ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΟ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Μελέτη της τρέχουσας τεχνολογικής στάθμισης στο πεδίο της επικύρωσης τίτλων σπουδών και διερεύνηση των προοπτικών αξιοποίησης της τεχνολογίας blockchain για τον ίδιο σκοπό

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Νικόλαου Γκιζελή

Επιβλέπων : Ασκούνης Δημήτριος
Καθηγητής Ε.Μ.Π.

Αθήνα, Μάρτιος 2020

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Μελέτη της τρέχουσας τεχνολογικής στάθμισης στο πεδίο της επικύρωσης τίτλων σπουδών και διερεύνηση των προοπτικών αξιοποίησης της τεχνολογίας blockchain για τον ίδιο σκοπό

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Νικόλαου Γκιζελή

Επιβλέπων: Ασκούνης Δημήτριος

Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 11η Μαρτίου 2020.

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας

Αθήνα, Μάρτιος 2020

.....

Νικόλαος Γκιζελής

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

Περίληψη

Η τεχνολογία blockchain είναι σχετικά πρόσφατη και έχει αποτελέσει σημείο έρευνας ως προς την εφαρμογή της σε πολλούς κλάδους. Στην παρούσα διπλωματική εργασία θα αναλυθεί η τεχνολογία blockchain σε επίπεδο δομής, αρχιτεκτονικής αλλά και λειτουργίας. Η βελτιστοποίηση του μηχανισμού πιστοποίησης των τίτλων σπουδών αποτελεί φλέγον θέμα στην ακαδημαϊκή κοινότητα. Θα αναλυθεί η υφιστάμενη κατάσταση στο τομέα της πιστοποίησης των τίτλων σπουδών τόσο με τον παραδοσιακό τρόπο όσο και με την χρήση υπαρχουσών ψηφιακών τεχνικών. Στην συνέχεια θα παρουσιαστεί η χρήση της τεχνολογίας blockchain γενικά στην εκπαίδευση, αλλά και πιο συγκεκριμένα στην πιστοποίηση των τίτλων σπουδών. Μετά την ανάλυση της υπάρχουσας βιβλιογραφίας η τεχνολογία blockchain φαίνεται να αποτελεί ένα πολύ ισχυρό εργαλείο για την αναβάθμιση της μεθόδου πιστοποίησης. Η τεχνολογία blockchain παρέχει στα πανεπιστήμια ή στους φορείς πιστοποίησης τη δυνατότητα να εκδίδουν αμετάβλητα ψηφιακά πιστοποιητικά με διαρκή ισχύ, καθώς η αυθεντικότητά τους μπορεί να επαληθευθεί με βάση το blockchain. Η τεχνολογία Blockchain καταργεί την ανάγκη οι εκπαιδευτικοί οργανισμοί να επικυρώνουν τα διαπιστευτήρια. Δεδομένου ότι τα πιστοποιητικά που εκδίδονται στο blockchain μπορούν να επαληθευτούν αυτόματα, οι εκπαιδευτικοί οργανισμοί δεν θα χρειάζεται πλέον να διαθέτουν πόρους για αυτή την ανάγκη, μειώνοντας σημαντικά το διοικητικό τους φορτίο. Η τεχνολογία Blockchain επιτρέπει σε όλα αυτά τα συστήματα να επικυρώνουν αυτόματα πιστοποιητικά από οποιονδήποτε εκδότη σε οποιαδήποτε μορφή (μεταδεδομένων) με πάρα πολύ χαμηλό κόστος. Παρόλα αυτά η τεχνολογία αυτή παρουσιάζει και κάποια μειονεκτήματα. Η τεχνολογία blockchain αντιμετωπίζει τόσο τεχνικούς όσο και νομοθετικούς φραγμούς. Ένας τρόπος κατάχρησης του συστήματος είναι η επίθεση κατά 51%. Αυτό σημαίνει ότι κάποιος ελέγχει το ήμισυ του δικτύου, δηλαδή το 51%, έτσι ώστε οι συναλλαγές να μην μπορούν να επαληθευτούν όπως πρέπει, και αυτό έχει ως αποτέλεσμα ψευδείς πληροφορίες να μπορούν να προστεθούν στο blockchain. Είναι σαφές όμως ότι τα πλεονεκτήματα της τεχνολογίας αυτής μέχρι στιγμής την καθιστούν απαραίτητο μελλοντικό εργαλείο για μια πληθώρα εφαρμογών.

Λέξεις Κλειδιά: Blockchain, Πιστοποίηση/Επικύρωση Τίτλων Σπουδών, Εκπαίδευση, Ψηφιακά Πιστοποιητικά

Abstract

Blockchain technology is relatively recent and has been the focus of research in many fields. In this diploma thesis, blockchain technology will be analyzed in terms of rationale, architecture and operation. The optimization of the certification mechanism is a burning issue in the academic community. The current situation in the field of qualification certification will be analyzed in the traditional way, as well as using existing digital techniques. As a following step, the use of blockchain technology in education and more specifically in qualification certification will be presented. After analyzing the existing literature, blockchain technology seems to be a very powerful tool for upgrading the certification method. Blockchain enables universities or certification bodies to issue unchanged digital certificates with enduring validity, as their authenticity can be verified by blockchain. Blockchain technology abolishes the status of educational organizations to validate credentials. As certificates issued on blockchain can be verified automatically, educational organizations will no longer need to allocate resources for this need, significantly reducing their administrative burden. Blockchain technology allows all these systems to automatically validate certificates from any publisher in any form (metadata) at a very low cost. However, this technology also has some drawbacks. Blockchain technology faces both technical and legislative barriers. One way to abuse the system is the attack by 51%. This means that someone controls half of the network, that is 51%, so that transactions cannot be verified properly, and this results in false information being added to the blockchain. But it is clear that the advantages of this technology so far make it an indispensable future tool for a multitude of applications.

Keywords: Blockchain Technology, Qualification Certification, Digital Certificates, Education

Ευχαριστίες

Με την ολοκλήρωση της παρούσας διπλωματικής εργασίας νιώθω την ανάγκη να εκφράσω τις ιδιαίτερες ευχαριστίες μου στον Καθηγητή του Ε.Μ.Π. κ. Δημήτριο Ασκούνη για την ευκαιρία που μου έδωσε με την εκπόνηση της εργασίας αυτής και για την επίβλεψη που παρείχε.

Επίσης, θα ήθελα να ευχαριστήσω θερμά τους Παναγιώτη Κοκκινάκο και Ουρανία Μακράκη για την πολύ καλή συνεργασία που είχαμε καθ' όλη τη διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας, καθώς και για την πολύτιμη βοήθεια και καθοδήγηση μου προσέφεραν.

Ευχαριστώ ακόμα τον καθηγητή κ. Ιωάννη Ψαρρά και τον Αναπληρωτή Καθηγητή Ε.Μ.Π κ. Χρυσόστομο Δούκα για την συμμετοχή τους στην επιτροπή εξέτασης της διπλωματικής εργασίας μου.

Τέλος θα ήθελα να ευχαριστήσω την οικογένεια μου για όλη τη στήριξη και βοήθεια που μου έδωσαν.

Πίνακας Περιεχομένων

Περίληψη 5

Abstract 7

Κεφάλαιο 1: Εισαγωγή 15

1.1 Ορισμός προβλήματος 15

1.2 Σημασία της πιστοποίησης των τίτλων σπουδών 15

Κεφάλαιο 2: Τρέχουσες πρακτικές πιστοποίησης 18

2.1Κατηγοριοποίηση μάθησης 18

2.2Τα βασικά χαρακτηριστικά της πιστοποίησης 19

2.3Οργανισμός πιστοποίησης τίτλων σπουδών 20

2.4Οργανισμός πιστοποίησης προσόντων και άτυπης μάθησης 20

2.5Συστήματα πιστοποίησης επαγγελματικών προσόντων στις χώρες της Ευρωπαϊκής Ένωσης 21

2.6Τεχνικές πιστοποίησης επαγγελματικών προσόντων 24

2.7 Κριτήρια επιλογής τεχνικών πιστοποίησης προσόντων 25

2.8 Προβλήματα και περιορισμοί της καθιερωμένης πιστοποίησης. 25

2.8.1 Προβλήματα για πιστοποίηση τίτλων σπουδών 25

2.8.2 Προβλήματα πιστοποίησης άτυπης μάθησης 27

Κεφάλαιο 3: Η τεχνολογία Blockchain 29

3.1 Ανάγκη για νέες μεθόδους - εισαγωγή για την τεχνολογία blockchain 29

3.2 Ιστορική αναδρομή των blockchain (bitcoin) 29

3.3 Αρχές και δομή λειτουργίας blockchain (hash) 31

3.3.1 Hash 33

3.3.2 Δημόσια και ιδιωτικά κλειδιά 34

3.3.3 Κρυπτογραφία 34
3.4 Αρχιτεκτονική ενός Blockchain 35
3.4.1 Αποκεντρωμένος, Κατανεμημένος Λογαριασμός 36
3.4.2 Σύστημα για την ανώνυμη επαλήθευση ταυτότητας και ιδιοκτησίας 36
3.4.3 Σύστημα για τη διασφάλιση μόνιμων άφθαρτων μητρώων 37
3.4.4 Έκδοση πιστοποιητικού με τη χρήση ψηφιακών υπογραφών 37
3.4.5 Υποδομές δημόσιου κλειδιού (Public Key Infrastructure) 39
3.5 Είδη blockchain (ιδιωτικά / δημόσια). 39
3.6 Κρυπτονομίσματα 41
3.7 Χρήση της τεχνολογίας blockchain ως δημόσια εγγραφή 42
3.8 Κοινωνική αξία και δυναμική της τεχνολογίας (αξιοπιστία, διαφάνεια) 43
3.8.1 Αυτοκυριαρχία και ταυτότητα 44
3.8.2 Εμπιστοσύνη 46
3.8.3 Διαφάνεια και προέλευση 47
3.8.4 Αμετάβλητο 48
3.8.5Διαμεσολάβηση 48
3.9 Προοπτική για μελλοντική αξιοποίηση σε πλήθος εφαρμογών 49
Κεφάλαιο 4: Η προστιθέμενη αξία της τεχνολογίας blockchain στην πιστοποίηση τίτλων σπουδών 52
4.1 Περιορισμοί των έντυπων πιστοποιητικών 52
4.2 Περιορισμοί ψηφιακών πιστοποιητικών (χωρίς blockchain) 53
4.3 Ψηφιακά πιστοποιητικά με τεχνολογία Blockchain 54
4.4 Πλεονεκτήματα για τον παραλήπτη 54
4.5 Πλεονεκτήματα για τον Εκδότη 55
4.6 Πιστοποίηση Ταυτότητας με χρήση Blockchain 55

4.7 Χρήση πιστοποιημένης αυτοκυρίαρχης ταυτότητας (self-sovereign identity) 56
4.8 Έκδοση Πιστοποιητικών με άμεση χρήση του Blockchain 57
4.9 Έκδοση συμπληρώματος διπλώματος (diploma supplement) σε blockchain 58
4.10 Ψηφιακά πιστοποιητικά με τη χρήση της τεχνολογίας Blockchain 59
4.10.1 Η προστιθέμενη αξία των Ψηφιακών Πιστοποιητικών με την ασφάλεια του Blockchain 59
4.10.2 Αρχιτεκτονική Ψηφιακών Πιστοποιητικών με ασφάλεια Blockchain 60
4.10.3 Αυτοκυριαρχικές ταυτότητες με χρήση της τεχνολογίας Blockchain 61
4.10.4 Πιστοποίηση αυτοκυρίαρχης ταυτότητας 62
4.11 Εφαρμογές της Τεχνολογίας Blockchain στην Εκπαίδευση 62
4.11.1 Έκδοση Πιστοποιητικών 63
4.12 Blockcerts: Ένα ανοικτό πρότυπο για πιστοποιητικά σπουδών με τη χρήση Blockchain 64
4.13 Μελέτες περίπτωσης εφαρμογής blockchain 66
4.13.1 Sony Global Education 66
4.13.2 Uport 67
4.13.3 Open University UK 68
4.13.4 Πανεπιστήμιο Λευκωσίας 68
4.13.5 Openbadges 69
Κεφάλαιο 5: Συμπεράσματα 74
5.1 Πλεονεκτήματα έκδοσης ψηφιακών πιστοποιητικών μέσω της τεχνολογίας blockchain .. 74
5.2. Προτάσεις για το μέλλον 76
5.3. Προκλήσεις εφαρμογής 77
Βιβλιογραφία 80

Κεφάλαιο 1: Εισαγωγή

1.1Ορισμός προβλήματος

Η πιστοποίηση των τίτλων σπουδών κατέχει κεντρικό ρόλο στον τομέα της εκπαίδευσης, αφού είναι απαραίτητη για την απόδειξη/επαλήθευση των προσόντων των εκπαιδευόμενων. Ωστόσο ο τρόπος με τον οποίο πραγματοποιείται επί του παρόντος τόσο η επικύρωση όσο και η διαχείριση τίτλων σπουδών παρουσιάζει πολλά μειονεκτήματα. Τα κυριότερα εξ αυτών αφορούν στη διάθεση των πιστοποιητικών σε μορφές ευάλωτες σε απώλεια, φθορά ή και καταδολίευση, στην εξάρτηση από τους ίδιους τους εκπαιδευτικούς οργανισμούς ή τρίτους φορείς για την έκδοση και επικύρωσή τους αλλά και τις ίδιες τις χρονοβόρες διαδικασίες που η τελευταία ενέχει, όπως και στην αδυναμία επαλήθευσης ανεπίσημων μορφών εκπαίδευσης που συνθέτουν ολοένα και περισσότερο την έννοια της δια βίου εκπαίδευσης.

Με βάση τα παραπάνω, αντικείμενο της διπλωματικής εργασίας αποτελεί η μελέτη της τρέχουσας τεχνολογικής στάθμισης στο πεδίο της διαχείρισης και επικύρωσης τίτλων σπουδών και προσόντων εργασιακής εμπειρίας και στο πλαίσιο αυτής η εύρεση και καταγραφή πρόσφατων σχετικών εξελίξεων και πρωτοβουλιών, που παρέχουν λύση σε ένα ή περισσότερα από τα προαναφερθέντα προβλήματα. Ιδιαίτερη έμφαση δίνεται στην τεχνολογία blockchain και στην ανάλυση των ωφελειών, αδυναμιών, ευκαιριών και κινδύνων που προκύπτουν από την αξιοποίησή της για τη διαχείριση και επαλήθευση τίτλων σπουδών και εργασιακής εμπειρίας.

1.2 Σημασία της πιστοποίησης των τίτλων σπουδών

Η διαδικασία της πιστοποίησης αποτελεί μια μορφή αξιολόγησης η οποία βασίζεται σε σαφή, προσδιορισμένα κριτήρια, διεθνώς αποδεκτά. Προϋπόθεση των αντικειμενικών αυτών κριτηρίων, είναι πρωτίστως να έχουν δημοσιοποιηθεί τόσο ποσοτικά όσο και ποιοτικά μαζί με τους δείκτες μέτρησης που χρησιμοποιούν και να προσαρμόζονται στις Αρχές και Κατευθυντήριες Οδηγίες για τη Διασφάλιση Ποιότητας στον Ευρωπαϊκό Χώρο Ανώτατης Εκπαίδευσης (ΕΧΑΕ). Οι ακαδημαϊκές πιστοποιήσεις αφορούν σε όλες τις μορφές σπουδών Ανώτατης Εκπαίδευσης

(διασυνοριακά, διακρατικά, e-learning), τα Δια Βίου Μάθησης και τα Εσωτερικά Συστήματα Διασφάλισης Ποιότητας των Ιδρυμάτων. Σύμφωνα με τις βασικές αρχές της πιστοποίησης, διακρίνεται ο σχεδιασμός και η αναθεώρηση των Προγραμμάτων Σπουδών έτσι ώστε να συμβαδίζουν με την αιχμή της επιστήμης, να είναι ελκυστικά ως προς το τι προφέρουν και να ακολουθούν την τρέχουσα αγορά εργασίας. Ένα επιπλέον βασικό χαρακτηριστικό αποτελεί η δυνατότητα έρευνας και καινοτομίας από μια πιο φοιτητοκεντρική οπτική. Επιπρόσθετα χαρακτηριστικά αποτελούν:

- Η Διασφάλιση Ποιότητας και η εφαρμογή της, η οποία βασίζεται στη ροή δεδομένων και πληροφοριών με στόχο την αποτελεσματικότερη διαχείριση των Προγραμμάτων Σπουδών και
- Η Επικύρωση της ποιότητας των Προγραμμάτων Σπουδών, ως μέσον επαλήθευσης της συμμόρφωσής τους με τις απαιτήσεις του προτύπου ποιότητας, ως καταλύτης για τη βελτίωσή τους και ως νέα προοπτική στη διεθνή ανταγωνιστικότητα των τίτλων που απονέμονται (Adip.gr, 2019).

Ο στόχος της πιστοποίησης είναι η διασφάλιση της απόκτησης ενός συνδυασμού γνώσεων, ικανοτήτων και δεξιοτήτων για τον σπουδαστή, τα οποία λειτουργούν προς όφελος των φοιτητών, των γονέων, των πανεπιστημίων και των εργοδοτών. Τα μαθησιακά αυτά αποτελέσματα, αντικατοπτρίζονται στα αντίστοιχα κριτήρια της πιστοποίησης. Κατά συνέπεια, η διαδικασία της πιστοποίησης διασφαλίζει το έκαστο εκπαιδευτικό πρόγραμμα από τη μία και τα επαγγελματικά προσόντα του σπουδαστή από την άλλη, μέσω μιας διαδικασίας εκπαίδευσης που καλύπτει τουλάχιστον το ελάχιστο των κριτηρίων που έχουν διαμορφωθεί στον Ευρωπαϊκό Χώρο Ανώτατης Εκπαίδευσης (ΕΧΑΕ) αλλά και στα διεθνή πρότυπα επαγγελματικών προσόντων (Doatap.gr, 2019).

Αντίστοιχα, στα Ελληνικά δεδομένα, η πιστοποίηση οδηγεί σε αναβάθμιση της αξίας των ελληνικών τίτλων σπουδών και κατά συνέχεια και σε διεθνή αναγνώρισή τους. Σε ανταγωνισμό προς τις ευρωπαϊκές χώρες έρχεται η Ελλάδα σε αυτόν τον τομέα, καθώς η πιστοποίηση εφαρμόζεται στη συντριπτική πλειοψηφία των προσφερόμενων προγραμμάτων σπουδών πανευρωπαϊκά. Αποτέλεσμα της πιστοποίησης είναι η δυνατότητα συμμετοχής και συνέχισης των σπουδαστών σε Μεταπτυχιακά Προγράμματα Σπουδών της Ευρώπης και διεθνώς, τα περισσότερα εκ των οποίων ανταποκρίνονται στη κατοχή πιστοποιημένου τίτλου σπουδών. Είναι γεγονός ότι η

κατοχή πιστοποιημένων τίτλων σπουδών αποτελεί βασικό παράγοντα στην τάση της αγοράς ως προς την εύρεση εργασία και αποτελεί κύριο πιστοποιητικό και κριτήριο πρόσληψης για την αγορά εργασίας (ειδικότερα σε περιπτώσεις έλλειψης εμπειρίας και πρακτικής). Ένας επιπλέον παράγοντας, είναι ότι μέσω της πιστοποίησης υπάρχει αυτομάτως μία σύνδεση ενός προγράμματος σπουδών με τον οικείο επαγγελματικό κλάδο και τα απαιτούμενα επαγγελματικά προσόντα. Για τον εργοδότη, η πιστοποίηση παρέχει μια μορφή εγγύησης και διασφαλίζει ότι ο απόφοιτος κατέχει τις απαιτούμενες γνώσεις, ικανότητες και δεξιότητες που απαιτεί μια συγκεκριμένη θέση εργασίας. Τέλος, οι διακρατικές συνεργασίες σε κοινά προγράμματα σπουδών προαπαιτούν την πιστοποίηση των προγραμμάτων αυτών (Γεροθανάσης, 2017).

Κεφάλαιο 2: Τρέχουσες πρακτικές πιστοποίησης

2.1 Κατηγοριοποίηση μάθησης

Οι μορφές και οι τύποι της μάθησης ποικίλουν, ωστόσο υπάρχει η δυνατότητα κατηγοριοποίησης τους σε ένα γενικότερο πλαίσιο. Κατά συνέχεια διακρίνονται οι εξής μορφές μάθησης: Κατ' αρχάς, είναι η τυπική μάθηση (Formal learning), η οποία αποτελεί μια μέθοδο διδασκαλίας (μαθησιακής δραστηριότητας) που συντελείται μέσα σε ένα μεθοδικό και δομημένο πλαίσιο (π.χ. το τυπικό εκπαιδευτικό σύστημα, η ενδοεπιχειρησιακή κατάρτιση κ.λπ.). Η άτυπη μάθηση (non-formal learning), αποτελεί μορφή μάθησης η οποία ενσωματώνεται σε προσχεδιασμένες δραστηριότητες, οι οποίες δεν είναι σαφώς ορισμένες ως διαδικασίες μάθησης, ωστόσο περιέχουν έναν σημαντικό παράγοντα διαδικασίας απόκτησης γνώσεων. Μελετώντας τις δυο αυτές μορφές μάθησης, θα μπορούσε να γίνει ένας περαιτέρω διαχωρισμός, σύμφωνα με τον οποίο στην άτυπη μάθηση περιλαμβάνεται κατ' αρχάς αυτό που μερικές φορές περιγράφεται ως ημιδομημένη μάθηση και αφορά στη μάθηση η οποία είναι ενσωματωμένη σε ένα περιβάλλον με στοιχεία μάθησης (όπως π.χ. η διοίκηση ολικής ποιότητας) και δεύτερον η περιστασιακή μάθηση, η οποία απορρέει μέσα από καθημερινές περιστάσεις (συμπεριλαμβανομένου και του χώρου εργασίας) και η οποία ορίζεται και ως ανεπίσημη μάθηση. Η ανεπίσημη μάθηση (informal learning) θα μπορούσε να ορισθεί ως η μέθοδος εκμάθησης μέσα από δράσεις της καθημερινής ζωής οι οποίες σχετίζονται με το εργασιακό περιβάλλον, το οικογενειακό περιβάλλον, τον ελεύθερο χρόνο (π.χ. το μεγάλωμα των παιδιών, τη συμμετοχή σε ένα πολιτιστικό σύλλογο κ.λπ.). Η ανεπίσημη μάθηση κατά συνέπεια, αποτελεί παρακλάδι της μη τυπικής μάθησης. Συχνά αναφέρεται ως εμπειρική μάθηση και μπορεί να γίνει κατανοητή έως ένα βαθμό ως περιστασιακή μάθηση (Garrick, 2012). Ένα άτομο, προκειμένου να μπορέσει να εργασθεί ή να εξελιχθεί σε ένα εργασιακό περιβάλλον, απαραίτητη απαίτηση αποτελούν τα προσόντα (qualifications) που διαθέτει, σε συνδυασμό (όχι πάντα) με κάποιο επίσημο έγγραφο (βεβαίωση, δίπλωμα) των επιτευγμάτων, το οποίο επιβεβαιώνει την επιτυχή ολοκλήρωση της εκπαίδευσης, της κατάρτισης ή της ικανοποιητικής απόδοσης σε τεστ ή εξετάσεις του ατόμου. Παρατηρείται μια διαφορετική αντίληψη για τον όρο «προσόντα» σε κάθε χώρα. Εν μέρει, εκφράζει τη δυνατότητα - επίσημα καθορισμένης από συμβόλαια εργασίας ή συλλογικές συμβάσεις - άσκησης μιας καθορισμένης δουλειάς ή την

ικανοποίηση των απαιτήσεων για έναν χώρο εργασίας. Επίσης, ο όρος προσόντα πιθανά αναφέρεται στο ατομικό επίπεδο εκπαίδευσης/κατάρτισης ή στις ικανότητες αντιμετώπισης επαγγελματικών προκλήσεων. Τα προσόντα εγείρουν ένα σύνολο αξιώσεων και πλεονεκτημάτων, τα οποία καθορίζουν τη θέση του ατόμου στην επαγγελματική ιεραρχία ή στο εργασιακό του περιβάλλον (Manutietal., 20150).

2.2Τα βασικά χαρακτηριστικά της πιστοποίησης

Ο βασικός ορισμός της πιστοποίησης, όπως έχει αναλυθεί και πρωτύτερα, καθορίζει μια επίσημη διαδικασία επικύρωσης του συνόλου των γνώσεων, της τεχνογνωσίας και των δεξιοτήτων ενός ατόμου, μέσω μιας τυποποιημένης διαδικασίας αξιολογήσεως. Είναι γνωστό ότι για την απόκτηση γνώσεων και κατ' ακόλουθα ένα πιστοποιητικό, βασικός παράγοντας είναι ο χρόνος για την εμπέδωση των απαραίτητων γνώσεων και ανάλογα με την χρονική διάρκεια είναι και το κόστος συμμετοχής σε συνάρτηση πάντα και με τον οργανισμό πιστοποίησης. Η κάθε επαγγελματική πρόταση για κατάρτιση, με σταθερά και τυπικά χαρακτηριστικά περιέχει πάντα την αντίφαση της σταθερότητας σε ένα διαρκώς μεταβαλλόμενο περιβάλλον. Γι' αυτόν τον λόγο τονίζεται ιδιαίτερα η έννοια της επικαιροποίησης των γνώσεων και των δεξιοτήτων μέσω της επαναπιστοποίησης. Η διάρκεια που απαιτείται της απόκτησης μιας πιστοποίησης αποτελεί μη υπολογίσιμο παράγοντα με την έννοια ότι έχει πολλές μεταβλητές οι οποίες πρέπει να λαμβάνονται υπόψιν. Ο παράγοντας του χρόνου σπουδών, επηρεάζεται τόσο από το είδος της πιστοποίησης όσο και από την προθυμία που έχει ο σπουδαστής στο να επικεντρωθεί σε αυτό που κάνει, να επιμορφωθεί και να αποκτήσει όλες τις κατάλληλες προϋποθέσεις που απαιτεί η κάθε πιστοποίηση πριν την εξέταση της (ΦΩΤΌΠΟΥΛΟΣ & ΖΆΓΚΟΣ, 2016).

Το κόστος αποτελεί έναν επιπλέον αστάθμητο παράγοντα, με την έννοια ότι το κόστος διαφέρει για κάθε πιστοποίηση κάθε οργανισμού. Σε έναν γενικό προϋπολογισμό, ένα μέσο κόστος απόκτησης πιστοποίησης κυμαίνεται γύρω στα 300 ευρώ. Σε όλες τις οικονομικά αναπτυσσόμενες χώρες, οι περισσότεροι επαγγελματίες προσχωρούν σε μία επαναπιστοποίηση αφενός των γνώσεων που ήδη διαθέτουν και αφετέρου των δεξιοτήτων τους, με σκοπό την επάρκειά τους στην άσκηση του επαγγελματικού τους προσανατολισμού. Ο λόγος που θα μπορούσε κάποιος να προβεί σε επαναπιστοποίηση έχει κάποιους συγκεκριμένους στόχους. Από τη μία έχει ως σκοπό την παρακολούθηση κάποιων συγκεκριμένων ωρών εκπαίδευσης και επομένως, την ύπαρξη τυπικών

προσόντων και δεξιοτήτων και από την άλλη είναι επιφορτισμένη με ένα πολύ σημαντικό και βασικό ρόλο, δηλαδή την πιστοποίηση-πέραν των τυπικών δεξιοτήτων- και των ουσιαστικών προσόντων και δεξιοτήτων των επαγγελματιών που θα μετατραπούν περισσότερο αποδοτικοί στον χώρο εργασίας τους(Τητήρου, 2017).

2.3Οργανισμός πιστοποίησης τίτλων σπουδών

Στη Ελλάδα, έως το 1979, η αρμοδιότητα της αναγνώρισης των τίτλων σπουδών Πανεπιστημιακής Εκπαίδευσης αποτελούσε αποκλειστικότητα των Πανεπιστημίων. Το 1979 με την ψήφιση ενός νέου νόμου ιδρύθηκε το Διεπιστημονικό Κέντρο Αναγνώρισης Τίτλων Σπουδών Αλλοδαπής (ΔΙ.Κ.Α.Τ.Σ.Α). Η αρμοδιότητα αναγνώρισης Πανεπιστημίων της Αλλοδαπής καθώς και των τίτλων που απονέμονται παρεχόταν αποκλειστικά από αυτή την Υπηρεσία και διεκπεραιωνόταν βάσει των διατάξεων του ιδρυτικού του νόμου 741/1977. Τον Απρίλιο του 2005 με την κατάργηση του νομικού προσώπου δημοσίου δικαίου (Ν.Π.Δ.Δ.), με την επωνυμία ΔΙ.Κ.Α.Τ.Σ.Α. (Ν. 741/1977) και της δημόσιας υπηρεσίας με τίτλο Ινστιτούτο Τεχνολογικής Εκπαίδευσης (Ι.Τ.Ε.) (Ν 1404/1983), οι αρμοδιότητές περιήλθαν στον Διεπιστημονικό Οργανισμό Αναγνώρισης Τίτλων Ακαδημαϊκών και Πληροφόρησης (Δ.Ο.Α.Τ.Α.Π.) με το Ν.3328/01-04-2005 (Α’ 80) - όπως τροποποιήθηκε με το Ν.3369/2005 (ΦΕΚ Α΄ 171/6-7-2005) και το Ν.3467/2006 (ΦΕΚ 128/Α/2006). Ο Δ.Ο.Α.Τ.Α.Π. είναι ο αρμόδιος Ελληνικός Οργανισμός για την αναγνώριση των τίτλων σπουδών από πανεπιστήμια του εξωτερικού, τόσο για προπτυχιακές όσο και για μεταπτυχιακές σπουδές. Ο Οργανισμός ιδρύθηκε με το Ν.3328/01-04-2005 (Α’ 80) ως νομικό πρόσωπο δημοσίου δικαίου (Ν.Π.Δ.Δ.), η έδρα του είναι στην Αθήνα, αν και διατηρεί παράρτημα και στη Θεσσαλονίκη και εποπτεύεται από το υπουργείο Εθνικής Παιδείας και Θρησκευμάτων (Doatap.gr, 2019).

