ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΥΠΟΛΟΓΙΣΤΩΝ

Αρχιτεκτονικές λογισμικού για ενοποίηση υπαρχόντων συστημάτων λογισμικού σε κλειστό ελεγχόμενο blockchain για εφαρμογές κρίσιμης αποστολής

Software architectures for integration of legacy software systems into private permissioned blockchains for critical mission applications

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θεόδωρος Διαμαντίδης

Επιβλέπων: Βασίλειος Βεσκούκης
Αν. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2021

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΥΠΟΛΟΓΙΣΤΩΝ

Αρχιτεκτονικές λογισμικού για ενοποίηση υπαρχόντων συστημάτων λογισμικού σε κλειστό ελεγχόμενο blockchain για εφαρμογές κρίσιμης αποστολής

Software architectures for integration of legacy software systems into private permissioned blockchains for critical mission applications

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θεόδωρος Διαμαντίδης

Επιβλέπων: Βασίλειος Βεσκούκης
Αν. Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 15η Ιουλίου 2021.

.....	.....	.....
Βασίλειος Βεσκούκης	Νικόλαος Παπασπύρου	Δημήτριος Φωτάκης
Αν. Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αν. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2021

(Υπογραφή)

.....

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

Περίληψη

Οι καινοτόμες ιδιότητες του Blockchain έχουν οδηγήσει στην υιοθέτησή του στην ανάπτυξη κρυπτονομισμάτων, σε εφαρμογές χρηματοοικονομικής, και πλέον σε εφαρμογές γενικού σκοπού, όπως οι εφοδιαστικές αλυσίδες ή οι υπηρεσίες υγείας. Τέτοιες εφαρμογές έχουν συχνά απαιτήσεις αποδοτικότητας και απορρήτου, επομένως δημιουργείται η ανάγκη για κλειστά και ελεγχόμενα συστήματα Blockchain. Προκειμένου να εκτιμηθεί ορθά η αξία που μπορεί να εισφέρει η υιοθέτηση του Blockchain, είναι κρίσιμο να κατανοηθεί ο τρόπος λειτουργίας του, οι διαφορετικοί αλγόριθμοι συναίνεσης και οι ιδιαιτερότητες της κάθε πλατφόρμας. Παράλληλα, οι τρέχουσες αδυναμίες του Blockchain να διαχειριστεί εγγενώς την αποθήκευση μεγάλου όγκου δεδομένων, την εκτέλεση απαιτητικών υπολογισμών και την αλληλεπίδραση με εξωγενή συστήματα, παρακινούν την εύρεση λύσεων που να διατηρούν ωστόσο τις ιδιότητες της αποκεντρικοποίησης και της ασφάλειας.

Σημαντικό εμπόδιο στην υιοθέτηση του Blockchain αποτελεί η συχνή ανάγκη για διατήρηση υπάρχοντων συστημάτων σε λειτουργία. Ενδιαφέρουσα τέτοια περίπτωση είναι οι εφαρμογές κρίσιμης αποστολής, λόγω της τομής των χαρακτηριστικών τους με τις ιδιότητες του Blockchain. Στην παρούσα εργασία εξετάζουμε πώς μπορεί να ενοποιηθεί ένα υπάρχον σύστημα με ένα σύστημα Blockchain με τρόπο που να ελαχιστοποιούνται οι παρεμβάσεις στο πρώτο, μελετώντας την περίπτωση των συστημάτων αεροδιακομιδής. Αναλύουμε τις ευκαιρίες, τις ανάγκες και τους περιορισμούς που προκύπτουν από την υιοθέτηση του Blockchain στην αεροδιακομιδή. Προτείνουμε τις αρχιτεκτονικές των “διεπαφών Blockchain” με ρόλο διαμεσολαβητή και τη χρήση τους σε ένα παράλληλο σύστημα για καταγραφή συμβάντων και για παραγωγή προτάσεων από smart contracts κατ’ αντιπαραβολή των αποφάσεων του υπάρχοντος συστήματος. Αναλύουμε τα δεδομένα του υπάρχοντος συστήματος και τον μετασχηματισμό τους για να καταχωρηθούν στο Blockchain και βάσει αυτών μοντελοποιούμε το προτεινόμενο σύστημα παρακινούμενοι από ιδέες του αναπτυσσόμενου κλάδου του blockchain-oriented software engineering (BOSE).

Λέξεις κλειδιά: Blockchain, τεχνολογία λογισμικού, αρχιτεκτονική λογισμικού, ενοποίηση, μοντελοποίηση, smart contracts, κρίσιμες αποστολές, αεροδιακομιδή

Abstract

Blockchain's novel properties have led to its adoption in cryptocurrency creation, financial applications and now in general-purpose applications for supply chain management, healthcare services etc. Such applications usually have performance and confidentiality requirements, and thus the need for closed and permissioned Blockchain systems emerges. In order to properly evaluate the value-added by adopting Blockchain, it is crucial that we comprehend its inner workings, the various consensus algorithms, and the specificities of each platform. At the same time, Blockchain's current weaknesses to manage large data storage, computationally-intensive calculations, and interaction with external systems, motivate us to discover solutions that preserve, nevertheless, the decentralization and security properties.

A significant hurdle when considering the adoption of Blockchain is the common need to maintain existing systems in operation. An interesting such case concerns critical mission applications, due to the intersection of their characteristics with Blockchain's properties. In this thesis, we address ways to integrate a legacy system with a Blockchain system in a manner that minimizes interventions to the former, while studying the case of air medical services. We examine the opportunities, needs and limitations that arise from adopting Blockchain in air medical services. We propose architectures for "Blockchain interfaces" that act as middleware and we advocate their use in a parallel system that records events and generates recommendations via smart contracts in juxtaposition to the legacy system's decisions. We analyze the legacy system's data items and the transformation needed to add them to the Blockchain. Based on that, we model the proposed system, motivated by ideas from the emerging field of blockchain-oriented software engineering (BOSE).

Keywords: Blockchain, software engineering, software architecture, integration, modeling, smart contracts, critical mission, air medical services

Ευχαριστίες

Στον επιβλέποντα και καθηγητή μου Βασίλη Βεσκούκη και τον υποψήφιο διδάκτορα Αντώνη Βιτοράτο για την ενασχόληση και καθοδήγησή τους στη διπλωματική μου εργασία.

Στην οικογένειά μου, τους κοντινούς ανθρώπους, και τους φίλους και φίλες που έτυχε να συναντηθούμε ή να συνεργαστούμε, για την ανεκτίμητη αγάπη τους.

Σε όσες και όσους προσέφεραν και προσφέρουν γύρω τους χωρίς να αποζητούν ανταπόδοση.

Περιεχόμενα

Κατάλογος σχημάτων

Κατάλογος πινάκων

Κατάλογος συντομογραφιών

ACK	Acknowledgement
BC	Blockchain
BFT	Byzantine-fault tolerance
BOS	Blockchain-oriented software
BOSE	Blockchain-oriented software engineering
BPMN	Business Process Model & Notation
CFT	Crash fault tolerance
DApp	Decentralized app
DAG	Directed acyclic graph
DB	Database
METAR	Meteorological Aerodrome Reports
N/A	Not available
OCR	Optical character recognition
PoW	Proof-of-Work
SWEBOK	Software Engineering Body of Knowledge
TAF	Terminal Aerodrome Forecasts
TEE	Trusted execution environment
UML	Unified Modeling Language
ΑΤΑ	Αρχηγείο Τακτικής Αεροπορίας
ΓΕΑ	Γενικό Επιτελείο Αεροπορίας
ΓΕΣ	Γενικό Επιτελείο Στρατού
ΔΑΣ	Διεύθυνση Αεροπορίας Στρατού
Ε/Π	Ελικόπτερα
ΕΚΑΒ	Εθνικό Κέντρο Άμεσης Βοήθειας
ΕΜΥ	Εθνική Μετεωρολογική Υπηρεσία
ΙΜΠ	Ι Μεραρχία Πεζικού
ΚΕΠΙΧ	Κέντρο Επιχειρήσεων
ΤΑΞΑΣ	1η Ταξιαρχία Αεροπορίας Στρατού

ΜΕΡΟΣ Α: ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ ΚΑΙ ΣΧΕΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1 Blockchain

1.1 Θεμελιώδεις έννοιες και ιδιότητες

Από τη σύλληψή της στο white paper του Bitcoin το 2008 [1] έως σήμερα, η ιδέα του Blockchain έχει συγκεντρώσει μαζικό ενδιαφέρον, αρχικά στον τομέα των κρυπτονομισμάτων [2], ακολούθως στον ευρύτερο τομέα της χρηματοοικονομικής για την ανταλλαγή αξιών και την αλγοριθμική εκτέλεση συμβολαίων [3], και πλέον σε συστήματα γενικού σκοπού που αφορούν από εφοδιαστικές αλυσίδες μέχρι υπηρεσίες υγείας. [3], [4]

Το Blockchain ως δομή δεδομένων αποτελεί μία κατανεμημένη καταγραφή συναλλαγών. Οι συναλλαγές ομαδοποιούνται σε blocks τα οποία, αφού επιβεβαιωθούν, συνδέονται κρυπτογραφικά σε μία συνεχόμενη ακολουθία όπου επιτρέπονται μόνο προσθήκες. Ένα σύστημα που υλοποιεί αυτήν τη δομή ονομάζεται σύστημα Blockchain. [5]

Βασικές έννοιες που αφορούν το Blockchain είναι οι εξής.

Συναλλαγή (transaction): Είναι η μικρότερη αυτοτελής μονάδα πληροφορίας που ανταλλάσσεται σε ένα σύστημα Blockchain και αποτελεί ένα μήνυμα στο οποίο καθορίζονται ο χρόνος δημιουργίας, οι εντολές που πρέπει να εκτελεστούν, οι παράμετροί τους, ο αποστολέας και ο παραλήπτης. [2], [5]

Block: Αποτελείται από ένα σύνολο ομαδοποιημένων συναλλαγών και μία επικεφαλίδα με κρυπτογραφικό σύνδεσμο προς το προηγούμενο block και άλλα μεταδεδομένα, ανάλογα με την υλοποίηση. [5]

Κόμβος (node): Συσκευή ή διαδικασία που συμμετέχει σε ένα δίκτυο Blockchain. Το δίκτυο είναι peer-to-peer, επομένως κάθε κόμβος συμμετέχει ισότιμα διατηρώντας ένα πλήρες ή μερικό αντίγραφο του ledger και εφαρμόζοντας την πολιτική συναίνεσης του συστήματος. [5]

Ledger: Η καταγραφή των συναλλαγών που διατηρείται κατανεμημένα με αντίγραφα σε κάθε κόμβο. Οι συναλλαγές του ledger είναι οριστικές και αναλλοίωτες. Ο στόχος του συστήματος Blockchain είναι να διασφαλίσει μέσω πρωτοκόλλου ότι τα ledger που διατηρούνται σε κάθε

κόμβο είναι πανομοιότυπα, ώστε να αντικατοπτρίζουν την ίδια κατάσταση (state). [2], [5]

Συναίνεση (consensus): Ονομάζεται ο αλγόριθμος με τον οποίο οι κόμβοι ενός συστήματος Blockchain συμφωνούν ότι μία συναλλαγή είναι έγκυρη και καταλήγουν σε μία κοινή κατάσταση του ledger με το ίδιο σύνολο συναλλαγών και την ίδια ταξινόμησή τους. [5]

Smart contract: Παρότι προγενέστερος [6], ο όρος smart contract έχει καθιερωθεί στις τεχνολογίες Blockchain για οποιοδήποτε πρόγραμμα μπορεί να καταχωρηθεί σε ένα σύστημα Blockchain, να εκτελεστεί από τους κόμβους και να καταγράψει τα αποτελέσματά του στο ledger. Ο κώδικάς του παραμένει αναλλοίωτος. [2], [5]

Το έντονο ενδιαφέρον για την τεχνολογία του Blockchain οφείλεται στις παρακάτω καινοτόμες ιδιότητές του.

Αμεταβλητότητα (immutability): Το ledger επιτρέπει μόνο την προσθήκη νέων συναλλαγών. Οι υπάρχουσες μένουν αναλλοίωτες και σε μόνιμη σειρά.

Αποκεντρικοποίηση (decentralization): Κάθε κόμβος διατηρεί το δικό του αντίγραφο του ledger, διενεργεί ανεξάρτητα τον έλεγχο των συναλλαγών και η εξουσία για τη λήψη αποφάσεων και η εμπιστοσύνη είναι διαμοιρασμένη στο σύνολο των κόμβων. Αποτελεί το θεμέλιο για την ύπαρξη αποκεντρικοποιημένων υποδομών όπως τα smart contracts ή τα DApps (decentralized apps).

Διαφάνεια (transparency): Όλοι έχουν πρόσβαση στο ledger με το ιστορικό των συναλλαγών και επομένως γνωρίζουν πώς έχει προκύψει το εκάστοτε blockchain state. [2], [7]

Ο βαθμός στον οποίο ισχύουν αυτά, εξαρτάται από τον τύπο του συστήματος Blockchain (permissionless ή permissioned) και τον αλγόριθμο συναίνεσης, οι οποίοι επιλέγονται ανάλογα με το threat model της εφαρμογής και τις απαιτήσεις αποδοτικότητας. [8]

1.2 Τύποι Blockchain και αλγόριθμοι συναίνεσης

Το πρώτο Blockchain προτάθηκε θεωρητικά το 2008 [1] και υλοποιήθηκε το 2009 [9] με τη δημιουργία του Bitcoin. Αποτελεί ένα ψηφιακό νόμισμα και σύστημα πληρωμών που χρησιμοποιεί κρυπτογραφικές τεχνικές για να ελέγξει τη γέννηση νέων νομισμάτων και να επαληθεύσει τη μεταφορά αξιών, ώστε να λειτουργεί ανεξάρτητα από μία κεντρική τράπεζα. [3]

Το Bitcoin χρησιμοποιεί ένα ανοικτό σύστημα Blockchain, με την έννοια ότι οποιαδήποτε έχει τη δυνατότητα να συμμετέχει και να αλληλεπιδράσει με αυτό. Κάθε χρήστρια γίνεται μέρος του δικτύου, αποκτά προσωπική διεύθυνση και μπορεί ισότιμα να δημιουργεί και να επαληθεύει συναλλαγές. Ακόμη, μπορεί να συμμετέχει στη διαδικασία του mining, με την οποία γίνονται δεκτές οι νέες συναλλαγές ως μέρος του αλγορίθμου συναίνεσης Proof-of-Work (PoW). [10]

Μετά το Bitcoin ακολούθησαν διάφορα παρόμοια συστήματα ανοικτού τύπου για την υλοποίηση κρυπτονομισμάτων, με αξιοσημείωτη περίπτωση το Ethereum το 2015 [11]. Η καινοτομία του Ethereum ήταν η δημιουργία του ως πλατφόρμα γενικού σκοπού με γλώσσα προγραμματισμού Turing-complete που εκτελείται από κάθε κόμβο στο περιβάλλον Ethereum Virtual Machine [12]. Έτσι, πέρα από τη χρήση του κρυπτονομίσματος, οι χρήστες μπορούν να αναπτύσσουν κατανεμημένες εφαρμογές με τη μορφή smart contracts. [3]

Παρότι τα πρώτα συστήματα Blockchain ήταν ανοικτά και βασιζόντουσαν σε περιβάλλοντα χωρίς εμπιστοσύνη και κεντρικές αρχές, δημιουργήθηκε η ανάγκη σε επιχειρήσεις να χρησιμοποιήσουν ιδιωτικές πλατφόρμες όπου κάθε κόμβος μπορεί να έχει διαφορετικά δικαιώματα και η πρόσβαση στο δίκτυο είναι περιορισμένη. [13]

1.2.1 Τύποι Blockchain

Permissionless: Πρόκειται για τα συστήματα ανοικτού τύπου που προαναφέραμε. Βασίζονται στην υπόθεση ότι δεν υπάρχει εμπιστοσύνη σε κανέναν κόμβο και ότι ο κοινός παρονομαστής είναι η χρηματική αξία. Η διακυβέρνηση τέτοιων συστημάτων στηρίζεται στην ύπαρξη ενός κοινού νομίσματος που μέσω κρυπτοοικονομικών μηχανισμών και οικονομικών κινήτρων δημιουργείται, ανταλλάσσεται και χρησιμοποιείται για να

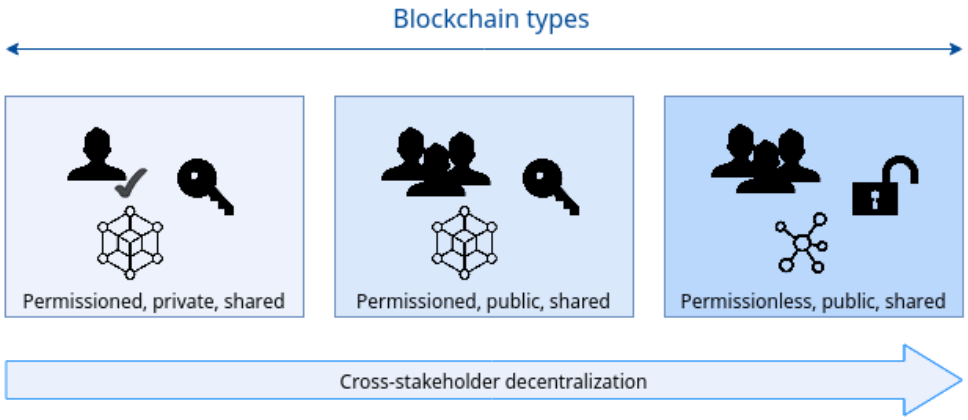
ενθαρρύνει μία ομάδα ατόμων χωρίς εμπιστοσύνη μεταξύ τους να συμμετέχουν σε ένα δίκτυο Blockchain και να διατηρήσουν ένα κοινό ledger, χωρίς την ανάγκη ύπαρξης κεντρικών αρχών. Η αντικατάσταση της συμβατικής εμπιστοσύνης με την αλγοριθμική εμπιστοσύνη βάσει οικονομικών κινήτρων λύνει τις ανάγκες για ανωνυμία και αποκεντρικοποίηση σε περιβάλλοντα όπου μπορεί να υπάρχει "κακόβουλη" συμπεριφορά, ωστόσο δημιουργεί ζητήματα αποδοτικότητας και κλιμακωσιμότητας. [14]

Permissioned: Πρόκειται για κλειστά και ιδιωτικά συστήματα Blockchain όπου κάποιος μπορεί να γίνει μέλος μόνο μετά από πρόσκληση της διαχειρίστριας του συστήματος. Εφόσον η ταυτότητα κάθε κόμβου είναι γνωστή, υπάρχει εγγενής προστασία από σιβυλλικές επιθέσεις όπου δημιουργούνται πολλαπλές ψευδείς ταυτότητες για απόκτηση επιρροής στο δίκτυο. Η γνωστή ταυτότητα και ο καθορισμός δικαιωμάτων σε κάθε κόμβο δημιουργεί έναν βαθμό εμπιστοσύνης που πηγάζει εκτός του Blockchain, αφαιρώντας έτσι την ανάγκη για συναίνεση μέσω οικονομικών κινήτρων. Με αυτόν τον τρόπο, τα permissioned συστήματα μπορούν να επιτύχουν μεγαλύτερη αποδοτικότητα καθώς και ιδιωτικότητα των δεδομένων τους καθόσον αυτά είναι προσβάσιμα μόνο εντός του δικτύου και από γνωστούς κόμβους [14]. Η κλειστότητα του συστήματος επιτρέπει την ευκολότερη παραμετροποίηση και προσαρμογή του στις ανάγκες των συμμετεχόντων, για παράδειγμα ως προς την επιλογή του αλγορίθμου συναίνεσης [10]. Από την άλλη υπάρχει θεωρητικά μείωση του βαθμού αποκεντρικοποίησης, αν και ορισμένοι συγγραφείς συγκρίνοντας με την πρακτική εφαρμογή των permissionless συστημάτων υποστηρίζουν ότι τα permissioned συστήματα μπορούν υπό προϋποθέσεις να αποδειχθούν πιο αποκεντρικοποιημένα. [15], [16]

Consortium: Θεωρείται υποκατηγορία των permissioned συστημάτων, παρουσιάζοντας την ιδιαιτερότητα ότι η διακυβέρνηση τους δεν γίνεται από μία οντότητα αλλά από μία ομάδα αυτών. Η συνεργατικότητα του μοντέλου αξιοποιεί σημαντικά τα οφέλη του blockchain με σκοπό να επιτρέψει τη συνύπαρξη οργανισμών που μπορεί να έχουν κοινούς στόχους αλλά ταυτόχρονα και αντικρουόμενα συμφέροντα. [17]

Hybrid: Στα υβριδικά συστήματα Blockchain συνδυάζονται οι ιδιότητες των permissionless και των permissioned συστημάτων. Οι

συμμετέχοντες μπορούν να καθορίζουν ποιες συναλλαγές και ποια δεδομένα θα είναι διαφανή δημοσίως και ποια θα παραμένουν ιδιωτικά. Το σύστημα περιλαμβάνει ένα permissioned Blockchain και ένα permissionless που είτε ανήκει στους συμμετέχοντες, είτε λειτουργεί ανεξάρτητα (πχ. Ethereum) και έχει τη δυνατότητα να διαλειτουργεί με το permissioned σύστημα. [17], [18]



Εικόνα 1: Φάσμα των τύπων Blockchain: permissioned (αριστερά), hybrid (μέση), permissionless (δεξιά). Ο βαθμός αποκεντρικοποίησης αυξάνεται από αριστερά προς τα δεξιά. [63]

1.2.2 Αλγόριθμοι συναίνεσης

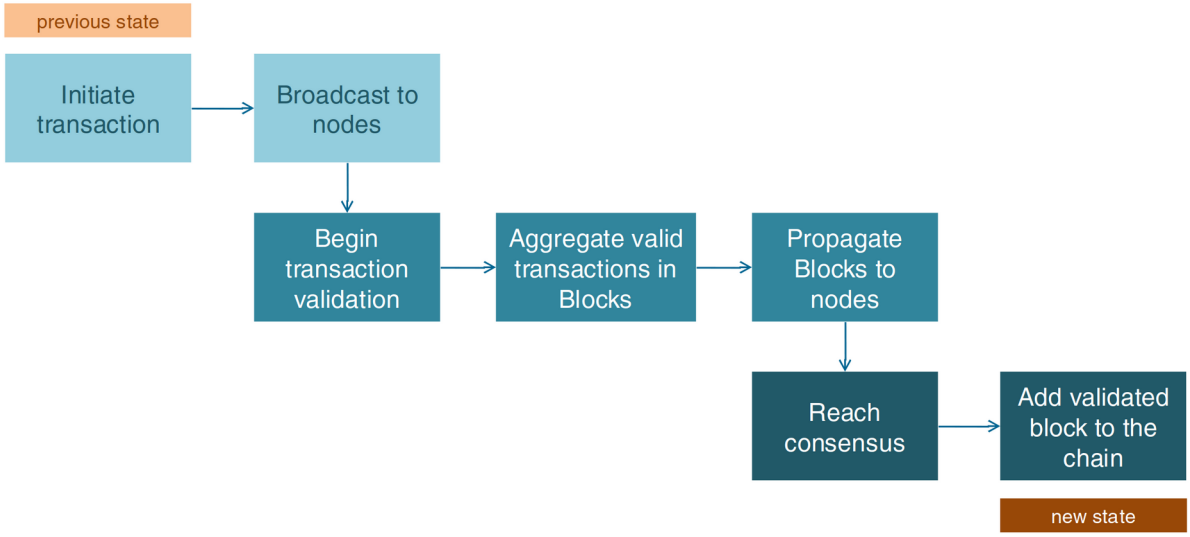
Η έννοια της συναίνεσης, δηλαδή του μηχανισμού με τον οποίο ένα σύνολο κόμβων καταλήγει σε συμφωνία για την κοινή κατάσταση του δικτύου, είναι προγενέστερη της τεχνολογίας Blockchain και προέρχεται από τη θεωρία των κατανεμημένων συστημάτων.

Βασική απαίτηση για έναν μηχανισμό συναίνεσης είναι η ανοχή σφαλμάτων (fault tolerance), δηλαδή η δυνατότητα του δικτύου να λειτουργεί ορθά ακόμη κι αν σε κάποια μέρη του παρουσιάζονται αστοχίες. Τα δύο πιο σημαντικά είδη αστοχιών για τα συστήματα Blockchain είναι τα crash faults και τα Byzantine faults. Ένας μηχανισμός που διαθέτει crash fault tolerance (CFT) μπορεί να επιτύχει συμφωνία στο δίκτυο ακόμη κι αν ορισμένοι κόμβοι πάψουν να λειτουργούν. Τα Byzantine faults περιγράφουν την αποτυχία ενός κόμβου να λειτουργήσει ορθά για οποιονδήποτε λόγο, όπως η αποτυχία υλικού ή λογισμικού, η αλλοίωση των μηνυμάτων, ή και ο κακόβουλος χειρισμός. Επομένως ένας μηχανισμός που διαθέτει Byzantine fault tolerance (BFT) έχει εξ ορισμού CFT, ενώ καλύπτει και ευρύτερες κατηγορίες σφαλμάτων. [8]

Η επιλογή του αλγορίθμου συναίνεσης σε ένα σύστημα Blockchain είναι κρίσιμη καθώς καθορίζει τον βαθμό ασφάλειας, εμπιστοσύνης, αποδοτικότητας και κλιμακωσιμότητάς του [8], [19]. Για παράδειγμα, η επιλογή ενός αλγορίθμου που διαθέτει μόνο τη CFT ιδιότητα, σημαίνει ότι το σύστημα Blockchain είναι ευάλωτο στην κακόβουλη συμπεριφορά ενός κόμβου που θα μπορούσε να παρουσιάζει μία αλλοιωμένη εκδοχή του ledger σε μία εφαρμογή που το ζητάει. [20]

Ανάλογα με τον τύπο του συστήματος Blockchain μπορεί να επιλέγονται διαφορετικού είδους αλγόριθμοι συναίνεσης. Στα permissionless συστήματα συναντώνται κυρίως αλγόριθμοι που βασίζονται σε αποδείξεις, όπως είναι ο Proof-of-Work (PoW), ο Proof-of-Stake (PoS) ή ο Proof-of-Elapsed-Time (PoET). Τέτοιοι αλγόριθμοι ονομάζονται και Nakamoto consensus, ένεκα του δημιουργού του PoW που ανακάλυψε για πρώτη φορά την ιδέα για αλγορίθμους συναίνεσης που βασίζονται σε οικονομικά κίνητρα με πιθανοτική συμπεριφορά. Αντίθετα, στα permissioned συστήματα συναντώνται κυρίως αλγόριθμοι που βασίζονται σε ψηφοφορίες. Καθόσον οι ταυτότητες των κόμβων είναι γνωστές και επομένως υπάρχει ένας προκαθορισμένος βαθμός εμπιστοσύνης, η συμφωνία μπορεί να επιτυχθεί μέσω εκλογών. Αξιοσημείωτοι τέτοιοι αλγόριθμοι είναι τα πρωτόκολλα Paxos [21] και ο Practical BFT (pBFT) [22] που προϋπάρχουν του Blockchain, ο Raft [23], ο Delegated BFT (dBFT) [24] και ο Federated Byzantine Agreement (FBA) [25]. Εξ αυτών, οι αλγόριθμοι Paxos και Raft διαθέτουν μόνο την ιδιότητα CFT, ενώ οι υπόλοιποι είναι BFT [26].

Οι περισσότερες πλατφόρμες permissioned συστημάτων Blockchain διαθέτουν αλγορίθμους συναίνεσης μόνο με την ιδιότητα CFT καθώς θεωρείται πιο σημαντική η αντιμετώπιση των crash faults από τα Byzantine faults [27] και για λόγους αποδοτικότητας. Ωστόσο έχει αντιταθεί ότι η ασφάλεια και η ιδιότητα του αναλλοίωτου που εγγυώνται οι αλγόριθμοι BFT δεν πρέπει να παραβλέπεται σε περιβάλλοντα χωρίς πλήρη εμπιστοσύνη. [8]



Εικόνα 2: Τα βήματα αποδοχής μιας συναλλαγής και ο ρόλος του αλγορίθμου συναίνεσης

1.3 Πλατφόρμες Blockchain

Για πληρέστερη κατανόηση του τοπίου των συστήματων Blockchain που χρησιμοποιούνται σήμερα και των δυνατοτήτων τους, θα εξετάσουμε τρεις χαρακτηριστικές πλατφόρμες και τα οικοσυστήματά τους.

1.3.1 Ethereum

Το Ethereum είναι permissionless σύστημα Blockchain. Χαρακτηρίζεται από το περιβάλλον εκτέλεσής του, Ethereum Virtual Machine (EVM), όπου εκτελούνται τα smart contracts, γραμμένα στην Turing-complete γλώσσα προγραμματισμού Solidity που δημιουργήθηκε για τις ανάγκες του Ethereum, από τον αλγόριθμο συναίνεσης Proof-of-Work που χρησιμοποιεί, καθώς και από το κρυπτονόμισμά του ονόματι Ether με το οποίο ανταμείβονται οι miners, γίνεται ανταλλαγή αξιών και εισπράττονται προμήθειες για συναλλαγές από τους συμμετέχοντες και τα smart contracts. [28]

Η ανοικτότητα του Ethereum και η δυνατότητα ανάπτυξης αποκεντρικοποιημένων εφαρμογών μέσω smart contracts, έχει επιτρέψει την υλοποίηση καινοτόμων ιδεών που αφορούν από αγορές τέχνης [29] μέχρι χρηματοοικονομικές λύσεις (decentralized finance, DeFi), π.χ. για δανεισμό [30], ή τη δημιουργία αποκεντρικοποιημένων εταιρειών (Decentralized Autonomous Organizations, DAOs). [28]

1.3.2 GoQuorum

Το GoQuorum αναπτύχθηκε κυρίως για χρήση σε χρηματοοικονομικές εφαρμογές από την J.P. Morgan και ύστερα από την ConsenSys, και είναι permissioned σύστημα Blockchain που έχει βασιστεί στον κώδικα του Ethereum. Διατηρεί τη δυνατότητα δημιουργίας και εκτέλεσης smart contracts γραμμένων σε Solidity, όπως και το Ethereum, ενώ αντικαθιστά τη χρήση του αλγόριθμου συναίνεσης PoW επιτρέποντας τη χρήση BFT (IBFT, Proof-of-Authority) ή CFT (Raft) αλγορίθμων.

Βασικό στοιχείο του GoQuorum είναι η δυνατότητα ιδιωτικότητας των δεδομένων. Κάθε κόμβος διατηρεί ένα δημόσιο και ένα ιδιωτικό ledger. Τα ιδιωτικά δεδομένα μπορούν να καθίστανται προσβάσιμα μόνο σε συγκεκριμένο υποσύνολο των κόμβων, ενώ ένα hash της αντίστοιχης

συναλλαγής προστίθεται στο δημόσιο ledger και είναι ορατό από όλους τους συμμετέχοντες ως απόδειξη ακεραιότητας. [13], [31], [32]

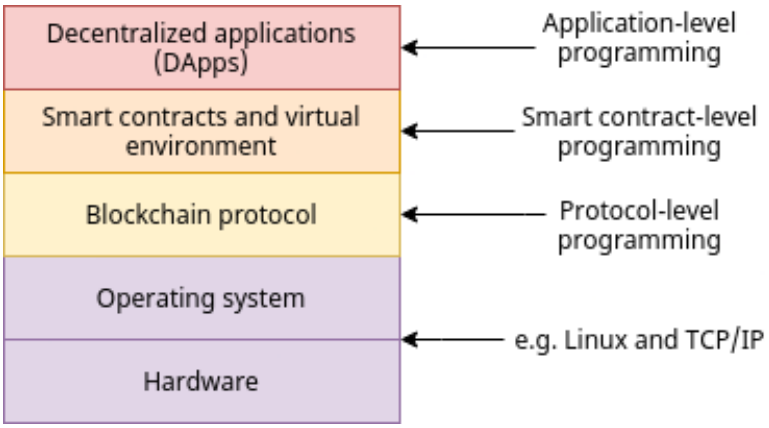
1.3.3 Hyperledger Fabric

Ανήκει στην οικογένεια projects ονόματι Hyperledger του Linux Foundation και αποτελεί permissioned σύστημα Blockchain γενικού σκοπού. Χρησιμοποιεί αλγόριθμο συναίνεσης CFT (Raft) και υποστηρίζει την ανάπτυξη smart contracts σε πολλαπλές γλώσσες προγραμματισμού (Go, JavaScript/Node.js, Java).

Στο Fabric μπορούν να υπάρχουν πολλαπλά κανάλια με διαφορετικούς συμμετέχοντες και διαφορετικά δικαιώματα ενώ εντός των καναλιών υπάρχει η δυνατότητα για ιδιωτικά δεδομένα ομοίως με το GoQuorum. Ακόμη, το Fabric επιτρέπει την προσαρμογή των στοιχείων του (π.χ. αντικατάσταση του μηχανισμού συναίνεσης με αλγόριθμο BFT) και δεν βασίζεται στην ύπαρξη νομίσματος. [33], [34]

1.4 Εφαρμογές Blockchain

Ο προγραμματισμός στα συστήματα Blockchain μπορεί να διαχωριστεί σε τρία επίπεδα: το επίπεδο πρωτοκόλλου (protocol-level programming), το επίπεδο smart contracts (smart contract-level programming) και το επίπεδο των εφαρμογών (application-level programming) [2]. Η δημιουργία λογισμικού που αλληλεπιδρά με το Blockchain βασίζεται στα δύο τελευταία επίπεδα.



Εικόνα 3: Μοντέλο των επιπέδων που απαρτίζουν ή αλληλεπιδρούν με ένα σύστημα Blockchain [2]

Οι εφαρμογές αυτού του τύπου ονομάζονται decentralized applications (DApps). Ένα DApp αλληλεπιδρά με το Blockchain μέσω smart contracts, ενώ μπορεί να διαθέτει διεπαφή χρήστη (frontend) που φιλοξενείται σε συμβατικά συστήματα ή σε υπηρεσίες αποκεντρικοποιημένης αποθήκευσης. Ακόμη μπορεί να επικοινωνεί με άλλα εξωτερικά συστήματα, όπως μια βάση δεδομένων ή τρίτες πηγές δεδομένων (π.χ. για ισοτιμίες νομισμάτων).

1.4.1 On-chain και off-chain διαδικασίες

Κρίσιμη έννοια στην ανάπτυξη και χρήση των DApps είναι η διάκριση μεταξύ των on-chain και off-chain διαδικασιών. Με τον όρο on-chain χαρακτηρίζουμε τα δεδομένα και τους υπολογισμούς που δημιουργούνται, εκτελούνται και αποθηκεύονται στο Blockchain με τη μορφή συναλλαγών, αποτελεσμάτων και συμβάντων (events) από smart contracts, ή με τη μορφή μεταδεδομένων. [2]

On-chain διαδικασίες δεν συναντούμε σε παραδοσιακά συστήματα λογισμικού, καθώς αποτελούν καινοτομία της τεχνολογίας Blockchain. Πέρα

από τα οφέλη που αντλεί από τις ιδιότητες του Blockchain, η χρήση on-chain διαδικασιών μειονεκτεί όσον αφορά την εκτέλεση απαιτητικών υπολογισμών ή την αποθήκευση μεγάλου όγκου δεδομένων, καθώς αυτές πρέπει να αναπαραχθούν στο σύνολο των κόμβων και να διατηρηθούν μόνιμα στο κάθε αντίγραφο του ledger. [2], [35]

Προκύπτει λοιπόν η ανάγκη για ανάπτυξη DApps που επικοινωνούν με εξωγενή συστήματα όπου η αποδοτική εκτέλεση υπολογισμών και η διατήρηση μεγάλων δεδομένων είναι πιο πρόσφορη. Ο Ramamurthy μάλιστα προκρίνει [2] την ελαχιστοποίηση των υπολογισμών και δεδομένων που λαμβάνουν χώρα on-chain ώστε να περιλαμβάνονται μόνο τα απολύτως απαραίτητα για την επιβολή των κανόνων επιχειρησιακής λογικής, των νομικών υποχρεώσεων, της ιχνηλάτησης των δεδομένων, της καταγραφής συμβάντων σε πραγματικό χρόνο και της καταγραφής και χρονοσήμανσης γεγονότων που συμβαίνουν εκτός Blockchain. Για τα off-chain δεδομένα μπορεί να παράγεται ένα hash από την τιμή τους που θα αποθηκεύεται on-chain ώστε να μπορεί να αποδειχθεί μελλοντικά η ιδιότητα του αναλλοίωτου. Τα μειονεκτήματα των off-chain διαδικασιών είναι η έλλειψη διαφάνειας, αποκεντρικοποίησης και εγγύησης διατήρησης των δεδομένων τους. [35]

1.4.2 Παραδείγματα off-chain συστημάτων

Παρουσιάζουμε παρακάτω κάποια χαρακτηριστικά εξωγενή συστήματα που χρησιμοποιούνται στα DApps.

IPFS: Κατανεμημένο σύστημα αρχείων για διαμοιρασμό περιεχομένου peer-to-peer σε ένα αποκεντρικοποιημένο δίκτυο. Η αναφορά σε κάθε αρχείο δεν γίνεται βάσει κάποιου ονόματος, αλλά με το hash από το ίδιο το περιεχόμενό του (content-addressable). Η χρήστρια μεταφορτώνει ένα αρχείο μέσω του δικού της κόμβου IPFS, που διαιρείται σε τμήματα των οποίων τα hash σχηματίζουν ένα Merkle DAG με ρίζα το hash του συνολικού αρχείου, ώστε να μπορεί να αποδειχθεί η ακεραιότητα, και στη συνέχεια κατανέμονται στο δίκτυο για μέγιστη διαθεσιμότητα. Από σχεδιασμού το περιεχόμενο των αρχείων είναι δημόσιο, οπότε αν υπάρχουν απαιτήσεις ιδιωτικότητας θα πρέπει να γίνεται κρυπτογράφηση πριν την ανάρτηση ενός αρχείου [36], [37]. Παρόμοια συστήματα με το IPFS είναι μεταξύ άλλων και τα Storj [38], Filecoin [39], Ethereum Swarm [40].

BigChainDB: Σύστημα για αποκεντρικοποιημένες βάσεις δεδομένων τύπου NoSQL document store. Λειτουργεί συμπληρωματικά με συστήματα αποθήκευσης αρχείων, όπως το IPFS, ώστε να επιτρέπει την αποθήκευση και εκτέλεση ερωτημάτων σε δομημένα δεδομένα. Ακόμη, διαθέτει κοινές ιδιότητες με το Blockchain όπως η αποκεντρικοποίηση, η χρήση αλγορίθμων συναίνεσης, η ακεραιότητα και η υποστήριξη νομισμάτων. [41], [42]

Golem: Το Golem συστήνεται ως ο πρώτος αποκεντρικοποιημένος υπερυπολογιστής. Οι χρήστες συμμετέχουν σε ένα peer-to-peer δίκτυο όπου μπορούν είτε να ζητήσουν και να ενοικιάσουν υπολογιστικούς πόρους από άλλους χρήστες, είτε να προσφέρουν τους δικούς τους προς ενοικίαση. Ακόμη, μπορούν να χρησιμοποιούν και να διαθέτουν λογισμικό που εκτελεί υπολογισμούς στους πόρους του Golem με τη μορφή microservices [43]. Παρόμοια συστήματα με το Golem είναι μεταξύ άλλων και τα iExec [44] και Truebit [45].

