ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

ΠΛΗΡΟΦΟΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

Διπλωματική Εργασία

Η επίδραση του Blockchain στην εξέλιξη των ελεγκτικών διαδικασιών

ΚΑΛΑΪΤΖΑΚΗ ΖΩΗ

ΑΘΗΝΑ, ΙΟΥΛΙΟΣ 2020

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

ΠΛΗΡΟΦΟΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τριμελής Εξεταστική Επιτροπή

ΕΠΙΒΛΕΠΩΝ ΜΙΧΑΛΑΚΕΛΗΣ ΧΡΗΣΤΟΣ

ΚΑΜΑΛΑΚΗΣ ΘΩΜΑΣ

ΔΕΔΕ ΓΕΩΡΓΙΑ

Η ΚΑΛΑΪΤΖΑΚΗ ΖΩΗ

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

Πίνακας Περιεχομένων

Περίληψη

Η παρούσα εργασία θα εξετάσει την επίδραση του Blockchain στην εξέλιξη των ελεγκτικών διαδικασιών, όπως και στις διαδρομές ελέγχου. Προς επίτευξη του σκοπού της, η εργασία θα εξετάσει την έννοια της διαδρομής ελέγχου (“Audit Trail”), την βιβλιογραφία της τεχνολογίας του Blockchain και των εφαρμογών της, συμπεριλαμβανομένων των «έξυπνων συμβολαίων», και το πως εφαρμόζεται στους ελέγχους και σε διάφορες περιπτώσεις όπως είναι τα ιδιωτικά και δημόσια Blockchain, το Data Hashing, η κρυπτογράφηση δεδομένων, κ.α. Έπειτα, θα συγκρίνει τα πλαίσια των τεχνολογιών BlockChain “Hyperledger Sawtooth”, “Hyperledger Fabric”, και “Quorum”, πριν εξετάσει το πόσο χρήσιμα είναι τα έξυπνα συμβόλαια blockchain στους ελέγχους. Τέλος, η εργασία εξάγει συμπεράσματα.

Λέξεις-Κλειδιά: Blockchain, ελεγκτική διαδικασία, Audit Trail, Hyperledger Sawtooth, Hyperledger Fabric, Quorum, έξυπνα συμβόλαια

Abstract

This paper will examine the effect of Blockchain on the development of audit processes, as well as on control pathways. In order to achieve its goal, the work will examine the concept of Audit Trail, the Blockchain technology literature and its applications, including "smart contracts" and how to implement controls and in various cases such as private and public Blockchain, Hashing data, data encryption, etc. Next, we'll compare BlockChain's "Hyperledger Sawtooth", "Hyperledger Fabric" and "Quorum" technologies before we look at how useful smart blockchain contracts are in auditing. Finally, the work draws conclusions.

Keywords: Blockchain, Audit, Audit Trail, Hyperledger Sawtooth, Hyperledger Fabric, Quorum, Smart Contracts

1 Εισαγωγή

Το Συμβούλιο Λογιστικής Εποπτείας της Δημόσιας Εταιρείας (“Public Company Accounting Oversight Board” – εφεξής PCAOB) αναζητά συνεχώς τρόπους βελτίωσης της αποτελεσματικότητας του ελέγχου και της ποιότητας του ελέγχου. Η πιο δαπανηρή δραστηριότητα στη διαδικασία ελέγχου είναι η απόκτηση και επαλήθευση πληροφοριών. Οι ελεγκτές πρέπει να ενημερώνονται σχετικά με τις συναλλαγές πελατών ή με εκείνες των συνεργατών τους για την επαλήθευση των ποσών των συναλλαγών. Ενώ κάθε ελεγκτικό γραφείο ή ομάδα ελέγχου (επίσης γενικά αναφέρεται ως "ελεγκτής") διαθέτει χρήσιμες πληροφορίες που μπορούν να μειώσουν σημαντικά το κόστος των άλλων ελεγκτών για την απόκτηση πληροφοριών, η διαδικασία ελέγχου είναι παραδοσιακά ανεξάρτητη από άλλες ελεγκτικές εταιρείες, διότι δεν συνηθίζεται να μοιράζονται ιδιοκτησιακά πληροφοριών μεταξύ των ελεγκτικών γραφείων. Ως αποτέλεσμα, είναι δύσκολο να βρούμε έναν αξιόπιστο τρίτο για να διευκολύνουμε τις έγκαιρες και ασφαλείς επικοινωνίες, για να μην αναφέρουμε την απροθυμία των πελατών να αποκαλύψουν πληροφορίες σε άλλους ελεγκτές και τους νόμους που αφορούν την ιδιωτική ζωή των δεδομένων, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (“General Data Protection Regulation” - GDPR).

Εν τω μεταξύ, η τεχνολογία blockchain έχει αναλάβει την κεντρική φάση της τεχνολογικής καινοτομίας στις επιχειρήσεις και θεωρείται ευρέως ότι διαταράσσει τις παραδοσιακές πρακτικές στον τομέα της εταιρικής διακυβέρνησης, της βιομηχανικής οργάνωσης, των πληρωμών και της επιχειρηματικής χρηματοδότησης (Appelbaum et al, 2017). Μεταξύ των διαφόρων προόδων, "μια θεωρητική εφαρμογή του blockchain είναι στην οικονομική πληροφόρηση και αυτό είναι ακριβώς το χρονικό σημείο για να συζητήσουμε τα πλεονεκτήματα και τα μειονεκτήματα" (Alles et al, 2006). Σύμφωνα με αυτή την άποψη, υπάρχει αυξημένη προσοχή των μέσων μαζικής ενημέρωσης και της βιομηχανίας σχετικά με το ρόλο των μπλοκ αλυσίδων στον κόσμο του ελέγχου. Παρόλο που όλες οι μεγάλες ελεγκτικές εταιρείες αφιερώνουν μεγάλους πόρους για να μπλοκάρουν την ανάπτυξη, δημιουργώντας ερευνητικά εργαστήρια ή παρέχοντας υπηρεσίες αποκλεισμού (Brafman & Beckstrom, 2006), δεν είναι ακόμη σαφές με ποιο τρόπο τα μπλοκ μπορούν να επηρεάσουν τον ελεγκτικό κλάδο και τον νέο ρόλο των ελεγκτών στην αναδυόμενη τεχνολογία. (Dai & Vasarheli, 2017).

1.1 Σκοπός και Δομή της Εργασίας

Η παρούσα εργασία θα εξετάσει την επίδραση του Blockchain στην εξέλιξη των ελεγκτικών διαδικασιών, όπως και στις διαδρομές ελέγχου. Προς επίτευξη του σκοπού της, η εργασία θα εξετάσει την έννοια της διαδρομής ελέγχου (“Audit Trail”), την βιβλιογραφία της τεχνολογίας του Blockchain και των εφαρμογών της, συμπεριλαμβανομένων των «έξυπνων συμβολαίων», και το πως εφαρμόζεται στους ελέγχους και σε διάφορες περιπτώσεις όπως είναι τα ιδιωτικά και δημόσια Blockchain, το Data Hashing, η κρυπτογράφηση δεδομένων, κ.α. Έπειτα, θα συγκρίνει τα πλαίσια των τεχνολογιών BlockChain “Hyperledger Sawtooth”, “Hyperledger Fabric”, και “Quorum”, πριν εξετάσει το πόσο χρήσιμα είναι τα έξυπνα συμβόλαια blockchain στους ελέγχους. Τέλος, η εργασία θα εξάγει συμπεράσματα.

2 Βιβλιογραφική Ανασκόπηση

2.1 Εννοιολογική Τοποθέτηση «Audit Trail»

Υπάρχουν πολλοί τομείς επιχειρηματικής δραστηριότητας που αξίζουν τον επιμελή έλεγχο και επαλήθευση από ένα αντικειμενικό άτομο ή οργανισμό εκτός του ίδιου του οργανισμού. Ορισμένες από αυτές μπορούν να αναληφθούν οικειοθελώς από την επιχείρηση, άλλες όπως ο έλεγχος των χρηματοπιστωτικών συστημάτων και τα αποτελέσματα είναι υποχρεωτικά. Ο καθαρός έλεγχος του cloud computing είναι ένα νέο, ανώριμο πεδίο και θα ήταν περίεργο αν δεν υπήρχαν μαθήματα που να μαθαίνουν από τις εμπειρίες και τις αποτυχίες των διαδικασιών ελέγχου και των πρακτικών που έχουν εξαντληθεί εδώ και δεκαετίες, αν όχι αιώνες. Κάθε φορά που αναδύεται ένας νέος τεχνικός χώρος, θα είναι δύσκολο να βρεθούν άτομα με τα κατάλληλα προσόντα - μια τεχνική γνώση της περιοχής και η ικανότητα να διενεργηθεί ένας έλεγχος. Ως εμπορικοί οργανισμοί, τα ελεγκτικά γραφεία ενδέχεται να επιδιώξουν να επεκτείνουν την ελεγκτική τους αρμοδιότητα σε νέους τεχνικούς τομείς, όχι μόνο τον έλεγχο του cloud, αλλά ίσως και τον περιβαλλοντικό έλεγχο ως άλλο παράδειγμα. Πάνω από έναν αιώνα εμπειρίας στην ανάπτυξη εργαλείων και πρακτικών ελέγχου πρέπει να εφαρμοστεί σε ένα νέο τεχνικό τομέα. Εναλλακτικά, οι ειδικοί υπολογιστών ενδέχεται να πάρουν ένα σύνολο δεξιοτήτων ελέγχου. Ένα λογικό αποτέλεσμα θα ήταν οι ελεγκτικές εταιρείες να προσλάβουν εμπειρογνώμονες του cloud computing και να επιδιώξουν να εναρμονίσουν τις δεξιότητές τους με εκείνες του ελέγχου που έχουν ήδη ενσωματωθεί στην επιχείρηση. Η σύγκρουση πολιτισμού μεταξύ λογιστών και εμπειρογνωμόνων σύννεφο θα ήταν μια πιθανή παρενέργεια από μια τέτοια στρατηγική (Appelbaum et al, 2017).

Ένα εργαλείο που έχουν χρησιμοποιήσει οι λογιστές εδώ και δεκαετίες είναι η διαδρομή ελέγχου και αυτή είναι μια φράση που υπάρχει ήδη στη βιβλιογραφία του cloud computing από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (“National Institute of Standards and Technology” - NIST), για παράδειγμα. Ωστόσο, η ίδια φράση μπορεί να μην έχει το ίδιο νόημα και στις δύο ρυθμίσεις. Αναφερόμενο από το λεξικό της Οξφόρδης (“Oxford English Dictionary” - OED): “α) Λογιστική: μέσο επαλήθευσης των λεπτομερών συναλλαγών στις οποίες βασίζεται οποιοδήποτε στοιχείο σε λογιστική εγγραφή. β) Πληροφορική: αρχείο των υπολογιστικών διαδικασιών που έχουν εφαρμοστεί σε ένα συγκεκριμένο σύνολο δεδομένων πηγής, που δείχνει κάθε στάδιο επεξεργασίας και επιτρέπει την ανασύσταση των αρχικών δεδομένων. ένα αρχείο των συναλλαγών στις οποίες έχει υποβληθεί μια βάση δεδομένων ή ένα αρχείο”. Έτσι, η διαφορά του ορισμού αναγνωρίζεται από τον OED (Power, 2019).

Οι λογιστές είναι μέλη επαγγελματικών φορέων (ορισμένων εθνικών, μερικών παγκόσμιων) που περιορίζουν την ιδιότητα μέλους σε όσους έχουν περάσει τις εξετάσεις και έχουν επιτύχει επαρκές εύρος και διάρκεια εμπειρίας που θεωρούνται άξια να εκπροσωπούν το επάγγελμα. Ο έλεγχος αποτελεί βασικό χαρακτηριστικό αυτών των αναλυτικών εξετάσεων και η επιστροφή στην πηγή κάθε λογιστική δραστηριότητα (το ίχνος) αποτελεί βασική πτυχή του ελέγχου. Ενώ το NIST έδωσε σαφή εξήγηση για ένα ίχνος ελέγχου σε ένα περιβάλλον ασφάλειας υπολογιστών και σύμφωνα με τον ορισμό του OED (β), η χρήση του όρου στην έρευνα στον έλεγχο cloud φαίνεται λιγότερο ακριβής και συνεπής. Για παράδειγμα, ο Bernstein, βλέπει το ίχνος που περιλαμβάνει: τα γεγονότα, τα ημερολόγια και την ανάλυση αυτών, ενώ ο Chaula δίνει έναν πιο μακροπρόθεσμο, λεπτομερέστερο κατάλογο: πρωτογενή δεδομένα, σημειώσεις ανάλυσης, σημειώσεις και ούτω καθεξής. Πράγματι, οι Pearson και Benameuer αποδέχονται ότι η επίτευξη συνεπών, ουσιαστικών διαδρομών ελέγχου στο σύννεφο είναι ένας στόχος παρά μια πραγματικότητα. Περισσότερο ανησυχητικά οι Ko et al., επισημαίνουν ότι είναι πολύ πιθανό να διαγραφεί ένα ίχνος ελέγχου μαζί με ένα παράδειγμα cloud, πράγμα που σημαίνει ότι δεν υπάρχει κανένα αρχείο για να εντοπιστούν, να κατανοηθούν και να κρατηθούν οι χρήστες να λογοδοτούν για τις ενέργειές τους και τις απαιτήσεις για λογοδοσία. Πράγματι, η ομάδα εργασίας της ΕΕ του άρθρου 29 υπογραμμίζει τις φτωχές διαδικασίες παρακολούθησης των ελέγχων ως ένα από τα ζητήματα ασφάλειας που καλύπτονται ανεπαρκώς από τις υπάρχουσες αρχές (στο Duncan et al, 2017).

Παρόλο που το ίχνος ελέγχου φαίνεται να είναι μια μακρά και κουραστική λίστα δραστηριοτήτων και παρεμβάσεων, μπορεί να έχει τεράστια αξία η καταδίωξη της ρίζας μιας επιθέσεις στον κυβερνοχώρο, με τον ίδιο τρόπο που ένας λογιστής μπορεί να το χρησιμοποιήσει για να εντοπίσει τα βήματα και τα άτομα συμμετέχει στη διευκόλυνση μιας ακατάλληλης πληρωμής. Από τη ρίζα της, η έννοια πρέπει να εφαρμοστεί με τέτοιο τρόπο ώστε να επιτρέψει ακόμη και την ανασυγκρότηση ενός συστήματος εάν είχε διαγραφεί εντελώς, και όχι μόνο να εντοπιστεί μια διαταραγμένη ενιαία συναλλαγή. Η διαδρομή ελέγχου μπορεί να είναι επικάλυψη, αλλά είναι αναγκαία δεδομένου του κινδύνου χειραγώγησης, συμβιβασμού ή απώλειας. Οι συζητήσεις μας με επαγγελματίες τεχνολογιών πληροφορικής, οι οποίοι επιβεβαίωσαν την εμπιστοσύνη τους στη δημιουργία αντιγράφων ασφαλείας δεδομένων, δείχνουν ένα επίπεδο αμείωτης εμπιστοσύνης, καθώς μια ακατάλληλη παρέμβαση θα επαναληφθεί σε κάθε αντίγραφο ασφαλείας μέχρι να ανακαλυφθεί. Τα εφεδρικά αντίγραφα ενός κατεστραμμένου συστήματος δεν θα επιτύχουν την ανοικοδόμηση σε ένα άκαμπτο - το

ίχνος ελέγχου δίνει αυτή την ευκαιρία. Αναφερόμενοι πίσω στους Ko et al., ο καθορισμός ενός άριστου διαγράμματος ελέγχου είναι άχρηστο εάν πρόκειται να διαγραφεί μόνο μαζί με ένα παράδειγμα cloud. Η δημιουργία επαρκούς διαδρομής ελέγχου συχνά πρέπει να είναι σαφής, καθώς το λογισμικό συχνά επιτρέπει την απενεργοποίηση των διαδρομών ελέγχου στις ρυθμίσεις του (Duncan & Whittington, 2016).

Μόλις δημιουργηθεί ένα ίχνος ελέγχου, το περιεχόμενο πρέπει να προστατεύεται από οποιαδήποτε προσαρμογή. Όπως τονίζει ο Anderson, ακόμη και οι διαχειριστές του συστήματος δεν πρέπει να έχουν την εξουσία να το τροποποιούν. Δεν είναι μόνο αυτή η καλή πρακτική ακόμη και με καλά εκπαιδευμένα και ηθικά άτομα, αλλά είναι πάντα πιθανό ότι ένας χάκερ μπορεί να είναι σε θέση να επιτύχει καθεστώς διαχειριστή. Επομένως, το μονοπάτι ελέγχου απαιτεί τη δημιουργία μιας αμετάβλητης βάσης δεδομένων (δηλ. μιας που καταγράφει μόνο νέες δραστηριότητες αλλά ποτέ δεν επιτρέπει προσαρμογή προηγούμενων). Αυτός είναι ο πρωταρχικός στόχος αυτής της πρώτης δοκιμής για την επιτυχή ανάπτυξη ενός συστήματος για τη διατήρηση τόσο της διαδρομής ελέγχου όσο και των ημερολογίων συστήματος (Duncan & Whittington, 2016).

2.2 Η Τεχνολογία BlockChain

Η έννοια του blockchain μπορεί να οριστεί ως «κοινόχρηστος κατανεμημένος λογαριασμός που διευκολύνει τη διαδικασία καταγραφής συναλλαγών και παρακολούθησης περιουσιακών στοιχείων σε ένα επιχειρηματικό δίκτυο. Ένα περιουσιακό στοιχείο μπορεί να είναι απτό - ένα σπίτι, ένα αυτοκίνητο, μετρητά, γη - ή άυλα όπως πνευματική ιδιοκτησία, όπως διπλώματα ευρεσιτεχνίας, πνευματικά δικαιώματα ή επωνυμία.». Αυτή η πληροφορία του ημερολογίου λειτουργεί με κρυπτογραφημένα δεδομένα για την εφαρμογή ταυτοποίησης, πιστοποίησης ταυτότητας και εξουσιοδότησης πρόσβασης σε πληροφορίες. Η ακεραιότητα και η εμπιστοσύνη στα δεδομένα, τα οποία βρίσκονται στα πληροφοριακά συστήματα, είναι ο κύριος στόχος της τεχνολογίας blockchain. Το Blockchain είναι ένα τεχνολογικό εργαλείο για τη συμμόρφωση με την ακεραιότητα των δεδομένων, από την άποψη της πληρότητας, της ορθότητας και της απουσίας αντιφάσεων, στα κατανεμημένα συστήματα λογισμικού. Τα κατανεμημένα συστήματα λογισμικού είναι ένας αριθμός ανεξάρτητων υπολογιστών που συνεργάζονται μεταξύ τους σε πολλές ενημερωτικές συναλλαγές, χωρίς να διαθέτουν κεντρικό υπολογιστή για τον έλεγχο ή την παρακολούθηση αυτών των συναλλαγών. Σε ένα κεντρικό σύστημα, μόνο ένας υπολογιστής μπορεί να ελέγξει όλες τις πληροφορίες που συνέβησαν σε ένα συγκεκριμένο περιβάλλον ή δίκτυο. Στην καθημερινή μας οικονομία, γνωρίζουμε ότι οι συναλλαγές δεν πρέπει

να είναι μόνο σε έναν υπολογιστή για την πρόληψη της απάτης, αλλά μάλλον σε πολλούς υπολογιστές (IBM, 2017).

Για το λόγο αυτό, οι εταιρείες χρησιμοποιούν αποκεντρωμένα συστήματα πληροφοριών. Στο πλαίσιο αυτού του αποκεντρωμένου συστήματος, η κατοχή των πληροφοριών πρέπει να επικυρώνεται, η απόδειξη ιδιοκτησίας έχει τρία στοιχεία: (1) τον προσδιορισμό του ιδιοκτήτη, (2) τον προσδιορισμό του αντικειμένου που ανήκει και (3) την αντιστοίχιση του ιδιοκτήτη με το αντίστοιχο αντικείμενο . Αυτό το αντικείμενο και η χαρτογράφηση στον ιδιοκτήτη του διατηρείται σε ένα ημερολόγιο, που αντιστοιχεί σε απόδειξη ιδιοκτησίας. Το επόμενο σχήμα απεικονίζει τις έννοιες ιδιοκτησίας που χρησιμοποιούνται για την πιστοποίηση και την απόδειξη ιδιοκτησίας (Mainelli & Smith, 2015).

Η πρόσβαση ιδιοκτήτη πληροφοριών διατηρείται μέσω της χρήσης ασύμμετρης κρυπτογραφίας κατά τη διάρκεια της συναλλαγής δεδομένων. Σε αυτή τη διαδικασία, τα δεδομένα προστατεύονται από την πρόσβαση από μη εξουσιοδοτημένα άτομα. Η ασύμμετρη κρυπτογραφία αποτελείται από δύο συμπληρωματικά κλειδιά (ιδιωτικό κλειδί & δημόσιο κλειδί). Το ιδιωτικό κλειδί προστατεύει τα δεδομένα με κιειφόρο κείμενο, μια λειτουργία που μετατρέπει οποιοδήποτε είδος δεδομένων σε ένα ορισμένο μήκος (hash), αυτή η διαδικασία ονομάζεται κρυπτογράφηση. Το δημόσιο κλειδί επιστρέφει το κείμενο σε μορφή cyphered σε χρήσιμα δεδομένα, αυτό το μέρος της διαδικασίας ονομάζεται αποκρυπτογράφηση. Σε κάθε μία από αυτές τις διαδικασίες, και για κάθε μία από αυτές, το blockchain παράγει ένα hash, έτσι ώστε τα δεδομένα να συνδέονται με τα παραγόμενα hashes που συνδέουν κάθε κομμάτι δεδομένων με ένα άλλο κομμάτι δεδομένων, μια αλυσίδα. Το Blockchain χρησιμοποιεί ασύμμετρη κρυπτογράφηση για τον εντοπισμό λογαριασμών (λογαριασμοί χρηστών που αντιστοιχούν στο δημόσιο κρυπτογραφικό κλειδί) και για την εξουσιοδότηση συναλλαγών. Όλες αυτές οι συναλλαγές κρατούνται (Yermack, 2017).

Το Blockchain σημαίνει διαφορετικά πράγματα σε διαφορετικούς ανθρώπους του υπόβαθρου. Για ορισμένους συγγραφείς το blockchain ορίζεται ως μια δομή δεδομένων, για τους άλλους είναι ένας αλγόριθμος, για τους άλλους μπορεί να οριστεί ως μια σουίτα τεχνολογίας, και ακόμη και για άλλους blockchain μπορεί να είναι μια ομάδα συστημάτων που μεταδίδουν peer-to-peer μέσα σε μια κοινή εφαρμογή περιοχή. Ο Drescher ορίζει το blockchain ως κατανεμημένο λογιστικό σύστημα, το οποίο χρησιμοποιεί έναν αλγόριθμο για να επικοινωνούν οι υπολογιστές μεταξύ τους με τεχνολογίες κρυπτογράφησης και ασφάλειας για την επίτευξη και διατήρηση της ακεραιότητας των δεδομένων (Deloitte, 2017).

2.2.1 Smart Contracts

Η πρόσφατη ανάπτυξη της τεχνολογίας blockchain έχει αναβιώσει την έννοια και διευκόλυνε τη δημιουργία έξυπνων συμβολαίων, που αρχικά οραματίστηκε από την Szabo το 1994 (Bartoletti & Pompianu, 2017): "Ένα έξυπνο συμβόλαιο είναι ένα μηχανογραφημένο πρωτόκολλο συναλλαγών που εκτελεί τους όρους ενός σύμβαση. Οι γενικοί στόχοι είναι να ικανοποιηθούν οι κοινές συμβατικές προϋποθέσεις (όπως όροι πληρωμής, εμπράγματες εγγυήσεις, εμπιστευτικότητα, ακόμη και επιβολή), να ελαχιστοποιηθούν οι εξαιρέσεις τόσο κακόβουλες όσο και τυχαίες και να ελαχιστοποιηθεί η ανάγκη για αξιόπιστους διαμεσολαβητές. Οι σχετικοί οικονομικοί στόχοι περιλαμβάνουν τη μείωση της απώλειας απάτης, των διαιτητικών αποφάσεων και των δαπανών εκτέλεσης και άλλων δαπανών συναλλαγής. " Παρόλο που δεν έχει επιτευχθεί ο ορισμός της συναίνεσης (χωρίς λογοκρισία) για έξυπνες συμβάσεις, η βασική λειτουργικότητα τους είναι σαφής - η σύναψη συμβολαίων σε περίπτωση αποκεντρωμένης συναίνεσης και η χαμηλού κόστους αλγοριθμική εκτέλεση. Προκειμένου να επιτευχθεί αποκεντρωμένη συναίνεση, απαιτείται ένας κατανεμημένος ρόλος, ο οποίος πρέπει επίσης να εκτελείται αυτόματα. Τα ενδεχόμενα (συμπεριλαμβανομένης της κατανομής δικαιωμάτων ιδιοκτησίας και ελέγχου) σε μια έξυπνη σύμβαση πρέπει να κωδικοποιηθούν, έτσι ώστε να είναι εφικτή η αυτόματη εκτέλεση, μειώνοντας το κόστος επιβολής (Brafman & Beckstrom, 2006).

