ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΛΟΓΙΣΤΙΚΗ ΦΟΡΟΛΟΓΙΑ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ

Διπλωματική Εργασία

Η Τεχνολογία Blockchain και οι Εφαρμογές της στη Λογιστική

Της

Ξένιας Δημητρίου

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος

στη

Λογιστική Φορολογία και Χρηματοοικονομική Διοίκηση

Θεσσαλονίκη 2022

Περίληψη

Η παρούσα διπλωματική εργασία ασχολείται με την ανάλυση της τεχνολογίας blockchain και την επίδραση που θα έχει στη λογιστική. Αρχικά, παρουσιάζεται η βιβλιογραφική επισκόπηση με σκοπό τον προσδιορισμό των βασικών θεμάτων της σύγχρονης βιβλιογραφίας σχετικά με το blockchain. Στη συνέχεια αναλύεται λεπτομερώς η τεχνολογία αυτή, περιγράφεται η πορεία της εξέλιξής της και το ενδιαφέρον επικεντρώνεται στη λογιστική βασισμένη στο blockchain. Σκοπός είναι να αναγνωριστούν οι λόγοι που καθιστούν το blockchain μία από τις σημαντικότερες τεχνολογίες της σύγχρονης εποχής και να καθοριστεί ο τρόπος που μπορεί να εφαρμοστεί στη λογιστική. Η επίδραση στον κλάδο της λογιστικής θα είναι αξιοσημείωτη και θα φέρει πολλά πλεονεκτήματα και ορισμένες προκλήσεις. Τέλος, αναφέρονται τα συμπεράσματα και αναγνωρίζονται προτάσεις για μελλοντική έρευνα που αναμένεται να έχουν μεγάλη αξία.

Λέξεις-Κλειδιά: blockchain, χαρακτηριστικά, εξέλιξη, εφαρμογές, λογιστική

Abstract

This thesis deals with the analysis of blockchain technology and its impact on accounting. Initially, a literature review is presented in order to identify interesting topics and the current state of blockchain technology. Hereafter, blockchain is analyzed in detail, its evolution is described and the analysis focuses on blockchain-based accounting. The aim is to identify the reasons why blockchain is considered to be one of the most important technologies of the modern age and to define how it can be applied in accounting. The impact in the field of accounting will be remarkable and will bring many advantages and challenges. Finally, conclusions and suggestions for future research are identified that are anticipated to be of a great value.

Keywords: blockchain, features, development, applications, accounting

Περιεχόμενα

Ευρετήριο Πινάκων

Ευρετήριο Εικόνων

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1. Εισαγωγικές Παρατηρήσεις

Μία νέα έννοια, το επίπεδο δημοσιότητας της οποίας έχει αυξηθεί ραγδαία τα τελευταία χρόνια είναι το κρυπτονόμισμα. Το κρυπτονόμισμα αποτελεί μία ηλεκτρονική μορφή χρήματος, ένα ψηφιακό νόμισμα χωρίς φυσική υπόσταση το οποίο διαθέτει ορισμένα χαρακτηριστικά που το καθιστούν διαφορετικό από τα συμβατικά νομίσματα. Η εμφάνιση των κρυπτονομισμάτων οδήγησε στην παράλληλη εμφάνιση μιας νέας τεχνολογίας, στην οποία βασίζεται η ύπαρξή τους που ονομάζεται blockchain. Η τεχνολογία blockchain είναι μία αναδυόμενη τεχνολογία, η οποία έχει προκαλέσει το ενδιαφέρον του ακαδημαϊκού και του επιχειρηματικού χώρου, καθώς θεωρείται μία από τις τεχνολογίες που μπορεί να συμβάλει στην τέταρτη βιομηχανική επανάσταση, να συνδυαστεί με άλλες τεχνολογίες όπως το Internet of Things, τα Big Data και την Τεχνητή Νοημοσύνη και να επιδράσει σημαντικά σε πολλούς τομείς μεταξύ των οποίων είναι η Χρηματοοικονομική Λογιστική.

1.2. Σκοπός και Ερευνητικά Ερωτήματα

Σκοπός της διπλωματικής εργασίας είναι η κατανόηση της τεχνολογίας blockchain και η ανάλυση της επίδρασής της στον κλάδο της λογιστικής. Τα ερευνητικά ερωτήματα τα οποία θα απαντηθούν μέσω της συγκεκριμένης εργασίας αφορούν την αναδυόμενη τεχνολογία blockchain, για ποιους λόγους θεωρείται μία από τις σημαντικότερες τεχνολογίες της σημερινής εποχής και ποιες οι αδυναμίες της. Επιπλέον, βασικό ερευνητικό ερώτημα αποτελούν οι εφαρμογές που θα έχει στη

λογιστική και ειδικότερα με ποιον τρόπο θα εφαρμοστεί και ποιες θετικές επιπτώσεις και προκλήσεις θα φέρει στον κλάδο της λογιστικής.

1.3. Δομή

Η δομή της διπλωματικής εργασίας είναι η παρακάτω: Μετά το πρώτο κεφάλαιο της Εισαγωγής ακολουθεί το δεύτερο κεφάλαιο στο οποίο παρατίθεται η βιβλιογραφική επισκόπηση όπου επισημαίνονται μερικά από τα βασικότερα ζητήματα που έχουν απασχολήσει τον ακαδημαϊκό χώρο σχετικά με την τεχνολογία blockchain. Το επόμενο κεφάλαιο αποτελεί μία λεπτομερή παρουσίαση της τεχνολογίας blockchain. Ειδικότερα, αναφέρονται οι διάφοροι ορισμοί που έχουν δοθεί για το blockchain, επεξηγείται η ορολογία και οι βασικές αρχές, περιγράφεται η αρχιτεκτονική του, τα χαρακτηριστικά του, η ταξινόμηση των δικτύων σε τρεις κατηγορίες αλλά και η κριτική που δέχεται λόγω των αδυναμιών που παρουσιάζει. Στο τέταρτο κεφάλαιο γίνεται λόγος για τις εφαρμογές της τεχνολογίας blockchain στον κλάδο της λογιστικής. Το κεφάλαιο αυτό επικεντρώνεται κυρίως στη χρηματοοικονομική λογιστική, στις νέες μεθόδους που θα εφαρμοστούν και την επίδραση που θα έχουν. Επιπλέον, εκτός από τα πλεονεκτήματα της εφαρμογής, εντοπίζονται και οι αρνητικές επιπτώσεις που θα προκύψουν αλλά και οι τρόποι αντιμετώπισης αυτών. Στο πέμπτο και τελευταίο κεφάλαιο αναφέρονται τα συμπεράσματα της εργασίας και γίνονται προτάσεις για μελλοντική έρευνα.

ΚΕΦΑΛΑΙΟ 2: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1. Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζεται εν συντομία η βιβλιογραφική επισκόπηση για την τεχνολογία αλυσίδας συστοιχιών και αναγνωρίζονται ορισμένα σημαντικά σημεία τα οποία αναλύονται εις βάθος και στα επόμενα κεφάλαια. Η τεχνολογία blockchain έχει προσελκύσει το ενδιαφέρον ιδιαίτερα τα τελευταία χρόνια, όπου όχι μόνο το ακαδημαϊκό αλλά και το επιχειρηματικό περιβάλλον συζητούν και επισημαίνουν τις εφαρμογές που μπορεί να έχει στο μέλλον. Με την είσοδο στην τέταρτη βιομηχανική επανάσταση και το βασικό ρόλο που θα μπορούσε να διαθέτει η τεχνολογία στη εξέλιξή της, το ερευνητικό ενδιαφέρον έχει αυξηθεί σημαντικά.

2.2. Βασικά Θέματα της Τεχνολογίας Blockchain

Η τεχνολογία blockchain αναπτύχθηκε μετά την παρουσίαση του κρυπτονομίσματος bitcoin το 2008 στο άρθρο «Bitcoin: A Peer-to-Peer Electronic Cash System» από το άτομο ή την ομάδα ατόμων Satoshi Nakamoto, η πραγματική ταυτότητα του οποίου δεν έχει αποκαλυφθεί έως και σήμερα. Με το πέρασμα του χρόνου πολλοί ερευνητές έχουν ασχοληθεί με τον ορισμό, τα χαρακτηριστικά, την αρχιτεκτονική, τις διάφορες κατηγορίες δικτύων, τα πλεονεκτήματα που προσφέρει η τεχνολογία αλλά και τις αδυναμίες της. Επιπλέον, πολλοί ορισμοί έχουν δοθεί που επικεντρώνονται συνήθως σε διαφορετικά στοιχεία της τεχνολογίας. Σύμφωνα με τους Viriyasitavat και Hoonsopon (2019), η τεχνολογία blockchain ορίζεται ως μια τεχνολογία που επιτρέπει την αμεταβλητότητα και την ακεραιότητα των δεδομένων για τα οποία τηρείται αρχείο των συναλλαγών που έγιναν σε ένα σύστημα σε πολλούς κατανεμημένους

κόμβους που είναι συνδεδεμένοι σε ένα δίκτυο peer-to-peer. Στον συγκεκριμένο ορισμό γίνονται φανερές κάποιες από τις ιδιότητες της τεχνολογίας αυτής.

Οι Zheng et al. (2018) πραγματοποίησαν μία λεπτομερής ανάλυση της τεχνολογίας blockchain. Πιο συγκεκριμένα, αναφέρονται στα χαρακτηριστικά, στην αρχιτεκτονική, στην ταξινόμηση των αλυσίδων συστοιχιών, στα πρωτόκολλα συναίνεσης αλλά και στις εφαρμογές της, στις προκλήσεις και στους τρόπους αντιμετώπισης αυτών. Ειδικότερα, τα χαρακτηριστικά που αναφέρουν είναι η αποκέντρωση, η αυθεντικότητα και αμεταβλητότητα, η ανωνυμία και η δυνατότητα ελέγχου. Από την άλλη πλευρά, οι περιορισμοί που υπάρχουν για την εφαρμογή της σύμφωνα με την έρευνά τους είναι τρείς: η επεκτασιμότητα, η ιδιωτικότητα και το selfish mining. Μεγάλη σημασία έχουν τα μελλοντικά σχέδια και οι τάσεις που περιγράφονται για την καλύτερη εφαρμογή της τεχνολογίας αλυσίδας συστοιχιών και περιλαμβάνουν πέντε τομείς: το blockchain testing, τη διακοπή της τάσης υιοθέτησης κεντρικών δικτύων (εστίαση σε αποκεντρωμένα δίκτυα), τα big data analytics, τα smart contracts και την τεχνητή νοημοσύνη.

Παρόμοια ανάλυση έχουν πραγματοποιήσει και οι Monrat et al. (2019). Στο άρθρο τους περιγράφουν την αρχιτεκτονική των blocks, τα χαρακτηριστικά και τις κατηγορίες δικτύων blockchain, δίνοντας έμφαση στα πρωτόκολλα συναίνεσης, στα πλεονεκτήματα και τα μειονεκτήματα της τεχνολογίας. Επιπροσθέτως, αναλύονται και διάφοροι όροι της τεχνολογίας που έχουν σημασία για την κατανόησή της όπως κόμβος, συναλλαγή, block, διπλή δαπάνη, mining και μηχανισμοί συναίνεσης. Επίσης, γίνεται αναφορά στη χρήση του blockchain σε διάφορους κλάδους αλλά και στο μελλοντικό πεδίο εφαρμογής του.

Μεταξύ άλλων οι Monrat et al. (2019) τονίζουν την ανάγκη που υπάρχει να ελέγχεται σε κάθε περίπτωση, εάν η τεχνολογία αυτή είναι κατάλληλη για μία επιχείρηση μέσω της διαδικασίας τυποποίησης και της δοκιμής. Επίσης, επισημαίνεται ότι το blockchain και ειδικά τα smart contracts μπορούν να συνδυαστούν και με άλλες αναδυόμενες τεχνολογίες όπως τα Big Data και το Internet of Things (IoT) αλλά και να βρουν εφαρμογή σε κλάδους όπως ο τραπεζικός. Για το λόγο αυτό κρίνεται σημαντικό να ερευνηθεί η επίδοση των έξυπνων συμβολαίων, η ασφάλειά τους και γενικότερα να αντιμετωπιστούν οι αδυναμίες της τεχνολογίας

blockchain, ώστε να αναπτυχθούν περισσότερες καινοτόμες εφαρμογές στο επιχειρηματικό περιβάλλον. Αναφορικά με τους περιορισμούς της τεχνολογίας προσθέτουν στην ανάλυση των Zheng et al. (2018) τη διαλειτουργικότητα, την κατανάλωση ενέργειας και τη θέσπιση ρυθμιστικού πλαισίου.

Μία άλλη προσέγγιση σχετικά με την ομαδοποίηση των χαρακτηριστικών της αλυσίδας συστοιχιών αναφέρουν οι Seebacher και Schüritz (2017) και οι Ali et al. (2020). Πιο συγκεκριμένα, κατηγοριοποιούν τα χαρακτηριστικά σε δύο μεγάλες ομάδες, οι οποίες είναι στενά συνδεδεμένες και περιλαμβάνουν όλα τα επιμέρους χαρακτηριστικά: την εμπιστοσύνη και την αποκέντρωση.

Ο Lu (2019) στην έρευνά του επικεντρώνεται στα χαρακτηριστικά με βάση κυρίως τα πλεονεκτήματα που προσφέρουν και αναφέρει τα εξής: αποκεντρωμένο σύστημα, εμπιστοσύνη, διαφάνεια, δυνατότητα εντοπισμού και αυθεντικότητα, ανωνυμία και αξιοπιστία. Επιπροσθέτως, εκτός από τα χαρακτηριστικά εστιάζει στην εξέλιξη της τεχνολογίας, στις κατηγορίες δικτύων, στην αρχιτεκτονική αλλά και στην συνεργασία του blockchain με άλλους τομείς όπως το Internet of Things, την κυβερνοασφάλεια, τη διαχείριση δεδομένων και το cloud computing. Ακόμη, παρέχει μία σφαιρική οπτική για το θέμα περιγράφοντας τις αδυναμίες και τις προσκλήσεις της τεχνολογίας που πρέπει να αντιμετωπιστούν για την ευρεία εφαρμογή της.

Στο σημείο αυτό μία έρευνα που αξίζει να σημειωθεί είναι των Baidyanath και Rohit (2019), οι οποίοι επικεντρώνονται στις προκλήσεις που συναντώνται κατά την υιοθέτηση του blockchain σε βιομηχανίες και υπηρεσίες. Αναλυτικότερα, αναγνωρίζονται οι εξαιρετικές δυνατότητες που έχει το blockchain λόγω του τρόπου λειτουργίας του αλλά και τα εμπόδια που πρέπει να ξεπεραστούν για την εφαρμογή του. Το άρθρο αυτό έχει στόχο να επισημάνει τα πιο βασικά εμπόδια που παρουσιάζονται στην υιοθέτηση του blockchain και να τα αξιολογήσει ανάλογα με τη σημαντικότητα και τις σχέσεις αιτίας-αποτελέσματος που διαθέτουν. Η αναγνώριση των εμποδίων γίνεται μέσα από τη επιστημονική βιβλιογραφία και τα σχόλια των ειδικών και η αξιολόγησή τους με την τεχνική DEMATEL. Από την έρευνα αυτή προκύπτει ότι τα εμπόδια με τη μεγαλύτερη σημασία είναι: η επεκτασιμότητα, ο κίνδυνος της αγοράς, η αβεβαιότητα σχετικά με το ρυθμιστικό πλαίσιο και τη

μετάβαση στην νέα κατάσταση, η χρήση στην παραοικονομία, η ιδιωτικότητα και η βιωσιμότητα.

Ένα άλλο αξιοσημείωτο ζήτημα, το οποίο συμβάλλει στην κατανόηση της τεχνολογίας blockchain είναι η πορεία εξέλιξής της και οι διαφορετικές κατηγοριοποιήσεις των εφαρμογών της. Πιο συγκεκριμένα, μία κατηγοριοποίηση των εφαρμογών της τεχνολογία αλυσίδας συστοιχιών είναι ανάλογα με τον κλάδο που μπορούν να χρησιμοποιηθούν (Crosby et al., 2016, Monrat et al.,2019, Casino et al., 2019, Zheng et al., 2018, Baiod et al., 2021). Ειδικότερα, οι Crosby et al. (2016) κατηγοριοποιούν τις εφαρμογές της τεχνολογίας σε χρηματοοικονομικές και μη χρηματοοικονομικές. Οι Monrat et al. (2019) τονίζοντας ότι το bitcoin είναι η πιο δημοφιλής εφαρμογή του blockchain στα χρηματοοικονομικά, επισημαίνουν τη χρήση που μπορεί να έχει η τεχνολογία στον κλάδο της υγείας, της χρηματιστηριακής αγοράς, της ασφάλισης, της διακυβέρνησης, της βιομηχανίας ενέργειας και της διαχείρισης ταυτότητας. Άλλη πρόσφατη μελέτη των Casino et al. (2019) παρουσιάζει μια πιο ολοκληρωμένη και λεπτομερή ταξινόμηση των εφαρμογών που βασίζονται σε blockchain, λαμβάνοντας υπόψη την πραγματική και την επικείμενη ετερογένεια των λύσεων που προσφέρει το blockchain: χρηματοοικονομικά, επαλήθευση ακεραιότητας, διακυβέρνηση, internet of things, υγεία, εκπαίδευση, απόρρητο και ασφάλεια, επιχειρήσεις και βιομηχανία, διαχείριση δεδομένων. Κάθε μία από αυτές τις κατηγορίες περιλαμβάνει και υποκατηγορίες, όπως για παράδειγμα ο κλάδος της διακυβέρνησης περιλαμβάνει την ηλεκτρονική ψηφοφορία, τη δημόσια διοίκηση, τη διαχείριση ταυτότητας, τα μητρώα, τις συμβολαιογραφικές και νομικές δραστηριότητες.

Σύμφωνα με τον Lu (2018) το blockchain θα γίνει ένα από τα πιο δημοφιλή θέματα, προσελκύοντας με το πέρασμα του χρόνου όλο και περισσότερη προσοχή. Οι κορυφαίες βιομηχανίες που θα εφαρμόσουν την τεχνολογία και θα παρουσιάσουν καινοτόμες εφαρμογές είναι οι εξής: cloud υπηρεσίες, IoT, Fintech, υγειονομική περίθαλψη και το σύστημα της έξυπνης πόλης. Επιπλέον, οι Viriyasitavat και Hoonsopon (2019) παραθέτουν ένα ακόμη σημαντικό σημείο σχετικά με το blockchain, το οποίο είναι η ενσωμάτωσή του στα συστήματα διαχείρισης επιχειρηματικών διαδικασιών (Business Process Management System – BPS). Πιο

συγκεκριμένα, αναλύονται διάφοροι ορισμοί και επεξηγήσεις σχετικά με τα χαρακτηριστικά της τεχνολογίας αλυσίδας συστοιχιών αλλά και των επιχειρηματικών διαδικασιών και εισάγουν μία αρχιτεκτονική για τη λύση προβλημάτων που προκύπτουν, όπως η χρονική ασυνέπεια στην επιβεβαίωση συμφωνιών και η μεροληψία και αναξιοπιστία.

Μία άλλη προσέγγιση των κατηγοριών blockchain, η οποία παρουσιάζει ιδιαίτερο ενδιαφέρον, αφορά την εξέλιξη της τεχνολογίας και ειδικότερα τις τρεις φάσεις ανάπτυξης: blockchain 1.0, blockchain 2.0 και blockchain 3.0 (Swan, 2015, Zhang, Jacobsen, 2018, Casino et al., 2018, Lu, 2018, Lu, 2019, Demirkan et al., 2020, Li et al., 2020). Όπως ανέφερε η Swan το 2015 και στη συνέχεια άλλοι ερευνητές, η πρώτη φάση περιλαμβάνει τα κρυπτονομίσματα και την ανάπτυξή τους σε εφαρμογές που σχετίζονται με μετρητά, όπως μεταφορά νομισμάτων, εμβάσματα και συστήματα ψηφιακών πληρωμών. Το δεύτερο στάδιο αναφέρεται στα έξυπνα συμβόλαια και το σύνολο της οικονομίας, της αγοράς και των χρηματοοικονομικών εφαρμογών που χρησιμοποιούν το blockchain και είναι πιο εκτεταμένες από απλές συναλλαγές σε μετρητά. Τέλος, η τρίτη φάση περιλαμβάνει τις εφαρμογές blockchain πέρα από το νόμισμα, τη χρηματοδότηση και τις αγορές, ιδιαίτερα στους τομείς της κυβέρνησης, της υγείας, της επιστήμης, της πληροφορικής, του πολιτισμού και της τέχνης.

Οι Demirkan et al. (2020) αναφέρονται στο άρθρο τους στην τεχνολογία blockchain και στις εφαρμογές της στο επιχειρηματικό περιβάλλον, κυρίως αναφορικά με τη λογιστική και την κυβερνοασφάλεια. Ειδικότερα, επικεντρώνονται στην εξέλιξη της τεχνολογίας από το blockchain 1.0 στο blockchain 3.0, σε μία λεπτομερής ανάλυση της τεχνολογίας αλυσίδας συστοιχιών και της επίδρασης που μπορεί να έχει στη χρηματοοικονομική, στην ελεγκτική και στην κυβερνοασφάλεια. Επιπλέον, γίνεται αναφορά στη λογιστική και σε άλλες ανερχόμενες τεχνολογίες όπως τα Big Data και στην αποτροπή οικονομικών παραπτωμάτων. Επισημαίνεται πως οι τεχνολογίες της νέας γενιάς και ειδικότερα το blockchain θα έχει σημαντικό αντίκτυπο στον λογιστικό κλάδο. Αναλυτικότερα, το blockchain θα επηρεάσει όχι μόνο τη λογιστική μέσω των πλεονεκτημάτων που διαθέτει και των νέων εφαρμογών, αλλά και την ελεγκτική, τα Big Data και τη θέσπιση πολιτικών και κανόνων. Ωστόσο,

σημειώνεται ότι δεν είναι εφικτό να καθοριστεί από σήμερα η ακριβής πορεία της τεχνολογίας λόγω της φύσης και των τεράστιων δυνατοτήτων που διαθέτει.

Ο Khandelwal (2019) πραγματοποίησε μία SWOT ανάλυση ώστε να επισημάνει τις δυνάμεις, αδυναμίες, ευκαιρίες και απειλές του blockchain στη λογιστική. Επιπλέον, υποστήριξε ότι η τεχνολογία blockchain θα επιφέρει πολύ σημαντικές αλλαγές αλλά η χρηματοοικονομική αναφορά και ο έλεγχος των οικονομικών καταστάσεων δεν μπορεί να αντικατασταθεί πλήρως από αυτή.