2.4Οργανισμός πιστοποίησης προσόντων και άτυπης μάθησης

Ο Εθνικός Οργανισμός Πιστοποίησης Προσόντων και Επαγγελματικού Προσανατολισμού (Ε.Ο.Π.Π.Ε.Π.) είναι ένα Νομικό Πρόσωπο Ιδιωτικού Δικαίου, εποπτευόμενο από τον Υπουργό Παιδείας και Θρησκευμάτων, Πολιτισμού και Αθλητισμού. Συγκροτεί το διάδοχο φορέα της

συνένωσης του Εθνικού Οργανισμού Πιστοποίησης Προσόντων (Ε.Ο.Π.Π.), του Εθνικού Κέντρου Πιστοποίησης Δομών Διά Βίου Μάθησης (Ε.Κ.Ε.Π.Ι.Σ.) και του Εθνικού Κέντρου Επαγγελματικού Προσανατολισμού (Ε.Κ.Ε.Π.). Βασικός σκοπός του οργανισμού αποτελεί η σύνδεση της εκπαίδευσης και της κατάρτισης με τις κατ' εξοχήν ανάγκες της αγοράς εργασίας, η αναβάθμιση των επαγγελματικών προσόντων του εργατικού δυναμικού, η ενδυνάμωση των προοπτικών απασχόλησής του και η ενίσχυση της κοινωνικής συνοχής. Ο Ε.Ο.Π.Π.Ε.Π. αποτελεί έναν επιτελικό φορέα διοίκησης του Εθνικού Δικτύου Διά Βίου Μάθησης ενώ παράλληλα είναι ο αρμόδιος φορέας για την ανάπτυξη του Εθνικού Πλαισίου Προσόντων (ΕΠΠ). Τα βασικά αντικείμενα της δράσης του αποτελούν η ανάπτυξη και η εφαρμογή ενός ολοκληρωμένου εθνικού συστήματος πιστοποίησης της μη τυπικής εκπαίδευσης (αρχική και συνεχιζόμενη επαγγελματική κατάρτιση και γενική εκπαίδευση ενηλίκων) και η παροχή επιστημονικής υποστήριξης των υπηρεσιών του Επαγγελματικού Προσανατολισμού και Συμβουλευτικής στη Ελλάδα. Επιπλέων, φέρει ευθύνη ως προς τη διασφάλιση και την αναβάθμιση της ποιότητας, στην παροχή της μη-τυπικής εκπαίδευσης. Ασχολείται με την πιστοποίηση των γνώσεων, των δεξιοτήτων και των ικανοτήτων που αποκτώνται μέσω μιας μη-τυπικής και άτυπης μαθησιακής διαδρομής και τέλος, παρέχει υπηρεσίες επαγγελματικού προσανατολισμού και συμβουλευτικής (Simota, 2019).

2.5Συστήματα πιστοποίησης επαγγελματικών προσόντων στις χώρες της Ευρωπαϊκής Ένωσης

Στις υπόλοιπες ευρωπαϊκές χώρες, παρατηρείται μια ποικιλομορφία ως προς τις μεθόδους αναγνώρισης και πιστοποίησης των προσόντων που έχουν προκύψει από τη συμμετοχή σε συνεχιζόμενη επαγγελματική κατάρτιση και από την άτυπη μάθηση. Ωστόσο, ένας κοινός παράγοντας τα τελευταία δεκαπέντε χρόνια, αποτελεί η ένταξη και διεύρυνση της συζήτησης και έχουν αναληφθεί νομοθετικές πρωτοβουλίες σε όλες τις χώρες. Οι ακολουθούμενες μέθοδοι εμφανίζουν μεταξύ τους διαφορές που σχετίζονται με τα υφιστάμενα εκπαιδευτικά συστήματα, την κοινωνική αποδοχή της συνεχιζόμενης κατάρτισης και τις πολιτικές διά βίου μάθησης, καθώς και τις ιδιομορφίες στην αγορά εργασίας. Σε μια προσπάθεια κατηγοριοποίησης των εφαρμοζόμενων συστημάτων, βασιζόμενη σε αντίστοιχη ομαδοποίηση των χωρών, προκύπτουν τα εξής:

Ως πρώτη ομάδα, είναι η Γερμανία και η Αυστρία. Οι δύο αυτές χώρες διαθέτουν ισχυρά συστήματα αρχικής επαγγελματικής εκπαίδευσης και κατάρτισης, τα οποία βασίζονται στο δυαδικό σύστημα (συνδυασμός εκπαίδευσης και εργασιακής εμπειρίας). Οι διαδικασίες που χρησιμοποιούν για την εκπαίδευση και τη πιστοποίηση είναι εξειδικευμένες και τυποποιημένες και ως τέτοιες αναγνωρίζονται από την κοινωνία και την αγορά εργασίας. Τόσο η εκπαίδευση / κατάρτιση, όσο και η πιστοποίηση δομούνται βάσει των επαγγελματικών περιγραμμάτων και συνδέονται με τα επαγγελματικά δικαιώματα, τις ευθύνες και τα επίπεδα ανταμοιβών. Δεν υφίσταται κάποια σημαντική παράδοση στους τρόπους εκμάθησης και πιστοποίησης εκτός του τυπικού συστήματος. Τα τελευταία χρόνια γίνεται μια συζήτηση και κάποιες απόπειρες γύρω από τις πρακτικές εφαρμογές της ενίσχυσης της δια βίου επαγγελματικής κατάρτισης και της εξασφάλισης μιας μεγαλύτερης ευελιξίας στην πιστοποίηση των αποτελεσμάτων της. Ως έννοια-κλειδί έχει θεωρηθεί η διαμόρφωση ενός αρθρωτού συστήματος θεματικών ενοτήτων (modules) για τη σύνδεση αρχικής και συνεχιζόμενης επαγγελματικής κατάρτισης, το οποίο θα δίνει τη δυνατότητα να επανέρχεται κάποιος στην αρχική του κατάρτιση και να αξιολογείται (πιστοποίηση με συμμετοχή σε εξετάσεις) σε συγκεκριμένες θεματικές ενότητες. Η άτυπη μάθηση για τις παραπάνω χώρες αποτελεί ακόμη τομέα αμφισβήτησής. Γενικότερα στη Γερμανία και στην Αυστρία δεν έχουν αναπτυχθεί συστήματα αναγνώρισης επιμέρους προσόντων ή ικανοτήτων, παρότι έχουν ξεκινήσει ορισμένες πειραματικές προσπάθειες (Villalba-Garcia, Souto-Otero & Murphy, 2014). Στη δεύτερη κατηγορία, ανήκουν οι μεσογειακές χώρες (Ελλάδα, Ιταλία, Ισπανία και Πορτογαλία). Τα βασικά χαρακτηριστικά τους που εντοπίζονται (παρ' όλες τις διαφορές μεταξύ τους), είναι η σχετικά αδύναμη παράδοση της επαγγελματικής εκπαίδευσης και της κατάρτισης και γενικότερα η υποτίμηση των επαγγελματικών ικανοτήτων ενός ατόμου. Η άτυπη μάθηση είναι η δεσπόζουσα μορφή ανανέωσης των επαγγελματικών ικανοτήτων και θεωρείται μέγιστης σημασίας η δυνατότητα αναγνώρισης και πιστοποίησής της. Επιπλέον, το κύρος της ακαδημαϊκής εκπαίδευσης και των τυπικών πιστοποιήσεων διατηρείται υψηλό. Ένα εύρος μεθοδολογικών και θεσμικών απαντήσεων έχει προσφάτως εισαχθεί. Ωστόσο, μολονότι τόσο ο δημόσιος, όσο και ο ιδιωτικός τομέας έχουν εστιάσει στην αξία της επιβράβευσης της άτυπης μάθησης, δεν έχουν γίνει ακόμα αρκετά πρακτικά βήματα. Υπάρχει συμφωνία για δημόσιο έλεγχο πάνω στα συστήματα αξιολόγησης ικανοτήτων και πιστοποίησης προσόντων (ιδίως στην Ιταλία και στην Ελλάδα). Παρ' όλα αυτά, υπάρχει έλλειψη σαφούς κανονιστικού πλαισίου και εθνικών προτύπων (π.χ. Μητρώο αναλυτικών επαγγελματικών περιγραμμάτων), πάνω στα οποία θα

μπορούσε να βασιστεί η συνεχιζόμενη εκπαίδευση/κατάρτιση και πιστοποίηση. Στην Ελλάδα έχουν προσφάτως νομοθετηθεί και ενεργοποιηθεί μηχανισμοί και θεσμοί που αναμένεται να αντιμετωπίσουν την ανάγκη πιστοποίησης προσόντων ιδίως μέσω του Εθνικού Συστήματος Σύνδεσης της Επαγγελματικής Εκπαίδευσης και Κατάρτισης με την Απασχόληση (Ε.Σ.Σ.Ε.Ε.Κ.Α.). Βασικοί φορείς πιστοποίησης στο επίπεδο της αρχικής και συνεχιζόμενης κατάρτισης αποτελούν ο Ο.Ε.Ε.Κ. (Οργανισμός Επαγγελματικής Εκπαίδευσης και Κατάρτισης - Υπουργείο Παιδείας) και ο Ε.ΚΕ.ΠΙΣ (Εθνικό Κέντρο Πιστοποίησης - Υπουργείο Απασχόλησης) (ERMENC, 2014). Στην Τρίτη κατηγορία, ανήκουν οι σκανδιναβικές χώρες (Φινλανδία, Νορβηγία, Σουηδία και Δανία), στις οποίες υπάρχουν δύο υποομάδες. Στη Φινλανδία και τη Νορβηγία, η άτυπη μάθηση είναι στο προσκήνιο των συζητήσεων για την εκπαίδευση και την κατάρτιση και επιφέρει προχωρημένου βαθμού πειράματα και θεσμικές μεταρρυθμίσεις. Στις άλλες δύο χώρες είναι πιο περιορισμένο το ενδιαφέρον για το ζήτημα αυτό, μέχρι στιγμής. Γενικότερα στις σκανδιναβικές χώρες υπάρχουν ανεπτυγμένοι θεσμοί στο επίπεδο του κύριου εκπαιδευτικού συστήματος που αφορούν σε όλες τις ηλικίες. Δίνεται μεγάλη σημασία στη μορφή μάθησης στα πλαίσια ενός εργασιακού περιβάλλοντος (ισχυρό σύστημα μαθητείας, ιδίως στη Νορβηγία). Γενικά η Νορβηγία και η Φινλανδία κινούνται πιο γρήγορα σε πρωτοβουλίες αναγνώρισης της άτυπης μάθησης και σύνδεσής της με το εκπαιδευτικό σύστημα. Ωστόσο, παραμένει ισχυρός ο ρόλος των κοινωνικών εταίρων (παράδοση τριμερούς συντονισμού) (MASLO, SURIKOVA,KARTTUNEN&AARNA, 2012). Στην τέταρτη ομάδα περιλαμβάνεται το Ηνωμένο Βασίλειο, η Ιρλανδία και η Ολλανδία. Σε αυτές τις χώρες, αντανακλάται η επίδραση του μοντέλου των Εθνικών Επαγγελματικών Προσόντων (National Vocational Qualifications– NVQ's). Σε αυτά τα κράτη μέλη, η σημασία της μάθησης, μη συμπεριλαμβανομένων των τυπικών συστημάτων, αναγνωρίζεται σχεδόν ομόφωνα. Τα Εθνικά Επαγγελματικά Προσόντα (NVQ's) που παρουσιάστηκαν στο Ηνωμένο Βασίλειο στα τέλη της δεκαετίας του'80, έχουν γίνει ένα κεντρικό σημείο αναφοράς σε ευρωπαϊκό επίπεδο. Το σύστημα βασίζεται στις ικανότητες του κάθε ατόμου και τις συνδέει με την αγορά εργασίας και ειδικότερα με την εργασιακή απόδοση. Τα βασικά του χαρακτηριστικά, δηλαδή η διάρθρωσή του σε θεματικές ενότητες, ο προσανατολισμός στις ικανότητες εργασιακής απόδοσης, η ευελιξία του, η επικέντρωση στις ανάγκες της αγοράς εργασίας (των ατόμων και των επιχειρήσεων), ώθησαν πολλές χώρες να μελετήσουν αυτό το σύστημα προκειμένου να αξιολογήσουν εάν αυτό ή μέρος αυτού είναι δυνατόν να μεταφερθούν με επιτυχία στις δικές τους δομές. Το συγκεκριμένο σύστημα έχει δεχθεί

κριτικές αναφορικά με την αδυναμία διαμόρφωσης αποδεκτών (συναινετικών) προτύπων και περιεχομένων πιστοποίησης, καθώς και ως προς την αξιοπιστία και εγκυρότητα των διαδικασιών αξιολόγησης (Stasz, 2011). Τέλος, η πέμπτη κατηγορία περιλαμβάνει τη Γαλλία, το Βέλγιο και το Λουξεμβούργο. Η Γαλλία έχει αποτελέσει πρωτοπόρο έργο στον προσδιορισμό, την αποτίμηση και την αναγνώριση των άτυπων ικανοτήτων. Το γαλλικό σύστημα ανάλυσης δεξιοτήτων (bilan de compétence) μπορεί να θεωρηθεί ως η πρώτη προσπάθεια για την εισαγωγή ενός πλήρους διαβαθμισμένου συστήματος για την αναγνώριση και αξιολόγηση της άτυπης μάθησης. Μολονότι όμως η χώρα έχει τη μεγαλύτερη και πιο εκτεταμένη εμπειρία σε αυτό το πεδίο, η κοινωνική αναγνώριση η οποία αντιστοιχεί σε αυτή τη μάθηση είναι ακόμα περιορισμένη. Ο νόμος που θεσμοθέτησε το γαλλικό σύστημα ανάλυσης δεξιοτήτων το 1985, προβλέπει την επικύρωση των επαγγελματικών ικανοτήτων που έχουν αποκτηθεί εκτός τυπικής εκπαίδευσης. Η πρωτοβουλία μπορεί να ανήκει είτε στην επιχείρηση είτε στον ίδιο τον εργαζόμενο. Αυτό το δικαίωμα ενισχύθηκε το 1991, έτσι ώστε οι εργαζόμενοι να έχουν το δικαίωμα της εκπαιδευτικής άδειας για να συμμετάσχουν στο σύστημα ανάλυσης δεξιοτήτων. Σκοπός του γαλλικού συστήματος ανάλυσης δεξιοτήτων είναι να υποστηρίζει τους εργαζόμενους έτσι ώστε να είναι σε θέση να κατανοήσουν τις επαγγελματικές και προσωπικές τους δεξιότητές, καθώς και να τους παρέχει κίνητρα για να υλοποιούν τα εκπαιδευτικά και τα επαγγελματικά τους σχέδια. Το Βέλγιο και το Λουξεμβούργο, σε αντίθεση με τη Γαλλία, βρίσκονται ακόμη σε ένα πιο πρωτογενές στάδιο ανάπτυξης και δεν έχουν χαράξει μια σαφή πορεία / στρατηγική (Charraud, 2010).

2.6Τεχνικές πιστοποίησης επαγγελματικών προσόντων

Οι μέθοδοι που χρησιμοποιούνται για τον προσδιορισμό της αξιολόγησης και της πιστοποίησης των αποτελεσμάτων της εκπαίδευσης – κατάρτισης είναι οι γραπτές εξετάσεις, βάσει περιεχομένων που έχουν διδαχθεί, οι γραπτές (ατομικές ή/και ομαδικές) εργασίες, οι προφορικές εξετάσεις βάσει περιεχομένων που έχουν διδαχθεί και οι εξετάσεις μέσω πρακτικής άσκησης - εργαστηριακές εξετάσεις. Στόχος αυτών των μορφών εξέτασης, είναι η αξιόπιστη αποτίμηση και πιστοποίηση της επαγγελματικής εμπειρίας. Οι τεχνικές αυτές, είναι διάφορες μορφές αξιολόγησης που χρησιμοποιούνται στο εκπαιδευτικό σύστημα (π.χ. εξετάσεις), η συγκρότηση, παρακολούθηση και αξιολόγηση ατομικού φακέλου γνώσεων και δεξιοτήτων, ο οποίος

περιλαμβάνει τυχόν πιστοποιητικά σπουδών, βεβαιώσεις εργοδοτών, συστατικές επιστολές, αποδεικτικά στοιχεία επαγγελματικής εμπειρίας κ.λπ., κάποια προσωπική συνέντευξη βασισμένη σεένα συγκεκριμένο ερωτηματολόγιο καθώς και ένας γενικότερος συνδυασμός των προαναφερόμενων, όπως π.χ. επαγγελματικών συνεντεύξεων (για την αναγνώριση του επαγγελματικού προφίλ και των ατομικών ικανοτήτων) και εξετάσεων για την επαγγελματική πιστοποίηση (η πρακτική αυτή ακολουθείται στην Ισπανία) (Τητήρου, 2017).

2.7 Κριτήρια επιλογής τεχνικών πιστοποίησης προσόντων

Τα κριτήρια της αξιοπιστίας και της εγκυρότητας συνδέονται άμεσα με την εμπιστοσύνη που αποδίδεται σε μια συγκεκριμένη μέθοδο πιστοποίησης των προσόντων, καθώς και στις τεχνικές που απορρέουν από αυτή. Η αξιοπιστία μιας αξιολόγησης εξαρτάται από τη δυνατότητα αναπαραγωγής των αποτελεσμάτων, σε περίπτωση επανεξέτασης σε μια δεύτερη φάση, από άλλους επιβλέποντες.

Η ισχύς συνδέεται με το κατά πόσο η διαδικασία, τα μέσα και οι τεχνικές αξιολόγησης και πιστοποίησης των προσόντων μετρούν αυτό που ήταν ο αρχικός στόχος και όχι κάτι άλλο. Το βασικότερο στοιχείο είναι η αξιοπιστία και η εγκυρότητα της διαδικασίας και είναι απαραίτητο να συσχετισθούν με κάποια σημεία αναφοράς, δηλαδή με κριτήρια αξιολόγησης. Τέτοια σημεία αναφοράς μπορούν να αποτελούνται από τις ολοκληρωμένες επαγγελματικές προδιαγραφές, τις οποίες καλείται να σκιαγραφήσει και να υποδείξει το επαγγελματικό περίγραμμα μιας ειδικότητας, εφόσον η ανάπτυξή του έχει τηρήσει τις βασικές επιστημονικές και μεθοδολογικές προϋποθέσεις και εφόσον έχει εξασφαλίσει τη συναίνεση των εμπλεκόμενων κοινωνικών συνομιλητών (εργαζομένων και εργοδοτών) (eoppep.gr, 2019).

2.8 Προβλήματα και περιορισμοί της καθιερωμένης πιστοποίησης.

2.8.1 Προβλήματα για πιστοποίηση τίτλων σπουδών

Το έργο που καλείται να φέρει εις πέρας ο Δ.Ο.Α.Τ.Α.Π. είναι ιδιαίτερα περίπλοκο δεδομένης της ποικιλομορφίας των διαφορετικών εκπαιδευτικών συστημάτων που ακολουθούνται τόσο μεταξύ

των κρατών-μελών της Ευρωπαϊκής Ένωσης όσο και μεταξύ διαφορετικών χωρών παγκοσμίως. Το διαφορετικό Νομικό Πλαίσιο που διέπει τις σπουδές στην αλλοδαπή αλλά και τα αλλιώτικα προγράμματα σπουδών που ακολουθούνται, παρεμποδίζουν την όλη διαδικασία. Σε περιπτώσεις αρκετών χωρών τα απαιτούμενα μαθήματα για τη λήψη πτυχίου είναι πολύ λιγότερα σε σχέση με τα αντίστοιχα των ελληνικών ή ευρωπαϊκών πανεπιστημίων. Σε αυτές τις περιπτώσεις, οι ενδιαφερόμενοι καλούνται συνήθως να εξεταστούν σε ένα συγκεκριμένο αριθμό μαθημάτων, με την διαδικασία της εξέτασης, η οποία διοργανώνεται από τον Δ.Ο.Α.Τ.Α.Π., προκειμένου να χορηγηθεί μια μορφή ισοτιμίας. Μετά τη διοικητική μεταρρύθμιση του οργανισμού που ακολούθησε τη μετονομασία του από ΔΙ.Κ.Α.Τ.Σ.Α. σε Δ.Ο.Α.Τ.Α.Π., καταβλήθηκε προσπάθεια για βελτίωση των παρεχόμενων υπηρεσιών και εισήχθησαν κριτήρια ποιότητας. Σε αυτό το πλαίσιο καταβάλλεται προσπάθεια ώστε η διαδικασία αναγνώρισης να ολοκληρώνεται σε ένα διάστημα τριών μηνών, σε περιπτώσεις τίτλων από προγράμματα πανεπιστημίων που έχουν ήδη αναγνωριστεί από τον Δ.Ο.Α.Τ.Α.Π. ή για τα οποία υπάρχει ήδη κάποια προηγούμενη διοικητική απόφαση. Εναλλακτικά, η αίτηση θα πρέπει να εξεταστεί από δύο ανεξάρτητους ακαδημαϊκούς συμβούλους (που συνήθως είναι καθηγητές πανεπιστημίου του εσωτερικού) και στη συνέχεια η απόφαση να εγκριθεί από ένα διοικητικό συμβούλιο και από τον πρόεδρο του Οργανισμού. Η διαδικασία της αναγνώρισης ισοτιμίας ξεκινάει με την υποβολή μιας αίτησης από τον ενδιαφερόμενο. Παράλληλα ο ενδιαφερόμενος πρέπει να καταθέσει το απολυτήριο λυκείου του, τους τίτλους σπουδών που διαθέτει από τα ελληνικά πανεπιστήμια, τον τίτλο προς αναγνώριση καθώς και ένα επίσημο πιστοποιητικό μαθημάτων από το πανεπιστήμιο που έκανε τις σπουδές του. Επίσης συχνά ζητείται και ο οδηγός σπουδών του προγράμματος που παρακολούθησε καθώς και η διπλωματική εργασία που κατέθεσε για την απόκτηση του τίτλου σπουδών. Τέλος, σε ορισμένες μόνο περιπτώσεις, από το πανεπιστήμιου του εξωτερικού ζητείται η χορήγηση μιας αίτησης, στην οποία βεβαιώνεται πως ο ενδιαφερόμενος πραγματοποίησε τις σπουδές του στην έδρα του πανεπιστημίου και όχι εξ’ αποστάσεως ή περνώντας μεγάλο μέρος αυτών σε κάποια άλλη πόλη από αυτήν όπου βρίσκεται το πανεπιστήμιο. Οι παραπάνω διαδικασίες είναι αρκετά χρονοβόρες και πολλές φορές με μεγάλο οικονομικό κόστος και με αρκετή γραφειοκρατική δουλειά (Doatap.gr, 2019).

2.8.2 Προβλήματα πιστοποίησης άτυπης μάθησης

Σύμφωνα με όσα έχουν αναπτυχθεί έως τώρα στις προηγούμενες ενότητες, οι βασικές προκλήσεις της πιστοποίησης προσόντων διακρίνονται σε τρείς. Καταρχάς, ποιος θα είναι ο βασικός στόχος της πιστοποίησης των προσόντων ενός ατόμου (επομένως και πότε χρειάζεται να υπάρχει πιστοποίηση), δεύτερον, πώς θα υιοθετηθούν κατάλληλοι μέθοδοι αποτίμησης των υφιστάμενων προσόντων. Το βασικό ερώτημα είναι το πως θα υιοθετηθούν μέθοδοι και τεχνικές που να ταιριάζουν στα διαφορετικά χαρακτηριστικά των ωφελούμενων, στις διαφοροποιημένες ανάγκες, στις διαφορετικές επιδιώξεις και στα διαφορετικά περιβάλλοντα πιστοποίησης, σεβόμενοι τις ιδιαιτερότητες των ενηλίκων και κατοχύρωση της αναγκαίας αξιοπιστίας και εγκυρότητας (Τητήρου, 2017). Και τρίτον, το πώς θα ικανοποιηθούν οι θεσμικές, κοινωνικές και πολιτικές απαιτήσεις ενός συστήματος πιστοποίησης προσόντων, δηλαδή πώς θα εξασφαλιστούν όροι αποτελεσματικής επικοινωνίας και διαλόγου μεταξύ των πολιτών, των κοινωνικών εταίρων και των αρμόδιων φορέων της πολιτείας. Αυτά τα στοιχεία είναι ύψιστης σημασίας και άκρως απαραίτητα για την εδραίωση ουσιαστικής κοινωνικής εμπιστοσύνης απέναντι στους θεσμούς που θα κληθούν να εξασφαλίσουν το εν λόγω σύστημα πιστοποίησης προσόντων. Αναφορικά με την πρώτη πρόκληση, το ερώτημα σχετικά με το σκοπό της πιστοποίησης προσόντων τίθεται ως εξής: αποτελεί βασικό στόχο της πιστοποίησης η εναρμόνιση των επαγγελματικών προσόντων με τα χαρακτηριστικά του επαγγέλματος (όπως αυτά περιγράφονται στο επαγγελματικό περίγραμμα), για τις περιπτώσεις όπου η αποτίμησή τους αποτελεί προϋπόθεση για την άσκηση του επαγγέλματος και η αναγνώρισή τους συνοδεύεται με σχετική διεύρυνση των εργασιακών δικαιωμάτων ή η πιστοποίηση στοχεύει κυρίως στην πληροφόρηση των επιχειρήσεων για τα προσόντα των εργαζομένων, στην προσαρμοστικότητά τους σε προσωρινές εργασιακές ανάγκες και μπορεί να εφαρμόζεται σε οποιοδήποτε σύνολο προτύπων εργασιακής απόδοσης, ανεξάρτητα από το εάν αυτά συνιστούν μία διακριτή επαγγελματική ειδικότητα. Επομένως, άμεσο ερώτημα που τίθεται είναι εάν θα αποτελεί στόχο της πιστοποίησης η αναγνώριση των αυξημένων επαγγελματικών προσόντων που προέρχονται από τη συνεχή επαγγελματική εμπειρία (Γεροθανάσης, 2017).

Αναφορικά με τη μεθοδολογική πρόκληση, ένα ιδιαίτερο τρέχον πρόβλημα, αλλά και σημαντικό θέμα για μελλοντική διερεύνηση, είναι η δυσκολία εξασφάλισης αποδεκτών κριτηρίων εγκυρότητας και αξιοπιστίας κατά την πιστοποίηση της άτυπης μάθησης. Επιπλέον το ποια θα

είναι η βάση (το σημείο αναφοράς) της πιστοποίησης. Τα εκπαιδευτικά περιεχόμενα, οι οριζόμενες από το επαγγελματικό περίγραμμα γνώσεις και δεξιότητες ή τα (οριζόμενα από τις επιχειρήσεις) πρότυπα εργασιακής απόδοσης. Το πώς θα υλοποιείται η διαδικασία της πιστοποίησης. Με κλασικές μορφές που χρησιμοποιεί το εκπαιδευτικό σύστημα (π.χ. εξετάσεις), με δοκιμασίες της μορφής της εργαστηριακής πρακτικής άσκησης ή με συνδυασμό ατομικού φακέλου (portfolio) και άλλων μορφών. Τέλος, αναφορικά στην τρίτη πρόκληση, δηλαδή τις πολιτικές και θεσμικές απαιτήσεις, κρίσιμο ζήτημα αποτελεί ο σχεδιασμός ενός ανοιχτού, ενιαίου και συνολικού (εθνικού) συστήματος, του οποίου βασικά στοιχεία θα είναι η οικονομική λειτουργία (το μηδενικό ή έστω πολύ χαμηλό κόστος για τους χρήστες), η ευελιξία, η εθελοντική συμμετοχή, η απλότητα και σαφήνεια των όρων και των διαδικασιών, ο συνυπολογισμός της άποψης των ενδιαφερόμενων και η εξασφάλιση συνθηκών ειλικρινούς και ουσιαστικού κοινωνικού διαλόγου, ο οποίος θα οδηγεί στη συναίνεση και συμφωνία μεταξύ εργαζομένων και εργοδοτών, ως βασική προϋπόθεση της δημιουργίας και εδραίωσης θεσμών και διαδικασιών πιστοποίησης προσόντων (Τητήρου, 2017).

Η εφαρμογή ενός τέτοιου συστήματος πιστοποίησης προσόντων μέσα από διαδικασίες αναγνώρισης των μαθησιακών αποτελεσμάτων αποτελεί μια εξαιρετικά χρονοβόρα και τεχνικά δυσεπίλυτη διαδικασία, η οποία εκτός από μια σειρά τεχνικών ζητημάτων απαιτεί διευρυμένη συναίνεση και εμπλοκή των ενδιαφερόμενων μερών. Σε περίπτωση που δεν είναι εφικτό να εκπληρωθούν αυτές οι προϋποθέσεις, ελλοχεύει ο κίνδυνος υποβάθμισης του ευρύτερου εγχειρήματος, με αποτέλεσμα την απαξίωση της γενικότερης διαδικασίας. Είναι σαφές πως όλα τα μαθησιακά αποτελέσματα είναι αναγκαίο να προσδιορίζονται μέσω κοινά αποδεκτών διαδικασιών, να οριοθετούνται και να επαναξιολογούνται σε τακτά διαστήματα – με σκοπό να προσδιοριστεί όχι μόνο αν επιτυγχάνονται κατά τη διάρκεια του μαθήματος, αλλά επίσης αν συνεχίζουν να αντικατοπτρίζουν με έγκυρο τρόπο τις λειτουργίες που απαιτείται να υπηρετούν. Η διαμόρφωση μιας θεσμικής διαδικασίας αποτελεί ένα ιδιαίτερα κρίσιμο ζήτημα, και προϋποθέτει μια βήμα προς βήμα προσέγγιση καθώς και μια προσεκτική εφαρμογή των μαθησιακών αποτελεσμάτων, προκειμένου να υπερπηδηθούν όλα τα προαναφερθέντα προβλήματα, καθώς και άλλα παρόμοια που αφορούν στην εφαρμογή των μαθησιακών αποτελεσμάτων (Galanis, Mayol, Alier & García-Peñalvo, 2016).

Κεφάλαιο 3: Η τεχνολογία Blockchain

3.1 Ανάγκη για νέες μεθόδους - εισαγωγή για την τεχνολογία blockchain

Πριν από την εφεύρεση των Blockchain (τεχνολογία κατανεμημένης εγγραφής), δεν υπήρχε κανένας τρόπος για τη διαχείριση μεμονωμένων δραστηριοτήτων μέσω του Διαδικτύου χωρίς κεντρικό έλεγχο για να εξασφαλιστεί η μη αποποίηση ευθυνών για τα δεδομένα. Δεν υπήρχε καμία εμπιστοσύνη μεταξύ των μερών ότι καθένας θα μπορούσε να αλλάξει τα δεδομένα για το δικό του κέρδος χωρίς κάποια συμφωνία με το δεύτερο μέρος. Μια ομάδα από κατανεμημένα άτομα δεν μπορούσε να ελέγχει τις συναλλαγές χωρίς να βασίζεται σε κάποια κεντρική εξουσία. Το πρόβλημα αυτό ήταν κυρίως γνωστό ως «πρόβλημα βυζαντινών στρατηγών». Ο άμεσος προβληματισμός ήταν στο πώς οι κατανεμημένοι υπολογιστές θα μπορούσαν να πάρουν μια απόφαση χωρίς να βασίζονται σε μια κεντρική αρχή, ώστε το δίκτυο των ηλεκτρονικών υπολογιστών να μπορεί να αμυνθεί από μια επίθεση από κακόβουλους παράγοντες (Gramoli, 2017). Η στρατηγική κάθε τμήματος θα έπρεπε να είναι ανεξάρτητη έτσι ώστε να μπορέσουν να αντιμετωπίσουν οποιοδήποτε πρόβλημα, αλλά έχοντας ωστόσο μια κοινή πορεία δράσης. Τα Blockchain χρησιμοποιούν μια πιθανή προσέγγιση για την επεξεργασία μιας λύσης για το «πρόβλημα των βυζαντινών στρατηγών». Τα δεδομένα κινούνται μέσω ενός δικτύου υπολογιστών που αυξάνει τη διαφάνεια και την αξιοπιστία. Ως αποτέλεσμα, η δυνατότητα των δυνητικών εισβολέων να καταστρέψουν μια κατανεμημένη βάση δεδομένων με ψεύτικα δεδομένα, μειώνεται σημαντικά. Η μόνη περίπτωση επίθεσης είναι όταν ο επιτιθέμενος μπορεί να χρησιμοποιήσει πολύ περισσότερη υπολογιστική ισχύ από ότι ολόκληρο το δίκτυο. Τα πρωτόκολλα του Blockchain μπορούν να διασφαλίσουν ότι οι συναλλαγές είναι σωστές και όχι διπλές (Sousa, Bessani & Vukolic, 2018).

