Επαλήθευση εγκυρότητας Ακαδημαϊκών Τίτλων με χρήση του Ethereum Blockchain

Γεώργιος Μιχούλης, Κώστας Βεργίδης, Σοφία Πετρίδου

{dai16067, kvergidis, spetrido}@uom.edu.gr

Τμήμα Εφαρμοσμένης Πληροφορικής, Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη

Περίληψη

Μια αλυσίδα ομάδων συναλλαγών (blockchain) αποτελεί ένα δημόσιο ψηφιακό κατάστιχο (ledger) υλοποιημένο με κατανεμημένο τρόπο γεγονός που απαλλάσσει από την ανάγκη ύπαρξης ενός κεντρικού αποθετηρίου και μιας κεντρικής αρχής. Η βασική ιδέα είναι ότι παρέχει τη δυνατότητα σε μια κοινότητα χρηστών να καταγράφει τις συναλλαγές της κρατώντας διαμοιραζόμενη την πληροφορία εκτέλεσής τους και διασφαλίζοντας ότι αυτές παραμένουν ανθιστάμενες αλλοιώσεων (tamper resistant). Το παρόν άρθρο αξιοποιεί την τεχνολογία blockchain ως τρόπο επαλήθευσης της εγκυρότητας ακαδημαϊκών τίτλων. Κίνητρο αποτελούν τα περιστατικά πλαστογράφησης τίτλων που κατατίθενται σε ακαδημαϊκούς και ερευνητικούς φορείς, αλλά και σε φορείς της αγοράς εργασίας. Οι συγγραφείς παρουσιάζουν και περιγράφουν την εφαρμογή VerDe (Verified Degrees) που ανέπτυξαν με χρήση της πλατφόρμας Ethereum Blockchain και του έξυπνου συμβολαίου ERC20 token. Τέλος, παραθέτουν ένα παράδειγμα λειτουργίας της εφαρμογής.

1. Εισαγωγή

Στις μέρες μας, αρκετά συχνά, δημοσιεύονται ειδήσεις για περιστατικά ανθρώπων που κατέχουν κρίσιμες θέσεις ιδιωτικού ή δημόσιου τομέα όντας κάτοχοι πλαστών ακαδημαϊκών τίτλων[1]. Ενδεικτικά παραδείγματα πλαστογράφησης πτυχίων περιλαμβάνουν διοικητικούς υπαλλήλους, εκπαιδευτικούς, ερευνητές, και ακόμη πιο ανησυχητικά, ιατρούς και χειρουργούς [1-4]. Τα περιστατικά αυτά μας ώθησαν να σκεφτούμε τον τρόπο που η ψηφιακή τεχνολογία μπορεί να συνδράμει στην αντιμετώπιση του φαινομένου. Θεωρώντας ότι: (i) η απόκτηση ενός ακαδημαϊκού τίτλου αποτελεί μια «δημόσια συναλλαγή» μεταξύ ενός Ακαδημαϊκού Ιδρύματος και ενός τελειόφοιτου, (ii) υπάρχουν κοινότητες φορέων που ενδιαφέρονται να έχουν πρόσβαση στην καταγραφή αυτών των συναλλαγών, και (iii) κάθε συναλλαγή δε μπορεί να αλλοιωθεί από τη στιγμή της δημιουργίας της, οδηγηθήκαμε στο συμπέρασμα ότι το blockchain αποτελεί μια κατάλληλη λύση [5]. Επιπλέον χαρακτηριστικά, όπως η κατανεμημένη αποθήκευση της πληροφορίας και η απουσία κεντρικής αρχής την καθιστούν και ελκυστική σε επίπεδο υλοποίησης.

Ιδέες παρόμοιες με την προτεινόμενη έχουν ήδη καταγραφεί στη βιβλιογραφία. Πρόσφατα οι Turkanovik et al. [6] πρότειναν την πλατφόρμα EduCTX, η οποία δημιουργεί ένα blockchain, με κόμβους τα ίδια τα Πανεπιστήμια και τα δικά της διαφορετικά ECTS (ECTX). Το EduCTX αναπτύχθηκε στο Ark blockchain και απαιτεί η κάθε πανεπιστημιακή μονάδα να διαθέτει τους δικούς της

[1] Περισσότερες πληροφορίες: https://www. topics. gr/crono/plasta-ptyxia/

εξυπηρετητές για να συμμετέχουν στο δίκτυο. Η πρώτη εφαρμογή που δημιουργήθηκε για την επαλήθευση των ακαδημαϊκών τίτλων (2015) είναι από το Πανεπιστήμιο της Νικοσίας (Block.co) [7] και χρησιμοποιεί μέχρι και σήμερα το blockchain του Bitcoin.

Ωστόσο, εφαρμογές όπως η [6] έχουν υψηλό κόστος διαχείρισης και υλοποίησης καθώς απαιτούν τόσο από τους φοιτητές όσο και από τις ακαδημαϊκές μονάδες να διαθέτουν κλειδιά επαλήθευσης των δεδομένων. Επίσης, η μεταφόρτωση ενός pdf από τους χρήστες στο blockchain δεν δίνει μια αξιόπιστη λύση στο πρόβλημα της επαλήθευσης των ακαδημαϊκών τίτλων [7]. Στόχος του άρθρου είναι να παρουσιάσει την αποκεντρωμένη εφαρμογή VerDe (Verified Degrees), που βασίζεται στην τεχνολογία blockchain και στα έξυπνα συμβόλαια, προκείμενου να παρέχει επαλήθευση της εγκυρότητας ενός ακαδημαϊκού τίτλου. Η καινοτομία της εφαρμογής έγκειται στο γεγονός ότι, χρησιμοποιεί το Ethereum blockchain για την επαλήθευση και χρησιμοποιεί «ψευδό-κρυπτονομίσματα», ως τρόπο επαλήθευσης των ακαδημαϊκών τίτλων. Τα πλεονεκτήματα της προτεινόμενης εφαρμογής είναι: (α) η ακεραιότητα των δεδομένων, (β) η αποκεντρωμένη αποθήκευση δεδομένων (γ) η γρήγορη επαλήθευση, (δ) το χαμηλό κόστος ανάπτυξης και συντήρησης, και (ε) η εύκολη πρόσβαση και χρήση.

Σε ό,τι αφορά στη δομή του άρθρου, η Ενότητα 2 αποτελεί μια παρουσίαση του θεωρητικού υποβάθρου της τεχνολογίας blockchain και των έξυπνων συμβολαίων στο Ethereum. Στην Ενότητα 3 παρουσιάζουμε την αρχιτεκτονική της εφαρμογής VerDe, ενώ στην Ενότητα 4 λεπτομέρειες της υλοποίησής της. Η Ενότητα 4 παρουσιάζει ένα παράδειγμα λειτουργίας της Verde και η Ενότητα 5 κλείνει το άρθρο με σύντομα συμπεράσματα και ιδέες για μελλοντική έρευνα.

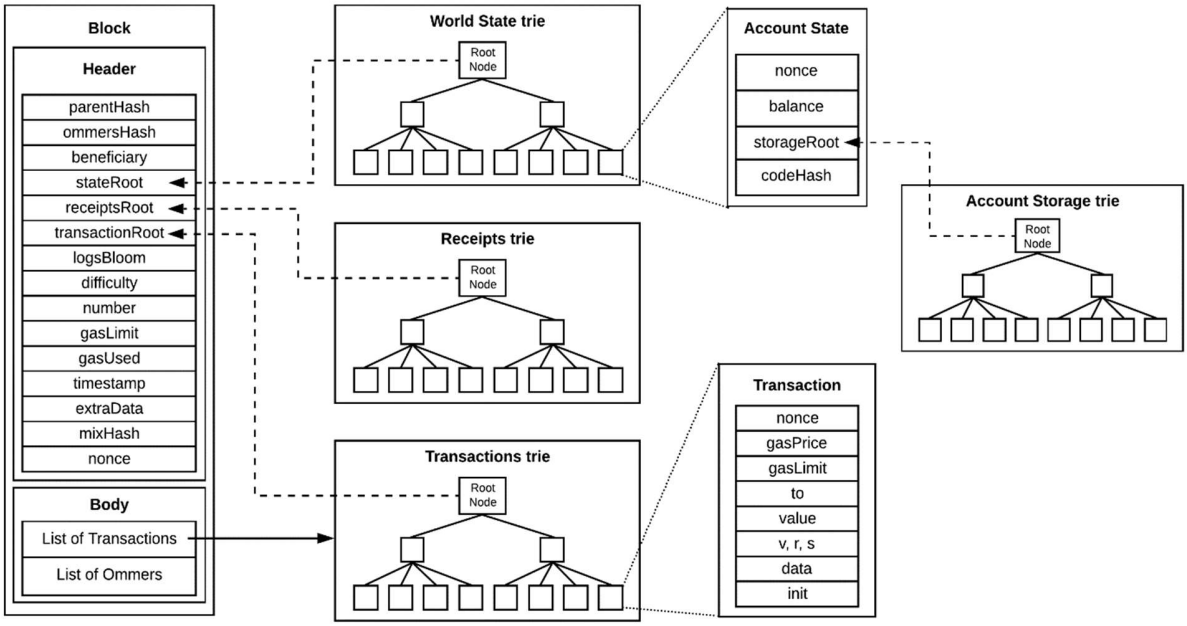
2. Η τεχνολογία blockchain και τα έξυπνα συμβόλαια στο Ethereum

Όπως αναφέρθηκε, το blockchain είναι ένα κατανεμημένο σύστημα αποτελούμενο από ομότιμους κόμβους και κατάστιχα. Χρησιμοποιεί έναν αλγόριθμο ο οποίος επεξεργάζεται τις πληροφορίες που υπάρχουν μέσα σε ταξινομημένα και συνδεδεμένα μεταξύ τους μπλοκ δεδομένων με τη χρήση κρυπτογραφίας και έχει ως στόχο την ακεραιότητα των πληροφοριών [8]. Ακολουθεί μία σύντομη περιγραφή της τεχνολογίας και των έξυπνων συμβολαίων στην πλατφόρμα Ethereum.