Τα προαναφερθέντα γεγονότα οδηγούν σε έναν φυσικό λειτουργικό ορισμό των έξυπνων συμβάσεων: Τα έξυπνα συμβόλαια είναι ψηφιακά συμβόλαια που επιτρέπουν όρους που εξαρτώνται από την αποκεντρωμένη συναίνεση, οι οποίοι είναι αυτοσυντηρούμενοι και αποτρέπονται από την αυτοματοποιημένη εκτέλεση (Bartoletti & Pompianu, 2017).

Ο ορισμός μας είναι συνεπής με τους ορισμούς που εμφανίζονται συνήθως στον νομικό κύκλο (Bartoletti & Pompianu, 2017). Είναι σημαντικό να σημειωθεί ότι οι έξυπνες συμβάσεις δεν είναι μόνο ψηφιακές συμβάσεις (πολλοί από τους οποίους βασίζονται στην εμπιστοσύνη για την επίτευξη συναίνεσης και εκτέλεσης), ούτε συνεπάγονται τεχνητή νοημοσύνη (αντίθετα είναι ρομποτικές). Χωρίς αποκεντρωμένη συναίνεση, το κόμμα που κατέχει την κεντρική συναίνεση συχνά απολαμβάνει τεράστια διαπραγματευτική δύναμη και μονοπωλιακό ενοίκιο (για παράδειγμα, ένα τρίτο μέρος με μονοπωλιακό χαρακτήρα δεδομένων). Και οι παραδοσιακές αποφάσεις τρίτων, όπως το δικαστήριο ή ένας διαιτητής, δεν ταιριάζουν καλά καθώς περιλαμβάνουν υψηλό βαθμό ανθρώπινης παρέμβασης που είναι λιγότερο αλγοριθμικές και θα μπορούσαν να είναι δαπανηρές επειδή οι αναλύσεις είναι τυπικά λιγότερο ντετερμινιστικές και συνεπώς ακριβές για τους παράγοντες που διακινούνται. Με την ενεργοποίηση της χρήσης

έξυπνων συμβολαίων, η τεχνολογία blockchain μπορεί να αυξήσει τη συμβατότητα και την εκτελεστότητα σε συμβάσεις ενδεχόμενων συναλλαγών που διευκολύνουν την ανταλλαγή χρημάτων, περιουσιακών στοιχείων, μετοχών, υπηρεσιών ή οτιδήποτε αξίας με αλγόριθμο αυτοματοποιημένο και χωρίς διενέξεις. Ακόμη και αν υιοθετήσουμε έναν πιο αδύναμο ορισμό για την έξυπνη σύναψη συμβάσεων και απαιτούμε την εκτέλεση από συγκεντρωτικά μέρη, η συμφωνία συναίνεσης μειώνει σημαντικά τις φθορές στις συμβάσεις και την εκτέλεση (Bartoletti & Pompianu, 2017).

2.2.2 Δημόσια και Ιδιωτικά Blockchains

Το Blockchain είναι μια ασφαλής και διαφανής τεχνολογία αποθήκευσης και μετάδοσης η οποία λειτουργεί χωρίς κεντρική συσκευή ελέγχου που μπορεί να χρησιμοποιηθεί για τη μεταφορά δεδομένων από το σημείο Α στο σημείο Β. Είναι μια κατανεμημένη βάση δεδομένων που διαχειρίζεται έναν κατάλογο αρχείων που προστατεύονται μηχανικά από παραβίαση ή τροποποίηση από αποθήκευση σε κόμβους μέσω του αποκεντρωμένου χρονοδιαγράμματος. Ένα blockchain, ως βάση δεδομένων, περιέχει το ιστορικό όλων των ανταλλαγών μεταξύ των χρηστών του από τη δημιουργία του. Μοιράζεται από τους διάφορους χρήστες της, χωρίς μεσάζοντες, που επιτρέπει σε καθένα να ελέγξει την εγκυρότητα του καναλιού. Το γεγονός να μοιραζόμαστε βασίζεται σε συναίνεση, και ιστορικά για να καταλήξουμε σε αυτό το είδος συναίνεσης χρησιμοποιήσαμε "απόδειξη της εργασίας". Αυτή η μέθοδος χρησιμοποιεί την ενέργεια ως μέσο επαλήθευσης ότι ο "ανθρακωρύχος" έχει κάνει καλή δουλειά. Επομένως, το πρωτόκολλο μπλοκ αλυσίδων χρησιμοποιεί ένα κρυπτογραφικό σύστημα που βασίζεται σε ένα αποκεντρωμένο σύστημα αποδείξεων: η επίλυση της απόδειξης απαιτεί υψηλή υπολογιστική ισχύ, που παρέχεται από τους ανθρακωρύχους. Προκειμένου να μην είναι παραπλανητικό, ένα blockchain απαιτεί ότι κανένας εχθρικός χειριστής δεν πρέπει να έχει οποιαδήποτε στιγμή περισσότερη από τη μισή υπολογιστική ισχύ της αλυσίδας. Προς το παρόν, εξετάζονται δύο τύποι blockchain (IBM, 2017):

Ένα blockchain ονομάζεται δημόσιος εάν οι συμμετέχοντες μπορούν να το διαβάσουν και να το χρησιμοποιήσουν για να πραγματοποιήσουν συναλλαγές αλλά και αν όλοι μπορούν να συμμετάσχουν στη διαδικασία δημιουργίας της συναίνεσης. Συνεπώς, δεν υπάρχει κεντρικό μητρώο, ούτε αξιόπιστο τρίτο μέρος. Η διακυβέρνηση των δημόσιων διαύλων, που προκύπτει από το ανοιχτό κίνημα και το cypherpunk, είναι απλή: "Ο κώδικας είναι νόμος". Σε αυτό το σύστημα, οι κόμβοι του δικτύου επικυρώνουν τις επιλογές που συζητήθηκαν και ξεκίνησαν από τους προγραμματιστές, αποφασίζοντας εάν θα ενσωματώσουν τις προτεινόμενες

τροποποιήσεις. Αυτή η λειτουργία βασίζεται στην "κρυπτοοικονομική", ο συνδυασμός οικονομικών κινήτρων και μηχανισμών επαλήθευσης που χρησιμοποιούν κρυπτογράφηση. Με βάση μια κοινοτική ή εναλλακτική προσέγγιση της οικονομίας, το σύστημα αυτό έχει αποδείξει τη δύναμή και την αντοχή του. Οποιαδήποτε δημόσια μπλοκ αλυσίδα λειτουργεί απαραίτητα με κέρμα ή συμβόλαιο (Mainelli & Smith, 2015).

Από την άλλη πλευρά, ένα blockchain ονομάζεται ιδιωτικό (ή ημι-ιδιωτικό) εάν η διαδικασία συναίνεσης μπορεί να επιτευχθεί μόνο από έναν περιορισμένο και προκαθορισμένο αριθμό συμμετεχόντων. Η πρόσβαση εγγραφής δίνεται από έναν οργανισμό και τα δικαιώματα ανάγνωσης μπορούν να είναι δημόσια ή περιορισμένα. Το "blockchain of place" που επισημάνθηκε σε αρκετά άρθρα είναι παραδείγματα ιδιωτικών καναλιών. Στην περίπτωση αυτή, η διαδικασία συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων. Το ιδιωτικό blockchain δεν χρησιμοποιεί απαραίτητα μηχανισμούς που βασίζονται στην κρυπτογραφία. - Στην περίπτωση του ιδιωτικού blockchain, δεν υπάρχει εξόρυξη, καμία απόδειξη εργασίας, καμία αμοιβή. Αυτό διαφοροποιεί πλήρως τους δύο τύπους αποθηκών και τεχνολογιών μετάδοσης (Yermack, 2017).

2.2.3 Η Τεχνολογία Blockchain στην Πράξη

Μια πλευρική αλυσίδα λειτουργεί ως χωριστά διαχειριζόμενος ρόλος, με δικό της κώδικα λογισμικού, ο οποίος είναι "συνδεδεμένος" με τον κύριο κατάλογο μπλοκ αλυσίδων έτσι ώστε να επιτρέπει τη μεταφορά βασικών πληροφοριών από την μία αλυσίδα στην άλλη. Συνάδει με την ιδέα των έξυπνων συμβολαίων (Power, 2019), τα οποία είναι ειδικά προγράμματα που χρησιμοποιούνται από έναν χρήστη του κύριου blockchain, προκειμένου να αποφασιστεί εάν μια συγκεκριμένη πράξη, δηλαδή μια δεδομένη πληρωμή, θα πρέπει να επιτρέπεται ή όχι. Ο οδηγός πλευρικής αλυσίδας συνδέει έμμεσα την υποκείμενη ισχύ εξακρίβωσης της κύριας μπλοκ αλυσίδας, εκμεταλλευόμενο ταυτόχρονα μια πιο ευέλικτη πλατφόρμα λογισμικού. Η πλευρική αλυσίδα συμβάλλει στην ευελιξία και την ελευθερία χρήσης πολλαπλών δικτύων, χωρίς να χρειάζεται να δημιουργεί νέα κρυπτογραφικά νομίσματα (δηλαδή αλλιώς), πράγμα που θα αποδυνάμωνε το φαινόμενο του δικτύου (ibid.) Και θα εμπόδιζε τη μαζική υιοθέτησή τους. Λόγω της αξίας που συνδέεται με την κατοχή κρυπτοσυχνότητας, υπάρχει μια φυσική αντίσταση να αγκαλιάσει μη ελεγμένες αλλαγές. Η πλευρική αλυσίδα και τα έξυπνα συμβόλαια προσφέρουν μια διέξοδο από αυτό το αδιέξοδο. Αρκετά σημαντικό είναι ότι μια ευρεία υιοθέτηση πλευρικών αλυσίδων θα απαιτούσε ωστόσο μικρές αλλαγές στο πρωτόκολλο Bitcoin (Appelbaum et al, 2017).

Πρώτον, οι «Εμπιστευτικές Συναλλαγές» είναι ένα νέο χαρακτηριστικό της πλευρικής αλυσίδας που εξασφαλίζει, μέσω της εισαγωγής μιας εμπιστευτικής διεύθυνσης, ότι τα ποσά κρυπτογραφημένων κεφαλαίων που μεταφέρονται είναι ορατά στο blockchain μόνο στους συμμετέχοντες στη συναλλαγή (ή / και εκείνους που ορίζουν). Αυτό ξεπερνά την ιδιωτική ζωή στο blockchain του Bitcoin, το οποίο βασίζεται αποκλειστικά σε ψευδώνυμες, αν και δημόσιες, ταυτότητες. Η οικονομική ιδιωτικότητα είναι μεγάλη ζήτηση από την κοινότητα κρυπτοσυχνότητας στις συναλλαγές για εμπορικούς και προσωπικούς σκοπούς. Δεύτερον, ο «διαχωρισμένος μάρτυρας» εξασφαλίζει ότι ο προσδιορισμός των αποτελεσμάτων μιας συναλλαγής στο βιβλίο διαχωρίζεται από τα δεδομένα που είναι απαραίτητα για να αποδειχθεί η εγκυρότητά του, εξαλείφοντας έτσι κάθε πιθανότητα αλλοιώσεως της συναλλαγής και ενισχύοντας τη συνολική ασφάλεια του blockchain (Kogan et al, 2014).

2.3 Εργαλεία και Τεχνικές Ελέγχου (Audit) Υποστηριζόμενα από Υπολογιστή (CAATTS)

Τα Εργαλεία Ελέγχου Υποβοηθούμενα από Ηλεκτρονικούς Υπολογιστές (“Computer-assisted Audit Tools” - CAAT), μπορούν να αντιμετωπίζονται ως οποιαδήποτε χρήση τεχνολογίας για την υποστήριξη της ολοκλήρωσης ενός ελέγχου. Η "(ευρεία) απόκλιση θα περιλάμβανε αυτοματοποιημένα έγγραφα εργασίας και παραδοσιακές εφαρμογές επεξεργασίας κειμένου" (Kuhn & Sutton, 2010) ή μπορεί να αναφέρεται ως "η χρήση ορισμένων λογισμικών που μπορούν να χρησιμοποιηθούν από τον ελεγκτή για την εκτέλεση τους ελέγχους και την επίτευξη των στόχων του ελέγχου» (Matthews, 2006). Η χρήση διακριτών ονομασιών για να εννοηθεί η τεχνολογία πληροφορικής / εργαλεία πληροφορικής και τεχνικές πληροφορικής για τον έλεγχο υπάρχει στις οδηγίες που παρέχονται από τα αρμόδια όργανα για τη βελτίωση της αποτελεσματικότητας και της αποτελεσματικότητας των διαδικασιών ελέγχου. Το πρότυπο αλλάζει ακόμα: οι νέες προσεγγίσεις προκαλούν ενδιαφέρον, όπως το λογισμικό γενικής λογιστικής ελέγχου, το GAS, η χρήση στο Web 2.0, χρησιμοποιώντας συνεργατικές προσεγγίσεις και διάφορα διαφορετικά προφίλ για τη βελτίωση της χρήσης λογισμικού (Murthy & Groomer, 2004).

Μια από τις πρώτες αναφορές που βρέθηκαν στον όρο "τεχνικές ελέγχου με τη βοήθεια υπολογιστών" είναι από το 1974 (AICPA 1979a, b). Δεδομένου ότι υπήρξε μεγάλη αύξηση στη χρήση υπολογιστικών συστημάτων με βάση τον υπολογιστή (AICPA 1984, 2001, 2002, 2011, 2013), όπου αναφέρεται ότι οι ελεγκτές πρέπει να εξετάζουν άλλες πτυχές πέραν των εσωτερικών ελέγχων και να λαμβάνουν υπόψη ολόκληρη την εικόνα, των αποτελεσμάτων της

επεξεργασίας υπολογιστών. Έκτοτε, πολλά νέα εργαλεία έχουν κυκλοφορήσει. Ο Lovata (1988) δηλώνει ότι ο αντίκτυπος στο περιβάλλον ελέγχου λόγω της αύξησης της τεχνολογίας των πληροφοριών είναι σημαντικός και το λογισμικό γενικής λογιστικής ελέγχου (GAS) είναι ένα από τα διάφορα εργαλεία που εξετάστηκαν στη μελέτη (Cash et al., 1977) ως οι πιο συχνά χρησιμοποιούμενες τεχνικές ελέγχου με τη βοήθεια υπολογιστών (Lovata 1988).

Τονίζει τα τρία χαρακτηριστικά της χρήσης του ΑΕΠ σε τρία επίπεδα της δομής του: οι περιβαλλοντικοί παράγοντες στην αρχική χρήση, το κόστος και τα οφέλη του ΑΗΣ και η αντιληπτή επίδραση των μικροϋπολογιστών στη χρήση του ΑΗΣ. Το κόστος-όφελος του GAS μελετήθηκε μετά τη σύσταση της AICPA σχετικά με τις Τεχνικές Ελέγχου Υποβοηθούμενης από Υπολογιστές (AICPA 1979a, b). Ο όρος "εργαλεία και τεχνικές ελέγχου υποβοηθούμενων από ηλεκτρονικούς υπολογιστές" προηγήθηκε άλλων ονομασιών που συνδέονται με την ιδέα της διενέργειας λογιστικού ελέγχου με τη χρήση ηλεκτρονικών εργαλείων: "Λογισμικό ηλεκτρονικού ελέγχου", "Πακέτα ελέγχου ηλεκτρονικών υπολογιστών" και "Ηλεκτρονική επεξεργασία δεδομένων", EDP. Οι όροι "Audit EDP" ή "Computer Auditing" μπορούν να παρουσιαστούν ως "ορισμός ομπρέλα, ο έλεγχος των πληροφοριακών συστημάτων σε μηχανογραφικό περιβάλλον" (Ma 1989, σελ. 2).

Το σύστημα ελέγχου ήταν δημοφιλές τότε (Vasarhelyi & Halper, 1991). Παρά την επιτυχία του λογισμικού, πολλοί ελεγκτές διατηρούν ακόμα τον έλεγχο τους γύρω από τον υπολογιστή (Byrnes et al., 2012). Παρόλα αυτά, παρόλο που είναι συνηθισμένο να χρησιμοποιούμε τον όρο "Εργαλεία και Τεχνικές Ελέγχου Υποβοηθούμενων από Ηλεκτρονικούς Υπολογιστές" στην πιο πρόσφατη έρευνα, υπάρχουν ακόμα αναφορές σήμερα στο "Λογισμικό Λογισμικού Ελέγχου" όπως και στις αναφορές σχετικά με το ποιο είναι το πιο κατάλληλο πακέτο λογισμικού για χρήση στην τάξη , όπου δύο εμπορικές συσκευασίες, IDEA και ACL, αξιολογούνται από παιδαγωγικές και λειτουργικές γωνίες. Κατευθυντήριες γραμμές για εκπαιδευτές στην τάξη παρέχονται: προσανατολισμός προγραμμάτων, διαφάνειες υποστήριξης, ασκήσεις και ερωτήσεις επανεξέτασης και εξέτασης (Bacani, 2017). Σε αυτό το έγγραφο, οι συγγραφείς χρησιμοποιούν επίσης την αναφορά στο "Γενικευμένο Λογισμικό Ελέγχου" για να ταξινομήσουν το IDEA και το ACL. Μικρότερος αριθμός συνεισφορών που υποβλήθηκαν από τον Vasarhelyi & Halper (1991), υπάρχουν σχετικές συνεισφορές από τα αρμόδια όργανα για τα πρότυπα εσωτερικού ελέγχου στους λογιστικούς ελέγχους που σχετίζονται με την εξέλιξη του λογιστικού ελέγχου, συγκεκριμένα τα πρότυπα AICPA SAS No. 3, SAS αρ. 48 (AICPA 1984) και SAS αριθ. 94. Το SAS αριθ. 104 έως 111, "Πρότυπα Αξιολόγησης Κινδύνων", σχετίζονταν επίσης με τις προσπάθειες

της AICPA για την τυποποίηση του ελέγχου των ΤΠ (Duncan & Whittington, 2017). Σήμερα, όλα τα SAS καταστέλλονται από το διευκρινισμένο SAS αριθ. 122 έως 128, που ισχύει την 1η Ιουνίου 2013 (AICPA 2014) (ASB 2011).

Στις τεχνικές ελέγχου υποβοηθούμενες από τους υπολογιστές του AICPA (AICPA 1979a, b, σελ. 2) οι τεχνικές παρουσιάζονται και ταξινομούνται ως: "Λογισμικό γενικευμένου λογισμικού ελέγχου, δεδομένα δοκιμών, συμπεριλαμβανομένης της χρήσης ολοκληρωμένης δοκιμαστικής εγκατάστασης και εντοπισμού προγραμμάτων, Συγκρίσεις, προγράμματα βοηθητικών προγραμμάτων, εξειδικευμένα προγράμματα ελέγχου, προγράμματα χρονομεριστικής μίσθωσης, πρόσθετες τεχνικές "(AICPA 1979a, β, σελ. 2). Οι τεχνικές αυτές συσχετίστηκαν με τέσσερις διεργασίες παγκόσμιου ελέγχου, όπως: αναθεώρηση του συστήματος εσωτερικού λογιστικού ελέγχου, δοκιμές συμμόρφωσης και ουσιαστικές διαδικασίες που περιελάμβαναν δοκιμές λεπτομερειών συναλλαγών και υπολοίπων και ανασκόπηση λογιστικού ελέγχου (Yuliana and Tangke 2006). Σύμφωνα με τους Wilken & Chenhall (2010), οι ελεγκτές δέχτηκαν τα CAAT, αλλά πιο πρόσφατες μελέτες (Teeter & Vasahelyi, 2010; Schmidt et al, 2016) δείχνουν ότι η αποδοχή της CAAT είναι ρηχή, ποικίλλει ανάλογα με τις εταιρείες και εξαρτάται από το μέγεθος της εταιρείας. Η χρήση του CAAT γίνεται σήμερα αποδεκτή στην ανάλυση δεδομένων, κυρίως επειδή τα εργαλεία αυξάνουν την ευεργεσία, ειδικά όταν οι ελεγκτές έχουν ανάγκη να επεξεργάζονται μεγάλα ποσά δεδομένων ή να αναλύουν σύνθετους δεσμούς μεταξύ των δεδομένων (Peffers et al, 2007). Επιπλέον, άλλοι ερευνητές έχουν συζητήσει αυτά τα τελευταία ερευνητικά συμπεράσματα (Muniswamy-Reddy et al, 2006).

Οι Lowers et al (2017) χρησιμοποίησαν την Unified Theory of Acceptance and Use of Technology (UTAUT) για να μελετήσουν την αποδοχή των ΤΠ από τους ελεγκτές. Κατέληξαν στο συμπέρασμα ότι μεταξύ έμπειρων ελεγκτών υπάρχουν σχέσεις μεταξύ της αποδοχής των νέων τεχνολογιών πληροφορικής και της πληθωρισμού της εταιρείας με τη χρήση μακροπρόθεσμων περιόδων αξιολόγησης του προϋπολογισμού και λογισμικού και, συνεπώς, με την ανατροφοδότηση των ανωτέρων από την έγκριση ειδικού λογισμικού. Σε αυτή την έρευνα, οι συγγραφείς συγκρίνουν την παρέμβαση της frm ή την απουσία της: τα ατομικά χαρακτηριστικά των ελεγκτών, όπως ο σχετικός κίνδυνος, και η επίδραση της πίεσης του προϋπολογισμού μπορούν επίσης να αποφασίσουν για ορισμένους τύπους υλοποίησης και αποδοχής λογισμικού. Η επαφή με τα CAAT που έχουν οι ελεγκτές κατά τη διάρκεια της επίσημης διδασκαλίας τους μπορεί να έχει σημασία για τον μετριασμό των ατομικών χαρακτηριστικών, των δυσκολιών και των αντιστάσεων που αναφέρθηκαν προηγουμένως. Όσον αφορά την οργάνωση της έρευνας

αποδοχής από τις χώρες CAAT, είναι δυνατόν να διευκρινιστεί ότι υπάρχουν περισσότερες συνεισφορές από χώρες που υιοθετούν ένα νομικό σύστημα με το κοινό δίκαιο από αυτές που χρησιμοποιούν κώδικα δικαίου. Οι χώρες του κοινού δικαίου είναι εκείνες που υιοθέτησαν ένα νομικό σύστημα που προέρχεται από το αγγλικό δίκαιο και προστατεύουν περισσότερο τους επενδυτές τους από εκείνους που ακολουθούν το αστικό δίκαιο που είχε τις ρίζες του στο ρωμαϊκό δίκαιο και συνδέονται με μια ισχυρότερη επιρροή από την κυβέρνηση (Henver et al, 2004).

Αυτοί οι συγγραφείς δημοσίευσαν επίσης ένα χάρτη που περιλαμβάνει μια κοινή ταξινόμηση των νόμιμων προελεύσεων των χωρών που χρησιμοποιήθηκε ως αναφορά για την ταξινόμηση καθεμιάς από τις ερευνητικές μελέτες που αναλύθηκαν: το κοινό δίκαιο και ο κώδικας δικαίου. Οι Elifoglu et al (2014) αναδιοργάνωσαν την "Θεωρητική τους άποψη για τη μελέτη των κινήτρων για την επιτυχή υιοθέτηση του CAAT", χρησιμοποιώντας μια προσέγγιση που μπορεί να θεωρηθεί ότι προσεγγίζει το UTAUT, αλλά περιλαμβάνει "Motivation" αντί για Behavioral Intention and Experience. Στο πρότυπο UTAUT, ο εθελοντισμός, που αντιπροσωπεύει "τον βαθμό στον οποίο η επιλογή υιοθεσίας είναι μία από τις οποίες ο εκλέγοντας έχει την εξουσία απόρριψης" (Gault, 2017), δρουν ως συντονιστές της σχέσης μεταξύ κοινωνικής επιρροής και κινήτρου εθελοντικότητα) και στην EE, την FC και τη SI, καθώς και τα κίνητρα (εμπειρία).