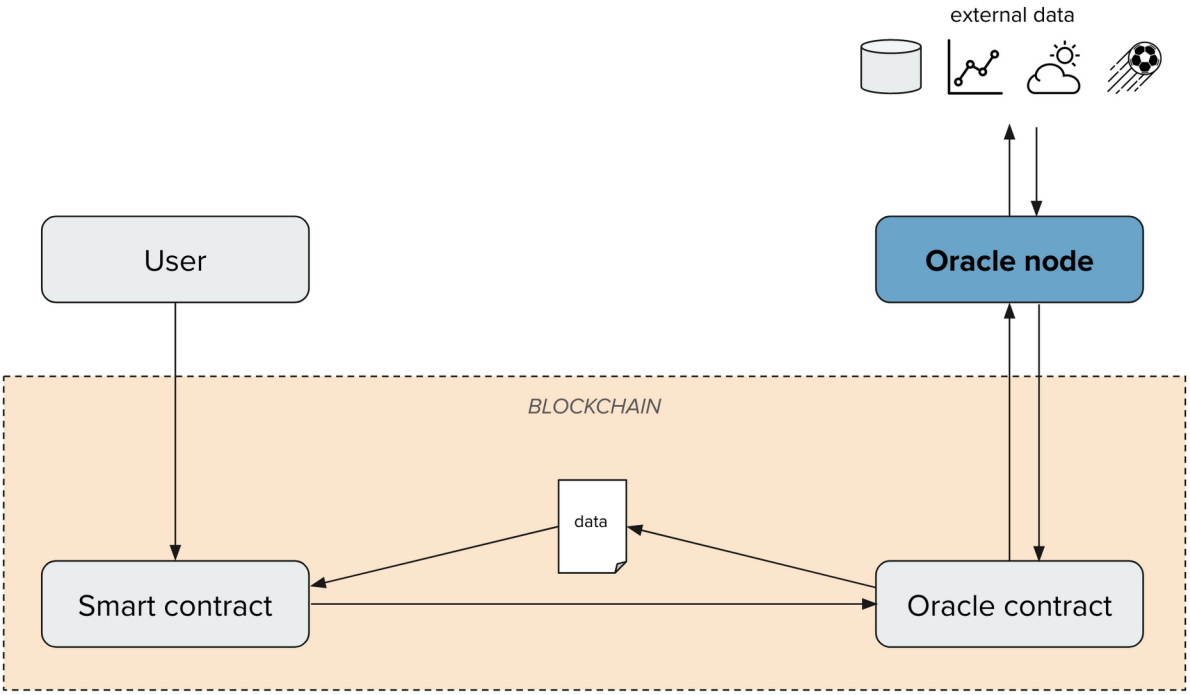
Φυσικά, δεν αποκλείεται η χρήση “συμβατικών” συστημάτων, όπως το Amazon S3 ή το BitTorrent για διαμοιρασμό αρχείων, η PostgreSQL για βάσεις δεδομένων κτλ.

1.4.3 Διασύνδεση με off-chain συστήματα

Η απομονωμένη αρχιτεκτονική των πλατφορμών Blockchain δεν τις επιτρέπει την άμεση λήψη ή αποστολή δεδομένων από και προς τον εξωτερικό κόσμο. Ωστόσο οι περισσότερες ευκαιρίες για εφαρμογή της τεχνολογίας του Blockchain είναι συνυφασμένες με την απαίτηση για διασύνδεση με εξωγενή συστήματα (off-chain).

Το ζήτημα αυτό έχει ονομαστεί “το πρόβλημα του μαντείου” (oracle problem), από τον όρο “μαντείο” (oracle) που χρησιμοποιείται για να περιγράψει ένα είδος λύσης που εφαρμόζεται για να επιτευχθεί η ανωτέρω διασύνδεση.

Τα oracles είναι τρίτες υπηρεσίες που συμμετέχουν ως κόμβοι στο σύστημα Blockchain και έτσι μεσολαβούν για να μεταβιβάσουν δεδομένα από και προς τον εξωτερικό κόσμο. Συγκεκριμένα, παρακολουθούν τις συναλλαγές του Blockchain και όταν υπάρξει κάποιο αίτημα δεδομένου, το ανακτούν από την πηγή του, το επεξεργάζονται και το καταχωρούν στο Blockchain, ενδεχομένως μαζί με μία απόδειξη για την εγκυρότητά του. [46]



Εικόνα 4: Οι αλληλεπιδράσεις ενός oracle με το σύστημα Blockchain και τον εξωτερικό κόσμο. [47]

Διακρίνονται ποικίλα είδη oracles, ανάλογα με την πηγή των δεδομένων (λογισμικό, υλικό ή άνθρωπος), την κατεύθυνση (από ή προς το Blockchain) και το μοντέλο εμπιστοσύνης (κεντρικοποιημένη ή αποκεντρικοποιημένη δομή).

Πηγές μπορεί να είναι μία ιστοσελίδα (π.χ. το Reuters.com για την τιμή ενός αγαθού), ένας αισθητήρας (π.χ. για τη θερμοκρασία στο ψυγείο μιας εφοδιαστικής αλυσίδας) ή ένας άνθρωπος για καταχώρηση πιο εξειδικευμένων δεδομένων (π.χ. έλεγχος γνησιότητας φωτογραφίας). [47]

Η χρήση oracles εισάγει πολλαπλά ρίσκα εμπιστοσύνης υποβαθμίζοντας δυνητικά την αξία της υιοθέτησης του Blockchain.

Τρόποι άμβλυνσης μπορούν να εντοπιστούν σε τρία επίπεδα· το επίπεδο ανάκτησης δεδομένων, το επίπεδο του περιβάλλοντος εκτέλεσης και το επίπεδο αποδοχής στο Blockchain.

Ανάκτηση δεδομένων: Η πηγή δεδομένων μπορεί να εισάγει ρίσκα που αφορούν από τη διαθεσιμότητα των δεδομένων, αν π.χ. η υπηρεσία πάψει να λειτουργεί, έως την κακόβουλη παραποίησή τους από την πηγή με σκοπό την επιρροή στο σύστημα Blockchain. Αυτό μπορεί να βελτιωθεί με τη

χρήση έμπιστων και ανεξάρτητων πηγών που πιθανολογείται ότι δεν έχουν συμφέρον από την κακόβουλη παραποίηση, καθώς και με τη χρήση πολλαπλών πηγών (π.χ. υπολογισμός τιμής μετοχής με χρήση median από 5 ανεξάρτητους παρόχους).

Περιβάλλον εκτέλεσης: Όταν η ανάκτηση και επεξεργασία των δεδομένων γίνεται από λογισμικό, τίθενται ζητήματα εμπιστοσύνης του λογισμικού καθώς μπορεί να μεταβληθεί ο κώδικας ή η μνήμη που χρησιμοποιεί χωρίς να γνωστοποιείται αυτό απαραίτητα στον εξωτερικό κόσμο. Για αυτόν τον σκοπό έχει παρουσιάσει αυξημένο ενδιαφέρον η χρήση των Trusted Execution Environments (TEE) στα συστήματα Blockchain. Τα TEEs, όπως το Intel SGX, λειτουργούν σε επίπεδο hardware του επεξεργαστή και παρέχουν τη δυνατότητα για απομονωμένη εκτέλεση κώδικα με δεδομένα σε ασφαλή μνήμη, για χρήση έμπιστων συναρτήσεων (π.χ. παραγωγή τυχαίων αριθμών, χρονοσήμανση), καθώς και για απομακρυσμένη επαλήθευση της ακεραιότητας του περιβάλλοντος εκτέλεσης (remote attestation). Περιορισμοί των TEEs είναι η χαμηλή χωρητικότητα μνήμης, η πιθανότητα διακοπής λειτουργίας από τον διαχειριστή τους και η ευαλωτότητα σε replay attacks, side-channel attacks και single-point-of-failure attacks. [48]

Αποδοχή στο Blockchain: Τα ρίσκα εμπιστοσύνης στα oracles μπορούν να περιοριστούν εάν εφαρμοστεί μία αποκεντρικοποιημένη αρχιτεκτονική όπου χρησιμοποιούνται πολλαπλά oracles για το ίδιο δεδομένο. Έτσι, η τελική τιμή του μπορεί να προκύπτει εντός Blockchain από έναν καθορισμένο αλγόριθμο συμφωνίας (π.χ. median ή κανόνας πλειοψηφίας). [47]

Αξιοσημείωτες υπηρεσίες για δημιουργία και φιλοξενία oracles είναι η Provable (πρώην Oraclize) [49] και η ChainLink [50].

2 Blockchain-oriented software engineering

Στο παρόν κεφάλαιο παρουσιάζουμε το θεωρητικό υπόβαθρο και τις τρέχουσες εξελίξεις σχετικά με την τεχνολογία λογισμικού, την ανάγκη εξειδίκευσης των περιοχών γνώσης της για την περίπτωση των λογισμικών που συνιστούν ή αλληλεπιδρούν με συστήματα Blockchain, απ' όπου ανακύπτει ο όρος "Blockchain-Oriented Software Engineering" (BOSE), καθώς και τις προτάσεις προσαρμογής των προτύπων μοντελοποίησης λογισμικού και διαδικασιών, όπως εμφανίζονται στη βιβλιογραφία.

2.1 Ορισμός

Η τεχνολογία λογισμικού (software engineering) ασχολείται με την εφαρμογή μιας συστηματικής, πειθαρχημένης, μετρήσιμης προσέγγισης στην ανάπτυξη, λειτουργία και συντήρηση του λογισμικού, δηλαδή την εφαρμογή των αρχών της μηχανικής στο λογισμικό. [51]

Η συνεχής επέκταση του λογισμικού σε κάθε πτυχή της οικονομικής και κοινωνικής ζωής, από την πιο απλή αριθμομηχανή μέχρι τη λειτουργία κρίσιμων συστημάτων, και κυρίως η αυξανόμενη πολυπλοκότητα και διασυνδεσιμότητα των εφαρμογών λογισμικού, δημιουργούν την απαίτηση αυτής της δομημένης προσέγγισης σε κάθε στάδιο ανάπτυξης του λογισμικού.

Ο οδηγός SWEBOK v3 (Software Engineering Body of Knowledge) του οργανισμού IEEE [51] εντοπίζει 15 περιοχές γνώσης (Knowledge Areas) που συγκροτούν την τεχνολογία λογισμικού (Πίνακας 1).

Στο πλαίσιο της εν λόγω κατηγοριοποίησης, οι Porru et al. (2017) [52] επιχείρησαν να αναλύσουν τις προκλήσεις στην ανάπτυξη λογισμικού το οποίο αλληλεπιδρά με τεχνολογίες Blockchain, και να εντοπίσουν ευκαιρίες για μελλοντική έρευνα και πειραματισμό.

Στη μελέτη, ορίζουν τα λογισμικά τέτοιου τύπου ως *Blockchain-oriented software* (BOS), ενώ ακόμη επινοούν τον όρο *Blockchain-oriented software engineering* (BOSE) για να περιγράψουν την εξειδίκευση της τεχνολογίας λογισμικού και των περιοχών γνώσης και πρακτικών της, πάνω στα συστήματα Blockchain.

Software Requirements (Απαιτήσεις)	**Software Design** (Σχεδιασμός)	**Software Construction** (Κατασκευή)
Software Testing (Έλεγχος)	**Software Maintenance** (Συντήρηση)	**Software Configuration Management** (Διαχείριση παραμετροποίησης)
Software Engineering Management (Διοίκηση)	**Software Engineering Process** (Διαδικασία)	**Software Engineering Models and Methods** (Μοντελοποίηση και μεθοδολογία)
Software Quality (Έλεγχος ποιότητας)	**Software Engineering Professional Practice** (Επαγγελματική πρακτική)	**Software Engineering Economics** (Οικονομικά)
Computing Foundations (Θεμέλια της επιστήμης υπολογιστών)	**Mathematical Foundations** (Μαθηματικά θεμέλια)	**Engineering Foundations** (Θεμέλια της μηχανικής)

Πίνακας 1: Οι περιοχές γνώσης της τεχνολογίας λογισμικού σύμφωνα με το SWEBOK v3

Η διάκριση μεταξύ της "κλασικής" τεχνολογίας λογισμικού και του Blockchain-oriented software engineering ανακύπτει από τα καινοτόμα χαρακτηριστικά του Blockchain ως δομή δεδομένων και την ανάγκη εφαρμογής ειδικών πρακτικών, για παράδειγμα στον σχεδιασμό, την κατασκευή, τον έλεγχο, τη μοντελοποίηση ή τη διοίκηση τέτοιων συστημάτων.

Όπως περιγράψαμε στο Κεφάλαιο 1, η τεχνολογία του Blockchain θεωρείται ότι θα έχει ανατρεπτική επίδραση στον ψηφιακό κόσμο, αντίστοιχη με αυτή του web, των κινητών συσκευών, ή του αναπτυσσόμενου ακόμη Internet of Things. Μάλιστα, οι συγγραφείς της μελέτης εκτιμούν ότι το Blockchain παρουσιάζει πιο δύσκολες προκλήσεις από άποψη τεχνολογίας λογισμικού σε σχέση με το λογισμικό για κινητές συσκευές, καθώς σε αντίθεση με το τελευταίο, η ανάγκη που κινεί την ανάπτυξη λογισμικού Blockchain είναι πρωτίστως επιχειρηματική και επομένως συνοδεύεται από επιτακτικές απαιτήσεις ασφαλείας και εξειδικευμένων διαδικασιών.

Στη μελέτη προσεγγίζονται λοιπόν οι εξής θεματικές.

Νέοι επαγγελματικοί ρόλοι: Πέραν των προγραμματιστριών Blockchain, οι συγγραφείς εκτιμούν ότι άτομα με εμπειρία στα χρηματοοικονομικά, τα νομικά και την τεχνολογία θα ήταν απαραίτητα στον τομέα και προτείνουν ως παράδειγμα νέου ρόλου τον μεσολαβητή μεταξύ επιχειρήσεων χαμηλής τεχνολογικής εξοικείωσης και επαγγελματιών της πληροφορικής για την υλοποίηση έργων Blockchain.

Ασφάλεια και αξιοπιστία: Το Blockchain γεννά νέες απαιτήσεις ασφαλείας που αφορούν την εμπιστοσύνη του λογισμικού και των συμμετεχόντων στο δίκτυο. Οι συγγραφείς προτείνουν τακτικές αξιολογήσεις του λογισμικού, ενδεχομένως μαθηματικές αναλύσεις για την απόδειξη των επιθυμητών ιδιοτήτων, καθώς και αυτοματοποιημένο έλεγχο (testing) στο λογισμικό, για παράδειγμα στα smart contracts ή στο σύστημα συναλλαγών.

Αρχιτεκτονική λογισμικού: Εξετάζεται ο ορισμός ειδικών design notations (σημειογραφίες σχεδιασμού), αρχιτεκτονικών μοτίβων ή μοντελοποιήσεων. Προτείνεται η χρήση κριτηρίων για την επιλογή της εκάστοτε υλοποίησης Blockchain ή κάποιου sidechain.

Γλώσσες μοντελοποίησης: Προτείνεται η προσαρμογή ή επέκταση υπάρχοντων προτύπων μοντελοποίησης, όπως η γλώσσα UML, ώστε να αναπαριστούν αποτελεσματικά τις έννοιες και διαδικασίες του Blockchain.

Μετρικές: Οι συγγραφείς εντοπίζουν μετρικές που αφορούν την αποκεντροποιημένη φύση του Blockchain, όπως η πολυπλοκότητα, η "χωρητικότητα" επικοινωνίας, η κατανάλωση πόρων και η απόδοση. Ακόμη προτείνουν την εύρεση νέων μετρικών με χρήση της μεθόδου Goal/Question/Metric (GQM) που ενδεχομένως να αναπαριστούν αποτελεσματικότερα τις εξεταζόμενες διαδικασίες.

Θεματική	Πιο σχετικές περιοχές γνώσης SWEBOK
Νέοι επαγγελματικοί ρόλοι	Software Engineering Professional Practice
Ασφάλεια και αξιοπιστία	Software Design, Software Testing
Αρχιτεκτονική λογισμικού	Software Design
Γλώσσες μοντελοποίησης	Software Engineering Models & Methods
Μετρικές	Software Requirements, Software Quality

Πίνακας 2: Αντιστοίχιση των θεματικών BOSE στις περιοχές γνώσης του SWEBOK v3

2.2 Μοντελοποίηση κλασικού λογισμικού

Προκειμένου να αναπτυχθεί ένα λογισμικό, χρειάζεται προηγουμένως ο καθορισμός των απαιτήσεων, η σταθερή επικοινωνία με τα ενδιαφερόμενα μέρη (stakeholders) για την ανανέωση και επέκταση των απαιτήσεων και για τη συμμετοχή στη λήψη αποφάσεων σχετικά με το τελικό προϊόν. Στόχος είναι η κοινή κατανόηση της δομής και της λειτουργίας του λογισμικού, και των αποφάσεων που οδήγησαν σε αυτές.

Έτσι, δημιουργείται η ανάγκη για μια κοινή γλώσσα που να περιγράφει τα παραπάνω χαρακτηριστικά, με τρόπο αφενός αφαιρετικό ώστε να είναι ανεξάρτητη από λεπτομέρειες των αρχιτεκτονικών επιλογών ή της υλοποίησης, αφετέρου περιεκτικό ώστε να επικοινωνεί επαρκώς τα κύρια στοιχεία του συστήματος.

Τέτοιες γλώσσες συναντώνται με τη μορφή διαγραμμάτων και οπτικών αναπαραστάσεων, και εμπίπτουν στην περιοχή γνώσης Software Engineering Models & Methods του SWEBOK, δηλαδή στη μοντελοποίηση. Στο παρόν κεφάλαιο θα εξετάσουμε τις μοντελοποιήσεις UML και BPMN, που θα φανούν χρήσιμες και στη συνέχεια της εργασίας.

2.2.1 Μοντελοποίηση UML

Η Unified Modeling Language (UML) είναι ένα πρότυπο γενικού σκοπού για την προδιαγραφή, την περιγραφή, τον σχεδιασμό, την οπτικοποίηση και την τεκμηρίωση συστημάτων λογισμικού. Ορίζει 13 διαγράμματα που ταξινομούνται σε δύο ευρείες κατηγορίες, τα διαγράμματα δομής και τα διαγράμματα συμπεριφοράς.

Στα πλαίσια της εργασίας θα συναντήσουμε το UML Class Diagram (διάγραμμα κλάσης), το UML Deployment Diagram (διάγραμμα παράταξης) και το UML Sequence Diagram (διάγραμμα ακολουθίας).

Class Diagram: Παραπέμπει στις έννοιες του αντικειμενοστρεφούς προγραμματισμού. Αποτυπώνει τον σχεδιασμό μίας οντότητας τύπου κλάσης, τη δομή, τις μεταβλητές και τις σχέσεις της με άλλες κλάσεις.

Deployment Diagram: Αναπαριστά την αρχιτεκτονική ενός συστήματος και τη φυσική τοποθεσία εγκατάστασης κάθε συστατικού του.

Sequence Diagram: Αποτυπώνει τις αλληλεπιδράσεις μεταξύ διαφορετικών συστατικών ενός συστήματος με τη μορφή μηνυμάτων που ανταλλάσσουν σύγχρονα ή ασύγχρονα. [53]

Ακόμη, αξίζει να σημειώσουμε τον μηχανισμό των στερεοτύπων (stereotypes) μέσω των οποίων οι σχεδιάστριες UML μπορούν να επεκτείνουν το πρότυπο για να αναπαραστήσουν έναν τύπο οντότητας ειδικού σκοπού που αφορά το σύστημα λογισμικού υπό εξέταση. Τα stereotypes σημειώνονται με εισαγωγικά (π.χ. «χρήστης web app»).

2.2.2 Μοντελοποίηση BPMN

Το Business Process Model and Notation (BPMN) αποτελεί ένα πρότυπο για τη γραφική αναπαράσταση επιχειρησιακών διαδικασιών. Αποτυπώνει δηλαδή με καθορισμένη σημειολογία τις δραστηριότητες, τη ροή πληροφορίας και τη λογική των αποφάσεων στις διάφορες διαδικασίες ενός συστήματος, με οπτικό διαχωρισμό ανάλογα με το εμπλεκόμενο άτομο ή τμήμα. [54]

2.3 Μοντελοποίηση λογισμικού BOS

Όπως σημειώνουν οι Porru et al. [52], η υιοθέτηση του BOS (Blockchain–oriented software) πιθανότατα δημιουργεί την απαίτηση για εξειδικευμένα γραφικά μοντέλα αναπαράστασής τους.

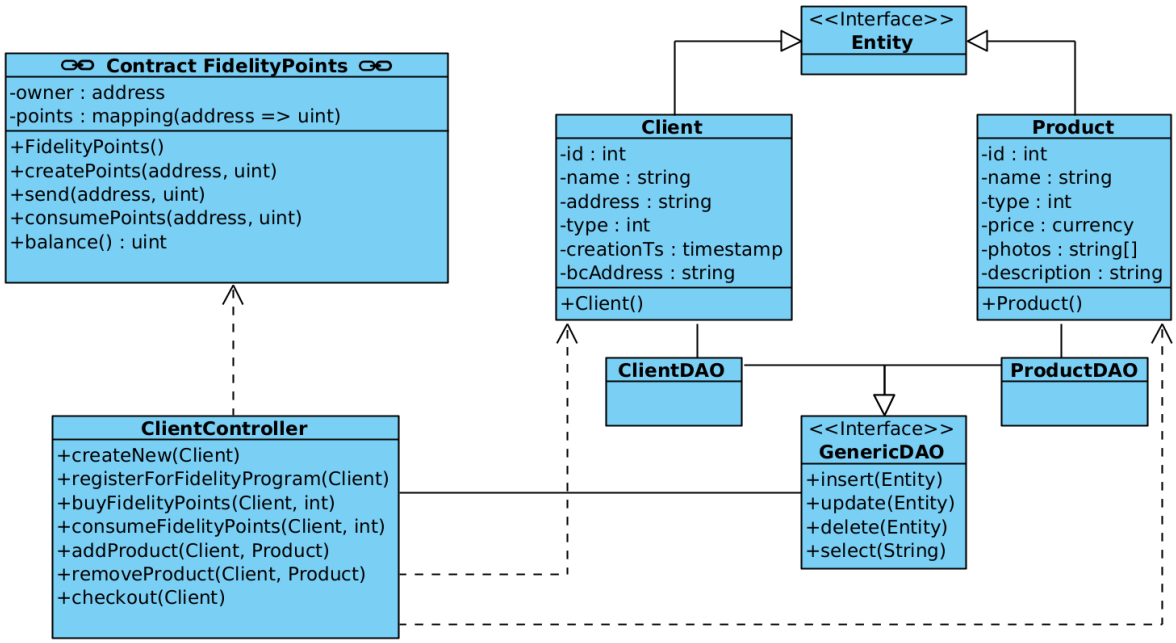
Εξετάζουν ενδεικτικά το ενδεχόμενο τροποποίησης ή επαναδημιουργίας των διαγραμμάτων UML για την προσαρμογή στις ιδιαιτερότητες του BOS, ενώ εκτιμούν ότι τα διαγράμματα Use Case, Activity και State είναι δύσκολο να αναπαραστήσουν, ως έχουν, το περιβάλλον των τεχνολογιών Blockchain και επομένως χρειάζονται προσαρμογή.

Στην κατεύθυνση αυτή, οι Rocha and Ducasse (2018) [55] συμφωνούν στην ανάγκη για ειδική σημειογραφία ώστε να διευκολύνεται η υιοθέτηση ή η μεταστροφή προς το BOS, καθώς διαφορετικά θα είναι αδύνατο να καθοριστεί σαφώς η διάδραση μεταξύ του Blockchain και της εκάστοτε εφαρμογής. Για τον σκοπό αυτό, προτείνουν επεκτάσεις σε τρεις

μοντελοποιήσεις – στο Entity Relationship Model, στο Class Diagram της UML και στο BPMN, χρησιμοποιώντας ως παράδειγμα μια εφαρμογή που εκτελείται σε περιβάλλον Ethereum και αφορά σύστημα ανταλλαγής πόντων.

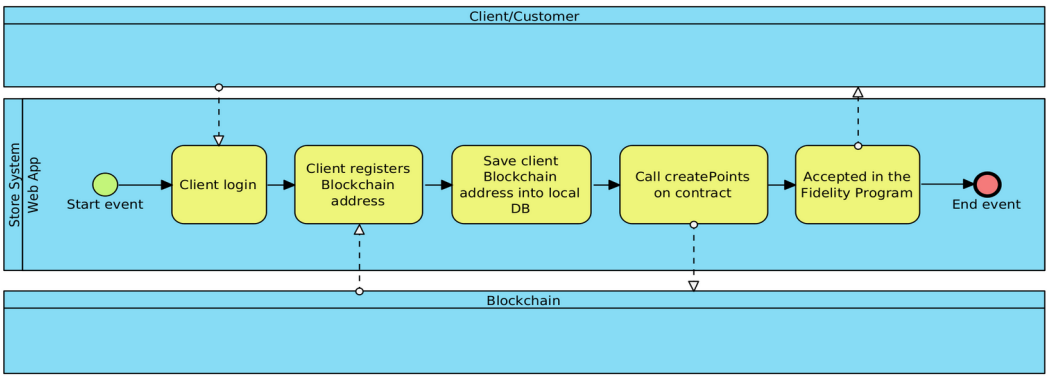
Συγκεκριμένα, χρησιμοποιούν τη μοντελοποίηση του Class Diagram για να αναπαραστήσουν ένα smart contract. Ένα smart contract μοιάζει με τις κλάσεις του αντικειμενοστρεφούς προγραμματισμού ως προς την ύπαρξη συναρτήσεων και πεδίων δεδομένων και έτσι, όπως παρατηρούν οι συγγραφείς, μπορεί εύκολα να αναπαρασταθεί με διαγράμματα δομής της UML, με μικρές προσαρμογές.

Στην Εικόνα 5, βλέπουμε πάνω αριστερά την αναπαράσταση του smart contract που ορίζει τους κανόνες δημιουργίας, ανταλλαγής και σπατάλης των πόντων με όνομα `FidelityPoints`. Οι μοναδικές διαφορές από μία συμβατική κλάση είναι αφενός η χρήση των τύπων δεδομένων του Ethereum (address, mapping κτλ.) και αφετέρου η σήμανση “Contract” και το εικονίδιο της αλυσίδας στην ετικέτα, ώστε να είναι διακριτό ότι πρόκειται για smart contract. Η αναπαράσταση είναι επαρκής για να κατανοήσουμε τα κύρια στοιχεία της δομής του smart contract, δηλαδή το όνομα, τις συναρτήσεις και τα πεδία δεδομένων του, καθώς και τον τρόπο που αλληλεπιδρά με τις υπόλοιπες κλάσεις.



Εικόνα 5: UML Class Diagram για την εφαρμογή ανταλλαγής πόντων των Rocha and Ducasse [55]

Όσον αφορά την επέκταση των συγγραφέων στο BPMN, αυτή έγκειται στην προσθήκη ενός *swimlane* που αντιστοιχεί στο Blockchain. Εκεί συνδέονται όσες δραστηριότητες περιλαμβάνουν ανταλλαγή δεδομένων με το Blockchain, ώστε να επικοινωνηθεί αυτό στη χρήστρια του διαγράμματος.



Εικόνα 6: BPMN για τη διαδικασία εγγραφής χρήστριας στην εφαρμογή ανταλλαγής πόντων των Rocha and Ducasse [55]

Στο παράδειγμα (Εικόνα 6), βλέπουμε δύο βέλη που αλληλεπιδρούν με το swimlane του Blockchain. Το πρώτο αναπαριστά ότι η χρήστρια της εφαρμογής λαμβάνει τη διεύθυνσή της από το Blockchain και έπειτα την καταχωρεί στο web app του καταστήματος. Το δεύτερο αναπαριστά την

κλήση εκ μέρους του καταστήματος στο smart contract ώστε να δημιουργηθούν πόντοι ανταλλαγής στον λογαριασμό της χρήστριας.

Ακόμη, προτείνουν τη σήμανση δραστηριοτήτων που αφορούν τη λειτουργία του Blockchain (πχ. την επικύρωση μιας συναλλαγής) με τη χρήση του εικονιδίου αλυσίδας.

Πέρα από τους Rocha and Ducasse, παρόμοιες προτάσεις έχουν διατυπώσει οι Marchesi et al. (2018) [56]. Στην εργασία τους παρατηρούν ότι το πεδίο της ανάπτυξης BOS είναι ακόμη σε πρώιμο στάδιο, ότι συχνά χαρακτηρίζεται από βεβιασμένες και άναρχες πρακτικές, και πως η υιοθέτηση σταθερών πρακτικών μπορεί να παρέχει τα οφέλη της δομημένης αρχιτεκτονικής σχεδίασης, ασφάλειας, δοκιμής και ποιότητας λογισμικού που υπάρχουν στην παραδοσιακή τεχνολογία λογισμικού.

Συμφωνούν στην αναπαράσταση των smart contracts μέσω UML Class Diagrams, ενώ ακόμη προτείνουν τη χρήση του UML State Diagram για τις μεταβολές στο state των δεδομένων ενός smart contract και τη χρήση UML Sequence Diagrams για τις ανταλλαγές μηνυμάτων (πχ. κλήση συνάρτησης, ενεργοποίηση event ή μεταφορά αξίας) μεταξύ διαφορετικών smart contracts.

Ορισμένα από τα stereotypes που μας αφορούν και με τα οποία επεκτείνουν το UML Class Diagram και το UML Sequence Diagram, φαίνονται στον παρακάτω πίνακα.

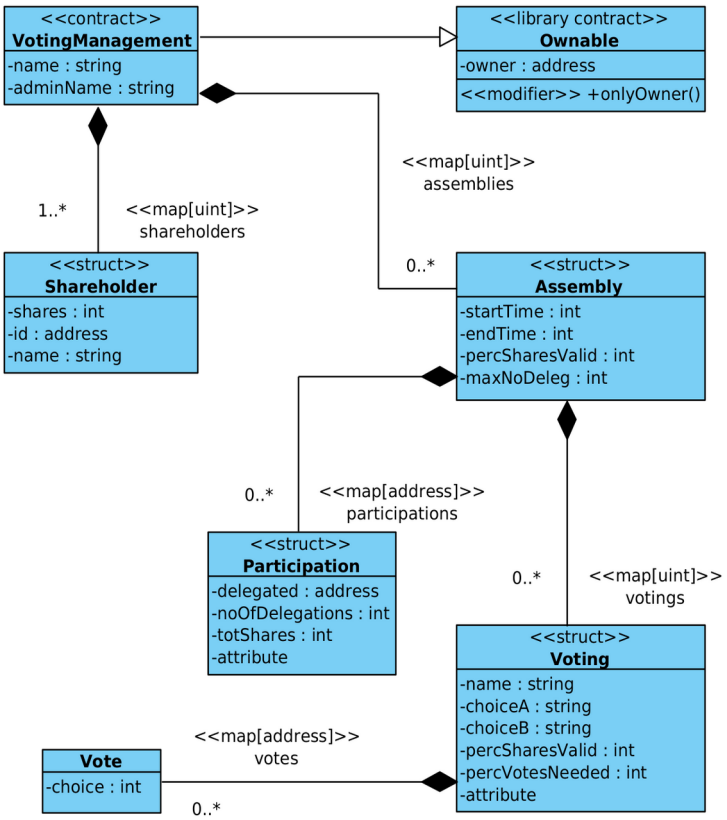
Stereotype	Περιγραφή
«contract»	Δηλώνει ένα smart contract.
«library contract»	Ένα smart contract που προέρχεται από κάποια βιβλιοθήκη (ενδεχομένως standard library).
«struct»	Δομή που περιέχει δεδομένα, χωρίς συναρτήσεις. Ορίζεται και χρησιμοποιείται στη δομή δεδομένων ενός smart contract.
«interface»	Ένα contract που περιέχει μόνο τις δηλώσεις των συναρτήσεων (δηλ. χωρίς υλοποίηση).

Πίνακας 3: Προσθήκες Marchesi et al. στο UML Class Diagram ως stereotypes [56]

Stereotype	Περιγραφή
«person»	Ρόλος ανθρώπου που αποστέλλει μηνύματα μέσω wallet ή άλλης εφαρμογής
«system»	Εξωτερικό σύστημα που μπορεί να στείλει μηνύματα στο Blockchain
«device»	Συσκευή (συνήθως IoT) που μπορεί να στείλει μηνύματα
«contract»	Ένα smart contract, εξωτερικό ή μέρος του συστήματος
«oracle»	Ειδικό smart contract που αλληλεπιδρά έμπιστα με τον εξωτερικό κόσμο (βλ. Κεφάλαιο 1)

Πίνακας 4: Προσθήκες Marchesi et al. στο UML Sequence Diagram [56]

Χρησιμοποιούν ως παράδειγμα μια εφαρμογή Ethereum για απομακρυσμένη ψηφοφορία σε εταιρικές συνελεύσεις, την οποία αναλύουν σε δύο συνιστώσες: το σύστημα Blockchain που αποτελείται από τα smart contracts της εφαρμογής, και το εξωτερικό σύστημα που αλληλεπιδρά με το σύστημα Blockchain προκειμένου να δημιουργήσει συναλλαγές και να λάβει δεδομένα. Για την ανάλυση αυτή ακολουθούν τυποποιημένη διαδικασία, την οποία προτείνουν ως μέρος μεθοδολογίας σχεδίασης BOS.



Εικόνα 7: UML Class Diagram για την εφαρμογή ψηφοφορίας σε εταιρικές συνελεύσεις των Marchesi et al. [56]

Στο ανωτέρω διάγραμμα βλέπουμε το UML Class Diagram με τα ειδικά stereotypes που περιγράφει τη δομή της εφαρμογής–παράδειγμα. Το κύριο στοιχείο είναι το smart contract `VotingManagement` που κληρονομεί από το library contract `Ownable` και διαθέτει λίστες με τους μετόχους (shareholders) και τις συνελεύσεις (assemblies), τα οποία αναπαρίστανται ως structs. Όπως ορίζεται και στον πίνακα επεκτάσεων, το smart contract επισημαίνεται με το stereotype «contract».

Συγκρίνοντας τις προσεγγίσεις των Marchesi et al. και των Rocha and Ducasse, παρατηρούμε ότι οι πρώτοι ακολουθούν την περισσότερο συμβατή με τις προδιαγραφές της UML έννοια του stereotype, ενώ οι τελευταίοι εισάγουν δική τους σημειογραφία και εικονίδιο. Κατά τα λοιπά, οι προσεγγίσεις ακολουθούν την ίδια λογική και δεν εμφανίζουν ουσιώδεις διαφορές ως προς την αναπαράσταση δομής της εφαρμογής μέσω UML Class Diagram.

Οι δύο δημοσιεύσεις συνεισφέρουν σημαντικά στη θεμελίωση τεχνικών μοντελοποίησης συστημάτων Blockchain, όπως το διάγραμμα δομής, και στην παρακίνηση για ανάπτυξη περισσότερων, με τις οποίες μπορεί να εδραιωθεί καλύτερα η κοινή κατανόηση των ενδιαφερόμενων μερών μιας τέτοιας εφαρμογής.

ΜΕΡΟΣ Β: ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ: ΕΦΑΡΜΟΓΕΣ ΚΡΙΣΙΜΗΣ ΑΠΟΣΤΟΛΗΣ – ΑΕΡΟΔΙΑΚΟΜΙΔΗ

3 Υπάρχον σύστημα

3.1 Γενικά για συστήματα κρίσιμης αποστολής

Η διαχείριση κρίσιμων αποστολών συνιστά τη διαδικασία λήψης αποφάσεων για την αντιμετώπιση μιας έκτακτης κατάστασης με στόχο την ελαχιστοποίηση των ανθρώπινων απωλειών, των καταστροφών στο περιβάλλον ή σε υποδομές, και της αποδιοργάνωσης της κοινωνικής και οικονομικής ζωής. [57]

Τα συστήματα κρίσιμης αποστολής παρουσιάζουν ορισμένες ιδιαιτερότητες με σημαντικό ενδιαφέρον για το πλαίσιο της εργασίας μας.

- Η διαχείριση κρίσιμων καταστάσεων εμπλέκει πολλούς διαφορετικούς φορείς που πρέπει να μοιράζονται την ίδια πληροφορία.

- Τα δεδομένα αυτά παράγονται σε διαφορετικούς μορφότυπους και από πολλές διαφορετικές πηγές–προορισμούς που έχουν την ευθύνη τους.

- Τα δεδομένα αυτά μπορεί να έχουν απαγορευτικό μέγεθος καθώς μπορεί να περιλαμβάνουν σαρωμένα έγγραφα, οπτικοακουστικό υλικό, μετεωρολογικά δεδομένα κτλ.

- Η κρισιμότητα της χρονοσήμανσης είναι σε υπερθετικό βαθμό, καθώς πρέπει να μπορεί να αποδειχθεί και να μην μπορεί να αλλοιωθεί η σειρά επικοινωνιών και γεγονότων.

- Η ετερογένεια των εμπλεκόμενων συστημάτων παραγωγής και διαχείρισης τέτοιων δεδομένων, καθώς και η πλήρης κλειστότητα τέτοιων πληροφοριακών είναι απολύτως ανελαστικά χαρακτηριστικά, δηλαδή δεν επιτρέπεται κανενός είδους τροποποίηση ή πρόσβαση σε τέτοια συστήματα, από οποιονδήποτε πλην του ιδιοκτήτη τους.

3.2 Περιγραφή συστήματος αεροδιακομιδής

Αεροδιακομιδή ονομάζεται η μεταφορά ασθενών που χρειάζονται άμεση φροντίδα, σε μία υγειονομική μονάδα με εναέρια μέσα. Οι ασθενείς τίθενται υπό ιατρικό έλεγχο και παρακολούθηση από συνοδευόμενο ιατρό. Αιτία μπορεί να είναι η τέλεση κάποιου ατυχήματος σε δυσπρόσιτη τοποθεσία, η ανάγκη διάσωσης ή εκκένωσης από μία περιοχή κινδύνου, ενώ συχνά παρατηρείται η ανάγκη, και στην Ελλάδα, για μεταφορά ασθενών από ακριτικές περιοχές όπου δεν υπάρχει η δυνατότητα έγκαιρης πρωτοβάθμιας περίθαλψης σε σοβαρά περιστατικά.

Για τις ανάγκες της εργασίας θα προσεγγίσουμε τη διαδικασία της αεροδιακομιδής στην Ελλάδα. Ορισμένες παραδοχές ενδέχεται να μην ανταποκρίνονται στο πραγματικό σύστημα αεροδιακομιδής και γίνονται για λόγους απλοποίησης ή έλλειψης πληροφοριών λόγω απορρήτου.

3.2.1 Φορείς

Στη διαδικασία της αεροδιακομιδής εμπλέκονται δυνητικά το Εθνικό Κέντρο Άμεσης Βοήθειας (ΕΚΑΒ), το Γενικό Επιτελείο της Αεροπορίας (ΓΕΑ), η Εθνική Μετεωρολογική Υπηρεσία (ΕΜΥ) και το Γενικό Επιτελείο Στρατού (ΓΕΣ).

Σε έκτακτα περιστατικά ασθενειών ή τραυματισμών και εφόσον ο γιατρός διαγνώσει την κρισιμότητα της κατάστασης ενημερώνει τηλεφωνικά το ΕΚΑΒ για την αναγκαιότητα αεροδιακομιδής. Το ΕΚΑΒ αφού καταγράψει την κλήση, προχωρά σε αξιολόγηση και διαβαθμίζει ως προς τον βαθμό του επείγοντος. Στην συνέχεια σε συνεργασία με το ΓΕΑ, εκτελεί αν είναι εφικτή την αεροδιακομιδή. Επίσης, το ΕΚΑΒ ενημερώνει την υγειονομική μονάδα υποδοχής για την κατάσταση του ασθενούς και τα μέτρα που πρέπει να ληφθούν για την καλύτερη δυνατή αντιμετώπιση του περιστατικού. Κατά τη διάρκεια της μεταφοράς τηρούνται όλοι οι προβλεπόμενοι κανόνες ασφαλείας που αφορούν και τον ασθενή και τους διασώστες, ενώ παράλληλα διατηρείται συνεχής επικοινωνία με το ΕΚΑΒ.

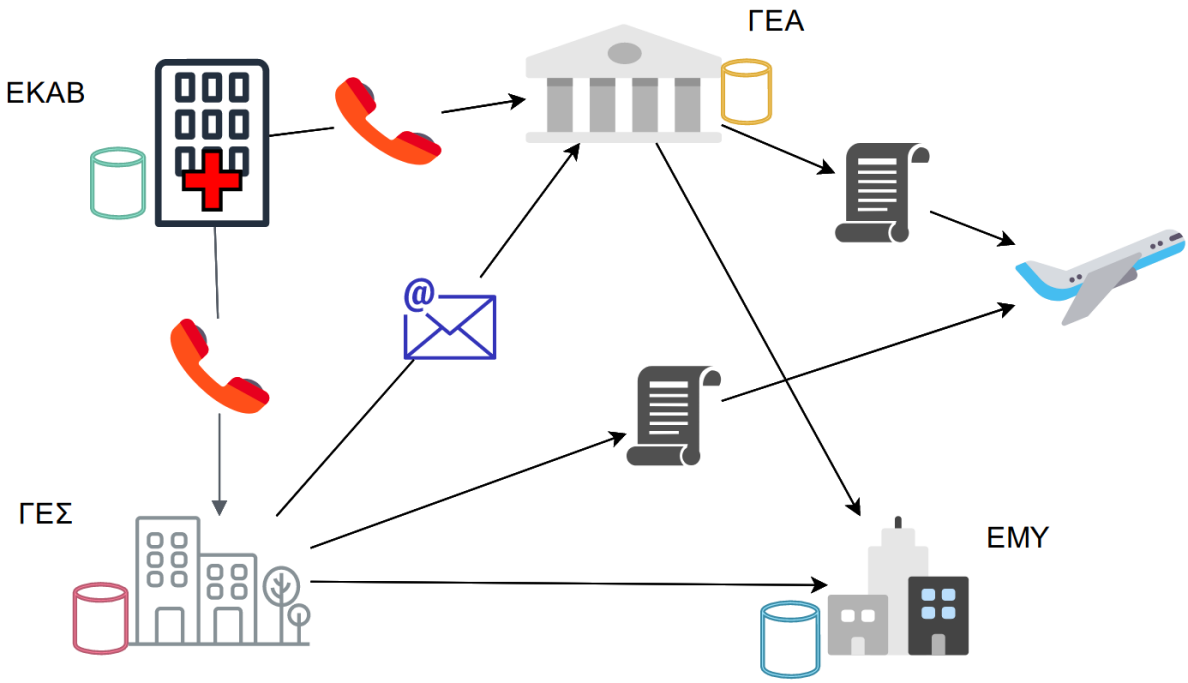
Λόγω της ιδιομορφίας του εδάφους της χώρας και της ύπαρξης πολλών νησιών που συνήθως δεν έχουν την κατάλληλη υγειονομική υποδομή για την αντιμετώπιση δύσκολων περιστατικών, η αεροδιακομιδή είναι σημαντικός παράγοντας στον τομέα της υγείας. Η οργάνωση του συστήματος

αεροδιακομιδής, η εποπτεία της σωστής λειτουργίας και ο συντονισμός απαιτούν τη δημιουργία συντονιστικών Κέντρων Επιχειρήσεων από τους βασικούς φορείς λήψης αποφάσεων.

