ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΙΑΤΡΙΚΗ

Ανάπτυξη αποκεντρωμένου πληροφοριακού συστήματος ληξιαρχείου με τη χρήση τεχνολογίας blockchain

Κωνσταντίνος Παπαγεωργίου

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Υπεύθυνος
Γεώργιος Σπαθούλας
Μέλος ΕΔΙΠ

Λαμία, 2022

Περιεχόμενα

1 ΕΙΣΑΓΩΓΗ

Βρισκόμαστε σε μία εποχή όπου τα δεδομένα και οι πληροφορίες περιτριγυρίζουν τους πολίτες, έτσι, η ανάγκη πρόσβασης και σωστής διαχείρισης αυτών από τους ίδιους τους πολίτες κρίνεται επιτακτική, ειδικότερα όσο αναφορά προσωπικά δεδομένα και πληροφορίες των ίδιων των πολιτών. Η παρουσία της Ηλεκτρονικής Διακυβέρνησης έχει σημαντικό ρόλο σε αυτό καθώς επίσης στην ασφάλεια και την ιδιωτικότητα των δεδομένων.

1.1 Ηλεκτρονική Διακυβέρνηση

Τα τελευταία χρόνια η ηλεκτρονική διακυβέρνηση γνώρισε ραγδαία αύξηση καθώς και αλλαγή από τον αρχικό της σκοπό. Αρχικά, τα θέματα που είχαν το επίκεντρο της προσοχής ήταν κυρίως τεχνικά σε σειρά με τις πρώτες δημόσιες ιστοσελίδες και υπηρεσίες που έκαναν εμφάνιση στο διαδίκτυο. Όταν έγινε η ομαλή ένταξή της σε βασικό επίπεδο στο διαδίκτυο και οι κυβερνήσεις ξεκίνησαν να εφαρμόζουν περισσότερες συναλλακτικές υπηρεσίες, το μέγεθος των οργανωτικών προκλήσεων που θα έπρεπε να διευθετηθούν ξεπερνούσαν τα απλά και καθαρά τεχνικά θέματα, ειδικά εν όψει των παραδοσιακών κυβερνητικών δομών και τρόπους λειτουργίας αυτών. Έτσι, το κέντρο προσοχής άλλαξε από τα περισσότερο τεχνικά θέματα, στις οργανωτικές προκλήσεις. Η εφαρμογή των ηλεκτρονικών υπηρεσιών στο δημόσιο τομέα με σκοπό τη βέλτιστη ποιοτική παροχή δημόσιας υπηρεσίας στους πολίτες, την αυξημένη κυβερνητική λογοδοσία στους πολίτες, διασφαλίζοντας έτσι μεγαλύτερη πρόσβαση των πολιτών σε πληροφορίες, βελτιώνει την αποτελεσματικότητα του δημοσίου τομέα, αποκτώντας έτσι περισσότερο οικονομικά αποδοτική κυβέρνηση. Η ηλεκτρονική διακυβέρνηση είχε μείζον ρόλο στην πολιτική μετατρέποντας τον δημόσιο τομέα, επηρεάζοντας την επιχειρηματική διαδικασία και ενθαρρύνοντας την ποιότητα παροχής υπηρεσιών.

1.2 Η εφαρμογή του GDPR για την διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων

Ανεπτυγμένες οικονομίες με ενδιαφέρον προς τους πολίτες τους προσπαθούν να σιγουρευτούν με κάθε τρόπο ότι τα δεδομένα των πολιτών αποθηκεύονται και χρησιμοποιούνται σωστά και πάνω απ' όλα ασφαλή. Με αυτόν τον τρόπο μπορούν να κερδίσουν αντίστροφα την εμπιστοσύνη των πολιτών. Στις 24 Μαΐου του 2016 τέθηκε σε ισχύ ο γενικός κανονισμός για την προστασία των δεδομένων (GDPR) από την Ευρωπαική Ένωση και εφαρμόστηκε στις 28 Μαΐου του 2018. Αυτός ο κανονισμός αποτελεί ένα σημαντικό βήμα για την ενίσχυση των βασικών δικαιωμάτων των πολιτών στην ψηφιακή εποχή καθώς επίσης διευκρινίζει τους κανόνες για επιχειρήσεις και δημόσιους φορείς για το πως χειρίζονται τα προσωπικά δεδομένα. Ακόμη και μετά την εφαρμογή του GDPR το 2018, οι πολίτες έχουν ακόμη ελάχιστο έλεγχο των προσωπικών τους δεδομένων από τη στιγμή που θα τα μοιραστούν με επιχειρήσεις, δημόσιους φορείς και υπηρεσίες.

1.3 Self-Sovereign Identity

Το τελευταίο καιρό, ένας από τους πιο ευρέως χρησιμοποιούμενους όρους στο τομέα του Identity Management είναι το Self-Sovereign Identity. Με τον ραγδαία αυξανόμενο ρυθμό των διαδικτυακών υπηρεσιών τη τελευταία δεκαετία περίπου, η διαχείριση των ταυτοτήτων των χρηστών και των υπηρεσιών έχει πάρει κεντρικό στάδιο και με πολλούς τρόπους έχει γίνει το θεμέλιο πάνω στο οποίο δημιουργούνται διάφορες διαδικτυακές υπηρεσίες. Διάφορες ανάγκες και απαιτήσεις σε διαφορετικές περιπτώσεις χρήσης έχουν οδηγήσει την ανάπτυξη πολλών Συστημάτων Διαχείρισης Ταυτότητας (IMS), τα περισσότερα από τα οποία είναι υπηρεσίες με επίκεντρο τον πάροχο, χωρίς να λαμβάνουν υπόψιν ότι δημιουργείται μια μπερδεμένη μάζα ταυτοτήτων. Η τελική συνέπεια αυτού, είναι ότι οι χρήστες, έχουν καταλήξει με έναν μεγάλο αριθμό ταυτοτήτων, σε σημείο που συχνά νιώθουν χαμένοι σε αυτό το χάος που έχει δημιουργηθεί. Γίνεται όλο και πιο δύσκολο αυτές οι διάσπαρτες ταυτότητες να διαχειριστούν. Το χειρότερο είναι ότι αυτά τα IMS εξυπηρετούν μόνο τις ανάγκες των παρόχων για τη διαχείριση των βάσεων των χρηστών τους και παρέχουν εξαιρετικά περιορισμένες δυνατότητες για τον χρήστη ώστε να ελέγξει τα δεδομένα της ταυτότητάς του. [26] Δεδομένου ότι τα περισσότερα από αυτά τα συστήματα διαχείρισης ταυτότητας βασίζονται σε

κεντρικές βάσεις δεδομένων, αποτελεί απειλή για τον χρήστη όταν βρίσκονται σε κίνδυνο. Νέα σχήματα διαχείρισης ταυτότητας, μπορούν να αποκαταστήσουν τα παραπάνω προβλήματα με τη χρήση της ίδιας ψηφιακής ταυτότητας σε διαφορετικούς ιστότοπους. Μερικά διαθέσιμα αυτήν τη στιγμή για παράδειγμα είναι το Facebook Login και το Google Login. Στα οποία δεν χρειάζεται πλέον όνομα χρήστη και κωδικό πρόσβασης για να εγγραφεί κάποιος σε μια συγκεκριμένη πλατφόρμα, μειώνοντας έτσι το πρόβλημα του πολλαπλασιασμού των πληροφοριών. Επίσης, δεδομένου ότι οι ομοσπονδιακές περιπτώσεις όπως το Facebook και η Google είναι αξιόπιστο ότι έχουν μια ασφαλή πολιτική ψηφιακής ταυτότητας φαίνεται ότι αντιμετωπίζεται επίσης το πρόβλημα της εξουσιοδότησης. Ωστόσο, αυτό σημαίνει ότι οι χρήστες πρέπει να βασίζονται στις ομοσπονδιακές οντότητες και να τις εμπιστεύονται, κάτι που τις καθιστά ισχυρές. Με αυτό το τρόπο οι χρήστες εξακολουθούν να μην έχουν κανέναν έλεγχο στην ψηφιακή τους ταυτότητα αφού δεν γνωρίζουν ποια ακριβώς δεδομένα συλλέγονται και ποιες πληροφορίες χρησιμοποιούνται. Ένα πρόσφατο παράδειγμα είναι το σκάνδαλο της Cambridge Analytica όπου το Facebook έδωσε αδέσμευτα και χωρίς άδεια, πρόσβαση σε στοιχεία προσωπικής ταυτοποίησης (PII) άνω των 87 εκατομμυρίων χρηστών του Facebook χωρίς τη συγκατάθεσή τους στα δεδομένα, στην εταιρεία Cambridge Analytica [28]. Το Self-Sovereign Identity (SSI) είναι μια πιο πρόσφατη λύση για αυτό το πρόβλημα.

Έτσι, με το τίτλο Self-Sovereign Identity περιγράφουμε ένα μοντέλο στο οποίο οι χρήστες έχουν τον πλήρη έλεγχο της ταυτότητάς τους. Ο Christopher Allen στο δοκίμιο The Path to Self-Sovereign Identity από το 2016 [23] εξηγήσει τι σημαίνει να είσαι κυρίαρχος του εαυτού σου, ή με άλλα λόγια, να έχει τον πλήρη έλεγχο της ταυτότητάς σου. Στο δοκίμιο The Path to Self-Sovereign Identity από το 2016 [23], ο Christopher Allen δημιούργησε μία ολοκληρωμένη λίστα των ιδιοτήτων του Self-Sovereign Identity. Οι 10 ιδιότητες του C. Allen του Self-Sovereign Identity είναι:

i. Ύπαρξη. Οι χρήστες πρέπει να έχουν ανεξάρτητη ύπαρξη.
ii. Έλεγχος. Οι χρήστες πρέπει να ελέγχουν την ταυτότητά τους.
iii. Πρόσβαση. Οι χρήστες πρέπει να έχουν πρόσβαση στα δικά τους δεδομένα.
iv. Διαφάνεια. Τα συστήματα και οι αλγόριθμοι πρέπει να είναι διαφανή.
v. Επιμονή. Οι ταυτότητες πρέπει να είναι μακροχρόνιες.
vi. Φορητότητα. Πληροφορίες και υπηρεσίες για την ταυτότητα πρέπει να είναι μεταφερόμενες.

vii. Διαλειτουργικότητα. Οι ταυτότητες πρέπει να είναι όσο το δυνατόν ευρέως χρησιμοποιήσιμες.
viii. Συγκατάθεση. Οι χρήστες πρέπει να συμφωνήσουν με τη χρήση της ταυτότητάς τους.
ix. Ελαχιστοποίηση. Η γνωστοποίηση των αξιώσεων πρέπει να ελαχιστοποιείται.
x. Προστασία. Τα δικαιώματα των χρηστών πρέπει να προστατεύονται.

Το SSI καταργεί την ανάγκη για μια κεντρική αξιόπιστη αρχή. Οι χρήστες μπορούν να αποθηκεύουν τα δεδομένα της ταυτότητάς τους σε τοπικές συσκευές και να παρέχουν τις απαιτούμενες πληροφορίες σε όσους τις χρειάζονται για σκοπούς επικύρωσης. Το Bitcoin έχει παίξει σημαντικό ρόλο στην εξέλιξη του SSI λόγω της υποστήριξής του Distributed Ledger Technology (DLT) [33]. Το DLT φαίνεται να είναι πολλά υποσχόμενο για την SSI δεδομένου ότι δεν απαιτεί μια κεντρική αρχή για την επικύρωση των συναλλαγών. Λόγω της φύσης του, όλα τα δημοσιευμένα τα δεδομένα αποθηκεύονται μόνιμα. Είναι επίσης διαφανές γιατί το αποκεντρωμένο δίκτυο είναι σε θέση να επιτύχει συναίνεση στο δίκτυο [33]. Αν και το blockchain φαίνεται πολλά υποσχόμενο, υπάρχουν ορισμένοι περιορισμοί σε σχέση με το SSI. Για παράδειγμα, όταν οι χρήστες χάνουν το ζεύγος ιδιωτικού/δημόσιου κλειδιού τους, αναγκάζονται να ξεκινήσουν τη διαδικασία επαλήθευσης ταυτότητας από την αρχή για την αποκατάσταση της ψηφιακής τους ταυτότητας.

1.4 Ασφάλεια και ιδιωτικότητα με τη χρήση τεχνολογίας Blockchain

Σημαντικό ρόλο στην ιδιωτικότητα και ασφάλεια των δεδομένων μπορεί να έχει η τεχνολογία του blockchain η οποία έκανε τα πρώτα τις βήματα με την εμφάνιση των πρώτων κρυπτονομισμάτων όπως το Bitcoin. Το blockchain έχει σημαντικά πλεονεκτήματα στην ιδιωτικότητα των δεδομένων όπως η αδύνατη παραποίηση των δεδομένων που υπάρχουν σε αυτό. Αν ένας πολίτης αποφασίσει να μοιραστεί κάποιες πληροφορίες και προσωπικά του δεδομένα με κάποια υπηρεσία ή έναν δημόσιο φορέα μέσω του blockchain, τα δεδομένα αυτά θα παραμείνουν στο blochchain αυτούσια. Αυτό σημαίνει ότι με βάση τα πρωτόκολλα που έχει δημιουργηθεί το blockchain, η πληροφορία που υπάρχει σε αυτό δεν μπορεί να παραποιηθεί και να μεταβληθεί από καμία υπηρεσία ή φορέα που έχει πρόσβαση στο blockchain. Αυτό ισχύει ακόμη και για τον ίδιο χρήστη που αποφάσισε να μοιραστεί την πληροφορία αυτή. Ένα ακόμη

προνόμιο που μπορεί να παρέχει στους πολίτες το blockchain είναι η ανωνυμία. Οποιαδήποτε δεδομένα αναρτώνται στο blockchain δεν απαιτούν κανένα στοιχείο που να συσχετίζεται με την φυσική ή ψηφιακή ταυτότητα του προσώπου που τα μοιράστηκε. Αυτό σημαίνει ότι ο κάθε πολίτης μπορεί να μοιραστεί προσωπικά του δεδομένα με κάποιο δημόσιο φορέα ή υπηρεσία σε απόλυτη εχεμύθεια. Αξιοσημείωτο είναι το γεγονός ότι το blockchain παρέχει μεγάλη σταθερότητα δικτύου. Η τεχνολογία blockchain αποκλίνει από το πρότυπο που ακολουθούν οι περισσότερες επιχειρήσεις ή δημόσιοι φορείς και υπηρεσίες. Δηλαδή, οι πληροφορίες και τα δεδομένα δεν αποθηκεύονται με κεντρικό τρόπο (π.χ. Servers). Αντιθέτως, είναι μία τεχνολογία που χρησιμοποιείται για τον χειρισμό δεδομένων αποκεντρωμένα. Αυτό σημαίνει ότι αν ένας πολίτης αποφασίσει να μοιραστεί δεδομένα του χρησιμοποιώντας το blockchain, θα μοιραστούν αυτομάτως σε όλους τους κόμβους που απαρτίζουν το blockchain. Δηλαδή, πληροφορίες των πολιτών δεν αποθηκεύονται κάπου μεμονωμένα. Με αυτόν τον τρόπο είναι αρκετά δύσκολο να χαθούν οι πληροφορίες αν υπάρξει κάποια βλάβη στο δίκτυο. Αυτές είναι κάποιες από τις προκλήσεις των κεντρικών συστημάτων που λύνει το blockchain.

2 Βιβλιογραφική έρευνα

Το γενικό χαρακτηριστικό του παρόντος αποκεντρωμένου συστήματος είναι ο πλήρης και ασφαλής έλεγχος των προσωπικών δεδομένων των πολιτών καθώς συμμετέχουν σε όλες τις διαδικασίες. Ένας βασικός παράγοντας προκειμένου να υλοποιηθεί αυτό το σύστημα είναι η αποθήκευση και η διάδοση δεδομένων. Με την ανάπτυξη του Bitcoin, πολλοί χρήστες από την κοινότητα θεώρησαν ότι το blockchain μπορούσε να χρησιμοποιηθεί ως μία πλατφόρμα διάδοσης δεδομένων πέραν από ένα σύστημα συναλλαγών. Έτσι, χρησιμοποιήθηκαν διάφορες μέθοδοι όπως η P2FKH (Pay-to-public-key-hash) που αναγράφεται στο άρθρο [15]. Βάσει αυτής της μεθόδου, ο χρήστης δεν έχει κάποιο δημόσιο κλειδί ώστε να κατακερματίσει τα δεδομένα που θέλει να αποθηκεύσει. Έτσι, οι εκροές αυτών των συναλλαγών δεν θα μπορέσουν να δαπανηθούν. Οι miners επειδή δεν μπορούν να γνωρίζουν αν το αποτέλεσμα αυτού του κατακερματισμού προέρχεται από κάποιο δημόσιο κλειδί, θα πρέπει να παρακολουθούν αυτές τις έγκυρες αδαπάνητες εκροές συναλλαγών για πάντα. Με αυτό τον τρόπο οι χρήστες μπορούν να αποθηκεύσουν δεδομένα όπως κείμενα, εικόνες ακόμη και αρχεία μορφής .mp3.[15]

Η εμφάνιση του Ethereum blockchain το Νοέμβριο του 2013 ξεπέρασε αρκετούς περιορισμούς που είχε το Bitcoin. Σύμφωνα με τον V.Buterin [18] ο σκοπός ήταν η δημιουργία ενός blockchain που να συνδυάζει δημόσιες οικονομικές συναλλαγές και ταυτόχρονα να έχει πληρότητα Turing ούτως ώστε οι προγραμματιστές να μπορούν να δημιουργήσουν εφαρμογές που να επωφελούνται από το αποκεντρωμένο blockchain. Αυτό το επιτυγχάνουν με την ένταξη των smart contracts, ένα σετ κρυπτογραφημένων κανόνων που εκτελούνται μόνο αν πληρούνται κάποιες συγκεκριμένες προϋποθέσεις.[12]

Με την ευελιξία που παρέχει το Ethereum blockchain εμφανίστηκαν ενδιαφέρουσες εργασίες σε διάφορους τομείς.

2.1 Διαχείριση προσωπικής ταυτότητας

Μία αξιοσημείωτη εργασία πάνω στον χειρισμό προσωπικών δεδομένων είναι η δημιουργία μίας αποκεντρωμένης εφαρμογής διαχείρισης στοιχείων ταυτοπροσωπίας[19]. Σύμφωνα με αυτή την εργασία, ο χρήστης έχει την πλήρη πρόσβαση στα προσωπικά του στοιχεία και μπορεί να διαχειριστεί όποια από αυτά θέλει να μοιραστεί με διάφορες υπηρεσίες. Με αυτόν τον τρόπο ο χρήστης μπορεί να

χρησιμοποιήσει τις πληροφορίες του όπως εκείνος επιθυμεί χωρίς να χρειάζεται άδεια από κάποιον τρίτο όπως θα γινόταν σε ένα κεντρικό σύστημα (π.χ. server).

Ακόμη μία παρόμοια εργασία πάνω στη διαχείριση των προσωπικών ταυτοτήτων είναι η δημιουργία ενός Domain Name System (DNS). Μέσω του DNS-IdM, ένα άτομο μπορεί να κάνει χρήση των πραγματικών χαρακτηριστικών της ταυτότητάς του για να δημιουργήσει μια ψηφιακή ταυτότητα που μπορεί να χρησιμοποιηθεί από διάφορους παρόχους υπηρεσιών για να επικυρώσουν τον χρήστη και να του προσφέρουν τις υπηρεσίες τους με βάση τα επαληθευμένα χαρακτηριστικά. Η χρήση του blockchain ως ασφαλούς και αξιόπιστου δικτύου για την παροχή ταυτοτήτων (με συναφή χαρακτηριστικά) και την εκμετάλλευση των smart contracts για την ασφαλή απόκτηση χαρακτηριστικών της ταυτότητας από αντίστοιχους χρήστες, ξεχωρίζει το DNS-IdM, όχι μόνο από τα συμβατικά συστήματα διαχείρισης ταυτότητας, αλλά και από τις πιο πρόσφατα εφαρμογές που έχουν γίνει στις υπηρεσίες ταυτότητας που βασίζονται σε blockchain. Τα συμβατικά συστήματα διαχείρισης ταυτότητας βασίζονται κυρίως σε τρίτες αρχές για την επαλήθευση των στοιχείων σχετικά με τα χαρακτηριστικά της ταυτότητας, τα οποία αφού επαληθευτούν, παραμένουν έγκυρα ακόμη και αν ανακληθούν ή ενημερωθούν από τους χρήστες· λαμβάνοντας υπόψη ότι, οι υπηρεσίες ταυτότητας που βασίζονται σε blockchain είτε βασίζονται αποκλειστικά στους χρήστες για τον καθορισμό των χαρακτηριστικών ταυτότητάς τους είτε επιτρέπουν στους χρήστες να ελέγχουν την αποκάλυψη των χαρακτηριστικών με βάση την αποδοχή τους. Το DNS-IdM επιτρέπει στους χρήστες να διαχειρίζονται την ταυτότητά τους, ενώ για τους παρόχους υπηρεσιών, τους δίνει τη δυνατότητα να κάνουν χρήση των υφιστάμενων χαρακτηριστικών ταυτότητας και, εάν δεν υπάρχουν τα απαιτούμενα χαρακτηριστικά, να τα ζητούν απευθείας από τους χρήστες μέσω έξυπνων συμβολαίων. Ολόκληρη η διαδικασία διαχείρισης ταυτότητας (δηλαδή, επιμονή χαρακτηριστικών, αίτημα και επαλήθευση) εκτελείται στο παρασκήνιο από το συνδυασμό ενός εξουσιοδοτημένου και ταυτόχρονα μη-εξουσιοδοτημένου blockchain σε συνδυασμό με smart contracts. Στις εγγενείς ιδιότητες του blockchain, η ανθεκτικότητα στην παραβίαση, η μονιμότητα και η ιχνηλασιμότητα καθιστούν το DNS-IdM ασφαλές και αξιόπιστο.[36]

2.2 Υγειονομική περίθαλψη

Μία ακόμη σημαντική εργασία που σχετίζεται με τον ιατρικό τομέα είναι η δημιουργία ενός ευρετηρίου το οποίο παρέχει φαρμακογονιδιωματικά δεδομένα[22]. Με τα φαρμακογονιδιωματικά δεδομένα να γίνονται όλο και πιο αναπόσπαστο

κομμάτι των αποφάσεων κλινικής θεραπείας, χρειάζεται ένας αποτελεσματικός τρόπος αποθήκευσης αυτών των δεδομένων ούτως ώστε να γίνεται γρήγορη αναζήτηση και η προσπέλαση σε αυτά. Η εργασία αυτή επιτυγχάνει την γρήγορη αναζήτηση ακόμη και σε πολύ μεγάλο ποσοστό εγγραφών στο ευρετήριο.

