



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN ΓΙΑ ΤΗΝ
ΑΠΟΘΗΚΕΥΣΗ ΚΑΙ ΑΝΑΚΤΗΣΗ ΕΓΓΡΑΦΩΝ
ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΦΟΡΕΑ

Χρήστος Βαρέσης

Επιβλέπων: Νικόλαος Γιαννακέας Αναπληρωτής καθηγητής

Άρτα, Ιούνιος, 2025

**Utilizing blockchain technology for the storage and retrieval of
educational institution documents**

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Αρτα, XX/06/2025

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπων καθηγητής

Νικόλαος Γιαννακέας,

Αναπληρωτής Καθηγητής

2. Μέλος επιτροπής

Αλέξανδρος Τζάλλας,

Αναπληρωτής Καθηγητής

3. Μέλος επιτροπής

Δημήτριος Δημόπουλος,

Πανεπιστημιακός Υπότροφος

© Βαρέσης, Χρήστος, 2025.

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα μεταπτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Βαρέσης, Χρήστος

Υπογραφή

Περίληψη

Η τεχνολογία Blockchain επιτρέπει τη δημιουργία ενός κατακευματισμένου συστήματος καταγραφής δεδομένων (distributed ledger) σε μορφή αλυσίδας. Τα δεδομένα προστίθενται στην αλυσίδα αυτή υπό τη μορφή ψηφιακών blocks δεδομένων. Τα νέα blocks δεδομένων προστίθενται με ασφαλή τρόπο στο τέλος της αλυσίδας και ταυτόχρονα, κάθε νέο block επαληθεύει τη γνησιότητα του προηγούμενου block, εξασφαλίζοντας έτσι ότι τα δεδομένα των προηγούμενων blocks δεν έχουν τροποποιηθεί ή καταστραφεί με οποιονδήποτε τρόπο. Δεν είναι επομένως δυνατή η εκ των υστέρων τροποποίηση ή κακοπροαίρετη αλλοίωση των δεδομένων τα οποία αποθηκεύονται στην αλυσίδα, εξασφαλίζοντας έτσι την ακεραιότητα των δεδομένων.

Ο τρόπος αυτός λειτουργίας ενός συστήματος που βασίζεται στην τεχνολογία Blockchain προσφέρει πολλά πλεονεκτήματα τα οποία μπορούν να χρησιμοποιηθούν σε διάφορους τομείς, όπως είναι η Εκπαίδευση. Με τη βοήθεια της τεχνολογίας Blockchain μπορεί να δημιουργηθεί ένα σύστημα καταγραφής και ανάκτησης ακαδημαϊκών τίτλων, η γνησιότητα των οποίων μπορεί να επιβεβαιωθεί οποιαδήποτε στιγμή από κάθε ενδιαφερόμενο. Τα τελευταία χρόνια έχουν προταθεί διάφορα συστήματα για τον χώρο της Εκπαίδευσης και της επαλήθευσης της απόκτησης ακαδημαϊκών τίτλων. Παρ' όλα αυτά υπάρχουν πολλά βήματα τα οποία πρέπει να γίνουν και αρκετές δυσκολίες που πρέπει να ξεπεραστούν για την καθολική χρήση της τεχνολογίας αυτής από το σύνολο των ακαδημαϊκών ιδρυμάτων.

Στην παρούσα εργασία παρουσιάζεται μία μελέτη των χαρακτηριστικών της τεχνολογίας Blockchain, τα οποία μπορούν να βοηθήσουν για την αξιόπιστη αποθήκευση δεδομένων που αφορούν ακαδημαϊκούς τίτλους. Παρουσιάζονται επίσης διάφορες ερευνητικές προσπάθειες οι οποίες αφορούν την χρήση της τεχνολογίας Blockchain στον χώρο της Εκπαίδευσης. Επιπρόσθετα, αναπτύσσεται και μία εφαρμογή η οποία μπορεί να χρησιμοποιηθεί για την καταχώρηση ακαδημαϊκών τίτλων με τη βοήθεια της πλατφόρμας HyperLedger Fabric.

Λέξεις κλειδιά: blockchain, εκπαιδευτικό σύστημα, ανάκτηση τίτλων, HyperLedger Fabric

Abstract

Blockchain technology allows the creation of a distributed ledger system in the form of a “chain”. The available data is added to this chain in the form of digital blocks. Each new added block is securely placed at the end of this chain while simultaneously verifying the authenticity of the previous block. This process enhances the fidelity of the previous block by ensuring it has not been modified or destroyed. Therefore, it is not possible to subsequently modify or maliciously alter the data stored in the chain. Through this process the integrity of the data set is ensured.

The nature of a blockchain system offers significant advantages and applications that can be integrated and utilized in various fields such as the educational system. In fact, the utilization of blockchain technology in education can enhance and upgrade the process of academic title recording and retrieval. The last years, various systems have been proposed for the verification of the acquisition of academic titles in the field of education. However, many “steps” need to be taken, and several difficulties need to be overcome for the universal use of this technology by all academic institutions.

The present paper presents a study of the characteristics of blockchain technology and the ways it can help in the reliable storage of data related to academic titles. Various research efforts are also presented regarding the use of blockchain technology in the field of education. In addition, an application is developed that can be used for the registration of academic titles with the help of the HyperLedger Fabric platform.

Keywords: blockchain, educational system, title retrieval, HyperLedger Fabric

Περιεχόμενα

Με επιφύλαξη παντός δικαιώματος. All rights reserved. Δήλωση μη λογοκλοπής	4
Περίληψη	6
Abstract.....	7
Ευρετήριο Εικόνων.....	10
1. Εισαγωγή	11
1.1 Τεχνολογία Blockchain.....	11
1.2 Πιθανές χρήσεις της τεχνολογίας Blockchain στην Εκπαίδευση	13
1.3 Σκοπός και στόχοι της εργασίας	17
2. Χαρακτηριστικά της τεχνολογίας Blockchain και η χρήση τους για την ανάπτυξη εφαρμογών στην Εκπαίδευση	19
2.1 Περιγραφή και χαρακτηριστικά της τεχνολογίας Blockchain.....	19
2.2 Δομή αλυσίδας Blockchain.....	21
2.3 Εφαρμογές και πλεονεκτήματα της τεχνολογίας Blockchain.....	22
2.4 Σχετική έρευνα.....	26
2.5 Εμπόδια και δυσκολίες	29
3. Ανάπτυξη Blockchain για την υποστήριξη εκπαιδευτικών αναγκών	32
3.1 Τρόπος λειτουργίας ενός δικτύου Blockchain.....	32
3.2 Πλατφόρμες Blockchain	34
3.3 Hyperledger Fabric	39
4. Υλοποίηση εφαρμογής Blockchain	44
4.1 Λειτουργίες και δυνατότητες της εφαρμογής	44
4.2 Εγκατάσταση και λειτουργία του HyperLedger Fabric.....	45
4.2.1 Προαπαιτούμενα	45
4.2.2 Διαδικασία της εγκατάστασης	47
4.2.3 Δημιουργία δικτύου	48
4.3 Περιγραφή της εφαρμογής.....	51
4.4 Παρουσίαση της εφαρμογής EduChain	52

5. Επίλογος και συμπεράσματα	58
Βιβλιογραφικές	61

Ευρετήριο Εικόνων

Εικόνα 1: Χρήσεις της τεχνολογίας Blockchain (Statista, [7])	23
Εικόνα 2: Αποφυγή διπλοπληρωμών.....	24
Εικόνα 3: Εταιρείες που χρησιμοποιούν το Hyperledger Fabric.....	40
Εικόνα 4: Αρχιτεκτονική δικτύου Hyperledger Fabric [31]	43
Εικόνα 5: Δημιουργία δικτύου HyperLedger Fabric	50
Εικόνα 6: Κεντρική οθόνη της εφαρμογής	53
Εικόνα 7: Αναζήτηση πιστοποιητικών	53
Εικόνα 8: Προβολή όλων των πιστοποιητικών	54
Εικόνα 10: Αναζήτηση με βάση τον κωδικό του φοιτητή.....	55
Εικόνα 9: Εμφάνιση πληροφοριών πιστοποιητικού	55
Εικόνα 11: Αναζήτηση με βάση το Εκπαιδευτικό ίδρυμα	56
Εικόνα 13: Οθόνη διαγραφής πιστοποιητικού.....	57
Εικόνα 12: Εισαγωγή νέου πιστοποιητικού.....	57

Κεφάλαιο 1^ο

1. Εισαγωγή

1.1 Τεχνολογία Blockchain

Η τεχνολογία Blockchain χρησιμοποιήθηκε για πρώτη φορά το 2008 από ένα άτομο ή μία ομάδα ανθρώπων με το όνομα Satoshi Nakamoto κατά τη δημιουργία του κρυπτονομίσματος Bitcoin [1]. Με τη χρήση της τεχνολογίας Blockchain, είναι δυνατή η χρήση του Bitcoin χωρίς την ανάγκη ύπαρξης ενός κεντρικού φορέα ο οποίος θα πρέπει να υπάρχει για να εξασφαλίζει την εγκυρότητα των συναλλαγών. Η τεχνολογία Blockchain επιτρέπει δηλαδή τη δημιουργία ενός κατακευματισμένου συστήματος καταγραφής δεδομένων (distributed ledger) σε μορφή αλυσίδας. Στην αλυσίδα αυτή, τα δεδομένα έχουν τη μορφή ψηφιακών blocks δεδομένων. Νέα blocks δεδομένων μπορούν να προστεθούν με ασφαλή τρόπο στο τέλος της αλυσίδας και να συνδεθούν με τα προηγούμενα blocks.

Κάθε block που προστίθεται στην αλυσίδα, εκτός από την καταγραφή της χρονικής στιγμής της συναλλαγής και τις πληροφορίες που την αφορούν, περιλαμβάνει και κάποιες επιπλέον πληροφορίες οι οποίες πρακτικά επαληθεύουν τη γνησιότητα του προηγούμενου block. Αυτό πρακτικά σημαίνει ότι κάθε φορά που δημιουργείται και προστίθεται ένα νέο block στην αλυσίδα, επαληθεύεται ταυτόχρονα ότι όλα τα δεδομένα στα προηγούμενα blocks δεν έχουν τροποποιηθεί ή καταστραφεί με οποιονδήποτε τρόπο. Δεν είναι επομένως δυνατή η εκ των υστέρων τροποποίηση ή κακοπροαίρετη αλλοίωση των δεδομένων τα οποία αποθηκεύονται στην αλυσίδα. Με τον τρόπο αυτόν εξασφαλίζεται η ακεραιότητα των δεδομένων που καταγράφονται.

Η διαχείριση της κατακευματισμένης αλυσίδας δεδομένων γίνεται συνήθως από ένα δίκτυο κόμβων peer-to-peer (P2P). Η καταγραφή και αποθήκευση νέων δεδομένων σε ένα block της αλυσίδας γίνεται μετά από συμφωνία των κόμβων του δικτύου, με βάση τον αλγόριθμο συμφωνίας (consensus algorithm) που χρησιμοποιεί το δίκτυο. Θα πρέπει δηλαδή η ορθότητα των δεδομένων τα οποία

αποθηκεύονται στην αλυσίδα, να επαληθευτεί από επαρκή αριθμό κόμβων του P2P δικτύου, ανάλογα με το πρωτόκολλο το οποίο χρησιμοποιείται στο δίκτυο Blockchain, προσφέροντας έτσι τους απαραίτητους μηχανισμούς για την ασφάλεια των συναλλαγών. Έτσι, οι συναλλαγές που καταγράφονται προστατεύονται από πιθανές απάτες και κακόβουλες επιθέσεις [2].

Η πρώτη πρόταση για τη δημιουργία τεχνολογίας παρόμοιας με αυτή του Blockchain έγινε το 1982 από τον κρυπτογράφο David Chaum στη διατριβή του [3]. Υπήρξαν και άλλες προτάσεις στη συνέχεια για τη δημιουργία ενός συστήματος καταγραφής συναλλαγών όπου δεν θα είναι δυνατή η εκ των υστέρων τροποποίηση της ημερομηνίας και των πληροφοριών της συναλλαγής. Ο σκοπός δηλαδή των ερευνών αυτών ήταν η δημιουργία ενός συστήματος καταγραφής συναλλαγών, όπου δεν θα μπορούσε να υπάρξει καμία αμφισβήτηση των συναλλαγών αυτών. Η τεχνολογία Blockchain σχεδιάστηκε με στόχο της εξάλειψη της ανάγκης ύπαρξης ενός κεντρικού φορέα που θα πρέπει να εγγυάται για τις συναλλαγές, προσφέροντας ταυτόχρονα τη δυνατότητα επαλήθευσης της ορθότητας των συναλλαγών ανά πάσα στιγμή. Με τον τρόπο αυτόν, η τεχνολογία Blockchain προσέφερε όλες τις απαραίτητες υπηρεσίες για την κυκλοφορία ενός ψηφιακού κρυπτονομίσματος, όπως είναι το Bitcoin, αλλά και τα χιλιάδες άλλα κρυπτονομίσματα που ακολούθησαν από το 2008 και μετά.

Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί σε πάρα πολλούς τομείς, πέρα από τον χώρο των κρυπτονομισμάτων. Τα χαρακτηριστικά της τεχνολογίας Blockchain είναι ιδανικά για τη δημιουργία έξυπνων συμβολαίων (smart contracts). Ένα έξυπνο συμβόλαιο βασίζεται σε ένα πρωτόκολλο συναλλαγής και έχει τη δυνατότητα επαλήθευσης των δεδομένων που καταγράφει, χωρίς την ανάγκη κάποιου κεντρικού φορέα που θα αναλάβει το ρόλο του διαμεσολαβητή και χωρίς τα κόστη που χρειάζονται για τα παραδοσιακά συμβόλαια. Το Ethereum αποτελεί μία δημόσια, ανοιχτού κώδικα, κατανεμημένη πλατφόρμα Blockchain η οποία ξεκίνησε το 2014 από τον Vitaly Buterin και δίνει τη δυνατότητα δημιουργίας έξυπνων συμβολαίων. Κατά την ανακοίνωση της πλατφόρμας Ethereum, το Bitcoin χαρακτηρίζεται ως μία αδύναμη υλοποίηση έξυπνου συμβολαίου και το Ethereum αποτελεί μία ισχυρότερη πρόταση για τη δημιουργία ασφαλών έξυπνων συμβολαίων [4]. Τα έξυπνα συμβόλαια και το Blockchain μπορούν να αποτελέσουν τη βάση για την Αποκεντρωμένη Οικονομία (Decentralized Finance – DeFi), όπου δεν θα υπάρχει η ανάγκη για ενδιάμεσους

φορείς εγγύησης συμβολαίων και συναλλαγών, όπως είναι τράπεζες, συμβολαιογράφοι κτλ. Η τεχνολογία Blockchain μπορεί να έχει επομένως, μέσω των έξυπνων συμβολαίων, πολλές χρήσεις στον χώρο της ψηφιακής Οικονομίας και των συναλλαγών.

Η πιθανή χρήση της τεχνολογίας Blockchain δεν περιορίζονται μόνο στον χώρο των κρυπτονομισμάτων, των πληρωμών, των έξυπνων συμβολαίων και της ψηφιακής Οικονομίας, αλλά μπορεί να επεκταθεί σε πάρα πολλούς άλλους χώρους. Στον χώρο της Εκπαίδευσης υπάρχουν διάφορες ανάγκες οι οποίες αφορούν την καταγραφή των πληροφοριών σχετικά με τις επιδόσεις των μαθητών, την επαλήθευση τίτλων και πιστοποιητικών που έχουν εκδοθεί από εκπαιδευτικούς φορείς, τη δημοσίευση ερευνητικών εργασιών, τη διανομή εκπαιδευτικού υλικού, τη δια Βίου μάθηση, την ανταλλαγή φοιτητών κλπ. Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία συστημάτων για τη συνεργασία εκπαιδευτικών φορέων και υποψήφιων εργοδοτών σχετικά με τη διαχείριση και την επαλήθευση της ακεραιότητας όλων αυτών των πληροφοριών. Αντίστοιχες εφαρμογές της τεχνολογίας Blockchain μπορούν να υπάρξουν σε όλους τους άλλους χώρους της οικονομικής και κοινωνικής ζωής, όπου υπάρχει ανάγκη για διασφάλιση της αξιοπιστίας συναλλαγών και την ασφαλή καταχώρηση δεδομένων.

Στην παρούσα πτυχιακή εργασία μελετώνται τα χαρακτηριστικά εκείνα της τεχνολογίας Blockchain, τα οποία μπορούν να χρησιμοποιηθούν στον χώρο της Εκπαίδευσης για την ανάπτυξη συστημάτων και πλατφορμών που μπορούν να δώσουν λύσεις σε προβλήματα και δυσλειτουργίες του χώρου. Παρουσιάζονται επίσης κάποια εργαλεία με τη βοήθεια των οποίων μπορεί να υλοποιηθεί ένα σύστημα επαλήθευσης ψηφιακών πιστοποιητικών και τίτλων που έχουν εκδοθεί από κάποιον εκπαιδευτικό φορέα.

1.2 Πιθανές χρήσεις της τεχνολογίας Blockchain στην Εκπαίδευση

Η τεχνολογία Blockchain μπορεί να φέρει σημαντικές και επαναστατικές αλλαγές στον χώρο της Εκπαίδευσης και τη συνεργασία ανάμεσα στους διάφορους εκπαιδευτικούς φορείς και τους υποψήφιους εργοδότες. Κάποια συστήματα και πλατφόρμες τα οποία βασίζονται στην τεχνολογία Blockchain έχουν ήδη υλοποιηθεί, όμως υπάρχει πολύς ακόμη δρόμος και αρκετές προκλήσεις και

δυσκολίες οι οποίες θα πρέπει να αντιμετωπιστούν. Κάποιες από τις βασικότερες πιθανές χρήσεις που θα μπορούσε να έχει η τεχνολογία στον χώρο της Εκπαίδευσης είναι οι πιο κάτω:

1. **Καταγραφή και επαλήθευση τίτλων σπουδών.** Τα εκπαιδευτικά ιδρύματα όλων των επιπέδων εκδίδουν τίτλους σχετικά με τους μαθητές/φοιτητές που παρακολουθούν τη φοίτηση του ιδρύματος. Η εγκυρότητα των τίτλων αυτών θα πρέπει πολλές φορές να επαληθευτεί είτε για την εγγραφή κάποιου απόφοιτου σε κάποιο άλλο εκπαιδευτικό ίδρυμα, είτε κατά την αναζήτηση εργασία κλπ. Με τον παραδοσιακό τρόπο επαλήθευσης τίτλων δεν είναι εύκολο να εξασφαλιστεί η εγκυρότητα της διαδικασίας. Κάθε φορέας κάνει χρήση του δικού του μηχανισμού επαλήθευσης και συχνά οι μηχανισμοί αυτοί είναι διάτρητοι σε εξαπατήσεις. Εμφανίζονται δηλαδή περιστατικά ψευδούς δήλωσης κατοχής τίτλων οι οποίοι είτε δεν υφίστανται στην πραγματικότητα, είτε ο βαθμός κτήσης του τίτλου ή ο ακριβής του τίτλος είναι διαφορετικός από αυτόν που έχει δηλωθεί. Με τη χρήση της τεχνολογίας Blockchain μπορούν να δημιουργηθούν κατανεμημένες πλατφόρμες όπου μπορεί να γίνει καταχώρηση των τίτλων που έχουν αποκτηθεί από μαθητές/φοιτητές εκπαιδευτικών ιδρυμάτων. Οι πλατφόρμες αυτές θα μπορούν να επαληθεύσουν άμεσα την εγκυρότητα και την ακεραιότητα των καταχωρημένων πληροφοριών, κάνοντας χρήση των έμφυτων χαρακτηριστικών που διαθέτει η τεχνολογία Blockchain. Η επαλήθευση αυτή θα μπορεί να γίνει με διάφανο τρόπο, είτε από άλλα εκπαιδευτικά ιδρύματα, είτε από κάποιους υποψήφιους εργοδότες. Τέτοια συστήματα καταγραφής και επαλήθευσης τίτλων έχουν ήδη προταθεί, όμως υπάρχει ανάγκη για εκτεταμένη αποδοχή τέτοιων συστημάτων, έτσι ώστε να εξασφαλιστεί η σωστή τους λειτουργία σε ολόκληρο τον χώρο της Εκπαίδευσης.
2. **Καταγραφή και επαλήθευση επιδόσεων σπουδαστών και πιστοποιητικών γνώσης.** Οι σπουδαστές ενός εκπαιδευτικού κατά κανόνα παρακολουθούν κάποια μαθήματα, υποβάλλουν εργασίες και συμμετέχουν σε εξετάσεις, ενώ πολλές φορές εκδίδονται από τους εκπαιδευτικούς φορείς πιστοποιητικά που αφορούν κάποιο μαθησιακό αντικείμενο και πιστοποιούν τις γνώσεις που απέκτησαν οι σπουδαστές. Οι επιδόσεις των μαθητών/φοιτητών και τα πιστοποιητικά γνώσης που

έχουν αποκτήσει, μπορούν να καταγράφονται σε ένα σύστημα που βασίζεται στην τεχνολογία Blockchain, έτσι ώστε να είναι δυνατή η επαλήθευσή τους από άλλους φορείς.