3.2.2 Ροή ενεργειών

Αρχικά, το ΕΚΑΒ λαμβάνει το αίτημα της αεροδιακομιδής ενός ασθενούς και προχωρά στην αποστολή εγκριτικού φαξ προς το ΓΕΑ. Κατόπιν αυτής της ειδοποίησης, το ΓΕΑ προχωρεί στην άμεση ενημέρωση των εμπλεκομένων φορέων όπως για παράδειγμα το πλήρωμα του ελικοπτέρου, το οποίο με τη σειρά του ελέγχει τις καιρικές συνθήκες που επικρατούν στις περιοχές αναχώρησης και προορισμού, για τις οποίες ενημερώνεται από την ΕΜΥ και το Αρχηγείο της Τακτικής Αεροπορίας (ΑΤΑ). Παράλληλα, εξετάζονται η ύπαρξη και η καταλληλότητα αεροδρομίου με δεδομένα καθώς και άλλες απαιτήσεις για τη δυνατότητα εκτέλεσης της αεροδιακομιδής από το ΓΕΑ.

Μόλις συγκεντρωθούν όλα τα δεδομένα λαμβάνεται η απόφαση για την εκτέλεση ή μη της αεροδιακομιδής από το ΓΕΑ. Σε περίπτωση έγκρισης, εκπληρώνεται η διαδικασία της μεταφοράς από το ΓΕΑ και εκδίδεται ένα έγγραφο με τη διαταγή της αεροδιακομιδής. Εφόσον η απάντηση στο αίτημα είναι αρνητική από το ΓΕΑ, αυτό αποστέλλεται στο Κέντρο Επιχειρήσεων του ΓΕΣ (ΓΕΣ/ΚΕΠΙΧ) με φαξ. Το ΚΕΠΙΧ ενημερώνει με τη σειρά του, τους δικούς του εμπλεκόμενους φορείς και το αίτημα μεταφέρεται σε διάφορες υπηρεσίες του ΓΕΣ και καταγράφεται στην βάση δεδομένων του. Στη συνέχεια, μετατρέπεται σε εντολή προς διερεύνηση που διαβιβάζεται στην Ι Μεραρχία Πεζικού (ΙΜΠ). Το αρμόδιο τμήμα μετατρέπει την εντολή σε διαταγή για διερεύνηση και τη μεταβιβάζει τηλεφωνικά και εγγράφως στην 1η Ταξιαρχία Αεροπορίας Στρατού (ΤΑΞΑΣ), όπου καταγράφεται η ώρα και η ημέρα που έλαβε χώρα η διαταγή. Ενημερώνεται τηλεφωνικά το πλήρωμα που αναλαμβάνει τον έλεγχο για την δυνατότητα πραγματοποίησης της αεροδιακομιδής. Συγκεκριμένα, ελέγχουν τις μετεωρολογικές συνθήκες και την καταλληλότητα του αεροδρομίου για την εκτέλεση της διακομιδής καθώς και την κατάσταση του πληρώματος.



Εικόνα 8: Επισκόπηση της συστάδας φορέων στο υπάρχον σύστημα αεροδιακομιδής και του τρόπου επικοινωνίας μεταξύ τους [64]

Όταν δεν είναι εφικτή η αποστολή, στέλνονται όλες οι λεπτομέρειες της μη δυνατότητας στο ΚΕΠΙΧ. Το ΚΕΠΙΧ εκδίδει ένα διαβιβαστικό με τις λεπτομέρειες της μη αποδοχής και στέλνει ένα φαξ μη αποδοχής στο ΓΕΣ. Το ΓΕΣ λαμβάνει τα δεδομένα με φαξ και τα καταγράφει στη βάση δεδομένων του, ενώ ταυτόχρονα ενημερώνει το ΓΕΑ, το οποίο με την σειρά του στέλνει την απόρριψη στο ΕΚΑΒ.

Όταν είναι εφικτή η αεροδιακομιδή, η ΤΑΞΑΣ ενημερώνει τηλεφωνικά και στη συνέχεια εκδίδει διαβιβαστικό αποδοχής της αποστολής που προωθείται στην ΙΜΠ. Η ΙΜΠ ενημερώνει τηλεφωνικά για κέρδος χρόνου τη Διεύθυνση Αεροπορίας Στρατού (ΔΑΣ) για την αποδοχή. Στη συνέχεια ενημερώνονται τα αρμόδια στελέχη και η ηγεσία στο ΓΕΣ, οι οποίοι αξιολογώντας τα δεδομένα και τα στοιχεία για την ασφάλεια και την επιτυχία της αποστολής λαμβάνουν την απόφαση για την έγκριση ή μη της αεροδιακομιδής. Στην περίπτωση που η ηγεσία δεν αποδεχτεί την αεροδιακομιδή, ενημερώνεται το ΚΕΠΙΧ και στην συνέχεια το ΓΕΑ, το οποίο αναλαμβάνει να καταγράψει την απόρριψη και να ενημερώσει το ΕΚΑΒ. Με την έγκριση της αποστολής ενημερώνεται το ΚΕΠΙΧ, που καταγράφει την ώρα έγκρισης και ενημερώνει προφορικά το ΔΑΣ. Ο αρμόδιος προϊστάμενος της ΔΑΣ λαμβάνοντας την έγκριση εκδίδει διαβιβαστικό διαταγής εκτέλεσης, την οποία στέλνει στην ΙΜΠ. Ακολουθούν αντίστοιχες διαταγές από όλους τους φορείς για την εκτέλεση της αποστολής.

Τέλος ενημερώνεται η ΤΑΞΑΣ με όλες τις πληροφορίες για την διακομιδή, ώστε να ξεκινήσει η προετοιμασία για την εκτέλεση της αποστολής.

Παράλληλα, ειδοποιείται το ΕΚΑΒ τηλεφωνικά και άμεσα από το ΓΕΑ και από το ΚΕΠΙΧ μετά την έγκριση της ηγεσίας για την έναρξη της προετοιμασίας της αποστολής που πρέπει να ολοκληρωθεί εντός μιας ώρας. Μετά την ολοκλήρωση της αποστολής, η ΤΑΞΑΣ εκδίδει έγγραφο με όλα τα δεδομένα για το πέρας της αποστολής που διαβιβάζεται σε όλους τους φορείς και όλοι οι εμπλεκόμενοι φορείς με τη σειρά τους εκδίδουν αντίστοιχες διαταγές με τα στοιχεία της αεροδιακομιδής και τα έγγραφα καταχωρούνται. Σε όλα τα στάδια επικοινωνίας δημιουργούνται έγγραφα, μηνύματα, φαξ, χάρτες, τηλεφωνικές κλήσεις και μετεωρολογικά δεδομένα, τα οποία στέλνονται επικυρωμένα απο τον έναν φορέα στον άλλο καθώς και μεταξύ των υπηρεσιών μέσα στον ίδιο φορέα.

3.2.3 Τεχνολογίες και πληροφοριακά συστήματα

Στην επικοινωνία μεταξύ των αρμόδιων φορέων χρησιμοποιούνται τηλεφωνικά κέντρα τελευταίας τεχνολογίας, καθώς και μηνύματα ηλεκτρονικού ταχυδρομείου ή φαξ. Το τηλέφωνο, το ραδιοτηλέφωνο, ο ασύρματος, το τηλέτυπο, το φαξ αποτελούν κύριες τηλεπικοινωνιακές συσκευές, που χρησιμοποιούνται για την ανταλλαγή δεδομένων μεταξύ υπηρεσιών. Ενδεικτικά, στην ΕΜΥ εξάγονται προγνώσεις καιρού για τις περιοχές ενδιαφέροντος σε μορφή χαρτών, διαγραμμάτων και στατιστικών ως δεδομένα που αποστέλλονται συνήθως με φαξ στις αρμόδιες υπηρεσίες.

Σε κάθε συντονιστικό κέντρο λειτουργεί ένα πληροφοριακό σύστημα μέσω του οποίου αντλούνται πληροφορίες απο την βάση δεδομένων του. Ένα πληροφοριακό σύστημα μπορεί να διαθέτει πληροφορίες σχετικά με τα αεροδρόμια και την κατάστασή τους σε πραγματικό χρόνο. Παράλληλα, έχει καταχωρημένα στοιχεία που αφορούν τα εναέρια μέσα, τη διαθεσιμότητα, τον εξοπλισμό, καθώς και το ιστορικό συντήρησης και βλαβών. Επίσης, ενημερώνεται καθημερινά με την αναλυτική κατάσταση των πληρωμάτων βάρδιας και των πιθανών αλλαγών.

Στο ιστορικό των αιτημάτων αεροδιακομιδής καταχωρούνται όλα τα δεδομένα που αφορούν την μελέτη έγκρισης ή απόρριψης της αποστολής και διαταγές και ενημερώσεις που εκδίδονται αντιστοίχως. Αναλυτικά,

αποθηκεύονται όλες οι ενέργειες, οι επικοινωνίες (με καταγραφή ώρας), οι εντολές, οι διαταγές, τα διαβιβαστικά έγγραφα και τα συνοδευτικά τους. Σε περίπτωση εκτέλεσης της αεροδιακομιδής καταχωρούνται με λεπτομέρειες οι ώρες έναρξης και λήξης, η διάρκεια εκτέλεσης, οι τόποι αναχώρησης και προορισμού, οι αναφορές των συμμετεχόντων και η έκβαση της αποστολής.

Βασικό ρόλο διαδραματίζουν οι ασύρματες τηλεπικοινωνίες και τα συστήματα ραντάρ. Παράλληλα, μπορεί να διατίθεται πραγματική εικόνα καιρού από δορυφόρο για την συνεχή πρόγνωση και μεταβολή των καιρικών συνθηκών. Οι επικοινωνίες φωνής μεταξύ του πιλότου του αεροσκάφους και του ελεγκτή του τμήματος εναέριας κυκλοφορίας διακρίνονται σε υψηλές συχνότητες (high-frequency, HF), πολύ υψηλές συχνότητες (very-high-frequency, VHF) και δορυφορικές επικοινωνίες SATCOM.

3.3 Ευκαιρίες, ανάγκες και περιορισμοί για τη χρήση blockchain

3.3.1 Ευκαιρίες

Όπως παρουσιάσαμε στο Κεφάλαιο 1, το Blockchain διαθέτει τις εξής καινοτόμες ιδιότητες:

- Αμεταβλητότητα (immutability)
- Αποκεντρικοποίηση (decentralization)
- Μηχανισμός συναίνεσης (consensus)
- Διαφάνεια (transparency)

Ο βαθμός στον οποίο ισχύουν αυτές, εξαρτάται από τον τύπο του συστήματος Blockchain (permissionless ή permissioned) και τον μηχανισμό συναίνεσης, οι οποίοι επιλέγονται ανάλογα με το threat model της εφαρμογής και τις απαιτήσεις αποδοτικότητας. [8]

Έχοντας αυτά υπ' όψιν, μπορούμε να αντιστοιχίσουμε τις απαιτήσεις ενός συστήματος κρίσιμης αποστολής με τις ιδιότητες του Blockchain. Για να αποφύγουμε τη γενική συζήτηση, εστιάζουμε στο σύστημα κρίσιμης αποστολής για αεροδιακομιδή, ώστε να εντοπίσουμε τις ευκαιρίες που θα δημιουργούσε η υιοθέτησή του.

Απαιτήσεις συστήματος αεροδιακομιδής	**Σχετικές ιδιότητες Blockchain**	**Ανάλυση**
Καταγραφή ενεργειών με ακριβή χρονοσήμανση	Αμεταβλητότητα, διαφάνεια	Χρήση ledger
Ορθή κατανομή πόρων	Αποκεντρικοποίηση, διαφάνεια	Κατανομή βάσει smart contracts, έλεγχος από σύνολο φορέων
Ταχύτητα αποφάσεων	Αποκεντρικοποίηση	Αυτοματοποίηση μέσω smart contracts
Εγκυρότητα και αντικειμενικότητα αποφάσεων	Αποκεντρικοποίηση	Αποτύπωση κανόνων και συμμόρφωση μέσω smart contracts

Ασφάλεια και αξιοπιστία	Μηχανισμός συναίνεσης	Crash fault tolerance για αξιοπιστία, Byzantine fault tolerance για ασφάλεια
Διαχείριση διαμοιρασμένων και ποικιλόμορφων πληροφοριών	Αποκεντρικοποίηση, διαφάνεια	Κοινό ledger

Πίνακας 5: Αντιστοίχιση απαιτήσεων συστήματος αεροδιακομιδής με ιδιότητες του Blockchain

3.3.2 Ανάγκες

Η ενσωμάτωση του Blockchain στο σύστημα αεροδιακομιδής δημιουργεί την ανάγκη ύπαρξης:

- Υποδομών public-key infrastructure (PKI), εικονικών μηχανών (VM) για τους κόμβους του blockchain και για τη φιλοξενία των DApps μέσω των οποίων θα γίνεται η διεπαφή των χρηστών του συστήματος με το Blockchain.

- Κατανόησης του threat model και των πιθανών απειλών ασφαλείας από κάθε φορέα.

- Διαδικασιών για την εισαγωγή και λήψη δεδομένων από/προς το Blockchain.

- Διαδικασιών για την ενημέρωση και τον έλεγχο ορθής λειτουργίας των smart contracts και της παραμετροποίησης του συστήματος Blockchain.

- Ανθρώπινου δυναμικού με εξειδικευμένη γνώση σε κάθε φορέα, για την υλοποίηση των παραπάνω.

3.3.3 Περιορισμοί

Είναι επίσης σκόπιμο να αναλύσουμε τους περιορισμούς που μπορεί να εισάγει η υιοθέτηση ενός συστήματος Blockchain για τη λειτουργία του συστήματος αεροδιακομιδής.

Αφενός, οι περιορισμοί που προκύπτουν λόγω της φύσης του Blockchain:

- **Καθυστέρηση εκτέλεσης:** Εισάγονται πρόσθετες διαδικασίες για αυθεντικοποίηση και εισαγωγή δεδομένων στο Blockchain που, ειδικά στο αρχικό στάδιο που δεν περιλαμβάνει αυτοματοποίηση, θα καθυστερούν περαιτέρω την εκτέλεση.

- **Απαγόρευση παρεκκλίσεων:** Η αυτοματοποίηση μέσω της εκτέλεσης smart contracts απαιτεί την αυστηρή τήρηση των διαδικασιών που έχουν προβλεφθεί, σε αντίθεση με χειροκίνητα συστήματα όπου συνήθως επιτρέπονται στιγμιαίες παρεκκλίσεις.

- **Απόδοση:** Η έγκαιρη εκτέλεση της αεροδιακομιδής θα εξαρτάται πλέον και από την απόδοση του Blockchain, δηλαδή την ταχύτητα διεκπεραίωσης των συναλλαγών από τη δημιουργία μέχρι την επιβεβαίωση. Η επιλογή του μηχανισμού συναίνεσης (consensus) αποτελεί κρίσιμο παράγοντα.

- **Off-chain υπολογισμοί:** Ο χειρισμός μεγάλων αρχείων, η εκτέλεση χρονοβόρων υπολογισμών και η διεπαφή με τον εξωτερικό κόσμο είναι ακατάλληλοι για διενέργεια εντός του συστήματος Blockchain.

Αφετέρου, οι περιορισμοί που οφείλονται στη φύση του συστήματος αεροδιακομιδής:

- Πρόσβαση μόνο σε συγκεκριμένους φορείς, άρα ανάγκη για permissioned σύστημα.

- Διαφορετικά δικαιώματα και διαδικασίες ανά φορέα.

- Απόρρητο επικοινωνιών, άρα ανάγκη για ιδιωτικά κανάλια επικοινωνίας για εσωτερική χρήση (intra-organizational) ή μεταξύ φορέων (inter-organizational).

- Αδυναμία/απροθυμία παρεμβάσεων στο legacy σύστημα.

- Ενδεχόμενη αδυναμία αποτύπωσης μέρους των κανόνων λειτουργίας του συστήματος αεροδιακομιδής, με τη μορφή smart contracts.

- Αδυναμία/απροθυμία για εφαρμογή αυτοματοποίησης σε τμήματα της διαδικασίας αεροδιακομιδής, π.χ. για νομικούς λόγους ή λόγω έλλειψης εμπιστοσύνης στην ορθή λειτουργία του συστήματος Blockchain.

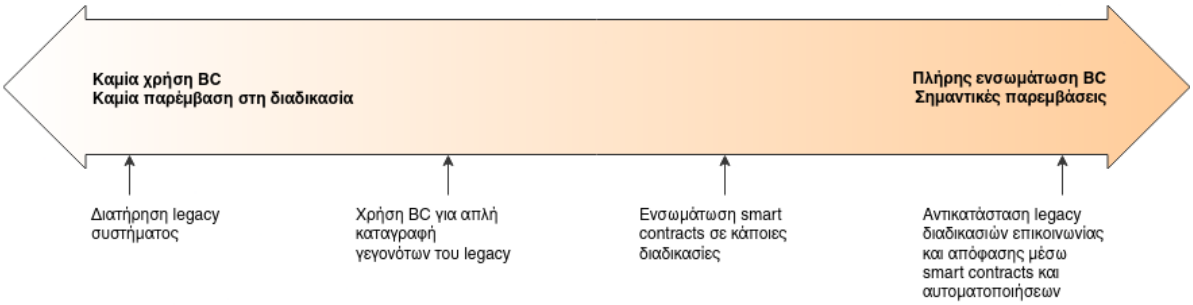
- Ύπαρξη μη μηχαναγνώσιμων δεδομένων, ή/και δεδομένων με μεγάλο όγκο, όπως εικόνες ή μετεωρολογικά δεδομένα.

- Δεν είναι εφικτή για όλους τους εμπλεκόμενους ρόλους η (άμεση) επικοινωνία με το Blockchain, π.χ. για το πλήρωμα ελικοπτέρων κατά την πτήση.

Βασικός σκοπός είναι η ελαχιστοποίηση των παρεμβάσεων που χρειάζονται στα ανεξάρτητα συστήματα των συμμετεχόντων φορέων για να αλληλεπιδρούν με το Blockchain. Μπορούν ακόμη να σχεδιαστούν κατά περίπτωση, χωρίς να απαιτείται πλήρης ομογενοποίηση. Αυτό αποτελεί και το βασικό αντικείμενο διερεύνησης της παρούσας εργασίας.

3.4 Το φάσμα της ενσωμάτωσης

Είδαμε προηγουμένως τα σημαντικά οφέλη που θα προέκυπταν από την αξιοποίηση όλων των ευκαιριών που εισάγει η τεχνολογία του Blockchain, όπως είναι η ελαχιστοποίηση του χρόνου εκτέλεσης ή η ορθότερη κατανομή πόρων. Ωστόσο, αυτό ενδεχομένως να μην είναι εφικτό ή και θεμιτό, λόγω των προεκτεθέντων περιορισμών και των αναγκών που θα δημιουργούνταν. Έτσι, οδηγούμαστε σε ένα φάσμα επιλογών για τον βαθμό ενσωμάτωσης του Blockchain στο υπάρχον σύστημα όσον αφορά την αυτοματοποίηση μέσω smart contracts και την παρέμβαση στις πραγματικές διαδικασίες.



Εικόνα 9: Το φάσμα επιλογών για τον βαθμό ενσωμάτωσης του Blockchain στο legacy σύστημα

Οι υβριδικές λύσεις για την ενσωμάτωση του Blockchain αποτελούν αντικείμενο μελέτης για τη βιβλιογραφία, ως ενδιάμεση επιλογή μεταξύ των πλήρως κεντρικοποιημένων και των πλήρως αποκεντρικοποιημένων συστημάτων. Σε αυτές συνυπάρχουν και τα δύο συστήματα με ποικίλο βαθμό ενσωμάτωσης, όπου λ.χ. το Blockchain χρησιμοποιείται για απλή καταγραφή δεδομένων και γεγονότων, ή για να εκτελεί μέρος των διαδικασιών μέσω smart contracts, ενώ το κεντρικοποιημένο σύστημα αναλαμβάνει την υπόλοιπη λειτουργικότητα. [58]

Η εύρεση του επιθυμητού βαθμού ενσωμάτωσης αποτελεί σχεδιαστική επιλογή και μπορεί να αφορά συνολικά το σύστημα ή να επιμερίζεται στις διαφορετικές διαδικασίες που περιλαμβάνει.

Αναφέρουμε, ενδεικτικά, παράγοντες που μπορούν να ληφθούν υπ’ όψιν:

- Είναι εφικτό να αυτοματοποιηθεί η διαδικασία ώστε να εκτελείται μέσω smart contract;

- Είναι θεμιτό να αυτοματοποιηθεί η διαδικασία; Μήπως πρέπει να καθορίζεται από ανθρώπινη απόφαση;

- Αν απαιτείται συμμετοχή ανθρώπου στη διαδικασία, έχει άμεση πρόσβαση στο Blockchain;

- Υπάρχει θεσμικό πλαίσιο που να επιτρέπει ή αποτρέπει την κοινοποίηση των δεδομένων στο Blockchain και την αυτοματοποίηση της διαδικασίας;

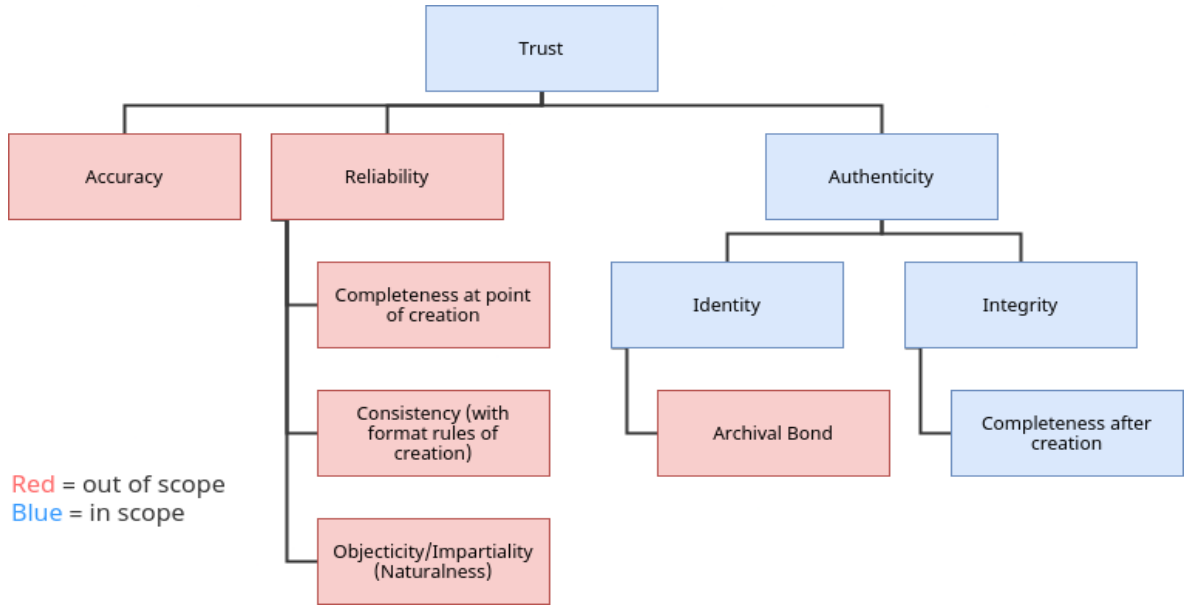
3.4.1 Χρήση του Blockchain ως immutable log

Έχοντας υπ' όψιν το παραπάνω φάσμα επιλογών, είναι σκόπιμο να εστιάσουμε στη συγκριτικά απλή ενσωμάτωση του Blockchain μόνο ως μέσου διατήρησης αναλλοίωτων καταγραφών (immutable log) των γεγονότων του legacy συστήματος. Παρότι έτσι μένουν αναξιοποίητες οι ευκαιρίες από τη συμμετοχή του Blockchain στη λήψη αποφάσεων, έχει αξία να εντοπίσουμε αν ακόμη και αυτή η απλή χρήση παρουσιάζει οφέλη, σε σύγκριση με την επιλογή της διατήρησης του υπάρχοντος συστήματος ως έχει.

Αρχικά, η καταγραφή συμβάντων έχει κομβική σημασία στη διαδικασία της αεροδιακομιδής. Η αποτύπωση των γεγονότων και των αποφάσεων, του χρόνου τέλεσης, της σειράς τους, των δεδομένων στα οποία βασίστηκαν και των συμμετεχόντων προσώπων, είναι επιβεβλημένη για τον εντοπισμό πιθανών βελτιώσεων της διαδικασίας έως και πειθαρχικών ή ποινικών ευθυνών από τους εμπλεκόμενους φορείς. Πέρα από καλοήθη σφάλματα, όπως η ακούσια διαγραφή μιας καταχώρισης σε βάση δεδομένων, ή η φθορά ενός εγγράφου από μία κούπα καφέ, το αναλλοίωτο της καταγραφής είναι ιδίως απαραίτητο και για την προστασία από κακοήθη σφάλματα, όπως η εκ των υστέρων παραποίηση για συγκάλυψη ευθύνης.

Οφείλουμε να σημειώσουμε ότι, αν και η ιδιότητα του αναλλοίωτου του Blockchain συχνά παρουσιάζεται ως η λύση για τη δημιουργία και διατήρηση έμπιστων δεδομένων σε περιβάλλοντα χωρίς εμπιστοσύνη, με μια στοιχειωδώς κριτική ματιά αυτό αποδεικνύεται ανακριβές. Σε δημοσίευσή της, η Lemieux (2017) [59] προτείνει ένα πλαίσιο αξιολόγησης συστημάτων Blockchain σχετικών με την καταγραφή, μέσω εφαρμογής αρχών της επιστήμης της αρχειονομίας. Παρατηρεί ότι για δεδομένα που δημιουργούνται εκτός Blockchain και καταχωρούνται σε αυτό, σαφώς το

Blockchain δεν μπορεί εγγενώς να εγγυηθεί την αλήθεια τους ή την αξιοπιστία τους ως προς το αν αναπαριστούν ορθά και πλήρως την πραγματική πληροφορία· ιδιότητες απαραίτητες για να χαρακτηριστούν έμπιστα (trustworthy). Η μόνη εγγύηση αφορά το αναλλοίωτο της πληροφορίας αφότου έχει καταχωρηθεί στο Blockchain και προϋποθέτει βέβαια την ασφάλεια έναντι επιθέσεων ή σφαλμάτων υλοποίησης, ενώ η επέκταση του αναλλοίωτου και στο πρωτότυπο αρχείο απαιτεί την ύπαρξη ντετερμινιστικής αντιστοίχισής του με την πληροφορία on-chain ώστε να μπορεί να διαπιστωθεί τυχόν μεταγενέστερη μεταβολή της ακεραιότητάς του.



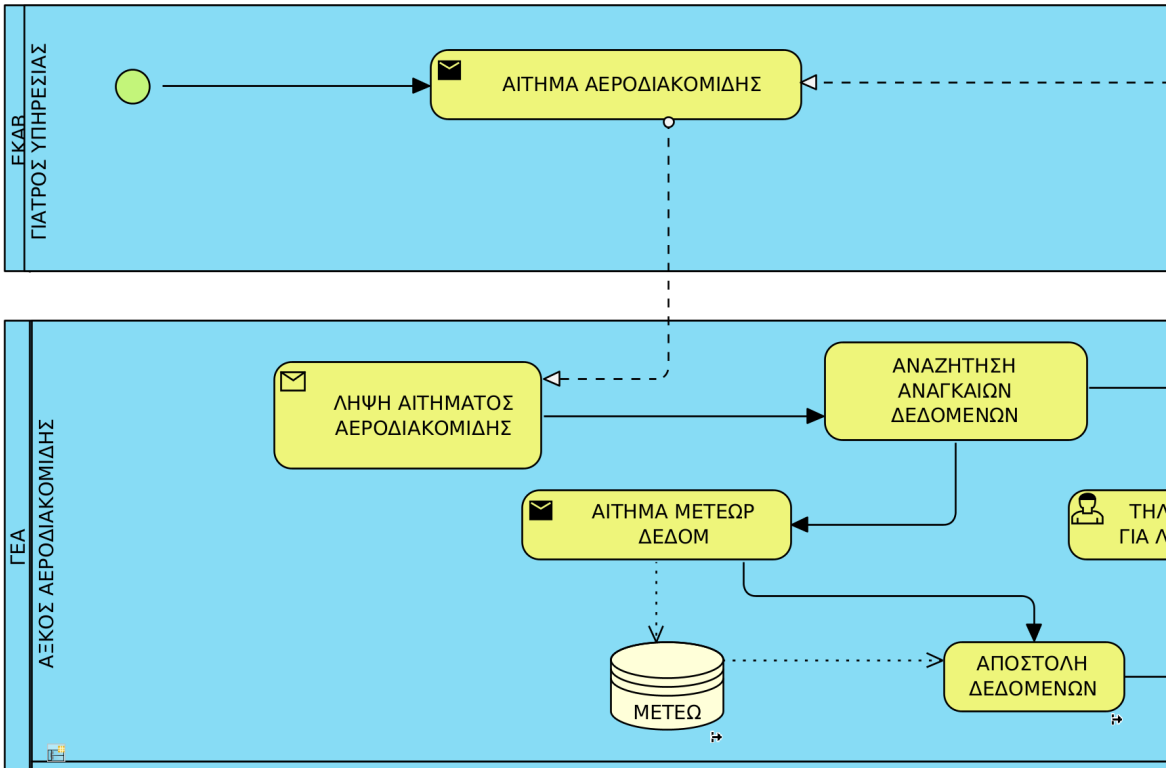
Εικόνα 10: Ιδιότητες που συνθέτουν την εμπιστοσύνη μιας καταγραφής. Με μπλε όσες καλύπτονται θεωρητικά από το Blockchain, με κόκκινο οι υπόλοιπες. [59]

Εφόσον λοιπόν υπάρχει η ντετερμινιστική αντιστοίχιση και η εύλογη ασφάλεια συστήματος του Blockchain, συμπεραίνουμε ότι η περίπτωση χρήσης του Blockchain για την καταγραφή συμβάντων μπορεί να μας εξασφαλίσει τις εξής ουσιαστικές και ωφέλιμες βελτιώσεις σε σχέση με το υπάρχον σύστημα: α) αναλλοίωτο των καταγραφών μετά την καταχώριση και β) διαφάνεια των καταγραφών ως προς κάθε συμμετέχοντα στο δίκτυο.

3.5 Μοντελοποίηση BPMN

Η εργασία μας βασίστηκε σε μοντελοποίηση [60] του υπάρχοντος συστήματος αεροδιακομιδής, με τη μορφή διαγράμματος Business Process Model (BPMN).

Παρακάτω βλέπουμε ενδεικτικά ένα τμήμα του διαγράμματος που αφορά την έναρξη της αεροδιακομιδής με την αποστολή αιτήματος από το ΕΚΑΒ προς το ΓΕΑ και την αναζήτηση μετεωρολογικών δεδομένων από τον αξιωματικό αεροδιακομιδής του ΓΕΑ. Το πλήρες διάγραμμα βρίσκεται στο Παράρτημα Α.



Εικόνα 11: Τμήμα του BPMN της διαδικασίας αεροδιακομιδής [60]

Η πρώτη μεταβίβαση δεδομένων αφορά το αίτημα από το ΕΚΑΒ προς το ΓΕΑ. Το αίτημα έχει τη μορφή σαρωμένου εγγράφου, δηλαδή είναι εικόνα raster. Όπως είδαμε σε προηγούμενο υποκεφάλαιο, υπάρχει φάσμα πιθανών σχεδιαστικών επιλογών για την ενσωμάτωση του Blockchain σε αυτήν τη μεταβίβαση. Ενδεικτικά, κάποιες προσεγγίσεις:

- Διατήρηση της διαδικασίας ως έχει και επιπλέον ο γιατρός υπηρεσίας και ο αξιωματικός αεροδιακομιδής να καταχωρούν την καταγραφή γεγονότος αποστολής και λήψης αντίστοιχα στο Blockchain.

- Αντί της τρέχουσας διαδικασίας, η ανάρτηση του εγγράφου να γίνεται σε κοινό σύστημα αρχείων, είτε συμβατικό (π.χ. FTP), είτε αποκεντρικοποιημένο (π.χ. IPFS), και ο αξιωματικός αεροδιακομιδής να ενημερώνει για την τοποθεσία του αρχείου με παράλληλη καταχώρηση στο Blockchain μίας αναφοράς σε αυτό για σκοπούς καταγραφής (π.χ. με τη μορφή hash).

- Αντί της τρέχουσας διαδικασίας, ο γιατρός υπηρεσίας να αποστέλλει το έγγραφο σε oracle που μέσω αλγορίθμου οπτικής αναγνώρισης χαρακτήρων (OCR) θα το μετατρέπει σε κείμενο και θα το καταχωρεί στο Blockchain. Ο αξιωματικός αεροδιακομιδής θα ενημερώνεται από DApp που παρακολουθεί το κατάλληλο smart contract event.

Η μοντελοποίηση BPMN μας επιτρέπει με αυτόν τον τρόπο να αναλύσουμε το σύστημα στους επιμέρους φορείς και συμμετέχοντες (actors), να καταγράψουμε τα δεδομένα που ανταλλάσσουν μεταξύ τους και να εντοπίσουμε τα σημεία όπου μπορεί να παρεμβληθεί το Blockchain.

4 Η προσέγγισή μας

4.1 Βασικές σχεδιαστικές κατευθύνσεις

Σύμφωνα με την ανάλυση των αναγκών και περιορισμών στο υποκεφάλαιο §3.3, καθώς και την προηγούμενη μοντελοποίηση BPMN, μπορούμε να διατυπώσουμε κάποιες βασικές κατευθύνσεις για την σχεδιαστική προσέγγιση και την αρχιτεκτονική ενός συστήματος Blockchain που θα εφαρμοζόταν σε ένα σύστημα αεροδιακομιδής με τα περιγραφέντα χαρακτηριστικά.

Ως προς την επιλογή πλατφόρμας, είναι απαραίτητη η χρήση consortium permissioned συστήματος. Η πρόσβαση στο Blockchain θα πρέπει να επιτρέπεται μόνο σε συγκεκριμένους χρήστες με προκαθορισμένα δικαιώματα, ενώ η διακυβέρνηση θα πρέπει να γίνεται συνεργατικά μεταξύ των φορέων καθόσον δεν υπάρχουν ιεραρχικές σχέσεις και για αποφυγή καταστάσεων single-point-of-failure.

Κρίσιμη είναι η δυνατότητα χρήσης BFT αλγορίθμων συναίνεσης, καθώς το περιβάλλον του συστήματος αεροδιακομιδής δεν περιλαμβάνει πλήρη εμπιστοσύνη μεταξύ των φορέων. Η χρήση αλγορίθμου που διαθέτει μόνο τη CFT ιδιότητα, όπως ο Raft, προστατεύει μόνο από crash faults. Σε αυτήν την περίπτωση θα επιτρεπόταν, για παράδειγμα, σε κάποιον διαχειριστή του κόμβου του ΓΕΑ, αν είχε επιλεγεί ως Raft leader, να παρουσιάσει αλλοιωμένες τις καταγραφές του ΓΕΣ σε έναν client, αποσκοπώντας σε διαφυγή ευθυνών. Ακόμη, ένας κόμβος θα μπορούσε να επαναλαμβάνει κακόβουλα τη διαδικασία εκλογής leader για να τελματώσει τη λειτουργία του Blockchain. [8], [20]

Ακόμη, η πλατφόρμα πρέπει να διαθέτει τη δυνατότητα ιδιωτικών καναλιών επικοινωνίας, όπως στο GoQuorum ή στο Hyperledger Fabric, για την εξυπηρέτηση αναγκών απορρήτου εντός του consortium (π.χ. επικοινωνίες ΓΕΣ-ΤΑΞΑΣ που θα πρέπει να μην είναι ορατές στο ΕΚΑΒ).

Αξίζει επίσης να εξετάσουμε το πρόβλημα των μεγάλων αρχείων (σαρωμένα έγγραφα, μετεωρολογικά δεδομένα κτλ.) που δημιουργεί την ανάγκη για off-chain διαδικασίες αποθήκευσης και υπολογισμών.

Όσον αφορά την αποθήκευση αρχείων μπορούν να υπάρξουν διάφορες προσεγγίσεις. Μία απλή προσέγγιση θα ήταν η χρήση μόνο των υπάρχοντων συστημάτων και η αναφορά στα αρχεία με αριθμούς πρωτοκόλλου, με την υπόθεση ότι η παραποίησή τους είναι πρακτικά αρκετά δύσκολη και επομένως θεωρούμε ότι διατηρείται η απαραίτητη ιδιότητα του αναλλοίωτου. Πιο σύνθετες προσεγγίσεις θα μπορούσαν να περιλαμβάνουν τη μεταφόρτωση των αρχείων σε ένα ιδιωτικό δίκτυο IPFS ή συγκεκριμένα για τα σαρωμένα έγγραφα, τη μετατροπή τους σε κείμενο, που λόγω μικρού μεγέθους μπορεί να αποθηκευθεί αυτούσιο, μέσω αλγορίθμου οπτικής αναγνώρισης κειμένου (OCR) που εκτελείται σε Trusted Execution Environment.

Όσον αφορά την εκτέλεση υπολογισμών, για παράδειγμα την επεξεργασία μετεωρολογικών δεδομένων για τον έλεγχο καταλληλότητας καιρικών συνθηκών από smart contract, θα μπορούσε να ανατεθεί σε μία συστάδα από oracles λογισμικού (βλ. §1.4) .

Σε κάθε περίπτωση, τα εξωγενή συστήματα θα χρειαζόταν να υπόκεινται στον έλεγχο των φορέων και να μην αποτελούν τρίτες υπηρεσίες, ώστε να διασφαλιστεί η κλειστότητα και απορρητότητα του συστήματος.

4.2 Παράλληλο σύστημα Blockchain για καταγραφή συμβάντων και παραγωγή προτάσεων

Για τους σκοπούς της εργασίας, θα εστιάσουμε στο σενάριο όπου επιλέγουμε την πλήρη διατήρηση του legacy συστήματος και των διαδικασιών του, και την υιοθέτηση του Blockchain ως ένα παράλληλο σύστημα με την ελάχιστη δυνατή παρέμβαση στην υπάρχουσα διαδικασία σε κάθε φορέα που εμπλέκεται στην αεροδιακομιδή.

Το σενάριο παρουσιάζει ενδιαφέρον καθώς προκύπτει από την εύλογη απαίτηση οργανισμών που εξετάζουν την ενσωμάτωση τεχνολογιών Blockchain, για μια ομαλή μετάβαση, τόσο προς αποφυγή διαταράξεων στο υπάρχον και λειτουργικό σύστημά τους όσο και λόγω διστακτικότητας. Η λειτουργία του παράλληλου συστήματος απαιτεί την καταχώριση στο Blockchain δεδομένων που βρίσκονται στο legacy σύστημα, είτε αυτούσια είτε με ένα αναγνωριστικό που αντιστοιχεί μοναδικά στο πρωτότυπο δεδομένο το οποίο είναι διαθέσιμο off-chain, ή επίσης τη δημιουργία νέων δεδομένων (π.χ. καταγραφές γεγονότων που δεν περιλαμβάνονται στο legacy). Παρόμοια προσέγγιση ακολουθήθηκε σε πιλοτική εφαρμογή Blockchain στον Δήμο Pelotas της Βραζιλίας, όπου καταγράφονταν οι τίτλοι ιδιοκτησίας και οι μεταβιβάσεις ακινήτων. [61]

Η μεθοδολογία που ακολουθήσαμε για τον σχεδιασμό του παράλληλου συστήματος περιελάμβανε αρχικά την απαρίθμηση των δεδομένων που υπάρχουν και ανταλλάσσονται στο legacy σύστημα. Έχοντας καταγράψει για κάθε δεδομένο τον τύπο, τον αποστολέα, τον παραλήπτη, τη διαδικασία όπου ανήκει, και τις εξαρτήσεις του, καθορίσαμε τον τύπο με τον οποίο θα αποθηκεύεται στο Blockchain και τον σχετικό μετασχηματισμό (βλ. §4.4).