Μία ακόμη εφαρμογή είναι η Guardtime, μια εταιρεία ασφάλειας δεδομένων με έδρα την Ολλανδία, η οποία συνεργάστηκε με την κυβέρνηση της Εσθονίας για τη δημιουργία ένα framework που βασίζεται σε blockchain για την επικύρωση της ταυτότητας των ασθενών[30]. Σε όλους τους πολίτες εκδόθηκε μια έξυπνη κάρτα, η οποία συνδέει τα δεδομένα EHR (Electronic Health Records) τους με την ταυτότητα που βασίζεται στο blockchain. Σε κάθε ενημέρωση του EHR εκχωρείται κατακερματισμός και καταχωρείται στο blockchain. Αυτή η προσέγγιση διασφαλίζει ότι τα δεδομένα εντός του EHR περιέχουν μια αμετάβλητη διαδρομή ελέγχου και ότι τα αρχεία δεν μπορούν να τροποποιηθούν κακόβουλα. Τα αμετάβλητα, χρονικά σφραγισμένα αρχεία καταγραφής δεδομένων μπορούν επίσης να αρχειοθετήσουν την κατάσταση των πληροφοριών από τις υπάρχουσες βάσεις δεδομένων υγειονομικής περίθαλψης. Οποιαδήποτε ενημέρωση στη βάση δεδομένων υγειονομικής περίθαλψης, όπως ο προγραμματισμός ραντεβού, εκχωρείται χρονική σήμανση και υπογράφεται κρυπτογραφικά σε ένα μπλοκ. Δεδομένης της πρόσφατης προσοχής στην ακεραιότητα των δεδομένων λόγω των ανησυχιών σχετικά με την απάτη στον προγραμματισμό στη Διοίκηση Βετεράνων και τον κίνδυνο χειραγώγησης δεδομένων εμφυτεύσιμων ιατρικών συσκευών, όπως βηματοδότες, ένα τέτοιο σύστημα έχει πολλά πιθανά οφέλη που εγγυώνται ότι τυχόν τροποποιήσεις στο αρχείο υγειονομικής περίθαλψης είναι ασφαλές και ελεγχόμενο.[24]

Η Gem είναι ακόμη μία εταιρία η οποία έχει εμπλακεί σε αυτό τον τομέα. Το Gem Health Network αντιπροσωπεύει ένα οικοσύστημα υγειονομικής περίθαλψης που συνδυάζει επιχειρήσεις, ιδιώτες και εμπειρογνώμονες οι οποίοι, ταυτόχρονα, βελτιώνουν την ασθενοκεντρική φροντίδα ενώ αντιμετωπίζουν ζητήματα λειτουργικής αποτελεσματικότητας. Αυτό το δίκτυο είναι επομένως ένα παράδειγμα προσέγγισης με blockchain που παρέχει σε όλους τους σχετικούς ιατρικούς φορείς διαφανή και σαφή πρόσβαση στις πιο πρόσφατες πληροφορίες θεραπείας. Από τη μία πλευρά, αυτό μπορεί να περιορίσει την ιατρική αμέλεια λόγω ξεπερασμένων πληροφοριών και ως εκ τούτου να αποτρέψει προβλήματα υγείας σε πρώιμο στάδιο. Αυτό μπορεί να οδηγήσει σε εκτεταμένη εξοικονόμηση κόστους αξίας. Από την άλλη πλευρά, επιτρέπει στους εμπλεκόμενους ιατρούς να παρακολουθούν τις

αλληλεπιδράσεις μεταξύ του ασθενούς και όλων των γιατρών που έχουν λάβει χώρα στο παρελθόν. Κατά συνέπεια, η συνολική θεραπεία ενός ασθενούς χαρακτηρίζεται με διαφανή τρόπο, σύμφωνα με την οποία δημιουργείται μια εντελώς νέα πληροφόρηση και επίπεδο εμπιστοσύνης μεταξύ όλων των ιατρικών ενδιαφερόμενων φορέων.[30]

2.3 Supply Chain

Μία εργασία που έχει γίνει πάνω στον τομέα του Supply Chain [27], επιδιώκει να αναλύσει ένα μοντέλο απλής αλυσίδας εφοδιασμού (SC). με κύριο στόχο την αξιολόγηση των λειτουργικών και οικονομικών οφελών που μπορούν να αποκομίσουν τα μέλη του SC κατά τη μετάβαση από μια παραδοσιακή πλατφόρμα σε blockchain κατά την πραγματοποίηση συναλλαγών. Από την άποψη αυτή, διερευνάται ένα SC που αποτελείται από δύο εταιρίες, έναν προμηθευτή και έναν λιανοπωλητή. Οι εταιρείες διαπραγματεύονται και ορίζουν τις στρατηγικές τους σε μια διαδικτυακή πλατφόρμα. Ο προμηθευτής είναι ο ηγέτης της αλυσίδας και ορίζει έναν ορισμένο αριθμό διαδικτυακών υπηρεσιών, που θα παραδοθούν. Ο έμπορος λιανικής είναι ο ακόλουθος της αλυσίδας, δείχνει μια συγκεκριμένη προθυμία να αγοράσει από τον προμηθευτή και ορίζει την τελική τιμή των προϊόντων, καθώς και τον αριθμό των αγαθών προς αγορά.

Παρόμοιες εφαρμογές στο τομέα του Supply Chain έχουν γίνει και στο κομμάτι του φαγητού όπως μπορούμε να δούμε στην εργασία ‘An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain’ [31]. Στην οποία εισάγεται ένα δίκτυο επικάλυψης peer-to-peer που περιλαμβάνει μέλη της εφοδιαστικής αλυσίδας. Το δίκτυο επικάλυψης σχηματίζει ένα κατανεμημένο δίκτυο που περιλαμβάνει πολλούς ενδιαφερόμενους. Αυτό το δίκτυο peer-to-peer είναι χτισμένο πάνω στο σύστημα της αλυσίδας εφοδιασμού, επιτρέποντας στους ενδιαφερομένους που συνδέονται με αυτό να επικοινωνούν. Όλα τα μέλη της εφοδιαστικής αλυσίδας αρχικοποιούνται στην αρχή της επικοινωνίας και προσδιορίζονται από ένα δημόσιο κλειδί. Ένα νέο μέλος γίνεται αποδεκτό στην επικάλυψη εάν εγκριθεί από απαρτία. «απαρτία» είναι ο ελάχιστος αριθμός μελών που απαιτείται για την επίτευξη μίας συμφωνίας. Όλα τα μέλη του δικτύου επικάλυψης έχουν μια λίστα εγκεκριμένων κλειδιών μελών που είναι αποθηκευμένα στο τοπικό χώρο αποθήκευσης τους. Χρησιμοποιούνται smart contracts για να διασφαλισθεί ότι οι κανόνες και οι πολιτικές τηρούνται από τα μέρη στο δίκτυο επικάλυψης. Σε αυτήν την αρχιτεκτονική χρησιμοποιούνται smart contracts με δύο τρόπους. Πρώτον,

εφαρμόζονται από μία τρίτη αρχή που προσφέρει διαφάνεια και αποτελεσματικότητα, δεύτερον, εφαρμόζονται για να διέπουν τις λειτουργίες μεταξύ των ενδιαφερομένων.

2.4 Internet of Things

Τα τελευταία χρόνια η βιομηχανία του Internet of Things (IoT) μεγαλώνει ραγδαία. Με ανάλογο ρυθμό αυξάνονται και τα δεδομένα που δημιουργούνται από τους αισθητήρες IoT. Στα πλαίσια του IoT έχει γίνει μια σχετική εργασία για την αξιοποίηση των δεδομένων από IoT αισθητήρες [34]. Σκοπός αυτής της μελέτης είναι η δημιουργία ενός Ethereum blockchain Decentralized Application (DApp) που επιτρέπει στους χρήστες να αγοράζουν και να πωλούν εύκολα δεδομένα αισθητήρα IoT, χρησιμοποιώντας ένα προσαρμοσμένο διακριτικό ως νόμισμα πληρωμής. Η εφαρμογή είναι ένα marketplace για αισθητήρες καιρού IoT, αλλά έχει δημιουργηθεί με τέτοιο τρόπο, ώστε με ελάχιστες τροποποιήσεις, θα μπορούσε να μετατραπεί σε εφαρμογή για οποιοδήποτε άλλο είδος συσκευής IoT.

Ακόμη μία εργασία πάνω στο κομμάτι των IoT συσκευών είναι η ‘Managing IoT Devices using Blockchain Platform’ [29] η οποία έχει ως σκοπό την διαχείριση πολλαπλών IoT συσκευών. Σε αυτή την εργασία χρησιμοποιήθηκαν μερικές συσκευές IoT ούτως ώστε να αποδειχθεί ένα concept. Πιο συγκεκριμένα, χρησιμοποιήθηκαν ένα smart phone, και τρία Raspberry Pis. Το κάθε Raspberry Pi χρησιμοποιήθηκε ως μετρητής για να παρακολουθεί τη χρήση ηλεκτρικής ενέργειας, ένα κλιματιστικό και μια λάμπα. Χρησιμοποιώντας το smart phone, ο χρήστης μπορεί να ρυθμίσει την πολιτική. Για παράδειγμα, ο χρήστης μπορεί να ρυθμίσει τις συσκευές ώστε να ενεργοποιούν τη λειτουργία εξοικονόμησης ενέργειας όταν η κατανάλωση ηλεκτρικής ενέργειας φτάσει τα 150 KW. Όταν ο χρήστης ρυθμίζει τη διαμόρφωση μέσω smartphone, τα δεδομένα αποστέλλονται στο δίκτυο Ethereum. Εν τω μεταξύ, συσκευές όπως ο λαμπτήρας ή το κλιματιστικό ανακτούν τις τιμές της πολιτικής περιοδικά από το Ethereum. Επίσης, ο μετρητής παρακολουθεί τη χρήση ηλεκτρικής ενέργειας και την ενημερώνει στο Ethereum. Έτσι, τρεις διαφορετικές διαδικασίες συμβαίνουν ταυτόχρονα.

Με την ευελιξία που παρέχει το Ethereum blockchain έχει βοηθήσει σε πολλούς τομείς όπως στα οικονομικά καθώς και τον χειρισμό προσωπικών πληροφοριών όπως είναι η δημιουργία ενός αποκεντρωμένου IPFS (InterPlanetary File System) συστήματος κοινωνικού δικτύου[14]. Η εργασία αυτή στοχεύει στη δημιουργία ενός συστήματος κοινωνικού δικτύου ενσωματώνοντας το IPFS. Το IPFS είναι ένα

πρωτόκολλο που σχεδιάστηκε να αποθηκεύει υπερμέσα με τη μέθοδο peer-to-peer σε ένα κατανεμημένο σύστημα αρχείων.

3 Τεχνολογία Blockchain

3.1 Τι είναι το Blockchain;

Το Blockchain είναι ένα σύστημα εγγραφών βάσει του οποίου γίνονται συναλλαγές αξιών μέσα σε ένα δίκτυο που είναι της μορφής peer-to-peer[1]. Αξίζει να σημειωθεί ότι αυτές οι αξίες δεν απαρτίζονται μόνο από χρήματα. Με αυτόν τον τρόπο δεν χρειάζονται αξιόπιστοι διαμεσολαβητές όπως τράπεζες ή άλλες υπηρεσίες μεσεγγύησης με σκοπό τη ύπαρξη κάποιου τρίτου αξιόπιστου μέρους.[1]

Το Blockchain είναι ένα κοινόχρηστο, αποκεντρωμένο, και ανοιχτό καθολικό (ledger) σύστημα συναλλαγών. Αυτή η καθολική βάση δεδομένων επαναλαμβάνεται και βρίσκεται σε ένα μεγάλο αριθμό κόμβων που το απαρτίζουν. Κάθε συναλλαγή προσαρτάται στη καθολική βάση δεδομένων, η οποία δεν μπορεί να αλλαχθεί. Έτσι, κάθε συναλλαγή καταγράφεται μόνιμα, Με κάθε επιπρόσθετη συναλλαγή, η καταγραφή αυτής αντικατοπτρίζεται σε όλους τους κόμβους που φιλοξενούν τη καθολική βάση δεδομένων.[1]

3.2 Ledger

Το ledger είναι μία συλλογή από συναλλαγές. Ιστορικά, το ledger χρησιμοποιούταν για την καταγραφή συναλλαγών σε διάφορα εμπορεύματα και υπηρεσίες. Με την ανάπτυξη της τεχνολογίας και της πληροφορικής, το ledger μπορούσε να αποθηκευτεί ψηφιακά σε μεγάλες βάσεις δεδομένων που είχαν στην κατοχή τους κεντρικοί έμπιστοι οργανισμοί. Στη συνέχεια, υπήρξε ενδιαφέρον στο να ερευνηθεί περεταίρω η διανομή κατοχής του ledger. Η τεχνολογία του Blockchain είχε την δυνατότητα να υποστηρίξει την διανομή κατοχής του ledger. Έτσι, η κατοχή του ledger είχε αποκεντρωμένη μορφή και λάθη όπως η καταστροφή του, μπορούσαν πλέον να

[1] Ένα δίκτυο υπολογιστών peer-to-peer (ή P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα.[3]

αποφευχθούν διότι υπήρχαν πολλαπλά αντίγραφα του ledger σε πολλαπλούς κόμβους όπου συγχρονίζονταν ταυτόχρονα με κάθε νέα εισαγωγή συναλλαγής που συνέβαινε.[2]

3.3 Blocks

Όταν ένας χρήστης του Blockchain υποβάλλει μία υποψήφια συναλλαγή προς πραγματοποίηση χρησιμοποιώντας ένα λογισμικό, στέλνεται αυτομάτως η συναλλαγή από το λογισμικό προς έναν ή περισσότερους κόμβους. Αυτοί οι κόμβοι μπορεί να έχουν τη δυνατότητα δημοσίευσης της συναλλαγής ή όχι. Ακόμη και μετά την διανομή της εκκρεμής συναλλαγής σε όλους τους κόμβους, θα πρέπει να περιμένει στην ουρά μέχρι να προστεθεί στο blockchain από ένα κόμβο που έχει τη δυνατότητα να το δημοσιεύσει. Η συναλλαγή προστίθεται στο blockchain όταν ένας κόμβος δημοσίευσης δημοσιεύσει ένα block.[2]

Το block περιέχει μία επικεφαλίδα και δεδομένα block. Η επικεφαλίδα περιέχει κάποια μεταδεδομένα. Τα δεδομένα block περιέχουν κάποιες επαληθευμένες και αυθεντικές συναλλαγές οι οποίες εισήχθησαν επιτυχώς στο δίκτυο του blockchain. Πιο συγκεκριμένα το block περιέχει:

- Επικεφαλίδα του block
  - Τον αύξον αριθμό του block
  - Την τιμή κατακερματισμού[2] (hash) της επικεφαλίδας του προηγούμενου block
  - Μια τιμή κατακερματισμού που αντιπροσωπεύει τα δεδομένα του block
  - Τη χρονική σήμανση
  - Το μέγεθος του block
  - Την τιμή nonce[3]
- Δεδομένα του block

[2] Μία τιμή κατακερματισμού (hash) είναι μία αριθμητική τιμή σταθερού μήκους η οποία προσδιορίζει μοναδικά τα δεδομένα.[4]

[3] Η τιμή nonce χρησιμοποιείται σε συστήματα Proof-of-Work (PoW) για να μεταβάλλουν την είσοδο σε μια συνάρτηση κατακερματισμού έτσι ώστε να ληφθεί μια τιμή κατακερματισμού για μια συγκεκριμένη είσοδο που πληροί ορισμένες αυθαίρετες προϋποθέσεις.[5]

- Μια λίστα συναλλαγών και συμβάντων του ledger που περιλαμβάνονται στο block
- Όποια άλλα δεδομένα μπορεί να χρειαστεί να καταγραφούν

Τα block δημιουργούν μια συνεχή αλυσίδα. Προκειμένου ένα block να προστεθεί στο τέλος αυτής της αλυσίδας πρέπει περιέχει τη σύνοψη του κατακερματισμού του προηγούμενου block στην επικεφαλίδα του. Έτσι έχουμε τον σχηματισμό του blockchain. [2]

3.4 Η χρήση ιδιωτικού blockchain και η διαφορά με το δημόσιο blockchain

Ένα blockchain ονομάζεται δημόσιο όταν ο κάθε συμμέτοχος μπορεί να το διαβάσει και να το χρησιμοποιήσει ώστε να φέρει εις πέρας διάφορες συναλλαγές. Έτσι δεν υπάρχει κάποια κεντρική καταχώρηση ούτε κάποιος έμπιστος τρίτος. Σε αυτό το σύστημα, οι κόμβοι του δικτύου επικυρώνουν τις επιλογές που τους παρέχουν οι προγραμματιστές αποφασίζοντας έτσι αν θα πρέπει να ενσωματώσουν τις προτεινόμενες καινούριες τροποποιήσεις.

Ένα blockchain ονομάζεται ιδιωτικό (ή ημιδιωτικό) όταν η ομόφωνη διαδικασία μπορεί να επιτευχθεί μόνο από περιορισμένους συμμέτοχους. Η πρόσβαση στην εγγραφή σε αυτό το σύστημα την έχουν οργανισμοί ενώ η πρόσβαση ανάγνωσης μπορεί να είναι δημόσια. Σε αυτή την περίπτωση δεν χρειάζεται να γίνει εξόρυξη των block[4], ούτε Proof-of-Work[5], ούτε ανταμοιβή για αυτούς που κάνουν εξόρυξη.[8]

3.5 Εξέλιξη του οικοσυστήματος

Όπως και το Bitcoin, το Ethereum είναι ένα πρωτόκολλο που βασίζεται σε blockchain. Ωστόσο, το Ethereum διαθέτει προηγμένη τεχνολογία blockchain που το καθιστά προγραμματιζόμενο, με άλλα λόγια, δεν είναι προκαθορισμένο και επιτρέπει στους χρήστες να δημιουργούν λειτουργίες διαφορετικής πολυπλοκότητας.

[4] Η εξόρυξη είναι μια υπηρεσία τήρησης αρχείων που γίνεται με τη χρήση της επεξεργαστικής ισχύς του υπολογιστή. Οι miners διατηρούν το blockchain συνεπές, πλήρες και αμετάβλητο, ομαδοποιώντας επανειλημμένα τις συναλλαγές που μεταδόθηκαν σε ένα block[6]

[5] Το Proof-of-Work (PoW) είναι μια μορφή κρυπτογραφικής απόδειξης μηδενικής γνώσης στην οποία ένα μέρος (Prover) αποδεικνύει σε άλλους (Verifiers) ότι έχει δαπανηθεί ένα συγκεκριμένο ποσό μιας συγκεκριμένης υπολογιστικής προσπάθειας. Οι επαληθευτές μπορούν στη συνέχεια να επιβεβαιώσουν αυτές τις δαπάνες με ελάχιστη προσπάθεια εκ μέρους τους (Work).[7]

Λειτουργώντας ως πλατφόρμα και με στόχο να γίνει μια γενικευμένη τεχνολογία για εφαρμογές, κοινότητες κ.λπ., το Ethereum επιτρέπει στους χρήστες του να δημιουργούν διάφορες εφαρμογές εξαιρουμένων των περιορισμών στα κρυπτονομίσματα. Η ομάδα του Ethereum δηλώνει επίσης ότι το ether δεν χρησιμοποιείται ως κύριο διακριτικό για το δίκτυο Ethereum, αλλά δημιουργείται κυρίως ως πληρωμή για υπολογισμούς. [18] Η εικονική μηχανή Ethereum είναι μια άλλη βασική τεχνολογία του Ethereum, παρόμοια με τον πυρήνα Bitcoin, το EVM στοχεύει στην εκτέλεση κώδικα αλγοριθμικής πολυπλοκότητας [34]. Για τους προγραμματιστές, το EVM επιτρέπει τη δημιουργία εφαρμογών που είναι γραμμένες σε γλώσσα προγραμματισμού συμβατή με το ίδιο το EVM. Το EVM θεωρείται επίσης ως μια από τις βασικές καινοτομίες για τον κόσμο των κρυπτονομισμάτων - ένα λογισμικό που είναι συμβατό με πολλές γλώσσες προγραμματισμού και που επιτρέπει στους προγραμματιστές να εκτελούν την εφαρμογή στην ενιαία πλατφόρμα αντί να δημιουργούν πολλές ξεχωριστές αλυσίδες μπλοκ. Με αυτόν τον τρόπο η ανάπτυξη εφαρμογών ανταποκρίνεται στα βασικά πλεονεκτήματα της τεχνολογίας blockchain, όπως η διαφάνεια, η ασφάλεια και ο μηδενικός χρόνος διακοπής λειτουργίας. Οι δυνατότητες της πλατφόρμας Ethereum προκάλεσαν μεγάλο ενδιαφέρον από διάφορους κλάδους: τραπεζικούς, κυβερνητικούς, μέσα ενημέρωσης - όλες αυτές οι βιομηχανίες είναι σε θέση να επιτρέψουν την ταχεία αυτοματοποίηση του τομέα τους εφαρμόζοντας λύσεις blockchain. Επιπλέον, η πλατφόρμα Ethereum φέρνει ευρύτερη δυνατότητα εφαρμογής και για τα κρυπτονομίσματα: εάν το βασικό ζήτημα για το Bitcoin είναι η χρήση του στον κλάδο και ότι δεν υπάρχει τίποτα πίσω από αυτό εκτός από εικασίες - η ανάπτυξη του Ethereum διασφαλίζεται από την ανάπτυξη της εφαρμογής, με βάση το EthOS - λειτουργικό σύστημα που ενεργοποιείται από το EVM. [18] Μέσω των εφαρμοζόμενων τεχνολογικών αναβαθμίσεων - το Ethereum έγινε πιο προηγμένο κρυπτονόμισμα με υψηλότερους και ταχύτερους ρυθμούς κατακερματισμού και στην ανάπτυξή του (ταχύτητα υπολογισμού λειτουργιών). Το γεγονός του μακροπρόθεσμου οράματος της εταιρείας για τη χρήση του Ethereum, η στρατηγική της μέχρι το 2030 και η στενή συνεργασία της Ethereum με τράπεζες με έδρα τις ΗΠΑ και την Ελβετία φέρνουν ισχυρότερες θέσεις στο κρυπτονόμισμα, ξεπερνώντας το Bitcoin, καθώς και σταθερότητα ως προς την τιμή , μειώνοντας τον αριθμό των εικασιών για το δίκτυο Ethereum.[35] Επιπλέον, η λύση Ethereum στο πρόβλημα της επεκτασιμότητας, της ταχύτητας και της τιμής των συναλλαγών - Raiden - υποτίθεται ότι είναι η πρώτη λύση «2 επιπέδων» για το δίκτυο Ethereum και