Μία πολύ ενδιαφέρουσα προσέγγιση για τη λογιστική βασισμένη στο blockchain η οποία λαμβάνει υπόψη το χρονικό ορίζοντα της εφαρμογής της τεχνολογίας περιέγραψαν οι Yu et al. (2018). Ειδικότερα, η ανάλυση ξεκίνησε από την εισαγωγή της λογιστικής τον 13^{ο} αιώνα, τις παραδοσιακές μεθόδους της λογιστικής (Waymire, Basu, 2008, Faccia, Mosteanu, 2019), την ασύμμετρη πληροφόρηση μεταξύ εσωτερικών και εξωτερικών χρηστών των οικονομικών καταστάσεων, τη σημασία του ανεξάρτητου ελέγχου (Watts, Zimmerman, 1983) και στη συνέχεια επικεντρώθηκε στην μακροπρόθεσμη και βραχυπρόθεσμη εφαρμογή της τεχνολογίας blockchain στη λογιστική. Σημειώνεται ότι μακροπρόθεσμα τα πλεονεκτήματα που θα προσφέρει το blockchain είναι αξιοσημείωτα και θα φέρουν τεράστιες αλλαγές στο λογιστικό κλάδο. Μεταξύ αυτών περιλαμβάνονται η υψηλή διαφάνεια, η ιχνηλασιμότητα, η επικαιρότητα, η ασφάλεια, η μείωση του κόστους, η βελτίωση της αξιοπιστίας, της συγκρισιμότητας και της ακρίβειας μέσω της αυτοματοποίησης της δημιουργίας οικονομικών καταστάσεων με τα έξυπνα συμβόλαια και της γνωστοποίησης τους στην πλατφόρμα blockchain. Ωστόσο, βραχυπρόθεσμα κυρίως λόγω του μικρού βαθμού ωριμότητας της τεχνολογίας παρουσιάζονται ορισμένες δυσκολίες που πρέπει να αντιμετωπιστούν. Στη συνέχεια, η μελέτη ολοκληρώνεται αναφέροντας τρόπους αντιμετώπισης των δυσκολιών και τυχών απειλών που θα προκύψουν μετά την εφαρμογή της τεχνολογίας μακροπρόθεσμα.

Μία άλλη οπτική γωνία σχετικά με την εφαρμογή της τεχνολογίας blockchain στη λογιστική η οποία αξίζει να σημειωθεί είναι η τριπλή εγγραφή στη λογιστική (triple-entry-accounting). Σύμφωνα με τους Faccia και Mosteanu (2019), η λογιστική τριπλής εγγραφής προσθέτει ένα επίπεδο σαφήνειας και ειλικρίνειας στην τήρηση

βιβλίων συγκριτικά με τη λογιστική διπλής εγγραφής, καθώς εκτός από τα δύο καθολικά των εμπλεκόμενων μερών προστίθεται και ένα τρίτο δημόσιο καθολικό, το οποίο επιτρέπει και στα δύο εμπλεκόμενα μέρη να εναρμονίσουν τα λογιστικά τους βιβλία και να επιβεβαιωθεί ότι και οι τρεις εγγραφές βρίσκονται σε συναίνεση.

Εκτός από τη λογιστική, όπως έχει αναφερθεί και παραπάνω, το blockchain είναι μία από τις τεχνολογίες που μπορεί να έχει δραστικό ρόλο στην τέταρτη βιομηχανική επανάσταση (Sikorski et al., 2017, Xu et al., 2018). Οι Sikorski et al. (2017) στο άρθρο τους ερευνούν τις εφαρμογές της τεχνολογίας blockchain στην τέταρτη βιομηχανική επανάσταση και παραθέτουν ένα παράδειγμα που αφορά την αγορά ηλεκτρικής ενέργειας και την εφαρμογή του blockchain στον ευρύ κλάδο της χημικής βιομηχανίας. Ειδικότερα, το σημείο που αξίζει να σημειωθεί, εκτός από την αναλυτική περιγραφή της ορολογίας της τεχνολογίας blockchain, είναι η σημασία που μπορεί να έχει το blockchain στην εξέλιξη πολλών κλάδων λόγω του τρόπου λειτουργίας και των δυνατοτήτων του. Τέλος, σύμφωνα με τους Xu et al. (2018) η τέταρτη βιομηχανική επανάσταση περιλαμβάνει διάφορες μεθόδους και τεχνολογίες προκειμένου να γίνει πραγματικότητα. Ειδικότερα αναφέρονται τα CPS (Cyber-Physical Systems), IoT, Cloud Computing, Industrial Integration, Enterprise Architecture, SOA, Business Process Management αλλά και το blockchain για το οποίο επισημαίνεται το αυξανόμενο ενδιαφέρον από ερευνητές, επιχειρήσεις για τη σημασία του στο βιομηχανικό και μεταποιητικό κλάδο.

ΚΕΦΑΛΑΙΟ 3: ΑΝΑΛΥΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN

3.1. Εισαγωγή

Η τεχνολογία blockchain ή τεχνολογία αλυσίδας συστοιχιών αναπτύχθηκε το 2009 όταν το κρυπτονόμισμα Bitcoin παρουσιάστηκε από ένα ανώνυμο άτομο ή ομάδα ατόμων με το ψευδώνυμο Satoshi Nakamoto. Το Bitcoin είναι ένα ψηφιακό νόμισμα του οποίου η εξόρυξη γίνεται από χρήστες υπολογιστών ανά τον κόσμο χρησιμοποιώντας λογισμικό για να λύσουν μαθηματικά προβλήματα (Nordgren et al., 2019).

Από το 2008 που προτάθηκε και το 2009 που εφαρμόστηκε η τεχνολογία blockchain μέσω του πρώτου κρυπτονομίσματος αξίζει να αναφερθεί η τεράστια ανάπτυξη του Bitcoin. Το Bitcoin ως το πρώτο κρυπτονόμισμα αξιολογήθηκε ως το νόμισμα με την καλύτερη απόδοση το 2015 και το εμπόρευμα με τις καλύτερες επιδόσεις το 2016. Το 2016 υπήρξε αξιοσημείωτη ανάπτυξη της κεφαλαιακής αγοράς φτάνοντας τα 10 δισεκατομμύρια δολάρια και το Φεβρουάριο του 2021 η κεφαλαιοποίηση της αγοράς ξεπέρασε το 1 τρισεκατομμύριο (Li et al., 2020).

Όπως αναφέρουν οι Nordgren et al. (2019) η τεχνολογία blockchain αποτελεί την τεχνολογία που βρίσκεται πίσω από το Bitcoin και δεν ταυτίζεται με αυτό. Παρά το γεγονός ότι έχουν αναπτυχθεί πολλές καινοτομίες οι οποίες έχουν κάνει τις συναλλαγές πιο γρήγορες, αποτελεσματικές και αξιόπιστες, πολλές επιχειρηματικές συναλλαγές παραμένουν αναποτελεσματικές, ευάλωτες και με μεγάλο κόστος. Η τεχνολογία αλυσίδας συστοιχιών υπόσχεται να λύσει τα παραπάνω προβλήματα που συνεχίζουν να υπάρχουν καθώς θα εμποδίσει τις απάτες, θα αυξήσει την εμπιστοσύνη, τη διαφάνεια και θα εξοικονομήσει χρόνο και χρήματα εξαλείφοντας τους διαμεσολαβητές στις συναλλαγές.

Ειδικότερα, το blockchain υπόσχεται να είναι η πιο καινοτόμα τεχνολογία, η οποία θα έχει τεράστια επίδραση παρόμοια με αυτή που είχε η εμφάνιση του

Διαδικτύου και του πρωτοκόλλου TCP/IP. Βασίζεται στην κατανεμημένη ψηφιακή εφαρμογή των καθολικών (λογιστικών βιβλίων) συναλλαγών και μερικές φορές αναφέρεται ως τεχνολογία κατανεμημένου καθολικού (Distributed Ledger Technology - DLT) (Baidyanath, Rohit, 2019).

Στις επόμενες ενότητες αυτού του κεφαλαίου αναλύονται οι ορισμοί που έχουν δοθεί για το blockchain και επεξηγούνται βασικοί όροι απαραίτητοι για την κατανόηση της τεχνολογίας, όπως κόμβος (node), δίκτυο peer-to-peer (P2P), συναλλαγή (transaction), block, διπλή δαπάνη (double spending), miners και mining, μηχανισμός συναίνεσης (consensus mechanism), κρυπτογραφικές συναρτήσεις κατακερματισμού (cryptographic hash functions) και ασύμμετρη κρυπτογραφία (asymmetric cryptography). Στη συνέχεια, ακολουθεί μία περιγραφή της αρχιτεκτονικής των blocks, των χαρακτηριστικών, πλεονεκτημάτων και αδυναμιών της τεχνολογίας αλυσίδας συστοιχιών. Τέλος, πραγματοποιείται κατηγοριοποίηση των δικτύων blockchain σε δημόσια (public ή permissionless), ιδιωτικά (private) και υβριδικά (federated ή consortium), επισημαίνοντας τα χαρακτηριστικά κάθε κατηγορίας.

3.2. Ορισμός

Η τεχνολογία blockchain είναι μία αλυσίδα από συστοιχίες (blocks) στις οποίες αποθηκεύονται όλες οι πραγματοποιούμενες συναλλαγές χρησιμοποιώντας ένα δημόσιο καθολικό. Το blockchain λειτουργεί σε ένα αποκεντρωμένο περιβάλλον το οποίο δημιουργείται με τον συνδυασμό πολλών βασικών τεχνολογιών, όπως ψηφιακές υπογραφές, κρυπτογραφικό κατακερματισμό και κατανεμημένους αλγόριθμους συναίνεσης (Zheng et al., 2018, Monrat et al., 2019). Όλες οι συναλλαγές πραγματοποιούνται με αποκεντρωμένο τρόπο που εξαλείφει την απαίτηση οποιουδήποτε διαμεσολαβητή να επικυρώνει και να επαληθεύει τις συναλλαγές.

Τα διοικητικά στελέχη αλλά και οι ακαδημαϊκοί θεωρούν την τεχνολογία blockchain από τις πιο σημαντικές τεχνολογικές καινοτομίες που θα υποστηρίξουν την ψηφιοποίηση της ιδιοκτησίας περιουσιακών στοιχείων. Χρηματοοικονομικά μέσα, όπως πληρωμές, αρχεία συναλλαγών και έξυπνα συμβόλαια μπορούν να βασιστούν στην τεχνολογία blockchain, η οποία θα αποτρέψει δυσμενείς συμπεριφορές και τις συναφείς επιπτώσεις τους, όπως το πρόβλημα της διπλής δαπάνης (double spending) και τις πλαστογραφίες. Το blockchain είναι μια ευέλικτη πλατφόρμα που μπορεί να προγραμματιστεί για τη διαχείριση συμβάσεων, την ιδιοκτησία προϊόντων και παρέχει μια κατανεμημένη και δίχως παραβιάσεις ελέγχου διαδρομή για εφαρμογές σε πραγματικό χρόνο (Baidyanath, Rohit, 2019).

Η τεχνολογία blockchain είναι μία κατανεμημένη βάση δεδομένων η οποία περιέχει πληροφορίες σχετικά με όλες τις δράσεις που πραγματοποιούνται από τους συμμετέχοντες του συστήματος. Οι πληροφορίες αποθηκεύονται με τη μορφή των συστοιχιών (blocks), σε καθένα από τα οποία ένας συγκεκριμένος αριθμός συναλλαγών είναι αποθηκευμένος. Η τεχνολογία αυτή είναι βασισμένη στα κατανεμημένα μητρώα δεδομένων. Αυτό σημαίνει ότι δεν υπάρχει ένα μόνο μέρος όπου είναι αποθηκευμένα αυτά τα καθολικά ή ένα φυσικό πρόσωπο που τα διατηρεί. Τα καθολικά αυτά κρατούνται ταυτόχρονα από όλους τους συμμετέχοντες του συστήματος, ενημερώνονται αυτόματα στην τελευταία έκδοση κατόπιν των αλλαγών που πραγματοποιούνται και οι συμμετέχοντες του συστήματος έχουν τη δυνατότητα να εγγυηθούν την αξιοπιστία της πληροφόρησης αυτής. Σημειώνεται ότι μετά την καταγραφή των πληροφοριών δεν μπορεί να διαγραφούν ή να καταστραφούν τα αρχεία (Melnychenko, Hartinger, 2017).

Σύμφωνα με τους Viriyasitavat και Hoonsopon (2019), στις περισσότερες τρέχουσες έρευνες, ο τρόπος με τον οποίο ορίζεται το blockchain είναι άτυπος, καθώς περιγράφεται κυρίως το πλαίσιο χρήσης του και χρησιμοποιούνται ορισμένες λέξεις μάρκετινγκ όσον αφορά τις ιδιότητες που προσφέρει το blockchain ή πώς μπορεί να επιτευχθεί η ασφάλεια. Οι ορισμοί περιλαμβάνουν για παράδειγμα τα εξής:

- ένα δημόσιο καθολικό για καταγραφή συναλλαγών που διατηρούνται από πολλούς κόμβους χωρίς κεντρική εξουσία μέσω ενός κατανεμημένου κρυπτογραφικού πρωτοκόλλου.
- μια αποκεντρωμένη βάση δεδομένων με δυνατότητα λειτουργίας σε αποκεντρωμένο περιβάλλον χωρίς να βασίζεται σε έμπιστους μεσάζοντες.
- ένα αποκεντρωμένο, αναπαραγόμενο, αμετάβλητο και προφανές αρχείο καταγραφής, που επιτρέπει σε οποιονδήποτε να διαβάζει δεδομένα και να επαληθεύει την ορθότητα αυτών.
- ένας τύπος κατανεμημένου καθολικού (δομή δεδομένων) που περιέχει πληροφορίες για συναλλαγές ή γεγονότα, που επαναλαμβάνονται και μοιράζονται μεταξύ των συμμετεχόντων στο δίκτυο.

Παρατηρείται ότι οι περισσότεροι από τους ανωτέρω ορισμούς περιλαμβάνουν τους όρους αμετάβλητο, δυνατότητα ελέγχου, διαφάνεια, κατανεμημένη βάση δεδομένων ή καθολικό και απουσία αξιόπιστου μεσάζοντα.

Το λεξικό της Οξφόρδης ορίζει το blockchain ως «Ένα σύστημα στο οποίο μια εγγραφή των συναλλαγών που γίνονται σε bitcoin ή άλλο κρυπτονόμισμα διατηρούνται σε πολλούς υπολογιστές που είναι συνδεδεμένοι σε ένα δίκτυο peer-to-peer». Ωστόσο, το πεδίο εφαρμογής είναι περιορισμένο στα κρυπτονομίσματα ενώ η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί περαιτέρω σε ένα ευρύ φάσμα εφαρμογών. Σύμφωνα με τους Viriyasitavat και Hoonsopon (2019), η τεχνολογία blockchain ορίζεται ως μια τεχνολογία που επιτρέπει την αμεταβλητότητα και την ακεραιότητα των δεδομένων στα οποία τηρείται αρχείο των συναλλαγών που έγιναν σε ένα σύστημα σε πολλούς κατανεμημένους κόμβους που είναι συνδεδεμένοι σε ένα δίκτυο peer-to-peer.

Ο παραπάνω ορισμός παρουσιάζει ορισμένες ιδιότητες της τεχνολογίας. Ειδικότερα, η διαφάνεια μπορεί να βελτιωθεί ανάλογα με τον βαθμό των πληροφοριών που αποκαλύπτονται στο κοινό εκτός συστήματος, γεγονός που επιτρέπει στο σύστημα να είναι ελεγχόμενο. Η ανθεκτικότητα είναι μία άλλη ιδιότητα που προκύπτει από τη δυνατότητα διαμοιρασμού. Ο βαθμός ανθεκτικότητας εξαρτάται από τον αριθμό των συμμετεχόντων κόμβων. Η ορθότητα του συστήματος

βασίζεται σε μεγάλο βαθμό στην υπόθεση ότι η πλειοψηφία των κόμβων είναι έμπιστοι. Λαμβάνοντας υπόψη ότι τα δεδομένα μπορούν να είναι αξιόπιστα, δεν απαιτούνται κεντρικές αρχές ως διαμεσολαβητές. Επιπλέον, η επιτυχία του blockchain βασίζεται και στις επιμέρους λειτουργίες που συνδυάζει όπως τον κρυπτογραφικό κατακερματισμό (cryptographic hash), την ασύμμετρη κρυπτογραφία (asymmetric cryptography) και τους μηχανισμούς συναίνεσης που καθορίζουν την απόδοση και την επεκτασιμότητα του συστήματος όπως θα αναλυθεί και σε επόμενη ενότητα.

Σύμφωνα με την IBM (2018) η τεχνολογία blockchain είναι ένα διαμοιραζόμενο, αμετάβλητο καθολικό το οποίο διευκολύνει τη διαδικασία της καταγραφής των συναλλαγών και της παρακολούθησης των περιουσιακών στοιχείων σε ένα επιχειρηματικό δίκτυο. Ένα περιουσιακό στοιχείο μπορεί να είναι ενσώματο (ένα σπίτι, ένα αυτοκίνητο, μετρητά ή γεωγραφική έκταση) ή άυλο (πνευματική ιδιοκτησία, ευρεσιτεχνία, πνευματικά δικαιώματα, επωνυμία προϊόντος). Οποιοδήποτε περιουσιακό στοιχείο το οποίο έχει αξία μπορεί να καταγραφεί και να γίνει αντικείμενο συναλλαγής σε ένα δίκτυο blockchain, μειώνοντας τον κίνδυνο και το κόστος για όλους τους εμπλεκόμενους. Συνεπώς, η τεχνολογία αλυσίδας συστοιχιών αποτελεί έναν ασφαλή για όλους τους εμπλεκόμενους τρόπο για την καταγραφή και αποθήκευση πληροφοριών.

Είναι σημαντικό να σημειωθεί ότι παρά το γεγονός ότι η τεχνολογία αλυσίδας συστοιχιών αποκαλείται τεχνολογία κατανεμημένου καθολικού (DLT – Distributed Ledger Technology) και αναλύονται οι πιθανές εφαρμογές στα χρηματοοικονομική και στη λογιστική, δεν αποτελεί αυτοτελώς ένα χρηματοοικονομικό εργαλείο. Ειδικότερα, το blockchain δεν είναι μία πλατφόρμα λογιστικής, ένα ημερολόγιο ή ένα λογισμικό λογιστικής. Η τεχνολογία αλυσίδας συστοιχιών βασίζεται στην παραδοσιακή ιδέα του διπλογραφικού συστήματος προσθέτοντας μία «τριπλή καταγραφή» η οποία περιλαμβάνει και τις δύο πλευρές της συναλλαγής επικυρωμένες στην ίδια συστοιχία (block). Με βάση την παραδοσιακή μέθοδο, τα δύο εμπλεκόμενα μέρη που συμμετέχουν σε μία συναλλαγή διατηρούν το δικό τους αρχείο των γεγονότων, τα δικά τους καθολικά. Με αυτό τον τρόπο επιτρέπεται το περιθώριο λάθους καθώς υπάρχει το ενδεχόμενο οι καταγραφές των εμπλεκόμενων

να μην συμφωνούν και επομένως κρίνεται σημαντική η επιβεβαίωση από ένα τρίτο μέλος με τη μορφή του ελέγχου. Με τη χρήση της τεχνολογίας blockchain η συναλλαγή επικυρώνεται αρχικά από τα δύο μέρη και έπειτα καταγράφεται στο κατανεμημένο καθολικό. Με αυτόν τον τρόπο όλοι έχουν τις σωστές πληροφορίες σε πραγματικό χρόνο γεγονός που έχει ως αποτέλεσμα την εξοικονόμηση χρόνου, την εξάλειψη λαθών και την ανάγκη να «διασταυρωθούν» οι λογαριασμοί μεταξύ των μελών στο τέλος της οικονομικής χρήσης (Nordgren et al., 2019).

3.3. Επεξήγηση της Ορολογίας και των Βασικών Αρχών της Τεχνολογίας Blockchain

Προκειμένου να γίνουν κατανοητά τα χαρακτηριστικά και οι αρχές που διέπουν την τεχνολογία blockchain, τα οποία περιγράφονται στην επόμενη ενότητα ακολουθεί η βασική ορολογία που χρησιμοποιείται αναφορικά με την τεχνολογία αλυσίδας συστοιχιών.

Κόμβος (Node)

Κόμβος ορίζεται ως μία οποιαδήποτε συσκευή που είναι μέρος ενός δικτύου και έχει μια μοναδική διεύθυνση δικτύου (Sikorski et al., 2017). Ένας κόμβος ξεκινά μια συναλλαγή σε ένα αποκεντρωμένο δίκτυο blockchain μέσω μιας ψηφιακής υπογραφής η οποία χρησιμοποιεί κρυπτογραφία ιδιωτικού κλειδιού (private key cryptography) (Monrat et al., 2019).

Δίκτυο peer-to-peer (P2P)

Το δίκτυο peer-to-peer είναι ένα δίκτυο κόμβων (peer) που συνδέονται άμεσα μεταξύ τους. Το σύστημα βασίζεται στους ομότιμους χρήστες (peers), οι οποίοι έχουν ίση θέση εντός του δικτύου και μοιράζονται τουλάχιστον όσους πόρους καταναλώνουν (Sikorski et al., 2017).

Συναλλαγή (Transaction) και Block

Μια συναλλαγή με blockchain (blockchain transaction) μπορεί να οριστεί ως ένα μικρό τμήμα μιας εργασίας που αποθηκεύεται σε δημόσια αρχεία. Αυτές οι εγγραφές είναι επίσης γνωστές ως τμήματα ή συστοιχίες ή blocks. Οι συστοιχίες αυτές εκτελούνται, υλοποιούνται και αποθηκεύονται στην αλυσίδα blockchain για επικύρωση από όλους τους miners που συμμετέχουν στο δίκτυο. (Monrat et al., 2019). Με άλλα λόγια μία συναλλαγή ορίζεται ως μία μεταφορά ενός ψηφιακού στοιχείου από μια διεύθυνση ή διευθύνσεις σε άλλη διεύθυνση ή διευθύνσεις (Sikorski et al., 2017). Ειδικότερα μπορεί να θεωρηθεί ως μια δομή δεδομένων που αντιπροσωπεύει τη μεταφορά ψηφιακών περιουσιακών στοιχείων μεταξύ ομότιμων χρηστών (peers) στο δίκτυο blockchain.

Σε αυτό το σημείο σημειώνεται ότι όλες οι συναλλαγές αποθηκεύονται σε μια ομάδα μη επιβεβαιωμένων συναλλαγών και διαδίδονται στο δίκτυο χρησιμοποιώντας ένα πρωτόκολλο flooding γνωστό ως πρωτόκολλο Gossip (Gossip Protocol). Στη συνέχεια, οι ομότιμοι χρήστες (peers) πρέπει να επιλέξουν και να επικυρώσουν αυτές τις συναλλαγές με βάση ορισμένα προκαθορισμένα κριτήρια. Για παράδειγμα, οι κόμβοι προσπαθούν να επαληθεύσουν και να επικυρώσουν αυτές τις συναλλαγές ελέγχοντας εάν το πρόσωπο που ξεκίνησε την συναλλαγή έχει αρκετό υπόλοιπο για να την ενεργοποιήσει ή προσπαθεί να εξαπατήσει το σύστημα κάνοντας «διπλή δαπάνη» (double spending). Μόλις η συναλλαγή επαληθευτεί και επικυρωθεί από τους miners, περιλαμβάνεται σε ένα τμήμα της αλυσίδας (block) (Monrat et al., 2019).

Διπλή δαπάνη (double spending)

Η «διπλή δαπάνη» αναφέρεται στη χρήση του ίδιου ποσού εισροών για δύο ή περισσότερες διαφορετικές συναλλαγές (Monrat et al., 2019).

