

IoTFeds

Κατανεμημένες Αγορές Δεδομένων για IoT Ομοσπονδίες
Distributed Data Marketplaces for IoT Federations

Π3.1– Αναφορά Μηχανισμών Καταγραφής και Ελέγχου Συναλλαγών

ΔΡΑΣΗ ΕΘΝΙΚΗΣ ΕΜΒΕΛΕΙΑΣ:
«ΕΡΕΥΝΩ-ΔΗΜΙΟΥΡΓΩ-ΚΑΙΝΟΤΟΜΩ Β' ΚΥΚΛΟΣ»
«ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ, ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ & ΚΑΙΝΟΤΟΜΙΑ» (ΕΠΑνΕΚ)
Ειδική Υπηρεσία Διαχείρισης Επιχειρησιακού Προγράμματος Ανταγωνιστικότητα
Επιχειρηματικότητα και Καινοτομία (ΕΥΔ ΕΠΑνΕΚ)
Ειδική Υπηρεσία Διαχείρισης και Εφαρμογής Δράσεων στους τομείς
Έρευνας, Τεχνολογικής Ανάπτυξης και Καινοτομίας
(ΕΥΔΕ ΕΤΑΚ)



Έργο	IoTFeds
Κωδικός Έργου	T2EΔK-02178
Ενότητα Εργασίας	EE3 (Δ3.1)
Υπεύθυνος Ενότητας	ΟΠΑ
Υπεύθυνος Παραδοτέου	EKETA
Έκδοση Παραδοτέου	1.0
Ημερομηνία	14/07/2023

Συντονιστές Παραδοτέου

Ευάγγελος Αθανασάκης, EKETA
Ζήσης Σακελλαρίου, EKETA
Γεώργιος Σπανός, EKETA
Αβραάμ Τεπελίδης, EKETA
Γεώργιος Χαρμάνας, EKETA

Υπεύθυνοι Συγγραφής

Απόστολος Νάσιου, ICOM
Δημήτριος Λασκαράτος, ICOM
Έλια Πιέτρη, ICOM
Κωνσταντίνος Τσάκαλος, ICOM
Μαρία Τσαρουχά, ICOM
Μάριος Χαραλαμπίδης, ICOM
Στέλιος Γκούσκος, TERRACOM
Κωνσταντίνος Καλαμπόκης, TERRACOM
Ναταλία Ουμνόβα, TERRACOM
Δήμητρα Καραδήμου ΟΠΑ
Ευάγγελος Μαρκάκης ΟΠΑ
Γεώργιος Νταρζάνος ΟΠΑ
Αθανάσιος Παπαϊωάννου ΟΠΑ
Γεώργιος Σταμούλης ΟΠΑ

Ακρωνύμια

Ακρωνύμιο	Ορισμός
BaaS	Blockchain as a Service
HLF	Hyperledger Fabric
ID	Identification
IoT	Internet of Things
EE	Ενότητα Εργασίας

Σύνοψη Παραδοτέου

Το παρόν έγγραφο αποτελεί παραδοτέο για το έργο IoTFeds, το οποίο χρηματοδοτείται από το Επιχειρησιακό Πρόγραμμα «Ανταγωνιστικότητα, Επιχειρηματικότητα & Καινοτομία» (ΕΠΑνΕΚ) υπό τη δράση εθνικής εμβέλειας «Ερευνώ – Δημιουργώ – Καινοτομώ Β' Κύκλος» του ΕΣΠΑ (2014-2020). Κύριος στόχος του συγκεκριμένου παραδοτέου είναι η παρουσίαση της υλοποίησης των μηχανισμών που αναπτύχθηκαν στα πλαίσια της Δ3.1 «Καταγραφή και Έλεγχος Συναλλαγών», που αποτελεί μέρος της ΕΕ3 – «Ομόσπονδη Αγορά IoT». Στόχος του συγκεκριμένου έργου είναι η δημιουργία και ανάπτυξη μιας λύσης που θα επιτρέπει σε εταιρείες IoT (πάροχοι ή καταναλωτές δεδομένων) να δραστηριοποιούνται σε αποκεντρωμένες συλλογικές αγορές IoT δεδομένων.

Το παρόν παραδοτέο (Π3.1 – «Αναφορά Μηχανισμών Καταγραφής και Ελέγχου Συναλλαγών») επικεντρώνεται στην ανάλυση του σχεδιασμού και της υλοποίησης των μηχανισμών καταγραφής των συναλλαγών, καθώς και με τους μηχανισμούς που επιτρέπουν τον έλεγχο και εποπτεία τους. Οι μηχανισμοί αυτοί στηρίζονται στην χρήση του blockchain, το οποίο επιτρέπει την καταγραφή των συναλλαγών στον ledger από προεπιλογή αφού αποτελεί έναν από τους βασικούς κανόνες που διέπουν τη λειτουργία του. Το πρώτο μέρος του παραδοτέου ασχολείται με την εξερεύνηση του τεχνολογικού υποβάθρου για τη χρήση μηχανισμών καταγραφής και ελέγχου συναλλαγών βασισμένων σε blockchain, τόσο ευρύτερα στη βιβλιογραφία όσο και στην εφαρμογή τους στον τομέα των IoT συσκευών και δεδομένων, όπως επίσης και τη χρήση ειδικών νομισμάτων βασισμένων στο Hyperledger Fabric.

Στο υπόλοιπο μέρος του παραδοτέου Π3.1 περιγράφονται οι μηχανισμοί που καλούνται να αναπτυχθούν στα πλαίσια του IoTFeds και ικανοποιούν τις απαιτήσεις της δράσης Δ3.1, σχετικά με την καταγραφή και έλεγχο των συναλλαγών με στόχο να χρησιμοποιηθούν τόσο από άλλες δράσεις της ενότητας ΕΕ3, όπως αυτή που ασχολείται με τον υπολογισμό των χρεώσεων. Οι συναλλαγές για τις οποίες θεωρούμε ότι είναι απαραίτητο να γίνεται η καταγραφή και ο έλεγχός τους, χωρίζονται σε δύο κατηγορίες. Οι δύο μηχανισμοί για κάθε κατηγορία αναλύονται σε ξεχωριστά υποκεφάλαια, και παρουσιάζονται οι υλοποιήσεις από την μεριά του στοιχείου του BaaS, αλλά και από την μεριά του simbloTe.

Τέλος, το Π3.1 ολοκληρώνεται με κάποια βασικά συμπεράσματα που προέκυψαν κατά την υλοποίηση της δράσης Δ3.1, αλλά και μελλοντικές ενέργειες για τις επόμενες και άμεσα συσχετιζόμενες δράσεις.

Πίνακας Περιεχομένων

1	Εισαγωγή	9
1.1	Αντικείμενο του Παραδοτέου.....	9
1.2	Υπόβαθρο	9
1.3	Δομή του Παραδοτέου.....	9
2	Εξερεύνηση Τεχνολογικού Υποβάθρου.....	10
2.1	Μηχανισμοί καταγραφής και ελέγχου συναλλαγών με χρήση Blockchain.....	10
2.2	Καταγραφή και έλεγχος συναλλαγών με χρήση Blockchain για IoT πόρους	14
3	Καταγραφή και έλεγχος συναλλαγών στο IoTFeds.....	17
3.1	Καταγραφή αγορών IoT προϊόντων στο BaaS.....	18
3.2	Έλεγχος αγορών IoT προϊόντων στο BaaS.....	22
3.3	Καταγραφή χρήσης IoT προϊόντων στο BaaS	30
3.4	Έλεγχος χρήσης IoT προϊόντων στο BaaS.....	34
3.5	Έλεγχος αγορών και χρήσεων IoT προϊόντων στο Marketplace	40
4	Συμπεράσματα	48
	Βιβλιογραφία	49

Ευρετήριο Εικόνων

Εικόνα 1: Αρχιτεκτονική και στοιχεία λογισμικού για τον μηχανισμό καταγραφής ενεργειών μεταξύ οργανισμών (L. Van Hove, 2019).....	11
Εικόνα 2 : Αρχιτεκτονική του JusticeChain (Belchior, 2019).	12
Εικόνα 3 : Διάγραμμα ροής για την καταγραφή ενός log στο προτεινόμενο σύστημα (Benedikt Putz, 2019).	13
Εικόνα 4 : Αρχιτεκτονική υψηλού επιπέδου του προτεινόμενου συστήματος blockchain (Brotsis, 2019)	14
Εικόνα 5 : Η συναλλαγή που πραγματοποιούν οι "μάρτυρες", μέσω των smart contracts και η αποθήκευσή της στον ledger (M. H. Chinaei, 2021).	15
Εικόνα 6 : Αρχιτεκτονική του προτεινόμενου συστήματος (S. Ali, 2018).	16
Εικόνα 7: Παράμετροι του endpoint για την αγορά προϊόντος στο BaaS.	19
Εικόνα 8: Αντικείμενο που επιστρέφεται και περιλαμβάνει την απόδειξη της αγοράς.	20
Εικόνα 9: Το αντικείμενο της απόδειξης αγοράς.	20
Εικόνα 10: Διάγραμμα ακολουθίας για την καταγραφή αγοράς ενός προϊόντος.	21
Εικόνα 11: Παράμετροι για το endpoint του ελέγχου των αγορών ενός χρήστη.	23
Εικόνα 12: Αντικείμενο που επιστρέφεται και περιλαμβάνει όλες τις αποδείξεις αγορών ενός χρήστη.	24
Εικόνα 13: Παράμετροι για το endpoint του ελέγχου των πωλήσεων ενός χρήστη.	25
Εικόνα 14: Αντικείμενο που επιστρέφεται και περιλαμβάνει τις πωλήσεις ενός χρήστη.	26
Εικόνα 15: Διάγραμμα ακολουθίας για τον έλεγχο των συναλλαγών ενός χρήστη.	27
Εικόνα 16: Παράμετροι για το endpoint του ελέγχου ακεραιότητας μιας απόδειξης αγοράς.	28
Εικόνα 17: Αντικείμενο που επιστρέφεται από τον έλεγχο ακεραιότητας.	28
Εικόνα 18: Διάγραμμα ακολουθίας για τον έλεγχο εγκυρότητας μιας απόδειξης συναλλαγής.	29
Εικόνα 19: Παράμετροι για το endpoint της ασφαλούς πρόσβασης σε ένα προϊόν.	31
Εικόνα 20: Αντικείμενο που επιστρέφεται και περιλαμβάνει τις πηγές δεδομένων και τις εναπομένουσες φορές πρόσβασης.	32
Εικόνα 21: Το αντικείμενο της απόδειξης χρήσης ενός προϊόντος.	32
Εικόνα 22: Διάγραμμα ακολουθίας για την καταγραφή απόδειξης χρήσης προϊόντος.	33
Εικόνα 23: Παράμετροι για το endpoint του ελέγχου της χρήσης IoT προϊόντων.	35
Εικόνα 24: Αντικείμενο που επιστρέφεται με τις καταγραφές χρήσης των IoT προϊόντων.	36
Εικόνα 25: Διάγραμμα ακολουθίας του ελέγχου απόδειξης χρήσης.	37
Εικόνα 26: Παράμετροι εισόδου για το endpoint του ελέγχου ακεραιότητας μιας απόδειξης χρήσεως ενός IoT προϊόντος.	38
Εικόνα 27: Το αντικείμενο που επιστρέφεται από τον έλεγχο ακεραιότητας μιας απόδειξης χρήσεως ενός IoT προϊόντος.	38
Εικόνα 28: Διάγραμμα ακολουθίας για τον έλεγχο εγκυρότητας απόδειξης χρήσης.	39
Εικόνα 29: Εμφάνιση του wallet με τα tokens του χρήστη.	41
Εικόνα 30: Endpoint για την ανάκτηση της λίστας των tokens του χρήστη (wallet) στο Marketplace.	41
Εικόνα 31: Επιλογές για έλεγχο αποδείξεων και logs του χρήστη.	42
Εικόνα 32: Αποδείξεις αγοράς ενός προϊόντος.	42
Εικόνα 33: Απάντηση με τη λίστα αποδείξεων αγοράς του χρήστη.	43
Εικόνα 34: Έλεγχος εγκυρότητας συναλλαγής για προϊόν που έχει αγοράσει ο χρήστης.	43
Εικόνα 35: Απάντηση αιτήματος ελέγχου εγκυρότητας συναλλαγής.	43
Εικόνα 36: Αναζήτηση αποδεικτικών χρήστη για προϊόντα που πούλησε.	44
Εικόνα 37: Αποδείξεις συναλλαγών χρήστη για προϊόντα που πούλησε.	44
Εικόνα 38: Έλεγχος εγκυρότητας συναλλαγής για προϊόν που έχει πουλήσει ο χρήστης.	45
Εικόνα 39: Αναζήτηση αποδεικτικών χρήσης στο Marketplace.	45
Εικόνα 40: Απάντηση αναζήτησης αποδεικτικών χρήσης.	46
Εικόνα 41: Έλεγχος εγκυρότητας αποδεικτικών χρήσης στο Marketplace.	46

Ευρετήριο Πινάκων

Πίνακας 1: Endpoint μέσω του οποίου πραγματοποιείται η καταγραφή της αγοράς.	18
Πίνακας 2: Endpoints που περιγράφουν τον συναλλαγών ενός χρήστη.	22
Πίνακας 3: Endpoint που περιγράφει τον έλεγχο πρόσβασης.	30
Πίνακας 4: Endpoint που περιγράφει τον έλεγχο χρήσης των IoT προϊόντων από το χρήστη.	34
Πίνακας 5: Διεπαφές σχετικά με τον έλεγχο αγορών και χρήσεων IoT προϊόντων στο Marketplace.	40

1 Εισαγωγή

Σκοπός αυτού του παραδοτέου είναι η περιγραφή και ανάλυση του σχεδιασμού και υλοποίησης των μηχανισμών καταγραφής και ελέγχου συναλλαγών που πραγματοποιούνται στα πλαίσια της IoTFeds πλατφόρμας, και βασίζονται στην τεχνολογία του blockchain. Οι συναλλαγές αυτές σχετίζονται με την αγορά προϊόντων, μέσα από την λειτουργία της ομοσπονδιακής και καθολικής αγοράς, αλλά και τη χρήση των προϊόντων. Στις ενότητες που ακολουθούν γίνεται εξερεύνηση του τεχνολογικού υποβάθρου σχετικά με υπάρχουσες μεθόδους καταγραφής και ελέγχου, ενώ στη συνέχεια παρουσιάζονται οι σχετικές μέθοδοι που υλοποιούνται στα πλαίσια του IoTFeds, για την καταγραφή και έλεγχο των συναλλαγών.

1.1 Αντικείμενο του Παραδοτέου

Στο συγκεκριμένο παραδοτέο του έργου IoTFeds παρουσιάζεται ο σχεδιασμός και η ανάπτυξη μεθόδων για την καταγραφή και έλεγχο των συναλλαγών, που σχετίζονται με την αγορά και χρήση των IoT προϊόντων.

Οι μηχανισμοί που περιγράφονται στη συνέχεια ως κύριο μέρος της δράσης Δ3.1, αποτελούν τόσο την αφετηρία για επόμενες δράσεις, όσο και μια αυτόνομη λειτουργία που παρέχεται στην πλατφόρμα του IoTFeds, με τη μορφή ενός μηχανισμού καταγραφής και ελέγχου (logging and auditing). Αναλυτικότερα, οι στόχοι που εκπληρώθηκαν στο παραδοτέο Π3.1 είναι οι ακόλουθοι:

- Μελέτη του τεχνολογικού υποβάθρου παρόμοιων μηχανισμών
- Περιγραφή και ανάλυση μεθόδων καταγραφής συναλλαγών με χρήση blockchain
- Περιγραφή και ανάλυση μεθόδων εποπτείας/ελέγχου των καταγεγραμμένων συναλλαγών (auditing)

1.2 Υπόβαθρο

Το παραδοτέο Π3.1 το οποίο περιγράφει τις ενέργειες που πραγματοποιούνται κάτω από την δράση Δ3.1 – «Καταγραφή και Έλεγχος Συναλλαγών», συνδέεται άμεσα με δράσεις τόσο της ενότητας ΕΕ2 (Δ2.4 – «Ασφαλής Πρόσβαση σε Δεδομένα IoT») που έχουν ήδη εκπονηθεί, όσο και με επερχόμενες δράσεις από την ενότητα ΕΕ3 (Δ3.2 – «Ανάθεση Τιμών και Πολιτικών Χρέωσης» και Δ3.3 – «Εναλλακτικός Μηχανισμός Ανταλλαγής Πόρων IoT»). Πιο συγκεκριμένα σχετίζεται με το παραδοτέο Π2.2 – «Αναφορά Μηχανισμών Διαφήμισης, Ανακάλυψης και Ασφαλούς Πρόσβασης σε Πόρους IoT», αφού η λειτουργία της καταγραφής της χρήσης ενός IoT προϊόντος συνδέεται με την ασφαλή πρόσβαση του χρήστη σε αυτό.

1.3 Δομή του Παραδοτέου

Το παραδοτέο έχει την ακόλουθη δομή:

- Το Κεφάλαιο 2 περιέχει τη μελέτη και την εξερεύνηση του τεχνολογικού υποβάθρου σχετικά με υπάρχοντες μηχανισμούς καταγραφής και ελέγχου ενεργειών με τη χρήση blockchain, τόσο στον τομέα του IoT, αλλά και γενικότερα σε διάφορες άλλες εφαρμογές.
- Το Κεφάλαιο 3 περιλαμβάνει την αναλυτική περιγραφή των μεθόδων καταγραφής, εποπτείας και ελέγχου ακεραιότητας συναλλαγών που υλοποιούνται κατά κύριο λόγο από το BaaS.
- Τέλος, το Κεφάλαιο 4 περιέχει τα συμπεράσματα που προκύπτουν από αυτό το παραδοτέο και θα αξιοποιηθούν από τις επόμενες και άμεσα εμπλεκόμενες δράσεις.