για το ζήτημα επεκτασιμότητας των κρυπτονομισμάτων συνολικά και μπορεί να προωθήσει την αγορά και όλα τα εξαρτώμενα altcoins που στέκονται ως βασικό υποκατάστατο του ταχύτατου δικτύου του Bitcoin. [25]

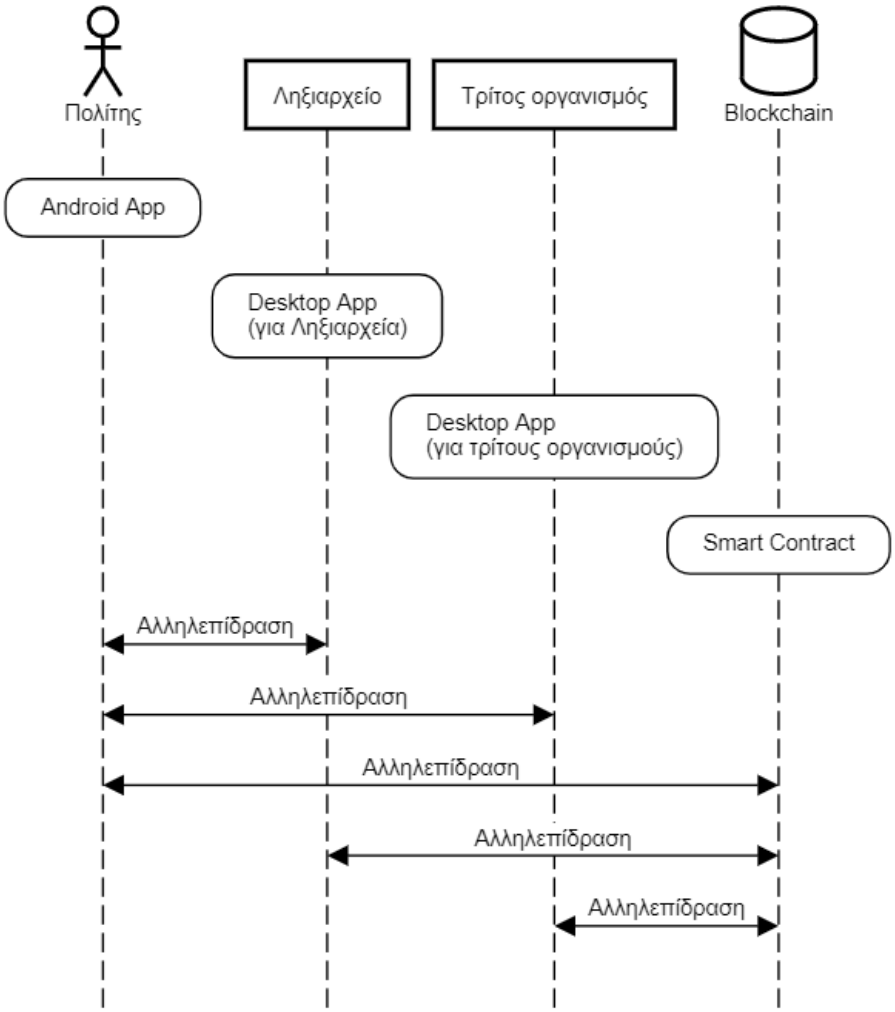
4 Σχεδιασμός Εφαρμογής

Υπάρχουν τρεις οντότητες που λαμβάνουν χώρα στη περιγραφή της διαδικασίας.

- **Πολίτης (χρήστης)**. Είναι η οντότητα που χρειάζεται να δημιουργηθούν πιστοποιητικά για αυτήν ή να λάβει δεδομένα πιστοποιητικών. Προκειμένου να γίνει αυτό θα πρέπει ο πολίτης να είναι καταχωρημένος στο σύστημα.
- **Ληξιαρχείο**. Είναι η οντότητα με την οποία αλληλεπιδρά ο πολίτης ώστε να καταχωρίσει προσωπικά του δεδομένα στο σύστημα και να δημιουργήσει ληξιαρχικές πράξεις όπως γάμου, γέννησης, θανάτου. Αυτή η οντότητα, έχει επίσης τη δυνατότητα να ζητήσει δεδομένα από τις ληξιαρχικές πράξεις του πολίτη.
- **Τρίτος οργανισμός**. Είναι η οντότητα με την οποία αλληλεπιδρά ο πολίτης ώστε να πράξει μία τρίτη διαδικασία, η οποία χρειάζεται δεδομένα από κάποιο πιστοποιητικό που έχει ο πολίτης.

Τα βασικά συστατικά που συνθέτουν αυτή τη διαδικασία είναι:

- **Smart Contract**. Παρέχει τη δυνατότητα εγγραφής και λήψης δεδομένων.
- **Blockchain**. Εκεί αναρτώνται τα δεδομένα που εισάγονται από τις συναρτήσεις του smart contract καθώς επίσης εκεί βρίσκεται όλο το smart contract.
- **Android εφαρμογή**. Είναι η εφαρμογή στη κινητή συσκευή του πολίτη ή αλλιώς χρήστη. Βάσει αυτής γίνεται η αλληλεπίδραση του πολίτη με κάποιο ληξιαρχείο ή έναν τρίτο οργανισμό.
- **Desktop εφαρμογή (ληξιαρχείου)**. Είναι η εφαρμογή που χρησιμοποιούν τα ληξιαρχεία για την εγγραφή του πολίτη στο σύστημα, για τη δημιουργία πιστοποιητικών του πολίτη καθώς και για την λήψη δεδομένων πιστοποιητικού από τον πολίτη. Η εφαρμογή αυτή αλληλεπιδρά με την android εφαρμογή.
- **Desktop εφαρμογή (τρίτου οργανισμού)**. Είναι η εφαρμογή που χρησιμοποιούν οι τρίτοι οργανισμοί για την λήψη δεδομένων πιστοποιητικού από τον πολίτη. Η εφαρμογή αυτή αλληλεπιδρά επίσης με την android εφαρμογή.



Εικόνα 1: Οι οντότητες αλληλεπιδρούν μεταξύ του μέσω των εφαρμογών και του smart contract

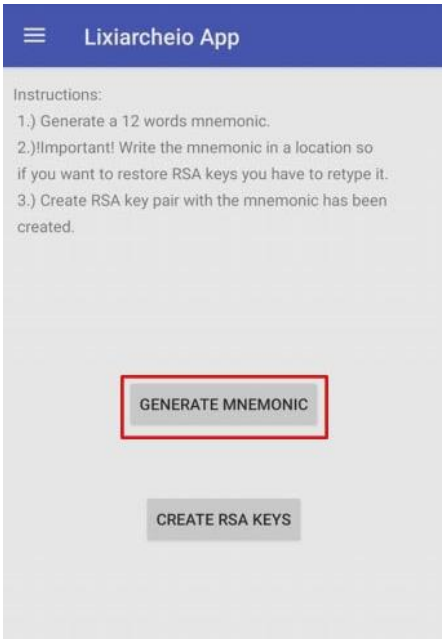
Για να γίνει κατανοητή η διαδικασία, θα αναλυθεί σε υποκεφάλαια, τόσο από την πλευρά του πολίτη όσο και από την πλευρά του ληξιαρχείου. Τα υποκεφάλαια έχουν ως εξής:

- Δημιουργία ζεύγους κλειδιών RSA από τον πολίτη
- Καταχώριση προσωπικών δεδομένων του πολίτη στο σύστημα ληξιαρχείου
- Κατανόηση της καταχώρισης ψηφιακής υπογραφής και των προσωπικών δεδομένων σε μορφή hash στο blockchain
- Περιγραφή διαδικαστικού δημιουργίας ληξιαρχικής πράξης
- Περιγραφή διαδικαστικού λήψης στοιχείων ληξιαρχικής πράξης
- Επιπλέον πληροφορίες

4.1 Δημιουργία ζεύγους κλειδιών RSA από τον πολίτη

4.1.1 Δημιουργία κλειδιών του πολίτη

Ως πρώτη φορά συμμετοχής του πολίτη στο σύστημα του ληξιαρχείου, θα πρέπει να γίνει λήψη της εφαρμογής σε κινητή συσκευή η οποία έχει λειτουργικό σύστημα Android. Κατά την πρώτη φορά εκτέλεσης της εφαρμογής ο χρήστης θα οδηγηθεί αυτομάτως σε ένα παράθυρο στο οποίο θα είναι σε θέση να δημιουργήσει το δικό του μοναδικό ζευγάρι κλειδιών RSA, σύμφωνα με το οποίο θα μπορεί να αλληλεπιδρά με το σύστημα του ληξιαρχείου. Για τη δημιουργία του θα χρειαστεί ένα μνημονικό δώδεκα λέξεων που παράγεται πατώντας το κουμπί “Generate Mnemonic”.



Εικόνα 2: Δημιουργία μνημονικού 12 λέξεων πατώντας το κουμπί "GENERATE MNEMONIC"

Αυτό το μνημονικό θα πρέπει να αποθηκευτεί κάπου ασφαλή, διότι είναι ο μόνος τρόπος να επαναφέρει το ζεύγος κλειδιών RSA σε περίπτωση που η εφαρμογή διαγραφτεί από τη κινητή συσκευή ή αν ο χρήστης επιθυμεί να αλλάξει συσκευή. Τέλος, τα κλειδιά RSA δημιουργούνται βάσει του μνημονικού που παράχθηκε πατώντας το κουμπί “Create RSA keys”.

Εικόνα 3: Δημιουργία ζεύγους RSA κλειδιών βάσει του τυχαίου μνημονικού που παράχθηκε πατώντας το κουμπί "CREATE RSA KEYS"

4.2 Καταχώριση προσωπικών δεδομένων του πολίτη στο σύστημα ληξιαρχείου

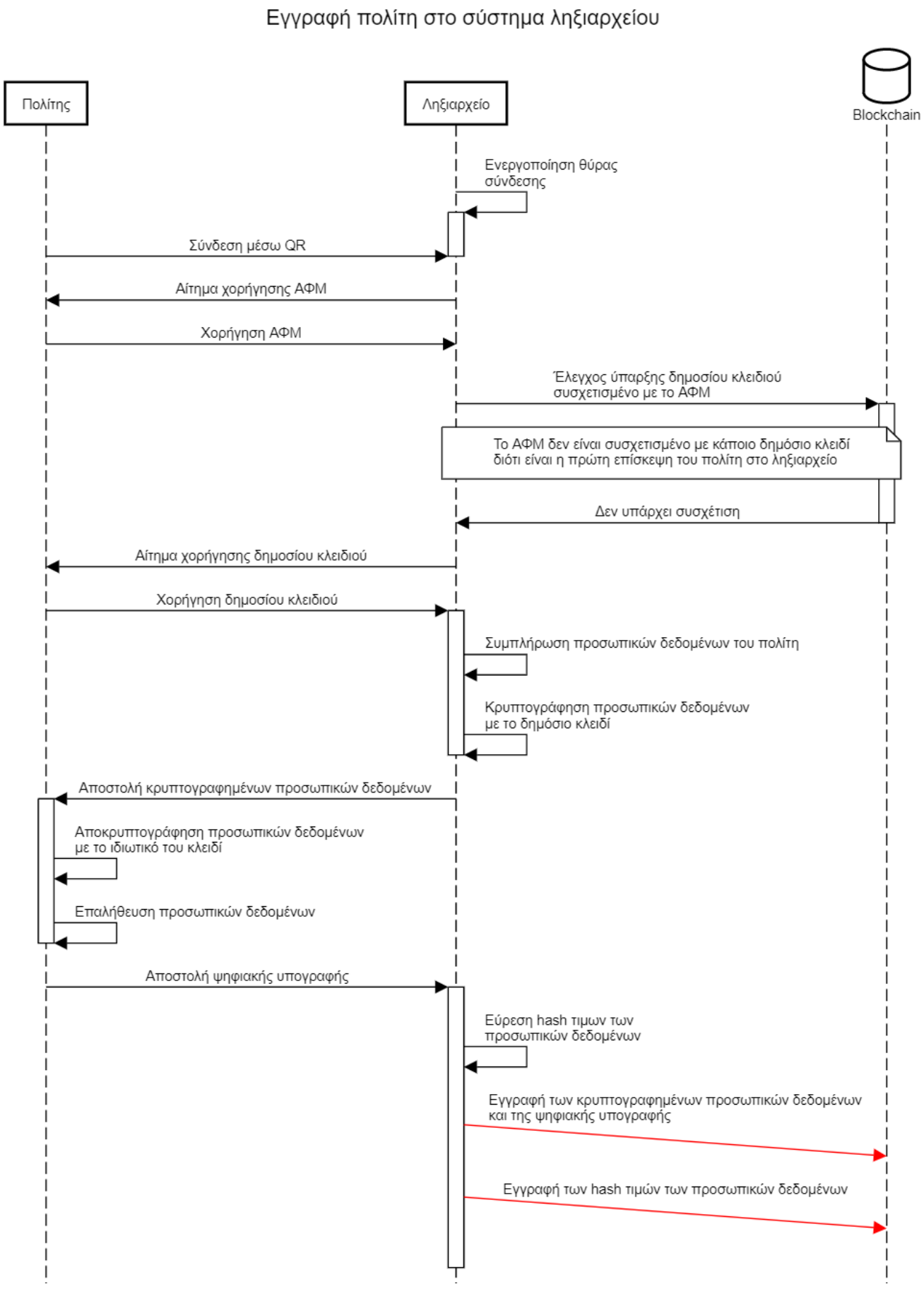
4.2.1 Πρώτη αλληλεπίδραση του πολίτη με το ληξιαρχείο

Ο πολίτης μετά από τη δημιουργία του ζευγαριού κλειδιών RSA πηγαίνει στο ληξιαρχείο. Ο υπάλληλος που τον εξυπηρετεί θα χρησιμοποιήσει την desktop εφαρμογή του, η οποία προορίζεται αποκλειστικά και μόνο για το προσωπικό των ληξιαρχείων και είναι η μόνη που μπορεί να καταχωρήσει δεδομένα στο ιδιωτικό blockchain. Κατά την πρώτη επίσκεψη του πολίτη στο ληξιαρχείο, ο υπάλληλος θα ανοίξει μια θύρα σύνδεσης για τον πολίτη. Ο πολίτης συνδέεται στο δίκτυο του ληξιαρχείου, ανοίγει την android εφαρμογή του και κάνει σάρωση του QR κωδικού που θα του παρέχει ο υπάλληλος, ώστε να γίνει η σύνδεση μεταξύ της android εφαρμογής και της desktop εφαρμογής. Μετά την εγκαθίδρυση της σύνδεσης, η εφαρμογή του ληξιαρχείου θα στείλει αυτομάτως αίτημα χορήγησης ΑΦΜ του πολίτη. Ο πολίτης θα λάβει το αίτημα χορήγησης του ΑΦΜ από το ληξιαρχείο και θα το εισάγει. Έπειτα, η desktop εφαρμογή του ληξιαρχείου, θα ελέγξει αν υπάρχει καταχωρημένο το δημόσιο κλειδί του πολίτη από το ζεύγος κλειδιών RSA που

δημιούργησε, σε αυτό το ΑΦΜ που δόθηκε. Επειδή, όπως αναφέρθηκε, ο πολίτης πηγαίνει πρώτη φορά στο ληξιαρχείο για να καταχωρήσει τα προσωπικά του δεδομένα στο σύστημα, η desktop εφαρμογή θα διαπιστώσει ότι δεν υπάρχει κάποια σύνδεση του δημοσίου κλειδιού του πολίτη με το ΑΦΜ του, άρα δεν θα είναι και καταχωρημένος στο σύστημα. Επομένως, η εφαρμογή του ληξιαρχείου θα προχωρήσει στην αποστολή αιτήματος χορήγησης του δημοσίου κλειδιού του πολίτη.

4.2.2 Εγγραφή του πολίτη στο σύστημα

Μετά την επιτυχή λήψη του δημοσίου κλειδιού, ο υπάλληλος του ληξιαρχείου θα πρέπει να καταχωρήσει τα προσωπικά δεδομένα του πολίτη (όνομα, επώνυμο, ΑΦΜ, ΑΜΚΑ), καθώς και το δημόσιο κλειδί του πολίτη. Έτσι, οποιαδήποτε αλληλεπίδραση γίνει μεταξύ του πολίτη και του ληξιαρχείου στο μέλλον, θα αφορά αυτό το δημόσιο κλειδί. Αφού συμπληρωθούν τα προσωπικά στοιχεία του πολίτη στην φόρμα από τον υπάλληλο του ληξιαρχείου, στέλνονται αυτομάτως στην android εφαρμογή του κρυπτογραφημένα, βάσει του δημοσίου κλειδιού του πολίτη. Ύστερα, αποκρυπτογραφούνται με το ιδιωτικό κλειδί από το ζεύγος κλειδιών RSA του πολίτη και εμφανίζονται στην οθόνη του χρήστη. Εκεί, ο πολίτης αποφασίζει αν τα δεδομένα που εισήχθησαν από τον υπάλληλο είναι έγκυρα. Αν δεν είναι έγκυρα ο χρήστης μπορεί να τα απορρίψει και να διακόψει την διαδικασία. Αν είναι έγκυρα, τότε αυτομάτως, υπογράφονται ψηφιακά οι τιμές των δεδομένων που δήλωσε ο πολίτης σε μορφή hash καθώς και οι κρυπτογραφημένες τιμές των δεδομένων. Η ψηφιακή υπογραφή που δημιουργήθηκε, στέλνεται από την android εφαρμογή προς το ληξιαρχείο. Σε τελικό στάδιο η desktop εφαρμογή καταχωρεί στο blockchain: τα δεδομένα κρυπτογραφημένα (όπως αυτά στάλθηκαν στον πολίτη για επιβεβαίωση), η ψηφιακή υπογραφή που στάλθηκε από τον πολίτη, καθώς και τις τιμές hash των προσωπικών δεδομένων του πολίτη.



Εικόνα 4: Διάγραμμα διαδικασίας εγγραφής του πολίτη στο σύστημα

4.3 Κατανόηση της καταχώρισης ψηφιακής υπογραφής και των προσωπικών δεδομένων σε μορφή hash στο blockchain

Με την καταχώριση της ψηφιακής υπογραφής στο blockchain. Μπορεί να γίνει επαλήθευση των στοιχείων που έχουν καταχωρισθεί. Δηλαδή, αν το ληξιαρχείο ή κάποιος τρίτος οργανισμός επιθυμήσει να κάνει επαλήθευση στοιχείων ενός πολίτη, μπορεί να λάβει από το blockchain: τις κρυπτογραφημένες τιμές, το δημόσιο κλειδί του πολίτη, καθώς και τις τιμές hash. Υστέρα, ενοποιεί τις κρυπτογραφημένες τιμές και τις τιμές hash. Έχοντας το αποτέλεσμα της ενοποίησης και το δημόσιο κλειδί του πολίτη, χρησιμοποιείται μια ειδική συνάρτηση με αυτά τα ορίσματα. Το αποτέλεσμα αυτής της συνάρτησης συγκρίνεται με την ψηφιακή υπογραφή που υπάρχει στο blockchain. Αν είναι όμοια, τότε τα δεδομένα είναι αυθεντικά και δεν υπήρξε κάποιο λάθος κατά τη καταχώριση των δεδομένων στο blockchain.

Με τη καταχώριση των προσωπικών δεδομένων του πολίτη σε μορφή hash, διασφαλίζεται η επαλήθευση στοιχείων που στέλνονται από τον πολίτη, όταν του ζητηθούν δεδομένα από ένα πιστοποιητικό του (θα δούμε παρακάτω). Το ληξιαρχείο ή ένας τρίτος οργανισμός όταν ζητήσει στοιχεία ενός πιστοποιητικού από τον πολίτη, μπορεί να επαληθεύσει τα δεδομένα του πιστοποιητικού που στέλνει ο πολίτης, εισάγοντας τα ξεχωριστά σε μια συνάρτηση hash. Τα αποτελέσματα που θα παραχθούν συγκρίνονται με τις τιμές hash που υπάρχουν στο blockchain. Αν είναι όμοιες, τότε τα δεδομένα του πιστοποιητικού που στάλθηκαν από τον πολίτη, είναι σωστά.

4.4 Περιγραφή διαδικαστικού δημιουργίας ληξιαρχικής πράξης

4.4.1 Σύνδεση του πολίτη με το ληξιαρχείο

Σε δεύτερο χρόνο, ο πολίτης καταχωρημένος πλέον στο σύστημα, μπορεί να δημιουργήσει ληξιαρχικές πράξεις, όπως, ληξιαρχική πράξη γάμου, γέννησης ή θανάτου. Για την συνέχεια περιγραφής της διαδικασίας υποτίθεται ότι ο πολίτης θέλει να δημιουργήσει μία ληξιαρχική πράξη γάμου. Κατά παρόμοιο τρόπο όπως περιεγράφηκε προηγουμένως ο χρήστης συνδέεται με το ληξιαρχείο ώστε να μπορέσει να αλληλεπιδράσει.

