ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ ΣΧΟΛΗ

ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ

ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εφαρμογή και μελέτη των διαφορετικών τεχνολογιών blockchain στη διαδικασία έκδοσης, επαλήθευσης πιστοποιητικών και τίτλων σπουδών

Λοντόρφος Νικόλαος-Ιωάννης

Επιβλέποντες :

Δρ. Κωνσταντίνος Σιασιάκος
Επιστημονικός Συνεργάτης Ε.Μ.Π

Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π

Αθήνα, Ιούνιος 2021

Περιεχόμενα

Πίνακας εικόνων 4

Κεφάλαιο 1:Εισαγωγή 5

1.1 Ο προβληματισμός που πραγματεύεται η διπλωματική 5

1.2 Σπουδαιότητα της πιστοποίησης των τίτλων σπουδών 6

1.3 Δομή διάρθρωση των κεφαλαίων της εργασίας 7

1.3 Βιβλιογραφική αιτιολόγηση 8

Κεφάλαιο 2:Σημερινές Πρακτικές πιστοποίησης και ο ρόλος των πιστοποιητικών σπουδών 9

2.1 Εισαγωγή 9

2.2 Πώς διεξάγεται μέχρι στιγμής η διαδικασία έγκρισης πιστοποιητικών στην Ευρώπη 10

2.3 Η αξία εφαρμογής τεχνλογιών blockchain σε πιστοποιητικά σπουδών 12

2.4 Θετικά και αρνητικά από τη χρήση της τεχνολογίας blockchain στην επαλήθευση και έγκριση πιστοποιητικών 14

2.5 Σύνοψη 17

Κεφάλαιο 3: Περιγραφή της τεχνολογίας blockchain 18

3.1 Εισαγωγή 18

3.2 Τεχνολογία blockchain 19

3.2.1 Δίκτυα Ομότιμων Κόμβων 21

3.3 Βασικά χαρακτηριστικά του Blockchain 23

3.3.2 Χρόνος εκτέλεσης των διαδικασιών στο blockchain 23

3.3.3 Εμπιστευτικότητα 24

3.3.4 Χαρακτηριστικά των blockchain 24

3.4 Τοπολογίες blockchain 26

3.4.1 Αναλυτική περιγραφή των τοπολογιών blockchain 30

3.5 Αρχιτεκτονική του blockchain και περιγραφή των δομικών μερών 35

3.5.1 Αρχιτεκτονική του blockchain 35

3.5.2 Τι είναι το block 37

3.5.3 Τι είναι η συναίνεση(consensus) 38

3.5.4 Τύποι εγγραφών που αποθηκεύονται στο blockchain 39

3.6 Στοιχειώδεις έννοιες του Blockchain 40

3.6.1 Κρυπτογραφία 40

3.6.2 Τι είναι το hash 41

3.6.3 Ψηφιακές υπογραφές 42

3.7 Ανάλυση Πλεονεκτημάτων μειονεκτημάτων της τεχνολογίας 42

3.7.1 Μειονεκτήματα της τεχνολογίας blockchain 42

3.8 Σύνοψη 43

Κεφάλαιο 4: Διαφορετικές εφαρμογές με τη χρήση της τεχνολογίας blockchain για την έγκριση πιστοποιητικών 44
4.1 Εισαγωγή 44
4.1 Open Badges 44
4.2 Ορισμός Blockcert 46
4.3.Ορισμός OpenCert 48
4.3.1 Περιγραφή Αρχιτεκτονικής OpenCert 49
4.3.2 Περιορισμοί των OpenCert 51
4.4 Ευρωπαϊκή Συνεργασία Blockchain(EBSI) 52
4.4.1 Περιγραφή της αρχιτεκτονικής της Ευρωπαϊκής Συνεργασίας(EBSI) 52
4.5 BTCeRT 55
4.5.1 Περιγραφή της ροής εργασίας του BTCeRT 56
4.5.2 Περιγραφή της αρχιτεκτονικής του BTCeRT 57
4.6 SmartCert 59
4.7 Velocity Network 60
4.8 Περιγραφή αρχιτεκτονικής BcER^2 62
4.8.1 Οντότητες που απαρτίζουν το BcER^2 63
4.8.2 Επιχειρηματικό μοντέλο και στοιχεία του BcER^2 65
4.9 Περιγραφή του EduCTX 66
4.9.1 Πρωτόκολλο πολλαπλών υπογραφών 71
4.10 RecordsKeeper 72
4.11 Sony Global Education 73
4.12 Η δράση Blockademic 74
4.13 Λύση ψηφιακών πιστοποιητικών της Oracle 76
4.14 TrueRec Ινστιτούτο SAP 76
4.15 Hyperledger Indy 77
4.16 Δίπλωμα Qualichain 80
4.17 LinkChain 83
4.18 Blockchain for education 84
4.19 Σύνοψη 85
Κεφάλαιο 5:Εφαρμογές της τεχνολογίας blockchain στην εκπαίδευση 86
5.1 Εισαγωγή 86
5.2 Πανεπιστήμιο της Λευκωσίας(UNIC) 86
5.3 Δημοκρατία της Μάλτας 87
5.4 Κοινοτικό Κολέγιο Κεντρικού Νέου Μεξικού(Central New Mexico Community College) 88

5.5 Πολυτεχνική Σχολή Σιγκαπούρης(Ngee Ann) ... 88
5.5 Εθνικό Δίκτυο Έρευνας και Εκπαίδευσης της Ελλάδας(GRNET) ... 88
5.6 Ανοικτό Πανεπιστήμιο Αγγλίας(KMI) ... 89
5.7 National University of La Plata(UNLP) ... 90
5.8 CredenceLedger ... 90
Κεφάλαιο 6: Συμπεράσματα ... 92
6.1 Εισαγωγή ... 92
Βιβλιογραφία ... 93

Πίνακας εικόνων

Εικόνα 1:Πιστοποίηση Udemy ... 13
Εικόνα 2:Πώς λειτουργεί το Blockchain ... 21
Εικόνα 3:Χαρακτηριστικά των Blockchain ... 27
Εικόνα 4:Επιγραμματικά οι τύποι αλυσίδας Blockchain ... 29
Εικόνα 5:Κατηγορίες blockchain ... 30
Εικόνα 6:Public Blockchain ... 31
Εικόνα 7:Private Blockchain ... 33
Εικόνα 8:Hybrid Blockchain ... 34
Εικόνα 9:Πώς λειτουργεί η τεχνολογία blockchain ... 35
Εικόνα 10:Δομικά μέρη ενός block ... 38
Εικόνα 11:Παράδειγμα πιστοποιητικού Open Badges.Η μορφή είναι JSON-LD και ως Linked Data αντικείμενο, επιτρέπει αναφορά σε διαδικτυακούς πόρους που περιέχουν πρόσθετες πληροφορίες. .. 45
Εικόνα 12:Διαδικασία εξακρίβωσης του πιστοποιητικού BlockCert ... 47
Εικόνα 13:Διαδικασία επαλήθευσης πιστοποιητικού BlockCert ... 48
Εικόνα 14:Δομή OpenCert ... 49
Εικόνα 15:Δομή Europass πιστοποιητικό ... 54
Εικόνα 16:Δομή πιστοποιητικού στο EBSI ... 55
Εικόνα 17:Μηχανισμός λειτουργίας BTCert ... 56
Εικόνα 18:Ροή εργασίας BTCert ... 57
Εικόνα 19:Αρχιτεκοτνική BTCert ... 58
Εικόνα 20:Το δίκτυο Velocity ... 62
Εικόνα 21:Περιγραφή δημιουργίας "Μητρώου Πιστοποιητικών" στο BcER^2 ... 63
Εικόνα 22:Βασικά στοιχεία του BcER2 ... 65
Εικόνα 23:Μια απεικόνιση της δομής του EduCTX ... 68
Εικόνα 24:Hyperledger Indy ... 80
Εικόνα 25:Αρχιτεκτονική οικοσυστήματος Qualichain Diploma ... 81
Εικόνα 26:Περιγραφή του HEI Client ... 82
Εικόνα 27:Διαδικασία επαλήθευσης αυθεντικότητας πιστοποιητικού ... 83
Εικόνα 28:Αρχιτεκτονική του Blockchain4Education ... 84
Εικόνα 29:Πιλοτικό έργο blockchain για εκπαιδευτικά ιδρύματα ... 89
Εικόνα 30:Αρχιτεκτονική Credenceledger ... 91

Κεφάλαιο 1:Εισαγωγή

1.1 Ο προβληματισμός που πραγματεύεται η διπλωματική

Ο έλεγχος και η επικύρωση των τίτλων σπουδών κατέχουν κυρίαρχη θέση στον τομέα της εκπαίδευσης, αφού είναι απαραίτητα για την επαλήθευση των προσόντων των εκπαιδευόμενων. Όμως ο μέχρι τώρα τρόπος με τον οποίο διεξάγεται η όλη διαδικασία παρουσιάζει αρκετά μειονεκτήματα στο σύνολο της. Τα πιο σημαντικά εξ 'αυτών αφορούν τη διάθεση των διαπιστευτηρίων σπουδών σε μορφές οι οποίες είναι εύκολο να αλλοιωθούν να πλαστογραφηθούν και να χαθούν, στην εξάρτηση τους από τρίτους φορείς όπως εκπαιδευτικούς οργανισμούς για την έκδοση και επικύρωση τους αλλά και στο ότι αυτές οι διαδικασίες είναι ιδιαίτερα χρονοβόρες ,στην αδυναμία επαλήθευσης ανεπίσημων μορφών εκπαίδευσης όπως π.χ. ένα online πιστοποιητικό παρακολούθησης ενός σεμιναρίου,γεγονός που αποτελεί ολοένα και περισσότερο συστατικό της δια βίου εκπαίδευσης.

Λαμβάνοντας υπόψη όλα τα ανωτέρω,στόχος της συγκεκριμένης διπλωματικής αποτελεί η μελέτη και ανάλυση της τρέχουσας τεχνολογίας blockchain που αναπτύσσεται στο τομέα της επικύρωσης και επαλήθευσης των τίτλων σπουδών και εργασιακών προσόντων, η αναφορά και καταγραφή πρόσφατων πρωτοβουλιών τόσο από εκπαιδευτικά ιδρύματα καθώς και πλατφόρμες από τρίτους,η περιγραφή των δομικών στοιχείων της τεχνολογίας,αλλά και η λύση που παρέχουν αυτές οι πρωτοβουλίες στα προαναφερθέντα προβλήματα.Τέλος, η εργασία εστιάζει στη τεχνολογία blockchain και στις ωφέλειες που αυτή παρέχει σε σχέση με την ήδη υπάρχουσα διαδικασία.

1.2 Σπουδαιότητα της πιστοποίησης των τίτλων σπουδών

Η διαδικασία της πιστοποίησης αποτελεί μια μορφή αξιολόγησης η οποία βασίζεται σε σαφή, προσδιορισμένα κριτήρια, διεθνώς αποδεκτά. Προϋπόθεση των αντικειμενικών αυτών κριτηρίων, είναι πρωτίστως να έχουν δημοσιοποιηθεί τόσο ποσοτικά όσο και ποιοτικά μαζί με τους δείκτες μέτρησης που χρησιμοποιούν και να προσαρμόζονται στις Αρχές και Κατευθυντήριες Οδηγίες για τη Διασφάλιση Ποιότητας στον Ευρωπαϊκό Χώρο Ανώτατης Εκπαίδευσης (ΕΧΑΕ). Οι ακαδημαϊκές πιστοποιήσεις αφορούν όλες τις μορφές σπουδών Ανώτατης Εκπαίδευσης(διασυνοριακά, διακρατικά, e-learning), τα Δια Βίου Μάθησης και τα Εσωτερικά Συστήματα Διασφάλισης Ποιότητας των Ιδρυμάτων. Σύμφωνα με τις βασικές αρχές της πιστοποίησης, διακρίνεται ο σχεδιασμός και η αναθεώρηση των Προγραμμάτων Σπουδών έτσι ώστε να συμβαδίζουν με την αιχμή της επιστήμης, να είναι ελκυστικά ως προς το τι προσφέρουν και να ακολουθούν την τρέχουσα αγορά εργασίας. Ένα επιπλέον βασικό χαρακτηριστικό αποτελεί η δυνατότητα έρευνας και καινοτομίας από μια πιο φοιτητοκεντρική οπτική. Επιπρόσθετα χαρακτηριστικά αποτελούν:

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

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

Αντίστοιχα, στα Ελληνικά δεδομένα, η πιστοποίηση οδηγεί σε αναβάθμιση της αξίας των ελληνικών τίτλων σπουδών και κατά συνέχεια και σε διεθνή αναγνώρισή τους. Σε ανταγωνισμό προς τις ευρωπαϊκές χώρες έρχεται η Ελλάδα σε αυτόν τον τομέα, καθώς η πιστοποίηση εφαρμόζεται στη συντριπτική πλειοψηφία των προσφερόμενων προγραμμάτων σπουδών πανευρωπαϊκά. Αποτέλεσμα της πιστοποίησης είναι η δυνατότητα συμμετοχής και συνέχισης των σπουδαστών σε Μεταπτυχιακά Προγράμματα Σπουδών της Ευρώπης και διεθνώς, τα περισσότερα εκ των οποίων ανταποκρίνονται στη κατοχή πιστοποιημένου τίτλου σπουδών. Είναι γεγονός ότι η κατοχή πιστοποιημένων τίτλων σπουδών αποτελεί βασικό παράγοντα στην τάση της αγοράς ως προς την εύρεση εργασίας και αποτελεί κύριο πιστοποιητικό και κριτήριο πρόσληψης για την αγορά εργασίας (ειδικότερα σε περιπτώσεις έλλειψης εμπειρίας και πρακτικής). Ένας επιπλέον παράγοντας, είναι ότι μέσω της πιστοποίησης υπάρχει αυτομάτως μία σύνδεση ενός προγράμματος σπουδών με τον οικείο επαγγελματικό κλάδο και τα απαιτούμενα επαγγελματικά προσόντα. Για τον εργοδότη, η πιστοποίηση παρέχει μια μορφή εγγύησης και διασφαλίζει ότι ο απόφοιτος κατέχει τις απαιτούμενες γνώσεις, ικανότητες και δεξιότητες που απαιτεί μια συγκεκριμένη θέση εργασίας. Τέλος, οι διακρατικές συνεργασίες σε κοινά προγράμματα σπουδών προαπαιτούν την πιστοποίηση των προγραμμάτων αυτών.

1.3 Δομή διάρθρωση των κεφαλαίων της εργασίας

Για την καλύτερη κατανόηση του θέματος της εργασίας παρατίθεται η διάρθρωση των κεφαλαίων της.

Στο κεφάλαιο 1 περιγράφεται το αντικείμενο της εργασίας και τίθενται οι στόχοι και τα θέματα τα οποία η παρούσα εργασία καλείται να μελετήσει και να παρουσιάσει.

Στο κεφάλαιο 2 γίνεται μια αναφορά στην διαδικασία έγκρισης πιστοποιητικών δεδομένων, με εκτενείς αναφορές στο πως πραγματοποιούνται σε ευρωπαϊκό πλαίσιο.Εν συνεχεία,γίνεται αναφορά στα οφέλη της τεχνολογίας όσον αφορά την έγκριση πιστοποιητικών καθώς και εκτενέστερα τα γενικότερα θετικά και αρνητικά χαρακτηριστικά τα οποία έχει.

Στο κεφάλαιο 3 παρουσιάζονται αναλυτικά,το κάθε ένα ξεχωριστά,τα δομικά στοιχεία από τα ποία απαρτίζεται αυτή η τεχνολογία καθώς και ο τρόπος με τον οποίο λειτουργούν.

Στο κεφάλαιο 4 αναφέρονται λεπτομερώς κάποιες ήδη υπάρχουσες δράσεις που αφορούν την τεχνολογία Blockchain και την έγκριση πιστοποιητικών,καθώς και κάποιες άλλες οι οποίες βρίσκονται σε πιλοτικό επίπεδο και δεν έχουν ανακοινωθεί ακόμα επίσημα.

Στο κεφάλαιο 5 παρουσιάζονται κάποια εκπαιδευτικά ιδρύματα,τα οποία έχουν αναπτύξει ήδη την τεχνολογία Blockchain για την έγκριση πιστοποιητικών και πως αυτή βελτιώνει την όλη τη διαδικασία έγκρισης σε σχέση με την ως τώρα διαδικασία.

1.3 Βιβλιογραφική αιτιολόγηση

Στην τρέχουσα διπλωματική εργασία χρησιμοποιήθηκαν τρείς διαφορετικές βιβλιογραφικές πηγές, που αναφέρονται στη συνέχεια:

- Άρθρα–δημοσιεύσεις στο Διαδίκτυο, τόσο στην Ελλάδα όσο και στο εξωτερικό.
- Εργασίες (papers) και βιβλία (έντυπα και ηλεκτρονικά) σχετικά με τον κίνδυνο αγοράς.
- Προηγούμενες διπλωματικές – πτυχιακές εργασίες που διαπραγματευόντουσαν παρόμοια και συναφή με αυτό της παρούσας διπλωματικής εργασίας θέματα.

Στο τέλος της εργασίας υπάρχει εκτενής βιβλιογραφική ανασκόπηση.

Κεφάλαιο 2:Σημερινές Πρακτικές πιστοποίησης και ο ρόλος των πιστοποιητικών σπουδών

2.1 Εισαγωγή

Η εκπαίδευση παίζει θεμελιώδη ρόλο στην ανθρώπινη ζωή.Σπουδάζουμε στο σχολείο,στη συνέχεια στο πανεπιστήμιο και κατά τη διάρκεια των περισσότερων σταδιοδρομιών θα παρακολουθήσουμε περαιτέρω μαθήματα για να βελτιώσουμε τις δεξιότητες μας και να γίνουμε πιο πολύτιμοι ως ειδικοί. Το εκπαιδευτικό μας χαρτοφυλάκιο δεν περιέχει άμεσα τις γνώσεις που αποκτούμε ,αλλά έντυπα πιστοποιητικά που επιβεβαιώνουν το γεγονός ,ότι έχουμε λάβει μια συγκεκριμένη ικανότητα όπως για παράδειγμα:

- Δίπλωμα τριτοβάθμιας εκπαίδευσης
- Πιστοποιητικά Coursera και Udemy
- Πιστοποιητικά για συμμετοχή σε συνέδρια ή συμμετοχή σε hackathlons

Αυτά τα έγγραφα επιτρέπουν στους εργοδότες να αξιολογούν τους εργαζόμενους και τους διοργανωτές εκπαιδευτικών εκδηλώσεων για να αυξήσουν την αξία τους. Ο ρόλος αυτών των εγγράφων συχνά υποτιμάται. Ωστόσο εάν δεν δώσουμε επαρκή προσοχή στην αυθεντικότητα της εκπαίδευσης ενός υποψηφίου, αυτό μπορεί να προκαλέσει τεράστια προβλήματα για ένα άτομο ή ακόμα και για μια ολόκληρη χώρα. Για παράδειγμα, τον Δεκέμβριο του 2019,ένα σκάνδαλο συνέβη στη Νιγηρία όταν έγινε γνωστό ότι περισσότεροι από 100 καθηγητές πανεπιστημίων κατείχαν πλαστά διπλώματα.Τέτοια προηγούμενα θα πρέπει να μας ωθήσουν στο να επανεξετάσουμε την προσέγγισή μας για την έκδοση πιστοποιητικών στο μέλλον..Επί του παρόντος,τα πιστοποιητικά εκδίδονται σε δύο μορφές:χαρτί και ηλεκτρονικό πιστοποιητικό.Ένα πιστοποιητικό,όπως αρχικά είχε σχεδιαστεί,είναι ένα κομμάτι χαρτί με πληροφορίες τυπωμένες σε αυτό ότι ο κομιστής έχει ολοκληρώσει ένα εκπαιδευτικό μάθημα.Αυτό μπορεί να φέρει σφραγίδα ή επωνυμία από τον οργανισμό που διεξήγαγε το μάθημα,αλλά σε κάθε περίπτωση είναι εξαιρετικά εύκολο να πλαστογραφηθεί ένα τέτοιο έγγραφο.ένα ψηφιακό πιστοποιητικό που εκδίδεται σε ηλεκτρονική μορφή,είναι πιο βολικό.Οι χρήστες δεν χρειάζεται να ανησυχούν για την αποθήκευση του,μπορεί να υπάρχει σε σκληρούς δίσκους ή λογαριασμούς email για όσο χρειάζεται.Ωστόσο,αυτό εξακολουθεί να μην επιλύει το πρόβλημα της απόδειξης γνησιότητας.Ένα πιστοποιητικό το οποίο έχει εγγραφεί στο blockchain είναι μια βελτιωμένη έκδοση ενός ηλεκτρονικού πιστοποιητικού.Αυτό εξακολουθεί

να αποστέλλεται στο email του χρήστη σε μορφή pdf,αλλά επιπλέον τα δεδομένα του αποθηκεύονται σε ένα επίσης εξαιρετικά αξιόπιστο μέσο το blockchain.

2.2 Πώς διεξάγεται μέχρι στιγμής η διαδικασία έγκρισης πιστοποιητικών στην Ευρώπη

Η έκδοση διπλώματος είναι μια λεπτή διαδικασία, γιατί πρέπει να λαμβάνει υπόψη πολλές πληροφορίες που δεν είναι τόσο εύκολο να τροποποιηθούν. Επιπλέον, η διαδικασία επαλήθευσης της απόκτησης ορισμένου ακαδημαϊκού τίτλου είναι ακόμη πιο λεπτή και πιο εύκολα επεξεργάσιμη. Η διαδικασία είναι επίσης δαπανηρή από την άποψη των πόρων και του χρόνου και επομένως των χρημάτων. Στο Πανεπιστήμιο της Ρώμης «Tor Vergata», ένας φοιτητής που χρειάζεται να μοιραστεί το δίπλωμα ώστε να χρησιμοποιηθεί για τις ανάγκες του,έχει δύο δυνατότητες να ζητήσει αντίγραφο.

- Αυτός ή ο εκπρόσωπός του μπορεί να πάει προσωπικά στο γραφείο της Γραμματείας φοιτητών και αφού αποδείξει την ταυτότητά του με προσωπικά έγγραφα και με αριθμό φοιτητικού πάσου, ζητάει το πιστοποιητικό αποφοίτησης του,το οποίο η Γραμματεία μπορεί να εκδώσει και να παραδώσει απευθείας στον φοιτητή.

- Εάν ο φοιτητής δεν μπορεί να προσέλθει προσωπικά στη Γραμματεία φοιτητών καθώς και κανένας από τους αντιπροσώπους του, ο φοιτητής μπορεί να στείλει το αίτημα του για πιστοποιητικό αποφοίτησης μέσω email. Για την επαλήθευση της ταυτότητας του, τα αρμόδια γραφεία απαιτούν ορισμένα διαπιστευτήρια που έχει ήδη το Πανεπιστήμιο στη διάθεση του, όπως τη διεύθυνση του ηλεκτρονικού ταχυδρομείου και τον αριθμό τηλεφώνου του,τα οποία χρησιμοποίησε ο φοιτητής κατά τη διάρκεια της πανεπιστημιακής περιόδου,καθώς και τα σαρωμένα αντίγραφα των δύο όψεων της ταυτότητας του.Αφού πραγματοποιηθούν οι απαραίτητοι έλεγχοι για την επαλήθευση των διαπιστευτήριων του φοιτητή και το δικαίωμα κατοχής του τίτλου, τα αρμόδια γραφεία προβαίνουν στην έκδοση του απαιτούμενου πιστοποιητικού με τις κατάλληλες σφραγίδες και υπογραφές με πλάγια γράμματα, σημαντικά για την αναγνώριση και την επικύρωση του από τρίτους. Το πιστοποιητικό σε ηλεκτρονική μορφή αποστέλλεται μέσω πιστοποιημένου email (Posta Elettronica Cartificata — PEC) στον φοιτητή.

- Εάν η διεύθυνση ηλεκτρονικού ταχυδρομείου και ο αριθμός κινητού τηλεφώνου είναι διαφορετικοί από αυτούς που χρησιμοποιεί ο φοιτητής κατά τη διάρκεια της πανεπιστημιακής περιόδου, το Πανεπιστήμιο θα ελέγξει τα έγγραφα για την

πραγματική κατοχή του πτυχίου. Εάν η διαδικασία είναι επιτυχής, τα αρμόδια γραφεία προβαίνουν στην έκδοση του πιστοποιημένου πιστοποιητικού που ζητήθηκε με τις κατάλληλες σφραγίδες και υπογραφές με πλάγια γράμματα, σημαντικά για την αναγνώριση και την επικύρωση. Το πιστοποιητικό σε ηλεκτρονική μορφή αποστέλλεται μέσω πιστοποιημένου email (PEC) στον μαθητή.

Η διαδικασία είναι διαφορετική όταν ένα τρίτο μέρος απαιτεί από το Πανεπιστήμιο διαπιστευτήρια για το εάν ένας φοιτητής έχει πραγματικά ένα συγκεκριμένο προσόν.

- Εάν το αίτημα υποβάλλεται από άλλη Δημόσια Διοίκηση μέσω του PEC, το Πανεπιστήμιο, μετά τη δέουσα επαλήθευση της κατοχής του τίτλου από τον φοιτητή, πάντα μέσω του PEC, επιβεβαιώνει ή αρνείται τον τίτλο

- Εάν το αίτημα προέρχεται από εταιρεία (ιταλική ή ξένη), το Πανεπιστήμιο δεν υποχρεούται να παράσχει πληροφορίες σχετικά με το πτυχίο που έλαβε ο φοιτητής . Το αίτημα πρέπει να υποβληθεί από τον ίδιο τον φοιτητή,ο οποίος αφού αποκτήσει το πτυχίο, μπορεί στη συνέχεια να κάνει την απαραίτητη χρήση.

Στο εξωτερικό, υπάρχουν εταιρείες που λειτουργούν ως διασύνδεση μεταξύ της εταιρείας που απαιτεί την επαλήθευση του πιστοποιητικού και του Πανεπιστημίου. Εάν το πιστοποιητικό αποφοίτησης υπάρχει,στο αίτημα που αποστέλλεται μέσω email από το φοιτητή, το Πανεπιστήμιο θα δώσει θετική ή αρνητική απάντηση όταν έχουν γίνει οι απαραίτητοι έλεγχοι. Εάν το πιστοποιητικό που πρόκειται να επαληθευτεί δεν επισυνάπτεται στο email, ο φοιτητής πρέπει να ζητήσει αντίγραφο του πιστοποιητικού πτυχίου και το Πανεπιστήμιο θα προχωρήσει, όπως φαίνεται προηγουμένως. Η διαδικασία αυτή έχει υποστηριχθεί από την Adonis Community Edition, και ως εκ τούτου εκτιμήθηκε το κόστος της. Στο Πανεπιστήμιο της Ρώμης «Tor Vergata», η διαδικασία επαλήθευσης ενός διπλώματος πιστοποιητικού κοστίζει περίπου 3,48 ευρώ ανά πιστοποιητικό. Το χρονικό διάστημα μεταξύ της παραλαβής του αιτήματος και της αποστολής της απάντησης είναι κατά μέσο όρο 3 ημέρες. Λαμβάνοντας υπόψη ότι ένας μέσος αριθμός αποφοίτων ετησίως ισούται με 5400, το συνολικό κόστος αυτής της δραστηριότητας είναι περίπου 18.792 ευρώ, το οποίο δεν είναι ασήμαντο, παρόλο που σε ένα οικονομικό δελτίο του Πανεπιστημίου θα μπορούσε να είναι αμελητέο.Στην πραγματικότητα, στόχος δεν είναι απλώς οικονομική εξοικονόμηση, αλλά η αποτελεσματικότητα και η επεκτασιμότητα της διαδικασίας που θα επηρέαζε όχι μόνο την ίδια τη διαδικασία, αλλά και άλλες διαδικασίες που θα μπορούσαν να κερδίσουν περισσότερο χρόνο και πόρους. Δεκαπέντε λεπτά για κάθε

πιστοποιητικό είναι περίπου 81.000 λεπτά, που αντιστοιχούν σε 1350 ώρες ή 36,5 εβδομάδες εργασίας. Χρησιμοποιώντας την τεχνολογία Bitcoin Blockchain, το Πανεπιστήμιο έχει τη δυνατότητα να καταγράψει σε μία μόνο συναλλαγή μια ολόκληρη συνεδρία αποφοίτησης. Πράγματι, ενώ είναι δυνατόν να εκδοθεί ένα πιστοποιητικό με μία συναλλαγή Bitcoin, είναι πολύ πιο αποτελεσματικό να χρησιμοποιηθεί μία συναλλαγή Bitcoin για να εκδωθεί μια παρτίδα πιστοποιητικών. Ο εκδότης του πιστοποιητικού δημιουργεί ένα Merkle δέντρο με κατακερματισμούς πιστοποιητικών και καταγράφει το Merkle root ως ένα πεδίο στη Bitcoin συναλλαγή. Λαμβάνοντας ως υπόθεση ότι η παρτίδα περιέχει n πιστοποιητικά και το πιστοποιητικό i περιέχει τις πληροφορίες του παραλήπτη. Ο εκδότης θα κατακερματίσει κάθε πιστοποιητικό και θα τα συνδυάσει όλα μαζί σε ένα Merkle δέντρο. Μια συναλλαγή Bitcoin καθορίζεται από το μέγεθος της συναλλαγής και το τέλος συναλλαγής. Τα μεγέθη συναλλαγών Blockcerts είναι στατικά και μικρά,προσθέτουν μία έξοδο σταθερού μεγέθους πάνω από μια τυπική συναλλαγή μίας εισόδου, μίας εξόδου.Αυτό ισχύει ανεξάρτητα από τον αριθμό των πιστοποιητικών σε παρτίδα. Επομένως, το κόστος έκδοσης παρτίδας Blockcerts επηρεάζεται σε μεγάλο βαθμό από το τέλος συναλλαγής, το οποίο είναι ένα τέλος που καταβάλλεται σε αυτούς που κάνουν εξόρυξη(mining) για να διασφαλιστεί η έγκαιρη εξόρυξη συναλλαγών. Η εκάστοτε χρέωση αλλάζει με την πάροδο του χρόνου. Στο έργο Blockcerts, το τέλος συναλλαγής είναι διαμορφώσιμο.Η προεπιλεγμένη τιμή (0,0006 bitcoin, περίπου πέντε ευρώ στην τρέχουσα συναλλαγματική ισοτιμία BTC / EURO) εγγυάται ότι η συναλλαγή με τη Merkle ρίζα των πιστοποιητικών είναι πολύ πιθανό να εισαχθεί στο επόμενο μπλοκ εξόρυξης.Αυτή η ρύθμιση μπορεί να παρακαμφθεί στο αρχείο προέλευσης για να μειωθεί το κόστος. Μετά από αυτήν την ενιαία λειτουργία στο Blockchain, οι φοιτητές είναι αμέσως κυρίαρχοι των διαπιστευτηρίων τους χωρίς περαιτέρω αλληλεπιδράσεις με το πανεπιστήμιο ή το ίδρυμα που παρέδωσε το δίπλωμα ή το πιστοποιητικό.

2.3 Η αξία εφαρμογής τεχνλογιών blockchain σε πιστοποιητικά σπουδών

Έχει ήδη αναφερθεί σε προηγούμενη ενότητα, το κύριο πρόβλημα των ψηφιακών πιστοποιητικών,το οποίο είναι ότι είναι εύκολο να παραποιηθούν.Ένας από τους πιο απλούς τρόπους είναι να πάρουμε το πιστοποιητικό κάποιου άλλου και να αλλάξουμε το όνομα του

κατόχου του χρησιμοποιώντας λογισμικό Adobe.Το κακό είναι ότι είναι τόσο δύσκολο να επαληθευτεί η αυθεντικότητα ενός πιστοποιητικού που συνήθως κανείς δεν ξοδεύει χρόνο να το κάνει,προτιμώντας απλώς να αποδεχθεί την αυθεντικότητά του ως γεγονός.Για παράδειγμα,εάν ένας υπεύθυνος πρόσληψης προσωπικού μιας εταιρίας λάβει μια αίτηση εργασίας που περιέχει ένα πιστοποιητικό π.χ. από το Changellenge,ο μόνος τρόπος για να επαληθεύσει την αυθεντικότητά του είναι να καλέσει το Changellenge και να το ελέγξει.Αυτό είναι πολύ δύσκολο και χρονοβόρο,ειδικά εφόσον αυτός ο υποψήφιος είναι πιθανότατα ένα από τους πολλούς στη λίστα των προσλήψεων.Ο υπεύθυνος πρόσληψης προσωπικού πιθανότατα θα υποθέσει ότι το πιστοποιητικό είναι αυθεντικό από προεπιλογή. Έτσι τα πιστοποιητικά έχουν χάσει μεγάλο μέρος της αξίας τους στη πάροδο του χρόνου,καθώς προσφέρουν ελάχιστες αποδείξεις ότι ο κάτοχος έχει εργαστεί με ειλικρίνεια για τη βελτίωση του χαρτοφυλακίου του. Πολλές εκπαιδευτικές εταιρίες προσπαθούν να λύσουν το πρόβλημα της πλαστογραφίας των πιστοποιητικών τους.Μία λύση που εφαρμόστηκε πριν λίγο καιρό,κυρίως από την εκπαιδευτική πλατφόρμα Udemy,αφορά μια σελίδα επαλήθευσης πιστοποιητικών,όπως αυτή απεικονίζεται παρακάτω:

Εικόνα 1:Πιστοποίηση Udemy

Όπως είναι φανερό στη κάτω αριστερή γωνία του πιστοποιητικού υπάρχει ένα μοναδικό αναγνωριστικό και ένας σύνδεσμος προς τον επαληθευτή του.Κάθε χρήστης του διαδικτύου μπορεί να επαληθεύσει αμέσως την αυθεντικότητα του κάνοντας κλικ στο σύνδεσμο,στη περίπτωση της εικόνας:**http://ude.my/UC-h0XTD899**.Αυτή η λύση που προτάθηκε είναι εξαιρετικά βολική και λύνει το πρόβλημα ενός εργοδότη που θα ήθελε να επαληθεύσει την αυθεντικότητα ενός πιστοποιητικού που παρέχεται από έναν υποψήφιο για μια θέση. Ωστόσο προκύπτει ένα άλλο θέμα στην παραπάνω προσέγγιση,κατά πόσο ο κάτοχος του πιστοποιητικού

και ο χρήστης του Udemy θα μπορούσαν εύκολα να υποβάλλουν την ερώτηση αυτή σε κάποια μεταγενέστερη περίοδο,ποιος εγγυάται ότι ο σύνδεσμος θα εξακολουθήσει να λειτουργεί σε 20 χρόνια?Εάν το Udemy σταματήσει να λειτουργεί ποιος θα μπορεί να επαληθεύσει το πιστοποιητικό?Στο συγκεκριμένο παράδειγμα δυστυχώς η απάντηση είναι κανείς.Για να διασφαλιστεί ότι τα δεδομένα πιστοποιητικών θα αποθηκεύονται για πάντα ,πρέπει να χρησιμοποιηθεί το blockchain.Σε υπάρχουσες λύσεις,όταν η πλατφόρμα εκδίδει ένα πιστοποιητικό για ένα χρήστη το αποθηκεύει σε ένα διακομιστή.Αυτή είναι μια κεντρική λύση που έχει γνωστά μειονεκτήματα. Εάν συμβεί κάτι στο διακομιστή όπως για παράδειγμα ο κάτοχος χρεοκοπήσει και σταματήσει να πληρώνει για φιλοξενία τότε τα δεδομένα σε αυτόν θα χαθούν.

2.4 Θετικά και αρνητικά από τη χρήση της τεχνολογίας blockchain στην επαλήθευση και έγκριση πιστοποιητικών

Τα οφέλη του Blockchain μπορούν να αξιοποιηθούν μόνο μέσω των «ανοιχτών εφαρμογών» της τεχνολογίας. Το Blockchain χρησιμοποιεί λογισμικό ανοικτού κώδικα.Το λογισμικό ανοιχτού κώδικα,πρόκειται για ένα τύπο λογισμικού υπολογιστή του οποίου ο πηγαίος κώδικας κυκλοφορεί με άδεια, στο οποίο ο κάτοχος πνευματικών δικαιωμάτων παραχωρεί στους χρήστες τα δικαιώματα μελέτης, αλλαγής και διανομής του λογισμικού σε οποιονδήποτε και για οποιονδήποτε σκοπό.Σύμφωνα με αρχείο pdf της EU Reportopens του blockchain στην εκπαίδευση,η περαιτέρω ανάπτυξη της τεχνολογίας στον εκπαιδευτικό τομέα θα πρέπει να θεωρηθεί ως κοινή αρμοδιότητα της αγοράς και των δημόσιων αρχών, προκειμένου να διασφαλιστεί η κατάλληλη ισορροπία της καινοτομίας του ιδιωτικού τομέα σε συνδυασμό με τη διασφάλισή της το δημόσιο συμφέρον. Επιπλέον, οι κύριο δικαιούχοι της υιοθέτησης τεχνολογιών βασισμένων σε blockchain στην εκπαίδευση είναι πιθανό να είναι δίκτυα εκπαιδευτικών οργανισμών και φοιτητών είτε οργανισμοί διαχείρισης που διαχειρίζονται πολλές σχολές μέσα σε ένα δίκτυο, που είναι ήδη ανοιχτοί στο να δοκιμάσουν νέους τρόπους εκπαίδευσης και ενημέρωσης των μαθητών τους, μπορεί να αποτελέσουν την τέλεια ομάδα που θα προσπαθήσει να εφαρμόσει αυτήν την τεχνολογία στο εγγύς μέλλον. Παρόλο που η τεχνολογία blockchain έχει μεγάλες δυνατότητες επίλυσης προβλημάτων στον τομέα της εκπαίδευσης λόγω του απίστευτου γνωρίσματος της, η έρευνα είναι ακόμα σε πρώιμο στάδιο. Για αυτό το λόγο φέρνει κινδύνους και προκλήσεις κατά την εφαρμογή της. Κάποιοι από αυτούς τους κινδύνους παρουσιάζονται παρακάτω:

- **Αμετάβλητο χαρακτηριστικό**: Στο blockchain με το που τοποθετηθούν δεδομένα σε αυτό,δεν μπορούν να αλλάξουν ή να τροποποιηθούν. Αυτό το αμετάβλητο χαρακτηριστικό μπορεί να επηρεάσει τη χρήσιμη λειτουργία του καθώς δεν επιτρέπει οποιαδήποτε αλλαγή ή τροποποίηση που συχνά απαιτείται. Η σωστή εφαρμογή της τεχνολογίας blockchain βελτιώνει σημαντικά αυτά τα κριτήρια, επιτρέποντας λιγότερες ανεπιθύμητες παρενέργειες.

Ποιος δίνει την έγκριση του πρώτου κόμβου στο δίκτυο? Στην αρχή, κάποιο ίδρυμα πρέπει να είναι ο πρώτος κόμβος δικτύου και εκείνη την στιγμή δεν θα υπάρχει κόμβος για την επαλήθευσή του, ένα τέτοιο χαρακτηριστικό μπορεί να θεωρηθεί ως κίνδυνος ασφαλείας. Ωστόσο, αναμένετε ότι με την αύξηση του αριθμού των κόμβων, τέτοια προβλήματα ασφαλείας θα ελαχιστοποιηθούν.

- **Έλλειψη προστασίας προσωπικού απορρήτου**: Δεδομένου ότι είναι open source και διαφανής τεχνολογία, η εγγραφή ή οι προσωπικές πληροφορίες σχετικά με τους φοιτητές μπορούν να κοινοποιηθούν χωρίς την προθυμία των φοιτητών ή κάποιος να έχει άμεση πρόσβαση σε αυτές
- **Πρόβλημα επεκτασιμότητας**: Το Blockchain πρέπει να κλιμακωθεί για τη βελτίωση των συναλλαγών του δικτύου που εκτελούνται ανά δευτερόλεπτο, επομένως, ζητήματα όπως οι «πλευρικές αλυσίδες» διερευνώνται.

Παρά τα αρνητικά τα οποία παρουσιάζει η τεχνολογία έχει σημαντικά οφέλη τα οποία μπορούν να τη κάνουν αναπόσπαστο κομμάτι στη διαδικασία επαλήθευσης πιστοποιητικών.Τα σημαντικότερα εξ'αυτών παρατίθενται παρακάτω.