Οι Dai & Vasarhelyi, (2017) ενέκριναν το μοντέλο αποδοχής τεχνολογίας (TAM), στο πλαίσιο της εργασίας των εσωτερικών ελεγκτών. Οι μεταβλητές TAM και τα χαρακτηριστικά της τεχνολογίας (COSO, 2012) και η πολυπλοκότητα των εργαλείων ελέγχθηκαν σε συνδυασμό με οργανωτικούς παράγοντες, κοινωνικούς παράγοντες και μεμονωμένους παράγοντες. Οι οργανωτικοί παράγοντες περιλαμβάνουν την υποστήριξη και την κατάρτιση (και οι δύο μπορεί να είναι εσωτερικές ή εξωτερικές του οργανισμού) και η υποστήριξη της διαχείρισης (Back, 2002). Οι κοινωνικοί παράγοντες αντιπροσωπεύουν την εσωτερίκευση και την εικόνα που αντιπροσωπεύει την επιρροή των ανθρώπων στους χρήστες της πληροφορικής, συμπεριλαμβανομένης της εσωτερικοποίησης και της εικόνας (Bacani, 2017).

Μεμονωμένους παράγοντες που κατανοούν τη συνάφεια της εργασίας, την ποιότητα της παραγωγής και την επίδειξη αποτελεσμάτων. ως εκ τούτου, γνωστικοί παράγοντες που σχετίζονται με τις ατομικές προσδοκίες (Armbrust et al, 2010). Κατέληξαν στο συμπέρασμα ότι οι εσωτερικοί ελεγκτές αποδέχονται βασικά χαρακτηριστικά τεχνολογίας (όπως ερωτήματα βάσης δεδομένων και δειγματοληψία), αλλά όχι τα προηγμένα χαρακτηριστικά (όπως ταξινόμηση, παλινδρόμηση και ψηφιακή ανάλυση), τα οποία σχετίζονται με την ανάγκη ενός

συγκεκριμένου ιστορικού. Καθώς η πολυπλοκότητα των χαρακτηριστικών αυξάνεται, η αντιληπτή ευκολία χρήσης μειώνεται. Η αντιληπτή χρησιμότητα έχει περισσότερη επιρροή όσον αφορά τα βασικά χαρακτηριστικά και η ευχέρεια της ευκολίας χρήσης είχε μεγαλύτερο αντίκτυπο στην αποδοχή όταν χρησιμοποιήθηκαν προηγμένα χαρακτηριστικά.

Οι Appelbaum & Nehmer (2017) προέβλεψαν ένα ερευνητικό μοντέλο για τη χρήση λογισμικού γενικού λογιστικού ελέγχου (GAS) με βάση τα κίνητρα και τους περιορισμούς που εντοπίζουν οι ελεγκτές και τα οδηγούν στη χρήση ή μη χρήση του GAS. Οι διαστάσεις περιελάμβαναν: "το μέγεθος του frm" ως μέρος των δημογραφικών χαρακτηριστικών και την κατανόηση της σχέσης μεταξύ του μεγέθους του frm και της χρήσης του GAS. "Εμπειρία στον ηλεκτρονικό έλεγχο" που ορίζεται από τον αριθμό των ετών εμπειρίας. "IT δεξιότητες" που ορίζονται ως πολύ καλές, καλές, επαρκείς, βασικές, πολύ βασικές. "Οργανωτική επιρροή": υποστήριξη ανώτατης διοίκησης, υποστήριξη IT, εμπειρία εμπειρογνωμοσύνης στον τομέα της πληροφορικής στον οργανισμό (οι τρεις μπορούν να χαρακτηριστούν ως UTAUT διευκολύνσεις), εσωτερική και εξωτερική κατάρτιση (εμπειρογνωμοσύνη στο εξωτερικό και στο εξωτερικό), υλοποίηση και συντήρηση αερίου . Εκτός από τους πόρους για τη χρήση του GAS, η πίεση της ανώτατης διοίκησης, η πίεση επίδοσης, η δέσμευση ελέγχου εξετάζονται στη βιβλιογραφία. "Παράγοντας πελάτη" ως δύναμη των εσωτερικών συστημάτων ελέγχου ενός πελάτη? την πολυπλοκότητα του περιβάλλοντα περιβάλλοντος των πελατών, την πολυπλοκότητα του επιχειρηματικού περιβάλλοντος, την ανησυχία των πελατών για την ασφάλεια των δεδομένων, το μέγεθος της επιχείρησης πελάτη και την υποστήριξη από τους πελάτες IT staf. "Κατανομή των ελεγκτικών υποχρεώσεων": αφορά τον φόρτο εργασίας, τον χρόνο και τον δημοσιονομικό προϋπολογισμό για την ελεγκτική δέσμευση · και την "αντιληπτή χρησιμότητα" αξία και χρησιμότητα του GAS στον έλεγχο.

2.4 Η Τεχνολογία BlockChain στον Έλεγχο (Audit)

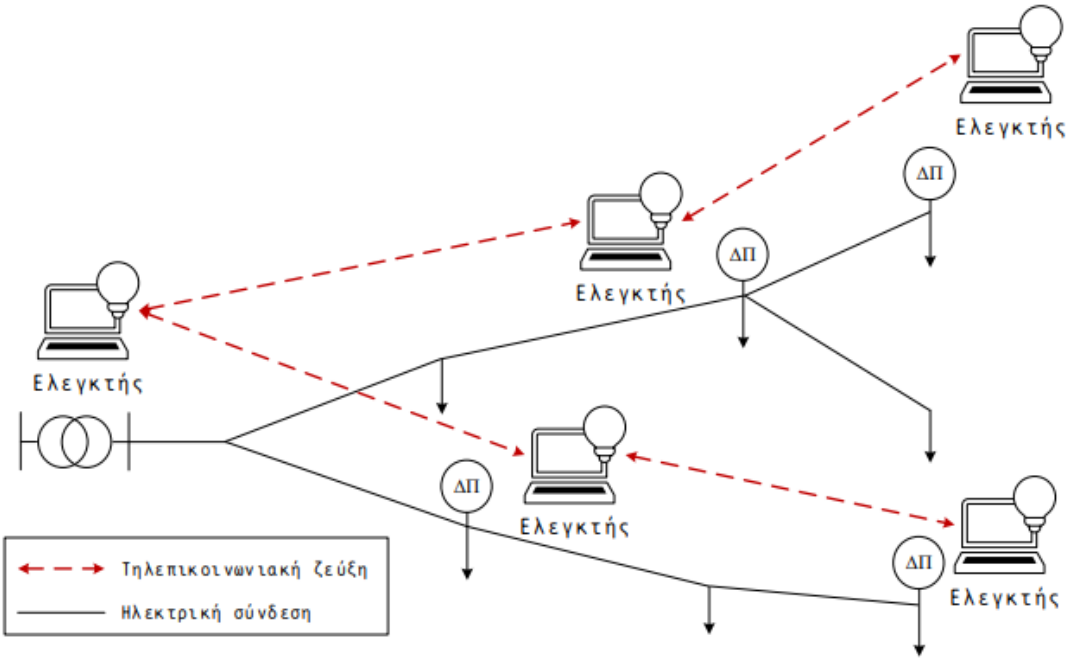
Το BlockChain είναι μια τεχνολογία που διανέμεται για την αποθήκευση δεδομένων και έχει τις εξής ιδιότητες: αμετάβλητη, προσαρμοσμένη, διατεταγμένη, χρονικά σφραγισμένη, ανοιχτή και διαφανή, ασφαλής και τελικά συνεπής. Σύμφωνα με τις ιδιότητες μπλοκ αλυσίδας, αυτή η τεχνολογία μπορεί να εφαρμοστεί σε διάφορες καταστάσεις, όταν χρειάζεται να εξασφαλιστεί η απόδειξη ύπαρξης, ανύπαρκτος, χρονοδιάγραμμα, ταυτότητα, πνευματική ιδιοκτησία και ιδιοκτησία. Ο έλεγχος είναι μια συστηματική, ανεξάρτητη και τεκμηριωμένη διαδικασία για την απόκτηση αποδεικτικών στοιχείων αξιολογώντας την αντικειμενικά για να παρακολουθεί εάν πληρούνται τα κριτήρια ελέγχου (Appelbaum, 2016).

Το blockchain μπορεί να χρησιμοποιηθεί όταν υπάρχει ανάγκη συμμόρφωσης των δραστηριοτήτων των επιχειρήσεων με τους κανονισμούς, διότι εξασφαλίζει ένα κομμάτι ελέγχου. Το blockchain μπορεί να χρησιμοποιηθεί ως βάση για την επαλήθευση των αναφερόμενων συναλλαγών. Ένα παράδειγμα μπορεί να είναι όπου οι ελεγκτές, αντί να ζητούν από τους πελάτες τους τραπεζικές δηλώσεις ή να στέλνουν αιτήματα επιβεβαίωσης σε τρίτους, μπορούν εύκολα να επαληθεύσουν τις συναλλαγές επί των διαθέσιμων στο κοινό βιβλιαρίων. Η αυτοματοποίηση αυτής της διαδικασίας επαλήθευσης θα οδηγήσει σε βελτίωση του κόστους στο περιβάλλον ελέγχου. Αυτό που διακρίνει τη χρήση του blockchain από άλλες μορφές χρονικής σήμανσης και ελέγχου ταυτότητας δεδομένων είναι ότι τα έγγραφα και άλλα σύνολα δεδομένων στο blockchain είναι αποκεντρωμένη απόδειξη. Βεβαιώνοντας ότι τα δεδομένα δεν μπορούν να διαγραφούν ή να τροποποιηθούν από κανέναν, όχι από τη δική σας εταιρεία, ούτε από ανταγωνιστές, τρίτους ή κυβερνήσεις, οι οποίες μπορούν να βοηθήσουν σε ένα από τα μεγαλύτερα ζητήματα κατά τη διενέργεια ελέγχων, απάτης και ανίχνευσης (Alles et al, 2008).

Σύμφωνα με μια μελέτη το 2011 (Geerts, 2011), τα κρυφά έγγραφα / πληροφορίες, τα τροποποιημένα έγγραφα, τα πλαστά έγγραφα και η συμπαιγνία με τρίτους αντιπροσωπεύουν συνολικά το 81% των συστημάτων αποδείξεων, μέσω των οποίων η διοίκηση δημιουργεί ή κρύβει στοιχεία που αποκρύπτουν την απάτη. Η πρόωρη αναγνώριση εσόδων, τα πλασματικά έσοδα, τα υπερτιμημένα περιουσιακά στοιχεία και τα υποεκτιμηθέντα έξοδα, οι παραλειφθείσες ή υποεκτιμημένες δαπάνες / υποχρεώσεις ανέρχονται συνολικά στο 78% των λογαριασμών, μέσω των οποίων η διοίκηση διαπράττει απάτη χειριζόμενοι τα υπόλοιπα λογαριασμών ή τις γνωστοποιήσεις. Η ύπαρξη ενός συστήματος blockchain, στο οποίο οι λογιστές πρέπει να εισάγουν τις οικονομικές καταστάσεις των εταιρειών, σε ένα ασφαλές και ανθεκτικό λογισμικό τροποποίησης, το οποίο θα μπορούσε να χρησιμοποιηθεί σε πραγματικό χρόνο, θα είχε σημαντικό θετικό αντίκτυπο στη μείωση αυτού του είδους των απατών. Υπάρχουν επίσης εξωτερικές δυνάμεις που πρέπει να λαμβάνονται υπόψη κατά τη μελέτη της εφαρμογής του blockchain στον έλεγχο. Ένα παράδειγμα είναι οι αλλαγές σε κανονισμούς όπως ο κανονισμός γενικής προστασίας δεδομένων (GDPR), ο οποίος στοχεύει στην προστασία όλων των πολιτών της ΕΕ από την παραβίαση της ιδιωτικής ζωής και των δεδομένων. Αυτό θα υποχρεώσει τις εταιρείες να αλλάξουν τον τρόπο με τον οποίο διατηρούν ευαίσθητα προσωπικά δεδομένα στα συστήματά τους και μπορεί να επηρεάσει τα αρχεία των χρηματοπιστωτικών συναλλαγών, τα χρεωστικά και πιστωτικά σημειώματα, τα τιμολόγια και τις αποδείξεις για παράδειγμα. Σε ολόκληρη την τελική έκδοση του κανονισμού που δημοσιεύθηκε στις 6 Απριλίου

2016, προτείνεται πολλές φορές να χρησιμοποιείται κρυπτογραφία για την κρυπτογράφηση λογικών δεδομένων. Χρησιμοποιώντας ένα ιδιωτικό blockchain, όπου μπορούν να αποκτήσουν πρόσβαση μόνο τα συμβαλλόμενα μέρη με εξουσιοδότηση, μπορεί να είναι μια επιλογή για να διατηρούνται αυτά τα αρχεία ασφαλή.

Διάγραμμα 1 – Αναπαράσταση του Δικτύου Διανομής (Kouveliotis, 2019)



Ορισμένες από τις αναδυόμενες τεχνολογίες περιλαμβάνουν τεχνικές εξόρυξης δεδομένων και ανίχνευση απάτης, μεγάλα δεδομένα και αναλύσεις, έλεγχος cloud και φέρνουν τη δική σας συσκευή (BYOD) και εργαλεία ελέγχου. Όλες αυτές οι τεχνολογικές καινοτομίες σημαίνουν ότι το επάγγελμα του ελεγκτή θα χρειαστεί άτομα που έχουν λογιστικές δεξιότητες αλλά έχουν επίσης εξαιρετικές γνώσεις πληροφορικής εξαιτίας ενός μέλλοντος που επιτρέπει τεχνολογικές πλατφόρμες. Σε μερικά χρόνια αναμένεται ότι οι αυτοματοποιημένες εκθέσεις ελέγχου, όπου οι πληροφορίες μεταφορτώνονται στα αποσπάσματα blockchain και τεχνητής νοημοσύνης και αναλύονται σε πραγματικό χρόνο, ίσως αποτελούν παράδειγμα αυτής της τεχνολογικής εξέλιξης (Gault, 2017).

2.5 Υφιστάμενες και Μελλοντικές Λύσεις BlockChain

Οι Louwers et al (2017) αναφέρονται στο blockchain ως «μηχανή αλήθειας» που περιέχει όλα τα απαραίτητα εργαλεία για να καθιερωθούν άνευ προηγουμένου επίπεδα εμπιστοσύνης και διαφάνειας. Λόγω του κατανεμημένου και αποκεντρωμένου χαρακτήρα της, η BT αναλαμβάνει τη λογιστική και τον έλεγχο σε τομέα ομότιμης συνεργασίας χωρίς θεσμική διαμεσολάβηση (Warncke, 2017). Η BT παρέχει κατανεμημένη ασφάλεια δεδομένων, διαφάνεια και αμετάβλητο

(Ducnan & Whittington, 2017). Σύμφωνα με πολλούς μελετητές, τα παραπάνω χαρακτηριστικά θα μπορούσαν να βελτιώσουν σημαντικά τη λογιστική και την ελεγκτική πρακτική και θα μπορούσαν να αναγκάσουν τους ελεγκτές και τους λογιστές να κάνουν μια σημαντική στροφή προς μια πιο διαφανή συμπεριφορά (Appelbaum et al, 2017). Η ΒΤ επιτρέπει στις εταιρείες να γράφουν συναλλαγές στο blockchain, όπου δημιουργούνται αμετάβλητα λογιστικά αρχεία. Η χειραγώγηση ή η καταστροφή αυτών των καταχωρίσεων συναλλαγών σε μια προσπάθεια να τους παραποιηθεί ή να εξαλειφθούν είναι πρακτικά αδύνατη επειδή είναι κρυπτογραφικά σφραγισμένες και διανεμημένες (Baderscher et al, 2017).

Αρκετές εκδόσεις, αναφορές και ιστότοποι υπογραμμίζουν τον τρόπο με τον οποίο η αμερόληπτη μεταβολή καθίσταται το κλειδί για τη λογοδοσία, καθώς τα blockchains επιτρέπουν στους συμμετέχοντες να βλέπουν κρυπτογραφημένες συναλλαγές και να διασφαλίζουν ότι ενημερώνονται και συγχρονίζονται (Bartoletti & Pompianu, 2017). Ως εκ τούτου, θεωρείται ότι η ΒΤ βελτιώνει σημαντικά τη διακυβέρνηση και τη διαφάνεια παρέχοντας στους μετόχους και τα ενδιαφερόμενα μέρη άμεση πρόσβαση στα λογιστικά δεδομένα, παρέχοντάς τους έτσι μια πραγματική και ακριβή εικόνα δεδομένων που είναι εγγενώς αξιόπιστα (Dai & Vasarhelyi, 2017). Δεδομένης της κλιμακούμενης και δομοστοιχειωτής δομής της, η ΒΤ - ιδιαίτερα ιδιωτικές, επιτρέπεται - προσφέρει τη δυνατότητα δημιουργίας διαφοροποιημένης πρόσβασης σε πληροφορίες για τους ενδιαφερόμενους και τους μετόχους, οι οποίοι συνήθως έχουν διαφορετικές ανάγκες για λογιστικές πληροφορίες (IBM, 2017). Για παράδειγμα, οι οικονομικοί διευθυντές και οι ελεγκτές απαιτούν πρόσβαση στο πλήρες φάσμα των λογιστικών στοιχείων, ενώ οι υπάλληλοι που πληρώνουν λογαριασμούς χρειάζονται μόνο λογιστικά στοιχεία που σχετίζονται με πληρωτέες συναλλαγές και οι επενδυτές μπορούν να χρησιμοποιήσουν μόνο συγκεντρωτικά λογιστικά στοιχεία.

Το αυξημένο επίπεδο διαφάνειας σε συνδυασμό με τον επαληθεύσιμο χαρακτήρα της ΒΤ είναι πιθανό να αυξήσει την εμπιστοσύνη των μετόχων και των εμπλεκόμενων φορέων (IAASB, 2017). Η ΒΤ μπορεί επίσης να παρέχει τη δυνατότητα αποκάλυψης συναλλαγών εκτός λογαριασμού και κρυφών λογαριασμών, γεγονός που έχει σοβαρές επιπτώσεις στη λογοδοσία και τη διαφάνεια, καθώς και στην ανταγωνιστική στάση και συμμόρφωση των εταιρειών στους κανόνες (Jarvenpaa & Teigland, 2017). Πρέπει να δοθεί προσοχή στο ζήτημα της επαλήθευσης των συναλλαγών (No & Vasarhelyi, 2017), επειδή η απλή καταγραφή δεδομένων στο blockchain δεν σημαίνει ότι η συναλλαγή έχει συμβεί στον πραγματικό κόσμο: «Απλά επειδή ένα

συναλλασσόμενο αρχείο είναι μηχανογραφημένο και "μπλοκαρισμένο" δεν σημαίνει απαραίτητα ότι το φυσικό παγκόσμιο υλικό του εμπορίου δεν έχει παραβιαστεί" (PCAOB, 2017).

Με άλλα λόγια, μόνο επειδή μια μεταβίβαση περιουσιακών στοιχείων έχει καταγραφεί σε ένα blockchain δεν εγγυάται ότι το περιουσιακό στοιχείο έχει μεταβιβαστεί ή ανταλλάξει, έχουν πραγματοποιηθεί πληρωμές και έχουν πραγματοποιηθεί συναλλαγές στον πραγματικό κόσμο. Ως εκ τούτου, ορισμένοι λογιστικοί μελετητές έχουν επικρίνει τις μεθόδους επαλήθευσης για την αδυναμία επαρκούς επικύρωσης των συναλλαγών (PCAOB, 2017). Επομένως, οι εταιρείες που χρησιμοποιούν το ΒΤ σε συνδυασμό με τις πληρωμές εκτός σύνδεσης δεν εγγυώνται ότι η συναλλαγή πραγματοποιήθηκε στον πραγματικό κόσμο. Ωστόσο, για τους ειδικούς σε θέματα λογιστικής, αυτό είναι μια σημαντική πτυχή που μπορούν να συμβάλουν στην αναζήτηση μηχανισμών για τον συμβιβασμό των συναλλαγών που έχουν καταγραφεί και των πραγματικών πληρωμών (Rozario & Thomas, 2017).

Τέλος, οι ερευνητές εκφράζουν ανησυχίες για το ότι τα blockchains είναι «απαλλαγμένα απάτης» (Yan, 2017). Πράγματι, η διάπραξη απάτης είναι ακόμα δυνατή στις μπλοκ αλυσίδες, καθώς τα ψέματα που κωδικοποιούνται στις μπλοκ αλυσίδες εξακολουθούν να είναι ψέματα. Είναι απλώς αμετάβλητα ψέματα (Yermack, 2017). Υποστηρίζοντας ότι η ΒΤ δεν είναι σε θέση να ανιχνεύσει δόλιες συναλλαγές, αν οι συναλλαγές αυτές ήταν δόλιες από την αρχή, οι ερευνητές προειδοποιούν τους επαγγελματίες ότι η δυνατότητα της ΒΤ να αποτρέψει την απάτη μπορεί να υπερεκτιμηθεί και να υπερκεραστεί (Appelbaum & Nehmer, 2017). Ωστόσο, αν και η ΒΤ δεν μπορεί να εξαλείψει τελείως την απάτη, μπορεί να βοηθήσει στην ταυτοποίηση της απάτης σε πραγματικό χρόνο (Bacani, 2017.

Η σύγχρονη ελεγκτική πρακτική είναι έντασης εργασίας. Στην αρχή κάθε ελεγκτή, οι ελεγκτές λαμβάνουν καταχωρήσεις περιοδικών, αρχεία υπολογιστικών φύλλων και άλλα έγγραφα, τόσο σε ηλεκτρονικό όσο και σε μη αυτόματο μορφότυπο. Πριν αρχίσει η διαδικασία ελέγχου, οι ελεγκτές πρέπει να επενδύσουν σημαντικό χρόνο στην προετοιμασία των δεδομένων και στον προγραμματισμό του ελέγχου. Αυτή η μακρά διαδικασία έρχεται με τη θυσία της αποτελεσματικότητας και της σχέσης κόστους-αποτελεσματικότητας (Dai & Vasarhelyi, 2017).

Ενώ οι σύγχρονοι έλεγχοι απαιτούν την έγκριση συναλλαγών και υπολοίπων στο τέλος των περιόδων αναφοράς, τα blockchains παρέχουν σχεδόν αμέσως τα επικυρωμένα αρχεία συναλλαγών (Deloitte, 2017). Μέσω της στιγμιαίας επιβεβαίωσης των συναλλαγών, η ΒΤ επιτρέπει τον συνεχή έλεγχο, ο οποίος ονομάζεται επίσης «έλεγχος σε πραγματικό χρόνο».

Ο Gault (2017) περιγράφει τον έλεγχο στην εποικοδομητική εποχή ως plug-in, πάντα με τον έλεγχο, τονίζοντας ότι οι εξωτερικοί έλεγχοι μεταβαίνουν από περιοδική ή ετήσια άσκηση σε συνεχή υπόθεση. Η παρακολούθηση του τι συμβαίνει σε πραγματικό χρόνο είναι μια ουσιαστική απόκλιση από τη σύγχρονη ελεγκτική πρακτική, η οποία εστιάζεται στη διερεύνηση όσων συνέβησαν εκ των υστέρων. Ο συνεχής έλεγχος εξαλείφει την παραδοσιακή ελεγκτική έννοια της δειγματοληψίας καθώς η ΒΤ προσφέρει ένα ενημερωμένο, αμετάβλητο ιστορικό αρχείο όλων των συναλλαγών.

Συνδυάζοντας την επεξεργασία των συναλλαγών με την καταγραφή και τη συμφιλίωση των συναλλαγών αυτών, η ΒΤ εισάγει σημαντικές βελτιώσεις αποτελεσματικότητας. Ακριβώς, εξαλείφεται η ανάγκη εισόδου και εναρμόνισης των λογιστικών δεδομένων σε πολλαπλές βάσεις δεδομένων, με αποτέλεσμα να εξοικονομείται χρόνος και να μειώνεται σημαντικά ο κίνδυνος ανθρώπινου σφάλματος. Πολλές αναλυθείσες εκθέσεις υποδεικνύουν ότι η αυξημένη δυνατότητα ελέγχου των λογιστικών πληροφοριών είναι ένα από τα σημαντικότερα οφέλη της ΒΤ (Louwers et al, 2017).