4.4.2 Σύνδεση του πολίτη με το ληξιαρχείο

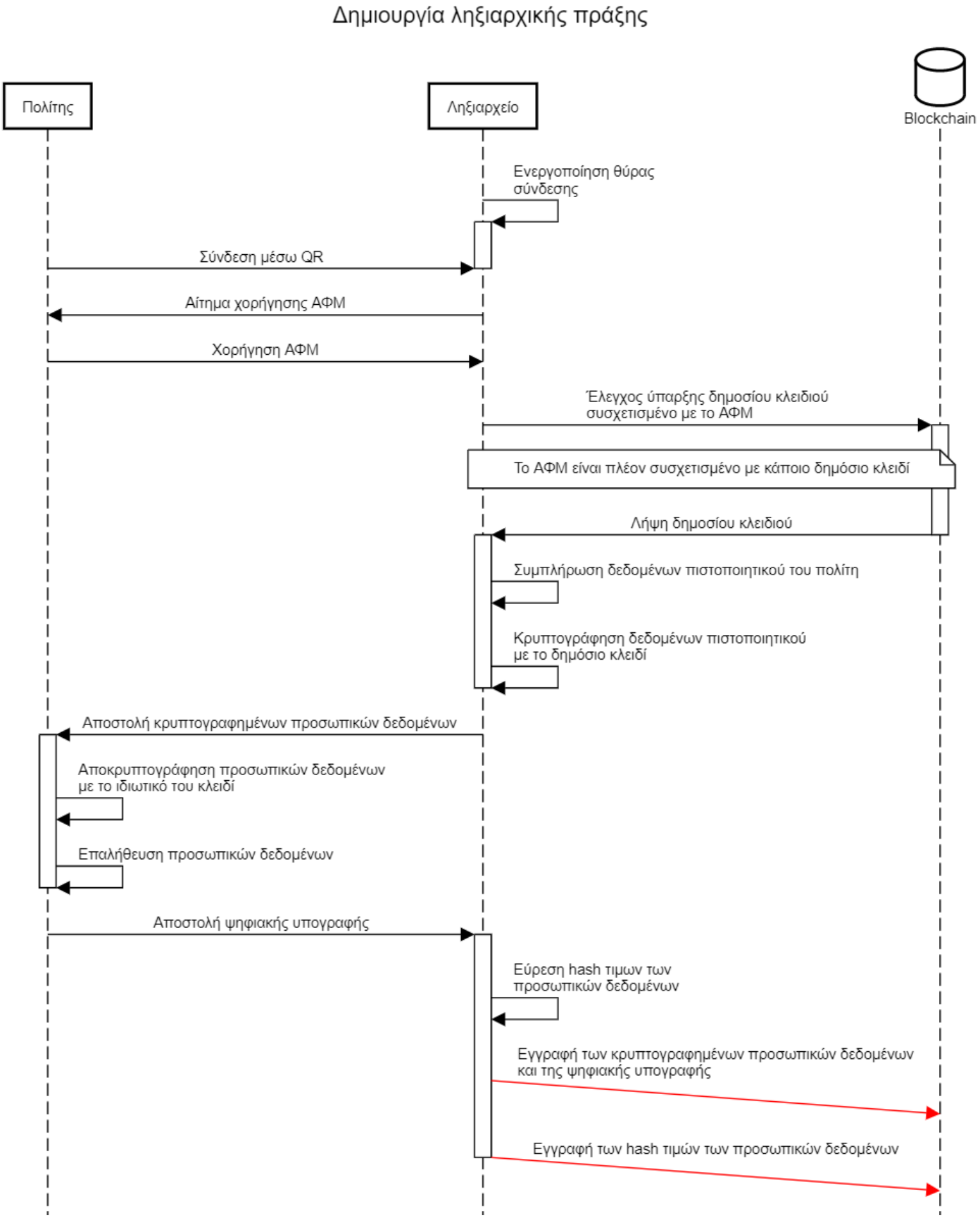
Το ληξιαρχείο θα ζητήσει το ΑΦΜ του πολίτη και πλέον θα παρατηρήσει ότι το ΑΦΜ του πολίτη είναι καταχωρημένο και συσχετισμένο με το δημόσιο κλειδί του. Ο υπάλληλος του ληξιαρχείου που τον εξυπηρετεί, χρησιμοποιώντας την desktop εφαρμογή για τα ληξιαρχεία, θα ανοίξει την φόρμα συμπλήρωσης των δεδομένων για τη δημιουργία της ληξιαρχικής πράξης γάμου. Αφού συμπληρωθεί, η desktop εφαρμογή θα στείλει τα δεδομένα στον χρήστη κρυπτογραφημένα με το δημόσιο κλειδί του πολίτη.

4.4.3 Επαλήθευση των δεδομένων από τον πολίτη

Η android εφαρμογή θα τα αποκρυπτογραφήσει με το ιδιωτικό κλειδί του πολίτη και θα τα εμφανίσει στην οθόνη του. Ο πολίτης θα πρέπει να αποφασίσει ως προς την εγκυρότητα των δεδομένων που εισήγαγε στην φόρμα ο υπάλληλος του ληξιαρχείου (ημερομηνία γάμου, τύπος γάμου, δόγμα, όνομα συζύγου, επώνυμο συζύγου, ΑΦΜ συζύγου, ΑΜΚΑ συζύγου). Σε περίπτωση που τα δεδομένα δεν είναι έγκυρα ο χρήστης μπορεί να ακυρώσει τη διαδικασία.

4.4.4 Καταχώρηση των δεδομένων στο blockchain

Αν είναι έγκυρα, τότε αυτομάτως, υπογράφονται ψηφιακά οι τιμές των δεδομένων που δήλωσε ο πολίτης σε μορφή hash καθώς και οι κρυπτογραφημένες τιμές των δεδομένων. Η ψηφιακή υπογραφή που δημιουργήθηκε, στέλνεται από την android εφαρμογή προς το ληξιαρχείο. Έπειτα, η desktop εφαρμογή του ληξιαρχείου καταχωρεί στο blockchain: τα δεδομένα κρυπτογραφημένα (όπως αυτά στάλθηκαν στον πολίτη για επιβεβαίωση), η ψηφιακή υπογραφή που στάλθηκε από τον πολίτη, καθώς και τις τιμές hash των προσωπικών δεδομένων του πολίτη.



Εικόνα 5: Διάγραμμα δημιουργίας ληξιαρχικής πράξης και εκχώρησή της στο σύστημα

4.5 Περιγραφή διαδικαστικού λήψης στοιχείων ληξιαρχικής πράξης

Έχοντας πλέον δημιουργήσει το πιστοποιητικό γάμου, ο πολίτης μπορεί να το χρησιμοποιήσει. Δηλαδή να δώσει κάποια ή όλα τα στοιχεία αυτού στο ληξιαρχείο ή σε κάποιον τρίτο οργανισμό που πιθανόν να τα χρειάζεται για δικούς του σκοπούς. Έστω ότι ο πολίτης πηγαίνει σε έναν τρίτο οργανισμό και θέλει να πραγματοποιήσει μία διαδικασία η οποία χρειάζεται κάποια στοιχεία από το πιστοποιητικό γάμου του.

4.5.1 Σύνδεση του πολίτη με τρίτο οργανισμό για τη χρήση του πιστοποιητικού

Έτσι, ο πολίτης πηγαίνει στον τρίτο οργανισμό και συνδέεται στο δίκτυό του. Ο υπάλληλος που τον εξυπηρετεί, χρησιμοποιεί μία desktop εφαρμογή παρόμοια με αυτή των ληξιαρχείων με τη μόνη διαφορά ότι δεν μπορεί να δημιουργήσει πιστοποιητικά (όπως γάμου, γέννησης, θανάτου), αλλά μόνο να ζητήσει δεδομένα αυτών. Όταν ο πολίτης συνδεθεί με την εφαρμογή του κινητού του στην εφαρμογή του τρίτου οργανισμού (ίδια διαδικασία σύνεσης με αυτή του ληξιαρχείου) θα του ζητηθεί να εισάγει το ΑΦΜ του. Αφού ελεγχθεί από τον τρίτο οργανισμό ότι το ΑΦΜ του πολίτη συσχετίζεται με το δημόσιο κλειδί του, θα είναι πλέον σε θέση να στείλει δεδομένα από τις ληξιαρχικές πράξεις του.

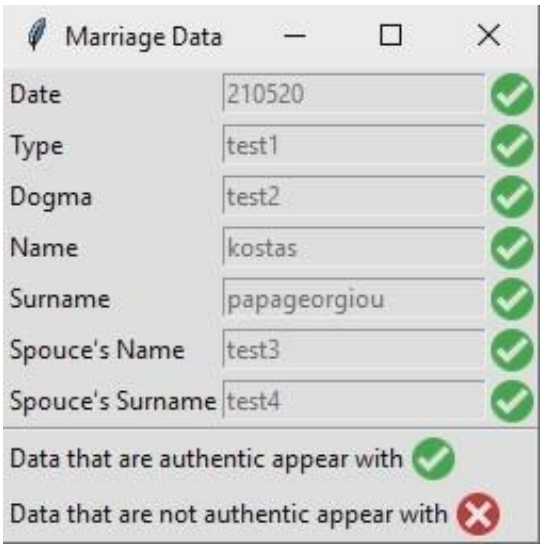
4.5.2 Αίτηση του τρίτου οργανισμού για λήψη πιστοποιητικού

Στην προκειμένη περίπτωση ο τρίτος οργανισμός θέλει να ζητήσει από το πιστοποιητικό γάμου τα στοιχεία : ημερομηνία γάμου, όνομα του πολίτη, όνομα συζύγου του πολίτη. Ο υπάλληλος ανοίγει το κατάλληλο παράθυρο της desktop εφαρμογής του για να αιτηθεί αυτά τα δεδομένα από τον πολίτη. Στο παράθυρο αυτό, από όλα τα διαθέσιμα στοιχεία που μπορεί να ζητήσει επιλέγει αυτά που προαναφέρθηκαν. Ύστερα το αίτημα φτάνει στην android εφαρμογή του πολίτη και ενημερώνεται με το αντίστοιχο μήνυμα στην οθόνη του. Ο πολίτης μπορεί να δεχθεί ή να απορρίψει τη διαδικασία. Αν δεχθεί, η εφαρμογή συνδέεται στο blockchain και κατεβάζει τα δεδομένα στο κινητό του, που είχαν καταχωρισθεί κατά τη δημιουργία της ληξιαρχικής πράξης γάμου στο ληξιαρχείο. Ύστερα, του εμφανίζονται στην οθόνη τα πεδία του πιστοποιητικού. Τα πεδία που ΔΕΝ ζητήθηκαν από τον τρίτο οργανισμό, είναι κρυμμένα και εμφανίζονται με αστερίσκους (*). Τα πεδία που ζήτησε ο

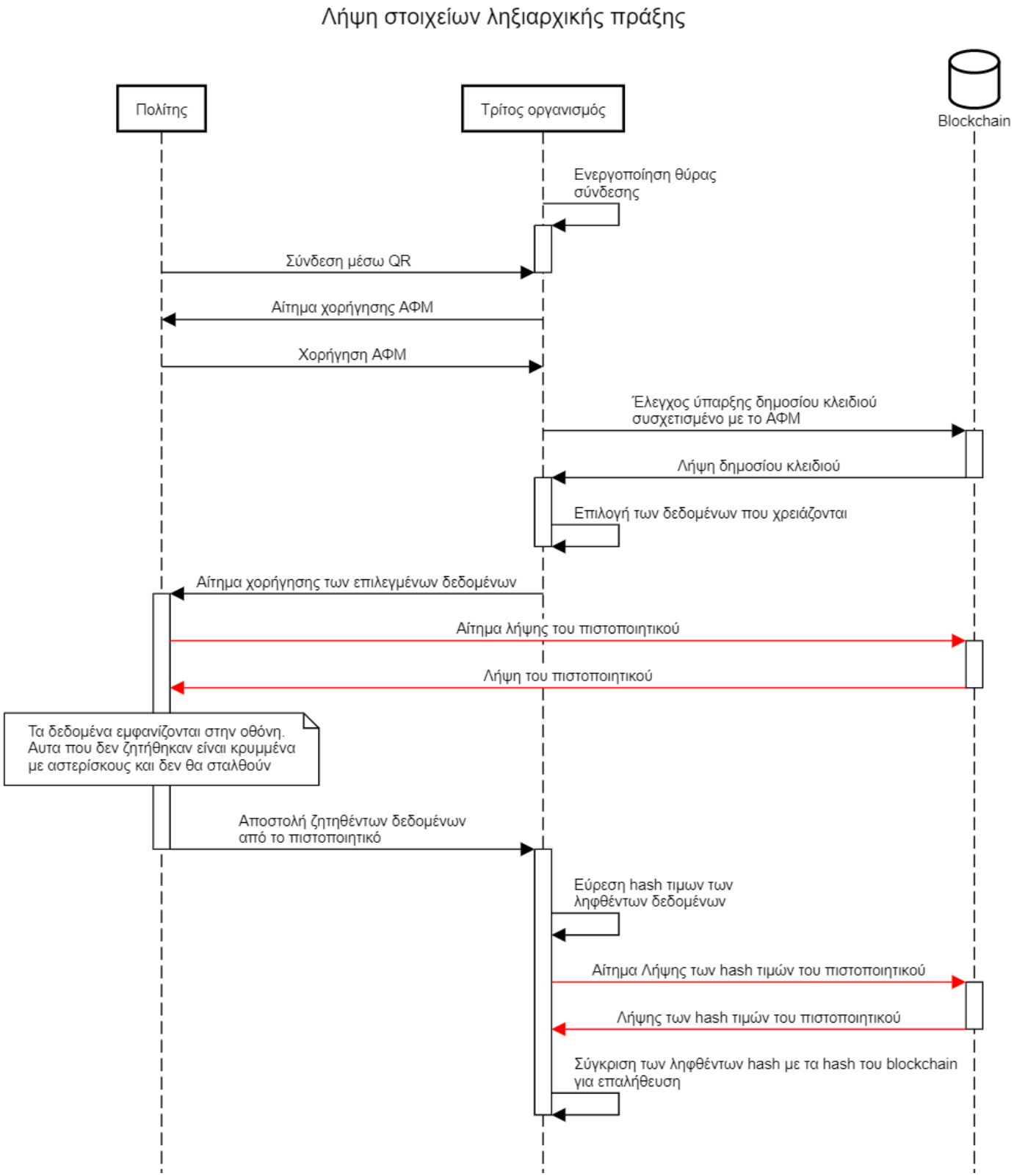
υπάλληλος του τρίτου οργανισμού αποκρυπτογραφήθηκαν με το ιδιωτικό κλειδί του πολίτη και εμφανίστηκαν κανονικά στην οθόνη του.Ο πολίτης σε αυτό το σημείο μπορεί να απορρίψει τη διαδικασία ή να προχωρήσει. Αν προχωρήσει, στέλνονται τα στοιχεία του πιστοποιητικού που ζητήθηκαν από τον υπάλληλο, σε απλή μορφή.

4.5.3 Λήψη του πιστοποιητικού και επαλήθευση των δεδομένων από τον τρίτο οργανισμό

Έπειτα, αυτομάτως, η εφαρμογή του τρίτου οργανισμού μετατρέπει της απλές τιμές που στάλθηκαν σε τιμές hash. Ταυτόχρονα, κατεβάζει τις hash τιμές που υπάρχουν στο blockchain (και αφορούν αυτό το πιστοποιητικό) και τις συγκρίνει μία προς μία μεταξύ τους. Τέλος, εμφανίζεται ένα παράθυρο στον υπάλληλο με τα πεδία που ζήτησε και τις αντίστοιχες τιμές που έδωσε ο πολίτης. Για κάθε μία προς μία σύγκριση των hash τιμών, εμφανίζεται στο παράθυρο του υπαλλήλου, για κάθε πεδίο που ζητήθηκε αντίστοιχο σύμβολο. Αν για ένα πεδίο οι τιμές hash ήταν όμοιες, τότε εμφανίζεται το σύμβολο «✓». Αυτό σημαίνει ότι το συγκεκριμένο στοιχείο που έστειλε ο πολίτης είναι ακριβώς πανομοιότυπο με αυτό που υπάρχει στο blockchain σε αυτό το πιστοποιητικό γάμου. Αν για ένα πεδίο οι τιμές hash δεν ήταν όμοιες, τότε εμφανίζεται το σύμβολο «✗». Αυτό σημαίνει ότι το συγκεκριμένο στοιχείο που έστειλε ο πολίτης δεν είναι πανομοιότυπο με αυτό που υπάρχει στο blockchain σε αυτό το πιστοποιητικό γάμου. Με αυτόν τον τρόπο εξασφαλίζεται η εγκυρότητα των δεδομένων που φτάνουν στον τρίτο οργανισμό ή στο ληξιαρχείο.



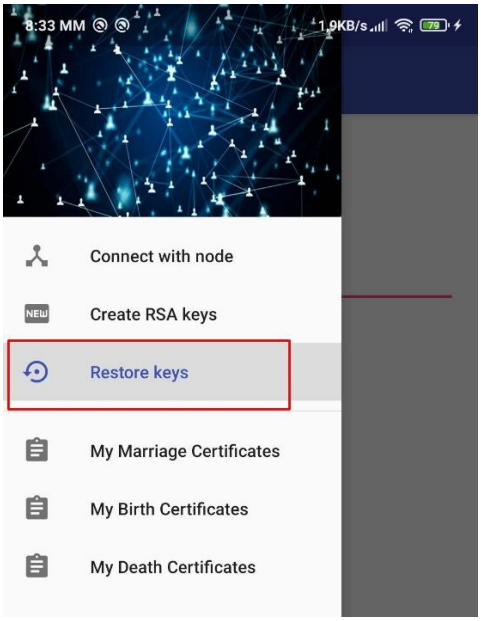
Εικόνα 6: Παράθυρο αποτελεσμάτων μετά την επαλήθευση στοιχείων

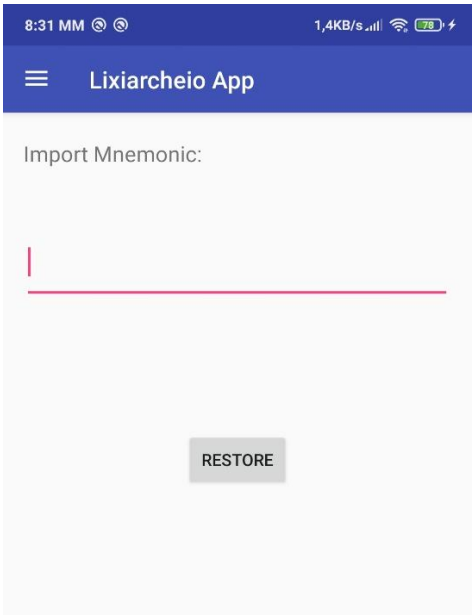


Εικόνα 7: Διάγραμμα διαδικασίας λήψης πιστοποιητικού

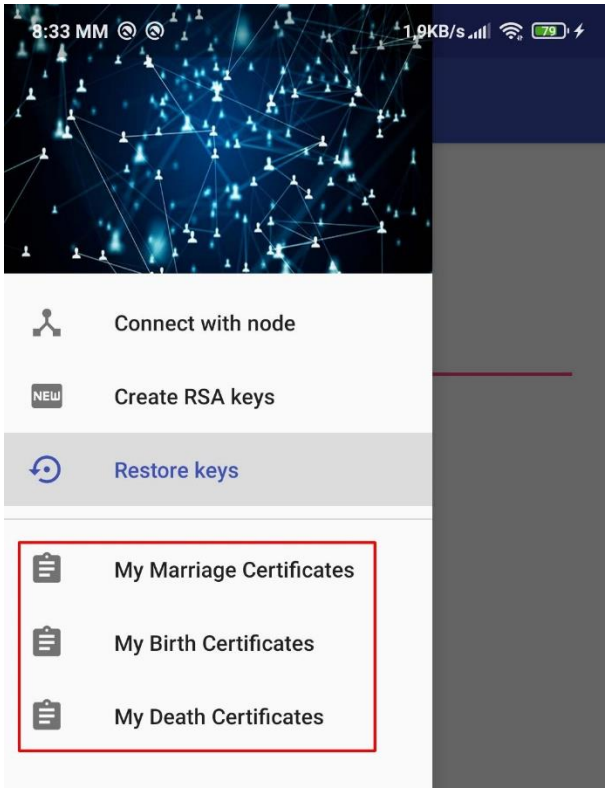
4.6 Επιπλέον πληροφορίες

Αξίζει να σημειωθεί, ότι ο πολίτης αν επιθυμήσει να αλλάξει συσκευή ή αν για κάποιο λόγο, η εφαρμογή διαγραφτεί από την Android συσκευή, μπορεί να ανακτήσει το ζεύγος κλειδιών RSA που είχε δημιουργήσει. Κατά την επανεγκατάσταση της Android εφαρμογής, μπορεί να πλοηγηθεί από το μενού, στο παράθυρο επαναφοράς ζεύγους RSA (Restore Keys). Σε αυτό το σημείο, θα προσθέσει το μνημονικό δώδεκα λέξεων που είχε παραχθεί κατά τη δημιουργία ζεύγους RSA κλειδιών αυτολεξεί! Εφόσον ολοκληρώσει τη διαδικασία πατώντας το κουμπί επαναφοράς (Restore) θα είναι σε θέση να αλληλεπιδρά με το σύστημα του ληξιαρχείου.





Ο πολίτης, μέσω της εφαρμογής στην κινητή συσκευή του έχει την επιλογή να δει τα πιστοποιητικά που έχει δημιουργήσει και αφορούν τον ίδιο. Αυτό μπορεί να γίνει όταν η συσκευή βρίσκεται συνδεδεμένη στο ίδιο ιδιωτικό δίκτυο που είναι εδραιωμένο το blockchain. Αν ο χρήστης είναι συνδεδεμένος σε αυτό το δίκτυο, μπορεί να δει τα πιστοποιητικά του επιλέγοντας από το μενού της εφαρμογής μία από τις επιλογές: My Marriage Certificates, My Birth Certificates ή My Death Certificates για τα πιστοποιητικά γάμου του, τα πιστοποιητικά γεννήσεών του ή τα πιστοποιητικά αποθανόντων του αντιστοίχως.



Εικόνα 8: Επιλογές για εμφάνιση διαφόρων πιστοποιητικών του πολίτη

5 Υλοποίηση Εφαρμογής

Για την καλύτερη κατανόηση της διαδικασίας σε τεχνικό επίπεδο, θα χρειαστεί να αναλυθεί σε υποκεφάλαια. Τα υποκεφάλαια είναι:

- Περιγραφή του smart contract και ανάλυση περιεχομένων του
- Τεχνική περιγραφή δημιουργίας ζεύγους κλειδιών RSA από τον πολίτη
- Τεχνική ανάλυση σύνδεσης ληξιαρχείου/τρίτου οργανισμού με τον πολίτη
- Τεχνική ανάλυση της καταχώρισης προσωπικών δεδομένων του πολίτη στο σύστημα ληξιαρχείου
- Κατανόηση της καταχώρισης ψηφιακής υπογραφής και των προσωπικών δεδομένων σε μορφή hash στο blockchain με τεχνική προσέγγιση
- Τεχνική περιγραφή διαδικαστικού δημιουργίας ληξιαρχικής πράξης
- Τεχνική περιγραφή διαδικαστικού λήψης στοιχείων ληξιαρχικής πράξης

5.1 Περιγραφή του smart contract και ανάλυση περιεχομένων του

Το smart contract που μεταφορτώνεται στο ιδιωτικό blockchain του ληξιαρχείου είναι υλοποιημένο με την υψηλού-επιπέδου αντικειμενοστραφή γλώσσα προγραμματισμού Solidity.