- **Αυξημένη διαφάνεια**: Η τεχνολογία αμετάβλητου καθολικού του Blockchain δημιουργεί μια χρονική λίστα συμβάντων που έχουν συμβεί σε πραγματικό χρόνο. Αυτό είναι χρήσιμο για την επαλήθευση απομαγνητοφωνημένων κειμένων, δείχνοντας μια κάρτα πλήρης αναφοράς,διατηρώντας τους φοιτητές ειλικρινείς όσον αφορά τη πρόοδό τους.Ο φοιτητής να υποβάλοντας την εργασία του μέσω του blockchain διασφαλίζει ότι δεν μπορεί να τη «χάσει» αλλά ούτε μπορεί να ισχυριστεί ότι ο δάσκαλος την έχασε.
- **Ανιχνεύσιμο με μνήμη:** Το Blockchain χρησιμοποιεί timestamps για τον εντοπισμό και την καταγραφή κάθε συναλλαγής, ενισχύοντας έτσι την χρονική σειρά των δεδομένων. Αυτό επιτρέπει στον κόμβο να διατηρεί τη σειρά των συναλλαγών και να κάνει τα δεδομένα ανιχνεύσιμα. Η χρονική σήμανση όχι μόνο εγγυάται την πρωτοτυπία των

δεδομένων, αλλά μειώνει επίσης το κόστος της ανιχνευσιμότητας των συναλλαγών. Παράλληλα, ενισχύει μη αναστρέψιμες τροποποιήσεις δεδομένων ή πληροφοριών. Μόλις μια συναλλαγή επικυρωθεί και προστεθεί στο block, δεν μπορεί να τροποποιηθεί. Οι συναλλαγές πρέπει να επανεξεταστούν από τους περισσότερους κόμβους του συστήματος πριν καταγραφούν. Ακόμα κι αν ένας εισβολέας έχει ισχυρή υπολογιστική ικανότητα, είναι δύσκολο για τον εν λόγω εισβολέα να αποφύγει το σύστημα και να τροποποιήσει το αρχείο. Αυτό μπορεί να συμβεί μόνο όταν ο εισβολέας ελέγχει 51% ή περισσότερους από όλους τους κόμβους. Αυτό το χαρακτηριστικό διασφαλίζει ότι το σύστημα είναι σταθερό και αξιόπιστο και λύνει τα προβλήματα «διπλής δαπάνης»

- **Αξιοπιστία:** Η ανταλλαγή δεδομένων στο Blockchain εξαρτάται πλήρως από τον αυτοέλεγχο. Στηρίζεται σε κάθε κόμβο για να σχηματίσει έναν ισχυρό υπολογισμό για να υπερασπιστεί τις εξωτερικές επιθέσεις χωρίς ανθρώπινη παρέμβαση. Οι συμμετέχοντες μπορούν να ολοκληρώσουν τη συναλλαγή υπό συνθήκες πλήρους ανωνυμίας. Προστατεύει την ιδιωτική ζωή όλων των εμπλεκόμενων μελών και αυξάνει την ασφάλεια και την αξιοπιστία της συναλλαγής. Επιπλέον, κάθε κόμβος στο Blockchain αποθηκεύει τα πλήρη δεδομένα. Όταν το 51% όλων των κόμβων του δικτύου δεν καταλαμβάνεται από χάκερς, το σύστημα είναι ακόμα ασφαλές και αξιόπιστο.
- **Ανωνυμία:** Το Blockchain κρυπτογραφεί τα δεδομένα χρησιμοποιώντας ασύμμετρες τεχνικές κρυπτογράφησης. Αυτή η ασύμμετρη κρυπτογράφηση έχει δύο χρήσεις σε Blockchains τη κρυπτογράφηση δεδομένων και τις ψηφιακές υπογραφές. Η κρυπτογράφηση δεδομένων στο Blockchain εξασφαλίζει την ασφάλεια των δεδομένων των συναλλαγών και μειώνει τον κίνδυνο απώλειας ή παραποίησης δεδομένων μιας συναλλαγής. Τα δεδομένα συναλλαγών μεταδίδονται μέσω του δικτύου και υπογράφονται ψηφιακά για να δηλώνεται η ταυτότητα του υπογράφοντος και αν έχει προσδιοριστεί η συναλλαγή.

  Στο σύστημα Blockchain, είναι περιττό να αποκαλυφθεί η πραγματική ταυτότητα του κόμβου που σχετίζεται με τον συμμετέχοντα. Το χαρακτηριστικό αυτό είναι αμφιλεγόμενο διότι βοηθά έμμεσα ορισμένες παράνομες δραστηριότητες, όπως η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, αλλά τουλάχιστον προστατεύει την ιδιωτική ζωή και την ασφάλεια των συμμετεχόντων.

2.5 Σύνοψη

Στο παρόν κεφάλαιο παρουσιάστηκε αναλυτικά το τι είναι ένα πιστοποιητικό σπουδών αλλά και το ρόλο του στη δια βιου μάθηση.Μέσω της αναφοράς στο Πανεπιστήμιο της Ρώμης «Tor Vergata»περιγράφηκετο πώς υλοποιείται μέχρι στιγμής η εν λόγω διαδικασία.

Εν συνεχεία, έγινε εκτενής αναφορά στη σημασία της εφαρμογής της τεχνολογίας blockchain στην επαλήθευση πιστιοποιητικών. Ξεχωριστά έγινε αναφορά στα θετικά και αρνητικά γνωρίσματα της τεχνολογίας ώστε να προσδιοριστούν οι καινοτομίες που προσφέρει.

Τέλος,όλα τα παραπάνω στοιχεία, μας οδηγούν στο συμπέρασμα της αξίας της εφαρμογής της τεχνολογίας στην επαλήθευση πιστοποιητικών,παρόλο τα κάποια αρνητικά που παρουσιάζει και στη παρουσίαση κάποιων μέχρι στιγμής πιλοτικών λύσεων που έχουν αξιοποιηθεί σε αυτό το τομέα με τη χρήση της.

\

Κεφάλαιο 3: Περιγραφή της τεχνολογίας blockchain

3.1 Εισαγωγή

Αρχικός σκοπός του συστήματος Blockchain ήταν η υποστήριξη του ηλεκτρονικού συστήματος συναλλαγών που βασίζεται πάνω σε κρυπτογραφικά τεκμήρια αντί για πειστήρια εμπιστοσύνης. Ενώ το εύρος χρήσης της τεχνολογίας αυτής αυξήθηκε, οι πρωταρχικοί στόχοι παραμένουν σταθεροί. Ο πρώτος από αυτούς είναι η διαβεβαίωση της ανωνυμίας των χρηστών. Αυτό επιτεύχθηκε με την χρήση δημόσιου/ιδιωτικού ζεύγους κλειδιών, με έναν νέο τρόπο που δεν μπορούν να ξανά δημιουργηθούν, μέσω της τεχνολογίας του Blockchain. Κάθε συμμετέχον ταυτοποιείται από το δημόσιο κλειδί και η επιβεβαίωση επιτυγχάνεται με την εισαγωγή του ιδιωτικού του κλειδιού. Ο δεύτερος πρωταρχικός στόχος είναι η παροχή μια δημόσιας καταγραφής του συνόλου των συναλλαγών οι οποίες δεν μπορούν να τροποποιηθούν μετά την επιβεβαίωση και συμφωνία τους. Η χρήση αυτής της καταγραφής αρχικά σχεδιάστηκε για να αποτρέπει τους χρήστες ηλεκτρονικών συναλλαγών από τις λανθασμένες διπλό συναλλαγές και να επιτρέπει δημόσιο έλεγχο όλων αυτών των συναλλαγών. Τρίτος και τελευταίος στόχος είναι η ανεξαρτησία από οποιαδήποτε κεντρική ή έμπιστη εξουσία. Αυτό οδηγεί στη δημιουργία ενός συστήματος στο οποίο καμία οντότητα δεν έχει περισσότερη ή λιγότερη εξουσία, ή αξιοπιστία από κάποια άλλη .

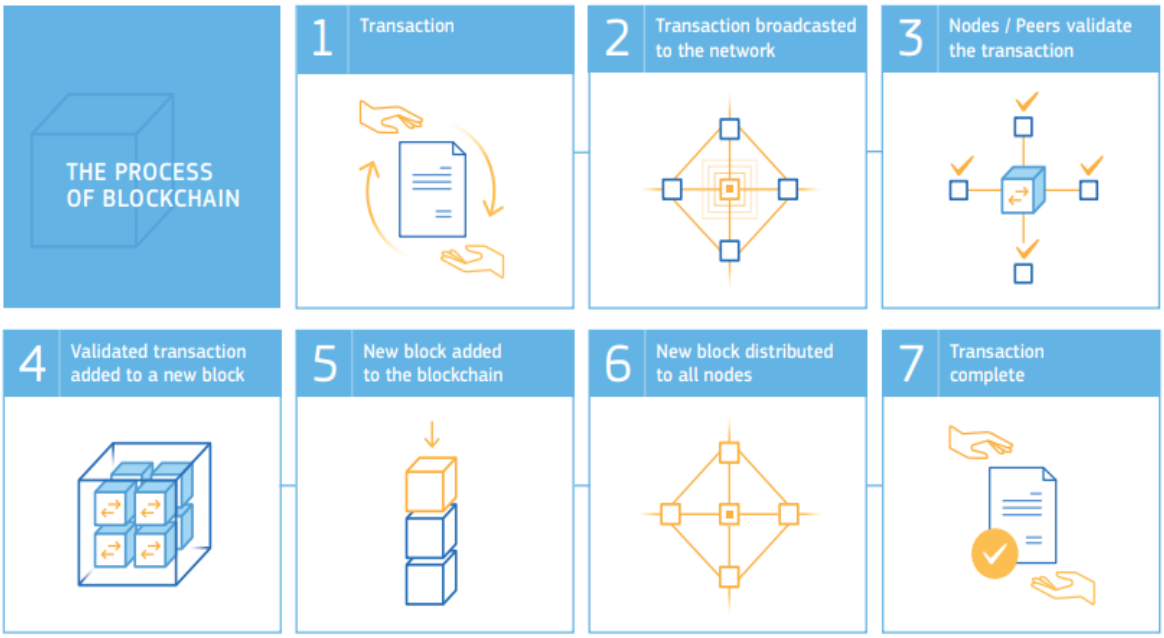
Πριν από την εφεύρεση των Blockchain (τεχνολογία κατανεμημένης εγγραφής), δεν υπήρχε κανένας τρόπος για τη διαχείριση μεμονωμένων δραστηριοτήτων μέσω του Διαδικτύου χωρίς κεντρικό έλεγχο για να εξασφαλιστεί η μη αποποίηση ευθυνών για τα δεδομένα. Δεν υπήρχε καμία εμπιστοσύνη μεταξύ των μερών ότι καθένας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

βάση δεδομένων με ψεύτικα δεδομένα, μειώνεται σημαντικά. Η μόνη περίπτωση επίθεσης είναι όταν ο επιτιθέμενος μπορεί να χρησιμοποιήσει πολύ περισσότερη υπολογιστική ισχύ από ότι ολόκληρο το δίκτυο. Τα πρωτόκολλα του Blockchain μπορούν να διασφαλίσουν ότι οι συναλλαγές είναι σωστές και όχι διπλές (Sousa, Bessani & Vukolic, 2018)

3.2 Τεχνολογία blockchain

Πρόκειται για ένα δημόσιο ψηφιακό λογιστικό βιβλίο που έχει σχεδιαστεί ώστε να είναι αδιαπέραστο από τους hacker.Παρόλο που χρησιμοποιείται κυρίως ως μέσο παρακολούθησης και επαλήθευσης των νομισματικών συναλλαγών,μπορεί επίσης να εντοπίζει και να ελέγχει σχεδόν οποιοδήποτε είδος δεδομένων,καθιστώντας το μια απίστευτα ασφαλή πλατφόρμα που έχει τη δυνατότητα να αλλάξει ολόκληρο το διαδίκτυο. Κάθε χρονολογική αλλαγή στο βιβλίο αναφέρεται ως block(μπλοκ), ενώ μια μεγαλύτερη σειρά αλλαγών ονομάζεται αλυσίδα Blockchain.Αυτό που κάνει το blockchain τόσο ασφαλές είναι ο **decentralized** (αποκεντρωμένος, χωρίς έδρα) χαρακτήρας του. Δεν υπάρχει σε κανένα διακομιστή, **Master Ledger (κυρίαρχο λογιστικό βιβλίο)**, αντίθετα, υπάρχει στον υπολογιστή του καθενός ταυτόχρονα.Αυτό σημαίνει ότι κάθε φορά που ενημερώνεται με νέες πληροφορίες, κάθε υπολογιστής που χρησιμοποιεί την πλατφόρμα, πρέπει να συμφωνεί ότι η αλλαγή είναι έγκυρη. Αυτό σημαίνει ότι αν κάποιος θελήσει να παραποιήσει τα αρχεία στο blockchain, θα χρειαζόταν να «μπει» **(hack)** σε κάθε έναν από αυτούς τους υπολογιστές ταυτόχρονα, σε αντίθεση με μια ενιαία κεντρική (centralized) βάση δεδομένων.Ο καθένας έχει πρόσβαση στο βιβλίο ανά πάσα στιγμή, αλλά χωρίς χαρακτηριστικά αναγνώρισης. Το blockchain μπορεί να ελέγξει με ασφάλεια τις συναλλαγές μεταξύ δύο μερών ενώ μειώνει αποτελεσματικά την ανάγκη για μεσάζοντα.Για παράδειγμα, ας πούμε ότι κάποιος θέλει να μεταφέρει χρήματα. Παραδοσιακά, αυτή η μεταφορά θα είχε πραγματοποιηθεί μέσω της τράπεζας. Η τράπεζά μιλάει στην τράπεζά του παραλήπτη και τα χρήματα μετακινούνται.Το Blockchain θα επαληθεύσει την ίδια συναλλαγή απλά και μόνο με βάση τον τρόπο λειτουργίας του. Επειδή πρέπει να «εγκριθεί» η συνναλαγή από όλους τους συμμετέχοντες σε αυτό το συγκεκριμένο blockchain, δεν χρειάζεται να επέμβει καμιά τράπεζα (εκτός και αν θέλουμε να μετατρέψουμε το Bitcoin σε άλλο νόμισμα).Επειδή η έννοια μπορεί να εφαρμοστεί σε οποιοδήποτε είδος μεταφοράς δεδομένων, ο Tim Berners-Lee, ο άνθρωπος που δημιούργησε το πραγματικό διαδίκτυο, συμφωνεί ότι το blockchain έχει τη δυνατότητα να διαταράξει ολόκληρο τον online κόσμο, λειτουργώντας ως βάση για ένα πραγματικά πιο ιδιωτικό και αποκεντρωμένο Διαδίκτυο. Το blockchain είναι ένα μητρώο συναλλαγών χωρίς κάποιον απόλυτα υπεύθυνο να

το ελέγχει, ούτως ώστε όλες οι συναλλαγές-πληροφορίες να είναι διαθέσιμες σε όλους τους χρήστες πάνω στο ίδιο δίκτυο.Στην περίπτωση των τραπεζικών συναλλαγών για παράδειγμα, οι συμβαλλόμενοι μπορούν να επιβεβαιώσουν μια συναλλαγή μεταξύ τους και να θεωρηθεί έγκυρη χωρίς οποιαδήποτε έγκριση από ένα κεντρικό χρήστη ή κάποιον με μεγαλύτερη εξουσία στο δίκτυο (πχ. Τράπεζα).Με την τεχνολογία αυτή αντιλαμβανόμαστε ότι η κοινή εξουσιοδότηση σε αρχεία στο Internet (file sharing) παίρνει άλλη διάσταση.Η τεχνολογία blockchain προκύπτει από ένα δίκτυο ανθρώπων που δημιουργούν και μοιράζονται κάτι κοινό.Το κύριο χαρακτηριστικό του δικτύου αυτού που χρησιμοποιείται από την τεχνολογία blockchain,ανήκει στη γλώσσα των υπολογιστών στην κατηγορία δικτύων υπό τον τίτλο **“δίκτυο ομότιμων κόμβων”.**Το δίκτυο αυτό είναι αποκεντρωμένο και διανεμημένο ισόποσα,αυτό σημαίνει ότι δεν υπάρχει κάποιο πρόσωπο του δικτύου που να υπερέχει έναντι κάποιου άλλου προσώπου κατ’ οποιονδήποτε τρόπο,οπότε υπάρχει απουσία προτεραιότητας (όποιου είδους),κάποιου προσώπου έναντι κάποιου άλλου.Τα πρόσωπα των συμμετεχόντων στο δίκτυο δεν είναι ίδια,αλλά είναι ίσα μεταξύ τους αναφορικά με οποιαδήποτε διαδικασία εκλογής ή/και επιλογής μεταξύ αυτών.Στατιστικά μιλώντας, εάν τεθεί θέμα εκλογής κάποιου προσώπου, η εκλογή αυτή θα δίνει ίσα ποσοστά επιτυχίας σε κάθε ένα από αυτά τα πρόσωπα και αυτή θα εκτελείται τυχαία.Όλα τα πρόσωπα του δικτύου blockchain, δημιουργούν και μοιράζονται από κοινού ένα αρχείο.Η διαδικασία δημιουργίας και διαφύλαξης του αρχείου αυτού καθορίζεται και ελέγχεται από ένα Σύνταγμα κανόνων, που ονομάζεται πρωτόκολλο συναίνεσης(consensus).Οι κανόνες αυτοί συντάσσονται με βασικό γνώμονα την κατ’ εξαίρεση ανάγκη ύπαρξης εμπιστοσύνης ανάμεσα στα πρόσωπα αυτά.Η σύνταξη ενός συμπαγούς πρωτοκόλλου συναίνεσης,απομακρύνει τη δημιουργία συνθηκών οι οποίες να οδηγούν στην ανάγκη να αποδείξουν τα πρόσωπα του δικτύου την τιμιότητά τους αναφορικά με την συμμετοχή τους στο δίκτυο, και έτσι ακολούθως, το δικαίωμα συνύπαρξης τους σε αυτό.



Εικόνα 2:Πώς λειτουργεί το Blockchain

3.2.1 Δίκτυα Ομότιμων Κόμβων

Στην ενότητα αυτή,γίνεται μία σύντομη περιγραφή της αρχιτεκτονικής ομότιμων κόμβων, που αποτελεί την αρχιτεκτονική πάνω στην οποία βασίζεται η τεχνολογία του blockchain. Την συγκεκριμένη χρονική περίοδο στο διαδίκτυο δύο είναι οι κύριες αρχιτεκτονικές που χρησιμοποιούνται για την ανάπτυξη και λειτουργία εφαρμογών. Αυτή του πελάτη εξυπηρετητή (client-server) με πληθώρα εφαρμογών σε αυτό το μοντέλο και αυτή των ομότιμων κόμβων (P2P) . Η διαφορά των δύο είναι κυρίως η ύπαρξη του server (εξυπηρετητή) όπου σε αυτή του client-server είναι απαραίτητη,ο οποίος δέχεται από τους χρήστες αιτήματα για να ολοκληρώσουν τις ενέργειες τους έναντι της αρχιτεκτονικής των ομότιμων κόμβων στην οποία δεν χρειάζεται.

Στο δίκτυο ομότιμων κόμβων οι υπολογιστές (peers) υπό τις εντολές των χρηστών αλληλεπιδρούν, επικοινωνούν σε ζεύγη χωρίς την μεσολάβηση κάποιου τρίτου για παροχή υπηρεσίας. Οι κόμβοι στο δίκτυο P2P είναι ταυτόχρονα και clients αλλά και server λόγω του ότι έχουν την δυνατότητα να διατηρούν την σωστή λειτουργία του δικτύου παρέχοντας πόρους αλλά και καταναλώνοντας, εξαλείφοντας με αυτόν τον τρόπο την αρχή που θα παρείχε υπηρεσίες και θα οργάνωνε το δίκτυο. Κατά την υλοποίηση μίας εφαρμογής είναι σύνηθες να χρησιμοποιούνται και οι δύο αυτές αρχιτεκτονικές σε μία με όνομα υβριδική αρχιτεκτονική. Τα δίκτυα ομότιμων χωρίζονται σε δύο μεγάλες κατηγορίες, στα αδόμητα και στα δομημένα. Τα αδόμητα P2P δίκτυα δημιουργούνται μέσω συνδέσεων των κόμβων χωρίς να είναι προκαθορισμένη η σύνδεση αυτών, χωρίς κάποια οργάνωση και αρχή και τέλος χωρίς τα

δεδομένα να έχουν κάποια σχέση με τους κόμβους από τους οποίους τα συλλέγουμε. Τα πλεονεκτήματα αυτών είναι η ευκολία για την δημιουργία τους μέσω της παραπάνω διαδικασίας, οι αλλαγές τοπικά για καλύτερα αποτελέσματα και η δυνατότητα που έχουν για εξέλιξη και δημιουργία σε διαφορετικές «κινήσεις» των κόμβων. Ένα σημαντικό μειονέκτημα είναι η σπατάλη πόρων στο δίκτυο όταν γίνεται αίτημα για αναζήτηση πληροφοριών και η επιθυμητή απάντηση στο αίτημα καθώς απαιτείται ο αρμόδιος κόμβος για συλλογή δεδομένων πράγμα που δεν είναι σίγουρο ότι θα πραγματοποιηθεί με επιτυχία.Τα δομημένα P2P δίκτυα διαμορφώνονται με τέτοιο τρόπο ώστε στην διαδικασία αιτήματος αναζήτησης δεδομένων ανεξάρτητα από ποιον κόμβο να εγγυάται το καλύτερο και επιθυμητό αποτέλεσμα. Μία μορφή-τύπος δομημένων δικτύων (P2P) επιλύει τον DHT κατανεμημένο πίνακα κατακερματισμού βάσει του οποίου μεταφέρονται στον κόμβο που πρέπει τα δεδομένα.

Ένας κατανεμημένος πίνακας κατακερματισμού είναι μια κατηγορία αποκεντρωμένου κατανεμημένου συστήματος που παρέχει μια υπηρεσία αναζήτησης παρόμοια με ένα πίνακα κατακερματισμού. Ο κατανεμημένος πίνακας κατακερματισμού DHT χρησιμοποιεί έναν τροποποιημένο αλγόριθμο της συνάρτησης κατακερματισμού για την παραπάνω διαδικασία όπου αποστέλλονται τα δεδομένα στον κάθε κόμβο από τον οποίο επίσης με τον DHT γίνεται και η αναζήτηση αυτών των δεδομένων γεγονός που κάνει τα δομημένα δίκτυα καλύτερα έναντι των αδόμητων .

Τα βασικότερα πλεονεκτήματα της αρχιτεκτονικής ομότιμων:

- Αυτο-κλιμακωσιμότητα (self-scalability) του δικτύου. Ταυτόχρονα με την αύξηση των κόμβων στο δίκτυο αυξάνεται και η ανάγκη σε πόρους τους οποίους πόρους όμως καλύπτουν οι ίδιο οι κόμβοι πράγμα το οποίο συμβαίνει λόγω της αρχιτεκτονικής του δικτύου αυτού.

- Μείωση κόστους για τον λόγο ότι δεν χρειάζεται να εγκατασταθεί κάποιος ιδιαίτερος τεχνολογικός εξοπλισμός ούτε υλοποίηση και διαμόρφωση κάποιου εξυπηρετητή.

- Μη ύπαρξη μοναδικού σημείου αστοχίας του δικτύου. Στην αρχιτεκτονική πελάτη εξυπηρετητή ένα λάθος που θα υπάρξει στον εξυπηρετητή έχει ως αποτέλεσμα την μη λειτουργία της εφαρμογής σε αντίθεση με μία βλάβη σε έναν κόμβο.

Μερικές από τις βασικές προκλήσεις που αντιμετωπίζουν οι εφαρμογές αρχιτεκτονικής ομότιμων:

- Ασφάλεια. Λόγω της κατανεμημένης και ανοικτής φύσης τους, οι εφαρμογές P2P μπορούν να δημιουργήσουν προβλήματα ασφαλείας.

• Η ανάκτηση δεδομένων ή η δημιουργία αντιγράφων ασφαλείας είναι δύσκολο να πραγματοποιηθεί για τον λόγο ότι κάθε υπολογιστής πρέπει να διαθέτει δικό του σύστημα δημιουργίας αντιγράφων ασφαλείας.

• Λόγω του ότι το σύστημα είναι αποκεντρωμένο δεν διαθέτει κάποιον κεντρικό διαχειριστή για αυτό και καθίσταται δύσκολη η ρύθμιση της κίνησης του δικτύου .

3.3 Βασικά χαρακτηριστικά του Blockchain

3.3.1 Αποκεντρωμένος Έλεγχος

Στο blockchain οι χρήστες χωρίς να γνωρίζουν τα άτομα που μοιράζονται πληροφορίες πραγματοποιούν συναλλαγές χωρίς κάποια κεντρική αρχή-διαχειριστή ο οποίος θα διαχειρίζεται τις πληροφορίες. Αντιθέτως όλοι οι κόμβοι-χρήστες λειτουργούν με βάση την εμπιστοσύνη μεταξύ τους με στόχο να έχουν την ίδια κατάσταση με όλους στο δίκτυο των ομότιμων κόμβων.

Το πλεονέκτημα αυτής της διαδικασίας είναι ότι δεν εξαρτώνται οι χρήστες από κάποιους που είναι υπεύθυνοι για την κεντρική βάση και με αυτόν τον τρόπο μειώνουν τις πιθανότητες να γίνει εσκεμμένα κάποια καταστροφή ή υποκλοπή στα δεδομένα. Οι χρήστες είναι υπεύθυνοι να τηρούν οι ίδιοι τις αλλαγές ενεργώντας με τρόπο τέτοιο που να διασφαλίζεται η ακεραιότητα της αλυσίδας. Οι περισσότερες κεντρικές βάσεις δεδομένων διατηρούν πληροφορίες που είναι ενημερωμένες σε μια συγκεκριμένη στιγμή.

Οι βάσεις δεδομένων Blockchain είναι σε θέση να διατηρούν πληροφορίες που είναι σχετικές με το τώρα, αλλά και όλες τις πληροφορίες που έχουν προηγηθεί. Δημιουργούν ένα ιστορικό από συναλλαγές με πληροφορίες όπου είχαν πραγματοποιηθεί και συνεχίζουν με τις νέες εγγραφές και καταχωρήσεις .

3.3.2 Χρόνος εκτέλεσης των διαδικασιών στο blockchain

Ενώ τα blockchain μπορούν να χρησιμοποιηθούν ως συστήματα εγγραφής και είναι ιδανικά ως πλατφόρμες συναλλαγών, θεωρούνται αργές ως βάσεις δεδομένων σε σύγκριση με το τι είναι

δυνατό για την τεχνολογία ψηφιακών συναλλαγών που βλέπουμε σήμερα με τις κάρτες Visa και PayPal. Αν και σίγουρα θα υπάρξουν βελτιώσεις σε αυτές τις επιδόσεις, η φύση της τεχνολογίας blockchain απαιτεί να θυσιάζεται κάποια ταχύτητα. Ο τρόπος με τον οποίο τα κατανεμημένα δίκτυα χρησιμοποιούνται σε τεχνολογία blockchain σημαίνει ότι δεν μοιράζονται και επεξεργάζονται ισχυρή δύναμη επεξεργασίας, εξυπηρετούν από κοινού το δίκτυο και στη συνέχεια συγκρίνουν τα αποτελέσματα της δουλειάς τους με το υπόλοιπο δίκτυο έως ότου υπάρξει συναίνεση ότι κάτι συνέβη. Αντίθετα οι κεντρικές βάσεις δεδομένων αυξάνουν την ταχύτητα τους συνέχεια δίνοντας στην ψηφιακή εποχή νέες τεχνολογικές καινοτομίες.

3.3.3 Εμπιστευτικότητα

Ένα από τα κύρια χαρακτηριστικά μίας βάσης δεδομένων blockchain είναι η εμπιστευτικότητα. Το χαρακτηριστικό αυτό προσδίδει τις εξής ιδιότητες:

- Στην βάση δεδομένων blockchain ο καθένας μπορεί να καταχωρήσει ένα νέο μπλοκ και να επεξεργαστεί χωρίς να πάρει άδεια από κάποιον διαχειριστή.

- Στο blockchain μπορεί το δίκτυο να διαμορφωθεί έτσι ώστε μόνο αυτοί που έχουν την άδεια να μπορούν να διαχειριστούν την βάση δεδομένων όπως γίνεται στην περίπτωση της κεντρικής βάσης δεδομένων.

- Για να γίνει απόκρυψη των πληροφοριών στο blockchain οι κόμβοι χρήστες απαιτείται να χρησιμοποιήσουν ισχυρή κρυπτογράφηση και κατ'επέκταση επιβαρύνονται με ένα υπολογιστικό βάρος.

3.3.4 Χαρακτηριστικά των blockchain

Τα σημεία που αναφέρονται και εξηγούνται παρακάτω θεωρούνται γενικά ως τα πιο σημαντικά χαρακτηριστικά της τεχνολογίας blockchain και σχετίζονται επίσης με την προτεινόμενη χρήση της τεχνολογίας.

▪ Αποκεντρωμένη και Κατανεμημένη Αρχιτεκτονική: Η χρήση της τεχνολογίας blockchain διασφαλίζει ότι οι συμμετέχοντες σε ένα σύστημα είναι συνδεδεμένοι μεταξύ τους,καθιστώντας έτσι τις συναλλαγές που πραγματοποιούνται μεταξύ τους διαφανείς χωρίς την ανάγκη εξωτερικού μέρους.Οι πληροφορίες που είναι αποθηκευμένες στο blockchain δεν

ελέγχονται από κανέναν και μπορούν να ελεγχθούν από μέρη που έχουν πρόσβαση στο σύστημα διασφαλίζοντας έτσι την κατάλληλη απόλυση (Atzori, 2017).

▪ Εμπιστευτική τεχνολογία blockchain:εξασφαλίζει ένα αξιόπιστο περιβάλλον χωρίς να απαιτείται η παρουσία τρίτων,σε αντίθεση με το παραδοσιακό σύστημα όπου οι συμμετέχοντες που δεν εμπιστεύονται ο ένας τον άλλο πρέπει να φέρουν τρίτο μέρος.Σύμφωνα με το Pernici και το Weske, (2016),η τεχνολογία blockchain θα πρέπει να χρησιμοποιείται σε περιπτώσεις συνεργασίας όπου πολλές επιχειρήσεις συγκεντρώνονται για να επιτύχουν ένα κοινό επιχειρηματικό σχέδιο.Εδώ, η τεχνολογία χρησιμοποιείται για να επιτρέψει την απίστευτη συνεργασία χωρίς την ανάγκη ελέγχου από μια οντότητα ή οποιοδήποτε εξωτερικό μέρος. Η χρήση της τεχνολογίας παρέχει ένα μηχανισμό για να διασφαλιστεί ότι έχει πραγματοποιηθεί μια συναλλαγή επειδή κάθε μπλοκ περιέχει πληροφορίες σχετικά με το μπλοκ που προηγείται.Έτσι,οι πληροφορίες σε κάθε μπλοκ πιστοποιούνται αυτόματα και μπορούν εύκολα να επαληθευτούν.

▪ Μη αναστρέψιμο:Μόλις καταγραφούν και επαληθευτούν οι συναλλαγές που πραγματοποιούνται στο blockchain,καθίσταται αδύνατο να τροποποιηθούν ή να αλλοιωθούν εύκολα αυτές οι εγγραφές επειδή κάθε μέρος έχει ένα αντίγραφο των διαθέσιμων πληροφοριών.Η τεχνολογία παρέχει επίσης μια αμετάβλητη διαδρομή ελέγχου όπου μπορείς να δεις ποιος πραγματοποίησε μια ενέργεια,διασφαλίζοντας έτσι την ακεραιότητα των δεδομένων,αυξάνοντας την διαφάνεια και μειώνοντας τον κίνδυνο που σχετίζεται με το σύστημα τρίτων (Pernici & Weske, 2016).

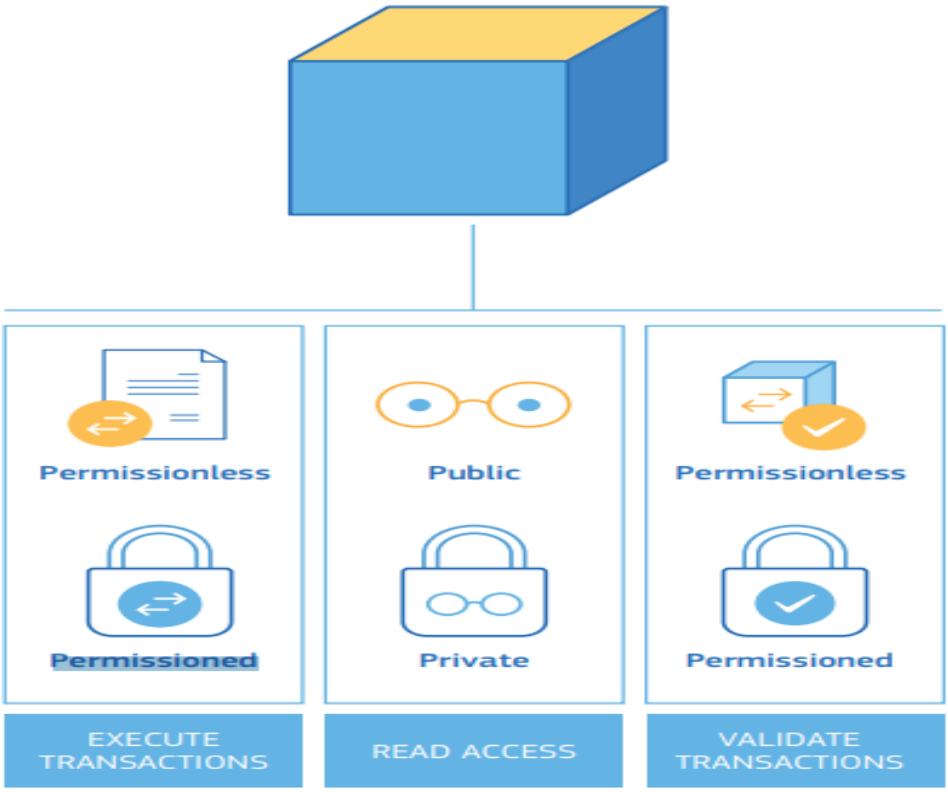
▪ Διαφάνεια:Σε ένα δίκτυο blockchain που είναι εντελώς χωρίς άδεια, αφού όλα τα μηνύματα ή οι συναλλαγές έχουν πιστοποιηθεί και επικυρωθεί,γίνονται ορατά σε όλους τους άλλους συμμετέχοντες στο δίκτυο.Αυτό διασφαλίζει ότι υπάρχει διαφάνεια καθώς όλα τα αρχεία μπορούν να εντοπιστούν στον αποστολέα ή στον εκδότη του.Ωστόσο, σε ένα blockchain με άδεια,το περιεχόμενο του μηνύματος είναι κρυπτογραφημένο και είναι ορατό μόνο σε εξουσιοδοτημένα μέρη που συμμετέχουν στο δίκτυο.Επομένως,είναι καλό να σημειωθεί ότι το επίπεδο διαφάνειας στο blockchain εξαρτάται από την ακριβή χρήση για την οποία το συγκεκριμένο blockchain έχει φτιαχτεί. (Fullbright, 2016).

▪ Χρονικά σημασμένο και προγραμματισμένο:Όλες οι συναλλαγές στο δίκτυο blockchain έχουν χρονική σήμανση και αυτό επιτρέπει σε όλα τα μέρη να γνωρίζουν πότε ακριβώς έγινε μια συναλλαγή.Αυτό είναι πολύ χρήσιμο σε περιπτώσεις όπου υπάρχει ανάγκη απόδειξης μιας συγκεκριμένης συναλλαγής για λόγους συμμόρφωσης ή για κανονιστικούς λόγους.Επίσης,οι

οδηγίες μπορούν να ενσωματωθούν σε κωδικούς γραμμένους σε ένα μπλοκ στο blockchain.Αυτές οι οδηγίες ονομάζονται έξυπνες συμβάσεις(smart contracts) και χρησιμοποιούνται για την εκτέλεση πολλών ενεργειών και μπορούν να εκτελεστούν μόνο όταν πληρούνται ορισμένες προϋποθέσεις.Από τα χαρακτηριστικά που αναφέρονται παραπάνω, είναι προφανές ότι η τεχνολογία blockchain δημιουργεί ένα απαραβίαστο περιβάλλον διασφαλίζοντας έτσι συστήματα ασφαλή και ασφαλισμένα.Αυτό συμβαίνει επειδή η τεχνολογία αυτή επιτρέπει το σύστημα να ελέγχεται και ενημερώνεται αυτόματα κάθε λίγα λεπτά,παρέχοντας έτσι ένα αυτοαναθεωρημένο και ισχυρό σύστημα.

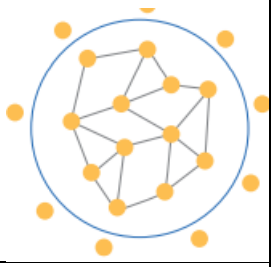
3.4 Τοπολογίες blockchain

Υπάρχουν πολλές διαφορετικές αλυσίδες blockchain με διακριτές λειτουργίες και αρχιτεκτονικές.Όταν ο καθένας μπορεί να διαβάσει και να αποκτήσει πρόσβαση σε ένα blockchain τότε αυτό κατηγοριοποιείται ως «δημόσιο» ή «ανοικτό» το οποίο σημαίνει ότι ο οποιοσδήποτε μπορεί να έχει πρόσβαση σε ένα ολόκληρο blockchain και να διαβάσει το περιεχόμενο του. Όταν επιτρέπεται μόνο σε εξουσιοδοτημένες οντότητες να έχουν πρόσβαση, τότε το blockchain θεωρείται «κλειστό» ή «ιδιωτικό».Τα Blockchain μπορούν να κατηγοριοποιηθούν περαιτέρω ως «χωρίς άδεια» (permissionless) ή «με άδεια» (permissioned) ανάλογα με το ποιος μπορεί να στείλει συναλλαγές και ποιος μπορεί να τις επικυρώσει.Αν κάποιος μπορεί να στείλει και να επικυρώσει συναλλαγές,το blockchain καλείται «χωρίς άδεια»(permissionless).Εάν πάλι οι οντότητες χρειάζεται να είναι εξουσιοδοτημένες για να εκτελέσουν ή να επικυρώσουν συναλλαγές, ή και για τα δύο, τότε το blockchain καλείται «με άδεια»(permissioned).



Εικόνα 3:Χαρακτηριστικά των Blockchain

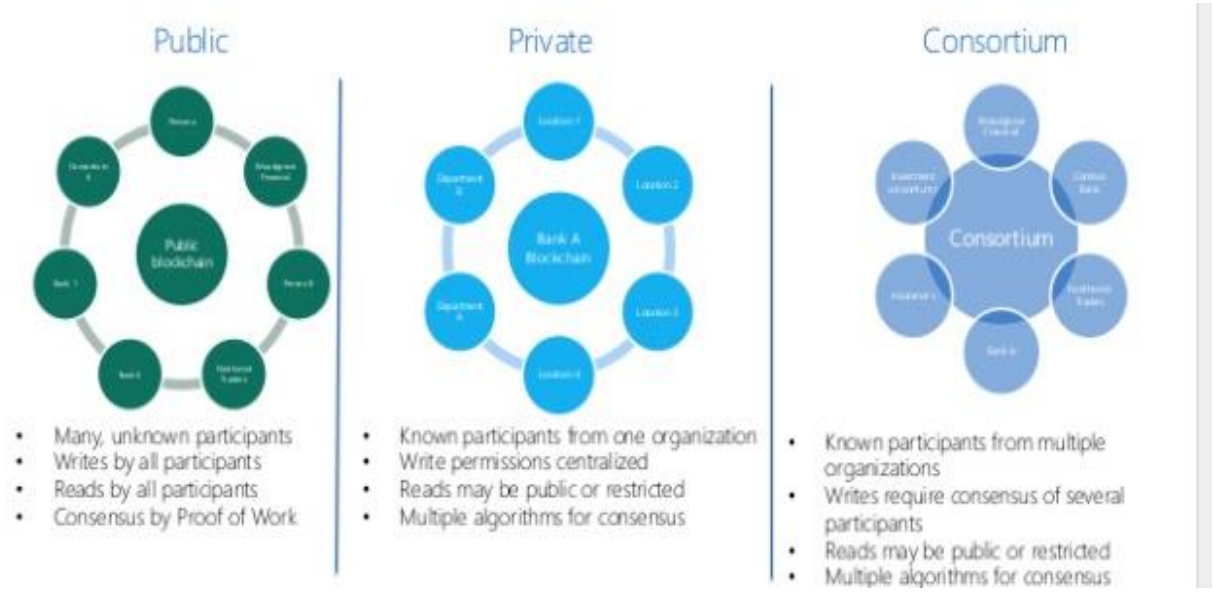
Σε γενικές γραμμές μπορούμε να διακρίνουμε τέσσερις βασικούς τύπους blockchain: δημόσιο χωρίς άδεια, δημόσιο με άδεια,ιδιωτικό χωρίς άδεια, ιδιωτικό με άδεια.Οι κίτρινες κουκκίδες είναι οι κόμβοι επικύρωσης, που σημαίνει ότι είναι σε θέση να επικυρώσουν τις συναλλαγές στο σύστημα και συμμετέχουν στο μηχανισμό συναίνεσης.Οι γαλάζιες κουκκίδες είναι οι συμμετέχοντες στο δίκτυο με την έννοια ότι μπορούν να κάνουν συναλλαγές αλλά δεν μπορούν να συμμετάσχουν στο μηχανισμό επικύρωσης.Οι γαλάζιες κουκκίδες δεν συμμετέχουν στο μηχανισμό συναίνεσης(consensus).Ο μπλε κύκλος σημαίνει ότι μόνο οι κόμβοι που βρίσκονται μέσα στο κύκλο μπορούν να δουν το ιστορικό των συναλλαγών.Οι εικόνες που δεν περιλαμβάνουν κύκλο σημαίνει ότι ο καθένας με σύνδεση στο διαδίκτυο μπορεί να δει το ιστορικό των συναλλαγών του blockchain.