Ακόμη, για κάθε επικοινωνία μεταξύ συμμετεχόντων που συμβαίνει off-chain, πέρα από τα δεδομένα που καταχωρεί ο αποστολέας στο Blockchain, προσθέτουμε ένα βήμα on-chain αναγνώρισης από τον παραλήπτη ότι τα έλαβε, έτσι ώστε για κάθε τέτοια αλληλεπίδραση να υπάρχει διπλή καταγραφή και από τα δύο μέρη.

Πέρα από την καταγραφή συμβάντων, προτείνουμε την υλοποίηση smart contracts που εφαρμόζουν τους κανόνες της αεροδιακομιδής (π.χ. το αν οι μετεωρολογικές συνθήκες είναι κατάλληλες για πτήση ελικοπτέρου), αλλά με

τη μορφή προτάσεων. Ονομάζουμε τα συγκεκριμένα smart contracts παθητικά (passive smart contracts), κατά την ορολογία των Molina-Jiménez et al. (2018) [58], εννοώντας ότι δεν επιβάλλουν συγκεκριμένα σενάρια εκτέλεσης και επομένως δεν επηρεάζουν τη διαδικασία. Οι προτάσεις προκύπτουν από τα δεδομένα του Blockchain, αποθηκεύονται στο world state και γνωστοποιούνται στους συμμετέχοντες.

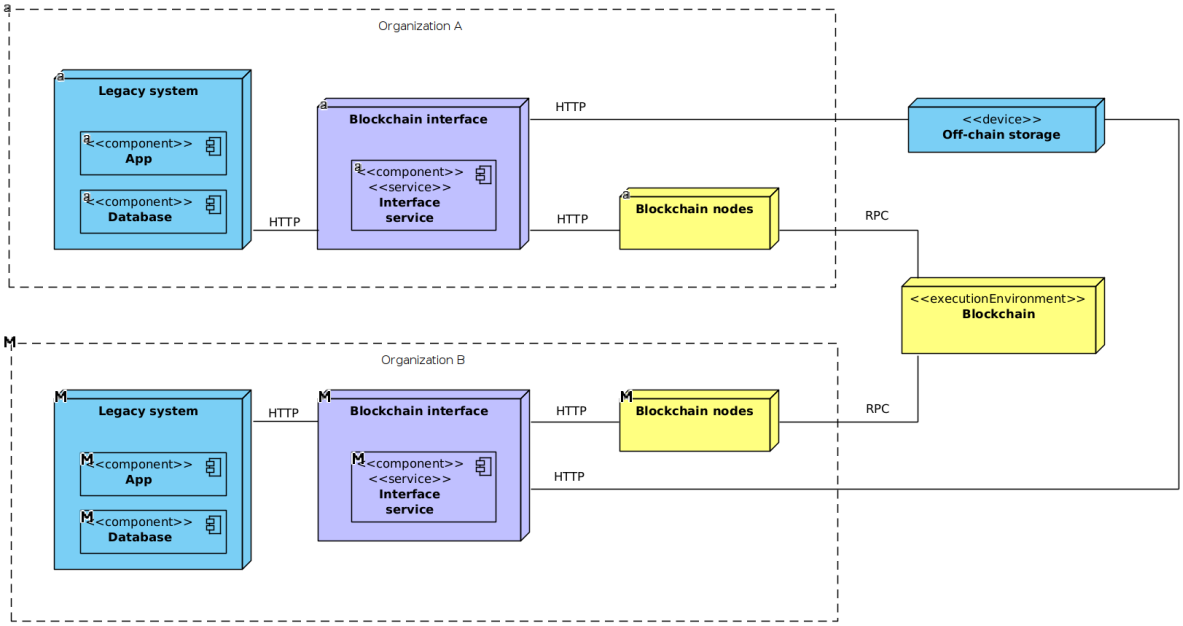
Τα οφέλη από αυτήν την προσέγγιση είναι ότι επιτυγχάνουμε να έχουμε μη-δεσμευτικά smart contracts που μπορούν όμως να εντοπίζουν τυχόν διαφωνίες ανάμεσα στο πώς θα “έπρεπε” να εκτελεστεί η διαδικασία σύμφωνα με τους κανόνες που έχουν αποτυπωθεί στο Blockchain, και στο πώς εκτελέστηκε τελικά από το legacy σύστημα. Παράλληλα, λειτουργούν ως ένα χρήσιμο πείραμα για μια ενδεχόμενη μελλοντική μετάβαση σε ένα σύστημα με μη-παθητικά smart contracts, τα οποία δηλαδή επηρεάζουν δεσμευτικά τη διαδικασία αεροδιακομιδής.

4.3 Αρχιτεκτονική με legacy-to-blockchain interfaces

Η ενσωμάτωση του Blockchain στο σύστημα αεροδιακομιδής απαιτεί από κάθε φορέα να δημιουργήσει νέες διαδικασίες ή να παρεμβάλει βήματα σε ήδη υπάρχουσες για την καταχώρηση, την παρακολούθηση και τον έλεγχο των δεδομένων στο Blockchain.

Ωστόσο, η απαίτηση για τη κατά το δυνατόν διατήρηση ως έχει του legacy συστήματος δεν μας επιτρέπει να τροποποιήσουμε το υπάρχον λογισμικό, ώστε για παράδειγμα η φόρμα με την οποία καταχωρείται το αίτημα αεροδιακομιδής σε μια βάση δεδομένων να δημιουργεί ταυτόχρονα συναλλαγές στο Blockchain.

Επ' αυτού προτείνουμε την ιδέα της διεπαφής Blockchain, η οποία υλοποιείται ως ενδιάμεσο λογισμικό και παρεμβάλλεται μεταξύ του legacy συστήματος και του Blockchain, ενώ μπορεί και να αλληλεπιδρά με εξωτερικές υπηρεσίες για την ανάκτηση ή αποστολή δεδομένων.



Εικόνα 12: Παράδειγμα UML Deployment με δύο οργανισμούς για χρήση ενδιάμεσου λογισμικού μεταξύ συστημάτων legacy και Blockchain. Ενδεικτικά θεωρούμε ότι το σύστημα legacy αποτελείται από μία εφαρμογή (π.χ. web) και μία βάση δεδομένων.

Η διεπαφή αναλαμβάνει να μετασχηματίσει τα δεδομένα που καταχωρεί ο

χρήστης στη μορφή που αναμένει το Blockchain, συμπεριλαμβανομένων ενεργειών όπως η μεταφόρτωση σε ένα off-chain περιβάλλον (π.χ. IPFS), η δημιουργία αναγνωριστικών hash κτλ. Παρακολουθεί τα συμβάντα που εκπέμπονται από τα smart contracts και μεταφέρει τυχόν ειδοποιήσεις στον χρήστη. Ακόμη, μπορεί να ελέγχει αν ο χρήστης έχει συμπληρώσει τα βήματα της εκάστοτε διαδικασίας και να ειδοποιεί για τυχόν παρεκκλίσεις.

Κάθε οργανισμός υλοποιεί τη δική του διεπαφή, ανάλογα με τα χαρακτηριστικά του legacy συστήματος, χωρίς εγγενείς περιορισμούς σχεδίασης πέραν της συμμόρφωσης με τις προδιαγραφές για τα δεδομένα και τις κλήσεις στα smart contracts. Μπορεί, για παράδειγμα, να είναι μια απλή εφαρμογή γραμμής εντολών που συνδέεται με μια βάση δεδομένων ή ένα ολοκληρωμένο σύστημα διαχείρισης και κωδικοποίησης εγγράφων.

Η εισαγωγή των διεπαφών Blockchain μπορεί να δημιουργήσει ορισμένα προβλήματα και ανάγκες, τα οποία αναλύουμε στον παρακάτω πίνακα μαζί με προτάσεις για την πιθανή αντιμετώπισή τους.

Πρόβλημα	**Πιθανή αντιμετώπιση**
Πρόσθετες ανάγκες για διαθεσιμότητα, αξιοπιστία, ασφάλεια, συντήρηση	Συνήθεις πρακτικές ποιότητας συστημάτων
Έλλειψη εμπιστοσύνης από τους υπόλοιπους φορείς για την ορθή λειτουργία	Εκτέλεση σε Trusted Execution Environment
Πρόσθετες διαδικασίες για τους χρήστες, ενδεχόμενα ασυμφωνίας με legacy	Λήψη δεδομένων από το legacy ώστε η εισαγωγή να γίνεται μία φορά εκεί, ή προσαρμογή ώστε η εισαγωγή δεδομένων στη διεπαφή να γίνεται όπως στο legacy για συνοχή

Πίνακας 6: Πιθανά προβλήματα από την υιοθέτηση των διεπαφών Blockchain

4.4 Ανάλυση data items

Με βάση το διάγραμμα BPMN, απαριθμήσαμε και αναλύσαμε το σύνολο των δεδομένων που ανταλλάσσονται στο πλαίσιο της διαδικασίας της αεροδιακομιδής μεταξύ των συμμετεχόντων (actors) και των φορέων. Στη συνέχεια, ορίσαμε για κάθε δεδομένο τον προτεινόμενο μετασχηματισμό του ώστε να αποθηκευθεί στο Blockchain.

Παρακάτω βλέπουμε ένα ενδεικτικό τμήμα του πίνακα δεδομένων (βλ. πλήρη πίνακα στο Παράρτημα Β). Οι γραμμές 1-6 μάλιστα αντιστοιχούν στις δραστηριότητες του διαγράμματος BPMN που είδαμε στην Εικόνα 11.

Α/Α	ΟΡΓΑΝΙΣΜΟΣ	ΣΥΜΜΕΤΕΧΩΝ	ΔΡΑΣΤΗΡΙΟΤΗΤΑ (BPMN)	LEGACY			BLOCKCHAIN				ΠΕΡΙΠΤΩΣΗ ΧΡΗΣΗΣ
				Δεδομένο	Τύπος δεδομένου	Σημειώσεις	Μετασχηματισμός	Δεδομένο BC	Τύπος δεδομένου BC	Σημειώσεις	
1	ΕΚΑΒ	Γιατρός υπηρεσίας	-	Αφετηρία και προορισμός αερ/δής	{src: location, dst: location}		=	Αφετηρία και προορισμός αερ/δής	{src: location, dst: location}		Αίτημα αεροδιακομιδής
2	ΕΚΑΒ	Γιατρός υπηρεσίας	Αίτημα αεροδιακομιδής	Αίτημα αεροδιακομιδής	document		hash	Αναφορά στο αίτημα αεροδιακομιδής	str		Αίτημα αεροδιακομιδής
3	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Λήψη αιτήματος αεροδιακομιδής	Καταγραφή συμβάντος	event			ACK	{}		Αίτημα αεροδιακομιδής
4	ΓΕΑ	Αξιωματικός αεροδιακομιδής	-	Εξεταζόμενη περιοχή πτήσης	image	Χάρτης	pick	Εξεταζόμενη περιοχή πτήσης	polygon		Έλεγχος δυνατότητας ΓΕΑ
5	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Αίτημα μετεωρολογικών δεδομένων	Query μετεωρολογικών δεδομένων	str		=	Query μετεωρολογικών δεδομένων	str		Συγκέντρωση δεδομένων ΓΕΑ
6	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Αποστολή δεδομένων	Μετεωρολογικά δεδομένα	str	TAF-METAR	=	Μετεωρολογικά δεδομένα	str		Συγκέντρωση δεδομένων ΓΕΑ
7	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Τηλ. επικοινωνία με ΑΤΑ για καιρό περιοχής	Κλήση προς ΑΤΑ	audio		hash	Αναφορά στην κλήση	str		Συγκέντρωση δεδομένων ΓΕΑ
8	ΓΕΑ	ΑΤΑ	Αποδοχή αιτήματος για μετεωρ. δεδομένα	Καταγραφή συμβάντος	event			ACK	{}		Συγκέντρωση δεδομένων ΓΕΑ

Πίνακας 7: Τμήμα του πίνακα δεδομένων για την αεροδιακομιδή με τους προτεινόμενους μετασχηματισμούς Blockchain

Πέρα από τα αναγραφόμενα δεδομένα, κάθε καταχώρηση στο Blockchain συνοδεύεται από τα εξής βασικά στοιχεία: `{type: str, requestId: str, refTime: datetime, entryTime: datetime}`.

Όρος	Επεξήγηση
type	Αναγνωριστικό του τύπου δεδομένου, π.χ. **ekavRequest** για το αίτημα αεροδιακομιδής από το ΕΚΑΒ.
requestId	Αναγνωριστικό του αιτήματος αεροδιακομιδής που αφορά το παρόν δεδομένο.
refTime	Χρόνος που έλαβε το δεδομένο από την πηγή του ο συμμετέχων (actor).
entryTime	Χρόνος που υπέβαλε το δεδομένο προς καταχώρηση στο Blockchain ο συμμετέχων (actor).
BC	Blockchain.
location	Τύπος δεδομένων για συντεταγμένες τοποθεσίας.
polygon	Λίστα με συντεταγμένες που αναπαριστούν ένα χωρικό πολύγωνο.
str	Κείμενο.
document	Έγγραφο επεξεργασίας κειμένου ή σε raster μορφή.
ACK	Αναγνώριση συμβάντος από συμμετέχοντα, συνήθως για επιβεβαίωση ότι έλαβε κάτι από άλλον συμμετέχοντα (βλ. §4.2).
TAF-METAR	TAF και METAR είναι διεθνείς πρότυπες μορφές κωδικοποίησης για δεδομένα καιρού που χρησιμοποιούνται κυρίως στην αεροπορία και έχουν τη μορφή απλού κειμένου. Το METAR αφορά τον παρόντα καιρό και αποτελείται από ωριαίες επιφανειακές παρατηρήσεις, ενώ το TAF αφορά πρόγνωση καιρού έως 30 ωρών σε αεροδρόμιο.
Μετασχηματισμός =	Το δεδομένο εισάγεται στο Blockchain με την ίδια μορφή όπως στο legacy σύστημα.
Μετασχηματισμός hash	Στο Blockchain εισάγεται ένα αναγνωριστικό του δεδομένου που παράγεται από συνάρτηση κατακερματισμού, π.χ. checksum.
Μετασχηματισμός pick	Επιλέγεται ή εξάγεται τμήμα της πληροφορίας από το δεδομένο, αντί να καταχωρηθεί αυτούσιο, για αποδοτικότητα και οικονομία χώρου.

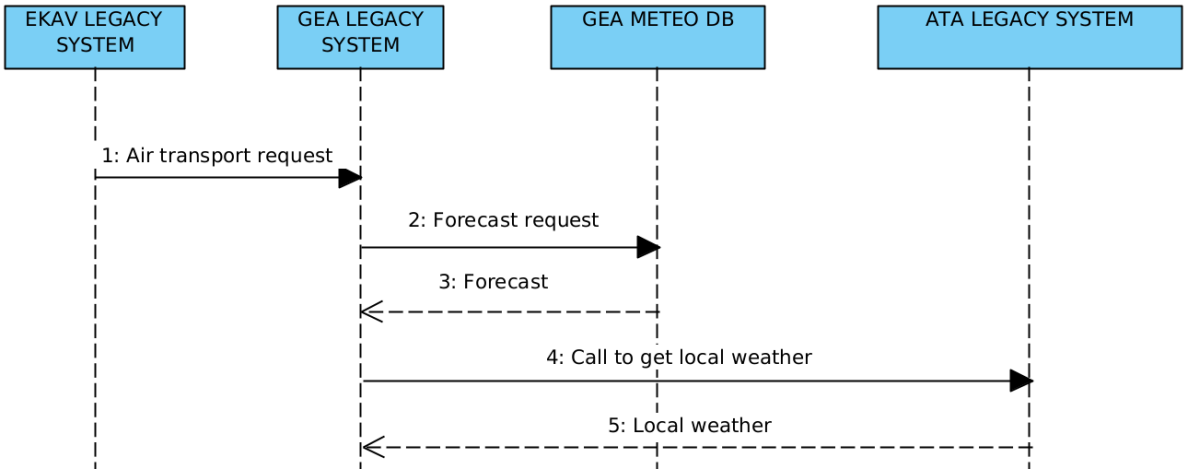
Πίνακας 8: Επεξήγηση όρων του Πίνακα 7. Πληροφορίες για TAF-METAR από [62]

Η γραμμή 3 αποτελεί εφαρμογή της πρότασής μας για την on-chain αναγνώριση της λήψης δεδομένων (βλ. §4.2), όπου πέραν του γιατρού υπηρεσίας ΕΚΑΒ που καταχωρεί αναγνωριστικό του αιτήματος αεροδιακομιδής στο Blockchain, έχουμε και την αναγνώριση από τη μεριά του αξιωματικού αεροδιακομιδής του ΓΕΑ ότι το έλαβε. Το ίδιο συμβαίνει στη γραμμή 8.

Επιπλέον, έχουμε σημειώσει με κίτρινο φόντο (γραμμές 4-6) τα δεδομένα που μπορούν θεωρητικά να υπολογιστούν μέσω smart contracts. Για αυτά προτείνουμε τη χρήση passive smart contracts (βλ. §4.2) που εφαρμόζουν τους κανόνες αεροδιακομιδής σε μορφή μη δεσμευτικών προτάσεων. Έτσι, στο σύστημα μπορούν να διατηρούνται παράλληλα οι τιμές όπως προέρχονται από το legacy και όπως προκύπτουν από τα smart contracts, ώστε να συγκρίνονται και να εντοπίζονται ασυμφωνίες.

4.5 Ανάλυση sequence diagrams

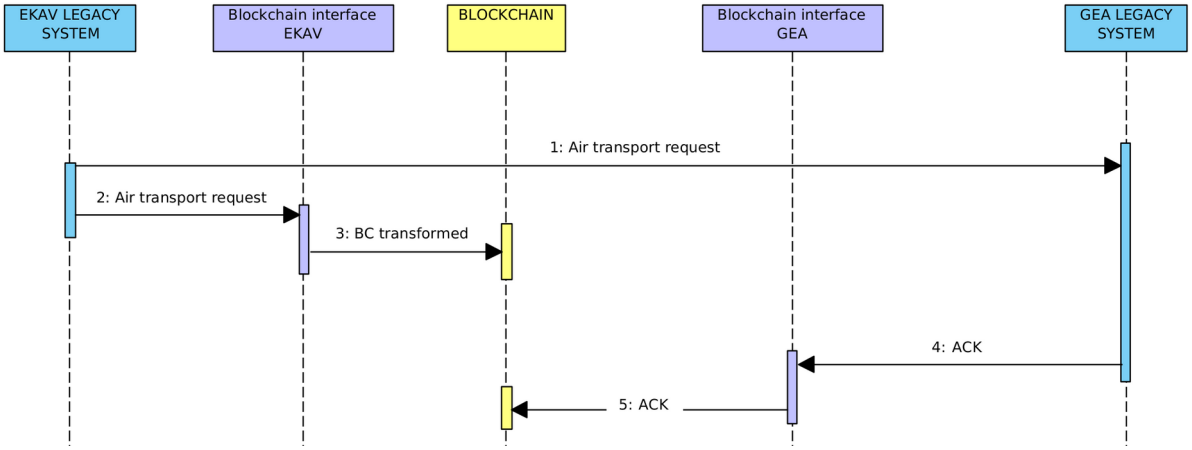
Στα πλαίσια της εργασίας χρειάστηκε ακόμη να αναλύσουμε την ακολουθία με την οποία καταχωρούνται και διαμοιράζονται τα δεδομένα στο σύστημα legacy. Με βάση το διάγραμμα BPMN, μοντελοποιήσαμε τη διαδικασία μέσω UML Sequence Diagram. Παρακάτω βλέπουμε ένα τμήμα του (βλ. Παράρτημα Γ για το πλήρες διάγραμμα) που αφορά τα πρώτα στάδια της αεροδιακομιδής και την επικοινωνία μεταξύ ΕΚΑΒ και ΓΕΑ.



Εικόνα 13: Τμήμα του UML Sequence Diagram για την αλληλουχία καταχωρήσεων και διαμοιρασμών δεδομένων στο σύστημα legacy

Η αποτύπωση της αλληλουχίας του συστήματος legacy μάς επιτρέπει να εντοπίσουμε με συστηματικό τρόπο τα σημεία όπου θα παρεμβληθεί η επικοινωνία με το Blockchain. Έχοντας υπ' όψιν και τον πίνακα δεδομένων του Παραρτήματος Β, θελήσαμε να μοντελοποιήσουμε με UML Sequence Diagrams το προτεινόμενο παράλληλο σύστημα.

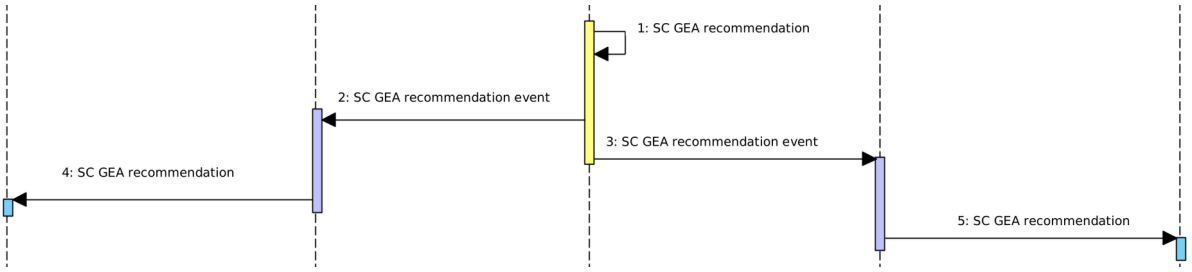
Βασικό στοιχείο της μοντελοποίησής μας είναι η εξής ακολουθία, όπως φαίνεται στο παρακάτω παράδειγμα για την αποστολή του αιτήματος αεροδιακομιδής από τον γιατρό υπηρεσίας του ΕΚΑΒ προς τον αξιωματικό αεροδιακομιδής του ΓΕΑ.



Εικόνα 14: Τμήμα UML Sequence Diagram για την παράλληλη αποστολή του αιτήματος αεροδιακομιδής και καταχώρησης στο Blockchain

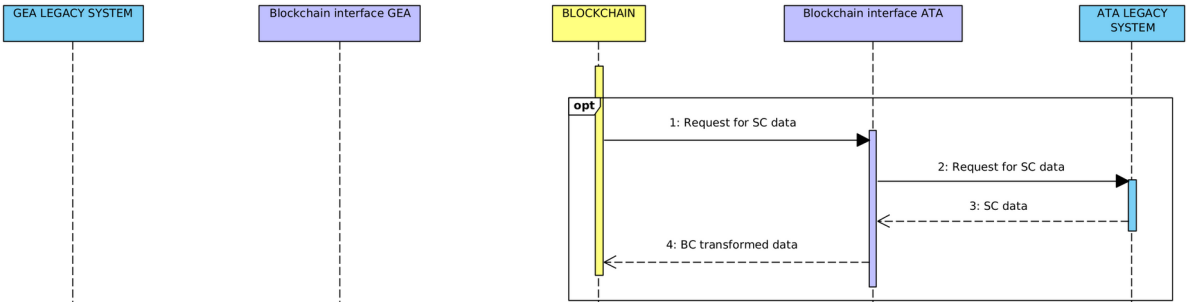
Το συγκεκριμένο μοτίβο έχει εφαρμοστεί καθ' όλη τη μοντελοποίησή μας. Σε αυτό οι συμμετέχοντες εκτελούν τη μετάδοση ενός δεδομένου κανονικά μέσω του συστήματος legacy και κατόπιν εισάγουν στο Blockchain –μέσω των διεπαφών Blockchain– το δεδομένο (αυτούσιο ή μετασχηματισμένο) από τη μία πλευρά, και την αναγνώριση λήψης του από την άλλη.

Ακόμη ένα βασικό μοτίβο αφορά τη διαμόρφωση προτάσεων από τα smart contracts και την ενημέρωση των συμμετεχόντων για αυτές μέσω smart contract events. Παρακάτω βλέπουμε την περίπτωση πρότασης για την απόφαση του ΓΕΑ ως προς το αν θα αναλάβει το αίτημα αεροδιακομιδής ή θα το μεταβιβάσει στο ΓΕΣ.



Εικόνα 15: Τμήμα UML Sequence Diagram για την παραγωγή και κοινοποίηση πρότασης από smart contract

Το τελευταίο μοτίβο που εμφανίζεται καθ' όλη τη μοντελοποίησή μας αφορά την πρόωρη λήψη δεδομένων από τους φορείς του συστήματος.



Εικόνα 16: Τμήμα UML Sequence Diagram για την πρόωρη λήψη δεδομένων από το ΑΤΑ προς καταχώρηση στο Blockchain

Η παραγωγή των προτάσεων των smart contracts για τη δυνατότητα των ΓΕΑ και ΓΕΣ να αποδεχθούν την εκτέλεση της αεροδιακομιδής, απαιτεί να έχουν συγκεντρωθεί πριν στο Blockchain τα απαραίτητα δεδομένα για τον υπολογισμό. Αν τα smart contracts ζητούν πρόωρα τα δεδομένα αντί να αναμένουν για το καθένα την εκτέλεση της αντίστοιχης διαδικασίας στο σύστημα legacy, μπορεί να επιταχυνθεί η έκδοση των προτάσεων, ώστε να γίνεται θεωρητικά ακόμη και αμέσως μετά την καταχώρηση του αιτήματος αεροδιακομιδής από το ΕΚΑΒ στο Blockchain.

Βάσει αυτών αναπαραστήσαμε το παράλληλο σύστημα με UML Sequence Diagrams. Για να αποφύγουμε ένα δυσανάγνωστο μοντέλο με 25 lifelines, διαχωρίσαμε τις αλληλεπιδράσεις ανά ζεύγος συμμετεχόντων (actors) του συστήματος legacy. Σε κάθε τέτοιο διάγραμμα συμμετέχει το ζεύγος, οι δύο διεπαφές Blockchain των αντίστοιχων φορέων, και το περιβάλλον του Blockchain που αναπαριστούμε ως ενιαία οντότητα.

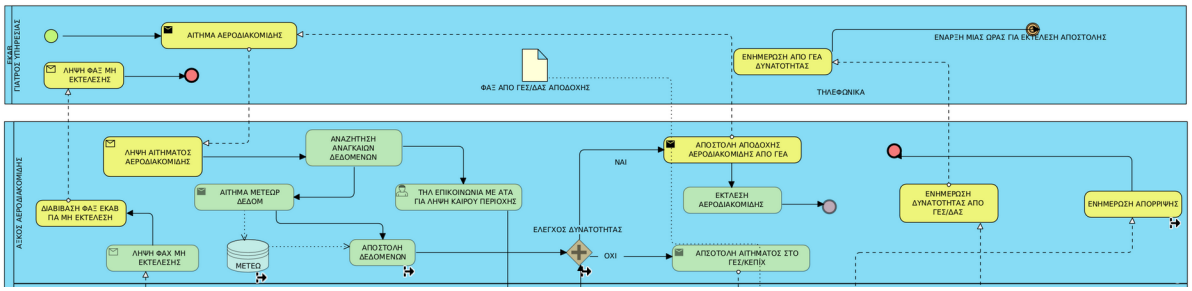
Η συγκεκριμένη μοντελοποίηση χρησιμεύει μεταξύ άλλων ως προδιαγραφή για τις αλλαγές που πρέπει να κάνει κάθε φορέας στις διαδικασίες του, καθώς επίσης για τον καθορισμό των δεδομένων εισόδου/εξόδου και την υλοποίηση των διεπαφών Blockchain και των smart contracts.

4.5.1 Sequence diagrams του παράλληλου συστήματος

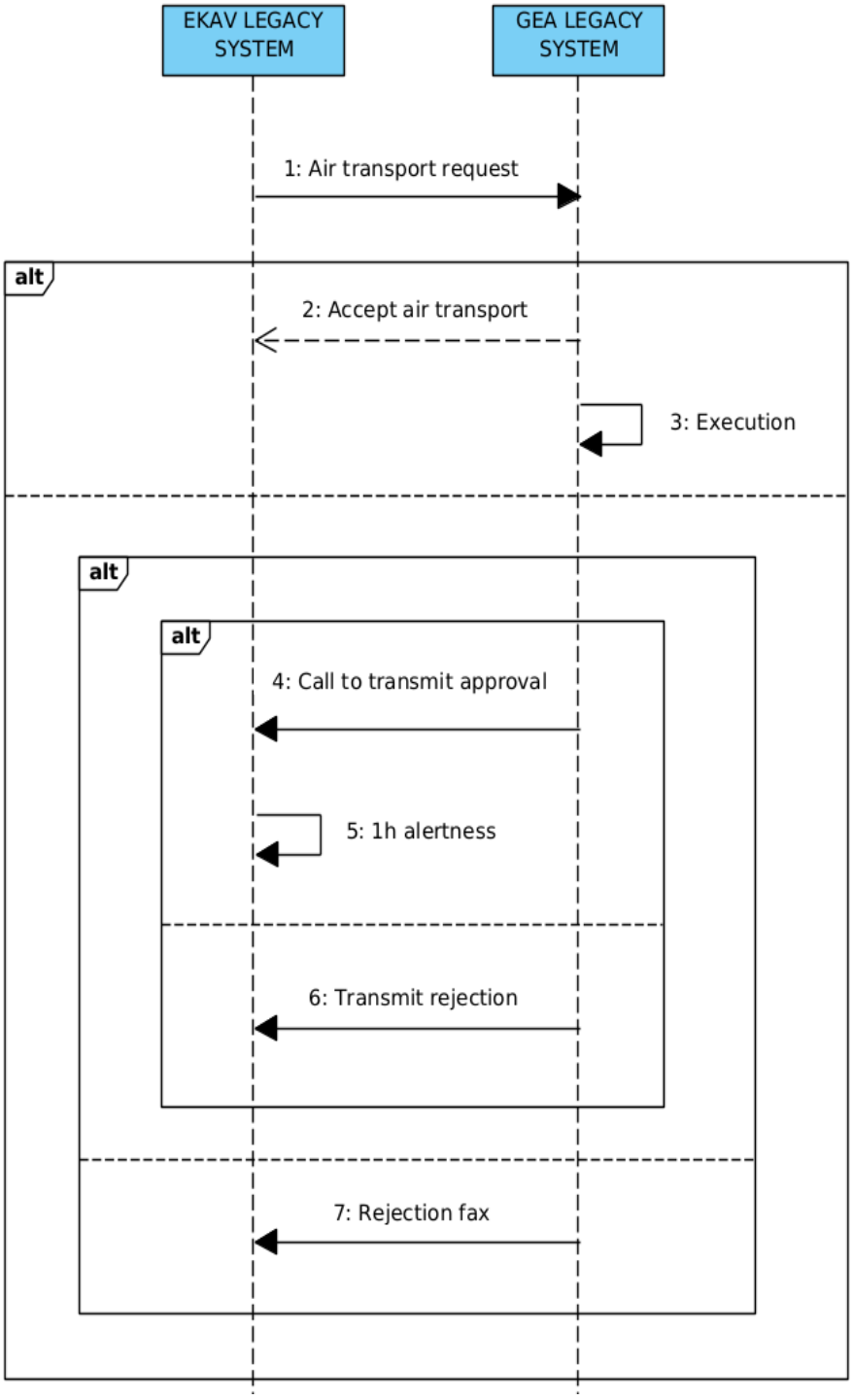
4.5.1.1 ΕΚΑΒ-ΓΕΑ

Σημειώσεις

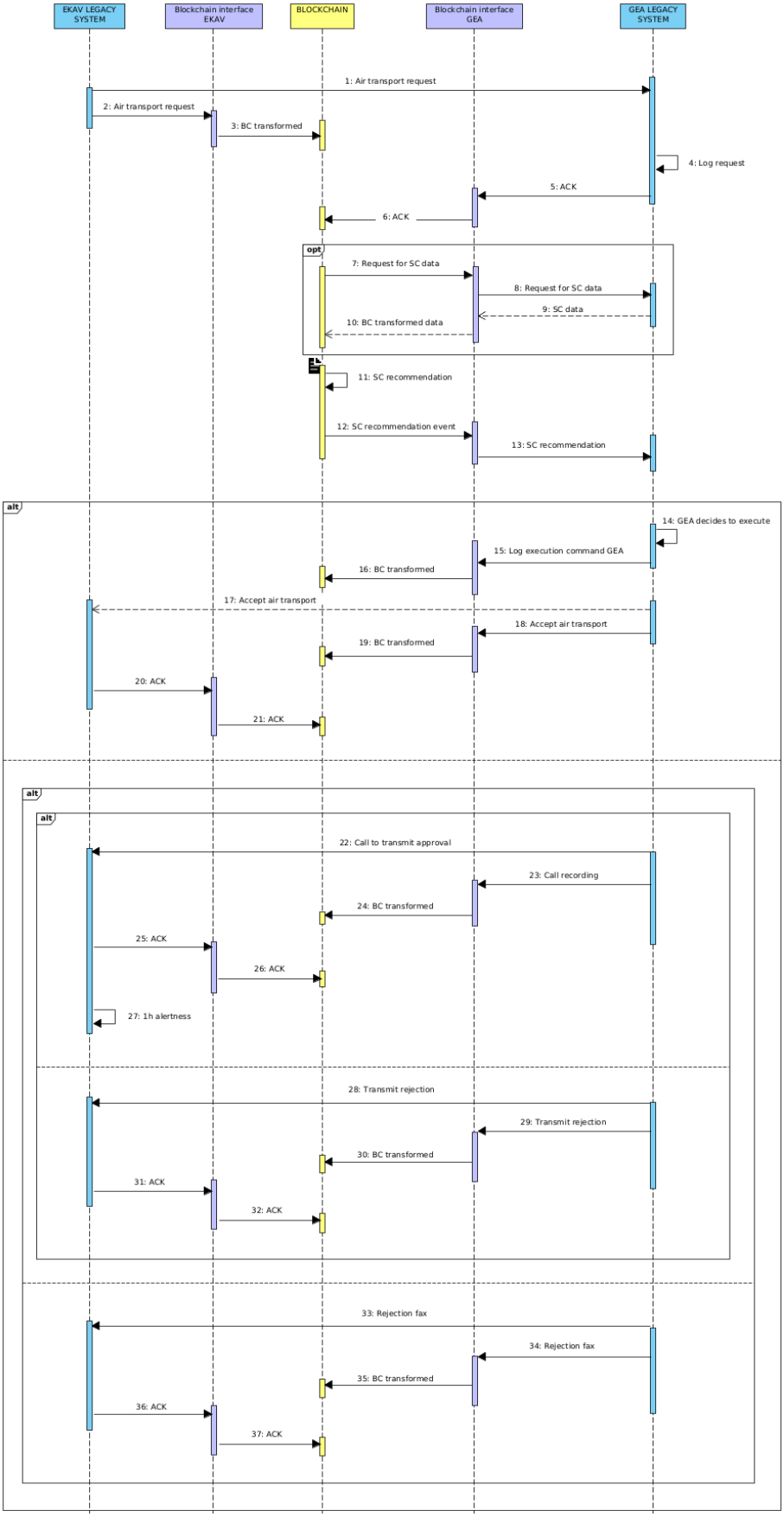
Στις γραμμές 1, 2, 3, 13, 15, 81, 82, 83, 111, 112 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ ΕΚΑΒ και ΓΕΑ.



Εικόνα 17: Τμήμα του BPMN για την επικοινωνία ΕΚΑΒ-ΓΕΑ στο σύστημα legacy



Εικόνα 18: UML Sequence Diagram για την επικοινωνία ΕΚΑΒ-ΓΕΑ στο σύστημα legacy

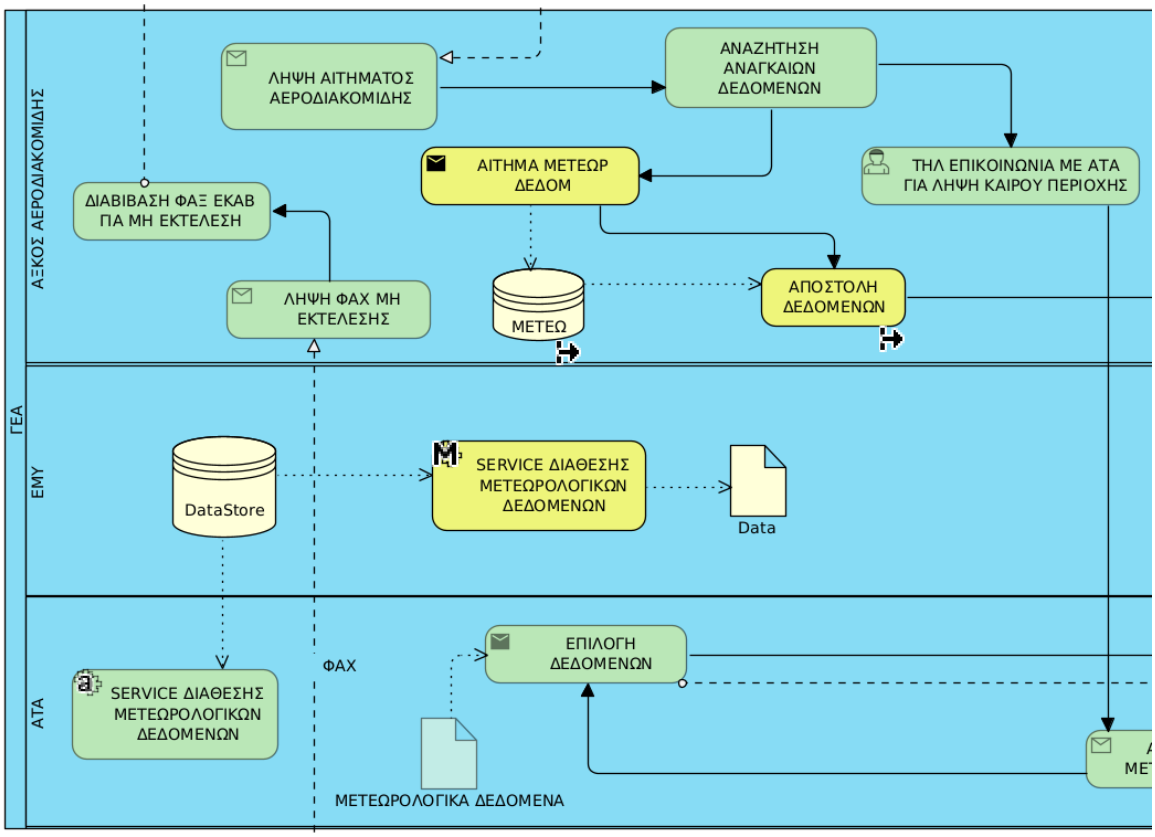


Εικόνα 19: UML Sequence Diagram για την επικοινωνία ΕΚΑΒ-ΓΕΑ στο παράλληλο σύστημα

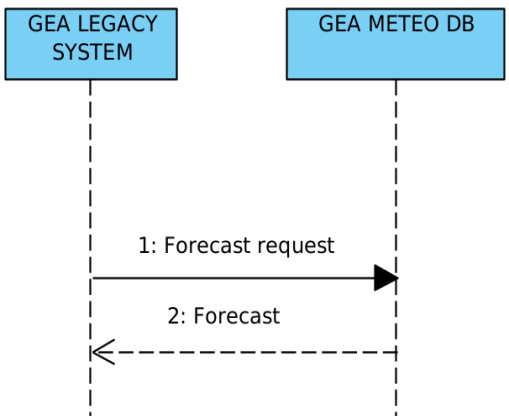
4.5.1.2 ΓΕΑ-ΜΕΤΕΟ DB

Σημειώσεις

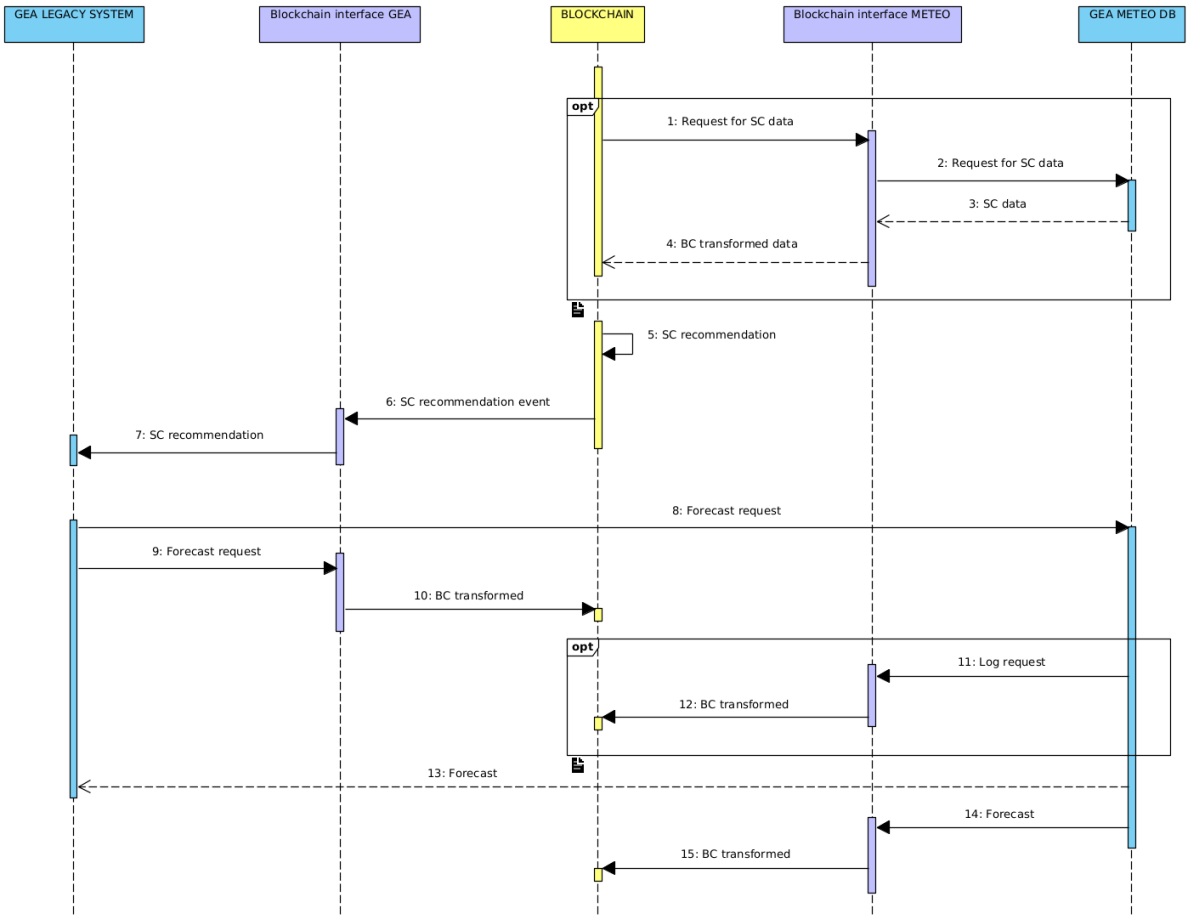
Στις γραμμές 4, 5, 6 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού αεροδιακομιδής ΓΕΑ και ΜΕΤΕΟ DB (βάση μετεωρολογικών δεδομένων).