Miners and Mining

Εξόρυξη ή mining θεωρείται η διαδικασία επαλήθευσης συναλλαγών και δημοσίευσης block. Η ακριβής διαδικασία ποικίλλει ευρέως ανάλογα με την κάθε εφαρμογή blockchain (Sikorski et al., 2017). Οι χρήστες του δικτύου που χρησιμοποιούν την υπολογιστική τους ισχύ για την εξόρυξη block ονομάζονται miners. Οι κόμβοι εξόρυξης (miner nodes) πρέπει να λύσουν ένα υπολογιστικό παζλ

και να ξοδέψουν αρκετούς από τους υπολογιστικούς πόρους τους για να δημοσιεύσουν ένα block. Ο miner που μπορεί να λύσει πρώτος το παζλ θα γίνει νικητής και θα αποκτήσει την ευκαιρία να δημιουργήσει ένα νέο block. Ένα μικρό ποσό κινήτρου δίνεται μετά την επιτυχή δημιουργία ενός νέου block (Monrat et al., 2019).

Μηχανισμός συναίνεσης (consensus mechanism)

Οι χρήστες του δικτύου επαληθεύουν το νέο block χρησιμοποιώντας ένα μηχανισμό συναίνεσης (consensus mechanism), ο οποίος είναι μια τεχνική που βοηθά ένα αποκεντρωμένο δίκτυο να καταλήξει σε συμφωνία για ορισμένα θέματα. Μετά από αυτό, το νέο block θα προστεθεί στην υπάρχουσα αλυσίδα και στο τοπικό αντίγραφο του αμετάβλητου καθολικού κάθε χρήστη. Σε αυτό το σημείο, η συναλλαγή επιβεβαιώνεται.

Αναλυτικότερα, στο blockchain η επίτευξη της συναίνεσης μεταξύ των μη αξιόπιστων κόμβων του δικτύου είναι μια μετατροπή του Προβλήματος των Βυζαντινών Στρατηγών (Byzantine Generals Problem- BG). Ειδικότερα, το πρόβλημα των BG αφορά μια ομάδα στρατηγών, οι οποίοι διοικούν μια μερίδα βυζαντινού στρατού και έχουν κυκλώσει μία πόλη. Η επίθεση θα αποτύγχανε εάν μόνο μέρος των στρατηγών επιτεθεί στην πόλη. Συνεπώς, οι στρατηγοί πρέπει να επικοινωνήσουν για να καταλήξουν σε συμφωνία για το αν θα επιτεθούν ή όχι. Ωστόσο, μπορεί να υπάρχουν προδότες μέσα στους στρατηγούς. Ο προδότης μπορούσε να στείλει διαφορετικές αποφάσεις σε διαφορετικούς στρατηγούς. Αυτό είναι ένα περιβάλλον χωρίς εμπιστοσύνη (trustless environment). Η επίτευξη της συναίνεσης σε ένα τέτοιο περιβάλλον είναι μια πρόκληση, όπως επίσης πρόκληση αποτελεί και για το blockchain, καθώς το δίκτυό του είναι κατανεμημένο. Αναλυτικότερα, στο blockchain δεν υπάρχει κεντρικός κόμβος που να διασφαλίζει ότι τα καθολικά στους κατανεμημένους κόμβους είναι όλα ίδια και συγχρόνως σημειώνεται ότι οι κόμβοι δεν χρειάζεται να εμπιστεύονται άλλους κόμβους. Επομένως, χρειάζονται ορισμένα πρωτόκολλα για να διασφαλιστεί ότι τα καθολικά σε διαφορετικούς κόμβους είναι συνεπή (Zheng et al., 2018, Monrat et al., 2019).

Σύμφωνα με τους Zheng et al. (2018) και τους Monrat et al. (2019) ορισμένες κοινές προσεγγίσεις για την επίτευξη συναίνεσης στο blockchain είναι οι εξής:

1. Proof of Work (PoW)
2. Proof of Stake (PoS)
3. Proof of Activity
4. Delegated Proof of Stake (DPoS)
5. Practical Byzantine Fault Tolerance (PBFT)
6. Tendermint

Στα υπάρχοντα συστήματα blockchain, υπάρχουν τέσσερις κύριοι μηχανισμοί συναίνεσης: Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT) και Delegated Proof of Stake (DPoS). Τα δύο πιο δημοφιλή συστήματα blockchain, δηλαδή το Bitcoin και το Ethereum χρησιμοποιούν τον μηχανισμό PoW. Το Ethereum ενσωματώνει επίσης τον μηχανισμό PoA (Li et al., 2020).

Proof-of-work (PoW)

Ο μηχανισμός PoW χρησιμοποιεί τη λύση παζλ για να αποδείξει την αξιοπιστία των δεδομένων. Το παζλ είναι συνήθως ένα υπολογιστικά δύσκολο αλλά εύκολα επαληθεύσιμο πρόβλημα. Όταν ένας κόμβος δημιουργεί ένα block, πρέπει να επιλύσει ένα παζλ PoW. Αφού επιλυθεί το παζλ PoW, θα μεταδοθεί σε άλλους κόμβους, έτσι ώστε να επιτευχθεί ο σκοπός της συναίνεσης (Li et al., 2020).

Αναλυτικότερα, σημειώνεται ότι ο μηχανισμός συναίνεσης PoW είναι μια στρατηγική συναίνεσης που χρησιμοποιείται στο δίκτυο Bitcoin (Nakamoto, 2008, Zheng et al., 2018). Ο μηχανισμός αυτός απαιτεί μια περίπλοκη υπολογιστική διαδικασία κατά τον έλεγχο γνησιότητας. Κάθε κόμβος του δικτύου υπολογίζει μια τιμή κατακερματισμού (hash value) της συνεχώς μεταβαλλόμενης κεφαλής του block. Η συναίνεση απαιτεί η υπολογιζόμενη τιμή να είναι ίση ή μικρότερη από μια ορισμένη δεδομένη τιμή. Στο αποκεντρωμένο δίκτυο, όλοι οι συμμετέχοντες πρέπει να υπολογίζουν την τιμή κατακερματισμού συνεχώς χρησιμοποιώντας διαφορετικούς τυχαίους αριθμούς (nonces) μέχρι να επιτευχθεί ο στόχος. Όταν ένας

κόμβος αποκτά τη σχετική τιμή, όλοι οι άλλοι κόμβοι πρέπει να επιβεβαιώνουν αμοιβαία την ορθότητα της τιμής.

Μετά από αυτό, οι συναλλαγές στο νέο block θα επικυρώνονται για περιπτώσεις απάτης. Στη συνέχεια, η συλλογή των συναλλαγών που χρησιμοποιούνται για τους υπολογισμούς εγκρίνεται ως το επαληθευμένο αποτέλεσμα, το οποίο υποδηλώνεται με ένα νέο block στο blockchain. Οι κόμβοι που υπολογίζουν τους κατακερματισμούς ονομάζονται miners και η διαδικασία PoW ονομάζεται εξόρυξη (Zheng et al., 2018). Δεδομένου ότι ο υπολογισμός της επαλήθευσης της γνησιότητας είναι μια χρονοβόρα διαδικασία, προτείνεται επίσης ένας μηχανισμός κινήτρων (π.χ. η χορήγηση ενός μικρού τμήματος Bitcoin στον miner) (Nakamoto, 2008).

Στο αποκεντρωμένο δίκτυο, έγκυρα block μπορεί να δημιουργηθούν ταυτόχρονα όταν πολλοί κόμβοι βρίσκουν τον κατάλληλο τυχαίο αριθμό (nonce) σχεδόν ταυτόχρονα. Ως αποτέλεσμα, μπορεί να δημιουργηθούν «διακλαδώσεις» (forks). Ωστόσο, είναι απίθανο δύο ανταγωνιστικές «διακλαδώσεις» να δημιουργήσουν το επόμενο block ταυτόχρονα. Στο πρωτόκολλο PoW, μια αλυσίδα που γίνεται μεγαλύτερη στη συνέχεια κρίνεται ως αυθεντική (Zheng et al., 2018).

Proof of Stake (PoS)

Ο μηχανισμός συναίνεσης Proof of Stake (PoS) χρησιμοποιεί την απόδειξη ιδιοκτησίας κρυπτονομισμάτων για να αποδείξει την αξιοπιστία των δεδομένων. Στο blockchain που βασίζεται στο PoS, κατά τη διαδικασία δημιουργίας block ή συναλλαγής, οι χρήστες υποχρεούνται να πληρώσουν ένα ορισμένο ποσό κρυπτονομίσματος. Εάν το block ή η συναλλαγή που δημιουργήθηκε μπορεί τελικά να επικυρωθεί, το κρυπτονόμισμα θα επιστραφεί στον αρχικό κόμβο ως μπόνους. Σε αντίθετη περίπτωση, θα επιβληθεί πρόστιμο.

Το PoS είναι μια εναλλακτική λύση αντί για το PoW με την οποία εξοικονομείται ενέργεια. Ειδικότερα, αντί να απαιτεί από τους χρήστες να βρουν ένα τυχαίο αριθμό (nonce), το PoS απαιτεί από τους χρήστες να αποδείξουν την κυριότητα του ποσού του νομίσματος. Αυτό συμβαίνει επειδή πιστεύεται ότι τα άτομα με περισσότερα νομίσματα είναι λιγότερο πιθανό να επιτεθούν στο δίκτυο.

Ωστόσο, η επιλογή βάσει του υπολοίπου του λογαριασμού θεωρείται άδικη, καθώς το πιο πλούσιο άτομο είναι βέβαιο ότι θα κυριαρχεί στο δίκτυο.

Σε σύγκριση με το PoW, το PoS εξοικονομεί περισσότερη ενέργεια και είναι πιο αποτελεσματικό. Δυστυχώς, καθώς το κόστος εξόρυξης είναι σχεδόν μηδενικό, ως συνέπεια μπορεί να προκύψουν επιθέσεις. Πολλά blockchains υιοθετούν το PoW στην αρχή και μετατρέπονται σε PoS σταδιακά. Για παράδειγμα, το Ethereum σχεδιάζει να μετακινηθεί από το Ethash (ένα είδος PoW) (Wood, 2014) στο Casper (ένα είδος PoS) (Zamfir, 2015).

Proof of Activity (PoA)

Προκειμένου να συνδυαστούν τα οφέλη του PoW και του PoS, προτείνεται το Proof of Activity (Bentov et al., 2014). Με τον μηχανισμό αυτόν, ένα block για το οποίο έχει πραγματοποιηθεί ήδη η διαδικασία της εξόρυξης, πρέπει να υπογραφεί από ορισμένους miners για να είναι έγκυρο. Με αυτόν τον τρόπο, εάν υπάρχει κάποιος κάτοχος του 50% όλων των νομισμάτων, δεν μπορεί να ελέγξει μόνος του τη δημιουργία νέων blocks (Zheng et al., 2018).

Όπως έχει ήδη αναφερθεί και στον ορισμό της τεχνολογίας blockchain, θεωρείται μία περίπλοκη τεχνολογία η οποία συνδυάζει πολλές βασικές τεχνολογίες. Ειδικότερα, αναλύοντας την τεχνολογία blockchain γίνεται εμφανές ότι χρησιμοποιεί μηχανισμούς της επιστήμης υπολογιστών, κρυπτογραφικές μεθόδους και έννοιες σχετικές με την καταγραφή αρχείων. Τα κύρια στοιχεία της τεχνολογίας αλυσίδας συστοιχιών είναι οι κρυπτογραφικές συναρτήσεις κατακερματισμού, η κρυπτογραφία ασύμμετρου κλειδιού, οι συναλλαγές, οι διευθύνσεις, τα καθολικά, τα blocks και η σύνδεση μεταξύ τους. Ακολουθεί μία περιγραφή των δύο πρώτων στοιχείων της τεχνολογίας ώστε να γίνει κατανοητή η λειτουργία της.

Κρυπτογραφικές Συναρτήσεις Κατακερματισμού (cryptographic hash functions)

Ένα σημαντικό στοιχείο της τεχνολογίας blockchain είναι η χρήση κρυπτογραφικών συναρτήσεων κατακερματισμού για διάφορες λειτουργίες. Ο κατακερματισμός (hashing) είναι μια μέθοδος εφαρμογής μιας κρυπτογραφικής συνάρτησης κατακερματισμού σε δεδομένα, η οποία υπολογίζει μια σχετικά

μοναδική «έξοδο» για μια «είσοδο» σχεδόν οποιουδήποτε μεγέθους (π.χ. αρχείο, κείμενο ή εικόνα). Με αυτό τον τρόπο, δίνεται η δυνατότητα έχοντας ορισμένα δεδομένα εισόδου τα οποία κατακερματίζονται χρησιμοποιώντας μία συνάρτηση κατακερματισμού να εξάγουν το ίδιο αποτέλεσμα. Οποιαδήποτε αλλαγή στην είσοδο (π.χ. αλλαγή ενός bit) θα έχει ως αποτέλεσμα μια εντελώς διαφορετική ανάλυση εξόδου.

Μια συγκεκριμένη συνάρτηση κατακερματισμού κρυπτογράφησης που χρησιμοποιείται σε πολλές λειτουργίες της τεχνολογίας blockchain είναι ο Security Hashing Algorithm (SHA) με μέγεθος εξόδου 256 bit (SHA-256). Το SHA-256 έχει έξοδο 32 byte (1 byte = 8 bit, 32 byte = 256 bit), που εμφανίζεται γενικά ως δεκαεξαδική συμβολοσειρά 64 χαρακτήρων (Yaga et al., 2019).

Σύμφωνα με τους Yaga et al. (2019) σε ένα δίκτυο blockchain οι κρυπτογραφικές συναρτήσεις κατακερματισμού έχουν διάφορες χρήσεις, ορισμένες από τις οποίες είναι οι εξής:

- Εξαγωγή μίας διεύθυνσης

  Ορισμένα δίκτυα blockchain χρησιμοποιούν μια διεύθυνση, η οποία είναι μια σύντομη, αλφαριθμητική σειρά χαρακτήρων που προέρχεται από το δημόσιο κλειδί του χρήστη του δικτύου blockchain χρησιμοποιώντας μια κρυπτογραφική συνάρτηση κατακερματισμού μαζί με ορισμένα πρόσθετα δεδομένα. Ένας τρόπος να δημιουργηθεί αυτή η διεύθυνση είναι να δημιουργηθεί ένα δημόσιο κλειδί, να εφαρμοστεί μία κρυπτογραφική συνάρτηση κατακερματισμού σε αυτό και να μετατραπεί σε κείμενο.
- Δημιουργία μοναδικών αναγνωριστικών
- Προστασία των δεδομένων που περιλαμβάνονται σε ένα block

  Ειδικότερα, ο κόμβος που συμβάλλει στη δημοσίευση ενός block θα χρησιμοποιήσει μία συνάρτηση κατακερματισμού στα δεδομένα του block και θα αποθηκευτούν στην κεφαλή του block.
- Προστασία της κεφαλής του block

Ένας κόμβος που συμβάλλει στη δημοσίευση ενός block θα κατακερματίσει την κεφαλή του block. Σε περίπτωση που το δίκτυο blockchain χρησιμοποιεί ως

μηχανισμό συναίνεσης το Proof of Work, ο κόμβος αυτός πρέπει να δοκιμάσει διαφορετικές τιμές nonce μέχρι να εκπληρωθούν οι απαιτήσεις του μαθηματικού προβλήματος και να κατακερματιστεί η κεφαλή του block. Η τιμή κατακερματισμού της κεφαλής του block συμπεριλαμβάνεται στην κεφαλή του επόμενου block, ώστε να διασφαλιστεί η αξιοπιστία και η αυθεντικότητα των δεδομένων και του blockchain.

Ασύμμετρη Κρυπτογραφία (asymmetric cryptography).

Η τεχνολογία blockchain χρησιμοποιεί κρυπτογραφία ασύμμετρου κλειδιού (αναφέρεται επίσης ως κρυπτογραφία δημόσιου κλειδιού). Η κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιεί ένα ζεύγος κλειδιών: ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί που σχετίζονται μαθηματικά μεταξύ τους. Το δημόσιο κλειδί δημοσιοποιείται χωρίς να μειώνεται η ασφάλεια της διαδικασίας, αλλά το ιδιωτικό κλειδί πρέπει να παραμείνει μυστικό εάν τα δεδομένα πρόκειται να διατηρήσουν την κρυπτογραφική τους προστασία. Παρόλο που υπάρχει σχέση μεταξύ των δύο κλειδιών, το ιδιωτικό κλειδί δεν μπορεί να προσδιοριστεί αποτελεσματικά με βάση τη γνώση του δημόσιου κλειδιού. Κάποιος μπορεί να κρυπτογραφήσει με ένα ιδιωτικό κλειδί και στη συνέχεια να αποκρυπτογραφήσει με το δημόσιο κλειδί. Εναλλακτικά, μπορεί κανείς να κρυπτογραφήσει με ένα δημόσιο κλειδί και στη συνέχεια να αποκρυπτογραφήσει με ένα ιδιωτικό κλειδί.

Η κρυπτογραφία ασύμμετρου κλειδιού επιτρέπει μια σχέση εμπιστοσύνης μεταξύ χρηστών που δεν γνωρίζουν ή δεν εμπιστεύονται ο ένας τον άλλον, παρέχοντας έναν μηχανισμό για την επαλήθευση της ακεραιότητας και της αυθεντικότητας των συναλλαγών, ενώ ταυτόχρονα επιτρέπει στις συναλλαγές να παραμένουν δημόσιες. Για να γίνει αυτό, οι συναλλαγές είναι «ψηφιακά υπογεγραμμένες». Αυτό σημαίνει ότι ένα ιδιωτικό κλειδί χρησιμοποιείται για την κρυπτογράφηση μιας συναλλαγής έτσι ώστε οποιοσδήποτε έχει το δημόσιο κλειδί να μπορεί να την αποκρυπτογραφήσει. Δεδομένου ότι το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο, η κρυπτογράφηση της συναλλαγής με το ιδιωτικό κλειδί αποδεικνύει ότι ο υπογράφων της συναλλαγής έχει πρόσβαση στο ιδιωτικό κλειδί. Εναλλακτικά, μπορεί κανείς να κρυπτογραφήσει δεδομένα με το δημόσιο κλειδί ενός χρήστη, έτσι ώστε μόνο οι χρήστες με πρόσβαση στο ιδιωτικό κλειδί να μπορούν να το

αποκρυπτογραφήσουν. Ωστόσο, ένα σημαντικό μειονέκτημα της κρυπτογραφίας ασύμμετρου κλειδιού είναι ότι είναι συχνά αργή στον υπολογισμό (Yaga et al., 2019).

Ορισμένες χρήσεις της ασύμμετρης κρυπτογραφίας και του ζεύγους δημόσιου-ιδιωτικού κλειδιού στην τεχνολογία αλυσίδας συστοιχιών είναι οι εξής:

- Τα ιδιωτικά κλειδιά χρησιμοποιούνται για την ψηφιακή υπογραφή συναλλαγών.
- Τα δημόσια κλειδιά χρησιμοποιούνται για την δημιουργία διευθύνσεων.
- Τα δημόσια κλειδιά χρησιμοποιούνται για την επαλήθευση υπογραφών που δημιουργούνται με ιδιωτικά κλειδιά.

Η κρυπτογραφία ασύμμετρου κλειδιού παρέχει τη δυνατότητα επαλήθευσης ότι ο χρήστης ο οποίος μεταφέρει αξία σε άλλο χρήστη έχει στην κατοχή του το ιδιωτικό κλειδί που μπορεί να υπογράψει τη συναλλαγή (Yaga et al., 2019).

3.4. Αρχιτεκτονική του Blockchain

Σύμφωνα με τους Zheng et al. (2018) και Monrat et al. (2019) το blockchain περιλαμβάνει μια ακολουθία συστοιχιών, η οποία αποθηκεύει τις πληροφορίες όλων των συναλλαγών, παρόμοια με ένα δημόσιο καθολικό. Αυτές οι συστοιχίες συνδέονται μεταξύ τους μέσω ενός κατακερματισμού αναφοράς που ανήκει στην προηγούμενη συστοιχία γνωστή ως γονική συστοιχία (parent block). Η αρχική συστοιχία ονομάζεται συστοιχία γένεσης (genesis block) και δεν έχει γονική συστοιχία.

Σύμφωνα με τους Ali et al. (2018) και Yaga et al. (2019), μία συστοιχία ή αλλιώς ένα block αποτελείται από την κεφαλή του block (block header) και το σώμα του block (block body). Η κεφαλή του block περιλαμβάνει μεταδεδομένα όπως την έκδοση, τον κατακερματισμό του γονικού block, τον κατακερματισμό της ρίζας του αλγορίθμου

των Merkle Trees, τη χρονική σφραγίδα, τα nBits και το nonce (τυχαίος αριθμός) όπως φαίνεται στον Πίνακα 1.

Πίνακας 1: Ανάλυση της Κεφαλής του block (Πηγή: Monrat et al.,2019)

Πεδία της Κεφαλής του Block	Ορισμοί
Έκδοση (Block Version)	Υποδεικνύει το σύνολο των κανόνων επικύρωσης του block που πρέπει να ακολουθηθεί.
Κατακερματισμός Γονικού Block (Previous Block Hash)	Μια τιμή κατακερματισμού 256-bit που οδηγεί στο προηγούμενο block, δημιουργώντας την «αλυσιδωτή» σχέση μεταξύ των συστοιχιών.
Ρίζα του αλγόριθμου των Merkle Trees (Merkle Tree Root)	Αφορά την τιμή κατακερματισμού της ρίζας του αλγορίθμου των Merkle Trees και χρησιμοποιείται για την ταχύτερη διαχείριση των συναλλαγών του block.
Χρονική Σφραγίδα (Timestamps)	Η χρονική σφραγίδα σε δευτερόλεπτα που αποδίδεται σε κάθε νέο block.
nBitis	Τρέχον στόχος κατακερματισμού σε συμβατή μορφή
Τυχαίος Αιρθμός (Nonce)	Ένα πεδίο 4 byte, το οποίο συνήθως ξεκινά με 0 και αυξάνεται για κάθε υπολογισμό κατακερματισμού

Το σώμα του block αποτελείται από έναν μετρητή συναλλαγών (transaction counter) και συναλλαγές (transactions). Ο μετρητής συναλλαγών αναφέρεται στο πόσες συναλλαγές ακολουθούν και οι συναλλαγές αντιπροσωπεύουν τη λίστα των

καταγεγραμμένων συναλλαγών στο block. Ο μέγιστος αριθμός συναλλαγών που μπορεί να περιέχει ένα block εξαρτάται από το μέγεθός του και το μέγεθος κάθε συναλλαγής. Το blockchain χρησιμοποιεί έναν μηχανισμό ασύμμετρης κρυπτογραφίας για την επικύρωση της ταυτοποίησης των συναλλαγών. Μια ψηφιακή υπογραφή που βασίζεται σε ασύμμετρη κρυπτογραφία χρησιμοποιείται σε ένα αναξιόπιστο περιβάλλον όπως το δίκτυο blockchain. Σε αυτή τη διαδικασία, κάθε συμμετέχων στο δίκτυο έχει ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί. Το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή ή την κρυπτογράφηση της συναλλαγής ενώ το δημόσιο κλειδί διανέμεται σε όλο το δίκτυο και είναι ορατό σε όλους, γεγονός που βοηθά στην αποκρυπτογράφηση της ακόλουθης συναλλαγής.