2.1. Περιγραφή της τεχνολογίας Blockchain

Το 2008 ξεκίνησε η ιδέα για το πρώτο blockchain με την δημιουργία του Bitcoin από τον Satoshi Nakamoto [9]. Η ιδέα αυτή είναι και η λύση του Byzantine Generals Problem [10]. Το πρόβλημα των Στρατηγών θα γίνει πιο κατανοητό μέσα από ένα παράδειγμα: κάθε στρατηγός έχει το δικό του στρατό και βρίσκεται σε διαφορετικές τοποθεσίες γύρω από την πόλη που πολιορκούν. Οι στρατηγοί πρέπει να συμφωνήσουν είτε σε επίθεση, είτε σε υποχώρηση. Δεν έχει σημασία αν θα επιτεθούν ή υποχωρήσουν αρκεί όλοι οι στρατηγοί να καταλήξουν σε συναίνεση. Επομένως, επικοινωνούν δια αλληλογραφίας ο ένας με τον άλλον για να αποφασίσουν την επόμενη κίνηση τους, όμως δεν γνωρίζουν αν το μήνυμα που στέλνουν ή δέχονται παραμένει ή είναι γνήσιο. Η λύση του Nakamoto χρησιμοποιεί τις συναρτήσεις διασποράς (hash functions) και την τυχαία τιμή μοναδικής χρήσης (nonce). Οπότε, ο Α στρατηγός θα στείλει στον Β ένα μήνυμα για επίθεση, το οποίο θα περιλαμβάνει το κείμενο (plaintext) και το κατάλληλο nonce, τέτοιο ώστε η σύνοψη των δύο (hash) να ικανοποιεί το κριτήριο (hash target) που έθεσε ο Β. Στη συνέχεια ο Β υπολογίζει την ίδια σύνοψη και εφόσον ικανοποιεί το κριτήριο που ίδιος έθεσε αποδέχεται το μήνυμα του Α ως αυθεντικό. Η διαδικασία που ακολουθεί ο Α στρατηγός ονομάζεται απόδειξη εργασίας (proof of work) [11] και απαιτεί μεγάλη υπολογιστική ισχύ. Στην περίπτωση που είχαμε πολλούς Α, οι Α θα εναπόθεταν τα μηνύματα τους σε ένα «μπλοκ» και θα έβρισκαν ένα μοναδικό nonce για όλο το μπλοκ που θα συνοψίσουν. Πριν την σύνοψη όμως ο Nakamoto πρότεινε να προστεθούν και άλλα στοιχεία στο μπλοκ για να γίνει πιο ισχυρή η

επαλήθευσή του και δύσκολος ο υπολογισμός της σύνοψης, ένα από αυτά είναι η σύνοψη του προηγούμενου μπλοκ. Έτσι δημιουργείται μια αλυσίδα από μπλοκ, το blockchain, που δεν μπορεί να παραποιηθεί.



Εικόνα 1. Η δομή του Ethereum Blockchain [14]

2.2. Η πλατφόρμα Ethereum

Το Bitcoin ήταν το πρώτο blockchain αλλά όχι το τελευταίο. Στην παρούσα εργασία μελετάμε το Ethereum blockchain το οποίο είναι εμπνευσμένο από το Bitcoin και προτάθηκε το 2015 από τον Gavin Wood [12]. Χρησιμοποιεί το μοντέλο συναίνεσης της απόδειξης εργασίας [11] και αποτελεί ένα permissionless blockchain [13]. Το Ethereum blockchain χρησιμοποιεί endpoints και λειτουργεί με JSON-RPC API το οποίο υποστηρίζεται, από το Ethereum Web3 Api δηλαδή, από την βιβλιοθήκη web3.js. Τα 4 βασικά χαρακτηριστικά της δομής του Ethereum φαίνονται στην Εικ. 1 και είναι [14]:

A. **Οι λογαριασμοί (Accounts).** Υπάρχουν 2 ειδών λογαριασμοί στο Ethereum [12] με διευθύνσεις που τους συνοδεύουν: 1) οι λογαριασμοί χρηστών (Externally Owned Accounts EOAs) οι οποίοι έχουν απαραιτήτως ένα ιδιωτικό κλειδί για τον έλεγχο των κεφαλαίων τους και των έξυπνων συμβολαίων τους (π.χ., MetaMask), και 2) οι λογαριασμοί των έξυπνων συμβολαίων (Contract Account) που δεν έχουν ιδιωτικό κλειδί και εξυπηρετούν στην επαλήθευση του περιεχομένου των συναλλαγών από τις οποίες προέκυψαν.
B. **Η Παγκόσμια Κατάσταση (World State).** Η Παγκόσμια κατάσταση (state), είναι μια αντιστοίχιση (mapping) μεταξύ διευθύνσεων (160 bit) και καταστάσεων λογαριασμού [13]. Δεν είναι αποθηκευμένη στο blockchain, η εφαρμογή θα διατηρήσει αυτήν την αντιστοίχιση σε ένα τροποποιημένο δέντρο τύπου Merkle Patricia[5]. Το World State μπορεί να παρομοιαστεί και με την βάση δεδομένων του blockchain. Οι συναλλαγές και η κατάσταση των λογαριασμών αποθηκεύονται εκεί και οι κλήσεις τους επιστρέφονται με την τελευταία ενημέρωση από το World State.

C. **Το Μπλοκ.** Το Μπλοκ στο Ethereum έχει τον ρόλο του κατάστιχου. Χωρίζεται σε 2 μέρη, την επικεφαλίδα και το σώμα. Η επικεφαλίδα περιλαμβάνει όλα εκείνα τα στοιχεία που αποδεικνύουν την σχέση της «αλυσίδας» με τα προηγούμενα μπλοκ,

ενώ το σώμα αποτελείται από ένα πλήθος συναλλαγών και μια λίστα με τις επικεφαλίδες των μπλοκ που βρίσκονται στην ίδια ιεραρχία με το μπλοκ-γονέα (ommers) [13].

D. **Οι συναλλαγές (Transactions).** Οι συναλλαγές είναι αυτές που κάνουν την παγκόσμια κατάσταση να αλλάζει από την τρέχουσα κατάσταση στην επόμενη κατάσταση. Υπάρχουν 3 είδη συναλλαγών: 1) αυτές που μεταφέρουν τιμές μεταξύ δύο λογαριασμών χρηστών (EOAs), 2) αυτές που στέλνουν μια κλήση μηνύματος σε ένα έξυπνο συμβόλαιο, και 3) αυτές που αναπτύσσουν ένα έξυπνο συμβόλαιο [12, 13].

2.3. Έξυπνα συμβόλαια στο Ethereum

Ένα χαρακτηριστικό του Ethereum είναι η χρήση της Εικονικής Μηχανής (Ethereum Virtual Machine - EVM) [12] που εκτελεί και επεξεργάζεται τα έξυπνα συμβόλαια. Ο σκοπός της είναι η ενημέρωση της κατάστασης του Ethereum με τον υπολογισμό τον έγκυρων μεταβάσεων της κατάστασης, ως αποτέλεσμα της εκτέλεσης του κώδικα των έξυπνων συμβολαίων [12]. Η πιο γνωστή γλώσσα προγραμματισμού υψηλού επιπέδου για έξυπνα συμβόλαια είναι η Solidity [12]. Αυτή είναι μια contract oriented γλώσσα («συμβολαιοστρεφής»), έχει αντίστοιχη δηλαδή λειτουργία με την αντικειμενοστρέφεια. Είναι μια γλώσσα Τούρινγκ πλήρης. Αυτό έχει το μειονέκτημα των ατέρμονων βρόχων και θα μπορούσε να δημιουργήσει σοβαρό πρόβλημα στο δίκτυο του Ethereum. Πρακτικά αντιμετωπίζεται καθώς για την ανάπτυξη και δημοσίευση ενός συμβολαίου το Ethereum χρησιμοποιεί ένα όριο που ορίζεται ως κατανάλωση αερίου και συσσωρεύει το κόστος των συναλλαγών ώστε αυτές να είναι πεπερασμένες. Το όριο στην κατανάλωση του αερίου κατά την ανάπτυξη ενός έξυπνου συμβολαίου φαίνεται και στα διαγράμματα της μελέτης των Tonelli et al [15]. Στη συγκεκριμένη έρευνα, μελετήθηκαν 12.094 έξυπνα συμβόλαια και συγκρίθηκαν με βάση τις καθολικές μετρικές και μετρικές που αφορούν μόνο αποκεντρωμένες εφαρμογές (κλήσεις από και προς άλλες διευθύνσεις, εσωτερικές κλήσεις στο έξυπνο συμβόλαιο, κατανάλωση αερίου, συναλλαγή κρυπτονομισμάτων και bytecode/ABI). Σε όλες τις παραπάνω μετρικές φαίνεται ότι φτάνουν σε ένα άνω όριο και αυτό οφείλεται στον περιορισμό του αερίου που μπορεί να καταναλωθεί από τα έξυπνα συμβόλαια. Το έξυπνο συμβόλαιο είναι πολύ σημαντικό κομμάτι στις αποκεντρωμένες εφαρμογές καθώς λειτουργεί ως η βάση δεδομένων για τις εφαρμογές αυτές. Όλα τα δεδομένα που αποθηκεύονται σε ένα συμβόλαιο αποθηκεύονται μοναδικά στην συγκεκριμένη διεύθυνση δηλαδή, στην κατάστασή του και επιστρέφονται από αυτή. Επίσης, μεταγλωττίζεται στο χαμηλό επίπεδο σε bytecode με την βοήθεια της EVM. Τέλος, μια πολύ σημαντική λειτουργία που διεκπεραιώνουν τα έξυπνα συμβόλαια είναι αυτή της αποστολής και αποθήκευσης κρυπτονομισμάτων.

Για την εφαρμογή μας επιλέξαμε το έξυπνο συμβόλαιο του ERC20 token που είναι δημόσιο [16]. Η λειτουργία του βασίζεται στην δημιουργία ενός πλήθους «ψευδό-κρυπτονομισμάτων» που ανήκουν και διαχειρίζονται από αυτόν που ανέπτυξε το έξυπνο συμβόλαιο και λειτουργούν όπως ένα κοινό κρυπτονόμισμα. Τα νομίσματα αυτά δημιουργούνται μια φορά και δεν μπορούν να ξανά παραχθούν ή να μεταφερθούν χωρίς την έγκριση του δημιουργού. Όλες οι συναλλαγές των νομισμάτων είναι αλληλένδετες με την διεύθυνση του συμβολαίου, δηλαδή η λίστα των συναλλαγών που έχουν πραγματοποιηθεί με αυτό το token εμφανίζεται στην διεύθυνση του συμβολαίου. Έτσι, υπάρχει η δυνατότητα επαλήθευσης της μεταφοράς μεταξύ της διεύθυνσης του αποστολέα και του παραλήπτη, δηλαδή υπάρχει διαφάνεια στις συναλλαγές. Τελικά, το ποσό των token που στέλνετε κάθε φορά στον παραλήπτη, αφαιρείται από το υπόλοιπο του αποστολέα και υπάρχει διαφάνεια στο υπόλοιπο τους.