3.2 Ιστορική αναδρομή των blockchain (bitcoin)

Για να γίνει κατανοητή η έννοια των Blockchain, πρέπει να συζητηθούν παρόμοιες θεωρητικές και πρακτικές προσεγγίσεις. Η τεχνολογία έγινε ευρέως γνωστή το 2008 με την εφεύρεση του Bitcoin. Ωστόσο, οι χρησιμοποιούμενες ιδέες έχουν τις ρίζες τους στη δεκαετία του 1980 και του

1990 στον 20ο αιώνα. Σύμφωνα με μελέτες, αναπτύχθηκε και διαμορφώθηκε η πρώτη έννοια του ψηφιακού νομίσματος βασιζόμενη στην κεντρική αρχιτεκτονική εξυπηρετητών, η λειτουργία της οποίας ήταν να αποφευχθούν οι διπλές δαπάνες. Ωστόσο, αυτή η έννοια εξακολουθούσε να μην έχει μια ενότητα διπλής εξόφλησης δαπανών, ανωνυμίας και συγκέντρωσης. Υπήρχαν μερικές ακόμα έννοιες στη δεκαετία του '90. Το 1991, διεξήχθη μια έρευνα σχετικά με τα κρυπτογραφικά τεμάχια μιας ασφαλισμένης αλυσίδας. Αργότερα το 1996 και το 1997, συνεχίστηκαν οι έρευνες και οι δημοσιεύσεις από θεωρητικούς. Την ίδια στιγμή στα τέλη της δεκαετίας του 1990, επιστήμονες υπολογιστών ανέπτυξαν ένα μηχανισμό για ένα αποκεντρωμένο ψηφιακό νόμισμα, το οποίο ονομάστηκε ως «bitgold». Αργότερα, μετά από πάνω από 10 χρόνια, εισήχθη η κρυπτογράφηση Bitcoin (Crosby, Pattanayak, Verma & Kalyanaraman, 2016).

Το κεντρικό σύστημα αντικαταστάθηκε από έναν μηχανισμό συναίνεσης, ο οποίος βασίζεται στην απόδειξη της εργασίας. Η αρχική τεχνολογία των bitcoin του blockchain με βάση ένα αποκεντρωμένο σύστημα είχε αναπτύξει μια ιδέα που είχε προηγηθεί, με ένα νέο όραμα. Σήμερα, η έννοια του blockchain είναι ευρέως διαδεδομένη, ενώ υπάρχουν αντίθετες απόψεις σχετικά με την τεχνολογία και ακόμη και την ιστορία του. Τα ουσιαστικά "μπλοκ" και "αλυσίδες" χρησιμοποιήθηκαν χωριστά και, αρχικά, η τεχνολογία ονομάστηκε αλυσίδα μπλοκ. Ωστόσο, μέχρι το 2016 η έννοια είχε συγχωνευθεί σε μία λέξη «Blockchain». Υπήρξαν πέντε σημαντικές εφευρέσεις με βάση τα Blockchain τα τελευταία δέκα χρόνια (Gramoli, 2017).

Η πρώτη σημαντική καινοτομία βασιζόμενη στο Blockchain ήταν το Bitcoin, το οποίο είναι ένα ψηφιακό νόμισμα. Η χρηματιστηριακή του κεφαλαιοποίηση υπολογίζεται μεταξύ $10 - $20 δισεκατομμύρια δολάρια. Επιπλέον, το Bitcoin χρησιμοποιείται από εκατομμύρια ανθρώπους για online και ασφαλείς πληρωμές, συμπεριλαμβανομένου του τραπεζικού τομέα.

Η δεύτερη εφεύρεση ήταν το ίδιο το Blockchain, το οποίο παρόλο που είναι κρυμμένη τεχνολογία, επέτρεψε στο Bitcoin να διαχωριστεί από το νόμισμα και να χρησιμοποιηθεί για όλους τους τύπους συνεργασίας. Τα περισσότερα μεγάλα χρηματοπιστωτικά ιδρύματα πραγματοποιούν έρευνα σχετικά με το Blockchain αυτή τη στιγμή. Οι προβλέψεις δείχνουν ότι το 15% των παγκόσμιων τραπεζών πρόκειται να χρησιμοποιούν το Blockchain το 2020.

Η τρίτη καινοτομία ονομάστηκε «έξυπνη σύμβαση». Στη δεύτερη γενιά ονομάζεται Ethereum. Η πλατφόρμα Ethereum αναπτύσσει μικρά προγράμματα απευθείας στο Blockchain (Ateniese, Magri, Venturi & Andrade, 2017). Αυτό επέτρεψε την παρουσίαση χρηματοπιστωτικών εργαλείων, όπως δανείων ή ομολόγων, αντί των νομισμάτων του bitcoin. Με την κεφαλαιοποίηση

της Ethereum το 2017 περίπου ένα δισεκατομμύριο αμερικάνικα δολάρια, και πολλά έργα κινούνται προς την αγορά.

Η τέταρτη μεγάλη καινοτομία, η πιο καινοτόμος από τη σκέψη Blockchain, είναι η «απόδειξη συμμετοχής». Η πραγματική γενιά Blockchains εξασφαλίζεται με «απόδειξη εργασίας», όπου οι αποφάσεις λαμβάνονται από μια ομάδα με το μεγαλύτερο ποσό υπολογιστικής ισχύος. Αυτές οι ομάδες είναι γνωστές ως «ανθρακωρύχοι» και ελέγχουν τεράστια κέντρα δεδομένων για να εξασφαλίσουν την ασφάλεια, έχοντας πληρωμές κρυπτογράφησης. Η απόδειξη των συστημάτων μεριδίων εξαλείφει αυτά τα κέντρα δεδομένων και τα αντικαθιστά με σύνθετα χρηματοοικονομικά εργαλεία, με παρόμοιο ή υψηλότερο επίπεδο ασφάλειας.

Τέλος, η πέμπτη σημαντική καινοτομία είναι μια κλιμάκωση του Blockchain (Kiviat, 2015). Επί του παρόντος, στο Blockchain, κάθε μέλος του δικτύου επεξεργάζεται κάθε συναλλαγή που είναι πολύ αργή. Με τη χρήση του κλιμακωτού Blockchain, υπάρχει η δυνατότητα να επιταχυνθεί η διαδικασία χωρίς απειλές για την ασφάλεια. Η ιδέα είναι να γνωρίζει κάποιος τον αριθμό των υπολογιστών που απαιτούνται για την επικύρωση κάθε συναλλαγής και τη βελτιστοποίηση της διαδικασίας εργασίας με τη χρήση αυτών των στατιστικών στοιχείων.

Όλες αυτές οι καινοτομίες εφευρέθηκαν τα τελευταία 10 χρόνια, αλλά το πλήρες δυναμικό της τεχνολογίας εξακολουθεί να είναι κρυφό και δεν μπορεί να εκτιμηθεί ακόμα. Αυτό σημαίνει ότι τα επόμενα χρόνια, η ανάπτυξη της τεχνολογίας θα συνεχιστεί και μερικές από τις λύσεις που βασίζονται στα Blockchain θα μπορούσαν ήδη να αποτελέσουν σημαντικό μέρος της ζωής των ανθρώπων, όπως το Facebook έγινε ένα ζωτικό μέρος ενός δισεκατομμυρίου ανθρώπων μόλις σε 13 χρόνια (Crosby, Pattanayak, Verma & Kalyanaraman, 2016).

3.3 Αρχές και δομή λειτουργίας blockchain (hash)

Το Blockchain είναι ένας κοινόχρηστος κατανεμημένος λογαριασμός που καταγράφει τις συναλλαγές εντός ενός δικτύου. Η τεχνολογία blockchain είναι χτισμένη σε δομές που διανέμονται σε διάφορους κόμβους (συμμετέχοντες) μέσα στο δίκτυο, οι οποίες αλληλοεπιδρούν με peer-to-peer (P2P – είναι αρχιτεκτονική κατανεμημένων εφαρμογών με χωρισμένες εργασίες μεταξύ ομότιμων υπολογιστών). Η αναπαραγωγή peer-to-peer μπορεί να εξηγηθεί καθώς κάθε κόμβος ενεργεί τόσο ως εκδότης όσο και ως συνδρομητής στις συναλλαγές που γίνονται στο δίκτυο. Λαμβάνουν και στέλνουν συναλλαγές σε άλλους, όπου οι πληροφορίες συγχρονίζονται με

όλους τους κόμβους του συγκεκριμένου δικτύου. Αυτή η μέθοδος εξαλείφει την ανάγκη για ένα αξιόπιστο τρίτο μέρος για τις συναλλαγές, π.χ. ένα χρηματοπιστωτικό ίδρυμα (Gupta, S2017). Αντί αυτού, το τεράστιο κατανεμημένο δίκτυο όπου η εγκυρότητα μιας συναλλαγής συμφωνείται από όλους τους κόμβους παρέχει αμετάβλητες εγγραφές. Το Blockchain χρησιμοποιεί ένα μοντέλο που βασίζεται στη συναίνεση για να εξασφαλίσει την εγκυρότητα, πράγμα που σημαίνει ότι όλοι οι κόμβοι πρέπει να συμφωνήσουν στη συναλλαγή. Δεδομένου ότι τα δεδομένα εντός του δικτύου διανέμονται σε όλους τους κόμβους και ότι η αναπαραγωγή από ομότιμους χρήστες αποτρέπει την αλλοίωση δεδομένων, το κατανεμημένο δίκτυο δεν απαιτεί το κεντρικό όργανο διοίκησης να είναι το έμπιστο σημείο αφού οι ανεξάρτητοι κόμβοι δημιουργούν συναίνεση (Lemieux, 2016).

Όπως περιγράφεται και σε περαιτέρω αναλύσεις, η μπλοκ αλυσίδα αποτελείται από μπλοκ που περιέχουν μια σειρά από συναλλαγές, οι οποίες στη συνέχεια συνδέονται μέσω κρυπτογράφησης, σχηματίζοντας το blockchain. Οι μπλοκ αλυσίδες αποτελούνται από τρία κύρια μέρη: μπλοκ, αλυσίδα και δίκτυο. Το μπλοκ είναι εκεί όπου όλες οι συναλλαγές καταγράφονται σε ένα ημερολόγιο κατά τη διάρκεια μιας δεδομένης περιόδου. Ανάλογα με τον στόχο του blockchain, προσδιορίζεται το μέγεθος, η περίοδος και τα γεγονότα ενεργοποίησης για κάθε μπλοκ, δηλ. δεν είναι το ίδιο για όλα τα blockchains. Τα μπλοκ αναπαράγονται σε ολόκληρο το δίκτυο για να δημιουργήσουν την εγκυρότητα και τη συναίνεση όπως προβλέπεται. Οι αλυσίδες είναι μπλοκ που συνδέονται μεταξύ τους, δημιουργώντας το blockchain (Swan, 2015). Η «κόλλα» που συνδέει τα μπλοκ μεταξύ τους είναι οι κρυπτογραφικές λειτουργίες κατακερματισμού, οι οποίες μπορούν να εξηγηθούν ως τα δακτυλικά αποτυπώματα των δεδομένων από το προηγούμενο μπλοκ που ενώνεται με το ίδιο, το οποίο αναφέρεται ως γονικό μπλοκ. Αυτή η διαδικασία αναφέρεται ως θεωρία παιγνίων αφού οι πλήρεις κόμβοι ανταγωνίζονται μεταξύ τους για να βρουν τη σωστή λειτουργία κατακερματισμού και να συλλέξουν την ανταμοιβή, η οποία συνήθως είναι ένα διακριτικό ενός κρυπτογράφου. Επιπλέον, δηλώνεται ότι όταν εντοπιστεί η σωστή συνάρτηση κατακερματισμού, τότε το μπλοκ κλειδώνει στο προηγούμενο μπλοκ κατά χρονολογική σειρά και είναι χρόνο-σφραγισμένο από το hash που δημιουργήθηκε. Το δίκτυο διατηρείται από όλους τους κόμβους του δικτύου (Ateniese, Magri, Venturi & Andrade, 2017). Οι κόμβοι που κατέχουν τους καταλόγους αναφέρονται και ως πλήρεις κόμβοι. Κάθε ένας από αυτούς τους κόμβους κρατά ένα πλήρες αρχείο όλων των συναλλαγών που γίνονται μέσα στο blockchain που δημιουργεί την συναίνεση στο οποίο βασίζεται το δίκτυο. Οι πλήρεις κόμβοι ασφαλίζουν το δίκτυο από τη στιγμή

που παράγουν τους κρυπτογραφικούς κώδικες που ενώνουν τα μπλοκ μεταξύ τους και κρατούν το ημερολόγιο που δημιουργεί την αναπαραγωγή ομότιμης αλληλεπίδρασης εντός του δικτύου. Μέσα στον κόσμο του κρυπτό-αναλογισμού, οι πλήρεις κόμβοι αναφέρονται ως «ανθρακωρύχοι». Αυτοί οι κόμβοι είναι αποκεντρωμένοι και λειτουργούν σε όλο τον κόσμο (Sousa, Bessani & Vukolic, 2018). Οποιοσδήποτε μπορεί να χειριστεί έναν πλήρη κόμβο, ανταμείβεται γι' αυτό λόγω της δυσκολίας και της δαπανηρότητας της λειτουργίας του. Η ανταμοιβή εξαρτάται από το δίκτυο, αλλά είναι συνήθως σε μορφές κρυπτό-συχνοτήτων ή συμβολικού σήματος. Αυτό το βιβλίο κατανεμημένο σε όλους τους πλήρεις κόμβους του δικτύου αντιγράφεται σε σχέση με τους άλλους πλήρεις κόμβους που δημιουργούν τη συναίνεση. Ένα μπλοκ εντός του blockchain αποτελείται από όλες τις συναλλαγές που γίνονται στο δίκτυο κατά τη διάρκεια της δεδομένης περιόδου, πριν από την αλυσίδα του μπλοκ και την δημιουργία ενός νέου μπλοκ. Κάθε συναλλαγή περιέχει τις πληροφορίες σχετικά με τον αποστολέα, τον αποδέκτη και από τί συνίσταται η συναλλαγή (Lemieux, 2016). Αυτά τα δεδομένα συναλλαγής είναι κρυπτογραφημένα, εμποδίζοντας το δίκτυο να αποκρυπτογραφήσει τις πληροφορίες παρόλο που είναι ορατό. Αυτό παρέχει μια ανωνυμία για τους κόμβους καθώς ταυτόχρονα καθιστά τη συναλλαγή επαληθεύσιμη. Η τεχνολογία blockchain βασίζεται στη συναίνεση, γεγονός που καθιστά δυνατή τη συμφωνία μεταξύ των μετόχων που είναι συνήθως δύσπιστοι. Ένας μοναδικός κόμβος δεν χρειάζεται να εμπιστεύεται έναν άλλο κόμβο, αλλά μάλλον το δίκτυο ως σύνολο, δημιουργώντας συναίνεση. Με άλλα λόγια, πρόκειται για ένα αυτό-διορθωτικό και τίμιο σύστημα που δεν απαιτεί την επιβολή των κανόνων από έναν αξιόπιστο τρίτο φορέα (Kiviat, 2015).

3.3.1 Hash

Το hash αποτελεί έναν σύντομο κώδικα καθορισμένου μήκους που χρησιμεύει ως δακτυλικό αποτύπωμα για ένα ψηφιακό έγγραφο. Ένα πρόγραμμα που ονομάζεται hash-generator επιτρέπει σε έναν χρήστη να φορτώσει οποιαδήποτε σειρά κειμένου και να δημιουργήσει ένα μοναδικό αναγνωριστικό. Κάθε φορά που εκτελείται η ίδια σειρά κειμένου μέσω του hash-generator, θα δοθεί το ίδιο αναγνωριστικό εγγράφου. Η συμβολή του κατακερματισμού ως συσκευή κατά της παρεμπόδισης είναι σημαντική: αν αλλάξει ένα γράμμα σε ένα έγγραφο, θα δημιουργηθεί αυτόματα ένα εντελώς διαφορετικό αναγνωριστικό. Τα hash είναι μονόδρομοι (Gupta, S2017). Αυτό σημαίνει ότι η γεννήτρια κατακερματισμού μπορεί να χρησιμοποιηθεί για να δημιουργήσει ένα hash από το έγγραφο, αλλά είναι μαθηματικά αδύνατο να δημιουργηθεί ένα έγγραφο από ένα

hash. Σε ένα blockchain, κάθε μπλοκ συναλλαγών είναι εξασφαλισμένο με τη συμπερίληψη ενός hash του μπλοκ πληροφοριών, καθώς και του προηγούμενου μπλοκ, επιτρέποντας έτσι σε όλα τα μέρη να εγγυηθούν ότι καμία από τις συναλλαγές δεν έχει τροποποιηθεί ή αλλοιωθεί (Lemieux, 2016).

3.3.2 Δημόσια και ιδιωτικά κλειδιά

Ένα δημόσιο κλειδί είναι ένας πραγματικά διαθέσιμος στο κοινό αναγνωριστικός αριθμός που μπορεί να χρησιμοποιηθεί για την αναγνώριση ενός ατόμου. Ένα ιδιωτικό κλειδί είναι ένας κωδικός πρόσβασης που έχει συνδεθεί μαθηματικά με το δημόσιο κλειδί. Όταν χρησιμοποιούνται ζεύγη δημόσιου / ιδιωτικού κλειδιού, ο χρήστης μπορεί να πιστοποιήσει ότι είναι πραγματικά ο «κάτοχος» ενός δημόσιου κλειδιού εισάγοντας τα στοιχεία του ιδιωτικού κλειδιού του στο λογισμικό. Αυτό με τη σειρά του θα ελέγξει εάν τα δύο κλειδιά είναι πραγματικά μαθηματικά συνδεδεμένα. Αυτή η λειτουργία δεν μπορεί πρακτικά να λειτουργήσει αντίστροφα, δηλαδή είναι σχεδόν αδύνατο να δημιουργηθεί το ιδιωτικό κλειδί εάν κάποιος έχει μόνο πληροφορίες για το δημόσιο κλειδί (Swan, 2015).

3.3.3 Κρυπτογραφία

Η κρυπτογραφία, ή αλλιώς η «επιστήμη των μυστικών», από την ελληνική κρυπτός (λόγος και επιστήμη), περιλαμβάνει παραδοσιακά δύο πολύ συγγενείς περιοχές: την κρυπτογραφία και την κρυπτοανάλυση. Η κρυπτογραφία ασχολείται με την κρυπτογράφηση των μηνυμάτων, δηλ. μετασχηματίζοντας τα μηνύματα σε κρυπτογραφικά κείμενα υπό τη χρήση ενός κλειδιού με τέτοιο τρόπο ώστε το απλό κείμενο να μπορεί να ανακτηθεί από το κρυπτό-σύστημα μόνο με τη γνώση του κλειδιού. Η κρυπτοανάλυση είναι το αντίστοιχο της κρυπτογραφίας και ασχολείται με την ανάκτηση απλών κειμένων από δεδομένα κρυπτό-κείμενα χωρίς τη γνώση του κλειδιού. Όταν οι προηγούμενοι σύγχρονοι υπολογιστές αναπτύχθηκαν κατά το πρώτο μισό του 20^{ου} αιώνα, η κρυπτογραφία και η κρυπτογράφηση ήταν από τις πρώτες εφαρμογές των αυτοματοποιημένων υπολογιστών (Gupta, 2017). Παραδείγματα πρώιμων ειδικών υπολογιστών για κρυπτογραφία είναι οι μηχανές κρυπτογράφησης Enigma που εφευρέθηκαν από τον Scherbius και κατοχυρώθηκαν με δίπλωμα ευρεσιτεχνίας το 1928 (Sch28). Το πιο διάσημο μοντέλο του Enigma, το αίνιγμα Wehrmacht, χρησιμοποιήθηκε από τα γερμανικά στρατεύματα κατά τη διάρκεια του Β’ Παγκοσμίου Πολέμου. Ένα παράδειγμα για πρώιμους εξειδικευμένους υπολογιστές για

κρυπτοαναλύσεις είναι οι αποκαλούμενες Bombes, που χρησιμοποιήθηκαν στην κύρια μονάδα αποκρυπτογράφησης του Ηνωμένου Βασιλείου στο Bletchley Park για να σπάσουν τα κρυπτογραφημένα πεδία που δημιουργούνται από το Wehrmacht Engima. Επίσης, η πρώτη ηλεκτρονική μηχανή ψηφιακής επεξεργασίας πληροφοριών, Colossus, κατασκευάστηκε για κρυπτοανάλυση και χρησιμοποιήθηκε στο πάρκο Bletchley από το 1943 (Gramoli, 2017).

3.4 Αρχιτεκτονική ενός Blockchain

Ως εφαρμογή λογισμικού προσανατολισμένη σε δίκτυο, ένα blockchain μετατοπίζει τον κίνδυνο και την ευθύνη εκτέλεσης κώδικα και αποθήκευσης δεδομένων από κεντρικά μηχανήματα σε αποκεντρωμένα δίκτυα. Το blockchain χρησιμοποιείται για να καταχωρήσει συναλλαγές ψηφιακών στοιχείων. Το πιο βασικό στοιχείο στις ενσωματωμένες συναλλαγές στη λειτουργία των περισσότερων πρωτοκόλλων blockchain είναι η κρυπτογράφηση με τη μορφή συμβόλων (όπως Bitcoin, Ether, Litecoin κ.λπ.). Μπορούν, επίσης, να χρησιμοποιηθούν για την ανταλλαγή άλλων στοιχείων, όπως τίτλοι γης ή έγγραφα ταυτότητας. Κάθε δίκτυο blockchain έχει διαφορετικούς κανόνες ανάλογα με το είδος των στοιχείων που συναλλάσσονται και με τους όρους που διεξάγεται η συναλλαγή. Οι κανόνες αυτοί κωδικοποιούνται στο λογισμικό του. Κάθε συσκευή που εκτελεί το λογισμικό blockchain είναι γνωστή ως κόμβος και συνδέεται με το δίκτυο κόμβων που εκτελούν το συγκεκριμένο λογισμικό (Grätheretal., 2018). Όταν κάποιος μπορεί να δημιουργήσει έναν κόμβο και να πραγματοποιήσει απευθείας συναλλαγή με οποιονδήποτε άλλο κόμβο στο δίκτυο, αυτό είναι γνωστό ως δημόσιο δίκτυο blockchain. Ωστόσο, εάν η συσκευή είναι συνδεδεμένη σε ένα δίκτυο (intranet), δηλαδή ένα ιδιωτικό δίκτυο στο οποίο έχουν πρόσβαση μόνο συγκεκριμένες συσκευές, τότε μπορούν να πραγματοποιηθούν συναλλαγές μεταξύ μιας επιλεγμένης ομάδας ατόμων στα οποία έχει δοθεί πρόσβαση στο εν λόγω δίκτυο. Αυτό είναι γνωστό ως ιδιωτικό δίκτυο blockchain. Η αρχιτεκτονική του λογισμικού blockchain εξασφαλίζει ότι μόνο ταυτόσημα αντίγραφα του blockchain λογισμικού μπορούν να αλληλεπιδρούν μεταξύ τους. Επομένως, εάν κάποιος αλλάξει ένα αντίγραφο του λογισμικού, δημιουργούν ένα εντελώς νέο blockchain. Αυτό είναι γνωστό ως "διακλάδωση" (fork). Από την εισαγωγή του πρωτοκόλλου Bitcoin το 2009 υπήρξαν πολλαπλά forks του λογισμικού blockchain. Τον Αύγουστο του 2017 δημιουργήθηκε ένα fork του blockchain Bitcoin σε ένα νέο blockchain που ονομάστηκε Bitcoin Cash. Η ταυτότητα πρωτοκόλλου διασφαλίζει ότι όλες οι συσκευές στο δίκτυο συναλλάσσονται

υπό ακριβώς ίδιες συνθήκες χωρίς να χρειάζεται μια κεντρική αρχή να επαληθεύσει ότι τηρούνται οι κανόνες (Zhengetal., 2017).

3.4.1 Αποκεντρωμένος, Κατανεμημένος Λογαριασμός

Στον πυρήνα του, ένα blockchain είναι ένας διαφανής και αυτόνομος αποκεντρωμένος λογαριασμός. Κάθε αντίγραφο λογισμικού blockchain αποθηκεύει ένα πλήρες αντίγραφο του λογαριασμού, γράφει νέες καταχωρήσεις στο λογαριασμό όταν λαμβάνει συναίνεση από το υπόλοιπο δίκτυο, μεταδίδει τις συναλλαγές που πραγματοποιεί ο χρήστης με το υπόλοιπο δίκτυο, για επαλήθευση με συναίνεση και καταχώρηση και ελέγχει τακτικά ότι το αντίγραφο του λογαριασμού είναι πανομοιότυπο με το καθένα του υπόλοιπου δικτύου (Kolvenbach, Ruland, Gräther & Prinz, 2018).

3.4.2 Σύστημα για την ανώνυμη επαλήθευση ταυτότητας και ιδιοκτησίας

Οι συναλλαγές παρατίθενται σε blockchain με τον ακόλουθο τρόπο. Το λογισμικό blockchain μπορεί να εκδώσει ένα άτομο με μια διεύθυνση bitcoin η οποία συνδέεται με το μοναδικό δημόσιο κλειδί και το κρυπτογραφικά συνδεδεμένο ιδιωτικό κλειδί. Για να γραφτεί μια νέα συναλλαγή σε ένα blockchain - δηλαδή, για να μεταφερθεί ένα στοιχείο που σχετίζεται με μια διεύθυνση bitcoin - ο χρήστης πρέπει να εισάγει το μυστικό ιδιωτικό κλειδί που σχετίζεται με τη συγκεκριμένη διεύθυνση δημόσιου κλειδιού/bitcoin που δόθηκε σε αυτόν κατά τη δημιουργία του. Η ιδιοκτησία στοιχείων που έχουν μεταφερθεί σε μια συγκεκριμένη διεύθυνση bitcoin/δημόσιο κλειδί επαληθεύεται με το ιδιωτικό κλειδί (Zhengetal, 2017). Έτσι, τόσο τα μέρη που συμμετέχουν σε μια συναλλαγή, όσο και το κοινό, μπορούν να δουν ότι έχει πραγματοποιηθεί μια συναλλαγή και μπορούν να προσδιορίσουν τον κάτοχο, χωρίς να είναι γνωστή η ταυτότητα των μερών στη συναλλαγή. Καθένα από αυτά τα μέρη στη συναλλαγή μπορεί στη συνέχεια να χρησιμοποιήσει τα στοιχεία εισάγοντας απλά το ιδιωτικό του κλειδί στο λογισμικό bitcoin, χωρίς να χρειάζεται να αποδείξει ή να εκθέσει την ταυτότητά του σε τρίτο ή μεσάζοντα (Crosby, Pattanayak, Verma & Kalyanaraman, 2016).

3.4.3 Σύστημα για τη διασφάλιση μόνιμων άφθαρτων μητρώων

Ο λογαριασμός σε ένα Bitcoin blockchain είναι "μόνο προσαρτημένος" (append-only), πράγμα που σημαίνει ότι οι συναλλαγές μπορούν να προστεθούν αλλά δεν μπορούν να υποστούν επεξεργασία ή να διαγραφούν. Έτσι, κάθε νέα συναλλαγή προστίθεται σε ένα μπλοκ, ενώ κάθε μπλοκ είναι συνδεδεμένο με ένα προηγούμενο μπλοκ που σχηματίζει αλυσίδα. Όλες οι συναλλαγές εντός ενός μπλοκ είναι συμπιεσμένες και καρφιτσωμένες στο μπλοκ με τη χρήση μιας ειδικής λειτουργίας κατακερματισμού που ονομάζεται ρίζα Merkle (Merkle root). Ο κατακερματισμός αυτό (hash) περιλαμβάνεται στην κεφαλίδα του μπλοκ (Shrier, Wu & Pentland, 2016). Η κεφαλίδα κάθε μπλοκ περιλαμβάνει επίσης το hash όλων των πληροφοριών από το προηγούμενο μπλοκ. Αν κάποιος επιχειρήσει να επεξεργαστεί μία από τις συναλλαγές στην αλυσίδα, θα ακυρώσει άμεσα το hash κάθε επόμενου μπλοκ. Έτσι, το χακάρισμα της αλυσίδας θα απαιτούσε όχι μόνο την αλλαγή της συναλλαγής αλλά και τον επανυπολογισμό και να την αλλαγή των πληροφοριών της κεφαλίδας του κάθε μπλοκ που έχει δημιουργηθεί από τη συγκεκριμένη συναλλαγή και αυτό να γίνε σε πάνω από τους μισούς υπολογιστές του δικτύου - μια εξαιρετικά μη πρακτική πρόταση. Για μεγαλύτερα blockchain καθίσταται αποτελεσματικά αδύνατη η αλλαγή οποιωνδήποτε συναλλαγών, διότι: α) θα απαιτούσε σημαντικά μεγάλα ποσοστά υπολογιστικής ισχύος για να επιτευχθεί, και β) καθώς ο αριθμός των μπλοκ στην αλυσίδα αυξάνεται συνεχώς, θα αυξανόταν επίσης και η ποσότητα υπολογιστικής ισχύος που απαιτείται για να γίνει μια τέτοια αλλαγή. Μια σημαντική παρατήρηση: η πρόοδος στην υπολογιστική ισχύ δεν θα υπονομεύσει ξαφνικά ούτε θα καταστήσει αδύνατη την ασφάλεια του blockchain (Grätheretal., 2018).

3.4.4 Έκδοση πιστοποιητικού με τη χρήση ψηφιακών υπογραφών

Μια ψηφιακή υπογραφή είναι διαφορετική από μια ηλεκτρονική υπογραφή, η οποία είναι απλώς μια παραδοσιακή υπογραφή που σχεδιάζεται σε ένα ηλεκτρονικό έγγραφο (για παράδειγμα με ηλεκτρονικό στυλό) ή μια σαρωμένη φυσική υπογραφή. Οι ηλεκτρονικές υπογραφές μπορούν εύκολα να αντιγραφούν ή να πλαστογραφηθούν χωρίς να διαθέτουν μηχανισμό επαλήθευσης ή τυποποίησης. Από την άλλη πλευρά, οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για να επαληθεύσουν ότι ένα συγκεκριμένο έγγραφο υπογράφηκε πράγματι από ένα συγκεκριμένο πρόσωπο (Sudia & Siritzky, 2011).

Μια ψηφιακή υπογραφή παρέχει έναν τρόπο έκδοσης πιστοποιητικών, επιτρέποντας σε ένα άτομο να σημειώσει ένα έγγραφο με σφραγίδα, που μπορεί να το δημιουργήσει μόνο αυτό το ίδιο και να διασφαλίσει ότι το έγγραφο δεν μπορεί να αλλοιωθεί, αφού υπογραφεί. Για να λειτουργούν οι ψηφιακές υπογραφές απαιτείται κάθε πρόσωπο να υπογράφει ένα έγγραφο που φέρει έναν αριθμό ταυτότητας (δημόσιο κλειδί) και έναν συνδεδεμένο κωδικό πρόσβασης (ιδιωτικό κλειδί).

Μια ψηφιακή υπογραφή αποτελείται από τέσσερα στοιχεία: α) SHA-256 hash, ο οποίος είναι ένας τύπος λειτουργίας κατακερματισμού. β) δημόσιο κλειδί, γ) ένα ιδιωτικό κλειδί. δ) η χρονική σφραγίδα που παραθέτει την ακριβή ώρα έκδοσης του πιστοποιητικού.