Τύπος Blockchain	Επεξήγηση	Παράδειγμα	Απεικόνιση
Δημόσια χωρίς άδεια Blockchain	Σε αυτά τα συστήματα Blockchain ο καθένας μπορεί να συμμετάσχει στο μηχανισμό συναίνεσης του blockchain. Επίσης, ο καθένας παγκοσμίως με μια σύνδεση στο διαδίκτυο μπορεί να πραγματοποιήσει συναλλαγές και να δει το πλήρες αρχείο καταγραφής συναλλαγών.	Bitcoin,Litecoin, Ethereum	
Δημόσια με άδεια Blockchain	Αυτά τα blockchain συστήματα επιτρέπουν στο καθένα με μια σύνδεση στο διαδίκτυο να κάνει συναλλαγές και να βλέπει το αρχείο καταγραφής των συναλλαγών του blockchain,αν και μόνο ένας περιορισμένος αριθμός κόμβων μπορεί να συμμετάσχει στο μηχανισμό συναίνεσης.	Ripple,private versions of Ethereum	
Ιδιωτικά με άδεια blockchain	Αυτά τα συστήματα blockchain περιορίζουν αμφότερα τη δυνατότητα συναλλαγής και προβολής του αρχείου καταγραφής των συναλλαγών του blockchain μόνο στους συμμετέχοντες κόμβους στο σύστημα ,και ο αρχιτέκτονας ή ιδιοκτήτης του blockchain συστήματος είναι σε θέση να προσδιορίσει ποιος μπορεί να συμμετάσχει στο σύστημα και το ποιοι κόμβοι μπορούν να συμμετάσχουν στο μηχανισμό συναίνεσης.	Rubix, Hyperledger	
Ιδιωτικά χωρίς άδεια Blockchain	Αυτά τα blockchain συστήματα περιορίζουν ποιος μπορεί να κάνει συναλλαγές και να δει το ιστορικό των συναλλαγών του blockchain,ωστόσο ο μηχανισμός συναίνεσης είναι ανοικτός σε οποιονδήποτε.	(Partially) Exonum	
Consortium(Κοινοπραξία)	Είναι ένας ειδικός τύπος ιδιωτικού blockchain(συχνά χαρακτηρίζεται ως ένας διακριτός τύπος),.Αυτός ο τύπος blockchain μπορεί να περιγραφεί ως μερικώς αποκεντρωμένος αφού κανένας κόμβος δεν έχει το πλήρη έλεγχο αλλά ούτε κανένας κόμβος δεν επιτρέπεται να γίνει μέλος και να συμμετέχει κατά βούληση.Τα μπλοκ κοινοπραξίας (consortium blockchain) διαφέρουν από τα	Quorum,Hyperledger ,Corda	

	αντίστοιχα δημόσια στο ότι είναι με άδεια ,έτσι όχι οποιοσδήποτε με μια σύνδεση στο ίντερνετ δεν μπορεί να αποκτήσει πρόσβαση στα μπλοκ κοινοπραξίας.Ο έλεγχος στα μπλοκ κοινοπραξίας δεν παραχωρείται σε μια μοναδική οντότητα όπως στα ιδιωτικά αλλά σε ένα γκρουπ προεγκεκριμένων ανθρώπων.Στη διαδικασία της συναίνεσης το πιο πιθανό είναι να συμμετέχει ένα γκρουπ προεγκεκριμένων κόμβων.Συνοψίζοντας τα consortium blockchain έχουν τα χαρακτηριστικά ασφαλείας που είναι έμφυτα στα δημόσια μπλοκ,ενώ επίσης επιτρέπουν μεγαλύτερο έλεγχο του δικτύου.Στη συγκεκριμένη κατηγορία ποικίλλει το ποιος μπορεί να διαβάσει την αλυσίδα κοινοπραξίας, είτε αυτοί οι οποίοι επικυρώνουν τις συναλλαγές με δυνατότητα εμφάνισης σε εξουσιοδτημένους ανθρώπους ή από όλους.		

Εικόνα 4:Επιγραμματικά οι τύποι αλυσίδας Blockchain

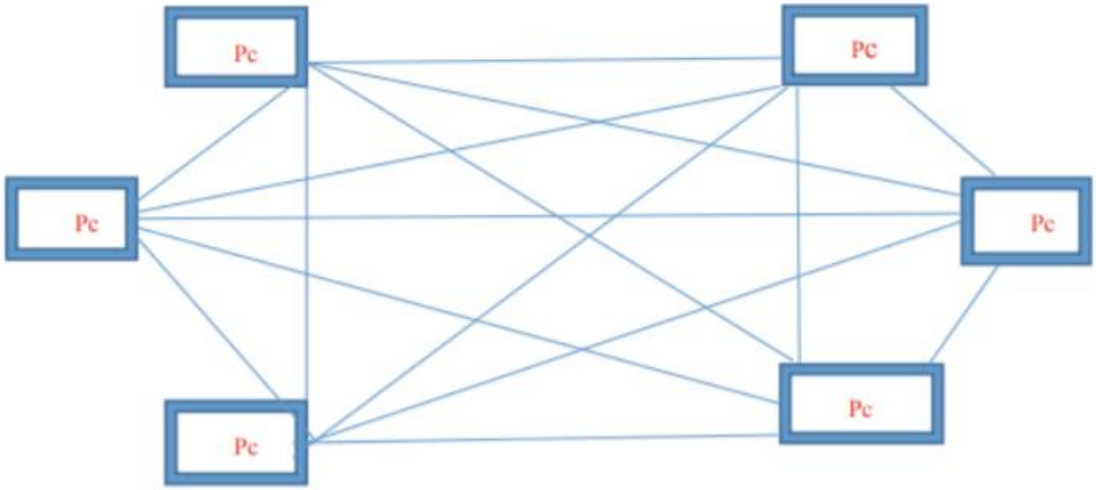
Αναλυτικότερα η διαφοροποίηση μεταξύ των αλυσίδων απεικονίζεται παρακάτω:



Εικόνα 5:Κατηγορίες blockchain

3.4.1 Αναλυτική περιγραφή των τοπολογιών blockchain

Public blockchain: Δημόσια συστήματα blockchain όπως το Bitcoin και το Ethereum επιτρέπουν σε οποιονδήποτε κόμβο να συμμετέχει στη διαδικασία συναίνεσης και οποιοσδήποτε κόμβος μπορεί να δημιουργήσει το επόμενο έγκυρο μπλοκ.Επομένως εάν όλοι οι κόμβοι έχουν τους ίδιους πόρους,τότε κάθε κόμβος έχει την ίδια πιθανότητα δημιουργίας ενός μπλοκ.Τα δημόσια Blockchain λειτουργούν χωρίς κεντρικές αρχές και μεσάζοντες.Ένα από τα πρώτα δημόσια Blockchain που κυκλοφόρησαν στο κοινό ήταν το Bitcoin public Blockchain.Επέτρεψε σε οποιονδήποτε συνδεδεμένο στο διαδίκτυο να κάνει συναλλαγές με αποκεντρωμένο τρόπο.Η επαλήθευση των συναλλαγών γίνεται μέσω μεθόδων συναίνεσης όπως Proofof-Work (PoW), Proof-of-Stake (PoS) και ούτω καθεξής.Στους πυρήνες ,οι συμμετέχοντες κόμβοι αναλαμβάνουν την επικύρωση των συναλλαγών για να λειτουργήσει το κοινό Blockchain.Το μεγαλύτερο πλεονέκτημα αυτού του είδους Blockchain είναι ότι δεν μπορεί να ελέγξει το δίκτυο πλήρως.Ως εκ τούτου,διασφαλίζει ότι τα δεδομένα είναι ασφαλή και βοηθά στο αμετάβλητο των εγγραφών. Τα Bitcoin, Ethereum και Litecoin είναι μερικά από τα παραδείγματα του Public Blockchain που χρησιμοποιούνται σε πραγματικά σενάρια.

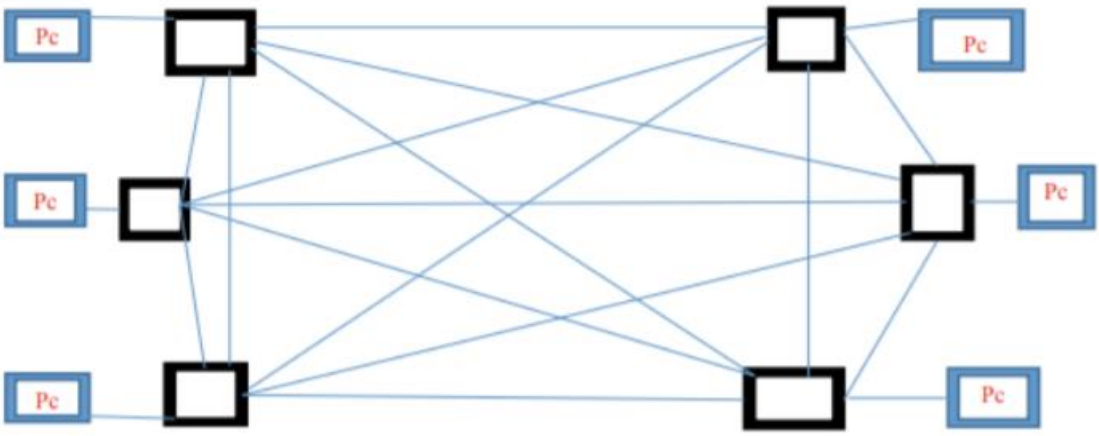


Εικόνα 6:Public Blockchain

Από την άλλη πλευρά, ένα από τα μειονεκτήματα τους είναι ότι υποφέρουν από έλλειψη ταχύτητας στις συναλλαγές . Μπορεί να χρειαστούν μερικά λεπτά έως ώρες πριν ολοκληρωθεί μια συναλλαγή. Για παράδειγμα, το Bitcoin μπορεί να διαχειρίζεται μόνο επτά συναλλαγές ανά δευτερόλεπτο σε σύγκριση με 24.000 συναλλαγές ανά δευτερόλεπτο που πραγματοποιούνται από τη VISA.

Αυτό συμβαίνει επειδή χρειάζεται αρκετός χρόνος για την επίλυση των μαθηματικών προβλημάτων και στη συνέχεια της ολοκλήρωσης της συναλλαγής. Ένα άλλο πρόβλημα με το δημόσιο Blockchain είναι η επεκτασιμότητα. Όσο περισσότεροι κόμβοι υπάρχουν, τόσο πιο αδέξιο και αργό γίνεται το δίκτυο. Έχουν ληφθεί μέτρα για την επίλυση αυτού του προβλήματος. Το Bitcoin για παράδειγμα υλοποιεί τις συναλλαγές εκτός αλυσίδας (off-chain transactions) για να κάνει το κύριο δίκτυο Bitcoin πιο γρήγορο και πιο επεκτάσιμο. Το τελευταίο μειονέκτημα ενός δημόσιου Blockchain είναι η επιλογή της μεθόδου συναίνεσης. Το Bitcoin, χρησιμοποιεί το Proof-of-Work (PoW), το οποίο καταναλώνει πολλή ενέργεια γεγονός που έχει προκαλέσει περιβαλλοντικές ανησυχίες. Συγκεκριμένα, το Blockchain του Bitcoin καταναλώνει τόση ηλεκτρική ενέργεια όσο η Ιρλανδία, ή έως και το 5% της παγκόσμιας κατανάλωσης ενέργειας που χρησιμοποιείται για την κατασκευή αλουμινίου. Ωστόσο, αυτό έχει επιλυθεί εν μέρει χρησιμοποιώντας πιο αποτελεσματικούς αλγόριθμους όπως το Proof-of-Stake (PoS).

Private Blockchain: Ένα ιδιωτικό σύστημα Blockchain μπορεί να οριστεί καλύτερα ως το Blockchain που λειτουργεί σε περιοριστικό περιβάλλον, δηλαδή κλειστό δίκτυο, και βρίσκεται υπό τον έλεγχο μιας οντότητας. Ανήκουν στο άλλο άκρο του φάσματος, καθώς επιτρέπουν μόνο μερικοί κόμβοι να είναι μέρος της διαδικασίας συναίνεσης, και μόνο ένα υποσύνολο αυτών των κόμβων μπορεί να δημιουργήσει το επόμενο μπλοκ. Τα ιδιωτικά Blockchain συνήθως έχουν έναν διαχειριστή δικτύου που μπορεί να ορίζει τα δικαιώματα χρήστη και παραμέτρους του δικτύου, όπως προσβασιμότητα, εξουσιοδότηση και ούτω καθεξής . Αυτά τα συστήματα θα μπορούσαν να χρησιμοποιηθούν μεταξύ τραπεζών για να σχηματίσουν ένα κατανεμημένο δίκτυο και να συναλλάσσονται μεταξύ τους. Αυτό προσφέρει το πλεονέκτημα μιας πιο απρόσκοπτης εμπορικής εμπειρίας, καθώς οι τράπεζες έχουν διαφορετικές τεχνολογίες οι οποίες πρέπει να επικοινωνούν μεταξύ τους για να πραγματοποιηθεί μια συναλλαγή με επιτυχία. Επιπλέον, τα ιδιωτικά Blockchain διατηρούν το απόρρητο των συμμετεχόντων και των δραστηριοτήτων τους, και έτσι, είναι η φυσική επιλογή για ιδρύματα που εκτιμούν την ιδιωτικότητα και την αποθήκευση ευαίσθητων πληροφοριών. Η κύρια διαφορά τους με τα δημόσια Blockchain εμφανίζεται στον τρόπο πρόσβασης και στην ταχύτητα. Τα ιδιωτικά Blockchain είναι γρηγορότερα. Αυτό συμβαίνει επειδή υπάρχουν λιγότεροι συμμετέχοντες σε σύγκριση με τα δημόσια Blockchain . Εν ολίγοις, απαιτείται λιγότερος χρόνος για το δίκτυο να επιτύχει συναίνεση με αποτέλεσμα γρηγορότερες συναλλαγές. Ταυτόχρονα, ιδιαίτερο πλεονέκτημα αποτελεί η επεκτασιμότητα τους. Η επεκτασιμότητα είναι δυνατή επειδή, σε ένα ιδιωτικό Blockchain, μόνο μερικοί κόμβοι έχουν εξουσιοδότηση για την επικύρωση των συναλλαγών . Αυτό σημαίνει ότι δεν έχει σημασία αν το δίκτυο μεγαλώνει, το ιδιωτικό Blockchain θα λειτουργεί με την προηγούμενη ταχύτητα και αποτελεσματικότητά του. Το κλειδί εδώ είναι η κεντρική πτυχή της λήψης αποφάσεων. Πέραν αυτού, προσφέρουν το ίδιο σύνολο δυνατοτήτων με αυτό του δημόσιου Blockchain, παρέχοντας διαφάνεια, εμπιστοσύνη και ασφάλεια στους επιλεγμένους συμμετέχοντες.



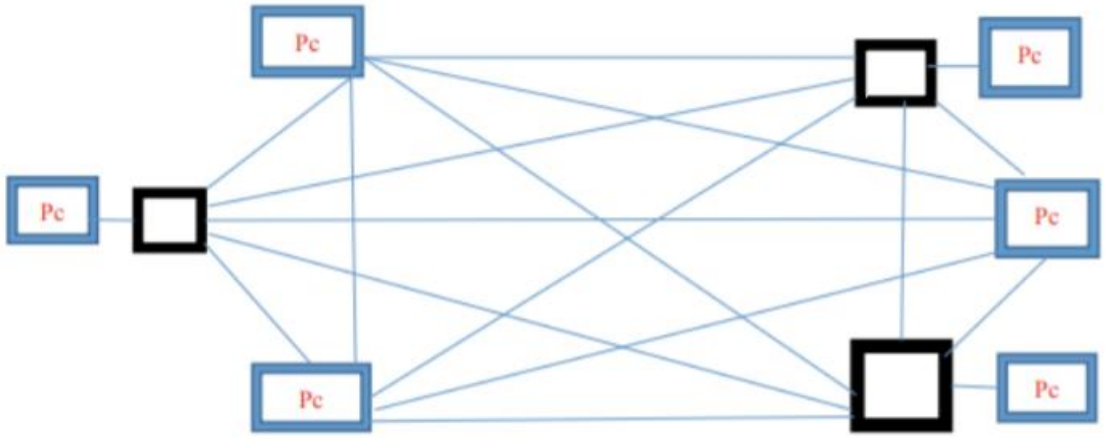
Εικόνα 7:Private Blockchain

Ωστόσο, τα ιδιωτικά Blockchain δεν είναι πραγματικά αποκεντρωμένα . Αυτό είναι ένα από τα μεγαλύτερα μειονεκτήματα τους και έρχεται σε αντίθεση με τη βασική φιλοσοφία της τεχνολογίας του κατανεμημένου καθολικού ή του Blockchain γενικά. Σε αντίθεση με τα Public Blockchain, τα οποία δεν απαιτούν από τους χρήστες να εμπιστεύονται κανέναν, δεδομένου ότι το δίκτυο είναι ανοιχτό στο κοινό, η ακεραιότητα του ιδιωτικού δικτύου Blockchain εξαρτάται από την αξιοπιστία των εξουσιοδοτημένων κόμβων, καθώς είναι απαραίτητη η εμπιστοσύνη στους κατόχους τους που υποτίθεται ότι επαληθεύουν και επικυρώνουν οι ίδιοι τις συναλλαγές. Ως αποτέλεσμα, η εγκυρότητα των εγγράφων δεν μπορεί να επαληθευτεί ανεξάρτητα. Τέλος, καθώς υπάρχουν μόνο μερικοί κόμβοι εδώ, η ασφάλεια δεν είναι τόσο καλή . Είναι σημαντικό να κατανοηθεί ότι μπορεί να χαθεί η ασφάλεια εάν κάποιος κόμβος θέσει σε κίνδυνο τη μέθοδο συναίνεσης που χρησιμοποιείται από το ιδιωτικό δίκτυο. Με λιγότερους κόμβους, είναι πολύ πιο εύκολο για έναν επιτιθέμενο να πάρει τον έλεγχο του δικτύου και να χειριστεί τα δεδομένα σε αυτό.

Consortium Blockchain: : Είναι ένας ημι-αποκεντρωμένος τύπος Blockchain όπου ένα δίκτυο Blockchain διαχειρίζεται από περισσότερους από έναν οργανισμούς. Είναι εν μέρει δημόσιο και εν μέρει ιδιωτικό και ως εκ τούτου ένας συνδυασμός τόσο δημόσιου όσο και ιδιωτικού Blockchain. Ο διαχωρισμός μεταξύ δημόσιου και ιδιωτικού χαρακτήρα συμβαίνει βάσει της συναίνεσης. Σε μια κοινοπραξία Blockchain, μόνο λίγοι κόμβοι ή χρήστες έχουν το δικαίωμα να εξουσιοδοτούν συναλλαγές και να επιβλέπουν τη διαδικασία συναίνεσης. Τις περισσότερες φορές, οι κοινοπραξίες Blockchain συνδέονται με επιχειρηματική χρήση, όπου μια ομάδα

οργανισμών συνεργάζεται για να αξιοποιήσει την τεχνολογία Blockchain για τη βελτίωση των επιχειρήσεων της. Ωστόσο, αυτός ο τύπος Blockchain μπορεί να επιτρέψει σε ορισμένους συμμετέχοντες να έχουν πρόσβαση ή να υιοθετήσουν μια υβριδική μέθοδο πρόσβασης. Για παράδειγμα, πηγές κατακερματισμού των μπλοκ και η διεπαφή προγράμματος εφαρμογής (API) ενδέχεται να είναι ανοιχτά στο κοινό. Επομένως, οι εξωτερικές οντότητες μπορούν να χρησιμοποιήσουν το API για να κάνουν έναν συγκεκριμένο αριθμό ερευνών και να λάβουν ορισμένες πληροφορίες που σχετίζονται με την κατάσταση του Blockchain. Μερικά από τα τυπικά παραδείγματα κοινοπραξιών Blockchain είναι το Korum, το Corda, Energy Web Foundation και το Hyperledger.

Hybrid Blockchain: Τα υβριδικά συστήματα Blockchain βρίσκονται στην μέση μεταξύ των δύο προαναφερθέντων. Το υβριδικό Blockchain διακρίνεται από το γεγονός ότι δεν είναι ανοιχτό σε όλους, αλλά ταυτόχρονα προσφέρει χαρακτηριστικά Blockchain όπως ακεραιότητα, διαφάνεια και ασφάλεια. Λειτουργεί σε κλειστό οικοσύστημα χωρίς να χρειάζεται να δημοσιοποιούνται τα πάντα, βέβαια οι κανόνες μπορούν να αλλάξουν ανάλογα με τις ανάγκες. Αυτά τα συστήματα επιτρέπουν σε οποιονδήποτε κόμβο να αποτελεί μέρος στη διαδικασία της συναίνεσης, αλλά μόνο καθορισμένοι κόμβοι επιτρέπεται να σχηματίσουν το επόμενο μπλοκ.



Εικόνα 8:Hybrid Blockchain

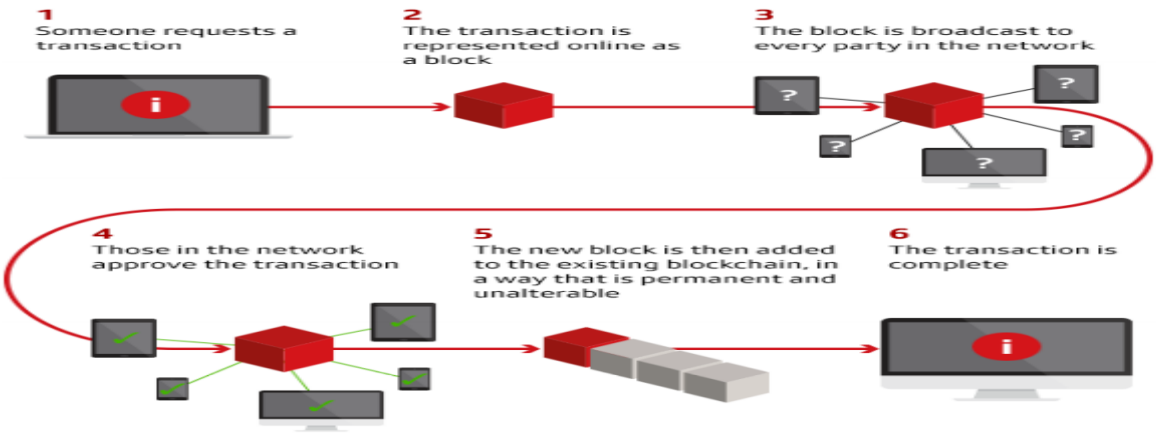
Ως συνήθως, το υβριδικό Blockchain είναι εντελώς προσαρμόσιμο. Τα μέλη του υβριδικού Blockchain μπορούν να αποφασίσουν ποιος μπορεί να συμμετάσχει στο Blockchain ή ποιες συναλλαγές δημοσιοποιούνται. Μόλις ένας χρήστης λάβει την άδεια για πρόσβαση στο υβριδικό Blockchain, μπορεί να συμμετάσχει πλήρως στις δραστηριότητες του ίδιου του

Blockchain. Όπως να μοιράζεται ίσα δικαιώματα για να πραγματοποιεί συναλλαγές, να τις βλέπει ή ακόμα και να προσαρτά ή να τροποποιεί συναλλαγές. Ωστόσο, η ταυτότητα των χρηστών διατηρείται μυστική από τους άλλους συμμετέχοντες. Αυτό γίνεται για την προστασία του απορρήτου του χρήστη. Ουσιαστικά, το κύριο χαρακτηριστικό του υβριδικού μοντέλου είναι ότι προσφέρει ιδιωτικό απόρρητο ενώ εξακολουθεί να συνδέεται με δημόσιο δίκτυο. Το κρυπτονόμισμα Ripple υποστηρίζει μια παραλλαγή του υβριδικού μοντέλου, όπου ορισμένα δημόσια ιδρύματα μπορούν να λειτουργήσουν ως επικυρωτές συναλλαγών.

3.5 Αρχιτεκτονική του blockchain και περιγραφή των δομικών μερών

3.5.1 Αρχιτεκτονική του blockchain

Σε αυτή την ενότητα εξηγείται πως λειτουργεί η τεχνολογία blockchain και η παρακάτω εικόνα απεικονίζει επίσης τα δομικά στοιχεία της τεχνολογίας τα οποία δημιουργούνται και φιλοξενούνται από το λογισμικό.



Εικόνα 9:Πώς λειτουργεί η τεχνολογία blockchain

Το σχήμα παραπάνω δείχνει ότι η συναλλαγή που πραγματοποιείται στο blockchain περιλαμβάνει τον αποστολέα,το μήνυμα ή τις πληροφορίες συναλλαγής και τον παραλήπτη.Επιπλέον,το δίκτυο blockchain αποτελείται από πολλά μπλοκ και κάθε μπλοκ περιέχει πολλές συναλλαγές και κρυπτογραφείται με ασφάλεια.Αυτό σημαίνει ότι ο οποιοσδήποτε δεν είναι μέρος του δικτύου δεν θα μπορεί να δει το περιεχόμενο του μηνύματος χωρίς κρυπτογραφικό κλειδί.Τα σημεία τα οποία παρατίθενται παρακάτω είναι τα βασικά στοιχεία της τεχνολογίας blockchain και έχουν απεικονιστεί και παραπάνω.

▪ Μήνυμα: Το μήνυμα που διαβιβάζεται στο blockchain, το οποίο θεωρείται επίσης συναλλαγή είναι η υποβολή δεδομένων ή πληροφοριών για την επεξεργασία από τους κόμβους(επίσης γνωστοί ως υπολογιστές των συμμετεχόντων στο δίκτυο) , σκοπός είναι η επικύρωση και επαλήθευση του μηνύματος που έφτασε σε αυτούς μέσω του πρωτόκολλου συναίνεσης που ακολουθείται,ώστε στο τέλος να γίνει ένα αρχείο συναλλαγών.Σύμφωνα με τον Morabito (2017), αυτό σημαίνει ότι ο αποστολέας ξεκινά ένα μήνυμα που πρέπει να μεταδοθεί σε όσους συμμετέχουν στο δίκτυο και το μήνυμα που μεταδίδεται πρέπει να περιλαμβάνει πληροφορίες σχετικά με τη δημόσια διεύθυνση του παραλήπτη, την αξία της συναλλαγής και ένα κρυπτογραφικό κλειδί,για την απόδειξη της γνησιότητας της συναλλαγής και για την επαλήθευση της εγκυρότητάς της.

▪ Έλεγχος ταυτότητας συναλλαγής:Αυτό επιτυγχάνεται μόλις οι κόμβοι (υπολογιστές ή χρήστες) στο δίκτυο λάβουν το μήνυμα που στάλθηκε, και στη συνέχεια προσπαθούν να το επικυρώσουν αποκρυπτογραφώντας την ψηφιακή υπογραφή και έπειτα τοποθετώντας την επικυρωμένη συναλλαγή σε μια ομάδα εκκρεμών συναλλαγών (Froystad & Holm, 2015).

▪ Δημιουργία μπλοκ:Εδώ, οι εκκρεμείς συναλλαγές ομαδοποιούνται από έναν από τους κόμβους του δικτύου σε άλλο για την ενημέρωση του καθολικού, το οποίο ονομάζεται επίσης μπλοκ.Στη συνέχεια, σε μια συγκεκριμένη ώρα, το ενημερωμένο μπλοκ μεταδίδεται σε άλλους κόμβους που περιμένουν επικύρωση. Είναι επίσης σημαντικό να σημειωθεί εδώ ότι τα μπλοκ μπορούν να είναι εντελώς δημόσια (το περιεχόμενό τους μπορεί να είναι ορατό σε όλους τους συμμετέχοντες) ή απλώς ημι-δημόσια (άλλοι συμμετέχοντες μπορούν να δουν το κοντέινερ και την ετικέτα του, αλλά δεν θα μπορούν να δουν το περιεχόμενό του χωρίς το κρυπτογραφικό κλειδί για την αποκρυπτογράφηση του μηνύματος 29) (Fullbright, 2016).

▪Επαλήθευση μπλοκ: Αυτή η διαδικασία ασχολείται με την επικύρωση και τον έλεγχο ταυτότητας των μπλοκ στο δίκτυο. Αυτό συμβαίνει όταν οι κόμβοι που είναι υπεύθυνοι για τη διαδικασία επικύρωσης στο δίκτυο λαμβάνουν ένα αίτημα για επικύρωση ενός προτεινόμενου ή ενημερωμένου μπλοκ, περνούν από μια επαναληπτική διαδικασία που απαιτεί συναίνεση από την πλειονότητα των κόμβων που συμμετέχουν στο δίκτυο, προκειμένου να γίνει έλεγχος

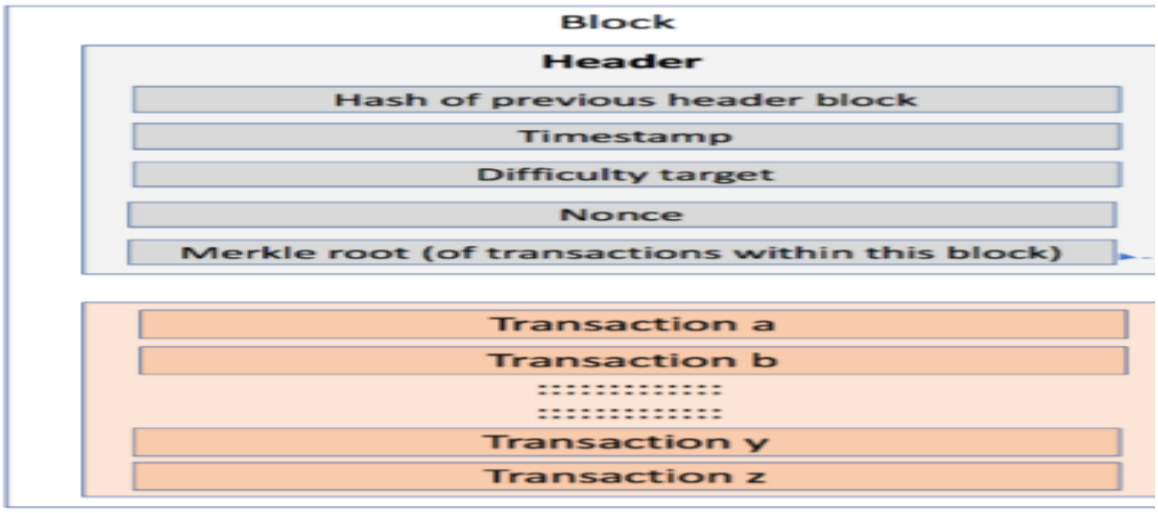
ταυτότητας του μπλοκ (Morabito, 2017). Οι Froystad και Holm (2015) ρίχνουν περισσότερο φως σε αυτό το έργο τους εξηγώντας ότι οι διάφοροι τύποι διαθέσιμων δικτύων blockchain χρησιμοποιούν διαφορετικές μορφές τεχνικών επικύρωσης. Αναφέρουν επίσης ότι το blockchain του Bitcoin χρησιμοποιεί την «απόδειξη της τεχνικής εργασίας», το Ripple χρησιμοποιεί μια τεχνική που ονομάζεται «κατανεμημένη συναίνεση», ενώ το Ethereum χρησιμοποιεί μια εντελώς διαφορετική τεχνική που ονομάζεται «απόδειξη πονταρίσματος». Στη συνέχεια καταλήγουν λέγοντας ότι αυτές οι τεχνικές χρησιμοποιούνται για να διασφαλιστεί ότι κάθε συναλλαγή είναι αυθεντική και έγκυρη και επίσης για να βεβαιωθεί ότι δεν υπάρχουν δόλιες συναλλαγές στο δίκτυο.

▪ Αλυσίδα μπλοκ: Μόλις εγκριθούν ή επικυρωθούν όλες οι συναλλαγές σε ένα μπλοκ, τότε το νέο μπλοκ συνδέεται με το προηγούμενο μπλοκ και όταν έχει ολοκληρωθεί, η τρέχουσα κατάσταση του καθολικού μεταδίδεται στους συμμετέχοντες στο δίκτυο (Fullbright, 2016). Αυτή η όλη διαδικασία διαρκεί περίπου 3-10 δευτερόλεπτα, καθιστώντας έτσι το blockchain μια πολύ γρήγορη τεχνολογία για την εκτέλεση διαφόρων δραστηριοτήτων σε διαφορετικές βιομηχανίες (Morabito, 2017). Επιπλέον, είναι καλό να γνωρίζουμε ότι σε άλλα πρότυπα για να αλλάχτει ένα μπλοκ στην αλυσίδα, θα ήταν υποχρεωτικό να αλλάξουν όλα τα μπλοκ που ακολούθησαν. Ως εκ τούτου, μόλις τροποποιηθούν οποιαδήποτε δεδομένα ή πληροφορίες στο δίκτυο blockchain, γίνονται αυτόματα ορατό σε όλα τα άλλα μέρη που συμμετέχουν στο δίκτυο καθώς αλλάζει ο κατακερματισμός του τρέχοντος μπλοκ καθώς και του προηγούμενου και του επόμενου μπλοκ.

3.5.2 Τι είναι το block

Το μπλοκ αποτελείται από μια λίστα καταγεγραμμένων συναλλαγών για μια χρονική περίοδο.Οι συναλλαγές μπορούν να αντιπροσωπεύουν οποιοδήποτε τύπο δραστηριότητας και αποθηκεύονται ως εγγραφή στο μπλοκ.Τυχόν κανόνες που αφορούν το ίδιο το μπλοκ θεσπίζονται κατά τη δημιουργία του δικτύου.Για παράδειγμα ο μέγιστος αριθμός συναλλαγών σε ένα μπλοκ ή το μέγεθος κάθε μπλοκ μπορεί να είναι περιορισμένο.Εν συνεχεία περιγράφονται τα δομικά μέρη ενός block

- Κάθε μπλοκ περιλαμβάνει μια κεφαλίδα(block header) και ένα Merkle Tree που περιέχει δεδομένα συναλλαγών.



Εικόνα 10:Δομικά μέρη ενός block

Τα περιεχόμενα της επικεφαλίδας κάθε μπλοκ είναι:

- Μια hash αναφορά στην επικεφαλίδα του προηγούμενου μπλοκ.
- Η χρονική στιγμή στην οποία ξεκίνησε η επίλυση του hash puzzle
- Το επίπεδο δυσκολίας του hash πάζλ.
- Το nounce που λύνει το hash πάζλ.
- Η ρίζα του Merkle tree που περιέχει τα δεδομένα των συναλλαγών.

Επομένως ,η σύνδεση μεταξύ των μπλοκ σε μια αλυσίδα γίνεται μέσω των hash αναφορών στις επικεφαλίδες των blocks,με κάθε μπλοκ να διατηρεί σύνδεση με τη hash αναφορά του προηγούμενού του block.Η κεφαλή δε του blockchain έχει ως τιμή την hash αναφορά στην επικεφαλίδα του πλέον πρόσφατα εισηγμένου μπλοκ.Η πρώτη συναλλαγή σε ένα μπλοκ είναι μια ειδική συναλλαγή που ονομάζεται «συναλλαγή coinbase» στην οποία τοποθετείται η εν δυνάμει αμοιβή την οποία θα λάβει ο miner εφόσον επιλύσει το μπλοκ.Για παράδειγμα,στο Bitcoin η αμοιβή αυτή με τις τρέχουσες τιμές είναι 12.5 bitcoins και μπορεί να χρησιμοποιηθεί μόνο εάν το μπλοκ αποτελέσει μέρος του blockchain και αφού έχουν προστεθεί ακόμα 100 μπλοκς στο blockchain.

3.5.3 Τι είναι η συναίνεση(consensus)

Η επιβολή των απαιτούμενων κανόνων στους κόμβους του δικτύου που είναι επιφορτισμένοι με την επαλήθευση των στοιχείων που πρόκειται να καταγραφούν στο καθολικό πραγματοποιείται μέσω αλγορίθμων συναίνεσης. Οι κόμβοι αυτοί ονομάζονται πλήρεις κόμβοι

(full nodes). Οι αλγόριθμοι συναίνεσης μπορεί να διαφέρουν από blockchain σε blockchain ανάλογα με το είδος της πληροφορίας που καταγράφεται και το εάν το δίκτυο είναι δημόσιο ή ιδιωτικό. Στο bitcoin για παράδειγμα καταγράφονται συναλλαγές στο κρυπτονόμισμα bitcoin (BTC) οι οποίες πριν προσαρτηθούν στο blockchain θα πρέπει να επαληθευτούν μέσω ενός ισχυρού αλγορίθμου συναίνεσης που ονομάζεται POW (Proof Of Work). Οι πλήρεις κόμβοι διαθέτουν υπολογιστική ισχύ σε αντάλλαγμα του να τους δοθεί η δυνατότητα να επαληθεύουν συναλλαγές και συνεπώς να έχουν τη πιθανότητα να κερδίσουν ως ανταμοιβή κάποια bitcoins. Από την άλλη μεριά και σε ένα ιδιωτικό blockchain μπορούν να καταγράφονται συναλλαγές. Σε αυτή την περίπτωση καθώς οι συμμετέχοντες έχουν γνωστή και επαληθεύσιμη ταυτότητα, μπορούν να χρησιμοποιηθούν ελαφρύτεροι και ταχύτεροι αλγόριθμοι συναίνεσης έτσι ώστε ο ρυθμός διεκπεραίωσης των συναλλαγών να είναι υψηλότερο.Λαμβάνοντας υπόψιν τα προηγούμενα υπάρχουν διαφορετικοί τύποι να πετύχεις συναίνεση.Ειδικότερα,υπάρχουν διαφορετικοί αλγόριθμοι συναίνεσης

- Απόδειξη εργασίας(Proof of Work):το οποίο απαιτεί από τους χρήστες του δικτύου να επιλύσουν ένα περίπλοκο μαθηματικό πάζλ με στόχο να επικυρώσουν μια συναλλαγή και να δημιουργήσουν ένα καινούργιο block
- Απόδειξη μεριδίου-πονταρίσματος(Proof of Stake): ο δημιουργός του επόμενου block επιλέγεται μέσω διάφορων συνδυασμών τυχαίας επιλογής καθώς και βασιζόμενος σε πολλούς παράγοντες σχετιζόμενους με το μερίδιο όπως η ηλικία και ο πλούτος.
- Practical Byzantine Fault Tolerance: ο οποίος επιτυγχάνει συναίνεση ως αποτέλεσμα ενός ελάχιστου αριθμού άλλων κόμβων στο δίκτυο τα οποία επικυρώνουν το καινούργιο block
- Απόδειξη χρόνου που παρήλθε(Proof of Elapsed Time): Το οποίο είναι ένα υβρίδιο βασισμένο σε αλγόριθμος τυχαίας λαχειοφόρου αγοράς και προτεραιότητας τύπου πρώτος έρχεται πρώτος εξυπηρετείται (first-come-first-serve basis).