3. Αρχιτεκτονική της εφαρμογής Verde

Στην παρούσα ενότητα παρουσιάζεται η αρχιτεκτονική της αποκεντρωμένης εφαρμογής Verde. Η συγκεκριμένη εφαρμογή, όπως όλες οι αποκεντρωμένες διαδικτυακές εφαρμογές, αποτελείται από τρία βασικά συστατικά στοιχεία: (α) το συστατικό τη παρουσίασης, (β) το συστατικό του ελέγχου, και, (γ) το συστατικό επικοινωνίας με το blockchain. Το πρώτο, αποτελεί την διεπαφή με τον χρήστη (Εικ. 2, Front-end) και διαβάζει τα στοιχεία που του καταχωρεί. Το τρίτο λειτουργεί με την βιβλιοθήκη web3.js και επικοινωνεί με το blockchain του Ethereum (Εικ. 2, back-end). Το συστατικό του ελέγχου ενώνει τα δύο παραπάνω και λειτουργεί ως ο «εγκέφαλος» της εφαρμογής [17]. Ακολουθεί η αναλυτική περιγραφή της προτεινόμενης αρχιτεκτονικής πάνω στην οποία υλοποιήθηκε η εφαρμογή VerDe.

3.1. Σκοπός της εφαρμογής

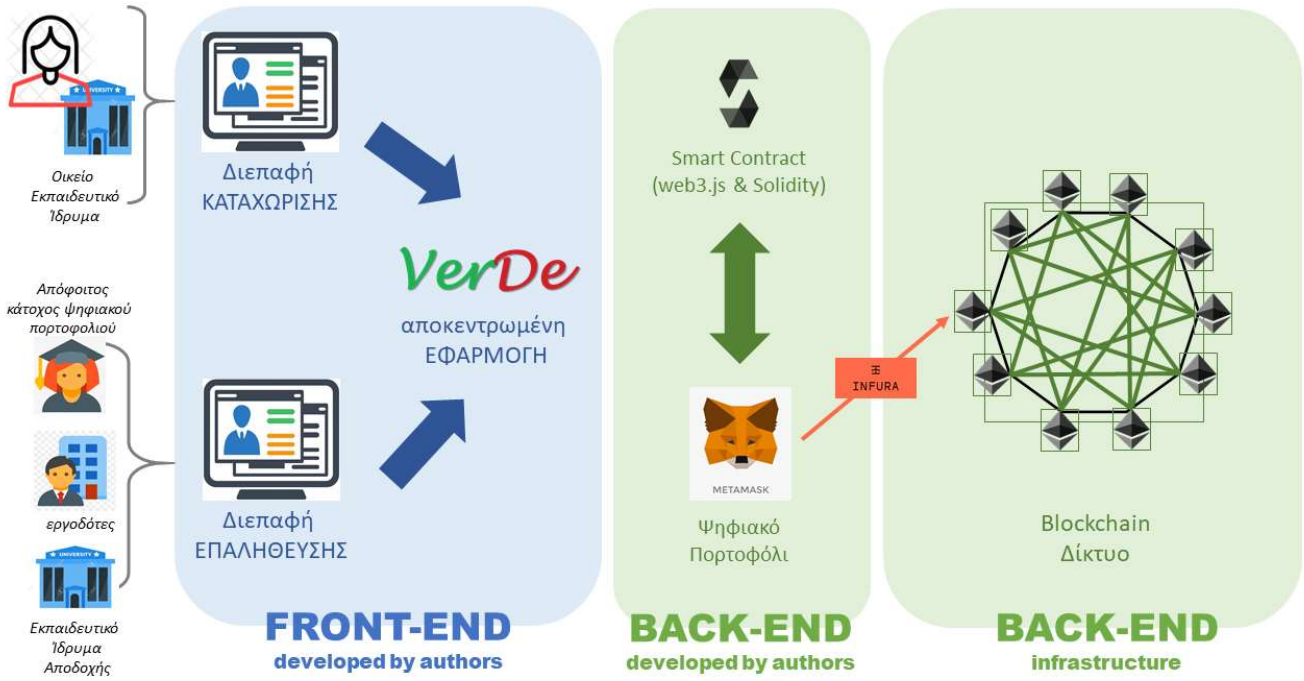
Η εφαρμογή Verde βασιζόμενη στην αξιοπιστίας του Ethereum blockchain επαληθεύει τους ακαδημαϊκούς τίτλους χωρίς να χρειάζεται η παρέμβαση της ακαδημαϊκής μονάδας κάθε φορά. Αποτελείται από 2 διεπαφές που είναι το front-end της: 1) τη διεπαφή καταχώρισης των δεδομένων στο Ethereum, και 2) τη διεπαφή επαλήθευσης των δεδομένων, όπως φαίνεται στην Εικ. 2. Η ύπαρξη 2 διεπαφών έχει ως στόχο την απομόνωση της διεπαφής καταχώρισης την οποία διαχειρίζεται κάθε ακαδημαϊκή μονάδα ξεχωριστά και μοναδικά από τη διεπαφή επαλήθευσης που είναι δημόσια και κατά συνέπεια προσβάσιμη από κάθε ενδιαφερόμενο. Η σύνδεση του back-end με το front-end επιτυγχάνεται μέσω της βιβλιοθήκης web3. js, που εγκαθίσταται στις διεπαφές και αποτελεί το back-end της εφαρμογής μαζί με το έξυπνο συμβόλαιο (Εικ. 2 back-end). Η λειτουργικότητα της εφαρμογής και η ιδιότητα της αποκέντρωσης επιτυγχάνεται πρακτικά με το έξυπνο συμβόλαιο. Όμως, για να επιτευχθεί η σύνδεση με το blockchain, χρειάζεται ένα ψηφιακό πορτοφόλι και η σύνδεση με έναν πλήρη κόμβο του. Το ψηφιακό πορτοφόλι περιλαμβάνει το υπόλοιπο των κεφαλαίων του χρήστη και το κόστος των συναλλαγών αφαιρείται από αυτό («φιλτράρει» τις συναλλαγές) ενώ, ο πλήρης κόμβος (ολόκληρα μπλοκ) ενημερώνεται για τα μπλοκ του blockchain και παράλληλα δημιουργεί νέα. Την επικοινωνία των 2 παραπάνω καλύπτει η εφαρμογή MetaMask που αποτελεί επίσης τμήμα του back-end της εφαρμογής Verde. Το MetaMask αναπτύχθηκε από την εταιρεία ConsenSys και αποτελεί διαδικτυακή εφαρμογή (επέκτασης περιηγητή) ψηφιακού πορτοφολιού. Επίσης, η σύνδεση με τους κόμβους του δικτύου Ethereum γίνεται μέσω της εφαρμογής Infura, η οποία εκτελείται στο back-end του MetaMask.

Δημιουργήσαμε την εφαρμογή VerDe στο περιβάλλον του Ethereum γιατί, είναι το δεύτερο μεγαλύτερο blockchain δίκτυο αυτήν την στιγμή [18] σε χρηματιστηριακή αξία, σε πλήθος κόμβων και συχνότητα συναλλαγών, ενώ επιπλέον είναι δημόσιο (permissionless), δεν χρειάζεται να δημιουργήσουμε εμείς τους κόμβους και έχει μεγάλη κοινότητα που το υποστηρίζει.

3.2. Αρχιτεκτονική της διεπαφής καταχώρισης

Ο σκοπός της διεπαφής καταχώρισης είναι η αποστολή των δεδομένων του φοιτητή από την ακαδημαϊκή μονάδα στο δίκτυο του Ethereum προκειμένου αργότερα να είναι εφικτή η επαλήθευση των στοιχείων ενός ακαδημαϊκού του τίτλου. Τα στοιχεία αυτά περιλαμβάνουν το ονοματεπώνυμο, όνομα πατέρα, μητέρας και την ημερομηνία γέννησης ενός φοιτητή και είναι τα απολύτως απαραίτητα για την ταυτοποίησή του. Επιπλέον, ωστόσο, περιλαμβάνουν τις πληροφορίες του Τμήματος, των μαθημάτων, των πιστωτικών μονάδων (ECTS) και των βαθμολογιών σε κάθε μάθημα. Όλα τα παραπάνω στοιχεία είναι απαραίτητα για την επαλήθευση του ακαδημαϊκού τίτλου και την ταύτιση του με τον φοιτητή. Οπότε, οι λειτουργίες της εφαρμογής Verde πρέπει να

έχουν την δυνατότητα να προβάλουν τα παραπάνω στοιχεία για να είναι ο τίτλος επαληθευμένος. Για να μπορέσει όμως να συμβεί η προβολή, θα πρέπει πρώτα να καταχωρηθούν στο blockchain λειτουργία που επιτελείται μέσω της διεπαφής καταχώρισης[2].



Εικόνα 2. Αφαιρετική απεικόνιση της αρχιτεκτονικής της εφαρμογής Verde

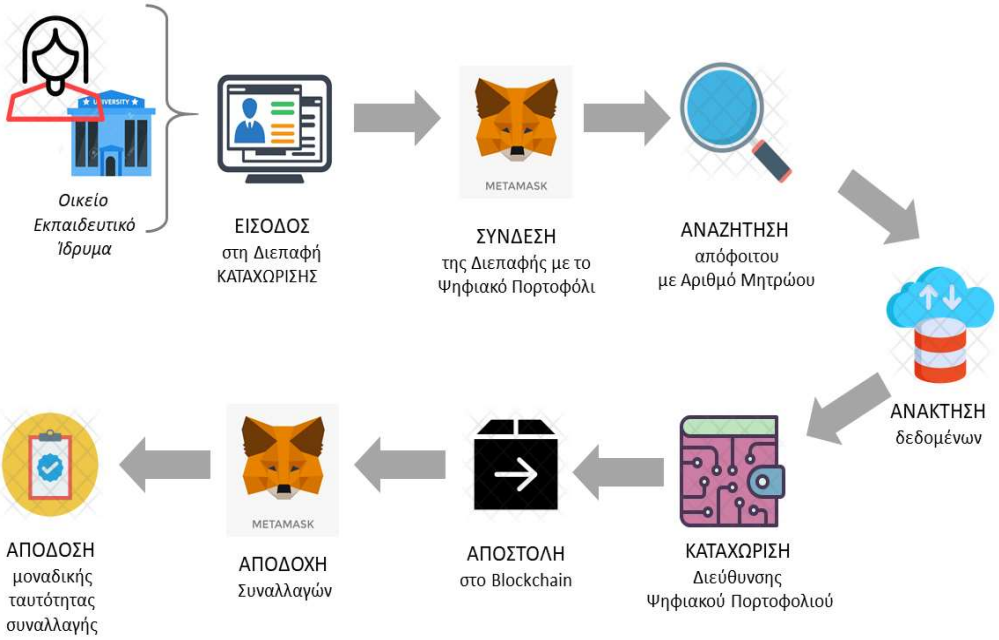
Η μεταφορά στο blockchain γίνεται πάντα μεταξύ ενός αποστολέα και ενός παραλήπτη, δηλαδή μεταξύ των διευθύνσεων του ψηφιακού πορτοφολιού της ακαδημαϊκής μονάδας και του φοιτητή, ενώ το μέσο είναι το Ethereum. Οποιαδήποτε ακαδημαϊκή μονάδα θελήσει να χρησιμοποιήσει την συγκεκριμένη διεπαφή, μπορεί, αρκεί να διαθέτει το δικό της ψηφιακό πορτοφόλι στο Ethereum. Τα βήματα για την πραγματοποίηση της καταχώρησης των στοιχείων και μεταφοράς στο blockchain είναι 8 και φαίνονται στην Εικ. 3α.