3. **Καταγραφή και επαλήθευση βιογραφικού σημειώματος.** Το βιογραφικό σημείωμα από το εκπαιδευτικό προσωπικό και τους φοιτητές ενός εκπαιδευτικού ιδρύματος μπορεί να χρησιμοποιηθεί για την πρόσληψή τους από κάποιον άλλον εργοδότη ή την αποδοχή τους από έναν άλλο εκπαιδευτικό φορέα. Είναι σημαντική επομένως η επαλήθευση όλων των στοιχείων τα οποία περιλαμβάνονται συνήθως σε ένα βιογραφικό σημείωμα. Η ανάπτυξη συστημάτων για την οργάνωση, καταχώρηση και επαλήθευση βιογραφικών σημειωμάτων είναι σημαντική και μπορεί να γίνει πολύ αποδοτικά και με διάφανο τρόπο με τη βοήθεια της τεχνολογίας Blockchain.
4. **Καταχώρηση ερευνητικών εργασιών.** Η έρευνα αποτελεί έναν αναπόσπαστο και πολύ σημαντικό τομέα στον χώρο της ανώτατης εκπαίδευσης. Το ερευνητικό προσωπικό των πανεπιστημίων, αλλά και άλλων ερευνητικών ιδρυμάτων, σε όλον τον κόσμο κάθε χρόνο δημοσιεύουν πολλές ερευνητικές εργασίες στις οποίες παρουσιάζονται και αναλύονται ερευνητικές προτάσεις και καινοτόμες ιδέες. Είναι σημαντικό οι ερευνητικές αυτές εργασίες να μπορούν να επαληθευτούν, τόσο ως προς τους ερευνητές που έχουν λάβει μέρος σε αυτές, όσο και ως προς το περιεχόμενό τους και τις προτάσεις τους. Η καταχώρηση και η επαλήθευση των ερευνητικών δημοσιεύσεων και η εξασφάλιση από περιπτώσεις λογοκλοπής, θα μπορούσε να γίνει με την χρήση ενός κατακευκαμένου συστήματος, βασισμένο στην τεχνολογία Blockchain, το οποίο θα προσφέρει εκτός των άλλων και την εξασφάλιση δικαιωμάτων καινοτόμων ιδεών. Σε ένα τέτοιο σύστημα, θα πρέπει να έχει εκτεταμένη αποδοχή και να συμμετέχει σε αυτό το σύνολο των ερευνητικών ιδρυμάτων.
5. **Διανομή διδακτικού υλικού.** Η λογοκλοπή αποτελεί ένα από τα σημαντικότερα προβλήματα που παρουσιάζονται κατά τη διανομή εκπαιδευτικού υλικού. Η διανομή εκπαιδευτικού υλικού θα μπορούσε να γίνεται από ειδικές πλατφόρμες, βασισμένες σε τεχνολογία Blockchain, με τη βοήθεια των οποίων θα μπορεί με εύκολο και διάφανο τρόπο να γίνει επαλήθευση του δημιουργού του υλικού αυτού.

6. **Υλοποίηση εξ αποστάσεως μαθημάτων.** Κατά τα τελευταία χρόνια έχει αυξηθεί κατακόρυφα η προσφορά προγραμμάτων σποδών και σεμιναρίων τα οποία προσφέρονται εξ' αποστάσεως. Οι εκπαιδευτικού φορείς προσφέρουν πληθώρα προγραμμάτων που περιλαμβάνουν εξ' αποστάσεως διδασκαλία. Ειδικά σε περιπτώσεις πανδημίας, όπως στην περίπτωση της πανδημίας Covid-19, η εξ' αποστάσεως διδασκαλία αποτελεί πολύ καλή λύση και μονόδρομο για την αποφυγή άσκοπων μετακινήσεων. Οι πλατφόρμες οι οποίες αναπτύσσονται από τους εκπαιδευτικούς φορείς μπορεί να λειτουργήσει με τη βοήθεια της τεχνολογίας Blockchain, έτσι ώστε να είναι δυνατή η εξασφάλιση της αξιοπιστίας των προγραμμάτων αυτών μέσω της επαλήθευσης της συμμετοχής των καταρτιζόμενων αλλά και του υλικού που διανέμεται σε αυτούς.
7. **Ανταλλαγή φοιτητών ανάμεσα σε ανώτατα εκπαιδευτικά ιδρύματα.** Τα εκπαιδευτικά ιδρύματα πολλές φορές συνεργάζονται και υποστηρίζουν προγράμματα ανταλλαγής φοιτητών. Στα πλαίσια της συνεργασίας αυτού του είδους, προσφέρεται η δυνατότητα στους φοιτητές να μεταφέρουν μονάδες πιστοποίησης από ένα πρόγραμμα σπουδών σε ένα άλλο. Για την πιστοποίηση της συμμετοχής των φοιτητών σε κάποιο πρόγραμμα ενός ανώτατου ιδρύματος, μπορεί να γίνει χρήση συστημάτων επαλήθευσης των συμμετοχών και των μονάδων πιστοποίησης που μεταφέρονται, τα οποία θα κάνουν χρήση της τεχνολογίας Blockchain.
8. **Καταγραφή και διαχείριση πόρων.** Η τεχνολογία Blockchain μπορεί να φανεί χρήσιμη και σε επίπεδο διαχείρισης των πόρων ενός εκπαιδευτικού ιδρύματος. Τα ιδρύματα αυτά διαθέτουν συνήθως αρκετούς πόρους, τόσο σε φυσική, όσο και σε ψηφιακή μορφή. Η καταχώρηση και η διαχείριση των πόρων αυτών θα μπορούσε να γίνει με τη βοήθεια συστημάτων που βασίζονται στην τεχνολογία Blockchain, έτσι ώστε να είναι εύκολη η επιβεβαίωση των πόρων αυτών και να μην είναι δυνατή η κακόβουλη διαγραφή ή τροποποίηση των δεδομένων που αφορούν τους πόρους αυτούς. Για παράδειγμα, λειτουργίες όπως η παραλαβή υλικού ή η καταστροφή υλικού θα μπορούσαν να γίνονται με τη βοήθεια ενός τέτοιου συστήματος.
9. **Καταγραφή εργασιών και projects.** Η καταχώρηση συμμετοχών του

διδασκτικού προσωπικού και των μαθητών/φοιτητών σε διαφόρων τύπων εργασίες και projects ενός εκπαιδευτικού φορέα θα μπορούσε να γίνει με τη βοήθεια κάποιας ειδικής πλατφόρμας η οποία βασίζεται στην τεχνολογία Blockchain. Θα μπορεί με τον τρόπο αυτόν να γίνει επαλήθευση της συμμετοχής τους, αλλά και των αποτελεσμάτων-παραδοτέων των project αυτών.

Κάποιες από τις βασικότερες πιθανές χρήσεις της τεχνολογίας Blockchain στον χώρο της Εκπαίδευσης αποτυπώθηκαν στην πιο πάνω λίστα. Η λίστα αυτή δεν είναι φυσικά περιοριστική και οι χρήσεις της τεχνολογίας Blockchain θα μπορούσαν να είναι πολύ περισσότερες. Τα χαρακτηριστικά της τεχνολογίας αυτής μπορούν να προσφέρουν σημαντικές λύσεις σε διάφορα προβλήματα της εκπαίδευσης παγκοσμίως. Ήδη υπάρχουν πολλές ερευνητικές εργασίες που εξετάζουν τις δυνατότητες αυτές και έχουν υλοποιηθεί κάποια συστήματα και εκπαιδευτικές πλατφόρμες που κάνουν χρήση της τεχνολογίας Blockchain, θα πρέπει όμως να υπάρξει συνολική αποδοχή έτσι ώστε να δοθούν καθολικές και καινοτόμες λύσεις.

1.3 Σκοπός και στόχοι της εργασίας

Ο σκοπός της παρούσας πτυχιακής εργασίας είναι να μελετήσει τα χαρακτηριστικά εκείνα της τεχνολογίας Blockchain τα οποία μπορούν να αποδειχθούν χρήσιμα στον χώρο της Εκπαίδευσης και τις χρήσεις που μπορεί να έχει η τεχνολογία αυτή. Στα πλαίσια της εργασίας, εξετάζονται και κάποια εργαλεία ανοικτού κώδικα, όπως είναι το HyperLedger Fabric, τα οποία μπορούν να χρησιμοποιηθούν για την ανάπτυξη εφαρμογών Blockchain στην Εκπαίδευση.

Οι επιμέρους στόχοι της εργασίας είναι:

- Ανάλυση των χαρακτηριστικών της τεχνολογίας Blockchain τα οποία είναι χρήσιμα για την ανάπτυξη εκπαιδευτικών εφαρμογών.
- Παρουσίαση κάποιων βασικών χρήσεων που μπορεί να έχει η τεχνολογία Blockchain στον χώρο της Εκπαίδευσης.
- Μελέτη της σχετικής έρευνας και κάποιων υλοποιήσεων που έχουν πραγματοποιηθεί κατά τα πρόσφατα χρόνια.
- Παρουσίαση κάποιων προγραμματιστικών εργαλείων ανοικτού κώδικα τα

οποία μπορούν να χρησιμοποιηθούν για την ανάπτυξη εφαρμογών Blockchain για τον χώρο της Εκπαίδευσης, όπως είναι το HyperLedger Fabric.

- Ανάπτυξη ενός απλού συστήματος για την επαλήθευση τίτλων με τη βοήθεια των εργαλείων του HyperLedger Fabric και της γλώσσας προγραμματισμού Javascript.
- Εξαγωγή κάποιων χρήσιμων συμπερασμάτων σχετικά με το μέλλον της τεχνολογίας Blockchain και τις χρήσεις τις οποίες μπορεί να έχει στην Εκπαίδευση.

Στο κεφάλαιο 2 παρουσιάζονται τα βασικά χαρακτηριστικά της τεχνολογίας Blockchain και περιγράφονται κάποιες από τις χρήσεις της τεχνολογίας αυτής στον χώρο της Εκπαίδευσης. Παρουσιάζεται επίσης σχετική έρευνα και υλοποιήσεις που έχουν πραγματοποιηθεί προς την κατεύθυνση αυτή. Στο κεφάλαιο 3 παρουσιάζονται κάποια από τα προγραμματιστικά εργαλεία ανοικτού κώδικα τα οποία μπορούν να χρησιμοποιηθούν για την ανάλυση και υλοποίηση μίας εφαρμογής Blockchain.

Στο κεφάλαιο 4 παρουσιάζεται ένα απλό σύστημα που αναπτύχθηκε πειραματικά για την επαλήθευση τίτλων. Το σύστημα κάνει χρήση της τεχνολογίας Blockchain για την καταχώρηση και επαλήθευση τίτλων που έχουν εκδοθεί από ένα εκπαιδευτικό ίδρυμα. Τέλος, στο κεφάλαιο 5 εξάγονται κάποια χρήσιμα συμπεράσματα από την εκπόνηση της εργασίας και της μελέτης που πραγματοποιήθηκε στις προηγούμενες ενότητες.

Κεφάλαιο 2^ο

2. Χαρακτηριστικά της τεχνολογίας Blockchain και η χρήση τους για την ανάπτυξη εφαρμογών στην Εκπαίδευση

2.1 Περιγραφή και χαρακτηριστικά της τεχνολογίας Blockchain

Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία κατακευμαμένων συστημάτων, τα οποία μπορεί να είναι δημόσια ή ιδιωτικά και περιλαμβάνουν καταγραφή καταχωρήσεων (ledger) από ομαδοποιημένες εγγραφές που καλούνται blocks, με τέτοιο τρόπο ώστε ένα block να μην είναι δυνατόν να μεταβληθεί εκ των υστέρων.

Η αρχιτεκτονική ενός συστήματος Blockchain αποτελείται από τα πιο κάτω συστατικά στοιχεία:

- **Υλικό υποδομής (infrastructure).** Είναι το υλικό όπου εκτελείται η εφαρμογή που υλοποιεί το Blockchain. Το υλικό αυτό είναι συνήθως κατακευμαμένο σε διαφορετικές τοποθεσίες.
- **Δίκτυο.** Υλοποιεί τις υπηρεσίες ανταλλαγής μηνυμάτων ανάμεσα στα εμπλεκόμενα μέρη και την υπηρεσία επαλήθευσης των καταχωρημένων συναλλαγών.
- **Πρωτόκολλο συναίνεσης (consensus protocol).** Ένα σύστημα Blockchain χρησιμοποιεί πρωτόκολλα όπως το Proof of Work (PoW) ή το Proof of Stake (PoS) για την καταγραφή νέων δεδομένων στην αλυσίδα και την επαλήθευσή των προηγούμενων. Υπάρχουν διάφοροι μηχανισμοί συναίνεσης που χρησιμοποιούνται σε διαφορετικά δίκτυα Blockchain. Το κοινό τους στοιχείο είναι ότι οι μηχανισμοί αυτοί αναλαμβάνουν την επαλήθευση μία συναλλαγής έτσι ώστε να εισαχθεί στην αλυσίδα συναλλαγών.
- **Δεδομένα.** Τα δεδομένα καταχωρούνται στα blocks της αλυσίδας και περιλαμβάνουν τα στοιχεία για τις συναλλαγές που πραγματοποιούνται.

- **Εφαρμογή.** Αποτελεί το λογισμικό για την υποστήριξη των υπηρεσιών του συστήματος. Περιλαμβάνει κώδικα για την δημιουργία νέων blocks στην αλυσίδα και την υλοποίηση του μηχανισμού συναίνεσης, κώδικα για τα έξυπνα συμβόλαια ανάμεσα στα συμβαλλόμενα μέρη και τη διαχείρισή τους κλπ.

Κάθε block που προστίθεται στην αλυσίδα υπογράφεται ψηφιακά και περιλαμβάνει, πέρα από τις πληροφορίες που πρέπει να καταχωρηθούν, επιπρόσθετες κρυπτογραφημένες πληροφορίες για την επαλήθευση της εγκυρότητας του προηγούμενου block της αλυσίδας, το οποίο επαληθεύει την εγκυρότητα του πιο προηγούμενου κ.ο.κ. Με τον τρόπο αυτόν σχηματίζεται η αλυσίδα blockchain, η οποία ξεκινά από το δημιουργό block (genesis block) ή το block-0 όπως συχνά αναφέρεται. Κάποιες φορές μπορούν να δημιουργηθούν διακλαδώσεις (forks) της αλυσίδας. Κάτι τέτοιο μπορεί να συμβεί όταν γίνονται για παράδειγμα μεταβολές στο πρωτόκολλο λειτουργίας του δικτύου ή προστίθενται νέες λειτουργίες. Όταν συμβεί κάτι τέτοιο, δημιουργείται μία δεύτερη αλυσίδα από νέα blocks, η οποία μοιράζεται το "ιστορικό" με την αρχική έκδοση της αλυσίδας. Αν μάλιστα δεν υπάρχει συμβατότητα ανάμεσα στις δύο διακλαδώσεις και οι χρήστες θα πρέπει υποχρεωτικά να κάνουν αναβάθμιση του λογισμικού τους, τότε η διακλάδωση αναφέρεται και σαν hard fork. Κάτι τέτοιο συνέβη για παράδειγμα στο δίκτυο Ethereum το 2016, όπου η αρχική έκδοσή του αναφέρεται ως Ethereum classic.

Ο χρόνος δημιουργίας ενός νέου block ονομάζεται block time και διαφέρει ανάλογα με το δίκτυο που χρησιμοποιείται και τους κανόνες που εφαρμόζονται σε αυτό. Για το δίκτυο Ethereum ο μέσος χρόνος για τη δημιουργία ενός block είναι περίπου 14-15 δευτερόλεπτα. Αντίθετα, για το δίκτυο Bitcoin ο αντίστοιχος χρόνος αντιστοιχεί σε περίπου 10 λεπτά.

Κάθε κόμβος στο δίκτυο peer-to-peer ενός κατακευματισμένου συστήματος Blockchain διατηρεί το δικό του αντίγραφο της αλυσίδας των καταχωρήσεων. Δεν υπάρχει κάποιου είδους επίσημη κεντρική οντότητα η οποία είναι υπεύθυνη για την αποθήκευση ενός επίσημου αντιγράφου της αλυσίδας δεδομένων. Κανένας χρήστης του δικτύου δεν θεωρείται πιο έμπιστος από κάποιον άλλον χρήστη.

Στο δίκτυο Bitcoin, για τη δημιουργία νέων blocks μπορεί να απαιτείται κάποια "απόδειξη" της προσπάθειας (Proof of Work – PoW) που έχει καταβάλει ένας

κόμβος για την επίλυση ενός ειδικού γρίφου και η διαδικασία αυτή αναφέρεται σαν εξόρυξη (mining). Επιλύοντας, έναν τέτοιο γρίφο ένας κόμβος επαληθεύει την εγκυρότητα κάποιων νέων συναλλαγών, κάτι που ισοδυναμεί με τη δημιουργία ενός νέου block συναλλαγών. Ο μηχανισμός Proof of Work αποτελεί έναν από τους μηχανισμούς συναίνεσης (consensus mechanisms) που χρησιμοποιούνται στα δίκτυα Blockchain και έχει το μειονέκτημα ότι απαιτεί μεγάλη κατανάλωση ενέργειας. Υπάρχουν άλλοι μηχανισμοί συναίνεσης, όπως ο μηχανισμός Proof of Stake (PoS), όπου η επαλήθευση των συναλλαγών γίνεται από επιλεγμένους κόμβους του δικτύου που καλούνται validators και επομένως υπάρχουν πολύ μικρότερες απαιτήσεις κατανάλωσης ενέργειας.

2.2 Δομή αλυσίδας Blockchain

Μία αλυσίδα blockchain, όπως περιγράφηκε στις προηγούμενες παραγράφους, αποτελείται από ένα σύνολο συνδεδεμένων μεταξύ τους blocks, όπου κάθε block επαληθεύει την ορθότητα των δεδομένων του προηγούμενου block. Η βασική δομή ενός block περιλαμβάνει τα πιο κάτω πεδία [9]:

- Το κρυπτογραφικό αποτύπωμα για το προηγούμενο block (previous block hash). Κατά τη δημιουργία ενός νέου block, εφαρμόζεται μία κρυπτογραφική συνάρτηση κατακερματισμού (hash function) με είσοδο τα δεδομένα του προηγούμενου block και επαληθεύει πρακτικά την εγκυρότητά του.
- Το κρυπτογραφικό αποτύπωμα για τις συναλλαγές που θα καταχωρηθούν στο νέο block. Στην περίπτωση αυτή εφαρμόζεται και πάλι μία συνάρτηση κατακερματισμού, αλλά σαν είσοδο στη συνάρτηση αυτή έχουμε τα δεδομένα των συναλλαγών που περιλαμβάνονται στο νέο (τρέχον) block της αλυσίδας.
- Την χρονοσφραγίδα (timestamp) για το νέο block. Είναι ο αριθμός των δευτερολέπτων που έχουν περάσει από την 1^η Ιανουαρίου του 1970 και αντιστοιχεί στον χρόνο δημιουργίας του νέου block.
- Έναν επιπρόσθετο κρυπτογραφικό κωδικό (cryptographic nonce). Πρόκειται για έναν κρυπτογραφικό αριθμό που σχηματίζεται με τέτοιο τρόπο έτσι ώστε κατά την εφαρμογή μίας συνάρτησης κατακερματισμού στα 4 πρώτα πεδία του block (συμπεριλαμβανομένου του nonce), παράγεται ως έξοδος η τιμή του πέμπτου πεδίου του block (το οποίο

περιγράφεται αμέσως μετά). Ο όρος "nonce" αναφέρεται στην φράση "number used once" και ο κωδικός αυτός χρησιμοποιείται κατά τη διαδικασία της εξόρυξης για την επαλήθευση των νέων blocks της αλυσίδας (μηχανισμός Proof of Work).