Δεδομένου ότι η ΒΤ παρέχει μια διαδρομή ελέγχου σε πραγματικό χρόνο, ο έλεγχος όχι μόνο καθίσταται σημαντικά πιο απλός, αλλά και σημαντικά φθηνότερος (Warncke, 2017). Οι ελεγκτές μπορούν να λειτουργούν αποτελεσματικότερα και αποτελεσματικότερα λόγω του μειωμένου χρόνου που απαιτείται για τη συμφιλίωση και την αμφισβήτηση αρχείων με τους πελάτες (Duncan & Whittington, 2017). Εκτός αυτού, θεωρείται ότι ο συνεχής έλεγχος καθιστά απλούστερο για τους ελεγκτές να διερευνούν την απάτη, δεδομένου ότι τα συστήματα σε πραγματικό χρόνο αναδεικνύουν ανωμαλίες κατά τη στιγμή της εμφάνισης, επιτρέποντας έγκαιρες έρευνες (AICPA, 2017).

Επιπλέον, ο συνεχής έλεγχος της ΒΤ θα μπορούσε να ενισχύσει την κατανόηση των επιχειρήσεων από τους ελεγκτές, καθώς η δέσμευση μεταξύ ελεγκτών και πελατών δεν περιορίζεται πλέον στην περίοδο αναφοράς του τέλους του οικονομικού έτους (AICPA 2017). Ωστόσο, είναι απίθανο να επιτευχθεί πλήρης συνεχής έλεγχος, εκτός εάν οι εταιρείες αποφασίσουν να καταγράψουν όλες τις συναλλαγές στο blockchain. Με την κωδικοποίηση μόνο συγκεκριμένων συναλλαγών, οι υποσχέσεις συνεχούς ελέγχου μπορούν να παραδοθούν μόνο εν μέρει (Appelbaum et al, 2017). Η ΒΤ όχι μόνο επιτρέπει την έγκαιρη εξέταση των συναλλαγών αλλά και την αυτοματοποίηση της καταγραφής συναλλαγών και της επαλήθευσης. Από την άποψη αυτή, γίνεται αναφορά σε έξυπνες συμβάσεις που επιτρέπουν τον αποτελεσματικό έλεγχο των συναλλαγών και των διαδικασιών καταγραφής (Dai and Vasarhelyi 2017).

2.5.1 Η Ευθυγράμμιση Των BlockChain Smart Contracts

Μια σιωπηρή διαδικασία στη λογιστική και στον έλεγχο είναι η συμμετοχή του ανθρώπινου στοιχείου σε όλα τα βήματα. Ωστόσο, η αναγκαιότητα για ανθρώπινη λειτουργία μπορεί να αλλάξει με την ανάπτυξη μπλοκ. Η ΒΤ μπορεί να μεταφέρει όχι μόνο συναλλακτικά δεδομένα σε πραγματικό χρόνο αλλά μπορεί επίσης να φέρει προγραμματισμένη έκδοση ανθρώπινης δράσης. Αυτά έχουν τη μορφή λεγόμενων έξυπνων συμβολαίων, τα οποία κωδικοποιούν τους σχετικούς όρους σε ένα blockchain και εκτελούνται αυτόματα όταν πληρούνται προκαθορισμένες συνθήκες (Rozario και Vasarhelyi 2018). Οι έξυπνες συμβάσεις διευκολύνουν ψηφιακά, ελέγχουν και επιβάλλουν συναλλαγές. Οι έξυπνες συμβάσεις εκτελούνται από ένα δίκτυο υπολογιστών που χρησιμοποιεί πρωτόκολλα συναίνεσης για να συμφωνεί με τη σειρά των ενεργειών που καθορίζονται σε μια σύμβαση (Deloitte 2018).

Πριν από την εμφάνιση της ΒΤ, η εκτέλεση έξυπνων συμβάσεων ήταν αδύνατη λόγω των επιχειρηματικών μερών που διατηρούσαν ξεχωριστές βάσεις δεδομένων. Με μια κοινή βάση δεδομένων που χρησιμοποιεί ένα πρωτόκολλο blockchain, οι έξυπνες συμβάσεις εκτελούνται αυτόματα με μειωμένο κίνδυνο σφάλματος ή χειραγώγησης και δεν υπάρχει ανάγκη για τρίτο μεσάζοντα (Dai and Vasarhelyi 2017, Yermack 2017, Rozario και Vasarhelyi 2018). Οι έξυπνες συμβάσεις βασικά επεκτείνουν την χρησιμότητα των μπλοκ αλυσίδων από την απλή καταγραφή των καταχωρίσεων συναλλαγών στην αυτόματη εφαρμογή των όρων πολυκομματικών συμφωνιών Deloitte 2018). Για τους λογιστές και τους ελεγκτές, οι έξυπνες συμβάσεις αναμένεται να διαδραματίσουν σημαντικό ρόλο δεδομένου ότι επιτρέπουν την αυτόνομη καταγραφή των συναλλαγών σύμφωνα με τους συμφωνημένους όρους (Yermack 2017). Εάν οι κανόνες όπως οι πωλήσεις ρεκόρ μετά την αποστολή αγαθών έχουν προγραμματιστεί σε έξυπνες συμβάσεις, το σύστημα ελέγχει αυτόματα και ελέγχει την ημερομηνία αποστολής πριν την καταγραφή των πωλήσεων στο blockchain (Dai and Vasarhelyi 2017).

Οι Rozario και Vasarhelyi (2018) προτείνουν στους εξωτερικούς ελεγκτές να χρησιμοποιούν έξυπνες συμβάσεις. Σύμφωνα με τους συντάκτες, οι έξυπνες συμβάσεις μπορούν να διευκολύνουν την εκτέλεση των διαδικασιών ελέγχου με την αυτοματοποίηση της διαδικασίας συμφιλίωσης συναλλαγών, παρέχοντας παράλληλα περισσότερη διαφάνεια στους ενδιαφερόμενους, μέσω της αναφοράς σε πραγματικό χρόνο του ελέγχου. Ο αυτοματοποιημένος συνδυασμός συναλλαγών όχι μόνο εξοικονομεί χρόνο αλλά και μειώνει σημαντικά τον κίνδυνο ανθρώπινου σφάλματος (Rozario και Vasarhelyi 2018). Εντούτοις, πρέπει να σημειωθεί ότι είναι απίθανο κάθε συναλλαγή να ελέγχεται από τις έξυπνες συμβάσεις της ΒΤ

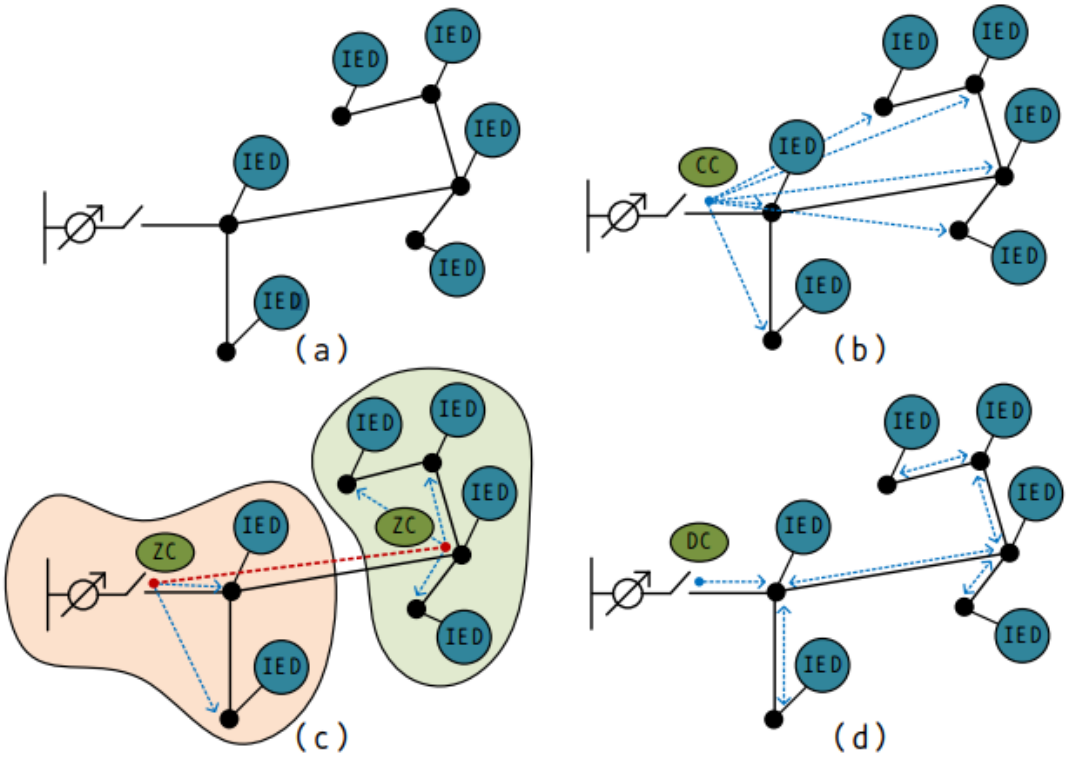
και να υποβληθεί σε αυτοματοποιημένη συμφωνία δεδομένων. Οι σύνθετες λογιστικές καταχωρίσεις, όπως η αποτίμηση της εύλογης αξίας ή οι λογιστικές μετρήσεις, όπως οι δοκιμές απομείωσης, απαιτούν εμπειρογνωμοσύνη και κρίση από τους λογιστές και τους ελεγκτές. Ως εκ τούτου, οι Rozario και Vasarhelyi (2018) προτείνουν ένα ολιστικό μοντέλο ελέγχου που αποτελείται από ένα υβρίδιο έξυπνων διαδικασιών ελέγχου και διαδικασιών ελέγχου που εκτελούνται έξω από το blockchain. Οι τεχνολογίες τεχνητής νοημοσύνης (AI) μπορούν να επεκτείνουν το δυναμικό των εφαρμογών έξυπνων συμβάσεων στην αξιολόγηση και την καταγραφή των φυσικών συνθηκών των προϊόντων. Σε συνδυασμό με την AI, οι έξυπνες συμβάσεις θα μπορούσαν να ανιχνεύσουν και να μετρήσουν τις ζημίες απογραφής και άλλων περιουσιακών στοιχείων και, ενδεχομένως, να αυτοματοποιήσουν τη λογιστική μέτρηση αυτών των περιουσιακών στοιχείων. Για παράδειγμα, όταν τα αποστελλόμενα προϊόντα είναι εφοδιασμένα με ειδικούς αισθητήρες ή τσιπ, αυτοί οι αισθητήρες ή τα τσιπ θα μπορούσαν να αναφέρουν αυτομάτως τις ζημιές απογραφής και το σήμα στις έξυπνες συμβάσεις για να προσαρμόσουν αμέσως τις αντίστοιχες λογιστικές μετρήσεις. (Dai and Vasarhelyi 2017, Kozlowski 2018).

Ο Kozlowski (2018) συνιστά την ενσωμάτωση των λογιστικών προτύπων στην υποδομή των blockchain, με την κωδικοποίησή τους σε έξυπνες συμβάσεις. Στο πλαίσιο του συνεχούς ελέγχου, οι ελεγκτές θα μπορούσαν τότε να ελέγξουν εάν οι συναλλαγές συμμορφώνονται με τους εν λόγω λογιστικούς κανόνες και να επισημάνουν περιπτώσεις αναντιστοιχίας. Οι έξυπνες συμβάσεις μπορούν να ανακαλέσουν τις συναλλαγές αν το σύστημα εντοπίσει ότι δεν τηρούνται οι κανόνες και τα πρότυπα που κωδικοποιούνται στη σύμβαση (CPA Canada 2016, Deloitte 2016a). Εκτός από την αυτοματοποίηση των συναλλαγών εγγραφής, τα έξυπνα συμβόλαια μπορεί να προσφέρουν μια λειτουργία πρόβλεψης, για παράδειγμα με κωδικοποίηση προτύπων προεπιλογής ή πρόβλεψης αξιολόγησης πιστοληπτικής ικανότητας (Dai and Vasarhelyi 2017). Τα μοντέλα αυτά θα είναι σε θέση να παρακολουθούν τον κίνδυνο αθέτησης των οφειλετών με βάση την αξιολόγηση της οικονομικής τους κατάστασης και της συμπεριφοράς αγοράς και να προσαρμόζουν αναλόγως τις εκτιμήσεις των επισφαλών χρεών, όταν είναι απαραίτητο.

3 Εφαρμογή Blockchain

Με τη στενή έννοια, η αλυσίδα μπλοκ είναι μια δομή δεδομένων αλυσίδας που αποτελείται από μπλοκ δεδομένων που συνδυάζονται σε χρονολογική σειρά. Και είναι ένα κατανεμημένο βιβλίο δεν μπορούσε να αλλοιωθεί ή να πλαστογραφηθεί με την εγγύηση από την κρυπτογραφία. Με μια ευρεία έννοια, η τεχνολογία blockchain είναι ένα νέο κατανεμημένο μοντέλο υποδομής και πληροφορικής που χρησιμοποιεί δομή δεδομένων αλυσίδας μπλοκ για την επαλήθευση και αποθήκευση δεδομένων, εφαρμόζει αλγόριθμο κατανεμημένου συναινετικού κόμβου για τη δημιουργία και ενημέρωση δεδομένων, κάνει χρήση κρυπτογραφίας για να εξασφαλίσει την ασφάλεια της μετάδοσης δεδομένων και την πρόσβαση και την εκμετάλλευση έξυπνων συμβάσεων που αποτελούνται από αυτοματοποιημένα σενάρια και κωδικούς για τον προγραμματισμό και τη λειτουργία δεδομένων. Ως υποστηρικτική τεχνολογία της χρηματοδότησης του Διαδικτύου, το blockchain ενσωματώνει τη γνώση των μαθηματικών και της οικονομίας και συνδυάζει την κρυπτογραφία, τη χρονική σφραγίδα, την κατανεμημένη τεχνολογία και τον μηχανισμό συναίνεσης (Bartoletti & Pompianu, 2017).

Διάγραμμα 2 – Διαφορετικές Ταξινομήσεις στις Δομές Ελέγχου, όπως παράγονται από τα στοιχεία αρχιτεκτονικής συντονισμού (Kouveliotis, 2019).



Στο ανωτέρω διάγραμμα, το σχήμα (a) απεικονίζει ταξινόμηση χωρίς επικοινωνία, το σχήμα (b) απεικονίζει τον κεντρικό έλεγχο, όπου το CC σημαίνει «κεντρικός ελεγκτής», το σχήμα (c)

απεικονίζει τον αποκεντρωμένο έλεγχο, όπου το ZC σημαίνει «ελεγκτής ζώνης» και το σχήμα (d) είναι ο ολικά αποκεντρωμένος έλεγχος, όπου το DC σημαίνει «κατανεμημένος ελεγκτής».

Στην ουσία, το blockchain είναι ένα αποκεντρωμένο σύστημα λογιστικής, το οποίο υποστηρίζεται από το δίκτυο υπολογιστών και τον μηχανισμό συναίνεσης. Στο πλαίσιο της εμπιστοσύνης (χωρίς τρίτο ως μεσάζοντα), οι πληροφορίες και τα δεδομένα καταγράφονται και αποθηκεύονται μέσω κατανεμημένου βιβλίου και τελικά ολοκληρώνεται η συναλλαγή peer-to-peer και ενημερώνεται το βιβλίο του λογαριασμού σε πραγματικό χρόνο. Από την άποψη της οικονομικής λογιστικής, το blockchain, ένα μεγάλο βιβλίο λογαριασμού δικτύου με προγράμματα υπολογιστών ως υποστηρικτική τεχνολογία, είναι χαρακτηριστικό των δημόσιων και διαφανών πληροφοριών. Εάν παίρνουμε blockchain ως το φυσικό βιβλίο λογαριασμών, τότε το ψηφιακό νόμισμα είναι η μονάδα λογιστικής στο blockchain. Κάθε τετράγωνο αντιστοιχεί στη σελίδα του φυσικού βιβλίου λογαριασμών και οι πληροφορίες που είναι αποθηκευμένες σε ένα μπλοκ είναι ισοδύναμες με τις δραστηριότητες συναλλαγής που καταγράφονται στη σελίδα του βιβλίου (Bartoletti & Pompianu, 2017).

Το μπλοκ είναι η μονάδα αποθήκευσης σε μπλοκ αλυσίδα, η οποία περιλαμβάνει τέσσερα κύρια στοιχεία, είναι η τιμή κατακερματισμού του προηγούμενου μπλοκ, η χρονική σήμανση του τρέχοντος μπλοκ, ο τυχαίος αριθμός που δημιουργήθηκε και ο αριθμός του κατακερματισμού στο τρέχον μπλοκ). Κάθε μπλοκ συνδέει το προηγούμενο μπλοκ με την τιμή κατακερματισμού του προηγούμενου μπλοκ και καταγράφει το χρόνο συναλλαγής μέσω της χρονικής σήμανσης. Και η απόδειξη εργασίας (Proof Of Work - POW), η οποία προκύπτει από τον υπολογισμό του μπλοκ, επιβραβεύεται για να ενθαρρύνει τους συμμετέχοντες στο σύστημα να παρέχουν συνεχή υπολογισμό. Τέλος, το δέντρο αριθμών της τιμής κατακερματισμού (“number tree of hash value”) στο τρέχον μπλοκ αντιπροσωπεύει τη συστοιχία κλειδιών των αποθηκευμένων πληροφοριών συναλλαγής (Bartoletti & Pompianu, 2017).

Κατά τη διάρκεια του περασμένου έτους, η έννοια των «ιδιωτικών μπλοκ αλυσίδων» έχει γίνει πολύ δημοφιλής στην ευρύτερη συζήτηση για την τεχνολογία blockchain. Ουσιαστικά, αντί να έχει μια πλήρως δημόσια και ανεξέλεγκτη δικτυακή και κρατική μηχανή ασφαλισμένη με κρυπτοοικονομική (π.χ. απόδειξη εργασίας, απόδειξη συμμετοχής), είναι επίσης δυνατό να δημιουργηθεί ένα σύστημα όπου τα δικαιώματα πρόσβασης ελέγχονται πιο στενά, με δικαιώματα τροποποίησης ή ακόμη και να διαβάσει την κατάσταση blockchain που περιορίζεται σε λίγους χρήστες, διατηρώντας παράλληλα πολλά είδη μερικών εγγυήσεων αυθεντικότητας και αποκέντρωσης που παρέχουν τα blockchains. Τέτοια συστήματα αποτελούσαν πρωταρχικό

στόχο συμφερόντων των χρηματοπιστωτικών ιδρυμάτων και οδήγησαν εν μέρει σε μια αντίδραση από όσους βλέπουν τέτοιες εξελίξεις είτε ως συμβιβασμούς σε ολόκληρο το σημείο της αποκέντρωσης είτε ως μια απεγνωσμένη πράξη των μεσολαβητών (Bartoletti & Pompianu, 2017).

3.1 Δημόσια Blockchain

Ένα δημόσιο blockchain είναι ένα blockchain που ο καθένας στον κόσμο μπορεί να διαβάσει, ο καθένας στον κόσμο μπορεί να στείλει συναλλαγές και να περιμένει να τις συμπεριλάβει αν είναι έγκυρες και οποιοσδήποτε στον κόσμο μπορεί να συμμετάσχει στη διαδικασία συναίνεσης - μπλοκ προστίθενται στην αλυσίδα και ποια είναι η τρέχουσα κατάσταση. Ως υποκατάστατο της κεντρικής ή ήμι-κεντρικής εμπιστοσύνης, τα δημόσια μπλοκ εμπορεύματα εξασφαλίζονται με την κρυπτοοικονομική - τον συνδυασμό οικονομικών κινήτρων και κρυπτογραφικής επαλήθευσης χρησιμοποιώντας μηχανισμούς όπως η απόδειξη εργασίας ή η απόδειξη συμμετοχής, ακολουθώντας μια γενική αρχή ότι ο βαθμός στον οποίο κάποιος μπορεί να έχει η επιρροή στη διαδικασία συναίνεσης είναι ανάλογη με την ποσότητα των οικονομικών πόρων που μπορούν να φέρουν. Αυτά τα μπλοκ αλυσίδες θεωρούνται γενικά "πλήρως αποκεντρωμένα" (Bartoletti & Pompianu, 2017).

3.2 Blockchain Κοινοπραξίας (Consortium)

Ένα blockchain της κοινοπραξίας είναι ένα blockchain όπου η διαδικασία συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων. Για παράδειγμα, μπορεί να φανταστεί κανείς μια κοινοπραξία 15 χρηματοπιστωτικών ιδρυμάτων, καθένα από τα οποία λειτουργεί έναν κόμβο και από τα οποία 10 πρέπει να υπογράψουν κάθε μπλοκ προκειμένου να είναι έγκυρο το μπλοκ. Το δικαίωμα ανάγνωσης του blockchain μπορεί να είναι δημόσιο ή να περιορίζεται στους συμμετέχοντες και υπάρχουν επίσης υβριδικές διαδρομές, που είναι δημόσιες μαζί με ένα API που επιτρέπει στα μέλη του κοινού να κάνουν έναν περιορισμένο αριθμό ερωτημάτων και να πάρετε πίσω κρυπτογραφικές αποδείξεις ορισμένων τμημάτων της κατάστασης blockchain. Αυτά τα μπλοκ αλυσίδες μπορούν να θεωρηθούν "μερικώς αποκεντρωμένα" (Bartoletti & Pompianu, 2017).

3.3 Ιδιωτικά Blockchain

Ένα πλήρως ιδιωτικό blockchain είναι ένα blockchain όπου τα δικαιώματα εγγραφής κρατούνται κεντρικά σε έναν οργανισμό. Τα δικαιώματα ανάγνωσης ενδέχεται να είναι δημόσια ή να περιορίζονται αυθαίρετα. Οι πιθανές εφαρμογές περιλαμβάνουν τη διαχείριση βάσεων

δεδομένων, τον έλεγχο κ.λπ. εσωτερικά σε μια ενιαία εταιρεία και, επομένως, η ευκρίνεια του κοινού μπορεί να μην είναι απαραίτητη σε πολλές περιπτώσεις, αν και σε άλλες περιπτώσεις είναι επιθυμητή η δημόσια εγγύηση (Bartoletti & Pompianu, 2017).

Σε γενικές γραμμές, μέχρι στιγμής δεν δόθηκε ιδιαίτερη έμφαση στη διάκριση μεταξύ μπλοκ αλυσίδων κοινοπραξίας και πλήρως ιδιωτικών μπλοκ αλυσίδων, αν και είναι σημαντικό: το πρώτο παρέχει ένα υβρίδιο μεταξύ της "χαμηλής εμπιστοσύνης" που παρέχεται από τα δημόσια μπλοκ και της "ενιαίας υψηλής εμπιστοσύνης οντότητας "Μοντέλο ιδιωτικών μπλοκ αλυσίδων, ενώ το τελευταίο μπορεί να περιγραφεί με μεγαλύτερη ακρίβεια ως ένα παραδοσιακό συγκεντρωτικό σύστημα με ένα βαθμό κρυπτογραφικής ελεγκτικότητας. Εντούτοις, σε κάποιο βαθμό υπάρχει ένας καλός λόγος για την επικέντρωση στην κοινοπραξία σε σχέση με την ιδιωτική: η θεμελιώδης αξία των μπλοκ αλυσίδων σε ένα πλήρως ιδιωτικό πλαίσιο, εκτός από τη λειτουργικότητα του μηχανισμού αναπαραγωγής, είναι κρυπτογραφική πιστοποίηση και δεν υπάρχει λόγος να πιστεύουμε ότι η βέλτιστη η μορφή μιας τέτοιας διάταξης εξακρίβωσης της γνησιότητας πρέπει να συνίσταται από μια σειρά πακέτων δεδομένων που συνδέονται με το hash που περιέχουν ρίζες δέντρων Merkle. Η γενικευμένη μηδενική τεχνολογία απόδειξης γνώσης παρέχει μια πολύ ευρύτερη σειρά συναρπαστικών δυνατοτήτων σχετικά με τα είδη των κρυπτογραφικών διαβεβαιώσεων που οι εφαρμογές μπορούν να παρέχουν στους χρήστες τους. Σε γενικές γραμμές, οι γενικευμένες αποδείξεις μηδενικής γνώσης είναι, στον εταιρικό χρηματοπιστωτικό κόσμο, πολύ υποβαθμισμένες σε σύγκριση με τα ιδιωτικά blockchains (Bartoletti & Pompianu, 2017).