3.3. Αρχιτεκτονική της διεπαφής επαλήθευσης

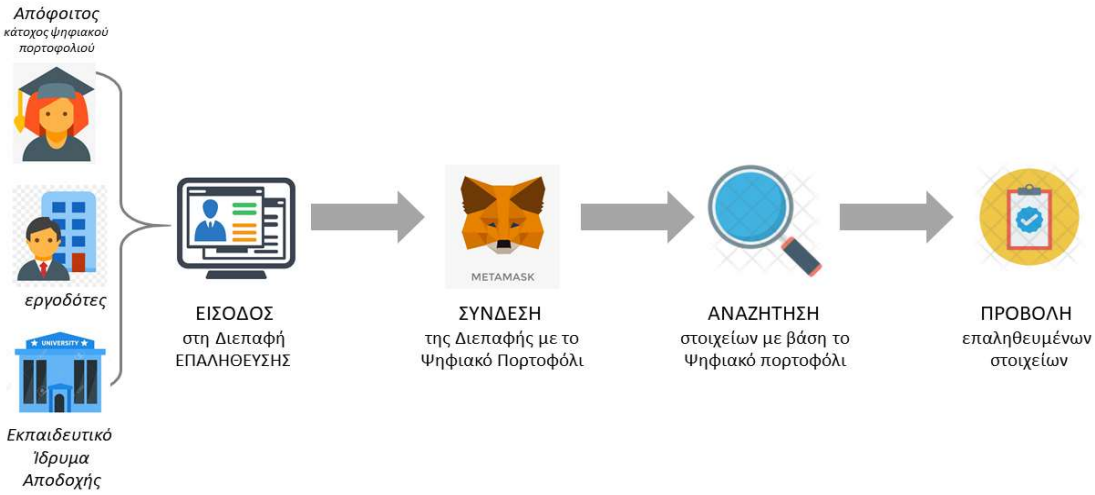
Η διεπαφή επαλήθευσης είναι επίσης εύχρηστη και απαιτεί μόλις 4 βήματα για να ολοκληρώσει την λειτουργία της. Βασίζεται στην αναζήτηση της διεύθυνσης του ψηφιακού πορτοφολιού του αποφοίτου. Η αναζήτηση ανακτά από το Ethereum, πιο συγκεκριμένα από την κατάσταση του έξυπνου συμβολαίου, τις πληροφορίες που σχετίζονται με τον απόφοιτο. Πρόκειται για τις πληροφορίες που μετέφερε στο Ethereum η διεπαφή καταχώρισης. Συνεπώς, οι πληροφορίες που επιστρέφονται είναι τα προσωπικά στοιχεία του αποφοίτου και οι πληροφορίες των μαθημάτων που διεκπεραίωσε κατά την διάρκεια των σπουδών του[3]. Από τα παραπάνω

[2] Η διεπαφή καταχώρησης έχει δημοσιευτεί και λειτουργεί στην: https://dry-sierra-28168.herokuapp.com/index.php
[3] Η διεπαφή επαλήθευσης έχει δημοσιευτεί και λειτουργεί στην: https://dry-sierra-28168. herokuapp. com/showStudents. html

αντιλαμβανόμαστε ότι, η διεπαφή αυτή έχει ως σκοπό την επαλήθευση των δεδομένων του ακαδημαϊκού τίτλου, του υποψήφιου εργαζομένου ή μεταπτυχιακού φοιτητή. Με αυτόν τον τρόπο, οι ακαδημαϊκές μονάδες ωφελούνται σε λειτουργικό χρόνο και κόστος, αφού αυτόν τον ρόλο τον ανέλαβε το Ethereum blockchain. Ο λόγος που είναι τόσο ισχυρό αυτό το διαπιστευτήριο είναι γιατί, τα δεδομένα στο blockchain δεν μπορούν να αλλοιωθούν.



(α). Διαδικασία καταχώρισης των στοιχείων του φοιτητή από την οικεία ακαδημαϊκή μονάδα



(β). Διαδικασία επαλήθευσης του ακαδημαϊκού τίτλου ενός αποφοίτου

Εικόνα 3. Διαδικασίες καταχώρισης και επαλήθευσης της εφαρμογής Verde

3.3. Αρχιτεκτονική του έξυπνου συμβολαίου

Το έξυπνο συμβόλαιο αποτελεί το back-end της αποκεντρωμένης εφαρμογής. Οι χρήστες δεν έρχονται ποτέ σε επαφή με τον κώδικα του έξυπνου συμβολαίου και ούτε αλληλοεπιδρούν άμεσα με αυτό. Το συμβόλαιο είναι πολύ σημαντικό για την εφαρμογή γιατί εκτελεί τις λειτουργίες καταχώρισης και επαλήθευσης των ακαδημαϊκών τίτλων. Οι λειτουργίες που χρειάζεται να έχει είναι οι εξής:

- Αποθηκεύει τα προσωπικά στοιχεία του φοιτητή στο έξυπνο συμβόλαιο (όνομα, επίθετο, όνομα μητέρας και πατέρα, τόπος καταγωγής, ημερομηνία γέννησης).
- Αποθηκεύει τους βαθμούς, τα μαθήματα, τον μέσο όρο και τα ECTS του φοιτητή.
- Δημιουργεί τα «ψευδό-κρυπτονομίσματα» με όνομα ECTS, με σκοπό την αποστολή του πλήθους που συγκέντρωσε ο φοιτητής, κατά την διάρκεια των σπουδών του.
- Επιστρέφει τα στοιχεία του φοιτητή.
- Επιστρέφει τους βαθμούς, τα μαθήματα, τον μέσο όρο και τα ECTS του φοιτητή.
- Χρησιμοποιεί το token ERC20 [4] για την δημιουργία των ECTS. Η εφαρμογή δημιουργεί ένα πλήθος τέτοιων ECTS ενός πολύ μεγάλου αριθμού, όπου το ακέραιο μέρος του είναι ένας 7-ψήφιος αριθμός και το δεκαδικό του μέρος ένας 18-ψήφιος. Η χρήση του έχει ως σκοπό την διπλή επαλήθευση των στοιχείων του φοιτητή, λόγω της διαφάνειας του.

Το έξυπνο συμβόλαιο από την στιγμή που αναπτύσσεται στο blockchain δεν μπορεί να αλλάξει. Επομένως, είναι σημαντικό οι λειτουργίες του να είναι αυστηρά καθορισμένες, να γίνουν δοκιμές προς μελέτη όλων των πιθανών περιπτώσεων και να δοθεί μεγάλη προσοχή στην υλοποίηση του.

4. Υλοποίηση της εφαρμογής *VerDe*

Σε αυτήν την ενότητα θα εξετάσουμε τις λεπτομέρειες υλοποίησης της εφαρμογής Verde. Οι διεπαφές δημιουργήθηκαν με κώδικα HTML, CSS (Bootstrap), Javascript (Jquerry) και PHP. Το έξυπνο συμβόλαιο είναι γραμμένο στην γλώσσα προγραμματισμού Solidity 0.5.7 και αναπτύχθηκε στο περιβάλλον Remix, στο δίκτυο του Ropsten.

4.1. Υλοποίηση της διεπαφής καταχώρισης

Η διεπαφή καταχώρισης είναι εύχρηστη και υλοποιήθηκε με χρήση PHP. Χρησιμοποιεί 4 διαφορετικές φόρμες HTML για την συλλογή όλων των στοιχείων εκείνων που απαιτούνται για την επαλήθευση του ακαδημαϊκού τίτλου ενός φοιτητή:

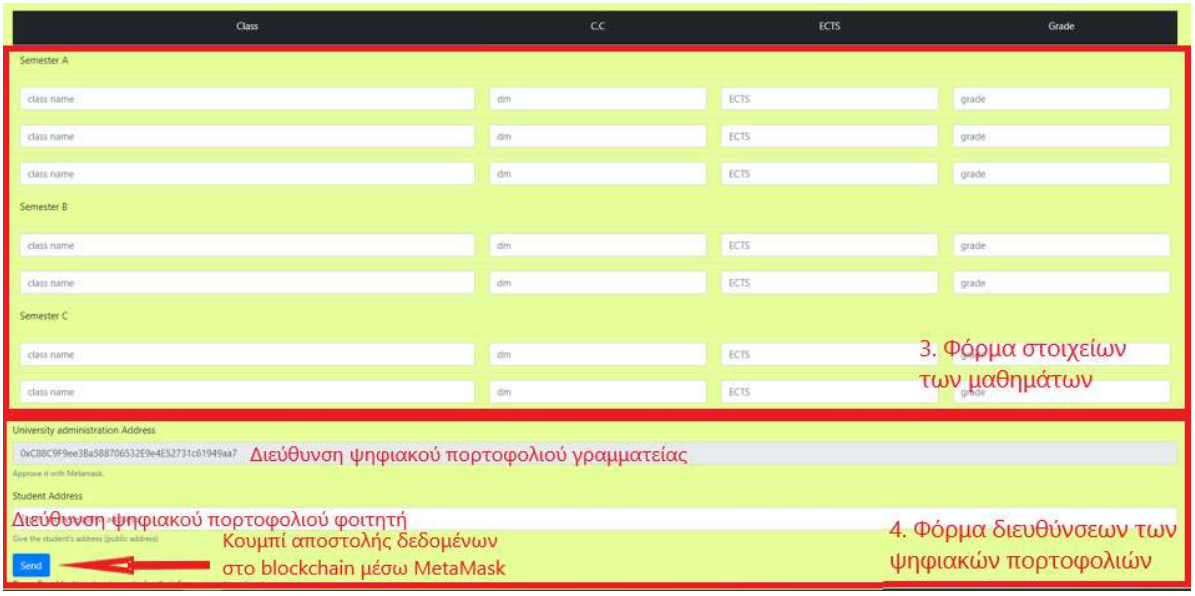
1. Η πρώτη περιέχει το λογότυπο του πανεπιστημίου και τον τίτλο της σχολής (Εικ. 4α).