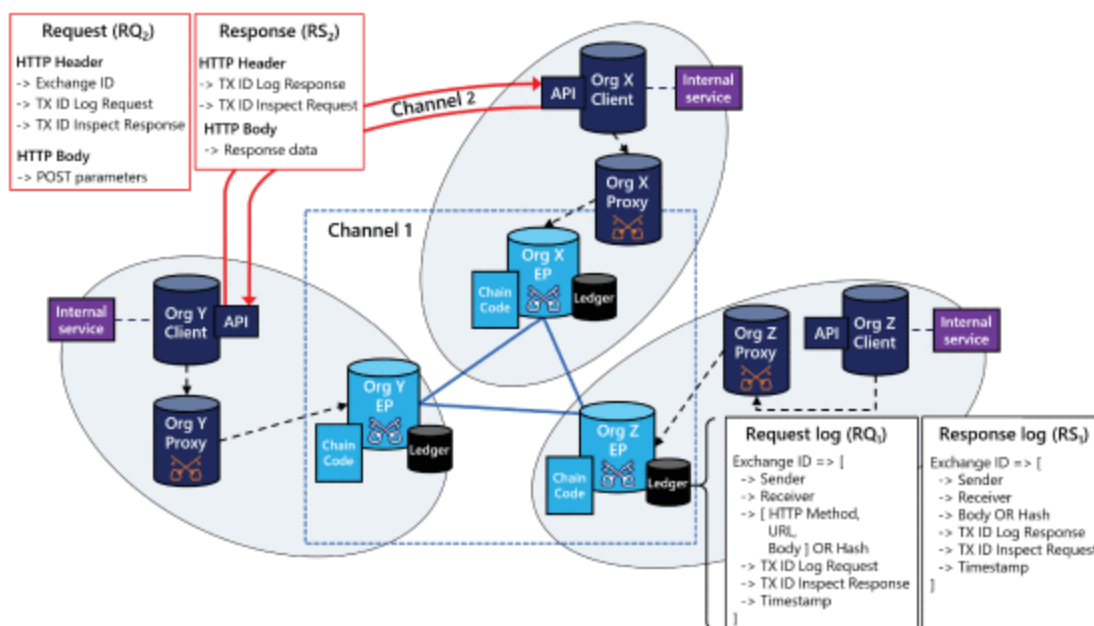
2 Εξερεύνηση Τεχνολογικού Υποβάθρου

Στο παρόν κεφάλαιο παρουσιάζεται μια σύντομη περιγραφή των μεθόδων καταγραφής (logging) και ελέγχου (auditing) συναλλαγών και διαφόρων ενεργειών, που πραγματοποιούνται με τη βοήθεια της τεχνολογίας του blockchain, όπως αυτές συναντώνται στη σύγχρονη βιβλιογραφία. Τέτοιοι μηχανισμοί ενσωματώνονται σε διάφορες εφαρμογές και τομείς της τεχνολογίας, όπως επίσης και σε εφαρμογές των IoT συσκευών και εφαρμογών. Επομένως, γίνεται μια προσπάθεια ώστε να καλυφθούν μέθοδοι από διάφορους τομείς, συμπεριλαμβανομένου και αυτού του IoT. Αυτές οι μέθοδοι αποτελούν το εφαλτήριο βήμα και τη βάση για τον σχεδιασμό και την υλοποίηση των αντίστοιχων μηχανισμών για την IoTFeds πλατφόρμα.

2.1 Μηχανισμοί καταγραφής και ελέγχου συναλλαγών με χρήση Blockchain

Οι μηχανισμοί καταγραφής συναλλαγών, οι οποίες με την ευρύτερη έννοια μπορούν θεωρηθούν ως οποιαδήποτε ενέργεια ενός χρήστη σε ένα σύστημα και οι οποίες ενεργοποιούν έναν τέτοιο μηχανισμό, μπορούν να καταγραφούν με αμετάβλητο τρόπο με τη χρήση του blockchain στον ledger. Σε πολλές περιπτώσεις, ιδιαίτερα όταν πρόκειται για εκτέλεση σημαντικών ενεργειών, όπως για παράδειγμα μεταφορά χρημάτων, διαμοιρασμό ευαίσθητων δεδομένων, είναι σημαντική η ύπαρξη στοιχείων με στόχο την απόδειξη της συγκεκριμένης ενέργειας, αν και όποτε αυτό απαιτηθεί. Το blockchain και οι μηχανισμοί του προσφέρουν όλα τα απαραίτητα χαρακτηριστικά, όπως είναι η μη μεταβλητότητα και η διαφάνεια στις συναλλαγές που πραγματοποιούνται, καθιστώντας το ένα χρήσιμο εργαλείο για την υλοποίηση παρόμοιων μεθόδων. Ωστόσο, ένας σημαντικός παράγοντας, είναι ότι το blockchain δεν ενδείκνυται για τη χρήση του ως βάση δεδομένων, δηλαδή για την αποθήκευση μεγάλου όγκου δεδομένων. Προς αυτή την κατεύθυνση, χρησιμοποιούνται συμπληρωματικά κι άλλες τεχνολογίες με δυνατότητες αποθήκευσης, όπως για παράδειγμα οι τεχνολογίες cloud. Παρακάτω αναλύονται μερικοί μηχανισμοί logging και auditing, όπως αυτοί σχεδιαστεί και παρουσιαστεί στην τρέχουσα βιβλιογραφία.

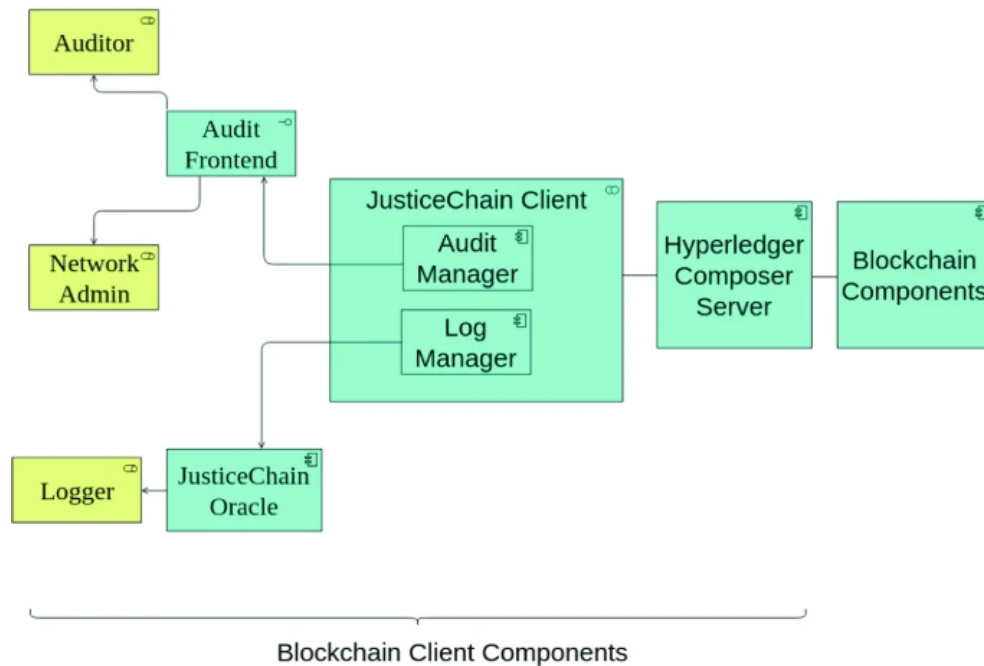
Οι (L. Van Hoya, 2019) προτείνουν έναν μηχανισμό καταγραφής ενεργειών που λαμβάνουν χώρα στα πλαίσια συνεργασίας διαφόρων οργανισμών, με στόχο την αύξηση της εμπιστοσύνης μεταξύ τους και τη διαφάνεια παρέχοντας πληροφορίες για τις καταγεγραμμένες ενέργειες και πιο συγκεκριμένα για το ποια δεδομένα ζητήθηκαν και παραδόθηκαν σε κάθε αίτημα ενός οργανισμού. Το HLF αξιοποιείται με την εγκαθίδρυση ενός κόμβου (peer) σε κάθε οργανισμό. Εξαιτίας του όγκου των ανταλλασσόμενων δεδομένων, μόνο ένα ίχνος/αποτύπωμα (fingerprint) αποθηκεύεται στον ledger, χρησιμοποιώντας μια hashing συνάρτηση, η οποία λαμβάνει υπόψη της διάφορες πληροφορίες των αιτημάτων ή απαντήσεων ενός οργανισμού. Κάθε οργανισμός είναι υπεύθυνος για να αποθηκεύσει τα πραγματικά δεδομένα που χρησιμοποιούνται σε κάθε αίτημα και απάντηση του, μαζί με τα αντίστοιχα hashes, σε κάποια εξωτερική βάση δεδομένων (Εικόνα 1).



Εικόνα 1: Αρχιτεκτονική και στοιχεία λογισμικού για τον μηχανισμό καταγραφής ενεργειών μεταξύ οργανισμών (L. Van Hove, 2019).

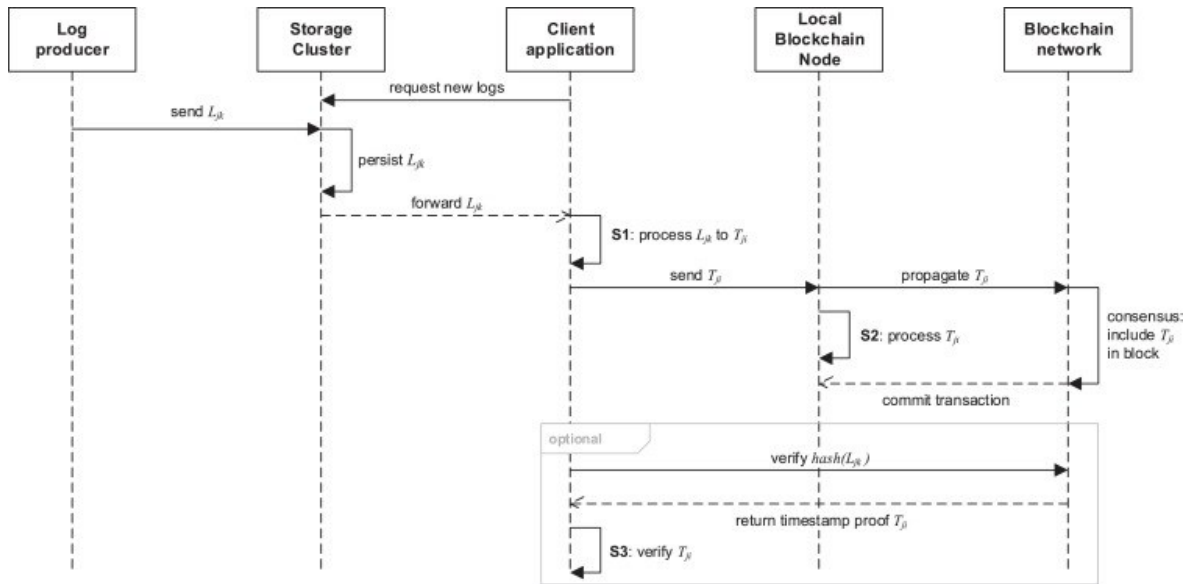
Στη μελέτη των (M. Kumar, 2018) αναπτύσσεται ένας μηχανισμός logging με στόχο την αναγνώριση επιθέσεων που είναι χρονικά διάσπαρτες, προτείνοντας μια αρχιτεκτονική που περιλαμβάνει τοπικούς servers που φιλοξενούν τα logs και συνδυάζει και τη χρήση του blockchain σε περιβάλλον «σύννεφου» (cloud). Οι τοπικοί servers αναλαμβάνουν την συλλογή των καταγραφών (logs) από διάφορες συσκευές και τις αποθηκεύουν προσωρινά. Μετά το πέρας μιας συγκεκριμένης χρονικής περιόδου ή όταν συγκεντρωθεί ένας συγκεκριμένος αριθμός καταγραφών, τότε τις προωθούν για μόνιμη αποθήκευση στο cloud. Εκεί οι καταγραφές αποθηκεύονται στο blockchain, χρησιμοποιώντας τεχνικές κρυπτογράφησης, δημιουργώντας ένα ψηφιακό αποτύπωμα της καταγραφής. Οι ίδιες τεχνικές χρησιμοποιούνται και για την σύνδεση των παραγόμενων blocks του blockchain μεταξύ τους. Ακόμη, προτείνουν τη δημιουργία «σημείων ελέγχου», τα οποία προκύπτουν μετά από συνδυασμό ενός συγκεκριμένου αριθμού καταγραφών, για πιο εύκολο έλεγχο και επαλήθευση των logs.

Οι (Belchior, 2019) προτείνουν ένα σύστημα που ονομάζουν JusticeChain και είναι υπεύθυνο για την καταγραφή και έλεγχο ενεργειών από πληροφοριακά συστήματα στο νομικό σύστημα της Πορτογαλίας. Το σύστημα αυτό είναι βασισμένο σε blockchain, και πιο συγκεκριμένα χρησιμοποιείται το HLF, και επιτρέπει την συμμετοχή ενδιαφερομένων με διαφορετικούς ρόλους και δικαιώματα. Υπάρχουν οντότητες που ονομάζουν «Loggers», οι οποίοι λαμβάνουν καταγραφές από πληροφοριακά συστήματα και στη συνέχεια τα αποθηκεύουν στο blockchain, ενώ οι «Auditors» είναι οντότητες υπεύθυνες για τον έλεγχο των logs στο blockchain. Οι καταγραφές που αποθηκεύονται στο blockchain αποτελούνται από συγκεκριμένα πεδία και μπορούν να είναι διαφόρων ειδών. Όλες οι ενέργειες αποτελούν αιτήματα προς το blockchain για την εκτέλεση συναρτήσεων που περιέχονται σε smart contracts (Εικόνα 2).



Εικόνα 2 : Αρχιτεκτονική του JusticeChain (Belchior, 2019).

Οι (Benedikt Putz, 2019) χρησιμοποιούν ένα permissioned blockchain δίκτυο για να υλοποιήσουν ένα σύστημα ασφαλούς καταγραφής και ελέγχου ενεργειών. Χρησιμοποιούν δύο ειδών καταγραφές. Η πρώτη αποτελεί την πραγματική καταγραφή («evidence data») μαζί με όλες τις διαθέσιμες πληροφορίες και μεταδεδομένα, και είναι αυτή που παράγεται από τις συσκευές στις οποίες λαμβάνει χώρα η προς καταγραφή ενέργεια. Η απόδειξη καταγραφής («integrity proof») είναι η δεύτερη κατηγορία καταγραφής και προκύπτει από την εφαρμογή μιας συνάρτησης hashing πάνω στην πραγματική καταγραφή, και η οποία περιέχει και τη χρονική στιγμή που συνέβη η καταγραφή (timestamp). Σκοπός τους είναι η χρήση και σύνδεση των παραπάνω ώστε να χρησιμοποιηθούν στην περίπτωση που παρουσιαστεί κάποια διαφωνία ή αποποίηση εκτέλεσης ενεργειών. Γι' αυτό το λόγο είναι απαραίτητη η αποθήκευση των παραπάνω με τρόπο που οι καταγραφές δεν μπορούν να τροποποιηθούν με οποιοδήποτε τρόπο, και επομένως αξιοποιούν την τεχνολογία του blockchain. Ωστόσο, αναγνωρίζουν τις περιορισμένες δυνατότητες ενός blockchain δικτύου και προτείνουν την αποθήκευση της πραγματικής καταγραφής σε κάποιο τοπικό σύστημα (cluster), στο οποίο έχουν εφαρμόσει κατάλληλες τεχνικές ασφάλειας πρόσβασης, και την αποθήκευση της απόδειξης της καταγραφής πάνω στο blockchain. Για τον έλεγχο της καταγραφής, ένας χρήστης μπορεί να υποβάλει κάποιο log προς επαλήθευση, στο οποίο εφαρμόζεται η hashing συνάρτηση και κατόπιν γίνεται η αναζήτηση αυτού του αποτελέσματος στον ledger. Αν υπάρχει, το αποτέλεσμα είναι θετικό και σημαίνει ότι δεν έχει υποστεί κάποια επεξεργασία στο αρχικό log. Σε αντίθετη περίπτωση, το αρχικό log έχει υποστεί κάποια (κακόβουλη ενδεχομένως) αλλαγή (Εικόνα 3).

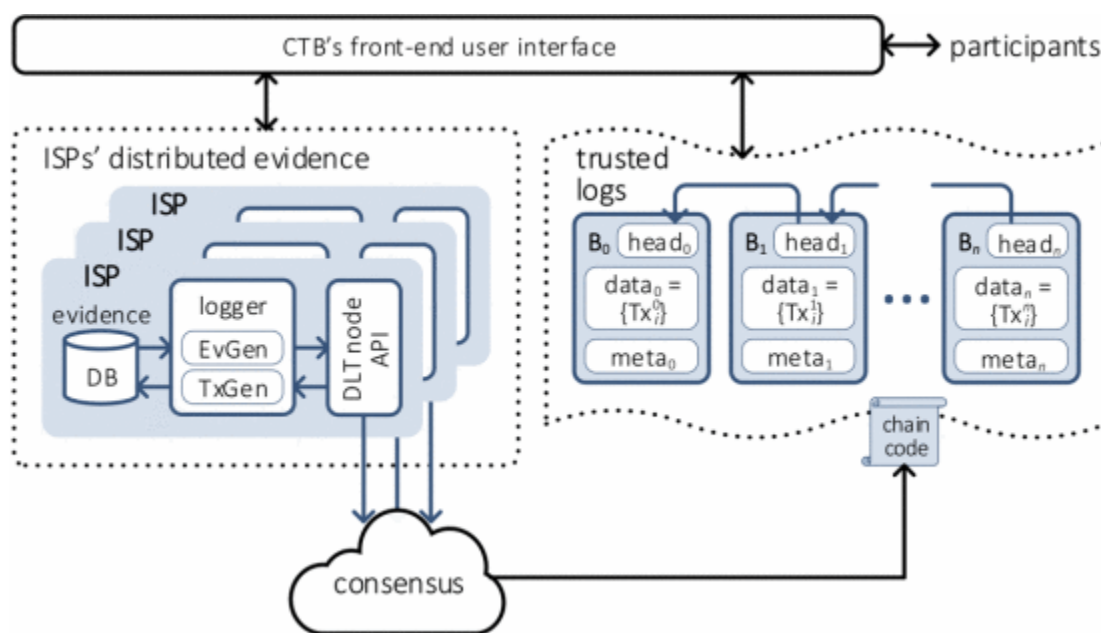


Εικόνα 3 : Διάγραμμα ροής για την καταγραφή ενός log στο προτεινόμενο σύστημα (Benedikt Putz, 2019).

2.2 Καταγραφή και έλεγχος συναλλαγών με χρήση Blockchain για IoT πόρους

Στον τομέα των IoT δεδομένων και συσκευών, το blockchain και τα smart contracts αξιοποιούνται με παρόμοιο τρόπο όπως και στους υπόλοιπους τομείς και εφαρμογές. Μιας και η αμετάβλητη καταγραφή των συναλλαγών σε ένα τέτοιο δίκτυο είναι μια από τις βασικές αρχές και ενσωματωμένες λειτουργίες του, αυτή εμπλουτίζεται ώστε να προσφέρει ασφάλεια και αποδεδειγμένη προέλευση των IoT δεδομένων. Και στις δύο περιπτώσεις εφαρμογών, απαντώνται κοινές τεχνικές και μέθοδοι. Μερικές μελέτες που παρουσιάζουν παρόμοιους μηχανισμούς, παρουσιάζονται παρακάτω.