3.5. Χαρακτηριστικά της Τεχνολογίας Blockchain

Μετά την ανάλυση ορισμένων βασικών εννοιών και λειτουργιών της τεχνολογίας αλυσίδας συστοιχιών πραγματοποιείται περιγραφή των χαρακτηριστικών και των δυνατοτήτων της.

Σύμφωνα με τους Zheng et al. (2018) και Monrat et al. (2019) η τεχνολογία blockchain παρουσιάζει ορισμένα ιδιαίτερα χαρακτηριστικά:

Αποκέντρωση

Στα παραδοσιακά συστήματα η κάθε συναλλαγή πρέπει να επικυρωθεί από μία κεντρική αξιόπιστη αρχή. Σε αντίθεση με ένα κεντρικό σύστημα, μια συναλλαγή στο δίκτυο blockchain μπορεί να διεξαχθεί μεταξύ οποιωνδήποτε δύο ομότιμων (P2P) χωρίς τον έλεγχο ταυτότητας από την κεντρική υπηρεσία. Το blockchain συνεπώς παρέχει την εξασφάλιση της εμπιστοσύνης στις συναλλαγές χρησιμοποιώντας διάφορες διαδικασίες συναίνεσης, μειώνει το κόστος του διακομιστή (συμπεριλαμβανομένου του κόστους ανάπτυξης και του κόστους λειτουργίας) και έχει τη δυνατότητα να μετριάσει τα σημεία συμφόρησης απόδοσης στον κεντρικό διακομιστή.

Ωστόσο, σε πολλές περιπτώσεις το blockchain παρουσιάζει ορισμένους συμβιβασμούς. Για παράδειγμα, σε περιπτώσεις που χρησιμοποιείται ο μηχανισμός συναίνεσης PoW όπως στο Bitcoin και στο Ethereum, το κόστος διακομιστή και ενέργειας είναι υψηλότερο, ενώ η απόδοση είναι αρκετά χαμηλοτερή.

Αυθεντικότητα και Αμεταβλητότητα

Η τεχνολογία αλυσίδας συστοιχιών παρέχει την υποδομή ώστε να εξασφαλίζεται ότι τα δεδομένα είναι αυθεντικά και αμετάβλητα. Ειδικότερα εάν η αλυσίδα συστοιχιών αποτελείται από 10 συστοιχίες ή τμήματα (blocks), το δέκατο block της αλυσίδας περιέχει την τιμή κατατεμαχισμού (hash) του προηγούμενου block και για να δημιουργηθεί ένα νέο block (το ενδέκατο) θα χρησιμοποιηθεί η τιμή κατατεμαχισμού (hash) του προηγούμενου block της αλυσίδας (του δέκατου). Συνεπώς όλες οι συστοιχίες είναι τμήματα της αλυσίδας και συνδέονται μεταξύ τους. Μία αλλαγή ή ενημέρωση σε οποιαδήποτε συναλλαγή θα αλλάξει σημαντικά τον κατακερματισμό του τμήματος της αλυσίδας. Εάν κάποιος θέλει να τροποποιήσει οποιαδήποτε πληροφορία, πρέπει να αλλάξει όλα τα δεδομένα κατακερματισμού του προηγούμενου τμήματος της αλυσίδας, κάτι που θεωρείται εξαιρετικά δύσκολο έως ανέφικτο έργο, λαμβάνοντας υπόψη τον όγκο της δουλειάς που πρέπει να πραγματοποιηθεί. Επιπλέον, μετά τη δημιουργία ενός τμήματος από έναν miner, επιβεβαιώνεται από άλλους χρήστες του δικτύου. Ως εκ τούτου, οποιαδήποτε παραποίηση δεδομένων θα εντοπιστεί από το δίκτυο. Επομένως, το blockchain είναι σχεδόν απαραβίαστο και θεωρείται ως ένα αμετάβλητο κατανεμημένο καθολικό.

Ανωνυμία

Είναι δυνατή η αλληλεπίδραση με το δίκτυο blockchain με μια διεύθυνση που δημιουργείται τυχαία. Ένας χρήστης μπορεί να έχει πολλές διευθύνσεις μέσα σε ένα δίκτυο Blockchain για να αποφύγει την έκθεση της ταυτότητάς του. Καθώς πρόκειται για ένα αποκεντρωμένο σύστημα, καμία κεντρική αρχή δεν παρακολουθεί ή καταγράφει τις ιδιωτικές πληροφορίες των χρηστών. Το blockchain παρέχει ένα ορισμένο επίπεδο ανωνυμίας και διακρίνεται καθώς οι χρήστες του δεν απαιτείται να εμπιστεύονται ο ένας τον άλλον για να λειτουργήσει το σύστημα.

Δυνατότητα Ελέγχου

Όλες οι συναλλαγές που πραγματοποιούνται σε ένα δίκτυο blockchain καταγράφονται σε ένα ψηφιακά κατανεμημένο καθολικό και επικυρώνονται με μια ψηφιακή χρονική σήμανση. Αυτό έχει ως αποτέλεσμα να είναι εφικτός ο έλεγχος και ο εντοπισμός προηγούμενων εγγραφών μέσω της πρόσβασης σε οποιονδήποτε κόμβο στο δίκτυο. Για παράδειγμα, όλες οι συναλλαγές θα μπορούσαν να ανιχνευθούν επαναληπτικά στο Bitcoin, κάτι που διευκολύνει τη δυνατότητα ελέγχου και τη διαφάνεια της κατάστασης δεδομένων στο blockchain. Ωστόσο, με τη διοχέτευση χρημάτων σε πολλούς λογαριασμούς, γίνεται πολύ δύσκολο να εντοπιστεί η προέλευσή τους.

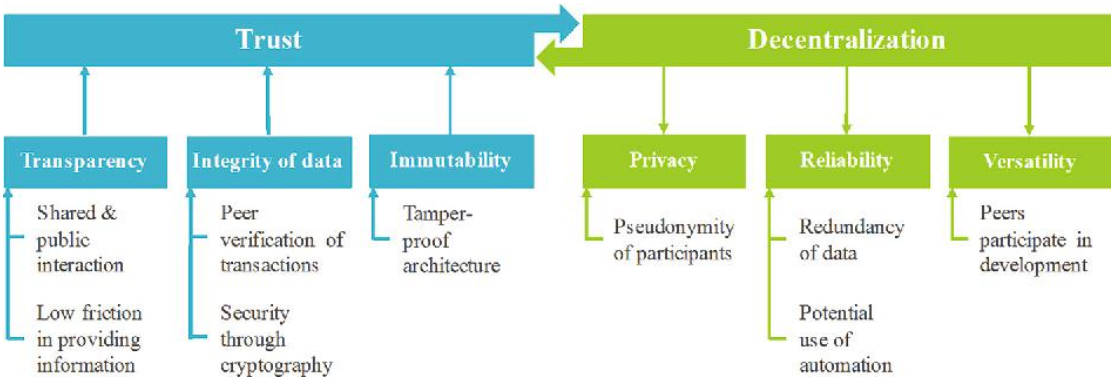
Τα παραπάνω χαρακτηριστικά είναι τα βασικά της τεχνολογίας αλυσίδας συστοιχιών και καλύπτουν τις περισσότερες δυνατότητες που προσφέρει. Ωστόσο η προσέγγιση και ανάλυση των χαρακτηριστικών αυτών μπορεί να πραγματοποιηθεί με διαφορετικό τρόπο τονίζοντας κάθε φορά κάποιο συγκεκριμένο πλεονέκτημα που προκύπτει. Ο Lu (2019) αναφέρει τα εξής χαρακτηριστικά:

- Αποκεντρωμένο σύστημα, επισημαίνοντας ότι η πληροφορία διαμοιράζεται αυτόματα και διανέμεται μεταξύ των κόμβων του δικτύου χωρίς καμία παρέμβαση.
- Εμπιστοσύνη στο σύστημα, το οποίο βασίζεται σε P2P δίκτυα και μαθηματικές μεθόδους χωρίς να είναι απαραίτητη η εμπιστοσύνη μεταξύ των συμμετεχόντων στο δίκτυο.
- Διαφάνεια, καθώς η τεχνολογία blockchain διασφαλίζει ότι καταγράφονται τα δεδομένα των συναλλαγών και κάθε χρήστης μπορεί να επιβεβαιώσει ή να αμφισβητήσει κάποια εγγραφή ώστε το σύστημα να είναι διαφανές και αξιόπιστο.
- Δυνατότητα εντοπισμού και αυθεντικότητα, χαρακτηριστικά που προκύπτουν από τη χρονική σήμανση που λαμβάνει κάθε block και την αποτροπή εισβολής στο δίκτυο με σκοπό την παραποίηση δεδομένων εκτός αν ο κακόβουλος χρήστης διαθέτει πρόσβαση στο 51% των κόμβων, γεγονός που είναι εξαιρετικά δύσκολο να συμβεί.
- Ανωνυμία μέσω των μεθόδων ασύμμετρης κρυπτογράφησης, οι οποίες περιλαμβάνουν κρυπτογράφηση δεδομένων και ψηφιακές υπογραφές.

- Αξιοπιστία, η οποία προκύπτει από το σύστημα το οποίο προστατεύει την ταυτότητα των εμπλεκόμενων μερών και θεωρείται αξιόπιστο παρόλο που δεν είναι απαραίτητο οι χρήστες να έχουν εμπιστοσύνη μεταξύ τους.

Σύμφωνα αρχικά με τους Seebacher και Schüritz (2017) και με τους Ali et al. (2020) τα χαρακτηριστικά μπορούν να κατηγοριοποιηθούν σε δύο μεγάλες ομάδες την εμπιστοσύνη και την αποκέντρωση, οι οποίες βασίζονται στα επιμέρους χαρακτηριστικά και στις σχέσεις που παρουσιάζουν αυτά όπως φαίνεται στην παρακάτω εικόνα:

Εικόνα 1: Κατηγορίες Χαρακτηριστικών της Τεχνολογίας Blockchain (Πηγή: Seebacher και Schüritz, 2017)



Ειδικότερα, τα δύο «χαρακτηριστικά-κλειδιά» της τεχνολογία αλυσίδας συστοιχιών είναι η εμπιστοσύνη και η αποκέντρωση του συστήματος. Η εμπιστοσύνη επεξηγείται από ορισμένους όρους όπως είναι η δημόσια και διαμοιρασμένη αλληλεπίδραση, η επαλήθευση συναλλαγών από χρήστες του δικτύου (peers), η χαμηλή τριβή στην παροχή πληροφοριών, η ασφάλεια μέσω κρυπτογραφίας και η αρχιτεκτονική που αποτρέπει την αλλοίωση δεδομένων. Το αποκεντρωμένο σύστημα βασίζεται σε έννοιες όπως η «ψευδωνυμία» των συμμετεχόντων, η δυνατότητα της χρήσης του αυτοματισμού, το πλεόνασμα των δεδομένων και η συμμετοχή των χρηστών στην ανάπτυξη της τεχνολογίας blockchain και του πολύπλευρου περιβάλλοντος του συστήματος.

Το σημείο που εστιάζουν οι Seebacher και Schüritz (2017) αναφορικά με τα χαρακτηριστικά στοιχεία της τεχνολογίας blockchain είναι ότι τόσο οι έννοιες της

εμπιστοσύνης όσο και της αποκέντρωσης είναι στενά συνδεδεμένες και αλληλένδετες. Αφενός, οι μηχανισμοί που χρησιμοποιούνται για την εδραίωση εμπιστοσύνης, όπως η διαφάνεια, η ακεραιότητα και το αμετάβλητο των δεδομένων, χρειάζονται για τη δημιουργία ενός αποκεντρωμένου δικτύου, στο οποίο θα μπορούν να πραγματοποιούνται αξιόπιστες συναλλαγές χωρίς αξιόπιστο τρίτο μέρος. Από την άλλη πλευρά, ο αποκεντρωτικός χαρακτήρας παρέχει το μέσο για τη συμμετοχή των χρηστών στο δίκτυο, θέτοντας τα θεμέλια για τον μηχανισμό συναίνεσης και καθιστώντας συγχρόνως την ανάγκη ενός αξιόπιστου διαμεσολαβητή παρωχημένη.

3.6. Κατηγορίες Δικτύων Blockchain

Στο σημείο αυτό είναι σημαντικό να αναγνωριστούν οι κατηγορίες του blockchain. Ειδικότερα, σύμφωνα με τους Casino et al. (2019) η τρέχουσα βιβλιογραφία κατηγοριοποιεί τα δίκτυα blockchain ανάλογα με τη διαχείριση και τις άδειες του δικτύου σε τρία διαφορετικά είδη: δημόσια, ιδιωτικά και υβριδικά.

Σε δημόσια blockchain (public or permissionless) οποιοσδήποτε μπορεί να συμμετέχει στο δίκτυο ως νέος χρήστης ή ως νέος miner. Επιπλέον, όλοι οι συμμετέχοντες μπορούν να εκτελούν λειτουργίες όπως συναλλαγές ή συμβόλαια. Στα ιδιωτικά blockchain, τα οποία μαζί με τα υβριδικά ανήκουν στην κατηγορία των permissioned blockchain, συνήθως ορίζεται μια λίστα επιτρεπόμενων χρηστών με συγκεκριμένα χαρακτηριστικά και άδειες στις λειτουργίες δικτύου. Δεδομένου ότι ο κίνδυνος επιθέσεων Sybil είναι σχεδόν αμελητέος εκεί, τα ιδιωτικά δίκτυα blockchain μπορούν να αποφύγουν τους ακριβούς μηχανισμούς PoW. Αντίθετα, θα μπορούσε να υιοθετηθεί ένα ευρύτερο φάσμα πρωτοκόλλων συναίνεσης που θα βασίζονται σε «αντι-κίνητρα». Ένα federated blockchain είναι ένας υβριδικός συνδυασμός δημόσιων και ιδιωτικών blockchain. Παρόλο που μοιράζεται παρόμοιο επίπεδο επεκτασιμότητας και προστασίας απορρήτου με το ιδιωτικό blockchain, η κύρια διαφορά τους είναι ότι επιλέγεται ένα σύνολο κόμβων, που ονομάζονται κόμβοι-αρχηγοί (leader nodes), αντί για μια μόνο οντότητα για την επαλήθευση των

διαδικασιών συναλλαγής. Αυτό επιτρέπει μια μερικώς αποκεντρωμένη σχεδίαση όπου οι κόμβοι-αρχηγοί μπορούν να χορηγούν άδειες σε άλλους χρήστες.

Στον παρακάτω πίνακα συνοψίζονται τα κύρια χαρακτηριστικά κάθε δικτύου blockchain σχετικά με την αποτελεσματικότητα, την ασφάλεια και τους μηχανισμούς συναίνεσης.

Πίνακας 2: Οι κατηγορίες blockchain και τα χαρακτηριστικά τους (Πηγή: Casino et al., 2019)

Ιδιότητα	Public	Private	Federated
Μηχανισμός Συναίνεσης	Δαπανηρό PoW - Όλοι οι miners	Μικρότερης αξίας PoW - Κεντρικός Οργανισμός	Μικρότερης αξίας PoW - Ομάδα των Leader nodes
Έλεγχος ταυτότητας& Ανωνυμία	Ψευδωνυμία - Πιθανότητα ύπαρξης κακόβουλων χρηστών	Αναγνωρισμένος και έμπιστος χρήστης	Αναγνωρισμένος και έμπιστος χρήστης
Αποδοτικότητα Πρωτοκόλλου& Κατανάλωση	Χαμηλή Αποδοτικότητα & Υψηλή Ενέργεια	Υψηλή Αποδοτικότητα & Χαμηλή Ενέργεια	Υψηλή Αποδοτικότητα & Χαμηλή Ενέργεια
Αμεταβλητότητα	Σχεδόν απίθανο να παραβιαστεί	Επιθέσεις Συνωμοσίας	Επιθέσεις Συνωμοσίας
Ιδιοκτησία& Διαχείριση	Δημόσια και χωρίς άδεια	Κεντρική και λίστα με επιτρεπόμενους χρήστες	Μερικώς Κεντρική και επιτρεπόμενοι χρήστες

Έγκριση Συναλλαγής	Εντός λεπτών	Εντός χιλιοστών του δευτερολέπτου	Εντός χιλιοστών του δευτερολέπτου

Οι Zheng et al (2018) και Monrat et al (2019) κατηγοριοποιούν τα δίκτυα Blockchain σε δημόσια (public), ιδιωτικά (private) και υβριδικά (consortium) και αναλύουν την κάθε κατηγορία από διαφορετική οπτική γωνία.

Καθορισμός του μηχανισμού συναίνεσης

Όλοι οι κόμβοι μπορούν να συμμετέχουν στη διαδικασία συναίνεσης στη δημόσια αλυσίδα συστοιχιών, όπως το Bitcoin, ενώ στην κοινοπρακτική αλυσίδα συστοιχιών μόνο μερικά επιλεγμένα σετ κόμβων είναι υπεύθυνα για την επιβεβαίωση ενός νέου block. Στο ιδιωτικό blockchain, μια κεντρική αρχή θα αποφασίσει τους αντιπροσώπους που θα μπορούσαν να καθορίσουν το επικυρωμένο block.

Άδεια Ανάγνωσης

Το public blockchain επιτρέπει την άδεια ανάγνωσης στους χρήστες, σε αντίθεση με το private και consortium blockchain όπου μπορούν να έχουν περιορισμένη πρόσβαση στο κατανεμημένο καθολικό.

Μεταβλητότητα

Στο αποκεντρωμένο δίκτυο blockchain, οι συναλλαγές αποθηκεύονται σε ένα κατανεμημένο καθολικό και επικυρώνονται από όλους τους ομότιμους, γεγονός που καθιστά σχεδόν αδύνατη την τροποποίηση σε ένα δημόσιο blockchain. Αντίθετα, η κοινοπραξία και το ιδιωτικό καθολικό blockchain μπορούν να παραβιαστούν από την επιθυμία της επικρατούσας αρχής.

Αποδοτικότητα

Στο δημόσιο blockchain, οποιοσδήποτε κόμβος μπορεί να ενταχθεί ή να αποχωρήσει από το δίκτυο, γεγονός που το καθιστά εξαιρετικά επεκτάσιμο. Ωστόσο, με την αυξανόμενη πολυπλοκότητα για τη διαδικασία εξόρυξης και την ευέλικτη

πρόσβαση νέων κόμβων στο δίκτυο, οδηγεί σε περιορισμένη απόδοση και μεγαλύτερη λανθάνουσα περίοδο (καθυστέρηση μεταφοράς). Εν αντιθέσει, με λιγότερους ελέγχους επικύρωσης και εκλεκτικά πρωτόκολλα συναίνεσης, η ιδιωτική και κοινοπρακτική αλυσίδα συστοιχιών μπορεί να διευκολύνει την καλύτερη απόδοση και την ενεργειακή απόδοση.

Κεντρικό

Η σημαντική διαφορά μεταξύ αυτών των τριών τύπων blockchain είναι ότι το δημόσιο blockchain είναι αποκεντρωμένο, ενώ η κοινοπραξία είναι μερικώς συγκεντρωτική και το ιδιωτικό blockchain ελέγχεται από μια κεντρική αρχή. Δεδομένου ότι το δημόσιο blockchain είναι ανοιχτό στον κόσμο, μπορεί να προσελκύσει πολλούς χρήστες. Για το blockchain της κοινοπραξίας, θα μπορούσε να εφαρμοστεί σε πολλές επιχειρηματικές εφαρμογές. Επί του παρόντος, η Hyperledger αναπτύσσει επιχειρηματικά πλαίσια consortium blockchain. Το Ethereum έχει επίσης παράσχει εργαλεία για τη δημιουργία consortium blockchain. Για το ιδιωτικό blockchain, υπάρχουν ακόμα πολλές εταιρείες οι οποίες το εφαρμόζουν για αποδοτικότητα και δυνατότητα ελέγχου.

Η παραπάνω ανάλυση παρουσιάζεται συνοπτικά στον πίνακα, επισημαίνοντας τα βασικά σημεία και τον τρόπο που διαφοροποιούνται οι τρείς κατηγορίες δικτύων.

Πίνακας 3: Οι Κατηγορίες Blockchain Και τα Χαρακτηριστικά τους (Πηγή: Zheng et al., 2018, Monrat et al., 2019)

Ιδιότητα	Public blockchain	Consortium blockchain	Private blockchain
Καθορισμός Μηχανισμού Συναίνεσης	Όλοι οι miners	Επιλεγμένο σύνολο κόμβων	Ένας οργανισμός
Άδεια ανάγνωσης	Public	Could be public or restricted	Could be public or restricted

Μεταβλητότητα	Σχεδόν απίθανο να παραβιαστεί	Μπορεί να παραβιαστεί	Μπορεί να παραβιαστεί
Απόδοση	Χαμηλή	Υψηλή	Υψηλή
Κεντρικό	Όχι	Μερικώς	Ναι
Διαδικασία Συναίνεσης	Χωρίς άδεια (Permissionless)	Με άδεια (Permissioned)	Με άδεια (Permissioned)

3.7. Προκλήσεις σχετικά με την Εφαρμογή της Τεχνολογίας Blockchain

Μετά την παραπάνω ανάλυση και την εστίαση στα χαρακτηριστικά της τεχνολογίας blockchain γίνεται φανερό ότι η τεχνολογία αυτή μπορεί να προσφέρει ευκαιρίες και έχει τεράστιες δυνατότητες αξιοποίησης. Ωστόσο, εκτός από τα πλεονεκτήματα που απορρέουν από τη λειτουργία και τα χαρακτηριστικά της, όπως σημειώθηκε στην προηγούμενη ενότητα, προκύπτουν και ορισμένες προκλήσεις και δυσκολίες στην εφαρμογή της.

Οι δυνατότητες που προκύπτουν από τη τεχνολογία blockchain είναι πολλές. Ειδικότερα, τα βασικά στοιχεία, οι αρχές και ο τρόπος λειτουργίας, τα οποία περιλαμβάνουν την ασύμμετρη κρυπτογραφία, τις συναρτήσεις κατακερματισμού, τα πρωτόκολλα συναίνεσης, το δίκτυο P2P, την απουσία κεντρικής αρχής, τα διανεμημένα καθολικά, τη δομή και την αρχιτεκτονική των blocks, αποδίδουν εξαιρετικά σημαντικά πλεονεκτήματα στην τεχνολογία αυτή. Το blockchain χαρακτηρίζεται για την εμπιστοσύνη που παρέχει ως σύστημα μέσω της διαφάνειας, της ακεραιότητας, της αμεταβλητότητας των δεδομένων αλλά και για την αποκέντρωση μέσω της ιδιωτικότητας και της αξιοπιστίας. Ωστόσο, παρά την καινοτόμα λειτουργία του και τα πλεονεκτήματα αυτής, παρουσιάζονται ορισμένοι περιορισμοί και εμπόδια στην εφαρμογή της.

Σύμφωνα με τους Zheng et al. (2018) οι προσκλήσεις και τα προβλήματα της τεχνολογίας αλυσίδας συστοιχιών παρουσιάζονται σε τρείς κύριες κατηγορίες οι οποίες είναι η επεκτασιμότητα, η διαρροή δεδομένων και το selfish mining. Παρακάτω αναλύονται οι κατηγορίες αυτές και προτείνονται και ορισμένες λύσεις και βελτιώσεις που μπορούν να πραγματοποιηθούν.