2. Η δεύτερη αποτελείται από τα πεδία για την συμπλήρωση των προσωπικών στοιχείων του φοιτητή και την αναζήτηση του φοιτητή στην βάση δεδομένων του πανεπιστημίου. Μόλις ενεργοποιηθεί η αναζήτηση, εκτελείται ένα Mysql αίτημα από τον κώδικα της PHP και επιστρέφει όλα τα στοιχεία του φοιτητή που έχει το συγκεκριμένο αριθμό μητρώου. Εάν η ανάκτηση είναι επιτυχής τότε, συμπληρώνονται τα πεδία με τα στοιχεία του φοιτητή. Σε αντίθετη περίπτωση η ανάκτηση δεν θα επιστρέψει τίποτα (Εικ. 4α).

3. Η τρίτη φόρμα περιέχει τον πίνακα με τα μαθήματα που ολοκλήρωσε με επιτυχία ο φοιτητής κατά την διάρκεια των σπουδών του (ονόματα μαθημάτων, διδακτικές μονάδες - ECTS, βαθμολογίες). Τα στοιχεία αυτά ανακτώνται με την αναζήτηση του προηγούμενου βήματος και συμπληρώνονται με την βοήθεια της PHP (Εικ. 4β).

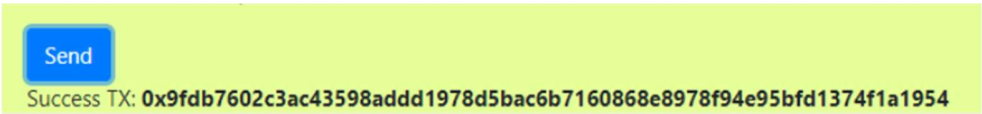
4. Η τέταρτη περιλαμβάνει τα πεδία συμπλήρωσης των διευθύνσεων των ψηφιακών πορτοφολιών και την αποστολή όλων των δεδομένων στο Ethereum. Η διεύθυνση ψηφιακού πορτοφολιού είναι μοναδική για κάθε Ακαδημαϊκό Ίδρυμα και ως εκ τούτου το αντίστοιχο πεδίο προσυμπληρωμένο, ενώ η διεύθυνση ψηφιακού πορτοφολιού του φοιτητή είναι και πάλι μοναδική αλλά την προσκομίζει ο φοιτητής προκειμένου να γίνει ενημέρωση του πορτοφολιού του με τα στοιχεία του τίτλου που πρόκειται να του αποδοθεί. Πριν την ολοκλήρωση της αποστολής πρέπει να γίνει δεκτό το κόστος των συναλλαγών από το MetaMask. Με την ολοκλήρωση και τη τελευταίας συναλλαγής εμφανίζεται το μοναδικό αναγνωριστικό της (transaction id) όπως φαίνεται στην Εικ. 5.

(α). Οι φόρμες 1 και 2 της διεπαφής και η λειτουργία ανάκτησης δεδομένων από την ΒΔ



(β). Οι φόρμες 3 και 4 και η λειτουργία αποστολής δεδομένων στο blockchain

Εικόνα 4. Η διεπαφή (front-end) της καταχώρησης.



Εικόνα 5. Η ταυτότητα μιας επιτυχημένης συναλλαγής (transaction id) σε δεκαεξαδική μορφή.

Η αποστολή των δεδομένων στο blockchain υλοποιήθηκε με χρήση της βιβλιοθήκης web3. js. Στην Εικ. 6, περιγράφεται το τμήμα του κώδικα της βιβλιοθήκης web3. js που είναι υπεύθυνο για την αποστολή των προσωπικών στοιχείων στο Ethereum. Ο κώδικας στην πρώτη γραμμή καλεί μία μέθοδο του έξυπνου συμβολαίου με όνομα “setStudent”. Στην πρώτη παρένθεση περιλαμβάνει τα στοιχεία-ορίσματα της μεθόδου αυτής. Η συνάρτηση “.send” μεταφέρει/αποθηκεύει τα δεδομένα στο έξυπνο συμβόλαιο και χρεώνει το κόστος συναλλαγής στην διεύθυνση του αποστολέα (fromAddress). Ο υπόλοιπος κώδικας αφορά την διαχείριση και εμφάνιση των μηνυμάτων επιτυχίας/αποτυχίας της συναλλαγής με το Ethereum. Η Εικ. 7 αφορά τον κώδικα της αποστολής των μαθημάτων του φοιτητή στο Ethereum και έχει τον ίδιο τρόπο λειτουργίας με την προηγούμενη μέθοδο.

```
Contract.methods.setStudent(toAddress,lastname,name,fname,mname,birthyear,registeryear,specialization).send({from: fromAddress},
function(error, result) {
 if (error) {
     console.log('error: ' + error);
$('#deposit-result').html('<b>Error: </b>' + error);
 else {
 $('#deposit-result').html('Success TX: <b>' + result + '</b>');
```

Εικόνα 6. Αποστολή προσωπικών στοιχείων στο Ethereum

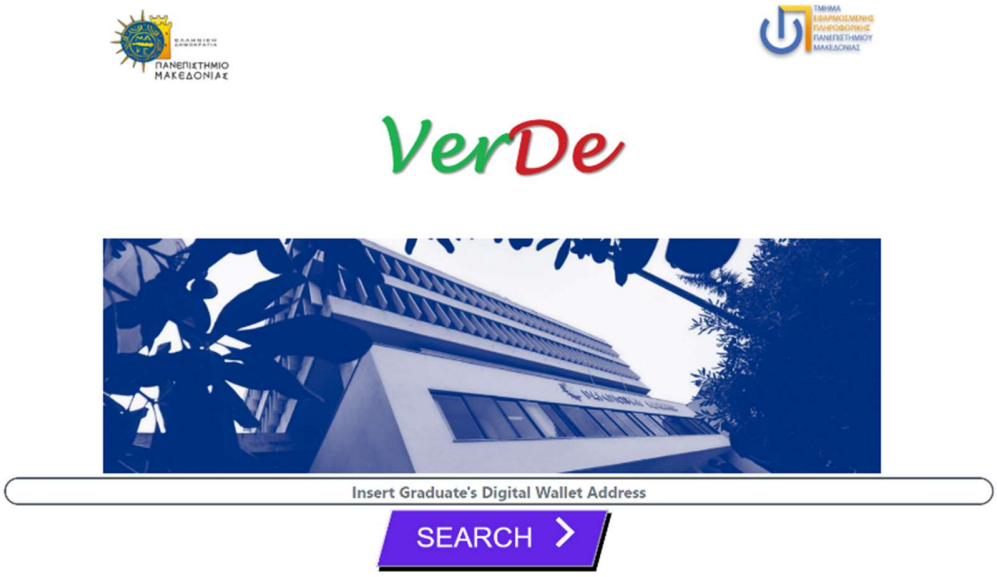
```
Contract.methods.setStudentGrades(toAddress,alldata).send({from: fromAddress},
function(error,result){
    if (error) { console.log('error: ' + error);
            $('#deposit-result').html('<b>Error: </b>' + error);}
    else {  $('#deposit-result').html('Success TX: <b>' + result + '</b>');}
```

Εικόνα 7. Αποστολή των στοιχείων των μαθημάτων που διεκπεραίωσε με επιτυχία ο φοιτητής.

Ο κώδικας των παραπάνω εικόνων εκτελείται στην περίπτωση που ενεργοποιηθεί το «Send» της Εικ. 4β. Σε αυτήν την περίπτωση, εμφανίζεται το MetaMask με δύο συναλλαγές σε αναμονή. Η κάθε συναλλαγή ζητάει την αποδοχή της απόδοσης του φόρου αποστολής στο Ethereum. Μετά την έγκριση, οι miners στο Ethereum εκτελούν την διαδικασία της εξόρυξης (mining) και στην περίπτωση επιτυχίας, εμφανίζεται στο τέλος της διεπαφής η ταυτότητα της συναλλαγής (Εικ. 5). Η ανάπτυξη του συμβολαίου κοστίζει περίπου 0.77$ και η αποθήκευση κάθε φοιτητή 0. 20$ (0. 13$ για τα προσωπικά στοιχεία και 0. 07$ για τα υπόλοιπα) την φορά. Το κόστος αυξομειώνεται ανάλογα τον αριθμό των δεδομένων που αποθηκεύουμε στο Ethereum και την τιμή του Ether την δεδομένη στιγμή αλλά, όχι με βάση τον αριθμό των tokens που στέλνουμε στους φοιτητές.

4.2. Υλοποίηση της διεπαφής επαλήθευσης

Η πρόσβαση και η χρήση της διεπαφής απαιτεί την εγκατάσταση του MetaMask στον περιηγητή του χρήστη. Σχεδιαστικός στόχος ήταν η ευχρηστία και ευκολία στην πρόσβαση. Χρησιμοποιεί δύο φόρμες HTML: την φόρμα για την αναζήτηση της διεύθυνσης του ψηφιακού πορτοφολιού ενός αποφοίτου και τη φόρμα με τα δεδομένα του που εμφανίζεται μετά την αναζήτηση.



