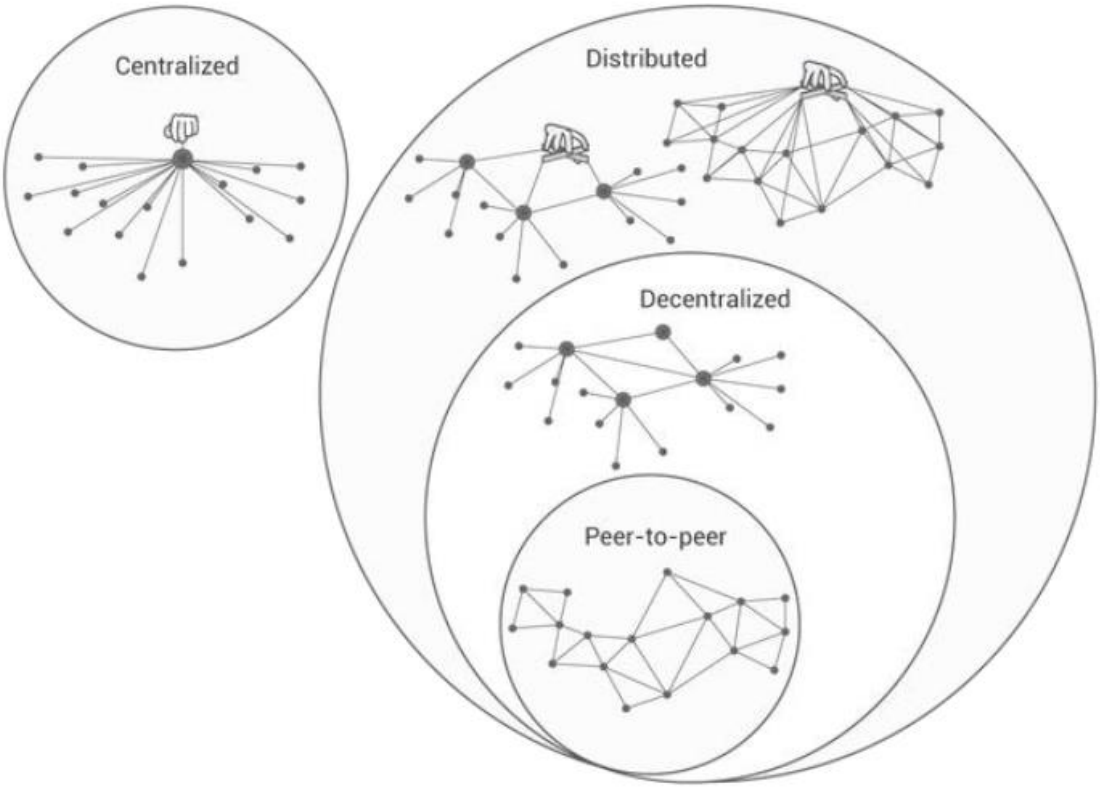
Εικόνα 3: Τα τρία βασικά είδη δικτύων

2.4.1 **Κεντρικοποιημένα και κατανεμημένα συστήματα**

Στα συστήματα αυτά, υφίσταται έλεγχος όλων των στοιχείων από μία κεντρική οντότητα με εμφανείς αδυναμίες και προτερήματα και κυριότερο αυτών ότι είναι ευάλωτα καθώς η καταστροφή του κεντρικού κόμβου συνεπάγεται την απώλεια επικοινωνίας σε όλο το δίκτυο. Το μοντέλο αυτό διαθέτει κεντρικά, σε ένα σημείο, το σύνολο τυχόν αναγκαίων δικτυακών πόρων.

Τα προτερήματα της αρχιτεκτονικής, συνοψίζονται στην ευκολότερη και καλύτερη πρόσβαση των διαχειριστών στα συστήματα και στην καλύτερη δικτυακή και φυσική ασφάλεια. Η βασική αδυναμία είναι, ως άνω, η αποτυχία του κεντρικού διακομιστή και σε όρους εργασίας, ο αυξημένος φόρτος του διαχειριστή. Αντιθέτως, η κατανομή στα κατανεμημένα συστήματα σημαίνει ότι δεν υπάρχει αντίστοιχο κεντρικό σημείο λήψης αποφάσεων για το δίκτυο. Κάθε

κόμβος συμμετέχει στο δίκτυο και το σύνολο των αποφάσεων και συμπεριφορών καθορίζουν την συμπεριφορική δομή του συστήματος στο σύνολο του.



Εικόνα 4: Αποκέντρωση και P2P δίκτυα

2.4.2 **Αποκεντρωμένα συστήματα**

Τα αποκεντρωμένα συστήματα αποτελούν ουσιαστικά μία υποκατηγορία των κατανεμημένων με τη διαφορά ότι ο έλεγχος εκτελείται από διαφορετικά στοιχεία και επιπλέον η εμπιστοσύνη δεν είναι διάχυτη αλλά υπάρχουν κεντρικοί κόμβοι επικοινωνίας ανά ομάδες.

Συνοπτικά, οι διαφορές των τριών αρχιτεκτονικών έχουν ως εξής [12]:

- Συντήρηση: Τα αποκεντρωμένα συστήματα είναι τα πλέον δύσκολα στη συντήρηση σε αντίθεση με τα ευκολότερα αλλά και πιο ευάλωτα κεντρικοποιημένα, δεδομένου του μοναδικού κέντρου βάρους. Τα κατανεμημένα απαιτούν ελαφρώς δυσκολότερη συντήρηση αλλά είναι και λιγότερο ευάλωτα λόγω των πεπερασμένων κεντρικών σημείων.
- Σταθερότητα: Τα αποκεντρωμένα συστήματα είναι εξαιρετικά σταθερά και οποιαδήποτε απώλεια κόμβου δεν επιφέρει ουσιαστική δυσλειτουργία. Τα κεντρικοποιημένα συστήματα είναι τα πλέον ασταθή λόγω, πάλι, του μοναδικού κέντρου βάρους. Στα κατανεμημένα συστήματα, η απώλεια ενός κεντρικού κόμβου συνήθως θα οδηγήσει σε διάσπαση του ενός δικτύου σε περισσότερα αλλά με αμφιλεγόμενο αποτέλεσμα.

- Επεκτασιμότητα: Τα αποκεντρωμένα συστήματα δεν έχουν κανέναν περιορισμό σε αντίθεση με τις μικρές δυνατότητες των κεντρικοποιημένων. Ενδιάμεσες επιδόσεις έχουν τα κατανεμημένα συστήματα.
- Ευκολία: Τα μη κεντρικοποιημένα συστήματα έχουν προφανείς δυσκολίες επικοινωνίας λόγω των πολλαπλών 'ανεξάρτητων' σημείων, οι οποίες πρέπει να επιλύονται προ λειτουργίας του δικτύου.
- Εξελιξιμότητα: Τα κεντρικοποιημένα συστήματα, έχοντας ένα και μοναδικό πλαίσιο λειτουργίας εξελίσσονται δύσκολα σε αντίθεση με τα μη κεντρικοποιημένα, όπου η εξέλιξη είναι ραγδαία εφόσον έχουν τεθεί οι βασικές δομές επικοινωνίας.

2.4.3 **Ομότιμα δίκτυα (Peer-to-Peer networks)**

Το ομότιμο δίκτυο αποτελεί ένα αποκεντρωμένο κατανεμημένο δίκτυο χωρίς οιαδήποτε κεντρική διεργασία. Το σύνολο των κόμβων σχηματίζουν ένα δίκτυο όπου μοιράζονται ισότιμα τις υποχρεώσεις και τους πόρους, προσφέροντας, κατά περίπτωση, το εύρος ζώνης τους, την επεξεργαστική ισχύ τους ή και τον αποθηκευτικό τους χώρο. Ο ρόλος του διακομιστή και του πελάτη εναλλάσσονται κατά το δοκούν και βάσει της εκάστοτε διεργασίας του δικτύου.

Για την απρόσκοπτη επικοινωνία μεταξύ των κόμβων, ανεξάρτητα και πάνω από την τοπολογία του φυσικού δικτύου, χρησιμοποιείται ένα εικονικό δίκτυο επικάλυψης (overlay network). Βασικό χαρακτηριστικό αυτού είναι η ευρετηριοποίηση (indexing) κόμβων με αποτέλεσμα τα δεδομένα να ανταλλάσσονται μεν απευθείας μέσω του φυσικού δικτύου αλλά σε επίπεδο εφαρμογής η επικοινωνία αυτή να γίνεται μέσω των συνδέσεων επικάλυψης [13].

Η χρήση P2P δικτύων προκρίνεται στις περιπτώσεις που απαιτείται αποκέντρωση, ανεκτικότητα στις βλάβες και εύκολη επεκτασιμότητα. Η δε μέθοδος που χρησιμοποιείται για τη δημιουργία του overlay network και του ευρετηρίου καθώς και ο τρόπος εκχώρησης πόρων, κατατάσσουν τα P2P δίκτυα σε αδόμητα (unstructured), δομημένα (structured) ή υβριδικά. Η σύνδεση στα πρώτα γίνεται τυχαία, ενώ στα δεύτερα σχηματίζεται μία ειδική, για την περίσταση, τοπολογία και επιλέγεται το βέλτιστο (θεωρητικά) πρωτόκολλο λειτουργίας και διαμοιρασμού πληροφοριών. Το πλέον σύνηθες είναι κάποιου είδους υλοποίηση κατανεμημένου πίνακα κατακερματισμού (DHT).

2.5 Μηχανισμοί συναίνεσης (consensus)

Τα κατανεμημένα συστήματα πλέον των προαναφερόμενων προβλημάτων, αντιμετωπίζουν και μία ουσιαστική δυσκολία όσον αφορά την αξιοπιστία της πληροφορίας και κατ' επέκταση των ιδίων, υπό την απειλή ελαττωματικών διαδικασιών. Η ανάγκη επίτευξης συμφωνίας μεταξύ κόμβων, οι οποίοι ενίοτε ενεργούν ασύγχρονα μεταξύ τους, αναφέρεται ως 'Το Πρόβλημα της Συναίνεσης' και έχει προσελκύσει εντατική έρευνα η οποία έχει παράξει πληθώρα πρωτοκόλλων τα οποία, ωστόσο, απευθύνονταν ανέκαθεν σε κλειστά συστήματα. Τυπικά παραδείγματα που απαιτείται συναίνεση κυμαίνονται από την εκτέλεση ή μη μιας συναλλαγής, την εκλογή ενός ηγέτη (κόμβου) για μία διεργασία έως το συγχρονισμό ρολογιού. Το πρόβλημα ουσιαστικά ανάγεται στη λήψη κοινής (ομόφωνης) απόφασης επί μίας δυαδικής τιμής.

Στην περίπτωση ασύγχρονης επικοινωνίας, έχει αποδειχτεί ότι υφίστανται περιπτώσεις μη λύσης έστω και λόγω μίας μοναδικής διαδικασίας [14]. Στα συγχρονισμένα συστήματα, όπως το Blockchain, το πρόβλημα, γνωστό και ως Πρόβλημα Βυζαντινών Στρατηγών BGP έχει αντιμετωπιστεί με διάφορες επιτυχείς μεθόδους [15], [16].

Προκειμένου να επιτευχθεί η απαραίτητη αξιοπιστία, τα πρωτόκολλα οφείλουν να διαθέτουν εγγενή ανθεκτικότητα σε βλάβες. Διαδικαστικά, οι εναλλακτικές τιμές διαμοιράζονται από τους κόμβους στο δίκτυο και εκτελείται κάποιου είδους αλληλεπίδραση ώστε να επιλεγεί η τελική κατάσταση. Συνήθως, ένα πρωτόκολλο συναίνεσης προϋποθέτει μία οριακή πλειοψηφία συμφωνίας σε μία εκ των προτεινόμενων τιμών και επιπλέον για να είναι επαρκές, πρέπει να πληροί μια σειρά απαιτήσεων:

• Τερματισμός: Κάθε μη ελαττωματική διαδικασία εξάγει μία τιμή V.

• Εγκυρότητα: Εάν το σύνολο των διαδικασιών εξάγει την ίδια τιμή V, συνεπάγεται ότι όλες οι μη ελαττωματικές διαδικασίες εξήγαγαν την τιμή V.

• Ακεραιότητα: Κάθε μη ελαττωματική διαδικασία εξάγει μία μοναδική τιμή, έτσι ώστε αν εξαχθεί η τιμή́ V, τότε εξυπακούεται ότι η V έχει προταθεί́ από́ κάποια διαδικασία.

• Συμφωνία: Κάθε μη ελαττωματική διαδικασία πρέπει να εξάγει την ίδια τιμή.

Επιπλέον, οι βασικές ιδιότητες των διαφόρων πρωτοκόλλων συναίνεσης είναι ο χρόνος και η πολυπλοκότητα των μηνυμάτων. Ο χρόνος αφορά, συνήθως, στο πλήθος των απαιτούμενων γύρων ανταλλαγής μηνυμάτων σε συνάρτηση με το πλήθος των διαδικασιών και το μέγεθος του τομέα εισόδου, ενώ η πολυπλοκότητα αναφέρεται στην ποσότητα των κυκλοφορούμενων μηνυμάτων. Το μέγεθος των μηνυμάτων και η απαίτηση χρήσης κάθε τύπου μνήμης αποτελούν, ομοίως, χαρακτηριστικά πρωτοκόλλων.

2.5.1 **Περί συναίνεσης**

Η απαίτηση ύπαρξης συναίνεσης στα κατανεμημένα συστήματα πηγάζει από την επιτακτικότητα της αντοχής τους έναντι της πιθανής αποτυχίας κόμβων που τηρούν αντίγραφα της κοινής βάσης δεδομένων. Τα πρωτόκολλα που έχουν αναπτυχθεί κατηγοριοποιούνται είτε βάσει της συμπεριφοράς τους έναντι των προβλεπόμενων αποτυχιών, είτε βάσει του τρόπου επικοινωνίας μεταξύ των κόμβων.

Βάσει συμπεριφοράς, μιλάμε για αντοχή σε συντριπτικές αποτυχίες (crash failures) ή βυζαντινές (byzantine) αποτυχίες. Στην πρώτη περίπτωση, οι κόμβοι λανθάνουν μη δυνάμενοι να επεξεργαστούν, αποστείλουν ή λάβουν μηνύματα. Στη δεύτερη περίπτωση, οι κόμβοι λαμβάνουν αυθαίρετες αποφάσεις όπως η αποστολή μηνυμάτων αντίθετων στο πρωτόκολλο συναίνεσης. Βάσει επικοινωνίας, τα δίκτυα όπου εφαρμόζεται το πρωτόκολλο, χωρίζονται σε σύγχρονα (synchronous), ασύγχρονα (asynchronous) ή εν μέρει ασύγχρονα. Η διαφορά μεταξύ σύγχρονων

και ασύγχρονων αφορά στην καθυστέρηση διαλογής των μηνυμάτων, με τα πρώτα να επιβάλλουν συσχετισμό με τον απόλυτο χρόνο.

2.5.2 **Το πρόβλημα των Βυζαντινών Στρατηγών (Byzantine Generals Problem)**

Οι Lamport, Shostak, & Pease [17] εισήγαγαν το Πρόβλημα των Βυζαντινών Στρατηγών ως ένα πρόβλημα συναίνεσης που εξετάζει την αξιοπιστία των συμμετεχόντων (κόμβων) στο δίκτυο. Η λογική του περιγράφει μία ομάδα Στρατηγών με αντίστοιχα στρατιωτικά τμήματα περιβάλλοντα μία εχθρική χώρα, οι οποίοι προσπαθούν να συμφωνήσουν μέσω αγγελιοφόρων στην βέλτιστη στρατηγική, πλην όμως κινούνται εν μέρει και από ιδιοτελή κίνητρα. Σύμφωνα με τους ανωτέρω, το σημείο καμπής είναι όταν το ένα τρίτο του συνόλου υπερβαίνει αριθμητικά το πλήθος των Στρατηγών που προωθούν ιδιοτελή κίνητρα.

Εφόσον επιτυγχάνεται τέτοια αναλογία, υπάρχει λύση στο πρόβλημα και άρα μπορεί να σχηματισθεί συναίνεση ως προς την απόφαση. Το πρόβλημα προφανώς ισχύει και στο blockchain που αποτελεί ένα κατανεμημένο δίκτυο και δεν υφίσταται κεντρικός κόμβος λήψης απόφασης. Ένας από τους πλέον γνωστούς αλγόριθμους που έχει προταθεί για την επίλυση του είναι ο PBFT [18]. Περιλαμβάνει ένα πρωτόκολλο τριών φάσεων και εισάγει την έννοια του κόμβου-ηγέτη ο οποίος μπορεί να αντικατασταθεί εφόσον επιδείξει συντριπτική ή βυζαντινή αποτυχία. Προϋπόθεσή του είναι ότι πλέον των δύο τρίτων (2/3) των κόμβων είναι μη ελλαττωματικοί. Το πρωτόκολλο αναφέρεται καθώς έχει χρησιμοποιηθεί εκτεταμένα σε αδειοδοτούμενα blockchains.

2.5.3 **Χρήση Πρωτοκόλλων**

Αν και οι διαφορές μεταξύ ανοικτών (permissionless) και αδειοδοτούμενων (permissioned) blockchains θα αναλυθούν στη συνέχεια, είναι ο τύπος αυτός σε συνδυασμό με τις αντιστάσεις που θέτει ο χειριστής ,τα στοιχεία που καθορίζουν το ποιο πρωτόκολλο θα χρησιμοποιηθεί [19].

Για παράδειγμα, σε ανοικτά δίκτυα τύπου bitcoin, υφίσταται ένας κίνδυνος, εκείνος των σιβυλλικών (sybil) επιθέσεων [20] που προφανώς δεν υφίσταται σε αδειοδοτούμενα, όπου οι συμμετέχοντες είναι εκ των προτέρων γνωστοί. Με δεδομένο ότι η πλειοψηφία των διαδεδομένων blockchains είναι ανοικτά και μη αδειοδοτούμενα, οι σιβυλλικές επιθέσεις αποτελούν μία βάσιμη απειλή για την ακεραιότητα του δικτύου, καθώς μία μειοψηφία μπορεί να αποκτήσει τον έλεγχο. Ο ‘Nakamoto’ συνδυάζοντας προγενέστερες αναφορές και ιδέες ολοκλήρωσε και εφάρμοσε μία καινοτόμο ιδέα για να καταπολεμήσει το πρόβλημα [21].

Αυξάνοντας αρκετά την απαίτηση υπολογιστικής ισχύος για τον αλγόριθμο συναίνεσης και μετατρέποντας τον σε έναν μηχανισμό PoW (Proof of Work), τον κατέστησε εξαιρετικά κοστοβόρο και κατ’ ουσία μετέτρεψε τη διαδικασία αυτή στην λεγόμενη ‘εξόρυξη’ (mining). Αποτέλεσμα αυτού, να ισοσκελίζεται η ευκολία της απόκτησης από έναν επιτιθέμενο πληθώρας κόμβων, με τη δυσκολία έως απιθανότητα να αποκτήσει και την αντίστοιχη απαιτούμενη υπολογιστική ισχύ.

Κατά πολλούς ερευνητές, η καινοτομία αυτή, που κατέστησε δυνατή την κατανεμημένη συναίνεση χωρίς έμπιστο μέρος, αποτέλεσε την συνταγή που κατέστησε αξιόπιστη και

ρεαλιστική την κατασκευή του bitcoin. Προκείμενου να γίνει κατανοητός ο μηχανισμός, μπορούμε να τον προσδιορίσουμε ως απαίτηση κοστοβόρων υπολογισμών (mining) που πρέπει να εκτελεστούν ώστε να επικυρωθεί μία ομάδα συναλλαγών (block) σε ένα κατανεμημένο μητρώο (ledger), το Blockchain.

2.6 Ο μαθηματικός γρίφος

Το σύνολο των προαναφερόμενων τεχνολογιών, από τη χρονοσφραγίδα έως την ασύμμετρη κρυπτογράφηση, και από τα δέντρα Merkle έως τα πρωτόκολλα συναίνεσης, αποτελούν την τροφοδότηση ενός και μόνο μηχανισμού, του ακρογωνιαίου λίθου κάθε blockchain, του κατακερματισμού.

Χωρίς να μας απασχολήσουν ιδιαίτερα οι διαφορές μεταξύ των χρησιμοποιούμενων αλγορίθμων, αρκεί να πούμε ότι η διαδικασία του κατακερματισμού περιγράφεται σχεδόν παντού ως mining. Το mining λοιπόν, αν πρέπει να το επεξηγήσουμε με μία πρόταση, είναι ο υπολογισμός της σύνοψης του, νεότερου προς προσθήκη στην αλυσίδα, block.

Ουσιαστικά, κατακερματίζει το block επικυρώνοντας το ως προς την νομιμότητα των συναλλαγών που περιέχει, ώστε να αποφεύγεται το πρόβλημα του double-spending, ενώ σε αρκετά blockchains, όπως το bitcoin και άλλα, αποτελεί και μέθοδο δημιουργίας και εισαγωγής νέων κρυπτονομισμάτων στο δίκτυο, ως αμοιβή στον ίδιο τον miner για τους πόρους που διέθεσε στη διαδικασία [22].

Ο μαθηματικός αυτός γρίφος, της εύρεσης δηλαδή του nonce, έχει μία βασική ιδιότητα, την ασυμμετρία. Η προσπάθεια που απαιτείται πρέπει να είναι σχετικά μεγάλη για την εξαγωγή του αποτελέσματος από τον miner αλλά σχετικά μικρή για την επιβεβαίωση ταύτισης δεδομένων block και σύνοψης από όλο το δίκτυο. Η πολυπλοκότητα όμως δεν έρχεται χωρίς αντίστοιχο κόστος, όπως θα δούμε πιο κάτω.

2.6.1 **Επίλυση του γρίφου**

Από τεχνικής άποψης, το mining είναι ένα είδος αντίστροφου κατακερματισμού. Δεν εννοούμε, όπως έχουμε ήδη δείξει, να εξάγει κάποιος τα αρχικά δεδομένα από μία σύνοψη, αλλά στόχος είναι η εξεύρεση του τυχαίου αριθμού (nonce) για τον οποίο ο αλγόριθμος κατακερματισμού δίνει μία τιμή κάτω από ένα, τεθέν συστημικά, όριο. Αν και θα δούμε παρακάτω διάφορες μεθόδους υπολογισμού, για αρχή θα εστιάσουμε στην οικογένεια PoW, μέλος της οποίας είναι του Hashcash του bitcoin. Ως PoW, εννοούμε δεδομένα που ενώ παρήχθησαν με μεγάλο κόστος, απαιτούν ελάχιστη προσπάθεια για να επιβεβαιωθεί η φύση τους.

Η διαδικασία εξαγωγής των δεδομένων περιλαμβάνει την έρευνα για μία τυχαία τιμή, το nonce, η οποία όταν κατακερματιστεί σε συνδυασμό με τα υπόλοιπα στοιχεία ενός block, προκύπτει μία τιμή μικρότερη από έναν στόχο. Είτε με Proof-of-Work (bitcoin), είτε με Proof-of-Stake (ethereum), είτε με άλλες προσεγγίσεις, η διαδικασία της εξεύρεσης του nonce και της επακόλουθης επικύρωσης του block, περιλαμβάνει και μία δυσκολία. Το τεθέν όριο ή αλλιώς ‘δυσκολία του αλγόριθμου’ είναι το στοιχείο που καθορίζει και την ανταγωνιστική φύση του

mining και ελέγχει και τη ροή των κρυπτονομισμάτων στο δίκτυο, καθώς όσο περισσότεροι κόμβοι συμμετέχουν ως miners ή όσο περισσότερη υπολογιστική ισχύς προστίθεται στο δίκτυο, τόσο αυξάνονται και οι απαιτούμενοι υπολογισμοί για τη δημιουργία ενός block [23].

2.6.2 **Εύρεση του nonce**

Για την εύρεση του nonce, ο κατακερματισμός πρέπει να συνυπολογίσει κάποια στοιχεία που είναι σταθερά, όπως η σύνοψη του προηγούμενου block, και κάποια που δεν είναι σταθερά, ή πιο σωστά, δύναται να αλλάξουν. Αυτά είναι οι συναλλαγές και η χρονοσφραγίδα. Είναι δυνατόν για ένα συγκεκριμένο σετ συναλλαγών, μία συγκεκριμένη χρονοσφραγίδα (για παράδειγμα της στιγμής που ξεκίνησε ο υπολογισμός) και δοκιμάζοντας όλα τα πιθανά nonces να μην προκύπτει σύνοψη.

Όπως έχουμε ήδη αναφέρει, στο bitcoin, το nonce είναι 32 bits, όσο και η χρονοσφραγίδα, το οποίο σημαίνει ότι αμφότερα μπορούν να λάβουν έως 4 δισεκατομμύρια διαφορετικές τιμές. Αν και για το nonce δεν υπάρχει κανένας περιορισμός, οι απαιτήσεις για την εγκυρότητα της χρονοσφραγίδας περιορίζουν πολύ το εύρος των δυνατών τιμών για να αποδειχθεί έγκυρο το block. Το μέγεθος όμως του nonce, επιφέρει δύο βασικούς προβληματισμούς.

Το πρώτο είναι ότι οποιοσδήποτε σύγχρονος υπολογιστής μπορεί να υπολογίσει περίπου 100 εκατομμύρια συνόψεις ανά δευτερόλεπτο, το οποίο συνεπάγεται ότι θα δοκιμάσει όλες τις πιθανές τιμές για το nonce σε 40 δευτερόλεπτα. Ο χρόνος αυτός μειώνεται δραστικά έως κλάσματα δευτερολολέπτου για πιο αφοσιωμένους miners με ειδικά μηχανήματα ή για mining pools, συνέργειες δηλαδή μεταξύ ξεχωριστών χρηστών που συνδυάζουν την ισχύ τους.

Το δεύτερο είναι ότι η πιθανότητα να βρεθεί έγκυρη σύνοψη απλώς ελέγχοντας όλες τις τιμές του nonce χωρίς να τροποποιείς τα υπόλοιπα δεδομένα είναι εξαιρετικά μικρή, της τάξης του 0.0000000001%. Μη αλλάζοντας καθόλου τις επιλεγμένες συναλλαγές, ο miner μπορεί να επανεκτελέσει τα 4 δισεκατομμύρια υπολογισμών του, το επόμενο δευτερόλεπτο, αλλαγή που επιφέρει, όπως έχει τονιστεί, μία εξαρχής καινούργια ομάδα παραγόμενων συνόψεων.

Η επόμενη παράμετρος που αλλάζει είναι οι συναλλαγές. Από τη στιγμή που το μέγεθος του block είναι περιορισμένο και δεν μπορεί να περιέχει όλες τις συναλλαγές που βρίσκονται σε αναμονή στην ‘ενδιάμεση’ μνήμη, στο mempool, ο miner επιλέγει ποιες θα χρησιμοποιήσει κάθε φορά και αυτό σχεδόν πάντα έχει σχέση με την ανταμοιβή που δίνει κάθε συναλλαγή στον miner. Αλλάζοντας, λοιπόν, τις επιλεγμένες συναλλαγές, αλλάζει αυτόματα και η σύνοψη τους από το Δέντρο Merkle, δημιουργώντας ένα καινούργιο πλήθος δυνατών συνδυασμών nonces.

Το εγχείρημα ολοκληρώνεται σε συνάρτηση με την εκάστοτε ‘δυσκολία του αλγορίθμου’ που ορίζει το όριο της τιμής κάτω από την οποία γίνεται αποδεκτή η σύνοψη ως έγκυρη. Από τη στιγμή που οι τιμές είναι όλες δεκαεξαδικές, κάθε μηδενικό που καταλαμβάνει μία θέση από αριστερά, μειώνει το μέγεθος της τιμής-ορίου με συντελεστή 16. Τη στιγμή της συγγραφής, στο bitcoin ο στόχος είχε τεθεί στα 18 μηδενικά, ουσιαστικά περιορίζοντας το πλήθος των έγκυρων συνόψεων σε 1646 (εφόσον απομένουν 64-18=46 μη μηδενικά ψηφία). Ο τρόπος που αλλάζει ο

στόχος θα περιγραφεί παρακάτω, αλλά αξίζει να αναφερθεί ότι ο αλγόριθμος του ‘Nakamoto’ στοχεύει στην παραγωγή ενός block ανά 10 λεπτά.

3 ΚΕΦΑΛΑΙΟ 3ο - ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

3.1 Εισαγωγή στην τεχνολογία Blockchain

Βρισκόμαστε στην αρχή μιας νέας επανάστασης που ξεκίνησε μια περιθωριακή οικονομία στο Διαδίκτυο, δηλαδή ένα εναλλακτικό νόμισμα που ονομάστηκε bitcoin και εκδόθηκε και υποστηρίχτηκε όχι από μια κεντρική αρχή, αλλά από μια αυτοματοποιημένη συναίνεση μεταξύ των δικτυωμένων χρηστών. Η πραγματικότητα της νέας επανάστασης είναι ότι δεν απαιτεί από τους χρήστες να εμπιστεύονται ο ένας τον άλλο, αλλά μέσω μιας αυτό-αστυνόμευσης ελέγχει οποιαδήποτε κακόβουλη προσπάθεια εξαπάτησης του συστήματος θα αποδειχθεί. Με ακριβή και τεχνικό ορισμό, το bitcoin είναι ψηφιακό ρευστό που διακινείται μέσα στο Διαδίκτυο σε ένα αποκεντρωμένο σύστημα χωρίς εμπιστοσύνη, χρησιμοποιώντας ένα δημόσιο βιβλίο που ονομάζεται Blockchain. Πρόκειται για μια νέα μορφή χρημάτων που συνδυάζει την κοινή χρήση αρχείων BitTorrent με κρυπτογράφηση δημόσιου κλειδιού. Από την έναρξή της το 2009, η Bitcoin δημιούργησε μια ομάδα μιμητών εναλλακτικών νομισμάτων, χρησιμοποιώντας την ίδια γενική προσέγγιση αλλά με διαφορετικές βελτιστοποιήσεις.

Με άλλα λόγια, το Blockchain αποτελεί έναν τύπο βάσης δεδομένων που δέχεται ένα πλήθος εγγραφών από τους χρήστες, τις οποίες τοποθετεί σε ένα φύλλο δεδομένων γνωστό ως block. Κάθε χρήστης διατηρεί ένα αντίγραφο αυτού του block. Καθώς οι εγγραφές αυξάνονται, κάθε block συνδέεται με μία γραμμική, χρονολογική σειρά με το επόμενο δημιουργώντας μία αλυσίδα (Blockchain), με τη χρήση μίας κρυπτογραφημένης υπογραφής. Η διαδικασία αυτή επιτρέπει στο Blockchain να χρησιμοποιείται σαν ένα δημόσιο λογιστικό βιβλίο (ledger), το οποίο μπορεί να μοιραστεί και να επιβεβαιωθεί από οποιοδήποτε εξουσιοδοτημένο χρήστη. Η ιδιότητα αυτή το καθιστά αποκεντρωμένο (decentralized) καθότι και η εποπτεία της ορθότητας της συναλλαγής διαμοιράζεται σε όλους τους χρήστες του και δεν περιορίζεται σε ένα χρηματοπιστωτικό ίδρυμα.

Πιο συγκεκριμένα, η τεχνολογία Blockchain θα μπορούσε να γίνει το απρόσκοπτο ενσωματωμένο οικονομικό στρώμα που δεν έχει ποτέ ο Ιστός, για να λειτουργήσει ως τεχνολογική βάση για πληρωμές, αποκεντρωμένες ανταλλαγές, μεταφορές ψηφιακών περιουσιακών στοιχείων και έξυπνες συμβάσεις. Η τεχνολογία Bitcoin και Blockchain , ως τρόπος αποκέντρωσης, θα μπορούσε να είναι η επόμενη μείζονα ανατρεπτική τεχνολογία της παγκόσμια Πληροφορική (ακολουθώντας το main-frame, το PC, το Διαδίκτυο και την κοινωνική δικτύωση/κινητό τηλέφωνα), με τη δυνατότητα να αναδιαμορφώνουν όλη την ανθρώπινη δραστηριότητα.

Αν και κάπως πρώιμο, η χρήση της τεχνολογίας Blockchain και των κρυπτονομισμάτων, το άμεσο παράγωγο αυτής, είναι ικανή να εμποδίσει την εμφάνιση χρηματικών απατών. Η χρήση των έξυπνων συμβολαίων – προγράμματα και πρωτόκολλα που διευκολύνουν την πραγματοποίηση των όρων μίας συμφωνίας αφού έχουν τηρηθεί οι διάφοροι όροι και η εκ ορισμού της τεχνολογίας καταγραφής όλων των συναλλαγών σε συνδυασμό με την κρυπτογραφική μοναδικότητα των νομισμάτων θα ελαχιστοποιήσουν τις πιθανότητες διαπροσωπικών ή και εταιρικών απατών μέσω «λογιστικών μαγειρεμάτων».

Το Blockchain είναι ένα διμερές σύστημα. Ο εξοστρακισμός των ενδιαμέσων επομένως οδηγεί σε εκμηδενισμό των τελών των συναλλαγών ή των συναλλαγματικών διαφορών που χρεώνονται από τα παραδοσιακά χρηματοπιστωτικά ιδρύματα. Οι επιπρόσθετες χρεώσεις μπορεί να αφορούν επίσης νομικές, μεσιτικές, ή άλλους είδους συμβουλευτικές υπηρεσίες. Η τεχνολογία Blockchain μπορεί να μετριάσει τις προκλήσεις ρευστότητας παρέχοντας ένα τρόπο μείωσης της τριβής μέσω της μαθηματικής επικύρωσης των συναλλαγών. Μόλις η συναλλαγή επιβεβαιωθεί, παρέχεται μία ενοποιημένη, ανθεκτική στην παραβίαση ορατότητα στο αρχείο συναλλαγών. Η χαμηλή τριβή και η καλύτερη ορατότητα βελτιώνουν την απόδοση όλων των τύπων των συναλλαγών, όχι μόνο των συναλλαγών ομολόγων και άλλων τίτλων.

Με την πρώτη ματιά, η τεχνολογία αυτή αποτελεί απειλή για το χρηματοπιστωτικό τομέα. Ωστόσο, μπορεί να επιφέρει σημαντική στην αποτελεσματικότητα τους. Αντί της συμμετοχής πολλών ανθρώπων στη διαδικασία επικύρωσης μίας συναλλαγής και μία γραφειοκρατικής διαδικασίας που διαρκεί μέρες ή εβδομάδες για διακρατικές συναλλαγές, η μαθηματική επικύρωση μπορεί να επιβεβαιώσει μεγάλο όγκο συναλλαγών αυτοματοποιημένα. Αυτή η εξέλιξη θα οδηγήσει στην κατάσταση των άμεσων συναλλαγών, εκσυγχρονίζοντας τη βιομηχανία. Τέλος, η τεχνολογία Blockchain διαθέτει τη δυναμική να εισβάλλει σε ποικίλες βιομηχανίες, συμπεριλαμβανομένων της μουσικής, του μάρκετινγκ, της υγείας, της δημόσιας διοίκησης και αλλού. Ο καταιγισμός ιδεών για συσχετιζόμενες εταιρίες και πλατφόρμες τα τελευταία χρόνια είναι σημαντικός και αποδίδει καρπούς. Πολλές εταιρίες ακόμα και χώρες πειραματίζονται ενεργά με την νέα τεχνολογία και τα αποτελέσματα είναι ιδιαιτέρως ενθαρρυντικά.

Η τεχνολογία Blockchain είναι απλά στην αρχή της και έχει σαφώς τη δυναμική να αλλάξει συνήθειες, μεθοδολογίες και συστήματα. Ωστόσο, οι αδυναμίες της τεχνολογίας είναι ορατές ακόμα και στους πιο πιστούς οπαδούς της. Για παράδειγμα, το περιβαλλοντολογικό κόστος, η έλλειψη κανονισμών, η πολυπλοκότητα της και τα τεχνικά της προβλήματα είναι μερικά από τα τρωτά της σημεία. Όπως και να έχει, αποτελεί σίγουρα μία εναλλακτική για να αντιμετωπιστούν τα προβλήματα του τρέχοντος χρηματοοικονομικού συστήματος που είναι αρκετά, και αποτέλεσαν την αφορμή για τη δημιουργία του Blockchain μετά την αμερικανική τραπεζική κρίση του 2008.