- Απόδειξη εξουσίας(Proof of Authority):Στο PoA,τα δικαιώματα δημιουργίας κόμβων απονέμονται σε κόμβους που έχουν αποδείξει την εξουσία τους να το κάνουν.Για να αποκτήσει αυτή την εξουσία και το δικαίωμα δημιουργίας νέων μπλοκ,ένας κόμβος πρέπει να περάσει έναν προκαταρτικό έλεγχο ταυτότητας.

3.5.4 Τύποι εγγραφών που αποθηκεύονται στο blockchain

Τα blockchain συνήθως χρησιμοποιούνται για την αποθήκευση εγγραφών:1)από συναλλαγές περιουσιακών στοιχείων,2)έξυπνων συμβάσεων,3)ψηφιακών υπογραφών και πιστοποιήσεων.

Οι εγγραφές συναλλαγών περιουσιακών στοιχείων συνήθως έχουν δύο μορφές

- Χρήματα εκφρασμένα σε μονάδες νομίσματος: όπου κάθε μεμονωμένη μονάδα του ίδιου νομίσματος έχει την ίδια τιμή με κάθε άλλη μονάδα κάθε φορά. Τα νομίσματα επίσης είναι ενδομετατρέψιμα με συναλλαγματική ισοτιμία. Η πιο συνηθισμένη μορφή νομίσματος χτισμένη με τη χρήση τεχνολογίας blockchain είναι το Bitcoin.
- Τεκμηριωτικά αποδεικτικά στοιχεία για τα δικαιώματα ιδιοκτησίας, νομικά γνωστά ως τίτλοι ιδιοκτησίας Αυτά συνήθως χρησιμοποιούνται για να αντιπροσωπεύσουν ακίνητη περιουσία ή άυλη ιδιοκτησία όπως δικαιώματα πνευματικής ιδιοκτησίας.

Έξυπνα συμβόλαια: τα οποία ουσιαστικά είναι μικρά προγράμματα υπολογιστών αποθηκευμένα σε blockchain,τα οποία θα εκτελέσουν συναλλαγές κάτω από συγκεκριμένες προϋποθέσεις. Έτσι , τα έξυπνα συμβόλαια συνήθως αποτελούν μια δήλωση όπως «μεταφορά του x στο y εάν συμβεί ο z».Σε αντίθεση με ένα κανονικό συμβόλαιο όπου μετά την επίτευξη της συμφωνίας, τα μέρη πρέπει να εκτελέσουν τη σύβαση για να λάβει χώρα, ένα έξυπνο συμβόλαιο αυτό-εκτελείται, με άλλα λόγια μόλις οι οδηγίες γράφονται σε ένα blockchain,η συναλλαγή θα πραγματοποιηθεί αυτόματα όταν ανιχνευθούν οι κατάλληλες συγθήκες,χωρίς περαιτέρω ενέργειες από τα μέρη της συναλλαγής ή από τρίτους.

Στην πιο ουσιαστική μορφή,η πιστοποίηση είναι το ζήτημα μιας δήλωσης από ένα μέρος σε στο άλλο ότι ένα συγκεκριμένο σύνολο γεγονότων είναι αλήθεια. Οι υπογραφές είναι αποδείξεις ότι η δήλωση εκδόθηκε από και προς τα εν λόγω μέρη. Το blockchain μπορεί να χρησιμοποιηθεί είτε για την αποθήκευση κρυπτογραφικών κατακερματισμών(«ψηφιακά δακτυλικά αποτυπώματα») από τα πιστοποιητικά ή για την αποθήκευση των αξιώσεων του εαυτού τους. Κατά αυτό το τρόπο το blockchain μπορεί να έχει τη λειτουργία ενός δημόσιου μητρώου πιστοποιητικών.

3.6 Στοιχειώδεις έννοιες του Blockchain

3.6.1 Κρυπτογραφία

Το δίκτυο Blockchain διασφαλίζει τη λειτουργία της αλυσίδας χρησιμοποιώντας κρυπτογράφηση ασύμμετρου κλειδιού. Η εκτέλεση οποιασδήποτε συναλλαγής απαιτεί από τους συμμετέχοντες να έχουν ψηφιακό πορτοφόλι το οποίο είναι ασφαλισμένο με το ιδιωτικό κλειδί τους. Η κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιείται για την υπογραφή συναλλαγών Bitcoin ή άλλων συναλλαγών Blockchain. Το Bitcoin χρησιμοποιεί ασύμμετρη κρυπτογράφηση για να βεβαιωθεί ότι μόνο ο ιδιοκτήτης ενός πορτοφολιού χρημάτων μπορεί

να κάνει ανάληψη ή να μεταφέρει χρήματα σε αυτό. Στην κρυπτογράφηση ασύμμετρου κλειδιού χρησιμοποιείται ζεύγος κλειδιών (key pair) για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Κάθε χρήστης παράγει το δικό του ζεύγος κλειδιών, δηλαδή τα κλειδιά δημόσιας κρυπτογράφησης (δημόσια διεύθυνση πορτοφολιού) και ιδιωτικής αποκρυπτογράφησης τα οποία είναι διαφορετικά μεταξύ τους . Έπειτα, γνωστοποιεί σε όλους τους χρήστες το δημόσιο κλειδί κρυπτογράφησης προκειμένου να μπορούν να του αποστείλουν κρυπτογραφημένα μηνύματα. Οποιοσδήποτε κατέχει το δημόσιο κλειδί κρυπτογράφησης μπορεί να στείλει μηνύματα, αλλά μόνο ο κάτοχος του ιδιωτικού κλειδιού μπορεί να τα αποκωδικοποιήσει. Οι ποιο διαδεδομένοι αλγόριθμοι για ασύμμετρα κρυπτοσυστήματα είναι οι εξής:

• Αλγόριθμος RSA

• Αλγόριθμος Elliptic-Curve Cryptography (ECC).

• Αλγόριθμος των Diffie-Hellman

• Αλγόριθμος Digital Signature Standard (DSS)

Ο συνδυασμός και των δύο κλειδιών δημιουργεί μια ψηφιακή υπογραφή. Αυτή η ψηφιακή υπογραφή αποδεικνύει την ιδιοκτησία των κρυπτονομισμάτων και επιτρέπει τον έλεγχο τους μέσω ενός πορτοφολιού.

3.6.2 Τι είναι το hash

Το hash αποτελεί έναν σύντομο κώδικα καθορισμένου μήκους που χρησιμεύει ως δακτυλικό αποτύπωμα για ένα ψηφιακό έγγραφο. Ένα πρόγραμμα που ονομάζεται hash-generator επιτρέπει σε έναν χρήστη να φορτώσει οποιαδήποτε σειρά κειμένου και να δημιουργήσει ένα μοναδικό αναγνωριστικό. Κάθε φορά που εκτελείται η ίδια σειρά κειμένου μέσω του hash-generator, θα δοθεί το ίδιο αναγνωριστικό εγγράφου. Η συμβολή του κατακερματισμού ως συσκευή κατά της παρεμπόδισης είναι σημαντική: αν αλλάξει ένα γράμμα σε ένα έγγραφο, θα δημιουργηθεί αυτόματα ένα εντελώς διαφορετικό αναγνωριστικό. Τα hash είναι μονόδρομοι (Gupta, S2017). Αυτό σημαίνει ότι η γεννήτρια κατακερματισμού μπορεί να χρησιμοποιηθεί για να δημιουργήσει ένα hash από το έγγραφο, αλλά είναι μαθηματικά αδύνατο να δημιουργηθεί ένα έγγραφο από ένα 34 hash. Σε ένα blockchain, κάθε μπλοκ συναλλαγών είναι εξασφαλισμένο με τη συμπερίληψη ενός hash του μπλοκ πληροφοριών, καθώς και του

προηγούμενου μπλοκ, επιτρέποντας έτσι σε όλα τα μέρη να εγγυηθούν ότι καμία από τις συναλλαγές δεν έχει τροποποιηθεί ή αλλοιωθεί (Lemieux, 2016).

3.6.3 Ψηφιακές υπογραφές

Οι ψηφιακές υπογραφές αποδεικνύουν την κυριότητα των κρυπτονομισμάτων κάποιου χρήστη και επιτρέπουν σε αυτόν να ελέγχει τα χρήματα του. Συνδέοντας μια ψηφιακή υπογραφή σε μια συναλλαγή, κανείς δεν μπορεί να αμφισβητήσει ότι αυτή η συναλλαγή δεν είναι γνήσια και είναι προϊόν πλαστογραφίας. Το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή συναλλαγών, ενώ το δημόσιο κλειδί στη συνέχεια χρησιμοποιείται για την επαλήθευση της υπογραφής από τους υπολογιστές επικύρωσης. Όταν ένας χρήστης δημιουργήσει για πρώτη φορά ένα πορτοφόλι, δημιουργείται ένα ζεύγος κλειδιών που αποτελείται από ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί.

3.7 Ανάλυση Πλεονεκτημάτων μειονεκτημάτων της τεχνολογίας

3.7.1 Μειονεκτήματα της τεχνολογίας blockchain

Το blockchain αποτελεί ένα πλήρως ομότιμο σύστημα που επιτρέπει σε οποιονδήποτε να διαβάσει το ιστορικό των συναλλαγών και να προσθέσει τις δικές του συναλλαγές οι οποίες ενσωματώνονται σε μια δομή δεδομένων που διατηρείται συλλογικά από τα μέλη του δικτύου. Συνεπώς, όλα τα στοιχεία των συναλλαγών είναι διαθέσιμα σε όλους και το γεγονός αυτό καθιστά προβληματική τη χρήση του blockchain σε περιπτώσεις που απαιτούνται υψηλά επίπεδα ιδιωτικότητας (privacy). Βέβαια, οι αριθμοί λογαριασμών είναι δημόσια κρυπτογραφικά κλειδιά και όχι πραγματικά ονόματα ή διευθύνσεις. Ωστόσο, αν για οποιοδήποτε λόγο το ιδιωτικό κλειδί ενός λογαριασμού δοθεί σε άλλους τότε η ασφάλεια του λογαριασμού καταρρέει.Ένα άλλο σημείο προβληματισμού έχει να κάνει με τις δυνατότητες κλιμάκωσης του συστήματος. Ο μηχανισμός επαλήθευσης των συναλλαγών μέσω της επίλυσης hash παζλς επιβάλει όρια στην ταχύτητα διεκπεραίωσης των συναλλαγών που μπορεί να μην είναι αποδεκτά για ορισμένα είδη εφαρμογών. Επιπλέον, το κόστος αγοράς εξειδικευμένου εξοπλισμού και το κόστος κατανάλωσης ηλεκτρικού ρεύματος είναι ιδιαίτερα υψηλά. Από την άλλη μεριά, υπάρχουν θέματα νομικής φύσεως που σχετίζονται με το ποιος έχει την ευθύνη

απέναντι στο νόμο για την επιβεβαίωση των συναλλαγών δεδομένου του συλλογικού τρόπου με τον οποίο πραγματοποιείται η επαλήθευση. Το γεγονός αυτό προκαλεί ανασφάλεια στους πιθανούς χρήστες και περιορίζει τον αριθμό των χρηστών που επιλέγουν να χρησιμοποιήσουν την τεχνολογία blockchain.

3.8 Σύνοψη

Στο κεφάλαιο αυτό, πραγματοποιήθηκε μια επεξήγηση της τεχνολογίας blockchain , όπου φάνηκε η σημασία της καθώς και περιγράφηκαν τα βασικά στοιχεία της.

Αναλύθηκαν ακόμα, τα δομικά της μέρη ώστε να γίνει πιο κατανοητή.Ιδιαίτερη έμφαση δόθηκε στη περιγραφή του μηχανισμού συναίνεσης καθώς και στις βασικές τις έννοιες ώστε να γίνουν αντιληπτά τα οφέλη από τη χρήση της. Τέλος, παρουσιάστηκαν αναλυτικά τα διάφορα είδη blockchain που υπάρχουν.

Με την ολοκλήρωση αυτού του κεφαλαίου, γίνονται αντιληπτοί οι λόγοι της εγκαθίδρυσης αυτής της τεχνολογίας ως μέσο επαλήθευσης πιστοποιητικών παρουσιάζοντας τα πλεονεκτήματα της χρήσης της σε αντίθεση από τα μειονεκτήματά της.

Κεφάλαιο 4: Διαφορετικές εφαρμογές με τη χρήση της τεχνολογίας blockchain για την έγκριση πιστοποιητικών

4.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο έγινε εκτενής περιγραφή της τεχνολογίας blockchain,των βασικών στοιχείων της και των δομικών στυστατικών της ώστε να γίνει κατανοητό πως καθένα λειτουργεί. Αναπτύχθηκε ιδιαίτερα η σημασία του μηχανισμού συναίνεσης αλλά και τα διαφορετικά είδη μηχανισμών συναίνεσης ανάλογα με το είδος του blockchain.

Σε αυτό το κεφάλαιο γίνεται η περιγραφή και ανάλυση διάφορων πλατφορμών που έχουν αναπτυχθεί για την επαλήθευση διαπιστευτηρίων,τα θετικά και τα επιπλεόν γνωρίσματα που έχει η καθεμία εξ'αυτών καθώς και σε μερικές περιπτώσεις τα πλεονεκτήματα που έχει καθεμία σε σχέση με τη πλατφόρμα πάνω στην οποία στηρίχτηκε η δημιουργία της.

Τέλος,αναφέρονται κάποια προβλήματα που αντιμετωπίζουν οι υπάρχουσες πλατφόρμες οι οποίες κατά κύριο λόγο λειτουργούν σε πιλοτικό επίπεδο και κάποιες λύσεις οι οποίες έχουν προταθεί για να αντιμετωπιστούν τα υπάρχοντα προβλήματα στο μέλλον.

4.1 Open Badges

Το έργο Open Badges δημιουργήθηκε το 2011 από την έρευνα του Erick Knight από το ίδρυμα Mozilla με χρηματοδότηση από το ίδρυμα McArthur.Τα πρώτα πρωτότυπα αναπτύχθηκαν στο Mozilla Φεστιβάλ το 2010.Το έγγραφο "**Open Badges for Lifelong Learning**" από τον Knight και τους συνεργάτες στο Peer to Peer πανεπιστήμιο και στο ίδρυμα MacArthur, δίνει μια πιο λεπτομερή ματιά στους στόχους του έργου. Τα Open Badges είναι επαληθεύσιμα ,ψηφιακά badges με ενσωματωμένα μεταδεδομένα σχετικά με τις δεξιότητες και τα επιτεύγματα. Οι προδιαγραφές του Open Badges είναι διαθέσιμες στο https://openbadgespec.org/. Τα Open Badges από την έκδοση 1.1 και πάνω, είναι αντικείμενα συνδεδεμένων δεδομένων σε μορφή JSON-LD που ορίζονται στην ενότητα σχετικό πλαίσιο JSON-LD (επί του παρόντος, Open Badges v2.0).Μπορούν να ενσωματωθούν σε ψηφιακές εικόνες σε PNG ή SVG φορμάτ που μπορεί στη συνέχεια να αναπαριστά το πιστοποιητικό με οπτικό τρόπο π.χ. με τις πληροφορίες του κατόχου του πιστοποιητικού και την υπογραφή και σφραγίδα του εκδότη(που ονομάζεται

“badge banking “),ή να χρησιμοποιηθεί ως ένα αυτόνομο πακέτο δεδομένων. Η παρακάτω εικόνα μας δείχνει ένα παράδειγμα αντικειμένου Open Badge όπως δίνεται στη προδιαγραφή:


```
{
  "@context": "https://w3id.org/openbadges/v2",
  "type": "Assertion",
  "id": "https://example.org/beths-robotics-badge.json",
  "recipient": {
    "type": "email",
    "hashed": true,
    "salt": "deadsea",
    "identity": "sha256$c7ef86405ba71b85acd8e2e95166c4b111448089f2e1599f42fe1bba46e865c5"
  },
  "issuedOn": "2016-12-31T23:59:59Z",
  "badge": {
    "id": "https://example.org/robotics-badge.json",
    "type": "BadgeClass",
    "name": "Awesome Robotics Badge",
    "description": "For doing awesome things with robots that people think is pretty great.",
    "image": "https://example.org/robotics-badge.png",
    "criteria": "https://example.org/robotics-badge.html",
    "issuer": {
      "type": "Profile",
      "id": "https://example.org/organization.json",
      "name": "An Example Badge Issuer",
      "image": "https://example.org/logo.png",
      "url": "https://example.org",
      "email": "steved@example.org",
    }
  },
  "verification": {
    "type": "hosted"
  }
}
```


Εικόνα 11:Παράδειγμα πιστοποιητικού Open Badges.Η μορφή είναι JSON-LD και ως Linked Data αντικείμενο, επιτρέπει αναφορά σε διαδικτυακούς πόρους που περιέχουν πρόσθετες πληροφορίες.

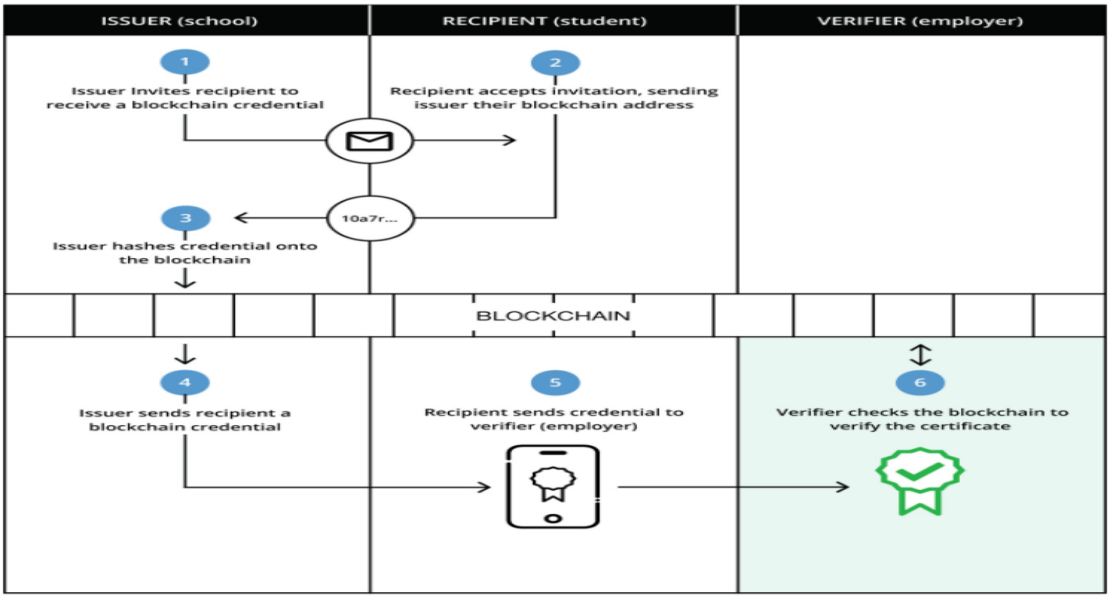
Ο ορισμός όλων των απαιτούμενων και προαιρετικών πεδίων στο JSON-LD αντικείμενο βρίσκονται στις προδιαγραφές του Open Badge.Τα Open Badges μπορούν να αποθηκευτούν στο διαδίκτυο(κατά προτίμηση σε αποθήκη δεδομένων με υποστήριξη Linked Data) ή offline ως αρχεία με την οποία μορφή μπορούν επίσης να μεταφερθούν εύκολα. Δεν παρέχουν περιορισμό πρόσβασης ή έλεγχο απορρήτου από μόνα τους. Αν και είναι δυνατή η αποθήκευση των δεδομένων ενός Open Badge σε πολλαπλά τελικά σημεία και να περιλαμβάνει έλεγχο πρόσβασης εκεί παρέχοντας μόνο μερική πρόσβαση θα ακυρώσει το badge.Τα Open Badges επιτρέπουν την ηλεκτρονική επαλήθευση των βραβευμένων Badges παρέχοντας έναν σύνδεσμο προς μια διαδικτυακή υπηρεσία επικύρωσης που φιλοξενείται από τον εκδότη ή από ένα τρίτο μέρος. Επιτρέπουν επίσης την ενσωμάτωση ηλεκτρονικών υπογραφών σε μορφή JSON,ηλεκτρονικών υπογραφών που επιτρέπουν την επαλήθευση εκτός σύνδεσης για κάθε badge.Η χρήση των Open Badges ξεκίνησε σχετικά πρόσφατα. Η IBM χρησιμοποιεί και εκδίδει Open Badges στην πύλη δεξιοτήτων της από το 2016 και έχει αναφερθεί ότι έχει εκδώσει ένα εκατομμύριο Badges τον Ιούνιο του 2018.Τα Open Badge είναι το ντε φάκτο πρότυπο μορφής δεδομένων για πιστοποιητικά ψηφιακής εκπαίδευσης. Ως Linked data αντικείμενα ακολουθώντας το πρότυπο JSON-LD,επιτρέπουν την ενσωμάτωση εξωτερικών πληροφοριών από διαδικτυακούς πόρους. Η δυνατότητα συμπερίληψή τους σε εικόνες θα βοηθήσει τη διαδικασία αποδοχής και υιοθέτησης κάνοντας τα έτσι ελκυστικά στους τελικούς χρήστες. Τα Open Badges δεν φροντίζουν τη διαχείριση ταυτότητας και δεν προσφέρουν καμία λύση στο πρόβλημα της διαρκούς αποθήκευσης του ίδιου του πιστοποιητικού. Επίσης δεν υπάρχει υποστήριξη για ιδιωτικότητα στα Open Badges από προεπιλογή-εάν η πρόσβαση σε περιοχές

δεδομένων είναι περιορισμένη, ο έλεγχος εγκυρότητας του badge θα αποτύχει. Ένα άλλο πρόβλημα των Open Badges που προκύπτει από το ότι είναι linked data,είναι η καταστροφή του συνδέσμου: εάν τα δεδομένα που είναι απαραίτητα για το badge που αναφέρεται από έναν σύνδεσμο δεν είναι πλέον διαθέσιμα, το badge δεν θα επικυρωθεί και το περιεχόμενο των συνδεδεμένων δεδομένων χάνεται. Αυτό είναι επίσης θέμα με την επαλήθευση του badge εάν η επαλήθευση γίνεται από μια ηλεκτρονική υπηρεσία. Για παράδειγμα εάν ο εκδότης ενός συνόλου badges σταματήσει να υπάρχει το ίδιο κάνει και η υπηρεσία επαλήθευσης. Στη συνέχεια όλα αυτά τα badges από αυτόν τον εκδότη δεν θα επαληθεύονται πλέον.

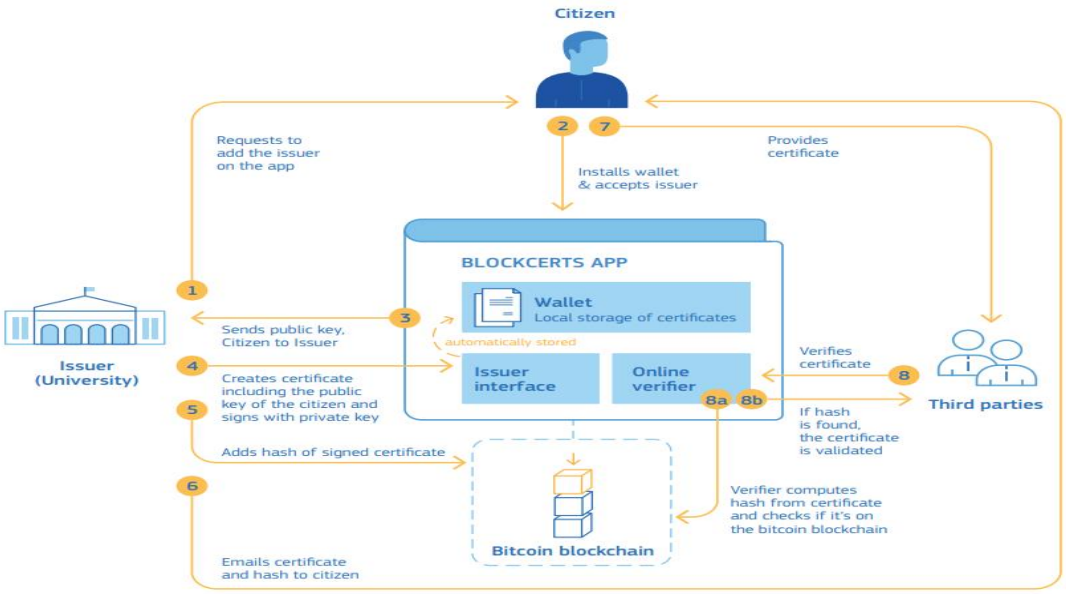
4.2 Ορισμός Blockcert

Το Blockerts είναι ένα ανοικτό πρότυπο για τη δημιουργία, την έκδοση, την προβολή και την επαλήθευση των πιστοποιητικών που βασίζονται σε blockchain. Αυτά τα ψηφιακά αρχεία καταγράφονται σε blockchain, κρυπτογραφικά υπογεγραμμένα, ανθεκτικά στις παραβιάσεις και κοινά. Ο στόχος είναι να δημιουργηθεί ένα κύμα καινοτομίας που δίνει στα άτομα τη δυνατότητα να κατέχουν και να μοιράζονται τα δικά τους επίσημα αρχεία. Ο αρχικός σχεδιασμός βασίστηκε σε πρωτότυπα που αναπτύχθηκαν στο MIT Media Lab και στο Learning Machine το 2016 με επικεφαλής τον Philipp Schmidt και τον Juliana Nazare (με τη βοήθεια πολλών άλλων, συμπεριλαμβανομένων των Guy Zyskind και Jeremy Rubin). Η Kim Hamilton ήταν η επικεφαλής της τεχνολογίας και διευθύντρια για το βασικό λογισμικό και πρότυπο που εκδόθηκε και ο Chris Downie ανέπτυξε την εφαρμογή για το iOS .Η πλατφόρμα Blockcerts επιτρέπει στους προγραμματιστές να δημιουργούν DApps(αποκεντρωμένες εφαρμογές) που είναι σε θέση να επικυρώσουν πιστοποιητικά για ακαδημαϊκά διαπιστευτήρια, επαγγελματικές πιστοποιήσεις και εγγραφές. Οι χρήστες αποκτούν πρόσβαση στην πλατφόρμα επαλήθευσης Blockcerts κατεβάζοντας την εφαρμογή Blockcerts για κινητά που είναι διαθέσιμη τόσο για συσκευές IOS όσο και για Android.Απόφοιτοι του Ινστιτούτου τεχνολογίας της Μασαχουσέτης μπορούν πλέον να λάβουν το δίπλωμα τους μέσω μιας εφαρμογής. Αυτή η εφαρμογή ονομάζεται Blockcerts Wallet και επιτρέπει σε οποιονδήποτε σπουδαστή να αποκτήσει ένα απαραβίαστο πτυχίο που μπορεί να επαληθευτεί από οποιονδήποτε εργοδότη ή πανεπιστήμιο.Το Blockcerts χρησιμοποιεί τα Open Badges ως πιστοποιητικά και διευθύνσεις blockchain για αναγνώριση παραλήπτη. Προκειμένου να εξασφαλίσει και να κρυπτογραφήσει

τα διαπιστευτήρια εκπαίδευσης κάθε πτυχιούχου, κάθε φοιτητής πρέπει να δημιουργήσει και να αποθηκεύσει τα αντίστοιχα δημόσια και ιδιωτικά κλειδιά του Αυτή η προσέγγιση βέβαια θα ήταν ανέφικτη και μη αποτελεσματική, λαμβάνοντας υπόψη την έλλειψη γνώσης των φοιτητών σχετικά με τη τεχνολογία blockchain καθώς και με τα κρυπτογραφικά κλειδιά, δημιουργώντας ένα τεράστιο εμπόδιο για τη μη αποτελεσματική χρήση του. Η εφαρμογή **Blockcerts Wallet** δημιουργήθηκε για την επίλυση αυτού του ζητήματος. Όταν ένας φοιτητής εγκαθιστά την εφαρμογή, δημιουργεί το δικό του μοναδικό ζεύγος κλειδιών, στέλνοντας το αντίστοιχο δημόσιο κλειδί του στο MIT,το οποίο το αποθηκεύει σε ψηφιακή εγγραφή.Το πιστοποιητικό του φοιτητή παράγεται ως **Open Badge** και το ψηφιακό hash του Badge αποθηκεύεται σε ένα δημόσιο blockchain (επί του παρόντος Bitcoin ή Ethereum) και προστίθεται στο Badge μαζί με το αναγνωριστικό της συναλλαγής που περιέχει το hash στο επιλεγμένο blockchain.Με αυτό το τρόπο μπορεί να επαληθευτεί η ημερομηνία έκδοσης κάθε Badge κοιτάζοντας την ημερομηνία του μπλοκ στο blockchain που περιέχει το hash του Badge.Πολλαπλά Badges μπορούν να ασφαλιστούν και εκδοθούν μαζί σε μια συναλλαγή δημιουργώντας ένα δέντρο Merkle με hashes των badges για εξοικονόμηση κόστους και όγκου συναλλαγών. Τέλος το MIT στέλνει το πιστοποιητικό στο φοιτητή, με το δημόσιο κλειδί του εγγεγραμμένο σε αυτό, επιτρέποντας του έτσι να αποδείξει εύκολα την ιδιοκτησία του διπλώματος του με το ιδιωτικό του κλειδί. Επιπλέον, οποιοσδήποτε εργοδότης επιθυμεί μπορεί να ελέγξει το δίπλωμα μέσω μιας πύλης στην οποία μπορεί να φορτώσει το δίπλωμα και το hash του υποψηφίου και να το συγκρίνει με αυτό που είναι αποθηκευμένο στο blockchain.



Εικόνα 12:Διαδικασία εξακρίβωσης του πιστοποιητικού BlockCert



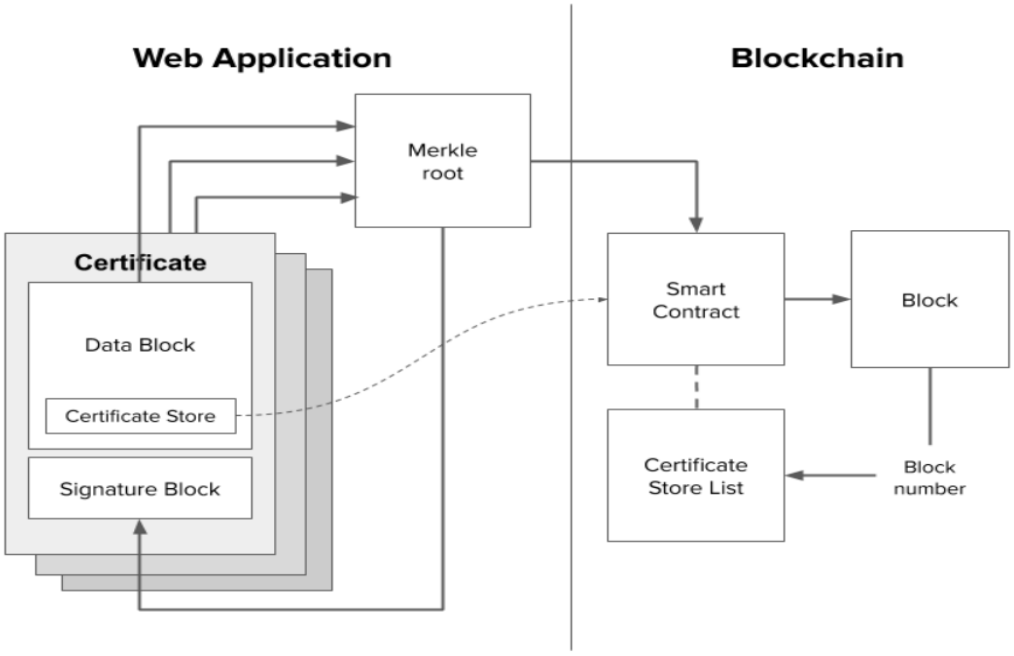
Εικόνα 13:Διαδικασία επαλήθευσης πιστοποιητικού Blockcert

4.3.Ορισμός OpenCert

Το πρότζεκτ OpenCerts παρέχει ένα κοινό πρότυπο για την έκδοση πιστοποιητικών και επαλήθευσης γνησιότητας αυτών των πιστοποιητικών. Υιοθετώντας αυτό το κοινό πρότυπο, στόχος είναι να επιτραπεί στους ανθρώπους που φοιτούν στην Σιγκαπούρη να μπορούν να ανακτήσουν και να έχουν εύκολη πρόσβαση στα ψηφιακά τους πιστοποιητικά από μια μόνο τοποθεσία μέσω του Skills Passport στο MySkillsFuture.Σε κάθε ψηφιακό πιστοποιητικό εκχωρείται μια κρυπτογραφική απόδειξη, η οποία είναι το ψηφιακό δακτυλικό αποτύπωμα του πιστοποιητικού, το οποίο επιτρέπει την ασφαλή επαλήθευση του ψηφιακού πιστοποιητικού. Αυτό το ψηφιακό δακτυλικό αποτύπωμα αποθηκεύεται σε ένα blockchain,ένα αποκεντρωμένο καθολικό.Επειδή το καθολικό είναι αποκεντρωμένο, με πολλαπλά αντίγραφα αποθηκευμένα σε διαφορετικούς διακοσμιτές,οι εγγραφές που έχουν φτιαχτεί πάνω σε αυτό δεν είναι δυνατόν να τροποποιηθούν είτε να καταστραφούν από ένα μόνο άτομο. Το πιστοποιητικό μπορεί εύκολα να επαληθευτεί απευθείας από τους εργοδότες απευθείας μέσω του OpenCerts(opencerts.io) το οποίο θα ελέγξει τα δεδομένα του πιστοποιητικού έναντι του κωδικού του στο blockchain για την εγκυρότητά του και τυχόν σημάδια παραβίασης.Το SkillsFutureSingapore(SSG) διατηρεί το μητρώο αναγνωρισμένων εκδοτών ακαδημαϊκών πιστοποιητικών και πιστοποιητικών δεξιοτήτων. Ο σχεδιασμός των OpenCerts περιγράφεται από τη GovTech ως χτισμένο πάνω στα OpenBadges και τα BlockCerts.Τα πιστοποιητικά έχουν ένα φιλικό προς το χρήστη οπτικό επίπεδο(μορφοποιημένο χρησιμοποιώντας τα πρότυπα της React) και ένα επαληθεύσιμο κρυπτογραφικό επίπεδο που συμμορφώνεται με το μοναδικό σχήμα JSON-LD των OpenCerts.Τα πιστοποιητικά βρίσκονται στο Ethereum blockchain.

4.3.1 Περιγραφή Αρχιτεκτονικής OpenCert

Το σχήμα OpenCerts περιλαμβάνει ένα φόρτο δεδομένων και μια υπογραφή.Ο σχεδιασμός αυτός υποστηρίζει το κατακερματισμό του φόρτου και τη καταγραφή μιας διεύθυνσης έξυπνου συμβολαίου στην υπογραφή. Αυτή η αντιστοιχία μεταξύ του κατακερματισμένου φόρτου και των δεδομένων που είναι γραμμένα σε ένα έξυπνο συμβόλαιο είναι αυτό που καθιστά δυνατή τη σύγκριση ενός πιστοποιητικού με το κατακερματισμό του στο blockchain,για να καθοριστεί εάν έχει παραβιαστεί το διαπιστευτήριο. Οι βιβλιοθήκες του προτύπου OpenCerts υποστηρίζουν τη μαζική επεξεργασία πιστοποιητικών. Καθώς, κάθε πιστοποιητικό φόρτου κατακερματίζεται, οι κατακερματισμοί συνδυάζονται σε ένα Merkle δέντρο(μια δομή δεδομένων στην οποία κάθε κόμβος χωρίς φύλλα είναι κατακερματισμός των αντίστοιχων θυγατρικών κόμβων του).Το Merkle δέντρο χωνεύεται σε μια Merkle ρίζα και αυτό καταγράφεται στο blockchain.Μέχρις στιγμής ο τρόπος που λειτουργούν τα OpenCerts μοιάζει με τον τρόπο λειτουργίας των BlockCerts.Τα OpenCerts χρησιμοποιούν μια αποθήκη πιστοποιητικών σε λίστες και ένα έξυπνο συμβόλαιο που περιέχει λειτουργίες επεξεργασίας και διαχείρισης λιστών.



Εικόνα 14:Δομή OpenCert

Το αποθετήριο των πιστοποιητικών αποτελεί το καθολικό των πιστοποιητικών που εκδίδονται ,ανακαλούνται, και ελέγχονται από ένα συγκεκριμένο ίδρυμα. Ένα ίδρυμα απαιτείται να αναπτύξει τουλάχιστον ένα στιγμιότυπο του έξυπνου συμβολαίου του αποθετηρίου της λίστας

των πιστοποιητικών στο δημόσιο κύριο δίκτυο Ethereum.Αυτό το συμβόλαιο χρησιμοποιείται από την υπηρεσία επαλήθευσης OpenCerts για να επιβεβαιώσει ότι έχουν εκδοθεί πιστοποιητικά,ότι δεν έχουν ανακληθεί και δεν έχουν αλλοιωθεί στη συνέχεια. Κάθε φορά που εκδίδεται μια παρτίδα(batch) πιστοποιητικών, το έξυπνο συμβόλαιο του πιστοποιητικού καταστήματος δημιουργεί μια νέα συναλλαγή Ethereum που καταγράφει τη merkle ρίζα για την παρτίδα.Επίσης,ο αριθμός αποκλεισμού αυτής της συναλλαγής και η merkle ρίζα προσαρτώνται σε μια λίστα που διατηρείται στο αποθετήριο λίστας πιστοποιητικών. Η πρόσβαση σε αυτό το έξυπνο συμβόλαιο είναι public-read(δηλαδή όλοι μπορούν να το διαβάσουν) και owner-write(μόνο αυτός που έχει άδεια μπορεί να γράψει σε αυτό).Η λίστα μπορεί να ελεγχθεί από τον οποιονδήποτε. Ως αποτέλεσμα των παραπάνω , μπορούν να επαληθευτούν πολλαπλά πιστοποιητικά χρησιμοποιώντας μια συναλλαγή blockchain μειώνοντας έτσι το χρόνο επεξεργασίας αλλά και τον όγκο των στοιχείων για επεξεργασία. Τα ιδρύματα έκδοσης πιστοποιητικών παρέχουν σε κάθε παραλήπτη αντίγραφο του πιστοποιήτικού τους, το οποίο διαβιβάζεται ως αρχείο JSON-LD μέσω της διεύθυνσης email της σχολής. Τουλάχιστον μια από τις σχολές περικλείει το πιστοποιητικό σε ένα πακέτο zip με κωδικό πρόσβασης. Με αυτό το τρόπο το ίδρυμα είναι σε θέση να διαβεβαιώσει ότι κάθε φοιτητής λαμβάνει τα σωστά πιστοποιητικά με σχετικά ιδιωτικό τρόπο. Μόλις εκδοθούν τα πιστοποιητικά, τα αρχεία μεταφέρονται στο Skills Future Data Hub όπου φιλοξενούνται μόνιμα και συνδέονται με το διαδικτυακό προφίλ καριέρας ενός ατόμου. Τα αρχεία αυτά δεν είναι κρυπτογραφημένα και οι παραλήπτες ενθαρρύνονται να μοιράζονται τα αρχεία πιστοποιητικών σε απλό κείμενο, για παράδειγμα στέλνοντάς τα μέσω ηλεκτρονικού ταχυδρομείου σε ένα πιθανό εργοδότη.Επίσης,η σελίδα η οποία παρέχεται από τη GovTech μπορεί να διαβάσει μόνο αρχεία πιστοποιητικών απλού κειμένου. Είναι σημαντικό να σημειωθεί ότι οι παραλήπτες δεν αποδέχονται ρητά τα πιστοποιητικά, αφήνοντας ανοιχτή τη δυνατότητα αποποίησης. Το σκεπτικό για τις σχολές στο να εκδίδουν πιστοποιητικά χωρίς διαδικασία αποδοχής είναι ότι οι σχολές στη Σιγκαπούρη διαθέτουν καλά συστήματα και μπορούν να εμπιστευθούν την έκδοση πιστοποιητικών χωρίς σφάλματα. Παρόλο που τα εκδοθέντα πιστοποιητικά εμφανίζονται αυτόματα στο προφίλ καριέρας ενός ατόμου ,ο παραλήπτης μπορεί να το κρύψει εάν το επιθυμεί. Με αυτό το σύστημα που παρέχεται από τα OpenCerts δίνεται η δυνατότητα στον αιτούντα ή αλλιώς παραλήπτη του πιστοποιητικού δυνατότητα να αποκρύψει κάποια στοιχεία του πιστοποιητικού ώστε να μην είναι εμφανή σε άλλους,χωρίς όμως αυτό να επηρεάζει το κατακερματισμό του πιστοποιητικού συνεχίζοντας έτσι να είναι έγκυρο. Τα στοιχεία αυτά είναι εμφανή στο JSON του πιστοποιητικού στην ενότητα ιδιωτικότητα (privacy). Εάν ένας παραλήπτης θεωρήσει ότι οι πληροφορίες στο πιστοποιητικό είναι εσφαλμένες, θα επικοινωνήσει με τον εκδότη τους μέσω email και θα ζητήσει την εκ νέου έκδοση του

πιστοποιητικού. Η αξία ενός συστήματος που εκδίδει επαληθεύσιμα πιστοποιητικά καθορίζεται σε μεγάλο βαθμό από το κατά πόσον αυτά τα πιστοποιητικά βασίζονται σε καταναλωτές, όπως εργοδότες και μεταπτυχιακές σχολές..Με τα OpenCerts, δίνεται στον παραλήπτη το ακατέργαστο αρχείο JSON και αυτός ενθαρρύνεται να το διαβιβάσει στους ενδιαφερόμενους.Τέλος,τίθεται ένα πολύ λογικό ερώτημα εάν οποιοσδήποτε λαμβάνει τέτοια δεδομένα :α)ξέρει ποιο σκοπό εκπληρώνουν και β)γνωρίζει πως να επαληθεύσει την αυθεντικότητα τους.