Εικόνα 8. Η διεπαφή επαλήθευσης πριν την ενεργοποίηση του «Search»

Οι δύο βασικές λειτουργίες που εκτελεί η διεπαφή αυτή, είναι η κλήση και η εμφάνιση των:

- Προσωπικών στοιχείων του αποφοίτου (Εικ. 9).
- Μαθημάτων που διεκπεραίωσε με επιτυχία ο απόφοιτος (Εικ. 10).

```
Contract.methods.getStudent(fromAddress).call(
    function(error, result) {
    if (error) { console.log('error: ' + error); }
    else { console.log(result);
```

Εικόνα 9. Εμφάνιση προσωπικών στοιχείων του αποφοίτου

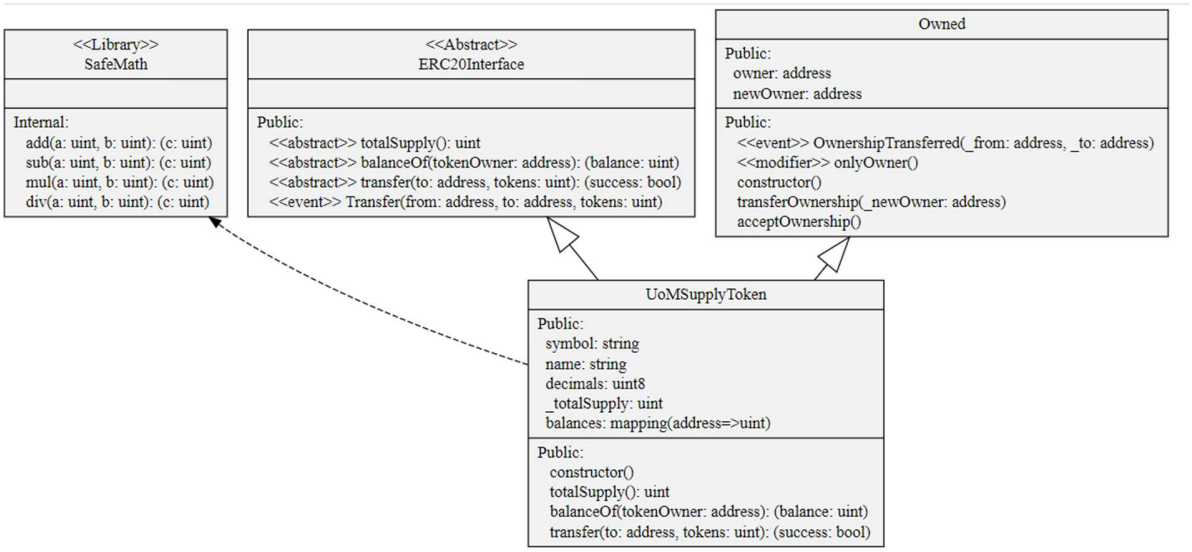
```
Contract.methods.getGradesOfStudent(fromAddress).call(
    function(error, result) {
        if (error) {console.log('error: ' + error);
        } else {
```

Εικόνα 10. Εμφάνιση στοιχείων των μαθημάτων του αποφοίτου

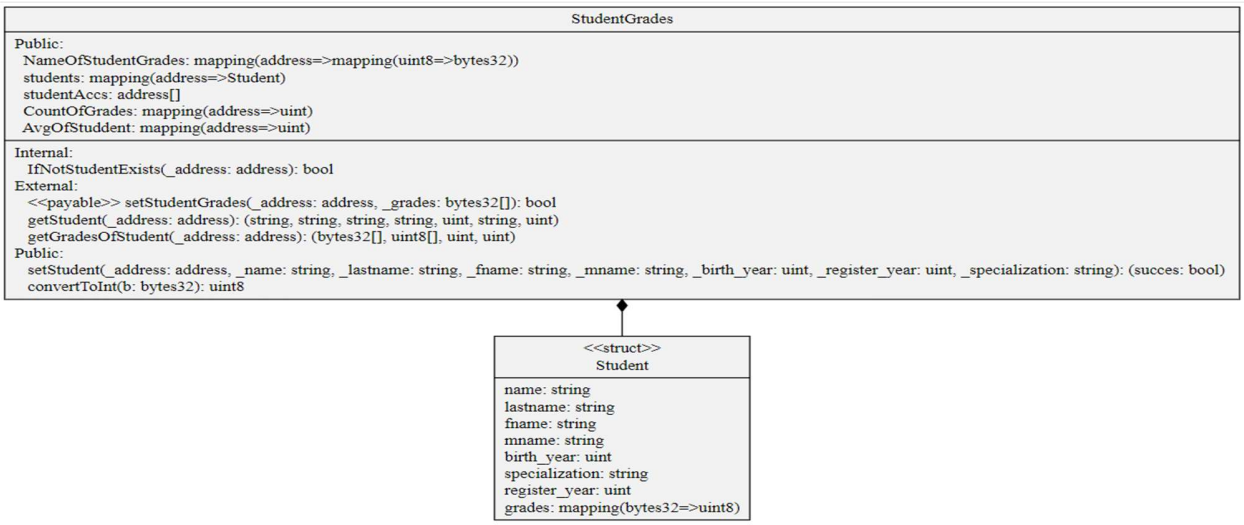
Οι δύο παραπάνω συναλλαγές έχουν ως κοινό σημείο την διεύθυνση του ψηφιακού πορτοφολιού του αποφοίτου («fromAddress»). Οι συναλλαγές είναι ήδη αποθηκευμένες στην κατάσταση του έξυπνου συμβολαίου και επιστρέφονται από αυτή. Οι κλήσεις για την ανάκτηση και επαλήθευση αυτών των πληροφοριών δεν έχουν κάποιο κόστος, καθώς δεν απαιτούν την εκτέλεση υπολογισμών από κάποιο miner του blockchain.

4.3 Υλοποίηση του έξυπνου συμβολαίου

Η υπο-ενότητα αυτή περιέχει μια γρήγορη ανασκόπηση του κώδικα του έξυπνου συμβολαίου της εφαρμογής μας μέσω της ενοποιημένης γλώσσας σχεδίασης προτύπων (Unified Modeling Language -UML). Η Εικ. 11α αναπαριστά τις κλάσεις-συμβόλαια του αρχείου UomToken.sol, που αποτελεί μια εκδοχή του ERC20 token και του StudentGrades.sol, που το δεύτερο κληρονομεί τις λειτουργίες του πρώτου και είναι υπεύθυνο για την αποθήκευση και προβολή των φοιτητών (Εικ. 11β).



(α). Η UML του UomToken.sol



(β). Η UML του StudentGrades.sol

Εικόνα 11. Η UML απεικόνιση του έξυπνου συμβολαίου της εφαρμογής VerDe

Το έξυπνο συμβόλαιο περιλαμβάνει: α) τη μέθοδο για τη δημιουργία του token, β) τη μέθοδο setStudent για την καταχώρηση των προσωπικών στοιχείων του φοιτητή, γ) τη μέθοδο setStudentGrades για τα στοιχεία των μαθημάτων του και την αποστολή των ECTS, δ) τη μέθοδο getStudent, και ε) τη μέθοσο getGradesOfStudent για την κλήση των στοιχείων του. Αυτές αποτελούν τις κύριες μεθόδους, ενώ υπάρχουν και άλλες βοηθητικές την επίτευξή τους. Τέλος, τα δεδομένα των φοιτητών αποθηκεύονται στην κατάσταση (state) του έξυπνου συμβολαίου και επιστρέφονται από αυτή.

4.4. Σύνδεση έξυπνου συμβολαίου με τις διεπαφές

Η σύνδεση με το MetaMask (Εικ. 12) πραγματοποιείται με συναρτήσεις της βιβλιοθήκης web3.js ενώ, η σύνδεση με το έξυπνο συμβόλαιο πραγματοποιείται με την διεύθυνσή του και το αρχείο abi (application binary interface) (Εικ. 13). Το abi είναι ο κώδικας του έξυπνου συμβολαίου σε JSON μορφή και στην Εικ. 13 αρχικοποιεί την μεταβλητή ‘Contract’, στην οποία βασίζονται όλες οι

λειτουργίες της εφαρμογής. Κάθε φορά που γίνεται η πρώτη είσοδος στις διεπαφές από τους χρήστες, το MetaMask ζητά την άδειά τους ώστε να επιτραπεί στην εφαρμογή Verde να χρησιμοποιήσει τα δεδομένα του ψηφιακού πορτοφολιού τους (Εικ. 12).

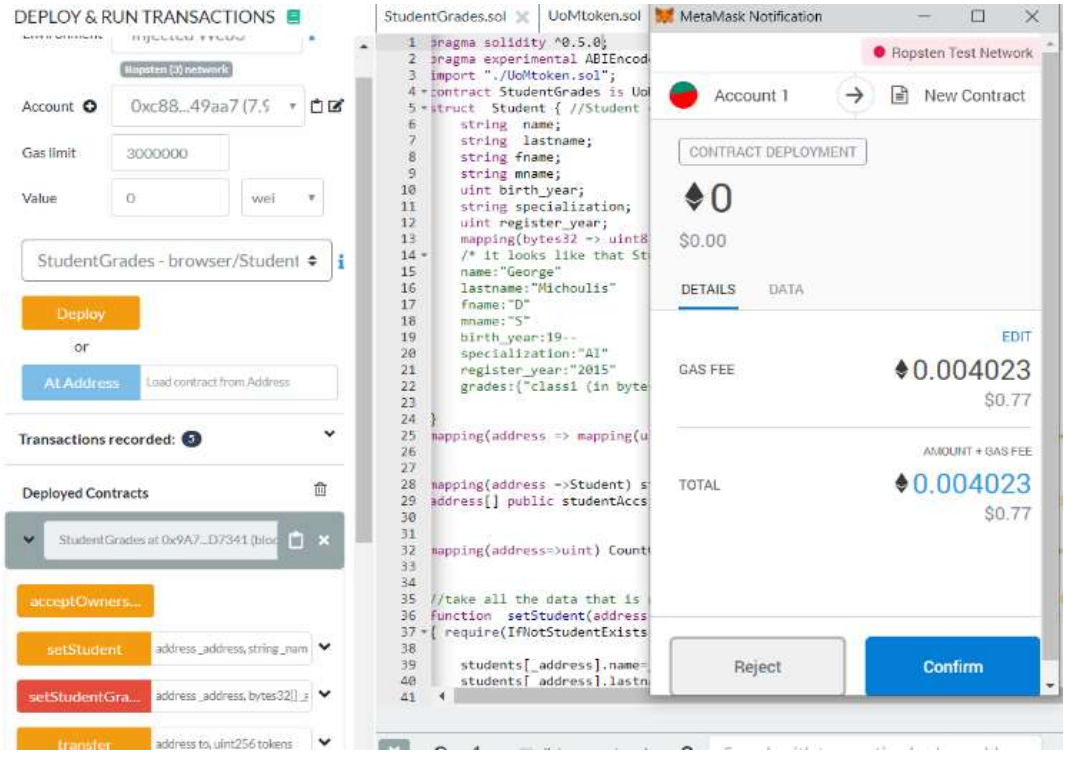
```
if (window.ethereum) {
    window.web3 = new Web3(ethereum);
    try {
        // Request account access if needed
        await ethereum.enable();
        // Acccounts now exposed
        web3.eth.sendTransaction({/* ... */});
    } catch (error) {
        // User denied account access...
    }
```

Εικόνα 12. Ο κώδικας για την σύνδεση με το Metamask

```
var contractAddress = "0x07dc4077f33c7bc71643df7029c59339540a0d1a";
var Contract = new web3.eth.Contract(abi, contractAddress);
```

Εικόνα 13. Ο κώδικας για την σύνδεση με το έξυπνο συμβόλαιο

Για την ανάπτυξη ενός έξυπνου συμβολαίου, χρησιμοποιείται είτε ένα τοπικό περιβάλλον που χρησιμοποιεί την EVM, είτε μια διαδικτυακή διεπαφή όπως το Remix. Το Verde αναπτύχθηκε στο Remix. Η ανάπτυξη του έξυπνου συμβολαίου εκτελείται με το πάτημα του «Deploy» στην καρτέλα «Run» (Εικ. 14). Στην συγκεκριμένη εικόνα έχει ενεργοποιηθεί το «Deploy» και εμφανίστηκε το MetaMask που ζητάει την έγκριση της συναλλαγής. Εάν εγκριθεί η συναλλαγή, τότε θα εμφανιστεί η διεύθυνση του δημοσιευμένου/ανεπτυγμένου έξυπνου συμβόλαιού στην κατηγορία «Deployed Contracts».