Ένα Blockchain (μπλοκ αλυσίδας) αποτελεί ένα νέο τρόπο αποθήκευσης και μεταφοράς πληροφορίας [56]. Οι κεντρικές βάσεις δεδομένων έχουν χρησιμοποιηθεί εδώ και πολλά χρονιά από τις χρηματοπιστωτικές εταιρίες για την αποθήκευσης στοιχείων πελατών και την καταγραφή συναλλαγών. Πρόκειται για συστήματα προσεκτικά φυλασσόμενα και κλειστά, στα οποία επιτρέπονται μόνο προνομιούχοι χρήστες. Αυτό συνεπάγεται ορισμένες συνέπειες. Ένα συγκεντρωτικό σύστημα είναι αυτό που εξ ορισμού έχει σημείο αποτυχίας. Είναι επίσης ένα γεγονός που συνεπάγεται διαφορά ισχύος, επειδή οι προνομιακοί φορείς εκμετάλλευσης έχουν το προνόμιο να παρεμβαίνουν μονομερώς, αντιστρέφοντας μια συναλλαγή ή επιβάλλοντας νέες χρεώσεις. Το Blockchain προσφέρει μια ριζικά διαφορετική προσέγγιση. Το πρωτόκολλο Bitcoin [57], το οποίο δρομολογήθηκε το 2009, καθιέρωσε για πρώτη φορά τη βιωσιμότητα της

μεταβίβασης αξίας σε ομότιμη βάση μέσω του Διαδικτύου, χωρίς την ανάγκη ενός αξιόπιστου διαμεσολαβητή. Ο Satoshi Nakamoto, ο ψευδώνυμος δημιουργός του Bitcoin, επιλύει το πρόβλημα της διπλής δαπάνης: το ζήτημα ότι οι ψηφιακές πληροφορίες μπορούν εύκολα να αντιγραφούν και, ως εκ τούτου, έπρεπε προηγουμένως να συγκεντρωθεί μια κεντρική αρχή για να αντικατοπτρίζει το που βρίσκονται τα κεφάλαια.

Πιο απλά, το Blockchain είναι ένα ψηφιακό αρχείο που αποθηκεύεται σε ένα δίκτυο υπολογιστών σε όλο τον κόσμο. Αντί να εξασφαλίζει πληροφορίες περιορίζοντας την πρόσβαση, το Blockchain μοιράζεται πληροφορίες μεταξύ όλων των χρηστών. Η ιδιοκτησία των κεφαλαίων ελέγχεται κρυπτογραφικά και η πλήρης διαφάνεια και η αμοιβαία ιδιοκτησία του συστήματος σημαίνει ότι ένας κακός φορέας είναι άμεσα αναγνωρίσιμος και ότι αγνοούνται οι συναλλαγές που υποβάλλονται από έναν τέτοιο κόμβο. Η αποκεντρωμένη δομή του Blockchain διαθέτει πολλά βασικά χαρακτηριστικά σε αντίθεση με τις παραδοσιακές συγκεντρωτικές προσεγγίσεις, τα οποία περιγράφονται στη συνέχεια:

- Διαφάνεια: είναι πιθανό ο καθένας να παρακολουθεί την κίνηση κεφαλαίων από το ένα λογαριασμό στον άλλο.
- Μεταβλητότητα: αφού επιβεβαιωθεί, μια συναλλαγή δεν μπορεί να αντιστραφεί. Κανείς δεν μπορεί να παρεμβαίνει σε μια ολοκληρωμένη μεταφορά.
- Χαμηλό κόστος: τα τέλη συναλλαγών είναι ελάχιστα.
- Διασυνοριακή επικοινωνία: τα χρήματα μπορούν να αποστέλλονται τόσο εύκολα σε κάποιον που βρίσκεται στην άλλη άκρη του κόσμου, όσο και σε κάποιον που είναι στο επόμενο δωμάτιο.
- Ταχύτητα: λόγω της επίπεδης και διαφανούς φύσης του Blockchain , οι μεταφορές εμφανίζονται σχεδόν άμεσα και συνήθως επιβεβαιώνονται σε λεπτά, αντί για ώρες ή ημέρες.

Παρόλο που το Bitcoin έχει πολύ μεγάλη επιτυχία στη μεταφορά της αξίας και είναι μια αποτελεσματική μορφή αποκεντρωμένου χρήματος, από την αρχή αναγνωρίστηκε ότι η ίδια προσέγγιση θα μπορούσε να χρησιμοποιηθεί για την καταγραφή πληροφοριών σχεδόν οποιουδήποτε είδους στην ίδια κοινή βάση [58]. Εκτός από τα χρήματα, οι ακολουθίες των χαρακτήρων (strings) στο Blockchain θα μπορούσαν να αντιπροσωπεύουν απλά μηνύματα, ιδιοκτησία φυσικών ή ψηφιακών περιουσιακών στοιχείων ή τίτλων, αποφάσεις ψηφοφορίας κ.ο.κ. Αυτή η ευρύτερη εφαρμογή αναπτύχθηκε από διάφορες πλατφόρμες '2.0' συμπεριλαμβανομένων των Nxt και BitShares, μεταξύ άλλων. Αυτό εξασφαλίζει ότι η ασφάλεια των χρημάτων είναι πλήρως ενημερωμένη. Εκτός από αυτό, το Blockchain εξασφαλίζει πλήρη ανωνυμία. Εκτός από τον παραλήπτη και τον αποστολέα του νομίσματος, κανένας τρίτος δεν έχει πρόσβαση στα δεδομένα. Ο λόγος για αυτό είναι ότι οι πληροφορίες δεν μεταδίδονται σε κεντρικό διακομιστή. Ένα χαρακτηριστικό του νομίσματος, το οποίο εκτιμάται ιδιαίτερα από τους επενδυτές, είναι η δυνατότητα συμμετοχής.

Πιο συγκεκριμένα, οι μέτοχοι και όλα τα μέλη της κοινότητας μπορούν να συμμετέχουν στις αποφάσεις σχετικά με τις μελλοντικές εξελίξεις. Αυτό ισχύει όχι μόνο για τις ανησυχίες σχετικά με την ασφάλεια αλλά και για τις αποφάσεις Μάρκετινγκ και εξυπηρέτησης. Οι επενδυτές επωφελούνται από αυτό, επειδή η δημοτικότητα του κέρματος διαδραματίζει καθοριστικό ρόλο. Και οι δύο αυτοί παράγοντες γενικά οδηγούν σε αύξηση της κεφαλαιοποίησης της αγοράς και, ως εκ τούτου, της τιμής ανά μονάδα. Για τους επενδυτές που εντάχθηκαν νωρίς, αυτό σημαίνει ισχυρές αποδόσεις κερδών. Μέχρι σήμερα, ωστόσο, όλα αυτά ήταν σχετικά περιορισμένα κατά τον ένα ή τον άλλο τρόπο και δεν είχαν την κατάλληλη μορφή στις τρέχουσες μορφές τους για υιοθέτηση από τις πραγματικές χρηματοπιστωτικές επιχειρήσεις. Το Blockchain μπορεί να αποθηκευτεί ως ένα απλό αρχείο, ή σε μια απλή βάση δεδομένων. Τα μπλοκ συνδέονται προς τα "πίσω", με το κάθε ένα να έχει αναφορά στο προηγούμενο μπλοκ στην αλυσίδα. Το Blockchain συχνά εμφανίζεται σαν μια κάθετη στοίβα, με τα μπλοκ σε επίπεδα το ένα πάνω από το άλλο και το πρώτο μπλοκ που εξυπηρετεί ως θεμέλιο της στοίβας. Η οπτικοποίηση των μπλοκ να στοιβάζονται το ένα πάνω στο άλλο έχει σαν αποτέλεσμα τη χρήση όρων όπως "ύψος" για την απόσταση από το πρώτο μπλοκ και "κορυφή" ή "άκρη" για το πιο πρόσφατο μπλοκ που προστέθηκε μέσα στην αλυσίδα.

Κάθε μπλοκ εντός της αλυσίδας του Blockchain προσδιορίζεται από μια συνάρτηση κατακερματισμού (hash function) που παράγεται με τη χρήση του SHA2566 αλγόριθμου κρυπτογράφησης στην κεφαλίδα του μπλοκ. Κάθε μπλοκ αναφέρεται επίσης στο προηγούμενο μπλοκ (parent block) μέσα από το πεδίο προηγούμενο μπλοκ hash στην κεφαλή του μπλοκ. Με άλλα λόγια, κάθε μπλοκ περιέχει το hash του γονέα μέσα στη δική του επικεφαλίδα. Η ακολουθία των hash συνδέει κάθε μπλοκ προς τον γονέα του, δημιουργώντας έτσι μία αλυσίδα η οποία πηγαίνει πίσω σε όλη τη διαδρομή μέχρι το πρώτο μπλοκ που δημιουργήθηκε ποτέ.

Παρά το γεγονός ότι ένα μπλοκ έχει ένα μόνο γονέα, μπορεί να έχει προσωρινά πολλαπλά παιδιά. Κάθε ένα από τα παιδιά αναφέρεται στο ίδιο μπλοκ ως γονέα και περιέχει το ίδιο γονικό hash στο πεδίο προηγούμενο μπλοκ hash. Πολλαπλά παιδιά μπορούν να προκύψουν κατά τη διάρκεια ενός Blockchain fork, που ουσιαστικά είναι μια προσωρινή κατάσταση που εμφανίζεται όταν τα διάφορα μπλοκ που ανακαλύπτονται σχεδόν ταυτόχρονα, προκύπτουν από διαφορετικούς εξορύκτες. Τελικά, μόνο ένα παιδί μπλοκ γίνεται μέρος του Blockchain και το Blockchain έχει επιλυθεί. Ακόμα κι αν ένα μπλοκ έχει περισσότερα από ένα παιδιά, μπορεί να έχει μόνο ένα γονέα. Αυτό οφείλεται στο γεγονός ότι κάθε μπλοκ έχει ένα μόνο πεδίο προηγούμενο μπλοκ hash το οποίο αναφέρεται στον μοναδικό γονέα του. Το πεδίο hash προηγούμενου μπλοκ είναι μέσα στην κεφαλίδα του μπλοκ και με τον τρόπο αυτό επηρεάζει το hash του τρέχοντος μπλοκ. Η ταυτότητα του παιδιού αλλάζει εάν αλλάξει η ταυτότητα του γονέα. Όταν ο γονέας έχει τροποποιηθεί με οποιονδήποτε τρόπο, αλλαγές πραγματοποιούνται στο hash του γονέα. Το αλλαγμένο hash του γονέα απαιτεί μια αλλαγή στο hash προηγούμενου μπλοκ δείκτη του παιδιού. Αυτό με τη σειρά του προκαλεί το hash του παιδιού να αλλάξει, το οποίο απαιτεί μια αλλαγή στο δείκτη του εγγονιού, το οποίο με τη σειρά του αλλάζει το εγγόνι, και ούτω καθεξής.

Αυτό το αποτέλεσμα αλληλουχίας εξασφαλίζει ότι μόλις ένα μπλοκ έχει πολλές γενεές να το ακολουθούν, δεν μπορεί να αλλάξει χωρίς να αναγκάζει τον επαναϋπολογισμό όλων των μεταγενέστερων μπλοκ. Επειδή ένας τέτοιος επαναϋπολογισμός θα απαιτούσε τεράστιους υπολογισμούς, η ύπαρξη μιας μακράς αλυσίδας μπλοκ κάνει τη ιστορία του Blockchain αμετάβλητη, κάτι το οποίο αποτελεί βασικό χαρακτηριστικό της ασφάλειας του. Όταν κάποιος θέλει να προσθέσει μια συναλλαγή στην αλυσίδα, όλοι οι συμμετέχοντες στο δίκτυο θα την επικυρώσουν. Αυτό γίνεται με την εφαρμογή ενός αλγορίθμου στην συναλλαγή για την επαλήθευση της εγκυρότητας της. Τι ακριβώς νοείται ως "έγκυρο" ορίζεται από το σύστημα Blockchain και μπορεί να διαφέρει μεταξύ των συστημάτων. Στη συνέχεια, εναπόκειται στην πλειοψηφία των συμμετεχόντων να συμφωνούν ότι η συναλλαγή είναι έγκυρη.

Ένα σύνολο των εγκεκριμένων συναλλαγών στη συνέχεια ομαδοποιείται σε ένα μπλοκ, το οποίο αποστέλλεται σε όλους τους κόμβους του δικτύου. Αυτοί με τη σειρά τους επικυρώνουν το νέο μπλοκ. Κάθε διαδοχικό μπλοκ περιέχει μια συνάρτηση κατακερματισμού (hash), η οποία αποτελεί ένα μοναδικό δακτυλικό αποτύπωμα, του προηγούμενου μπλοκ. Κατ’ αυτό τον τρόπο, το Blockchain λειτουργεί ως ένα αποκεντρωμένο (decentralized) λογιστικό καθολικό, το οποίο είναι κοινό για όλους τους συμμετέχοντες, μιας και όλοι οι εμπλεκόμενοι αποθηκεύουν ένα αντίγραφό του, κάτι που εξασφαλίζει την ασφάλεια και η διαφάνεια των συναλλαγών. Η ειδοποιός διαφορά -αναφορικά με την προστασία- προκύπτει από το γεγονός ότι δεν είναι πλέον απαραίτητη η ύπαρξη μιας ενδιάμεσης «έμπιστης» αρχής (π.χ. μιας τράπεζας), ενώ η εμπιστοσύνη των συναλλασσόμενων μερών βασίζεται σε αλγοριθμική επιβεβαίωση.

3.2 Οφέλη και περιορισμοί τεχνολογίας Blockchain

Ενώ τις τελευταίες δεκαετίες το κεντρικοποιημένο μοντέλο λειτουργεί ικανοποιητικά στην πράξη, θα υπάρξει πρόβλημα όταν ο αριθμός των κόμβων ενός δικτύου μεγαλώσει αρκετά και δημιουργήσει πλήθος συναλλαγών, και αυτό θα συμβεί διότι εκτός της αύξησης των υπολογιστικών απαιτήσεων θα έχουμε αύξηση και στο κόστος [60]. Ακόμα, σε μια τέτοια περίπτωση μπορεί να παρατηρηθεί στους διακομιστές ενός δικτύου κυκλοφοριακή συμφόρηση (bottlenecks) και επίσης και σημεία αποτυχίας, καθιστώντας τα δίκτυα του Διαδικτύου των Πραγμάτων (IoT) ευάλωτα σε επιθέσεις τύπου DoS (Denial of Service). Επίσης, σε βιομηχανικές περιοχές είναι δύσκολη η εγκατάσταση κεντρικοποιημένων δικτύων, γιατί οι κόμβοι του IoT θα επεκταθούν σε μεγάλες περιοχές με τις ταχύτητες σύνδεσης να είναι χαμηλές.

Η Blockchain τεχνολογία μπορεί να προστατεύσει αποτελεσματικά την αυθεντικότητα (authenticity) και την ακεραιότητα (integrity) των συναλλαγών και έχει την δυνατότητα να παίξει σημαντικό ρόλο στο οικοσύστημα του IoT, μειώνοντας το κόστος και το χρόνο της κάθε εργασίας. Επίσης μειώνει την ανάγκη για κανονισμούς και δίνει την δυνατότητα της ενσωμάτωσης νόμων στον κώδικα, που με την σειρά τους θα μπορούν να εκτελούνται αυτόματα. Επιπλέον, χρησιμοποιώντας αυτή την τεχνολογία θα δοθεί η δυνατότητα δημιουργίας ασφαλών δικτύων πλέγματος, όπου με τρόπο αξιόπιστο οι έξυπνες συσκευές του IoT θα μπορούν να διασυνδεθούν, αποφεύγοντας έτσι απειλές όπως η κλοπή στοιχείων ταυτότητας και η

πλαστογράφηση μιας υπογραφής. Έτσι ο εντοπισμός συσκευών στην αλυσίδα Blockchain και η πραγματοποίηση ελέγχων ταυτότητας χωρίς την ανάγκη πιστοποίησης από κάποιον κεντρικό διακομιστή είναι εύκολος.

Η ύπαρξη εμποδίων που δυσχεραίνουν την ευρεία υιοθέτηση της τεχνολογίας Blockchain είναι όμως αναμφισβήτητη. Όμως, ο όγκος των συναλλαγών, το κόστος της ενέργειας, αλλά και η αποθήκευση των δεδομένων που αποτελούν τα τρία μεγαλύτερα προβλήματα, θα πρέπει να μας απασχολούν. Η χρήση των Merkle Trees είναι μια πρόταση για τη μείωση της πολυπλοκότητας στην επαλήθευση μιας συναλλαγής. Είναι δεδομένο ότι η δημόσια πρόσβαση στο Blockchain κάνει ευκολότερη τη διαφάνεια στις συναλλαγές και τη διάχυση της πληροφορίας. Επιπλέον, διευκολύνεται και η ελεγκτική διαδικασία με την εξάλειψη κάθε ενδεχομένου παραβιάσεων, εξαιτίας της δημόσιας χρήσης των δεδομένων. Ακόμα, μειώνεται και η ανάγκη για μεσολαβητές που αυξάνοντας τα κόστη αποκομίζουν κέρδη, και αυτό γιατί βρίσκονται κρυπτογραφημένες μέσα στο Blockchain όλες οι πληροφορίες που αφορούν τις συναλλαγές,. Έτσι, οι τράπεζες έχουν τη δυνατότητα να εξοικονομήσουν αρκετά δισεκατομμύρια κάθε χρόνο με τη μείωση του χρόνου διακανονισμού αλλά και την κατάργηση μιας σειράς διαδικασιών και μεθόδων που κοστίζουν τόσο σε χρόνο όσο και χρήμα.

Στη συνέχεια, παρατίθεται μια σειρά από υπηρεσίες του χρηματοπιστωτικού κλάδου που θα μπορούσαν να βελτιωθούν και να γίνουν πιο ασφαλείς και πιο γρήγορες για τη χρήση του Blockchain. Λόγω των προαναφερόμενων, μπορούμε να συμπεράνουμε ότι τα πλεονεκτήματα που προκύπτουν από τη χρήση της Blockchain τεχνολογίας, είναι τα ακόλουθα:

- Παροχή δεδομένων υψηλής ποιότητας: τα δεδομένα Blockchain είναι ακριβή, συνεπή και ευρέως διαθέσιμα.
- Απλούστευση οικοσυστήματος: όλες οι συναλλαγές συσσωρεύονται σε ένα ενιαίο δημόσιο καθολικό (ledger), ελαχιστοποιώντας τα προβλήματα που θα μπορούσαν να δημιουργηθούν από την ύπαρξη πολλών καθολικών.
- Χαμηλότερο κόστος συναλλαγών: εξαλείφοντας τους μεσάζοντες και τα γενικά έξοδα που χρειάζονται για την ανταλλαγή περιουσιακών στοιχείων, πετυχαίνεται σημαντική μείωση των εξόδων συναλλαγής.
- Ταχύτερες συναλλαγές: σε μια τράπεζα οι συναλλαγές μπορεί να χρειαστούν και ημέρες για να μπορέσουν να διευθετηθούν. Αντίθετα, στις συναλλαγές Blockchain υπάρχει η δυνατότητα να μειωθεί ο συνολικός χρόνος συναλλαγής και αυτές να λειτουργούν χωρίς χρονικούς περιορισμούς.
- Ακεραιότητα διαδικασιών: Στις συναλλαγές Blockchain οι χρήστες μπορούν να εμπιστοσύνη και έτσι επί της ουσίας η ανάγκη για ένα έμπιστο τρίτο μέρος, όπως είναι οι τράπεζες, καταργείται.

Στην αντίπερα όχθη τα μειονεκτήματα στην τεχνολογία Blockchain , που μπορούμε να παρατηρήσουμε είναι τα ακόλουθα [70]:

- Έλεγχος, ασφάλεια και προστασία της ιδιωτικότητας: ενώ υπάρχει η δυνατότητα για μία ισχυρή κρυπτογράφηση, εξακολουθούν να υπάρχουν ανησυχίες για την ασφάλεια, έτσι το κοινό δυσκολεύεται να αναθέσει τα προσωπικά του δεδομένα σε ένα Blockchain.
- Μεγάλη κατανάλωση ενέργειας: στο Blockchain οι miners εκτελούν πάρα πολλές λύσεις ανά δευτερόλεπτο για την επικύρωση των συναλλαγών, καταναλώνοντας έτσι σημαντικές ενεργειακές ποσότητες του υπολογιστή.
- Υψηλό αρχικό κόστος κεφαλαίου: ενώ το Blockchain προσφέρει τεράστια εξοικονόμηση του κόστους συναλλαγών, λόγω του υψηλού αρχικού κόστους κεφαλαίου που απαιτείται, θα μπορούσε να αποτελέσει αποτρεπτικό παράγοντα προς την χρήση της συγκεκριμένης τεχνολογίας.

Η άνοδος του Bitcoin και των παρόμοιων πρωτοκόλλων συνοδεύτηκε από ταχεία επανεξέταση των υφιστάμενων παραδειγμάτων από τις κυβερνήσεις, τις ρυθμιστικές αρχές και τον κλάδο των χρηματοπιστωτικών υπηρεσιών [61]. Λόγω της θέσης του Bitcoin εκτός του ελέγχου των κρατικών και χρηματοπιστωτικών αρχών και των δυνατοτήτων κατάχρησης ως μέσου απάτης, νομιμοποίησης εσόδων από παράνομες δραστηριότητες και άλλων παράνομων δραστηριοτήτων, καθώς και άλλων προβλημάτων, όπως η αστάθεια και ο μη ρυθμιζόμενος χαρακτήρας των ανταλλαγών στις οποίες οι πρώτες αντιδράσεις τείνουν να είναι σκεπτικισμός και ανησυχία. Ωστόσο, ένας αυξανόμενος αριθμός φορέων αναγνώρισε επίσης το δυναμικό της τεχνολογίας Blockchain και το ευρύ φάσμα των περιπτώσεων χρήσης, στις οποίες προσφέρεται.

Σημαντική μετατόπιση έχει σημειωθεί με μια σειρά εθνικών κυβερνήσεων και μεγάλων τραπεζών να διεξάγουν ενεργά έρευνα για την κατανεμημένη τεχνολογία λογιστικών βιβλίων (DLT) ως μέσο για τη δημιουργία πιο αποτελεσματικών χρημάτων και την παροχή αποτελεσματικότερων δημόσιων υπηρεσιών - τουλάχιστον η βρετανική κυβέρνηση, η Κίνα, η Νότια Κορέα, η Goldman Sachs και η UBS, μεταξύ άλλων. Περίπου 1 δισεκατομμύριο δολάρια επενδύθηκαν σε εταιρείες που σχετίζονται με το Bitcoin μόνο το 2015. Τα οφέλη της τεχνολογίας Blockchain για εταιρείες και οργανισμούς όλων των μεγεθών και τύπων γίνονται ολοένα και πιο σαφή. Ωστόσο, μέχρι στιγμής υπάρχουν λίγες επιλογές για όσους επιθυμούν να αναπτύξουν ή να χρησιμοποιήσουν τεχνολογία Blockchain. Πρέπει είτε να επενδύσουν το χρόνο και τα χρήματα για να δημιουργήσουν και να διατηρήσουν το δικό τους πρωτόκολλο από το μηδέν, είτε να χρησιμοποιήσουν μια υπάρχουσα ανοιχτή πλατφόρμα (όπως η ίδια η Bitcoin), με όλους τους περιορισμούς και τα προβλήματα που αυτό συνεπάγεται.

Το Blockchain αποτελεί ήδη μια μορφή μετρητών για το Διαδίκτυο, ένα σύστημα ψηφιακών πληρωμών, και αυτό μπορεί να γίνει το "Διαδίκτυο των χρημάτων", που συνδέει τα οικονομικά με τον τρόπο που το Διαδίκτυο των πραγμάτων (IoT) συνδέουν τα μηχανήματα. Το νόμισμα και οι πληρωμές αποτελούν το πρώτο και το μεγαλύτερο προφανή εφαρμογή. Τα εναλλακτικά νομίσματα έχουν νόημα βάσει ενός οικονομικού επιχειρήματος μόνο: μείωση των τελών πληρωμής των και εμπορικών πιστωτικών καρτών παγκοσμίως από 3% όσο και μέχρι κάτω από το 1% έχει προφανή οφέλη για την Οικονομία, ειδικά στην Οικονομία 514 δισεκατομμύρια

δολάρια διεθνή εμβασμάτων στην αγορά, όπου τα τέλη συναλλαγών μπορούν να τρέξουν από 7 σε 30 %.

Επιπλέον, οι χρήστες μπορούν να λάβουν άμεσα χρήματα σε ψηφιακά πορτοφόλια αντί να περιμένουν ημέρες για μεταφορές. Το Bitcoin και οι μιμητές του θα μπορούσαν να ανοίξουν το δρόμο για το νόμισμα και το εμπόριο, προκειμένου αυτό να επαναπροσδιοριστεί πλήρως. Σε γενικές γραμμές, το Bitcoin δεν είναι μόνο μια καλύτερη έκδοση της Visa, θα μπορούσε επίσης να μας επιτρέψει να κάνουμε πράγματα δεν έχουμε ακόμη σκεφτεί ακόμα. Το νόμισμα και οι πληρωμές είναι μόνο η πρώτη αίτηση. Η βασική λειτουργικότητα των νομισμάτων Blockchain είναι ότι κάθε συναλλαγή μπορεί να προέλθει και να ολοκληρωθεί απευθείας μεταξύ δύο ατόμων μέσω του Διαδικτύου. Με χρήση των altcoins, μπορεί να γίνει η ανταλλαγή πόρων μεταξύ ατόμων με αποκεντρωμένο, διανεμημένο και παγκόσμιο τρόπο. Με αυτήν την ικανότητα, μια κρυπτογράφηση μπορεί να είναι ένα προγραμματιζόμενο ανοιχτό δίκτυο για την αποκεντρωμένη διαπραγμάτευση όλων των πόρων, πολύ πέρα από το νόμισμα και τις πληρωμές. Έτσι, το Blockchain 1.0 για το νόμισμα και τις πληρωμές είναι ήδη επεκταθεί σε Blockchain 2.0, για να επωφεληθεί από την πιο ισχυρή λειτουργικότητα του Bitcoin ως προγραμματιζόμενα χρήματα.

Επειδή πολλές από τις ιδέες και τις έννοιες πίσω από Bitcoin και την τεχνολογία Blockchain είναι νέες και τεχνικά περίπλοκες, ένα αρνητικό σημείο είναι το γεγονός ότι οι κρυπτοσυχνότητες είναι πολύ περίπλοκες για την υιοθέτηση της νέας τεχνολογίας. Ωστόσο, το ίδιο ισχύει και για το Διαδίκτυο και γενικότερα για την αρχή κάθε νέας τεχνολογικής εποχής, οι τεχνικές λεπτομέρειες του "τι είναι" και του "πώς λειτουργεί" παρουσιάζουν ενδιαφέρον για ένα δημοφιλές κοινό. Αυτό δεν είναι πραγματικό εμπόδιο; Για παράδειγμα, δεν είναι απαραίτητο να γνωρίζουμε πώς λειτουργεί το TCP/IP, προκειμένου να σταλθεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου και ότι οι νέες τεχνολογικές εφαρμογές μεταφέρονται στη δημόσια χρήση χωρίς να εξετάζονται περαιτέρω οι τεχνικές λεπτομέρειες, όσο αναπτύσσονται κατάλληλες και αξιόπιστες εφαρμογές διεπαφών.

Υπάρχουν πολλά ζητήματα ασφαλείας κρυπτογράφησης για να αντιμετωπιστεί ένα κρυπτογραφημένο κοινό με χρήσιμα πορτοφόλια πελατών, συμπεριλαμβανομένων του πως να δημιουργηθούν αντίγραφα ασφαλείας των χρημάτων, τι να κάνει κάποιος, εάν χάσει το ιδιωτικό του κλειδί και τι να κάνει αν λάβει ένα νόμισμα απαγορευμένο (δηλαδή πριν κλαπεί) σε μια συναλλαγή και τώρα δεν μπορεί να το ξεφορτωθεί. Ωστόσο, αυτά τα ζητήματα αντιμετωπίζονται από τη βιομηχανία Blockchain. Η υιοθέτηση των νομισματικών εφαρμογών θα μπορούσε να είναι απλή με αξιόπιστα χρήσιμα στοιχεία, αλλά η επιτυχής καθολική υιοθέτηση εφαρμογών μπλοκ αλυσίδων πέρα από το νόμισμα θα μπορούσε να είναι πιο λεπτή. Αποθηκεύοντας δεδομένα σε όλο του το δίκτυο, το Blockchain εξαλείφει τους κινδύνους που εγκυμονεί από το να διατηρούνται αυτά τα δεδομένα κεντρικά. Το δίκτυο του δεν έχει κεντρικά σημεία, τα οποία είναι ευπαθή και τα οποία μπορούν να εκμεταλλευτούν οι hackers. Το σημερινό Διαδίκτυο παρουσιάζει προβλήματα ασφάλειας, όπως είναι ευρέως γνωστό. Οι χρήστες χρησιμοποιούν τον συνδυασμό «όνομα χρήστη/κωδικό πρόσβασης» για να προστατέψουμε την ταυτότητα και τα περιουσιακά

μας στοιχεία στο διαδίκτυο. Οι μέθοδοι ασφαλείας του Blockchain χρησιμοποιούν τεχνολογία κρυπτογράφησης.

Η βάση αυτού είναι τα επονομαζόμενα δημόσια και ιδιωτικά «κλειδιά». Ένα δημόσιο κλειδί (ακολουθία αριθμών που έχουν παραχθεί τυχαία) είναι η διεύθυνση του χρήστη στο Blockchain. Τα Bitcoins που στέλνονται σε όλο το δίκτυο καταγράφονται ότι ανήκουν σε αυτή την διεύθυνση. Το ιδιωτικό κλειδί είναι σαν ένας κωδικός που δίνει στον ιδιοκτήτη του πρόσβαση στο Bitcoin του ή σε άλλα ψηφιακά περιουσιακά του στοιχεία.

Η δημόσια πρόσβαση στο Blockchain διευκολύνει τη διαφάνεια στις συναλλαγές καθώς και τη διάχυση της πληροφορίας. Στο ίδιο πλαίσιο, διευκολύνεται η ελεγκτική διαδικασία με την εξάλειψη κάθε ενδεχομένου παραβάσεων, ακριβώς εξαιτίας της δημόσιας φύσης των δεδομένων. Ταυτόχρονα, εξαλείφεται και η ανάγκη για ενδιάμεσα μέρη που αυξάνουν τα κόστη, αφού όλες οι πληροφορίες που αφορούν στη συναλλαγή βρίσκονται κρυπτογραφημένες μέσα στο Blockchain. Έτσι, για παράδειγμα οι τράπεζες μπορούν να εξοικονομήσουν αρκετά δισεκατομμύρια κάθε χρόνο με την ελαχιστοποίηση του χρόνου διακανονισμού, αλλά και την κατάργηση μίας σειράς διαδικασιών που κοστίζουν σε χρόνο και χρήμα. Από εκεί και πέρα, υπάρχουν μία σειρά από υπηρεσίες και λύσεις στον χρηματοπιστωτικό κλάδο που θα μπορούν να γίνουν καλύτερες, πιο ασφαλείς και να απαιτούν λιγότερο χρόνο υλοποίησης με τη χρήση του Blockchain. Όπως υπάρχουν και αρκετές ακόμη ιδέες που θα μπορούσαν να αξιοποιήσουν τη συγκεκριμένη τεχνολογία και να δημιουργήσουν πολλά νέα προϊόντα και λύσεις για τον χρηματοπιστωτικό κλάδο.

3.3 Τομείς εφαρμογής της Τεχνολογίας Blockchain

Υπάρχει μια νέα τεχνολογία που έχει ταράξει τα νερά στις χρηματοπιστωτικές αγορές. Και ενώ το όνομά της – τεχνολογία κατανεμημένου καθολικού (distributed ledger technology - DLT) – μπορεί να ακούγεται τεχνικό, κάποιοι ισχυρίζονται ότι έχει τη δυνατότητα να αλλάξει ολοκληρωτικά τον τρόπο λειτουργίας των χρηματοπιστωτικών αγορών και του τραπεζικού τομέα [62]. Τι ακριβώς είναι λοιπόν αυτή η τεχνολογία και γιατί είναι σημαντική για κεντρικές τράπεζες όπως η ΕΚΤ; Η τεχνολογία κατανεμημένου καθολικού είναι ένα εργαλείο για την καταγραφή της κυριότητας – θα μπορούσε να αναφέρεται για παράδειγμα στην κυριότητα χρήματος ή περιουσιακών στοιχείων, όπως τα ακίνητα. Σήμερα, όταν οι τράπεζες διενεργούν συναλλαγές – δηλαδή όταν μεταβιβάζεται η κυριότητα χρήματος ή χρηματοοικονομικών περιουσιακών στοιχείων – χρησιμοποιούν κεντρικά συστήματα, τα οποία συχνά διαχειρίζονται οι κεντρικές τράπεζες. Οι τράπεζες καταγράφουν τις συναλλαγές τους σε τοπικές βάσεις δεδομένων, οι οποίες επικαιροποιούνται μετά την ολοκλήρωση της συναλλαγής στο κεντρικό σύστημα. Το κατανεμημένο καθολικό, από την άλλη, είναι μια βάση δεδομένων όσον αφορά τις συναλλαγές που, αντί να αποθηκεύεται σε μια κεντρική τοποθεσία, κατανέμεται σε ένα δίκτυο πολλών υπολογιστών. Συνήθως, όλα τα μέλη του δικτύου μπορούν να διαβάζουν τις πληροφορίες και, ανάλογα με τις άδειες που τους έχουν δοθεί, να προσθέτουν στοιχεία.

Ο πιο κοινός τύπος τεχνολογίας κατανεμημένου καθολικού ονομάζεται αλυσίδα συστοιχιών (Blockchain). Η ονομασία αυτή προέρχεται από το γεγονός ότι οι συναλλαγές ομαδοποιούνται προκειμένου να σχηματίσουν συστοιχίες (blocks) οι οποίες συνδέονται μεταξύ τους με χρονολογική σειρά σχηματίζοντας μια αλυσίδα (chain). Η αλυσίδα προστατεύεται στο σύνολό της από σύνθετους μαθηματικούς αλγορίθμους με σκοπό να διασφαλίζεται η ακεραιότητα και η ασφάλεια των δεδομένων. Αυτή η αλυσίδα αποτελεί την ολοκληρωμένη καταγραφή όλων των συναλλαγών που περιλαμβάνονται στη βάση δεδομένων.

Οι αλυσίδες των μπλοκ μετασχηματίζουν ήδη βασικούς κλάδους. Για τις εταιρείες, φαντάζει ιδιαίτερα ελκυστικό να έχουν μια ασφαλή εφοδιαστική αλυσίδα, να ξεφορτωθούν τους μεσάζοντες και να μειώσουν τα κόστη. Στη συνέχεια ακολουθούν ορισμένα παραδείγματα εφαρμογής της τεχνολογίας Blockchain :

Ναυτιλία: Η Maersk, η μεγαλύτερη ναυτιλιακή εταιρεία στον κόσμο, ολοκλήρωσε μια δοκιμή χρήσης μιας αλυσίδας των μπλοκ για την παρακολούθηση των φορτίων της. Η δοκιμή περιελάβανε όχι μόνο τη Maersk αλλά και τρίτα μέρη, όπως τα ολλανδικά τελωνεία και το υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ, και όλοι μαζί παρακολουθούσαν τα εμπορευματοκιβώτια εξ' αποστάσεως. Οι κρυπτογραφικές υπογραφές καθιστούν δυσκολότερη την παραποίηση των ετικετών, ενώ το φορτίο βρίσκεται εν κινήσει, και μπορούν να μειώσουν τον χρόνο της μεταφοράς.

Τραπεζική: Ο τραπεζικός κλάδος ταλαιπωρείται από αργά συστήματα τα οποία χρειάζονται ώρες, ακόμη και μέρες, για την επικύρωση βασικών συναλλαγών, όπως η πώληση μετοχών και η μεταφορά χρημάτων. Η υιοθέτηση των Blockchain s από τη Barclays και άλλες τράπεζες δείχνει ότι τα πράγματα αλλάζουν. Στο εγγύς μέλλον, αναμένεται να αυξηθεί η ταχύτητα των τραπεζικών υπηρεσιών, ενώ οι μεσάζοντες θα αποδιοργανωθούν. Μάλιστα, οι τράπεζες σκέφτονται να χρησιμοποιήσουν αλυσίδες των μπλοκ για τη μετατροπή του συστήματος SWIFT, το οποίο χρησιμοποιείται για παγκόσμιες διατραπεζικές συναλλαγές.