- Το κρυπτογραφικό αποτύπωμα για το τρέχον block (current block hash). Στην περίπτωση αυτή εφαρμόζεται και πάλι μία συνάρτηση κατακερματισμού, αλλά σαν είσοδο στη συνάρτηση αυτή έχουμε το σύνολο των πληροφοριών που περιλαμβάνονται στο νέο (τρέχον) block της αλυσίδας.

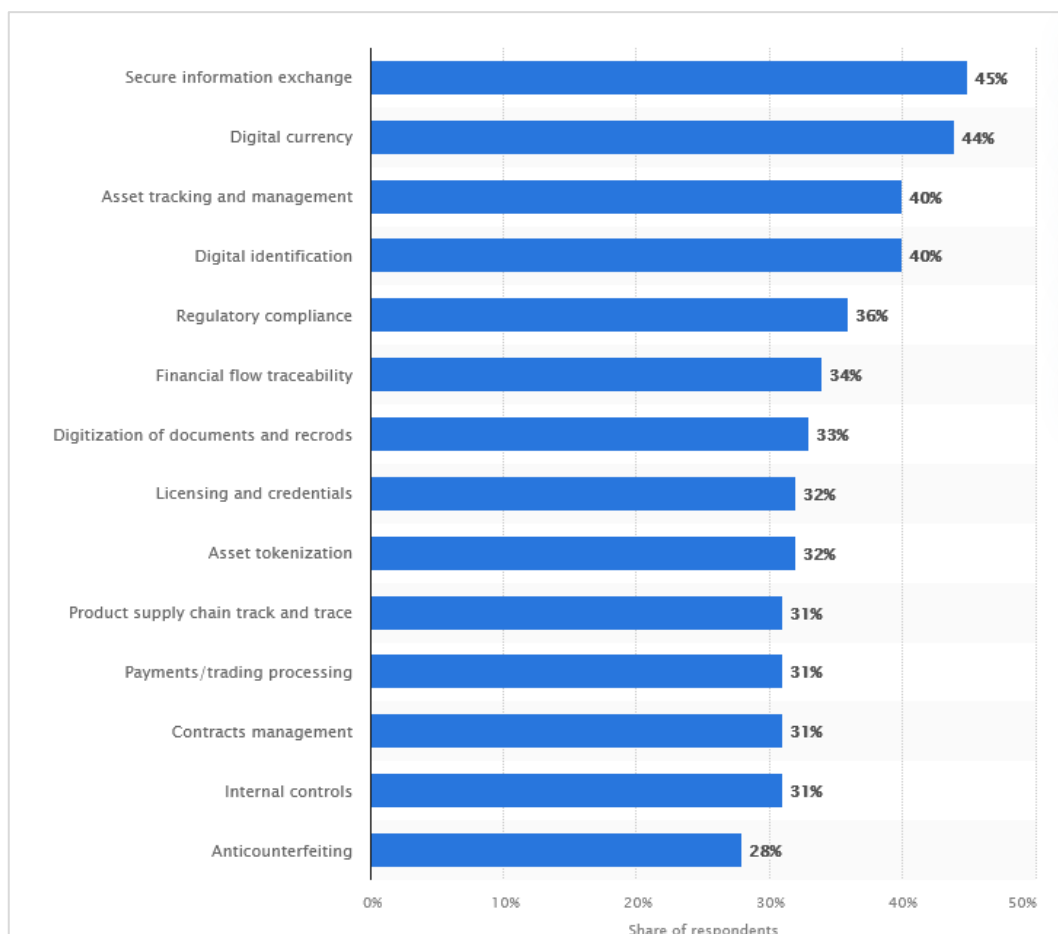
2.3 Εφαρμογές και πλεονεκτήματα της τεχνολογίας Blockchain

Οι εφαρμογές που κάνουν χρήση της τεχνολογίας Blockchain συνήθως βασίζονται σε ένα δίκτυο peer-to-peer (P2P) στο οποίο οι συμμετέχοντες μπορούν να κάνουν επαλήθευση των δεδομένων που καταχωρούνται σε μορφή αλυσίδας από blocks. Για την καταχώρηση ενός νέου block θα πρέπει να υπάρξει συμφωνία ανάμεσα στα μέλη του δικτύου και να καταγραφούν τα αντίστοιχα δεδομένα, όπως και ο χρόνος δημιουργίας του block (timestamp). Θα πρέπει να γίνει επαλήθευση επίσης του προηγούμενου block της αλυσίδας. Με τον τρόπο αυτόν, γίνεται συνεχής επαλήθευση των δεδομένων της αλυσίδας, γεγονός που εγγυάται για την ασφάλεια των συναλλαγών που καταχωρούνται και για την ακεραιότητα των δεδομένων.

Η συνολική χωρητικότητα των δεδομένων που αποθηκεύονται σε ένα δίκτυο Blockchain μπορεί να είναι πολύ μεγάλη και ένα από τα πλεονεκτήματα της τεχνολογίας αυτής είναι η δυνατότητες κλιμάκωσης που προσφέρει (scaling). Τον Αύγουστο του 2024 στο δίκτυο του Bitcoin υπήρχαν δεδομένα για συναλλαγές συνολικού μεγέθους 20 GB, ενώ το 2020 το αντίστοιχο μέγεθος ήταν της τάξης των 200 GB [5]. Επίσης, η χρήση της τεχνολογίας Blockchain αναμένεται να αυξηθεί κατά πολύ τα επόμενα χρόνια. Υπάρχει πρόβλεψη ότι η αγορά Blockchain μέχρι το 2030 θα αγγίξει τα 1.431 δισεκατομμύρια δολάρια, ενώ το 2022 υπήρχαν 83.434.000 περίπου χρήστες της τεχνολογίας που ήταν κάτοχοι ψηφιακών πορτοφολιών (digital wallets) [6]. Το 60% των υπευθύνων πληροφορικής (Chief Information Officers – CIOs) στις μεγάλες εταιρείες σκέφτονται σοβαρά την χρήση της τεχνολογίας Blockchain

Η τεχνολογία Blockchain προσφέρει τέτοια χαρακτηριστικά ώστε η χρήση της σε διάφορους τομείς να προσφέρει μεγάλα πλεονεκτήματα και κέρδη. Υπολογίζεται ότι η χρήση Blockchain μπορεί να μειώσει κατά 30% τα έξοδα στον τραπεζικό χώρο, κάτι που μεταφράζεται σε κέρδος μεγαλύτερο από 10 δισεκατομμύρια δολάρια, ενώ στο κοντινό μέλλον το 55% των υπηρεσιών υγείας θα κάνει χρήση συστημάτων που βασίζονται στο Blockchain [6].

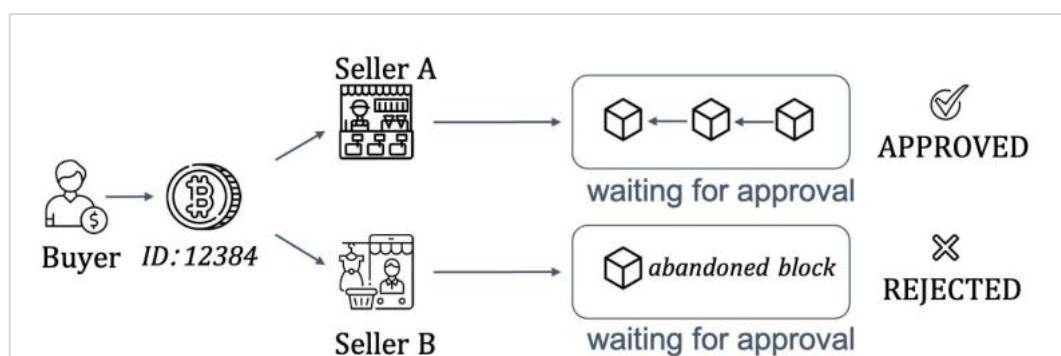
Στην Εικόνα 1 φαίνονται οι σημαντικότερες χρήσεις της τεχνολογίας Blockchain από οργανισμούς και ιδιωτικές εταιρείες σε όλον τον κόσμο για το 2021 [7]. Παρατηρούμε ότι το Blockchain χρησιμοποιείται σε πολύ μεγάλο βαθμό για την ασφαλή ανταλλαγή πληροφοριών, για την απόκτηση και μεταφορά κρυπτονομισμάτων, για τη διαχείριση και ιχνηλάτηση περιουσιακών στοιχείων και για περιπτώσεις έκδοσης ψηφιακών αναγνωριστικών. Χρησιμοποιείται όμως και για διάφορους άλλους σκοπούς (Εικόνα 1).



Εικόνα 1: Χρήσεις της τεχνολογίας Blockchain (Statista, [7])

Ένα από τα πρώτα προβλήματα που κλήθηκε να αντιμετωπίσει η τεχνολογία Blockchain με τη δημιουργία του Bitcoin, ήταν η αποφυγή των διπλοπληρωμών (double-spending problem) χωρίς τη χρήση κάποιου κεντρικού ελέγχου. Το

πρόβλημα αυτό προκύπτει όταν ο κάτοχος ενός ψηφιακού πορτοφολιού καταφέρει να χρησιμοποιήσει τα ίδια χρήματα για την πραγματοποίηση δύο ή και περισσότερων αγορών. Το δίκτυο Bitcoin επιτυγχάνει την αποφυγή διπλοπληρωμών με τον μηχανισμό συναίνεσης που χρησιμοποιεί [1], όπως φαίνεται στην Εικόνα 2. Στην εικόνα φαίνεται μία περίπτωση όπου ένας αγοραστής προσπαθεί να ξοδέψει τα ίδια κρυπτονομίσματα για να κάνει δύο διαφορετικές αγορές, από τον αγοραστή A και τον αγοραστή B. Ο μηχανισμός συναίνεσης εγκρίνει την μία μόνο συναλλαγή, αυτήν με τον αγοραστή A, ενώ η άλλη απορρίπτεται και το block εγκαταλείπεται (abandoned block).



Εικόνα 2: Αποφυγή διπλοπληρωμών

Τα σημαντικότερα κέρδη από την χρήση της τεχνολογίας Blockchain από έναν οργανισμό ή εταιρεία είναι τα πιο κάτω [8]:

- **Αύξηση αξιοπιστίας.** Η χρήση της τεχνολογίας Blockchain μπορεί να βοηθήσει στην αύξηση της εμπιστοσύνης ανάμεσα σε οντότητες οι οποίες συνδιαλλάσσονται μεταξύ τους, ειδικά για τις περιπτώσεις όπου έχουμε εμπλεκόμενα μέρη τα οποία δεν γνωρίζονται μεταξύ τους και δεν υπάρχουν άλλοι τρόποι για την εγγύηση της αξιοπιστίας τους.
- **Εξάλειψη της ανάγκης ύπαρξης κεντρικού ελέγχου.** Με τη χρήση της τεχνολογίας Blockchain δεν υπάρχει η ανάγκη ύπαρξης μίας κεντρικής δομής για τον έλεγχο των πληροφοριών που διακινούνται, κάτι που μπορεί να βοηθήσει στην αποκέντρωση των υπηρεσιών που προσφέρει μία εταιρεία ή οργανισμός.
- **Αυξημένη ασφάλεια και ιδιωτικότητα.** Η τεχνολογία Blockchain κάνει χρήση ισχυρών αλγόριθμων κρυπτογράφησης και συναρτήσεων κατακερματισμού (hash functions) για την αποθήκευση και την

επαλήθευση των δεδομένων. Χρησιμοποιείται επίσης κατά κανόνα από ένα δίκτυο πολλών κόμβων οι οποίοι είναι σε θέση να κάνουν ανά πάσα στιγμή επαλήθευση μίας συναλλαγής. Με τους πιο πάνω τρόπους, οι εφαρμογές Blockchain προφέρουν αυξημένη ασφάλεια και μπορούν να εγγυηθούν την ιδιωτικότητα των εμπλεκόμενων μερών.

- **Μείωση κόστους.** Η χρήση της τεχνολογίας Blockchain μπορεί να μειώσει δραστικά τα κόστη συλλογής, καταχώρησης και επαλήθευσης των δεδομένων που χρησιμοποιούνται από έναν οργανισμό ή εταιρεία και είναι ευκολότερη η εξαγωγή αναφορών.
- **Ταχύτητα.** Η ταχύτητα για την ολοκλήρωση των συναλλαγών σε σχέση με άλλους παραδοσιακούς τρόπους μπορεί να είναι σημαντικά μεγαλύτερη. Για παράδειγμα, για την μεταφορά χρηματικών ποσών με τον παραδοσιακό τρόπο μέσω του υπάρχοντος τραπεζικού συστήματος μπορεί να απαιτείται μεγάλος χρόνος, όμως μέσω εφαρμογών Blockchain, όπως π.χ. γίνεται με τα κρυπτονομίσματα, ο χρόνος που απαιτείται είναι σημαντικά μικρότερος.
- **Δυνατότητα ιχνηλάτησης συναλλαγών.** Με τη χρήση της τεχνολογίας Blockchain είναι εφικτή η πλήρης ιχνηλάτηση των συναλλαγών που έχουν πραγματοποιηθεί με διάφανο τρόπο. Σε περιπτώσεις όπου έχουμε διαδοχικές συναλλαγές που μπορεί να επεκτείνονται σε βάθος χρόνου, μία τέτοιου είδους ιχνηλάτηση δεν είναι καθόλου εύκολη, με την χρήση όμως της τεχνολογίας Blockchain είναι πλέον εφικτή.
- **Μονιμότητα καταγεγραμμένων δεδομένων και συναλλαγών.** Τα δεδομένα και οι συναλλαγές που καταγράφονται με τη βοήθεια της τεχνολογίας Blockchain δεν μπορούν να τροποποιηθούν εκ των υστέρων. Για παράδειγμα, όταν πιστοποιηθεί η κατοχή ενός φυσικού ή ψηφιακού πόρου από κάποιον χρήστη, στη συνέχεια μπορεί να γίνει μόνο μεταβίβαση του πόρου αυτού, όμως δεν μπορεί να αμφισβητηθεί το γεγονός ότι κάποια συγκεκριμένη χρονική στιγμή έγινε συναλλαγή με την οποία ο χρήστης απέκτησε τον συγκεκριμένο πόρο.
- **Δυνατότητα ελέγχου από τον τελικό χρήστη των δεδομένων που τον αφορούν.** Η τεχνολογία Blockchain μπορεί να δώσει τη δυνατότητα στον τελικό χρήστη να διαχειριστεί ο ίδιος τα δεδομένα τα οποία τον αφορούν, αφού μπορεί να έχει άμεση πρόσβαση σε αυτά, χωρίς τη διαμεσολάβηση κάποιου κεντρικού φορέα.

- **Καινοτομία.** Με την χρήση της τεχνολογίας Blockchain μπορούν οι διάφοροι φορείς να υλοποιήσουν καινοτόμες λύσεις και υπηρεσίες για να αντιμετωπίσουν τα πιθανά εμπόδια και δυσκολίες κατά τη λειτουργία τους.

2.4 Σχετική έρευνα

Έχουμε πραγματοποιηθεί διάφορες ερευνητικές εργασίες για τη χρησιμότητα της τεχνολογίας Blockchain στην Εκπαίδευση και όλες καταλήγουν στο συμπέρασμα ότι η τεχνολογία Blockchain μπορεί να βοηθήσει σημαντικά και να δώσει επαναστατικές λύσεις σε πολλά από τα προβλήματα που υπάρχουν στον χώρο αυτόν [10], [11]. Σε αρκετές από αυτές τις έρευνες εξετάζεται η προοπτική δημιουργίας συστημάτων για την επαλήθευση ακαδημαϊκών τίτλων, χωρίς όμως να προτείνουν συγκεκριμένες υλοποιήσεις και πρακτικές [10].

Οι Alammery et al μελέτησαν τις χρήσεις που μπορεί να έχει η τεχνολογία Blockchain στην εκπαίδευση, τα κέρδη που μπορούν να προκύψουν και πιθανές εμπλοκές που μπορούν να παρουσιαστούν [12]. Δεν αναφέρουν όμως τρόπους με τους οποίους η τεχνολογία Blockchain θα μπορούσε να ενσωματωθεί και να συνεργαστεί με υπάρχοντα πληροφοριακή συστήματα που λειτουργούν στα διάφορα εκπαιδευτικά ιδρύματα. Οι Kamisalic et al. κατηγοριοποίησαν τις έρευνες που έχουν γίνει πάνω στη χρήση της τεχνολογίας Blockchain από εκπαιδευτικά ιδρύματα ανώτατης εκπαίδευσης [13].

Οι Cheng et al παρουσίασαν ένα σύστημα για την έκδοση και επαλήθευση πιστοποιητικών σπουδών με τη χρήση τεχνολογίας Blockchain και έξυπνων συμβολαίων (smart contracts) [14]. Το σύστημά τους αποτελείται από τρεις οντότητες: τον φορέα που εκδίδει το πιστοποιητικό, τον φοιτητή ή την εταιρεία που θέλει να κάνει επαλήθευση του πιστοποιητικού και τον πάροχο της υπηρεσίας. Οι μαθητές/φοιτητές λαμβάνουν ένα ηλεκτρονικό πιστοποιητικό που περιλαμβάνει QR-code για την επαλήθευσή του, όπως επίσης και πληροφορίες για την πρόσβαση στα δεδομένα του πιστοποιητικού.

Οι Duan et al παρουσίασαν το πρωτότυπο για ένα σύστημα που χρησιμοποιήθηκε ως proof of concept σε μία ομάδα φοιτητών στο πανεπιστήμιο Xiangtan το 2017 [15]. Με τον όρο proof of concept (PoC) αναφερόμαστε στη διαδικασία εκείνη όπου εξετάζεται και επιδεικνύεται η δυνατότητα υλοποίησης ενός συστήματος,

αποδεικνύοντας έτσι ότι μία ιδέα μπορεί να εφαρμοστεί στην πραγματικότητα. Οι Gresch et al πρότειναν το 2019 μία εξειδικευμένη λύση για το πανεπιστήμιο της Ζυρίχης, παρουσιάζοντας ένα απλό μοντέλο το οποίο βασίζεται στην τεχνολογία Blockchain και τα έξυπνα συμβόλαια και μπορεί να χρησιμοποιηθεί για την έκδοση και επαλήθευση διπλωμάτων, απλοποιώντας τις σύνθετες διαδικασίες που ακολουθούνται με τον παραδοσιακό τρόπο [16]. Ένα παρόμοιο σύστημα πρότειναν οι Vidal et al την ίδια περίπου περίοδο για την έκδοση πιστοποιητικών στο πανεπιστήμιο Fernando Pessoa στην Πορτογαλία και παρουσίασαν μετρικές σχετικά με τις επιδόσεις του συστήματος [17].

Οι San et al παρουσίασαν το 2019 ένα θεωρητικό μοντέλο για τη διαχείριση πιστοποιητικών και την επαλήθευσή τους [18]. Σύμφωνα με το μοντέλο αυτό, ο ιδιοκτήτης ενός πιστοποιητικού μπορεί να επιλέξει ποια στοιχεία θα περιλαμβάνονται στην προβολή του πιστοποιητικού. Το μοντέλο αυτό διαφέρει θεωρητικά με άλλα μοντέλα, όπως το μοντέλο Open Badges, επειδή κάνει χρήση δέντρων Merkle κατά τη δημιουργία των ψηφιακών πιστοποιητικών. Το μοντέλο μπορεί να χρησιμοποιηθεί και για τη διαχείριση και άλλου είδους πιστοποιητικά, εκτός από ακαδημαϊκά.

Ένα πρωτότυπο επαλήθευσης διπλωμάτων το οποίο βασίζεται στο πρότυπο Blockcerts προτάθηκε από τους Nikolskaia et al [19]. Το πρότυπο Blockcerts αποτελεί ένα ανοικτό πρότυπο για την έκδοση, προβολή και επαλήθευση πιστοποιητικών βασισμένα στη τεχνολογία Blockchain. Το πρότυπο σχεδιάστηκε από το Massachusetts Institute of Technology (MIT) Media Lab και αναπτύχθηκε περαιτέρω από την Learning Machine (τωρινή Hyland Credentials). Αρχικά το πρότυπο προτάθηκε το 2016 για το δίκτυο του Bitcoin, αλλά στη συνέχεια επεκτάθηκε και στο Ethereum, όπως και σε άλλα δίκτυα. Ένα πρωτότυπο για την επαλήθευση πιστοποιητικών που εκδίδονται από ανώτατα εκπαιδευτικά ιδρύματα, όπου εξετάζονται διάφορα θέματα που αφορούν την αποκέντρωση (decentralization) της υπηρεσίας παρουσιάστηκε το 2020 από τους Senarito et al [20]. Η υλοποίηση της αποκέντρωσης των υπηρεσιών δεν είναι ένα εύκολο ζήτημα σύμφωνα με τους συγγραφείς, επειδή δεν είναι κάτι αυτονόητο για την αρχιτεκτονική των συστημάτων που χρησιμοποιούνται από τα εκπαιδευτικά ιδρύματα και τους προγραμματιστές τους.