4.3.2 Περιορισμοί των OpenCert

Θεσμική συγκέντρωση

- Το GovTech και το SkillsFuture ως κυβερνητικοί φορείς είναι και οι δύο συγκεντρωτικοί.
- Για να διασφαλιστεί ότι οι εκδότες είναι αξιόπιστοι, υπάρψει ένα Μητρώο, αλλά είναι ανοικτό μόνο σε διαπιστευμένα εκπαιδευτικά ιδρύματα στη Σιγκαπούρη, περιορίζοντας σημαντικά τη γενική εφαρμογή.
- Η αρχιτεκτονική του μητρώου και του αποθετηρίου λίστας πιστοποιητικών, επιτρέπει στην κυβέρνηση της Σιγκαπούρης να παρακολουθεί κάθε εκδότη και κάθε συναλλαγή πιστοποιητικού. Ως αποτέλεσμα αυτού οποιοσδήποτε εκδότης μπορεί να λογοκριθεί για κάποιον έγκυρο λόγο ή χωρίς κανένα λόγο.
- Η πρόσβαση στο σύστημα αποθήκευσης βασίζεται σε ένα εθνικό σύστημα ταυτότητας που δεν είναι προσβάσιμο σε ξένους φοιτητές και αποφοίτους.

Αδυναμία διαχείρισης ταυτότητας

- Οι παραλήπτες δεν απαιτείται να αποδεχτούν τα πιστοποιητικά τους, δημιουργώντας έτσι ευκαιρίες για απόρριψη (π.χ. ο παραλήπτης λέει ότι δεν παρατήρησε ένα προφανές σφάλμα).
- Τα πιστοποιητικά βασίζονται μόνο στα ονόματα του εκδότη και του παραλήπτη. Αυτά σίγουρα δεν είναι μοναδικά αναγνωριστικά και (εκτός από τον μηχανισμό μητρώου εκδότη) θα μπορούσαν εύκολα να πλαστογραφηθούν
- Δεν υπάρχει μηχανισμός που να διασφαλίζει ότι ο κάτοχος διαπιστευτηρίου είναι στην πραγματικότητα ο παραλήπτης που αναφέρεται στο διαπιστευτήριο.

Κακή προστασία της ιδιωτικής ζωής

- Τα πιστοποιητικά αποθηκεύονται ως μη κρυπτογραφημένα αρχεία JSON και οι παραλήπτες ενθαρρύνονται να τα μοιράζονται σε μορφή απλού κειμένου. Η επαλήθευση απαιτεί επίσης πιστοποιητικά απλού κειμένου. Αυτό περιορίζει τον τύπο πληροφοριών που μπορούν να πιστοποιηθούν χωρίς να παραβιάζεται το απόρρητο του παραλήπτη.

Περιορισμένη γνωστοποίηση

- Στην ιδανική περίπτωση όπου κάποιος θα ήθελε να καταγραφεί το αναγνωριστικό συναλλαγής blockchain στο μπλοκ υπογραφής JSON-LD και ενδεχομένως να εμφανίζεται στα πιστοποιητικά,η εφαρμογή του αποθετηρίου πιστοποιητικών(Certificate Store) αποκρύπτει το αναγνωριστικό συναλλαγής blockchain.

4.4 Ευρωπαϊκή Συνεργασία Blockchain(EBSI)

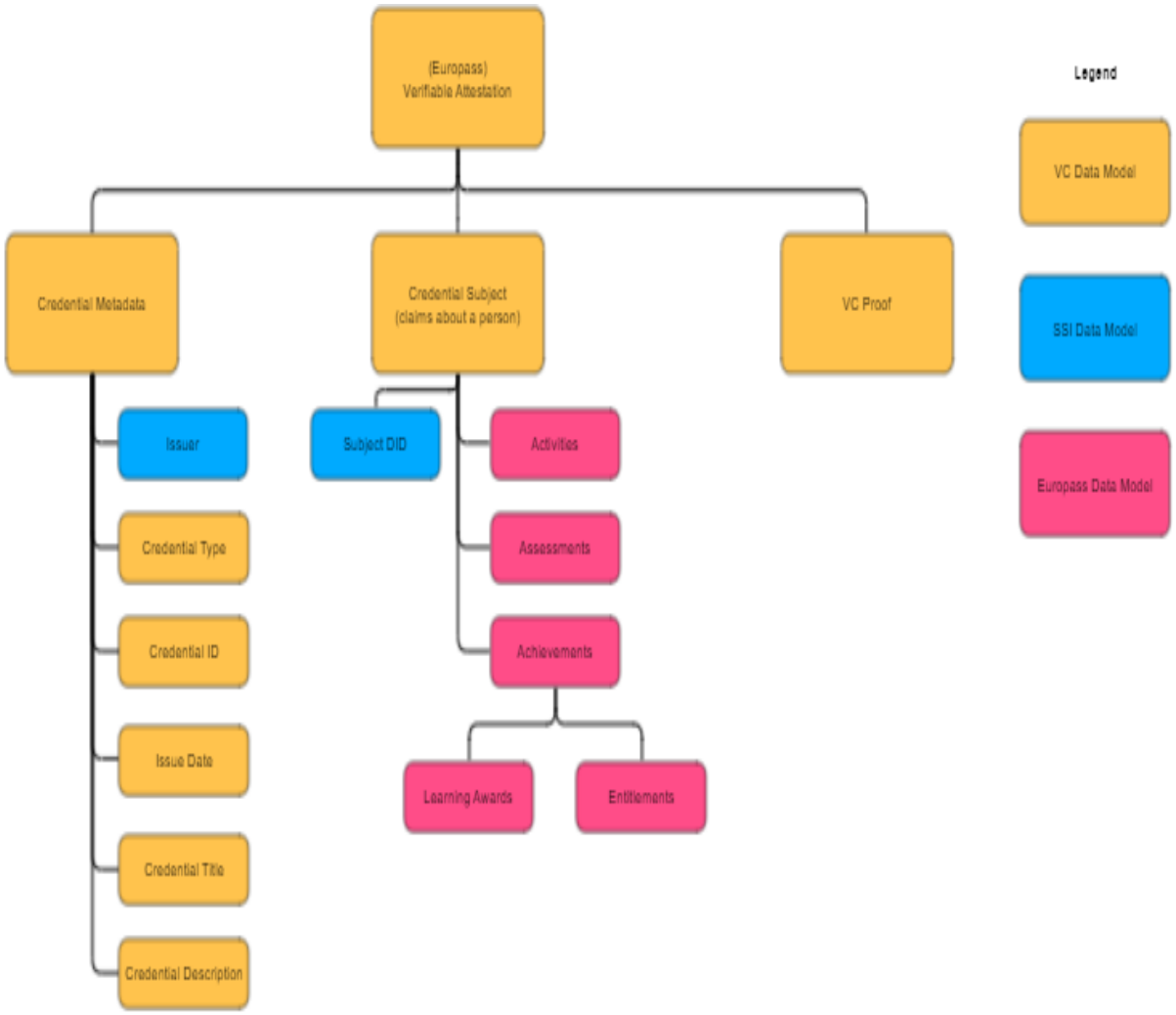
Η ευρωπαϊκή υποδομή υπηρεσιών blockchain(EBSI) είναι ένα δίκτυο κατανεμημένων κόμβων σε όλη την Ευρώπη που παρέχει διασυνοριακές δημόσιες υπηρεσίες. Η τεχνολογία blockchain ενισχύει ουσιαστικά τον τρόπο αλληλεπίδρασης των πολιτών, των κυβερνήσεων και των επιχειρήσεων στην Ευρώπη. Το EBSI είναι το αποτέλεσμα της Ευρωπαϊκής Συνεργασίας blockchain,μιας Διακήρυξης που υπεγράφη μεταξύ 27 κρατών μελών, του Λιχτενστάιν και της Νορβηγίας για τη συνεργασία στην παροχή διασυνοριακών ψηφιακών δημόσιων υπηρεσιών, με τα υψηλότερα πρότυπα ασφάλειας και ιδιωτικότητας.Το EBSI είναι ένα από τα δομικά στοιχεία της CEF,που παρέχει δωρεάν επαναχρησιμοποιούμενο λογισμικό, προδιαγραφές και υπηρεσίες για να υποστηρίξει την υιοθέτηση του από δημόσια όργανα της Ευρωπαϊκής Ένωσης, τις επιχειρήσεις και τους πολίτες.

4.4.1 Περιγραφή της αρχιτεκτονικής της Ευρωπαϊκής Συνεργασίας(EBSI)

Το EBSI δημιουργεί μια υποδομή blockchain με βάση κόμβους που φιλοξενούνται από τα κράτη μέλη. Ένα βασικό στοιχείο αυτής της πρωτοβουλίας είναι η ανάγκη ύπαρξης ενός πλαισίου ταυτότητας όχι μόνο για την υποδομή αλλά και που να παρέχει τη δυνατότητα προσθήκης αποκεντρωμένης ταυτότητας(DID) σε πολλές διαδικασίες. Ενώ υπάρχει μεγάλο ενδιαφέρον στα κράτη μέλη και τους δημόσιους και ιδιωτικούς φορείς γενικά, έχει καταστεί

σαφές ότι οι πιο ενδιαφέρουσες περιπτώσεις για νέες προσεγγίσεις ταυτότητας βρίσκονται σε διασυνοριακές καταστάσεις. Το EBSI προσπαθεί να εφαρμόσει και να επιταχύνει ένα επίπεδο διασυνοριακής διαλειτουργικότητας που μπορεί να χρησιμοποιηθεί σε πολλές περιπτώσεις για να διευκολύνει τις αλληλεπιδράσεις, έτσι ώστε τα κράτη μέλη να μην χρειάζεται να χτίσουν το δικό τους πλαίσιο αυτοκυρίαρχης ταυτότητας (SSI) αλλά να έχουν ένα έτοιμο προς χρήση σε ευρωπαϊκό επίπεδο. Η αυτοκυρίαρχη ταυτότητα πρέπει να επιτρέπει στους χρήστες να παρέχουν αξιώσεις για τον εαυτό τους,οι οποίες θα μοπορούσαν να περιλαμβάνουν προσωπικά δεδομένα ή χαρακτηριστικά,είτε ακόμη και να περιλαμβάνουν πληροφορίες που ισχυρίζονται άλλοι.Το EBSI δημιουργεί τα βασικά στοιχεία, αλλά επενδύει επίσης στην ανάπτυξη τεχνικών προδιαγραφών, έτσι ώστε οι κυβερνήσεις να μπορούν να εφαρμόσουν εύκολα το οικοσύστημα αυτό αυτοκυρίαρχης ταυτότητας.Επίσης, προσπαθεί να εμπλέξει περισσότερες κυβερνήσεις και κράτη μέλη σε αυτά τα οικοσυστήματα SSI για να δει πώς μπορεί να σχετίζεται με το υπάρχον πλαίσιο εμπιστοσύνης. Το EBSI θέλει το SSI να μην είναι μόνο για αυτοανακηρυγμένες πληροφορίες αλλά κάτι αξιόπιστο που να μπορεί να χρησιμοποιηθεί σε αλληλεπιδράσεις με τράπεζες και κυβερνητικές υπηρεσίες. Εδώ το eIDAS έχει κάτι ισχυρό, και έτσι το EBSI προσπαθεί να συνδυάσει αυτές τις πτυχές.Με τον όρο eIDAS εννοούμε τις υπηρεσίες ηλεκτρονικής αναγνώρισης και εμπιστοσύνης για τις ηλεκτρονικές συνναλαγές.Αυτό που κάνει το eIDAS είναι ότι διασφαλίζει τη νομική ισχύ των ηλεκτρονικών εγγράφων και υπηρεσιών διασυνοριακής εμπιστοσύνης όπως ηλεκτρονικές υπογραφές και σφραγίδες.Για να κάνει διαθέσιμο το ESBI το eIDAS δημιούργησε τη γέφυρα eIDAS,έχει κυκλοφορήσει μια πρώτη έκδοση που λειτουργεί πιλοτικά και στο μέλλον ελπίζει να δημιουργήσει μια δεύτερη έκδοση που να είναι πιο έτοιμη για πιλότος. Αφενός το SSI και το blockchain βασίζονται σε τεχνολογίες και πράγματα όπως οι ηλεκτρονικές υπογραφές που είναι εξαιρετικά σταθερές και μπορούν να χρησιμοποιηθούν για να παρέχουν εμπιστοσύνη, από την άλλη το eIDAS είναι μια ευκαιρία για να αναπτυχθεί το SSI σε ένα πλαίσιο διασυνοριακών αλληλεπιδράσεων. Όσον αφορά τα πρότυπα που χρησιμοποιεί ,το EBSI δεν θέλει να εφεύρει κάτι συγκεκριμένο για την Ευρώπη,έτσι παρακολουθεί στενά την ανάπτυξη αναδυόμενων παγκόσμιων προτύπων όπως αυτά που προέρχονται από το W3C. Το EBSI αλληλεπιδρά επίσης σε ότι αφορά το οικοσύστημα και με άλλους ενδιαφερόμενους,όπως για παράδειγμα την ομάδα εργασίας INATBA για την ταυτότητα.Τα διπλώματα στο EBSI μοντελοποιούνται ως W3C επαληθεύσιμα διπιστευτήρια(VC).Για την ενίσχυση της συμβατότητας με ήδη υπάρχουσες πρωτοβουλίες χρησιμοποιεί την επέκταση Europass η οποία ενσωματώνεται στη δομή των διαπιστευτηρίων.Τα διαπιστευτήρια εκδίδονται σε μορφή JSON-LD,ένα παράδειγμα της δομής αυτού του πιστοποιητικου καθώς και τη μορφής του απεικονίζεται στις εικόνες παρακάτω. Με

το που εγκριθεί το πιστοποιητικό ο κατακερματισμός του αποθηκεύεται στην αλυσίδα blockchain.



Εικόνα 15:Δομή Europass πιστοποιητικού

```
{
    "@context": ["https://www.w3.org/2018/credentials/v1", "http://EBSI-WEBSITE.EU/schemas/vc/2019/v1
    "id": "CREDENTIAL-ID",
    "type": ["VerifiableCredential", "EuropassCredential"],

    "issuer": {
        "id": "ISSUER-DID",
        "organization": {
            "id": "LEGAL ORGANISATION-ID",
            "legalIdentifier": "LEGAL IDENTIFIER",
            "vatIdentifier": "VAT ID",
            "taxIdentifier": "TAX ID",
            "preferredName": "LEGAL PREFERRED NAME",
            "alternativeName": "LEGAL ALTERNATIVE NAME",
            "homePage": "ORGANISATION HOMEPAGE",
            "escoOrganizationType": "ESCO TYPE",
            "siteLocation": "ORGANISATION LOCATION",
            "hasAccreditation": {
                "targetFramework": "Europass Accreditation Database",
                "targetResource": "https://accreditation.europass.eu/12341455"
            },

            "issuanceDate": "2020-01-01:00:00Z",
            "expirationDate": null, // Not applicable

            "title": [{
                "lang": "en_GB",
                "contentType": "text/plain",
                "text": "VC TITLE"
            }],
            "description": [{
                "lang": "en_GB",
                "contentType": "text/plain",
                "text": "SHORT VC DESCRIPTION"
            }],

            "credentialSubject": {
                "id": "did:ebsi:SUBJECT-DID",

                "achievements": [{
                    "id": "1cb8ef7e-0024-46f0-9555-61fb4280d122/ach1",
```

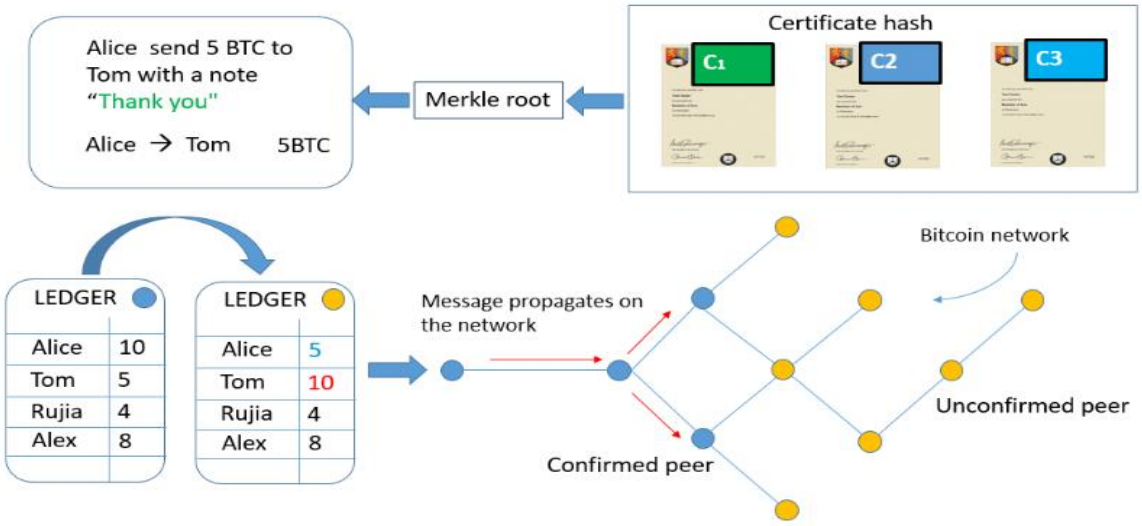
Εικόνα 16:Δομή πιστοποιητικού στο EBSI σε μορφή JSON-LD

Τέλος, το ESBI δημιουργήσει μια κοινότητα χρηστών έτσι ώστε όχι μόνο τα κράτη μέλη αλλά και ο ιδιωτικός τομέας, να μπορούν να δουν τι συμβαίνει και τι είδους υπηρεσίες παρέχει το EBSI. Στα επόμενα στάδια, το EBSI θα ξεκινήσει πιλότους για να δει πώς μπορεί να χρησιμοποιηθεί από τα κράτη μέλη και τους εταίρους τους. Αυτή τη στιγμή στο επίκεντρο είναι οι δημόσιες υπηρεσίες, αλλά στο μέλλον το EBSI θα εξελιχθεί σε κάτι που θα αλληλεπιδρά και με τον ιδιωτικό τομέα.

4.5 BTCeRT

Το BTCeRT επικυρώνει ακαδημαϊκά πιστοποιητικά μέσω μιας ψηφιακής απόδειξης που επιτρέπει την άμεση επαλήθευση τους από τρίτους.Το BTCeRT εμπνεύστηκε από το έργο ανοικτού κώδικα Blockcerts.Όπως το Blockcerts έτσι και το BTCeRT εκδίδει ψηφιακά διαπιστευτήρια στέλνοντας μια συναλλαγή Bitcoin από το ίδρυμα ανάθεσης στο παραλήπτη/κάτοχο του πιστοποιητικού.Όπως απεικονίζεται στη παρακάτω εικόνα,ένα σύνολο

τιμών κατακερματισμού πιστοποιητικών θα επισυνάπτεται στη συναλλαγή Bitcoin όταν η Alice πλήρωσε 5 BTC στον Tom.Με τη σχεδίαση του BTCeRT,η Alice αντικαθιστά τη σημείωση «ευχαριστώ» με τη Merkle ρίζα που αντιστοιχεί σε μια ομάδα πιστοποιητικών.Στην συνέχεια το BTCeRT επιτρέπει σε έναν ανεξάρτητο επαληθευτή να ελέγξει την αυθεντικότητα τέτοιων πιστοποιητικών,ανακτώντας τη τιμή κατακερματισμού από το Bitcoin blockchain και συγκρίνοντάς το με τη τοπική απόδειξη.

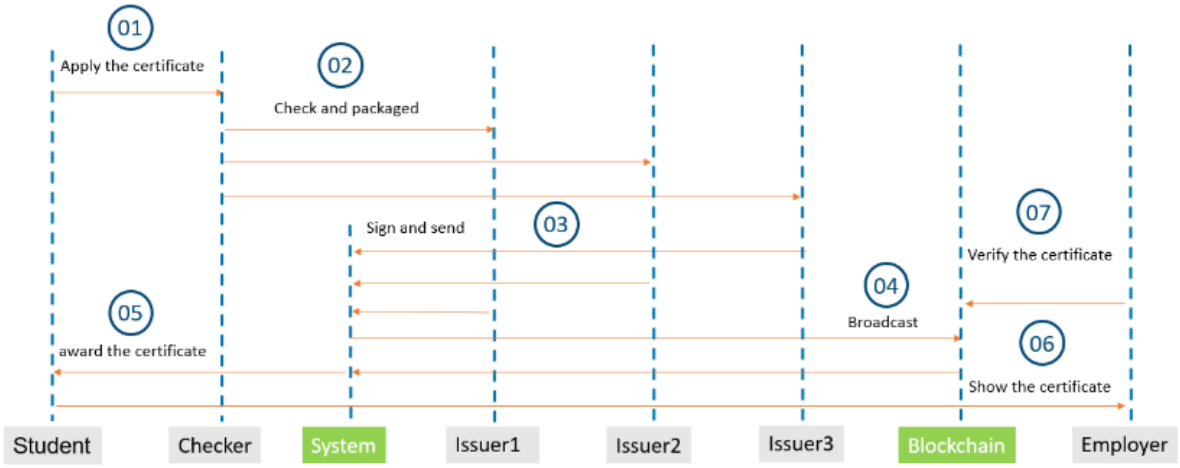


Εικόνα 17:Μηχανισμός λειτουργίας BTCeRT

Το BTCeRT χρησιμοποιεί επιπλέον κρυπτογραφικές τεχνικές για να βελτιώσει την ανθεκτικότητα και τη διαθεσιμότητα της λειτουργίας έκδοσης διαπιστευτηρίων. Το BTCeRT χρησιμοποιεί πολλαπλές υπογραφές για να βελτιώσει την ασφάλεια της έκδοσης ψηφιακών διαπιστευτηρίων,αλλά και προσθέτει ένα μηχανισμό ανάκλησης που βασίζεται στη διεύθυνση BTC για την ανάκληση ενός πιστοποιητικού πιο αξιόπιστα και την εγκαθίδρυση μιας ασφαλούς ομόσπονδης ταυτότητας με σκοπό την επαλήθευση της ταυτότητας του αναθέτοντος ιδρύματος.Τα βασικά κρυπτογραφικά μέρη έχουν αναπτυχθεί σε JavaScript,η οποία καθιστά δυνατή τη διαχείριση όλων των ευαίσθητων δεδομένων από τη πλευρά του πελάτη(πρόγραμμα περιήγησης).Με άλλα λόγια το BTCert δεν μεταφέρει ποτέ ούτε αποθηκεύει ευαίσθητα δεδομένα,όπως ιδιωτικά κλειδιά από τη μεριά του διακομιστή.

4.5.1 Περιγραφή της ροής εργασίας του BTCeRT

Για να γίνει καλύτερα κατανοητό το BTCeRT,περιγράφεται σε ένα μοντέλο της ροής εργασίας από τέσσερις πρωταρχικούς ρόλους,που περιλαμβάνει μαθητή,ελεγκτή,εκδότη,σύστημα και εργοδότη.Η ροή εργασίας για το BTCeRT φαίνεται στη παρακάτω εικόνα.

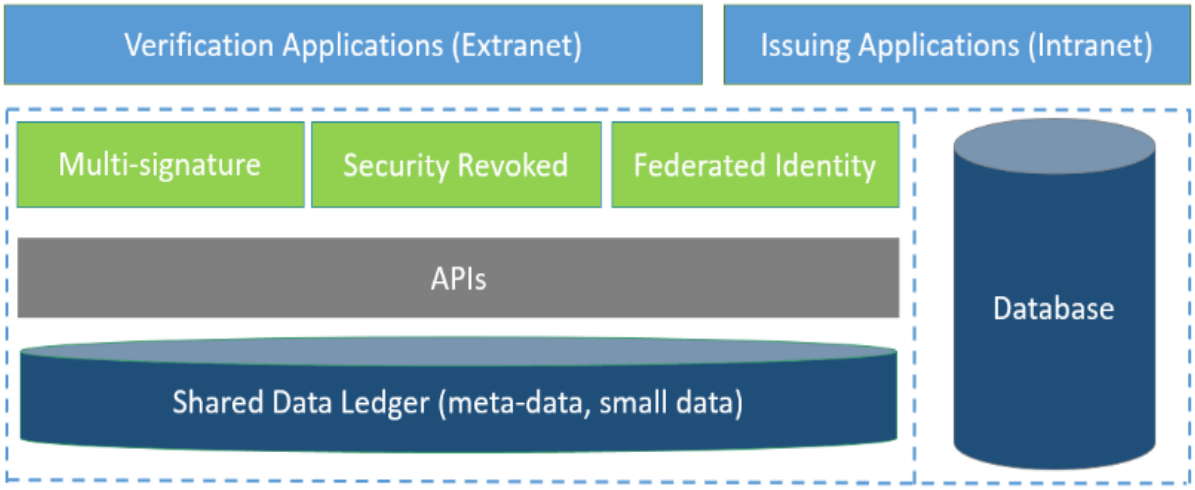


Εικόνα 18:Ροή εργασίας BTCeRT

Πρώτον, ο φοιτητής υποβάλλει αίτηση στο πανεπιστήμιο για πιστοποιητικό,και ο φορέας πιστοποίησης ελέγχει τις πληροφορίες του φοιτητή και συγχωνεύει το πιστοποιητικό με μια συναλλαγή Bitcoin μόλις εγκριθεί.Στη συνέχεια, ένα δεδομένο κατώφλι των μελών της επιτροπής έκδοσης το υπογράφει με τα ιδιωτικά του κλειδιά.Μετά από αυτό το σύστημα μεταδίδει τη συναλλαγή που περιέχει τη Merkle ρίζα όλων των πιστοποιητικών.Εν συνέχεια,ο φοιτητής λαμβάνει ένα πιστοποιητικό σε δομή JSON μόλις επιβεβαιωθεί η συναλλαγή και προστεθεί στο Bitcoin blockchain.Στο επόμενο στάδιο,ο φοιτητής παρέχει το πιστοποιητικό με δομή JSON στον επαληθευτή(π.χ. μια εταιρία στην οποία υποβάλλει αίτηση για εργασία).Τέλος η εταιρία επαληθεύει το πιστοποιητικό μέσω της πρόσβασης στο Blockchain και ελέγχει το κωδικό επιβεβαίωσης για να επαληθεύσει την ταυτότητα του ιδρύματος.

4.5.2 Περιγραφή της αρχιτεκτονικής του BTCeRT

Το σύστημα BTCeRT αποτελείται από τέσσερα στοιχεία:την εφαρμογή επαλήθευσης συμπεριλαμβανομένης της ομόσπονδης ταυτότητας,την εφαρμογή έκδοσης που περιλαμβάνει ανάκληση βάσει πολλαπλών υπογραφών και BCT-address blockchain, και τη τοπική βάση δεδομένων που χρησιμοποιείται η MongoDB



Εικόνα 19:Αρχιτεκοτνική BTCeRT

Η αίτηση έκδοσης είναι υπεύθυνη για την κύρια επιχειρηματική λογική,συμπεριλαμβανομένων της αίτησης,της εξέτασης,της υπογραφής και της έκδοσης των διαπιστευτηρίων που πιστοποιούν την ύπαρξη του ακαδημαϊκού πιστοποιητικού.Η εφαρμογή έκδοσης έχει σχεδιαστεί για να συγχωνεύσει το κατακερματισμό του πιστοποιητικού με ένα Merkle δέντρο και να στείλει τη Merkle ρίζα στο blockchain Bitcoin.Επίσης, η εφαρμογή έκδοσης ασχολείται με την ανάκληση πιστοποιητικών.Οι κύριες συνιστώσες στην εφαρμογή έκδοσης είναι:

- Λειτουργία σύνδεσης
- Έλεγχος προνομίων
- Η διαδικασία έγκρισης(φοιτητής->>ελεγκτής->>επιβλέπων->>διοικητικό προσωπικό->>επικεφαλής του σχολείου)
- Λειτουργία πολλαπλών υπογραφών
- Έλεγχος του πιστοποιητικού
- Προβολή του δημοσιευμένου πιστοποιητικού
- Προβολή του υπογεγραμμένου πιστοποιητικού
- Προβολή του πιστοποιητικού έτοιμο για υπογραφή
- Ανάκληση του πιστοποιητικού κατά παρτίδες
- Σελίδα διαχείρισης για τη διαχείριση του χρήστη,τα προνόμια και το πιστοποιητικό

.Η αίτηση επαλήθευσης επικεντρώνεται στον έλεγχο της γνησιότητας και της ακεραιότητας των πιστοποιητικών που έχουν εκδοθεί .Περιλαμβάνει δύο βασικά στοιχεία:μια σελίδα που βασίζεται στο κινητό,μια εφαρμογή που βασίζεται σε Android και οι δύο χρησιμοποιούν τον ίδιο μηχανισμό:ανάκτηση του μηνύματος συναλλαγής μέσω του API blockchain και σύγκριση του μηνύματος συναλλαγής με τα δεδομένα επαλήθευσης από την ψηφιακή

απόδειξη.Ο μηχανισμός μπορεί να περιγραφεί εν συντομία με τον ακόλουθο τρόπο:έλεγχος του κωδικού ελέγχου ταυτότητας(επιβεβαίωσης),έλεγχος του κατακερματισμού με τοπικό πιστοποιητικό,επιβεβαίωση του κατακερματισμού στο Merkle δέντρο,εξέταση της Merkle ρίζας στο blockchain,επαλήθευση εάν το πιστοποιητικό έχει ανακληθεί,επικύρωση της ημερομηνίας λήξης του πιστοποιητικού.Επίσης,για την ευκολία κοινοποίησης των πιστοποιητικών,η εφαρμογή που βασίζεται στο Android επιτρέπει την επαλήθευση σαρώνοντας κατευθείαν τον κωδικό QR.Οι κύριες συνιστώσες για την εφαρμογή επαλήθευσης είναι οι εξής:

- Ανέβασμα των PDF/JSON αρχείων / σκανάρισμα του QR κωδικού
- Υπολογίζουμε το κατακερματισμό για το PDF αρχείο
- Η αλληλεπίδραση με το blockchain API
- Διαχείριση ελέγχου ταυτότητας: τη σχέση της διεύθυνσης έκδοσης με τη σχολή
- Η λογική της επαλήθευσης:

Κατά της διαδικασία της επαλήθευσης ελέγχονται η τιμή κατακερματισμού στο πιστοποιητικό(για να ελεγχθεί εάν έχει γίνει κάποια παραβίαση του πιστοποιητικού), εάν η τιμή του κατακερματισμού βρίσκεται στο Merkle δέντρο και εάν η τιμή κατακερματισμού της ρίζας του Merkle δέντρου βρίσκεται στο blockchain για επιβεβαίωση,η εγκυρότητα του πιστοποιητικού(για να αποφευχθεί η ανάκληση του πιστοποιητικού) και τέλος η έγκυρη ημερομηνία του πιστοποιητικού (για να αποφευχθεί ληγμένο πιστοποιητικό).Το blockchain λειτουργεί ως υποδομή εμπιστοσύνης αλλά και ως κατανεμημένη βάση δεδομένων για την αποθήκευση των δεδομένων ελέγχου ταυτότητας.Συνήθως, τα δεδομένα ελέγχου επιβεβαίωσης αποτελούνται από τη Merkle ρίζα που δημιουργείται χρησιμοποιώντας κατακερματισμένα δεδομένα από πολλές δεκάδες πιστοποιητικών.Η MongoDB χρησιμοποιείται ως τοπική βάση δεδομένων ,καθώς η MongoDB μπορεί να διαχειριστεί με επιτυχία πιστοποιητικά που στηρίζονται σε φορμάτ JSON,παρέχοντας ταυτόχρονα υψηλή διαθεσιμότητα και επεκτασιμότητα.

4.6 SmartCert

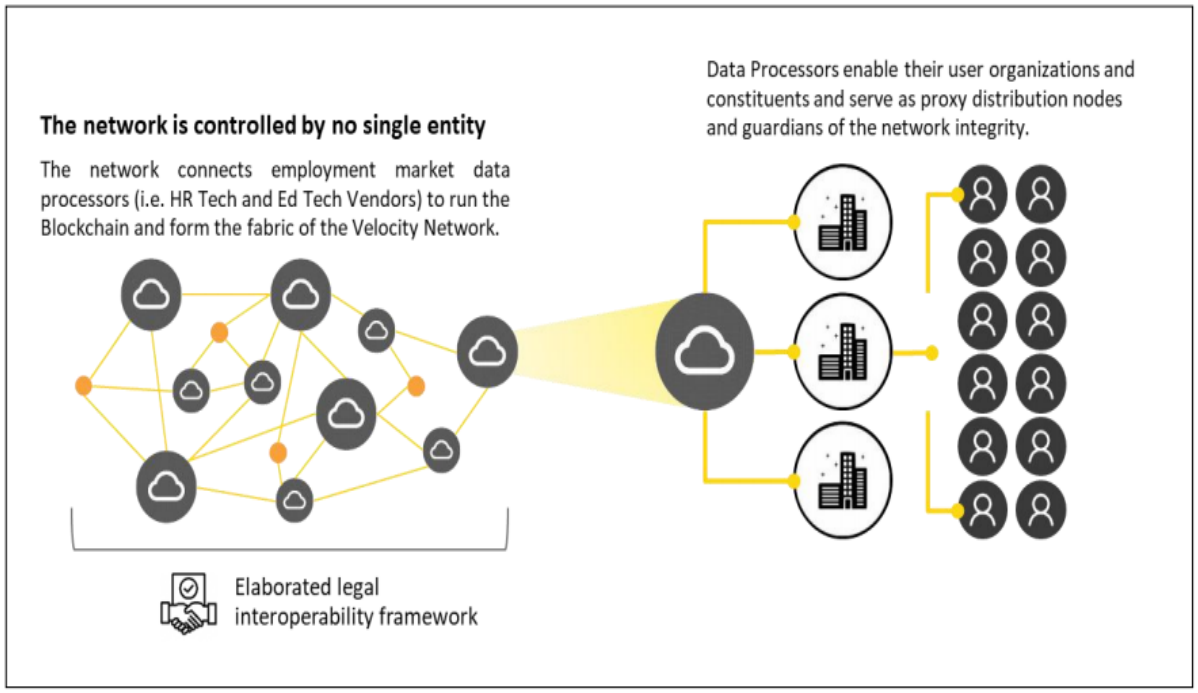
Το SmartCert είναι μια πλατφόρμα επαλήθευσης πιστοποιητικών βασισμένη στη τεχνολογία blockchain.Το SmartCert αναπτύχθηκε για να εγκαθιδρύσει την αυθεντικότητα των ακαδημαϊκών πιστοποιητικών σε ένα blockchain και να ξεπεράσει έτσι το πρόβλημα των

πλαστών πιστοποιητικών.Το SmartCert κάνει χρήση της κρυπτογραφικής υπογραφής των εκπαιδευτικών πιστοποιητικών για να παρέχει διαφάνεια στην περίπτωση πρόσληψης.Ο φοιτητής είναι σε θέση να μοιραστεί το κατακερματισμό(hash) του με τον υποψήφιο εργοδότη για επαλήθευση του πιστοποιητικού του.Ωστόσο,μπορεί να είναι δύσκολο για έναν νόμιμο χρήστη να αποκτήσει πρόσβαση σε αυτό επειδή ο υπολογιστής που έχει πρόσβαση σε αυτά τα δεδομένα μπορεί να έχει δεχθεί επίθεση από εισβολέα.Ένα άλλο ζήτημα στην εφαρμογή SmartCert είναι ότι η κρυπτογραφία που χρησιμοποιείται δεν εξασφαλίζει την ασφάλεια των δεδομένων και για αυτό το λόγο θεμελιώδες μέτρα ασφαλείας πρέπει να εφαρμοστούν στο μέλλον για τη προστασία από τις απειλές για την εξασφάλιση της ιδιωτικότητας,παράλληλα όμως τα κρυπτογραφικά ασφαλή πιστοποιητικά στο SmartCert αποτρέπουν την εύκολη πλαστογράφηση των πιστοποιητικών.Τέλος,είναι σημαντικό η συγκεκριμένη πρωτοβουλία να βελτιώσει τα μέτρα ασφαλείας της ώστε να γίνει πιο ασφαλή η χρήση της.