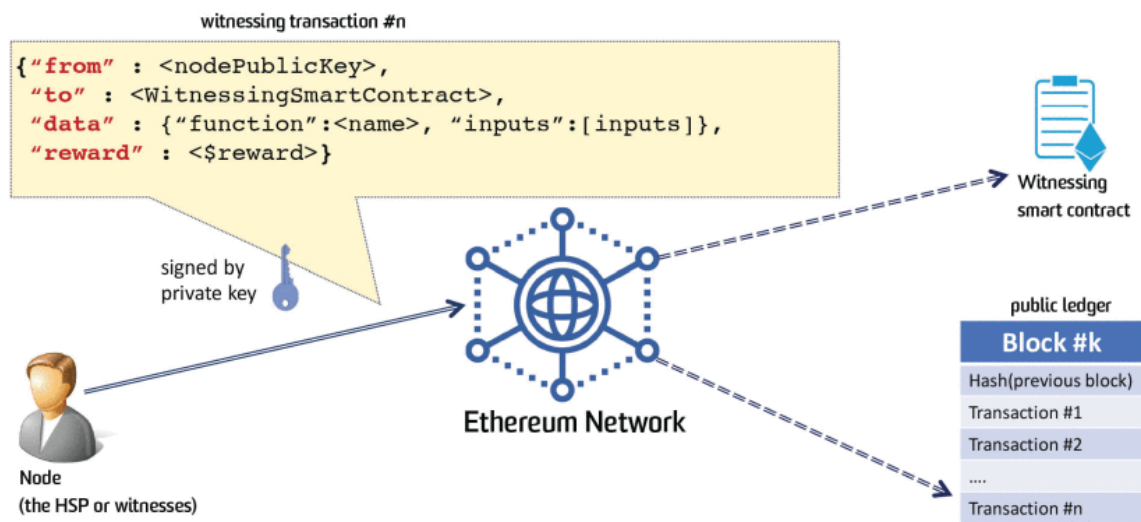
Μια άλλη μελέτη (Brotsis, 2019) χρησιμοποιεί το blockchain σε ένα «έξυπνο» περιβάλλον, και πιο συγκεκριμένα στην περίπτωση ενός «έξυπνου σπιτιού», με σκοπό την συλλογή, την καταγραφή και τη διατήρηση ψηφιακών αποδείξεων (digital forensic evidence) από ένα IoT δίκτυο, σε περιπτώσεις πιθανών επιθέσεων. Ένας «έξυπνος» gateway agent έχει εγκατασταθεί στο περιβάλλον του «έξυπνου σπιτιού» και είναι υπεύθυνος για τον γενικότερο ασφάλεια του IoT δικτύου, μπορεί σε περίπτωση που παρατηρήσει κάποια περίεργη «συμπεριφορά» ή κινητικότητα στο δίκτυο, να συλλέγει τις απαραίτητες πληροφορίες και τις αποθηκεύει σε μια εξωτερική βάση δεδομένων. Αυτή η ενέργεια ενεργοποιεί έναν logger, ο οποίος υποβάλλει μια συναλλαγή στο δίκτυο του blockchain. Κατά τη διάρκεια αυτής της συναλλαγής, υπολογίζεται ένα αναγνωριστικό που προκύπτει από μια hashing συνάρτηση που παίρνει ως είσοδο την απόδειξη που έχει αποθηκευτεί μαζί με μια τυχαία τιμή, ώστε να καταστήσει μοναδικό αυτό το αναγνωριστικό (id). Το παραγόμενο id λειτουργεί ως απόδειξη ακεραιότητας της καταγραφής της απόδειξης (digital forensic evidence) που έχει αποθηκευτεί στην εξωτερική βάση, στην οποία αποθηκεύονται και η τυχαία τιμή αλλά και αυτό το id. Χρησιμοποιώντας τον συνδυασμό του id αλλά και της πραγματικής απόδειξης, είναι η δυνατός έλεγχος εγκυρότητας αυτών των πληροφοριών (Εικόνα 4).



Εικόνα 4 : Αρχιτεκτονική υψηλού επιπέδου του προτεινόμενου συστήματος blockchain (Brotsis, 2019)

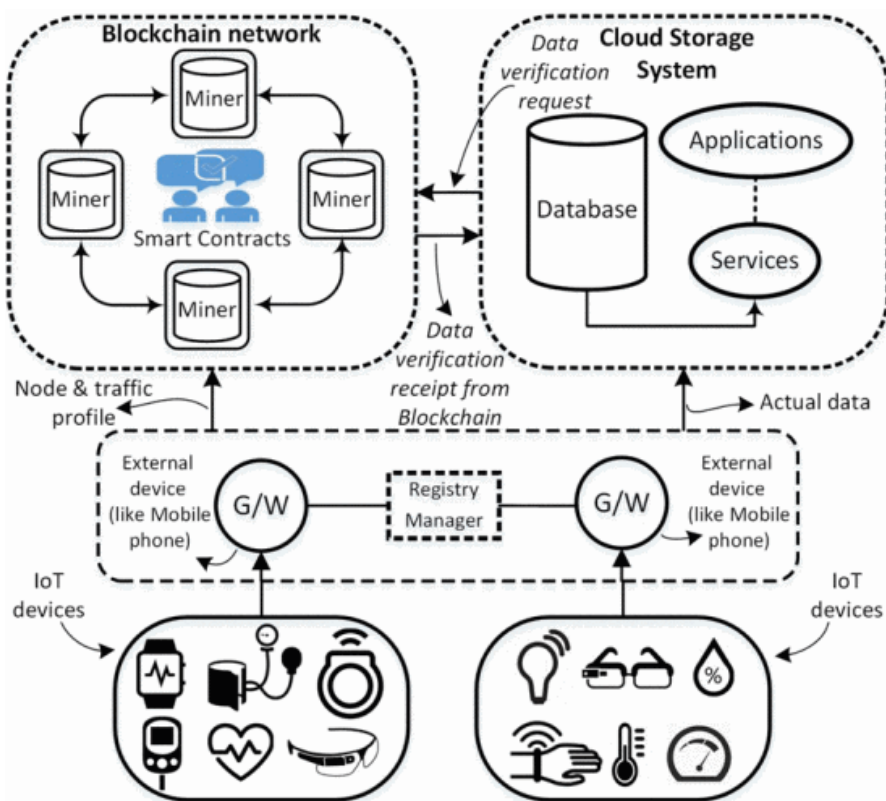
Οι (M. H. Chinaei, 2021) προτείνουν ένα σύστημα «μαρτύρων» (witnessing) για ιατρικά IoT δεδομένα βασισμένο στη χρήση blockchain και smart contracts. Πιο συγκεκριμένα, στοχεύουν στην επαλήθευση δεδομένων που προέρχονται από wearable IoT συσκευές, με στόχο την ανίχνευση πιθανών επιθέσεων (man in the middle attack). Κακόβουλοι χρήστες ή προγράμματα που είναι μέλη του δικτύου μέσω του οποίου μεταφέρονται τα IoT δεδομένα, μπορούν να πραγματοποιήσουν επιθέσεις με στόχο την αλλοίωση τους. Το

προτεινόμενο σύστημα εγκαθιστά αξιόπιστους «μάρτυρες» (witnesses) στο ίδιο δίκτυο, οι οποίοι είναι κόμβοι με πρόσβαση στο Internet και πρόσβαση στο blockchain δίκτυο, μέσω της εκτέλεσης smart contracts καταγράφουν επίσης τις (κρυπτογραφημένες) μετρήσεις των IoT συσκευών, καθώς και άλλες χρήσιμες πληροφορίες, και σχηματίζουν ένα statement, το οποίο αποθηκεύεται στα blocks του blockchain, μαζί με την ίδια την συναλλαγή. Η επιλογή των «μαρτύρων» στο δίκτυο μιας συγκεκριμένης IoT συσκευής γίνεται με τυχαίο τρόπο, και η υλοποίηση του ενώ περιγράφεται στη μελέτη, είναι εκτός ορίων ενδιαφέροντος για αυτό το παραδοτέο. Με την καταγραφή των statements στο blockchain επιτυγχάνεται η διασφάλιση της ακεραιότητας των δεδομένων και ταυτόχρονα μπορούν να ελεγχθούν αν αυτό ζητηθεί. Για τη μελέτη αυτή χρησιμοποιήθηκε ένα δημόσιο blockchain, αυτό του Ethereum (Εικόνα 5).



Εικόνα 5 : Η συναλλαγή που πραγματοποιούν οι "μάρτυρες", μέσω των smart contracts και η αποθήκευσή της στον ledger (M. H. Chinaei, 2021).

Στη μελέτη των (S. Ali, 2018) χρησιμοποιούν το blockchain και τα smart contracts με σκοπό την διασφάλιση της προέλευσης IoT δεδομένων. Πιο συγκεκριμένα, τα IoT δεδομένα μεταφέρονται από τις IoT συσκευές σε κόμβους που δρουν ως gateways, και είναι υπεύθυνοι να συγκεντρώνουν τα δεδομένα, να εφαρμόζουν μια συνάρτηση κρυπτογράφησης (hash) και να προωθούν τα πραγματικά δεδομένα σε ένα περιβάλλον σύννεφου και τα κρυπτογραφημένα δεδομένα στο blockchain. Τα smart contracts χρησιμοποιούνται για να εγγράψουν τα μετά-δεδομένα των συσκευών στον ledger, αλλά και το hash των δεδομένων, που αποστέλλονται με τη μορφή συναλλαγών. Μια ακόμη χρήσιμη λειτουργία των smart contracts είναι η εκτέλεση μιας συνάρτησης, η οποία είναι υπεύθυνη για τον έλεγχο της ταυτότητας της συσκευής, την προέλευση των δεδομένων, αλλά και την κυκλοφορία του δικτύου της IoT συσκευής (Εικόνα 6).



Εικόνα 6 : Αρχιτεκτονική του προτεινόμενου συστήματος (S. Ali, 2018).

3 Καταγραφή και έλεγχος συναλλαγών στο IoTFeds

Στα πλαίσια του έργου IoTFeds, μια από τις πλέον σημαντικές λειτουργίες είναι αυτή της αγοράς προϊόντων, όπως αυτά έχουν σχηματιστεί από τις διάφορες ομοσπονδίες, από άλλους παρόχους ή και καταναλωτές δεδομένων. Η σύνθεση των προϊόντων επιτυγχάνεται μέσω της συνεργασίας του symbIoTe API και του BaaS, και η οποία περιγράφεται αναλυτικά στο παραδοτέο Π2.2 – «Αναφορά Μηχανισμών Διαφήμισης, Ανακάλυψης και Ασφαλούς Πρόσβασης σε Πόρους IoT». Η αγορά των προϊόντων επιτυγχάνεται με τη διάθεσή τους στο Marketplace και την καταβολή ενός αντιτίμου, είτε αυτό είναι εκφρασμένο σε κάποιο ψηφιακό νόμισμα, είτε σε πραγματικά νομίσματα. Στην περίπτωση του IoTFeds, η αγορά των προϊόντων, αλλά και οποιαδήποτε άλλη οικονομική συναλλαγή, πραγματοποιείται με ένα ψηφιακό νόμισμα που δημιουργήθηκε αποκλειστικά για τις ανάγκες του έργου, και ονομάζεται Fedcoin. Περισσότερες πληροφορίες για το Fedcoin, υπάρχουν στο παραδοτέο Π3.2 – «Αναφορά Μηχανισμών Αγοράς IoT». Είναι σημαντικό επομένως κάθε τέτοια αγορά να καταγράφεται και να τη συνοδεύει η αντίστοιχη απόδειξη, αντίτυπο της οποίας έχουν στην κατοχή τους τόσο ο αγοραστής, όσο και ο πωλητής. Αυτή η λειτουργία στο IoTFeds επιτυγχάνεται μέσω του BaaS και της χρήσης του blockchain, όπου κάθε αγορά προϊόντος καταγράφεται στον κατανεμημένο καθολικό (ledger) και εκδίδεται η αντίστοιχη απόδειξη, την οποία μπορούν να χρησιμοποιήσουν οι οντότητες που συμμετείχαν στην αγορά.

Εκτός από την αγορά προϊόντων, εξίσου σημαντική είναι και η χρήση τους. Η χρήση ενός οποιουδήποτε προϊόντος αποτελεί μια ενέργεια που πρέπει να καταγραφεί, καθώς με αυτό τον τρόπο εξασφαλίζεται διαφάνεια κατά την κατανάλωση δεδομένων. Μια εν λόγω καταγραφή μπορεί να χρησιμοποιηθεί μπορεί να χρησιμοποιηθεί από έναν χρήστη που χρησιμοποιεί ένα προϊόν και θέλει να επιβεβαιώσει τον αριθμό των χρήσεων που έχει πραγματοποιήσει. Αυτές οι λειτουργίες επιτυγχάνονται και πάλι από το BaaS, προσφέροντας διαφάνεια και αξιοπιστία στην χρήση των IoT προϊόντων από τους χρήστες της πλατφόρμας.

Αφετηρία αυτών των μηχανισμών είναι πάντα η αγορά ενός προϊόντος, η οποία και καταγράφεται και για τους δύο συμμετέχοντες της αγοράς. Αυτές οι καταγραφές μπορούν να ελεγχθούν ανά πάσα στιγμή και από τους δύο εμπλεκόμενους (αγοραστής και πωλητής). Τόσο ο αγοραστής, όσο και ο πωλητής, μιας διαδικασίας αγοράς, μπορούν να εκτελέσουν τη λειτουργία του ελέγχου εγκυρότητας μιας απόδειξης αγοράς.

Σε συνέχεια της αγοράς ενός προϊόντος, γίνεται καταγραφή χρήσης του, κάθε φορά που αυτό χρησιμοποιείται από τον κάτοχό του. Ο έλεγχος των αποδεικτικών χρήσης, αλλά και ο έλεγχος εγκυρότητας τους, εκτελούνται από τους χρήστες για τα προϊόντα στα οποία έχουν αποκτήσει πρόσβαση.

Στις παρακάτω παραγράφους αναλύονται οι προαναφερθέντες μηχανισμοί.

3.1 Καταγραφή αγορών IoT προϊόντων στο BaaS

Η καταγραφή της πράξης της αγοράς IoT προϊόντων στο BaaS πραγματοποιείται αυτόματα, αφού η εκτέλεση της αγοράς γίνεται με τη χρήση Έξυπνου Συμβολαίου (Smart Contract). Πιο αναλυτικά, η διαδικασία της αγοράς πραγματοποιείται μέσω της γραφικής διεπαφής χρήστη στην πύλη αγοράς (Marketplace) και στη συνέχεια η λειτουργικότητα μεταφέρεται στο υποσύστημα BaaS, όπως περιγράφεται αναλυτικά στο παραδοτέο Π3.2 – «Αναφορά μηχανισμών Αγοράς IoT». Η απόδειξη της αγοράς σχηματίζεται αφού έχουν πραγματοποιηθεί όλοι οι απαραίτητοι έλεγχοι για την ορθή αγορά του προϊόντος, όπως για παράδειγμα ο έλεγχος υπολοίπου των Fedcoins που διαθέτει ο αγοραστής. Η απόδειξη έχει τη μορφή ενός JSON αντικειμένου και τα πεδία που την αποτελούν είναι, το μοναδικό αναγνωριστικό της αγοράς, που συμπίπτει με το αναγνωριστικό της συναλλαγής όπως την αντιλαμβάνεται το Fabric και το οποίο δίνεται αυτόματα από το ίδιο το Fabric, τον αγοραστή, τον πωλητή και το αναγνωριστικό του προϊόντος, αλλά και την ακριβή χρονική στιγμή που πραγματοποιήθηκε η αγορά. Προκειμένου να μειωθεί ο όγκος των δεδομένων που καταγράφονται on-chain, αλλά και για λόγους ασφάλειας και αμεταβλητότητας των δεδομένων που καταγράφονται, στο αντικείμενο της απόδειξης εφαρμόζεται μια hashing συνάρτηση, και πιο συγκεκριμένα η SHA-512. Στη συνέχεια, το αναγνωριστικό της συναλλαγής μαζί με το αντίστοιχο hash αποθηκεύονται on-chain, ενώ η απόδειξη της αγοράς, όπως αυτή σχηματίστηκε στην αρχή, αποθηκεύεται στην MongoDB, μέσα από την απαραίτητη συνάρτηση.

Για την καταγραφή της αγοράς ενός IoT προϊόντος, χρησιμοποιείται το service της αγοράς προϊόντος που γίνεται expose από το BaaS, και το οποίο περιγράφεται στον παρακάτω πίνακα (Πίνακας 1).

Πίνακας 1: Endpoint μέσω του οποίου πραγματοποιείται η καταγραφή της αγοράς.

#	Inter- face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Respons e	Description
1	REST	buyPr oduct	Marketpla ce	BaaS	POST	/baas/products /buy_resources	(String, String, String, String, Integer, Boolean, String, String, String)	(Object, Object)	Request for buying a product

Το service της αγοράς ενός προϊόντος δέχεται ως είσοδο το αναγνωριστικό του προϊόντος, τα usernames του αγοραστή και του πωλητή, την τιμή του προϊόντος, το αναγνωριστικό του marketplace στο οποίο ανήκει το προϊόν, μια παράμετρο που ορίζει αν μιλάμε για προϊόν διακριτών χρήσεων ή ροής δεδομένων, τον αριθμό των ημερών/χρήσεων για τον οποίο ο αγοραστής έχει πρόσβαση στο προϊόν, δύο ημερομηνίες που ορίζουν το χρονικό παράθυρο για το οποίο ο χρήστης μπορεί να πάρει δεδομένα και τέλος τη συχνότητα με την οποία το προϊόν δίνει νέες τιμές (Εικόνα 7). Σε περίπτωση επιτυχημένης αγοράς, επιστρέφεται ένα αντικείμενο σε μορφή JSON, που περιέχει άλλα δύο JSON αντικείμενα. Το πρώτο αποτελεί την απόδειξη της αγοράς και περιέχει τα αναγνωριστικά της αγοράς και του προϊόντος, τον πωλητή και τον αγοραστή, αλλά και την ημερομηνία αγοράς (Εικόνα 8), ενώ το δεύτερο αποτελεί το access token του χρήστη για το συγκεκριμένο προϊόν.

product_id * required	The product's id
(body)	Example Value Model
	string
	Parameter content type
	application/json
buyer * required	The buyer's id
(body)	Example Value Model
	string
	Parameter content type
	application/json
seller * required	The seller's id
(body)	Example Value Model
	string
	Parameter content type
	application/json
price * required	The product's price
(body)	Example Value Model
	string
	Parameter content type
	application/json
access * required	The number of observations or days the buyer will have access to the product
(body)	Example Value Model
	()
	Parameter content type
	application/json
streaming * required	Represents if the access will be streaming (time based) or number of observations (times based). True if the access is streaming, False otherwise.
(body)	Example Value Model
	Unknown Type: bool
	Parameter content type
	application/json
lp * required	The lower threshold for data availability (the lower bound the user is eligible to get data from)
(body)	Example Value Model
	string
	Parameter content type
	application/json
hp * required	The upper threshold for data availability (the upper bound the user is eligible to get data until)
(body)	Example Value Model
	string
	Parameter content type
	application/json
fp	The frequency that the product gives new values/measurements
(body)	Example Value Model
	string

Εικόνα 7: Παράμετροι του endpoint για την αγορά προϊόντος στο BaaS.