Κτηνοτροφία: Η εταιρεία Walmart ξεκίνησε να χρησιμοποιεί την τεχνολογία της αλυσίδας των μπλοκ το 2016 για να παρακολουθεί το ταξίδι των γουρουνιών από την Κίνα, μέσω της εφοδιαστικής αλυσίδας της εταιρείας, στο τραπέζι των Αμερικανών καταναλωτών [63]. Και τον Αύγουστο ένας κτηνοτροφικός συνεταιρισμός στο Αρκάνσας χρησιμοποίησε κωδικούς QR σε παλέτες με κοτόπουλα για την παρακολούθηση όλων των συναλλαγών που αφορούσαν το συγκεκριμένο φορτίο. Όλα αυτά αναμένεται να βοηθήσουν τις εταιρείες να μειώσουν τα αλλοιωμένα τρόφιμα και να αποτρέψουν τη μετάδοση ασθενειών.

Δίκαιο: Όλα τα είδη συμφωνιών – από πωλήσεις ακινήτων μέχρι επιχειρηματικές αγορές και εργατικές συμβάσεις – απαιτούν δικηγόρους και δικαστήρια για να εφαρμόζονται. Πλέον, ολοένα και περισσότερες εταιρείες πειραματίζονται με «έξυπνες συβάσεις» που εκτελούνται μόνες τους: Ένα σύστημα Blockchain μπορεί, για παράδειγμα, να αποδεσμεύσει τα χρήματα μιας εγγύησης μόλις ένα συμβαλλόμενο μέρος μεταφέρει έναν τίτλο ιδιοκτησίας.

Ενώ είναι ακόμα στα πρώτα στάδια ανάπτυξης του, το IoT αποτελείται ως επί το πλείστο από τεχνολογίες που επιτρέπουν τη συλλογή δεδομένων, την απομακρυσμένη παρακολούθηση και τον έλεγχο των συσκευών. Καθώς η τεχνολογία προχωράει, το IoT θα εξελιχθεί σε ένα δίκτυο αυτόνομων συσκευών που μπορούν να αλληλοεπιδρούν μεταξύ τους και με το περιβάλλον τους και να λαμβάνουν έξυπνες αποφάσεις χωρίς την ύπαρξη ανθρώπινης παρέμβασης. Σε αυτήν την εξέλιξη, η τεχνολογία Blockchain μπορεί να αναπτυχθεί και να αποτελέσει τη βάση που θα υποστηρίξει την επικοινωνία μηχανή -με - μηχανή (M2M – Machine – to - Machine). Η συγκεκριμένη τεχνολογία αποτελεί το συνδετικό κρίκο για να διευθετήσει τις όποιες ανησυχίες για την προστασία της ιδιωτικής ζωής και την αξιοπιστία του IoT. Μπορεί να χρησιμοποιηθεί για την παρακολούθηση δισεκατομμυρίων συνδεδεμένων συσκευών, καθώς επιτρέπει την επεξεργασία των συναλλαγών και του συντονισμού μεταξύ των συσκευών. Αυτό επιτρέπει μια σημαντική εξοικονόμηση για τους κατασκευαστές της βιομηχανίας IoT.

Αυτή η αποκεντρωμένη προσέγγιση θα εξαλείψει ενιαία σημεία της αποτυχίας, δημιουργώντας ένα πιο ανθεκτικό οικοσύστημα για συσκευές που θα τρέξουν πάνω σε αυτό. Οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στην τεχνολογία Blockchain , θα καταστήσουν τα δεδομένα των καταναλωτών πιο ιδιωτικά και ασφαλή. Το καθολικό (ledger) του Blockchain είναι απαραβίαστο και δεν μπορεί να χειραγωγηθεί από κακόβουλους παράγοντες, διότι δεν υπάρχει σε μία μόνο θέση, και επιθέσεις δεν μπορούν να οργανωθούν επειδή δεν υπάρχει ένα ενιαίο νήμα της επικοινωνίας που μπορεί να υποκλαπεί. Το Blockchain καθιστά δυνατή ασφαλή, peer-to-peer ανταλλαγή μηνυμάτων και έχει ήδη αποδείξει την αξία του στον κόσμο μέσω των υπηρεσιών κρυπτονομισμάτων, όπως το Bitcoin, παρέχοντας εγγυημένες peer - to-peer υπηρεσίες πληρωμών, χωρίς την ανάγκη για τρίτους.

3.4 Permissioned και Permissionless Blockchains

Υπάρχουν πολλές υλοποιήσεις blockchain. Αυτές μπορούν να κατηγοριοποιηθούν σε δύο μεγάλα σύνολα, τα δημόσια blockchains χωρίς δικαιώματα και τα ιδιωτικά ή επιχειρηματικά blockchains με δικαιώματα [64]. Στα δημόσια οποιοσδήποτε ενδιαφερόμενος μπορεί να συμμετάσχει στο δίκτυο. Η πρόσβαση είναι ανοιχτή στα δεδομένα τους διαβάζοντας την αλυσίδα και επαληθεύοντας τα μπλοκ δημιουργώντας διαφάνεια στην πληροφορία. Η επαλήθευση των μπλοκ γίνεται από τους εξορυκτές (miners) και υπάρχει η δυνατότητα να εξορύξουν όλοι αναζητώντας την ανταμοιβή τους. Έτσι επιτυγχάνεται η ασφαλής αποκέντρωση του συστήματος μιας και δεν χρειάζεται τα μέλη να εμπιστεύονται το ένα τον άλλο. Από την άλλη πλευρά ένα πρόβλημα για τις επιχειρήσεις προέκυψε λόγω του δημόσιου blockchains, οι συναλλαγές είναι εντελώς διαφανείς για όλους. Αυτό εξαλείφει την ανταγωνιστικότητα των επιχειρήσεων, επειδή δεν θέλουν να παρουσιάζουν όλες τις πληροφορίες τους [65]. Υπάρχουν πολλές περιπτώσεις εφαρμογών όπου οι συναλλαγές ή τα περιουσιακά στοιχεία δεν πρέπει να κοινοποιούνται ή να είναι προσβάσιμα από όλους, αλλά από επιλεγμένους συμμετέχοντες, π.χ. συναλλαγές ανταγωνιστών, ιατρικό ιστορικό και μεταφορά αγαθών. Γι’ αυτό το λόγο δημιουργήθηκαν τα ιδιωτικά blockchains. Είναι χρήσιμα σε περιπτώσεις όπου η ακεραιότητα του ίχνους δεν είναι το

πιο σημαντικό και υπάρχει η ανάγκη να τυποποιηθεί η ανταλλαγή πληροφοριών με ασφαλή τρόπο μεταξύ εταίρων, όπως ανάμεσα στις βιομηχανίες.

3.5 Κατανεμημένο καθολικό (Distributed Ledger)

Η τεχνολογία του κατανεμημένου καθολικού (distributed ledger technology ή DLT) είναι μια νέα τεχνολογία στα πρώτα στάδια ανάπτυξής της. Είναι ένας τύπος βάσης δεδομένων που έχει την ιδιότητα να αναπαράγει, να διαμοιράζεται και να συγχρονίζει τα δεδομένα του σε πολλαπλά σημεία, κόμβων και συσκευών (UK Office for Science, 2016). Χαρακτηριστικό του κατανεμημένου καθολικού είναι ότι δεν υπάρχει κεντρικός διαχειριστής ή κεντρική αποθήκευση δεδομένων. Μόλις υπάρξει η συναίνεση, το κατανεμημένο καθολικό ενημερώνεται και όλοι οι κόμβοι διατηρούν το δικό τους όμοιο αντίγραφο του [66].

3.6 Έξυπνα συμβόλαια (Smart Contracts)

Ο όρος των έξυπνων συμβολαίων χρησιμοποιήθηκε αρχικά από τον Αμερικάνο επιστήμονα πληροφορικής και κρυπτογράφο Nick Szabo [67]. Χαρακτηριστικά αναφέρει το παράδειγμα της ενοικίασης ενός αυτοκινήτου με έξυπνο συμβόλαιο έτσι ώστε να αποτραπεί η κλοπή του αν δεν ικανοποιηθεί το πρωτόκολλο παράδοσης. Το ίδιο θα μπορούσε να συμβεί σε μία περίπτωση τραπεζικού δανείου για αγορά αυτοκινήτου όπου ο ιδιοκτήτης δεν μπορούσε να πραγματοποιήσει τις πληρωμές, το έξυπνο συμβόλαιο αυτομάτως θα έκανε κατάσχεση επισωρεύοντας τα κλειδιά του αυτοκινήτου στην τράπεζα.

Τα έξυπνα συμβόλαια είναι μικρά αυτόνομα προγράμματα που λαμβάνουν μια συναλλαγή ως είσοδο, επεξεργάζονται και παράγουν μια νέα έξοδο. Η εκτέλεσή τους ξεκινάει αυτόματα, υπό συγκεκριμένες συνθήκες και παράγει ένα αποτέλεσμα. Αυτό πραγματοποιείται στο επίπεδο του blockchain όπου ζει η επιχειρηματική λογική και συγκεκριμένες προγραμματικές λειτουργίες που εξυπηρετούν μια περίπτωση χρήσης. Το κυριότερα οφέλη του συμβολαίου είναι ότι το blockchain εγγυάται πως οι συμβατικοί όροι δεν μπορούν να τροποποιηθούν και είναι αδύνατη η παραβίαση τους. Με την εφαρμογή αυτών αναμένεται να μειωθεί το κόστος εκτέλεσης, επαλήθευσης, ελέγχου και αποφυγής απάτης μια σύμβασης. Τέλος, με τα έξυπνα συμβόλαια ξεπερνιέται το πρόβλημα του ηθικού κινδύνου.

Η χρήση έξυπνων συμβολαίων σε ένα blockchain ξεκίνησε με το Bitcoin, το οποίο προσέφερε μια περιορισμένη ψευδό-γλώσσα (scripting language). Αυτή η γλώσσα έχει «κλαδευτεί» ακόμη περισσότερο μετά την εισαγωγή της καθώς εντοπίστηκαν ευπάθειες όταν εκτελούνταν ορισμένες λειτουργίες. Το Ethereum επέκτεινε αυτή την έννοια, των έξυπνων συμβολαίων, με την επεξεργασία των συναλλαγών σε μια ειδικά δημιουργημένη εικονική μηχανή. Τα έξυπνα συμβόλαια γράφονται σε γλώσσα υψηλότερου επιπέδου, πιο συχνά την Solidity, τα οποία στη συνέχεια μεταγλωττίζονται σε ψηφιακό κώδικα Ethereum Virtual Machine (EVM). Η λογική του συμβόλαιο και ο κώδικας διαμοιράζεται στο δίκτυο ούτος ώστε να χρησιμοποιηθεί από τους συμμετέχοντες για να επικυρώσουν και να επεξεργαστούν τις συναλλαγές. Το αποτέλεσμα της εσωτερικής κατάστασης του συμβολαίου γράφεται κατανεμημένα.

Σε σύγχρονες εφαρμογές blockchain για επιχειρήσεις αξιοποιείται μια ακόμα υλοποίηση από έξυπνα συμβόλαια, αυτά του Hyperledger Fabric. Έχει αναπτυχθεί ο chaincode που είναι ο κώδικας στον οποίο γράφονται τα έξυπνα συμβόλαια. Περιλαμβάνει την ερμηνεία αυτών σε λογική μεθόδων και αλγορίθμων μαζί με επιπρόσθετες λειτουργίες [68]. Με συγκεκριμένες ρυθμίσεις στην πολιτική ορίζεται ποιοι ακριβώς κόμβοι ή χρήστες, ή πόσοι από αυτούς θα εκτελέσουν ένα smart contract. Επόμενος η κάθε συναλλαγή εκτελείται μόνο από ένα υποσύνολο κόμβων. Αυτό επιτρέπει παράλληλες εκτελέσεις, αυξάνοντας τη συνολική απόδοση και την κλίμακα του συστήματος. Η γλώσσα προγραμματισμού που μπορούν να συνταχθούν είναι είτε Go είτε Node.js. Παράλληλα υπάρχει η δυνατότητα ανάπτυξης εφαρμογών blockchain στο Hyperledger Composer όπου για την δημιουργία έξυπνων συμβολαίων χρησιμοποιείτε διερμηνέας σε γλώσσα JavaScript που εκτελεί τη λογική για την επεξεργασία της συναλλαγής σε chaincode του HyperLedger Fabric [69].

3.7 Συναίνεση (Consensus)

Ως συναίνεση στην τεχνολογία αυτή ορίζεται η διαδικασία κατά την οποία επικυρώνεται η αξιοπιστία των συναλλαγών σε ολόκληρο το δίκτυο και η απόρριψη των ελαττωματικών διαδικασιών. Υπάρχουν πολλοί αλγόριθμοι συναινέσεις με διαφορετικά χαρακτηριστικά αλλά εξυπηρετώντας τον ίδιο σκοπό. Σε ένα ανοιχτό blockchain, όπως το bitcoin χρειάζεται μεγάλη επεξεργαστική ισχύ για τον PoW. Οι εξορυκτές (miners) ανταγωνίζονται μεταξύ τους για να ολοκληρώσουν τις συναλλαγές στο δίκτυο και να ανταμειφθούν [70]. Δείχνοντας μεγαλύτερη εμπιστοσύνη για τις επικυρώσεις των συναλλαγών, π.χ. το παγκόσμιο σύστημα χρηματοπιστωτικών συναλλαγών Ripple, επιλέγει μια λίστα επικυρωτών (validators) γνωστών ή μερικώς γνωστών. Κάθε λίγα δευτερόλεπτα εφαρμόζεται ο αλγόριθμος RPCA (Ripple Consensus Algorithm) από όλους τους κόμβους. Είναι βασισμένος στην έννοια του proof of correctness και είναι βελτιστοποιημένος και ταχύτερος από αυτόν του PoW [71]. Ένα ακόμη διαδεδομένο μοντέλο κατανεμημένης συναίνεσης είναι το Proof-of-Stake, στο οποίο επιλέγεται ο δημιουργός του επόμενου μπλοκ βάση συνδυασμών τυχαίας επιλογής π.χ. πλούτου, ηλικίας. Αυτό είναι το ποντάρισμα (stake) για την επικύρωση του μπλοκ. Τέλος ακόμα ένας ευρέως διαδεδομένος αλγόριθμος είναι ο Byzantine Fault Tolerance (BFT) που εγγυάται την κάλυψη ή την ικανότητα να επιτύχει συναίνεση, ακόμα και αν υπάρχουν αντίπαλοι κόμβοι (κακόβουλοι) ή αν οι κόμβοι βρεθούν εκτός δικτύου. Δεν χρειάζεται εξορυκτές και βρίσκει μεγάλη εφαρμογή σε ιδιωτικά blockchain όπως το Hyperledger Fabric.

3.8 Οι τύποι του BlockChain

Το Blockchain αποτελείται από 3 διαφορετικούς τύπους. Η επιλογή του Blockchain τύπου που θα χρησιμοποιηθεί εξαρτάται από τους εξής παράγοντες:

- Αν το βιβλιάριο θα είναι κατανεμημένο ή όχι.
- Ποιοι χρήστες θα έχουν πρόσβαση σε αυτό.
- Ποιοι χρήστες θα επαληθεύουν και θα καταχωρούν τις συναλλαγές δεδομένων στο βιβλιάριο.

3.8.1 **Public**

Τα δημόσια Blockchains όπως είναι για παράδειγμα το Bitcoin και το Ethereum είναι από τα μεγαλύτερα σε αριθμό συμμετεχόντων κατανεμημένα δίκτυα. Ο κώδικας εκδίδεται ανοιχτά προς όλους και οποιοσδήποτε μπορεί να τον επιθεωρήσει. Ο κάθε χρήστης λοιπόν έχει πρόσβαση στο δίκτυο και χρησιμοποιώντας το εκάστοτε κρυπτονόμισμα δύναται να συμμετάσχει στο επίπεδο λειτουργιών που επιθυμεί. Για παράδειγμα μπορεί να συμμετέχει στο σύστημα σαν απλός χρήστης ή να λάβει μέρος σε πιο σύνθετες λειτουργίες όπως είναι η συμμετοχή στην επαλήθευση και επικύρωση των συναλλαγών. Επιπλέον το δίκτυο έχει συνήθως έναν μηχανισμό παροχής κινήτρων κατά τον οποίο οι χρήστες κερδίζουν κρυπτονομίσματα κατά την επαλήθευση και επικύρωση των συναλλαγών τους, προκειμένου να ενθαρρύνει περισσότερους συμμετέχοντες να ενταχθούν σε αυτό και να χρησιμοποιήσουν το κρυπτονόμισμα.

Αξιοσημείωτο κρίνεται και το γεγονός ότι τα δημόσια Blockchains τείνουν να είναι πιο ασφαλή από τους υπόλοιπους τύπους Blockchain λόγω του ότι κανένας οργανισμός ή κυβέρνηση δεν ελέγχει το δίκτυο και η συμμετοχή γίνεται ανώνυμα. Ο κώδικας με τη σειρά του ανανεώνεται αποκλειστικά από την κοινότητα του κάθε Blockchain δικτύου στην οποία συμμετέχουν εθελοντικά προγραμματιστές.

Εξετάζοντας τα μειονεκτήματα των δημόσιων Blockchains καθίσταται φανερό ότι απαιτείται σημαντικό ποσό υπολογιστικής ισχύος για να επιτευχθεί ο συγχρονισμός και η διατήρηση του κατανεμημένου βιβλιαρίου. Επίσης το δημόσιο Blockchain είναι συχνά πιο αργό από τους υπόλοιπους τύπους Blockchain και με τη συνεχόμενη αύξηση των συναλλαγών αντιμετωπίζει προβλήματα αποθηκευτικού χώρου [72].

3.8.2 **Permissioned**

Το εξουσιοδοτημένο Blockchain διατηρεί και αυτό ένα κατανεμημένο βιβλιάριο δεδομένων, όμως η συμμετοχή σε αυτό ελέγχεται από μια κεντρική αρχή. Η κεντρική αυτή αρχή γνωρίζει τους συμμετέχοντες και δίνει το δικαίωμα επικύρωσης των συναλλαγών σε έμπιστα προς αυτούς άτομα. Αυτό το χαρακτηριστικό διευκολύνει την αύξηση του όγκου των συναλλαγών που πραγματοποιούνται ημερησίως και ταυτόχρονα τα εξουσιοδοτημένα δίκτυα μπορούν να είναι πολύ γρήγορα με μεγαλύτερη αποθηκευτική χωρητικότητα. Επίσης ο βασικός κώδικας του κάθε εξουσιοδοτημένου Blockchain μπορεί να εκδίδεται ανοιχτά προς όλους για να τον επιθεωρήσουν ή και όχι [73].

3.8.3 **Private**

Τα ιδιωτικά Blockchains τείνουν να είναι πολύ πιο μικρά σε αριθμό συμμετεχόντων σε σχέση με τους υπόλοιπους τύπους Blockchain. Ενδέχεται μάλιστα ο κόσμος να μην γνωρίζει καν την ύπαρξή τους επειδή τις περισσότερες φορές δεν είναι ορατά στο κοινό . Η συμμετοχή κάθε χρήστη είναι ελεγχόμενη από μια κεντρική αρχή. Ως προς τα χαρακτηριστικά τους θα πρέπει να αναφερθεί ότι είναι πολύ πιο γρήγορα από τους υπόλοιπους τύπους και ενδέχεται να μην παρουσιάζουν καμία καθυστέρηση στο χρόνο επικύρωσης των δεδομένων. Έχουν επίσης χαμηλό κόστος λειτουργείας, απεριόριστη χωρητικότητα και μπορούν να κατασκευαστούν σε πολύ

γρήγορο χρονικό διάστημα. Εντούτοις τα περισσότερα ιδιωτικά Blockchain δεν χρησιμοποιούν κρυπτονόμισμα και δεν έχουν την ίδια ασφάλεια που παρέχει ένα αποκεντρωμένο Blockchain δίκτυο [74].

Η διαφορετικές εφαρμογές της τεχνολογίας που αναφέρθηκαν διαχωρίζουν την τεχνολογία σε δύο κατηγορίες. Η πρώτη αφορά τις περιπτώσεις των εφαρμογών blockchain (ή κατανεμημένων κατάστιχών) που ο καθένας μπορεί να συμμετέχει σε όλες τις διεργασίες μέσα σε αυτό και παράλληλα να συμβάλλει στην εξέλιξη του αν το επιθυμεί. Η περίπτωση αυτή είναι γνωστή ως «μη αδειοδοτούμενα blockchain » (permissionless blockchain). Σε αυτή την κατηγορία ανήκουν το Bitcoin και το Ethereum.

Η δεύτερη περίπτωση αφορά εφαρμογές blockchain όπου οι χρήστες δεν έχουν τις ίδιες ιδιότητες μέσα στο δίκτυο. Στην περίπτωση του δικτύου του Ripple που θα αναλυθεί στην συνέχεια, οι κόμβοι που διαχειρίζονται την επικύρωση των συναλλαγών και την μεγέθυνση του κατανεμημένου κατάστιχου είναι συγκεκριμένοι και ορισμένοι από τους ιδιοκτήτες οι οποίοι είναι υπεύθυνοι για την εξέλιξη και την λειτουργία του. Οι συγκεκριμένες υλοποιήσεις όπου εφαρμόζουν αυτές τις πρακτικές είναι γνωστές ως αδείοδοτούμενα blockchain (permissioned blockhain) [75]. Ο Buterin [76] τις διαχωρίζει ως blockchain κοινοπραξίας (consortium blockchains)

Το έντονο ενδιαφέρον αρκετών εταιριών (όπως η IBM) για την τεχνολογία του blockchain οδήγησε αρκετές από αυτές να αναπτύξουν δικές τους υλοποιήσεις κατανεμημένου κατάστιχου. Πρόκειται για «δομές» (frameworks), οι οποίες στοχεύουν στην υλοποίηση ιδιωτικών δικτύων. Τα συγκεκριμένα δίκτυα διαχειρίζονται αποκλειστικά από την επιχείρηση ή τις επιχειρήσεις που το υλοποιούν. Το ίδιο ισχύει και τις διαδικασίες επικύρωσης. Ωστόσο, η βασικότερη διαφορά με τις υλοποιήσεις στις δύο προηγούμενες υποκατηγορίες που αναφέρθηκαν, είναι ότι για την συμμετοχή στο δίκτυο είναι ελεγχόμενη από τον «ιδιοκτήτη» του δικτύου [77].

3.8.4 **Χαρακτηριστικά των διαφορετικών κατηγοριών του Blockchain**

Για την ανάλυση των βασικών χαρακτηριστικών γίνεται αναφορά των γενικών χαρακτηριστικών της τεχνολογίας του blockchain. Ο διαμοιρασμός μίας κοινής βάσης δεδομένων αλλά και όλων των διαδικασιών σε αυτό είναι ίσως το πιο διακριτό χαρακτηριστικό ενός blockchain δικτύου, στοιχείο που ενισχύει την διαφάνεια ως προς την διεκπεραίωση των συναλλαγών μέσα στο δίκτυο. Παράλληλα η αδυναμία αλλαγής ή των δεδομένων δημιουργούν μια αμετάβλητη βάση δεδομένων.

3.8.4.1 Public Permissionless blockchain

Ο Evans [77] αναφέρει ότι όλες οι κατανεμημένες δημόσιες πλατφόρμες πληρωμών έχουν τα εξής χαρακτηριστικά:

1. Βασίζονται στο διαδίκτυο και συγκεκριμένα σε όσους θέλουν να διαθέσουν την επεξεργαστική ισχύ του υπολογιστή τους για την λειτουργία τους (χωρίς να υπάρχει

περιορισμός ως προς την συμμετοχή) σε αντίθεση με άλλες πλατφόρμες που χρησιμοποιούν ιδιωτικά δίκτυα (όπως η Visa).

2. Έχουν ένα πρωτόκολλο το οποίο είναι απαραίτητο για την μεταφορά των νομισμάτων και την αποθήκευση τους στο blockchain το οποίο βασίζεται στην κρυπτογραφία (όπως έχει περιγραφεί στη δεύτερη ενότητα για την περίπτωση του bitcoin) δημιουργώντας ένα δίκτυο το οποίο . Παράλληλα συμβάλει στην επίτευξη συναίνεσης μέσα σε αυτό.
3. Περιέχουν τα εικονικά νομίσματα τα οποία χρησιμοποιούνται για την μεταφορά αξίας.
4. Υπάρχει ένα ανταποδοτικό σύστημα το οποίο ανταμείβει όσους συμμετέχουν στην αποθήκευση των συναλλαγών για την επεξεργαστική ισχύ και τους πόρους που δαπανούν.
5. Χρησιμοποιούν ένα ανοιχτού κώδικα λογισμικό επιτρέποντας δηλαδή την χρήση του και την συμμετοχή στην επεξεργασία του από τον καθένα.
6. Το σύστημα διακυβέρνησης που χρησιμοποιούν είναι παρόμοιο με αυτό του ανοιχτού κώδικα και βασίζεται κυρίως σε εθελοντές για την εξέλιξή του.
7. Επιπλέον σε αυτά μπορεί να προστεθεί η δυνατότητα της απόκρυψης των στοιχείων των χρηστών μέσω της κρυπτογραφίας και συγκεκριμένα της τεχνολογίας δημόσιου/ιδιωτικού κλειδιού. Η συγκεκριμένη τεχνολογία επιτρέπει την διατήρηση της ανωνυμίας μέσα στο δίκτυο, καθώς δεν υπάρχει κάποιος κεντρικός πάροχος που να ελέγχει και να ταυτοποιεί τους χρήστες των πλατφορμών. Παράλληλα η δυνατότητα χρήσης πολλαπλών κλειδιών δυσκολεύει ακόμη περισσότερο την ταυτοποίηση των χρηστών. Επομένως ενώ οι συναλλαγές είναι εμφανής στον καθένα, η ταυτοποίηση των χρηστών είναι πρακτικά αδύνατη.

3.8.4.2 Πλεονεκτήματα-Μειονεκτήματα της χρήσης public permissionless blockchain πλατφορμών

Τα βασικό πλεονέκτημα μιας public permissionless blockchain είναι η ετοιμότητα ως προς την χρήση για την επίτευξη των συναλλαγών. Πρόκειται δηλαδή για έτοιμες πλατφόρμες στις οποίες ο χρήστης μπορεί να τις χρησιμοποιήσει εφόσον διαθέτει πορτοφόλι δηλαδή ένα δημόσιο και ένα ιδιωτικό κλειδί. Σε κάποιες περιπτώσεις το κόστος συναλλαγής μπορεί να είναι χαμηλό και η ταχύτητα των συναλλαγών αυξημένη σε σχέση με τους συμβατικούς τρόπους συναλλαγών.

Τα μειονεκτήματα των public permssionless blockchain δικτύων είναι αρκετά όπως αναλύονται στις επόμενες παραγράφους. Τα βασικά προβλήματα μιας τέτοιας πλατφόρμας απορρέουν κατά κύριο λόγο με την έλλειψη κεντρικής αρχής, την έντονη εξάρτηση από τις τεχνολογίες της πληροφορίας και την ανωνυμία των χρηστών.

Η δημιουργία ενός δικτύου που η εμπιστοσύνη μεταξύ των συμμετεχόντων δεν είναι απαραίτητη έχει όμως και αρκετά μειονεκτήματα. Το πρωτόκολλο συναίνεσης Proof-of-Work που χρησιμοποιείται σε αυτές τις περιπτώσεις που αναλύθηκαν δημιουργεί προβλήματα στην μεγέθυνση του δικτύου και στην ταχύτητα των συναλλαγών. Στην περίπτωση του bitcoin

παράγεται κατά μέσο όρο 1 block ανά 10 λεπτά. Παράλληλα ο αριθμός των συναλλαγών που επεξεργάζεται είναι περίπου 2 ανά δευτερόλεπτο. Το πρόβλημα είναι εμφανές αν συγκριθεί με το αριθμό διαχείρισης συναλλαγών της Visa που υπολογίζεται περίπου στις 4000 συναλλαγές ανά δευτερόλεπτο.

Η συνεχής μεγέθυνση ενός public permissionless blockchain δημιουργεί έντονο ανταγωνισμό μεταξύ των κόμβων που διαχειρίζονται την διαδικασία της επικύρωσης (δηλαδή την διεργασία του mining). Παράλληλα, σε συνδυασμό με τον σταθερό μέσο αριθμό των παραγόμενων blocks, η διαδικασία του Proof-Of-Work (δηλαδή η επίλυση του προβλήματος που περιγράφεται στα προηγούμενα κεφάλαια) γίνεται ενεργειακά δαπανηρή. Συγκεκριμένα στην περίπτωση του Bitcoin, η ετησία κατανάλωση ενέργειας υπολογίζεται πλέον σε 24TWh που αντιστοιχεί στην ετήσια κατανάλωση ενέργειας ολόκληρης της Ιρλανδίας [78].

Η δυσκολία ως προς την κατανόηση του τρόπου λειτουργίας και τη συμμετοχή σε πλατφόρμες κρυπτονομισμάτων (δηλαδή την αγορά και την ανταλλαγή τους) για τους χρήστες είναι ένα βασικό μειονέκτημα των public permssionless blockchain. Αυτό μπορεί να οδηγήσει σε παρανοήσεις και πιθανές ζημίες για τους χρήστες [79].

Η έλλειψη Κεντρικής Αρχής, που να ελέγχει τα κρυπτονομίσματα, όπως οι Κεντρικές Τράπεζες και το Διεθνές Νομισματικό Ταμείο που επιτηρούν τα χρηματοπιστωτικά ιδρύματα, δημιουργεί κινδύνους ως προς την χρήση τους. Η συνέχεια της λειτουργίας της μιας public permssionless blockchain πλατφόμας βασίζεται καθαρά στην ύπαρξη των κόμβων επικύρωσης (miners). Τα κίνητρά τους για την συνέχεια της προσφοράς των υπολογιστικών πόρων που διαθέτουν στο σύστημα βασίζεται μόνο στα οικονομικά κίνητρα (δηλαδή την παραγωγή νέων νομισμάτων και τα κόστη συναλλαγής που συλλέγουν από την συγκεκριμένη διαδικασία) που τους παρέχει το δίκτυο χωρίς να υπάρχει κάποιος δεσμευτικός όρος που να τους δεσμεύει να συνεχίσουν την διαδικασία. Συνεπώς υπάρχει πιθανότητα διακοπής της λειτουργίας ανά πάσα στιγμή αφήνοντας τους ιδιοκτήτες των κρυπτονομισμάτων με νομίσματα άνευ αξίας.

Η μείωση των miners μπορεί να επέλθει και από άλλες διαδικασίες όπως την διαδικασία του Hard-Fork. Η άγνοια του συστήματος για την υπολογιστική ισχύ που κατέχει ο κάθε κόμβος είναι ένα σημαντικό μειονέκτημα.

Η πιθανότητα χρεοκοπίας ή κλοπής νομισμάτων από ανταλλακτήρια κρυπτονομισμάτων είναι ένα υπαρκτό πρόβλημα σε αυτές τις πλατφόρμες μπορεί να οδηγήσει σε απώλεια των νομισμάτων των χρηστών τους. Καθώς τα περισσότερα ανταλλακτήρια δεν επιβλέπονται από κάποια ρυθμιστική αρχή είναι πολύ πιθανό η απώλεια αυτή να είναι μη αναστρέψιμη. Χαρακτηριστικά παραδείγματα τέτοιων περιπτώσεων είναι η χρεοκοπία του ανταλλακτηρίου Mt Gox τον Φεβρουάριο του 2014 που οδήγησε σε απώλεια χιλιάδων Bitcoin από τους χρήστες του ανταλλακτηρίου ενώ τον Ιανουάριο του 2015 κλάπηκαν 19.000 Bitcoin από το ανταλλακτηρίο Bitcoin [79].

Η έλλειψη Κεντρικής Αρχής, καθιστά αδύνατη την επίλυση την περιπτώσεων όπως η μη εγκεκριμένη από το χρήστη συναλλαγή, η μεταφορά λανθασμένου ποσού ή μεταφορά νομισμάτων σε λάθος χρήστη. Επιπλέον, η αδυναμία αναγνώρισης του παραλήπτη καθώς η συναλλαγές γίνονται μόνο με την χρήση της τεχνολογίας δημόσιων/ιδιωτικών κλειδιών οδηγούν σε μη αντιστρέψιμη απώλεια για τον αποστολέα. Σε ότι αφορά τα έξυπνα συμβόλαια, η έλλειψη ρυθμιστικού πλαισίου ή Κεντρικής Αρχής που να ρυθμίζει την σύναψη συμβολαιακών σχέσεων δημιουργεί ερωτήματα ως προς την χρηστικότητά τους, ιδιαίτερα σε περιπτώσεις διαφωνιών μεταξύ των συναλλασσόμενων.

Αν και υπάρχει διαφάνεια ως προς τις συναλλαγές καθώς στο σύνολο τους αποθηκεύονται στην κατανεμημένη και αμετάβλητη βάση δεδομένων του blockchain ουσιαστικά σε αυτές αποθηκεύονται μόνο τα ψευδώνυμα δηλαδή των χρηστών (δηλαδή οι διευθύνσεις των πορτοφολιών τους) ενώ υπάρχει δυνατότητα χρήσης περισσότερων από ένα πορτοφολιών. Η αδυναμία σύνδεσης των χρηστών με τα ψευδώνυμα επιτρέπει την χρήση των συγκεκριμένων πλατφορμών για παράνομών και δόλιων διαδικασιών όπως αγοροπωλησίες παράνομών ουσιών και ξέπλυμα χρημάτων [80].

Η έντονη εξάρτηση των permissioned public blockchain πλατφορμών από τις τεχνολογίες της πληροφορικής και των δικτύων δημιουργούν είναι ένα μειονέκτημα των συγκεκριμένων πλατφορμών. Πιθανά τεχνικά προβλήματα στο δίκτυο ή περιπτώσεις κυβερνοεπιθέσεων είναι συχνό φαινόμενο. Επιπλέον, σε επίπεδο χρήστη η απώλεια των ιδιωτικών κλειδιών στα οποία αποθηκεύονται τα κρυπτονομίσματα μπορεί να οδηγήσει σε μη αντιστρέψιμη απώλειά τους.

Ένα από τα βασικότερα προβλήματα των κρυπτονομισμάτων είναι έντονες αυξομειώσεις στην συναλλαγματική αξία των νομισμάτων. Όπως έχει ήδη αναλυθεί στο δεύτερο κεφάλαιο, η τιμή του Bitcoin (αλλά και γενικότερα στις περισσότερες περιπτώσεις κρυπτονομισμάτων) η συναλλαγματική τους αξία παρουσιάζει έντονες αυξομειώσεις. Συγκεκριμένα σε διάστημα λιγότερο των 2 μηνών (από 16 Δεκεμβρίου του 2017 μέχρι 5 Φεβρουαρίου του 2018) η συναλλαγματική του αξία έπεσε από τις 19.343,04$ στις 6.914,26$. Το ίδιο ισχύει και για τα κόστη συναλλαγής. Για την ίδια περίοδο παρατηρείται μία μείωση στο μέσο κόστος συναλλαγής από 26,893$ στα 6,193$.

Τέλος, η δυνατότητα εξερεύνησης και ελέγχου κάθε συναλλαγής μέσα στο δίκτυο είναι ένας περαιτέρω λόγος που αποτρέπει τα χρηματοπιστωτικά ιδρύματα την χρήση αυτής της κατηγορίας πλατφορμών για λόγους ιδιωτικότητας και προστασίας των συναλλαγών. Ο Peter και Panayi [92] κάνουν αναφορά για την σημασία της διαθεσιμότητας, της ακεραιότητας και της ασφάλειας και της ιδιωτικότητα των δεδομένων σε εταιρίες και οργανισμούς. Η ιδωτικότητα των συναλλαγών δεν είναι ένα στοιχεία αυτής της κατηγορίας του blockchain, καθώς τα στοιχεία των συναλλαγών διαμοιράζονται σε όλους τους κόμβους του δικτύου, κάτι που θέτει σε κίνδυνο την ασφάλεια των πληροφοριών των συναλλαγών. Παράλληλα η διαθεσιμότητα των δεδομένων των συναλλαγών σε όλους τους κόμβους αυξάνει τον κίνδυνο ακεραιότητας των δεδομένων.