4.7 Velocity Network

Το Velocity Network είναι ένα βασισμένο σε blockchain, ελεγμένο βοηθητικό στρώμα ανταλλαγής διαπιστευτηρίων ανοικτού κώδικα. Το Velocity με τα βασικά του στοιχεία και τη μηχανική των συμβόλων που διαθέτει,παρέχει τυποποιημένα πρωτόκολλα επικοινωνίας, διακυβέρνησης, ράγες συμμόρφωσης και πληρωμής που επιτρέπουν αξιόπιστη, ιδιωτική και ασφαλή ανταλλαγή διαπιστευτηρίων σταδιοδρομίας μεταξύ ατόμων και οργανώσεων.Αυτό το βοηθητικό στρώμα επιτρέπει στους προμηθευτές HR και Ed Tech,τις αγορές εργασίας, τις ελεύθερες επαγγελματικές πλατφόρμες,στους παρόχους στελέχωσης και πρόσληψης, και στους επεξεργαστές ιστορικού και αξιολόγησης να παρέχουν στα συστατικά τους την ικανότητα έκδοσης κοινοποίησης και επαλήθευσης διαπιστευτηρίων σταδιοδρομίας,να αναπτύξουν περιπτώσεις χρήσης προστιθέμενης αξίας καθώς και καινοτόμες εφαρμογές. Τα άτομα μπορούν να μετατρέπουν τα επιτεύγματα σταδιοδρομίας τους σε ψηφιακά διαπιστευτήρια τα οποία θα είναι επαληθεύσιμα,ασφαλή και δημόσια,θα μπορούν να τα κατέχουν, και να τα χρησιμοποιούν για πρόσβαση σε καλύτερες ευκαιρίες. Ταυτόχρονα, εργοδότες εκπαιδευτικά ιδρύματα και άλλα ενδιαφερόμενα μέρη θα μπορούν να βασίζονται σε αξιόπιστα, αμετάβλητα και επαληθεύσιμα δεδομένα αιτούντων υποψηφίων,υπαλλήλων και φοιτητών, απρόσκοπτα,αποδοτικά και οικονομικά εξαλείφοντας τους κινδύνους πρόσληψης, και ενισχύοντας έτσι τη παραγωγικότητα.Το Velocity θα έχει θετικό αντίκτυπο τόσο στους υπαλλήλους όσο και στους εργοδότες, καθώς τα άτομα έχουν τη δυνατότητα να διατηρούν και

να ελέγχουν την πρόσβαση σε κατανοητά, αξιόπιστα αρχεία για την εκπαίδευσή, τις δεξιότητες καθώς και την κατάρτιση τους αλλά και σε σχετιζόμενα με τη καριέρα τους δεδομένα. Με το ίδιο διακριτικό εφαρμόζοντας analytics και τεχνητή νοημοσύνη στα δεδομένα οι οργανισμοί θα είναι σε θέση να ταιριάξουν άτομα με ρόλους πολύ πιο αποτελεσματικά και με ακρίβεια, με δραστηριότητες μάθησης, εκπαίδευσης και ανάπτυξης και να σχεδιάσουν ειδικές δραστηριότητες διαχείρισης και διατήρησης ταλέντων, το οποίο με τη σειρά του θα προσφέρει την απαραίτητη αύξηση στη παραγωγικότητα, η οποία είναι χαμηλότερη σε σχέση με παλαιότερα έτη παρά τις τεράστιες τεχνολογικές εξελίξεις.Το Velocity εφαρμόζεται ως μια δημόσια υπηρεσία πάνω από ένα δίκτυο blockchain με άδεια που εκτελεί το κατανεμημένο καθολικό που είναι κοινόχρηστο, αναπαράγεται και συγχρονίζεται μεταξύ των μελών ενός αποκεντρωμένου δικτύου(κόμβοι).Επίσης,υπάρχει ένα κοινό βοηθητικό πρόγραμμα που επιτρέπει την αυτόνομη ταυτότητα σταδιοδρομίας στο διαδίκτυο, επιτρέποντας στα άτομα να συλλέγουν, να κρατούν και να επιλέγουν ποια επαληθεύσιμα διαπιστευτήρια θέλουν να μοιράζονται με τα ενδιαφερόμενα μέλη.Κάθε εγγραφή στο δίκτυο έχει χρονική σήμανση και μοναδική κρυπτογραφική υπογραφή καθιστώντας έτσι το καθολικό ένα ελεγχόμενο και αμετάβλητο ιστορικό της καριέρας του χρήστη. Οι κόμβοι επικοινωνούν μεταξύ τους για να επιτύχουν ομοφωνία σχετικά με τα περιεχόμενα του καθολικού και δεν απαιτούν κάποια κεντρική αρχή συντονισμού και επικύρωσης των συναλλαγών. Οι αλγόριθμοι συναίνεσης(ομοφωνίας) διασφαλίζουν ότι τα κοινόχρηστα βιβλία είναι ακριβή αντίγραφα και μειώνουν τον κίνδυνο των δόλιων συναλλαγών. Το αποκεντρωμένο P2P δίκτυο αποτρέπει οποιοδήποτε μεμονωμένο συμμετέχων ή ομάδα συμμετεχόντων από τον έλεγχο της υποκείμενης υποδομής ή την υπονόμευση του συνολικού συστήματος. Οι συμμετέχοντες στο δίκτυο είναι όλοι ίσοι, ακολουθώντας πιστά τα ίδια πρωτόκολλα. Το δίκτυο δεν ανήκει σε κανέναν και διευθύνεται από τα μέλη του..Το Velocity δίκτυο κυβερνάται από το ίδρυμα Velocity,μια συνεταιριστική μη κερδοσκοπική οργάνωση.Η οργάνωση αυτή δημιουργήθηκε για να:1)διέπει τη χρήση του δίκτυου από τα εμπλεκόμενα μέρη,2)χτίζει συνεχώς το βιβλίο κανόνων,3)υποστηρίζει ένα κοινό πλαίσιο που διασφαλίζει τη λειτουργική συνοχή και νομική σαφήνεια για κάθε συναλλαγή,4)να προωθεί την παγκόσμια υιοθέτηση του δικτύου και την υποστήριξη μεταξύ των ενδιαφερόμενων και των συστατικών μερών,5)να καθοδηγεί την ανάπτυξη των αποκεντρωμένων πρωτοκόλλων,6)να υποστηρίζει την έρευνα και την ανάπτυξη εφαρμογών και συναφών υπηρεσιών ,προωθώντας έτσι μια κοινότητα προγραμματιστών ανοικτού κώδικα.



Εικόνα 20:Το δίκτυο Velocity

Η συναίνεση(Consensus) διασφαλίζει ότι τα κοινόχρηστα ledgers είναι ακριβή αντίγραφα και μειώνει τον κίνδυνο δόλιων συναλλαγών γιατί θα πρέπει να γίνει η παραβίαση σε πολλά σημεία ταυτόχρονα. Τα κρυπτογραφικά hashes διασφαλίζουν ότι οποιαδήποτε αλλαγή στην είσοδο συναλλαγής, ακόμα και η πιο ελάχιστη αλλαγή έχει ως αποτέλεσμα μια διαφορετική τιμή hash υπολογισμένη, το οποίο δηλώνει δυνητικά παραβιασμένο είδος συναλλαγής. Οι ψηφιακές υπογραφές διασφαλίζουν ότι οι συναλλαγές προέρχονται από αποστολείς(υπογράφονται με ιδιωτικά κλειδιά και όχι απατεώνες). Οι συμμετέχοντες στο δίκτυο μπορεί να είναι μεμονωμένα άτομα,το κράτος,οργανισμοί ή συνδυασμός όλων αυτών των τύπων συμμετεχόντων.Στο πυρήνα του,το σύστημα καταγράφει τη χρονολογική σειρά των συναλλαγών με όλους τους κόμβους να συμφωνούν στην εγκυρότητα των συναλλαγών και με βάση το επιλεγμένο μοντέλο συναίνεσης είτε να επαληθεύονται είτε όχι με βάση ένα κατώφλι που έχει οριστεί.Τέλος, οι συναλλαγές δεν μπορούν να τροποποιηθούν ή να αντιστραφούν,εκτός εάν η αλλαγή έχει συμφωνηθεί από όλα τα μέλη στο δίκτυο σε μεταγενέστερη συναλλαγή.

4.8 Περιγραφή αρχιτεκτονικής BcER^2

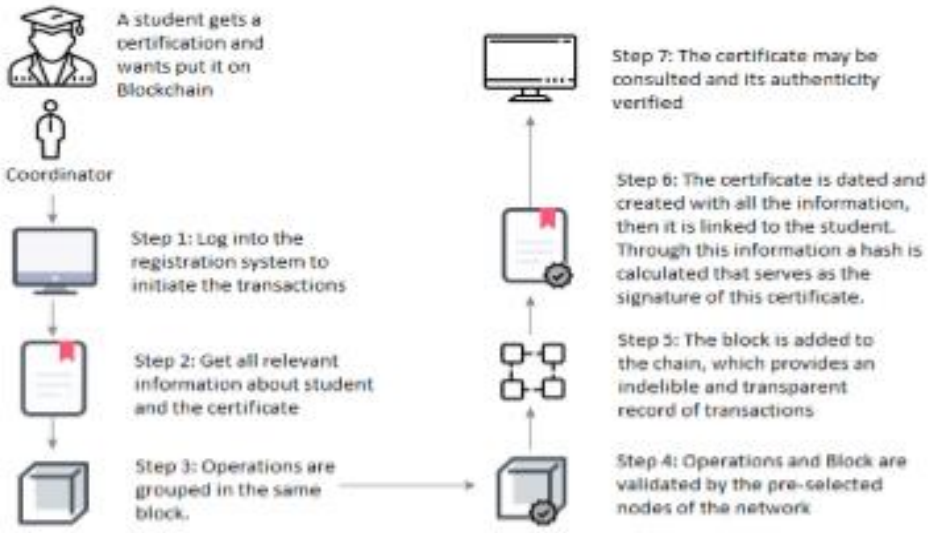
Ο αποθηκευτικός χώρος BcER^2 έχει υιοθέτησει το σύστημα κοινοπραξίας blockchain(consortium blockchain) αφού μόνο εξουσιοδοτημένα άτομα είναι δυνατό να δημιουργήσουν καταχωρήσεις πιστοποιητικών στο δίκτυο.Από την άλλη πλευρά ο καθένας

μπορεί να επαληθεύσει την αυθεντικότητα τους.Έτσι κατά την καταγραφή μιας εκπαιδευτικής εγγραφής ,για παράδειγμα ο υπεύθυνος για τη δημιουργία της εγγραφής γράφει στο μητρώο ή στη βάση δεδομένων χρησιμοποιώντας το δικό του ιδιωτικό κλειδί.Οι χρήστες που θέλουν να ελέγξουν την ακρίβεια της εγγραφής πρέπει να έχουν ένα αντίστοιχο αριθμό αναγνώρισης που θα εισαχθεί στο σύστημα.Η δομή του BcER^2 χρησιμοποιεί τα βασικά βήματα και τη ροή λειτουργίας μιας εφαρμογής που βασίζεται σε blockchain:

- αιτείται μια συναλλαγή από κάποιον που έχει προηγούμενη εξουσιοδότηση και χρειάζεται να δημιουργήσει ένα εκπαιδευτικό αρχείο
- η αιτηθείσα συναλλαγή εγγραφής αποστέλλεται στους κόμβους που ανήκουν στο σύστημα του BcER^2
- η εκπαιδευτική συναλλαγή εγγραφής εξακριβώνεται από το καθολικό(ledger) και ένα νέο μπλοκ δεδομένων που αντιστοιχεί στη εκπαιδευτική συναλλαγή εγγραφής δημιουργείται και προσαρτάται στο καθολικό μόνιμα και αμετάβλητα ολοκληρώνοντας τη συναλλαγή.

4.8.1 Οντότητες που απαρτίζουν το BcER^2

Οι οντότητες που ανήκουν στο BcER^2 εκπαιδευτικό αποθετήριο είναι οι ακόλουθες: α)προσόντα, β)καταχωρήσεις , γ)συναλλαγές και δ)συμμετέχοντες.Ένα «προσόν» μπορεί να είναι οτιδήποτε αξίας που μπορεί να κρατηθεί με ασφάλεια από το εκπαιδευτικό αποθετήριο.Εκπαιδευτικές εγγραφές όπως πιστοποιητικά,διπλώματα εκπαιδευτικά αρχεία και παρόμοια έγγραφα είναι BcER^2 προσόντα.



Εικόνα 21:Περιγραφή δημιουργίας "Μητρώου Πιστοποιητικών" στο BcER^2

«Συμμετέχοντες» είναι οι εκπρόσωποι των εκπαιδευτικών οργανισμών,φοιτητές και άνθρωποι γενικότερα που κατά κάποιο τρόπο ενδιαφέρονται είτε να διανείμουν είτε να έχουν πρόσβαση σε εκπαιδευτικά αρχεία.Οι συμμετέχοντες είναι καθορισμένοι στο «επιχειρηματικό μοντέλο του δικτύου» το οποίο υιοθετήθηκε από τη διαδικασία εφαρμογής του blockchain.Στο $BcER^2$,οι συντονιστές,οι φοιτητές και οποιοσδήποτε άλλος να έχει πρόσβαση στα εκπαιδευτικά αρχεία είναι οι συμμετέχοντες που ανήκουν στο δίκτυο.Καθένας έχει συγκεκριμένες λειτουργίες ,ευθύνες και περιορισμούς πρόσβασης. Οι «συναλλαγές» υποβάλλονται από τους συμμετέχοντες για να να έχουν πρόσβαση στα προσόντα που διατηρούνται στα στηριγμένα στο blockchain μητρώα προσόντων στο καθολικό.Οι συναλλαγές γενικά ανήκουν σε ένα επιχειρηματικό δίκτυο και,ως εκ τούτου απαιτούν ένα «επιχειρηματικό μοντέλο δικτύου».Το επιχειρηματικό μοντέλο δικτύου από την οπτική γωνία του συστήματος blockchain,προσδιορίζει τη λειτουργία που σχετίζεται με τα προσόντα.Οι «καταχωρήσεις» μπορούν να οριστούν ως ένα σετ δεδομένων που σχετίζονται με τα προσόντα,συναλλαγές και τους συμμετέχοντες,το σετ αυτό είναι που θα περιληφθεί στο μπλοκ μετά την επαλήθευση,οι «καταχωρήσεις» είναι νέα πληροφορία που προστίθεται στο καθολικό του blockchain.Στο $BcER^2$ εκπαιδευτικό αποθετήριο η προσθήκη ενός «μητρώου» πραγματοποιείται μέσω της εκτέλεσης βημάτων.Σε αυτά τα βήματα το επιχειρηματικό μοντέλο υιοθέτει τις ακόλουθες επιχειρηματικές υποθέσεις:1)ο συντονιστής του μαθήματος ή ο εκπρόσωπος του εκπαιδευτικού ιδρύματος είναι η αρχή για τη δημιουργία νέων προσόντων και 2)οι μαθητές και το ευρύ κοινό είναι οι συμμετέχοντες που έχουν πρόσβαση στα επικυρωμένα και ασφαλή εκπαιδευτικά περιουσιακά στοιχεία που διατηρεί το σύστημα.

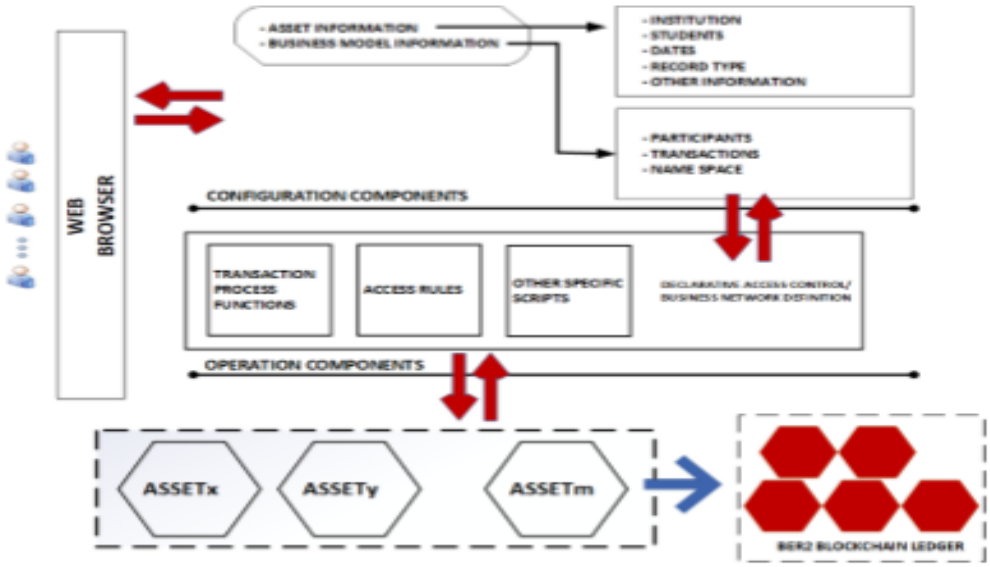
Η δημιουργία ενός μητρώου εκτελείται όπως φαίνεται παραπάνω στην Εικόνα 21:

- Ένας συντονιστής πηγαίνει να γράψει μια εγγραφή στο λογαριασμό blockchain που σημαίνει ότι δημιουργεί το πιστοποιητικό με ένα αναγνωριστικό,σε αυτή τη διαδικασία ο συντονιστής επιλέγει το πιστοποιητικό και μέσω του αναγνωριστικού του αριθμού είναι δυνατόν να το συνδέσει με ένα φοιτητή.
- Η εγγραφή αποθηκεύεται και σφραγίζεται χρονικά σε ένα μπλοκ χρησιμοποιώντας αριθμητικές πράξεις
- Στη συνέχεια,το μπλοκ επικυρώνεται από προεπιλεγμένους κόμβους δικτύου μέσω τεχνικών κρυπτογράφησης.
- Το μπλοκ φέρει ημερομηνία και προστίθεται στην αλυσίδα μπλοκ,έτσι ώστε όλοι οι χρήστες να έχουν πρόσβαση στην ίδια αλυσίδα εφόσον κάθε κόμβος χτίζει το δικό του υπόδειγμα ανεξάρτητα.

Με το που εκτελεστούν αυτά τα βήματα μπορούμε να αποκτήσουμε πρόσβαση σε εκπαιδευτικά αρχεία με αυθεντικότητα και ακεραιότητα χρησιμοποιώντας απλά μια πιστοποίηση(ταυτότητα(ID Card)) μέσω ενός προγράμματος περιήγησης ιστού.

4.8.2 Επιχειρηματικό μοντέλο και στοιχεία του BcER^2

Το επιχειρηματικό δίκτυο είναι ένας θεμελιώδης ορισμός για την ανάπτυξη του BcER^2.Συνοπτικά μοντελοποιεί το «εκπαιδευτικό μοντέλο» BcER^2,προσδιορίζοντας τα υπάρχοντα περιουσιακά στοιχεία,τις συναλλαγές και τους συμμετέχοντες που σχετίζονται με αυτά.Το επιχειρηματικό δίκτυο καθορίζει τις συναλλαγές που αλληλεπιδρούν με τα περιουσιακά στοιχεία.Το μοντέλο περιλαμβάνει επίσης των ορισμό των συμμετεχόντων που αλληλεπιδρούν με περιουσιακά στοιχεία και τα συνδέει με μια μοναδική ταυτότητα σε πολλά δίκτυα επιχειρήσεων.Όπως περιγράφηκε και πρωτύτερα,το BcER^2 αποτελείται από περιουσιακά στοιχεία, συμμετέχοντες και συναλλαγές με καθεμία από αυτές τις οντότητες να μοντελοποιείται σε σχέση με την εκπαιδευτική της λειτουργία.Τα βασικά στοιχεία που ανήκουν στο αποθετήριο εκπαιδευτικών αρχείων BcER^2 απεικονίζονται στην Εικόνα 22 και βασικά αντικατοπτρίζουν το επιχειρηματικό δίκτυο που έχει υιοθετηθεί και το οποίο είναι κατάλληλο για ένα αποθετήριο εκπαιδευτικών αρχείων,που καταγράφει διαχειρίζεται και παρέχει πρόσβαση σε αυτά.



Εικόνα 22:Βασικά στοιχεία του BcER^2

Το στοιχείο «πληροφορίες περιουσιακών στοιχείων»(asset information) περιέχει πληροφορίες σχετιζόμενες με το εκπαιδευτικό αρχείο που διαχειρίζεται το BcER^2.Αυτό το στοιχείο είναι

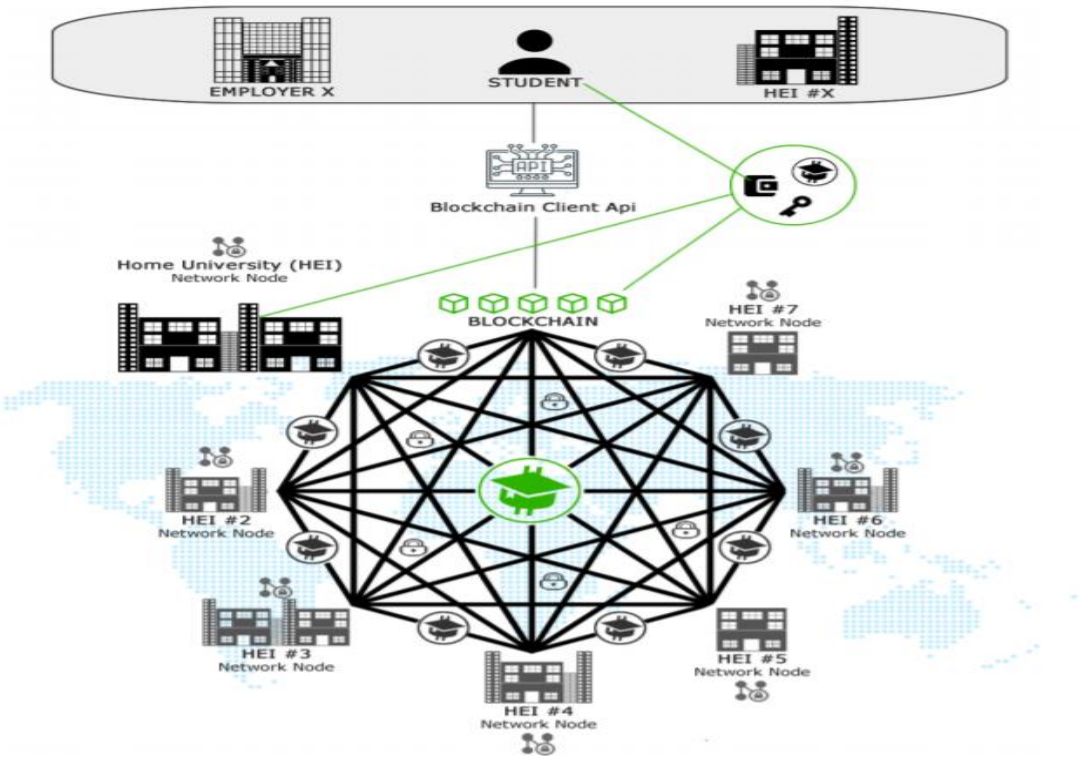
υπεύθυνο για τον ορισμό και την συνέπεια του περιουσιακού στοιχείου.Το στοιχείο «επιχειρηματικό μοντέλο πληροφοριών»(Business Model Information) περιέχει πληροφορίες που σχετίζονται με τη διαδικασία που εμπλέκεται στη διαχείριση περιουσιακών στοιχείων.Ορίζει βασικά τους συμμετέχοντες,το όνομα χώρου και τις συναλλαγές που εμπλέκονται στη διαδικασία.Το στοιχείο «Λειτουργία διαδικασίας συναλλαγής»(Transaction Process Function) περιέχει τις πληροφορίες σχετικά με τις εξειδικευμένες συναρτήσεις που καλούνται στο επιχειρηματικό μοντέλο για τη διαχείριση του περιουσιακού στοιχείου.Το στοιχείο «Κανόνες πρόσβασης»(Access Rules) περιέχει όπως υποδηλώνει το όνομα του τους κανόνες πρόσβασης συμπεριλαμβανομένων όλων των προτεραιοτήτων μεταξύ των συμμετεχόντων που εμπλέκονται στο επιχειρηματικό μοντέλο.Οι διαχειριστές και οι γενικοί χρήστες έχουν πρόσβαση στο αποθετήριο μέσω ενός προγράμματος περιήγησης στο Web χρησιμοποιώντας κάρτες αναγνώρισης,όπως κάρτες ταυτότητας(ID Cards) που περιλαμβάνουν προφίλ σύνδεσης και διαπιστευτήρια.Τα περιουσιακά στοιχεία αναπτύσσονται ενεργά στο καθολικό blockchain του BcER[2],με τη χρήση ενός πλαισίου(framework) του Hyperledger Composer.

4.9 Περιγραφή του EduCTX

Το EduCTX πρόκειται για μια πλατφόρμα που αφορά τη παγκόσμια πίστωση τριτοβάθμιας εκπαίδευσης,με χρήση της τεχνολογίας blockchain.Αυτή η πλατφόρμα βασίζεται στην έννοια του ευρωπαϊκού συστήματος μεταφοράς πίστωσης και συσσώρευσης(ECTS). Αποτελεί ένα παγκόσμια αξιόπιστο,αποκεντρωμένο σύστημα πίστωσης και βαθμολόγησης της τριτοβάθμιας εκπαίδευσης που προσφέρει παγκοσμίως ενοποιημένη άποψη για φοιτητές και ιδρύματα τριτοβάθμιας εκπαίδευσης(AEI),καθώς και για άλλους πιθανούς ενδιαφερόμενους,όπως εταιρείες, ιδρύματα και οργανισμούς.Το EduCTX επεξεργάζεται,διαχειρίζεται και ελέγχει τα διακριτικά(tokens) ECTX,τα οποία αντιπροσωπεύουν πιστώσεις που κερδίζουν οι φοιτητές για ολοκληρωμένα μαθήματα αντίστοιχα με τα ECTS.Τα AEI(HEIs) αποτελούν τους ομότιμους(peers) του δικτύου blockchain.Η πλατφόρμα αποτελεί μια πιο διαφανή και τεχνολογικά προηγμένη μορφή συστημάτων τριτοβάθμιας εκπαίδευσης.Η πλατφόρμα EduCTX αντιπροσωπεύει τη βάση της πρωτοβουλίας της EduCTX,η οποία προβλέπει ότι διάφορα AEI θα μπορούσαν να συνενώσουν τις δυνάμεις τους για να δημιουργήσουν ένα παγκόσμια αποτελεσματικό,απλοποιημένο και πανταχού παρόν περιβάλλον προκειμένου να αποφευχθούν τα γλωσσικά και διοικητικά εμπόδια.Εν συνεχεία,αποτελεί και μια πλατφόρμα τριτοβάθμιας εκπαίδευσης και βαθμονόμησης που βασίζεται στη τεχνολογία blockchain.Η

πλατφόρμα EduCTX οραματίστηκε για την επεξεργασία, την διαχείριση και τον έλεγχο,τη χρήση διακριτικών ECTX ως ακαδημαϊκών πιστώσεων και η λειτουργία της στηρίζεται σε ένα παγκόσμιο κατανεμημένο δίκτυο P2P όπου οι ομότιμοι κόμβοι του δικτύου(peers) είναι ιδρύματα ανώτερης εκπαίδευσης(HEIs) και οι χρήστες της πλατφόρμας είναι φοιτητές και οργανισμοί(π.χ. εταιρίες ως πιθανοί εργοδότες). Τα διακριτικά ECTX αντιπροσωπεύουν ένα ισοδύναμο με την πιστωτική αξία των φοιτητών για ολοκληρωμένα μαθήματα,όπως και με τις πιστώσεις ECTS που αποκτούν οι Ευρωπαίοι φοιτητές. Κάθε φοιτητής θα έχει ένα αποκλειστικό πορτοφόλι blockchain EduCTX,όπου θα συλλέγει ECTX διακριτικά,δηλαδή την αξία των πιστώσεων που έχουν καταχωρηθεί από το ΑΕΙ για τα ολοκληρωμένα μαθήματά του.Κάθε φορά που ένας φοιτητής ολοκληρώνει ένα μάθημα,το ΑΕΙ στο οποίο φοιτεί θα μεταφέρει τον κατάλληλο αριθμό ECTX στη blockchain διεύθυνση του.Οι πληροφορίες μεταφοράς αποθηκεύονται στο blockchain,όπου αποθηκεύονται τα ακόλουθα δεδομένα 1)ο αποστολέας αναγνωρίζεται ως το σχετικό ΑΕΙ με το επίσημο όνομά του,2)ο παραλήπτης φοιτητής παρουσιάζεται ανώνυμα,3)διακριτικό πίστωσης(token credit) τιμή πίστωσης(credit value),4)αναγνώριση μαθημάτων. Επιπλέον, χρησιμοποιώντας τη διεύθυνση blockchain του,ο φοιτητής ως παραλήπτης των ECTX διακριτικών,θα είναι σε θέση να αποδείξει παγκοσμίως τα ολοκληρωμένα μαθήματά του,χωρίς κανένα διοικητικό σενάριο ή γλωσσικό εμπόδιο,απλώς παρουσιάζοντας τη διεύθυνση blockchain του.Για λόγους ασφαλείας έχει εκχωρηθεί στους φοιτητές μια διεύθυνση πολλαπλών υπογραφών 2-2 από το ΑΕΙ τους,έτσι ώστε να μην είναι σε θέση να μεταφέρουν κανένα από τα κερδισμένα ECTX που απέκτησαν σε άλλες διευθύνσειςΗ διεύθυνση πολλαπλών υπογραφών 2-2 σημαίνει ότι απαρτίζεται από τις διευθύνσεις δύο μερών(τα δημόσια κλειδιά τους) και τουλάχιστον δύο από αυτά πρέπει να υπογράψουν μια συναλλαγή από αυτή την διεύθυνση πολλαπλών υπογραφών για επεξεργασία.Η διαδικασία εκχώρησης σε φοιτητές διακριτικών ECTX και η ικανότητα τους να αποδείξουν την κατοχή αυτών αντιμετωπίζεται μέσω ενός απλού στη χρήση API πελάτη του EduCTX,κάνοντας έτσι τη χρήση της πλατφόρμας όσο το δυνατόν πιο διαισθητική. Οποιοδήποτε διαπιστευμένο ΑΕΙ και τα μέλη του θα μπορούν να εγγραφούν στο δίκτυο. Κατά την είσοδό του στο δίκτυο,το ΑΕΙ θα πρέπει να δημιουργήσει έναν κόμβο δικτύου προκειμένου να διατηρήσει μια παγκόσμια υποδομή και ένα ασφαλές δίκτυο.Ένας πλήρως λειτουργικός κόμβος μεταδίδει μηνύματα σε ολόκληρο το δίκτυο,το οποίο είναι το πρώτο βήμα στη διαδικασία συναλλαγής που οδηγεί σε επιβεβαίωση μπλοκ,επομένως επιβεβαίωση μεταφοράς πιστώσεων ECTX για ολοκληρωμένα μαθήματα σε φοιτητές.Ο κόμβος του ΑΕΙ θα έχει επίσης το βασικό EduCTX blockchain πελάτη στο στιγμιότυπο του server του με πλήρες αντίγραφό του στο καθολικό.Αυτό αυξάνει την ασφάλεια καθώς όσο περισσότεροι κόμβοι υπάρχουν,τόσο

πιο ασφαλές είναι το δίκτυο. Μια αφηρημένη απεικόνιση της πλατφόρμας παρουσιάζεται στη εικόνα που παρατίθεται παρακάτω



Εικόνα 23:Μια απεικόνιση της δομής του EduCTX

Τα ΑΕΙ και συνεπώς οι κόμβοι δεν χρειάζεται να κάνουν εξόρυξη των συναλλαγών καθώς η πλατφόρμα blockchain EduCTX βασίζεται στο πρωτόκολλο συναίνεσης DPoS.Επομένως δεν απαιτείται υπολογιστική ισχύς από τον ΑΕΙ κόμβο.Τέτοια προσέγγιση είναι επίσης κατάλληλη από την πλευρά ασφαλείας για το δίκτυο EduCTX,δεδομένου ότι τυχαίοι ομότιμοι(peers) δεν μπορούν να συμμετάσχουν στο δίκτυο και να δημιουργήσουν νέα διακριτικά ECTX εξορύσσοντας το.Ως εκ τούτου,το blockchain EduCTX μπορεί να θεωρηθεί ως μια έκδοση κοινοπραξίας ενός blockchain.Κάθε νέο ΑΕΙ που συμμετέχει στο δίκτυο ελέγχεται από άλλα μέλη ΑΕΙ του εκχωρούνται διακριτικά και του ζητείται να δημιουργήσει έναν νέο κόμβο δικτύου. Δεδομένου ότι στο EduCTX χρησιμοποιείται μια έκδοση συναίνεσης η κατ'εξουσιοδότηση απόδειξη συμμετοχής (DPoS) του blockchain ,κάθε μέλος του ΑΕΙ θα μπορεί να εγγραφεί ως αντιπρόσωπος στην πλατφόρμα blockchain EduCTX και η κοινότητα EduCTX ΑΕΙ θα ψηφίσει έναν εκπρόσωπο ο οποίος με τη σειρά του θα επιβεβαιώσει συναλλαγές και θα σφραγίσει τα μπλοκ. Αυτό σημαίνει ότι η κοινότητα θα ψηφίσει για το ΑΕΙ που θα είναι το πιο θετικό και συνεχές στη δουλειά του.Προκειμένου,να εξασφαλιστεί μια επιτρεπόμενη έκδοση της πλατφόρμας blockchain και μια δημοκρατική και μη κερδοσκοπική κοινότητα,έχει προταθεί να μειωθεί η ανταμοιβή έγκρισης στο μηδέν.Παρακάτω

περιγράφονται λεπτομερώς,τα τέσσερα σημαντικά σενάρια τα οποία θα υπάρχουν στο EduCTX.

Το ΑΕΙ συμμετέχει στο EduCTX

Ένα νέο ΑΕΙ επιχειρεί να συμμετάσχει στο δίκτυο blockchain EduCTX χρησιμοποιώντας το EduCTX API για να δημιουργήσει το blockchain πορτοφόλι του και τη διεύθυνση του που περιέχει τα δημόσια και ιδιωτικά κλειδιά του.Το νέο ΑΕΙ θα πρέπει να αποθηκεύει με ασφάλεια το αποκτημένο ιδιωτικό κλειδί του.Αφού δημιουργήσει τη διεύθυνση επικοινωνεί με ένα από τα υπάρχοντα ΑΕΙ,μέλη του δικτύου blockchain EduCTX (εφεξής αναφερόμενο ως memHEI).Το μέλος ΑΕΙ λαμβάνει ένα νέο αίτημα(ένταξη) εγγραφής.Αρχικά επαληθεύει τις επίσημες πληροφορίες του νέου ΑΕΙ και μετά μεταφέρει ένα διακριτικό ECTX στη διεύθυνση blockchain του νέου ΑΕΙ.Στη συνέχεια η συναλλαγή υποβάλλεται σε επεξεργασία μέσω του δικτύου blockchain.Όταν επιβεβαιωθεί η συναλλαγή,το μέλος ΑΕΙ στέλνει ένα αίτημα αποζημίωσης τυχαίων 0.00X ECTX διακριτικών μέσω ενός ιδιωτικού καναλιού στο νέο ΑΕΙ,το οποίο εριλαμβάνει 1)τον αριθμό των X (0.00X) EduCTX (π.χ. 235781- που σημαίνει 0,00235781 EduCTX) και 2)την blockchain διεύθυνση.Όταν το νέο ΑΕΙ λαμβάνει το αίτημα επιστροφής για ένα ιδιωτικό κανάλι μεταφέρει 0.00X EduCTX στη διεύθυνση του μέλους ΑΕΙ(η συναλλαγή επεξεργάζεται μέσω του δικτύου blockchain).Στη συνέχεια,το νέο ΑΕΙ ειδοποιεί το μέλος ΑΕΙ αφότου η συναλλαγή έχει ολοκληρωθεί.Το μέλος ΑΕΙ επαληθεύει την ύπαρξη της συναλλαγής από το νέο ΑΕΙ.Εάν η μυστική τιμή της επιστροφής χρημάτων είναι λανθασμένη, το μέλος ΑΕΙ τερματίζει τη διαδικασία εγγραφής. Διαφορετικά μεταφέρει το κατάλληλο αριθμό διακριτικών ECTX στο νέο ΑΕΙ. Το μέλος ΑΕΙ διαδίδει τις πληροφορίες στο νέο ΑΕΙ μέσω του δικτύου μελών του EduCTX και του στέλνει οδηγίες για τη ρύθμιση ενός κόμβου δικτύου. Το νέο ΑΕΙ ρυθμίζει το κόμβο δικτύου blockchain σύμφωνα με τις οδηγίες.Τέλος, αφού η διαδικασία ρύθμισης του κόμβου δικτύου ολοκληρωθεί με επιτυχία, η διαδικασία ένταξης του νέου ΑΕΙ στο EduCTX ολοκληρώνεται**.**

Εγγραφή φοιτητή

Όταν ένας φοιτητής εγγράφεται στο ΑΕΙ(μέλος του δικτύου blockchain EduCTX),εκείνο εκδίδει ένα αναγνωριστικό και δημιουργεί μια διεύθυνση blockchain για το φοιτητή, που περιέχει ένα δημόσιο και ένα ιδιωτικό κλειδί.Επιπλέον,το ΑΕΙ δημιουργεί μια νέα πολλαπλών υπογραφών 2-2 διεύθυνση blockchain με το δημόσιο του κλειδί και το δημόσιο κλειδί του

φοιτητή που δημοσιεύθηκε πρόσφατα. Αυτή η διεύθυνση πολλαπλών υπογραφών σε συνδυασμό με το αναγνωριστικό του φοιτητή αποθηκεύονται στη βάση δεδομένων του ΑΕΙ. Το ΑΕΙ μεταφέρει 0.1 διακριτικά ECTX στη διεύθυνση blockchain πολλαπλών υπογραφών 2-2 του φοιτητή και μέσω ενός ιδιωτικού καναλιού παρέχει στο φοιτητή τις πληροφορίες που απαιτούνται για τη ρύθμιση του blockchain πορτοφολιού του. Οι παρεχόμενες πληροφορίες περιλαμβάνουν 1)οδηγίες για τη δημιουργία ενός πορτοφολιού EduCTX blockchain,2)τη διεύθυνση blockchain του φοιτητή που περιέχει δημόσια και ιδιωτικά κλειδιά,3)το δημόσιο κλειδί του ΑΕΙ,4)τη γραφή εξαργύρωσης. Με τις ληφθείσες πληροφορίες ο φοιτητής δημιουργεί το blockchain πορτοφόλι του και μια διεύθυνση χρησιμοποιώντας τα δημόσια και ιδιωτικά κλειδιά που ελήφθησαν από τη διεύθυνση ΑΕΙ. Αυτός δημιουργεί επίσης μια διεύθυνση blockchain πολλαπλών υπογραφών 2-2 με το δημόσιο κλειδί του και το δημόσιο κλειδί του ΑΕΙ,έτσι τα δεδομένα του πορτοφολιού αποθηκεύονται με ασφάλεια. Χρησιμοποιώντας το πορτοφόλι πολλαπλών υπογραφών 2-2,ο φοιτητής δημιουργεί και υπογράφει μια συναλλαγή 0,1 διακριτικού ECTX στη διεύθυνση blockchain του ΑΕΙ.Έπειτα, το ΑΕΙ υπογράφει τη συναλλαγή χρησιμοποιώντας το ιδιωτικό κλειδί του. Η συναλλαγή υποβάλλεται σε επεξεργασία μέσω του δικτύου blockchain.Όταν η συναλλαγή επιβεβαιωθεί, το ΑΕΙ αποθηκεύει τις πληροφορίες στη βάση δεδομένων του, επιβεβαιώνοντας την επιτυχημένη δημιουργία του πορτοφολιού του φοιτητή.

Ολοκλήρωση μαθήματος φοιτητή

Αφού ο φοιτητής συμμετάσχει σε κάποια εξετάση-διαγώνισμα, ο καθηγητής πρέπει να επαληθεύσει τα αποτελέσματα. Εάν ο φοιτητής είναι επιτυχής,ο καθηγητής είναι σε θέση να δηλώσει ατομικά την ολοκλήρωση των υποχρεώσεων του φοιτητή, τα αποτελέσματα αυτά αποθηκεύονται στην κεντρική βάση δεδομένων. Διαφορετικά, ο καθηγητής ειδοποιεί το γραφείο διοίκησης για την εκτέλεση της διαδικασίας που απαιτείται για την καταχώριση της κατάστασης των υποχρεώσεων του φοιτητή. Τα αποτελέσματα μπορούν να αποθηκευτούν ταυτόχρονα στην κεντρική βάση δεδομένων σε περίπτωση που το ΑΕΙ διατηρεί ένα παράλληλο σύστημα που υπόκειται στους κανονισμούς της εθνικής νομοθεσίας το οποίο έχει υποβληθεί για αξιολόγηση από ομοτίμους στις 20 Οκτωβρίου 2017, έως ότου το σύστημα blockchain EduCTX αποδειχθεί ως πλήρως υλοποιημένο και σε λειτουργία. Ο καθηγητής ή το γραφείο διοίκησης εντοπίζει τη διεύθυνση blockchain του φοιτητή στην κεντρική βάση δεδομένων, βρίσκει το ποσό του ECTS που έχει καθορίσει το μάθημα και χρησιμοποιεί το πορτοφόλι blockchain για να μεταφέρει το κατάλληλο ποσό των διακριτικών ECTX στη διεύθυνση blockchain 2-2 πολλαπλών υπογραφών του μαθητή. Η συναλλαγή υποβάλλεται σε επεξεργασία

μέσω του δικτύου blockchain. Όταν επιβεβαιωθεί η συναλλαγή, ο καθηγητής ή το γραφείο διοίκησης καταγράφει την επιτυχή μεταφορά μαρκών ECTX στην κεντρική βάση δεδομένων.