Οι Capece et al υλοποίησαν το 2021 ένα πιλοτικό σύστημα επαλήθευσης πιστοποιητικών για το πανεπιστήμιο Tor Vergata στην Ρώμη [21]. Το σύστημα

αυτό βασίζεται στο πρότυπο Blockcerts. Οι συγγραφείς εξέτασαν τρόπους για την αύξηση της εμπιστοσύνης και της ταχύτητας των λειτουργιών του συστήματος και κατέληξαν στο συμπέρασμα ότι οι φοιτητές είναι πρόθυμοι να αποδεχτούν τέτοιου είδους καινοτομίες.

Οι Meyliana et al παρουσίασαν ένα σύστημα για την αποτύπωση και επαλήθευση της πλήρους ακαδημαϊκής πορείας των φοιτητών σε πανεπιστήμια της Ινδονησίας [22]. Η εργασία τους δεν εξετάζει κάποια πολύ σημαντικά ζητήματα, όπως είναι η επεκτασιμότητα (scalability) του συστήματός που πρότειναν ή ο τρόπος διαμοιρασμού και η ιδιωτικότητα των πληροφοριών που καταχωρούνται στο σύστημα.

Τα στοιχεία τα οποία καταχωρούνται σε ένα σύστημα Blockchain δεν μπορούν να μεταβληθούν. Η ιδιότητα αυτή αποτελεί ένα από τα βασικά χαρακτηριστικά της τεχνολογίας Blockchain. Οι Vidal et al παρουσίασαν προτάσεις για την περίπτωση όπου είναι επιθυμητή η ανάκληση ενός πιστοποιητικού [23]. Λόγω της φύσης της τεχνολογίας Blockchain, αλλαγές όπως η ανάκληση πιστοποιητικών αποτελούν μεγάλες προκλήσεις και είναι θέματα που θα πρέπει να εξεταστούν προσεκτικά.

Μπορούμε να παρατηρήσουμε ότι πολλές ερευνητικές προτάσεις βασίζονται σε ανοικτά πρότυπα που έχουν δημιουργηθεί και αφορούν την έκδοση και επαλήθευση πιστοποιητικών. Το πρότυπο Blockcerts που περιγράφεται στις προηγούμενες παραγράφους δοκιμάστηκε σε διάφορα πανεπιστήμια, όπως το State University της Νότιας Κορέας, το πανεπιστήμιο Tor Vergata της Ρώμης και το πανεπιστήμιο Fernando Pessoa στο Πόρτο. Για το πρότυπο αυτό μάλιστα έχει δημιουργηθεί και μία εφαρμογή για κινητά, όπου ο φοιτητής αποθηκεύει ένα ψηφιακό πορτοφόλι και μπορεί να προβάλει ή να μοιραστεί με άλλους τα πιστοποιητικά του [25].

Το πρότυπο Blockcerts δεν είναι το μοναδικό πολλά υποσχόμενο ανοικτό πρότυπο. Το πανεπιστήμιο της Λευκωσίας ήταν από τα πρώτα ιδρύματα που σχεδίασαν μία λύση για την έκδοση πιστοποιητικών η οποία βασίζεται στο δίκτυο Bitcoin [26]. Μάλιστα, το πανεπιστήμιο αυτό υπήρξε το πρώτο το οποίο έκανε δεκτά Bitcoins για την πληρωμή των διδάκτρων.

Υπάρχουν και άλλα ιδρύματα, όπως το πανεπιστήμιο της Ζυρίχης, το πανεπιστήμιο της Λισαβώνας και το πανεπιστήμιο Ho Chi Minh City (HCMC)

στο Βιετνάμ, τα οποία έχουν προτείνει λύσεις οι οποίες βασίζονται στο δίκτυο Ethereum [27]. Το δίκτυο Ethereum έχει παρόμοια χαρακτηριστικά με το δίκτυο Bitcoin, αφού προσφέρει ασφάλεια και διαφάνεια στις συναλλαγές, όμως δίνει τη δυνατότητα για τη σύναψη έξυπνων συμβολαίων. Στην πραγματικότητα και το δίκτυο Bitcoin έχει κάποιες δυνατότητες δημιουργίας έξυπνων συμβολαίων, αλλά το δίκτυο Ethereum έχει σχεδιαστεί ειδικά προς την κατεύθυνση αυτή και μπορεί να χρησιμοποιηθεί για τη δημιουργία σύνθετων έξυπνων συμβολαίων.

Από την έρευνα που έχει γίνει στον χώρο της Εκπαίδευσης σχετικά με την επαλήθευση πιστοποιητικών με τη βοήθεια της τεχνολογίας Blockchain, μπορούμε να καταλήξουμε στο συμπέρασμα ότι υπάρχει πολύ μεγάλο ενδιαφέρον από τους εκπαιδευτικούς φορείς για την ανάπτυξη τέτοιων συστημάτων. Ήδη έχουν αναπτυχθεί κάποια ανοικτά πρότυπα και έχουν υποβληθεί αρκετές προτάσεις, όμως υπάρχουν κάποια σημαντικά εμπόδια και δυσκολίες που θα πρέπει να αντιμετωπιστούν έτσι ώστε να υπάρξει ευρεία αποδοχή των λύσεων αυτών. Κάποια από τα σημαντικότερα εμπόδια και τις δυσκολίες περιγράφονται στην επόμενη παράγραφο.

2.5 Εμπόδια και δυσκολίες

Πάντοτε όταν πρόκειται για την μετάβαση του τρόπου λειτουργίας ενός συστήματος σε μία νέα τεχνολογία προκύπτουν προβλήματα και εμπόδια τα οποία θα πρέπει να ξεπεραστούν. Οι εκπαιδευτικοί φορείς έχουν ήδη πληροφοριακά συστήματα τα οποία είναι υπεύθυνα για την έκδοση πιστοποιητικών και διπλωμάτων και ακολουθούν συγκεκριμένες διαδικασίες για τον έλεγχο και την επαλήθευση αυτών των πιστοποιητικών. Η μετάβαση σε ένα νέο σύστημα λειτουργίας δεν είναι εύκολη.

Κάποια από τα σημαντικότερα προβλήματα, δυσκολίες και εμπόδια τα οποία θα πρέπει να αντιμετωπιστούν είναι τα εξής:

- **Κόστος της μετάβασης.** Το κόστος για τη δημιουργία και εγκατάσταση νέου λογισμικού δεν είναι πάντοτε αμελητέο ακόμη και όταν προτιμώνται ανοικτά πρότυπα και λογισμικό ανοικτού κώδικα. Πολλές φορές θα πρέπει να γίνει παραμετροποίηση του λογισμικού (software) και/ή προγραμματισμός κάποιων τμημάτων του. Μπορεί επίσης να χρειαστεί και νέο υλικό (hardware), το οποίο θα πρέπει να εγκατασταθεί και να

δοκιμαστεί σε συνδυασμό με το νέο λογισμικό.

- **Διαλειτουργικότητα και χρήση κοινών προτύπων.** Είναι πολύ σημαντική η συνεργασία ανάμεσα σε διαφορετικούς εκπαιδευτικούς φορείς και υποψήφιους εργοδότες. Θα πρέπει επομένως να ακολουθηθούν κοινά πρότυπα και πρωτόκολλα, τα οποία κατά προτίμηση θα είναι ανοικτά, έτσι ώστε να είναι δυνατή η συνεργασία ανάμεσα σε διαφορετικούς φορείς και διαφάνεια στις συναλλαγές. Θα πρέπει επίσης να αποφασιστούν θέματα που αφορούν τη λειτουργία του συστήματος και να υπάρχει μία κοινή πολιτική από όλους τους φορείς. Θα πρέπει να απαντηθούν ερωτήσεις όπως: Θα υπάρχει η δυνατότητα ανάκλησης ενός πιστοποιητικού και ποια θα είναι η διαδικασία για να γίνει αυτό; Θα υπάρχουν πιστοποιητικά με πολλαπλούς κατόχους; Θα μπορεί να επιλέγει ο ενδιαφερόμενος τα στοιχεία που επιθυμεί να εμφανίζονται πάνω σε κάποιο πιστοποιητικό;
- **Ιδιωτικότητα και ασφάλεια δεδομένων.** Κατά την ανταλλαγή δεδομένων ανάμεσα σε διαφορετικούς φορείς θα πρέπει να ληφθεί μέριμνα για την ιδιωτικότητα και την ασφάλεια κάποιων ευαίσθητων προσωπικών δεδομένων. Θα πρέπει να αποφασιστεί ποια δεδομένα θα πρέπει να εμφανίζονται κατά την προβολή ψηφιακών πιστοποιητικών, εάν θα φαίνεται η πλήρης πορεία του φοιτητή στις σπουδές του και οι βαθμολογίες του κλπ.
- **Ωριμότητα της τεχνολογίας.** Εκτός του ότι υπάρχουν πολλά πρότυπα και δίκτυα στον χώρο της τεχνολογίας Blockchain, πολλά από αυτά δεν έχουν "ωριμάσει" τεχνολογικά και δεν έχουν δοκιμαστεί σε ανάλογες υλοποιήσεις συστημάτων.
- **Αποδοχή από εκπαιδευτική κοινότητα.** Ένα νέο σύστημα της εμβέλειας αυτής θα πρέπει να τύχει αποδοχής από το σύνολο της εκπαιδευτικής κοινότητας. Πέρα από τις διοικήσεις και το προσωπικό των εκπαιδευτικών ιδρυμάτων, υπάρχουν και οι διδάσκοντες, οι μαθητές/φοιτητές του ιδρύματος κτλ. Καλά θα είναι να γίνει κατανοητός ο σκοπός της αλλαγής του συστήματος και να γίνει σαφές ότι δεν υπάρχουν κίνδυνοι ασφάλειας και διαρροής προσωπικών δεδομένων.
- **Εκπαίδευση προσωπικού και μαθητών/φοιτητών.** Για τη λειτουργία του νέου συστήματος θα πρέπει να γίνει εκπαίδευση όλων των εμπλεκόμενων στην νέα τεχνολογία. Η εκπαίδευση θα πρέπει να αφορά

θέματα όπως η διαχείριση ενός ψηφιακού πορτοφολιού (digital wallet) όπου περιλαμβάνονται τα ψηφιακά πιστοποιητικά, η διαδικασία επαλήθευσης ενός πιστοποιητικού κλπ.

- **Συνεργασία με τα υπάρχοντα πληροφοριακά συστήματα.** Οι εκπαιδευτικοί φορείς ήδη διαθέτουν πληροφοριακά συστήματα για τη λειτουργία τους. Τα πληροφοριακά αυτά συστήματα συχνά είναι πολύπλοκα και διαθέτουν πάρα πολλές λειτουργίες. Δεδομένα όπως τα στοιχεία φοιτητών, διδακτικού προσωπικού και μαθημάτων, βαθμολογίες σε εξεταστικές και εργασίες, συμμετοχές σε projects κλπ. είναι συνήθως αποθηκευμένα σε κάποια βάση δεδομένων, διαφορετική για το κάθε ίδρυμα. Είναι πολύ σημαντικό το νέο σύστημα να έχει τη δυνατότητα να συνεργάζεται με τα υπάρχοντα πληροφοριακά συστήματα και να είναι σε θέση να αντλεί στοιχεία από αυτά, κάτι που προφανώς έχει αρκετά μεγάλη πολυπλοκότητα.

Είδαμε πιο πάνω κάποιες από τις δυσκολίες και τα εμπόδια τα οποία θα πρέπει να ξεπεραστούν για τη λειτουργία ενός νέου συστήματος καταγραφής και επαλήθευσης ακαδημαϊκών πιστοποιητικών και διπλωμάτων το οποίο θα βασίζεται στην τεχνολογία Blockchain. Η τεχνολογία Blockchain είναι πολλά υποσχόμενη και αναμένεται να δώσει πολλές λύσεις στον χώρο της παιδείας γενικότερα, αλλά και ειδικότερα στην επαλήθευση τίτλων και πιστοποιητικών. Η μετάβαση όμως δεν θα είναι εύκολη, αφού θα πρέπει να ξεπεραστούν αρκετά μεγάλα εμπόδια.

Κεφάλαιο 3^ο

3. Ανάπτυξη Blockchain για την υποστήριξη εκπαιδευτικών αναγκών

3.1 Τρόπος λειτουργίας ενός δικτύου Blockchain

Γενικά ένα δίκτυο Blockchain αποτελεί ένα δίκτυο κόμβων που επικοινωνούν μεταξύ τους, χωρίς να υπάρχει ένας κεντρικός κόμβος ο οποίος αποθηκεύει να δεδομένα των συναλλαγών και είναι υπεύθυνος για τον έλεγχο της εγκυρότητάς τους. Ένα δίκτυο δηλαδή είναι γενικά ένα peer-to-peer δίκτυο το οποίο αποτελείται από ομότιμους κόμβους που ονομάζονται peers και μοιράζονται τα δικαιώματα δημιουργίας και αποθήκευσης συναλλαγών. Επομένως, τα δεδομένα που διαφυλάσσονται στο δίκτυο δεν μπορεί να τα τροποποιήσει ένας κόμβος από μόνος του, χωρίς να υπάρχει έγκριση και από τους υπόλοιπους. Αντίγραφα της βάσης δεδομένων όπου αποθηκεύονται τα δεδομένα των συναλλαγών συνήθως είναι αποθηκευμένα σε διαφορετικούς κόμβους του δικτύου. Εκτός αυτού, η βάση δεδομένων μπορεί να είναι κατανεμημένη, δηλαδή διαφορετικά τμήματα της βάσης να είναι αποθηκευμένα σε διαφορετικούς κόμβους.

Τα δεδομένα τα οποία καταγράφονται σε ένα δίκτυο Blockchain τοποθετούνται σε ομάδες που ονομάζονται blocks. Το σύνολο των blocks δημιουργεί μία αλυσίδα, όπου κάθε block συνδέεται με το προηγούμενό του. Το αρχικό block ονομάζεται genesis block. Τα blocks αποθηκεύονται με χρονολογική σειρά και για κάθε block δεδομένων καταχωρείται η στιγμή δημιουργίας του (timestamp). Δεν υπάρχει τρόπος να τροποποιηθεί ή να διαγραφεί ένα ήδη αποθηκευμένο block της αλυσίδας. Για τον λόγο αυτόν λέμε ότι τα δεδομένα που αποθηκεύονται σε ένα δίκτυο Blockchain είναι αμετάβλητα (immutable).

Συχνά τα δεδομένα των blocks αναπαριστούν συναλλαγές που έχουν γίνει ανάμεσα στους χρήστες του δικτύου και οι συναλλαγές αυτές αφορούν την αγορά κάποιων αγαθών. Η ιδιοκτησία των αγαθών μπορεί να αλλάξει αποθηκεύοντας μία συναλλαγή σε ένα νέο block, το οποίο θα έχει ένα νέο timestamp. Δεν μπορεί

όμως να αλλάξει το γεγονός ότι αυτό το αγαθό ήταν στην ιδιοκτησία ενός άλλου χρήστη κάποια προγενέστερη χρονική στιγμή [28].

Κάθε block περιλαμβάνει μία ακολουθία από χαρακτήρες η οποία έχει προέλθει από το περιεχόμενο του συγκεκριμένου block, αλλά και το περιεχόμενο του προηγούμενου block. Αυτή η ακολουθία από χαρακτήρες ονομάζεται hash code και είναι ένας μοναδικός κωδικός που εξαρτάται πλήρως από τα δεδομένα των blocks. Αν μεταβληθεί το περιεχόμενο του blocks, τότε το νέο περιεχόμενο θα αντιστοιχεί σε διαφορετικό hash code. Επομένως, μία τέτοια τροποποίηση θα γίνει εύκολα αντιληπτή από το δίκτυο και θα απορριφθεί από τους κόμβους του δικτύου. Με τον τρόπο αυτό εξασφαλίζεται η μη μεταβλητότητα (immutability) των δεδομένων που αποθηκεύονται.

Οι νέες συναλλαγές που πραγματοποιούνται δεν εγκρίνονται από μία κεντρική αρχή, όπως συμβαίνει στον παραδοσιακό τρόπο λειτουργίας των συστημάτων καταχώρησης συναλλαγών. Αντίθετα, εφαρμόζεται ένας αλγόριθμος ή μηχανισμός συναίνεσης (συμφωνίας) που ονομάζεται consensus algorithm. Ο αλγόριθμος αυτός καθορίζει τον τρόπο με τον οποίο επαληθεύονται οι συναλλαγές που αποθηκεύονται στο δίκτυο. Υπάρχουν διάφοροι μηχανισμοί συναίνεσης οι οποίοι μπορούν να χρησιμοποιηθούν σε ένα δίκτυο Blockchain, όπως είναι ο μηχανισμός Proof of Work (PoW) και ο μηχανισμός Proof of Stake (PoS). Ο πρώτος μηχανισμός συναίνεσης που χρησιμοποιήθηκε είναι ο Proof of Work, ο οποίος χρησιμοποιήθηκε από το Bitcoin του Nakamoto. Ο μηχανισμός αυτός έχει πολύ μεγάλη κατανάλωση ενέργειας και για τον λόγο αυτόν έχουν προταθεί και διάφοροι άλλοι μηχανισμοί με πολύ μικρότερη κατανάλωση ενέργειας. Ένας τέτοιος μηχανισμός είναι ο μηχανισμός Proof of Stake, ο οποίος χρησιμοποιείται στην πλατφόρμα Ethereum 2. Αρχικά η πλατφόρμα Ethereum χρησιμοποιούσε τον μηχανισμό Proof of Work, όμως στην πορεία άλλαξε και κάνοντας fork της αλυσίδας δεδομένων, έγινε η μετάβαση στον μηχανισμό Proof of Stake.

Αρχικά τα δίκτυα Blockchain χρησιμοποιήθηκαν για την συναλλαγή κρυπτονομισμάτων (cryptocurrencies). Στην πορεία όμως προστέθηκε η δυνατότητα για τη δημιουργία έξυπνων συμβολαίων (smart contracts). Τα έξυπνα συμβόλαια περιλαμβάνουν κώδικα ο οποίος εφαρμόζει ένα προκαθορισμένο σύνολο κανόνων οι οποίοι εκτελούνται με ντετερμινιστικό (deterministic) και ασφαλή τρόπο [29]. Με τη βοήθεια των έξυπνων συμβολαίων μπορεί να

καθοριστεί η πολιτική (policy) που εφαρμόζεται στο δίκτυο και να εξασφαλιστεί η ακεραιότητα (integrity) και η αυθεντικότητα (authentication) των αποθηκευμένων δεδομένων. Τα έξυπνα συμβόλαια παρουσιάστηκαν για πρώτη φορά το 2014 με την πλατφόρμα Ethereum. Με τη βοήθεια των έξυπνων συμβολαίων μπορούν να αναπτυχθούν κατανεμημένες εφαρμογές dApps (distributed Applications) οι οποίες έχουν πρόσβαση στα δεδομένα ενός δικτύου Blockchain και μπορούν να διαχειριστούν τα ψηφιακά πορτοφόλια (digital wallets) των χρηστών. Για παράδειγμα, μπορεί με ένα έξυπνο συμβόλαιο να οριστεί ότι εάν το ποσό που είναι καταχωρημένο στο πορτοφόλι ενός χρήστη ξεπεράσει ένα συγκεκριμένο όριο, τότε να εκτελεστεί κάποια καθορισμένη από πριν συναλλαγή.

Η σύνδεση ενός χρήστη σε ένα δίκτυο Blockchain μπορεί να απαιτεί ειδική άδεια (permission) ή να μπορεί να γίνει χωρίς άδεια. Στην πρώτη περίπτωση λέμε ότι έχουμε ένα permissioned δίκτυο Blockchain, ενώ στη δεύτερη περίπτωση έχουμε ένα permissionless δίκτυο. Τα δίκτυα τα οποία χρησιμοποιούνται για την αγορά και πώληση κρυπτονομισμάτων είναι κατά κανόνα permissionless και οποιοσδήποτε χρήστης του Internet μπορεί να συμμετέχει στα δίκτυα αυτά. Τα permissioned δίκτυα όμως μπορούν να προσφέρουν μεγαλύτερη ιδιωτικότητα και καλύτερες αποδόσεις, δεδομένου ότι ο αριθμός των κόμβων σε ένα τέτοιο δίκτυο είναι μικρότερος. Η πλατφόρμα Hyperledger Fabric που περιγράφεται στη συνέχεια μπορεί να χρησιμοποιηθεί για τη δημιουργία permissioned δικτύων Blockchain.