Επεκτασιμότητα

Καθώς ο αριθμός των συναλλαγών αυξάνεται μέρα με τη μέρα, το blockchain γίνεται πιο «ογκώδες». Όλες οι συναλλαγές πρέπει να αποθηκεύονται για την επικύρωσή τους. Επιπλέον, λόγω του αρχικού περιορισμού του μεγέθους του block και του χρονικού διαστήματος που χρησιμοποιείται για τη δημιουργία ενός νέου block, το blockchain Bitcoin μπορεί να επεξεργαστεί μόνο σχεδόν 7 συναλλαγές ανά δευτερόλεπτο, κάτι που δεν μπορεί να εκπληρώσει την απαίτηση επεξεργασίας εκατομμυρίων συναλλαγών σε πραγματικό χρόνο. Εν τω μεταξύ, καθώς η χωρητικότητα των block είναι πολύ μικρή, πολλές μικρές συναλλαγές ενδέχεται να καθυστερήσουν, καθώς οι mines προτιμούν τις συναλλαγές που έχουν υψηλό κόστος συναλλαγής. Ωστόσο, το μεγάλο μέγεθος block θα επιβράδυνε την ταχύτητα διάδοσης και θα οδηγούσε σε διακλαδώσεις blockchain. Συνεπώς, το πρόβλημα επεκτασιμότητας είναι αρκετά δύσκολο.

Για την αντιμετώπιση του προβλήματος της επεκτασιμότητας προτάθηκαν διάφορες λύσεις, όπως η βελτιστοποίηση της αποθήκευσης και ο επανασχεδιασμός του blockchain. Πιο συγκεκριμένα, η βελτιστοποίηση του συστήματος θα πραγματοποιηθεί μέσω ενός σχήματος, όπου τα αρχεία των συναλλαγών έχουν αφαιρεθεί από το δίκτυο και χρησιμοποιείται μία βάση δεδομένων για να διατηρεί το υπόλοιπο όλων των μη κενών διευθύνσεων. Με αυτόν τον τρόπο, οι κόμβοι δεν χρειάζεται να αποθηκεύουν όλες τις συναλλαγές για να ελέγξουν αν μια συναλλαγή είναι έγκυρη ή όχι. Ακόμη, αναφορικά με τον επανασχεδιασμό του blockchain οι Eyal et al. (2016) πρότειναν το Bitcoin-NG (Next Generation), κύρια ιδέα του οποίου είναι να αποσυνδέσει το συμβατικό block σε δύο μέρη: key block για την εκλογή αρχηγού και microblock για την αποθήκευση συναλλαγών. Οι miners ανταγωνίζονται για να έχουν τη θέση του αρχηγού, ο οποίος θα είναι υπεύθυνος για τη δημιουργία microblock μέχρι να εμφανιστεί ένας νέος αρχηγός. Το Bitcoin-NG επέκτεινε επίσης

τη στρατηγική μεγαλύτερης αλυσίδας όπου μετρούν μόνο τα βασικά block και τα microblock δεν έχουν κανένα «βάρος». Με αυτόν τον τρόπο, το blockchain επανασχεδιάζεται ώστε να αντιμετωπιστεί η αντιστάθμιση μεταξύ μεγέθους block και ασφάλειας δικτύου.

Διαρροή προσωπικών δεδομένων

Το blockchain πιστεύεται ότι είναι πολύ ασφαλές καθώς οι χρήστες κάνουν συναλλαγές μόνο με διευθύνσεις που έχουν δημιουργήσει και όχι με πραγματική ταυτότητα. Οι χρήστες θα μπορούσαν επίσης να δημιουργήσουν πολλές διευθύνσεις σε περίπτωση διαρροής πληροφοριών. Όπως αναφέρουν οι Zheng et al (2018) σε μελέτες που έχουν γίνει τονίζεται ότι υπάρχουν περιπτώσεις που έχουν δείξει ότι το blockchain δεν είναι πάντα ασφαλές. Ειδικότερα, φαίνεται στους Meiklejohn et al. (2013) και Kosba et al. (2016) ότι το blockchain δεν μπορεί να εγγυηθεί το απόρρητο των συναλλαγών, καθώς η αξία όλων των συναλλαγών και των υπολοίπων για κάθε δημόσιο κλειδί είναι δημόσια ορατές. Επιπλέον, άλλη μελέτη (Barcelo, 2014) έδειξε ότι οι συναλλαγές ενός χρήστη με Bitcoin μπορούν να συνδεθούν για να αποκαλύψουν τις πληροφορίες του χρήστη. Ακόμη, οι Biryukov et al. (2014) παρουσίασαν μια μέθοδο για τη σύνδεση ψευδωνύμων χρηστών με διευθύνσεις IP ακόμα και όταν οι χρήστες βρίσκονται πίσω από Network Address Translation (NAT) ή τείχη προστασίας. Ειδικότερα, κάθε πελάτης μπορεί να αναγνωριστεί από ένα σύνολο κόμβων στους οποίους συνδέεται.

Εγωιστική Εξόρυξη

Το blockchain είναι επιρρεπές σε επιθέσεις από miners που συνωμοτούν (selfish miners). Γενικά, είναι γνωστό ότι οι κόμβοι με πάνω από 51% υπολογιστική ισχύ θα μπορούσαν να αντιστρέψουν το blockchain και να αντιστρέψουν τη συναλλαγή που συνέβη. Ωστόσο, έρευνα δείχνει ότι ακόμη και οι κόμβοι με λιγότερη ισχύ 51% εξακολουθούν να είναι επικίνδυνοι. Συγκεκριμένα, οι Eyal και Sirer (2014) έδειξαν ότι το δίκτυο είναι ευάλωτο ακόμα κι αν μόνο ένα μικρό μέρος της ισχύος κατακερματισμού χρησιμοποιείται για εξαπάτηση. Στην εγωιστική στρατηγική εξόρυξης, οι selfish miners διατηρούν τα blocks που έχουν εξορύξει χωρίς μετάδοση και η ιδιωτική διακλάδωση θα αποκαλυφθεί στο κοινό μόνο εάν ικανοποιούνται

ορισμένες απαιτήσεις. Όταν η ιδιωτική διακλάδωση είναι μεγαλύτερη από την τρέχουσα δημόσια αλυσίδα, γίνεται δεκτή από όλους τους miners. Πριν από τη δημοσίευση της ιδιωτικής διακλάδωσης, οι έντιμοι miners (honest miners) σπαταλούν τους πόρους τους σε μία άχρηστη διακλάδωση, ενώ οι selfish miners εξορύσσουν την ιδιωτική τους αλυσίδα χωρίς ανταγωνιστές. Έτσι, οι εγωιστές miners τείνουν να έχουν περισσότερα έσοδα. Οι ορθολογικοί miners θα προσελκύονταν να ενταχθούν στην εγωιστική δεξαμενή και οι εγωιστές θα μπορούσαν να ξεπεράσουν γρήγορα το 51% της ισχύος. Εκτός από το selfish mining έχουν παρουσιαστεί κι άλλες επιθέσεις για να δείξουν ότι το blockchain δεν είναι τόσο ασφαλές.

Οι Monrat et al. (2019) αναφέρουν πως όπως και άλλες αναδυόμενες τεχνολογίες, έτσι και το blockchain δεν είναι εφικτό να εφαρμοστεί σε όλα τα επιχειρηματικά μοντέλα και προσθέτει στις αδυναμίες που έχουν αναφέρει οι Zheng et al. (2018) τη διαλειτουργικότητα, τη κατανάλωση ενέργειας και το ρυθμιστικό πλαίσιο.

Σχετικά με τους περιορισμούς που αναφέρουν και οι Zheng et al. (2018) και οι Monrat et al. (2019), δηλαδή την απόδοση και επεκτασιμότητα, την ιδιωτικότητα και την αμεροληψία και ασφάλεια επισημαίνονται ορισμένα σημαντικά σημεία. Οι Monrat et al. (2019) αναφέρουν ότι η επεκτασιμότητα αφορά τον αριθμό των αντιγράφων στο δίκτυο και η απόδοση διακρίνεται κυρίως για τον αριθμό συναλλαγών ανά δευτερόλεπτο και τον απαιτούμενο χρόνο για την προσθήκη νέου block στην αλυσίδα. Αυτό που αξίζει να σημειωθεί είναι σχετικά με το bitcoin όπου χρησιμοποιείται το PoW και το μέγεθος των block είναι περιορισμένο γεγονός που οδηγεί στο να μην μπορεί να επεξεργαστεί πολλές συναλλαγές ταυτόχρονα η πλατφόρμα. Σχετικά με τα πρωτόκολλα συναίνεσης, το PoW καταναλώνει πολύ μεγάλη ποσότητα ενέργειας, χρειάζεται χρόνος για τη δημοσίευση νέου block και κατά τη δημιουργία του νέου block μπορεί να δημιουργηθούν διακλαδώσεις και να συμβούν «διπλές δαπάνες» πριν καθοριστεί η πιο μακριά αλυσίδα. Εν αντιθέσει, στο πρωτόκολλο PBFT δεν μπορούν να πραγματοποιηθούν διακλαδώσεις, βελτιώνεται η κατανάλωση ενέργειας αλλά είναι περίπλοκο και τα ζητήματα επεκτασιμότητας δεν αντιμετωπίζονται επαρκώς. Για τους άλλους δύο περιορισμούς σημειώνεται ότι με την ιδιωτικότητα αναφέρονται στο γεγονός ότι το σύστημα μπορεί να είναι ευάλωτο

όσον αφορά το απόρρητο των συναλλαγών και με την αμεροληψία και ασφάλεια περιγράφουν το selfish mining.

Οι αδυναμίες του blockchain που προσθέτουν οι Monrat et al. (2019) είναι οι εξής:

Διαλειτουργικότητα

Πολλές επιχειρήσεις και οργανισμοί που ανήκουν σε διαφορετικούς κλάδους ενδιαφέρονται να υιοθετήσουν την τεχνολογία blockchain. Ωστόσο, δεν υπάρχει συγκεκριμένο πρωτόκολλο που θα επιτρέψει σε αυτές να συνεργάζονται μεταξύ τους. Αυτή η κατάσταση χαρακτηρίζεται ως έλλειψη διαλειτουργικότητας και έχει επιζήμιες συνέπειες στην ανάπτυξη της τεχνολογίας αλυσίδας συστοιχιών. Για το λόγο αυτό, αντί να προσφέρει διαφορετικές πρακτικές λύσεις σε μια ποικιλία επιχειρηματικών μοντέλων, τα κρυπτονομίσματα εξακολουθούν να είναι η κύρια πλατφόρμα για την τεχνολογία blockchain. Από τη μία πλευρά, η έλλειψη διαλειτουργικότητας παρέχει ελευθερία στους προγραμματιστές blockchain να κωδικοποιούν σε διαφορετικές πλατφόρμες προγραμματισμού, όμως από την άλλη πλευρά όλα αυτά τα δίκτυα είναι απομονωμένα και δεν μπορούν να αλληλοεπιδράσουν μεταξύ τους. Ως εκ τούτου, απαιτείται τυποποίηση και συνεργασία των επιχειρήσεων στην ανάπτυξη εφαρμογών για κοινή χρήση λύσεων που βασίζονται σε blockchain καθώς και για την ενσωμάτωσή του σε υπάρχοντα συστήματα.

Κατανάλωση Ενέργειας

Ο αλγόριθμος PoW επέτρεψε στο bitcoin να εκτελεί συναλλαγές μεταξύ χρηστών σε ένα κατανεμημένο αποκεντρωμένο περιβάλλον χωρίς εμπιστοσύνη. Κατά τη διάρκεια αυτής της διαδικασίας, οι υπολογιστές των miners καταναλώνουν τεράστια ποσότητα ηλεκτρικής ενέργειας. Σημειώνεται ότι ο μηχανισμός κινήτρων παρακινεί ανθρώπους σε όλο τον κόσμο να εξορύξουν Bitcoin. Η διαδικασία εξόρυξης παρέχει μια σταθερή ροή εσόδων που προσελκύει άτομα να λειτουργούν συσκευές που χρειάζονται ενέργεια για να αποκτήσουν κάποιο κέρδος. Ως αποτέλεσμα, ο συνολικός ρυθμός κατανάλωσης ενέργειας του δικτύου Bitcoin έφτασε σε νέο υψηλό μαζί με την αξία του κρυπτονομίσματος.

Προκειμένου να τονιστεί η επίδραση της εξόρυξης κρυπτονομισμάτων και ειδικότερα του Bitcoin επισημαίνεται ότι εκτός από την τεράστια κατανάλωση

ενέργειας συμβάλλει και στο πολύ έντονο αποτύπωμα άνθρακα. Ακόμη, συγκριτικά με άλλα συστήματα πληρωμών, όπως η VISA γίνεται φανερό ότι οι εφαρμογές blockchain όπως το bitcoin καταναλώνουν μεγαλύτερα ποσά ενέργειας. Συνεπώς, αν και στο blockchain δεν επιβαρύνεται ο χρήστης με το κόστος του ενδιάμεσου, παρουσιάζονται διαφορετικά είδη επιβαρύνσεων. Πιθανές λύσεις που ερευνώνται γι' αυτό το ζήτημα είναι ο επανασχεδιασμός της υποδομής του blockchain ή η χρήση ενός εναλλακτικού αλγόριθμου συναίνεσης όπως το PoS όπου καταναλώνεται λιγότερη ενέργεια.

Νομοθεσία και Ρυθμιστικό πλαίσιο

Οι πλατφόρμες blockchain όπως τα κρυπτονομίσματα αντιμετωπίζουν ρυθμιστικά προβλήματα. Η αιτία είναι ότι τα χαρακτηριστικά αυτού του αποκεντρωμένου συστήματος αποδυναμώνουν την ικανότητα των κεντρικών τραπεζών να κυριαρχούν στην οικονομική πολιτική, γεγονός που καθιστά τις κυβερνήσεις συγκρατημένες ως προς τις τεχνολογίες blockchain (Kakavand et al., 2017). Αναλυτικότερα, πολλές κυβερνήσεις απείλησαν ή ακόμη και έκαναν τα κρυπτονομίσματα παράνομα στην επικράτειά τους. Για παράδειγμα, το Bitcoin απαγορεύεται σε χώρες όπως το Πακιστάν, το Ιράν, ο Ισημερινός, το Μαρόκο και άλλες (Yeoh, 2017).

Παρά τις χρήσεις και τις θετικές επιδράσεις που μπορεί να έχει η τεχνολογία αλυσίδας συστοιχιών, οι ευρύτερες εφαρμογές της αμφισβητούνται και δημιουργούνται ορισμένοι ενδοιασμοί σχετικά με τη στενή ταύτισή της με τα bitcoin λόγω των ύποπτων συσχετισμών του bitcoin με δραστηριότητες νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Σχετικά με τους νόμους και τους περιορισμούς είναι σημαντικό να τονιστεί ότι μπορούν να επηρεάσουν σημαντικά τον τρόπο εξέλιξης και την ταχύτητα ανάπτυξης της τεχνολογίας. Ως εκ τούτου, οι ρυθμιστικές προσεγγίσεις θα πρέπει να εξισορροπηθούν έξυπνα με το καινοτόμο πνεύμα του blockchain, ενώ αναγνωρίζεται και η πιθανότητα της τεχνολογίας να συμβάλλει ακούσια σε συστημικούς κινδύνους στο χρηματοπιστωτικό σύστημα.

Οι Casino et al. (2019) περιγράφουν τα ζητήματα σχετικά με την τεχνολογία αλυσίδας συστοιχιών που έχουν αναγνωριστεί προσθέτοντας ορισμένες νέες οπτικές γωνίες και αναζητώντας κατάλληλες λύσεις γι' αυτά:

1. Καταλληλότητα της τεχνολογίας ανάλογα με τον κλάδο και το πεδίο εφαρμογής

   Επισημαίνεται η σημασία της κατανόησης της λειτουργίας του blockchain αλλά και των λόγων που θα οδηγήσουν στην επιλογή αυτής της τεχνολογίας. Πριν την απόφαση για την εφαρμογή είναι σημαντικό να έχει γίνει αξιολόγηση της κάθε περίπτωσης και να έχει εξασφαλιστεί ότι χρησιμοποιώντας την τεχνολογία αυτή θα υπάρξει προστιθέμενη αξία και βελτιώσεις στην οντότητα που θα εφαρμοστεί.

2. Λανθάνων χρόνος και δυνατότητα επέκτασης του συστήματος

   Ο λανθάνων χρόνος αναφέρεται στο χρόνο που χρειάζεται για να ολοκληρωθεί η συναλλαγή. Αναλυτικότερα, το Bitcoin χρειάζεται περίπου δέκα λεπτά για να επεξεργαστεί ένα νέο block και μαζί με τους σχετικούς ελέγχους ασφαλείας η διαδικασία για την ολοκλήρωση της συναλλαγής διαρκεί κάποια λεπτά. Εν αντιθέσει, το δίκτυο επεξεργασίας των πιστωτικών καρτών της VISA μπορεί να διαχειριστεί χιλιάδες συναλλαγές ανά δευτερόλεπτό. Αναφορικά με τη δυνατότητα επέκτασης του συστήματος σε συνδυασμό και με την απόδοση, η ύπαρξη περισσότερων αντιγράφων στο δίκτυο οδηγεί σε καθυστερήσεις, καθώς γίνεται σαφές ότι όσο ο αριθμός των συναλλαγών που αποθηκεύεται από τους κόμβους μειώνεται, ταυτόχρονα βελτιώνεται και το στάδιο επικύρωσης της συναλλαγής.

3. Βιωσιμότητα του πρωτόκολλου Blockchain

   Ένα από τα σημαντικότερα μειονεκτήματα της τεχνολογίας blockchain είναι η μεγάλη κατανάλωση ενέργειας κατά τη διαδικασία εξόρυξης, ειδικά στα δημόσια δίκτυα που χρησιμοποιούν ως μηχανισμό συναίνεσης το PoW.

4. Κβαντική Ανθεκτικότητα (Quantum resilience)

   Στα περισσότερα blockchain, ο αλγόριθμος κατακερματισμού είναι SHA-256, τον οποίο ένας κβαντικός υπολογιστής χρειάζεται 2^{128} λειτουργίες για να σπάσει χρησιμοποιώντας τον αλγόριθμο του Grover. Αν και αυτό καθιστά το SHA-256 ανθεκτικό σε κβαντικές επιθέσεις, δεν ισχύει το ίδιο για τους αλγόριθμους κρυπτογράφησης δημόσιου κλειδιού που χρησιμοποιούν τα περισσότερα δίκτυα blockchain.

5. Υιοθέτηση του blockchain και διαλειτουργικότητα

Η υιοθέτηση του blockchain αυξάνεται συνεχώς, ωστόσο ορισμένες επιχειρήσεις δεν επιλέγουν την τεχνολογία αλυσίδας συστοιχιών καθώς δεν θα προσφέρει βελτιώσεις στα συστήματα που χρησιμοποιούν ή αποτρέπονται λόγω της έλλειψης ρυθμιστικού πλαισίου. Επιπλέον, ο αριθμός των εφαρμογών που βασίζονται σε blockchain αυξάνεται με γρήγορο ρυθμό, δημιουργώντας έναν τεράστιο αριθμό ετερογενών λύσεων. Ενώ η μεγάλη ποικιλία εφαρμογών και χαρακτηριστικών παρουσιάζει πολλά θετικά, έχει όμως ως συνέπεια σημαντικά ζητήματα διαλειτουργικότητας, εμποδίζοντας την τυποποίηση.

6. Διαχείριση Δεδομένων και θέματα ιδιωτικότητας και ασφάλειας

   Η τεχνολογία blockchain παρουσιάζει περιορισμούς και αδυναμίες στο πεδίο της διαχείρισης και αποθήκευσης ασφαλών και ιδιωτικών δεδομένων. Η αποθήκευση των δεδομένων σε ένα δημόσιο καθολικό δημιουργεί προβλήματα στην εμπιστευτικότητα. Επίσης, η ιδιωτικότητα των συναλλαγών και ο εντοπισμός αυτών είναι άλλο ένα ζήτημα το οποίο χρειάζεται επίλυση. Τέλος, τα smart contracts παρά τις δυνατότητες που προσφέρουν μπορούν να δημιουργήσουν προβλήματα καθώς είναι προγράμματα που μπορεί να περιέχουν λάθη.

ΚΕΦΑΛΑΙΟ 4: ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN ΣΤΗ ΛΟΓΙΣΤΙΚΗ

4.1. Εισαγωγή

Το συγκεκριμένο κεφάλαιο αφορά την εξέλιξη της τεχνολογίας αλυσίδας συστοιχιών και την εφαρμογή της στη λογιστική. Πιο συγκεκριμένα, η εξέλιξη της τεχνολογίας κατηγοριοποιείται είτε ανάλογα με το κλάδο που αφορούν οι εφαρμογές της, δηλαδή κυρίως σε χρηματοοικονομικές και μη χρηματοοικονομικές, είτε στις φάσεις ανάπτυξής της σε blockchain 1.0, blockchain 2.0, blockchain 3.0. Στη συνέχεια, γίνεται λόγος για τις μεθόδους της παραδοσιακής λογιστικής και τον τρόπο που θα επιδράσει το blockchain σε αυτές. Ειδικότερα, αναλύεται η διαδικασία εφαρμογής του στη χρηματοοικονομική λογιστική σε βραχυπρόθεσμο και μακροπρόθεσμο ορίζοντα, οι νέες δυνατότητες που θα προσφέρει αλλά και οι προκλήσεις που θα προκύψουν και οι τρόποι αντιμετώπισης αυτών.

4.2. Στάδια Εξέλιξης του Blockchain

Σχετικά με την εξέλιξη της τεχνολογίας blockchain και τις φάσεις ανάπτυξής της έχουν γίνει ορισμένες κατηγοριοποιήσεις. Ειδικότερα, έχει πραγματοποιηθεί κατηγοριοποίηση των εφαρμογών της τεχνολογίας σε χρηματοοικονομικές και μη-χρηματοοικονομικές (Crosby et al., 2016), λόγω της ύπαρξης πολυάριθμων εφαρμογών που έχουν σχέση με τον ευρύ τομέα των χρηματοοικονομικών αλλά και άλλων τομέων. Επιπλέον, μία ακόμη κατηγοριοποίηση που αξίζει να σημειωθεί αφορά την εξέλιξη της τεχνολογίας και ειδικότερα τις τρεις φάσεις ανάπτυξης:

blockchain 1.0, blockchain 2.0 και blockchain 3.0 (Swan, 2015, Zhang και Jacobsen, 2018, Casino et al., 2018, Lu, 2018, Lu, 2019, Demirkan et al., 2020, Li et al., 2020).