3.8.4.3 Public permissioned blockchain πλατφόρμες

Τα χαρακτηριστικά μιας public permissioned blockchain πλατφόρμας είναι τα εξής:

1. Η λειτουργία του βασίζεται σε ένα συγκεκριμένο διαχειριστή που είναι ο ιδιοκτήτης της
2. Βασίζεται, όπως και στην προηγούμενη κατηγορία, στην κρυπτογραφία για την μεταφορά, την αποθήκευση και την συναίνεση μεταξύ των κόμβων, υιοθετώντας ένα πρωτόκολλο το οποίο διαφέρει από το αντίστοιχο των permissionless πλατφορμών καθώς οι κόμβοι επικύρωσης είναι ορισμένοι από το ιδιοκτήτη.
3. Είναι πιθανή η χρήση εικονικών νομισμάτων για την μεταφορά αξίας αλλά όχι απαραίτητη.
4. Δεν υπάρχει ανταποδοτικό σύστημα σε όσους συμμετέχουν στην αποθήκευση και επικύρωση των συναλλαγών (τουλάχιστον όχι άμεσο όπως στην προηγούμενη περίπτωση).
5. Χρησιμοποιούν ένα λογισμικό το οποίο είναι ανοιχτού κώδικά και επιτρέπουν την συμμετοχή αλλά όχι την επικύρωση από τον καθένα.
6. Η διακυβέρνηση του συστήματος γίνεται από τον ιδιοκτήτη της πλατφόρμας.
7. Παρόλο που χρησιμοποιείται η τεχνολογία του δημόσιου/ιδιωτικού κλειδιού, η ανωνυμία είναι περιορισμένη γιατί οι πάροχοι των συγκεκριμένων κλειδιών για την συμμετοχή στο δίκτυο είναι ορισμένοι από τον ιδιοκτήτη και ακολουθούν τις διαδικασίες αναγνώρισης του πελάτη.

3.8.4.4 Πλεονεκτήματα-Μειονεκτήματα χρήσης public permissioned blockchain πλατφορμών

Το βασικό πλεονέκτημα, όπως και στην προηγούμενη περίπτωση, είναι ότι πρόκειται για έτοιμες προς χρήση πλατφόρμες, που ωστόσο διεκπεραιώνουν τις συναλλαγές μέσα σε πολύ λίγα δευτερόλεπτα και με σχετικά χαμηλότερο κόστος σε σχέση με τις συμβατικές μεθόδους συναλλαγών, εφόσον ο χρήστης διαθέτει εφόσον διαθέτει πορτοφόλι δηλαδή ένα δημόσιο και ένα ιδιωτικό κλειδί. Παράλληλα επιτρέπει τις συναλλαγές εντός του δικτύου και άλλων νομισμάτων με την χρήση των πυλών (gateways) οι οποίοι είναι υπεύθυνοι για την αποθήκευση και την έκδοση του ψηφιακού νομίσματος.

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

Η χρήση ενός εικονικού νομίσματός, για την επίτευξη των συναλλαγών, που δεν ελέγχεται από Κεντρική Αρχή και δεν υπόκειται σε κάποιο ρυθμιστικό πλαίσιο μπορεί να οδηγήσει σε καταστροφικές συνέπειες για τους χρήστες. Χαρακτηριστικά, οι αυξομειώσεις της συναλλαγματικής αξίας των νομισμάτων από πιθανή χειραγώγηση της αγοράς, αλλά και προβλήματα όπως η μη εγκεκριμένη αποστολή νομισμάτων ή η αποστολή εικονικών νομισμάτων σε λάθος χρήστη είναι αδύνατο να επιλυθούν λόγω της έλλειψης Κεντρικής Αρχής. Παράλληλα

η δυσκολία ως προς την κατανόηση του τρόπου λειτουργίας και τη συμμετοχή σε πλατφόρμες κρυπτονομισμάτων ισχύει και σε αυτή την κατηγορία πλατφορμών.

Η πιθανότητα χρεωκοπίας ή κλοπής των εικονικών νομισμάτων, από ανταλλακτήρια που δεν διέπονται από κάποιο ρυθμιστικό πλαίσιο, υπάρχει και σε αυτή την περίπτωση όπως και η πιθανότητα απώλειας ή κλοπής των ιδιωτικών κλειδιών. Και στις δύο περιπτώσεις ο χρήστης οδηγείται σε μη αντιστρέψιμη απώλεια των εικονικών νομισμάτων. Επιπλέον χρήση των συγκεκριμένων πλατφορμών για συναλλαγές που σχετίζονται με παράνομες διαδικασίες είναι πιθανή και σε αυτή την περίπτωση. Αυτό συμβαίνει λόγω της αδυναμίας της ταυτοποίησης των χρηστών μέσα από την χρήση του δημόσιου/ιδιωτικού κλειδιού. Αν και πλατφόρμα του Ripple, που ανήκει στην συγκεκριμένη περίπτωση, δεν ενδείκνυται για τέτοιες χρήσεις (καθώς υπάρχουν άλλες πλατφόρμες της προηγούμενης κατηγορίας που διακρίνονται για την ανωνυμία των χρηστών τους) ο κίνδυνος είναι ορατός.

Καθώς ο ιδιοκτήτης της πλατφόρμας ορίζει συγκεκριμένου κόμβους για την επικύρωση των συναλλαγών, η λειτουργία και η σταθερότητα της πλατφόρμας είναι αρμοδιότητα του πάροχου. Επομένως τίθεται το θέμα της αξιοπιστίας ως προς πάροχο για την συνέχεια λειτουργίας του δικτύου. Αν και οι κόμβοι επικύρωσης δεν έχουν κάποιο οικονομικό κίνητρο όπως στην προηγούμενη περίπτωση, η «σύμβαση» για την λειτουργία των κόμβων επικύρωσης γίνεται με τον πάροχο της πλατφόρμας.

Τέλος, σε ότι αφορά την ακεραιότητα την ιδιωτικότητα των δεδομένων των συναλλαγών, στοιχείο που επιζητούν οι επιχειρήσεις και τα χρηματοπιστωτικά ιδρύματα, το πρόβλημα συνεχίζει να υφίσταται όπως στην προηγούμενη περίπτωση καθώς τα δεδομένα αποστέλλονται σε όλους τους κόμβους επικύρωσης αλλά και στο ευρύ κοινό.

3.8.4.5 Χαρακτηριστικά private blockchain πλατφορμων

Τα χαρακτηριστικά μια private blockchain πλατφορμας είναι τα εξής:

1. Πρόκειται για «δομές» (frameworks) που εφαρμόζονται εντός ενός οργανισμού ή μεταξύ οργανισμών για την βελτίωση συγκεκριμένων διαδικασιών. Στην περίπτωση του εγχειρήματός Ubin ο αρχικός στόχος ήταν η δημιουργία μιας αποκεντρωμένης πλατφόρμας για την επίτευξη των διακανονισμών σε συνεχή χρόνο.
2. Χρησιμοποιείται και σε αυτή την περίπτωση πρωτόκολλα βασισμένα στην κρυπτογραφία για τις συναλλαγές και την επίτευξη συμφωνίας των συμμετεχόντων μέσα σε αυτό.
3. Δεν περιέχουν εικονικά νομίσματα όπως στις προηγούμενες κατηγορίες. Στην περίπτωση του Ubin δημιουργήθηκε ένα ψηφιακό νόμισμα που υπεύθυνη για την έκδοση του ήταν η Κεντρική Τράπεζα της Σιγκαπούρης και αντικατόπτριζε το συμβατικό νόμισμα.
4. Δεν υπάρχει ανταποδοτικό σύστημα για τους κόμβους επικύρωσης καθώς οι ίδιοι οι συμμετέχοντες αναλαμβάνουν την συγκεκριμένη διαδικασία.

5. Οι δομές που χρησιμοποιούν μπορεί να είναι ανοιχτού κώδικα, ωστόσο στις συγκεκριμένες υλοποιήσεις έχουν πρόσβαση μόνο οι συμμετέχοντες.
6. Η διακυβέρνηση του δικτύου γίνεται από τον χρήστη ή τους χρήστες που είναι υπεύθυνοι για την σταθερότητα και την εξέλιξή του.
7. Η χρήση κρυπτογραφίας για την ενίσχυση της ανωνυμίας δεν ισχύει σε αυτή την περίπτωση καθώς μιλάμε για ένα δίκτυο που δημιουργήθηκε από τους ίδιους τους χρήστες και δεν επιτρέπει την συμμέτοχη σε νέους χωρίς την έγκριση του διαχειριστή. Ωστόσο, ενδέχεται να χρησιμοποιηθεί για την ενίσχυση της ιδιωτικότητας των πληροφοριών των συναλλαγών (όπως συνέβη στην περίπτωση του εγχειρήματος Ubin, αποτρέποντας σε κάποιες περιπτώσεις τους μη συμμετέχοντες από τον έλεγχο των πληροφοριών των συναλλαγών).

3.8.4.6 Πλεονεκτήματα Μειονεκτήματα των private blockchain πλατφορμών

Η συγκεκριμένη κατηγορία αναφέρεται σε κλειστά δίκτυα, τα οποία έχουν ως στόχο να αντικαταστήσουν τα υπάρχοντα κεντρικά συστήματα των οργανισμών βελτιώνοντας πιθανά προβλήματα όπως σφάλματα που οφείλονται στην δομή ενός κεντρικού συστήματος, αυξάνοντας την διαλειτουργικότητα και την ταχύτητα των συναλλαγών. Επιπλέον, η ιδιωτικότητα και η ασφάλεια των πληροφοριών των συναλλαγών μεταξύ των συμμετεχόντων παραμένει σταθερή.

Τα μειονεκτήματα σε αυτή την περίπτωση πλατφορμών σχετίζονται κυρίως με την σύνδεση τους στο υπάρχον σύστημα των οργανισμών. Καθώς στις περισσότερες περιπτώσεις οι πλατφόρμες αυτές αντικαθιστούν κεντρικά συστήματα συγκεκριμένων διαδικασιών, όπως αναλύθηκε στο εγχείρημα Ubin, η προσαρμογή και η σύνδεση ενός κατανεμημένου δικτύου στα υπάρχοντα συστήματα μπορεί να παρουσιάσει αρκετές δυσκολίες. Συγκεκριμένα θα πρέπει να αναπτυχθεί ένα ρυθμιστικό πλαίσιο (όπως συμφωνίες σε επίπεδο παροχής υπηρεσιών μεταξύ των συμμετεχόντων και της Κεντρικής Τράπεζας της Σιγκαπούρης στο εγχείρημα Ubin) που να ορίζει τον τρόπο λειτουργίας της πλατφόρμας αλλά και την εγκυρότητα των συναλλαγών εντός αυτής. Επιπλέον η πιθανή μεγέθυνση ή τροποποίηση ενός κατανεμημένου δικτύου μπορεί να αυξήσει την πολυπλοκότητα των διαδικασιών. Σε αυτή την περίπτωση, η ταχύτητα των διαδικασιών μπορεί να μειωθεί αισθητά. Στην περίπτωση του Ubin το δίκτυο αποτελούταν από ένα περιορισμένο αριθμό τραπεζών (8 χρηματοπιστωτικά ιδρύματα), επιτρέποντας την διεκπεραίωση των συναλλαγών.

Για την λειτουργία και την χρήση ενός κατανεμημένου δικτύου οι οργανισμοί θα πρέπει να υιοθετήσουν νέες δεξιότητες σχετικές με το λογισμικό και τον εξοπλισμό που χρησιμοποιεί το κατανεμημένο δίκτυο. Συγκεκριμένα, απαιτούνται δεξιότητες σχετικές με τις τεχνολογίες πληροφοριών και με την κρυπτογραφία. Στην περίπτωση του εγχειρήματος Ubin, το ίδιο ισχύει και για την Κεντρική Τράπεζα της Σιγκαπούρης, η οποία είναι υπεύθυνη για την εύρυθμη λειτουργία και την εξέλιξη της πλατφόρμας. Παράλληλα, οι πάροχοι υπηρεσιών σύννεφου πρέπει να προσαρμόσουν τον εξοπλισμό τους για την εφαρμογή ενός κατανεμημένου δικτύου. Οι δομές σε αυτή την περίπτωση αναπτύσσονται από εταιρίες πληροφορικής ή εταιρίες συμβουλευτικής

όπως η Accenture και η Deloitte. Επομένως, οι συγκεκριμένες εταιρίες πρέπει να αναπτύξουν νέες δεξιότητες σχετικές με την δημιουργία δομών blockchain για κάθε περίπτωση εφαρμογής.

Τέλος σε ότι αφορά τους συμμετέχοντες, ανάπτυξη νέων δεξιοτήτων και το κόστος για την συμμετοχή σε ένα κατανεμημένο δίκτυο μπορεί να λειτουργήσει ως αντικίνητρο για την συμμετοχή τους σε αυτό. Ειδικότερα σε περιπτώσεις όπως του εγχειρήματος Ubin, η χρηστικότητα μιας private blockhain πλατφόρμας διαφέρει σε κάθε χρηματοπιστωτικό ίδρυμα με αποτέλεσμα η ανάπτυξη και η συμμετοχή τους κυρίως για μικρότερες επιχειρήσεις να θεωρείται ασύμφορη.

Στο παρακάτω πίνακα παρουσιάζονται τα κίνητρα και τα εμπόδια για την υιοθέτηση της blockchain τεχνολογίας στις τρεις κατηγορίες που αναλύθηκαν.

3.9 Η διακυβέρνηση των Blockchain δικτύων

Αν και η λειτουργία ενός Blockchain δικτύου δεν απαιτεί κάποια κεντρική διαχείριση ωστόσο η εξέλιξη και η συντήρηση και η διευθέτηση προβλημάτων του λογισμικού απαιτεί την συμμετοχή των ανθρώπινου παράγοντα. Στην περίπτωση του Bitcoin ο Satoshi Nakamoto παρέδωσε την διαχείριση του δικτύου στον προγραμματιστή Gavin Andersen. Αν και θεωρητικά η εξέλιξη εγχειρήματος, όπως σε όλα τα εγχειρήματα ανοιχτού κώδικα, στηρίζονται στο καθένα που θέλει να συμμετέχει στην εξέλιξή του. Ωστόσο μία ομάδα προγραμματιστών ορισμένη από τον Andersen πρέπει να αποδεχτεί αυτές τις αλλαγές για να ενσωματωθούν στην πλατφόρμα του Bitcoin. Οι συγκεκριμένοι προγραμματιστές ανήκουν στο Ίδρυμα του Bitcoin, ένα μη κερδοσκοπικό οργανισμό που στηρίζουν την λειτουργία του δικτύου. Το ίδιο ισχύει και για την περίπτωση του Ethereum με το Ethereum Foundation. Σε ότι αφορά τις αλλαγές στο δίκτυο, αυτές πρέπει να αποδεχθούν από τους κόμβους που συμμετέχουν στην διαδικασία του mining [81]. Σε αντίθετη περίπτωση, δηλαδή αν ένα ποσοστό δεν αποδεχτεί τις αλλαγές και συνεχίσει να λειτουργεί ως διαχωρισμένο δίκτυο δημιουργεί μία νέα πλατφόρμα blockchain. Η συγκεκριμένη διαδικασία ονομάζεται «hard fork». Στην περίπτωση του Bitcoin η συγκεκριμένη διαδικασία έχει συμβεί πολλές φορές δημιουργώντας νέα κρυπτονομίσματα με το πιο γνωστό από αυτά είναι το Bitcoin Cash. Όπως είναι προφανές, στην εξέλιξη των πρωτόκολλών των κρυπτονομισμάτων παίζουν σημαντικό ρόλο οι miners. Σύμφωνα με τους Hileman & Rauchs [94] πάνω από το 51% miners θεωρούν ότι η επιρροή στην εξέλιξη των κρυπτονομισμάτων είναι υψηλή έως πολύ υψηλή.

3.10 Πλατφόρμες blockchain για το IoT

3.10.1 **Blockchain και Internet of Things**

Με τον όρο Internet of Things αναφερόμαστε σ΄ ένα δίκτυο φυσικών αντικειμένων ενσωματωμένα με ηλεκτρονικά μέσα, λογισμικό, και διαφορετικά είδη αισθητήρων , με δυνατότητα σύνδεσης στο διαδίκτυο μέσω ετερογενών δικτύων πρόσβασης, ώστε να επιτρέπεται η ανταλλαγή πληροφορίας. Η έννοια ‘Thing’ αντικατοπτρίζει μία αρκετά μεγάλη ποικιλία συσκευών-κατασκευών όπως για παράδειγμα αυτοκίνητα, σπίτια, smartwatches, κάμερες

ασφαλείας κ.α. Σαν αποτέλεσμα μια τεράστια και σε ορισμένες περιπτώσεις real-time ροή δεδομένων μπορεί να παραχθεί αυτόματα από συνδεδεμένα πράγματα και αισθητήρες. Η συλλογή των δεδομένων Προβλέπεται πως δισεκατομμύρια φυσικά πράγματα ή αντικείμενα θα εξοπλιστούν με διαφορετικά είδη αισθητήρων και ενεργοποιητών και θα συνδεθούν στο διαδίκτυο, μετατρέποντας τα αντικείμενα του πραγματικού κόσμου σε εικονική πληροφορία.

Εικόνα 5: FUTURE SMART CITY – HOW THE INTERNET OF THINGS IS TRANSFORMING OUR CITIES

3.10.2 **Enigma**

Ο Guy Zyskind, ο Oz Nathan και ο Alex Sandy Pentland [95] ανέπτυξαν μία πλατφόρμα που ονομάζεται Enigma, ένα δίκτυο peer-to-peer το οποίο βασίζεται σε ένα αποκεντρωμένο σύστημα διαχείρισης των προσωπικών δεδομένων, που επιτρέπει σε διαφορετικά συμβαλλόμενα μέρη την από κοινού την αποθήκευση και τον υπολογισμό των δεδομένων, διατηρώντας παράλληλα τα δεδομένα εντελώς ιδιωτικά. Η πλατφόρμα αυτή εγγυάται την ιδιωτικότητα βάσει σχεδιασμού, συνδυάζοντας αποτελεσματικά blockchain τεχνολογία και offchain αποθήκευση δεδομένων. Το Enigma είναι μια αποκεντρωμένη πλατφόρμα υπολογισμού με εγγυημένη προστασία της ιδιωτικής ζωής. Στόχος στον σχεδιασμό του enigma ήταν η προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό, end-to-end αποκεντρωμένες εφαρμογές, χωρίς καμία ανάγκη για ένα έμπιστο τρίτο μέρος. Το Enigma είναι ιδιωτικό. Χρησιμοποιώντας ασφαλή multi-party υπολογισμούς (sMPC ή MPC), τα δεδομένα υπολογίζονται με ένα κατανεμημένο τρόπο, χωρίς ένα έμπιστο τρίτο μέρος. Τα δεδομένα είναι χωρισμένα μεταξύ των διαφόρων κόμβων και υπολογίζουν τις λειτουργίες μαζί, χωρίς διαρροή πληροφοριών σε άλλους κόμβους. Συγκεκριμένα, κανένας

μεμονωμένος κόμβος δεν έχει πρόσβαση στα δεδομένα στο σύνολό τους. Αντ'αυτού, κάθε κόμβος έχει ένα χωρίς νόημα κομμάτι από αυτό.

Το Enigma είναι επεκτάσιμο. Σε αντίθεση με τα κλασικά blockchains, οι υπολογισμοί και η αποθήκευση δεδομένων δεν αναπαράγονται από κάθε κόμβο στο δίκτυο. Μόνο ένα μικρό υποσύνολο κόμβων εκτελεί τους υπολογισμούς σε διαφορετικά τμήματα των δεδομένων. Το νέο πρόγραμμα Enigma φέρνει την ικανότητα να γίνονται υπολογισμοί στα δεδομένα, χωρίς υπάρχει πρόσβαση στο ίδια τα ανεπεξέργαστα δεδομένα. Σήμερα, η ανταλλαγή δεδομένων είναι μια μη αναστρέψιμη διαδικασία, από την στιγμή που θα αποσταλούν, δεν υπάρχει κανένας τρόπος δεν υπάρχει κανένας τρόπος να τα πάρουν πίσω. Η πρόσβαση σε δεδομένα για ασφαλής υπολογισμούς είναι αναστρέψιμη και ελεγχόμενη, αφού κανείς, αλλά μόνο ο αρχικός ιδιοκτήτης(ες) των δεδομένων μπορούν να δουν τα ανεπεξέργαστα δεδομένα. Αυτό αποτελεί μία θεμελιώδη αλλαγή στην τρέχουσες προσεγγίσεις για την ανάλυση των δεδομένων.

Το Enigma έχει σχεδιαστεί για να συνδεθεί σε ένα υπάρχον blockchain και να αναθέτει τους πολύπλοκους υπολογισμούς σε ένα δίκτυο off-chain. Όλες οι συναλλαγές διευκολύνονται από το blockchain, το οποίο επιβάλλει ελεγχόμενη πρόσβαση η οποία βασίζεται σε ψηφιακές υπογραφές και προγραμματιζόμενα δικαιώματα. Ο κώδικας εκτελείται τόσο στο blockchain (δημόσια μέρη) όσο και στο Enigma (ιδιωτικό ή υπολογισμός πολύπλοκων κομματιών). Η εκτέλεση του Enigma εξασφαλίζει την ιδιωτικότητα και την ορθότητα, ενώ ένα blockchain μόνο του μπορεί να εξασφαλίσει μόνο το τελευταίο. Οι αποδείξεις της ορθής εκτέλεσης αποθηκεύονται στο blockchain και μπορούν να ελεγχθούν. Παρέχεται μια scripting γλώσσα για το σχεδιασμό end-to-end αποκεντρωμένων εφαρμογών που χρησιμοποιούν ιδιωτικές συμβάσεις, οι οποίες είναι παραλλαγές των έξυπνων συμβάσεων που μπορούν να χειριστούν ιδιωτικές πληροφορίες (δηλαδή, η κατάστασή τους δεν είναι αυστηρά δημόσια). Η εκτέλεση του κώδικα στα blockchains είναι αποκεντρωμένη, αλλά δεν διανέμεται, έτσι ώστε κάθε κόμβος εκτελεί τον ίδιο κώδικα και διατηρεί την ίδια δημόσια κατάσταση. Στο Enigma, η υπολογιστική εργασία διανέμεται αποτελεσματικά σε όλο το δίκτυο. Τα κύρια χαρακτηριστικά του Enigma είναι:

- Off-blockchain αποθήκευση δεδομένων. Το Enigma προστατεύει την ιδιωτικότητακαι είναι σχεδιασμένο να είναι ανεκτικό σε σφάλματα. Αποτελείται από ένα αποκεντρωμένο off-chain κατανεμημένο hash-table (DHT), μια ιδιωτική αλυσίδα κόμβων προσβάσιμα μέσω του blockchain. Αποθηκεύει αναφορές στα δεδομένα, αλλά όχι τα ίδια τα δεδομένα, τα οποία χωρίζονται και διανέμονται τυχαία. Κανένας κόμβος δεν έχει πρόσβαση σε ολόκληρο το σύνολο των δεδομένων.
- Το blockchain. Λειτουργεί ως μη έμπιστος αυτοματοποιημένος διαχειριστής ελέγχου πρόσβασης. Αναγνωρίζει τους ιδιοκτήτες των δεδομένων, παρέχει ελεγχόμενη πρόσβαση σε άλλους κόμβους και χρησιμεύει ως απαραβίαστη καταγραφή των γεγονότων.
- Επιβολή υπολογισμού της ιδιωτικότητας . Το κατανεμημένο υπολογιστικό μοντέλο Enigma βασίζεται σε ασφαλή Multi Party Computation (MPC). Ερωτήματα δεδομένων και υπολογισμοί υποβάλλονται σε επεξεργασία με ένα εντελώς κατανεμημένο τρόπο,

χωρίς την ανάγκη από ένα τρίτο μέρος. Κάθε κόμβος εκτελεί υπολογισμούς πάνω σε διαφορετικά τμήματα των δεδομένων χωρίς την αποκρυπτογράφηση τους πρώτα και χωρίς την διαρροή των δεδομένων στους κόμβους. Το αποτέλεσμα εξασφαλίζεται μέσω ενός επαληθεύσιμου μυστικά μοιραζόμενου σχήματος.

- Off-chain βαριά επεξεργασία. Πολύπλοκοι υπολογισμοί και ανάλυση των δεδομένων γίνονται μόνο εκτός της αλυσίδας. Εφόσον οι συναλλαγές δεν αναπαράγονται σε κάθε κόμβο, το blockchain δεν έχει προβλήματα επεκτασιμότητας. Ο μειωμένος πλεονασμός στην αποθήκευση και στους υπολογισμούς των δεδομένων επιτρέπει ακόμη πιο πολύπλοκους υπολογισμούς.

Αξίζει να σημειωθεί ότι με τη χρήση του Enigma προκύπτουν κάποια οφέλη [82]:

- Κυριότητα δεδομένων και την ανταμοιβή: Οι χρήστες κατέχουν και ελέγχουν τους προσωπικά δεδομένα; μπορούν επίσης να λάβουν ένα κουπόνι ως αποζημίωση για τη χρήση των δεδομένων τους.
- Διαφάνεια και δυνατότητα ελέγχου: οι χρήστες μπορούν να παρακολουθούν ό, τι τα δεδομένα που συλλέγονται, πώς θα είναι προσβάσιμα και από ποιον.
- Λεπτομερής έλεγχο πρόσβασης: οι χρήστες μπορούν να τροποποιήσουν το σύνολο των δικαιωμάτων και να ανακαλέσουν την πρόσβαση σε δεδομένα που συλλέχθηκαν ανά πάσα στιγμή. Παραδοσιακές mobile εφαρμογές, αντίθετα, απαιτούν χρήστες να συμφωνήσουν σε ένα σύνολο δικαιωμάτων, έτσι ώστε να μπορούν μόνο αυτοί να μπορούν να αποχωρήσουν.
- Πρόσβαση στα δεδομένα και χρήση: οι ενδιαφερόμενα κόμβοι μπορούν να έχουν πρόσβαση και να χρησιμοποιούν τα δεδομένα, χωρίς να ανησυχούν για την ασφάλεια. Κίνδυνοι που σχετίζονται με την αλυσίδα διαχείρισης δεδομένων θα μειωθούν αναλόγως.
- Ελάχιστη ρυθμιστική παρέμβαση: νόμοι σχετικά με τη συλλογή, την αποθήκευση και την ανταλλαγή ευαίσθητων δεδομένων μπορεί να απλοποιηθεί.
- Ενσωματωμένη ρύθμιση: νομικό πλαίσιο μπορεί να ενσωματωθεί και να εκτελείται αυτόματα μέσω του blockchain κώδικα.
- Παροχή νομικών αποδεικτικών στοιχείων: το blockchain εξασφαλίζει την ακεραιότητα των δεδομένων και παρέχει ένα απαραβίαστο log των γεγονότων, ενεργώντας ως νομική απόδειξη για την πρόσβαση και την αποθήκευση δεδομένων.

3.10.3 **IOTA-TANGLE**

Το IOTA [83] είναι μια cryptocurrency πλατφόρμα η οποία δημιουργήθηκε από τον David Sønstebø και αναπτύχθηκε ειδικά για μικρο-πληρωμές και στοχεύει στο να γίνει ένα πρότυπο σύστημα διακανονισμού του IoT και της μηχανήςπρος-μηχανή (M2M) οικονομίας. Εκτός από τις επιχειρήσεις-προς-επιχειρήσεις εφαρμογές, το IOTA μπορεί επίσης να χρησιμοποιηθεί για τα νοικοκυριά και για wearable συσκευές. Για παράδειγμα, επιτρέπει στους χρήστες να έχουν την κυριότητα και να πωλούν τα δεδομένα τους σε πραγματικό χρόνο, αντί να παρακολουθούνται εν άγνοιά τους για ανάλυση της αγοράς.

Πιθανές IOTA εφαρμογές είναι αναμφίβολα πολύ υποσχόμενες. Όπως ο δημιουργός του επισήμανε, η αυξανόμενη ανάπτυξη του IoT οδηγεί στην εμφάνιση του λεγόμενου Fog and Mist Computing. Το Fog and Mist μειώνει την καθυστέρηση του δικτύου που υπάρχει όταν μεγάλα κέντρα δεδομένων Cloud, βρίσκονται πολύ μακριά από τις τελικές συσκευές. Ειδικότερα, το Fog ωθεί εφαρμογές μεγάλης υπολογιστικής έντασης στην πύλη, ενώ ο Mist ωθεί τις λιγότερο υπολογιστικά εντατικές εργασίες στις άκρες του δικτύου, δηλαδή προς τους ίδιους αισθητήρες και τους ενεργοποιητές της συσκευής.

Αναμένεται οι συναλλαγές στο Fog και Mist περιβάλλον να αυξηθούν εκθετικά, επιτρέποντας την άνοδο σε νέα επιχειρηματικά μοντέλα, προϊόντα και υπηρεσίες. Είναι ως εκ τούτου ζωτικής σημασίας για τη βιομηχανία να βασίζεται σε ένα real-time και αποκεντρωμένο σύστημα διακανονισμού, χωρίς καμία επιβάρυνση.

Το IOTA προσφέρει επίσης μια έγκυρη και μοναδική λύση για το πρόβλημα της ασφάλειας στο περιβάλλον IoT. Μέσα από hashes των δεδομένων, επιτρέπει την πιστοποιημένες, απαραβίαστες και αποκεντρωμένες συναλλαγές μεταξύ των συσκευών και των αισθητήρων, έτσι ώστε η αλληλεπίδραση μηχανής προς μηχανή να μπορεί να αυτοματοποιηθεί με έναν ασφαλή τρόπο.

Το IOTA είναι χτισμένο στην κορυφή του «Tangle», ένα ελαφρύ blockchain "χωρίς blocks" και το πιο σημαντικό χωρίς τέλη (fees), ένας βασικός παράγοντας για τη διατήρηση κόστουςαποτελεσματικότητας. Σύμφωνα με τα λόγια του Sønstebø, «το IOTA είναι σήμερα το μόνο έργο που λύνει το ζήτημα της κλιμάκωσης και των τελών χωρίς ad hoc λύσεις που θέτουν σε κίνδυνο την ακεραιότητα της ασφάλειας ή του αποκεντρωμένου χαρακτήρα της οικονομίας». Τα κύρια χαρακτηριστικά του IOTA-Tangle είναι:

- Η τυπική αλυσίδα των μπλοκ των δικτύων όπως το Bitcoin, έχει αντικατασταθεί από ένα κουβάρι ή DAG (directed acyclic graph), δηλαδή μία συλλογή κόμβων που δρα ως καθολικό προς την αποθήκευση των συναλλαγών.
- Το δίκτυο είναι ασύγχρονο και οι συναλλαγές επιβεβαιώνονται από τις άμεσες και έμμεσες εγκρίσεις των κόμβων. Δεν επιβάλλετε κανένας κανόνας προς την έγκριση, μόνο οι κανόνες αναφοράς υπάρχουν.
- Σε περίπτωση αντικρουόμενων συναλλαγών, ένας κόμβος αποφασίζει ποια συναλλαγή θα μείνει ορφανή μέσα από έναν αλγόριθμο που προβλέπει ποια συναλλαγή είναι πιο πιθανή να εγκριθεί από το δίκτυο.
- Οι κόμβοι πρέπει να λύσουν ένα απαιτητικό μαθηματικό παζλ για την επαλήθευση μιας συναλλαγής και θα πρέπει να διαδίδονται μέσω του δικτύου. Σε περίπτωση που ένας κόμβος είναι υπερβολικά χαλαρός, θα αφαιρεθεί από τους άλλους κόμβους.
- Οι συναλλαγές δεν εγκρίνονται σε blocks, αλλά μεμονωμένα και χωρίς καμία επιβάρυνση.

Τροφοδοτούμενη από το Tangle και από ανθεκτικούς κβαντικούς αλγορίθμους, η IOTA αρχιτεκτονική είναι αποτελεσματική, επεκτάσιμη, πολύ ελαφριά και σύμφωνα με τους προγραμματιστές, πιο ανθεκτική σε παραβιάσεις ασφάλειας από οποιαδήποτε άλλη

cryptocurrency πλατφόρμα. Επιπλέον, το IOTA είναι διαλειτουργικό, μπορεί να επικοινωνεί με άλλα καθιερωμένα blockchains όπως το Bitcoin και το Ethereum, παρέχοντας σημεία ελέγχου για αυτά τα δίκτυα και ενισχύοντας το οικοσύστημά τους. Πράγματι, η πρόθεση των προγραμματιστών με το IOTA δεν είναι να αντικαταστήσει τα ανοικτά blockchains εντελώς, αλλά να είναι συμπληρωματικό προς το τρέχων οικοσύστημα και να λειτουργεί σε συνδυασμό με αυτό. Η χρήση του IOTA-Tangle οδηγεί σε μία σειρά από οφέλη:

- Ένα από τα κύρια αποτελέσματα που θα φέρει η άφιξη του IoT στην κοινωνία, είναι η κατανομή των πόρων. Δεδομένου ότι ο αριθμός των συσκευών αυξάνεται και οι δύο αυτές ενεργοποιούν, αλλά και απαιτούν πολλούς τεχνολογικούς πόρους. Διαχείριση των εν λόγω πόρων είναι το κλειδί. Για να λειτουργήσει σωστά το IoT χρειάζεται ανοικτότητα και διαλειτουργικότητα, ακόμη και μεταξύ των ανταγωνιστών. Δεν υπάρχει κανένας λόγος να πιστεύουμε ότι οι εταιρείες θα υιοθετήσουν αυθόρμητα ένα αλτρουιστικά επιχειρηματικό μοντέλο, οπότε η αγορά θα εξυψωθεί οργανικά.
- Όπως τα σπίτια, οι δρόμοι και οι πόλεις μας βυθίζονται σε μια απέραντη θάλασσα αισθητήρων και ενεργοποιητών, θα υπάρξει μια αδιάκοπη ζήτηση για υπολογιστική ισχύ για να αναλύσει την αέναη ροή των δεδομένων από τους αισθητήρες αυτούς. Στέλνοντας τα δεδομένα πίσω στο σύννεφο για ανάλυση είναι πολύ δαπανηρό λόγω των περιορισμών του εύρους ζώνης και των καθυστερήσεων. Αντ 'αυτού το σύννεφο πρέπει να περιλαμβάνει τις συσκευές αυτές. Αυτό σημαίνει ότι θα δούμε έναν συνδυασμό των έξυπνων αισθητήρων, όπου η υπολογιστική ικανότητα εμπεριέχεται στον ίδιο τον αισθητήρα (Mist Computing), σε συνδυασμό με σταθμούς επεξεργασίας που απλώνονται (ομίχλη Computing). Οι IOTA μικρο-συναλλαγές επιτρέπουν τα δεδομένα του αισθητήρα στον κόμβο Α να υποβληθούν σε επεξεργασία με επεξεργαστές του κόμβου Β σε πραγματικό χρόνο. Σε αντάλλαγμα ο κόμβος Β μπορεί να χρησιμοποιήσει τα iotas που παίρνει αντισταθμίζεται με το να αγοράσει τα στοιχεία από τον κόμβο Α ή οποιονδήποτε άλλο τεχνολογικού πόρο από άλλο κόμβο μέσα σε αυτό το συμβιωτικό οικοσύστημα.
- Θα υπάρξουν δεκάδες δισεκατομμύρια αισθητήρων στον κόσμο μας μέχρι το 2025. Αυτά τα δεδομένα μπορεί να είναι χρήσιμα για παραπάνω από έναν κόμβο. Ωστόσο, λόγω των φυσικών περιορισμών του εύρους ζώνης, την αποθήκευση και την ενέργεια, καθώς και το κόστος του υλικού, είναι απίθανο ότι αυτά τα δεδομένα πραγματικού χρόνου θα μοιραστούν ελεύθερα, εκτός και αν οι ιδιοκτήτες αυτών των δεδομένων αισθητήρων αποζημιωθούν.
- Ακριβώς όπως θα υπάρξει μια περίσσεια υπολογιστική ισχύ εξαπλωμένη ως αποτέλεσμα του πολλαπλασιασμού των συσκευών, έτσι θα υπάρχει ένας τεράστιος χώρος αποθήκευσης. Αυτή η αδράνεια των πόρων αποθήκευσης θα μπορούσε εύκολα να γίνει χρήσιμη και πάλι με το πραγματικό χρόνο αποζημίωσης που λαμβάνει χώρα μέσω του IOTA.
- Ένα από τα μεγαλύτερα εμπόδια που αντιμετωπίζει ένα σύστημα IoT είναι το ζήτημα των παρεμβολών. Όλοι έχουμε έστω μία φορά την ενοχλητική εμπειρία της γειτονικής σύνδεσης στο internet που παρεμβαίνει με την δική μας, γεγονός που οδηγεί σε

αποσυνδέσεις και καθυστερήσεις. Για τον ελεύθερο χρόνο στο σπίτι είναι ενοχλητικό, όμως για την βιομηχανία και την κοινωνία των υποδομών μπορεί να είναι εξαιρετικά δαπανηρό. Μέσω μικρο-συναλλαγών μπορεί κανείς να αποζημιώσει και να παροτρύνει για την κοινή χρήση του δικτύου, μειώνοντας τον αριθμό των συνολικών ενεργών κόμβων σε ένα περιορισμένο χώρο και κατά συνέπεια τη μείωση των παρεμβολών.