3.4 Προτερήματα Ιδιωτικού και Δημόσιου Blockchain

Σε σύγκριση με τα δημοφιλή μπλοκ, τα ιδιωτικά blockchains έχουν πολλά πλεονεκτήματα (Guegan, 2017):

- Η κοινοπραξία ή η εταιρεία που εκμεταλλεύεται ένα ιδιωτικό blockchain μπορεί εύκολα, αν το επιθυμεί, να αλλάξει τους κανόνες ενός blockchain, να επαναφέρει τις συναλλαγές, να τροποποιήσει τα υπόλοιπα κ.λπ. Σε ορισμένες περιπτώσεις, π.χ. εθνικών κτηματολογίων, η λειτουργία αυτή είναι απαραίτητη · δεν υπάρχει κανένας τρόπος για να υπάρξει ένα σύστημα όπου ο Dread Pirate Roberts μπορεί να έχει νόμιμα δικαιώματα ιδιοκτησίας πάνω σε ένα απλά ορατό κομμάτι γης και επομένως μια προσπάθεια δημιουργίας ενός ανεξέλεγκτου κτηματολογικού μητρώου στην πράξη θα μεταφερθεί στην πράξη γρήγορα σε ένα που δεν αναγνωρίζεται από την ίδια την κυβέρνηση. Φυσικά,

μπορεί κανείς να υποστηρίξει ότι μπορούμε να το κάνουμε αυτό σε ένα δημόσιο blockchain δίνοντας στην κυβέρνηση ένα backdoor κλειδί σε μια σύμβαση; το αντίθετο επιχείρημα είναι ότι μια τέτοια προσέγγιση είναι ουσιαστικά μια εναλλακτική λύση Rube Goldbergian για την πιο αποτελεσματική πορεία της κατοχής ενός ιδιωτικού blockchain, αν και υπάρχει με τη σειρά του ένα μερικό αντίστροφο επιχείρημα.

- Οι έλεγχοι επικύρωσης είναι γνωστοί, επομένως δεν ισχύει οποιοσδήποτε κίνδυνος επίθεσης κατά 51% που προέρχεται από κάποια αθέμιτη σύμπραξη στην Κίνα.
- Οι συναλλαγές είναι φθηνότερες, αφού χρειάζεται να επαληθευτούν μόνο από λίγους κόμβους που μπορούν να εμπιστευτούν ότι έχουν πολύ υψηλή επεξεργαστική ισχύ και δεν χρειάζεται να επαληθεύονται από δέκα χιλιάδες φορητούς υπολογιστές. Αυτό είναι ένα τεράστιο ενδιαφέρον τώρα, καθώς τα δημόσια blockchains τείνουν να έχουν τέλη συναλλαγών που ξεπερνούν τα $ 0.01 ανά tx, αλλά είναι σημαντικό να σημειωθεί ότι μπορεί να μεταβληθεί μακροπρόθεσμα με την κλιμακωτή τεχνολογία blockchain που υπόσχεται να μειώσει το κόστος του blockchain μέσα σε μία ή δύο τάξεις ενός βέλτιστα αποτελεσματικού ιδιωτικού συστήματος blockchain.
- Οι κόμβοι μπορούν να είναι πολύ καλά συνδεδεμένοι και τα σφάλματα μπορούν γρήγορα να διορθωθούν με χειρωνακτική παρέμβαση, επιτρέποντας τη χρήση αλγόριθμων συναίνεσης που προσφέρουν το τελικό αποτέλεσμα μετά από πολύ μικρότερους χρόνους μπλοκ. Οι βελτιώσεις στη δημόσια τεχνολογία blockchain, όπως η έννοια του Ethereum 1.0 και η μεταγενέστερη απόδειξη του ποσοστού, μπορούν να φέρουν τα δημόσια blockchain πολύ πιο κοντά στο ιδανικό "άμεσο επιβεβαίωση" (π.χ., προσφέροντας τελικό μετά από 15 δευτερόλεπτα αντί για 99,9999% ώρες, όπως και ο Bitcoin), αλλά ακόμη και τα ιδιωτικά blockchains θα είναι πάντα ταχύτερα και η διαφορά λανθάνουσας κατάστασης δεν εξαφανίζεται ποτέ, καθώς δυστυχώς η ταχύτητα του φωτός δεν αυξάνεται κατά 2x ανά διετία από το νόμο του Moore.
- Εάν τα δικαιώματα ανάγνωσης είναι περιορισμένα, τα ιδιωτικά blockchains μπορούν να παρέχουν μεγαλύτερο επίπεδο προστασίας προσωπικών δεδομένων.

Δεδομένων όλων αυτών, μπορεί να φανεί ότι τα ιδιωτικά blockchains είναι αναμφισβήτητα μια καλύτερη επιλογή για τα ιδρύματα. Ωστόσο, ακόμη και σε ένα θεσμικό πλαίσιο, τα δημόσια μπλοκ έχουν ακόμα πολύτιμη αξία και στην πραγματικότητα αυτή η αξία βρίσκεται σε σημαντικό βαθμό στις φιλοσοφικές αρετές που προωθούν οι υποστηρικτές των δημοσίων μπλοκ αλυσίδων, μεταξύ των οποίων πρωταγωνιστές είναι η ελευθερία, ουδετερότητα και διαφάνεια. Τα

πλεονεκτήματα των δημόσιων αποκλεισμών γενικά εμπίπτουν σε δύο μεγάλες κατηγορίες (Guegan, 2017):

Τα δημόσια blockcards παρέχουν έναν τρόπο προστασίας των χρηστών μιας εφαρμογής από τους προγραμματιστές, διαπιστώνοντας ότι υπάρχουν ορισμένα πράγματα που ακόμη και οι προγραμματιστές μιας εφαρμογής δεν έχουν εξουσία να κάνουν. Από μια αφελούς άποψη, μπορεί να είναι δύσκολο να καταλάβουμε γιατί ένας προγραμματιστής εφαρμογών θα ήθελε να εγκαταλείψει οικειοθελώς την εξουσία και να υποχωρήσει. Ωστόσο, η πιο προηγμένη οικονομική ανάλυση παρέχει δύο λόγους για τους οποίους, σύμφωνα με τα λόγια του Thomas Schelling, η αδυναμία μπορεί να είναι μια δύναμη. Πρώτον, εάν ο χρήστης κάνει πιο δύσκολο ή αδύνατο για τον εαυτό του να κάνει κάποια πράγματα, τότε οι άλλοι θα έχουν περισσότερες πιθανότητες να τους εμπιστεύονται και να αλληλεπιδρούν μαζί τους, καθώς είναι σίγουροι ότι αυτά τα πράγματα είναι λιγότερο πιθανό να συμβούν σε αυτά. Δεύτερον, αν αυτοί εξαναγκαστούν ή πιεστούν από μια άλλη οντότητα, τότε λέγοντας ότι «δεν έχω καμία εξουσία να το κάνω αυτό ακόμα κι αν ήθελα» είναι ένα σημαντικό κομμάτι διαπραγμάτευσης, καθώς αποθαρρύνει την εν λόγω οντότητα από το να προσπαθεί να τις αναγκάσει να το κάνει. Μια μεγάλη κατηγορία πίεσης ή εξαναγκασμού που οι προγραμματιστές εφαρμογών κινδυνεύουν είναι ότι από τις κυβερνήσεις, έτσι η «αντίσταση λογοκρισίας» δεσμεύεται έντονα σε αυτό το είδος επιχείρησης.

Τα δημόσια blockchains είναι ανοικτά και επομένως είναι πιθανό να χρησιμοποιηθούν από πάρα πολλές οντότητες και να αποκτήσουν κάποια εφέ δικτύου.

3.5 Data Hashing & Blockchain Anchoring

Μια κρυπτογραφική συνάρτηση κατακερματισμού είναι ένας μαθηματικός αλγόριθμος που χαρτογραφεί δεδομένα αυθαίρετου μεγέθους σε ένα string bit σταθερού μεγέθους (hash) και έχει σχεδιαστεί για να είναι μια λειτουργία μονής κατεύθυνσης, δηλαδή μια λειτουργία που είναι ανέφικτη να αναστρέφεται. η λειτουργία λαμβάνει μια είσοδο (ή 'μήνυμα') και επιστρέφει μια αλφαριθμητική συμβολοσειρά σταθερού μεγέθους. Το string ονομάζεται "άθροισμα κατακερματισμού", "τιμή κατακερματισμού", "ψηφιακό δακτυλικό αποτύπωμα", "digest" ή "checksum". Η ιδανική συνάρτηση κατακερματισμού έχει τρεις κύριες ιδιότητες: (i) είναι εύκολο να υπολογιστεί ένα hash για οποιαδήποτε δεδομένα, (ii) είναι εξαιρετικά δύσκολο (υπολογιστικά) να υπολογιστεί ένα αλφαριθμητικό κείμενο που έχει ένα συγκεκριμένο hash, (iii)

είναι εξαιρετικά απίθανο τα δύο ελαφρώς διαφορετικά μηνύματα να έχουν το ίδιο hash [Gupta, 2017].

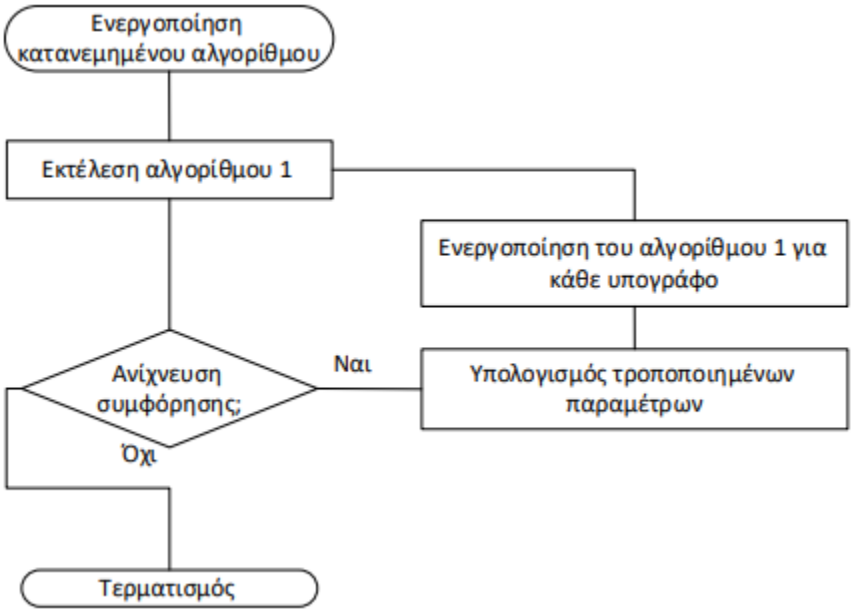
Επιπλέον, εάν εφαρμόζεται η ίδια λειτουργία κατακερματισμού στα ίδια δεδομένα, δίνει πάντα σε κάθε χρήστη που ενεργεί ανεξάρτητα το ίδιο ποσό κατακερματισμού με το αποτέλεσμα ανά πάσα στιγμή. Από την άποψη των δημόσιων μητρώων, εάν το άθροισμα κατακερματισμού μιας καταχώρησης αποθηκεύεται με ασφάλεια, τότε επιτρέπει να αποκαλυφθούν τυχόν περαιτέρω αλλαγές στην αρχική καταχώριση. Έτσι, είναι χρήσιμο στην έκθεση πλαστογραφίας, αν και δεν προστατεύει τα ίδια τα δεδομένα. Η εισαγωγή δεδομένων είναι μία από τις πρώτες χρήσιμες εφαρμογές του blockchain πέρα από τη διαφημιστική εκστρατεία των κρυπτοσυχνοτήτων. Σε γενικές γραμμές, ο κατακερματισμός στο blockchain αναφέρεται στην εισαγωγή ενός ποσού κατακερματισμού σε μια συναλλαγή blockchain. Η ένθεση υποδηλώνει ότι τα δεδομένα "δημοσιεύονται στο βιβλίο και δεν μπορούν να λογοκρίνονται ή να αποσύρονται και θα είναι μόνιμα διαθέσιμα στον κόσμο" [Seok et al, 2019]

3.6 Κρυπτογράφηση

Ένα blockchain συνήθως χρησιμοποιεί κρυπτοσυστήματα δημόσιου κλειδιού για την εξασφάλιση ανταλλαγών πληροφοριών μεταξύ των μερών μέσω της επικύρωσης των συναλλαγών μέσω ψηφιακών υπογραφών. Κατά τη διαδικασία υπογραφής, ο υπογράφων υπογράφει με ιδιωτικό κλειδί, ενώ το δημόσιο κλειδί, το οποίο μοιράζεται δημοσίως, χρησιμοποιείται για να επαληθεύσει ότι η υπογραφή είναι έγκυρη. Έτσι, όταν ο αλγόριθμος υπογραφής είναι ασφαλής, διασφαλίζεται ότι μόνο το άτομο με ιδιωτικό κλειδί θα μπορούσε να έχει δημιουργήσει κάποια υπογραφή. Για παράδειγμα, το Bitcoin χρησιμοποιεί υπογραφές ECDSA με την καμπύλη Koblitz, η οποία εξαρτάται από ένα ιδιωτικό κλειδί για την υπογραφή μηνυμάτων και από το αντίστοιχο δημόσιο κλειδί για τον έλεγχο της υπογραφής. Η κρυπτογραφία δημόσιου κλειδιού είναι επίσης απαραίτητη για τα επονομαζόμενα πορτοφόλια, τα οποία είναι ιδιωτικά κλειδιά που αποθηκεύουν αρχεία και απλά δεδομένα. Έτσι, σε ένα σύστημα blockchain κάθε χρήστης έχει ένα πορτοφόλι που συνδέεται με τουλάχιστον μια δημόσια διεύθυνση (συνήθως ένα hash του δημόσιου κλειδιού του χρήστη) και ένα ιδιωτικό κλειδί που ο χρήστης χρειάζεται για υπογραφή συναλλαγών. Για παράδειγμα, σε blockchains όπως το Bitcoin κάθε συναλλαγή καταλήγει να «αποστέλλεται» στην δημόσια διεύθυνση του δέκτη και να υπογράφεται με το ιδιωτικό κλειδί του αποστολέα. Για να ξοδέψουν τα bitcoins, ο ιδιοκτήτης τους πρέπει να αποδείξει την ιδιοκτησία ενός ιδιωτικού κλειδιού. Για να επαληθευτεί η αυθεντικότητα του ληφθέντος νομίσματος, κάθε οντότητα που λαμβάνει bitcoins επαληθεύει

την ψηφιακή υπογραφή του χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (Lin & Liao, 2017).

Διάγραμμα 3 – Ροή Μεθόδου κατανεμημένης οικονομικής ΚΦ με όρια υπερφόρτωσης των γραμμών (Kouveliotis, 2019)



4 Σύγκριση Πλαισίων Blockchain

Εάν χρησιμοποιήσουμε την προσέγγιση των δεδομένων hash και την επεκτείνουμε με την αγκύρωση του blockchain, τα δεδομένα πρέπει να αποθηκευτούν σε ένα ιδιωτικό blockchain, το οποίο μπορεί να αγκυροβοληθεί σε ένα δημόσιο blockchain. Για να βοηθήσουν στην οικοδόμηση ιδιωτικών μπλοκ αλυσίδων, πολλές εταιρείες δημιούργησαν πλαίσια για την κατασκευή μπλοκ αλυσίδων, το καθένα με τα δικά του ξεχωριστά χαρακτηριστικά. Τρία από τα μεγαλύτερα από αυτά τα πλαίσια είναι το Hyperledger Sawtooth, το Hyperledger Fabric και το Quorum.

4.1 Hyperledger Sawtooth

Το Hyperledger Sawtooth είναι ένα πλαίσιο στην οικογένεια Hyperledger, το οποίο επικεντρώνεται στη σπονδυλωτότητα και την ευελιξία [Cachin, 2016]. Ως εκ τούτου, επιτρέπει στον δημιουργό του blockchain να χρησιμοποιεί το δικό του αλγόριθμο συναίνεσης, εφαρμόζοντας μια ξεχωριστή διεπαφή για τη δημοσίευση ενός μπλοκ, την επαλήθευση αυτού του μπλοκ και την επίλυση των πιρουνιών [Cachin, 2016]. Παρόλο που ο Sawtooth παρέχει αυτές τις δυνατότητες, περιλαμβάνει επίσης τον δικό του αλγόριθμο συναίνεσης, Proof-of-Elapsed-Time, ο οποίος λειτουργεί με τυχαία λειτουργία λαχειοφόρων αγορών [Cachin, 2016]. Ένα άλλο χαρακτηριστικό γνώρισμα του Hyperledger Sawtooth είναι η δυνατότητα συναλλαγών παρτίδας. Όταν ένας χρήστης υποβάλλει συναλλαγές, αυτό γίνεται πάντα σε μια παρτίδα, αν και μια παρτίδα μπορεί να περιέχει μόνο μία συναλλαγή [Cachin, 2016].

Αυτές οι παρτίδες στη συνέχεια υποβάλλονται σε έναν κόμβο επικύρωσης, ο οποίος ελέγχει την (προκαθορισμένη) εγκυρότητα όλων των συναλλαγών μέσα στην παρτίδα. Εάν κάποια από τις συναλλαγές εντός της παρτίδας ακυρωθεί, ολόκληρη η παρτίδα απορρίπτεται. Εάν όλες οι συναλλαγές θεωρούνται έγκυρες, εφαρμόζονται από τον κόμβο επικύρωσης και προστίθενται στο blockchain [Cachin, 2016]. Στη συνέχεια, ο Sawtooth ορίζει τις οικογένειες συναλλαγών ως τον τρόπο αλλαγής της κατάστασης του blockchain. Αυτές οι οικογένειες συναλλαγών είναι καθορισμένες ομάδες λειτουργιών που επιτρέπονται στο blockchain. Περιορίζοντας το ποσό των πράξεων που επιτρέπονται σε μια οικογένεια συναλλαγών, η Sawtooth μπορεί να μειώσει τον κίνδυνο σε λάθη με αυτές τις συναλλαγές [Androulaki et al, 2018]. Το Sawtooth έχει πολλές προκαθορισμένες οικογένειες συναλλαγών που μπορούν να χρησιμοποιηθούν εύκολα μέσα σε μπλοκ αλυσίδες που είναι χτισμένα επάνω του, από την οικογένεια Integer Key με μόνο την

αύξηση, μείωση και ρύθμιση των λειτουργιών, σε μια πλήρη οικογένεια συναλλαγών EVM [Androulaki et al, 2018].

Εκτός από αυτές τις οικογένειες συναλλαγών, οι φορείς εκμετάλλευσης δικτύων μπορούν να ορίσουν τις δικές τους οικογένειες συναλλαγών με την εφαρμογή ενός λεγόμενου επεξεργαστή συναλλαγών, ο οποίος μπορεί να προγραμματιστεί σε διάφορες γλώσσες προγραμματισμού [Androulaki et al, 2018]. Επιλέγοντας τις επιτρεπόμενες οικογένειες συναλλαγών μέσα στο δίκτυο, είναι δυνατό να επιλέξετε το επίπεδο ευελιξίας / κινδύνου που ισχύει για το συγκεκριμένο δίκτυο [Androulaki et al, 2018]. Τέλος, οι εφαρμογές είναι σε θέση να διασυνδέονται με ένα blockwain Sawtooth μέσω ενός σαφώς καθορισμένου και σαφώς τεκμηριωμένου API REST και το Sawtooth προσφέρει SDK σε πολλές γλώσσες για να βοηθήσει στην ανάπτυξη [Androulaki et al, 2018].

4.2 Hyperledger Fabric

Το Hyperledger Fabric είναι παρόμοιο με το Hyperledger Sawtooth με τον τρόπο που επιτρέπει προσαρμοσμένους αλγόριθμους για συναίνεση και επίσης για επαλήθευση ταυτότητας. Η συναίνεση στο Hyperledger Fabric χωρίζεται σε τρία στάδια: επικύρωση, παραγγελία, επικύρωση και δέσμευση [Androulaki et al, 2018]. Όταν μια συναλλαγή προτείνεται από έναν πελάτη, αποστέλλεται στην υπογραφή συνομιλητών. Αυτοί οι συνομιλητές ομολογούν τη συναλλαγή και επιστρέφουν τα λεγόμενα σύνολα RW, τα οποία καταγράφουν όλα τα δεδομένα από τα οποία διαβάζεται η συναλλαγή και τα γράφουν στην παγκόσμια πολιτεία [Androulaki et al, 2018]. Εάν η συναλλαγή περνά την προκαθορισμένη πολιτική επικύρωσης (π.χ. μια πλειοψηφία των συνομηλίκων πρέπει να υποστηρίξει μια συναλλαγή), η συναλλαγή που έχει εγκριθεί αποστέλλεται σε μια υπηρεσία παραγγελιών [Androulaki et al, 2018]. Αυτή η υπηρεσία παραγγελιών καθορίζει τη σειρά με την οποία οι συναλλαγές προστίθενται σε ένα μπλοκ [Androulaki et al, 2018].

Η υλοποίηση αυτής της υπηρεσίας παραγγελιών μπορεί να προσαρμοστεί από τον δημιουργό του δικτύου. η προεπιλεγμένη υλοποίηση της υπηρεσίας παραγγελίας βασίζεται στον Apache Kafka [Androulaki et al, 2018]. Ενώ αυτή η υπηρεσία προεπιλογής παραγγελιών είναι ανεκτική σε σύγκρουση, δεν είναι ακόμα βολική για την ανοχή βλάβης και αυτό είναι ένα από τα επόμενα μεγάλα βήματα που το Hyperledger Fabric εργάζεται προς την κατεύθυνση [Androulaki et al, 2018]. Μετά την παραγγελία, οι συναλλαγές μεταφέρονται πίσω στους ομοτίμους συναδέλφους, καθώς και στη δέσμευση συνομηλίκων. Αυτοί οι συμμαθητές επιβεβαιώνουν για

μια ακόμη φορά ότι τα σύνολα RW των συναλλαγών εξακολουθούν να ταιριάζουν με την τρέχουσα παγκόσμια πολιτεία, με βάση την οποία επικυρώνουν ή ακυρώνουν τη συναλλαγή και δεσμεύονται στο blockchain. Ακόμη και όταν ακυρωθούν, θα καταγράφονται ακόμα στο blockchain, αλλά έχουν επισημανθεί ως μη έγκυρα και δεν θα εκτελεστούν [Androulaki et al, 2018]. Ένα από τα πιο σημαντικά χαρακτηριστικά γνωρίσματα του Hyperledger Fabric είναι η δυνατότητα δημιουργίας καναλιών, τα οποία είναι πλήρεις χωριστές μπλοκ αλυσίδες στο ίδιο δίκτυο [Androulaki et al, 2018]. Με τον περιορισμό του ποιος μπορεί να συμμετάσχει σε ορισμένα κανάλια του δικτύου, είναι δυνατό να διατηρηθούν ορισμένες συναλλαγές ιδιωτικές μεταξύ των εμπλεκομένων μερών μέσα στο κανάλι. Τέλος, η λογική συναλλαγών και τα έξυπνα συμβόλαια στο Hyperledger Fabric ονομάζονται chaincode και είναι γραμμένα στο Go [Androulaki et al, 2018].

Οι επικλήσεις αλυσιδωτού κώδικα εκτελούν συναλλαγές έναντι των δεδομένων της τρέχουσας κατάστασης. Για να γίνει αυτό πιο αποτελεσματικό, τα πιο πρόσφατα ζεύγη κλειδιών / τιμών για όλα τα στοιχεία ενεργητικού αποθηκεύονται σε μια βάση δεδομένων LevelDB [Androulaki et al, 2018]. Αυτή η βάση δεδομένων είναι μια ευρετηριακή προβολή στις δεσμευμένες συναλλαγές του blockchain και μπορεί πάντα να αναγεννηθεί με την αναπαραγωγή όλων των συναλλαγών. Οι εφαρμογές μπορούν να αλληλεπιδρούν με ένα μπλοκ αλυσίδας Fabric μέσω ενός κόμβου ή ενός Java SDK και πολλά άλλα SDK αναπτύσσονται ενεργά [Cachin, 2016].

4.3 Quorum

Το Quorum είναι ένα blockchain πλαίσιο που δημιουργήθηκε από τον J.P. Morgan ως έναν τρόπο δημιουργίας επιτρεπόμενων εκδόσεων του μπλοκ αλυσίδας Ethereum. Κατά την εφαρμογή τους επικεντρώθηκαν στην παραμονή πολύ κοντά στην αρχική εφαρμογή του Ethereum, ώστε οι προγραμματιστές της Ethereum να μην έχουν κανένα πρόβλημα να μεταβούν στην Quorum. Ο μηχανισμός έξυπνων συμβολαίων είναι πολύ παρόμοιος με αυτόν της εταιρείας Ethereum και είναι δυνατή η εκτέλεση τακτικών έξυπνων συμβάσεων του Ethereum σε δίκτυο Quorum χωρίς τροποποιήσεις [Androulaki]. Δεδομένου ότι η Quorum προορίζεται να χρησιμοποιηθεί για ιδιωτικά εξουσιοδοτημένα blockchains, προσφέρουν διαφορετικά είδη αλγόριθμων συναίνεσης ανάλογα με τις ανάγκες του δικτύου. Το πρώτο βασίζεται στο πρωτόκολλο Raft 1, το οποίο λειτουργεί με την εκλογή ενός ηγέτη, ο οποίος είναι ο μόνος δημιουργός μπλοκ μέσα στο δίκτυο (Papenfort & Bassler, 2016). Αυτό επιτρέπει την υψηλή απόδοση μέσα στο δίκτυο, αλλά δεν είναι ανεκτική για “Byzantine Fault Tolerant”, επομένως δεν είναι βιώσιμη σε κάθε περίπτωση. Ως εναλλακτική λύση, η Quorum εφαρμόζει το πρωτόκολλο συναίνεσης Instabul BFT, το οποίο

λειτουργεί επιλέγοντας έναν νέο κόμβο επικύρωσης ως προτείνοντα κάθε μπλοκ (Papenfort & Bassler, 2016).