3.2 Πλατφόρμες Blockchain

Μία πλατφόρμα Blockchain είναι μία συλλογή λογισμικού με τη βοήθεια της οποίας μπορεί να αναπτυχθεί ένα δίκτυο Blockchain. Υπάρχουν διάφορες πλατφόρμες Blockchain οι οποίες αναφέρονται και ως Blockchain frameworks. Ένα Blockchain framework περιλαμβάνει όλα εκείνα τα εργαλεία τα οποία επιτρέπουν τη δημιουργία ενός δικτύου Blockchain και την ανάπτυξη εφαρμογών για τη διαχείριση των συναλλαγών που θα αποθηκεύονται στο δίκτυο. Περιλαμβάνει δηλαδή όλα εκείνα τα εργαλεία και τις βιβλιοθήκες τα οποία έχουν σκοπό να απλοποιήσουν τη διαδικασία της δημιουργίας μίας εφαρμογής για δίκτυο Blockchain. Σε ένα Blockchain framework ενσωματώνονται κάποιες λειτουργικότητες, πρότυπα και πρακτικές οι οποίες επιταχύνουν τον κύκλο

ανάπτυξης μίας εφαρμογής και μειώνουν την πιθανότητα για σφάλματα (bugs) που θα μπορούσαν να εμφανιστούν.

Ανάλογα με τις λειτουργίες στις οποίες καλούνται να βοηθήσουν, τα Blockchain frameworks μπορούν να ταξινομηθούν στις πιο κάτω κατηγορίες [30]:

- Πλατφόρμες ανάπτυξης δικτύου Blockchain (Blockchain Development Frameworks). Είναι frameworks τα οποία προσφέρουν εργαλεία και βιβλιοθήκες για την ανάπτυξη ενός νέου δικτύου Blockchain και τη διαχείριση των δεδομένων του δικτύου μέσω των κατάλληλων εφαρμογών. Περιλαμβάνουν συνήθως εργαλεία τα οποία μπορούν να εκτελέσουν τις πιο κάτω λειτουργίες:
 - Αυτοματοποίηση της διαδικασίας δημιουργίας του δικτύου (Blockchain automation). Το framework περιλαμβάνει εργαλεία τα οποία αυτοματοποιούν την πολύπλοκη διαδικασία δημιουργίας και αρχικοποίησης ενός δικτύου Blockchain.
 - Διαχείριση των δεδομένων της αλυσίδας (on-chain data management). Με τη βοήθεια των κατάλληλων εργαλείων επιτρέπουν την καταχώρηση δεδομένων στην αλυσίδα και την λήψη-ανάγνωση των υπαρχόντων δεδομένων.
 - Ανάπτυξη και έλεγχος έξυπνων συμβολαίων (smart contract testing and deployment). Παρέχουν φιλικό περιβάλλον για την ανάπτυξη έξυπνων συμβολαίων τα οποία εφαρμόζονται στην αλυσίδα δεδομένων του δικτύου.
 - Εργαλεία για την υποστήριξη της κοινότητας του framework. Τα πιο δημοφιλή Blockchain frameworks διαθέτουν μεγάλη κοινότητα προγραμματιστών που επικοινωνούν μεταξύ τους και βοηθούν στην επίλυση προβλημάτων.
 - Υποστήριξη διαφόρων γλωσσών προγραμματισμού και εργαλείων ανάπτυξης λογισμικού. Τα περισσότερα frameworks υποστηρίζουν δημοφιλείς γλώσσες προγραμματισμού όπως είναι η Javascript, η Java, η Python κλπ.
- Πλατφόρμες εξασφάλισης της ασφάλειας (security assurance frameworks). Τα frameworks αυτά παρέχουν εργαλεία και οδηγούς για την εξασφάλιση της ασφάλειας στο δίκτυο και την καταπολέμηση κινδύνων και ευπαθειών του συστήματος.

- Frameworks για την κλιμάκωση και βελτίωση της απόδοσης του δικτύου (scalability and performance optimization frameworks). Πρόκειται για εργαλεία τα οποία έχουν ως στόχο να βελτιώσουν την απόδοση του δικτύου όταν το μέγεθός του αυξάνεται, δίνοντας δηλαδή δυνατότητες κλιμάκωσης του συστήματος.b
- Πλατφόρμες διαχείρισης ψηφιακών ταυτοτήτων (Blockchain-based PKI management frameworks). Τα frameworks αυτά περιλαμβάνουν εργαλεία τα οποία επιτρέπουν τη διαχείριση ψηφιακών ταυτοτήτων (digital identities) των χρηστών και των κόμβων του δικτύου. Το PKI (Public Key Infrastructure) αφορά τη διαχείριση των ρόλων και των πολιτικών που ελέγχουν την πρόσβαση στο δίκτυο Blockchain, την αυθεντικοποίηση (authentication) των χρηστών και των κόμβων του δικτύου, τα δικαιώματα των χρηστών κτλ. Κάθε χρήστης θα πρέπει να διαθέτει ένα ψηφιακό πορτοφόλι (digital wallet) με ένα ζευγάρι κλειδιών, το ιδιωτικό κλειδί (private) και το δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί είναι αυστηρά προσωπικό και θα πρέπει να παραμένει απολύτως ασφαλές και κρυφό από τους υπόλοιπους χρήστες, ενώ το δημόσιο κλειδί μπορεί να είναι φανερό προς όλους. Με τη βοήθεια των κλειδιών αυτών μπορεί να γίνουν λειτουργίες όπως:
 - Κρυπτογράφηση των μηνυμάτων που αποστέλλονται. Όταν ένας χρήστης στέλνει ένα μήνυμα σε έναν άλλο χρήστη, τότε κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη και άρα μόνο ο παραλήπτης μπορεί να το αποκρυπτογραφήσει με τη βοήθεια του ιδιωτικού του κλειδιού.
 - Αυθεντικοποίηση χρήστη. Με τη βοήθεια του ιδιωτικού του κλειδιού ένας χρήστης μπορεί να υπογράψει ψηφιακά ένα μήνυμα που στέλνει. Ο παραλήπτης μπορεί στη συνέχεια να επιβεβαιώσει την ταυτότητα του αποστολέα, χρησιμοποιώντας απλά το δημόσιο κλειδί του.

Η επιλογή ενός framework για την ανάπτυξη ενός δικτύου Blockchain δεν είναι εύκολη γιατί υπάρχουν αρκετές επιλογές με διαφορετικές ιδιότητες. Η επιλογή θα πρέπει να γίνει με βάση τις ανάγκες και τα επιθυμητά χαρακτηριστικά του δικτύου που θα αναπτυχθεί. Ένα βασικό κριτήριο επιλογής του κατάλληλου framework έχει σχέση με τον τύπο του δικτύου Blockchain το οποίο πρόκειται να αναπτυχθεί. Οι βασικοί τύποι δικτύων Blockchain είναι οι πιο κάτω:

- **Δημόσια δίκτυα (Public Blockchain).** Στα δίκτυα αυτά μπορεί να συμμετέχει οποιοσδήποτε χρήστης του Internet. Τέτοιο είναι τα δίκτυα Bitcoin, Ethereum κτλ.
- **Ιδιωτικά δίκτυα (Private Blockchain).** Στα ιδιωτικά δίκτυα χρειάζεται κάποιου είδους εξουσιοδότηση για συμμετοχή στο δίκτυο. Τα δίκτυα αυτά είναι μικρότερο συνήθως σε μέγεθος και έχουν μεγαλύτερες απαιτήσεις ταχύτητας. Οι χρήστες μπορεί να είναι χωρισμένοι ανάλογα με το επίπεδο δικαιωμάτων που διαθέτουν. Ένα παράδειγμα τέτοιου δικτύου είναι το Hypeledger Fabric, όπως επίσης και το Ripple (XPR).
- **Δίκτυα σύμπραξης (Consortium Blockchain).** Τα δίκτυα consortium είναι κατάλληλα για τις περιπτώσεις όπου υπάρχει ένα σύνολο φορέων, όπως εταιρείες, τράπεζες, οργανισμοί κτλ., οι οποίοι ανταλλάσσουν πληροφορίες και κάνουν συναλλαγές. Τέτοια δίκτυα είναι το Energy Web Foundation και το IBM Food Trust.
- **Υβριδικά δίκτυα (Hybrid Blockchain).** Είναι δίκτυα τα οποία συνδυάζουν χαρακτηριστικά των ιδιωτικών και των δημοσίων δικτύων Blockchain. Κάποιες από τις πληροφορίες που αποθηκεύονται στο δίκτυο μπορεί να είναι προσβάσιμες προς όλους τους χρήστες, ενώ σε άλλες έχουν πρόσβαση μόνο συγκεκριμένοι χρήστες του δικτύου. Ένα τέτοιο δίκτυο είναι το Dragonchain.

Πέρα από τον τύπο του δικτύου που πρόκειται να αναπτυχθεί, υπάρχουν και άλλα κριτήρια τα οποία θα πρέπει να εξεταστούν για την επιλογή του κατάλληλου framework, όπως για παράδειγμα οι γλώσσες προγραμματισμού που υποστηρίζονται, η ωριμότητα του λογισμικού, η υποστήριξη που έχει από την αντίστοιχη κοινότητα, η διαλειτουργικότητα και οι δυνατότητες συνεργασίας με άλλα συστήματα κλπ.

Κάποια από τα πιο δημοφιλή frameworks για την ανάπτυξη δικτύου Blockchain παρουσιάζονται πολύ συνοπτικά πιο κάτω:

1. **Hyperledger Fabric.** Είναι μία πλατφόρμα ανοικτού κώδικα για τη δημιουργία δικτύου κατανεμημένου ledger (distributed ledger). Περιγράφεται αναλυτικότερα στη συνέχεια.
2. **Ethereum.** Αποτελεί μία από τις παλαιότερες πλατφόρμες κρυπτονομισμάτων και ξεκίνησε τη λειτουργία της το 2013 από τον

Ρωσοκαναδό προγραμματιστή Vitalk Buterin. Ήταν πρωτοπόρος πλατφόρμα στη χρήση έξυπνων συμβολαίων και κάνει χρήση του μηχανισμού Proof of Stake αντί του μηχανισμού Proof of Work που χρησιμοποιούσε κατά τα πρώτα χρόνια. Χρησιμοποιεί τεχνολογία εικονικής μηχανής (Ethereum Virtual Machine) για τη δημιουργία νέων εφαρμογών και τη χρήση έξυπνων συμβολαίων. Υπάρχουν διάφορες πλατφόρμες που λειτουργούν με παρόμοιο τρόπο όπως η πλατφόρμα Ethereum και έχουν προταθεί κατά καιρούς ως “Ethereum-killers”. Τέτοιες είναι οι πλατφόρμες Solana, Cardano, Fantom, Tezos κλπ.

3. **Corda.** Είναι μία πλατφόρμα που υποστηρίζει έξυπνα συμβόλαια (smart contracts) και dApps και χρησιμοποιείται στον χώρο των επιχειρήσεων και ειδικά για την παροχή αποκεντρωμένων χρηματοοικονομικών υπηρεσιών (Decentralized Finance – DeFi). Ο όρος DeFi αναφέρεται σε υπηρεσίες οι οποίες παραδοσιακά προσφέρονται από τράπεζες και χρηματιστηριακούς οίκους.
4. **BSV Blockchain.** Το BSV Blockchain είναι η πλατφόρμα ανάπτυξης του Bitcoin από τον Satoshi Nakamoto η οποία έχει εμπλουτιστεί με τη δυνατότητα χρήσης έξυπνων συμβολαίων. Το μέγεθος του block είναι 1 GB, ενώ στο δίκτυο Bitcoin το μέγεθος είναι μόλις 1 MB. Αυτό το χαρακτηριστικό δίνει τη δυνατότητα αποθήκευσης μεγάλου πλήθους συναλλαγών στο ίδιο block και επεξεργασίας 50.000 έως 100.000 συναλλαγών ανά δευτερόλεπτο.
5. **Hyperledger Sawtooth.** Όπως και η πλατφόρμα Hyperledger Fabric, ανήκει και αυτή στην οικογένεια του Hyperledger project. Η πλατφόρμα Hyperledger Sawtooth προσφέρει μία modular αρχιτεκτονική για τη δημιουργία δικτύων Blockchain για επιχειρήσεις, δίνοντας μεγάλες δυνατότητες κλιμάκωσης και τη δυνατότητα εκτέλεσης έξυπνων συμβολαίων χωρίς να είναι απαραίτητα γνωστός ο εσωτερικός τρόπος λειτουργίας του συστήματος. Από την άλλη μεριά όμως, το Hyperledger Fabric προσφέρει δυνατότητα για διπλάσιες συναλλαγές ανά δευτερόλεπτο. Επίσης το Hyperledger Fabric υποστηρίζει περισσότερα από ένα επίπεδα ιδιωτικότητας, ενώ το Hyperledger Sawtooth υποστηρίζει μόνο ένα επίπεδο.
6. **Ripple.** Αποτελεί μία πλατφόρμα η οποία υλοποιεί τον αλγόριθμο Ripple Transaction Protocol (RTXP) για την αποστολή χρημάτων και εκτέλεση

πληρωμών ανάμεσα σε δύο συναλλασσόμενα μέρη. Αναπτύχθηκε το 2012 με στόχο να προσφέρει μικρότερη κατανάλωση ενέργειας και ταχύτερες συναλλαγές σε σχέση με το Bitcoin.

7. **EOSIO.** Είναι μία ευέλικτη πλατφόρμα ανοικτού κώδικα η οποία αναπτύχθηκε σε C++ και υποστηρίζει τόσο δημόσια, όσο και ιδιωτικά δίκτυα Blockchain. Προσφέρει διάφορα παραμετροποιήσιμα εργαλεία για την ανάπτυξη Blockchain εφαρμογών.

Στην επόμενη παράγραφο παρουσιάζονται αναλυτικότερα κάποια από τα χαρακτηριστικά της πλατφόρμας Hyperledger Fabric η οποία επιλέχθηκε για την ανάπτυξη του δικτύου που περιγράφεται στο τέταρτο κεφάλαιο.

3.3 Hyperledger Fabric

Το Hyperledger Fabric είναι ένα project ανοικτού κώδικα για τη δημιουργία ενός δικτύου Blockchain. Αποτελεί ένα από τα πολλά projects του Hyperledger Foundation που αποτελεί μέλος του Linux Foundation (LF) Decentralized Trust. Το LF Decentralized Trust είναι μία κοινότητα για την προώθηση έργων και προτύπων ανοικτού κώδικα. Το Hyperledger Fabric ανακοινώθηκε το 2015 από το ίδρυμα Linux Foundation και κυκλοφόρησε το επόμενο έτος. Το Hyperledger Fabric χρησιμοποιείται από πολλές εταιρείες παγκοσμίως για τα δίκτυα Blockchain που χρησιμοποιούν. Μία λίστα από κάποιες μεγάλες εταιρείες που χρησιμοποιούν το Hyperledger Fabric φαίνεται στην Εικόνα 3. Στην εικόνα φαίνεται ότι το Hyperledger Fabric χρησιμοποιείται από διάφορες εταιρείες που προσφέρουν ευρύ φάσμα υπηρεσιών, κάτι που δείχνει τις δυνατότητες που δίνει η συγκεκριμένη πλατφόρμα.

Το Hyperledger Fabric εισήγαγε μία νέα αρχιτεκτονική με στόχο την ευελιξία, την αντοχή στα σφάλματα, τη δυνατότητα κλιμάκωσης και την εμπιστευτικότητα ανάμεσα στους χρήστες του δικτύου. Ήταν η πρώτη Blockchain πλατφόρμα που υποστήριξε τη χρήση γλωσσών προγραμματισμού γενικού σκοπού (general-purpose programming languages).

	BairesDev	 United States	It Services And It Consulting	3.3K	\$105M
	HealthVerity	 United States	Software Development	241	\$19M
	iteratec GmbH	 Germany	It Services And It Consulting	410	\$45M
	NP Solution Limited		Staffing And Recruiting		
	Nillion	 Switzerland	Computer And Network Security	56	
	MARKETNODE PTE. LTD.				
	IBM	 United States	It Services And It Consulting	329K	\$61B
	SyncFab	 United States	Defense And Space Manufacturing	13	
	R3	 United Kingdom	Financial Services	500	\$50M
	HESPERIE CONSEIL		Professional Services	11	

Εικόνα 3: Εταιρείες που χρησιμοποιούν το Hyperledger Fabric

Το Hyperledger Fabric δημιουργήθηκε για να αντιμετωπίσει κάποιες από τις αδυναμίες που αντιμετώπιζαν τα δίκτυα permissioned Blockchain. Τέτοιες αδυναμίες είναι οι εξής [31]:

- Ο μηχανισμός συναίνεσης (consensus mechanism) ήταν ενσωματωμένος στην "λογική" του δικτύου και δεν ήταν εύκολο να επιλεγούν άλλοι μηχανισμοί συναίνεσης. Με τους μηχανισμούς συναίνεσης δεν ισχύει η πρόταση "one size fits all" και επομένως είναι πολύ σημαντική η υποστήριξη από την πλατφόρμα διαφορετικών μηχανισμών συναίνεσης, έτσι ώστε να επιλέγεται κάθε φορά αυτήν που ταιριάζει καλύτερα με τις ανάγκες της επιχείρησης.
- Τα έξυπνα συμβόλαια έπρεπε να είναι γραμμένα σε μία προκαθορισμένη και πλήρως εξαρτώμενη από την πλατφόρμα γλώσσα προγραμματισμού και δεν μπορούσαν να χρησιμοποιηθούν δημοφιλείς γλώσσες προγραμματισμού γενικού σκοπού.
- Οι συναλλαγές έπρεπε να εκτελεστούν από όλους τους κόμβους (peers) του δικτύου, κάτι που επιβάρυνε το δίκτυο και το έκανε ευάλωτο σε επιθέσεις της μορφής "denial-of-service".
- Οι συναλλαγές έπρεπε να εκτελεστούν με ντετερμινιστικό και αυστηρά καθορισμένο τρόπο, κάτι που δεν ήταν εύκολο να υλοποιηθεί προγραμματιστικά.

- Τα έξυπνα συμβόλαια έπρεπε να εκτελούνται και να εφαρμόζονται σε όλους τους κόμβους του δικτύου.

Το Hyperledger Fabric ήρθε να ξεπεράσει πολλές από αυτούς τους περιορισμούς, εισάγοντας μία νέα αρχιτεκτονική και ένα νέο μοντέλο λειτουργίας που βασίζεται στα βήματα: "execute-order-validate". Τα βήματα αυτά περιγράφονται πιο κάτω:

- **Execute.** Αρχικά εκτελούνται οι συναλλαγές αφού πρώτα ελεγχθεί η εγκυρότητά τους. Οι κόμβοι που εκτελούν τις συναλλαγές θα πρέπει να τις υπογράψουν (endorse). Το στάδιο αυτό είναι παρόμοιο με το στάδιο "transaction validation" που αναφέρεται σε άλλες πλατφόρμες.
- **Order.** Στη συνέχεια έχουμε εφαρμογή του μηχανισμού συναίνεσης με την υπηρεσία ordering service του δικτύου.
- **Validate.** Τέλος έχουμε την προσθήκη του block με τις συναλλαγές στο δίκτυο, στο τέλος της αλυσίδας.

Σε ένα δίκτυο Hyperledger Fabric μία συναλλαγή δεν είναι απαραίτητο να εκτελεστεί σε όλους τους κόμβους (peers) του δικτύου. Αρκεί να εκτελεστεί σε ένα υποσύνολο των κόμβων αυτών, επιτρέποντας έτσι την παράλληλη εκτέλεση πολλών συναλλαγών και την κατακόρυφη αύξηση των συναλλαγών που εκτελούνται ανά δευτερόλεπτο. Χρησιμοποιώντας μία ευέλικτη πολιτική, μπορεί να καθοριστεί το πλήθος των κόμβων οι οποίοι θα πρέπει να εγκρίνουν μία συναλλαγή, ανάλογα με το επιθυμητό ποσοστό συναίνεσης.