Το έγγραφο υπογράφεται με τον συνδυασμό του hash του εγγράφου με το ιδιωτικό κλειδί του ατόμου για να δημιουργηθεί ένας νέος μοναδικός κώδικας (Ting, Yuen, Lee & Leong, 2002). Η υπογραφή που προκύπτει στη συνέχεια "σφραγίζεται" ή ενώνεται στο έγγραφο μαζί με τη χρονική σήμανση. Δεδομένου ότι η υπογραφή είναι ένας συνδυασμός αυτών των δύο συνιστωσών, αυτό είναι μοναδικό στο συγκεκριμένο έγγραφο, αφού δημιουργήθηκε από το hash του εγγράφου, και έχει δημιουργηθεί μόνο από το άτομο που κατέχει το ιδιωτικό κλειδί. Πρέπει να σημειωθεί ότι, εφόσον η υπογραφή σφραγίζεται στο ψηφιακό έγγραφο και το υπογεγραμμένο ψηφιακό έγγραφο έχει διαφορετική τιμή κατακερματισμού σε σχέση με το ψηφιακό έγγραφο που δεν έχει υπογραφεί, ακόμα και αν αλλάξει μόνο ένα γράμμα του εγγράφου μετά την υπογραφή, θα έχει ξανά μια εντελώς διαφορετική τιμή κατακερματισμού. Επιπλέον, η υπογραφή δεν μπορεί να κατασκευαστεί αντίστροφα για να ανακαλύψει το ιδιωτικό κλειδί του ατόμου (Brown & Brown, 2017).

Εάν κάποιος τρίτος επιθυμεί να επαληθεύσει μια ψηφιακή υπογραφή, πρέπει να γνωρίζει το δημόσιο κλειδί του ατόμου που υπέγραψε το έγγραφο. Δεδομένου ότι τα δημόσια κλειδιά είναι στην πραγματικότητα μόνο κωδικοί ταυτότητας, μπορούν συνήθως να αναζητηθούν σε δημόσιους καταλόγους, παρόμοιους με τους τηλεφωνικούς καταλόγους. Το λογισμικό επαλήθευσης λειτουργεί με την εισαγωγή του εγγράφου και του δημόσιου κλειδιού και ελέγχει δύο πράγματα. Αφενός, το ότι η υπογραφή στο έγγραφο ταιριάζει με το hash του πρωτότυπου εγγράφου. Αφετέρου, ότι η υπογραφή του εγγράφου σχετίζεται μαθηματικά με το δημόσιο κλειδί του ατόμου που ισχυρίζεται ότι υπέγραψε το έγγραφο με το ιδιωτικό κλειδί του. Το λογισμικό επαλήθευσης είναι σε θέση να το κάνει χωρίς να αποκαλύπτει ποτέ το ιδιωτικό κλειδί (Ting, Yuen, Lee & Leong, 2002).

3.4.5 Υποδομές δημόσιου κλειδιού (Public Key Infrastructure)

Σχετικά με την υποδομή δημόσιου κλειδιού (PKI), αξιόπιστα όργανα, γνωστά ως αρχές πιστοποίησης, διαχειρίζονται κεντρικά το σύστημα με την έκδοση των συνδεδεμένων ιδιωτικών και δημόσιων κλειδιών, τρέχουν έναν διακομιστή για τη χρονική σήμανση κάθε υπογραφής και εκτελούν το λογισμικό επαλήθευσης. Συνήθως, η αρχή πιστοποίησης ενσωματώνει το δημόσιο κλειδί σε ένα πιστοποιητικό που περιέχει ένα σύνολο πρόσθετων μεταδεδομένων για τη διευκόλυνση της χρήσης (Won & Bollella, 2019). Αυτό προσφέρει πολλά πλεονεκτήματα, όπως το γεγονός ότι οι αρχές πιστοποίησης μπορούν να επαληθεύσουν την ταυτότητα των ατόμων στα οποία εκδίδονται τα κλειδιά, συνδέοντας έτσι τα δημόσια κλειδιά με τις πραγματικές ταυτότητες. Επίσης, ο καθένας μπορεί να έχει εμπιστοσύνη για την ημερομηνία υπογραφής, δεδομένου ότι το «ρολόι» διατηρείται μόνο από την αρχή πιστοποίησης (Ølnes, 2016). Ωστόσο, οι υποδομές δημόσιου κλειδιού δημιουργούν επίσης κεντρικό σημείο ελέγχου και αποτυχίας. Πιο συγκεκριμένα, εάν η αρχή πιστοποίησης που φιλοξενεί το λογισμικό επαλήθευσης κλείσει (για παράδειγμα, λόγω πτώχευσης, πολιτικών αναταραχών, αναδιάρθρωσης κλπ.), θα ακυρώσει αποτελεσματικά οποιοδήποτε έγγραφο υπογράφηκε μέσω αυτού. Αυτό αποτελεί σημαντικό πρόβλημα για πιστοποιητικά όπως αυτά της γέννησης, του γάμου ή σπουδών που διαρκούν για μια ζωή. Επιπλέον, η αρχή πιστοποίησης μπορεί να καταχραστεί την εμπιστοσύνη που τους έχει δοθεί. Εάν διαρρεύσει ένα ιδιωτικό κλειδί, τίποτα δεν εμποδίζει τον εισβολέα να εκδίδει πλαστά αρχεία και να υποστηρίζει το περιεχόμενο. Ακόμη και αν ένας υπεύθυνος έκδοσης πιστοποιητικών ανακαλέσει δημοσίως τα εν λόγω αρχεία, ένας ανεξάρτητος επαληθευτής δεν θα γνωρίζει τη διαφορά μεταξύ έγκυρου και μη έγκυρου μητρώου, εκτός εάν υπάρχει κάποια πρόσθετη εξουσιοδότηση που βεβαιώνει πότε πραγματοποιήθηκε η συναλλαγή (Shrier, Wu & Pentland, 2016).

3.5 Είδη blockchain (ιδιωτικά / δημόσια).

Το Blockchain είναι ένας τρόπος δομής των δεδομένων που επιτρέπει τη διατήρηση ψηφιακών καταλόγων και την κοινή χρήση μεταξύ ανεξάρτητων κόμβων στο δίκτυο. Η τεχνολογία blockchain έχει διάφορους τομείς χρήσης. Ανάλογα με τις απαιτήσεις ή το πλαίσιο της

κατάστασης, έκαστο blockchain έχει ρυθμιστεί να ανταποκρίνεται αντιστοίχως και υπάρχουν διαφορετικοί τύποι ρυθμίσεων στο blockchain που μπορούν να χρησιμοποιηθούν για την εκπλήρωση του σκοπού του. Υπάρχουν δύο αντικρουόμενοι στόχοι που καθορίζουν τον τύπο του blockchain. Οι συγκρούσεις έχουν να κάνουν με το εάν πρέπει τα blockchain να είναι διαφανή ή ιδιωτικά, και επιπλέον αν υπερισχύει η ασφάλεια έναντι της ταχύτητας (Ateniese, Magri, Venturi & Andrade, 2017). Η διαφάνεια έναντι της ιδιωτικής ζωής σχετίζεται με τη σύγκρουση όσον αφορά στην ανάγκη διαφάνειας για τη διευκρίνιση της κυριότητας ενός υλικού / άυλου περιουσιακού στοιχείου και των απαιτήσεων της ιδιωτικής ζωής των χρηστών. Η κυριότητα καθορίζεται από το σύνολο του ιστορικού των συναλλαγών που μπορεί να θεωρηθεί δημόσιο μητρώο ή μητρώο συναλλαγών, δεδομένου ότι είναι διαθέσιμο στο κοινό (Gabison, 2016). Η βασική ιδέα για την επαλήθευση των συναλλαγών και της ιδιοκτησίας εντός του μπλοκ αλυσίδας είναι η διαφάνεια. Ωστόσο, δημιουργείται σύγκρουση με την έννοια της ιδιωτικής ζωής, η οποία σχετίζεται με το επίπεδο προστασίας της ιδιωτικής ζωής όσον αφορά στα δεδομένα συναλλαγών και σε άλλες λεπτομέρειες, όπως οι λογαριασμοί ή τα ποσά που συμμετέχουν, κρυφά. Η άλλη σύγκρουση σχετίζεται με την προσπάθεια που απαιτείται για την εξασφάλιση του ιστορικού συναλλαγών του blockchain έναντι της επεκτασιμότητας και της ταχύτητας που απαιτείται για ορισμένες εμπορικές εφαρμογές του blockchain (Gupta, S2017). Λόγω της ανάγκης επίλυσης ενός πάζλ / αλγορίθμου κατακερματισμού για την αλυσίδα ενός μπλοκ στο προηγούμενο γονικό μπλοκ, η εξασφάλιση του ιστορικού συναλλαγών του blockchain σε έναν χαρακτήρα χωρίς παραβίαση, καθιστά τη διαδικασία πολύ χρονοβόρα και μειώνει την ταχύτητα με την οποία νέες οι συναλλαγές μπορούν να καταχωρηθούν στο blockchain. Όταν περιγράφεται το blockchain, συνήθως, είναι ο δημόσιος και άχρηστος τύπος δεδομένου που είναι θεμελιώδης και συμβαίνει στις περισσότερες κρυπτό-συχνότητες (Zhengetal., 2017). Ωστόσο, υπάρχουν δύο θεμελιώδεις λειτουργίες μιας δομής blockchain, οι οποίες διαβάζουν το ιστορικό δεδομένων συναλλαγής και καταγράφουν τα δεδομένα συναλλαγών. Με αυτή τη προσέγγιση, ορίζονται τέσσερις τύποι blockchains από αυτές τις λειτουργίες: δημόσιο και χωρίς άδεια, ιδιωτικό και χωρίς άδεια, δημόσιο και επιτρεπόμενο και ιδιωτικό & επιτρεπόμενο. Η ανάγνωση μπορεί να σχετίζεται με τη σύγκρουση μεταξύ διαφάνειας και ιδιωτικού απορρήτου, όπου αποφασίζεται ποιος θα επιτρέψει την πρόσβαση στην ανάγνωση (Swan, 2015). Μόνο ένας περιορισμένος αριθμός κόμβων ή ο καθένας ξεχωριστά, μπορεί να έχει πρόσβαση στην ανάγνωση του ιστορικού των συναλλαγών. Υπάρχουν δύο τύποι μπλοκ αλυσίδων που σχετίζονται με αυτό, τα δημόσια blockchains και τα ιδιωτικά blockchains. Όλοι οι χρήστες

έχουν πρόσβαση στην ανάγνωση όλων των ιστορικών συναλλαγών και στη δημιουργία νέων συναλλαγών εντός δημόσιων μπλοκ αλυσίδων, σε σύγκριση με τα ιδιωτικά blockchains όπου η πρόσβαση περιορίζεται σε μια προκαθορισμένη ομάδα κόμβων. Η πραγματική καταγραφή των συναλλαγών μπορεί να σχετίζεται με τη σύγκρουση μεταξύ ασφάλειας και ταχύτητας, όπου προσήκει η απόφαση σχετικά με το ποιος θα έχει το δικαίωμα να καταγράψει τις συναλλαγές. Εάν σε όλους γίνει η παραχώρηση για να καταγράφουν συναλλαγές, η απαιτούμενη προσπάθεια θα προχωρήσει, δηλαδή θα γίνει πολύ δαπανηρή, αφού το δίκτυο θα πρέπει να παρέχει ασφάλεια (Gabison, 2016). Αλλά εάν η πρόσβαση περιορίζεται σε αξιόπιστους κόμβους, απαιτείται μια λιγότερο προηγμένη προσπάθεια. Υπάρχουν δύο τύποι blockchains που σχετίζονται με αυτό: οι επιτρεπόμενες μπλοκ αλυσίδες και οι αόριστες μπλοκ αλυσίδες. Τα αδύναμα blockchains επιτρέπουν σε όλους να καταγράφουν τις συναλλαγές, δίνοντας σε κάθε κόμβο τη δυνατότητα να επαληθεύει τις συναλλαγές, καθώς και να δημιουργεί και να προσθέτει νέα μπλοκ. Τα παραχωρημένα blockchains έχουν μια προκαθορισμένη ομάδα αξιόπιστων ομάδων κόμβων στους οποίους έχει δοθεί πρόσβαση καταγραφής μέσα στο δίκτυο. Αυτό σημαίνει ότι μόνο αυτή η ομάδα κόμβων είναι μέρος της κατανεμημένης δομής συναίνεσης και επαληθεύει τις συναλλαγές. Οι άδειες για δημόσια blockchains περιορίζονται στην πληρέστερη χρήση λόγω της ανάγκης για πρόσθετες προσπάθειες, καθώς είναι χρονοβόρες. Αναφέρεται επίσης ότι αρκετά χρηματοπιστωτικά ιδρύματα εξετάζουν το ενδεχόμενο να έχουν το δικό τους blockchain με προκαθορισμένα δίκτυα και με αξιόπιστα μέρη για να περιορίσουν τις απαιτήσεις της προσπάθειας και να αυξήσουν τη διακίνηση των συναλλαγών (Zhengetal., 2017).

3.6 Κρυπτονομίσματα

Η καθιέρωση ενός ορισμού των κρυπτονομισμάτων (cryptocurrencies) δεν είναι εύκολη υπόθεση. Όπως το blockchain, οι cryptocurrencies έχουν γίνει ένα «τσιτάτο» (buzzword) για να αναφερθούν σε ένα ευρύ φάσμα τεχνολογικών εξελίξεων που χρησιμοποιούν μια τεχνική, γνωστή ως κρυπτογραφία. Με απλά λόγια, η κρυπτογραφία είναι η τεχνική της προστασίας της πληροφορίας μετασχηματίζοντάς την (δηλαδή την κρυπτογραφεί) σε μια μη αναγνώσιμη μορφή που μπορεί μόνο να αποκρυπτογραφηθεί (ή να αποκρυπτογραφηθεί) από κάποιον που διαθέτει ένα μυστικό κλειδί. Τα cryptocurrencies, όπως το Bitcoin, χρησιμοποιούν μια τεχνική με ένα έξυπνο σύστημα δημόσιων και ιδιωτικών ψηφιακών κλειδιών (Hileman & Rauchs, 2017). Η Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ) έχει ταξινομήσει τα κρυπτονομίσματα ως υποσύνολο εικονικών νομισμάτων. Σε

μια έκθεση σχετικά με τα εικονικά νομισματικά προγράμματα του 2012, ορίζονται τα νομίσματα αυτά ως μορφή μη ελεγχόμενων ψηφιακών χρημάτων, που συνήθως εκδίδονται και ελέγχονται από τους προγραμματιστές τους και χρησιμοποιούνται και γίνονται αποδεκτά μεταξύ των μελών μιας συγκεκριμένης εικονικής κοινότητας. Όπως και η ΕΚΤ, το Διεθνές Νομισματικό Ταμείο (ΔΝΤ) έχει κατηγοριοποιήσει τα cryptocurrencies ως ένα υποσύνολο εικονικών νομισμάτων, το οποίο ορίζει ως ψηφιακές παραστάσεις, αξίες που εκδίδονται από ιδιώτες επενδυτές και εκφράζονται στη δική τους λογιστική μονάδα (Chuen, Guo & Wang, 2017). Σύμφωνα με το ΔΝΤ, η έννοια των εικονικών νομισμάτων καλύπτει ένα ευρύτερο φάσμα νομισμάτων, που κυμαίνονται από απλά IOUs (Informal certificates of debt ή Ioweyou's - άτυπα πιστοποιητικά χρέους) από εκδότες (όπως κουπόνια διαδικτύου ή κινητής τηλεφωνίας), εικονικά νομίσματα που υποστηρίζονται από περιουσιακά στοιχεία όπως ο χρυσός και τα κρυπτονομίσματα όπως το Bitcoin (Liu & Tsyvinski, 2018).

Τα κρυπτονομίσματα και τα blockchain έχουν γίνει επικρατή θέματα τα τελευταία δύο χρόνια. Ενώ και τα δύο αναφέρονται συχνά στην ίδια φράση και είναι σαφώς συνδεδεμένα μεταξύ τους, δεν πρέπει να ταυτιστεί το ένα με το άλλο. Το Blockchain είναι ένας τύπος κατανεμημένης τεχνολογίας χαρτονομισμάτων που αποτελεί τη ραχοκοκαλιά της κρυπτογραφικής αγοράς. Είναι η τεχνολογία πίσω από τη μεγάλη ποικιλία κρυπτονομισμάτων που κυκλοφορούν σήμερα. Το πεδίο εφαρμογής του δεν περιορίζεται. Όπως αναφέρθηκε παραπάνω, το blockchain μπορεί να εφαρμοστεί σε διάφορους τομείς και μπορεί να έχει ένα ευρύ φάσμα εφαρμογών. Είναι σημαντικό να σχεδιαστεί μια σαφής γραμμή μεταξύ αυτών των εφαρμογών και των κρυπτό-συχνοτήτων, οι οποίες είναι μόνο μια συγκεκριμένη εφαρμογή της τεχνολογίας blockchain. Σε αυτό το πλαίσιο, οι ρυθμιστικές αρχές δεν χρειάζεται να φοβούνται με το να καταπνίγουν την καινοτομία όταν αντιμετωπίζουν το θέμα των κρυπτό-συχνοτήτων (Chuen, Guo & Wang, 2017).

3.7 Χρήση της τεχνολογίας blockchain ως δημόσια εγγραφή

Η πιο ευρέως γνωστή εφαρμογή ενός blockchain είναι ως publicledger (δημόσια εγγραφή) των συναλλαγών για τα cryptocurrencies όπως για παράδειγμα το Bitcoin και το Ether. Όπως και στην περίπτωση άλλων δημόσιων εγγραφών, η βιβλιογραφία παρέχει την καταγραφή της προέλευσης και της μεταβίβασης της κυριότητας ενός περιουσιακού στοιχείου. Η δομή των συναλλαγών των πρωτοκόλλων blockchain διευκολύνει όχι μόνο στη μεταφορά μιας κρυπτό-συχνότητας, αλλά και

άλλων ψηφιακών στοιχείων (Hileman & Rauchs, 2017). Ένα περιουσιακό στοιχείο μπορεί να είναι απτό, όπως ένα σπίτι, ένα αυτοκίνητο, μετρητά, γη ή άυλη πνευματική ιδιοκτησία, όπως διπλώματα ευρεσιτεχνίας, πνευματικά δικαιώματα ή επωνυμία. Ουσιαστικά, οτιδήποτε αξίας μπορεί να εντοπιστεί και να διακινηθεί σε ένα blockchain δίκτυο, μειώνοντας τον κίνδυνο και το κόστος για όλους τους εμπλεκόμενους (Gupta, S2017). Δεδομένου ότι έχουν σχεδιαστεί για την καταγραφή και τη διατήρηση συναλλαγών, όλα τα blockchains έχουν παραδοσιακά ένα ψηφιακό νόμισμα κάποιου είδους που συνδέεται με αυτά ως το πιο βασικό στοιχείο συναλλαγών στο δίκτυο. Αυτό έχει επίσης ενθαρρύνει την υιοθέτηση του πρωτοκόλλου αυτού του blockchain, καταβάλλοντας τους συνεισφέροντες στο δίκτυο, με τη δική του κρυπτογράφηση. Ως εκ τούτου, οι μπλοκ αλυσίδες καταγράφουν ομάδες συναλλαγών, αλλιώς γνωστές ως μπλοκ, οι οποίες συνδέονται μεταξύ τους κρυπτογραφικά σε μια γραμμική χρονική ακολουθία. Άλλες βασικές ιδιότητες που σχετίζονται με ένα blockchain (ασφάλεια, αμετάβλητο, προγραμματισμός) εξαρτώνται από την αρχιτεκτονική του blockchain και τον χαρακτήρα του συναινετικού πρωτοκόλλου που είναι σε ισχύ από αυτό το blockchain (Gabison, 2016). Ορισμένες μπλοκ αλυσίδες έχουν δομηθεί για να διευκολύνουν τις συναλλαγές από ομότιμους με μη ιεραρχικούς κόμβους. Αυτό είναι γνωστό ως κατανεμημένη δομή δικτύου. Ορισμένες μπλοκ αλυσίδες, όπως και το blockchain Bitcoin, εξασφαλίζουν επίσης τη σταθερότητα των καταγραφών τους, μέσω του μοναδικού πρωτοκόλλου συναίνεσής τους. Για να προσδιοριστεί το ποιος κατέχει ένα συγκεκριμένο στοιχείο, ένα συμβαλλόμενο μέρος πρέπει απλώς να συμβουλευθεί τις καταγραφές και να ελέγξει ποιος είναι ο πιο πρόσφατος ιδιοκτήτης του. Κατά την περιγραφή του μπλοκ, είναι σημαντικό να γίνει κατανοητό τόσο το σύνολο των κοινωνικών αρχών που στηρίζουν το βασικό ήθος και τη φιλοσοφία του (την «κοινωνική του αξία») όσο και τα χαρακτηριστικά της υποκείμενης αρχιτεκτονικής του για την υποστήριξη της κοινωνικής χρησιμότητάς του (Zhengetal., 2017).

3.8 Κοινωνική αξία και δυναμική της τεχνολογίας (αξιοπιστία, διαφάνεια)

Κατά την ενασχόληση με ένα θέμα όπως το blockchain, η τάση είναι να επικεντρώνεται κάποιος πρώτα σε ζητήματα που σχετίζονται με την ψηφιακή διαταραχή, την ψηφιακή οικονομία, τις βιομηχανίες γνώσης και το σύστημα καινοτομίας. Αυτό του επιτρέπει να κατανοήσει το πλαίσιο για την ψηφιακή σύγχυση. Ωστόσο, τυπικά δεν είναι μόνο η ψηφιακή τεχνολογία που έχει

σημασία. Εξίσου, αν όχι περισσότερο, σημαντικοί παράγοντες είναι και οι κοινωνικό-οικονομικοί οδηγοί που δημιουργούν τη ζήτηση για τεχνολογία (ή η αλλαγή ως ανταπόκριση σε αυτήν). Τα ψηφιακά επιχειρηματικά μοντέλα που λειτουργούν καλύτερα, έχουν καταλάβει την ψηφιακή τεχνολογία (Hou, 2017). Οι διαφορετικές υλοποιήσεις μπλοκ αλυσίδων αντιμετωπίζουν αυτές τις αρχές με διάφορους τρόπους και σε διαφορετικό βαθμό. Δεν είναι όλες οι μπλοκ αλυσίδες και / ή οι εφαρμογές τους κοινές, με αποτέλεσμα οι διαφορετικοί τύποι μπλοκ αλυσίδων να περικλείουν το σύνολο των αρχών που στηρίζουν και την πρόταση κοινωνικής αξίας της τεχνολογίας blockchain με διαφορετικό τρόπο. Υπάρχει συζήτηση για το ποιο είναι το πιο πιθανό blockchain για να ενσωματώσει ολόκληρο το σύνολο των αρχών, εντούτοις, μπορεί να υπάρχει μια ισχυρή περίπτωση που, ως δημόσιο μπλοκ με μεγάλο πρωτόκολλο συναίνεσης, το blockchain Bitcoin να βρίσκεται στην κορυφή της λίστας (Lemieux, 2016).

3.8.1 Αυτοκυριαρχία και ταυτότητα

Η πρώιμη βιβλιογραφία σχετικά με το blockchain κάνει συχνές αναφορές στην αυτονομία και την ικανότητα του ατόμου να κατέχει και να ελέγχει την ταυτότητά του στο διαδίκτυο. Σύμφωνα με μελέτες, τα δημόσια μπλοκ εμποδίζουν την κυριαρχία, δίνοντας στα άτομα τη δυνατότητα να είναι ο τελικός διαιτητής του ποιος μπορεί να έχει πρόσβαση και να χρησιμοποιεί τα δεδομένα και τις προσωπικές τους πληροφορίες. Σε ένα εκπαιδευτικό πλαίσιο, ο όρος είναι στο να γίνει συνώνυμος με την ενδυνάμωση των μεμονωμένων χρηστών να κατέχουν, να διαχειρίζονται και να μοιράζονται τα στοιχεία των διαπιστευτηρίων τους, χωρίς να χρειάζεται να καλούν το εκπαιδευτικό ίδρυμα ως αξιόπιστο διαμεσολαβητή (Beck, StenumCzepluch, Lollike & Malone, 2016). Αυτό μπορεί επίσης να θεωρηθεί ότι οι πολίτες αποκτούν σημαντική αυτοδυναμία για τον τρόπο με τον οποίο μοιράζονται τα προσωπικά τους δεδομένα και την ταυτότητά τους σε απευθείας σύνδεση και μπορούν να επιλέξουν να αποδεσμεύσουν όλα ή μέρος αυτών σε αντάλλαγμα της πρόσβασης στις υπηρεσίες που επιθυμούν. Η ταυτότητα είναι (η βάση για) εμπιστοσύνη στις αλληλεπιδράσεις μεταξύ του κοινού και της κυβέρνησης και αποτελεί έναν κρίσιμο παράγοντα παροχής υπηρεσιών, ασφάλειας, ιδιωτικότητας και δημόσιας ασφάλειας και βρίσκεται στο επίκεντρο της δημόσιας διοίκησης και των περισσότερων κυβερνητικών επιχειρηματικών διαδικασιών. Το πώς τα στοιχεία ταυτότητας συλλέγονται, χρησιμοποιούνται, διαχειρίζονται και εξασφαλίζονται είναι κρίσιμου ενδιαφέροντος για τους ηγέτες του δημόσιου τομέα. Η ταυτότητα αποτελεί μια περίπλοκη περιοχή για τους πολίτες και εκείνους που πρέπει να

την επαληθεύσουν. Πρόκειται για την αξιολόγηση της επαλήθευσης προσωπικών χαρακτηριστικών, η προσωπική ιστορία, οι σχέσεις και / ή οι ιστορικές συναλλαγές (Chen, Xu, Lu & Chen, 2018).

Η αξιολόγηση της ταυτότητας χρησιμοποιείται για την ελαχιστοποίηση οποιουδήποτε αντιληπτού χάσματος στην εμπιστοσύνη. Αυτό το χάσμα είναι ανάλογο του μέτρου κινδύνου που αντικατοπτρίζει την αντίληψη της ταυτότητας και τυχόν απωλειών. Ο συμβιβασμός είναι συχνά μια απώλεια ιδιωτικού απορρήτου με αντάλλαγμα την πρόσβαση σε συναλλαγές υψηλής αξίας. Το μειονέκτημα ιστορικά, ήταν η απώλεια της ιδιωτικής ζωής όπου η συναλλαγή είναι μέτριας έως ελάχιστης αξίας για το άτομο που ελέγχεται σε σύγκριση με τον κίνδυνο που παρουσιάζεται. Για να επαληθεύσουν ορισμένα χαρακτηριστικά της ταυτότητάς τους για να ολοκληρώσουν τη συναλλαγή, εκθέτουν επίσης άλλα χαρακτηριστικά των ταυτότητα που ενδεχομένως δεν επιθυμούν να αποκαλύψουν (Seebacher & Schüritz, 2017). Αυτή η αποκάλυψη θέτει όλα τα χαρακτηριστικά τους, σε αυτό το έγγραφο, σε κίνδυνο περαιτέρω ανεπιθύμητης αποκάλυψης ή παράνομης χρήσης. Η ψηφιακή ταυτότητα βρίσκεται σε εξέλιξη ως ένα ανθρώπινο δικαίωμα. Εντούτοις, δεν υπάρχει ακόμα κάποια μέθοδος ασφαλούς αποτυχίας για να αντιμετωπιστεί μία από τις ατέλειες του διαδικτύου π.χ. να εντοπιστούν άνθρωποι ή μηχανές online. Όταν οι πολίτες υποχρεούνται ή συμφωνούν να αποκαλύψουν την ηλεκτρονική τους ταυτότητα, δημιουργούνται νέα προβλήματα, όπως η χρήση ιδιωτικών αλγορίθμων για τη μεγιστοποίηση της εμπορικής χρήσης των προσωπικών δεδομένων των χρηστών στα κοινωνικά μέσα. Η τεχνολογία αλλάζει ριζικά την ικανότητά του καθενός να εκπροσωπεί τον εαυτό του. Ταυτόχρονα, η φύση του συνδεδεμένου κόσμου αλλάζει την αντίληψή για τη ταυτότητα και την εμπιστοσύνη (Ateniese, Magri, Venturi & Andrade, 2017).

Η κρυπτογραφία στον πυρήνα της τεχνολογίας του blockchain υπόσχεται να αντιμετωπίσει τα κενά της ταυτότητας και να «παλέψει» την ιδιοκτησία και τον έλεγχο των προσωπικών δεδομένων πίσω από τον μεμονωμένο χρήστη. Οι άνθρωποι, οι επιχειρήσεις και τα ιδρύματα μπορούν να αποθηκεύουν τα δικά τους δεδομένα ταυτότητας στις δικές τους συσκευές και να τα παρέχουν αποτελεσματικά σε εκείνους που πρέπει να την επικυρώσουν χωρίς να βασίζονται σε κεντρικό αποθετήριο δεδομένων ταυτότητας (Beck, StenumCzepluch, Lollike & Malone, 2016). Η τεχνολογία blockchain δεν παρέχει μόνο έναν νέο τρόπο ψηφιοποίησης τμημάτων χαρτιού που έχουν εγγενή αξία, όπως τα διαπιστευτήρια - παρέχει τα μέσα για να ελέγχει κάποιος την ταυτότητά του online και να την διαχειρίζεται κατάλληλα. Στην πραγματικότητα, ορισμένοι

ισχυρίστηκαν ότι η πλήρης ψηφιακή αυτονομία μπορεί τελικά να απομακρυνθεί από την κοινή χρήση οτιδήποτε μόνιμης «ταυτότητας», αλλά να γίνει ένα σύστημα επαλήθευσης αξιώσεων. Με άλλα λόγια, αντί να ζητούν εξωγενείς πληροφορίες, τα ερωτώμενα μέρη θα ζητήσουν αντί αυτού μόνο πληροφορίες που είναι άμεσα σχετικές με τη συναλλαγή, όπως για παράδειγμα, αν είναι το άτομο ηλικίας άνω των 18 ετών, εάν έχει λάβει διδακτορικό στη Νευροεπιστήμη από το MIT, εάν είναι πολίτης της Ιταλίας κ.λπ.. Αφού επαληθευτεί ικανοποιητικά, οι ισχυρισμοί μπορούν στη συνέχεια να αποσύρονται από το άτομο (Crosby, Pattanayak, Verma & Kalyanaraman, 2016).