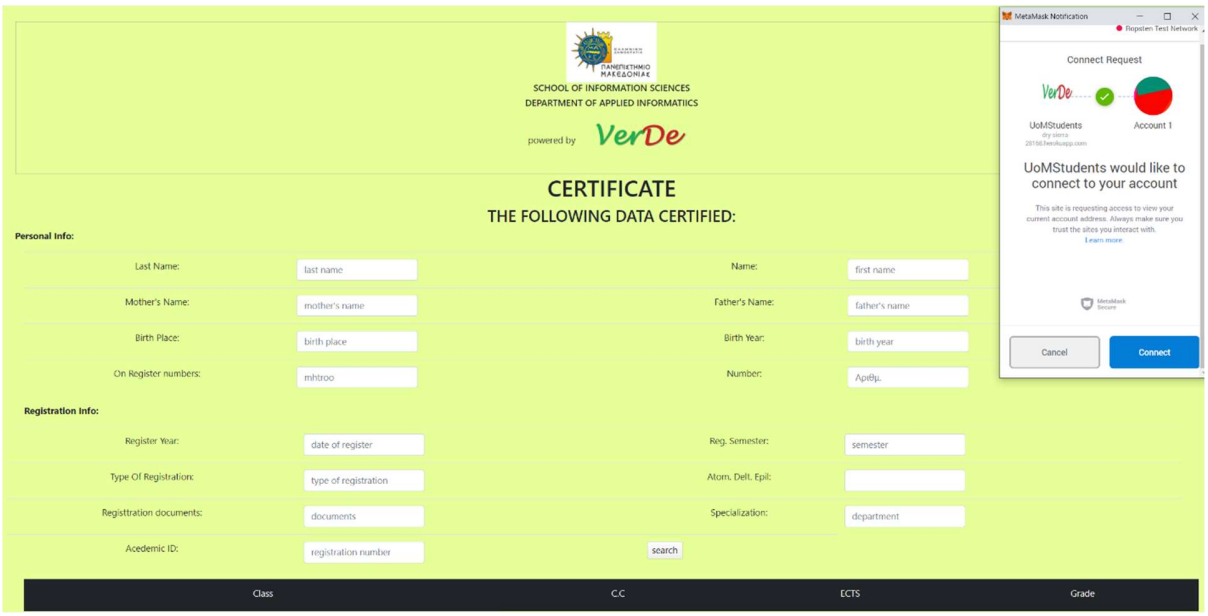
Εικόνα 14. Στιγμιότυπο του Remix και το κόστος ανάπτυξης του έξυπνου συμβολαίου της εφαρμογής Verde

Όταν εκτελείται και αναπτύσσεται το έξυπνο συμβόλαιο στο ολοκληρωμένο περιβάλλον ανάπτυξης (IDE) του Remix τότε, αυτό επεξεργάζεται τον κώδικα του συμβολαίου και απαιτεί να πληρωθεί ένα ποσό σε Ether, το οποίο υπολογίζεται με βάση τον κώδικα του συμβολαίου. Εφόσον ο χρήστης αποδεχτεί το κόστος ανάπτυξης του έξυπνου συμβολαίου, ο μεταγλωττισμένος κώδικάς του μεταφέρετε σε έναν κόμβο για να πραγματοποιηθεί η εξόρυξη. Τέλος, από την στιγμή που διεκπεραιώθηκε η διαδικασία της εξόρυξης δημιουργείται η διεύθυνση του έξυπνου συμβολαίου.

5. Λειτουργία της εφαρμογής Verde

Η ενότητα αυτή παρουσιάζει ένα παράδειγμα λειτουργίας της εφαρμογής VerDe και περεταίρω κατανόηση. Έστω ότι ο φοιτητής Γ.Μ. έχει διεκπεραιώσει τις ακαδημαϊκές του υποχρεώσεις και καταθέτει τα δικαιολογητικά του στο οικείο Ίδρυμα για την έκδοση του πτυχίου του. Μία από τις πληροφορίες που θα καταθέσει θα είναι η διεύθυνση του ψηφιακού του πορτοφολιού. Το οικείο Ίδρυμα διαθέτει πλέον όλα τα απαραίτητα στοιχεία για να προχωρήσει στην καταχώριση του τίτλου του στο blockchain.

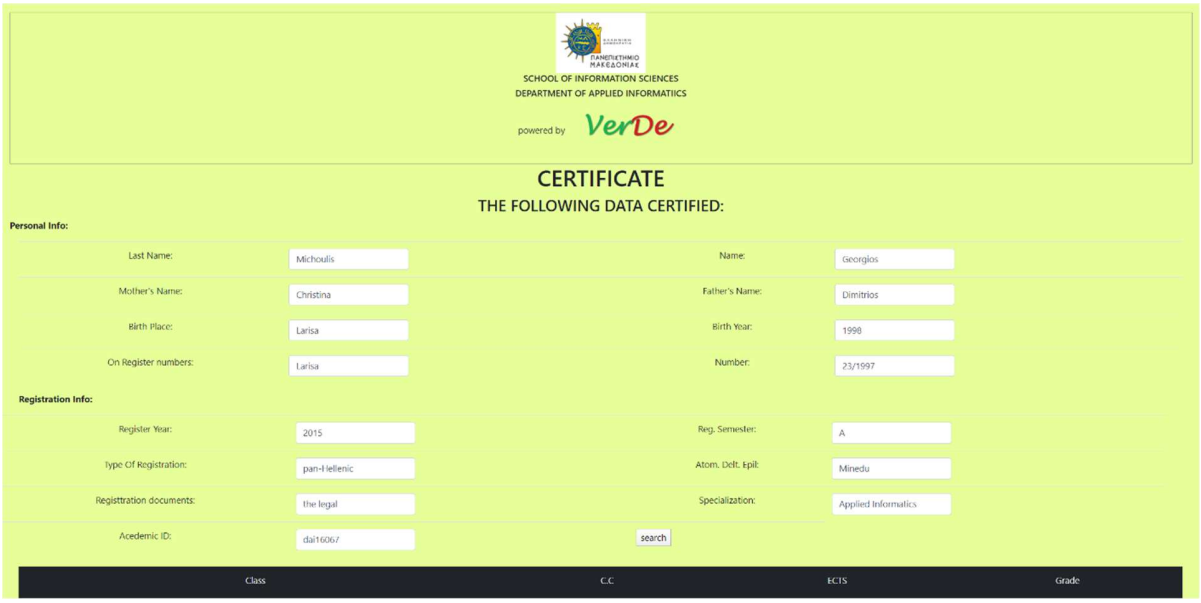
Ξεκινά τη διαδικασία αποδεχόμενο τη σύνδεση του ψηφιακού του πορτοφολιού στο MetaMask (Εικ. 15). Εφόσον αυτή είναι επιτυχής ακολουθεί η μετάβαση στη διεπαφή καταχώρισης. Σε αυτό το σημείο η Ακαδημαϊκή μονάδα εισάγει τον αριθμό μητρώου του φοιτητή στο πεδίο «Academic ID» και ανακτά τα δεδομένα του από την Βάση Δεδομένων της, όπως φαίνεται στην Εικ. 16. Τα στοιχεία αυτά θα αποσταλούν στο Ethereum blockchain μέσω του MetaMask με την εκτέλεση μιας διπλής συναλλαγής (Εικ. 17). Στη περίπτωση επιτυχούς αποστολής στο δίκτυο blockchain θα ειδοποιηθεί ο χρήστης που καταχωρεί τα στοιχεία με την απόδοση και εμφάνιση του transaction id όπως είχαμε δει παραπάνω (Εικόνα 4). Με την απόδοση αυτού του μοναδικού αναγνωριστικού στη συναλλαγή τα στοιχεία του φοιτητή είναι πλέον δημοσιευμένα και χωρίς δυνατότητα μελλοντικής αλλοίωσης στο Ethereum.



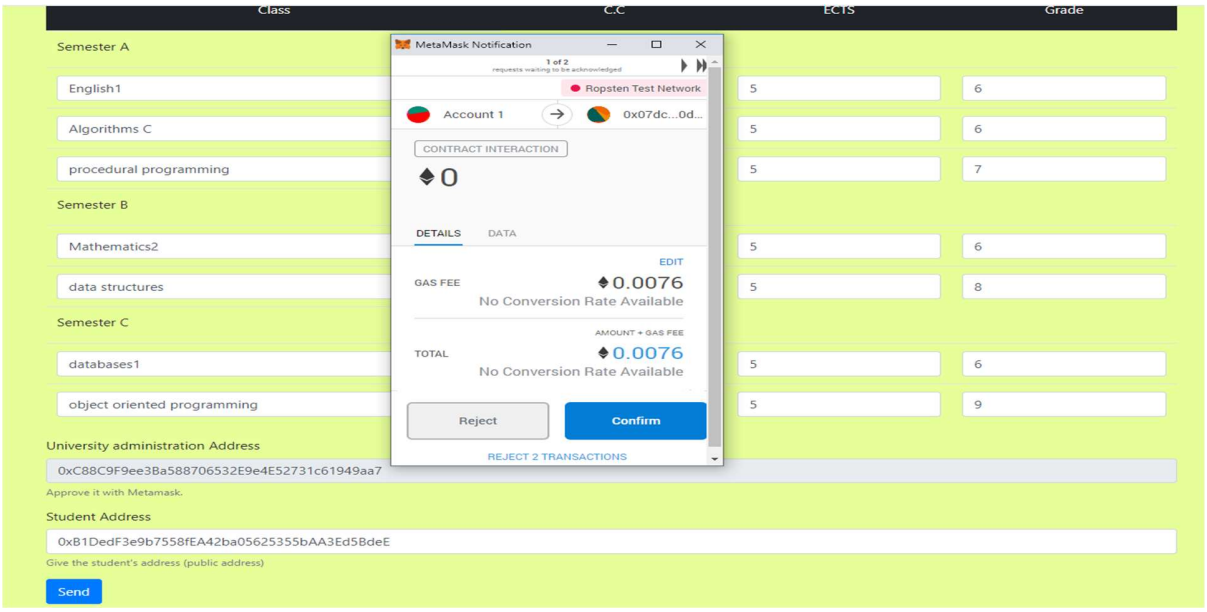
Εικόνα 15. Η είσοδος του πανεπιστημίου στην εφαρμογή