5.1.1 Το smart contract και οι συναρτήσεις του

Το smart contract έχει καθοριστικό ρόλο στο σύστημα του ληξιαρχείου διότι είναι το σημείο αναφοράς των υπολοίπων λογισμικών (τα υπόλοιπα λογισμικά αλληλεπιδρούν με το smart contract) καθώς επίσης σε αυτό περιέχονται οι συναρτήσεις με τις οποίες καταχωρούνται στοιχεία στο blockchain, όπως επίσης και συναρτήσεις που επιτρέπουν την προσπέλαση των στοιχείων αυτών. Ενδεικτικά, κάποιες από τις συναρτήσεις που υπάρχουν και μας ενδιαφέρουν είναι:

- setPubFromAfm: Χρησιμοποιείται για να καταχωρίσει το δημόσιο κλειδί του πολίτη στο ΑΦΜ του. Η συνάρτηση αυτή καλείται όταν ο πολίτης επισκέπτεται για πρώτη φορά το ληξιαρχείο ώστε να κάνει καταχώριση των προσωπικών του δεδομένων στο σύστημα.
- getPubFromAfm: Χρησιμοποιείται για να ελεγχθεί αν για το δοθέν ΑΦΜ του πολίτη, υπάρχει συσχέτιση με το δημόσιο κλειδί του.
- registerPerson: Χρησιμοποιείται για την καταχώριση των προσωπικών δεδομένων του πολίτη. Οι τιμές των προσωπικών του δεδομένων που καταχωρούνται είναι κρυπτογραφημένες με το δημόσιο κλειδί του.
- registerPersonHash: Χρησιμοποιείται για την καταχώριση των προσωπικών του δεδομένων του πολίτη σε μορφή hash. Αξίζει να σημειωθεί ότι τα προσωπικά δεδομένα που καταχωρούνται σε μορφή hash δεν είναι κρυπτογραφημένα.
- registerMarriage: Χρησιμοποιείται για την καταχώριση των στοιχείων ενός γάμου του πολίτη. Τα στοιχεία που καταχωρούνται είναι επίσης κρυπτογραφημένα με το δημόσιο κλειδί του. Αυτή η συνάρτηση δηλαδή, δημιουργεί ένα πιστοποιητικό γάμου
- registerMarriageHash: Χρησιμοποιείται για την καταχώριση των στοιχείων ενός γάμου του πολίτη σε μορφή hash. Τα στοιχεία που καταχωρούνται σε μορφή hash δεν είναι κρυπτογραφημένα.
- registerBirth: Χρησιμοποιείται για την καταχώριση των στοιχείων μίας γεννήσεως. Τα στοιχεία που καταχωρούνται είναι επίσης

κρυπτογραφημένα με το δημόσιο κλειδί του πολίτη. Αυτή η συνάρτηση δηλαδή, δημιουργεί ένα πιστοποιητικό γεννήσεως.

- registerBirthHash: Χρησιμοποιείται για την καταχώριση των στοιχείων μίας γεννήσεως σε μορφή hash. Τα στοιχεία που καταχωρούνται σε μορφή hash δεν είναι κρυπτογραφημένα με το δημόσιο κλειδί του πολίτη.
- registerDeath: Χρησιμοποιείται για την καταχώριση των στοιχείων ενός αποθανόντα πολίτη, πρώτου βαθμού συγγένειας με τον δηλών. Τα στοιχεία που καταχωρούνται είναι επίσης κρυπτογραφημένα με το δημόσιο κλειδί του δηλών. Αυτή η συνάρτηση δηλαδή, δημιουργεί ένα πιστοποιητικό θανάτου.
- registerDeathHash: Χρησιμοποιείται για την καταχώριση των στοιχείων ενός αποθανόντα σε μορφή hash SHA-256. Τα στοιχεία που καταχωρούνται σε μορφή hash δεν είναι κρυπτογραφημένα με το δημόσιο κλειδί του δηλών.
- registerAdmin: Χρησιμοποιείται για να καταχωρήσει τη διεύθυνση ethereum ενός ληξιαρχείου σε μια λίστα. Οι καταχωρημένες διευθύνσεις σε αυτή τη λίστα, δηλαδή το σύνολο των ληξιαρχείων, μπορούν να καλέσουν τις συναρτήσεις που αφορούν την οποιαδήποτε εγγραφή δεδομένων στο blockchain.
- getMarriageCert1: Χρησιμοποιείται για να επιστρέψει κάποια από τα κρυπτογραφημένα στοιχεία ενός πιστοποιητικού γάμου για κάποιον πολίτη. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Ημερομηνία, Τύπος γάμου, Δόγμα, Όνομα δηλών, Επώνυμο δηλών, α.φ.μ. δηλών και α.μ.κ.α. δηλών. Τα δεδομένα που επιστρέφει η συνάρτηση είναι κρυπτογραφημένα με το δημόσιο κλειδί του πολίτη.
- getMarriageCert2: Χρησιμοποιείται για να επιστρέψει κάποια από τα κρυπτογραφημένα στοιχεία ενός πιστοποιητικού γάμου για κάποιον πολίτη. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Όνομα συζύγου, Επώνυμο συζύγου, α.φ.μ. συζύγου, α.μ.κ.α. συζύγου και η ψηφιακή υπογραφή του δηλών. Τα δεδομένα που επιστρέφει η συνάρτηση είναι κρυπτογραφημένα με το δημόσιο κλειδί του πολίτη.
- getMarriageCertHash1: Χρησιμοποιείται για να επιστρέψει κάποια από τα στοιχεία σε μορφή hash ενός πιστοποιητικού γάμου για κάποιον πολίτη. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Ημερομηνία, Τύπος γάμου,

Δόγμα, Όνομα δηλών, Επώνυμο δηλών, α.φ.μ. δηλών και α.μ.κ.α. δηλών. Τα δεδομένα που επιστρέφει η συνάρτηση είναι σε μορφή hash SHA-256.

- getMarriageCertHash2: Χρησιμοποιείται για να επιστρέψει κάποια από τα στοιχεία σε μορφή hash ενός πιστοποιητικού γάμου για κάποιον πολίτη. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Όνομα συζύγου, Επώνυμο συζύγου, α.φ.μ. συζύγου και α.μ.κ.α. συζύγου. Τα δεδομένα που επιστρέφει η συνάρτηση είναι σε μορφή hash SHA-256.
- getBirthCert1: Χρησιμοποιείται για να επιστρέψει κάποια από τα κρυπτογραφημένα στοιχεία ενός πιστοποιητικού γεννήσεως που δήλωσε κάποιος πολίτης. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Όνομα παιδιού, Επώνυμο παιδιού, α.μ.κ.α. παιδιού, Όνομα δηλών, Επώνυμο δηλών, α.φ.μ. δηλών και α.μ.κ.α. δηλών. Τα δεδομένα που επιστρέφει η συνάρτηση είναι κρυπτογραφημένα με το δημόσιο κλειδί του υπογράφοντα πολίτη.
- getBirthCert2: Χρησιμοποιείται για να επιστρέψει κάποια από τα κρυπτογραφημένα στοιχεία ενός πιστοποιητικού γεννήσεως που δήλωσε κάποιος πολίτης. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Όνομα δεύτερου γονέα, Επώνυμο δεύτερου γονέα, α.φ.μ., δεύτερου γονέα, α.μ.κ.α. δεύτερου γονέα και η ψηφιακή υπογραφή του δηλών. Τα δεδομένα που επιστρέφει η συνάρτηση είναι κρυπτογραφημένα με το δημόσιο κλειδί του υπογράφοντα πολίτη.
- getBirthCertHash1: Χρησιμοποιείται για να επιστρέψει κάποια από τα στοιχεία ενός πιστοποιητικού γεννήσεως σε μορφή hash που δήλωσε κάποιος πολίτης. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Όνομα παιδιού, Επώνυμο παιδιού, α.μ.κ.α. παιδιού, Όνομα δηλών, Επώνυμο δηλών, α.φ.μ. δηλών και α.μ.κ.α. δηλών. Τα δεδομένα που επιστρέφει η συνάρτηση είναι σε μορφή hash SHA-256.
- getBirthCertHash2: Χρησιμοποιείται για να επιστρέψει κάποια από τα στοιχεία ενός πιστοποιητικού γεννήσεως σε μορφή hash που δήλωσε κάποιος πολίτης. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Όνομα δεύτερου γονέα, Επώνυμο δεύτερου γονέα α.φ.μ. δεύτερου γονέα και α.μ.κ.α. δεύτερου γονέα. Τα δεδομένα που επιστρέφει η συνάρτηση είναι σε μορφή hash SHA-256.

- getDeathCert: Χρησιμοποιείται για να επιστρέψει κάποια από τα κρυπτογραφημένα στοιχεία ενός πιστοποιητικού θανάτου που δήλωσε κάποιος πολίτης. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Όνομα αποθανόντα, Επώνυμο αποθανόντα, α.φ.μ. αποθανόντα, α.μ.κ.α. αποθανόντα και την ψηφιακή υπογραφή του δηλών. Τα δεδομένα που επιστρέφει η συνάρτηση είναι κρυπτογραφημένα με το δημόσιο κλειδί του υπογράφοντα πολίτη.
- getDeathCertHash: Χρησιμοποιείται για να επιστρέψει κάποια από τα στοιχεία ενός πιστοποιητικού θανάτου σε μορφή hash που δήλωσε κάποιος πολίτης. Πιο συγκεκριμένα, επιστρέφονται τα πεδία: Όνομα αποθανόντα, Επώνυμο αποθανόντα, α.φ.μ. αποθανόντα και α.μ.κ.α. αποθανόντα. Τα δεδομένα που επιστρέφει η συνάρτηση είναι σε μορφή hash SHA-256.
- getMarriageCounters: Χρησιμοποιείται για να επιστρέψει τον αύξον αριθμό των πιστοποιητικών γάμου που έχει δημιουργήσει κάποιος πολίτης
- getBirthCounters: Χρησιμοποιείται για να επιστρέψει τον αύξον αριθμό των πιστοποιητικών γεννήσεως που έχει δημιουργήσει κάποιος πολίτης
- getDeathCounters: Χρησιμοποιείται για να επιστρέψει τον αύξον αριθμό των πιστοποιητικών θανάτου που έχει δημιουργήσει κάποιος πολίτης

5.2 Τεχνική περιγραφή δημιουργίας ζεύγους κλειδιών RSA από τον πολίτη

5.2.1 Χρήση του Android keystore για ασφαλή αποθήκευση των RSA κλειδιών

Ο πολίτης έχοντας εγκαταστήσει στην κινητή του συσκευή την εφαρμογή για android, κατά την εκτέλεσή της, γίνεται έλεγχος αν υπάρχει καταχωρημένο ζεύγος κλειδιών RSA στο σύστημα Android keystore. Το σύστημα Android keystore επιτρέπει την αποθήκευση κρυπτογραφικών κλειδιών με κάποιο ψευδώνυμο ως αναγνωριστικό(στη παρούσα διαδικασία χρειάζεται να αποθηκευτεί ζεύγος κλειδιών RSA με το ψευδώνυμο “RSAkeys”), τα οποία μπορούν να χρησιμοποιηθούν για κρυπτογραφικούς σκοπούς χωρίς όμως να υπάρχει κίνδυνος να εξαχθούν και κατόπιν να φανερωθούν. Ως πρώτη φορά εκτέλεσης της εφαρμογής, το android keystore δεν

θα περιέχει ζεύγος κλειδιών RSA με το ψευδώνυμο “RSAkeys”, οπότε ο χρήστης θα οδηγηθεί αυτομάτως στο παράθυρο δημιουργίας κλειδιών RSA.

5.2.2 Δημιουργία ζευγαριού κλειδιών RSA

Το πρώτο βήμα που πρέπει να κάνει ο χρήστης είναι να πατήσει το κουμπί που παράγει ένα μνημονικό δώδεκα λέξεων. Η τυχαία δημιουργία μνημονικού βασίζεται στο πρότυπο BIP39 (Bitcoin Improvement Proposal). Η εφαρμογή παράγει τυχαία δώδεκα λέξεις βάσει ενός λεξιλογίου που υπάρχει στις πηγές της εφαρμογής, και τις τοποθετεί με τυχαία σειρά. Αφού ο χρήστης λάβει το μνημονικό, ύστερα πατάει το κουμπί για τη δημιουργία ζεύγους RSA κλειδιών. Ο τρόπος με τον οποίο δημιουργείται το ζεύγος RSA κλειδιών είναι ντετερμινιστικός. Αυτό οφείλεται στο γεγονός ότι για τη δημιουργία των κλειδιών RSA χρησιμοποιείται ως παράμετρος το μνημονικό. Με αυτό τον τρόπο εξασφαλίζεται η δυνατότητα επαναφοράς των κλειδιών RSA, εισάγοντας αυτούσιο το μνημονικό που είχε παραχθεί κατά τη διαδικασία της δημιουργίας των κλειδιών. Το ζεύγος κλειδιών RSA κατά τη δημιουργία του έχει χαρακτηριστικά:

- Μέγεθος: 2048 bits
- Block Mode: ECB (Electronic Codebook)
- Digests Algorithms: SHA-256, SHA-1
- Encryption Paddings: RSA-OAEP
- Signature Paddings: RSA-PKCS1

Εφόσον τα κλειδιά RSA δημιουργηθούν, θα αποθηκευτούν στο Android keystore με το ψευδώνυμο “RSAkeys” και από αυτό το σημείο η εφαρμογή θα χειρίζεται οποιαδήποτε διαδικασία χρίζει κλειδιά RSA, αυτά που αποθηκεύτηκαν στο Android keystore.

5.3 Τεχνική ανάλυση σύνδεσης Ληξιαρχείου/τρίτου οργανισμού με τον πολίτη

Για τη αλληλεπίδραση του πολίτη με το ληξιαρχείο ή με κάποιον τρίτο οργανισμό (ο τρόπος σύνδεσης του πολίτη με το ληξιαρχείο είναι ίδιος με αυτόν του τρίτου οργανισμού), θα πρέπει να βρίσκονται στο ίδιο δίκτυο. Από τη πλευρά του ληξιαρχείου, ο εκάστοτε υπάλληλος θα ανοίξει την desktop εφαρμογή και θα εισάγει μια θύρα επικοινωνίας. Όταν εισάγει τη θύρα, θα πρέπει να πατήσει το κουμπί

παραγωγής κωδικού QR. Ύστερα, θα πρέπει να πατήσει το κουμπί “Establish” ώστε να ενεργοποιήσει την θύρα υποδοχής. Από τη στιγμή που ο πολίτης συνδεθεί στο ίδιο δίκτυο, μπορεί να ανοίξει την android εφαρμογή του και να πατήσει στο μενού την επιλογή “Connect with node”. Τέλος, θα πατήσει το κουμπί “SCAN” και θα ενεργοποιηθεί η πίσω κάμερα του κινητού ώστε να μπορέσει να σαρώσει τον κωδικό QR. Μετά την επιτυχή σάρωση του κωδικού QR, η κινητή συσκευή αυτομάτως θα συνδεθεί με την desktop εφαρμογή. Ο τρόπος που γίνεται η σύνδεση αυτή είναι μέσω TCP socket με address family: Internet Protocol v4 addresses (AF_INET).

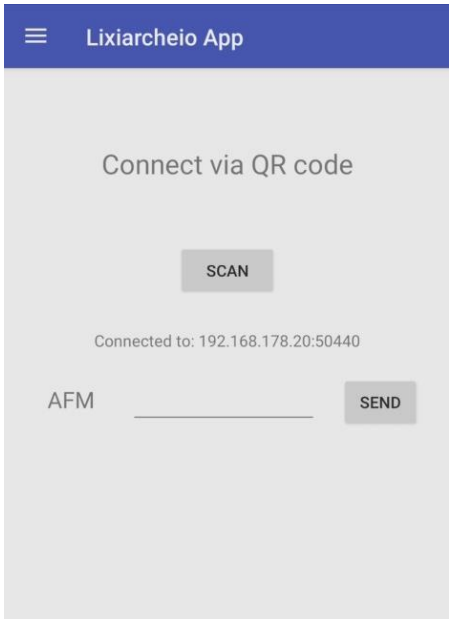
Εικόνα 9: Βήματα για την ίδρυση σύνδεσης από το ληξιαρχείο για τον πολίτη

5.4 Τεχνική ανάλυση της καταχώρισης προσωπικών δεδομένων του πολίτη στο σύστημα ληξιαρχείου

Κατά την πρώτη επίσκεψη του πολίτη στο ληξιαρχείο, θα πρέπει να συνδεθεί μέσω της android εφαρμογής του στην εφαρμογή του ληξιαρχείου κατά τον ίδιο τρόπο που εξηγήθηκε παραπάνω.

5.4.1 Διαδικασία αλληλεπίδρασης του πολίτη με το ληξιαρχείο κατά τη πρώτη φορά

Όταν συνδεθεί, η εφαρμογή του ληξιαρχείου θα στείλει στην εφαρμογή android αίτημα με κωδικό “AFM” αυτό θα σηματοδοτήσει ότι ο πολίτης θα πρέπει να αποστείλει το ΑΦΜ του στο Ληξιαρχείο. Έτσι, θα του εμφανιστεί στην οθόνη της κινητής του συσκευής ένα πεδίο ώστε να μπορέσει να συμπληρώσει το ΑΦΜ του. Μετά την συμπλήρωση του, θα πρέπει να πατήσει το κουμπί “SEND” για την αποστολή του.



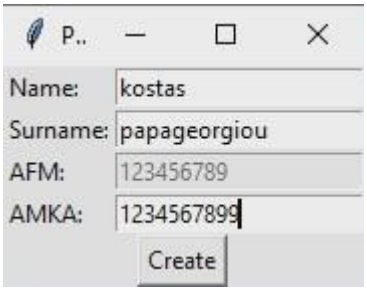
Εικόνα 10: Αίτημα χορήγησης Α.Φ.Μ. του πολίτη

Η desktop εφαρμογή θα λάβει την απάντηση, δηλαδή, την τιμή του ΑΦΜ έχοντας στο τέλος το μήνυμα σηματοδότησης "_afm_" με αυτό τον τρόπο η desktop εφαρμογή καταλαβαίνει ότι το μήνυμα που λήφθηκε ήταν το ΑΦΜ του πολίτη. Ύστερα, η εφαρμογή, καλεί τη συνάρτηση "getPubFromAfm" από το smart contract με όρισμα την τιμή του ΑΦΜ που δόθηκε. Η συνάρτηση δεν θα επιστρέψει κάτι, διότι, ο πολίτης επισκέπτεται πρώτη φορά το ληξιαρχείο, οπότε δεν έχει καταχωρηθεί δημόσιο κλειδί σε αυτό το ΑΦΜ. Έτσι, εφόσον η desktop εφαρμογή δεν κατάφερε να κάνει λήψη του δημοσίου κλειδιού για αυτό το ΑΦΜ από το blockchain, θα εμφανίσει σχετικό μήνυμα στον υπάλληλο ότι δεν υπάρχει πολίτης που να έχει στοιχεία καταχωρισμένα στο σύστημα με αυτό το ΑΦΜ. Για την καταχώριση του πολίτη στο σύστημα θα σταλθεί από την εφαρμογή του ληξιαρχείου αίτημα με κωδικό "PUB_KEY". Η android εφαρμογή λαμβάνοντας αυτό τον κωδικό, θα λάβει από το android keystore το δημόσιο κλειδί του πολίτη, θα το μετατρέψει σε μορφή base64 και θα το αποστείλει στην εφαρμογή του ληξιαρχείου έχοντας στο τέλος τον κωδικό "_pubkey_". Η εφαρμογή ληξιαρχείου, λαμβάνοντας το μήνυμα με κωδικό "_pubkey_", αποθηκεύει προσωρινά το δημόσιο κλειδί που στάλθηκε.

5.4.2 Εγγραφή του πολίτη στο σύστημα του ληξιαρχείου

Ύστερα, ο υπάλληλος οδηγείται στο παράθυρο συμπλήρωσης προσωπικών στοιχείων. Ο πολίτης δίνει τα προσωπικά του στοιχεία (όνομα, επώνυμο, ΑΦΜ,

ΑΜΚΑ) στον υπάλληλο και αυτός τα συμπληρώνει. Αφού τα συμπληρώσει, πατάει το κουμπί “Create” και η desktop εφαρμογή καλεί συνάρτηση η οποία κρυπτογραφεί ένα προς ένα τα δεδομένα που καταχωρίστηκαν με το δημόσιο κλειδί του πολίτη.

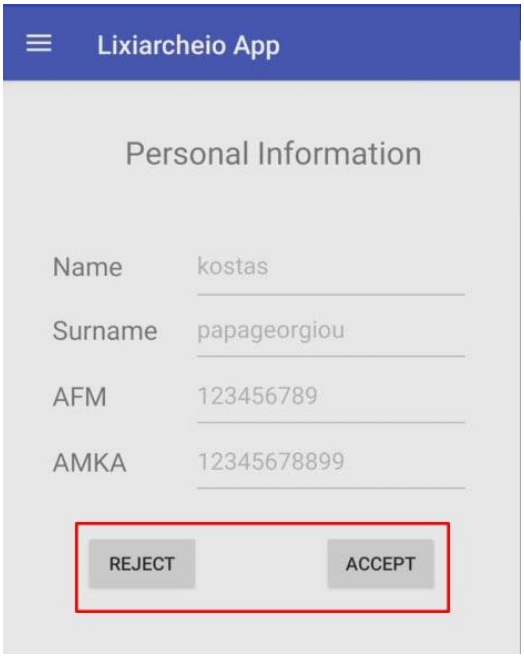


Εικόνα 11: Συμπλήρωση στοιχείων πολίτη από το ληξιαρχείο

Μετά την κρυπτογράφησή τους, μετατρέπονται σε μορφή δεκαεξαδικού αλφαριθμητικού το καθένα και ύστερα γίνεται η συνένωση αυτών διαχωρίζοντας το κάθε αλφαριθμητικό με τον χαρακτήρα « | ». Το τελικό αποτέλεσμα στέλνεται στην android εφαρμογή έχοντας στο τέλος τον κωδικό “_REG_”. Η android εφαρμογή λαμβάνοντας το μήνυμα με κωδικό “_REG_”, θα το αποθηκεύσει προσωρινά και θα αρχίσει την αντίστροφη διαδικασία, δηλαδή, θα χωρίσει το αλφαριθμητικό σε διαδοχικά κομμάτια με τεκμήριο το σύμβολο « | ». Θα μετατρέψει το κάθε κομμάτι που βρίσκεται σε δεκαεξαδική μορφή σε bytes και θα το αποκρυπτογραφήσει με το ιδιωτικό κλειδί που βρίσκεται στο σύστημα android keystore.