3.8.2 Εμπιστοσύνη

Μια ισχυρή, πειστική μελέτη της κυβέρνησης του Ηνωμένου Βασιλείου, δείχνει ότι η εμπιστοσύνη είναι μια κρίση για τον κίνδυνο μεταξύ δύο ή περισσοτέρων ανθρώπων, οργανώσεων ή εθνών, και στον κυβερνοχώρο, βασίζεται σε δύο βασικές απαιτήσεις: στον έλεγχο ταυτότητας (απόδειξη ότι είναι κάποιος αυτός που λέει ότι είναι) και δεύτερον στην εξουσιοδότηση (απόδειξη ότι έχει κάποιος τις απαραίτητες άδειες για να κάνει ό,τι ζητάει). Εάν ένα από τα μέρη δεν είναι ικανοποιητικό από την απάντηση, ενδέχεται να επιτραπεί εξαιτίας του 2^{ου} μέρους να προχωρήσει η διαδικασία, αλλά υποβόσκουν επιπλέον κίνδυνοι. Ωστόσο, δεν υπάρχει βιώσιμη σχέση, εκτός αν τα μέρη εμπιστεύονται το ένα το άλλο. Υπό αυτή την έννοια, η εμπιστοσύνη σε μια κοινωνία είναι ανάλογη με την αξιοπιστία (Chen, Xu, Lu & Chen, 2018). Αυτή η βασική έννοια της εμπιστοσύνης παραμένει αμετάβλητη στον ψηφιοποιημένο κόσμο, όπου πρέπει να βασίζεται κάποιος σε πολλούς παράγοντες, τους οποίους δεν θα συναντήσει ποτέ και να ενεργεί με καλή πίστη. Η εμπιστοσύνη συχνά παρέχεται μόνο για μια πολύ συγκεκριμένη εφαρμογή, μέσα σε ένα συγκεκριμένο περιβάλλον και για ορισμένο χρονικό διάστημα. Σε μια παγκόσμια, ψηφιακή οικονομία, οι προκλήσεις της διατήρησης της εμπιστοσύνης - με τους προκύπτοντες ελέγχους και τις ισορροπίες, καθίστανται όλο και πιο δαπανηρές, χρονοβόρες και αναποτελεσματικές. Η τεχνολογία blockchain μπορεί να αποτελέσει μια βιώσιμη εναλλακτική λύση στην τρέχουσα διαδικαστική, οργανωτική και τεχνολογική υποδομή που απαιτείται για τη δημιουργία θεσμικής εμπιστοσύνης (Beck, StenumCzepluch, Lollike & Malone, 2016). Η βελτιωμένη εμπιστοσύνη μεταξύ των ενδιαφερόμενων μερών συνδέεται με τη χρήση αποκεντρωμένων δημόσιων βιβλίων, καθώς και με κρυπτογραφικούς αλγόριθμους που εγγυώνται ότι οι εγκεκριμένες συναλλαγές δεν μπορούν να τροποποιηθούν μετά την επικύρωσή τους. Τα κατανεμημένα βιβλία συμβάλλουν στην εμπιστοσύνη, δημιουργώντας ένα γεγονός σε ένα δεδομένο χρονικό σημείο, το οποίο στη συνέχεια

μπορεί να εμπιστευτεί κανείς. Αυτό επιτυγχάνεται αυτοματοποιώντας τους τρεις ρόλους του αξιόπιστου τρίτου μέρους: α) επικύρωση, β) συναλλαγές ασφαλούς φύλαξης και γ) τη διατήρησή τους εν συνεχεία. Η ελπίδα είναι ότι με τον ίδιο τρόπο που το Internet επανέλαβε την επικοινωνία και επηρέασε την κοινωνική συμπεριφορά, τα blockchains μπορούν επίσης να βοηθήσουν στην αντιμετώπιση των σημερινών κενών στις συναλλαγές, στις συμβάσεις και στις βάσεις εμπιστοσύνης των επιχειρήσεων, της κυβέρνησης και της κοινωνίας (Seebacher & Schüritz, 2017).

3.8.3 Διαφάνεια και προέλευση

Η ευκολία στην κοινή χρήση και η ορατότητα είναι βασικά χαρακτηριστικά ενός blockchain. Η έλλειψη του ενός ή του άλλου από αυτά τα χαρακτηριστικά στα υπάρχοντα συστήματα είναι συχνά ένας κεντρικός μοχλός για την υιοθέτηση του blockchain. Αυτά γίνονται ιδιαίτερα κρίσιμα στις συναλλαγές, όπου περισσότερες από μία οργανώσεις, πραγματοποιούν μπλοκαρίσματα συμμετοχών. Τα blockchains παρέχουν στους συμμετέχοντες πληροφορίες σχετικά με την προέλευση κάθε περιουσιακού στοιχείου και τον τρόπο με τον οποίο η ιδιοκτησία έχει αλλάξει με την πάροδο του χρόνου. Ωστόσο, αυτή η διαφάνεια λειτουργεί μόνο εάν οι συναλλαγές του blockchain συνδέονται με ένα αναγνωριστικό. Χωρίς δημόσιο αναγνωριστικό, όπως συνδεδεμένο έγγραφο ή σειριακό αριθμό, οι συναλλαγές του blockchain δεν μπορούν να αποκωδικοποιηθούν και να εντοπιστούν (McConaghyetal., 2017). Με αυτόν τον τρόπο, οι μπλοκ αλυσίδες (ακόμη και οι δημόσιες μπλοκ αλυσίδες) είναι ιδιωτικές από προεπιλογή, αλλά μπορούν επίσης να χρησιμοποιηθούν για την παρακολούθηση των συναλλαγών συγκεκριμένων ατόμων με την πάροδο του χρόνου μέσω συνδεδεμένων δεδομένων εκτός έδρας. Η τεχνολογία blockchain παρέχει έναν αναμφισβήτητο μηχανισμό για την επαλήθευση της ύπαρξης δεδομένων μιας συναλλαγής σε μια συγκεκριμένη χρονική στιγμή. Επιπλέον, επειδή κάθε μπλοκ της αλυσίδας περιέχει πληροφορίες σχετικά με το προηγούμενο μπλοκ, το ιστορικό, τη θέση και την ιδιοκτησία, κάθε μπλοκ πιστοποιείται αυτόματα και δεν μπορεί να τροποποιηθεί. Ένα ενιαίο, κοινόχρηστο λογότυπο παρέχει ένα μέρος για να προσδιοριστεί η ιδιοκτησία ενός περιουσιακού στοιχείου ή η ολοκλήρωση μιας συναλλαγής (Atzori, 2015).

3.8.4 Αμετάβλητο

Μια αμετάβλητη εγγραφή, αποτελεί ένα αμετάβλητο αρχείο του οποίου η κατάσταση δεν μπορεί να τροποποιηθεί μετά τη δημιουργία του. Η μετατόπιση συνδέεται με την ασφάλεια και τις κλασικές ιδιότητες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Η μετατόπιση αφορά επίσης την ανθεκτικότητα και τη μη αναστρεψιμότητα. Τα δεδομένα μπλοκαρίσματος δεν μπορούν εύκολα να αλλάξουν επειδή συνεχώς αναπαράγονται σε πολλές διαφορετικές τοποθεσίες. Με τη κρυπτογραφία του ιδιωτικού και του δημόσιου κλειδιού, ως μέρος του υποκείμενου πρωτοκόλλου, η ασφάλεια συναλλαγών και η εμπιστευτικότητα καθίστανται ουσιαστικά αδύνατες (Seebacher & Schüritz, 2017). Η αμετάβλητη χρήση των μπλοκ αλυσίδων σημαίνει ότι είναι ουσιαστικά αδύνατο να γίνουν αλλαγές μετά την καθιέρωσή τους. Με τον τρόπο αυτό αυξάνεται η εμπιστοσύνη στην ακεραιότητα των δεδομένων και μειώνονται οι δυνατότητες απάτης. Για να θεωρηθεί έγκυρη μια συναλλαγή σε ένα blockchain, όλοι οι συμμετέχοντες στη συναλλαγή πρέπει να συμφωνήσουν ότι οι κόμβοι εγκυρότητας που εκτελούν το πρωτόκολλο του blockchain πρέπει να καταλήξουν σε συναίνεση σχετικά με την εγκυρότητα της συναλλαγής. Ο μηχανισμός με τον οποίο συμβαίνει αυτό διαφέρει από blockchain σε blockchain, αλλά γενικά διανέμεται σε κάποιο βαθμό, πράγμα που σημαίνει ότι κανένας εκτελεστής δεν μπορεί να είναι διαιτητής της αλήθειας στο δίκτυο (Tamaetal., 2017). Κανένας συμμετέχων δεν μπορεί να παραβιάσει μια συναλλαγή αφού έχει καταγραφεί στο βιβλίο. Εάν μια συναλλαγή είναι λανθασμένη, πρέπει να χρησιμοποιηθεί μια νέα συναλλαγή για τη διόρθωση του σφάλματος και οι δύο συναλλαγές θα είναι ορατές στο ημερολόγιο. Η ανθεκτικότητα του blockchain προέρχεται από τη δομή του, αφού έχει σχεδιαστεί ως ένα κατανεμημένο δίκτυο κόμβων στο οποίο κάθε ένας από αυτούς τους κόμβους αποθηκεύει ένα αντίγραφο ολόκληρης της αλυσίδας. Επομένως, όταν μια συναλλαγή επαληθεύεται και εγκρίνεται από τους συμμετέχοντες κόμβους, είναι σχεδόν αδύνατο κάποιος να αλλάξει τα δεδομένα της συναλλαγής. Οι προσπάθειες αλλαγής δεδομένων σε μια τοποθεσία θα ερμηνευθούν ως δόλιες και θα γίνει επίθεση προς την ακεραιότητα του συστήματος από τους άλλους συμμετέχοντες, με αποτέλεσμα να απορριφθεί (Hou, 2017).

3.8.5Διαμεσολάβηση

Με την αντικατάσταση των μεσαζόντων, το blockchain μπορεί επίσης να προχωρήσει σε κάποια διατήρηση της εμπιστοσύνης. Οι συμμετέχοντες σε ένα blockchain συνδέονται μεταξύ τους σε μια αγορά, κατά την οποία μπορούν να διεξάγουν συναλλαγές και να μεταβιβάσουν την κυριότητα

των αποτιμημένων περιουσιακών στοιχείων μεταξύ τους με διαφάνεια και χωρίς τη βοήθεια ή την παρέμβαση τρίτων διαμεσολαβητών. Ένα δίκτυο τιμών λειτουργεί χωρίς καθορισμένη κεντρική αρχή. Με την τεχνολογία του blockchain, οι αλγόριθμοι συναίνεσης μεταξύ των ομότιμων συνεργατών καταγράφουν και επαληθεύουν με διαφάνεια τις συναλλαγές χωρίς κάποιον τρίτο παράγοντα, ενδεχομένως μειώνοντας ή και εξαλείφοντας το κόστος, τις καθυστερήσεις και τη γενική πολυπλοκότητα (Chen, Xu, Lu & Chen, 2018). Για παράδειγμα, τα blockchains μπορούν να μειώσουν τα γενικά έξοδα όταν τα μέρη εμπορεύονται τα περιουσιακά στοιχεία άμεσα μεταξύ τους ή γρήγορα αποδεικνύουν την κυριότητα ή την πνευματική ιδιοκτησία των πληροφοριών, ένα καθήκον το οποίο, διαφορετικά, είναι δίπλα αδύνατο χωρίς κεντρική αρχή ή αμερόληπτο διαμεσολαβητή. Επιπλέον, η ικανότητα των blockchains να εγγυάται την αυθεντικότητα στα θεσμικά όρια είναι πιθανό να βοηθήσει τα μέρη να επικεντρωθούν σε νέους τρόπους πιστοποίησης των εγγραφών, του περιεχομένου και των συναλλαγών. Μεγαλύτερη αποκέντρωση του διαδικτύου θα έδινε μεγαλύτερο έλεγχο στα χέρια του χρήστη ή πιο συγκεκριμένα των συσκευών του χρήστη αντί να βασίζεται σε πλατφόρμες που λειτουργούν από όσους κανουν χρήση π.χ. του Google ή του Amazon (McConaghyetal., 2017).

3.9 Προοπτική για μελλοντική αξιοποίηση σε πλήθος εφαρμογών

Η τεχνολογία blockchain έχει αρκετές εφαρμογές που μπορούν να χρησιμοποιηθούν ευεργετικά στον κατασκευαστικό κλάδο καθώς και σε άλλες βιομηχανίες. Οι ερευνητές δηλώνουν ότι οι μάρκες (brands) είναι ένα πολύ σημαντικό μέρος των μπλοκ αλυσίδων. Σύμφωνα με τους ίδιους, οι μπλοκ αλυσίδες δεν μπορούν να υπάρξουν χωρίς αυτές και δεν συνδέονται κατ’ ανάγκη με μια κρυπτό-συχνότητα. Μπορεί να συνδεθεί με δικαιώματα ψήφου, διορατικότητα, δεδομένα, άδειες και πολλές άλλες εφαρμογές που μπορούν να χρησιμοποιηθούν για χρηματικό όφελος. Μπορεί επίσης να είναι συμβολικό όπως στην καταβολή του μισθού που μετατρέπονται σε χρήματα στο επόμενο βήμα (Atzori, 2015). Μια άδεια μπορεί εύκολα να συνδεθεί με ένα κέρμα. Από τεχνικής απόψεως, δεν υπάρχει πρόβλημα σε μια τέτοια λύση. Ωστόσο, είναι πολύ σημαντικό να εκτιμηθεί εάν μια λύση με blockchain σε αυτούς τους όρους αρχειοθέτησης λύνει τα προβλήματα που προκύπτουν. Στις έρευνες δηλώνεται περαιτέρω ότι όλες οι συναλλαγές εντός ενός δικτύου μπορούν να ανιχνευθούν με τέλεια έλεγχο, αλλά δεν υπάρχουν κίνητρα γι’ αυτό, αφού το κόστος μπορεί να υπερβεί τα πιθανά κέρδη. Απαιτείται σχεδόν ρυθμιστικό αίτημα για να συμβεί αυτό.

Όπως περιγράφεται, μια πιθανή λύση είναι ένας προμηθευτής δευτέρου ή τρίτου επιπέδου να δημοσιοποιεί τα δεδομένα των συναλλαγών (Tamaetal., 2017) Η επιχείρηση εστίασης μπορεί στη συνέχεια να επαληθεύσει ότι οι πληρωμές πραγματοποιούνται για να αποφευχθούν οι παράνομες δραστηριότητες και να ενισχυθούν οι κοινωνικές πτυχές του εμπορίου. Το συμφέρον αυτό βρίσκεται επίσης στον προμηθευτή με το να πληρώσει για τα προϊόντα του. Τα πραγματικά οφέλη του blockchain θα προκύψουν όταν οι εφαρμογές αναπτύσσονται περαιτέρω σύμφωνα με τις έρευνες. Η τεχνολογία που μπλοκάρει και το τι θα οδηγήσει μπορεί να συγκριθεί με το διαδίκτυο (Hou, 2017).

Το διαδίκτυο δημιουργήθηκε ως οργανισμός κοινής ωφελείας και όλες οι εφαρμογές στο ανώτατο σημείο του, μετέτρεψαν το διαδίκτυο σε αυτό που είναι σήμερα. Όπως υποστηρίζεται στις έρευνες, το ίδιο πράγμα θα συμβεί και στα blockchain. Η IBM δηλώνει ότι αυτό που έκανε το διαδίκτυο για τις επικοινωνίες, το blockchain θα το κάνει για πιο αξιόπιστες συναλλαγές. Η διαχείριση της αλυσίδας εφοδιασμού είναι ένας τομέας όπου η IBM βλέπει πολλές δυνατότητες, με μια μακροπρόθεσμη προοπτική. Σήμερα, οι αλυσίδες εφοδιασμού είναι ολοκληρωμένες συναλλαγές, οι οποίες πραγματοποιούνται μέσω, για παράδειγμα, συστημάτων ERP (Enterprise Resource Planning). Η μορφή πρέπει να ενσωματωθεί στους εταίρους της αλυσίδας εφοδιασμού, όπου μεταφράζεται στην κατάλληλη μορφή για το άλλο μέρος. Αυτή είναι μια πολύ δαπανηρή διαδικασία που μπορεί να κοστίσει πολλά χρήματα ανά 36 μηνύματα που πρέπει να μεταφραστούν (Banerjee, 2018). Εντούτοις, οι λύσεις στοχεύουν στο blockchain, για αυτό δεν προβλέπεται να γίνουν βραχυπρόθεσμα, ειδικά οι προβληματικές περιοχές που δεν είναι ακόμη αυτοματοποιημένες ή ψηφιοποιημένες. Η IBM δηλώνει ότι ο χρηματοπιστωτικός τομέας βλέπει ένα μεγάλο δυναμικό με την τεχνολογία του blockchain. Πρόκειται για ένα συνεχιζόμενο έργο όπου οκτώ τράπεζες στην Ευρώπη βρίσκονται σε κοινοπραξία, αναπτύσσοντας μια εμπορική πλατφόρμα βασισμένη στην τεχνολογία του blockchain (Scott, 2016). Ο στόχος πίσω από αυτή την κοινοπραξία είναι να διευκολυνθούν οι διεθνείς συναλλαγές για τις Μικρές και Μεσαίες Επιχειρήσεις. Οι διεθνείς μεταφορές χρημάτων είναι σήμερα πολύ ακριβές και συνεπάγονται πολλές χειρωνακτικές εργασίες, οι οποίες μπορούν να ελαχιστοποιηθούν από την τεχνολογία του blockchain. Θα διευκολύνει ένα πιο διαφανές και αξιόπιστο περιβάλλον εντός του δικτύου αλυσίδας εφοδιασμού για τους πελάτες όπου οι διαδικασίες θα γίνονται πιο ψηφιοποιημένες. Το blockchain έχει αποδείξει τις δυνατότητές του ως ένας καλός τρόπος ανίχνευσης υλικών. Ορισμένα αντικείμενα μπορούν να ανιχνευθούν καταλλήλως, όπως το κρέας όπου μπορεί να

ελεγχθεί το DNA (Chen, Xu, Lu & Chen, 2018).. Είναι, ωστόσο, αδύνατο, για παράδειγμα, για τα μέταλλα, όπου θα μπορούν να τα λιώσουν σε διάφορα ορυχεία, πράγμα που καθιστά αδύνατο τον εντοπισμό. Οι έρευνες επεξηγούν περαιτέρω ότι η τεχνολογία μπορεί να διευκολύνει τον εντοπισμό της πηγής σφαλμάτων στην αλυσίδα εφοδιασμού. Μπορεί να μειώσει την προσπάθεια να ανιχνεύσει τα λάθη με ευεργετικό τρόπο. Η τεχνολογία του blockchain παρέχει τα μέσα για πιο εύκολο και αποτελεσματικό ίχνος, όταν υπάρχει στην αλυσίδα εφοδιασμού κάποιο σφάλμα, σε σύγκριση με το χειροκίνητο εντοπισμό που υφίσταται στην σημερινή εποχή (Lemieux, 2016).

Κεφάλαιο 4: Η προστιθέμενη αξία της τεχνολογίας blockchain στην πιστοποίηση τίτλων σπουδών

4.1 Περιορισμοί των έντυπων πιστοποιητικών

Τα έντυπα πιστοποιητικά εξακολουθούν να θεωρούνται σε πολλές περιπτώσεις ως η πιο ασφαλής μορφή πιστοποίησης, δεδομένου ότι είναι δύσκολο να πλαστογραφηθούν λόγω των χαρακτηριστικών ασφαλείας που ενσωματώνονται στα ίδια τα πιστοποιητικά, ότι (συνήθως) λαμβάνονται απευθείας από τον παραλήπτη, ο οποίος επομένως έχει τον πλήρη έλεγχο για αυτό, ότι είναι σχετικά εύκολο να αποθηκευτούν με ασφάλεια για μεγάλες χρονικές περιόδους, π.χ. με τη διατήρησή τους σε ασφαλές μέρος και, τέλος, μπορούν να υποβάλλονται από τον παραλήπτη οπουδήποτε, σε οποιοδήποτε πρόσωπο για οποιονδήποτε σκοπό (Johnson, 2006).

Ωστόσο, τα έντυπα πιστοποιητικά παρουσιάζουν επίσης σημαντικά μειονεκτήματα. Ενώ είναι δύσκολο να πλαστογραφηθούν, κανένα πιστοποιητικό δεν προστατεύεται από τον κίνδυνο πλαστογραφίας. Έτσι, ο εκδότης είναι υποχρεωμένος να διατηρεί κεντρικό μητρώο εκδοθέντων πιστοποιητικών που μπορούν να χρησιμοποιηθούν για την επαλήθευση της αυθεντικότητας του πιστοποιητικού. Τα μητρώα πιστοποιητικών ενέχουν κίνδυνο αποτυχίας, αφού, ενώ τα πιστοποιητικά μπορεί να παραμείνουν έγκυρα, χάνεται η δυνατότητα επαλήθευσης τους. Η τήρηση ενός τέτοιου μητρώου απαιτήσεων και η απάντηση σε ερωτήματα σχετικά με την εγκυρότητα των πιστοποιητικών είναι μια γραφειοκρατική διαδικασία, η οποία απαιτεί σημαντικούς πόρους (Contreras & Gollin, 2009). Τα χαρακτηριστικά ασφαλείας στο φυσικό πιστοποιητικό απορρέουν αποκλειστικά από το επίπεδο δυσκολίας και την εμπειρογνωμοσύνη που απαιτείται για την σύνταξη του εγγράφου. Όσο πιο ασφαλές είναι το πιστοποιητικό, τόσο πιο ακριβό είναι να εκδοθεί. Τα ενιαία πιστοποιητικά ασφαλείας, όπως τα διαβατήρια, κοστίζουν συνήθως € 20- € 150. Επίσης, δεν υπάρχουν περιορισμοί στην ικανότητα του εκδότη να χρησιμοποιήσει παράνομα τη χρονική σφραγίδα ή άλλες λεπτομέρειες του πιστοποιητικού. Αφού εκδοθεί, δεν υπάρχει κανένας τρόπος να ανακληθεί ένα πιστοποιητικό χωρίς ο κάτοχος να παραιτηθεί από τον έλεγχό του. Αν κάποιος τρίτος πρέπει να χρησιμοποιήσει τα πιστοποιητικά, π.χ. για να επαληθεύσει τους ισχυρισμούς σε βιογραφικό σημείωμα, πρέπει να διαβάσει και να

επαληθεύσει κάθε πιστοποιητικό μεμονωμένα και χειροκίνητα, μια διαδικασία που είναι σημαντικά χρονοβόρα (GARWE, 2015).

4.2 Περιορισμοί ψηφιακών πιστοποιητικών (χωρίς blockchain)

Τα ψηφιακά πιστοποιητικά διαθέτουν πολλά πλεονεκτήματα έναντι των έντυπων πιστοποιητικών. Αρχικά, απαιτούν πολύ λιγότερους πόρους για έκδοση, συντήρηση και χρήση, καθώς η αυθεντικότητα των πιστοποιητικών μπορεί να ελέγχεται αυτόματα από το μητρώο χωρίς ανθρώπινη παρέμβαση. Όπου κάποιος τρίτος πρέπει να χρησιμοποιήσει τα πιστοποιητικά, αυτά μπορούν να ταξινομηθούν αυτόματα, να επαληθευτούν και ακόμη να συνοψιστούν εάν εκδοθούν σε τυποποιημένη μορφή. Επιπλέον, η ασφάλεια του πιστοποιητικού απορρέει από την ασφάλεια των κρυπτογραφικών πρωτοκόλλων, τα οποία διασφαλίζουν ότι το πιστοποιητικό είναι φτηνό να εκδοθεί, αλλά εξαιρετικά δαπανηρό να εκδοθεί από τον οποιονδήποτε εκτός από τον εκδότη. Τα πιστοποιητικά μπορούν να ανακληθούν από τον εκδότη. Τέλος, ορισμένες μορφές απάτης, όπως η αλλαγή της χρονικής σήμανσης ή η αλλαγή του σειριακού πιστοποιητικού, μπορεί να καταστεί αδύνατη ανάλογα με τον σχεδιασμό του συστήματος (Maurer, 2003).

Ωστόσο, τα ψηφιακά πιστοποιητικά έχουν επίσης σημαντικά μειονεκτήματα. Χωρίς τη χρήση ψηφιακών υπογραφών, είναι εξαιρετικά εύκολο να πλαστογραφηθούν. Επίσης, τις περιπτώσεις που χρησιμοποιούνται ψηφιακές υπογραφές, απαιτείται η συμμετοχή τρίτων παρόχων πιστοποιητικών για την εξασφάλιση της ακεραιότητας της συναλλαγής. Αυτά τα τρίτα μέρη ελέγχουν σημαντικά κάθε πτυχή της διαδικασίας πιστοποίησης και επαλήθευσης, στην οποία μπορεί να γίνει κατάχρηση. Σε πολλές χώρες, δεν υπάρχει καθολικά χρησιμοποιούμενο ανοιχτό πρότυπο για ψηφιακές υπογραφές που να οδηγεί σε πιστοποιητικά που μπορούν να εξακριβωθούν μόνο στο πλαίσιο συγκεκριμένων οικοσυστημάτων λογισμικού. Ακόμα, είναι ευκολότερο να καταστραφούν τα ηλεκτρονικά αρχεία, η διατήρησή τους σε ασφαλή κατάσταση απαιτεί πολύπλοκα, πολυεπίπεδα εφεδρικά συστήματα τα οποία είναι επιρρεπή σε αποτυχία. Αν το μητρώο αποτύχει, τα ίδια τα πιστοποιητικά καθίστανται άνευ αξίας, δεδομένου ότι σε αντίθεση με τα έντυπα πιστοποιητικά, δεν κατέχουν εσωτερική αξία χωρίς το μητρώο. Τα μητρώα ψηφιακών πιστοποιητικών είναι επιρρεπή σε διαρροές δεδομένων μεγάλης κλίμακας (Schukat & Cortijo, 2015).

4.3 Ψηφιακά πιστοποιητικά με τεχνολογία Blockchain

Η τεχνολογία Blockchain είναι ιδανική ως νέα υποδομή για να εξασφαλίσει, να μοιραστεί και να επαληθεύσει τα αποτελέσματα εκπαίδευσης. Στην περίπτωση πιστοποιήσεων, ένα blockchain μπορεί να διατηρεί έναν κατάλογο του εκδότη και του παραλήπτη κάθε πιστοποιητικού μαζί με την υπογραφή εγγράφου (hash) σε μια δημόσια βάση δεδομένων (blockchain) η οποία αποθηκεύεται πανομοιότυπα σε χιλιάδες υπολογιστές σε όλο τον κόσμο. Έτσι, τα ψηφιακά πιστοποιητικά που αποθηκεύονται σε ένα blockchain έχουν σημαντικά πλεονεκτήματα έναντι των «κανονικών» ψηφιακών πιστοποιητικών, καθώς δεν μπορούν να πλαστογραφηθούν και είναι δυνατόν να επαληθευθεί με βεβαιότητα ότι το πιστοποιητικό είχε αρχικά εκδοθεί και παραληφθεί από τα ίδια πρόσωπα που αναφέρονται σε αυτό (Crosby, Pattanayak, Verma & Kalyanaraman, 2016). Η επαλήθευση του πιστοποιητικού μπορεί να γίνει από οποιονδήποτε έχει πρόσβαση στο blockchain, με λογισμικό ανοιχτού κώδικα που είναι εύκολα διαθέσιμο και δεν υπάρχει ανάγκη για μεσάζοντες. Επειδή ακριβώς δεν απαιτείται από μεσάζοντες να επικυρώσουν το πιστοποιητικό, αυτό μπορεί να επικυρωθεί ακόμη και αν ο οργανισμός που το εξέδωσε δεν υπάρχει πλέον ή δεν έχει πλέον πρόσβαση στο εκδοθέν αρχείο. Η καταγραφή των πιστοποιητικών που έχουν εκδοθεί και ληφθεί σε blockchain μπορεί να καταστραφεί μόνο εάν καταστραφεί κάθε αντίγραφο σε κάθε υπολογιστή στον κόσμο που φιλοξενεί το λογισμικό. Το hash είναι απλώς ένας τρόπος δημιουργίας ενός συνδέσμου (link) με το πρωτότυπο έγγραφο, το οποίο κατέχει ο χρήστης. Αυτό σημαίνει ότι ο προαναφερόμενος μηχανισμός επιτρέπει η υπογραφή ενός εγγράφου να δημοσιευτεί, χωρίς να χρειάζεται να δημοσιευτεί το ίδιο το έγγραφο, διατηρώντας έτσι το απόρρητο των εγγράφων (Grätheretal., 2018).

4.4 Πλεονεκτήματα για τον παραλήπτη

Τα Blockchains δημιουργούν τις ακόλουθες ιδανικές προϋποθέσεις για ένα πιστοποιητικό από την πλευρά του παραλήπτη:

- Ανεξαρτησία: ο παραλήπτης είναι κάτοχος της πιστοποίησης και δεν απαιτεί από τον εκδότη ή τον τρίτο να επαληθεύσει τη συμμετοχή του μετά τη λήψη των διαπιστευτηρίων
- Ιδιοκτησία: ο παραλήπτης μπορεί να αποδείξει την κυριότητα του πιστοποιητικού

- Έλεγχος: ο παραλήπτης ελέγχει τον τρόπο με τον οποίο διαχειρίζεται τα διαπιστευτήρια που του ανήκουν. Μπορεί να επιλέξει να συνδέσει τα διαπιστευτήρια με ένα καθιερωμένο προφίλ που κατέχει ή όχι.
- Επαλήθευση: η πιστοποίηση είναι επαληθεύσιμη από τρίτους, όπως εργοδότες, επιτροπές αποδοχής και οργανισμούς επαλήθευσης
- Μονιμότητα: η πιστοποίηση είναι μόνιμη εγγραφή (με την επιφύλαξη περιορισμών) (Ølnes, 2016).

4.5 Πλεονεκτήματα για τον Εκδότη

Τα Blockchains δημιουργούν τις ακόλουθες ιδανικές προϋποθέσεις για ένα πιστοποιητικό από την πλευρά του εκδότη. Ο εκδότης μπορεί να αποδείξει ότι εξέδωσε το πιστοποιητικό, μπορεί να ορίσει μια προθεσμία λήξης για τα διαπιστευτήρια και μπορεί να ανακαλέσει την πιστοποίηση. Το σύστημα πιστοποίησης είναι ασφαλές και επιβάλλει ελάχιστη συνεχή επιβάρυνση προκειμένου να παραμένει έτσι (Grätheretal., 2018).

Προκειμένου η πραγματική πιστοποίηση να έχει νόημα και χρησιμότητα, ένας τρίτος φορέας επαλήθευσης, όπως ένα ίδρυμα που λαμβάνει την πιστοποίηση ως μέρος μιας αίτησης, πρέπει να είναι βέβαιος για την ακρίβεια ενός πιστοποιητικού. Οι τυπικές προϋποθέσεις είναι οι εξής:

- Ακεραιότητα: το περιεχόμενο δεν έχει αλλοιωθεί, δηλαδή συμφωνεί με αυτό που ο εκδότης είχε αρχικά επιδιώξει.
- Γνησιότητα: εμπιστοσύνη ότι ο εκδότης είναι ο δικαιούχος του πιστοποιητικού και δεν έχει πλαστογραφηθεί (Crosby, Pattanayak, Verma & Kalyanaraman, 2016).