Αυτή η επιλογή γίνεται με τρόπο στρογγυλό, που σημαίνει ότι επιλέγονται το ένα μετά το άλλο, με κυκλικό τρόπο. Αυτός ο προτείνων μεταδίδει στη συνέχεια μια νέα πρόταση μπλοκ στους άλλους κόμβους επικύρωσης, οι οποίοι όλες επικυρώνουν την πρόταση μπλοκ (Papenfort & Bassler, 2016). Αφού γίνει, μεταδίδουν ένα μήνυμα COMMIT σε όλους τους άλλους κόμβους. Στη συνέχεια, όταν ένας κόμβος έχει λάβει ένα μήνυμα COMMIT από τουλάχιστον τα δύο τρίτα όλων των επικυρωτών, το μπλοκ εισάγεται στο blockchain (Papenfort & Bassler, 2016). Τέλος, ένα από τα πιο σημαντικά χαρακτηριστικά της Quorum είναι η προσθήκη ιδιωτικών συναλλαγών στο blockchain τους. Το Hyperledger Fabric προσφέρει επίσης ιδιωτικές συναλλαγές, αλλά οι μέθοδοι Quorom και Fabric για να επιτευχθεί αυτό είναι τελείως διαφορετικές. Ενώ το Fabric χρησιμοποιεί κανάλια, η Quorum διαθέτει ξεχωριστό Διαχειριστή Συναλλαγών, ο οποίος παρακολουθεί τα άτομα που έχουν πρόσβαση σε ορισμένες συναλλαγές (Papenfort & Bassler, 2016). Πριν από τη μετάδοση μιας τέτοιας συναλλαγής, ένας κόμβος αντικαθιστά αρχικά το αρχικό φορτίο συναλλαγής με ένα hash της κρυπτογραφημένης έκδοσης του ωφέλιμου φορτίου που λαμβάνει από το Διαχειριστή Συναλλαγών. Τα μέρη που περιλαμβάνονται στους αποδέκτες της συναλλαγής θα λάβουν στη συνέχεια το πραγματικό ωφέλιμο φορτίο, ενώ άλλα θα δουν μόνο το hash (Papenfort & Bassler, 2016).

4.4 Smart Contracts στον Έλεγχο

Οι τρέχουσες μεθοδολογίες ελέγχου προδιαγράφουν 1) δειγματοληψία συναλλαγών για τη συλλογή ελεγκτικών τεκμηρίων σχετικά με τον κίνδυνο ουσιώδους ανακρίβειας, 2) μια οπτική προσέγγιση του ελέγχου και 3) μια ετήσια γνωμοδότηση με χρονική βάση. Σε μια σύγχρονη οικονομία όπου οι βάσεις δεδομένων αποθηκεύουν χιλιάδες καθημερινές συναλλαγές που ενδέχεται να εκτίθενται σε επιθέσεις στον κυβερνοχώρο, είναι απαραίτητο το παραδοσιακό μοντέλο ελέγχου να εξελιχθεί καθώς οι έλεγχοι των οικονομικών καταστάσεων γίνονται προοδευτικά αυτοματοποιημένοι και προληπτικοί.

Ως εκ τούτου, είναι ζωτικής σημασίας για τους εξωτερικούς ελεγκτές να εξετάσουν τον αντίκτυπο των εξελιγμένων αναλυτικών ελεγκτικών συστημάτων καθώς και άλλων αναδυόμενων τεχνολογιών, συμπεριλαμβανομένων των έξυπνων συμβάσεων και του blockchain, προκειμένου να παραμείνουν σχετικοί και να συνεχίσουν να προσθέτουν αξία στο κοινό, διενεργώντας ελέγχους υψηλής ποιότητας σε μεγάλο βαθμό πολύπλοκο οικοσύστημα.

Καθώς οι επιχειρηματικοί οργανισμοί συνεχίζουν να υιοθετούν δεσμευτικές συμβάσεις και έξυπνες συμβάσεις για τη βελτίωση της αποτελεσματικότητας των επιχειρηματικών διαδικασιών (Tapscott και Tapscott, 2016), είναι σημαντικό οι εξωτερικοί ελεγκτές να κατανοήσουν τις ευκαιρίες και τις προκλήσεις που προσφέρουν αυτές οι τεχνολογίες (Dai and Vasarhelyi, 2017, Rozario and Thomas, 2017). Επί του παρόντος, οι ελεγκτές έχουν την επιλογή να αναπτύσσουν εργαλεία ανάλυσης δεδομένων εσωτερικά ή να αγοράζουν εργαλεία ανάλυσης δεδομένων από προμηθευτές λογισμικού ελέγχου, όπως το IDEA ή το ACL. Ωστόσο, αυτά τα εργαλεία ανάλυσης δεδομένων υπάρχουν σε διαφορετικές πλατφόρμες, συμπεριλαμβανομένων πλατφορμών ιδιωτικής εταιρείας ελέγχου και πλατφόρμων προμηθευτών. Επιπλέον, η ενσωμάτωση πολλών αναλυτικών εργαλείων ελέγχου θα ήταν απαραίτητη για την ικανοποίηση των αιτημάτων των κατοχυρωμένων μερών για πιο έγκαιρη αναφορά και διαφάνεια του ελέγχου (Romero et al., 2012, No και Vasarhelyi, 2017).

Ως αποτέλεσμα, παρόλο που αυτά τα αναλυτικά εργαλεία ελέγχου θα μπορούσαν να μεταφορτωθούν από τον ελεγκτή στο νέφος και να δημοσιοποιηθούν σε κατοχυρωμένα μέρη, η εξοικονόμηση των αποτελεσμάτων των διαδικασιών ελέγχου στο σύννεφο σε πραγματικό χρόνο θα μπορούσε να αποδειχθεί επαχθής έλεγχος έργο. Δεδομένου ότι ο προγραμματισμός ενός ελέγχου απαιτεί αρκετές εκτιμήσεις κόστους / οφέλους, συμπεριλαμβανομένων των λογαριασμών που πρέπει να εξεταστούν, τη φύση, το χρονοδιάγραμμα και την έκταση των ελεγκτικών διαδικασιών (Louwers et al., 2013, Badertscher et al., 2017) προς την κατεύθυνση ενός αναλυτικού εργαλείου αναλυτικού εργαλείου αναλυτικού εργαλείου που θα επιτρέπει την αναφορά στο οικοσύστημα, δεν θα ήταν εφικτή από τη στάση κόστους / οφέλους. Δεδομένης της εγγενής πολυπλοκότητας της προσαρμογής των υφιστάμενων τεχνολογιών ώστε να αντικατοπτρίζεται ένα προληπτικό και πιο διαφανές μοντέλο ελέγχου, είναι σημαντικό να εξεταστούν οι συνέπειες των αναλύσεων λογιστικού ελέγχου βάσει έξυπνων συμβάσεων (εφεξής "έξυπνες διαδικασίες ελέγχου"). Ουσιαστικά, οι έξυπνες συμβάσεις που αναπτύσσονται σε ένα blockchain που δημιουργείται από τον εξωτερικό ελεγκτή μπορούν να διευκολύνουν την εκτέλεση των ελεγκτικών διαδικασιών και ταυτόχρονα να παρέχουν πληρέστερη αναφορά στον έλεγχο σε πραγματικό χρόνο και μεγαλύτερη διαφάνεια στους ενδιαφερόμενους (Rozario and Thomas, 2017). Από τώρα και στο εξής, η έννοια των έξυπνων συμβολαίων επεκτείνεται ώστε να περιλαμβάνει έξυπνες διαδικασίες ελέγχου που βοηθούν τους εξωτερικούς ελεγκτές να προσφέρουν αποτελεσματικότερους και αποτελεσματικότερους ελέγχους.

Οι έξυπνες διαδικασίες ελέγχου είναι αυτόνομες διαδικασίες ελέγχου, συμπεριλαμβανομένων αυτοτελών δοκιμών εσωτερικού ελέγχου (εφεξής "έξυπνοι έλεγχοι ελέγχου") και αυτόνομων αναλυτικών διαδικασιών (στο εξής "έξυπνες αναλυτικές διαδικασίες"), οι οποίες αναπτύσσονται στον μπλοκ αλυσίδας του εξωτερικού ελεγκτή. Η ανάπτυξη διαδικασιών έξυπνων ελέγχων στο κατανεμημένο βιβλίο κατακερματισμού θα οδηγούσε σε πληρέστερη αναφορά σε λογιστικό έλεγχο σε πραγματικό χρόνο για πολλούς ενδιαφερόμενους, όπως βασικούς επενδυτές, προμηθευτές, επιθεωρητές ελέγχου, SEC και επιτροπή ελέγχου. Δεδομένου ότι το blockchain παρέχει μια πλατφόρμα για την εκτέλεση έξυπνων διαδικασιών ελέγχου και κοντά σε εκθέσεις ελέγχου σε πραγματικό χρόνο, αυτές οι νέες διαδικασίες ελέγχου έχουν μεγάλες δυνατότητες να βελτιώσουν την ποιότητα του ελέγχου, επιτρέποντας στους ελεγκτές να εκτελούν αποτελεσματικότερα τις διαδικασίες ελέγχου και ως εκ τούτου, πόρους σε περιοχές υψηλότερου κινδύνου. Τέλος, καθώς οι έξυπνες διαδικασίες ελέγχου θα διανεμηθούν στους συμμετέχοντες κόμβους στο blockchain του ελεγκτή, σε πραγματικό χρόνο, θα συμβάλουν στην κάλυψη των αναγκών μεγαλύτερης διαφάνειας και έγκαιρης υποβολής εκθέσεων ελέγχου.

Οι έξυπνες συμβάσεις εισήχθησαν για πρώτη φορά από την Szabo (1994) ως ένα «πρωτόκολλο ηλεκτρονικής συναλλαγής που εκτελεί τους όρους μιας σύμβασης», συμπεριλαμβανομένων των σταδίων εκτέλεσης, επαλήθευσης και απόδοσης της διαδικασίας σύναψης συμβάσεων. Ο Szabo περιγράφει έξυπνα συμβόλαια χρησιμοποιώντας ένα παράδειγμα μηχάνημα αυτόματης πώλησης για να περιγράψει τη λειτουργία τους στον πραγματικό κόσμο.

4.4.1 Smart Contract Αυτόματου Πωλητή

Ένα μηχάνημα αυτόματης πώλησης είναι μια έξυπνη σύμβαση μεταξύ ενός πελάτη και ενός πωλητή και έχει σχεδιαστεί για να δέχεται ένα σύνολο εισροών βάσει προκαθορισμένων κανόνων και εξόδων διανομής, δηλαδή τη μεταφορά ιδιοκτησίας, εάν πληρούνται αυτοί οι κανόνες. Ένας πελάτης θα εισάγει ένα συγκεκριμένο χρηματικό ποσό και θα επιλέξει ένα προϊόν. Στην περίπτωση αυτή, ο πελάτης θα εισάγει 5,00 δολάρια για να αγοράσει μια τσάντα με τσιπ που κοστίζει 3,00 δολάρια. Το έξυπνο συμβόλαιο ενεργοποιεί και αναζητά το προϊόν και την αντίστοιχη τιμή του. Εάν το προϊόν βρεθεί και η τιμή είναι ίση ή μικρότερη από το χρηματικό ποσό που παρείχε ο πελάτης, η έξυπνη σύμβαση θα μεταβιβάσει την ιδιοκτησία του προϊόντος απελευθερώνοντας το προϊόν στον πελάτη και επιστρέφοντας το διαφορικό για την τιμή του προϊόντος και το ποσό που παρέχει ο χρήστης, εάν τα χρήματα που παρέχει ο πελάτης υπερβαίνουν την τιμή του επιλεγμένου προϊόντος. Κατά συνέπεια, το μηχάνημα αυτόματης πώλησης απελευθερώνει μια τσάντα από τσιπ και αλλάζει $ 2,00 στον πελάτη και η συναλλαγή

μεταξύ του πωλητή και του πελάτη διευθετείται. Εάν το προϊόν δεν βρίσκεται ή εάν τα χρήματα που παρέχει ο χρήστης δεν επαρκούν για την αγορά του προϊόντος, η συναλλαγή δεν μπορεί να ολοκληρωθεί.

4.4.2 Blockchain Smart Contract

Αν και μια καινοτομία στις αρχές της δεκαετίας του 1990, οι έξυπνες συμβάσεις δεν ευδοκιμούσαν κατά τη διάρκεια αυτής της περιόδου, δεδομένου ότι ένας εξουσιοδοτημένος εμπιστευόμενος τρίτος ήταν απαραίτητος για την παρακολούθηση των όρων και της εκτέλεσης των κωδικοποιημένων συμβάσεων, πράγμα που δημιουργεί τον κίνδυνο να μην εκπληρώσει τις συμβατικές υποχρεώσεις του ένα συμβαλλόμενο μέρος (Kiviat, 2015). Με την τεχνολογία blockchain, η εκτέλεση έξυπνων συμβολαίων καθίσταται εφικτή καθώς οι αρμοδιότητες επίβλεψης διανέμονται στους συμμετέχοντες κόμβους (Buterin, 2014 · Dai and Vasarhelyi, 2017). Η προκαθορισμένη επιχειρησιακή λογική μπορεί να συμφωνηθεί από τα συμβαλλόμενα μέρη, προγραμματισμένη και αποθηκευμένη στο βιβλιαράκι. Στη συνέχεια, οι χρήστες μπλοκ αλυσίδων θα ενεργοποιούν το έξυπνο συμβόλαιο αποστέλλοντας δεδομένα σε αυτόν, τότε το έξυπνο συμβόλαιο θα επαληθεύει ότι οι πληροφορίες που λαμβάνονται είναι εντός των ορίων των προκαθορισμένων κανόνων και απελευθερώνουν μια έξοδο, όπως πληρωμή για αγαθά. Αν δεν πληρούνται οι συνθήκες, η έξοδος δεν απελευθερώνεται και εμφανίζεται ένα μήνυμα σφάλματος, που υποδεικνύει ότι η συναλλαγή δεν ολοκληρώθηκε. Η κατάσταση της έξυπνης σύμβασης θα είναι ορατή στα συμβαλλόμενα μέρη στο μπλοκ αλυσίδα, περιορίζοντας έτσι τον κίνδυνο αθέτησης υποχρέωσης από τον αντισυμβαλλόμενο.

Συνολικά, τα οφέλη από τις έξυπνες συμβάσεις στο blockchain περιλαμβάνουν 1) τη διαμεσολάβηση, καθώς δεν είναι απαραίτητο να επιλέγουμε προληπτικά μια εμπιστευτική κεντρική αρχή. 2) εμπιστοσύνη σε ένα περιβάλλον χωρίς εμπιστοσύνη, επειδή οι πληροφορίες είναι κρυπτογραφημένες και ορατές από τα συμβαλλόμενα μέρη στο blockchain. 3) τον μετριασμό του κινδύνου απάτης ή ανθρώπινου σφάλματος, διότι οι έξυπνες συμβάσεις πραγματοποιούν ακριβείς υπολογισμούς και 4) την αποτελεσματικότητα της διαδικασίας, καθώς οι έξυπνες συμβάσεις εκτελούνται αυτομάτως.

Συνεπώς, οι έξυπνες συμβάσεις είναι απλώς πράκτορες λογισμικού που εκτελούν αυτόματα εργασίες στο blockchain βάσει προκαθορισμένων συνθηκών που μιμούνται τις ενέργειες ενός ανθρώπινου χρήστη (Nwana and Ndumu, 1999, Vasarhelyi and Hoitash, 2005). Η έρευνα για το λογισμικό των πρακτορείων λογισμικού προηγήθηκε των έξυπνων συμβολαίων και του blockchain όπως εμφανίστηκε στη δεκαετία του '80 (Nwana and Ndumu, 1999) με σκοπό την

ανάπτυξη προγραμμάτων ηλεκτρονικών υπολογιστών που βοηθούν τον ανθρώπινο χρήστη στην παρακολούθηση των γεγονότων ή την εκτέλεση των καθηκόντων (Maes, 1994). Ως αποτέλεσμα, είναι φυσικό να επεκταθεί ο ορισμός των έξυπνων συμβολαίων ώστε να αντιπροσωπεύουν μια ποικιλία προγραμμάτων ηλεκτρονικών υπολογιστών που περιέχουν προκαθορισμένους κανόνες και εκτελούν καθήκοντα βάσει αυτών των κανόνων. Παρόλο που υπάρχουν γενικές εφαρμογές των έξυπνων συμβάσεων αποκλεισμού, συμπεριλαμβανομένου του αυτόματου διακανονισμού των χρηματοοικονομικών παραγώγων και της ασφαλούς μεταβίβασης τίτλων ιδιοκτησίας (DeCovny, 2015, Fanning and Centers, 2016), οι αιτήσεις στον τομέα του ελέγχου παραμένουν ανεξερεύνητες. Εφαρμόζεται στον τομέα του εξωτερικού ελέγχου, διευρύνεται ο ορισμός των έξυπνων συμβάσεων αποκλεισμού για να συμπεριλάβει έξυπνες διαδικασίες ελέγχου (π.χ. αναλύσεις ελεγκτικών τεκμηρίων) οι οποίες εκτελούνται αυτόνομα εκ μέρους του ελεγκτή με σκοπό τη βελτίωση της αποτελεσματικότητας του ελέγχου, της αποτελεσματικότητας και της ανταπόκρισης τις ενημερωτικές ανάγκες διαφόρων ενδιαφερόμενων μερών για πιο έγκαιρη και πιο διαφανή αναφορά ελέγχου.

Κάθε χρόνο, η PCAOB δημοσιεύει μια επιθεώρηση προσωπικού σχετικά με τις επιθεωρήσεις του τρέχοντος έτους, επισημαίνοντας περιοχές ελέγχου στις οποίες τα ελεγκτικά γραφεία ήταν ελλιπή. Οι τομείς αυτοί περιλαμβάνουν τον εσωτερικό έλεγχο της χρηματοοικονομικής πληροφόρησης, την επικύρωση των εκτιμήσεων της εύλογης αξίας και την ανταπόκριση σε κινδύνους σε σχέση με ουσιώδεις ανακρίβειες (PCAOB, 2017). Εφαρμόζοντας τον έλεγχο, τα οφέλη των έξυπνων ελεγκτικών διαδικασιών είναι επικείμενες, καθώς μπορούν να συμβάλουν στη μείωση του χάσματος αναμονής που υπάρχει σήμερα μεταξύ των ελεγκτών των διαδικασιών έναντι αυτών των διαδικασιών οι επιθεωρητές ελέγχου και οι ρυθμιστικές αρχές αναμένουν ότι θα εκτελέσουν.

Στον blockchain του εξωτερικού ελεγκτή, η ομάδα επιστημόνων δεδομένων της ελεγκτικής εταιρείας μπορεί να αναπτύξει έξυπνες διαδικασίες ελέγχου βάσει των ελεγκτικών διαδικασιών που έχουν συμφωνηθεί με τον ελεγκτικό ελεγκτή. Ουσιαστικά, αυτές οι έξυπνες διαδικασίες ελέγχου θα ελεγχθούν από τον επιθεωρητή για να μειωθεί το κενό προσδοκιών, επιτρέποντας παράλληλα την προληπτική επιθεώρηση ελέγχου2. Μόλις επιτευχθεί συναίνεση, οι έξυπνες διαδικασίες ελέγχου θα φορτωθούν στο blockchain και ο εξωτερικός ελεγκτής θα επικαλεστεί αυτές τις διαδικασίες στέλνοντας σχετικές ελεγκτικές αποδείξεις σε αυτές. Οι έξυπνες διαδικασίες ελέγχου και τα αποτελέσματά τους θα είναι ορατές από τον εξωτερικό ελεγκτή, ως ιδιοκτήτη του τμήματος ελέγχου και από τον ελεγκτή ελέγχου. Εξίσου σημαντικό, τα

εγγεγραμμένα μέρη, συμπεριλαμβανομένης της Επιτροπής Κεφαλαιαγοράς, των βασικών επενδυτών και της επιτροπής ελέγχου, θα μπορούσαν να έχουν περιορισμένη πρόσβαση για να αναθεωρήσουν τα συγκεντρωτικά αποτελέσματα των έξυπνων διαδικασιών ελέγχου, δίνοντας έμφαση σε τυχόν μηνύματα σφάλματος (κόκκινες σημαίες) , et al., 2006, Issa and Kogan, 2014). ως εκ τούτου, μείωση του χάσματος αναμονής μεταξύ ελεγκτών και χρηστών οικονομικών καταστάσεων σε κοντινή απόσταση από την εκδήλωση, τη σύγχρονη οικονομία. Επιπλέον, η ανασκόπηση των αποτελεσμάτων των έξυπνων διαδικασιών ελέγχου θα επέτρεπε στην Επιτροπή Κεφαλαιαγοράς να ακολουθεί μια προορατική προσέγγιση παρακολουθώντας τους πελάτες ελέγχου που ενδέχεται να απαιτούν επιθεώρηση ή εντοπίζοντας δυνητικούς δείκτες που ενδεχομένως να υποδηλώνουν οικονομική κρίση. Συλλογικά, η εφαρμογή έξυπνων διαδικασιών ελέγχου στο blockchain έχει τη δυνατότητα να βελτιώσει την ποιότητα του ελέγχου και να ανταποκριθεί στις απαιτήσεις διαφόρων μερών.

4.4.3 Λειτουργικότητα και Προσαρμοστικότητα των Blockchain Smart Contracts

Όπως αναφέρθηκε στην προηγούμενη ενότητα, υπάρχουν πολυάριθμες εφαρμογές έξυπνων συμβολαίων τύπου blockchain. Η πλατφόρμα Ethereum (Buterin, 2014) αντιπροσωπεύει μία από τις διάφορες πλατφόρμες που διευκολύνουν την ανάπτυξη και εκτέλεση μιας ποικιλίας έξυπνων συμβολαίων, αποκαλούμενων αποκεντρωμένων εφαρμογών (dapps). Αυτά τα 'dapps' κυμαίνονται από απλά έξυπνα συμβόλαια, όπως η ανταλλαγή της ψηφιακής αξίας, σε πιο σύνθετα έξυπνα συμβόλαια, όπως ένας διανεμημένος αυτόνομος οργανισμός (DAO) (PwC, 2016). Η αποστολή ενός bitcoin, ή αιθέρα, στο blockchain είναι ένα παράδειγμα μιας απλής έξυπνης σύμβασης ως προκαθορισμένοι κανόνες που εξασφαλίζουν την εγκυρότητα της συναλλαγής που εκτελείται στην blockchain. Έχουν αναπτυχθεί έξυπνες υποθέσεις χρήσης μπλοκαρίσματος στη μεταποιητική βιομηχανία. Μια έξυπνη συμβολοσειρά μεταξύ πωλητή και πελάτη περιλαμβάνει κώδικα υπολογιστή που αντικατοπτρίζει τους όρους αποστολής μιας σύμβασης και επιβάλλει την κατάλληλη μεταφορά και ιδιοκτησία των αγαθών. Συντηρημένα με το Διαδίκτυο των πραγμάτων, τα έξυπνα συμβόλαια μπλοκαρίσματος για την κατασκευή μπορούν επίσης να παρακολουθούν συνεχώς τη θέση και τη θερμοκρασία των προϊόντων. Τέλος, το μακροπρόθεσμο όραμα για τις έξυπνες συμβάσεις αποκλεισμού περιλαμβάνει την ανάπτυξη διανεμημένων και αποκεντρωμένων αυτόνομων οργανισμών (DAO) που λειτουργούν με αυτοματοποιημένο τρόπο (Jarvenpaa και Teigland 2017, Swan 2015, Benkler 2006). Αυτοί οι DAO θα αντιπροσωπεύουν έναν νέο τύπο οργανισμού που τους επιτρέπει το Διαδίκτυο (Brafman and Beckstrom, 2006) αλλά είναι επίσης αυτόνομοι ως αποτέλεσμα της μετατροπής

της επιχειρησιακής λογικής στο πρωτόκολλο ηλεκτρονικών υπολογιστών. Κατά τον έλεγχο, μπορούν να χρησιμοποιηθούν έξυπνα συμβόλαια blockchain για την αυτόνομη εκτέλεση ελέγχων εσωτερικού ελέγχου και αναλυτικών διαδικασιών. Οι έξυπνες συμβάσεις στο blockchain είναι ευέλικτες και μπορούν να εφαρμοστούν στις διαδικασίες των επιχειρήσεων καθώς και στις διαδικασίες ελέγχου που μπορούν να διαμορφωθούν.