Έστω εν συνεχεία ότι ο Γ.Μ. ως απόφοιτος πλέον επιθυμεί να υποβάλει τον Ακαδημαϊκό του τίτλο στο φάκελο υποψηφιότητάς του για μεταπτυχιακές σπουδές σε άλλο Πανεπιστήμιο. Πρακτικά μπορεί να υποβάλει τη διεύθυνση του ψηφιακού του πορτοφολιού στο Ίδρυμα Υποδοχής με χρήση του οποίου μπορεί να γίνει επαλήθευση του τίτλου του που βρίσκεται δημοσιευμένο στο Ethereum

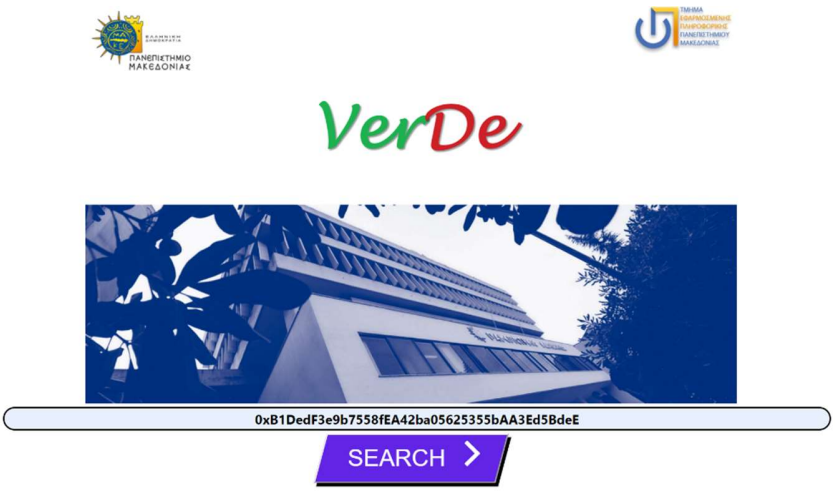
blockchain. Το Ίδρυμα υποδοχής συνδέεται και αυτό μέσω του MetaMask (Εικ. 15) στην εφαρμογή Verde, αλλά πλέον στην διεπαφή επαλήθευσης αυτής. Αναζητεί τον τίτλο πτυχίου του υποψηφίου για μεταπτυχιακές σπουδές εισάγοντας τη διεύθυνση του ψηφιακού του πορτοφολιού στο πεδίο της Εικ. 18 και λαμβάνει τα επαληθευμένα δεδομένα του όπως δείχνει η Εικ. 19. Επειδή τα δεδομένα ανακτήθηκαν από το Ethereum blockchain, το Ίδρυμα υποδοχής τα αποδέχεται ως αυθεντικά και μπορεί να προχωρήσει με την αξιολόγηση της υποψηφιότητας του Γ.Μ.



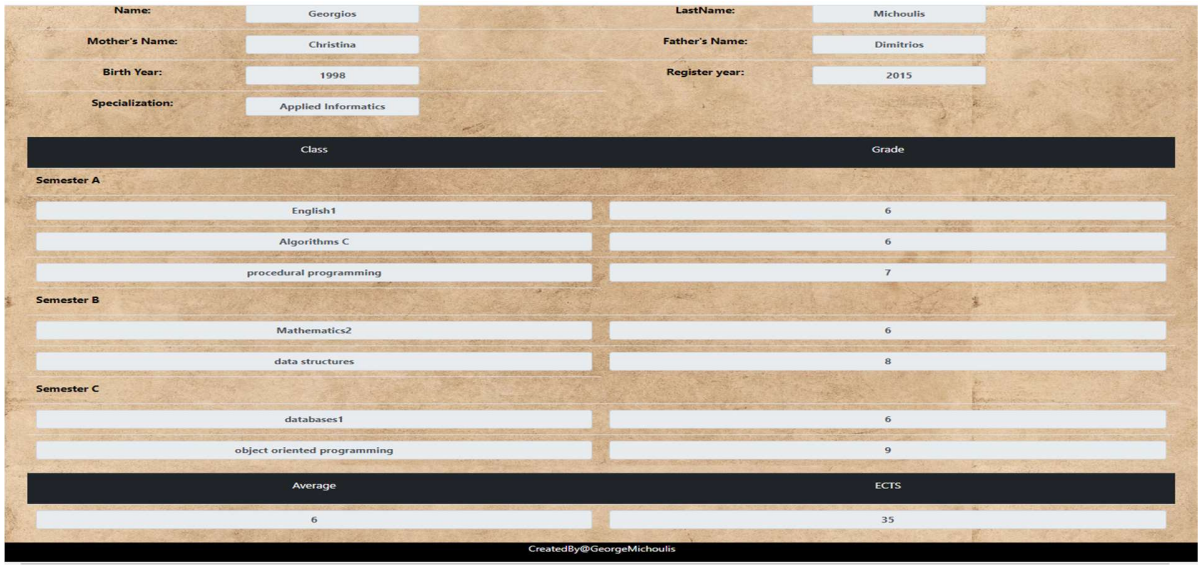
Εικόνα 16. Η ενεργοποίηση του "search" και εμφάνιση των στοιχείων του φοιτητή



Εικόνα 17. Η αποστολή των δεδομένων του φοιτητή στο Ethereum μέσω του MetaMask



Εικόνα 18. Η καταχώριση της διεύθυνσης του ψηφιακού πορτοφολιού του αποφοίτου



Εικόνα 19. Η επαλήθευση των στοιχείων του πτυχίου του αποφοίτου

6. Επίλογος και μελλοντική έρευνα

Ολοκληρώνοντας το άρθρο, η ενότητα αυτή καταγράφει κάποιους περιορισμούς της εφαρμογής Verde και ιδέες για το πως μπορούν να αντιμετωπιστούν. Η εφαρμογή υποθέτει την ύπαρξη μιας αρχής (π.χ. Υπουργείο Παιδείας) που θα εκδίδει και θα γνωστοποιεί τη διεύθυνση ψηφιακού πορτοφολιού κάθε Ακαδημαϊκού Ιδρύματος, επιπλέον χρησιμοποιεί το token ERC20 και αρχικοποιεί ένα πλήθος tokens που δεν μπορούν να επαναδημιουργηθούν, οπότε μετά από κάποιο χρονικό όριο θα εξαντληθούν και τότε θα χαθεί η λειτουργία της αποστολής των ECTS. Επιπλέον, αν σταλούν τα δεδομένα του φοιτητή σε λάθος διεύθυνση (π.χ., λόγω κεκτημένης ταχύτητας) δεν υπάρχει τρόπος ανάκλησης της συναλλαγής. Οι λύσεις σε αυτά τα ζητήματα αποτελούν αντικείμενο της μελλοντικής μας έρευνας. Εξετάζουμε επίσης το ζήτημα επαλήθευσης τίτλων όταν αυτοί υποβάλλονται σε Ιδρύματα του εξωτερικού. Είναι

σίγουρο ότι στα χρόνια που έπονται οι υπηρεσίες ασφάλειας που παρέχει η τεχνολογία blockchain θα συνδράμουν σημαντικά στις ηλεκτρονικές υπηρεσίες του ιδιωτικού και δημόσιου φορέα.

Βιβλιογραφία

[1] " Διευθυντής κλινικής χειρουργούσε για χρόνια με πλαστό τίτλο σπουδών", 21-11-2015. Διαθέσιμο: https://www.tovima.gr/2015/11/21/society/dieythyntis-klinikis-xeiroyrgoyse-gia-xronia-me-plasto-titlo-spoydwn/.

[2] "Το στηθοσκόπιο δεν κάνει τον γιατρό", 07-06-2014. Διαθέσιμο: https://www.kathimerini.gr/770855/article/epikairothta/ellada/to-sth8oskopio-den-kanei-ton-giatro.

[3] "Στο Ελεγκτικό Συνέδριο η επιστροφή αποδοχών νοσηλεύτριας για πλαστό πτυχίο", 05-02-2020. Διαθέσιμο: https://www.kathimerini.gr/1063512/article/epikairothta/ellada/sto-elegktiko-synedrio-h-epistrofh-apodoxwn-noshleytrias-gia-plasto-ptyxio.

[4] "Μεσσηνία: 10 μήνες φυλάκιση γιατί είχε πλαστό πτυχίο!", 31-05-2017. Διαθέσιμο: https://eleftheriaonline.gr/local/koinonia/dikastiko/item/125650-messinia-10-mines-fylakisi-giati-eixe-plasto-ptyxio.

[5] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview", National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8202, Oct. 2018.

[6] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, "EduCTX: A Blockchain-Based Higher Education Credit Platform", IEEE Access, vol. 6, pp. 5112–5127, 2018.

[7] Block.co, "Our Product", Block.co. [Online]. Διαθέσιμο: https://block.co/our-product/

[8] N. Kube, "Daniel Drescher: Blockchain basics: a non-technical introduction in 25 steps", *Financial Markets and Portfolio Management*, vol. 32, no. 3, pp. 329–331, Aug. 2018.

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[10] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, p. 20.

[11] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Crypto-Currencies, 1st ed. O'Reilly Media, Inc., 2014.

[12] D. G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger".

[13] A. M. Antonopoulos and G. W. Ph. D, Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media, Inc., 2018.

[14] "Ethereum Explained: Merkle Trees, World State, Transactions, and More", *kauri. io*. Διαθέσιμο: /ethereum-explained-merkle-trees-world-state-transa/1f4196c3db7f41e5845f063dc1581a4e/a.

[15] R. Tonelli, G. Destefanis, M. Marchesi, and M. Ortu, "Smart Contracts Software Metrics: a First Study", Feb. 2018.

[16] "ERC20 Token Standard – Ethereum Smart Contracts – BitcoinWiki", Διαθέσιμο: https://en. bitcoinwiki. org/wiki/ERC20.

[17] D. Zinca and V. -A. Negrean, "Development of a Road Tax Payment Application using the Ethereum Platform", International Symposium on Electronics and Telecommunications (ISETC), Timisoara, 2018, pp. 1–4.

[18] "Ethereum (ETH) price, charts, market cap, and other metrics", CoinMarketCap. Διαθέσιμο: https://coinmarketcap. com/currencies/ethereum/.