Responses Response content type: **message**

Code	Description
200	successful operation
400	Buy product failed

Example Value | Model

```
{
  "Receipt": {
    "TransactionID": "string",
    "ProductID": "string",
    "Seller": "string",
    "Buyer": "string",
    "DateBought": "string"
  },
  "AccessToken": {
    "product 1": {
      "AccessTimes": "2",
      "userHasRated": false,
      "toBeExchanged": false,
      "inUse": false,
      "DataAvailableFrom": "2023-07-01T00:00:00.000Z",
      "DataAvailableUntil": "2023-07-10T00:00:00.000Z",
      "Marketplace": "IoTFeds",
      "ValidUntil": "2023-08-10T00:00:00.000Z",
      "Frequency": ""
    }
  }
}
```

Εικόνα 8: Αντικείμενο που επιστρέφεται και περιλαμβάνει την απόδειξη της αγοράς.

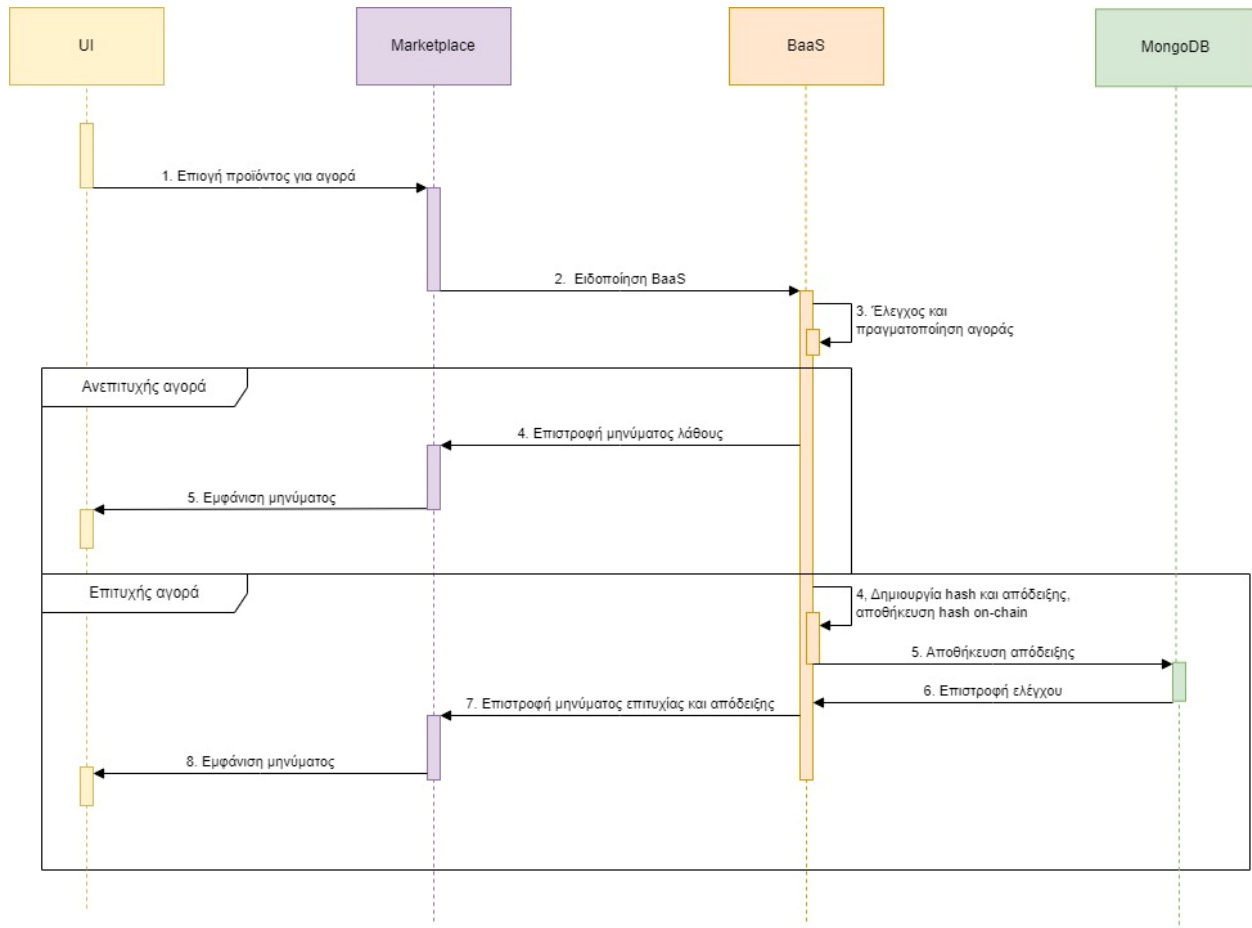
Στην επόμενη εικόνα (Εικόνα 9) φαίνεται το σχήμα της απόδειξης αγοράς, το οποίο ταυτίζεται με το σχήμα του document στην βάση της Mongo. Η απόδειξη περιλαμβάνει το αναγνωριστικό της συναλλαγής, το αναγνωριστικό του προϊόντος, τους συμμετέχοντες της αγοράς, δηλαδή τον αγοραστή και πωλητή, και τέλος την ημερομηνία κατά την οποία πραγματοποιήθηκε η αγορά.

```
Receipt {
  TransactionID string
  ProductID string
  Seller string
  Buyer string
  DateBought string
}
```

Εικόνα 9: Το αντικείμενο της απόδειξης αγοράς.

Στο παρακάτω διάγραμμα ακολουθίας (Εικόνα 10) περιγράφεται η διαδικασία καταγραφής αγοράς ενός προϊόντος. Η διαδικασία ξεκινά με την επιλογή ενός προϊόντος για αγορά από το Marketplace. Στη συνέχεια ειδοποιείται το BaaS, αφού είναι υπεύθυνο για την εκτέλεση (ή μη) της αγοράς. Μέσω της χρήσης των smart contracts πραγματοποιείται μια σειρά ελέγχων, όπως είναι ο έλεγχος του διαθέσιμου υπολοίπου του χρήστη (αγοραστή) σε Fedcoins, που διαθέτει στο wallet του. Αν τα Fedcoins που διαθέτει ο αγοραστής δεν επαρκούν, τότε η αγορά αποτυγχάνει και ένα κατάλληλο μήνυμα επιστρέφεται στον χρήστη. Περισσότερες λεπτομέρειες για τους ελέγχους και πως αυτοί πραγματοποιούνται, καθώς και για την διαδικασία της αγοράς, υπάρχουν στο παραδοτέο της ενότητας 3, Π3.2 – «Αναφορά Μηχανισμών Αγοράς IoT». Στην περίπτωση της επιτυχημένης αγοράς, το τελευταίο βήμα που πραγματοποιείται σύμφωνα με το

σχετικό smart contract, είναι η δημιουργία του αντικειμένου της απόδειξης και ο υπολογισμός και αποθήκευση στον ledger του hash και του αναγνωριστικού της απόδειξης (συναλλαγής). Τέλος από το αντίστοιχο API του BaaS, γίνεται η επικοινωνία με την Mongo, και λαμβάνει χώρα η αποθήκευση της απόδειξης στη βάση. Τέλος το κατάλληλο μήνυμα επιτυχίας αγοράς επιστρέφεται στον χρήστη από το marketplace.



Εικόνα 10: Διάγραμμα ακολουθίας για την καταγραφή αγοράς ενός προϊόντος.

3.2 Έλεγχος αγορών IoT προϊόντων στο BaaS

Όπως συμβαίνει και στις συμβατικές αγορές προϊόντων, αντίτυπο της απόδειξης κρατάει τόσο ο αγοραστής, όσο και ο πωλητής, οι οποίοι μπορούν να ανατρέξουν σε αυτή ανά πάσα στιγμή και να την ελέγξουν. Οι υπηρεσίες αυτές προσφέρονται από το BaaS, ως services που επικοινωνούν με την MongoDB και επιστρέφουν τα επιθυμητά αποτελέσματα. Ένας χρήστης, ως αγοραστής, μπορεί να καλέσει το αντίστοιχο service, για συγκεκριμένη χρονική περίοδο, και να του επιστραφούν οι αγορές που έχει πραγματοποιήσει σε αυτό το διάστημα. Αν δεν ορίσει κάποια χρονική περίοδο, του επιστρέφονται όλες οι αγορές του. Ακόμη του δίνεται η δυνατότητα να ψάξει για την αγορά ενός συγκεκριμένου προϊόντος, αν το επιθυμεί, χρησιμοποιώντας το αναγνωριστικό του προϊόντος. Η ίδια υπηρεσία προσφέρεται και για χρήστες που δρουν ως πωλητές, οπότε και θα του επιστραφούν οι πωλήσεις που έχει πραγματοποιήσει.

Ακόμη, οι χρήστες έχουν τη δυνατότητα να επαληθεύσουν την ορθότητα και την ακεραιότητα μιας απόδειξης αγοράς που έχουν στην διάθεσή τους. Αυτό επιτυγχάνεται μέσα από ένα service που δημιουργεί εκ νέου το αποτύπωμα (hash) της απόδειξης και στη συνέχεια ελέγχει, με βάση το αναγνωριστικό της συναλλαγής, αν το hash αυτό αντιστοιχεί με το hash που είχε αποθηκευτεί on-chain. Αν τα δύο hashes είναι ίδια αυτό συνεπάγεται την ακεραιότητα της απόδειξης, δηλαδή δεν έχει υποστεί κάποιο κακόβουλο επεξεργασία.

Στον Πίνακα 2 φαίνεται η περιγραφή των παραπάνω services.

Πίνακας 2. Endpoints που περιγράφουν τον συναλλαγών ενός χρήστη.

#	Inter- face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Respons e	Description
1	REST	retrieve Receipts Buyer	Marketpla ce	BaaS	POST	/baas/auditing/g et_receipts_buy er	(String, String, String, String)	(Object, Message)	Request for retrieving receipts as a buyer
2	REST	retrieve Receipts Seller	Marketpla ce	BaaS	POST	/baas/auditing/g et_receipts_selle r	(String, String, String, String)	(Object, Message)	Request for retrieving receipts as a seller
3	REST	verifyRe ceipt	Marketpla ce	BaaS	POST	/baas/auditing/v erify_receipt	(Object, String)	(Object, Message)	Request for verifying a receipt

Τα δύο πρώτα services, δέχονται ως είσοδο τις ίδιες παραμέτρους οι οποίες περιλαμβάνουν το όνομα του χρήστη που τα καλεί, το αναγνωριστικό του προϊόντος και το χρονικό διάστημα μέσα στο οποίο επιθυμεί ο χρήστης να ελέγξει τις αποδείξεις του (με τη μορφή ημερομηνιών). Σε περίπτωση επιτυχημένης κλήσης του αντίστοιχου service, επιστρέφεται ένα αντικείμενο JSON που περιέχει έναν πίνακα με τις αποδείξεις. Οι παράμετροι, αλλά και τα αποτελέσματα που επιστρέφονται, φαίνονται στις παρακάτω εικόνες (Εικόνα 11, Εικόνα 12, Εικόνα 13, Εικόνα 14).

POST /retrieveReceiptsBuyer Retrieves the transactions' receipts where user is the buyer

Retrieves the transactions' receipts where user is the buyer

Parameters Try it out

Name	Description
user * required (body)	The buyer calling this function Example Value Model string Parameter content type application/json
product_id (body)	The product to see the receipts for Example Value Model string Parameter content type application/json
fromDate (body)	The date from which onward buyer wants to see the receipts Example Value Model string Parameter content type application/json
toDate (body)	The date up to which buyer wants to see the receipts Example Value Model string Parameter content type application/json

Εικόνα 11: Παράμετροι για το endpoint του ελέγχου των αγορών ενός χρήστη.

Responses		Response content type
		application/json
Code	Description	
200	Object with array of receipts	
	Example Value Model	
	<pre>{ "Receipts": [{ "TransactionID": "8ce5ece422cf83aadfcf4fdb505d62376ce0bfb18d66db899e4df872e51ab33c", "Buyer": "evathana", "Seller": "spolymeni", "ProductID": "product3", "DateBought": "2023-05-17T13:09:01.000Z" }, { "TransactionID": "eabb26b7d54ff3aa953aa4e4dbe35a794867f2bd259807e1260812acd6648c25", "Buyer": "gspanos", "Seller": "spolymeni", "ProductID": "product3", "DateBought": "2023-05-17T13:37:49.000Z" }] }</pre>	
400	Retrieve receipts operation failed ...Malformed request	
500	Retrieve receipts operation failed ...	

Εικόνα 12: Αντικείμενο που επιστρέφεται και περιλαμβάνει όλες τις αποδείξεις αγορών ενός χρήστη.

POST `/retrieveReceiptsSeller` Retrieves the transactions' receipts where user is the seller

Retrieves the transactions' receipts where user is the seller

Parameters Try it out

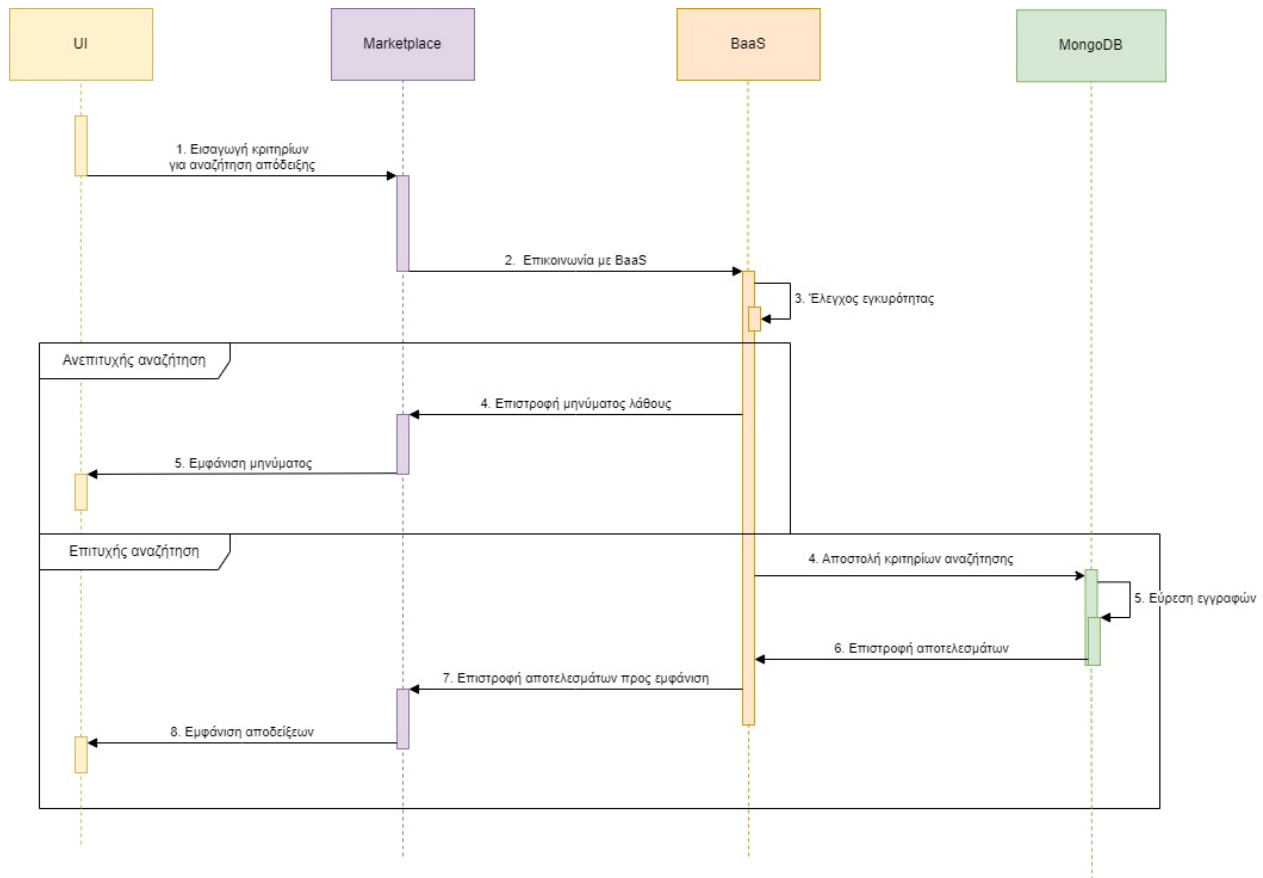
Name	Description
user * required (body)	The seller calling this function Example Value Model string Parameter content type application/json
product_id (body)	The product to see the receipts for Example Value Model string Parameter content type application/json
fromDate (body)	The date from which onward seller wants to see the receipts Example Value Model string Parameter content type application/json
toDate (body)	The date up to which seller wants to see the receipts Example Value Model string Parameter content type application/json

Εικόνα 13: Παράμετροι για το endpoint του ελέγχου των πωλήσεων ενός χρήστη.

Responses		Response content type
		application/json
Code	Description	
200	Object with array of receipts	
	Example Value Model	
	<pre>{ "Receipts": [{ "TransactionID": "8ce5ece422cf83aadfcf4fdb505d62376ce0bfb18d66db899e4df872e51ab33c", "Buyer": "evathana", "Seller": "spolymeni", "ProductID": "product3", "DateBought": "2023-05-17T13:09:01.000Z" }, { "TransactionID": "eabb26b7d54ff3aa953aa4e4dbe35a794867f2bd259807e1260812acd6648c25", "Buyer": "gspanos", "Seller": "spolymeni", "ProductID": "product3", "DateBought": "2023-05-17T13:37:49.000Z" }] }</pre>	
400	Retrieve receipts operation failed ...Malformed request	
500	Retrieve receipts operation failed ...	

Εικόνα 14: Αντικείμενο που επιστρέφεται και περιλαμβάνει τις πωλήσεις ενός χρήστη.