5.4.3 Απόφαση του πολίτη για την εξέλιξη της διαδικασίας

Μετά την αποκρυπτογράφηση, τα δεδομένα θα φανούν στην οθόνη του πολίτη και θα πρέπει να αποφασίσει αν αυτά είναι σωστά.



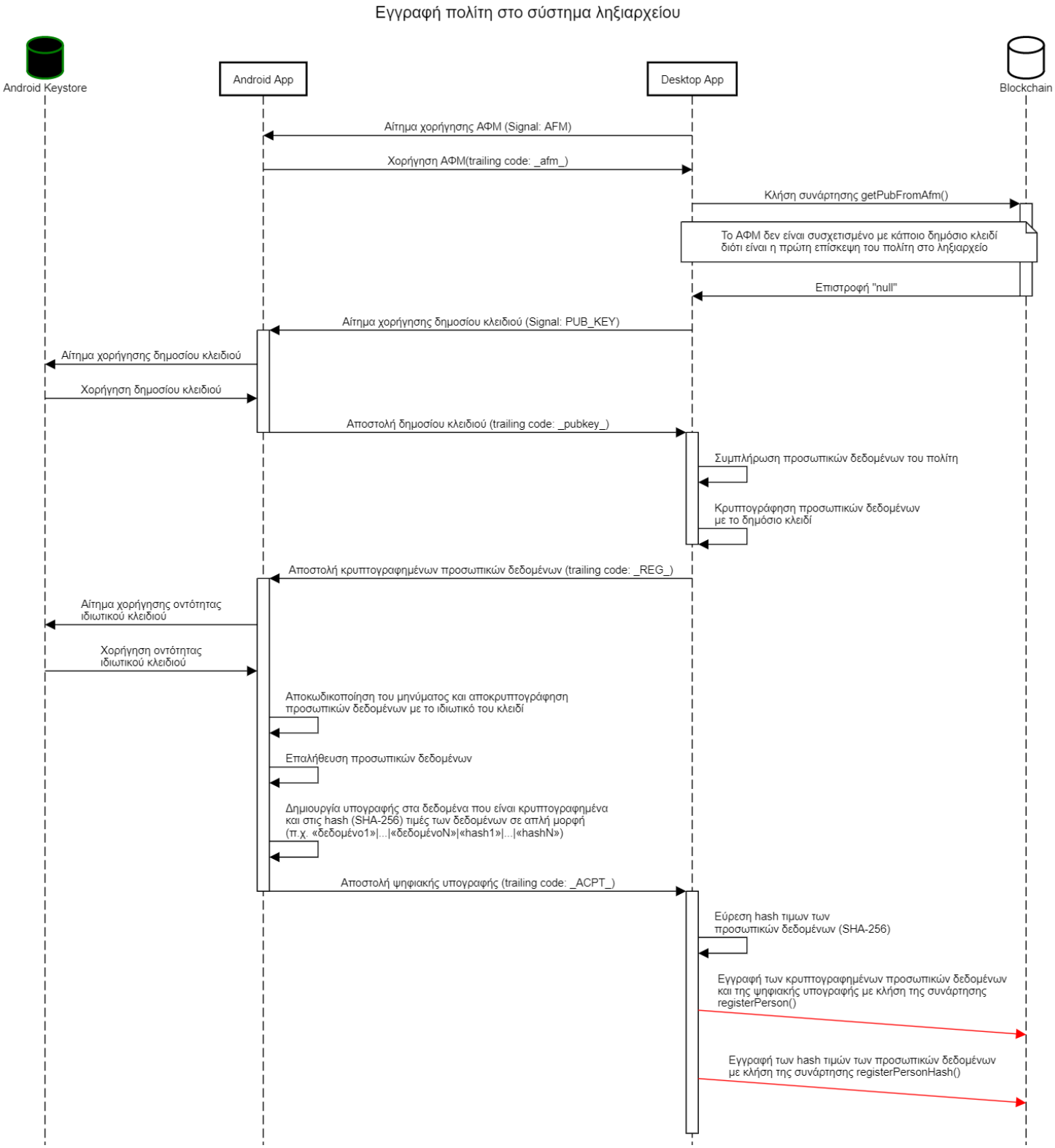
Εικόνα 12: Επαλήθευση δεδομένων από τον πολίτη

Αν δεν είναι σωστά, τότε, μπορεί να πατήσει το κουμπί "REJECT" και θα σταλθεί ο κωδικός "RJCT" στην desktop εφαρμογή ώστε να τερματίσει η διαδικασία. Αν είναι σωστά, τότε, μπορεί να πατήσει το κουμπί "ACCEPT" και να προχωρήσει τη διαδικασία.

5.4.4 Διαδικασία εγγραφής δεδομένων του πολίτη στο blockchain

Μετά το πάτημα του κουμπιού "ACCEPT", η android εφαρμογή καλεί μία συνάρτηση η οποία μετατρέπει τα δεδομένα που εμφανίστηκαν στην οθόνη του πολίτη, σε μορφή hash τύπου SHA-256. Ύστερα, ενοποιεί το μήνυμα που λήφθηκε προηγουμένως και αποθήκευσε προσωρινά (δηλαδή τα κρυπτογραφημένα δεδομένα σε δεκαεξαδική μορφή χωρισμένα με το σύμβολο « | ») με τα δεδομένα σε hash μορφή (τα οποία χωρίζονται πάλι με το σύμβολο « | ») και δημιουργεί μια ψηφιακή υπογραφή χρησιμοποιώντας το ιδιωτικό κλειδί του πολίτη που βρίσκεται στο σύστημα android keystore. Τέλος, η android εφαρμογή μετατρέπει την ψηφιακή υπογραφή σε δεκαεξαδική μορφή και τη στέλνει στη desktop εφαρμογή, έχοντας στο τέλος του μηνύματος τον αναγνωριστικό κωδικό "_ACPT_". Η desktop εφαρμογή, αφού παραλάβει το μήνυμα με κωδικό "_ACPT_", θα αποθηκεύσει προσωρινά την υπογραφή και θα καλέσει τις συναρτήσεις "registerPerson" και " registerPersonHash" από το smart contract. Η registerPerson θα καταχωρίσει και θα συσχετίσει στο δημόσιο κλειδί του πολίτη τα κρυπτογραφημένα στοιχεία του καθώς και τη ψηφιακή υπογραφή στο blockchain σε bytes (Σημείωση: το ΑΦΜ του πολίτη είναι το μόνο που

δεν αποθηκεύεται κρυπτογραφημένο, διότι, είναι το σημείο αναφοράς και βάση αυτού γίνεται η λήψη του δημοσίου κλειδιού από το blockchain). Επιπλέον, η “registerPersonHash” θα αποθηκεύσει σε bytes τα προσωπικά δεδομένα του πολίτη που βρίσκονται σε μορφή hash SHA-256. Αν τα δεδομένα καταχωρίστηκαν επιτυχώς, τότε θα εμφανιστεί μήνυμα στην οθόνη του υπαλλήλου ότι η συναλλαγή στο blockchain ήταν επιτυχής. Από αυτό το σημείο, ο πολίτης μπορεί να δημιουργήσει ληξιαρχικές πράξεις και γενικότερα να αλληλεπιδρά με το ληξιαρχείο ή με τρίτους οργανισμούς.



Εικόνα 13: Αναλυτικό διάγραμμα εγγραφής του πολίτη στο σύστημα

5.5 Κατανόηση της καταχώρισης ψηφιακής υπογραφής και των προσωπικών δεδομένων σε μορφή hash στο blockchain με τεχνική προσέγγιση

Κατά τη καταχώριση των προσωπικών δεδομένων ή τη δημιουργία μιας ληξιαρχικής πράξης (Γάμου, Γέννησης, Θανάτου) του πολίτη στο blockchain, καταχωρείται και η ψηφιακή του υπογραφή. Όταν το ληξιαρχείο αποστείλει τα δεδομένα προς επαλήθευση στην android εφαρμογή του πολίτη, ο πολίτης θα πρέπει να ελέγξει αν τα δεδομένα που καταχώρισε ο υπάλληλος του ληξιαρχείου ήταν σωστά. Εφόσον τα δεδομένα επαληθευτούν και είναι σωστά, η εφαρμογή του πολίτη θα υπογράψει ψηφιακά με το ιδιωτικό του κλειδί από το σύστημα android keystore τα δεδομένα προς καταχώριση στο blockchain. Δηλαδή, θα γίνει μία ενοποίηση μεταξύ των προσωπικών δεδομένων σε κρυπτογραφημένη μορφή και των δεδομένων σε μορφή hash SHA-256. Μετά την επιτυχή δημιουργία της ψηφιακής υπογραφής, η εφαρμογή android θα αποστείλει την υπογραφή στην desktop εφαρμογή, η οποία θα καταχωρήσει τα δεδομένα μαζί με την ψηφιακή υπογραφή στο blockchain. Με την καταχώριση της ψηφιακής υπογραφής στο blockchain, θα μπορεί να γίνει επαλήθευση των δεδομένων που καταχώρισε ο υπάλληλος. Πιο συγκεκριμένα, αν ένα ληξιαρχείο ή ένας τρίτος οργανισμός χρειαστεί να ελέγξει αν η διαδικασία της δημιουργίας ενός πιστοποιητικού στο blockchain έγινε ορθά, μπορεί να το πραγματοποιήσει. Αν για παράδειγμα, πρέπει να γίνει επαλήθευση ενός πιστοποιητικού γάμου για κάποιον πολίτη, θα πρέπει να κληθεί η συνάρτηση getMarriageCert1 και getMarriageCert2 καθώς επίσης η getMarriageCertHash1 και getMarriageCertHash2 από το smart contract, ώστε να ληφθούν τα δεδομένα σε μορφή bytes. Ύστερα γίνεται προσάρτηση του ενός δεδομένου πίσω από το άλλο σύμφωνα με τη σειρά που λήφθηκαν από το blockchain. Τα προσωπικά στοιχεία του πολίτη δεν προσαρτώνται! Δηλαδή, στην προκειμένη περίπτωση τα δεδομένα σε bytes που θα ενοποιηθούν είναι: Ημερομηνία γάμου, Τύπος γάμου, Δόγμα, Όνομα συζύγου, Επώνυμο συζύγου, α.φ.μ. συζύγου και α.μ.κ.α. συζύγου (όπως φαίνεται, τα προσωπικά δεδομένα του πολίτη δεν εισήχθησαν). Ύστερα γίνεται προσάρτηση και τως hash τιμών που λήφθηκαν από τις αντίστοιχες συναρτήσεις που προαναφέρθηκαν. Δηλαδή, Ημερομηνία γάμου, Τύπος

γάμου, Δόγμα, Όνομα συζύγου, Επώνυμο συζύγου, α.φ.μ. συζύγου και α.μ.κ.α. συζύγου (αυτές οι τιμές είναι σε μορφή hash και όχι κρυπτογραφημένες!). Ύστερα, το αποτέλεσμα της ενοποίησης που είναι σε bytes εισάγεται σε ειδική συνάρτηση μαζί με το δημόσιο κλειδί του πολίτη και την ψηφιακή υπογραφή που έχει αποθηκευτεί στο blockchain. Τέλος, γίνεται έλεγχος αν η ψηφιακή υπογραφή που δημιουργήθηκε μόλις, είναι πανομοιότυπη με αυτή που έχει αποθηκευτεί στο blockchain.

Οι καταχωρίσεις των hash τιμών των δεδομένων στο blockchain, χρησιμοποιούνται για την επαλήθευση των δοθέντων στοιχείων από τον πολίτη όταν του ζητηθούν στοιχεία για ένα πιστοποιητικό που έχει δημιουργήσει. Όταν ένα ληξιαρχείο ή ένας τρίτος οργανισμός θελήσει να ζητήσει από έναν πολίτη κάποια στοιχεία από ένα πιστοποιητικό του, η android εφαρμογή θα αντλήσει αυτό το πιστοποιητικό και θα στείλει τα ζητηθέντα δεδομένα στην desktop εφαρμογή (ο τρόπος που γίνεται αυτό θα αναλυθεί παρακάτω). Το ληξιαρχείο ή ο τρίτος οργανισμός προκειμένου να επαληθεύσει ότι τα δεδομένα που έστειλε ο πολίτης για το συγκεκριμένο πιστοποιητικό είναι σωστά, θα πρέπει να τα μετατρέψει ένα προς ένα σε μορφή hash SHA-256. Ύστερα, θα πρέπει να καλέσει τις κατάλληλες συναρτήσεις για τη λήψη των hash τιμών για τη συγκεκριμένη κατηγορία πιστοποιητικού από το smart contract (π.χ. για πιστοποιητικό γάμου: getMarriageCertHash1, getMarriageCertHash2). Μετά, θα τις εκφράσει σε μορφή δεκαεξαδικού (από bytes) και θα συγκρίνει αν τα hash που έστειλε ο πολίτης με τα hash που λήφθηκαν από το blockchain είναι ένα προς ένα ίδια μεταξύ τους. Αν είναι ίδια, τότε τα δεδομένα που έστειλε ο πολίτης για το συγκεκριμένο πιστοποιητικό είναι επαληθευμένα και είναι αυθεντικά. Αν κάποια από αυτά δεν είναι ίδια, τότε αυτό σημαίνει ότι ο πολίτης έστειλε λάθος δεδομένα στο ληξιαρχείο ή στο τρίτο οργανισμό και σταματάει η διαδικασία.

5.6 Τεχνική περιγραφή διαδικαστικού δημιουργίας ληξιαρχικής πράξης

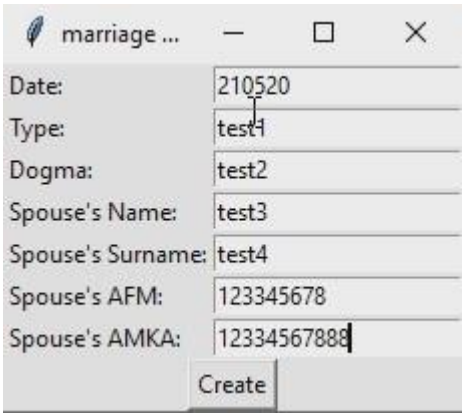
Όταν ο πολίτης έχει συμπληρώσει τα στοιχεία του και είναι πλέον καταχωρημένος στο σύστημα, μπορεί να δημιουργήσει κάποια ληξιαρχική πράξη (Γάμου, Γεννήσεως, Θανάτου). Έστω ότι κάποιος πολίτης θέλει να δημιουργήσει μια ληξιαρχική πράξη γάμου. Προκειμένου να γίνει αυτό, θα πρέπει να πάει σε κάποιο ληξιαρχείο. Από εκεί θα συνδεθεί στο δίκτυο κατά τον ίδιο τρόπο που εξηγήθηκε σε παραπάνω υποκεφάλαιο, ώστε να μπορέσει να αλληλεπιδράσει με το ληξιαρχείο.

5.6.1 Συμπλήρωση στοιχείων πιστοποιητικού από το ληξιαρχείο

Όταν συνδεθεί ο υπάλληλος θα πρέπει να διαλέξει από το μενού της desktop εφαρμογής την επιλογή Create Certificate → Marriage Certificate.

Εικόνα 14: Βήματα για τη συμπλήρωση στοιχείων πιστοποιητικού από ληξιαρχείο

Εφόσον γίνει αυτό, θα πρέπει να δηλώσει τα στοιχεία που θα του δώσει ο πολίτης (Ημερομηνία γάμου, Τύπος γάμου, Δόγμα, Όνομα συζύγου, Επώνυμο συζύγου, α.φ.μ. συζύγου, α.μ.κ.α. συζύγου).



Εικόνα 15: Τα δεδομένα που χρειάζεται να συμπληρωθούν

5.6.2 Διαδικασία μορφοποίησης των δεδομένων

Αφού συμπληρωθούν επιτυχώς και ο υπάλληλος πατήσει το κουμπί Create, τα δεδομένα θα κρυπτογραφηθούν ένα προς ένα με το δημόσιο κλειδί του πολίτη και θα μετατραπούν σε μορφή δεκαεξαδικού αλφαριθμητικού. Μετά, θα ενοποιηθούν σε ένα αλφαριθμητικό με διαχωριστή το σύμβολο « | ». Στο τελικό αλφαριθμητικό που θα παραχθεί, θα προστεθεί και η λέξη κλειδί "_ID1_" και θα σταλθεί μέσω του καναλιού σύνδεσης στην android εφαρμογή. Από εκεί, θα ελεγχθεί ποια λέξη κλειδί υπάρχει στο τέλος του μηνύματος (δηλαδή "_ID1_"). Αφού δει ότι η λέξη κλειδί είναι το "_ID1_", θα χωρίσει το υπόλοιπο μήνυμα σε κομμάτια με το συντελεστή διαχωρισμού « | ». Ύστερα, η android εφαρμογή θα μετατρέψει τα δεδομένα σε bytes, θα λάβει ως

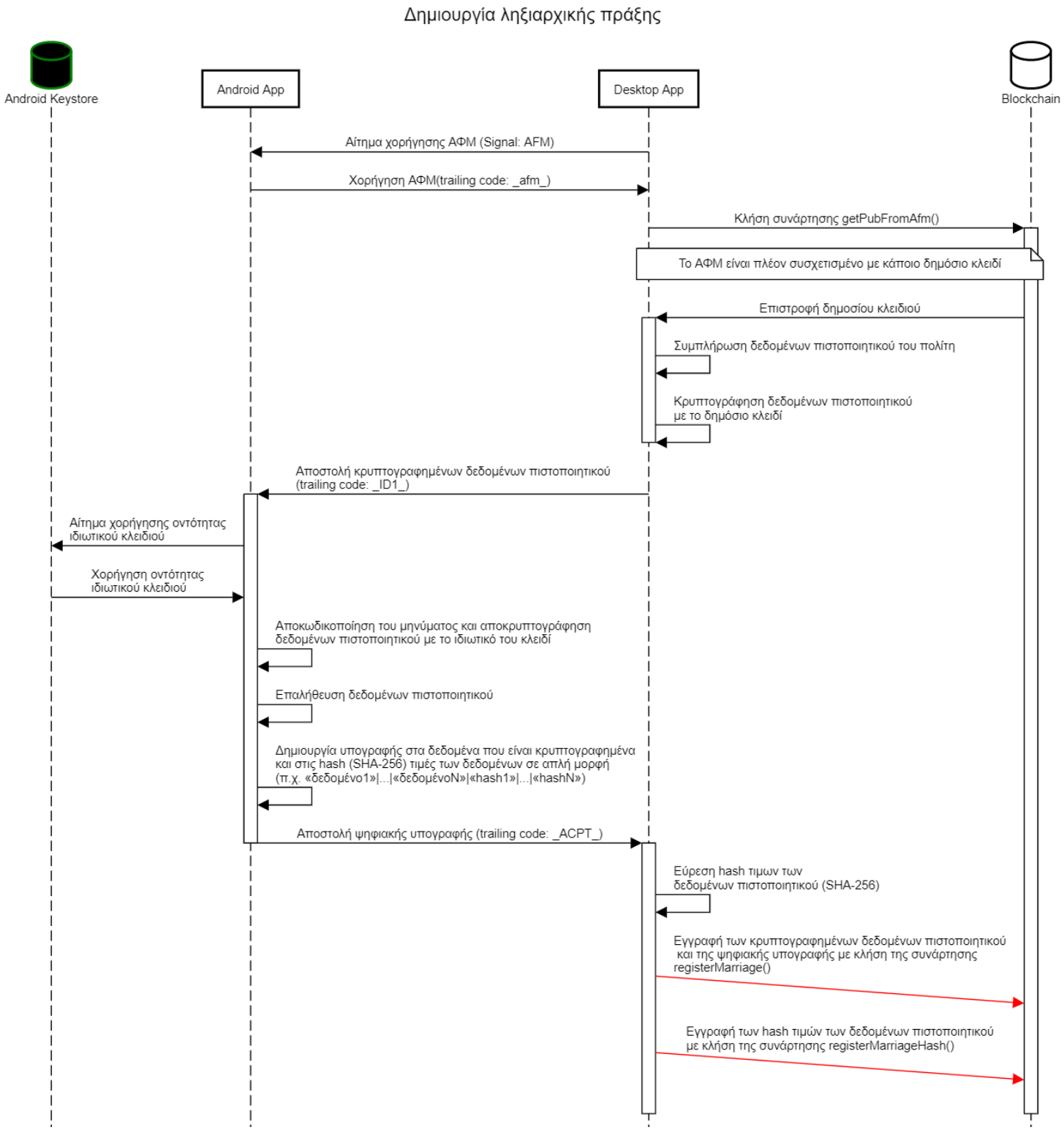
οντότητα το ιδιωτικό κλειδί του πολίτη που υπάρχει στο σύστημα android keystore και θα αποκρυπτογραφήσει ένα προς ένα τα δεδομένα που στάλθηκαν από την εφαρμογή ληξιαρχείου.

5.6.3 Έλεγχος εγκυρότητας δεδομένων από τον πολίτη

Αφού τα δεδομένα αποκρυπτογραφηθούν επιτυχώς, θα εμφανιστούν στην οθόνη της κινητής συσκευής του χρήστη. Από εκεί, ο χρήστης θα πρέπει να επαληθεύσει αν τα στοιχεία που εισήγαγε ο υπάλληλος του ληξιαρχείου είναι πανομοιότυπα με αυτά που του είπε. Σε περίπτωση που δεν είναι, ο πολίτης, πατάει το κουμπί “REJECT” και θα σταλθεί ο κωδικός “RJCT” στην desktop εφαρμογή ώστε να τερματίσει η διαδικασία δημιουργίας πιστοποιητικού γάμου. Αν τα δεδομένα είναι πανομοιότυπα με αυτά που είπε ο πολίτης ώστε να καταχωριστούν, πατάει το κουμπί “ACCEPT” και η διαδικασία συνεχίζεται.