4.4.3.1 Smart Contracts για Κατασκευές

Η κατανόηση της λειτουργίας των έξυπνων συμβάσεων που εφαρμόστηκαν με επιτυχία μπορεί να καθοδηγήσει τη συζήτηση σχετικά με την εφαρμογή των έξυπνων διαδικασιών ελέγχου. Ένας προμηθευτής και ένας αγοραστής συμφωνούν με τους συμβατικούς όρους συμπεριλαμβανομένης της τιμής, της ποσότητας, της περιγραφής του προϊόντος, των συνθηκών αποστολής και πληρωμής. Αυτοί οι όροι θα προγραμματιστούν ως επιχειρησιακή λογική και θα αναπτυχθούν στο blockchain. Το blockchain προσφέρει στον αγοραστή την ευκαιρία να βρει το έξυπνο συμβόλαιο και να ελέγξει την κατάσταση των συναλλαγών που περνούν από το έξυπνο συμβόλαιο και να είναι σε θέση να επαληθεύσει την ποιότητα και την τοποθεσία των αγαθών. Εάν υπάρχει παραβίαση σε έναν κανόνα ή σε πολλούς κανόνες που έχουν ενσωματωθεί στο έξυπνο συμβόλαιο, ενεργοποιείται ένα μήνυμα σφάλματος και η συναλλαγή δεν μπορεί να ολοκληρωθεί. Αυτή η παραβίαση θα πρέπει να αντιμετωπιστεί από έναν άνθρωπο χρήστη, προφανώς έναν εσωτερικό ελεγκτή ή ιδιοκτήτη επιχειρηματικής διαδικασίας, για να επαληθεύσει τη νομιμότητα της συναλλαγής. Εναλλακτικά, η παράβαση θα μπορούσε να αντιμετωπιστεί με μια αυτοματοποιημένη διαδικασία που χειρίζεται τις έξυπνες παραβιάσεις σύμβασης. Διαφορετικά, αν δεν υπάρχουν παραβιάσεις, η σύμβαση αυτοεξυπηρετείται όταν τα εμπορεύματα φθάσουν στον προορισμό τους και η πληρωμή τους ικανοποιηθεί.

4.4.3.2 Smart Contracts για Έλεγχο

Ομοίως, κατά τον έλεγχο του εξωτερικού ελεγκτή και του επιθεωρητή θα συμφωνούσε τις προκαθορισμένες διαδικασίες ελέγχου για την αντιμετώπιση του κινδύνου ότι τα εμπορεύματα που αποστέλλονται δεν καταγράφονται με ακρίβεια. Αυτές οι προκαθορισμένες διαδικασίες θα κατανεμηθούν, παραδείγματος χάριν, σε κανόνες IFFTEN από την ελεγκτική εταιρεία και θα ενσωματωθούν σε μια έξυπνη αναλυτική διαδικασία που θα φορτωθεί στον μπλοκ αλυσίδας του εξωτερικού ελεγκτή και θα εγκριθεί εκ των προτέρων τόσο από την ελεγκτική εταιρεία όσο και από τον επιθεωρητή (Rozario and Thomas , 2017).

Μια περιγραφή μιας έξυπνης αναλυτικής διαδικασίας για την αντιμετώπιση αυτού του κινδύνου θα συνίστατο στον 1) κανόνα για την πρόβλεψη των σημερινών εβδομαδιαίων

πωλήσεων με βάση ένα εκπαιδευμένο μοντέλο παλινδρομικής παλινδρόμησης που περιλαμβάνει οικονομικές και μη οικονομικές παραμέτρους, συμπεριλαμβανομένων των εβδομαδιαίων πωλήσεων, της θέσης και των δεδομένων θερμοκρασίας από προηγούμενες εβδομάδες. Το μοντέλο πολλαπλασιαστικής παλινδρόμησης θα επανεκπαιδεύεται και θα δοκιμάζεται εκ νέου καθώς θα συλλέγονται περισσότερα δεδομένα κάθε φορά που ο ελεγκτής καλεί την έξυπνη διαδικασία. 2) οι προβλεπόμενες πωλήσεις από την πολυπολιτισμική παλινδρόμηση μπορούν στη συνέχεια να χρησιμοποιηθούν ως σημείο αναφοράς για να συγκριθούν οι τρέχουσες πραγματικές πωλήσεις (Yoon, 2016). Η λογική «IF-THEN» μπορεί να εκφράσει ότι εάν οι σημερινές πραγματικές πωλήσεις είναι ίσες ή μικρότερες από ή ίσες με το 5% της συνολικής σημαντικότητας, τότε δεν απαιτούνται περαιτέρω διαδικασίες ελέγχου και ο ελεγκτής είναι σε θέση να ποσοτικοποιήσει τον κίνδυνο υλικών ανακρίβεια για το λογαριασμό εσόδων. Εάν η είσοδος, δηλαδή οι πραγματικές πωλήσεις, δεν ταιριάζει με τους προγραμματισμένους κανόνες, θα εμφανιστεί ένα μήνυμα σφάλματος που υποδεικνύει ότι απαιτείται περαιτέρω διερεύνηση. Ο εξωτερικός ελεγκτής μπορεί στη συνέχεια να προτείνει εναλλακτικές λύσεις για την επεξεργασία αυτών των μηνυμάτων σφάλματος. Η πρώτη εναλλακτική λύση συνεπάγεται τη δημιουργία μιας ακολουθίας έξυπνης διαδικασίας ελέγχου που αλληλεπιδρά με την προαναφερθείσα έξυπνη διαδικασία ανάλυσης. Οι κανόνες που έχουν προγραμματιστεί σε αυτή τη δοκιμή παρακολούθησης έξυπνου ελέγχου θα περιλαμβάνουν κανόνες που αντικατοπτρίζουν φίλτρα κινδύνου που διαχωρίζουν αυτές τις συναλλαγές με σφάλματα που θα απαιτούσαν την προσοχή του ελεγκτή. Μια προϋπόθεση «IF-THEN» που υποδεικνύει αν οι πωλήσεις αυξήθηκαν λόγω της εποχικότητας, για παράδειγμα, θα προκαλούσε διακρίσεις στις συναλλαγές πώλησης που αυξήθηκαν για νόμιμους λόγους σε σύγκριση με τις συναλλαγές που αυξήθηκαν για μη επαληθεύσιμους και ενδεχομένως δόλιους ή εσφαλμένους λόγους που, φυσικά, από τον εξωτερικό ελεγκτή.

Από την άλλη πλευρά, η επεξεργασία μηνυμάτων σφάλματος δεν απαιτείται να είναι αυτόνομη, επομένως ο εξωτερικός ελεγκτής θα μπορούσε να επιλέξει να ελέγξει με μη αυτόματο τρόπο τις συναλλαγές που επισημάνθηκαν με την έξυπνη αναλυτική διαδικασία, αν και αυτό μπορεί να οδηγήσει στο πρόβλημα των εξαιρετικών εξαιρέσεων που είναι που είναι ήδη εμφανή με πιο εξελιγμένα αναλυτικά εργαλεία που εκτελούνται έξω από το blockchain (Issa και Kogan, 2014). Στον blockchain του εξωτερικού ελεγκτή ο επιθεωρητής ελέγχου έχει την ικανότητα να ελέγχει ενεργά τα αποτελέσματα της προαναφερόμενης έξυπνης αναλυτικής διαδικασίας καθώς μπορεί να έχει πρόσβαση στη διαδικασία έξυπνου ελέγχου και στην κατάσταση των συναλλαγών που

περνούν τη διαδικασία κοντά σε πραγματικό χρόνο. Επιπλέον, η Επιτροπή Κεφαλαιαγοράς, οι βασικοί επενδυτές και η επιτροπή ελέγχου μπορούν να δουν τα αποτελέσματα αυτής της διαδικασίας και να προβούν σε εκτίμηση των εσόδων, εάν δεν απαιτούνται πρόσθετες διαδικασίες ή προβαίνουν σε προκαταρκτική αξιολόγηση στο σενάριο ότι τα μηνύματα λάθους πρέπει να υποστούν επεξεργασία.

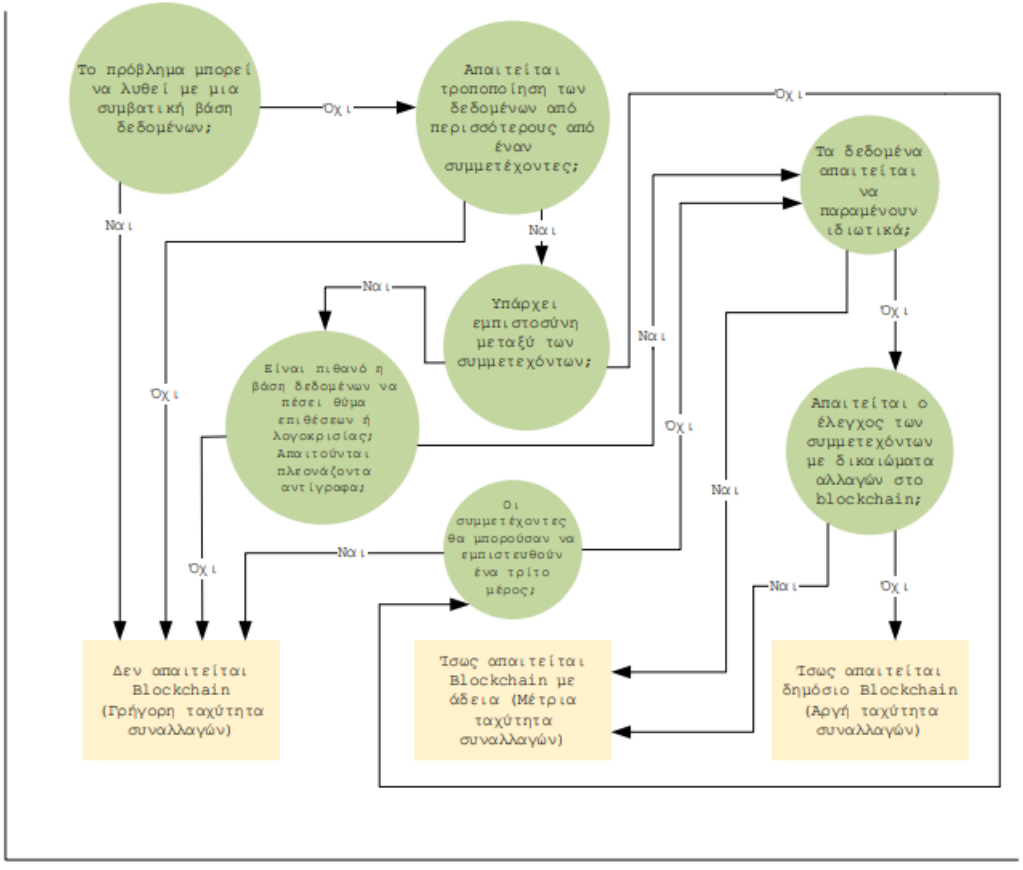
Είναι σημαντικό να σημειωθεί ότι μπορούν να αναπτυχθούν απλούστερες αλλά νέες έξυπνες διαδικασίες ελέγχου. Για παράδειγμα, επειδή το blockchain επιτρέπει την ασφαλή παρακολούθηση και παρακολούθηση διαφόρων συσκευών IoT, η ελεγκτική εταιρεία μπορεί να σχεδιάσει μια δοκιμή εσωτερικού ελέγχου για να επαληθεύσει την πραγματική θέση των εμπορευμάτων και να συγκριθεί με την αναμενόμενη θέση των εμπορευμάτων (Dai and Vasarhelyi, 2017; Rozario and Thomas, 2017), προκειμένου να εκτιμηθεί ο κίνδυνος μεταφοράς αγαθών σε εσφαλμένη τοποθεσία. Δεδομένου ότι οι επιχειρηματικές οργανώσεις έχουν αρχίσει να διερευνούν τις συνέργειες του blockchain και του Διαδικτύου των Πραγμάτων (IBM, 2017), είναι εύλογο να συμπεράνουμε ότι οι ελεγκτές θα πρέπει να σχεδιάσουν νέες διαδικασίες ελέγχου που θα τους βοηθήσουν να εκτιμήσουν με μεγαλύτερη ακρίβεια τον κίνδυνο ουσιώδους ανακρίβειας.

4.4.4 Διαδικασίες Έξυπνου Ελέγχου

Η εμφάνιση νέων τεχνολογιών, όπως η άνοδος του Διαδικτύου και του ηλεκτρονικού εμπορίου, τα μοντέλα μηχανοκίνητης εκμάθησης που μαθαίνουν από τα μεγέθη των μεγάλων δεδομένων, και επί του παρόντος τα blockchain και οι έξυπνες συμβάσεις έχουν οδηγήσει σε συζητήσεις μεταξύ διαφόρων ενδιαφερομένων σχετικά με το ρόλο της τεχνολογίας στο πρότυπο ελέγχου (IAASB , 2016, PCAOB, 2016). Οι Vasarhelyi και Halper (1991) σχεδίασαν και εφάρμοσαν για πρώτη φορά εφαρμογές συνεχούς ελέγχου στα εργαστήρια της AT & T Bell. Μερικά χρόνια αργότερα, ο τομέας της έρευνας απέκτησε σημαντική έλξη με την εφαρμογή συνεχούς παρακολούθησης ελέγχου (Alles et al., 2006), τη συνεχή διασφάλιση δεδομένων (Kogan, et al., 2014), τη συνεχή παρακολούθηση και αξιολόγηση κινδύνων (Moon, 2016) συνεχής έλεγχος σε XML και ERP (Murthy and Groomer, 2004, Kuhn και Sutton, 2010). Οι μελέτες περιπτώσεων για την επίδειξη των πρακτικών εφαρμογών της χρήσης της τεχνολογίας στον τομέα του ελέγχου περιορίστηκαν στον τομέα του εσωτερικού ελέγχου, δεδομένου ότι περιορίζονται λιγότερο από περιοριστικές κανονιστικές απαιτήσεις (Kuenkaikaew and Vasarhelyi, 2013). Ωστόσο, καθώς οι τεχνολογίες συνεχίζουν να αναπτύσσονται με εκθετικό ρυθμό, είναι λογικό το εξωτερικό ελεγκτικό επάγγελμα να ανταποκρίνεται σε τέτοιες αλλαγές προκειμένου να παραμείνει σχετικό

σε έναν σύγχρονο και ψηφιακό κόσμο. Από κοινού, είναι ζωτικής σημασίας να εξεταστεί η μετατροπή του παραδοσιακού μοντέλου εξωτερικού ελέγχου στο πλαίσιο των τεχνολογικών αλλαγών. Το παραδοσιακό μοντέλο εξωτερικού ελέγχου που επιτρέπει στους ελεγκτές να συνάπτουν συμπεράσματα σχετικά με τις υποκείμενες πληροφορίες στις οικονομικές καταστάσεις του πελάτη ελέγχου αποτελείται από αναλυτικές διαδικασίες αξιολόγησης κινδύνου, διαδικασίες για τη δοκιμή της λειτουργικής αποτελεσματικότητας των εσωτερικών ελέγχων και ουσιαστικές διαδικασίες, συμπεριλαμβανομένων ουσιαστικών αναλυτικών διαδικασιών και δοκιμών των λεπτομερειών (Louwers et al., 2013). Η DA (ανάλυση δεδομένων) διαπερνά το παραδοσιακό μοντέλο ελέγχου, στην πραγματικότητα είναι δύσκολο να οραματιστεί ένας έλεγχος των οικονομικών καταστάσεων που δεν χρησιμοποιεί το DA (Stewart, 2015).

Διάγραμμα 4 – Χρήση από διαφορετικές τεχνολογίες Blockchain βάσει των απαιτήσεων της εκάστοτε εφαρμογής (Kouveliotis, 2019)



4.4.4.1 Ανάλυση Δεδομένων Ελέγχου 1.0 & 2.0

Δεδομένου ότι η ανάλυση δεδομένων είναι μια σημαντική συνιστώσα του μοντέλου εξωτερικού ελέγχου, είναι ενδιαφέρον να διαιρέσουμε αυτό το κατασκεύασμα σε ταξινομίες που αντικατοπτρίζουν τη δυνητική του εξέλιξη. Προς το παρόν, οι εξωτερικοί ελεγκτές εκτελούν

διαδικασίες DA, όπως ανάλυση σάρωσης, τάσης ή αναλογίας (Stewart, 2015). Αυτές είναι απλές ΑΣ και αρχικά εισήχθησαν γύρω στη δεκαετία του 1980 όταν η AICPA εξέδωσε καθοδήγηση για αναλυτικές διαδικασίες (AICPA, 1989). Ως εκ τούτου, είναι λογικό να συμπεράνουμε ότι πρόκειται για την πρώτη γενιά αναλύσεων δεδομένων ελέγχου, Audit Data Analytics 1.0. Καθώς η τεχνολογία προχώρησε και αυξήθηκε η ισχύς της πληροφορικής, οι πωλητές λογισμικού ελέγχου, συμπεριλαμβανομένων των IDEA και ACL, οι οποίοι εξυπηρετούν κυρίως τον τομέα εσωτερικού ελέγχου, άρχισαν να αναπτύσσουν αναλυτικά εργαλεία ελέγχου που βελτίωσαν τη διαδικασία ελέγχου, επιτρέποντας στους ελεγκτές να εξετάζουν πλήρεις πληθυσμούς δεδομένων με αυξημένη συχνότητα ανθρώπινη παρέμβαση. Αυτά τα εργαλεία ελέγχου κυμαίνονται από απλούς αλγορίθμους μάθησης έως πιο εξελιγμένα μοντέλα στατιστικής και μηχανικής μάθησης και περιλαμβάνουν τη δεύτερη γενιά αναλύσεων δεδομένων ελέγχου Audit Data Analytics 2.0. Σήμερα, το επάγγελμα του εξωτερικού ελεγκτή εξελίσσεται αργά αλλά σταθερά από το Audit Data Analytics 1.0 στο Audit Data Analytics 2.0 (Appelbaum et al., 2017).

4.4.4.2 Ανάλυση Δεδομένων Ελέγχου 3.0

Με τα έξυπνα συμβόλαια blockchain, το Audit Data Analytics προχωρά στην επόμενη φυσική εξέλιξή του, το Audit Data Analytics 3.0. Ουσιαστικά, η πλατφόρμα blockchain διευκολύνει την ανάπτυξη έξυπνων διαδικασιών ελέγχου, οι οποίες εκτελούν αυτόνομα προγνωστικά μοντέλα, εντοπίζουν αξιοσημείωτα στοιχεία και παράγουν κοντινές εκθέσεις ελέγχου σε πραγματικό χρόνο εκ μέρους του εξωτερικού ελεγκτή. Οι έξυπνες διαδικασίες ελέγχου έχουν τη δυνατότητα να βελτιώσουν την ποιότητα του ελέγχου και να μετριάσουν το χάσμα αναμονής μεταξύ ελεγκτών και ενδιαφερομένων. Όταν διενεργείται έλεγχος μέσω έξυπνων διαδικασιών ελέγχου, υπάρχουν δύο προοπτικές που πρέπει να λαμβάνονται υπόψη: 1) οι κίνδυνοι που σχετίζονται με τον έλεγχο των διαδικασιών αυτών, δηλαδή οι επιχειρηματικοί κίνδυνοι του πελάτη ελέγχου, και 2) οι διαδικασίες ελέγχου ποιότητας για τις διαδικασίες αυτές αξιοπιστία). Όσον αφορά τις πρώτες συνέπειες, οι επιχειρηματικές πρακτικές αποκλεισμού και έξυπνων συμβάσεων για τους πελάτες ελέγχου δημιουργούν νέους κινδύνους ελέγχου και συνεπώς οι έξυπνες διαδικασίες ελέγχου θα σχεδιάζονται έτσι ώστε να ανταποκρίνονται στους υπάρχοντες ελεγκτικούς κινδύνους και στους νέους κινδύνους που προκύπτουν ως αποτέλεσμα αυτών των νέων επιχειρηματικών πρακτικών. Δεύτερον, η ανάπτυξη εργαλείων ανάλυσης δεδομένων θα πρέπει να επικυρώνεται εκ των προτέρων και εκ των υστέρων για την αξιολόγηση της αξιοπιστίας τους (IAASB, 2016). Οι έξυπνες διαδικασίες ελέγχου και τα άλλα εργαλεία που αλληλεπιδρούν με αυτές τις διαδικασίες, όπως το blockchain που αναπτύσσεται από τον εξωτερικό ελεγκτή, και οι

ορθογραφικοί έλεγχοι5 που αλληλεπιδρούν με το μπλοκ αλυσίδας του εξωτερικού ελεγκτή πρέπει να επαληθεύονται για να διασφαλιστεί ότι λειτουργούν όπως προβλέπεται. Συλλογικά, τα σχήματα αντίδρασης σε κινδύνους των έξυπνων διαδικασιών ελέγχου και η επικύρωση του πρωτοκόλλου των έξυπνων διαδικασιών ελέγχου είναι σημαντικοί παράγοντες.

4.4.4.3 Κίνδυνοι Ελέγχου

Οι έξυπνες διαδικασίες ελέγχου που βοηθούν τους ελεγκτές στην εκτίμηση των κινδύνων ελέγχου περιλαμβάνουν έξυπνες αναλυτικές διαδικασίες και έξυπνες δοκιμές εσωτερικού ελέγχου που εκτελούν αυτόνομα τους στόχους του ελέγχου για λογαριασμό του εξωτερικού ελεγκτή. Οι κίνδυνοι ελέγχου κατηγοριοποιούνται ως υφιστάμενοι κίνδυνοι, για τους κινδύνους που υπάρχουν στα έσοδα, ανεξάρτητα από το σύστημα που συλλαμβάνει τις συναλλαγές εσόδων και τους νέους κινδύνους, για τους κινδύνους που προκύπτουν ως αποτέλεσμα του μπλοκαρίσματος και της υιοθέτησης έξυπνων συμβάσεων από τους πελάτες ελέγχου. Για τον κίνδυνο εισαγωγής πλασματικών, μη εξουσιοδοτημένων ή εσφαλμένων συμβάσεων πώλησης, οι ελεγκτές επιλέγουν επί του παρόντος δείγμα συμβάσεων πώλησης και επανεξετάζουν χειροκίνητα τους όρους αυτών των συμβάσεων. Εναλλακτικά, οι ελεγκτές μπορούν να χρησιμοποιήσουν το NLP (φυσική επεξεργασία γλώσσας) και το λογισμικό βαθιάς εκμάθησης για να επανεξετάσουν αυτόματα τους όρους των συμβάσεων για τον πλήρη πληθυσμό των συμβάσεων πώλησης (Yan, 2017). Τα αποτελέσματα αυτής της διαδικασίας συγκεντρώνονται μαζί με τα αποτελέσματα άλλων διαδικασιών για να προκύψει μια ποιοτική ελεγκτική γνώμη σχετικά με το εύλογο των υποκείμενων οικονομικών πληροφοριών στις οικονομικές καταστάσεις του πελάτη. Ωστόσο, καθώς οι χρήστες των οικονομικών καταστάσεων και οι ρυθμιστικές αρχές έχουν διαφορετικές ανάγκες πληροφόρησης (Romero et al., 2012), οι έξυπνες διαδικασίες ελέγχου μπλοκαρίσματος έχουν τεράστιο δυναμικό όχι μόνο να βοηθήσουν τον εξωτερικό ελεγκτή στη βελτίωση της ποιότητας του ελέγχου αλλά και να καλύψουν τις διάφορες ανάγκες πληροφόρησης των διαφόρων μερών που επεκτείνονται πέρα από μια ποιοτική ελεγκτική γνώμη.