Στο διάγραμμα ακολουθίας παρακάτω (Εικόνα 15), φαίνεται η διαδικασία που ακολουθείται για τον έλεγχο των συναλλαγών ενός χρήστη. Η διαδικασία ξεκινά από το γραφικό περιβάλλον του Marketplace, όπου ο χρήστης εισάγει τα κριτήρια αναζήτησης. Αυτά περιλαμβάνουν τις ημερομηνίες ανάμεσα στις οποίες ο χρήστης επιθυμεί να ελέγξει τις συναλλαγές του, όπως επίσης και το αναγνωριστικό του προϊόντος. Στη συνέχεια, τα κριτήρια αυτά ελέγχονται για την ορθότητά τους από το BaaS, και στην περίπτωση που είναι έγκυρα, πραγματοποιείται η αναζήτηση στην βάση δεδομένων. Σε περίπτωση επιτυχούς αναζήτησης, επιστρέφονται στο χρήστη τα αποτελέσματα.



Εικόνα 15: Διάγραμμα ακολουθίας για τον έλεγχο των συναλλαγών ενός χρήστη.

Το endpoint που είναι υπεύθυνο για τον έλεγχο ακεραιότητας μιας απόδειξης δέχεται ως είσοδο δύο παραμέτρους. Η πρώτη αποτελεί το αντικείμενο της απόδειξης και η δεύτερη είναι το όνομα του χρήστη που εκτελεί αυτό το service. Το αντικείμενο που επιστρέφεται περιλαμβάνει μια λογική μεταβλητή (true ή false). Στην περίπτωση που έχει «αληθή» τιμή, υποδηλώνεται ότι αυτή η απόδειξη δεν έχει παραποιηθεί με οποιονδήποτε τρόπο, ενώ στην περίπτωση «ψευδούς» τιμής, υποδηλώνεται ότι κάποια κακόβουλη οντότητα έχει καταφέρει να παραποιήσει τα αποτελέσματα. Στις παρακάτω εικόνες (Εικόνα 16, Εικόνα 17) φαίνονται οι παράμετροι και το επιστρεφόμενο αντικείμενο.

POST **/verifyReceipt** Used for verifying the integrity of a receipt

Used for verifying the integrity of a receipt

Parameters Try it out

Name	Description
receipt * required object (body)	The object of the receipt to be verified Example Value Model <pre>{ "TransactionID": "string", "ProductID": "string", "Seller": "string", "Buyer": "string", "DateBought": "string"}</pre> Parameter content type application/json
user_id * required (body)	The user that calls this action Example Value Model <pre>string</pre> Parameter content type application/json

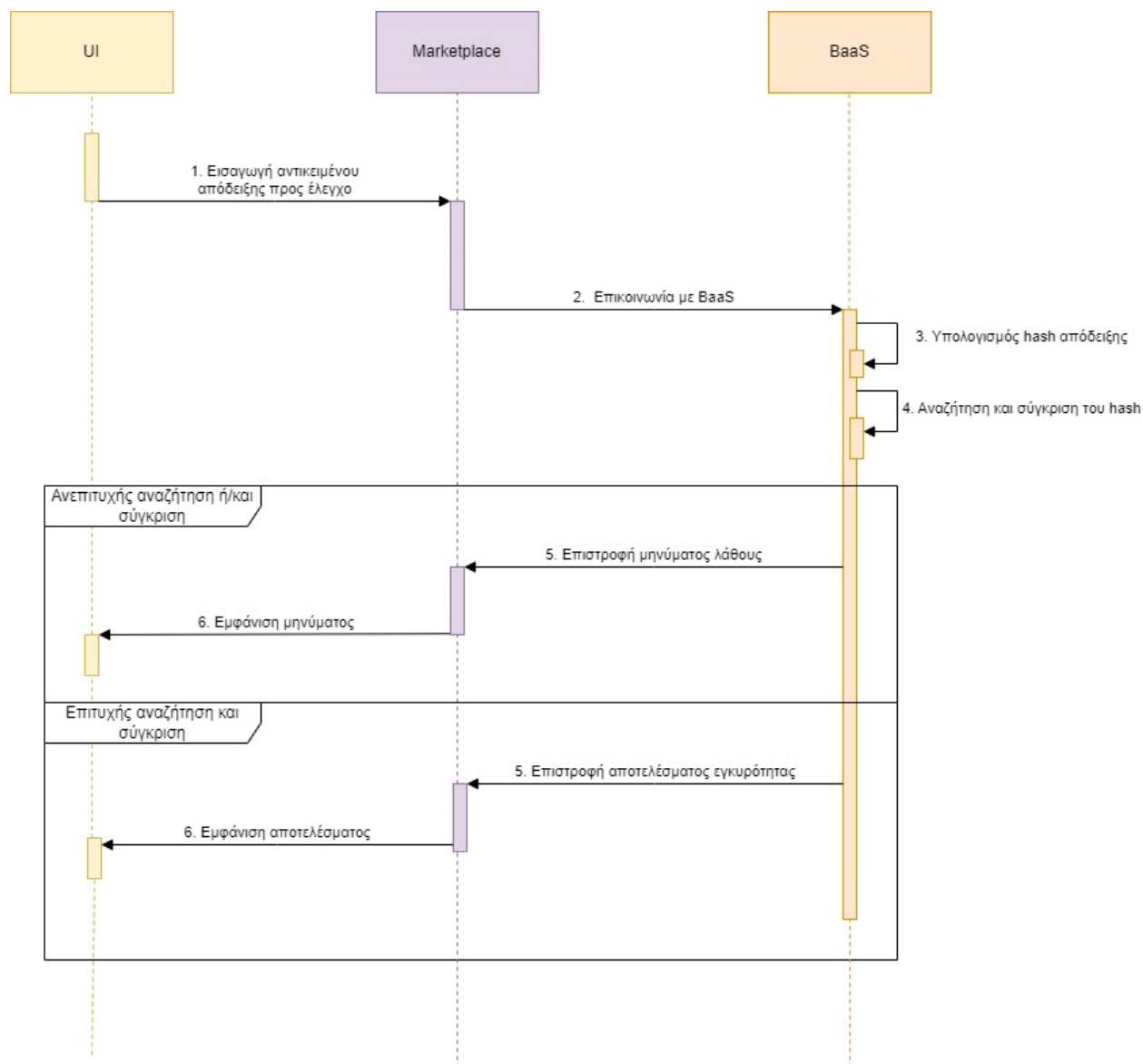
Εικόνα 16: Παράμετροι για το endpoint του ελέγχου ακεραιότητας μιας απόδειξης αγοράς.

Responses Response content type application/json

Code	Description
200	Object with a boolean value stating if the verification was successful Example Value Model <pre>{ "Verified": true}</pre>
400	Verify receipt operation failed ...Malformed receipt...
500	Verify receipt operation failed ...

Εικόνα 17: Αντικείμενο που επιστρέφεται από τον έλεγχο ακεραιότητας.

Στο διάγραμμα που ακολουθεί (Εικόνα 18), περιγράφεται η ροή της διαδικασίας του ελέγχου εγκυρότητας μιας απόδειξης συναλλαγής. Και αυτή η λειτουργία ξεκινά από το γραφικό περιβάλλον του Marketplace. Ο χρήστης εισάγει την απόδειξη, της οποίας την εγκυρότητα επιθυμεί να ελέγξει. Το Marketplace επικοινωνεί με το BaaS, το οποίο υπολογίζει την hash τιμή της απόδειξης. Έπειτα πραγματοποιείται αναζήτηση στον ledger με βάση το αναγνωριστικό της απόδειξης. Στην περίπτωση επιτυχημένης αναζήτησης, η αποθηκευμένη τιμή hash ανασύρεται από τον ledger και συγκρίνεται με αυτή που υπολογίστηκε λίγο πριν. Αν οι δύο τιμές είναι ίδιες, τότε επιστρέφεται μήνυμα επιτυχίας στον χρήστη. Στις περιπτώσεις ανεπιτυχούς αναζήτησης, αλλά και ανεπιτυχούς σύγκρισης, επιστρέφεται στο χρήστη κατάλληλο μήνυμα λάθους.



Εικόνα 18: Διάγραμμα ακολουθίας για τον έλεγχο εγκυρότητας μιας απόδειξης συναλλαγής.

3.3 Καταγραφή χρήσης IoT προϊόντων στο BaaS

Για την καταγραφή της χρήσης ενός IoT προϊόντος αξιοποιείται η λειτουργία του BaaS για τον έλεγχο πρόσβασης σε αυτό. Η αναλυτική περιγραφή του ελέγχου πρόσβασης σε ένα προϊόν υπάρχει σε παραδοτέο της ΕΕ2, και πιο συγκεκριμένα στο Π2.2 – «Αναφορά Μηχανισμών Διαφήμισης, Ανακάλυψης και Ασφαλούς Πρόσβασης σε Πόρους IoT». Αφού ελεγχθεί ότι ο χρήστης έχει ακόμη πρόσβαση σε ένα συγκεκριμένο προϊόν, και επομένως του δίνεται το δικαίωμα να το χρησιμοποιήσει, με τη χρήση Έξυπνων Συμβολαίων, δημιουργείται η απόδειξη χρήσης. Σε αυτή περιέχονται το αναγνωριστικό της συγκεκριμένης συναλλαγής όπως αυτή αναγνωρίζεται από το Fabric, το όνομα του χρήστη, το αναγνωριστικό του προϊόντος που χρησιμοποιεί αλλά και την ημερομηνία και ώρα της χρήσης. Όλα αυτά τα στοιχεία είναι μέρος ενός JSON αντικειμένου, που για λόγους ασφάλειας και εξοικονόμησης χώρου (όπως αναφέρθηκε και στην παράγραφο 3.1 Καταγραφή αγορών IoT προϊόντων), εφαρμόζεται πάνω του μια hashing συνάρτηση (SHA-512) και στη συνέχεια χρησιμοποιώντας το αναγνωριστικό της συναλλαγής και το hash που έχει προκύψει, η απόδειξη χρήσης αποθηκεύεται στον ledger. Στη συνέχεια, μόλις ο έλεγχος επιστρέψει από το blockchain και την εκτέλεση του Συμβολαίου πίσω στο service που είναι υπεύθυνο για τον έλεγχο πρόσβασης, καλείται το service που αποθηκεύει την απόδειξη στην εξωτερική βάση.

Το endpoint για τον έλεγχο πρόσβασης έχει ήδη περιγραφεί στο παραδοτέο Π2.2, ωστόσο συμπεριλαμβάνεται και εδώ για λόγους πληρότητας (Πίνακας 3). Λεπτομέρειες για την ροή επικοινωνίας και την υλοποίηση για την προσπέλαση προϊόντος σε ομοσπονδιακή ή καθολική αγορά που πραγματοποιείται από το marketplace API και το οποίο ενσωματώνει την χρήση της διεπαφής αυτής για τον έλεγχο πρόσβασης περιγράφονται στο Π2.2.

Πίνακας 3: Endpoint που περιγράφει τον έλεγχο πρόσβασης.

#	Inter- face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	checkAccess	Marketplace	BaaS	POST	/baas/products/ check_access	(String, String, String, String, String)	(Object, Message)	Request for checking the access to a product

Στις επόμενες εικόνες (Εικόνα 19, Εικόνα 20) φαίνονται οι παράμετροι που δέχεται ως είσοδο το service για τον έλεγχο ασφαλούς πρόσβασης αλλά και το αντικείμενο που επιστρέφεται. Οι παράμετροι εισόδου περιλαμβάνουν το αναγνωριστικό του προϊόντος και του χρήστη, τις δυο ημερομηνίες που ορίζουν το χρονικό παράθυρο μέσα στο οποίο ο χρήστης έχει πρόσβαση στο προϊόν καθώς και τον ζητούμενο αριθμό χρήσεων (observations) στην περίπτωση που πρόκειται για προϊόν διακριτών χρήσεων. Το αντικείμενο που επιστρέφεται αποτελεί το access token με όλες του τις πληροφορίες.

POST /checkAccess When accessing a product, the user's access tokens are checked and either grants him access to the product or not

When accessing a product, the user's access tokens are checked and either grants him access to the product or not

Parameters Try it out

Name	Description
product_id * required (body)	The product's id Example Value Model string Parameter content type application/json
user_id * required (body)	The user's id Example Value Model string Parameter content type application/json
data_from * required (body)	the lower bound (timestampA) that the user wants to get data from Example Value Model string Parameter content type application/json
data_until * required (body)	the upper bound (timestampB) that the user wants to get data until Example Value Model string Parameter content type application/json
req_observations * required (body)	The number of requested observations Example Value Model string Parameter content type application/json

Εικόνα 19: Παράμετροι για το endpoint της ασφαλούς πρόσβασης σε ένα προϊόν.

Responses		Response content type
		message
Code	Description	
200	The access token for that particular product	
	Example Value Model	
	<pre>{ "product 1": { "AccessTimes": "2", "userHasRated": false, "toBeExchanged": false, "inUse": false, "DataAvailableFrom": "2023-07-01T00:00:00.000Z", "DataAvailableUntil": "2023-07-10T00:00:00.000Z", "Marketplace": "IoTFeds", "ValidUntil": "2023-08-10T00:00:00.000Z", "Frequency": "" } }</pre>	
403	Product access failed ...You can't have access to product you haven't bought/You no longer have access to this product./Requested data are out of the data bounds you have bought the product for...	

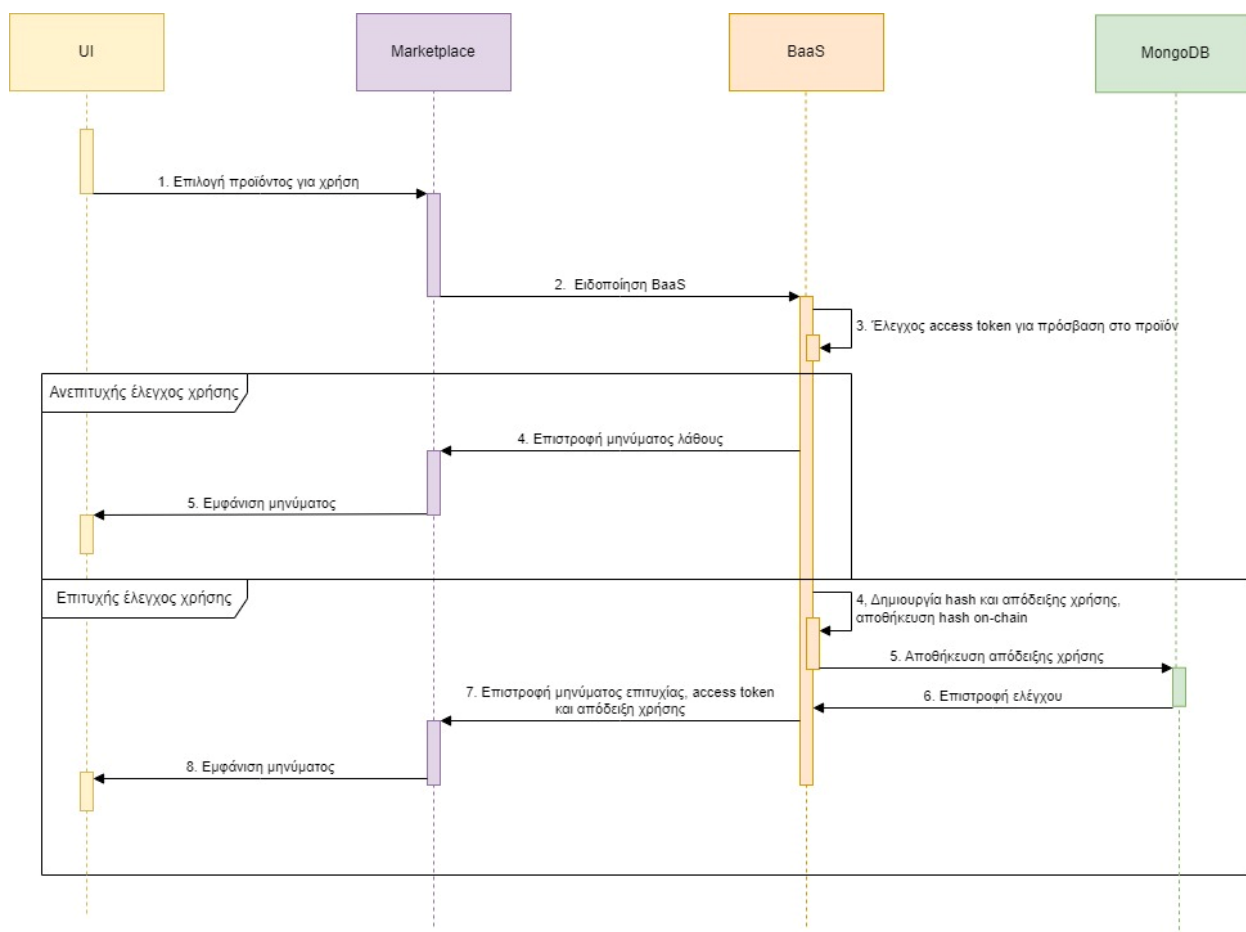
Εικόνα 20: Αντικείμενο που επιστρέφεται και περιλαμβάνει τις πηγές δεδομένων και τις εναπομένουσες φορές πρόσβασης.

Η απόδειξη χρήσης όπως αυτή δημιουργείται πριν περάσει από την διαδικασία της απόκρυψης (hashing) και όπως αυτή αποθηκεύεται στην MongoDB, φαίνεται στην Εικόνα 21. Η απόδειξη χρήσης περιλαμβάνει το αναγνωριστικό της συναλλαγής, το αναγνωριστικό προϊόντος, τον χρήστη που έκανε χρήση του προϊόντος, αλλά και την ημερομηνία πρόσβασης.

```
Log {
  TransactionID string
  ProductID string
  User string
  DateAccessed string
}
```

Εικόνα 21: Το αντικείμενο της απόδειξης χρήσης ενός προϊόντος.

Στο παρακάτω διάγραμμα ακολουθίας (Εικόνα 22) αποτυπώνεται η διαδικασία του ελέγχου για ασφαλή πρόσβαση προϊόντος, μέσω της οποίας πραγματοποιείται και η καταγραφή της απόδειξης χρήσης. Ο χρήστης επιλέγει το προϊόν που θέλει να χρησιμοποιήσει. Αφού πραγματοποιηθεί ο έλεγχος πρόσβασης με βάση το access token του χρήστη, και σε περίπτωση επιτυχούς ελέγχου, δημιουργείται από το BaaS η απόδειξη χρήσης και υπολογίζεται το hash αυτής της απόδειξης. Το αναγνωριστικό της απόδειξης και η hash τιμή αποθηκεύονται στον ledger, ενώ τόσο η hash τιμή όσο και η πραγματική απόδειξη χρήσης αποθηκεύονται στην εξωτερική βάση δεδομένων (MongoDB). Ένα μήνυμα επιτυχούς ελέγχου χρήσης επιστρέφεται στον χρήστη και του επιτρέπεται η πρόσβαση στο προϊόν. Σε περίπτωση ανεπιτυχούς ελέγχου, επιστρέφεται στο χρήστη μήνυμα λάθους.