Σύμφωνα με την έρευνα και ανάλυση πολλών ερευνητών (Swan, 2015, Zhang και Jacobsen, 2018, Casino et al., 2018, Lu, 2018, 2019, Demirkan et al., 2020, Li et al., 2020) οι φάσεις ανάπτυξης της τεχνολογίας αλυσίδας συστοιχιών περιγράφονται ως εξής:

Blockchain 1.0

Στο στάδιο αυτό περιλαμβάνεται το νόμισμα και η ανάπτυξη κρυπτονομισμάτων σε εφαρμογές που σχετίζονται με μετρητά, όπως μεταφορά νομισμάτων, εμβάσματα και συστήματα ψηφιακών πληρωμών (Swan, 2015). Τα κρυπτονομίσματα είναι αντιπροσωπευτικά αυτού του σταδίου και το Bitcoin είναι το πιο σημαντικό (Lu, 2019). Εκτός από το Bitcoin υπάρχουν πάνω από 700 είδη κρυπτονομισμάτων, όπως το Ethereum, το Litecoin, το Dogecoin κ.ά., η κεφαλαιοποίηση των οποίων ανέρχεται σε ποσό πάνω από 26 δισεκατομμύρια δολάρια. Συγκρίνοντας κάποιο κρυπτονόμισμα, με το παραδοσιακό νόμισμα, το πρώτο έχει τα εξής χαρακτηριστικά και πλεονεκτήματα: μη αναστρέψιμες, ανιχνεύσιμες συναλλαγές, αποκεντρωμένο δίκτυο, ανωνυμία, ασφάλεια, ταχύτητα και απαλλαγή από περιορισμούς όπως η γεωγραφική τοποθεσία των χρηστών (Li, X. et al.,2020).

Blockchain 2.0

Στην φάση αυτή περιλαμβάνονται τα έξυπνα συμβόλαια και το σύνολο της οικονομίας, της αγοράς και των χρηματοοικονομικών εφαρμογών που χρησιμοποιούν το blockchain και είναι πιο εκτεταμένες από απλές συναλλαγές σε μετρητά: μετοχές, ομόλογα, συμβόλαια μελλοντικής εκπλήρωσης, δάνεια, στεγαστικά δάνεια, τίτλοι, έξυπνα ακίνητα και έξυπνα συμβόλαια (Swan, 2015).

Τα έξυπνα συμβόλαια έχουν ενισχύσει τον μηχανισμό αμοιβαίας εμπιστοσύνης μεταξύ των χρηστών στο IoT και έχουν γίνει η βασική τεχνολογία του blockchain 2.0. Πιο αναλυτικά, υπάρχουν δύο αξιοσημείωτα σημεία σχετικά με την εξέλιξη του blockchain 2.0. Το ένα είναι η ψηφιοποίηση των περιουσιακών στοιχείων,

στην περίπτωση που τα περιουσιακά στοιχεία είτε είναι απαραίτητο είτε έχουν τη δυνατότητα να ψηφιοποιηθούν σε blockchain. Το άλλο είναι το έξυπνο συμβόλαιο, το οποίο είναι και η μεγαλύτερη διαφορά στην πρόοδο του blockchain 2.0, σε σύγκριση με το blockchain 1.0. Το έξυπνο συμβόλαιο μπορεί να εφαρμόσει τη λογική του πραγματικού κόσμου στο blockchain μέσω μιας προηγμένης γλώσσας προγραμματισμού, όπως το Ethereum και το Hyperledger. Πολλά πολύπλοκα συστήματα του πραγματικού «φυσικού» κόσμου μπορούν να επιτευχθούν μέσω έξυπνων συμβολαίων στο σύστημα blockchain. Τα ψηφιακά περιουσιακά στοιχεία και τα έξυπνα συμβόλαια υπάρχουν σε ψηφιακή μορφή και γίνονται όλο και πιο δημοφιλή. Η τεχνολογία blockchain που εφαρμόζεται σε ψηφιακά περιουσιακά στοιχεία και έξυπνα συμβόλαια μπορεί να εντοπίσει πιο αποτελεσματικά πως το περιεχόμενο έχει δημιουργηθεί και να αποδείξει την απόδοση και την αυθεντικότητά του (Lu, 2018).

Επιπλέον μέσω των έξυπνων συμβολαίων οι προγραμματιστές μπορούν να δημιουργήσουν διάφορες εφαρμογές. Ένα έξυπνο συμβόλαιο θεωρείται ως ένα είδος dAPP (Decentralized Application – Αποκεντρωμένη Εφαρμογή). Ειδικότερα, το Ethereum είναι ένα τυπικό σύστημα της τεχνολογίας blockchain της δεύτερης φάσης. Κάθε κόμβος Ethereum «τρέχει» μία EVM (Ethereum Virtual Machine) που εκτελεί έξυπνα συμβόλαια. Στο Ethereum, οι προγραμματιστές μπορούν να χρησιμοποιήσουν μια ποικιλία γλωσσών προγραμματισμού για να αναπτύξουν έξυπνα συμβόλαια, όπως Solidity (η συνιστώμενη γλώσσα), Serpent και LLL. Δεδομένου ότι αυτές οι γλώσσες είναι Turing-complete, τα έξυπνα συμβόλαια μπορούν να επιτύχουν πλούσιες λειτουργίες. Κάθε αναπτυγμένο έξυπνο συμβόλαιο αντιστοιχεί σε μια μοναδική διεύθυνση, μέσω της οποίας οι χρήστες μπορούν να αλληλεπιδρούν με το έξυπνο συμβόλαιο μέσω συναλλαγών από διαφορετικούς πελάτες. Δεδομένου ότι τα έξυπνα συμβόλαια μπορούν να καλούν το ένα το άλλο μέσω μηνυμάτων, οι προγραμματιστές μπορούν να αναπτύξουν dAPPs με περισσότερες δυνατότητες με βάση τα διαθέσιμα έξυπνα συμβόλαια. Σε σύγκριση με την παραδοσιακή εφαρμογή, μια dAPP έχει τα ακόλουθα χαρακτηριστικά και πλεονεκτήματα: αυτονομία και αυτοματοποίηση, σταθερότητα στη λειτουργία, δυνατότητα ανίχνευσης και ασφάλεια (Li et al., 2020).

Blockchain 3.0

Το τρίτο στάδιο ανάπτυξης της τεχνολογίας είναι οι εφαρμογές blockchain πέρα από το νόμισμα, τη χρηματοδότηση και τις αγορές, ιδιαίτερα στους τομείς της κυβέρνησης, της υγείας, της επιστήμης, της πληροφορικής, του πολιτισμού και της τέχνης (Swan, 2015). Το Blockchain 3.0 είναι πέρα από το 1.0 και το 2.0 και περιλαμβάνει εφαρμογές όπως το domain name, την ψηφιακή ταυτότητα, την ηλεκτρονική διακυβέρνηση, τις έξυπνες πόλεις και την ηλεκτρονική ψηφοφορία μεταξύ άλλων (Demirkan et al., 2020).

Σημειώνεται ότι η επόμενη γενιά του blockchain είναι πιο ασαφής συγκριτικά με τις προηγούμενες. Πιο συγκεκριμένα, λόγω της ταχείας ανάπτυξης του blockchain δεν είναι εύκολο να προσδιοριστεί με ακρίβεια η επόμενη γενιά της τεχνολογίας αυτής. Στο μέλλον η τεχνολογία blockchain θα έχει τη δυνατότητα να ενσωματώνει και να διαλειτουργεί με άλλες αναδυόμενες τεχνολογίες όπως το Internet of Things (IoT) και την Τεχνητή Νοημοσύνη (Artificial Intelligence-AI) με σκοπό την παροχή υπηρεσιών με υψηλή ποιότητα στην κοινωνία. Η φάση αυτή της νέας εποχής της προγραμματιζόμενης κοινωνίας (programmable society) είναι η τρίτη φάση ανάπτυξης του blockchain, το οποίο προβλέπεται ότι θα έχει επίδραση σε πολλές πτυχές της ζωής των ανθρώπων και της κοινωνίας (Lu, 2018).

Επιπλέον, σύμφωνα με τον Lu (2019) επισημαίνεται ότι η επόμενη γενιά του blockchain θα είναι η εποχή της προγραμματιζόμενης κοινωνίας με το blockchain of things ή αλλιώς το «blockchain των πραγμάτων». Οι πτυχές που σχετίζονται με το blockchain θα επηρεάσουν τόσο την ανθρώπινη ιδεολογία όσο και την κοινωνική μορφή. Οι κατανεμημένες εφαρμογές συστημάτων τεχνητής νοημοσύνης, όπως Decentralized Application (Dapp), Decentralized Autonomous Organisation (DAO), Decentralized Autonomous Corporation (DAC), αρχίζουν να εμφανίζονται στον πραγματικό κόσμο. Επιπροσθέτως, την εμφάνιση στον κλάδο κάνουν ο αυτοματισμός και η ευφυΐα. Ειδικότερα, η σύγχρονη βιομηχανία έχει εισέλθει σε μια νέα εποχή της τέταρτης βιομηχανικής επανάστασης (Industry 4.0). Στο εγγύς μέλλον, η τεχνολογία blockchain θα γίνει ένα ισχυρό εργαλείο του Industry 4.0, καθώς ενσωματώνει και διαλειτουργεί αρχιτεκτονικές, τεχνολογίες, συσκευές και άλλα συναφείς τεχνικές για την παροχή προϊόντων και υπηρεσιών υψηλής ποιότητας για την κοινωνία.

4.3. Τεχνολογία Blockchain και Λογιστική: Οι Μέθοδοι Εφαρμογής και οι Επιπτώσεις

4.3.1. Οι Παραδοσιακές Μέθοδοι της Χρηματοοικονομικής Λογιστικής και Ελεγκτικής

Η λογιστική και ο έλεγχος είναι εξελιγμένοι μηχανισμοί για την υλοποίηση της αμοιβαίας εμπιστοσύνης και της προστασίας των επενδυτών. Η σύγχρονη λογιστική προήλθε από τις εμπορικές συναλλαγές στην Ιταλία του 13ου αιώνα. Προκειμένου να βελτιωθεί η ακρίβεια των λογιστικών αρχείων, οι έμποροι επινόησαν τη μέθοδο διπλής εγγραφής, η οποία υιοθετήθηκε ευρέως αφού ο Luca Pacioli τη συνόψισε στο εγχειρίδιο μαθηματικών του που δημοσιεύτηκε στη Βενετία το 1494 (Waymire, Basu, 2008, Faccia, Mosteanu, 2019).

Η συνεχής επέκταση των δραστηριοτήτων των επιχειρήσεων οδήγησε σταδιακά σε αναζήτηση εξωτερικής χρηματοδότησης, με τις επιχειρήσεις να έχουν κίνητρο να αποκτήσουν την εμπιστοσύνη των παρόχων κεφαλαίων για να μειώσουν το κόστος κεφαλαίου. Συγχρόνως, οι πάροχοι κεφαλαίων, συμπεριλαμβανομένων των επενδυτών και των δανειστών, απαιτούν επίσης πληροφορίες για να παρακολουθούν τις οικονομικές θέσεις και τα λειτουργικά αποτελέσματα της εταιρείας προκειμένου να διασφαλίσουν την ασφάλεια των κεφαλαίων τους. Προκειμένου να κερδίσουν την εμπιστοσύνη των επενδυτών, οι εταιρείες έχουν κίνητρα να παρέχουν οικονομικές πληροφορίες σε υπάρχοντες και δυνητικούς παρόχους κεφαλαίων. Θεωρητικά, οι εσωτερικοί χρήστες των οικονομικών καταστάσεων έχουν καλύτερη πληροφόρηση για τις επιχειρηματικές δραστηριότητες της εταιρείας από τους εξωτερικούς χρήστες. Η ύπαρξη της ασύμμετρης πληροφόρησης παρέχει ευκαιρίες στις επιχειρήσεις να χειραγωγούν τις αναφορές. Για την απόκτηση περισσότερων κεφαλαίων ή λόγω προσωπικών συμφερόντων, η

διοίκηση της επιχείρησης έχει κίνητρα να παραπλανήσει τους εξωτερικούς παρόχους κεφαλαίων σχετικά με τις οικονομικές θέσεις και τα λειτουργικά αποτελέσματα της οντότητας (Watts, Zimmerman, 1983).

Προκειμένου να διασφαλιστεί η ακεραιότητα των οικονομικών καταστάσεων και η δημοσίευσή τους, προέκυψε το ανεξάρτητο σύστημα εξωτερικού ελέγχου. Μέσω της εφαρμογής των ελεγκτικών διαδικασιών, οι ελεγκτές θα μπορούσαν να ανακαλύψουν απάτες και λάθη στις οικονομικές καταστάσεις και κατά συνέπεια να μειώσουν τις ευκαιριακές συμπεριφορές απόκτησης κερδών των κατόχων εσωτερικής πληροφόρησης σε κάποιο βαθμό. Ως εκ τούτου, το σύστημα εξωτερικού ελέγχου θα μπορούσε σε κάποιο βαθμό να μειώσει την ασυμμετρία πληροφοριών μεταξύ των εσωτερικών χρηστών πληροφοριών των επιχειρήσεων και των εξωτερικών και να αυξήσει την αξία της εταιρείας (Watts, Zimmerman, 1983, Yu et al., 2018).

Ωστόσο, ορισμένα λογιστικά σκάνδαλα, όπως αυτό της Enron και της WorldCom, έδειξαν ότι οι εξωτερικοί ελεγκτές δεν διατήρησαν σωστά την ανεξαρτησία τους ή δεν μπορούσαν να ανακαλύψουν πλήρως την απάτη και τα λάθη στις οικονομικές καταστάσεις των εταιρειών. Εκτός από τους ελεγκτές, οι οποίοι αποτυγχάνουν να μειώσουν αποτελεσματικά τον κίνδυνο ανίχνευσης, ο εγγενής κίνδυνος και ο κίνδυνος ελέγχου ή κίνδυνος ελέγχου εσωτερικού συστήματος είναι επίσης σημαντικοί παράγοντες των ελεγκτικών κινδύνων. Ειδικότερα, ο κίνδυνος ανίχνευσης θεωρείται ως η πιθανότητα παρά την εφαρμογή κατάλληλων ελεγκτικών διαδικασιών, ο ελεγκτής να μην αποτρέψει ή να μην εμποδίσει ουσιώδη σφάλματα ή λογιστικές παραλείψεις με αποτέλεσμα να συνεχίσουν να εμφανίζονται στις οικονομικές καταστάσεις. Ο κίνδυνος αυτός προσαρμόζεται από τον ελεγκτή ενώ ο εγγενής κίνδυνος και ο κίνδυνος ελέγχου είναι κίνδυνοι που αφορούν την ελεγχόμενη εταιρεία. Σκοπός των ελεγκτών είναι να μειώσουν τον κίνδυνο σε ένα χαμηλό επίπεδο και να υποστηρίξουν ότι οι οικονομικές αναλύσεις δίνουν μια πραγματική και δίκαιη εικόνα. Ωστόσο, ο έλεγχος μπορεί να μειώσει αλλά όχι να εξαλείψει στο έπακρο την απάτη και τα λάθη στις δημοσιευμένες οικονομικές καταστάσεις των εταιρειών (Νεγκάκης, Ταχυνάκης, 2017).

Συνοπτικά, η εμφάνιση και η ανάπτυξη της χρηματοοικονομικής λογιστικής και του ανεξάρτητου ελέγχου θεωρούνται εξαιρετικά σημαντικές καθώς μεταξύ άλλων στοχεύουν στη λύση του προβλήματος της ασυμμετρίας των πληροφοριών μεταξύ επιχειρήσεων και εξωτερικών χρηστών πληροφοριών. Ωστόσο, λόγω της σύγκρουσης των συμφερόντων μεταξύ εσωτερικών και εξωτερικών προσώπων, της ασάφειας που μπορεί να υπάρξει στη λογιστική και της μη ανεξάρτητης διεξαγωγής του ελέγχου, η χρηματοοικονομική λογιστική και ο εξωτερικός έλεγχος δεν είναι εφικτό να λύσουν πλήρως το πρόβλημα της ασύμμετρης πληροφόρησης μεταξύ εσωτερικών και εξωτερικών χρηστών πληροφοριών (Yu et. Al, 2018).

4.3.2. Ανάλυση της Διαδικασίας Εφαρμογής του Blockchain στη Χρηματοοικονομική Λογιστική

Οι εισηγμένες εταιρείες πρέπει να γνωστοποιούν τις οικονομικές τους καταστάσεις σε τακτική βάση σύμφωνα με το εκάστοτε ρυθμιστικό πλαίσιο. Οι οικονομικές καταστάσεις περιλαμβάνουν όπως αναφέρει το πρώτο Διεθνές Λογιστικό Πρότυπο την κατάσταση οικονομικής θέσης ή ισολογισμό, την κατάσταση αποτελεσμάτων χρήσεων, την κατάσταση ταμειακών ροών, την κατάσταση μεταβολών ιδίων κεφαλαίων και τις σημειώσεις (Νεγκάκης, 2015). Προκειμένου να επωφεληθεί η διοίκηση της εταιρείας και να μεγιστοποιήσει τα συμφέροντά της, μπορεί να παραπλανήσει τους χρήστες πληροφοριών χειραγωγώντας δεδουλευμένα, κατασκευάζοντας συναλλαγές και αποκαλύπτοντας ψευδείς πληροφορίες. Η αξιοπιστία των δημοσιευμένων οικονομικών καταστάσεων και σημειώσεων είναι εγγυημένη σε κάποιο βαθμό μετά τον έλεγχο. Ωστόσο, οι χρήστες εξωτερικών πληροφοριών δεν είναι σε θέση να παρατηρήσουν τις πραγματικές συναλλαγές και την λογιστική διαδικασία μιας εταιρείας, εξετάζοντας αποκλειστικά τις τελικές οικονομικές καταστάσεις, καθώς δεν μπορούν να αποκτήσουν πλήρη, ακριβή και έγκαιρη κατανόηση της οικονομικής θέσης, της λειτουργικής απόδοσης και της κατάστασης ταμειακών ροών της εταιρείας (Yu et. Al, 2018).

Σύμφωνα με τους Demirkan et al. (2020) πραγματοποιούνται δραματικές αλλαγές στον τομέα της λογιστικής με την εισαγωγή λογισμικού ικανού να παράγει διαφορετικές πληροφορίες και να διατηρεί αρχεία συναλλαγών. Ειδικότερα, η χρήση του λογισμικού από περιορισμένο ή κεντρικό σύστημα λογιστικής σταδιακά επεκτάθηκε σε ένα αποκεντρωμένο σύστημα με χρήση διαδικτύου. Καθώς η τεχνολογία αλυσίδας συστοιχιών εξελίσσεται, η λογιστική βασισμένη στην τεχνολογία αυτή (blockchain accounting) έχει αρχίσει να παρουσιάζεται με σκοπό να βελτιώσει τον κλάδο της λογιστικής και να παρακολουθεί τις διαδικασίες που πραγματοποιούνται σε blocks με ασφαλή τρόπο.

Αναλυτικότερα, το blockchain καταγράφει και επικυρώνει τις πληροφορίες με αποκεντρωμένο τρόπο και η όλη διαδικασία δεν απαιτεί κάποια κεντρική αρχή. Επιπλέον, η τεχνολογία blockchain εγγυάται ότι οι πληροφορίες είναι διαφανείς, ασφαλείς, απαραβίαστες και αξιόπιστες μέσω της τεχνολογίας κατανεμημένου καθολικού, της συνάρτησης hash και του μηχανισμού PoW. Ως αποτέλεσμα, η τεχνολογία blockchain έχει μεγάλες δυνατότητες ενίσχυσης της εμπιστοσύνης μεταξύ των συμμετεχόντων στην αγορά (Yermack, 2017) και υποστηρίζεται ότι η εφαρμογή της τεχνολογίας blockchain στη χρηματοοικονομική λογιστική προσφέρει τη δυνατότητα να καταστήσει τη λογιστική των επιχειρήσεων ως μία διαφανή διαδικασία, βελτιώνοντας την ποιότητα των πληροφοριών των εξωτερικών αναφορών και μειώνοντας αποτελεσματικά την ασυμμετρία των πληροφοριών μεταξύ επιχειρήσεων και εξωτερικών επενδυτών (Yu et al., 2018).

Αναφορικά με το σχέδιο της εφαρμογής του blockchain στη χρηματοοικονομική λογιστική σύμφωνα με τους Yu et al. (2018) περιλαμβάνονται δύο πτυχές. Πιο συγκεκριμένα, από τη μία πλευρά οι εισηγμένες εταιρείες αποκαλύπτουν λογιστικές πληροφορίες μέσω του blockchain. Οι εταιρείες δημοσιεύουν τα έγγραφα από τα οποία αποδεικνύονται οι συναλλαγές και τα γεγονότα καθώς και τις λογιστικές πολιτικές και μεθόδους που ενσωματώνονται στα έξυπνα συμβόλαια στο blockchain της λογιστικής. Μόλις δημιουργηθεί το έξυπνο συμβόλαιο, εάν η εταιρεία το αλλάξει διακριτικά, όλες οι τροποποιήσεις θα καταγράφονται στο blockchain και θα είναι ανιχνεύσιμες. Από την άλλη πλευρά, διάφοροι ενδιαφερόμενοι, ως κόμβοι blockchain, θα συμμετέχουν στο

ανταγωνιστικό mining, θα καταγράφουν, θα επικυρώνουν αμέσως τις πληροφορίες που υποβάλλονται από την εταιρεία σε ένα νέο block και στη συνέχεια θα τις αναμεταδίδουν στο δίκτυο blockchain. Μεταξύ των κόμβων μπορούν να είναι οι θεσμικοί επενδυτές, οι οποίοι κινητοποιούνται εκτός από τις ανταμοιβές εξόρυξης νέων blocks και από το πλεονέκτημα της έγκαιρης πρόσβασης σε εταιρικές πληροφορίες, οι ελεγκτές και δικηγόροι καθώς μπορούν να ελέγξουν τα αποδεικτικά έγγραφα και τα έξυπνα συμβόλαια που δημοσιεύονται από την εταιρεία και να εκδώσουν τη γνώμη ελέγχου τους για το blockchain και τέλος οι ρυθμιστικές αρχές και τα χρηματιστήρια, ώστε να είναι πιο αποτελεσματική η παρακολούθηση των δραστηριοτήτων των εταιρειών και της αγοράς.

Μία άλλη οπτική γωνία σχετικά με την εφαρμογή της τεχνολογίας blockchain στη λογιστική η οποία αξίζει να σημειωθεί είναι η τριπλή εγγραφή στη λογιστική (triple-entry-accounting). Σύμφωνα με τους Faccia και Mosteanu (2019), η λογιστική τριπλής εγγραφής προσθέτει ένα επίπεδο σαφήνειας και ειλικρίνειας στην τήρηση βιβλίων που δεν μπορεί να προσφέρει η λογιστική διπλής εγγραφής, η οποία είναι η μέθοδος που χρησιμοποιείται εδώ και πολύ καιρό. Ο τρόπος με τον οποίο συμβαίνει αυτό είναι ότι διατίθενται οι διευθύνσεις Α, Β και μία τρίτη διεύθυνση που είναι η απόδειξη επιβεβαίωσης. Το τρίτο δημόσιο καθολικό επιτρέπει και στα δύο εμπλεκόμενα μέρη να εναρμονίσουν τα λογιστικά τους βιβλία και να επιβεβαιωθεί ότι και οι τρεις εγγραφές βρίσκονται σε συναίνεση. Επιπλέον σημειώνεται ότι εμφανίζονται όλες οι συναλλαγές και όλες οι χρεώσεις και πιστώσεις που πραγματοποιούνται.