Εικόνα 20: Τμήμα του BPMN για την επικοινωνία ΓΕΑ-ΜΕΤΕΟ DB στο σύστημα legacy



Εικόνα 21: UML Sequence Diagram για την επικοινωνία ΓΕΑ-ΜΕΤΕΟ DB στο σύστημα legacy

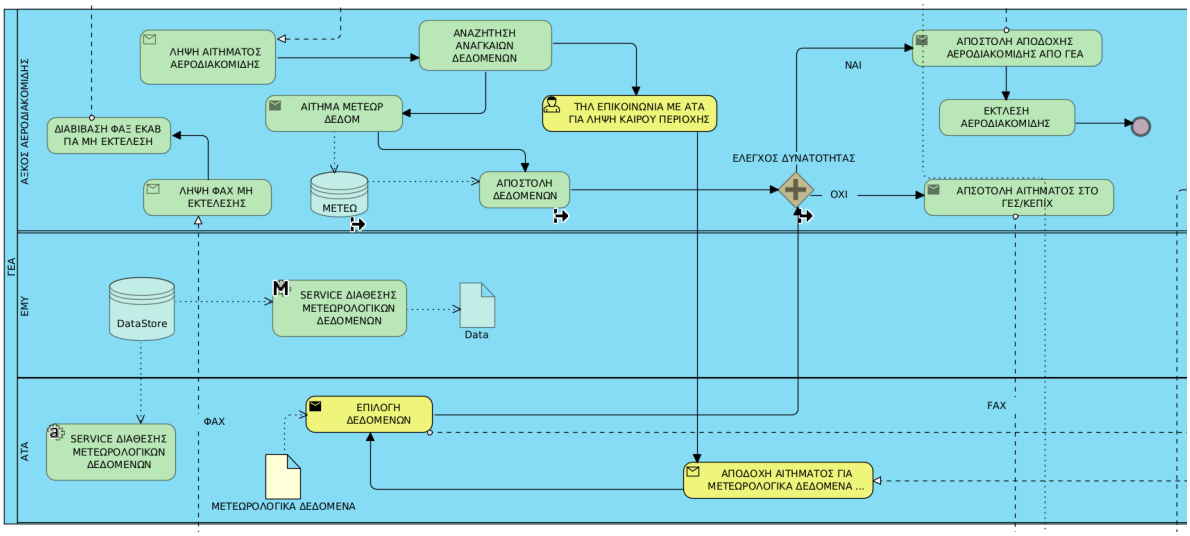


Εικόνα 22: UML Sequence Diagram για την επικοινωνία ΓΕΑ-METEO DB στο παράλληλο σύστημα

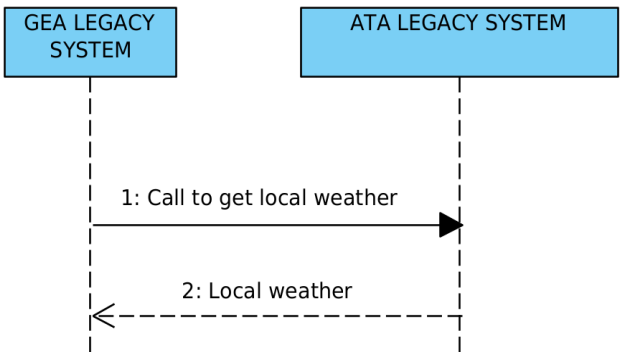
4.5.1.3 ΓΕΑ-ΑΤΑ

Σημειώσεις

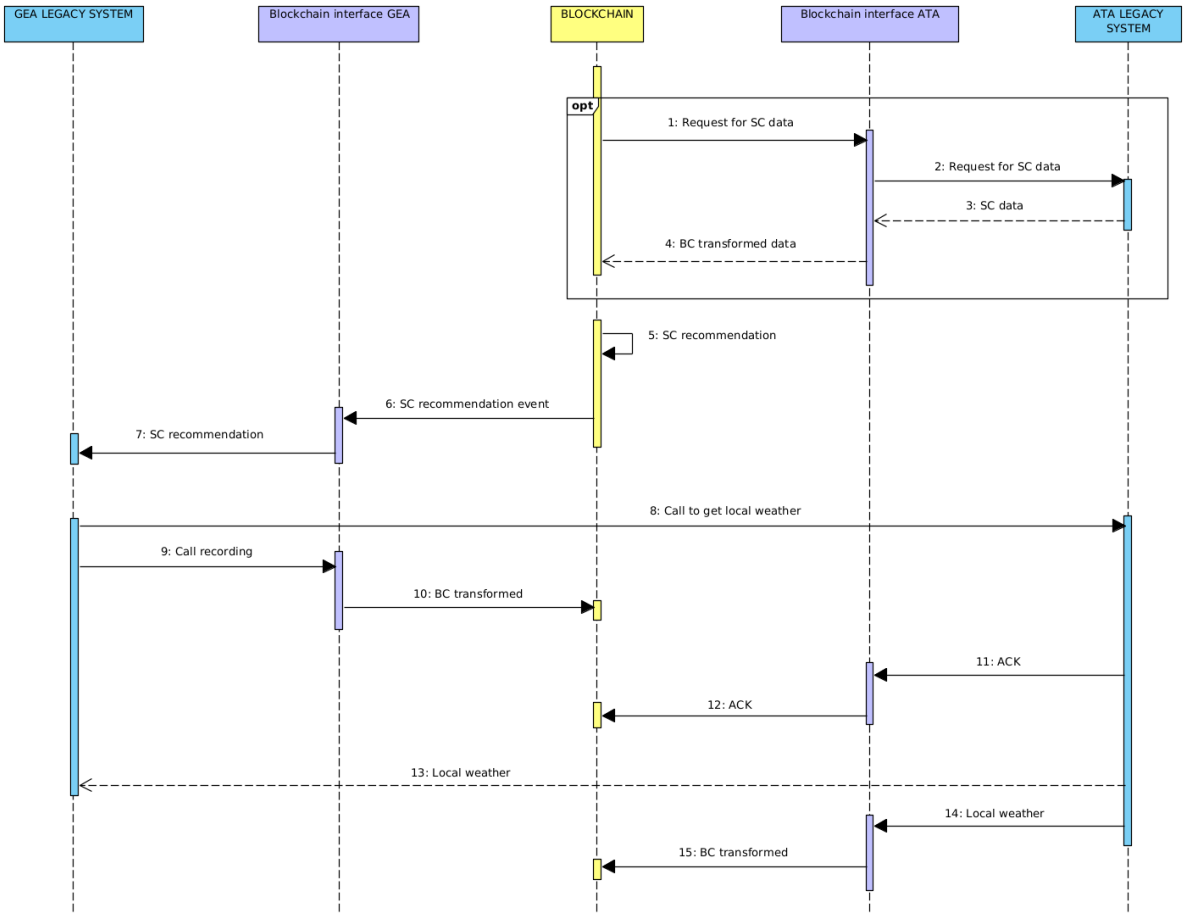
Στις γραμμές 7, 8, 9, 10 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού αεροδιακομιδής ΓΕΑ και ΑΤΑ.



Εικόνα 23: Τμήμα του BPMN για την επικοινωνία ΓΕΑ-ΑΤΑ στο σύστημα legacy



Εικόνα 24: UML Sequence Diagram για την επικοινωνία ΓΕΑ-ΑΤΑ στο σύστημα legacy

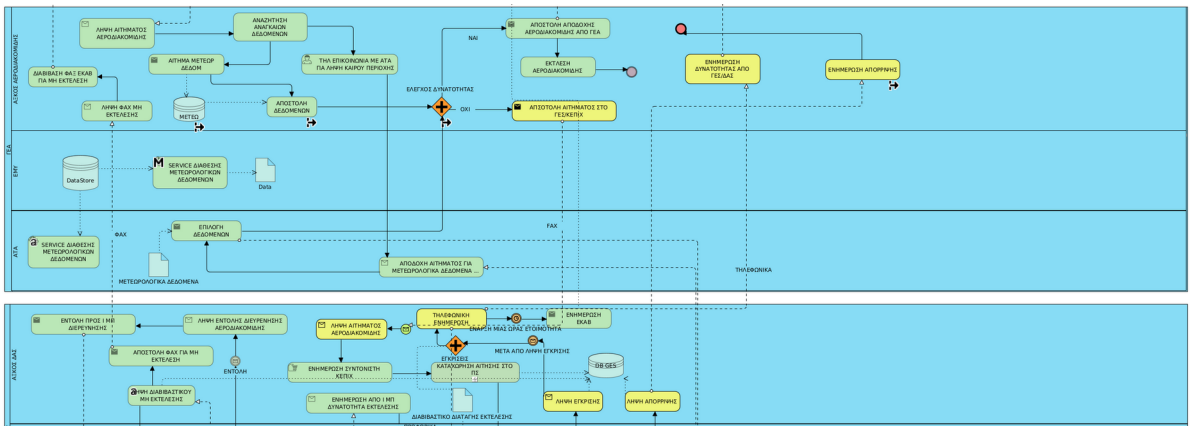


Εικόνα 25: UML Sequence Diagram για την επικοινωνία ΓΕΑ-ΑΤΑ στο παράλληλο σύστημα

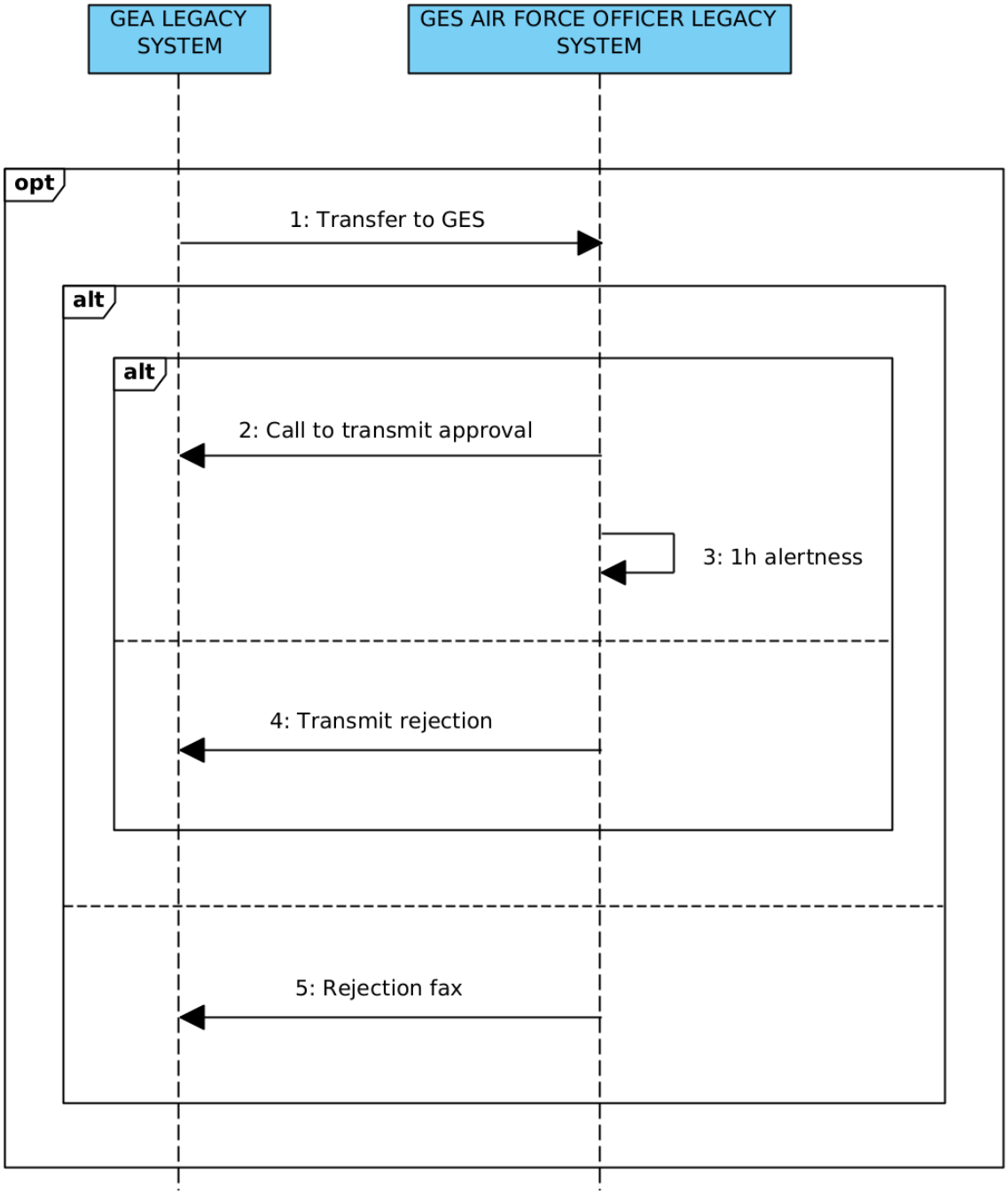
4.5.1.4 ΓΕΑ-Αξιωματικός ΔΑΣ ΓΕΣ

Σημειώσεις

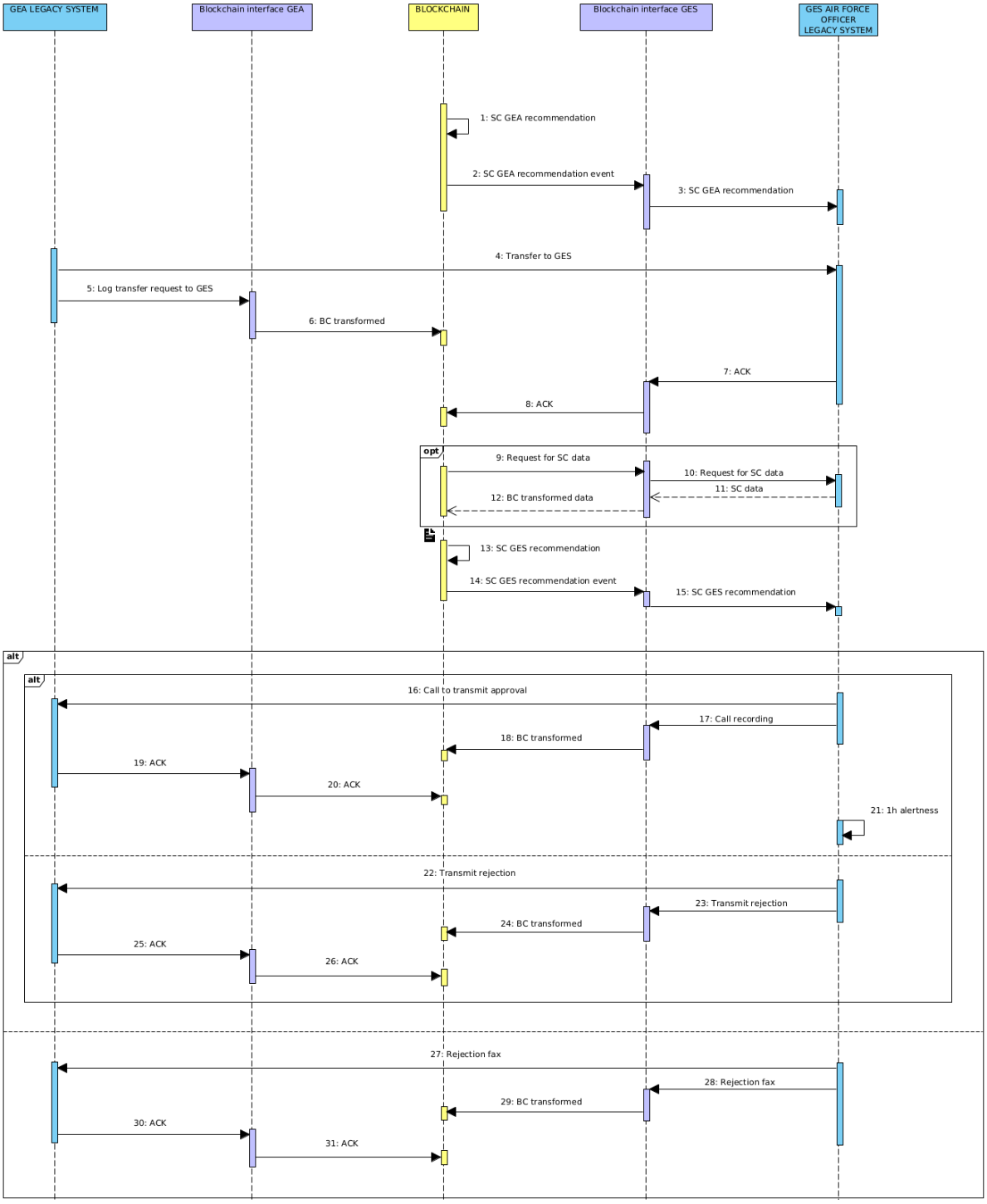
Στις γραμμές 17, 18, 79, 80, 91, 92, 109, 110 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού αεροδιακομιδής ΓΕΑ και αξιωματικού ΔΑΣ ΓΕΣ.



Εικόνα 26: Τμήμα του BPMN για την επικοινωνία ΓΕΑ-ΓΕΣ στο σύστημα legacy



Εικόνα 27: UML Sequence Diagram για την επικοινωνία ΓΕΑ-ΓΕΣ στο σύστημα legacy



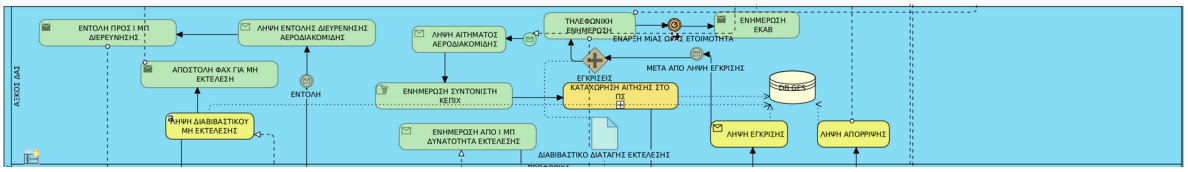
Εικόνα 28: UML Sequence Diagram για την επικοινωνία ΓΕΑ-ΓΕΣ στο παράλληλο σύστημα

4.5.1.5 Αξιωματικός ΔΑΣ ΓΕΣ-ΓΕΣ DB

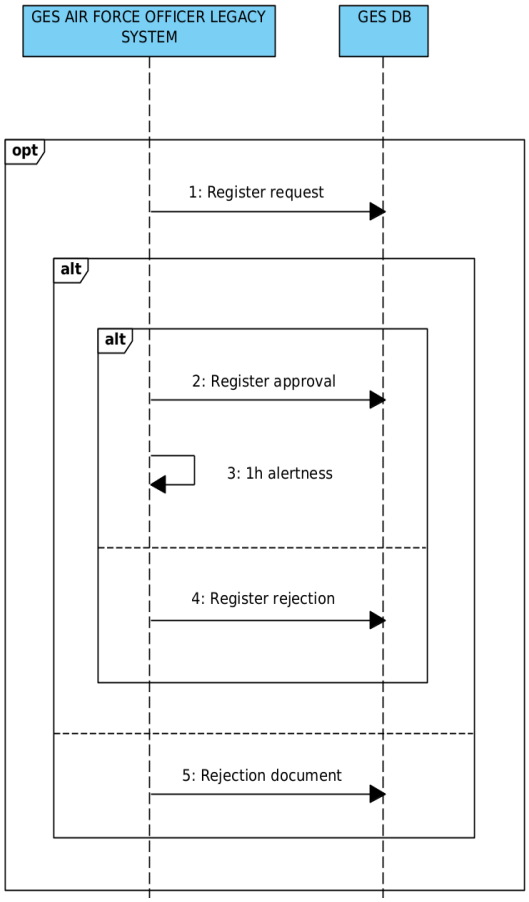
Σημειώσεις

Στις γραμμές 19, 62, 89, 105 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού ΔΑΣ ΓΕΣ και ΓΕΣ DB (βάση δεδομένων ΓΕΣ).

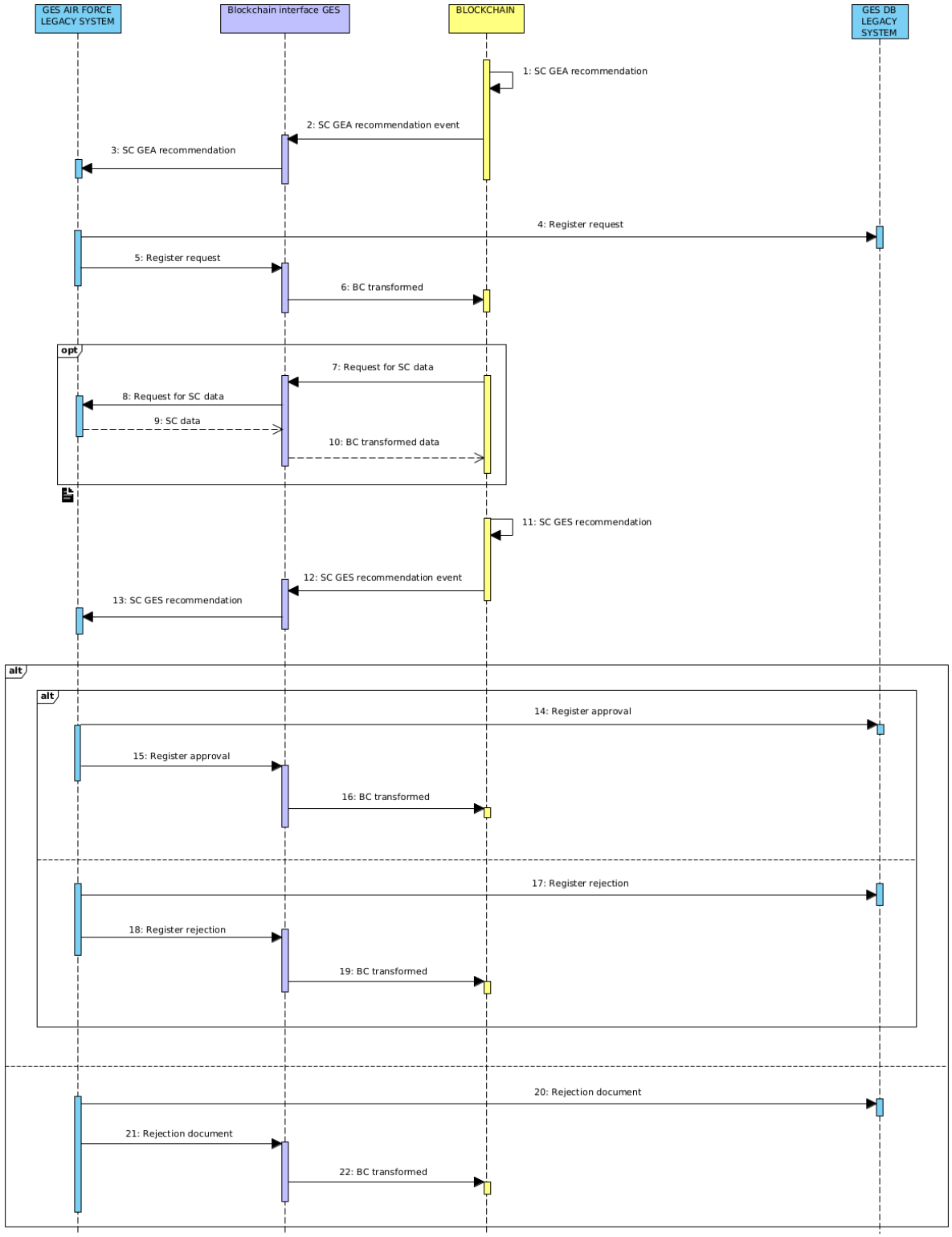
Στο παράλληλο σύστημα δεν υπάρχει αλληλεπίδραση της βάσης δεδομένων ΓΕΣ με το Blockchain, όπως φαίνεται από τα ακόλουθα διαγράμματα.



Εικόνα 29: Τμήμα του BPMN για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-ΓΕΣ DB στο σύστημα legacy



Εικόνα 30: UML Sequence Diagram για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-ΓΕΣ DB στο σύστημα legacy



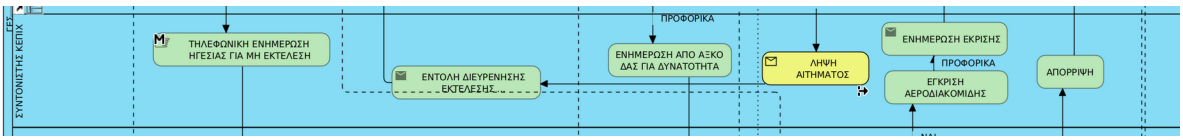
Εικόνα 31: UML Sequence Diagram για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-ΓΕΣ DB στο παράλληλο σύστημα

4.5.1.6 ΓΕΣ DB-ΓΕΣ ΚΕΠΙΧ

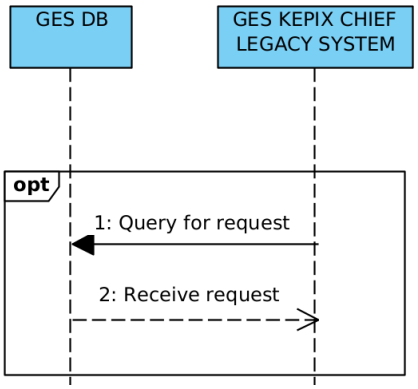
Σημειώσεις

Στη γραμμή 20 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ ΓΕΣ DB (βάση δεδομένων ΓΕΣ) και συντονιστή ΚΕΠΙΧ ΓΕΣ.

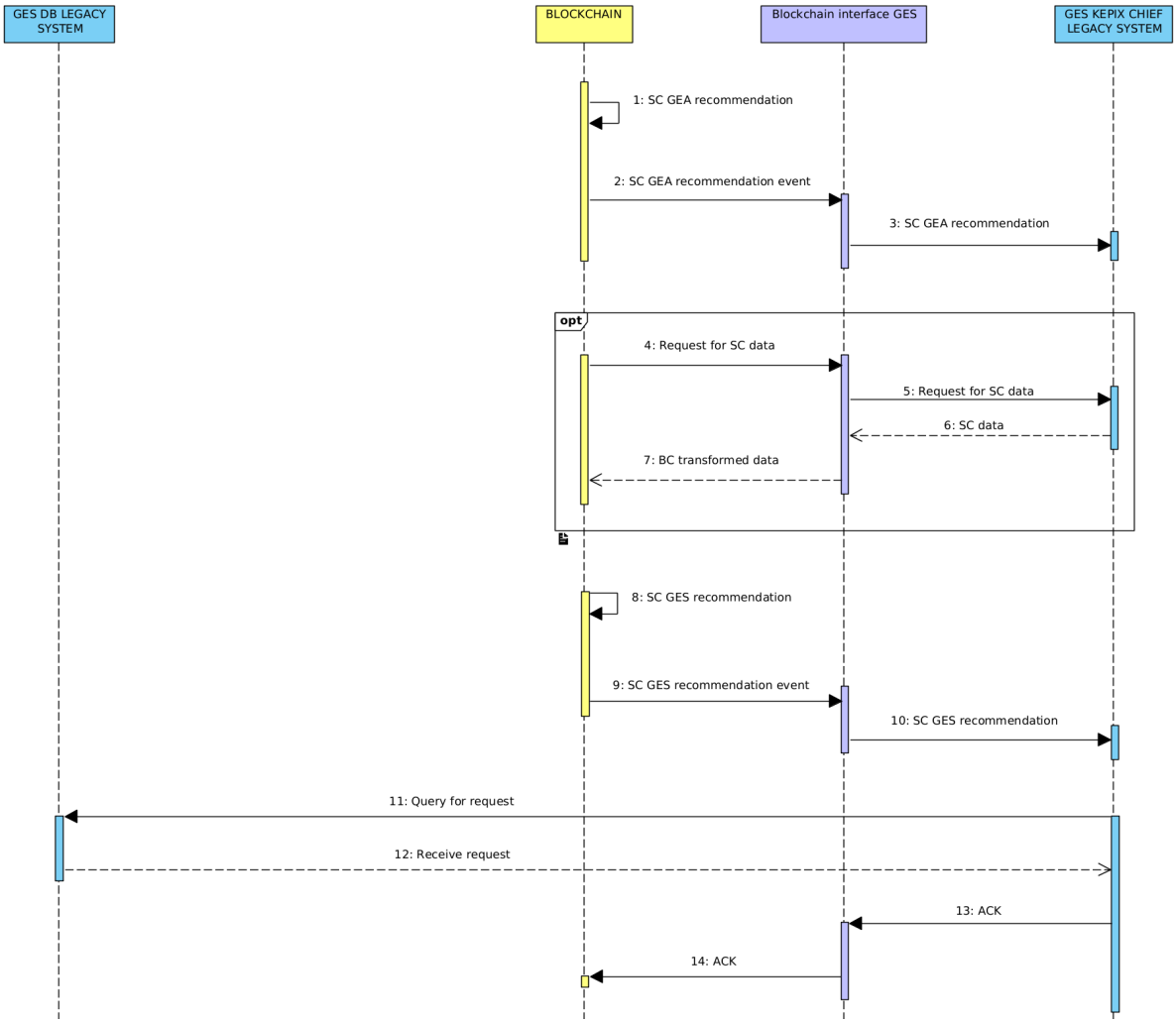
Στο παράλληλο σύστημα δεν υπάρχει αλληλεπίδραση της βάσης δεδομένων ΓΕΣ με το Blockchain, όπως φαίνεται από τα ακόλουθα διαγράμματα.



Εικόνα 32: Τμήμα του BPMN για την επικοινωνία ΓΕΣ DB-συντονιστή ΚΕΠΙΧ ΓΕΣ στο σύστημα legacy



Εικόνα 33: UML Sequence Diagram για την επικοινωνία ΓΕΣ DB-συντονιστή ΚΕΠΙΧ ΓΕΣ στο σύστημα legacy

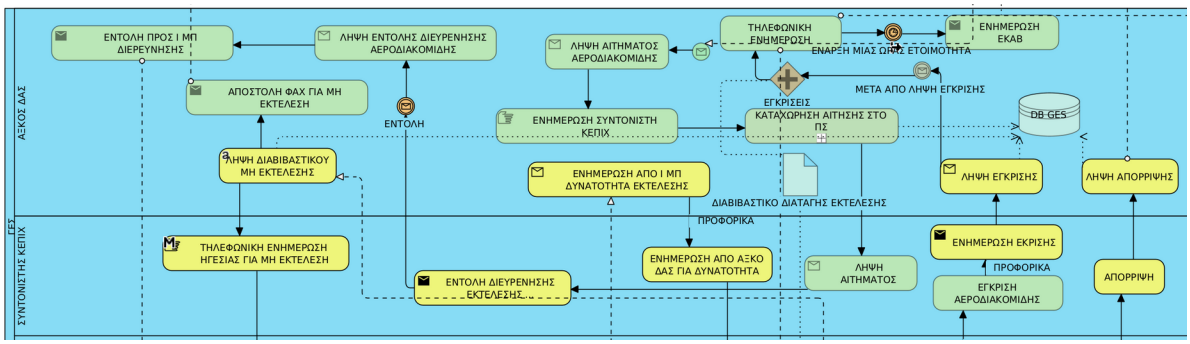


Εικόνα 34: UML Sequence Diagram για την επικοινωνία ΓΕΣ DB-συντονιστή ΚΕΠΙΧ ΓΕΣ στο παράλληλο σύστημα

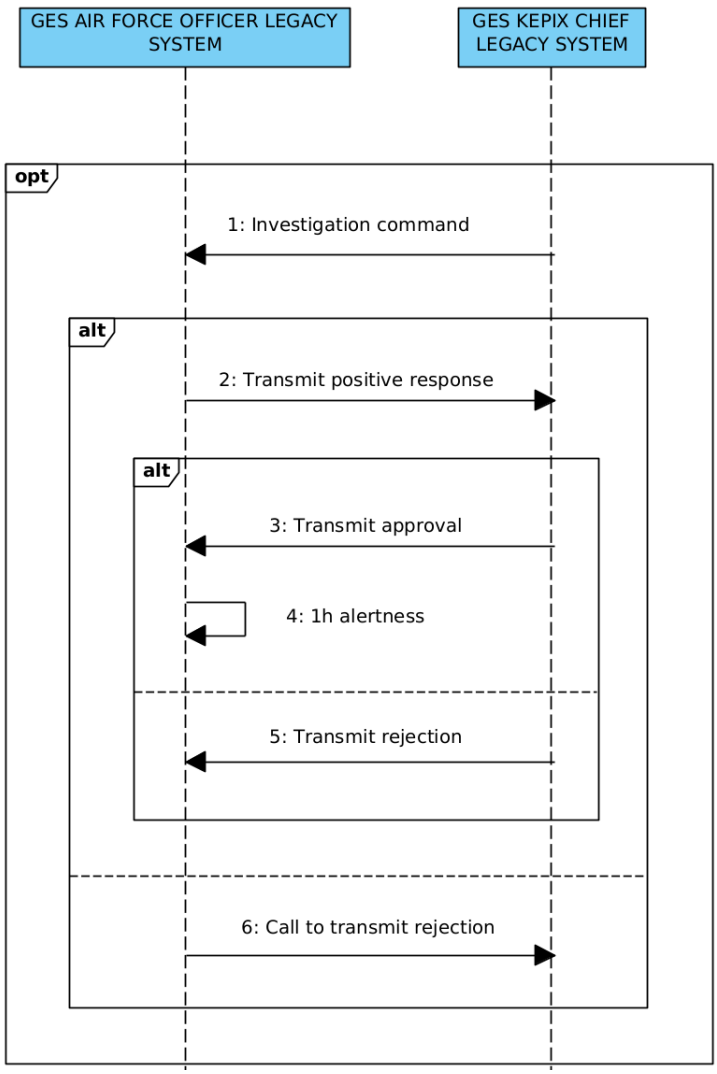
4.5.1.7 Αξιωματικός ΔΑΣ ΓΕΣ-ΓΕΣ ΚΕΠΙΧ

Σημειώσεις

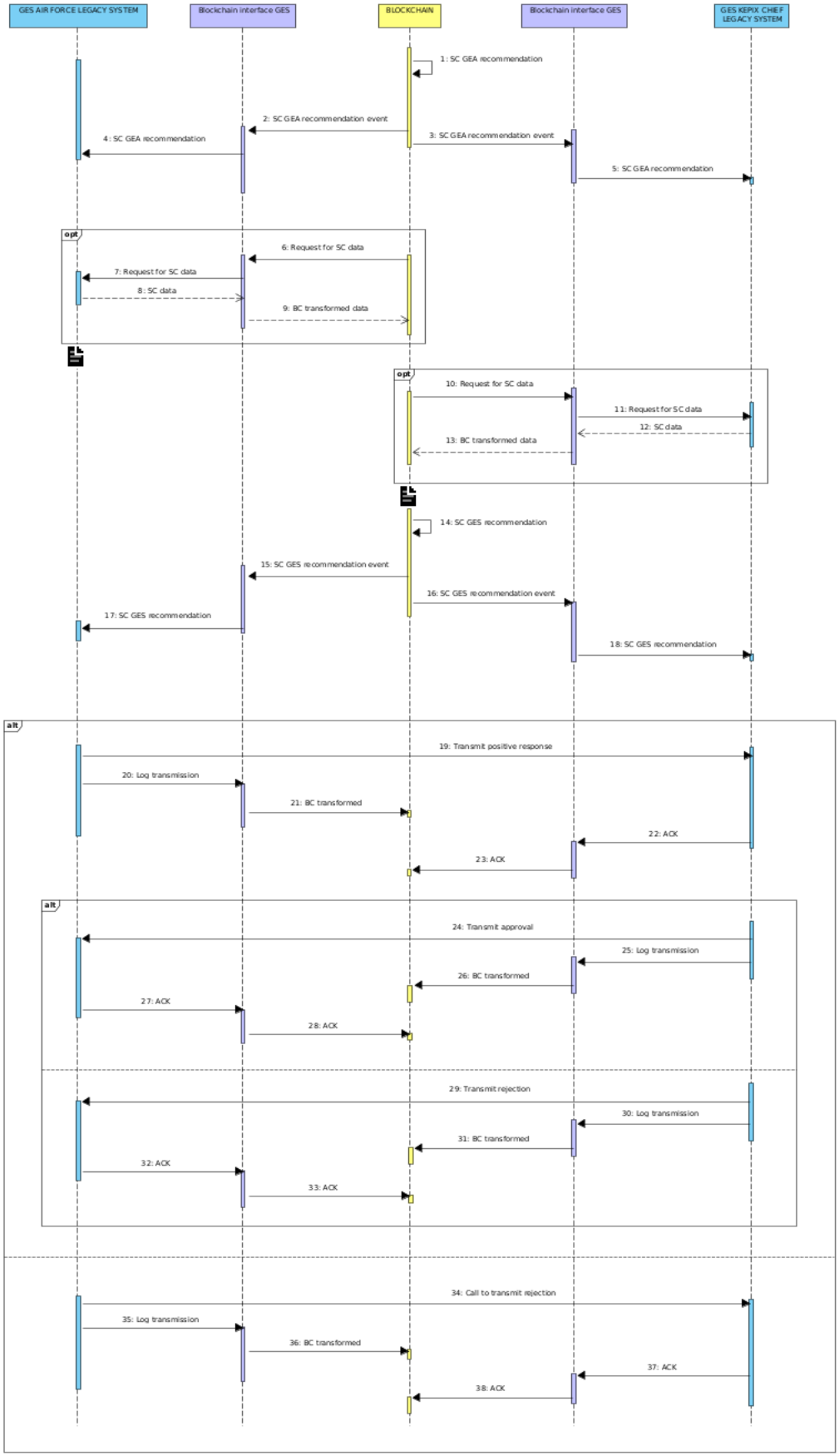
Στις γραμμές 21, 22, 53, 54, 60, 61, 89, 90, 106, 107 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού ΔΑΣ ΓΕΣ και συντονιστή ΚΕΠΙΧ ΓΕΣ.