Εικόνα 22: Διάγραμμα ακολουθίας για την καταγραφή απόδειξης χρήσης προϊόντος.

3.4 Έλεγχος χρήσης IoT προϊόντων στο BaaS

Σε ένα έργο όπως το IoTFeds, όπου ένα από τα κύρια χαρακτηριστικά του είναι η χρήση IoT προϊόντων, είναι σημαντικό αυτή να καταγράφεται αλλά και να ελέγχεται, με στόχο την εξασφάλιση της εγκυρότητας και αξιοπιστίας. Όπως και η καταγραφή της χρήσης των IoT προϊόντων, και ο έλεγχός τους προσφέρεται από το BaaS. Κάθε χρήστης μπορεί να εκτελέσει την λειτουργία του ελέγχου χρήσης προϊόντων για τα προϊόντα που έχει πρόσβαση, ώστε να ελέγξει πότε τα χρησιμοποίησε και να την ακεραιότητα της πράξης του,

Ο έλεγχος ακεραιότητας μιας απόδειξης χρήσης ενός IoT προϊόντος, με στόχο την διασφάλιση της αξιοπιστίας και της εγκυρότητας του αποδεικτικού, εκτελείται από τον χρήστη μέσω του λογισμικού του BaaS. Αφού υπολογιστεί το hash της απόδειξης που επιθυμεί ο χρήστης να ελέγξει (με τον ίδιο τρόπο που υπολογίστηκε μέσα από το Smart Contract όταν και αποθηκεύτηκε on-chain), χρησιμοποιείται το αναγνωριστικό της απόδειξης ώστε να εντοπιστεί η αντίστοιχη συναλλαγή στον ledger. Αν εντοπιστεί, τότε ελέγχεται η τιμή hash που ήταν ήδη αποθηκευμένη με αυτή που μόλις δημιουργήθηκε. Αν οι τιμές ταυτίζονται, τότε αυτό σημαίνει ότι η απόδειξη χρήσης δεν έχει υποστεί καμία αλλαγή. Αν η συναλλαγή δεν εντοπιστεί ή αν δεν ταυτίζονται οι τιμές, τότε αυτό συνεπάγεται ότι η απόδειξη δεν είναι έγκυρη.

Πίνακας 4. Endpoint που περιγράφει τον έλεγχο χρήσης των IoT προϊόντων από το χρήστη.

#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	retrieve AccessLogs	marketplace	BaaS	POST	/baas/auditing/get_logs	(String, String, String, String)	(Object, Message)	Request for checking the logs for access/usage to an IoT product
2	REST	verifyAccessLog	marketplace	BaaS	POST	/baas/auditing/verify_access_logs	(Object, String)	(Object, Message)	Request for verifying the access to an IoT product

Το service της αναζήτησης των αποδεικτικών χρήσης δέχεται ως είσοδο τέσσερις παραμέτρους, το όνομα του χρήστη, ο οποίος επιθυμεί να ελέγξει τις χρήσεις προϊόντων του, το αναγνωριστικό του προϊόντος που χρησιμοποιήθηκε και τέλος δύο ημερομηνίες, ανάμεσα στις οποίες θα γίνει η αναζήτηση των καταγραφών. Αν ο χρήστης δεν καθορίσει το προϊόν, τότε θα επιστραφούν οι καταγραφές που αφορούν όλα τα προϊόντα του. Αντίστοιχα παρόμοιο αποτέλεσμα θα προκύψει και αν ο χρήστης δεν ορίσει κάποια από τις δύο ημερομηνίες. Το αντικείμενο που επιστρέφεται είναι ένα αντικείμενο τύπου JSON, που περιλαμβάνει έναν πίνακα με όλες τις καταγραφές που ικανοποιούν τα κριτήρια αναζήτησης που έθεσε ο χρήστης. Στην Εικόνα 23 φαίνονται οι παράμετροι εισόδου, ενώ στην Εικόνα 24 φαίνεται το αντικείμενο που επιστρέφεται.

POST

/retrieveAccessLogs

The admin can retrieve the logs based on the usage/access of the products

^

The admin can retrieve the logs based on the usage/access of the products

Parameters

Try it out

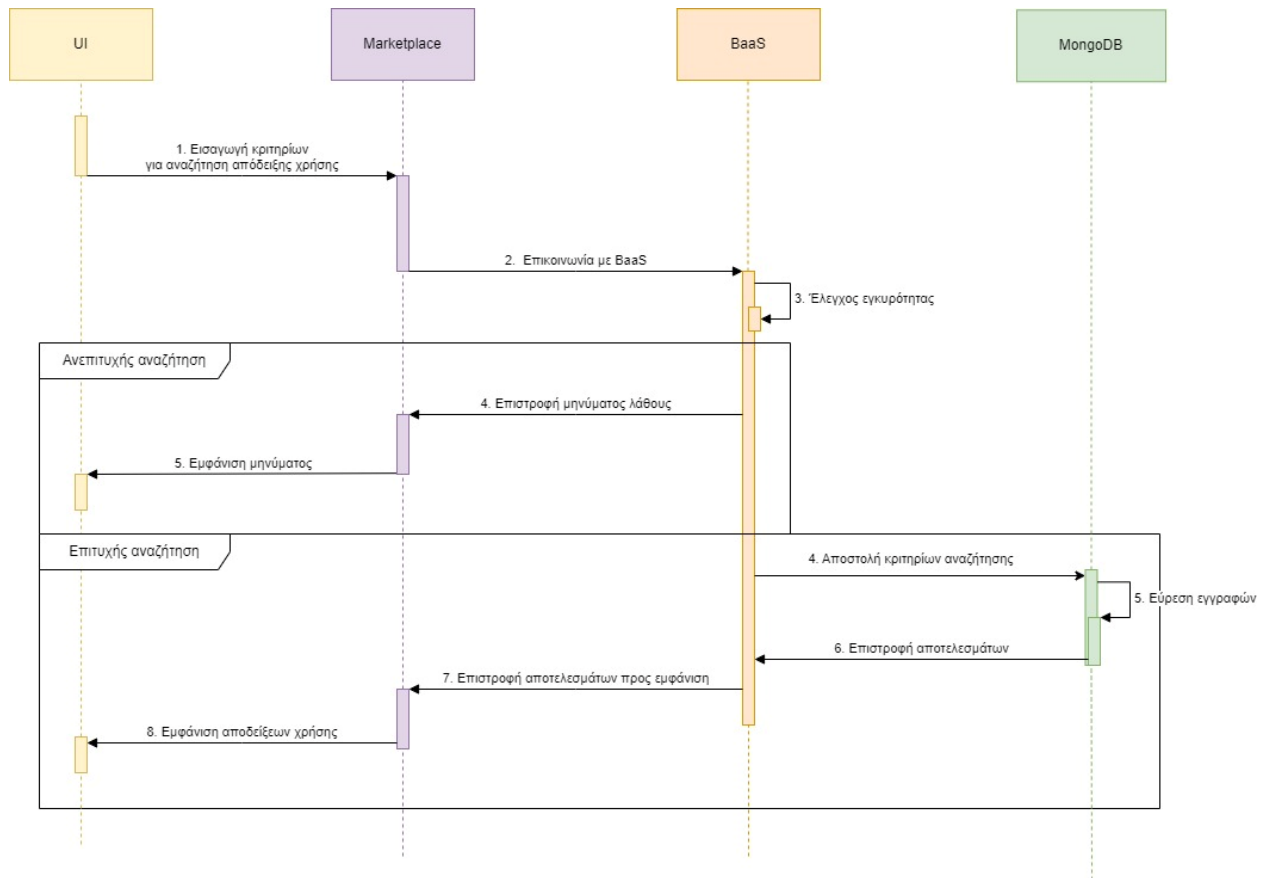
Name	Description
user (body)	The user for whom this function is called Example Value Model string Parameter content type application/json
product_id (body)	The product to see the receipts for Example Value Model string Parameter content type application/json
fromDate (body)	The date from which onward admin wants to see the receipts Example Value Model string Parameter content type application/json
toDate (body)	The date up to which admin wants to see the receipts Example Value Model string Parameter content type application/json

Εικόνα 23: Παράμετροι για το endpoint του ελέγχου της χρήσης IoT προϊόντων.

Responses		Response content type application/json
Code	Description	
200	Object with array of logs	
	Example Value Model	
	<pre>{ "Logs": [{ "TransactionID": "62d5586b78df064bcd2b9332230b07a80d8cf48c23dc60d02dfa9033a25645c", "User": "evathana", "ProductID": "product3", "DateAccessed": "2023-05-23T10:41:53.973Z" }, { "TransactionID": "8b9ee0283155a542c498a5b4bcfdc40114228aaf431825d3bdf434cfe29108a8", "User": "evathana", "ProductID": "product2", "DateAccessed": "2023-05-23T10:42:15.765Z" }] }</pre>	
400	Retrieve logs operation failed ...Malformed request	
500	Retrieve logs operation failed ...	

Εικόνα 24: Αντικείμενο που επιστρέφεται με τις καταγραφές χρήσης των IoT προϊόντων.

Το παρακάτω διάγραμμα ακολουθίας (Εικόνα 25) παρουσιάζει τον έλεγχο των αποδείξεων χρήσης ενός προϊόντος από έναν χρήστη. Μέσα από το Marketplace, ο χρήστης εισάγει τα κριτήρια αναζήτησης (αναγνωριστικό προϊόντος, ημερομηνίες, όνομα χρήστη) για τις αποδείξεις χρήσεων που επιθυμεί. Η εγκυρότητα των κριτηρίων ελέγχεται από το BaaS και στην περίπτωση που είναι έγκυρα πραγματοποιείται η αναζήτηση στην εξωτερική βάση δεδομένων και επιστρέφονται τα αποτελέσματα που ικανοποιούν αυτά τα κριτήρια. Σε περίπτωση λάθους, επιστρέφεται το αντίστοιχο μήνυμα στον χρήστη.



Εικόνα 25: Διάγραμμα ακολουθίας του ελέγχου απόδειξης χρήσης

Το endpoint που υλοποιεί τον έλεγχο εγκυρότητας δέχεται ως είσοδο ένα αντικείμενο τύπου JSON, και πιο συγκεκριμένα ένα αντικείμενο Log (Εικόνα 21), που αντιπροσωπεύει την απόδειξη χρήσης που θα υποβληθεί σε έλεγχο. Επιπλέον, δέχεται και μια δεύτερη παράμετρο εισόδου, το όνομα του χρήστη που εκτελεί τον έλεγχο.. Σε περίπτωση επιτυχημένης κλήσης και εκτέλεσης του service, επιστρέφεται ένα αντικείμενο που περιλαμβάνει μια δυαδική τιμή (true, false) που υποδηλώνει αν η απόδειξη χρήσης είναι έγκυρη ή όχι. Στην Εικόνα 26 φαίνονται οι παράμετροι εισόδου, ενώ στην Εικόνα 27 φαίνεται το επιστρεφόμενο αντικείμενο.

POST **/verifyAccessLog** Used for verifying the integrity of a receipt

Used for verifying the integrity of a receipt

Parameters Try it out

Name	Description
receipt * required object (body)	The object of the receipt to be verified Example Value Model <pre>{ "TransactionID": "string", "ProductID": "string", "User": "string", "DateAccessed": "string" }</pre> Parameter content type application/json
user_id * required (body)	The user that calls this action Example Value Model <pre>string</pre> Parameter content type application/json

Εικόνα 26: Παράμετροι εισόδου για το endpoint του ελέγχου ακεραιότητας μιας απόδειξης χρήσεως ενός IoT προϊόντος.

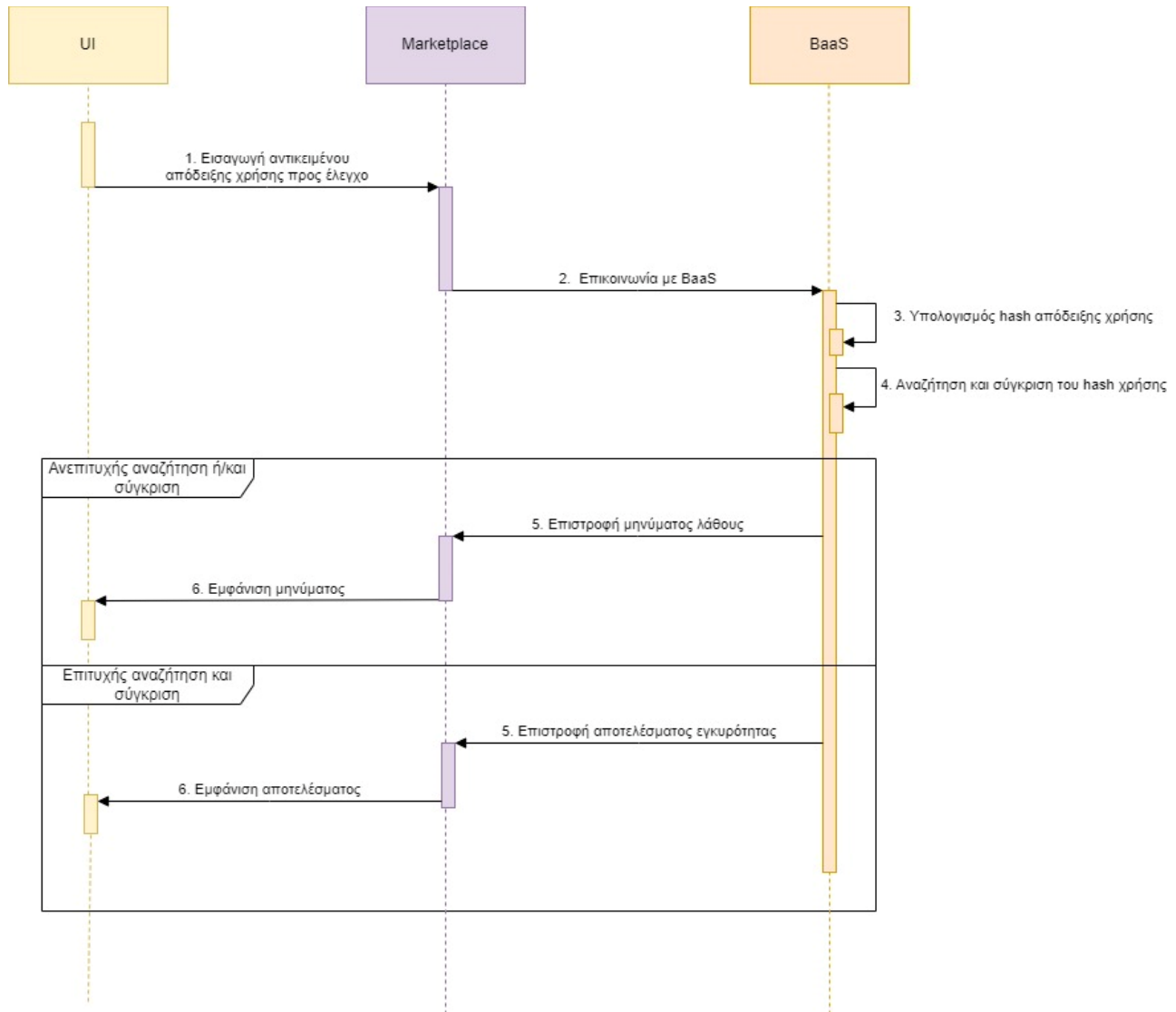
Responses Response content type application/json

Code	Description
200	Object with a boolean value stating if the verification was successful Example Value Model <pre>{ "Verified": true }</pre>
400	Verify access log operation failed ...Malformed access log...
500	Verify access log operation failed ...

Εικόνα 27: Το αντικείμενο που επιστρέφεται από τον έλεγχο ακεραιότητας μιας απόδειξης χρήσεως ενός IoT προϊόντος.

Τέλος, στο παρακάτω διάγραμμα ακολουθίας (Εικόνα 28) απεικονίζεται ο έλεγχος εγκυρότητας μιας απόδειξης χρήσης για ένα προϊόν. Ο χρήστης μέσα από το Marketplace, εισάγει την απόδειξη χρήσης που επιθυμεί να ελέγξει. Η τιμή hash της εισαχθείσας απόδειξης υπολογίζεται από το BaaS και στη συνέχεια

γίνεται αναζήτηση στον ledger με βάση το αναγνωριστικό της απόδειξης. Αν αυτό εντοπιστεί, τότε ανασύρεται και η αποθηκευμένη τιμή hash. Οι δύο τιμές hash συγκρίνονται και σε περίπτωση που αυτές είναι ίδιες, ένα μήνυμα επιτυχίας επιστρέφεται στο χρήστη. Διαφορετικά, ένα κατάλληλο μήνυμα αποτυχίας επιστρέφεται στο χρήστη.



Εικόνα 28: Διάγραμμα ακολουθίας για τον έλεγχο εγκυρότητας απόδειξης χρήσης.