Ένα δίκτυο Hyperledger Fabric αποτελείται από τα πιο κάτω βασικά συστατικά μέρη:

- **Ordering Service (OS).** Είναι η υπηρεσία η οποία είναι υπεύθυνη για την εφαρμογή της πολιτικής συναίνεσης και η οποία στέλνει τα μηνύματα ενημέρωσης της κατάστασης του δικτύου προς όλους τους κόμβους, έτσι να γίνει η επικύρωση των αλλαγών.
- **Membership Service Provider (MSP).** Είναι ένας ή περισσότεροι peers του δικτύου οι οποίοι είναι υπεύθυνοι για την αυθεντικοποίηση των χρηστών και των κόμβων που συμμετέχουν στο δίκτυο.
- **Peer-to-peer gossip service.** Είναι μία προαιρετική υπηρεσία όπου οι κόμβοι του δικτύου ανταλλάσσουν μηνύματα μεταξύ τους σχετικά με την κατάστασή τους και σχετικά με την κατάσταση των άλλων κόμβων που

ήδη τους είναι γνωστοί.

- **Έξυπνα συμβόλαια (smart contracts).** Είναι λογισμικό το οποίο εκτελείται σε ένα περιβάλλον container, όπως είναι το docker, έτσι ώστε να εξασφαλιστεί ότι εκτελείται μέσα στο κατάλληλο περιβάλλον, χωρίς να επηρεάζεται από άλλες εφαρμογές (isolation). Τα έξυπνα συμβόλαια καλούνται και chaincode και περιλαμβάνουν τον κώδικα που εκτελείται κατά το πρώτο στάδιο του μοντέλου λειτουργίας (execution). Κάποια chaincodes χρησιμοποιούνται για τη διαχείριση (management) και συντήρηση (maintenance) του συστήματος και καλούνται system chaincodes.
- **Distributed Ledger.** Το σύνολο των δεδομένων που βρίσκεται στην αλυσίδα των blocks αναφέρεται ως ledger. Το ledger μπορεί να είναι κατακεκομμένο (distributed) σε περισσότερους από έναν κόμβους (peers) του δικτύου.

Ένα δίκτυο Hyperledger Fabric μπορεί να επιτύχει ρυθμό μέχρι 3.500 συναλλαγές ανά δευτερόλεπτο, τη στιγμή που ένα δίκτυο Hyperledger Sawtooth μπορεί να υποστηρίξει μέχρι 1.000 συναλλαγές ανά δευτερόλεπτο. Η καθυστέρηση (latency) για τη συναλλαγή είναι μερικές εκατοντάδες milliseconds (ms) για δίκτυο με 100 peers [32].

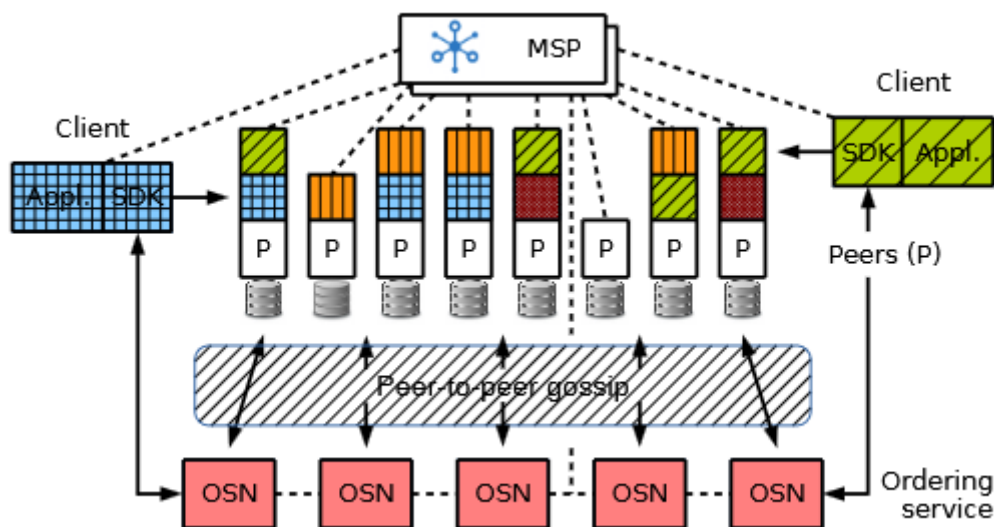
Οι κόμβοι ενός δικτύου Hyperledger Fabric μπορούν να διακριθούν ανάλογα με τον ρόλο τους στις πιο κάτω κατηγορίες:

- **Πελάτες (clients).** Μέσω των εφαρμογών που χρησιμοποιούν οι πελάτες υποβάλουν προτάσεις (proposals) για εκτέλεση συναλλαγών και δημοσιοποιούν τις συναλλαγές αυτές στους άλλους peers του δικτύου μέσω της υπηρεσίας Ordering Service (OS).
- **Κόμβοι (Peers).** Εκτελούν και επικυρώνουν τις συναλλαγές. Οι peers έχουν αποθηκευμένο το ledger, ολόκληρο ή μέρος του και μπορούν να προσθέσουν blocks σε αυτό (append-only). Δεν εκτελούν όλοι οι peers απαραίτητα όλες τις συναλλαγές. Ένα μόνο μέρος των peers μπορεί να τις εκτελεί, όπως καθορίζεται από την πολιτική του δικτύου. Οι peers αυτοί ονομάζονται endorsing peers ή απλά endorsers. Σε ένα δίκτυο θα πρέπει να εφαρμόζεται μία συγκεκριμένη endorsing policy και η πολιτική αυτή μπορεί να καθοριστεί μόνο από διαχειριστές του δικτύου που έχουν το δικαίωμα αυτό. Η πολιτική αυτή μπορεί να καθορίσει ποιοι ή πόσοι θα

πρέπει να είναι οι endorsers, με τη βοήθεια εκφράσεων που κάνουν χρήση λογικών τελεστών, όπως ο "ΚΑΙ", "Η" κτλ.

- **Κόμβοι υπηρεσίας ταξινόμησης (Ordering service nodes - OSN).** Οι κόμβοι αυτοί προσφέρουν την υπηρεσία Ordering Service (OS). Η υπηρεσία αυτή καθορίζει τη σειρά με την οποία θα πρέπει να εκτελεστούν οι συναλλαγές. Κάθε συναλλαγή περιλαμβάνει το κατάλληλο μήνυμα ενημέρωσης της κατάστασης του συστήματος και τις προϋποθέσεις-εξαρτήσεις για την εκτέλεση της συναλλαγής. Περιλαμβάνει επίσης και τις ψηφιακές υπογραφές των μελών που συμμετέχουν στη συναλλαγή.

Η αρχιτεκτονική ενός δικτύου Hyperledger Fabric και οι τύποι των κόμβων που υπάρχουν σε ένα τέτοιο δίκτυο, εμφανίζεται στην Εικόνα 4. Στο σχήμα αυτό φαίνεται η διεπαφή ανάμεσα στον client και τον MSP και ο ρόλος που έχουν οι



Εικόνα 4: Αρχιτεκτονική δικτύου Hyperledger Fabric [31]

OSN κόμβοι για την ταξινόμηση των συναλλαγών.

Κεφάλαιο 4^ο

4. Υλοποίηση εφαρμογής Blockchain

4.1 Λειτουργίες και δυνατότητες της εφαρμογής

Στα πλαίσια της πτυχιακής εργασίας αναπτύχθηκε μία εφαρμογή Blockchain η οποία έχει σκοπό την μελέτη των δυνατοτήτων που προσφέρει η τεχνολογία Blockchain στον χώρο της εκπαίδευσης. Στις προηγούμενες παραγράφους είδαμε διάφορες προσπάθειες που έχουν γίνει, σε όλες τις βαθμίδες της Εκπαίδευσης για την ανάπτυξη υπηρεσιών οι οποίες βασίζονται στην τεχνολογία Blockchain. Στο κεφάλαιο αυτό παρουσιάζεται η διαδικασία υλοποίησης μίας εφαρμογής με τη βοήθεια του HyperLedger Fabric framework και την γλώσσα προγραμματισμού Javascript. Σκοπός της προσπάθειας αυτής είναι να μελετήσει τα διαθέσιμα εργαλεία που προσφέρει το HyperLedger Fabric, για την ανάπτυξη ενός απλού συστήματος το οποίο θα επιτρέπει την εισαγωγή σε ένα Blockchain των πληροφοριών που σχετίζονται με την κτήση ενός ακαδημαϊκού τίτλου από κάποιον φοιτητή ενός ιδρύματος της τριτοβάθμιας Εκπαίδευσης.

Η εφαρμογή η οποία αναπτύχθηκε μπορεί να εκτελεί τις πιο κάτω λειτουργίες:

- Εισαγωγή των πληροφοριών που αφορούν την κτήση ενός ακαδημαϊκού τίτλου. Οι πληροφορίες αυτές περιλαμβάνουν δεδομένα όπως το id του τίτλου, όνομα του κατόχου του τίτλου, ο τύπος του τίτλου, το όνομα του ιδρύματος που εκδίδει τον τίτλο, η ημερομηνία κτήσης του τίτλου, ο βαθμός κτλ.
- Αναζήτηση για την εύρεση ενός τίτλου. Η αναζήτηση μπορεί να γίνει με βάση το id του τίτλου ή με βάση κάποιας άλλης από τις πληροφορίες οι οποίες αποθηκεύονται σχετικά με κάποιον τίτλο.
- Προβολή όλων των τίτλων οι οποίοι είναι καταχωρημένοι στην αλυσίδα Blockchain. Οι πληροφορίες εμφανίζονται με τη χρονολογική σειρά με την οποία έχουν καταχωρηθεί στην αλυσίδα.

Οι εγγραφές οι οποίες καταχωρούνται σε ένα block της αλυσίδας δεν μπορούν να τροποποιηθούν ή να αλλοιωθούν εκ των υστέρων, αφού αυτός είναι ο τρόπος που λειτουργεί μία αλυσίδα Blockchain. Για την υλοποίηση του συστήματος χρησιμοποιήθηκε το HyperLedger Fabric framework με γλώσσα προγραμματισμού Javascript και χρήση της τεχνολογίας node.js για την εκτέλεση αρχείων με κώδικα Javascript χωρίς τη διαμεσολάβηση ενός προγράμματος πλοήγησης Παγκόσμιου Ιστού.

Η διαδικασία εγκατάστασης του HyperLedger Fabric και η εγκατάσταση και λειτουργία των τεχνολογιών που χρησιμοποιήθηκαν παρουσιάζονται αναλυτικότερα στις παραγράφους που ακολουθούν.

4.2 Εγκατάσταση και λειτουργία του HyperLedger Fabric

4.2.1 Προαπαιτούμενα

Για την εγκατάσταση του HyperLedger Fabric θα πρέπει να υπάρχουν εγκατεστημένες οι πιο κάτω προαπαιτούμενες εφαρμογές:

- **cURL.** Το cURL (Client URL) είναι λογισμικό το οποίο μέσω της γραμμής εντολών επιτρέπει τη μεταφορά δεδομένων από έναν διακομιστή (server) ή προς αυτόν. Η μεταφορά μπορεί να γίνει μέσω μέσω πρωτοκόλλων του Διαδικτύου, όπως είναι το HTTP, το HTTPS, το FTP κλπ. Η λήψη του απαραίτητου λογισμικού επομένως, μπορεί να γίνει με τη βοήθεια του εργαλείου cURL.
- **Docker.** Είναι λογισμικό το οποίο επιτρέπει τη δημιουργία, εκτέλεση και διαχείριση εφαρμογών μέσα σε containers. Με τον όρο containers αναφερόμαστε σε φορητές και απομονωμένες μονάδες οι οποίες περιλαμβάνουν τον κώδικα και τις βιβλιοθήκες για την εκτέλεση μίας εφαρμογής και τη διαχείριση των εξαρτήσεών της με άλλες μονάδες λογισμικού. Με την χρήση containers μπορεί να εξασφαλιστεί ότι μία εφαρμογή θα εκτελεστεί με τον επιθυμητό τρόπο, χωρίς να επηρεάζεται από το περιβάλλον, δηλαδή το λειτουργικό σύστημα, όπου βρίσκεται. Το HyperLedger Fabric χρησιμοποιεί κάποια containers όπου εκτελείται το απαραίτητο λογισμικό.

- **Docker Compose:** Το Docker Compose είναι ένα εργαλείο το οποίο δίνει τη δυνατότητα διαχείρισης πολλαπλών Docker containers που λειτουργούν σε ένα σύστημα, αναλαμβάνοντας την επικοινωνία ανάμεσά τους. Η περιγραφή και η διαχείριση των containers μπορεί να γίνει με τη βοήθεια αρχείων σε γλώσσα YML (YAML Ain't Markup Language).
- **Git.** Το Git είναι λογισμικού ανοικτού κώδικα το οποίο κάνει έλεγχο εκδόσεων λογισμικού VCS (Version Control System), δηλαδή ελέγχει τη διαχείριση και παρακολούθηση αλλαγών που γίνονται κατά την ανάπτυξη λογισμικού.
- **Go.** Η Go ή Golang είναι γλώσσα προγραμματισμού ανοικτού κώδικα που αναπτύχθηκε από την Google και δίνει τη δυνατότητα ανάπτυξη αποδοτικών εφαρμογών. Είναι γλώσσα που χρησιμοποιείται συχνά για την ανάπτυξη backend συστημάτων και υποδομές Cloud. Αποτελεί την γλώσσα ανάπτυξης του HyperLedger Fabric.
- **Python.** Η Python είναι μία γλώσσα προγραμματισμού υψηλού επιπέδου ανοικτού κώδικα, η οποία είναι γνωστή για την απλότητά της και διαθέτει μία πολύ ενεργή κοινότητα και προσφέρει μεγάλο πλήθος βιβλιοθηκών οι οποίες επιτρέπουν την γρήγορη ανάπτυξη κώδικα. Η Python χρησιμοποιείται για τη διαχείριση των εξαρτήσεων και την αυτοματοποίηση των διαδικασιών που απαιτούνται για το HyperLedger Fabric. Υπάρχει επίσης διαθέσιμο το εργαλείο Fabric Python SDK, το οποίο μπορεί να χρησιμοποιηθεί για την αλληλεπίδραση με ένα δίκτυο που βασίζεται στο HyperLedger Fabric. Το SDK περιλαμβάνει λειτουργίες, όπως:
 - Δημιουργία συναλλαγών και υποβολή τους προς τα έξυπνα συμβόλαια (smart contracts).
 - Διαχείριση των ταυτοτήτων των χρηστών και των ψηφιακών τους πιστοποιητικών.
 - Διασύνδεση με τους ομότιμους κόμβους (peers) του δικτύου, τους orderers κτλ.
- **Node.js.** Το node.js αποτελεί μία πλατφόρμα ανοικτού κώδικα, η οποία βασίζεται στην γλώσσα προγραμματισμού Javascript. Η πλατφόρμα node.js μπορεί να χρησιμοποιηθεί για την διαχείριση εφαρμογών στη μεριά του εξυπηρετητή (server-side), δίνοντας τη δυνατότητα εκτέλεσης προγραμμάτων Javascript στη μεριά του server και όχι στο

"προστατευμένο" περιβάλλον ενός προγράμματος πλοήγησης (browser), όπως γίνεται συνήθως. Το Node.js χρησιμοποιείται σε μεγάλο βαθμό για την ανάπτυξη APIs και εφαρμογών Παγκοσμίου Ιστού και χρησιμοποιείται συχνά σε δίκτυα HyperLedger Fabric για την ανάπτυξη της διεπαφής με τον χρήστη. Πολλές από τις λειτουργίες του δικτύου μπορούν να αυτοματοποιηθούν με τη βοήθεια του Node.js, αφού η γλώσσα Javascript είναι ευρέως διαδεδομένη και τα scripts που γράφουν οι προγραμματιστές μπορούν να εκτελεστούν άμεσα με τη βοήθεια της πλατφόρμας Node.js.

Αφού γίνει ο απαραίτητος έλεγχος ότι όλες οι προαπαιτούμενες εφαρμογές και βιβλιοθήκες είναι ήδη εγκατεστημένες, στη συνέχεια μπορεί να γίνει η εγκατάσταση της πλατφόρμας HyperLedger Fabric, όπως περιγράφεται στην επόμενη παράγραφο. Το προτεινόμενο λειτουργικό σύστημα για την εγκατάσταση του HyperLedger Fabric είναι το Linux, αλλά η εγκατάσταση μπορεί να γίνει είτε σε περιβάλλον Microsoft Windows, είτε σε περιβάλλον macOS. Για την ανάπτυξη του δικτύου που περιγράφεται στη συνέχεια, έγινε χρήση του λειτουργικού συστήματος Linux και πιο συγκεκριμένα της δημοφιλούς διανομής Ubuntu, έκδοση 24.10.

4.2.2 Διαδικασία της εγκατάστασης

Για την εγκατάσταση του HyperLedger Fabric θα πρέπει να γίνει πρώτα λήψη του κατάλληλου προγράμματος (script) εγκατάστασης. Η λήψη μπορεί να γίνει άμεσα από τα αποθετήρια του HyperLedger Fabric, με το εργαλείο curl, δίνοντας από τη γραμμή εντολών την εντολή:

```
curl -sLO https://raw.githubusercontent.com/hyperledger/fabric/main/scripts/install-fabric.sh && chmod +x install-fabric.sh
```

Στη συνέχεια αρκεί να γίνει εκτέλεση του προγράμματος εγκατάστασης με την εντολή

```
./install-fabric.sh docker samples binary
```

Το πρόγραμμα εγκατάστασης:

- Αντιγράφει έναν κλώνο από με δείγματα του HyperLedger Fabric το αποθετήριο hyperledger/fabric-samples.
- Κατεβάζει την πιο πρόσφατη Docker εικόνα (image) της πλατφόρμας HyperLedger Fabric.
- Κατεβάζει τα πιο πρόσφατα εργαλεία, δυαδικά αρχεία και αρχεία ρυθμίσεων τα οποία είναι απαραίτητα για τη λειτουργία του δικτύου. Τα αρχεία αυτά τοποθετούνται στους φακέλους fabric-samples, bin και config.

Γενικότερα η εγκατάσταση του HyperLedger Fabric μπορεί να γίνει πολύ εύκολα και με αυτοματοποιημένο τρόπο, όταν είναι διαθέσιμες όλες οι προαπαιτούμενες εφαρμογές. Είναι δυνατόν κατά τη διαδικασία της εγκατάστασης να προσδιοριστεί από τον χρήστη η επιθυμητή έκδοση της πλατφόρμας, διαφορετικά γίνεται λήψη της πιο πρόσφατης έκδοσης.

4.2.3 Δημιουργία δικτύου

Κατά την εγκατάσταση του HyperLedger Fabric δημιουργείται ένας φάκελος με το όνομα fabric-samples, όπου υπάρχουν κάποια δείγματα τα οποία μπορούν να χρησιμοποιηθούν είτε αυτούσια, είτε αφού τροποποιηθούν για τη δημιουργία ενός δικτύου Blockchain. Το δίκτυο αυτό μπορεί να χρησιμοποιηθεί για τη δοκιμή έξυπνων συμβολαίων (smart contracts) και blockchain εφαρμογών που έχουν αναπτυχθεί.

Το δίκτυο περιλαμβάνει 2 ομότιμους οργανισμούς (peers) και έναν οργανισμό που λειτουργεί ως orderer. Το δίκτυο μπορεί να ενεργοποιηθεί με τις εντολές:

```
cd fabric-samples/test-network  
  
./network.sh up
```

Κάθε κόμβος που συμμετέχει στο δίκτυο θα πρέπει να ανήκει σε κάποιον οργανισμό (organization), έτσι ώστε να μπορεί να συνδιαλλάσσεται με το δίκτυο και με τους άλλους κόμβους. Το δοκιμαστικό δίκτυο που περιλαμβάνεται με τα αρχεία εγκατάστασης του HyperLedger Fabric, αποτελείται από 2 οργανισμούς που ονομάζονται Org1 και Org2 αντίστοιχα. Οι ομότιμοι κόμβοι (peers) αποθηκεύουν τα δεδομένα της αλυσίδας και εγκρίνουν τις νέες συναλλαγές, πριν

αυτές υποβληθούν στην αλυσίδα. Σε κάθε έναν από τους οργανισμούς που εγκαθίστανται από το δοκιμαστικό δίκτυο (test network) περιλαμβάνεται ένας ομότιμος κόμβος. Οι ονομασίες των peers αυτών είναι peer0.org1.example.com και peer0.org2.example.com αντίστοιχα.

Κατά την ενεργοποίηση του δικτύου εμφανίζονται μηνύματα δημιουργίας των οργανισμών του δικτύου, όπως φαίνεται στην Εικόνα 1. Στα μηνύματα αυτά περιλαμβάνονται μηνύματα για τη δημιουργία των peers peer0.org1.example.com και peer0.org2.example.com, όπως και του orderer. Κάθε κόμβος και χρήστης του δικτύου, θα πρέπει να ανήκει σε έναν οργανισμό, έτσι ώστε να μπορεί να συναλλάσσεται με το δίκτυο.