4.6 Πιστοποίηση Ταυτότητας με χρήση Blockchain

Όταν κάποιος επιθυμεί να επιβεβαιώσει την ταυτότητά του σε άλλο άτομο ή ίδρυμα, θα μοιραστεί μεγάλο μέρος αυτών των προσωπικά αναγνωρίσιμων πληροφοριών. Ως εκ τούτου, για παράδειγμα ένας υποψήφιος φοιτητής μπορεί να επιβεβαιώσει την ταυτότητά του σε ένα γραφείο υποδοχής πανεπιστημίου, παρέχοντας το όνομα, τη διεύθυνση, τον αριθμό ταυτοποίησης του κράτους, το

φύλο και τους βαθμούς. Τυπικά, το γραφείο υποδοχής θα κρατήσει όλα αυτά τα δεδομένα σε μια κεντρική βάση δεδομένων, απαιτώντας από τον χρήστη να το εμπιστευθεί για την ασφάλεια των δεδομένων του. Ωστόσο, λόγω της αξίας τέτοιων δεδομένων, αυτή η διαδικασία είναι εξαιρετικά ευαίσθητη σε κινδύνους όπως η κατάχρηση, η απάτη και η κλοπή, όπως αποδεικνύεται από πρόσφατο κύμα κλοπών μεγάλης κλίμακας σε μαζικά δεδομένα από κυβερνήσεις και εταιρείες σε όλο τον κόσμο (Ølnes, 2016). Επί του παρόντος, κάθε φορά που ένα άτομο χρειάζεται να πραγματοποιήσει μια συναλλαγή με ένα νέο άτομο ή οργανισμό πρέπει και πάλι να προσκομίσει τα δεδομένα του και να δώσει σε άλλο πρόσωπο τον έλεγχο σχετικά με το πώς τα δεδομένα αυτά διασφαλίζονται και μοιράζονται. Η τεχνολογία Blockchain επιτρέπει μια νέα αντίληψη της αυτοκυρίαρχης ταυτότητας (sovereign identity), κατά την οποία ο χρήστης αποθηκεύει τις δικές του προσωπικές πληροφορίες σε προσωπική συσκευή όπως το smartphone και μοιράζεται με τρίτους μόνο ό,τι είναι απαραίτητο. Αυτό είναι το ψηφιακό ισοδύναμο για τη διατήρηση των έντυπων πιστοποιητικών σε ένα ασφαλές περιβάλλον και για την επίδειξή τους σε τρίτο προκειμένου να αποδειχθεί η ταυτότητα, με τη διατήρηση όμως του ελέγχου σχετικά με το πόσο αυτά τα τρίτα μέρη μπορούν να αντιγράψουν αυτά τα έγγραφα ή όχι. Η τεχνολογία Blockchain επιτρέπει επίσης στον χρήστη να πιστοποιεί την ταυτότητά του χωρίς να είναι απαραίτητο να μοιράζεται τα βασικά δεδομένα που αποτελούν αυτή την ταυτότητα (Grätheretal., 2018).

4.7 Χρήση πιστοποιημένης αυτοκυρίαρχης ταυτότητας (self-sovereign identity)

Στην περίπτωση που ένα άτομο έχει μια πλήρη αυτοκυρίαρχη ταυτότητα, τα προσωπικά του δεδομένα αποθηκεύονται ψηφιακά σε μια συσκευή στην οποία έχει πρόσβαση μόνο αυτό και τα οποία ελέγχει, όπως ένα ψηφιακό πορτοφόλι. Ο κατατεμαχισμός (hash) των δεδομένων αυτών, είτε αποτελείται από ισχυρισμούς είτε από ψηφιακά έγγραφα, μπορεί να αποθηκεύεται στο blockchain. Η εγκυρότητα των δεδομένων αυτών πιστοποιείται από τρίτους, όπως είναι ο φορέας έκδοσης ή επαλήθευσης (Baars, 2016). Έτσι, τα πιστοποιητικά είναι επίσης αποθηκευμένα στη συσκευή ασφαλείας με τα υπόλοιπα δεδομένα του ατόμου και κατατεμαχισμένα σε ένα blockchain. Με αυτά τα στοιχεία, ένα άτομο μπορεί να ταυτοποιηθεί με ασφάλεια σε οποιοδήποτε μέρος το οποίο εμπιστεύεται επίσης το ίδρυμα επαλήθευσης απλώς αποδεικνύοντας ότι είναι ο κάτοχος του δημόσιου κλειδιού που συνδέεται με την αξίωση πιστοποιητικού και χωρίς να είναι απαραίτητη η κοινοποίηση οποιουδήποτε στοιχείου προσωπικής ταυτοποίησης - ούτε καν το

όνομά τους. Συνεπώς, όταν ο φοιτητής στο πανεπιστήμιο λάβει υποτροφία (παράδειγμα ενότητας 4.6), μπορεί να χρειαστεί να ταυτοποιηθεί ως αποδέκτης υποτροφιών σε άλλα μέρη του πανεπιστημίου προκειμένου να λάβει κάποιες υπηρεσίες (Crosby, Pattanayak, Verma & Kalyanaraman, 2016).

Για παράδειγμα, ενδέχεται να δικαιούνται δωρεάν βιβλία από το βιβλιοπωλείο του πανεπιστημίου. Κατά παράδοση, το βιβλιοπωλείο του πανεπιστημίου θα πρέπει να κατέχει τα στοιχεία των φοιτητών που δικαιούνται υποτροφίες και δωρεάν βιβλία για να είναι σε θέση να προσφέρει αυτήν την υπηρεσία. Έτσι, για να δικαιούται ελεύθερα βιβλία, ο φοιτητής θα χρειαστεί να επιτρέψει σε ένα βιβλιοπωλείο να κρατήσει εξαιρετικά ευαίσθητες πληροφορίες από τις οποίες θα μπορούσε κανείς να συμπεράνει την οικονομική κατάσταση του σπουδαστή και εκείνη της οικογένειάς του (Kolvenbach, Ruland, Gräther & Prinz, 2018). Με μια επαληθευμένη αυτοκυρίαρχη ταυτότητα, το βιβλιοπωλείο δεν θα χρειαστεί να κρατήσει κανένα στοιχείο. Ο φοιτητής απλώς θα εμφανιστεί, θα παρουσιάσει την ιδιότητά του ως υπότροφου (αποθηκευμένος στο τηλέφωνο ή σε άλλη συσκευή) και στη συνέχεια θα αποδείξει ότι είναι κάτοχος αυτού του δικαιώματος εισάγοντας τον κωδικό πρόσβασής του ή σαρώνοντας τα δακτυλικά αποτυπώματα στο τηλέφωνό του. Δεδομένου ότι ο ιδιοκτήτης του βιβλιοπωλείου εμπιστεύεται ότι ο εκδότης πιστοποιητικού (δηλαδή το γραφείο υποδοχής) έχει επαληθεύσει την ταυτότητα κατάλληλα και μπορεί να εμπιστευτεί το πιστοποιητικό λόγω της ασφάλειας και του αμετάβλητου που χαρακτηρίζουν το blockchain, θα μπορούσε να παραχωρήσει τα βιβλία χωρίς να χρειάζεται να αποθηκεύσει οποιοδήποτε κομμάτι πληροφοριών σχετικά με τον φοιτητή (Ølnes, 2016).

4.8 Έκδοση Πιστοποιητικών με άμεση χρήση του Blockchain

Όπου ένα πιστοποιητικό μπορεί να έχει μετρήσιμη αξία, μπορεί να εμφανίζεται ως ένα διακριτικό σύμβολο (token) και να λειτουργεί απευθείας σε ένα προσαρμοσμένο blockchain. Έτσι, παραδείγματος χάριν σε ένα blockchain για τα απολυτήρια του σχολείου, ένα μόνο πιστοποιητικό μπορεί να θεωρηθεί ως ένα διακριτικό σύμβολο, για τις εκπαιδευτικές πιστωτικές μονάδες, 1 ECTS θα ισοδυναμούσε με ένα διακριτικό σύμβολο, για αναφορές παρακολούθησης (tracking) σε περιοδικά. Έτσι, τα πιστοποιητικά θα μπορούσαν να μεταφερθούν από ένα άτομο σε ένα άλλο, απλά με τη μεταφορά ενός διακριτικού στο blockchain. Πρόσθετες πληροφορίες σχετικά με το πιστοποιητικό θα μπορούσαν να αποθηκευτούν είτε απευθείας στο blockchain είτε με τη

δημιουργία σύνδεσης (linking) του πιστοποιητικού με την είσοδο του blockchain (Kolvenbach, Ruland, Gräther & Prinz, 2018). Έτσι, είναι δυνατό να σχεδιαστεί μια βάση δεδομένων όπου κάποιες πληροφορίες θα είναι ιδιωτικές και θα διατηρούνται από τον χρήστη, ενώ άλλες πληροφορίες θα κρατούνται δημόσια σε ένα blockchain. Το πλεονέκτημα της έκδοσης πιστοποιητικών απευθείας σε ένα blockchain είναι ότι τα ίδια τα πιστοποιητικά, και όχι μόνο η απόδειξη της υπογραφής τους, γίνονται αμετάβλητα και μόνιμα. Το μειονέκτημα είναι ότι κάθε blockchain γενικής χρήσης που χρησιμοποιείται με αυτόν τον τρόπο θα αυξηθεί σημαντικά σε μέγεθος, πράγμα που σημαίνει ότι θα οδηγούσε σε χαμηλές επιδόσεις και υψηλή χρήση πόρων. Έτσι, ένα τέτοιο μοντέλο θα μπορούσε να εφαρμοστεί μόνο ως ιδιωτικό/εξουσιοδοτημένο blockchain (Baars, 2016).

4.9 Έκδοση συμπληρώματος διπλώματος (diploma supplement) σε blockchain

Πραγματικά, ένα πιστοποιητικό πτυχίου έχει ελάχιστες πληροφορίες. Περιέχει την ημερομηνία, το θεσμικό όργανο ανάθεσης, τον δικαιούχο και τον τίτλο του πτυχίου. Για παράδειγμα, *το Πανεπιστήμιο της Μάλτας εξέδωσε Bachelors in Science (Hons) στην Jane Doe στις 15 Ιουνίου 2017.* Κάτι τέτοιο είναι ένα μικρό ποσό πληροφοριών που προσφέρεται για να αποθηκευτεί σε ένα λογαριασμό, δεσμεύοντας λίγο χώρο στην αλυσίδα. Έτσι, θα μπορούσε να δημοσιευθεί σε ένα blockchain είτε ως απλό κείμενο, αν σκοπός είναι να δημιουργηθεί μια δημόσια διαθέσιμη βάση δεδομένων με πτυχία που απονέμονται, είτε με κατακερματισμό (hash) του πιστοποιητικού (με χρήση ενός συστήματος, όπως το Blockcerts), αν σκοπός είναι να εξασφαλίσει το ψηφιακό πιστοποιητικό που απονέμεται στον φοιτητή (Allessie, Sobolewski, Vaccari & Pignatelli, 2019). Οι απόφοιτοι του Ευρωπαϊκού Χώρου Τριτοβάθμιας Εκπαίδευσης έχουν το δικαίωμα να λάβουν συμπληρωματικό δίπλωμα μαζί με τα προσόντα τους, το οποίο επιπλέον να δείχνει το επίπεδο και τη λειτουργία του τίτλου σπουδών, το περιεχόμενο και τα αποτελέσματα που αποκτήθηκαν, την πιστοποίηση του συμπληρώματος, τις λεπτομέρειες του εθνικού συστήματος τριτοβάθμιας εκπαίδευσης, οποιεσδήποτε πρόσθετες σχετικές πληροφορίες. Αυτές οι πληροφορίες μπορούν να εμφανιστούν σε αρκετές σελίδες και, ενώ είναι κατάλληλες για αποθήκευση σε μια βάση δεδομένων, δεν είναι κατάλληλες για αποθήκευση σε έναν λογαριασμό. Επιπλέον, θα ήταν απαγορευτικά δαπανηρό να αποθηκεύεται αυτό το επίπεδο πληροφοριών απευθείας σε ένα blockchain. Ως εκ τούτου, τα προσόντα μαζί με το συμπλήρωμα διπλωμάτων τους θα μπορούσαν

να δημοσιευθούν σε blockchain είτε ως απλό κείμενο που περιλαμβάνει χρονική σφραγίδα, θεσμικό όργανο ανάθεσης, δικαιούχο, τίτλο πτυχίου και σύνδεσμο προς το πλήρες κείμενο του συμπληρωματικού διπλώματος που κρατείται εκτός αλυσίδας (offchain), είτε ως hash του πιστοποιητικού (χρησιμοποιώντας ένα σύστημα όπως το Blockcerts) εάν ο σκοπός είναι να εξασφαλίσει το ψηφιακό πιστοποιητικό που απονέμεται στον φοιτητή (Crosby, Pattanayak, Verma & Kalyanaraman, 2016).

4.10 Ψηφιακά πιστοποιητικά με τη χρήση της τεχνολογίας Blockchain

4.10.1 Η προστιθέμενη αξία των Ψηφιακών Πιστοποιητικών με την ασφάλεια του Blockchain

Η τεχνολογία Blockchain είναι ιδανική ως νέα υποδομή για να εξασφαλίσει, να μοιραστεί και να επαληθεύσει τα αποτελέσματα της εκπαίδευσης. Στο blockchain, η υποδομή δημόσιου κλειδιού αντικαθιστά την κεντρική αρχή με ένα πιο ισχυρό αποκεντρωμένο δίκτυο. Η αποκεντρωμένη αυτή δομή ενισχύει τη μακροζωία του δικτύου διότι τα διπλά κείμενα των μπλοκ, στα οποία αποθηκεύονται οι υπογραφές, είναι πολυάριθμα. Η αποκέντρωση του blockchain δίνει ένα επιπλέον πλεονέκτημα, καθώς κανένας τρίτος δεν μπορεί να αλλάξει ή να διαγράψει τις συναλλαγές που είναι αποθηκευμένες στα μπλοκ, χωρίς να καταργήσει τις αποδεικτικές κινήσεις που τις είχαν επαληθεύσει (Won & Bollella, 2019). Πέρα από το ότι εξαλείφουν την ανάγκη οποιασδήποτε αρχής πιστοποίησης ή κάποιο αξιόπιστο τρίτο μέρος, τα blockchains παρέχουν ανεξάρτητη χρονική σφράγιση, γεγονός που δημιουργεί σημαντικά οφέλη για την ασφάλεια (Shrier, Wu & Pentland, 2016). Η αξιόπιστη χρονική σφραγίδα είναι σαφώς σημαντική στις περιπτώσεις που λήγουν τα διαπιστευτήρια, αλλά είναι επίσης ουσιαστική για πρακτικό λόγο, καθώς ο εκδότης πρέπει να είναι σε θέση να εναλλάσσει τα κλειδιά σε τακτική βάση, τόσο ως μέρος των βέλτιστων πρακτικών ασφαλείας, αλλά περισσότερο στην περίπτωση διαρροής κλειδιών. Για να διαπιστωθεί ότι ένα αρχείο εκδόθηκε από έναν συγκεκριμένο εκδότη όταν το κλειδί έκδοσης ήταν έγκυρο, απαιτεί γνώση ενός ανεξάρτητου χρονικού σήματος. Σε αντίθεση με πολλά συστήματα υποδομών δημόσιου κλειδιού, οι υπογραφές σε blockchain είναι επίσης ανεξάρτητες από το αρχείο. Το ίδιο λογισμικό μπορεί να χρησιμοποιηθεί για την υπογραφή κάθε

είδους αρχείου, ανεξάρτητα από τα (ιδιωτικά) πρότυπα με τα οποία δημιουργήθηκε (Thompson, 2017).

4.10.2 Αρχιτεκτονική Ψηφιακών Πιστοποιητικών με ασφάλεια Blockchain

Στην περίπτωση πιστοποιήσεων, το blockchain διατηρεί έναν κατάλογο με τον εκδότη και τον παραλήπτη κάθε πιστοποιητικού, μαζί με την υπογραφή εγγράφου (hash) σε μια δημόσια βάση δεδομένων που αποθηκεύεται πανομοιότυπα σε χιλιάδες υπολογιστές σε όλο τον κόσμο. Το ψηφιακό αρχείο που δημιουργείται περιέχει μερικές βασικές πληροφορίες, όπως το όνομα του εκδότη και του παραλήπτη, το όνομα του εκδότη (MIT Media Lab), ημερομηνία έκδοσης, το διαπιστευτήριο, το οποίο είναι δομημένο σύμφωνα με το πρότυπο IMS open beats, κ.λπ.. Ο εκδότης υπογράφει κρυπτογραφικά τα περιεχόμενα του πιστοποιητικού χρησιμοποιώντας ένα ιδιωτικό κλειδί στο οποίο έχει πρόσβαση μόνο ο εκδότης (Sudia & Siritzky, 2011). Στη συνέχεια, επισυνάπτει την υπογραφή αυτή στο ίδιο το πιστοποιητικό και δημιουργεί ένα κρυπτογραφικό hash του αρχείου διαπιστευτηρίων - μια σύντομη ακολουθία γραμμάτων και αριθμών που μπορούν να χρησιμοποιηθούν για να επαληθευτεί ότι κανείς δεν έχει παραποιήσει το περιεχόμενο του πιστοποιητικού. Όπως αναφέρθηκε προηγουμένως, υπάρχει ένας πιθανός συνδυασμός γραμμάτων και αριθμών που αντιστοιχεί σε ένα ψηφιακό αρχείο και οποιαδήποτε αλλαγή στο αρχείο θα είχε ως αποτέλεσμα διαφορετικό hash. Τέλος, ο εκδότης χρησιμοποιεί ξανά το ιδιωτικό του κλειδί για να δημιουργήσει μια εγγραφή στο blockchain του Bitcoin που δηλώνει ότι εκδόθηκε ένα συγκεκριμένο πιστοποιητικό σε ένα συγκεκριμένο άτομο σε μια συγκεκριμένη ημερομηνία (Grätheretal., 2018).

Τα ίδια τα ψηφιακά διαπιστευτήρια μπορούν να αποθηκευτούν από έναν χρήστη σε έναν σκληρό δίσκο ή σε ένα κινητό πορτοφόλι (mobile wallet) από όπου μπορούν εύκολα να μοιραστούν με άλλους ή ακόμα και να εκτυπωθούν σε χαρτί. Είναι επομένως δυνατό για ένα χρήστη να επαληθεύσει για ποιον εκδόθηκε το πιστοποιητικό, από ποιον και να επικυρώσει το περιεχόμενο του ίδιου του πιστοποιητικού. Τα δεδομένα που απαιτούνται για την επαλήθευση της ακεραιότητας και της αυθεντικότητας ενός πιστοποιητικού αποθηκεύονται σε blockchain. Για παράδειγμα, προκειμένου να επικυρωθούν τα διαπιστευτήρια, ο εργοδότης (ή μια εταιρεία που προσφέρει υπηρεσίες επαλήθευσης) θα ακολουθήσει ουσιαστικά την παραπάνω διαδικασία προς τα πίσω για να διασφαλίσει ότι ο κατακερματισμός αντιστοιχεί στον αρχικό φάκελο και ότι τα

κλειδιά που χρησιμοποιεί ο εκδότης οδηγούν πίσω στο σωστό ίδρυμα (Shrier, Wu & Pentland, 2016). Όταν χρησιμοποιείται ένα μη εξουσιοδοτημένο (ή δημόσιο) blockchain που εκδίδει ή λαμβάνει πιστοποιητικά, αυτό σημαίνει ότι ο καθένας μπορεί να το χρησιμοποιήσει για να διασφαλίσει ότι οι υπογραφές και ο μηχανισμός επαλήθευσης διατίθενται επ' αόριστον, εφόσον εκτελείται τουλάχιστον ένα αντίγραφο της βάσης δεδομένων. Η επαλήθευση γίνεται με τη σύγκριση του κατακερματισμού του εγγράφου που επαληθεύεται με τον καταγεγραμμένο κατακερματισμό στο blockchain. Εάν ταιριάζουν, το έγγραφο είναι αυθεντικό. Επίσης, αυτό σημαίνει ότι όποιος λαμβάνει ένα πιστοποιητικό που έχει υπογραφεί στο blockchain μπορεί να επαληθεύσει την αυθεντικότητά του, ακόμη και αν ο εκδότης του πιστοποιητικού δεν υπάρχει πλέον. Όπου χρησιμοποιείται εξουσιοδοτημένο (ή ιδιωτικό) blockchain, αυτό σημαίνει ότι μόνο τα άτομα στα οποία επιτρέπεται η πρόσβαση στο συγκεκριμένο δίκτυο blockchain θα μπορούν να εκδίδουν, να λαμβάνουν ή να επαληθεύουν τις υπογραφές στο blockchain (Won & Bollella, 2019).

4.10.3 Αυτοκυριαρχικές ταυτότητες με χρήση της τεχνολογίας Blockchain

Διάφορα νέα μοντέλα αναγνώρισης παρουσιάζονται, αν και οι επιπτώσεις τους δεν είναι απαραιτήτως σαφείς αυτή τη στιγμή. Το μοντέλο ενός μοναδικού πιστοποιητικού που εκδόθηκε από το κράτος εξελίχθηκε σε μια ενισχυμένη και δικτυωμένη προσέγγιση που χρησιμοποιεί ως εκκίνηση την πιστοποίηση που εκδόθηκε από το κράτος. Τώρα η τρέχουσα εξέλιξη αφορά συγκέντρωση χαρακτηριστικών ταυτότητας που βασίζονται στη γνώση, συχνά πολύ περισσότερο υπό τον έλεγχο του χρήστη. Αυτό περιλαμβάνει πράγματα όπως τα αποτελέσματα από τα κοινωνικά μέσα, την κοινή χρήση peer-to-peer και τις πλατφόρμες οικονομίας (Ølnes, 2016). Όπως και με τις ψηφιακές υπογραφές, σε ένα σύστημα αυτοκυρίαρχης ταυτότητας βασισμένο σε blockchain, ένα άτομο αναγνωρίζεται από το δημόσιο κλειδί. Με αυτόν τον τρόπο, το άτομο αποδεικνύει ότι είναι ο ιδιοκτήτης του δημόσιου κλειδιού εισάγοντας το μυστικό ιδιωτικό κλειδί τους. Στα περισσότερα συστήματα αυτοκυρίαρχης ταυτότητας, αυτό το ιδιωτικό κλειδί συνδέεται με ένα κομμάτι βιομετρικών αναγνωρίσιμων πληροφοριών, όπως ένα δακτυλικό αποτύπωμα. Για να δημιουργήσει την αυτο-κυρίαρχη ταυτότητα, το άτομο πρέπει απλώς να καταχωρήσει τις προσωπικές του πληροφορίες και να το συσχετίσει με το δημόσιο κλειδί του. Αυτό γίνεται με τη χρήση του προσαρμοσμένου λογισμικού, το οποίο κατά κανόνα υπάρχει στο smartphone του, στο

οποίο μπορεί να συνδεθεί χρησιμοποιώντας το ιδιωτικό κλειδί/βιομετρικό δεδομένο. Το λογισμικό κρυπτογραφεί τα προσωπικά του δεδομένα στη συσκευή και μεταφορτώνει ένα hash των πληροφοριών αυτών σε ένα blockchain (Baars, 2016).

4.10.4 Πιστοποίηση αυτοκυρίαρχης ταυτότητας

Σε περίπτωση που κάποιος τρίτος πρέπει να πιστοποιήσει ότι τα δεδομένα ενός ατόμου είναι αληθή, θα έπρεπε να απαιτεί από το άτομο να μοιραστεί τα εν λόγω δεδομένα, καθώς και να ζητάει τα αποδεικτικά στοιχεία ότι τα δεδομένα αυτά είναι αληθή. Μετά την επαλήθευση των δεδομένων, ο τρίτος θα μπορούσε να εκδώσει ένα πιστοποιητικό που να βεβαιώνει ότι οι πληροφορίες είναι αληθείς με μια δήλωση όπως "Βεβαιώνω ότι οι πληροφορίες με αυτό το hash είναι αληθείς". Εάν αυτή η δήλωση μεταφορτωθεί σε ένα blockchain, παρέχει δημόσια βεβαίωση ότι τα στοιχεία ταυτότητας του ατόμου είναι αληθινά, χωρίς να χρειάζεται να αποκαλύπτονται πληροφορίες σχετικά με το άτομο, εκτός από το δημόσιο κλειδί του. Συνεπώς, για να συνεχίσουμε το παράδειγμα της ενότητας 4.6, αν ο υποψήφιος πανεπιστημίου επιθυμούσε να λάβει υποτροφία, το γραφείο υποδοχής θα ζητούσε ενδεχομένως την απόδειξη της ταυτότητάς του με τη μορφή διαβατηρίου ή πιστοποιητικού γέννησης, αποδεικτικά βαθμολογίας και οικονομικής κατάστασης. Εάν το γραφείο υποδοχής, αφού ελέγξει αυτές τις πληροφορίες, τις θεωρήσει επαρκείς, μπορεί να εκδώσει πιστοποιητικό που δηλώνει ότι το άτομο δικαιούται υποτροφία. Το hash αυτού του πιστοποιητικού μπορεί με τη σειρά του να αποθηκευτεί στο blockchain, ενώ το ίδιο το πιστοποιητικό μπορεί να αποθηκευτεί στο άτομο (Coelho, Zúquete & Gomes, 2018).

4.11 Εφαρμογές της Τεχνολογίας Blockchain στην Εκπαίδευση

Το Blockchain είναι μια τεχνολογία που έχει σαφώς εφαρμογές στον χώρο της εκπαίδευσης σε ατομικό, θεσμικό, ομαδικό, εθνικό και διεθνές επίπεδο. Είναι συναφές σε όλα τα είδη των περιπτώσεων: σχολεία, κολέγια, πανεπιστήμια, ΜΚΟ, CPD, επιχειρήσεις, μαθητείες και βάσεις γνώσεων. Αντί των παλαιών ιεραρχικών δομών, η τεχνολογία γίνεται το επίκεντρο, με την αξιοπιστία να μεταναστεύει προς την τεχνολογία και όχι στα θεσμικά όργανα. Είναι πραγματικά μια τεχνολογία χωρίς μεσολαβητές. Τα ψηφιακά έγγραφα του Donald Clark μπορούν να είναι εξίσου εφήμερα με το χαρτί. Αυτά, επειδή συχνά εκδίδονται σε ιδιωτικές μορφές από πωλητές σε

πελάτες, τα ιδρύματα χωρίς το σωστό λογισμικό ενδέχεται να μην μπορούν να τα διαβάσουν ή να τα επαληθεύσουν. Ακόμη και με την πρόσβαση στο σωστό λογισμικό, σε πολλές περιπτώσεις, η διαδικασία επαλήθευσης μπορεί να είναι κουραστική και αβέβαιη (Baars, 2016). Το ίδιο ισχύει και για τις ψηφιακές υπογραφές: ακόμη και σε μέρη που η νομοθεσία έχει επιβάλει την αποδοχή τους, οι ψηφιακές υπογραφές εισάγονται σε μια ευρεία ποικιλία μορφών με ποικίλα επίπεδα ασφάλειας, τα οποία δεν είναι όλα αποδεκτά ως νομική απόδειξη. Μια άλλη πρόκληση με ψηφιακά έγγραφα είναι ότι ένας από τους πρωταρχικούς τρόπους που οι άνθρωποι μοιράζονται πληροφορίες ψηφιακά (ηλεκτρονικό ταχυδρομείο) δεν είναι συνήθως ασφαλής, επομένως πρέπει να δημιουργηθούν ιδιωτικές υποδομές μεταφοράς για την αποστολή ευαίσθητων εγγράφων, όπως τα αρχεία υγείας. Αυτό βελτιώνει σημαντικά την ασφάλεια των ταχυδρομικών αποστολών, αλλά αυξάνει τους πονοκεφάλους διαλειτουργικότητας. Τέλος, όπως τα έντυπα έγγραφα, τα ψηφιακά έγγραφα μπορούν επίσης να παραποιούνται από προχωρημένους χρήστες με τρόπους που είναι δύσκολο να εντοπιστούν (Albeanu, 2017).

4.11.1 Έκδοση Πιστοποιητικών

Όταν χρησιμοποιείται η τεχνολογία blockchain στην έκδοση πιστοποιητικών, υπάρχει η δυνατότητα όχι μόνο να επαληθεύονται τα διαπιστευτήρια χωρίς διαμεσολαβητή αλλά και να εμπλουτίζεται και να προστίθεται αξία στο ήδη υπάρχον οικοσύστημα ψηφιακής πιστοποίησης. Τα BADGR και Mozilla Open Badge χρησιμοποιούνται ήδη για την παροχή ψηφιακών πιστοποιήσεων για φοιτητές σε ορισμένα αναγνωρισμένα ακαδημαϊκά ιδρύματα. Ο στόχος της επικύρωσης πιστοποιητικών σε ένα blockchain είναι, συνεπώς, να μετατραπεί το ψηφιακό πιστοποιητικό, που ένας φοιτητής συνήθως δέχεται ιδιωτικά, σε μια αυτόματα επαληθεύσιμη πληροφορία που μπορεί να συμβουλευτεί ένας τρίτος μέσω ενός αμετάβλητου συστήματος αποδείξεων σε ένα δημόσιο Blockchain. Στην τρέχουσα πρακτική, η πρόσβαση σε μια δημόσια πλατφόρμα απαιτεί σχεδόν αναπόφευκτα από έναν φοιτητή να μοιράζεται ή να αποκαλύπτει «ευαίσθητα» μεταδεδομένα, τα οποία τείνουν να περιλαμβάνουν ιδιωτικές πληροφορίες (Kamišalić, Turkanović, Mrdović & Heričko, 2019). Με τη χρήση ενός blockchain ως «απόδειξη της γνώσης», αυτές οι ιδιωτικές πληροφορίες δεν είναι απαραίτητο να αποκαλυφθούν κατά τη διάρκεια δημοσίευσης των μεταδεδομένων που σχετίζονται με τις πιστοποιήσεις. Βραχυπρόθεσμα, είναι πιθανό οι φοιτητές να μπορούν να προσεγγίσουν ακαδημαϊκά ιδρύματα και

εργοδότες διατηρώντας παράλληλα ένα διακριτικό επίπεδο εμπιστευτικότητας. Καταρχήν, μόνο οι πληροφορίες που οι φοιτητές θα χαρακτηρίζουν ως δημόσιες κατά τη διάρκεια της διαδικασίας δημιουργίας αποδεικτικών στοιχείων θα είναι προσβάσιμες σε τρίτους συμβαλλόμενα μέρη. Σύμφωνα με μελέτες, υπάρχουν ευκαιρίες για οργανώσεις λογισμικού που μπορούν να διευκολύνουν και να απλοποιήσουν τη διαδικασία πρόσβασης στο Blockchain για φοιτητές και φορείς (ινστιτούτα, εταιρείες, σχολεία κλπ.) (Albeanu, 2017). Ιδανικά, οι εφαρμογές θα κατασκευαστούν σε μια αρχιτεκτονική open source, η οποία θα εγγυάται τη συνέχεια των δεδομένων των εκπαιδευτικών αποτελεσμάτων ισόβια και χωρίς δέσμευση κλειδώματος με μία συγκεκριμένη λύση. Τα ακαδημαϊκά ιδρύματα και οι εταιρείες δεν θα είναι τα μόνα που θα επωφεληθούν από την υπευθυνότητα και τη σταθερότητα των πληροφοριών που είναι διαθέσιμες στην πλατφόρμα και στο Blockchain. Οι φοιτητές με τη σειρά τους θα μπορούν να χρησιμοποιήσουν τα δημόσια μεταδεδομένα για να αναζητήσουν παρόμοια προφίλ και, εν προκειμένω, να προωθήσουν τη δημιουργία νέων μοντέλων κοινωνικής ένταξης και επιχειρηματικότητας. Όλα αυτά χωρίς την ανάγκη μιας κεντρικής αρχής που εγγυάται την εγκυρότητα των πληροφοριών (Coelho, Zúquete & Gomes, 2018).