Επιπροσθέτως σημειώνεται ότι σε ορισμένες περιπτώσεις το permissioned blockchain μπορεί να εφαρμοστεί. Μέσω αυτού του τύπου blockchain, τα εμπλεκόμενα μέρη μπορούν να έχουν διαφορετικές προβολές δεδομένων, περιορίζοντας την πρόσβαση σε ορισμένα δεδομένα. Τα συστήματα τριπλής εγγραφής μέσω blockchain μπορούν να προγραμματιστούν ώστε να ακολουθούν λογιστικά πρότυπα και κανονισμούς αυτόματα χρησιμοποιώντας έξυπνα συμβόλαια και θα μπορούσαν ακόμη και να αυτοματοποιήσουν τις φορολογικές δηλώσεις μέσω συνεχών ενημερώσεων.

Ακόμη, τονίζεται ότι η τεχνολογία Blockchain επιτρέπει την έγκαιρη εξέταση πιθανών σφαλμάτων ή απάτης στις λογιστικές εγγραφές (π.χ. διπλές πληρωμές), καθώς και την αυτοματοποίηση της επαλήθευσης συναλλαγών χρησιμοποιώντας δεδομένα από επιχειρηματικούς εταίρους. Επιπλέον, τα έξυπνα συμβόλαια που κωδικοποιούνται με λογιστικούς και επιχειρηματικούς κανόνες θα μπορούσαν να επιτρέψουν τον αποτελεσματικό έλεγχο της διαδικασίας καταγραφής (Dai, Vasarhelyi, 2017, Faccia, Mosteanu, 2019).

Ο Khandelwal (2019) εκτελεί μια ανάλυση SWOT του blockchain στη λογιστική και τα χρηματοοικονομικά στην εργασία του. Μερικά από τα δυνατά σημεία και τις ευκαιρίες που απαριθμεί είναι: αυξημένη αποδοτικότητα, οικονομικά αποτελεσματική, διακυβέρνηση και εμπιστοσύνη με συναλλαγές που βασίζονται στη συναίνεση, ψηφιοποίηση του λογιστικού συστήματος, ενίσχυση της απασχόλησης και αρχεία εκδόσεων και διαπραγμάτευσης μετοχών. Επίσης, αναφέρει το παράδειγμά της ICICI Bank όπου αποδεικνύεται ότι η αποτελεσματικότητα του λογιστικού συστήματος έχει αυξηθεί με τη χρήση της τεχνολογίας blockchain. Σημειώνεται ότι δεδομένου ότι τα περισσότερα μέρη πρέπει να συμφωνήσουν όταν γίνεται μια αλλαγή ή όταν πρέπει να προστεθούν δεδομένα στο blockchain, αυτό δημιουργεί ένα πιο αξιόπιστο σύστημα. Αναλυτικότερα, επιτρέπει οποιεσδήποτε αμφισβητούμενες αλλαγές να επανεξετάζονται άμεσα από τα εμπλεκόμενα μέρη, γεγονός που είναι εξαιρετικά σημαντικό για το επίπεδο ασφάλειας του blockchain για την εταιρεία. Συνεπώς, θεωρείται ότι το blockchain είναι η εναλλακτική των παραδοσιακών μεθόδων λογιστικής.

Παρακάτω ακολουθεί ολοκληρωμένη η SWOT ανάλυση που πραγματοποίησε ο Khandelwal (2019).

Πίνακας 4: Ανάλυση SWOT για τη λογιστική με βάση το blockchain (Πηγή: Khandelwal, 2019)

Δυνάμεις	Αδυναμίες
➢ Δυσκολία να πραγματοποιηθούν κακόβουλες επιθέσεις ➢ Αυξημένη Απόδοση	➢ Ανθρώπινοι πόροι με ειδίκευση στον τομέα IT και στο χρηματοοικονομικό ή λογιστικό κλάδο

➢ Αποδοτικό από οικονομικής άποψης ➢ Ενισχυμένη Ιδιωτικότητα ➢ Διαφάνεια και δυνατότητα ελέγχου ➢ Διακυβέρνηση και εμπιστοσύνη μέσω των συναλλαγών που βασίζονται σε πρωτόκολλα συναίνεσης	➢ Εξοικείωση με τη νέα τεχνολογία ➢ Περισσότερη χρήση του διαδικτύου ➢ Νέοι κανονισμοί και συμμόρφωση με το ρυθμιστικό πλαίσιο ➢ Διασφάλιση της αξιοπιστίας των αρχείων ➢ Αρχική κλιμάκωση και bootstrapping ➢ Περισσότερος χρόνος και κόστος ➢ Τεράστια υπολογιστική ισχύ
Opportunity ➢ Ψηφιοποίηση λογιστικού συστήματος ➢ Ενίσχυση της απασχόλησης ➢ Έλεγχος έξυπνων συμβολαίων ➢ Εφαρμογή στο εταιρικό σύστημα ψηφοφορίας ➢ Αρχεία έκδοσης και διαπραγμάτευσης μετοχών ➢ Οικονομικές και μη εφαρμογές	Threat ➢ Διακυβέρνηση Blockchain και «επίθεση του 51%» ➢ Κακόβουλες επιθέσεις ➢ Απώλεια κλειδιών ➢ SYN flood επίθεση/ direct denial of service (DDoS) ➢ Επίθεση Sybil ➢ «Empty voting» - «Εκμετάλλευση» ιδιοκτησίας για προσωρινή απόκτηση δικαιώματος ψήφου ➢ Εμπιστοσύνη των αρχείων

4.3.3. Το Blockchain στη Χρηματοοικονομική Λογιστική και η Επιρροή του

Η λογιστική είναι ένας κλάδος που επηρεάζεται σημαντικά από τη χρήση νέων τεχνολογιών. Οι εταιρείες πρέπει να αρχίσουν να πραγματοποιούν προσαρμογές για να συμμορφωθούν με την νέα κατάσταση. Το blockchain είναι μια από τις κύριες τεχνολογίες που προορίζονται να αλλάξουν τον λογιστικό κλάδο (Dai, Vasarhelyi, 2017, Demirkan et al., 2020). Ακολουθεί μία ανάλυση βασισμένη στο έργο των Yu et

al. (2018) για τον τρόπο με τον οποίο η τεχνολογία blockchain θα ενσωματωθεί στη λογιστική λαμβάνοντας υπόψη το χρονικό ορίζοντα αναφοράς. Ειδικότερα, σε μακροπρόθεσμη βάση επισημαίνονται οι αλλαγές που θα πραγματοποιηθούν στις λογιστικές εργασίες όπως γίνονται σήμερα και σε βραχυπρόθεσμη βάση σημειώνονται οι δυσκολίες που εμφανίζονται αναφορικά με τα προβλήματα που πρέπει να αντιμετωπιστούν και την ωριμότητα της τεχνολογίας.

Η μακροπρόθεσμη εφαρμογή του blockchain στη χρηματοοικονομική λογιστική.

Αν και οι εταιρείες υποχρεούνται να εφαρμόζουν λογιστικές μεθόδους που καθορίζονται από τα λογιστικά πρότυπα για την καταγραφή, την παρουσίαση και τη γνωστοποίηση στην παραδοσιακή λογιστική, εξακολουθούν να έχουν διακριτική ευχέρεια ως προς τις λογιστικές μεθόδους όπως οι λογιστικές πολιτικές που χρησιμοποιούνται και οι λογιστικές εκτιμήσεις και κρίσεις που πραγματοποιήθηκαν. Οι εισηγμένες εταιρείες παρέχουν τακτικά οικονομικές καταστάσεις στην αγορά, αλλά δεν δημοσιοποιούν αναλυτικά όλες τις λογιστικές διαδικασίες για την προετοιμασία των αναφορών. Μολονότι αυτή η θεσμική ρύθμιση θα μπορούσε να προστατεύσει ορισμένες ιδιωτικές πληροφορίες των επιχειρήσεων, υπάρχει επίσης μια σειρά αρνητικών συνεπειών. Πρώτον, ο κίνδυνος αλλοίωσης των συναλλαγών υπάρχει είτε η εταιρεία χρησιμοποιεί έντυπο είτε ηλεκτρονικό καθολικό. Δεύτερον, τα διοικητικά στελέχη ή οι μέτοχοι εισηγμένων εταιρειών μπορούν να προβούν σε χειραγώγηση ή να κατασκευάσουν συναλλαγές για να μεγιστοποιήσουν τα προσωπικά τους συμφέροντα. Τέλος, ακόμη και αν υπάρχει εξωτερικός έλεγχος, οι ελεγκτές μπορεί να μην είναι σε θέση να εντοπίσουν όλες τις απάτες και τα λάθη της εταιρείας ή μπορεί να μην έχουν την ανεξαρτησία να ενημερώσουν την αγορά για τα προβλήματα που ανακαλύφθηκαν.

Οι Yu et al. (2018) και Byström (2019) επισημαίνουν ορισμένα σημαντικά σημεία σχετικά με την χρήση της λογιστικής βασισμένη στο blockchain:

- Οι εταιρείες μπορούν να δημοσιεύουν αποδεικτικά έγγραφα στο δημόσιο blockchain και το δημόσιο blockchain θα δημιουργεί αυτόματα λογιστικά βιβλία και οικονομικές καταστάσεις μέσω έξυπνων συμβολαίων. Τα λογιστικά πρότυπα και οι παραδοχές που χρησιμοποιούνται από τις εταιρείες θα

αντικατοπτρίζονται σε έξυπνα συμβόλαια, τα οποία θα καταγράφονται μόνιμα. Αυτή η διαδικασία αλλάζει θεμελιωδώς τη μέτρηση, την παρουσίαση και τη γνωστοποίηση στη χρηματοοικονομική λογιστική.

- Η εφαρμογή της τεχνολογίας blockchain στη χρηματοοικονομική λογιστική μπορεί να μειώσει τον λειτουργικό κίνδυνο και τα σφάλματα μέτρησης, καθώς οι οικονομικές καταστάσεις δημιουργούνται αυτόματα από έξυπνα συμβόλαια. Επιπλέον, η έγκαιρη παροχή λογιστικών πληροφοριών μειώνει εν μέρει τη χρονική καθυστέρηση μεταξύ της δημιουργίας λογιστικών πληροφοριών και της δημοσίευσής τους και η διαφάνεια και η ιχνηλασιμότητα του blockchain της λογιστικής θα αυξήσει την πιθανότητα εντοπισμού απάτης. Τα παραπάνω έχουν ως αποτέλεσμα η διαχείριση κερδών (earnings management) να μειωθεί.
- Η χρήση του blockchain στη χρηματοοικονομική λογιστική σημαίνει ότι θα υπάρχουν χιλιάδες αντίγραφα ασφαλείας μόλις αναρτηθεί στη δημόσια αλυσίδα συστοιχιών και όλες οι συναλλαγές είναι ορατές σε όλα τα μέλη του δικτύου (Yermack, 2017). Αυτό θα καταστήσει τη διαδικασία λογιστικής και αναφοράς πιο διαφανή και ανιχνεύσιμη, καθώς επαληθεύονται και εποπτεύονται από όλους τους κόμβους του blockchain, γεγονός που θα αυξήσει την αξιοπιστία των λογιστικών πληροφοριών.
- Με την εφαρμογή της τεχνολογίας blockchain, οι οικονομικές καταστάσεις μπορούν να παράγονται έγκαιρα αυξάνοντας τη χρησιμότητα και επικαιρότητα των καταστάσεων, σε αντίθεση με την παραδοσιακή μέθοδο δημοσίευσης των οικονομικών καταστάσεων σε ετήσια βάση. Επισημαίνεται ότι με αυτό τον τρόπο οι εξωτερικοί χρήστες των πληροφοριών μπορούν ακόμη και να συγκεντρώνουν τις συναλλαγές των επιχειρήσεων από τις οποίες προκύπτουν οι οικονομικές καταστάσεις ανά πάσα στιγμή μόνοι τους (Yermack, 2017).

Εν ολίγοις, η έλευση της τεχνολογίας blockchain θα έχει τεράστιο αντίκτυπο στη μέτρηση, την παρουσίαση και τη γνωστοποίηση στη χρηματοοικονομική λογιστική, η οποία μειώνει τα σφάλματα στη γνωστοποίηση και τη διαχείριση κερδών, βελτιώνει

σε μεγάλο βαθμό τα ποιοτικά χαρακτηριστικά των πληροφοριών και μετριάζει το πρόβλημα της ασυμμετρίας πληροφοριών.

Η βραχυπρόθεσμη εφαρμογή του blockchain στη χρηματοοικονομική λογιστική.

Ωστόσο, με βάση την ανάλυση που έχει πραγματοποιηθεί και σε προηγούμενα κεφάλαια, η τεχνολογία blockchain βρίσκεται σε πειραματικό στάδιο όσον αφορά την εφαρμογή της και παρουσιάζονται ορισμένα προβλήματα όπως τα αναφέρουν οι Yu et al. (2018): περιορισμένη ικανότητα επεξεργασίας δεδομένων, εμπιστευτικότητα πληροφοριών και ρυθμιστικές δυσκολίες, τα οποία περιγράφονται παρακάτω.

1. Περιορισμένη ικανότητα επεξεργασίας δεδομένων

   Ο όγκος των λογιστικών πληροφοριών των εταιρειών είναι τεράστιος και η τρέχουσα τεχνολογία blockchain δεν είναι σε θέση να διαχειριστεί αποτελεσματικά. Το σημείο αυτό είναι σημαντικό καθώς θα μπορούσε να προκαλέσει σημαντικό κόστος σε εταιρείες που θέλουν να εφαρμόσουν αυτήν την τεχνολογία, καθώς τα τέλη χρέωσης θα ήταν πολύ μεγάλα.
2. Εμπιστευτικότητα πληροφοριών

   Λόγω των χαρακτηριστικών διαφάνειας και μονιμότητας, οι πληροφορίες μπορούν να ληφθούν και να προβληθούν από οποιονδήποτε οπουδήποτε, γεγονός που θα αυξήσει το κόστος των εταιρειών που διαθέτουν αποκλειστικές πληροφορίες ή πληροφορίες που αφορούν πνευματική ιδιοκτησία. Ειδικότερα, εάν η αποκάλυψη πληροφοριών διαρρέει τα εμπορικά μυστικά του παρόχου πληροφοριών, συνεπάγεται αποκλειστικό κόστος, το οποίο θα επηρεάσει δυσμενώς τη λειτουργία της εταιρείας. Ως αποτέλεσμα, οι εταιρείες με εξαιρετικά υψηλό κόστος ιδιοκτησίας ενδέχεται να μην έχουν κίνητρα να χρησιμοποιήσουν το blockchain για γνωστοποίηση πληροφοριών.
3. Ρυθμιστικές δυσκολίες

   Με την ποικιλομορφία και την ανωνυμία των κόμβων και την ύπαρξη της «επίθεσης 51%», η δυσκολία στη θέσπιση ρυθμιστικού πλαισίου θα αυξηθεί. Επειδή η αποκάλυψη εταιρικών πληροφοριών είναι σημαντική για να επηρεάσει την τιμή της μετοχής, είναι πιθανό ορισμένοι κόμβοι να προσθέσουν ψευδείς πληροφορίες στο blockchain για να χειραγωγήσουν την

τιμή της μετοχής και να αποκομίσουν ένα εφάπαξ κέρδος. Αυτό το πρόβλημα επιδεινώνεται εάν οι κόμβοι που συνεννοούνται μπορούν να χειριστούν περισσότερο από το 50% της υπολογιστικής ισχύς.

Επομένως, βραχυπρόθεσμα, δεν είναι ρεαλιστικό για όλες τις εταιρείες να πραγματοποιούν τη λογιστική και την υποβολή εκθέσεων μέσω της αλυσίδας συστοιχιών.

4.3.4. Πιθανές Αρνητικές Επιπτώσεις και Απειλές της Εφαρμογής του Blockchain στη Λογιστική

Σύμφωνα με τους Yu et al. (2018) εκτός από τα θετικά στοιχεία που μπορεί να προσφέρει η τεχνολογία blockchain με την εφαρμογή της στη λογιστική, εντοπίζονται και ορισμένα προβλήματα και μειονεκτήματα. Πιο συγκεκριμένα, με το νέο λογιστικό σύστημα αυξάνεται η δυσκολία των εταιρειών να αλλοιώσουν λογιστικά δεδομένα, αλλά αυτό δεν σημαίνει ότι η χρήση του blockchain στη χρηματοοικονομική λογιστική μπορεί να εξαλείψει ολοκληρωτικά τις απάτες. Ειδικότερα, εφόσον τα πιθανά οφέλη είναι αρκετά μεγάλα και εξακολουθούν να υπάρχουν κίνητρα για τις εταιρείες να εξαπατήσουν παραποιώντας τα αποδεικτικά έγγραφα, είναι πιθανό να πραγματοποιηθούν λογιστικές απάτες. Συνεπώς, μία πιθανή απειλή της υιοθέτησης του blockchain στη χρηματοοικονομική λογιστική είναι ότι οι εταιρείες μπορεί να στραφούν στην «κατασκευή» συναλλαγών για να λάβουν τα επιθυμητά αποτελέσματα.

Επιπροσθέτως, η μακροπρόθεσμη εφαρμογή του blockchain στη λογιστική έχει ως αποτέλεσμα την ανακατεύθυνση των καθηκόντων των λογιστών. Αναλυτικότερα, η τεχνολογία blockchain θα μπορούσε να αυτοματοποιήσει την αναγνώριση, την μέτρηση, την παρουσίαση και τη γνωστοποίηση, η οποία αντικαθιστά τη θέση των μεθόδων της παραδοσιακής χρηματοοικονομικής λογιστικής μακροπρόθεσμα. Αυτό έχει ως αποτέλεσμα να μειωθούν οι θέσεις

εργασίας των λογιστών με την παραδοσιακή έννοια, δηλαδή λογιστικές εργασίες όπως η καταγραφή και η προετοιμασία των οικονομικών καταστάσεων, αλλά να δημιουργηθούν περισσότερες θέσεις εργασίας για τη διασφάλιση της αυθεντικότητας των αποδεικτικών στοιχείων και της λογικής των έξυπνων συμβολαίων. Συμπερασματικά, οι νέες συνθήκες που θα διαμορφωθούν στον τομέα της λογιστικής με την εισαγωγή του blockchain αποτελούν μία νέα πρόκληση για τους λογιστές.

Επιπλέον, εντοπίζεται και το πρόβλημα του απορρήτου των πληροφοριών, το οποίο προσεγγίζεται διαφορετικά ανάλογα με το χρονικό ορίζοντα. Ειδικότερα, βραχυπρόθεσμα επηρεάζει μόνο την ποσότητα των πληροφοριών που οι εταιρείες αποκαλύπτουν οικειοθελώς στο blockchain. Ωστόσο, μακροπρόθεσμα η ριζική αλλαγή της αυτοματοποίησης της δημιουργίας οικονομικών καταστάσεων θα αυξήσει σε μεγάλο βαθμό το κόστος για τις εταιρείες που κατέχουν αποκλειστικές ιδιόκτητες πληροφορίες, το οποίο πιθανότατα θα προκαλούσε εμπόδιο στην εφαρμογή της τεχνολογίας αλυσίδας συστοιχιών (Yu et al., 2018). Επιπλέον, όπως αναφέρουν και οι Wang και Kogan (2018) για την επιτυχή ανάπτυξη του blockchain σε συστήματα πληροφοριών επιχειρήσεων και την επίτευξη υψηλού επιπέδου αντοχής σε παραβίαση δεδομένων, απαιτείται μεγάλος αριθμός συμμετεχόντων που θα έχουν πρόσβαση στο πλήρες αντίγραφο κάθε συναλλαγής. Συνεπώς είναι απαραίτητο να βρεθεί μια αντιστάθμιση μεταξύ του οφέλους της ανταλλαγής πληροφοριών και του κόστους της αποδυνάμωσης της εμπιστευτικότητας.

Ένα άλλο ζήτημα που θα πρέπει να ληφθεί υπόψη είναι η θέσπιση ρυθμιστικού πλαισίου. Με την ποικιλομορφία και την ανωνυμία των κόμβων, οι κερδοσκόποι θα μπορούσαν να κάνουν χρήση του δικαιώματος εξόρυξης για να τοποθετήσουν ορισμένες πληροφορίες με σκοπό να αποκομίσουν πρόσκαιρο κέρδος. Ακόμη και στην περίπτωση που οι ψευδείς πληροφορίες ανακαλύπτονται άμεσα, είναι δύσκολο να αποκαλυφθεί ο κερδοσκόπος που τις δημοσίευσε. Επιπλέον, η μικρή αλλά υπαρκτή πιθανότητα της «επίθεσης 51%» αυξάνει τη δυσκολία θέσπισης κανόνων και ρυθμιστικού πλαισίου. Αν και είναι πολύ δύσκολο να πραγματοποιηθεί συγκέντρωση άνω του 51% της υπολογιστικής ισχύς του blockchain, συνεχίζει να

υπάρχει η πιθανότητα συνομωσίας μεταξύ των κόμβων. Οι ρυθμιστικές αρχές είναι αδύνατο να περιορίσουν αυτήν την ενέργεια εάν συμβεί (Yu et al., 2018)

Τέλος, συνδυαστικά και με τα παραπάνω ζητήματα, στην αρνητική πλευρά της νέας λογιστικής blockchain σημειώνεται ότι το επιχειρηματικό δίκτυο παραμένει ευάλωτο λόγω των κυβερνοεπιθέσεων. Το μέλλον και η περιουσία πολλών μεγάλων εταιρειών σε όλο τον κόσμο εξαρτάται πλέον από τις δυνατότητές τους να προστατεύονται από τέτοιες εξωτερικές απειλές. Οι περισσότερες από αυτές τις επιθέσεις επικεντρώνονται πάντα στην απόκτηση πρόσβασης στις προσωπικές πληροφορίες σχετικά με τις συναλλαγές και τους οικονομικούς πόρους που καταλαμβάνουν οποιεσδήποτε εταιρείες ή άτομα. Η απειλητική αυτή κατάσταση απαιτεί συνεργασία διεθνούς κλίμακας των εμπλεκόμενων επιχειρήσεων και μερών, να ενώσουν τις δυνάμεις τους και να μοιραστούν την τεχνογνωσία προς όφελος τους ώστε να καταστεί η λογιστική με την τεχνολογία αλυσίδας συστοιχιών πιο ασφαλής και προστατευμένη (Demirkan et al.,2020).

4.3.5. Τρόπος Αντιμετώπισης των Αδυναμιών και Μετάβαση από το Βραχυπρόθεσμο στο Μακροπρόθεσμο Σχέδιο Εφαρμογής

Όπως αναφέρθηκε παραπάνω, τα τεχνικά χαρακτηριστικά του blockchain καθιστούν τις πληροφορίες που αποκαλύπτονται εξαιρετικά διαφανείς, ανιχνεύσιμες και απαραβίαστες. Σύμφωνα με τους Yu et al. (2018) για τις εταιρείες που επιδιώκουν να μειώσουν την ασυμμετρία πληροφοριών με τους επενδυτές, η εθελοντική γνωστοποίηση μέσω του blockchain είναι ένας πολύ ελκυστικός τρόπος αντιμετώπισης της κατάστασης. Βραχυπρόθεσμα, οι εταιρείες μπορεί να αποκαλύψουν ορισμένες πολύτιμες αλλά όχι υποχρεωτικές πληροφορίες μέσω του blockchain, όπως προβλέψεις κερδών και εκθέσεις εταιρικής κοινωνικής ευθύνης. Αυτή η γνωστοποίηση βοηθά τους επενδυτές να κατανοήσουν καλύτερα την επιχείρηση και να λαμβάνουν πιο ενημερωμένες αποφάσεις.