Εικόνα 35: Τμήμα του BPMN για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-συντονιστή ΚΕΠΙΧ ΓΕΣ στο σύστημα legacy



Εικόνα 36: UML Sequence Diagram για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-συντονιστή ΚΕΠΙΧ ΓΕΣ στο σύστημα legacy

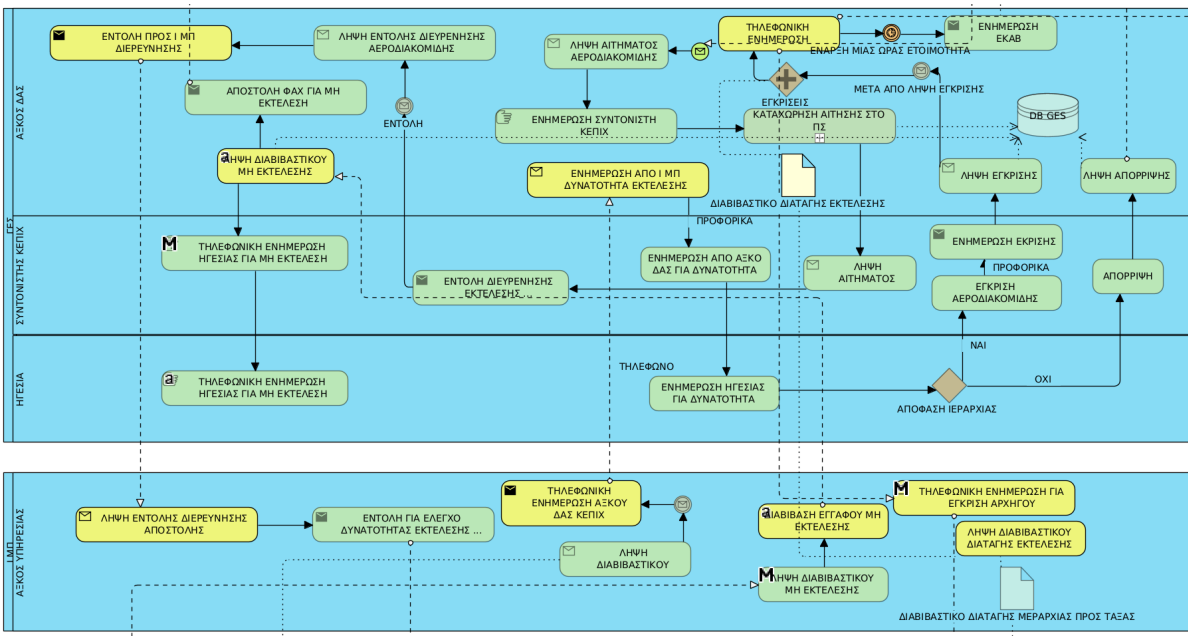


Εικόνα 37: UML Sequence Diagram για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-συντονιστή ΚΕΠΙΧ ΓΕΣ στο παράλληλο σύστημα

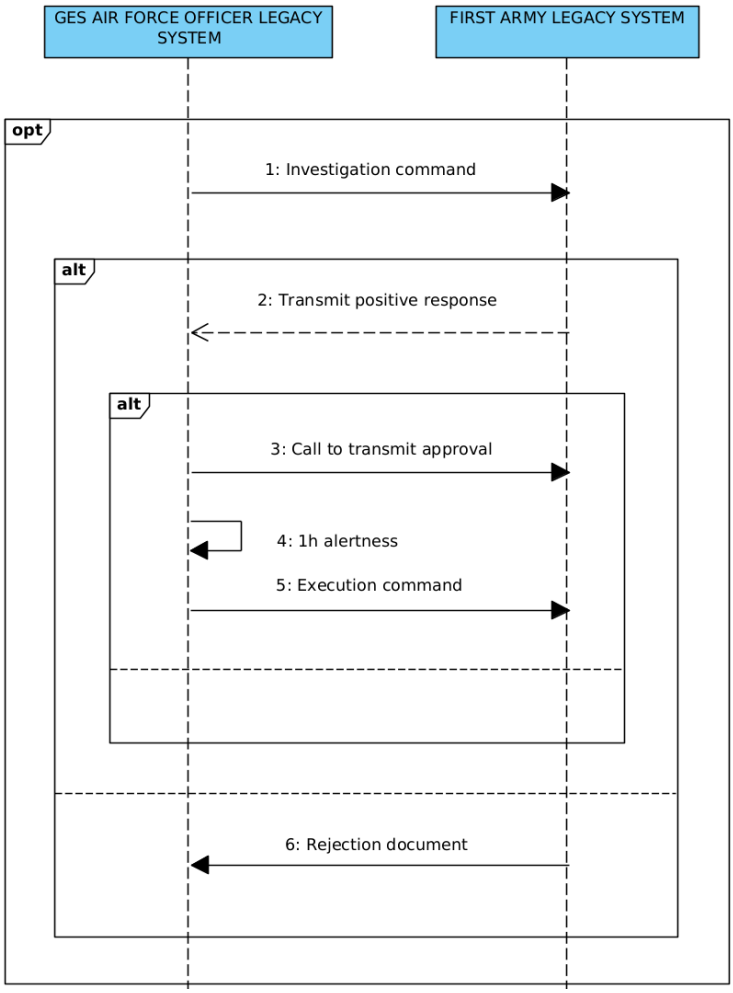
4.5.1.8 Αξιωματικός ΔΑΣ ΓΕΣ-ΙΜΠ

Σημειώσεις

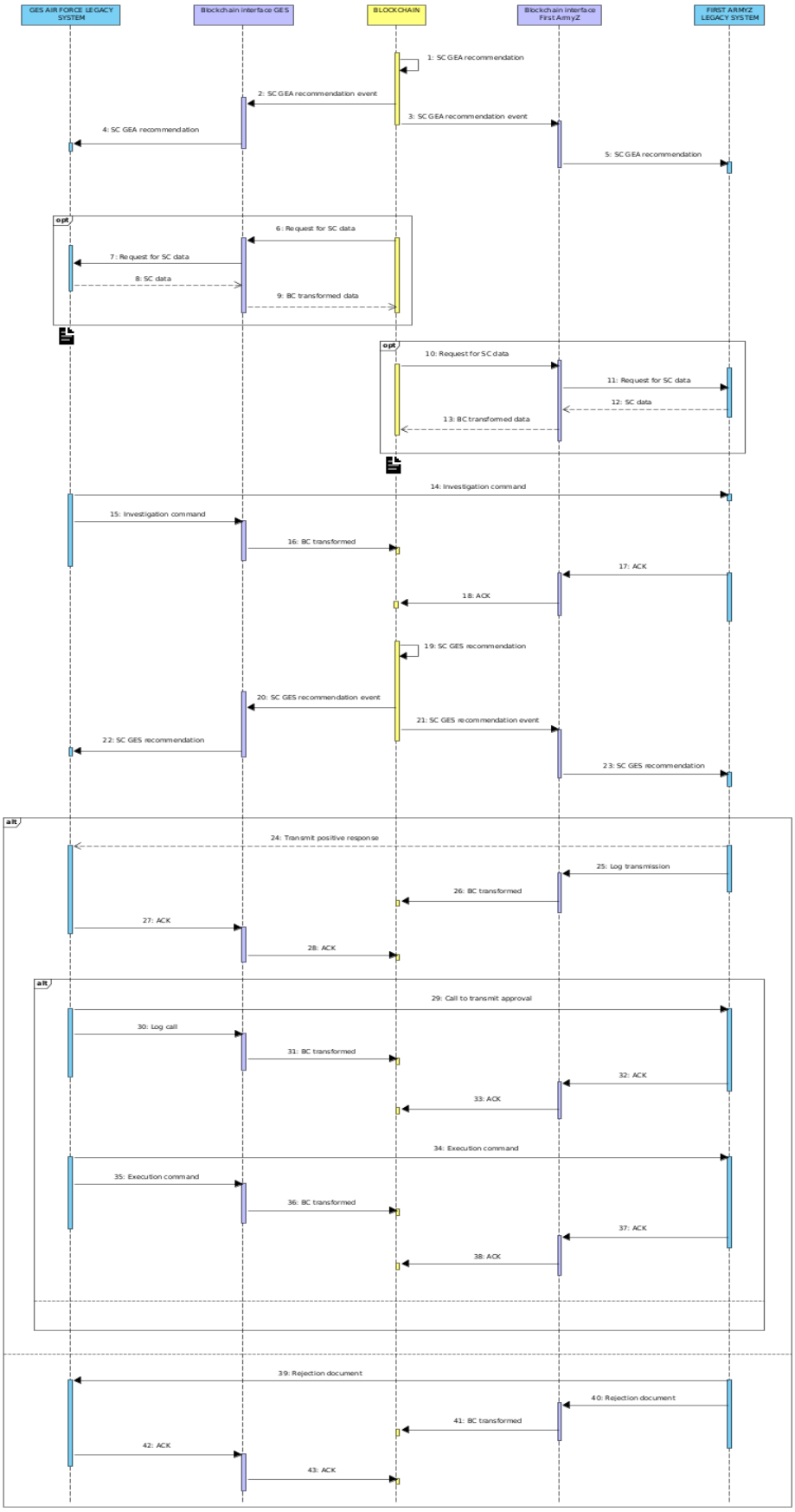
Στις γραμμές 23, 24, 51, 52, 64, 65, 70, 71, 103, 104 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού ΔΑΣ ΓΕΣ και ΙΜΠ.



Εικόνα 38: Τμήμα του BPMN για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-ΙΜΠ στο σύστημα legacy



Εικόνα 39: UML Sequence Diagram για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-ΙΜΠ στο σύστημα legacy

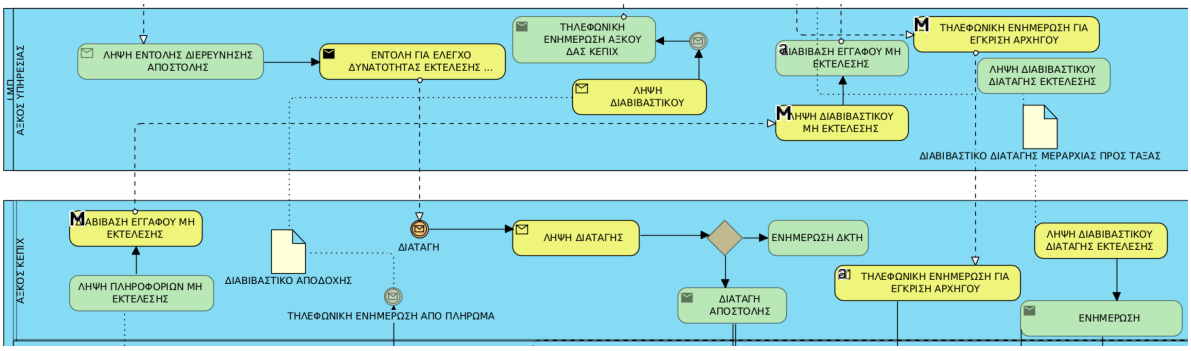


Εικόνα 40: UML Sequence Diagram για την επικοινωνία αξιωματικού ΔΑΣ ΓΕΣ-ΙΜΠ στο παράλληλο σύστημα

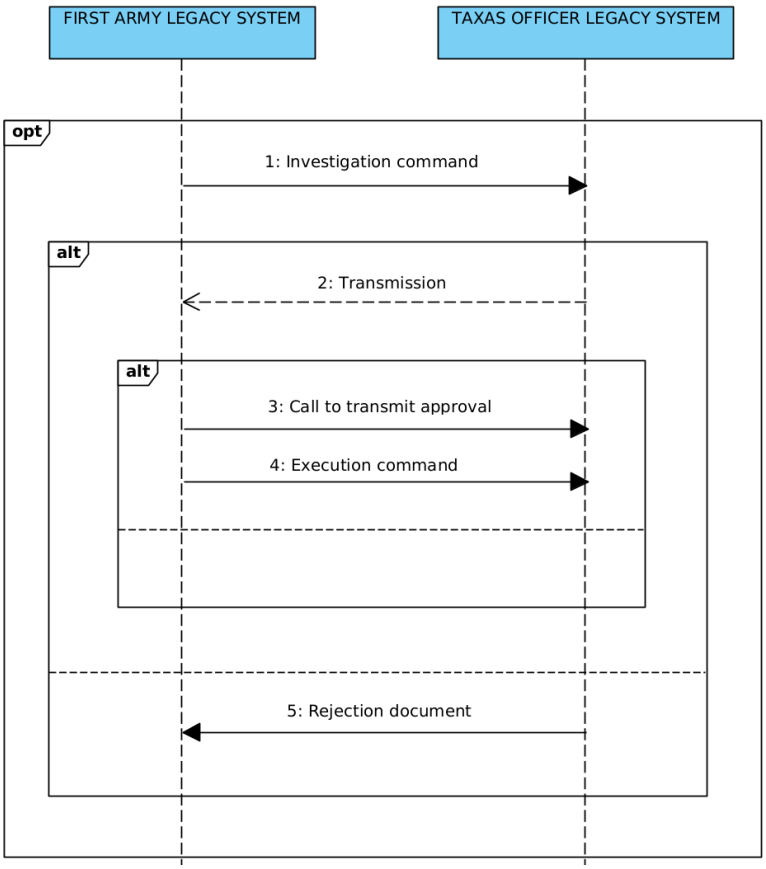
4.5.1.9 ΙΜΠ-Αξιωματικός ΚΕΠΙΧ ΤΑΞΑΣ

Σημειώσεις

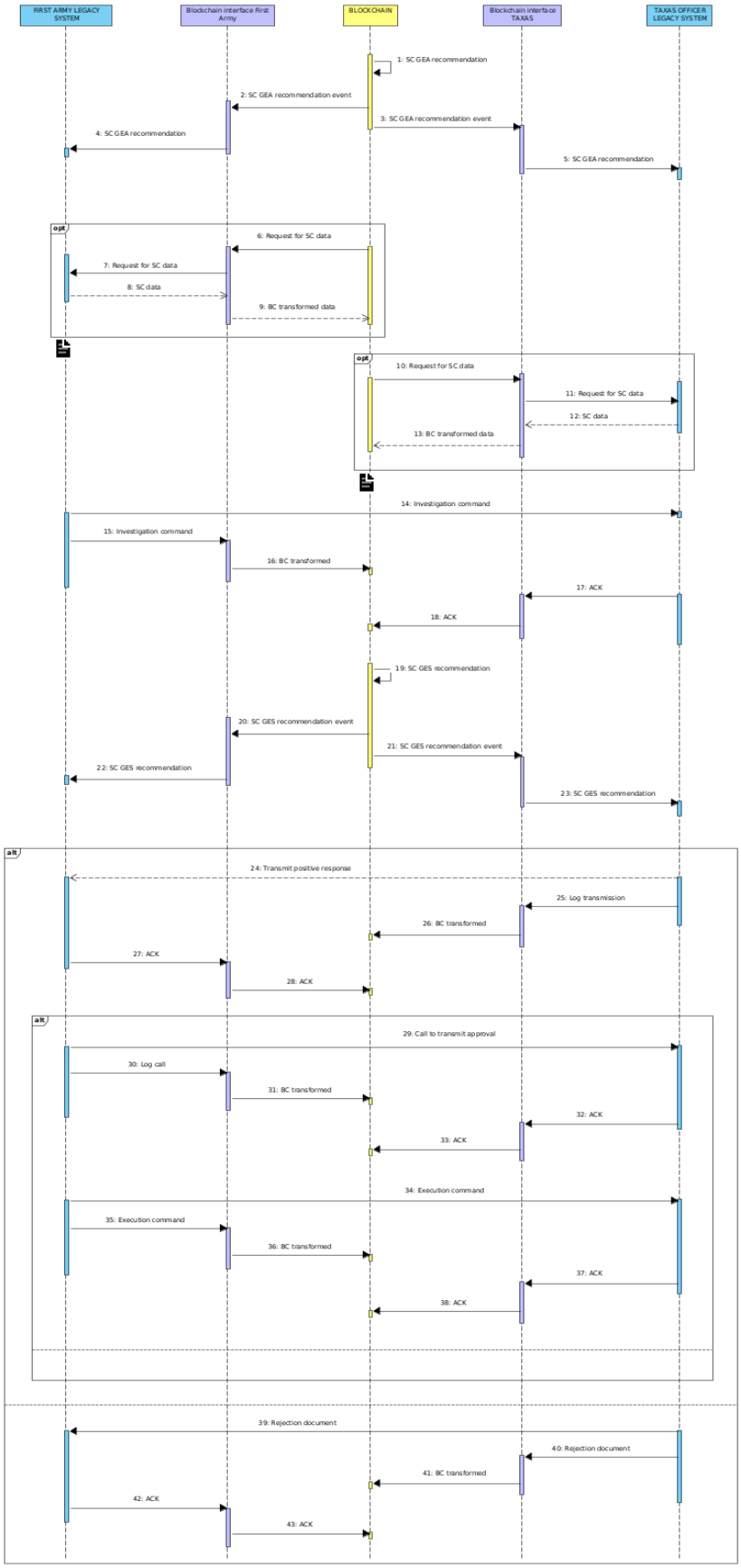
Στις γραμμές 25, 26, 48, 50, 66, 67, 72, 72, 100, 101 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ ΙΜΠ και αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ.



Εικόνα 41: Τμήμα του BPMN για την επικοινωνία ΙΜΠ-αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ στο σύστημα legacy



Εικόνα 42: UML Sequence Diagram για την επικοινωνία ΙΜΠ-αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ στο σύστημα legacy

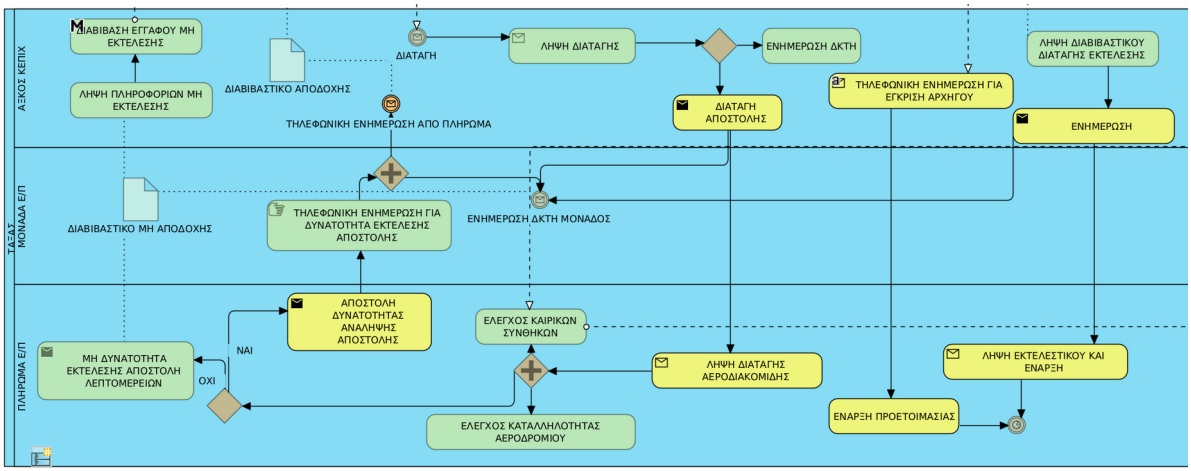


Εικόνα 43: UML Sequence Diagram για την επικοινωνία ΙΜΠ-αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ στο παράλληλο σύστημα

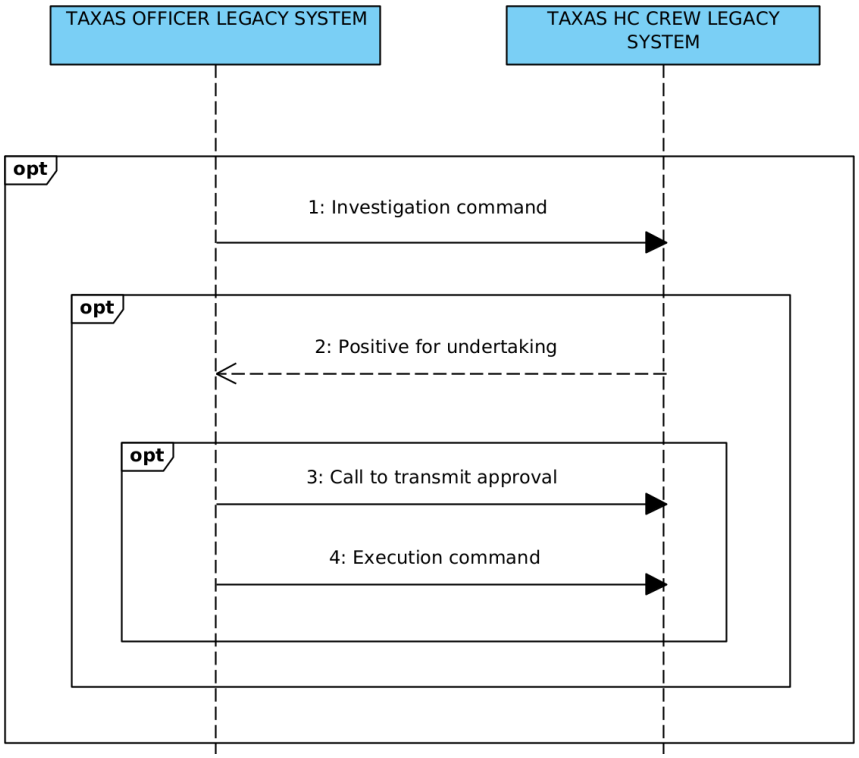
4.5.1.10 Αξιωματικός ΚΕΠΙΧ ΤΑΞΑΣ-Πλήρωμα Ε/Π ΤΑΞΑΣ

Σημειώσεις

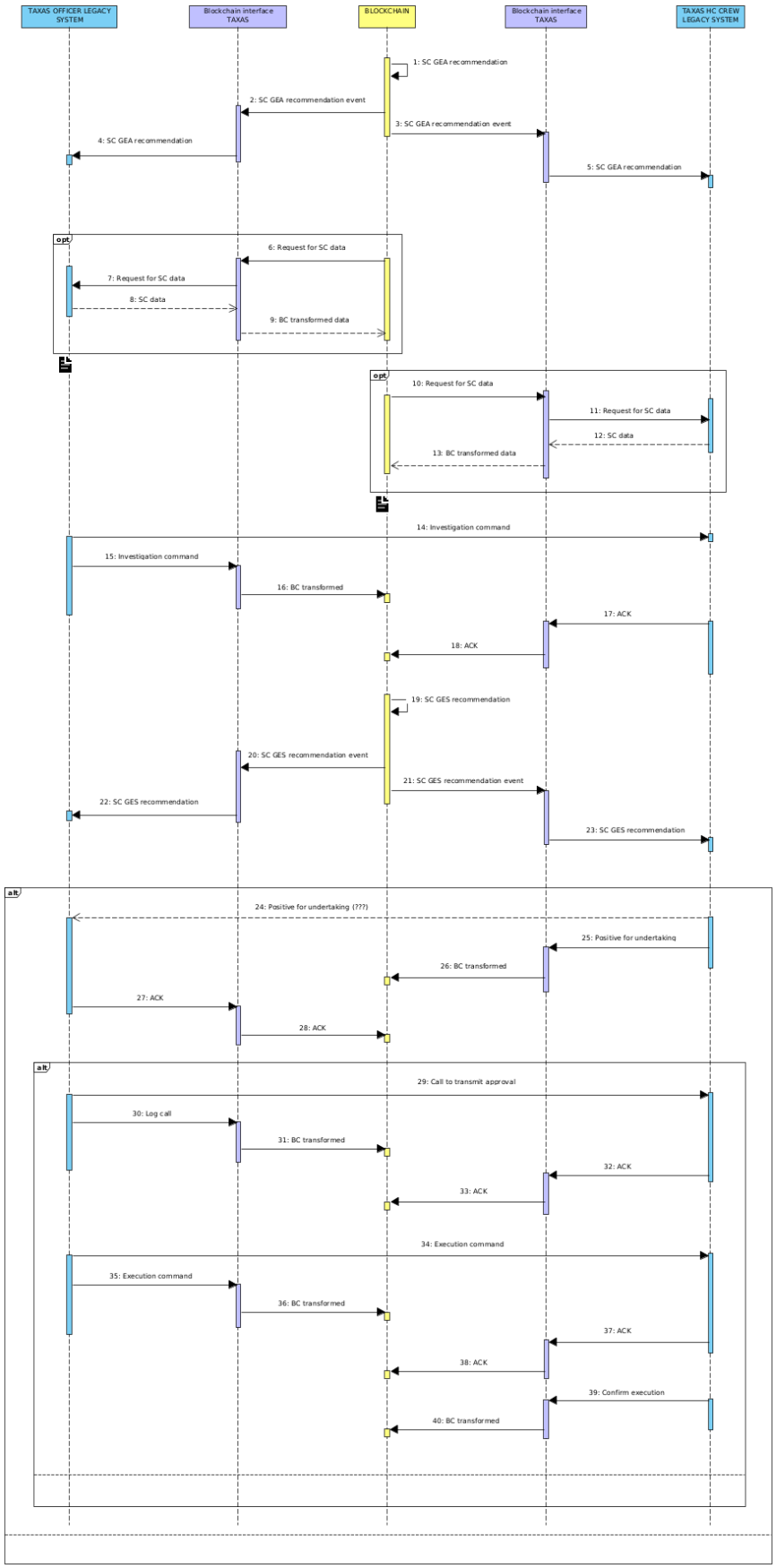
Στις γραμμές 29, 32, 42, 44, 66, 67, 73, 76, 77 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ και πληρώματος Ε/Π ΤΑΞΑΣ.



Εικόνα 44: Τμήμα του BPMN για την επικοινωνία αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ-πληρώματος Ε/Π ΤΑΞΑΣ στο σύστημα legacy



Εικόνα 45: UML Sequence Diagram για την επικοινωνία αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ-πληρώματος Ε/Π ΤΑΞΑΣ στο σύστημα legacy

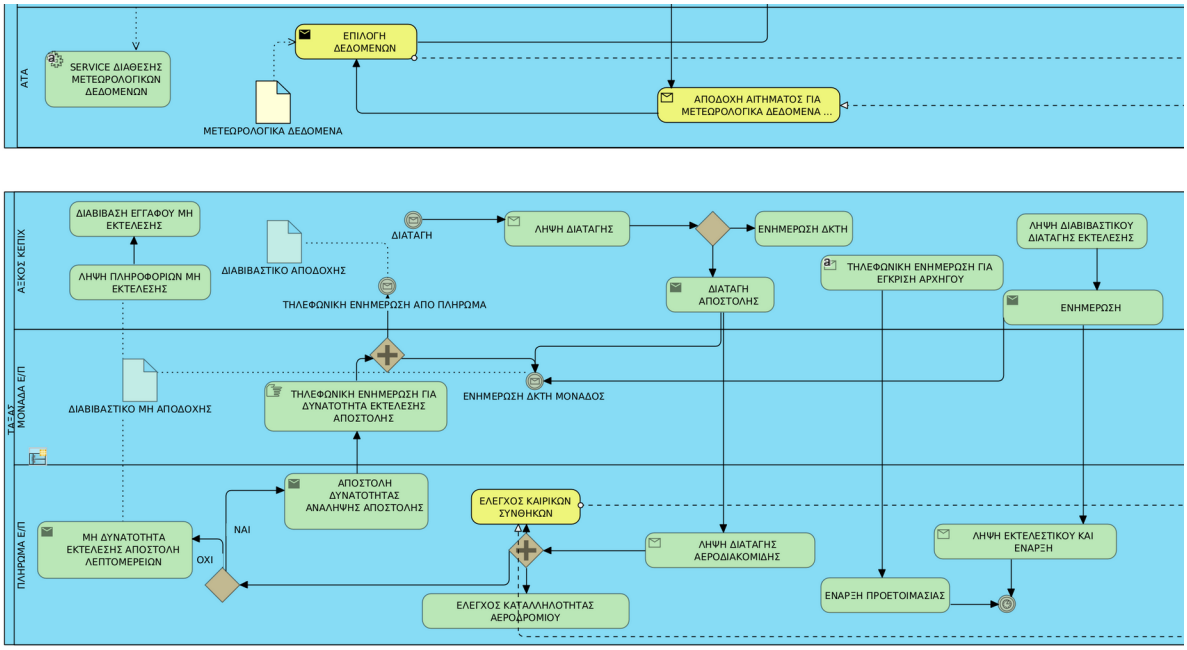


Εικόνα 46: UML Sequence Diagram για την επικοινωνία αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ-πληρώματος Ε/Π ΤΑΞΑΣ στο παράλληλο σύστημα

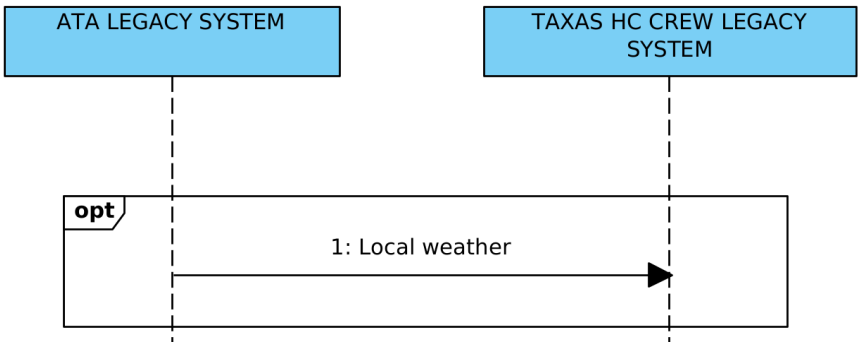
4.5.1.11 ΑΤΑ-Πλήρωμα Ε/Π ΤΑΞΑΣ

Σημειώσεις

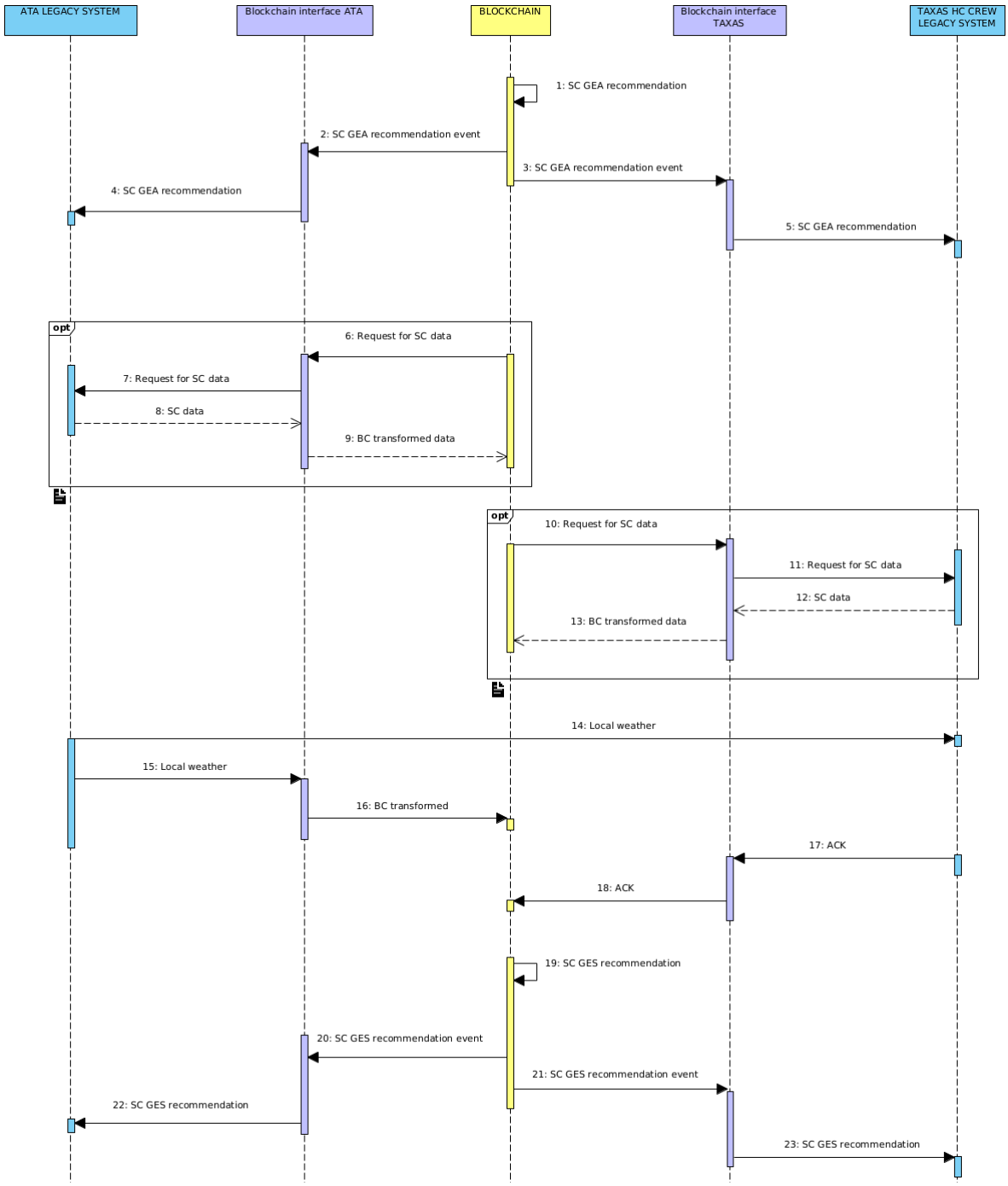
Στις γραμμές 29, 32, 41, 44, 68, 69, 74, 77, 78 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ και πληρώματος Ε/Π ΤΑΞΑΣ.



Εικόνα 47: Τμήμα του BPMN για την επικοινωνία ΑΤΑ-πληρώματος Ε/Π ΤΑΞΑΣ στο σύστημα legacy



Εικόνα 48: UML Sequence Diagram για την επικοινωνία ΑΤΑ-πληρώματος Ε/Π ΤΑΞΑΣ στο σύστημα legacy

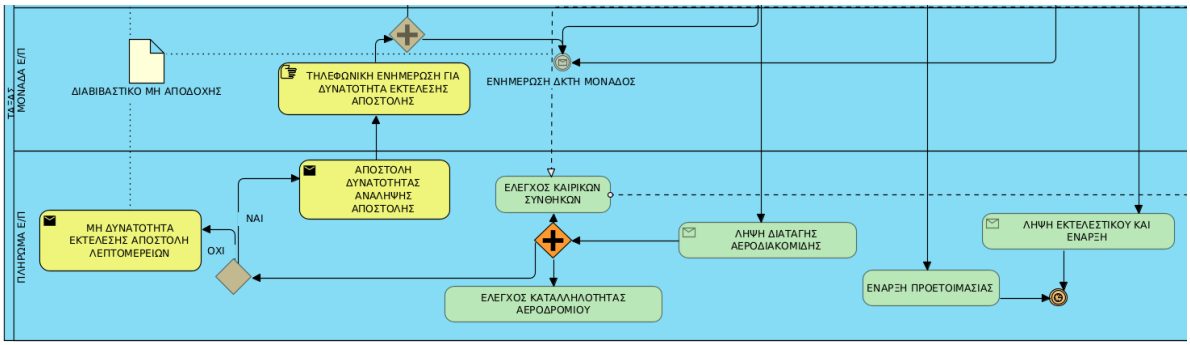


Εικόνα 49: UML Sequence Diagram για την επικοινωνία ΑΤΑ-πληρώματος Ε/Π ΤΑΞΑΣ στο παράλληλο σύστημα

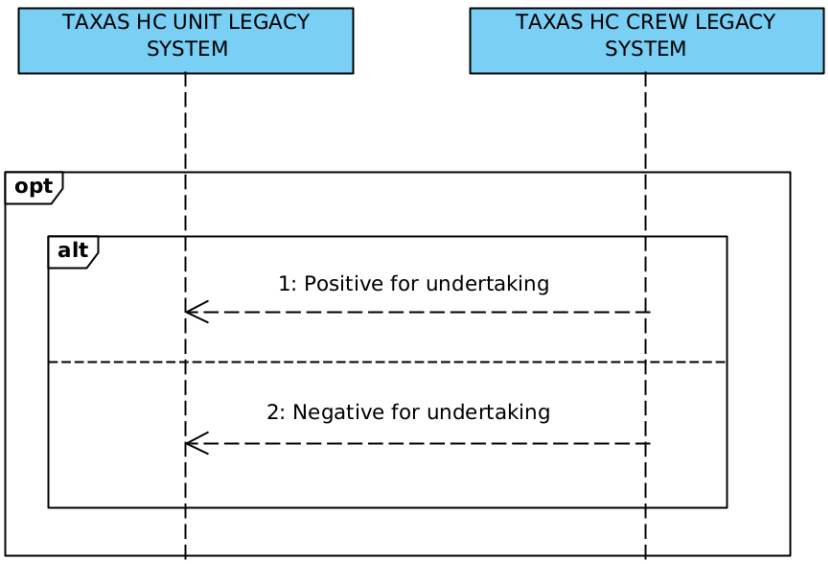
4.5.1.12 Μονάδα Ε/Π ΤΑΞΑΣ-Πλήρωμα Ε/Π ΤΑΞΑΣ

Σημειώσεις

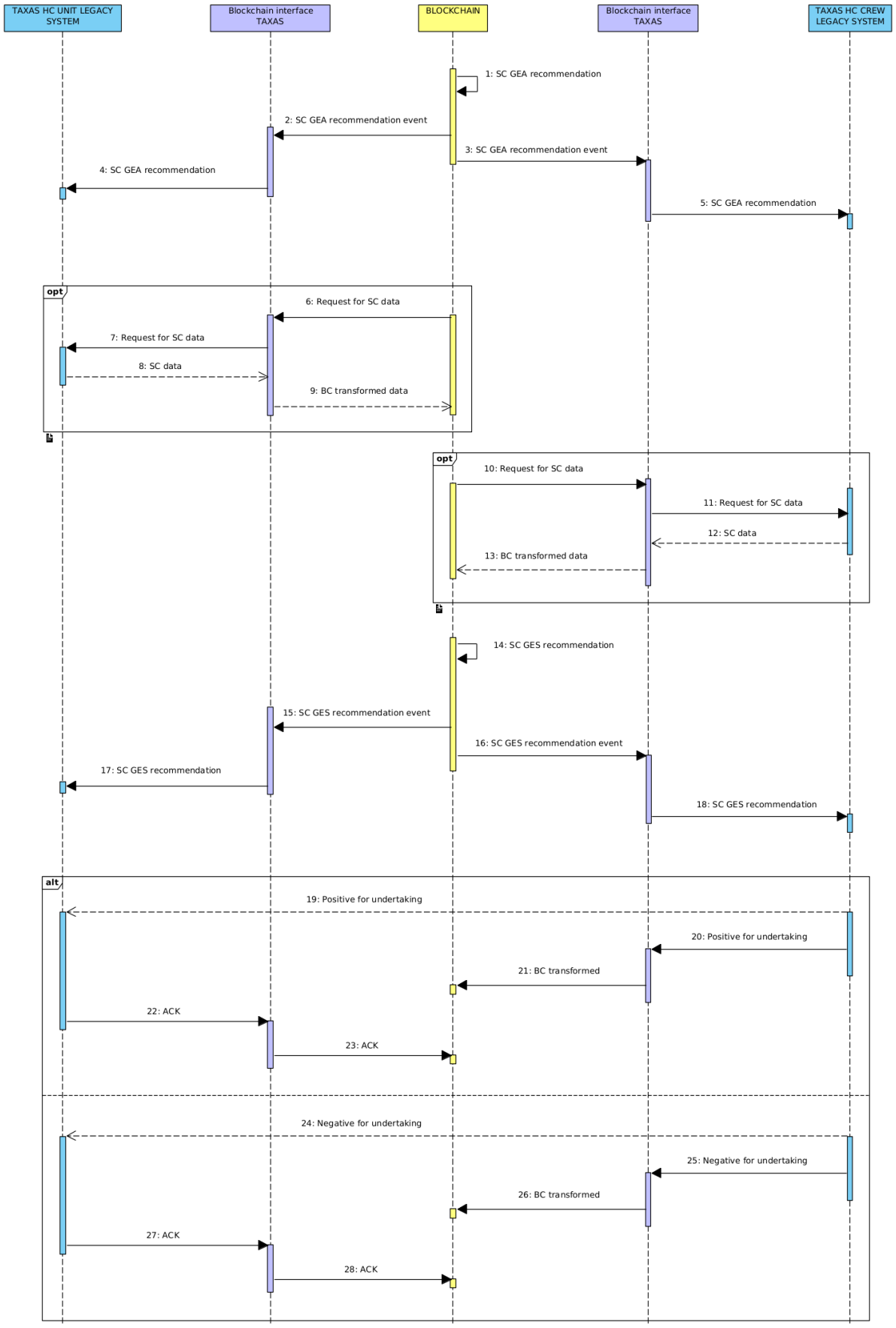
Στις γραμμές 42, 43, 94, 95 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ μονάδας Ε/Π ΤΑΞΑΣ και πληρώματος Ε/Π ΤΑΞΑΣ.