5.6.4 Υπογραφή δεδομένων ψηφιακά και εγγραφή στο blockchain

Μετά την αποδοχή του πολίτη, αυτομάτως η android εφαρμογή κάνει hash τύπου SHA-256 τις τιμές των δεδομένων σε απλή μορφή, και ύστερα τις προσάπτει στο τέλος των κρυπτογραφημένων τιμών με διαχωριστικό χαρακτήρα « | ». Ύστερα, για το τελικό αλφαριθμητικό που παράχθηκε, δημιουργείται ψηφιακή υπογραφή βάσει του ιδιωτικού κλειδιού του πολίτη από το ζεύγος κλειδιών του RSA. Τέλος, η ψηφιακή υπογραφή που δημιουργήθηκε, στέλνεται ως μήνυμα σε μορφή δεκαεξαδικού αλφαριθμητικού έχοντας στο τέλος τη λέξη κλειδί “_ACPT_” στην desktop εφαρμογή. Η desktop εφαρμογή, διαβάζοντας τη λέξη κλειδί “_ACPT_” θα αποθηκεύσει την ψηφιακή υπογραφή και θα την αποθηκεύσει προσωρινά. Θα μετατρέψει τα δεδομένα που έδωσε ο πολίτης σε μορφή hash SHA-256 και θα καλέσει τις συναρτήσεις registerMarriage και registerMarriageHash από το smart contract. Με τη συνάρτηση registerMarriage, θα καταχωρηθούν στο blockchain τα δεδομένα που έδωσε ο πολίτης, κρυπτογραφημένα με το δημόσιο κλειδί του καθώς και η ψηφιακή υπογραφή που έλαβε ο υπάλληλος του ληξιαρχείου. Με τη συνάρτηση registerMarriageHash, θα καταχωρηθούν στο blockchain, τα δεδομένα του πολίτη σε μορφή hash SHA-256. Αν τα δεδομένα καταχωρίστηκαν επιτυχώς στο blockchain, θα εμφανιστεί ανάλογο μήνυμα στην desktop εφαρμογή του ληξιαρχείου.



Εικόνα 16: Αναλυτικό διάγραμμα δημιουργίας πιστοποιητικού

5.7 Τεχνική περιγραφή διαδικαστικού λήψης στοιχείων ληξιαρχικής πράξης

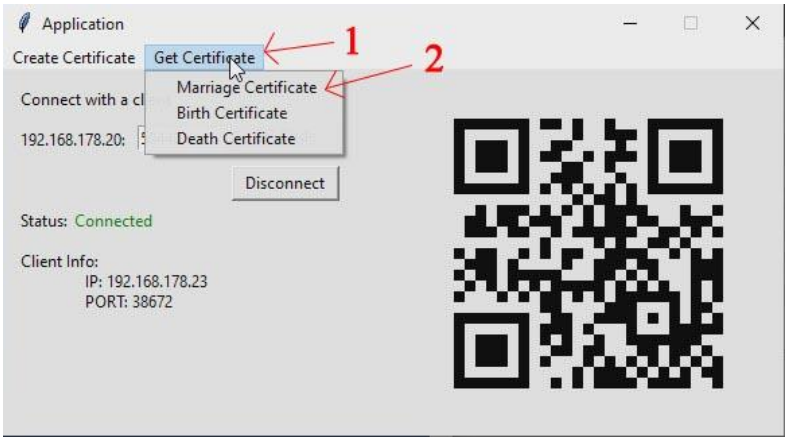
Από τη στιγμή που ο πολίτης δημιούργησε επιτυχώς μια ληξιαρχική πράξη στο ληξιαρχείο (στο παρόν παράδειγμα δημιούργησε ένα πιστοποιητικό γάμου), μπορεί πλέον να το χρησιμοποιήσει σε κάποιο τρίτο οργανισμό που ενδεχομένως χρειάζεται κάποια ή όλα τα δεδομένα αυτού του πιστοποιητικού. Έστω ότι ο πολίτης προκειμένου να ολοκληρώσει κάποια τρίτη διαδικασία, χρειάζεται να δώσει δεδομένα από το πιστοποιητικό που δημιούργησε στο ληξιαρχείο. Θα πρέπει να συνδεθεί στον εκάστοτε τρίτο οργανισμό που χρειάζεται αυτά τα δεδομένα κατά τον ίδιο τρόπο που εξηγήθηκε σε προηγούμενο υποκεφάλαιο.

5.7.1 Διαδικασία σύνδεσης πολίτη με τρίτο οργανισμό

Εφόσον ο πολίτης συνδεθεί με την desktop εφαρμογή του τρίτου οργανισμού (η οποία προορίζεται για τα τους τρίτους οργανισμούς και μπορεί μόνο να ζητήσει δεδομένα από πιστοποιητικά και όχι να δημιουργήσει), θα σταλθεί αυτομάτως από την εφαρμογή του υπαλλήλου προς την android εφαρμογή μήνυμα με τη λέξη κλειδί “AFM” . Όταν η android εφαρμογή το λάβει και αναλύσει την λέξη κλειδί, θα εμφανίσει στην οθόνη του πολίτη ένα πεδίο ώστε να εισάγει το α.φ.μ. του. Αφού το εισάγει και πατήσει το κουμπί “SEND” θα σταλθεί στη desktop εφαρμογή το α.φ.μ. του έχοντας στο τέλος τη λέξη κλειδί “_afm_”. Από εκεί η desktop εφαρμογή θα αναλύσει τη λέξη κλειδί και θα αποθηκεύσει προσωρινά το α.φ.μ. του πολίτη. Ύστερα, θα κληθεί αυτόματα η συνάρτηση getPubFromAfm που υπάρχει στο smart contract ώστε να γίνει έλεγχος αν για αυτό το α.φ.μ. υπάρχει κάποιο δημόσιο κλειδί. Δηλαδή, θα ελεγχθεί αν υπάρχει κάποιος πολίτης καταχωρισμένος με αυτό το α.φ.μ. . Εφόσον, ο πολίτης όπως ειπώθηκε έχει καταχωρήσει τα δεδομένα του στο blockchain, η συνάρτηση αυτή θα επιστρέψει το δημόσιο κλειδί του.

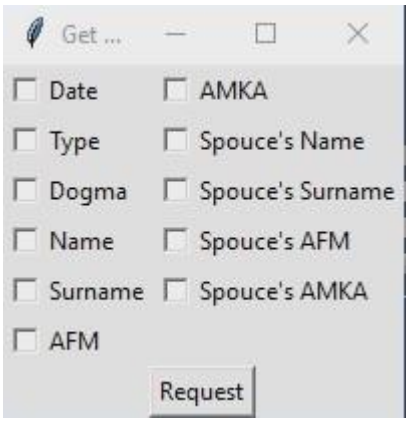
5.7.2 Δημιουργία αιτήματος από τον τρίτο οργανισμό για λήψη δεδομένων πιστοποιητικού

Από εκεί, ο υπάλληλος του τρίτου οργανισμού θα πλοηγηθεί στο μενού της εφαρμογής του πατώντας την επιλογή “Get Certificate” → “Marriage Certificate”.



Εικόνα 17: Βήματα για την δημιουργία αιτήματος λήψης δεδομένων πιστοποιητικού

Σε αυτό το σημείο θα του εμφανιστεί ένα παράθυρο έχοντας όλα τα πεδία που μπορεί να έχει το πιστοποιητικό γάμου σε μορφή check boxes. Με αυτό τον τρόπο, ο υπάλληλος μπορεί να επιλέξει ποια στοιχεία του πιστοποιητικού γάμου του πολίτη είναι χρήσιμα για αυτόν.



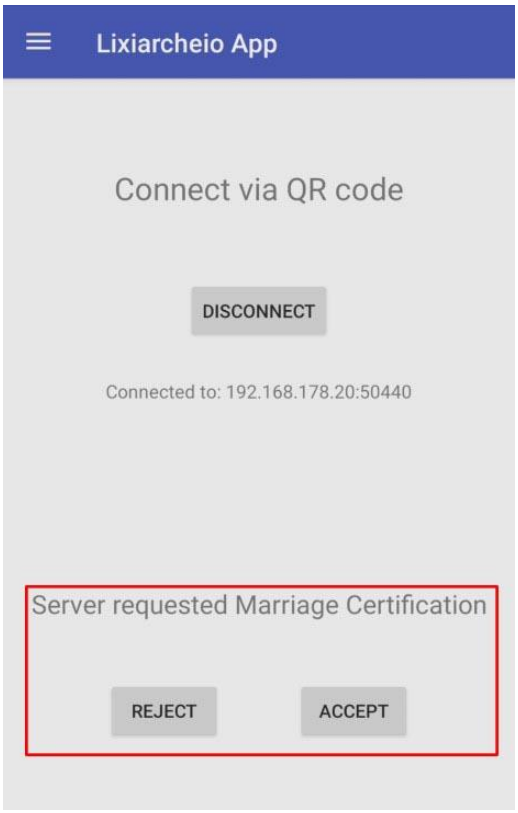
Εικόνα 18: Διαθέσιμα πεδία που μπορεί να εισάγει στην αίτηση ο τρίτος οργανισμός

5.7.3 Μορφοποίηση του αιτήματος για την λήψη δεδομένων πιστοποιητικού

Αφού επιλέξει τα πεδία, θα πατήσει το κουμπί “Request” και θα γίνει αυτομάτως η ανάλυση των επιλογών του. Δηλαδή θα δημιουργηθεί ένα αλφαριθμητικό στο οποίο τα πεδία που επέλεξε ο υπάλληλος αντιπροσωπεύονται με τη τιμή «1» και αυτά που δεν επέλεξε αντιπροσωπεύονται με τη τιμή «0». Το κάθε ψηφίο χωρίζεται με τον χαρακτήρα « | » και στο τέλος του αλφαριθμητικού προστίθεται η λέξη κλειδί «CERT1». Το τελικό αυτό αλφαριθμητικό στέλνεται στην android εφαρμογή του πολίτη και γίνεται ανάλυση της λέξης κλειδί.

5.7.4 Απόφαση του χρήστη για την εξέλιξη της διαδικασίας

Όταν γίνει ανάλυση της λέξης κλειδί «CERT1», η android εφαρμογή θα εμφανίσει ένα μήνυμα αιτήματος χορήγησης δεδομένων πιστοποιητικού γάμου.



Εικόνα 19: Οθόνη χρήστη όταν ληφθεί το αίτημα

Αν ο πολίτης δεν επιθυμεί να δώσει τα δεδομένα, τότε, μπορεί να πατήσει το κουμπί "REJECT" και θα σταλθεί ο κωδικός "RJCT" στην desktop εφαρμογή ώστε να τερματίσει η διαδικασία. Αν επιθυμεί να συνεχίσει τη διαδικασία τότε μπορεί να πατήσει το κουμπί "ACCEPT".

5.7.5 Διαδικασία λήψης πιστοποιητικού στη συσκευή του πολίτη από το blockchain

Εφόσον θελήσει να συνεχιστεί η διαδικασία, τότε, η android εφαρμογή θα χωρίσει τα ψηφία του αλφαριθμητικού στα σημεία με τον χαρακτήρα « | » προκειμένου να γνωστοποιηθούν τα πεδία που επέλεξε ο υπάλληλος. Ύστερα, η android εφαρμογή θα συνδεθεί στο blockchain και θα καλέσει τις συναρτήσεις getMarriageCert1 και getMarriageCert2 που βρίσκονται στο smart contract, ώστε να λάβει τα κρυπτογραφημένα δεδομένα του από το blockchain. Από εκεί θα αποκρυπτογραφήσει το κάθε στοιχείο ξεχωριστά με μία οντότητα του ιδιωτικού του κλειδιού που βρίσκεται στο σύστημα android keystore. Ύστερα θα εμφανιστούν τα δεδομένα του

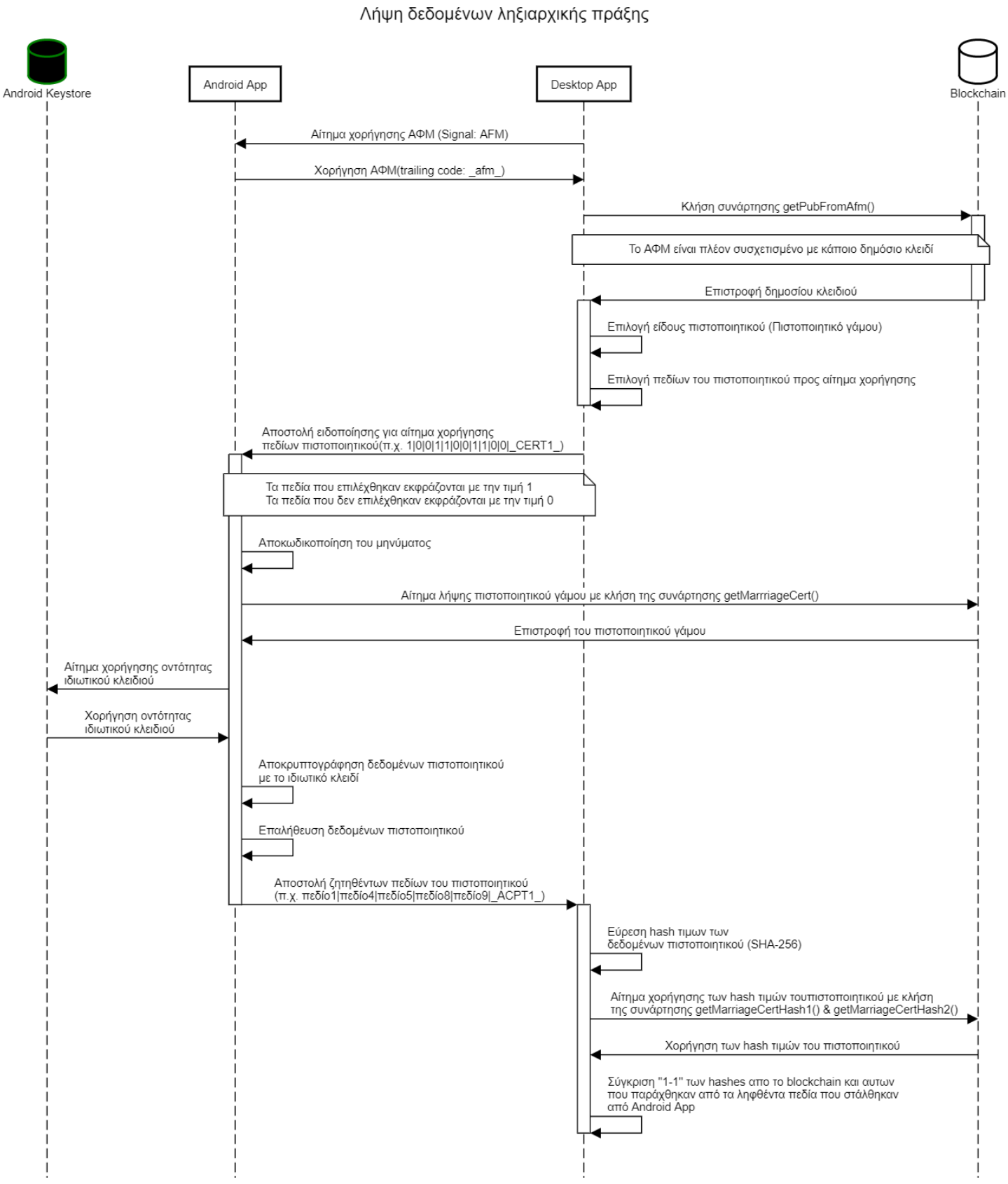
πιστοποιητικού γάμου στην οθόνη του πολίτη. Τα στοιχεία που ζήτησε ο υπάλληλος θα έχουν κανονική μορφή ενώ αυτά που δεν ζήτησε θα είναι κρυμμένα με αστερίσκους (*). Δηλαδή αυτά που είναι κρυμμένα και που δηλαδή, δεν ζήτησε ο υπάλληλος δεν θα σταλθούν προς αυτόν.

5.7.6 Διαδικασία μορφοποίησης των δεδομένων και αποστολή στον τρίτο οργανισμό

Σε επόμενο στάδιο, η android εφαρμογή θα ενοποιήσει τα δεδομένα που ζητήθηκαν από τον υπάλληλο σε ένα αλφαριθμητικό, χωρίζοντας τα με το σύμβολο « | ». Στο τελικό αλφαριθμητικό που θα παραχθεί, θα προστεθεί και η λέξη κλειδί "_ACPT1_" και θα σταλθεί προς την desktop εφαρμογή. Όταν η desktop εφαρμογή αναλύσει τη λέξη κλειδί, θα ξεκινήσει αυτομάτως να χωρίζει το αλφαριθμητικό που λήφθηκε στα σημεία που βρίσκεται ο χαρακτήρας « |».

5.7.7 Διαδικασία επαλήθευσης δεδομένων πιστοποιητικού ως προς την εγκυρότητα

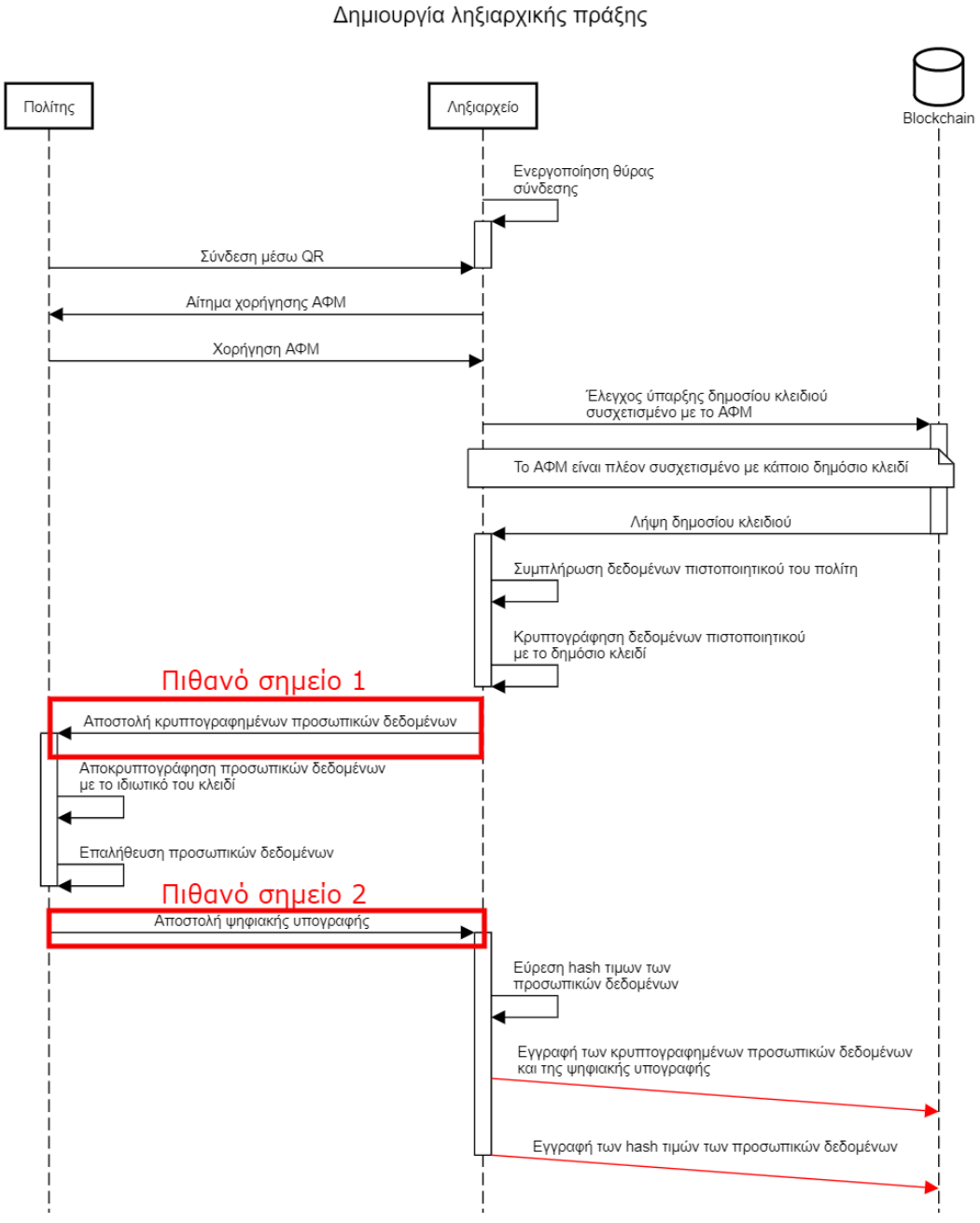
Το κάθε ένα από τα χωρισμένα δεδομένα που λήφθηκαν θα μετατραπεί σε μορφή hash SHA-256. Μετά, η desktop εφαρμογή θα καλέσει τις συναρτήσεις getMarriageCertHash1 και getMarriageCertHash2 που βρίσκονται στο smart contract ώστε να λάβει τα hashes των δεδομένων που είχαν καταχωριστεί κατά τη δημιουργία του πιστοποιητικού γάμου του πολίτη. Θα απομονώσει και θα μετατρέψει τα hashes των πεδίων που ζήτησε ο υπάλληλος σε δεκαεξαδική μορφή και θα τα συγκρίνει με τα hashes των δεδομένων που έστειλε ο πολίτης από την android εφαρμογή του. Αν είναι ένα προς ένα πανομοιότυπα τότε τα δεδομένα που έστειλε ο πολίτης είναι αυθεντικά. Αν κάποιο hash διαφέρει, τότε, το συγκεκριμένο δεδομένο δεν θα είναι αυθεντικό δηλαδή δεν θα είναι ίδιο με αυτό που καταχωρίστηκε κατά τη διαδικασία δημιουργίας του πιστοποιητικού γάμου.



Εικόνα 20: Αναλυτικό διάγραμμα διαδικασίας λήψης δεδομένων πιστοποιητικού

6 Ανάλυση Ασφαλείας

Ο βασικός στόχος του προτεινόμενου συστήματος είναι η διασφάλιση των βασικών ιδιοτήτων ασφαλείας, όσον αφορά την επικοινωνία των πολιτών/χρηστών με το ληξιαρχείο καθώς και την αποθήκευση των στοιχείων των πιστοποιητικών. Ο σχεδιασμός του συστήματος έχει εξαρχής λάβει υπόψη την κάλυψη των πιθανών ευπαθειών, έτσι ώστε να μειωθεί ή εξαλειφθεί η πιθανότητα κάποιος τρίτος να υποκλέψει πληροφορίες κάποιου χρήστη ή κάποιος πολίτης να επιδείξει ένα πλαστό πιστοποιητικό. Παρακάτω παρουσιάζονται τα πιθανά ευπαθή σημεία και αναλύεται το πως το σύστημα επιτυγχάνει να διασφαλίσει την ορθή λειτουργία του.