- Με τη συνεχιζόμενη υιοθέτηση ηλιακών συλλεκτών και project για σπίτια όπως το Project Sunroof της Google και το Powerwall του Τέσλα, είναι δυνατόν να προβλέψει κάοπιος ένα μέλλον όπου η ενέργεια μπορεί να κατανεμηθεί. Και πάλι σε πραγματικό χρόνο αποζημίωση για κοινή χρήση αυτών των τεχνολογικών πόρων, θα ενεργοποιήσει νέες καινοτομίες και μια πιο δίκαιη διαβίωσης για όλους. Στην επερχόμενη εποχή της ασύρματης ενέργειας, είναι εύκολο να φανταστεί κανείς ηλιακούς συλλέκτες πώλησης ηλεκτρικής ενέργειας με αισθητήρες στη σκιά.

3.10.4 **ADEPT**

Με την από κοινού έρευνα της Samsung Electronics, η IBM αποτελεί μια από τις πρώτες εταιρίες που έκανε από τα πρώτα βήματα για κινηθεί προς την κατεύθυνση blockchain λύσεις για το IoT, με στόχο την ανάπτυξη ενός νέου επιχειρηματικού προτύπου και οράματος του κόσμου, την Οικονομία των Πραγμάτων. Σε ένα σχέδιο που κυκλοφόρησε τον Ιανουάριο του 2015 με τίτλο «ADEPT [84]: Μια επαγγελματική IoT προοπτική», η εταιρεία πρότεινε ένα έργο blockchain-based που ονομάζεται ADEPT, δηλαδή Αυτόνομη Αποκεντρωμένη Peer-to-Peer Τηλεμετρία (Autonomous Decentralized Peer-to-Peer Telemetry).

Η τελική έκδοση του εν λόγω εγγράφου εκδόθηκε στο διαδίκτυο, με τίτλο «Δημοκρατία των συσκευώνΔιασφαλίζοντας το μέλλον του IoT » (Device democracy - Saving the future of the Internet of Things). Η IBM αναγνωρίζει την αξία ενός blockchain με βάση την αποκεντρωμένη προσέγγιση στο IoT, προκειμένου να αποκτήσει μεγαλύτερη επεκτασιμότητα, αξιοπιστία, ασφάλεια, καθώς και προστασία.

Το αποτέλεσμα είναι «το Διαδίκτυο των Αποκεντρωμένων, Αυτόνομων Πραγμάτων» (“the Internet of Decentralized, Autonomous Things) μια δυναμική δημοκρατία αντικειμένων συνδεδεμένων με ένα καθολικό ψηφιακό μοχλό, το οποίο παρέχει στους χρήστες μια ασφαλή ταυτοποίηση και γνησιότητα. Η έννοια αυτή, στο όραμα της IBM, πρόκειται να διαμορφώσει ένα ολοκαίνουργιο μοντέλο επιχειρηματικότητας στο πολύ άμεσο μέλλον. Η αρχιτεκτονική ADEPT βασίζεται στο TeleHash (όπως το πρωτόκολλο ανταλλαγής μηνυμάτων), στο BitTorrent (ως ένα αποτελεσματικό στρώμα διανομής) και στο Ethereum (ως πλατφόρμα για τις έξυπνες συμβάσεις και Αποκεντρωμένες αυτόνομες οργανώσεις). Τα κύρια χαρακτηριστικά του ADEPT μπορούν να συνοψισθούν ως εξής [85]:

- Διαφανές σύστημα και πλήρως κατανεμημένο: Η επικύρωση των συναλλαγών γίνεται μέσω ενός συνδυασμού της απόδειξης εργασίας (proof-of-work) και την απόδειξη της συμμετοχής (proof-of-stake).

- Αρχιτεκτονική κατάλληλη για διαφορετικούς κόμβους: οι κόμβοι του δίκτυού μπορούν να διακριθούν ανάλογα με το επίπεδο της υπολογιστικής τους ισχύς και μνήμης:
    1. Απλοί Peers (π.χ. Raspberry Pi, Beaglebone, ή Arduino) έχουν χαμηλους πόρους: μπορούν να εκτελέσουν μηνυμάτων και λειτουργούν ως απλα πορτοφόλια, αλλά δεν είναι σε θέση να διαχειριστουν blockchain, αλλα μονον να αποκτήσουν τα blockchain συναλλαγών από άλλες αξιόπιστους Peers.
    2. Οι τυπικοί Peers είναι εξοπλισμένοι με υψηλότερα μέσα αποθήκευσης και πόρους επεξεργασίας, έτσι ώστε να μπορούν ανταποκριθούν στις απαιτήσεις των blockchain και να υποστηρίζουν απλούς Peers, ανάλογα με τις δυνατότητές τους. Καθώς το κόστος των chips πέφτει, η IBM αναμένει ότι ένας αυξανόμενος αριθμός των έξυπνων αντικειμένων θα είναι σε θέση να συμπεριλαμβάνονται σε αυτήν κατηγορία των κόμβων.
    3. Οι Peers ανταλλαγής ή ADEPT Peers έχουν μεγάλη μνήμη και υπολογιστική ισχύ, έτσι ώστε να είναι σε θέση να διαχειριστούν και να αποθηκεύουν πλήρη αντίγραφα blockchain. Μπορούν να φιλοξενήσουν αγορές και μπορούν να ανήκουν σε οργανώσεις ή σε άλλους εμπορικούς φορείς, παρέχοντας blockchain αναλυτικής υπηρεσίας και να είναι σε θέση να πραγματοποιήσουν σύνθετα ερωτήματα. Αυτοί οι κόμβοι αποτελούν τον πυρήνα της ADEPT φιλοσοφίας και τις γρήγορες διαδρομές ενός νέου οικονομικού προτύπου. Πράγματι, μπορούν εκτελέσουν το ρόλο των οικονομικών ανταλλαγών μεταξύ των κοινοτήτων, στο βαθμό που είναι σε θέση να εξισορροπήσουν τη ζήτηση και την παροχής υπηρεσιών, τα περιουσιακά στοιχεία και τα προϊόντα. Μπορούν να λάβουν υπόψη τους διαθέσιμους πόρους σε μια κοινότητα και να βρουν τους αγοραστές σε μια άλλη, εκτελώντας τη λειτουργία του «Ρευστοποίηση των περιουσιακών στοιχείων".
- Ένα μοντέλο με επίκεντρο τον χρήστη: συσκευές θα ενεργούν προς το καλύτερο συμφέρον του χρήστη και όχι των τρίτων (π.χ. κατασκευαστές, κυβερνήσεις ή φορείς παροχής υπηρεσιών).
- Blockchain από προεπιλογή: προϊόντα και συσκευές θα πρέπει να έχουν καταγραφεί από τον κατασκευαστή σε εάν καθολικό blockchain, κατά την έναρξη του κύκλου ζωής στους.

4 ΚΕΦΑΛΑΙΟ 4º - ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΩΝ BLOCKCHAINS

Βρισκόμαστε στην αρχή μιας νέας επανάστασης που ξεκίνησε μια περιθωριακή οικονομία στο Διαδίκτυο, δηλαδή ένα εναλλακτικό νόμισμα που ονομάστηκε bitcoin και εκδόθηκε και υποστηρίχτηκε όχι από μια κεντρική αρχή, αλλά από μια αυτοματοποιημένη συναίνεση μεταξύ των δικτυωμένων χρηστών [24]. Η πραγματικότητα της νέας επανάστασης είναι ότι δεν απαιτεί από τους χρήστες να εμπιστεύονται ο ένας τον άλλο, αλλά μέσω μιας αυτό-αστυνόμευσης ελέγχει οποιαδήποτε κακόβουλη προσπάθεια εξαπάτησης του συστήματος θα αποδειχθεί. Με ακριβή και τεχνικό ορισμό, το bitcoin είναι ψηφιακό ρευστό που διακινείται μέσα στο Διαδίκτυο σε ένα αποκεντρωμένο σύστημα χωρίς εμπιστοσύνη, χρησιμοποιώντας ένα δημόσιο βιβλίο που ονομάζεται Blockchain. Πρόκειται για μια νέα μορφή χρημάτων που συνδυάζει την κοινή χρήση αρχείων BitTorrent με κρυπτογράφηση δημόσιου κλειδιού. Από την έναρξή της το 2009, η Bitcoin δημιούργησε μια ομάδα μιμητών εναλλακτικών νομισμάτων, χρησιμοποιώντας την ίδια γενική προσέγγιση αλλά με διαφορετικές βελτιστοποιήσεις.

Με άλλα λόγια, το Blockchain αποτελεί έναν τύπο βάσης δεδομένων που δέχεται ένα πλήθος εγγραφών από τους χρήστες, τις οποίες τοποθετεί σε ένα φύλλο δεδομένων γνωστό ως block. Κάθε χρήστης διατηρεί ένα αντίγραφο αυτού του block. Καθώς οι εγγραφές αυξάνονται, κάθε block συνδέεται με μία γραμμική, χρονολογική σειρά με το επόμενο δημιουργώντας μία αλυσίδα (Blockchain), με τη χρήση μίας κρυπτογραφημένης υπογραφής. Η διαδικασία αυτή επιτρέπει στο Blockchain να χρησιμοποιείται σαν ένα δημόσιο λογιστικό βιβλίο (ledger), το οποίο μπορεί να μοιραστεί και να επιβεβαιωθεί από οποιοδήποτε εξουσιοδοτημένο χρήστη. Η ιδιότητα αυτή το καθιστά αποκεντρωμένο (decentralized) καθότι και η εποπτεία της ορθότητας της συναλλαγής διαμοιράζεται σε όλους τους χρήστες του και δεν περιορίζεται σε ένα χρηματοπιστωτικό ίδρυμα.

Πιο συγκεκριμένα, η τεχνολογία Blockchain θα μπορούσε να γίνει το απρόσκοπτο ενσωματωμένο οικονομικό στρώμα που δεν έχει ποτέ ο Ιστός, για να λειτουργήσει ως τεχνολογική βάση για πληρωμές, αποκεντρωμένες ανταλλαγές, μεταφορές ψηφιακών περιουσιακών στοιχείων και έξυπνες συμβάσεις. Η τεχνολογία Bitcoin και Blockchain , ως τρόπος αποκέντρωσης, θα μπορούσε να είναι η επόμενη μείζονα ανατρεπτική τεχνολογία της παγκόσμια Πληροφορική (ακολουθώντας το main-frame, το PC, το Διαδίκτυο και την κοινωνική δικτύωση/κινητό τηλέφωνα), με τη δυνατότητα να αναδιαμορφώνουν όλη την ανθρώπινη δραστηριότητα.

Η αρχιτεκτονική δικτύωσης peer-to-peer είναι η βάση για την λειτουργία των αποκεντρωμένων υπολογιστών. Οι Ανδρουτσέλης-Θεοτόκης και Σπινέλλης [25] θεωρούν ότι τα χαρακτηριστικά των peer-to-peer αρχιτεκτονικών είναι δύο. Το πρώτο χαρακτηριστικό είναι ο απευθείας διαμοιρασμός υπολογιστικών πόρων μεταξύ των χρηστών χωρίς να απαιτείται η ύπαρξη ενδιάμεσου κεντρικού διακομιστή. Κεντρικοί διακομιστές μπορεί να υπάρχουν για την διεκπεραίωση συγκεκριμένων λειτουργιών όπως την στήριξη του συστήματος, την προσθήκη νέων κόμβων/χρηστών, διάφορες διαδικασίες σχετικές με την κρυπτογράφηση των δεδομένων

αλλά ακόμη και για την επίτευξη της βασικής λειτουργίας του συστήματος. Στην περίπτωση που της έλλειψης ενός κεντρικού διακομιστή, τις παραπάνω λειτουργίες αναλαμβάνουν οι χρήστες/κόμβοι του. Το δεύτερο χαρακτηριστικό των συγκεκριμένων αρχιτεκτονικών αναφέρεται στην δυνατότητα του συστήματος να διαχειρίζεται την αστάθεια και την μεταβλητή συνδεσιμότητα ως κάτι συνηθισμένο. Συγκεκριμένα έχει την δυνατότητα να προσαρμόζεται αυτόματα σε σφάλματα της συνδεσιμότητας του δικτύου και των υπολογιστών όπως και στην παροδικότητα των κόμβων. Η ιδιότητα του να μπορεί να αντιμετωπίζει τα σφάλματα και να οργανώνεται αυτόματα του επιτρέπουν να διατηρεί την συνδεσιμότητα μέσα στο δίκτυο όπως και την απόδοσή του. Οι δύο περιπτώσεις που αναφέρθηκαν αποτελούν ουσιαστικά και τις δύο βασικές κατηγορίες, τα δομημένα και τα αδόμητα peer-to-peer δίκτυα.

Η διαφορετικότητα των δικτύων που βασίζονται στην αρχιτεκτονική peer-to-peer καθιστά δύσκολη την ύπαρξη ενός ορισμού που να καλύπτει το σύνολο αυτών. Ο Shirky [26] ορίζει ως peer-to-peer «μία σειρά εφαρμογών η οποία εκμεταλλεύεται μια σειρά πόρων όπως η αποθήκευση, η επεξεργαστικοί ισχύ, οι πληροφορίες και η ανθρώπινη παρουσία που βρίσκονται μέσα στο Διαδίκτυο». Οι Ανδρουτσέλης-Θεοτόκη και Σπινέλλης [25] θεώρησαν ότι ο συγκεκριμένος ορισμός δεν καλύπτει όλο το φάσμα των p2p συστημάτων και ορίσαν ως peer-to-peer «τα κατανεμημένα συστήματα τα οποία αποτελούνται από διασυνδεδεμένους κόμβους ικανούς να οργανώνονται αυτόνομα σε διαδικτυακές τοπολογίες με στόχο τον διαμοιρασμό πόρων, ικανών να προσαρμόζονται στα σφάλματα, και στον παροδικό αριθμό των κόμβων ενώ παράλληλα διατηρούν την συνδεσιμότητα και την απόδοσή τους χωρίς να απαιτούν την ύπαρξή ή την στήριξη ενός κεντρικού διακομιστή ή μίας κεντρικής αρχής.

Η εφαρμογή αυτών των συστημάτων μπορεί να διαχωριστεί δύο κατηγορίες σύμφωνα. Η πρώτη κατηγορία αφορά συστήματα ανταλλαγής αρχείων. Τέτοια συστήματα επιτυγχάνουν την απλή μεταφορά αρχείων μέσα στο δίκτυο και επιτρέπουν την αναζήτηση αρχείων. Η ασφάλεια, η διαθεσιμότητα των αρχείων και η ανθεκτικότητα των συστημάτων δεν είναι κύριο μέλημα τους. Τα συγκεκριμένα συστήματα ευθύνονται κατά κύριο λόγο για την αύξηση της δημοσιότητας των peer-to-peer τεχνολογιών. Η δεύτερη κατηγορία αφορά συστήματα δημοσίευσης περιεχομένου και δημοσίευσης αρχείων. Αυτά τα συστήματα στοχεύουν στην δημιουργία ενός κατανεμημένου μέσου αποθήκευσης, μέσα από το οποίο οι χρήστες μπορούν να δημοσιεύσουν να αποθηκεύσουν και να διανέμουν τα αρχεία. Η πρόσβαση στα αρχεία γίνεται ελεγχόμενα και ο στόχος αυτών των συστημάτων είναι η ασφάλεια και η ανθεκτικότητα. Παράλληλα στοχεύουν στην ενσωμάτωση διατάξεων που αφορούν την αξιοπιστία, την ανωνυμία και την αντίσταση λογοκρισία αλλά και την συνεχή διαχείριση των αρχείων.

Χαρακτηριστικό παράδειγμα ενός p2p συστήματος για μεταφορά αρχείων είναι το Napster. Πρόκειται για μία πλατφόρμα p2p που επέτρεπε στους χρήστες τον διαμοιρασμό τραγουδιών η οποία δημιουργήθηκε στα τέλη του ΄90. Η εύκολη πρόσβαση σε ένα πολύ μεγάλο αριθμό αρχείων μουσικής χωρίς αντίτιμο την έκανε διάσημη φτάνοντας μέχρι και 80 εκατομμύρια εγγεγραμμένους χρήστες. Ωστόσο τα προβλήματα πνευματικής ιδιοκτησίας που αντιμετώπιζε, σε

ότι αφορά την μεταφορά διανομή των μουσικών αρχείων, το οδήγησαν σε οριστική παύση λειτουργίας το 2001 [27].

4.1 Τυπική Λειτουργία του Blockchain

Η δομή των δεδομένων στο blockchain είναι μία ταξινομημένη back-linked λίστα των μπλοκ των συναλλαγών. Το blockchain μπορεί να αποθηκευτεί ως ένα απλό αρχείο, ή σε μια απλή βάση δεδομένων. Π.χ. το Bitcoin αποθηκεύει τα blockchain δεδομένα χρησιμοποιώντας τη βάση δεδομένων LevelDB της Google. Τα μπλοκ συνδέονται προς τα "πίσω", με το κάθε ένα να έχει αναφορά στο προηγούμενο μπλοκ στην αλυσίδα. Το blockchain συχνά εμφανίζεται σαν μια κάθετη στοίβα, με τα μπλοκ σε επίπεδα το ένα πάνω από το άλλο και το πρώτο μπλοκ που εξυπηρετεί ως θεμέλιο της στοίβας. Η οπτικοποίηση των μπλοκ να στοιβάζονται το ένα πάνω στο άλλο έχει σαν αποτέλεσμα τη χρήση όρων όπως "ύψος" για να αναφερθούμε στην απόσταση από το πρώτο μπλοκ και "κορυφή" ή "άκρη" για να ανατρέξουμε στο πιο πρόσφατα προστιθέμενο μπλοκ.

Κάθε μπλοκ εντός του blockchain προσδιορίζεται από ένα hash το οποίο παράγεται με τη χρήση του SHA256 αλγόριθμου κρυπτογράφησης στην κεφαλίδα του μπλοκ. Κάθε μπλοκ αναφέρεται επίσης στο προηγούμενο μπλοκ, γνωστή ως γονέας μπλοκ (parent block), μέσα από το πεδίο "προηγούμενο μπλοκ hash" στην κεφαλή του μπλοκ. Με άλλα λόγια, κάθε μπλοκ περιέχει το hash του γονέα μέσα στη δική του επικεφαλίδα . Η ακολουθία των hash συνδέει κάθε μπλοκ προς τον γονέα του, δημιουργώντας έτσι μία αλυσίδα η οποία πηγαίνει πίσω σε όλη τη διαδρομή μέχρι το πρώτο μπλοκ που δημιουργήθηκε ποτέ.

Παρά το γεγονός ότι ένα μπλοκ έχει ένα μόνο γονέα, μπορεί να έχει προσωρινά πολλαπλά παιδιά. Κάθε ένα από τα παιδιά αναφέρεται στο ίδιο μπλοκ ως γωνέα και περιέχει το ίδιο γονικό hash στο πεδίο «προηγούμενο μπλοκ hash». Πολλαπλά παιδιά μπορούν να προκύψουν κατά τη διάρκεια ενός αποκαλούμενου ως «blockchain fork», μια προσωρινή κατάσταση που εμφανίζεται όταν τα διάφορα μπλοκ που ανακαλύπτονται σχεδόν ταυτόχρονα από διαφορετικούς miners. Τελικά, μόνο ένα παιδί μπλοκ γίνεται μέρος του blockchain και το blockchain έχει επιλυθεί. Ακόμα κι αν ένα μπλοκ έχει περισσότερα από ένα παιδιά, κάθε μπλοκ μπορεί να έχει μόνο ένα γονέα. Αυτό οφείλεται στο γεγονός ότι κάθε μπλοκ έχει ένα μόνο πεδίο «προηγούμενο μπλοκ hash» το οποίο αναφέρεται στον μοναδικό γονέα του.

Το πεδίο «hash προηγούμενου μπλοκ" είναι μέσα στην κεφαλίδα του μπλοκ και με τον τρόπο αυτό επηρεάζει το hash του τρέχοντος μπλοκ. Η ταυτότητα του παιδιού αλλάζει εάν αλλάξει η ταυτότητα του γονέα. Όταν ο γονέας έχει τροποποιηθεί με οποιονδήποτε τρόπο, αλλαγές πραγματοποιούνται στο hash του γονέα. Το αλλαγμένο hash του γονέα απαιτεί μια αλλαγή στο «hash προηγούμενου μπλοκ" δείκτη του παιδιού. Αυτό με τη σειρά του προκαλεί το hash του παιδιού να αλλάξει, το οποίο απαιτεί μια αλλαγή στο δείκτη του εγγονιού, το οποίο με τη σειρά του αλλάζει το εγγόνι, και ούτω καθεξής. Αυτό το αποτέλεσμα αλληλουχίας εξασφαλίζει ότι μόλις ένα μπλοκ έχει πολλές γενεές να το ακολουθούν, δεν μπορεί να αλλάξει χωρίς να αναγκάζει τον επανυπολογισμό όλων των μεταγενέστερων μπλοκ. Επειδή ένας τέτοιος επανυπολογισμός θα

απαιτούσε τεράστιους υπολογισμούς, η ύπαρξη μιας μακράς αλυσίδας μπλοκ κάνει την βαθιά ιστορία του blockchain αμετάβλητη, κάτι το οποίο αποτελεί βασικό χαρακτηριστικό της ασφάλειας του blockchain.

Όταν κάποιος θέλει να προσθέσει μια συναλλαγή στην αλυσίδα, όλοι οι συμμετέχοντες στο δίκτυο θα την επικυρώσουν. Αυτό γίνεται με την εφαρμογή ενός αλγορίθμου στην συναλλαγή για την επαλήθευση της εγκυρότητας της. Τι ακριβώς νοείται ως "έγκυρο" ορίζεται από το σύστημα blockchain και μπορεί να διαφέρει μεταξύ των συστημάτων. Στη συνέχεια, εναπόκειται στην πλειοψηφία των συμμετεχόντων να συμφωνούν ότι η συναλλαγή είναι έγκυρη.

Ένα σύνολο των εγκεκριμένων συναλλαγών στη συνέχεια ομαδοποιείται σε ένα μπλοκ, το οποίο αποστέλλεται σε όλους τους κόμβους του δικτύου. Αυτοί με τη σειρά τους επικυρώνουν το νέο μπλοκ. Κάθε διαδοχικό μπλοκ περιέχει ένα hash, το οποίο είναι ένα μοναδικό δακτυλικό αποτύπωμα, του προηγούμενου μπλοκ.

Κατ' αυτό τον τρόπο, το blockchain λειτουργεί ως ένα αποκεντρωμένο (decentralized) λογιστικό καθολικό, το οποίο είναι κοινό για όλους τους συμμετέχοντες, μιας και όλοι οι εμπλεκόμενοι αποθηκεύουν ένα αντίγραφό του, κάτι που εξασφαλίζει την ασφάλεια και η διαφάνεια των συναλλαγών.

Η ειδοποιός διαφορά -αναφορικά με την προστασία- προκύπτει από το γεγονός ότι δεν είναι πλέον απαραίτητη η ύπαρξη μιας ενδιάμεσης «έμπιστης» αρχής (πχ. μιας τράπεζας), ενώ η εμπιστοσύνη των συναλλασσόμενων μερών βασίζεται σε αλγοριθμική επιβεβαίωση.

Ένας τρόπος για να σκεφτεί κάποιος το blockchain είναι σαν στρώσεις σε ένα γεωλογικό σχηματισμό ή ένα δείγμα από πυρήνα παγετώνα. Τα επιφανειακά στρώματα μπορεί να αλλάξουν με τις εποχές, ή ακόμα και να αφαιρεθούν πριν να έχουν ακόμα χρόνο για να εγκατασταθούν. Αλλά από τη στιγμή που θα πάμε μερικά μέτρα πιο βαθιά, τα γεωλογικά στρώματα γίνονται όλο και πιο σταθερά. Μέχρι τη στιγμή που θα δούμε μερικές εκατοντάδες μέτρα πιο κάτω, που ψάχνετε σε ένα στιγμιότυπο του παρελθόντος που έχει παραμείνει αδιατάρακτο επί χιλιετίες ή και εκατομμύρια χρόνια. Στο blockchain, τα πιο πρόσφατα μπλοκ μπορεί να αναθεωρηθούν αν υπάρχει επανυπολογισμός της αλυσίδας ο οποίος οφείλεται σε ένα blockchain fork. Τα έξι πιο πρόσφατα μπλοκ είναι σαν μερικά μέτρα κάτω από τη γη. Αλλά μόλις κάποιος κοιτάξει βαθύτερα στο blockchain, πέραν των έξι μπλοκ, τα μπλοκ είναι όλο και λιγότερο πιθανό να αλλάξει. Λίγες χιλιάδες μπλοκ πίσω (ένα μήνα) και το blockchain είναι πλέον εγκατεστημένο και ποτέ δεν θα αλλάξει [28].

4.1.1 **Συμμετοχή στην αλυσίδα**

Η βασική διάκριση μεταξύ των blockchains αφορά στην ελευθερία συμμετοχής τόσο στην υποδομή τους (πρόσβαση στην αλυσίδα), όσο και στην εφαρμογή των κανόνων συναίνεσης που τα διέπουν (πρόσβαση στην επικύρωση). Η φύση του εκάστοτε blockchain αποτελεί συγκερασμό της επιδιωκόμενης ελευθερίας πρόσβασης και της απαιτούμενης εμπιστοσύνης μεταξύ των

συμμετεχόντων, ενώ ο διαχωρισμός στην εικόνα, συνοδεύεται και από ενδεικτικούς μηχανισμούς συναίνεσης.

Ο εκάστοτε προγραμματιστής πρέπει να καταλήξει στο επιθυμητό πεδίο εφαρμογής του blockchain που σχεδιάζει, δηλαδή στο αν απαιτείται να είναι public, private ή consortium [29] καθώς και στην ύπαρξη ή όχι περιορισμών στα δικαιώματα των χρηστών, δηλαδή αν θα είναι permissioned ή permissionless. Επιγραμματικά, η πλειοψηφία των κρυπτονομισμάτων εδράζονται σε public permissionless blockchains (η ευρεία δυνατότητα συμμετοχής αποτελεί απαιτούμενο), ένα consortium blockchain έχει λογική για χρήση μεταξύ πολλαπλών εταίρων ή οργανισμών, ενώ σε ένα private blockchain πρόσβαση έχει συγκεκριμένος αριθμός αδειοδοτημένων χρηστών.

Με δεδομένο ότι ο υπό εξέταση κόμβος έχει τις απαραίτητες αδειοδοτήσεις, εκκινεί τη συμμετοχή του στην αλυσίδα με χρήση ενός λογισμικού το οποίο συνήθως ονομάζεται ‘πορτοφόλι’ (wallet) ένεκα της λογικής διαχείρισης του πρώτου blockchain για το κρυπτονόμισμα Bitcoin. Αν και από κάποια wallets δίνεται η δυνατότητα χειροκίνητης επιλογής του ιδιωτικού κλειδιού από το χρήστη, το πιο πιθανό είναι να γίνεται χρήση μηχανισμού τυχαίας παραγωγής του.

Το δημόσιο κλειδί εξάγεται στη συνέχεια εφαρμόζοντας στο ιδιωτικό κάποιον κρυπτογραφικό αλγόριθμο, παραδείγματα των οποίων θα δούμε στο επόμενο κεφάλαιο και ακολούθως εξάγεται η μοναδική διεύθυνση ή λογαριασμός του κόμβου / χρήστη που αποτελεί και το ψευδώνυμο του. Οι ίδιοι κόμβοι, πιθανόν, να έχουν τη δυνατότητα να συμμετέχουν στην εφαρμογή των κανόνων της συναίνεσης ως προς την κύρωση των συναλλαγών που εξετάζονται κάθε φορά για συνάθροιση στο επόμενο block.

Ακολούθως, το νεοσχηματισθέν block, όπως είδαμε, εκπέμπεται στους λοιπούς κόμβους οι οποίοι ελέγχουν την εγκυρότητα αυτού και των περιεχομένων του (συναλλαγές, συμβόλαια, χρονοσφραγίδα, συνόψεις κ.ο.κ) και το επανεκπέμπουν έως ότου αυτό φτάσει και γίνει αποδεκτό από όλους τους κόμβους, πάλι στο πλαίσιο του μηχανισμού συναίνεσης που έχει καθορισθεί. Η αλυσίδα επεκτείνεται με το νέο block και τηρείται από όλους τους (επιτρεπτούς) κόμβους.

4.1.2 **Θεμελιώδεις ιδιότητες**

Η τεχνολογία του Blockchain έχει κάποια ειδικά χαρακτηριστικά, τα οποία είναι τα στοιχεία που την καθιστούν επαναστατική και πρωτοπόρα. Χωρίς να εισέλθουμε σε ανάλυση των χιλιάδων εφαρμογών που υφίστανται και στις ιδιαιτερότητές τους, θα επικεντρωθούμε σε εκείνα τα βασικά που χαρακτηρίζουν την τεχνολογία στο σύνολο της.

Όπως έχει ειπωθεί κατ’ επανάληψη, το Blockchain είναι μία αποκεντρωμένη τεχνολογία κατανεμημένου μητρώου συναλλαγών. Η επικοινωνία σε επίπεδο δικτύου, μεταξύ των συμμετεχόντων, δεν εκτελείται μέσω ενός κεντρικού διαμετακομιστή, αλλά διενεργείται μέσω του ομότιμου δικτύου P2P. Επιπλέον, η αποκέντρωση αυτή, αφορά και την λήψη αποφάσεων, οι οποίες λαμβάνονται συλλογικά στο πλαίσιο των κανόνων συναίνεσης. Τέλος, επιλύει το

πρόβλημα ασφάλειας και αξιοπιστίας των κεντρικοποιημένων δικτύων και διασπάται σε δύο ξεχωριστά θέματα, τον αποκεντρωμένο έλεγχο και την αποκεντρωμένη συναίνεση.

Όσον αφορά στη συναίνεση, η κατανομή της αφορά στο ποιοι κόμβοι έχουν άδεια να συμμετέχουν στη διαδικασία επικύρωσης των συναλλαγών. Ομοίως με τα παραπάνω, τα public blockchains είναι πλήρως αποκεντρωμένα καθώς στα δίκτυα αυτά, οποιοσδήποτε μπορεί να συμμετέχει τόσο ως απλός κόμβος, όσο και ως επικυρωτής. Στα private blockchains ισχύει το αντίθετο, καθώς μόνο ένα μέρος των κόμβων έχει την άδεια να συμμετέχει στο μηχανισμό συναίνεσης.

Σημαντικότατη είναι η επίτευξη μίας περιορισμένης αλλά αποτελεσματικής ανωνυμίας και η συνεπακόλουθη εκτέλεση συναλλαγών με χρήση μόνο της διεύθυνσης του κόμβου, του δημόσιου και του ιδιωτικού κλειδιού του χρήστη. Η 'ανωνυμία' αυτή επιτυγχάνεται με χρήση ψευδωνύμων συνδυαστικά τόσο με την απαίτηση αδυναμίας απόδοσης διαφορετικών διευθύνσεων στον ίδιο χρήστη, όσο και με την απαίτηση αδυναμίας ταύτισης διεύθυνσης στο blockchain (ή δημοσίου κλειδιού γενικώς) με μία πραγματική (real-world) διεύθυνση IP [30].

Ένα τρίτο χαρακτηριστικό αφορά στην προσβασιμότητα των δεδομένων μεταξύ των χρηστών, όπου σε ένα public blockchain άπαντες μπορούν να τα διαβάσουν, ενώ στις private ή consortium υλοποιήσεις, η πρόσβαση είναι περιορισμένη σε κάποιους χρήστες. Κατ' αντιστοιχία με τα δικαιώματα πρόσβασης σε αρχεία υπολογιστή, η ιδιότητα αυτή αποτελεί ένα τύπου read permission.

Τέταρτο χαρακτηριστικό, η αμεταβλητότητα / σταθερότητα των δεδομένων, χαρακτηριστικό που μας ενδιαφέρει ιδιαίτερα υπό το πρίσμα των public blockchains καθώς στα υπόλοιπα, θεωρητικά γνωρίζουμε τους συμμετέχοντες και ασκείται ο πρέπον έλεγχος. Στα συστήματα αυτά, όπου γίνεται χρήση μηχανισμών συναίνεσης PoW, είναι κοστοβόρα η προσπάθεια παραποίησης των δεδομένων με συνέπεια η χρήση των ίδιων πόρων να είναι πιο αποδοτική εφόσον τηρούνται οι κανόνες. Πέραν αυτού, η χρήση συνόψεων δεικτών στην αλυσίδα των block καθιστά αδύνατη την αλλαγή πρότερων δεδομένων χωρίς η αλλαγή αυτή να γίνει αντιληπτή.

Πέμπτο χαρακτηριστικό είναι ο τρόπος διανομής και αναπαραγωγής των δεδομένων, τέτοιος ώστε κάθε κόμβος που έχει άδεια συμμετοχής στον κανονισμό συναίνεσης, να τηρεί ένα πλήρες και έγκυρο αντίγραφο του blockchain κάθε στιγμή. Σε συνάφεια με την σταθερότητα των δεδομένων, θεμελιώδες χαρακτηριστικό είναι η αυθεντικότητα και μη αποκήρυξη των συναλλαγών, ήτοι η επικύρωση και ακεραιότητα τους με χρήση του ζεύγους ιδιωτικού-δημόσιου κλειδιού ως έγκυρη ψηφιακή υπογραφή.

Η αυθεντικότητα αποδεικνύει ότι η συναλλαγή δεν έχει αλλοιωθεί ενώ η μη αποκήρυξη βεβαιώνει ότι κανείς δεν μπορεί να αρνηθεί την ύπαρξη και εκτέλεσή της. Τέλος, η αυθεντικότητα βεβαιώνεται και ως προς τη χρονική αλληλουχία από τη χρονοσφραγίδα επί του κάθε block, ενώ προαιρετικά δίνεται η δυνατότητα σε αρκετά blockchains να εκτελείται κώδικας εντός αυτών,

υπό τη μορφή των έξυπνων συμβολαίων (smart contracts) ή των αποκεντρωμένων εφαρμογών (decentralized apps ή dApps).

4.1.3 **Πλεονεκτήματα Χρήσης**

Η σχέση χαρακτηριστικών και πλεονεκτημάτων των blockchains εμπεριέχει μία ανάδρομη και κυκλική αιτιότητα, καθώς είναι μια τεχνολογία που αναπτύχθηκε ώστε να πετύχει κάποιους στόχους, οι οποίοι προφανώς επιτυγχάνονται από τις ιδιότητες που της προσδόθηκαν.

Παρόλο που έχει ήδη γίνει σποραδικά και επιγραμματικά αναφορά στους στόχους αυτούς, είναι ουσιώδης η ανάλυση συγκεντρωτικά του συνόλου των πλεονεκτημάτων που συναντάμε σε κάθε είδους blockchain. Πρώτος στόχος είναι η εξάλειψη κάθε είδους έμπιστου τρίτου μέρους. Ανάλογα την υλοποίηση, ο στόχος αυτός επιτυγχάνεται μερικώς (permissioned) ή ολικώς (permissionless) με χρήση του προαναφερθέντος P2P δικτύου όπου τελείως (public) ή εν μέρει (private) άγνωστοι χρήστες επικοινωνούν και συναλλάσσονται χωρίς να απαιτείται επικύρωση από κεντρική αρχή. Η επικύρωση γίνεται αποκεντρωμένα από όσους χρήστες επιθυμούν να συμμετέχουν στη διαδικασία και έχουν (αν απαιτείται) σχετικά δικαιώματα. Η μέθοδος αυτή συνεπάγεται γενικά μειωμένη χρήση πόρων και επίτευξη ταχύτερης συναίνεσης μεταξύ των χρηστών και αναφέρεται και ως ‘αποδιαμεσολάβηση’.