Εικόνα 50: Τμήμα του BPMN για την επικοινωνία μονάδας Ε/Π ΤΑΞΑΣ-πληρώματος Ε/Π ΤΑΞΑΣ στο σύστημα legacy



Εικόνα 51: UML Sequence Diagram για την επικοινωνία μονάδας Ε/Π ΤΑΞΑΣ-πληρώματος Ε/Π ΤΑΞΑΣ στο σύστημα legacy



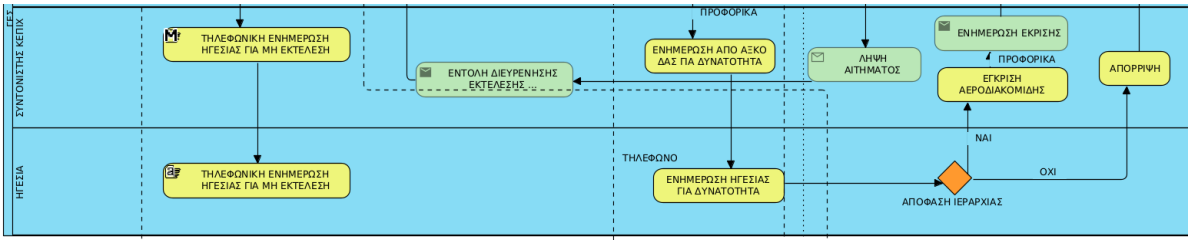
Εικόνα 52: UML Sequence Diagram για την επικοινωνία μονάδας Ε/Π ΤΑΞΑΣ-πληρώματος Ε/Π ΤΑΞΑΣ στο παράλληλο σύστημα

4.5.1.13 ΓΕΣ ΚΕΠΙΧ-Ηγεσία ΓΕΣ

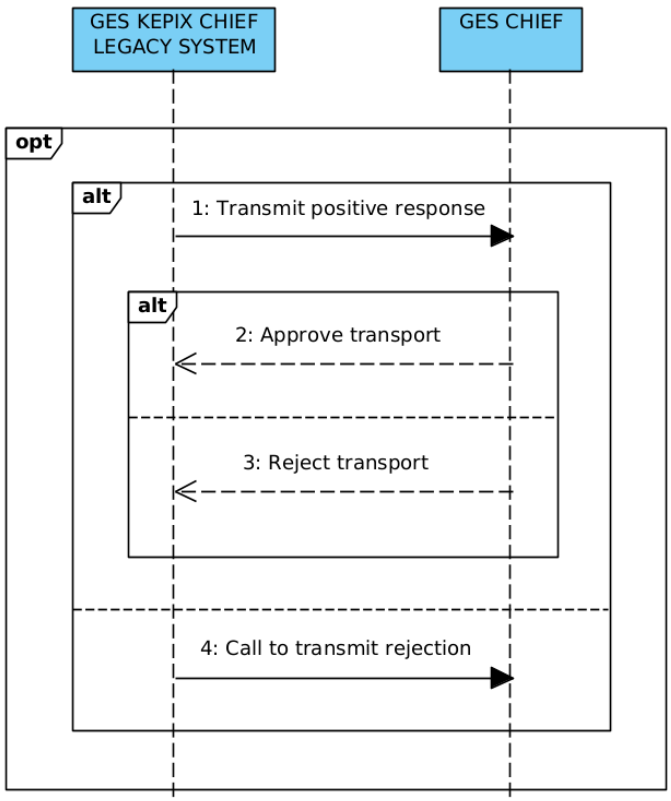
Σημειώσεις

Στις γραμμές 55, 56, 58, 59, 87, 88, 108 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ συντονιστή ΚΕΠΙΧ ΓΕΣ και ηγεσίας ΓΕΣ.

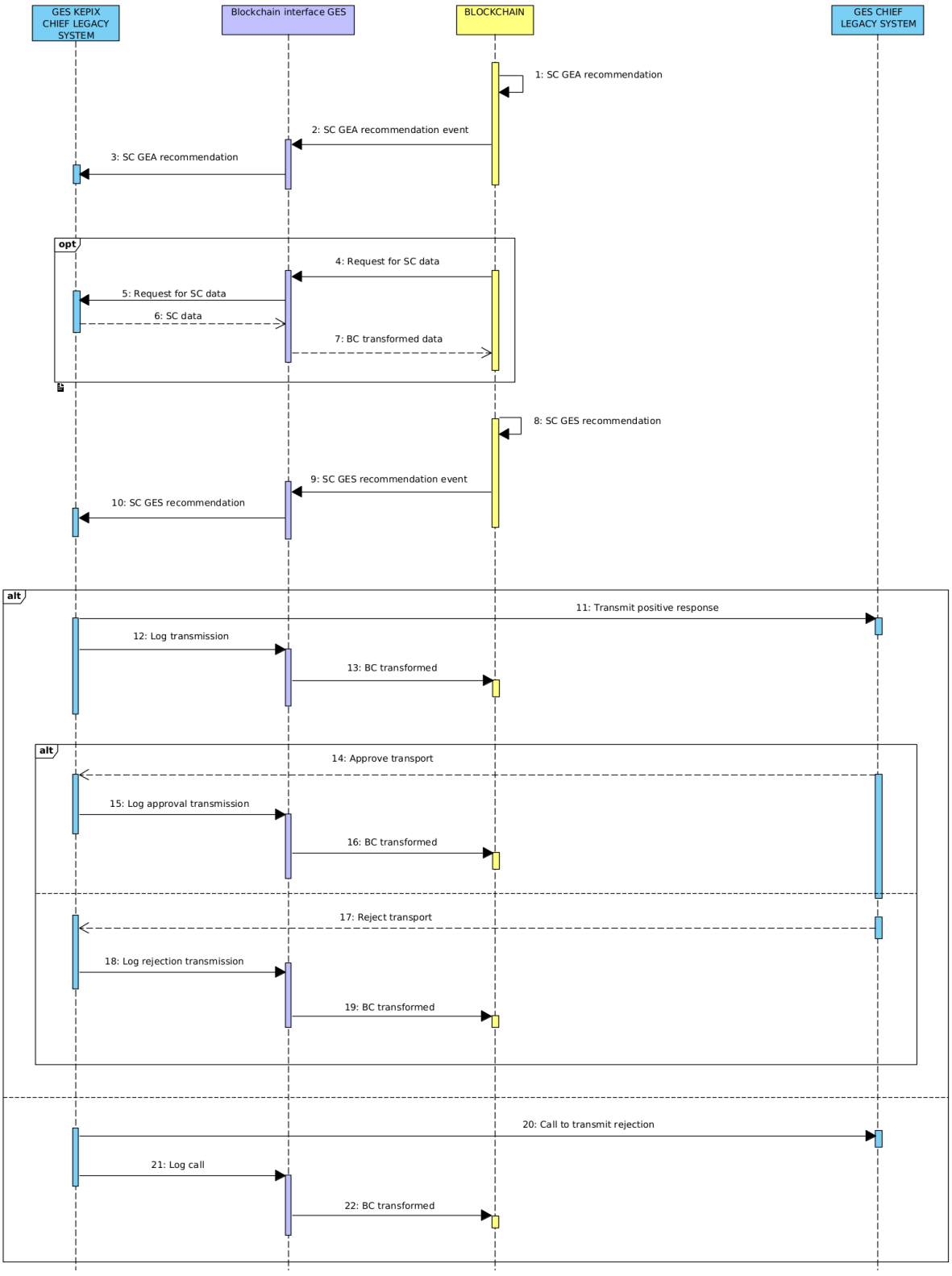
Στο παράλληλο σύστημα η ηγεσία ΓΕΣ δεν έχει πρόσβαση στο Blockchain, παρά μόνον μέσω του συντονιστή ΚΕΠΙΧ ο οποίος καταγράφει τις επικοινωνίες και ενέργειές της.



Εικόνα 53: Τμήμα του BPMN για την επικοινωνία συντονιστή ΚΕΠΙΧ ΓΕΣ-ηγεσίας ΓΕΣ στο σύστημα legacy



Εικόνα 54: UML Sequence Diagram για την επικοινωνία συντονιστή ΚΕΠΙΧ ΓΕΣ-ηγεσίας ΓΕΣ στο σύστημα legacy

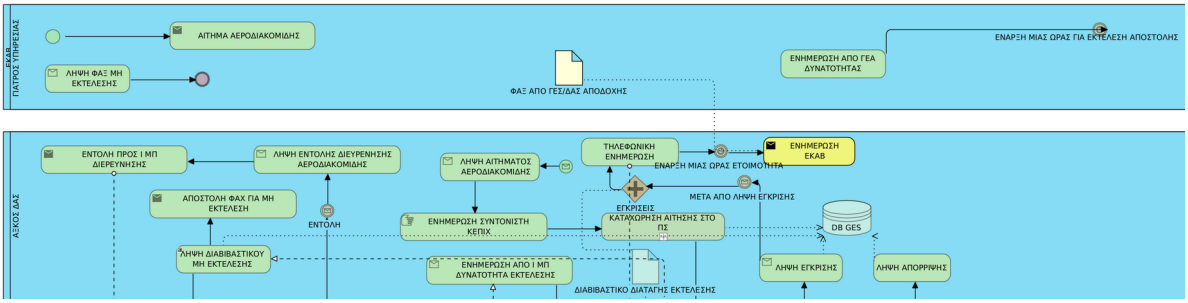


Εικόνα 55: UML Sequence Diagram για την επικοινωνία συντονιστή ΚΕΠΙΧ ΓΕΣ-ηγεσίας ΓΕΣ στο παράλληλο σύστημα

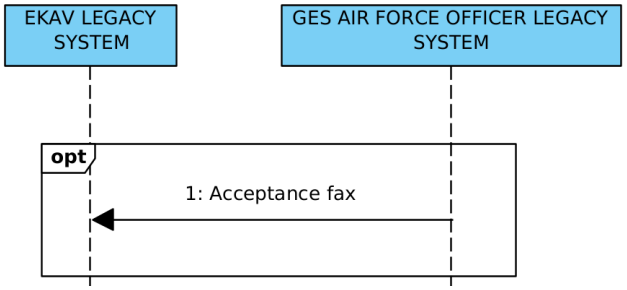
4.5.1.14 ΕΚΑΒ-Αξιωματικός ΔΑΣ ΓΕΣ

Σημειώσεις

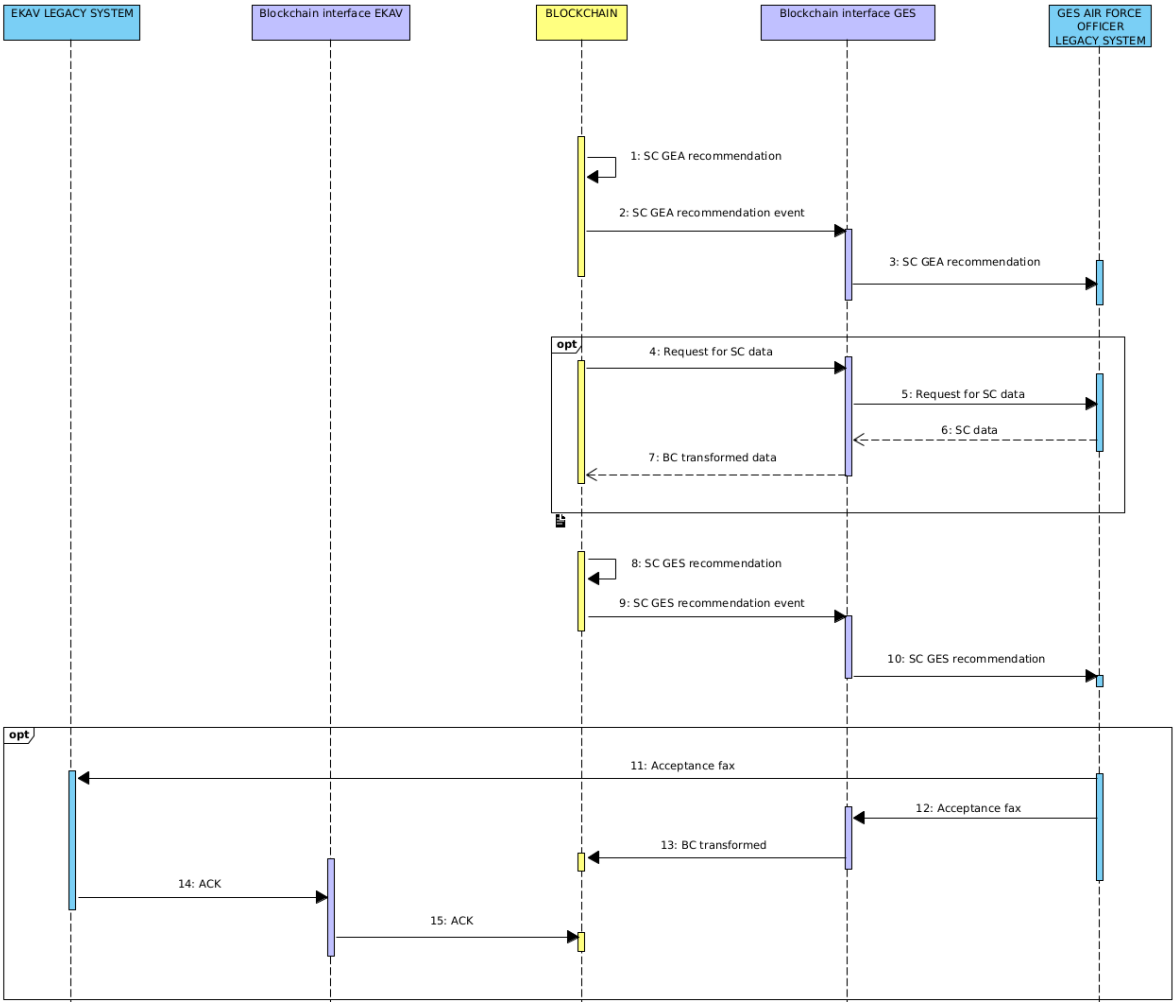
Στις γραμμές 85, 86 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ ΕΚΑΒ και αξιωματικού ΔΑΣ ΓΕΣ.



Εικόνα 56: Τμήμα του BPMN για την επικοινωνία ΕΚΑΒ-αξιωματικού ΔΑΣ ΓΕΣ στο σύστημα legacy



Εικόνα 57: UML Sequence Diagram για την επικοινωνία ΕΚΑΒ-αξιωματικού ΔΑΣ ΓΕΣ στο σύστημα legacy

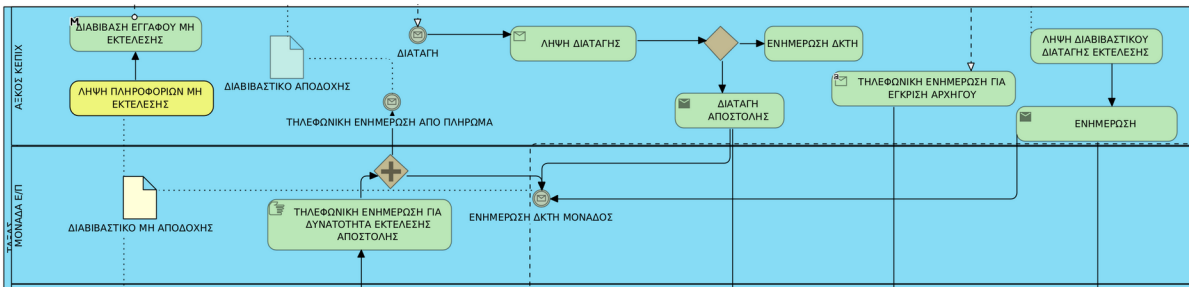


Εικόνα 58: UML Sequence Diagram για την επικοινωνία ΕΚΑΒ-αξιωματικού ΔΑΣ ΓΕΣ στο παράλληλο σύστημα

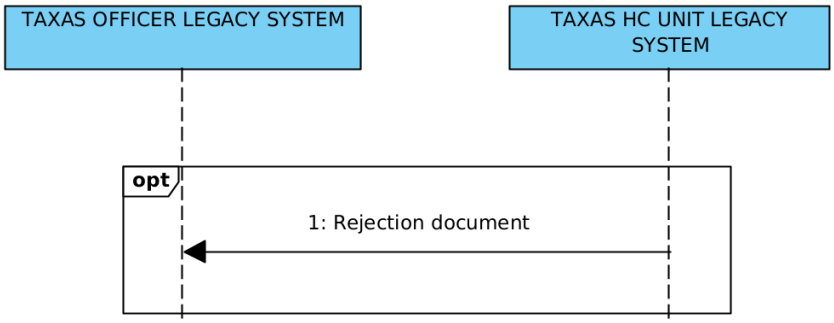
4.5.1.15 Αξιωματικός ΚΕΠΙΧ ΤΑΞΑΣ-Μονάδα Ε/Π ΤΑΞΑΣ

Σημειώσεις

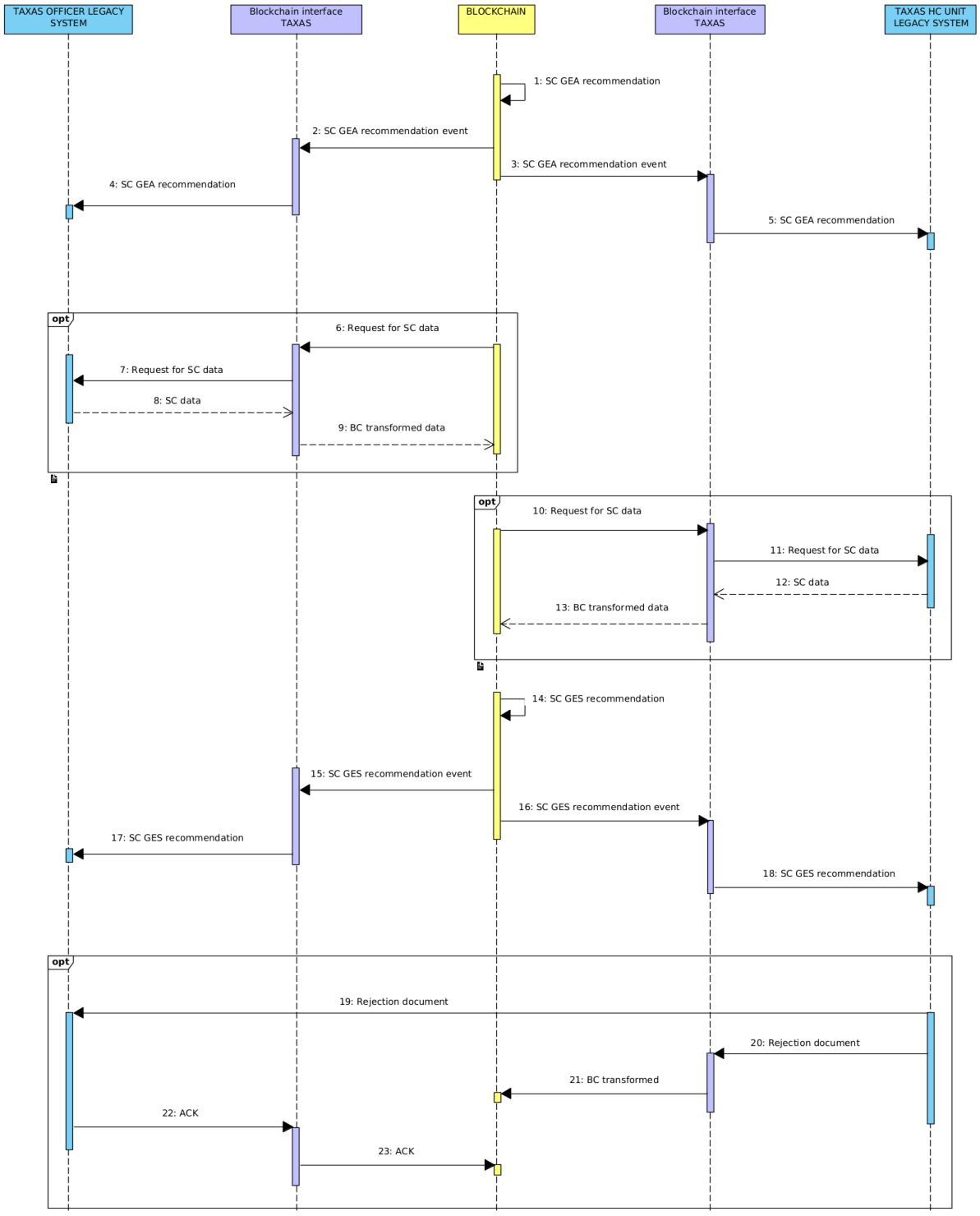
Στις γραμμές 99, 100 του Πίνακα 9 περιέχονται τα σχετικά δεδομένα που ανταλλάσσονται μεταξύ αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ και μονάδας Ε/Π ΤΑΞΑΣ.



Εικόνα 59: Τμήμα του BPMN για την επικοινωνία αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ-μονάδας Ε/Π ΤΑΞΑΣ στο σύστημα legacy



Εικόνα 60: UML Sequence Diagram για την επικοινωνία αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ-μονάδας Ε/Π ΤΑΞΑΣ στο σύστημα legacy



Εικόνα 61: UML Sequence Diagram για την επικοινωνία αξιωματικού ΚΕΠΙΧ ΤΑΞΑΣ-μονάδας Ε/Π ΤΑΞΑΣ στο παράλληλο σύστημα

5 Επίλογος

5.1 Σύνοψη

Στην εργασία εξετάστηκε το πλαίσιο λειτουργίας των συστημάτων κρίσιμης αποστολής, μελετώντας συγκεκριμένα την περίπτωση του συστήματος αεροδιακομιδής. Εκτέθηκαν οι ευκαιρίες, οι ανάγκες και οι περιορισμοί που προκύπτουν από την εξεταζόμενη υιοθέτηση της τεχνολογίας Blockchain και αναλύθηκε το φάσμα των πιθανών επιλογών ως προς την ενσωμάτωσή της.

Η κύρια συνεισφορά της εργασίας είναι η πρότασή μας για παράλληλη λειτουργία του υπάρχοντος συστήματος με το σύστημα Blockchain, με σκοπό την αναλλοίωτη καταγραφή συμβάντων της διαδικασίας αεροδιακομιδής και τη χρήση παθητικών smart contracts για παραγωγή προτάσεων βάσει των διατυπωμένων κανόνων εκτέλεσης. Η αρχιτεκτονική βασίζεται στην ιδέα των διεπαφών Blockchain που μεσολαβούν μεταξύ του υπάρχοντος συστήματος και του Blockchain ώστε να ελαχιστοποιηθεί η παρέμβαση στο υπάρχον σύστημα.

Το προτεινόμενο σύστημα μοντελοποιήθηκε με χρήση UML Sequence Diagrams και έγινε ανάλυση των δεδομένων όπως διατηρούνται στο υπάρχον σύστημα και όπως θα μετασχηματίζονταν για την καταχώρησή τους στο Blockchain.

5.2 Ανοικτά θέματα

Μελλοντικές προεκτάσεις της εργασίας θα μπορούσαν να περιλαμβάνουν:

- Υλοποίηση και δοκιμή του προτεινόμενου συστήματος ώστε να αξιολογηθεί η αρχιτεκτονική ως προς την επίτευξη των στόχων και ως προς τους περιορισμούς της.

- Μελέτη για την αρχιτεκτονική και την υλοποίηση της αποθήκευσης off-chain και του μετασχηματισμού των διάφορων μορφών δεδομένων που εμφανίζονται στο σύστημα αεροδιακομιδής (φαξ και σαρωμένα

έγγραφα, καταγραφές τηλεφωνικών κλήσεων, χάρτες, μετεωρολογικά δεδομένα κτλ.)

- Ανάλυση της διαδικασίας και της υλοποίησης για τη μετάβαση από ένα σύστημα παθητικών smart contracts σε ένα σύστημα όπου η λήψη αποφάσεων γίνεται εντός του Blockchain.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” 2009 [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[2] B. Ramamurthy, *Blockchain in action*. 2020 [Online]. Available: https://www.manning.com/books/blockchain-in-action

[3] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. O’Reilly Media, Inc., 2015.

[4] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain Technology in Healthcare: A Systematic Review,” *Healthcare*, vol. 7, no. 2, p. 56, Jun. 2019, doi: 10.3390/healthcare7020056. [Online]. Available: https://www.mdpi.com/2227-9032/7/2/56. [Accessed: 11-Jul-2021]

[5] ISO/TC 307, “Blockchain and distributed ledger technologies — Vocabulary,” International Organization for Standardization, ISO 22739:2020, 2020 [Online]. Available: https://www.iso.org/standard/73771.html

[6] N. Szabo, “Smart Contracts,” 1994. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. [Accessed: 12-Jul-2021]

[7] K. Sultan, U. Ruhi, and R. Lakhani, “Conceptualizing Blockchains: Characteristics & Applications,” presented at the IADIS International Conference Information Systems 2018, 2018, pp. 49–57 [Online]. Available: http://www.iadisportal.org/digital-library/conceptualizing-blockchains-characteristics-applications. [Accessed: 21-Jun-2021]

[8] B. Podgorelec, V. Keršič, and M. Turkanović, “Analysis of Fault Tolerance in Permissioned Blockchain Networks,” 2019, pp. 1–6, doi: 10.1109/ICAT47117.2019.8938836.

[9] S. Nakamoto, “Bitcoin v0.1 released,” *The Mail Archive*, 09-Jan-2009. [Online]. Available: https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html. [Accessed: 12-Jul-2021]

[10] “Permissioned vs Permissionless Blockchains,” *101 Blockchains*, 28-May-2020. [Online]. Available: https://101blockchains.com/permissioned-vs-permissionless-blockchains/. [Accessed: 12-Jul-2021]

[11] V. Buterin, “A next-generation smart contract and decentralized application platform,” 2013 [Online]. Available: https://translatewhitepaper.com/wp-content/uploads/2021/04/EthereumOrijinal-ETH-English.pdf

[12] D. G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” p. 40, Jul. 2021 [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[13] J. Polge, J. Robert, and Y. Le Traon, “Permissioned blockchain frameworks in the industry: A comparison,” *ICT Express*, vol. 7, no. 2, pp. 229–233, Jun. 2021, doi: 10.1016/j.icte.2020.09.002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959520301909. [Accessed: 12-Jun-2021]

[14] S. Voshmgir, *Token economy: how blockchains and smart contracts revolutionize the economy*. 2019 [Online]. Available: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

[15] Y. Bakos, H. Halaburda, and C. Mueller-Bloch, “When permissioned blockchains deliver more decentralization than permissionless,” *Commun. ACM*, vol. 64, no. 2, pp. 20–22, Jan. 2021, doi: 10.1145/3442371. [Online]. Available: https://doi.org/10.1145/3442371. [Accessed: 24-Jun-2021]

[16] Y. Bakos and H. Hałaburda, “Tradeoffs in Permissioned vs Permissionless Blockchains: Trust and Performance,” *SSRN Electronic Journal*, Jan. 2021, doi: 10.2139/ssrn.3789425.

[17] “What Different Types of Blockchains are There?,” *Dragonchain*, 18-Apr-2019. [Online]. Available: https://dragonchain.com/blog/differences-between-public-private-blockchains. [Accessed: 12-Jul-2021]

[18] “What are the 4 different types of blockchain technology?,” *SearchCIO*. [Online]. Available: https://searchcio.techtarget.com/feature/What-are-the-4-different-types-of-blockchain-technology. [Accessed: 12-Jul-2021]

[19] “How the Consensus Protocol Impacts Blockchain Throughput,” *NEC*. [Online]. Available: https://www.nec.com/en/global/insights/article/2020022520/index.html. [Accessed: 13-Jul-2021]

[20] G. Bitzes, “Distributed consensus and fault tolerance,Lecture 2/2,” *iCSC*, p. 44, 2017 [Online]. Available: https://indico.cern.ch/event/591368/contributions/2402667/attachments/1422936/2181385/Distributed_consensus_and_fault_tolerance_-_part_2.pdf

[21] L. Lamport, “The part-time parliament,” *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, May 1998, doi: 10.1145/279227.279229. [Online]. Available: https://doi.org/10.1145/279227.279229. [Accessed: 13-Jul-2021]

[22] M. Castro, “Practical Byzantine Fault Tolerance,” Apr. 2001.

[23] D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm,” in *Proceedings of the 2014 USENIX conference on USENIX Annual Technical Conference*, USA, 2014, pp. 305–320.

[24] I. M. Coelho, V. N. Coelho, R. P. Araujo, W. Yong Qiang, and B. D. Rhodes, “Challenges of PBFT-Inspired Consensus for Blockchain and Enhancements over Neo dBFT,” *Future Internet*, vol. 12, no. 8, p. 129, Aug. 2020, doi: 10.3390/fi12080129. [Online]. Available: https://www.mdpi.com/1999-5903/12/8/129. [Accessed: 13-Jul-2021]

[25] J. Yoo, Y. Jung, D. Shin, M. Bae, and E. Jee, “Formal Modeling and Verification of a Federated Byzantine Agreement Algorithm for Blockchain Platforms,” in *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 2019, pp. 11–21, doi: 10.1109/IWBOSE.2019.8666514.

[26] N. Tomić, “A Review of consensus protocols in permissioned blockchains,” *Journal of Computer Science Research*, vol. 3, Apr. 2021, doi: 10.30564/jcsr.v3i2.2921.

[27] M. Du, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” 2017, pp. 2567–2572, doi: 10.1109/SMC.2017.8123011.

[28] “Ethereum 101,” *CoinDesk*. [Online]. Available: https://www.coindesk.com/learn/ethereum-101/what-is-a-decentralized-application-dapp. [Accessed: 13-Jul-2021]

[29] “KnownOrigin | Digital Art Marketplace | NFT Crypto Art.” [Online]. Available: https://knownorigin.io/. [Accessed: 13-Jul-2021]

[30] “Nexo - Unlock the Power of Your Crypto,” *Nexo*. [Online]. Available: https://nexo.io. [Accessed: 13-Jul-2021]

[31] “GoQuorum.” [Online]. Available: https://docs.goquorum.consensys.net/en/stable/. [Accessed: 13-Jul-2021]

[32] “What Is Quorum Blockchain? A Platform for The Enterprise,” *Blockgeeks*, 06-May-2020. [Online]. Available: https://blockgeeks.com/guides/quorum-a-blockchain-platform-for-the-enterprise/. [Accessed: 13-Jul-2021]

[33] E. Androulaki *et al.*, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceedings of the Thirteenth EuroSys*

Conference, New York, NY, USA, 2018, pp. 1–15, doi: 10.1145/3190508.3190538 [Online]. Available: https://doi.org/10.1145/3190508.3190538. [Accessed: 14-Jun-2021]

[34] "A Blockchain Platform for the Enterprise," *Hyperledger Fabric Documentation*. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/. [Accessed: 13-Jul-2021]

[35] "Off-Chain vs On-Chain Transactions," *ECOchain*, 09-Jul-2020. [Online]. Available: https://ecoc.io/new3/. [Accessed: 13-Jul-2021]

[36] C. Antal, T. Cioara, I. Anghel, M. Antal, and I. Salomie, "Distributed Ledger Technology Review and Decentralized Applications Development Guidelines," *Future Internet*, vol. 13, no. 3, p. 62, Mar. 2021, doi: 10.3390/fi13030062. [Online]. Available: https://www.mdpi.com/1999-5903/13/3/62. [Accessed: 13-Jul-2021]

[37] "Privacy." [Online]. Available: https://docs.ipfs.io/concepts/privacy/. [Accessed: 13-Jul-2021]

[38] "Storj: A Decentralized Cloud Storage NetworkFramework," *Storj Labs, Inc.*, Oct. 2018 [Online]. Available: https://storj.io/storj.pdf. [Accessed: 13-Jul-2021]

[39] "Filecoin: A Decentralized Storage Network," *Protocol Labs*, Jul. 2017 [Online]. Available: https://filecoin.io/filecoin.pdf. [Accessed: 13-Jul-2021]

[40] "Swarm: Storage and Communication Infrastructure for a Self-Sovereign Digital Society," Jun. 2021 [Online]. Available: https://www.ethswarm.org/swarm-whitepaper.pdf. [Accessed: 13-Jul-2021]

[41] T. McConaghy, "Blockchain Infrastructure Landscape: A First Principles Framing," *Medium*, 23-Sep-2017. [Online]. Available: https://medium.com/@trentmc0/blockchain-infrastructure-landscape-a-first-principles-framing-92cc5549bafe. [Accessed: 13-Jul-2021]

[42] "Swarm, IPFS and BigchainDB: Comparing Data Storage and Decentralization | Hacker Noon." [Online]. Available: https://hackernoon.com/swarm-ipfs-and-bigchaindb-comparing-data-storage-and-decentralization-4a2o3wf8. [Accessed: 13-Jul-2021]

[43] "The Golem Project," *Golem*, Nov. 2016 [Online]. Available: https://assets.website-files.com/60005e3965a10f31d245af87/60352707e6dd742743c75764_Golemwhitepaper.pdf. [Accessed: 13-Jul-2021]

[44] "iExec: Blockchain-Based Decentralized Cloud Computing," *iExec*, Apr. 2018 [Online]. Available: https://iex.ec/wp-content/uploads/pdf/iExec-WPv3.0-English.pdf. [Accessed: 13-Jul-2021]

[45] J. Teutsch and C. Reitwießner, “A scalable verification solution for blockchains,” *arXiv:1908.04756 [cs, econ]*, Aug. 2019 [Online]. Available: http://arxiv.org/abs/1908.04756. [Accessed: 13-Jul-2021]

[46] “What Is the Blockchain Oracle Problem?,” *Chainlink*, 27-Aug-2020. [Online]. Available: https://blog.chain.link/blockchain-oracle-problem-chainlink. [Accessed: 13-Jul-2021]

[47] A. Beniiche, “A Study of Blockchain Oracles (pre-print),” *arXiv:2004.07140 [cs]*, Jul. 2020 [Online]. Available: http://arxiv.org/abs/2004.07140. [Accessed: 13-Jul-2021]

[48] “When Blockchain Meets SGX: An Overview, Challenges, and Open Issues.” [Online]. Available: https://ieeexplore.ieee.org/document/9197584. [Accessed: 13-Jul-2021]

[49] “Provable - blockchain oracle service, enabling data-rich smart contracts.” [Online]. Available: https://provable.xyz/. [Accessed: 13-Jul-2021]

[50] “ChainLink: A Decentralized Oracle Network,” *ChainLink*, Sep. 2017 [Online]. Available: https://research.chain.link/whitepaper-v1.pdf. [Accessed: 13-Jul-2021]

[51] “Software Engineering — Guide to the software engineering body of knowledge (SWEBOK),” ISO/IEC TR 19759:2015.

[52] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, “Blockchain-Oriented Software Engineering: Challenges and New Directions,” 2017, pp. 169–171, doi: 10.1109/ICSE-C.2017.142 [Online]. Available: https://dl.acm.org/doi/10.1109/ICSE-C.2017.142

[53] Object Management Group, “Unified Modeling Language,” Version 2.5.1, Dec. 2017 [Online]. Available: https://www.omg.org/spec/UML/2.5.1/PDF. [Accessed: 14-Jul-2021]

[54] Object Management Group, “Business Process Model and Notation,” Version 2.0.2, Jan. 2014 [Online]. Available: https://www.omg.org/spec/BPMN/2.0.2/PDF. [Accessed: 14-Jul-2021]

[55] H. Rocha and S. Ducasse, “Preliminary Steps Towards Modeling Blockchain Oriented Software,” in *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, 2018, pp. 52–57 [Online]. Available: https://ieeexplore.ieee.org/document/8445060

[56] M. Marchesi, L. Marchesi, and R. Tonelli, “An Agile Software Engineering Method to Design Blockchain Applications,” 2018, pp. 1–8, doi: 10.1145/3290621.3290627.

[57] V. Vescoukis, “Ολοκληρωμένα συστήματα διαχείρισης κρίσεων Μελέτη περίπτωσης δασικών πυρκαγιών - PDF Free Download,” 11-Dec-2007. [Online]. Available: https://docplayer.gr/1916010-Olokliromena-systimata-diaheirisis-kriseon-meleti-periptosis-dasikon-pyrkagion.html. [Accessed: 14-Jul-2021]

[58] C. Molina-Jiménez, E. Solaiman, I. Sfyrakis, I. Ng, and J. Crowcroft, “On and Off-Blockchain Enforcement Of Smart Contracts,” in *Euro-Par Workshops*, 2018, doi: 10.1007/978-3-030-10549-5_27.

[59] V. Lemieux, “Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework,” 2017.

[60] A. Vitoratos, “Business Process Model Diagram: Επικοινωνία μεταξύ των εμπλεκόμενων φορέων στην αεροδιακομιδή.” s.n., 2019.

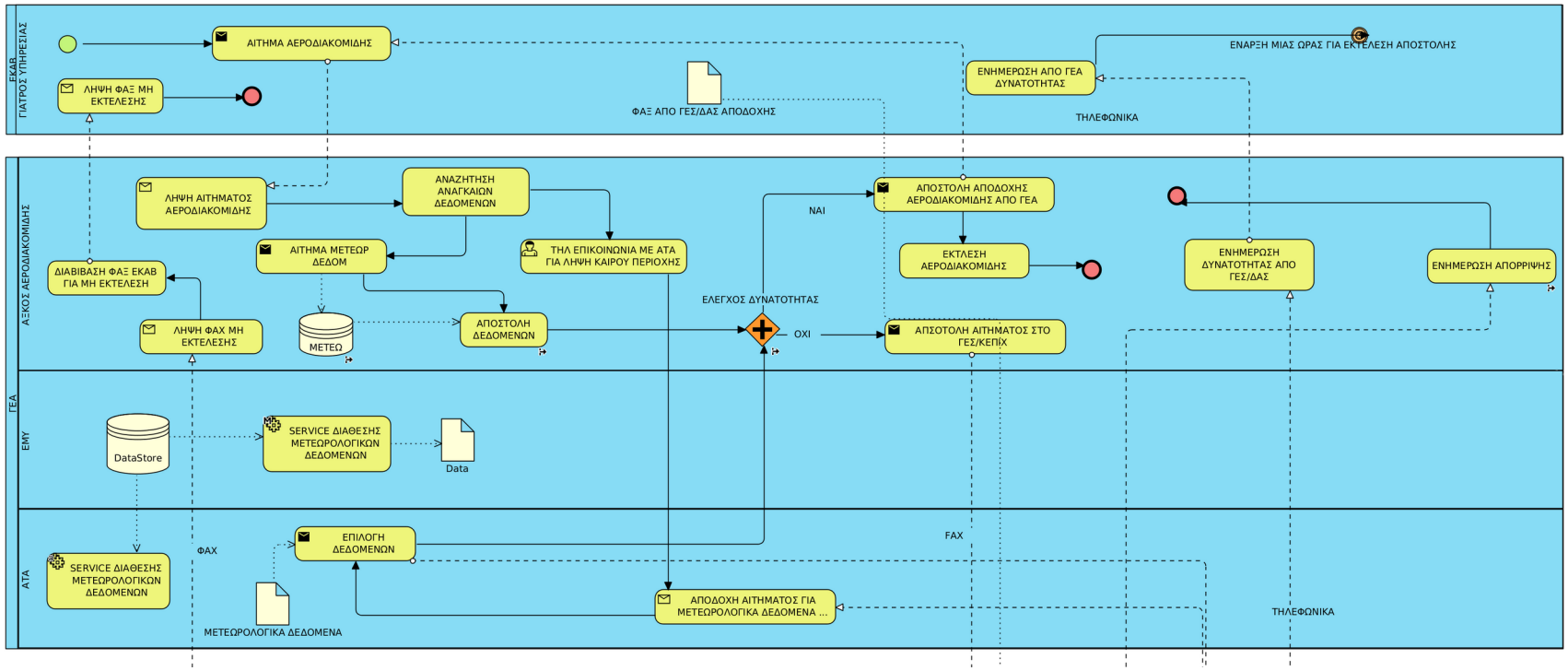
[61] V. Lemieux, D. Flores, and C. Lacombe, “Real Estate Transaction Recording in the Blockchain in Brazil (pre-print),” University of British Columbia, Case Study RCPLAC-01, Jan. 2018.