4.12 Blockcerts: Ένα ανοικτό πρότυπο για πιστοποιητικά σπουδών με τη χρήση Blockchain

Ο ακρογωνιαίος λίθος του ανοιχτού προτύπου Blockcerts είναι η πεποίθηση ότι οι άνθρωποι πρέπει να είναι σε θέση να κατέχουν και να αποδεικνύουν την ιδιοκτησία των σημαντικών ψηφιακών τους αρχείων. Αυτά τα αρχεία αποτελούν τη βάση για την απόδειξη πτυχών του εαυτού μας, σύμφωνα με τις αρχές της αυτο-κυρίαρχης ταυτότητας. Στο πλαίσιο αυτό, το Blockchain θεωρείται ότι είναι μια τεχνολογία που επιτρέπει στα άτομα να κατέχουν τα επίσημα αρχεία τους και να τα μοιράζονται με οποιονδήποτε τρίτο για άμεση επαλήθευση, απαγορεύοντας κάθε προσπάθεια να παραβιάζονται ή να γίνονται αντικείμενο επεξεργασίας (Turcu, Turcu & Chiuchisan, 2019). Το MIT Media Lab και η Learning Machine, προμηθευτής λογισμικού για επιχειρήσεις, έχουν αναπτύξει το ανοικτό πρότυπο Blockcerts για την έκδοση και επαλήθευση των διαπιστευτηρίων στο Bitcoin blockchain. Το Blockcerts είναι σήμερα το μόνο ανοιχτό πρότυπο για την έκδοση και την επαλήθευση αρχείων σχετικά με το blockchain και στόχος της κοινότητας Blockcerts είναι να προωθήσει την υιοθέτησή του ως κύριου παγκόσμιου προτύπου (στο πλαίσιο

της κοινωνικής υιοθεσίας) για την έκδοση αρχείων στο blockchain. Το πρότυπο επιτρέπει σε κάθε χρήστη, συμπεριλαμβανομένων των εκπαιδευτικών ιδρυμάτων και των κυβερνήσεων, να χρησιμοποιούν τον βασικό κώδικα και να αναπτύσσουν το δικό τους λογισμικό για έκδοση και επαλήθευση. Το Blockcerts είναι δωρεάν και διαθέσιμο για οποιονδήποτε χωρίς πίστωση ή δικαιώματα για τους βασικούς προγραμματιστές του. Από τη σάρωση του κοινοτικού φόρουμ Blockcerts, είναι σαφές ότι πολλές οργανώσεις, νεοσύστατες επιχειρήσεις και άτομα σε όλο τον κόσμο το χρησιμοποιούν για την ανάπτυξη εφαρμογών (Williams, 2019). Το Blockcerts παρέχεται επίσης δωρεάν για χρήστες που έχουν την εφαρμογή και το πορτοφόλι Blockcerts τόσο σε λογισμικό iOS όσο και σε Android. Ο κώδικας του είναι επίσης εντελώς ανοιχτός. Ο σκοπός της δημιουργίας ανοιχτού κώδικα Blockcerts ήταν να αποφευχθούν η διαμάχη προτύπων και οι δεσμεύσεις από προμηθευτές, τα οποία θεωρήθηκαν από τους προγραμματιστές ως δύο βασικά εμπόδια στην εύκολη διαλειτουργικότητα και την ευρεία υιοθέτηση που είναι απαραίτητες προϋποθέσεις για την πραγματική αποδέσμευση των επίσημων αρχείων (Juričić, Radošević & Fuzul, 2019). Τα δεδομένα που παγιδεύονται σε σιλό είναι το status quo και θεωρούνται από την κοινότητα Blockcerts ως μια σημαντική πρόκληση την οποία μπορεί να δεχτεί το blockchain. Έρευνες υποστηρίζουν ότι το Blockcerts ρυθμίζει το προηγούμενο για ένα κινητό πορτοφόλι που πληροί τα πιο σημαντικά κριτήρια της ψηφιακής αυτοκυριαρχίας: την ιδιοκτησία του κατόχου και την ανεξαρτησία του πωλητή. Στο πλαίσιο αυτό: - η ιδιοκτησία του κατόχου σημαίνει ότι τα άτομα ελέγχουν τα ιδιωτικά κλειδιά που τους επιτρέπουν να επιδεικνύουν ιδιοκτησία των χρημάτων ή των ψηφιακών τους αρχείων. - η ανεξαρτησία του πωλητή σημαίνει ότι η πρόσβαση, η εμφάνιση και η επαλήθευση δεν βασίζονται σε κανένα συγκεκριμένο προμηθευτή. Όταν βασίζονται σε πρότυπα ανοιχτού κώδικα, τα αρχεία μπορούν επομένως να μεταφερθούν, να μοιραστούν και να επαληθευτούν ανεξάρτητα από οποιονδήποτε προμηθευτή. Ο συνδυασμός αυτών των δύο συνθηκών αναφέρεται ως ο μόνος τρόπος για να εξασφαλιστεί η ανεξαρτησία των προσωπικών δεδομένων (Kamišalić, Turkanović, Mrdović & Heričko, 2019).

Τα Blockcerts έχουν δημιουργηθεί για να παρέχουν ένα κοινό σύνολο μοτίβων έτσι ώστε τα διαπιστευτήρια να μπορούν να εκδίδονται και να επαληθεύονται σε οποιοδήποτε blockchain και σε διαφορετικούς τομείς της αγοράς. Σύμφωνα με τους κύριους προγραμματιστές που συμμετείχαν στην πρωτοβουλία, όταν ξεκίνησε η έρευνα, το 2015, το Bitcoin blockchain ήταν η εύλογη επιλογή για το βασικό blockchain στο οποίο στηρίχθηκαν στα δια βίου ψηφιακά αρχεία. Το 2016, υπήρξε κάποια συζήτηση για την επέκταση των πόρων στην Ethereum, αλλά η βασική

διακλάδωση (hardfork) του Ethereum εκείνη την περίοδο κατέστησε αναξιόπιστα τα διαπιστευτήρια που θα διαρκούσαν για μια ζωή (Williams, 2019). Η απόφαση που ελήφθη σε εκείνη τη φάση ήταν να καταστεί όσο το δυνατόν πιο χρήσιμη η τεκμηρίωση για το Bitcoin, παράλληλα με τη διατήρηση ανοιχτής της κάλυψης άλλων Blockchains στο μέλλον. Το 2017, η Ethereum είχε αποκτήσει σημαντική δυναμική με τους προγραμματιστές και πολλοί ζητούσαν τα Blockcerts να επεκτείνουν την τεκμηρίωση (και τις εφαρμογές αναφοράς) για να συμπεριλάβουν το Ethereum. Επομένως, εφόσον το Blockcerts είναι μια κοινότητα ανοιχτού κώδικα, αρκετοί προγραμματιστές συμβάλλουν στην υλοποίηση αυτής της επέκτασης. Η κοινότητα Blockcerts έρχεται σε συμφωνία (και συνεισφέρει) με τις ακόλουθες κοινότητες τυποποίησης: IMS Open Badges; W3C Verifiable Claims; W3C Linked Data Signatures και W3C/Rebooting Web of Trust Decentralised Identifiers. Το MIT, το Πανεπιστήμιο της Λευκωσίας και οι ερευνητές του Πανεπιστημίου του Μπέρμιγχαμ αναπτύσσουν τα δικά τους συστήματα χρησιμοποιώντας την ανοιχτή προδιαγραφή Blockcerts (Turcu, Turcu & Chiuchisan, 2019).

4.13 Μελέτες περίπτωσης εφαρμογής blockchain

4.13.1 Sony Global Education

Από το 2016, η Sony έχει ανακοινώσει ότι έχει αναπτύξει εσωτερικό σύστημα έκδοσης πιστοποιητικών που χρησιμοποιεί τεχνολογίες blockchain. Στις 10 Αυγούστου 2017, η Sony Corporation και η Sony Global Education (SGE) ανακοίνωσαν την ανάπτυξη ενός συστήματος που θα εφαρμόζει ειδικά την τεχνολογία blockchain στον τομέα της εκπαίδευσης. Το Δελτίο Τύπου αναφέρει ότι χρησιμοποιώντας “την τεχνολογία που κάνει κοινή χρήση των εκπαιδευτικών αποτελεσμάτων και των αρχείων με έναν ανοιχτό και ασφαλή τρόπο”, αυτό το αξιόπιστο σύστημα συγκεντρώνει τη διαχείριση των δεδομένων από πολλαπλά εκπαιδευτικά ιδρύματα και καθιστά δυνατή την καταγραφή και την αναφορά εκπαιδευτικών δεδομένων και ψηφιακών απομαγνητοφωνήσεων". Το σύστημα βασίζεται στο IBM Blockchain, το οποίο παρέχεται μέσω του IBM Cloud και υποστηρίζεται από το Hyperledger Fabric 1.0, που αποτελεί μια μορφή blockchain και ένα από τα πρότζεκτ Hyperledger που φιλοξενεί το Linux Foundation. Συγκεντρώνει 1) μια λειτουργία που πιστοποιεί και ελέγχει τα δικαιώματα χρήσης στα εκπαιδευτικά δεδομένα και 2) μια διασύνδεση προγραμματισμού εφαρμογών για τη διαχείριση

αυτών των δικαιωμάτων που απευθύνονται σε εκπαιδευτικά ιδρύματα. Το 2018, η Sony θα αρχίσει να αναπτύσσει τις δικές της προσφορές υπηρεσιών, ξεκινώντας με την Global Challenge Math Challenge, η οποία συγκεντρώνει 150.000 συμμετέχοντες από όλο τον κόσμο (Albeanu, 2017).

4.13.2 Uport

Το Uport είναι ένα ασφαλές, εύχρηστο σύστημα για αυτο-κυρίαρχη ταυτότητα που αναπτύχθηκε από την ConsenSys και κατασκευάστηκε από την Ethereum. Η τεχνολογία uPort αποτελείται από τρία βασικά στοιχεία: έξυπνες συμβάσεις, βιβλιοθήκες προγραμματιστών και μια εφαρμογή κινητού. Η εφαρμογή για κινητά διατηρεί τα κλειδιά του χρήστη. Οι έξυπνες συμβάσεις του Ethereum αποτελούν τον πυρήνα της ταυτότητας και περιέχουν λογική που επιτρέπει στον χρήστη να ανακτήσει την ταυτότητά του εάν χάσει την κινητή συσκευή του. Τέλος, οι βιβλιοθήκες προγραμματιστών είναι οι τρόποι με τους οποίους οι προγραμματιστές εφαρμογών τρίτων κατασκευαστών θα μπορούσαν να ενσωματώσουν την υποστήριξη για το uPort στις εφαρμογές τους. Οι ταυτότητες uPort μπορούν να λάβουν πολλές μορφές, όπως πρόσωπα, συσκευές, οντότητες ή ιδρύματα. Οι ταυτότητες Uport είναι αυτοκυρίαρχες, δηλαδή ανήκουν πλήρως και ελέγχονται από τον δημιουργό και δεν βασίζονται σε συγκεντρωτικά τρίτα μέρη για δημιουργία ή επικύρωση. Βασική λειτουργία της ταυτότητας uPort είναι ότι μπορεί να υπογράψει και να επαληθεύσει ψηφιακά ένα δικαίωμα, ενέργεια ή συναλλαγή - η οποία καλύπτει ένα ευρύ φάσμα περιπτώσεων. Η ταυτότητα μπορεί να συνδέεται κρυπτογραφικά με αποθήκες δεδομένων εκτός αλυσίδας. Κάθε ταυτότητα είναι ικανή να αποθηκεύει το hash μιας χαρακτηριστικής μάζας δεδομένων, όπως σε IPFS, Azure, AWS, Dropbox, κλπ., όπου όλα τα δεδομένα που σχετίζονται με την ταυτότητα αυτή αποθηκεύονται με ασφάλεια. Οι ταυτότητες είναι σε θέση να ενημερώνουν το ίδιο το αρχείο, όπως η προσθήκη μιας φωτογραφίας προφίλ ή ενός φίλου, ή μπορούν επίσης να παραχωρήσουν σε τρίτους προσωρινή άδεια για ανάγνωση ή εγγραφή συγκεκριμένων αρχείων. Δεδομένου ότι μπορούν να αλληλοεπιδρούν με blockchain, οι ταυτότητες του uPort μπορούν επίσης να ελέγχουν τα στοιχεία του ψηφιακού κομιστή, όπως οι κρυπτοσυχνότητες ή άλλα τεκμηριωμένα στοιχεία (Jacobovitz, 2016).

4.13.3 Open University UK

Το KMI στο Open University (OU) ασχολείται με διάφορες ερευνητικές πρωτοβουλίες Blockchain. Αυτό το ερευνητικό ενδιαφέρον βασίζεται κυρίως στο ενδιαφέρον για την επόμενη γενιά του διαδικτύου, των μέσων ενημέρωσης, της αυξημένης πραγματικότητας, των έξυπνων πόλεων και των αναλυτικών στοιχείων: το OU είναι ο επικεφαλής της Learning Analytics στο Ηνωμένο Βασίλειο. Στο πλαίσιο της έρευνας και της διαπίστευσης αποκλεισμού, η KMI ενδιαφέρεται ιδιαίτερα για την αύξηση των προτύπων για αναγνωριστικό σήμα (badging), πιστοποίηση και φήμη στο διαδίκτυο με τη χρήση του blockchain ως αξιόπιστου επικεφαλής. Σύμφωνα με τον καθηγητή Domingue, ήταν φυσική εξέλιξη να ενσωματωθούν ανοιχτά αναγνωριστικά (badges) στο πλαίσιο του πρότζεκτ με blockchain και να διεξαχθεί έρευνα σχετικά με τη μικρο-διαπίστευση και τα ηλεκτρονικά χαρτοφυλάκια. Το KMI αξιοποιεί το δυναμικό της Ethereum για διαπίστευση προκειμένου να μετατρέψει τα αναγνωριστικά σε έξυπνα συμβόλαια και να αναπτύξει ένα πρότυπο για τη συγκέντρωση και την έκδοση μικροπιστωτικών στοιχείων σε ένα blockchain. Το OU, με περισσότερους από 170.000 φοιτητές, τη δική του πλατφόρμα MOOC (FutureLearn) και την πλατφόρμα της Open Learn (με περισσότερους από 5 εκατομμύρια επισκέπτες το χρόνο και 8 χιλιάδες ώρες εργασίας) έδωσε στο KMI την ευκαιρία να αναγνωρίσει όλα τα μαθήματα του OU στο blockchain. Η στρατηγική blockchain του KMI είναι ολιστική, με τους ερευνητές να ενθαρρύνονται να διερευνήσουν το πλήρες δυναμικό της τεχνολογίας σε αντίθεση με μια συγκεκριμένη πτυχή (όπως η κρυπτογραφία). Ο καθηγητής Domingue το εξισώνει με τις πρώτες μέρες του κινηματογράφου: "Χρειάστηκαν αιώνες για τις κινούμενες εικόνες να γίνουν κινηματογράφος, επειδή οι άνθρωποι ενδιαφέρονται μόνο για τη μαγνητοσκόπηση των παιχνιδιών!" (Sharplesetal., 2016)

4.13.4 Πανεπιστήμιο Λευκωσίας

Το Πανεπιστήμιο της Λευκωσίας (UNIC) έχει προβάλει μια σειρά «πρωταθλητών» στη δέσμευσή του να μεγιστοποιήσει τις δυνατότητες του blockchain στην εκπαίδευση. Το UNIC θεωρείται το πρώτο πανεπιστήμιο που δέχεται το Bitcoin για δίδακτρα για οποιοδήποτε πρόγραμμα σπουδών στο πανεπιστήμιο (Οκτώβριος 2013) και διδάσκει μάθημα κρυπτοαναλογιστικών σπουδών πανεπιστημιακού επιπέδου, το οποίο παραδόθηκε με MOOC και τίτλο «Εισαγωγή στα ψηφιακά

νομίσματα» (Ιανουάριος 2014). Επιπλέον, προσφέρει ένα διαπιστευμένο πανεπιστημιακό πτυχίο, Master of Science σε ψηφιακό νόμισμα, που διδάσκεται ηλεκτρονικά στα αγγλικά (Μάρτιος 2014 με τους πρώτους σπουδαστές να αποφοιτούν τον Ιούνιο του 2016). Τέλος, εκδίδει ακαδημαϊκά πιστοποιητικά στο Bitcoin blockchain, χρησιμοποιώντας τη δική του πλατφόρμα λογισμικού (Σεπτέμβριος 2014). Σύμφωνα με τον Αντώνη Πολεμητή, Διευθύνοντα Σύμβουλο του UNIC στις ASU GSV Summit το 2017 και τους συντονιστές της Πρωτοβουλίας Blockchain, καθηγήτρια Soulla Louca και καθηγητή George Giaglis, το UNIC θεωρεί την τεχνολογία Blockchain ως ακρογωνιαίο λίθο της στρατηγικής και στοιχείο διαφοροποίησης από άλλα ιδρύματα τριτοβάθμιας εκπαίδευσης. Παρόλο που το εισαγωγικό δωρεάν MOOC για τα ψηφιακά νομίσματα του UNIC δεν είναι μοναδικό, τοποθετείται ως το πρώτο μάθημα του MSc στο ψηφιακό νόμισμα. Οι συνιστώσες του MSc με τη σειρά τους επανασυγκεντρώνονται σε επαγγελματικά προγράμματα πιστοποίησης τύπου blockchain, τα οποία μεταφέρονται σε CPD και ECTS. Τον Σεπτέμβριο του 2017, ξεκίνησε η όγδοη έκδοση του MOOC. Μέχρι σήμερα, το MOOC έχει προσελκύσει σπουδαστές από 80 διαφορετικές χώρες και έχει δείξει καλά ποσοστά ολοκλήρωσης. Το περιεχόμενο του μαθήματος φιλοξενείται από το UNIC και συνεχίζει να εξελίσσεται λόγω της δικτύωσης του πανεπιστημίου στην παγκόσμια εκπαιδευτική κοινότητα. Το ερευνητικό κέντρο Blockchain τοποθετείται ως κέντρο παγκόσμιας κλάσης για τις αναδυόμενες τεχνολογίες, οι οποίες θα ενσωματώσουν, θα διευρύνουν το πεδίο εφαρμογής και θα ενισχύσουν την διεπιστημονική έρευνα που έχει ήδη πραγματοποιηθεί σε αυτόν τον εξελισσόμενο τομέα (Giaglis, 2018).

4.13.5 Openbadges

Το ζήτημα σχετικά με τα Openbadges πρέπει να ξεκινήσει με το πρόγραμμα Mozilla Open Badges (openbadges.org). Η αρχή του ήταν το 2011 από την Mozilla, με χρηματοδότηση από το Ίδρυμα MacArthur (2013). Στόχος του Open Badge Project ήταν να προχωρήσει το ψηφιακό αναγνωριστικό ένα βήμα παραπέρα. Το ανοικτό αναγνωριστικό βασίζεται σε ελεύθερο λογισμικό με ανοιχτό τεχνικό πρότυπο και, επομένως, μπορεί να υιοθετηθεί από οποιονδήποτε οργανισμό. Τα Openbadges δεν είναι απλώς ένα εικονίδιο. Πίσω από τα Openbadges υπάρχουν σημαντικές πληροφορίες σχετικά με τα διαπιστευτήρια και συχνά παραδείγματα της εργασίας που πραγματοποιήθηκε προκειμένου να επιτευχθεί το αναγνωριστικό. Η ιδέα πίσω από τα Openbadges

είναι ότι οι εκπαιδευόμενοι μπορούν να επιτύχουν αναγνωριστικά από μια ποικιλία οργανισμών και μπορούν να εντάξουν τις επιτυχίες τους σε ένα ενιαίο ψηφιακό "σάκο" (backpack). Στη συνέχεια μπορούν να αποθηκεύσουν και να εμφανίσουν τα διακριτικά τους σε έναν προσωπικό ιστότοπο ή σε έναν ιστότοπο όπως το LinkedIn (Devedžić & Jovanović, 2015). Το κλειδί για την έννοια των Openbadges είναι ότι αυτό δεν ελέγχεται από οποιαδήποτε οργάνωση αλλά μόνο ο χρήστης έχει τον έλεγχο. Επίσης, σε αντίθεση με ένα ψηφιακό αναγνωριστικό, το οποίο τυπικά είναι μόνο μια ηλεκτρονική εικόνα, το ανοιχτό αναγνωριστικό βασίζεται σε αποδείξεις ολοκλήρωσης και η απόδειξη του ατόμου συνδέεται με το αναγνωριστικό ή θεωρείται "ψημένο" (baked). Ο όρος "ψημένο" προέρχεται από το ψημένο κέικ, που, μόλις ψηθεί, τα συστατικά δεν μπορούν πλέον να διαχωριστούν από το αναγνωριστικό. Η baked πτυχή αποσκοπεί στη βελτίωση της νομιμότητας του αναγνωριστικού. Τα ανοικτά αναγνωριστικά μπορούν επίσης να στοιβαχτούν και να μεταβιβαστούν. Αυτό σημαίνει ότι τα αναγνωριστικά μπορούν να χτιστούν το ένα πάνω από το άλλο, οπότε κάποιος δεν μπορεί να ολοκληρώσει το δεύτερο αναγνωριστικό προτού να ολοκληρωθεί το θεμελιώδες. Το τελικό αναγνωριστικό μπορεί στη συνέχεια να επιβεβαιώσει ότι έχουν ολοκληρωθεί όλα τα αναγνωριστικά στη στοίβα (Holotescu, 2018).

Μέσω του προϊόντος της Acclaim, η Pearson επιτρέπει σε αναγνωρισμένες επωνυμίες να προωθούν τα μαθησιακά επιτεύγματα μέσω μιας τυποποιημένης και επαληθευμένης πλατφόρμας. Δύο σημαντικοί χρήστες της πλατφόρμας είναι το Open EdX[1] και το P2PU[2]. Το backpack Mozilla εξακολουθεί να υπάρχει και, πρόσφατα, η DigitalMe, μη κερδοσκοπικός οργανισμός, ανέλαβε την περαιτέρω ανάπτυξη του backpack για το Mozilla. Το DigitalMe[3] δεσμεύεται στον αρχικό κύριο στόχο του backpack Mozilla να παράσχει στους κατόχους αναγνωριστικών τη δυνατότητα να μεταφέρουν το αναγνωριστικό τους σε ένα ανοιχτό περιβάλλον που δεν συνδέεται με συγκεκριμένη εταιρεία. Επιπλέον, η Mozilla και το Ίδρυμα MacArthur προσχώρησαν στην IMS Global για να συνεχίσουν το πρότζεκτ ανοικτών αναγνωριστικών. Ο στόχος της IMS Global ήταν να συνεχίσει να εργάζεται για την ανάπτυξη ενός οικοσυστήματος που υποστηρίζει μια ανοικτή αρχιτεκτονική για την τεκμηρίωση της εκπαίδευσης από ένα ευρύ φάσμα πόρων. Από το 2017, η Mozilla αποχώρησε από το πρότζεκτ και τα πρότζεκτ που χρηματοδοτούνται από το MacArthur

[1] (https://open.edx.org)
[2] (https://badges.p2pu.org/en/about)
[3] (http://www.digitalme.co.uk/credly/)

έχουν λήξει. Η IMS Global έχει αναλάβει την ιστοσελίδα openbadges.org (Kuhmonen, Pöyry-Lassila & Seppälä, 2018).

Ένα ακόμα σημαντικό γεγονός συνέβη στις αρχές του 2017, η έκδοση του OpenBadges 2.0. Έρευνες έδειξαν ότι μια καταχώρηση blog του Ιουνίου 2017 παρέχει την καλύτερη μη τεχνική περιγραφή των αλλαγών. Η πιο σημαντική αλλαγή είναι η δυνατότητα προσθήκης περισσότερων πληροφοριών στο αναγνωριστικό, συμπεριλαμβανομένων γενικών πληροφοριών σχετικά με το σήμα (αναγνωρισμένο ως "τάξη" αναγνωριστικού), καθώς και τεκμηρίωσης που παρέχεται από τον εκπαιδευόμενο που υποστηρίζει τα κριτήρια του αναγνωριστικού (με τον όρο "ισχυρισμός"). Πολλές εταιρείες αναγνωριστικών που χρησιμοποιούν το backpack Mozilla έχουν μετακινηθεί σε αυτή τη νέα έκδοση (Hickey & Otto, 2017).

Τα ψηφιακά αναγνωριστικά έχουν γίνει δημοφιλή στην εξέλιξη των εκπαιδευτικών. Ένα παράδειγμα είναι το Νέο Τεχνολογικό Δίκτυο (NTN). Το μοντέλο NTN βασίζεται στη μάθηση βασισμένη στο πρόβλημα (PBL) και εστιάζει στη διδασκαλία και την αξιολόγηση των δεξιοτήτων του 21ου αιώνα, στη χρήση της τεχνολογίας στην τάξη και στη μοναδική κουλτούρα που δίνει στους μαθητές τη δυνατότητα να συνδέονται με το σχολείο τους και τους συνομηλίκους.

Ένας εκπαιδευτικός περιέγραψε την εμπειρία του ως εξής: “Για την απόκτηση της πιστοποίησης των εκπαιδευτικών του NTN, υπήρχαν 22 διδακτικές εμπειρίες που απαιτούσαν υποβολή αποδεικτικών στοιχείων. Η έγκριση βασίστηκε στην εφαρμογή από μέρους μου ή στην εφαρμογή της συγκεκριμένης πρακτικής PBL που απαιτούνταν για τη συγκεκριμένη διδακτική εμπειρία. Μετά την επιτυχία σε όλες τις διδακτικές εμπειρίες για ένα συγκεκριμένο αναγνωριστικό, ήταν εφικτή η απόκτηση του αναγνωριστικού. Αφού επέτυχα όλα τα αναγνωριστικά, έλαβα ειδοποίηση για την ιδιότητά μου ως αναγνωρισμένου καθηγητή NTN "(Bodoroff, 2016).

Ορισμένα πανεπιστήμια χρησιμοποιούν αναγνωριστικά σε περιορισμένη βάση στις αίθουσες διδασκαλίας. Το Κρατικό Πανεπιστήμιο του Κολοράντο χρησιμοποιεί ψηφιακά αναγνωριστικά για τρία προγράμματα: Foundations of 3D Printing, CSU Extension Certified Gardener Program and Integrated Sustainability Management Program (Online.colostate.edu, 2019). Οι φοιτητές λαμβάνουν αναγνωριστικά κατά την ολοκλήρωση κάθε σταδίου του προγράμματος και στη συνέχεια τελειώνουν με την απόκτηση ενός ανώτερου αναγνωριστικού. Άλλα πανεπιστήμια χρησιμοποιούν αναγνωριστικά για την ανάπτυξη του τμήματος. Το Πανεπιστήμιο Texas Wesleyan, για παράδειγμα, προσφέρει τρία επίπεδα αναγνωριστικών: ένα για την περάτωση

εργαστηρίου, ένα για την εφαρμογή αυτής της γνώσης, και το τελικό αναγνωριστικό για τη δυνατότητα διδασκαλίας αυτής της δεξιότητας σε ένα άλλο άτομο. Ορισμένα προγράμματα έχουν δοκιμαστεί με ψηφιακά αναγνωριστικά, μόνο για να καταργηθούν σταδιακά. Το UC Davis, το 2012, άρχισε να χρησιμοποιεί αναγνωριστικά ως μέρος του προγράμματός του για την αειφόρο γεωργία και τα συστήματα τροφίμων, αλλά από το 2014 σταμάτησε τη χρήση αναγνωριστικών. Δεν ήταν ξεκάθαρο τι οδήγησε αυτό το πρόγραμμα στην κατάργηση του αναγνωριστικού, αλλά ορισμένα πρότζεκτ αναγνωριστικών που υποστηρίχθηκαν από χρηματοδότηση καταργήθηκαν (Imsglobal.org, 2019).

Άλλα θεσμικά όργανα, ωστόσο, εξακολουθούν να δεσμεύονται με αναγνωριστικά. Το Carnegie Mellon διαθέτει ένα εκτεταμένο πρόγραμμα αναγνωριστικών για προγραμματισμό ηλεκτρονικών υπολογιστών (http://www.cs2n.org/certifications). Ο ιστότοπος αναφέρει: "Είτε είστε άτομο είτε εκπαιδευτικός, οποιοσδήποτε μπορεί να αποκτήσει πιστοποιητικά CS-STEM. Οι περισσότερες πιστοποιήσεις είναι διαθέσιμες για όλους και αυτο-ρυθμιζόμενες, μελετήστε με δική σας ευκολία. Κερδίστε αναγνωριστικά, καθώς μελετάτε τα μαθήματά σας και κάντε μια online εξέταση στο τέλος (Cs2n.org, 2019)."

Μια άλλη φυσιολογική χρήση ψηφιακών αναγνωριστικών αφορά τους νεότερους φοιτητές. Μετά το σχολείο, τα προγράμματα K-12 στη Βοστώνη και στο Providence παρέχουν ψηφιακά αναγνωριστικά για φοιτητές που πληρούν ορισμένα κριτήρια (Bostonbeyond.org, 2019). Τα αναγνωριστικά είναι: επικοινωνία, κριτική σκέψη, εμπλοκή στη μάθηση, επιμονή και ομαδική εργασία. Η προσφορά αναγνωριστικού σε νέους ενήλικες βοηθά τα άτομα να αποκτήσουν εμπιστοσύνη στις ικανότητές τους και είναι χρήσιμη για τα βιογραφικά προς δυνητικούς εργοδότες και κολέγια / πανεπιστήμια. Η πλατφόρμα Makewaves επικεντρώνεται στα αναγνωριστικά για τα παιδιά, προκειμένου να δημιουργηθεί ένα ασφαλές περιβάλλον για να μάθουν και να αλληλεπιδρούν. Μια από τις δραστηριότητες αυτές είναι η ενασχόληση με τον Σαίξπηρ, η συνεργασία με τον Διεθνή Διαστημικό Σταθμό, οι γραφικές τέχνες και διάφορα άλλα θέματα. Οι εκπαιδευτικοί μπορούν να χρησιμοποιήσουν αυτήν την πλατφόρμα για να παρακολουθήσουν την πρόοδο των μαθητών και να επιδείξουν εξαιρετικές δεξιότητες των φοιτητών (Makewav.es, 2019). Το Penn State προσφέρει ψηφιακά αναγνωριστικά εγγραμματισμού. Αυτά συνδέονται με την ταξινόμηση του Bloom. Είναι διαθέσιμα εκτός κολλεγίων μέσω του λογαριασμού Google, Twitter ή Facebook (Stubbs, 2019).

Οι εταιρείες και οι βιομηχανίες έχουν επίσης υιοθετήσει ανοιχτά αναγνωριστικά. Η Εθνική Ένωση Ξύλινων Δαπέδων έχει αναπτύξει αναγνωριστικά, χρησιμοποιώντας την Credly, για το online πρόγραμμα κατάρτισης. Η IBM έχει επιβραβεύσει το πρόγραμμα Open Badges, το οποίο ξεκίνησε το 2015 και βασίζεται σε παιχνίδια. Τα αποτελέσματα ήταν εντυπωσιακά. Παρατηρήθηκε: 125% αύξηση των νέων συμμετεχόντων, αύξηση κατά 226% των ποσοστών ολοκλήρωσης του μαθήματος, 694% αύξηση στα ποσοστά επιτυχίας σε εξετάσεις και αύξηση κατά 64% στις λήψεις δοκιμαστικών προϊόντων (Bratcher, 2019).