Η αποκέντρωση έχει και ένα έτερο και διπλό προφανές πλεονέκτημα. Τα δίκτυα επιτυγχάνουν ανθεκτικότητα καθώς δεν υφίσταται κεντρικός κόμβος ως κέντρο βάρους αποτυχίας (για λόγους επίθεσης ή τεχνικούς) ενώ οποιαδήποτε απώλεια ή διαφθορά ομότιμου κόμβου αντιμετωπίζεται, μετά την επαναφορά του, με επανεκπομπή σε αυτόν από τους έγκυρους κόμβους ενός ενημερωμένου αντιγράφου της βάσης δεδομένων. Επιπλέον, η διατήρηση του αντιγράφου από όλους τους κόμβους οδηγεί και στη συνεχή διαθεσιμότητα των δεδομένων.

Επίσης, η αποκέντρωση αφορά και στην ίδια την ακεραιότητα των δεδομένων. Η συναίνεση που επιτυγχάνεται μεταξύ των κόμβων, ανεξαρτήτως πρωτοκόλλου, διασφαλίζει την εγκυρότητα των δεδομένων και την πρακτική αδυναμία αυτά να αλλοιωθούν χωρίς να επηρεαστεί το σύνολο της αλυσίδας. Η ιδιότητα αυτή της αμεταβλητότητας και αποκεντρωμένης επικύρωσης των συναλλαγών είναι που προσδίδει και την βελτιωμένη ασφάλεια.

Η κατασκευή του blockchain προσφέρει επιπλέον οφέλη στην εύρεση και τον έλεγχο πληροφορίας καθώς η χρονοσήμανση των blocks και η ανοιχτή δομή τους επιτρέπουν τον απροκάλυπτο εντοπισμό της αλληλουχίας του συνόλου των επικυρωμένων συναλλαγών και αν απαιτείται την και επανεπικύρωση τους από τους χρήστες. Η προσέγγιση αυτή προσδίδει, φυσικά, και διαφάνεια στα δεδομένα και τις συναλλαγές με δύο εξαιρέσεις. Η πρώτη είναι η τήρηση της ανωνυμίας στα ανοιχτά δίκτυα και η δεύτερη είναι η μερική ή ολική απώλεια της διαφάνειας στα blockchains που απαιτούν κάποιο είδος αδειοδότησης (private ή permissioned).

Εντούτοις, σε αδειοδοτημένα και περιορισμένης πρόσβασης δίκτυα (private ή permissioned) υφίσταται απώλεια της ανωνυμίας αυτής προσδίδοντας ευθύνη στον χρήστη για τις ενέργειες του. Αντιθέτως, η εκτέλεση κώδικα (smart contracts και dApps) επί μίας πλατφόρμας της οποίας δεν

υφίσταται κεντρικός διαχειριστής / ιδιοκτήτης (public), γίνεται δίκαια και ουδέτερα ως προς τα αντισυμβαλλόμενα μέρη [31].

4.1.4 **Σύνοψη Πλεονεκτημάτων-Μειονεκτημάτων**

<u>Πλεονεκτήματα</u>

- Αποδιαμεσολάβηση

Δύο μέρη είναι σε θέση να κάνουν μια συναλλαγή χωρίς την επίβλεψη ή την διαμεσολάβηση ενός τρίτου μέρους.

- Εξουσιοδοτημένοι χρήστες

Οι χρήστες έχουν τον έλεγχο όλων των πληροφοριών και των συναλλαγών τους.

- Υψηλής ποιότητας δεδομένα

Τα blockchain δεδομένα είναι πλήρης, συνεπής, έγκαιρα, ακριβή και ευρέως διαθέσιμα.

- Αντοχή, αξιοπιστία και μακροζωία

Λόγω των αποκεντρωμένων δικτύων, το blockchain δεν έχει ένα κεντρικό σημείο αποτυχίας και είναι σε καλύτερη θέση να αντέξει σε κακόβουλες επιθέσεις.

- Ακεραιότητα της διαδικασίας

Οι χρήστες μπορούν να εμπιστευθούν ότι οι συναλλαγές θα εκτελούνται όπως ακριβώς ορίζουν οι εντολές του πρωτοκόλλου, καταργώντας την ανάγκη για ένα έμπιστο τρίτο μέρος.

- Διαφάνεια και αμεταβλητότητα

Οι αλλαγές στο δημόσιο blockchain είναι ορατές στο κοινό από όλα τα μέρη δημιουργώντας διαφάνεια, καθώς και όλες οι συναλλαγές είναι αμετάβλητες, που σημαίνει ότι δεν μπορούν να τροποποιηθούν ή να διαγραφούν.

- Απλούστευση του οικοσυστήματος

Όλες οι συναλλαγές προστίθενται σε ένα ενιαίο δημόσιο καθολικό (ledger), μειώνοντας έτσι την ακαταστασία και τις επιπλοκές των πολλαπλών ledgers.

- Ταχύτερες συναλλαγές

Οι συναλλαγές σε μία τράπεζα μπορεί ενδεχομένως να χρειαστούν μέρες για την εκκαθάριση και τελική διευθέτηση, ιδίως εκτός του ωραρίου εργασίας. Οι blockchain συναλλαγές μπορούν να μειώσουν το χρόνο συναλλαγής σε λεπτά και επεξεργάζονται 24/7.

- Χαμηλότερο κόστος συναλλαγών

Με την εξάλειψη των μεσαζόντων τρίτων και των γενικών εξόδων για την ανταλλαγή περιουσιακών στοιχείων, τα blockchains έχουν τη δυνατότητα να μειώσουν σημαντικά τα έξοδα συναλλαγής.

Μειονεκτήματα

- Εκκολαπτόμενη τεχνολογία

Η επίλυση των προκλήσεων όπως η ταχύτητα των συναλλαγών, η διαδικασία επαλήθευσης, και τα όρια των δεδομένων θα είναι καθοριστικής σημασίας στο να γίνει το blockchain ευρέως εφαρμόσιμο.

- Αβέβαιο ρυθμιστικό καθεστώς

Επειδή τα σύγχρονη νομίσματα δημιουργούνται και ελέγχονται από τις εθνικές κυβερνήσεις, το blockchain και το Bitcoin αντιμετωπίζουν εμπόδια στην ευρεία υιοθέτηση από τα προϋπάρχοντα χρηματοπιστωτικά ιδρύματα, εφόσον το καθεστώς ρύθμιση της κυβέρνησης του παραμένει ακαθόριστο.

- Μεγάλη κατανάλωση ενέργειας

Οι miners του blockchain για το δικτύο Bitcoin επιχειρούν 450.000 τρισεκατομμύρια λύσεις ανά δευτερόλεπτο για την επικύρωση των συναλλαγών, χρησιμοποιώντας σημαντικές ποσότητες ενέργειας του υπολογιστή.

- Έλεγχος, ασφάλεια και προστασία της ιδιωτικότητας

Ενώ υπάρχουν λύσεις, συμπεριλαμβανομένων των ιδιωτικών blockchains και ισχυρή κρυπτογράφηση, εξακολουθούν να υπάρχουν ανησυχίες στον κυβερνοχώρο για την ασφάλεια που πρέπει να αντιμετωπιστούν πριν το ευρύ κοινό αναθέσει τα προσωπικά του δεδομένα σε ένα blockchain.

- Ανησυχίες ενσωμάτωσης

Οι blockchain εφαρμογές προσφέρουν λύσεις που απαιτούν σημαντικές αλλαγές, ή την πλήρη αντικατάσταση των υπαρχόντων συστημάτων. Για να πραγματοποιηθούν αυτές οι αλλαγές, οι εταιρείες πρέπει να καταστρώσουν σχέδια στρατηγικής για την μετάβαση.

- Πολιτιστική έκδοση

Το blockchain αντιπροσωπεύει μια πλήρη στροφή προς ένα αποκεντρωμένο δίκτυο που απαιτεί την συμφωνία των χρηστών και των φορέων της.

- Κόστος

Το blockchain προσφέρει τεράστια εξοικονόμηση του κόστους, των συναλλαγών και του χρόνου, αλλά το υψηλό αρχικό κόστος κεφαλαίου θα μπορούσε να αποτελέσει αποτρεπτικό παράγοντα.

4.2 Διάκριση βάσει ιδιοκτησίας του δικτύου

Η ταξινόμηση των blockchains δεν είναι οριστικοποιημένη και οι μελετητές χρησιμοποιούν τη δική τους προσέγγιση, ενώ η εξέλιξη των εφαρμογών που χρησιμοποιούν κάποιου είδους blockchain, ήδη αριθμούν μερικές χιλιάδες. Με οδηγό την εκτεταμένη ταξινόμηση που παρουσιάζεται στο έργο των Tasca & Tessone (2017) και προκειμένου όπως γίνει εφικτή η απαιτούμενη γενίκευση, ώστε να προχωρήσουμε στην ουσία της μελέτης, επιλέχθηκαν τρεις βασικοί τρόποι διάκρισης τους. Βάσει ιδιοκτησίας του δικτύου, βάσει δικαιωμάτων των χρηστών και βάσει των χρησιμοποιούμενων μηχανισμών συναίνεσης.

Συνοπτικά, μπορούμε να θέσουμε ότι εφόσον το δίκτυο είναι δημόσιο (public), επιτρέπει σε όλους την ανάγνωση της βάσης δεδομένων και όλες οι εγγραφές είναι γνωστές και αξιόπιστες. Αντίθετα, εφόσον το δίκτυο είναι ιδιωτικό (private), συνεπάγεται περιορισμό του πλήθους των αναγνωστών με επίγνωση της ταυτότητας τους αλλά χωρίς κάποια δημόσια επικύρωση [32]. Ο διαχωρισμός απαντά στα ερωτήματα:

- Ποιος μπορεί να συμμετέχει στο δίκτυο;
- Ποιος μπορεί να εκτελεί το πρωτόκολλο συναίνεσης;
- Ποιος μπορεί να τηρεί αντίγραφο του μητρώου;

4.2.1 **Public blockchains**

Το πλέον διαδεδομένο είδος με τους περισσότερους χρήστες και το μεγαλύτερο μερίδιο αγοράς, σε επίπεδο κρυπτονομισμάτων με πάνω από 70 δισεκατομμύρια USD ($), είναι το πρότυπο με το οποίο παρουσιάστηκε στον ψηφιακό κόσμο και η πρώτη αλυσίδα, εκείνη του bitcoin.

Η χρήση τους επιτυγχάνει σχεδόν το σύνολο των προτερημάτων που έχουν αναφερθεί και κυρίως τη διαφάνεια και τον έλεγχο της πληροφορίας με κόστος την απόδοση και χωρητικότητα του δικτύου και την ανάγκη για εκτεταμένη χρήση κρυπτογράφησης και κατακερματισμού με συνέπεια συνήθως την υπερβολική χρήση πόρων, και δει, ενέργειας.

Η διαφορά μεταξύ public και private blockchains, αφορά στην ιδιοκτησία της υποδομής που συνεπάγεται και το εύρος πρόσβασης στους χρήστες [33]. Οι διαμετακομιστές (servers) είναι δημόσιοι και ανοιχτοί και οποιοσδήποτε μπορεί να συμμετέχει ανώνυμα και να προσπελαύνει τη βάση δεδομένων με αποτέλεσμα, ωστόσο, την έλλειψη ιδιωτικότητας και άρα ασφάλειας δεδομένων.

Η ελεύθερη πρόσβαση στο σύνολο της βάσης δεδομένων δεν είναι άνευ αρνητικών σημείων καθώς είναι αβέβαιο το αν ευαίσθητα δεδομένα θα μπορέσουν να αποκωδικοποιηθούν, αναγνωσθούν και χρησιμοποιηθούν από κακόβουλους χρήστες. Αντίθετα, όμως, η δομή αυτή διαθέτει και τη μέγιστη προοπτική διεύρυνσης.

Βασικό χαρακτηριστικό της συμμετοχής των κόμβων στη διαδικασία συνάθροισης των συναλλαγών σε block, ήτοι στον μηχανισμό συναίνεσης στα public blockchains, είναι η παροχή κινήτρου που συνήθως είναι το οικονομικό όφελος, είτε μέσω πίστωσης, στη διεύθυνση τους, ενός αριθμού κρυπτονομισμάτων είτε μέσω είσπραξης τελών επί των συναλλαγών που εγκρίθηκαν, δεδομένου του περιορισμένου μεγέθους των blocks το οποίο υπερκαλύπτεται από τις, αναμένουσες έγκριση, συναλλαγές.

4.2.2 **Private blockchains**

Η δεύτερη επιλογή που έχει ένας προγραμματιστής ως προς την πρόσβαση των χρηστών, είναι να καταστήσει το blockchain ιδιωτικό (private), εγκαθιστώντας έναν διαχειριστή (operator) ή ένα αυστηρό πρωτόκολλο κανόνων για παροχή αυθεντικοποιημένης και επικυρωμένης πρόσκλησης συμμετοχής σε υποψήφιους κόμβους. Με άλλα λόγια, το blockchain καθίσταται ελεγχόμενο ως προς το ποιοι μπορούν να συμμετέχουν και να αναγνώσουν τη βάση δεδομένων.

Το αποτέλεσμα είναι ένα πλήρως κεντρικοποιημένο δίκτυο, τοποθετημένο σε ιδιωτικούς διακομιστές, το οποίο φυσικά επιλύει το πρόβλημα της ιδιωτικότητας. Αναπόφευκτα, το μεγάλο μειονέκτημα είναι η μη απαίτηση συναίνεσης, καθώς το δίκτυο είναι διευθυνόμενο κεντρικά, είτε από πρωτόκολλα, είτε από έναν οργανισμό, είτε από έναν μόνο διαχειριστή.

Θα μπορούσαμε να πούμε ότι τα private blockchains δεν είναι τίποτα περισσότερο από κλειστές ασφαλείς βάσεις δεδομένων που εδράζουν την ασφάλεια αυτή σε έννοιες κρυπτογραφίας. Επιπλέον, ο διαχειριστής μπορεί να δικαιούται, κατά περίπτωση, να επεμβαίνει στα δεδομένα, ακόμα και αν αυτά έχουν ήδη εγγραφεί, γεγονός που καθιστά τη δομή αυτή ευκολότερη στη διαχείριση μεν, αδιαφανή δε και οδηγεί στην απεμπόληση των επαναστατικών ιδεών πίσω από την τεχνολογία των blockchains. Χαρακτηριστικά, τα private blockchains δεν απαιτούν και συνήθως δεν έχουν κάποιο κρυπτονόμισμα συνδεδεμένο με τη λειτουργία τους.

4.2.3 **Consortium blockchains**

Μία υβριδική μορφή που συνδυάζει και ξεπερνά μέρος της χαμηλής εμπιστοσύνης των public blockchains και του μοντέλου ύπαρξης μοναδικής οντότητας υψηλής εμπιστοσύνης των private blockchains, είναι τα consortium blockchains. Η δομή τους είναι μερικώς ιδιωτική και αποκεντρωμένη και συνεπάγεται μικρό αριθμό προδιαγεγραμμένων κόμβων με αποτέλεσμα μεγαλύτερη αποτελεσματικότητα, ενώ η ‘ηγεσία’ ασκείται από ομάδα κόμβων και όχι από έναν κεντρικό. Το σχήμα προτιμάται σε απαιτήσεις οργανωτικής συνεργασίας.

Ο μηχανισμός συναίνεσης και πρόσβασης ελέγχεται από προκαθορισμένους κόμβους (χρήστες, οργανισμούς ή επιχειρήσεις). Η ανάγνωση των δεδομένων μπορεί να είναι και ελεύθερη (public) εφόσον εξυπηρετούνται οι σκοποί ή να είναι και αυτή περιορισμένη. Αξίζει να σημειωθεί ότι ο διαχωρισμός μεταξύ των private και των consortium blockchains δεν είναι εύκολος με τις διαφορές να είναι περισσότερο διαχειριστικές ως προς την υλοποίηση, παρά τεχνικές, χωρίς ωστόσο να αποκλείεται και ουσιαστική απόκλιση σε ακραίες περιπτώσεις μεταξύ διαφορετικών εφαρμογών.

Items	Public	Private	Consortium
Openness	Completely open	Open to individual or entity	Open to specific organizations or groups
Read access	Anybody	Open to the public or to be restricted by any degree	Anybody
Write access	Anybody	Completely internal control	Specified multiple nodes
Transaction speed	Slow	Extremely fast	Fast
Anonymity	High	Low	Low
Decentralization	Fully distributed	Partial decentralization	Partial decentralization
Examples	Bitcoin Ethereum	Hyperledger Corda Quorum	R3

Πίνακας 1: Σύγκριση Public-Private-Consortium Blockchains

4.3 Διάκριση βάσει δικαιωμάτων των χρηστών

Ο τρόπος αυτός διαχωρισμού είναι μη ανατρεπτικός ως προς τον προηγούμενο αλλά συμπληρωματικός του καθώς, σε αντίθεση με τη σύγχυση μεταξύ επιστημόνων του χώρου που συγχέουν τους όρους public με permissionless και private με permissioned, η αδειοδότηση αφορά στην ίδια την πρόσβαση εγγραφής στο μητρώο συναλλαγών. Επ' αυτού, κατά τους Bozic, Pujolle & Secci (2017) και άλλων, η διαφορά μεταξύ αδειοδοτημένων (permissioned) και μη

(permissionless) μητρώων, επιδρά ουσιαστικά στη διαφοροποίηση και δυσκολία που επιβάλλεται σε έναν φορέα επίθεσης ο οποίος προσβάλλει τους μηχανισμούς συναίνεσης.

4.3.1 **Permissioned ledgers**

Τα αδειοδοτημένα μητρώα είναι εκείνα με τις μεγαλύτερες δυνατότητες παραμετροποίησης, καθώς δύναται να περιλαμβάνουν ειδικά δικαιώματα για κάθε έναν από τους χρήστες, ή ομάδες χρηστών. Το βασικό στοιχείο τους είναι η περιορισμένη εκχώρηση του δικαιώματος εγγραφής δεδομένων στην αλυσίδα (συναλλαγές, συμβόλαια κ.ο.κ.) και συνεπακόλουθα συμμετοχής στο μηχανισμό συναίνεσης, στοιχεία που οδηγούν σε κεντρικοποίηση των αποφάσεων.

Σημείο προβληματισμού επίσης, σε περίπτωση δραστικής επέκτασης των permissioned blockchains, αποτελεί η συνδυαστική πολυπλοκότητα που απορρέει από τη δυνητική ανάγκη επικοινωνίας μεταξύ τους, παράλληλα με την τήρηση των κανόνων τους και την ανανέωση των δικαιωμάτων των χρηστών.

4.3.2 **Permissionless ledgers**

Η πλήρως αποκεντρωμένη μορφή του μητρώου, όπου όλοι οι συμμετέχοντες έχουν το δικαίωμα εγγραφής και συμμετοχής στη διαδικασία συναίνεσης, άρα έχουν και όλα τα δικαιώματα πλην της επεξεργασίας / τροποποίησης εγγραφών. Εξ' ου και απαιτείται η επιβολή ισχυρού μηχανισμού συναίνεσης. Το κύριο μειονέκτημα εδώ είναι η δυσκολία κλιμάκωσης, ήτοι η αδυναμία επέκτασης και βελτίωσης της βάσης δεδομένων. Χαρακτηριστικά αναφέρεται ότι η κλιμάκωση σε επίπεδο συναλλαγών ανά δευτερόλεπτο (TPS) κυμαίνεται μεταξύ 3 και 20 στα blockchains στα οποία δεν απαιτείται αδειοδότηση, τη στιγμή που το δίκτυο της VISA ο μέσος όρος είναι περί τις 1500. Τρεις συνιστώσες καθορίζουν τη δυσκολία αυτή, η στασιμότητα του ρυθμού επεξεργασίας των δεδομένων, το άνω όριο του μεγέθους της βάσης δεδομένων και του block και τέλος οι καθυστερήσεις επικοινωνίας μεταξύ των κόμβων. Επιπλέον καθυστερήσεις επιβάλλονται και από τους μηχανισμούς συναίνεσης που χρησιμοποιούνται κατά το δοκούν [34].

4.3.3 **Σύνοψη των τύπων**

Μπορούμε να συνδυάσουμε τα ανωτέρω σε τέσσερις υποπεριπτώσεις και με αυτόν τον τρόπο έχουμε:

1. Public Permissionless blockchains:
   - Τοποθετημένο σε δημόσιους διακομιστές
   - Ψευδωνυμία που συνεπάγεται υψηλή ανθεκτικότητα
   - Ανοιχτό σε πρόσβαση, ανάγνωση και εγγραφή στο μητρώο
   - Μειονεκτήματα η έλλειψη ιδιωτικότητας και η χαμηλή επεκτασιμότητα
2. Public Permissioned blockchains:
   - Ανοιχτό σε πρόσβαση και ανάγνωση του μητρώου
   - Εξουσιοδότηση για εκτέλεση εγγραφής στο μητρώο
   - Μερική επίλυση του προβλήματος της επεκτασιμότητας
   - Μειονεκτήματα η κεντρικοποίηση και η έλλειψη ιδιωτικότητας

3. Private Permissionless blockchains:
    - Τοποθετημένο σε ιδιωτικούς διακομιστές
    - Εξουσιοδότηση για συμμετοχή/πρόσβαση στο δίκτυο
    - Δυνατότητα για μεγάλη επεκτασιμότητα
    - Μειονέκτημα η μη απαίτηση συναίνεσης
4. Private Permissioned blockchains:
    - Εξουσιοδότηση για πρόσβαση αλλά και ανάγνωση στο μητρώο
    - Μόνο ο διαχειριστής μπορεί να εγγράψει και να τροποποιήσει το μητρώο
    - Πλήρης κεντρικοποίηση με πολύ υψηλή επεκτασιμότητα
    - Υπερφίαλη χρήση αποκεντρωμένου μητρώου με κρυπτογραφία
5. Consortium blockchains:
    - Υποκατηγορία των private blockchains
    - Μερικώς ιδιωτικά και αποκεντρωμένα
    - Χρήση μεταξύ εταίρων ή οργανισμών με περιορισμένη πρόσβαση
    - Αντί διαχειριστή, ο μηχανισμός συναίνεσης ασκείται από ομάδα κόμβων

4.4 Διάκριση βάσει μηχανισμών συναίνεσης

Την επίτευξη της απαραίτητης συναίνεσης μεταξύ των κόμβων, ελλείψει ενός κεντρικού έμπιστου τρίτου μέρους, ως παραλλαγή του Προβλήματος των Βυζαντινών Στρατηγών (BGP) όπως το παρουσίασαν οι Lamport, Shostak & Pease[40]. Η συναίνεση αντικατοπτρίζεται στην εκλογή ενός κόμβου-ηγέτη ο οποίος και επιλέγει το προτεινόμενο αποτέλεσμα.

Στη συνέχεια και προκειμένου όπως ολοκληρώσουμε την προτεινόμενη διάκριση των υλοποιήσεων, παρουσιάζουμε τους πιο διαδεδομένους μηχανισμούς συναίνεσης, στηριζόμενοι στην ταξινόμηση των Bano κ.α. [35] και στην ήδη παρουσιασθείσα άποψη των Christidis & Devetsikiotis [36] για τη σχεδιαστική επίδραση δικαιωμάτων (permissioned/permissionless) και απαιτήσεων ασφάλειας.

Η πρώτη ολοκληρωμένη και σύνθετη προσέγγιση στο πρόβλημα, εκείνη του ‘Nakamoto’ στο bitcoin, αποτέλεσε τη βάση επίλυσης του προβλήματος των σιβυλλικών επιθέσεων στα public permissionless blockchains, εισάγοντας ένα κοστοβόρο, σε πόρους, σύστημα απόδειξης εργασίας (PoW) το οποίο φυσικά δεν αποτρέπει τον επιτιθέμενο από το να υιοθετήσει πολλαπλές ταυτότητες, αλλά του καθιστά ανέφικτο να τις αξιοποιήσει, καθώς είναι εξαιρετικά δύσκολο να συγκεντρώσει παράλληλα και την απαιτούμενη υπολογιστική ισχύ.

Ωστόσο, το πρωτόκολλο PoW δεν είναι πανάκεια, καθώς, πέραν του προβλήματος υψηλότατης κατανάλωσης ηλεκτρικής ενέργειας, η ίδια η τεχνολογία του Blockchain εξελίσσεται και παρουσιάζονται συνεχώς νέες υλοποιήσεις με διαφορετικές απαιτήσεις που αναπόφευκτα οδηγούν τους προγραμματιστές σε ανάπτυξη νέων πρωτοκόλλων. Αποτέλεσμα αυτού, να διακρίνουμε τρεις γενικές κατηγορίες:

- Πρωτόκολλα εκλογής βάσει εργασίας (PoW)

- Πρωτόκολλα εκλογής βάσει ιδιότητας (PoX)
- Υβριδικά πρωτόκολλα

4.4.1 **Proof-of-Work (PoW)**

Η λειτουργία του πρωτοκόλλου που περιγράφει ο ‘Nakamoto’ [37], βασιζόμενος πάνω στο hashcash του Back, «περιλαμβάνει τη σάρωση για μία αξία η οποία κατακερματισμένη, όπως με το SHA-256, η σύνοψη άρχεται με έναν αριθμό μηδενικών bits». Η διαδικασία αυτή μπορεί να παραλληλιστεί με την εύρεση ενός ακεραίου μικρότερου από έναν αριθμό-στόχο, όπου ακέραιος (long integer) είναι η ίδια η σύνοψη.

Εν τάχει, οι συμμετέχοντες στη διαδικασία του μηχανισμού συναίνεσης (miners) διαγωνίζονται για την επίλυση ενός φαινομενικά δύσκολου, υπολογιστικά, γρίφου. Ο κάθε υποψήφιος ηγέτης επιλέγει από τη δεξαμενή αναμονής (mempool) έναν αριθμό έγκυρων συναλλαγών, τις οποίες εισάγει σε ένα δέντρο Merkle, του οποίου τη ρίζα εισάγει στην επικεφαλίδα. Ακολούθως, προσθέτει τη χρονοσφραγίδα και ένα δείκτη κατακερματισμού προς το τελευταίο έγκυρο block της αλυσίδας. Αυτό το ιδιότυπο πακέτο δυαδικής πληροφορίας, συμπληρώνεται από έναν τυχαίο αριθμό (nonce) με απώτερο σκοπό ο κατακερματισμός της να εξάγει μία σύνοψη μικρότερη από μία τεθείσα τιμή [38]. Η αναζήτηση του nonce γίνεται με αλλεπάλληλες δοκιμές κατακερματισμού χρησιμοποιώντας ‘ωμή δύναμη’ (brute force), έως ότου βρεθεί έγκυρο block με αποτέλεσμα την επιβράβευση του ηγέτη με νομίσματα.

Εικόνα 6: Proof of Work

Κατόπιν, ο κόμβος εκπέμπεται στο δίκτυο και οι λοιποί κόμβοι ελέγχουν την εγκυρότητα του. Εφόσον η σύνοψη πληροί την προϋπόθεση του στόχου, περιλαμβάνει έγκυρες συναλλαγές και ο δείκτης δείχνει ορθά στο τελευταίο έγκυρο block, ο ηγέτης ‘εκλέγεται’, το προτεινόμενο block γίνεται αποδεκτό και οι miners εκκινούν την αναζήτηση του επόμενου block επί αυτού. Οι καθυστερήσεις στο δίκτυο (network latency) δημιουργούν μία παρενέργεια στην όλη διαδικασία, την ταυτόχρονη εισαγωγή στο δίκτυο δύο (ή περισσότερων) blocks για αποδοχή ως έγκυρων και

τελευταίων στην αλυσίδα. Αποτέλεσμα αυτού η διακλάδωση (forking) της ισχύουσας σε δύο (ή περισσότερες) blockchains που αναπτύσσονται παράλληλα έως ότου επικρατήσει εκείνη που αναπτύσσεται με μεγαλύτερη ταχύτητα και συναίνεση.

Ο εκάστοτε χρησιμοποιούμενος μηχανισμός PoW καθορίζει επακριβώς και τα κριτήρια επικράτησης μεταξύ τους. Η διαδικασία αυτή είναι συνήθης, ενώ μπορεί να συμβεί και λόγω διαφωνίας των μελών ενός blockchain ως προς ριζικές αλλαγές των πρωτοκόλλων, οπότε ονομάζεται σκληρή διακλάδωση (hard forking). Το πρωτόκολλο που ανέπτυξε ο 'Nakamoto' έχει αποδειχθεί αποτελεσματικό καθώς επιτυγχάνεται συναίνεση σταδιακά, εφόσον τηρούνται οι κανόνες [40]. Ο ίδιος ο 'Nakamoto' υπολόγισε εξαρχής την γεωμετρική αύξηση της υπολογιστικής ισχύος που έρχεται με την ανάπτυξη της τεχνολογίας και όρισε δικλείδες ασφαλείας επαναπροσαρμογής της δυσκολίας εύρεσης του nonce με σκοπό την απαίτηση χρόνου 10 λεπτών μεταξύ του σχηματισμού δύο νέων blocks (inter-block interval).

Η προσπάθεια των επίδοξων miners συνοδεύτηκε και από την εφεύρεση εξειδικευμένου εξοπλισμού προς τούτο, στοιχείο που δεν είχε υπολογίσει ο 'Nakamoto' με αποτέλεσμα σήμερα ο απαιτούμενος χρόνος να έχει μειωθεί, αναμένοντας τον επανακαθορισμό της τιμής-στόχου, ο οποίος γίνεται κάθε 2016 blocks, ήτοι περί τις 15 ημέρες. Η λειτουργία του συστήματος βασίζεται στην εξισορρόπηση κόστους/οφέλους των miners, δηλαδή η αποζημίωση σε συνάρτηση με τα έξοδα για εξοπλισμό και ενέργεια. Η αποζημίωση αυτή είναι δύο ειδών [41] διαχωριζόμενη στην απόδοση νέων νομισμάτων αλλά και τελών για την συμπερίληψη των συγκεκριμένων συναλλαγών στο block.

Η μεγάλη κατανάλωση ενέργειας χωρίς ουσιαστικό αντίκρισμα, δεν είναι το μοναδικό πρόβλημα που αντιμετωπίζει το πρωτόκολλο PoW, θέμα που πραγματεύονται οι Bonneau κ.α. [48] και οι Tschorsch και Scheuermann [42]. Οι τελευταίοι προτείνουν και την υλοποίηση του Primecoin [43] ως παράδειγμα χρήσης των υπολογισμών για την εύρεση του nonce σε πραγματικά προβλήματα. Ένα άλλο πρόβλημα είναι η συγκέντρωση της υπολογιστικής ισχύος είτε με χρήση εξειδικευμένου εξοπλισμού 'εξόρυξης' από τους έχοντες τους πόρους, είτε μέσω δημιουργίας 'συνεταιρισμών' (mining pools) που διαμοιράζουν τα έσοδα στους συμμετέχοντες αναλόγως της συμβολής τους. Αμφότερες οι προσεγγίσεις απομειώνουν δραστικά την αποκέντρωση και την 'δημοκρατικότητα' των public permissionless blockchains και μπορούν να οδηγήσουν και σε κακόβουλο αποκλεισμό συναλλαγών και χρηστών.

4.4.2 **Proof-of-X (PoX)**

Το υψηλότατο κόστος και οι αδυναμίες των μηχανισμών PoW, οδήγησαν στην ανάπτυξη μίας νέας κατηγορίας μηχανισμών επίτευξης συναίνεσης που αντικαθιστά την εργασία με κάποια άλλη ιδιότητα X (εξ' ου και το όνομα της). Η κατηγορία περιλαμβάνει πληθώρα διαφορετικών ιδιοτήτων που χρησιμοποιούνται ως κομβικές και είθισται να αφαιρούν πλήρως την απαίτηση υπολογιστικής εργασίας από την εξίσωση.

Θα ακολουθήσουμε το πλαίσιο αξιολόγησης που προτείνουν οι Bano κ.α., και περιλαμβάνει τρεις συνιστώσες. Ασφάλεια, απόδοση και σχεδιασμός που επεκτείνονται σε τρεις ιδιότητες ασφαλείας, τρεις ιδιότητες απόδοσης καθώς και τη λογική σχεδιασμού που ακολουθείται κάθε φορά. Η ασφάλεια εξετάζεται βάσει της συνέπειας, της απουσίας λογοκρισίας και της αντίστασης σε επιθέσεις DoS, ενώ η απόδοση εξετάζεται βάσει της ταχύτητας, της καθυστέρησης και της κλιμάκωσης.

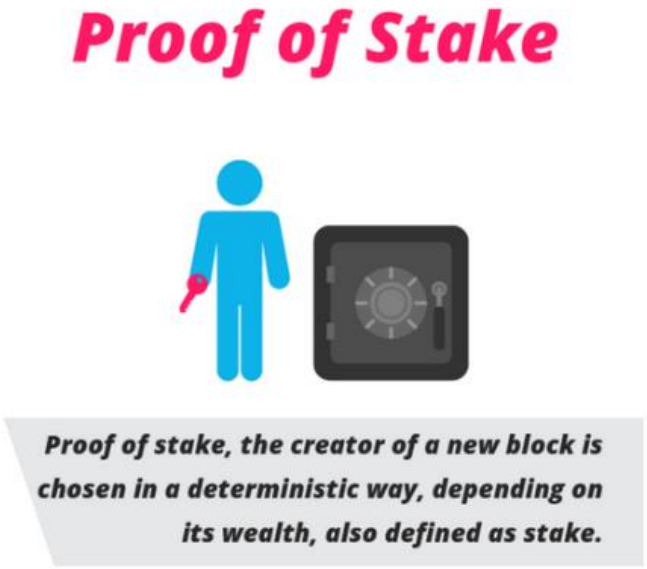
Η συνέπεια αφορά στο «αν το σύστημα θα φτάσει σε συναίνεση για μία συγκεκριμένη τιμή», η αντοχή στη λογοκρισία συναλλαγών στην «ανθεκτικότητα του συστήματος σε κακόβουλους κόμβους που καταστέλλουν συναλλαγές» ενώ η αντίσταση σε επιθέσεις DoS αυτονόητα σε «επιθέσεις κατά κόμβων που συμμετέχουν στη συναίνεση». Ως ταχύτητα, δε, (throughput) εννοούμε «το μέγιστο ποσοστό κατά το οποίο οι τιμές μπορούν να συμφωνηθούν μέσω του πρωτοκόλλου συναίνεσης», ως καθυστέρηση (latency) «το χρόνο που απαιτείται από τη στιγμή που προτείνεται μια τιμή, έως ότου επιτευχθεί συναίνεση σε αυτήν» και ως δυνατότητα κλιμάκωσης (scalability) «την ικανότητα του συστήματος να επιτυγχάνει μεγαλύτερη ταχύτητα μετάδοσης όταν η συναίνεση περιλαμβάνει μεγαλύτερο αριθμό κόμβων» [44].

4.4.3 **Proof-of-Stake (PoS)**

Η ελληνική απόδοση του όρου είναι η απόδειξη μέσω της διακύβευσης ή του πονταρίσματος, ήτοι μέσω της τρέχουσας κατανομής των νομισμάτων εντός του blockchain. Με άλλα λόγια η εκλογή του ηγέτη/εξορύκτη βασίζεται σε κάποιο τρόπο απόδειξης εκ μέρους των υποψηφίων του πόσα κατέχοντα κρυπτονομίσματα διακυβεύουν στη διαδικασία. Ο τρόπος αυτός ουσιαστικά ταυτίζει την ορθή λειτουργία του δικτύου με τα κίνητρα των κατόχων του αντίστοιχου νομίσματος.

Η εκλογή βέβαια δεν γίνεται με βάση την ποσότητα των νομισμάτων αυτή καθ’ εαυτή, καθώς μία τέτοια λογική θα είχε ως αποτέλεσμα το μονοπώλιο του μηχανισμού συναίνεσης από τον ‘πλουσιότερο’ κόμβο. Αντιθέτως, έχει προταθεί σειρά λύσεων που συνδυάζουν την περιουσία με κάποιο άλλο χαρακτηριστικό, όπως την τυχαιότητα της επιλογής μεταξύ εχόντων έναν αριθμό νομισμάτων (Blackcoin), την παλαιότητα/αρχαιότητα των κόμβων (Peercoin) ή ακόμα και τη δυνατότητα να ποντάρεις σε έναν άλλο, έμπιστο σου, κόμβο να αναλάβει αυτός τη διαδικασία αντ’εσού (BitShares).

Η απουσία ανάγκης επεξεργαστικής ισχύος, είτε επεξεργαστικής (CPU, GPU) είτε μνημονικής (RAM), επιβάλλει ένα επιπλέον θετικό χαρακτηριστικό το οποίο είναι η δυσκολία ένας επιτιθέμενος να αποκτήσει πλειοψηφία κρυπτονομισμάτων από την αγορά ειδικού εξοπλισμού εξόρυξης. Ακόμα και αν το πετύχει αυτό, θα βρίσκεται στο δίλημμα αν τον συμφέρει να επιτεθεί στο δίκτυο, απομειώνοντας δραστικά την αξία της περιουσίας του.