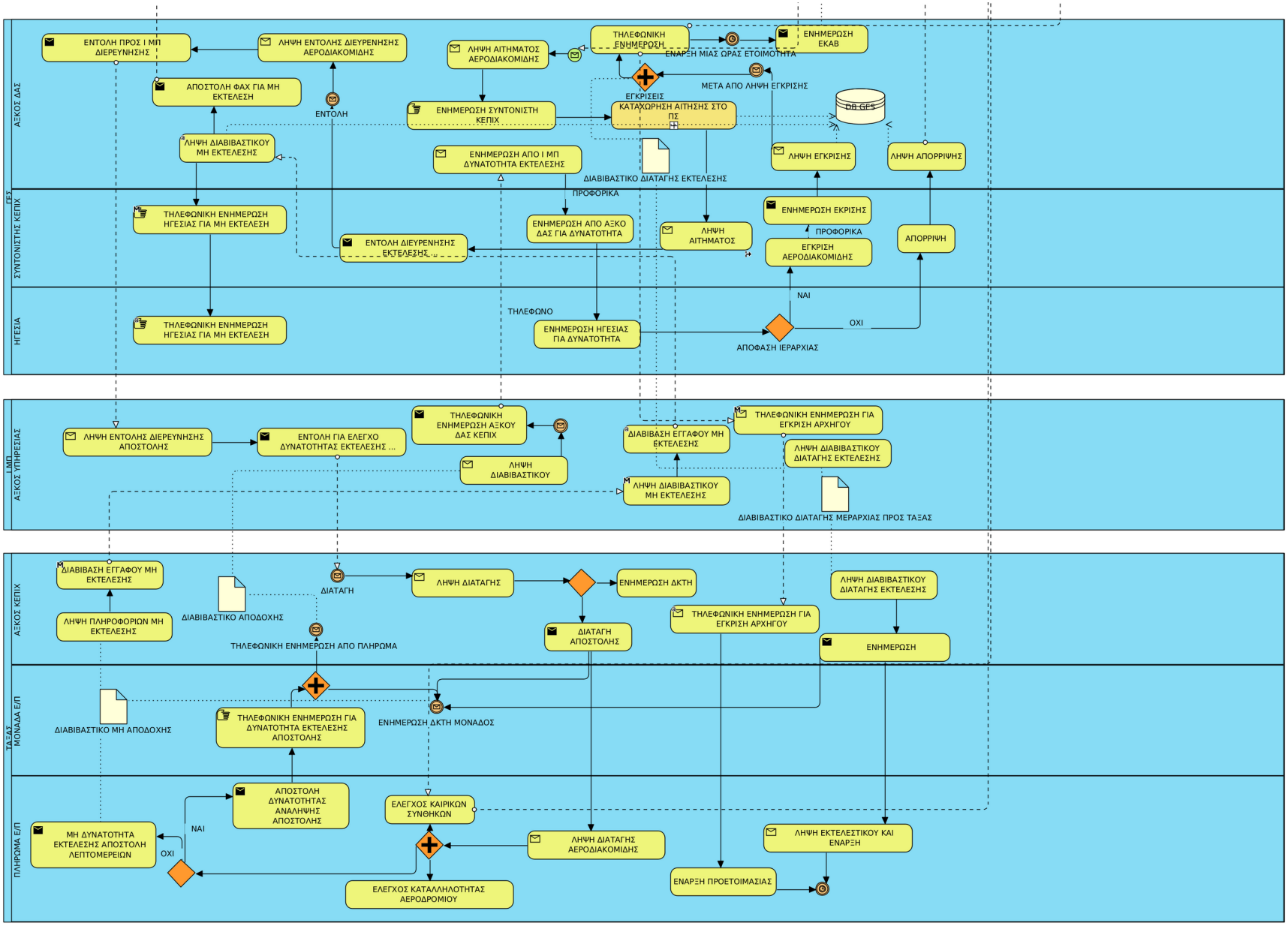
[62] World Meteorological Organization (WMO), *Aerodrome reports and forecasts : A Users’ Handbook to the Codes*, 2020 Edition. Geneva: WMO, 2020.

[63] OECD Directorate for Financial and Enterprise Affairs, “Blockchain and Competition – MULLIGAN – June 2018 OECD discussion,” 08-Jun-2018 [Online]. Available: https://www.slideshare.net/OECD-DAF/blockchain-and-competition-mulligan-june-2018-oecd-discussion. [Accessed: 13-Jul-2021]

[64] C. Nakou, “Αξιοποίηση τεχνολογιών Blockchain σε εφαρμογές κρίσιμης αποστολής: μια μελέτη περίπτωσης στο οικοσύστημα Hyperledger,” Nov. 2019 [Online]. Available: http://artemis.cslab.ece.ntua.gr:8080/jspui/handle/123456789/17421. [Accessed: 14-Jul-2021]

ΠΑΡΑΡΤΗΜΑ Α: Διάγραμμα BPMN για τη διαδικασία αεροδιακομιδής στο σύστημα legacy





Εικόνα 62: Διάγραμμα BPMN για τη διαδικασία αεροδιακομιδής στο σύστημα legacy [60]

ΠΑΡΑΡΤΗΜΑ Β: Πίνακας δεδομένων

Β1: Πίνακας

Α/Α	ΟΡΓΑΝΙΣΜΟΣ	ΣΥΜΜΕΤΕΧΩΝ	ΔΡΑΣΤΗΡΙΟΤΗΤΑ (BPMN)	LEGACY			BLOCKCHAIN				ΠΕΡΙΠΤΩΣΗ ΧΡΗΣΗΣ
				Δεδομένο	**Τύπος δεδομένου**	**Σημειώσεις**	**Μετασχηματισμός**	**Δεδομένο BC**	**Τύπος δεδομένου BC**	**Σημειώσεις**	
1	ΕΚΑΒ	Γιατρός υπηρεσίας	-	Αφετηρία και προορισμός αερ/δής	{src: location, dst: location}		=	Αφετηρία και προορισμός αερ/δής	{src: location, dst: location}		Αίτημα αεροδιακομιδής
2	ΕΚΑΒ	Γιατρός υπηρεσίας	Αίτημα αεροδιακομιδής	Αίτημα αεροδιακομιδής	document		hash	Αναφορά στο αίτημα αεροδιακομιδής	str		Αίτημα αεροδιακομιδής
3	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Λήψη αιτήματος αεροδιακομιδής	Καταγραφή συμβάντος	event			ACK	{}		Αίτημα αεροδιακομιδής
4	ΓΕΑ	Αξιωματικός αεροδιακομιδής	-	Εξεταζόμενη περιοχή πτήσης	image	Χάρτης	pick	Εξεταζόμενη περιοχή πτήσης	polygon		Έλεγχος δυνατότητας ΓΕΑ
5	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Αίτημα μετεωρολογικών δεδομένων	Query μετεωρολογικών δεδομένων	str		=	Query μετεωρολογικών δεδομένων	str		Συγκέντρωση δεδομένων ΓΕΑ
6	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Αποστολή δεδομένων	Μετεωρολογικά δεδομένα	str	TAF-METAR	=	Μετεωρολογικά δεδομένα	str		Συγκέντρωση δεδομένων ΓΕΑ
7	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Τηλ. επικοινωνία με ΑΤΑ για καιρό περιοχής	Κλήση προς ΑΤΑ	audio		hash	Αναφορά στην κλήση	str		Συγκέντρωση δεδομένων ΓΕΑ
8	ΓΕΑ	ΑΤΑ	Αποδοχή αιτήματος για μετεωρ. δεδομένα	Καταγραφή συμβάντος	event			ACK	{}		Συγκέντρωση δεδομένων ΓΕΑ
9	ΓΕΑ	ΑΤΑ	-	Query μετεωρολογικών δεδομένων	str		=	Query μετεωρολογικών δεδομένων	str		Συγκέντρωση δεδομένων ΓΕΑ

10	ΓΕΑ	ΑΤΑ	Επιλογή δεδομένων	Μετεωρολογικά δεδομένα	str	TAF-METAR	=	Μετεωρολογικά δεδομένα	str	Συγκέντρωση δεδομένων ΓΕΑ
11	ΓΕΑ	Αξιωματικός αεροδιακομιδής	-	Αξιολογήσεις κυβερνητών	audio[]	Επικοινωνία αξ/κού με κυβερνήτη για ετοιμότητα πληρώματος και αεροσκάφους	hash	Αναφορές στις αξιολογήσεις κυβερνητών	str[]	Έλεγχος δυνατότητας ΓΕΑ
12	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Έλεγχος δυνατότητας	Δυνατότητα ΓΕΑ	bool		=	Δυνατότητα ΓΕΑ	bool	Έλεγχος δυνατότητας ΓΕΑ
13	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Αποστολή αποδοχής αεροδιακομιδής ΓΕΑ	Αποδοχή ΓΕΑ	document		hash	Αναφορά στην αποδοχή ΓΕΑ	str	Εκτέλεση ΓΕΑ
14	ΓΕΑ	Αξιωματικός αεροδιακομιδής	-	Σχέδιο πτήσης	N/A		pick	Σχέδιο πτήσης	{planeId: str, crew: str[], eta: datetime}	Εκτέλεση ΓΕΑ
15	ΕΚΑΒ	Γιατρός υπηρεσίας	Αίτημα αεροδιακομιδής	N/A	N/A			ACK	{}	Ενημέρωση για εκτέλεση ΓΕΑ
16	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Εκτέλεση αεροδιακομιδής	Εκτέλεση αεροδιακομιδής	{}		=	Εκτέλεση αεροδιακομιδής	{}	Εκτέλεση ΓΕΑ
17	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Αποστολή αιτήματος στο ΓΕΣ/ΚΕΠΙΧ	Αίτημα προς ΓΕΣ	document		hash	Αναφορά στο αίτημα προς ΓΕΣ	str	Αίτημα προς ΓΕΣ
18	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη αιτήματος αεροδιακομιδής	Καταγραφή συμβάντος	event			ACK	{}	Αίτημα προς ΓΕΣ
19	ΓΕΣ	Αξιωματικός ΔΑΣ	Καταχώρηση αιτήματος στο ΠΣ	Αίτημα αεροδιακομιδής	N/A		pick	Αίτημα αεροδιακομιδής	{src: location, dst: location}	Αίτημα προς ΓΕΣ
20	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Λήψη αιτήματος από ΠΣ	Καταγραφή συμβάντος	event			ACK	{}	Αίτημα προς ΓΕΣ
21	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Εντολή διερεύνησης εκτέλεσης	Εντολή διερεύνησης	str	Στην DB GES	hash	Αναφορά στην εντολή διερεύνησης	str	Αίτημα προς ΓΕΣ
22	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη εντολής διερεύνησης	Καταγραφή συμβάντος	event			ACK	{}	Αίτημα προς ΓΕΣ

23	ΓΕΣ	Αξιωματικός ΔΑΣ	Εντολή προς ΙΜΠ διερεύνησης	Εντολή διερεύνησης	document		hash	Αναφορά στην εντολή διερεύνησης	str	Αίτημα προς ΓΕΣ
24	ΙΜΠ	Αξιωματικός υπηρεσίας	Λήψη εντολής διερεύνησης	Καταγραφή συμβάντος	event			ACK	{}	Αίτημα προς ΓΕΣ
25	ΙΜΠ	Αξιωματικός υπηρεσίας	Εντολή για έλεγχο δυνατότητας εκτέλεσης	Εντολή διερεύνησης	document		hash	Αναφορά στην εντολή διερεύνησης	str	Αίτημα προς ΓΕΣ
26	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Λήψη διαταγής	Καταγραφή συμβάντος	event			ACK	{}	Αίτημα προς ΓΕΣ
27	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Ενημέρωση διοικητή	?	?			Επιβεβαίωση ενημέρωσης	{}	Αίτημα προς ΓΕΣ
28	ΤΑΞΑΣ	Διοικητής ΤΑΞΑΣ	Ενημέρωση διοικητή	Καταγραφή συμβάντος	event			ACK	{}	Αίτημα προς ΓΕΣ
29	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Διαταγή αποστολής	Διαταγή αποστολής	document		hash	Αναφορά στη διαταγή αποστολής	str	Αίτημα προς ΓΕΣ
30	ΤΑΞΑΣ	Μονάδα Ε/Π	Ενημέρωση διοικητή μονάδας	N/A	N/A			Επιβεβαίωση ενημέρωσης	{}	Αίτημα προς ΓΕΣ
31	ΤΑΞΑΣ	Μονάδα Ε/Π	Ενημέρωση διοικητή μονάδας	N/A	N/A			ACK	{}	Αίτημα προς ΓΕΣ
32	ΤΑΞΑΣ	Πλήρωμα Ε/Π	Λήψη διαταγής αεροδιακομιδής	N/A	N/A			ACK	{}	Αίτημα προς ΓΕΣ
33	N/A	N/A	-	Εξεταζόμενη περιοχή πτήσης	N/A		=	Εξεταζόμενη περιοχή πτήσης	polygon	Έλεγχος δυνατότητας από ΓΕΣ
34	ΤΑΞΑΣ	Μονάδα Ε/Π	-	Διαθεσιμότητα Ε/Π	N/A		pick	Διαθεσιμότητα Ε/Π	ts<{id: str, loc: location, available: bool} []>	Συγκέντρωση δεδομένων ΤΑΞΑΣ
35	ΤΑΞΑΣ	Μονάδα Ε/Π	-	Ετοιμότητα πληρωμάτων Ε/Π	N/A		pick	Διαθεσιμότητα πληρωμάτων Ε/Π	ts<{id: str, loc: location, available: bool} []>	Συγκέντρωση δεδομένων ΤΑΞΑΣ
36	ΓΕΑ	ΑΤΑ	Επιλογή δεδομένων	Μετεωρολογικά δεδομένα	str	TAF-METAR	=	Μετεωρολογικά δεδομένα	str	Συγκέντρωση δεδομένων ΤΑΞΑΣ

37	ΤΑΞΑΣ	Πλήρωμα Ε/Π	Έλεγχος καιρικών συνθηκών	Καταγραφή συμβάντος	event		ACK	{}	Συγκέντρωση δεδομένων ΤΑΞΑΣ
38	ΤΑΞΑΣ	Πλήρωμα Ε/Π	Έλεγχος καιρικών συνθηκών	Αξιολόγηση καιρικών συνθηκών	str	=	Αξιολόγηση καιρικών συνθηκών	str	Έλεγχος δυνατότητας από ΤΑΞΑΣ
39	ΤΑΞΑΣ	Πλήρωμα Ε/Π	-	Δεδομένα καταλληλότητας αεροδρομίου	N/A	=	Καταλληλότητα αεροδρομίου	N/A	Συγκέντρωση δεδομένων ΤΑΞΑΣ
40	ΤΑΞΑΣ	Πλήρωμα Ε/Π	Έλεγχος καταλληλότητας αεροδρομίου	Αξιολόγηση καταλληλότητας	str	=	Αξιολόγηση καταλληλότητας	str	Έλεγχος δυνατότητας από ΤΑΞΑΣ
41	ΤΑΞΑΣ	Πλήρωμα Ε/Π	-	Δυνατότητα πληρώματος Ε/Π	bool	=	Δυνατότητα πληρώματος Ε/Π	bool	Έλεγχος δυνατότητας από ΤΑΞΑΣ
42	ΤΑΞΑΣ	Πλήρωμα Ε/Π	Αποστολή δυνατότητας ανάληψης αποστολής	Δυνατότητα ανάληψης αποστολής	str	hash	Αναφορά στη δυνατότητα ανάληψης	str	Ενημέρωση για αποδοχή ΤΑΞΑΣ
43	ΤΑΞΑΣ	Μονάδα Ε/Π	Αποστολή δυνατότητας ανάληψης αποστολής	Καταγραφή συμβάντος	event		ACK	{}	Ενημέρωση για αποδοχή ΤΑΞΑΣ
44	ΤΑΞΑΣ	Μονάδα Ε/Π	Τηλ. ενημέρωση από πλήρωμα	Κλήση προς αξιωματικό ΚΕΠΙΧ	audio	hash	Αναφορά στην κλήση προς αξιωματικό ΚΕΠΙΧ	str	Ενημέρωση για αποδοχή ΤΑΞΑΣ
45	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Τηλ. ενημέρωση από πλήρωμα	Καταγραφή συμβάντος	event		ACK	{}	Ενημέρωση για αποδοχή ΤΑΞΑΣ
46	ΤΑΞΑΣ	Μονάδα Ε/Π	Ενημέρωση διοικητή μονάδας	Κλήση προς διοικητή μονάδας	audio	hash	Αναφορά στην κλήση προς διοικητή μονάδας	str	Ενημέρωση για αποδοχή ΤΑΞΑΣ
47	ΤΑΞΑΣ	Μονάδα Ε/Π	Ενημέρωση διοικητή μονάδας	N/A	N/A		ACK	{}	Ενημέρωση για αποδοχή ΤΑΞΑΣ
48	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Διαβιβαστικό αποδοχής	Διαβιβαστικό αποδοχής	document	hash	Αναφορά στο διαβιβ. αποδοχής	str	Ενημέρωση για αποδοχή ΤΑΞΑΣ
49	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	-	Πρόταση σχεδίου πτήσης	N/A	pick	Πρόταση σχεδίου πτήσης	{helicopterId: str, crew: str[], eta: datetime}	Ενημέρωση για αποδοχή ΤΑΞΑΣ

50	ΙΜΠ	Αξιωματικός υπηρεσίας	Λήψη διαβιβαστικού	Καταγραφή συμβάντος	event			ACK	{}	Ενημέρωση για αποδοχή ΤΑΞΑΣ
51	ΙΜΠ	Αξιωματικός υπηρεσίας	Τηλεφωνική ενημέρωση αξιωματικού ΔΑΣ ΚΕΠΙΧ	Κλήση προς αξιωματικό ΔΑΣ	audio		hash	Αναφορά στην κλήση προς αξιωματικό ΔΑΣ	str	Ενημέρωση για αποδοχή ΤΑΞΑΣ
52	ΓΕΣ	Αξιωματικός ΔΑΣ	Ενημέρωση από ΙΜΠ δυνατότητα εκτέλεσης	Καταγραφή συμβάντος	event			ACK	{}	Ενημέρωση για αποδοχή ΤΑΞΑΣ
53	ΓΕΣ	Αξιωματικός ΔΑΣ	Ενημέρωση από αξιωματικό ΔΑΣ	Ενημέρωση από αξιωματικό ΔΑΣ	προφορικά			Επιβεβαίωση ενημέρωσης	{}	Ενημέρωση για αποδοχή ΤΑΞΑΣ
54	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Ενημέρωση από αξιωματικό ΔΑΣ	Καταγραφή συμβάντος	event			ACK	{}	Ενημέρωση για αποδοχή ΤΑΞΑΣ
55	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Ενημέρωση ηγεσίας για δυνατότητα	Ενημέρωση ηγεσίας για δυνατότητα	προφορικά			Επιβεβαίωση ενημέρωσης	{}	Ενημέρωση για αποδοχή ΤΑΞΑΣ
56	ΓΕΣ	Ηγεσία	Ενημέρωση ηγεσίας για δυνατότητα	N/A	N/A					Ενημέρωση για αποδοχή ΤΑΞΑΣ
57	ΓΕΣ	Ηγεσία	Απόφαση ιεραρχίας	Απόφαση ηγεσίας ΓΕΣ	bool	ΗΓΕΣΙΑ=ΟΚ, τυπικό.				Έλεγχος δυνατότητας από ΓΕΣ
58	ΓΕΣ	Ηγεσία	Έγκριση αεροδιακομιδής	Έγκριση αεροδιακομιδής	προφορικά					Εκτέλεση ΓΕΣ
59	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Έγκριση αεροδιακομιδής	Καταγραφή συμβάντος	event			ACK	{}	Εκτέλεση ΓΕΣ
60	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Ενημέρωση έγκρισης	Έγκριση αεροδιακομιδής	προφορικά			Επιβεβαίωση ενημέρωσης	{}	Εκτέλεση ΓΕΣ
61	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη έγκρισης	Καταγραφή συμβάντος	event			ACK	{}	Εκτέλεση ΓΕΣ
62	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη έγκρισης	Έγκριση αεροδιακομιδής	str	Στην DB GES	=	Έγκριση αεροδιακομιδής	str	Εκτέλεση ΓΕΣ
63	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη έγκρισης	Καταγραφή συμβάντος	event			ACK	{}	Εκτέλεση ΓΕΣ
64	ΓΕΣ	Αξιωματικός ΔΑΣ	Τηλεφωνική ενημέρωση	Κλήση προς ΙΜΠ	audio		hash	Αναφορά στην κλήση προς ΙΜΠ	str	Εκτέλεση ΓΕΣ

65	ΙΜΠ	Αξιωματικός υπηρεσίας	Τηλεφωνική ενημέρωση για έγκριση αρχηγού	Καταγραφή συμβάντος	event		ACK	{}	Εκτέλεση ΓΕΣ
66	ΙΜΠ	Αξιωματικός υπηρεσίας	Τηλεφωνική ενημέρωση για έγκριση αρχηγού	Κλήση προς ΤΑΞΑΣ	audio	hash	Αναφορά στην κλήση προς ΤΑΞΑΣ	str	Εκτέλεση ΓΕΣ
67	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Τηλεφωνική ενημέρωση για έγκριση αρχηγού	Καταγραφή συμβάντος	event		ACK	{}	Εκτέλεση ΓΕΣ
68	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Έναρξη προετοιμασίας	Εντολή έναρξης προετοιμασίας	document	hash	Εντολή έναρξης προετοιμασίας	str	Εκτέλεση ΓΕΣ
69	ΤΑΞΑΣ	Πλήρωμα Ε/Π	-	N/A	N/A		ACK	{}	Εκτέλεση ΓΕΣ
70	ΓΕΣ	Αξιωματικός ΔΑΣ	Διαβιβαστικό διαταγής εκτέλεσης	Διαταγή εκτέλεσης	document	hash	Αναφορά στη διαταγή εκτέλεσης	str	Εκτέλεση ΓΕΣ
71	ΙΜΠ	Αξιωματικός υπηρεσίας	Λήψη διαβιβαστικού διαταγής εκτέλεσης	Καταγραφή συμβάντος	event		ACK	{}	Εκτέλεση ΓΕΣ
72	ΙΜΠ	Αξιωματικός υπηρεσίας	Διαβιβαστικό διαταγής Μεραρχίας προς ΤΑΞΑΣ	Διαταγή μεραρχίας προς ΤΑΞΑΣ	document	hash	Αναφορά στη διαταγή μεραρχίας προς ΤΑΞΑΣ	str	Εκτέλεση ΓΕΣ
73	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Λήψη διαβιβαστικού διαταγής εκτέλεσης	Καταγραφή συμβάντος	event		ACK	{}	Εκτέλεση ΓΕΣ
74	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Ενημέρωση	Διαταγή εκτέλεσης	document	hash	Αναφορά στη διαταγή εκτέλεσης	str	Εκτέλεση ΓΕΣ
75	ΤΑΞΑΣ	Μονάδα Ε/Π	Ενημέρωση διοικητή μονάδας	N/A	N/A		Επιβεβαίωση ενημέρωσης	{}	Εκτέλεση ΓΕΣ
76	ΤΑΞΑΣ	Μονάδα Ε/Π	Ενημέρωση διοικητή μονάδας	N/A	N/A		ACK	{}	Εκτέλεση ΓΕΣ
77	ΤΑΞΑΣ	Πλήρωμα Ε/Π	Λήψη εκτελεστικού και έναρξη	N/A	N/A		ACK	{}	Εκτέλεση ΓΕΣ
78	ΤΑΞΑΣ	Πλήρωμα Ε/Π	Λήψη εκτελεστικού και έναρξη	N/A	N/A		Επιβεβαίωση έναρξης	{}	Εκτέλεση ΓΕΣ

79	ΓΕΣ	Αξιωματικός ΔΑΣ	Τηλεφωνική ενημέρωση	Κλήση προς αξιωματικό αεροδιακομιδής ΓΕΑ	audio			hash	Αναφορά στην κλήση προς αξ. αεροδιακομιδής	str	Ενημέρωση για εκτέλεση ΓΕΣ
80	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Ενημέρωση δυνατότητας από ΓΕΣ	Καταγραφή συμβάντος	event				ACK	{}	Ενημέρωση για εκτέλεση ΓΕΣ
81	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Ενημέρωση από ΓΕΑ δυνατότητας	Κλήση προς ΕΚΑΒ	audio			hash	Αναφορά στην κλήση προς ΕΚΑΒ	str	Ενημέρωση για εκτέλεση ΓΕΣ
82	ΕΚΑΒ	Γιατρός υπηρεσίας	Ενημέρωση από ΓΕΑ δυνατότητας	N/A	N/A				ACK	{}	Ενημέρωση για εκτέλεση ΓΕΣ
83	ΕΚΑΒ	Γιατρός υπηρεσίας	Έναρξη μιας ώρας ετοιμότητα	N/A	N/				Επιβεβαίωση έναρξης	{}	Εκτέλεση ΕΚΑΒ
84	ΓΕΣ	Αξιωματικός ΔΑΣ	Έναρξη μιας ώρας ετοιμότητα	N/A	N/A				Επιβεβαίωση έναρξης	{}	Εκτέλεση ΓΕΣ
85	ΓΕΣ	Αξιωματικός ΔΑΣ	Ενημέρωση ΕΚΑΒ	Φαξ αποδοχής ΓΕΣ/ΔΑΣ	document			hash	Αναφορά στο φαξ αποδοχής ΓΕΣ/ΔΑΣ	str	Ενημέρωση για εκτέλεση ΓΕΣ
86	ΕΚΑΒ	Γιατρός υπηρεσίας	Φαξ από ΓΕΣ/ΔΑΣ αποδοχής	N/A	N/A				ACK	{}	Ενημέρωση για εκτέλεση ΓΕΣ
87	ΓΕΣ	Ηγεσία	Απόρριψη	Απόρριψη ηγεσίας	προφορικά						Ενημέρωση για απόρριψη ΓΕΣ
88	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Απόρριψη	Καταγραφή συμβάντος	event				ACK	{}	Ενημέρωση για απόρριψη ΓΕΣ
89	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη απόρριψης	Απόρριψη ηγεσίας	document	Στην DB GES		=	Απόρριψη ηγεσίας	str	Ενημέρωση για απόρριψη ΓΕΣ
90	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη απόρριψης	Καταγραφή συμβάντος	event				ACK	{}	Ενημέρωση για απόρριψη ΓΕΣ
91	ΓΕΣ	Αξιωματικός ΔΑΣ	Ενημέρωση απόρριψης	Κλήση προς αξιωματικό αεροδιακομιδής ΓΕΑ	audio			hash	Αναφορά στην κλήση προς αξ. αεροδιακομιδής	str	Ενημέρωση για απόρριψη ΓΕΣ
92	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Ενημέρωση απόρριψης	Καταγραφή συμβάντος	event				ACK	{}	Ενημέρωση για απόρριψη ΓΕΣ
93	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Τέλος	Καταγραφή συμβάντος	event				Λήξη αιτήματος	{}	Ενημέρωση για απόρριψη ΓΕΣ

94	ΤΑΞΑΣ	Πλήρωμα Ε/Π	Μη δυνατότητα εκτέλεσης	Κλήση προς μονάδα Ε/Π	audio		hash	Αναφορά στην κλήση προς μονάδα Ε/Π	str	Ενημέρωση για απόρριψη ΤΑΞΑΣ
95	ΤΑΞΑΣ	Μονάδα Ε/Π	Μη δυνατότητα εκτέλεσης	N/A	N/A			ACK	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
96	ΤΑΞΑΣ	Μονάδα Ε/Π	Διαβιβαστικό μη αποδοχής	Διαβιβαστικό απόρριψης	document		hash	Αναφορά στο διαβιβ. απόρριψης	str	Ενημέρωση για απόρριψη ΤΑΞΑΣ
97	ΤΑΞΑΣ	Μονάδα Ε/Π	Ενημέρωση διοικητή μονάδας	Διαβιβαστικό απόρριψης	document			Επιβεβαίωση διαβίβασης	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
98	ΤΑΞΑΣ	Μονάδα Ε/Π	Ενημέρωση διοικητή μονάδας	N/A	N/A			ACK	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
99	ΤΑΞΑΣ	Μονάδα Ε/Π	Λήψη πληροφοριών μη εκτέλεσης	Διαβιβαστικό απόρριψης	document			Επιβεβαίωση διαβίβασης	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
100	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Λήψη πληροφοριών μη εκτέλεσης	Καταγραφή συμβάντος	event			ACK	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
101	ΤΑΞΑΣ	Αξιωματικός ΚΕΠΙΧ	Διαβίβαση εγγράφου μη εκτέλεσης	Διαβιβαστικό απόρριψης	document			Επιβεβαίωση διαβίβασης	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
102	ΙΜΠ	Αξιωματικός υπηρεσίας	Λήψη διαβιβαστικού μη εκτέλεσης	Καταγραφή συμβάντος	event			ACK	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
103	ΙΜΠ	Αξιωματικός υπηρεσίας	Διαβίβαση εγγράφου μη εκτέλεσης	Διαβιβαστικό απόρριψης	document			Επιβεβαίωση διαβίβασης	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
104	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη διαβιβαστικού μη εκτέλεσης	Καταγραφή συμβάντος	event			ACK	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
105	ΓΕΣ	Αξιωματικός ΔΑΣ	-	Διαβιβαστικό απόρριψης	str	Στην DB GES		Επιβεβαίωση αποθήκευσης	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
106	ΓΕΣ	Αξιωματικός ΔΑΣ	Λήψη διαβιβαστικού μη εκτέλεσης	Διαβιβαστικό απόρριψης	document			Επιβεβαίωση διαβίβασης	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
107	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Λήψη διαβιβαστικού μη εκτέλεσης	Καταγραφή συμβάντος	event			ACK	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ

108	ΓΕΣ	Συντονιστής ΚΕΠΙΧ	Τηλ. ενημέρωση ηγεσίας για μη εκτέλεση	Κλήση προς ηγεσία	audio	hash	Αναφορά στην κλήση προς ηγεσία	str	Ενημέρωση για απόρριψη ΤΑΞΑΣ
109	ΓΕΣ	Αξιωματικός ΔΑΣ	Αποστολή φαξ για μη εκτέλεση	Φαξ απόρριψης ΤΑΞΑΣ	document	hash	Αναφορά στο φαξ απόρριψης ΤΑΞΑΣ	str	Ενημέρωση για απόρριψη ΤΑΞΑΣ
110	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Λήψη φαξ μη εκτέλεσης	Φαξ απόρριψης ΤΑΞΑΣ	document		Επιβεβαίωση λήψης	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ
111	ΓΕΑ	Αξιωματικός αεροδιακομιδής	Διαβίβαση φαξ ΕΚΑΒ για μη εκτέλεση	Φαξ απόρριψης ΤΑΞΑΣ	document		Επιβεβαίωση διαβίβασης		Ενημέρωση για απόρριψη ΤΑΞΑΣ
112	ΕΚΑΒ	Γιατρός υπηρεσίας	Λήψη φαξ μη εκτέλεσης	Φαξ απόρριψης ΤΑΞΑΣ	document		Επιβεβαίωση λήψης	{}	Ενημέρωση για απόρριψη ΤΑΞΑΣ

Πίνακας 9: Πίνακας δεδομένων για την αεροδιακομιδή με τους προτεινόμενους μετασχηματισμούς Blockchain

Πέρα από τα αναγραφόμενα δεδομένα, κάθε καταχώρηση στο Blockchain συνοδεύεται από τα εξής βασικά στοιχεία: `{type: str, requestId: str, refTime: datetime, entryTime: datetime}`.

Οι γραμμές που έχουν επισημανθεί με κίτρινο φόντο αναπαριστούν δεδομένα που μπορούν θεωρητικά να υπολογιστούν μέσω smart contracts. Για αυτά προτείνουμε τη χρήση passive smart contracts (βλ. §4.2) που εφαρμόζουν τους κανόνες αεροδιακομιδής σε μορφή μη δεσμευτικών προτάσεων.

Οι ενδείξεις `N/A` σηματοδοτούν στοιχεία που δεν είναι γνωστά για το πραγματικό σύστημα αεροδιακομιδής για λόγους απορρήτου ή/και δεν χρειάζεται να προσδιοριστούν με μεγαλύτερη ακρίβεια.

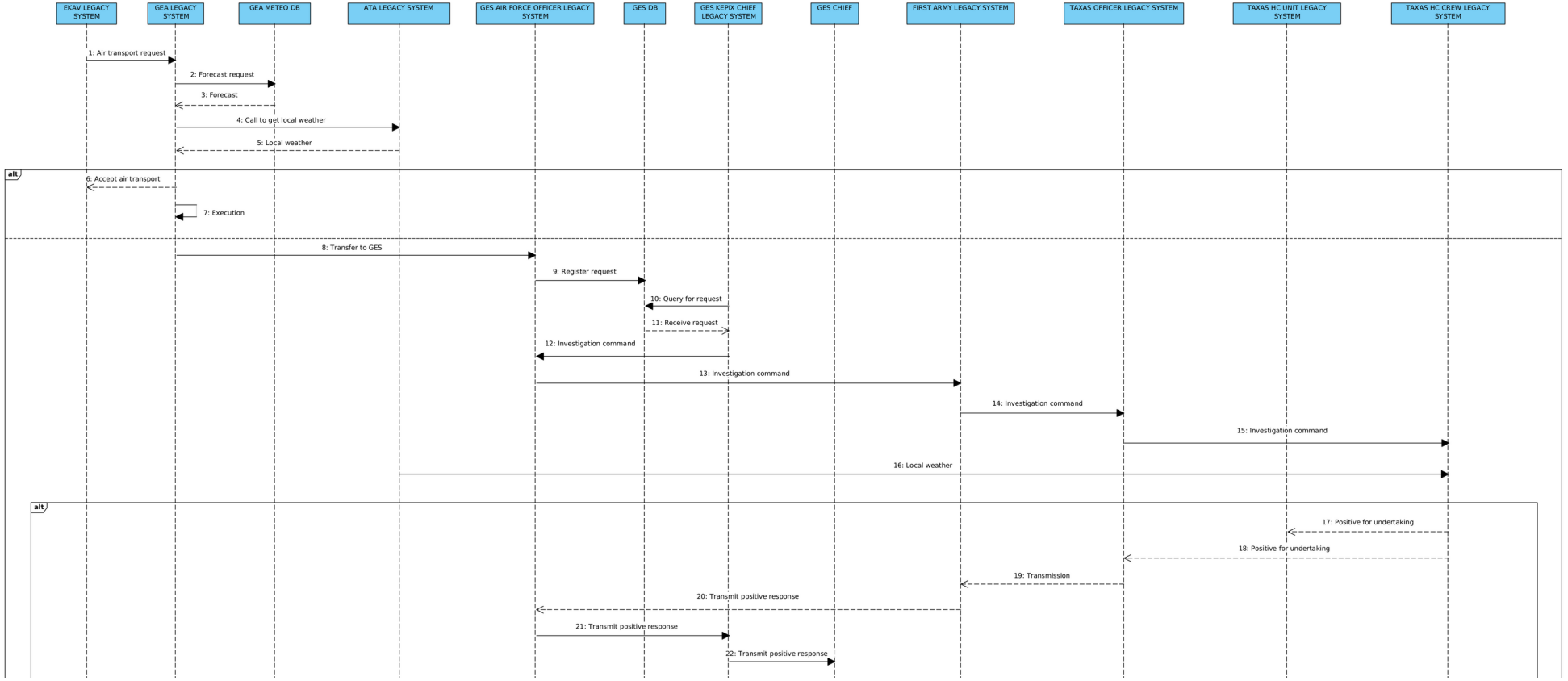
Β2: Επεξήγηση όρων

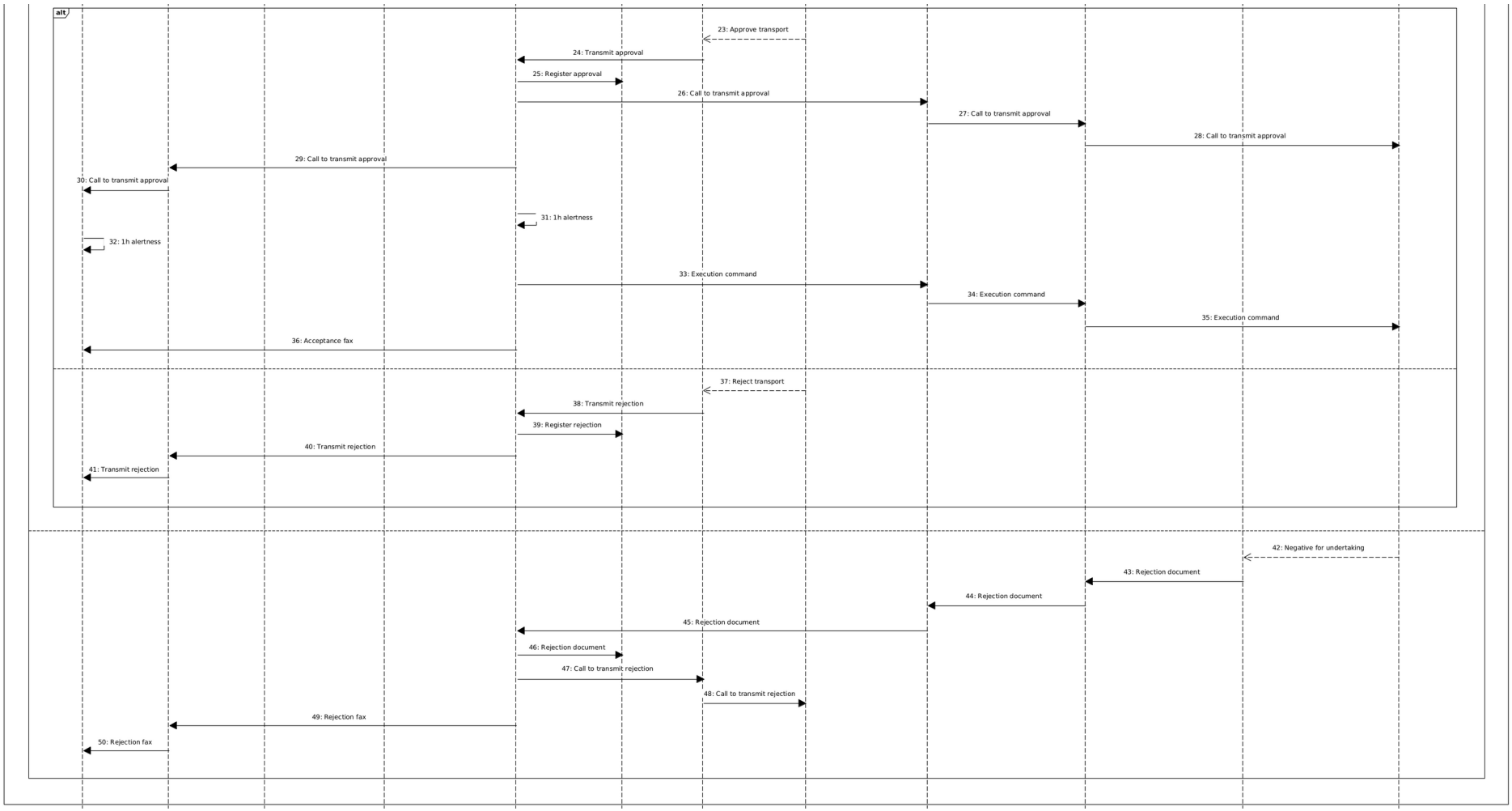
Όρος	Επεξήγηση
type	Αναγνωριστικό του τύπου δεδομένου, π.χ. **ekavRequest** για το αίτημα αεροδιακομιδής από το ΕΚΑΒ.
requestId	Αναγνωριστικό του αιτήματος αεροδιακομιδής που αφορά το παρόν δεδομένο.
refTime	Χρόνος που έλαβε το δεδομένο από την πηγή του ο συμμετέχων (actor).
entryTime	Χρόνος που υπέβαλε το δεδομένο προς καταχώρηση στο Blockchain ο συμμετέχων (actor).
BC	Blockchain.
location	Τύπος δεδομένων για συντεταγμένες τοποθεσίας.
polygon	Λίστα με συντεταγμένες που αναπαριστούν ένα χωρικό πολύγωνο.
str	Κείμενο.
document	Έγγραφο επεξεργασίας κειμένου ή σε raster μορφή.
eta	Εκτιμώμενος χρόνος άφιξης (Estimated Time of Arrival).
ts<T>	Χρονοσειρά που περιέχει την τιμή ενός τύπου δεδομένων (T) σε διακριτές χρονικές στιγμές.
ACK	Αναγνώριση συμβάντος από συμμετέχοντα, συνήθως για επιβεβαίωση ότι έλαβε κάτι από άλλον συμμετέχοντα (βλ. §4.2).
TAF-METAR	TAF και METAR είναι διεθνείς πρότυπες μορφές κωδικοποίησης για δεδομένα καιρού που χρησιμοποιούνται κυρίως στην αεροπορία και έχουν τη μορφή απλού κειμένου. Το METAR αφορά τον παρόντα καιρό και αποτελείται από ωριαίες επιφανειακές παρατηρήσεις, ενώ το TAF αφορά πρόγνωση καιρού έως 30 ωρών σε αεροδρόμιο.
Ε/Π	Ελικόπτερα.
Μετασχηματισμός =	Το δεδομένο εισάγεται στο Blockchain με την ίδια μορφή όπως στο legacy σύστημα.
Μετασχηματισμός hash	Στο Blockchain εισάγεται ένα αναγνωριστικό του δεδομένου που παράγεται από συνάρτηση κατακερματισμού, π.χ. checksum.

Μετασχηματισμός pick	Επιλέγεται ή εξάγεται τμήμα της πληροφορίας από το δεδομένο, αντί να καταχωρηθεί αυτούσιο, για αποδοτικότητα και οικονομία χώρου.

Πίνακας 10: Επεξήγηση όρων του Πίνακα 9. Πληροφορίες για TAF-METAR από [62].

ΠΑΡΑΡΤΗΜΑ Γ: UML sequence diagram για το σύστημα legacy





Εικόνα 63: UML Sequence Diagram για το σύνολο επικοινωνιών μεταξύ φορέων του συστήματος legacy