Εικόνα 21: Πιθανά ευπαθή σημεία

Πιθανό σημείο 1: Προστασία εμπιστευτικότητας κατά την αποστολή των προσωπικών δεδομένων

Σενάριο: Το πρώτο πιθανό σενάριο αφορά στην απόπειρα ενός τρίτου χρήστη να υποκλέψει τα δεδομένα που στέλνονται από το Ληξιαρχείο στον πολίτη κατά τη δημιουργία μια ληξιαρχικής πράξης, προκειμένου ο πολίτης να τα επιβεβαιώσει.

Αντιμετώπιση: Στη περίπτωση αυτή, τα στοιχεία δεν μπορούν να φανερωθούν ακόμη και αν κάποιος τρίτος έχει πρόσβαση στο κανάλι επικοινωνίας. Αυτό συμβαίνει διότι τα δεδομένα στέλνονται προς τον πολίτη κρυπτογραφημένα με το δημόσιο κλειδί του και μπορεί να τα αποκρυπτογραφήσει μόνο αυτός με το ιδιωτικό του κλειδί.

Πιθανό σημείο 1: Προστασία ακεραιότητας κατά την αποστολή των προσωπικών δεδομένων

Σενάριο: Στο ίδιο σημείο κάποιος τρίτος με πρόσβαση στο κανάλι επικοινωνίας θα μπορούσε να μεταβάλλει τα δεδομένα με σκοπό να καταστήσει την υπηρεσία μη λειτουργική ή να εξαπατήσει τον χρήστη.

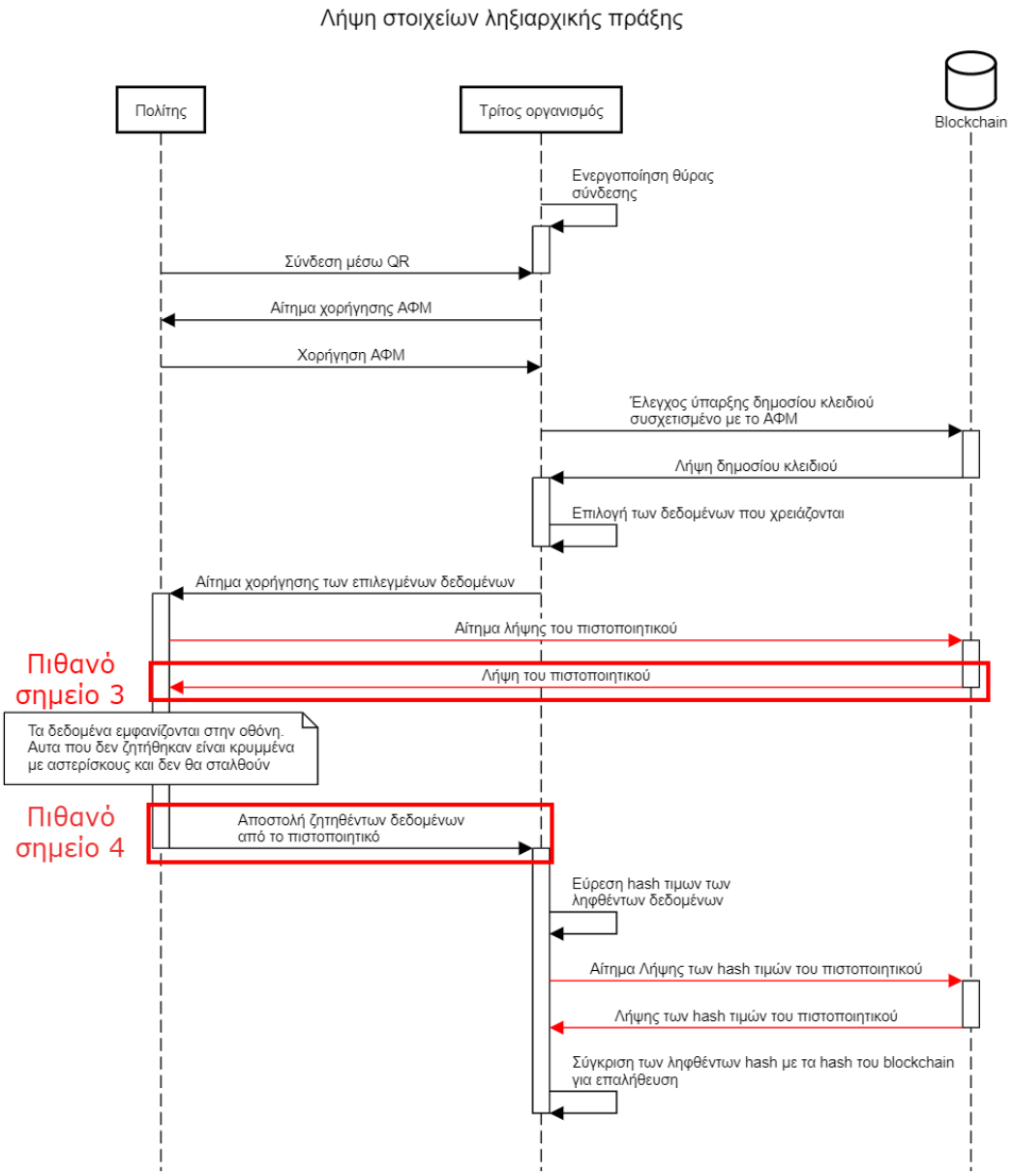
Αντιμετώπιση: Στην περίπτωση αυτή, η συσκευή του πολίτη θα προσπαθούσε να αποκρυπτογραφήσει μια πληροφορία η οποία είναι μη έγκυρη, έτσι ο αλγόριθμος αποκρυπτογράφησης στην χειρότερη περίπτωση δεν θα αποκρυπτογραφούσε τίποτα λόγω εσφαλμένων byte και στην καλύτερη περίπτωση να έβγαζε λάθος αποτέλεσμα αποκρυπτογράφησης όπου ο πολίτης εμφανώς θα το απόρριπτε κατά την επαλήθευση.

Πιθανό σημείο 2: Προστασία ακεραιότητας κατά την αποστολή της ψηφιακής υπογραφής

Σενάριο: Το δεύτερο πιθανό σενάριο αφορά την απόπειρα να επέμβει κάποιος τρίτος χρήστης κατά την αποστολή της ψηφιακής υπογραφής. Δηλαδή, να μεταβάλλει την ψηφιακή υπογραφή που στέλνεται από τον πολίτη προς το ληξιαρχείο.

Αντιμετώπιση: Σε αυτή τη περίπτωση, ο υπάλληλος του ληξιαρχείου έχει ακόμη τα αυθεντικά δεδομένα που του είπε ο πολίτης οπότε ο υπάλληλος του ληξιαρχείου μπορεί να τα επαληθεύσει έχοντας το δημόσιο κλειδί του πολίτη.

Ακόμη δύο σημεία που θα αναλυθούν είναι κατά την διαδικασία ανάκτησης δεδομένων από ένα πιστοποιητικό.



Εικόνα 22: Πιθανά ευπαθή σημεία

Πιθανό σημείο 3: Προστασία εμπιστευτικότητας κατά την λήψη του πιστοποιητικού από το blockchain

Σενάριο: Αυτό το σενάριο αφορά την απόπειρα υποκλοπής των δεδομένων από κάποιον τρίτο, όταν ο χρήστης κατεβάσει κάποια ληξιαρχική πράξη από το blockchain.

Αντιμετώπιση: Σε αυτό το σενάριο ο τρίτος δεν θα μπορέσει να πάρει πρόσβαση στις πληροφορίες διότι τα δεδομένα είναι κρυπτογραφημένα ακόμη και κατά την αποθήκευσή τους στο blockchain.

Πιθανό σημείο 4: Προστασία ακεραιότητας κατά την αποστολή των προσωπικών δεδομένων προς το ληξιαρχείο

Σενάριο: Το τελευταίο σενάριο αφορά την απόπειρα μετατροπής των δεδομένων κατά την αποστολή τους στο ληξιαρχείο από τον χρήστη. Δηλαδή, όταν ο χρήστης στέλνει τα δεδομένα που ζήτησε το ληξιαρχείο ή ένας τρίτος οργανισμός από τη ληξιαρχική

του πράξη. Τα δεδομένα δεν μπορούν να φανούν σε κάποιον τρίτο διότι είναι κρυπτογραφημένα. Όμως σε αυτό το σενάριο αναλύουμε το ενδεχόμενο ο επιτιθέμενος να είναι ο ίδιος ο χρήστης ή κάποιος που έχει πρόσβαση στην εφαρμογή του χρήστη. Σε αυτή τη περίπτωση μπορεί να στείλει άλλα δεδομένα κρυπτογραφημένα με το ιδιωτικό κλειδί του πολίτη.

Αντιμετώπιση: Μία τέτοια κακόβουλη πράξη θα απορριφθεί διότι όταν φτάσουν τα δεδομένα στον δέκτη, αυτομάτως θα ληφθούν τα hashes των δεδομένων που δημιουργήθηκαν κατά την εγγραφή του πιστοποιητικού. Έτσι θα συγκριθούν τα hashes των τιμών που έστειλε ο χρήστης με αυτά που υπάρχουν στο blockchain. Αν είναι διαφορετικά, τότε τα δεδομένα έχουν φθαρεί.

7 Συμπεράσματα

Η εργασία αυτή είχε ως σκοπό τη δημιουργία ενός συστήματος που αφορά την αλληλεπίδραση μεταξύ των πολιτών, των ληξιαρχείων και τρίτων οργανισμών που σχετίζονται έμμεσα με ληξιαρχικές πράξεις πολιτών. Η ύπαρξη ενός τέτοιου συστήματος επιταχύνει τον χρόνο που χρειάζεται να πραγματοποιηθούν σχετικά διαδικαστικά απαλλάσσοντας τόσο τον πολίτη, όσο και τον υπάλληλο από την γραφειοκρατία. Ένα από τα κύρια χαρακτηριστικά του συστήματος είναι η αποκεντρωμένη υλοποίηση του, βασισμένη σε ένα ιδιωτικό Ethereum blockchain. Με αυτό τον τρόπο αποφεύγεται η συλλογή και αποθήκευση των προσωπικών δεδομένων των πολιτών σε ένα σημείο. Η παρουσία ενός μεσολαβητή για την προσπέλαση των προσωπικών δεδομένων σταματάει να υπάρχει και ο χρήστης αποκτάει την πλήρη πρόσβαση στα προσωπικά του δεδομένα. Τα δεδομένα αποθηκεύονται με πλήρη διαύγεια ως προς τον χρήστη και η άντληση των δεδομένων από τρίτους οργανισμούς χρήζει απαραίτητη την συναίνεση του ίδιου του πολίτη. Τα προσωπικά δεδομένα του πολίτη διαχειρίζονται και μεταφέρονται κρυπτογραφημένα ώστε να αποφευχθούν όσο το δυνατόν περισσότερα σενάρια υποκλοπής και αλλοίωσης δεδομένων από πιθανόν κακόβουλες επιθέσεις. Ένα ακόμη αξιοσημείωτο χαρακτηριστικό είναι η μεμονωμένη αποστολή προσωπικών δεδομένων. Για μία διαδικασία ενός τρίτου οργανισμού που χρειάζεται κάποια δεδομένα από ένα πιστοποιητικό πολίτη, δεν είναι απαραίτητη η φανέρωση όλων των δεδομένων του πιστοποιητικού αλλά μόνο η φανέρωση των απαραίτητων δεδομένων για την διαδικασία. Ένας από τους βασικούς γνώμονες που λήφθηκαν υπόψιν κατά την υλοποίηση της εφαρμογής που έχει ο χρήστης στο κινητό του, είναι η απλότητα και η ιδιότητα να είναι φιλικό ως προς τον χρήστη. Με αυτό τον τρόπο, ο πολίτης δεν χρειάζεται να έχει κάποια προηγμένη γνώση στο αντικείμενο

αυτό. Τα βήματα για την πλήρη χρήση της εφαρμογής είναι όσο τον δυνατόν πιο απλά χωρίς να συσχετίζουν τον χρήστη με τις πολύπλοκες διαδικασίες που εκτελούνται στο παρασκήνιο.

Το παρόν σύστημα δημιουργήθηκε και χρησιμοποιήθηκε πλήρως ώστε να αποδειχθούν τα παραπάνω. Ωστόσο, βρίσκεται σε ένα πρώιμο στάδιο και μπορεί να δεχθεί αρκετές βελτιστοποιήσεις ούτως ώστε να είναι πιο ευέλικτο, ασφαλές, και γρήγορο. Κάποιες από τις πιθανόν μελλοντικές βελτιώσεις είναι:

- Η ένταξη περισσότερων πεδίων που απαρτίζουν μια ληξιαρχική πράξη. Τα πεδία που υπάρχουν ήδη είναι λίγα και χρησιμοποιήθηκαν ενδεικτικά. Στη πραγματικότητα υπάρχουν περισσότερα.
- Η ένταξη περισσότερων ληξιαρχικών πράξεων. Αυτή τη στιγμή το σύστημα υποστηρίζει τρία πιστοποιητικά: Γάμου, Γέννησης και Θανάτου.
- Η υποστήριξη κοινής χρήσης πιστοποιητικού μεταξύ δύο πολιτών. Για παράδειγμα, η ληξιαρχική πράξη γάμου να δημιουργείται ταυτόχρονα και στα δύο άτομα. Αποτελεί ένα πρόβλημα που χρειάζεται λύση διότι τα δεδομένα κρυπτογραφούνται και αποκρυπτογραφούνται σύμφωνα με ένα κλειδί που ανήκει σε έναν πολίτη.
- Η προσθήκη κρυπτογράφησης μηνυμάτων στο κανάλι επικοινωνίας μεταξύ του πολίτη και του ληξιαρχείου/τρίτου οργανισμού
- Η πιο εκτεταμένη πειραματική δοκιμή του συστήματος με σκοπό την επισκόπηση του κατά πόσον το προτεινόμενο σύστημα θα μπορούσε να ανταποκριθεί στις απαιτήσεις που θα προέκυπταν αν ο φόρτος των εισερχόμενων αιτημάτων αυξανόταν σημαντικά.

Βιβλιογραφία

1. Singhal, Bikramaditya, Gautam Dhameja, και Priyansu Sekhar Panda. *Beginning Blockchain*. Berkeley, CA: Apress, 2018. https://doi.org/10.1007/978-1-4842-3444-0.

2. Yaga, Dylan, Peter Mell, Nik Roby, και Karen Scarfone. 'Blockchain Technology Overview'. Gaithersburg, MD: National Institute of Standards and Technology, Οκτώβριος 2018. https://doi.org/10.6028/NIST.IR.8202.

3. 'Peer-to-peer'. Στο *Βικιπαίδεια*, 24 Απρίλιος 2020. https://el.wikipedia.org/w/index.php?title=Peer-to-peer&oldid=8202757.

4. IEvangelist. 'Ensuring Data Integrity with Hash Codes'. Ημερομηνία πρόσβασης 11 Ιούνιος 2021. https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes.

5. 'Cryptographic Nonce'. Στο *Wikipedia*, 4 Μάιος 2021. https://en.wikipedia.org/w/index.php?title=Cryptographic_nonce&oldid=1021348196.

6. 'Bitcoin'. Στο *Wikipedia*, 11 Ιούνιος 2021. https://en.wikipedia.org/w/index.php?title=Bitcoin&oldid=1027984181.

7. 'Proof of Work'. Στο *Wikipedia*, 21 Μάιος 2021. https://en.wikipedia.org/w/index.php?title=Proof_of_work&oldid=1024374682.

8. Guegan, Dominique. 'Public Blockchain versus Private Blockhain', χ.χ., 8.

9. Wang, Dan, Jindong Zhao, και Yingjie Wang. 'A Survey on Privacy Protection of Blockchain: The Technology and Application'. *IEEE Access* 8 (2020): 108766–81. https://doi.org/10.1109/ACCESS.2020.2994294.

10. Oliva, Gustavo A., Ahmed E. Hassan, και Zhen Ming Jiang. 'An Exploratory Study of Smart Contracts in the Ethereum Blockchain Platform'. *Empirical Software Engineering* 25, τχ. 3 (Μάιος 2020): 1864–1904. https://doi.org/10.1007/s10664-019-09796-5.

11. Niranjanamurthy, M., B. N. Nithya, και S. Jagannatha. 'Analysis of Blockchain Technology: Pros, Cons and SWOT'. *Cluster Computing* 22, τχ. S6 (Νοέμβριος 2019): 14743–57. https://doi.org/10.1007/s10586-018-2387-5.

12. Vujicic, Dejan, Dijana Jagodic, και Sinisa Randic. 'Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview'. Στο *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 1–6. East Sarajevo: IEEE, 2018. https://doi.org/10.1109/INFOTEH.2018.8345547.

13. Swan, Melanie. 'Blockchain Thinking : The Brain as a Decentralized Autonomous Corporation [Commentary]'. *IEEE Technology and Society Magazine* 34, τχ. 4 (Δεκέμβριος 2015): 41–52. https://doi.org/10.1109/MTS.2015.2494358.

14. Xu, Quanqing, Zhiwen Song, Rick Siow Mong Goh, και Yongjun Li. 'Building an Ethereum and IPFS-Based Decentralized Social Network System'. Στο *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, 1–6. Singapore, Singapore: IEEE, 2018. https://doi.org/10.1109/PADSW.2018.8645058.

15. Sward, Andrew, Ivy Vecna, και Forrest Stonedahl. 'Data Insertion in Bitcoin's Blockchain'. *Ledger* 3 (3 Απρίλιος 2018). https://doi.org/10.5195/ledger.2018.101.

16. Chugunov, Andrei, Yuri Misnikov, Evgeny Roshchin, και Dmitrii Trutnev, επιμ. *Electronic Governance and Open Society: Challenges in Eurasia: 5th International Conference, EGOSE 2018, St. Petersburg, Russia, November 14-16, 2018, Revised Selected Papers*. τ. 947. Communications in Computer and Information Science. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-13283-5.

17. Pardo, Theresa A., και Yuanfu Jiang. 'Electronic Governance and Organizational Transformation'. Στο *Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance - ICEGOV '07*, 99. Macao, China: ACM Press, 2007. https://doi.org/10.1145/1328057.1328081.

18. Buterin, Vitalik. 'Ethereum: Platform Review', χ.χ., 45.

19. Alessi, M, A Camillo, E Giangreco, M Matera, S Pino, και D Storelli. 'Make Users Own Their Data: A Decentralized Personal Data Store Prototype Based on Ethereum and IPFS', χ.χ., 7.

20. Guegan, Dominique. 'Public Blockchain versus Private Blockhain', χ.χ., 8.

21. Davies, Jim, Tomasz Janowski, Adegboyega Ojo, και Aadya Shukla. ‘Technological Foundations of Electronic Governance’. Στο *Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance - ICEGOV ’07*, 5. Macao, China: ACM Press, 2007. https://doi.org/10.1145/1328057.1328063.

22. Gürsoy, Gamze, Charlotte M. Brannon, και Mark Gerstein. ‘Using Ethereum Blockchain to Store and Query Pharmacogenomics Data via Smart Contracts’. *BMC Medical Genomics* 13, τχ. 1 (Δεκέμβριος 2020): 74. https://doi.org/10.1186/s12920-020-00732-x.

23. Allen, Christopher. ‘The path to self-sovereign identity (2016)’. *Url: http://www. lifewithalacrity. com/2016/04/the-path-to-self-soverereignidentity. html*, 2020.

24. Angraal, Suveen, Harlan M Krumholz, και Wade L Schulz. ‘Blockchain Technology’, χ.χ., 3.

25. Buterin, Vitalik. ‘Chain interoperability’. *R3 Research Paper* 9 (2016).

26. Ferdous, Md Sadek, Farida Chowdhury, και Madini O. Alassafi. ‘In Search of Self-Sovereign Identity Leveraging Blockchain Technology’. *IEEE Access* 7 (2019): 103059–79. https://doi.org/10.1109/ACCESS.2019.2931173.

27. Giovanni, Pietro De. ‘Blockchain and smart contracts in supply chain management: A game theoretic model’. *International Journal of Production Economics* 228 (2020): 107855. https://doi.org/10.1016/j.ijpe.2020.107855.

28. Heawood, Jonathan. ‘Pseudo-Public Political Speech: Democratic Implications of the Cambridge Analytica Scandal’. *Information Polity* 23, τχ. 4 (10 Δεκέμβριος 2018): 429–34. https://doi.org/10.3233/IP-180009.

29. Huh, Seyoung, Sangrae Cho, και Soohyung Kim. ‘Managing IoT Devices Using Blockchain Platform’. Στο *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 464–67. Pyeongchang, Kwangwoon Do, South Korea: IEEE, 2017. https://doi.org/10.23919/ICACT.2017.7890132.

30. Mettler, Matthias. ‘Blockchain Technology in Healthcare: The Revolution Starts Here’. Στο *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)*, 1–3. Munich, Germany: IEEE, 2016. https://doi.org/10.1109/HealthCom.2016.7749510.

31. Moudoud, Hajar, Soumaya Cherkaoui, και Lyes Khoukhi. ‘An IoT Blockchain Architecture Using Oracles and Smart Contracts: The Use-Case of a Food Supply Chain’. Στο *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 1–6. Istanbul, Turkey: IEEE, 2019. https://doi.org/10.1109/PIMRC.2019.8904404.

32. Papadodimas, Georgios, Georgios Palaiokrasas, Antonios Litke, και Theodora Varvarigou. ‘Implementation of Smart Contracts for Blockchain Based IoT Applications’. Στο *2018 9th International Conference on the Network of the Future (NOF)*, 60–67. Poznan: IEEE, 2018. https://doi.org/10.1109/NOF.2018.8597718.

33. Stokkink, Quinten, και Johan Pouwelse. ‘Deployment of a Blockchain-Based Self-Sovereign Identity’. Στο *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1336–42. Halifax, NS, Canada: IEEE, 2018. https://doi.org/10.1109/Cybermatics_2018.2018.00230.

34. Wood, Gavin και others. ‘Ethereum: a secure decentralised generalised transaction ledger (2014)’, 2017.

35. Zmaznev, Egor. ‘BITCOIN AND ETHEREUM EVOLUTION’, χ.χ., 66.

36. Alsayed Kassem, Jamila, Sarwar Sayeed, Hector Marco-Gisbert, Zeeshan Pervez, και Keshav Dahal. ‘DNS-IdM: A blockchain identity management system to secure personal data sharing in a network’. *Applied Sciences* 9, τχ. 15 (2019): 2953.

37. Giovanni, Pietro De. ‘Blockchain and smart contracts in supply chain management: A game theoretic model’. *International Journal of Production Economics* 228 (2020): 107855. https://doi.org/10.1016/j.ijpe.2020.107855.