Εικόνα 7: Proof of Stake

Ένα αρνητικό αυτού είναι ότι ο μηχανισμός προωθεί τη συγκέντρωση περιουσίας παρά την διάδοση του νομίσματος μέσω της χρήσης του, ενώ η απουσία υπολογιστικών απαιτήσεων μπορεί να έχει ως παράπλευρο αποτέλεσμα και την αύξηση των επιθέσεων. Είναι χαρακτηριστικό ότι πολλά blockchains ξεκινούν με μηχανισμό PoW και σταδιακά υιοθετούν κάποια PoS υλοποίηση.

Οι διάφορες υλοποιήσεις που έχουν εμφανιστεί δεν φημίζονται για την ολοκληρωμένη επεξεργασία προ εφαρμογής τους. Παράδειγμα αποτελεί το In Ouroboros [45], όπου οι συμμετέχοντες τρέχουν ένα πολύπλευρο πρωτόκολλο ρίψης νομίσματος ώστε να επιλεγεί μία τυχαία διασπορά. Αυτή εισάγεται σε μία ψευδοτυχαία συνάρτηση η οποία εκλέγει τόσο τον ηγέτη σε αναλογία με το ποντάρισμα του, όσο και τους συμμετέχοντες στην επόμενη ‘κλήρωση’. Ωστόσο, η αμοιβή διαμοιράζεται σε όλους τους συμμετέχοντες και όχι αποκλειστικά στον εκλεχθέντα κόμβο.

Μία άλλη προσέγγιση αποτελεί το Ouroboros Praos [46], όπου οι συμμετέχοντες εξάγουν έναν τυχαίο αριθμό με χρήση μίας επαληθεύσιμης τυχαίας συνάρτησης (VRF) και εφόσον αυτός είναι μικρότερος από ένα όριο, εκπέμπουν το block και την απόδειξη του αριθμού. Η εκλογή εδώ δεν κοινοποιείται δημόσια, γεγονός που προσφέρει αντίσταση σε επιθέσεις DoS, ενώ το κίνητρο είναι ίδιο με το Ouroboros blockchain. Πέραν των ανωτέρω, εμφανίζονται τριών ειδών επιθέσεις που σχετίζονται με τη δομή των πρωτοκόλλων PoS:

- Nothing-At-Stake: Οι υποψήφιοι έχουν κίνητρο να συμμετέχουν σε όλες τις πιθανές διακλαδώσεις καθώς αυξάνεται η πιθανότητα έτσι να βρεθεί το block τους στην επικρατούσα αλυσίδα. Προκειμένου να αποφευχθεί αυτό, καλή λύση είναι ένας μηχανισμός ποινής για πολλαπλή συμμετοχή.

- Grinding: Επίθεση κατά την οποία οι υποψήφιοι επαναδημιουργούν ένα block πολλαπλά μέχρι τη στιγμή που θα μπορέσουν να δημιουργήσουν ταυτόχρονα ή άμεσα και το επόμενο, αποκτώντας μεγάλο προβάδισμα. Η λύση στο πρόβλημα περιλαμβάνει τυχαιότητα ή προκαθορισμό στη διαδικασία επιλογής του επόμενου, κατά σειρά, ηγέτη.
- Long-range: Η προσπάθεια εξαγοράς των ιδιωτικών κλειδιών χρηστών που δεν έχουν πλέον περιουσία και χρήση τους για επέμβαση σε όλο το blockchain. Το πρόβλημα επιλύεται με χρονικό περιορισμό της δυνατότητας επέμβασης σε block ή της ισχύος των πονταρισμένων νομισμάτων.

Οι Bonneu κ.α. παρουσιάζουν και άλλες, μη εφαρμοσμένες, παραλλαγές PoS με γενικό χαρακτηριστικό την απαίτηση απόδειξης των υποψηφίων ότι κατέχουν κρυπτονομίσματα.

Μία επιπλέον ενδιαφέρουσα πρόταση επί αυτού καταθέτουν και οι Bentov, Lee, Mizrahi & Rosenfeld [47]:

- Proof-of-deposit: Οι υποψήφιοι δεσμεύουν ένα ποσό κρυπτονομισμάτων για τη διάρκεια της εξόρυξης. Εφαρμόζεται στο Tendermint (Bistarelli, Mantilacci, Santancini, & Santini, 2017), όπου η πιθανότητα εκλογής αυξάνεται ανάλογα με το δεσμευμένο ποσό.
- Proof-of-burn: Οι υποψήφιοι συμμετείχαν αποδεικνύοντας την καταστροφή αριθμού νομισμάτων. Η τεχνική υιοθετήθηκε στο Slimcode [48] αλλά απεσύρθη.
- Proof-of-coin-age: Η βαρύτητα των νομισμάτων συσχετίζεται με το χρόνο παραμονής τους στην κατοχή του υποψηφίου. Η υλοποίηση εφαρμόζεται στο Peercoin από τους Zheng, Xie, Dai, Chen & Wang [56].
- Proof-of-Activity: Στην υλοποίηση αυτή προτείνεται μία κληρωτίδα μεταξύ όλων των νομισμάτων και η επιλογή να γίνεται με περιοδικά διαφορετικούς τυχαίους αλγορίθμους. Απαιτεί, ωστόσο, την άμεση γνωστοποίηση λήψης του αποτελέσματος από τον επιλεγμένο κόμβο.

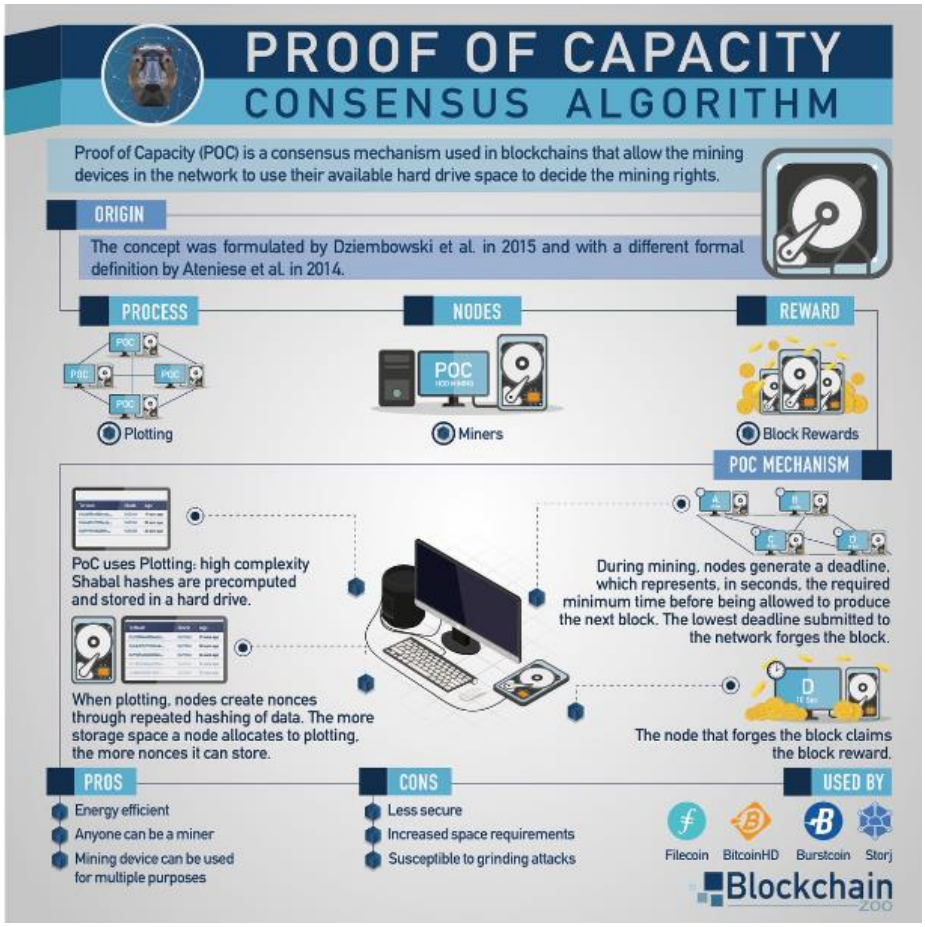
4.4.4 **Proof-of-Capacity (PoC)**

Μία ενδιαφέρουσα, οικολογική αλλά και σχετικά επικίνδυνη πρόταση κατατίθεται στο άρθρο του Andrew [49], ο οποίος προτείνει τη σχεδίαση σε οικόπεδα (plots) του σκληρού δίσκου από τον υποψήφιο ηγέτη και διάθεση τους στο δίκτυο. Σε γενικές γραμμές, όσο περισσότερος χώρος διατίθεται, τόσο πιο πιθανή είναι η επιλογή του ηγέτη, αλλά η πολυπλοκότητα του αλγορίθμου καθιστά αδύνατη τη σύγχρονη εκτέλεση του, οπότε οι υποψήφιοι πρέπει να προετοιμάσουν τα οικόπεδα πριν τη διαδικασία εκλογής. Η επικινδυνότητα του μηχανισμού έγκειται στην πιθανή πρόσβαση κακόβουλων χρηστών σε δεδομένα που βρίσκονται στο δίσκο. Η διαδικασία διακρίνεται σε δύο μέρη:

- Σχεδίαση (plotting): Κάνοντας επαναλαμβανόμενη χρήση ενός πολύ αργού και δύσκολου να υπολογιστεί αλγορίθμου κατακερματισμού, του Shabal [58], ο χρήστης δημιουργεί ένα αρχείο με nonces, το λεγόμενο ‘οικόπεδο’. Αυτονόητα, όσο περισσότερα θέλουμε, τόσο μεγαλύτερο χώρο δεσμεύουμε και άρα απαιτείται αντίστοιχα περισσότερος χρόνος. Κάθε

nonce καταλήγει να περιέχει 8192 συνόψεις, οργανωμένες σε ζευγάρια που ονομάζονται scoops και στα οποία εκχωρείται ένας αριθμός από 0 έως 4095.

- Εξόρυξη (mining): Η διαδικασία ξεκινά με τον υπολογισμό από τον miner ενός από τα προετοιμασμένα scoops που αριθμούν από 0 έως 4095, έστω x. Ανατρέχεις στο scoop x για όλα τα nonces, έστω y, που έχεις χαρτογραφήσει στο δίσκο και εξάγεις αντίστοιχους y χρόνους/προθεσμίες (deadlines). Κρατάς τη μικρότερη εξ' αυτών και εφόσον κανείς δεν κοινοποιεί άλλη μικρότερη από τη δική σου, εκλέγεσαι ηγέτης.



Εικόνα 8: Proof of Capacity

Ο μηχανισμός έχει πλεονεκτήματα καθώς δεν απαιτεί πολλή ενέργεια, ειδικό εξοπλισμό και προσφέρει καλή κατανομή καθώς υπάρχει περίσσεια ελεύθερου χώρου παγκοσμίως σε ήδη υπάρχοντες δίσκους, ενώ η αγορά τους δεν είναι απαγορευτική για το μέσο χρήστη.

Εντούτοις, οι Bano κ.α. το θεωρούν δυνητικά κεντρικοποιήσιμο λόγω της δυνατότητας ανάθεσης χώρου σε εξωτερικό φορέα. Το πρόβλημα επιλύεται, επί παραδείγματι, στην πλατφόρμα του SpaceMint [50] με τη διαφοροποίηση του PoC σε Proof-Of-Space (PoS) και το οποίο προσφέρει και επαρκή αντοχή στη λογοκρισία συναλλαγών και στις επιθέσεις DoS.

4.4.5 **Proof-of-Elapsed Time (PoET)**

Ένας άλλος τρόπος αντικατάστασης του PoW είναι με χρήση ειδικού υλικού παραγωγής Intel με αυξημένες επεκτάσεις ασφαλείας, τα SGX CPUs [51]. Οι επεκτάσεις αυτές παρέχουν προστασία τόσο στην εκτέλεση αξιόπιστου κώδικα όσο και σε δεδομένα από γνωστοποίηση ή τροποποίηση. Σε γενικές γραμμές, οι υποψήφιοι αιτούνται έναν τυχαίο χρόνο αναμονής και εκλέγεται εκείνος με τον ελάχιστο χρόνο.

Ο ηγέτης αποδεικνύει με υπογεγραμμένη βεβαίωση στους συνυποψηφίους του, ότι είχε όντως τον ελάχιστο χρόνο και ότι δεν εξέπεμψε το νέο block πρόωρα. Οι βεβαιώσεις αυτές είναι δυνατές μόνο μέσω της Υπηρεσίας Πιστοποιητικών της Intel (IAS), οπότε και ο μηχανισμός μπορεί να προσδιορισθεί ως σχετικά αποκεντρωμένος [52].

Πλεονεκτήματα αποτελεί η φύση του ως δίκαιο σύστημα κλήρωσης και μειωμένης απαίτησης ενέργειας σε συνδυασμό με την επαύξηση της απόδοσης των συστημάτων λόγω της διάθεσης σε άλλα έργα των επεξεργαστών όταν δεν συμμετέχουν στη διαδικασία [53]. Στο άρθρο του, ο Rilee [54], διαχωρίζει δύο γενικές φάσεις του μηχανισμού:

- Συμμετοχή ενός νέου υποψηφίου, ο οποίος κατεβάζει τον έμπιστο κώδικα για το blockchain και κατά την αρχικοποίηση ο κώδικας του παρέχει ένα νέο ζευγάρι κλειδιών, το οποίο χρησιμοποιεί για να αποστείλει πιστοποιημένη αίτηση συμμετοχής στο δίκτυο.
- Συμμετοχή στην κλήρωση, όπου ο υποψήφιος εξάγει από τον κώδικα ένα χρονόμετρο και αναμένει για το χρόνο που του υποδεικνύεται από αυτό. Εφόσον ο χρόνος παρέλθει, ο υποψήφιος αποστέλλει το πιστοποιητικό που το επιβεβαιώνει μαζί με το νέο block στο δίκτυο.

Παραδείγματα υλοποιήσεων είναι το Hyperledger Sawtooth και το REM με το δεύτερο να αποτελεί μια υβριδική προσέγγιση με το PoW, την PoUW καθώς δίνει τη δυνατότητα χρήσης των SGX CPUs για χρήσιμους υπολογισμούς παράλληλα με τη συμμετοχή τους στο μηχανισμό συναίνεσης. Οι υλοποιήσεις έχουν δύο μειονεκτήματα:

- Broken chip problem: Εάν υπάρξει παραβίαση της ασφάλειας των συστημάτων, ο επιτιθέμενος μπορεί να κερδίζει μονίμως την κλήρωση. Στα δύο προαναφερθέντα παραδείγματα, το πρόβλημα επιλύεται με χρήση στατιστικής ανάλυσης επί των νέων blocks.
- Stale chip problem: Θεωρητικά, κάθε νέο ολοκληρωμένο που εισάγεται στο δίκτυο αποκτά μία ακόμη ψήφο, αδυναμία που μπορεί να οδηγήσει σε συγκεντρωτισμό. Οι δημιουργοί του PoUW, στο REM, υποστηρίζουν ότι το πρόβλημα επιλύεται στην υλοποίηση τους λειτουργεί με τέτοιο τρόπο που πριμοδοτείται η εργασία και όχι η κατοχή ολοκληρωμένων.

4.4.6 **Υβριδικά**

Πέραν των προαναφερθέντων, εγκυκλοπαιδικά αναφέρεται και η δυνατότητα ύπαρξης υβριδικών πρωτοκόλλων κλασσικών αρχών συναίνεσης τα οποία καθοδηγούνται από τις λεγόμενες

επιτροπές συναίνεσης (μία ή περισσότερες), που αποτελούν ένα υποσύνολο κόμβων. Στις περιπτώσεις αυτές γίνεται χρήση μηχανισμών αντοχής σε σφάλματα βυζαντινού τύπου (BFT) όπως ο PBFT.

Οι υλοποιήσεις μίας επιτροπής μπορούν να εφαρμοστούν σε διαφορετικού είδους blockchains, αλλά τα πολλαπλής αλυσίδας προτιμώνται σε private permissioned εφαρμογές λόγω της πολυπλοκότητας τους. Παραδείγματα των δεύτερων βρίσκονται στο έργο των Cachin & Vukolić [55].

	Energy	***Rewards***	***Mining power***	**Examples**
Proof-of-Work (PoW)	High energy cost (Requires expensive computer calculations)	A reward is given to the first miner who solves each blocks problem.	More computing power = more mining power	Bitcoin, Etherum
Proof-of-Stake (PoS)	Low energy cost (Requires coins holders chosen in a deterministic way that is called staking)	There is no block reward, the miners take the transaction fees.	More wealth = more mining power	Dash
Proof-of-Capacity (PoC)	Low energy cost.	There is block reward	More space on hard drive = more mining power	Burstcoin
Proof-of-Elapsed Time (PoET)	Low energy cost	A separate random timer determines whether or not that node creates the new block and gets the reward	Randomization also ensures that every node is equally likely to be the winner	Sawtooth

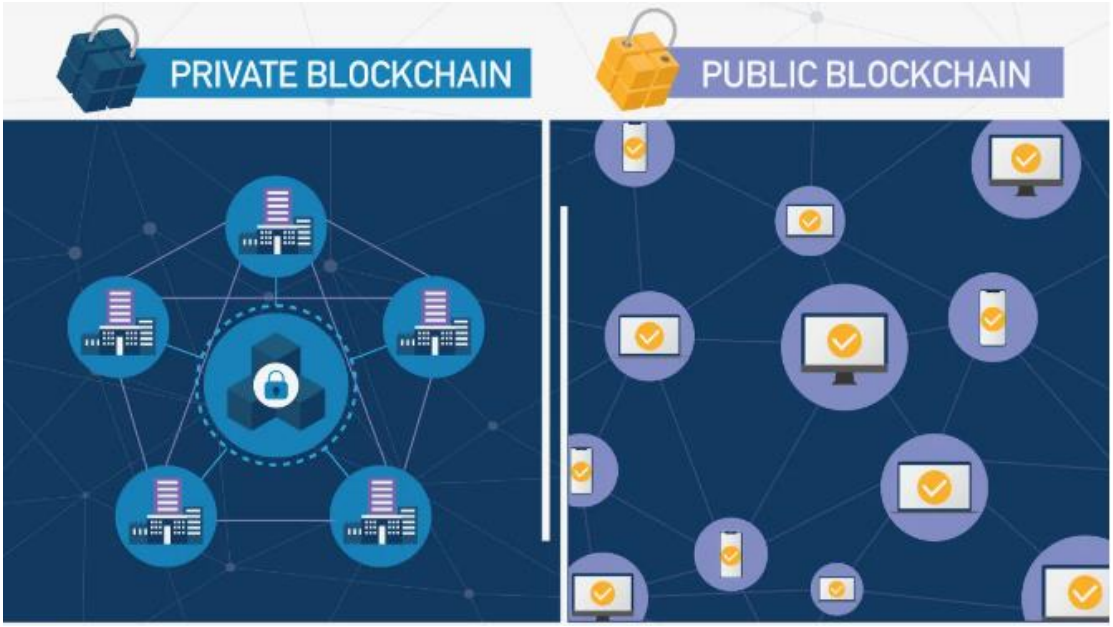
Πίνακας 2: Σύγκριση μηχανισμών συναίνεσης

5 ΚΕΦΑΛΑΙΟ 5: ΣΥΓΚΡΙΣΗ ΤΕΧΝΟΛΟΓΙΩΝ BLOCKCHAIN

5.1 Περιπτώσεις Public Blockchains

Η διαφορετικές εφαρμογές της τεχνολογίας που αναφέρθηκαν διαχωρίζουν την τεχνολογία σε δύο κατηγορίες. Η πρώτη αφορά τις περιπτώσεις των εφαρμογών blockchain (ή κατανεμημένων κατάστιχών) που ο καθένας μπορεί να συμμετέχει σε όλες τις διεργασίες μέσα σε αυτό και παράλληλα να συμβάλλει στην εξέλιξη του αν το επιθυμεί. Η περίπτωση αυτή είναι γνωστή ως «μη αδειοδοτούμενα blockchain» (permissionless blockchain). Σε αυτή την κατηγορία ανήκουν το Bitcoin και το Ethereum.

Η δεύτερη περίπτωση αφορά εφαρμογές blockchain όπου οι χρήστες δεν έχουν τις ίδιες ιδιότητες μέσα στο δίκτυο. Στην περίπτωση του δικτύου του Ripple που θα αναλυθεί στην συνέχεια, οι κόμβοι που διαχειρίζονται την επικύρωση των συναλλαγών και την μεγέθυνση του κατανεμημένου κατάστιχου είναι συγκεκριμένοι και ορισμένοι από τους ιδιοκτήτες οι οποίοι είναι υπεύθυνοι για την εξέλιξη και την λειτουργία του.



Εικόνα 9: Private and Public Blockchain

5.1.1 Η περίπτωση του Bitcoin ως ένα public permissionless blockchain

Το Bitcoin είναι το πρώτο γνωστό και διεθνώς χρησιμοποιούμενο κρυπτονόμισμα ανοιχτού κώδικα. Βασίζεται σε μια συλλογή τεχνολογιών και εννοιών που σχηματίζουν ένα οικοσύστημα ψηφιακών χρημάτων. Η λειτουργικότητα του βασίζεται σε ένα peer-to-peer δίκτυο, χωρίς κεντρική τράπεζα ή κεντρικό διαχειριστή. Είναι λοιπόν ένα αποκεντρωμένο ψηφιακό νόμισμα η μεταφορά του οποίου γίνεται από χρήστη σε χρήστη, χωρίς την ανάγκη κάποιας ενδιάμεσης παρέμβασης.

Η διαχείριση των συναλλαγών πραγματοποιείται συλλογικά από το δίκτυο blockchain. Κάθε ψηφιακό νόμισμα ορίζεται ως μία αλυσίδα ψηφιακών υπογραφών. Κάθε ιδιοκτήτης μεταφέρει το νόμισμα στον επόμενο, υπογράφοντας ψηφιακά ένα κατακερματισμό της προηγούμενης συναλλαγής και με το δημόσιο κλειδί του επόμενου κατόχου. Αυτή η πληροφορία καταγράφεται επίσης στο τέλος του νομίσματος. Το ερώτημα που προκύπτει φυσικά από την παραπάνω περιγραφή είναι πως μπορούμε να επαληθεύσουμε πως κάποιος κάτοχος δεν έχει 'διπλο-ξόδεψε' το νόμισμα. Σ' αυτό το σημείο μια κοινή λύση θα ήταν η εισαγωγή μιας κεντρικής αρχής, η οποία θα έλεγχε κάθε συναλλαγή για διπλές δαπάνες. Το πρόβλημα με αυτήν την λύση είναι ότι ολόκληρο το σύστημα θα εξαρτιόταν από αυτήν την αρχή/εταιρεία , με κάθε συναλλαγή να ελέγχεται από αυτήν , όπως με μία τράπεζα.

Λύση στα παραπάνω δίνει ο αλγόριθμος συναίνεσης Proof-of-Work (PoW), με τον οποίο οι ανθρακωρύχοι (miners) ανταγωνίζονται ο ένας τον άλλον για να επαληθεύσουν συναλλαγές στο δίκτυο και να ανταμειφθούν. Όπως έχει ήδη αναφερθεί και σε προηγούμενο κεφάλαιο το mining είναι ένα είδος αντίστροφου κατακερματισμού. Δε μπορεί να εξάγει κάποιος τα αρχικά δεδομένα, αλλά στόχος είναι η εξεύρεση ενός τυχαίου αριθμού (nonce) για τον οποίο ο αλγόριθμος κατακερματισμού δίνει μία τιμή κάτω από ένα, συγκεκριμένο συστημικά, όριο. Λόγω της πολυπλοκότητας του αλγορίθμου απαιτείται αρκετά μεγάλη κατανάλωση ενέργειας, με αποτέλεσμα επίδοξοι miners να επιδιώκουν την εφεύρεση ειδικά κατάλληλου εξοπλισμού εξόρυξης και να δημιουργούν συνεταιρισμούς για διαμοιρασμό των εξόδων. Υπολογίζεται πως η παρούσα ετήσια κατανάλωση ρεύματος για την παραγωγή Bitcoin είναι 44.71 TWh (terawatt hours). Οι TWh αντιστοιχούν σε περίπου ίδιο κόστος παραγωγής και συνολικών εσόδων καθιστώντας την εξόρυξη μία πολύπλοκη επένδυση Αποτέλεσμα αυτών είναι η μείωση της αποκέντρωσης και η περιθωριοποίηση άλλων χρηστών.

Επίσης το Bitcoin αν και αποτελεί μακράν το ευρύτερα χρησιμοποιούμενο κρυπτονόμισμα δεν προσφέρει υποστήριξη για σύνθετα έξυπνα συμβόλαια. Ακόμα και κάποιες απλές περιπτώσεις που υποστηρίζονται είναι συχνά δυσκίνητες στον σχεδιασμό και πολύ δαπανηρές για να εκτελεστούν[110].

5.1.2 **Η περίπτωση της Ripple ως ένα public permissioned blockchain**

Η Ripple είναι η πρώτη εταιρία που δημιούργησε αυτή τη κατηγορία του δικτύου δημιουργώντας ένα νέο επιχειρηματικό μοντέλο για την αξιοποίηση της τεχνολογίας του blockchain. Η Ripple παρέχει υπηρεσίες διακανονισμού σε συνεχή χρόνο (real time gross settlement) μέσα από μία κατανεμημένη πλατφόρμα πληρωμών. Το εικονικό νόμισμα της πλατφόρμας είναι το XRP [86]. Πρόκειται για μία έτοιμη προς χρήση πλατφόρμα, δεν περιορίζει τον αριθμό των χρηστών ωστόσο οι διαδικασία επικύρωσης γίνεται μονό από εγκεκριμένους κόμβους.

Η Ripple επιτρέπει τις συναλλαγές, πέρα από το εικονικό νόμισμα XRP, οποιοδήποτε άλλου εικονικού ή συμβατικού νομίσματος μέσα στο δίκτυο της Ripple. Για να επιτευχθεί αυτό ορίζονται από το Ripple οργανισμοί (όπως χρηματοπιστωτικά ιδρύματα και πάροχοι υπηρεσιών πληρωμών) ως πύλες (gateways) για την έκδοση του αντίστοιχου ψηφιακού στοιχείου για την

απεικόνισή τους μέσα στο δίκτυο. Για την συναλλαγές περιουσιακών στοιχειών πέρα του εικονικού νομίσματος XRP δημιουργούνται γραμμές εμπιστοσύνης (trust lines) μεταξύ των πυλών.

Η δομή ενός block (η εταιρία Ripple το ονομάζει ledger) στο δίκτυο του Ripple δεν διαφέρει ιδιαίτερα από αυτή των Bitcoin και Ethereum. Συγκεκριμένα ένα ledger αποτελείται από ένα αριθμό που λειτουργεί ως επικεφαλίδα μέσα στο δίκτυο, στοιχεία που αφορούν τους λογαριασμούς (όπως το υπόλοιπο), το σύνολο των συναλλαγών που περιέχει και την ώρα και ημερομηνία της χρονικής αποτύπωσης [87].

Η διαφορά έγκειται στον τρόπο που καταγράφονται οι συναλλαγές μέσα στο δίκτυο αλλά και στο σύστημα συναίνεσης που εφαρμόζεται και της επιτρέπει την διεκπεραίωση των συναλλαγών μέσα σε 4 δευτερόλεπτα. Το δίκτυο της Ripple έχει τρία είδη συμμετεχόντων μέσα στο δίκτυο της. Η πρώτη κατηγορία είναι οι αποκεντρωμένοι εξυπηρετητές που ονομάζονται κόμβοι επικύρωσης και είναι υπεύθυνοι να δέχονται και προωθούν τις συναλλαγές. Η δεύτερη κατηγορία αφορά τους χρήστες που πραγματοποιούν τις συναλλαγές. Σε αυτή την κατηγορία ανήκουν τα ηλεκτρονικά πορτοφόλια, χρηματοπιστωτικά ιδρύματα που συνεργάζονται με την Ripple και διαδικτυακές πλατφόρμες συναλλαγών. Η τρίτη ομάδα συμμετεχόντων είναι οι κόμβοι παρακολούθησης. Πρόκειται για τους για «ενδιαμέσους» μεταξύ των κόμβων επικύρωσης και των χρηστών στέλνοντας τις νέες συναλλαγές από τους χρήστες στο κόμβους επικύρωσης. Οι κόμβοι παρακολούθησης είναι επιπλέον υπεύθυνοι για τις ίδιες διαδικασίες με αυτές των κόμβων επικύρωσης εκτός από την διαδικασία επικύρωσης, δηλαδή την προώθηση και την αναμετάδοση των συναλλαγών εκτός από την διαδικασία της επικύρωσης. Για τους κόμβους επικύρωσης η Ripple έχει αναθέσει την λειτουργία τους σε πάνω από 50 ινστιτούτα και επιχειρήσεις.

Σημαντική παρατήρηση είναι ότι οι κόμβοι επικύρωσης δεν ανταμείβονται με νέα XRP. Η Ripple δημιούργησε 100 δισεκατομμύρια XRP από την αρχή της λειτουργίας της πλατφόρμας εκ των οποίων πλέον κατέχει 7,114,004,047. Στην αγορά βρίσκονται 39,178,259,468 και τα υπόλοιπα 53,700,000,024 η Ripple τα τοποθέτησε σε ένα κρυπτογραφικά προστατευμένο καταπιστευτικό λογαριασμό (escrow account). Με αυτό τον τρόπο, όπως αναφέρει η ίδια, επιτρέπει στους ενδιαφερόμενους να υπολογίζουν τη μέγιστη προσφορά μέσα στο δίκτυο (XRP Market Performance, 2018). Καθώς δεν υπάρχει οικονομικό κίνητρο κατά την διαδικασία επικύρωσης, δεν είναι σαφές ποιο είναι το κίνητρο των συγκεκριμένων κόμβων επικύρωσης για την συμμετοχή τους στο δίκτυο.

Το σύστημα συναίνεσης διαφέρει από αυτά των δύο περιπτώσεων που αναλύθηκαν. Η βασική διαφορά είναι η αδυναμία συμμετοχής ως κόμβοι επικύρωσης χωρίς την συγκατάθεση της Ripple. Αν και η ύπαρξη εγκεκριμένων κόμβων επικύρωσης έρχεται σε αντίθεση με την αρχική ιδέα του Nakamoto (2009) για την δημιουργία μιας πλατφόρμας που δεν απαιτείται εμπιστοσύνη για την επίτευξη των συναλλαγών. Ωστόσο αυτό διευκολύνει αρκετά την επίτευξης συναίνεσης μεταξύ των κόμβων. Οι Schwartz κ.α [88] αναφέρουν ότι ο αλγόριθμος της συναίνεσης εφαρμόζεται κάθε λίγα δευτερόλεπτα σε κάθε κόμβο και περιγράφουν την διαδικασία στα εξής βήματα.

1. Κάθε κόμβος επικύρωσης και παρακολούθησης δέχεται ως σημείο εκκίνησης το τελευταίο ledger που έχει αποδεχτεί το δίκτυο. Κάθε κόμβος επικύρωσης και παρακολούθησης επεξεργάζεται μια ομάδα συναλλαγών ελέγχοντας την εγκυρότητά τους (σε αυτές μπορεί να περιέχονται νέες ή προηγούμενες συναλλαγές που έχουν απορριφθεί). Σε περίπτωση που είναι έγκυρες, τις μεταδίδει στους υπόλοιπους κόμβους ως υποψήφιο σετ.
2. Στην συνέχεια, κάθε κόμβος ελέγχει τις τελικές ομάδες που προτείνουν μόνο οι κόμβοι επικύρωσης. Οι συναλλαγές που έχουν το μεγαλύτερο αριθμό αποδοχών από το σύνολο των κόμβων περνάνε στην επόμενη φάση.
3. Οι συναλλαγές που προκρίθηκαν ελέγχονται από τους κόμβους επικύρωσης. Αν έχουν αποδοχή μεγαλύτερη του 80% εισάγονται στο νέο ledger το οποίο συνδέεται με τα υπόλοιπα και αποστέλλεται σε όλους τους κόμβους. Οι υπόλοιπες συναλλαγές που δεν προκρίθηκαν είτε απορρίπτονται είτε παραμένουν να ενταχθούν στο νέο ledger.

Για την αποφυγή της υπερβολικής μεγέθυνσης του blockchain και της κακόβουλης χρήσης του, η Ripple έχει θέσει ένα ελάχιστο ποσό που θα πρέπει να υπάρχει σε κάθε λογαριασμό για την δημιουργία και την χρήση του. Το ποσό ορίζεται στα 20 XRP (Reserves, 2018). Παράλληλα σε κάθε συναλλαγή υπάρχει ένα ποσό που δαπανά ο αποστολέας και ορίζεται ως κόστος συναλλαγής. Το ποσό ορίζεται στα 0.00001 XRP. Το ποσό αυτό δεν δίνεται ως αντίτιμο σε άλλους κόμβους αλλά καταστρέφεται [103].

5.2 Περιπτώσεις Private Blockchains

Σε αυτή την κατηγορία θα αναλυθούν οι δομές των τριών περιπτώσεων που προαναφέρθηκαν, δηλαδή του Hyperledger Fabric, του Corda και του Quorum.

5.2.1 **Η περίπτωση του Hyperledger Fabric**

Το ίδρυμα Linux τον Δεκέμβρη του 2015 δημιούργησε ένα διακλαδικό Blockchain πρόγραμμα ανοιχτού κώδικα. Σε αυτό το πρόγραμμα αναπτύσσονται διαφορετικές «δομές» (frameworks) βασισμένες στην τεχνολογία του Blockchain και τα αντίστοιχα εργαλεία για την χρήση τους. Συγκεκριμένα το πρόγραμμα, αποτελείται από 5 προσαρμοζόμενες «δομές» κατανεμημένου κατάστιχου (Indy, Fabric, Burrow, Iroha και Sawtooth) οι οποίες στοχεύουν στην κάλυψη των διαφορετικών αναγκών των επιχειρήσεων. Από αυτές η πιο διαδεδομένη είναι η Hyperleger Fabric. Στο πρόγραμμα συμμετέχουν διάφορες εταιρίες και χρηματοπιστωτικά ιδρύματα. Σε αυτές περιλαμβάνονται η IBM, η Intel, η J.P. Morgan, η Accenture, η Deutsche Bank και η American Express [104].

Το Hyperedger Fabric είναι μια πλατφόρμα που αναπτύχθηκε από την IBM και την Digital Asset. Η βασική διαφορά σε σχέση με τις πλατφόρμες που αναλύθηκαν είναι ότι η υλοποίηση τους γίνεται από τον οργανισμό ή τους οργανισμούς που το χρησιμοποιούν σε κάθε περίπτωση. Πρόκειται για μια «δομή» που υποστηρίζει την χρήση έξυπνων συμβολαίων (η ίδια το ονομάζει chaincode) και μπορεί να αναπαρασταθεί μέσα σε αυτό οποιαδήποτε μορφή υλικού ή άυλου περιουσιακού στοιχείου απεικονίζοντάς το με μία αυθαίρετη τιμή.

Ένα δίκτυο βασισμένο στην αρχιτεκτονική του Hyperleger Fabric αποτελείται από κόμβους οι οποίοι χρησιμοποιούν τα έξυπνα συμβόλαια για την συμμετοχή τους στο κατανεμημένο κατάστιχο. Η βασική διαφορά, με τις υπόλοιπες κατανεμημένες πλατφόρμες είναι ότι ένας κόμβος μπορεί να διαθέτει, εκτός από διαφορετικά έξυπνα συμβόλαια (που περιγράφουν τις διαφορετικές συμβάσεις μεταξύ των κόμβων), διαφορετικά κατανεμημένα κατάστιχα για κάθε συμβόλαιο χωρίς βέβαια αυτό να είναι δεσμευτικό. Επιπλέον για να μπορέσει κάποιος να συνδεθεί το δίκτυο απαιτείται πρώτα η συγκατάθεση του διαχειριστή του δικτύου.

Μία εφαρμογή (την οποία χρησιμοποιεί ένας χρήστης για να συνδεθεί στο blockchain) πρέπει να είναι συνδεδεμένη με ένα κόμβο στο δίκτυο. Μέσα από την εφαρμογή μπορεί να ξεκινήσει μία «υποψήφια» νέα συναλλαγή, η οποία αποστέλλετε στον κανονικό βασικό κόμβο (peer) για να εκτελέσει το έξυπνο συμβόλαιο που αφορά την συγκεκριμένη συναλλαγή. Στην συνέχεια ενημερώνονται για το συγκεκριμένο συμβόλαιο οι ενδιαφερόμενοι βασικοί κόμβοι (endorsing peers). Εφόσον συμφωνούν και το υπογράψουν ψηφιακά αυτό αποστέλλεται πίσω στον χρήστη μέσω της εφαρμογής. Αυτό είναι το πρώτο στάδιο μίας συναλλαγής.