Ο οργανισμός επαληθεύει το πιστωτικό αρχείο του φοιτητή

Όταν ένας οργανισμός (π.χ. εργοδότης, πανεπιστήμιο κ.λπ.) θέλει να επαληθεύσει την ολοκλήρωση της υποχρέωσης του φοιτητή, ο φοιτητής πρέπει να στείλει τη διεύθυνση blockchain του και τη διεύθυνση blockchain 2-2 πολλαπλών υπογραφών του για να εξαργυρώσει το σενάριο στον επαληθευτή - οργανισμό. Ο οργανισμός ελέγχει το σενάριο εξαργύρωσης για να επαληθεύσει τη διεύθυνση του φοιτητή και τη διεύθυνση 2-2 πολλαπλών υπογραφών. Χρησιμοποιώντας το API ιστού blockchain για πρόσβαση σε δεδομένα blockchain, ο οργανισμός ελέγχει τον αριθμό των διακριτικών ECTX στη διεύθυνση πολλαπλών υπογραφών 2-2, η οποία αντιπροσωπεύει τα ακαδημαϊκά πιστωτικά επιτεύγματα του φοιτητή. Στη συνέχεια, μέσω ενός ιδιωτικού καναλιού, ο οργανισμός απαιτεί από τον φοιτητή να υπογράψει ένα μήνυμα (π.χ. "XYZ") με τη διεύθυνση του / της για να επαληθεύσει την ταυτότητά του. Όταν ο φοιτητής, χρησιμοποιώντας το API ιστού blockchain, υπογράφει το μήνυμα με τη διεύθυνση και το ιδιωτικό του κλειδί, ειδοποιεί τον οργανισμό, ο οποίος ελέγχει το υπογεγραμμένο μήνυμα. Εάν το υπογεγραμμένο μήνυμα επικυρωθεί, ο οργανισμός μπορεί να εμπιστευτεί ότι η διεύθυνση blockchain που παρουσιάζεται και η τιμή των διακριτικών ECTS είναι πράγματι δικά του.Ως εφαρμογή πρωτοτύπου έχει επιλεχθεί το ARK Blockchain, ως η υποκείμενη τεχνολογία της πλατφόρμας EduCTX. Το ARK δεν είναι μόνο ένα κρυπτονόμισμα, αλλά είναι επίσης ένα οικοσύστημα που προορίζεται για μαζική υιοθέτηση blockchain. Χτίζοντας την πλατφόρμα EduCTX πάνω από ένα εξαιρετικά ασφαλές και γρήγορο blockchain πυρήνα ARK, ενσωματώνοντας βασικές αποκεντρωμένες τεχνολογίες, η πλατφόρμα γίνεται φιλική προς το χρήστη-πανεπιστήμιο για να αυξήσει την υιοθέτηση της τεχνολογίας blockchain συνολικά. Οι κύριοι λόγοι για την επιλογή της τεχνολογίας ARK ως βάση κώδικα είναι η ευελιξία και η ανοιχτή προέλευσή της και η συνολική διαθεσιμότητα εφαρμογών API πελάτη. Κατά τη στιγμή της γραφής, το ARK παρέχει περισσότερες από 12 διαφορετικές γλώσσες προγραμματισμού των εφαρμογών πελατών, επιτρέποντας έτσι σε άλλους φορείς (ΑΕΙ, φοιτητές, εργοδότες) να συμμετάσχουν στην πλατφόρμα στη γλώσσα προγραμματισμού της επιλογής τους

4.9.1 Πρωτόκολλο πολλαπλών υπογραφών

Ένα πρωτόκολλο πολλαπλών υπογραφών είναι μια πολύ γνωστή ιδέα στο κόσμο της κρυπτογραφίας δημόσιου κλειδιού.Επιτρέπει σε πολλά μέρη να υπογράψουν από κοινού

ψηφιακά ένα συμφωνημένο μήνυμα καθένα με το δικό του ιδιωτικό κλειδί.Μια τέτοια επιλογή είναι επιθυμητή σε περιπτώσεις όπου πολλαπλά μέρη πρέπει να συμφωνήσουν ομοιόμορφα,όπως στη περίπτωση του κοινού τραπεζικού λογαριασμού.Ένας τέτοιος τραπεζικός λογαριασμός είναι για παράδειγμα ένας διεθνής αριθμός τραπεζικού λογαριασμού(IBAN),ο οποίος στη περίπτωση εισερχόμενης συναλλαγής,δεν απαιτεί καμία ενέργεια από τους κατόχους λογαριασμού και ακόμη περισσότερο,κρύβει τις ταυτότητες των κατόχων του λογαριασμού.Αντιθέτως,όταν μια εξερχόμενη συναλλαγή πρέπει να διεξαχθεί,κάθε κάτοχος λογαριασμού πρέπει να δώσει έγκριση πριν από την επεξεργασία της συναλλαγής από την τράπεζα.Μια τέτοια ιδέα είναι κοινή πρακτική στον κόσμο των κρυπτονομισμάτων ,σύμφωνα με την οποία μπορούν M-προς-N blockchain πορτοφόλια να δημιουργηθούν.Εδώ το M δηλώνει τον ελάχιστο αριθμό υπογραφόντων μιας συναλλαγής και το N υποδηλώνει τον πλήρη αριθμό πιθανών διευθύνσεων(κάτοχοι λογαριασμού).Ένα παράδειγμα είναι μια διεύθυνση πολλαπλών υπογραφών 2-3,η οποία αποτελείται από τρία μέρη(τα δημόσια κλειδιά τους) και τουλάχιστον δύο από αυτά πρέπει να υπογράψουν μια συναλλαγή από αυτή την διεύθυνση πολλαπλών υπογραφών για επεξεργασία.Στο κόσμο των κρυπτονομισμάτων,η χρήση μιας τέτοιας προσέγγισης για τη διεξαγωγή συναλλαγών αναφέρεται ως pay-to-script-hash(P2SH),σε αντίθεση με τη συνηθισμένη pay-to-public-key-hash(P2PKH) η οποία διευκολύνει όχι πολυυπογεγραμμένες διευθύνσεις.

4.10 RecordsKeeper

Το RecordsKeeper είναι μια άλλη λύση που βασίζεται σε blockchain για επαλήθευση ακαδημαϊκών πιστοποιητικών, τα εκπαιδευτικά ιδρύματα μπορούν να εκδώσουν πιστοποιητικά και να παρέχουν μια απόδειξη στον χρήστη που μπορεί να κοινοποιηθεί σε τρίτο μέρος για να αποδείξει ότι το πιστοποιητικό είναι αυθεντικό.Η απόδειξη που λαμβάνεται από τον φοιτητή θα χρησιμοποιηθεί από το τρίτο συμβαλλόμενο μέρος για την επαλήθευση της αυθεντικότητας του πιστοποιητικού στο RecordKeeper καθολικό.Δεν υπάρχουν πολλές επιπλοκές σε αυτόν τον μηχανισμό, αλλά τα μέρη που ενδιαφέρονται να δουν το πιστοποιητικό στο RecordKeeper blockchain πρέπει να έχουν δικαιώματα ιδιοκτησίας.Αυτό ισοδυναμεί με μια μεταβίβαση κυριότητας σε τρίτο μέρος που μπορεί να οδηγήσει σε παραβίαση.Αυτό μπορεί να λειτουργήσει καλά σε ένα ιδιωτικό blockchain για να διασφαλίσει την ασφάλεια του πιστοποιητικού.

Λύση	Λειτουργικότητα	Επαλήθευση	Εξουσιοδότηση	Εμπιστευτικότητα	Ιδιοκτησία	Ιδιωτικότητα
RecordsKeeper	Απόδειξη αυθεντικότητας του πιστοποιητικού (proof of authenticity(PoA). Ολόκληρη η διαδικασία της επαλήθευσης βασίζεται στην ιδιοκτησία	Ναι	Όχι	Όχι	Κοινόχρηστη	Όχι

Το θέμα ελέγχου ταυτότητας αντιμετωπίζεται από τη λύση που ονομάζεται RecordsKeeper. Η λύση blockchain RecordsKeeper παρέχει επαλήθευση εκπαιδευτικού πιστοποιητικού μέσω του ιδιόκτητου API της.Το πρωτόκολλο συναίνεσης που χρησιμοποιεί το Records Keeper αφορά την απόδειξη ιδιοκτησίας (PoA).Η αυθεντικότητα και η ακεραιότητα επαληθεύονται για τα δημοσιευμένες εγγραφές στο blockchain. Τα χαρακτηριστικά αυτής της λύσης είναι διαθέσιμα ως ένα δημόσιο blockchain.

4.11 Sony Global Education

Από το 2016, η Sony είχε ανακοινώσει ότι είχε αναπτύξει εσωτερικό σύστημα έκδοσης πιστοποιητικών που χρησιμοποιεί τεχνολογίες blockchain. Στις 10 Αυγούστου 2017, η Sony Corporation και η Sony Global Education (SGE) ανακοίνωσαν την ανάπτυξη ενός συστήματος που θα εφαρμόζει ειδικά την τεχνολογία blockchain στον τομέα της εκπαίδευσης. Το Δελτίο Τύπου αναφέρει ότι χρησιμοποιώντας "την τεχνολογία που κάνει κοινή χρήση των εκπαιδευτικών αποτελεσμάτων και των αρχείων με έναν ανοιχτό και ασφαλή τρόπο", αυτό το αξιόπιστο σύστημα συγκεντρώνει τη διαχείριση των δεδομένων από πολλαπλά εκπαιδευτικά ιδρύματα και καθιστά δυνατή την καταγραφή και την αναφορά εκπαιδευτικών δεδομένων και ψηφιακών απομαγνητοφωνήσεων. Το σύστημα βασίζεται στο IBM Blockchain, το οποίο παρέχεται μέσω του IBM Cloud και υποστηρίζεται από το Hyperledger Fabric 1.0, που αποτελεί μια μορφή blockchain και ένα από τα πρότζεκτ Hyperledger που φιλοξενεί το Linux Foundation. Συγκεντρώνει 1) μια λειτουργία που πιστοποιεί και ελέγχει τα δικαιώματα χρήσης στα εκπαιδευτικά δεδομένα ,2) μια διασύνδεση προγραμματισμού εφαρμογών για τη διαχείριση αυτών των δικαιωμάτων που απευθύνονται σε εκπαιδευτικά ιδρύματα. Το 2018, η

Sony άρχισε να αναπτύσσει τις δικές της προσφορές υπηρεσιών, ξεκινώντας με την Global Challenge Math Challenge, η οποία συγκεντρώνει 150.000 συμμετέχοντες από όλο τον κόσμο.

4.12 Η δράση Blockademic

Το BlockAdemic στοχεύει στη δημιουργία ενός ψηφιακού συστήματος κατανεμημένης ασφάλειας (distributed cybersecurity) για την πιστοποίηση και επαλήθευση εκπαιδευτικών δραστηριοτήτων, τίτλων σπουδών και δεξιοτήτων στον τομέα της τριτοβάθμιας εκπαίδευσης και δια βίου μάθησης, δημιουργώντας ένα αδιάβλητο εκπαιδευτικό διαβατήριο.Η συγκεκριμένη δράση επεκτείνει τη λογική του Ευρωπαϊκού συστήματος Μεταφοράς και Συσσώρευσης Μονάδων(ECTS) και του Ευρωπαϊκού Πλαισίου Προσόντων(ΕΠΠ),την οποία προσαρμόζει σε εκπαιδευτικά σενάρια με πιλοτική εφαρμογή.Το συγκεκριμένο έργο χρησιμοποιώντας κάποια εργαλεία της τεχνολογίας blockchain έχει σκοπό να εξασφαλίσει τον απαραίτητο βαθμό κυβερνασφάλειας και εμπιστοσύνης τόσο σε επίπεδο χρηστών όσο και σε θεσμικό επίπεδο.Στο Blockademic η καταγραφή των εκπαιδευτικών δραστηριοτήτων δεν καλύπτει μόνο ειδικές δεξιότητες αλλά και γενικές δεξιότητες ,κάτι που δεν έχει εφαρμοστεί μέχρι στιγμής σε άλλη εκπαιδευτική εφαρμογή.Η βασική διαφορά αυτής της δράσης με άλλες αφορά τη παρακολούθηση της συνολικής δραστηριότητας των φοιτητών στις φοιτητικές πλατφόρμες και η αυτόματη μετατροπή κάθε εκπαιδευτικής δραστηριότητας που κρίνεται επιτυχής σε ECTS,γεγονός που συνιστά πολύ πιο λεπτομερή μονάδα μέτρησης από το αποτέλεσμα ενός διαγωνίσματος. Η τεχνολογική λύση του Blockademic θα υποστηρίζει ένα ολοκληρωμένο οικοσύστημα που θα ενσωματώσει μαθησιακή αναλυτική (learning analytics) και παιχνιδοποίηση (gamification) για την σύνδεση μετρικών με μαθησιακά αποτελέσματα και αποκτώμενες γνώσεις, ικανότητες και δεξιότητες, με σκοπό την υποστήριξη και ενίσχυση της προαναφερθείσας παρακολούθησης, καταχώρησης, επαλήθευσης και αποτίμησης. Τα πλεονεκτήματα που παρέχει βασίζονται στα μοναδικά χαρακτηριστικά της τεχνολογίας blockchain,μέσω των οποίων τα μαθησιακά αποτελέσματα αλλά και οι τίτλοι σπουδών θα πιστοποιούνται χωρίς να είναι δυνατή η παραποίηση τους, προσφέροντας έτσι την απαραίτητη βάση ώστε να ξεπεραστούν τα εμπόδια της εμπιστοσύνης μεταξύ των φορέων, ιδρυμάτων και επιχειρήσεων καθώς και της μετακίνησης των εκπαιδευόμενων μεταξύ διαφορετικών ιδρυμάτων είτε σε εθνικό είτε σε διεθνές επίπεδο, παρέχοντας έτσι ένα απαραβίαστο και ταυτόχρονα αναλλοίωτο εκπαιδευτικό διαβατήριο. Έχοντας ως γνώμονα τα ανωτέρω, μια τεχνολογική πλατφόρμα κατανεμημένης ψηφιακής ασφάλειας θα αναπτυχθεί με στόχο την καταχώρηση εκπαιδευτικών δραστηριοτήτων, τίτλων σπουδών και πιστοποιήσεων σε αλυσίδα

blockchain – εκπαιδευτικό διαβατήριο.Οι χρήστες στο σύστημα Blockademic πιστοποιούνται με τη χρήση ψηφιακών πιστοποιητικών και διαθέτουν ψηφιακές υπογραφές.Στο σύστημα υπάρχουν επίσης διακριτικά(tokens) τα οποία υπάρχουν με τη χρήση έξυπνων συμβολαίων και εφόσον ικανοποιηθούν οι μαθησιακοί στόχοι που έχουν τεθεί εκ των προτέρων θα μεταφέρονται στους προσωπικούς λογαριασμούς (wallets) των εκπαιδευόμενων.Οι εγγραφές σε αυτό το κατανεμημένο σύστημα ασφαλείας είναι αδιάβλητες για αυτό το λόγο οι εκπαιδευόμενοι θα μπορούν να αποδεικνύουν σε τρίτους (όπως π.χ. άλλα ιδρύματα, φορείς ή επιχειρήσεις) το βαθμό εμπλοκής τους σε κάθε εκπαιδευτική δραστηριότητα, ώστε να αξιολογείται η γνώση και οι ικανότητες που έχουν αποκτήσει σε συγκεκριμένα αντικείμενα και αποτελούν απαραίτητη προϋπόθεση για την εισαγωγή τους στην παρακολούθηση μελλοντικών μαθημάτων/σεμιναρίων ή για την πρόσληψή τους σε θέσεις εργασίας.Κάθε ένας σε αυτό το σύστημα είτε πρόκειται για φορέα είτε για επιχείρηση θα μπορεί ανάλογα με τα δικαιώματα χρήσης του είτε να εγγράφει τίτλους σπουδών και πιστοποιητικά των εκπαιδευόμενων, είτε μόνο να τα επαληθεύει. Τα πρόσθετα tokens τα οποία θα έχει αποκομίσει κάποιος σπουδαστής και δεν θα έχουν μεταφραστεί σε μονάδες ECTS για τη λήψη τίτλου σπουδών, θα παραμένουν στο λογαριασμό του ως απόδειξη των επιτευγμάτων του στις αντίστοιχες δραστηριότητες και αντικείμενα αυξάνοντας τη «φήμη» του. Προκειμένου η συγκεκριμένη καινοτομία του BlockAdemic να δοκιμαστεί,αναμένεται να εφαρμοστεί πιλοτικά για να επικυρωθεί η λειτουργία της σε πραγματικές συνθήκες στην τριτοβάθμια εκπαίδευση από τους εμπλεκόμενους φορείς(ένα ερευνητικό κέντρο, ένα πανεπιστήμιο και δύο επιχειρήσεις).

Συνοψίζοντας το οικοσύστημα του Blockademic θα περιλαμβάνει:

- Παρακολούθηση εκπαιδευτικών δραστηριοτήτων με χρήση έξυπνων συμβολαίων (smart contracts)
- Καταχώρηση τίτλου σπουδών από τους αρμόδιους φορείς σε blockchain με χρήση αλγορίθμων συναίνεσης
- Επαλήθευση τίτλων σπουδών και εκπαιδευτικών δραστηριοτήτων με χρήση αποκεντρωμένης
  εφαρμογής
- Ακριβέστερη καταγραφή της μαθησιακής πορείας με αποτίμηση της μαθησιακής δραστηριότητας με επιπρόσθετες μετρικές πέρα των μαθησιακών αποτελεσμάτων σε τακτά χρονικά διαστήματα
- Μαθησιακή αναλυτική (learning analytics) και παιχνιδοποίηση (gamification) για την σύνδεση μετρικών με μαθησιακά αποτελέσματα και αποκτώμενες γνώσεις, ικανότητες

και δεξιότητες, με σκοπό την υποστήριξη και ενίσχυση της προαναφερθείσας παρακολούθησης, καταχώρησης, επαλήθευσης και αποτίμησης

- Διασφάλιση της διαλειτουργικότητας των μαθησιακών εργαλείων μέσω διεθνών προτύπων

4.13 Λύση ψηφιακών πιστοποιητικών της Oracle

Αντιμέτωποι με ταχέως μεταβαλλόμενους δημογραφικούς και οικονομικούς παράγοντες και τις προσδοκίες των φοιτητών, οι τρέχουσες διαδικασίες για την έκδοση και την επαλήθευση των φοιτητικών πιστοποιητικών είναι πολύ αναποτελεσματικές και χρονοβόρες. Συχνά,επίσης μπορούν να οδηγήσουν σε δόλιες ή πλαστές πιστοποιήσεις.Η Λύση Ψηφιακών Πιστοποιητικών της Oracle, που βασίζεται στην πλατφόρμα Oracle Blockchain (βασισμένη στο Hyperledger Fabric), παρέχει μια ολοκληρωμένη, από άκρο σε άκρο λύση στα εκπαιδευτικά ιδρύματα,να εκδίδουν επαληθεύσιμη απόδειξη παραβίασης και ασφαλής πιστοποίησης που βελτιώνει την εμπειρία των φοιτητών μετά την αποφοίτηση καθώς και τη λειτουργική απόδοση. Η λύση που προτείνει η Oracle δίνει τη δυνατότητα στα ιδρύματα να εκδίδουν ψηφιακά πιστοποιητικά αλλά και να παρέχουν αυτοδύναμη δυνατότητα στους φοιτητές ώστε να μπορούν να τα μοιραστούν με ασφάλεια με τρίτους μέσω διακριτικού πρόσβασης.Αυτή η λύση έχει αναπτυχθεί επιτυχώς στην παραγωγή από πελάτες όπως η China Distance Education Holdings Limited (CDEL) και το Πανεπιστήμιο Taibah Valley. Το CDEL χρησιμοποιεί το Oracle Blockchain για να μοιράζεται εκπαιδευτικά αρχεία και επαγγελματικές πιστοποιήσεις με πολλά εκπαιδευτικά ιδρύματα για να βοηθήσει τους εργοδότες και τους ανθρώπους που ασχολούνται με τις προσλήψεις να επαληθεύσουν τα εκπαιδευτικά διαπιστευτήρια που διεκδικούν τα άτομα.Πολλά άλλα ιδρύματα όπως τα εθνικά πανεπιστήμια, οι οργανισμοί απασχόλησης, οι κυβερνητικοί οργανισμοί, οι ακαδημίες επαγγελματικών δεξιοτήτων και τα πανεπιστήμια που παρέχουν υποτροφίες / υποτροφίες χρησιμοποιούν τη λύση αυτή ως μέρος πιλοτικών προγραμμάτων που βρίσκονται σε εξέλιξη ή έχουν προγραμματιστεί.

4.14 TrueRec Ινστιτούτο SAP

Στο πλαίσιο της συνεχιζόμενης καινοτομίας του γύρω από το blockchain, το SAP Innovation Center Network παρουσίασε το TrueRec, ένα ασφαλές και αξιόπιστο ψηφιακό πορτοφόλι για την αποθήκευση επαγγελματικών και ακαδημαϊκών διαπιστευτηρίων.Αυτά τα διαπιστευτήρια θα μπορούσαν να περιλαμβάνουν οτιδήποτε από ταυτότητες, όπως διαβατήριο, άδεια οδήγησης

ή ταυτότητα ψηφοφόρου, έως εκπαιδευτικά διαπιστευτήρια όπως πανεπιστημιακά πτυχία και πιστοποιητικά εργασίας.Όπως γνωρίζουμε, οι πιστοποιήσεις δεν είναι πάντα εύκολο να επαληθευτούν. Μπορούν εύκολα να παραποιηθούν, να κλαπούν ή να χαθούν, και είναι κουραστικά όσον αφορά τον έλεγχο ταυτότητας. Ένας πιλότος, για παράδειγμα, πρέπει να επικυρώνει συχνά την άδειά του ή ένας υποψήφιος εργοδότης πρέπει να ξεκινήσει μακροχρόνιους ελέγχους ιστορικού για να επαληθεύσει τα διαπιστευτήρια ενός υποψηφίου.Σε έναν κόσμο όπου η κλοπή ταυτότητας είναι μια πολύ πραγματική απειλή, το TrueRec, μία από τις πρώτες εφαρμογές blockchain της SAP που επιτρέπει στους χρήστες να διατηρούν την αποκλειστική ιδιοκτησία των πληροφοριών τους, να αποδεικνύουν εύκολα τη νομιμότητα των διαπιστευτηρίων τους, να τα συλλέγουν σε μια κεντρική τοποθεσία και να τα μοιράζονται με ασφάλεια με το καθένα ενδιαφερόμενο.Το TrueRec επίσης δεν αποθηκεύει το πιστοποιητικό,το πιστοποιητικό μπορεί να αποθηκευτεί όπου θέλουμε, για παράδειγμα, στο τηλέφωνό μας. Υπάρχει η δυνατότητα προβολής του αρχείου TRU στην εφαρμογή TrueRec και ο διαμοιρασμός του εύκολα από την εφαρμογή με τον τρέχοντα εργοδότη , άλλα ιδρύματα ή όποιον επιλεχθεί οποτεδήποτε, οπουδήποτε. Τα διαπιστευτήριά μπορούν να επαληθευτούν συγκρίνοντας απλά τα έγγραφα με τον κατακερματισμό στο blockchain.Το TrueRec τροφοδοτείται από το Ethereum, μια ανοιχτού κώδικα, δημόσια, πλατφόρμα κατανεμημένης υπολογιστικής που διαθέτει λειτουργίες έξυπνης σύμβασης (scripting), η οποία διευκολύνει τις διαδικτυακές συμβατικές συμφωνίες.Το TrueRec διατέθηκε πρόσφατα σε οποιονδήποτε εγγράφηκε στο "Touch IoT course for SAP Leonardo" που προσφέρεται από το openSAP, μια διαδικτυακή πλατφόρμα εκμάθησης και πάροχο μαζικών ανοιχτών διαδικτυακών μαθημάτων (MOOCs). Πάνω από 4500 μαθητές που είναι εγγεγραμμένοι στο μάθημα "Touch IoT" έχουν λάβει και μπορούν να διαχειριστούν την πιστοποίησή τους για το μάθημα μέσω του TrueRec.

4.15 Hyperledger Indy

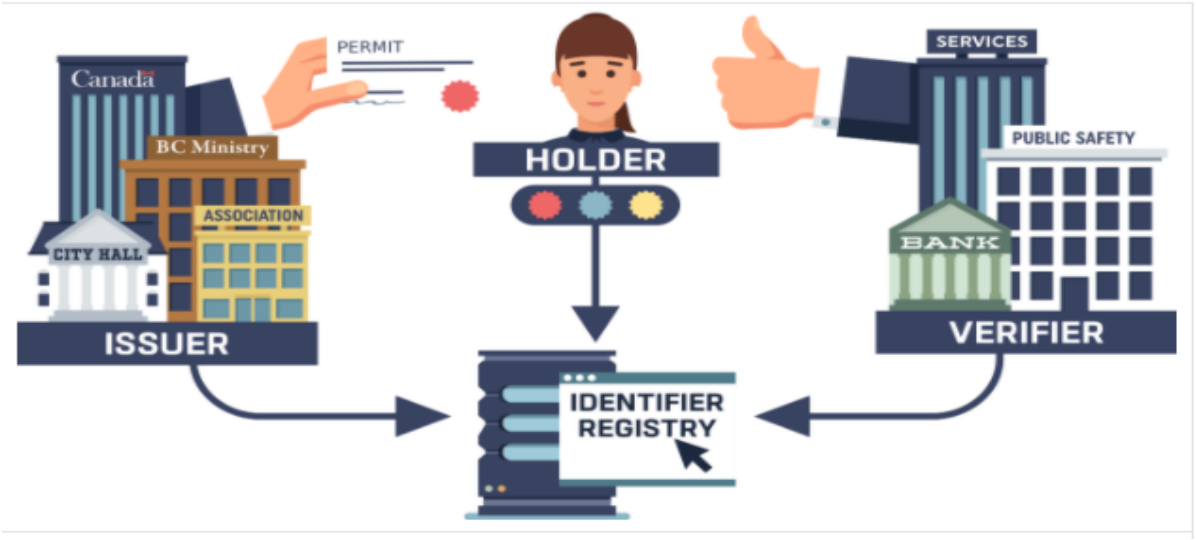
Το Hyperledger Indy σχεδιάστηκε και κατασκευάστηκε από την Sorvin foundation,η οποία διαχειρίζεται ένα ψηφιακό κατανεμημένο δίκτυο ταυτότητας που βασίζεται σε αυτό.Το Hyperledger Indy είναι ένα σύστημα βασισμένο σε blockchain,σχεδιάστηκε για να λειτουργεί έτσι ώστε να είναι δημόσιο δηλαδή όλοι να μπορούν να δουν τα περιεχόμενα του blockchain, αλλά με άδεια που σημαίνει ότι μόνο προεγκεκριμένοι συμμετέχοντες γνωστοί ως «Stewards» μπορούν να συμμετέχουν στην διαδικασία επικύρωσης.Το Indy είναι πολύ διαφορετικό από τα άλλα συστήματα Hyperledger,ενώ όλα τα άλλα πρότζεκτ blockchain είναι γενικής χρήσης(μπορούν να χρησιμοποιηθούν σε πολλές περιπτώσεις), το Hyperledger Indy χρησιμοποιείται για έναν μόνο σκοπό, την αποκεντρωμένη ταυτότητα στο διαδίκτυο ,έχει

σχεδιαστεί ώστε να μπορεί να αποδείξει στους άλλους ποιος είσαι και να είσαι σίγουρος εσύ ποιοι είναι.Ποια είναι όμως η μεγάλη υπόθεση για την ταυτότητα; Λοιπόν, όταν δημιουργήθηκε για πρώτη φορά το Διαδίκτυο, όλοι οι υπολογιστές που συνδέονταν μεταξύ τους ήταν «αξιόπιστοι».Ο αριθμός των συστημάτων ήταν μικρός και οι άνθρωποι που τρέχανε αυτά τα συστήματα γνώριζαν ο ένας τον άλλον, οπότε δεν χρειάζονταν μηχανισμούς για να γνωρίζουν ποιος έστειλε τι δεδομένα μεταξύ των συστημάτων. Καθώς ο αριθμός των συστημάτων στο Διαδίκτυο μεγάλωνε ,αυτή η εμπιστοσύνη μειώθηκε γρήγορα και ήταν ο πρώτος από πολλούς μηχανισμούς που προστέθηκε στα συστήματα για να προσδιορίσει ποιος επικοινωνεί με ποιον. Δυστυχώς, το πρόβλημα δεν επιλύθηκε ποτέ. Το πιο συνηθισμένο (και παγκοσμίως μισητό) σύστημα, εκείνο των κωδικών χρήστη και κωδικών πρόσβασης, είναι γεμάτο με προβλήματα.Η προκύπτουσα έλλειψη βεβαιότητας για το ποιος είναι στο άλλο πληκτρολόγιο έχει οδηγήσει σε απώλεια δισεκατομμυρίων από, παραβιάσεις δεδομένων, κλοπή ταυτότητας, απάτες και άλλα. Επιπλέον, η ίδια έλλειψη βεβαιότητας έχει καταστήσει αδύνατο πολλούς τύπους επιχειρηματικών συναλλαγών στο Διαδίκτυο καθώς ο κίνδυνος είναι πολύ υψηλός.Το Hyperledger Indy δημιουργήθηκε για να προσθέσει ένα επίπεδο ταυτότητας στο Διαδίκτυο χρησιμοποιώντας έναν μηχανισμό που είναι εύχρηστος, επιτρέπει την εμπιστοσύνη στο διαδίκτυο και ενισχύει το απόρρητο. Είναι ένας μεγάλος στόχος που έχει ζωτική σημασία για όλους στο Διαδίκτυο,και ένας στόχος που έγινε πρόσφατα πραγματικότητα με την έλευση του blockchain.Το Indy υποστηρίζει επίσης το αναδυόμενο πρότυπο το W3C για αποκεντρωμένα αναγνωριστικά(DID). Οι ταυτότητες αποθηκεύονται ως αποκεντρωμένα αναγνωριστικά(DID),όπως ορίζεται από το πρότυπο του W3C.Τα DID είναι παγκοσμίως μοναδικά αποκεντρωμένα αναγνωριστικά που δημιουργούνται από τον κάτοχο τους,ανεξάρτητα από οποιαδήποτε κεντρική αρχή.Κάθε DID έχει συσχετιστεί με ένα ή περισσότερα δημόσια κλειδιά που δημιουργήθηκαν από τον κάτοχο του(και ο κάτοχος κατέχει τα αντίστοιχα ιδιωτικά κλειδιά) και ένα ή περισσότερα τελικά σημεία.Ένα DID μπορεί να επιλυθεί με ένα μοναδικό τρόπο(όπως μια διεύθυνση URL) για την επιστροφή των δεδομένων(δημόσια κλειδιά και τελικά σημεία) που σχετίζονται με το DID.Το Indy χρησιμοποιεί το DID,για τη δημιουργία συνδέσεων μεταξύ δύο ταυτοτήτων,όπως ενός χρήστη και ενός ιστότοπου μιας υπηρεσίας,ώστε να μπορούν να επικοινωνούν με ασφάλεια.Ένα παράδειγμα τρόπου με τον οποίο χρησιμοποιούνται τα DID:ένας χρήστης εγγράφεται στον ιστότοπο μιας υπηρεσίας δημιουργώντας και δίνοντας στην υπηρεσία ένα νέο που δεν χρησιμοποιήθηκε ποτέ πριν DID και λαμβάνει από την υπηρεσία το ίδιο πράγμα ένα νέο που δεν χρησιμοποιήθηκε ποτέ πριν DID από την υπηρεσία.Καθένα καταγράφει τη «σχέση» DID έτσι ώστε όταν κάποιος θέλει να επικοινωνήσει με τον άλλο,έχουν ένα τελικό σημείο για την αποστολή του μηνύματος και ένα δημόσιο κλειδί για την κρυπτογράφηση του μηνύματος από

άκρη σε άκρη.Αργότερα,όταν ο χρήστης επιστρέψει στον ιστότοπο για να συνδεθεί, ο χρήστης και η υπηρεσία ανταλλάσσουν κρυπτογραφημένα μηνύματα για να επιβεβαιώσουν ότι ο καθένας διατηρεί το ιδιωτικό κλειδί για την αποκρυπτογράφηση των μηνυμάτων. Μετά την ολοκλήρωση, η υπηρεσία γνωρίζει ότι είναι ο χρήστης, επειδή ο χρήστης χρησιμοποίησε το DID του και ο χρήστης γνωρίζει ότι είναι η υπηρεσία επειδή η υπηρεσία χρησιμοποίησε το DID της.Τακτοποιημένα έτσι αντιμετωπίζεται μια από τις προκλήσεις που τίθενται με τη ταυτότητα του διαδικτύου,αυτή της αμφίδρομης επαλήθευσης.Πέραν των πολλών προβλημάτων τα οποία λύνουν τα DID όσον αφορά την ταυτότητα στο διαδίκτυο είναι αναγκαίο να γνωρίζουμε ποιος δημιούργησε το DID και με κάποιο τρόπο να επαληθεύεται η ταυτότητά του,για αυτό δημιουργήθηκαν τα επαληθεύσιμα διαπιστευτήρια.Τα επαληθεύσιμα διαπιστευτήρια (VC Verifiable Credentials), επιτρέπουν έναν αξιόπιστο τρόπο για την παροχή χαρακτηριστικών ταυτότητας για εμάς.Τα διαπιστευτήρια είναι πράγματα όπως άδειες οδήγησης, διαβατήρια ή πτυχία πανεπιστημίου που μας δίνονται από μια αρχή έκδοσης που μπορούμε να χρησιμοποιήσουμε για να τα δείξουμε σε άλλους όταν χρειαστεί. Τα VC είναι ψηφιακά ισοδύναμα διαπιστευτηρίων χαρτιού που υποβάλλονται σε κρυπτογραφική επεξεργασία έτσι ώστε όταν τα εμφανίζουμε ("αποδεικνύουμε") τις αξιώσεις (στοιχεία δεδομένων από τα διαπιστευτήρια), ο δέκτης ("Επαληθευτής") να μπορεί να είναι βέβαιος.

- Ποιος εξέδωσε τις αξιώσεις
- Ότι οι αξιώσεις εκδόθηκαν στην ταυτότητα που τις παρουσίαζε
- Ότι οι ισχυρισμοί δεν έχουν αλλοιωθεί
- Ότι το διαπιστευτήριο των αξιώσεων δεν έχει ανακληθεί από τον εκδότη

Όπως δείχνει η παρακάτω εικόνα, η ροή δεδομένων για επαληθεύσιμα διαπιστευτήρια είναι η ίδια με εκείνη των έντυπων εγγράφων - Οι εκδότες παρέχουν επαληθεύσιμα διαπιστευτήρια στον κάτοχο και ο κάτοχος μπορεί να τα αποδείξει στους επαληθευτές ανά πάσα στιγμή.



Εικόνα 24:Hyperledger Indy

Τα αιτήματα απόδειξης και τα αποδεικτικά στοιχεία στο Indy είναι συναλλαγές που πραγματοποιούνται μεταξύ του κατόχου του VC και του επαληθευτή. Ο εκδότης του VC δεν εμπλέκεται στη διαδικασία απόδειξης,ένα πολύ σημαντικό χαρακτηριστικό του μοντέλου VC. Δεν θέλουμε (για παράδειγμα) την κυβέρνηση να γνωρίζει κάθε φορά που χρησιμοποιούμε την άδεια οδήγησης για να αποδείξουμε την ηλικία μας. Τέλος αξίζει να σημειωθεί ότι παρόλο που το Indy έχει σχεδιαστεί για να λειτουργεί ως δημόσιο δίκτυο,μια παρουσία του Indy (ή οποιουδήποτε άλλου δημοσίου blockchain),θα μπορούσε να εκτελεστεί ως ιδιωτικό δίκτυο προσβάσιμο μόνο σε όσους χρησιμοποιούν το δίκτυο.

4.16 Δίπλωμα Qualichain

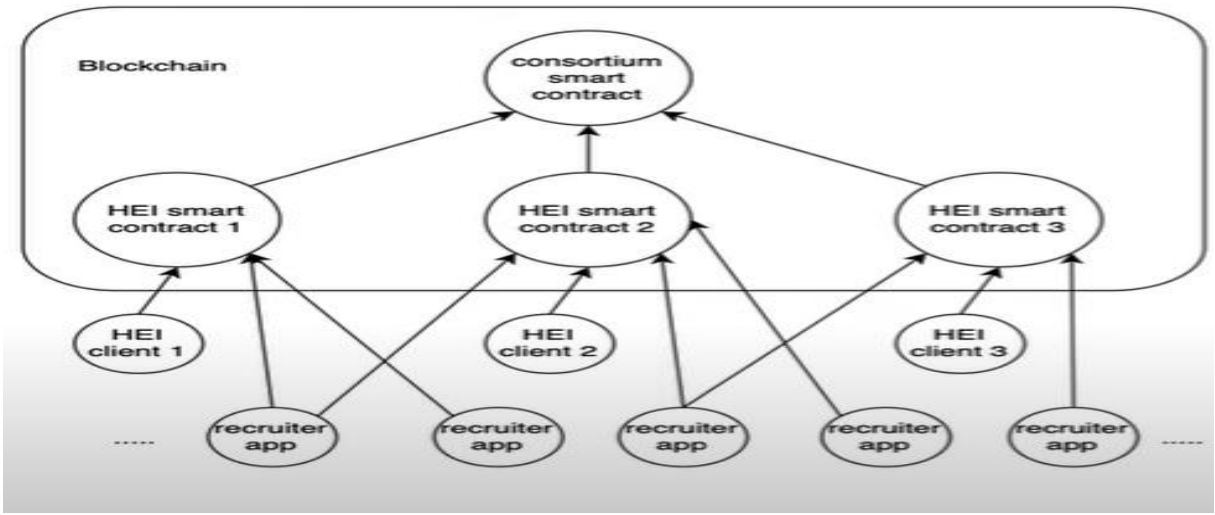
Με τη βοήθεια διάφορων συνεργαζόμενων εταιρειών από την Ευρώπη αλλά και της Ευρωπαϊκής επιτροπής ξεκίνησε το πρότζεκτ Qualichain μια πτυχή του οποίου αφορούσε τη δια βίου μάθηση με σκοπό την αντιμετώπιση του προβλήματος των πλαστών πιστοποιητικών.Ως αποτέλεσμα των ανωτέρω έχει προταθεί ένα οικοσύστημα που στηρίζεται στη τεχνολογία blockchain,η πλατφόρμα «δίπλωμα Qualichain»,η οποία βοηθάει ώστε η διαδικασία έκδοσης ή επαλήθευσης πιστοποιητικών που θέλει να κάνει ο εκάστοτε ενδιαφερόμενος να γίνεται ηλεκτρονικά χωρίς να απαιτείται επικοινωνία με τον εκάστοτε φορέα έκδοσης ούτε η διατήρηση του πιστοποιητικού σε έντυπη μορφή.Αυτό το οικοσύστημα στηρίζεται σε ένα χωρίς άδεια(permissionless) blockchain το Ethereum.Η πλατφόρμα που έχει προταθεί πρόκειται για ένα οικοσύστημα από κοινοπραξίες(consortium) από ανώτερα εκπαιδευτικά ιδρύματα.Το οικοσύστημα αυτό πιθανό να απαρτίζεται από περισσότερες από μια κοινοπραξίες και βασίζεται σε δύο έξυπνα συμβόλαια 1)ένα που διαχειρίζεται τις

κοινοπραξίες,2)ένα που αποθηκεύει τους κατακερματισμούς πιστοποιητικών κάθε ανώτατου εκπαιδευτικού ιδρύματος.Τα δύο αυτά έξυπνα συμβόλαια περιγράφονται στη συνέχεια.

Το έξυπνο συμβόλαιο κοινοπραξίας:για τα εκπαιδευτικά ιδρύματα ώστε να διαχειριστούν την συμμετοχή στην κοινοπραξία και στους υπεύθυνους των προσλήψεων να λάβουν τη διεύθυνση του έξυπνου συμβολαίου του εκπαιδευτικού ιδρύματος(επιτρέπει στα ανώτερα εκπαιδευτικά ιδρύματα να συμμετέχουν στην κοινοπραξία είτε να φύγουν από την κοινοπραξία,αλλά και στους υπεύθυνους προσλήψεων να ελέγξουν την αυθεντικότητα του πιστοποιητικού).Παράδειγμα:νέο εκπαιδευτικό ίδρυμα συμμετέχει στη κοινοπραξία,πρέπει να ακολουθηθεί το παρακάτω πρωτόκολλο.

- Το καινούργιο εκπαιδευτικό ίδρυμα αναπτύσσει ένα έξυπνο συμβόλαιο
- Το καινούργιο εκπαιδευτικό ίδρυμα καλεί τη συνάρτηση της Solidity registerHEI(id,address)
- Τα μέλη της κοινοπραξίας καλούν τη συνάρτηση voteRegisterHEI(myId,id) για να υποστηρίξουν τη συμμετοχή.
- Η διαδικασία της καταγραφής του εκπαιδευτικού ιδρύματος πραγματοποιείται όταν και αν η διαδικασία της ψηφοφορίας φθάσει το επιθυμητό κατώφλι που έχει τεθεί.