Μακροπρόθεσμα, όταν οι εταιρείες και οι επενδυτές αναγνωρίζουν ότι η εθελοντική γνωστοποίηση στο blockchain είναι ένας μηχανισμός σηματοδότησης υψηλής ποιότητας πληροφοριών και αύξησης της εμπιστοσύνης, όλο και περισσότερες εταιρείες θα επιλέξουν να προβούν σε εθελοντική αποκάλυψη πληροφοριών στο blockchain αφού εξισορροπήσουν τα οφέλη και το κόστος. Καθώς περισσότερες πληροφορίες αποκαλύπτονται για το blockchain, η συγκρισιμότητα των πληροφοριών θα γίνει πρόβλημα. Οι ρυθμιστικές αρχές ενδέχεται να απαιτήσουν την τυποποίηση των πληροφοριών για τη βελτίωση της συγκρισιμότητας των πληροφοριών.

Προβλέποντας ότι η τεχνολογία blockchain θα μπορούσε να αυξήσει την αυθεντικότητα, την ακρίβεια και τη συγκρισιμότητα των πληροφοριών αποκάλυψης και να μειώσει τη διαχείριση κερδών των εταιρειών, οι ρυθμιστικές αρχές μπορούν ακόμη και να χρησιμοποιήσουν το blockchain ως κύρια πλατφόρμα για υποχρεωτική γνωστοποίηση πληροφοριών. Το περιεχόμενο της υποχρεωτικής γνωστοποίησης θα είναι τα αποδεικτικά έγγραφα των συναλλαγών και γεγονότων, καθώς και οι λογιστικές πολιτικές και μέθοδοι που ενσωματώνονται στα έξυπνα συμβόλαια. Αυτού του είδους οι πληροφορίες θα πρέπει να αποκαλύπτονται σε πραγματικό χρόνο. Άλλες μη εμπιστευτικές πληροφορίες, όπως προβλέψεις κερδών, εκθέσεις εταιρικής κοινωνικής ευθύνης και επιχειρηματικές αξιολογήσεις, που είναι περιεχόμενο που οι εταιρείες θα ήθελαν να αποκαλύψουν οικειοθελώς βραχυπρόθεσμα, θα πρέπει επίσης να γνωστοποιούνται στο blockchain. Ωστόσο, η συχνότητα γνωστοποίησης θα πρέπει να εξαρτάται από τη διακριτική ευχέρεια των εταιρειών. Εάν οι εταιρείες θέλουν να κάνουν καλή εντύπωση στην αγορά, θα έχουν το κίνητρο να αποκαλύψουν τις μη εμπιστευτικές πληροφορίες εγκαίρως.

Εκτός από την εθελοντική γνωστοποίηση σε βραχυπρόθεσμο ορίζοντα και την χρήση της πλατφόρμας blockchain για υποχρεωτική δημοσίευση πληροφοριών μακροπρόθεσμα, επισημαίνονται και τα εξής τα οποία μπορούν να δώσουν λύσεις σε ορισμένα προβλήματα που έχουν εντοπιστεί:

- Συνεργασία διεθνούς κλίμακας των εμπλεκόμενων επιχειρήσεων και οργανισμών του τομέα της λογιστικής ώστε να μοιραστούν την τεχνογνωσία

προς όφελος τους και να καταστήσουν τη λογιστική με την τεχνολογία αλυσίδας συστοιχιών πιο ασφαλή και προστατευμένη (Demirkan et al., 2020).

- Εφαρμογή της κατηγορίας blockchain που χαρακτηρίζεται ως permissioned αντί της εφαρμογής του public blockchain. Ειδικότερα, όπως έχει αναφερθεί, η βασική ιδέα του permissioned blockchain είναι ότι ένας κεντρικός οργανισμός ελέγχου έχει το δικαίωμα να διαβάζει ή/και να γράφει νέες πληροφορίες στο blockchain. Ωστόσο, σημειώνεται ότι μπορεί να λύσει εν μέρει το πρόβλημα του απορρήτου των πληροφοριών και την αυξανόμενη δυσκολία θέσπισης ρυθμιστικού πλαισίου, ωστόσο θα αποδυναμώσει τα θεμελιώδη χαρακτηριστικά της τεχνολογίας blockchain που είναι το ότι είναι αποκεντρωμένο και αμετάβλητο (Yu et al., 2018).
- Η αύξηση του βαθμού ωριμότητας της τεχνολογίας μέσω έρευνας και εφαρμογής σε ακαδημαϊκό και επιχειρηματικό επίπεδο αντίστοιχα, ώστε η τεχνολογία να εξελιχθεί, να πραγματοποιηθεί εξοικείωση και να καθοριστούν οι νέοι ρόλοι που πρέπει να αναλάβουν οι λογιστές και οι επιχειρήσεις ως σύνολο (Qasim, Kharbat, 2020).

Συμπερασματικά, σε σύγκριση με τις παραδοσιακές μεθόδους χρηματοοικονομικής αναφοράς, η χρήση της τεχνολογίας blockchain στη χρηματοοικονομική λογιστική έχει τα πλεονεκτήματα της υψηλής διαφάνειας, της ιχνηλασιμότητας, της επικαιρότητας και της ασφάλειας. Επιπλέον, τα έξυπνα συμβόλαια μπορούν να πραγματοποιήσουν την αυτοματοποίηση της δημιουργίας οικονομικών καταστάσεων, η οποία όχι μόνο μπορεί να μειώσει σημαντικά το κόστος της χρηματοοικονομικής λογιστικής, αλλά και να βελτιώσει την επικαιρότητα, την αξιοπιστία και τη συγκρισιμότητά των πληροφοριών. Επιπροσθέτως, μπορεί να μειώσει τα λάθη στη γνωστοποίηση και τη διαχείριση κερδών, έτσι ώστε οι οικονομικές καταστάσεις να αντικατοπτρίζουν πραγματικά και με ακρίβεια την οικονομική θέση, τα αποτελέσματα και τις επιδόσεις της εταιρείας. Αντίστοιχα, το πρόβλημα της ασυμμετρίας πληροφοριών μπορεί να μετριαστεί. Ωστόσο, λόγω των υφιστάμενων ελλείψεων της τεχνολογίας blockchain, τα παραπάνω πλεονεκτήματα χρειάζονται χρόνο για να γίνουν πραγματικότητα. Με την ωρίμανση της τεχνολογίας

blockchain, η λογιστική και η χρηματοοικονομική αναφορά μέσω του blockchain θα γίνουν μια βιώσιμη και ελκυστική επιλογή μακροπρόθεσμα.

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ ΠΕΡΙΟΡΙΣΜΟΙ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Ανακεφαλαιώνοντας, μετά την βιβλιογραφική επισκόπηση όπου αναφέρθηκαν συνοπτικά τα βασικότερα θέματα που αφορούν την τεχνολογία blockchain, πραγματοποιήθηκε μια ενδελεχής ανάλυση της τεχνολογίας επεξηγώντας την ορολογία και εστιάζοντας στις βασικές αρχές και στα ιδιαίτερα χαρακτηριστικά που προσδίδουν τα πλεονεκτήματά της και την καθιστούν ως μία από τις πιο επαναστατικές τεχνολογίες της σημερινής εποχής.

Η τεχνολογία blockchain θεωρείται μία περίπλοκη τεχνολογία η οποία συνδυάζει πολλές βασικές τεχνολογίες. Τα κύρια στοιχεία της τεχνολογίας αλυσίδας συστοιχιών είναι οι κρυπτογραφικές συναρτήσεις κατακερματισμού, η κρυπτογραφία ασύμμετρου κλειδιού, οι συναλλαγές, οι διευθύνσεις, το κατανεμημένο καθολικό, τα blocks και η σύνδεση μεταξύ τους. Ο αποκεντρωτικός χαρακτήρας, η αυθεντικότητα, η αμεταβλητότητα, η ανωνυμία, η δυνατότητα ελέγχου και εντοπισμού είναι τα χαρακτηριστικά που προσδίδουν τη μεγαλύτερη αξία στη τεχνολογία. Ωστόσο, η τεχνολογία παρουσιάζει και αδυναμίες οι σημαντικότερες εκ των οποίων είναι η δυνατότητα επέκτασης, η διαρροή δεδομένων, το selfish mining, η κατανάλωση ενέργειας, η έλλειψη διαλειτουργικότητας και ρυθμιστικού πλαισίου. Επιπλέον, σημειώνεται ότι ανάλογα με τη διαχείριση και τις άδειες του δικτύου, το blockchain ταξινομείται σε δημόσιο, ιδιωτικό και υβριδικό.

Στο τέταρτο κεφάλαιο γίνεται αρχικά μια περιγραφή της εξέλιξης του blockchain και των εφαρμογών του σε διάφορους τομείς. Η πρώτη φάση ανάπτυξης αναφέρεται κυρίως στα κρυπτονομίσματα, η δεύτερη φάση στα έξυπνα συμβόλαια και στη ψηφιοποίηση περιουσιακών στοιχείων και η τρίτη φάση αφορά τομείς εκτός των κρυπτονομισμάτων, της χρηματοδότησης και των αγορών, όπως τη διακυβέρνηση, την υγεία, την πληροφορική, τον πολιτισμό και την τέχνη. Αν και η ταχεία εξέλιξη της τεχνολογίας δεν επιτρέπει να υπάρχουν σαφή όρια στο blockchain

3.0, πλέον γίνεται λόγος για την εποχή της προγραμματιζόμενης κοινωνίας (programmable society) με το “blockchain of things”, όπου η ανθρώπινη ιδεολογία όσο και η κοινωνική μορφή θα επηρεαστούν. Ειδικότερα, η σύγχρονη βιομηχανία έχει εισέλθει σε μια νέα εποχή της τέταρτης βιομηχανικής επανάστασης και θεωρείται ότι μελλοντικά η τεχνολογία blockchain θα γίνει ένα ισχυρό εργαλείο της, καθώς θα συνδυαστεί και με άλλες τεχνολογίες της νέας γενιάς.

Στη συνέχεια το ενδιαφέρον επικεντρώνεται στον κλάδο της λογιστικής. Οι παραδοσιακές μέθοδοι και οι λογιστικές εργασίες όπως πραγματοποιούνται σήμερα μπορούν να μεταβληθούν με την είσοδο της τεχνολογίας blockchain στο γνωστικό αυτό πεδίο. Η λογιστική διπλής εγγραφής θα μετατραπεί σε λογιστική τριπλής εγγραφής, δηλαδή θα προστεθεί ένα τρίτο δημόσιο καθολικό που δίνει τη δυνατότητα στα δύο εμπλεκόμενα μέρη μίας συναλλαγής να εναρμονίσουν τα λογιστικά τους βιβλία. Επιπλέον, δύο βασικά σημεία της μακροπρόθεσμης εφαρμογής της λογιστικής blockchain είναι πρώτον ότι οι εταιρίες θα δημοσιεύουν τα έγγραφα από τα οποία αποδεικνύονται οι συναλλαγές και τα γεγονότα, δηλαδή τα έγγραφα από τα οποία προκύπτουν οι οικονομικές καταστάσεις και δεύτερον θα ενσωματώνουν σε έξυπνα συμβόλαια τις λογιστικές πολιτικές και μεθόδους τις οποίες ακολουθούν κατά τη δημιουργία των οικονομικών καταστάσεων. Επιπροσθέτως, επισημαίνεται ότι ως κόμβοι του blockchain θα μπορούν να συμμετέχουν στο mining, να καταγράφουν, να επικυρώνουν αμέσως τις πληροφορίες που υποβάλλονται από την εταιρεία σε ένα νέο block και να τις αναμεταδίδουν στο δίκτυο του blockchain θεσμικοί επενδυτές, ελεγκτές, δικηγόροι, ρυθμιστικές αρχές και χρηματιστήρια.

Συμπερασματικά, όλα τα παραπάνω αποδεικνύουν ότι η μακροπρόθεσμη εφαρμογή της τεχνολογίας blockchain στη λογιστική θα έχει τεράστιο θετικό αντίκτυπο, καθώς οι πληροφορίες καταγράφονται και επικυρώνονται με αποκεντρωμένο τρόπο, αυξάνεται η διαφάνεια, η ασφάλεια, η αξιοπιστία μέσω της τεχνολογίας κατανεμημένου καθολικού, της συνάρτησης hash και του μηχανισμού συναίνεσης, βελτιώνεται η επικαιρότητα, η χρησιμότητα και η ορθότητα των οικονομικών καταστάσεων αλλά και το πρόβλημα της ασύμμετρης πληροφόρησης.

Ωστόσο, βραχυπρόθεσμα λόγω του χαμηλού επιπέδου ωριμότητας της τεχνολογίας και των περιορισμών όπως η μειωμένη ικανότητα επεξεργασίας δεδομένων, η εμπιστευτικότητα των πληροφοριών και η έλλειψη ρυθμιστικού πλαισίου είναι φανερό ότι δεν είναι ρεαλιστικός ο στόχος της άμεσης εφαρμογής της τεχνολογίας. Στο σημείο αυτό, σημαντικό είναι να σημειωθεί ότι παρά τα πολλά πλεονεκτήματα που προσφέρει το blockchain, δεν έχει τη δυνατότητα να εξαλείψει πλήρως τη πιθανότητα σφαλμάτων και απατών. Επιπροσθέτως, η μακροπρόθεσμη εφαρμογή της τεχνολογίας blockchain δεν θα έχει μόνο θετικές επιπτώσεις αλλά θα επιφέρει και ορισμένες προκλήσεις που θα πρέπει να αντιμετωπιστούν, όπως η ανακατεύθυνση του ρόλου του λογιστή, το πρόβλημα με τις απόρρητες και αποκλειστικές πληροφορίες που μπορεί να διαθέτει κάποια εταιρεία, η θέσπιση του ρυθμιστικού πλαισίου και οι πιθανές κυβερνοεπιθέσεις.

Η αντιμετώπιση των ζητημάτων που αναφέρθηκαν σχετικά με τη βραχυπρόθεσμη εφαρμογή προτείνεται να επιτευχθεί με τη συνεργασία διεθνούς κλίμακας επιχειρήσεων και οργανισμών για τη διάχυση τεχνογνωσίας, την εφαρμογή του permissioned blockchain και γενικότερα την έρευνα για την αύξηση του βαθμού ωριμότητας. Μακροπρόθεσμα, συνίσταται αρχικά η εθελοντική γνωστοποίηση πληροφοριών για την εδραίωση εμπιστοσύνης και ποιοτικότερης πληροφόρησης και σε δεύτερο χρόνο η υποχρεωτική γνωστοποίηση πληροφοριών μετά τη θέσπιση του κατάλληλου ρυθμιστικού πλαισίου.

Κλείνοντας, στις προτάσεις για μελλοντική έρευνα της παρούσας εργασίας περιλαμβάνεται η ανάλυση του τρίτου σταδίου εξέλιξης της τεχνολογίας blockchain (blockchain 3.0) και των διαστάσεων που θα λάβει στο μέλλον. Επιπλέον, μία άλλη πρόταση είναι να ερευνηθεί η λογιστική βασισμένη στο blockchain μέσω κάποιας πειραματικής εφαρμογής, όπως επίσης και η επίδραση που μπορεί να έχει το blockchain σε άλλα γνωστικά πεδία της λογιστικής όπως η ελεγκτική ή η διοικητική λογιστική.

Βιβλιογραφία

Ελληνική

Νεγκάκης, Χ. και Ταχυνάκης, Π. (2017), Ελεγκτική Εσωτερικός Έλεγχος, Θεωρία και Εφαρμογές, Εκδόσεις Αειφόρος Λογιστική.

Νεγκάκης, Χ. (2015), Διεθνή Πρότυπα Χρηματοοικονομικής Αναφοράς, Θεωρία και Εφαρμογές, Εκδόσεις Αειφόρος Λογιστική.

Ξένη

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018), "Applications of blockchains in the Internet of Things: A comprehensive survey", *IEEE Communications Surveys & Tutorials*, Vol. 21, No 2, pp. 1676-1717.

Ali, O., Ally, M., & Dwivedi, Y. (2020), "The state of play of blockchain technology in the financial services sector: A systematic literature review", *International Journal of Information Management*, Vol. 54, pp. 102199.

Biswas, B., Gupta, R. (2019), "Analysis of barriers to implement blockchain in industry and service sectors", *Computers & Industrial Engineering*, Vol. 136, pp. 225-241.

Baiod, W., Light, J., & Mahanti, A. (2021), "Blockchain Technology and its Applications Across Multiple Domains: A Survey", *Journal of International Technology and Information Management*, Vol. 29, Iss. 4, Article 4, pp. 78-119.

Barcelo, J. (2014), "User privacy in the public bitcoin blockchain".

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014), "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y." *ACM SIGMETRICS Performance Evaluation Review*, Vol. 42, No 3, pp. 34-37.

Biryukov, A., Khovratovich, D. and Pustogarov, I. (2014) "Deanonymisation of clients in bitcoin p2p network", *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp.15–29.

Byström, H. (2019). Blockchains, real-time accounting, and the future of credit risk modeling. Ledger, 4.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019), “A systematic literature review of blockchain-based applications: Current status, classification and open issues”, *Telematics and informatics*, Vol. 36, pp. 55-81.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. (2016), “Blockchain technology: beyond bitcoin”, *Applied Innovation*, No 2, pp. 6–10.

Dai, J., & Vasarhelyi, M. A. (2017), “Toward blockchain-based accounting and assurance”, *Journal of Information Systems*, Vol. 31, No 3, pp. 5–21.

Demirkan, S., Demirkan, I., & McKee, A. (2020), “Blockchain technology in the future of business cyber security and accounting”, *Journal of Management Analytics*, Vol. 7, No 2, pp. 189-208.

Eyal, I., Gencer, A.E., Sirer, E.G., Van Renesse, R. (2016), “Bitcoin-ng: a scalable blockchain protocol”, *Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pp.45–59.

Eyal, I. and Sirer, E.G. (2014), “Majority is not enough: Bitcoin mining is vulnerable”, *Proceedings of International Conference on Financial Cryptography and Data Security*, pp.436–454

Faccia, A., Mosteanu, N. R. (2019), “Accounting and blockchain technology: from double-entry to triple-entry”, *The Business & Management Review*, Vol. 10, No 2, pp. 108-116.

Gupta, M. (2018), “Blockchain for Dummies", IBM Limited Edition, p. 51.

Kakavand, H., Kost De Sevres, N., Chilton, B. (2017), “The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies”, *SSRN Electronic Journal.*

Khandelwal, S. (2019), “Blockchain Technology: Heart of digital financial infrastructure for managing trust and governance system”, *In Proceedings of 10th International Conference on Digital Strategies for Organizational Success*.

Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C. (2016), “Hawk: the blockchain model of cryptography and privacy-preserving smart contracts”, *Proceedings of IEEE Symposium on Security and Privacy (SP),* pp.839–858.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. Savage, S. (2013), “A fistful of bitcoins: Characterizing payments among men with no names”, *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC’13)*.

Melnychenko O., Hartinger R. (2017), “Role of Blockchain Technology in Accounting and Auditing”, *European Cooperation*, Vol. 9(28), pp. 27-34

Monrat, A. A., Schelén, O., & Andersson, K. (2019), “A survey of blockchain from the perspectives of applications, challenges, and opportunities”, *IEEE Access*, Vol. 7, pp. 117134-117151.

Nakamoto, S. (2008), “Bitcoin: A peer-to-peer electronic cash system”, *Decentralized Business Review*, 21260.

Nordgren, A. I. N. O., Weckström, E. L. L. E. N., Martikainen, M. I. N. N. A., & Lehner, O. M. (2019), “Blockchain in the fields of finance and accounting: a disruptive technology or an overhyped phenomenon”, *ACRN Oxford Journal of Finance and Risk Perspectives*, Vol. 8, No 1, pp. 47-58.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020), “A survey on the security of blockchain systems”, *Future Generation Computer Systems*, Vol. 107, pp. 841-853

Lu, Y. (2018), “Blockchain and the related issues: A review of current research topics”, *Journal of Management Analytics*, Vol. 5, No 4, pp. 231-255.

Lu, Y. (2019), “The blockchain: State-of-the-art and research challenges”, *Journal of Industrial Information Integration*, Vol. 15, pp. 80-90.

Qasim, A., Kharbat, F. F. (2020), “Blockchain technology, business data analytics, and artificial intelligence: Use in the accounting profession and ideas for inclusion into the accounting curriculum. Journal of emerging technologies in accounting”, Vol. 17, No 1, pp. 107-117.

Seebacher, S., Schüritz, R. (2017), “Blockchain technology as an enabler of service systems: A structured literature review”, *In International Conference on Exploring Services Science,* pp. 12-23.

Sikorski, J. J., Haughton, J., Kraft, M. (2017), “Blockchain technology in the chemical industry: Machine-to-machine electricity market”, *Applied energy*, Vol. 195, pp. 234-246.

Swan, M. (2015), “Blockchain: Blueprint for a new economy”, O'Reilly Media, Inc.

Viriyasitavat, W., Hoonsopon, D. (2019), “Blockchain characteristics and consensus in modern business processes”, *Journal of Industrial Information Integration*, Vol. 13, pp. 32-39.

Wang, Y., Kogan, A. (2018), “Designing confidentiality-preserving Blockchain-based transaction processing systems”, *International Journal of Accounting Information Systems*, Vol. 30, pp. 1-18.

Watts, R. L., Zimmerman, J. L. (1983), “Agency problems, auditing, and the theory of the firm: Some evidence”, *Journal of Law and Economics*, Vol. 26, No 3, pp. 613–633.

Waymire, G. B., Basu, S. (2008), “Accounting is an evolved economic institution”, *Foundations and Trends in Accounting*, Vol. 2, No 1–2, pp. 1–174.

Wood, G. (2014), “Ethereum: A secure decentralised generalised transaction ledger”, Ethereum project yellow paper, pp. 1-32.

Xu, L. D., Xu, E. L., Li, L. (2018), “Industry 4.0: state of the art and future trends”, *International journal of production research*, Vol. 56, No 8, pp. 2941-2962.

Yaga, D., Mell, P., Roby, N., Scarfone, K. (2019), “Blockchain technology overview”, *National Institute of Standards and Technology*

Yeoh, P. (2017), “Regulatory issues in blockchain technology”, *Journal of Financial Regulation and Compliance.*

Yermack, D. (2017), “*Corporate governance and blockchains*”, *Review of Finance*, Vol. 21, No 1, pp. 7–31.

Yu, T., Lin, Z., Tang, Q. (2018), “Blockchain: the introduction and its application in financial accounting”, *Journal of Corporate Accounting & Finance*, Vol. 29, No 4, pp. 37-47.

Zamfir, V. (2015), “Introducing casper the friendly ghost”, *Ethereum Blog*.

Zhang, K., & Jacobsen, H. A. (2018), “Towards dependable, scalable, and pervasive distributed ledgers with blockchains (Technical Report)”

Zheng, Z., Xie, S., Dai, H. N., Chen, X., Wang, H. (2018), “Blockchain challenges and opportunities: A survey”, *International Journal of Web and Grid Services*, Vol. 14, No 4, pp. 352-375.

Διαδικτυακές Πηγές

www.blockchain.com

www.coindesk.com

https://blog.ethereum.org/