Το δεύτερο στάδιο της συναλλαγής περιλαμβάνει ένα άλλο είδος κόμβου ο οποίος λειτουργεί ως «ελεγκτής-ταξινομητής» (orderer) των συναλλαγών. Συγκεκριμένα είναι αυτός που δημιουργεί τα blocks, ελέγχει αν οι «υποψήφιες» νέες συναλλαγές παραβιάζουν κάποιους από τους όρους του συμβολαίου και μεταδίδει τα blocks στους κόμβους που συμμετέχουν στο συγκεκριμένο κατάστιχο που αφορά το έξυπνο συμβόλαιο που εκτελέστηκε. Αν και στην συγκεκριμένη περίπτωση ο «ελεγκτής» είναι ένας κόμβος, υπάρχει δυνατότητα εφαρμογής ενός κατανεμημένου συστήματος ελέγχου.

Τέλος, το τρίτο στάδιο αφορά την αποδοχή των blocks από τους κόμβους που συμμετέχουν στο συγκεκριμένο κατάστιχο. Σε περίπτωση που αποδεχτούν τις νέες συναλλαγές τότε αυτές πραγματοποιούνται. Η διαφορά με τις υπόλοιπες πλατφόρμες είναι ότι ακόμη και στην περίπτωση που δεν γίνει αποδεκτή μία συναλλαγή αυτή καταγράφεται στο blockchain.

5.2.2 **Η περίπτωση του Corda**

Το Corda [105] είναι μια δομή (framework) που χρησιμοποιεί την τεχνολογία του Blockchain και των έξυπνων συμβολαίων αλλά δεν οργανώνει το χρόνο σε blocks. Αντ’ αυτού ένα δίκτυο Corda έχει ένα ή περισσότερα συμβολαιογραφικά συμπλέγματα που παρέχουν υπηρεσίες συναλλαγών και χρονικής σήμανσης, αφαιρώντας έτσι τον ρόλο που παίζουν οι ανθρακωρύχοι σε άλλες πλατφόρμες. Αυτό σημαίνει ότι η υλοποίηση μπορεί να διαφέρει σε κάθε περίπτωση εφαρμογής. Σε όλες τις περιπτώσεις ωστόσο υπάρχουν τρία βασικά είδη κόμβων.

Η πρώτη κατηγορία κόμβων αφορά τις επιχειρήσεις τις οποίες χρησιμοποιούν το δίκτυο για την επίτευξη των συναλλαγών. Οι συγκεκριμένες έχουν την δυνατότητα χρήσης των έξυπνων συμβολαίων «CorDapps». Παράλληλα, κάθε κόμβος αποθηκεύει όλες τις συναλλαγές που συμμετέχει στο κατάστιχο «CordaVault» που διαθέτει αλλά και τις υποχρεώσεις προς τους

άλλους κόμβους χωρίς να χρειάζεται να δημοσιεύει τις πληροφορίες των συναλλαγών σε μη εμπλεκόμενους κόμβους.

Η δεύτερη κατηγορία κόμβων αφορά τους κόμβους που παρέχουν την βεβαίωση της μοναδικότητας της συναλλαγής και την οριστικοποίηση της συναλλαγής. Η κόμβοι αυτοί ονομάζονται «συμβολαιογραφικοί» κόμβοι (Notary Nodes). Ο αριθμός των κόμβων, όπως και στην περίπτωση των «ελεγκτών» στο Hyperledger Fabric, διαφέρει σε κάθε περίπτωση ενώ μπορεί να επιτευχθεί και με την χρήση ενός κεντρικού κόμβου.

Τέλος, υπάρχει μία τρίτη κατηγορία κόμβων που λειτουργεί ως διαχειριστής των δημόσιων κλειδιών των οργανισμών που συμμετέχουν όπως και τις IP διευθύνσεις τους έτσι ώστε να γίνεται η ταυτοποίηση των οργανισμών και να επιτυγχάνεται η σύνδεση στο δίκτυο.

5.2.3 **Η περίπτωση του Quorum**

Το Quorum [89] χαρακτηρίζεται ως μία έκδοση της πλατφόρμας του Ethereum για επιχειρήσεις. Όπως και οι δύο προηγούμενες περιπτώσεις ιδιωτικών blockchain υποστηρίζει την χρήση των έξυπνων συμβολαίων. Παράλληλα, δίνει την δυνατότητα στους κόμβους που συμμετέχουν να δημιουργούν ιδιωτικές συναλλαγές στα συμβόλαια των οποίων έχουν πρόσβαση μόνο οι συμμετέχοντες. Ωστόσο το σύνολο των συναλλαγών αποθηκεύεται κρυπτογραφημένο σε ένα ενιαίο κατανεμημένο κατάστιχο σε όλους τους κόμβους (Quorum Whitepaper). Το πρωτόκολλο συναίνεσης που χρησιμοποιεί το Quorum είναι το πρωτόκολλο Raft. Ουσιαστικά, ορίζει ένα κόμβο ως «καθοδηγητή» ο οποίος είναι υπεύθυνος για την δημιουργία και την διάδοση των blocks ενώ οι υπόλοιποι κόμβοι αποδέχονται το νέο block. Ο καθοδηγητής ορίζεται μέσα από μία διαδικασία ψηφοφορίας για την δημιουργία κάθε νέου block. Παράλληλα για την υποστήριξη των ιδιωτικών συμβολαίων διαχωρίζει τα έξυπνα συμβόλαια σε ιδιωτικά και δημόσια σε κάθε κόμβο. Η διαφορά με τις δύο προηγούμενες περιπτώσεις ιδιωτικών blockchain είναι ότι δεν απαιτείται κάποιος τρίτος κόμβος (Orderer node και Notary Node) για τον επίτευξη των ιδιωτικών συμβολαίων. Αυτό το επιτυγχάνει με την υιοθέτηση του πρωτοκόλλου ασφαλείας του κρυπτονομίσματος Zcash, Zero-knowledge security layer (ZSL). Συγκεκριμένα δημιουργεί κατακερματισμένες ακολουθίες (hash values) του ισοζύγιού των συναλλασσόμενων, του ποσού της συναλλαγής και του τελικού ισοζυγίου που λειτουργούν ως αποδεικτικά στοιχεία χωρίς να αποκαλύπτονται τα στοιχεία των συναλλασσόμενων και των στοιχείων της συναλλαγής. Οι ακολουθίες ελέγχονται από τους υπόλοιπους κόμβους του δικτύου και εφόσον οι συναλλασσόμενοι τηρούν τα κριτήρια του ιδιωτικού συμβολαίου, η συναλλαγή πραγματοποιείται

[107]

6 ΚΕΦΑΛΑΙΟ 6ο – ΣΥΜΠΕΡΑΣΜΑΤΑ

6.1 Σύνοψη και συμπεράσματα

Το blockchain και η τεχνολογία κατανεμημένης υποδομής είναι συναρπαστικές πολλά υποσχόμενες εξελίξεις για τον κλάδο των χρηματοπιστωτικών υπηρεσιών. Ενώ υπάρχουν σημαντικά δυνητικά οφέλη από την εφαρμογή της τεχνολογίας, το να την εφαρμόσει κάποιος με επιτυχία είναι μια πρόκληση. Λαμβάνοντας υπόψη προσεκτικά το πώς η τεχνολογία θα μπορούσε να καλύψει τις ανάγκες των επιχειρήσεων, καθώς και το ρόλο άλλων εξωτερικών και εσωτερικών παραγόντων, οι επιχειρήσεις μπορούν να βελτιώσουν σημαντικά την πιθανότητα ότι οι πρωτοβουλίες τους για την κατανεμημένη υποδομή θα πετύχουν.

Για την προσέγγιση της σωστής υλοποίησης θα πρέπει ο εκάστοτε οργανισμός ή επιχείρηση να είναι ενημερωμένοι σχετικά με τους διαφορετικούς τύπους BlockChain που υπάρχουν, καθώς και για τα πλεονεκτήματα και τα μειονεκτήματα του καθενός. Τα τέσσερα αρχικά ερωτήματα που πρέπει να τεθούν είναι τα εξής:

- Το βιβλιάριο θα είναι κατανεμημένο?
- Ποιοι χρήστες και με ποιο τρόπο θα έχουν πρόσβαση σε αυτό το δίκτυο?
- Θα έχουν όλοι οι συμμετέχοντες τα ίδια δικαιώματα?
- Με ποιο τρόπο θα επαληθεύονται και θα καταχωρούνται οι συναλλαγές πληροφορίας στο βιβλιάριο, με ποιον τρόπο θα γίνεται δηλαδή η συναίνεση στο σύστημα?

Λαμβάνοντας υπόψιν λοιπόν τα παραπάνω, πριν ξεκινήσει η υλοποίηση θα πρέπει να έχει μελετηθεί και αποφασιστεί ο τύπος του Blockchain ως προς το δικαίωμα συμμετοχής σ' αυτό. Αν το επιθυμητό αποτέλεσμα είναι ο κάθε χρήστης να έχει πρόσβαση και να συμμετέχει στο δίκτυο, τότε θα πρέπει να είναι τύπου public. Από την άλλη πλευρά αν η συμμετοχή θα πρέπει να ελέγχεται από κάποια κεντρική αρχή, η οποία θα γνωρίζει όλους τους συμμετέχοντες, τότε θα πρέπει η υλοποίηση να βασιστεί στον τύπο των private Blockchains. Όπως αναλυτικά περιγράψαμε στο κεφάλαιο 4 τα public blockchains μπορεί να είναι permissionless ή permissioned, καταλήγοντας έτσι σε δύο υπό-κατηγορίες, public-permissionless και public-permissioned blockchains, οι κύριες διαφορές των οποίων αφορούν κυρίως τα δικαιώματα των χρηστών στο δίκτυο.

Στην συνέχεια για τον σχεδιασμό της πλατφόρμας blockchain καθοριστικό ρόλο παίζει ο τρόπος με τον οποίο θα επαληθεύονται και θα καταχωρούνται οι συναλλαγές στο βιβλιάριο. Η διαδικασία αυτή στην συγκεκριμένη τεχνολογία ορίζεται ως συναίνεση και έχουν ήδη δημιουργηθεί πολλοί αλγόριθμοι με διαφορετικά χαρακτηριστικά , αλλά εξυπηρετώντας τον ίδιο σκοπό. Σ' ένα public blockchain , όπως είναι το Bitcoin για παράδειγμα χρειάζεται αρκετά μεγάλη επεξεργαστική ισχύς για τον μηχανισμό συναίνεσης, γνωστός ως Proof-of-Work. Ο συγκεκριμένος μηχανισμός έχει υιοθετήσει την λογική της ανταμοιβής των χρηστών που συμβάλλουν στην επαλήθευση. Με μία τελείως διαφορετική τακτική προσεγγίζει η πλατφόρμα Ripple το θέμα της συναίνεσης, επιλέγει μία ομάδα επικυρωτών η οποία είναι υπεύθυνη για την επικύρωση των συναλλαγών. Ο

αλγόριθμος συναίνεσης της συγκεκριμένης πλατφόρμας είναι γνωστός ως Proof-of-Correctness και είναι βελτιστοποιημένος και ταχύτερος από τον PoW. Κάποια επίσης αρκετά διαδεδομένα μοντέλα κατανεμημένης επικύρωσης είναι το Proof-of-Stake στο οποίο επιλέγεται ο δημιουργός του επόμενου μπλοκ βάση συνδυασμών τυχαίας επιλογής και το Byzantine Fault Tolerance (BFT) που εξασφαλίζει την ικανότητα να επιτύχει η επαλήθευση και στην περίπτωση που υπάρχουν αντίπαλοι κόμβοι ή αν οι κόμβοι βρεθούν εκτός δικτύου. Δεν χρειάζεται εξορύκτες και βρίσκει μεγάλη εφαρμογή σε ιδιωτικά blockchain όπως το Hyperledger Fabric.

Συνοψίζοντας η blockchain τεχνολογία έχει μεγάλες δυνατότητες για να οδηγήσει το επόμενο κύμα της καινοτομίας στο IoT και μπορεί να προωθήσει την εμφάνιση νέων επιχειρηματικών μοντέλων, τροποποιώντας σημαντικά τα υπάρχοντα συστήματα και τις διαδικασίες σε διάφορους τομείς της σύγχρονης καθημερινότητας. Πιθανές επιπτώσεις της εφαρμογής της, ωστόσο, θα πρέπει να λαμβάνουν υπόψη συγκεκριμένα πλαίσια χρήσης.

Κλείνοντας, με την ολοκλήρωση της διπλωματικής εργασίας προκύπτει ένα κρίσιμο και βασικό ζήτημα. Καθώς η τεχνολογία του blockchain εξελίσσεται, για την επιτυχημένη εφαρμογή της απαιτούνται μία σειρά νέων δεξιοτήτων που πρέπει να αποκτηθούν από τις επιχειρήσεις. Πέρα από τις τεχνικές δεξιότητες που απαιτούνται για την υλοποίηση και εγκατάσταση των δικτύων, απαραίτητες είναι και οι ικανότητες σχετικές με την αναγνώριση των ωφελειών από την χρήση της συγκεκριμένης τεχνολογίας, των πλαισίων εφαρμογής της και του πιθανού ρίσκου που αναλαμβάνουν οι επιχειρήσεις σε κάθε περίπτωση. Οι συγκεκριμένες ικανότητες απαιτούν την πλήρη κατανόηση της τεχνολογίας και των αλλαγών που μπορεί να επιφέρει [91].

Στον πίνακα 3 αξιολογούνται οι παράμετροι που πρέπει να λαμβάνονται υπόψιν πριν την δημιουργία ή τη χρήση κάποιου δικτύου για ορισμένες από τις πιο διαδεδομένες πλατφόρμες Blockchain, καθώς επίσης καταγράφονται και κάποιες πληροφορίες για κάθε τεχνολογία.

	Bitcoin	**Ripple**	**Hyperledger Fabric**	**Corda**	**Quorum**
Initial Release	2009	2012	2016	2016	2016
Network Permission	Public-Permissionless	Public-Permissioned	Private	Private	Private
Consensus Algorithm	(Proof-of-Work) PoW	Ripple Protocol Consensus Algorithm (RPCA) Proof-of-Correctness (PoC)	Byzantine Fault Tolerance (BFT)	Notary nodes can run several consensus algorithm	Raft

Smart Contracts Support	Possible, but not obvious	No	Yes	Yes	Yes
Mining for New Public Coins	Yes	No	No	No	No
Open Source	Yes	Yes	Yes	Yes	Yes
Average Transaction per Second	5-7tps	>1500tps	Can achieve thousands tps (depending upon number of endorsers, orderers and committers)	~170tps	A few 100s
Energy Consumption	High	Very Low	Very Low	Low	Low
Cryptocurrency	Bitcoin(BTC)	Ripple(XRP)	None	None	None
Programming Language	Most of the code is written in C++	C++	Go, Java, JavaScript	Kotlin, Java	Solidity
Governance	Bitcoin Developers	Ripple Labs	Linux Foundation in charge	R3 Company in charge	Ethereum developers

Πίνακας 3: Σύγκριση Πλατφορμών Blockchain

6.2 Όρια και περιορισμοί της έρευνας

Στο παρόν κεφάλαιο γίνεται μια σύντομη ανάλυση στα όρια και στους περιορισμούς που αντιμετωπίστηκαν κατά την έρευνα γι' αυτήν την εργασία. Είναι σημαντική η αναφορά πως τα δίκτυα Blockchain είναι μια νέα σχετικά τεχνολογία, η οποία τα τελευταία χρόνια έχει προκαλέσει το ενδιαφέρον μεγάλου μέρους της επιστημονικής κοινότητας. Λόγω της πρόσφατης εμφάνισης της λοιπόν αλλά και της σημαντικότητας της, ο όγκος των πληροφοριών και των θεωριών ήταν αρκετά μεγάλος , αλλά από την άλλη πλευρά οι εφαρμογές την δεν έχουν δοκιμαστεί ακόμα εκτενώς. Ήταν λοιπόν αρκετά δύσκολο να διαχωριστεί η χρήσιμη και αξιόπιστη πληροφορία από ασαφείς αναφορές. Καθώς το Blockchain αποτελεί κάτι νέο, με επέκταση σε πολλούς τομείς δεν υπάρχουν ακόμα σαφείς βέλτιστες πρακτικές αλλά ούτε και πλήρεις έρευνες και πειραματισμοί γύρω από αυτό. Η επεκτασιμότητα και τα όρια του Blockchain

δεν έχουν καθοριστεί ακόμα, με αποτέλεσμα πολλές επιχειρήσεις να επενδύουν σε δαπανηρές εφαρμογές και λύσεις αναζητώντας την καλύτερο τρόπο αξιοποίησης των δυνατοτήτων του.

Τέλος οι διαρκείς αλλαγές της συγκεκριμένης τεχνολογίας, η συνεχής εμφάνισης νέων τεχνολογιών και αλγορίθμων και η παραλλαγή ήδη υπάρχοντών συστημάτων αποτέλεσαν άλλο ένα εμπόδιο για την συγκεκριμένη εργασία. Όπως προκύπτει από τα παραπάνω για την ανάλυση αυτών των καταστάσεων απαιτείται έρευνα καθ΄ όλη τη διάρκεια της εκπόνησης για την αποφυγή καταγραφής αναξιόπιστων πληροφοριών.

6.3 Μελλοντικές επεκτάσεις

Είναι αρκετά δύσκολο να προβλέψουμε τα όρια επέκτασης αυτής της νέας τεχνολογίας, τον βαθμό υιοθέτησης από τους ενδιαφερόμενους, την εξέλιξη και την τελική της πορεία. Το μόνο για το οποίο μπορούμε να είμαστε βέβαιοι είναι πως η παρούσα διπλωματική εργασία αποτελεί έναν τεχνολογικό οδηγό για την βελτίωση διαδικασιών όπου τα δίκτυα Blockchain μπορούν να προσφέρουν τα πλεονεκτήματα τους.

Η υιοθέτηση της από οργανισμούς, κεντρικές αρχές ακόμα και κυβερνήσεις εξαρτάται σαφώς σε μεγάλο βαθμό και από τους πολίτες. Το κατά πόσο οι τελευταίοι έχουν την θέληση αλλά και την ωριμότητα να ανταπεξέλθουν στις απαιτήσεις που ορίζει η αποκεντρωμένη φιλοσοφία και να εκμεταλλευτούν τις ευκαιρίες που μπορεί να τους προσφέρει. Θα ήταν σίγουρα πιο εύκολη η διαδικασία της υιοθέτησης αν κάθε ενδιαφερόμενος θα μπορούσε να ενημερωθεί για τις υπάρχουσες τεχνολογίες αναλυτικά μέσω έγκυρων αποτελεσμάτων και δεδομένων και να οδηγηθεί στις καταλληλότερες βάσει της αξιολόγησης των χαρακτηριστικών που επιθυμεί να έχει η πλατφόρμα Blockchain που θέλει να υλοποιήσει ή να συμμετάσχει.

Σκοπός της παρούσας διπλωματικής εργασίας ήταν η μελέτη , η κατηγοριοποίηση και η σύγκριση των ήδη υπαρχουσών τεχνολογιών Blockchain, με περεταίρω ανάλυση όμως της πληροφορίας και των συμπερασμάτων θα μπορούσε να γίνει κάποια εφαρμογή συνεχούς συλλογής δεδομένων με στόχο την κατηγοριοποίηση όλων των τεχνολογιών βάσει των πλεονεκτημάτων, μειονεκτημάτων τους, της δημοτικότητας, των μοντέλων ασφαλείας, των απαιτήσεων εξοπλισμού και ενέργειας και άλλων χαρακτηριστικών με στόχο την ενημέρωση των πολιτών σύμφωνα με τις τελευταίες εξελίξεις. Επίσης μία ακόμα προοπτική επέκτασης του περιεχομένου της εργασίας είναι η μοντελοποίηση των δεδομένων και το μοντέλο αυτό να χρησιμοποιηθεί σ’ ένα αυτοματοποιημένο πληροφοριακό σύστημα το οποίο θα προτείνει κατάλληλες τεχνολογίες σε κάποιον που ενδιαφέρεται να αναπτύξει μια εφαρμογή βασισμένη σε Blockchain ή να συμμετάσχει σε κάποια από τις προαναφερθείσες πλατφόρμες.

7 ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΝΑΦΟΡΕΣ

7.1 Βιβλιογραφία

[1] Dennis Luciano and Gordon Prichett, "Cryptology: From Caesar Ciphers to Public-Key Cryptosystems". [Online]. Available: http://www.math.stonybrook.edu/~moira/mat331-spr10/papers/1987%20LucianoCryptology%20From%20Caesar%20Ciphers%20to.pdf

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[3] H. Adkins, "Google online security blog: An update on attempted man-in-themiddle attacks.," Google, 2011. [Online]. Available: https://security.googleblog.com/2011/08/update-on-attempted-man-in-middle.html.

[4] M. Bastiaan, "Preventing the 51%-Attack: a Stochastic Analysis of TwoPhase Proof of Work in Bitcoin,"[Online]. Available: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf.

[5] I. Eyal and E. G. Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," in International Conference on Financial Cryptography and Data Security, Heidelberg, 2014.

[6] A. Antonopoulos, Mastering Bitcoin: unlocking digital cryptocurrencies, O'Reilly Media, Inc., 2014.

[7] I. B. Damgard, "A design principle for hash functions," Conference on the Theory and Application of Cryptography, pp. 416 - 427, 20 August 1989.

[8] J. Katz and Y. Lindell, "Introduction to modern cryptography," CRC press, 6 November 2014.

[9] S. Haber and S. W. Stornetta, "How to time-stamp a digital document," Conference on the Theory and Application of Cryptography, pp. 437 - 455, 11 August 1990.

[10] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten Princeton University , "The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries " [Online]. Available: https://pdfs.semanticscholar.org/c55a/6c95b869938b817ed3fe3ea482bc65a7206b.pdf.

[11] R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," in Conference on the Theory and Application of Cryptographic Techniques, Heidelberg, 2000.

[12] A. Lobil and J. Naab, "Namecoin," 2014. [Online]. Available: namecoin.info.

[13] Y. Assia, V. Buterin, M. Resonfeld and R. Lev, "Colored Coins - Whitepaper," [Online]. Available: https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit#heading=h.pr8n14cpqri5.

[14] V. Buterin, "Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform," 2013. [Online].

[15] T. Swanson, "Great chain of numbers: A guide to smart contracts, smart property and trustless asset management," Amazon Digital Services, 2014.

[16] C. Dannen, Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners, 2017.

[17] "Gas and transaction costs," [Online]. Available: https://ethereum.gitbooks.io/frontier-guide/content/costs.html.

[19] J. C. Benton, "Global Information Assurance Certification Paper," GIAC Certifications, 2003.

[20] A. Carlisle and S. Lloyd, Understanding PKI: concepts, standards, and deployment considerations, Addison-Wesley Professional, 2003.

[21] J. R. Vacca, Public key infrastructure: building trusted applications and Web services, CRC Press, 2004.

[22] F. Warwick and M. S. Baum, Secure electronic commerce: building the infrastructure for digital signatures and encryption, Prentice Hall PTR, 2000.

[23] C. Germano, "Walking the web of trust," in Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2000). Proeedings. IEEE 9th International Workshops on. IEEE, 2000.

[24] C. Fromknecht, D. Velicanu and S. Yakoubov, "A Decentralized Public Key Infrastructure with Identity Retention," IACR Cryptology ePrint Archive, p. 803, 2014.

[25] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau and A. Narayanan, "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design," WEIS, 2015.

[26] K. Lewison and F. Corella, "Backing Rich Credentials with a Blockchain PKI," Tech. Rep, 2016.

[27] M. Baldi, F. Chiaraluce, E. Frontoni, G. Gottardi, D. Sciarroni and L. Spalazzi, "Certificate Validation Through Public Ledgers and Blockchains," ITASEC, pp. 156 - 165, 2017.

[28] M. Al-Bassam, "SCPKI: A Smart Contract-based PKI and Identity System," in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017.

[29] B. Fredriksson, "A Distributed Public Key Infrastructure for the Web Backed by a Blockchain," 2017.

[30] M. Ali, J. C. Nelson, R. Shea and M. J. Freedman, "Blockstack: A Global Naming and Storage System Secured by Blockchains," in USENIX Annual Technical Conference, 2016.

[31] S. Matsumoto and R. M. Reischuk, "IKP: Turning a PKI Around with Blockchains," in IACR Cryptology ePrint Archive, 2014.

[32] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," 2018. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf.

[33] D. R. L. Brown, "SEC 2: Recommended Elliptic Curve Domain Parameters," Certicom Research, 27 January 2010.

[34] D. Derler, C. Hanser and D. Slamanig, "Revisiting Cryptographic Accumulators, Additional Properties and Relations to Other Primitives," in Cryptographers' Track at the RSA Conference, Cham, 2015.

[35] Hyperledger Fabric Docs, 2018. Smart Contracts. [Ηλεκτρονικό] Available at: https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html?highlight=smart%20contracts#smart-contracts

[36] Galvin, D., 2018. IBM and Walmart: Blockchain for Food Safety, s.l.: s.n.

[37] Buterin, V., 2013. Ethereum White Paper. [Ηλεκτρονικό] Available at: https://web.archive.org/web/20161021061647/https://www.weusecoins.com/assets/pdf/library/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[38] Bauerle, N., 2017. What is a Distributed Ledger?. [Ηλεκτρονικό] Available at: https://www.coindesk.com/information/what-is-a-distributed-ledger

[39] Meunier, S., 2016. Blockchain technology - a very special kind of Distributed Database. [Ηλεκτρονικό] Available at: https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118

[40] Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. [Ηλεκτρονικό] Available at: https://bitcoin.org/bitcoin.pdf

[41] Σκούφου, Δ., 2018. Έντονη κινητικότητα σε όλα τα πεδία της Γαλακτοβιομηχανίας. σελφ σέρβις, 8, Issue 485, pp. 38-40.

[42] Tapscott, D. & Tapscott, A. (2016). Blockchain Revolution. Great Britain: Clays Ltd, St Ives plc

[43] Vincenzo Morabito (2017). Business Innovation Through Blockchain. Cham, Switzerland Springer International Publishing AG.

[44] Swan, M. (2015). Blockchain Blueprint for a new economy. United States of America: O,Reilly Media, Inc.

[45] Introducing Piclo. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://www.openutility.com/piclo/

[46] Gupta, M. (2017). Blockchain IBM Limited Edition. United States of America: John Wiley & Sons, Inc.

[47] Laurence, T. (2017). Blockchain. Canada: John Wiley & Sons, Inc.

[48] Local renewable energy for businesses. (2018, Φεβρουάριος 20). Ανακτήθηκε από https://piclo.uk/

[49] Antonopoulos, A.M. (2017). Mastering Bitcoin (2nd Edition). United States of America: O,Reilly Media Inc.

[50] Abernathy, W. J. (1978). Patterns of industrial innovation. Technology review, 80(7), 40-47.

[51] Accenture, Monatery Authority Of Singapore. (2017). Project Ubin Phase 2: Re-imagining Interbank Real Time Gross Settlement System Using Distributed Ledger Tecnhlogoies.

[52] Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. ACM computing surveys (CSUR), 36(4), 335–371.

[53] Angela S.M. Irwin and George Milad. (2016). The use of crypto-currencies in funding violent jihad. Journal of Money Laundering Control, 19(4), 407-425.

[54] Delloitte, Monetary Authority of Singapore. (2016). Project Ubin: SGD on Distributed Ledger - Phase 1.

[55] Liu, J., Kauffman, R. J., & Ma, D. (2015). Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem. Electronic Commerce Research and Applications, 14(5), 372-391.

[56] Nielsen, P. M. (2017). ZSL Proof of Concept. Github Repository.

[57] Schwartz, D., Youngs, N., & Britto, A. (2014). The Ripple protocol consensus algorithm. Ripple Labs Inc White Paper(5).

[58] Shin, L. (2017, October 23). Will This Battle For The Soul Of Bitcoin Destroy It? Ανάκτηση από Forbes: https://www.forbes.com/sites/laurashin/2017/10/23/will-this-battle-for-the-soul-of-bitcoin-destroy-it/#16f973c03d3c

[59] Southurst, J. (2014, December 3). Australian Federal Investigators Look at Bitcoin's Organized Crime Role. Ανάκτηση από Coindesk: https://www.coindesk.com/australian-federal-investigators-look-bitcoins-organized-crime-role/

[60] Souto, J. E. (2015). Business model innovation and business concept innovation as the context of incremental innovation and radical innovation. Tourism Management, 51, 142-155.

[61] Morgan, J. P. (2016). Quorum Whitepaper. New York: JP Morgan Chase.

[62] Mills, D., Wang, K., Malone, B., Ravi A.,Marquardt J., Chen, Badev, A., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellirhorpe, M., Ng, W., Baird, M. (2016). Distributed ledger technology in payments, clearing, and settlement. Finance and Economics Discussion Series, Washington: Board of Governors of the Federal Reserve System.

[63] Euro Banking Association. (2015). Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios. An exploration for transaction banking and payments professionals. EBA Working Group on Electronic and Alternative Payments, 5(11).

[64] European Central Bank. (2015). Virtual currency schemes – a further analysis.

[65] Walport, M. G. C. S. A. (2016). Distributed ledger technology: Beyond blockchain. UK Government Office for Science.

[66] Waters, R. (2016, May 17). Automated company raises equivalent of $120M in digital currency. Ανάκτηση από CNBC: https://www.cnbc.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html

[67] Zohar, A. (2015). Bitcoin: under the hood. Communications of the ACM, 58(9), 104-113.

[68] Wessel R. the Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies [Βιβλίο]. - 2016.

[69] Salah K. IoT Security: Review, Blockchain Solutions, and Open Challenges [Βιβλίο]. - 2017.

[70] Sivaraman V. Network-level security and privacy for smarthome IoT devices [Άρθρο]. - 2015. - σσ. 163-167.

[71] Steve H. Internet of Things, Blockchain and Shared Economy Applications [Άρθρο]. - 2014.

[72] Arabo A. Privacy in the age of mobility and smart devices in smart homes [Συνέδριο]. - 2014. - σσ. 819-826.

[73] Carminati B. Enhancing user control on personal data udage in internet of things ecosystems [Άρθρο]. - 2016. - σσ. 291-298.

[74] David G. Kickstarter My Heart: Extraordinary Popular Delusions and the Madness of Crowdfunding Constraints and Bitcoin Bubbles [Άρθρο]. - 2014.

[75] Hashemi S. H. World of empowered IoT users [Άρθρο]. - 2016. - σσ. 13-24.

[76] Angela S.M. Irwin and George Milad. (2016). The use of crypto-currencies in funding violent jihad. Journal of Money Laundering Control, 19(4), 407-425.

[77] C. Fromknecht, D. Velicanu and S. Yakoubov, "A Decentralized Public Key Infrastructure with Identity Retention," IACR Cryptology ePrint Archive, p. 803, 2014.

[78] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau and A. Narayanan, "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design," WEIS, 2015.

[79] K. Lewison and F. Corella, "Backing Rich Credentials with a Blockchain PKI," Tech. Rep, 2016.

[80] M. Baldi, F. Chiaraluce, E. Frontoni, G. Gottardi, D. Sciarroni and L. Spalazzi, "Certificate Validation Through Public Ledgers and Blockchains," ITASEC, pp. 156 - 165, 2017.

[81] David, B., Gaži, P., Kiayias, A., & Russell, A. (2018). Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 10821 LNCS, pp. 66–98). Springer, Cham. https://doi.org/10.1007/978-3-319-78375-8_3

[82] Lindell, Y., & Pinkas, B. (2018). Secure Multiparty Computation for Privacy-Preserving Data Mining. Journal of Privacy and Confidentiality, 1(1). https://doi.org/10.29012/jpc.v1i1.566

[83] Schneier, B. (2018). Cryptography after the aliens land. IEEE Security and Privacy, 16(5), 87–88. https://doi.org/10.1109/MSP.2018.3761724

[84] Tasca, P., & Tessone, C. J. (2017). Taxonomy of Blockchain Technologies. Principles of Identification and Classification. Retrieved from http://arxiv.org/abs/1708.04872

[85] Troncoso, C., Isaakidis, M., Danezis, G., & Halpin, H. (2017). Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments. Proceedings on Privacy Enhancing Technologies, (4), 307–329. https://doi.org/10.1515/popets-2017-0052

[86] Ζορκάδης, Β. (2002). Κρυπτογραφία. Πάτρα: Εκδόσεις ΕΑΠ.

[87] Πολυτίδου, Ε. (2018). Τεχνολογίες Blockchain σε Συστήματα Υποδομής Δημόσιου Κλειδιού και Διαχείρισης Ηλεκτρονικής Ταυτότητας. Ελληνικό Ανοικτό Πανεπιστήμιο.

[88] Stallings, W. (2017). Cryptography and network security principles and practice (Seventh). Pearson.

[89] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. IJACSA) International Journal of Advanced Computer Science and Applications, 9(3). https://doi.org/10.14569/IJACSA.2018.090354

[90] Accenture, Monatery Authority Of Singapore. (2017). Project Ubin Phase 2: Re-imagining Interbank Real Time Gross Settlement System Using Distributed Ledger Technologies.

[91] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303.

7.2 Ιστότοποι

[92] http://cacr.uwaterloo.ca/hac/

[93]https://www.researchgate.net/publication/220688776_The_Foundations_of_Cryptography_-_Volume_1_Basic_Techniques

[94] Blair, M. (2017). How does ECDSA work in Bitcoin. Retrieved December 28, 2018, from https://medium.com/@blairlmarshall/how-does-ecdsa-work-in-bitcoin-7819d201a3ec

[95] J. Boersma and M. Bulters, "Blockchain Technology: 9 Benefits & 7 Challenges," Deloitte, [Online]. Available: https://blog.deloitte.com.ng/blockchain-technology-benefits-challenges/.

[96] Bauerle, N., 2017. What is a Distributed Ledger?. [Ηλεκτρονικό] Available at: https://www.coindesk.com/information/what-is-a-distributed-ledger

[97] The Linux Foundation, 2018. Blockchain for Business - An Introduction to Hyperledger Technologies. [Ηλεκτρονικό] Available at: https://www.edx.org/course/blockchain-for-business-an-introduction-to-hyperledger-technologies

[98] Newman, L. H. (2016). Friday's East Coast Internet Outage Is a Major DDOS Attack | WIRED. Retrieved December 5, 2019, from https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

[99] https://www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf

[100] Lumb, R., Treat, D., & Jelf, O. (2016). Why distributed ledger technology must adapt to an imperfect world. Retrieved from https://www.accenture.com/t00010101T000000__w__/es-es/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf

[101] Jayachandran, P. (2017). The difference between public and private blockchain - Blockchain Unleashed. Retrieved January 26, 2019, from https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[102] Schneier, B. (2018). Cryptography after the aliens land. IEEE Security and Privacy, 16(5), 87–88. https://doi.org/10.1109/MSP.2018.3761724

[103] Intel Corporation. (2017). Proof of Elapsed Time. Sawtooth Lake. Retrieved from https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp

[104] Insights, M. (2015, June 25). Survey Shows Americans Trust Technology Firms More Than Banks and Retailers. Ανάκτηση από Medici: https://gomedici.com/survey-shows-americans-trust-technology-firms-more-than-banks-and-retailers/

[105] Naughton, J. (2017). The trouble with bitcoin and big data is the huge energy bill. Retrieved January 16, 2019, from https://www.theguardian.com/commentisfree/2017/nov/26/trouble-with-bitcoin-big-data-huge-energy-bill

[106] Coin Market Cap. (2018). All Cryptocurrencies | CoinMarketCap. Retrieved January 25, 2019, from https://coinmarketcap.com/all/views/all/

[107] Ripple. (2015). Transaction Cost. Ανάκτηση από Ripple: https://developers.ripple.com/transaction-cost.html

[108] Nathan Reiff. (2017). what is ERC-20 and what Does it Mean for Ethereum? Ανακτήθηκε Φεβρουάριος 24, 2018 από https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

[109] The World Bank. (2018). Commercial bank branches (per 100,000 adults). Ανάκτηση από International Monetary Fund, Financial Access Survey: https://data.worldbank.org/indicator/FB.CBK.BRCH.P5