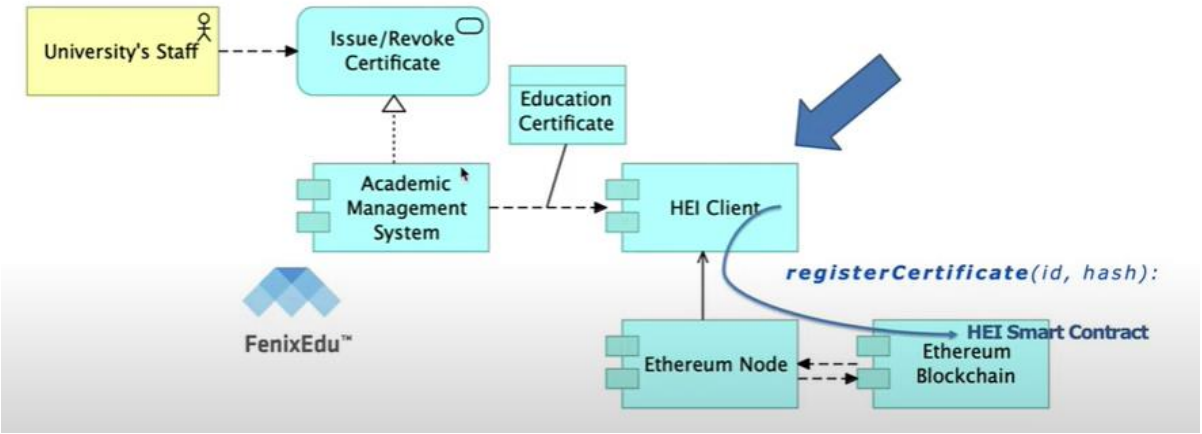
Το έξυπνο συμβόλαιο του ανώτερου εκπαιδευτικού ιδρύματος: το οποίο ανήκει στο ανώτερο εκπαιδευτικό ίδρυμα. Μια περιγραφή της αρχιτεκτονικής του οικοσυστήματος παρουσιάζεται παρακάτω.



Εικόνα 25:Αρχιτεκτονική οικοσυστήματος Qualichain Diploma

Ο πελάτης του ανώτερου εκπαιδευτικού ιδρύματος(HEI Client):για την καταγραφή και την ανάκληση του πιστοποιητικού.Το εκπαιδευτικό ίδρυμα εκτελεί το HEI Client και μόλις το

εκτελεί αυτό βάζει το πιστοποιητικό στο έξυπνο συμβόλαιο του εκπαιδευτικού ιδρύματος στο Ethereum blockchain.

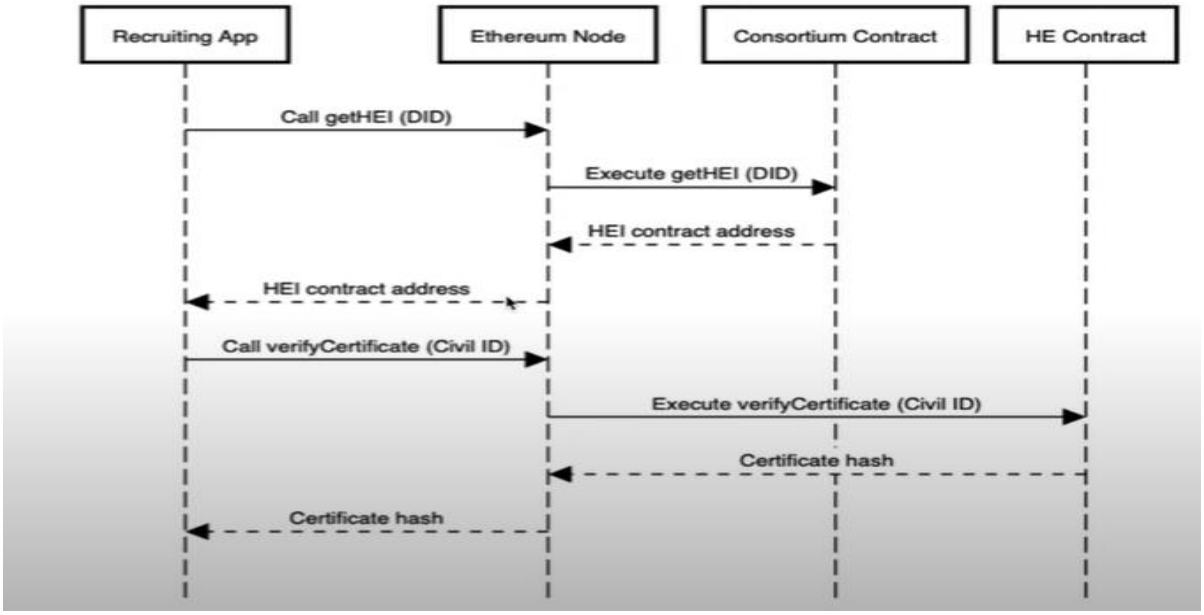


Εικόνα 26:Περιγραφή του HEI Client

Κύριε λειτουργίες των έξυπνων συμβολάιων των εμπλεκόμενων μερών:

- Για το έξυπνο συμβόλαιο κοινοπραξίας η καταγραφή,η διαγραφή ενός εκπαιδευτικού ιδρύματος στη κοινοπαραξία και η κλήση του για να πάρουμε τη διεύθυνση του με τις αντίστοιχες εντολές στη γλώσσα Solidity για τα έξυπνα συμβόλαια.
- Για το έξυπνο συμβόλαιο του ανώτερου εκπαιδευτικού ιδρύματος:η καταγραφή ενός πιστοποιητικού στο blockchain αποθηκεύοντας το κρυπτογραφικό κατακερματισμό του,η ανάκληση του πιστοποιητικού και η διαδικασία επαλήθευσης του για να ελεγχθεί εάν ένα πιστοποιητικό έχει ανακληθεί. Κάθε κοινοπραξία διαχειρίζεται από ένα έξυπνο συμβόλαιο και οι αποφάσεις παίρνονται μετά από ψηφοφορία των μελών με βάση ένα κατώφλι(threshold) το οποίο έχει οριστεί.
- Η διαδικασία της επαλήθευσης από τον υπεύθυνο προσλήψεων. Ο υπεύθυνος προσλήψεων αλληλοεπιδρά με δύο έξυπνα συμβόλαια για να εξακριβώσει την

αυθεντικότητα του πιστοποιητικού.Στην εικόνα παρακάτω περιγράφεται όλη η διαδικασία για την επαλήθευση της αυθεντικότητας του πιστοποιητικού.



Εικόνα 27:Διαδικασία επαλήθευσης αυθεντικότητας πιστοποιητικού

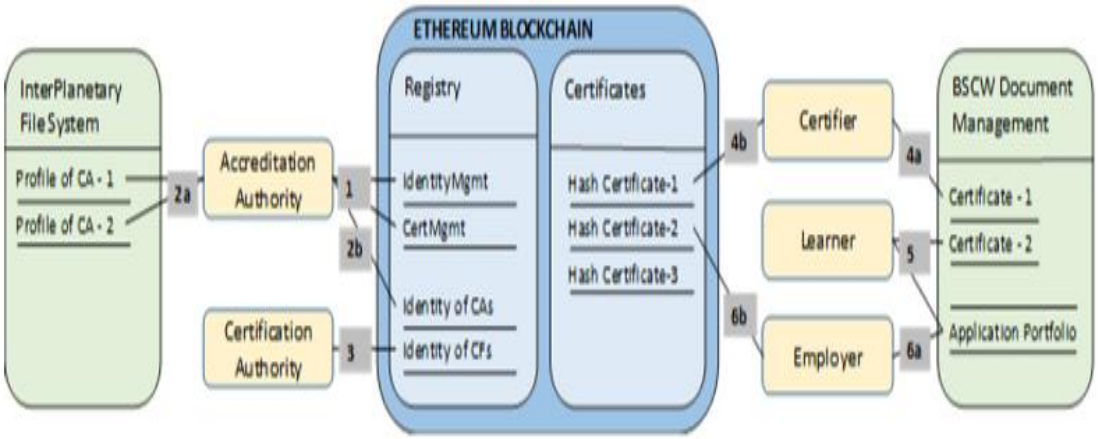
4.17 LinkChain

Το LinkChain είναι μια συνδεδεμένη πλατφόρμα δεδομένων με χρήση της τεχνολογίας Blockchain που απευθύνεται σε εκδότες δεδομένων και καταναλωτές(συμπεριλαμβανομένων όλων των ενδιαφερομένων στην εκπαίδευση και την απασχόληση, μεταξύ άλλων) που παρέχει πιστοποιητικό επαλήθευσης ισοδυναμίας, έλεγχο διαπιστευτηρίων και επαλήθευση, ενώ υποστηρίζει πολυγλωσσικές δυνατότητες επίσης.

Το LinkChain είναι μια πολλά υποσχόμενη πλατφόρμα υπό ανάπτυξη που συνδυάζει τη δύναμη της σημασιολογίας και του blockchain. Περιλαμβάνει μια ποικιλία λειτουργιών για επαλήθευση πιστοποιητικών και διαπιστευτηρίων υποστηρίζοντας επίσης εξωτερικές αναλύσεις που μπορούν να χρησιμοποιηθούν για την ανάλυση προσόντων, την ικανότητα ανάπτυξης και άλλα καθήκοντα που σχετίζονται με το ανθρώπινο δυναμικό. Η πλατφόρμα θα υποστηρίζει πολλές γλώσσες γεγονός που την κάνει έτοιμη να εφαρμοστεί σε όλη την ΕΕ.

4.18 Blockchain for education

Το Blockchain για την εκπαίδευση,επιτρέπει στους φοιτητές να παρουσιάσουν τα ψηφιακά τους πιστοποιητικά και να υποστηρίξουν τις αρχές πιστοποίησης στη διαχείριση και αρχειοθέτηση ψηφιακών πιστοποιητικών. Το εργαλείο χρησιμοποιείται ήδη για πιστοποίηση μαθημάτων Fraunhofer και είναι διαθέσιμο ως πρότυπο ανοιχτού κώδικα για επαναχρησιμοποίηση και επέκταση.Το εργαλείο και η πλατφόρμα βασίζονται στο Ethereum blockchain για να επιτρέψουν την αρχειοθέτηση των πιστοποιητικών και την σωστή και μόνιμη κατανομή τους στους μαθητές. Το υπάρχον εργαλείο βασίζεται σε Open Badges και χρησιμοποιεί JSON / JSON-LD για μεταδεδομένα και ως βάση για την αναζήτηση (σκοπούς επαλήθευσης)Η βασική αρχιτεκτονική του Blockchain για την εκπαίδευση παρουσιάζεται στην εικόνα παρακάτω.



Εικόνα 28:Αρχιτεκτονική του Blockchain4Education

Όπως φαίνεται και παραπάνω το IPFS(Interplanetary File System) για την αποθήκευση προφίλ των αρχών πιστοποίησης και το σύστημα διαχείρισης εγγράφων BSCW για να αποθηκεύει ψηφιακά πιστοποιητικά αντιπροσωπεύονται ως εκτεταμένα Open Badges.Το BSCW υποστηρίζει τις αρχές πιστοποίησης στη διαχείριση των πιστοποιητικών και τους εκπαιδευόμενους στην οργάνωση και τη κοινή χρήση χαρτοφυλακίων εφαρμογών.Οι εργοδότες υποστηρίζονται από μια υπηρεσία επαλήθευσης για ψηφιακά πιστοποιητικά. Έχουν αναπτυχθεί δύο έξυπνα συμβόλαια σε Solidity.Σε μια εξελισσόμενη διαδικασία, τα έξυπνα συμβόλαια IdentityMgmt και CertMgmt γράφονται στο blockchain Ethereum από την αρχή διαπίστευσης. Μετά από αυτό, η αρχή διαπίστευσης μπορεί να καταχωρήσει τα προφίλ των αρχών πιστοποίησης και ταυτόχρονα τις αντίστοιχες ταυτότητές τους στο blockchain. Οι φορείς πιστοποίησης συλλέγουν όλες τις απαραίτητες πληροφορίες, υπογράφουν και εκδίδουν τα πιστοποιητικά.Τα πιστοποιητικά αποθηκεύονται στο σύστημα διαχείρισης εγγράφων

BSCW και το δακτυλικό τους αποτύπωμα είναι γραμμένο στο Ethereum blockchain. Οι σπουδαστές λαμβάνουν τα πιστοποιητικά τους και μπορούν να δημιουργήσουν χαρτοφυλάκια εφαρμογών που θα μπορούσαν να κοινοποιηθούν σε πιθανούς εργοδότες. Οι εργοδότες χρησιμοποιούν μια υπηρεσία επαλήθευσης για να ελέγξουν την αυθεντικότητα των πιστοποιητικών.

4.19 Σύνοψη

Στο κεφάλαιο αυτό, παρουσιάστηκαν μια επεξήγηση οι πιο σημαντικές πρωτοβουλίες blockchain στο τομέα της επαλήθευσης πιστοποιητικών, όπου φάνηκαν τα σημαντικά πλεοντεκτήματα που προσφέρει στην όλη διαδικασία

Στη συνέχεια σε κάποιες περιπτώσεις αναλύθηκαν τα δομικά μέρη της εκάστοτε λύσης ώστε να εξηγηθεί ο τρόπος λειτουργίας της.Ιδιαίτερη έμφαση δόθηκε στη περιγραφή του μηχανισμού συναίνεσης που ακολουθεί η εκάστοτε πρωτοβουλία καθώς και το είδος blockchain που χρησιμοποιεί.

Με την ολοκλήρωση αυτού του κεφαλαίου, γίνονται αντιληπτά κάποια κενά ασφαλείας τα οποία παρουσιάζει η τεχνολογία μέχρι στιγμής στις διάφορες λύσεις τα οποία είναι αμελητέα σε σχέση με την δυνατότητα της αποκεντρωμένης ταυτότητας που αυτή παρέχει γεγονός που την κάνει συνεχώς να αναπτύσσεται.

Κεφάλαιο 5:Εφαρμογές της τεχνολογίας blockchain στην εκπαίδευση

5.1 Εισαγωγή

Σε προηγούμενο κεφάλαιο,αναφέρθηκαν οι σημαντικότερες πρωτοβουλίες με χρήση του blockchain στην έγκριση πιστοποιητικών καθώς και πλατφόρμες που αναπτύχθηκαν για τον ίδιο λόγο.

Σε αυτό το κεφάλαιο,γίνεται μια εκτενής αναφορά σε πανεπιστήμια τα οποία ήδη έχουν χρησιμοποιήσει πιλοτικά ή μη τις πλατφόρμες. Τέλος,αναφέρονται κάποια θετικά και αρνητικά από τη ήδη υπάρχουσα χρήση

5.2 Πανεπιστήμιο της Λευκωσίας(UNIC)

Το Πανεπιστήμιο της Λευκωσίας (UNIC) ανήκει στη σειρά «πρωταθλητών» στη δέσμευσή του να μεγιστοποιήσει τις δυνατότητες του blockchain στην εκπαίδευση. Το UNIC θεωρείται το πρώτο πανεπιστήμιο που δέχεται το Bitcoin για δίδακτρα για οποιοδήποτε πρόγραμμα σπουδών στο πανεπιστήμιο (Οκτώβριος 2013) και διδάσκει μάθημα κρυπτοαναλογιστικών σπουδών πανεπιστημιακού επιπέδου, το οποίο παραδόθηκε με MOOC και τίτλο «Εισαγωγή στα ψηφιακά νομίσματα» (Ιανουάριος 2014). Επιπλέον, προσφέρει ένα διαπιστευμένο πανεπιστημιακό πτυχίο, Master of Science σε ψηφιακό νόμισμα, που διδάσκεται ηλεκτρονικά στα αγγλικά (Μάρτιος 2014 με τους πρώτους σπουδαστές να αποφοιτούν τον Ιούνιο του 2016). Τέλος, εκδίδει ακαδημαϊκά πιστοποιητικά στο Bitcoin blockchain, χρησιμοποιώντας τη δική του πλατφόρμα λογισμικού (Σεπτέμβριος 2014). Σύμφωνα με τον Αντώνη Πολεμητή, Διευθύνοντα Σύμβουλο του UNIC στις ASU GSV Summit το 2017 και τους συντονιστές της Πρωτοβουλίας Blockchain, καθηγήτρια Soulla Louca και καθηγητή George Giaglis, το UNIC θεωρεί την τεχνολογία Blockchain ως ακρογωνιαίο λίθο της στρατηγικής και στοιχείο διαφοροποίησης από άλλα ιδρύματα τριτοβάθμιας εκπαίδευσης. Παρόλο που το εισαγωγικό

δωρεάν MOOC για τα ψηφιακά νομίσματα του UNIC δεν είναι μοναδικό, τοποθετείται ως το πρώτο μάθημα του MSc στο ψηφιακό νόμισμα. Οι συνιστώσες του MSc με τη σειρά τους επανασυγκεντρώνονται σε επαγγελματικά προγράμματα πιστοποίησης τύπου blockchain, τα οποία μεταφέρονται σε CPD και ECTS. Τον Σεπτέμβριο του 2017, ξεκίνησε η όγδοη έκδοση του MOOC. Μέχρι σήμερα, το MOOC έχει προσελκύσει σπουδαστές από 80 διαφορετικές χώρες και έχει δείξει καλά ποσοστά ολοκλήρωσης. Το περιεχόμενο του μαθήματος φιλοξενείται από το UNIC και συνεχίζει να εξελίσσεται λόγω της δικτύωσης του πανεπιστημίου στην παγκόσμια εκπαιδευτική κοινότητα. Το ερευνητικό κέντρο Blockchain τοποθετείται ως κέντρο παγκόσμιας κλάσης για τις αναδυόμενες τεχνολογίες, οι οποίες θα ενσωματώσουν, θα διευρύνουν το πεδίο εφαρμογής και θα ενισχύσουν την διεπιστημονική έρευνα που έχει ήδη πραγματοποιηθεί σε αυτόν τον εξελισσόμενο τομέα.

5.3 Δημοκρατία της Μάλτας

Έχοντας τη πεποίθηση ότι η τεχνολογία blockchain μπορεί να μεταμορφώσει τα εκπαιδευτικά συστήματα,η Μάλτα άρχισε να συνεργάζεται με τη Learning Machine Technologies από το 2017 σε ένα δοκιμαστικό έργο που επιτρέπει στους φοιτητές τριτοβάθμιας εκπαίδευσης και επαγγελματικής εκπαίδευσης να έχουν πρόσβαση και να ανακτούν εκπαιδευτικά αρχεία μέσω της τεχνολογίας blockchainΜέσω του Υπουργείου Παιδείας της και Απασχόλησης, η Μάλτα είναι η πρώτη που εφαρμόζει διαπιστευτήρια που βασίζονται σε blockchain χρησιμοποιώντας ένα Ομοσπονδιακό Εκδοτικό Σύστημα.

Το σύστημα αυτό τους παρέχει μια αναλυτική εικόνα της προόδου τους στον εκπαιδευτικό τομέα.Επίσης,επιτρέπει στους μαθητές της Μάλτας και στο εργατικό δυναμικό να έχουν τα αρχεία τους για τη διά βίου μάθηση σε ένα χώρο αποθήκευσης ,να αποδεικνύουν την ιδιοκτησία τους ,καθώς και να τα μοιράζονται με οποιονδήποτε από οπουδήποτε στον κόσμο δωρεάν.Αυτό έχει ως αποτέλεσμα να εξοικονομεί χρόνο και χρήμα στους εργοδότες κατά τη διάρκεια της επαλήθευσης,βοηθάει τα ιδρύματα να περιορίσουν την απάτη και να σώσουν τις επωνυμίες τους από ζημιές στη φήμη.Από το 2018 αρκετά ιδρύματα στη Μάλτα ονομαστικά:το Ινστιτούτο Τουριστικών Σπουδών(ITS),η Εθνική Επιτροπή για Ανώτατη και Ανώτερη Εκπαίδευση(NCFHE),το κολλέγιο Τεχνών,Επιστημών και Τεχνολογίας της Μάλτας(MCAST) και το Υπουργείο Παιδείας και Απασχόλησης(MEDE),εξέδωσαν πιστοποιητικά σε τέσσερα δευτεροβάθμια σχολεία.

5.4 Κοινοτικό Κολέγιο Κεντρικού Νέου Μεξικού(Central New Mexico Community College)

Κανένα άλλο κοινοτικό κολέγιο δεν έχει εκδώσει ασφαλή ψηφιακά διπλώματα σε φοιτητές εκτός από το Κοινοτικό κολέγιο του Νέου Μεξικού.Το Δεκέμβριο του 2017 το κολέγιο εξέδωσε ψηφιακά πιστοποιητικά στους απόφοιτους των Ingenuity προγραμμάτων τους μέσω της εφαρμογής Blockcerts mobile.Μέχρι τη θερινή περίοδο τον ίδιο χρόνο,περίπου 300 διπλώματα είχαν εκδοθεί στους φοιτητές του Ingenuity.Έπειτα,το κολέγιο προχώρησε σε εκμετάλλευση των ψηφιακών πιστοποιητικών στα διάφορα προγράμματα του και τον Αύγουστο του 2018,όλοι οι φοιτητές είχαν την επιλογή να λάβουν τα πιστοποιητικά μέσω της εφαρμογής Blockcert.

5.5 Πολυτεχνική Σχολή Σιγκαπούρης(Ngee Ann)

Το 2018, η πολυτεχνική σχολή Ngee Ann,μια από τις τριτοβάθμιες πολυτεχνικές σχολές της Σιγκαπούρης σε συνεργασία με τη Κυβερνητική Υπηρεσία Τεχνολογίας(GovTech) άρχισε για πρώτη φορά να δοκιμάζει τη χρήση των OpenCerts για έκδοση και επαλήθευση ψηφιακών πιστοποιητικών.Μετά την επιτυχή εφαρμογή του πιλοτικού προγράμματος με την πρώτη παρτίδα αποφοίτων ως αποδέκτη,έγινε καταλύτης για ολόκληρο το τομέα εκπαίδευσης στο πλαίσιο ενός εθνικού προγράμματος.Το OpenCerts είναι μια από τις πρωτοβουλίες της Σιγκαπούρης για την ανάπτυξη ενός έξυπνου έθνους.Το SkillsFutureSingapore(SSG),ο κυβερνητικός οργανισμός τεχνολογίας(GovTech), η πολυτεχνική σχολή Ngee Ann και το Υπουργείο Παιδείας της Σιγκαπούρης διαχειρίζονται από κοινού την εφαρμογή των OpenCerts.Τον Σεπτέμβριο του 2019,ο υπουργός Παιδείας ανακοίνωσε την υιοθέτησή τους για όλους τους αποφοίτους,με τη συμμετοχή δεκαοκτώ ιδρυμάτων (Ngee Ann Polytechnic, 2019).

5.5 Εθνικό Δίκτυο Έρευνας και Εκπαίδευσης της Ελλάδας(GRNET)

Σύμφωνα με τους ,το Εθνικό Δίκτυο Έρευνας και Εκπαίδευσης της Ελλάδας αποθηκέυει τους κατακερματισμούς(hashes) των διπλωμάτων σε ένα blockchain για να εξασφαλίσει τα δεδομένα των φοιτητών του.Στόχος του είναι να δημιουργήσει ένα μηχανισμό επαλήθευσης των διπλωμάτων των φοιτητών του στο Cardano blockchain για να αντικαταστήσει τη μη αυτόματη διαδικασία επαλήθευσης και να αποτρέψει τα περιστατικά πλαστών πιστοποιητικών.Το έργο GRNET έχει διαφορετική προσέγγιση από το Blockcerts επειδή αποθηκεύει κατακερματισμούς πιστοποιητικών και το σύστημα επαλήθευσης.Το σύστημα

επαλήθευσης που αποτελείται από τα αιτήματα επαλήθευσης,το αποτέλεσμα του αιτήματος και το σύστημα ανατροφοδότησης για τον αιτούντα αποθηκεύονται.Η επικράτηση της απάτης στα πιστοποιητικά καθώς και η αυξημένη ανάγκη προστασίας των εμπορικών τους σημάτων,οδήγησαν πολλά ιδρύματα να αναπτύξουν ενδιαφέρον για την τεχνολογία blockchain για την έκδοση πιστοποιητικών.Αν και αυτό δεν είναι εξαντλητικό, η Εικόνα 28 εδώ δείχνει ότι αρκετά ιδρύματα σε διάφορες χώρες έχουν εξετάσει και εκτελούν επί του παρόντος ένα πιλοτικό έργο με blockchain για επαλήθευση πιστοποιητικών. Ο Πίνακας δείχνει την παρουσία πολλών άλλων προμηθευτών εκτός από το Blockcerts και ότι, ως επί το πλείστον, τα πειράματα τεχνολογίας σε συστήματα ακαδημαϊκής πιστοποίησης

Εκπαιδευτικό ίδρυμα	Χώρα	Χρήση	Πάροχοι Υπηρεσιών
Πανεπιστήμιο του Δελχί	Ινδία	Ψηφιακά πιστοποιητικά(Digital Certificates)	IndiaChain
Ινστιτούτο Τεχνολογίας Ινδίας	Ινδία	Ψηφιακά πιστοποιητικά	IndiaChain
Πανεπιστήμιο Επιστήμης και Τεχνολογίας της Pohang	Νότια Κορέα	Ψηφιακά πιστοποιητικά	ICONLOOP
Πολυτεχνικό Πανεπιστήμιο της Καρταχένα	Ισπανία	Ψηφιακά πιστοποιητικά	UPCT & Decision Habitat
Καθολικό Πανεπιστήμιο του Σαν Αντόνιο	Ισπανία	Ψηφιακά πιστοποιητικά	UPCT & Decision Habitat
Πανεπιστήμιο του Μπαχρέιν	Μπαχρέιν	Ψηφιακά πιστοποιητικά	Learning Machine
Ινστιτούτο τεχνολογίας Νότια Αλμπέρτα	Καναδάς	Ψηφιακά πιστοποιητικά	On Demand Education Marketplace (ODEM)
Πανεπιστήμιο της Βασιλείας	Ελβετία	Ψηφιακά πιστοποιητικά	Proxeus
Πανεπιστήμιο της Μελβούρνης	Αυστραλία	Ψηφιακά πιστοποιητικά	Blockcerts
Πανεπιστήμιο Tec de Monterrey	Μεξικό	Ακαδημαϊκές Εγγραφές	Sony Global Education, IBM Blockchain

Εικόνα 29:Πιλοτικό έργο blockchain για εκπαιδευτικά ιδρύματα

5.6 Ανοικτό Πανεπιστήμιο Αγγλίας(KMI)

Το KMI στο Open University (OU) ασχολείται με διάφορες ερευνητικές πρωτοβουλίες Blockchain. Αυτό το ερευνητικό ενδιαφέρον βασίζεται κυρίως στο ενδιαφέρον για την επόμενη γενιά του διαδικτύου, των μέσων ενημέρωσης, της αυξημένης πραγματικότητας, των έξυπνων πόλεων και των αναλυτικών στοιχείων: το OU είναι ο επικεφαλής της Learning Analytics στο Ηνωμένο Βασίλειο. Στο πλαίσιο της έρευνας και της διαπίστευσης αποκλεισμού, η KMI ενδιαφέρεται ιδιαίτερα για την αύξηση των προτύπων για αναγνωριστικό σήμα (badging), πιστοποίηση και φήμη στο διαδίκτυο με τη χρήση του blockchain ως αξιόπιστου επικεφαλής. Σύμφωνα με τον καθηγητή Domingue, ήταν φυσική εξέλιξη να ενσωματωθούν ανοιχτά αναγνωριστικά (badges) στο πλαίσιο του πρότζεκτ με blockchain και να διεξαχθεί έρευνα σχετικά με τη μικρο-διαπίστευση και τα ηλεκτρονικά χαρτοφυλάκια. Το KMI αξιοποιεί το

δυναμικό της Ethereum για διαπίστευση προκειμένου να μετατρέψει τα αναγνωριστικά σε έξυπνα συμβόλαια και να αναπτύξει ένα πρότυπο για τη συγκέντρωση και την έκδοση μικροπιστωτικών στοιχείων σε ένα blockchain.

Το OU, με περισσότερους από 170.000 φοιτητές, τη δική του πλατφόρμα MOOC (FutureLearn) και την πλατφόρμα της Open Learn (με περισσότερους από 5 εκατομμύρια επισκέπτες το χρόνο και 8 χιλιάδες ώρες εργασίας) έδωσε στο KMI την ευκαιρία να αναγνωρίσει όλα τα μαθήματα του OU στο blockchain. Η στρατηγική blockchain του KMI είναι ολιστική, με τους ερευνητές να ενθαρρύνονται να διερευνήσουν το πλήρες δυναμικό της τεχνολογίας σε αντίθεση με μια συγκεκριμένη πτυχή (όπως η κρυπτογραφία). Ο καθηγητής Domingue το εξισώνει με τις πρώτες μέρες του κινηματογράφου: "Χρειάστηκαν αιώνες για τις κινούμενες εικόνες να γίνουν κινηματογράφος, επειδή οι άνθρωποι ενδιαφέρονται μόνο για τη μαγνητοσκόπηση των παιχνιδιών!"

5.7 National University of La Plata(UNLP)

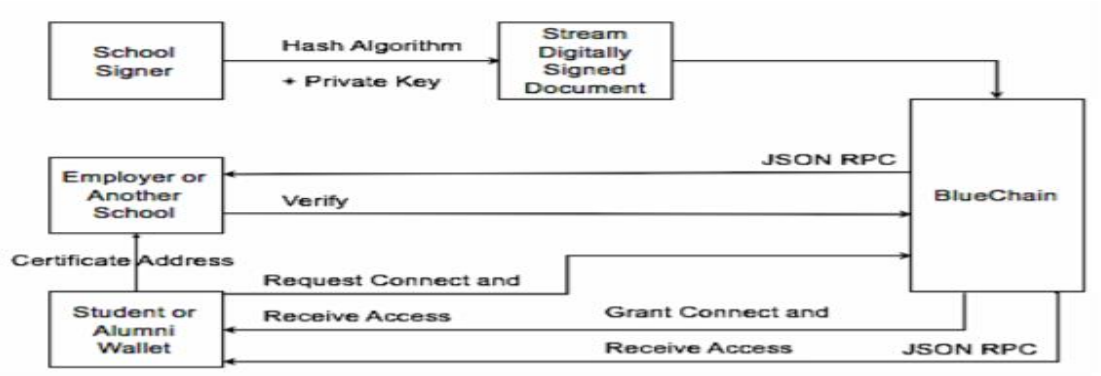
Το Εθνικό Πανεπιστήμιο της La Plata (UNLP) άρχισε να αναπτύσσει ένα πλαίσιο για την επαλήθευση του ακαδημαϊκού επιτεύγματος που βασίζεται σε blockchain, αλλά μέχρι σήμερα δεν έχουν αποκαλυφθεί περαιτέρω λεπτομέρειες . Η ίδια προσέγγιση υιοθετήθηκε επίσης από το Αργεντινό Κολλέγιο CESYT . Και οι δύο λύσεις χρησιμοποιούν τεχνολογία blockchain και κρυπτογραφία (π.χ. ψηφιακή υπογραφή, χρονικά σήματα κ.λπ.) για την έκδοση διπλωμάτων για φοιτητές. Ωστόσο, η προσέγγισή τους δεν αντιμετωπίζει το ζήτημα των αποκτηθέντων πιστώσεων για ολοκληρωμένα ακαδημαϊκά επιτεύγματα. Η προσέγγιση επικεντρώνεται μόνο στην έκδοση διπλωμάτων (πτυχίων) χρησιμοποιώντας το bitcoin blockchain.

5.8 CredenceLedger

Το CredenceLedger είναι μια προτεινόμενη πλατφόρμα βασισμένη σε blockchain με άδεια για αποκεντρωμένη επαλήθευση ακαδημαϊκών διαπιστευτηρίων.Το CredenceLedger αποτελεί ένα σύστημα που αποθηκεύει συμπαγείς αποδείξεις δεδομένων από ψηφιακά ακαδημαϊκά διαπιστευτήρια στο καθολικό του Blockchain τα οποία είναι εύκολα επαληθεύσιμα για ενδιαφερόμενους για την εκπαίδευση και ενδιαφερόμενους τρίτους οργανισμούς.Αυτό το πρότζεκτ βασίζεται στο Multichain μια ανοιχτή πλατφόρμα για την κατασκευή blockchains που βοηθά τους οργανισμούς να δημιουργήσουν και να αναπτύξουν γρήγορα εφαρμογές.Το

CredenceLedger παρέχει μια εφαρμογή για το κινητό η οποία μπορεί να χρησιμοποιηθεί από τους φοιτητές για να έχουν πρόσβαση στα εκπαιδευτικά πιστοποιητικά τους, με τρόπο που μπορεί εύκολα να επαληθευτεί από τους εργοδότες.

Το απόρρητο είναι ένα από τα πιο σημαντικά χαρακτηριστικά αυτής της λύσης ,επομένως τα ψηφιακά πιστοποιητικά προστατεύονται ώστε να διατίθενται μόνο περιορισμένες πληροφορίες σχετικά με αυτά. Εάν ένα τρίτο μέρος ενδιαφέρεται να λάβει περισσότερες πληροφορίες σχετικά με ένα πιστοποιητικό, μπορεί να πραγματοποιήσει ένα αίτημα που θα υπόκειται στην έγκριση του κατόχου.Η αποκεντρωμένη επαλήθευση της γνησιότητας και ο πλήρης έλεγχος του παραλήπτη όσον αφορά την ιδιωτικότητα του αποτελούν δύο σημαντικές πτυχές σε αυτή τη λύση.Η υιοθέτηση ενός blockchain με άδεια (permissioned),επιτρέπει στο CredenceLedger να διατηρεί πολλά σημαντικά χαρακτηριστικά από blockchain χωρίς άδεια,αλλά προσθέτει και ένα σύστημα με ρυθμιζόμενες λειτουργίες ,με ένα ελεγχόμενο σύνολο κανόνων και αδειών.



Εικόνα 30:Αρχιτεκτονική Credence ledger

Όλα τα προνόμια που παρέχονται χρησιμοποιώντας το λογισμικό μπορούν να τροποποιηθούν χρησιμοποιώντας τα μεταδεδομένα συναλλαγής ανάλογα με τα δικαιώματα διαθέσιμα στους χρήστες του.Αυτά τα δικαιώματα μπορούν να χωριστούν σε τρεις κατηγορίες : «Χαμηλού κινδύνου»,όπως σύνδεση,αποστολή και λήψη αδειών, «Μεσαίου κινδύνου» όπως ζήτημα,δημιουργία,ενεργοποίηση δικαιωμάτων και «Υψηλού κινδύνου» όπως εξόρυξης και άδειες.Το Credence Ledger χρησιμοποιεί ροές έτσι ώστε να μην χρειάζεται να συναλλασσόμαστε χρησιμοποιώντας κρυπτονομίσματαΟι ροές αναπαρίστανται από μια blockchain συναλλαγή και ενσωματώνονται με τα δικαιώματα που έχουν τεθεί σε εφαρμογή στο δίκτυοΣυνοψίζοντας τα πλεονεκτήματα του Credence ledger είναι τα ακόλουθα:1)μπορεί να απονείμει ψηφιακή έκδοση των διαπιστευτήριων του φοιτητή τα οποία είναι εύκολα επαληθεύσιμα και χωρίς να χρειάζεται να συναλλασόμαστε μέσω δημόσιου blockchain χρησιμοποιώντας κρυπτονομίσματα.Παρέχει επίσης την ευκαιρία σε τρίτους,όπως εργοδότες

,για ανεξάρτητη και κοινής χρήση με ιδιωτική επαλήθευση,2)αυτό το επιτρεπόμενο blockchain μπορεί να είναι ένα αποτελεσματικό κατανεμημένο σύστημα για κοινόχρηστη βάση δεδομένων στο οποίο πολλαπλές οντότητες επαληθεύουν δεδομένα χωρίς την ανάγκη κεντρικού συστήματος,τέλος 3)αποτελεί ένα αποτελεσματικό σύστημα για τη διαχείριση ψηφιακών ακαδημαϊκών διαπιστευτήριων κυρίως όσον αφορά την διεκπεραιωτική ικανότητα πολλών συναλλαγών,το χαμηλό κόστος και τη κατανάλωση πόρων.

Κεφάλαιο 6: Συμπεράσματα

6.1 Εισαγωγή

Ο σκοπός της παρούσας μεταπτυχιακής εργασίας, είναι η παρουσίαση της τεχνολογίας blockchain, των αλλαγών και των προκλήσεων που θα επιφέρει στα πανεπιστήμια και στους οργανισμούς, καθώς και η μελέτη και αξιοποίηση όλων των πλατφορμών και πρωτοβουλιών που υπάρχουν μέχρι στιγμής διαθέσιμα, που θα βοηθήσουν τις επιχειρήσεις να ενσωματώσουν τη τεχνολογία στη καθημερινότητά τους για την επαλήθευση πιστοποιητικών.

Για τους λόγους αυτούς, έγινε μια πλήρης αναφορά στα δομικά στοιχεία της,στις βασικές τις έννοιες της τεχνολογίας ,όπως επίσης και στο τρόπο που διεξάγεται ως τώρα η διαδικασία της επαλήθευσης διαπιστευτηρίων, που έχει οδηγήσει οργανισμούς αλλά και σε ευρύτερο επίπεδο τα κράτη,στην ενασχόληση τους με τη συγκεκριμένη τεχνολογία ώστε να προταθούν λύσεις και σε διακρατικό επίπεδο .Εν συνεχεία,περιγράφηκαν τα κύρια χαρακτηριστικά της τεχνολογίας η αποκέντρωση,η εμπιστευτικότητα,η χρονική σήμανση,η μη αναστρεψιμότητα και η διαφάνεια τα οποία αποτελούν πλεονεκτήματα σε σχέση με την υπάρχουσα διαδικασία.

Δόθηκαν ιδιαίτερη έμφαση σε αυτά καθώς προσφέρουν μεγαλύτερη ασφάλεια στην όλη διαδικασία έγκρισης.Επιπρόσθετα,αναλύθηκε όλη η διαδικασία της επαλήθευσης πιστοποιητικών σε κάποιες πλατφόρμες ώστε να τονιστούν τα θετικά που η τεχνολογία προσφέρει.Σε αυτή τη φάση,αναλύθηκαν τα δομικά μέρη της εκάστοτε πλατφόρμας τι τεχνολογίες χρησιμοποιεί,η τοπολογία blockchain που χρησιμοποιοεί ώστε να εξηγηθούν κάποια προβλήματα ασφαλείας αλλά και ταχύτητα τα οποία λύνονται αντίστοιχα.

Τέλος,αναφέρονται κάποια αρνητικά της τεχνολογίας τα οποία επικρατούν με κάποιες υπάρχουσες λύσεις αλλά και με μελλοντικές λύσεις για την αντιμεώπιση τους.

Βιβλιογραφία

(https://medium.com/wavesprotocol/educational-certificates-on-the-blockchain-why-and-how-c6be37121465 n.d.).

Στο *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains*, του/της E. Androulaki et al. 2018.

Amati F. First official career diplomas on Bitcoin's blockchain;. 2015. https://blog.signatura.co/ first-official-career-diplomas-on-bitcoin-s-blockchain-69311acb544d.

Bond F, Amati F, Blousson G. Blockchain, academic verification use case; 2015. https://s3.amazonaws.com/signatura-usercontent/ blockchain_academic_verification_use_case.pdf.

CredenceLedger_A_Permissioned_Blockchain.pdf.

https://github.com/hyperledger-archives/education/blob/master/LFS171x/docs/introduction-to-hyperledger-indy.md#introduction-to-hyperledger-indy.

https://medium.com/wavesprotocol/educational-certificates-on-the-blockchain-why-and-how-c6be37121465.

https://www.hyperledger.org/blog/2020/08/26/hyperledger-powered-education-solutions-in-action.

https://www.hyperledger.org/blog/2020/08/26/hyperledger-powered-education-solutions-in-action.

Initiative MLL. Digital Certificates Project. http://certificates.media.mit.edu/.

Invoices, C.B. Στο *Hyperledger Fabric in practice . Main components and running them locally.*, 1-6. 2019.

Mili Rafi, Sherin Mary Shaji, Prof. Ashly Thomas. *https://www.irjet.net/.* 05 May 2020.

OMAR S. SALEH, OSMAN GHAZALI, MUHAMMAD EHSAN RANA. *BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION.* http://www.jcreview.com/fulltext/197-1583403182.pdf.

Στο *Hyperledger Frameworks & Modules*, του/της M.S. Paul, Chapter 2. 2018.

Rodelio Arenas, Proceso Fernandez. *CredenceLedger_A_Permissioned_Blockchain.pdf.* 2018.

Santos, Andreia Inamorato dos. *https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf.* 2017.

Third A, Domingue J, Bachler M, Quick K. Blockchains and the Web Position Paper. In: A W3C Workshop on Distributed Ledgers on the Web. Cambridge; 2016. https://www.w3.org/2016/04/blockchain-workshop/interest/third.html.

Universidad Nacional De la Plata;. https://www.unlp.edu.ar/.

https://dl.eusset.eu/bitstream/20.500.12015/3132/1/ecscw2018_p7.pdf

https://www.fit.fraunhofer.de/en/fb/cscw/projects/blockchain-for-education.html

https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/

https://www.altoros.com/blog/sap-stores-academic-credentials-using-blockchain-and-cloud-foundry/