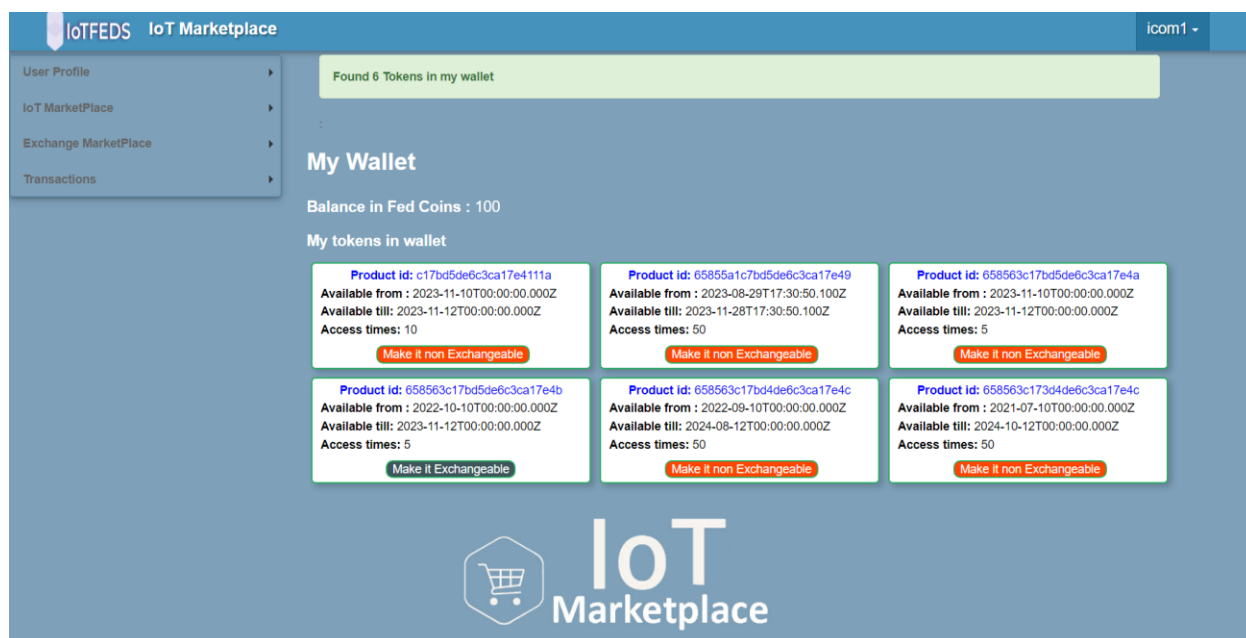
3.5 Έλεγχος αγορών και χρήσεων IoT προϊόντων στο Marketplace

Οι λειτουργικότητες για τον έλεγχο αγορών και χρήσεων IoT προϊόντων που παρουσιάστηκαν στις προηγούμενες ενότητες παρέχονται στον χρήστη μέσω της γραφικής διεπαφής πύλης αγοράς (marketplace) που υλοποιήθηκε στα πλαίσια του έργου. Το αίτημα του χρήστη προωθείται από το στοιχείο λογισμικού αγοράς (marketplace) στην αντίστοιχη υπηρεσία του BaaS και ο χρήστης ενημερώνεται με την απάντηση. Στον παρακάτω πίνακα (Πίνακας 5) συνοψίζονται οι διεπαφές στο στοιχείο λογισμικού αγοράς.

Πίνακας 5: Διεπαφές σχετικά με τον έλεγχο αγορών και χρήσεων IoT προϊόντων στο Marketplace

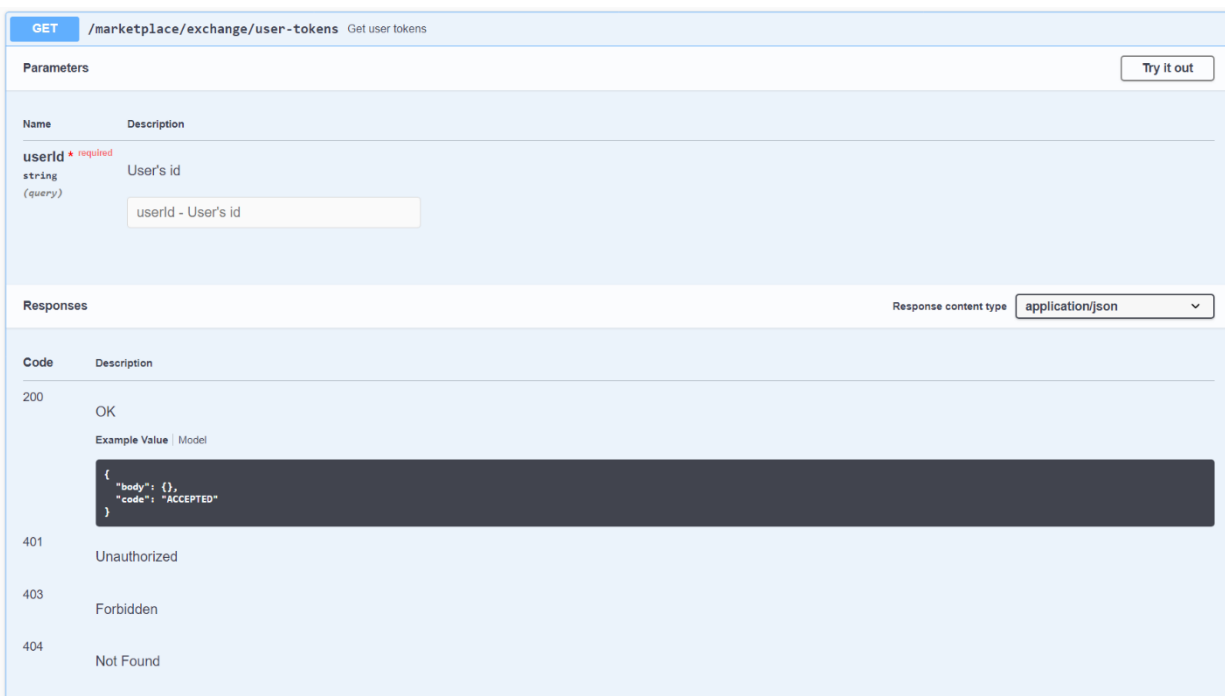
#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	User tokens	Marketplace GUI	Marketplace backend	GET	/exchange/user-tokens	(String, String, String)	(List<Object>, Message)	Request to retrieve user's token (wallet)
2	REST	receipt_buyer	Marketplace GUI	Marketplace backend	POST	/SymbIoTeMarketplace/auditing/receipt_buyer	(String, String, String)	(Object, Message)	Request for retrieving receipts as a buyer
3	REST	receipt_seller	Marketplace GUI	Marketplace backend	POST	/SymbIoTeMarketplace/auditing/receipt_seller	(String, String, String)	(Object, Message)	Request for retrieving receipts as a seller
4	REST	logs	Marketplace GUI	Marketplace backend	POST	/SymbIoTeMarketplace/auditing/logs	(String, String, String)	(Object, Message)	Request for checking the logs for access/usage to an IoT product
5	REST	verify_receipt	Marketplace GUI	Marketplace backend	POST	/SymbIoTeMarketplace/auditing/verify_receipt	(Object, String)	(Object, Message)	Request for verifying a receipt
6	REST	verify_access_log	Marketplace GUI	Marketplace backend	POST	/SymbIoTeMarketplace/auditing/verify_access_log	(Object, String)	(Object, Message)	Request for verifying the access to an IoT product

Μετά τη σύνδεση στην πύλη αγοράς, ένας χρήστης μπορεί να ανακτήσει τη λίστα με τα tokens που έχει στην κατοχή του όπως φαίνεται στην Εικόνα 29.



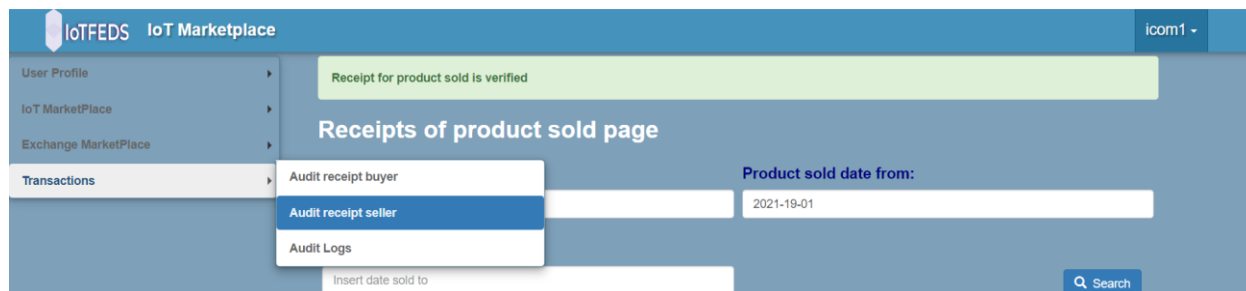
Εικόνα 29: Εμφάνιση του wallet με τα tokens του χρήστη.

Το αίτημα του χρήστη προωθείται στο παρακάτω endpoint (Εικόνα 30) στο Marketplace το οποίο προωθεί το αίτημα στο BaaS για να ανακτήσει τα έγκυρα tokens που έχει στην κατοχή του ο χρήστης. Δέχεται ως παράμετρος το αναγνωριστικό του χρήστη (userId), καθώς και προαιρετικά το αναγνωριστικό της αγοράς (MarketplaceId) και το αναγνωριστικό του προϊόντος (productId) στην περίπτωση αναζήτησης για ένα συγκεκριμένο προϊόν. Ο χρήστης ενημερώνεται με τη λίστα των tokens ή αντίστοιχο μήνυμα λάθους.



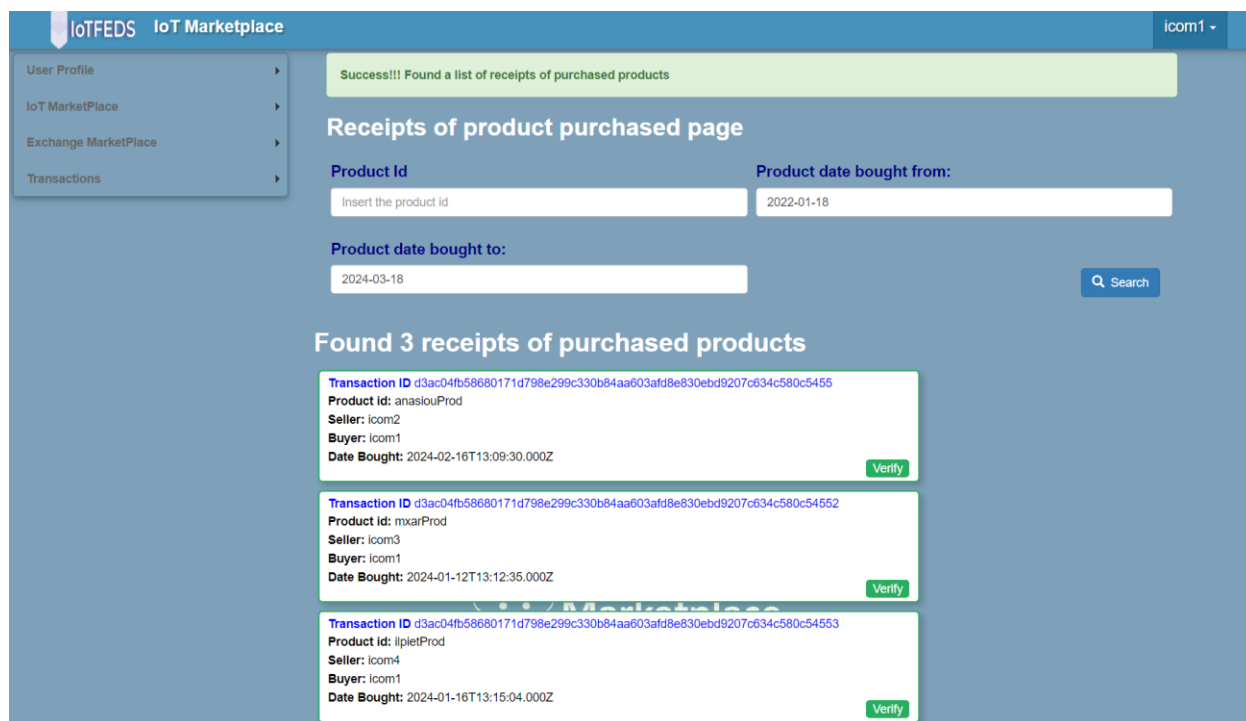
Εικόνα 30: Endpoint για την ανάκτηση της λίστας των tokens του χρήστη (wallet) στο Marketplace.

Στη συνέχεια ο χρήστης μπορεί να ελέγξει τις αποδείξεις του και τα logs από το μενού “Transactions” όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 31: Επιλογές για έλεγχο αποδείξεων και logs του χρήστη.

Ο χρήστης μπορεί να αναζητήσει τα αποδεικτικά αγοράς ενός προϊόντος όπως φαίνεται στην Εικόνα 32.



Εικόνα 32: Αποδείξεις αγοράς ενός προϊόντος.

Το αίτημα προωθείται στο endpoint 2 του πίνακα που δέχεται ως παραμέτρους το αναγνωριστικό του προϊόντος και το χρονικό διάστημα μέσα στο οποίο επιθυμεί ο χρήστης να ελέγξει τις αποδείξεις του (με τη μορφή ημερομηνιών), ενώ απαιτείται και το όνομα του χρήστη το οποίο προκύπτει από το token που έχει από τη σύνδεση του. Η επιστροφή του endpoint είναι μια λίστα με τις αποδείξεις συναλλαγών (Εικόνα 33).

Code	Details
200	Response body <pre>{ "TransactionID": "d3ac04fb58680171d798e299c330b84aa603afd8e830ebd9207c634c580c5455", "Buyer": "icom2", "Seller": "icom1", "ProductID": "anaslouProd", "DateBought": "2024-01-16T13:49:30.000Z" }</pre> Download

Εικόνα 33: Απάντηση με τη λίστα αποδείξεων αγοράς του χρήστη.

Ο χρήστης επιπλέον μπορεί να ζητήσει τον έλεγχο εγκυρότητας μίας συναλλαγής πατώντας το κουμπί «Verify» στη συναλλαγή που ενδιαφέρεται. Ο χρήστης ενημερώνεται με αντίστοιχο μήνυμα για την εγκυρότητα της συναλλαγής όπως φαίνεται στην Εικόνα 34.

The screenshot shows the 'IoT MarketPlace' interface. On the left is a sidebar with navigation links: 'User Profile', 'IoT MarketPlace', 'Exchange MarketPlace', and 'Transactions'. The main content area is titled 'Receipts of product purchased page'. It features a search bar with 'Product Id' and 'Product date bought from' fields. Below the search bar, it says 'Found 3 receipts of purchased products'. Three receipt cards are displayed, each with transaction details and a 'Verify' button. The first card shows Transaction ID d3ac04fb58680171d798e299c330b84aa603afd8e830ebd9207c634c580c5455, Product id: anaslouProd, Seller: icom2, Buyer: icom1, and Date Bought: 2024-02-16T13:09:30.000Z. The second card shows Transaction ID d3ac04fb58680171d798e299c330b84aa603afd8e830ebd9207c634c580c54552, Product id: mxarProd, Seller: icom3, Buyer: icom1, and Date Bought: 2024-01-12T13:12:35.000Z. The third card shows Transaction ID d3ac04fb58680171d798e299c330b84aa603afd8e830ebd9207c634c580c54553, Product id: ilpletProd, Seller: icom4, Buyer: icom1, and Date Bought: 2024-01-16T13:15:04.000Z.

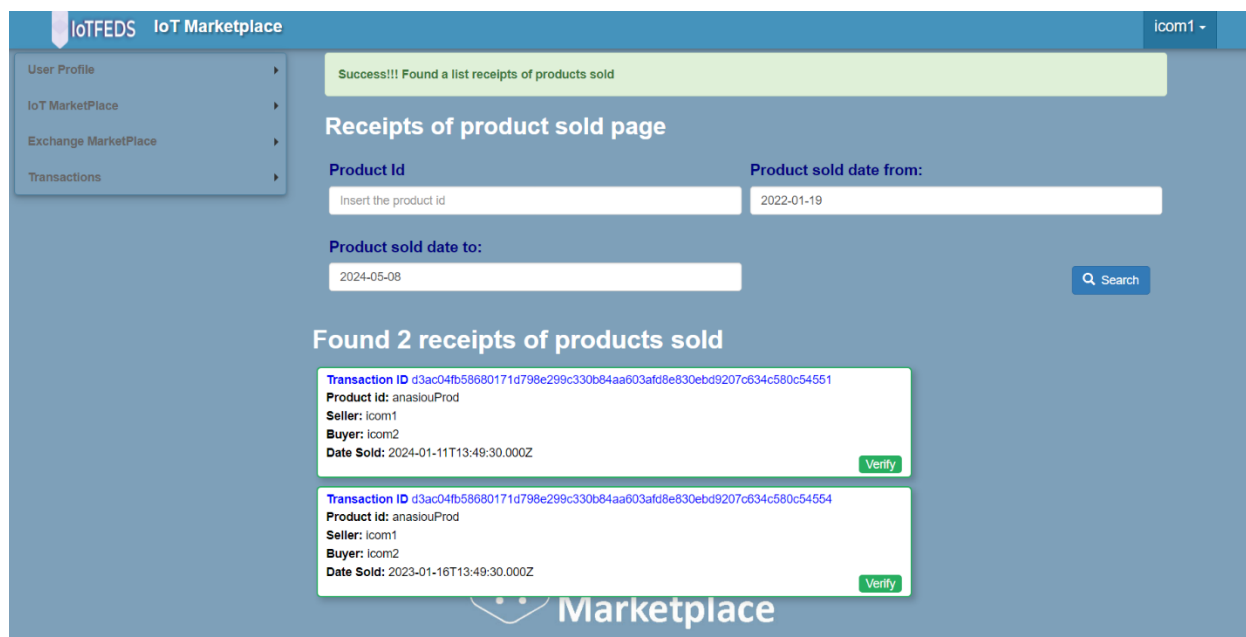
Εικόνα 34: Έλεγχος εγκυρότητας συναλλαγής για προϊόν που έχει αγοράσει ο χρήστης.

Για την εξυπηρέτηση του αιτήματος του χρήστη αξιοποιείται το endpoint 4 του πίνακα που είναι υπεύθυνο για τον έλεγχο ακεραιότητας μιας απόδειξης και δέχεται ως είσοδο δύο παραμέτρους. Η πρώτη αποτελεί το αντικείμενο της απόδειξης. Η δεύτερη είναι το όνομα του χρήστη που προκύπτει από το token που έχει από τη σύνδεση του. Η απάντηση παραλαμβάνεται από το BaaS μετά από προώθηση του αιτήματος στην αντίστοιχη διεπαφή του BaaS. Το αντικείμενο που επιστρέφεται περιλαμβάνει μια λογική μεταβλητή (true ή false) όπως φαίνεται παρακάτω:

Code	Details
200	Response body <pre>{ "Verified": true }</pre> Download

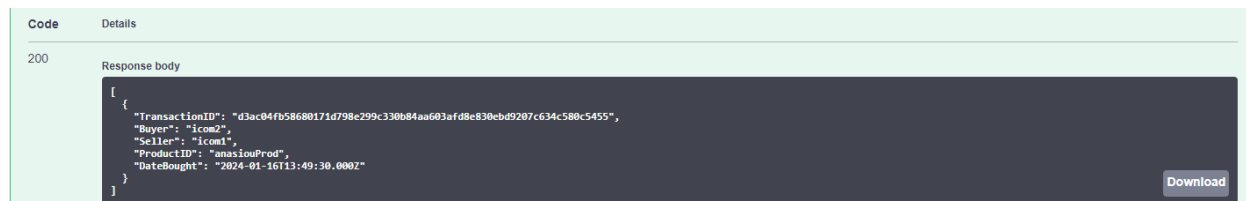
Εικόνα 35: Απάντηση αιτήματος ελέγχου εγκυρότητας συναλλαγής.

Ένας χρήστης επιπλέον μπορεί να αναζητήσει τα αποδεικτικά για τα προϊόντα που πούλησε (Εικόνα 36).