5 Συμπεράσματα

Είναι αναμφισβήτητο ότι η τεχνολογία blockchain μπορεί να έχει βαθιά θετική επίδραση στο περιβάλλον ελέγχου και να φέρει την απαιτούμενη βελτιστοποίηση στις υπάρχουσες διαδικασίες. Με την αύξηση των γνώσεων γύρω από αυτό και την συνειδητοποίηση της σπουδαιότητάς της, οι εταιρείες αρχίζουν να αναπτύσσουν λύσεις σε πολλούς διαφορετικούς τομείς όπου τα αξιόπιστα και ασφαλή δεδομένα είναι κρίσιμα και αρχίζουν να βλέπουν τα blockchains αποδεικτικής βάσης ως βιώσιμη εναλλακτική στις τρέχων λύσεις. Ο έλεγχος είναι ένας από αυτούς τους τομείς και είναι ήδη δυνατή η χρήση λύσεων που αναπτύχθηκαν από το Factom και στο μέλλον από τους Libra και Verady. Είναι επίσης σημαντικό να εξεταστεί πώς να ταιριάζει η τεχνολογία blockchain με άλλες αναδυόμενες τεχνολογίες όπως τα Computer Assisted Audit Tools and Techniques (CAATT). Όπως τα μεγάλα δεδομένα και τα αναλυτικά στοιχεία που επιτρέπουν στους ελεγκτές να αξιολογούν τον αυξανόμενο όγκο δεδομένων, καθώς και το λογισμικό συνεχούς παρακολούθησης και ελέγχου της τεχνητής νοημοσύνης, αλλά και τις μη τεχνολογικές δυνάμεις, η αυξανόμενη πολυπλοκότητα του κανονιστικού τοπίου για παράδειγμα. Η κατοχύρωση των επίσημων φορέων, όπως οι Ομοσπονδίες Πιστοποιημένων Λογιστών-Δημόσιων Λογιστών, θα αποτελέσει ουσιαστική ώθηση για την υιοθέτηση της τεχνολογίας blockchain, θα μπορούσε, για παράδειγμα, να αποτελέσει μέρος της ανασκόπησης. Η αλήθεια είναι ότι υπάρχει ακόμη πολύς δρόμος για να περάσετε μέχρις ότου γίνει ευρεία υιοθέτηση σε αυτόν τον τομέα. Οι επενδύσεις ξεπερνούν σήμερα την προσφορά και την τεχνογνωσία. Οι λογιστές και οι ελεγκτές δεν έχουν ακόμη εξοικειωθεί με την τεχνολογία αυτή και πώς μπορούν να την χρησιμοποιήσουν. Είναι απαραίτητο οι εταιρείες να αφιερώσουν ομάδες καινοτομίας για να κάνουν τη μετάβαση από τον τυποποιημένο έλεγχο στον βελτιστοποιημένο έλεγχο χρησιμοποιώντας τεχνολογία blockchain. Σε ένα τόσο γρήγορο τεχνολογικό περιβάλλον, είναι σημαντικό να παρακολουθήσουμε τη διακοπή τεχνολογιών όπως το blockchain για να είναι επιτυχής.

Δεδομένων των πρόσφατων συζητήσεων σχετικά με τη σημασία του επαγγέλματος του ελεγκτή σε έναν ταχέως μεταβαλλόμενο επιχειρηματικό κόσμο, είναι σημαντικό οι ελεγκτικές εταιρείες, οι ρυθμιστικές αρχές, οι ακαδημαϊκοί και οι εκπρόσωποι τυποποίησης να ενημερώνονται σχετικά με τις πρόσφατες τεχνολογικές εξελίξεις που έχουν τη δυνατότητα να διαταράξουν τα επιχειρηματικά οικοσυστήματα και, το οικοσύστημα ελέγχου. Οι πολυάριθμες πρωτοβουλίες σχετικά με τον αντίκτυπο των νέων τεχνολογιών στους ελέγχους των οικονομικών καταστάσεων υποδεικνύουν ότι οι εξωτερικοί ελεγκτές καταβάλλουν προληπτικά προσπάθεια να

ανταποκριθούν σε μια ψηφιακή και σύγχρονη οικονομία. Προχωρώντας προς ένα υβριδικό μοντέλο ελέγχου που περιλαμβάνει διαδικασίες έξυπνων ελεγκτικών διαδικασιών, μπορούν να βελτιώσουν την ποιότητα του ελέγχου, να ανταποκριθούν στις απαιτήσεις πληροφόρησης των διαφόρων ενδιαφερομένων και, συνεπώς, παράλληλα σε έναν ψηφιακό επιχειρηματικό κόσμο.

Ο νέος τύπος Analytics Audit Data Analytics που επιτρέπεται από blockchain και έξυπνες συμβάσεις, έχουν προταθεί έξυπνες διαδικασίες ελέγχου. Οι έξυπνες διαδικασίες ελέγχου θα είναι η επόμενη γενιά του Audit Data Analytics, του Audit Data Analytics 3.0 και θα έχουν τη δυνατότητα να αλλάξουν τον τρόπο εκτέλεσης και παράδοσης των ελέγχων των οικονομικών καταστάσεων. Ωστόσο, προτού καταστούν εφικτές οι έξυπνες διαδικασίες ελέγχου, υπάρχουν προκλήσεις που δεν πρέπει να παραμεληθούν, συμπεριλαμβανομένων των προκλήσεων που σχετίζονται με τις ισχύουσες κανονιστικές απαιτήσεις και τις προκλήσεις που σχετίζονται με τις αποδιοργανωτικές τεχνολογίες που παραμένουν στα πρώτα στάδια της έγκρισής τους.

Ενώ περιγράφηκε η εφαρμογή και οι προκλήσεις των έξυπνων συμβάσεων στον έλεγχο, αυτή η μελέτη μπορεί να επεκταθεί με διάφορους τρόπους. Κατ 'αρχάς, η επικύρωση του blockchain του πελάτη ελέγχου είναι πρωταρχικής σημασίας και θα οδηγήσει σε ένα νέο τύπο ελέγχου IT blockchain. Η πτυχή του ελέγχου του αποκλεισμού μιας επιχειρηματικής οντότητας θεωρήθηκε εν συντομία δεδομένου ότι είναι πέρα από το πεδίο εφαρμογής του παρόντος εγγράφου. Δεύτερον, η εννοιοποίηση ενός blockchain εξωτερικού ελεγκτή προϋποθέτει ότι εφαρμόζεται ένα blockchain με άδεια.

Τέλος, μπορεί να υπάρξει σύγκρουση μεταξύ των βασικών φιλοσοφιών του blockchain και του ελέγχου. Το Blockchain είναι μια αποκεντρωμένη τεχνική με ελάχιστη ρύθμιση, δομή και εξουσία, όπου όλοι οι συμμετέχοντες έχουν μια ίση ψήφο. Μέσα στον τομέα των κατανεμημένων λογιστικών βιβλίων υπάρχουν ελάχιστες οδηγίες σχετικά με τη δομή των αλυσίδων και τις συμβάσεις τους. Στο πλαίσιο των κατανεμημένων λογιστικών βιβλίων δεν υπάρχει κεντρική ρυθμιστική αρχή ή αξιόπιστος τρίτος επαληθευτής. Στην πραγματικότητα, οι κατανεμημένες τεχνολογίες λογιστικών βιβλίων θεωρούνται από ορισμένους ως τέλειο παράδειγμα μιας ελευθεριακής, αποκεντρωμένης δημοκρατίας (Warncke 2017). Ο έλεγχος, ωστόσο, είναι ένα επάγγελμα που καθοδηγείται από κανονισμούς. Είναι ιδιαίτερα δομημένη και οι πρακτικές της υπαγορεύονται από την PCAOB και την SEC. Είναι δυνατόν ένας γάμος αυτού του συντηρητικού επαγγέλματος ελεγκτών να γίνει με τον φιλελεύθερο μη δομημένο τομέα των κατανεμημένων τεχνολογιών βιβλίου; Η απάντηση σε αυτό το ερώτημα θα οδηγήσει και θα βοηθήσει να διατυπώσει τις απαντήσεις στις ερωτήσεις που τίθενται στην προηγούμενη

ενότητα και σε άλλη έρευνα. Και οι δύο πρακτικές βρίσκονται στα αντίθετα άκρα του φάσματος - μπορούν και οι δύο τομείς να συμβιβαστούν και να προσαρμοστούν για να συναντηθούν στη μέση; Το παρόν έγγραφο επικεντρώνει την προσοχή στα θέματα που αντιμετωπίζει το επάγγελμα του ελεγκτή όσον αφορά τη δυνατότητα ελέγχου των συναλλαγών αποκλεισμού, ιδίως σε τομείς νέφους. Οι εκτιμήσεις κινδύνου και οι πολιτικές διακυβέρνησης των πελατών πρέπει να εξεταστούν σε αυτή τη νέα μορφή κατανεμημένων υπολογιστών cloud computing. Ελπίζεται ότι οι προαναφερθείσες πολυπλοκότητες του Blockchain και του Cloud Computing δεν περιθωριοποιούνται από το ελεγκτικό επάγγελμα καθώς διεξάγει τις υποθέσεις του με πελάτες που σπεύδουν να υιοθετήσουν κατανεμημένες τεχνολογίες λογιστικών καταλόγων και διανέμουν τεχνολογίες λογισμικού στο σύννεφο.

6 Βιβλιογραφία

AICPA (1989): Analytical Procedures, AU Section 320, New York, NY. https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/au-00329.pdf AICPA (2017): Rutgers

AICPA Data Analytics Research Initiative. https:// www.aicpa.org/interestareas/frc/assuranceadvisoryservices/radarprojects.html

ALLES, M.; BRENNAN, G.; KOGAN, A.; VASARHELYI, M. A. (2006): "Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens", International Journal of Accounting Information Systems, vol. 7, n. 2: 137-161. https://doi.org/ 10.1016/j.accinf. 2005.10.004

Alles, M.G., Kogan, A., and Vasarhelyi, M.A. 2008. Audit Automation for Implementing Continuous Auditing: Principles and Problems. Working paper, Rutgers, the State University of New Jersey.

American Institute of Certified Public Accountants (AICPA), 2006. Audit Evidence: Statement on Auditing Standards No. 106. AU Section 326. New York, NY: AICPA.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Muralidharan, S. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference* (pp. 1-15).

Appelbaum, D. 2016. Securing Big Data Provenance for Auditors: The Big Data Provenance Black Box as Reliable Evidence. Journal of Emerging Technologies in Accounting, Vol. 13, No. 1 Spring 2016, pp. 17-36

Appelbaum, D. and Nehmer, R. 2017. Using Drones in Internal and External Audits: An Exploratory Framework. Journal of Emerging Technologies in Accounting, Volume 14, Number 1, 2017.

APPELBAUM, D.; KOGAN, A.; VASARHELYI, M. A. (2017): "Big Data and analytics in the modern audit engagement: Research needs", Auditing: A Journal of Practice and Theory: November 2017, vol. 36, n. 4: 1-27. https://doi. org/10.2308/ajpt-51684

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. Communications of the ACM, 53(4), pp.50-58.

Assunção, M.D., Calheiros, R.N., Bianchi, S., Netto, M.A. and Buyya, R., 2015. Big Data computing and clouds: Trends and future directions. Journal of Parallel and Distributed Computing, 79, pp.3-15.

Bacani, C. 2017. "The Death of Accounting and Auditing and What to do About It." CFO Innovation, Tuesday March 21, 2017. https://www.cfoinnovation.com/story/12767/deathaccounting-and-auditing-and-what-do-about-it

Back, A. 2002. Hashcash – A Denial of Service Counter-Measure. http://www.hashcash.org/papers/hashcash.pdf.

BADERTSCHER, B. A.; KIM, J.; KINNEY W.; OWENS, E. L. (2017): "Audit Procedures and Financial Statement Quality: The Positive Effects of Negative Assurance", Working Paper.

BARTOLETTI, M.; POMPIANU, L. (2017): "An empirical analysis of smart contracts: platforms, applications, and design patterns". https://arxiv.org/pdf/ 1703.06322.pdf. https://doi.org/10.1007/978-3-319-70278-0_31

BENKLER, Y. (2007): "The wealth of networks: How social production transforms markets and freedom", The Yale Law Journal, vol. 116, n. 7: 1472. https://doi.org/10.2307/20455766

BRAFMAN, O.; BECKSTROM, R. A. (2006): The starfish and the spider: The unstoppable power of leaderless organizations, Penguin. BUTERIN, V. (2014): "A next-generation smart contract and decentralized application platform", White paper

Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310, p. 4).

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2012). Enterprise Risk Management for Cloud Computing. https://www.coso.org/Documents/Cloud-Computing-Thought-Paper.pdf.

Dai, J, and Vasarhelyi, M.A. (2017) Towards Blockchain-based Accounting and Assurance. , In-Press. https://doi.org/10.2308/isys-51804

DAI, J.; VASARHELYI, M. A. (2017): "Towards Blockchain-based Accounting and Assurance", Journal of Information Systems: Fall 2017, vol. 31, n. 3: 5-21. https://doi.org/10.2308/isys-51804

DECOVNY, S. (2015): "Chips Off the Old Blockchain", CFA Institute Magazine, vol. 26, n. 6: 24-25. https://doi.org/10.2469/cfm.v26.n6.8

Deloitte. 2017. “Blockchain Technology: A game-changer in accounting?” www.Deloitte.com/de/blockchain

Duncan, B., & Whittington, M. (2016). Cloud cyber-security: Empowering the audit trail. *International Journal on Advances in Security Volume 9, Number 3 & 4, 2016*.

Duncan, R. A. K., & Whittington, M. (2016). Enhancing cloud security and privacy: the power and the weakness of the audit trail. *CLOUD COMPUTING 2016*.

Duncan, R. A. K., & Whittington, M. (2017, February). Creating an immutable database for secure cloud audit trail and system logging. In *Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017-23 February 2017, Athens, Greece*.

Elifoglu, I.H., Guzey, Y., and Tasseven, O. 2014. Cloud Computing and the Cloud User’s Auditor. Review of Business; Jamaica 35.1 (Summer/Fall 2014): 76-83.

FANNING, K.; CENTERS, D. P. (2016): “Blockchain and Its Coming Impact on FinancialServices”, Journal of Corporate Accounting & Finance, vol. 27, n. 5: 53-57.onlinelibrary.wiley.com/doi/10.1002/jcaf.22179/pdf

FORBES (2016): “Thirteen Companies that Use Deep Learning to Produce ActionableResults”.https://www.forbes.com/sites/kevinmurnane/2016/04/01/thirte en-companies-that-use-deep-learning-to-produce-actionable-results/#59f0590633 b8

Gault, M. 2017. “BlockCloud: Re-inventing Cloud with Blockchains.” May 13, 2017: https://guardtime.com/blog/blockcloud-re-inventing-cloud-with-blockchains

Geerts, G. L. 2011. A Design Science Research Methodology and its Application to Accounting Information Systems Research. International Journal of Accounting Information Systems, 12(2), 142 – 151.

Guegan, D. (2017). Public blockchain versus private blockhain.

Gupta, S. S. (2017). *Blockchain*. John Wiley & Sons, Inc.

Hevner, A., March, S. T., Park, J. & Ram, S. 2004. Design Science in Information Systems Research. MIS Quarterly, 28(1), 75 – 105.

IAASB (2016): Exploring the Growing Use of Technology in the Audit, with a Focus on Data Analytics. New York, NY: IFAC.

IAASB (2017): Data Analytics. http://www.iaasb.org/projects/data-analytics

IBM (2017): "Implementing Blockchain for Cognitive IoT Applications". https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitiveiot-apps-trs/cl-blockchain-for-cognitive-iot-apps-trs-pdf.pdf

Information and Communication Technology Literature. Journal of emerging

ISSA, H.; KOGAN, A. (2014): "A predictive ordered logistic regression model as a tool for quality review of control risk assessments", Journal of Information Systems, vol. 28, n. 2: 209-229. https://doi.org/10.2308/isys-50808

JARVENPAA, S.; TEIGLAND, R. (2017): "Introduction to Trust, Identity, and Trusted Systems in Digital Environments Minitrack", In Proceedings of the 50th Hawaii International Conference on System Sciences.

KIVIAT, T. I. (2015): "Beyond Bitcoin: Issues in Regulating Blockchain Transactions", DukeLaw Journal, vol. 65: 569-569.

KOGAN, A.; ALLES, M. G.; VASARHELYI, M. A.; WU, J. (2014): "Design and evaluation of a continuous data level auditing system", Auditing: A Journal of Practice & Theory, vol. 33, n.4: 221-245. https://doi.org/10.2308/ajpt-50844

Kouveliotis-Lysikatos, I. (2019). Συμβολή στην ανάπτυξη κατανεμημένων αλγορίθμων για τον έλεγχο και τη λειτουργία ευφυών δικτύων διανομής (Doctoral dissertation, National Technical University of Athens (NTUA); Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ)).

KPMG. 2013. "Cloud Computing: Risks and Auditing." Presented at the IIA Chicago 53rd Annual Seminar, April 15, 2013. https://chapters.theiia.org/chicago/Annual%20Seminar%20Presentations/E3%20-%20Cloud%20Computing%20Risks%20and%20Auditing.pdf

KUENKAIKAEW, S.; VASARHELYI, M. A. (2013): "The Predictive Audit Framework",The International Journal of Digital Accounting Research, vol. 13, n. 2: 37-71. https://doi.org/10.4192/1577-8517-v13_2

KUHN, J. R.; SUTTON, S. G. (2010): "Continuous auditing in ERP system environments: The current state and future directions", Journal of Information Systems, vol. 24, n. 1: 91-112. https://doi.org/10.2308/jis.2010.24.1.91

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *IJ Network Security*, *19*(5), 653-659.

LOUWERS, T. J.; RAMSAY, R. J.; SINASON, D. H.; STRAWSER, J. R.; THIBODEAU, J. C. (2013): Auditing and assurance services: McGraw-Hill/Irwin New York, NY.

Louwers, T., Blay, A., Sinason, D., Strawser, J., and Thibodeau, J. 2017 Auditing & Assurance Services 7e, McGraw Hill Education, New York: NY

MAES, P. (1994): "Agents that reduce work and information overload", Communications of the ACM, vol. 37, n. 7: 30-40. https://doi.org/10.1145/ 176789.176792

MAINELLI, M.; SMITH, M. (2015): "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)", The Journal of Financial Perspectives, vol. 3, n.3: 38-69.

MATTHEWS, D. (2006): "From ticking to clicking: changes in auditing techniques in Britain from the 19th century to the present", The Accounting Historians Journal, vol. 33, n. 2: 63-102. https://doi.org/10.2308/0148- 4184.33.2.63

MOON, D. (2016): Continuous risk monitoring and assessment: CRMA. Doctoral dissertation, Rutgers University-Graduate School-Newark.

Muniswamy-Reddy, K. K., D. A. Holland, U. Braun, and M. I. Seltzer. 2006. "ProvenanceAware Storage Systems." In USENIX Annual Technical Conference, General Track, pp. 43-56.

MURTHY, U. S.; GROOMER, S. M. (2004): "A continuous auditing web services model for XML-based accounting systems", International Journal of Accounting Information Systems, vol. 5, n.2: 139-163. https://doi.org/10.1016/ j.accinf.2004.01.007

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Nehmer, R. A. and Srivastava, R. 2016. Using Belief Functions in Software Agents to Test the Strength of Application Controls: A Software Agent Framework. International Journal of Intelligent Information Technologies, 12(3), pp.

NO, W. G.; VASARHELYI, M. A. (2017): "Cybersecurity and Continuous Assurance", Journal of Emerging Technologies in Accounting, vol. 14, n. 1: 1-12. https://doi.org/10.2308/jeta-10539

NWANA, H. S.; NDUMU, D. T. (1999): “A perspective on software agents research”, The Knowledge Engineering Review, vol. 14, n. 2: 125-142. https://doi.org/10.1017/s0269888999142012

O’Driscoll, A., Daugelaite, J. and Sleator, R.D., 2013. ‘Big data’, Hadoop and cloud computing in genomics. Journal of biomedical informatics, 46(5), pp.774-781.

Papenfort, K., & Bassler, B. L. (2016). Quorum sensing signal–response systems in Gram-negative bacteria. *Nature Reviews Microbiology*, *14*(9), 576.

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. 2007. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45 – 77.

Power, M. (2019). Modelling the microfoundations of the audit society: Organizations and the logic of the audit trail. *Academy of Management Review*, (ja).

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (2016): Audit Expectations Gap: A Framework for Regulatory Analysis. Washington, D.C: PCAOB. https://pcaobus.org/News/Speech/Pages/Franzel-speech-Institute-12-13- 16.aspx

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (2017): PCAOB Adopts New Standard to Enhance the Relevance and Usefulness of the Auditor's Report with Additional Information for Investors. Washington, D.C: PCAOB. https://pcaobus.org/News/Releases/Pages/auditors-report-standard-adop tion-6-1- 17.aspx

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (2017): Staff Inspection Brief. https://pcaobus.org/News/Releases/Pages/staff-inspection-brief2017-issuers-8-30-17.aspx

Public Compnay Accounting Oversight Board (PCAOB). 2010. Audit Evidence. PCAOB Auditing Standards No. 15. Washington, DC: PCAOB.

PWC (2016): How Smart Contracts Automate Digital Business. http://usblogs.pwc.com/emerging-technology/how-smart-contracts-automate-digit al-business/

ROMERO, S.; GAL, G.; MOCK, T. J.; VASARHELYI, M. A. (2012): “A measurement theory perspective on business measurement”, Journal of Emerging Technologies in Accounting, vol. 9, n. 1: 1-24. https://doi.org/10.2308/jeta-50396

ROZARIO, A.; THOMAS, C. (2017): “Reshaping the Audit with Blockchain and Artificial Intelligence: An External Auditor Blockchain for Close to Real-Time Audit Reporting”, Rutgers University Working

Paper. SZABO, N. (1994): “Smart contracts”. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Sakka, M.A., Defude, B. and Tellez, J., 2010. Document provenance in the cloud: constraints and challenges. In Networked Services and Applications- Engineering, Control and Management (pp. 107-117). Springer Berlin Heidelberg.

Schmidt, P. J., Wood, J. T. and Grabski, S. V., 2016. Business in the Cloud: Research Questions on Governance, Audit, and Assurance. Journal of Information Systems 20(3), 173 – 189.

Seok, B., Park, J., & Park, J. H. (2019). A Lightweight Hash-Based Blockchain Architecture for Industrial IoT. *Applied Sciences*, *9*(18), 3740.

STEWART, T. (2015): Data analytics for financial-statement Audits, Chapter 5 in AICPA, Audit Analytics and Continuous Audit: Looking Toward the Future, American Institute Of Certified Public Accountants. New York, NY 2015

SWAN, M. (2015): Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

SZABO, N. (1997): “Formalizing and securing relationships on public networks”. First Monday, vol. 2, n. 9. https://doi.org/10.5210/fm.v2i9.548

TAPSCOTT, D.; TAPSCOTT, A. (2016): “Blockchain revolution”, 1st ed. New York: Portfolio-Penguin.

technologies in accounting.

Teeter, R.A. and Vasarhelyi, M.A., 2010. Remote Audit: A Review of Audit-Enhancing

VASARHELYI, M. A.; HALPER, F. B. (1991): “The continuous audit of online systems”, In Auditing: A Journal of Practice and Theory.

VASARHELYI, M. A.; HOITASH, R. (2005): “Intelligent Software Agents In Accounting: an evolving scenario”, The Evolving Paradigms of Artificial Intelligence and Expert Systems: An International View, 6.

VASARHELYI, M. A.; KOGAN, A.; TUTTLE, B. M. (2015): “Big data in accounting: An overview”, Accounting Horizons, vol. 29, n. 2: 381-396. https://doi.org/10.2308/acch-51071

Vasarhelyi, M.A. and Halper, F.B., 1991. The continuous audit of online systems. In Auditing: A Journal of Practice and Theory.

VAZIRI, A. (2016): “SMART BOL – Reducing Contractual Enforcement Costs”. https://www.chainofthings.com/news/2016/11/23/smart-bol-reducing-contractualenforcement-costs

Warncke, E. 2017. “Beyond Bitcoin-Decentralized Banking.” Published online June 30, 2017: https://hackernoon.com/beyond-bitcoin-truly-decentralized-banking-d7793edc7d99

Wilken, C. L. and Chenhall, R. H., 2010. A Review of IT Governance: A taxonomy to inform accounting information systems. Journal of Information Systems 24(2), 107 – 146.

YAN, Z. (2017): “Automate Contract Analysis in Auditing”, Rutgers University Working Paper.

YERMACK, D. (2017): “Corporate governance and blockchains”, Review of Finance, vol. 21, n. 1: 7-31. https://doi.org/10.1093/rof/rfw074

YOON, K. (2016): “Weather Variables as Audit Evidence”, Doctoral dissertation – Chapter 4, Rutgers University-Graduate School-Newark.