Για τον έλεγχο εάν το δίκτυο λειτουργεί σωστά και την προβολή των docker containers του δικτύου αρκεί η εντολή:

```
docker ps -a
```

Η απενεργοποίηση του δικτύου γίνεται με την εντολή

```
./network.sh down
```

Για την ενεργοποίηση της δυνατότητας επικοινωνίας ανάμεσα στους οργανισμούς θα πρέπει να εγκατασταθεί ένα κανάλι (channel) ανάμεσά τους. Τα κανάλια προσφέρουν ένα επιπλέον επίπεδο ασφάλειας ανάμεσα στα μέλη του δικτύου. Κάθε κανάλι έχει διαφορετική αλυσίδα δεδομένων. Για τη δημιουργία ενός νέου καναλιού θα πρέπει να εκτελεστεί η εντολή

```
./network.sh createChannel -c channel1
```

Με την παράμετρο -c δηλώνεται το όνομα του καναλιού. Σε περίπτωση που παραληφθεί η παράμετρος αυτή, τότε δημιουργείται κανάλι με όνομα “mchannel”. Το όνομα του καναλιού πρέπει να αποτελείται από μικρούς λατινικούς χαρακτήρες και ψηφία. Επίσης επιτρέπεται το σύμβολο της τελείας και της παύλας και μπορεί να περιλαμβάνει το πολύ 250 χαρακτήρες συνολικά.

Μετά τη δημιουργία του καναλιού, μπορεί να γίνει η χρήση έξυπνων συμβολαίων (smart contracts) για την πραγματοποίηση των συναλλαγών με το δίκτυο. Τα έξυπνα συμβόλαια περιλαμβάνουν την επιχειρηματική λογική για τη διαχείριση των πόρων (assets) του δικτύου. Οι εφαρμογές που εκτελούνται από τα μέλη του

δικτύου, μπορούν να χρησιμοποιήσουν τα έξυπνα συμβόλαια για την πραγματοποίηση συναλλαγών, όπως είναι η δημιουργία και επικύρωση νέων block δεδομένων, η ανάγνωση των δεδομένων της αλυσίδας, η μεταφορά ενός πόρου (asset) σε κάποιον άλλο χρήστη του δικτύου κτλ.

Στο HyperLedger Fabric τα έξυπνα συμβόλαια ενεργοποιούνται στο δίκτυο υπό τη μορφή κώδικα που αναφέρεται ως chaincode. Το chaincode είναι λογισμικό που εγκαθίσταται στους κόμβους του δικτύου και στη συνέχεια χρησιμοποιείται για την επικύρωση των συναλλαγών. Η εφαρμογή του chaincode σε ένα δίκτυο μπορεί να γίνει με την εντολή:

```
./network.sh deployCC -ccn basic -ccp ../asset-transfer-basic/chaincode-go -ccl go
```

όπου αντί για τη γλώσσα go μπορεί να χρησιμοποιηθεί κάποια από τις γλώσσες προγραμματισμού που υποστηρίζονται από το HyperLedger Fabric. Το chaincode δηλαδή υπάρχει διαθέσιμο στο test network στις γλώσσες προγραμματισμού Go, Javascript, Typescript και Java.

```
Creating network "fabric_test" with the default driver
Creating volume "net_orderer.example.com" with default driver
Creating volume "net_peer0.org1.example.com" with default driver
Creating volume "net_peer0.org2.example.com" with default driver
Creating peer0.org2.example.com ... done
Creating orderer.example.com ... done
Creating peer0.org1.example.com ... done
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS
b6b117c81c7f	hyperledger/fabric-peer:latest	"peer node start"	2 seconds ago	Up 1 second
703ead770e05	hyperledger/fabric-orderer:latest	"orderer"	2 seconds ago	Up Less than
718d43f5f312	hyperledger/fabric-peer:latest	"peer node start"	2 seconds ago	Up 1 second

Εικόνα 5: Δημιουργία δικτύου HyperLedger Fabric

Η εφαρμογή η οποία αναπτύχθηκε κάνει χρήση της γλώσσας Javascript και επομένως θα πρέπει να εκτελεστεί η εντολή:

```
./network.sh deployCC -ccn basic -ccp ../asset-transfer-basic/chaincode-javascript -ccl javascript
```

Ο κώδικας Javascript εκτελείται στη συνέχεια με τη βοήθεια του περιβάλλοντος του Node.js, το οποίο επιτρέπει την εκτέλεση κώδικα Javascript αυτόνομα και όχι μέσω ενός προγράμματος πλοήγησης (browser).

Στις επόμενες παραγράφους θα γίνει αναλυτική περιγραφή της εφαρμογής που αναπτύχθηκε.

4.3 Περιγραφή της εφαρμογής

Η εφαρμογή η οποία αναπτύχθηκε αφορά τη διαχείριση πιστοποιητικών που εκδίδονται από ανώτατα εκπαιδευτικά ιδρύματα και αφορούν την επιτυχημένη φοίτηση σε αυτά. Στο δοκιμαστικό δίκτυο αποθηκεύονται πληροφορίες που αφορούν προπτυχιακές ή μεταπτυχιακές σπουδές και οδηγούν στην απόκτηση πτυχίου ή μεταπτυχιακού τίτλου (master ή διδακτορικό). Η εφαρμογή μελετά τις δυνατότητες που μπορεί να έχει ένα δίκτυο Blockchain για την καταχώρηση δεδομένων της μορφής αυτής.

Τα χαρακτηριστικά της τεχνολογία Blockchain και τα πλεονεκτήματα που προσφέρει, είναι πολύ χρήσιμα για την καταχώρηση πιστοποιητικών που έχουν αποκτήσει κάποιοι απόφοιτοι ανωτάτων εκπαιδευτικών ιδρυμάτων. Θα μπορούσε ένα τέτοιο δίκτυο να επεκταθεί, έτσι ώστε να περιλαμβάνει ένα σύνολο ιδρυμάτων από όλον τον κόσμο. Τα δίκτυα αυτά θα μπορούν να καταχωρούν πληροφορίες για τα πιστοποιητικά που εκδίδουν και αφορούν απόφοιτους τους. Τα πιστοποιητικά αυτά θα μπορούν να ελεγχθούν στη συνέχεια από άλλους φορείς, οι οποίες μπορεί να είναι άλλα εκπαιδευτικά ιδρύματα, εργοδότες, κυβερνητικοί φορείς κλπ. Τα πιστοποιητικά που καταχωρούνται στο σύστημα δεν θα μπορούν να αλλοιωθούν ή να παραποιηθούν στη συνέχεια και αυτό είναι κάτι που εγγυάται η φύση της τεχνολογίας Blockchain.

Οι λειτουργίες οι οποίες προσφέρονται από δίκτυο Blockchain και την εφαρμογή που αναπτύχθηκε είναι οι ακόλουθες:

- Εισαγωγή (αποθήκευση) νέων πιστοποιητικών στο δίκτυο. Τα πιστοποιητικά αυτά μπορεί να είναι κάποιος προπτυχιακός ή μεταπτυχιακός τίτλος που έχει αποκτήσει κάποιος απόφοιτος ενός ανώτατου εκπαιδευτικού ιδρύματος.
- Αναζήτηση πληροφοριών που αφορούν πιστοποιητικά τα οποία έχουν αποθηκευτεί στο σύστημα. Η αναζήτηση αυτή μπορεί να γίνει με τη βοήθεια διάφορων κριτηρίων, όπως είναι ο κωδικός του πιστοποιητικού, ο κωδικός του ιδιοκτήτη του πιστοποιητικού ή το εκπαιδευτικό ίδρυμα που εκδίδει ένα πιστοποιητικό.
- Ανάκληση ενός πιστοποιητικού. Ένα εκπαιδευτικό ίδρυμα, σε κάποιες περιπτώσεις που συνήθως είναι σπάνιες, έχει το δικαίωμα να κάνει ανάκληση ενός πιστοποιητικού. Οι καταχωρήσεις οι οποίες γίνονται σε

μία αλυσίδα δεδομένων δεν είναι δυνατόν να αλλοιωθούν ή να τροποποιηθούν, λόγω της φύσης της τεχνολογίας Blockchain, είναι δυνατόν όμως να εισαχθεί νέα καταχώρηση στην αλυσίδα δεδομένων η οποία πληροφορεί το δίκτυο σχετικά με την ανάκληση κάποιου συγκεκριμένου πιστοποιητικού. Με τον τρόπο αυτόν, επιτυγχάνουμε την έμμεση «διαγραφή» ενός πιστοποιητικού που έχει εκδοθεί.

Οι πληροφορίες οι οποίες καταχωρούνται και αφορούν ένα πιστοποιητικό που εκδίδεται από ένα ανώτατο εκπαιδευτικό ίδρυμα, περιλαμβάνουν:

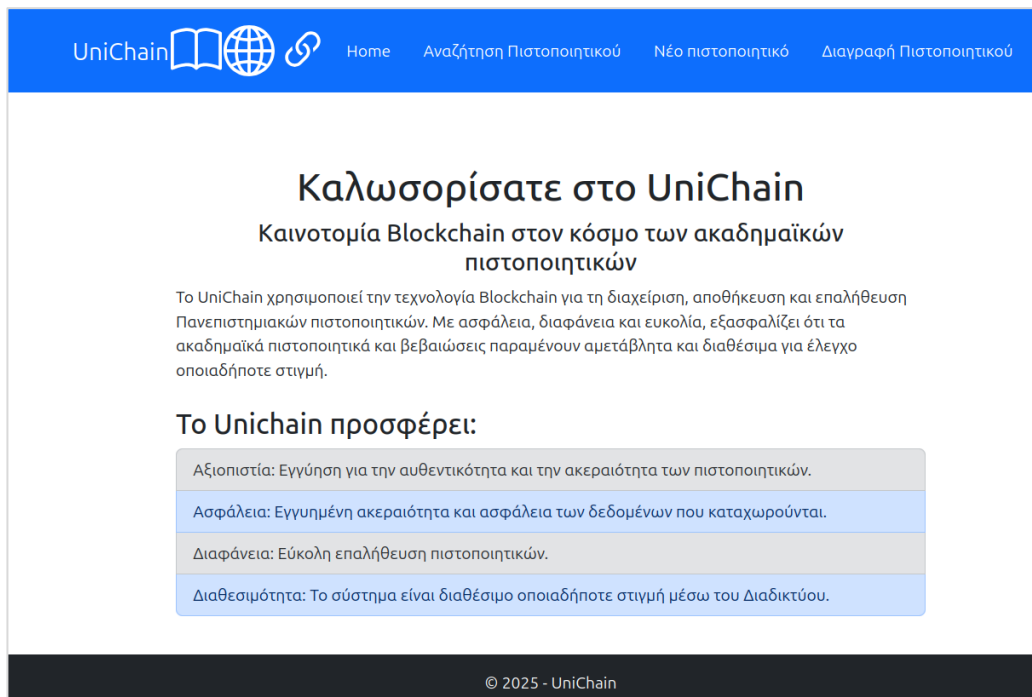
- Τον κωδικό του πιστοποιητικού (asset).
- Τον κωδικό του κατόχου (owner).
- Το όνομα του κατόχου.
- Το επώνυμο του κατόχου.
- Τη χώρα καταγωγής του κατόχου.
- Τη διεύθυνση του κατόχου.
- Το όνομα του εκπαιδευτικού ιδρύματος που εκδίδει το πιστοποιητικό.
- Τον τίτλο του πιστοποιητικού
- Τον τύπο του πιστοποιητικού. Το τύπος μπορεί να είναι προπτυχιακός τίτλος (bachelor), μεταπτυχιακός τίτλος (master) ή διδακτορικός τίτλος (PhD).
- Την ημερομηνία έκδοσης του πιστοποιητικού.
- Τον βαθμό με τον οποίο πήρε ο κάτοχος το πιστοποιητικό (αν υπάρχει βαθμός).
- Το έτος έκδοσης του πιστοποιητικού (προκύπτει και από την ημερομηνία έκδοσης).

Θα μπορούσαν προφανώς να προστεθούν και άλλες πληροφορίες οι οποίες αφορούν ένα πιστοποιητικό αλλά οι συγκεκριμένες πληροφορίες είναι αρκετές για τη δοκιμή της λειτουργίας του συστήματος.

4.4 Παρουσίαση της εφαρμογής EduChain

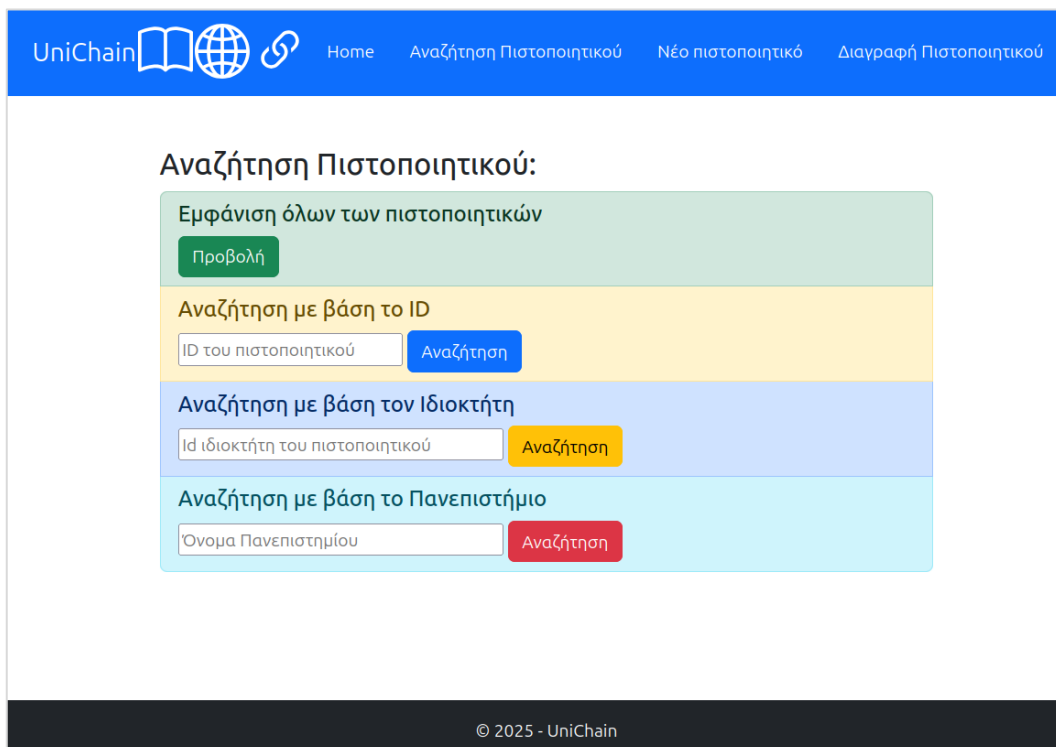
Στην παράγραφο αυτή παρουσιάζονται αναλυτικά οι λειτουργίες της εφαρμογής που αναπτύχθηκε με τη βοήθεια εικόνων (screenshots). Η εφαρμογή αυτή ονομάστηκε EduChain και δημιουργεί ένα δίκτυο Blockchain, όπου

αποθηκεύονται πιστοποιητικά τίτλων τα οποία εκδίδονται από ανώτατα εκπαιδευτικά ιδρύματα.



Εικόνα 6: Κεντρική οθόνη της εφαρμογής

Η κεντρική οθόνη της εφαρμογής φαίνεται στην Εικόνα 6. Η κεντρική οθόνη δίνει κάποιες γενικές πληροφορίες στον χρήστη και προσφέρει σε αυτόν τις επιλογές που εμφανίζονται στο μενού στο επάνω μέρος.



Εικόνα 7: Αναζήτηση πιστοποιητικών

Για την αναζήτηση πληροφοριών που αφορούν πιστοποιητικά ο χρήστης μπορεί να επιλέξει την επιλογή «Αναζήτηση Πιστοποιητικού» στο κεντρικό μενού της εφαρμογής. Εμφανίζονται τότε οι επιλογές που παρουσιάζονται στην Εικόνα 7. Στην σελίδα που εμφανίζεται, παρουσιάζονται στον χρήστη οι επιλογές αναζήτησης που μπορεί να χρησιμοποιήσει.

UniChain  Home Αναζήτηση Πιστοποιητικού Νέο πιστοποιητικό Διαγραφή Πιστοποιητικού	
Πιστοποιητικό με ID: asset1	
ID:	asset1
Owner:	student001
Όνομα:	Nick
Επώνυμο:	Pavlou
Εθνικότητα:	Greek
Διεύθυνση:	Thessaloniki, Greece
Πανεπιστήμιο:	University of Ioannina
Τίτλος:	undefined
Τύπος τίτλου:	Bachelor
Ημερομηνία:	23/6/2023
Βαθμός:	7.19
Έτος:	2023
© 2025 - UniChain	

Εικόνα 8: Προβολή όλων των πιστοποιητικών

Για την εμφάνιση όλων των πιστοποιητικών θα πρέπει ο χρήστης να πατήσει το κουμπάκι «Προβολή». Εμφανίζονται τότε πληροφορίες για όλα τα πιστοποιητικά, όπως φαίνεται στην Εικόνα 8. Οι πληροφορίες που αντιστοιχούν στο κάθε πιστοποιητικό εμφανίζονται σε μορφή πίνακα. Ο χρήστης μπορεί να κάνει επισκόπηση των πληροφοριών του κάθε πιστοποιητικού και εάν τον ενδιαφέρει κάποιο συγκεκριμένο πιστοποιητικό, μπορεί να κάνει κλικ στον κωδικό πιστοποιητικού που περιλαμβάνεται στην πρώτη στήλη του πίνακα. Εμφανίζονται τότε στην οθόνη οι πληροφορίες του συγκεκριμένου πιστοποιητικού, όπως φαίνεται στην Εικόνα 9. Παρόμοια αποτελέσματα εμφανίζονται εάν στην οθόνη που εμφανίζεται στην Εικόνα 7 ο χρήστης πληκτρολογήσει τον κωδικό ενός πιστοποιητικού που υπάρχει στο δίκτυο. Εάν δεν υπάρχει πιστοποιητικό με το συγκεκριμένο ID, τότε εμφανίζεται κατάλληλο μήνυμα λάθους.

UniChain											
Home Αναζήτηση Πιστοποιητικού Νέο πιστοποιητικό Διαγραφή Πιστοποιητικού											
Πιστοποιητικά του owner με ID: student003											
ID	Owner	Όνομα	Επώνυμο	Εθνικότητα	Διεύθυνση	Πανεπιστήμιο	Τίτλος	Τύπος	Ημερομηνία	Βαθμός	Έτος
asset4	student003	Maria	Dimitriou	Greek	Athens, Greece	Aristotle University of Thessaloniki	Computer Science	Bachelor	23/10/2019	8.5	2019
asset5	student003	Maria	Dimitriou	Greek	Athens, Greece	Aristotle University of Thessaloniki	Data Science	Master	23/10/2020	9	2020
asset6	student003	Maria	Dimitriou	Greek	Athens, Greece	Aristotle University of Thessaloniki	Data Analysis of Financial Transactions	PhD	23/2/2025	10	2024

© 2025 - UniChain

Εικόνα 10: Εμφάνιση πληροφοριών πιστοποιητικού

UniChain											
Home Αναζήτηση Πιστοποιητικού Νέο πιστοποιητικό Διαγραφή Πιστοποιητικού											
Όλα τα πιστοποιητικά											
ID	Owner	Όνομα	Επώνυμο	Εθνικότητα	Διεύθυνση	Πανεπιστήμιο	Τίτλος	Τύπος	Ημερομηνία	Βαθμός	Έτος
asset1	student001	Nick	Pavlou	Greek	Thessaloniki, Greece	University of Ioannina	Computer Science	Bachelor	23/6/2023	7.19	2023
asset10	student006	Alexandra	Nikolaou	Greek	Cyprus	University of Crete	Computer Science	Bachelor	5/2/2022	8.15	2022
asset2	student001	Nick	Pavlou	Greek	Thessaloniki, Greece	University of Ioannina	Data Analysis	Master	27/6/2024	9	2024
asset3	student002	George	Papadopoulos	Greek	Ioannina, Greece	University of Ioannina	Computer Engineer	Bachelor	7/9/2024	6.12	2024
asset4	student003	Maria	Dimitriou	Greek	Athens, Greece	Aristotle University of Thessaloniki	Computer Science	Bachelor	23/10/2019	8.5	2019
asset5	student003	Maria	Dimitriou	Greek	Athens, Greece	Aristotle University of Thessaloniki	Data Science	Master	23/10/2020	9	2020
asset6	student003	Maria	Dimitriou	Greek	Athens, Greece	Aristotle University of Thessaloniki	Data Analysis of Financial	PhD	23/2/2025	10	2024

© 2025 - UniChain

Εικόνα 9: Αναζήτηση με βάση τον κωδικό του φοιτητή

Εάν ο χρήστης κάνει κλικ στον κωδικό ενός φοιτητή (owner), τότε εμφανίζονται όλα τα πιστοποιητικά που διαθέτει, όπως φαίνεται στην Εικόνα 10. Παρόμοια αποτελέσματα εμφανίζονται εάν στην οθόνη που εμφανίζεται στην Εικόνα 7 ο χρήστης πληκτρολογήσει τον κωδικό ενός ιδιοκτήτη (owner) πιστοποιητικού που έχει καταχωρηθεί στο δίκτυο. Εάν δεν υπάρχει πιστοποιητικό με το συγκεκριμένο κωδικό ιδιοκτήτη, τότε εμφανίζεται κατάλληλο μήνυμα λάθους.

Ο χρήστης μπορεί να κάνει επίσης κλικ στο όνομα ενός εκπαιδευτικού ιδρύματος, έτσι ώστε να εμφανιστούν τα πιστοποιητικά που έχει εκδώσει το συγκεκριμένο εκπαιδευτικό ίδρυμα, όπως φαίνεται στην Εικόνα 11. Παρόμοια αποτελέσματα

εμφανίζονται εάν στην οθόνη που εμφανίζεται στην Εικόνα 7 ο χρήστης πληκτρολογήσει το όνομα ενός εκπαιδευτικού ιδρύματος.

Ο χρήστης μπορεί να εισάγει τα στοιχεία ενός νέου πιστοποιητικού το οποίο θα

UniChain    Home Αναζήτηση Πιστοποιητικού Νέο πιστοποιητικό Διαγραφή Πιστοποιητικού											
Πιστοποιητικά του Πανεπιστημίου: University of Ioannina											
ID	Owner	Όνομα	Επώνυμο	Εθνικότητα	Διεύθυνση	Πανεπιστήμιο	Τίτλος	Τύπος	Ημερομηνία	Βαθμός	Έτος
asset1	student001	Nick	Pavlou	Greek	Thessaloniki, Greece	University of Ioannina	Computer Science	Bachelor	23/6/2023	7.19	2023
asset2	student001	Nick	Pavlou	Greek	Thessaloniki, Greece	University of Ioannina	Data Analysis	Master	27/6/2024	9	2024
asset3	student002	George	Papadopoulos	Greek	Ioannina, Greece	University of Ioannina	Computer Engineer	Bachelor	7/9/2024	6.12	2024

© 2025 - UniChain

Εικόνα 11: Αναζήτηση με βάση το Εκπαιδευτικό ίδρυμα

καταχωρηθεί στο δίκτυο. Αυτό μπορεί να γίνει με τη βοήθεια της επιλογής «Νέο πιστοποιητικό» που εμφανίζεται στο κεντρικό μενού της εφαρμογής. Εμφανίζεται τότε η σελίδα που παρουσιάζεται στην Εικόνα 12. Στη σελίδα αυτή εμφανίζεται μία φόρμα όπου ο χρήστης θα πρέπει να εισάγει τις πληροφορίες που αφορούν ένα πιστοποιητικό και στη συνέχεια μπορεί να πατήσει το κουμπάκι «Δημιουργία». Εμφανίζεται τότε μία σελίδα η οποία ενημερώνει για την επιτυχή καταχώρηση του πιστοποιητικού, εμφανίζοντας μάλιστα τις πληροφορίες που το συνοδεύουν, όπως φαίνεται στην Εικόνα 9.

Τέλος, ο χρήστης μπορεί να διαγράψει ένα πιστοποιητικό, κάνοντας χρήση της επιλογής «Διαγραφή Πιστοποιητικού» στο κεντρικό μενού της σελίδας. Εμφανίζεται τότε η σελίδα που παρουσιάζεται στην Εικόνα 13. Η σελίδα εμφανίζει ένα πλαίσιο κειμένου όπου ο χρήστης θα πρέπει να εισάγει τον κωδικό του πιστοποιητικού που επιθυμεί για διαγραφή. Ο χρήστης θα πρέπει να εισάγει τον κωδικό του πιστοποιητικού που επιθυμεί να διαγράψει και να πατήσει το κουμπάκι «Αναζήτηση». Εάν βρεθεί ένα τέτοιο πιστοποιητικό, τότε εμφανίζονται τα στοιχεία του πιστοποιητικού με τρόπο παρόμοιο με αυτόν στην Εικόνα 9, αλλά υπάρχει ένα κουμπάκι στο κάτω μέρος που γράφει πάνω του «Διαγραφή», το οποίο μπορεί να χρησιμοποιήσει ο χρήστης για την οριστική διαγραφή του

πιστοποιητικού. Εάν δεν βρεθεί τέτοιο πιστοποιητικό, τότε εμφανίζεται το κατάλληλο μήνυμα λάθους. Πρέπει να σημειωθεί ότι στην πραγματικότητα πραγματοποιείται απενεργοποίηση του πιστοποιητικού και όχι πραγματική διαγραφή από την αλυσίδα Blockchain. Η απενεργοποίηση γίνεται μεταβιβάζοντας το πιστοποιητικό σε έναν νέο owner με τιμή null.

The screenshot shows the 'Δημιουργία νέου Πιστοποιητικού' (Create New Certificate) form in the UniChain application. The form includes the following fields:

- Asset id: Το ID του ιδιοκτήτη
- Owner: Ιδιοκτήτης πιστοποιητικού
- Όνομα: Το όνομα του owner
- Επώνυμο: Το επώνυμο του owner
- Εθνικότητα: Η εθνικότητα του owner
- Διεύθυνση: Η διεύθυνση του owner
- Πανεπιστήμιο: Το πανεπιστήμιο που εκδίδει το Πιστοποιητικό
- Τίτλος: Ο τίτλος του Πιστοποιητικού
- Τύπος: Bachelor (dropdown menu)
- Ημερομηνία: mm/dd/yyyy (date picker)
- Θαλάκι: (checkbox)

A green 'Δημιουργία' (Create) button is at the bottom right. The footer shows '© 2025 - UniChain'.

Εικόνα 13: Εισαγωγή νέου πιστοποιητικού

The screenshot shows the 'Διαγραφή πιστοποιητικού:' (Delete Certificate) form in the UniChain application. It features a yellow box with the text 'Αναζήτηση με βάση το ID' (Search by ID). Below this is a text input field labeled 'ID του πιστοποιητικού' and a blue 'Αναζήτηση' (Search) button. The footer shows '© 2025 - UniChain'.

Εικόνα 12: Οθόνη διαγραφής πιστοποιητικού

Κεφάλαιο 5^ο

5. Επίλογος και συμπεράσματα

Η τεχνολογία Blockchain επιτρέπει τη δημιουργία ενός κατακευματισμένου συστήματος καταγραφής δεδομένων (distributed ledger) σε μορφή αλυσίδας. Τα δεδομένα προστίθενται στην αλυσίδα αυτή υπό τη μορφή ψηφιακών blocks δεδομένων. Τα νέα blocks δεδομένων προστίθενται με ασφαλή τρόπο στο τέλος της αλυσίδας και ταυτόχρονα, κάθε νέο block επαληθεύει τη γνησιότητα του προηγούμενου block, εξασφαλίζοντας έτσι ότι τα δεδομένα των προηγούμενων blocks δεν έχουν τροποποιηθεί ή καταστραφεί με οποιονδήποτε τρόπο. Δεν είναι επομένως δυνατή η εκ των υστέρων τροποποίηση ή κακοπροαίρετη αλλοίωση των δεδομένων τα οποία αποθηκεύονται στην αλυσίδα, εξασφαλίζοντας έτσι την ακεραιότητα των δεδομένων.

Η τεχνολογία Blockchain μπορεί να φέρει σημαντικές και επαναστατικές αλλαγές στον χώρο της Εκπαίδευσης και τη συνεργασία ανάμεσα στους διάφορους εκπαιδευτικούς φορείς και τους υποψήφιους εργοδότες. Ένα δίκτυο Blockchain μπορεί να βοηθήσει στην καταγραφή και επαλήθευση τίτλων σπουδών, αποθήκευση και επαλήθευση βιογραφικών σημειωμάτων, καταχώρηση ερευνητικών εργασιών, διανομή διδακτικού υλικού, υλοποίηση εξ αποστάσεως μαθημάτων, ανταλλαγή φοιτητών ανάμεσα σε ανώτατα εκπαιδευτικά ιδρύματα, καταγραφή και διαχείριση πόρων κλπ. Από την έρευνα που έχει γίνει στον χώρο της Εκπαίδευσης σχετικά με την επαλήθευση πιστοποιητικών με τη βοήθεια της τεχνολογίας Blockchain, μπορούμε να καταλήξουμε στο συμπέρασμα ότι υπάρχει πολύ μεγάλο ενδιαφέρον από τους εκπαιδευτικούς φορείς για την ανάπτυξη τέτοιων συστημάτων. Ήδη έχουν αναπτυχθεί κάποια ανοικτά πρότυπα και έχουν υποβληθεί αρκετές προτάσεις, όμως υπάρχουν κάποια σημαντικά εμπόδια και δυσκολίες που θα πρέπει να αντιμετωπιστούν έτσι ώστε να υπάρξει ευρεία αποδοχή των λύσεων αυτών. Συμπερασματικά μπορούμε να πούμε ότι υπάρχει πολύς ακόμη δρόμος και αρκετές προκλήσεις και δυσκολίες οι οποίες θα πρέπει να αντιμετωπιστούν.

Με τη βοήθεια της τεχνολογίας Blockchain είναι δυνατόν να δημιουργηθεί ένα σύστημα καταγραφής και ανάκτησης ακαδημαϊκών τίτλων, η γνησιότητα των οποίων μπορεί να επιβεβαιωθεί οποιαδήποτε στιγμή από κάθε ενδιαφερόμενο. Υπάρχουν διάφορες πλατφόρμες Blockchain (frameworks). Ένα Blockchain framework περιλαμβάνει όλα εκείνα τα εργαλεία τα οποία επιτρέπουν τη δημιουργία ενός δικτύου Blockchain και την ανάπτυξη εφαρμογών για τη διαχείριση των συναλλαγών που θα αποθηκεύονται στο δίκτυο. Περιλαμβάνει δηλαδή όλα εκείνα τα εργαλεία και τις βιβλιοθήκες τα οποία έχουν σκοπό να απλοποιήσουν τη διαδικασία της δημιουργίας μίας εφαρμογής για δίκτυο Blockchain.

Η επιλογή ενός framework για την ανάπτυξη ενός δικτύου Blockchain δεν είναι εύκολη γιατί υπάρχουν αρκετές επιλογές με διαφορετικές ιδιότητες. Η επιλογή θα πρέπει να γίνει με βάση τις ανάγκες και τα επιθυμητά χαρακτηριστικά του δικτύου που θα αναπτυχθεί. Ένα βασικό κριτήριο επιλογής του κατάλληλου framework έχει σχέση με τον τύπο του δικτύου Blockchain το οποίο πρόκειται να αναπτυχθεί. Ένα από τα πιο δημοφιλή frameworks για την ανάπτυξη δικτύου Blockchain είναι το Hyperledger Fabric, το οποίο αποτελεί μία πλατφόρμα ανοικτού κώδικα για τη δημιουργία δικτύου κατακεντρωμένου ledger (distributed ledger). Το Hyperledger Fabric εισάγει μία νέα αρχιτεκτονική με στόχο την ευελιξία, την αντοχή στα σφάλματα, τη δυνατότητα κλιμάκωσης και την εμπιστευτικότητα ανάμεσα στους χρήστες του δικτύου. Η πλατφόρμα δημιουργήθηκε για να αντιμετωπίσει κάποιες από τις αδυναμίες που αντιμετώπιζαν τα δίκτυα permissioned Blockchain.

Στην παρούσα εργασία παρουσιάζεται μία μελέτη των χαρακτηριστικών της τεχνολογίας Blockchain τα οποία μπορούν να βοηθήσουν για την αξιόπιστη αποθήκευση δεδομένων που αφορούν ακαδημαϊκούς τίτλους. Σκοπός της προσπάθειας αυτής ήταν να μελετήσει τα διαθέσιμα εργαλεία που προσφέρει το HyperLedger Fabric, για την ανάπτυξη ενός απλού συστήματος το οποίο θα επιτρέπει την εισαγωγή σε ένα Blockchain των πληροφοριών που σχετίζονται με την κτήση ενός ακαδημαϊκού τίτλου από κάποιον φοιτητή ενός ιδρύματος της τριτοβάθμιας Εκπαίδευσης.

Συμπερασματικά μπορούμε να πούμε ότι η πλατφόρμα HyperLedger Fabric απλοποιεί σε μεγάλο βαθμό πολλές από τις δυσκολίες που εμφανίζονται κατά την ανάπτυξη ενός δικτύου Blockchain. Η τεχνολογία Blockchain με τη βοήθεια

frameworks όπως είναι το HyperLedger Fabric, είναι αρκετά ώριμη έτσι ώστε να μπορεί να χρησιμοποιηθεί τον ακαδημαϊκό χώρο για να λύσει το πρόβλημα της επαλήθευσης ακαδημαϊκών τίτλων.

Βιβλιογραφικές

- [1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 2008.
<https://bitcoin.org/bitcoin.pdf>
- [2] Marco Iansiti & Karim R. Lakhani. "The truth about Blockchain. It will take years to transform business, but the journey begins now.", 2017.
<https://hbr.org/2017/01/the-truth-about-blockchain>
- [3] Sherman, Alan T., Javani, Farid, Zhang, Haibin & Golaszewski, Enis (January 2019). "On the Origins and Variations of Blockchain Technologies". IEEE Security Privacy. 17 (1): 72–77. arXiv:1810.06130.
doi:10.1109/MSEC.2019.2893730. ISSN 1558-4046. S2CID 53114747
- [4] Ethereum. "Ethereum Whitepaper", 2014. <https://ethereum.org/en/whitepaper/>.
- [5] Wikipedia. "Blockchain", 2025. <https://en.wikipedia.org/wiki/Blockchain#>.
- [6] Jordan Tuwiner. "79+ Blockchain Statistics, Facts, and Trends (2024)". Σεπτέμβριος 2023. <https://buybitcoinworldwide.com/blockchain-statistics/>
- [7] Statista. "Blockchain technology use cases in organizations worldwide as of 2021". Ιανουάριος 2025.
<https://www.statista.com/statistics/878732/worldwide-use-cases-blockchain-technology/>
- [8] Mary K. Prat. "Top 10 benefits of blockchain for business". Σεπτέμβριος 2023. <https://www.techtarget.com/searchcio/feature/Top-10-benefits-of-blockchain-technology-for-business>
- [9] Wikipedia. "Blockchain". Ιανουάριος 2025.
<https://el.wikipedia.org/wiki/Blockchain>.
- [10] A. Grech and A. F. Camilleri. "Blockchain in Education". Luxembourg, U.K.: 824 Publications Office of the European Union, 2017.
- [11] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology 843 and its potential applications for education" Smart Learn. Environ., vol. 5, 844 no. 1, pp. 1–10, 2018.
- [12] A. Alammery, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based 846 applications in education: A systematic review" Appl. Sci., vol. 9, no. 12, 847 p. 2400, 2019

- [13] Kamisalic, A., Turkanovic, M., Mrdovic, S. & Hericko, M. "A Preliminary Review of Blockchain-Based Solutions in Higher Education". In Proceedings of the 8th International Workshop on Learning Technology for Education Challenges, LTEC 2019; Liberona, D., Uden, L., Sanchez, G., Rodriguez-Gonzalez, S., Eds.; Springer Nature: Basingstoke, UK, 2019; pp. 114–124.
- [14] Cheng, J.C., Lee, N.Y., Chi, C. & Chen, Y.H. "Blockchain and Smart Contract for Digital Certificate". Presented at the 4th IEEE International Conference on Applied System Innovation, ICASI, Chiba, Japan, 13–17 April 2018.
- [15] Duan, B., Zhong, Y. & Liu, D. "Education Application of Blockchain Technology: Learning Outcome and Meta-Diploma". Presented at the 23rd IEEE International Conference on Parallel and Distributed Systems, ICPADS, Shenzhen, China, 15–17 December 2017.
- [16] Gresch, J., Rodrigues, B., Scheid, E., Kanhere, S.S. & Stiller, B. "The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling". In Proceedings of the 21st International Conference on Business Information Systems, BIS 2018; Abramowicz, W., Paschke, A., Eds.; Springer Nature: Basingstoke, UK, 2019; pp. 185–196.
- [17] Vidal, F., Gouveia, F. & Soares, C. "Analysis of Blockchain Technology for Higher Education". Presented at the 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC, Guilin, China, 17–19 October 2019.
- [18] San, A.M., Chotikakamthorn, N., Sathitwiriawong & C. "Blockchain-Based Learning Credential Verification System with Recipient Privacy Control". Presented at the 2019 IEEE International Conference on Engineering, Technology and Education, TALE, Yogyakarta, Indonesia, 10–13 December 2019.
- [19] Nikolskaia, K., Snegireva, D. & Minbaleev, A. "Development of the Application for Diploma Authenticity Using the Blockchain Technology". Presented at the 2019 IEEE International Conference “Quality Management, Transport and Information Security, Information Technologies”, IT and QM and IS, Sochi, Russia, 23–27 September 2019.
- [20] Serranito, D., Vasconcelos, A., Guerreiro, S., Correia & M. Blockchain

- "Ecosystem for Verifiable Qualifications". Presented at the 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS, Paris, France,, 28–30 September 2020.
- [21] Capece, G., Ghiron, N.L. & Pasquale, F. "Blockchain Technology: Redefining Trust for Digital Certificates". Sustainability 2020, 12, 8952.
- [22] Meyliana, Chandra, Y.U., Cassandra, C. Surjandy, Eka Widjaja, H.A., Fernando, E., Prabowo, H. & Joseph, C. "Defying the Certification Diploma Forgery with Blockchain Platform: A Proposed Model". Presented at the 12th International Conference on ICT, Society and Human Beings, ICT 2019, 5th International Conference on Connected Smart Cities, CSC 2019 and the 16th International Conference on Web Based Communities and Social Media, WBC, Porto, Portugal, 19 July 2019.
- [23] Vidal, F.R., Gouveia, F. & Soares, C. "Revocation Mechanisms for Academic Certificates Stored on a Blockchain". Presented at the 15th Iberian Conference on Information Systems and Technologies, CISTI, Seville, Spain, 24–27 June 2020.
- [24] Taufiq, R., Trisetyarso, A., Meyliana, Kosala, R., Ranti, B., Supangkat, S. & Abdurachman, E. "Robust Crypto-Governance Graduate Document Storage and Fraud Avoidance Certificate in Indonesian Private University". Presented at the 4th International Conference on Information Management and Technology, ICIMTech, Jakarta/Bali, Indonesia, 19–20 August 2019.
- [25] Blockcerts, "The Open Standard for Blockchain Credentials", Ιανουάριος 2025, <https://www.blockcerts.org/>.
- [26] Sharples, M. & Domingue, J. "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward". In Adaptive and Adaptable Learning, Ec-Tel 2016 9891; Springer Nature: Basingstoke, UK, 2016; pp. 490–496.
- [27] Nguyen, D.H., Nguyen-Duc, D.N., Huynh-Tuong, N. & Pham, H.A. "Cvss: A Blockchainized Certificate Verifying Support System". Presented at the 9th International Symposium on Information and Communication Technology, SoICT, Danang City, Vietnam, 6–7 December 2018.
- [28] Underwood, S. "Blockchain beyond bitcoin" Communications of the ACM, vol. 59, no. 11, p. 15(17), 2016. Available: <https://dl.acm.org/citation>.

- [29] N. Szabo, "Smart contracts: Building blocks for digital markets", 1994.
Available: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/DROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smartcontracts2.html>
- [30] Tatum, "An In-depth Look Into Blockchain Frameworks", Available:
<https://tatum.io/blog/blockchain-frameworks>.
- [31] Androulaki, E., Cachin, C., Ferris, C., Muralidharan, S., Murthy, C., Nguyen, B. & Sethi, M. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains", EuroSys '18: Proceedings of the Thirteenth EuroSys Conference, Article No.: 30, Pages 1 – 15.
- [32] M. Vukolić. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication". In International Workshop on Open Problems in Network Security (iNetSec), pages 112–125, 2015.