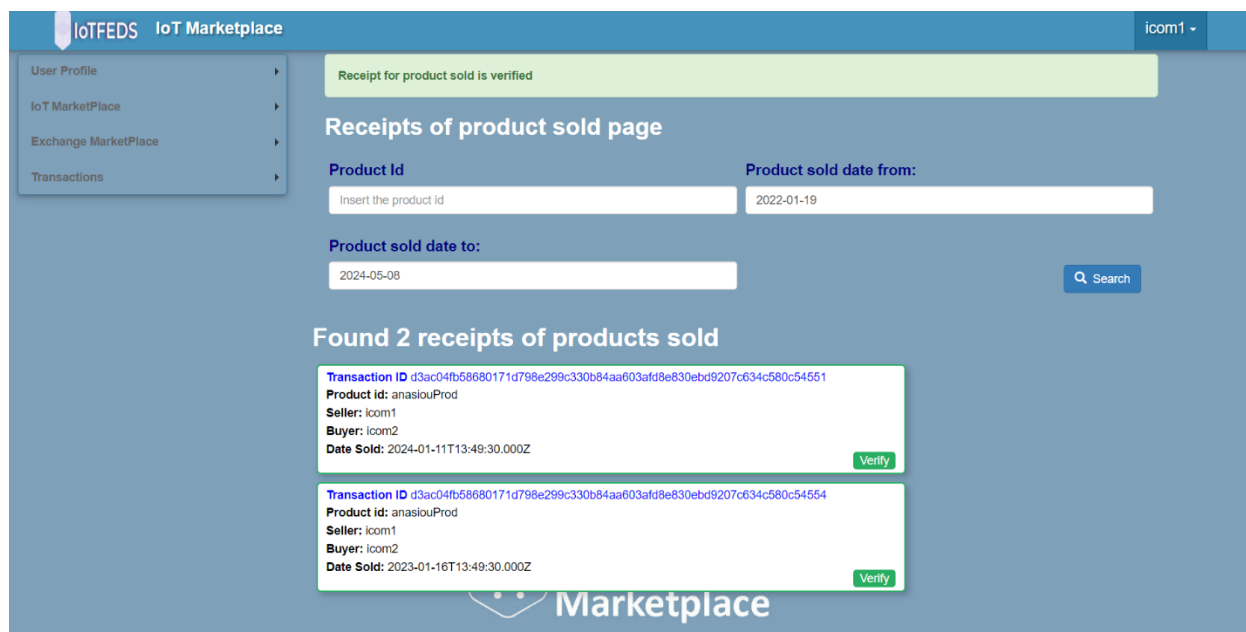
Εικόνα 36: Αναζήτηση αποδεικτικών χρήση για προϊόντα που πούλησε.

Το αίτημα προωθείται στο endpoint 3 του πίνακα που ομοίως δέχεται ως παραμέτρους το αναγνωριστικό του προϊόντος και το χρονικό διάστημα μέσα στο οποίο επιθυμεί ο χρήστης να ελέγξει τις αποδείξεις του (με τη μορφή ημερομηνιών), ενώ απαιτείται και το όνομα του χρήστη το οποίο προκύπτει από το token που έχει από τη σύνδεση του. Η επιστροφή του endpoint είναι μια λίστα με τις αποδείξεις συναλλαγών (Εικόνα 33). Η λίστα παραλαμβάνεται από το BaaS προωθώντας το αίτημα στην αντίστοιχη διεπαφή του BaaS.



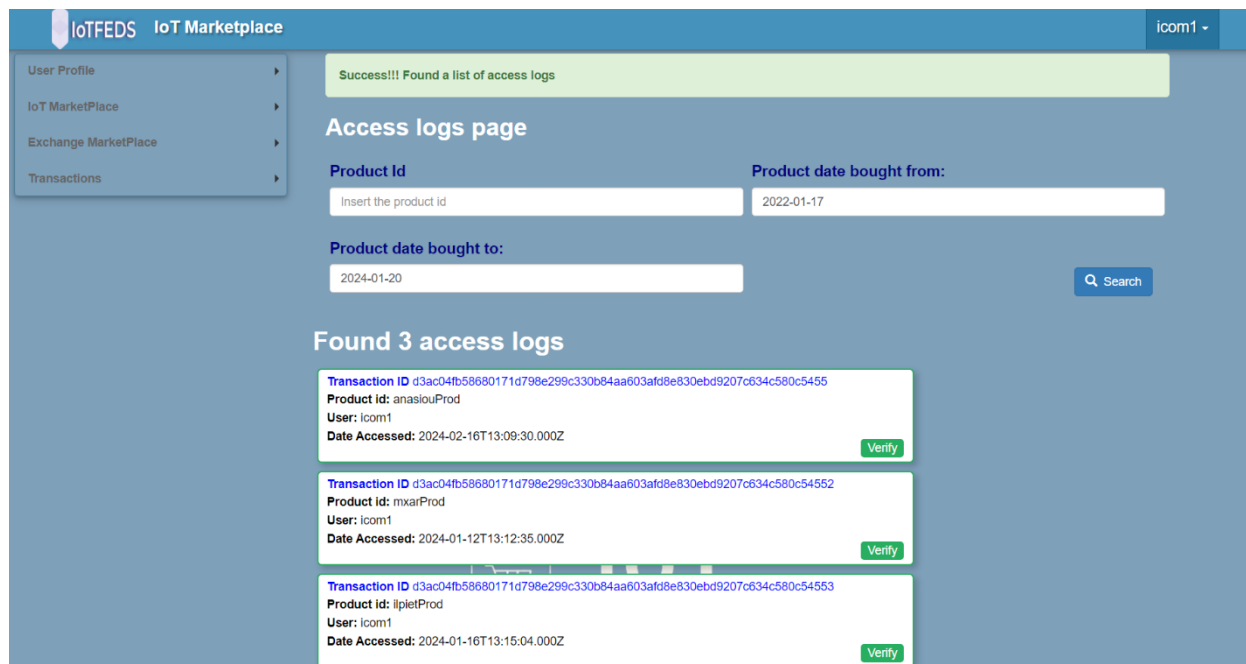
Εικόνα 37: Αποδείξεις συναλλαγών χρήση για προϊόντα που πούλησε.

Ομοίως, πατώντας το κουμπί “Verify” σε μία συναλλαγή μπορεί να ελέγξει την εγκυρότητα του αποδεικτικού για ένα προϊόν που πούλησε, το οποίο προωθείται στο endpoint 4 που περιγράφηκε νωρίτερα.



Εικόνα 38: Έλεγχος εγκυρότητας συναλλαγής για προϊόν που έχει πουλήσει ο χρήστης

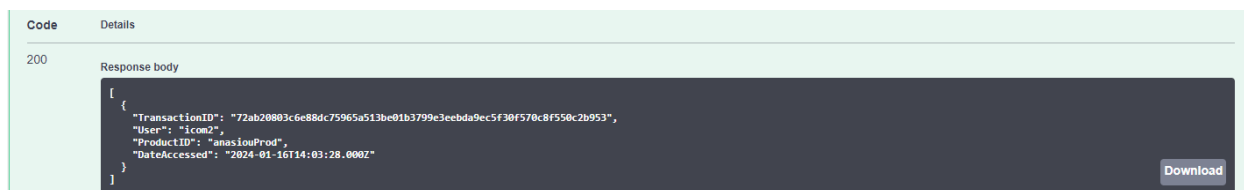
Ένας χρήστης μπορεί να αναζητήσει τα αποδεικτικά χρήσης ενός προϊόντος, στο οποίο έχει πρόσβαση, προσδιορίζοντας το επιθυμητό διάστημα (ημ/νιες) για την αναζήτηση, όπως φαίνεται στην Εικόνα 39.



Εικόνα 39: Αναζήτηση αποδεικτικών χρήσης στο Marketplace.

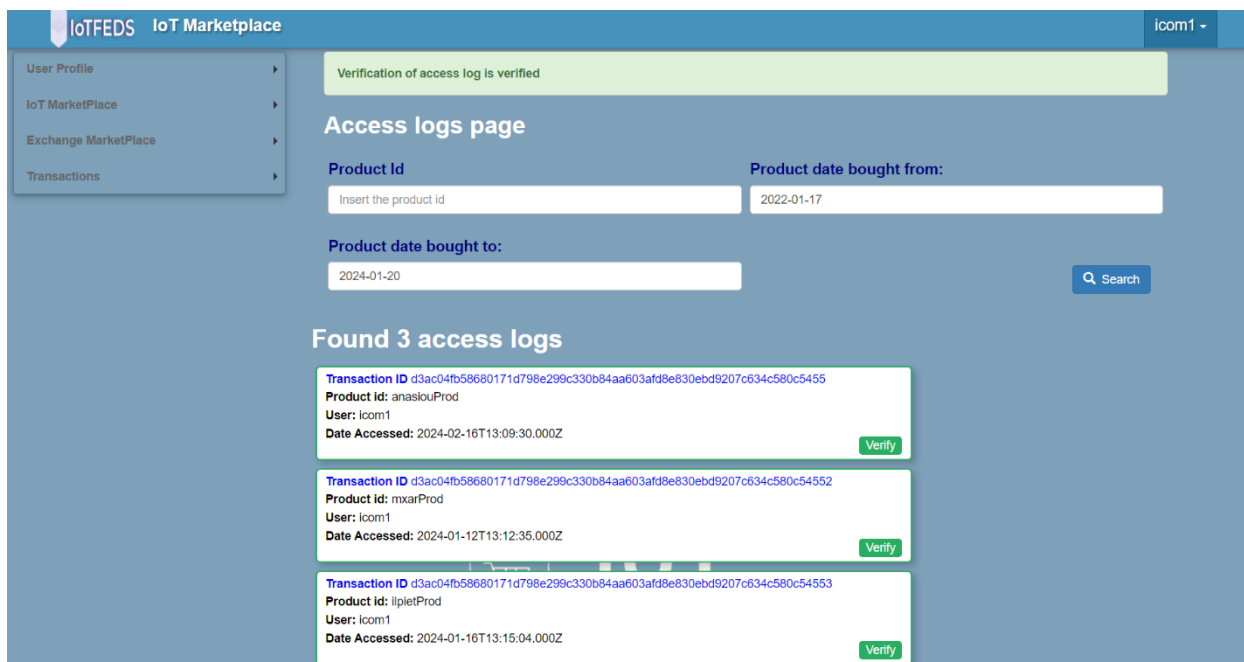
Το αίτημα του χρήστη προωθείται στην αντίστοιχη διεπαφή του marketplace (endpoint 5 του πίνακα) που είναι υπεύθυνο για την αναζήτηση των αποδεικτικών χρήσης και δέχεται ως είσοδο τρεις παραμέτρους: το αναγνωριστικό του προϊόντος (productId) που χρησιμοποιήθηκε και δύο ημερομηνίες (dateFrom, dateTo), ανάμεσα στις οποίες θα γίνει η αναζήτηση των καταγραφών. Το όνομα του χρήστη προκύπτει από το token

που έχει από τη σύνδεση του στο σύστημα και το οποίο χρησιμοποιείται για την αλληλεπίδραση του χρήστη με το Marketplace. Ο χρήστης ενημερώνεται με το αναγνωριστικό της συναλλαγής (TransactionID), τον κάτοχο της συναλλαγής (userId), το αναγνωριστικό του προϊόντος (productId) και την ημ/νία προσπέλασης (dataAccessed) ή αντίστοιχο μήνυμα λάθους όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 40: Απάντηση αναζήτησης αποδεικτικών χρήσης.

Ένας χρήστης μπορεί να ελέγξει την εγκυρότητα ενός αποδεικτικού χρήσης επιλέγοντας το κουμπί “Verify” για μία συγκεκριμένη συναλλαγή, όπως φαίνεται στην Εικόνα 41. Το αίτημα προωθείται στο marketplace για το συγκεκριμένο αναγνωριστικό συναλλαγής, το αναγνωριστικό προϊόντος, τον χρήστη και την ημ/νία προσπέλασης. Σε περίπτωση που ο έλεγχος είναι επιτυχής (έγκυρο αποδεικτικό) ο χρήστης ενημερώνεται με τις πληροφορίες του αποδεικτικού, διαφορετικά με μήνυμα μη εγκυρότητας.



Εικόνα 41: Έλεγχος εγκυρότητας αποδεικτικών χρήσης στο Marketplace.

Το endpoint 6 είναι αυτό που υλοποιεί τον έλεγχο εγκυρότητας αποδεικτικών χρήσης και δέχεται ως είσοδο το αποδεικτικό χρήσης που θέλουμε να ελέγξουμε. Επιπλέον, δέχεται το όνομα του χρήστη που προκύπτει από το token που έχει από τη σύνδεση του. Το αντικείμενο που επιστρέφεται μετά από επικοινωνία με την αντίστοιχη διεπαφή του BaaS περιλαμβάνει μια λογική μεταβλητή (true ή false).

Code	Details
200	Response body <pre>{ "Verified": true }</pre> Download

Εικόνα: Απάντηση για την εγκυρότητα ενός αποδεικτικού χρήσης ενός προϊόντος.

4 Συμπεράσματα

Το παραδοτέο αυτό ασχολήθηκε με μηχανισμούς καταγραφής και ελέγχου συναλλαγών στα πλαίσια της ΕΕ 3, και πιο ειδικά κάτω από την Δ3.1 – «Καταγραφή και Έλεγχος Συναλλαγών». Η προσέγγιση που ακολουθήθηκε βασίστηκε στις ανάγκες του έργου, καθώς και στις κατευθυντήριες γραμμές που έχουν τεθεί με την ανάπτυξη μηχανισμών και στοιχείων λογισμικού που υλοποιήθηκαν στα πλαίσια των προηγούμενων Ενοτήτων Εργασίας, και έχουν περιγραφεί σε άλλα παραδοτέα (Π2.2) , αλλά και σε μηχανισμούς που ανήκουν σε μελλοντικές δράσεις (Δ3.2 – «Ανάθεση Τιμών και Πολιτικών Χρέωσης», Δ3.3 – «Εναλλακτικός Μηχανισμός Ανταλλαγής Πόρων IoT»). Όλοι οι μηχανισμοί που αναλύθηκαν σε αυτό το παραδοτέο, τόσο αυτοί που αναφέρθηκαν ως τεχνολογικό υπόβαθρο, όσο και αυτοί που τελικά υλοποιήθηκαν, είναι βασισμένοι στο στοιχείο λογισμικού του BaaS και στην τεχνολογία του blockchain, αφού αυτή πληροί τις προϋποθέσεις με τον καλύτερο δυνατό τρόπο για την ανάπτυξη τέτοιου είδους μηχανισμών.

Η συνεισφορά αυτού του παραδοτέου είναι διπλή και μπορεί να διαχωριστεί στην εξερεύνηση του τεχνολογικού υποβάθρου μηχανισμών καταγραφής και ελέγχου συναλλαγών βασισμένων σε τεχνολογίες blockchain, και η ανάπτυξη αντίστοιχων μηχανισμών για την υλοποίηση της δράσης Δ3.1. Πιο συγκεκριμένα, αρχικά γίνεται μια ανάλυση των λύσεων που συναντώνται στη σύγχρονη βιβλιογραφία για την καταγραφή και έλεγχο σημαντικών ενεργειών, όπου και διακρίθηκαν τα κοινά χαρακτηριστικά που παρουσιάζουν αυτές οι λύσεις. Στη συνέχεια, και βασιζόμενοι σε αυτά τα χαρακτηριστικά, αναπτύχθηκαν και περιγράφηκαν οι μηχανισμοί που υλοποιήθηκαν για το έργο IoTFeds, και μπορούν να διακριθούν σε δύο κατηγορίες. Η πρώτη αφορά την καταγραφή και τον έλεγχο των αγορών IoT προϊόντων που πραγματοποιούνται στην αγορά του IoTFeds, και η δεύτερη στην καταγραφή και έλεγχο της χρήσης αυτών των προϊόντων. Ο έλεγχος που αναφέρεται παραπάνω έχει την έννοια της επίβλεψης αυτών των καταγραφών, από συγκεκριμένους χρήστες κάθε φορά (ανάλογα με το use case). Ωστόσο, κρίθηκε απαραίτητος και ένας μηχανισμός ελέγχου ακεραιότητας αυτών των συναλλαγών, που επιτρέπει στον χρήστη να ελέγξει την ορθότητα και την εγκυρότητα ενός αποδεικτικού, είτε χρήσης, είτε αγοράς ενός προϊόντος.

Οι παραπάνω μηχανισμοί θέτουν τη βάση για τις επόμενες δράσεις της ενότητας ΕΕ3 και μπορούν να χρησιμοποιηθούν όπως αυτό κρίνεται απαραίτητο. Επιπρόσθετα, μπορούν να σταθούν και μόνοι τους ως λύσεις που στόχο έχουν την διασφάλιση της ακεραιότητας και της διαφάνειας για ενέργειες που κρίνονται σημαντικό να επιβλέπονται μέσα στο οικοσύστημα του IoTFeds.

Βιβλιογραφία

- L. Van Hoya, P. -J. Maenhaut, T. Wauters, B. Volckaert and F. De Turck, "Logging mechanism for cross-organizational collaborations using Hyperledger Fabric," *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Seoul, Korea (South), 2019, pp. 352-359, doi: 10.1109/BLOC.2019.8751380
- M. Kumar, A. K. Singh and T. V. Suresh Kumar, "Secure Log Storage Using Blockchain and Cloud Infrastructure," *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bengaluru, India, 2018, pp. 1-4, doi: 10.1109/ICCCNT.2018.8494085.
- Belchior, R., Correia, M., Vasconcelos, A. (2019). JusticeChain: Using Blockchain to Protect Justice Logs. In: Panetto, H., Debruyne, C., Hepp, M., Lewis, D., Ardagna, C., Meersman, R. (eds) On the Move to Meaningful Internet Systems: OTM 2019 Conferences. OTM 2019. Lecture Notes in Computer Science(), vol 11877. Springer, Cham. https://doi.org/10.1007/978-3-030-33246-4_21
- Benedikt Putz, Florian Menges, Günther Pernul, A secure and auditable logging infrastructure based on a permissioned blockchain, *Computers & Security*, Volume 87, 2019, 101602, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2019.101602>.
- M. H. Chinaei, H. Habibi Gharakheili and V. Sivaraman, "Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract," in *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10117-10130, 15 June 2021, doi: 10.1109/JIOT.2021.3051433.
- S. Ali, G. Wang, M. Z. A. Bhuiyan and H. Jiang, "Secure Data Provenance in Cloud-Centric Internet of Things via Blockchain Smart Contracts," *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Guangzhou, China, 2018, pp. 991-998, doi: 10.1109/SmartWorld.2018.00175.