Κεφάλαιο 5: Συμπεράσματα

5.1 Πλεονεκτήματα έκδοσης ψηφιακών πιστοποιητικών μέσω της τεχνολογίας blockchain

Η τεχνολογία Blockchain έχει τη δυνατότητα να επιταχύνει την κατάργηση του συστήματος των έντυπων πιστοποιητικών. Μέχρι τώρα, η υιοθέτηση ψηφιακών πιστοποιητικών έχει ανασταλεί λόγω της ευκολίας με την οποία μπορούν να πλαστογραφηθούν. Το blockchain παρέχει στους οργανισμούς τη δυνατότητα να εκδίδουν αμετάβλητα ψηφιακά πιστοποιητικά με διαρκή ισχύ, καθώς η αυθεντικότητά τους μπορεί να επαληθευθεί με βάση το blockchain. Στις περιπτώσεις που τα πιστοποιητικά μεταφέρονται ως διακριτικά σύμβολα (token) στο blockchain, αυτά τα πιστοποιητικά μπορούν να είναι διαθέσιμα συνεχώς. Τα πλεονεκτήματα αυτά σε σχέση με τα υπάρχοντα συστήματα αυξάνουν σημαντικά την αξία των ψηφιακών πιστοποιητικών και πιθανότατα να μπορούν να προωθήσουν την ψηφιακή πιστοποίηση στο mainstream (Baars, 2016). Η τεχνολογία Blockchain καταργεί το καθεστώς των εκπαιδευτικών οργανισμών να επικυρώνουν τα διαπιστευτήρια. Δεδομένου ότι τα πιστοποιητικά που εκδίδονται στο blockchain μπορούν να επαληθευτούν αυτόματα, οι εκπαιδευτικοί οργανισμοί δεν θα χρειάζεται πλέον να διαθέτουν πόρους για αυτή την ανάγκη, μειώνοντας σημαντικά το διοικητικό τους φορτίο και ουσιαστικά εξαλείφοντας την υποστήριξη μετά την πώληση (after-sales support), την οποία πρέπει να παρέχουν στους φοιτητές μετά το πέρας των μαθημάτων. Ωστόσο, δεδομένου ότι πολλές οργανώσεις προσφέρουν αυτή την υπηρεσία κερδοσκοπικά, τα ιδρύματα θα πρέπει να προσαρμόσουν ανάλογα τα επιχειρηματικά τους μοντέλα. Το Blockchain έχει τη δυνατότητα να παρουσιάσει ένα κύμα καινοτομίας γύρω από τα δεδομένα των εκπαιδευομένων. Τα δεδομένα των φοιτητών αποτελούν κρίσιμη συνιστώσα πολλών εφαρμογών, συμπεριλαμβανομένων των συστημάτων διαχείρισης ανθρώπινων πόρων, των εκθέσεων και των επαγγελματικών κοινωνικών δικτύων (Alammary, Alhazmi, Almasri & Gillani, 2019). Η τεχνολογία Blockchain επιτρέπει σε όλα αυτά τα συστήματα να επικυρώνουν αυτόματα πιστοποιητικά από οποιονδήποτε εκδότη σε οποιαδήποτε μορφή (μεταδεδομένων). Αυτή η δυνατότητα αποθήκευσης επαληθευμένων στοιχείων και όχι απλών στοιχείων, θα πρέπει να ενισχύσει σημαντικά τη χρησιμότητα τέτοιων συστημάτων στους διάφορους ενδιαφερόμενους. Μπορεί κανείς να σκεφτεί εφαρμογές που επαληθεύουν αυτόματα βιογραφικά σημειώματα, συγκεντρώνουν τους υποψηφίους με τα

κατάλληλα προσόντα και άλλες εφαρμογές που θα κατέτασσαν αυτόματα τους υπαλλήλους σε υψηλότερο εισόδημα με βάση τα στοιχεία των ολοκληρωμένων εκπαιδευτικών και επαγγελματικών δικτύων (Shrier, Wu & Pentland, 2016).

Αμέτρητες άλλες ιδέες είναι πιθανό να σκεφτεί κανείς από τις νεοσύστατες επιχειρήσεις και τις καθιερωμένες εταιρείες που εργάζονται στον τομέα αυτόν. Οι αυτοκυρίαρχες ταυτότητες έχουν τη δυνατότητα να μειώσουν σημαντικά το κόστος διαχείρισης των δεδομένων των εκπαιδευτικών οργανισμών. Το ευρωπαϊκό δίκαιο επιβάλλει σημαντικές υποχρεώσεις στις οργανώσεις που λειτουργούν ως φύλακες προσωπικών δεδομένων, καθώς είναι υποχρεωμένες να ελέγχουν ποιος έχει πρόσβαση σε αυτά μέσα σε έναν οργανισμό και να εξασφαλίζουν την ασφαλή αποθήκευση σε αυτόν τον οργανισμό. Όσο περισσότεροι άνθρωποι έχουν πρόσβαση στα δεδομένα, τόσο πιο σύνθετη είναι η διαχείριση, τόσο υψηλότερο είναι το κόστος και τόσο μεγαλύτερος είναι ο κίνδυνος παραβίασης ή κατάχρησης δεδομένων. Οι αυτοκυρίαρχες ταυτότητες δημιουργούν αποτελεσματικά ένα ασφαλές δελτίο ταυτότητας το οποίο μπορεί να κατέχει ένας φοιτητής και το οποίο μπορεί να συνδέεται βιομετρικά με αυτόν, επιτρέποντας στον σπουδαστή να αναγνωρίζεται χωρίς να προσκομίζει πραγματικά δεδομένα και χωρίς να διαβιβάζει δεδομένα από τη βάση δεδομένων που κατέχει το ίδρυμα. Το ίδρυμα θα είναι σε θέση να ταυτοποιήσει τον σπουδαστή χωρίς να κατέχει και χωρίς να διατηρεί τα δεδομένα του. Αυτό μειώνει σημαντικά τα διοικητικά έξοδα, καθώς και το δυνητικό "αποτύπωμα" για παραβίαση ή κατάχρηση δεδομένων (Hanetal., 2018).

Η τεχνολογία Blockchain επιτρέπει πολύ πιο εξελιγμένα συστήματα για αξιόπιστη παρακολούθηση της χρήσης της πνευματικής ιδιοκτησίας. Επίσης, έχει τη δυνατότητα να φέρει επανάσταση στη διαχείριση της πνευματικής ιδιοκτησίας. Ανάλογα με τις πολιτικές επιλογές, θα μπορούσε να χρησιμοποιηθεί για να διευρύνει ή να περιορίσει την πνευματική ιδιοκτησία. Με την έκδοση hash των εγγράφων σε ένα blockchain, ένα άτομο μπορεί να αποδείξει την πρώτη δημοσίευση χωρίς να χρειάζεται να κοινοποιήσει το έγγραφο ή το προϊόν που δημοσιεύεται. Αυτό αλλάζει τις συμβατικές έννοιες του δικαιώματος πνευματικής ιδιοκτησίας και του νόμου για τα διπλώματα ευρεσιτεχνίας, παρέχοντας τη δυνατότητα ενός πολύ πιο περιοριστικού συστήματος, σύμφωνα με το οποίο η γνώση θα μπορούσε να προστατευθεί χωρίς να μοιραστεί. Η τεχνολογία Blockchain επιτρέπει, επίσης, λεπτομερή και αυξανόμενη παρακολούθηση του ατόμου που έχει χρησιμοποιήσει την πνευματική ιδιοκτησία, του τόπου και του τρόπου με τον οποίο θα συνδεθεί με την πίστωση είτε με τη μορφή πληρωμής είτε με τη μορφή ακαδημαϊκής πίστωσης. Τέτοια

συστήματα πνευματικής ιδιοκτησίας θα μπορούσαν, για παράδειγμα, να χρησιμεύσουν ως βάση για μελλοντικά περιοδικά ή ακόμη και ως βάση για την παρακολούθηση της παραγωγής και της επαναχρησιμοποίησης ανοικτών εκπαιδευτικών πόρων. Ως εκ τούτου, θα είναι σε θέση να ενθαρρύνουν σημαντικά την πρόσβαση στην εκπαίδευση και σε εκπαιδευτικούς πόρους (Zhengetal., 2017).

5.2. Προτάσεις για το μέλλον

Οι υπεύθυνοι χάραξης πολιτικής θα πρέπει να εξετάσουν το ενδεχόμενο να διερευνήσουν και να υποστηρίξουν την εφαρμογή της τεχνολογίας blockchain σε συγκεκριμένες περιπτώσεις εκπαιδευτικής χρήσης. Αξίζει να αναφερθούν οι σημαντικές δυνατότητες του blockchain σε τομείς όπως η έκδοση πιστοποιητικών, η επαλήθευση των οδών διαπίστευσης, τα διαβατήρια για δια βίου μάθηση, η διαχείριση πνευματικής ιδιοκτησίας και η διαχείριση δεδομένων, καθώς και η ανάπτυξη εφαρμογών για την αντιμετώπιση αυτών προβλημάτων, ώστε να μελετηθούν περαιτέρω και να επιταχυνθούν οι έρευνες. Για τον λόγο ότι κάθε μία από αυτές τις περιπτώσεις χρήσης έχει διαφορετικούς περιορισμούς και υπάρχουν αρκετά τεχνολογικά μονοπάτια για την αντιμετώπιση κάθε χρήσης, προτείνεται η ΕΕ να χρηματοδοτήσει και να υποστηρίξει πιλοτικά προγράμματα για την κάθε χρήση, ώστε να επιτρέψει να προωθηθούν οι βέλτιστες τεχνολογικές λύσεις. Τα πιλοτικά προγράμματα θα πρέπει να ενθαρρύνουν τη συνεργασία ιδιωτικών επιχειρήσεων, νεοσύστατων επιχειρήσεων, εκπαιδευτικών οργανισμών και δημόσιων αρχών από διάφορες χώρες, χρησιμοποιώντας για παράδειγμα ένα μέσο όπως το Horizon 2020. Οι καλύτερες ιδέες θα λάβουν στη συνέχεια συμπληρωματική χρηματοδότηση παρακολούθησης και έτσι θα ολοκληρωθεί μια πλήρης πορεία καινοτομίας (Halpin & Piekarska, 2017).

Πρέπει να αναπτυχθούν πρότυπα για την ταυτοποίηση των σπουδαστών, για την καταγραφή επιτυχιών των φοιτητών σε επίσημο και μη τυπικό περιβάλλον σε διάφορα επίπεδα εκπαίδευσης, για την καταχώριση βεβαιώσεων και πιστοποιήσεων των ιδρυμάτων, χρήσης και επαναχρησιμοποίησης εκπαιδευτικών πόρων. Τα ψηφιακά πρότυπα μεταδεδομένων θα πρέπει να αναπτυχθούν μέσω διάφορων χωρών και φορέων, προκειμένου να διασφαλιστεί ότι θα αντιμετωπίσουν όλες τις τεχνικές εμπορικές προδιαγραφές (που σχετίζονται με τα πρότυπα). Η Ευρωπαϊκή Επιτροπή, από κοινού με τα κράτη μέλη, θα πρέπει να δρομολογήσει μια επείγουσα

και σημαντική προσπάθεια τυποποίησης σε αυτόν τον τομέα, ενδεχομένως σε συνεργασία με την CEN ή το ISO (Holotescu, 2018).

Η χρήση του blockchain στη μέγιστη δυναμική της για την εκπαίδευση απαιτεί από τους υπεύθυνους χάραξης πολιτικής να συνειδητοποιήσουν ότι η εμφάνιση του blockchain μπορεί να έχει σημαντικό αντίκτυπο στις υπάρχουσες και προγραμματισμένες δραστηριότητες και στρατηγικές. Συγκεκριμένα, οι υπεύθυνοι χάραξης πολιτικής πρέπει να έχουν πρόσβαση στην γνώση για να καθορίσουν αυτή την πτυχή, ώστε να τη λάβουν υπόψη στον αρχικό προγραμματισμό των blockchain. Κάτι τέτοιο απαιτεί άμεση γνώση μεταξύ των τομέων. Συστήνεται η συγκρότηση μιας συμβουλευτικής ομάδας, η οποία θα παρέχει τακτικές συμβουλές στους υπεύθυνους χάραξης πολιτικής σε επίπεδο ΕΕ και κρατών μελών όσον αφορά τις πιθανές τεχνολογικές απολαβές για συγκεκριμένες εφαρμογές και, επιπλέον, θα βοηθάει τα κράτη μέλη να εξισορροπήσουν τους κινδύνους και να διαχειριστούν τις προσδοκίες. Αυτό θα απαιτήσει την εμπλοκή και την υποστήριξη επαγγελματιών και εμπειρογνωμόνων διάφορων κλάδων, συμπεριλαμβανομένων των εξειδικευμένων οργανισμών του ιδιωτικού τομέα και των βιομηχανιών που εμπλέκονται. Επιπλέον, προτείνεται μια τέτοια ομάδα να καλύπτει το φάσμα της επίσημης εκπαίδευσης, της άτυπης εκπαίδευσης και της εργασιακής απασχόλησης (Skiba, 2017).

5.3. Προκλήσεις εφαρμογής

Παρόλο που η τεχνολογία blockchain θεωρείται ότι προκαλεί επανάσταση στους τρόπους επιχειρηματικής δραστηριότητας, η αλλαγή από τον τρόπο που υπάρχει σήμερα σε ένα σύστημα βασισμένο σε blockchain θα απαιτήσει χρόνο. Η ευρεία χρήση της τεχνολογίας πιστεύεται ότι υπάρχει εδώ και δέκα χρόνια τουλάχιστον. Επιπλέον, η σημερινή αξιοποίηση της τεχνολογίας είναι πολύ περιορισμένη σε σύγκριση με τη χρήση που θα υπάρχει σε λίγα χρόνια. Είναι πιθανό ότι εάν η τεχνολογία αυτή εφαρμοστεί παγκοσμίως με εκατομμύρια χρήστες, δεν θα μπορούσε να υποστηρίξει όλες τις υπηρεσίες με ασφάλεια για όλους. Η τεχνολογία blockchain αντιμετωπίζει τόσο τεχνικούς όσο και νομοθετικούς φραγμούς. Η δημιουργία νέων block στο blockchain έχει αρνητικό αντίκτυπο στο περιβάλλον (Holotescu, 2018). Η διαδικασία εξόρυξης καταναλώνει τεράστιες ποσότητες ηλεκτρικού και εξορυκτικού εξοπλισμού κάθε φορά που δημιουργείται ένα νέο block ή ελέγχεται μια συναλλαγή. Αυτό καίει συνεχώς τις πρώτες ύλες και την ενέργεια. Ακόμη και όλα τα τρισεκατομμύρια των προσπαθειών για την επίλυση των δύσκολων παζλ

καταναλώνουν ενέργεια. Όσο περισσότεροι άνθρωποι χρησιμοποιούν προγράμματα βασισμένα σε blockchain τόσο περισσότερη ενέργεια καταναλώνεται. Τον Οκτώβριο του 2015, έρευνες έδειξαν ότι αν οι ανθρακωρύχοι χρησιμοποιούν την πιο αποδοτική τεχνολογία, η κατανάλωση ηλεκτρικής ενέργειας μπορεί να διαρκέσει έως και δύο terawatt ετησίως. Αυτό αντιστοιχεί στη χρήση ηλεκτρικής ενέργειας για περισσότερους από 150.000 κατοίκους στην Καλιφόρνια. Ως εκ τούτου, απαιτείται δευτερεύουσα χρήση της σπατάλης ενέργειας και μια φιλικότερη προς το περιβάλλον διαδικασία εξόρυξης (Yang, Li, Wu & Zhao, 2017).

Στην πραγματικότητα υπάρχει μια άλλη εναλλακτική λύση στη διαδικασία εξόρυξης. Η εικονική εξόρυξη μπορεί να αντικαταστήσει τη διαδικασία χειρωνακτικής επίλυσης των μαθηματικών παζλ, πράγμα που μειώνει επίσης την ανάγκη εξοπλισμού. Αυτό υποστηρίζεται για να μειωθεί το «περιβαλλοντικό αποτύπωμα» που προκαλείται από τη διαδικασία εξόρυξης και, ακόμα πιο σημαντικό, να διασφαλιστεί ότι η εξόρυξη εκτελείται από εκείνους τους εμπλεκόμενους που έχουν το συμφέρον του συστήματος στο επίκεντρο. Επιπλέον, η τεχνολογία blockchain μπορεί επίσης να χρησιμοποιηθεί ακατάλληλα. Ένας τρόπος κατάχρησης του συστήματος είναι η επίθεση κατά 51%. Αυτό σημαίνει ότι κάποιος ελέγχει το ήμισυ του δικτύου, δηλαδή το 51%, έτσι ώστε οι συναλλαγές να μην μπορούν να επαληθευτούν όπως πρέπει, και αυτό έχει ως αποτέλεσμα ψευδείς πληροφορίες να μπορούν να προστεθούν στο blockchain (Reynaetal., 2018). Αυτό είναι εξαιρετικά απίθανο λόγω του τεράστιου μεγέθους του δικτύου. Ωστόσο, υπάρχει ένας ακόμα τρόπος για να παραπλανηθεί το σύστημα. Εάν το πρώτο κομμάτι των πληροφοριών που προστέθηκαν στο blockchain είναι ψευδές, το σύστημα μπορεί να πιστεύει ότι είναι νόμιμο. Υπάρχουν επίσης νομοθετικοί φραγμοί, εκ των οποίων ο ένας είναι η ρύθμιση. Αυστηρότεροι κανονισμοί ενδέχεται να εμποδίσουν την ανάπτυξη της τεχνολογίας blockchain. Έτσι, προτού γίνει γνωστό το σύνολο των δυνατοτήτων της τεχνολογίας, θα ήταν λάθος να περιοριστούν οι κανονισμοί των ιδρυμάτων στα οποία η τεχνολογία μπορεί να εφαρμοστεί. Ένα άλλο ζήτημα που αντιμετωπίζουν οι τεχνολογίες είναι οι άνθρωποι που διστάζουν να αλλάξουν. Οι βιομηχανίες που στηρίζονται στην αξιοπιστία, όπως τα χρηματοπιστωτικά ιδρύματα, επηρεάζονται περισσότερο από αυτήν την τεχνολογία. Παρόλο που πολλά χρηματοπιστωτικά ιδρύματα εργάζονται για να προσαρμόσουν αυτήν την τεχνολογία, άλλοι σίγουρα θα την πολεμήσουν. Μπορεί να μην είναι ελκυστική η ξαφνική αλλαγή από ένα σύστημα που μια εταιρεία ή μια τράπεζα διατηρεί προσωπικές και εμπιστευτικές πληροφορίες σε ένα σύστημα βασισμένο σε αποδεικτικά που δεν ελέγχεται από κανέναν. Η αντιμετώπιση αυτών των προκλήσεων απαιτεί συμφωνία ολόκληρης

της κοινότητας. Μόνο τότε θα είναι δυνατή η πλήρης προσαρμογή της τεχνολογίας blockchain. (Batubara, Ubacht & Janssen, 2018).

Βιβλιογραφία

1. Adip.gr. (2019). Πιστοποίηση | Αρχή Διασφάλισης & Πιστοποίησης της Ποιότητας. Retrieved 24 July 2019, from https://www.adip.gr/el/basic-page/677/pistopoiisi
2. Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-Based Applications in Education: A Systematic Review. *Applied Sciences*, *9*(12), 2400.
3. Albeanu, G. (2017, October). Blockchain technology and education. In *Proceedings of the 12th International Conference on Virtual Learning* (pp. 271-275).
4. Allessie, D., Sobolewski, M., Vaccari, L., & Pignatelli, F. (2019). Blockchain for digital government. *EUR*, *29677*, 2019-04.
5. Ateniese, G., Magri, B., Venturi, D., & Andrade, E. (2017). Redactable blockchain–or–rewriting history in bitcoin and friends. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 111-126). IEEE.
6. Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?. *Available at SSRN 2709713*.
7. Baars, D. S. (2016). *Towards self-sovereign identity using blockchain technology* (Master's thesis, University of Twente).
8. Banerjee, A. (2018). Blockchain technology: supply chain insights from ERP. In *Advances in Computers* (Vol. 111, pp. 69-98). Elsevier.
9. Batubara, F. R., Ubacht, J., & Janssen, M. (2018, May). Challenges of blockchain technology adoption for e-government: a systematic literature review. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age* (p. 76). ACM.
10. Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain–the gateway to trust-free cryptographic transactions.
11. Bostonbeyond.org. (2019). Skill Badges | Boston After School & Beyond. Retrieved 9 October 2019, from https://bostonbeyond.org/initiatives/digital-badges/
12. Bratcher, E. (2019). New Money: Close the Gap With Digital Badging. Retrieved 9 October 2019, from http://associationsnow.com/2017/02/new-money-close-gap-digital-badging/ Bratcher, E. (2019). New Money: Close the Gap With Digital Badging. Retrieved

9 October 2019, from http://associationsnow.com/2017/02/new-money-close-gap-digital-badging/

13. Brown, M. K., & Brown, M. S. (2017). *U.S. Patent No. 9,621,352*. Washington, DC: U.S. Patent and Trademark Office.
14. Charraud, A. M. (2010). European Inventory on Validation of Non-Formal and Informal Learning 2010. Country Report: France.
15. Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1), 1.
16. Chuen, D. L. K., Guo, L., & Wang, Y. (2017). Cryptocurrency: A new investment opportunity?. *The Journal of Alternative Investments*, *20*(3), 16-40.
17. Coelho, P., Zúquete, A., & Gomes, H. (2018). Federation of Attribute Providers for User Self-Sovereign Identity. *Journal of Information Systems Engineering & Management*, *3*(4), 32.
18. Contreras, A., & Gollin G. (2009). The real and the fake degree and diploma mills. Change. 41(2), 36-43. http://dx.doi.org/10.3200/CHNG.41.2.36-43
19. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.
20. Cs2n.org. (2019). CS-STEM Network. Retrieved 9 October 2019, from https://www.cs2n.org/
21. Devedžić, V., & Jovanović, J. (2015). Developing open badges: A comprehensive approach. *Educational Technology Research and Development*, *63*(4), 603-620.
22. Doatap.gr. (2019). Διεπιστημονικός οργανισμός αναγνώρισης τίτλων ακαδημαϊκών και πληροφόρησης. Retrieved 24 July 2019, from http://www.doatap.gr/gr/nomos.php
23. eoppep.gr. (2019). *Εθνικό Πλαίσιο Προσόντων*. ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ. Retrieved from https://www.eoppep.gr/images/European/ETHNIKO_PLAISIO_PROSONTON_NOVEMBER_2016.pdf
24. ERMENC, K. S. (2014). CHAPTER NINE QUALIFICATIONS FRAMEWORKS AND LEARNING OUTCOMES AS SUPPORTERS OF VALIDATION OF NON–FORMAL AND INFORMAL LEARNING1. *From formal to non-formal: education, learning and knowledge*, 191.

25. Gabison, G. (2016). Policy considerations for the blockchain technology public and private applications. *SMU Sci. & Tech. L. Rev.*, *19*, 327.
26. Galanis, N., Mayol, E., Alier, M., & García-Peñalvo, F. J. (2016). Supporting, evaluating and validating informal learning. A social approach. *Computers in Human Behavior*, *55*, 596-603.
27. Garrick, J. (2012). *Informal learning in the workplace: Unmasking human resource development*. Routledge.
28. GARWE, E. C. (2015). Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe. *Journal of Studies in Education ISSN*, 2162-6952.
29. Giaglis, G. M. (2018). The Emerging Blockchain Revolution and its Implications for Cyprus. *The Cyprus Review*, *30*(2), 157-158.
30. Gramoli, V. (2017). From blockchain consensus back to byzantine consensus. *Future Generation Computer Systems*.
31. Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., & Wendland, F. (2018). Blockchain for education: lifelong learning passport. In *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET).
32. Gupta, S. S. (2017). *Blockchain*. John Wiley & Sons, Inc.
33. Halpin, H., & Piekarska, M. (2017, April). Introduction to Security and Privacy on the Blockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 1-3). IEEE.
34. Han, M., Li, Z., He, J. S., Wu, D., Xie, Y., & Baba, A. (2018, September). A Novel Blockchain-based Education Records Verification Solution. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education* (pp. 178-183). International World Wide Web Conferences Steering Committee.
35. Hickey, D. T., & Otto, N. (2017). Endorsement 2.0: Taking Open Badges and E-Credentials to the Next Level.
36. Hileman, G., & Rauchs, M. (2017). Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*, *33*.

37. Holotescu, C. (2018). Understanding Blockchain Opportunities and Challenges. In *Conference proceedings of» eLearning and Software for Education «(eLSE)* (Vol. 4, No. 14, pp. 275-283). ” Carol I” National Defence University Publishing House.
38. Hou, H. (2017). The application of blockchain technology in E-government in China. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-4). IEEE.
39. Hurley, B. (2017). Open Badges and Alternative Credentialing. *International Journal on Innovations in Online Education*, *1*(3).
40. Imsglobal.org. (2019). Open Badges v2.0. Retrieved 9 October 2019, from http://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html
41. Jacobovitz, O. (2016). Blockchain for identity management. *The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva Google Scholar*, *1*, 9.
42. Johnson, C. (2006). Credentialism and the Proliferation of Fake Degrees: The Employer Pretends to Need a Degree; The Employee Pretends to Have One. Hofstra Labor & Employment Law Journal, 23(2), 269-344.
43. Juričić, V., Radošević, M., & Fuzul, E. (2019, May). Creating student’s profile using blockchain technology. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 521-525). IEEE.
44. Kamišalić, A., Turkanović, M., Mrdović, S., & Heričko, M. (2019, April). A Preliminary Review of Blockchain-Based Solutions in Higher Education. In *International Workshop on Learning Technology for Education in Cloud* (pp. 114-124). Springer, Cham.
45. Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain tranactions. *Duke LJ*, *65*, 569.
46. Kolvenbach, S., Ruland, R., Gräther, W., & Prinz, W. (2018). Blockchain 4 education. In *Proceedings of 16th European Conference on Computer-Supported Cooperative Work-Panels, Posters and Demos*. European Society for Socially Embedded Technologies (EUSSET).
47. Kuhmonen, A., Pöyry-Lassila, P., & Seppälä, H. (2018, October). Open Badges: Experiences From a Game Development Skills Open Badge Co-Creation Process.

In *ECGBL 2018 12th European Conference on Game-Based Learning* (p. 307). Academic Conferences and publishing limited.

48. Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer?. *Records Management Journal*, *26*(2), 110-139.
49. Liu, Y., & Tsyvinski, A. (2018). *Risks and returns of cryptocurrency* (No. w24877). National Bureau of Economic Research.
50. Makewav.es. (2019). Makewaves is Closed. Retrieved 9 October 2019, from https://www.makewav.es/
51. Manuti, A., Pastore, S., Scardigno, A. F., Giancaspro, M. L., & Morciano, D. (2015). Formal and informal learning in the workplace: a research review. *Internationaljournaloftraininganddevelopment*, *19*(1), 1-17.
52. MASLO, I., SURIKOVA, S., KARTTUNEN, A., & AARNA, O. (2012). Validation of non-formal and informal learning in Latvia, Estonia and Finland: An analysis of the context. *Journal of Educational Sciences/Revista de Stiintele Educatiei*, *14*(2).
53. Maurer, U. (2003). Intrinsic limitations of digital signatures and how to cope with them. In *International Conference on Information Security* (pp. 180-192). Springer, Berlin, Heidelberg.
54. McConaghy, M., McMullen, G., Parry, G., McConaghy, T., & Holtzman, D. (2017). Visibility and digital art: blockchain as an ownership layer on the Internet. *Strategic Change*, *26*(5), 461-470.
55. Ølnes, S. (2016, September). Beyond bitcoin enabling smart government using blockchain technology. In *International Conference on Electronic Government* (pp. 253-264). Springer, Cham.
56. Online.colostate.edu. (2019). Digital Badges - CSU Online. Retrieved 9 October 2019, from https://www.online.colostate.edu/badges/
57. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173-190.
58. Schukat, M., & Cortijo, P. (2015, June). Public key infrastructures and digital certificates for the Internet of things. In *2015 26th Irish signals and systems conference (ISSC)* (pp. 1-5). IEEE.

59. Scott, B. (2016). *How can cryptocurrency and blockchain technology Play a role in building social and solidarity finance?*(No. 2016-1). UNRISD Working Paper.
60. Seebacher, S., & Schüritz, R. (2017). Blockchain technology as an enabler of service systems: A structured literature review. In *International Conference on Exploring Services Science* (pp. 12-23). Springer, Cham.
61. Sharples, M., de Roock, R., Ferguson, R., Gaved, M., Herodotou, C., Koh, E., ...& Weller, M. (2016). Innovating pedagogy 2016: Open University innovation report 5.
62. Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). *Massachusetts Institute of Technology-Connection Science*, *1*(3), 1-19.
63. Simota, T. (2019). Εισαγωγή. Retrieved 24 July 2019, from https://www.eoppep.gr/index.php/el/qualification-certificate/introductionepp
64. Skiba, D. J. (2017). The potential of blockchain in education and health care. *Nursing education perspectives*, *38*(4), 220-221.
65. Sousa, J., Bessani, A., & Vukolic, M. (2018). A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In *2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN)* (pp. 51-58). IEEE.
66. Stasz, C. (2011). The purposes and validity of vocational qualifications.
67. Stubbs, C. (2019). Information Literacy Badges at Penn State | Informing and supporting Penn State's use of digital badges for information literacy skills. Retrieved 9 October 2019, from http://sites.psu.edu/informationliteracybadges/
68. Sudia, F. W., & Siritzky, B. (2011). *U.S. Patent No. 7,904,722*. Washington, DC: U.S. Patent and Trademark Office.
69. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".
70. Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K. H. (2017). A critical review of blockchain and its current applications. In *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)* (pp. 109-113). IEEE.
71. Ting, K. K., Yuen, S. C., Lee, K. H., & Leong, P. H. (2002, September). An FPGA based SHA-256 processor. In *International Conference on Field Programmable Logic and Applications* (pp. 577-585). Springer, Berlin, Heidelberg.
72. Turcu, C., Turcu, C., & Chiuchisan, I. (2019). Blockchain and its Potential in Education. *arXiv preprint arXiv:1903.09300*.

73. Villalba-Garcia, E., Souto-Otero, M., & Murphy, I. (2014). The 2014 European Inventory on validation of non-formal and informal learning. Prospects and trends on validation in Europe. *Berufsbildung in Wissenschaft und Praxis*, *5*, 16-19.
74. Williams, P. (2019). Does competency-based education with blockchain signal a new mission for universities?. *Journal of higher education policy and management*, *41*(1), 104-117.
75. Won, J. H., & Bollella, G. (2019). *U.S. Patent Application No. 10/382,485*.
76. Yang, X. M., Li, X., Wu, H. Q., & Zhao, K. (2017). The application model and challenges of blockchain technology in education. *Modern distance education research*, (2), 34-45.
77. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557-564). IEEE.
78. Γεροθανάσης, Ι. (2017). *Αρχή Διασφάλισης & Πιστοποίησης της Ποιότητας στην Ανώτατη Εκπαίδευση*. Athens: Αρχή Διασφάλισης & Πιστοποίησης της Ποιότητας στην Ανώτατη Εκπαίδευση. Retrievedfromhttps://www.adip.gr/sites/default/files/news/13/654-3_paroysiasi_antiproedroy_ig.pdf
79. Λιόση, Φ. (2019). Επικύρωση της μη-τυπικής και άτυπης μάθησης: Από τις ευρωπαϊκές πολιτικές στις εθνικές εφαρμογές. *ACADEMIA*, (14). Retrieved from https://imegsevee.gr/wp-content/.../02/EKPAIDEUSH_DIA_VIOU_PISTOPOIHSH.pdf
80. Τητήρου, Χ. (2017). Δια Βίου Μάθηση και Αγορά Εργασίας Η Δια Βίου Μάθηση στον Οργανισμό Απασχόλησης Εργατικού Δυναμικού. *Εκπαίδευση, Δια Βίου Μάθηση, Έρευνα Και Τεχνολογική Ανάπτυξη, Καινοτομία Και Οικονομία*, *1*, 173. doi: 10.12681/elrie.784
81. ΦΩΤΟΠΟΥΛΟΣ, Ν., & ΖΆΓΚΟΣ, Χ. (2016). *Διά βίου μάθηση, πιστοποίηση προσόντων και διασφάλιση ποιότητας Όψεις και διερεύνηση της ευρωπαϊκής εμπειρίας*. Retrieved from https://www.inegsee.gr/wp-content/uploads/2016/12/MELETH-45.pdf